

COFFORENSE

CONFERÊNCIA DE CAFÉ COM FORENSE

DIA 10 DE DEZEMBRO DE 08:H AS 12H NO AUDITORIO CENTRAL DO CENTRO

UNIVERSITÁRIO ESTACIO DO CEARÁ - PARANGABA

AV. SENADOR FERNANDES TÁVORA, 137 - JOQUEI CLUBE

PROGRAMAÇÃO:

8:00H **DEGUSTACAO DE CAFÉ** - APOIO CAFÉ 3CORACOES

9:00H **FORENSE EM RAM** - IDENTIFICANDO UM MALWARE ESCONDIDO -
PROF. MARCOS MONTEIRO - PRESIDENTE DA ASSOCIACAO DE PERITOS EM COMPUTACAO
FORENSE (APECOF).

10:00H **FORENSE EM SMARTPHONES** - DESCOBRINDO A SENHA DE
UM ANDROID E ACESSANDO A BASE DE DADOS CRIPTOGRAFADA DO WHATSAPP
- PROF. PEDRO VERÍSSIMO - PERITO AD-HOC E ANALISTA DE REDES.

11:00H **COPIA E ELIMINACAO DE DADOS** - A IMPORTÂNCIA DA COPIA
FORENSE PARA INTEGRIDADE E WIPE PARA CONFIDENCIALIDADE DOS DADOS -
ÉRICO MANFREDI - CONSULTOR EM COMPUTACAO FORENSE E SOCIO DA EMPRESA FLASHMEMORY
BRASIL;

INSCRIÇÕES EM WWW.MARCOSMONTEIRO.COM.BR



— COFFORENSE
CONFERÊNCIA DE CAFÉ COM FORENSE

Forense em RAM – Identificando Malware

Prof. Marcos Monteiro

Presidente

Associação de Peritos em Computação Forense

APECOF

www.marcosmonteiro.com.br



Condutas Indevidas Praticadas por Computador



Condutas Indevidas Praticadas por Computador

Crimes Cibernéticos



Condutas Indevidas Praticadas por Computador

Crimes Cibernéticos

**Ações Prejudiciais Atípicas
ou Conduta Danosa Atípica**



Condutas Indevidas Praticadas por Computador

Crimes Cibernéticos

**Ações Prejudiciais Atípicas
ou Conduta Danosa Atípica**

**Impróprios ou
Abertos**



Condutas Indevidas Praticadas por Computador

Crimes Cibernéticos

Ações Prejudiciais Atípicas ou Conduta Danosa Atípica

**Impróprios ou
Abertos**

**Próprios ou
Exclusivamente
Cibernéticos**



Escopo da Investigação e perícia

Extrajudicial Judicial

Investigação extrajudicial

- Equipe interna
- Profissional externo
- Empresa externa



Pessoa Física



Pessoa Jurídica de Direito Privado



Pessoa Jurídica de Direito Público

Sindicância

- Comissão de sindicância
- Corregedoria

Polícia Judiciária
(civil ou federal)

Judicial



Judiciário

Ação Judicial

- Perito Oficial
- Assistente Técnico



Ministério Público

Promotor

Inquérito Policial

- Investigador
- Perito Criminal
- Médico legista



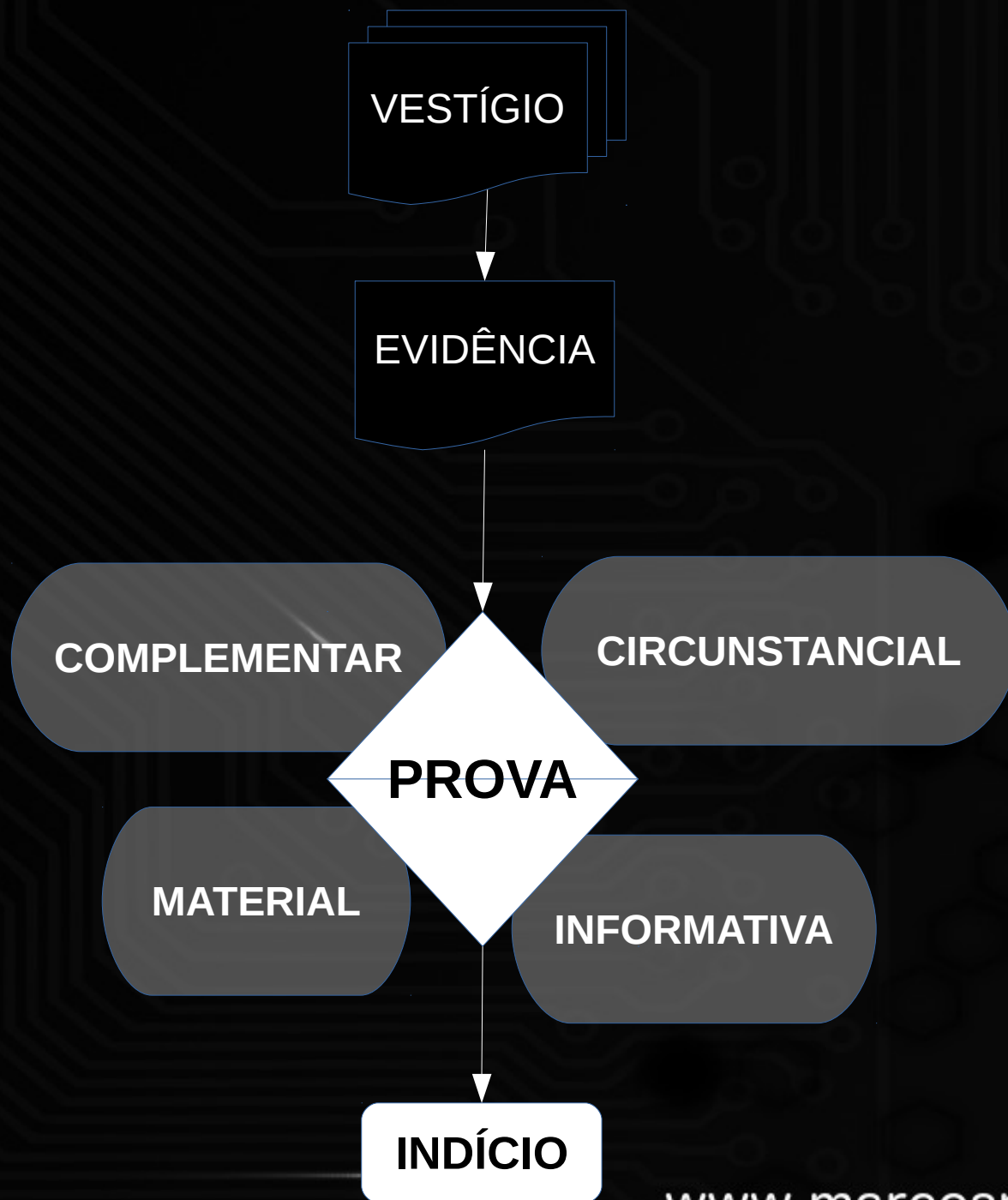
Lei nº 12.737

“Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.







Materialidade Digital

- Dados Voláteis
 - Podem ser modificados
 - usuários logados, processos, conexões de redes, área de transferência...
- Dados Transitórios (de curta duração)
 - Reside na memória a cache
 - usuários que fizeram logout informações de abertura de conexão de rede...



Materialidade Digital

- Dados Voláteis
 - Podem ser modificados
 - usuários logados, processos, conexões de redes, área de transferência...
- Dados Transitórios (de curta duração)
 - Reside na memória a cache
 - usuários que fizeram logout informações de abertura de conexão de rede...
- Dados Não Voláteis
 - Usado no armazenamento secundário
 - arquivos em geral, swap, registros, eventos...



Materialidade Digital

- Dados Voláteis
 - Podem ser modificados
 - usuários logados, processos, conexões de redes, área de transferência...
- Dados Transitórios (de curta duração)
 - Reside na memória a cache
 - usuários que fizeram logout informações de abertura de conexão de rede...
- Dados Não Voláteis
 - Usado no armazenamento secundário
 - arquivos em geral, swap, registros, eventos...
- Dados Frágeis
 - Arquivos temporários
 - podem ser modificados como ultimo acesso, acesso de arquivos...



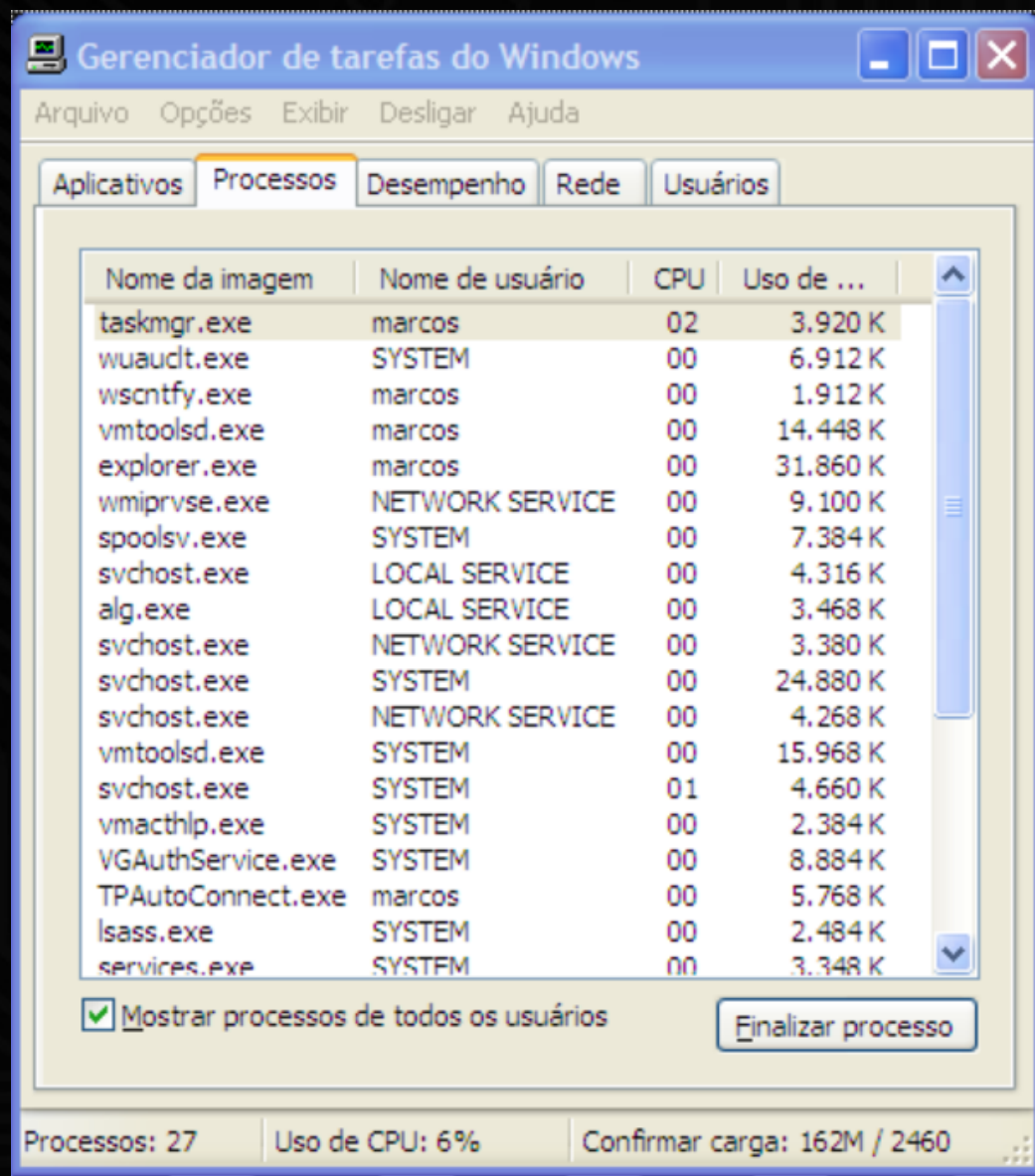
Caso Concreto



Joaozinho é um promissor empresário do ramo de importação de chiclete PLOC e caramelo Zorro; muito preocupado com segurança, possui um microcomputador exclusivo para transações bancárias pela Internet, sempre mantendo o Sistema Operacional e Antivírus atualizados, porem Joaozinho percebeu uma transferência bancária no valor de R\$ 9.000,00 de sua conta na qual ele desconhecia, em contato com o banco, eles recomendaram que o empresario modificasse suas senhas de Internet, mas mesmo com a mudança uma nova transferencia bancária continuou ocorrendo.



Processo = Programa em execução





Conexões de redes

netstat -nab

C:\WINDOWS\system32\cmd.exe

C:\>netstat -nab

Conexões ativas

Proto	Endereço local	Endereço externo	Estado
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
	c:\windows\system32\WS2_32.dll		
	C:\WINDOWS\system32\RPCRT4.dll		
	c:\windows\system32\RPCSS.dll		
	C:\WINDOWS\system32\svchost.exe		
	C:\WINDOWS\system32\ADVAPI32.dll		
	[svchost.exe]		
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
	[System]		
TCP	10.0.0.22:139	0.0.0.0:0	LISTENING
	[System]		
TCP	127.0.0.1:1028	0.0.0.0:0	LISTENING
	[alg.exe]		
UDP	0.0.0.0:500	*:*	
	[lsass.exe]		
UDP	0.0.0.0:4500	*:*	
	[lsass.exe]		

UDP 10.0.0.22:123 *:*

c:\windows\system32\WS2_32.dll

c:\windows\system32\W32TIME.dll

ntdll.dll

C:\WINDOWS\system32\kernel32.dll

[svchost.exe]

UDP 127.0.0.1:1900 *:*

c:\windows\system32\WS2_32.dll

c:\windows\system32\SSDPSRV.dll

ntdll.dll

C:\WINDOWS\system32\kernel32.dll

[svchost.exe]

UDP 127.0.0.1:1078 *:*

c:\windows\system32\WS2_32.dll

C:\WINDOWS\system32\WLDP32.dll

C:\WINDOWS\system32\winrnr.dll

c:\windows\system32\WS2_32.dll

c:\windows\system32\W32TIME.dll

[svchost.exe]

UDP 127.0.0.1:123 *:*

c:\windows\system32\WS2_32.dll

c:\windows\system32\W32TIME.dll

ntdll.dll

C:\WINDOWS\system32\kernel32.dll

[svchost.exe]

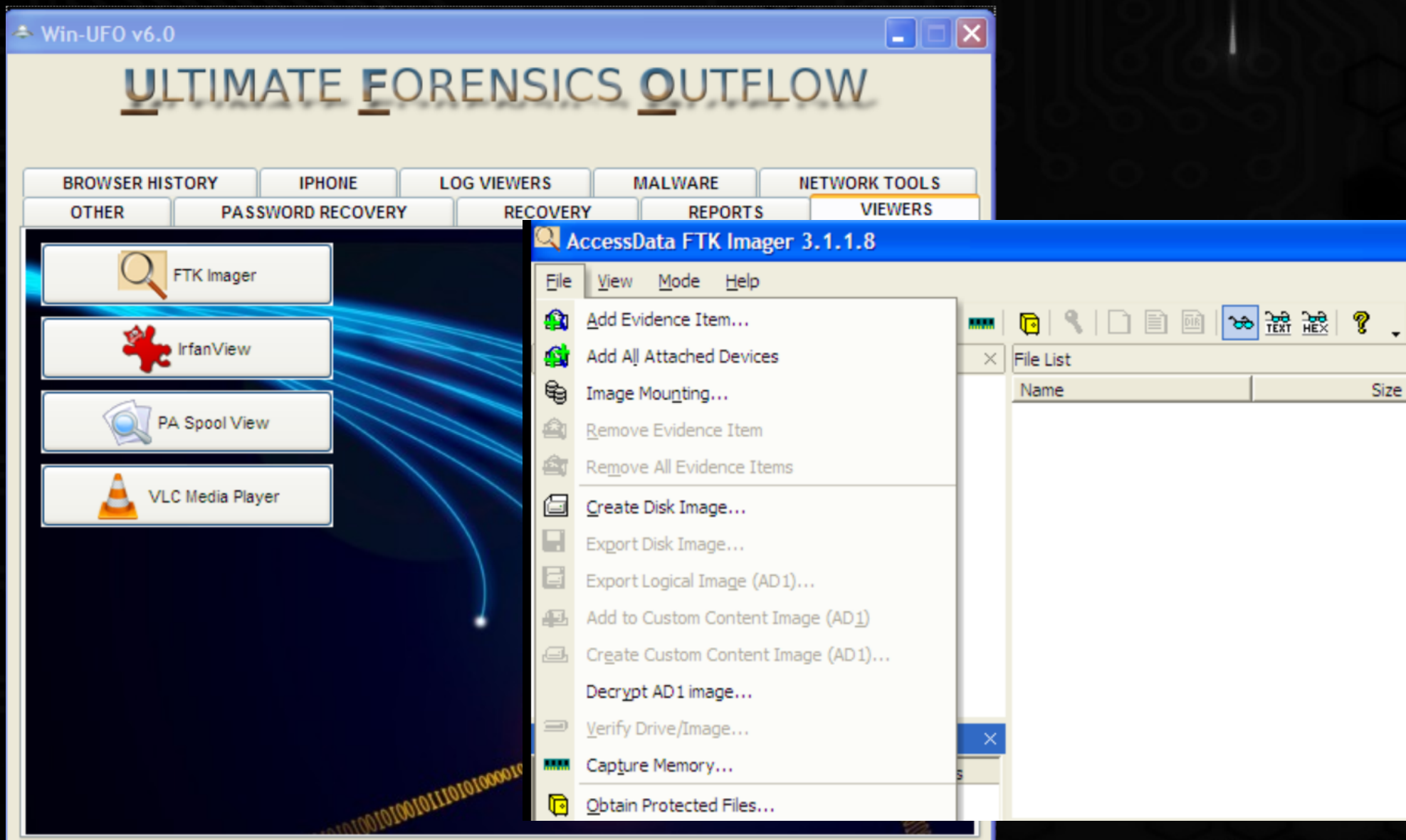


DUMP de RAM





FTK-Imager





Volatility

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@mm:~# volatility -h
Volatility Foundation Volatility Framework 2.5
Usage: Volatility - A memory forensics analysis platform.

Options:
-h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
--conf-file=/root/.volatilityrc
                        User based configuration file
-d, --debug           Debug volatility
--plugins=PLUGINS     Additional plugin directories to use (colon separated)
--info               Print information about all registered objects
--cache-directory=/root/.cache/volatility
                        Directory where cache files are stored
--cache              Use caching
--tz=TZ              Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
-f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
--profile=WinXPSP2x86
                        Name of the profile to load (use --info to see a list
                        of supported profiles)
-l LOCATION, --location=LOCATION
                        A URN location from which to load an address space
-w, --write          Enable write support
--dtb=DTB            DTB Address
--shift=SHIFT        Mac KASLR shift address
--output=text        Output in this format (support is module specific, see
                        the Module Output Options below)
--output-file=OUTPUT_FILE
                        Write output in this file
-v, --verbose        Verbose information
-g KDBG, --kdbg=KDBG Specify a KDBG virtual address (Note: for 64-bit
                        Windows 8 and above this is the address of
                        KdCopyDataBlock)
--force             Force utilization of suspect profile
-k KPCR, --kpcr=KPCR Specify a specific KPCR address
--cookie=COOKIE     Specify the address of nt!ObHeaderCookie (valid for
                        Windows 10 only)
```

O **Volatility** é uma coletânea de ferramentas abertas em python formando um framework sob a licença GNU GPL v2 para a extração de vestígios digitais voláteis presentes em memória RAM de máquinas com Sistema Operacional Microsoft Windows.



O que é possível ?

- Processos em execução;
- Sockets de rede;
- Conexões abertas de rede;
- Arquivos e DLLs carregados para cada processo;
- Registros utilizados para cada processo;
- Módulos de Kernel do Sistema Operacional;
- Mapeamento de Endereços físicos e virtuais;
- Mapa de Memória de cada processo;
- E mais outras coisas ...



volatility -h

```
root@mm: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@mm:~# volatility -h
Volatility Foundation Volatility Framework 2.5
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help                list all available options and their default values.
                           Default values may be set in the configuration file
                           (/etc/volatilityrc)
  --conf-file=/root/.volatilityrc
                           User based configuration file
  -d, --debug               Debug volatility
  --plugins=PLUGINS         Additional plugin directories to use (colon separated)
  --info                    Print information about all registered objects
  --cache-directory=/root/.cache/volatility
                           Directory where cache files are stored
  --cache                   Use caching
  --tz=TZ                   Sets the (Olson) timezone for displaying timestamps
                           using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                           Filename to use when opening an image
  --profile=WinXPSP2x86     Name of the profile to load (use --info to see a list
                           of supported profiles)
  -l LOCATION, --location=LOCATION
                           A URN location from which to load an address space
  -w, --write               Enable write support
  --dtb=DTB                DTB Address
  --shift=SHIFT             Mac KASLR shift address
  --output=text              Output in this format (support is module specific, see
                           the Module Output Options below)
  --output-file=OUTPUT_FILE
                           Write output in this file
  -v, --verbose             Verbose information
  -g KDBG, --kdbg=KDBG      Specify a KDBG virtual address (Note: for 64-bit
                           Windows 8 and above this is the address of
                           KdCopyDataBlock)
  --force                   Force utilization of suspect profile
  -k KPCR, --kpcr=KPCR      Specify a specific KPCR address
  --cookie=COOKIE           Specify the address of nt!ObHeaderCookie (valid for
                           Windows 10 only)
```



Informações do DUMP

volatility -f dumpmemoria.vmem imageinfo

```
root@mm:/# volatility -f DumpRAM.vmem imageinfo
Volatility Foundation Volatility Framework 2.5
INFO      : volatility.debug      : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
          AS Layer1           : IA32PagedMemoryPae (Kernel AS)
          AS Layer2           : FileAddressSpace (/DumpRAM.vmem)
          PAE type            : PAE
          DTB                 : 0x319000L
          KDBG                 : 0x80544ce0L
          Number of Processors : 1
          Image Type (Service Pack) : 2
          KPCR for CPU 0       : 0xffdff000L
          KUSER_SHARED_DATA    : 0xffdf0000L
          Image date and time  : 2010-08-15 19:17:56 UTC+0000
          Image _local date and time : 2010-08-15 15:17:56 -0400
```



PROCESSOS

volatility -f dumpmemoria.vmem pslist

```
root@mm:/# volatility -f DumpRAM.vmem pslist
```

Volatility Foundation Volatility Framework 2.5

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Ex
0x810b1660	System	4	0	58	379	-----	0		
0xff2ab020	smss.exe	544	4	3	21	-----	0	2010-08-11 06:06:21 UTC+0000	
0xfflecda0	csrss.exe	608	544	10	410	0	0	2010-08-11 06:06:23 UTC+0000	
0xfflec978	winlogon.exe	632	544	24	536	0	0	2010-08-11 06:06:23 UTC+0000	
0xff247020	services.exe	676	632	16	288	0	0	2010-08-11 06:06:24 UTC+0000	
0xff255020	lsass.exe	688	632	21	405	0	0	2010-08-11 06:06:24 UTC+0000	
0xff218230	vmacthlp.exe	844	676	1	37	0	0	2010-08-11 06:06:24 UTC+0000	
0x80ff88d8	svchost.exe	856	676	29	336	0	0	2010-08-11 06:06:24 UTC+0000	
0xff217560	svchost.exe	936	676	11	288	0	0	2010-08-11 06:06:24 UTC+0000	
0x80fbf910	svchost.exe	1028	676	88	1424	0	0	2010-08-11 06:06:24 UTC+0000	
0xff22d558	svchost.exe	1088	676	7	93	0	0	2010-08-11 06:06:25 UTC+0000	
0xff203b80	svchost.exe	1148	676	15	217	0	0	2010-08-11 06:06:26 UTC+0000	
0xff1d7da0	spoolsv.exe	1432	676	14	145	0	0	2010-08-11 06:06:26 UTC+0000	
0xff1b8b28	vmtoolsd.exe	1668	676	5	225	0	0	2010-08-11 06:06:35 UTC+0000	
0xff1fdc88	VMUpgradeHelper	1788	676	5	112	0	0	2010-08-11 06:06:38 UTC+0000	
0xff143b28	TPAutoConnSvc.e	1968	676	5	106	0	0	2010-08-11 06:06:39 UTC+0000	
0xff25a7e0	alg.exe	216	676	8	120	0	0	2010-08-11 06:06:39 UTC+0000	
0xff364310	wscntfy.exe	888	1028	1	40	0	0	2010-08-11 06:06:49 UTC+0000	
0xff38b5f8	TPAutoConnect.e	1084	1968	1	68	0	0	2010-08-11 06:06:52 UTC+0000	
0x80f60da0	wuauc.lt.exe	1732	1028	7	189	0	0	2010-08-11 06:07:44 UTC+0000	
0xff3865d0	explorer.exe	1724	1708	13	326	0	0	2010-08-11 06:09:29 UTC+0000	
0xff3667e8	VMwareTray.exe	432	1724	1	60	0	0	2010-08-11 06:09:31 UTC+0000	
0xff374980	VMwareUser.exe	452	1724	8	207	0	0	2010-08-11 06:09:32 UTC+0000	
0x80f94588	wuauc.lt.exe	468	1028	4	142	0	0	2010-08-11 06:09:37 UTC+0000	
0xff224020	cmd.exe	124	1668	0	-----	0	0	2010-08-15 19:17:55 UTC+0000	20

```
root@mm:/#
```



PROCESSOS por ORDEM DE CHAMADA

volatility -f dumpmemoria.vmem pstree

```
root@mm:/# volatility -f DumpRAM.vmem pstree
Volatility Foundation Volatility Framework 2.5
```

Name	Pid	PPid	Thds	Hnds	Time
0x810b1660:System	4	0	58	379	1970-01-01 00:00:00 UTC+0000
. 0xff2ab020:smss.exe	544	4	3	21	2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe	632	544	24	536	2010-08-11 06:06:23 UTC+0000
... 0xff255020:lsass.exe	688	632	21	405	2010-08-11 06:06:24 UTC+0000
... 0xff247020:services.exe	676	632	16	288	2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe	1668	676	5	225	2010-08-11 06:06:35 UTC+0000
..... 0xff224020:cmd.exe	124	1668	0	----	2010-08-15 19:17:55 UTC+0000
.... 0x80ff88d8:svchost.exe	856	676	29	336	2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0:spoolsv.exe	1432	676	14	145	2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe	1028	676	88	1424	2010-08-11 06:06:24 UTC+0000
..... 0x80f60da0:wuauc.lt.exe	1732	1028	7	189	2010-08-11 06:07:44 UTC+0000
..... 0x80f94588:wuauc.lt.exe	468	1028	4	142	2010-08-11 06:09:37 UTC+0000
..... 0xff364310:wsntfy.exe	888	1028	1	40	2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe	936	676	11	288	2010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e	1968	676	5	106	2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e	1084	1968	1	68	2010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe	1088	676	7	93	2010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe	844	676	1	37	2010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0:alg.exe	216	676	8	120	2010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe	1148	676	15	217	2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper	1788	676	5	112	2010-08-11 06:06:38 UTC+0000
.. 0xff1ecda0:csrss.exe	608	544	10	410	2010-08-11 06:06:23 UTC+0000
0xff3865d0:explorer.exe	1724	1708	13	326	2010-08-11 06:09:29 UTC+0000
. 0xff374980:VMwareUser.exe	452	1724	8	207	2010-08-11 06:09:32 UTC+0000
. 0xff3667e8:VMwareTray.exe	432	1724	1	60	2010-08-11 06:09:31 UTC+0000



ALOCAÇÃO DE MEMÓRIA DO PROCESSO

volatility -f dumpmemoria.vmem psscan

```
root@mm: /# volatility -f DumpRAM.vmem psscan
```

```
Volatility Foundation Volatility Framework 2.5
```

Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
0x00000000010c3da0	wuauc1t.exe	1732	1028	0x06cc02c0	2010-08-11 06:07:44 UTC+0000	
0x00000000010f7588	wuauc1t.exe	468	1028	0x06cc0180	2010-08-11 06:09:37 UTC+0000	
0x0000000001122910	svchost.exe	1028	676	0x06cc0120	2010-08-11 06:06:24 UTC+0000	
0x000000000115b8d8	svchost.exe	856	676	0x06cc00e0	2010-08-11 06:06:24 UTC+0000	
0x0000000001214660	System	4	0	0x00319000		
0x0000000001211ab28	TPAutoConnSvc.e	1968	676	0x06cc0260	2010-08-11 06:06:39 UTC+0000	
0x000000000149c15f8	TPAutoConnect.e	1084	1968	0x06cc0220	2010-08-11 06:06:52 UTC+0000	
0x00000000014a065d0	explorer.exe	1724	1708	0x06cc0280	2010-08-11 06:09:29 UTC+0000	
0x00000000014b5a980	VMwareUser.exe	452	1724	0x06cc0300	2010-08-11 06:09:32 UTC+0000	
0x00000000014be97e8	VMwareTray.exe	432	1724	0x06cc02e0	2010-08-11 06:09:31 UTC+0000	
0x00000000014c2b310	wscntfy.exe	888	1028	0x06cc0200	2010-08-11 06:06:49 UTC+0000	
0x00000000015471020	smss.exe	544	4	0x06cc0020	2010-08-11 06:06:21 UTC+0000	
0x00000000015f027e0	alg.exe	216	676	0x06cc0240	2010-08-11 06:06:39 UTC+0000	
0x00000000015f47020	lsass.exe	688	632	0x06cc00a0	2010-08-11 06:06:24 UTC+0000	
0x00000000016015020	services.exe	676	632	0x06cc0080	2010-08-11 06:06:24 UTC+0000	
0x000000000161ef558	svchost.exe	1088	676	0x06cc0140	2010-08-11 06:06:25 UTC+0000	
0x00000000016238020	cmd.exe	124	1668	0x06cc02a0	2010-08-15 19:17:55 UTC+0000	2010-08-15 19:17:56 UTC+0000
0x00000000016384230	vmacthlp.exe	844	676	0x06cc00c0	2010-08-11 06:06:24 UTC+0000	
0x000000000163c5560	svchost.exe	936	676	0x06cc0100	2010-08-11 06:06:24 UTC+0000	
0x00000000016499b80	svchost.exe	1148	676	0x06cc0160	2010-08-11 06:06:26 UTC+0000	
0x0000000001655fc88	VMUpgradeHelper	1788	676	0x06cc01e0	2010-08-11 06:06:38 UTC+0000	
0x000000000166f0978	winlogon.exe	632	544	0x06cc0060	2010-08-11 06:06:23 UTC+0000	
0x000000000166f0da0	csrss.exe	608	544	0x06cc0040	2010-08-11 06:06:23 UTC+0000	
0x00000000016945da0	spoolsv.exe	1432	676	0x06cc01a0	2010-08-11 06:06:26 UTC+0000	
0x000000000169a7328	VMip.exe	1944	124	0x06cc0320	2010-08-15 19:17:55 UTC+0000	2010-08-15 19:17:56 UTC+0000
0x000000000169d5b28	vmtoolsd.exe	1668	676	0x06cc01c0	2010-08-11 06:06:35 UTC+0000	

```
root@mm: /# █
```



SID de cada processo

volatility -f dumpmemoria.vmem getsids

```
root@mm:/# volatility -f DumpRAM.vmem getsids
Volatility Foundation Volatility Framework 2.5
System (4): S-1-5-18 (Local System)
System (4): S-1-5-32-544 (Administrators)
System (4): S-1-1-0 (Everyone)
System (4): S-1-5-11 (Authenticated Users)
smss.exe (544): S-1-5-18 (Local System)
smss.exe (544): S-1-5-32-544 (Administrators)
smss.exe (544): S-1-1-0 (Everyone)
smss.exe (544): S-1-5-11 (Authenticated Users)
csrss.exe (608): S-1-5-18 (Local System)
csrss.exe (608): S-1-5-32-544 (Administrators)
csrss.exe (608): S-1-1-0 (Everyone)
csrss.exe (608): S-1-5-11 (Authenticated Users)
winlogon.exe (632): S-1-5-18 (Local System)
winlogon.exe (632): S-1-5-32-544 (Administrators)
winlogon.exe (632): S-1-1-0 (Everyone)
winlogon.exe (632): S-1-5-11 (Authenticated Users)
services.exe (676): S-1-5-18 (Local System)
services.exe (676): S-1-5-32-544 (Administrators)
services.exe (676): S-1-1-0 (Everyone)
services.exe (676): S-1-5-11 (Authenticated Users)
lsass.exe (688): S-1-5-18 (Local System)
lsass.exe (688): S-1-5-32-544 (Administrators)
lsass.exe (688): S-1-1-0 (Everyone)
lsass.exe (688): S-1-5-11 (Authenticated Users)
vmacthlp.exe (844): S-1-5-18 (Local System)
```



DLL de cada processo

volatility -f dumpmemoria.vmem dlllist

```
root@mm:/# volatility -f DumpRAM.vmem dlllist
Volatility Foundation Volatility Framework 2.5
```

```
*****
```

```
System pid:      4
Unable to read PEB for task.
```

```
*****
```

```
smss.exe pid:    544
Command line : \SystemRoot\System32\smss.exe
```

Base	Size	LoadCount	Path
0x48580000	0xf000	0xffff	\SystemRoot\System32\smss.exe
0x7c900000	0xb0000	0xffff	

```
*****
```

```
csrss.exe pid:    608
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,30
72,512 Windows=0n SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllI
nitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequest
Threads=16
Service Pack 2
```



É possível ler o Registro do Windows Ver Firewall

volatility printkey -f dumpmemoria.vmem -K

'ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile'

```
Volatile Systems Volatility Framework 2.0
```

```
Legend: (S) = Stable (V) = Volatile
```

```
-----
```

```
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
```

```
Key name: StandardProfile (S)
```

```
Last updated: 2010-08-15 19:17:24
```

```
Subkeys:
```

```
(S) AuthorizedApplications
```

```
Values:
```

```
REG_DWORD EnableFirewall : (S) 0
```



Alterações do SAM

volatility printkey -f dumpmemoria.vmem userassist

Values:

Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SAM

Key name: SAM (S)

Last updated: 2010-06-10 12:01:43 UTC+0000

Subkeys:

(S) SAM



Alterações de Perfis Existentes

**# volatility printkey -f dumpmemoria.vmem -K
'Software\Microsoft\Windows\CurrentVersion\Run'**

```
Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT  
Key name: Run (S)  
Last updated: 2010-06-10 16:11:25
```

Subkeys:

Values:

```
-----  
Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT  
Key name: Run (S)  
Last updated: 2010-06-10 16:11:21
```

Subkeys:

Values:

```
-----  
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT  
Key name: Run (S)  
Last updated: 2010-06-10 16:11:42
```



Conexões de Rede no momento do DUMP

volatility -f dumpmemoria.vmem connections

Arquivo Editar Ver Pesquisar Terminal Ajuda

```
root@mm:/# volatility -f DumpRAM.vmem connections
```

```
Volatility Foundation Volatility Framework 2.5
```

Offset(V)	Local Address	Remote Address	Pid
-----------	---------------	----------------	-----

```
root@mm:/#
```



Conexões de Rede que foram recentemente encerradas

volatility -f dumpmemoria.vmem connscan

```
root@mm:/# volatility -f DumpRAM.vmem connscan
Volatility Foundation Volatility Framework 2.5
Offset(P)  Local Address          Remote Address          Pid
-----
0x02214988 172.16.176.143:1054      193.104.41.75:80        856
0x06015ab0 0.0.0.0:1056             193.104.41.75:80        856
```



whois

```
inetnum:      193.104.41.0 - 193.104.41.255
netname:      VVPN-NET
descr:        PE Voronov Evgen Sergiyovich
country:      MD
org:          ORG-PESV2-RIPE
admin-c:      ESV1-RIPE
tech-c:       ESV1-RIPE
status:       ASSIGNED PI
mnt-by:       VVPN-MNT
mnt-by:       RIPE-NCC-END-MNT
mnt-lower:    RIPE-NCC-END-MNT
mnt-routes:   VVPN-MNT
mnt-domains:  VVPN-MNT
source:       RIPE # Filtered
```

```
organisation: ORG-PESV2-RIPE
org-name:     PE Voronov Evgen Sergiyovich
org-type:     OTHER
descr:        PE Evgen Sergeevich Voronov
address:      25 October street, 118-15
address:      Tiraspol, Transdnistria
phone:        +373 533 50404
admin-c:      ESV1-RIPE
tech-c:       ESV1-RIPE
mnt-ref:      VVPN-MNT
mnt-by:       VVPN-MNT
source:       RIPE # Filtered
```



Google

[Encyclopedia entry: PWS:Win32/Zbot.QW - Learn more about ...](#)

[www.microsoft.com/security/.../Entry.aspx?...](#) - Traduzir esta página

3 Dec 2009 – QW connects to the IP address '**193.104.41.75**' to download a configuration file, which is saved in the system as: <system folder>\local.ds ...

[The following IP address represent a list of Zeus C&C servers ...](#)

[malc0de.com/.../zbot_cc_servers.t...](#) - Estados Unidos - Traduzir esta página

... 193.104.41.68 20091201:http://**193.104.41.75**/kissme/rec.php, **193.104.41.75** 20091201:http://1.amiral-system.mobi/admin/gate.php, Cannot be resolved ...

The following system changes may indicate the presence of this malware:

- The presence of the following file:
 <system folder>\sdra64.exe
- The presence of the following registry modification:
 Added value: "userinit"
 With data: "<system folder>\userinit.exe, <system folder>\sdra64.exe"
 To subkey: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
- You have received and opened an e-mail message about the H1N1 virus with a hyperlink to a remotely hosted file named "vacc_profile.exe"



Zeus

O “Zeus ou Zbot” é um trojan que rouba nomes e senhas de acessos a internet relacionados a “internet banking” bem como permite um atacante remoto acessar um backdoor deixado ou presente na máquina;

Desabilita o firewall da máquina;

Geralmente disseminado por e-mail por meio de SPAM;
Cria um arquivo com nome mutex “AVIRA_210X” que realiza um “bypass” no firewall para depois ser copiado com um arquivo de nome “sdra64.exe” de forma escondida para o Sistema Operacional;



Zeus

- Modifica as entradas de registro do windows para que o arquivo autoexec.bat rode o malware toda vez que o sistema operacional reiniciar
 - Adds value: "ParseAutoexec"
 - With data: "1"
 - To subkey: HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
- Conecta-se no IP 193.104.41.75 para **baixar o arquivo de configuração do malware** e salva como **local.ds** onde irá conter diversos sites relacionados a internet banking;
- Armazena as **informações roubadas** no arquivo **user.ds**;



Arquivos abertos

volatility -f dumpmemoria.vmem filescan

```
root@mm:/# volatility -f DumpRAM.vmem filescan
```

```
Volatility Foundation Volatility Framework 2.5
```

```
Offset(P)          #Ptr    #Hnd Access Name
```

```
-----
```

0x000000000000096ca0	1	0	R--r-d	\Device\HarddiskVolume1\Documents and Settings\Adminis
trator\Start Menu\Programs\Windows Media Player.lnk				
0x000000000000353ad0	1	0	R--rwd	\Device\HarddiskVolume1\WINDOWS\system32\crypt32.dll
0x000000000000353cb8	1	0	R--rwd	\Device\HarddiskVolume1\WINDOWS\system32\apphelp.dll
0x0000000000003f34f8	3	0	RWD---	\Device\HarddiskVolume1\Directory
0x0000000000003f3f08	1	0	R--r-d	\Device\HarddiskVolume1\WINDOWS\system32\ipconf.tsp
0x000000000000471028	4	1	RW----	\Device\HarddiskVolume1\Documents and Settings\Adminis
trator\NTUSER.DAT				
0x000000000000471170	1	0	R--r--	\Device\HarddiskVolume1\WINDOWS\system32\wzcdlg.dll
0x000000000000471208	1	0	-WD---	\Device\HarddiskVolume1\System Volume Information_res
tore{4DA604DF-69BB-4F4A-9B3B-BBAA44DAE949}\RP15\snapshot\ComDb.Dat				
0x0000000000004715c0	1	0	R--r-d	\Device\HarddiskVolume1\WINDOWS\system32\cnbjmon.dll
0x0000000000004a06a0	1	0	R--r-d	\Device\HarddiskVolume1\WINDOWS\system32\urlmon.dll
0x0000000000004a09c8	1	0	R--r-d	\Device\HarddiskVolume1\WINDOWS\system32\localspl.dll
0x0000000000004aa4a0	3	0	RWD---	\Device\HarddiskVolume1\Directory
0x0000000000004aac10	3	1	RW-r--	\Device\HarddiskVolume1\WINDOWS\system32\wbem\Reposito
ry\FS\INDEX.BTR				
0x0000000000004aaef8	3	1	RW-r--	\Device\HarddiskVolume1\WINDOWS\system32\wbem\Reposito



Arquivos abertos

```
# volatility -f dumpmemoria.vmem filescan  
| egrep -i 'sdra64|user.ds|local.ds|AVIRA'
```

```
root@mm:/# volatility -f DumpRAM.vmem filescan | egrep 'sdra64|user.ds|local.ds|AVIRA'  
Volatility Foundation Volatility Framework 2.5  
0x0000000001061028      1      0 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\lowsec\user.ds  
0x00000000010bfd78      3      1 ----- \Device\NamedPipe\_AVIRA_2109  
0x000000000115ab90      1      1 R----- \Device\HarddiskVolume1\WINDOWS\system32\lowsec\user.ds  
0x00000000029d9b40      1      1 R----- \Device\HarddiskVolume1\WINDOWS\system32\sdra64.exe  
0x00000000029d9cf0      1      0 -WD--- \Device\HarddiskVolume1\WINDOWS\system32\sdra64.exe  
0x0000000002a528c0      3      1 ----- \Device\NamedPipe\_AVIRA_2108  
0x0000000002bbe470      1      1 R----- \Device\HarddiskVolume1\WINDOWS\system32\lowsec\local.ds  
root@mm:/#
```





VERITAS ASSEVERARE
www.apecof.org.br

www.marcosmonteiro.com.br



Obrigado!

Prof. Marcos Monteiro

+55 (85) 9 8805-4112

contato@marcosmonteiro.com.br

www.marcosmonteiro.com.br

