Cópia e Eliminação de Dados

(Investigação, ciclo de vida da informação e Carving File)

flash memory
brasil

Programação

1. Apresentação Institucional (5 minutos)
2. Duplicação Forense
3. WIPE Disk (Sanitização)
4. Cases nacionais e internacionais
5. Anti-Forense, como combater
6. Encerramento (10 minutos para perguntas)

Sobre nós

A FMB - Flash Memory Brasil é especializada em soluções tecnológicas voltadas a Segurança da Informação.

Atua oferecendo soluções em dois seguimentos da Segurança da Informação:

- ✓ Mitigar riscos e ações de engenharia social
  - ➢ Fornece equipamentos e serviços para Sanitização de mídias magnéticas e Estado Sólido

- ✓ Investigação e Forense Digital
  - ➢ Fornece equipamentos e serviços para Coleta de evidências, e investigação digital, com 100% de validade jurídica.

- ✓ As soluções oferecidas são diferenciadas pois dão ênfase em documentar automaticamente os processos, gerando evidencias para auditorias.

Forense Digital

FR100

COLETA de DADOS Investigação Forense Digital

Duplicador de discos recomendado para investigação forense de pequeno porte, para alunos ou iniciantes. Ótima opção para uso do time interno. **Baixo custo.** Garante a integridade durante as investigações. Aderente a normas internacionais..

- Oferece recuperação de dados (File Carving)
- Sistema de segurança HOT SWAP, protege o HDD e preserva a mídia
- Alta velocidade nas cópias bit a bit
- Detecção automática e exibição das características físicas, modelo, número de série do HD, promovendo cadeia de custória durante coleta
- WIPE Disk - Sanitiza os HDDs conforme o modelo DoD, aderentes à NIST, R2, SOX e Basileia
- Conexão USB 3.0 - comunicação rápida com a estação de trabalho
- Write-Protect Lock - permite investigar o HDD garantindo a integridade dos dados (FPGA System).

Forense Digital

FR200

COLETA de DADOS Investigação Forense Digital

Duplicador Forense recomendado para investigação forense de grande porte, para as Forças Armadas, Segurança Pública, Corporações ou profissionais Sênior.

- Ótima opção para uso do time de campo ou em bancada. Solução definitiva. Possui todas as garantias e atende às principais normas internacionais.
- Alto desempenho (18 GB/min), reduz o tempo de coleta
- **Hash SHA1, MD5 e SHA256.**
- Garante a integridade gera dados para custódia e registra o processo de coleta
- Promove a investigação (100% de validade jurídica)
- Wipe: Full Erase, DoD erase, Secure Erase, ...
- Multi Platforma - suportar várias Interfaces: HDD/SSD. (SATA, IDE, SAS, IVDR, SD, ..., etc.)
- Relatório de Logs, registram detalhes e processos, para cadeia de custódia.
- Oferece solução de File Carving, através de técnicas de duplicação

Produtos para SANITIZATION

O Carry HDD, a tecnologia mais avançada para garantir a compliance .

- Alta velocidade (até 6.5GB /min.)
- Compatível com os HDD´s e cartões SSD disponíveis
- File Carving através de modelos de cópia
- Suporta vários formatos: Windows, Linux e Mac
- Controle de energia automático nas portas.

  protege o HDD contra danos durante o processo (HOT SWAP).

Sanitização

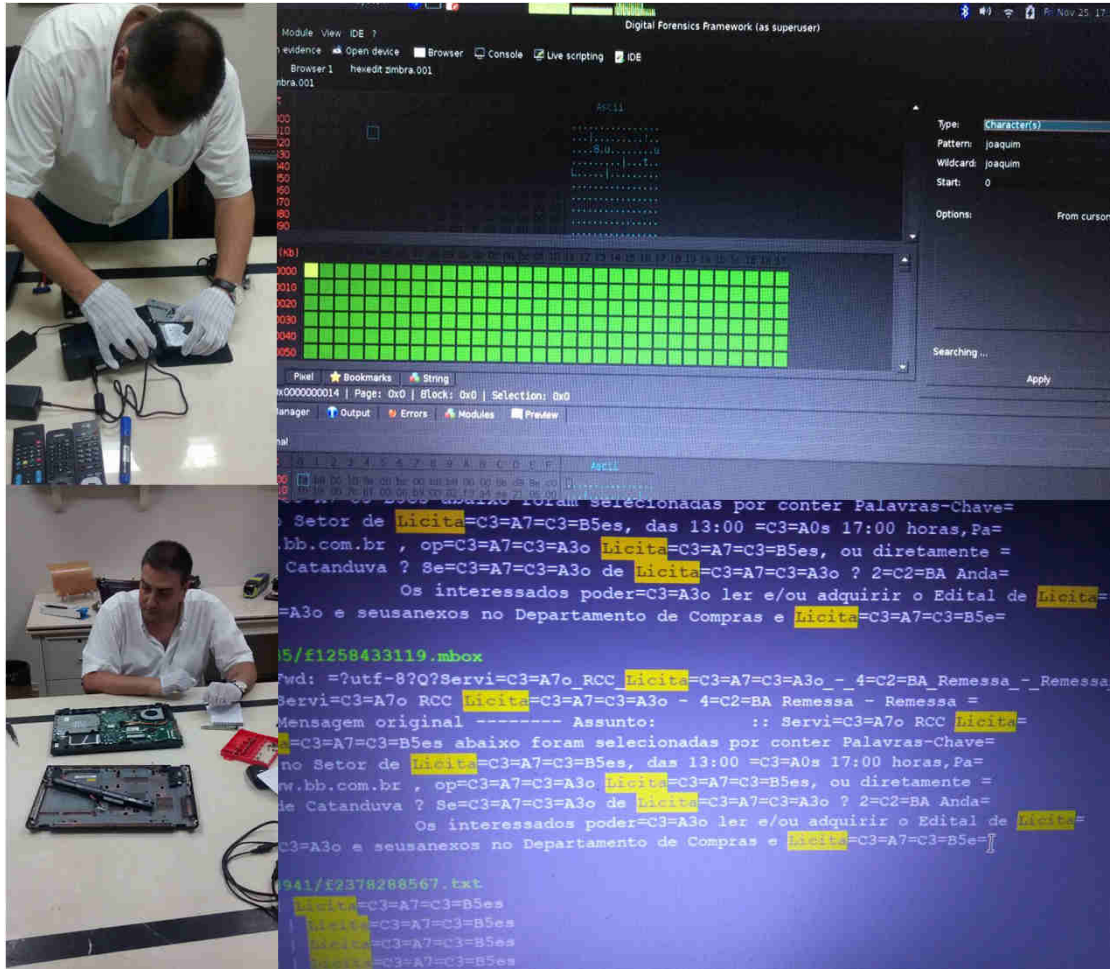
Produtos para SANITIZATION

O TP400G é a solução definitiva que sua empresa precisa para ser Compliance. Combata você mesmo a Engenharia Social.

- Alto desempenho, equipamentos com velocidade de 18 GB/min, (desempenho varia de acordo com a velocidade do HDD).
- Compatibilidade: FAT16/32/64, NTFS, Linux(Ext2/Ext3/Ext4), Mac(HFS, HFS+, HFSX.)
- Atende aos modelos: Quick Erase, Full Erase, DoD Erase, e Secure Erase
- Open-Platform Design - suporta Múltiplas Interfaces para HDD/SSD. Possuem adaptadores para todos os tipos de conexões como: SATA, SAS, IDE, IVDR, etc.
- Audit Compliance: Relatório de logs de todas as atividades, gerando métricas para as equipes de auditorias
- File Carving, através de técnicas de cópia.

Alguns Clientes

DUPLICAÇÃO FORENSE



COLETA E INVESTIGAÇÃO

Uma boa solução precisa ser 100% compatível com os principais Sistemas Operacionais, softwares de Investigação Forense e resultado válido.

- Garantir a integridade dos dados.
- Validade jurídica comprobatória.
- Especialista
- Idoneidade, imparcialidade
- Documentação (metodologia, clareza)

SANITIZAÇÃO

- Novas tecnologias de segurança para SI, gerenciar o **ciclo de vida** e garantir o **sigilo** da informação.
- Apagar por **completo** e de forma **irreversível,** o conteúdo dos HDDs, preparando-os para estarem limpos e seguros em momentos críticos como: - **manutenção, transporte**, **substituição** ou **descarte**.
- Em conformidade com as normas:
- NIST, R2, ISO, ABNT, Basileia ...
- Dados de clientes, DB´s, projetos e quaisquer informações estarão **fora de risco**

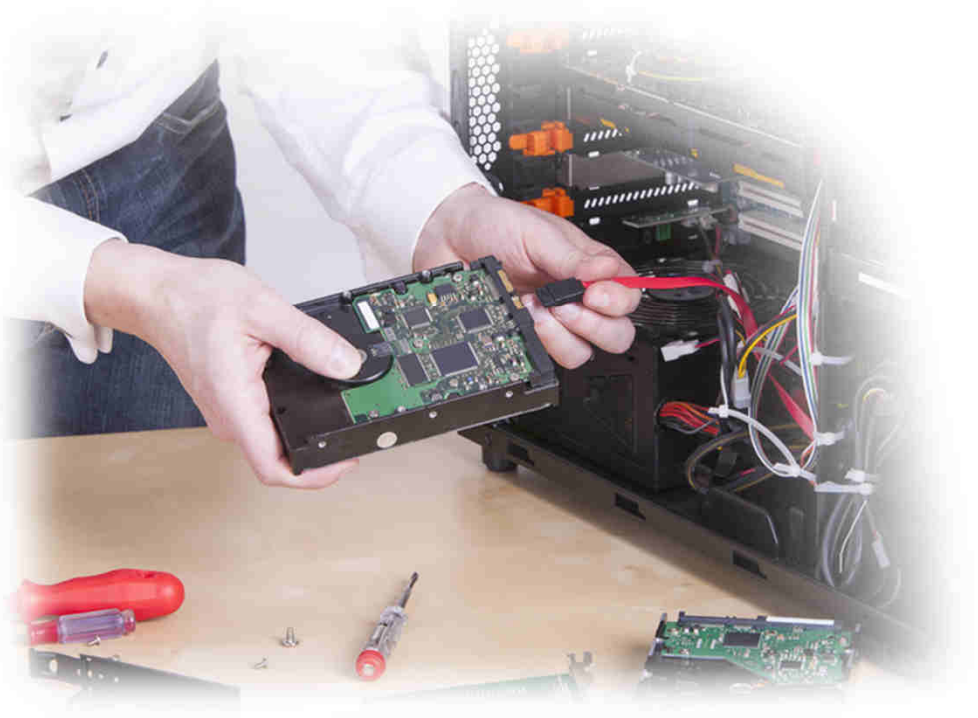
SANITIZAÇÃO

ORIGEM E NECESSIDADE

O processo de SANITIZAÇÃO é utilizado pelos principais players mundiais na área de segurança: IBM, HP, SAP, Bigs Four, Financial, Armed Forces, Data Centers...

Diante das necessidades de segurança observadas junto ao mercado, desenvolveram o modelo(DoD), para reuso e descarte contínuo de mídias de dados.

SANITIZAÇÃO



BRECHAS NA SEGURANÇA DA INFORMAÇÃO

Organizações onde o modelo de segurança não foi adotado, estão vulneráveis à incidentes de Engenharia Social (vazamento de informação).

Principais alvos do crime: Cartórios, Forças policiais, Política...

Existem 4 momentos críticos que podem gerar vulnerabilidade das informações contidas nos HDDs:

VULNERABILIDADES

ESTAÇÃO DE TRABALHO
(HDDS)

ENGENHARIA SOCIAL
(Roubo de informaçõe

1 MANUTENÇÃO

Estação de trabalho é encaminhada para realização de manutenção com os dados disponíveis nos HDDs

2 SUBSTITUIÇÃO

Estocar o HDD que foi substituído, para que aguarde o Erase, gera risco.

3 DESCARTE

Os métodos atuais adotados para destruição de HDDs são inseguros.
É necessário executar o Erase antes de retirar a midia da empresa

4 DOCUMENTAÇÃO

Falta de organização, processos, o não cumprimento das normas comprometem o sigilo.

WIPE - SEGURANÇA

O processo SANITIZATION foi desenvolvido para atender as exigências e demandas do Departamento de Defesa e Forças Armadas dos EUA, devido a incidentes ocorridos

National Institute of Standards and Technology
U.S. Department of Commerce

WIPE DISK tem sido amplamente adotado pelas corporações que trabalham com alto nível de segurança de dados e se comprometem em seguir as orientações das normas vigentes, NIST e R2

Modelo DoD

SANITIZAÇÃO

AMBIENTE INTERNO DO CLIENTE (usuário)

1 ORIGEM

Estação de trabalho (HDD) para Manutenção, Substitição ou Descarte

2 MANUSEIO

HDDs são coletados

3 INSERÇÃO

duplicação de conteúdo e custódia

4 SANITIZATION

Aplicação de Secure ou DOD Erase nos HDDs

5 DOCUMENTAÇÃO

Emissão de documento de conformidade para atender a ISO e SOX.

6 DESTINO HDDs

Prontos para uso, reuso ou destruição

AMBIENTE INTERNO DO CLIENTE (Suporte)

AMBIENTE INTERNO DO CLIENTE (TI)

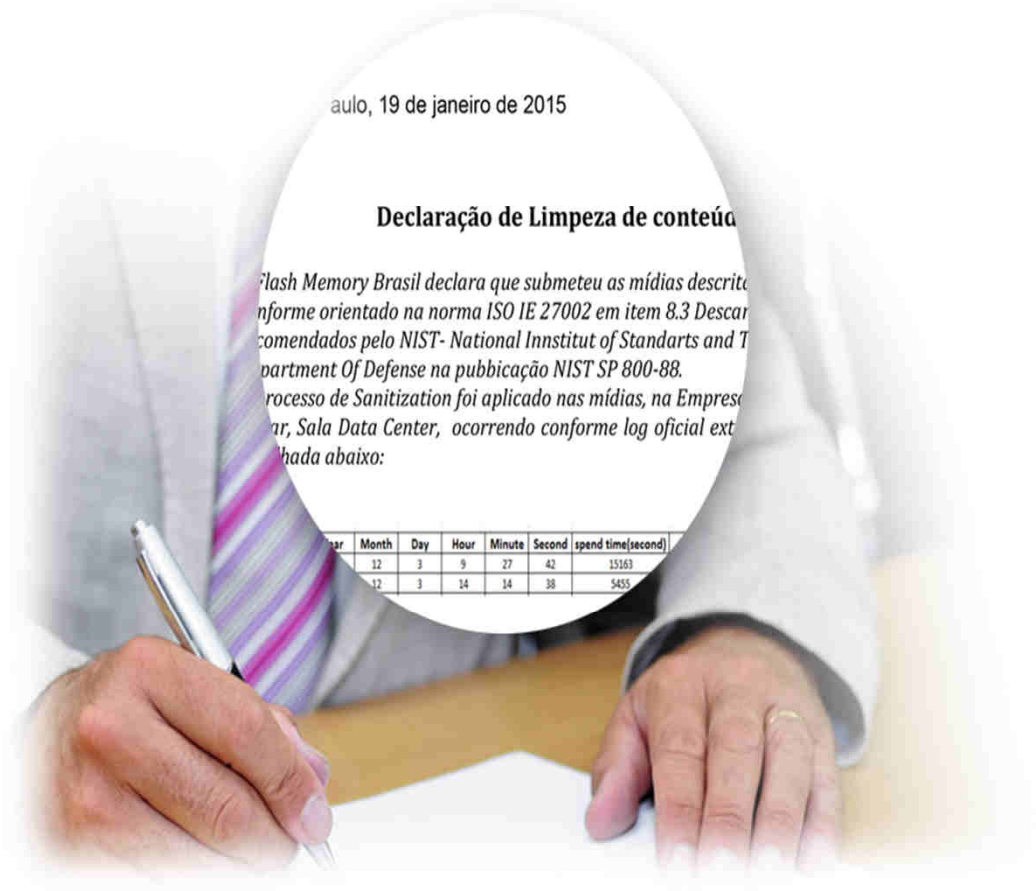
Processo Wipe

CARACTERÍSTICAS DO PROCESSO SANITIZATION

1. CICLO DE VIDA DA INFORMAÇÃO.

- Aplicado conforme necessidade, pela empresa ou prestador de serviços especializado, que atende a um contrato de confidencialidade.
- Erase executado de acordo com a demanda, eliminando o risco por haver custodia prolongada.
- Executado in loco e **acompanhado** pelo ponto focal. (a informação não sai da empresa – Mod. MAC)

Processo Wipe



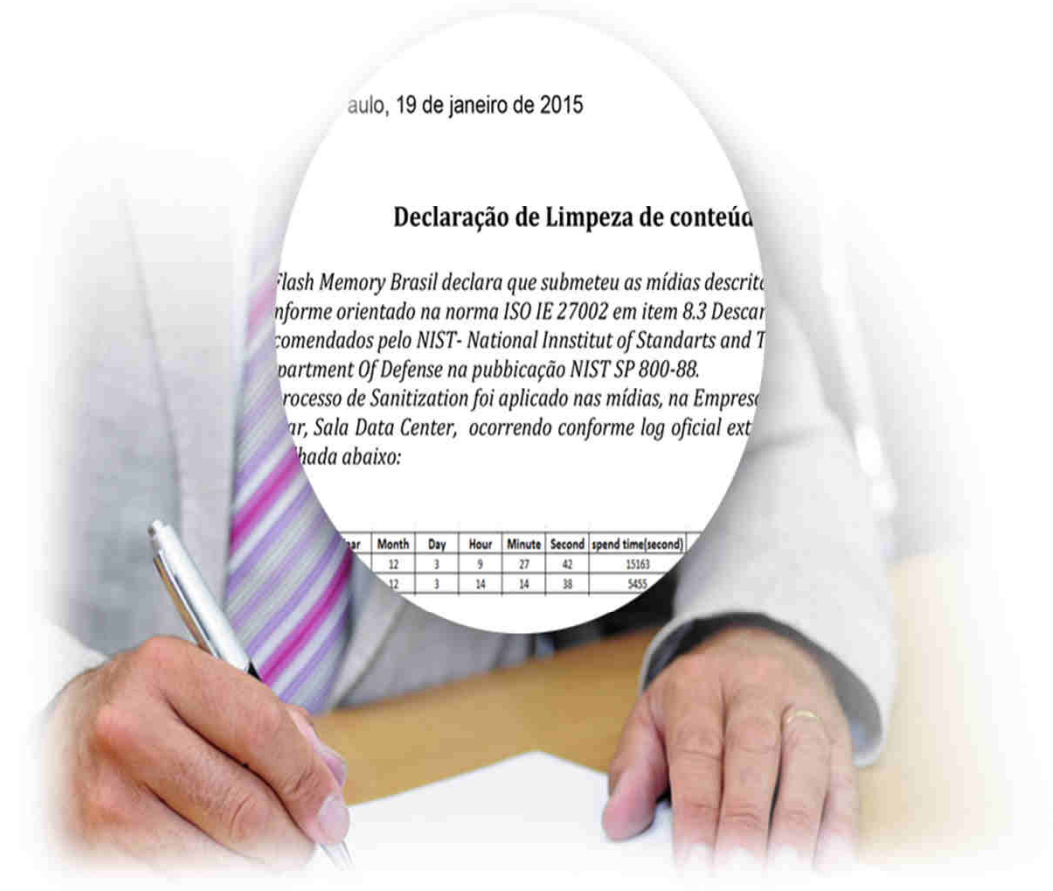
2. DESTRUIÇÃO SEGURA

Realizada após Erase dos dados e da documentação do processo. Desta forma os HDDs podem esperar com segurança pela descaracterização.

3. AGILIDADE E BAIXO CUSTO

Processo executado por solução especialista, que permite uma aplicação rápida ou em massa.

Processo Wipe

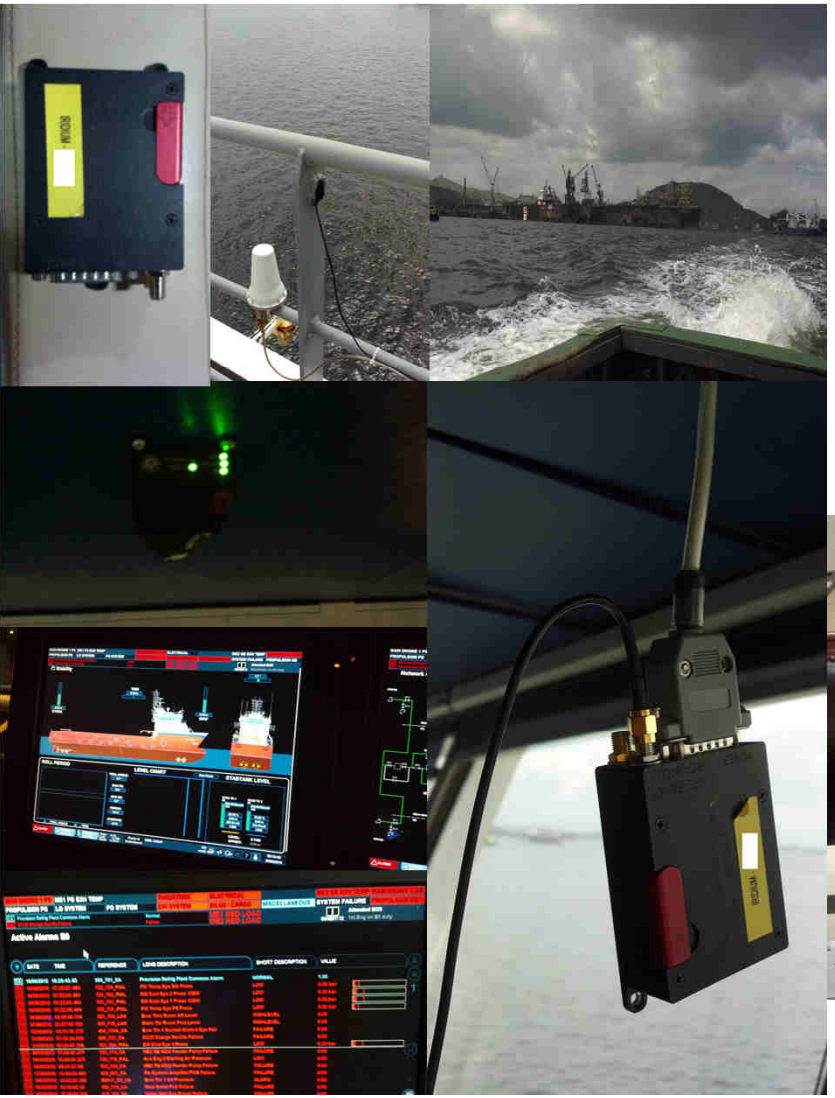


4. DOCUMENTAÇÃO E GARANTIAS

Devido aos quesitos de auditoria, o log do processo Wipe oferece documentação especifica, que demonstra de forma consistente, a execução e aderência as exigências normativas.

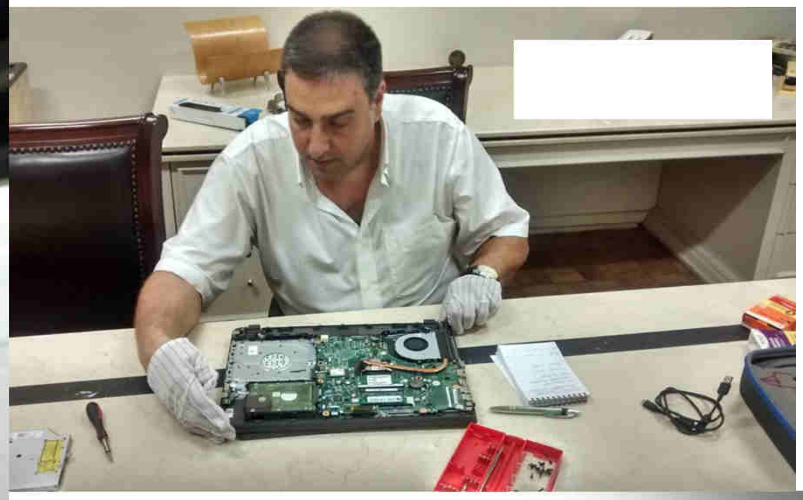
A equipe de SI, precisa da **comprovação** da realização do saneamento das mídias, garantindo autenticidade do ato, diante de qualquer auditoria.

CASE - Coleta

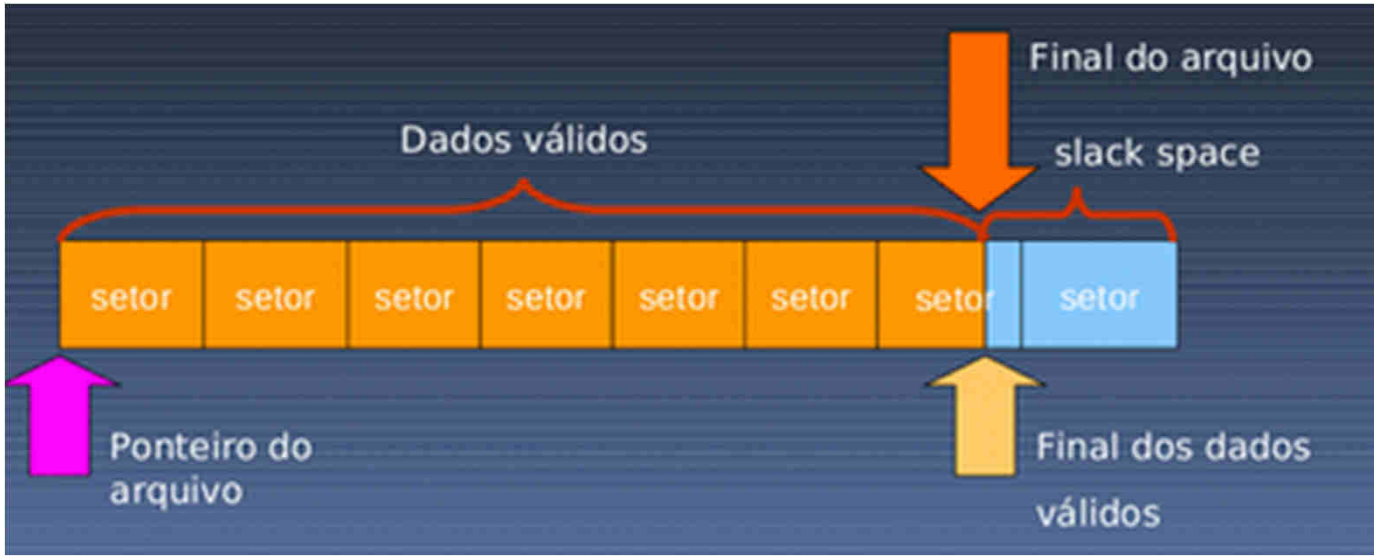


Principais quesitos

1. Conhecimento
2. Ferramental
3. Imparcialidade
4. Pragmatismo (Inquirir mais...)



Anti-forense – Slack Files



Técnica de análise de informações extraídas das áreas não acessíveis através de um sistema de arquivos.

- É na maioria das vezes, um processo tedioso e demorado.
- Esses dados geralmente constituem um fluxo de bits sem estrutura alguma aparente.
- Com o uso de ferramentas adequadas, pode-se obter bons resultados no processo investigativo.

Investigação

,;O×9http://by155w.bay155.mail.live.com/default.aspx#!/mail/InboxLight.aspx?n=97787036!n=907315104&fid=1&fav=1&mid=bdcd8a3c-7a80-11e2-af6a-002264c1d724&fv=1Hotmail - investigado@hotmail.com Windows Liveâ„¢ Hotmail (43) Messenger SkyDrive MSN â–¼ investigado perfil | sair Hotmail Caixa de Entrada (43) Pastas Lixo (19) Rascunhos (9) Enviados ExcluÃdos Nova pasta VisualizaÃ§Ãµes rÃ¡pidas Documentos (26) Fotos (6) Sinalizadas Nova categoria Messenger 18 convites Entrar no Messenger InÃcio Contatos Calendário Novo | Responder Responder a todos Encaminhar | Excluir Lixo EletrÃ´nico Limpar â–¼ Marcar como â–¼ Mover para â–¼ Categorias â–¼ | OpÃ§Ãµes â–¼ | Voltar para mensagens

RE: acerto Receptador 2â€ 13:40

Responder à Receptador Anaryrou Adicionar a contatos

Para investigado

acerto financeiro c vc fixo ok..DB, comissões acertaremos 100% depois pois obras com mma tem valor alto e não comportam 1 % de comissão. O que fazemos aqui e um escalonamento.até um patamar de custeio da estrutura 0..depois aumenta até 1.25%..no mma q envolve mao de obra propria ,sera algo assim.

Receptador Enviado do Samsung Galaxy Note

investigado <investigado@hotmail.com> escreveu:

Receptador, Boa noite Desculpe me mais uma vez o longo texto por email .... confirmado o acordo abaixo ! retificando: a comissão que mencionei que ganho hoje sobre revendas é 0,7 % + 1% AE e fixo de R$ 5.700,00 com o cargo de Arquiteta Coordenador Segmento Decorativo ficou acertada a situação do Fulano? Conforme conversarmos aceito o desafio de dirigir/gerenciar (cargo de Diretora ou Gerente Nacional) do SEGMENTO DECORATIVO DA RECEPTADOR, sendo as divisões de atendimento AE (Arquitetura e Engenharia), REVENDEDORES e divisão

ˆcŸA„ Ohttp://by155w.bay155.mail.live.com/default.aspx#!/mail/InboxLight.aspx?n=97787036!n=907315104&view=1&cmid=bdcd8a3c-7a80-11e2-af6a-002264c1d724&csem=receptador%40receptador.com.br&cdid=&cfid=1&cau=1&cmad=2914%7C0%7C8CFDCA4A5B35570%7C%7C0%7C1%7C0%7C0%7C2%7C3&cacc=1Hotmail - **investigado**@hotmail.com

Windows Liveâ„¢ Hotmail (43) Messenger SkyDrive MSN â–¼ **investigado** perfil | sair Hotmail Caixa de Entrada (43) Pastas Lixo (19) Rascunhos (10) Enviados ExcluÃdos Nova pasta VisualizaÃ§Ãµes rÃ¡pidas Documentos (26) Fotos (6)

Sinalizadas Nova categoria Messenger 18 convites Entrar no Messenger InÃcio Contatos CalendÃ¡rio Â© 2013 MicrosoftTermosPrivacidadeSobre os nossos anÃºnciosAnunciarDesenvolvedores Central de AjudaComentÃ¡riosPortuguÃªs (Brasil) Novo OpÃ§Ãµes Sua mensagem foi enviada Retornar Ã caixa de entrada NÃ£o estÃ¡ na sua lista de contatos **receptador**@receptador.com.br Nome Sobrenome Esperamos que esta pÃ¡gina ajude a manter sua lista de contatos atualizada e a certificá-lo de que sua mensagem foi enviada. Você pode alterar suas configurações se não desejar vê-la.

File Tools Tools 28Â° Californi... Share 373k http://emailnotifier.services.va.cont.com

EVIDÊNCIA

Análise do e-mail (RECEPTADOR)

Data de envio: 15/02/2013 (baseado na data de criação do arquivo periciado)

Hora de envio: 13:40hs.(baseado nos dados da coleta)

Queira o Sr. Perito comentar:

Através desse e-mail a Usuária aceita o acordo do concorrente e dará inicio ao novo desafio profissional.

HASH do arquivo periciado:

MD5	**4043b7e130403f417902728b3fc9e5fc**
SHA1	8**688bfdf5c5d8a477e219ac40dcdba0150508667**
FileNames	RecentPlaces.lnk\Volume2 (C) [237576MB]\NONAME [NTFS]\[root]\System Volume Information**tracking.log.FileSlack**"

Anti-Forense - bmap

Para listar o conteúdo armazenado no slack space de um arquivo, o comando abaixo pode ser executado:

```
[root@grego ~]# bmap --mode slack /etc/hosts
getting from block 2148457
file size was: 277
slack size: 3819
block size: 4096
Hello World
```

Anti-Forense - bmap

Para apagar o conteúdo armazenado no slack space, preservando o conteúdo original de um arquivo, o comando abaixo pode ser executado:

```
[root@grego ~]# bmap --mode wipe /etc/hosts
```

Para identificar se um arquivo têm seu slack space utilizado, podemos utilizar o comando abaixo:

```
[root@grego ~]# bmap --mode checkslack /etc/hosts
/etc/hosts does not have slack
```

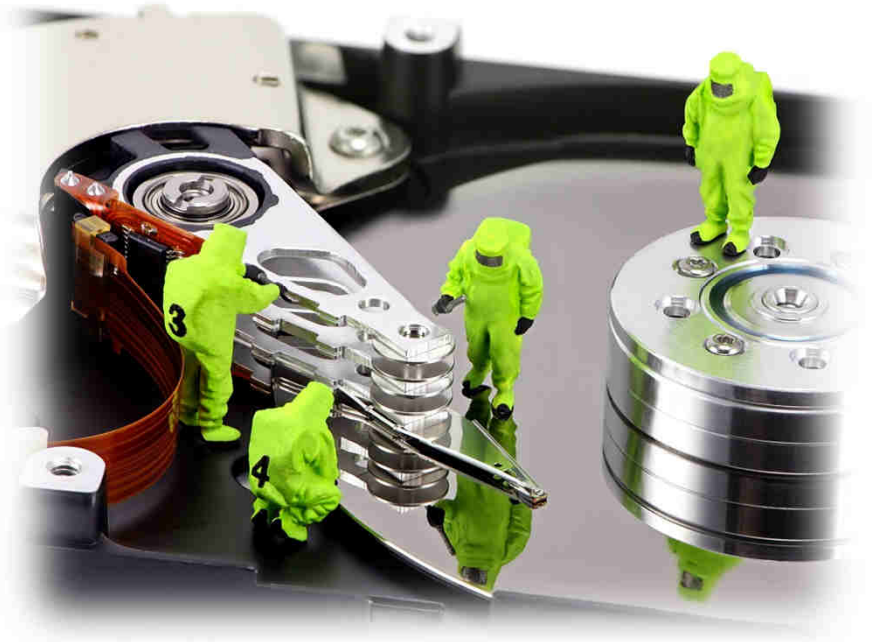
Anti-Forense

APAGANDO EVIDENCIAS OU INDICIOS PELA ANTI-FORENSE

“A utilização de métodos para evitar a aplicação de técnicas forenses, assim limitando a quantidade e qualidade de informação disponível para uso de forma a dificultar a reconstrução de eventos”.

- Ocultação de evidências é o processo de tornar dados difíceis de serem encontrados e ao mesmo tempo mantê-los acessíveis para uso futuro.
- Algumas das formas mais comuns de ocultação de dados incluem criptografia e esteganografia.
- Cada um dos diferentes métodos de ocultação de dados dificulta exames forenses digitais e quando combinados eles podem tornar uma investigação forense quase impossível.

Anti-Forense



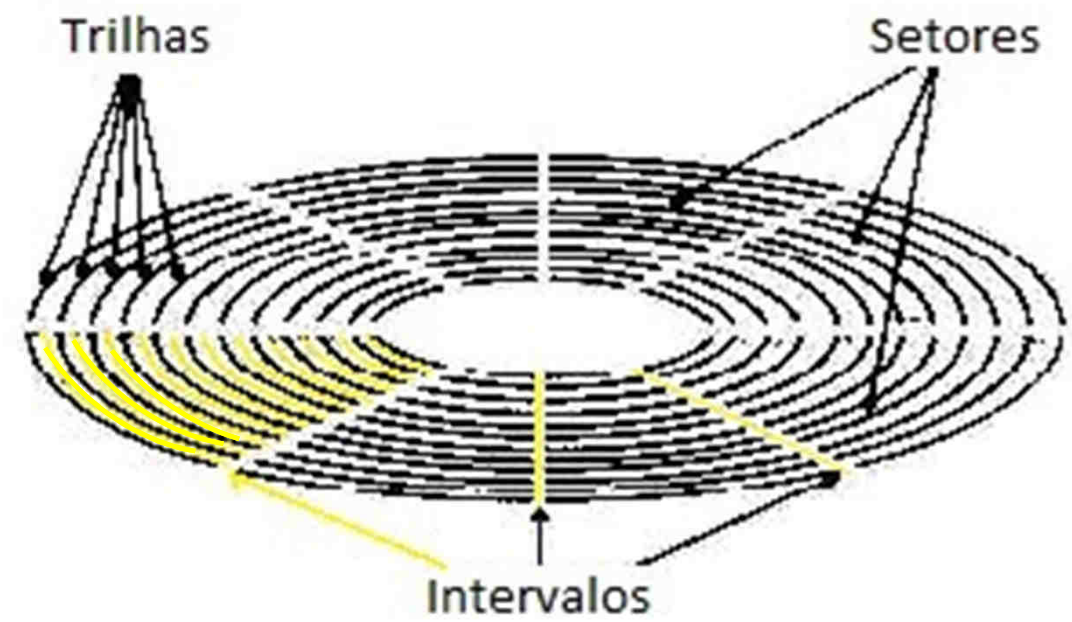
BUSCANDO FRAGMENTOS PÓS ANTI-FORENSE (File Carving)

File Carving, ou às vezes simplesmente Carving(**Entalhe),** é a prática de procurar uma entrada para arquivos ou outros tipos de objetos com base no conteúdo, em vez de metadados.

Carving arquivo é uma ferramenta poderosa para recuperar arquivos e fragmentos de arquivos quando entradas de diretório são corruptos ou em falta, como pode ser o caso com arquivos antigos que tenham sido apagados ou quando se realiza uma análise em mídia danificada.

Anti-Forense

Os meta dados que não foram apagados



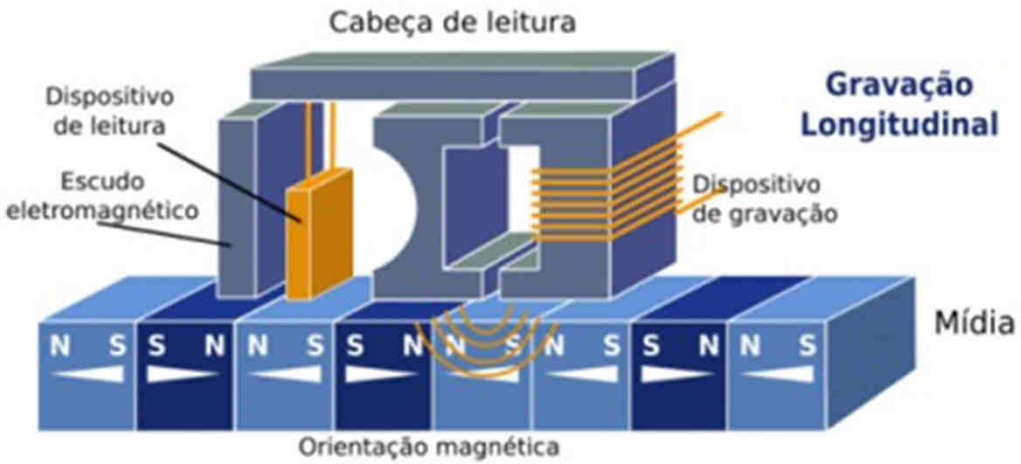
Nasir Memon

Nasir Memon é professor no Departamento de Ciência e Engenharia da Computação no Instituto Politécnico da Universidade de Nova York. Ele é o diretor do laboratório de Sistemas de Informação e Internet Security (ISIS) na Politécnica NYU. Seus interesses de pesquisa incluem compressão de dados, Informática e Segurança de Rede, Forense Digital e Multimedia Segurança de Dados
Nasir também é um membro fundador da Assembleia Digital .

A EVOLUÇÃO DO CARVING - Superparamagnetismo

Tecnologia de Gravação Perpendicular

A tecnologia de gravação longitudinal foi usada desde os primeiros HDs, mas como a tecnologia não para de evoluir, os arquivos ficam cada vez maiores. Para fazer com que o HD possa armazenar arquivos maiores e em maior quantidade, é preciso diminuir o tamanho das partículas magnéticas, mas ao fazer isso as partículas ficam sujeitas a um fenômeno conhecido como **superparamagnetismo.**

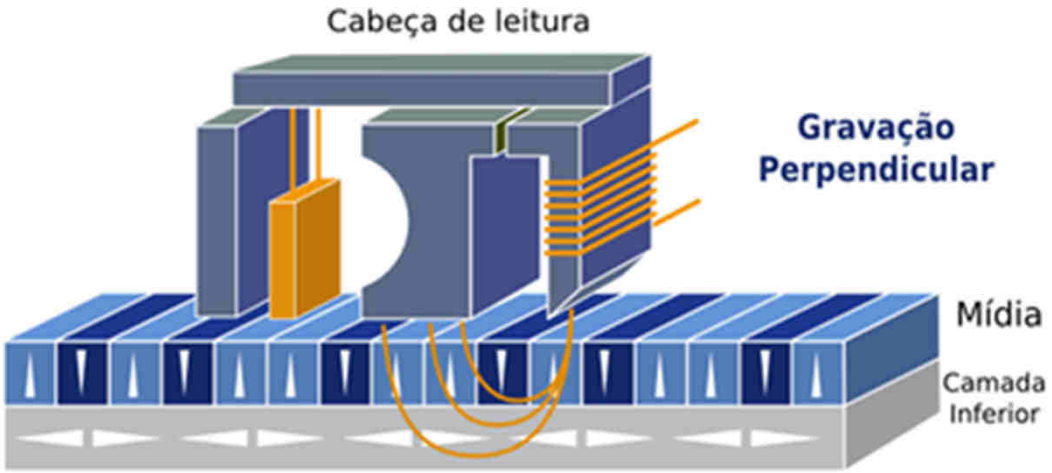


Esse fenômeno acontece quando as partículas ficam muita pequenas e a **variação de temperatura do HD**, fazem com que os campos magnéticos se invertam, esse problema resulta em dados corrompidos.

Esse é o motivo que limita o aumento da capacidade de HDs com tecnologia de gravação longitudinal. .

A EVOLUÇÃO DO CARVING - Superparamagnetismo

A tecnologia de **gravação perpendicular resolveu os problemas da longitudinal**, pois na gravação perpendicular as partículas são alinhadas verticalmente, possibilitando uma maior capacidade de armazenamento de dados, sem ter complicações com o superparamagnetismo.



Essa tecnologia beneficiou os dispositivos portáteis, pois em um espaço menor têm uma maior capacidade de armazenamento de dados, **sem atrapalhar o CARVING EXEC**.

Anti-Forense

REMODELANDO AS EVIDENCIAS OU INDICIOS PÓS ANTI-FORENSE

- Existem várias ferramentas de recuperação de dados... Softwares e Hardwares.

- Quando o HDD se encontra nesta fase final, fica muito mais fácil recuperar os dados de arquivos, através de método e concatenação de fragmentos de arquivos.

- O Método citado no singular, foi porque a única forma é a de estressar a mídia através de uma sequencia de tentativas de leitura, provocando aquecimento, dilatação do disco do HDD e finalmente, o acesso as áreas entre trilhas, que possam ainda conter fragmentos a serem considerados.

Obrigado...

PERGUNTAS?

flash memory brasil

(11) 2063-6134

www.flashmemorybrasil.com.br

Érico C. Manfredi – Perito Forense

aesmo@hotmail.com