# AUTOPSY & SLEUTHKIT: RECUPERANDO INFORMAÇÕES DESCARTADAS EM MÍDIAS COMPUTA CIONAIS COM SISTEMAS MICROS OFT. ESTUDO DE CASO: PEDOFILIA

**Claudemir Costa SANTOS**[1]

**RESUMO**: É consenso na comunidade forense a necessidade de se compreender o comportamento de mídias computacionais nos cenários de alocação, deleção e recuperação da informação. Estudo de caso oferecendo a dinâmica de operação do kit forense open source sleuthkit.

**PALAVRAS-CHAVE:** Forense computacional; sistemas de arquivos; autopsy sleuthkit; pedofilia.

## Introdução

Em abril de 2004, a polícia civil de Sorocaba foi levada, após uma denúncia anônima, até a casa de um executivo, o qual estaria abusando de duas crianças. Na ocasião, o suspeito foi preso, um computador e um notebook foram apreendidos.

Numa análise preliminar realizada pelos policiais que atenderam a ocorrência, observou-se uma aparente ausência de imagens comprometedoras. As crianças, bem como seus responsáveis, negaram a existência de qualquer situação que orientasse o autor à prática de algum crime envolvendo atividade sexual com crianças.

Até aquela ocasião não utilizávamos uma metodologia específica na análise de mídias computacionais envolvendo pedofihia. Estávamos concluindo um estudo sobre sistemas de arquivos, mas não havia uma convergência para algum método em especial. Um pacote de ferramentas, na forma de linha de comando, era muito comentada em uma Universidade do interior do Estado de São Paulo, a qual chamou a atenção pela sua simplicidade.

### 1.1. Investigação de mídias computacionais

Seja qual for à investigação policial envolvendo um crime de informática, é praticamente certo que as evidências estarão em algum tipo de mídia digital. Apesar da grande variedade de dispositivos de armazenamento, os computadores pessoais convergem para um modelo desenvolvido em 1981 pela IBM, tendo o MS-DOS como sistema operacional.

Neste modelo, temos como principal alternativa ao público em geral, sistemas operacionais da Microsoft. Sistemas alternativos têm conquistado um espaço cada vez maior neste contexto, contudo os sistemas Windows se impõem como a opção mais popular em todas as camadas de uso.

Desde o início dos computadores pessoais na década de 80, dois sistemas operacionais se destacavam: o MS-DOS e o UNIX. A abordagem deste trabalho, apesar de restrita aos sistemas Windows da Microsoft, pode ser estendida a outros sistemas.

Um policial examinando um computador analisa a manipulação e utilização de informações, disponíveis na forma de um mecanismo de abstração denominado “arquivo”. Cada sistema disponibiliza ao usuário uma estratégia para esta tarefa, conhecida como sistema de

[1]Perito Criminal da Polícia Civil de São Paulo. Docente de Cursos de Extensão na Faculdade Eduvale de Avaré. claudemir.ccs @ sptc.sp.gov.br

arquivos.

Um sistema de arquivos busca gerenciar o modo como eles serão estruturados, nomeados, acessados e protegidos. É certo que todo aplicativo precisa armazenar e recuperar uma quantidade cada vez maior de informações, elas precisam permanecer integras e muitas vezes são acessadas simultaneamente por múltiplos processos do sistema.

Segundo Brian Carrier, em sua obra File System Forensic Analysis, podemos examinar um sistema computacional de duas formas:

§ Live Analysis: exame com o sistema instalado, risco de alterar o estado de informações armazenadas, como a data de acesso de um arquivo por exemplo;

§ Dead Analysis: exame realizado normalmente a partir da retirada da mídia e feito a partir de aplicativos forenses, a análise é realizada a partir de uma imagem do sistema;

Neste trabalho, debruçados em um caso real de pedofilia atendido na cidade de Sorocaba, ilustraremos as características dos principais sistemas de arquivos da Microsoft, buscando estabelecer uma metodologia de investigação e perícia, na coleta e interpretação de evidências provenientes de mídias computacionais.

## 2. Pedofihia: visão psiquiátrica e legislação

O romance Lolita, do russo Vladimir Nabokov (1899-1977), conta a história de um padrasto que vive um tórrido caso com uma adolescente, a americana Dolores Haze, apelidada de Lolita. Sua obra lançaria termos utilizados até os dias de hoje, como ninfeta ou lolita.

O crime contra a criança é um dos mais abomináveis, na visão de Alexandre Jean Daoun em seu artigo "Pornografia infantil na internet: redundância na lei". Estamos tratando de forma equivocada o termo pedofilia, pornografia infantil é crime, enquanto pedofilia corresponde aquele que gosta de criança, podendo ser entendido como anomalia, implicando inimputabiidade do agente.

Segundo José Roberto Paiva, psicanalista sexologista, Diretor do PROSex (Programa de Reabilitação e Orientação Sexual), pedofilia é um distúrbio de conduta sexual, em que o indivíduo adulto sente desejo compulsivo, de caráter homossexual (quando envolve meninos) ou heterossexual (quando envolve meninas), por crianças ou pré-adolescentes.

É mais comum em homens, em especial naqueles com problemas de satisfação sexual com mulheres adultas. Surpreendemos envolvidos com pedofihia padres, médicos, professores e tantos outros ligados à criança. Mais triste é saber que na maioria das vezes, nos Estados Unidos algo em torno de 80%, o agressor é pessoa de confiança da vítima, envolvendo pai ou parentes.

À luz da psiquiatria, pedofilia envolve pessoa que mantém atividade sexual com crianças, de uma maneira geral do sexo feminino, com dez anos. Os meninos costumam ser um pouco mais velhos. O autor é maior de dezesseis anos e pelo menos cinco anos mais velho que a criança.

A Lei 8 069/90, Estatuto da Criança e do Adolescente, define criança como sendo pessoa de até doze anos e adolescente entre doze e dezoito anos de idade. Em seu artigo 241, estabelece:

**Art. 241.** Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena - detenção de seis meses a dois anos, e multa.

Publicar significa tornar público, permitir o acesso ao público, o sentido de um conjunto de pessoas, pouco importando o processo de publicação (Nélson Hungria, Comentários ao Código Penal, Rio de Janeiro, Editora Forense, 1958, VII:340).

Um ponto crucial nestes casos se refere à identificação das vítimas, que são muitas vezes envolvidas pelo agressor, que desenvolve técnicas complexas para obter a confiança dos responsáveis, a qual pode estar ligada à superioridade financeira sobre a família das vítimas ou à função que exercem, como médicos e professores. Um constrangimento proveniente de uma mistura perigosa de medo e confiança.

## 3. Visão geral dos sistemas de arquivos microsoft

Quando analisamos mídias computacionais com sistemas Microsofi, visualizamos dois sistemas de arquivos: FAT e NTFS. Inicialmente, é preciso oferecer uma visão geral dos conceitos chaves, buscando ao fim focar a localização de informações descartadas pelas razões mais diversas: “deleção”, “file slack” ou arquivos temporários. Atualmente, podemos nos amparar em diversos aplicativos forenses, que irão realizar sem muitos questionamentos a localização de informações, muitas vezes despercebidas pelo mundo policial.

### 3.1. FAT — File Aliocation Table

O modelo FAT foi criado pela Microsoft. Já nas primeiras versões do sistema operacional denominado MS-DOS, a empresa se deparou com um crescente aumento de capacidade dos discos rígidos. Um primeiro tipo de sistema de arquivo persiste até hoje em disquetes. AFAT12 e endereçar 4096 clusters. À medida que novas tecnologias de armazenamento foram surgindo, a FAT evoluiu para FAT16 e em seguida para FAT32.

A evolução da FAT, em síntese, buscou atender o aumento da capacidade de armazenamento das unidades. AFAT1 6 continua no mercado, agora em mídias removíveis como cartões de memória de câmeras fotográficas e celulares, pen drives e tantos outros.

A menor unidade de armazenamento de uma mídia computacional comporta 512 bytes, isto quer dizer que um arquivo de 4 bytes ocupará um bloco de 512 bytes. O modelo desenvolvido pela Microsoft agrupa estes setores em unidades denominadas “clusters”. A idéia é administrar um número menor de endereços. A tabela abaixo ilustra quantos setores por cluster são utilizados. O número de setores é definido de acordo com o tamanho da unidade.

| | Drive Size (lógical Volume) | FAT Type | Sectors Per Cluster | Cluster Size |
|---|---|---|---|---|
| (Floppy Disks) | 360K | 12-BIT | 2 | 1K |
| | 720K | 12-BIT | 2 | 1K |
| | 1.2MB | 12-BIT | 1 | 512BYTES |
| | 1.44MB | 12-BIT | 1 | 512BYTES |
| | 2.88MB | 12-BIT | 2 | 1K |

| | | | | |
|---|---|---|---|---|
| | 0MB – 15MB | 12-BIT | 8 | 4K |
| | 16MB – 127 MB | 16-BIT | 4 | 2K |
| | 128MB - 255 MB | 16-BIT | 8 | 4K |
| (Hard Disks) | 256MB – 511MB | 16-BIT | 16 | 8K |
| | 512MB – 1023MB | 16-BIT | 32 | 16K |
| | 1024MB – 2047MB | 16-BIT | 64 | 32K |

**Imagem 1—Número de setores(agrupamento de 512 bytes) por cluster em função do tamanho da unidade para FAT12 e FAT16**

Os disquetes utilizam um endereçamento de 12 bits, o que significa dizer capacidade para 4096(2^12) unidades de alocação. Em um dispositivo de 1.44Mb, temos 2880 clusters. Nestas mídias cada cluster corresponde a um setor de 512 bytes. Em discos rígidos, à medida que a mídia aumenta, o número de setores por cluster evolui, podendo chegar no modelo de alocação de 16 bits a no máximo 64 agrupamentos por cluster.

Setores de 512bytes —

Cluster -

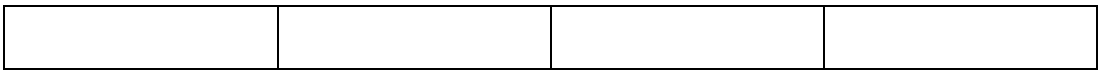

**Imagem 2—Ilustram clusters de 2kb (agrupamentos de quatro blocos de 5l2bytes)**

### 3.1.1. Estrutura

O modelo FAT é, sem dúvida, simples de se compreender. Foi o primeiro sistema de arquivos da Microsoft. Seu uso não se restringe a discos rígidos e disquetes se estende a flash cards para câmeras digitais e pen drives. Um sistema FAT se divide em três setores:

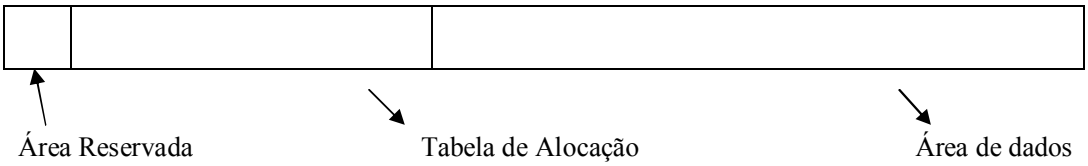


**Imagem 3—Ilustra uma estrutura de um sistema de arquivos FAT**

Neste modelo, cada arquivo ou diretório é armazenado numa estrutura de dados denominada "entrada de diretório". Ela contem o nome do arquivo, tamanho e endereço do primeiro cluster, além de outros metadados.

Entrada de diretório

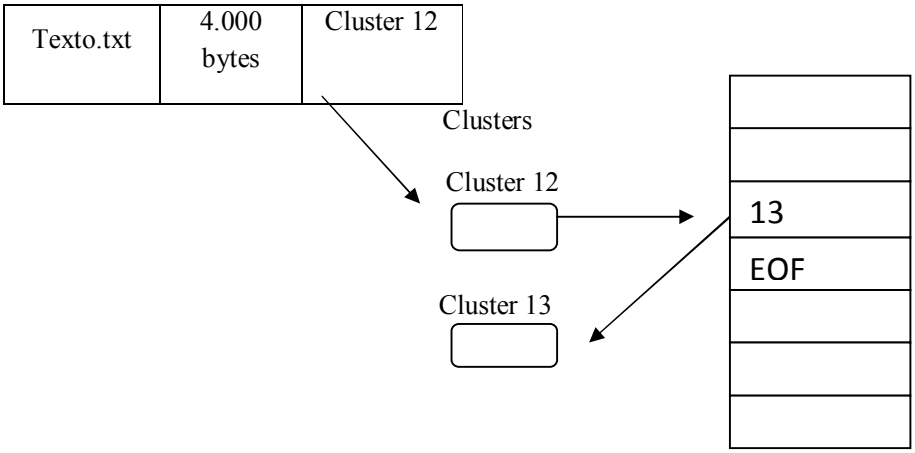


**Imagem 4—Ilustra o relacionamento entre as estruturas de dados**

Em síntese, a FAT é usada para apontar qual será o próximo cluster de um arquivo e também para identificar seu status. A maior diferença entre as três versões de FAT (FAT12, FAT16 e FAT32) está no número de clusters administrados pela tabela.

### 3.2. NTFS — New Technology File System

Muito do que se vê em um sistema de arquivos FAT, pode se estender a sistemas NTFS. Mais uma vez, o aumento crescente da capacidade de armazenamento foi preponderante na opção NTFS.

Ao contrário do sistema FAT, que delimitava áreas, neste sistema tudo acontece em bancos de dados colocados no HD em áreas específicas. A essência permanece, contudo, a forma como as informações são armazenadas e recuperadas apresenta significativa diferença.

Durante a formatação de um sistema NTFS, o sistema de arquivos cria uma tabela denominada MFT (Máster File Table). Existe um record dentro de uma MFT para cada arquivo

ou pasta existente no sistema. Cada record aponta para arquivos que correspondem ao que podemos denominar de metadados:

| MFT File | Nome do arquivo | Descrição |
|---|---|---|
| 0 | $MFT | MASTER FILE TABLE (MFT) |
| 1 | $MFTMIRR | Cópia dos dezesseis primeiros record's da MFT |
| 2 | $LOGFILE | Lista de transações do sistema de arquivos |
| 3 | $VOLUME | Informações sobre o volume: nome, versão e data e hora de criação |
| 4 | $ATTRDEF | Tabela de definição de atributos |
| 5 | . | Pasta root |
| 6 | $BITMAP | Semelhante a FAT, informações da disponibilidade de um cluster |
| 7 | $BOOT | Bootstrape loader se o volume é bootable |
| 8 | $BADCLUS | Lista de cluster com problemas |
| 9 | $SECURE | Diretivas de segurança |
| 10 | $UPCASE | Tabela de conversão de maiúsculas e minúsculas |
| 11 | $EXTEND | Habilita extensões do sistema de arquivo em quotas |

### 3.3.. Cenários Forenses: Alocação, Deleção e recuperação de arquivos

Em futuros cursos de formação para Peritos Criminais, bem como todas carreiras policiais, pretendo impor a necessidade de se compreender o que a bibliografia forense computacional denomina cenários forenses: alocação, deleção e recuperação de arquivos.

No passado, fomos usuários de aplicativos domésticos como unerase. Atualmente, conhecemos as principais estratégias de armazenamento, podendo desta forma avaliar com segurança a eficiência e funcionamento de ferramentas forenses.

Este estudo ocuparia dezenas de páginas que precisam ser escritas e compartilhadas, fugindo infelizmente do escopo deste trabalho. Contudo, já deixando o recado de que um perito oficial não poderá fazer uma análise de uma mídia computacional sem antes conhecer todos meandros da informação da alocação a deleção.

## 4. Sleuth Kit & Autopsy

O pacote de aplicativos Sleuth Kit criado por Brian Carrier, identificado como TSK, surgiu no cenário forense em meados de 2001. Composto por uma coleção de vinte ferramentas, disponibilizadas ao usuário na forma de linha de comando, permite a análise física de um disco, bem como o estudo de imagens de sistemas de arquivos.

O uso eficiente destes aplicativos implica um profundo conhecimento dos principais sistemas de arquivos. Poucos profissionais no mundo forense conseguiriam obter um uso satisfatório destas ferramentas. Desta forma, visando facilitar o uso forense, Brian Carrier disponibilizou o Autopsy, um front end que executa internamente os principais comandos do TSK. Informações detalhadas dos aplicativos, bem como downloaded das últimas versões, podem ser obtidas através do site http://www.sleuthkit.org.

Poderíamos discutir de forma intensa os comandos disponibilizados pelo TSK. Na verdade, o front end Autopsy automatizou os processos, transformando o trabalho do perito em algo simples e principalmente muito prático e amigável.

A análise de uma mídia computacional pode ser feita de duas formas: instalando o aplicativo em uma estação de trabalho ou posto em um cd bootável, como no F.I.R.E., por exemplo. Em nosso caso fizemos uso do TSK em uma estação de trabalho.

O professor de informática da Academia de Polícia de São Paulo, Carlos Henrique AntunesTapareli, em recente participação em um Congresso de Informática na Coréia, relata que a ferramenta é uma realidade em grande parte do planeta. No Brasil temos pouca documentação entre os peritos oficiais. É importante perceber que estamos falando de um pacote de aplicativos poderoso que ainda não faz parte do dia-a-dia da comunidade pericial oficial, pelo menos no Estado de São Paulo.

O fato do TSK não operar no ambiente Windows pode ter sido o limitador de sua popularidade. O ambiente de origem da ferramenta em Linux causa uma certa insegurança.

**4. Estudo de caso: Pedofihia**

Nosso estudo partiu de um caso de pedofilia em que o autor acreditava ter sido capaz de esconder fotos tiradas de uma câmera digital e armazenadas em um arquivo compactado. Por estar em andamento, vamos preservar nomes.

Chamou a atenção da perícia a ousadia, em utilizando o winzip, armazenar dezenas de imagens com senha e ter a absoluta certeza que não seríamos capazes de revelar o conteúdo das imagens.

Já tínhamos vivido uma situação semelhante em São Paulo, na ocasião do seqüestro de Washington Olivetto, um caso importante envolvendo criptografia e esteganografia. Desta vez, constatamos uma grande quantidade de imagens em um arquivo no formato zip.

Quando da perícia, observamos que não tínhamos imagens deletadas. Desta forma, aplicativos domésticos não surtiriam efeito algum. A idéia era aplicar a busca por arquivos não alocados, isto é, sem nenhuma referência, resíduos deixados para trás em arquivos temporários, quando da visualização ou momentos antes de serem coletados no winzip.

O aplicativo Autopsy possui a opção de rastrear todo o disco rígido em busca de conteúdo alocado, deletado e não alocado, o que implica dizer que mesmo arquivos residuais seriam recuperados, evidentemente sem nome ou qualquer referência de seus metadados.

O resultado leva algumas horas para se delinear, Contudo, o que obtivemos foram mais de trinta mil imagens que puderam ser visualizadas em um formato semelhante a uma página web. Destas imagens, pelo menos três mil correspondiam a crianças em cenas no mínimo humilhantes.

Chama a atenção o uso de um aplicativo sem qualquer custo, sem documentação na perícia oficial, capaz de resultados surpreendentes. Contudo, mais uma vez se observa a necessidade de um estudo aprimorado dos chamados cenários forenses.

Do estudo verifica-se a possibilidade e eficácia do aplicativo:

a) busca através de palavra-chave em espaço alocado e não-alocado;

b) processo automatizado de recuperação de todos arquivos deletados;

c) construção de detalhado timeline, apontando para todos arquivos manipulados com data e hora de alteração;

d) processo realizado sem qualquer alteração do conteúdo da mídia analisada.

**Conclusões**

Deste trabalho observa-se a necessidade de um amplo preparo do perito oficial em ações ligadas a perícias computacionais, não bastando conhecer aplicativos forenses. E essencial ter conhecimento do funcionamento de um sistema de arquivos.

Ainda não documentado na comunidade pericial, o aplicativo produzido por Brian Carrier resulta em trabalhos surpreendentes, com um relacionamento amigável com o usuário. Ao contrário do Encase da Guidance, que pode custar alguns milhares de dólares, o Autopsy é gratuito, podendo ser baixado pela Internet por qualquer colega, de qualquer parte do planeta.

---

**AUTOPSY & SLEUTHKIT: RECOVERING IMSCARDED INFORMATION IN COMPUTACIONAL MIDIAS WITH SYSTEMS MICROSOFT. STIJIJY OF CASE: PEDOPIJILIA**

**SANTOS, Claudemir Costa**

**ABSTRACT**: li is consensus in the forensic community the necessity of ifunderstanding the behavior of computational medias in the allocation scenes, deleted and recovery of the information. Study of case offering the dynamics of operation of forensic kit open source sleuthkit.

**KEY WORDS**: Forensic computacional; file system; autopsy; sleuthkit; pedophilia

---

**Referências Bibliográficas**

CASEY, Eoghan. **Handbook of Computer Crime Investigation**. 2. ed. San Diego/ California: Academic Press, 2002.

CARRIER, Brian. **File System ForensicAnalysis**. s.c.: Addison Wesley, 2005.

FARMER, Dan; \ÏENEMA, Wietse. Forensic CornputerAnalysis: An Introduction. **Dr. Dobb's Journal.** Setembro, 2000.

GARFINKEL e SPAFFORD. **Comércio & Segurança na Web.** São Paulo: Market Press, 1999

N. MURILO K. Steding-Jessen. Métodos para a Detecção Local de Rootkits e Módulos de Kernel Maliciosos em Sistemas Unix, **Anais do 3o. Simpósio sobre Segurança em Informática.** SSI2001, São José dos Campos/São Paulo, Novembro de 2001, pp.l33-139.

NOBLETT, Michael G.; POLLITT, Mark M.; PRESLEY, Lawrence A. Recovering and Examining Computer Forensic Evidence. **Forense Science Communications**, Federal Bureau oflnvestigation, No. 4, outubro 2000, vol. 2.

KAMINSKI, Ornar. **Internet Legal**. s.c.: Juruá, 2003

PAINE, Stephen. **Criptografia e Segurança**. Rio de Janeiro: Campus, 2002.

PIRES, Paulo 5. da Mota. Forense Computacional: uma proposta de Ensino. **Universidade Federal do Pará**, novembro 2003.

SCHNEIER, Bruce. **ApIied Criptography**. 2. ed. New York: Wiley, 2000.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**. 2.ed. Rio de Janeiro: Campus, 2003

SWGMAT. Scientific Working Group on Materiais Analysis; Trace Evidence Recovery Guidelines.

**Forense Science Communications**, Federal Bureau of Investigation, No. 3, vol. 1, outubro 1999.
TANENBAUM, ANDREW S. **Redes de Computadores**. 3. ed. Rio de Janeiro: Campus, 1999.
_____ Sistemas Operacionais Modernos. 2. ed. Rio de Janeiro: Campus, 2000.
TERADA, Routo. **Segurança de Dados**. s.c.: Edgard Biucher, 2001.
WARREN, G Kruse. **Computer Forensic.** s.c.: Addison-Wesley Professional, 2001.

**Webgrafia**

http:Ilwww.fbi.gov
http://www.htcia.org
http:Ilwww. nic.br/nbso.html http:llwww.cais.rnp.br