GTER 40 | GTS 26

Osmany Dantas R. de Arruda

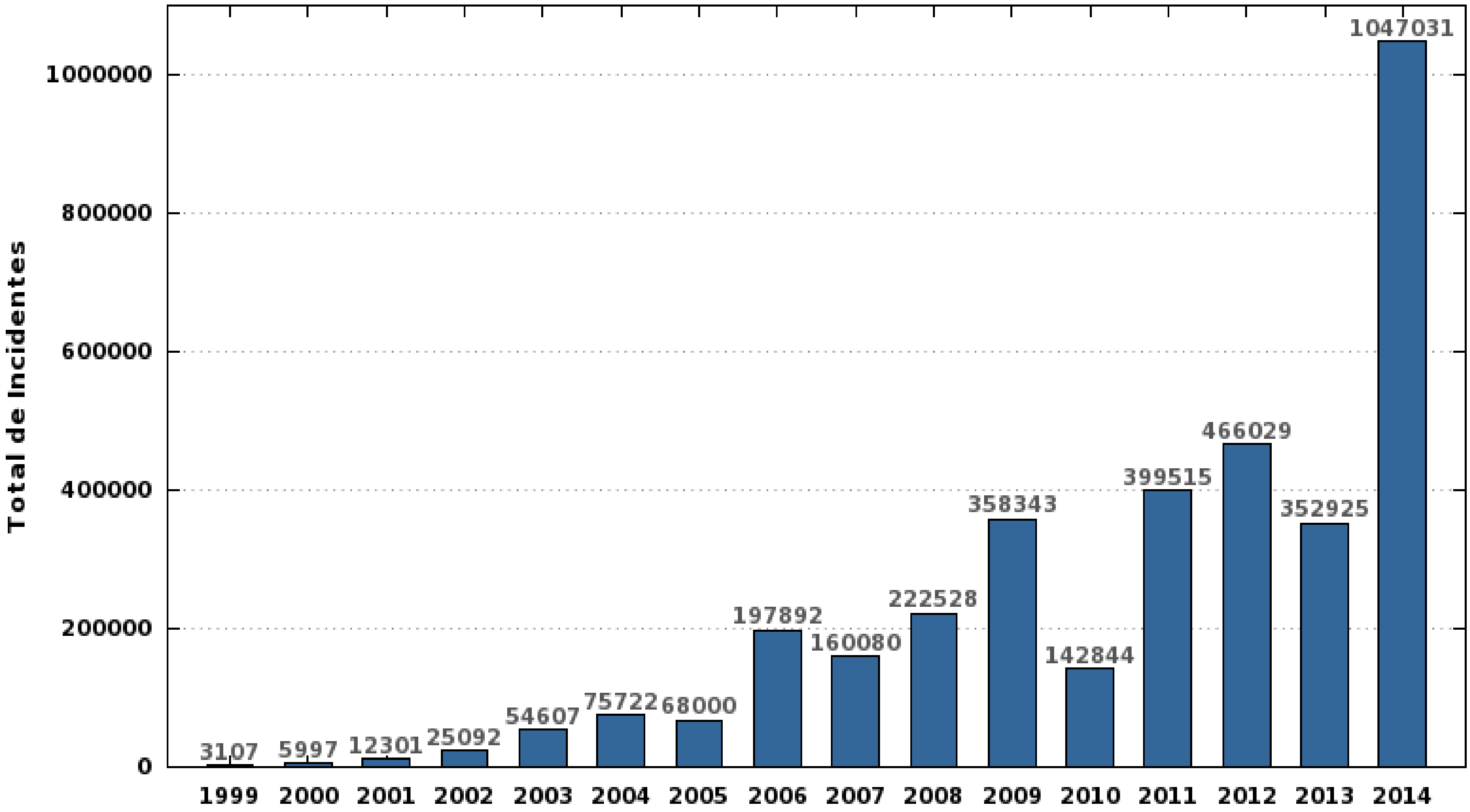
Análise Forense do Conteúdo da Memória Volátil

agenda

- Contextualização
- Relevância
- Motivação
- Objetivo da palestra
- Considerações sobre o processo e ferramentas
- Considerações finais

Contextualização

Incidentes reportados ao CERT.br - Acumulado - 1999 a 2014



Ref.: http://www.cert.br/stats/incidentes/

Relevância

Investigação dos incidentes de segurança da informação

- Continuidade de negócio
- Segurança de informação
- Mitigação de riscos
- Preservação da imagem corporativa

Motivação

Investigação forense da RAM

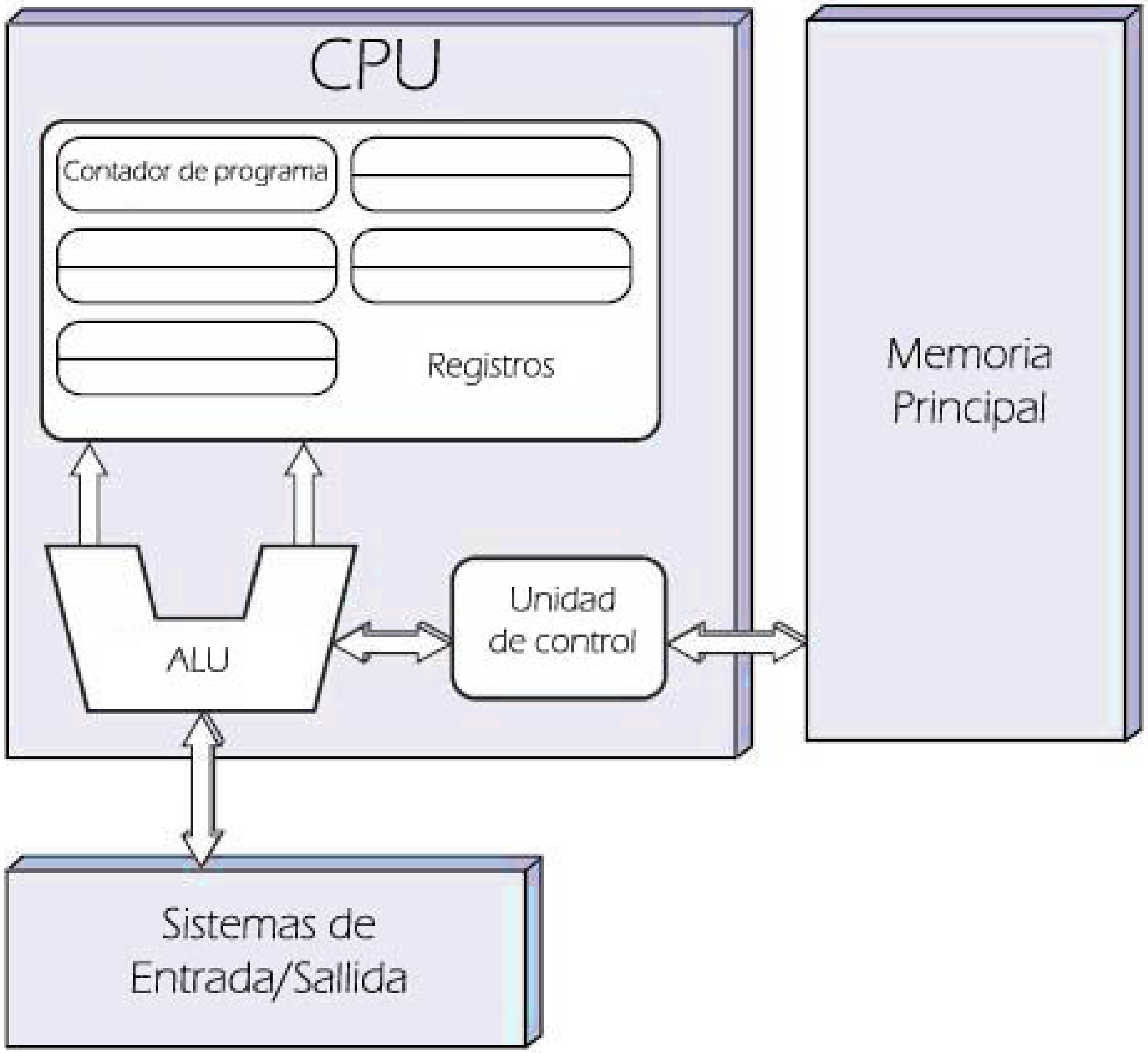
Necessidade de:

- **Preservação da segurança da informação**
- **Investigação de incidentes de segurança**
- **Análise de códigos maliciosos (malwares)**

Objetivo da palestra

Discutir alguns dos principais fundamentos da perícia forense do conteúdo da memória volátil, independentemente de ferramentas.

O modelo de Von Neumann



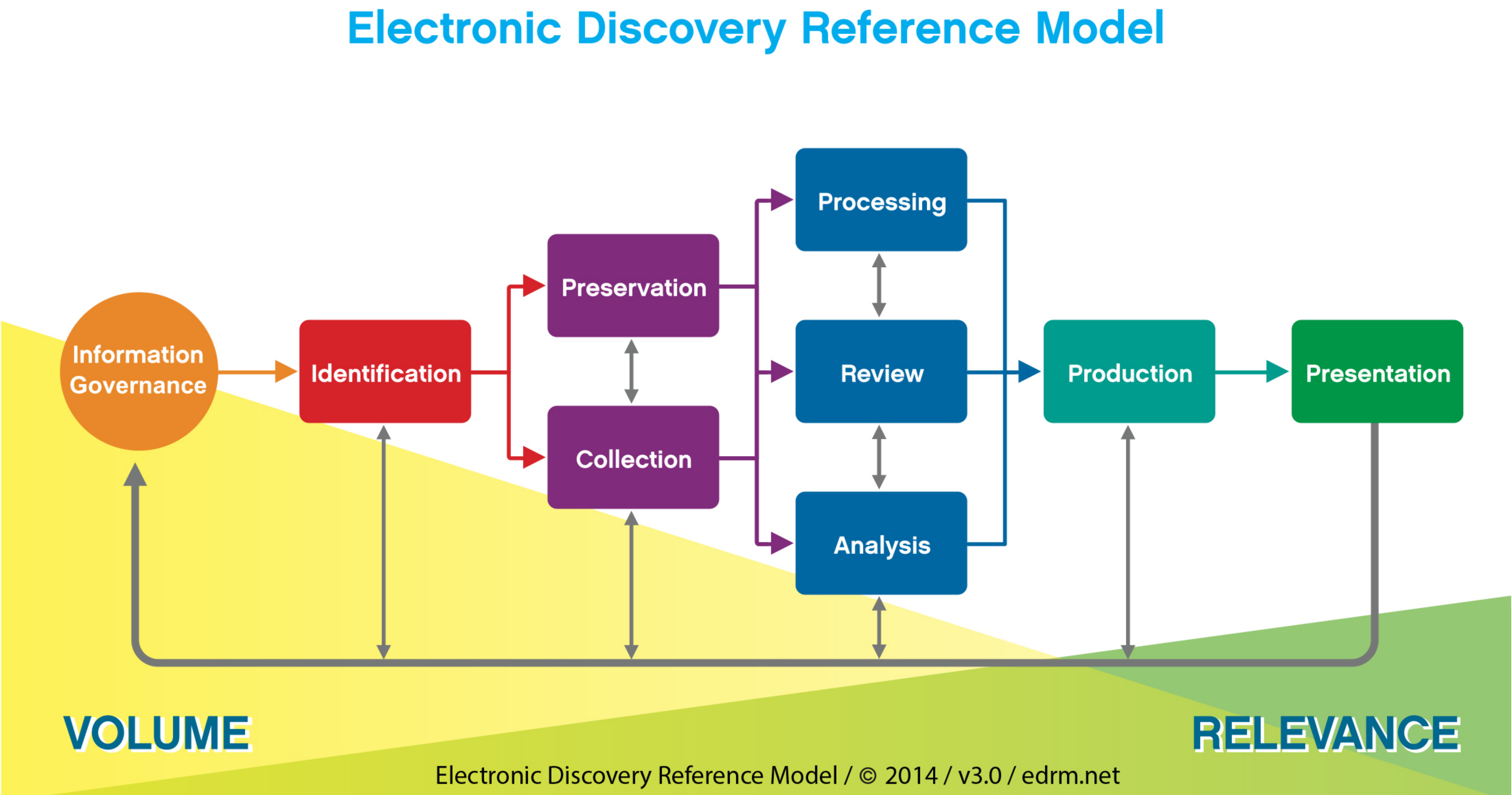
Disponível em https://commons.wikimedia.org/wiki/File:Arquitecturaneumann.jpg#/media/File:Arquitecturaneumann.jpg

O que pode ser encontrado?

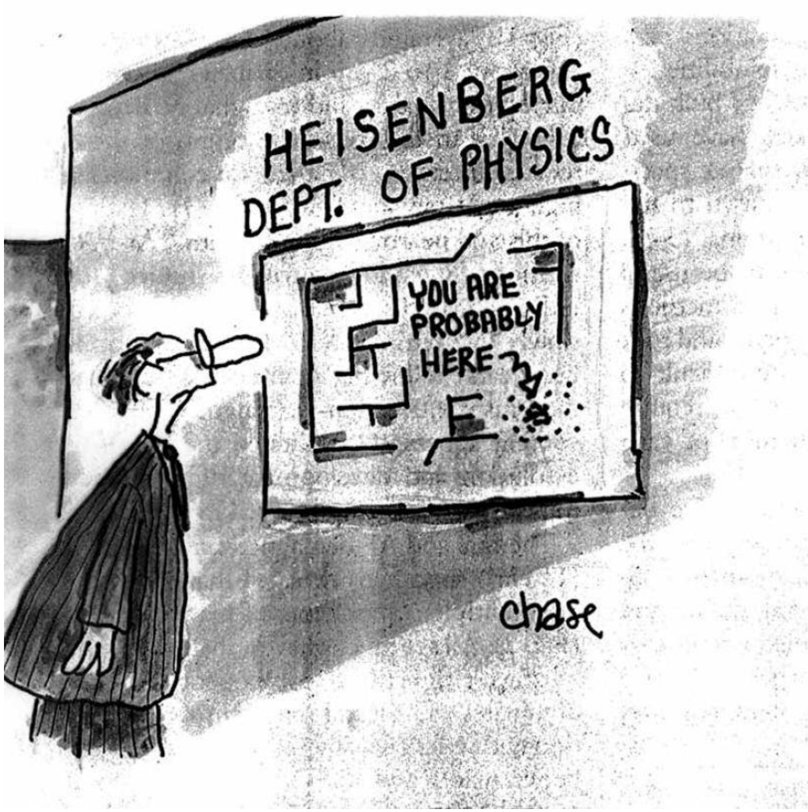
Elementos com valor probatório:

- **Timestamps**
- **Processos e usuários**
- **Sockets e conexões de rede**
- **Hashes de senhas**
- **Chaves criptográficas**
- **Módulos do kernel**
- **...**

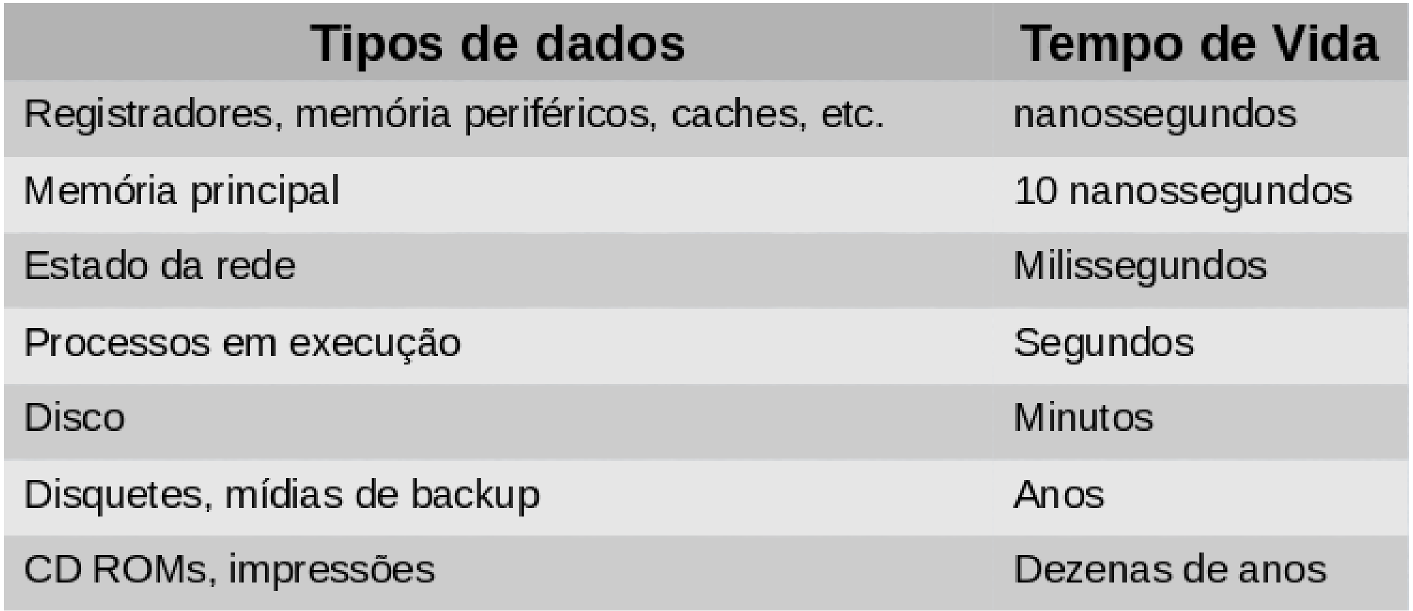
e-Discovery


Electronic Discovery Reference Model
Information Governance
Identification
Preservation
Collection
Processing
Review
Analysis
Production
Presentation
VOLUME
RELEVANCE
Electronic Discovery Reference Model / © 2014 / v3.0 / edrm.net

O Princípio da Incerteza de Heisenberg



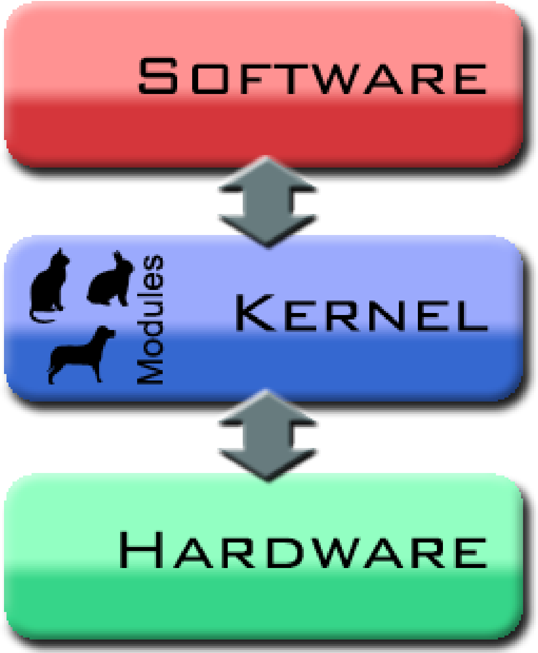
A ordem de volatilidade

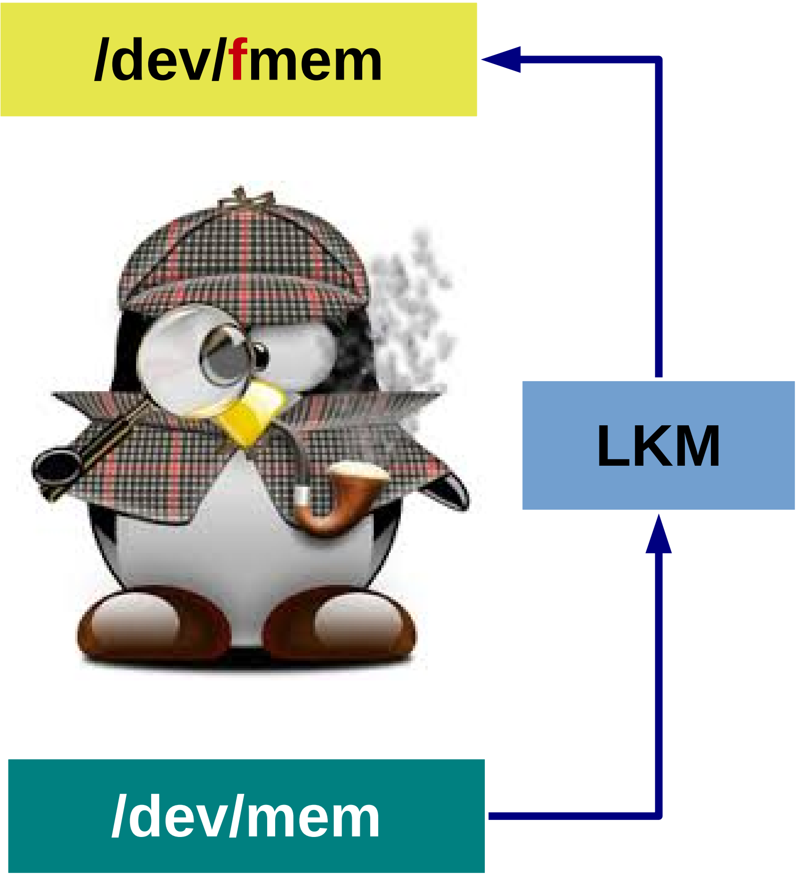


Tipos de dados	Tempo de Vida
Registradores, memória periféricos, caches, etc.	nanossegundos
Memória principal	10 nanossegundos
Estado da rede	Milissegundos
Processos em execução	Segundos
Disco	Minutos
Disquetes, mídias de backup	Anos
CD ROMs, impressões	Dezenas de anos

Ref.: Farmer,D. ; Venema,W. “Perícia Forense Computacional – Teoria e Prática” , 2007

Acessando a memória





/dev/fmem

LKM

/dev/mem

Dump da memória

Ferramentas mais populares

fmem (http://hysteria.sk/~niekt0/foriana/fmem_current.tgz)

- fmem é um LKM(Linux Kernel Module) para acessar /dev/fmem sem limitações.
- Permite acesso direto a memória física de forma semelhante ao /dev/mem.
- A memória física poderá ser copiada através de ferramentas como o dd.

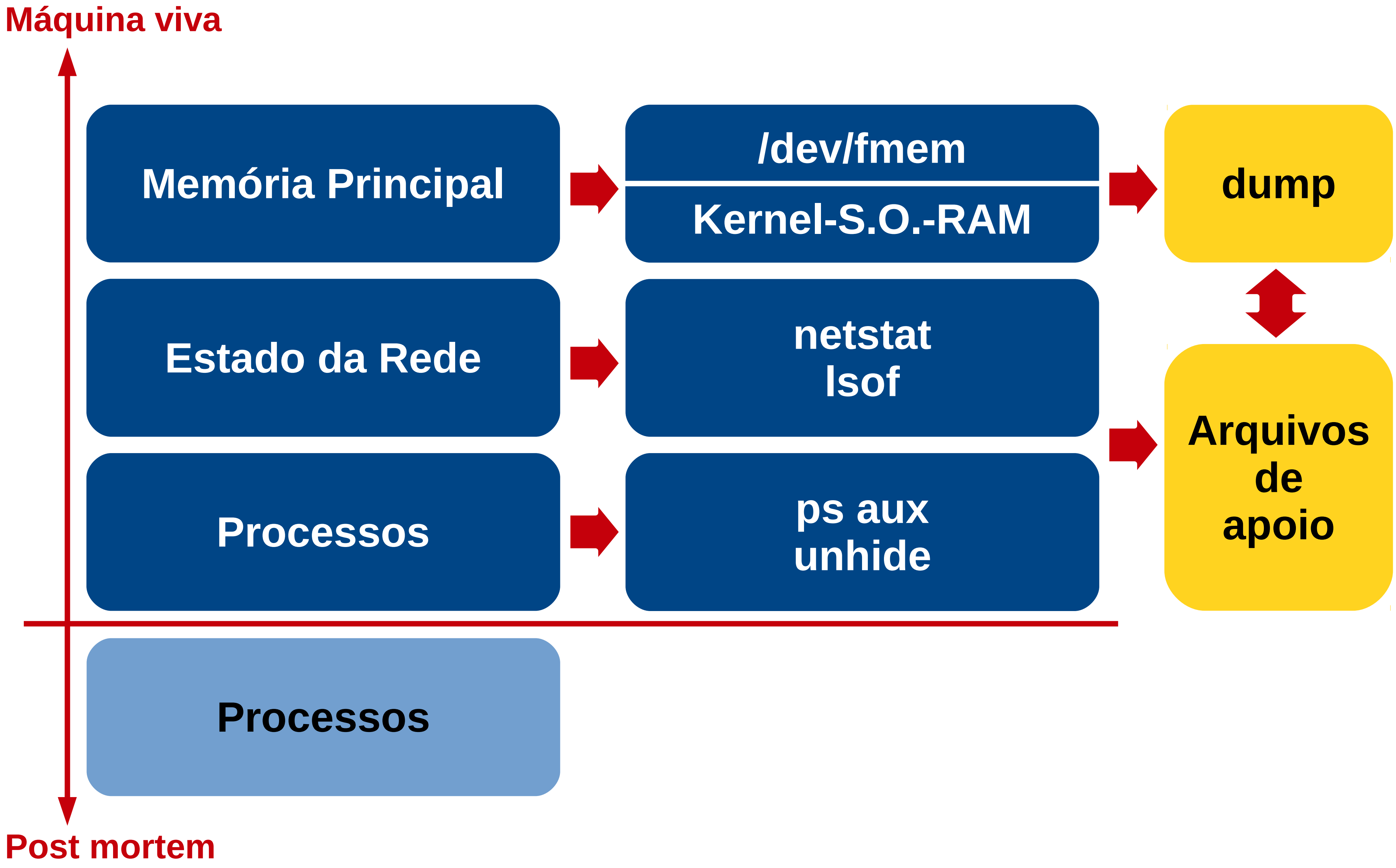
LiME (http://code.google.com/p/lime-forensics/)

- LiME é um LKM(Linux Kernel Module) para aquisição do conteúdo da memória volátil.
- Tem suporte ao Android e ao dump via rede

Second Look®: The Linux Memory Forensic Acquisition (http://secondlookforensics.com/)

- Solução comercial para dump da memória em sistemas Linux
- Utiliza CLI ou GUI
- Identificação automática da versão do kernel

Planejamento (Ordem de Volatilidade)


Máquina viva

Memória Principal → /dev/fmem | Kernel-S.O.-RAM → dump

Estado da Rede → netstat lsof

Processos → ps aux unhide → Arquivos de apoio

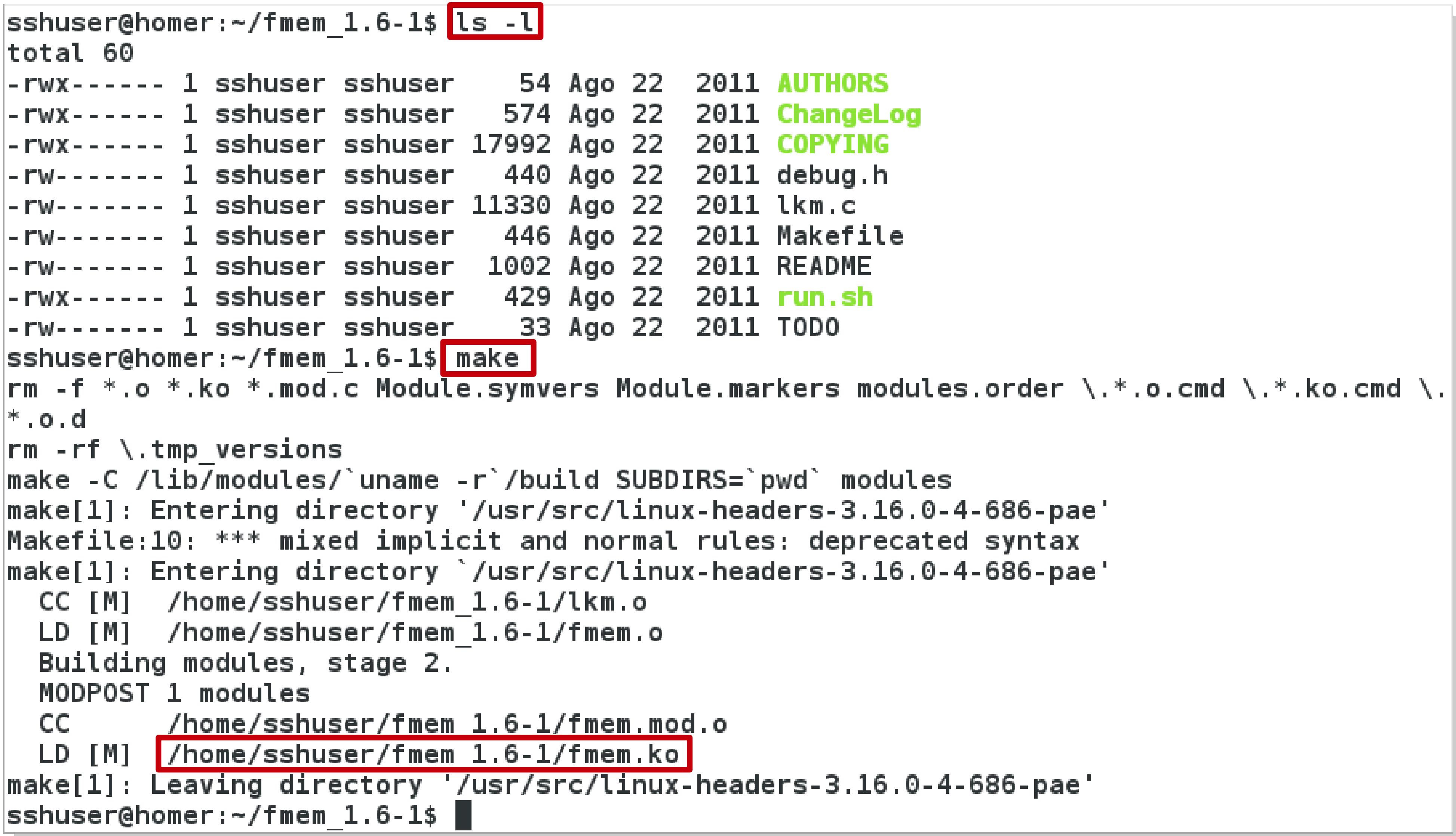
dump ↕ Arquivos de apoio

Processos

Post mortem

LKM (fmem)

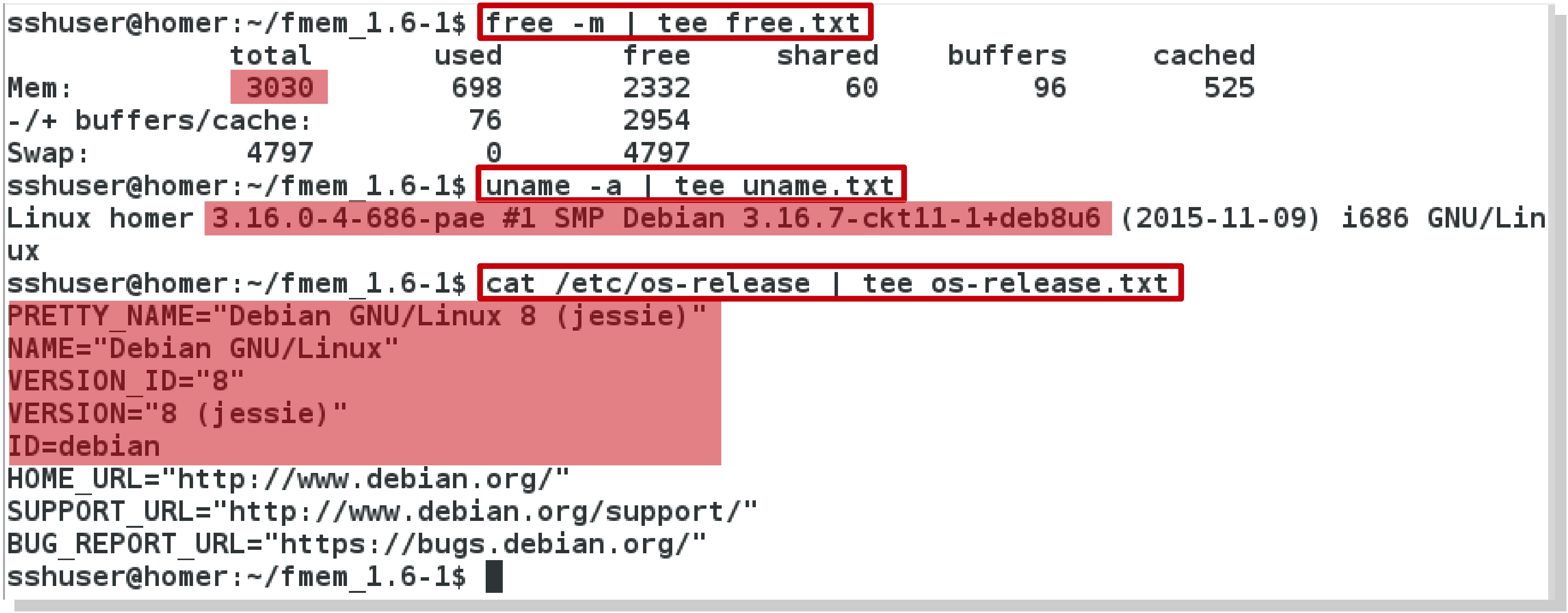
Coleta de dados para compilação do módulo



```
sshuser@homer:~/fmem_1.6-1$ ls -l
total 60
-rwx------ 1 sshuser sshuser    54 Ago 22  2011 AUTHORS
-rwx------ 1 sshuser sshuser   574 Ago 22  2011 ChangeLog
-rwx------ 1 sshuser sshuser 17992 Ago 22  2011 COPYING
-rw------- 1 sshuser sshuser   440 Ago 22  2011 debug.h
-rw------- 1 sshuser sshuser 11330 Ago 22  2011 lkm.c
-rw------- 1 sshuser sshuser   446 Ago 22  2011 Makefile
-rw------- 1 sshuser sshuser  1002 Ago 22  2011 README
-rwx------ 1 sshuser sshuser   429 Ago 22  2011 run.sh
-rw------- 1 sshuser sshuser    33 Ago 22  2011 TODO
sshuser@homer:~/fmem_1.6-1$ make
rm -f *.o *.ko *.mod.c Module.symvers Module.markers modules.order \.*.o.cmd \.*.ko.cmd \.
*.o.d
rm -rf \.tmp_versions
make -C /lib/modules/`uname -r`/build SUBDIRS=`pwd` modules
make[1]: Entering directory '/usr/src/linux-headers-3.16.0-4-686-pae'
Makefile:10: *** mixed implicit and normal rules: deprecated syntax
make[1]: Entering directory `/usr/src/linux-headers-3.16.0-4-686-pae'
  CC [M]  /home/sshuser/fmem_1.6-1/lkm.o
  LD [M]  /home/sshuser/fmem_1.6-1/fmem.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/sshuser/fmem_1.6-1/fmem.mod.o
  LD [M]  /home/sshuser/fmem_1.6-1/fmem.ko
make[1]: Leaving directory '/usr/src/linux-headers-3.16.0-4-686-pae'
sshuser@homer:~/fmem_1.6-1$ █
```

LKM (fmem)

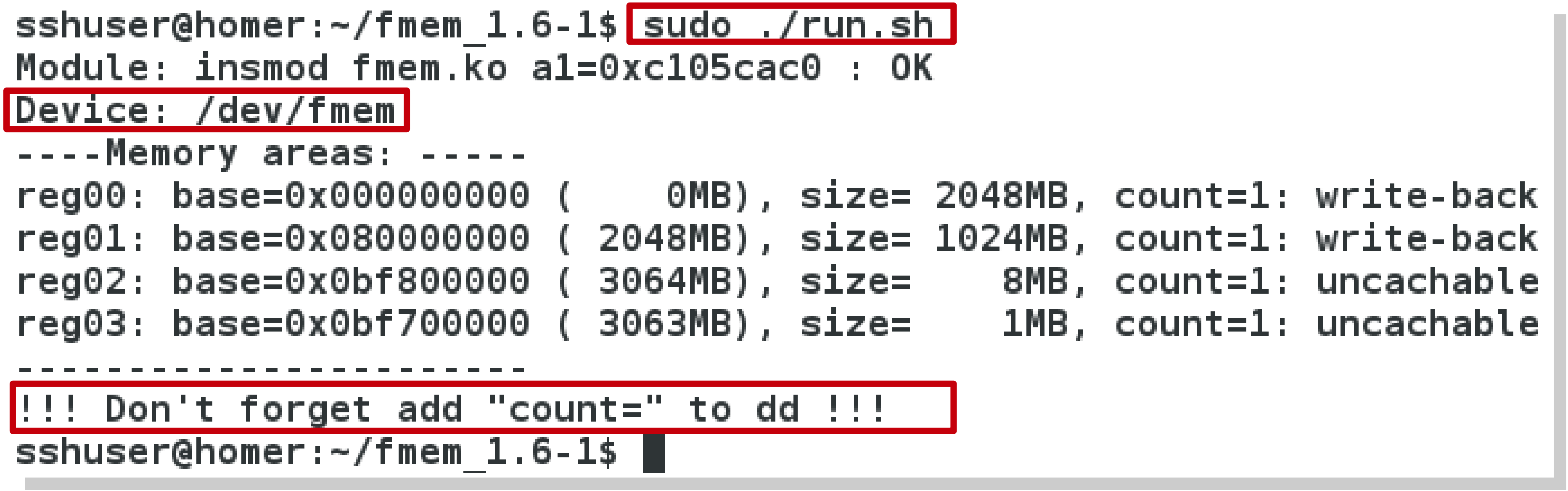
Coleta de dados para carga do módulo



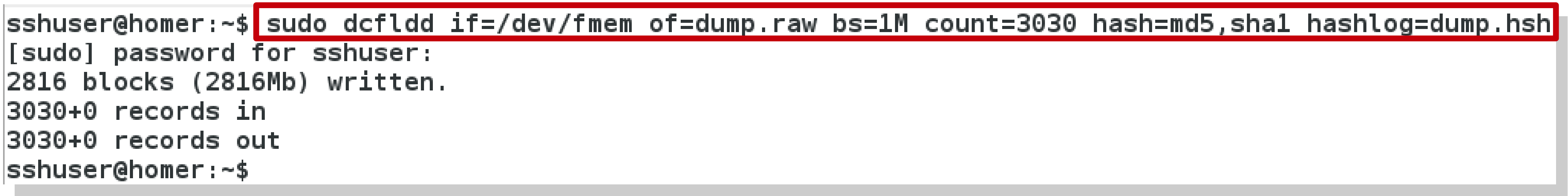
```
sshuser@homer:~/fmem_1.6-1$ free -m | tee free.txt
             total       used       free     shared    buffers     cached
Mem:          3030        698       2332         60         96        525
-/+ buffers/cache:         76       2954
Swap:         4797          0       4797
sshuser@homer:~/fmem_1.6-1$ uname -a | tee uname.txt
Linux homer 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt11-1+deb8u6 (2015-11-09) i686 GNU/Lin
ux
sshuser@homer:~/fmem_1.6-1$ cat /etc/os-release | tee os-release.txt
PRETTY_NAME="Debian GNU/Linux 8 (jessie)"
NAME="Debian GNU/Linux"
VERSION_ID="8"
VERSION="8 (jessie)"
ID=debian
HOME_URL="http://www.debian.org/"
SUPPORT_URL="http://www.debian.org/support/"
BUG_REPORT_URL="https://bugs.debian.org/"
sshuser@homer:~/fmem_1.6-1$ 
```

LKM (fmem)

Carga do módulo e dump da RAM



```
sshuser@homer:~/fmem_1.6-1$ sudo ./run.sh
Module: insmod fmem.ko a1=0xc105cac0 : OK
Device: /dev/fmem
----Memory areas: -----
reg00: base=0x000000000 (    0MB), size= 2048MB, count=1: write-back
reg01: base=0x080000000 ( 2048MB), size= 1024MB, count=1: write-back
reg02: base=0x0bf800000 ( 3064MB), size=    8MB, count=1: uncachable
reg03: base=0x0bf700000 ( 3063MB), size=    1MB, count=1: uncachable
-----------------------
!!! Don't forget add "count=" to dd !!!
sshuser@homer:~/fmem_1.6-1$
```

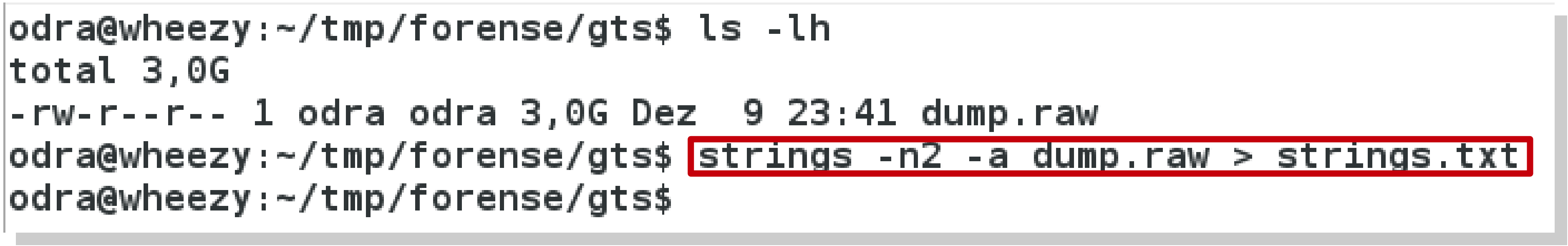


```
sshuser@homer:~$ sudo dcfldd if=/dev/fmem of=dump.raw bs=1M count=3030 hash=md5,sha1 hashlog=dump.hsh
[sudo] password for sshuser:
2816 blocks (2816Mb) written.
3030+0 records in
3030+0 records out
sshuser@homer:~$
```

Extração de dados do dump

Análise do dump

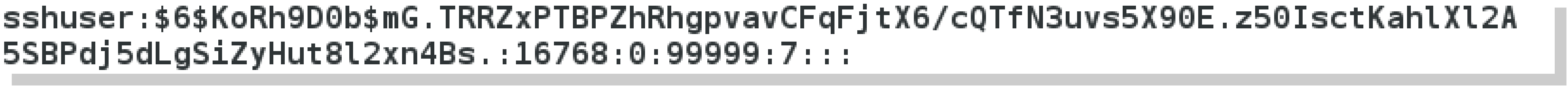
Extração de dados do dump



```
odra@wheezy:~/tmp/forense/gts$ ls -lh
total 3,0G
-rw-r--r-- 1 odra odra 3,0G Dez  9 23:41 dump.raw
odra@wheezy:~/tmp/forense/gts$ strings -n2 -a dump.raw > strings.txt
odra@wheezy:~/tmp/forense/gts$
```

Dados encontrados:

1. Hash das senha do usuário



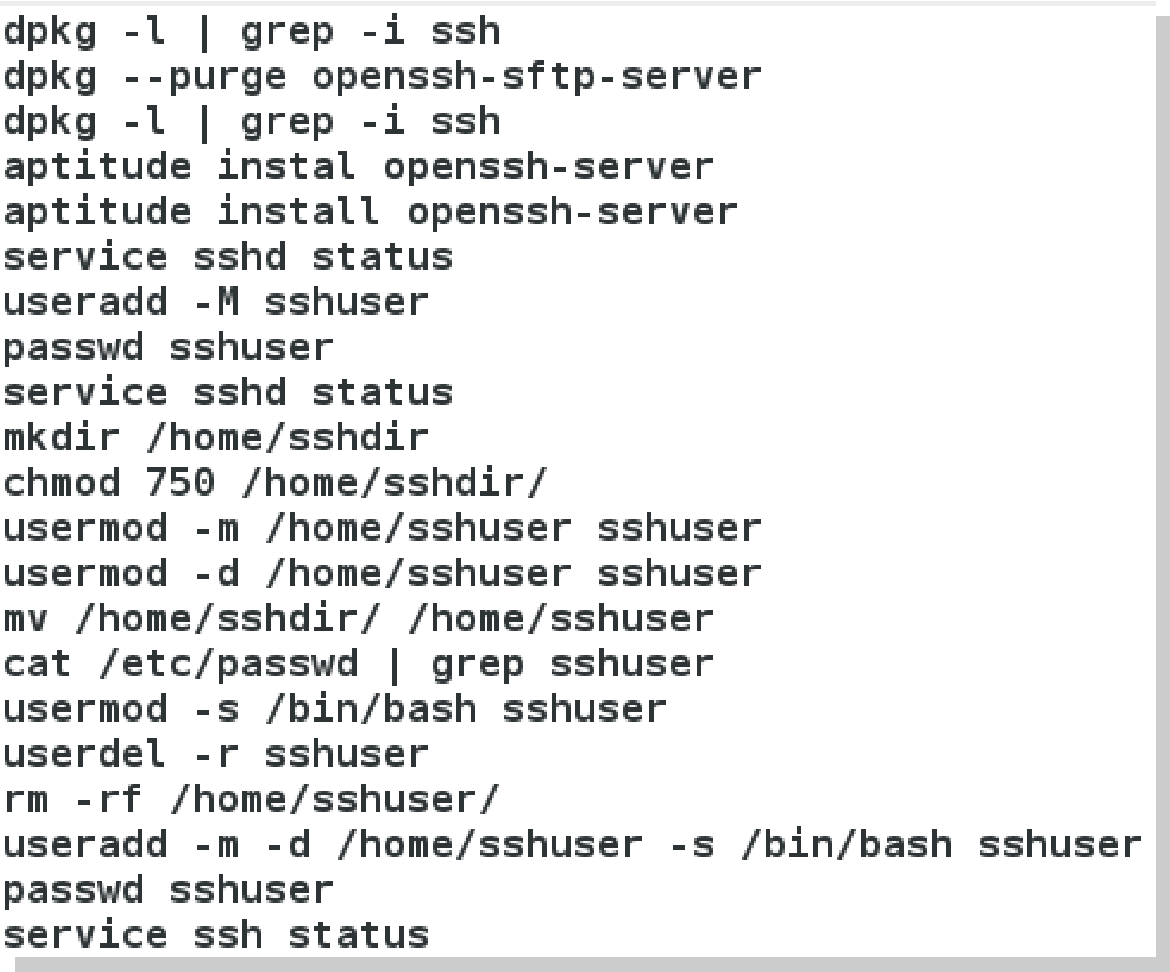
```
sshuser:$6$KoRh9D0b$mG.TRRZxPTBPZhRhgpvavCFqFjtX6/cQTfN3uvs5X90E.z50IsctKahlXl2A
5SBPdj5dLgSiZyHut8l2xn4Bs.:16768:0:99999:7:::
```

Extração de dados do dump

Análise do dump

Dados encontrados:

2. Histórico de comandos



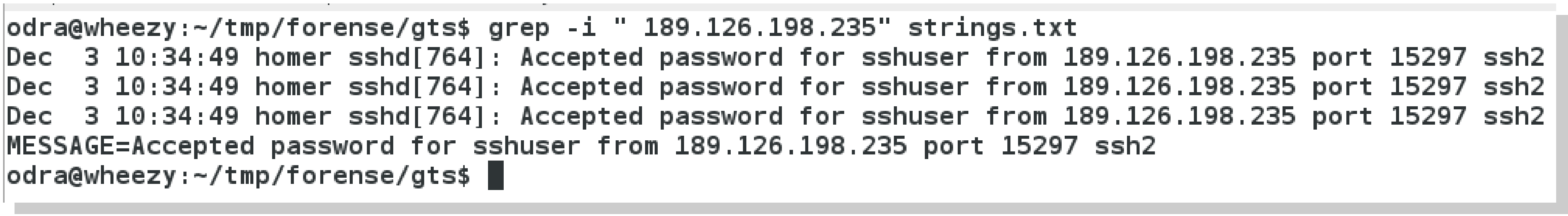
```
dpkg -l | grep -i ssh
dpkg --purge openssh-sftp-server
dpkg -l | grep -i ssh
aptitude instal openssh-server
aptitude install openssh-server
service sshd status
useradd -M sshuser
passwd sshuser
service sshd status
mkdir /home/sshdir
chmod 750 /home/sshdir/
usermod -m /home/sshuser sshuser
usermod -d /home/sshuser sshuser
mv /home/sshdir/ /home/sshuser
cat /etc/passwd | grep sshuser
usermod -s /bin/bash sshuser
userdel -r sshuser
rm -rf /home/sshuser/
useradd -m -d /home/sshuser -s /bin/bash sshuser
passwd sshuser
service ssh status
```

Extração de dados do dump

Análise do dump

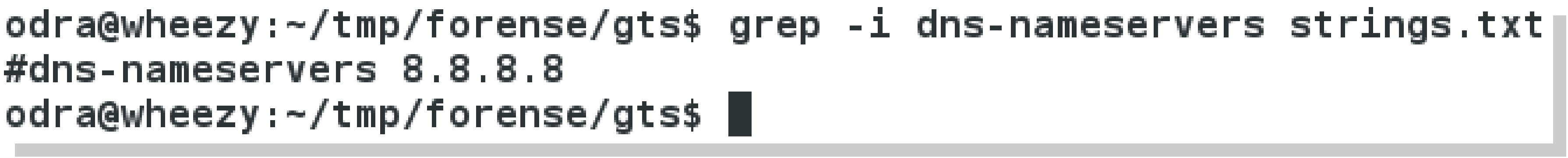
Dados encontrados:

3. Registro de acesso remoto (SSH)



```
odra@wheezy:~/tmp/forense/gts$ grep -i " 189.126.198.235" strings.txt
Dec  3 10:34:49 homer sshd[764]: Accepted password for sshuser from 189.126.198.235 port 15297 ssh2
Dec  3 10:34:49 homer sshd[764]: Accepted password for sshuser from 189.126.198.235 port 15297 ssh2
Dec  3 10:34:49 homer sshd[764]: Accepted password for sshuser from 189.126.198.235 port 15297 ssh2
MESSAGE=Accepted password for sshuser from 189.126.198.235 port 15297 ssh2
odra@wheezy:~/tmp/forense/gts$ 
```

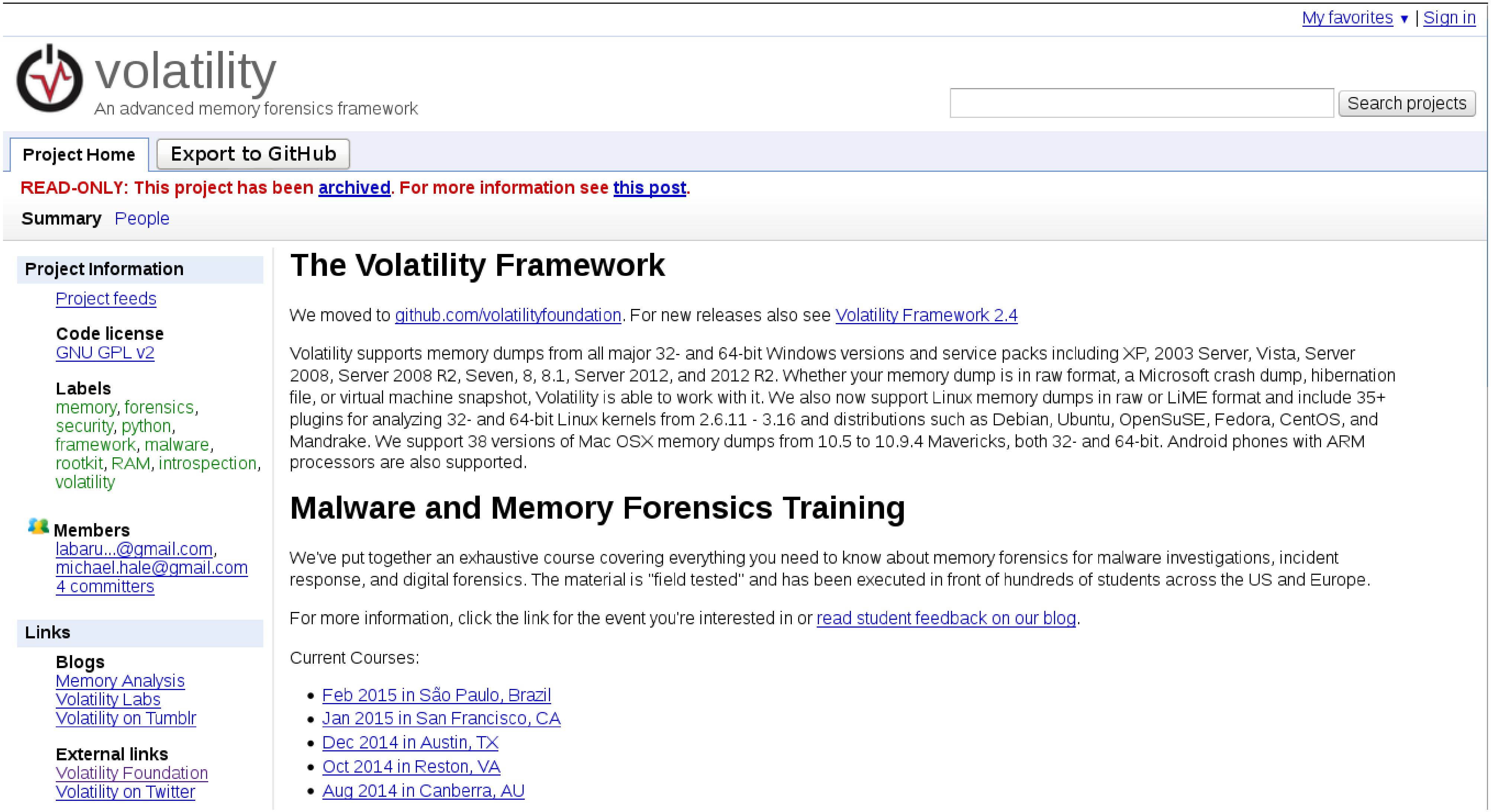
4. Configuração dos servidores DNS



```
odra@wheezy:~/tmp/forense/gts$ grep -i dns-nameservers strings.txt
#dns-nameservers 8.8.8.8
odra@wheezy:~/tmp/forense/gts$ 
```

Volatility framework

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



READ-ONLY: This project has been archived. For more information see this post.

Summary People

Project Information

Project feeds

Code license
GNU GPL v2

Labels
memory, forensics, security, python, framework, malware, rootkit, RAM, introspection, volatility

Members
labaru...@gmail.com,
michael.hale@gmail.com
4 committers

Links

Blogs
Memory Analysis
Volatility Labs
Volatility on Tumblr

External links
Volatility Foundation
Volatility on Twitter

The Volatility Framework

We moved to github.com/volatilityfoundation. For new releases also see Volatility Framework 2.4

Volatility supports memory dumps from all major 32- and 64-bit Windows versions and service packs including XP, 2003 Server, Vista, Server 2008, Server 2008 R2, Seven, 8, 8.1, Server 2012, and 2012 R2. Whether your memory dump is in raw format, a Microsoft crash dump, hibernation file, or virtual machine snapshot, Volatility is able to work with it. We also now support Linux memory dumps in raw or LiME format and include 35+ plugins for analyzing 32- and 64-bit Linux kernels from 2.6.11 - 3.16 and distributions such as Debian, Ubuntu, OpenSuSE, Fedora, CentOS, and Mandrake. We support 38 versions of Mac OSX memory dumps from 10.5 to 10.9.4 Mavericks, both 32- and 64-bit. Android phones with ARM processors are also supported.

Malware and Memory Forensics Training

We've put together an exhaustive course covering everything you need to know about memory forensics for malware investigations, incident response, and digital forensics. The material is "field tested" and has been executed in front of hundreds of students across the US and Europe.

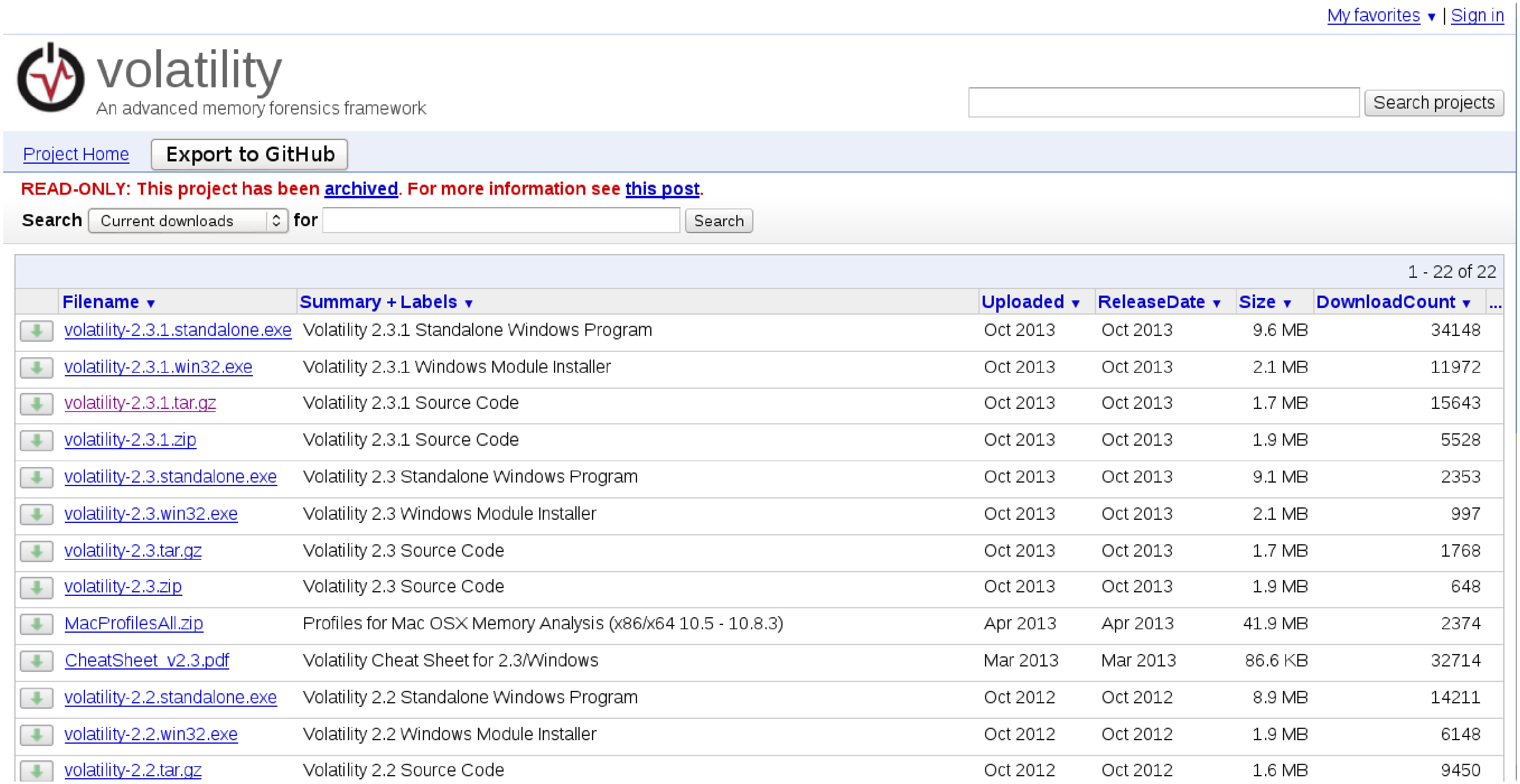
For more information, click the link for the event you're interested in or read student feedback on our blog.

Current Courses:

- Feb 2015 in São Paulo, Brazil
- Jan 2015 in San Francisco, CA
- Dec 2014 in Austin, TX
- Oct 2014 in Reston, VA
- Aug 2014 in Canberra, AU

Volatility framework

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



READ-ONLY: This project has been archived. For more information see this post.

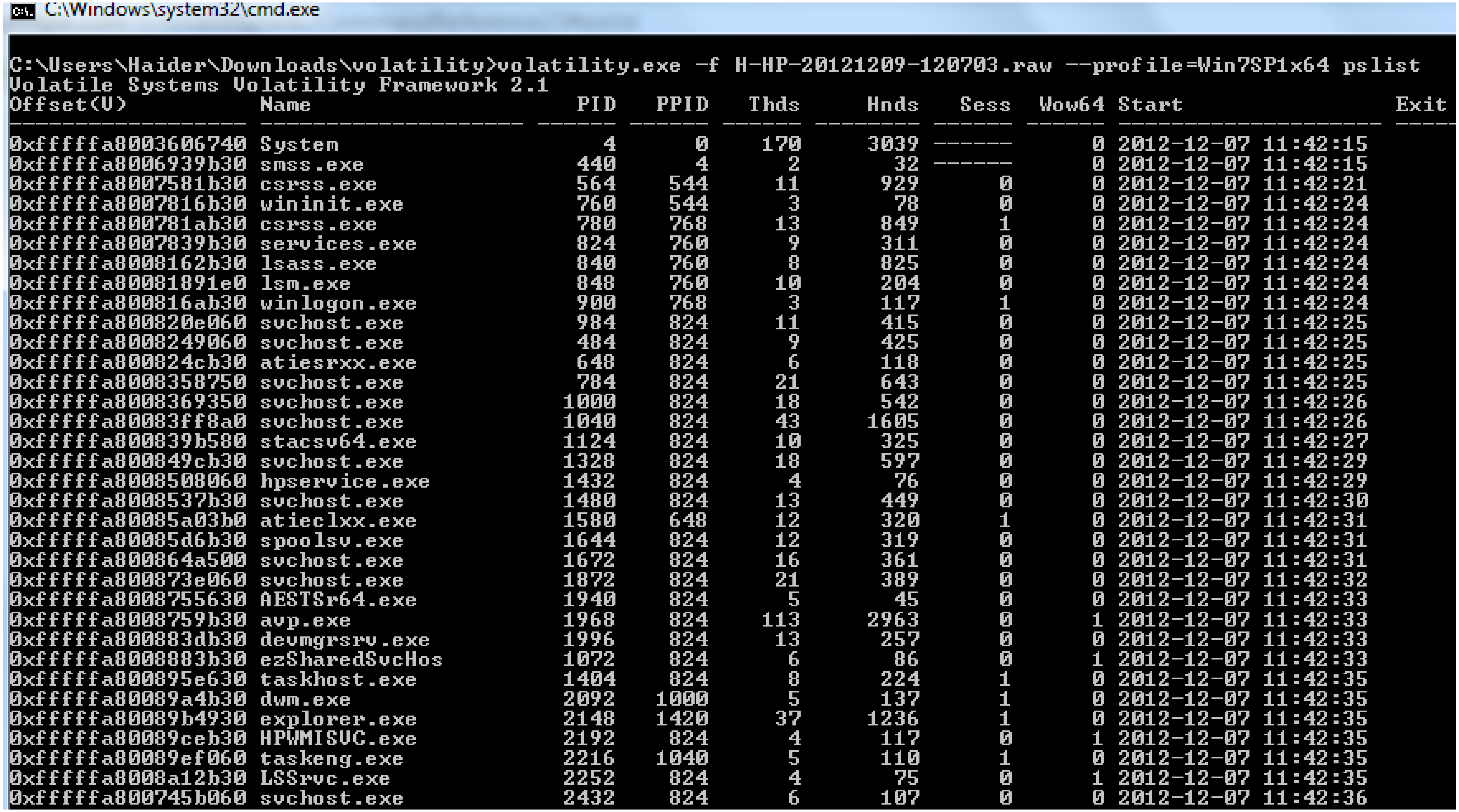
Search Current downloads for Search

1 - 22 of 22

	Filename ▾	Summary + Labels ▾	Uploaded ▾	ReleaseDate ▾	Size ▾	DownloadCount ▾
⬇	volatility-2.3.1.standalone.exe	Volatility 2.3.1 Standalone Windows Program	Oct 2013	Oct 2013	9.6 MB	34148
⬇	volatility-2.3.1.win32.exe	Volatility 2.3.1 Windows Module Installer	Oct 2013	Oct 2013	2.1 MB	11972
⬇	volatility-2.3.1.tar.gz	Volatility 2.3.1 Source Code	Oct 2013	Oct 2013	1.7 MB	15643
⬇	volatility-2.3.1.zip	Volatility 2.3.1 Source Code	Oct 2013	Oct 2013	1.9 MB	5528
⬇	volatility-2.3.standalone.exe	Volatility 2.3 Standalone Windows Program	Oct 2013	Oct 2013	9.1 MB	2353
⬇	volatility-2.3.win32.exe	Volatility 2.3 Windows Module Installer	Oct 2013	Oct 2013	2.1 MB	997
⬇	volatility-2.3.tar.gz	Volatility 2.3 Source Code	Oct 2013	Oct 2013	1.7 MB	1768
⬇	volatility-2.3.zip	Volatility 2.3 Source Code	Oct 2013	Oct 2013	1.9 MB	648
⬇	MacProfilesAll.zip	Profiles for Mac OSX Memory Analysis (x86/x64 10.5 - 10.8.3)	Apr 2013	Apr 2013	41.9 MB	2374
⬇	CheatSheet_v2.3.pdf	Volatility Cheat Sheet for 2.3/Windows	Mar 2013	Mar 2013	86.6 KB	32714
⬇	volatility-2.2.standalone.exe	Volatility 2.2 Standalone Windows Program	Oct 2012	Oct 2012	8.9 MB	14211
⬇	volatility-2.2.win32.exe	Volatility 2.2 Windows Module Installer	Oct 2012	Oct 2012	1.9 MB	6148
⬇	volatility-2.2.tar.gz	Volatility 2.2 Source Code	Oct 2012	Oct 2012	1.6 MB	9450

Volatility framework

http://blog.creativeitp.com/wp-content/uploads/2012/12/volatility03.png



```
C:\Users\Haider\Downloads\volatility>volatility.exe -f H-HP-20121209-120703.raw --profile=Win7SP1x64 pslist
Volatile Systems Volatility Framework 2.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ -------------------- -----
0xfffffa8003606740 System                    4      0    170     3039 ------      0 2012-12-07 11:42:15
0xfffffa8006939b30 smss.exe                440      4      2       32 ------      0 2012-12-07 11:42:15
0xfffffa8007581b30 csrss.exe               564    544     11      929      0      0 2012-12-07 11:42:21
0xfffffa8007816b30 wininit.exe             760    544      3       78      0      0 2012-12-07 11:42:24
0xfffffa800781ab30 csrss.exe               780    768     13      849      1      0 2012-12-07 11:42:24
0xfffffa8007839b30 services.exe            824    760      9      311      0      0 2012-12-07 11:42:24
0xfffffa8008162b30 lsass.exe               840    760      8      825      0      0 2012-12-07 11:42:24
0xfffffa80081891e0 lsm.exe                 848    760     10      204      0      0 2012-12-07 11:42:24
0xfffffa800816ab30 winlogon.exe            900    768      3      117      1      0 2012-12-07 11:42:24
0xfffffa800820e060 svchost.exe             984    824     11      415      0      0 2012-12-07 11:42:25
0xfffffa8008249060 svchost.exe             484    824      9      425      0      0 2012-12-07 11:42:25
0xfffffa800824cb30 atiesrxx.exe            648    824      6      118      0      0 2012-12-07 11:42:25
0xfffffa8008358750 svchost.exe             784    824     21      643      0      0 2012-12-07 11:42:25
0xfffffa8008369350 svchost.exe            1000    824     18      542      0      0 2012-12-07 11:42:26
0xfffffa80083ff8a0 svchost.exe            1040    824     43     1605      0      0 2012-12-07 11:42:26
0xfffffa800839b580 stacsv64.exe           1124    824     10      325      0      0 2012-12-07 11:42:27
0xfffffa800849cb30 svchost.exe            1328    824     18      597      0      0 2012-12-07 11:42:29
0xfffffa8008508060 hpservice.exe          1432    824      4       76      0      0 2012-12-07 11:42:29
0xfffffa8008537b30 svchost.exe            1480    824     13      449      0      0 2012-12-07 11:42:30
0xfffffa80085a03b0 atieclxx.exe           1580    648     12      320      1      0 2012-12-07 11:42:31
0xfffffa80085d6b30 spoolsv.exe            1644    824     12      319      0      0 2012-12-07 11:42:31
0xfffffa800864a500 svchost.exe            1672    824     16      361      0      0 2012-12-07 11:42:31
0xfffffa800873e060 svchost.exe            1872    824     21      389      0      0 2012-12-07 11:42:32
0xfffffa8008755630 AESTSr64.exe           1940    824      5       45      0      0 2012-12-07 11:42:33
0xfffffa8008759b30 avp.exe                1968    824    113     2963      0      1 2012-12-07 11:42:33
0xfffffa800883db30 devmgrsrv.exe          1996    824     13      257      0      0 2012-12-07 11:42:33
0xfffffa8008883b30 ezSharedSvcHos         1072    824      6       86      0      1 2012-12-07 11:42:33
0xfffffa800895e630 taskhost.exe           1404    824      8      224      1      0 2012-12-07 11:42:35
0xfffffa80089a4b30 dwm.exe                2092   1000      5      137      1      0 2012-12-07 11:42:35
0xfffffa80089b4930 explorer.exe           2148   1420     37     1236      1      0 2012-12-07 11:42:35
0xfffffa80089ceb30 HPWMISVC.exe           2192    824      4      117      0      1 2012-12-07 11:42:35
0xfffffa80089ef060 taskeng.exe            2216   1040      5      110      1      0 2012-12-07 11:42:35
0xfffffa8008a12b30 LSSrvc.exe             2252    824      4       75      0      1 2012-12-07 11:42:35
0xfffffa800745b060 svchost.exe            2432    824      6      107      0      0 2012-12-07 11:42:36
```

Disponível em http://blog.creativeitp.com/wp-content/uploads/2012/12/volatility03.png

Considerações finais

QUESTIONS?
CONCERNS?
COMMENTS?

osmany.arruda@fatec.sp.gov.br
osmany.arruda@gmail.com