AS DIFICULDADES DA FORENSE COMPUTACIONAL EM DISCOS DE ESTADO SOLIDO, SEUS DESAFIOS E PERSPECTIVAS

Pedro Fabrício Ubaldo

Resumo: Nos últimos anos, os discos de estado sólido se desenvolveram drasticamente e agora estão aumentando a popularidade em comparação com os discos rígidos convencionais. Enquanto as unidades de disco rígido funcionam previsivelmente, o método de trabalho dos SSD funcionam em segundo plano sem o conhecimento do usuário. Este artigo apresenta uma análise conceitual da usabilidade e da eficácia de técnicas usuais de recuperação de dados e de forense digital nos dispositivos de SSD - disco de estado sólido utilizando as ferramentas usuais de recuperação de dados juntamente colocando de modo geral os desafios que esta tecnologia traz para a forense digital nos dias de hoje.

Palavras-chave: SSD, Forense Digital, Sistema de Arquivos, Sistemas Operacionais

1 INTRODUÇÃO

Do mesmo modo como na esfera criminal, a tecnologia cada dia mais está presente nas interações sociais, onde os sistemas de computadores são usados para cometer ou mediar crimes. Diante disto, surge a atuação da Forense Digital, que é o processo de identificação, preservação, análise e apresentação de evidências digitais legalmente aceitável.

O objetivo da Forense Digital é realizar uma investigação estruturada, mantendo uma cadeia documentada de evidências para descobrir exatamente o que aconteceu em um dispositivo de computação e quem foi responsável por ele.

Diante do atual cenário mundial, os discos de estado sólido estão conquistando cada vez mais o seu espaço no mercado em relação aos discos rígidos. Tudo isso devido a, de um tempo para cá, sua redução de custo, aumento significativo na velocidade de leitura e escrita, baixo consumo de energia, e outras diversas características positivas.

Mas, SSD (*Solid-State Drive*) não é uma evolução da tecnologia de disco rígido, é uma tecnologia completamente nova bem diferente do comportamento de um disco

rígido. Existem grandes diferenças subjacentes que tem consequências graves para a segurança e para a forense digital.

Devido ao modo como os SSDs funcionam, nem sempre é certo que os dados excluídos sejam apagados do disco. Por outro lado, os SSDs, por vezes, podem limpar os dados por si mesmos, mesmo que eles não estejam conectados a qualquer interface, estando apenas ligados.

Em vez de previsível e da alta probabilidade de recuperação de informações como é atualmente nos discos rígidos, não podemos mais supor se e quanto dados podem ser recuperado com essa nova tecnologia.

Isso significa que as diretrizes normais destinadas a discos rígidos sobre como preservar a evidencia forense digital não são apenas inadequadas, mas poderiam, se seguidas, resultar em perda potencial, perdido ou considerado invalido como evidência.

Em virtude de quaisquer modificações no cenário da informática, a forense computacional necessita estar sempre pareada com o surgimento de novas tecnologias buscando entender e desenvolver métodos que permitam a mesma manipular novas formas de evidências eletrônicas.

A partir de pesquisas realizadas e de um referencial teórico é apresentada a tecnologia SSD e as diferenças entre ela e sua antecessora, os HDs (*Hard Drives*). Destaca-se também sobre forense computacional em discos de estado sólido, assim como a influência de seus mecanismos internos para a forense digital dessas mídias. Por fim descreve-se quais são os maiores desafios enfrentados pela forense digital quando se refere as investigações nos discos de estado solido, juntamente com uma visão do que se espera para o futuro diante de tal tecnologia.

2 MÍDIAS DE ARMAZENAMENTO

Uma mídia de armazenamento pode ser definida como um meio digital no qual dados são armazenados e operacionados. Cada tipo de mídia de armazenamento possui especificidades quanto aos aspectos citados anteriormente, como gerência de espaço e consistência dos dados, e por sua vez demandará o uso de um Sistema de Arquivos com certas características.

2.1 A arquitetura flash e discos rígidos:

Existe uma grande diferença na arquitetura entre as duas tecnologias de memória flash e discos rígidos. Enquanto os discos rígidos guardam dados em discos giratórios na forma de áreas

magnetizadas, uma memória flash não consiste em partes móveis, o que traz múltiplas vantagens em consumos de energia, velocidades de leitura e gravação e robustez.

2.1.2 A arquitetura das unidades de disco rígido:

As unidades de disco rígido convencionais armazenam dados em discos giratórios feitos de alumínio ou vidro, cobertos com um material magnético fino. Esses discos giram devido a um motor que é montado em um eixo através de um furo no centro do disco e, dependendo da aplicação, a velocidade varia entre 6.000 e 10.000 rotações por minuto. Nos computadores de mesa, as velocidades de 7.200 rpm são padrão, enquanto em aplicações de alto desempenho, 10.000 rpm são mais comuns. Fornecedores diferentes usam quantidades diferentes desses discos em cima uns dos outros para multiplicar o espaço de armazenamento (Mamum, 2007).

A menor unidade de informações gravadas em mídia magnética é de um *bit*. Esses *bits* são dispostos em formas circulares em trilhas ou faixas ao redor do disco. Um típico disco rígido contém 70.000 a 100.000 faixas em cada superfície.

Antes que os dados possam ser armazenados em um disco por um sistema operacional, o disco deve ser formatado e uma partição deve ser criada. Uma partição é uma unidade lógica que divide o disco em diferentes partes lógicas. No *Master Boot Record* (MBR), uma tabela de partição é armazenada no primeiro setor no disco, informando ao sistema operacional como o disco está dividido. Sistemas operacionais como *Linux*, *Windows* ou *Macintosh* colocam sistemas de arquivos diferentes nas partições. Enquanto o *Windows* usa FAT e NTFS, *Linux* usa EXT2 ou EXT3. Um sistema de arquivos acompanha a localização no disco físico de que os dados são armazenados. O *Windows* usa a tabela de arquivos mestre como um índice para os arquivos que ele armazena em discos rígidos. Contrariamente à crença popular, excluir uma partição ou reformatar não afeta os dados reais. Ele simplesmente exclui a tabela de alocação de arquivos (FAT) e os dados ainda podem ser recuperados (Casey, 2011).

2.1.3 A arquitetura da memoria flash

O que torna a memória flash mais rápida, mais eficiente em termos de energia e mais resistente a choque é a falta de peças móveis. Não há discos giratórios ou cabeças móveis lendo e gravando em um disco. Os dispositivos de memória flash são sistemas pequenos completos em que cada componente é soldado a uma placa de circuito impresso. As memórias de semicondutores (memórias de flash) podem ser divididas em duas categorias principais: RAM (memória de acesso aleatório) e ROM (somente leitura de memória). Os dados sobre a memória ROM só podem ser escritos e as informações serão armazenadas praticamente para sempre,

enquanto a memória RAM é regravável e perde suas informações assim que o dispositivo perder energia. Na década de 1970, as primeiras memórias não voláteis (MNV) foram inventadas. As informações armazenadas em MNVs podem ser alteradas, mas também são preservadas após a desligação. No início da década de 1990, os primeiros MNVs encontraram aplicação em memórias flash usadas para unidades USB e cartões de memória flash. Existem dois tipos diferentes de memórias flash: NAND e NOR.

2.2 Memoria flash NAND

Memórias flash como cartões SD, unidades USB e SSDs são baseadas na memória NAND; Suas células são baseadas na tecnologia *Floating Gate* (FG), como a memória NOR, embora os *chips* NAND sejam menores e mais rápidos, eles custam cerca de 60% do preço de um *chip* equivalente NOR para produzir. O aspecto negativo é que nem cada célula pode ser escrita e excluída de forma independente, mas precisa ser gerenciada em matrizes de *bytes*, setores e blocos, enquanto os *chips* NOR manipulam cada célula de forma independente (Changyi , 2016)

Uma célula NAND, é construída com dois *gates* sobrepostos, um completamente rodeado por óxido e outro formando o *floating gate*. Se a tensão é aplicada ao *floating gate*, os elétrons podem passar da fonte através dos dielétricos e se instalar no *floating gate*. Aqui estão presos e podem permanecer preservados por décadas. Isso altera a carga da célula de neutro para negativo e é chamado de programação. Somente se a tensão for aplicada ao dreno, os elétrons passarão do FG e retornarão a célula para o ponto morto. Cada célula continha um *bit* de informação (célula de nível único, CNU) até que as células de múltiplas camadas (CMC) fossem inventadas, que contêm dois ou mais *bits*. Uma *array* geralmente contém 8192 blocos, onde um bloco consiste em 64 páginas (4000 + 128 Bytes) (Figura 1). Na memória NAND, uma operação de gravação pode ser feita no nível da página, mas devido a limitações de *hardware*, os comandos de apagar sempre afetam blocos inteiros.

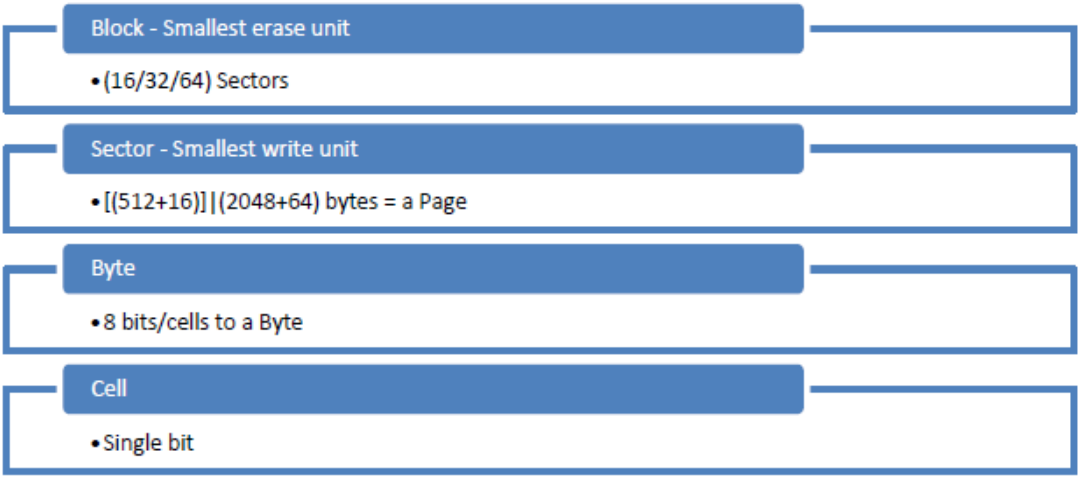

Figura 1. Disposição do dispositivo serial NAND

2.2.1 Controlador de memória de uma unidade de memória flash

O controlador de memória da memória flash tem duas tarefas fundamentais; Ele fornece a interface entre o disco e o *host* e lida com os dados no disco. O controlador aqui traduz e acompanha o LBA (*logical block address*) e os endereços físicos dos dados na memória. Esta tarefa é semelhante à tarefa do controlador em um HD. Embora o controlador em HDs tenha apenas uma pequena funcionalidade adicional, como S.M.A.R.T. (*Self-Monitoring, Analysis, and Reporting Technology* - Tecnologia de Auto Monitoramento, Análise e Relatório) e manipulação do setor ruim, os controladores de flash possuem alguns recursos adicionais significativos. Essas funcionalidades são incorporadas no *Flash File System* (FFS), o sistema de arquivos que permite o uso de SSDs como unidades convencionais. Ambas as funcionalidades dependem completamente do fabricante. Cada fabricante segue uma abordagem diferente e nenhum padrão já foi criado. As duas funções mais importantes são o nivelamento do desgaste e a coleta de lixo.

2.2.2 Controlador de memória SSD

Embora existam mais de 100 vendedores que oferecem unidades SSD, existem apenas poucos fabricantes de controladores SSD (Maleval, 2011). Normalmente, os fornecedores de SSD estão comprando controladores de outras empresas e combinam seus próprios ou outros *chips* de memória NAND com eles. Portanto, alguns fornecedores ganharam uma enorme quota de mercado. O maior produtor de controlador de memória SSD é SandForce, que era um produtor americano de controladores de memória SSD, mais tarde comprado pela LSI, Avago e Seagate

em 2014 (Vatto, 2014). Uma vez que existem apenas algumas empresas produtoras de controladores, a concorrência entre os fabricantes é realmente forte. As rotinas internas de um controlador de memória, a implementação de nivelamento de desgaste e coleta de lixo, compressão e criptografia é o que diferencia um SSD de outro e influenciam diretamente as velocidades de leitura e gravação das unidades.

2.3 TRIM

Uma função importante dos SSDs e que não existe em HDs é o comando TRIM. TRIM é um atributo do comando de gerenciamento de conjunto ATA e permite que o sistema operacional informe o SSD de blocos excluídos. Ele dirá ao dispositivo quais blocos são seguros para remover. Uma vez que a função é habilitada por padrão em sistemas operacionais que suportam TRIM, nenhuma ação é necessária, exceto para desabilitar propositadamente o TRIM para fins de teste.

2.4 Evidência Digital

A evidência digital é definida por Eoghan Casey como "qualquer dado armazenado ou transmitido usando um computador que suporte ou refute uma teoria de como uma ofensa ocorreu desse endereço elementos críticos da ofensa, como a internet do álibi"(Casey, 2011). Digital é um dado que pode estabelecer uma ligação entre um crime e uma vítima ou um suspeito ou pode provar a ocorrência de um crime. Esses dados podem consistir em textos, imagens, áudio e vídeo. Exemplos de evidências digitais são arquivos de e-mail, histórico de conversas IRC ou em redes sociais, imagens, vídeos de vigilância ou arquivos de log que mostram acesso a determinados recursos.

2.5 Forense Digital

Quando um crime foi cometido no mundo físico, várias vezes a evidência pode ser encontrada em dispositivos digitais de um suspeito ou na internet. A internet se expande com mais sensores supervisionando o mundo real diariamente, como câmeras de trânsito, caixas eletrônicos e *webcams*. As pessoas também tendem a publicar mais mensagens em sites de redes sociais ou a conversar em salas IRC, onde os endereços IP revelam a localização e as conversas estão sendo registradas. Sempre que uma investigação está em andamento e há chance de evidência digital, uma investigação forense digital precisa ser conduzida. Isso normalmente inclui apreender os

dispositivos digitais de um suspeito, como computador pessoal, telefone celular, dispositivo de navegação, dispositivos de memória e pesquisar possíveis provas ou pistas.

Quando um meio digital é examinado por especialistas forenses, a evidência deve às vezes ser recuperada de memória quebrada ou intencionalmente destruída, dados excluídos ou perdidos. Independentemente do estado do dispositivo e dos dados, um passo muito importante deve ser tomado primeiro: crie uma imagem que é uma cópia digital do estado quando o dispositivo foi coletado. Esta imagem é importante para provar a cadeia de custódia, a integridade da evidência possivelmente encontrada durante a investigação, portanto, pode-se comprovar que os dados no meio não foram alterados pelo investigador ou por um terceiro a partir do momento em que o dispositivo foi coletado até uma possível apresentação no tribunal. O passo de verificar a integridade geralmente inclui uma comparação da impressão digital entre a imagem inicial e as evidências apresentadas. Esta evidência digital consiste principalmente em um valor de *hash* da imagem, o que significa uma soma de verificação calculada dos dados. Esta soma de verificação é mais comumente calculada por um algoritmo MD5 ou SHA-1. Todos os algoritmos *hash* produzem uma impressão digital quase única, que sempre será a mesma dada a mesma entrada. Por exemplo, o algoritmo *hash* MD5 produz um *checksum* de 128 *bits* de qualquer entrada com comprimento arbitrário. Portanto, uma cópia ou imagem exata de um dispositivo terá a mesma impressão digital do que o original. Uma pequena alteração causaria uma impressão digital diferente do original.

Depois de adquirir um dispositivo que contenha memória digital, o investigador tentará tirar uma imagem digital do dispositivo coletado antes de procurar evidências. Às vezes, isso não é inicialmente possível devido a falhas de *hardware* de natureza intencional ou não intencional. Portanto, uma recuperação baseada em *hardware* ou *software* deve ser realizada.

2.6 Recuperação de hardware em HDs

Falhas de *hardware* não precisam ser de natureza intencional. A eletrônica em discos é muito frágil, assim como as cabeças de leitura e gravação. Em qualquer dos casos acima, a maneira mais promissora de restaurar dados de um dispositivo quebrado está substituindo as peças que estão quebradas. Na maioria das vezes os pratos ainda estão intactos, apenas os mecanismos, para ler as informações deles, não estão funcionando corretamente. Nestes casos, é muito importante obter o mesmo *hardware* que o defeituoso, porque cada fornecedor e modelo usa tecnologias ligeiramente diferentes. Basicamente, três componentes podem ser substituídos. Se um braço, corrediça ou cabeça estiver quebrada, todo o braço precisa ser substituído, caso contrário, a placa eletrônica que contém *chips* e *firmware* pode ser substituída, bem como o motor do fuso. Todo o fuso pode ser colocado em uma caixa diferente contendo todo o outro *hardware*.

Aqui é crucial que os discos no fuso não mudem sua posição para os outros discos. As chances de restaurar dados de uma unidade defeituosa nos casos acima são muito altas se a substituição for feita com muito cuidado e em um ambiente limpo (Moulton, 2006).

2.6.1 Recuperação de hardware na memória flash

A recuperação de dados da memória flash é mais difícil que as unidades de disco rígido; Todos os *chips* de controle e memória são soldados a uma placa. Portanto, não podemos simplesmente substituir uma parte do dispositivo sem encontrar exatamente o mesmo modelo e substituir as peças por ressoldá-los. Dependendo do tipo de memória flash, 2 a 20 fichas se encontram em uma placa. Ressoldá-los à mão é um trabalho difícil e frágil e quase impossível para vários *chips* (Moulton, 2011).

Outra possibilidade é a dessoldar cada *chip* de memória e ler cada um separadamente usando *hardware* e ferramentas especiais. Isso é possível para varetas de memória com um *chip*, em SSDs com múltiplos *chips*, este método torna-se muito complexo porque cada fornecedor usa estratégias diferentes sobre como usar *chips*, como realizar o nivelamento de desgaste e coleta de lixo e como distribuir dados. A Figura abaixo mostra um *hardware* usado para ler um único *chip* de memória flash.

Figura 2 - PC-3000 Flash SSD Edition

2.6.2 Recuperação de software em HDs

A recuperação de dados nem sempre é relacionada ao *hardware*. Em muito mais casos, a análise do disco que usa o *software* é suficiente para recuperar informações de um disco. Como mencionado anteriormente, o arquivo real não é excluído das unidades de disco rígido e, eventualmente, será sobrescrito por um novo arquivo. Esse fato é comumente usado para recuperar dados. Mais importante ainda, ao restaurar dados de discos e reunir provas, os dados originais devem permanecer intactos e alterados o mínimo possível. Portanto, especialistas usam *hardware* específico para copiar as informações no disco para um arquivo de imagem ou outro disco. Este dispositivo é chamado de bloqueador de escrita que é usado como conexão entre o disco rígido e o computador e monitora os comandos que estão sendo emitidos e impede que o computador escreva dados no disco. Os comandos de leitura são passados para o dispositivo enquanto os comandos de gravação serão bloqueados.

2.6.3 Ferramenta de software forense

Muitas ferramentas foram desenvolvidas que o pessoal forense pode usar para recuperar dados de unidades de disco rígido e outras memórias digitais, conjunto de *software* caros, bem como ferramentas de código aberto. No entanto, uma das ferramentas de coleta de evidências forenses mais conhecidas e comuns é EnCase. Ele pode copiar discos usando tecnologia *bit stream* para criar uma reconstrução virtual do sistema de arquivos. FTK (*Forensic Toolkit by Access Data*) e X-Ways são duas ferramentas baseadas em *Windows* diferentes e a característica especial dessas três ferramentas são os dados adicionais armazenados com a imagem do disco como valores de *hash* MD5 para comprovar a integridade da imagem. Sleuth Kit é um conjunto de *software* de código aberto que é executado em diferentes sistemas operacionais e suporta todos os sistemas de arquivos comuns. Autopsy é uma plataforma de forense digital e uma interface gráfica para o Sleuth Kit e outras ferramentas de forense digital. Outras ferramentas de *freeware* bem conhecidas são Recuva, classificada como muito boa, e o PCI File Inspector também classificou "3.5 de 5". Após a criação de imagens de um disco rígido usando tecnologia de fluxo de *bits*, cada *bit* na unidade original é armazenado no arquivo de imagem e pode então ser examinado. As ferramentas acima mencionadas podem ajudar o examinador a reunir possíveis evidências em arquivos existentes e também são capazes de restaurar dados de arquivos excluídos ou partições formatadas. Todas as ferramentas mencionadas só são capazes de processar discos não criptografados, se o sistema de arquivos criptografado (EFS) é usado, uma imagem pode ser feita, mas a análise dos dados requer muito mais esforço (Casey, 2011).

2.6.4 Recuperação de software em memória flash

Para examinar um SSD e reunir provas de arquivos existentes, a mesma tecnologia é usada com as unidades de disco rígido convencionais. EnCase ou qualquer outra ferramenta descrita é usada para capturar uma imagem do meio, para não alterar os dados originais e para coletar arquivos de provas potenciais (Casey, 2011). Quando as partições foram formatadas ou os arquivos foram excluídos antes, os examinadores do exame têm poucas chances de recuperação de dados. Isso ocorre porque, em contraste com as unidades de disco rígido, a memória flash e, em particular, os SSDs possuem rotinas internas que não podem ser influenciadas pelo exterior, por exemplo, com um bloqueador de escrita (Moulton, 2011).

2.6.5 Ferramentas forenses para memória flash

As ferramentas que podem ser usadas para capturar imagens e reunir evidências potenciais em SSDs são as mesmas que para HDs. Para ler *chips* de memória individuais de um SSD ou outra memória flash em caso de um problema de *hardware* ou para evitar rotinas internas para alterar os dados salvos nos *chips* de memória, essas quatro ferramentas podem ser usadas:

- PC-3000 Flash SSD Edition (ACE Data Recovery - Russia)
- Dumppicker (Russia)
- Flash Extractor (Russia)
- Flash Doctor (China)

Todas as ferramentas acima funcionam de forma semelhante. O *hardware*, lê o conteúdo de um *chip* de memória. O *software* então compara o fabricante e modelo de *chips* com um banco de dados e ajuda a recuperar arquivos existentes.

Em 2015, a ACE Data Recovery anunciou uma cooperação alargada entre a empresa de recuperação de dados e o SandForce e o desenvolvimento de um novo *software* personalizado para melhorar a recuperação de dados SSD baseada em SandForce. Como mencionado anteriormente, os fabricantes do controlador SSD enfrentam uma competição muito forte e não estão dispostos a compartilhar a visão das rotinas internas, criptografia, nivelamento do desgaste e coleta de lixo. Portanto, a cooperação entre uma grande empresa de recuperação de dados e o maior fabricante de controladores SSD é um enorme passo e melhoria para examinadores forenses e especialistas em recuperação de dados e aumentou drasticamente a taxa de recuperação para SSD baseado em SandForce.

2.7 Desafios dos SSDs para a Forense Computacional

O crescente uso dos SSDs, por conta de seus mecanismos e características, pode representar um desafio para a prática atual de Recuperação Forense ou Forense Digital.

Os SSD são completamente diferente dos HDs. Como qualquer tecnologia nova e em evolução, os fabricantes ainda estão mexendo no *design* e na implementação. Em comparação com unidades magnéticas, não existe uma abordagem padronizada para produzi-los. Com isso, o antigo entendimento entre pesquisadores forenses e discos rígidos foi destruído. De repente, nossa fonte de evidência previsível "pão e manteiga" tornou-se um dispositivo misterioso e secreto.

Em síntese, os possíveis obstáculos ou impedimentos são:

• a execução das rotinas de coleta de lixo e nivelamento de desgaste realizadas pela controladora de acordo de forma autônoma;

• o provisionamento de blocos realizado pela controladora;

• o fato das rotinas acima estarem encapsuladas na *Flash Translation Layer*, não sendo visíveis ou manipuláveis de forma direta;

• o comando TRIM, tanto nas formas automáticas (montagem de volume com *flag discard* ou agendado) quanto na forma manual.

É possível afirmar que, de modo geral, a prática da anti-forense em dispositivos de armazenamento (memória secundária) foi altamente favorecida em detrimento da prática forense com a introdução dos SSDs, tanto passivamente quanto ativamente. Passivamente com a execução das rotinas do SSD sem interferência ou com interferência mínima. Blocos apagados possuem efemeridade quanto ao seu conteúdo, a depender da conveniência e da oportunidade dos algoritmos implementados na controladora. Ativamente com a execução manual do TRIM.

Diante desse contexto, é possível imaginar alguns casos práticos. Um criminoso precavido pode programar a sua máquina de modo a fazer *backups* automáticos utilizando criptografia e *scripts* para execução do TRIM periodicamente, limpando possíveis rastros deixados por arquivos de log, por exemplo. Um indivíduo que tendo conhecimento da chegada da polícia, pode acionar um "*kill switch*" excluindo dados sensíveis e executando o TRIM. Em ambos os cenários, assume-se o pior caso (que os dados não podem ser recuperados como nos HDs, pelo menos não com as práticas atuais.)

No curto prazo, sem nenhum método confiável de obter repetidamente o mesmo *hash* duas vezes, os SSD terão que ser tratados exatamente como qualquer outra fonte de evidência volátil. Os investigadores terão que confiar em documentação e habilidades de demonstração para mostrar exatamente quais as medidas que foram tomadas ao trabalhar na evidência, e esperar a

compreensão do júri. Isso é menos do que ideal e não pode continuar para sempre. A longo prazo, o ônus é certamente sobre os fabricantes dessas unidades. Eles precisarão abrir ou padronizar a forma como estas rotinas de limpeza são implementadas. Talvez todas as placas controladoras possam receber um comando "não apagar" de um bloqueador de escrita, bloqueando-os efetivamente. Seria apenas uma questão de tempo antes de alguém piratear o *firmware* de uma unidade e configurar o controlador para fazer exatamente o oposto após o recebimento deste comando. Estamos apenas no início desta fase desafiadora para o forense digital, e é um lugar muito interessante e emocionante.

3 CONCLUSÕES

A partir das pesquisas realizadas, conclui-se que o cenário das práticas de Forense Digital aplicadas aos discos de estado sólido ainda é incerto, porém pessimista.

Tendo em vista os SSDs terem ganho e continuarem ganhando cada vez mais espaço no mercado onde os discos rígidos predominavam, juntamente ao constante avanço tecnológico na área, torna um tanto quanto difícil a tarefa da Forense Digital de acompanhar a nova realidade dos dispositivos de armazenamento secundário.

A pesquisa mostra os problemas do tópico e a diferença que as tecnologias de memória recém-introduzidas criaram para especialistas em recuperação de dados e pesquisadores forenses. Enquanto as unidades de disco rígido, os cartões de memória flash e os dispositivos de memória USB continuam a armazenar dados após a exclusão, os dispositivos de memória SSD excluem 95 a 100% de todos os dados imediatamente ou tornam-se ilegíveis. A aquisição de dados na memória SSD é imprevisível e varia de diferentes modelos e fabricantes. Portanto, nenhum método aceitável para aquisição de dados em memória flash foi encontrado ainda. É, portanto, um fato que os examinadores forenses não podem seguir as diretrizes tradicionais, a fim de processar e obter evidências digitais que podem ser comprovadas 100% sem alterações.

Se podemos recuperar arquivos apagados de um SSD*?* Provavelmente não. Não utilizando as técnicas atuais, já aplicadas aos discos rígidos. Vários fatores orbitam a questão: modelos e marcas específicas, sistemas computacionais, Sistemas Operacionais, Sistemas de Arquivos e usuários são alguns desses fatores. Combinados entre si, as possibilidades são diversas.

A prática de crimes digitais, que utilizam os SSDs como meio ou como fim para sua realização, inegavelmente é beneficiada com os mecanismos internos de um SSD, concebidos para aumentar o tempo de vida e uso do dispositivo. Mesmo já existindo métodos concretos de remoção segura e de anti-forense, só o fato de usar um SSD já pode ser considerado, até certo ponto, como uma medida antecipada de anti-forense.

Esperamos que fatores como algoritmos, mecanismos e funcionamento dos discos de estado sólido se uniformizem no futuro, à medida que o mercado se expande, e à medida que são feitos avanços na área de engenharia reversa, levando a uma melhor elucidação das características dos SSDs e consequentemente à avanços nas práticas

forenses digitais. Acredita-se, entretanto, que o futuro destas resida no desenvolvimento de estudos e técnicas voltadas para a parte de *hardware*, em vez do caminho via *software*.

Pesquisas anteriores mostram que a consciência geral do tema está aumentando após um período em que ninguém parecia notar o problema. Este é um primeiro passo importante e a base para novas pesquisas com a esperança de criar padrões e novas diretrizes no futuro.

REFERÊNCIAS

BERG, E. C. **Legal ramifications of digital imaging in law enforcement**. Forensic Science Communications. Disponível em: <https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/berg.htm>. Acesso em 30 mar. 2017.

BODDINGTON, R., HOBBS, V. J., & MANN, G. **Validating digital evidence for legal argument**. Paper presented at the SECAU Security Conferences: The 6th Australian Digital Forensics Conference, Perth, WA. Disponível em: <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1041&context=adf>. Acesso em 30 mar. 2017.

CARRIER, B. **File system forensic analysis**. Upper Saddle River, New Jersey: Addison-Wesley. Disponível em: <http://www.campus64.com/digital_learning/data/cyber_forensics_essentials/info_file_system_forensic_analysis.pdf >. Acesso em 01 abr. 2017.

CASEY, E, Digital Evidence and Computer Crime Third Edition, Watham, San Diego, London: Academic Press, 2011.

CERT, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (2015). **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em: < https://www.cert.br/stats/incidentes/2015-jan-dec/analise.html> Acesso em: 24 mai. 2017.

CHANGYI, G. "**Building Embedded Systems: Programmable Hardware**", 2016. Disponível em: <https://books.google.com.br/books?id=wFlBDAAAQBAJ&lpg=PA20&ots=E9-7Yvkkd7&dq=Understanding%20the%20Differences%20Between%20NAND%20Flash%20and%20NOR&pg=PP1#v=onepage&q&f=false >. Acessado em 22 jun. 2017.

datarecovery.net, "**ACE Data Recovery Develops Breakthrough SSD Technology to Recover Data from SandForce-based SSDs**", 2015. Disponível em: <http://www.datarecovery.net/pressreleases/pr_20150206.html> Acessado em 23 jun. 2017.

ELEUTÉRIO, P. M. S.; MACHADO, M. P. **Desvendando a computação forense.** São Paulo: Novatec, 2011.

FARMER, D., VENEMA, W. Forensic discovery—chapter 1: The spirit of forensic discover, 2006. Disponível em: <http://www.porcupine.org/forensics/forensic-discovery/chapter1.html> Acesso em 24 mai. 2017.

FULTON, J. W. **"Solid State Disk Forensics: Is therea Path Forward?"** Utica College, Maio 2014. Disponível em: <http://ordinaryskill.org/wp-content/uploads/2014/05/Fulton_7_Riddell_Solid_State_Disk_Forensics_May_2014.pdf>. Acesso em 03 abr. 2017.

GALVÃO, R. K. M**. Introdução à análise forense em redes de computadores:** Conceitos, técnicas e ferramentas para "grampos digitais". São Paulo: Novatec, 2013.

GARFINKEL, S. L.; (2010). **Digital Forensic Research: The next 10 years**. Digital Investigation 7. P.64-73. doi: 10.1016/j.diin.2009.06.016.

GUBANOVIS, Y., AFONIN, A. **"Recovering Evidence from SSD Drive in 2014: Understanding TRIM, Garbage Collection and Exclusions."** Forensic Focus Articles.

Belkasoft, 23 Set. 2014. Disponível em: <https://articles.forensicfocus.com/2014/09/23/recovering-evidence-from-ssd-drives-in-2014-understanding-trim-garbage-collection-and-exclusions/>. Acesso em 03 abr. 2017.

MALEVAL, J. "**SSD Manufacturers in the world**", 2011. Disponível em: <http://www.storagenewsletter.com/2011/06/14/91-ssd-manufacturers-in-the-world-document/>. Acessado em: 24 jun. 2017.

MAMUM, A. Hard Drive Mechatronics and Control, Boka Raton, FL: CRC Press, 2007.

MILLER, M. "**Understanding the Differences Between NAND Flash and NOR Flash Memory and Key Future Trends**". Disponível em: <http://www.em.avnet.com/en-us/design/technical-rticles/Pages/Articles/Understanding-the-Differences-Between-NAND-Flash-and-NOR-Flash-Memory-and-Key-Future-Trends.aspx>. Acessado em 23 jun. 2017].

MOULTON, S. "**Solid State Drives Destroy Forensics & Data Recovery Jobs**" Las Vegas, 2011 Disponível em: <http://captf.com/conferences/TakeDownCon%20Dallas/SSD%20Solid%20State%20Drives%20&%20How%20They%20Work%20For%20Data%20Recovery%20and%20Forensics%20-%20Scott%20Moulton.pdf>. Acessado em: 24 jun. 2017.

MOULTON, S. "**Hard Drive Recovery Part 3 at Toorcon**" San Diego, 2006. Disponível em: <https://allaboutdatarecoveries.wordpress.com/2009/01/30/hacking-hard-drives-for-data-recovery-part-3/>. Acessado em: 24 jun. 2017.

PECK, P. **Direito Digital.** São Paulo: Saraiva, 2002.

TOFFLER, A. **"A road map for digital forensic research,"** *DFRWS Techinical Report*, 2001. Disponível em: <http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf>. Acesso em 24 mai. 2017.

VATTO, K. **"Seagate Acquires SandForce From Avago"**, 2014. Disponível em: <http://www.anandtech.com/show/8073/seagate-acquires-sandforce-from-avagolsi>. Acessado em: 24 jun. 2017.