GTER
GTS .br

ETHICAL HACKER ACADEMY

# Análise Forense Computacional no Sistema Operacional Windows® 8


Ricardo Kléber Martins Galvão
www.ricardokleber.com
ricardokleber@ricardokleber.com
@ricardokleber


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

# Microsoft Windows 8

## A nova "cara" do sistema Desktop da Microsoft

GTER GTS .br

## Motivação:

- Além da "estética" o que mudou (estruturalmente)?
- Técnicas e ferramentas convencionais são suficientes para uma perícia (análise forense computacional)?

# Novidades do Windows 8

## Por que isso é importante?

http://www.blogmicrosoftbrasil.com.br/windows-8-aos-seis-meses-uma-sessao-de-perguntas-e-respostas-com-tami-reller/

## Avanço no Número de Usuários:

- Em seis meses...
  - 100 milhões de licenças vendidas em 6 meses
  - 250 milhões de apps baixados pela Windows Store

Fonte: Tami Reller [marketing e finanças da Microsoft]

(07/05/2013)

# Novidades do Windows 8

## Por que isso é importante?

http://www.w3schools.com/browsers/browsers_os.asp

## Avanço no Número de Usuários:

### OS Platform Statistics

| 2013 | Win8 | Win7 | Vista | NT* | WinXP | Linux | Mac | Mobile |
|---|---|---|---|---|---|---|---|---|
| April | 7.3% | 56.4% | 2.2% | 0.4% | 16.4% | 4.8% | 9.7% | 2.2% |
| March | 6.7% | 55.9% | 2.4% | 0.4% | 17.6% | 4.7% | 9.5% | 2.3% |
| February | 5.7% | 55.3% | 2.4% | 0.4% | 19.1% | 4.8% | 9.6% | 2.2% |
| January | 4.8% | 55.3% | 2.6% | 0.5% | 19.9% | 4.8% | 9.3% | 2.2% |
| | | | | | | | | |
| **2012** | **Win8** | **Win7** | **Vista** | **NT*** | **WinXP** | **Linux** | **Mac** | **Mobile** |
| December | 2.5% | 55.6% | 2.8% | 1.8% | 21.1% | 4.7% | 8.7% | 2.2% |
| November | | 56.5% | 2.9% | 3.0% | 20.8% | 4.8% | 9.4% | 2.0% |
| October | | 56.8% | 3.0% | 1.8% | 22.1% | 4.8% | 9.2% | 1.8% |

## Analisando a Estrutura do Novo Sistema:

- Interface do Usuário (User Interface)
- Artefatos (Artifacts)
- Registro (Registry)
- Logs de Eventos (Event Logs)
- Lixeira (Recycle Bin)

# Microsoft Windows 8

## Análise Estrutural :: User Interface

- User Interface
- Artifacts
- Registry
- Event Logs
- Recycle Bin

- "Metro-Style" Interface (suporte a touchscreen)

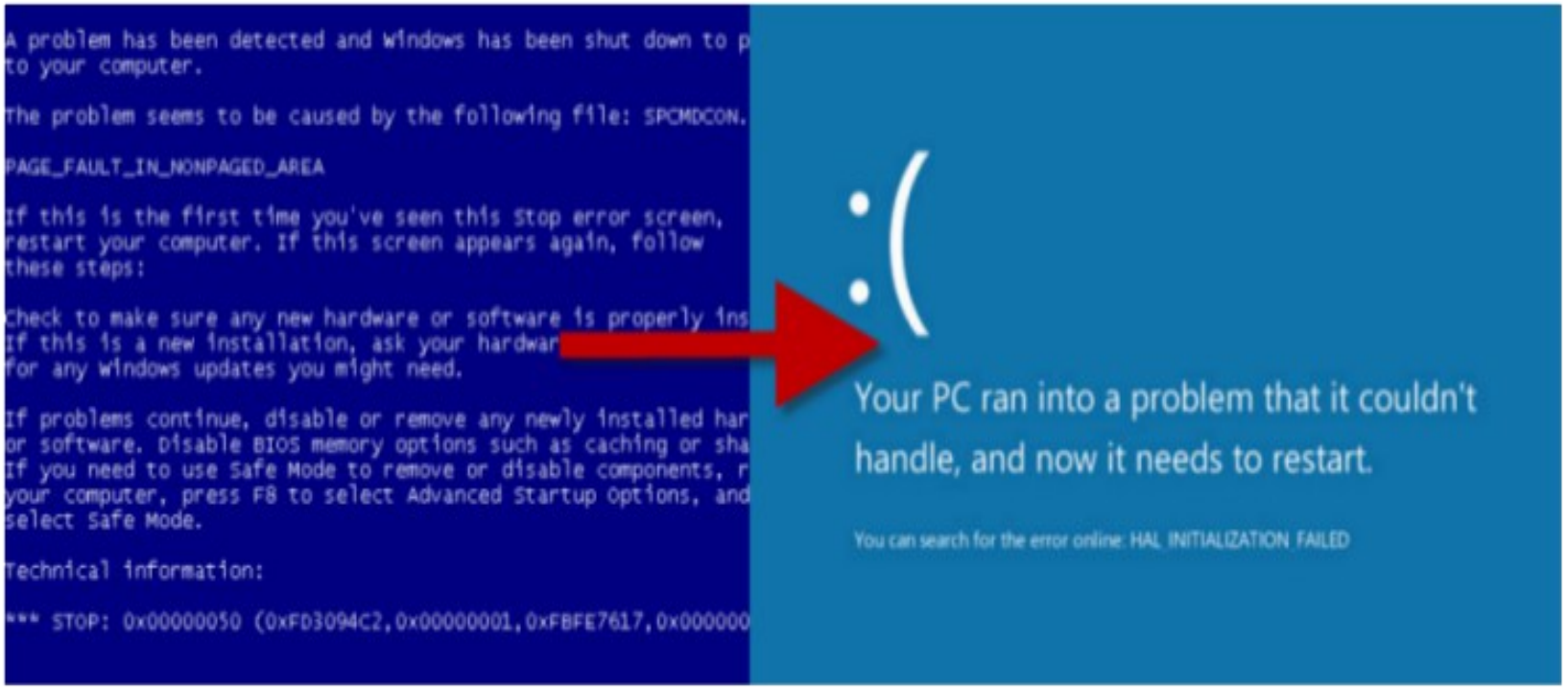

Irrelevante !? para Computação Forense

# Microsoft Windows 8

## Análise Estrutural :: User Interface

- User Interface
- Artifacts
- Registry
- Event Logs
- Recycle Bin

## A tela azul da morte mudou !!!

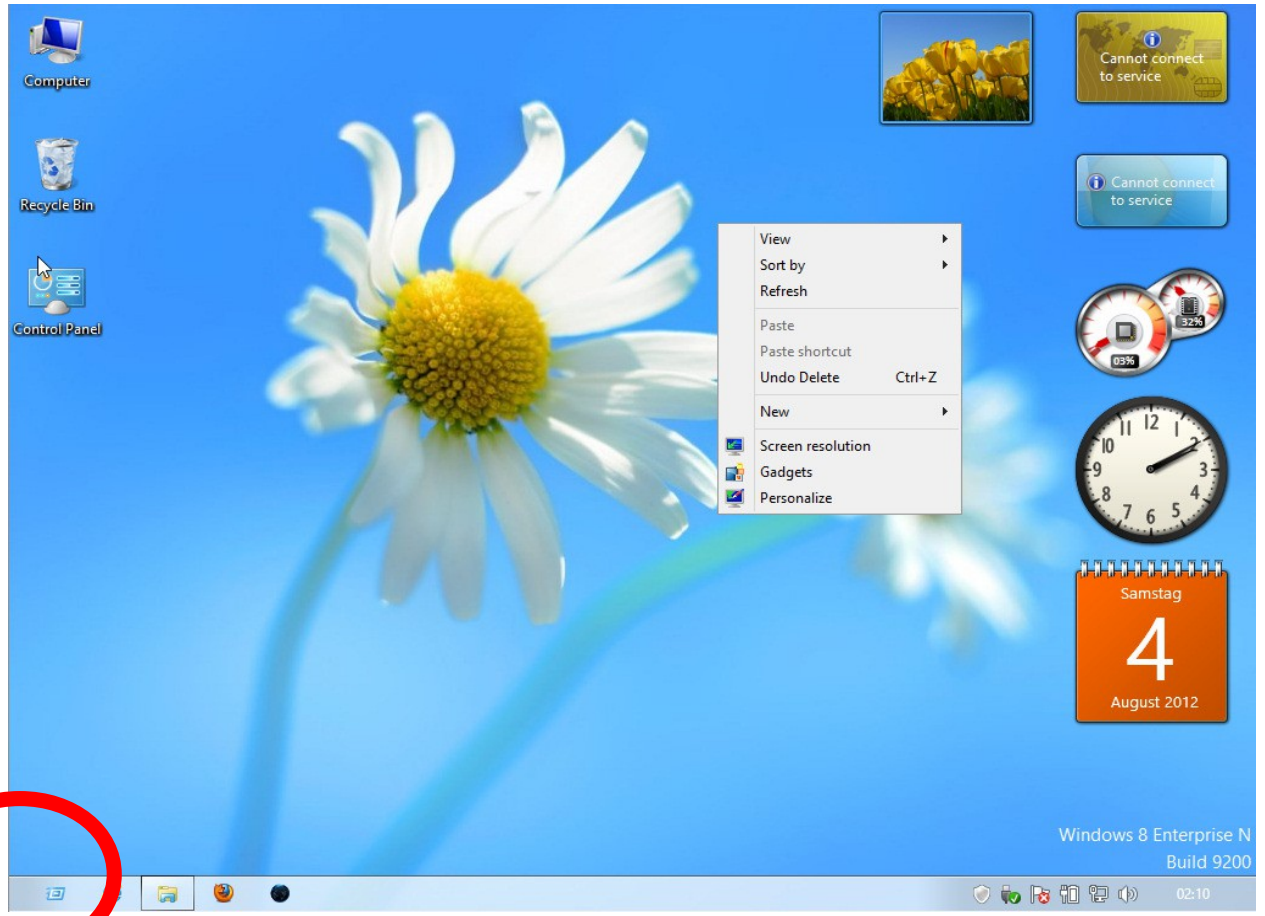



## Mas continua **AZUL :P**

- User Interface
- Artifacts
- Registry
- Event Logs
- Recycle Bin

# O Botão Iniciar “sumiu! !!!??

????



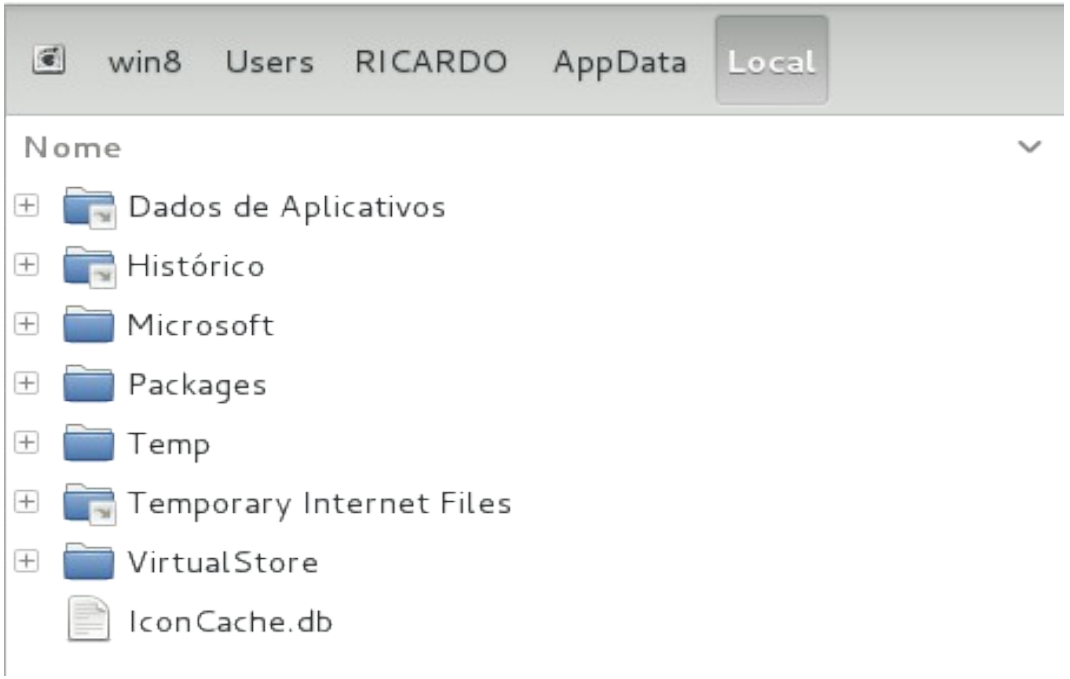

Mas a sua volta está quase certa

- Local Folder
- Metro Apps
- Internet Explorer 10
- Communication App

## Local Folder:

- Armazena dados de cada usuário em pasta específica

```
%Root%\Users\%User%\AppData\Local\
```



- Local Folder :: O que há de novo (e relevante) ?
  - Atividades Recentes do Usuário

    `%Root%\Users\%User%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations`

    `Microsoft\Windows\Recent\CustomDestinations`
  - Cookies (usados recentemente)

    `%Root%\Users\%User%\AppData\Roaming\Microsoft\Windows\Cookies`

# Microsoft Windows 8

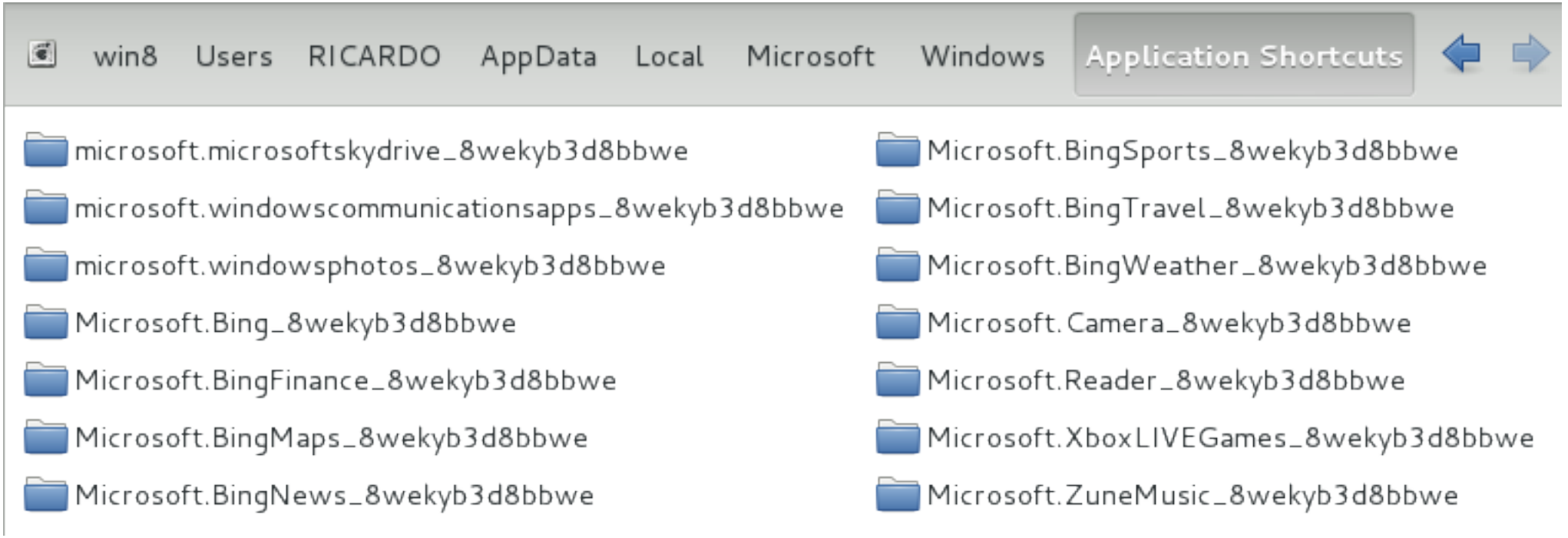
## Análise Estrutural :: Artifacts

- User Interface
- Artifacts
- Registry
- Event Logs
- Recycle Bin

## Metro Apps:

- Aplicativos (Apps) instalados e exibidos no Desktop
- Cada App no Desktop tem um arquivo (texto) de registro indicando o App que o criou e a sua localização

```
%Root%\Users\%User%\AppData\Local\Microsoft\Windows\Application Shortcurts
```



## Metro Apps:

- Metro App Cache
  - Web cache específico de cada Metro App

`%Root%\Users\%User%\AppData\Local\Packages\%MetroAppName%\AC\INetCache`

- Metro App Cookies
  - Arquivos (texto) de cookies específicos de cada Metro App

`%Root%\Users\%User%\AppData\Local\Packages\%MetroAppName%\AC\INetCookies`

- Metro App History
  - Arquivos de históricos de acesso à internet específicos de cada Metro App

`%Root%\Users\%User%\AppData\Local\Packages\%MetroAppName%\AC\INetHistory`

## Internet Explorer 10:

- No Windows 8 o browser Internet Explorer é utilizado de nas formas Imersiva (via App) e acesso direto via Desktop
- Websites Visitados por Apps de forma "Imersiva" via IE 10

  `%Root%\Users\%User%\AppData\Local\Microsoft\InternetExplorer\Recovery\Immersive\Active`

  - Websites Visitados via Internet Explorer (acessado no Desktop)

    `%Root%\Users\%User%\AppData\Local\Microsoft\InternetExplorer\Recovery\Active`

  - Cache de Páginas Visitadas via Internet Explorer

    `%Root%\Users\%User%\AppData\Local\Microsoft\Windows\WebCache\WebcacheV01.dat`

## Communication App:

- Concentra dados de acesso a serviços (Internet) como:
  - Correio Eletrônico (E-mail)
  - Redes Sociais (Twitter, Facebook, ...)
  - Serviços de Bate Papo (Chats)
  - Outros serviços de comunicação com pessoas via rede

## Communication App:

- Communication App [Web Cache]

  `%Root%\Users\%User%\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\AC\INetCache`

  - Communication App [Cookies]

    `%Root%\Users\%User%\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\AC\INetCookies`

  - Communication App [History]

    `%Root%\Users\%User%\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\AC\INetHistory`

## Communication App (User Contacts):

- Contatos de Usuários de Communication Apps

  %Root%\Users\%User%\AppData\Local\Packages\
  microsoft.windowscommunicationsapps_8wekyb3d8bbwe\
  LocalState\LiveComm\%Rótulo do Endereço WindowsLive do Usuário%\
  %Versão do Appn%\DBStore\LogFiles\

  edb.log

  edb00002.log

  edb###.log

  edbtmp.log

# Microsoft Windows 8

## Análise Estrutural :: Registry

- User Interface
- Artifacts
- Registry
- Event Logs
- Recycle Bin

- SAM
- SYSTEM
- SOFTWARE
- SECURITY
- NTUSER.DAT (para cada usuário)
- BBI (Browser-Based Interface)
- COMPONENTS
- DRIVERS
- ELAM (Early Launch Anti-Malware)

} Novidade !!!

- User Interface
- Artifacts
- Registry
- Event Logs
- Recycle Bin

## SAM :: Informações Relevantes (pré-existentes)

`%System Root%\Windows\System32\Config\SAM`

- Último Login do Usuário [LastLogon]
- Última Mudança de Senha [LastPasswordChange]
- Expiração de Conta [Account Expiration]
- ÚLtima vez que que o Login Falhou [LastFailedLogon]
- Primeiro Nome do Usuário [GivenName]
- Sobrenome do Usuário [Surname]

## SAM :: O que há de novo (e relevante) ?

- Nome de Usuário na Internet (Internet User Name)

  `%System Root%\Windows\System32\Config\SAM`

  `Domains\Account\Users\InternetUserName`

- Identificador de UserTile

  `%System Root%\Windows\System32\Config\SAM`

  `Domains\Account\Users\UserTile`

## SYSTEM :: Informações Relevantes (pré-existentes)

`%System Root%\Windows\System32\Config\SYSTEM`

- **Nome do Computador** (ComputerName)

  `ControlSet001\Control\ComputerName\ComputerName`

  - **Dispositivos de Armazenamento** (STORAGE)

    `ControlSet001\Enum\STORAGE`

  - **Dispositivos de Armazenamento USB** (USBSTOR) [desde Win7]

    `ControlSet001\Enum\USBSTOR`

    - Vendor ID, Product ID, Revision Number, Serial Number
    - Nova Sub-Key: Dispositivos Montados (Mounted Devices)

- User Interface
- Artifacts
- Registry
- Event Logs
- Recycle Bin

## SYSTEM :: Informações Relevantes (pré-existentes)

`%System Root%\Windows\System32\Config\SYSTEM`

- Lista e detalhes de Drivers Instalados (Driver Database)
  - DriverFiles / DriverInfFiles / DriverPackages
  - Impressoras

    ControlSet001\Enum\SWD\PRINTENUM\%Id_Impressora%\FriendlyName

## SOFTWARE :: Informações Relevantes (pré-existentes)

`%System Root%\Windows\System32\Config\SOFTWARE`

`Microsoft\WindowsNT\CurrentVersion\`

- CurrentBuild
- CurrentVersion
- EditionID
- InstallDate
- ProductName
- Registered (empresa)
- RegisteredOwner (usuário)

# SOFTWARE :: O que há de novo (e relevante) ?

- Metro Apps Instalados no Sistema

  `%System Root%\Windows\System32\Config\SOFTWARE`

  `Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\Applications`

- Metro Apps Instalados para um Usuário do Sistema

  `%System Root%\Windows\System32\Config\SOFTWARE`

  `Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\%SID%`

## NTUSER.DAT :: Informações Relevantes (pré-existentes)

`%System Root%\Users\%User%\NTUSER.DAT`

- **Documentos Acessados Recentemente**

  `Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`

- **Sites (URLs) Visitados**

  `Software\Microsoft\Internet Explorer\TypedURLs`

---

## NTUSER.DAT :: O que há de novo (e relevante) ?

- **Data/Hora de Acesso a Sites (URLs)**

  `Software\Microsoft\Internet Explorer\TypedURLsTime`

## BBI (Browser-Based Interface)

- Dados de configuração do Windows Live
- Usado em conjunto com os Metro Apps

- %System Root%\Windows\System32\Config\BBI
  - Events
    - {07637a49-713b-4114-8776-585cb1d48193}
      - BrokerId, EventInformation, Flags, PackageFullName, UserSid, EventType
    - (...)
  - WorkItems
    - {ff5cb789-f2e6-414c-a221-ac63d644c596}
      - ActivationType, Conditions, Flags, Name, TriggerEvent, TaskEntryPoint
    - (...)

- User Interface
- Artifacts
- Registry
- Event Logs
- Recycle Bin

## COMPONENTS

%System Root%\Windows\System32\Config\COMPONENTS

- Canonical Data
  - Catalogs
  - Deploy
- Configuration
- Derived Data
  - Components
  - VersionedIndex
    - 6.2.9200.16384 (win8_rtm.120725-1247)
      - Component Families
  - Installers
    - Shortcurt
  - Servicing Stack Versions
  - ccpinterface

- User Interface
- Artifacts
- Registry
- Event Logs
- Recycle Bin

## DRIVERS

%System Root%\Windows\System32\Config\DRIVERS

- Driver Database
  - Device Ids
  - Driver Files
  - Driver Inf Files
  - Driver Package

## ELAM (Early Launch Anti-Malware)

- Dados de configuração do Windows Defender e aplicativos relacionados

%System Root%\Windows\System32\Config\ELAM

- Windows Defender
  - Measured

- Logs de Eventos (Event Logs)

`%System Root%\Windows\System32\winevt\Logs`

  - System.evtx
  - Setup.evtx
  - Security.evtx
  - Operational.evtx
  - Application.evtx
  - HardwareEvents.evtx
  - *******.evtx

- Mudou a localização
- Alterou a extensão (.evt p/ .evtx)
- Diversificou
  (cada App tem seu log específico)

- Lixeira : Pasta Única + SID (por usuário)

  `%System Root%\$Recycle.Bin\%USER_SID%`

  - Arquivos Apagados (e não excluídos da Lixeira)
  - Pasta pode ser referenciada para recuperação de arquivos apagados utilizando ferramentas específicas

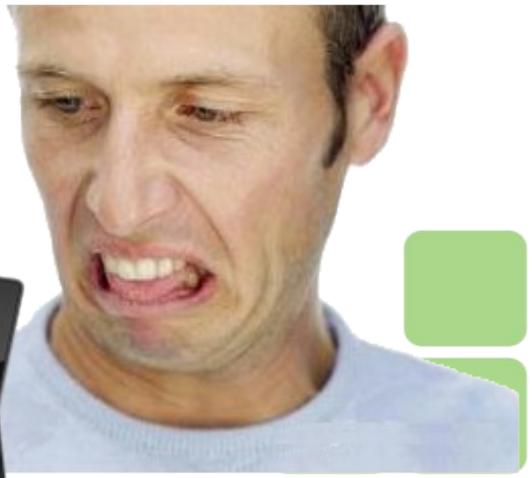
# Microsoft Windows 8

## Análise Estrutural :: Outros Recursos

- Recovery Drive (PC Refresh / PC Reset)
- Bitlocker (Driver Encryption)
- Sky Drive (Free Cloud)
- Arquivos Adicionais (classificados) de caches Thumbs
  - Novo formato [ ferramenta Vinetto fail :( ]
- Iso Automount
- Suporte a USB3

# ESTUDO DE CASO

Windows® 8



## Colocando a mão na massa...

## Roteiro do Estudo de Caso:

- Instalar o sistema operacional Windows 8
  - Em uma máquina virtual (Virtualbox); e/ou
  - Em uma máquina real
- Executar operações comuns de usuário no sistema
  - Acessar sites, conectar dispositivos externos, abrir arquivos e criar contas
- Fazer uma imagem (raw) da(s) partição(ões) do sistema
- Analisar arquivo de imagem da(s) partição(ões) do sistema
- Fazer um dump da memória do sistema
- Analisar arquivo de dump de memória

# Instalar o sistema operacional Windows 8:

- Comprar uma licença !!??
  - R$ 359,00
  - R$ 610,00 (versão pró)

Atualização do Windows 8
R$ 359,00 (Preço estimado)*


Atualização do Windows 8 Pro
R$ 610,00 (Preço estimado)*

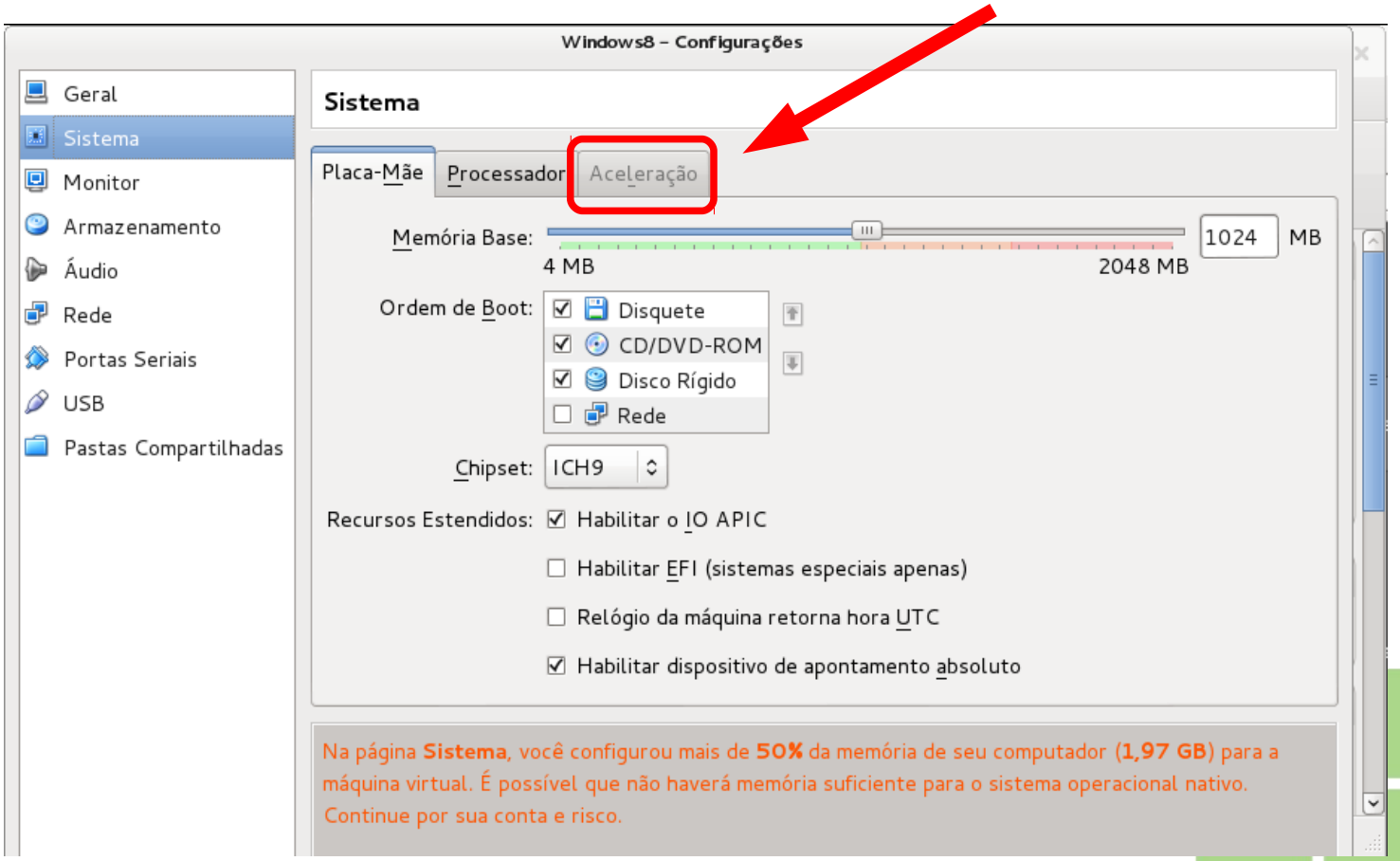

  - http://windows.microsoft.com/pt-BR/windows/buy

- Baixar versão "Enterprise Evaluation"
  - http://msdn.microsoft.com/windows/apps/br229516/
    - Versão especial disponibilizada para desenvolvedores/testes (90 dias)
    - Sem possibilidade de atualização
    - Registro obrigatório / logon conta Microsoft (ou nome/email/país)
    - 10 dias para ativação (on-line) após instalação
    - Não é necessária chave de ativação do produto

# Instalação do Windows 8 em máquina virtual (Virtualbox):

## - Sistema utilizado não suporta Virtualização por Hardware

- Pré-requisito para instalação (do Windows 8) em ambiente virtualizado



# Instalação do Windows 8 em máquina real:

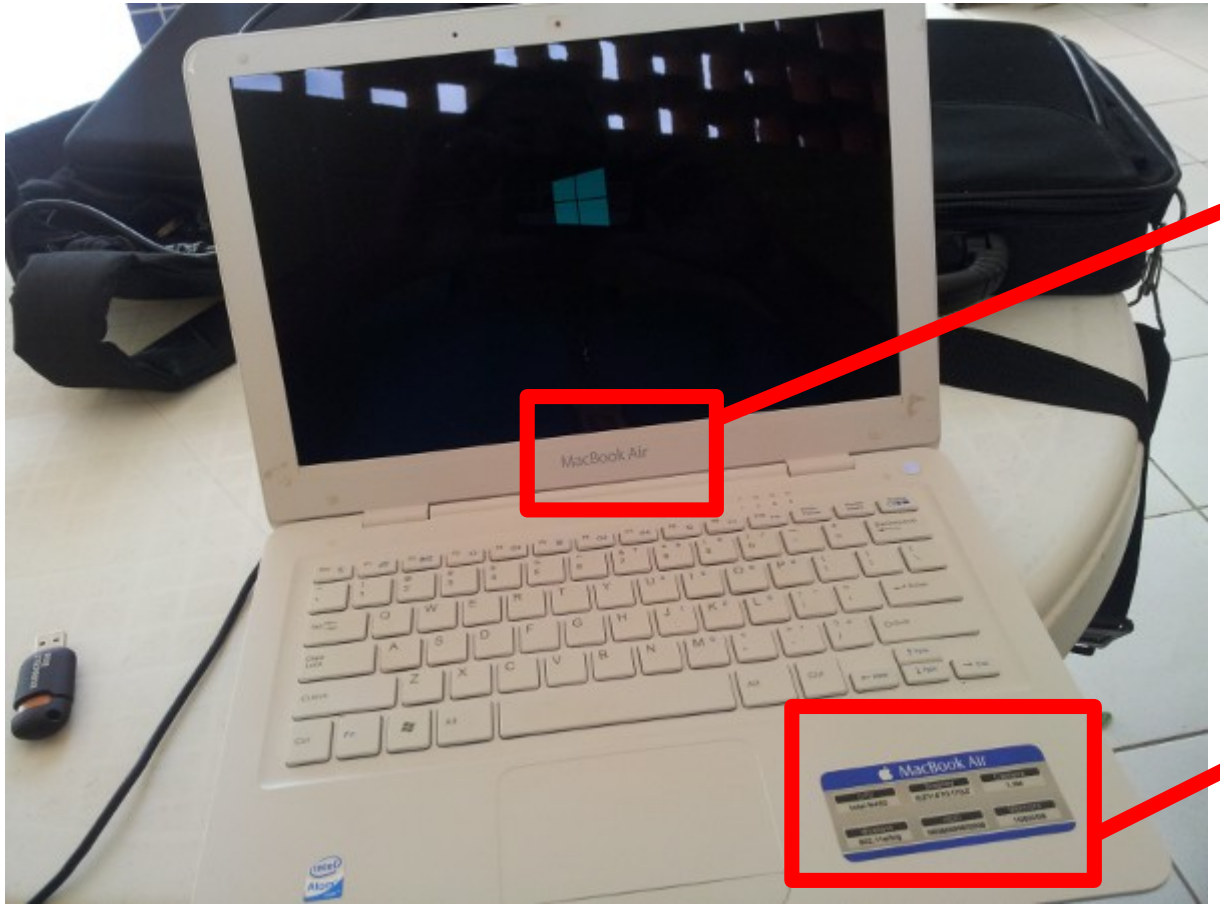
## - Requisitos (mínimos) recomendados:

- Processador: 1 GHz ou mais rápido
- RAM: 1 GB (32 bits) ou 2 GB (64 bits)
- Espaço do disco rígido: 16 GB (32 bits) ou 20 GB (64 bits)
- http://msdn.microsoft.com/pt-br/evalcenter/jj554510.aspx

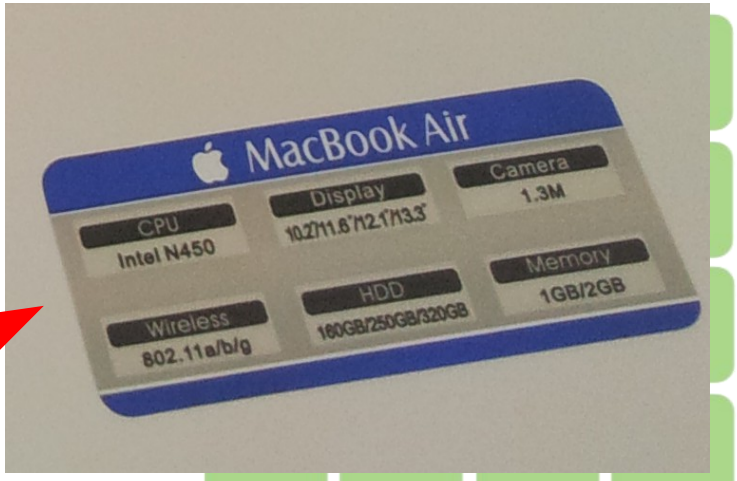
# Instalação do Windows 8 em máquina real:

## - Equipamento Utilizado:

- Macbook Air (clone) = Xingling chinês ☺ (thanks DealExtreme)







# Instalação do Windows 8 em máquina real:


- Processador:
  - Intel Atom N450
  - 1.66 GHz
- Memória RAM: 1 GB
- Espaço em Disco: 10 GB
  - Instalação utilizou 2 partições:
    - 350MB
    - 9,5GB

# Imagem (raw) da(s) partição(ões) do Sistema:

## - Boot na estação com Live-USB:

- Distribuição Utilizada: Kali Linux 1.0
- http://www.kali.org
- Substituto da Distribuição BackTrack
- Diversas ferramentas para Análise Forense / Pentest
- Ferramenta Utilizada para imagem = dcfldd
- Instalação do Windows 8 utilizou 2 partições
  - Imagem das duas partições do sistema:

```
# dcfldd if=/dev/sdb1 of=/media/pendrive/win8_part01.dd
# dcfldd if=/dev/sdb2 of=/media/pendrive/win8_part02.dd
```

## Coletando Informações do Sistema de Arquivos

- Montando a imagem do disco sem permissão de escrita:

```
# mkdir /media/win8
# mount /imagens/win8_part02.dd /media/win8 -o ro,loop
```

- O acesso e análise aos arquivos importantes do sistema de arquivo podem ser feitos normalmente sem o risco de alteração
- Para o acesso foi utilizado o gerenciador de arquivos padrão do Debian Linux: Nautilus

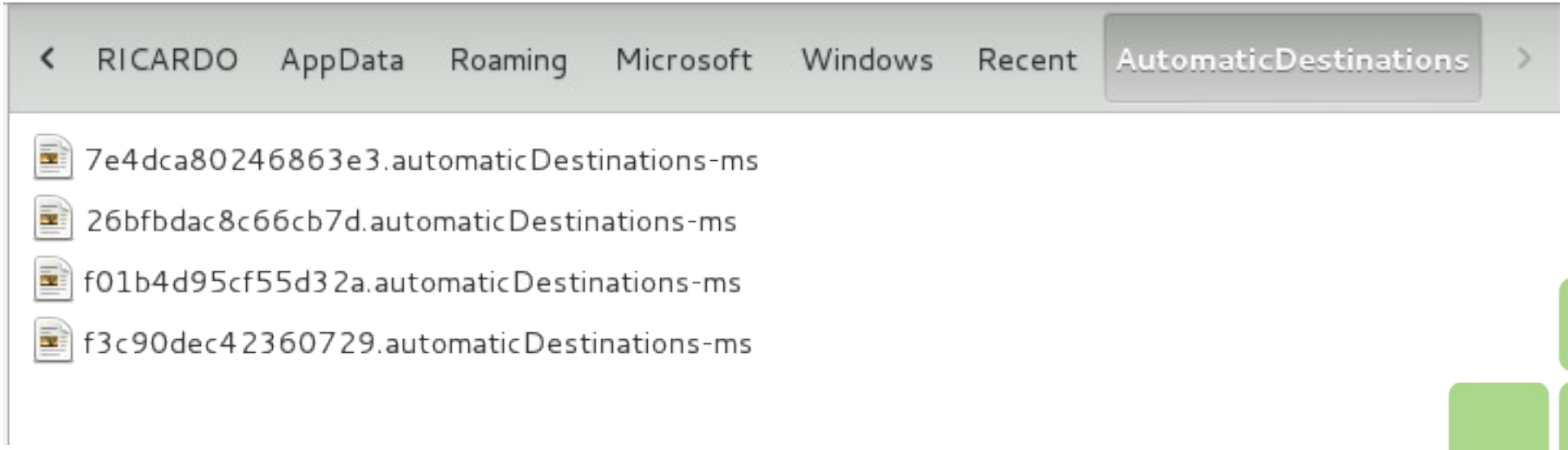
```
# nautilus /media/win8
```

## Local Folder :: (Usuário RICARDO)

```
\media\win8\Users\RICARDO\AppData\Local\
```

## Local Folder :: (Usuário RICARDO) :: Atividades Recentes

```
\media\win8\Users\RICARDO\AppData\Roaming\
Microsoft\Windows\Recent\AutomaticDestinations
```



## Local Folder :: (Usuário RICARDO) :: Atividades Recentes

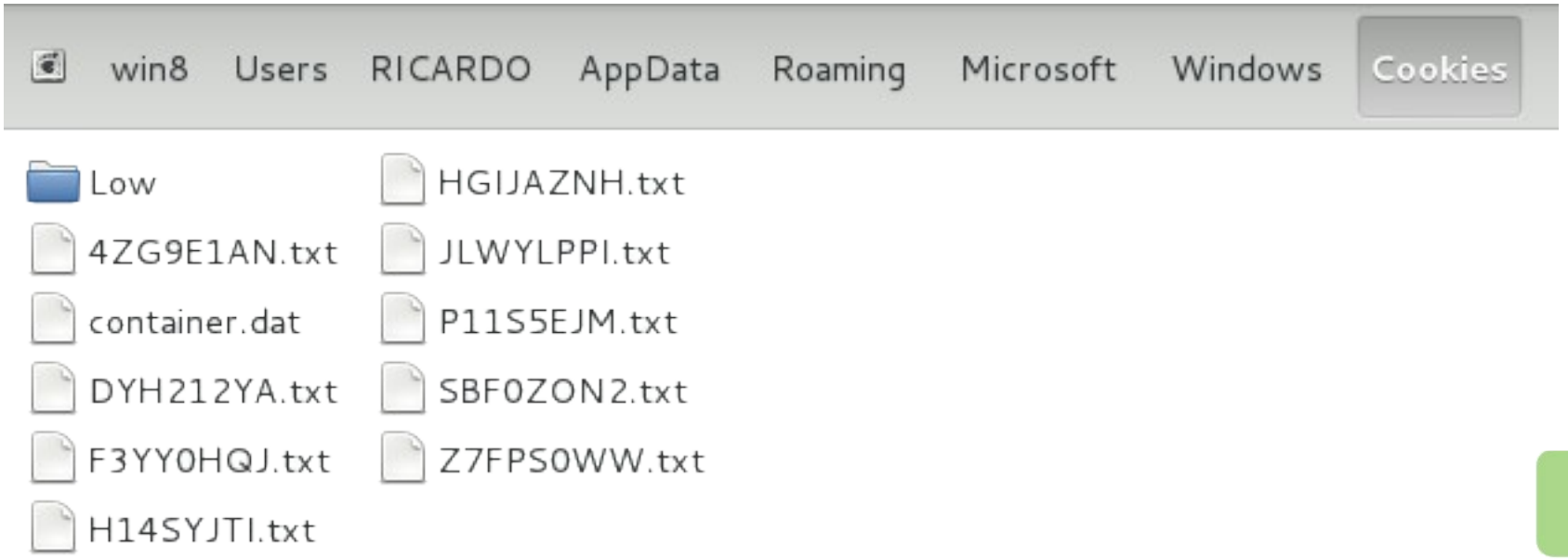
```
\media\win8\Users\RICARDO\AppData\Roaming\
Microsoft\Windows\Recent\AutomaticDestinations
```

- Acesso a arquivos com Editor Hexadecimal (Hexdump)

```
# hexdump -C 26bfbdac8c66cb7d.automaticDestinations-ms
*
00000d90  00 00 0b 00 00 00 00 00  00 00 00 00 80 3f 13 36  |.............?.6|
00000da0  5c 19 7c 55 ce 01 ff ff  ff ff 14 00 44 00 3a 00  |\.|U........D.:.|
00000db0  5c 00 66 00 6f 00 74 00  6f 00 73 00 5c 00 72 00  |\.f.o.t.o.s.\.r.|
00000dc0  6b 00 5f 00 30 00 30 00  31 00 31 00 2e 00 70 00  |k._.0.0.1.1...p.|
00000dd0  6e 00 67 00 fb 10 c1 4a  8c 3e 1f cc 00 00 00 00  |n.g....J.>......|
00000de0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
```

## Local Folder :: (Usuário RICARDO) :: Cookies Recentes

```
\media\win8\Users\RICARDO\AppData\Roaming\
Microsoft\Windows\Cookies
```



## Local Folder :: (Usuário RICARDO) :: Cookies Recentes

```
\media\win8\Users\RICARDO\AppData\Roaming\
Microsoft\Windows\Cookies
```

- Acesso a arquivos com Extrator de Cookies (Galleta)

```
# galleta F3YY0HQJ.txt
Cookie File: F3YY0HQJ.txt

SITE         VARIABLE   VALUE  CREATION     TIME       EXPIRE       TIME       FLAGS
c.live.com/  MR         0      05/20/2013   14:33:32   06/19/2013   14:26:35   1024
c.live.com/  ANONCHK    1      05/20/2013   14:33:32   05/23/2013   14:26:35   1024
```

## Coletando Informações do Registro

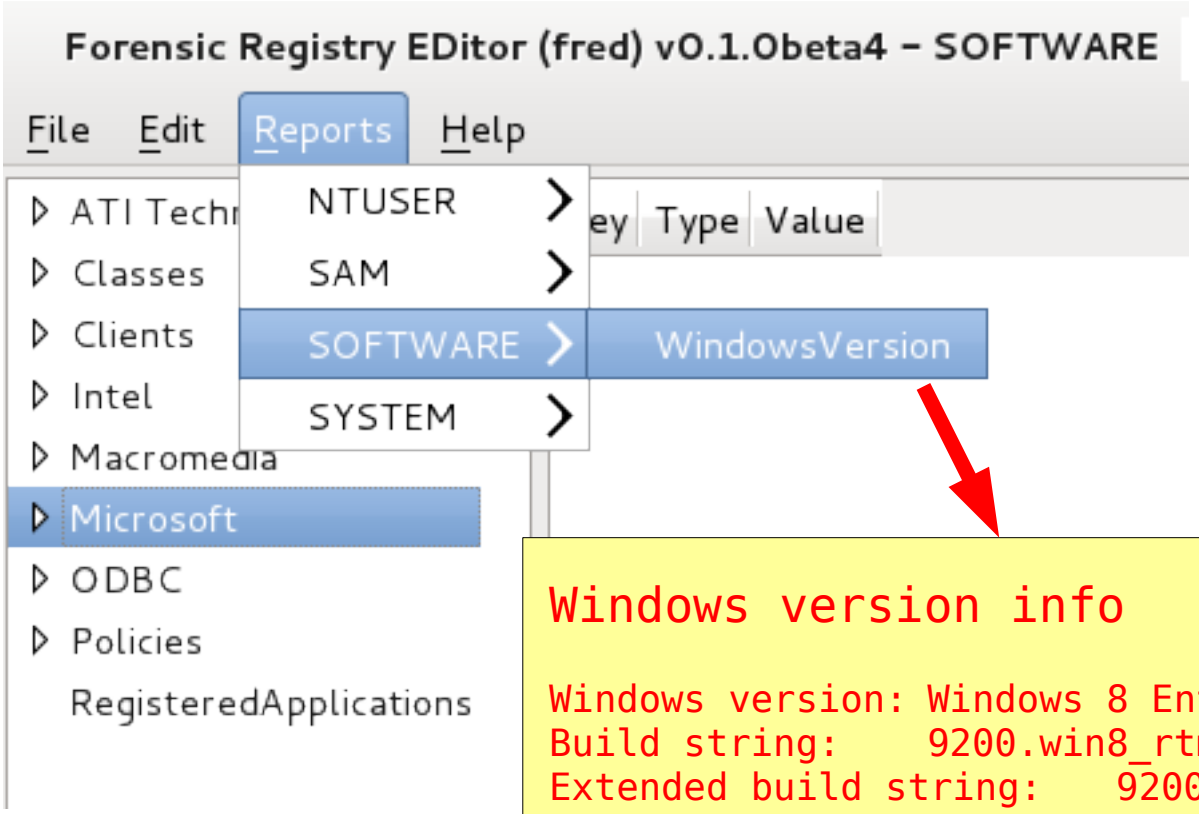
- Copiar registros/hives para manipular com ferramentas específicas

```
# mkdir /root/forense/win8
# cd /media/win8/Windows/System32/config
# cp SAM /root/forense/win8
# cp SYSTEM /root/forense/win8
# cp SOFTWARE /root/forense/win8
# cp SECURITY /root/forense/win8
# cd /media/win8/Users/RICARDO
# cp NTUSER.DAT /root/forense/win8
```

## Manipulando/Analisando Informações do Registro

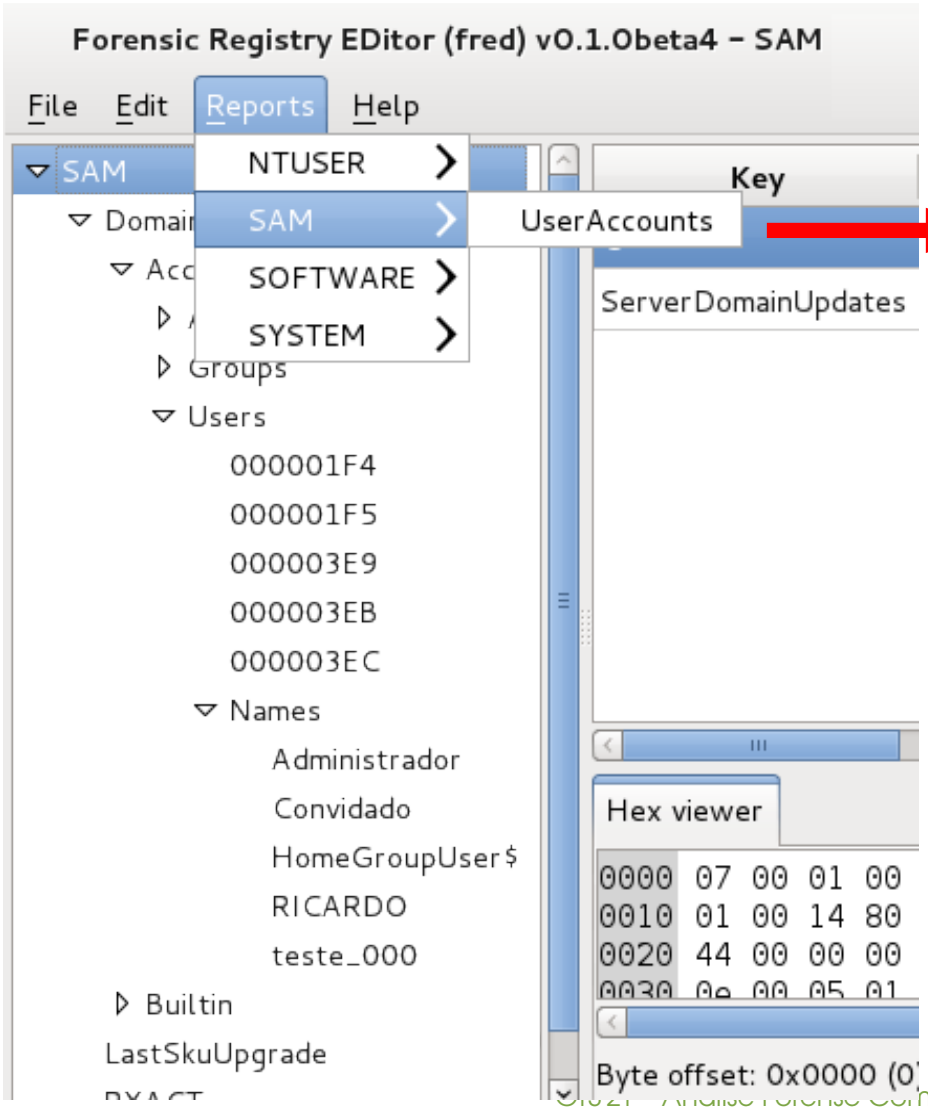
- O que usar?
  - FRED (Forensic Registry EDitor) / FRED Reports
    - Ferramenta gráfica que permite navegar em cada hive
    - Exibe relatórios (reports) padrões para alguns itens
  - Chntpw
    - Ferramenta modo texto que pernite navegar em cada hive
    - Comandos interativos (disponibiliza “help”)
  - RegRipper (Registry Ripper)
    - Ferramenta modo texto que extrai (rip) informações de cada hive
    - Resultado de cada extração é gerado em um arquivo texto
    - Plugins definidos para os principais registros/hives

# Análise do Registro :: Exemplo de Uso do FRED




```
Windows version info

Windows version: Windows 8 Enterterprise Evaluation build 9200
Build string:    9200.win8_rtm.120725-1247
Extended build string:    9200.16384.x86fre.win8_rtm.120725-1247
Install date:    2013/05/20 16:48:44
Registered owner:    scardusklebs@gmail.com
Registered organization:
Product ID:  00178-40000-00001-AA094
Product Key: RR3DQ-7QJ9T-QHYYK-C6XTW-HMFDM
Install path:    C:\Windows
Source path: n/a
```

# Análise do Registro :: Exemplo de Uso do FRED

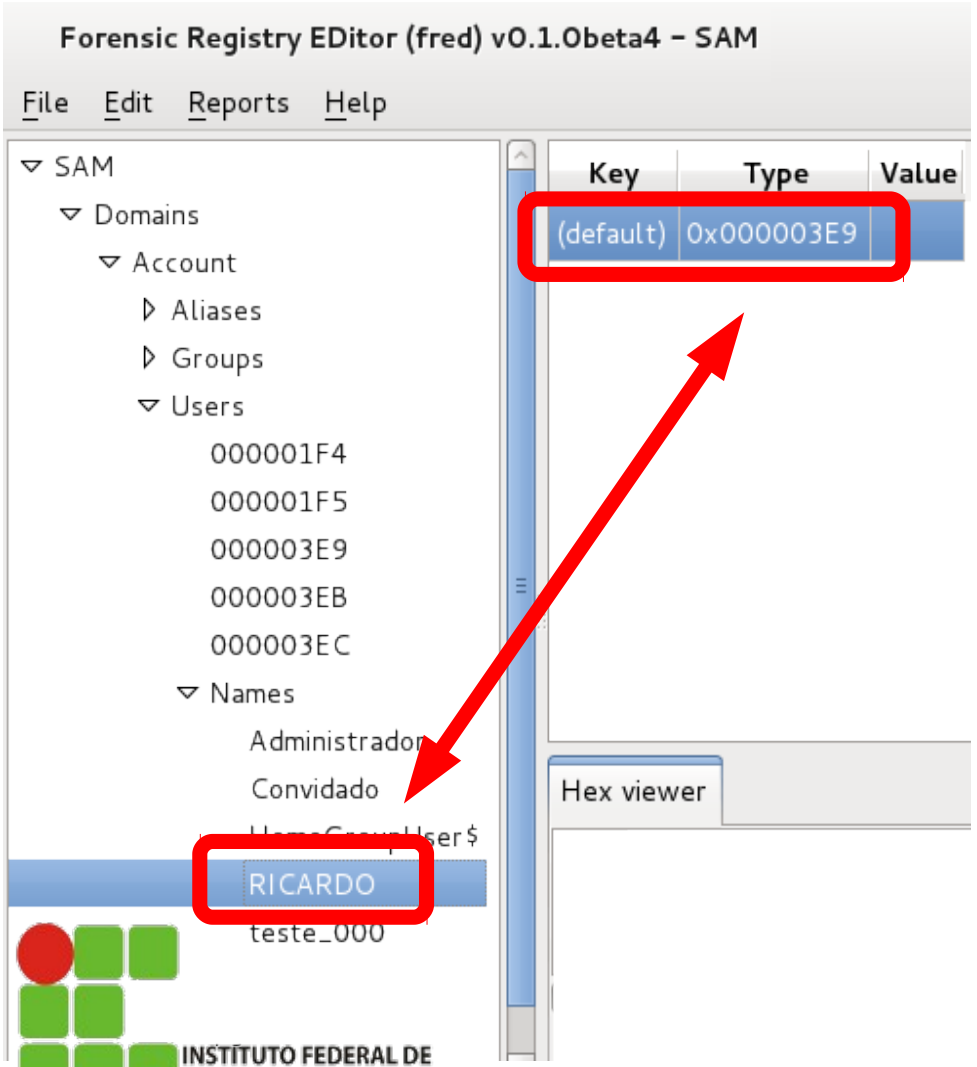


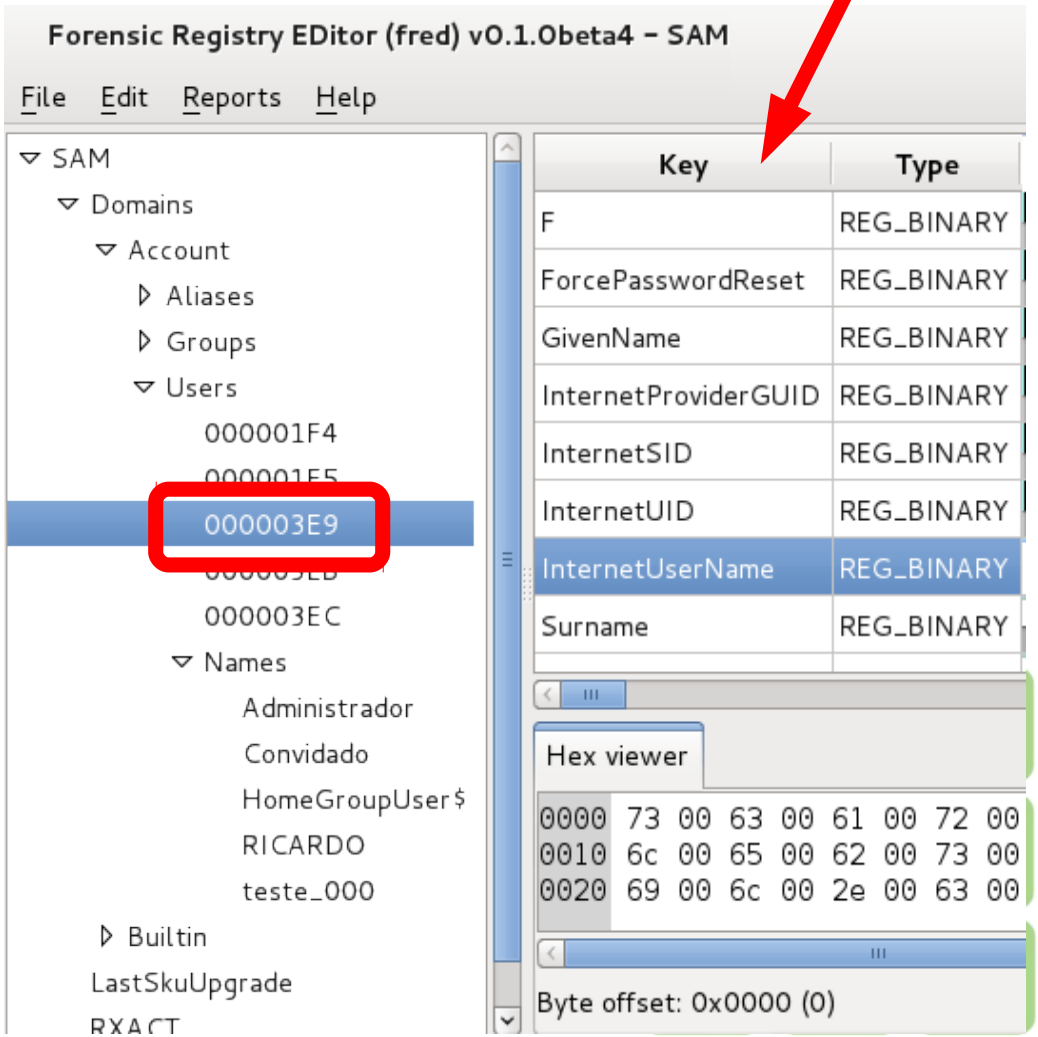

```
User accounts

Administrador
RID: 500 (0x000001F4)
Comment: Conta interna para a administração do
computador/domínio
Last login time: 2012/07/26 06:05:02
Last pw change: 2012/07/26 06:08:18
Last failed login: n/a
Account expires: n/a
Total logins: 1
Failed logins: 0
Account flags: Disabled NoPwExpiry (529)

(...)

RICARDO
RID: 1001 (0x000003E9)
Full name: RICARDO GALVAO
Last login time: n/a
Last pw change: 2013/05/20 17:34:27
Last failed login: n/a
Account expires: 1975/01/22 22:55:33
Total logins: 0
Failed logins: 0
Account flags: NoPwExpiry (528)
```

# Análise Forense do Windows 8

## Análise de Arquivo com Imagem do Disco

## Análise do Registro :: Exemplo de Uso do FRED



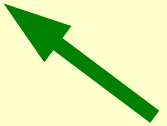

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

## Análise do Registro :: Exemplo de Uso do chntpw

```
# chntpw -l SAM
chntpw version 0.99.6 080526 (sixtyfour), (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
(...)
| RID -|---------- Username --------- tpw -| Admin? |- Lock? --|
| 01f4 | Administrador                    | ADMIN  | dis/lock |
| 01f5 | Convidado                        |        | dis/lock |
| 03eb | HomeGroupUser$                   |        |          |
| 03e9 | RICARDO                          | ADMIN  |          |
| 03ec | teste_000                        |        |          |
```

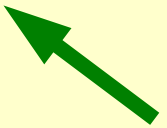
## Análise do Registro :: Exemplo de Uso do chntpw

```
# chntpw -e SAM
> cd SAM\Domains\Account\Users\000003E9
\SAM\Domains\Account\Users\000003E9> cat InternetUserName
Value <InternetUserName> of type REG_BINARY, data length 44 [0x2c]
:00000  73 00 63 00 61 00 72 00 64 00 75 00 73 00 6B 00 s.c.a.r.d.u.s.k.
:00010  6C 00 65 00 62 00 73 00 40 00 67 00 6D 00 61 00 l.e.b.s.@.g.m.a.
:00020  69 00 6C 00 2E 00 63 00 6F 00 6D 00            i.l...c.o.m.
```

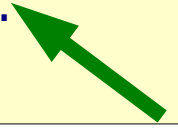


chntpw

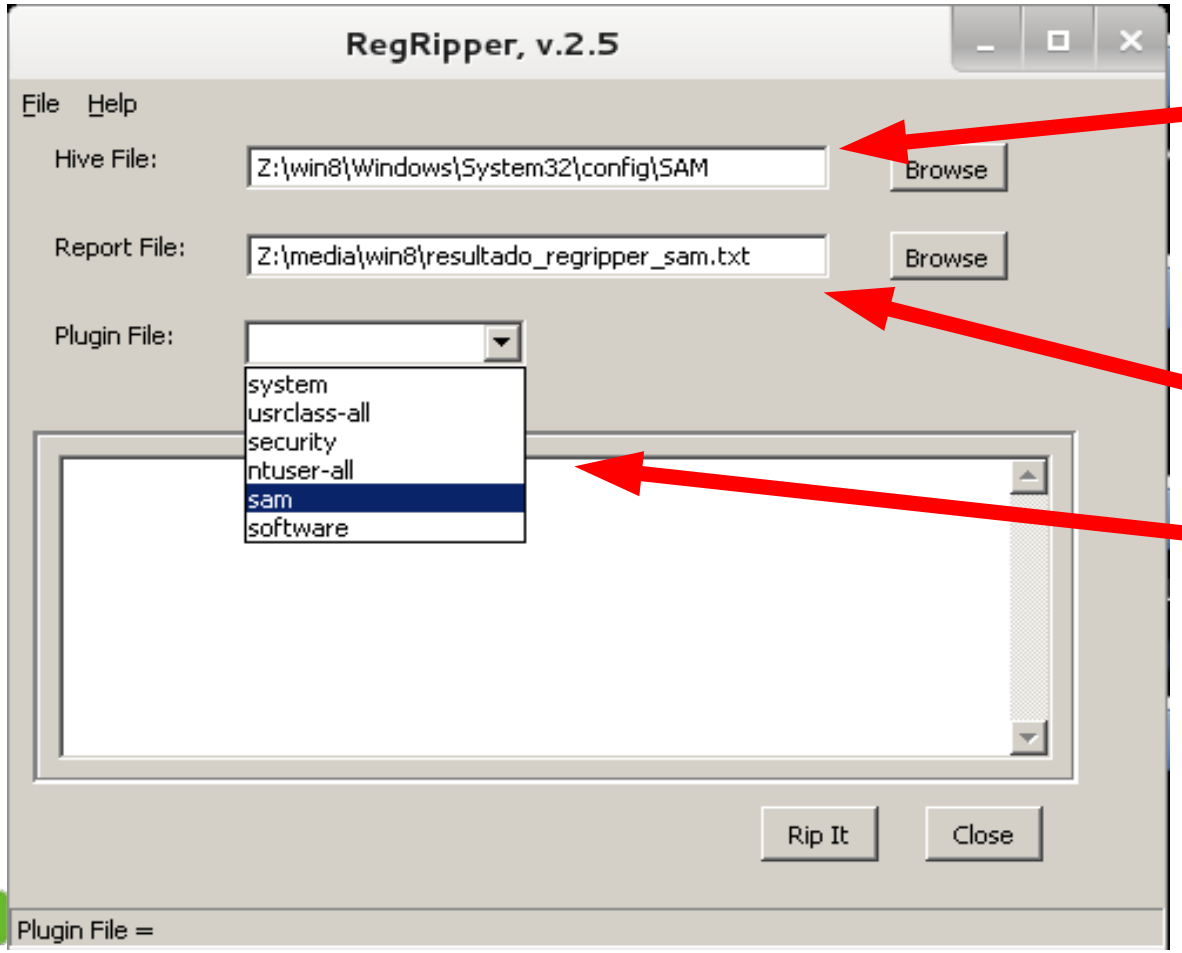
```
\SAM\Domains\Account\Users\000003E9> cat GivenName
Value <GivenName> of type REG_BINARY, data length 14 [0xe]
:00000  52 00 49 00 43 00 41 00 52 00 44 00 4F 00       R.I.C.A.R.D.O.
```



```
\SAM\Domains\Account\Users\000003E9> cat Surname
Value <Surname> of type REG_BINARY, data length 12 [0xc]
:00000  47 00 41 00 4C 00 56 00 41 00 4F 00             G.A.L.V.A.O.
```



# Análise do Registro :: Exemplo de Uso do RegRipper




Seleciona Arquivo HIVE

Arquivo onde será gerado (RIP) o relatório

Plugin Utilizado

## Análise do Registro :: Exemplo de Uso do RegRipper

```
# cat resultado_sam.txt

(...)
(NTUSER.DAT) Returns contents of user's TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Mon May 20 17:41:58 2013 (UTC)
  url1 -> http://www.google.com.br/
  url2 -> http://images.google.com/
  url3 -> http://www.terra.com.br/
  url4 -> http://gts.nic.br/
  url5 -> http://www.ifrn.edu.br/
(...)
```

## Análise do Registro :: Exemplo de Uso do RegRipper

```
# cat resultado_sam.txt

(...)
(NTUSER.DAT) Returns contents of user's TypedURLsTime key.

TypedURLsTime
Software\Microsoft\Internet Explorer\TypedURLsTime
LastWrite Time Mon May 20 17:41:58 2013 (UTC)
  url1 -> Mon May 20 17:36:37 2013 Z (http://www.google.com.br/)
  url2 -> Mon May 20 17:15:09 2013 Z (http://images.google.com/)
  url3 -> Mon May 20 17:14:07 2013 Z (http://www.terra.com.br/)
  url4 -> Mon May 20 17:13:35 2013 Z (http://gts.nic.br/)
  url5 -> Mon May 20 17:13:05 2013 Z (http://www.ifrn.edu.br/)
(...)
```

## Manipulando/Analisando Informações do Registro

- Conclusões
  - FRED (Forensic Registry EDitor) / FRED Reports
    - Visualizar informações relevantes dos hives (novas e préexistentes)
    - Visualização parcial dos Valores (Value Name) das chaves (Keys)
  - Chntpw
    - Visualiza todas as informações (novas e preexistentes) inclusive Value Names
    - É uma ferramenta "modo-texto" (!!??)
  - RegRipper (Registry Ripper)
    - Facilita análise pós-extração
    - Necessita de plugins para extração
    - Não estão disponiveis (ainda) plugins dos novos hives

## Senhas de Usuários por Força Bruta

(Nenhuma Alteração nesta nova versão)

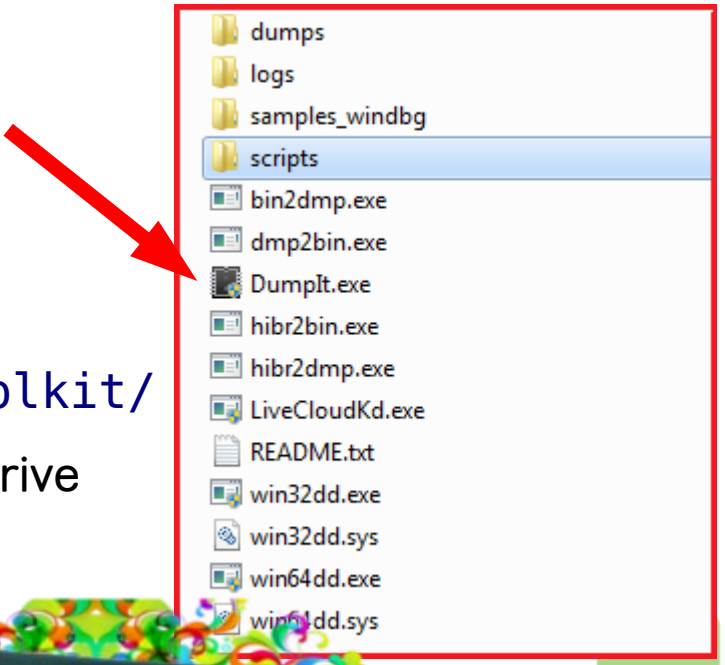

- Ferramentas bkhive, samdump2 e John The Ripper (john)
  - Pré-instaladas no sistema Kali Linux

```
# mkdir /media/win8
# mount /imagens/win8_part02.dd /media/win8 -o ro,loop
# bkhive /media/win8/Windows/System32/config/SYSTEM syskey.txt
# samdump2 /media/win8/Windows/System32/config/SAM syskey.txt > hashes.txt
# john hashes.txt
```

# Dump da Memória do Sistema:

## - Ferramenta Utilizada:

- MoonSols Windows Memory Toolkit
- Freeware (Community Version)
- 500 Euros (Professional Version)
- http://www.moonsols.com/windows-memory-toolkit/
  - Executável baixado e executado direto de um pendrive
  - Dump gerado direto no pendrive
    - E:\DumpIt.exe
      → rkwin8-20130420-175441.raw




# Analisando o Arquivo de dump da Memória do Sistema:


https://code.google.com/p/volatility

- GNU / GPL v2
- Python
- Suporte a vários SO's

---

## - Utilizando a versão disponível (Kali Linux) do Volatility

```
# vol imageinfo -f rkwin8-20130520-175441.raw
    Volatile Systems Volatility Framework 2.1
    Determining profile based on KDBG search...
    Suggested Profile(s) : No suggestion (Instantiated with no profile)
```

## Suporte do Volatility para Windows8:

- Versão 3.0 (em desenvolvimento)
  - Addition of Windows 8 / Server 2012 Support/Testing

Novos Profiles para Windows 8 = `Win8SP0x86 | Win8SP0x64`

- Tutorial da nova versão:

`https://volatility.googlecode.com/svn/branches/scudette/docs/index.html`

- Versão Atual (desenvolvimento) [24/02/2013] Preview Release 0.2:

`https://volatility.googlecode.com/files/volatility-tp2.zip`

- Instalação via SVN:

```
svn checkout http://volatility.googlecode.com/svn/branches/scudette/ volatility
```

```
# ./vol.py --help
The Volatility Memory Forensic Framework technology preview (3.0_tp2)
```

# Exemplo de Utilização/Resultados:

## Plugin: pslist

```
# ./vol.py -f rkwin8-20130420-175441.raw --profile=Win8SP0x86 pslist
The Volatility Memory Forensic Framework technology preview (3.0_tp2)
 Offset(V)  Name                    PID    PPID   Thds   Hnds   Time
---------- -------------------- ------ ------ ------ ------ ----------------
0x8274aa00 System                    4      0     80 ------ 2013-04-20 17:52:31
0x83967040 smss.exe                232      4      2 ------ 2013-04-20 17:52:31
0x836916c0 cmd.exe                1508   3488      8 ------ 2013-04-20 17:54:24
0x83704d00 DumpIt.exe             3840   1508      2 ------ 2013-04-20 18:15:43
```

## Exemplo de Utilização/Resultados:

### Plugin: userassist

```
# ./vol.py -f rkwin8-20130420-175441.raw --profile=Win8SP0x86 userassist
The Volatility Memory Forensic Framework technology preview (3.0_tp2)
REG_BINARY    %windir%\system32\cmd.exe :
Time Focused:   0:07:34.501000
Last updated:   2013-04-20 17:54:24
0x00000000  00 00 00 00 02 00 00 00 05 00 00 00 71 ed 06 00   ............q...
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 50 0f 69 94   ............P.i.
0x00000040  c0 73 cc 01 00 00 00 00                           .s......
```

# Exemplo de Utilização/Resultados:

## Plugin: userassist

```
# ./vol.py -f rkwin8-20130420-175441.raw --profile=Win8SP0x86 userassist
The Volatility Memory Forensic Framework technology preview (3.0_tp2)
REG_BINARY    E:\DumpIt\DumpIt.exe :
Time Focused:   0:01:27.500000
Last updated:   2013-04-20 18:15:43
0x00000000  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00   ................
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 00 00 00 00   ................
0x00000040  00 00 00 00 00 00 00 00                           ........
```

## Plugins Disponíveis (versão 3.0_tp2):

- kdbgscan
- pslist
- pstree
- psscan
- dlllist
- dlldump
- pedump
- handles
- getsids
- cmdscan
- consoles
- procinfo
- memmap
- procexedump
- vadinfo
- vadwalk
- vadtree
- vaddump
- evtlogs
- modules
- modscan
- moddump
- driverscan
- filescan
- mutantscan
- symlinkscan
- thrdscan
- connections
- connscan
- sockets
- sockscan
- netscan
- hivescan
- hivelist
- printkey
- hivedump
- hashdump
- lsadump
- userassist
- shimcache
- getservicesids
- crashinfo
- hibinfo
- imagecopy
- raw2dmp
- malfind
- yarascan
- svcscan
- ldrmodules
- impscan
- apihooks
- idt
- gdt
- threads
- callbacks
- driverirp
- devicetree
- psxview
- timers

## Última Dica sobre o Volatility:

### - Versão 3.0 (em desenvolvimento)

- Traz, adicionalmente, ferramenta de Dump de Memória:

**WinPMEM**

- `/usr/share/volatility-3.0-tp2/tools/windows/winpmem`
- Versão 1.1
- Copyright 2012 Michael Cohen <scudette@gmail.com>
- Licença: Apache 2.0

# Análise Forense do Windows 8

## Conclusões / Resumo / Finalmentes...

### O que interessa na análise forense em sistemas Windows?

- Dados de usuários e do sistema disponíveis...
  - No disco (sistema de arquivos) / na memória / no registro

### O que há de novidades relevantes no Windows 8?

- Aumento do registro das atividades dos usuários
- Mudanças na localização de arquivos de registro pré-existentes
- Conceito de App (Metro Interface) → mais dados relevantes

### Ferramentas para versões anteriores estão adequadas/atualizadas?

- Parcialmente
  - As que fazem uso de plugins e templates estão em fase de atualização
  - A coleta de todas as informações disponíveis necessárias já é possível (com um pouco de esforço)

Esta apresentação não levou em consideração soluções/ferramentas comerciais e/ou baseadas no sistema operacional Microsoft Windows

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

# Perguntas

## Referências / Agradecimentos:


- Amanda C. F. Thomson (The George Washington University) :: Windows 8 Forensic Guide
- Josh Brunty (Marshal University) :: Windows 8: A Forensic First Look
- Forensic Insight Seminar (F-Insight) :: Windows 8 Forensics
- Khawla Alghafli (Khalifa University) :: Forensic Analysis of the Windows 7 Registry
- Karl Sigler (Skeleton Security) :: Memory Analysis with Volatility
- Offensive Security :: Kali Kinux
- Gillen Dan (Pinguin's HQ) :: Forensic Registry EDitor (FRED)
- Petter Nordahl :: Chntpw
- Harlan Carvey :: RegRipper
- IFRN – Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
- NIC/BR / GTS

GTER
GTS .br

ETHICAL HACKER ACADEMY

# Análise Forense Computacional no Sistema Operacional

Windows® 8™


Ricardo Kléber Martins Galvão
www.ricardokleber.com
ricardokleber@ricardokleber.com
@ricardokleber


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