

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

Data Carving em Mídias e em Redes

Ricardo Kléber Martins Galvão

www.ricardokleber.com.br

ricardo.galvao@ifrn.edu.br

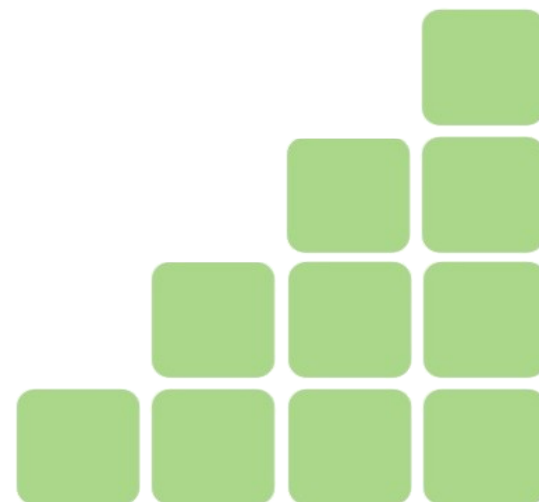


SEGINFO - WORKSHOP DE SEGURANÇA DA INFORMAÇÃO

Rio de Janeiro/RJ – 03 de Novembro de 2010



REDE FEDERAL
DE EDUCAÇÃO
PROFISSIONAL
E TECNOLÓGICA
1909 2009



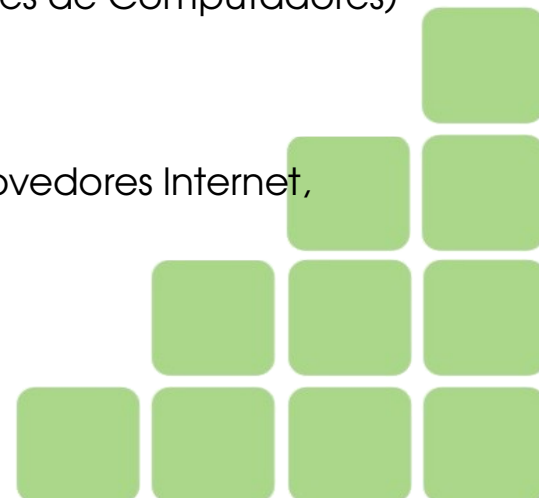
Ricardo Kléber

- Professor do IFRN (Segurança de Redes)
- Diretor de Regulação do Ensino (IFRN)
- Professor da FARN (Especialização em Redes de Computadores)
- Professor da Universidade Potiguar (Especialização em Computação Forense)
- Professor da Uninorte/AC (Especialização em Computação Forense)
- Bacharel em Ciências da Computação, Mestre em Engenharia Elétrica (Sistemas Distribuídos) e Doutorado em Engenharia Elétrica (Sistemas Inteligentes) (UFRN)
- Certificação Linux Conectiva e Brainbench
- Colunista do Blog Seginfo
- Membro do Comitê Técnico do Seginfo'2010
- Publicações/Apresentações no SSI, Seginfo, Iccyber, GTS/NicBR, Encsirt, FISL, Ensol, Epsl e outros eventos nas áreas de Segurança da Informação e Software Livre



Atividades Recentes

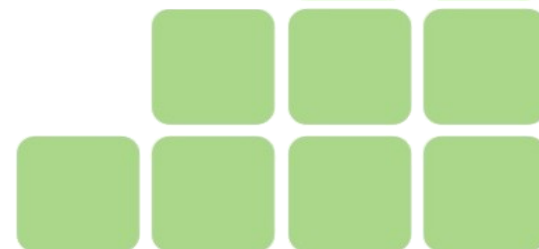
- Ex-Security Officer da UFRN (Superintendência de Informática)
- Fundador do CSIRT NARIS (Núcleo de Atendimento e Resposta a Incidentes de Segurança) da UFRN
- Ex-Professor da UFRN (Sistemas Operacionais, Linguagens de Programação e Redes de Computadores)
- Ex-Diretor de Redes do Detran/PE
- Ex-Diretor de Ensino e Coordenador de TI do IFRN/Campus Currais Novos
- Fundador do NUPETIS – Núcleo de Pesquisa em TI no Seridó
- Consultoria e treinamentos em Segurança da Informação e Software Livre em provedores Internet, empresas e órgãos governamentais do RN, PI, PE e AP.



Identificando o Perfil do Público

.....

Quem atua/conhece a Área de
Computação Forense?



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**



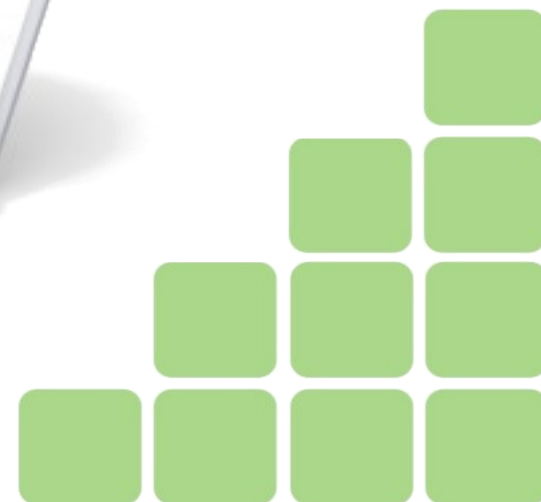
Contextualizando...

Análise Forense Computacional



Principais Etapas

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

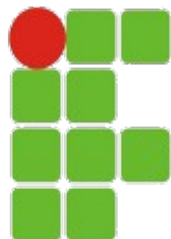
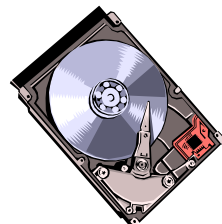


Contextualizando...

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

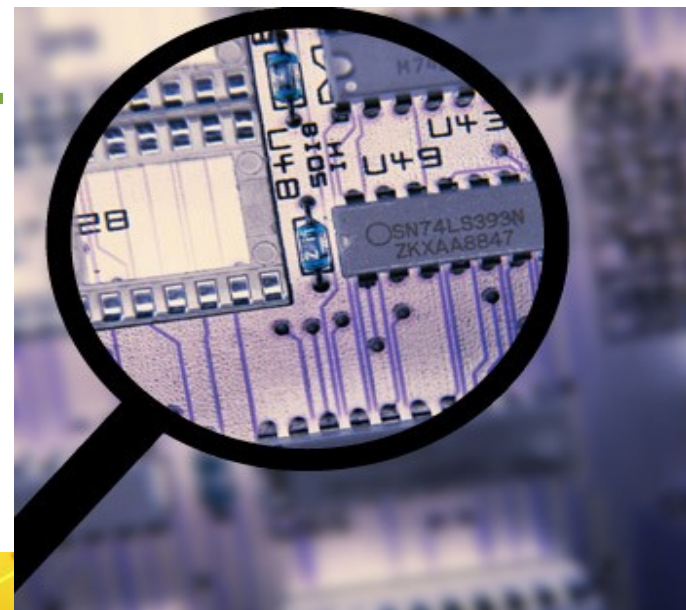


Contextualizando...

Análise Forense Computacional

Conceitos Importantes

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

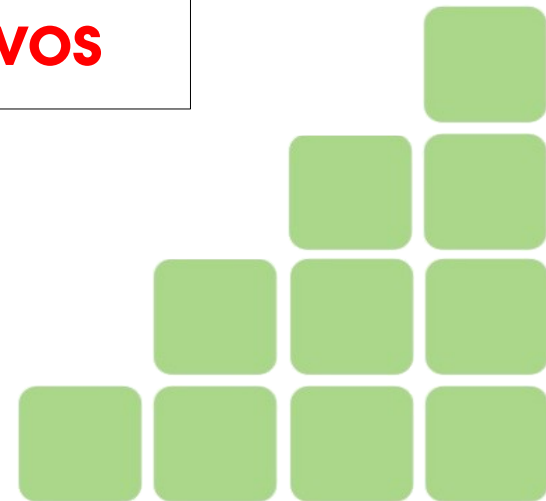


Contextualizando...

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



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)



Data Carving (Visão Geral)

.....

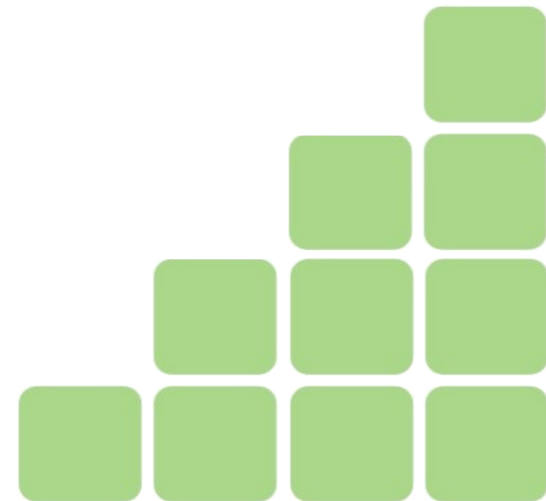
“Data carving is the process of **extracting** a collection of data from a larger data set.

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.**

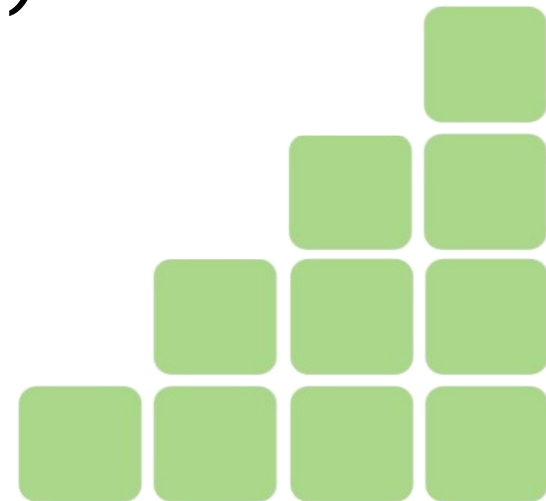
File system structures are not used during the process.”

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



Demonstração

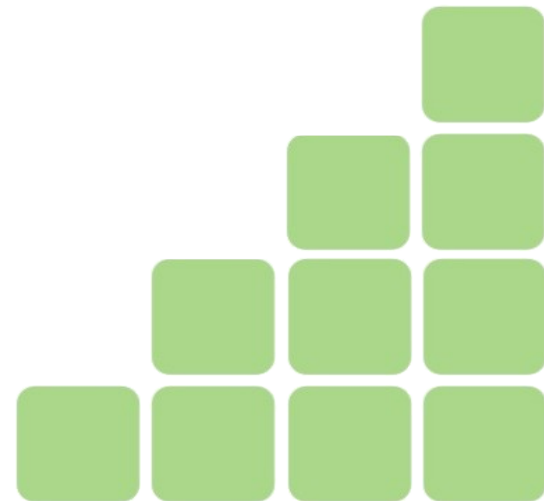
Preparando a mídia
(apagamento acidental !?)



Carving (Extração) em Mídias

Magicrescue

- 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 magicrescue**)



Carving (Extração) em Mídias

Magicrescue

.....

Funcionamento

- Executar aplicativo com parâmetros específicos

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

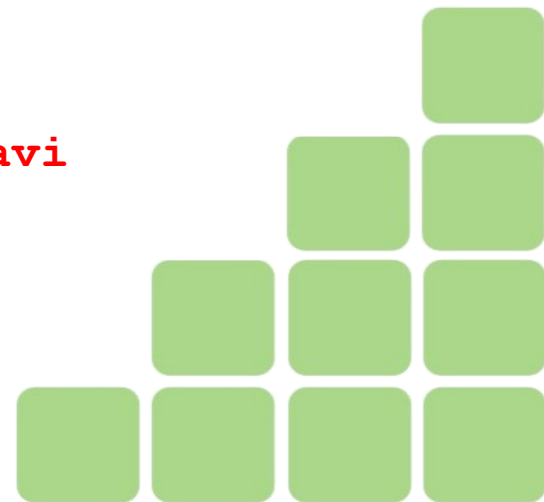
- **diretorio_destino** :: Diretório onde será gravado o resultado
- **base_tipos** :: Base com padrão do tipo de arquivo buscado

(/usr/share/magicrescue/recipes)

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

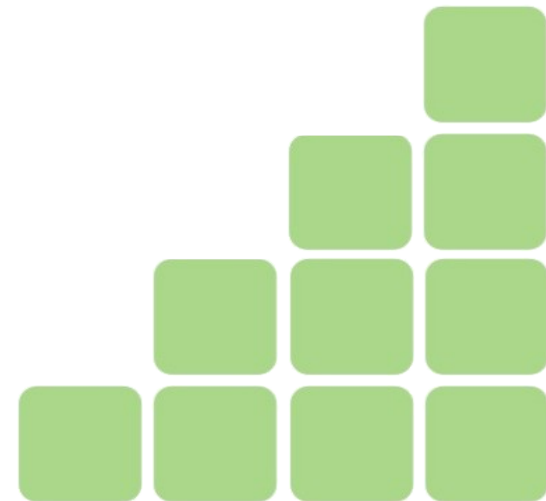
Exemplo:

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



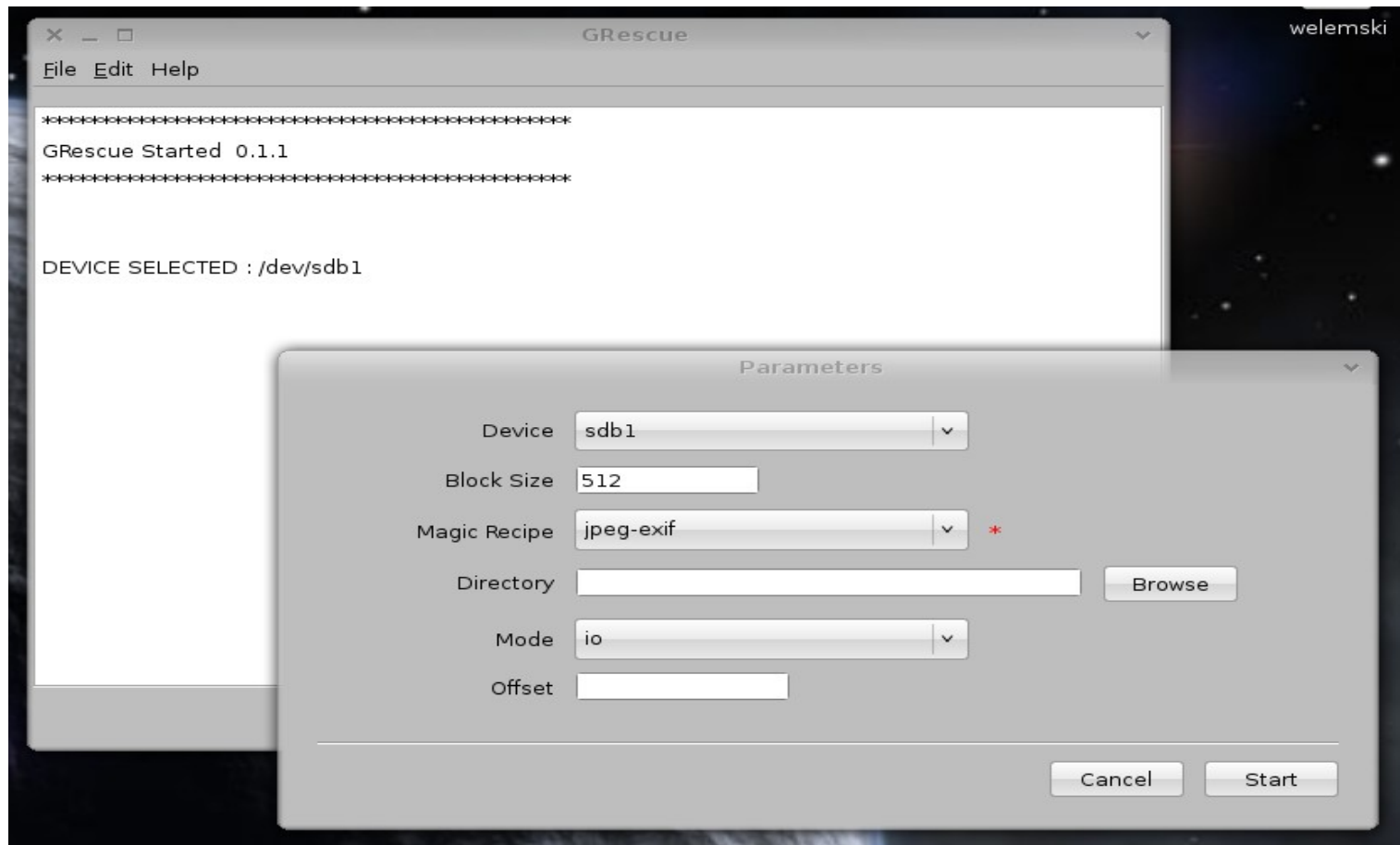
Demonstração

Data Carving com Magicrescue



Carving (Extração) em Mídias Magicrescue / GRescue

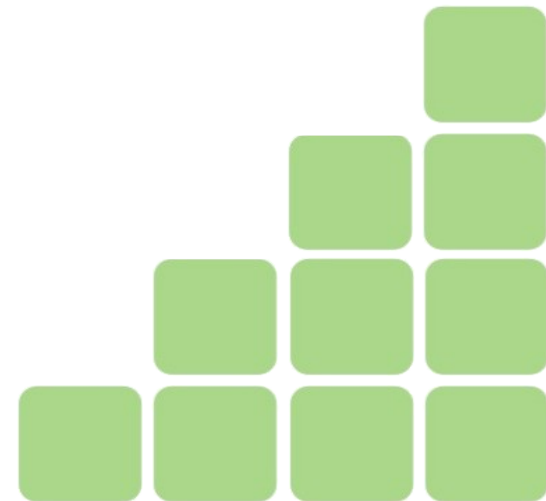
- GRescue = Interface Gráfica do Magicrescue (em desenvolvimento)



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
```



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

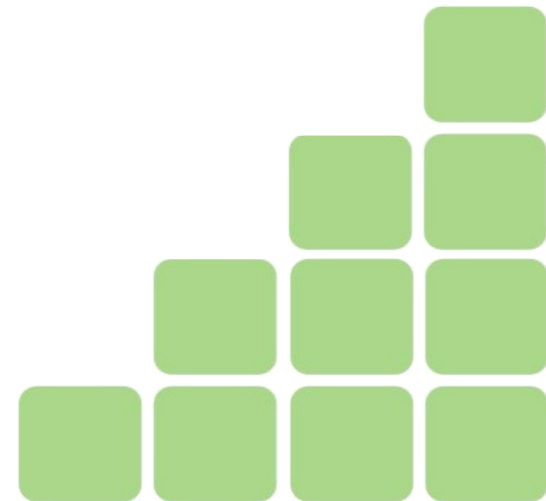
.....

- Opção sugerida para corrigir fragilidades do dd: dcfldd

Exemplo de Utilização:

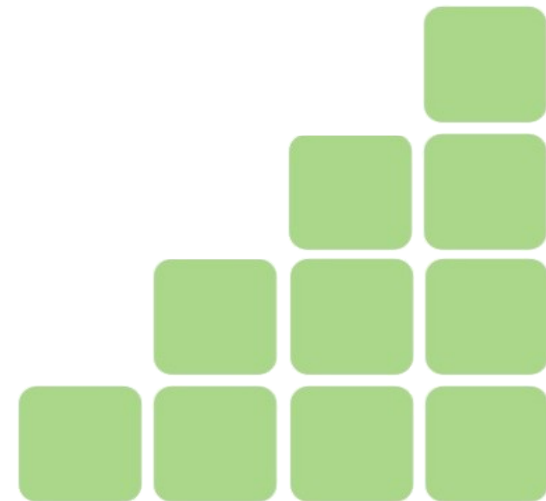
```
dcfldd if=/dev/sda1 hash=md5,sha256 hashwindow=1G \  
md5log=md5.txt sha256log=sha256.txt hashconv=after \  
conv=noerror,sync split=1G splitformat=aa of=image.dd
```

- **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 / ...



Demonstração

Duplicação de Dispositivo (Pendrive) com dcfldd



Carving em Imagem de Mídia

Magicrescue

.....

- Executar aplicativo com parâmetros específicos

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

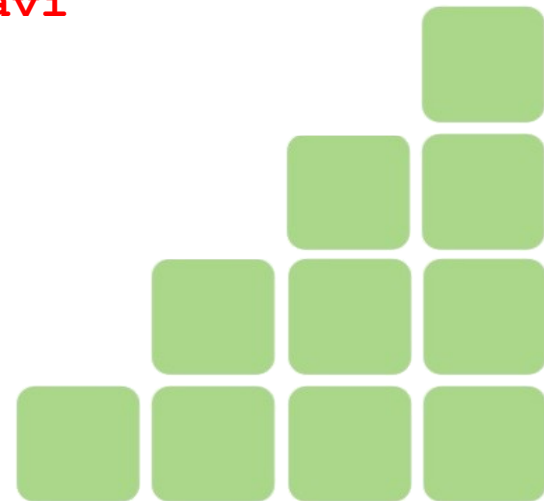
- **diretorio_destino** :: Diretório onde será gravado o resultado
- **base_tipos** :: Base com padrão do tipo de arquivo buscado

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

- **imagem** :: imagem do dispositivo analisado

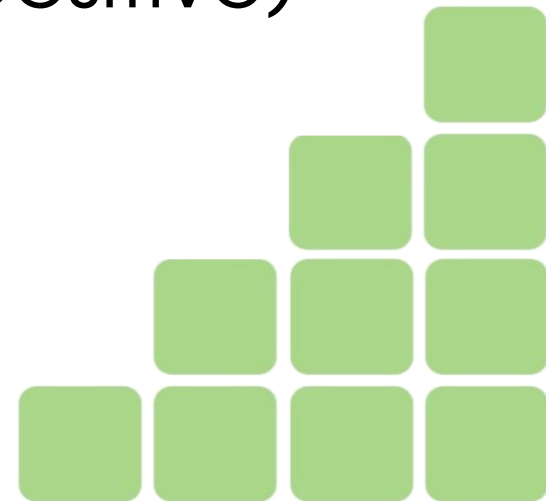
Exemplo:

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



Demonstração

Data Carving com Magicrescue
(a partir de uma imagem de dispositivo)



Carving em Imagem de Mídia

Foremost

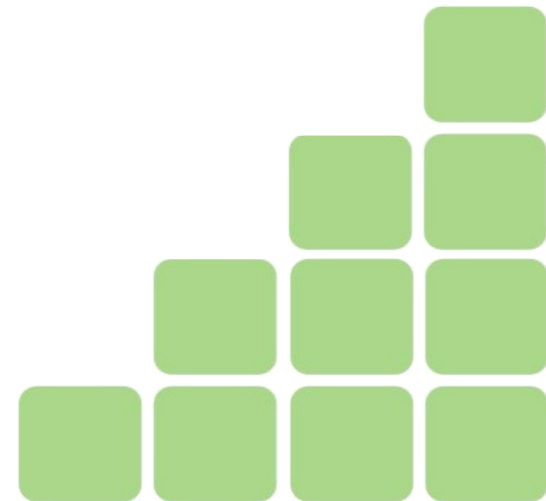
.....

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

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

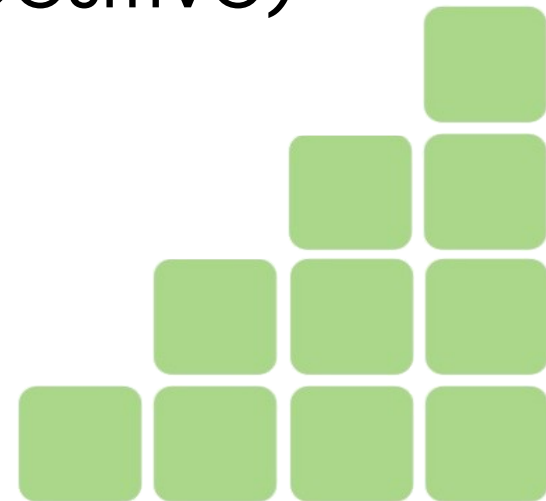
- Tipos de arquivos reconhecidos: jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, htm, cpp, ...
- Para todos os tipos de arquivos: **-t all**

Ex.: foremost pendrive.dd -o diretorio_destino



Demonstração

Data Carving com Foremost
(a partir de uma imagem de dispositivo)



Carving em Imagem de Mídia

Scalpel

.....

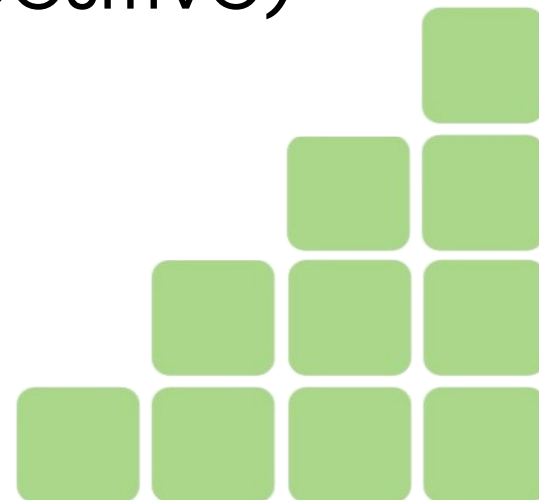
- Semelhante ao foremost: **scalpel**
- Debian-like (`apt-get install scalpel`)
scalpel <imagem> -o <destino>
- Por padrão, todos os tipos de arquivos no banco de dados (`/etc/scalpel/scalpel.conf`) estão comentados (não gera resultados se não for alterado)
- Para especificar quais tipos de arquivos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

Ex.: scalpel pendrive.dd -o diretorio_destino



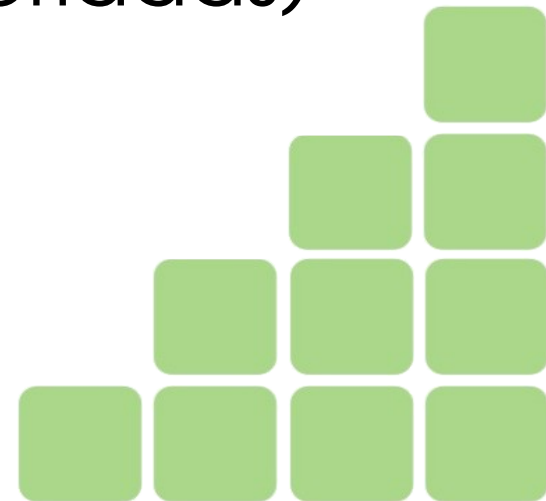
Demonstração

Data Carving com Scalpel
(a partir de uma imagem de dispositivo)



E se o alvo/objeto for Tráfego de Redes?

Capturar tráfego e realizar o realizar a
Extração (com ferramentas apropriadas)

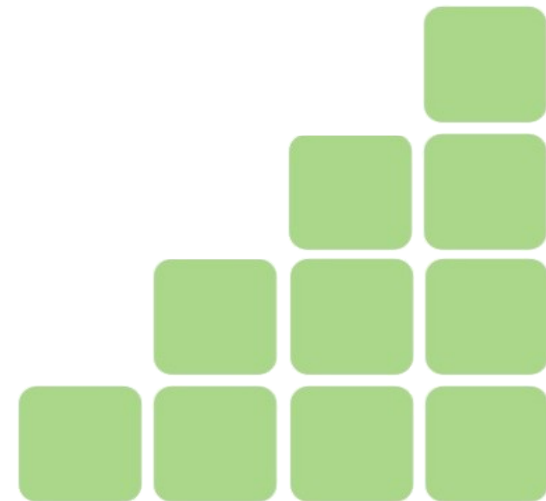


Antes do Processo de Extração Coleta em Redes

- 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]`

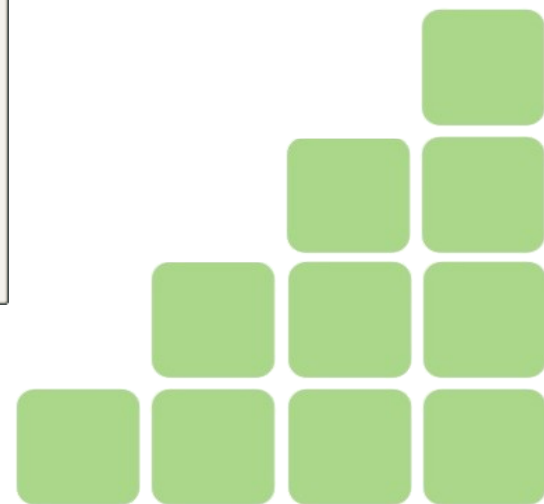
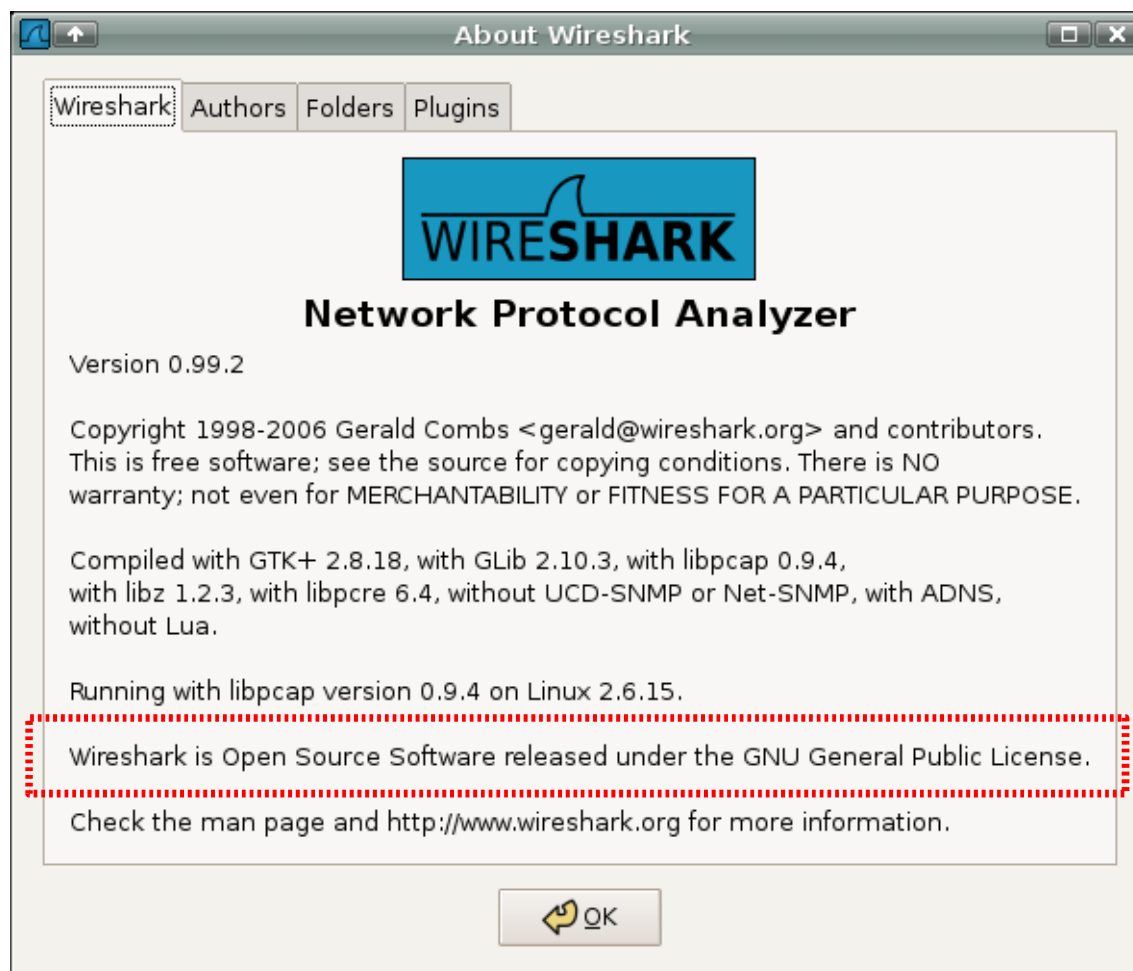
`dst [destino]`

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

Antes do Processo de Extração

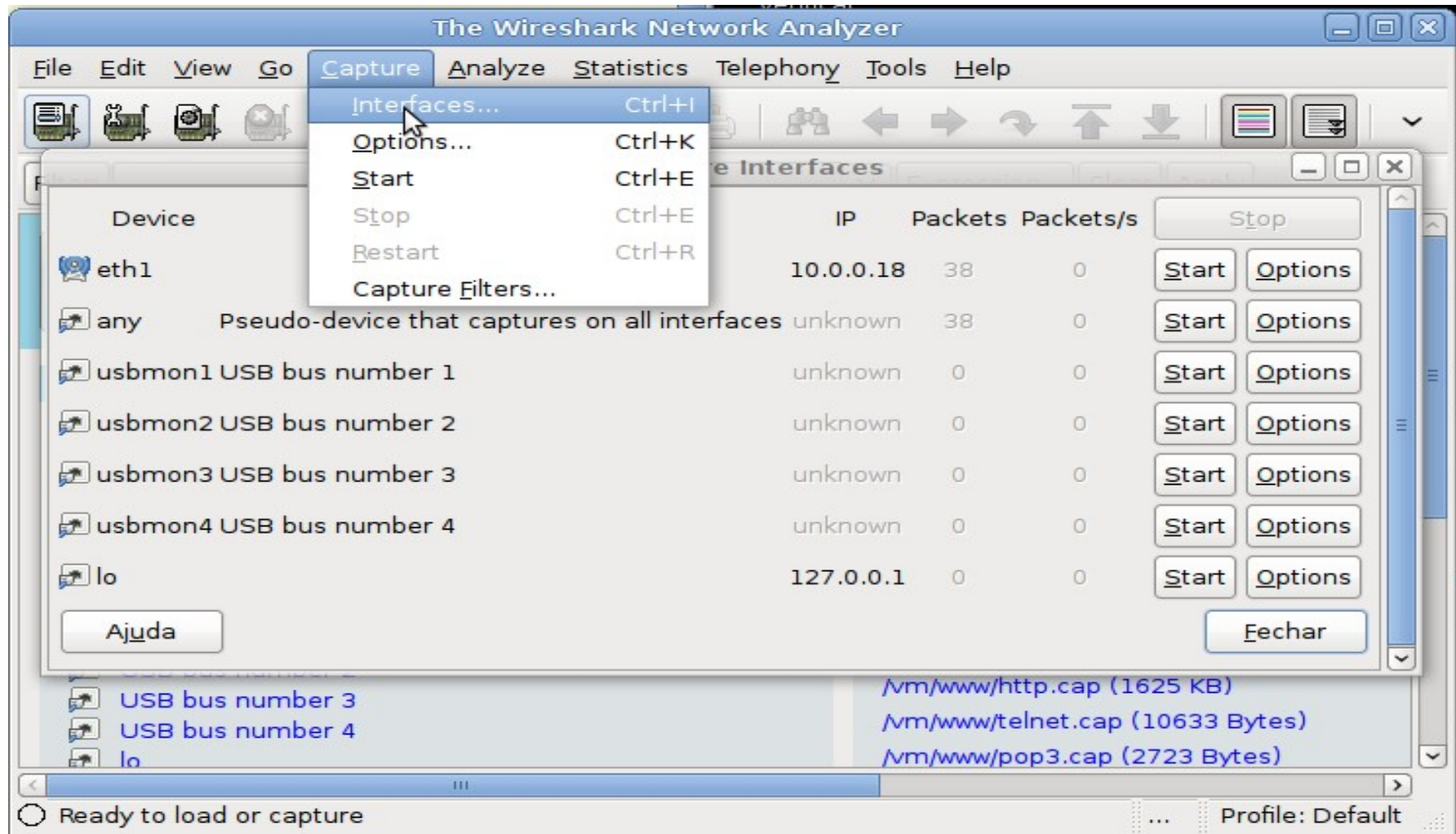
Coleta em Redes (Modo Gráfico: Ethereal/Wireshark)

<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)

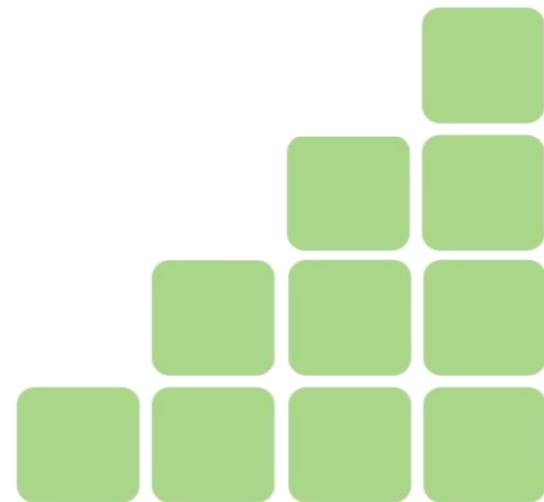
- `tcpextract -d /dev/device -o diretorio_destino`

- `tcpextract -f arquivo_cap -o diretorio_destino`

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

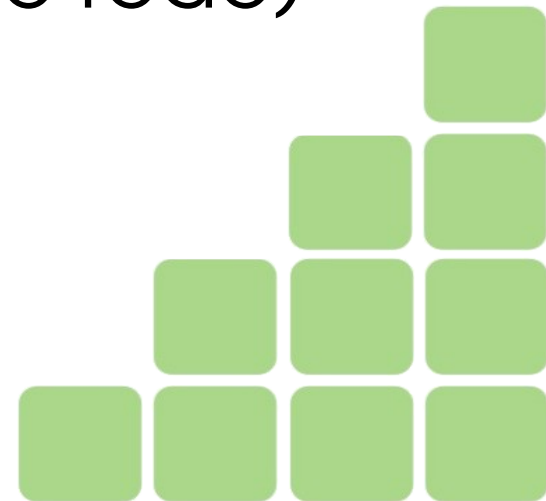
```
# tcpextract -f http.cap -o examinar
```

```
# nautilus examinar
```



Demonstração

Data Carving com Tcpxtrace
(a partir de captura de tráfego de rede)



Carving em Imagem de Tráfego de Redes

Chaosreader

.....

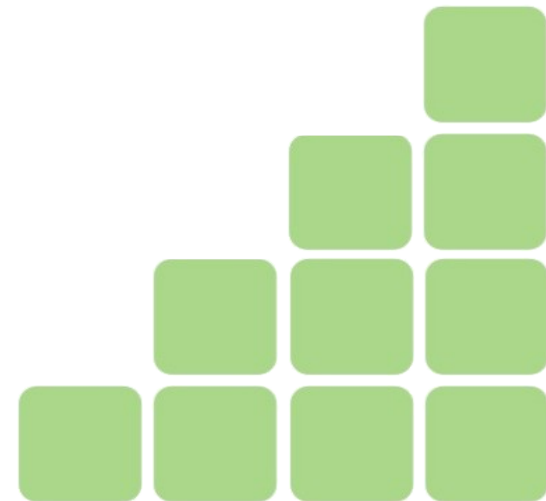
- Semelhante ao tcpextract
- Maior nível de detalhes sobre tráfegos (origem/destino)
- Gera relatório HTML (mais adequado para laudos)
- Relatório sumarizado por protocolos capturados/identificados
- Analisa arquivo .CAP (formato tcpdump)

- `chaosreader arquivo_cap -D diretorio_destino`

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

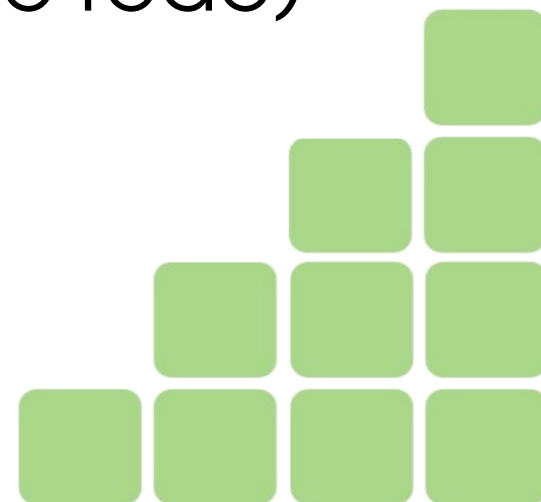
```
# chaosreader http.cap -D examinar
```

```
# firefox index.html
```



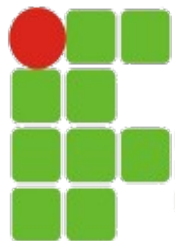
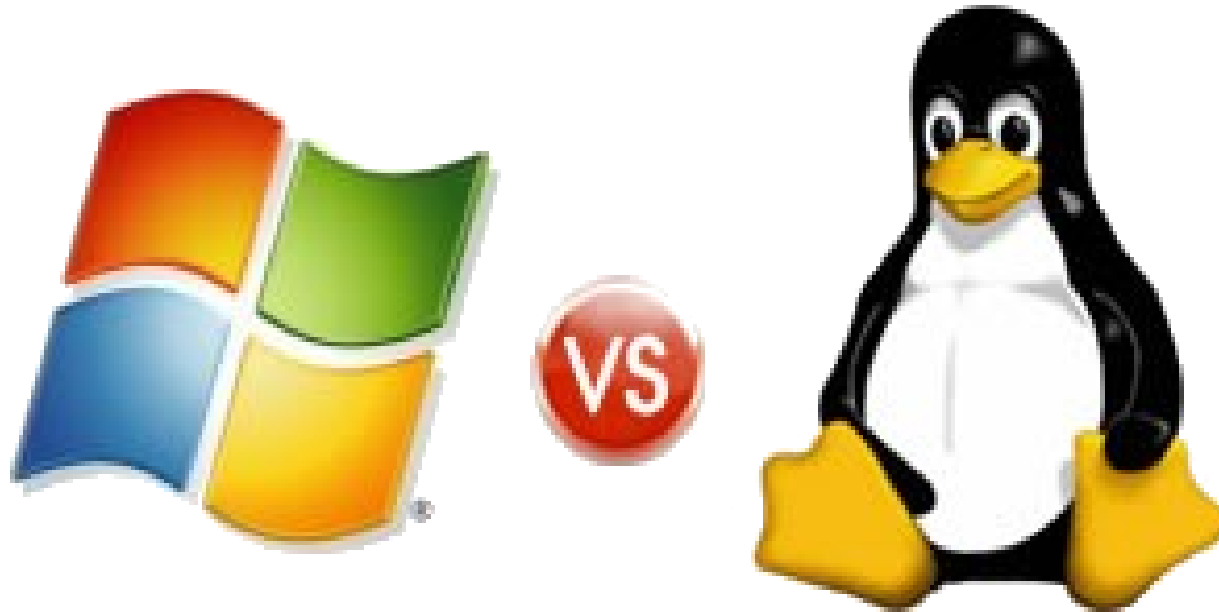
Demonstração

Data Carving com Chaosreader
(a partir de captura de tráfego de rede)



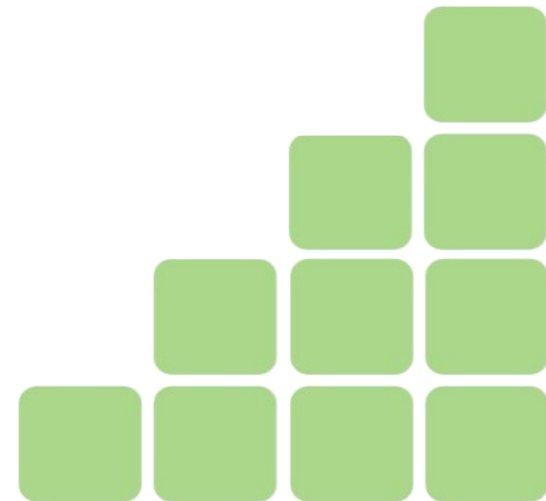
E a Plataforma Windows???

.....



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

Data Carving em Mídias e em Redes :: Ricardo Kléber



E a Plataforma Windows???

.....

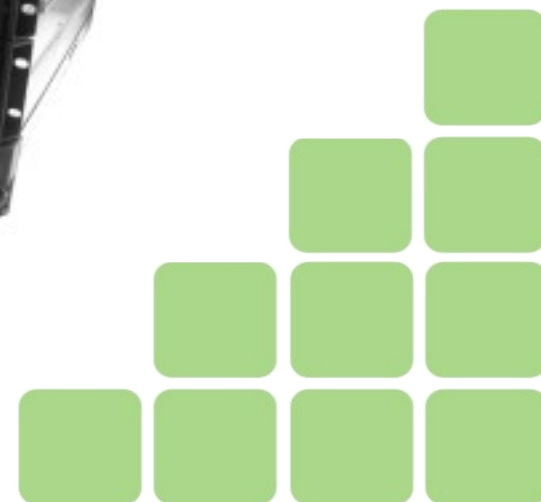
- Existem ferramentas comerciais (inclusive mais fáceis de utilizar) baseadas no sistema operacional Windows, mas esse não foi o foco desta apresentação.

- Sugestão = Netwitness



- Investigator (freeware)

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



NetWitness Investigator

100_142_2004_01_08_16_09_07.nwm:1 - NetWitness Browser

File Edit View Navigate Help

Open Close Find Report Edit Help About

Protocol
Address
Port
Alias
Size
Service
Action
Content
Properties
User
Account
test = 1
E-mail
test@tmsoft.com = 2
Resource
Database
Name
/ = 2
/banner.htm = 1
/border1.htm = 1
/css/border.css = 1
/css/default.css = 1
/css/menu.css = 1
/flash/netwitnessintro.swf =
/images/feborderrev.gif = 1
/images/felogobblue-curve.gif =
/images/menu-bkgnd.jpg = 1
/images/next.gif = 1
/images/web_logo_left.gif =
/logos/newyear04.gif = 1
/main.html = 1
/menu.asp = 1
/nav_current.gif = 1
/nav_first.gif = 1
/nav_next.gif = 1
/nav_page.gif = 1
/search = 2
/url = 1
/wanipconnection = 1
Handle


Less More First Page Prev Next Page Last Add Export

Displaying 1 - 2 of 2 sessions

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

Side 1 Side 2 Auto Details Text Strings Hex Onf Packets Mail Web Audio Save

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 /



Web Images Groups Directory News

Google Search I'm Feeling Lucky

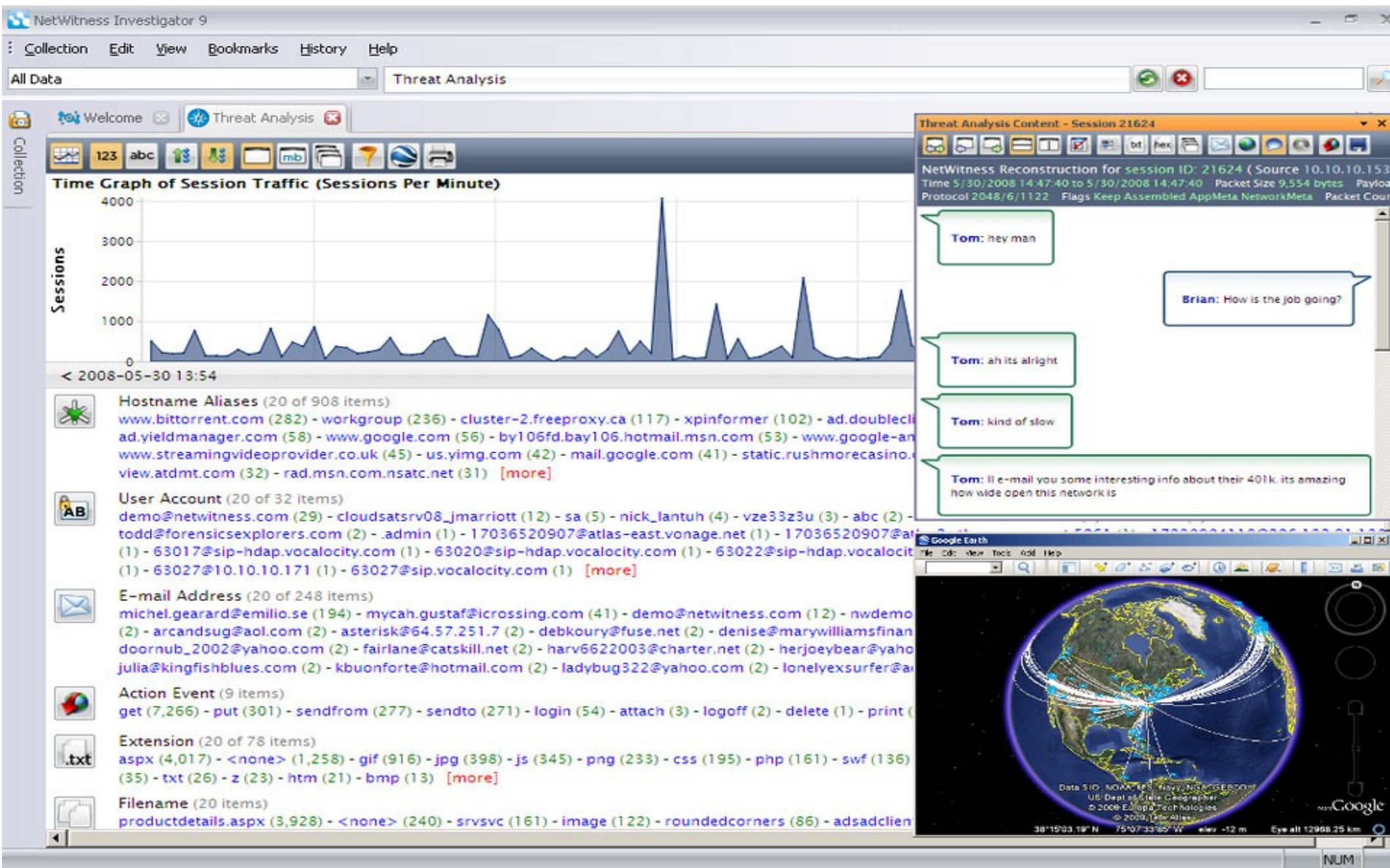
Advanced Search
Preferences
Language Tools

Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

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

Ready NUM

NetWitness Investigator



Netwitness Analysis

Forensics Explorers - NetWitness Analysis 3.53 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

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



admin is logged into NW_35

- NetWitness
 - Analysis
 - Bookmarked Groups
 - All Data
 - Sales Unit
 - Sys Admin
 - Network Report
 - Custom Report
 - Media Report
 - Alerts
 - Search
 - Chronology
 - Keyword
 - World
 - Utilities
 - Preferences
 - Change Password
 - Help
 - Logoff

Network Forensics Report for Sys Admin

1/29/2003 12:31:18 PM

Print this page

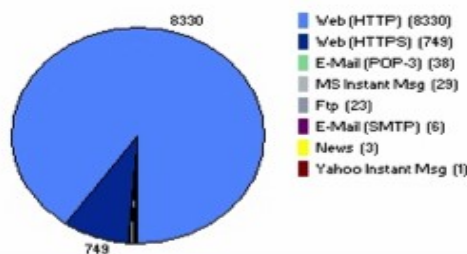
This is a forensics report. The report provides information rich statistics that enables target discovery and event analysis of computer evidence. For analysis select the total number to view event, and select the entity to build a report profiling that entity. The data group details are listed below.

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.

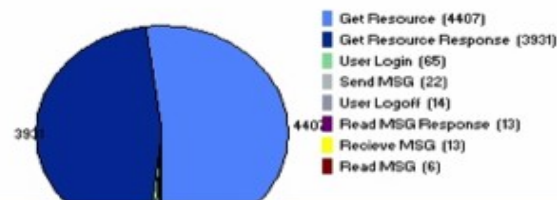
Application Type:	Session Total
Web (HTTP)	8330
Web (HTTPS)	749
E-Mail (POP-3)	38
MS Instant Msg	29
Ftp	23
E-Mail (SMTP)	6
News	3
Yahoo Instant Msg	1



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	13



[illegible]

“Resposta” Open Source



www.xplico.org

Xplico Interface User: xplico

Help Forum Wiki Logout

Case

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: ...

Interface: Choose adaptor

Start

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

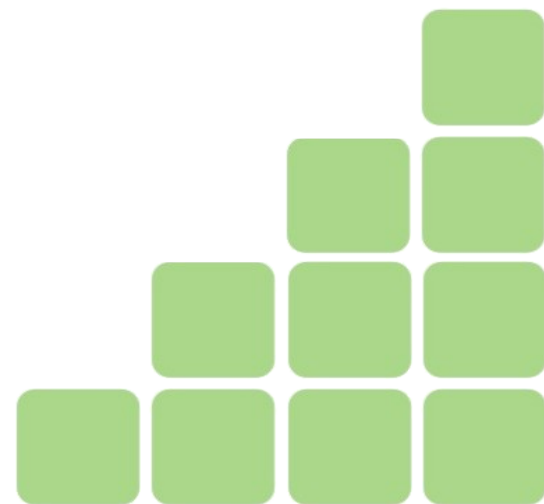
Xplico.org Version 0.5 CRACKED POWER

© 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%	—

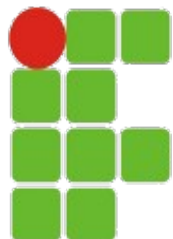
Considerações Finais

- Diversidade (e robustez) de softwares livres para *Data Carving*;
- A homologação de ferramentas para o uso pericial passa pela abertura do código (para validação);
- Se você não é (nem pretende ser) perito em informática, pelo menos espero que saiba recuperar seus arquivos apagados acidentalmente :)



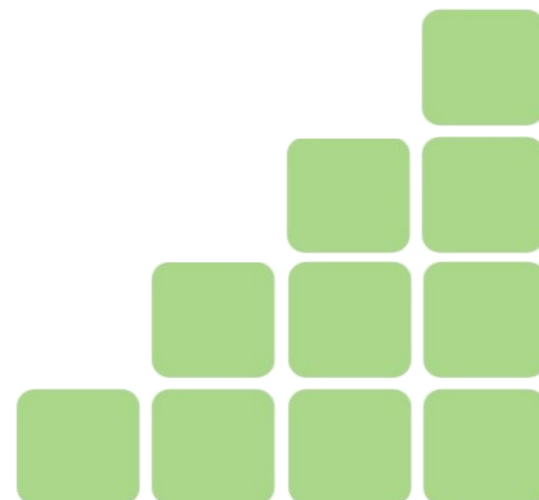
Perguntas

.....



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

Data Carving em Mídias e em Redes :: Ricardo Kléber



Para saber mais...



- (DFRWS) **Digital Forensic Research Workshop**. (<http://dfrws.org>)
- Princeton University, (2008). **Lest We Remember: Cold Boot Attacks on Encryption Keys**. Center for Information Technology Policy (<http://citp.princeton.edu/memory/>)
- Mikus, N. (2005). **An Analysis of Disc Carving Techniques** (Tese de Mestrado) (<http://handle.dtic.mil/100.2/ADA432468>)
- Kessler, Gary C. (10/2/2008). **File Signature Table**. (http://www.garykessler.net/library/file_sigs.html)
- Carrier, Brian (2005). **File System Forensic Analysis**. Addison Wesley.
- Garfinkel, Simson **File Carving**. (<http://www.forensicswiki.org/wiki/Carving>)

