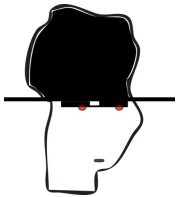
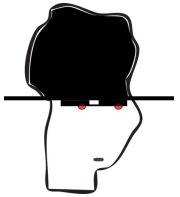
Introducción a la Forensia (2)

Seguridad Ofensiva



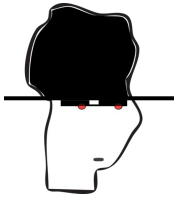
Informatica Forense



Informática Forense ⊂ Forense Digital ⊂ Ciencia Forense

Es la ciencia de adquirir, preservar,obtener, y presentar datos presentados electrónicamente y guardados en un medio informático.

Concepto: Forensic Computing

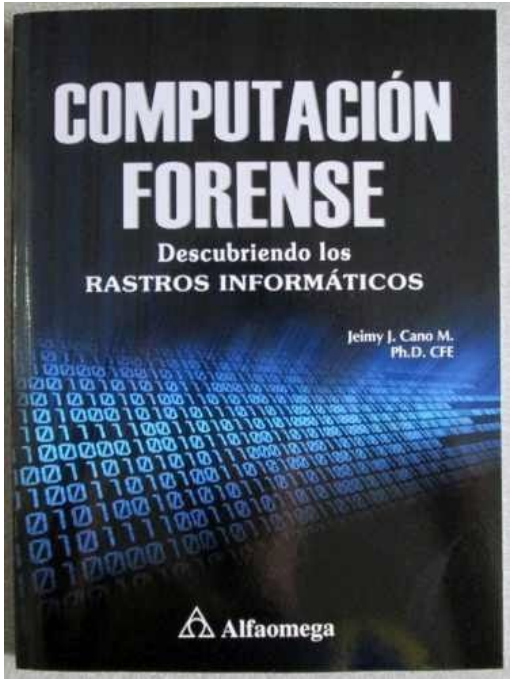


Es el proceso de identificar, preservar, analizar y presentar evidencia digital de manera tal que sea legalmente aceptable.

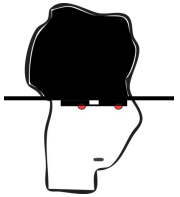
Rodney McKemmish,1999

OBJETIVO: Producir evidencia legal

Jeimy Cano



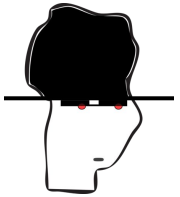
Principio de intercambio de Locard



"...siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto"

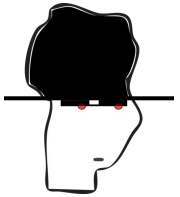
Rodney McKemmish,1999

Cybercrime



- Incluye crimen sobre internet
- Complementa el término “Computer Crime”

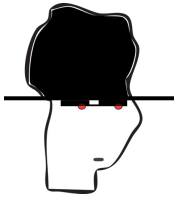
Tipos de Investigación



- PÚBLICAS
  - Contextualizadas en casos Criminales
  - Llevadas a cabo por agentes de la ley
  - Conducidas por estatutos en ley criminal (Robo, narcotráfico, explotación sexual, ...)

- PRIVADAS
  - Contextualizadas en casos internos
  - Llevadas a cabo por organizaciones o empresas
  - Conducidas por estatutos civiles o políticas organizacionales (sabotaje , malversación de fondos, espionaje industrial)

Algunas Tools

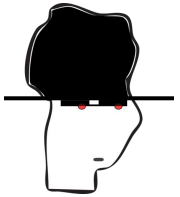


- Autopsy
- Ghex, HxD, HexWorkshop(comercial)
- FTK imager
- Volatility
- dcfldd
- OpenStego / Stegonline

IDENTIFICAR, PRESERVAR, ANALIZAR y PRESENTAR

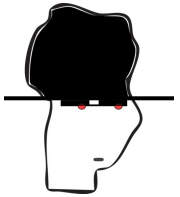
Steganography

Anti-forensia



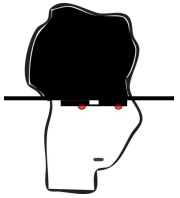
- Encryption
- Deletion (data or metadata)
- Steganography
- Unreachable places

Volatility (ejemplo)



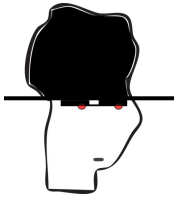
- Volatility introduced people to the power of analyzing the runtime state of a system using the data found in volatile storage (RAM).
- It also provided a cross-platform, modular, and extensible platform to encourage further work into this exciting area of research.

Volatility (ejemplo)



```
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win200
8R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7S
P1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/joe/Seg/Forensia/Otterc
tf/OtterCTF.vmem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002c430a0L
          Number of Processors : 2
```

Volatility (CheetSheet)



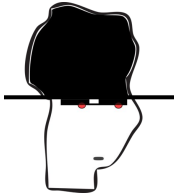
```
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem kdbgscan
Volatility Foundation Volatility Framework 2.6
**************************************************
Instantiating KDBG using: /home/joe/Seg/Forensia/Otterctf/OtterCTF.vmem WinXPSP2
x86 (5.1.0 32bit)
Offset (P)                    : 0x2c430a0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x64
PsActiveProcessHead           : 0x2c79b90
PsLoadedModuleList            : 0x2c97e90
KernelBase                    : 0xfffff80002a52000

**************************************************
Instantiating KDBG using: /home/joe/Seg/Forensia/Otterctf/OtterCTF.vmem WinXPSP2
x86 (5.1.0 32bit)
Offset (P)                    : 0x2c430a0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win2008R2SP1x64_24000
PsActiveProcessHead           : 0x2c79b90
PsLoadedModuleList            : 0x2c97e90
KernelBase                    : 0xfffff80002a52000
```

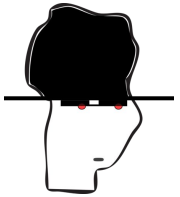
Volatility

```
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----

No suitable address space mapping found
Tried to open image as:
 MachOAddressSpace: mac: need base
 LimeAddressSpace: lime: need base
 WindowsHiberFileSpace32: No base Address Space
 WindowsCrashDumpSpace64BitMap: No base Address Space
 VMWareMetaAddressSpace: No base Address Space
 WindowsCrashDumpSpace64: No base Address Space
 HPAKAddressSpace: No base Address Space
 VirtualBoxCoreDumpElf64: No base Address Space
 VMWareAddressSpace: No base Address Space
 QemuCoreDumpElf: No base Address Space
 WindowsCrashDumpSpace32: No base Address Space
 SkipDuplicatesAMD64PagedMemory: No base Address Space
 WindowsAMD64PagedMemory: No base Address Space
 LinuxAMD64PagedMemory: No base Address Space
 AMD64PagedMemory: No base Address Space
 IA32PagedMemoryPae: No base Address Space
 IA32PagedMemory: No base Address Space
 OSXPmemELF: No base Address Space
 MachOAddressSpace: MachO Header signature invalid
 LimeAddressSpace: Invalid Lime header signature
 WindowsHiberFileSpace32: No xpress signature found
 WindowsCrashDumpSpace64BitMap: Header signature invalid
 VMWareMetaAddressSpace: VMware metadata file is not available
 WindowsCrashDumpSpace64: Header signature invalid
 HPAKAddressSpace: Invalid magic found
 VirtualBoxCoreDumpElf64: ELF Header signature invalid
```



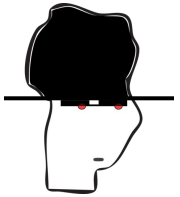
Volatility



```
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Rick:1000:aad3b435b51404eeaad3b435b51404ee:518172d012f97d3a8fcc089615283940:::
```

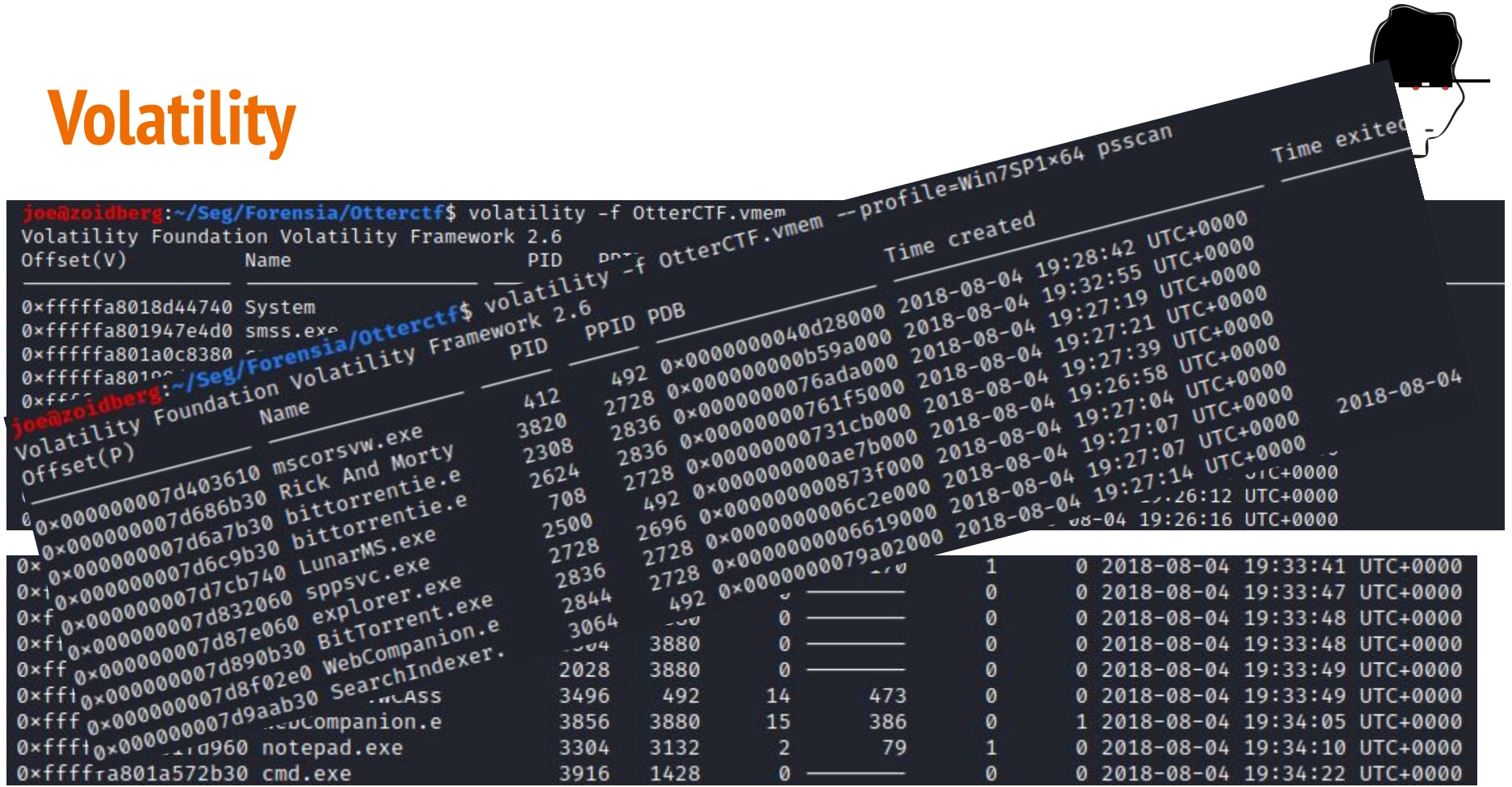
```
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x7d60f010         UDPv4    0.0.0.0:1900                   *:*                                   2836     BitTorrent.exe 2018-08-04 19:27:17 UTC+0000
0x7d62b3f0         UDPv4    192.168.202.131:6771           *:*                                   2836     BitTorrent.exe 2018-08-04 19:27:22 UTC+0000
0x7d62f4c0         UDPv4    127.0.0.1:62307                *:*                                   2836     BitTorrent.exe 2018-08-04 19:27:17 UTC+0000
0x7d62f920         UDPv4    192.168.202.131:62306          *:*                                   2836     BitTorrent.exe 2018-08-04 19:27:17 UTC+0000
0x7d6424c0         UDPv4    0.0.0.0:50762                  *:*                                   4076     chrome.exe     2018-08-04 19:33:37 UTC+0000
0x7d6b4250         UDPv6    ::1:1900                       *:*                                   164      svchost.exe    2018-08-04 19:28:42 UTC+0000
0x7d6e3230         UDPv4    127.0.0.1:6771                 *:*                                   2836     BitTorrent.exe 2018-08-04 19:27:22 UTC+0000
0x7d6ed650         UDPv4    0.0.0.0:5355                   *:*                                   620      svchost.exe    2018-08-04 19:34:22 UTC+0000
0x7d71c8a0         UDPv4    0.0.0.0:0                      *:*                                   868      svchost.exe    2018-08-04 19:34:22 UTC+0000
0x7d71c8a0         UDPv6    :::0                           *:*                                   868      svchost.exe    2018-08-04 19:34:22 UTC+0000
0x7d74a390         UDPv4    127.0.0.1:52847                *:*                                   2624     bittorrentie.e 2018-08-04 19:27:24 UTC+0000
0x7d7602c0         UDPv4    127.0.0.1:52846                *:*                                   2308     bittorrentie.e 2018-08-04 19:27:24 UTC+0000
0x7d787010         UDPv4    0.0.0.0:65452                  *:*                                   4076     chrome.exe     2018-08-04 19:33:42 UTC+0000
0x7d789b50         UDPv4    0.0.0.0:50523                  *:*                                   620      svchost.exe    2018-08-04 19:34:22 UTC+0000
```

Volatility? uh - oh

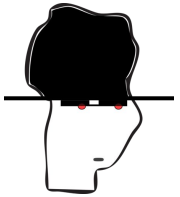


```
joe@zoidberg:~/Seg/Forensia/Otterctf$ strings OtterCTF.vmem | grep COMPUTERNAME | head
COMPUTERNAME=WIN-LO6FAF3DTFE
COMPUTERNAME=WIN-LO6FAF3DTFE
COMPUTERNAME=WIN-LO6FAF3DTFE
COMPUTERNAME=WIN-LO6FAF
COMPUTERNAME=WIN-LO6FAF3DTFE
COMPUTERNAME=WIN-LO6FAF3DTFE
COMPUTERNAME=WIN-LO6FAF3DTFE
COMPUTERNAME=WIN-LO6FAF3DTFE
COMPUTERNAME=WIN-LO6FAF3DTFE
COMPUTERNAME=WIN-LO6FAF3DTFE
```

Volatility


joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID
0xfffffa8018d44740 System
0xfffffa801947e4d0 smss.exe
0xfffffa801a0c8380
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P) Name PID PPID PDB Time created Time exited
0x000000007d403610 mscorsvw.exe 412 492 0x000000040d28000 2018-08-04 19:28:42 UTC+0000
0x000000007d686b30 Rick And Morty 3820 2728 0x000000000b59a000 2018-08-04 19:32:55 UTC+0000
0x000000007d6a7b30 bittorrentie.e 2308 2836 0x000000076ada000 2018-08-04 19:27:19 UTC+0000
0x000000007d6c9b30 bittorrentie.e 2624 2836 0x000000761f5000 2018-08-04 19:27:21 UTC+0000
0x000000007d7cb740 LunarMS.exe 708 2728 0x000000731cb000 2018-08-04 19:27:39 UTC+0000
0x000000007d832060 sppsvc.exe 2500 492 0x000000ae7b000 2018-08-04 19:26:58 UTC+0000
0x000000007d87e060 explorer.exe 2728 2696 0x000000873f000 2018-08-04 19:27:04 UTC+0000
0x000000007d890b30 BitTorrent.exe 2836 2728 0x000006c2e000 2018-08-04 19:27:07 UTC+0000
0x000000007d8f02e0 WebCompanion.e 2844 2728 0x000619000 2018-08-04 19:27:07 UTC+0000
0x000000007d9aab30 SearchIndexer. 3064 492 0x079a02000 2018-08-04 19:27:14 UTC+0000
0x000000007d9d960 notepad.exe 3304 3132 2 79 1 0 2018-08-04 19:34:10 UTC+0000
0xfffffa801a572b30 cmd.exe 3916 1428 0 ---------- 0 0 2018-08-04 19:34:22 UTC+0000

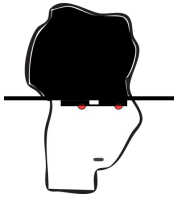
Volatility



```
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem --profile=Win7SP1x64 memdump -D outs/  -p 3304
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing notepad.exe [  3304] to 3304.dmp
joe@zoidberg:~/Seg/Forensia/Otterctf$ ls outs/
3304.dmp  708.dmp
joe@zoidberg:~/Seg/Forensia/Otterctf$ file  outs/3304.dmp
outs/3304.dmp: data
```

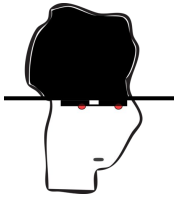
```
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem --profile=Win7SP1x64 clipboard
Volatility Foundation Volatility Framework 2.6
Session    WindowStation Format                         Handle Object             Data
---------- ------------- ------------------ ---------------- ------------------ ----------------
         1 WinSta0       CF_UNICODETEXT             0x602e3 0xfffff900c1ad93f0 M@il_Pr0vid0rs
         1 WinSta0       CF_TEXT                       0x10 ------------------
         1 WinSta0       0x150133L          0x200000000000 ------------------
         1 WinSta0       CF_TEXT                        0x1 ------------------
         1 ------------- ------------------         0x150133 0xfffff900c1c1adc0
```

Volatility



```
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem --profile=Win7SP1x64 filescan | head -20
Volatility Foundation Volatility Framework 2.6
Offset(P)          #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----
0x0000000005def290      6      0 RW-rwd \Device\HarddiskVolume1\$Directory
0x0000000005df67f0      1      1 R--rw- \Device\HarddiskVolume1\Windows\System32
0x000000007d402680     14      0 R--r-d \Device\HarddiskVolume1\Nexon\MapleStory\l3codeca.acm
0x000000007d405270      1      1 R--r-- \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\dlimag
0x000000007d405d20      1      0 R--r-- \Device\HarddiskVolume1\Windows\System32\config\systemprofile\AppDat
E20E6ACF6CACA76D5C942_4D9486FF3A1DA70CF6B67432FCEC9330
0x000000007d406510     16      0 R--r-d \Device\HarddiskVolume1\Windows\assembly\NativeImages_v2.0.50727_32\
cs.ni.dll
0x000000007d413930      1      0 R--r-- \Device\HarddiskVolume1\Windows\Microsoft.NET\Framework64\v2.0.50727
0x000000007d414dc0      1      1 R--r-d \Device\HarddiskVolume1\Windows\System32\en-US\setupapi.dll.mui
0x000000007d418290     16      0 RWDr-- \Device\HarddiskVolume1\Windows\System32\Tasks\Microsoft\Windows Def
0x000000007d418f20      9      0 R--r-d \Device\HarddiskVolume1\Windows\SysWOW64\dinput8.dll
0x000000007d42b7b0      1      1 ------ \Device\Afd\Endpoint
0x000000007d42c5b0     12      0 R--r-d \Device\HarddiskVolume1\Windows\SysWOW64\hid.dll
0x000000007d42d070      7      0 R--r-d \Device\HarddiskVolume1\Windows\AppPatch\AcLayers.dll
```

Volatility

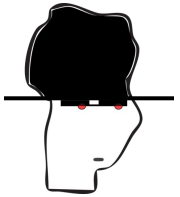


```
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem --profile=Win7SP1x64 filescan | grep download.exe
Volatility Foundation Volatility Framework 2.6
0x000000007d63dbc0     10      0 R--r-d \Device\HarddiskVolume1\Torrents\Rick And Morty season 1 download.exe
0x000000007d8813c0      2      0 RW-rwd \Device\HarddiskVolume1\Users\Rick\Downloads\Rick And Morty season 1 download.exe.torrent
0x000000007da56240      2      0 RW-rwd \Device\HarddiskVolume1\Torrents\Rick And Morty season 1 download.exe
```

```
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem --profile=Win7SP1x64 filescan | grep txt
Volatility Foundation Volatility Framework 2.6
0x000000007d61b070     16      0 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\Microsoft\Windows\Recent\Flag.txt.WINDOWS.lnk
0x000000007d660500      2      0 -W-r-- \Device\HarddiskVolume1\Users\Rick\Desktop\READ_IT.txt
0x000000007d7272a0      3      0 R--r-- \Device\HarddiskVolume1\ProgramData\Lavasoft\Web Companion\Options\partner.txt
0x000000007d731900      2      0 -W-r-- \Device\HarddiskVolume1\ProgramData\Lavasoft\Web Companion\Options\LatestReleaseNotes.txt
0x000000007d7faf20      2      0 -W---- \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\Microsoft\Windows\Cookies\rick@localhost[2].txt
0x000000007dbd6550      1      1 -W-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Temp\FXSAPIDebugLogFile.txt
0x000000007dc895b0     34      2 -W-rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware VGAuth\logfile.txt.0
0x000000007dd45070      2      0 R--r-- \Device\HarddiskVolume1\ProgramData\Lavasoft\Web Companion\Options\UpgradeAttemptInfo.txt
0x000000007e410890     16      0 R--r-- \Device\HarddiskVolume1\Users\Rick\Desktop\Flag.txt
```

```
joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007e410890 --name -D dumpfiles/
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7e410890   None   \Device\HarddiskVolume1\Users\Rick\Desktop\Flag.txt
```

Volatility



```
Process: WebCompanion.e Pid: 3856 Address: 0x4990000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 27, PrivateMemory: 1, Protection: 6

0x04990000  13 e6 17 8b 1b 43 00 01 ee ff ee ff 00 00 00 00   .....C..........
0x04990010  a8 00 99 04 a8 00 99 04 00 00 99 04 00 00 99 04   ................
0x04990020  40 00 00 00 88 05 99 04 00 00 9d 04 25 00 00 00   @...........%...
0x04990030  01 00 00 00 00 00 00 00 f0 af 9a 04 f0 af 9a 04   ................

0x04990000 13e6             ADC ESP, ESI
0x04990002 17               POP SS
0x04990003 8b1b             MOV EBX, [EBX]
0x04990005 43               INC EBX
0x04990006 0001             ADD [ECX], AL
0x04990008 ee               OUT DX, AL
0x04990009 ff               DB 0xff
0x0499000a ee               OUT DX, AL
0x0499000b ff00             INC DWORD [EAX]
0x0499000d 0000             ADD [EAX], AL
0x0499000f 00a8009904a8     ADD [EAX-0x57fb6700], CH
0x04990015 009904000099     ADD [ECX-0x66fffffc], BL
0x0499001b 0400             ADD AL, 0x0
0x0499001d 009904400000     ADD [ECX+0x4004], BL
0x04990023 008805990400     ADD [EAX+0x49905], CL
0x04990029 009d04250000     ADD [EBP+0x2504], BL
0x0499002f 0001             ADD [ECX], AL
0x04990031 0000             ADD [EAX], AL
0x04990033 0000             ADD [EAX], AL
0x04990035 0000             ADD [EAX], AL
0x04990037 00f0             ADD AL, DH
0x04990039 af               SCASD
0x0499003a 9a               DB 0x9a
0x0499003b 04f0             ADD AL, 0xf0
0x0499003d af               SCASD
0x0499003e 9a               DB 0x9a
0x0499003f 04               DB 0x4

joe@zoidberg:~/Seg/Forensia/Otterctf$ volatility -f OtterCTF.vmem --profile=Win7SP1x64 malfind > malfind
```

Open Source

Extensible

Maduro (v1.0 a 2001)

Multiplataforma

Multiusuario

Key Features

- Simple Windows installation
- Automated, intuitive workflow
- Supports hard drives and smartphones
- Extracts artifacts from web browsers
- MD5 hash lookup
- Indexed keyword search
- Deleted file carving
- EXIF data extraction from JPEG images
- Timeline analysis for all events
- Standard Android database parsing
- Extension mismatch detection
- Image gallery for picture review
- Email message extraction
- Network-based collaboration

Autopsy

Sistemas de archivos

Imágenes forenses

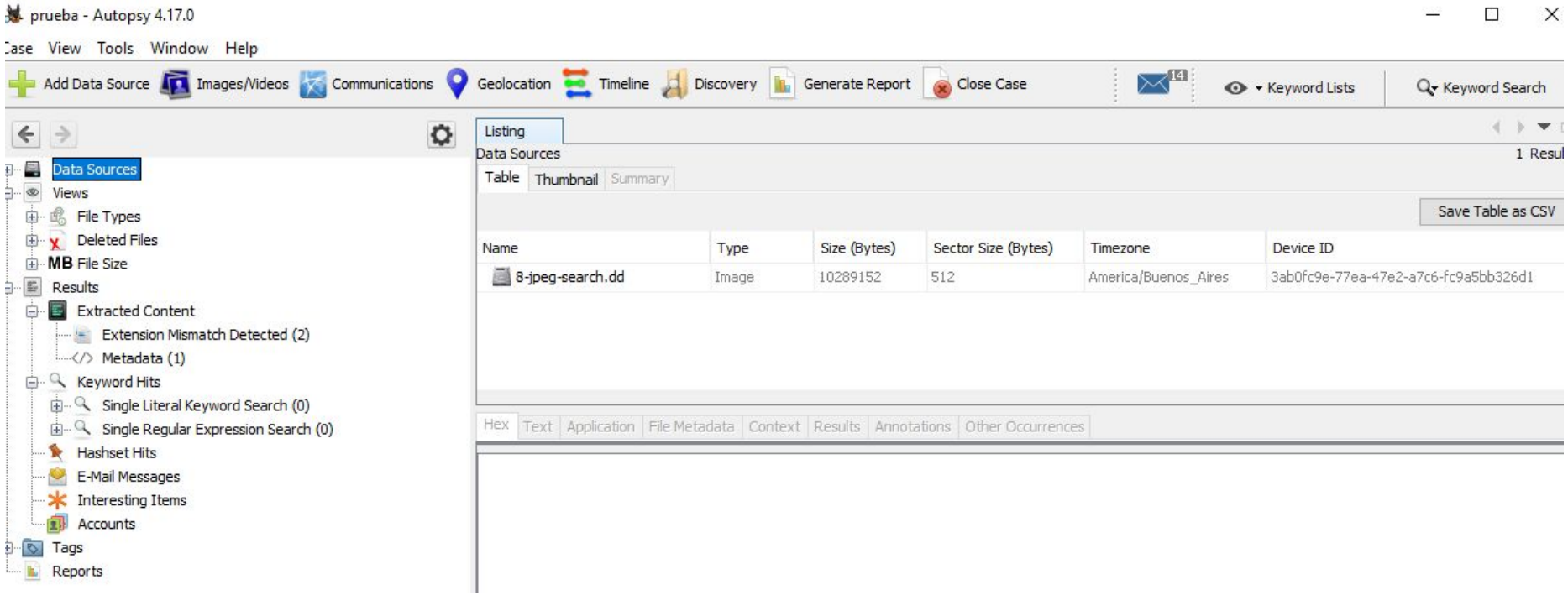
Archivos comprimidos

Carving

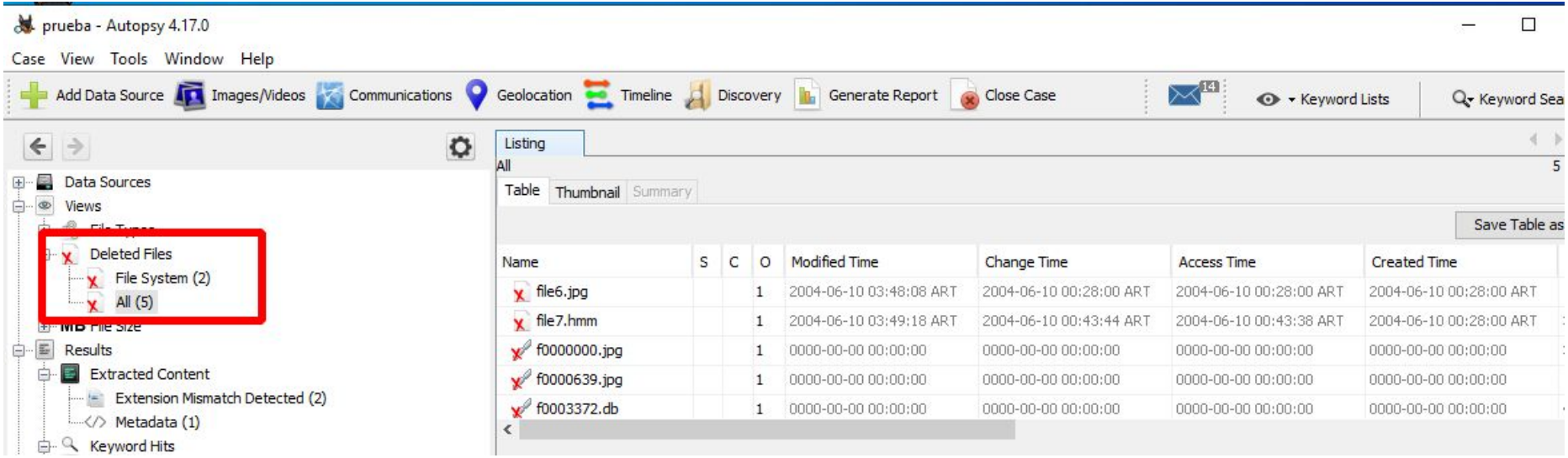
Máquinas virtuales

- Crear un nuevo caso
- Ingresar datos básicos
    - Agregar evidencia
        - Dispositivo
        - Imagen forense
        - Otros

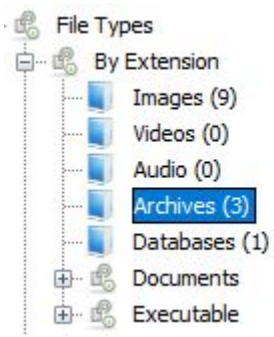
Autopsy

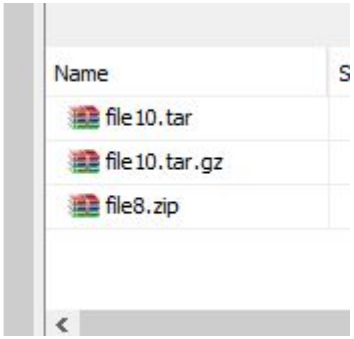

prueba - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
14
Keyword Lists
Keyword Search
Data Sources
Views
File Types
Deleted Files
MB File Size
Results
Extracted Content
Extension Mismatch Detected (2)
Metadata (1)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
Data Sources
1 Resul
Table
Thumbnail
Summary
Save Table as CSV
Name
Type
Size (Bytes)
Sector Size (Bytes)
Timezone
Device ID
8-jpeg-search.dd
Image
10289152
512
America/Buenos_Aires
3ab0fc9e-77ea-47e2-a7c6-fc9a5bb326d1
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences

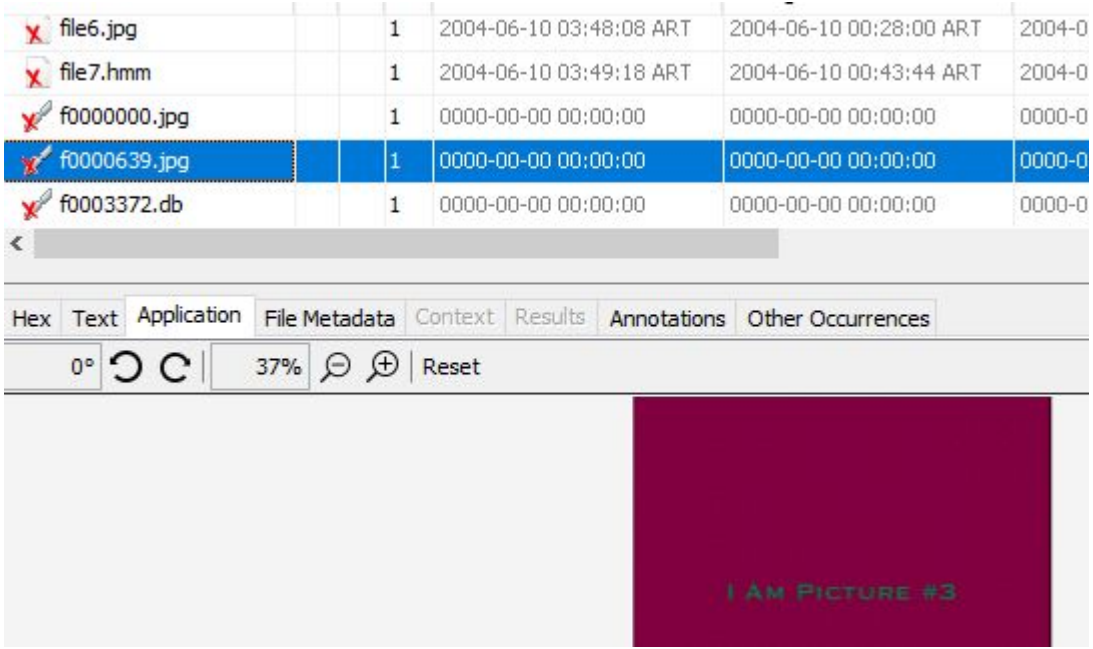
Autopsy


prueba - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Data Sources
Views
Deleted Files
File System (2)
All (5)
Results
Extracted Content
Extension Mismatch Detected (2)
Metadata (1)
Keyword Hits
Listing
All
5
Table
Thumbnail
Summary
Save Table as
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
file6.jpg
1
2004-06-10 03:48:08 ART
2004-06-10 00:28:00 ART
2004-06-10 00:28:00 ART
2004-06-10 00:28:00 ART
file7.hmm
1
2004-06-10 03:49:18 ART
2004-06-10 00:43:44 ART
2004-06-10 00:43:38 ART
2004-06-10 00:28:00 ART
f0000000.jpg
1
0000-00-00 00:00:00
0000-00-00 00:00:00
0000-00-00 00:00:00
0000-00-00 00:00:00
f0000639.jpg
1
0000-00-00 00:00:00
0000-00-00 00:00:00
0000-00-00 00:00:00
0000-00-00 00:00:00
f0003372.db
1
0000-00-00 00:00:00
0000-00-00 00:00:00
0000-00-00 00:00:00
0000-00-00 00:00:00

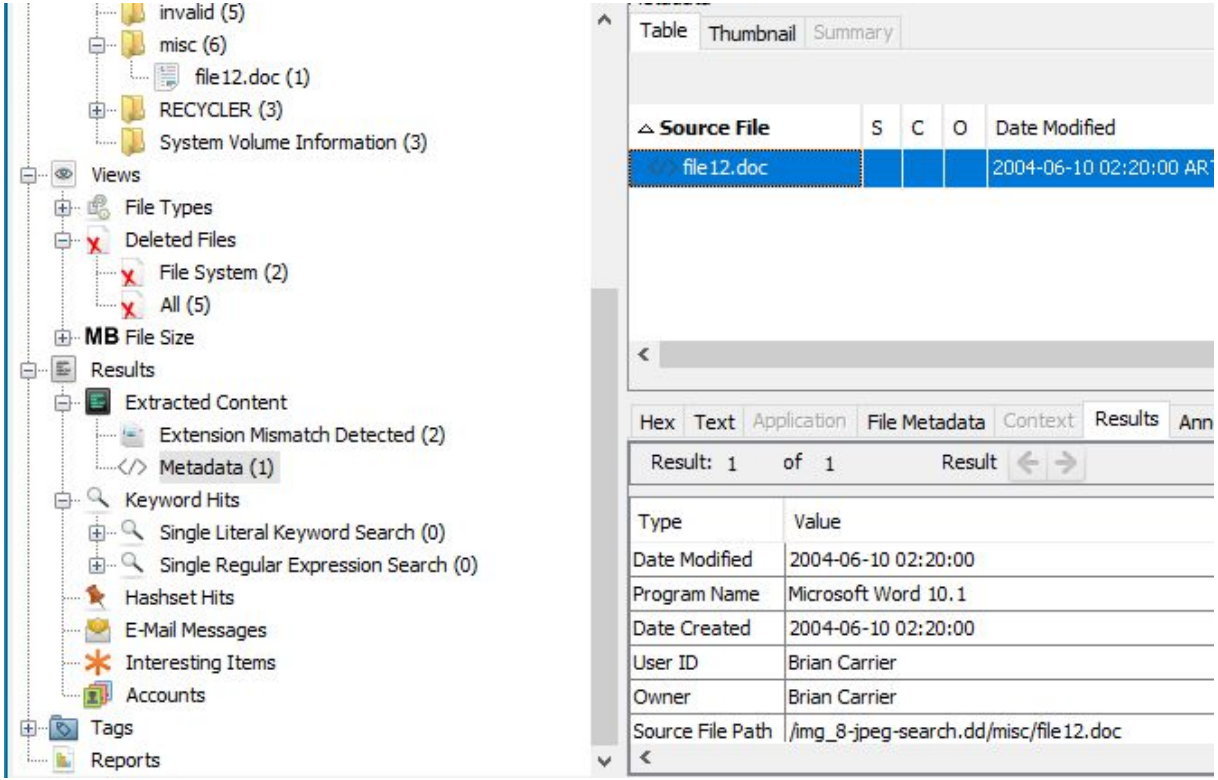
Autopsy


File Types
By Extension
Images (9)
Videos (0)
Audio (0)
Archives (3)
Databases (1)
Documents
Executable


Name
file10.tar
file10.tar.gz
file8.zip


file6.jpg 1 2004-06-10 03:48:08 ART 2004-06-10 00:28:00 ART 2004-0
file7.hmm 1 2004-06-10 03:49:18 ART 2004-06-10 00:43:44 ART 2004-0
f0000000.jpg 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-0
f0000639.jpg 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-0
f0003372.db 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-0
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
0°
37%
Reset
I AM PICTURE #3

Autopsy


invalid (5)
misc (6)
file12.doc (1)
RECYCLER (3)
System Volume Information (3)
Views
File Types
Deleted Files
File System (2)
All (5)
MB File Size
Results
Extracted Content
Extension Mismatch Detected (2)
Metadata (1)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Table
Thumbnail
Summary
Source File
S
C
O
Date Modified
file12.doc
2004-06-10 02:20:00
Hex
Text
Application
File Metadata
Context
Results
Result: 1 of 1 Result
Type
Value
Date Modified
2004-06-10 02:20:00
Program Name
Microsoft Word 10.1
Date Created
2004-06-10 02:20:00
User ID
Brian Carrier
Owner
Brian Carrier
Source File Path
/img_8-jpeg-search.dd/misc/file12.doc

Autopsy

```
from org.sleuthkit.autopsy.report \
    import GeneralReportModuleAdapter

class NotKnownBackup(
    GeneralReportModuleAdapter):

    moduleName = "Copy Not Known Files"

    def getName(self):
        return self.moduleName

    def getDescription(self):
        return "Copy Not Known Files,”

    def getRelativeFilePath(self):
        return "hashes.csv"
```