

# **Aula 04**

# **Forense Computacional**

## **Investigação Forense II**

✓ Equipamentos

# Equipamentos

---

- ✓ O **FREDDIE** foi desenvolvido para o uso no local onde as cenas dos crimes ou incidentes eletrônicos ocorreram. Para adquirir as evidências digitais, o perito remove o Disco Rígido do sistema suspeito e o pluga no FREDDIE, que faz a captura diretamente do HD e dos storages IDE/EIDE/ATA/SATA/ATAPI/SCSI I/SCSI II/SCSI III. O FREDDIE também é capaz de suportar disquetes 3½ bem como CD-ROM e DVD.



\$7,999.00

# Equipamentos

---

- Placa mãe i7 com chipset Intel X58 / ICH10R
- CPU Intel i7 920 (Quad Processor), 2.66 Ghz, 8M Cache, 4.80 GT/s Intel® QPI
- Slots 3 x PCI-Express (x16), 1 x PCI-Express (x1), 2 x PCI
- Canal triplo de memória 6 GB DDR3-1333
- Nvidia GT240 PCI-Express Video Card (512MB) com HDMI saída de monitor dupla
- Adaptadores duplos 10/100/1000 Mbs rede Gigabit Ethernet
- 8 controles de canais de áudio de alta definição
- 6 Portas (6 Drives) primárias 3.0 Gb/s Serial ATA (SATA) controles (1 Back Mounted)
- 2 portas (2 Drives) Marvell PCIe SATA 6.0 Gb/s Controller
- 2 portas PS/2 (Teclado e mouse)
- 2 portas traseiras USB 3.0/2.0
- 7 portas USB 2.0/1.x: 6 portas traseiras, 1 porta frontal (Com proteção de escrita)
- 1 porta traseira FireWire IEEE 1394a (400 MB/s)
- 1 porta traseira FireWire IEEE 1394b (800 MB/s) Ports

- Hardware bloqueador de escrita Digital Intelligence UltraBay:
  - Drive Bloqueador de escrita integrado IDE, SATA, SCSI e USB;
- Bloqueador de escrita Digital Intelligence UltraBlock USB
- Cartão de leitura forense de mídia Digital Intelligence – um cambiável Leitura-Apenas/Leitura -Escrita (MSC, MS Pro, SMC, CFC, MD, XD, SDC e Memória MMC (Memory Card Compatible))
- 1 x 150 Gb 10,000 RPM 3.0 Gb/s SATA Hard Drive in Shock-Mounted Tray – OS Drive
- 1 x 1.5 Tb 7200 RPM 3.0 Gb/s SATA Hard Drive in Shock-Mounted Tray – Data Drive
- Baia para HD removível 2 x Shock Mounted SATA (Capacidade IDE)
- Combo Drive BD-R/BD-RE/DVD ± RW/CD ± RW Blu-ray Burner Dual-Layer
- Drive para Disquete USB 3 1/2" com interruptor de proteção de escrita.

# Equipamentos

---



## FRED-RM (Forensic Recovery of Evidence – Rackmount Module)

- ✓ O modulo FRED-RM tem a mesma funcionalidade de processamento da evidência digital de um sistema FRED, mas está integrado a um rackmount. Ele também é capaz de adquirir dados de discos rígidos e dispositivos **IDE/EIDE/ATA/ATAPI/SATA**. É equipado com o protetor de escrita UltraBay, usado para aquisição forense (bloqueado à escrita) de dispositivos SCSI, Parallel IDE e Serial ATA.
- ✓ O módulo FRED-M RAID Array oferece acesso em alta velocidade, a 16 TB de dados (14 TB em RAID-5 com Hotspare). Esse módulo possui 16 baias para discos e 3U de tamanho, com 16 Discos Rígidos de 1 GB, 7.200 RPM em Hotswap com gavetas removíveis. <http://forensedigital.com.br/product/fred-m/>

# Equipamentos

---



## UltraBlock Forensic Card Reader

O Cartão de leitura forense pode ser usado para ler (e opcionalmente escrever) os seguintes formatos de cartão:

- Compact Flash Card (CFC)
- MicroDrive (MD)
- Memory Stick Card (MSC)
- Memory Stick Pro (MS Pro)
- Smart Media Card (SMC)
- xD Card (xD)
- Secure Digital Card (SDC and SDHC)
- MultiMedia Card (MMC)

Com adaptadores (não fornecidos de fábrica) o cartão de leitura suporta ainda cartões TransFlash, Mini SD e Micro SD.

<http://forensedigital.com.br/product/ultrablock-forensic-card-reader-and-writer/>

## Tableau T4 Forensic SCSI Bridge



O **T4** escaneia automaticamente o SCSI bus para encontrar equipamentos SCSI, evitando que o usuário se preocupe com identidades SCSI.

O equipamento inclui tanto interfaces de servidor FireWire 800 e USB 2.0, oferecendo flexibilidade máxima quando conectado ao computador servidor.

O FireWire 800 (1394B) oferece a melhor performance e ao mesmo tempo retém a compatibilidade com sistemas FireWire 400 (1394A).

Já o USB 2.0 oferece flexibilidade por suportar computadores que não possuem FireWire, mas possuem interface USB 2.0 ou USB 1.1.

# Equipamentos

## TABLEAU T35es



O **T35es** eSATA Forensic Bridge suporta nativamente aquisições de bloqueios de escrita de drives SATA e IDE sem necessidade de cabos especiais ou adaptadores. Assim como em todos as forensic bridges da Tableau, o T35es reconhece e vence regiões HPA (Host Protected Area) ou DCO (Device Configuration Overlay). Não há mistério em sua utilização: basta ligá-lo na tomada e começar a coletar evidências.

# Equipamentos

## FAR (Forensic Archive & Restore)

O backup das evidências ou pastas é feito pelo FAR em locais de rede ou anexos locais de HDs, englobando, automaticamente o conteúdo de uma série de discos em diferentes mídias.

O software realiza verificação de hashes MD5 e SHA1 para validar o arquivo.

A unidade também imprime etiquetas (incluindo seu logotipo) diretamente no DVD ou CDROM media.

- ✓ Capacidade de DVD: 100
- ✓ Capacidade de backup por semana: 3TB/ 780 DVDs
- ✓ Número de gravadores de DVD: 1
- ✓ Tipo de Gravador: Plextor PX716A
- ✓ Unidade de Rack Ocupadas: 6U
- ✓ Sistema Operacional PC: XP Pro, Server 2003
- ✓ Requisitos de Sistema do PC: Intel Pentium 4, 3GHz ou mais, 1GB de memória RAM





# Equipamentos

## XACT

**XACT** é uma solução completa que inclui hardware, software e cabos – todas os itens necessários para acessar de telefones a cartões de memória. (Suporta 202 tipos de aparelhos)

- ✓ Dumps de memória
- ✓ Acesso a conteúdo protegido ou deletado
- ✓ Procedimento uniforme para todos os aparelhos suportados
- ✓ Todos os hardwares necessários incluídos
- ✓ Suporte a memória interna e mídia removível
- ✓ Valores de hash da imagem da memória
- ✓ Decodificador automático do conteúdo da memória
- ✓ Reconstrução das estruturas lógicas de dados
- ✓ Reconstrução de dados apagados
- ✓ Apresentação dos dados em aplicações .XRY
- ✓ Ferramentas para análises manuais
- ✓ Poderosa função de pesquisa
- ✓ Diferença binária
- ✓ Exportação de dados para análises aprofundadas.



# Equipamentos

## Image MASter Solo 4



<http://forensedigital.com.br/product/image-masster-solo-4/>

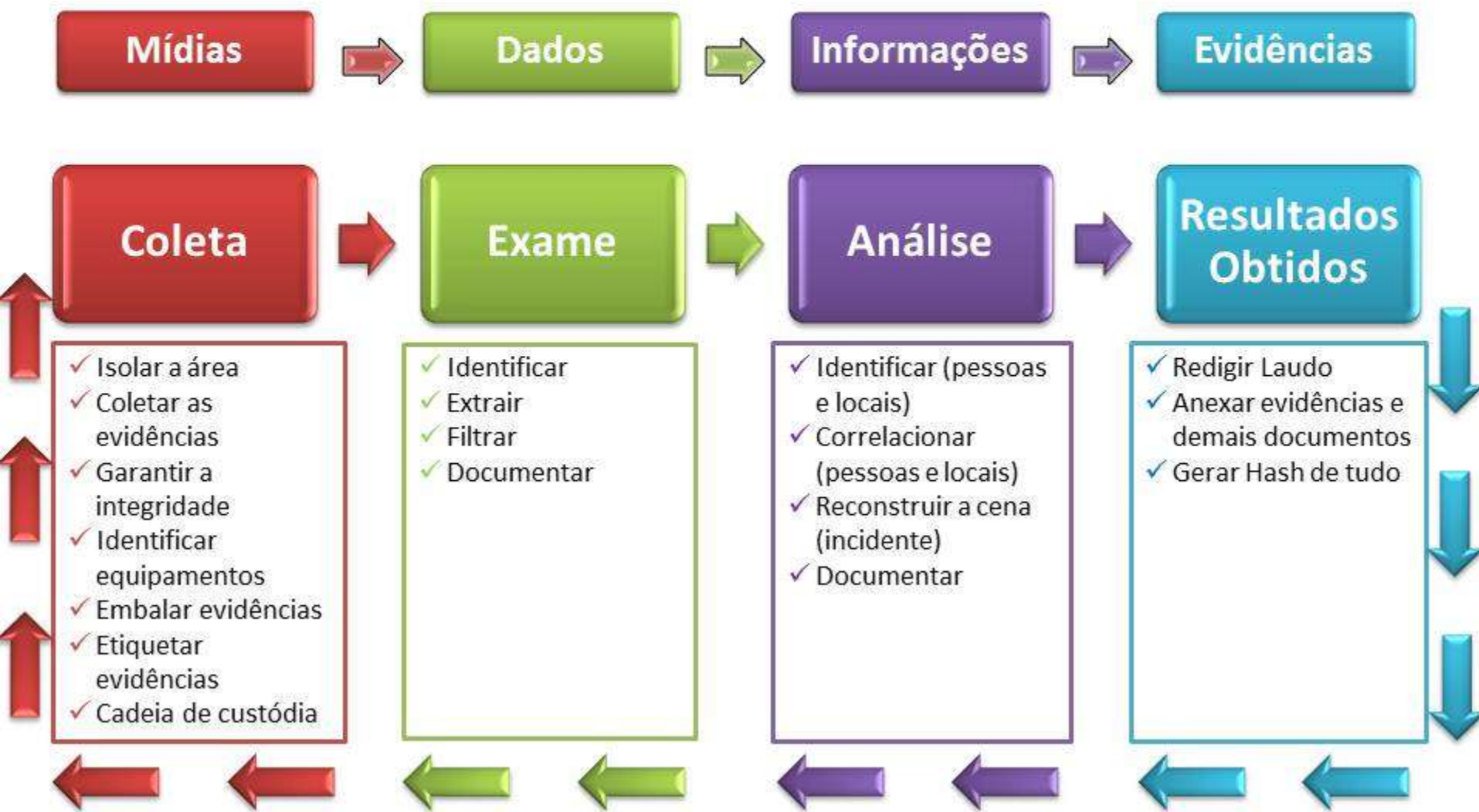
## Detector de pornografia digital

A empresa americana Paraben, sediada em Utah e especializada em tecnologia forense digital, anunciou o lançamento de um pendrive Detector de Pornografia o gadget foi projetado para obter informações digitais e está sendo vendido pela [E-Net Security Solutions](#).

O Detector de Pornografia chega ao Brasil ao preço de R\$550 e será vendido nas grandes redes varejistas, pelo [site](#) ou pelo telefone (41) 3014-3101




# Ciclo de uma investigação





# Coleta Live Windows

WinTaylor 2.1



## WinTaylor for **caine**

Welcome to WinTaylor, select your favourite forensic tools

**CHOOSE THE OUTPUT DIRECTORY FIRST!**  
**!!! DIRECTORY NAME WITH NO SPACES !!!!**

c: \

- C:\
- Forense
- wintaylor2.1**
- Programs

**NirSoft**  
NirsoftMegaReport

**HELP**

The Report file is:

**System Info** **WinAudit** **DriveManager** **Testdisk**

**FTK Imager** **PC On/Off** **Whois** **Lan Scanner**


**Hex Editor** **Photorec** **RAM Dump** **Recuva**

**USB Write Blocker** **USB Devices** **File Analyzer** **More Tools**

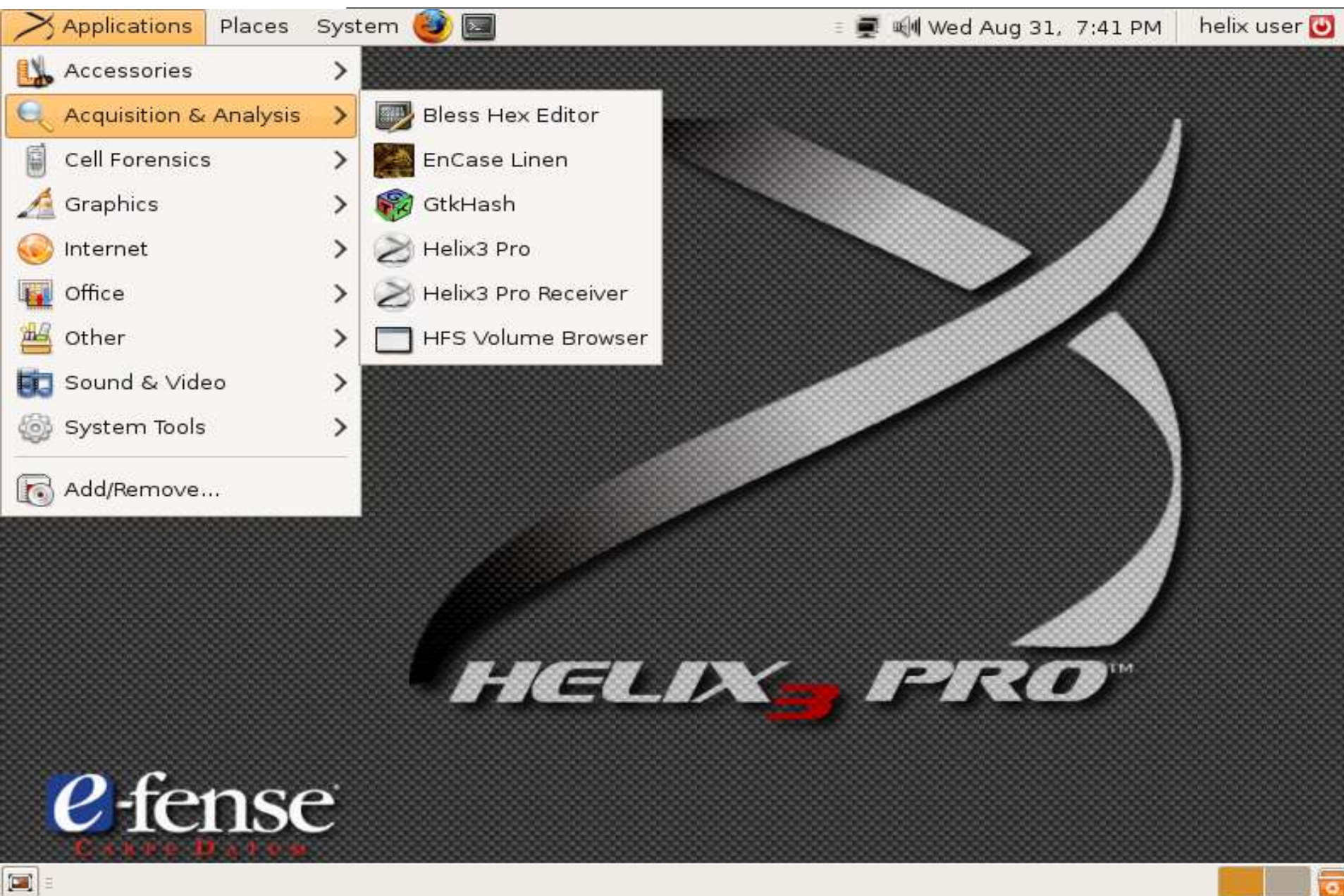
**Hash Calculator** **Take a snapshot**

<http://www.caine-live.net>

**About** **Exit**



# Coleta Live & Post-Morte Linux & Windows







Info



Acquire



Hash



Search

## System



Windows Vista (64 Bit) (Service Pack 1 )



Volatile Data

## Disks



ST9500420AS 0006HPM1  
466 GB PhysicalDrive0



C:\  
401 GB



F:\ Helix3Pro  
690 MB

## Memory



Physical: 5,80 GB



## Acquire Volatile Data:

Start Acquisition



### Network



**ARP table**- Show the converted Internet Protocol(IP) address for corresponding physical network address. This shows computers that are connected to a networked machine.



**Interface tables** - List what interfaces are in use on the system and what the individual MAC address is for each of them.



**The routing table**- List the set of rules, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed.



**Network statistics and connections**- Display network connections (both incoming and outgoing), with processes and executable paths associated to each connection.



### System



**Drivers** - List of all installed system drivers.



**Volume Information** - List all of the drives installed on the system including their sizes, file systems.




**Environment variables** - Get a hardware profile for the system. Includes computer name, operating system info, processor info, timezone, uptime.



**Installed Applications**- List all of the installed applications.




**User Info** - Show all the information about the current user.

  
Info

  
Acquire

  
Hash

  
Search


# System


 Windows Vista (64 Bit) (Service Pack 1 )

 Volatile Data

# Disks


 ST9500420AS 0006HPM1  
466 GB PhysicalDrive0

 C:\  
401 GB

 F:\ Helix3Pro  
690 MB

# Memory

 Physical: 5,80 GB

 **Acquire Device:** System Memory

Output Type: RAW

Examiner: Paulo Neukamp

Case Number: 00001-2011

Item Number: 001

Description: Notebook HP Pavilion DV4-2090br

Notes: Maquina suspeita de armazenar conteúdo pornografico e pedofilia.

Segmentation: Single File

Read Size: 512

Hash Protocol: ☐ MD5 ☐ SHA1 ☒ SHA256 ☐ SHA512

Image Disk to Attached Device

C:\Dados\Unisinos\2011-2

Select...

-

+

Start Acquisition



- ✓ Em uma cena em que algum equipamento tenha sido comprometido, o que devemos fazer primeiro?
- ✓ Dados voláteis?
- ✓ Dados não Voláteis?
- ✓ Coleta Live ou Post-Mortem?
- ✓ Coleta Live Windows – Linux!
- ✓ Coleta Linux – Kit de Ferramentas e scripts!
- ✓ Coleta Windows – WinTaylor - Distro Caine!

- ✓ Utilizar Pendrive ou CD com Kit de Ferramentas pré-compiladas;
- ✓ Coletar dados voláteis:
  - Data/Hora do sistema;
  - Identificação do equipamento;
  - Sistema operacional;
  - Estado da memória;
  - Tempo de utilização do equipamento;
  - Tempo de funcionamento;
  - Usuário(s) logado(s);
  - Configuração IP;
  - Estado das conexões;
  - Tabela de roteamento;
  - Utilização do(s) disco(s);
  - Processos em execução,
  - Lista de todos os arquivos do equipamento;
  - Hash de todos os arquivos;

- ✓ Criar o seu próprio kit de coleta live para equipamentos Linux;
  - ✓ Pode ser um script que faça todas as operações de forma automatizada;
  - ✓ Deve ter uma pasta com todas as ferramentas necessárias;
  - ✓ Os dados coletados não devem ser armazenados na mídia investigada;
  - ✓ Gerar hash de tudo;