Pós-Graduação em Ciência da Computação

Marcos Antonio Costa Corrêa Júnior

Solid State Drive como fonte de prova no Processo Penal do Brasil

Universidade Federal de Pernambuco
posgraduacao@cin.ufpe.br
http://cin.ufpe.br/~posgraduacao

Recife
2019

Marcos Antonio Costa Corrêa Júnior

Solid State Drive como fonte de prova no Processo Penal do Brasil

Tese de Doutorado apresentada ao Programa de Pós-graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Doutor em Ciência da Computação.

Área de Concentração: forense computacional
Orientador: Ruy José Guerra Barretto de Queiroz

Recife
2019

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

C824s Corrêa Júnior, Marcos Antonio Costa
Solid state drive como fonte de prova no processo penal do Brasil / Marcos Antonio Costa Corrêa Júnior. – 2019.
149 f.: il., fig., tab.

Orientador: Ruy José Guerra Barretto de Queiroz.
Tese (Doutorado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2019.
Inclui referências e apêndices.

1. Ciência da informação. 2. Forense computacional. 3. Recuperação de dados. I. Queiroz, Ruy José Guerra Barretto de (orientador). II. Título.

004 CDD (23. ed.) UFPE- MEI 2019-113

Marcos Antonio Costa Corrêa Júnior

"***Solid State Drive* como fonte de prova no Processo Penal do Brasil"**

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Doutor em Ciência da Computação.

Aprovado em: 12/03/2019.

Orientador: Ruy José Guerra Barretto de Queiroz

BANCA EXAMINADORA

Prof. Dr. Djamel Fawzi Hadj Sadok
Centro de Informática / UFPE

Prof. Dr. Vinícius Cardoso Garcia
Centro de Informática / UFPE

Prof. Dr. Rodrigo Elia Assad
Departamento de Estatística e Informática / UFRPE

Prof. Dr. Ricardo Cícero de Carvalho Rodrigues
Centro Universitário do Vale do Ipojuca / UNIFAVIP

Profa. Dra. Cinthia Obladen de Almeida Freitas
Programa de Pós Graduação em Informática Aplicada / PUC/PR

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, Pai todo-poderoso, criador de todas as coisas, que me concedeu a graça de existir e que sempre iluminou meu caminho.

À minha família - Mariana, Marquito e Malu - pelo apoio durante os vários momentos difíceis enfrentados durante o período que cursei o doutorado, à minha sogra Audecy.

Aos meus pais - Marcos e Maria - que me forneceram subsídios para que eu chegasse até aqui, às minhas irmãs - Diana e Ana Paula.

Ao meu orientador, Ruy José Guerra Baretto de Queiroz, pela confiança no meu trabalho, pela tranquilidade com que sempre me recebeu, ajudando-me a sempre acreditar que iria dar certo.

Aos demais professores que participaram de minha formação e, com suas disciplinas, contribuíram para a qualidade de minha formação.

Ao Centro de Informática da Universidade Federal de Pernambuco pela infraestrutura e por ser um Centro de Excelência que oferece aos alunos a possibilidade de uma formação de altíssimo nível.

RESUMO

Este trabalho tem por ideia inicial estudar as dificuldades de recuperação e de comprovação da mesmidade dos dados durante procedimentos de forense computacional em drives de estado sólido. A partir do estudo dessas unidades de memória secundária, surgiram questionamentos quanto ao funcionamento interno e a possibilidade de destruição completa das evidências dentro de um SSD que possibilitaram o estabelecimento de uma problematização. O enriquecimento das informações e a definição do problema foram possíveis através da análise de documentos encontrados na literatura, mencionados em grande no Capítulo 2 - Trabalhos Relacionados, os quais forneceram subsídio para o início de uma investigação mais aprofundada, de modo a responder às indagações e a construir técnicas e metodologias que possam trazer solução para a problemática em geral, ou para casos isolados. A partir do problema, surgiu a necessidade de ampliar a pesquisa na literatura técnica, estudar o contexto jurídico e também realizar trabalhos experimentais. Esse trabalho colabora para a resposta às dúvidas que possuem repercussão na atividade forense computacional tanto do ponto de vista técnico quanto jurídico. Este trabalho também pauta-se por nortear novas pesquisas, por criar procedimentos operacionais que contribuem para a padronização da atividade pericial. Como contribuições, pode-se enumerar a proposição de um novo modelo de investigação forense computacional, a sugestão de um procedimento operacional padrão específico para recuperação forense de dados em *solid state drive* (SSD) e, por fim, a demonstração prática de que apesar dos procedimentos internos de otimização do SSD destruírem dados apagados, é possível em muitos casos a recuperação de arquivos apagados ou de fragmentos deles que não tenham sido sobrescritos.

Palavras-chaves: Forense computacional. SSD. Recuperação de dados.

ABSTRACT

The main idea of this work is to study the difficulties encountered in digital forensic for dealing with data stored persistently in solid state drives. From the study of this auxiliary memory, there are questions unsolved in computer forensics. A deeper knowledge and the problem definition were made possible through the analysis of documents found in the literature, which provided subsidies for the start of further investigation, in order to answer questions and build techniques and methodologies that can bring solution to the problem in general or individual cases. Arising then the need to expand research in technical literature and conducting experimental work. This work must contributes to answer the questions that have repercussions in computational forensics activity in technical and legal context. This work is also guided by new research, for creating operational procedures that contribute to the standardization of expert activity. As contributions, we can enumerate a proposition of a specific standard operating procedure for forensic data retrieval in SSD, and finally the practical demonstration that despite internal SSD optimization procedures to destroy deleted data, it is possible in many cases to recover deleted files or fragments of them that have not been overwritten.

Keywords: Digital forensics. SSD. Data retrieval.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O surgimento da *World Wide Web*, dos smartphones, da computação em nuvem, das diversas redes sociais, dos serviços on-line (bancários, comerciais, governamentais) afetaram profundamente e permanecem influenciando a vida das pessoas.

Não há uma previsão que indique uma parada no crescimento da tecnologia digital e na oferta de serviços. Esse mundo altamente conectado mudou as relações interpessoais, bem como as das organizações, muitas vezes, para melhor. Em contrapartida, a tecnologia digital cria oportunidades novas para os criminosos.

O mundo se encontra em contínua reestruturação. Na sociedade atual há muita comunicação ocorrendo em virtude das redes de computadores. Junto com toda essa conectividade, a tecnologia vem alterando a forma como as pessoas interagem entre si, com governos, com empresas. A evolução contínua do comportamento humano, das diversas formas de interação e do acesso a produtos e serviços, como resultado de inovações tecnológicas, oportunizou-se um propício ambiente para o crime e para comportamentos que subvertem o projeto benéfico original do uso de dispositivos computacionais (computadores, *smartphones*, *tablets*) e da Internet.

Crimes que utilizam de alguma forma computadores começaram a crescer no final dos anos 90 e no início do ano 2000, esse crescimento ainda continua. De sorte que para combater essa nova criminalidade, um ramo da ciência chamado de forense computacional se desenvolveu. Além disso, com o aumento e diversificação do número de tecnologias, os dispositivos os quais podem ser usados na coleta de dados que possam elucidar crimes cresceu, desse modo o termo forense digital (do inglês *digital forensic*) parece ser mais adequado e é mais utilizado internacionalmente. Portanto, embora alguns autores façam uma distinção da forense digital em diversas categorias (conforme será detalhado na Seção 4), neste trabalho os termos forense computacional e forense digital serão tratados como sinônimos.

Para Raghavan em (RAGHAVAN, 2013), forense digital é o ramo da ciência que envolve a aplicação de princípios científicos para a investigação de artefatos presentes em um ou mais dispositivos digitais cujo objetivo é o de entender e reconstruir a sequência de eventos que deve ter precedido a geração de tais artefatos.

A forense digital experimenta um desenvolvimento fantástico, criando uma sofisticação em redor da atividade. A evidência que a forense digital recebe, retira-a de uma posição secundária na qual era tratada como uma atividade de nicho para colocá-la em um patamar de importância. A atividade demonstra ser capaz de recuperar evidências que permanecem em dispositivos computacionais e em tráfegos de redes de forma a servir de prova em um tribunal (BEEBE, 2009). Essa exposição tem a sua face negativa, junto com a enorme divulgação da atividade - principalmente em séries de TV - começa-se a

retratar de forma distorcida o dia-a-dia desse serviço investigativo, gerando o chamado "efeito CSI". Este termo é citado por Thomas em (THOMAS, 2006), Shelton e outros em (SHELTON; KIM; BARAK, 2006), Scweitzer e Saks em (SCHWEITZER; SAKS, 2007) para descrever a situação em que se atribui uma crença exagerada e, às vezes, falsa acerca das ciências forenses.

Está claro que a Internet também proporciona um local para que pessoas se envolvam em crimes e em outras atividades escusas, de tal forma que esses crimes, bem como a troca de informações não seriam possíveis através de outro modo no mundo real.

Ao longo dos últimos anos, houve um aumento substancial no uso da tecnologia pelos criminosos de rua e de novas aplicações da tecnologia para criar formas de crime que não existiam anteriormente. Marc Goodman em 2012, em um vídeo feito para o TED Talk (GOODMAN, 2012), mostrou várias situações de emprego de tecnologia por parte de criminosos mundo afora. Mais recentemente, em 2015, escreveu o livro *Future Crimes* (GOODMAN, 2015) que se tornou um *best-seller*. Para Goodman, as tecnologias ao longo do tempo têm facilitado a comunicação entre criminosos e, ao mesmo tempo dificultado o trabalho investigativo e de rastreamento por parte das autoridades competentes.

Mas não há apenas maior dificuldade de investigação e de rastreamento, o Direito e a tecnologia não trabalham de forma síncrona, a forma e o tempo que o Direito leva para se apropriar, para tipificar novas condutas não acompanham a evolução da tecnologia.

Em 2018, um relatório da McAfee e do *Center for Strategic and International Studies* (CSIS) revelou que o custo do crime cibernético foi estimado em 0,8% do PIB global ou US$600bi, o estudo destacou que as empresas precisam levar mais a sério o impacto econômico do crime, especialmente na Europa, onde o impacto do cibercrime foi mais alto, com 0,84% do PIB regional. As razões para o crescimento do cibercrime, ainda segundo esse relatório, são a rápida adoção de novas tecnologias, aumento do número de usuários on-line, aumento de "centros" de cibercrime (Brasil, Índia, Coreia do Norte e Vietnã foram incluidos), crescente sofisticação financeira, monetização do sequestro de dados e de cibercrimes com as criptomoedas(LEWIS, 2018).

De acordo com outro estudo, dessa vez da empresa Bromium e publicado na *Computer Weekly* por Warwick Ashford, o cibercrime está se tornando uma atividade tão rentável que os cibercriminosos mais bem sucedidos chegam a ganhar US$2 milhões por ano, quase o mesmo salário de CEOs das maiores organizações (ASHFORD, 2018).

Além do crescimento do crime cibernético, há um cenário em que quase todos os crimes, sejam eles cometidos utilizando meios computacionais ou não, incorporam alguma forma de evidências digitais (filmagens de câmeras, registros em servidores, rastreamento por GPS). Desse modo, cabe aos encarregados da aplicação da lei desenvolverem a capacidade de identificar as possíveis fontes de informação, os locais onde tais informações podem ser encontradas, obtê-las e preservá-las, para que possam ser examinadas, analisadas e, se for o caso, utilizadas como meio de prova em um tribunal.

Na atualidade, vários dispositivos periféricos, como discos magnéticos, SSD, CD, DVD, até mesmo sistemas de jogos podem conter evidências digitais e, por isso, são passíveis de recolhimento ou apreensão. Há também dispositivos conhecidos como "espiões", os quais podem de forma bastante discreta, produzir a gravação de áudio e de vídeo que componham potencial material que será utilizado em um tribunal. Esses dispositivos podem ter câmera, microfone e memória de armazenamento ocultos em um par de óculos de sol, em um relógio ou em uma pulseira. Com dispositivos digitais cada vez mais relevantes - tanto para criminosos quanto para os agentes do Estado - as autoridades, os policiais, os promotores, os advogados e os juízes devem entender a natureza da cena do crime além de sua face tangível e começar a perceber que as mídias digitais e o ambiente virtual podem trazer fortes evidências do cometimento de um crime ou de uma ação de alta reprovabilidade social.

Apesar de um panorama futuro que demonstra com clareza a importância da forense digital, Garfinkel (GARFINKEL, 2010) demonstra pessimismo ao afirmar que entre 1999 e 2007 a forense digital viveu seus anos de ouro e eles estão chegando ao fim. Isso porque, durante o período compreendido entre 1999 e 2007, demonstrou-se ser possível ver o passado através da recuperação de dados residuais sobre os quais se acreditava que estavam definitivamente apagados e entrar na mente do criminoso mediante o rastreamento de mensagens instantâneas e e-mail. Tornou-se possível ainda reconstruir o crime passo-a-passo e observar a forma por meio da qual ele foi cometido.

O pessimismo de Garfinkel e de Marc Goodman (autor de *Future Crimes*) não é à toa, o trabalho de forense digital está ficando muito mais complexo, enquanto isso tecnologias que dificultam o trabalho forense estão se popularizando. Algumas das tecnologias que tornam a tarefa forense mais árdua são:

- Uso de computação em nuvem para armazenamento e processamento;
- Evidências misturadas a uma grande quantidade de dados completamente irrelevantes para o trabalho pericial;
- Uso de criptografia tanto no armazenamento de dados quanto na troca de mensagens (instantâneas ou e-mail);
- Proliferação de diversos formatos de arquivos, sistemas operacionais;
- Sistemas de armazenamento muito diversificado, de forma que há hardware com diferentes interfaces de acesso e processos internos de armazenamento bem distintos.

Dentre os obstáculos criados por novas tecnologias, pode-se citar a dificuldade de recuperação e de comprovação da mesmidade dos dados durante procedimentos de forense computacional em drives de estado sólido (SSD). Acredita-se de que devido ao funcionamento interno do SSD, há possibilidade de destruição completa das evidências.

Com esse cenário de novas tecnologias, as quais tornam o trabalho forense digital mais complexo, não é incomum que os profissionais não sejam capazes de recuperar dados úteis na execução de seu trabalho. É vital para a área que novas pesquisas possam recolocar a forense em um patamar, pelo menos de igualdade com a evolução das tecnologias.

1.1 MOTIVAÇÃO

A busca por evidências digitais pode ser muito difícil, por isso há vários trabalhos que tem como objeto de estudo a dificuldade de se realizar o trabalho forense digital, dentre esses estudos está *Taxonomy of Challenges for Digital Forensics* de Karie e Venter (KARIE; VENTER, 2015) que menciona alguns dos fatores que desafiam as pesquisas de forense computacional. Em seu trabalho, Karie e Venter propõem uma nova taxonomia para os desafios da forense computacional, eles os separam em quatro grandes categorias, a saber: desafios técnicos (aqueles que podem ser enfrentados com conhecimento, protocols ou operações existentes), desafios jurídicos (se há leis que tipificam adequadamente as condutas criminosas, se há apoio legal na condução de um processo penal ou de um processo civil), desafios relativos a pessoas (capacitação técnica, comprometimento com o trabalho) e desafios operacionais (os quais dizem respeito a diretrizes básicas que possam ser adotadas mundialmente e também a recomendação de ferramentas de hardware e software). Na Seção 4.6 a taxonomia proposta por (KARIE; VENTER, 2015) é novamente mencionada, esse trabalho não propõe nova classificação, mas destaca na seção anteriormente mencionada os desafios que mais afetam o trabalho pericial com SSD. Para este estudo, o cerne é no desafio técnico de recuperação da informação em *solid state drive* (SSD).

A recuperação da informação em SSD é um desafio para a forense digital, que pode ser categorizada de diferentes maneiras, logo, se for adotada a classificação de Karie e Venter (KARIE; VENTER, 2015), é um desafio tecnológico da subcategoria "Dispositivos e Tecnologias Emergentes" ou "Antiforense". Porém, pode ser considerada um desafio operacional por dificultar a "Confiabilidade de Trilhas de Auditoria" e também um desafio para o sistema legislativo ou para a aplicação das leis pela indefinição quanto à "Admissibilidade das Ferramentas e Técnicas de Forense Computacional".

Flash memory solid-state drives (SSDs), até pouco tempo atrás, eram muito difíceis de serem encontrados. Hoje, observa-se uma utilização crescente deles em computadores pessoais, além de sua utilização em servidores nos *data centers*. A Maximize Market Research afirma que em 2016 o mercado de SSDs atingiu a cifra de US$ 26.3 bilhões e se estima que alcançará US$ 60.23 bilhões em 2024 (MAXIMIZE, 2018).

Especialistas divergem no que diz respeito a definir uma data para a substituição dos antigos *hard disk drives* (HDDs) pelos modernos SSDs. Conforme Jim O'Reilly, em artigo de 2015 na *Network Computing* (O'REILLY, 2015), com o aumento da capacidade e diminuição do preço dos SSDs (com o advento da 3D NAND) não haverá muitos motivos

para alguém comprar um HDD. A expectativa é que, com a queda de custos e aumento de capacidade, ocorra um crescimento natural no uso de drives de estado sólido.

A inovação permitiu que dispositivos de armazenamento baseado em flash NAND, como o SSD, substituíssem o HDD na maioria das aplicações, mas não em todas (UNSWORTH JOSEPF E MONROE, 2018). A coexistência de várias tecnologias de armazenamento é algo normal e, é possível que mesmo com o aumento da utilização de SSD o HDD continue a existir em determinados nichos.

Estudos recentes do IDC apontam que a receita da indústria de SSDs superou a receita de HDD pela primeira vez em 2017, marcando um ponto de inflexão para a indústria de armazenamento, espera-se que a receita do setor de SSD cresça 8,1% ao ano durante o período compreendido entre 2017 e 2022(JANUKOWICZ, 2018). Durante esse mesmo período a capacidade de armazenamento corporativo em SSD deverá crescer 53,2% e o custo por GB deverá cair 26,1% (CRAIG, 2018).

Com o incontestável crescimento da utilização de SSD como meio de armazenamento, muitos estudos comparativos entre essa tecnologia e o HDD foram realizados, boa parte desses estudos chama atenção para falta de padronização entre os diversos fabricantes de SSD e para falta de divulgação acerca do comportamento dos mecanismos internos de um SSD. Diversas pesquisas vêm sendo realizadas com a finalidade de compreender o funcionamento desses mecanismos internos (CHEN; KOUFATY; ZHANG, 2009)(JÚNIOR; QUEIROZ, 2015b). O desafio que representa o *solid state drive* para a forense computacional, bem como o forte interesse tanto da indústria quanto da Academia com relação a ele - graças ao seu bom desempenho frente ao HDD - motivam o desenvolvimento desse projeto que deverá somar-se a trabalhos anteriores com o fim de detalhar o funcionamento e avaliar a influência destes mecanismos internos em unidades de características diferentes.

1.2 OBJETIVOS

O objetivo geral desta tese é otimizar a recuperação de provas válidas a partir de um SSD. Esses procedimentos devem ser especificados a partir da literatura existente, dos conhecimentos gerados pelo estudo detalhado do SSD e da experimentação prática realizada em diferentes cenários. Os procedimentos devem, em sua elaboração, levar em consideração a legislação, doutrina e jurisprudência brasileiras; a integridade da evidência digital; a recuperação de dados que sejam apagados de forma intencional pelo usuário ou ainda que sejam apagados pelos mecanismos internos do SSD, neste último caso com ou sem a intervenção do usuário. Em particular, a proposta deve ser abrangente, tentando assim atingir indistintamente todos os *solid state drives*, porém, devido à existência de implementações internas não padronizadas, admite-se que se encontrem procedimentos individualizados para cada SSD. Além disso, os procedimentos devem se pautar pelo contato mínimo com as evidências, seguindo os postulados de Edmond Locard (POLLITT, 2008).

Para alcançar o objetivo geral, os seguintes objetivos específicos foram definidos:

- Estudar sobre a Teoria Geral da Prova;
- Estudar sobre a Forense Computacional e seus modelos de investigação;
- Estudar as partes que compõem o SSD;
- Estudar os mecanismos internos do drive de estado sólido que se propõem a aumentar a vida útil e conferir um melhor desempenho ao dispositivo;
- Avaliar como os mecanismos internos implementados por diferentes unidades de estado sólido alteram os dados armazenados;
- Utilizar procedimentos de recuperação de dados apagados e de verificação de integridade de dados em diferentes unidades e também com a utilização de diferentes sistemas operacionais;
- Avaliar o reflexo do emprego do SSD em diferentes cenários, comparando no que couber com os trabalhos relacionados;
- Apresentar as conclusões quanto aos resultados obtidos nos diversos cenários.

1.3 ORGANIZAÇÃO

A Seção 1 apresenta um panorama geral da evolução tecnológica e de como o crime está presente no mundo virtual, enaltece a importância de uma capacitação diferenciada de autoridades policiais e judiciais. Ainda na seção inicial são mostrados a motivação e os objetivos deste trabalho, bem como sua organização. A Seção 2 traz uma visão geral dos trabalhos científicos que guardam relação com SSD e a forense computacional desenvolvida em tais mídias. Os trabalhos são organizados de forma cronológica, permitindo, com isso, entender como foi a evolução tecnológica das unidades de estado sólido e também como os estudos evoluíram. A Seção 3 apresenta parte do estudo realizado no campo jurídico, principalmente no que diz respeito à Teoria Geral da Prova, para que toda a obtenção de dados/informações provenientes da unidade SSD, seja realizada de acordo com o que estabelece o processo penal brasileiro. A Seção 4 propõe-se a mostrar o trabalho das ciências forenses, em especial da forense computacional, no auxílio à formação da convicção do magistrado; apresenta alguns desafios no campo forense computacional, com destaque para aqueles que guardam relação com a forense em dispositivos de armazenamento SSD. Essa seção trata ainda da importante temática de modelos de investigação em forense computacional, propõe um novo modelo que servirá de embasamento para o Procedimento Operacional Padrão também proposto neste trabalho e descrito no Apêndice A. A Seção 5 apresenta, detalhadamente, a tecnologia de um SSD, seus principais componentes físicos e os mecanismos internos que tornam o seu funcionamento complexo e eficiente. A Seção 6 enumera e detalha os experimentos que foram realizados com os arquivos listados no

Apêndice B que foram salvos e manipulados nas unidades SSD utilizadas, a características e especificações das unidades SSD podem ser encontradas no Apêndice C. Finalmente, a Seção 7 apresenta as conclusões deste trabalho e o que se pretende realizar no futuro.

2 TRABALHOS RELACIONADOS

Dentro da área de forense computacional não são poucos os estudos que se debruçam sobre questões envolvendo SSD. Há trabalhos que aprofundam nas questões relativas aos mecanismos internos do SSD, tratando-os em conjunto ou isoladamente. Outros trabalhos focam na (im)possibilidade de recuperar informação após a formatação da unidade ou após o apagamento de arquivos. Há ainda aqueles que tratam da dificuldade de se gerar evidências que possam ser admitidas em um tribunal, uma vez que os resultados obtidos como saída do *hash* dos discos variam constantemente.

Como será visto, muitos pesquisadores percebem a importância de analisar as várias situações que ocorrem quando são realizadas análises forenses em unidades de estado sólido, sob pena de que as evidências digitais presentes na unidade sejam perdidas ou, ainda que obtidas, não possam ser utilizadas adequadamente em um tribunal devido a possibilidade de terem sofrido algum tipo de adulteração. Há muitas possibilidades de análise que não foram contempladas na literatura, alguns desses cenários serão objeto de análise desta pesquisa.

Esta Seção 2 demonstra através de estudos envolvendo unidades de armazenamento SSD, várias hipóteses formuladas e observações experimentais que foram realizadas e publicadas, desde 2008 até os dias atuais.

2.1 ANTONELLIS

Antonellis (ANTONELLIS, 2008) em seu trabalho afirma que o SSD possui muitas vantagens como meio de armazenamento, quando comparado com HDD, afirma ainda que ele pode ser empregado para aplicações militares e aeroespaciais. É mais caro, mas sua capacidade de operação em ambientes hostis o diferencia positivamente. Algumas das vantagens enumeradas são: ausência de partes móveis o que leva a uma maior robustez contra choques mecânicos, a um menor consumo de energia, além disso SSD praticamente não apresenta latência de acesso.

Do ponto de vista de funcionamento das unidades SSD, Antonellis afirma que pode ocorrer de partes da unidade (blocos) sofrerem danos permanentes de forma muito rápida caso sejam alvo de repetidos ciclos de escrita e apagamento. Foi necessária a criação de mecanismos que tornem a escrita mais uniforme ao longo da unidade e que impeçam que a atualização de arquivos seja feita no local físico da unidade em que eles estão salvos, isso já traz uma das fundamentais diferenças entre SSD e HDD. Atualmente os firmwares e controladores escrevem dados através de células de forma mais uniforme. O processo completamente transparente para o sistema hospedeiro é feito de forma diferente por cada fabricante, esse processo permite aumentar o tempo de vida útil de SSDs.

Sobre a forense em unidades de estado sólido, Antonellis continua com sua comparação entre o SSD e o HDD tradicional. Segundo ele, ambos armazenam dados usando uma MFT (*Master File Table*)/FAT (*File Allocation Table*). A relevância disto para a forense é que mesmo se um arquivo é deletado, ele só é removido da MFT/FAT, ou seja, acontece apenas uma remoção lógica; este espaço que foi apagado se torna disponível para uso e pode ser sobrescrito. Nesta situação dados devem estar disponíveis para recuperação com métodos similares aos métodos de discos magnéticos.

Na teoria, como o processo de apagamento é similar, deveríamos recuperar dados de SSDs usando métodos tradicionais, na prática, no experimento realizado por Antonellis isto não ocorreu. No trabalho publicado em 2008, ele afirma que o prognóstico parecia bom; o software empregado era o FTK, através dele foi possível descobrir arquivos apagados. Contudo quando os arquivos foram examinados, após recuperados com sucesso, tudo que continham eram 00s na visualização hexadecimal. A única informação recuperada foi o nome do arquivo que estava intacto; mas não houve a recuperação de dados úteis, eles não continham qualquer conteúdo além de zeros.

Diferente de outros produtos de armazenamento, não existem padrões para fabricantes armazenarem ou apagarem dados. Uma vez que os fabricantes respeitem a padronização de interfaces IDE/SATA, eles têm total liberdade para implementar as melhorias que desejarem internamente (a implementação interna é proprietária e não há qualquer padronização). Fabricantes podem controlar se o espaço de arquivos é deletado ou não. Para Antonellis, como há métodos proprietários envolvidos, é provável que softwares específicos sejam necessários para recuperar um arquivo que foi apagado.

De forma geral, o trabalho adverte que SSD impõe dificuldades para a área forense, afirma que essas dificuldades precisam ser melhor estudadas e enfrentadas. O autor com seu experimento prático obteve resultados os quais ele considera inesperados e alarmantes, uma vez que ele não consegue recuperar informação útil com as ferramentas tradicionalmente empregadas em forense. Segundo Antonellis, unidades de estado sólido devem retornar dados usando métodos já padronizados de recuperação.

2.2 BELL E BODDINGTON

Para Bell e Boddignton (BELL; BODDINGTON, 2010), evidências armazenadas em mídia eletrônica, tais como datas, hora e arquivos podem ser consideradas mais contundentes do que evidências em papel. Contudo, evidência digital é facilmente manipulável e pode ser contaminada se os processos de recuperação utilizados forem mau conduzidos ou ineficazes. Eles alertam, remetendo-se a outros trabalhos, que qualquer perda de conteúdo ou alteração de metadados pode atrapalhar a admissibilidade penal e diminuir o peso da evidência durante o processo em um tribunal. A evidência digital é normalmente tecnicamente complexa e difícil de ser entendida pela maior parte dos juízes e profissionais do direito.

A evidência digital requer validação para testar a confiabilidade e mensurar seu peso e admissibilidade, os autores afirmam que é importante identificar qualquer possível contaminação ou perda de dados que pode ocorrer durante o processo de recuperação. Se uma imagem forense de uma unidade foi (ou parece ter sido) alterada durante a recuperação, a obrigação de provar a integridade da imagem fica com a parte que apresentou a evidência. A parte que se opõe pode questionar a integridade da imagem forense por conta da deficiência no processo de recuperação e preservação.

Baseando-se em trabalhos de outros autores, Bell e Boddington afirmam que para minimizar a contaminação, o processo de recuperação deve evitar a sobrescrita de dados no drive exibido. Quando mudanças ocorrerem ou forem inevitáveis, a natureza e a causa das mudanças devem ser explicadas e descritas convincentemente. Os autores citam do trabalho de Kennealy e Brown (KENNEALLY; BROWN, 2005) que a prevenção de contaminação é essencial durante a recuperação, afirmam que a utilização de hardware de bloqueio de escrita, combinado a um processo de cópia de imagem pode ser usado.

Apesar de deixar claro a necessidade de evitar a contaminação da evidência digital em seu artigo, os autores descrevem que mesmo na ausência de instruções de computador específicas, um dispositivo de armazenamento moderno de estado sólido pode permanentemente destruir evidências, durante um curto espaço de tempo, de uma forma que não aconteceria em discos magnéticos. O fenômeno de autodestruição foi observado em reproduções práticas de ambientes usando SSDs.

Os autores chamam atenção para o fato de que a simplicidade e consistência dos HDDs é um benefício enorme para a perícia e para a lei. Processos bem estabelecidos e tecnologias digitais, tais como análise *post-mortem* e bloqueadores de escrita tornam conveniente e aceitável para a investigação capturar as informações físicas dos discos e validá-las perante um tribunal. Estes procedimentos internacionalmente aceitos incluem situações de recuperação automática que foi previamente apagada pelo réu ou investigado. A peculiaridade está no fato de que a informação foi apagada, mas não esquecida e muitas vezes é usada no tribunal em desfavor do réu ou como elemento para aprofundar uma investigação. HDDs tem velocidade de acesso pequena com relação a capacidade de armazenamento (o que faz o apagamento total um incoveniente), e devido ao fato de que não há qualquer perda de desempenho ou penalidade em se escrever sobre dados existentes - os quais tiveram seu local físico de armazenamento marcado como disponível para escrita - o apagamento completo se torna algo desnecessário.

SSDs estão aumentando a sua importância no mercado na medida em que estão equipando muitos dispositivos, isto tem importância para a prática forense e para validação de dados digitais no tribunal. A tecnologia SSD disputa mercado diretamente com a tecnologia dos HDDs, não é uma tecnologia simples, nem bem conhecida, muito menos homogênea; pelo contrário, é mal documentada, complexa e altamente heterogênea. Para os autores, o pior de tudo é que o SSD pode agir por iniciativa própria e tomar ações

que destroem as evidências existentes em um disco sem a ação de comandos enviados por uma pessoa, potencialmente inviabilizando os esforços da polícia e de analistas forenses que queiram recuperar evidências válidas.

HDDs magnéticos operam criando ou detectando campos magnéticos orientados em regiões fixas de uma superfície magnética, conhecida como blocos. Cada bloco tem uma posição 3D e área dentro do disco conhecida como endereço cilindro/cabeça/setor. Isto especifica o prato do disco particular (discos modernos têm várias superfícies magnéticas), uma trilha particular do disco (distante do centro) e o setor particular (distância angular ao redor do disco). Quando o disco é solicitado para escrever em um bloco particular, ele traduz matematicamente na posição do cilindro/cabeça/setor e magnetisa a superfície magnética do disco na região apropriada. Se há dados antigos no local, eles prontamente assumirão novos valores sem nenhuma preparação especial do meio.

SSDs de nova geração possuem dois problemas. O primeiro é que blocos individuais dentro do SSD possuem um limite ciclos de talvez 10000-100000 vezes antes de correr o risco de falhar. Consequentemente, um esquema de mecanismo interno precisa ser usado para evitar escrever dados continuamente no mesmo local. Em vez disso, uma camada intermediária de tradução é usada para manter a informação do que o computador pensa que está escrevendo. A medida que o computador escreve um bloco repetidamente, o SSD rapidamente traduz cada escrita para um novo e menos usado local; então o computador não sabe que está armazenando os dados em um lugar diferente a cada momento. Isso reduz de forma significativa os danos físicos causados pelos blocos quando um arquivo é atualizado várias vezes. Os autores empregam uma analogia para explicar esse procedimento, o qual ficou conhecido como *wear leveling*. Imagine um hotel em que o gerente renumera os quartos a cada dia para assegurar que os quartos sejam igualmente utilizados, frustrando o hóspede que quer reservar o quarto que mais gosta. Como consequência, o usuário tem pouca ideia de onde os dados realmente estão armazenados fisicamente dentro das páginas de memória do drive. A parte da controladora que mantém as informações de onde cada bloco está sendo escrito é conhecido como *Flash Translation Layer* (FTL). Como segundo problema, o *wear leveling* empregado para solucionar o problema da vida útil das unidades de SSD, pode levar a uma significativa diminuição da velocidade de transferência. Isso ocorre porque a tecnologia flash geralmente requer que blocos sejam apagados eletronicamente antes que eles possam ser usados novamente. Isso difere da propriedade “escreva-sobre-dados-antigos” de fitas e dados magnéticos. O processo de apagamento é muito lento comparado com a leitura e escrita, levando até 10 milisegundos.

Os autores esclarecem que as soluções criadas para problemas pontuais criam novas demandas que tornam todo o funcionamento interno cada vez mais complexo. Em SSD, mudança de um só byte pode resultar na necessidade de ler, apagar e escrever. Muitos fabricantes para aperfeiçoar as unidades adotaram a estratégia conhecida como *Garbage Collection*, cuja ideia é identificar áreas que não estão em uso e resetá-las assim que

possível. O principal problema é que as controladoras das unidades não sabem qual o SO que será usado e por isso a comunicação entre controladora e SO fica prejudicada. Alguns fabricantes como a Samsung escreveram algoritmos capazes de olhar aspectos do NTFS "usado/ não usado" através do exame do bitmap de espaço livre. Consequentemente, pode descobrir áreas que foram marcadas como não usadas pela perspectiva do SO. Os SSDs podem reagir a comandos de seus computadores e em outras vezes agir por sua própria iniciativa.

É possível que tecnologias de *Garbage Colection* sejam disparadas e ativadas em cenários que esteja ocorrendo uma captura física, análise forense ou processo de validação, na ausência de comandos escritos explícitos do computador (a marcação de arquivos como deletados pode ser uma ação do passado). Se a *garbage collection* ocorre antes ou durante o processo de extração forense da imagem do drive, resultará no apagamento irreversível de quantidades potencialmente grandes de dados valiosos que foram ordinariamente obtidos como evidência durante o processo forense - chamamos isso de corrosão ou destruição da evidência -, esse é o primeiro problema. O segundo problema é que qualquer alteração do drive durante ou após a extração pode fazer a validação da evidência difícil. Para ilustrar o quão preocupante é o disparo de *garbage collection* os autores colocam uma situação em que um perito pega a imagem do drive (com *checksum*) para analisá-la, depois de pegar a imagem, o drive é ligado para validação. Neste momento o drive entra no processo de *garbage collection* e deleta parte de seus dados, quando comparar a imagem com a cópia "original", vai parecer que o perito trabalhava com uma cópia corrompida, que pode eventualmente ter recebido de forma mal intencionada alguma informação. Sem saber quando o *garbage collection* está ocorrendo é difícil garantir que uma cópia feita em qualquer momento é autêntica.

A partir de experimentações realizadas, Bell e Boddington afirmam que logo após reiniciar uma máquina com SSD, todos os arquivos estavam danificados e quase todos eliminados completamente, incluindo os metadados do sistema de arquivos. Depois de só alguns minutos, só um arquivo do experimento dentre 316666 foi 50% recuperado; e apenas 0,03% dos dados foram recuperados. Chamou atenção dos autores o fato de que o drive iniciou apagamento de bloco sem qualquer disparo do usuário, o que parece indicar algum tipo de sistema baseado no tempo usado pelo mecanismo de *garbage collection* dentro do SSD.

Há um potencial tremendo para que os dados sejam silenciosamente apagados sem nenhum sinal perceptível, não foram observados leds piscando, vibração, ruído, tudo permanece silencioso durante o processo como se nada estivesse acontecendo.

Os resultados mostram que a eliminação de evidências pode ocorrer apesar da presença de um hardware físico de bloqueio de escrita, isto demonstra o perigo de se depositar confiança demasiada nos processos e tecnologias forenses atuais, que podem ser ineficazes ou podem ser burladas ao passo que a tecnologia evolui.

Por ser um artigo mais antigo, o comando TRIM é tratado ainda de forma superficial. O TRIM é referido como um novo padrão para comunicação disco-a-computador (ATA), que permite o sistema operacional tal como o Windows 7 informar ao drive que uma área de dados não está mais sendo usada e pode ser apagada. Para este artigo, o TRIM é uma ação que é tipicamente tomada imediatamente, a partir de dados associados com um único arquivo, no momento do apagamento individual do arquivo.

Bell e Boddington concluem o artigo afirmando que os resultados encontrados no trabalho pode ter implicações significativas para questões legais que envolvem provas digitais, mais especialmente nos casos em que dados digitais pareçam ter sido excluídos intencionalmente ou deliberadamente por alguém. Dado o ritmo de desenvolvimento da tecnologia de SSD e de sua controladora, além da proliferação cada vez maior de fabricantes, unidades e versões de firmware, provavelmente nunca será possível eliminar ou limitar essa nova área cinza dentro dos domínios forense e jurídico. Parece possível que o período de ouro para a recuperação e análise de metadados e dos próprios dados excluídos tenha chegado ao fim.

2.3 BEDNAR E KATOS

Para Bednar e Katos (BEDNAR; KATOS, 2011), SSD não é uma evolução da tecnologia de *hard disk drive*, ela é uma tecnologia completamente nova que, de certa forma, copia o comportamento de um HDD. Devido à forma de funcionamento interno do SSD, não é sempre que dados que foram apagados são removidos da unidade. Por outro lado, o SSD pode às vezes remover dados de seus locais de armazenamento, mesmo se eles não estiverem conectados a uma interface, desde que o SSD esteja alimentado.

Esse funcionamento do SSD, faz com que procedimentos padronizados para o HDD cujo intuito seja preservar evidências forenses digitais não sejam apenas inapropriadas, mas possam, ainda que seguidas da forma como está padronizado para procedimentos forenses em discos magnéticos tradicionais, resultar em evidências sendo perdidas, destruídas ou consideradas inválidas perante um tribunal.

Uma desvantagem da tecnologia SSD sobre o HDD é que os dados existentes devem ser apagados antes que os blocos possam ser reusados (essa necessidade é comumente referenciada como “apague-antes-de-escrever”, isso indica que os dados não podem ser simplesmente sobrescritos). Para otimização, o SSD através de sua controladora limpa preventivamente os blocos que contém dados que já não são referenciados pelo sistema de arquivos. No entanto, os autores enaltecem que o mapa lógico a que o computador tem acesso não reflete a camada física que é acessada pela controladora do disco. Devido a isso, dados os quais foram apagados pelo usuário, podem ou não serem removidos fisicamente da unidade. Em um laboratório forense, o SSD original pode ser alterado “autonomamente” sem qualquer intervenção dos investigadores. Com essa alteração, a cópia do SSD não será igual ao original e o processo de empregar uma função será inapropriada e ineficaz.

Isto permitirá ao suspeito desenvolver uma defesa no tribunal e arguir que a evidência foi alterada.

2.4 KING E VIDAS

SSD tem armazenamento e funcionalidades diferentes do HDD e necessitam de cuidados especiais de recuperação. Fabricantes têm implementações variadas de *garbage collection*, o que afeta a quantidade de dados preservados no disco. Em seu artigo, King e Vidas (KING; VIDAS, 2011) realizam estudos empíricos e também discutem problemas de recuperação de dados enfrentados por examinadores forenses devido à comandos como o TRIM ATA8, que pode limpar discos em segundos. Experimentos mostram que sem o TRIM, quase todos os dados são recuperados, mas com TRIM só até 27% de blocos são recuperáveis a depender da controladora do fabricante.

SSD tem um aumento na velocidade de leitura da ordem de 10 vezes e de escrita da ordem de 5 vezes em relação ao HDD segundo o trabalho de Gray e Fitzgerald (GRAY; FITZGERALD, 2008) e o de Lee e outros (LEE et al., 2008), ambos citados neste trabalho. Fabricantes de hardware usam firmware e algoritmos de *garbage collection* que reduzem a efetividade das técnicas de recuperação de dados existente. As variações no *Garbage Collection* aumentam a carga de análise para investigadores devido ao tempo necessário para analisar um disco. Mostra-se que um SSD com TRIM habilitado, usando um SO que suporta TRIM, em geral, nenhum dado será recuperado.

Para aumentar a vida útil de unidades SSD, os autores afirmam que é usado o mecanismo de *Wear Leveling*. Ele assegura que cada bloco no dispositivo é escrito uma vez antes de escrever aquele bloco novamente.

Um software conseguir acessar blocos físicos em um SSD é quase impossível sem saber os comandos ATA proprietários do fabricante, devido a uma característica chamada *Flash Translation Layer* (FTL). A FTL executa no interior da controladora do SSD e traduz os blocos de comandos do SO para comandos na flash. FTL também mapeia o LBA (endereço de blocos lógicos) do SO para os PBA (endereços de blocos físicos) do chip.

Investigadores devem perceber que os dados estão se realocando fisicamente no drive mesmo que o SO afirme que os blocos não mudaram. O mecanismo que realiza *garbage collection* executa em segundo plano, move as páginas ativas do bloco e apaga o bloco. O mecanismo de *wear leveling* requer que todas as células do disco sejam reescritas pelo menos uma vez antes de escrever a mesma célula novamente. O que limita o *garbage collector* e o *wear leveling* é a degradação de desempenho à medida que o disco se torna cheio.

As perdas de desempenho levaram a atualização da especificação ATA8 para incluir a função TRIM no *DATA SET MGMT command*(STEVENS, 2006). TRIM é um método relativamente novo, usado para lidar com degradação de desempenho que é resultado do problema “apague-antes-de-escrever”. TRIM muda o *garbage collector* do disco permitindo

o SO marcar blocos como apagados. O controlador do disco ainda decide quando iniciar e desempenhar a coleta. O uso do TRIM permitiu aos SSDs manter seu alto desempenho mesmo depois de alto uso, e a maior parte dos fabricantes de SSD tem um modelo de drive com TRIM habilitado.

Para a forense digital é importante destacar que TRIM e *garbage collection* em SSDs criam o equivalente a uma limpeza de disco. Uma operação de apagamento em um SSD requer do controlador escrever "1s" nos blocos, que é equivalente a limpar aquele bloco. É importante destacar que o *wear leveling* pode deixar dados remanescentes não acessíveis através do FTL, segundo informações retiradas pelos autores de Wei e outros (WEI et al., 2011).

Por meio dos experimentos realizados, os autores chegaram a conclusão de que a recuperação de dados usando discos com TRIM habilitado no Win7 é praticamente impossível. Todos os drives com TRIM retornam valores próximos a 0% de recuperação de dados para arquivos grandes. Enquanto em arquivos pequenos há grande variação. Usando os mesmos drives, e comparando os com um SO sem suporte a TRIM, a diferença é significativa. Testes de apagamento de arquivos grandes e pequenos tem quase 100% de recuperação.

TRIM pode ser usado para anti-forense. Muitos fabricantes criaram ferramentas que permitem ao usuário iniciar TRIM ou *garbage collection* no disco à vontade. Como ATA8 suporta TRIM para até 65536 blocos em um único comando, é possível que o TRIM possa limpar um disco inteiro em segundos. A execução de tais comandos pode ser automatizada e permitir que indivíduos limpem os discos rapidamente por demanda ou por disparo baseado em eventos.

King e Vidas afirmam que com o advento do comando TRIM a recuperação de dados completa é impossível com as técnicas atuais, frequentemente não haverá dados recuperados. Sem TRIM a quantidade de dados recuperada varia, mas a média é de aproximadamente 100%. Com a adoção do SSD e uso do SO com suporte a TRIM, recuperação tradicional de dados não será viável para investigadores.

Investigadores devem saber o SO e se o sistema está usando SSD antes de desligar o sistema. Em certos casos, análise de memória volátil pode ser mais útil para coletar evidência do que análise de material apagado. Além dos impactos em forense computacional, os autores afirmam que é possível que um vírus ou worm com privilégios administrativos possam usar comandos TRIM e esvaziar o drive em segundos.

2.5 NISBET E OUTROS

Nisbet e outros (NISBET; LAWRENCE; RUFF, 2013) iniciam o artigo descrevendo as vantagens de drives SSD: são mais leves, possuem tempos de acesso mais rápidos e menor geração de calor, há uma significativa resistência a danos causados por choque físico, o consumo de energia é baixo, essas características os torna especialmente atraentes para uso em computadores portáteis.

Em um disco rígido tradicional, geralmente quando os dados são apagados, eles ficam armazenados até que novos dados sejam gravados no mesmo local. Se não houver novos dados a serem gravados sobre os dados apagados, então o investigador forense pode recuperar os dados apagados, ainda que muitas vezes em fragmentos. Um computador que não tiver sido utilizada por anos ainda pode ter dados recuperados a partir do seu disco rígido. Para contrariar esta situação, os usuários podem deliberadamente substituir dados excluídos usando um software que irá escrever zeros sobre os dados excluídos.

SSDs sofrem de desgaste nas células o que reduz significativamente o tempo de vida da unidade. O artigo afirma, com base no trabalho de (PERDUE, 2008), que se os blocos em uma unidade são continuamente gravados e apagados a unidade pode perder uma quantidade significativa de espaço devido a uma falha de células individuais, o que faz com que todo o bloco de células seja inútil. Para evitar a ocorrência de falhas como a citada anteriormente, os SSDs realizam nivelamento de desgaste (ou *wear leveling*). Quando o mecanismo de *garbage collection* é realizado, a antiga área de onde os dados foram movidos é escrita com zeros. Isso significa que os usuários não precisam proativamente excluir locais de dados, pois isso é feito automaticamente pela unidade. E por um lado isso prolonga o tempo de vida da unidade, por outro reduz significativamente os dados que podem ser recuperados a partir da unidade pelo investigador forense. Para aumentar ainda mais a vida útil da unidade, um comando chamado de TRIM pode ser ativado. O TRIM força o sistema operacional a notificar a unidade de que os dados foram apagados de um local e a unidade pode marcar esse local como inválido. Isso ocorre logo após os dados serem excluídos, e a rotina de *garbage collection* do SSD vai agora pular a coleta a partir desses locais, poupando o desgaste da unidade e acelerando o processo de *garbage collection*.

Neste artigo, avaliou-se a eficácia do TRIM como uma ferramenta anti-forense para eliminar dados apagados também foi testado no nível do dispositivo no nosso caso de teste anti-forense.

Os objectivos dos experimentos foram os seguintes:

1 - Testar a retenção de dados do SSD em sistemas de arquivos NTFS, Ext4, e HFS + nas seguintes condições:

- carga de trabalho em espera
- carga de trabalho em atividade
- baixo uso da unidade
- alto uso da unidade
- TRIM ativado e desativado

2 - Testar a eficácia de TRIM como uma medida anti-forense sob a seguinte condição:

- Passagem do comando TRIM manualmente no nível do dispositivo

Esses casos de teste foram planejados para cobrir três ambientes distintos: o NTFS no Windows 7 (SP1), Ext4 no Ubuntu 11.10 usando o kernel versão 3.0.0, e HFS + no Mac OS X 10.7. Usou-se a versão de 64-Bit de cada sistema operacional. Esses sistemas operacionais todos suportam a instrução TRIM sob certas condições. Cada sistema operacional é instalado usando as opções de configuração padrão, incluindo a criação de partições.

O caso de teste anti-forense repetiu o experimento realizado por King e Vidas (KING; VIDAS, 2011). Eles descobriram que o TRIM manual, utilizando a ferramenta de software *hdparm* poderia ser usada como uma medida de anti-forense. Os autores mencionam, com base no trabalho de Shu e Obr (SHU; OBR, 2007), que desde o ATA-8 há suporte a TRIM de até 65.536 blocos (com um único comando é possível realizar um TRIM no disco inteiro em questão de segundos). A unidade é capaz então de destruir todos os dados rapidamente.

Através dos experimentos práticos, chegou-se a conclusão de que o SSD decide muito rapidamente por apagar células quando um comando TRIM para esse setor é emitido. Isso não significa, contudo, que as instruções de TRIM são sempre ágeis. O TRIM pode, em alguns casos, limpar efetivamente os dados em questão de segundos, proporcionando assim apenas um pequeno pedaço de um arquivo como algo que restou.

Os resultados encontrados após uma hora mostram que a chance de recuperação de quantidades substanciais de dados nestes casos é quase nula. Um investigador forense teria, portanto, de realizar uma extração muito rapidamente após o comando TRIM ter sido emitido.

Os resultados obtidos durante o nosso experimento anti-forense indicam que TRIM por si só não é uma medida confiável para limpeza adequada de um SSD. O cenário padrão de teste de repetição indica uma limpeza da unidade de 99,8% usando um método TRIM em toda a unidade. Em um SSD de 120GB usado para estes testes, recupera-se entre 185MB e 214MB, em certos casos.

A partir dos trabalhos relacionados e dos experimentos realizados, Nisbet e outros chegaram a conclusão que sistemas de arquivos com TRIM habilitado podem, em questão de minutos, remover dados e torná-los irrecuperáveis. Se um processo de *garbage collection* está sendo iniciado na unidade, ele não é tão rápida quanto a operação TRIM. O processo de *garbage collection* funciona de sua própria maneira, com seus algoritmos e seu atraso de tempo. Ambos NTFS e HFS+ têm mostrado isso em seus resultados. Ext4, no entanto, opera exclusivamente como e quando o comando TRIM é enviado devido à implementação de descarte em lotes.

A implementação de descarte de lotes no sistema de arquivos Ext4 no Linux cria uma oportunidade para uma melhor chance de recuperação dos dados quando comparado com sistemas de arquivos NTFS e HFS+ em uma configuração TRIM ativada. Em todos os três sistemas de arquivos testados, TRIM é capaz de destruir dados apagados quando o SSD envia o comando TRIM. Em um cenário não TRIM há um processo de *garbage*

collection mais agressivo quando o uso elevado de unidade e de atividade da unidade estão ocorrendo em todas as três plataformas. Enquanto na literatura autores indicam que o comando TRIM manual para todo o SSD é um meio rápido e eficaz de realizar anti-forense, os experimentos têm mostrado que alguns dados mínimos são mantidos.

2.6 BONETTI E OUTROS

Bonetti e outros (BONETTI et al., 2014) afirmam que os mecanismos de otimizações mais comuns dos SSDs são *wear-leveling*, *TRIM*, compressão de dados e *garbage collection*, os quais trabalham de forma transparente no SO host e, em certos casos, trabalham até mesmo quando os discos estão desconectados de um computador, desde que estejam alimentados.

As otimizações podem ter impacto significativo na análise forense de SSD. A causa principal é que as células de memória poderiam ser antecipadamente apagados, enquanto nos discos tradicionais seria necessária uma reescrita para fisicamente destruir os dados. Infelizmente as conclusões são muito contraditórias na literatura. A ideia deste artigo é propor um guia genérico, prático e uma metodologia dirigida a teste que guie os pesquisadores e analistas forenses através de uma série de passos que avaliem a capacidade do SSD de sofrer procedimentos forenses.

Chips flash baseados em NAND, de fato, tem um limite físico de aproximadamente 10000 ciclos de escrita e apagamento. Outra limitação que também não pode ser negligenciada, é que sempre que um bloco precisa ser reescrito, ele deve ser apagado primeiro, causando um *overhead* não desprezível nas unidades de SSD.

Como consequência da complexidade encontrada em SSD gerada pelos sucessivos melhoramentos da controladora (que hoje contém diversos mecanismos que aumentam a confiabilidade e o desempenho dos discos), procedimentos de aquisição e análise, existentes e amplamente adotados em forense não são totalmente aplicáveis aos SSDs (o *hash* do SSD pode não ser estável através do tempo, pois dados obsoletos podem ser automaticamente apagado por otimizações internas). Este trabalho afirma que, em muitos casos, a única opção viável pode ser uma aquisição em *white-box* que burle o controlador e leia as informações diretamente dos chips NAND. Uma aquisição em *white-box* é cara, nem sempre realizável, pode possivelmente destruir a unidade, e pode levar a conclusão de que dados foram perdidos ou danificados.

Na metodologia foram conduzidos testes para observar se o SSD implementa algumas características (independente das características anunciadas pelo vendedor, que frequentemente se mostra incorreta).

Como conclusões do trabalho, confirmou-se que para conseguir superar as limitações intrínsecas de SSDs, controladoras adotam um número de estratégias avançadas, preventivamente apagando blocos de arquivos deletados (possivelmente mesmo que não tenha sido solicitado pelo SO) e até mesmo realizando compressão ou cifragem dos dados.

Cada fabricante implementa um controlador de forma diferente, e portanto cada SSD age de forma diferente. A combinação de controladora, SO, sistemas de arquivos e até mesmo uso do disco pode influenciar profundamente na quantidade de informação que pode ser recuperada de uma unidade usando os procedimentos forenses.

2.7 SHAH E OUTROS

O artigo de Shah e outros (SHAH; MAHMOOD; SLAY, 2014) estuda as possibilidades de se empregar em técnicas e métodos com o fito de extrair informações as quais possam ser úteis em uma investigação que utilize como fonte de prova as unidades de estado sólido (SSD).

Nesse artigo é mencionado que há pesquisas as quais encontram resultados que parecem se contradizer: por um lado há a afirmação de que os SSDs destroem as evidências forenses automaticamente e, por outro lado, há trabalhos que afirmam que, mesmo após a sanitização[1] de SSDs, os dados podem ser recuperados.

Tal trabalho visa à investigação dessas duas questões e,por meio dele, são relatadas descobertas experimentais as quais demonstram que certos SSDs parecem destruir evidências forenses enquanto outros SSDs não. Os experimentos fornecem informações e análises do comportamento de SSDs quando certas funções do SO como o TRIM e algoritmos como o *garbage collector* são executados no SSD.

Os autores afirmam que experimentalmente foi verificada uma mudança de comportamento do SSD, de sorte que há diferenças quando ele está conectado às portas SATA secundárias e quando está conectado às portas SATA principais com o sistema operacional instalado. Segundo os autores, o comando TRIM só funciona no último caso, além do mais, os autores afirmam que o algoritmo de *garbage collector* (GC) não é implementado em todos os SSDs disponíveis no mercado e, naqueles com GC só se inicia o apagamento dos blocos de lixo aproximadamente 150 segundos após a exclusão ser realizada. O artigo sustenta ainda que o *firmware* não limpa ou zera o SSD automaticamente, e que é necessário um SO que suporte o comando TRIM para apagar os dados permanentemente.

2.8 JOSHI E HUBBARD

O trabalho de Joshi e Hubbard (JOSHI BINAYA RAJ E HUBBARD, 2016) sobre a análise forense em SSD afirma que a necessidade de técnicas avançadas de forense computacional se deve ao aumento de investigações criminais que envolvem o mau uso de sistemas computacionais. Além disso, as tecnologias computacionais estão cada vez mais presentes no nosso cotidiano, de forma que para extrair dados dos dispositivos computacionais, a análise forense computacional é indispensável.

[1] Sanitização - é o processo de remover ou destruir permanente e irreversivelmente dados armazenados em um dispositivo de memória para torná-lo irrecuperável. Mesmo com o auxílio de ferramentas forenses avançadas, os dados nunca serão recuperados.(IDSC, 2019)

Esse trabalho de pesquisa fornece estudos detalhados de técnicas usadas sobre HDDs tradicionais e técnicas utilizadas sobre SSDs para realizar a investigação forense digital. Unidades de estado sólido (SSD) dependem de memória flash para armazenamento dos dados, de modo que essa tecnologia ultrapassou os discos rígidos tradicionais e, atualmente são o padrão para armazenamento secundário em laptops.

Esse artigo também descreve como o tempo de vida útil limitado e a preparação dos blocos de memória do espaço não alocados dentro do SSD moderno irão gerar complicações durante as investigações forenses. A análise realizada para esse projeto envolve testes de espaço alocado e não alocado dentro de SSDs em laptops, com a funcionalidade TRIM ativada ou desativada, de modo que é feito uso de bloqueador de escrita e de várias versões de sistema operacional.

O *garbage collector* do disco rígido contém dados que foram excluídos e os marca como excluídos, fazendo com que sejam preparados para nova escrita subsequentemente. Contudo, com as modernas técnicas do SSD, esses setores são reescritos com novas informações o tempo todo, o que tornará mais difícil para os investigadores forenses recuperar a evidência necessária para provar crimes diante de um tribunal.

Os autores mencionam que o TRIM não atua na maior parte dos ambientes RAID, também não atua nas unidades SSD externas conectadas via interface USB ou FireWire.

Esse trabalho de pesquisa se concentra na exploração de métodos que possam reduzir o impacto de todos os recursos descritos, a fim de tornar a investigação forense em SSD mais fácil e viável no futuro.

2.9 CHAURASIA E SHARMA

O artigo de Chaurasia e Sharma (CHAURASIA; SHARMA, 2017) afirma que a forense digital é necessária para resolver os casos de investigação criminal que envolvam dados armazenados em computador e em telefones móveis.

A análise forense digital é um avanço da análise forense, junto com esse avanço estão surgindo leis que auxiliam o controle de casos legais e procuram acompanhar o avanço da tecnologia. O artigo relata os estudos de importantes técnicas usadas sobre o HDD e a técnica atualizada, necessária para executar a investigação forense sobre os *Solid State Drives*.

Os autores sustentam que o uso de SSD é bastante acessível e, para muitos propósitos, é usado como um disco rígido normal, com a vantagem de ser muitas vezes mais rápido e possuir um menor consumo de energia. Eles ressaltam que a unidade de estado sólido não é uma mudança na tecnologia do disco rígido; é uma tecnologia completamente diferente, mas que imita o comportamento de um disco rígido.

O SSD introduz um novo desafio para especialistas em análise forense digital. A obtenção de informações efetivas a partir de unidades de estado sólido (SSD) é uma tarefa

forense desafiadora, uma vez que o uso de comandos TRIM, além da ativação de algoritmos internos do SSD, dificultam a investigação forense.

2.10 MARUPUDI

O trabalho intitulado *Solid State Drive: New Challenge for Forensic Investigation* (MARUPUDI, 2017) foi submetido a *St. Cloud State University* como requisito parcial para a obtenção do grau de mestre.

Marupudi supõe que futuramente o número de casos que exigirão análise forense digital provavelmente será maior. Por décadas, os discos rígidos dominaram o mercado devido ao seu custo e capacidade. No entanto, as unidades de estado sólido popularmente conhecidas como SSD substituem os HDDs em várias aplicações. O autor chama a atenção para o fato de que operações internas ao SSD são altamente destrutivas aos dados tradicionalmente recuperáveis. Essas operações internas potencialmente dificultam a validação dos valores de *hash* gerados a partir de evidências digitais e podem prejudicar o processo de recuperação e da análise *live* e *post-mortem* e também podem complicar e frustrar a análise forense pós-recuperação.

Esse trabalho comparou as principais diferenças que foram identificadas entre um HDD e um SSD, e discutiu as principais características que fazem o SSD apagar seus próprios dados e causar dificuldades para investigações forenses.

2.11 FREILING E OUTROS

O artigo de Freiling e outros (FREILING et al., 2018) sustenta que agências de inteligência e encarregadas de investigações estão sempre interessadas em obter dados a partir de dispositivos computacionais pessoais, para encontrar evidências, guiar investigações, ou usar informações diretamente como provas diante de um tribunal.

Para os autores, qualquer dispositivo capaz de armazenar dados pode ser útil, não importando se é um notebook, um tablet, um sistema de navegação, um roteador doméstico ou qualquer equipamento "inteligente" como um relógio ou refrigerador.

No entanto, para que os dados desses dispositivos possam ser utilizados como evidência, eles devem ser obtidos de forma adequada, afastando ao máximo a possibilidade de alterações. O modo mais conveniente de se obter esses dados é criar e seguir procedimentos investigativos padronizados, de acordo com o que exige o arcabouço legal do local.

Na tecnologia SSD, em contraste com o que ocorre no HDD, leitura e escrita são duas operações completamente diferentes: apagar dados inclui a aplicação de uma alta voltagem à célula de memória, o que causa um desgaste. Esse desgaste gera um número máximo de ciclos de escrita/apagamento, isso, por sua vez, limita a vida útil da memória flash.

Para otimizar o tempo de vida útil, é feita uma distribuição do desgaste entre as várias células de memória, através do uso de algoritmos apropriados. Para otimizar o algoritmo de distribuição do desgaste (ou simplesmente *wear leveling*) um comando específico chamado de TRIM foi introduzido no padrão ATA. Com o TRIM, o sistema operacional é capaz de avisar ao drive quais setores ele apagou. Esses setores poderão a partir do TRIM, serem preparados para uma nova escrita pelo drive (usando algoritmos de *garbage collection*).

Todo esse funcionamento interno que o SSD apresenta, segundo os autores, traz consequências ruins para a manipulação de dados forenses, de tal forma que calcular o *hash* de todo o drive não é mais uma técnica confiável para provar que a evidência não mudou, por exemplo.

2.12 RESUMO

Nesta seção, onze trabalhos foram analisados. Os trabalhos aqui descritos tratam das unidades de estado sólido de diferentes maneiras e podem ser resumidos pela Tabela 1 e serão posteriormente comparados com os resultados obtidos neste trabalho, em especial com dados obtidos por meio dos experimentos demonstrados na Seção 6.

A Tabela 1 mostra o ano de publicação dos artigos, o objetivo, o resultado alcançado, as etapas e ferramentas utilizadas para se chegar ao resultado, além do SSD e do sistema operacional (SO).

Tabela 1 – Comparação entre os trabalhos relacionados

Trabalhos	Ano	Objetivo(s)	Resultado(s)	Etapas	Ferramenta(s)	SO/SSD
Antonellis	2008	Recuperar dados de SSD usando métodos empregados em HDD	Recuperou apenas o nome do arquivo	Realizar wipe com um passo; Formatar o SSD com uma partição NTFS; Copiar duas pastas contendo arquivos de texto e gráficos para a unidade SSD; Deletar os arquivos gráficos e apenas um arquivo de texto usando a função "normal" de deletar; Gerar imagem com FTK e criar um arquivo do tipo .dd; Analisar a imagem com FTK.	FTK	SO Windows e SSD Transcend de 32GB
Bell e Boddington	2010	Verificar se SSD e HDD preservam dados apagados da mesma forma, e se dispositivos bloqueadores de escrita podem evitar o disparo do Garbage Collection.	Nos experimentos realizados foi clara a diferença entre SSD e HDD, logo após apagar dados e reiniciar um dispositivo com SSD arquivos haviam sido eliminados, inclusive metadados, bloqueadores de escrita não contribuem para minimizar a situação	Foram preenchidos um HDD e um SSD com a palavra "EVIDENCE", Realizou-se uma formatação rápida, Começou-se a fazer a recuperação e comparação dos dados recuperados das duas unidades. Depois realizou-se experimento com as etapas descritas, porém com bloqueador de escrita.	Formatação rápida com o comando diskmgmt.msc, códigos para comparação entre a recuperação do SSD e do HDD.	SO Windows XP, menciona Windows 7 como tecnologia futura; SSD Corsair P64 CMFSSD-64GBG2D.
Bednar e Katos	2011	Visão geral dos principais desafios que o SSD trouxe para investigadores forenses,	Em um laboratório forense, o SSD original pode ser alterado autonomamente sem qualquer intervenção dos investigadores, com essa alteração, a cópia do SSD não será igual ao original e o processo de empregar uma função será inapropriado e ineficaz.	-	-	-
King e Vidas	2011	Análise de dados remanescentes em SSD com base em experimentos empregando 16 unidades diferentes	Recuperação de dados no Win 7 com TRIM habilitado é praticamente impossível atualmente e frequentemente não haverá dados recuperados. Sem o TRIM a taxa de recuperação é alta, quase 100%. A taxa varia de acordo com a unidade SSD.	Realizou experimentos com unidades SSD formatadas, com baixa utilização (poucos arquivos) e com alta utilização, em todos os casos os dados foram apagados e buscou-se recuperá-los.	The Sleuth Kit	SO Win XP, Win 7 e Ubuntu 9.04; SSD Intel, OCZ, Corsair, Crucial, PQI, Patriot, Kingston, Imation, RiData, Transcend
Nisbet e outros	2013	Examinar a dificuldade para investigação forense, em SSD com TRIM habilitado em Windows, Linux e Mac OS X.	O TRIM ativado deixa menos dados do que TRIM desativado, em se tratando de investigação forense e recuperação de dados apagados.	Não há detalhamento das etapas.	dcfldd	SO Win7, Mac OS X 10.7 e Ubuntu 11.10; SSD Sandforce
Bonetti e outros	2014	Usa metodologia "caixa-preta"para determinar se um SSD com TRIM, Garbage Collection e Wear Leveling está sofrendo impacto desses mecanismos no que concerne a chance de recuperar dados.	Consegue recuperar informação em alguns casos. A combinação entre controlador(a), SO, sistema de arquivos e uso de disco influencia a quantidade de dados recuperada.	Escolha de arquivos fáceis de recuperar com técnicas de carving, Cálculo de hash de arquivos Encher o disco com arquivos, Formatação rápida, Geração de imagem, Carving, Cálculo de hash de arquivos recuperados, Check de integridade de arquivos recuperados.	Scalpel	SO Windows ou Linux; SSD Samsung, Corsair e Crucial.
Shah e outros	2014	Investiga se SSD destroi evidências automaticamente e se após uma sanitização do SSD, dados podem ser recuperados.	Na ausência de um Garbage Collection e TRIM efetivo é possível recuperar. Verificou-se que o Garbage Collection apresenta um atraso para iniciar a operar	Realiza três experimentos com formas de conexão distintas. Os passos seguidos são: Criação de uma partição, Enche o SSD com arquivos repetidos. Realiza-se formatação rápida, Desliga-se o sistema 15 minutos após formatar, Reinicia, Após boot completo inicia a recuperação com PC Inpector	PC Inspector, Paragon Partition Manager	SO Win 7 Home e Win 7 Pro; SSD Crucial m4 64GB, Samsung 470 Series 64GB, Kingston SSD Now V100 64GB.
Joshi e Hubbard	2016	Descrever como o tempo de vida limitado e garbage collection complicam a investigação forense	O uso do TRIM permite o SO informar ao SSD blocos inválidos para que sejam apagados sem deixar rastros	Carrega Win 7 Pro, Apaga arquivos e imediatamente desliga o computador, Copia o SSD para um HDD, Compara o Hash do SSD e do HDD, Conecta o SSD ao bloqueador de escrita e gera o hash, Usa utilitário de recuperação para buscar, Se bem sucedido aguarde 1 hora para gerar novo hash e comparar.	dd, Recuva	SO Win 7 Pro, Linux 2.6.28 e Ubuntu 15.10
Chaurasia e Sharma	2017	Investigar desafios do SSD para análise forense	Da forma como são usados no HDD os métodos de preservação, identificação e extração são inúteis.	Artigo de Revisão	-	-
Marupudi	2017	O principal objetivo é identificar porque investigadores estão encontrando problemas ao buscar evidências em SSD, diferentemente do que ocorre com HDD	Mesmo com a semelhança de procedimentos executados entre SSD e HDD, os resultados são diferentes.	As unidades SSD e HDD são preenchidas com os mesmos arquivos, formatados da mesma forma. São geradas imagens com FTK Imager, as quais são analisadas com FTK Toolkit.	FTK Imager, FTK Toolkit	SO Win 10; SSD Lexar 512GB
Freiling e outros	2018	Estudar as atuais práticas de forense e dar uma visão geral dos resultados de pesquisas recentes	Conteúdo da unidade SSD pode ser alterado apenas com o fornecimento de energia.	-	-	-

3 *A PROVA NO PROCESSO PENAL BRASILEIRO*

O Direito Processual Penal é o ramo do Direito que tem por finalidade a aplicação no caso concreto da Lei Penal violada. Nas palavras de José Frederico Marques, o Direito Processual Penal é "o conjunto de princípios e normas que regulam a aplicação jurisdicional do Direito Penal, bem como as atividades persecutórias da Polícia Judiciária, e a estruturação dos órgãos da função jurisdicional e respectivos auxiliares" (MARQUES; FERRARI; DEZEM, 2009).

O processo em si, pode, nas palavras de Júlio Fabbrini Mirabete, ser definido como "(...) conjunto de atos cronologicamente concatenados (procedimentos), submetido a princípios e regras jurídicas destinadas a compor as lides de caráter penal. Sua finalidade é, assim, a aplicação do direito penal objetivo" (MIRABETE, 2004).

O tema da prova possui elevada importância no que diz respeito ao processo penal, dentro de um sistema que seja alicerçado na garantia de direitos dos sujeitos processuais e que ao mesmo tempo zele pelo cumprimento de deveres necessários à convivência e à manutenção da paz social em um Estado Democrático de Direito [1].

Em direito penal, só a prova do fato criminoso deverá ser capaz de superar a presunção de inocência do acusado, que é um princípio jurídico constitucionalmente assegurado pelo art 5º, LVII, da CR/88 - ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória. A Carta Magna fornece essa garantia contra o uso arbitrário do poder punitivo do Estado.

A palavra "prova" possui a mesma origem etimológica de probo (do latim, probatio e probus) a qual traduz a ideia de aprovação, confiança, correção, conforme afirma Antonio Magalhães Gomes Filho (FILHO, 2005). No âmbito do processo penal, passou a ser empregada de forma ampla, indicando indistintamente os meios utilizados para demonstração dos fatos, atividade utilizada pelas partes para levar ao processo os meios de prova, designando, também o resultado do procedimento probatório, ou seja, o próprio convencimento que o magistrado externa.

Na doutrina, Paulo Rangel conceitua prova como sendo "o meio instrumental de que se valem os sujeitos processuais (autor, juiz e réu) para comprovar os fatos da causa, ou seja, os fatos deduzidos pelas partes como fundamento do exercício dos direitos de ação e de defesa" (RANGEL, 2009).

Contudo, o estudo da matéria Prova, como vários outros no âmbito do Direito, reveste-se de complexidade, envolve questões culturais e muda ao longo do tempo. Para construir

[1] Estado Democrático de Direito - é um conceito que designa qualquer Estado que se aplica a garantir o respeito das liberdades civis, ou seja, o respeito pelos direitos humanos e pelas garantias fundamentais, através do estabelecimento de uma proteção jurídica. Em um estado de direito, as próprias autoridades políticas estão sujeitas ao respeito das regras de direito.(SANTOS, 2011)

uma base sólida no estudo e na aplicação da perícia forense computacional, não se poderia deixar de estudar a Prova, as Perícias em Geral.

Esta seção 3 demonstra o estudo realizado no campo jurídico para que toda a obtenção de dados/informações provenientes da unidade SSD, seja realizada de acordo com o que estabelece o processo penal, de modo que esse estudo é pilar para garantia da admissibilidade da prova, bem como para o correto entendimento da importância de se proceder com rigor em todas as etapas e de se manter uma cadeia de custódia.

3.1 A PROVA

3.1.1 Mudança ao longo dos anos

O Código de Processo Penal (CPP) de 1941 (BRASIL, 1941) demonstrava uma ideologia autoritária que vigorava à época. A respeito, por exemplo, da interceptação de correspondência, constava naquele diploma no art. 233 que "as cartas particulares, interceptadas ou obtidas por meios criminosos, não serão admitidas em juízo"; por outro lado, o art. 240, § 1°, alínea f, autorizava a apreensão de cartas, abertas ou não, destinadas ao acusado ou em seu poder, "quando haja suspeita de que o seu conteúdo possa ser útil à elucidação do fato" (FILHO, 2010). De forma que um indivíduo que esteja sendo acusado pode ter sua correspondência violada, a pretexto de interesse na apuração dos fatos, contudo outras cartas apreendidas com violação à lei penal, serão inválidas como prova.

Para Canuto Mendes de Almeida, "todos os gêneros e espécies de prova podem ser objeto de investigação. E devem ser sempre que necessários à descoberta da verdade[2]. A limitação da liberdade investigatória só é admissível quando a discrição e arbítrio policiais possam representar uma injusta lesão a direitos individuais e suas garantias. Por isso, cerceia-se, mui justamente, a liberdade de investigação, quando, por exemplo, envolva invasões domiciliares, buscas e apreensões forçadas, detenções prolongadas (...)" (ALMEIDA, 1973).

Essa limitação à busca da verdade colocada por Canuto Mendes de Almeida, passa a ser expressa pelo legislador no Código de Processo Civil de 1973, o qual prevê, no art. 332, que "todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar os fatos, em que se funda a ação ou a defesa".

Percebe-se que, mesmo antes da Constituição da República de 1988, já havia movimentações doutrinária e legislativa no sentido de que ao Estado não se pode permitir a violação de leis, com o objetivo de colher elementos probatórios. A forma como a prova é obtida é tão (ou até mais) importante quanto a própria prova.

[2] O Processo Penal deve buscar a verdade real, mas o que importará será a verdade processual. Ou seja, o magistrado formará sua convicção sobre os fatos com base no que está no processo.

Um estudo elaborado por Ricardo Cintra de Torres de Carvalho (CARVALHO, 1995) mostrou que, nos tribunais brasileiros, durante muito tempo, abstraía-se a forma pela qual a prova fora obtida; eventual irregularidade era apurada em processo próprio, não interferindo na admissibilidade da prova. A partir da década de 1960, começou-se a verificar uma tendência nos tribunais paulistas a considerar que irregularidades praticadas pelo Estado, em casos de busca e apreensão, contaminavam todo o processo.

A visão de que os fins não (mais) justificam os meios, direcionando as provas ilícitas para a inadmissibilidade processual, foi também adotada pelo STF em importantes julgamentos quando foi suscitada a questão da validade de interceptações telefônicas clandestinas, tanto em matéria cível quanto em matéria penal (FILHO, 2010).

Em 1988 a Carta Magna consagrou essa tendência do direito brasileiro e incluiu no capítulo "Dos Direitos e Garantias Fundamentais" o inc. LVI do art. 5º, o qual estabelece que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos".

3.1.2 Várias acepções do termo prova

Antonio Magalhães Gomes Filho em seu estudo sobre a terminologia da prova (FILHO, 2005), afirma que o CPP emprega o termo prova em três acepções diferentes: o art. 155 a utiliza como meio de prova; o art. 156, como resultado de prova e o art. 157, como conjunto dos elementos de prova.

Ainda segundo Gomes Filho (2005), na linguagem do direito processual o termo pode ser empregado em um primeiro sentido de demonstração, pois ainda que não seja possível chegar-se a uma verdade absoluta sobre fatos discutidos, é possível chegar a um conhecimento processualmente verdadeiro sobre esses fatos, que permita um determinado grau de certeza sobre a ocorrência deles.

O termo, em um segundo sentido, pode ser empregado como atividade ou procedimento, destinado a colher e analisar os elementos necessários para confirmar ou refutar uma hipótese ou uma afirmação.

Prova pode ser empregado como desafio a ser superado para se demonstrar algo que se afirma, vez que o ônus da prova é o encargo que cabe à parte que realiza a alegação. A prova é usada para demonstrar a existência de fatos alegados e, em regra, é produzida na fase judicial e na presença do juiz, sendo obrigatória a observância dos princípios constitucionais do contraditório e da ampla defesa.

Finalmente, mas certamente sem esgotar o tema, a palavra prova na terminologia do processo pode ser utilizada para indicar dados objetivos que confirmam ou negam uma asserção a respeito de um fato que interessa à decisão da causa.

3.1.3 Elementos de convicção, vestígios, evidências e indícios

Os termos "elementos de convicção" ou "elementos informativos" são empregados pelo CPP para designar elementos angariados no decorrer do Inquérito Policial e que podem

auxiliar o titular da ação penal para que este ofereça a denúncia, cabe ressaltar que antes do crivo do contraditório judicial não parece ser pertinente o emprego do termo "prova", portanto há - além de elementos de convicção - termos mais adequados, subsequentemente deslindados.

Nos ensinamentos do perito Décio de Moura Mallmith (MALLMITH, 2007), pode-se diferenciar vestígios, evidências e indícios da seguinte forma:

- Vestígios - constituem-se de qualquer marca, objeto ou sinal sensível que possa ter relação com o fato investigado. A existência do vestígio pressupõe a existência de um agente provocador (que o causou ou contribuiu para tanto) e de um suporte adequado (local em que o vestígio se materializou).

- Evidências - constitui uma evidência o vestígio que, após analisado pelos peritos, mostrar-se diretamente relacionado com o delito investigado. As evidências são, portanto, os vestígios depurados pelos peritos. São puramente objetivos.

- Indício - encontra-se explicitamente definido no artigo 239 do CPP: "Considera-se indício a circunstância conhecida e provada que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra ou outras circunstâncias."

3.1.4 Elementos de prova, fontes de prova, meios de prova e meios de investigação da prova

Rubens Pereira e Silva Júnior (JUNIOR; PEREIRA, 2018) afirmam que elemento de prova é tudo aquilo que pode ser levado ao processo, que possa servir de fundamento para o julgador. Como exemplo, tem-se a declaração de uma testemunha, o parecer de um perito e o conteúdo de uma certidão juntada ao processo.

Gomes Filho (FILHO, 1997) afirma que elementos de prova são "os dados objetivos que confirmam ou negam uma asserção a respeito de um fato que interessa à decisão da causa".

Na terminologia processual do livro de Antonio Carlos de Araújo Cintra (CINTRA; GRINOVER; DINAMARCO, 2015), as expressões fonte de prova, meios de prova e meios de investigação da prova, devem ser assim distinguidas:

- Fontes de prova - termo empregado para designar as pessoas ou as coisas por meio das quais pode-se conseguir a prova. Podem ser fontes pessoais (testemunhas, peritos, vítima, acusado) e fontes reais (dispositivos de armazenamento de dados, como o SSD).

- Meios de prova - instrumentos ou atividades por intermédio dos quais os dados probatórios (elementos de prova) são introduzidos e fixados no processo (produção da prova). São, em síntese, os canais de informação de que se serve o juiz.

- Meios de pesquisa ou Meios de investigação da prova - um meio para se chegar a coisas materiais, informações dotadas de força probatória, que podem ter como destinatários a polícia investigativa ou o Ministério Público, são exemplos as inspeções, interceptações telemáticas, buscas e apreensões.

O código de processo penal italiano distingue explicitamente os meios de prova dos chamados meios de pesquisa ou meios de investigação da prova (*mezzi di ricerca della prova*, na terminologia do CPP italiano). No CPP italiano de 1988 os meios de prova (*mezzi di prova*) se caracterizam por oferecer ao juiz resultados probatórios que podem ser empregados diretamente na decisão, são exemplos: o testemunho, as perícias e os documentos. Já os meios de pesquisa ou meios de investigação da prova (*mezzi di ricerca della prova*) não são fonte de conhecimento, mas sim um meio para se chegar a coisas materiais, informações dotadas de força probatória, que podem ter como destinatários a polícia investigativa ou o Ministério Público. São exemplos: inspeções, interceptações telemáticas, buscas e apreensões.

No CPP brasileiro, o Título VII, "Da Prova", vale-se de diferentes capítulos para tratar dos meios de prova (perícias, documentos) e de meio de investigação (busca e apreensão). Há, ainda, outras leis que disciplinam matérias ligadas a meios de investigação, tais como a Lei n° 9.296/96 (Interceptações Telefônicas), a Lei n° 12.850/2013 (define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal) e a lei 12.965/2014 (Marco Civil da Internet - dispõe, dentre outras coisas, sobre requerimento judicial de registros de conexão ou de acesso a aplicações de Internet).

De forma mais objetiva, pode-se dizer que os meios de prova se caracterizam por oferecer ao juiz resultados probatórios que podem ser empregados diretamente na decisão; enquanto que os meios de pesquisa ou meios de investigação da prova são procedimentos que podem levar às fontes de prova.

3.1.5 Classificação das Provas

As leis ou a doutrina apresentam uma vasta classificação das provas sendo estas baseadas no seu objeto, valor, sujeito, procedimento e forma. A classificação feita por Fernando Capez (CAPEZ, 2016) cita:

Quanto ao seu objeto, as provas podem ser classificadas como direta e indireta:

- prova direta - demonstra o que de fato ocorreu de forma clara, ou seja, quando a mesma dá certeza por meio de documentos ou testemunhas. Exemplo: testemunha de um delito, que no depoimento, comprova diretamente a ocorrência do crime.

- provas indiretas - não provam diretamente o fato, elas auxiliam a alcançar o fato principal por meio de um raciocínio lógico-dedutivo, considerando também outros

fatores de natureza secundária, relacionados com o primeiro. Exemplo: uso de álibi, por meio do qual o acusado comprova de forma inequívoca que estava em outro lugar quando o crime ocorreu.

Quanto ao valor as provas podem ser classificadas como plenas, não plenas ou indiciárias:

- provas plenas - são as chamadas provas convincentes, completas, as quais possibilitam um juízo de certeza ao julgador, dando-lhe condições de fundamentar a sua decisão de mérito em apenas uma delas, se for o caso. Exemplo: exame de corpo de delito.

- provas não-plenas ou indiciárias - são provas que auxiliam a reforçar a convicção do Juiz, contribuindo na formação de sua certeza, mas não possuem o poder de formar sua convicção, de forma que ele não pode fundamentar sua decisão de mérito apenas em um prova não-plena. Exemplo: fundada suspeita (art. 240, § 2º do CPP).

As provas quanto ao sujeito, podem ser divididas em real e pessoal.

- provas pessoais são aquelas que derivam de uma pessoa, são subjetivas. Exemplo: afirmações pessoais como interrogatório, depoimentos.

- provas reais - são aquelas que se relacionam com alguma coisa ou objeto, não derivam de uma pessoa. Exemplo: arma ou um cadáver.

Com relação à sua forma ou aparência, as provas podem ser classificadas como testemunhal, documental e material.

- prova de caráter testemunhal - é apresentada por meio dos depoimentos das testemunhas. Nesta prova, a pessoa declara, sob compromisso de dizer a verdade sobre o que lhe for perguntado (art. 203 do CPP).

- prova documental - é gerada por meio de documentos escritos, instrumentos ou papéis públicos ou particulares (art. 232 do CPP).

- provas materiais - são qualquer elemento que materializa a demonstração do fato, como exemplo, o instrumento do crime.

Já dos ensinamentos de João Batista Lopes(LOPES, 2010), as provas ser classifiacadas quanto ao procedimento, daí podem ser típicas ou atípicas.

- prova típica - são aquelas em que o procedimento está previsto na Lei.

- prova atípica - possui na doutrina duas correntes distintas: na primeira corrente, prova atípica é somente aquela que não está prevista na legislação; para a segunda corrente, é atípica aquela prova que está prevista na lei, mas seu procedimento não, e também é atípica, aquela que nem ela nem seu procedimento está previsto em lei.

Os exemplos mais comuns de provas atípicas, segundo (LOPES, 2010), são a prova emprestada, as declarações de terceiros e as perícias extrajudiciais. Mas, por sua própria definição, pode-se dizer que também é exemplo de prova atípica a prova informática.

O CPP, com a redação dada pela lei 11.690/2008, traz ainda no artigo 155 as provas cautelares, não repetíveis e antecipadas.

- provas cautelares - produzidas antes do processo principal, em juízo, quando existe um risco de desaparecimento do objeto pelo decurso do tempo, aqui o contraditório pleno é diferido, pois se dá em momento posterior. Exemplo: interceptação telefônica e busca e apreensão.

- provas não repetíveis - são aquelas obtidas na fase investigatória e cuja reprodução na fase judicial é materialmente impossível, são consideradas "provas" (e não apenas "elementos informativos") obtidas na etapa extrajudicial. Exemplo: exame do corpo de delito.

- provas antecipadas - produzidas antes de seu momento processual oportuno e até antes do início efetivo do processo judicial, porém, com a observância do contraditório pleno e real, em virtude da relevância e urgência de sua realização. Exemplo: depoimento de testemunha que está em fase de doença terminal e poderá não sobreviver até a etapa judicial (previsto no artigo 225 do CPP).

Essas diferentes formas de classificar as provas não esgotam o tema. Diferentes doutrinadores do direito podem propor novas formas de classificação e suprimir algumas daquelas que foram apresentadas.

No Código Penal, para que uma conduta seja considerada crime o núcleo dá ação deve estar tipificado, não sendo admitida a analogia. O Código de Processo Penal é diferente, admite-se a analogia, para ser considerada prova não a necessidade da descrição da prova nem de sua forma de obtenção.

O conhecimento e classificação das provas, visa a chamar atenção de que a prova informática pode ser classificada, assim como qualquer outra prova, de diferentes maneiras, mas quando trata-se de classificação de provas quanto ao procedimento, a prova informática é uma prova atípica pois não faz parte de um rol previsto em lei, nem seu procedimento de obtenção precisa estar expressamente previsto em nosso CPP.

O nosso CPP, em outras palavras, admite todo e qualquer tipo de prova, ainda que esta não esteja prevista neste código, desde que legítima. Essa abertura maior dada a novos tipos de prova, permite que o Direito possa receber provas oriundas de tecnologias não conhecidas no momento da discussão legislativa, como é o caso dos arquivos recuperados a partir de uma unidade estado sólido (SSD).

3.1.6 Princípios que regem o sistema probatório

Apesar de se admitir provas de todo e qualquer tipo, ainda que não previstas no CPP, a busca da verdade material[3] possui limites. Esses limites são impostos pela dignidade da pessoa humana, sustentam-se em princípios estruturantes do Estado Democrático de Direito e muitos desses princípios encontram-se expressos na Constituição da República de 1988. Alguns dos princípios a serem observados no momento de produção das provas são:

1. Princípio do Contraditório - estabelece a necessidade de garantir a ambas as partes o direito de presenciar a produção das provas ou de conhecer o seu teor, de manifestar-se sobre elas e, ainda, de influir no convencimento do juiz por meio da produção de contraprova. De outra maneira, todas as provas produzidas por quaisquer das partes, poderão ser contraditadas pela outra parte; Uma preocupação ao desenvolver esta seção, o qual inclui um estudo jurídico e correlacioná-lo com o SSD, justifica-se também pela possibilidade desse dispositivo violar o princípio do contraditório, uma vez que a prova colhida pode se modificar sem intervenção humana e, poderá sempre partir da defesa a alegação de que houve manipulação da prova.

2. Princípio da Comunhão das Provas - estabelece que, uma vez produzida por quaisquer das partes ou determinada pelo Juiz, após ser juntada aos autos do processo, deixa de pertencer àquele que a produziu, passando a ser utilizada em benefício de qualquer das partes;

3. Princípio da Oralidade - consagra a preponderância da linguagem falada sobre a escrita em relação aos atos destinados a formar o convencimento do juiz. Decorre desse princípio que, sempre que possível, as provas devem ser produzidas oralmente na presença do juiz, salvo em casos excepcionais, em que a forma escrita é expressamente admitida (art. 221, § 1º, do CPP);

4. Princípio da autorresponsabilidade das partes - atribui às partes o ônus de produzir prova de suas alegações. De tal forma que, caso o titular da ação penal não consiga provar a autoria e materialidade do fato, terá de arcar com a consequência processual que é a absolvição do acusado;

5. Princípio da não auto-incriminação - entende-se desse princípio, consagrado no Brasil, que o investigado ou acusado possui o direito de abster-se de praticar qualquer conduta que possa acarretar a obtenção de prova em seu desfavor. Não está o acusado obrigado a responder às perguntas que lhe forem feitas, nem a participar de reconstituição simulada, nem a fornecer material gráfico para exame grafotécnico.

[3] Verdade Material (ou real) - É aquela verdade a que se busca chegar o julgador, reveladora dos fatos tal como ocorreram historicamente e não como querem as partes que apareçam realizados. (HADDAD, 2012)

6. Princípio da imediação (ou imediatidade) - exige que o juiz tenha contato direto com as provas de que se valerá para decidir, daí porque, em regra, é inválida a prova produzida sem a presença do magistrado.

7. Princípio da identidade física do juiz - determina que a decisão seja proferida, salvo em hipóteses excepcionais, pelo juiz que teve contato direto com a colheita da prova (art. 399, § 2º, do CPP).

8. Princípio da boa fé objetiva, conforme citado em (MARTINS-COSTA, 2018) - é um princípio cuja função é estabelecer um padrão ético de conduta para as partes ao longo de todas as fases da relação obrigacional.

   Ao se discutir a produção da prova informática, não há surpresa em afirmar que ela deve ser produzida com observância aos princípios já enumerados. Conforme será visto, a medida que um aprofundamento técnico sobre o SSD for alcançado, esse dispositivo possui um potencial de dificultar o contraditório judicial e, para evitar que a prova obtida de tal dispositivo seja deteriorada um trabalho meticuloso precisa ser desenvolvido, a fim de que não só o princípio do contraditório, mas também todos os demais princípios sejam devidamente observados.

3.2 LEGALIDADE DA PROVA

Embora o Código de Processo Penal enumere alguns meios probatórios, como o exame do corpo de delito e outras perícias (arts. 158 a 184), o interrogatório do acusado (arts. 185 a 196), a confissão (arts. 197 a 200), as declarações do ofendido (art. 201), as testemunhas (art. 202 a 225), o reconhecimento de pessoas ou coisas (arts. 226 a 228), a acareação (arts. 229 e 230), os documentos (arts. 231 a 238), os indícios (art. 239), é consenso na doutrina que tal relação não esgota os meios de prova admitidos em nosso ordenamento, já que não tem caráter taxativo, mas exemplificativo.

Na tarefa de identificar se uma prova pode ser empregada em um processo, há importante lição que pode ser retirada do art. 369 do Código de Processo Civil (CPC)(BRASIL, 2015): "As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz."

Consagra-se, a partir do texto do recente CPC, a possibilidade de se utilizar de quaisquer meios de prova, desde que esses meios de prova sejam legítimos, não sendo absoluta, por limitação constitucional.

3.2.1 Momentos da produção da prova

Segundo Fabiano Yugi Takayanagi (TAKAYANAGI, 2012) para que uma prova seja devidamente analisada pelo juiz deve passar por momentos probatórios que são essenciais à

verificação de sua legalidade e possível inclusão ao processo, com o intuito de se alcançar a máxima confiabilidade a respeito dos fatos investigados, pode-se subdividir a atividade probatória em cinco momentos (ou fases), são eles: a investigação, a propositura, a admissão, a produção, e a valoração (ou apreciação), como mostra a Figura 1.

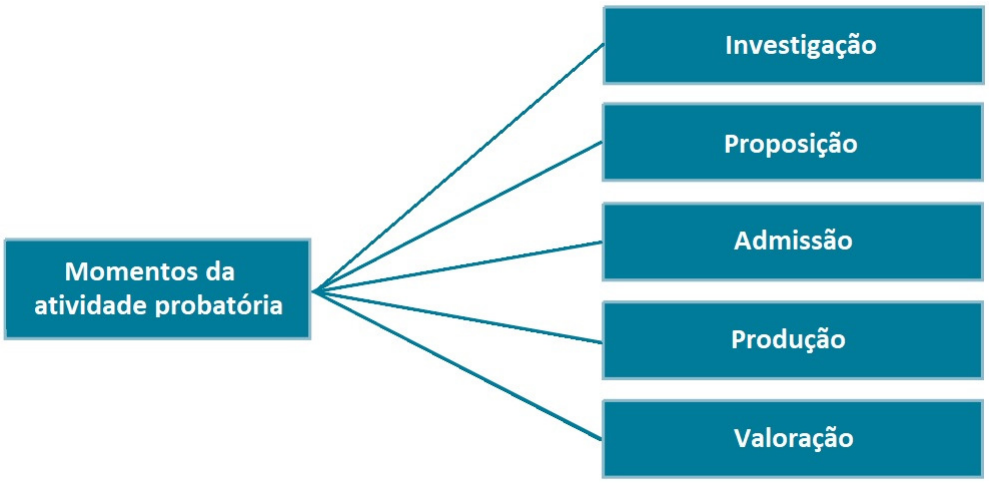


Figura 1 – Momentos da atividade probatória

1. Fase de investigação - esse primeiro momento está diretamente ligado à busca da materialidade e autoria delitiva. No Brasil, o principal meio de apuração da existência de infração e de sua respectiva autoria é o inquérito policial (art. 4º do Código de Processo Penal), porém há casos em que são utilizados outros meios de investigações prévios, ou pelo fato de a materialidade e de a autoria delitivas se encontrarem tão evidentes que não seria necessária uma investigação. A investigação é, independente de como será conduzida (inquérito policial, comissão parlamentar), de evidente importância pelo fato de buscar elementos necessários para fundamentar uma possível ação penal, bem como para corroborar a sua inexistência.

2. Fase de proposição - refere-se ao momento em que as partes manifestam seu desejo no tocante à produção de determinada prova. Em relação a alguns meios de prova, a lei estabelece um determinado momento em que devem ser requeridas. Essa faculdade deve ser exercida em uma etapa procedimental determinada, tal como ocorre com as testemunhas, que devem ser indicadas, necessariamente, na denúncia ou na queixa (art. 41 do CPP) ou, ainda, na resposta escrita (art. 396-A), sob pena de preclusão (perda do direito de se manifestar em um processo, por não ter exercido essa manifestação no momento correto). Outros meios de prova, contudo, podem ser propostos a qualquer tempo como a apresentação de documentos (art. 231 do CPP). Cabe ressaltar, porém, sem aprofundar a discussão, vez que foge do escopo deste trabalho, que o direito de proposição de provas, é um poder de iniciativa em relação à introdução do material probatório no processo, que seria reconhecido pelas

legislações como direito não só das partes, como também de outros interessados (art. 156 do CPP). Logo, deixando de lado as controvérsias doutrinárias, pelo art. 156 do CPP, é facultado ao juiz determinar produção antecipada de provas consideradas urgentes e relevantes. Ou seja, a lei não contempla outra maneira senão a iniciativa judicial para a antecipação de atos tendentes à formação de provas. Com a mudança proposta no Código de Processo Penal (Novo CPP - Projeto de Lei n. 8.045/2010), ao juiz ainda caberá: analisar as medidas cautelares e decidir sobre os pedidos de busca e apreensão domiciliar, de interceptação telefônica, de interceptação de fluxo de comunicações em sistemas de informática e telemática ou de interceptação de outras formas de comunicação. Destaque-se que nesse momento probatório, no qual muita ilegalidade é cometida, para que o Juiz possa exercer a faculdade de ordenar a produção antecipada de provas, é necessário que exista um procedimento investigativo em andamento (um inquérito policial em andamento, por exemplo) e algum pedido colocado para sua análise (STJ REsp 582.881/PR).

3. Fase de admissão - diz respeito à análise, pelo juiz, da pertinência e da necessidade da aquisição da prova. É o momento em que o juiz defere ou não a produção de provas, é o momento propício à exclusão das provas que não estejam de acordo com a legislação vigente, de outra forma, é o momento oportuno para exclusão de provas inadmissíveis. Segundo Gomes Filho (1997), "por operar em momento anterior à prática ou ao ingresso do ato no processo, impede a produção de qualquer efeito válido, aproximando-se mais da ideia da inexistência (jurídica) do ato vedado pela lei processual". A exclusão das provas nesse momento impede que estas ingressem no processo e influenciem o convencimento judicial. É uma prévia valoração legal na qual o magistrado decide se cabe a inclusão ou não da prova ao processo e, para tanto, há disposições constitucionais e processuais regulando tal proibição.

4. Fase da produção - é o momento em que a prova é trazida para dentro do processo, após a requisição e admissão. Em regra, os meios de prova, devem ser produzidos em contraditório, na presença das partes e do juiz. Porém não basta o contraditório sobre a prova, exige-se também o contraditório na produção da prova. O princípio do contraditório deve ser respeitado no momento de produção de provas, pois se trata de uma atividade que busca a constituição do material probatório a ser utilizado pelo órgão jurisdicional julgador na formação de seu convencimento. Destaque-se que a prova documental não precisa ser produzida em contraditório, bastando que seja submetida a um contraditório diferido, após sua juntada aos autos. Um exemplo dessa possibilidade é a produção antecipada de provas (art. 156 do CPP), desde que sejam consideradas urgentes e relevantes.

5. Fase da valoração - é o momento no qual o juiz exerce a análise crítica dos elementos de prova, atribuindo a cada qual o valor que julgar pertinente (sistema do livre

convencimento), de modo a permitir que, racionalmente, conclua sobre a procedência ou improcedência da pretensão punitiva. É importante salientar que a opção por uma, entre duas ou mais versões que se revelem conflitantes ou excludentes, deve ser feita por meio de aplicação de raciocínio lógico, razão pela qual incumbe ao magistrado conferir crédito somente àquilo que se mostrar verossímil e afinado com as regras da experiência comum, desconsiderando, por outro lado, tudo que se afigurar improvável. Toda prova produzida deve ser valorada pelo juiz, que ao fundamentar a sentença, deve pronunciar-se acerca de todas as provas produzidas, acolhendo aquelas que firmarão o seu convencimento em prejuízo das outras que serão desconsideradas. Segundo Takayanagi (2012), a valoração é, portanto, não só uma fase conclusiva de todo o procedimento probatório, mas também um ponto de observação privilegiado para se apreciar a efetividade do direito das partes a influir no acertamento dos fatos.

O devido respeito à legalidade em cada um dos momentos da atividade probatória culminando com a devida valoração, permite evitar arbitrariedades, julgamentos subjetivos e trilhar um caminho na busca da verdade que seja calcado no respeito aos direitos e garantias fundamentais constitucionalmente assegurados.

3.2.2 Provas Ilegais

Maria Cristina da Conceição Afonso (AFONSO, 2016) afirma que a proibição de prova surge como uma consequência necessária do princípio da legalidade probatória, com um amplo âmbito de aplicação quanto aos sujeitos abrangidos, pois aplica-se não apenas aos arguidos e autoridades judiciárias, mas a todas as pessoas que estejam envolvidas na obtenção e produção de prova com relevância para o processo. Afirma ainda que as provas proibidas são processualmente inadmissíveis em qualquer nível ou momento em que surjam. Acrescenta ainda que a demonstração de fatos nada valerá se a prova produzida e trazida a juízo tiver sido obtida fora do que é legalmente exigido, isso se sustenta no respeito a dignidade humana e nas garantias de defesa, correlacionadas com o processo penal.

Não haveria lógica em o Estado, buscando justiça, permitir que agentes agindo em seu nome ou mesmo particulares, violassem normas jurídicas para colheita de elementos de prova.

As provas ditas ilegais são gênero do qual derivam três espécies: as provas ilícitas, as provas ilícitas por derivação e as provas ilegítimas.

3.2.2.1 Provas Ilícitas

São aquelas obtidas com violação de regras de direito material (normas legais ou normas constitucionais). Notadamente, as garantias da pessoa, elencadas na Constituição, caso

sejam violadas, tornarão a prova ilícita. Nos termos do art. 5º, LVI da CR/88:

> Art. 5º (. . .) LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos;

Exemplos de provas ilícitas:

- confissão do acusado obtida por meio de tortura, por violar o art. 5º, III da Constituição da República;
- interceptação telefônica realizada sem ordem judicial, por violação do art. 5º da Constituição da República;
- busca e apreensão domiciliar sem ordem judicial, por violação do art. 5º, XI da Constituição da República; logo, ainda que se encontre material probatório que comprovem a corrupção ou outro crime em um SSD, o qual tenha sido obtido com invasão domiciliar não autorizada, essas provas são ilícitas.

Qualquer prova obtida por meio ilícito é uma prova ilegal. Mesmo antes de a lei 11.690/2008 ter alterado a redação do art. 157 do CPP, e fornecer uma definição do que se deve entender por provas ilícitas, os tribunais já vinham dando efetiva aplicação à sanção de inadmissibilidade prevista na Lei Maior, ora não permitindo o ingresso da prova ilícita no processo, ora determinando seu desentranhamento, ou mesmo desconsiderando tal prova no momento da valoração e, em consequência, absolvendo o acusado contra a prova ilícita a qual havia sido produzida (FILHO, 2010).

Deve-se destacar que não admitir no processo penal uma prova ilícita é, antes de tudo, uma forma de condenar a maneira de obtenção da prova.

3.2.2.2 Provas Ilícitas por Derivação

Essa questão remonta do ano de 1920, no caso Silverthorne Lumber Co. v. U.S., analisado pela Suprema Corte Americana, que a partir desse caso formulou a chamada Teoria dos Frutos da Árvore Envenenada (*fruits of the poison three doctrine*). Em termos práticos, essa teoria diz que provas que, embora sejam lícitas em sua essência, se derivam de uma prova ilícita, devem também ser afastadas.

> "A doutrina da ilicitude por derivação (teoria dos *fruits of the poison three doctrine*) repudia, por constitucionalmente inadmissíveis, os meios probatórios, que, não obstante produzidos, validamente, em momento ulterior, acham-se afetados, no entanto, pelo vício (gravíssimo) da ilicitude originária, que a eles se transmite, contaminando-os, por efeito de repercussão causal. Hipótese em que os novos dados probatórios somente foram conhecidos, pelo Poder Público, em razão de anterior transgressão praticada, originariamente, pelos agentes

> estatais, que desrespeitaram agarantia constitucional da inviolabilidade domiciliar." (HC 93.050 - RJ, 2.ª T., rel. Celso de Mello, 10.06.2008,v.u.).

Sem aprofundar mais na Teoria dos Frutos da Árvore Envenenada, mas realizando uma correlação com o exemplo da busca e apreensão domiciliar citada na subseção 3.2.2.1, não só as provas encontradas no SSD apreendido e que foi obtido com a violação ilegal do domicílio serão consideradas ilegais, mas também todas as outras provas que derivam de provas obtidas a partir do SSD.

Essa teoria foi expressamente colocada no CPP, a partir da Lei 11.690/2008 que deu a seguinte redação ao art. 157, parágrafo primeiro:

> §1º São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras.

O mesmo artigo traz duas ressalvas às provas ilícitas por derivação: quando não houver nexo de causalidade entre a ilicitude da obtenção da primeira prova e a obtenção da segunda ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras.

A primeira ressalva feita é desnecessária, uma vez que se não há relação de causalidade entre a primeira prova (obtida ilicitamente) e a segunda, não há que se falar em derivação.

Na segunda ressalva, estamos diante do que se chama de fonte independente capaz de conduzir ao objeto de prova. Ou seja, se a prova ilícita por derivação tiver sido obtida também por uma fonte independente da fonte contaminada, a prova deixará de ser ilícita por derivação e poderá ser utilizada no processo. A ressalva da fonte independente (*independent source limitation*) foi reconhecida pela Suprema Corte Americana em 1960. Outro caso consagrado pela jurisprudência americana é a descoberta inevitável (*inevitable discovery*), formulada também pela Suprema Corte Americana em 1984, segundo o qual também poderá ser utilizada a prova que, embora obtida por meio de uma prova ilícita, teria sido obtida inevitavelmente pela autoridade e não teria relação com a ilegalidade previamente cometida.

3.2.2.3 Provas Ilegítimas

São as provas obtidas com violação às regras de ordem processual, sem que haja nenhum reflexo de violação a normas constitucionais, um exemplo é a utilização de prova nova no plenário do júri, sem ter sido juntada aos autos com antecedência mínima de três dias, violando a regra contida no art. 479 do CPP.

3.3 ADMISSIBILIDADE DA PROVA

Com base no que já foi exposto, tanto sobre o CPP, quanto sobre o que consta no CPC, bem como no que há na doutrina, pode-se afirmar que a admissibilidade dos meios de prova é estabelecida por exclusão: em princípio, tudo aquilo que, direta ou indiretamente, possa servir para formar a convicção acerca da ocorrência de um fato é aceito como meio de prova.

Mas, como pode-se interpretar da discussão acerca das provas ilegais, é inadmissível que os fins - busca da verdade - justifiquem os meios - cometimentos de ilícitos por agentes do Estado ou particulares, violações imperdoáveis aos direitos e garantias fundamentais.

De acordo com João Conde Correia (CORREIA, 2006), citado na dissertação de mestrado de Vivaldino Manuel Guedes Tomás (TOMÁS, 2015):

> "Os horrores que o processo inquisitório (...) permitiu, demonstram que a busca da verdade não pode ser o fim exclusivo do processo penal. As experiências da inquisição, do nazismo ou de outros regimes totalitários não são para repetir. É hoje inquestionável que a justiça não pode ser alheia ao processo onde é gerada."

3.3.1 Admissibilidade da Prova antes da Constituição de 1988

No Brasil, mesmo antes da Constituição de 1988, já havia doutrinadores, legislação e jurisprudência que destacavam a importância de se limitar a atividade probatória. Assim, como doutrinador, pode-se citar Joaquim Canuto Mendes de Almeida (ALMEIDA, 1973) que afirma: "cerceia-se, mui justamente, a liberdade de investigação, quando, por exemplo, envolva invasões domiciliares, buscas e apreensões forçadas (...)".

Do ponto de vista legislativo, pode-se citar o art. 233 do CPP de 1941, ainda hoje com a mesma redação: "As cartas particulares, interceptadas ou obtidas por meios criminosos, não serão admitidas em juízo". O legislador deixou claro que cartas apreendidas com violação à lei não serão admitidas.

Quanto à jurisprudência, a partir do final da década de 1960 e antes ainda da Constituição de 1988, havia tendência de os tribunais considerarem que eventuais irregularidades em casos de buscas e apreensões, eram inaceitáveis e contaminavam todo o processo. Antonio Magalhães Gomes Filho (FILHO, 2010) cita o julgamento da Ap. 275.881 em que se afirma:

> "A ilegalidade da busca e apreensão domiciliar, por si só, prejudica, irreparavelmente, a ação penal, independentemente da própria acusação.(...) O direito da prova, meramente adjetivo, não se sobrepõe às garantias individuais de natureza constitucional substantiva." (TACRIM-SP, Ap. 275.881, rel. Albano Nogueira, j. 19.4.83, RT 579/348).

Do ponto de vista jurisprudencial, também não havia um entendimento pacífico sobre a questão de violações da lei para a obtenção de provas. Ricardo Cintra de Carvalho (CARVALHO, 1995) em sua pesquisa afirmou que durante um longo período a prova era analisada pela sua carga de convencimento, independente de sua forma de obtenção. As irregularidades cometidas durante a fase de obtenção eram tratadas como ilícitos administrativos ou penais, mas em procedimento separado que não impossibilitava a sua admissibilidade.

Antonio Magalhães Gomes Filho (FILHO, 2010) cita afirmações extraídas de acórdãos dos antigos Tribunais de Alçada e Alçada Criminal de São Paulo: "eventuais maus tratos impostos ao réu não infirmam o valor probante da confissão, que os demais elementos de convicção demonstram ter sido veraz". (TASP, ApCrim. 43797, rel Azevedo Franceschini, j. 05.02.1964, RT 356/293). Esse enunciado demonstra claramente que o Estado, em muitos julgamentos admitia a violação da lei, a pretexto da colheita de elementos probatórios.

Nessa nova visão que se sobressai, de tornar inadmissíveis as provas ilícitas, há posições do STF sobre a validade de interceptações telefônicas clandestinas. Nesses julgados o STF determinou que eram inadmissíveis as gravações de conversas telefônicas realizadas de forma irregular.

3.3.2 Admissibilidade da Prova após a Constituição de 1988

A inadmissibilidade das provas ilegais recebeu maior relevância com o advento da Constituição de 1988, uma vez que foi incluído no título "Dos Direitos e Garantias Fundamentais" o inciso LVI do art. 5º, que estabelece: "são inadmissíveis, no processo, as provas obtidas por meios ilícitos".

Mesmo com a clareza do texto constitucional, havia discordâncias doutrinárias ainda que minoritárias, são exemplos:

- Na doutrina, José Roberto Bedaque (BEDAQUE, 1996) afirma que não se pode concordar com a absoluta desconsideração das provas ilícitas (...) com a rejeição de uma prova obtida irregularmente, poderá o julgador ficar sem elementos suficientes para proferir uma decisão justa.

- Na jurisprudência, Gomes Filho (2010) cita que havia à época o argumento presente de que a política criminal deve ser orientada no sentido de proteger a sociedade e não o criminoso, de tal sorte que ao aplicar a nulidade por provas ilícitas de forma generalizada, será simplesmente impossível flagrar crimes que costumam disfarçar-se e, raramente, estes são praticados em praça pública.

No Brasil, no momento atual, o sistema de liberdade de prova, que se afina com as aspirações do processo penal de busca da verdade real, é limitado pelo princípio de vedação da prova ilícita, que tem previsão constitucional (art. 5°, LVI, no título "Dos Direitos e

Garantias Fundamentais") e também está explicitada no art. 157 do CPP (redação dada pela Lei nº 11.690/2008). Cabe aqui destacar uma exceção, qual seja, há autorização para a admissão da prova ilícita em favor do réu, para sua absolvição ou para comprovar fato importante para sua defesa. A jurisprudência dominante entende que a prova ilícita só pode ser utilizada *pro reo*, e nunca *pro societate*.

Além da liberdade de prova concedida às partes, no Brasil, o juiz forma sua convicção pela livre apreciação das provas produzidas em contraditório judicial, de acordo com sua análise dos fatos comprovados nos autos, é o chamado sistema do livre convencimento motivado. Esse sistema adotado no Brasil, contrapõe-se ao sistema da prova tarifada e ao sistema da íntima convicção, o juiz não está obrigado a conferir determinado "peso" a alguma prova, permite-se ao juiz dar o valor a prova que ele reputar pertinente. No entanto, essa liberdade dada ao Magistrado não é absoluta: o magistrado deverá fundamentar suas decisões, de forma que as provas devem estar nos autos do processo e sido produzidas sobre o crivo do contraditório judicial.

3.3.3 A importância das autorizações de Busca e Apreensão

Os procedimentos de busca e apreensão podem ocorrer tanto na fase judicial quanto na fase de investigação policial (com contraditório diferido). Podem ser determinados de ofício, a requerimento do Ministério Público, do defensor do réu, ou por pedido da autoridade policial. O procedimento de busca e apreensão pode ser lido no capítulo XI do CPP e pode ser domiciliar ou pessoal. Será de particular interesse para este trabalho a busca domiciliar e seus desdobramentos.

A busca domiciliar só pode ser realizada após decisão favorável da autoridade judiciária, em razão do princípio da inviolabilidade de domicílio, previsto no art. 5º, XI, da Constituição: "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial".

Para a doutrina e jurisprudência predominantes o CPP traz um rol taxativo de razões que autorizam a busca domiciliar. Essas razões estão enumeradas no art. 240 do CPP.

Os requisitos para a busca e apreensão estão no art. 243 do CPP: indicação da casa em que será realizada a diligência e o nome do respectivo proprietário ou morador; o motivo e os fins da diligência; subscrição pelo escrivão e assinatura do magistrado; constar, se houver, ordem de prisão.

O mandado de busca e apreensão deve ser o mais preciso possível, de forma a limitar ao estritamente necessário a ação da autoridade que realizará a diligência. Porém, a autoridade policial quando faz o pedido à autoridade judiciária, não tem como precisar a exata característica do objeto buscado, do seu quantitativo, pois podem ser documentos escritos, dispositivos computacionais, mídias de armazenamento externo de dados, por exemplo.

O art. 6º do CPP diz que:

> Art. 6º . Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
>
> II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;
>
> III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;
>
> (...)
>
> VII - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;

Ou seja, nem as disposições presentes no CPP no art. 240, nem as presentes no art. 6º mencionam qualquer obrigatoriedade de descrição pormenorizada do objeto buscado. Nos dois artigos do CPP são usados termos como: "objetos", "coisas achadas", "instrumentos", "qualquer elemento"; de sorte que o uso desses termos torna claro o caráter de "busca" e exige que esses artigos estejam relacionados com o fato ou que sirvam para o esclarecimento desse fato ou circunstância.

O mandado judicial de busca e apreensão pode ser melhor entendido como uma decisão judicial capaz de afastar a garantia constitucional da inviolabilidade de domicílio (art. 5º, XI, da Constituição), pode ser vista como uma medida cautelar que, portanto, busca evitar o perecimento da prova. Para que seja autorizada a busca e apreensão, assim como em outras medidas cautelares, devem estar presentes os requisitos para cautelaridade, que são o *fumus comissi delicti* (presença de indícios de materialidade e autoria de delito) e o *periculum in mora* (perigo que o retardo na produção torne impossível a colheita da prova).

Quanto à busca e apreensão de computadores que podem ocasionar a paralisação das atividades laborais de uma pessoa ou de uma organização, há uma situação ainda mais delicada a se tratar: uma punição para aquele que ainda está sendo investigado, o que configura um prejuízo ainda maior.

Para entender a importância da busca e apreensão com ênfase em dispositivos computacionais em sentido amplo, pode-se começar por citar o conteúdo da Portaria 1.287/2005-MJ (MJ, 2005) que nos arts. 3º e 4º afirma:

> Art. 3º Salvo expressa determinação judicial em contrário, não se fará a apreensão de suportes eletrônicos, computadores, discos rígidos, bases de dados ou quaisquer outros repositórios de informação que, sem prejuízo para as investigações, possam ser analisados por cópia (back-up) efetuada por perito criminal federal especializado.

> Parágrafo único. O perito criminal federal, ao copiar os dados, objeto da busca, adotará medidas para evitar apreender o que não esteja relacionado ao crime sob investigação.
>
> Art. 4º Os objetos e documentos arrecadados serão formalmente apreendidos e encaminhados a exame pericial assim que possível.
>
> § 1º Será facultado ao interessado extrair cópia dos documentos apreendidos, inclusive dos dados eletrônicos.
>
> § 2º Os objetos arrecadados ou apreendidos que não tiverem relação com o fato em apuração serão imediatamente restituídos a quem de direito, mediante termo nos autos.

A portaria 1.287/2005-MJ sofreu alterações significativas em 2009 com o advento da portaria 759 também do Ministério da Justiça (MJ, 2009), a qual revogou o art. 3º e seu parágrafo único. Reconhece-se colocar como regra que o perito forense computacional deva *in loco* realizar cópia (back-up) o que é uma limitação que cria obstáculo que certamente prejudicaria a busca pelos elementos informativos, e atrapalha a adoção das melhores práticas em forense computacional. A regra agora passa a ser a apreensão de suportes eletrônicos, computadores, discos rígidos, bases de dados ou quaisquer outros repositórios de informação, sem que seja necessária expressa determinação judicial para isso. A apreensão do material para análise não cria empecilho para a solicitação de backup de arquivos ou cópias de documentos apreendidos.

Ricardo Carneiro Gomes (GOMES, 2017) sustenta que o regramento jurídico pátrio estabelece regras para o cumprimento do mandado de busca e apreensão seja em residências, locais de trabalho, a serem observadas pela polícia. O mesmo autor declara que o mandado de busca e apreensão é dispensável para situações de flagrante delito. Sua afirmação sustenta-se na posição adotada por Tribunais Superiores:

> "Este Tribunal Superior prega que, por ser permanente o crime de tráfico de drogas, a sua consumação se protrai no tempo, de sorte que a situação de flagrância configura-se enquanto o entorpecente estiver sob o poder do infrator, sendo possível, portanto, em tal hipótese, o ingresso da polícia na residência, ainda que não haja mandado de prisão ou de busca e apreensão, já que incide a excepcionalidade inscrita no art. 5.º, XI, da CF/1988, a afastar a inviolabilidade do domicílio." (STJ, HC 208.957/SP, 6.ª T. rel. Des. convocado Vasco della Giustina, DJe 19.12.2011).
>
> "Estando o agente em situação de flagrante delito, torna-se desnecessário para acesso ao seu domicílio, o mandado de busca e apreensão judicialmente autorizado, bem como o consentimento do morador." (STJ, AgRg no Ag 1.357.515/DF, 5.ª T., rel. Min. Jorge Mussi, DJe 26.08.2011).

O professor Rogério Lauria Tucci (TUCCI, 2006) ensina - ao analisar procedimento cautelar de busca e apreensão, realizado a pedido de Delegado de Polícia que preside os autos do Inquérito Policial 117/03 - que a extrapolação dos limites da medida cautelar de busca e apreensão, possui manifesta ilegalidade, uma vez que só poderão ser apreendidos documentos que interessem à investigação em andamento, conforme consta do mandado de busca e apreensão expedido. Assim sendo, tais provas ilegitimamente colhidas[4], deverão ser excluídas, não tendo como permanecer, nem nos autos do procedimento em que foram originalmente inseridas, nem em outros procedimentos dele derivados.

Não só a busca domiciliar para apreensão de objetos relacionados com a infração penal apurada, mas também interceptações telefônicas são medidas cautelares que devem ser precedidas dos respectivos mandados judiciais, obtidos mediante representações. Há exemplos de atuações em que a inobservância dos princípios processuais ou a violação de normas de direito material acaba por tornar ilegal a prova produzida.

Foi citada, ao longo do texto da Seção 3, a ilegalidade da prova fruto de busca e apreensão de um SSD dentro de uma residência, sem o amparo de um mandado de busca e apreensão. Outro caso que necessitaria também de autorização judicial seria o acesso a dados que sirvam de prova de crimes e que estejam armazenados na nuvem. A não observância da solicitação de autorização para acesso desses dados na nuvem, estaria violando o art. 154-A do Código Penal Brasileiro, o que tornaria as provas porventura obtidas ilegais.

[4] Colhidas e coletadas, no contexto deste trabalho, estão empregadas indistintamente

4 *FORENSE COMPUTACIONAL*

De acordo com a *American Academy of Forensic Sciences* (AAFS), a Ciência Forense é a utilização de princípios científicos e práticas tecnológicas cujo objetivo é o de colaborar com a justiça na resolução de questões relacionadas a procedimentos criminais, civis e regulatórios. (AAFS, Boards of Directors , 1993)

Para o termo Forense Digital, uma definição amplamente adotada foi concebida no *Digital Forensic Research Workshop* (DFRWS) em 2001, "forense digital é o uso de métodos científicos acreditados para preservar, colher, validar, identificar, analisar, interpretar, documentar e apresentar evidências derivadas de fontes digitais com o intuito de facilitar ou reconstruir eventos criminosos, ou auxiliar a antecipar ações não autorizadas que se mostrem danosas às operações planejadas."

O *National Institute of Standards and Technology* (NIST) define a análise forense digital como a aplicação da ciência na identificação, colheita, exame e análise de dados, preservando a integridade das informações e mantendo uma cadeia de custódia estrita para os dados. (KENT et al., 2006)

Em sua mais restrita conotação, forense digital pode ser entendida como a aplicação da ciência da computação e de procedimentos investigativos envolvendo o exame de evidências digitais - seguindo a busca adequada, a cadeia de custódia, a verificação de integridade, ouso de ferramentas validadas, a repetibilidade, os relatórios e, possivelmente, o testemunho de especialistas (peritos).

O glossário do *Comittee on National Security Systems* (CNSSI 4009-2015) (DUKES, 2015) não distingue forense digital de forense computacional. Com certo preciosismo, pode-se dizer que tais termos não se confundem, uma vez que a forense digital se divide em várias categorias, sendo forense computacional apenas uma delas; assim como também são categorias: a forense em *cloud computing*, a forense em redes, a forense em dispositivos móveis.

Este Capítulo 4 propõe-se a mostrar o trabalho das ciências forenses, em especial da forense computacional, no auxílio à formação da convicção do magistrado. Procura-se aqui mostrar o elo que há entre a parte jurídica e a ciência, além do mais, demonstra-se que a falha nos campos jurídico, científico ou ainda procedimental pode causar prejuízos à persecução penal. Aqui se discute como diferentes sistemas jurídicos avaliam as provas informáticas e periciais. Alguns dos principais desafios no campo forense computacional são apresentados, com destaque para aqueles que guardam relação com a forense em dispositivos de armazenamento SSD. Trata-se aqui da importante temática de modelos de investigação, de modo que este trabalho apresenta um novo modelo, alinhado com a legislação brasileira e que servirá de embasamento para o Procedimento Operacional Padrão proposto adiante no Apêndice A. Por fim, aborda-se o tema "cadeia de custódia"

e a perspectiva de sua introdução no ordenamento jurídico brasileiro a partir do novo CPP (PL 8.045/2010) (DEPUTADOS, 2010), que encontra-se em tramitação.

4.1 ORIGEM DA PRÁTICA FORENSE E INÍCIO DAS DISCUSSÕES EM FORENSE DIGITAL

As ciências forenses voltam-se para o emprego do conhecimento científico diante de um tribunal, o propósito delas é contribuir para um debate qualificado sobre vestígios encontrados, além de fornecer respostas para questionamentos relevantes dentro de um processo judicial.

No documento da Secretaria Nacional de Segurança Pública (SENASP) intitulado Procedimento Operacional Padrão (SENASP, 2013) há procedimentos padronizados para sete áreas distintas de atuação, já a Polícia Federal (órgão ligado ao Ministério da Justiça) apresenta dezenove áreas de atuação para perito criminal federal.

Dentro do campo da forense, há as perícias tradicionais e a forense digital. A Figura 2 mostra alguns dos vestígios e dos objetos de estudo dos diferentes tipos de perícias.

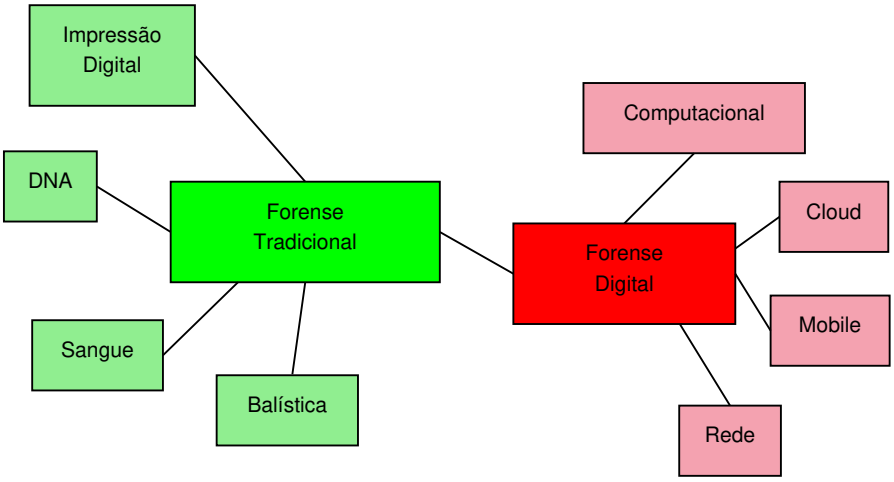


Figura 2 – Perícias tradicionais e digitais (LUTUI, 2016)

A forense tradicional, conforme mostrado na Figura 2, trabalha com elementos físicos, tangíveis como sangue, amostras de fluídos corporais ou pêlos (de onde se podem retirar amostras de DNA), impressões digitais, armas, substâncias ilegais.

Com o passar dos anos - e consequente avanço da ciência e da tecnologia -, um perito generalista já não era capaz de deter um conhecimento condizente com tantos campos diversos da ciência, logo, a especialização cada vez mais se fazia (e se faz) necessária, o que forçou o desmembramento ou a criação de novas áreas de perícia. Essas novas áreas da forense são necessárias a fim de se tentar acompanhar o desenvolvimento de novas técnicas e/ou de novas metodologias dentro de cada área. Com essa evolução, uma das áreas de especialização forense que mais têm se desenvolvido e recebido demandas judiciais é a área de forense digital.

A forense digital, talvez por ainda ser muito recente, enfrenta o ceticismo dos operadores do direito, de sorte que muitos deles não creditam confiança aos métodos utilizados. Outro motivo que pode justificar a desconfiança com a forense computacional e, de forma mais ampla, com o emprego de arquivos como prova em um tribunal é o fato de que a informação não é visível. De forma que o fato de os dados estarem armazenados - ainda que temporariamente - passam a ideia de que podem ser alterados a qualquer tempo sem deixar nenhum rastro dessa alteração, o que normalmente não é verdade conforme será discutido.

A Forense digital foi concebida durante muito tempo como a atividade de extrair evidências de dispositivos digitais para uso em procedimentos judiciais, essa é a tarefa mais comum e a que vai interessar a este trabalho, mas sua aplicabilidade foi ampliada e hoje há várias diferentes categorias, cada uma com suas respectivas peculiaridades:

- Forense em *Cloud*;
- Forense em Dispositivos Móveis;
- Forense em Redes;
- Forense Computacional;
- Forense em *Malware*;

Mesmo com tantas divisões, pode-se dizer que a forense digital é algo recente, tanto o é que o principal fórum de discussões em forense digital - o *Digital Forensics Research Workshop* (DFRWS) - teve a sua primeira edição realizada em 2001. Foi, portanto, no DFRWS que alguns dos principais tópicos de pesquisa e melhores práticas foram apresentadas.

4.2 PRÁTICA FORENSE COMPUTACIONAL

A forense computacional tem por objetivo extrair provas digitais de sistemas computacionais suspeitos, de forma que preserve seu valor legal, usando essa evidência para construir e provar hipóteses sobre crimes e, finalmente, dando subsídios para que o juiz encarregado do caso possa formar sua convicção. Envolve também as mídias de armazenamento persistente (SSD, HDD, pen drive) que são empregadas nos computadores.

A análise do armazenamento persistente de dados é feita, em regra, através do sistema computacional - no qual a mídia de armazenamento estava originalmente instalada - desligado, dando origem à técnica de forense computacional conhecida como *post mortem*, em oposição à *live analysis*.

O processo de investigação forense, a princípio, dividia-se nas duas técnicas mencionadas *live analysis* e *post-mortem*. (HUEBNER; BEM; BEM, 2007) sugeriu uma terceira técnica que se baseava na ideia de recriar o cenário a ser investigado.

Live Analysis

Essa técnica se presta a colher também as informações que possuem alta ordem de volatilidade[1]. A *live analysis* altera os dados armazenados na memória de forma que essas alterações são aceitas por serem inevitáveis, contudo há alterações que não são admitidas. Uma manipulação mal feita pode gerar dados falsos ou omitir informações, além de haver o risco de que uma conexão aberta esteja sendo usada para apagar evidências contidas no dispositivo enquanto ele está sendo analisado por peritos.

Post-mortem

Abordagem tradicional, cuja premissa é a preservação das evidências armazenadas em mídias não voláteis. Os equipamentos estão previamente desligados ou, se estiverem ligados, serão desligados após encontrados. A fonte de informação é o conteúdo de informação contido nas mídias não voláteis o que torna mais fácil garantir que as mídias não sofram alteração. Consiste em realizar uma análise em laboratório, em um ambiente controlado em que inicialmente se faz uma cópia forense dos dados para só então iniciar a análise, visando assim evitar alterações na mídia original.

Reprodução do Ambiente

Uma nova abordagem em investigação forense computacional é tentar recriar o sistema computacional e seu ambiente. Mesmo que a abordagem não seja admitida em um tribunal, ela é muito útil e poderá determinar as razões da brecha de segurança causada por um *bug*, quando não há intenções criminosas, por exemplo(HUEBNER; BEM; BEM, 2007).

4.2.1 Técnicas de forense computacional

Segundo (JÚNIOR; QUEIROZ, 2014), além da definição da estrutura geral dos processos ou modelos[2] de investigação de forense computacional (passos básicos da análise forense computacional) que deve ser seguida, outra questão que ainda suscita discussão em forense computacional diz respeito à melhor abordagem a se adotar ao se deparar no local das buscas com uma máquina ainda em funcionamento. Nesse caso três abordagens são possíveis:

1. realizar alguns procedimentos aproveitando-se da máquina ligada (técnica de *live analysis* e de reprodução do ambiente);
2. desligá-la através da interrupção do fornecimento de energia (*post-mortem* 1);
3. proceder desligamento administrativo normal (*post-mortem* 2).

Em (AULER et al., 2011), afirma-se que em casos de busca e apreensão de computadores é recomendável realizar uma colheita de dados voláteis e de dados lógicos de áreas

[1] diz que possuem alta ordem de volatilidade aqueles dispositivos de armazenamento que após a retirada da fonte de energia rapidamente perdem a informação armazenada

[2] os modelos de investigação de forense computacional serão discutidos na Seção 4.7.

protegidas por senha enquanto o computador ainda estiver ligado, antes de efetuar o desligamento da máquina para apreensão tradicional.

4.3 A PROVA INFORMÁTICA

A tecnologia tem sido protagonista nessa transição em que se busca maior grau de certeza e confiabilidade da prova. Na forense computacional, podem ser fontes de prova os computadores e suas mídias de armazenamento, uma vez que esses dispositivos estão sendo cada vez mais empregados em várias áreas diferentes e, por meio deles, negócios podem ser realizados ou documentados. Com isso, registros informáticos e cópias impressas desses registros podem ser usados como meio de prova. Segundo Taruffo (TARUFFO; MICHELI, 2014), quando o computador é usado apenas para redigir um documento que será impresso e assinado pelas partes, não se vislumbram problemas, uma vez que pode ser apresentado como qualquer outra prova documental. Contudo, na atualidade os dados e arquivos informáticos estão sendo empregados como o único suporte em muitas transações.

O terma "prova eletrônica" é também empregado de forma similar ao "prova informática". Para (LESSA, 2010) prova eletrônica é aquela cujo local de armazenamento seja eletrônico e cujo elemento armazenado consista em uma sequência de números binários que, reconhecidos pelo computador, representam uma informação.

4.3.1 A prova informática no *commom law*

Nos EUA e Inglaterra o *Common law*[3] é a base do sistema jurídico.

Nos EUA, para se verificar a confiabilidade da prova informática, exige-se a prova de que todo o maquinário que produziu o documento eletrônico funcionou correta e apropriadamente.

Na Inglaterra, havia uma definição ampla do termo "documento" o qual incluía os arquivos informáticos, havia uma seção que se ocupava especificamente da admissibilidade de documentos produzidos por computador e exigia o cumprimento de várias condições específicas. Posteriormente, documentos informáticos passaram a ser tratados como outro tipo de documento, presumindo-se a sua autenticidade, salvo prova em contrário (TARUFFO; MICHELI, 2014).

Assim, pode-se dizer que ambos os sistemas estabeleceram a admissibilidade das provas informáticas.

4.3.2 A prova informática no *civil law*

Países como EUA e Inglaterra que adotam um sistema jurídico que se baseia, em grande parte, em decisões de casos anteriores, eles diferem de países que adotam um sistema

[3] Common law - sistema jurídico que se desenvolve por meio das decisões dos tribunais.

jurídico em que há uma preocupação em escrever leis para que os julgadores baseiem nelas as suas decisões. A visão dominante em sistemas de *civil law*[4] é de que são possíveis analogias entre provas informáticas e provas documentais, reconhecendo que documentos podem ser criados também por novas tecnologias (TARUFFO; MICHELI, 2014).

Na França, após a lei 2000-230 promulgada em 2000, adotou-se o princípio da plena equivalência entre as provas informáticas e as provas escritas sempre que o autor da declaração possa ser identificado facilmente e que o documento eletrônico tenha sido criado e conservado adequadamente. Na Itália, segue-se também a equivalência, mas há disposições detalhadas de técnicas a serem adotadas para a criação de documentos eletrônicos (TARUFFO; MICHELI, 2014).

Portanto, tanto na França quanto na Itália há uma regulamentação a ser seguida, e desde que a assinatura eletrônica [5] seja formulada conforme métodos técnicos e jurídicos específicos, é equivalente à forma manuscrita.

4.3.3 A prova informática no Brasil

Não só o trâmite judicial está adotando ferramentas tecnológicas oriundas da informática, mas também as decisões dos tribunais demonstram a aceitação de arquivos eletrônicos como provas. O Supremo Tribunal Federal, por exemplo, já entendeu como válida a utilização de arquivo eletrônico (SILVA, 2011).

Além de julgados dos Tribunais Superiores, a Medida Provisória 2.200/2001, que instituiu a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, trata o arquivo eletrônico como documento e garantiu-lhe a presunção de veracidade, se ele for assinado digitalmente[6] com certificado digital emitido pela ICP-Brasil ou outro certificado aceito pelas partes (BRASIL, 2001).

Muitos órgãos governamentais, além do já mencionado judiciário, utilizam-se de sistemas de tramitação eletrônica de documentos, em que as assinaturas dos documentos são realizadas por meio de assinatura digital. Destaca-se o Sistema Eletrônico de Informações (SEI) (BRASIL, 2019) que vem sendo adotado no Governo Federal em vários ministérios, os documentos gerados e assinados inteiramente dentro da plataforma SEI gozam de fé pública e sua tramitação pode ocorrer inteiramente através de sistemas informáticos, sem que seja necessária qualquer impressão em papel ou assinatura física.

[4] Civil law - sistema jurídico, baseado no direito romano, por meio do qual o direito é escrito e organizado em códigos.

[5] Assinatura eletrônica - é o gênero referente a todos os métodos utilizados para assinar um documento eletrônico, assinatura digital é uma das espécies de assinatura eletrônica.

[6] Assinatura digital - é um método de autenticação de informação digital que utiliza sistemas de criptografia de chave pública e é capaz de substituir à assinatura física, uma vez que elimina a necessidade de ter uma versão física do documento que necessita ser assinado.

4.3.4 Controvérsias da Prova Informática no Brasil

Para Demócrito Reinaldo Filho, há alguns problemas em relação à prova eletrônica, tais como o fato de que a informação em formato eletrônico é dinâmica, de sorte que o mero ato de ligar ou desligar um computador pode alterar a informação que ele armazena. Isso porque "os computadores quando em funcionamento reescrevem e deletam informação, quase sempre sem o conhecimento específico do operador" e "a informação armazenada eletronicamente, ao contrário de textos escritos em papel, pode se tornar incompreensível quando separada do sistema que a criou" (FILHO, 2006). Renato Blum afirma que é uma questão de extrema relevância a validade dos documentos eletrônicos, visto que por meio de recursos técnicos é possível alterar documentos digitais sem deixar vestígios (BLUM, 2012). Breno Lessa em seu artigo intitulado "A inviabilidade das provas digitais no processo judiciário" (LESSA, 2010) afirma: "a integridade do documento eletrônico só poderia ser confirmada se fosse possível assegurar que o documento não foi atacado, não foi alterado ou adulterado, mas isso é praticamente impossível, principalmente nos computadores pessoais".

Desse modo, a aceitação da prova eletrônica, como já visto, é perfeitamente possível, mas uma série de procedimentos devem ser tomados para que a prova não seja descartada por suspeita de sua adulteração, por exemplo. A força probante de um documento digital será maior quanto maior for definida sua autoria, sua autenticidade e sua integridade.

4.4 A PROVA PERICIAL

A prova pericial é o meio de prova que tem como objetivo esclarecer fatos que exijam um conhecimento técnico específico quando o julgador não possuir conhecimento técnico ou científico necessários para estabelecer ou avaliar alguns fatos em discussão, ou quando o julgador acreditar que é conveniente, de forma que pode recorrer ao(s) perito(s) para que sejam prestados esclarecimentos que o auxiliem a decidir.

4.4.1 A prova pericial no *commom law*

Na *comomm law*, a apresentação de provas periciais baseia-se na condição de testemunha do perito, daí o termo *expert witness* (testemunha especialista, em tradução livre). Nos Estados Unidos, os peritos podem ser apresentados pelas partes, o que demonstra que se trata de uma profissão bem estabelecida para assessorar acusação e defesa em casos judiciais. Na Inglaterra, as partes não podem utilizar provas periciais sem autorização do tribunal e este possui amplos poderes de controle sobre tais provas. A partir de uma reforma que houve em 1999 na Inglaterra, o perito tem a obrigação fundamental de proceder com a verdade, imparcialidade e transparência perante o tribunal (TARUFFO; MICHELI, 2014).

4.4.2 A prova pericial no *civil law*

Nos sistemas de *civil law*, o perito não é uma testemunha, e a prova pericial não tem nada em comum com a prova testemunhal. A função principal do perito é oferecer ao tribunal conhecimento especializado a ser utilizado no seu veredicto do juiz acerca dos fatos em litígio.

No *civil law*, o princípio mais importante é o da neutralidade do perito. Segundo Taruffo (TARUFFO; MICHELI, 2014), o Código de Processo Civil francês inclui uma regulação ampla e muito articulada das provas periciais, de sorte que o perito é obrigado a desempenhar sua tarefa pessoalmente e com objetividade e imparcialidade, sob a direção e o controle do juiz.

Pelo menos dois princípios relacionados à perícia são comuns no *civil law* e no *commom law*:

- a garantia do devido processo legal também nas provas periciais, sendo assegurada às partes oportunidade de participar nas atividades do perito;
- a não vinculação do julgador, de modo que a prova pericial é sempre apreciada de forma discricionária pelo tribunal.

4.4.3 A prova pericial no Brasil

No Brasil, o Capítulo II do CPP trata dos institutos de exame de corpo de delito e das perícias em geral. O sistema do livre convencimento motivado (previsto no art. 155 do CPP) permanece válido e guarda estreita relação com o sistema liberatório de apreciação da prova pericial (art. 182 do CPP).

Assim sendo, caso convocado perito oficial, apenas um perito é necessário e este, por ser servidor público e já ter obrigação de lisura, não presta compromisso. No caso de peritos não oficiais, são necessários dois peritos, portadores de diploma de nível superior, os quais deverão prestar compromisso (art. 159 § 2º do CPP).

Muitas das informações constantes do CPP sobre perícia foram atualizadas em 1994 pela lei 8.862/94 e em 2008 pela lei 11.690/2008, e não seguem a redação original do Código de Processo Penal de 1941. São exemplos de atualizações:

> Art. 159. O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.(Redação dada pela Lei nº 11.690, de 2008)
>
> § 1o Na falta de perito oficial, o exame será realizado por 2 (duas) pessoas idôneas, portadoras de diploma de curso superior preferencialmente na área específica, dentre as que tiverem habilitação técnica relacionada com a natureza do exame.(Redação dada pela Lei nº 11.690, de 2008)

§ 2o Os peritos não oficiais prestarão o compromisso de bem e fielmente desempenhar o encargo.(Redação dada pela Lei nº 11.690, de 2008)

§ 3o Serão facultadas ao Ministério Público, ao assistente de acusação, ao ofendido, ao querelante e ao acusado a formulação de quesitos e indicação de assistente técnico. (Incluído pela Lei nº 11.690, de 2008)

§ 4o O assistente técnico atuará a partir de sua admissão pelo juiz e após a conclusão dos exames e elaboração do laudo pelos peritos oficiais, sendo as partes intimadas desta decisão.(Incluído pela Lei nº 11.690, de 2008)

§ 5o Durante o curso do processo judicial, é permitido às partes, quanto à perícia: (Incluído pela Lei nº 11.690, de 2008)

I - requerer a oitiva dos peritos para esclarecerem a prova ou para responderem a quesitos, desde que o mandado de intimação e os quesitos ou questões a serem esclarecidas sejam encaminhados com antecedência mínima de 10 (dez) dias, podendo apresentar as respostas em laudo complementar;(Incluído pela Lei nº 11.690, de 2008)

II - indicar assistentes técnicos que poderão apresentar pareceres em prazo a ser fixado pelo juiz ou ser inquiridos em audiência.(Incluído pela Lei nº 11.690, de 2008)

§ 6o Havendo requerimento das partes, o material probatório que serviu de base à perícia será disponibilizado no ambiente do órgão oficial, que manterá sempre sua guarda, e na presença de perito oficial, para exame pelos assistentes, salvo se for impossível a sua conservação.(Incluído pela Lei nº 11.690, de 2008)

§ 7o Tratando-se de perícia complexa que abranja mais de uma área de conhecimento especializado, poder-se-á designar a atuação de mais de um perito oficial, e a parte indicar mais de um assistente técnico.(Incluído pela Lei nº 11.690, de 2008)

Art. 160. Os peritos elaborarão o laudo pericial, onde descreverão minuciosamente o que examinarem, e responderão aos quesitos formulados.(Redação dada pela Lei nº 8.862, de 28.3.1994)

Parágrafo único. O laudo pericial será elaborado no prazo máximo de 10 dias, podendo este prazo ser prorrogado, em casos excepcionais, a requerimento dos peritos.(Redação dada pela Lei nº 8.862, de 28.3.1994)

4.5 IMPORTÂNCIA DA FORENSE COMPUTACIONAL

A atividade pericial tem sido determinante em diversos delitos que se utilizam de dispositivos computacionais para a sua execução, por exemplo:

Crimes Sexuais Contra Vulneráveis - tem-se tornado comum no Brasil e no mundo o desbaratamento de redes internacionais de compartilhamento de pornografia infantil. Há casos, inclusive, por meio dos quais se chega também aos autores que podem ser enquadrados, no Brasil, em diversos artigos distintos do Estatuto da Criança e do Adolescente (Lei nº 8.069, de 1990), tais como estupro de vulnerável, favorecimento a prostituição, comércio de material pedófilo, aliciamento de crianças, dentre outros.

Comércio de Substâncias Ilícitas - como ocorria de forma bastante organizada na *Darknet*[7] em um site chamado Silk Road[8], que realizava o comércio de drogas ilícitas, dentre outros produtos, por meio de mecanismos que mantinham o anonimato de vendedores e de compradores.

Crimes Financeiros - com a quantidade de serviços disponibilizados por bancos e por lojas virtuais, os criminosos frequentemente usam a Internet para encontrar vítimas de fraude, usando diferentes tipos de *malware* ou de técnicas de engenharia social. De sorte que o crime financeiro mudou e foi para a Internet, o mesmo acontece com o trabalho das polícias, cada vez mais necessário no mundo virtual.

Em síntese, muitos tipos de crimes estão agora sendo cometidos por meio de sistemas computacionais, portanto, diante da demanda de combater essa diferente prática delituosa, vem sendo desenvolvida a forense computacional, cujo objetivo é permitir que os criminosos possam ser presos e que provas produzidas subsidiem adequadamente a condenação, quando for o caso.

Além de buscar identificar o crime, os criminosos e angariar elementos suficientes que permitam uma condenação, dependendo do país, os peritos podem auxiliar a defesa, auxiliar a acusação e/ou auxiliar o julgador.

Em termos gerais, os métodos e algoritmos computacionais permitem ao perito revelar evidências, analisá-las e identificá-las de maneira objetiva e reproduzível; avaliar a qualidade de um método de exame; relatar e padronizar procedimentos investigativos; pesquisar grandes volumes de dados de forma eficiente; visualizar e documentar os resultados da análise; auxiliar na interpretação dos resultados; e contribuir para a geração de novos conhecimentos.

4.6 DESAFIOS DA FORENSE COMPUTACIONAL

Como campo em constante evolução, nem mesmo os crescentes desenvolvimento e especialização de novos processos e práticas tecnológicas são suficientes para resolver todos os

[7] Darknet - associado à parte cifrada da Internet e, muitas vezes, com restrições ao acesso, onde podem ocorrer negociações ilícitas

[8] Silk Road - site de comércio eletrônico, muito conhecido por ser uma plataforma de comércio de produtos ilegais, que foi fechado pelo FBI

casos que se apresentam ao perito, a pesquisa de Karie e Venter (KARIE; VENTER, 2015) enumerou uma grande quantidade de desafios para o campo forense. Desafios os quais formam uma longa lista que pode ser agrupada em quatro grandes grupos: técnicos, jurídicos, pessoais e operacionais. A partir dessa lista de desafios criada por Karie e Venter, que não encerra todos, foram destacados nesta tese alguns desafios guardam relação com a forense computacional de unidades de armazenamento SSD.

4.6.1 Desafios Técnicos

Há vários impactos no trabalho forense computacional tratados como desafios técnicos, no trabalho (MOHAY, 2005) são tratados como desafios técnicos que surgiam àquela época o grande volume de dados, o impacto de sistemas computacionais embarcados, a governança corporativa.

Para (KARIE; VENTER, 2015), desafios Técnicos são aqueles que podem ser enfrentados com conhecimento, protocols ou operações existentes. Nesse trabalho de Karie e Venter são elencados como desafios tecnológicos: cifragem, grande volume de dados, volatilidade da evidência digital, vida útil limitada da mídia digital, sofisticação dos crimes digitais, tecnologias emergentes, técnicas anti-forense.

A seguir estão destacados três desafios tecnológicos mencionados por Karie e Venter que guardam estreita relação com o trabalho forense computacional sobre dispositivos de estado sólido.

Vida Útil Limitada da Mídia Digital - um bloco de memória flash suporta um número limitado de ciclos P/E [9] antes de causar o comprometimento dos dados, conforme será discutido mais detalhadamente na Seção 5.

Tecnologias Emergentes - o SSD é uma tecnologia que funciona internamente diferente de um HDD e sua adoção vem crescendo com o barateamento da tecnologia e o crescimento da capacidade de armazenamento, essa tecnologia impôs sérias dúvidas quanto a viabilidade de procedimentos forenses computacionais.

Grande quantidade de dados não estruturados - a grande quantidade de dados e a evidência digital que frequentemente está com erro, é incerta ou é incompleta (FRANKE; ÅRNES, 2017).

4.6.2 Desafios Jurídicos

Os desafios jurídicos recebem especial destaque na Seção 3 e nesta Seção 4. O trabalho em forense computacional não pode negligenciar questões e discussões jurídicas, caso nuances do direito tenham sido negligenciadas no decorrer do trabalho forense, pode-se ter a completa inutilização do material probatório obtido. Pode-se dizer que desafios jurídicos

[9] ciclos de Programação/Apagamento (do inglês *Program/Erase*)

dizem respeito a existência de leis que tipificam adequadamente as condutas criminosas, se há apoio legal na condução de um processo penal ou de um processo civil. A seguir, destacam-se pontos jurídicos que podem influenciar na atividade forense computacional relacionada a trabalhos com SSD.

Admissibilidade de Ferramentas e Técnicas Forenses Digitais - como em todas as outras disciplinas forenses, as técnicas e ferramentas forenses digitais devem atender aos padrões básicos de evidência e padrões científicos a serem permitidos como evidência em procedimentos legais. Isso também significa que as ferramentas, as técnicas, os processos e os procedimentos devem ser provados como corretos através de testes empíricos. No contexto da análise forense digital, isso significa que as ferramentas técnicas, processos e procedimentos usados na colheita e análise de dados de evidências digitais devem ser validados e comprovados para atender aos padrões científicos. (KARIE; VENTER, 2015).

Múltiplas Jurisdições Dificultam Prisões - crimes que envolvem o emprego de computadores e a internet não respeitam fronteiras, de modo que há necessidade de uma cooperação internacional para o combate deste tipo de criminalidade. Muitos indivíduos passam a agir, a realizar ataques a partir de países em que o sistema jurídico ainda não coibe determinadas ações.

Robustez Forense - qualquer método usado para análise forense digital deve levar em consideração a integridade forense. A perícia computacional deve assegurar que a integridade das evidências e a cadeia de custódia sejam incorporadas, reduzindo assim a probabilidade de erros não intencionais e adulteração de evidências intencionais.

4.6.3 Desafios Relacionados ao Pessoal

A evidência digital deve estar sob o controle de pessoal responsável e peritos bem treinados para assegurar ao tribunal o fato de que a evidência está completa e não foi adulterada de alguma forma.

Falta de Pessoal Qualificado (Treinamento, Educação e Certificação) - a forense digital tornou-se um campo importante devido ao aumento de crimes digitais. No entanto, há uma escassez de pessoal treinado neste campo. Peritos forenses digitais qualificados são difíceis. Logo, ainda que especialistas tecnicamente proficientes estejam disponíveis, muito poucos são treinados ou certificados para fornecer testemunhos convincentes, cientificamente válidos diante de um tribunal.

4.6.4 Desafio Operacional

Para Karie e Venter, há necessidade de estabelecer princípios gerais, que incluam um padrão mínimo de planejamento, de desempenho, de monitoramento, de registro e de

relatório, além disso é possível se fazer a recomendação de processos, procedimentos, soluções de software e hardware.

Com culturas, legislações tão diversas, estabelecer modelos para nortear o trabalho pericial é uma tarefa difícil, porém importante, vários dos modelos criados serão citados na Seção 4.7, porém sem que um deles se sobressaia perante aos demais, talvez por isso, em (KARIE; VENTER, 2015) um dos desafios operacionais é a falta de processos e procedimentos padronizados.

Falta de processos e procedimentos padronizados - a falta de padronização em análise forense digital dificulta seriamente o processo de investigação e dificulta a produção de provas digitais legalmente admissíveis. Atualmente, não existe um modelo de processo de investigação forense digital padronizado para recuperar possíveis evidências digitais. Há um grande número de modelos forenses digitais, alguns deles serão mostrados na Seção 4.7.

4.6.5 Panorama no Brasil

No que tange os desafios de se realizar trabalhos de perícia no Brasil, em geral, é necessário maior apoio e investimentos por parte do Poder Público.

O documento Diagnóstico Perícia Criminal (SENASP, 2012) emitido pela Secretaria Nacional de Segurança Pública - SENASP, mostra a falta de estruturas minimamente padronizadas dos institutos de perícia criminal existentes no Brasil. Ainda segundo o documento, se falta pessoal, equipamentos e capacitação, falta mais do que tudo uma gestão adequada, sem a qual o país seguirá carente desse serviço tão relevante o qual, em conjunto com outras provas, contribui para que a autoridade judicial forme a sua convicção, seja para absolver ou para condenar, protegendo direitos e reduzindo a impunidade.

A lei 12.735/2012 (BRASIL, 2012) acrescenta ao Código Penal Brasileiro um artigo que obriga os órgãos de polícia judiciária a se estruturarem para o combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

4.7 PRINCÍPIOS E MODELOS FORENSE DIGITAIS

As investigações forenses para que sejam melhor conduzidas, devem ser feitas respeitando determinados princípios e seguindo etapas padronizadas. Ao longo dos anos, a forense digital vem sendo melhor compreendida e muitas pesquisas científicas sugerem princípios para o trabalho pericial e modelos que buscam identificar as etapas ideais para a condução desse processo investigativo.

Alguns dos princípios que norteiam o trabalho pericial são enunciados em manuais de procedimentos policiais (DIVISION, 2018) (ACPO, Police Central e-crime Unit, 2012) quatro princípios consagrados para o trabalho forense computacional são:

- Nenhuma ação tomada pelos encarregados de aplicação da lei, por peritos ou pessoas que tenham acesso às evidências deve alterar os dados (em um computador ou mídia de armazenamento) que poderão ser usados como prova;
- Diante de situações excepcionais em que seja necessário acesso aos dados originais, aquela pessoa deve ser competente para fazê-lo e capacitada para justificar a importância de suas ações;
- Um rastreamento ou registro de tudo que foi feito com a evidência deve ser criado e preservado, para que possa ser reproduzível por terceiros;
- A pessoa responsável pela investigação tem a responsabilidade geral de garantir que a lei e esses princípios sejam cumpridos.

Um princípio fundamental que deve ser mantido através de todas as etapas de uma investigação forense foi enunciado por (JR; ROSA, 2015) e diz respeito a **mesmidade**. Mesmidade, segundo os autores, é a garantia de que a prova valorada é exatamente e integralmente aquela que foi colhida, correspondendo portanto "a mesma".

Os modelos de investigação buscam entregar a prova, portanto, da mesma forma que foi colhida, para isso dividem as fases da investigação em diferentes etapas interligadas.

Além do estudo de modelos e procedimentos, baseada em trabalhos anteriores que veremos a seguir (da Seção 4.7.1 até a Seção 4.7.9), será feita a propositura de um novo modelo na Seção 4.7.10.

4.7.1 DFRWS (2001)

O processo investigativo passou a estabelecer um processo linear que pode ser ilustrado através da Figura 3, esse processo foi proposto no documento da primeira *Digital Forensic Research Conference*.

4.7.2 Modelo de Kruse e Heiser (2002)

Kruse e Heiser desenvolveram um modelo para realização da atividade forense computacional baseada em três etapas básicas: adquirir, autenticar e analisar (GUO; JIN; HUANG, 2010). As três etapas preocupam-se em manter a integridade da evidência durante toda a investigação e, para garantir a integridade, é essencial documentar toda a investigação. Caso a integridade seja inevitavelmente violada, com uma documentação detalhada será possível pelo menos saber o que foi realizado.

As três etapas podem ser resumidas da seguinte forma:

1. Adquirir - colher a evidência sem alterar ou danificar a original, pode ter como passos: manipulação da evidência, cadeia de custódia, colheita, identificação, armazenamento, documentação da investigação;

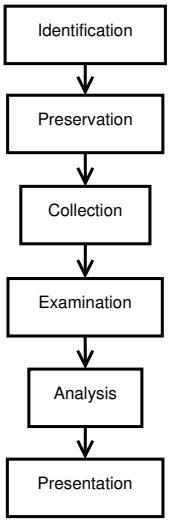


Figura 3 – Modelo de Investigação DFRWS (PALMER, 2001)

2. Autenticar - para demonstrar que a evidência recuperada é a mesma da que foi originalmente apreendida;

3. Analisar - analisar os dados sem modificá-los.

O modelo proposto por Kruse e Heiser é simples e já demonstrava a importância de manter uma documentação do processo forense computacional, a importância de verificar a integridade, mas não se preocupava com aspectos da legislação, no que diz respeito a busca e apreensão.

4.7.3 Abstract Model (2002)

Basicamente trata-se de um aperfeiçoamento do modelo DFRWS. Adiciona duas fases extra entre a identificação (*identification*) e a preservação (*preservation*), que são a preparação (*preparation*) e a estratégia de abordagem (*approach strategy*). Foi adicionada ainda uma fase de retorno da evidência (*returning evidence*). A Figura 4 ilustra este modelo.

4.7.4 NIJ (2001), NIST (2006) e ACPO (2007)

Trata-se de um modelo reduzido, com apenas quatro passos. Segundo (JAFARI; SATTI, 2015) não é apropriado para realizar uma investigação digital minuciosa, a fase de análise deles é indevidamente definida e ambígua.

4.7.5 Modelo de Guo e outros (2010)

O modelo proposto por Guo e outros (GUO; JIN; HUANG, 2010) é apresentado na Figura 6 e contempla nove componentes, são eles: *identification*, *preparation*, *collection*, *preservation*, *examination*, *analysis*, *review*, *documentation* e *report*.

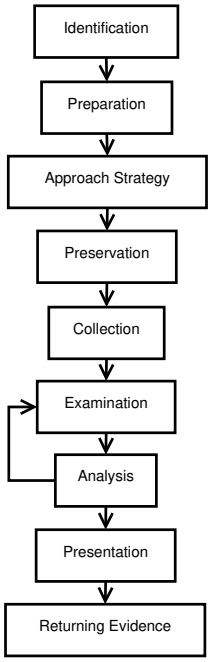


Figura 4 – *Abstract Digital Forensic Model* (REITH; CARR; GUNSCH, 2002)

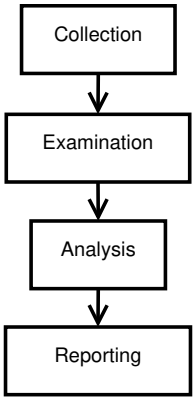


Figura 5 – *Forensic Investigation Process* (KENT et al., 2006)

O modelo proposto por Guo e outros, apesar de trazer importantes contribuições, acrescenta muitas etapas, elas não são bem detalhadas ao longo do artigo (GUO; JIN; HUANG, 2010). Embora na prática algumas tarefas possam acontecer em paralelo, dependendo do que seja realizado nas etapas de *Examination* e *Analysis*, a atividade em paralelo não faria sentido. Outro ponto que merece uma análise cuidadosa é que a autorização legal para uma busca e apreensão (*Preparation*) em um local de crime, em regra, precede a identificação do que será a fonte da evidência (*Identification*).

4.7.6 Yusoff (2011)

No trabalho *Common Phases of Computer Forensics Investigation Models*(YUSOFF; ISMAIL; HASSAN, 2011) os autores propõe um novo modelo de investigação forense computacional que eles denominaram *generic computer forensics investigation model* e que está

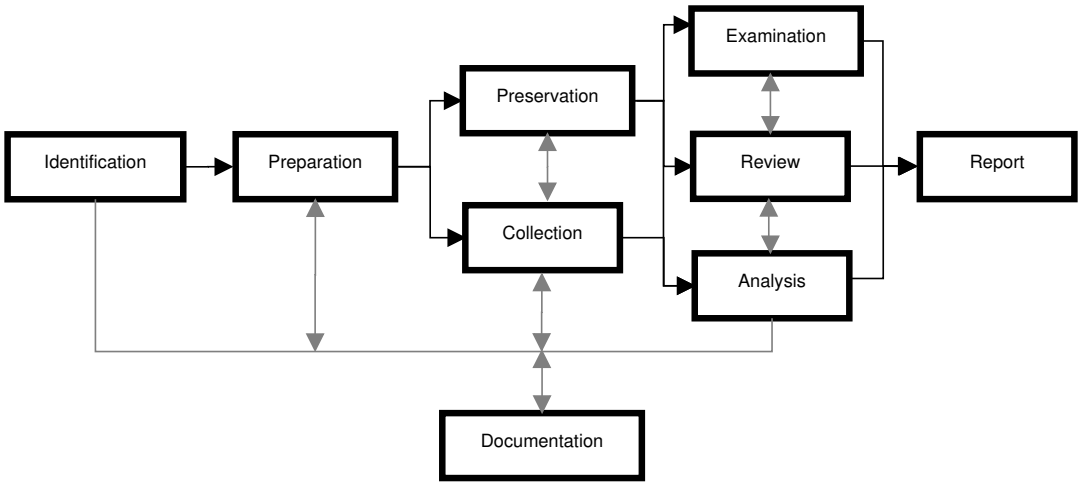


Figura 6 – Modelo de Investigação Proposto por Guo e outros (GUO; JIN; HUANG, 2010)

ilustrado na Figura 7.

No lugar de um processo sequencial, os autores sugerem que se deve permitir voltar para fases anteriores, não só para corrigir possíveis erros, mas também para adquirir novas informações.

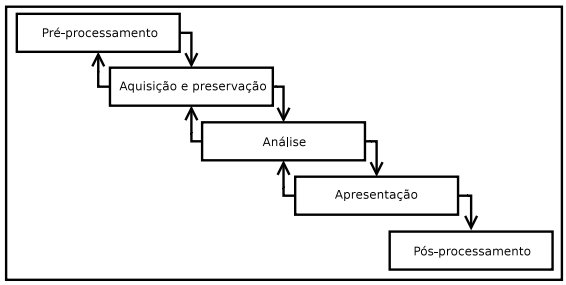


Figura 7 – *Generic Computer Forensic Investigation Model* (YUSOFF; ISMAIL; HASSAN, 2011)

4.7.7 Integrated Digital Forensic Process Model (2012)

O *Integrated Digital Forensic Process Model* ou simplesmente IDFPM consiste dos seguintes processos: *preparation*, *incident*, *incident response*, *physical investigation*, *digital forensic investigation* e *presentation*.

A documentação da investigação que acompanha todo o processo e a cadeia de custódia registram de forma precisa toda a investigação. O diagrama representativo do modelo pode ser observado na Figura 8.

O trabalho *Review of Digital Forensic Investigation Frameworks* (AGARWAL; KOTHARI, 2015) afirma que este modelo não pode ser aplicado em todos os casos e faz apenas consideração de alguns modelos forenses. Enumera que os modelos atuais apresentam complicações tais como processos ou etapas escritas com nomes similares, ou explicações de cada fase alteradas.

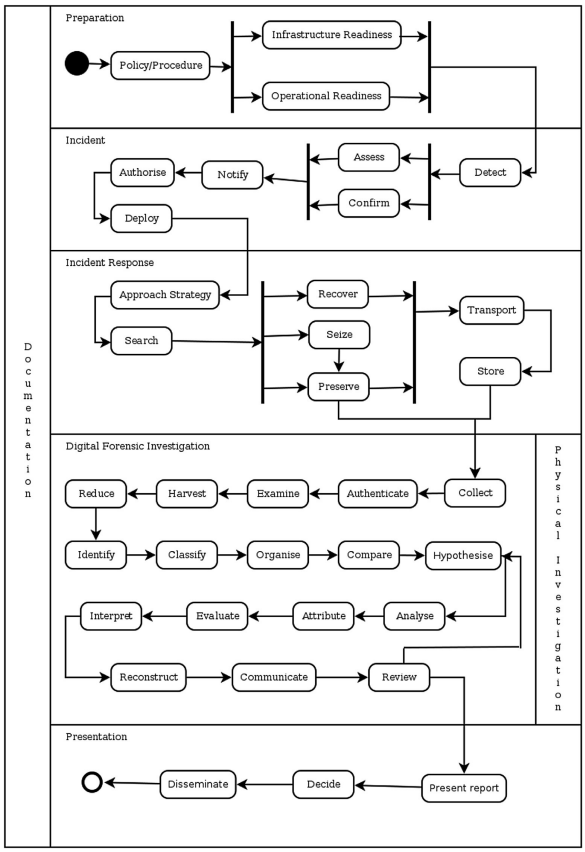


Figura 8 – *Integrated Digital Forensic Process Model* (KOHN; ELOFF; ELOFF, 2013)

4.7.8 ISO 27043 (2014)

O padrão ISO/IEC 27037 fornece diretrizes para atividades específicas de manuseio de evidências digitais, a Figura 9 mostra como está dispoto o modelo que inclui a identificação, colheita, aquisição e preservação de possíveis evidências digitais que possam ser de valor probatório. Essas etapas são necessárias em um processo de investigação que é projetado para manter a integridade da evidência digital - uma metodologia aceitável na obtenção de provas digitais garantirá sua admissibilidade no cumprimento de seus propósitos.

Identification - inclui procurar, detectar e documentar a evidência digital (lógica e física);

Collection - depois de identificar o dispositivo, removê-lo do seu local original e transferi-lo para o laboratório, onde será Analisado e Processado. O processo de colheita deve ser todo documentado;

Acquisition - processamento inicial consiste em fazer uma cópia da evidência (ex.: todo o HDD) e documentar os métodos usados;

Preservation - processo para manter e salvaguardar a integridade e / ou condição original da evidência digital potencial.

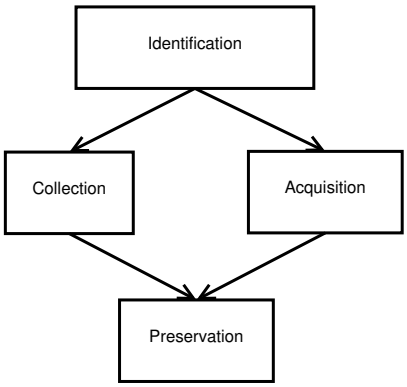


Figura 9 – ISO 27037 *procedure for Evidence Handling* (ISO, 2012)

4.7.9 Deconstruct and Preserve (DaP) (2017)

O método proposto no documento (MITCHELL et al., 2017) apresenta as etapas dispostas em uma tabela que serviu de base para a construção da Figura 10. O experimento é realizado em SSD e fornece um procedimento para preservar a evidência, as melhores práticas de procedimentos em forense priorizam que a evidência deve ser preservada, ou se houver alguma alteração é necessária uma robusta documentação e a possibilidade de que o procedimento seja repetível.

O método DaP é uma proposta que se destina à preservação da evidência em SSD e assegura que as cópias forenses geradas a partir do SSD mantenham a "mesmidade".

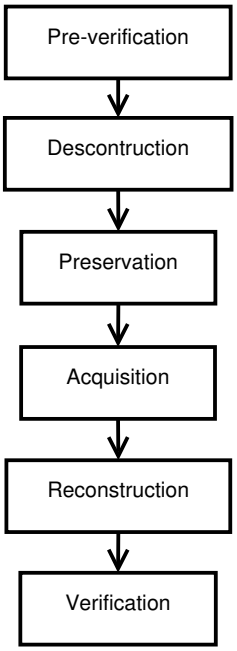


Figura 10 – Estapas para o DaP

4.7.10 Modelo Proposto

Um modelo de investigação forense é importante porque fornece uma estrutura de referência para a execução de um trabalho forense computacional, independente de qualquer tecnologia ou ambiente organizacional específico, é útil para a discussão de técnicas e tecnologias para apoiar o trabalho dos pesquisadores. Pode fornecer uma terminologia comum para apoiar a discussão e o compartilhamento de conhecimentos. O modelo pode ser usado para ajudar a desenvolver e aplicar metodologias às novas tecnologias à medida que elas surgem e se tornam objeto de investigações.

O modelo proposto foi concebido após a análise dos modelos anteriormente mencionados, ele acrescenta etapas que são necessárias para que se possa, diante de um tribunal, demonstrar que a legislação foi sempre cumprida durante o transcorrer do trabalho forense, desde a autorização da busca e apreensão até a apresentação diante de um tribunal, fazendo uso ao longo das etapas de uma cadeia de custódia bem documentada.

O estudo desses diversos modelos de investigação forense anteriormente mencionados, bem como da legislação, doutrina e jurisprudências brasileiras serviram de alicerce para a propositura deste modelo, ilustrado na Figura 11.

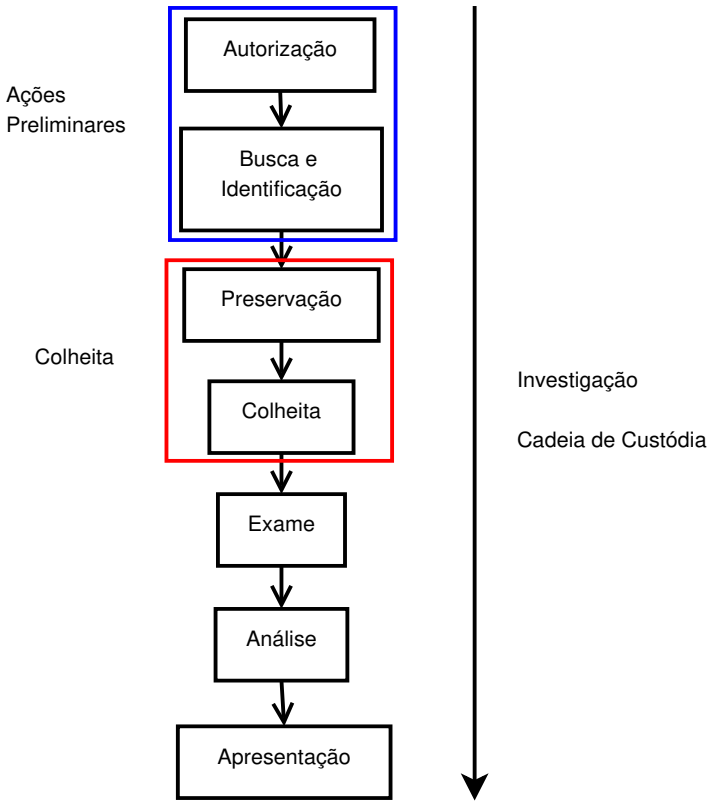


Figura 11 – Modelo de Investigação de Forense Computacional

A Figura 11 explicita as etapas do modelo proposto, que é descrito abaixo e serve para guiar o procedimento operacional padrão também proposto neste trabalho e descrito integralmente no Apêndice A.

O modelo deve seguir, em regra, uma sequência lógica de etapas, mas nada impede que se for detectado que há necessidade de retornar a uma etapa anterior, esse retorno ocorra de forma excepcional.

Autorização - Após a necessidade de uma investigação ser realizada, alguns ritos devem ser seguidos para que a prova eventualmente obtida seja considerada legal e, por conseguinte, admitida em um processo (ver Seção 3). Para que a busca por evidências seja realizada é necessário obter autorização para realizá-la, isso pode ser muito complexo e exigir interação com entidades externas e internas para obter a autorização necessária. O nível de estrutura formal associado à autorização varia consideravelmente, dependendo do tipo de investigação. Dentro de uma empresa privada, um administrador de uma infraestrutura de tecnologia poderia exigir apenas uma aprovação verbal simples da administração da empresa para realizar uma investigação detalhada dos sistemas de computador da empresa; no outro extremo, os órgãos responsáveis pela aplicação da lei geralmente precisam uma autorização legal formal, estabelecendo com detalhes precisos o que é permitido em uma investigação (exemplo: mandado judicial de busca e apreensão ver subseção 3.3.3). Há a possibilidade de o perito prescindir de autorização, por se tratar por exemplo de flagrante delito. Nesta fase, deve-se obter a autorização e consignar os dados da autorização dentre os dados do processo que devem ser escritos no documento da cadeia de custódia.

Busca e Identificação - Essa atividade lida com a localização das evidências e a identificação da mesma. No caso mais simples, isso pode envolver encontrar o computador usado por um suspeito e confirmar que é o de interesse dos investigadores. No entanto, em ambientes mais complexos, essa atividade pode não ser tão simples, muitas vezes o documento de autorização já discrimina muito especificamente o que é alvo da busca e que deve ser identificado para que sirva como fonte de prova. Mas há casos que podem exigir o rastreamento de computadores por meio de várias redes e, possivelmente, em outros países. Conforme tratado na subseção 3.3.3, muitas das vezes não há clareza do que poderá ser fonte de prova, cabendo a peritos e encarregados de aplicação da lei a observação de materiais no local do crime que possam servir de fonte de prova. A identificação, que está associada a busca, consiste também em rotular (sempre que possível) os documentos, equipamentos para que seja formado um vínculo entre estes e uma determinada investigação. Devem-ser apostos minimamente no rótulo, etiqueta ou saco lacrado dados básicos da investigação, data, hora e o indivíduo que localizou e identificou para que essas informações sejam juntadas a cadeia de custódia.

Preservação - é uma etapa que apresenta desdobramentos em todas as etapas, trata do gerenciamento dos dados, gestão e geração de cópias forenses, cadeia de custódia e

sincronização de eventos. A preservação é uma etapa da mais alta relevância, nesta etapa o objetivo principal é garantir integridade e/ou condição original da evidência.

Colheita - a atividade na qual a organização investigadora toma posse da evidência em uma forma que pode ser preservada e analisada, por ex. imagens de discos rígidos ou apreensão de computadores inteiros. Esta etapa apresenta muitas discussões na literatura por causa de sua importância para o restante da investigação. Erros ou más práticas nesta fase podem tornar a evidência inútil, particularmente em investigações que estão sujeitas a requisitos legais estritos.

Exame - envolverá o uso de um número potencialmente grande de técnicas para encontrar e interpretar dados significativos. Pode exigir a reconstrução/religação de dados fragmentados, o reparo de dados danificados, tudo de forma a preservar a mesmidade. Dependendo dos resultados das atividades prévias de busca/identificação, preservação e colheita, pode haver volumes muito grandes de dados a serem examinados, portanto, são necessárias técnicas automatizadas para auxiliar o trabalho forense computacional.

Análise - baseia-se no exame das evidências, os peritos devem construir uma documentação (prova pericial), cujo nível de detalhamento dependerá do tipo de investigação, da clareza e robustez do que foi encontrado. Pode eventualmente ocorrer retorno a passos anteriores, principalmente à etapa de exame, para que dúvidas na análise possam ser melhor esclarecidas.

Apresentação - a análise deverá ser preparada e apresentada a pessoas que não possuam um conhecimento técnico científico aprofundado. A prova pericial será colocada diante de um juiz, de um júri. Caso se trate de uma investigação interna de uma organização será apresentada aos tomadores de decisão daquela empresa.

Cabe ressaltar, que a cadeia de custódia não consta como uma etapa isolada, ela não só faz parte da etapa "Preservação", mas também se comunica com todas as outras etapas da investigação, inicia-se nas "Ações Preliminares" ("Autorização" e "Busca e Identificação") e vai até a "Apresentação", como está ilustrado na Figura 11. Na Seção 4.8 a cadeia de custódia é vista com maiores detalhes.

4.8 CADEIA DE CUSTÓDIA

Segundo Köhn (KOHN; ELOFF; ELOFF, 2013), o número de modelos forenses digitais existentes aumentou a complexidade do campo. Há necessidade de uma padronização para facilitar o processo de investigação. Porém, uma observação mais apurada observa que há muita similaridade entre os processos e, por vezes a diferença é em relação a nomenclatura, verifica-se também que há muitas etapas comuns aos modelos.

Em comum a todos os modelos está a ideia de realizar controle sobre a evidência, documentando quem teve acesso a ela, o que foi feito com ela durante o período. A evidência deve ser protegida fisicamente, de tal forma que ela sofra menos adulteração e diminua sensivelmente a manipulação indevida. Outra preocupação presente nos modelos diz respeito ao estabelecimento e a manutenção de uma apropriada Cadeia de Custódia.

A cadeia de custódia é um conjunto de procedimentos técnicos e científicos os quais irão oferecer conhecimento aos operadores do Direito, permitindo-se avaliar se aquela prova que está no tribunal, e que representa a materialidade de um ato criminoso, foi tratada com o devido rigor técnico-científico legal desde sua origem de colheita no local da infração penal - podendo a falha na Cadeia de Custódia gerar prejuízos econômicos indevidos, inocentar prováveis culpados ou condenar inocentes. Tal fidedignidade na Cadeia de Custódia visa demonstrar a verdadeira autoria e materialidade do fato criminoso de forma imparcial e inequívoca.

A cadeia de custódia não se constitui apenas em uma anotação da cronologia da posse do material probatório, ela vai além, volta-se à integridade da prova, à preservação da fiabilidade do armazenamento, da manipulação e do rastreamento da movimentação da prova no decorrer do tempo.

Segundo Dias Filho [Dias Filho 2009], a cadeia de custódia está prevista no ordenamento jurídico de outros países, porém não está presente na legislação brasileira de forma precisa, tampouco normatizada.

O projeto de lei 8.045/2010 que tramita na Câmara dos Deputados e que (se aprovado) substituirá o CPP vigente, inova ao disciplinar a cadeia de custódia (art. 192 ao 194 do PL 8.045/2010).

Apesar de não aparecer atualmente como um procedimento normatizado em lei, isso não quer dizer que evidências colhidas prescindam de preservação e de uma cadeia de custódia. Ademais, a Secretaria Nacional de Segurança Pública (SENASP) publicou documentos que ratificam esse entendimento; primeiramente em 2012, através do documento intitulado Diagnóstico da Perícia Criminal (SENASP, 2012), em seguida em 2013 e 2014 por meio dos documentos Procedimento Operacional Padrao: Perícia Criminal (SENASP, 2013) bem como da portaria 82 (SENASP, 2014), a qual estabeleceu diretrizes sobre os procedimentos a serem observados no tocante a cadeia de custódia de vestígios.

Sabe-se que é constitucionalmente assegurado o acesso a arquivos digitais, interceptações telefônicas e telemáticas para a defesa, bem como para acusação, mesmo com esse acesso (que é garantido pela ampla defesa e pelo contraditório) há a obrigação da manutenção da mesmidade. Apesar de não prevista no atual Código de Processo Penal, a cadeia de custódia ao ser violada pode tornar a prova ilícita e demandar o desentranhamento da prova no processo, conforme considera a Relatora Ministra Assussete Magalhães no HC nº 160662/RJ 6ª Turma, j. 18/02/2014. Para Eberhardt (EBERHARDT, 2014), a eventual quebra da cadeia de custódia importa, portanto, na ilicitude da prova a que se

refere aquele conjunto de atos. Disso decorre que o magistrado deverá considerá-las como provas ilícitas, bem como todas aquelas que tenham sido por meio delas obtidas (provas derivadas da ilícita).

Cabe ressaltar que ainda não há um entendimento pacífico, nem jurisprudência consolidada, há casos em que se reconhece a quebra da cadeia de custódia, mas não se considera a ilicitude da prova, como no caso da Operação Ouro Verde da Polícia Federal.

Na pesquisa de Maria Alice dos Santos Severo (SEVERO, 2018), há a afirmação de que diante da manifesta quebra da cadeia de custódia da prova na Operação Ouro Verde[10], consignada nos autos do processo, tal elemento probatório torna-se inconfiável, não devendo possuir nenhum valor probatório para o processo. Nesta operação, os dados informáticos foram acessados pela Autoridade Policial sem a cautela de preservação da integridade da prova e sem qualquer mecanismo de comprovação desta preservação, tornando possível a alteração do conteúdo, pois nada assegura que os dados apresentados representam o conteúdo real no instante da apreensão. A defesa alegou a imprestabilidade da prova por violação de sua fidedignidade; argumentou a não ocorrência do crime de evasão de divisas. A sentença não acolheu o pedido de exclusão da prova, mesmo reconhecendo a existência de falhas no manuseio e conservação da mídia em questão. Em grau recursal, mais uma vez reconheceu-se ter havido acesso direto à mídia antes da realização da cópia forense. Porém, dado o curto espaço de tempo para que ocorressem modificações substanciais na prova, não se considerou possível haver alteração substancial da prova por parte da Autoridade Policial.

Por fim, para permitir assegurar a mesmidade da prova, uma cadeia de custódia bem conduzida deverá, segundo a RFC3227 (BREZINSKI; KILLALEA, 2002), descrever claramente como a evidência foi encontrada, como ela foi tratada e tudo o que aconteceu com ela. Para isso deve ser documentado:

- Onde, quando e por quem a evidência foi descoberta e colhida;
- Onde, quando e por quem as evidências foram tratadas ou examinadas;
- Quem teve a custódia da evidência, durante o período;
- Como foi armazenada;
- Quando a evidência mudou de custódia, quando e como ocorreu a transferência.

[10] Segundo (SEVERO, 2018) dados no HDD de um computador foram abertos e manuseados, após a apreensão pela própria polícia, sem que se fizesse registro de tal abertura e manipulação, o que contamina de tal forma a prova que só poderia ser considerada imprestável para cumprir o papel de traduzir a verdade.

5 *SOLID STATE DRIVE*

O sistema de memória de um dispositivo computacional pode empregar diferentes tipos de memórias para que haja um equilíbrio entre custo, velocidade e capacidade de armazenamento. Discos magnéticos (HDDs) e drives de estado sólido (SSDs) são dispositivos de armazenamento secundário, eles têm como característica a preservação das informações ali armazenadas, mesmo na ausência de uma fonte de alimentação externa.

A terminologia "estado sólido" refere-se ao fato de que dados são armazenados em arranjos fixos de transistores eletrônicos, os quais permitem que a leitura e escrita sejam executadas de forma bem mais rápida nos drives de estado sólido.

Uma comparação realizada pela Intel, apresentada na Tabela 2, mostra vantagens do SSD sobre seu concorrente direto, o HDD (INTEL, 2010).

Tabela 2 – Comparação entre SSD e HDD(INTEL, 2010)

	SSD	HDD	Vantagem do SSD
Tempo de inicialização de um SO	$\sim$ 19 s	$\sim$ 30 s	$\sim$37% menor
Resistência a impacto e vibração	1.500 G[1]	900 G	$\sim$ 60% mais imune
Consumo de energia (por semana)	$\sim$ 35 Wh	$\sim$ 55 Wh	mais de 20% menor
Confiabilidade (MTBF)	$\sim$ 1,2 x 10^6 h	$\sim$ 0,6 x 10^6 h	$\sim$ 100% mais confiável
Ruído de operação	0 dB	25 dB	nenhum ruído

O SSD é um dispositivo mais complexo, é um sistema que pode internamente gerenciar troca de dados, funções de criptografia e compactação, além de outros mecanismos específicos por meio de um processador interno ao drive. Para entender o funcionamento interno, divide-se didaticamente o SSD em dois componentes fundamentais: as células de memória flash e o controlador de memória.

5.1 COMPONENTES PRINCIPAIS DE UM SSD

5.1.1 Controlador de Memória

O controlador de memória é o principal responsável pelo desempenho e confiabilidade do SSD, na arquitetura de alto nível do controlador de memória apresentado na Figura 12, podem-se distinguir três diferentes partes:

- interface do *HOST* - situa-se entre o *host* (computador) e o SSD, os protocolos precisam ser compatíveis com padrões da indústria usados para HDDs, são exemplos desses padrões: SATA, SAS e PCIe;

- *firmware* também conhecido como *flash file system* - algoritmos internos de leitura, escrita, modificação, apagamento e outras funções inerentes a processos internos como *wear leveling*, gerenciamento de *bad block*, *garbage collection*, TRIM;
- código corretor de erro (ECC) - identifica e corrige erros de bits.

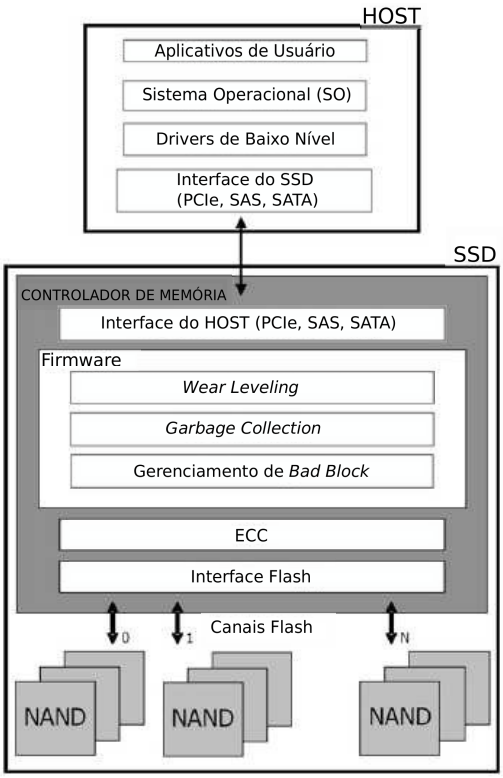


Figura 12 – Visão da arquitetura de alto nível do controlador de memória flash (MICHELONI; ESHGHI, 2013)

Diferentemente de outros produtos de armazenamento, para SSDs não há padrões específicos da indústria de como deve-se armazenar ou apagar os dados. Após a interface que existe entre o computador e o drive de estado sólido, cada fabricante constrói livremente a estrutura e algoritmos internos com o intuito de atingir a máxima performance, logo há uma grande variação entre diferentes marcas e modelos.

5.1.2 Células de Memória

Memória flash NAND é um tipo de memória não volátil (*Non-Volatile Memories* - NVM), ou seja, o conteúdo armazenado é preservado após a retirada da fonte de alimentação, além disso, o conteúdo pode ser eletricamente alterado. Solid State Drive (SSD) é uma das últimas aplicações de memórias flash (MICHELONI; ESHGHI, 2013).

Célula flash NAND recebe essa denominação devido à operação lógica "Not AND" empregada em sua construção. A célula é baseada na tecnologia de *Floating Gate* (FG).

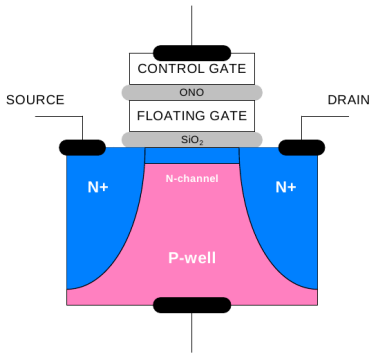


Figura 13 – Uma representação em corte transversal de uma célula de memória floating gate MOSFET (OLSON; LANGLOIS, 2008)

Pode-se observar a representação de um *floating gate MOSFET* na Figura 13. Um transistor do tipo MOSFET é construído com dois *gates* sobrepostos em lugar de apenas um: o primeiro é completamente envolvido por óxido, enquanto o segundo é utilizado para formar o terminal. As operações realizadas para injetar e remover elétrons no *gate* isolado são chamadas de programação e apagamento (do inglês, *program and erase* - P/E), respectivamente. Essas operações modificam a voltagem V_{TH} deste tipo especial de transistor do tipo MOS (*floating gate MOSFET*)(MICHELONI; ESHGHI, 2013).

Brown e Brewer (BROWN; BREWER, 1998) afirmam que os processos de programação e apagamento são destrutivos para a fina camada de isolamento dielétrico feita de SiO_2 (*silicon dioxide glass*) que existe entre o *floating gate* e o canal de um transistor. Os processos destrutivos utilizados nesses processos causam degradação do dispositivo e limitam a vida útil da memória flash de forma proporcional ao número de ciclos de Programação/Apagamento (*Program/Erase* - P/E) (PERDUE, 2008).

Células de memória flash são organizadas em uma hierarquia em que a menor unidade é a própria célula, o agrupamento de células são páginas, o agrupamento de páginas são blocos e o conjunto de blocos constitui a memória flash NAND.

As páginas, formadas por um conjunto de células, representam a menor unidade de escrita e leitura, há tamanhos de páginas de 2KB, 4KB, 8KB ou 16KB. Os blocos, por sua vez, são conjuntes de 128 ou 256 páginas, possuem tamanho de 256KB a 4MB, representam a menor unidade de apagamento.

A expectativa do tempo de utilização de um SSD está ligada diretamente à maneira através da qual as células de memória flash são usadas, mais especificamente em relação ao número de ciclos de escrita a que são submetidos cada bloco. Blocos individuais dentro do SSD só podem ser escritos cerca de 10000-100000 vezes antes que eles corram sério risco de falhar (OLSON; LANGLOIS, 2008).

5.2 MECANISMOS INTERNOS DO SSD

5.2.1 *Wear Leveling*

Devido às operações de apagamento, um bloco de memória flash suporta apenas um número limitado de ciclos P/E (*worn-out property*) (YANG et al., 2014) antes de se deteriorar e causar destruição ou comprometimento dos dados.

O *wear leveling* é um mecanismo cuja proposta é distribuir os apagamentos sucessivos entre os blocos do drive. Ele procura nivelar o desgaste dos blocos evitando que apagamentos sucessivos sejam realizados em um mesmo subconjunto de blocos e com isso atinge o objetivo para o qual foi criado: aumentar a vida útil de um SSD. Esse aperfeiçoamento impede que parte do chip seja inutilizado rapidamente por meio dessas repetidas tentativas de apagamento em um mesmo local. O *wear leveling* age de forma a assegurar que cada um dos blocos do dispositivo seja escrito uma vez, e só volte a ser escrito depois que todos os outros blocos já tenham sido escritos (KING; VIDAS, 2011). Atualmente os firmwares e controladores escrevem dados através de células de forma mais uniforme em razão do processo de *wear leveling*. O *wear leveling* é completamente transparente para o sistema hospedeiro e feito de forma diferente por cada fabricante, ele gera um aumento da vida útil dos SSDs (ANTONELLIS, 2008).

É importante destacar que em um processo de modificação de um setor S, em vez de o conteúdo alterado do setor S ser escrito no mesmo local em que as informações estavam, acontece de aquelas informações serem salvas em outro local (um setor T) e ser realizada uma atualização no mapeamento, então as informações do antigo setor S - agora modificadas -, encontram-se no setor T e aparecem no endereço lógico de bloco (LBA). Com isso a antiga versão das informações do S permanecem na memória flash e são chamados de dados remanescentes(WEI et al., 2011). Esse comportamento é gerado pelo procedimento natural do *wear leveling* que, por um lado, estende a vida útil dos SSDs e, por outro, pode deixar dados remanescentes não acessíveis através da FTL, mas que ainda permite um trabalho de recuperação eficaz - porém muito difícil de ser realizado - desses dados remanescentes.

O *wear leveling* pode levar a um uso extensivo da capacidade de armazenamento do drive, que pode levar a um segundo problema: uma significativa diminuição da velocidade de transferência. Isso ocorre por causa da caraterística “apague-antes-escreva-depois”, a qual difere da característica “escreva-sobre-dados-antigos” de fitas e discos magnéticos. O processo de apagamento é muito lento comparado aos processos de leitura e escrita, levando até 10 ms. Em SSD, mudança de um só byte pode resultar na necessidade de ler/apagar e escrever, por isso quando a unidade está cheia, o desempenho é sensivelmente afetado pelo *wear leveling*. Muitos fabricantes, para enfrentar a perda de desempenho ao ter que apagar antes de usar novamente um bloco, adotaram a estratégia conhecida como *Garbage Collection* ou *Self-Healing* (auto-cura)(BELL; BODDINGTON, 2010).

5.2.2 *Garbage Collection*

Utiliza-se a *garbage collection* para apagar o espaço de memória flash que possua dados desatualizados, de modo a liberar mais espaço livre para escritas posteriores.

Páginas com dados desatualizados, as páginas inválidas ou *dead pages*, poderão ser recuperadas e reusadas através da *garbage collection*. Para recuperar essas páginas inválidas da flash são selecionados um ou mais blocos ("blocos vítimas"), que contenham alguma página inválida, os dados atualizados (páginas válidas ou *live pages*) do "bloco vítima" são copiados para outro(s) bloco(s), em seguida apaga-se o "bloco vítima" com o intuito de transformar as páginas inválidas do "bloco vítima" em páginas livres para as escritas subsequentes. Com a finalidade de preservar as páginas do usuário que são válidas e estão no "bloco vítima", as páginas válidas devem ser copiadas para outro(s) bloco(s) antes que o "bloco vítima" seja apagado. Como resultado deste cuidadoso processo para que dados válidos não sejam perdidos, a *garbage collection* pode consumir muito tempo e ser um limitador de desempenho da memória flash, em decorrência do grande número de páginas válidas que podem ser copiadas durante esse processo. A criação de algoritmos que permitam maior eficiência à *garbage collection* tem sido uma área destacada de pesquisa (YANG et al., 2014).

A utilização da *garbage collection* deve se preocupar com eficiência e também com a longevidade da memória. O mecanismo é uma maneira de minimizar a perda de desempenho pois se antecipa à característica "apague-antes-escreva-depois", já que apaga os dados das células de memória antes que elas possam receber novas informações.

O processo acontece de forma automática, ou seja, sem que haja a necessidade de interferência do usuário. É uma operação que acontece de forma transparente para o usuário, uma vez que dados que foram previamente marcados como dados desatualizados são apagados por blocos e o espaço apagado volta a ser uma opção de espaço para escrita. No tocante à longevidade, é importante reduzir tanto quanto possível o número de apagamentos/escritas e também tornar o mais uniforme possível o número de apagamentos que cada bloco sofre.

Em (BELL; BODDINGTON, 2010) é mencionado um problema que influencia a execução do mecanismo, o problema diz respeito à comunicação entre sistema operacional (SO) e drive. O SO normalmente não comunica ao disco quando um arquivo foi apagado, com isso o SSD (mais especificamente a camada FTL) não dispara o mecanismo de *garbage collection*; a fim de solucionar o problema criou-se uma nova instrução, a instrução TRIM.

5.2.3 TRIM

Os *Hard Disk Drives* (HDDs) podem realizar atualizações em locais físicos marcados como disponíveis ainda que haja dados escritos lá. Nos HDDs os dados costumam permanecer intocados até que aquele espaço de armazenamento seja alocado para outro arquivo. Devido

ao fato de o SSD possuir características diferentes (o SSD tem a caraterística "apague-antes-escreva-depois" enquanto o HDD tem característica "escreva-sobre-dados-antigos"), manter o arquivo em um local de armazenamento impede que a escrita seja realizada e cria a necessidade de se esperar até que o apagamento da área de armazenamento seja feita para que só então a escrita ocorra.

O comando TRIM foi publicado no padrão Serial ATA em 2007, esse comando permite que o sistema operacional informe ao SSD que determinados dados não são mais válidos e podem ser apagados. O *garbage collection* não precisa preservar dados inválidos, o que evita a necessidade de movimentar e armazenar esses dados, mitigando um problema conhecido como *write amplification*[2].

Cabe ressaltar que o controlador do disco também decide quando iniciar e desempenhar a operação de *garbage collection*, o comando TRIM sinaliza ao SSD que há blocos de dados que não estão em uso e podem ser preparados para uma nova escrita. TRIM é uma solução adicional implementada em diversos sistemas operacionais modernos como NTFS no Windows 7 e posteriores, Ext4 usado na versão Linux Kernel 2.6.33 e posteriores, HFS+ usado no Mac OS X 10.6.8 ou posterior (NISBET; LAWRENCE; RUFF, 2013).

Quando o sistema operacional possui a instrução TRIM implementada, após um arquivo ser apagado o SO envia essa instrução para o controlador do SSD indicando os endereços lógicos dos blocos que correspondem aos blocos que eram utilizados pelo arquivo recentemente apagado. De modo que os endereços lógicos dos blocos são mapeados para os endereços físicos dos blocos pela FTL, para que seja realizada a limpeza (GEBRE-MARYAM, 2011).

Por isso, os problemas de degradação de desempenho e de falta de comunicação entre sistema operacional e disco impulsionaram a busca por soluções para o aperfeiçoamento dos SSDs, a instrução TRIM foi um desses aperfeiçoamentos. A multiplicidade de algoritmos não padronizados que operam internamente tornam o SSD um dispositivo bem mais complexo e muito diferente do HDD. Essas diferenças afetam profundamente o trabalho de peritos que buscam a recuperação de arquivos apagados em SSDs.

A especificação do comando TRIM é parte do padrão ATA publicado pelo *Technical Committe* T13 da INCITS, só é possível o envio de comandos TRIM por meio de interfaces Serial ATA (SATA) ou Parallel ATA (IDE, PATA). TRIM é implementado no *DATA SET MANAGEMENT* e possui a finalidade de fornecer informação ao dispositivo de armazenamento para que ele possa atingir maior desempenho e aumente a integridade de dados.

TRIM permite especificar para o dispositivo de armazenamento quais *Logical Block Addresses* não estão sendo usados pelo sistema de arquivos.

O padrão (STEVENS, 2018) define diferentes tipos de TRIM:

[2] Write amplification - é uma situação indesejada em que a quantidade real de informações gravadas fisicamente na mídia de armazenamento é um múltiplo da quantia lógica a ser gravada.

Non-deterministic TRIM - cada comando de leitura enviado para o *Logical Block Address* (LBA), depois de um TRIM, pode retornar dados diferentes;

Deterministic Read After TRIM (DRAT) - todos os comandos de leitura para o LBA, após um TRIM, devem retornar os mesmos dados, ou tornarem-se determinados;

Read Zeroes After TRIM (RZAT) - todos os comandos de leitura para o LBA depois de um TRIM devem retornar zero.

No documento mais atual (STEVENS, 2018) o bit TRIM é encontrado no comando de 48 bits para dispositivos ATA, neste documento há o detalhamento de como o hardware do SSD deverá funcionar com relação aos comandos passados pelo sistema operacional. A Tabela 3 retirada do padrão ATA (STEVENS, 2018) resume os dados que são retornados por setores lógicos após o comando TRIM ser disparado.

Apesar de haver a padronização de três comandos TRIM distintos, não é possível assegurar que os fabricantes implementem corretamente a funcionalidade desses três comandos TRIM em seus dispositivos de armazenamento. Talvez a diferença de implementação possa explicar a divergência de resultados na recuperação de dados das unidades de armazenamento SSD.

Tabela 3 – Dados que são retornados por setores lógicos após diferentes tipos de comando TRIM (STEVENS, 2018)

Bit			Dados retornados por um setor lógico submetido ao TRIM após receber um comando de leitura
Suporte a TRIM	Suporte a DRAT	Suporte a RZAT	
0	-	-	Não aplicável
1	0	-	Dados diferentes podem ser retornados a cada comando de leitura.
	1	0	Os mesmos dados retornados na primeira leitura do setor lógico processado, depois daquele setor lógico ser submetido ao TRIM.
	1	1	Os dados retornados são zeros.

6 EXPERIMENTOS PRÁTICOS

6.1 EXPERIMENTOS

Com a compreensão do funcionamento interno do SSD, a partir do que foi visto na Seção 5, serão detalhados experimentos realizados no decorrer do desenvolvimento deste trabalho.

O SSD emprega uma arquitetura que não apresenta uniformidade entre os diferentes fabricantes, no entanto há um modelo em camadas retirado do artigo de Joshi e Hubbard (JOSHI BINAYA RAJ E HUBBARD, 2016) que permite entender com detalhes o funcionamento interno de modernos dispositivos SSD e que complementa a Figura 12 apresentada na Seção 5. O modelo em camadas aparece na Figura 14, em que aparece também a interface de comunicação entre o SSD e o *host computer*.

A *Flash Translation Layer* (FTL) vai realizar as principais tarefas de dados (leitura, gravação), é uma verdadeira interface que se posiciona entre os canais de comunicação dos barramentos (ATA, PCIe, USB) de um lado, com os chips de memória do outro lado, bem como poderá compactar, criptografar ou mover blocos de dados para executar otimizações. Em SSD, o sistema operacional não possui acesso direto aos dados contidos nos chips de memória flash NAND, não acesso direto à localização física. A FTL de SSDs executa funções complexas de tradução de endereços de bloco lógicos (*Logical Block Address* - LBA), em decorrência de solicitações do SO, para os respectivos endereços de bloco físico (*Physical Block Address* - PBA) em chips de memória.

Todos os experimentos realizados recebem as informações repassadas pelo SSD através da camada FTL. Não há acesso direto aos endereços físicos (PBA) das memórias flash NAND, o acesso é feito por meio dos endereços lógicos (LBA) que são traduzidos pela camada FTL. Em outras palavras, os experimentos utilizam a abordagem conhecida como caixa-preta, nesta abordagem as informações apresentadas pela camada FTL são colhidas. A abordagem caixa-preta para forense em unidades de estado sólido foi estudada por Bonetti e outros (BONETTI et al., 2013), nesse trabalho a abordagem caixa-preta foi considerada mais prática, conveniente, menos intrusiva e mais barata que a abordagem caixa-branca[1].

Nos experimentos práticos conduzidos nesta seção, assume-se que já há uma autorização legal para a busca domiciliar e apreensão de elementos de prova ou que está autorização é desnecessária, conforme discutido na Subseção 3.3.3. No que diz respeito as etapas de "Busca e Identificação" e "Preservação", todas as unidades foram identificadas,

[1] Caixa-branca - a abordagem caixa-branca em SSD, avalia a possibilidade de obter dados diretamente do chip de memória flash. Apesar de teoricamente possível, é muito difícil acessar diretamente o chip, consome muito tempo, é uma alternativa cara, requer hardware específico e, ainda que se consiga colher dados sem destruir o chip, será necessário reconstruir os dados que foram distribuídos ao longo dos chips em endereços físicos (PBA) pela FTL. Segundo (BONETTI et al., 2013), o sucesso na aplicação das técnicas de caixa-branca dependeriam ainda assim de cada SSD.

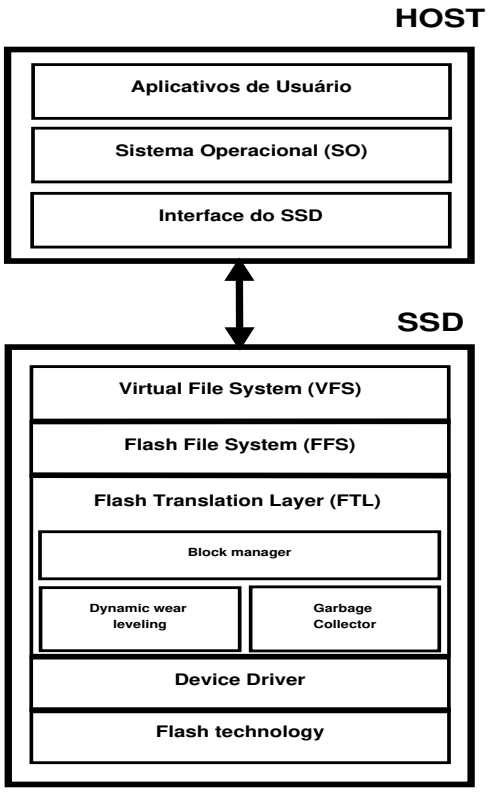


Figura 14 – Arquitetura em camadas de um dispositivo SSD e sua comunicação com um *host*

as imagens geradas a partir das unidades receberam nomes que permitem referenciar a qual unidade àquela imagem se refere, por exemplo **SSD120G_dc3ddPOS60.dd** exibido na linha de comando da Subseção D.2 do Apêndice D, pelo própio nome do arquivo conforme foi convencionado, é possível reconhecer que é uma imagem da unidade SSD de 120GB da SanDisk, a etapa da "Preservação" também está - em parte - expressa na linha de comando, por meio da geração do arquivo de *hash* do tipo SHA [2] de 256 bits **SSD120Gsha256POS60.log**.

As etapas de "Colheita" e "Exame" estão contempladas nos experimentos, aquela diz respeito a imagem de disco (é o momento em que se toma posse da evidência e se pode partir para etapa de "Exame") e esta última diz respeito a etapa de encontrar, recuperar e interpretar os dados.

A etapa de "Análise" e "Apresentação" não foram demonstradas nos experimentos e estão descritas na Subseção 4.7.10.

No restante desta seção são apresentados três experimentos distintos, o Experimento 1 trata de uma recuperação pericial comum, em que não há muitos detalhes sobre o conteúdo da unidade SSD; o Experimento 2 foi usado para observar as modificações das unidades SSD que podem ser atribuídas aos mecanismos internos, são avaliados aspectos

[2] SHA (*Secure Hash Algorithm*) - faz parte de um conjunto de funções de hash projetadas pela NSA (*National Security Agency* dos EUA) e que são adotadas mundialmente como mecanismo de verificação de integridade.

de duração das alterações com base nos resultados dos *hashes* obtidos; o Experimento 3, último experimento apresentado foi dividido em três partes que se assemelham no aspecto de buscar a recuperação de dados, mas diferem nos procedimentos e nos arquivos envolvidos na recuperação.

6.1.1 Experimento 1 - Recuperação Pericial Comum

Esse experimento consiste de um SSD que já foi usado por um tempo e foi formatado. Faz-se mister ressaltar que não é relevante nesta pesquisa o sistema operacional nem o sistema de arquivos no qual os dados estavam armazenados antes do processo de formatação, pois o foco está na recuperação de arquivos. Trabalhos futuros poderão especificar melhor o ambiente no que diz respeito ao SO e ao sistema de arquivos, além de avaliar como eles influenciam no processo de recuperação.

Foi utilizado um SSD da marca ADATA, modelo Premier SP800 - 32GB. Esse SSD possui: suporte ao comando TRIM, controlador de memória Sand Force SF-1222, interface SATA 3Gb/s.

Antes dos experimentos, o SSD era usado por um usuário doméstico típico, cujas aplicações incluem: reprodutor de áudio e vídeo, navegador web, e-mail e pacote de escritório.

Sabe-se que em um processo judicial os dados recuperados podem ser usados como prova para demonstrar a verdade. A admissibilidade de arquivos recuperados depende das qualidades percebidas pelo juiz ou pelos jurados. Giuliano Giova (GIOVA, 2011) considera que a prova digital não pode ser admitida sem uma cadeia de custódia, porque geralmente essa prova fica longe da percepção sensorial. Nesta pesquisa deseja-se saber se remanescência de dados é um problema em SSD, porém não é relevante neste momento saber a finalidade que será dada aos dados, é relevante saber se é possível encontrar dados e recuperá-los.

6.1.1.1 Geração da Imagem

Geração de Imagem[3] de uma unidade é o processo de copiar o arquivo da mídia original para outro local, separado e seguro. A imagem gerada é uma cópia que deverá manter a integridade e mesmidade, de tal forma que essa cópia possa ser usada como se original fosse, por exemplo durante o trabalho forense.

O Linux tem a vantagem de possuir ferramentas livres que permitem fazer a captura da imagem. No Windows, uma das ferramentas de imagem mais populares é o FTK Imager (*Forensic Tool Kits*). Nesse passo foram utilizados três softwares diferentes, dois deles são ferramentas do Linux, o último é um software do Windows, com cada um desses softwares foi criada uma imagem forense. Os softwares utilizados para criar a imagem forense são:

[3] Geração de Imagem - deverá ser realizada na etapa de Colheita do modelo proposto neste trabalho (ver Figura 11)

1. FTK Imager 3.2.0 (Windows 64 bits) - é uma ferramenta de imagem de disco gratuita, fornecida pela AccessData;

2. dcfldd (dcfldd) 1.3.4-1 (Kali Linux 32 bits) - é uma versão melhorada do GNU *dd* com vários aprimoramentos forenses, desenvolvida por Nicholas Harbour que trabalhava para o *Department of Defense Computer Forensic Lab*;

3. dc3dd (dc3dd) 7.1.614 (Kali Linux 32 bits) - é uma outra versão melhorada do programa GNU *dd* existente. É desenvolvida e mantida pelo *US Department of Defense Cyber Crime Centre*. A maioria dos recursos foi inspirada no software *dcfldd* e modificada para o dc3dd.

A geração da imagem é uma fase crítica e a falta de cuidados pode levar a inutilização da prova, por meio de procedimentos inadequados, como por exemplo sobrescrever os dados da unidade original com os dados contidos na cópia. É comum na prática o emprego de dispositivos ou de softwares bloqueadores de escrita, os quais impediriam que houvesse escrita na mídia original.

Em dispositivos de estado sólido, os algoritmos internos do SSD geram alterações que tornam a utilização dos bloqueadores de escrita inócuos para eles, neste trabalho não foram empregados bloqueadores de escrita. A não utilização de um bloqueador de escrita exige maior atenção da equipe, a contaminação dos dados por comandos externos, por falhas em procedimentos, caso houvesse, seria evidenciada por meio dos mecanismos de verificação de integridade utilizados nos experimentos.

6.1.1.2 Recuperação de Dados

O segundo passo para investigar a presença de dados em espaços não alocados é o processo chamado de recuperação de dados[4]. Nessa etapa o objetivo é recuperar os dados que foram perdidos, corrompidos, apagados ou tornados inacessíveis por qualquer motivo.

Neste passo, foram utilizadas as imagens geradas na etapa anterior, a elas foram aplicadas softwares de recuperação de dados. Os softwares utilizados foram: Foremost, Scalpel, Magic Rescue, Photorec e Recoverjpeg.

Não está no escopo deste trabalho avaliar a capacidade dos softwares de geração de imagem (Subseção 6.1.1.1) também não está no escopo avaliar os softwares de recuperação de dados. É suficiente, para atingir o objetivo de recuperar dados, conseguir encontrar e recuperar dados válidos com qualquer combinação de softwares de geração de imagem e de recuperação de dados.

[4] Recuperação de dados - é um conjunto de processos ou técnicas para restaurar, acessar, encontrar dados que foram corrompidos, danificados, apagados ou sofreram formatação. A etapa de Exame (contida na Figura 11 do modelo proposto neste trabalho) é a etapa em que deverá ser feita a recuperação de dados.

6.1.1.3 Resultados e Discussão

A realização do experimento 1, já descrita, está ilustrada na Figura 15.

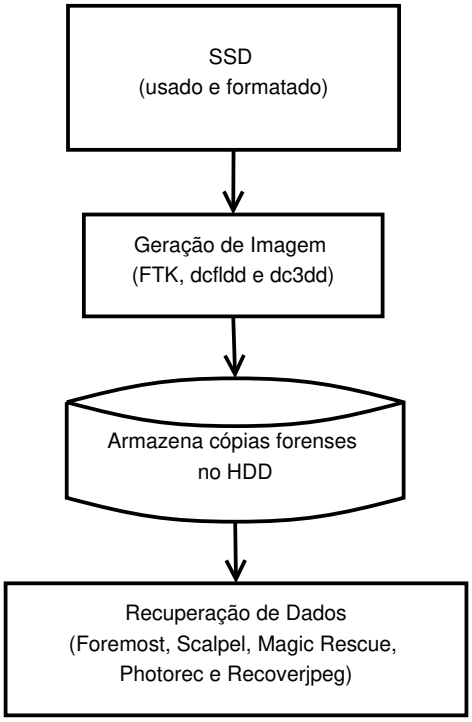


Figura 15 – Experimento 1 - Recuperação pericial comum

Nesse experimento, devido a trabalhos anteriores, esperava-se encontrar arquivos contendo "00s" na visualização em hexadecimal conforme mencionado por Antonellis em (ANTONELLIS, 2008) ou uma taxa muito baixa de recuperação de dados. Isso demonstraria que dados após apagados são praticamente irrecuperáveis, isso seria trágico para o trabalho forense ou de recuperação de dados. Sabe-se com base no trabalho de Skorobogatov (SKOROBOGATOV, 2005) que dispositivos de memória com *floating gate* possuem problemas de remanescência de dados e que, até mesmo depois de uma operação de apagamento, o transistor não retorna totalmente ao seu estado inicial. Há um método para leitura do conteúdo do chip NAND de forma direta ignorando algumas camadas, esse método é conhecido como aquisição de caixa-branca. Entretanto ele é caro e nem sempre é viável.

Esta pesquisa utiliza uma abordagem conhecida como caixa-preta (lê os dados tal como apresentados pelo controlador de memória SSD) que é um método mais conveniente, barato e fácil de executar. No entanto, há trabalhos que obtêm resultados extremamente insatisfatórios com essa metodologia, um exemplo que pode ser mencionado é a pesquisa de Bell e Boddington (BELL; BODDINGTON, 2010). Eles são malsucedidos em sua intenção de recuperar dados a partir de unidades de estado sólido.

Apesar de haver artigos que descrevem unidades de estado sólido como capazes de destruir provas catastroficamente, nesta pesquisa os resultados obtidos contradizem (AN-

TONELLIS, 2008) e (BELL; BODDINGTON, 2010) e o objetivo de encontrar e recuperar dados é alcançado.

A metodologia foi aplicada em uma unidade que era usada em um computador com tarefas típicas de um usuário doméstico, incluindo a criação de documentos, navegação web, música. Depois de certo tempo um comando de formatação rápida foi executado, o sistema operacional supostamente enviou comando ao SSD de que toda a unidade poderia ser "zerada". O SSD utilizado possui suporte ao comando TRIM que é utilizado para otimizar o desempenho da unidade, mas é útil também como ferramenta anti-forense (NISBET; LAWRENCE; RUFF, 2013). Com esses procedimentos espera-se que os blocos do drive sejam inteiramente apagados em questão de segundos (NISBET; LAWRENCE; RUFF, 2013).

Os primeiros procedimentos tomados foram as execuções de cada um dos softwares voltados para geração de imagens forenses mencionados na Subseção 6.1.1.1, com isso foram obtidas três imagens distintas:

1. Com o FTK Imager 3.2.0 - arquivo de 1.535.888 KB;
2. Com o dcfldd (dcfldd) 1.3.4-1 - arquivo de 16.035.748 KB;
3. Com o dc3dd (dc3dd) 7.1.614 - arquivo de 31.263.744 KB.

A segunda etapa (Subseção 6.1.1.2) obtém o resultado final, ou seja, permite saber se é possível restaurar arquivos a partir das imagens forenses geradas na etapa anterior. Com o desfecho da segunda etapa, chega-se ao principal objetivo do trabalho, o qual é responder à seguinte pergunta: É possível recuperar dados apagados em SSD?

A dúvida é pertinente porque SSD há algumas características que podem destruir todos os dados residuais sem intervenção do usuário, mencionadas na Seção 5.2.

Ferramentas para recuperação de dados são usadas quando se deseja recuperar pastas e arquivos apagados ou para recuperar dados de mídias danificadas. Nesta pesquisa, todos os softwares utilizados foram mencionados no início na Subseção 6.1.1.2 e houve recuperação bem sucedida de dados a partir da imagem criada do SSD.

Com todos os softwares empregados houve recuperação de muitos arquivos: imagens (*.jpg, *.bmp, *.gif, *.png), vídeos (*.avi, *.mpg), documentos (*.pdf, *.doc) e outros arquivos (*.java, *.sys, *.dll).

Testes realizados nesta pesquisa demonstram que os arquivos, eliminados após a formatação, puderam ser recuperados com essas ferramentas de *carving*. Depois da formatação o SSD parece estar completamente vazio, mas diferentemente de resultados obtidos em pesquisas anteriores (ANTONELLIS, 2008) (BELL; BODDINGTON, 2010), foram restaurados arquivos típicos, como documentos e figuras a partir da imagem forense gerada a partir desse SSD formatado. Foi analisado um cenário em que um SSD passou por um processo de formatação, a partir do SSD formatado foram geradas três imagens forenses com três diferentes ferramentas (FTK Imager, DCFLDD, DC3DD). A partir dessas imagens foram

utilizados cinco softwares de recuperação de dados (Foremost, Scalpel, Magic Rescue, PhotoRec, Recoverjpeg) para otimizar a chance de recuperação de informações válidas.

Muitas pesquisas indicam que SSDs não podem ser tratados como HDDs convencionais, mas é possível recuperar os dados residuais, mesmo depois da formatação dessa unidade. Devido ao extenso tempo de uso da tecnologia de discos rígidos magnéticos há ferramentas padronizadas e técnicas bem conhecidas desenvolvidas para recuperar dados apagados. No caso de unidades de estado sólido, também há dados remanescentes, e mesmo com mecanismos específicos que podem destruir dados, ficou demonstrado que algumas informações podem ser recuperadas ainda que utilizando as ferramentas já disponíveis para recuperação de dados em HDDs.

Há diferentes controladores, e, portanto, alguns SSDs agem de forma diferente. (BONETTI et al., 2014) mostra que a combinação de controlador, sistema de arquivos, sistema operacional e até mesmo o uso do SSD podem influenciar profundamente na quantidade de informações que podem ser recuperadas.

6.1.2 Experimento 2 - Alterações dos Dados do SSD

Esse experimento difere bastante do experimento descrito em 6.1.1 e ilustrado na Figura 15.

O ambiente utilizado para experimentos, as unidades de estado sólido utilizadas, o computador e o sistema operacional, os dados utilizados na gravação e na recuperação serão, em seguida, detalhados a fim de aferir o tempo em que os mecanismos internos deixam de alterar os dados presentes na unidade, recuperar dados - quando possível - por meio da técnica baseada no sistema de arquivos.

6.1.2.1 Computador

O computador empregado possui processador AMD FX-8350 de oito núcleos, com 8GB DDR3 1600MHz, executando Linux 4.9.0-4-amd64 (Debian). O computador está instalado com um HDD e quatro SSDs. O HDD (HDD Seagate ST2000DM001-1CH1 - 2 TB) contém o sistema operacional e todos os softwares necessários para o experimento, dentre eles: dc3dd (versão 7.2.646) para geração de imagens e hash criptográfico, bem como foremost (v1.5 - maio 2009), scalpel (v1.6 - dezembro 2006), Magic Rescue (v1.1.9 - outubro 2008), photorec (v7.0 - abril 2015), recoverjpeg (novembro 2016) e ntfsundelete (v2016.2.22AR.1) para recuperação dos dados. As unidades de SSD que serão objeto de análise são detalhadas na Tabela 4.

Adotou-se a criação de partições de 32GB para padronizar o tamanho utilizado nas unidades SSD que foram adquiridas para esses experimentos e que são mais modernas (uma de 120GB e uma de 240GB). A capacidade de armazenamento das unidades mais antigas empregadas no experimento apresentam 32GB. Os SSDs estão ligados a interfaces SATA por meio da AMD SB950 Southbridge da placa-mãe ASUS M5A99X EVO R2.0,

Tabela 4 – Solid State Disks Testados

Model	Controller	Capacity
Kingston 32GB	JMF616	32 GB
Sandisk U100	Sandisk 20-82-00270-1	32 GB
Sandisk SSD Plus 120G	SM2256 P4 RX95.00	120 GB
Sandisk SSD Plus 240G	SM2256 P4 TA85.00	240 GB

são formatados com o sistema de arquivos NTFS, passam por um processo de wipe [5] e recebem dados de diversos tipos: .txt, .doc, .docx, .pdf, .jpg, .png, .wmv, .mts, .mpg, .flv, .zip. A descrição dos arquivos utilizados está detalhada no Apêndice B.

A utilização de um computador em que há uma unidade HDD separada para o sistema operacional e softwares necessários, visa assegurar que a leitura, escrita e apagamento nas unidades SSD serão realizados por programas que estejam no HDD, minimizando atividade indesejada que porventura gerem erros na observação.

6.1.2.2 Parada nas Alterações Originadas pelos Mecanismos Internos do SSD

Nessa fase da pesquisa, o objetivo é encontrar um momento em que, após o apagamento dos dados, os mecanismos internos param de modificar os bits que estão nas células de memória.

O apagamento de dados deve causar o início da execução de processos internos ao SSD, *garbage-collection* e *wear-leveling*.

No período de pausa nas alterações ou de inatividade, a unidade não está sofrendo alteração de dados devido aos processos internos de um SSD. O experimento foi realizado de forma controlada e a inatividade foi verificada pelo *hash* (SHA-256) das unidades.

6.1.2.3 Geração da Imagem

Os passos detalhados para geração de imagem e geração de *hash* desse experimento são:

1. Todas as unidades foram particionadas com 32GB; foi realizado um wipe nas unidades, o sistema de arquivos escolhido foi o NTFS; pelo fato de ainda termos o Windows (que utiliza o NTFS) como sistema operacional prevalente.

2. Foram gerados cinco arquivos em formato texto (sem formatação). Os arquivos possuem apenas duas palavras (hello world) em linhas distintas e que se repetem formando arquivos de diferentes tamanhos (12B, 96B, 12.6MB, 402.7MB e 25.8GB).

3. Todos os arquivos foram copiados através do programa nautilus para os SSDs.

[5] Wipe - é um termo empregado para designar o processo de tornar todos os dados em uma unidade de armazenamento ilegíveis. Frequentemente usado em referência a tornar os dados armazenados em um computador, smartphone ou tablet inacessíveis antes de descartar o dispositivo

4. Com todos os arquivos já presentes nas unidades, foi empregado o software dc3dd para gerar imagem e gerar hash para posterior comparação.

5. Os arquivos foram apagados através do nautilus e a lixeira foi esvaziada.

6. Novamente foi empregado o software dc3dd para gerar imagens em formato **"dd"** e *hashes*, em intervalos determinados (20 minutos, 30 minutos, 1 hora, 8 horas e 24 horas após o apagamento e esvaziamento da lixeira no software nautilus).

7. As imagens e hashes gerados foram armazenados no HDD, os *hashes* foram utilizados para identificar os períodos de inatividade e para montar a Tab 4.

6.1.2.4 Resultados e Discussão

As etapas seguidas no Experimento 2, estão ilustradas na Figura 16.

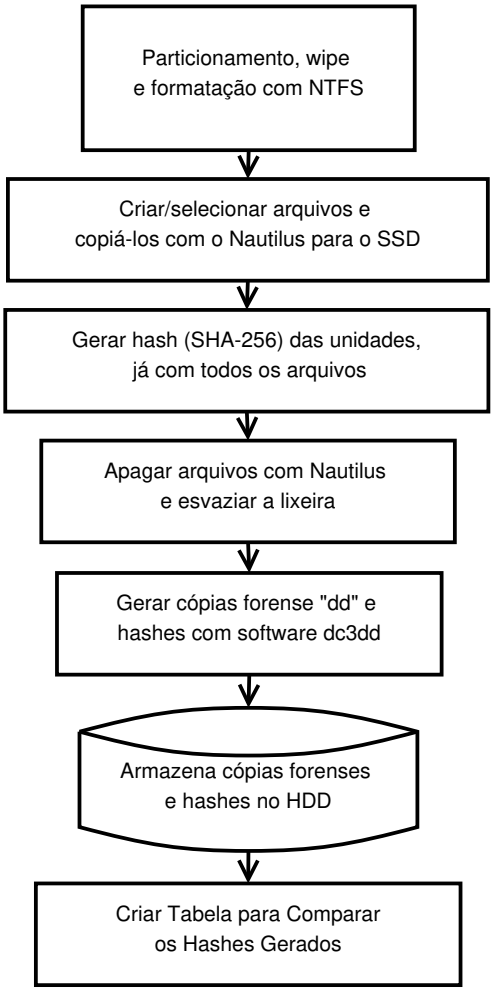


Figura 16 – Experimento 2 - Verificação da alteração dos dados do SSD

A partir dos *hashes* gerados, como etapa do Experimento 2, foi construída a Tabela 5 que permite observar claramente a pausa nas alterações dos bits:

Tabela 5 – Saídas *Hash* - SHA-256.

Model	Hash (20min)	Hash (30min)	Hash (1hr)	Hash (8hrs)	Hash (24hrs)
Kingston 32GB	ba393185ccd1a217ec1673c9f81bc0f30997b9d20706b9816a159da18be83b77	1fc0f93e2d6f3932f8eaf45d0fab7bf98ea230ba1fba6c35712a7fc208382f13	1fc0f93e2d6f3932f8eaf45d0fab7bf98ea230ba1fba6c35712a7fc208382f13	1fc0f93e2d6f3932f8eaf45d0fab7bf98ea230ba1fba6c35712a7fc208382f13	1fc0f93e2d6f3932f8eaf45d0fab7bf98ea230ba1fba6c35712a7fc208382f13
Sandisk U100	ec87c075b881c669d2069c1dacfc8c43c854c709d5bad0a7a282afc6ce6ed2b2	a585e975f65cbefaee03e08d9d5f49f2bda7990e1c88e7ba469995f444166d08	a585e975f65cbefaee03e08d9d5f49f2bda7990e1c88e7ba469995f444166d08	a585e975f65cbefaee03e08d9d5f49f2bda7990e1c88e7ba469995f444166d08	a585e975f65cbefaee03e08d9d5f49f2bda7990e1c88e7ba469995f444166d08
Sandisk SSD Plus 120G	9adc42dbe7c3d8fe09f5c698a4d1599cb9714329dde34f82258831f1749eb204	9160e8e5a12aa0e2497621a949933b9a58a97f6e2208f149d497f245088e1f5b	9160e8e5a12aa0e2497621a949933b9a58a97f6e2208f149d497f245088e1f5b	9160e8e5a12aa0e2497621a949933b9a58a97f6e2208f149d497f245088e1f5b	9160e8e5a12aa0e2497621a949933b9a58a97f6e2208f149d497f245088e1f5b
Sandisk SSD Plus 240G	b8066c86b89fc8463ebcd81aa4f3a4788853fa6e3eab3190df9034dce36350a4	8fed8765c408cdfe4aef0b5b004208dd14f7a82baf585aa2a7c6bb87b7fa60e7	8fed8765c408cdfe4aef0b5b004208dd14f7a82baf585aa2a7c6bb87b7fa60e7	8fed8765c408cdfe4aef0b5b004208dd14f7a82baf585aa2a7c6bb87b7fa60e7	8fed8765c408cdfe4aef0b5b004208dd14f7a82baf585aa2a7c6bb87b7fa60e7

†**Observação:** Foi utilizado o SHA-256 por estar disponível no software dc3dd e por facilitar a apresentação

Através da Tabela 4, observa-se que após 30 minutos o conteúdo do *hash* criptográfico gerado não se altera. Esse resultado demonstra que após certo tempo os mecanismos internos já realizaram as tarefas que deveriam após o disparo ocasionado pelo apagamento dos dados e a unidade de estado sólido entra em um período de inatividade em que não há mais alteração interna de dados. A partir da identificação do ponto de inatividade será possível, sem prejuízo, realizar uma cópia bit-a-bit do SSD para um HDD e demonstrar que o conteúdo da cópia forense gerada e armazenada no HDD (ou outra mídia de armazenamento persistente) é idêntico ao conteúdo do SSD. De forma que o que nos garantirá a fiabilidade é o mecanismo de verificação de integridade escolhido (preferencalmente SHA-3). Para validar os resultados, o processo foi repetido em todas as unidades.

Mesmo após decorridos 7 dias, com as unidades desmontadas e alimentadas, não houve alteração do *hash* criptográfico gerado, todos os valores de *hash* obtidos permaneceram iguais àqueles da Tabela 4 na coluna de 30 minutos, o que indica que TRIM, *garbage collection* e *wear-leveling* não entraram em execução e permaneceram inativos.

6.1.3 Experimento 3 - Recuperação de Dados

Esse experimento utilizou-se do mesmo ambiente descrito em 6.1.2, ou seja, o computador descrito em 6.1.2.1 e as unidades SSD descritas na Tabela 2.

Nesse experimento o objetivo deixa de ser saber em que momento as alterações dos

dados do SSD cessam, e passa a ser o foco a recuperação dos dados de espaços não alocados. Os dados que estiverem alocados a arquivos já estão disponíveis para o perito, bastando-se realizar a cópia forense e demais passos pertinentes conforme o procedimento operacional padronizado. A recuperação de dados será feita em espaços não alocados para arquivos.

Conforme descreve Nadeem Alherbawi e outros (ALHERBAWI N.; SHUKUR, 2016), as imagens geradas pelas cópias bit-a-bit podem conter, em regra, dados alocados a arquivos ou dados não alocados. Mesmo nos dados não alocados, pode haver informações relevantes para uma investigação. Esses dados presentes em espaços não alocados podem ter sido intencionalmente ou acidentalmente apagados.

6.1.3.1 A Recuperação de Dados

A recuperação de arquivos precisa de métodos que permitam preservar a prova, de tal forma que seja possível assegurar a integridade dos arquivos que foram colhidos e que serão utilizados como prova no tribunal. Na área da forense computacional, a comparação entre valores gerados de *hash* criptográfico, gerados a partir de cópias bit-a-bit da unidade ou de arquivos, são os procedimentos mais largamente utilizados para determinar se a integridade da prova foi violada, o que comprometeria a validade da prova porque ela poderia ter sofrido algum tipo de manipulação mal-intencionada.

Para que a recuperação de dados não seja comprometida com valores de *hash* que se alterem durante o processo de forense computacional, foram criadas cópias bit-a-bit com o software "dc3dd" e gerados *hashes* criptográficos de cada uma dessas imagens, conforme descrito em 6.1.2.3. Aguardou-se um período de 7 dias com as unidades em período de inatividade, daí foram geradas novas imagens e *hashes* criptográficos, para só então iniciar-se o processo de recuperação de dados, de forma a garantir a validade, a verificabilidade e a reprodutibilidade diante de um tribunal.

Há múltiplas formas de recuperar dados de espaços não alocados, a maior parte das técnicas usa informações de *file system* para localizar e recuperar arquivos que foram apagados (ALHERBAWI N.; SHUKUR, 2016). Segundo Anandabrata Pal e Nasir Memon (PAL; MEMON, 2009), a abordagem baseada em *file system* possui a vantagem de ser mais rápida e de ter a possibilidade de recuperar os metadados, que são muito úteis em forense computacional. Na abordagem baseada em *filesystem* foi utilizada a ferramenta NTFSUNDELETE, mais detalhes da ferramenta e de sua utilização neste trabalho podem ser encontrados no Apêndice E.

Se não for possível recuperar por meio de abordagens baseadas em *file system*, há técnicas que trabalham de forma independente, buscando-se informações diretamente dos dados brutos (*raw data*). O termo geralmente empregado para a recuperação de dados diretamente de *raw data* é *carving*. Segundo Laurenson (LAURENSON, 2013), as técnicas de *carving* podem ser baseadas em cabeçalho/rodapé (ou cabeçalho/tamanho máximo),

estrutura de arquivos e em blocos de conteúdo. Para abordagem baseada em *carving* foram utilizadas diversas ferramentas, mais detalhes das ferramentas e de sua utilização neste trabalho podem ser encontrados no Apêndice F.

Para a recuperação baseada no sistema de arquivos, há técnicas especificamente desenvolvidas com base no *file system* utilizado e, como as unidades da pesquisa utilizavam NTFS, optou-se pela ferramenta "ntfsundelete" desenvolvido para recuperar arquivos apagados em um sistema de arquivos NTFS e que faz parte do pacote "ntfsprogs". Alguns dos resultados encontrados estão disponíveis no Apêndice E.

Para assegurar que o apagamento dos arquivos disparou os mecanismos internos do SSD para *garbage collection* e *wear-leveling*, foi realizada a execução forçada do TRIM nas unidades (através do comando linux *fstrim -v /caminho/nomeUnidade*) e verificou-se que havia mudança nas unidades por meio da comparação dos valores de *hash* criptográficos gerados. No entanto, não há como assegurar que o TRIM foi implementado de forma correta pelos fabricantes, de modo que há trabalhos os quais procuram caracterizar a operação do TRIM em SSD pelo monitoramento da corrente elétrica do dispositivo (SHEY et al., 2018). Esse detalhamento foge do escopo deste trabalho, sendo relevante para esse experimento saber que houve o disparo dos mecanismos internos os quais, de forma isolada ou em conjunto, dificultam a recuperação de dados forenses realizada por um perito.

6.1.3.2 Experimento 3 - parte 1 - Recuperação de Dados Apenas de Texto ".txt" sem sobrescrita

Os passos detalhados do experimento foram:

1. Todas as unidades foram particionadas com 32GB; foi realizado um wipe nas unidades; o sistema de arquivos escolhido foi o NTFS, pelo fato de ainda termos o Windows (que utiliza o NTFS) como sistema operacional prevalente.

2. Foram gerados cinco arquivos em formato texto (sem formatação). Os arquivos possuem apenas duas palavras (hello world) em linhas distintas e que se repetem formando arquivos de diferentes tamanhos (12B, 96B, 12.6MB, 402.7MB e 25.8GB).

3. Todos os arquivos foram copiados através do programa nautilus para os SSDs.

4. Com todos os arquivos já presentes nas unidades, foi empregado o software dc3dd para gerar imagem e gerar hash para posterior comparação.

5. Os arquivos foram apagados através do nautilus e a lixeira foi esvaziada.

6. Novamente foi empregado o software dc3dd para gerar imagens em formato dd e hashes.

7. As imagens e hashes gerados foram armazenados no HDD, as imagens foram utilizadas na recuperação de dados e os hashes foram utilizados para identificar os períodos de inatividade.

6.1.3.3 Experimento 3 - parte 2 - Recuperação de Dados Apenas de Texto ".txt" com sobrescrita

Os passos detalhados do experimento foram:

1. Todas as unidades foram particionadas com 32GB; foi realizado um wipe nas unidades; o sistema de arquivos escolhido foi o NTFS, pelo fato de ainda termos o Windows (que utiliza o NTFS) como sistema operacional prevalente.
2. Foram gerados cinco arquivos em formato texto (sem formatação). Os arquivos possuem apenas duas palavras (hello world) em linhas distintas e que se repetem formando arquivos de diferentes tamanhos (12B, 96B, 12.6MB, 402.7MB e 25.8GB).
3. Todos os arquivos foram copiados através do programa nautilus para os SSDs.
4. Com todos os arquivos já presentes nas unidades, foi empregado o software dc3dd para gerar imagem e gerar hash para posterior comparação.
5. Os arquivos foram apagados através do nautilus e a lixeira foi esvaziada.
6. Realiza-se a recuperação do maior arquivo, gravando-o na mesma unidade em que ele foi recuperado, sobrescrevendo dados que poderiam estar nos espaços não alocados.
7. Novamente foi empregado o software dc3dd para gerar imagem em formato dd e hash.
8. Realiza-se a montagem da unidade e força-se a execução do comando TRIM.
9. Gera-se uma nova imagem e um novo hash, desmonta-se a unidade.
10. Com a unidade desmontada, mais uma imagem e mais um hash são gerados.
11. Os discos são formatados com o software gparted, mais uma imagem e hash são gerados, prossegue-se com a utilização de ferramentas para recuperação de dados baseada em sistemas de arquivos e baseadas em carving de arquivos.

6.1.3.4 Experimento 3 - parte 3 - Recuperação de Dados de Diferentes Tipos

Já os passos detalhados do experimento foram:

1. Todas as unidades foram particionadas com 32GB, foi realizado um wipe nas unidades, o sistema de arquivos escolhido também foi o NTFS.

2. Foram escolhidos arquivos em formato texto (.txt, .doc e .docx), em formato .pdf, arquivos de imagem (.jpg e .png), arquivos de vídeo (.wmv, .mts, .mpg e .flv) e arquivos compactados (.zip).

3. Todos os arquivos foram copiados através do programa nautilus para os SSDs.

4. Com todos os arquivos já presentes nas unidades, foi empregado o software dc3dd para gerar imagem e gerar hash para posterior comparação.

5. Os arquivos foram apagados através do nautilus e a lixeira foi esvaziada.

6. Novamente, foi empregado o software dc3dd para gerar imagens em formato dd e hashes, em intervalos determinados (20 minutos, 30 minutos, 1 hora, 8 horas e 24 horas após o apagamento e esvaziamento da lixeira no software nautilus).

7. As imagens e hashes gerados foram armazenados no HDD, as imagens foram utilizadas na recuperação de dados e os hashes foram utilizados para ratificar que os períodos de inatividade já ocorriam, para que se pudesse proceder com a recuperação forense dos dados.

8. Prossegue-se com a utilização de ferramentas para recuperação de dados baseada em sistemas de arquivos e baseada em *carving* de arquivos.

Nessa pesquisa é relevante saber se, uma vez disparados os procedimentos internos de um SSD (TRIM, *gabage collection* e *wear-leveling*), torna-se inviável uma recuperação forense dos dados.

6.1.3.5 Resultados e Discussão

6.1.3.5.1 Experimento 3 parte 1

- buscou recuperar dados apenas de texto sem sobrescrita, seguindo as etapas mostradas na Figura 17.

Recuperação de Dados Baseada em *Filesystem* Após uma semana foi usado o software ntfsundelete capaz de recuperar arquivos apagados de um volume NTFS. No modo de operação *scan*, foram listados os arquivos que poderiam ser recuperados, bem como o percentual de recuperação possível.

O resultado do ntfsundelete foi o mesmo em todas as unidades SSD, todos os cinco arquivos-texto de diferentes tamanhos (12B, 96B, 12.6MB, 402.7MB e 25.8GB) foram completamente recuperados.

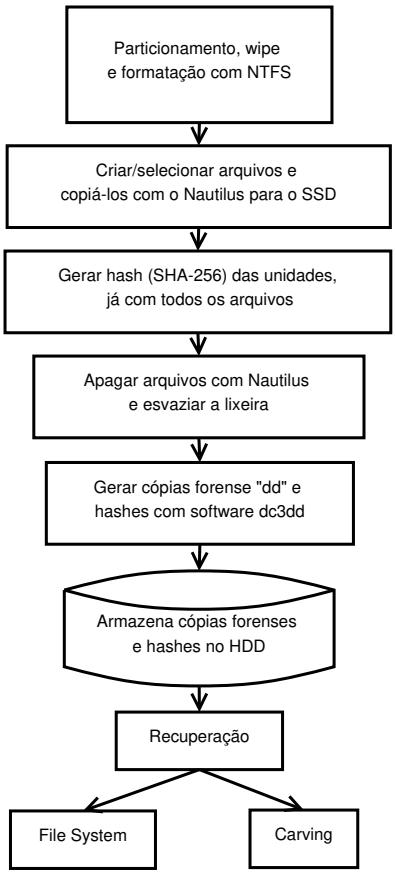


Figura 17 – Experimento 3 parte 1 - Recuperação de dados apenas de texto sem sobrescrita

Recuperação de Dados Baseada em *Carving* Foram empregadas diversas ferramentas, tais como: magicrescue, recoverjpeg, scalpel, photorec. Todas as ferramentas conseguiram recuperar informações dos arquivos-texto, porém não havia informação dos metadados dos arquivos, nem a delimitação de onde terminava um arquivo e onde começava o outro, uma vez que os conteúdos eram idênticos: apenas duas palavras (hello world) em linhas distintas e que se repetem. Não faz parte do escopo da pesquisa a comparação entre as ferramentas, nem o levantamento de estatísticas de recuperação.

Para comparação de ferramentas utilizadas para recuperação baseada em *carving* há os trabalhos de Courrejou e Garfinkel (COURREJOU; GARFINKEL, 2011), além do artigo de Laurenson (LAURENSON, 2013) e do trabalho para obtenção do grau de *Master of Science* de Sonnekus (SONNEKUS, 2014) .

6.1.3.5.2 Experimento 3 parte 2

- buscou recuperar dados apenas de texto com sobrescrita e posteriormente com a formatação da unidade SSD, seguindo as etapas mostradas na Figura 18.

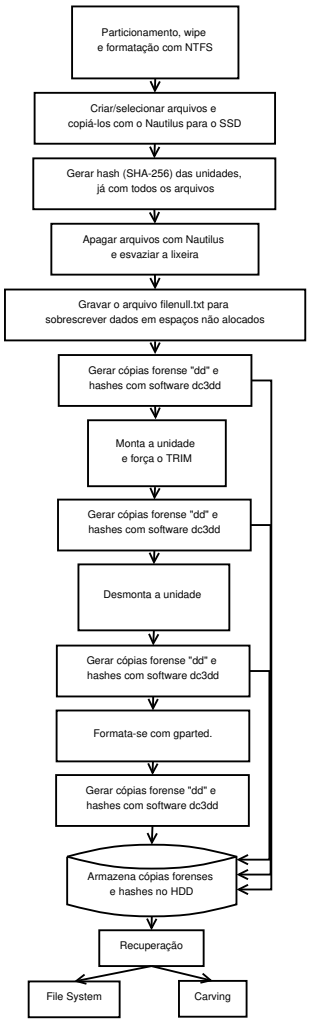


Figura 18 – Experimento 3 parte 2 - Recuperação de dados apenas de texto com sobrescrita e com formatação

Recuperação de Dados Baseada em *Filesystem* Após uma semana foi usado o software ntfsundelete capaz de recuperar arquivos apagados de um volume NTFS. No modo de operação scan, foram listados os arquivos que poderiam ser recuperados, bem como o percentual de recuperação possível.

Diferentemente do experimento 1, foi realizada a recuperação apenas do maior arquivo, o qual foi salvo na mesma unidade SSD, para que esse arquivo venha a sobrescrever parte dos arquivos que ainda estavam no espaço não alocado das unidades SSD. As estatísticas de recuperação entre os diferentes SSDs através do ntfsundelete variaram, mas sempre houve recuperação de arquivos ou parte deles nos espaços não alocados. Foi verificada também a recuperação tanto dos arquivos de poucos bytes (12B e 96B), quanto dos arquivos de alguns megabytes (12.6MB e 402.7MB), que poderiam ter sido completamente sobrescritos pelo arquivo maior previamente recuperado de 25.8GB. Após se forçar a execução do TRIM (por meio do comando *fstrim*) o resultado de recuperação com o ntfsundelete sofreu alteração, conforme se pode observar no Apêndice E a unidade SSD SanDisk

U100 teve apenas dois arquivos recuperados completamente (file.txt e file16.txt) (Subseção E.3.1.1), assim como a unidade Kingston 32G (Subseção E.3.2.1) e a SanDisk 240G (Subseção E.3.4.1).A exceção ficou por conta da unidade SSD SanDisk 120G (Subseção E.3.3.1) cuja recuperação de quatro arquivos foi possível.

No entanto, ao se empregar o software *gparted* para remover as partições e criar novas em seu lugar (formatação lógica [6]), o ntfsundelete não se mostrou capaz de identificar os arquivos presentes no espaço não alocado, conforme também pode ser observado no Apêndice E nas Subseções E.3.1.2, E.3.2.2, E.3.3.2 e E.3.4.2, as quais correspondem respectivamente às tentativas de recuperação de daods das unidades SanDisk U100 32G, Kingston 32G, SanDisk 120G e SanDisk 240G.

Recuperação de Dados Baseada em *Carving* Foram empregadas as ferramentas do experimento 1, da mesma forma, todas as ferramentas conseguiram recuperar informações dos arquivos texto, porém não havia informação dos metadados dos arquivos, nem a delimitação de onde terminava um arquivo e onde começava o outro. Mesmo com a utilização do TRIM e do software *gparted* para remover as partições e criar novas em seu lugar foi possível a recuperação de várias linhas com as palavras hello e world. Esse resultado demonstra que, mesmo após apagar um arquivo, esvaziar a lixeira, forçar a execução do TRIM, remover partições e recriá-las, ainda assim, é possível recuperar fragmentos dos arquivos.

6.1.3.5.3 Experimento 3 parte 3

- buscou recuperar dados de diferentes tipos de arquivos, mais próximo da realidade dos usuários contemplando arquivos não só em diversos formatos de texto (.txt, .doc e .docx), mas também em formatos diversificados .pdf, arquivos de imagem (.jpg e .png), arquivos de vídeo (.wmv, .mts, .mpg e .flv) e arquivos compactados (.zip). O experimento 3 parte 3 seguiu as etapas mostradas na Figura 19.

Recuperação de Dados Baseada em *Filesystem* Pelas estatísticas geradas pelo próprio software ntfsundelete, pode-se descrever a recuperação da unidade SSD Kingston 32G da seguinte forma:

- conseguiu recuperar 4 dentre os 5 arquivos .txt;
- conseguiu recuperar 20 dos 20 arquivos .doc e .docx, com a ressalva de que um dos arquivos .doc só seria possível a recuperação de 72% do conteúdo;
- conseguiu recuperar todos os 20 arquivos .pdf;

[6] Formatação lógica - processo por meio do qual a unidade é preparada para ser utilizada e reconhecida pelo Sistema Operacional (SO), pode ser desfeita e refeita.

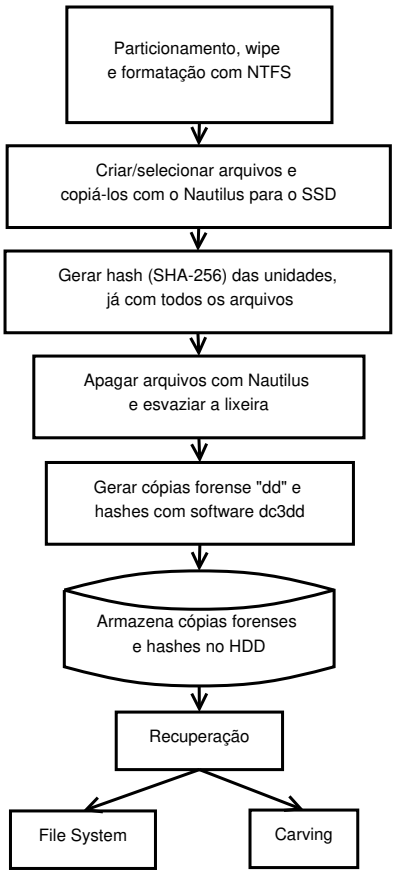


Figura 19 – Experimento 3 parte 3 - Recuperação de dados de diferentes tipos de arquivos

- conseguiu recuperar todos os 20 arquivos .jpg e .png;
- conseguiu recuperar todos os 20 arquivos .wmv, .mts, .mpg e .flv;
- conseguiu recuperar 19 dos 20 arquivos .zip.

Foram encontrados resultados similares na unidade SSD Sandisk SSD Plus de 120GB, ou seja, nas unidades Kingston de 32GB e Sandisk de 120GB, praticamente todos os arquivos foram recuperados. No entanto, nas unidades Sandisk U100 de 32GB e Sandisk de 240GB nada foi recuperado com o software ntfsundelete.

Recuperação de Dados Baseada em *Carving* Foram empregadas as ferramentas de recuperação de dados do Experimento 1 (6.1.1.2), com exceção do Foremost, o qual por sua semelhança com o Scalpel e sendo este melhor que aquele em termos de desempenho, foi preterido.

Na avaliação final todas as ferramentas conseguiram recuperar dados dos arquivos "dd" analisados, com a ressalva de que não houve a recuperação dos metadados.

Detalhes sobre a recuperação de diversos tipos de arquivos, descrição das ferramentas baseadas em *carving* de forense computacional utilizadas, comandos para execução dessas ferramentas podem ser encontrados no Apêndice F.

7 CONCLUSÃO

Desde os primeiros trabalhos, os quais alertavam sobre as dificuldades impostas pelo SSD para a forense computacional publicados no ISSA Journal de julho de 2008 por Antonellis e na DEFCON 16 em agosto de 2008 por Scott Moulton, pesquisas vêm sendo desenvolvidas. Dentre esses trabalhos e pesquisas desenvolvidos são encontrados resultados contraditórios.

Juntamente com o aprofundamento das pesquisas, houve um aumento no número de vendas, na capacidade de armazenamento e na complexidade de algoritmos das controladoras dos SSDs. Até o momento, nenhum procedimento operacional padrão específico para a realização de exames que envolvam SSD foi publicado, tampouco ferramentas específicas.

Logo, diante da ausência de padronização do funcionamento interno das controladoras dos SSDs, é difícil determinar o quanto de dados é possível recuperar. Na literatura acadêmica citada no 2 há propostas que se contradizem, as contradições ocorrem devido aos diferentes ambientes de teste que foram montados (há diferentes comportamentos internos de controladoras, de sistemas operacionais, de ferramentas de geração de imagem e de recuperação).

Dentre os trabalhos relacionados, é possível encontrar situações que desafiam aqueles que trabalham com forense computacional (MOULTON, 2008), (ANTONELLIS, 2008) e (BELL; BODDINGTON, 2010). Porém há autores que encontraram maneiras de demonstrar que mesmo diante da complexidade envolvida, é possível a recuperação sob determinadas condições (BONETTI et al., 2014) (JÚNIOR; QUEIROZ, 2015b) .

A contribuição que este trabalho traz é mostrar as partes principais de um *Solid State Drive* e descrever os mecanismos internos os quais tornam essa unidade de armazenamento persistente diferente dos tradicionais discos magnéticos. Ademais, é realizada uma revisão bibliográfica, de modo que alguns dos principais trabalhos encontram-se mencionados ao longo do texto.

A partir dos experimentos conduzidos, pode-se destacar quatro observações:

Primeiro, verificou-se que o SSD, após a atuação dos seus mecanismos internos, atinge um momento de estabilidade e, à partir desse momento, uma cópia forense pode ser realizada e o código de verificação de integridade (valor de *hash*) da unidade SSD, que contém possíveis vestígios, será igual ao valor de *hash* gerado sobre a cópia forense, restando demonstrado que não houve adulteração dos dados. Valores encontrados para quatro unidades analisadas deram conta de que o tempo para atingir a estabilidade é de cerca de 30 min nos experimentos realizados.

A segunda observação, à partir dos experimentos é a de que a recuperação de dados pode ocorrer, tanto com emprego de ferramentas baseadas em *file system*, quanto em

ferramentas baseadas em *carving*, ademais essas recuperações podem ser empregadas como prova, desde que sejam respeitadas as normas processuais e de direito material. Sendo assim, as provas obtidas a partir do SSD não serão provas ilegais, serão apenas provas atípicas.

A terceira contribuição consiste na proposta de um modelo de investigação forense computacional, baseado na legislação nacional e que, em particular, explicita a necessidade de autorização antes de se proceder às buscas de provas.

Por fim, a quarta contribuição é sugerir um procedimento operacional padrão (POP) específico para dispositivos de armazenamento persistente do tipo SSD, nos moldes dos documentos que já foram publicados pela SENASP(SENASP, 2013).

Como trabalhos futuros e com o prosseguimento de atividades como perito, pretende-se:

- Realizar experimentos com outras unidades de estado sólido;
- Realizar os experimentos com diferentes sistemas operacionais, com diferentes formas de apagamento de arquivos e de conexão da unidade com o computador;
- Testar a recuperação da informação com a combinação de diversas ferramentas livres de geração de imagem forense e de recuperação de dados;
- Tabular resultados estatísticos de recuperação levando-se em conta: modelo de SSD, controladora, sistema operacional, conexão da unidade com o computador, ferramenta de geração de imagem forense e ferramenta de recuperação de dados.

Essa proposta de tese gerou publicações no XIV e no XV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSEG) promovido pela Sociedade Brasileira de Computação (SBC). A primeira publicação foi intitulada "Uso de funções hash em forense computacional"(JÚNIOR; QUEIROZ, 2014); já a segunda, "Forense em *Solid State Drive*: entendendo os mecanismos internos que podem inviabilizar a recuperação de dados" (JÚNIOR; QUEIROZ, 2015b) e a terceira, por sua vez, "Após um processo de formatação, é possível recuperar dados em um SSD?" (JÚNIOR; QUEIROZ, 2015a).

Como continuidade das publicações dessa pesquisa, pretende-se submeter trabalhos ao *IEEE Transactions on Information Forensics and Security* (A2) ou *Journal of Convergence Information Technology* (B1), com ênfase nos resultados encontrados de experimentos com as unidades SSD. E, com ênfase no estudo jurídico, na admissibilidade da prova informática obtida a partir do SSD almeja-se submeter no *Forensic Science International* (B3).

REFERÊNCIAS

AAFS, Boards of Directors . *American Academy of Forensic Sciences*. 1993. <https://www.aafs.org/about-aafs/>.

ACPO, Police Central e-crime Unit. *ACPO Good Practice Guide for Digital Evidence*. 2012. <https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf>.

AFONSO, M. C. d. C. *A reconstituição informática e as provas atípicas em processo penal*. Dissertação (Mestrado) — Universidade Nova de Lisboa, 2016.

AGARWAL, R.; KOTHARI, S. Review of digital forensic investigation frameworks. In: *Information Science and Applications*. [S.l.]: Springer, 2015. p. 561–571.

ALHERBAWI N.; SHUKUR, Z. S. R. A survey on data carving in digital forensic. *Asian Journal of Information Technology*, Medwell Journals, v. 15, p. 5137–5144, 2016.

ALMEIDA, J. C. M. d. Princípios fundamentais do processo penal. *São Paulo: Revista dos Tribunais*, p. 82, 1973.

ANTONELLIS, C. J. Solid state disks and computer forensics. *ISSA Journal*, Citeseer, p. 36–38, 2008.

ASHFORD, W. *Cyber criminals earn up to USD 2m a year, study shows*. [S.l.]: Computer Weekly, 2018. <https://www.computerweekly.com/news/252438668/Cyber-criminals-earn-up-to-2m-a-year-study-shows>.

AULER, P.; MELO, L. P. de; DEUS, F. E. G. de; JR, R. T. de S. Uma Nova Abordagem em Apreensão de Computadores. In: . [S.l.]: ICoFCS, 2011.

BEDAQUE, J. R. dos S. *Poderes instrutórios do juiz*. [S.l.]: Editora Revista dos Tribunais, 1996.

BEDNAR, P.; KATOS, V. Ssd: New challenges for digital forensics. In: ITAIS. *ItAIS 2011, Proceedings of the 8th Conference of the Italian Chapter of the Association for Information Systems*. [S.l.], 2011.

BEEBE, N. Digital forensic research: The good, the bad and the unaddressed. In: SPRINGER. *IFIP International Conference on Digital Forensics*. [S.l.], 2009. p. 17–36.

BELL, G. B.; BODDINGTON, R. Solid state drives: The beginning of the end for current practice in digital forensic recovery? *Journal of Digital Forensics, Security and Law*, Association of Digital Forensics, Security and Law, v. 5, n. 3, p. 1–20, 2010.

BLUM, R. M. O. Internet e os Tribunais. *Revista da Academia de Peritos*, v. 1, n. 1, 2012.

BONETTI, G.; VIGLIONE, M.; FROSSI, A.; MAGGI, F.; ZANERO, S. A comprehensive black-box methodology for testing the forensic characteristics of solid-state drives. In: ACM. *Proceedings of the 29th Annual Computer Security Applications Conference*. [S.l.], 2013. p. 269–278.

BONETTI, G.; VIGLIONE, M.; FROSSI, A.; MAGGI, F.; ZANERO, S. Black-box forensic and antiforensic characteristics of solid-state drives. *Journal of Computer Virology and Hacking Techniques*, Springer, v. 10, n. 4, p. 255–271, 2014.

BRASIL. *DECRETO-LEI Nº 3.689, DE 3 DE OUTUBRO DE 1941. Código de Processo Penal*. 1941.

BRASIL. Medida Proviória. Nº2.200, de 24 de agosto de 2001. 2001.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. *DOU de 3.12.2012*, 2012.

BRASIL. *Novo código de processo civil-Lei 13.105/2015* . [S.l.: s.n.], 2015.

BRASIL. *Sistema Eletrônico de Informações (SEI)*. 2019.

BREZINSKI, D.; KILLALEA, T. *RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group. February*. 2002. <https://tools.ietf.org/html/rfc3227>.

BROWN, W. D.; BREWER, J. E. *Nonvolatile semiconductor memory technology: a comprehensive guide to understanding and to using NVSM devices*. [S.l.]: Wiley-IEEE Press, 1998.

CAPEZ, F. *Curso de processo penal*. [S.l.]: Editora Saraiva, 2016.

CARVALHO, R. C. T. d. A inadmissibilidade da prova ilícita no processo penal: um estudo comparativo das posições brasileira e norte-americana. *Revista Brasileira de Ciências Criminais*, v. 12, p. 162, 1995.

CGSECURITY. *PhotoRec, Digital Picture and File Recovery*. 2015. <https://www.cgsecurity.org/wiki/PhotoRec>.

CHAURASIA, R. K.; SHARMA, P. *Solid State Drive (SSD) Forensics Analysis: A New Challenge*. 2017. <http://ijsrcseit.com/paper/CSEIT1726289.pdf>.

CHEN, F.; KOUFATY, D. A.; ZHANG, X. Understanding intrinsic characteristics and system implications of flash memory based solid state drives. In: ACM. *ACM SIGMETRICS Performance Evaluation Review*. [S.l.], 2009. v. 37, n. 1, p. 181–192.

CINTRA, A. d. A.; GRINOVER, A. P.; DINAMARCO, C. R. *Teoria geral do processo*. [S.l.]: Malheiros editores, 2015.

CORREIA, J. C. A distinção entre prova proibida por violação dos direitos fundamentais e prova nula numa perspectiva essencialmente jurisprudencial. *Revista do CEJ*, v. 1, p. 175, 2006.

COURREJOU, T.; GARFINKEL, S. L. *A Comparative Analysis of File Carving Software*. [S.l.], 2011.

CRAIG, S. *Storage from Edge to Cloud - Enabling the next generation of Anywhere Intelligence*. 2018. <https://www.westerndigital.com/content/dam/western-digital/en-us/assets/events/eventdocs/Presentation-Steven-Craig.pdf>.

DEPUTADOS, C. *Projeto de lei Nº 8.045, de 2010*. 2010.

DIVISION, P. S. S. C. *Digitally Stored Evidence Standard Operating Procedure*. 2018. <http://www.scotland.police.uk/assets/pdf/151934/184779/Digitally-Stored-Evidence-SOP>.

DUKES, C. *Committee on national security systems (CNSS) glossary*. [S.l.], 2015.

EBERHARDT, M. *O STJ e a preservação da cadeia de custódia da prova*. 2014. <https://canalcienciascriminais.jusbrasil.com.br/artigos/198219283/o-stj-e-a-preservacao-da-cadeia-de-custodia-da-prova>.

FILHO, A. M. G. O direito à prova no processo penal. *Revista dos Tribunais*, p. 94, 1997.

FILHO, A. M. G. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). *Estudos em homenagem à professora Ada Pellegrini Grinover. São Paulo: DPJ*, p. 303–318, 2005.

FILHO, A. M. G. A inadmissibilidade das provas ilícitas no processo penal brasileiro. *Revista brasileira de ciências criminais*, n. 85, p. 393, 2010.

FILHO, D. R. *A exibição da prova eletrônica em juízo–Necessidade de alteração das regras do processo civil*. 2006. <http://coad.com.br/app/webroot/files/trab/pdf/ct_net/2006/ct4806.pdf>.

FRANKE, K.; ÅRNES, A. Challenges in digital forensics. *Digital Forensics*, Wiley Online Library, p. 313–317, 2017.

FREILING, F.; GROSS, T.; LATZO, T.; MÜLLER, T.; PALUTKE, R. Advances in forensic data acquisition. *IEEE Design & Test*, IEEE, v. 35, n. 5, p. 63–74, 2018.

GARFINKEL, S. L. Digital forensics research: The next 10 years. *Digital Investigation*, Elsevier, v. 7, p. S64–S73, 2010.

GEBREMARYAM, F. Y. *Solid State Drive (SSD). Digital Forensics Construction*. Dissertação (Mestrado) — Politecnico Di Milano, 2011.

GIOVA, G. Improving chain of custody in forensic investigation of electronic digital systems. *International Journal of Computer Science and Network Security*, v. 11, n. 1, p. 1–9, 2011.

GOMES, R. C. The implementation of search and seizure, the chief of police representation capacity, labeling and judicial review. news. *Revista dos Tribunais*, v. 2017, p. 02–16, 2017.

GOODMAN, M. *A vision of crimes in the future*. 2012. <https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future>.

GOODMAN, M. *Future crimes: Everything is connected, everyone is vulnerable and what we can do about it*. [S.l.]: Anchor Books, 2015.

GRAY, J.; FITZGERALD, B. Flash disk opportunity for server applications. *Queue*, ACM, v. 6, n. 4, p. 18–23, 2008.

GUO, H.; JIN, B.; HUANG, D. Research and review on computer forensics. In: SPRINGER. *International Conference on Forensics in Telecommunications, Information, and Multimedia*. [S.l.], 2010. p. 224–233.

HADDAD, C. H. Verdade material e verdade formal: antiga distinção ou moderna concepção? *Revista CEJ*, v. 16, n. 56, 2012.

HUEBNER, E.; BEM, D.; BEM, O. Computer forensics–past, present and future. *Information security Technical report*, v. 8, n. 2, p. 32–46, 2007.

IDSC, I. D. S. C. *Data Sanitization Terminology and Definitions*. [S.l.]: International Data Sanitization Consortium, 2019. <https://www.datasanitization.org/data-sanitization-terminology/>.

INTEL, C. *Intel® Solid-State Drives: An Introduction*. 2010. <http://www.intel.com/content/www/us/en/solid-state-drives/intel-solid-state-drives-an-introduction.html>.

ISO. Iso/iec 27037:2012 information technology - security techniques - guidelines for identification, collection, acquisition, and preservation of digital evidence. In: INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. [S.l.], 2012.

JAFARI, F.; SATTI, R. S. Comparative Analysis of Digital Forensic Models. In: . [S.l.: s.n.], 2015. v. 3, n. 1, p. 82–86.

JANUKOWICZ, J. *Worldwide Solid State Drive Forecast, 2018-2022*. 2018. <https://www.idc.com/getdoc.jsp?containerId=US42606818>.

JOSHI BINAYA RAJ E HUBBARD, R. Forensics analysis of solid state drive (ssd). In: *2016 Universal Technology Management Conference (UTMC)*. [S.l.: s.n.], 2016. p. 1–12.

JR, A. L.; ROSA, A. Moras da. *A importância da cadeia de custódia para preservar a prova penal*. [S.l.]: Conjur, 2015. <https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal#_edn2>.

JÚNIOR, M. A. C.; QUEIROZ, R. J. G. B. de. Uso de Funções de Hash em Forense Computacional. In: SBC. *Anais do XIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. [S.l.], 2014. p. 545–558.

JÚNIOR, M. A. C.; QUEIROZ, R. J. G. B. de. Após um processo de formatação, é possível recuperar dados em um SSD? In: SBC. *Anais do XV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. [S.l.], 2015. p. 544–553.

JÚNIOR, M. A. C.; QUEIROZ, R. J. G. B. de. Forense em *Solid State Drive*: entendendo os mecanismos internos que podem inviabilizar a recuperação de dados. In: SBC. *Anais do XV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. [S.l.], 2015. p. 524–533.

JUNIOR, S.; PEREIRA, R. As alterações na teoria geral da prova no projeto de lei 8045/2010: o novo código de processo penal. IDP/EDAP, 2018.

KARIE, N. M.; VENTER, H. S. Taxonomy of challenges for digital forensics. *Journal of forensic sciences*, Wiley Online Library, v. 60, n. 4, p. 885–893, 2015.

KENNEALLY, E. E.; BROWN, C. L. Risk sensitive digital evidence collection. *Digital Investigation*, Elsevier, v. 2, n. 2, p. 101–119, 2005.

KENT, K.; CHEVALIER, S.; GRANCE, T.; DANG, H. National institute of standards and technology.?guide to integrating forensic techniques into incident response. nist sp 800-86? *Online [Aug. 2006]*, 2006.

KING, C.; VIDAS, T. Empirical analysis of solid state disk data retention when used with contemporary operating systems. *Digital Investigation*, Elsevier, v. 8, p. S111–S117, 2011.

KOHN, M. D.; ELOFF, M. M.; ELOFF, J. H. Integrated digital forensic process model. *Computers & Security*, Elsevier, v. 38, p. 103–115, 2013.

LAURENSON, T. Performance analysis of file carving tools. In: SPRINGER. *IFIP International Information Security Conference*. [S.l.], 2013. p. 419–433.

LEE, S.-W.; MOON, B.; PARK, C.; KIM, J.-M.; KIM, S.-W. A case for flash memory ssd in enterprise database applications. In: ACM. *Proceedings of the 2008 ACM SIGMOD international conference on Management of data*. [S.l.], 2008. p. 1075–1086.

LESSA, B. M. *A inviabilidade das provas digitais no processo judiciário*. [S.l.]: JUS Navigandi, 2010. <http://jus.com.br/artigos/14555>.

LEWIS, J. Economic Impact of Cybercrime. In: MCAFEE AND CSIS. *Economic Impact of Cybercrime - No Slowing Down*. [S.l.], 2018. p. 28.

LOPES, J. B. Provas atípicas e efetividade do processo. *Revista Eletrônica de Direito Processual*, v. 5, n. 5, 2010.

LUTUI, R. A multidisciplinary digital forensic investigation process model. *Business Horizons*, Elsevier, v. 59, n. 6, p. 593–604, 2016.

MALLMITH, D. d. M. Local de crime. *Departamento de Criminalística do Instituto Geral de Perícias/RS. Secretaria de Segurança Pública do Estado do Rio Grande do Sul. Porto Alegre*, 2007.

MAN, P. *wipe(1) - Linux man page*. 2006. <https://linux.die.net/man/1/wipe>.

MAN, P. *scalpel(1) - Linux man page*. 2013. <https://linux.die.net/man/1/scalpel>.

MAN, P. *photorec(8) - Linux man page*. 2015. <https://linux.die.net/man/8/photorec>.

MAN, P. *ntfsundelete(8) - Linux man page*. 2018. <https://linux.die.net/man/8/ntfsundelete>.

MARQUES, J. F.; FERRARI, E. R.; DEZEM, G. M. *Elementos de direito processual penal*. [S.l.]: Editora Millenium, 2009.

MARTINS-COSTA, J. *A boa-fé no direito privado: critérios para a sua aplicação*. [S.l.]: Saraiva Jur, 2018.

MARUPUDI, S. S. R. *Solid State Drive: New Challenge for Forensic Investigation*. Dissertação (Mestrado) — St. Cloud State University, 2017.

MAXIMIZE, M. R. *Global Solid-State Drive (SSD) Market*. 2018. <https://www.maximizemarketresearch.com/market-report/global-solid-state-drive-market/8397/>.

MICHELONI, R.; ESHGHI, K. Ssd architecture and pci express interface. In: *Inside Solid State Drives (SSDs)*. [S.l.]: Springer, 2013. p. 19–45.

MIRABETE, J. F. Processo penal. 18. ª. *São Paulo*, 2004.

MITCHELL, I.; ANANDARAJA, T.; HARA, S.; HADZHINENOV, G.; NEILSON, D. Deconstruct and preserve (dap): a method for the preservation of digital evidence on solid state drives (ssd). In: SPRINGER. *International Conference on Global Security, Safety, and Sustainability*. [S.l.], 2017. p. 3–11.

MJ. *PORTARIA Nº 1.287, DE 30 DE JUNHO DE 2005*. 2005.

MJ. *Portaria MJ nº 759 de 17/04/2009*. 2009.

MOHAY, G. Technical challenges and directions for digital forensics. In: IEEE. *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*. [S.l.], 2005. p. 155–161.

MOULTON, S. *Solid State Drives Destroy Forensic & Data Recovery Jobs Animated* [S.l.]: DEFCON 16, 2008. <https://www.youtube.com/watch?v=vLoYduckmuo>.

NISBET, A.; LAWRENCE, S.; RUFF, M. A forensic analysis and comparison of solid state drive data retention with trim enabled file systems. In: *Proceedings of the 11th Australian Digital Forensics Conference*. [S.l.]: SRI Security Research Institute, Edith Cowan University, Perth, Western Australia, 2013.

OLSON, A. R.; LANGLOIS, D. J. Solid state drives data reliability and lifetime. *Imation White Paper*, 2008.

O'REILLY, J. *SSD Prices In A Free Fall*. [S.l.]: Network Computing, 2015. <http://www.networkcomputing.com/storage/ssd-prices-in-a-free-fall/a/d-id/1320958>.

PAL, A.; MEMON, N. The evolution of file carving. *IEEE signal processing magazine*, IEEE, v. 26, n. 2, p. 59–71, 2009.

PALMER, G. A road map for digital forensics research–report from the first digital forensics research workshop (dfrws); 2001. *Utica, New York*, 2001.

PALMIERI, G.; ZARGARI, S. Using open source forensic carving tools on split dd and ewf files. In: *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. [S.l.]: IEEE, 2017. p. 379–383.

PERDUE, K. Wear leveling. *Spansion Application Note (Wear_Leveling_AN_01)*, 2008.

POLLITT, M. Applying traditional forensic taxonomy to digital forensics. In: SPRINGER. *IFIP International Conference on Digital Forensics*. [S.l.], 2008. p. 17–26.

RAGHAVAN, S. Digital forensic research: current state of the art. *CSI Transactions on ICT*, Springer, v. 1, n. 1, p. 91–114, 2013.

RANGEL, P. Direito processual penal. *Lumen Juris*, 2009.

REITH, M.; CARR, C.; GUNSCH, G. An examination of digital forensic models. *International Journal of Digital Evidence*, v. 1, n. 3, p. 1–12, 2002.

SANTOS, A. A. d. *O Estado Democrático de Direito*. [S.l.]: Âmbito Jurídico, 2011. <http://ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10143>.

SCHWEITZER, N. J.; SAKS, M. J. The csi effect: Popular fiction about forensic science affects the public's expectations about real forensic science. *Jurimetrics*, JSTOR, p. 357–364, 2007.

SENASP. *Diagnóstico da Perícia Criminal no Brasil*. [S.l.]: SENASP - Depto. de Pesquisa, Análise da Informação e Desenv. de Pessoal em Seg. Pública, 2012.

SENASP. *Procedimento Operacional Padrão - Perícia Criminal*. [S.l.]: SENASP - Depto. de Pesquisa, Análise da Informação e Desenv. de Pessoal em Seg. Pública, 2013.

SENASP. *PORTARIA Nº 82, DE 16 DE JULHO DE 2014*. [S.l.]: SENASP - Depto. de Pesquisa, Análise da Informação e Desenv. de Pessoal em Seg. Pública, 2014.

SEVERO, M. A. d. S. *Quebra da Cadeia de Custódia na Operação Ouro Verde: a Preservação das Fontes da Prova Penal e sua Confiabilidade*. [S.l.]: PUCRS, 2018. <http://conteudo.pucrs.br/wp-content/uploads/sites/11/2018/09/maria_severo.pdf>.

SHAH, Z.; MAHMOOD, A. N.; SLAY, J. Forensic potentials of solid state drives. In: SPRINGER. *International Conference on Security and Privacy in Communication Systems*. [S.l.], 2014. p. 113–126.

SHELTON, D. E.; KIM, Y. S.; BARAK, G. Study of juror expectations and demands concerning scientific evidence: Does the csi effect exist, a. *Vand. J. Ent. & Tech. L.*, HeinOnline, v. 9, p. 331, 2006.

SHEY, J.; BLANCO, J. A.; WALKER, O.; TEDESSO, T.; NGO, H.; RAKVIC, R.; FAIRBANKS, K. D. Monitoring device current to characterize trim operations of solid-state drives. *IEEE Transactions on Information Forensics and Security*, IEEE, 2018.

SHU, F.; OBR, N. Data set management commands proposal for ata8-acs2. *Management*, v. 2, p. 1, 2007.

SILVA, L. A. d. Valor Probante dos Documentos Eletrônicos. *Revista Jurídica do MPRN - Ano 1 v.1 Jun/Dez 2011*, p. 120–143, 2011.

SKOROBOGATOV, S. Data remanence in flash memory devices. In: *Cryptographic Hardware and Embedded Systems–CHES 2005*. [S.l.]: Springer, 2005. p. 339–353.

SONNEKUS, M. H. *A Comparison of Open Source and Proprietary Digital Forensic Software*. Dissertação (Mestrado) — Rhodes University, 2014.

STEVENS, C. E. 8-ata/atapi command set (ata8-acs). Working Draft Project Americaion Nat. Standard Jun, 2006.

STEVENS, C. E. *Working Draft Project - ATA/ATAPI Command Set - 4 (ACS-4) - Revision 20*. 2018. <https://standards.incits.org/apps/group_public/download.php/93215/eb-2017-00575-Public-review-register-INCITS-529-Comments-due-1-30-2018.pdf>.

TAKAYANAGI, F. Y. Os momentos probatórios no direito processual penal. *Revista da Faculdade de Direito, Universidade de São Paulo*, v. 106, n. 106-107, p. 779–807, 2012.

TARUFFO, M.; MICHELI, G. A. *A prova*. [S.l.]: Marcial Pons, 2014.

THOMAS, A. P. The csi effect: fact or fiction. *Yale LJ Pocket Part*, v. 115, p. 70, 2006.

TOMÁS, V. M. G. *Provas ilícitas. Problemática da sua (in) admissibilidade no processo penal*. Tese (Doutorado), 2015.

TUCCI, R. L. Ordem judicial de busca e apreensão e ilicitude da prova dela extrapolante. *Revista dos Tribunais*, v. 848/2006, p. 457–470, 2006.

UBUNTU. *Magic Rescue - Ubuntu man page*. 2016. <http://manpages.ubuntu.com/manpages/xenial/man1/magicrescue.1.html>.

UBUNTU. *recoverjpeg - Ubuntu man page*. 2018. <http://manpages.ubuntu.com/manpages/bionic/man1/recoverjpeg.1.html>.

UNSWORTH JOSEPF E MONROE, J. Market insight: Preparing for the ssd rise and hdd demise. Gartner Group, 2018.

US, H. S. *PhotoRec v7.0-WIP - Graphic File Carving*. 2014. <https://www.dhs.gov/sites/default/files/publications/508_Test%20Report_NIST_PhotoRec%20v7.0-WIP_August%202015_Final_0.pdf>.

US, H. S. *PhotoRec v7.0-WIP - Video File Carving*. 2014. <https://www.dhs.gov/sites/default/files/publications/508_Test%20Report_NIST_PhotoRec%20v7.0-WIP_0_August%202015_Final_0.pdf>.

WEI, M. Y. C.; GRUPP, L. M.; SPADA, F. E.; SWANSON, S. Reliably erasing data from flash-based solid state drives. In: *FAST*. [S.l.: s.n.], 2011. v. 11, p. 8–8.

YANG, M.-C.; CHANG, Y.-M.; TSAO, C.-W.; HUANG, P.-C.; CHANG, Y.-H.; KUO, T.-W. Garbage collection and wear leveling for flash memory: past and future. In: IEEE. *Smart Computing (SMARTCOMP), 2014 International Conference on*. [S.l.], 2014. p. 66–73.

YUSOFF, Y.; ISMAIL, R.; HASSAN, Z. Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology*, Citeseer, v. 3, n. 3, p. 17–31, 2011.

APÊNDICE A – *PROCEDIMENTO OPERACIONAL PADRÃO (POP) Nº 3.5 - INFORMÁTICA FORENSE*

PROCEDIMENTO OPERACIONAL PADRÃO (POP) PERÍCIA CRIMINAL	
POP Nº 3.5 - INFORMÁTICA FORENSE	**EXAME PERICIAL DE SSD**
FINALIDADE: Orientar o profissional da perícia da área de informática a realizar exames que envolvam dados contidos em mídias de armazenamento do tipo SSD em dispositivo desligado.	**PÚBLICO ALVO:** Peritos Criminais afetos à atividade deste POP.

A.1 ABREVIATURAS E SIGLAS

HDD: Hard Disk Drive

SSD: Solid State Disk ou Solid State Drive

A.2 RESULTADOS ESPERADOS

Padronização dos exames periciais de mídias de armazenamento computacional do tipo SSD em dispositivo desligado.

A.3 MATERIAL

- Acesso irrestrito à Internet e privilégios administrativos na estação de trabalho pericial.
- Equipamento que permita a realização de duplicação dos dados.
- Estação de trabalho pericial (hardware + software) que permita o processamento/análise dos dados e a elaboração do laudo e seus anexos.
- Mídia de armazenamento computacional do tipo HDD com capacidade livre superior ao da mídia SSD a ser examinada.
- Mídia de armazenamento computacional do tipo HDD com capacidade suficiente para armazenamento do resultado do exame.

A.4 PROCEDIMENTOS

A.4.1 Ações preliminares

Esta etapa tem como objetivo determinar a possibilidade, viabilidade de realização do exame e organizar o material recebido. Para tanto, deve-se:

- Portar a autorização de busca e apreensão, que é a regra.
- Atentar ao fato de que os equipamentos podem conter vestígios físicos que podem ser de interesse da investigação ou exigir cuidados de manipulação, tais como impressões digitais, resíduos orgânicos (cabelo, pele, sangue, etc) ou outros materiais contaminantes. Para maiores detalhes de Exame Pericial de Local de Informática ver POP nº 3.3.
- Conferir os itens constantes do expediente e analisar a viabilidade do exame pericial requisitado. Havendo inconsistência ou inviabilidade, adotar os procedimentos definidos pelas normas locais.
- Realizar um levantamento do ambiente computacional fotografando-o, caso necessário (POP nº 3.3).
- Buscar e localizar equipamento(s) a que se refere a autorização de busca e apreensão.
- Estando a mídia de armazenamento computacional instalada em um equipamento:
  - Removê-la quando viável;
  - Checar data e hora do equipamento que a unidade estava instalada, sempre que possível;
  - Identificar e documentar o dispositivo computacional (hardware e software, sempre que possível) em que está a mídia;
  - Após identificado o equipamento com o máximo detalhamento, remover a mídia do local original e documentar todo o processo, isso faz parte da Cadeia de Custódia.

A.4.2 Colheita

A.4.2.1 Preservação

Anotação dos procedimentos tomados respeitando-se a ordem cronológica dos eventos e o(s) profissional(is) responsável(is). Anotação das ferramentas de software e de hardware empregados. Se houver uso de quaisquer técnicas de recuperação nesta fase, deve haver menção apropriada na cadeia de custódia.

A.4.2.2 Cópia forense

Esta etapa visa a duplicar os dados contidos na mídia original para uma mídia de trabalho de forma a garantir a preservação dos dados e documentar os softwares, hardwares e métodos que foram empregados para tal.

A duplicação pode ser feita de duas formas:

1. por meio de equipamento forense específico para esse fim;
2. utilizando-se um microcomputador.

No último caso, é imperativo impedir que ocorra qualquer alteração nos dados da mídia original, utilizando-se bloqueadores de escrita por hardware ou software.

A.4.2.2.1 Cópia Forense 1

- Deve ser efetuada uma cópia forense da unidade SSD, essa cópia (doravante denominada de Cópia 1) será mantida como se original fosse.
- Recomenda-se para a Cópia 1:
    1. identificação externa da unidade;
    2. estabelecimento de uma cadeia de custódia específica para essa unidade com anotações de dados da unidade (marca, modelo, capacidade, número de série, para manter uma cadeia de custódia), detalhamento dos procedimentos tomados (registro de atividades e horários);
    3. duplicação de dados do SSD com cópia integral para a Cópia 1 (de uma mídia para outra ou cópia bit-a-bit) com ferramentas (hardware/software) que não alterem o SSD durante a colheita;
    4. geração de hash para verificação da integridade da Cópia 1 que deverá ser adicionado à cadeia de custódia.

A.4.2.2.2 Cópia Forense 2

- Deve ser efetuada uma cópia forense da Cópia 1 (doravante denominada de Cópia 2); sobre a Cópia 2, deverá ser efetuado o exame.
- Recomenda-se para a Cópia 2:
    1. identificação externa da unidade;
    2. estabelecimento de uma cadeia de custódia específica para essa unidade com anotações de dados da unidade (marca, modelo, capacidade, número de série, para manter uma cadeia de custódia), detalhamento dos procedimentos tomados (registro de atividades e horários);

3. duplicação de dados da Cópia 1 para a Cópia 2 (de uma mídia para outra ou cópia bit-a-bit) com ferramentas (hardware/software) que não alterem a Cópia 1 durante a colheita;
4. geração de hash para verificação da integridade da Cópia 2 que deverá ser adicionado à cadeia de custódia e comparado com o hash da Cópia 1 (a Cópia 1 e a Cópia 2 devem gerar a mesma saída *hash*).

ALERTA: Deve-se ficar claro que, mesmo sem a ação de escrita, por comando externo ao SSD, este pode alterar seu conteúdo de forma a prejudicar a verificação da integridade dos dados, isso também pode inviabilizar a comparação dos *hashes* do SSD e da Cópia 1. Esse alerta deve estar escrito na documentação de Cadeia de Custódia.

A.4.3 Exame

Esta etapa visa à preparação dos dados para a análise e pode ser feita por meio de ferramentas livres ou proprietárias. Inclui, a depender do interesse pericial, dentre outros os seguintes procedimentos:

- Preservação;
- Rastreabilidade;
- Descoberta e recuperação de arquivos apagados, incluindo *data carving*;
- Expansão de arquivos compostos (.zip, .pst);
- Checagem de assinatura de arquivos;
- Cálculo de *hashes*;
- Indexação de dados.

A.4.4 Análise dos dados

Esta fase consiste no exame das informações processadas na fase anterior, a fim de identificar e selecionar evidências digitais relacionadas ao escopo pericial. Inclui, a depender do interesse pericial, os seguintes procedimentos, entre outros:

- Preservação;
- Rastreabilidade;
- Técnicas estatísticas;
- Conversão de arquivos;
- Reconstrução de fragmentos;

- Mineração de dados;
- Linha do tempo;
- Ligações entre dados armazenados e eventos;
- Resposta a quesitos formulados.

Exemplos de análises:

1. Esclarecer se um determinado arquivo foi enviado ou recebido pelo usuário do computador examinado.
2. Determinar quando o computador foi utilizado pela última vez.
3. Determinar quais arquivos foram acessados pelo usuário mais recentemente.
4. Reconstrução de imagens ou vídeos que estejam corrompidas através de protocolos/metodologias cientificamente comprovadas

A.4.5 Apresentação

Esta etapa envolve a descrição dos exames efetuados e a apresentação, de forma clara e sucinta, dos procedimentos e métodos utilizados, esclarecendo os temas relevantes para a compreensão dos exames. A apresentação pode ser feita através de:

- Laudo pericial;
- Testemunha pericial;
- Esclarecimentos;
- Resposta escrita a quesitos;
- Recomendação de contramedidas.

A.4.5.1 Tópicos a serem observados

Descrever que todos os exames foram realizados sobre a Cópia 2 e que há o estabelecimento de uma Cadeia de Custódia e mecanismos de garantia da "mesmidade" para cada uma das unidades SSD, Cópia 1 e Cópia 2.

- Relatar, se for o caso, que procedimentos de recuperação de dados apagados ou corrompidos (dentre outros) foram utilizados, e que os exames foram feitos não apenas sobre os arquivos diretamente acessíveis, mas também sobre aqueles apagados (fragmentados, corrompidos, etc.) e passíveis de recuperação;

- Descrever os exames de forma proporcional à sua complexidade, evitando-se assim descrições extensas e complexas para laudos simples, e vice-versa;
- Descrever as técnicas periciais propriamente ditas, e não os detalhes da utilização dos aplicativos forenses;
- Para o caso de existência de mídia anexa ao laudo, explicar que os arquivos ali gravados foram submetidos a uma função de *hash* para fins de garantia de integridade;
- Mencionar eventuais alterações (físicas ou lógicas) promovidas no material examinado e, sempre que possível, sua justificativa;
- Mencionar, em texto padronizado dentro da corporação e com referências atualizadas, que alterações no SSD sem comandos externos de escrita, por pessoas que tenham tido acesso à fonte de prova, podem ocorrer devido aos mecanismos internos do dispositivo;
- O perito deve ser capaz de descrever claramente como a evidência foi encontrada, como ela foi tratada e tudo o que aconteceu com ela.

A.4.5.2 Geração de mídias anexas

Esta etapa visa a normatizar a criação de mídia anexa ao laudo contendo os dados de interesse recuperados da mídia original. A vantagem de geração de mídia anexa é possibilitar que um grande volume de dados seja anexado ao laudo e facilitar a visualização das informações, permitindo, por exemplo, a procura por palavras-chave.

- Recomenda-se, para este fim, a utilização de mídia não regravável, como CDs ou DVDs, com todas as seções fechadas.
- A integridade dos dados contidos na mídia anexa deve ser garantida por meio de utilização de uma função de *hash* (SHA3). Permite-se, dessa forma, a checagem futura de possíveis alterações dos dados gravados.
- A mídia anexa deve conter um arquivo contendo os *hashes* de todos os arquivos existentes na mídia. Por sua vez, o *hash* desse arquivo deve ser impresso no corpo do laudo.
- Não se recomenda a gravação de programas de "cálculo de *hash*" na mídia anexa gerada, exceto quando objeto dos exames.

A.5 PONTOS CRÍTICOS

Este item visa a destacar os seguintes cuidados necessários durante os exames:

- A evidência digital deve ser examinada apenas por peritos criminais com treinamento específico para esse propósito;
- Deve-se evitar a inicialização do equipamento estando a mídia original nele instalada;
- Atentar-se para a possibilidade de que mídias não reconhecidas pelos equipamentos de duplicação estejam protegidas por senha de disco;
- Atentar-se para a possibilidade de que dados ininteligíveis podem significar a utilização de criptografia ou, no caso de existência de mais de um disco no equipamento, o uso de algum tipo de arranjo de discos (RAID, JBOD);
- Cuidar para que, no processo de duplicação dos dados, os dados da mídia original sejam copiados para a mídia de trabalho, e não o contrário;
- Observar a ordem de inicialização no BIOS quando a mídia não puder ser removida do equipamento (mídias soldadas na placa-mãe de notebooks). Nesses casos, a duplicação deve ser feita utilizando-se o próprio equipamento, através de suas interfaces externas (USB), e a inicialização por meio de um live CD ou equivalente (e não por meio do sistema operacional da mídia original).

A.6 ESTRUTURA BÁSICA DO LAUDO

- Preâmbulo
- Histórico (opcional)
- Objetivo
- Material
- Exame
- Considerações Técnico-Periciais (opcional)
- Conclusão/Resposta aos Quesitos
- Anexos (opcional)

A.7 REFERÊNCIAS

DOMINGOS, Tochetto e ALBERI, Espíndula. Criminalística: Procedimentos e Metodologias. (Coord.). 2. ed. Porto Alegre, 2009.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Márcio Pereira. Desvendando a computação forense. São Paulo: Novatec Editora, 2010.

RFC 3227. Guidelines for evidence collection and archiving. 2002.

ISO/IEC 27037. Information technology - Security techniques. Guidelines for identification, collection, acquisiton, and preservation of digital evidence. Switzerland, 2012.

U.S. DEPARTMENT OF JUSTICE. Electronic Crime Scene Investigation: a guide for first responders. 2ª Ed. Washington, 2008.

A.8 GLOSSÁRIO

ARQUIVOS COMPOSTOS: arquivos que contêm outros arquivos.

ASSINATURA DE ARQUIVOS: informação contida nos arquivos que permite identificar seu formato.

BLOQUEIO DE ESCRITA: equipamento ou software que previne a escrita de dados em uma mídia de armazenamento computacional e, assim, garante que os dados não serão alterados através de procedimentos (escritas) oriundos de ações externas à mídia, durante os procedimentos periciais.

CADEIA DE CUSTÓDIA: sucessão de eventos concatenados, de forma a proteger a integridade de um vestígio do local de crime ao seu reconhecimento como prova material até o trânsito em julgado.

CÓPIA FORENSE: cópia de uma unidade que venha a preservar todos os dados sob todos os aspectos (conteúdo, propriedades/metadados e estrutura).

DATA CARVING: processo de recuperação de arquivos com base na procura de assinaturas de arquivos conhecidas.

ESTAÇÃO DE TRABALHO PERICIAL: equipamento com as seguintes características:

1. capacidade de processamento, armazenamento e memória condizentes com as várias exigências de procedimentos de informática forense utilizados durante os exames;
2. possibilidade de substituição de mídias de armazenamento e periféricos;
3. possibilidade de gravação de mídias a serem encaminhadas em anexo aos laudos;
4. dispositivo de prevenção contra ataques, programas maliciosos e acessos remotos não autorizados;
5. proteção contra interrupções de energia;
6. licenças de uso válidas para equipamentos, sistemas operacionais e aplicativos.

FUNÇÃO DE HASH: algoritmo que gera, a partir de uma entrada de qualquer tamanho, uma saída de tamanho fixo, ou seja, é a transformação de uma grande quantidade de informações em uma pequena sequência de bits (*hash*). Esse hash altera se um único bit da entrada for alterado, acrescentado ou retirado.

HDD: *Hard Disk Drive*, ou simplesmente disco rígido, utilizado para armazenamento persistente, grava e lê as informações através do magnetismo.

INDEXAÇÃO: catalogação das ocorrências alfanuméricas de um conjunto de dados, de forma que sejam acessadas e recuperadas rapidamente.

LIVE CD: mídia ótica contendo versão de um sistema operacional carregável em memória RAM, ou seja, sem necessidade de instalação.

MESMIDADE: garantia de que a prova colhida é a mesma que a apresentada em juízo; indica que a prova tem preservadas as suas integridade e confiabilidade

METADADOS: informações sobre os arquivos, tais como tamanho, datas de criação, modificação e acesso, atributos e permissões.

MÍDIA DE ARMAZENAMENTO COMPUTACIONAL: qualquer meio que possa ser utilizado para o armazenamento de dados digitais. Exemplos incluem discos rígidos, CDs, DVDs, pendrives, cartões de memória e disquetes.

MÍDIA DE TRABALHO: mídia de armazenamento computacional onde será armazenada a cópia dos dados da mídia original.

MÍDIA ORIGINAL: mídia de armazenamento computacional encaminhada para exame.

SSD: *Solid State Disk* ou *Solid State Drive*, unidade de estado sólido, utilizada para armazenamento persistente em substituição ao HDD.

APÊNDICE B – *ARQUIVOS UTILIZADOS NA PESQUISA*

B.1 ARQUIVOS ".TXT"

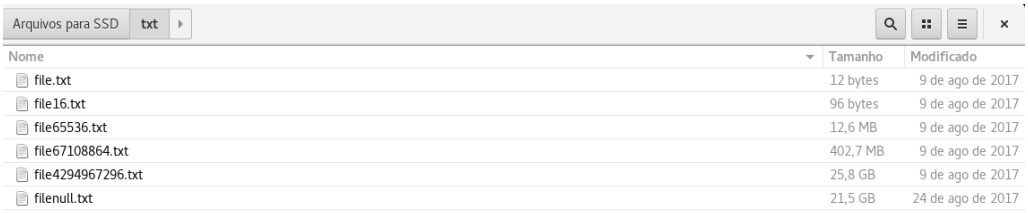


Figura 20 – Arquivos de texto sem formatação utilizados

B.2 ARQUIVOS ".DOC", ".DOCX"

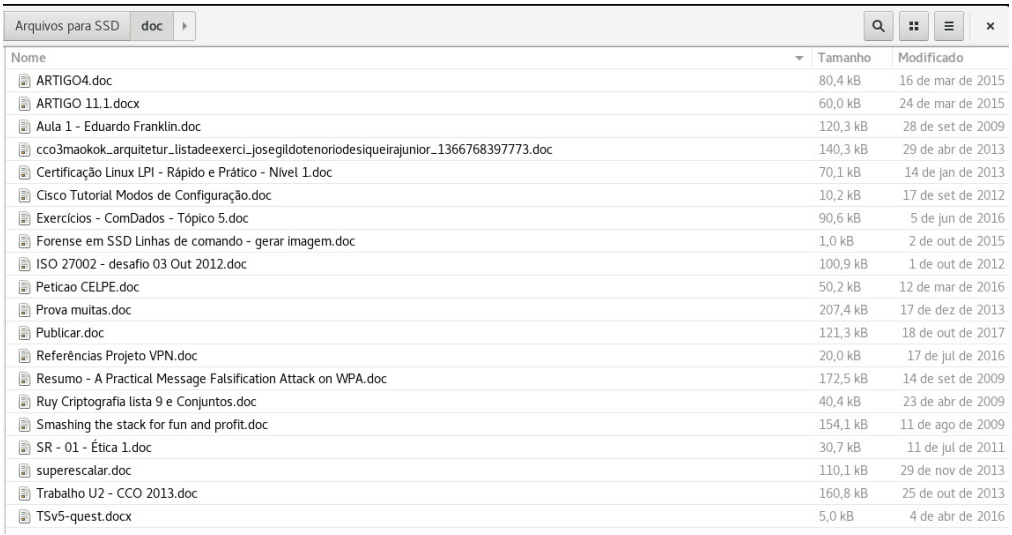


Figura 21 – Arquivos texto .doc e .docx

B.3 ARQUIVOS ".PDF"

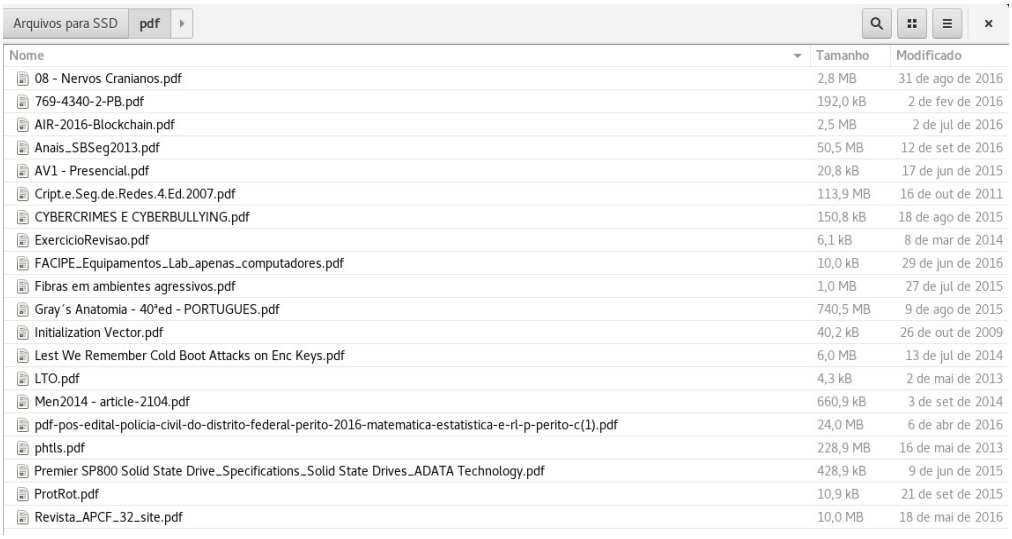


Figura 22 – Arquivos .pdf

B.4 ARQUIVOS “.JPG”, “.PNG”

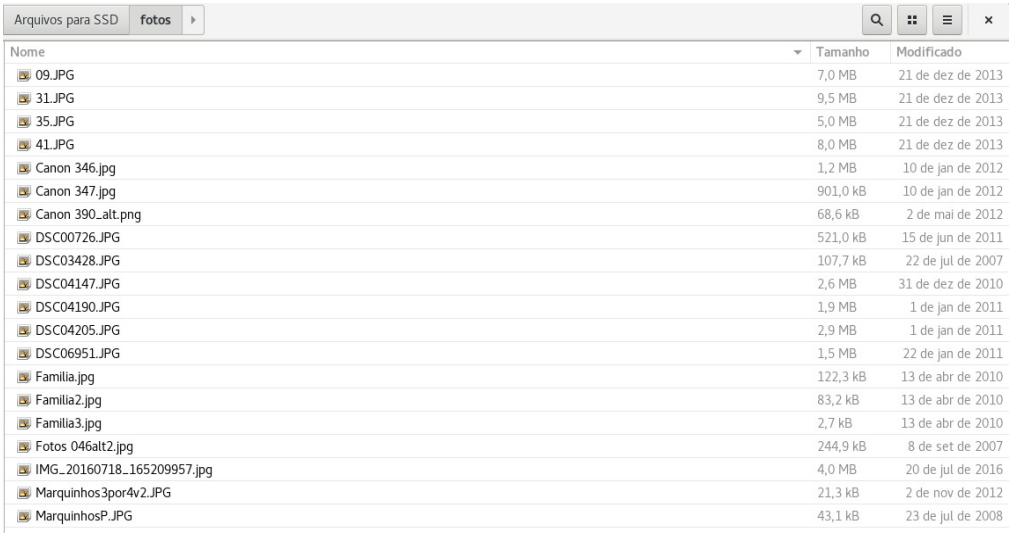


Figura 23 – Arquivos de imagem .jpg e .png

B.5 ARQUIVOS “.WMV”, “.FLV”, “.MPG”, “.MTS”

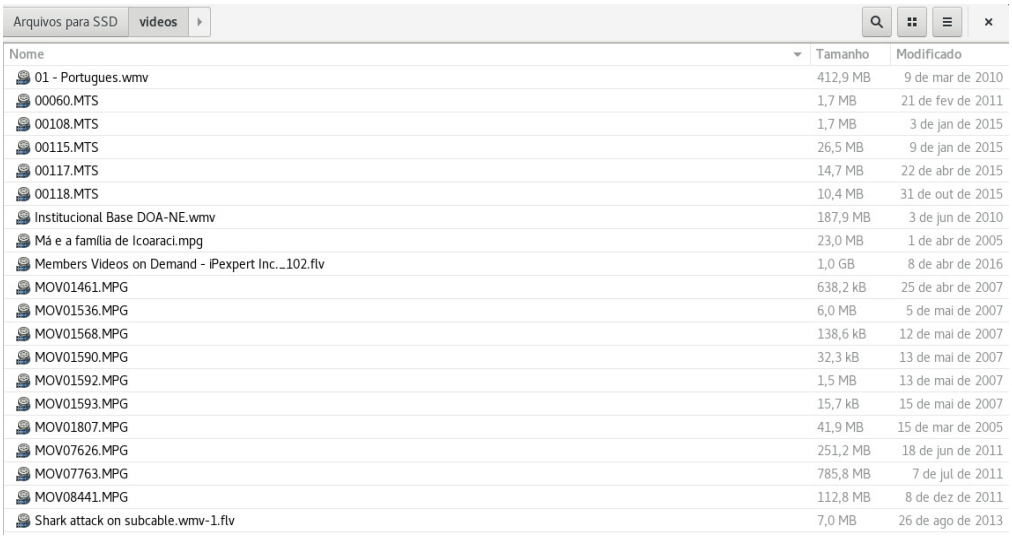


Figura 24 – Arquivos de vídeo .wmv, .flv, .mpg e .mts

B.6 ARQUIVOS ".ZIP"

Figura 25 – Arquivos compactados .zip

APÊNDICE C – *UNIDADES SSD*

C.1 ADATA SP800 32GB

ADATA Premier SP800 Solid State Drive SATA 3 Gb/sec

Specifications

> **Capacities:** 32/64 GB
> **NAND Flash Components:** Multi-Level Cell (MLC) NAND Flash Memory
> **Interface:** 2.5”
> **Controller :** SandForce 2141
> **Form Factor:** SATA 3 Gb/sec (SATA II)
> **Dimensions:** 100 x 69.85 x 9.5mm (L x W x H)
> **Weight:** 76g

Performance

Capacity	Read Speed ATTO (MB/sec)	Write Speed ATTO (MB/sec)	Sequential Read AS-SSD (MB/sec)	Sequential Write AS-SSD (MB/sec)	4K Random Read AS-SSD (MB/sec)	4K Random Write AS-SSD (MB/sec)
32 GB	Up to 280	Up to 260	200	40	25	40
64 GB	Up to 280	Up to 265	250	85	55	85

Features

> **MTBF: 1,000,000 hrs**
> **Trim Support (Requires OS Support)**
> **NCQ Support**
> **Smart Support**
> **3.5” desktop conversion bracket**
> **Acronis True Image HD, Disk Migration Utility**
> **3-Year warranty**
> **OS Compatibility: Windows 7/Windows XP/ Windows Vista / Mac OS X / Linux**

Environmental Parameters

> **Power Consumption (W):** 0.5W Idle
> 0.7W Active
> **Operating Temperature:** 0~70°
> **Storage Temperature:** -40~85°
> **Shock Resistance:** 1500G
> **Certifications CE / FCC / VCCI / BSMI**

ADATA™ Love·Life·Dreams

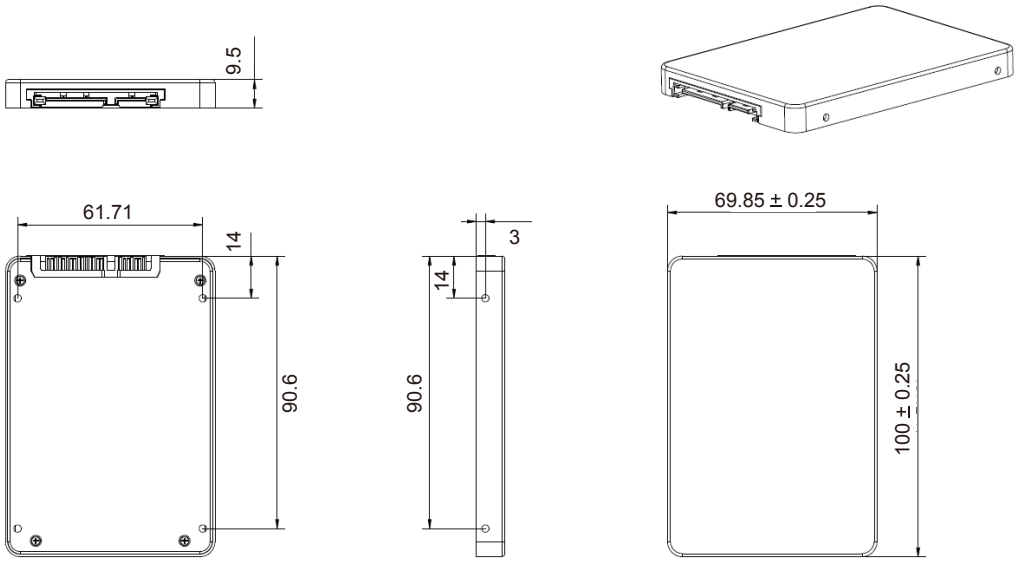
www.adata-group.com

ADATA Premier SP800 Solid State Drive SATA 3 Gb/sec

Ordering Information

Description	Capacity	ADATA Part No.	EAN Code
SP800S 32GB SF2141	32 GB	ASP800S-32GM-C	4713435794777
SP800S 64GB SF2141	64 GB	ASP800S-64GM-C	4713435794630

Dimensional Drawings



C.2 KINGSTON 32G SSD NOW 100

SSD*Now* V100

Melhora o desempenho e prolonga a vida útil do atual sistema.

SSD Now da Kingston *Technology* V100 da Kingston Technology melhora o desempenho radicalmente com velocidades impressionantes. Aumenta a produtividade acelerando os tempos de inicialização e carregamento de aplicativos enquanto remove o travamento e outras falhas do disco rígido.

SSD*Technology* V100 é ideal para consumidores ou pequenas empresas que procuram uma maneira acessível de prolongar a vida útil de desktops ou notebooks a custos mais baixos do que a substituição de um sistema. É perfeito para usuários domésticos, projetistas e fotógrafos freelance, editores de vídeo, pesquisadores, administradores e educadores e qualquer pessoa que precisa viajar a trabalho. É construído sem peças móveis para fornecer durabilidade e confiabilidade para atender as necessidades de profissionais no escritório ou em viagens.

A mudança para uma solução SSD é facilitada por kits de upgrade para sistemas de desktop. Os kits V100 incluem tudo que é necessário para a instalação do SSD, tais como cabos, suportes e software para clonar todos os arquivos principais do usuário — documentos, filmes, música, jogos — e Sistema Operacional em minutos.

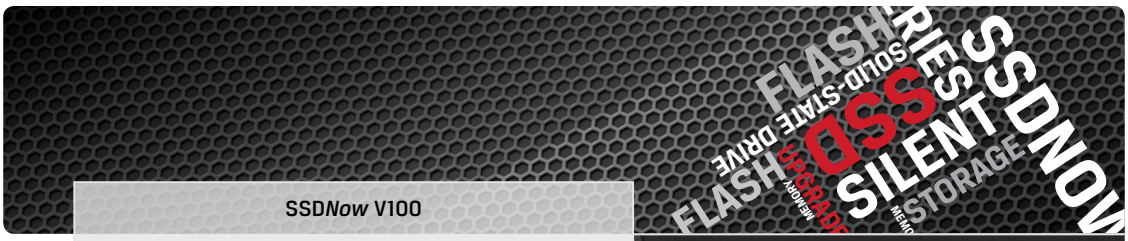
SSD*Now* tem garantia de três anos e a reconhecida confiabilidade Kingston®.

- > Melhora o desempenho do sistema em 50%
- > Compatíveis com TRIM e S.M.A.R.T
- > caixa 2,5 pol ou design half-slim sem caixa

Produto sem caixa somente disponível sob encomenda especial.

Características/especificações no verso››

KINGSTON.COM/BR/SSD



SSD*Now* V100

CARACTERÍSTICAS/BENEFÍCIOS

> **Desempenho** — melhora a produtividade; torna os usuários mais eficientes

> **Componentes** — por não possuir peças mecânicas móveis, o SSD resiste às condições mais extremas

> **Silencioso** — opera de forma silenciosa e produz menos calor, sem peças mecânicas móveis

> **Confiável** — menor probabilidade de falha do que um disco rígido padrão

> **Resistentes a impactos** — por não possuir peças mecânicas móveis, o SSD resiste às condições mais extremas

> **Suporta TRIM** — garante desempenho máximo em sistemas operacionais compatíveis[1]

> **Suporta as funções S.M.A.R.T.**

> **Garantia** — garantia de três anos, suporte técnico gratuito

ESPECIFICAÇÕES

> **Formato** 2,5 pol ou design sem caixa half-slim

> **Interface** SATA 1,5GB/seg e 3,0GB/seg

> **Capacidades**[2] 32GB

> **Dimensões** Caixa de 2,5 pol: 69,85 x 100 x 9,5 mm
Sem caixa half-slim: 54 x 40 mm

> **Peso** Caixa de 2,5 pol: 78 gramas
Sem caixa half-slim: 8,32 gramas

> **Temperatura de Armazenagem** -40°C a 85°C

> **Temperatura de operação** 0°C a 70°C

> **Vibração quando em operação** 2,7G

> **Vibração quando não está em operação** 20G

> **Velocidade para Leitura Sequencial**[3]
32GB – 160MB/s para leitura

> **Velocidade de Gravação Sequencial**[3]
32GB – 70MB/s para gravação

> **Especificações de potência**
6,4 W (típico) Ativa / 1,0 W (típico) inativa

> **Tempo Médio entre Falhas** 1.000.000 Horas

NÚMEROS DE PEÇAS KINGSTON

SV100S2/32G	(unidade independente)
SV100S2D/32G	(kit para PC)
KG-S2632	(Sem caixa half-slim)

Produto sem caixa somente disponível sob encomenda especial.

CONTEÚDO DA EMBALAGEM

Kit para PC
- Suporte de 3,5 pol e parafusos de montagem
- Cabo de dados SATA e cabo de energia
- Software de Clonagem de HD[4]
- Guia de Instalação

Este SSD foi projetado para uso em trabalhos realizados em PCs e notebooks e não é destinado a ambientes de Servidor.

1 Windows 7, Windows Server 2008 R2

2 Parte da capacidade mencionada em um dispositivo de armazenamento de memória Flash é utilizada para a formatação e para outras funções, portanto não está disponível para o armazenamento de dados. Isso significa que a capacidade real de armazenamento de dados é inferior à relacionada nos produtos. Para mais informações, acesse o Guia de Memória Flash da Kingston em kingston.com/brasil/flash_memory_guide.

3 A velocidade pode variar de acordo com o hardware do host, do software e da utilização.

4 Sistemas operacionais suportados pelo software: Windows® 7, Windows Vista® (SP2), Windows XP (SP3)

C.3 SANDISK SSD PLUS 120G E 240G

120GB, 240GB, 480GB*

SanDisk® SSD PLUS

Step up to SSD speeds

Performance

- Up to 20X faster than a typical hard disk drive[1]
- Boosts burst write performance, making it ideal for typical PC workloads
- Faster boot-up, shutdown, application load and response[1]

Proven Reliability

- Shock resistant for proven durability[2]—even if you drop your computer
- SanDisk SSD Dashboard monitors drive status and software updates[3]
- Generous battery life

Inject new life into your laptop or desktop PC with a durable solid state drive from SanDisk. You'll experience quicker boot-up and shutdown, quicker application response and data transfer speeds than with a typical hard disk drive[1], at just a fraction of the cost of a new computer. SLC caching boosts burst write performance, making it ideal for typical PC workloads such as web browsing, email, casual gaming, office productivity, and audio/video entertainment. Plus a solid state drive doesn't overheat, make noise or burn through battery. SanDisk® SSDs are resistant to shock, vibration and temperature extremes[2], so your SSD keeps working, no matter where or how hard you use your computer.

SanDisk®

SanDisk® SSD PLUS Specifications	
Available capacities:	120GB, 240GB, 480GB*
Dimensions:	2.75 x 3.96 x 0.28 in. (69.95 x 100.50 x 7.00 mm)
Interface:	SATA Revision 3.0 (6 Gbit/s)
Operating temperature:	0°C to 70°C
Shock:	Resistant up to 1,500 G @ 0.5m/sec
Vibration (Operating/Non operating):	5 gRMS, 10 – 2000 Hz / 4.9 gRMS, 7 – 800 Hz
Warranty:	3-year limited warranty (U.S.); 3-year warranty (ROW)

SanDisk® SSD PLUS	120GB	240GB	480GB
Performance			
Sequential Read (up to)	530MB/s**	530MB/s	535MB/s
Sequential Write (up to)	400MB/s	440MB/s	445MB/s

SKU	Part Number	UPC	MC UPC
SDSSDA-120G-G26	80-56-15592-120G	619659146689	40619659146687
SDSSDA-240G-G26	80-56-15592-240G	619659146726	40619659146724
SDSSDA-480G-G26	80-56-15592-480G	619659146757	40619659146755
SDSSDA-120G-Q25	80-56-15596-120G	619659125363	40619659125361
SDSSDA-240G-Q25	80-56-15596-240G	619659125400	40619659125408
SDSSDA-480G-Q25	80-56-15596-480G	619659141493	40619659141491
SDSSDA-120G-Z26	80-56-15598-120G	619659125370	40619659125378
SDSSDA-240G-Z26	80-56-15598-240G	619659125417	40619659125415
SDSSDA-480G-Z26	80-56-15598-480G	619659141509	40619659141507

For more information, please visit
www.sandisk.com

SanDisk®

At SanDisk, we're expanding the possibilities of data storage. For more than 25 years, SanDisk's ideas have helped transform the industry, delivering next generation storage solutions for consumers and businesses around the globe.

SanDisk Corporation, Corporate Headquarters
951 SanDisk Drive | Milpitas | CA 95035 | USA

SanDisk International
The Concourse Building | Airside Business Park
Swords | County Dublin | Ireland

* 1GB = 1,000,000,000 bytes. Actual user storage less.
** Based on internal testing; performance may vary depending upon drive capacity, host device, OS and application. 1MB = 1,000,000 bytes.
[1] As compared to 7200 RPM SATA 2.5" hard drive. Based on published specifications and internal benchmarking tests using PCMark Vantage scores.
[2] Shock resistant (up to 1500G) and vibration resistant (5gRMS, 10-2000 HZ/4.9 gRMS, 7-800 HZ), temperature (from 0°C to 70°).
[3] Download required from http://www.sandisk.com/ssdswap/download. Limit one time use per system.

C.4 SSD SANDISK - U100 32G

SanDisk® U100 SSD (Solid State Drive)

Introducing Serial-ATA (SATA) Performance, Low Power, Form Factor Miniaturization and Cost Efficient Storage Solution.

SanDisk® U100 SSD Benefits:

- High SATA 6 Gb/s performance: Up to 450/350 MB/s[4] Read/Write Sequential
- Supports form factor innovation: Half-Slim SATA, mSATA, mSATA mini, 2.5" Cased
- Low slumber mode power consumption: 10mW[5]
- Competitive Pricing
- Wide capacity offering: 8 GB - 256 GB[2]
- Improves user experience:
  - Fast boot and applications launch time
  - Speedy browsing, emailing and social usage capabilities
  - Enhanced multi tasking capabilities
- Based on SATA signaling and JEDEC standard package: grounded in the industry's most mature storage ecosystem

The SanDisk® U100 SSD delivers high SATA 6 Gb/s performance at a competitive cost. It is conveniently offered in a variety of light weight and small form factors, making it the natural fit for a variety of thin and mobile computing platforms such as ultra-thin notebooks and high end tablets.

A bundle of benefits. Affordable cost

OEMs are now looking for a storage solution that meets thin form factor requirements, supports diverse feature sets and also satisfies performance and power requirements, while maintaining an affordable cost profile.

SanDisk U100 SSD meets challenging OEM size requirements, while delivering fast sequential/random performance and solid long-term data endurance[1] that is also cost effective. It is rugged and reliable; light weight and delivers silent operation.

SanDisk U100 SSD's unique power management features enable OEMs to optimize battery life while still meeting demanding performance requirements evolving in the market. Take advantage of SSD performance while avoiding the power penalty typically associated with SATA performance. Factor in SanDisk U100 SSD's wide range of capacities (8 GB - 256 GB[2]) and competitive pricing and it makes an ideal storage choice for a variety of thin and mobile computing platforms.

SanDisk® U100 SSD Supported by Key Innovations and Technology Leadership

nCache™ Acceleration Technology[3]: At the heart of SanDisk's Adaptive Flash Management (AFM), there is a large non-volatile SLC write cache technology that enables fast user response, no stuttering, better multi tasking capabilities and significantly improves the drive's long-term data endurance, ensuring an enhanced user experience.

Power Classes: Power budgets are paramount in mobile computing applications. U100 SSD supports Power Classes, which provide the ability to limit SSD performance and in turn, limit power consumption. This allows for optimized flexibility between power and performance enabling, OEMs to take

Contact information

USA - OEMinfo@sandisk.com
Japan - OEMsalesjp@sandisk.com
Taiwan - OEMAsia@sandisk.com
China - OEMAsia@sandisk.com
Korea - OEMAsia@sandisk.com
Europe - CSDEMEA@sandisk.com

For more information, please visit www.sandisk.com/ssd

1. Approximations based on an industry metric, introduced by SanDisk, that quantifies how much data can be written to a SSD in its lifespan expressed in terabytes written (TBW). Data is written using typical PC transfer size, written at a constant rate over the life of the SSD and data is retained for at least 1 year upon TBW exhaustion. Based on SanDisk internal measurements, a typical client PC user writes 4 GB/day.
2. 1 gigabyte (GB) = 1 billion bytes. 1 terabyte (TB) = 1 trillion bytes. Some capacity not available for data storage.
3. nCache™ acceleration technology is a large Non Volatile Write Cache, a unique feature in SanDisk SSDs that improves random write performance to ensure an improved user experience. Studies show that modern operating systems mostly access the storage device using 4k access blocks. The cache is filled during these small write commands and emptied during idle time when the host is not accessing the drive, with no risk of data loss. For a typical everyday use, the write performance that the users see is the nCache™ (burst) high performance, and not steady state (sustained) SanDisk U100 SSD performance. Based on IOmeter 4K random write test.
4. Based on SanDisk internal testing; performance may be lower depending upon host device. Technical specifications are preliminary and subject to change.
5. With Slumber (SATA PHY state) power mode and DIPM enabled. Lower power modes can be achieved by implementing advanced low power management techniques. Technical specifications are preliminary and subject to change.
6. MTBF – Mean Time Between Failures based on part stress analysis.
7. Applies to U100 SSD mSATA Mini form factor. 8 GB - 32 GB. Dimensions and weight vary based on form factor and capacity.

SanDisk®

SanDisk Corporation, Corporate Headquarters,
601 McCarthy Boulevard, Milpitas, CA 95035

advantage of numerous SSD benefits even when maximum performance is not required.

Form Factor Miniaturization Leadership: SanDisk SSD U100 is offered in a variety of innovative form factors. Form factors such as Half-Slim SATA, mSATA, mSATA mini and the SATA µSSD™ form factor standard (see SanDisk iSSD™ integrated storage device) as well as a customized form factor option, support an array of design needs making SanDisk U100 SSD an ideal fit for the ultra thin, light weight and highly mobile computing devices.

SanDisk® SSD – A Trusted Partner:

New usage models and innovative mobile computing designs are attracting key players in the ecosystem to SATA and U100 SSD. Ecosystem partners include chipset vendors, OS vendors and box manufacturers (ODMs). This ecosystem enablement leads to OEM adoption. SanDisk is consistently listening to market needs from OEMs, partners, application developers and other relevant ecosystem stakeholders. This ensures that our offerings are optimally aligned to market needs and fast-moving requirements.

Supported by vertical integration and over 20 years of experience in the flash memory business, SanDisk continues to deliver ground breaking solutions that repeatedly revolutionize the world of mobile computing and beyond. SanDisk is a trusted partner that you can always count on to guide you into the future.

SanDisk® U100 SSD product features and specifications Specifications are preliminary and subject to change	
Device	SanDisk U100 SSD
Form Factor	Half-Slim SATA, mSATA, mSATA mini, 2.5" cased
Interface	SATA 6Gb/s
Capacity (GB)[2]	8, 16, 24, 32, 64, 128, 256
Performance[4] Sequential Read/Write Random Write IOPs – sustained: 4K Random Read	 Up to 450 MB/s 350 MB/s 1200 IOPs 9400 IOPs (across 8GB capacity range)
MTBF[6]	Up to 4,000,000 hours
Endurance[1]	5 TBW (8 GB), 10 TBW (16 GB), 15 TBW (24GB) 20 TBW (32 GB), 40 TBW (64 GB), 80 TBW (128 GB), 160 TBW (256 GB)
Size[7]	26.8 mm x 30 mm x 3.4 mm
Weight[7]	3.4 g
Low Power Consumption	
DC Supply	+5.0V, +3.3V ±5%
Slumber Power Mode (Typical)[5]	10mW
Active Power (Typical)	3W (@ 3.3 V)
Environmental Specifications	
Operating Temperatures	0°C to +70°C
Storage Temperatures	-55°C to +85°C
Acoustic Noise	0dB
Other	
Supporting Features	TRIM SMART Commands Advanced Flash Management NCQ
OS Support	Windows® XP, Windows® 7, Google Chrome™ OS
Warranty	Limited 3 year Warranty 3 year Warranty in regions not recognizing limited

APÊNDICE D – *COMANDO WIPE E GERAÇÃO DE CÓPIA FORENSE*

Neste apêndice serão apresentadas a ferramenta *wipe* e a *dc3dd* que foram utilizadas no desenvolvimento do trabalho e, as quais poderão ser utilizadas para que os experimentos sejam reproduzidos e verificados em trabalhos futuros.

D.1 WIPE

O comando de wipe pode ser usado para apagar com segurança arquivos de unidades de armazenamento. O comando de wipe tem a seguinte sintaxe:

wipe [opções] <unidade-alvo>

Fazer o wipe de uma unidade pode apagar dados permanentemente, mas é difícil garantir que os dados das unidades sejam realmente não recuperáveis. Ele é empregado na unidade, para depois haver a escrita dos dados. A Figura 26 mostra como foi utilizado no linux o comando wipe para cada uma das unidades utilizadas nos experimentos do Capítulo 6.

```
Para o Kingston32G:
root@kali:/home/kali# wipe -r -q /dev/sde1


Para o U10032G:
root@kali:/home/kali# wipe -r -q /dev/sdd1


Para o SSD120G:
root@kali:/home/kali# wipe -r -q /dev/sdb1


Para o SSD240G:
root@kali:/home/kali# wipe -r -q /dev/sdc1
```

Figura 26 – Formas de utilização do Wipe durante os experimentos

Segundo a descrição do *wipe(1) - Linux man page* (MAN, 2006), o comando wipe apaga arquivos através da sobrescrita repetida utilizando padrões especiais.

As opções utilizadas na preparação das unidades SSD no início dos experimentos, conforme Figura 26, são:

- "-r" a qual serve recursão em subdiretórios e permitirá a remoção de toda a árvore de diretórios;

- "-q" a qual realiza uma limpeza rápida, quando esta opção é usada, o apagamento só fará (por padrão) 4 passagens em cada arquivo, gravando dados aleatórios.

D.2 DC3DD

O dc3dd foi desenvolvido no *Cyber Crime Center* do *Departement of Defense* e é uma versão aperfeiçoada do "dd", com recursos adicionais para forense computacional. O dc3dd oferece a possibilidade de gerar um código *hash* junto com a geração da imagem, para tanto pode empregar diversos algoritmos (MD5, SHA-1, SHA-256 e SHA-512).

O dc3dd foi empregado para gerar imagens da unidade e o *hash* criptográfico da imagem. Um exemplo de linha de comando utilizada é:

dc3dd if=/dev/sdb1 of=/home/kali/Downloads/SSDtest1/SSD120G_dc3ddPOS60.dd hash=sha256 log=/home/kali/Downloads/SSDtest1/SSD120Gsha256POS60.log

Os parâmetros utilizados estão resumidos na Tabela 6.

Tabela 6 – Parâmetros usados do dc3dd

Parâmetros	Uso
if	arquivo de entrada
/dev/sdb1	drive de origem
of	arquivo de saída (imagem ".dd")
hash	algoritmo de hash
log	caminho e nome do arquivo ".log"

A imagem gerada a partir da unidade é indicada logo após o "of=" e também encontrará o arquivo de log (que contém a saída em execução) no caminho que é indicado a direita do parâmetro "log=". No arquivo de "log" também aparecerá o *hash* calculado da imagem.

Durante o decorrer dos experimentos diversas imagens, bem como seus respectivos *hashes* foram gerados. Como recomendam as boas práticas forenses, o exame e a análise foram feitos sobre as imagens geradas e sobre seus respectivos *hashes*.

As linhas de comando utilizadas para gerar as cópias forenses ao longo do tempo, para as diferentes unidades, são variações dos seguintes comandos:

U100 32G

dc3dd if=/dev/sdd1 of=/home/kali/Downloads/SSDtest1/U10032G_dc3dd.dd hash=sha256 log=/home/kali/Downloads/SSDtest1/U10032Gsha256.log

SSD 120GB

ddc3dd if=/dev/sdb1 of=/home/kali/Downloads/SSDtest1/SSD120G_dc3dd.dd hash=sha256 log=/home/kali/Downloads/SSDtest1/SSD120Gsha256.log

SSD 240G

dc3dd if=/dev/sdc1 of=/home/kali/Downloads/SSDtest1/SSD240G_dc3dd.dd hash=sha256 log=/home/kali/Downloads/SSDtest1/SSD240Gsha256.log

Kingston 32GB

dc3dd if=/dev/sde1 of=/home/kali/Downloads/SSDtest1/Kingston32G_dc3dd.dd hash=sha256 log=/home/kali/Downloads/SSDtest1/Kingston32Gsha256.log

APÊNDICE E – *RECUPERAÇÃO COM O NTFSUNDELETE*

E.1 VERSÃO

Versão 2016.2.22AR.1.

E.2 EXECUÇÃO

A sintaxe para execução do NTFSUNDELETE pode ser feita através do comando:

ntfsundelete [options] [dispositivo|image.dd]

Ao se utilizar o NTFSUNDELETE, buscou-se a verificação dos arquivos que poderiam ser recuperados, para isso utilizou-se a opção "-s" (scan).

Scan permite a busca através de um volume NTFS e impressão de uma lista de arquivos que podem ser recuperados. Esta lista pode empregar ainda vários filtros e a saída possui as informações: Inode, Flags, %age, Date, Size e Filename.

A descrição das Flags está na Tabela 7.

Tabela 7 – Flags do ntfsundelete

Flags	Descrição
F / D	Arquivo / Diretório
N / R	Fluxo de Dados (Não-)Residente
C / E	Fluxo de Dados Comprimido /Encriptado
!	Atributos ausentes

O parâmetro %age é um campo que mostra quanto do arquivo pode ser recuperado, é um valor numérico seguido pelo símbolo "%". Mais detalhes sobre as opções e parâmetros utilizados podem ser encontrados na *Linux man page* (MAN, 2018).

E.3 RESULTADOS DE RECUPERAÇÃO

E.3.1 U100 32G

E.3.1.1 Após TRIM

Apenas os arquivos file.txt e file16.txt podem ser completamente recuperados, conforme mostrado na Figura 27.

E.3.1.2 Após Formatação

Após a formatação, todas as informações do *filesystem* acabam sendo alteradas, os inodes, metadados de arquivos acabam não sendo mais recuperados através do comando ntfsundelete, conforme mostrado na Figura 28.

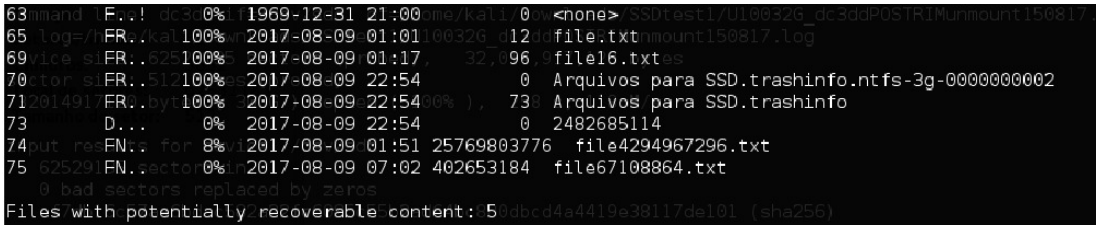


Figura 27 – Arquivos de texto que podem ser recuperados no SSD U100 de 32G

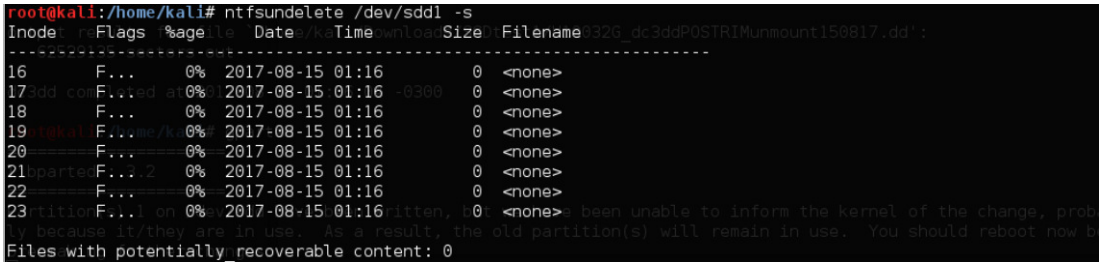


Figura 28 – SSD SanDisk U100 32G após formatação

E.3.2 Kingston 32G

E.3.2.1 Após TRIM

De forma similar ao que ocorreu com o SSD Sandisk U100 32G, apenas os arquivos file.txt e file16.txt podem ser completamente recuperados, conforme mostrado na Figura 29.

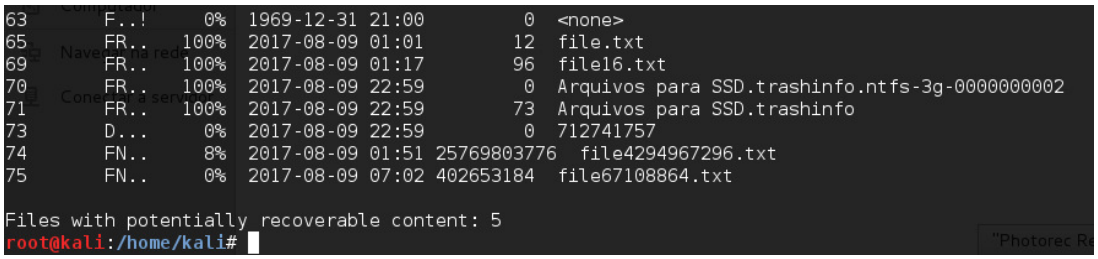


Figura 29 – Arquivos de texto que podem ser recuperados no SSD Kingston 32G

E.3.2.2 Após Formatação

Após a formatação, inodes, metadados de arquivos não são recuperados através do comando ntfsundelete, conforme mostrado na Figura 30.

E.3.3 SSD 120G

E.3.3.1 Após TRIM

Os arquivos file.txt, file16.txt, file65536.txt e file67108864.txt podem ser completamente recuperados, conforme mostrado na Figura 31.

```
root@kali:/home/kali# ntfsundelete -s /dev/sde1
Inode     Flags  %age      Date     Time        Size  Filename
-----------------------------------------------------------------------
16        F...      0%  2017-08-18 21:46          0  <none>
17        F...      0%  2017-08-18 21:46          0  <none>
18        F...      0%  2017-08-18 21:46          0  <none>
19        F...      0%  2017-08-18 21:46          0  <none>
20        F...      0%  2017-08-18 21:46          0  <none>
21        F...      0%  2017-08-18 21:46          0  <none>
22        F...      0%  2017-08-18 21:46          0  <none>
23        F...      0%  2017-08-18 21:46          0  <none>

Files with potentially recoverable content: 0
root@kali:/home/kali#
```

Figura 30 – SSD Kingston 32G após formatação

```
63        F..!      0%  1969-12-31 21:00          0  <none>
65        FN..      0%  2017-08-09 01:51 25769803776  file4294967296.txt
66        FN..    100%  2017-08-09 07:02 402653184  file67108864.txt
67        FN..    100%  2017-08-09 01:18  12582912  file65536.txt
68        FR..    100%  2017-08-09 01:01        12  file.txt
69        FR..    100%  2017-08-09 01:17        96  file16.txt
74        FR..    100%  2017-08-09 23:00        73  Arquivos para SSD.trashinfo

Files with potentially recoverable content: 5
root@kali:/home/kali#
```

Figura 31 – Arquivos de texto que podem ser recuperados no SSD de 120G

E.3.3.2 Após Formatação

Após a formatação, inodes, metadados de arquivos não são recuperados através do comando ntfsundelete, conforme mostrado na Figura 32.

```
root@kali:/home/kali# ntfsundelete /dev/sdb1 -sInode     Flags  %age     Date     Time        Size  Filename
-----------------------------------------------------------------------
16        F...      0%  2017-08-18 21:34          0  <none>
17        F...      0%  2017-08-18 21:34          0  <none>
18        F...      0%  2017-08-18 21:34          0  <none>
19        F...      0%  2017-08-18 21:34          0  <none>
20        F...      0%  2017-08-18 21:34          0  <none>
21        F...      0%  2017-08-18 21:34          0  <none>
22        F...      0%  2017-08-18 21:34          0  <none>
23        F...      0%  2017-08-18 21:34          0  <none>

Files with potentially recoverable content: 0
root@kali:/home/kali#
```

Figura 32 – SSD Kingston 120G após formatação

E.3.4 SSD 240G

E.3.4.1 Após TRIM

Os arquivos file.txt, file16.txt podem ser completamente recuperados, enquanto file4294967296 pode ser, em parte, recuperado, conforme mostrado na Figura 33.

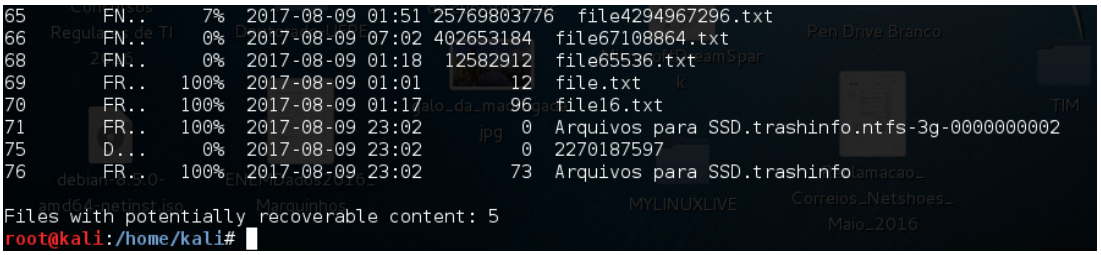


Figura 33 – Arquivos de texto que podem ser recuperados no SSD de 240G

E.3.4.2 Após Formatação

Após a formatação, inodes, metadados de arquivos não são recuperados através do comando ntfsundelete, conforme mostrado na Figura 34.

Portanto, com o ntfsundelete nenhum dos arquivos é recuperado, mas há a possibilidade de recuperação de dados por meio de ferramentas de carving, com a desvantagem de não se conseguir recuperar os metadados e, por vezes, esses arquivos serem recuperados de forma fragmentada.

Figura 34 – SSD Kingston 240G após formatação

APÊNDICE F – *RECUPERAÇÃO COM FERRAMENTAS DE CARVING*

Ao se utilizar o NTFSUNDELETE, após a formatação da unidade, a recuperação de inodes, metadados de arquivos já não é mais possível. Porém, há ferramentas que utilizam outras técnicas para recuperar arquivos, são as ferramentas de *carving*, as quais podem utilizar-se de técnicas baseadas em cabeçalho/rodapé (ou cabeçalho/tamanho máximo), estrutura de arquivos e em blocos de conteúdo, conforme mencionado no item 6.1.3.1 com base no trabalho de Laurenson (LAURENSON, 2013).

Sem adentrar na especificidade de cada ferramenta, porque essa não é a proposta da pesquisa, consegue-se demonstrar que ainda é possível recuperar dados de unidades SSD em que houve disparo do TRIM, mesmo que essas unidades tenham sido formatadas. Algumas das ferramentas de *carving* utilizadas, comandos utilizados para execução, bem como resultados das recuperações de dados de diferentes tipos (os tipos de arquivos utilizados foram detalhados no Apêndice B).

F.1 PHOTOREC

O PhotoRec é um software de recuperação de dados projetado para recuperar arquivos perdidos ou apagados, incluindo vídeo, documentos e arquivos de diversas mídias de armazenamento. O PhotoRec ignora o sistema de arquivos e busca os dados, de modo que funcionará mesmo que o sistema de arquivos da mídia tenha sido seriamente danificado ou reformatado (CGSECURITY, 2015).

O PhotoRec é gratuito - aplicativo multiplataforma de código aberto e distribuído sob a Licença Pública Geral GNU (GPLV v2 +).

PhotoRec usa acesso somente de leitura para manipular a unidade da qual se deseja recuperar dados perdidos.

Em duas pesquisas realizadas pelo programa *Computer Forensics Tool Testing* (CFTT [1].) o PhotoRec foi bem-sucedido ao recuperar e reconstruir arquivos gif, bmp, png, jpg e tiff na maioria dos casos de teste, também foi capaz de recuperar arquivos de vídeo (por exemplo, mp4, mov, avi, wmv, 3gp e ogv) (US, 2014a) (US, 2014b).

F.1.1 Versão

Versão 1.5 (abril 2015).

[1] CFTT é um projeto formado por diversas organizações norte-americanas, tais como o *Department of Homeland Security* (DHS), o *National Institute of Justice* (NIJ), o *National Institute of Standards - Technology Law Enforcement Standards Office* (NIST OLES) e o *National Institute of Standards - Information Technology Laboratory* (NIST ITL). A iniciativa conta ainda com a participação do *Federal Bureau of Investigation*, e do *U.S. Department of Defense Cyber Crime Center*. O objetivo do programa CFTT é fornecer medidas, para pesquisadores e comunidade em geral, a cerca das ferramentas utilizadas em investigações forense computacionais

F.1.2 Execução

A sintaxe para execução do PhotoRec nas versões voltadas para o Linux podem ser feitas através do comando:

photorec [/log] [/debug] [/d recup_dir] [dispositivo|image.dd|image.e01]

Mais detalhes sobre as opções e parâmetros utilizados podem ser encontrados na *Linux man page* (MAN, 2015) ou mesmo na página Web do desenvolvedor (CGSECURITY, 2015).

F.1.3 Resultados de recuperação

O PhotoRec conseguiu recuperar diversos arquivos e fragmentos de arquivos, a partir das imagens "dd" geradas das unidades SSD.

Na Figura 35 podem ser vistos arquivos de texto que foram recuperados durante experimentos realizados com essa ferramenta baseada em *carving*.

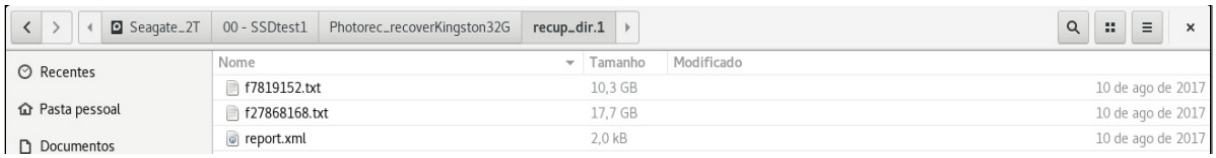


Figura 35 – Arquivos de texto que podem ser recuperados com PhotoRec na unidade Kingston de 32GB

Na Figura 36 podem ser vistas pastas que contém arquivos e fragmentos de arquivos recuperados durante o experimento 3 (conforme descrito em 6.1.3.4) realizados com a ferramenta baseada em *carving*.

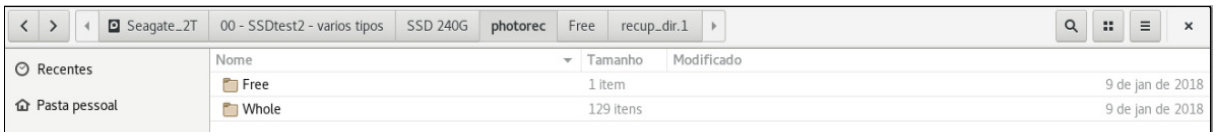


Figura 36 – Pastas contendo arquivos de vários formatos que podem ser recuperados no SSD de 240G

F.2 SCALPEL

Scalpel é um programa *open source* para recuperação de dados, compartilha parte do código do oftware *foremost*, mas implementa um método mais rápido e eficiente.

Recupera arquivos a partir de imagens de disco ou dispositivos de armazenamento, a recuperação é realizada com base em uma base de dados contendo cabeçalhos e rodapés (PALMIERI; ZARGARI, 2017).

Antes da execução da sintaxe do Scalpel há um arquivo de configuração "scalpel.conf" que está incluído na distribuição e que permite ao usuário especificar os tipos de arquivos que o Scalpel tentará recuperar.

F.2.1 Versão

Versão 1.6 (dezembro de 2006, baseada no foremost 0.69).

F.2.2 Execução

A sintaxe para execução do Scalpel podem ser feitas através do comando:

scalpel [-b] [-c <config file>] [-d] [-e] [-h] [-i <file>] [-n] [-o <dir>] [-O] [-p] [-q <clustersize>] [-r] [-V] [-v] [FILES]...

Mais detalhes sobre as opções e parâmetros utilizados podem ser encontrados na *Linux man page* (MAN, 2013).

F.2.3 Resultados de recuperação

O Scalpel conseguiu recuperar diversos arquivos e fragmentos de arquivos, a partir das imagens "dd" geradas das unidades SSD.

Na Figura 37 podem ser vistas pastas contendo arquivos de diversos tipos que foram recuperados durante experimentos realizados com essa ferramenta baseada em *carving* na unidade SSD de 120 GB e na Figura 38 podem ser vistas pastas contendo arquivos de diversos tipos que foram recuperados durante experimentos na unidade SSD U100 de 32GB.

Nas duas figuras (Figura 37 e 38) podem ser vistas pastas que contém arquivos e fragmentos de arquivos recuperados durante o experimento 3 (conforme descrito em 6.1.3.4), nesses casos mostrados a ferramenta empregada foi Scalpel.

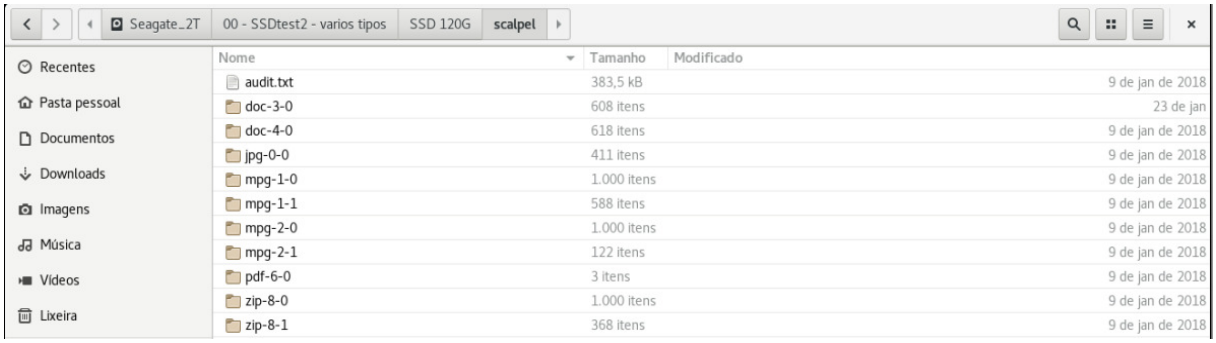


Figura 37 – Pastas de arquivos recuperados com Scalpel na unidade SSD de 120GB

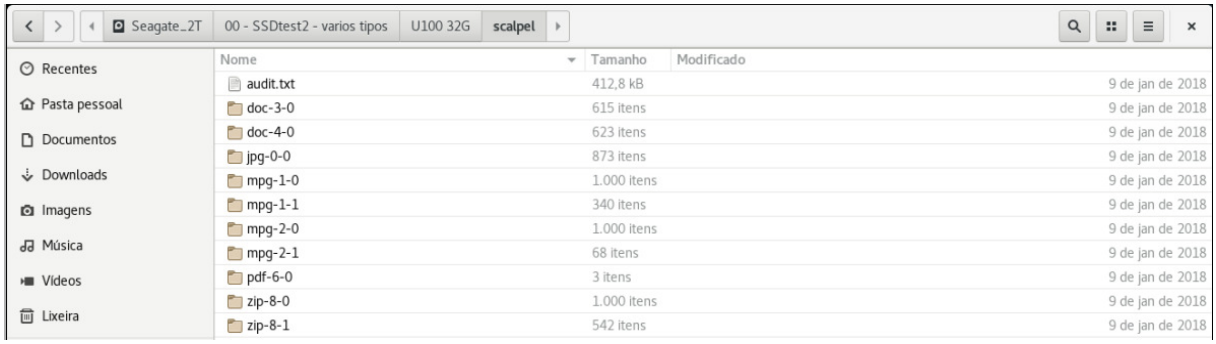


Figura 38 – Pastas de arquivos recuperados com Scalpel na unidade SSD de U100 32GB

F.3 RECOVERJPEG

O Recoverjpeg é um software de recuperação de dados projetado para recuperar arquivos de imagem no formato JPEG, que tenham sido apagados acidental ou intencionalmente. Para recuperação dos arquivos, o software procura por estruturas de um arquivo jpeg em dispositivos ou em arquivos que contenham imagens do dispositivo, exemplo imagens "dd".

Por padrão a recuperação é iniciada pela procura de estruturas jpeg em blocos iniciais de 512 bytes, porém esse valor pode ser alterado por meio do parâmetro "-B".

O Recoverjpeg é Open Source e foi desenvolvido por Samuel Tardieu.

Recoverjpeg é limitado quando comparado com outras ferramentas de *carving*, no entanto é muito eficiente e leve (PALMIERI; ZARGARI, 2017).

F.3.1 Versão

Versão 2.6 (novembro 2016).

F.3.2 Execução

A sintaxe para execução do Recoverjpeg é:

recoverjpeg [options] file|device

Mais detalhes sobre as opções e parâmetros utilizados podem ser encontrados na *Ubuntu Manpage Repository* (UBUNTU, 2018).

F.3.3 Resultados de recuperação

No resultado mostrado na Figura 39 é possível visualizar que foram recuperados 227 arquivos jpeg ou fragmentos de arquivos.

No resultado da Figura 39 é possível visualizar que foram recuperados 766 arquivos jpeg ou fragmentos de arquivos.

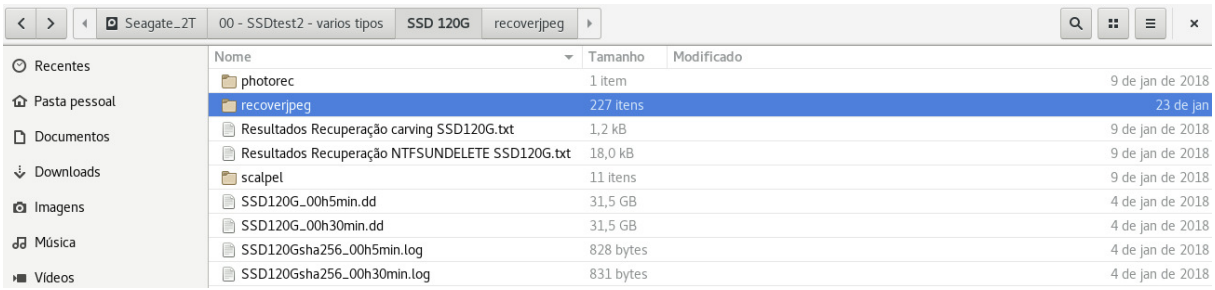


Figura 39 – Pastas de arquivos recuperados com Recoverjpeg na unidade SSD de 120GB

Não há garantias de que os arquivos recuperados estejam íntegros, mas o resultado demonstra a capacidade de recuperação de dados a partir de unidades SSD com o recoverjpeg.

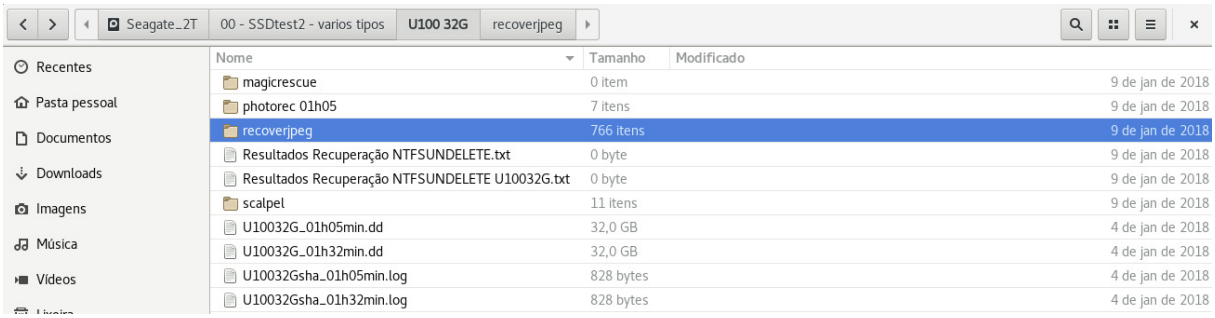


Figura 40 – Pastas de arquivos recuperados com Recoverjpeg na unidade SSD de U100 32GB

F.4 MAGIC RESCUE

O Magic Rescue é um software de *carving*, ou seja, pode buscar dados com sucesso independentemente do *filesystem*. Seu funcionamento consiste em acessar dispositivos e verificar no conteúdo dos dados a presença de "magic bytes".

O Magic Rescue, segundo afirmação na própria descrição da *man page* (UBUNTU, 2016), é muitas vezes utilizado em adição a outras ferramentas, pois a combinação de várias ferramentas que não são mutuamente excludentes costuma apresentar bons resultados.

F.4.1 Versão

Versão 1.1.9 (outubro 2008).

F.4.2 Execução

A sintaxe para execução do Magic Rescue é:

magicrescue [-I FILE] [-M MODE] [-O [+-=][0x]OFFSET] [-b BLOCKSIZE] -d OUTPUT_DIR -r RECIPE1 [-r RECIPE2 [...]] DEVICE1 [DEVICE2 [...]]

Mais detalhes sobre as opções e parâmetros utilizados podem ser encontrados na *Ubuntu Manpage Repository* (UBUNTU, 2016).

F.4.3 Resultados de recuperação

A busca por arquivos do tipo ".txt" não trouxe resultados significativos, mas houve recuperação de arquivos, conforme demonstram a Figura 41 (recuperação de 1 arquivo do tipo ".txt" da unidade Kingston 32GB) e a Figura 42 (recuperação de 2 arquivos do tipo ".txt" da unidade SSD 240 GB).

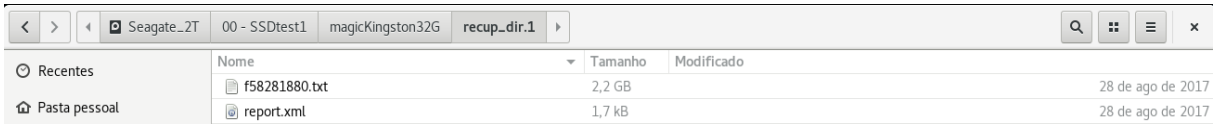


Figura 41 – Arquivos de texto recuperados com Magic Rescue na unidade Kingston de 32GB

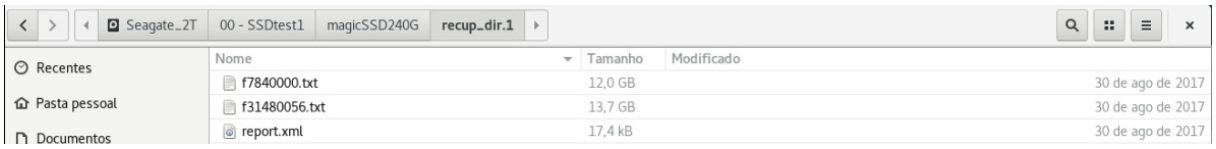


Figura 42 – Arquivos de texto recuperados com Magic Rescue na unidade SSD de 240GB

Na busca por arquivos de vários tipos distintos foram enumerados 34730 arquivos ou fragmentos de arquivos na pasta de saída (magicrescue), conforme Figura 43.

Um quantitativo de 34730 arquivos ou fragmentos de arquivos é significativo, mas é necessária uma depuração para que a utilidade desses arquivos para uma investigação possa ser adequadamente avaliada.

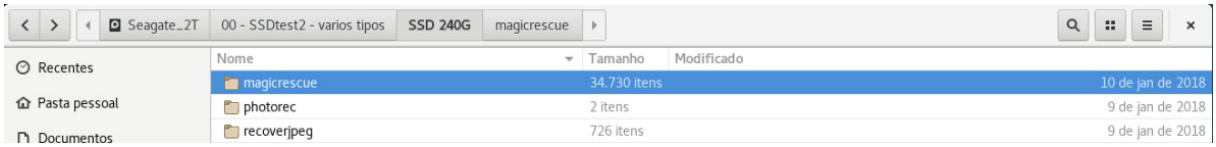


Figura 43 – Pastas de arquivos recuperados com Magic Rescue na unidade SSD de 240GB