

**INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA**
RIO GRANDE DO NORTE

Coleta, Identificação e Extração de Dados (Data Carving) em Mídias e em Redes

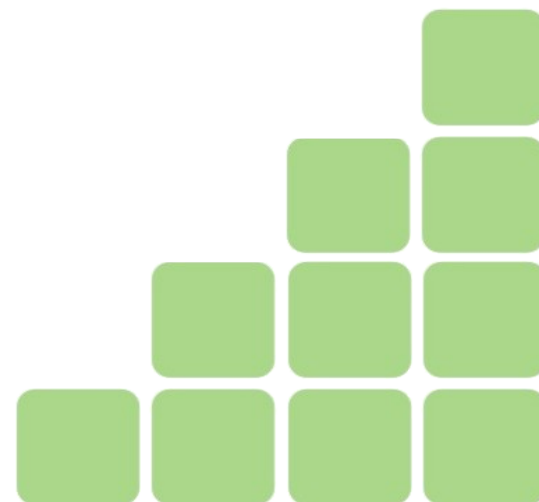
27/11/2010

Ricardo Kléber M. Galvão
ricardo.galvao@ifrn.edu.br
www.ricardokleber.com



REDE FEDERAL
DE EDUCAÇÃO
PROFISSIONAL
E TECNOLÓGICA
1909-2009

GTS'16 :: UNISINOS :: São Leopoldo/RS



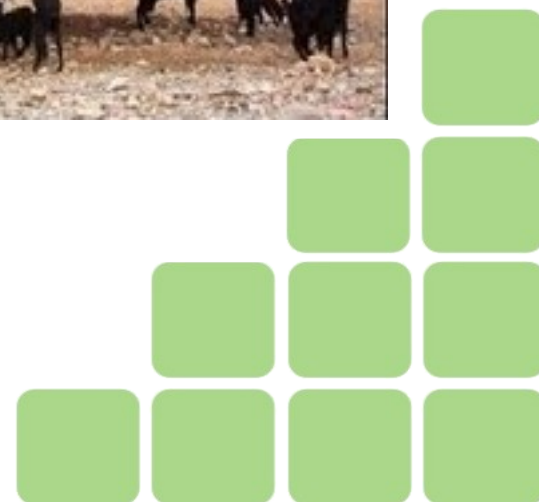
Contextualizando...

Objetivos !!??

Qual o melhor pé-de-cabra?



Conhecer as ferramentas
para fazer a melhor escolha



Contextualizando...

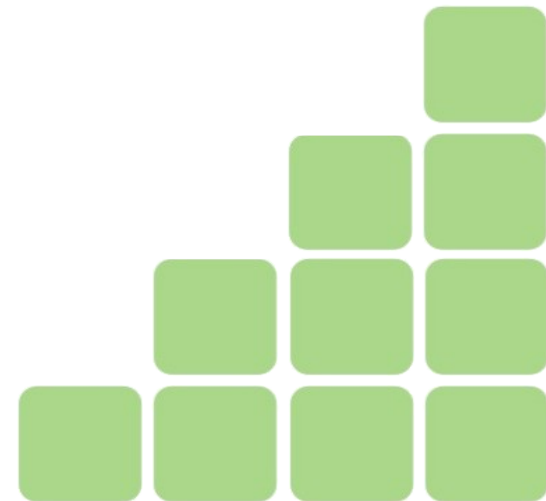
Objetivos !!??

- *A contestação de técnicas periciais utilizadas (quando provada tecnicamente) pode inviabilizar todo o esforço pericial...*
- *Na maioria das vezes é mais fácil provar que as técnicas utilizadas foram inadequadas que provar que o acusado é inocente...*



Boaz Guttman (www.4law.co.il)

**Conhecer as ferramentas
para fazer a melhor escolha**



Contextualizando...

Análise Forense



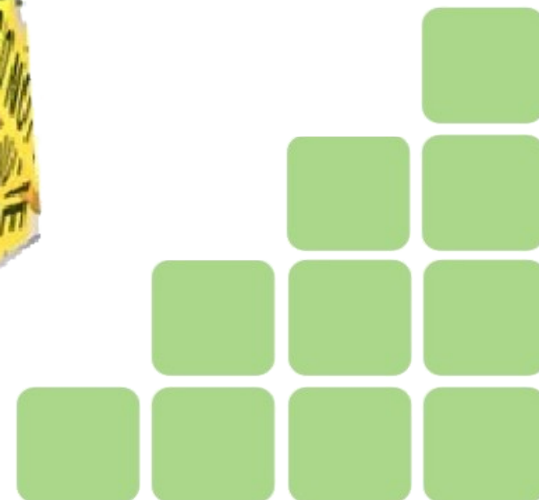
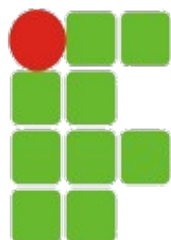
“A aplicação de princípios das ciências físicas ao direito
na busca da verdade em questões cíveis, criminais
e de comportamento social
para que não se cometam injustiças
contra qualquer membro da sociedade”

(Manual de Patologia Forense do Colégio de Patologistas Americanos, 1990).

- Levantar evidências que contam a história do fato:

- Quando?
- Como?
- Porque?
- Onde?

- **Normas e Procedimentos**

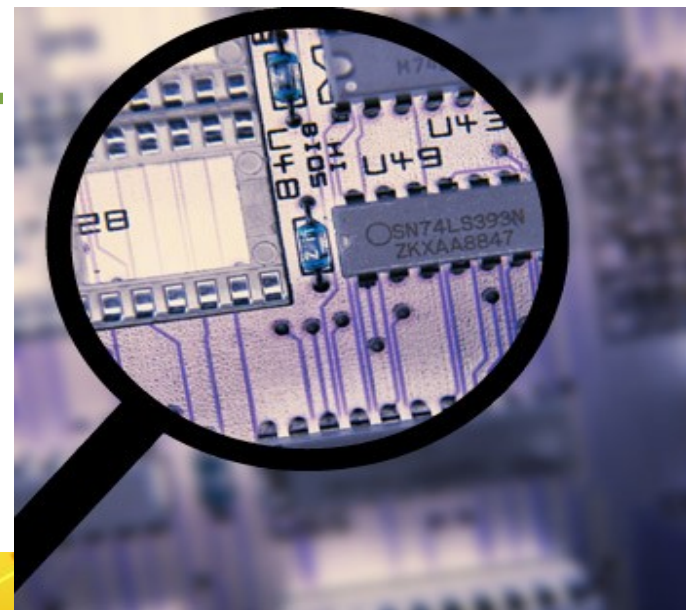


Contextualizando...

Análise Forense Computacional

Conceitos Importantes

- Evidências
 - **Não-Voláteis x Voláteis**
- Tipos de Análise:
 - ***In Loco***
 - ***Post mortem***
- **Recuperação**
- **Extração**



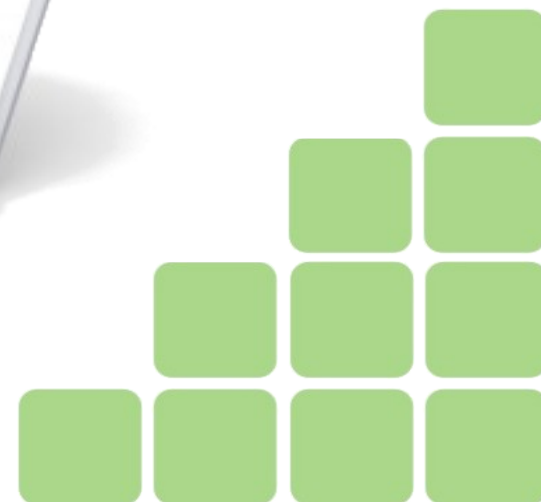
Contextualizando...

Análise Forense Computacional



Principais Etapas

- **Aquisição**
- Identificação
- Avaliação
- Apresentação



Contextualizando...

Definição do Objeto da Perícia

O que Coletar/Analisar ?

- **Mídias**

- Hds, pendrives, cds, dvds...

- **Dispositivos não convencionais**

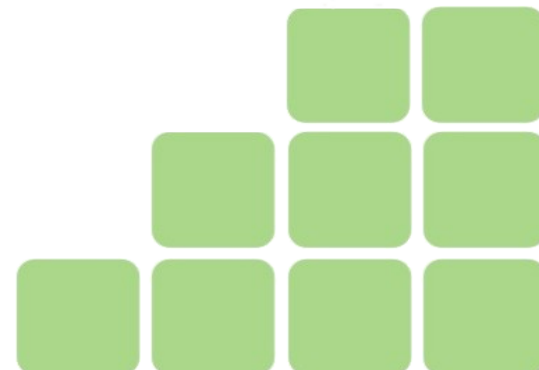
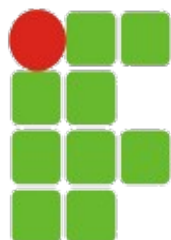
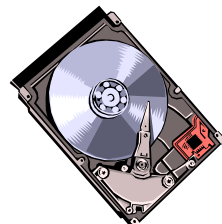
- Câmeras digitais, óculos/relógios/pulseiras...
(com dispositivos de armazenamento).

- **Dados trafegando na rede**

- Em investigações de tráfego de informações
- Também com equipamentos ligados

- **Dados em memória**

- Em análises com equipamentos ligados



Antes do Processo de Extração

Coleta em Mídias

- Ferramenta **dd** (ou evolução dela)
 - Linux (nativo em todas as principais distribuições)
 - Windows (<http://www.chrysocome.net/dd>)

dd if=origem of=destino

- Ex.: Geração da Imagem (partição hda1 para arquivo imagem.dd):

```
# dd if=/dev/hda1 of=imagem.dd
```

*Importante: o dd (e ferramentas semelhantes) fazem a cópia **bloco a bloco** (e não bit-a-bit). O sistema operacional disponibiliza os dados para as ferramentas em forma de blocos (ou clusters, em sistemas de arquivos Microsoft). Os blocos mais comuns têm 4KB. (Agradecimento a Eriberto Mota)*



Antes do Processo de Extração

Coleta em Mídias

- Apesar de ser a maneira mais simples e eficiente de realizar a duplicação, o utilitário dd não oferece algumas funcionalidades importantes;
- O **dd_rescue** serve para realizar aquisições de mídias com problemas (em algumas situações o dd é interrompido ao encontrar erros na mídia);
- O **sdd** realiza aquisições mais rápido do que o dd, quando o tamanho de bloco dos dispositivos de origem e destino são diferentes;
- O **rdd** foi desenvolvido pelo Netherlands Forensic Institute (NFI) e sua documentação indica que ele é bem mais robusto em relação a tratamento de erros, divisão de arquivos (split) e hash.
- O **dcfldd** possui um log de toda a operação, faz divisão da imagem (split) e permite verificar diretamente a integridade da operação através de vários algoritmos de hash.



Antes do Processo de Extração

Coleta em Mídias

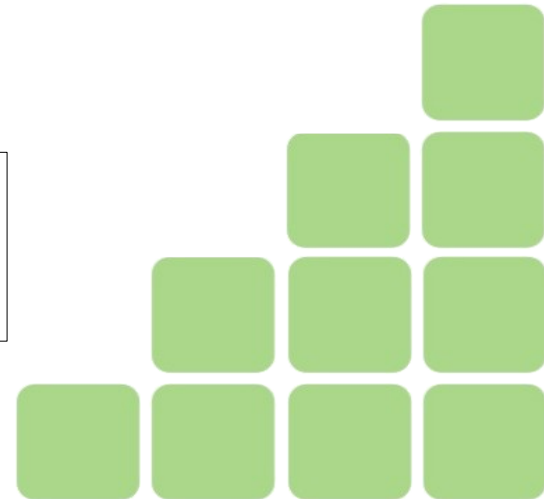
- Opção sugerida para corrigir fragilidades do dd: dcfldd

Exemplo de Utilização:

```
dcfldd if=/dev/sda1 hash=md5,sha256 hashwindow=1G \  
md5log=md5.txt sha256log=sha256.txt hashconv=after \  
conv=noerror,sync split=1G splitformat=aa of=image.dd
```

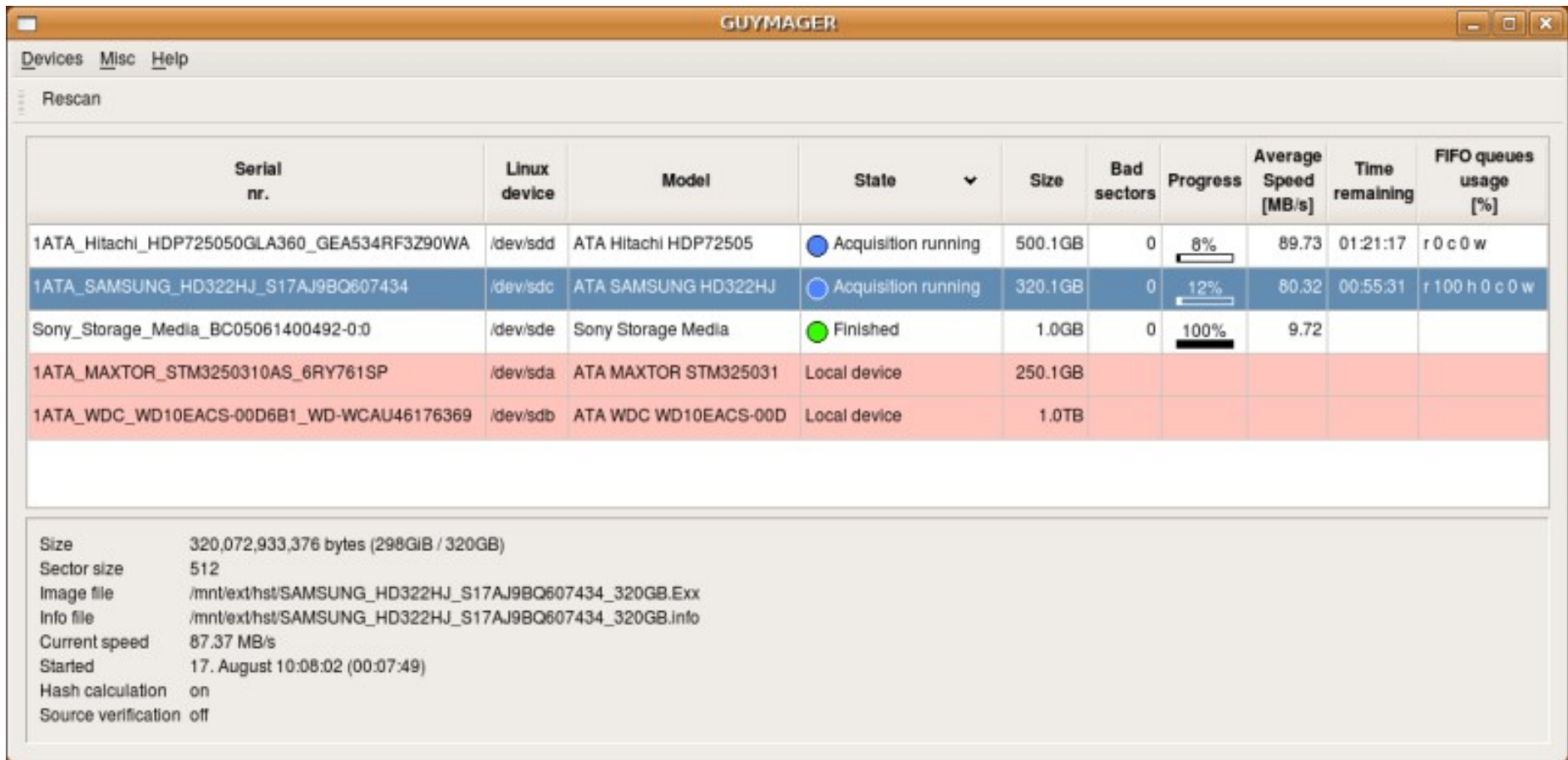
- **noerror** = não para caso encontre erros
- **sync** = se encontrar erro preenche com 0 (zero)
- Tamanho máximo de cada arquivo = 1Gb
- Nomes: image.dd.aa / image.dd.bb / ...

O dc3dd é uma re-escrita do dcfldd
(ferramenta atualmente mais completa)



Antes do Processo de Extração Coleta em Mídias

- Guymanager/Adepto/Air



The screenshot shows the GUYMAGER application window. At the top, there are menu options: Devices, Misc, and Help. Below the menu is a 'Rescan' button. The main area contains a table with the following columns: Serial nr., Linux device, Model, State, Size, Bad sectors, Progress, Average Speed [MB/s], Time remaining, and FIFO queues usage [%].

Serial nr.	Linux device	Model	State	Size	Bad sectors	Progress	Average Speed [MB/s]	Time remaining	FIFO queues usage [%]
1ATA_Hitachi_HDP725050GLA360_GEA534RF3Z90WA	/dev/sdd	ATA Hitachi HDP72505	Acquisition running	500.1GB	0	8%	89.73	01:21:17	r 0 c 0 w
1ATA_SAMSUNG_HD322HJ_S17AJ9BQ607434	/dev/sdc	ATA SAMSUNG HD322HJ	Acquisition running	320.1GB	0	12%	80.32	00:55:31	r 100 h 0 c 0 w
Sony_Storage_Media_BC05061400492-0:0	/dev/sde	Sony Storage Media	Finished	1.0GB	0	100%	9.72		
1ATA_MAXTOR_STM3250310AS_6RY761SP	/dev/sda	ATA MAXTOR STM325031	Local device	250.1GB					
1ATA_WDC_WD10EACS-00D6B1_WD-WCAU46176369	/dev/sdb	ATA WDC WD10EACS-00D	Local device	1.0TB					

Below the table, there is a summary of the current acquisition process:

- Size: 320,072,933,376 bytes (298GiB / 320GB)
- Sector size: 512
- Image file: /mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.Exx
- Info file: /mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.info
- Current speed: 87.37 MB/s
- Started: 17. August 10:08:02 (00:07:49)
- Hash calculation: on
- Source verification: off

Antes do Processo de Extração Coleta em Mídias

- **Guymanager/Adepto/Air**

- Interfaces Gráficas para Duplicação Pericial

Acquire image of /dev/sda

File format

Linux dd raw image (file extension .dd or .xxx)

Expert Witness Format, sub-format Encase5 (file extension .E0x)

Advanced forensic image (file extension .aff)

Split image files

Split size (MiB)

Case number

Evidence number

Examiner

Description

Notes

Destination

Image directory

Image filename (without extension)

Info filename (without extension)

Hash calculation / verification

Calculate MD5 Calculate SHA-256

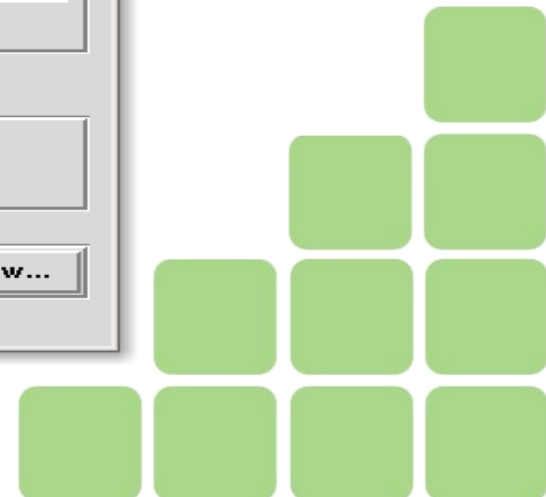
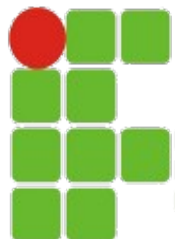
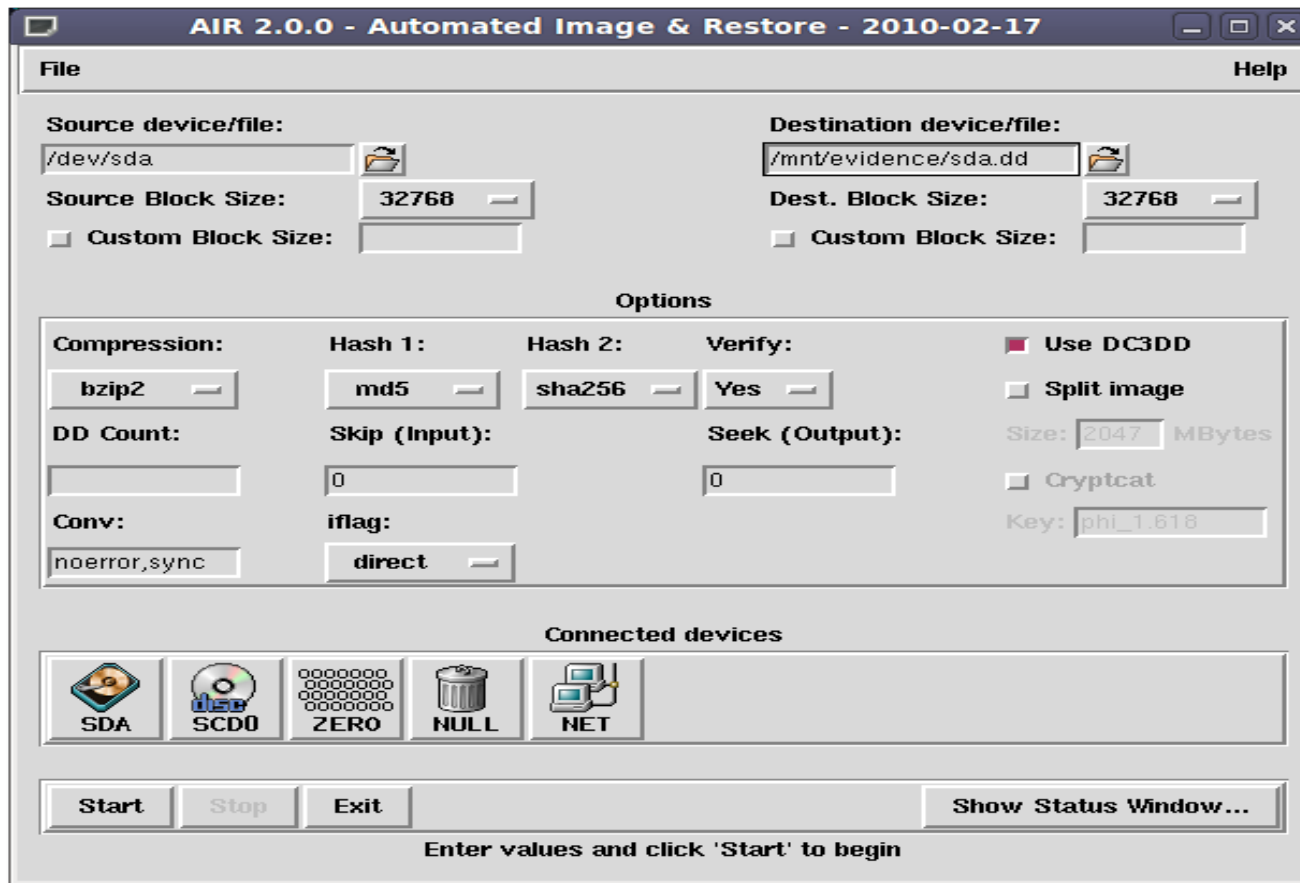
Re-read source after acquisition for verification (takes twice as long)

Verify image after acquisition (takes twice as long)

Antes do Processo de Extração Coleta em Mídias

- **Guymanager/Adepto/Air**

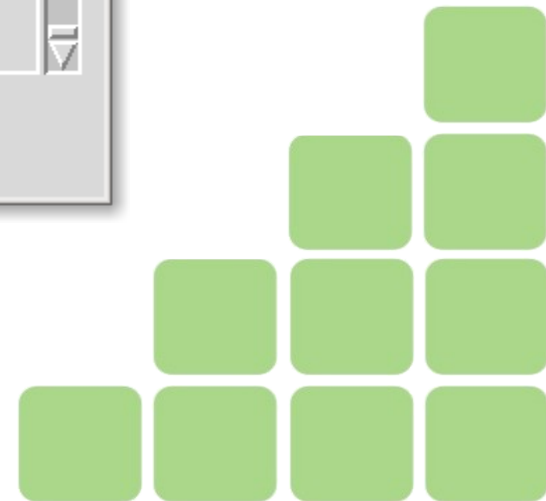
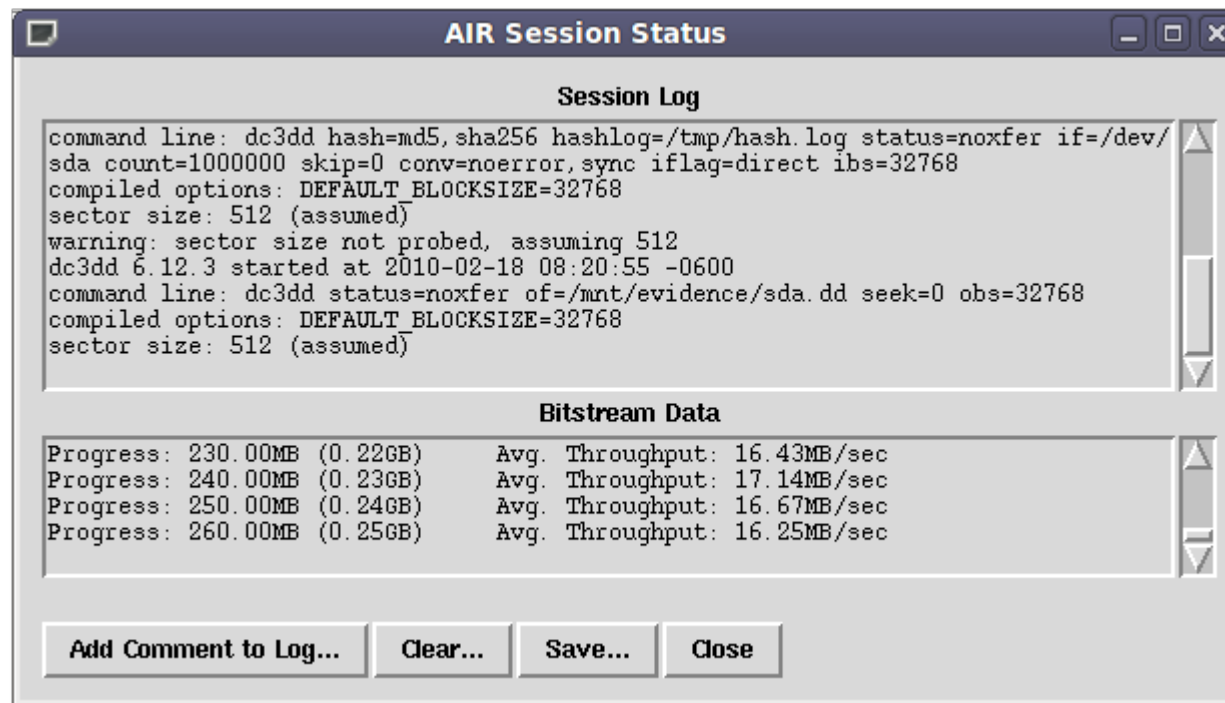
- Interfaces Gráficas para Duplicação Pericial



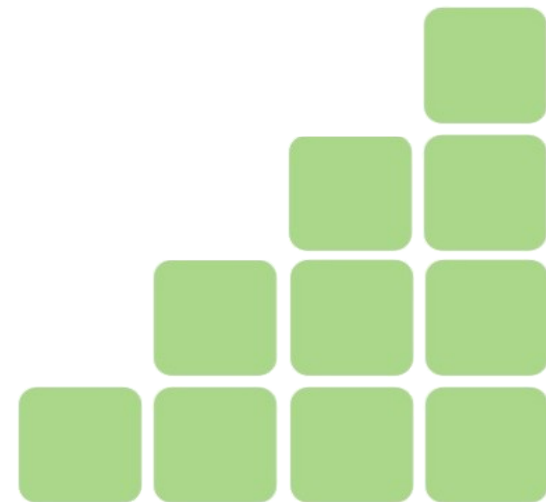
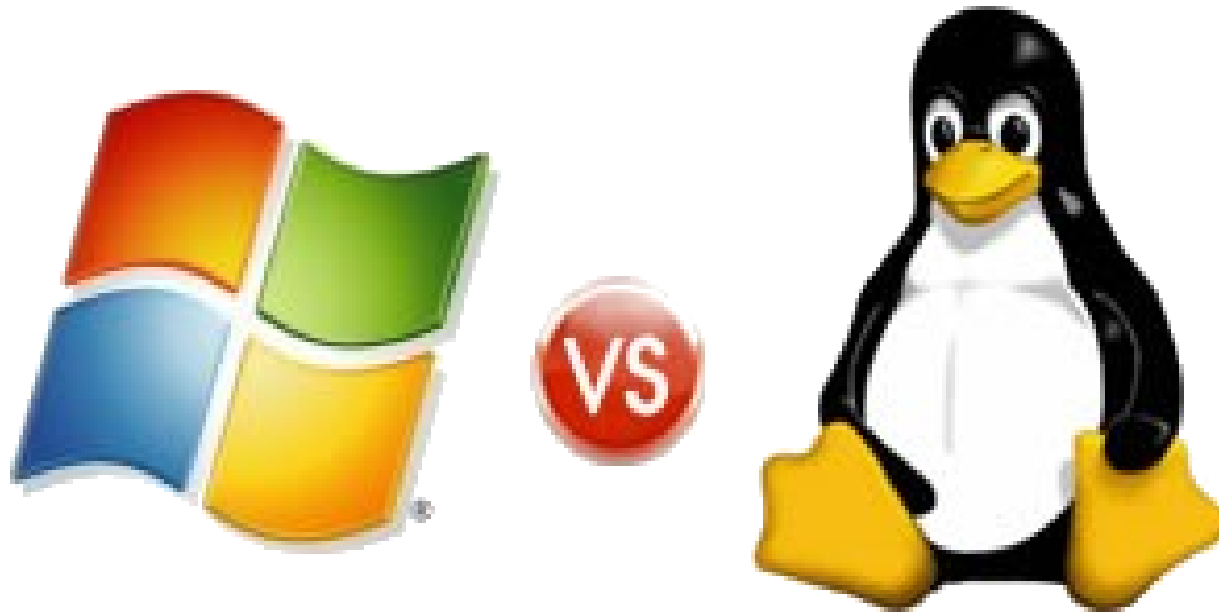
Antes do Processo de Extração Coleta em Mídias

- **Guymanager/Adepto/Air**

- Interfaces Gráficas para Duplicação Pericial



E a Plataforma Windows???



Coleta em Mídias :: Ferramentas Windows

- **Encase**

- www.guidancesoftware.com

- **FTK Imager**

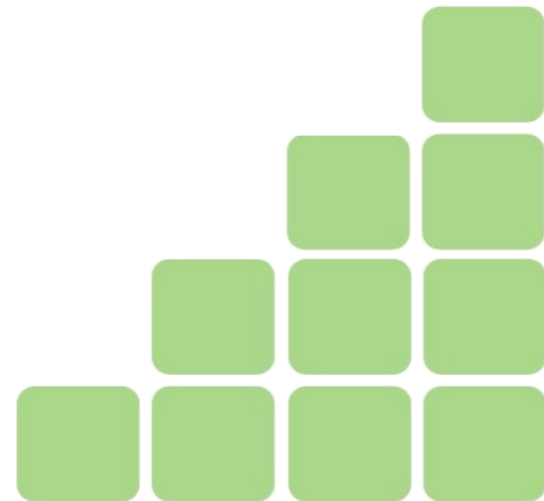
- www.accessdata.com

- **Access Data: R.A.D.A.R. (Read, Acquire, Decrypt, Analyse and Report)**

- www.accessdata.com

- **ASR**

- www.asrdata.com



Data Carving (Visão Geral)

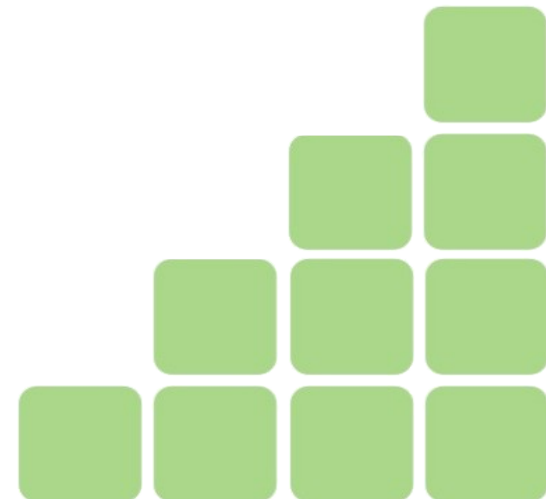
“Data carving is the process of **extracting** a collection of data from a larger data set.

Data carving techniques frequently occur during a digital investigation when the unallocated file system space is analyzed to extract files.

The files are "carved" from the unallocated space **using file type-specific header and footer values.**

File system structures are not used during the process.”

**Digital Forensic Research Workshop
(DFRWS) <http://dfrws.org>**

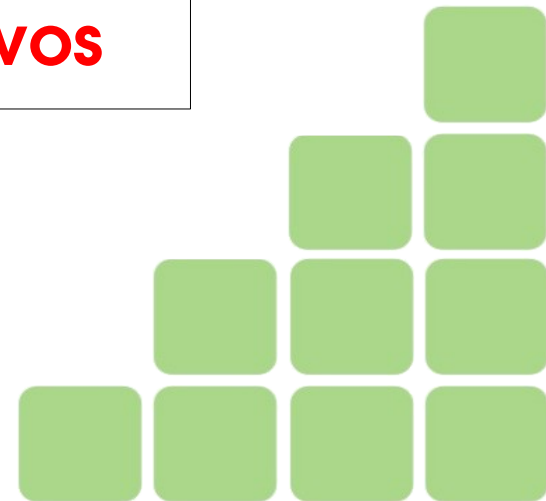


Data Carving :: Contextualizando...

Sistema de Arquivos

- “conjunto de estruturas lógicas e de rotinas, que permitem ao sistema operacional controlar o acesso ao disco rígido”
- Sistemas de Arquivos padrões Windows: FAT16, FAT32, NTFS
- Sistemas de Arquivos padrões Linux/Unix: EXT2, EXT3, EXT4, ReiserFS, XFS, JFS, ...

**Data Carving (ou File Carving)
independe de sistema de arquivos**



Data Carving :: Contextualizando...

Magic Numbers / File Signatures

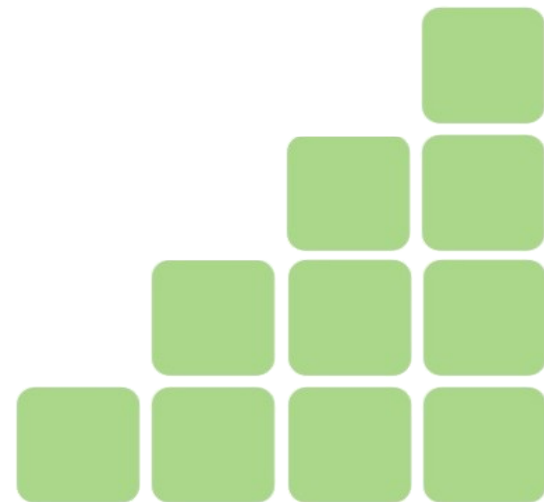
- Funciona como uma “assinatura” do tipo de arquivo.
- Método de identificação de arquivos independente de sistema operacional/sistema de arquivos.
- Baseia-se em informações inseridas/coletadas dentro de cada arquivo (cabeçalhos, rodapés, campos específicos)



Carving (Extração) em Mídias

Magicscue

- Concebido (inicialmente) para recuperação de imagens (fotos) apagadas
- Recupera arquivos específicos (com padrão definido em base específica) a partir de uma partição, para um diretório especificado.
 - avi canon-cr2 elf flac gimp-xcf gpl gzip jpeg-exif jpeg-jfif mp3-id3v1 mp3-id3v2 msoffice nikon-raw perl png ppm zip
- **Debian-like** (**apt-get install magicscue**)



Carving em Dispositivo (Mídia)

Magicrescue

Funcionamento

- Executar aplicativo com parâmetros específicos

```
magicrescue -d diretorio_destino -r base_tipos /dev/device
```

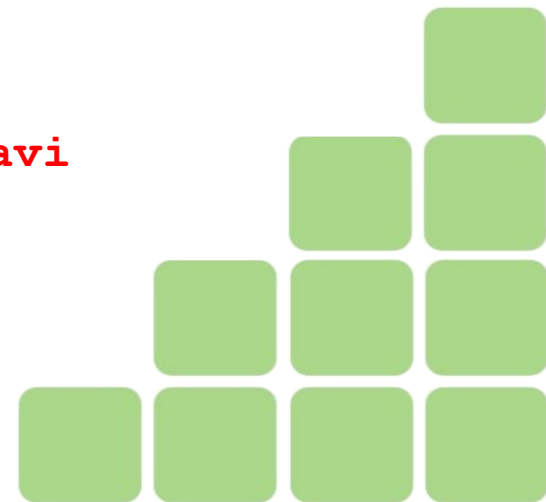
- **diretorio_destino** :: Diretório onde será gravado o resultado
- **base_tipos** :: Base com padrão do tipo de arquivo buscado

```
(/usr/share/magicrescue/recipes)
```

- **/dev/device** :: caminho do dispositivo analisado

Exemplo:

```
magicrescue -d /home/forense/analisar  
-r /usr/share/magicrescue/recipes/avi  
/dev/sda1
```



Carving em Imagem de Mídia

Magicrescue

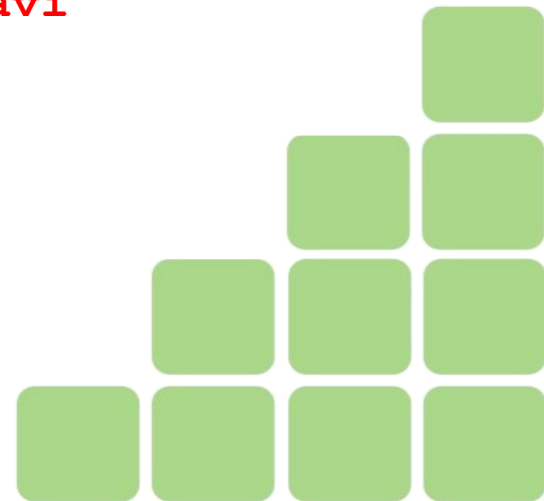
- Executar aplicativo com parâmetros específicos

```
magicrescue -d diretorio_destino -r base_tipos imagem
```

- **diretorio_destino** :: Diretório onde será gravado o resultado
- **base_tipos** :: Base com padrão do tipo de arquivo buscado
(`/usr/share/magicrescue/recipes`)
- **imagem** :: imagem do dispositivo analisado

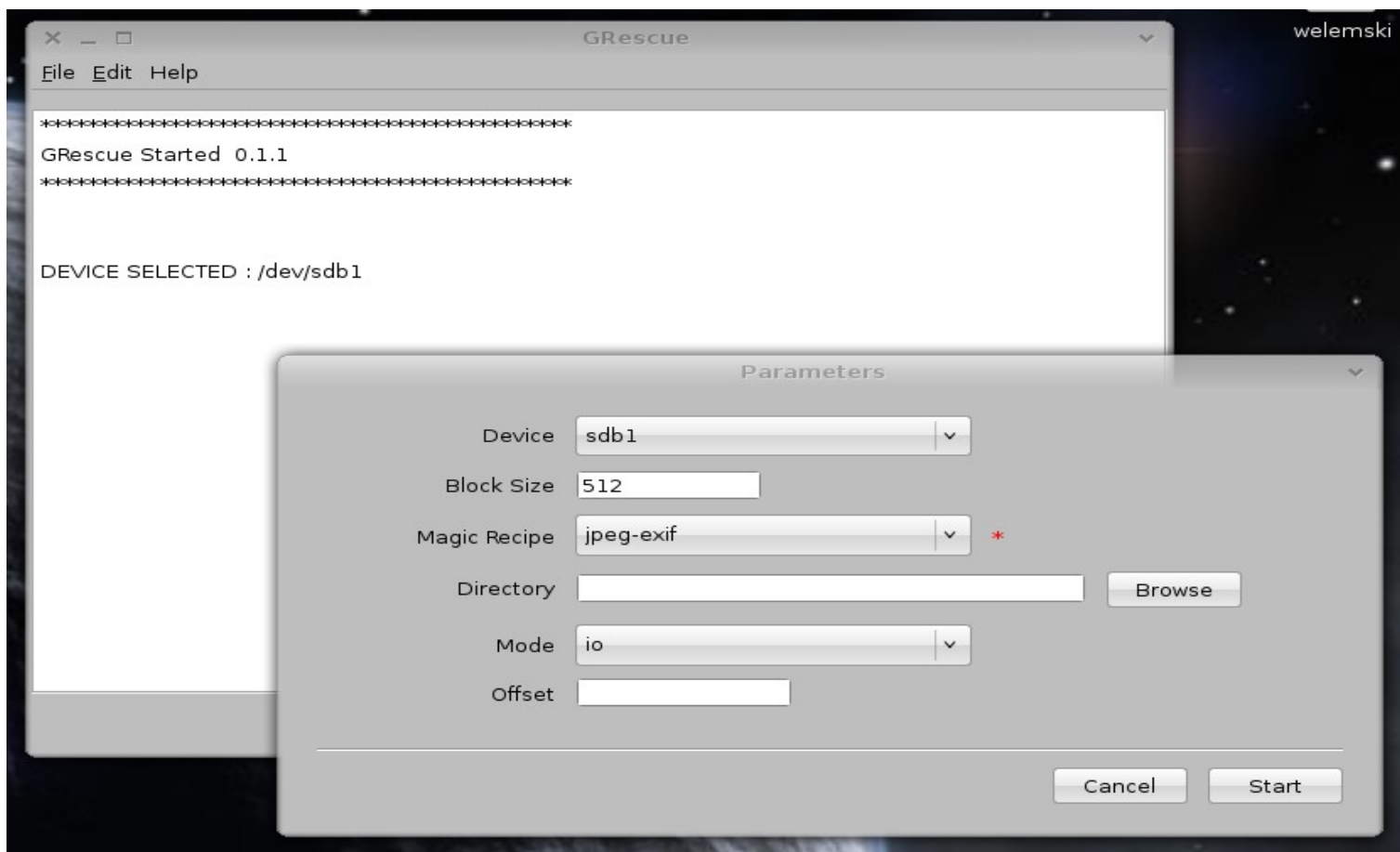
Exemplo:

```
magicrescue -d /home/forense/analisar  
-r /usr/share/magicrescue/recipes/avi  
pendrive.dd
```



Carving (Extração) em Mídias Magicrescue / GRescue

- GRescue = Interface Gráfica do Magicrescue (em desenvolvimento)



Carving em Dispositivo (Mídia)

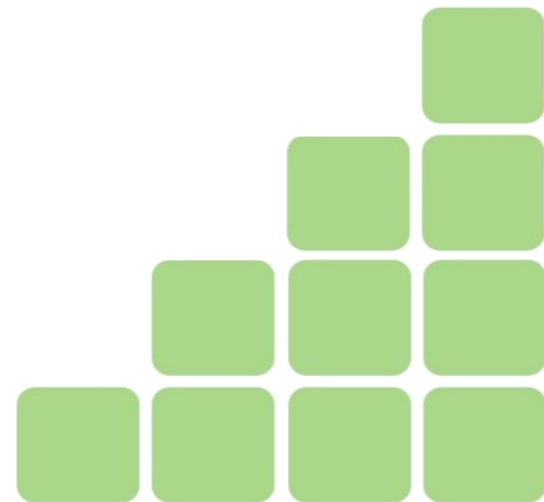
Foremost

- Rápido, fácil e robusto: **foremost**
- Debian-like (`apt-get install foremost`)

```
foremost -t <tipo1,tipo2,...> -i <dispositivo> -o <destino>
```

- Tipos de arquivos reconhecidos: jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, htm, cpp, ...
- Para todos os tipos de arquivos: **-t all**

```
Ex.: foremost -i /dev/sda1 -o diretorio_destino
```



Carving em Imagem de Mídia

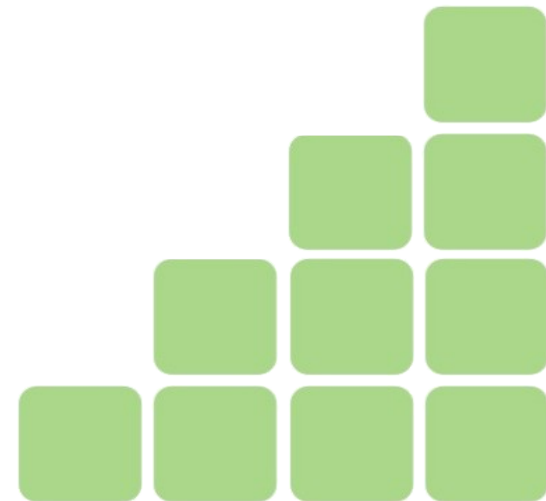
Foremost

- Rápido, fácil e robusto: **foremost**
- Debian-like (`apt-get install foremost`)

```
foremost -t <tipo1,tipo2,...> -i <imagem> -o <destino>
```

- Tipos de arquivos reconhecidos: jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, htm, cpp, ...
- Para todos os tipos de arquivos: **-t all**

```
Ex.: foremost pendrive.dd -o diretorio_destino
```



Carving em Imagem de Mídia

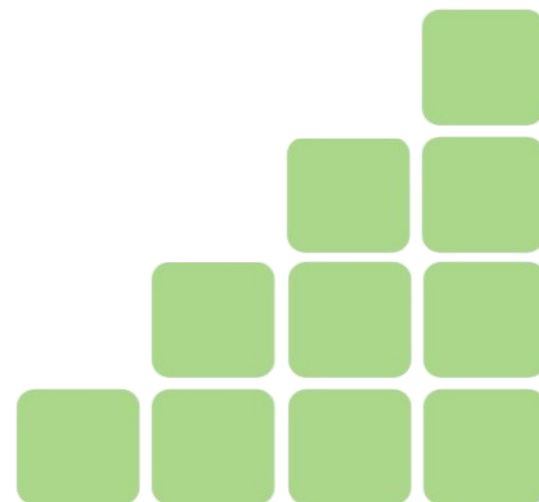
Foremost

- **Arquivo de Configuração (/etc/foremost.conf)**

- Extensão, case sensitive (y/n), tamanho máximo, cabeçalho, rodapé (opcional)

```
# PNG
png      y          200000  \x50\x4e\x47?  \xff\xfc\xfd\xfe

# Word documents
doc      y          12500000 \xd0\xcf\x11\xe0\xa1\xb1
```

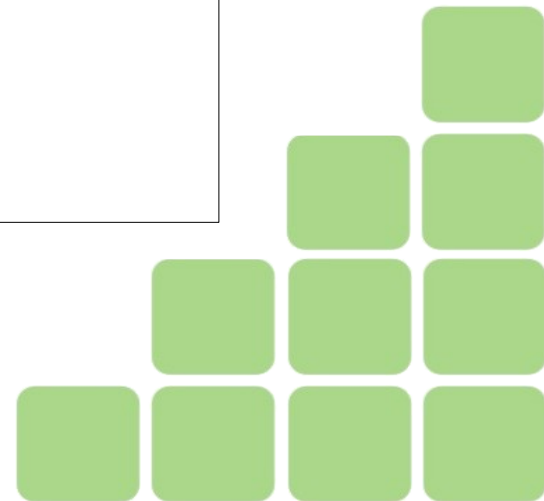


Carving em Imagem de Mídia

Foremost

```
$ mkdir apagados
$ foremost -i pendrive.dd -o apagados/
Processing: pendrive.dd
*****|
$
$ cd apagados
$ ls
audit.txt  exe  htm  jpg  pdf  png  ppt  wav  xls  zip
```

```
$ cat audit.txt
Foremost started at Fri Nov 15 16:37:00 2010
Invocation: foremost -i pendrive.dd -o apagados/
Output directory: /home/notebook/apagados
Configuration file: /etc/foremost.conf
(...)
Finish: Fri Nov 15 16:39:08 2010
1498 FILES EXTRACTED
```



Carving em Imagem de Mídia

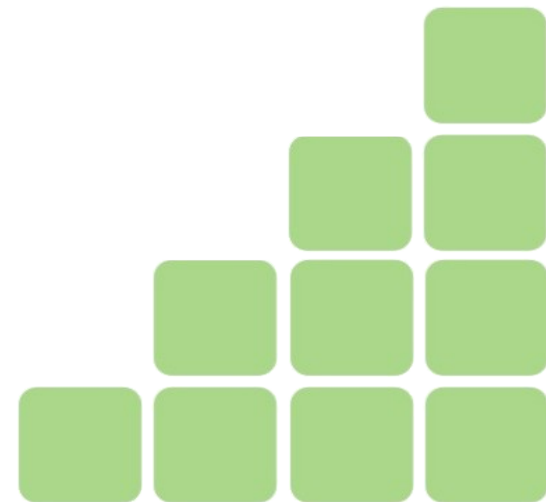
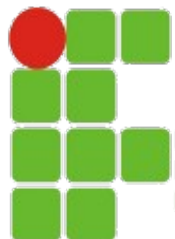
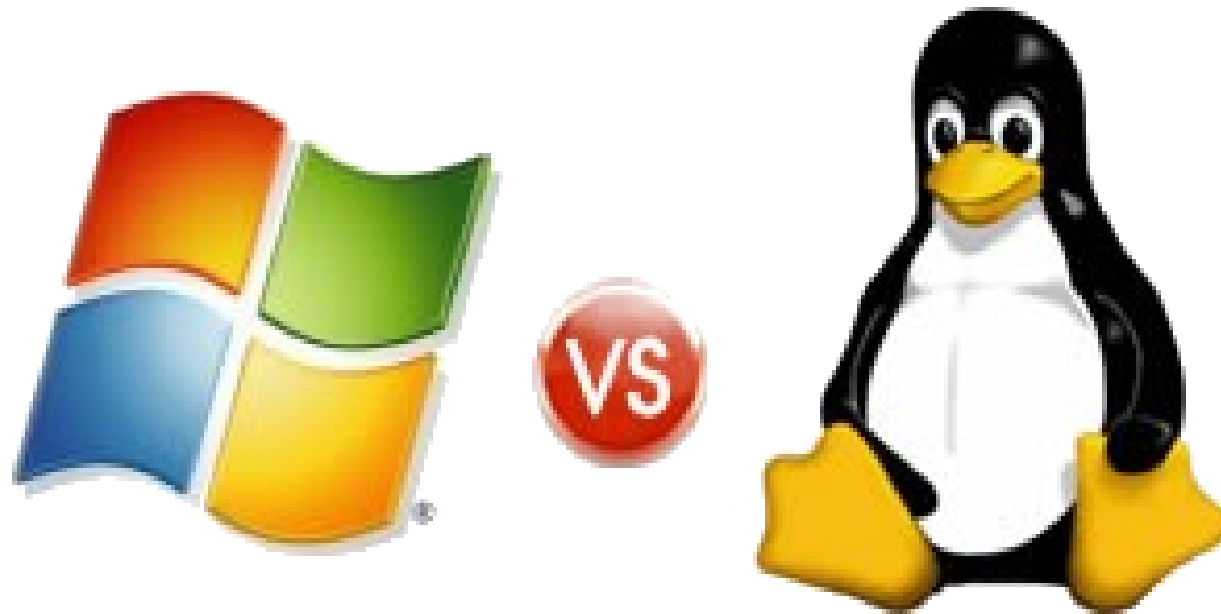
Scalpel

- Semelhante ao foremost: **scalpel**
- Debian-like (`apt-get install scalpel`)
scalpel <imagem> -o <destino>
- Por padrão, todos os tipos de arquivos no banco de dados (`/etc/scalpel/scalpel.conf`) estão comentados (não gera resultados se não for alterado)
- Para especificar quais tipos de arquivos se deseja extrair, é preciso editar o arquivo e descomentar as linhas desejadas.

Ex.: scalpel pendrive.dd -o diretorio_destino

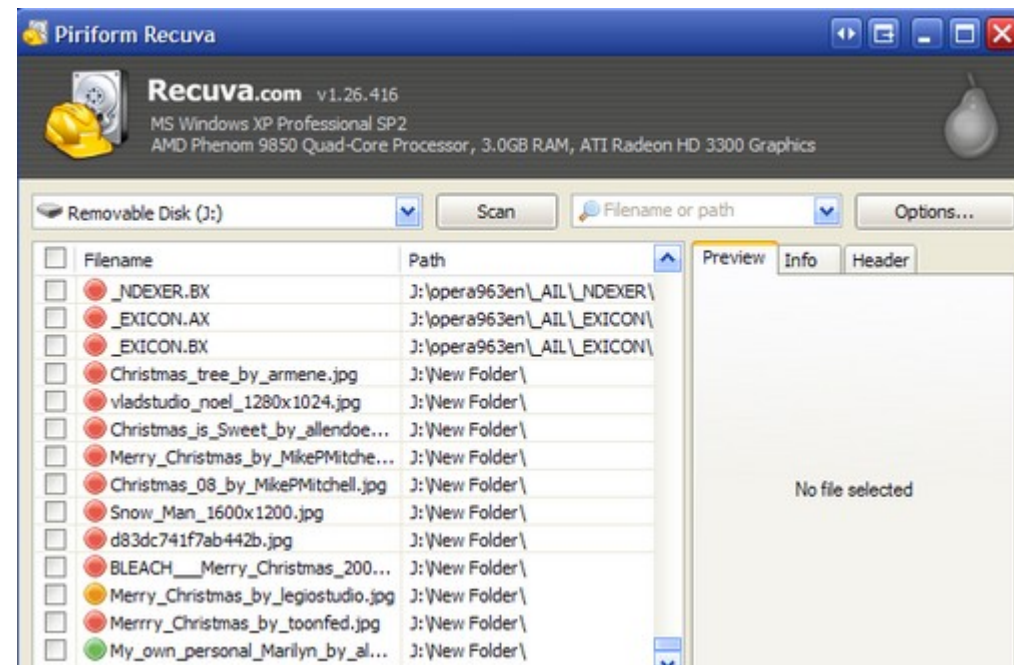
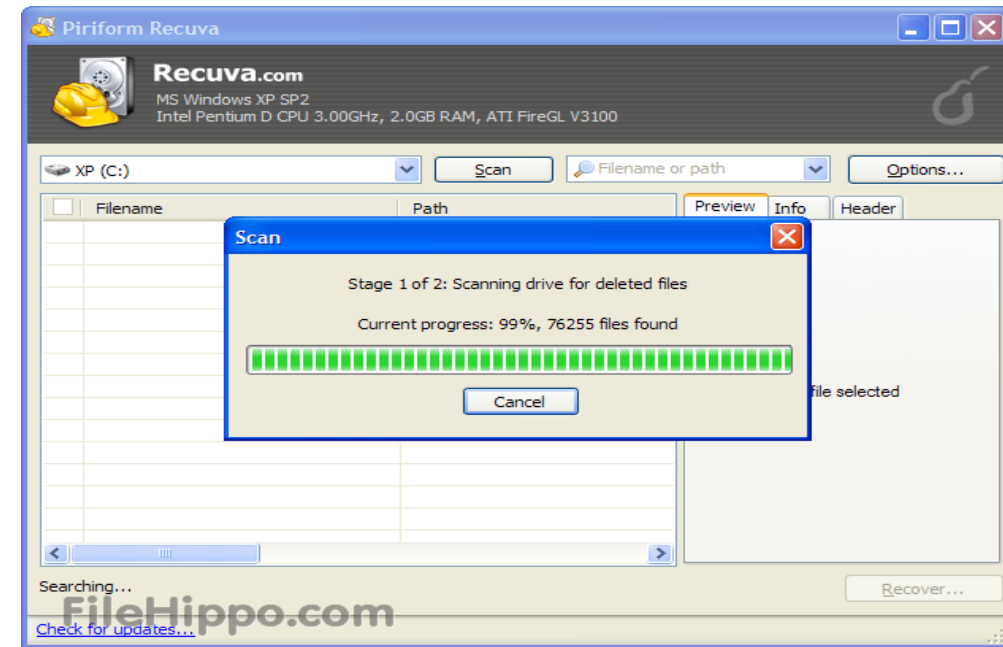
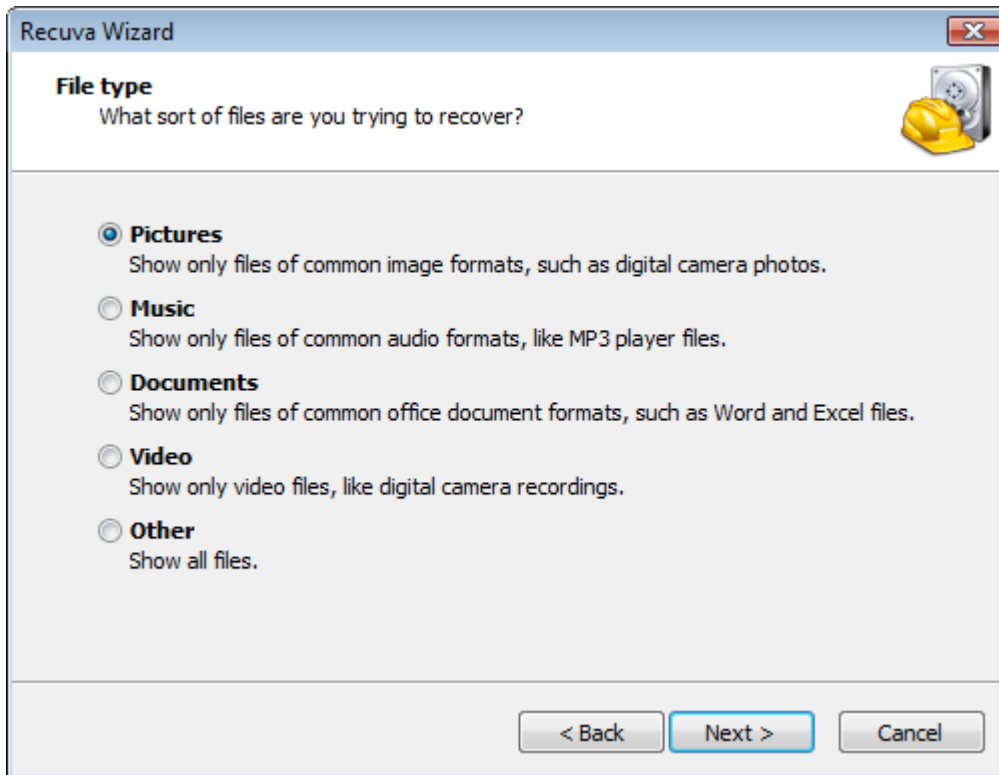


E a Plataforma Windows???



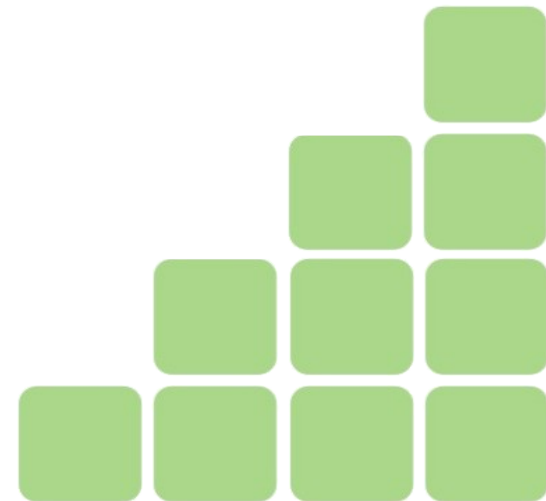
Recuva (Windows/Freeware)

- www.piriform.com/recuva



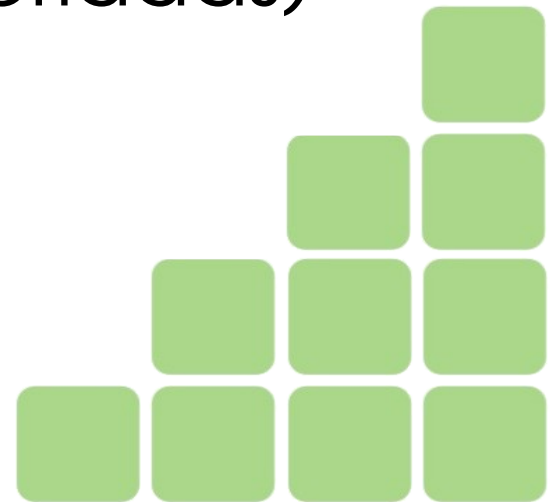
Outras Ferramentas de Recuperação/Extração (Windows)

- File Scavenger
- Data Recovery Wizard
- GetDataBack
- Restoration
- Undelete Plus
- R-Studio
- Stellar Data Recovery
- Active@ Uneraser
- Adroid Photo Recovery
- DataLifter
- SimpleCarver
- PhotoRec
- PhotoRescue
- Revit



E se o alvo/objeto for Tráfego de Redes?

Captura de tráfego e realização da
Extração (com ferramentas apropriadas)

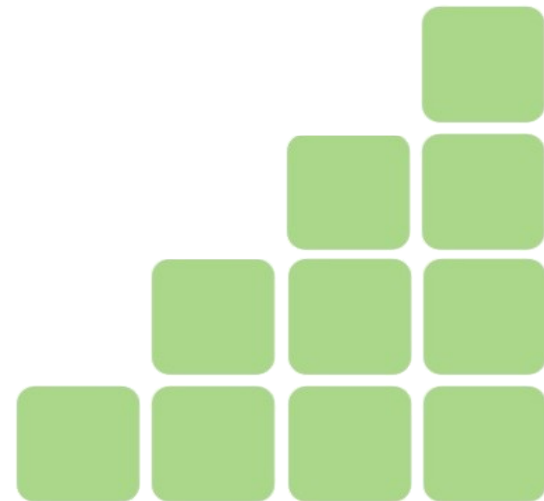


Antes do Processo de Extração Coleta em Redes

- Interface em modo monitor ("promíscuo") = Sniffer

LibPcap + TcpDump

WinPcap + WinDump



Antes do Processo de Extração

Coleta em Redes

Captura de Tráfego Específico :: Tcpdump

- `tcpdump -i <interface> port <porta/serviço> -w <arquivo_captura>`

- **Tráfego de E-mails:**

- SMTP: (porta) = 25

- POP3: (porta) = 110

- **Tráfego Web: (porta) = 80**

`port [porta]`

`src [origem]`

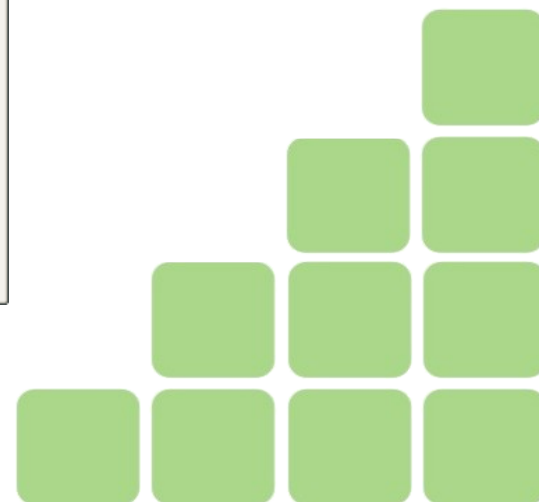
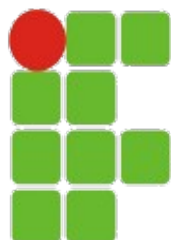
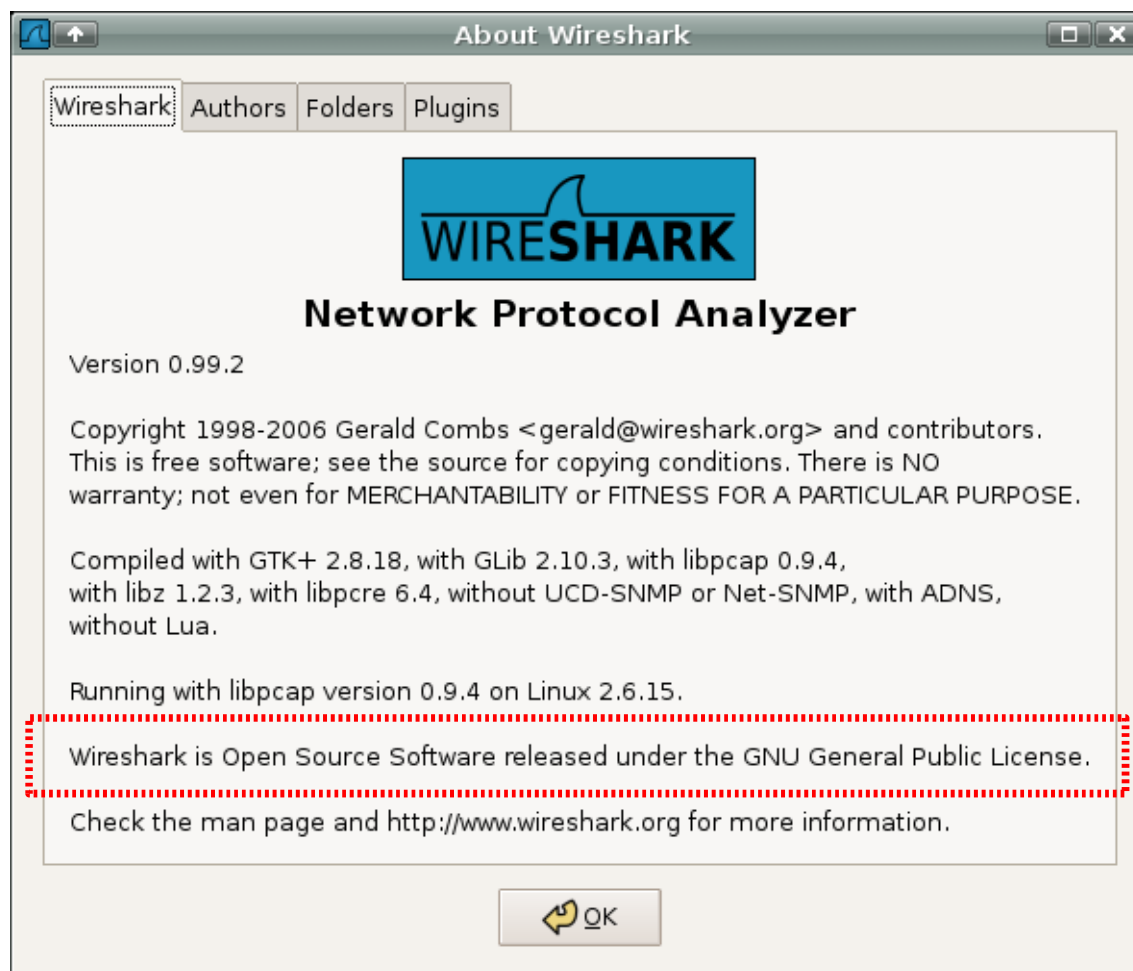
`dst [destino]`

```
tcpdump -X -vvv -i eth0 -s 1518 -n port 80 -w coleta.cap
```

Antes do Processo de Extração

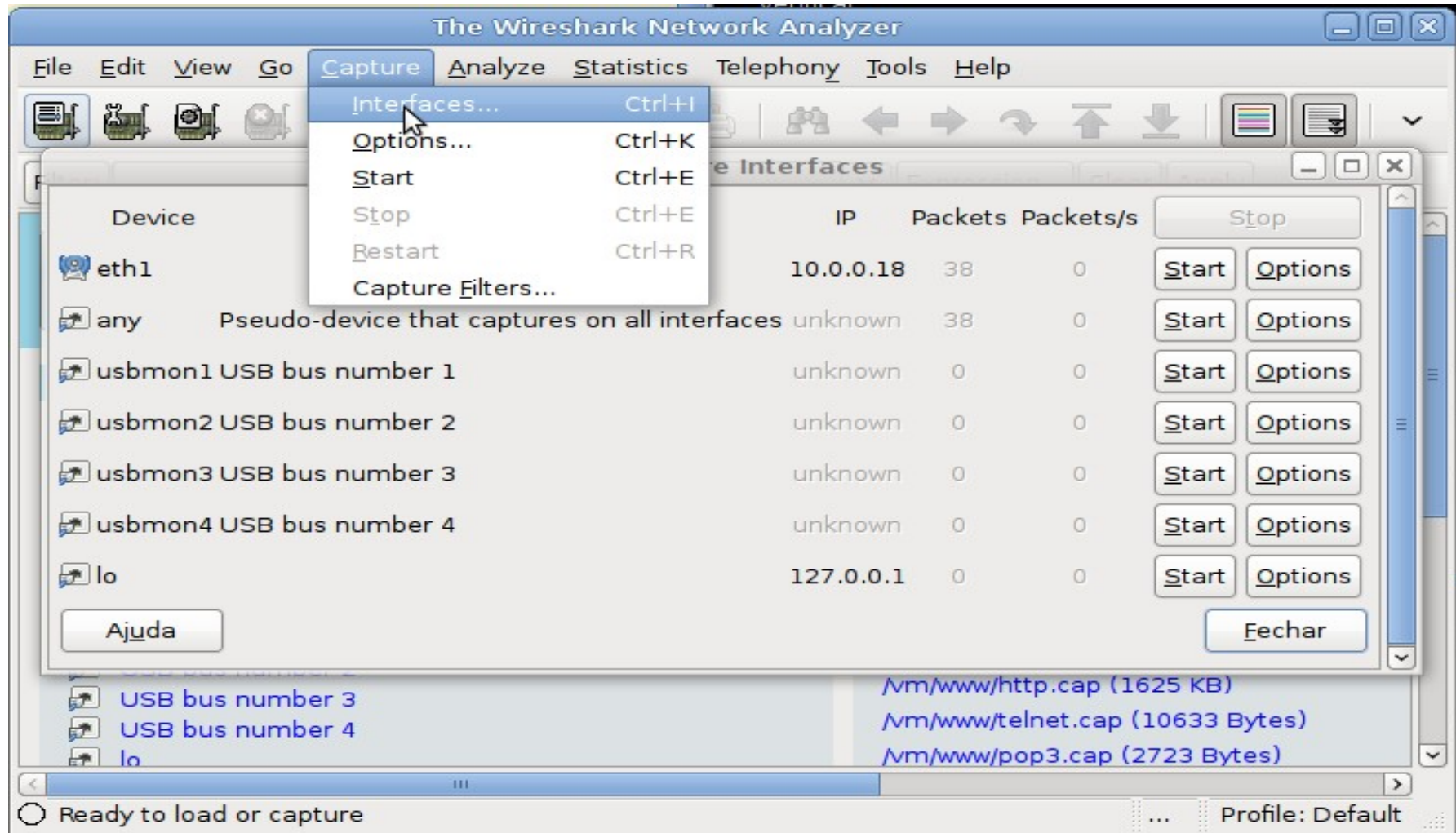
Coleta em Redes (Modo Gráfico: Ethereal/Wireshark)

<http://www.wireshark.org>



Antes do Processo de Extração

Coleta em Redes (Modo Gráfico: Ethereal/Wireshark)



Carving em Imagem de Tráfego de Redes

Tcpextract

- Extrai arquivos (file carving) de tráfego de redes baseado em assinaturas/padrões de arquivos.
- Pode ser usado diretamente capturando/analizando o tráfego de uma rede ou analisando um arquivo .CAP (formato tcpdump)

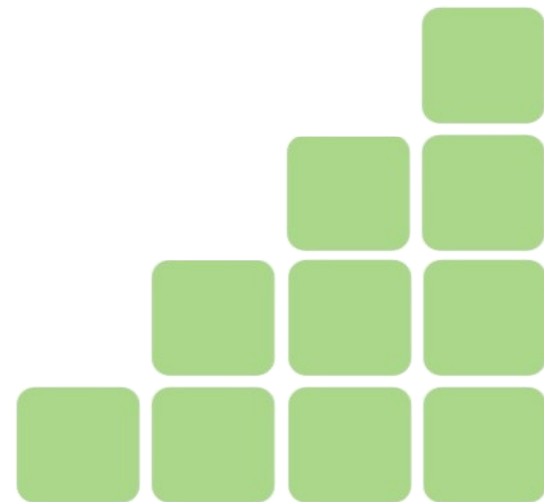
- `tcpextract -d /dev/device -o diretorio_destino`

- `tcpextract -f arquivo_cap -o diretorio_destino`

```
# tcpdump -X -vvv -n -s 1518 -i eth0 tcp port 80 -w http.cap
```

```
# tcpextract -f http.cap -o examinar
```

```
# nautilus examinar
```



Carving em Imagem de Tráfego de Redes

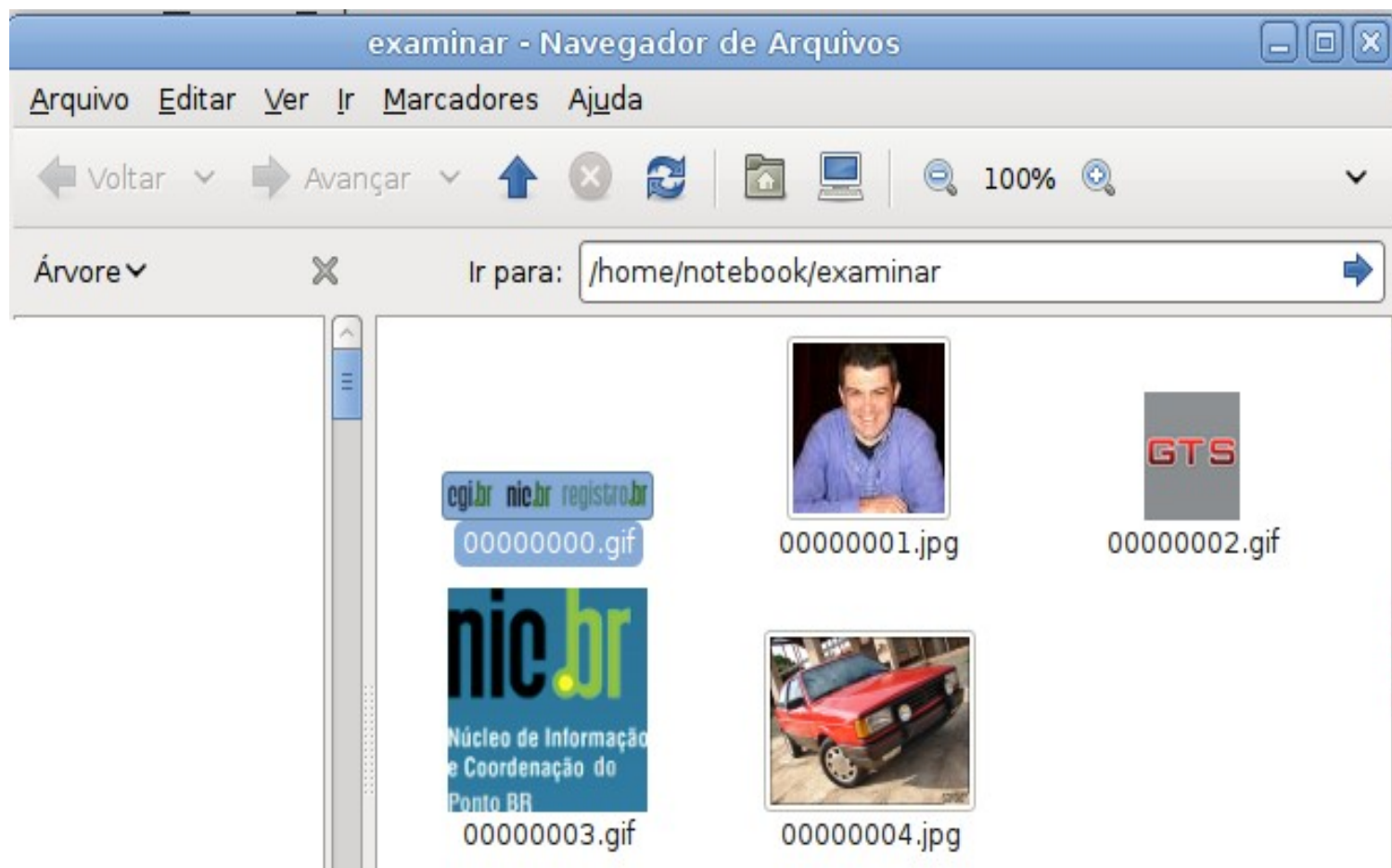
Tcpextract

```
$ mkdir examinar
```

```
$ tcpextract -f http.cap -o examinar
```

```
Found file of type "gif" in session [72.14.204.103:20480 -> 192.168.2.100:15495], exporting to examinar/00000000.gif  
Found file of type "png" in session [72.14.204.103:20480 -> 192.168.2.100:15751], exporting to examinar/00000001.jpg  
Found file of type "png" in session [72.14.204.103:20480 -> 192.168.2.100:15495], exporting to examinar/00000002.gif  
Found file of type "png" in session [72.14.204.103:20480 -> 192.168.2.100:15495], exporting to examinar/00000003.gif  
Found file of type "gif" in session [72.14.204.103:20480 -> 192.168.2.100:15751], exporting to examinar/00000004.jpg
```

```
$ nautilus examinar
```



Carving em Imagem de Tráfego de Redes

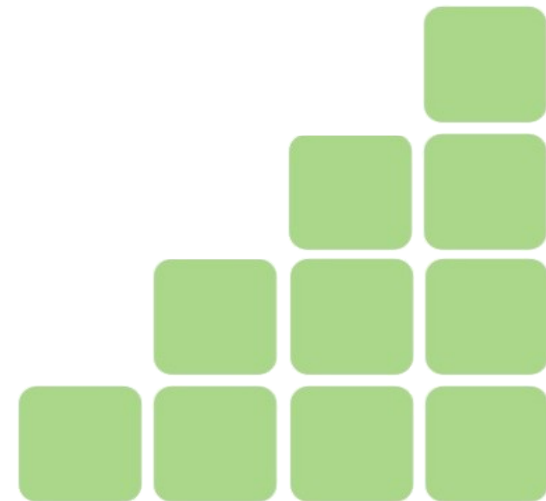
Chaosreader

- Semelhante ao tcpextract
- Maior nível de detalhes sobre tráfegos (origem/destino)
- Gera relatório HTML (mais adequado para laudos)
- Relatório sumarizado por protocolos capturados/identificados
- Analisa arquivo .CAP (formato tcpdump)
 - `chaosreader arquivo_cap -D diretorio_destino`

```
# tcpdump -X -vvv -n -s 1518 -i eth0 tcp port 80 -w http.cap
```

```
# chaosreader http.cap -D examinar
```

```
# firefox index.html
```



Carving em Imagem de Tráfego de Redes

Chaosreader

Chaosreader Report, http.cap - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

file:///home/notebook/examinar/index.html

Chaosreader Report, http.cap

Chaosreader Report

File: http.cap, Type: tcpdump, Created at: Fri Nov 26 17:02:26 2010

[Image Report](#) - Click here for a report on captured images.
[GET/POST Report](#) - Click here for a report on HTTP GETs and POSTs.
[HTTP Proxy Log](#) - Click here for a generated proxy style HTTP log.

TCP/UDP/... Sessions

1.	Fri Nov 26 16:46:53 2010	43 s	192.168.2.100:34620 -> 72.14.204.103:80	www	71783 bytes	<ul style="list-style-type: none">• as_html• session_0001.part_01.gz 4537 bytes• session_0001.part_02.gif 8561 bytes• session_0001.part_03.data 5656 bytes• session_0001.part_04.data 30622 bytes• session_0001.part_05.gz 3506 bytes• session_0001.part_06.gz 3459 bytes• session_0001.part_07.gz 4682 bytes
2.	Fri Nov 26 16:46:53 2010	43 s	192.168.2.100:34621 -> 72.14.204.103:80	www	210297 bytes	<ul style="list-style-type: none">• as_html• session_0002.part_01.data 387 bytes• session_0002.part_02.data 198057 bytes• session_0002.part_03.gif 2525 bytes• session_0002.part_04.gz 142 bytes
3.	Fri Nov 26 16:46:53 2010	43 s	192.168.2.100:34622 -> 72.14.204.103:80	www	73727 bytes	<ul style="list-style-type: none">• as_html• session_0003.part_01.gz 10995 bytes• session_0003.part_02.data 1104 bytes• session_0003.part_03.gz 35968 bytes• session_0003.part_04.gz 4767 bytes

Concluído

Carving em Imagem de Tráfego de Redes

Chaosreader

Chaosreader Report, http.cap - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

file:///home/notebook/examinar/index.html

Chaosreader Report, http.cap

IP Count

192.168.2.100	1746
72.14.204.103	545
200.160.4.20	244
72.14.204.104	194
72.14.204.99	141
200.160.7.130	106
200.160.4.6	91
72.14.204.147	89
72.14.204.100	27
200.160.4.14	10
128.242.245.212	8
187.115.167.218	7
209.107.220.82	6
70.84.199.18	4

TCP Port Count

www	3209
-----	------

UDP Port Count

IP Protocol Count

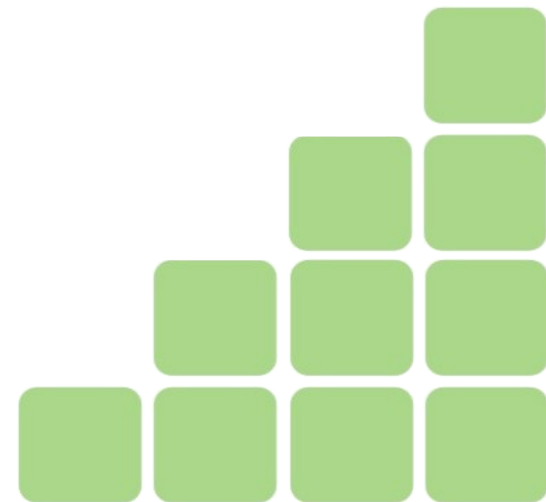
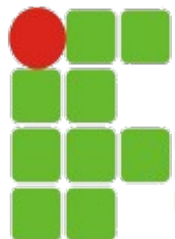
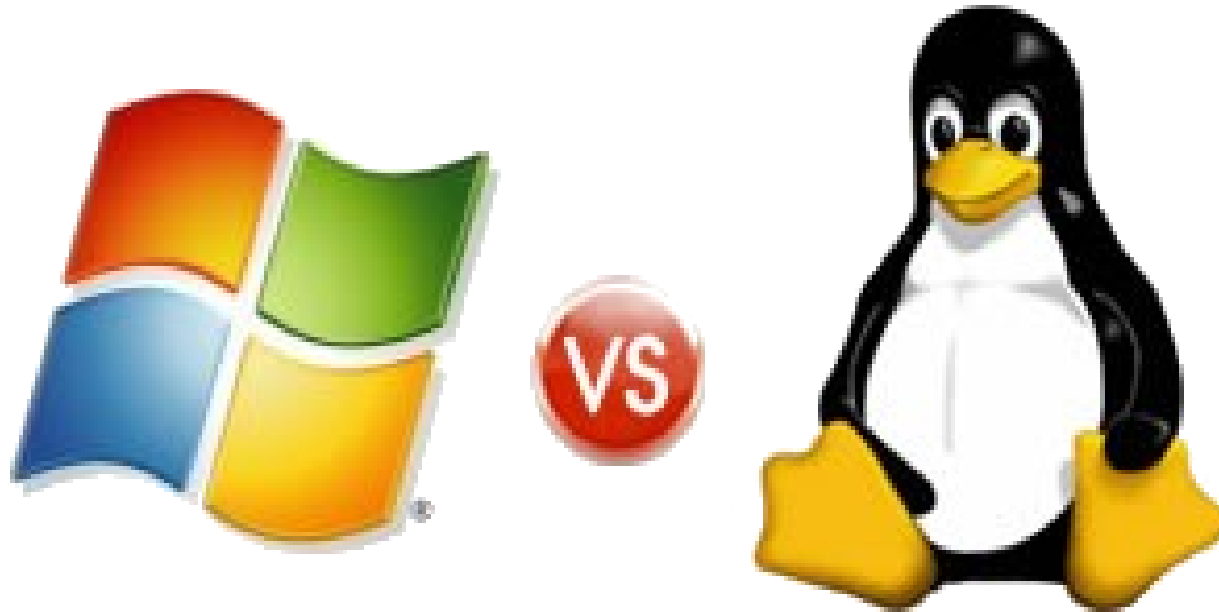
TCP	3218
-----	------

Ethernet Type Count

0800	3218
------	------

Concluído

E a Plataforma Windows???



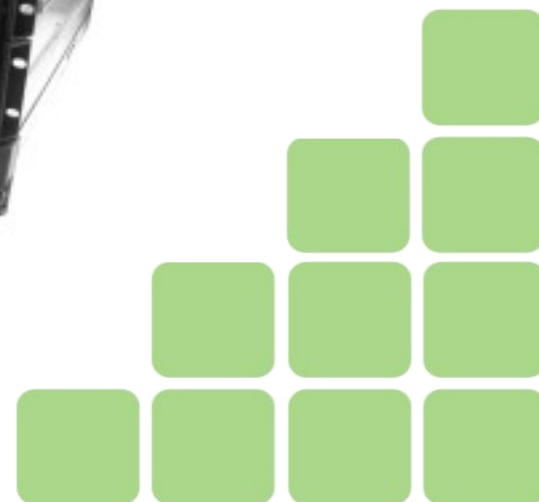
E a Plataforma Windows???

- Existem ferramentas comerciais (inclusive mais fáceis de utilizar) baseadas no sistema operacional Windows, mas esse não foi o foco desta apresentação.

- Sugestão = Netwitness

- Investigator (freeware)

- Visualize (\$\$\$\$\$)



NetWitness Investigator

The screenshot displays the NetWitness Investigator interface. The left sidebar shows a tree view of resources, including a list of files and folders. The main window shows a table of sessions and a detailed view of a specific session.

Session List:

Time	Service	Size	Events
1/02/2004 11:53:03	HTTP	54,555	192.168.0.10 : 3497 ↔ 207.21.253.76 : 80
1/02/2004 11:52:50	HTTP	26,627	192.168.0.10 : 3494 ↔ 216.239.39.99 : 80

Session Details:

ID: 100-142-12202 **Date:** 1/02/2004 11:52:50 **Size:** 26627 bytes
192.168.0.10 : 3494 ↔ 216.239.39.99 : 80

GET /

©2003 Google - Searching 3,307,998,701 web pages

NetWitness Investigator

The screenshot displays the NetWitness Investigator 9 interface. The main window shows a 'Time Graph of Session Traffic (Sessions Per Minute)' for session ID 21624, with a significant spike in traffic around 13:54 on 2008-05-30. Below the graph, a list of categories and items is shown, including Hostname Aliases, User Account, E-mail Address, Action Event, Extension, and Filename.

Threat Analysis Content - Session 21624

NetWitness Reconstruction for session ID: 21624 (Source 10.10.10.153)
Time 5/30/2008 14:47:40 to 5/30/2008 14:47:40 Packet Size 9,554 bytes Payload
Protocol 2048/6/1122 Flags Keep Assembled AppMeta NetworkMeta Packet Count

Chat Log:

- Tom: hey man
- Brian: How is the job going?
- Tom: ah its alright
- Tom: kind of slow
- Tom: ll e-mail you some interesting info about their 401k. its amazing how wide open this network is

Google Earth

Map showing network connections over a globe. Data SIO: NOAA, U.S. Navy, NGA, GEBCO
US: Dept of State, Geographer
© 2008 Europa Technologies
© 2008, 1st Air All...
30°19'03.19" N 75°07'33.65" W elev -12 m Eye alt 12968.25 km

Netwitness Analysis

Forensics Explorers - NetWitness Analysis 3.53 - Microsoft Internet Explorer

Address: http://localhost/nw35/frame.asp

1/29/2003 12:31:18 PM

Print this page

Network Forensics Report for Sys Admin

admin is logged into NW_35

This is a forensics report. The report provides information rich statistics that enables target discovery and event analysis of computer evidence. For analysis select the total number to view event, and select the entity to build a report profiling that entity. The data group details are listed below.

Collection Duration: Tue Jan 7 07:18:00 EST 2003 - TO - Fri Jan 10 11:11:00 EST 2003

Collection Session Volume: 9179

Application Type

Identified applications present in the network traffic. Applications are identified by the content(not port) of the traffic present in the traffic. Select the Application Type to build a report or session total to view events.

Application Type:	Session Total
Web (HTTP)	8330
Web (HTTPS)	749
E-Mail (POP-3)	38
MS Instant Msg	29
Ftp	23
E-Mail (SMTP)	6
News	3
Yahoo Instant Msg	1

Action Type

Network traffic actions identified in the network traffic. Select the Action Type to build a report or session total to view events.

Action Type:	Session Total
Get Resource	4407
Get Resource Response	3931
User Login	65
Send MSG	22
User Logoff	14
Read MSG Response	13
Recieve MSG	13
Read MSG	6

Netwitness Visualize

INFORMER VISUALIZE

Dashboard Define Schedule View Tools Visualize Admin Help

Informer User [preferences] [logout]

Department Monitoring

Tutorial Data Leakage Personnel Investigation

Grid Timeline

Filter: none

Time: none

- ip.src
- service
- client
- content
- country.dst
- alert
- ad.username.src
- ad.computer.src
- keyword.subjects
- time

“Resposta” Open Source



www.xplico.org

Xplico Interface User: xplico

Help Forum Wiki Logout

- Case
- Cases
- Sessions
- Session
- Graphs
- Web
- Mail
- Voip
- Share
- Chat
- Shell

Session Data

Case and Session name: live sample -> sample

Start Time: 0000-00-00 00:00:00

End Time: 0000-00-00 00:00:00

Status: EMPTY

Hosts: ...

Live

Interface:

HTTP
Post: 0
Get: 0
Video: 0
Images: 0

MMS
Number: 0
Contents: 0
Video: 0
Images: 0

Emails
Received: 0
Sent: 0
Unreaded: 0/0

FTP - TFTP
Connections: 0-0
Downloaded: 0-0
Uploaded: 0-0

Web Mail
Total: 0
Received: 0
Sent: 0

Facebook Chat
Users: 0
Chats: 0

IRC

SIP
Calls: 0

RTP/VoIP
Video: 0
Audio: 0

NNTP
Groups: 0
Articles: 0

Feed (RSS & Atom)
Number: 0

Printed files
Pdf: 0

Dns
Host res: 0

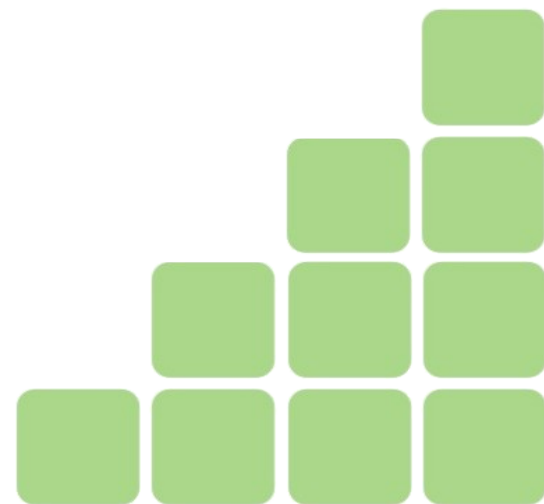
Telnet
Connections: 0

© 2007-2010 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

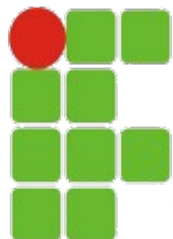
Dissector	Status	Note	Dissector	Status	Note
Ethernet	100%	—	IPP	90%	—
PPP	90%	—	PJL	90%	—
VLAN	95%	—	NNTP	95%	—
L2TP	70%	—	MSN	10%	—
IPv4	98%	—	IRC	15%	—
IPv6	98%	—	YAHOO	0%	—
TCP	95%	—	GTALK	0%	—
UDP	100%	—	EMULE	0%	—
DNS	80%	—	SSL/TLS	0%	with keys
HTTP	100%	—	IPsec	0%	with keys
SMTP	95%	—	802.11	60%	no encryp.
POP	95%	—	LLC	60%	—
IMAP	95%	—	MMSE	95%	over HTTP
SIP	80%	—	Linux cooked	95%	SLL
RTP	70%	—	TFTP	90%	—
RTCP	60%	—	SNOOP	100%	Format
SDP	70%	—	PPPoE	90%	—
FB chat	90%	—	Telnet	90%	—
FTP	90%	—	WebMail	90%	—

Considerações Finais

- Diversidade (e robustez) de softwares livres para computação forense;
- A homologação de ferramentas para o uso pericial passa pela abertura do código (para validação);
- Ferramentas adequadas podem facilitar (e diminuir) o trabalho do perito.



Perguntas



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Ricardo Kléber :: GTS'16 :: UNISINOS :: São Leopoldo/RS

