Minicurso Forense Digital

UniInfo-2012

Roteiro

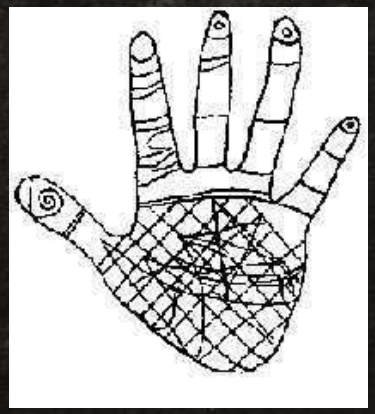
- ✓ Apresentação
- ✓ Histórico
- ✓ O que é Forense Computacional?
- ✓ Principais desafios da Forense Computacional
- ✓ Crime Cibernético
- ✓ Etapas de uma Investigação
- ✓ Passos de uma Investigação
- ✓ Análise Viva e Post Mortem
- ✓ Distribuições Linux para Forense
- ✓ Ferramentas Livres e Toolkits para Forense

Apresentação

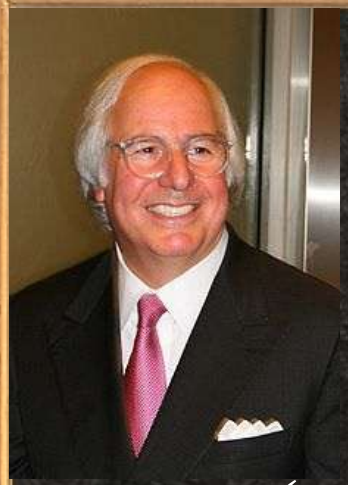
- ✓ **Mais de 15 anos de atuação na área do TI;**
- ✓ **Formando da 1ª turma do curso de Segurança da Informação + MBA em Administração da Tecnologia da Informação;**
- ✓ **Criador e mantenedor da Distro FDTK – Forense Digital ToolKit;**
- ✓ **Um dos autores do Minicurso *"Forense Computacional: fundamentos, tecnologias e desafios atuais" SBSeg 2007;***
- ✓ **Palestrante no 1º Seminário de Segurança da Informação – SENAI –CTAI;**
- ✓ **Um dos autores do Artigo *"Ensino da Forense Digital Baseado em Ferramentas Open Source" ICCYBER 2011;***
- ✓ **Professor do Curso de Segurança da Informação a 4 anos;**
- ✓ **Administrador de infraestrutura;**

Histórico

- **Século 19**
  - **Francis Galton** elabora um estudo complexo sobre as impressões digitais (5%); **(Papiloscopia)**



- **Século 20**
  - **Leone Lattes** descobre que os tipos sanguíneos podem ser divididos em grupos de acordo com caraterísticas próprias; (Genética)
  - http://www.portalsaofrancisco.com.br/alfa/corpo-humano-sistema-cardiovascular/tipos-de-sangue.php
  - **Calvin Goddard** desenvolve um estudo sobre a comparação entre projéteis de armas de fogo. (Balística)



Histórico

Frank Abagnale JR

Catch Me If You Can (2002)

- ✓ **Albert Osborn** - desenvolve uma pesquisa sobre as características e metodologias para análise de documentos;
- ✓ **Hans Gross** - desenvolve o método científico para a realização de investigações criminalísticas.

✓ **1932**

- ✓ No **FBI**, foi organizado um laboratório para prover serviços de análise forense a todos os agentes de campo e outras autoridades legais Americanas.

O que é Forense Computacional?

"Aplicação da ciência física à lei na busca pela verdade em assuntos civis, criminais e de comportamento social, com o fim de que nenhuma injustiça seja feita à nenhum membro da sociedade".

Handbook of Forensic Pathology College of American Pathologists

"Forense Computacional compreende a aquisição, preservação, identificação, extração, restauração, análise e documentação de evidências computacionais, quer sejam componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais."

Warren G. Kruse II & Jay G. Heiser

Desafios da Forense Computacional

- ✓ Ainda é mais uma arte do que ciência;
- ✓ Ainda está em seus estados iniciais de desenvolvimento;
- ✓ Há pouco conhecimento teórico sobre o qual as hipóteses empíricas são baseadas;
- ✓ Há falta de treinamento apropriado;
- ✓ Não há padronização de ferramentas.

Por que Forense Computacional?

- ✓ *"A forense computacional é o equivalente ao levantamento na cena de um crime ou a autópsia da vítima "*. - James Borek
  - ✓ Busca identificar dados em um computador;
  - ✓ Recuperar arquivos deletados, encriptados ou corrompidos em um sistema;
  - ✓ Fundamentar demissões de funcionários que desrespeitam normas organizacionais;
  - ✓ Auxiliar na quebra de contratos que não são respeitados;
  - ✓ Provar fatos;
  - ✓ Fazer cumprir as leis de privacidade.

Crime Cibernético

- ✓ Um crime cibernético é definido como qualquer ato ilegal envolvendo um computador, seu sistema ou suas Aplicações.
- ✓ Para ser tipificado como crime, o ato deve ser intencional, e não acidental.

  - ✓ **Três aspectos:**
    - ✓ Ferramentas do crime;
    - ✓ Alvo do crime;
    - ✓ Tangente do crime;

  - ✓ **Duas categorias:**
    - ✓ Ataque interno
    - ✓ Ataque externo

Exemplos e Motivações

- **Exemplos:**
  - Roubo de propriedade intelectual;
  - Avaria na rede das empresas;
  - Fraude financeira;
  - Invasão de hackers;
  - Distribuição e execução de vírus ou worm.
- **Motivações:**
  - Testes ou tentativas de aprender na prática, por script kiddies;
  - Necessidade psicológica;
  - Vingança ou outras razões maliciosas;
  - Espionagem Corporativa ou Governamental;

Função do Investigador

- ✓ O principal objetivo do investigador forense computacional é determinar a natureza e os eventos relacionados a um crime ou ato malicioso e localizar quem o perpetrou, seguindo um procedimento de investigação estruturado.

- ✓ **4W1H**
  - ✓ **W**hat – Qual;
  - ✓ **W**ho – Quem;
  - ✓ **W**hen – Quando;
  - ✓ **W**here – Onde
  - ✓ **H**ow – Como

Conduta do Investigador

- ✓ A conduta profissional determina a credibilidade de uma investigação forense;
- ✓ O profissional deve demonstrar o mais alto nível de integridade ética e moral;
- ✓ Confidencialidade é uma característica essencial que todo investigador deve possuir;
- ✓ Discutir detalhes dos casos investigados apenas com as pessoas que possuem permissão para tomar conhecimento do processo;

Investigação Forense Computacional

- ✓ Uma investigação Forense Computacional, pode assumir diversas características, dependendo do contexto onde a investigação é realizada.

Passos de uma Investigação

- ✓ Avaliação inicial do caso;
- ✓ Preparar um projeto detalhado;
- ✓ Determinação dos recursos necessários;
- ✓ Identificação dos riscos envolvidos;
- ✓ Coletar as evidências;
- ✓ Investigação das informações recuperadas;
- ✓ Preenchimento do relatório do caso;
- ✓ Conclusão do caso.

  - ➢ O trabalho de processar as evidências é composto de quatro parte básicas, que consistem na Coleta, Análise, Exame e Documentação das mesmas.

Ciclo de uma investigação

Mídias → Dados → Informações → Evidências

Coleta

- ✓ Isolar a área
- ✓ Coletar as evidências
- ✓ Garantir a integridade
- ✓ Identificar equipamentos
- ✓ Embalar evidências
- ✓ Etiquetar evidências
- ✓ Cadeia de custódia

Exame

- ✓ Identificar
- ✓ Extrair
- ✓ Filtrar
- ✓ Documentar

Análise

- ✓ Identificar (pessoas e locais)
- ✓ Correlacionar (pessoas e locais)
- ✓ Reconstruir a cena (incidente)
- ✓ Documentar

Resultados Obtidos

- ✓ Redigir Laudo
- ✓ Anexar evidências e demais documentos
- ✓ Gerar Hash de tudo

Avaliação inicial do caso

- ✓ Situação do caso;
- ✓ Natureza do caso;
- ✓ Questões específicas;
- ✓ Tipo de evidências;
- ✓ Sistema operacional envolvido;
- ✓ Formato do disco;
- ✓ Localização das evidências;
- ✓ Motivações do caso.

Recursos necessários

- ✓ Disponibilidade de profissionais habilitados e com expertise para o caso;
  - Ter certeza de que o perito tenha capacidade, se necessário, de testemunhar em um tribunal;
  - O perito é capaz de explicar a metodologia utilizada ao logo da investigação de forma simples e sem fazer uso de terminologias;
  - O perito é capaz de explicar questões do júri utilizando analogias, como por exemplo, a de arquivos em espaços ocultos (ex. biblioteca);

Recursos necessários (continuação)

- ✓ Disponibilidade dos recursos físicos e lógicos necessários;
  - Mídias esterilizadas (processo documentado);
  - Etiquetas para provas;
  - Câmera fotográfica;
  - Formulário de cadeia de custódia;
  - Envelopes para provas;
- ✓ Definir atribuições de cada membro da equipe;
- ✓ Definir qual perito fará o deslocamento se necessário até o local do incidente;

Local do incidente ou Crime

- ✓ Isolar a área;
- ✓ Fotografar todo o ambiente e os equipamentos detalhadamente (conexões, anotações, telas de equipamentos);
- ✓ Se possível filmar o ambiente;
- ✓ Fazer anotações detalhadas do que está sendo visualizado;
  - ➢ Detalhes como fotografias e objetos pessoais podem auxiliar em descobertas de senhas;
- ✓ De acordo com os quesitos, definir a necessidade de mudar o status dos equipamentos a ser investigados (Coleta Live ou puxar o cabo de força Post-Mortem);

Análise Viva e Post Mortem

- **Dados Voláteis**
  - São informações que ficam armazenados na memória principal do computador. Isso quer dizer que elas possuem um ciclo de vida curto. Esse tipo de análise é chamada de "**Análise Viva**".

- **Dados não-voláteis**
  - Dados não voláteis, são dados que podem permanecer na máquina durante longos períodos de tempo e podem ser recuperados mesmo após a mesma ser desligada. As análises baseadas em dados armazenados em mídia de backup, pendrives, CDs, ou memória auxiliar como um HD, são chamadas de "**Análise Post-Mortem**".

Coleta Live

- ✓ Documentar todas as etapas do processo;
- ✓ Fotografar conexões do equipamento;
- ✓ Utilizar Pendrive com Kit de Ferramentas pré-compiladas;
- ✓ Coletar dados voláteis:

- Data/Hora do sistema;
- Identificação do equipamento;
- Sistema operacional;
- Estado da memoria;
- 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;

Coleta Live - Linux

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 - Windows

Helix3 Pro

File Edit Help

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

Refresh Device List

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
- **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.

Coleta Live - Windows

Helix3 Pro

File Edit Help

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

Refresh Device List

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

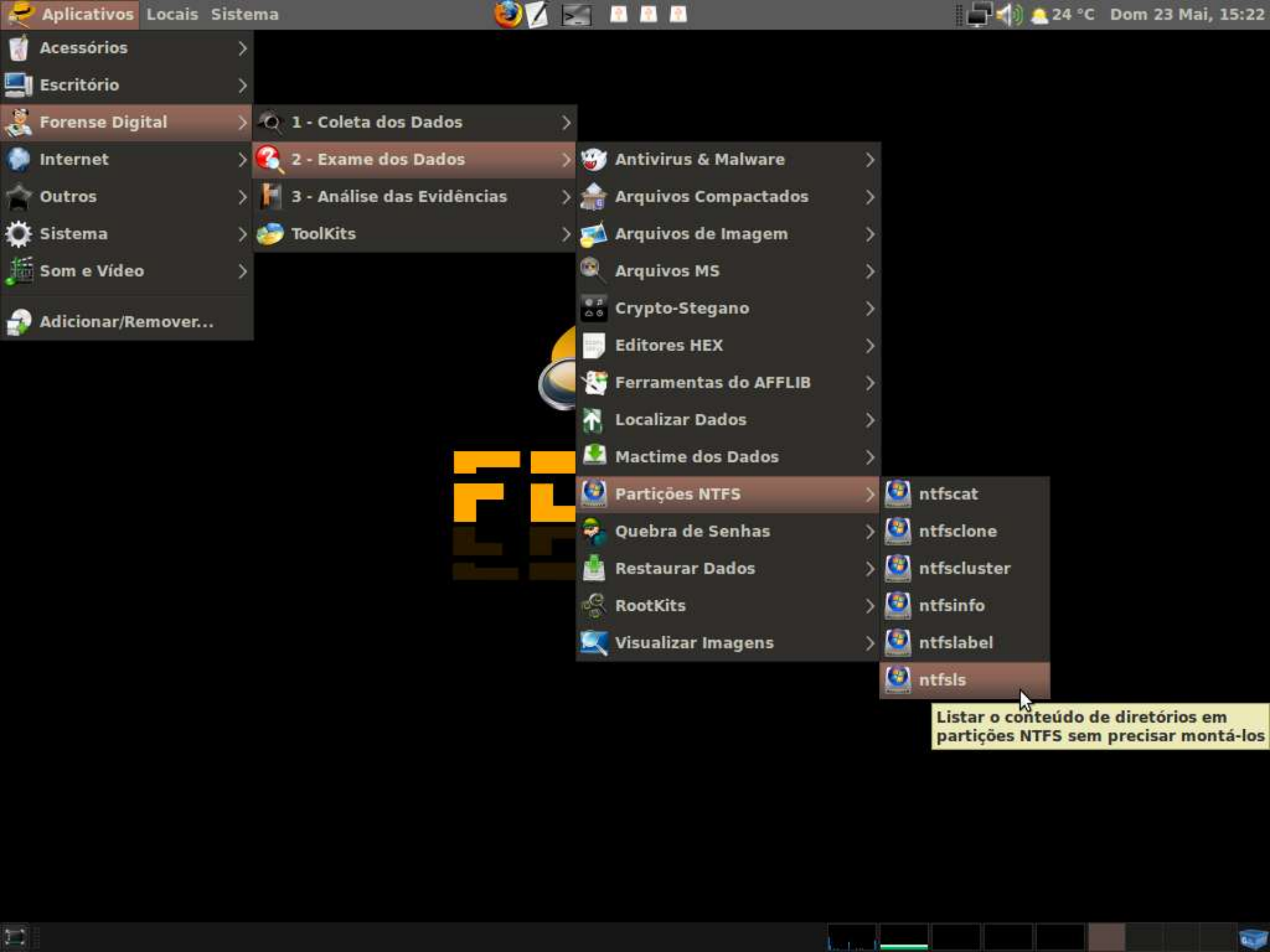
Hash Protocol: ☐ MD5 ☐ SHA1 ☑ SHA256 ☐ SHA512

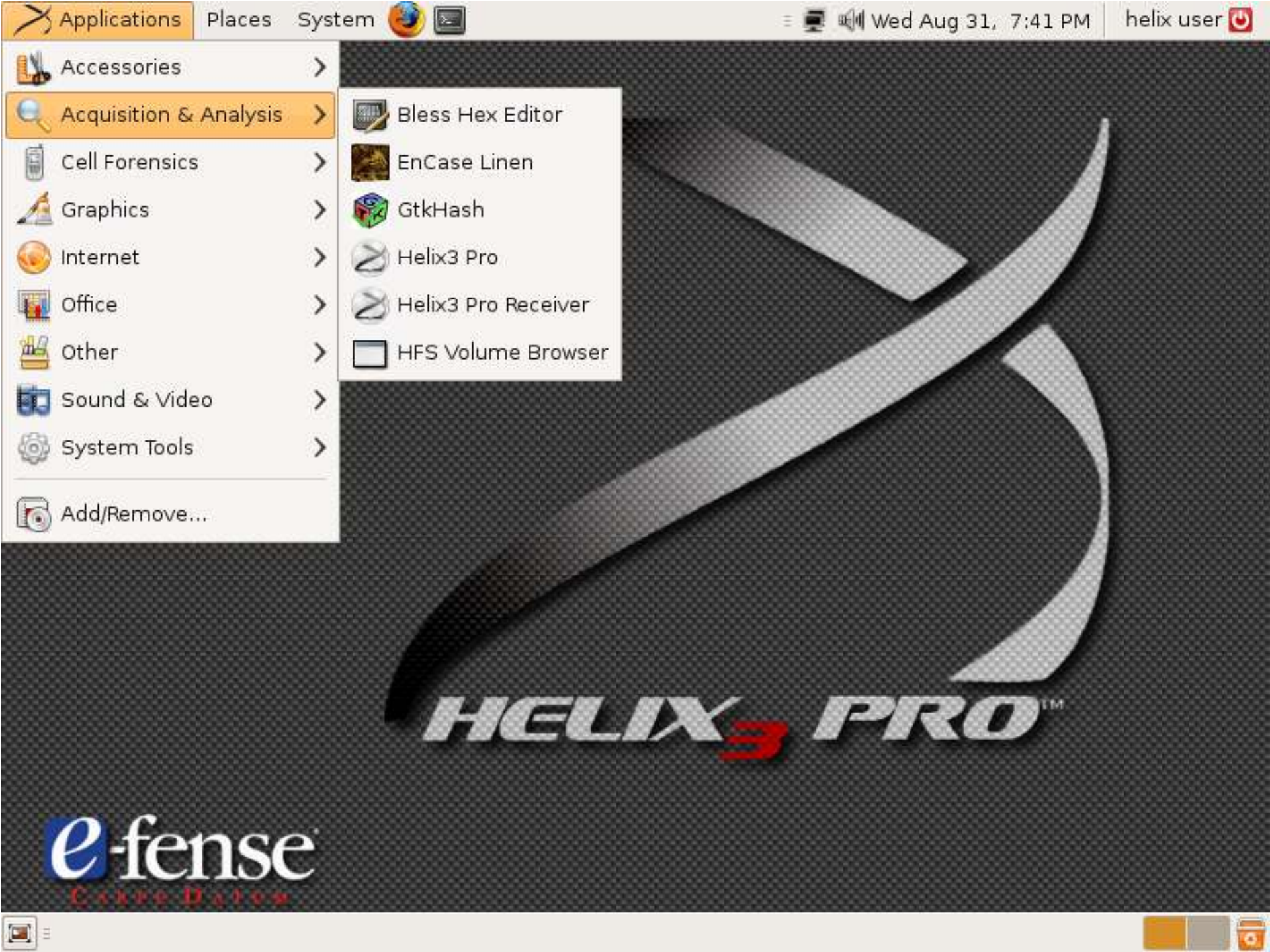
Image Disk to Attached Device | C:\Dados\Unisinos\2011-2 | Select... | − | +

Start Acquisition

Coleta Post-Mortem

- ✓ Documentar todas as etapas do processo (data hora inicial e final);
- ✓ Fotografar TUDO;
- ✓ Abrir equipamento;
- ✓ Fotografar conexões internas e externas do equipamento;
- ✓ Desconectar o(s) disco(s) para cópia (modo somente leitura ou utilizar bloqueador de escrita);
- ✓ Anotar os dados do(s) disco(s) no Formulário de Custódia;
- ✓ Etiquetar o(s) Disco(s);
- ✓ Conectar o(s) Disco(s) a estação forense para realizar 2 cópias bit-a-bit;
- ✓ Embalar, lacrar e etiquetar o(s) disco(s);
- ✓ Fotografar o(s) discos(s) etiquetados;


Aplicativos
Locais
Sistema
24 °C
Dom 23 Mai, 15:22
Acessórios
Escritório
Forense Digital
Internet
Outros
Sistema
Som e Vídeo
Adicionar/Remover...
1 - Coleta dos Dados
2 - Exame dos Dados
3 - Análise das Evidências
ToolKits
Antivirus & Malware
Arquivos Compactados
Arquivos de Imagem
Arquivos MS
Crypto-Stegano
Editores HEX
Ferramentas do AFFLIB
Localizar Dados
Mactime dos Dados
Partições NTFS
Quebra de Senhas
Restaurar Dados
RootKits
Visualizar Imagens
ntfscat
ntfsclone
ntfscluster
ntfsinfo
ntfslabel
ntfsls
Listar o conteúdo de diretórios em partições NTFS sem precisar montá-los


Applications
Places
System
Wed Aug 31, 7:41 PM
helix user
Accessories
Acquisition & Analysis
Cell Forensics
Graphics
Internet
Office
Other
Sound & Video
System Tools
Add/Remove...
Bless Hex Editor
EnCase Linen
GtkHash
Helix3 Pro
Helix3 Pro Receiver
HFS Volume Browser
HELIX3 PRO™
e-fense
Case Data


Accessories
Forensic Tools
Graphics
Internet
Office
Other
Programming
Sound & Video
System Tools
Ubuntu Software Center
Places
System
Log Out caine...
Shut Down...
Caine Interface
Storage Device Manager
Safe Mount
Disk Utility
AIR 2.0.0
Guymager
Autopsy 2.24
Bash Scripts Tools
GtkHash
dvdisaster
Hex Editor
NBTempo
Photorec
Testdisk
TSK GUI
XHFS
XMount
XSteg
SUPERNOVA
ChangeKeyboardLayout
Caine Interface
USA
Fri Nov 18, 4:19 PM


evidence
Install DEFT Linux 7
LXTerminal
computer forensics
network forensics
deft 7
incident response
Accessories
DEFT
Graphics
Internet
Office
Services
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analisys tools
Antimalware tools
Carving tools
Hashing tools
Imaging tools
Mobile Forensics
Network Forensics
OSINT tools
Password recovery
Reporting tools
Disk Utility
File Manager
GParted
Midnight Commander
Mount ewf
MountManager
Wipe
Xmount
14:05

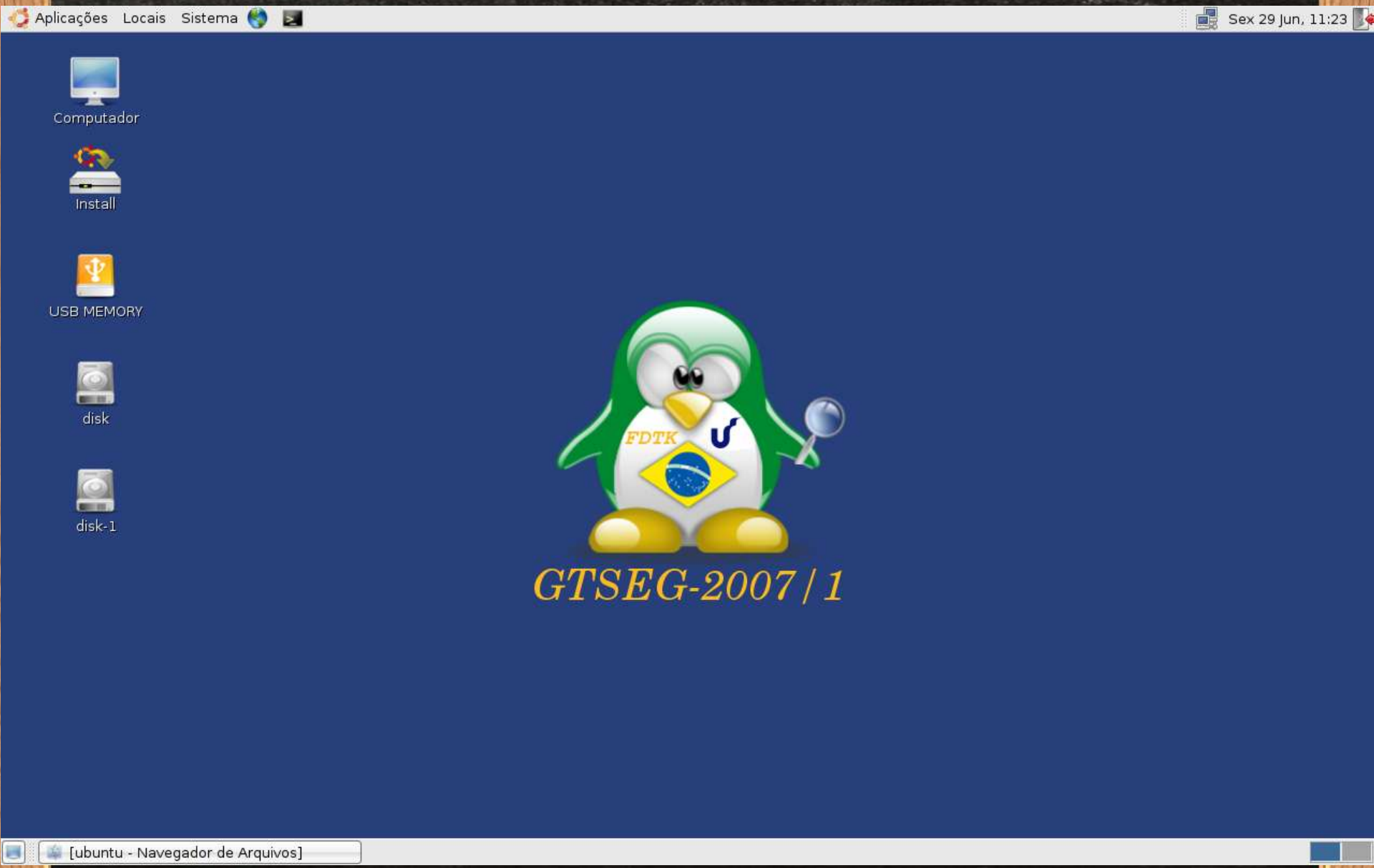
Distribuições linux para Forense

- ✓ FDTK – Forense Digital ToolKit
- ✓ Helix
- ✓ CAINE - Computer Aided INvestigative Environment
- ✓ DEFT - Digital Evidence Forense Toolkit
- ✓ REMnux
- ✓ Backtrack

Ferramentas Livres e Toolkits para Forense

- ✓ **Toolkits**
  - ✓ Autopsy;
  - ✓ Framework Volatility;
  - ✓ Sleuth Kit;
  - ✓ PTK;
  - ✓ DFF;
- ✓ **Ferramentas**
  - ✓ foremost;
  - ✓ dcfldd;
  - ✓ john the ripper;
  - ✓ shred;
  - ✓ pasco;
  - ✓ etc, etc, etc...


FDTK-UbuntuBr


Aplicações Locais Sistema
Sex 29 Jun, 11:23
Computador
Install
USB MEMORY
disk
disk-1
FDTK
GTSEG-2007 / 1
[ubuntu - Navegador de Arquivos]

Testar o Ubuntu sem qualquer mudança no seu computador

Instalar o Ubuntu

Verificar os discos para defeitos

Teste de memória

Inicializar pelo primeiro disco rígido

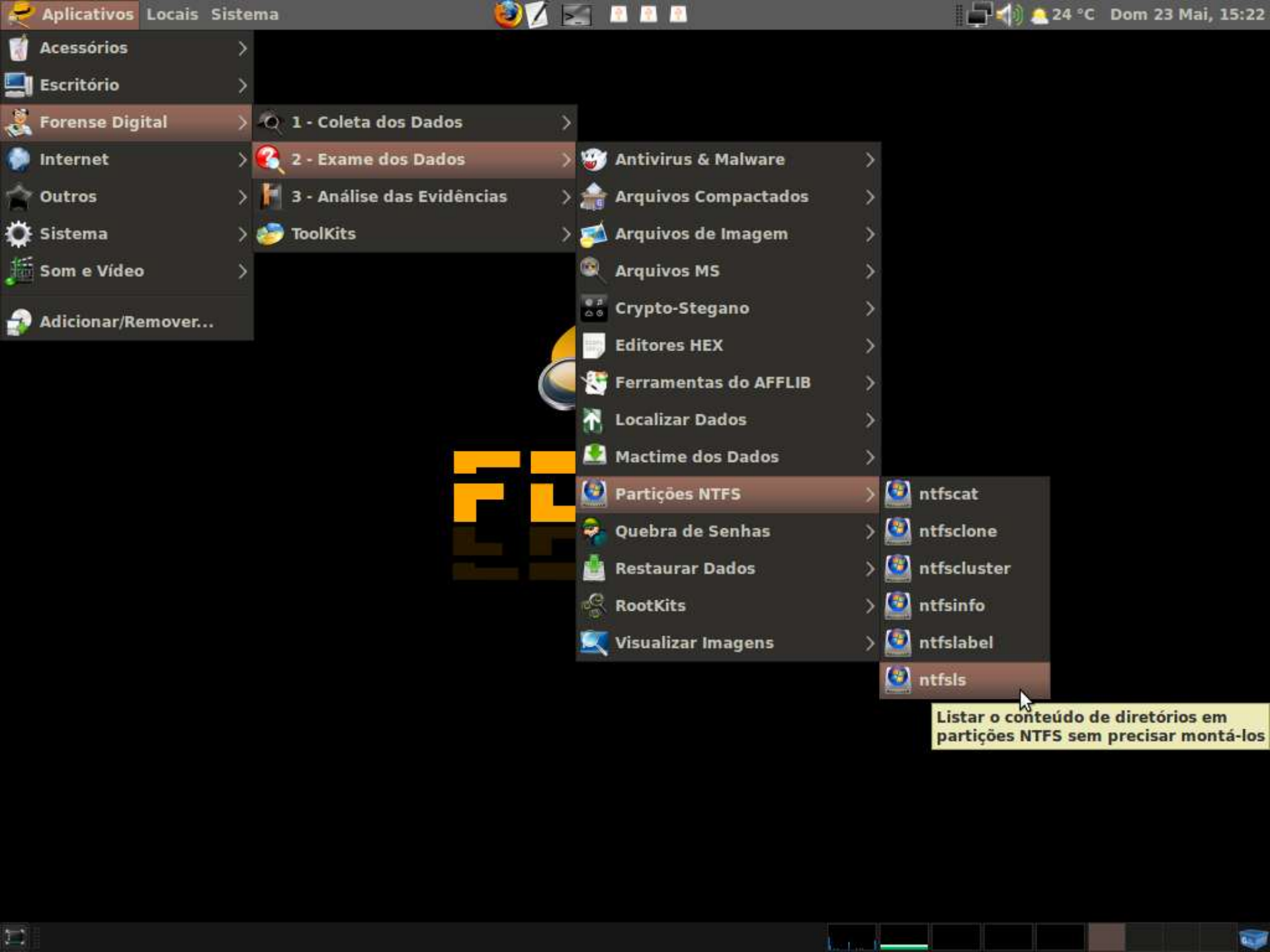
Pressione F4 para selecionar modos alternativos de inicializar e instalar.

F1 Ajuda F2 Idioma F3 Mapa de teclas F4 Modos F5 Acessibilidade F6 Outras Opçõe


```
Running /scripts/init-premount          ok
Mounting root file system...
Running /scripts/casper-premount        ok
Running /scripts/casper-bottom
Moving mount points...                  ok
Adding live session user...
```


Configura Teclados


ptk_config


Aplicativos
Locais
Sistema
24 °C
Dom 23 Mai, 15:22
Acessórios
Escritório
Forense Digital
Internet
Outros
Sistema
Som e Vídeo
Adicionar/Remover...
1 - Coleta dos Dados
2 - Exame dos Dados
3 - Análise das Evidências
ToolKits
Antivirus & Malware
Arquivos Compactados
Arquivos de Imagem
Arquivos MS
Crypto-Stegano
Editores HEX
Ferramentas do AFFLIB
Localizar Dados
Mactime dos Dados
Partições NTFS
Quebra de Senhas
Restaurar Dados
RootKits
Visualizar Imagens
ntfscat
ntfsclone
ntfscluster
ntfsinfo
ntfslabel
ntfsls
Listar o conteúdo de diretórios em partições NTFS sem precisar montá-los

CONTATOS

- ✓ www.fdtk.com.br
- ✓ professor.unisinos.br/pneukamp

- ✓ pneukamp@unisinos.br
- ✓ pneukamp@gmail.com
- ✓ paulo@fdtk.com.br