Os Discos de Estado Sólido e a Forense Computacional

Resumo

Este trabalho tem como objetivo abordar a problemática da recuperação de dados e a forense computacional nos discos de estado sólido - *solid state disk*. Os SSDs possuem mecanismos que podem prejudicar ou até inviabilizar a recuperação de dados e a análise forense nessas mídias. Tais mecanismos podem atuar de maneira automática, independente do usuário, ou podem ser aliados a práticas anti-forenses para potencializar seus efeitos. No âmbito jurídico, têm-se a potencial perda de informação que poderia configurar evidências da prática de crimes.

Palavras-chave: forense computacional, discos de estado sólido, prova.

Introdução

A tecnologia, de modo geral, está cada vez mais presente nas interações sociais, bem como na esfera criminal, onde sistemas computacionais são utilizados para cometer ou mediar crimes. Nos últimos tempos, tem-se verificado um crescimento no uso dos discos de estado sólido (SSD) - *solid state disk* - nos sistemas computacionais, em detrimento dos discos rígidos - *hard disk drive* - convencionais. Ambos os tipos de mídia constituem o que é denominado por armazenamento secundário.

1 Discos de Estado Sólido

Dados em um meio digital são armazenados de maneira discreta e persistente por longos períodos de tempo em dispositivos de armazenamento secundário, tais como discos rígidos, *pen drives*, CDs, DVDs, etc.

Entre eles, há os SSDs, que são comumente construídos utilizando arranjos de memória *Flash* , conectados por um barramento serial a uma controladora *(*Chen et. al, 2009). A controladora desempenha um papel fundamental em um disco de estado sólido, pois é responsável pela execução e controle de rotinas e gerenciamento de mecanismos internos do disco.

É possível pensar a arquitetura de um SSD em três abstrações: HIL – *Host Interface Layer*,

FTL – *Flash Translation Layer* e FIL – *Flash Interface Layer*. Na HIL, comandos de E/S fornecidos pelo Sistema de Arquivos e/ou pelo Sistema Operacional são recebidos e atendidos: é a camada de interface com o sistema computacional; Na FTL, ocorre a gerência de mecanismos de otimização do desempenho do disco e também ocorre a emulação de um disco rígido em termos lógicos; por fim, a camada FIL é constituída pela interface com a memória física (blocos físicos) (Chen et. al, 2009).

Não serão abordados detalhes técnicos dos SDDs e suas arquiteturas, sendo relevante ressaltar algumas características e nuances desse tipo de mídia. Os discos de estado sólido possuem em geral, desempenho consideravelmente superior que os discos rígidos. Além disso, possuem menor consumo de energia, maior resistência e durabilidade. No entanto, ainda são superados (de modo geral) pelos HDDs quanto à capacidade de armazenamento.

O fator de maior relevância é que diferentemente dos discos rígidos, nos discos de estado sólido, para a realização de operações de escrita em blocos (ou células) em uso, é necessário o apagamento prévio de blocos (ou células) (Bell & Boddington, 2010). Esse processo é conhecido como ciclo *erase before write*, custoso, e que constitui um dos grandes limitadores do desempenho desse tipo de mídia. Isso se deve pelo fato de que a memória utilizada nos SSDs só pode ser escrita um número limitado de vezes. Essa limitação serviu como motivação para a concepção de dois mecanismos que atuam de maneira conjunta para aumentar o tempo de vida e desempenho do dispositivo: a coleta de lixo e o comando TRIM mencionados.

2 Coleta de lixo

A coleta de lixo em um SSD pode ser entendida por meio de etapas. Primeiro a controladora identifica os blocos contendo páginas não utilizadas ou que contenham dados desatualizados, antes de realizar uma operação de escrita (ou prevendo uma). As páginas inválidas são copiadas para um bloco vazio e o bloco original é apagado, estando este pronto para escrita novamente.

Podem ser definidos conceitualmente, dois tipos de coleta de lixo, a *background garbage collection* e a *filesystem-aware garbage collection.* A primeira é o caso mais geral, onde por meio da HIL foi recebida uma requisição de escrita a um bloco em uso. Já a segunda se refere a uma situação na qual a controladora "tem algum conhecimento" a respeito do Sistema de Arquivos e utiliza informações "fornecidas" por este bem como informações globais a respeito dos arquivos para realizar o procedimento mencionado no parágrafo anterior. A coleta de lixo, tratando-se de um processo interno do SSD, é independente do sistema computacional subjacente, ou seja, não depende logicamente do computador para ser realizada.

3 Comando TRIM

O comando TRIM (em inglês aparar) é um comando a nível de Sistema Operacional que sinaliza à controladora que existem blocos suscetíveis à coleta de lixo. O efeito prático é uma antecipação desse processso. Cada SSD implementa de uma maneira diferente o comando TRIM, (Gubanov & Afonin, 2016), pois não há um padrão, ficando a critério do fabricante a implementação do comando.

O Sistema Operacional deve oferecer suporte ao comando para que ele possa ser utitilizado. Por ser um comando a nível de SO e pelo fato de cada SSD o implementar de maneira diferente, o comportamento do comando TRIM varia dependendo de cada par SO, Sistema de Arquivos, para um mesmo SSD. Não só isso, é possível que o TRIM seja enviado de maneira automática ou agendada, ou manualmente, pelo usuário.

4 Recuperação de dados e Forense Computacional

Com base em trabalhos anteriores, como os de Antonellis(Antonellis. 2008), Bell e Boddington (Bell & Boddington, 2010), Gebremaryam (Gebremaryam, 2011), King e Vidas (King & Vidas, 2011), Nisbet e Lawrence (Nisbet & Lawrence, 2013), entre outros, e especialmente em um estudo de caso por Ribeiro (Ribeiro, 2016), é possível reconhecer o potencial danoso que o uso dos SSDs pode representar para a recuperação de dados e para a forense digital para certas configurações de sistemas computacionais que utilizam SSDs. No estudo de caso realizado por Ribeiro, verficaram-se expressivos resultados negativos para a recuperação de arquivos excluídos, em especial no sistema operacional *Linux* e na presença do comando TRIM. Também foi possível verificar a atuação agressiva do comando TRIM no sistema operacional *Windows*.

Conclusão

O futuro da forense digital de discos de estado sólido ainda é incerto, porém pessimista (Ribeiro, 2016). As técnicas atuais, aplicadas comumente aos discos rígidos, se mostram incapazes de acompanhar a nova realidade dos dispositivos de armazenamento secundário.

O usuário do sistema computacional desempenha um papel central nessa problemática

pois, se este detém conhecimentos mínimos de informática, pode aliar técnicas de anti-forense às funcionalidades e aos mecanismos do SSD para tornar a exclusão de arquivos (e a potencial destruição de provas) um processo trivial e efetivo. Ademais, em algumas situações, conforme dito, apenas o fato de se utilizar um SSD para armazenamento secundário pode levar a perda de dados sensíveis excluídos, dado que o processo de coleta de lixo (e o TRIM, a depender do sistema operacional) ocorre muitas vezes de maneira automática nos SSDs, e frequentemente sem o conhecimento do usuário.

A prática de crimes informáticos, que utilizam os SSDs como meio ou como fim para sua realização, inegavelmente é beneficiada com a presença dos mecanismos internos do SSD, concebidos para aumentar o tempo de vida e uso do dispositivo. Embora já existam métodos consolidados de remoção segura e de anti-forense, o uso por si só de um SSD já pode ser considerado, até certo ponto, como uma medida antecipada de anti-forense.

Referências

C. J. Antonellis. Solid State Disks and Computer Forensics, 2008 ISSA Journal, pgs 36-38. Artigo em formato eletrônico. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.173.7020&rep=rep1&type=pdf Última visualização em 04.04.2017.

G.B. Bell e R. Boddington. Solid state drives: The beginning of the end for current practice in digital forensic recovery? , Journal of Digital Forensics, Security and Law, 5(3):1–20. Australia, 2010.

D. A. Koufaty C. Feng e X. Zhang. Understanding intrinsic characteristics and system implications of flash memory based solid state drives , 2009. In ACM SIGMETRICS Performance Evaluation Review, volume 37, pages 181–192. ACM.

F. Y. Gebremaryam. Solid State Drive (SSD) Digital Forensics Construction , 2011 Master of Science in Computing System Engineering, Politecnico di Milano. Documento em formato eletrônico. Disponível em: https://www.politesi.polimi.it/bitstream/10589/37402/3/SSD%20Digital%20forensics%20Construction.pdf

Y. Gubanov e O. Afonin. Recovering Evidence from SSD Drives in 2014: Understanding TRIM, Garbage Collection and Exclusions, 2014 Sítio eletrônico.

C. King e T. Vidas. Empirical analysis of solid state disk data retention when used with contemporary operating systems , 2011 Digital Investigation Journal. Artigo em formato eletrônico. Disponível em: https://www.dfrws.org/sites/default/files/session-files/paper-empirical_analysis_of_solid_state_disk_data_retention_when_used_with_contemporary_operating_systems.pdf

A. Nisbet e S. Lawrence. 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. SRI Security Research Institute, Edith Cowan University, Perth, Western Australia, 2013.

RIBEIRO, João Vitor A. Forense computacional em discos de estado sólido: desafios e perspectivas. 2016. xii, 73 f., il. . Monografia (Bacharelado em Ciência da Computação)—Universidade de Brasília, Brasília, 2016.