UTILIZANDO O HELIX (LINUX) PARA FORENSE DE DADOS

Facilitadora: Alessandra Martins

Femme IT
O JEITO FEMININO DE FALAR DE TI

ROTEIRO

- Conceitos e Definições
- Contexto & Técnicas
- Ferramentas
- Inclusão de medidas de proteção de mídia – Bloqueio de Escrita
- Cálculo de Hash
- Como utilizar ferramentas padrão da versão Helix para Forense de dados ?
- Editando cabeçalhos para recuperação de arquivos ou partições corrompidos ou excluídos

CONCEITOS E DEFINIÇÕES

Ciência Forense

- Diz-se da aplicação de campo científico específico à investigação de fatos relacionados a crimes e/ou contendas judiciais.
- Ou simplesmente: A aplicação da Ciência no Direito

The Forensic Science Society
(http://www.forensic-science-society.org.uk)

Informática forense

- Ramo da criminalística que permite análise de evidências digitais.
- No âmbito criminal, auxilia na investigação de crimes de informática e crimes cometidos com a utilização de computador.

COMPUTAÇÃO FORENSE

Conceito

"A Computação Forense é a ciência que, através de técnicas especializadas, trata do exame, recuperação, autenticação, análise e investigação de dados eletrônicos em um incidente computacional, ou seja, que envolvam a computação como meio, sob a ótica forense, sendo ela civil ou penal. Na criminalística a Computação Forense trata o incidente computacional na esfera penal, determinando causas, meios, autoria e conseqüências."

Contexto

"A Forense Computacional pode ser definida como a ciência que estuda a *aquisição, preservação, recuperação e análise de dados* que estão em *formato eletrônico* e armazenados em algum tipo de *mídia computacional*."

CONCEITOS E DEFINIÇÕES

COMPUTAÇÃO FORENSE X PERÍCIA DIGITAL

"Computação forense é simplesmente a aplicação de um processo de investigação computacional, utilizando técnicas e realizando análises no interesse de determinar evidências em potencial ao processo legal. As evidências podem ser buscada em uma ampla gama de crimes ou incidentes computacionais, incluindo, mas não limitado a furto de segredos comerciais, furto ou destruição de propriedade intelectual, fraude ou mesmo disseminar vírus/ malware para capturar dados de interesse.“

Ref: Robbins, Judd, PC Software Forensics

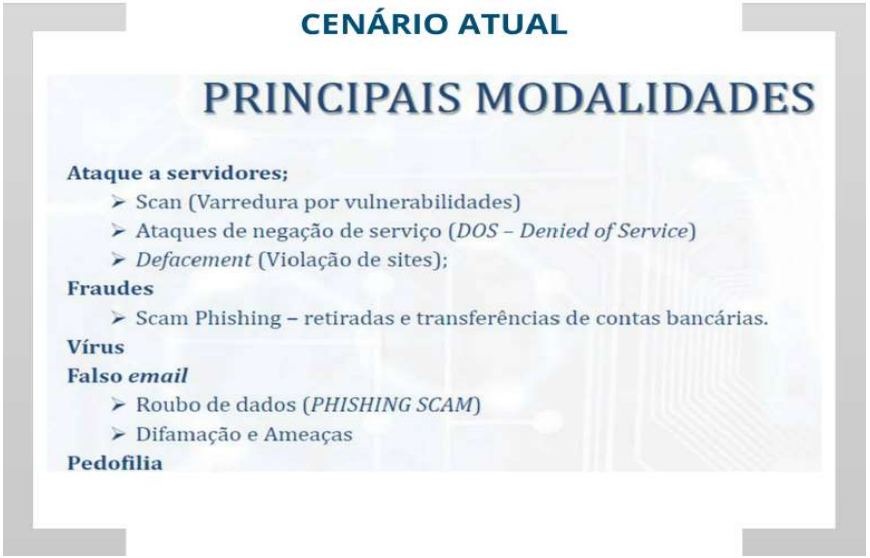
A utilização de métodos cientificamente comprovados e derivados para a preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais derivada das fontes digitais com a finalidade de facilitar ou promover a reconstrução de eventos encontrado para ser criminal, ou contribuem para antecipar ações não autorizadas mostrados para ser prejudicial para as operações planejadas. É mais abrangente que a computação forense, abarcando forense em redes, celulares, a própria computação forense, entre outros.

Ref: Digital Forensics Research Workshop (DFRW)

CONCEITOS E DEFINIÇÕES

- O que a perícia faz e não faz?
- Não faz estimativas, dando-se preferência aos fatos. Quando apesar destes, não se consegue construir um quadro completo, não há outro recurso senão a utilização da opinião e estimativa. Esta habilidade de construção desta estratégia de estimativa deve ser a dos especialistas, bem informados sobre os problemas em questão, de elevada capacidade técnico – profissional e sempre que possível, com experiência no trabalho de gestão da informação.
- Apoia a definição de uma estratégia de investigação pericial para que em determinados casos, seja possível obter as provas suficientes para a convicção do resultado de um laudo pericial. Quando um Perito Criminal avalia um fato criminal deverá adotar determinadas **estratégias a fim de alcançar o objetivo de produção de prova. A perícia produz prova.**
- O que não é Forense Computacional ?

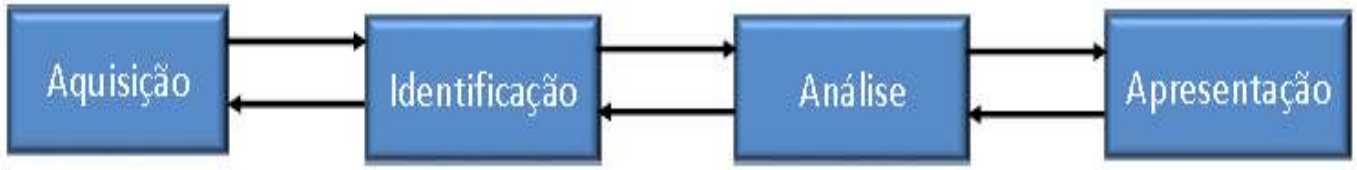
1. Não é Teste de Segurança
2. Não faz ou garante a prevenção de ataques
3. Não garante ausência de falhas



CONTEXTO & TÉCNICAS

Processo de Investigação:

Método em 4 etapas:



Fontes de Evidências Digitais

- Computadores
  - Disco rígido
  - Dispositivos auxiliares (impressora, scanners, ..)
- Dispositivos de Rede
  - Roteadores
  - Switches
  - Firewall
  - Detectores de Intrusão
- Servidores
  - Logs de autenticação
  - Logs de transações
- Outros dispositivos
  - MP3 Players
  - Máquinas Fotográficas Etc..

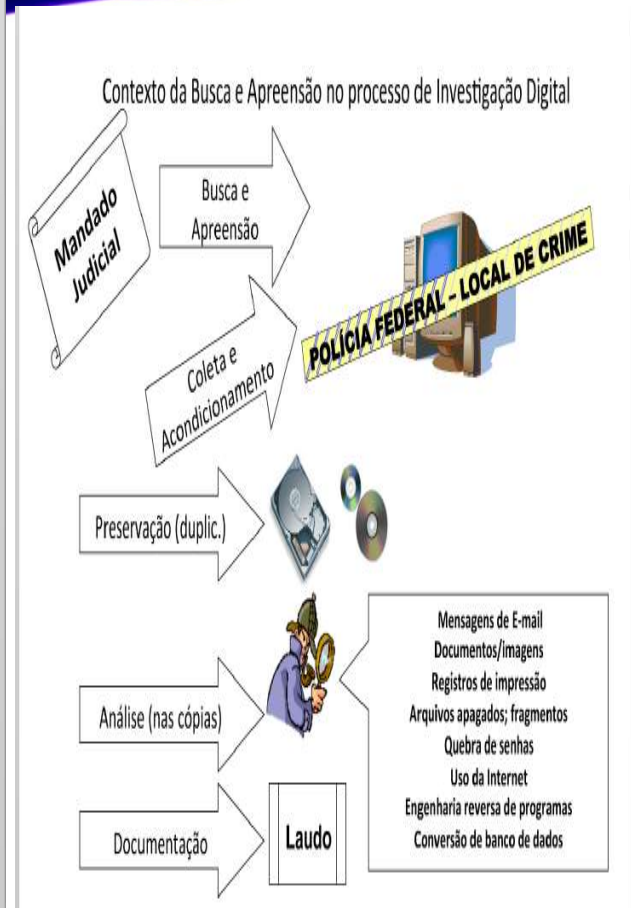
Evidência Digital

Qualquer informação que possa ser extraída de computadores ou dispositivos eletrônicos, interpretada por especialistas e apresentadas num formato intelegível.

Qualquer informação com valor probatório armazenada ou transmitida no formato digital.

Exemplos:

- Recuperação de arquivos/emails apagados
- Investigação de atividades suspeitas
- Recuperação de dados de um HD formatado



Exemplo de Exame

- Inicialmente, o disco rígido encaminhado a exame foi duplicado para outra mídia de igua ou maior capacidade através de um processo conhecido como espelhamento, visando preservar o conteúdo da mídia original.
- Na sequencia, utilizando-se de softwares forenses apropriados, foi feita a extração dos arquivos do disco. Esse processo atingiu não apenas os arquivos acessíveis mas também aqueles apagados que puderam ser recuperados.

CONTEXTO & TÉCNICAS

CONTEXTO & TÉCNICAS

- Coleta de dados consiste em obter, recuperar e catalogar todos os dados ativos (explícitos) ou inativos (ocultos) contidos nos dispositivos computacionais investigados;

- Bloqueio de Escrita;
- Cálculo de Hash;
- Espelhamento de disco – Clonagem;

- Imagem de disco consiste na duplicação das informações de um dispositivo de armazenamento, assim como o espelhamento, porém, o destino de gravação dessas informações é um arquivo e não o disco inteiro;

- *Data Carving* – recuperaração de arquivos apagados, é o método mais utilizado, e sua busca é baseada em assinaturas de arquivos;

- Em ambos os casos (espelhamento ou imagem), a cópia dos dados deve ser fiel aos dados contidos no dispositivo original;

Cadeia de custódia

Quem teve acesso aos vestígios?

Que procedimentos foram adotados por quem acessou o vestígio?

Como provar que a análise foi baseada em cópias idênticas aos originais?

Documentação, hashes, timestamps

CONTEXTO & TÉCNICAS

O termo MACTIME refere-se ao registro de data e hora da última modificação (*Modification time*), do último acesso (*Access time*) e da data de alteração (*Change time*) de certo arquivo.

MACTimes, é simplesmente uma maneira abreviada de se referir aos três atributos de tempo – mtime, atime e ctime – que são anexados a qualquer arquivo ou diretório no Unix, Windows e em outro sistemas de arquivos.

Farmer e Venema (2007, p. 16)

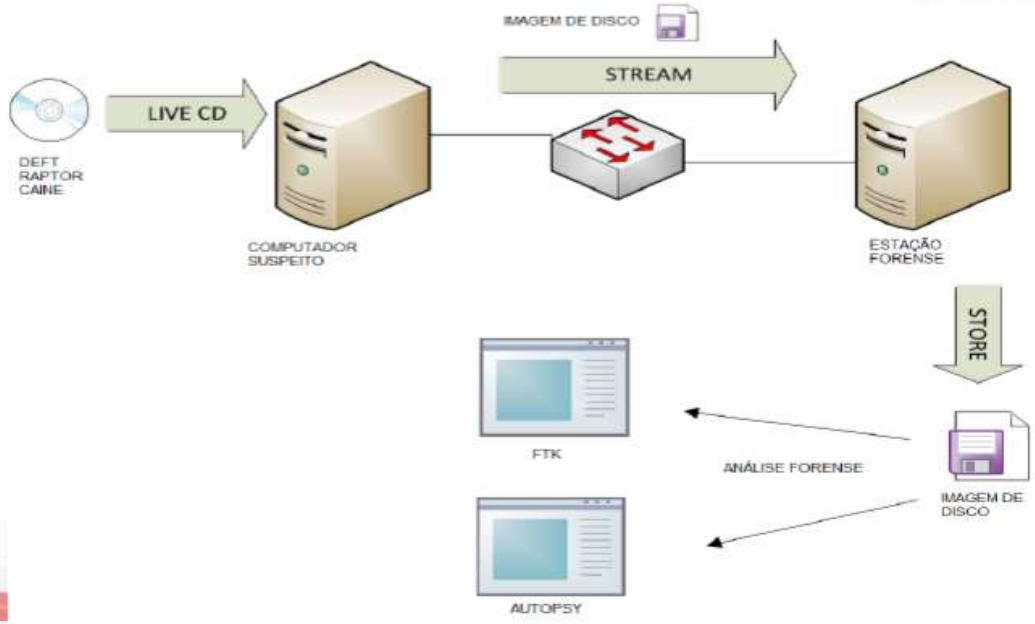
Tabela 1 – Ordem de volatilidade dos principais elementos computacionais

Tipos de Dados	Tempo de Vida
Registradores, memória periférica, caches	Nanossegundos
Memória principal	Dez nanossegundos
Estado da rede	Milissegundos
Processos em execução	Segundos
Disco	Minutos
Disquetes, midia de backup	Anos
CD-ROMs, impressões	Dezenas de anos

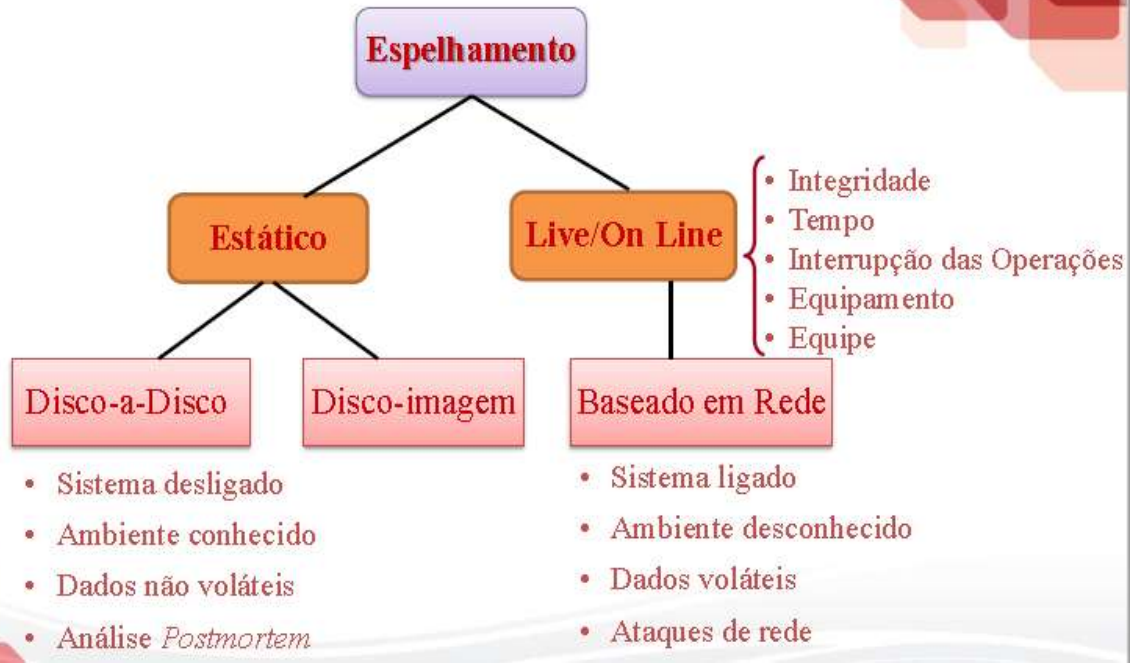
Fonte: FARMER; VENEMA, 2007, p. 6

CONTEXTO & TÉCNICAS

Arquiteturas de espelhamento



Métodos de Trabalho



FERRAMENTAS

Análise de ambiente Windows

•LastActivityView – http://www.nirsoft.net/utils/computer_activity_view.html
•USBDeview – http://www.nirsoft.net/utils/usb_devices_view.html
•Registry Workshop – http://www.torchsoft.com/en/rw_information.html
•Ultimate Forensics Outflow Win-UFO – http://win-ufo.org/downloads.shtml
•PrefetchForensics – http://www.woanware.co.uk/forensics/prefetchforensics.html

Análise de emails

•Kernel for Exchange Server Recovery – http://www.nucleustechnologies.com/Exchange-Server-Data-Recovery.html

Cálculo de Hash

•MultiHasher – http://www.abelhadigital.com/multihasher

Captura e análise de rede

•Wireshark – https://www.wireshark.org
•Xplico – http://www.xplico.org

Carving Tools e Recuperação de Arquivos

•Foremost – http://foremost.sourceforge.net
•ReviveIT – https://github.com/libyal/reviveit
•TestDisk and PhotoRec – http://www.cgsecurity.org/wiki/PhotoRec
•Ontrack EasyRecovery – http://www.krollontrack.com/data-recovery/recovery-software

FERRAMENTAS

Dispositivos Móveis (smartphones)

•MOBILedit! Forensic – http://www.mobiledit.com

•Oxygen Forensic Suite – http://www.oxygen-forensic.com/en/products/oxygen-forensic-suite/features

Dump e Análise de Memória

•Belkasoft Live RAM Capturer – https://belkasoft.com/en/ram-capturer

•Memoryze – https://www.mandiant.com/resources/download/memoryze

•Volatility – https://github.com/volatilityfoundation

Duplicação de mídia (bit a bit)

•FTK Imager – http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.2.0

Emulador de Android

•Genymotion – https://www.genymotion.com/#!/download

Inventário de PC hardware e software

•Free PC Audit (standalone) – http://www.misutilities.com/free-pc-audit/index.html

•Network Asset Tracker (network) – http://www.misutilities.com/network-asset-tracker/index.html

Plataforma de investigação

•Autopsy – http://www.sleuthkit.org/autopsy

•Belkasoft Evidence Center – https://belkasoft.com/en/ec

•EnCase Forensic – https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx

•Forensic Toolkit (FTK) – http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

•OS Forensics – http://www.osforensics.com

Recuperação de Senhas

•Passware Password Recovery Kit Forensic – http://www.lostpassword.com/kit-forensic.htm

FERRAMENTAS

Sites com casos para estudo ou testes de ferramentas

Digital forensics tool testing images (SF.net)
Network Forensics Puzzle Contest
SANS Computer Forensics Challeges (SANS)
Volatility: sample memory images.
The CFReDS Project (NIST)

Algumas distribuições para forense
Baseadas em Debian e derivados

Pendrive de boot com Debian Lenny customizado (neste wiki)
Distribuição BackTrack (DVD)
Distribuição CAINE (CD)
Distribuição DEFT Linux (CD)
Distribuição Kali (DVD)
Pacote para Windows WinTaylor (Zip)
SANS Investigate Forensic Toolkit (SIFT) Workstation (Imagem para VMWare)

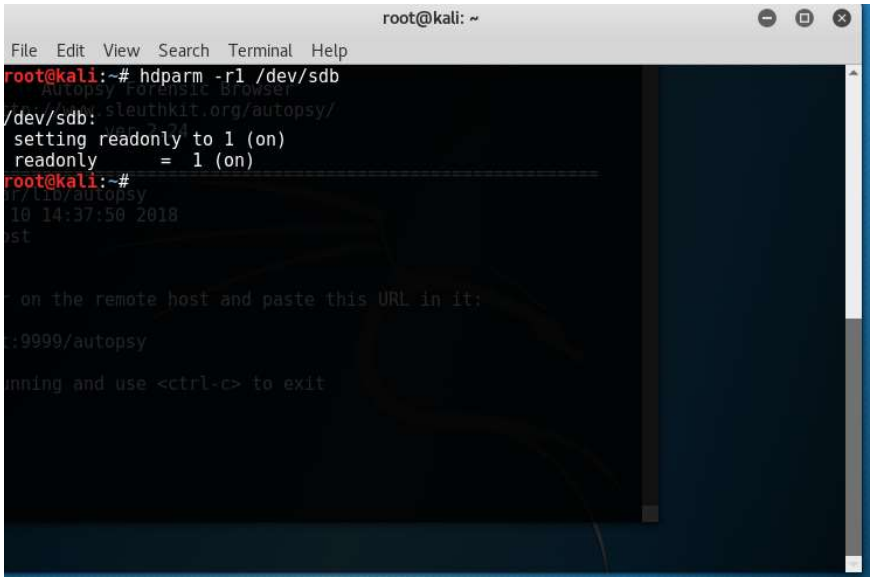
Páginas com ferramentas e tutoriais sobre forense

Computer forensic resources
Forensics Wiki (atualizado constantemente)
Open Source Forensic Tools (atualizado constantemente)
The Electronic Evidence Information Center

INCLUSÃO DE MEDIDAS DE PROTEÇÃO DE MÍDIA – BLOQUEIO DE ESCRITA

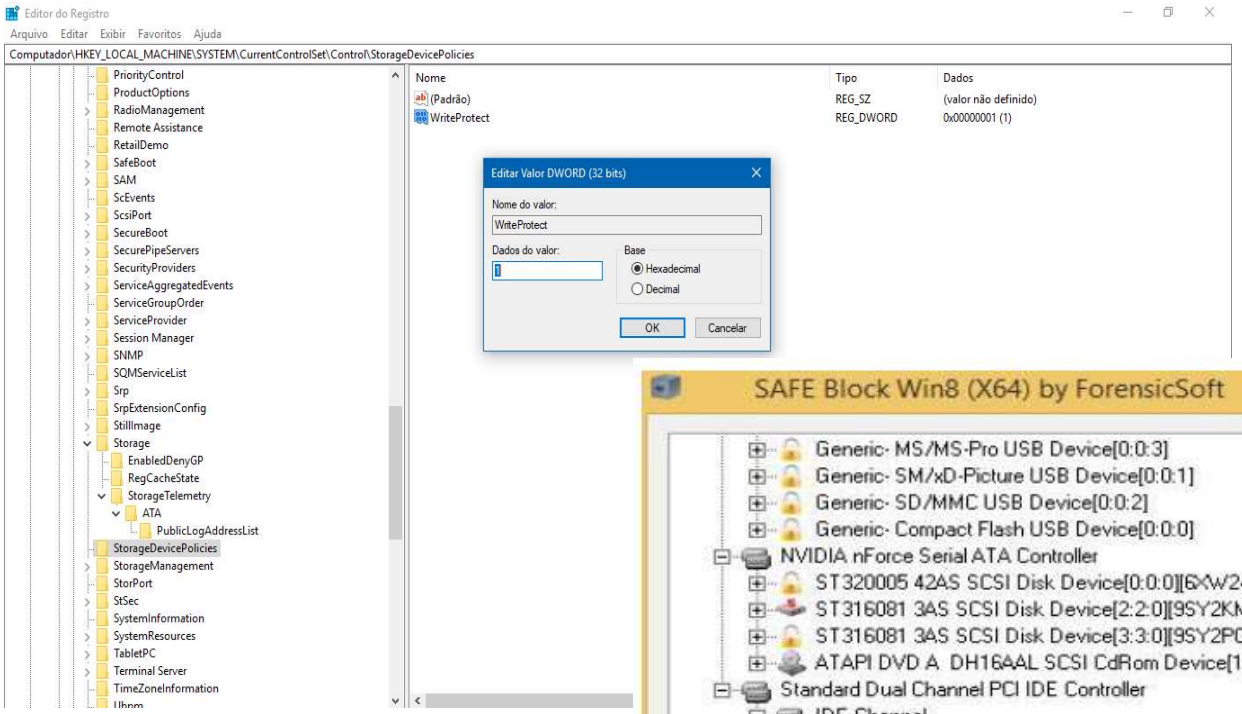
Dispositivo Tableau T4 Forensic SCSI Bridge

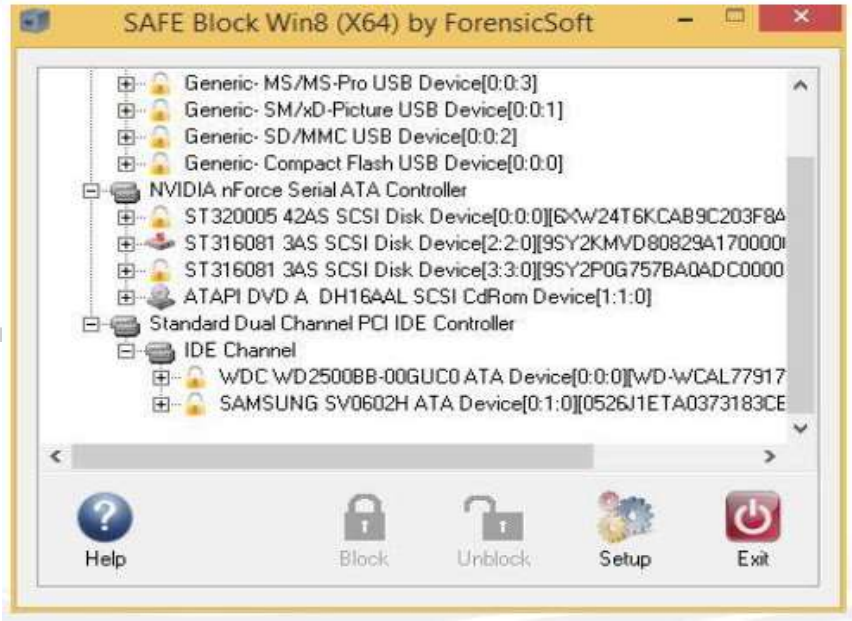
Solo 4 – Bloqueador Via Hardware com Software de Apoio



Em Sistemas Linux o Comando hdparm –r1 /dev + o caminho do disco coloca-o em modo somente leitura

INCLUSÃO DE MEDIDAS DE PROTEÇÃO DE MÍDIA – BLOQUEIO DE ESCRITA





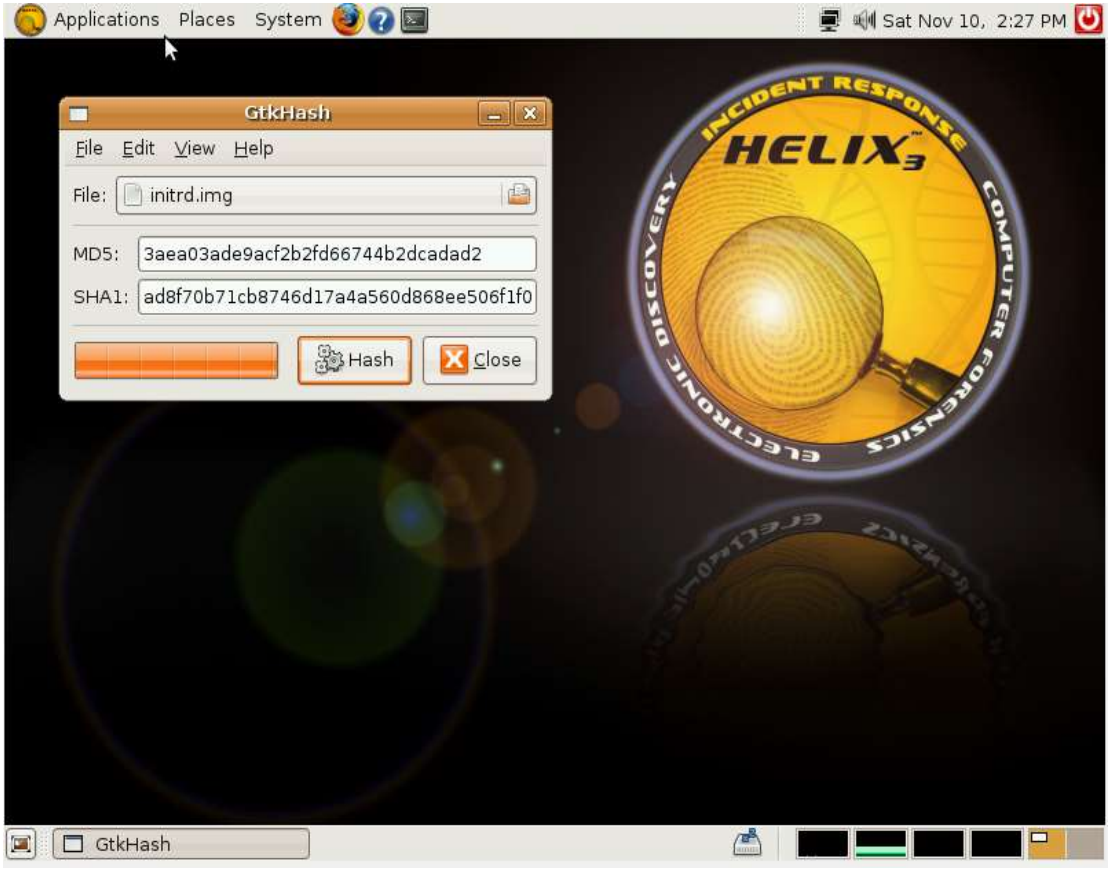
Em Sistemas Windows é Preciso Abrir o Editor de Registros, caso não exista inclui a Chave StorageDevicePolicies , criar o Dword valore de Registro conforme a imagem e setar o valor para 1

CALCULO DE HASH

Um **hash** (ou escrutínio) é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F), representando um nibble cada. O conceito teórico diz que "hash é a transformação de uma grande quantidade de dados em uma pequena quantidade de informações".

Essa sequência busca identificar um arquivo ou informação unicamente.

Uma **função hash** é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo. Os valores retornados por uma função hash são chamados **valores hash**, **códigos hash**, **somas hash** (**hash sums**), **checksums** ou simplesmente **hashes**. Um uso é uma estrutura de dados chamada de tabela hash, amplamente usada em softwares de computador para consulta de dados rápida. Funções hash aceleram consultas a tabelas ou bancos de dados por meio da detecção de registros duplicados em um arquivo grande.



GERAÇÃO DE COPIA PARA FORENSE/ AUDITORIA/INSPEÇÃO DE DADOS

1º Passo Formato de Imagens, é preciso escolher:

3 Modelos de formatos:

- Formato RAW
- Formatos Proprietários
- Formato Forense Avançado – AFF – Advanced Forensics Format

- Desvantagens do Formato Proprietário:

- Pode haver problemas de incompatibilidade com diferentes ferramentas forenses

- Limite de tamanho de arquivo para os segmentos de arquivos – Tipicos tamanhos são 650 MB ou 2 GB

- Formato Expert Witness é o padrão não oficial:

- Utilizado pelo Encase, FTK, X-ways e Smart
- Pode produzir arquivos comprimidos
- Extensão: .E01, .E02 ...

Formato Raw:

- Foi utilizado originalmente pela Ferramenta dd
- Copia bit-a-bit do dispositivo para um arquivo

Principais Vantagens: Transferência de dados rápida

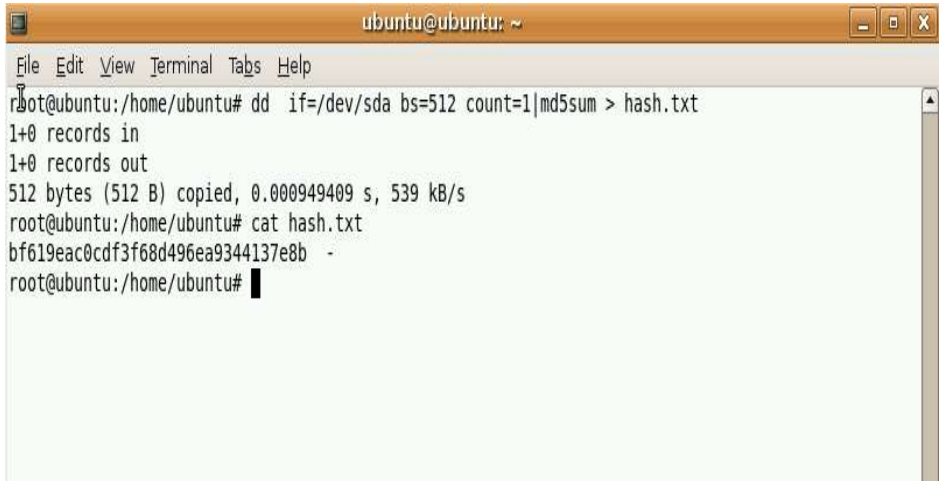
- Pode Ignorar pequenos erros de leitura na evidência
- A maioria das ferramentas forenses podem ler esse formato

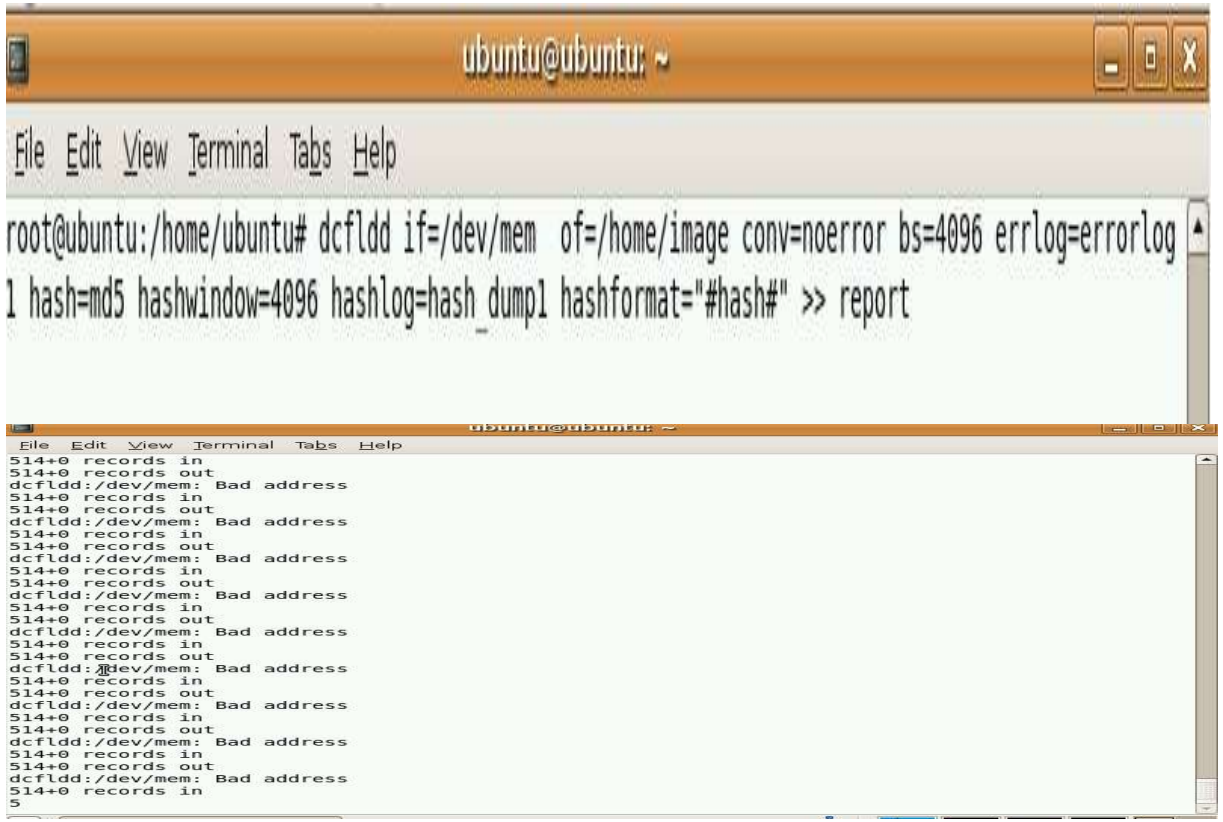
- Desvantagens:
- Requer tanto espaço de armazenamento quanto o tamanho da mídia original
- As ferramentas podem não conseguir copiar bad sectors:

1 - Limite baixo de tentativas em mídias com defeito
2 - Ferramentas comerciais costumar realizar mais tentativas que ferramentas free

Validações devem ser armazenadas em arquivos separados:

1. Message Digest 5 (MD5)
2. Secure Hash Algorithm (SHA-1 ou mais recente)
3. Cyclic Redundancy Check (CRC-32)





GERAÇÃO DE COPIA PARA FORENSE/ AUDITORIA/INSPEÇÃO DE DADOS

2º Passo, Ferramentas:

dd

Bs=n Tamanho do bloco de dados (512b, 2k,4K)
Skip=n
Count=n

Na sintaxe de comando a opção bs deve vir antes do skip/count

#dd if=/dev/das of=/root/lynn.dd bs=4096 count=1

```
root@ubuntu:/home/ubuntu# dd  if=/dev/sda bs=512 count=1|md5sum > hash.txt
1+0 records in
1+0 records out
512 bytes (512 B) copied, 0.000949409 s, 539 kB/s
root@ubuntu:/home/ubuntu# cat hash.txt
bf619eac0cdf3f68d496ea9344137e8b  -
root@ubuntu:/home/ubuntu# 
```

dcfldd

- Dísponivel em todas as distribuições Linux
- Muito parecido com dd, porém, com alguns recursos extras

```
root@ubuntu:/home/ubuntu# dcfldd if=/dev/mem  of=/home/image conv=noerror bs=4096 errlog=errorlog
1 hash=md5 hashwindow=4096 hashlog=hash_dump1 hashformat="#hash#" >> report
```

```
514+0 records in
514+0 records out
dcfldd:/dev/mem: Bad address
514+0 records in
514+0 records out
dcfldd:/dev/mem: Bad address
514+0 records in
514+0 records out
dcfldd:/dev/mem: Bad address
514+0 records in
514+0 records out
dcfldd:/dev/mem: Bad address
514+0 records in
514+0 records out
dcfldd:/dev/mem: Bad address
514+0 records in
514+0 records out
dcfldd:/dev/mem: Bad address
514+0 records in
514+0 records out
dcfldd:/dev/mem: Bad address
514+0 records in
514+0 records out
dcfldd:/dev/mem: Bad address
514+0 records in
514+0 records out
dcfldd:/dev/mem: Bad address
514+0 records in
5
```

GERAÇÃO DE COPIA PARA FORENSE/ AUDITORIA/INSPEÇÃO DE DADOS

3º Passo, Setores Defeituosos (Bad Sectors):

dcfldd

✓ Conv=noerror, sync
Converte bad sectors para zeros
Continua se um erro é encontrado

✓ Hashconv=after
Calcula o hash após a conversão dos bad sectors
Pode ser questionado

✓ Outra Soluções:
Janelas de Hash menores
Comparar as janelas
Mostrar que onde há setores defeituosos os hashes são inconsistentes

3º Passo, Setores Defeituosos (Bad Sectors):

Dd_rescue

✓ Parecido com o dd
✓ Algumas opções foram melhoradas
✓ Foco na correção de bad sectors
✓ Costuma realizar um bom trabalho de espelhamento
✓ Pode demorar um bom tempo para concluir a tarefa

COMO UTILIZAR FERRAMENTAS PADRÃO DA VERSÃO HELIX PARA FORENSE DE DADOS ?

4º Passo, Estruturas e Partições:

Estrutura MBR

Byte	Descrição
0	Bootable Flag
1-3	Starting CHS Address
4	Partition Type
5-7	Ending CHS Address
8-11	Starting LBA Address
12-15	Size in sectors

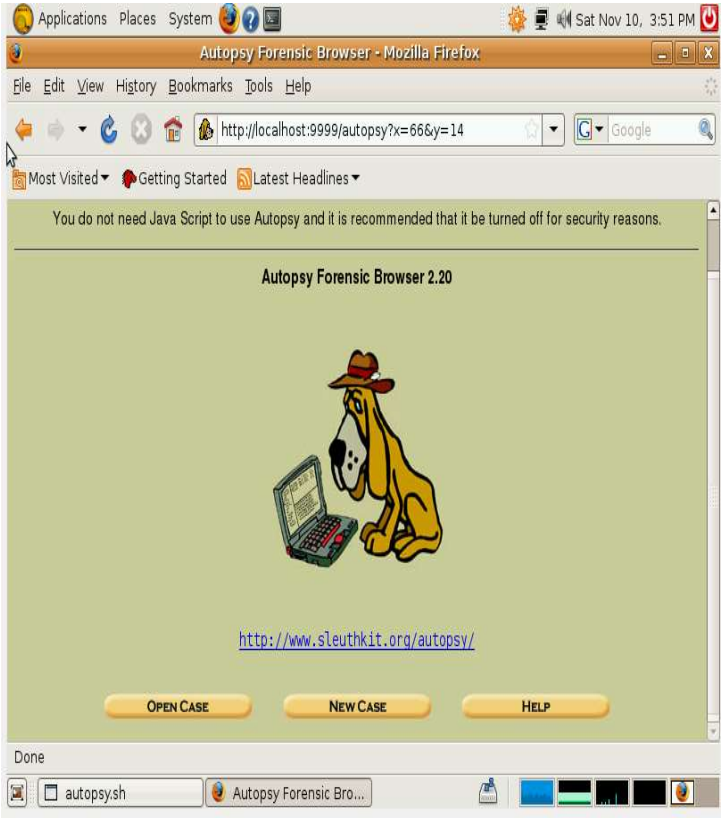
Tipo	Descrição
0X00	Em branco (empty)
0x01	Fat 12, CHS
0x04	Fat 16,16-32MB, CHS
0x05	Microsoft Extended, CHS
0x06	Fat 16, 32-MB- 2GB, CHS
0x07	NTFS
0xb	Fat 32, CHS
0x0c	Fat 32,LBA
0x0e	Fat 16, 32MB-2GB, LBA
0x0f	Microsoft Extended, LBA
0x11	Hidden Fat 12, CHS
0x14	Hiden Fat16, 16-32MB, CHS
0x016	Hiden Fat16, 32MB - 2 GB, LBA
0x1b	Hidden Fat 32, CHS
0x1c	Hidden Fat 32, LBA
0x1e	Hidden Fat 16, 32MB-22GB, LBA

COMO UTILIZAR FERRAMENTAS PADRÃO DA VERSÃO HELIX PARA FORENSE DE DADOS ?

5º Passo, Camada Física, ferramentas:

- Fdisk -> lista partições
- Mmls -> mostra o conteúdo de um volume (tabela de partições incluindo áreas não alocadas)
- File -> identifica arquivos
- Mmstat -> detalhes sobre um volume especifico do disco
- Mmcat -> extrai conteúdo de um volume especifico

- 6º Passo,algumas ferramentas usando o Autopsy:
- tsk_comparedir;
- tsk_gettimes;
- tsk_loaddb;
- tsk_recover;
- fsstat;
- ffind;
- fls;
- icat;ifind; ils; istat;
- jcat; jls;
- img_stat; img_cat;
- disk_sreset; disk_stat;
- hfind;
- cactime;
- sorter;
- sigfind;



COMO UTILIZAR FERRAMENTAS PADRÃO DA VERSÃO HELIX PARA FORENSE DE DADOS ?

7º Passo, Camada de Metadados, ferramentas:

- **lls -> detalhes sobre os inodes**
- **lstat -> informações sobre um inode especifico**
- **lcat -> mostra o conteúdo de um bloco alocado a um inode**
- **lfind: determina que inode encontra-se alocado para um bloco em um arquivo de imagem**

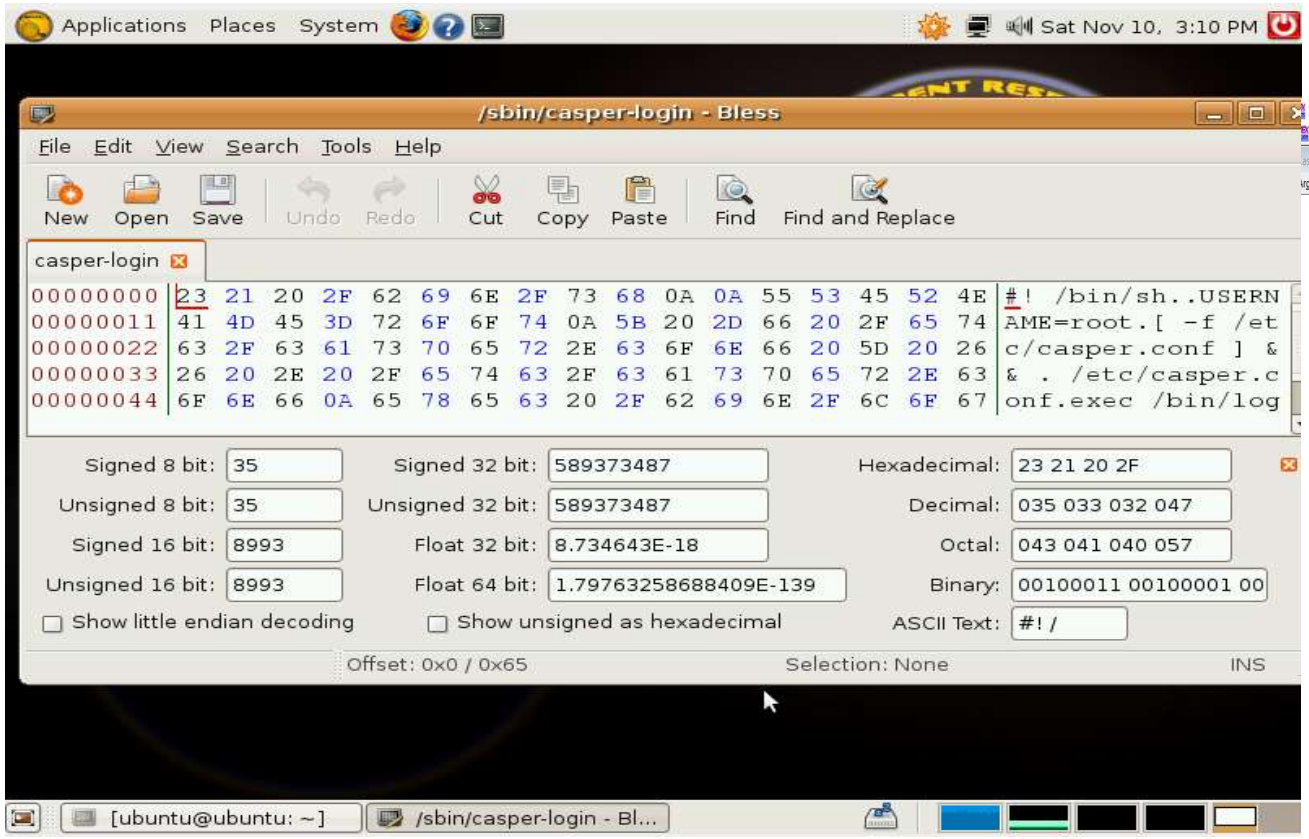
8º Camada de Interface Humana:

- **ffind -> busca por nomes de arquivos em áreas alocadas e não alocadas;**
- **fls -> lista nomes de arquivos alocados e deletados em um diretório**

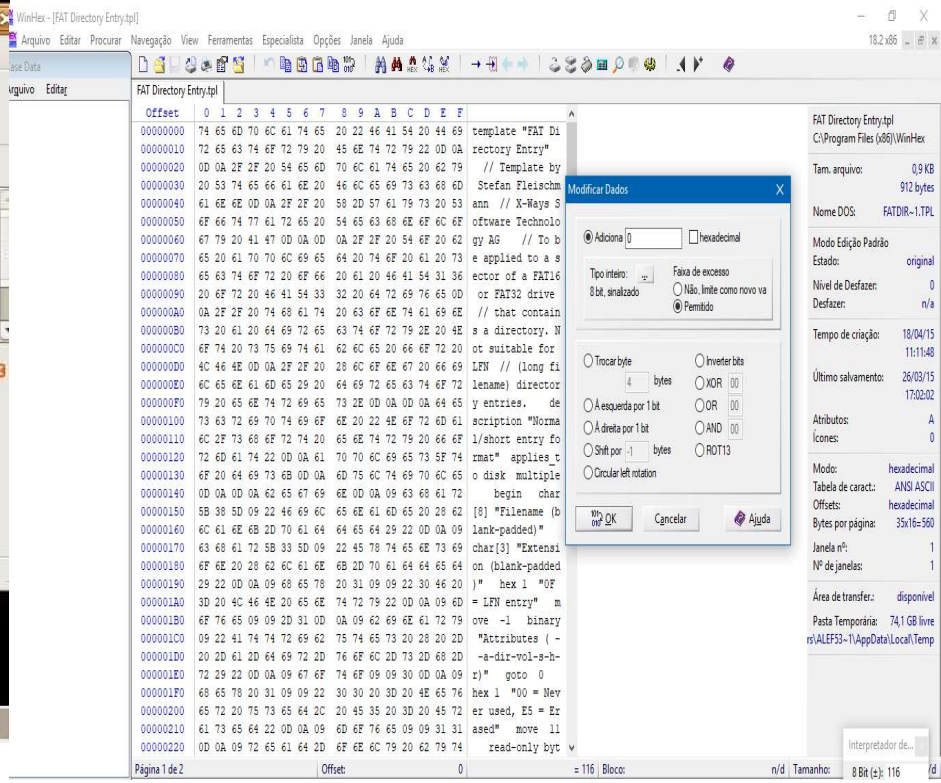
9º Passo, Camada de Dados, ferramentas:

- **blkcat -> extraí o conteúdo de uma unidade específica**
- **blkls -> extrai o conteúdo de espaço não alocado do FS**
- **blkstat -> mostra as estatísticas sobre uma dada unidade**
- **Blkcalc -> calcula onde o dado no espaço não alocado extraído do blkls existia na imagem do disco.Utilizado quando a evidência procurada está na área de espaço não alocado**

EDITANDO CABEÇALHOS PARA RECUPERAÇÃO DE ARQUIVOS OU PARTIÇÕES CORROMPIDOS OU EXCLUÍDOS



No Linux com Bless



No Windows com WinHex

REFERÊNCIAS:

- https://monografias.brasilescola.uol.com.br/computacao/forense-computacional-tecnicas-para-preservacao-evidencias-coleta-analise-artefatos.htm#capitulo_4.1
- https://pt.wikipedia.org/wiki/Computa%C3%A7%C3%A3o_forense
- https://pt.wikipedia.org/wiki/Ci%C3%AAncia_forense
- http://www.ciberforense.com.br/ferramentas/
- https://blog.ipog.edu.br/tecnologia/principais-ferramentas-utilizadas-na-investigacao-forense-computacional/
- http://www.sleuthkit.org/autopsy/download.php
- https://pt.wikipedia.org/wiki/Fun%C3%A7%C3%A3o_hash
- Desvendando a Computação Forense -