



The OWASP Foundation

<http://www.owasp.org>

# **Análisis Forense de un Ataque Web**

**Mauricio Urizar**

**[murizar@open-sec.com](mailto:murizar@open-sec.com)**

** [@MauricioUrizar](https://twitter.com/MauricioUrizar)**



# Open-Sec

Ethical Hacking/Forensics/InfoSec



- Trabajando los últimos 07 años como parte del equipo de hacker eticos de Open-Sec.
- Instructor de cursos de Ethical Hacking en Perú y Ecuador.

**C|EH (Certified | Ethical Hacker)**

**CEI (Certified EC-Council Instructor)**

**CPTE (Certified Penetration Tester)**

**CPTE Mile2 - Authorized Instructor**

**OSEH (Open-Sec Ethical Hacker)**

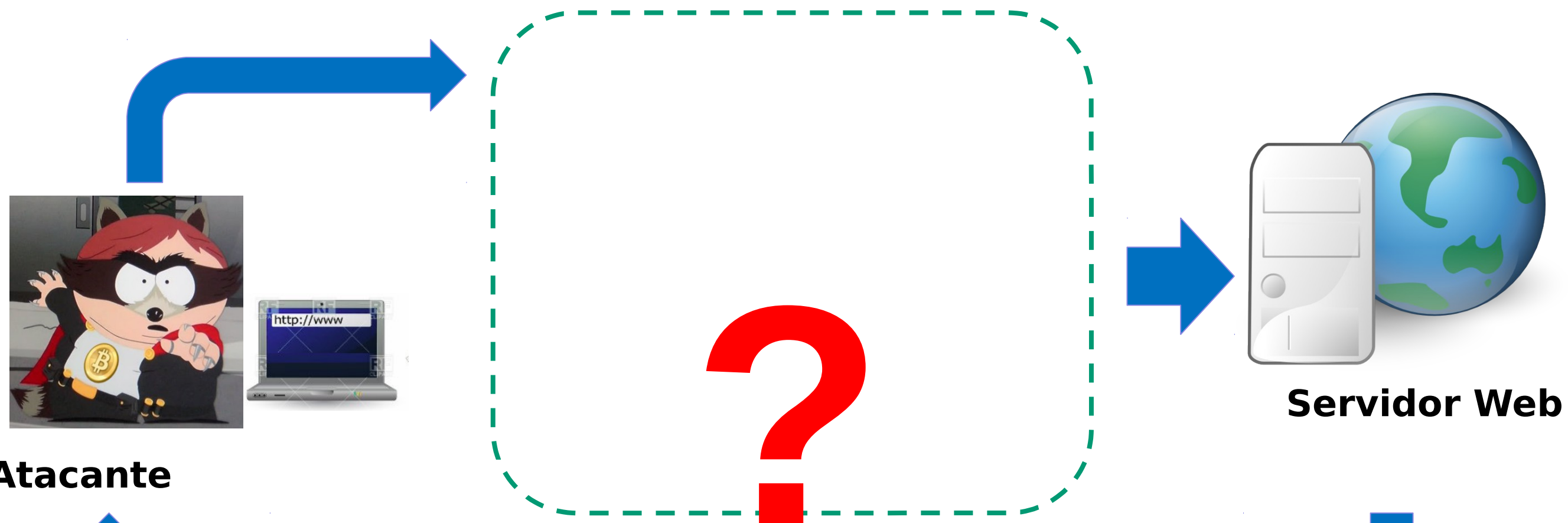


# DESCARGO DE RESPONSABILIDADES

- ▮ Esta presentación tiene como propósito proveer únicamente información. No aplicar este material ni conocimientos sin el consentimiento explícito que autorice a hacerlo. Los lectores (participantes, oyentes, videntes) asumen la responsabilidad completa por la aplicación o experimentación de este material y/o conocimientos presentados. El(los) autor(es) quedan exceptuados de cualquier reclamo directo o indirecto respecto a daños que puedan haber sido causados por la aplicación de este material y/o conocimientos expuestos.
- ▮ La información aquí expuesta representa las opiniones y perspectivas propias del autor respecto a la materia y no representan ninguna posición oficial de alguna organización asociada.



# Escenario



Atacante

Servidor Web

Card Type	Card Number	Issue	CV2	Address	PostCode
Visa (VISA)	49290000000006		123	88	412
MasterCard (MC)	5404000000000001		123	88	412
Visa Debit / Delta (DELTA)	4462000000000003		123	88	412
Solo (SOLO)	6334900000000005	1	123	88	412
UK Maestro / International Maestro (MAESTRO)	5641820000000005	01	123	88	412
American Express (AMEX)	3000000000000004	N/A	123	88	412
Visa Electron (UKE)	3742000000000004		123	88	412
JCB (JCB)	4917300000000008		123	88	412
Diner's Club (DINERS)	3569990000000009		123	88	412
Laser (LASER)	3600000000000008		123	88	412
	63049900000000044		123	88	412







# Que buscamos..

## En busca de respuestas...

- ¿ Qué sucedió ?
- ¿ Donde ?
- ¿ Cuándo ?
- ¿ Por qué ?
- ¿ Quién ?
- ¿ Cómo ?





# Investigación Forense



**Investigación sobre un acontecimiento del pasado con el fin de determinar las posibles causas y responsables de dicho acontecimiento.**





# Definición de la Metodología

[http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usab5601.pdf](http://www.justice.gov/usao/eousa/foia_reading_room/usab5601.pdf)

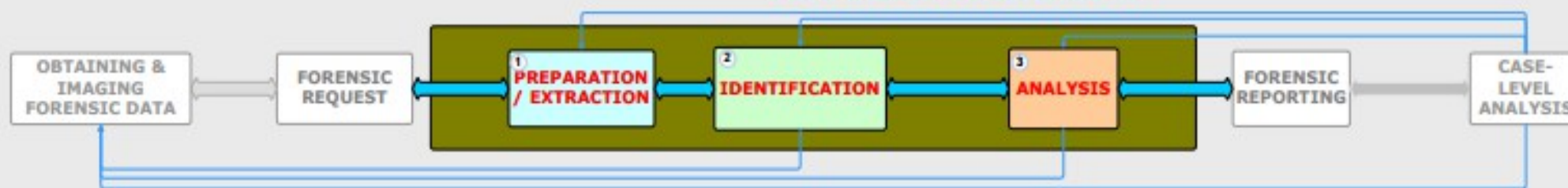


## DIGITAL FORENSIC ANALYSIS METHODOLOGY

Last Updated: August 22, 2007



### PROCESS OVERVIEW



### LISTS

Search Leads	Comments/Notes/Messages
<b>Data Search Leads</b> Generally, this involves opening a case file in the tool of choice and importing forensic image files. This could also include recreating a network environment or database to mimic the original environment.  <b>Sample Data Search Leads:</b> <ul style="list-style-type: none"><li>Identify and extract all email and deleted items.</li><li>Search media for evidence of child pornography.</li><li>Configure and load second database for data mining.</li><li>Recover all deleted files and index drive for review by case agent/forensic examiner.</li></ul>	<b>Comments/Notes/Messages</b> Use this section as needed.  <b>Sample Notes:</b> <ul style="list-style-type: none"><li>Please notify case agent when forensic data preparation is completed.</li></ul>

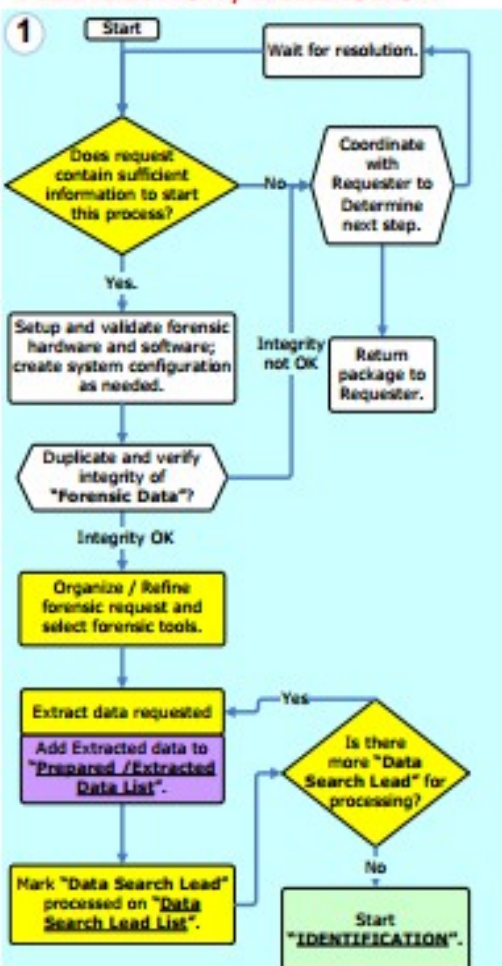
Extracted Data	Comments/Notes/Messages
<b>Prepared / Extracted Data</b> Prepared / Extracted Data List is a list of items that are prepared or extracted to allow identification of data pertaining to the forensic request.  <b>Sample Prepared / Extracted Data Items:</b> <ul style="list-style-type: none"><li>Processed hard drive image using Encase or FTK to allow a case agent to image the contents.</li><li>Exported registry files and included registry viewer to allow a forensic examiner to examine registry entries. A second database file is loaded on a database server ready for data mining.</li></ul>	<b>Comments/Notes/Messages</b> Use this section as needed.  <b>Sample Messages:</b> <ul style="list-style-type: none"><li>Enclosed files located in cyrptex directory have not been examined but are actually Root spreadsheets.</li></ul>

Relevant Data	Comments/Notes/Messages
<b>Relevant Data</b> Relevant Data List is a list of data that is relevant to the forensic request. For example: <ul style="list-style-type: none"><li>If the forensic request is finding information relating credit card fraud, any credit card number, image of credit card, receipt, discussing credit card, web tracks that show the date, time and search term used to find credit card number program, etc are Relevant Data as evidence. In addition, victim information relevant to the forensic request is also Relevant Data for purpose of victim notification.</li></ul>	<b>Comments/Notes/Messages</b> Use this section as needed.  <b>Sample Notes:</b> <ul style="list-style-type: none"><li>Attachment in Outlook and messages file is a virus in E. This is an anti-virus software is installed before reporting and scanning it.</li><li>Identified and recovered 12 records including plan to commit crime.</li></ul>

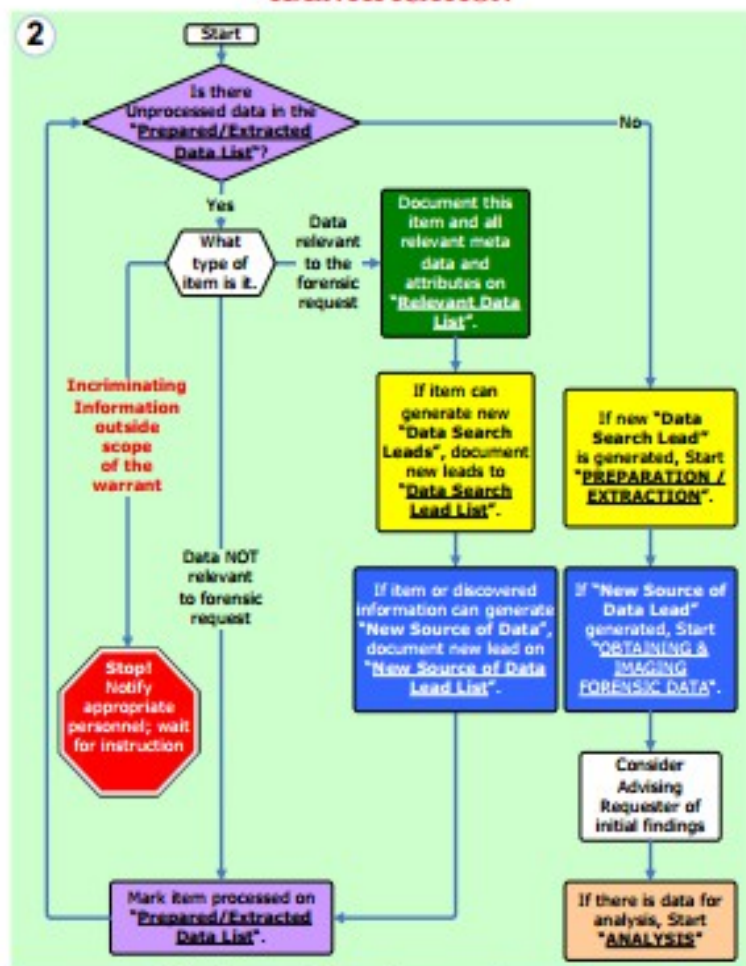
New Data Source Leads	Comments/Notes/Messages
<b>New Source of Data Leads</b> New Source of Data List is a list of data that should be obtained to corroborate or further investigative efforts.  <b>Sample New Source of Data Leads:</b> <ul style="list-style-type: none"><li>Email address: John@johnd.com.</li><li>Source from FTP server.</li><li>Subscriber information for an IP address.</li><li>Transaction logs from server.</li></ul>	<b>Comments/Notes/Messages</b> This is not necessary. Use this section as needed.  <b>Sample Notes:</b> <ul style="list-style-type: none"><li>During forensic analysis of subject John Doe's hard drive image on credit card fraud, a email message revealed that John Doe adds John Doe for payment and credit card pending machine.</li></ul>

Analysis Results	Comments/Notes/Messages
<b>Analysis Results</b> Analysis Results List is a list of meaningful data that answers the who, what, when, where and how questions in satisfying the forensic request.  <b>Sample Analysis Results:</b> <ul style="list-style-type: none"><li>1. To delete messages and attachments from John Doe's hard drive image lead to find a text file image in 00444 at 11:43 PM 01/09/02 and emailed it to John Doe at 11:03 PM 01/09/02.</li></ul>	<b>Comments/Notes/Messages</b> Use this section as needed.  <b>Sample Notes:</b> <ul style="list-style-type: none"><li>1. 00444, messages and attachments from John Doe's hard drive image lead to find a text file image in 00444 at 11:43 PM 01/09/02 and emailed it to John Doe at 11:03 PM 01/09/02.</li></ul>

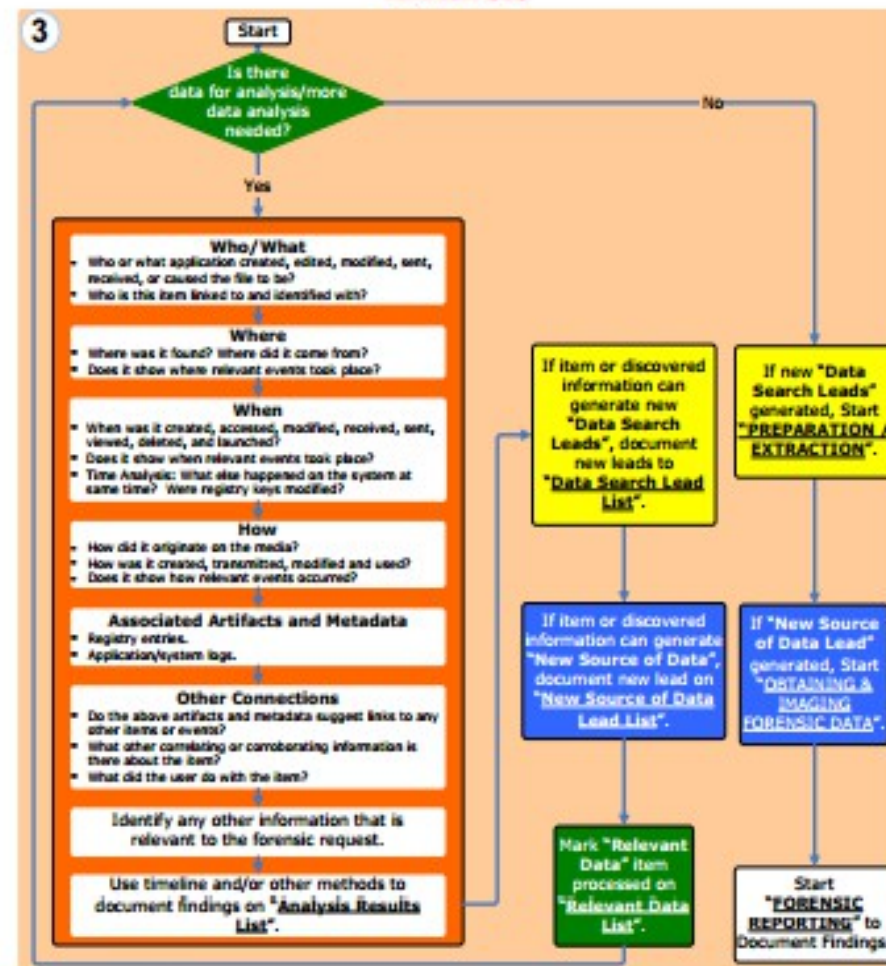
### PREPARATION / EXTRACTION



### IDENTIFICATION



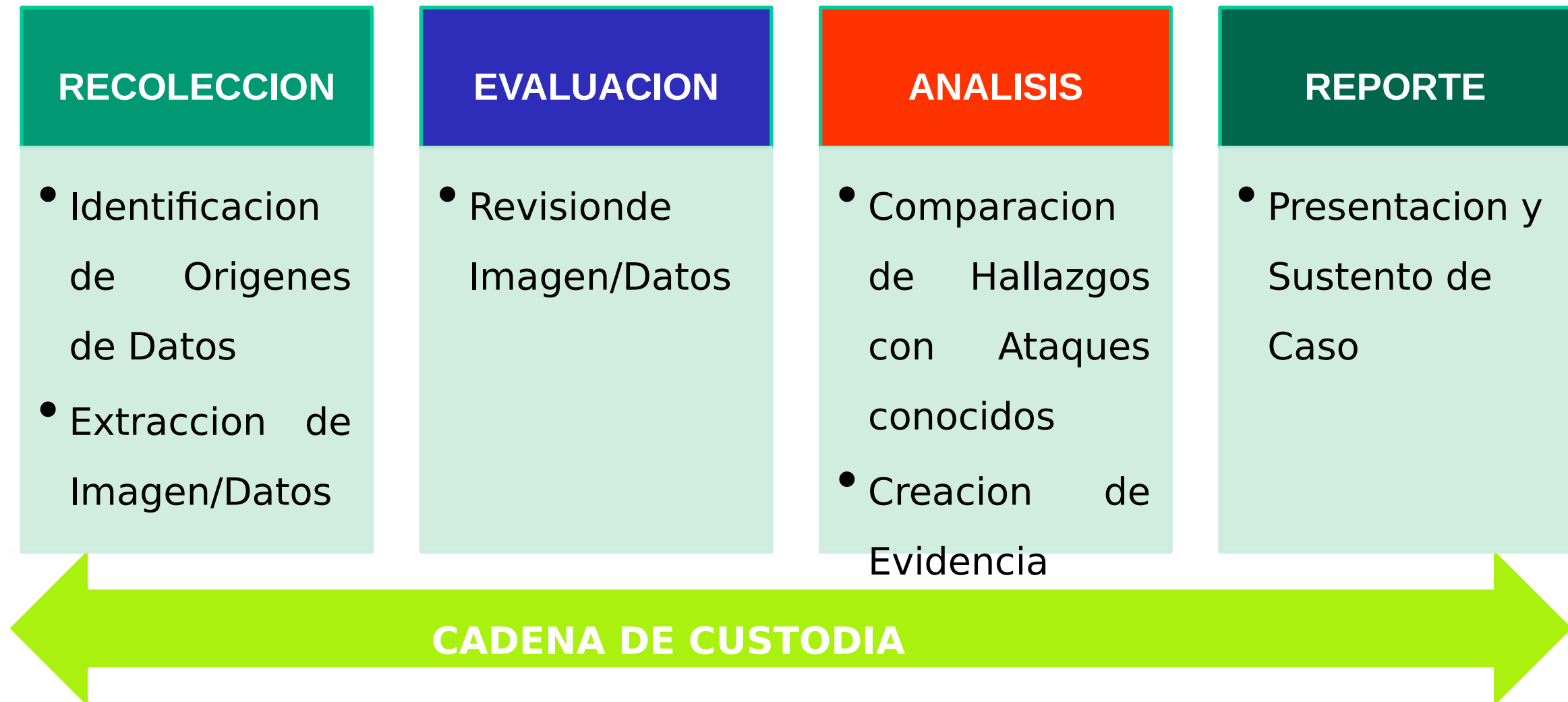
### ANALYSIS



**Return On Investment** (Determine when to stop this process. Typically, after enough evidence is obtained for prosecution, the value of additional forensic analysis diminishes.)



# Proceso Forense Tradicional

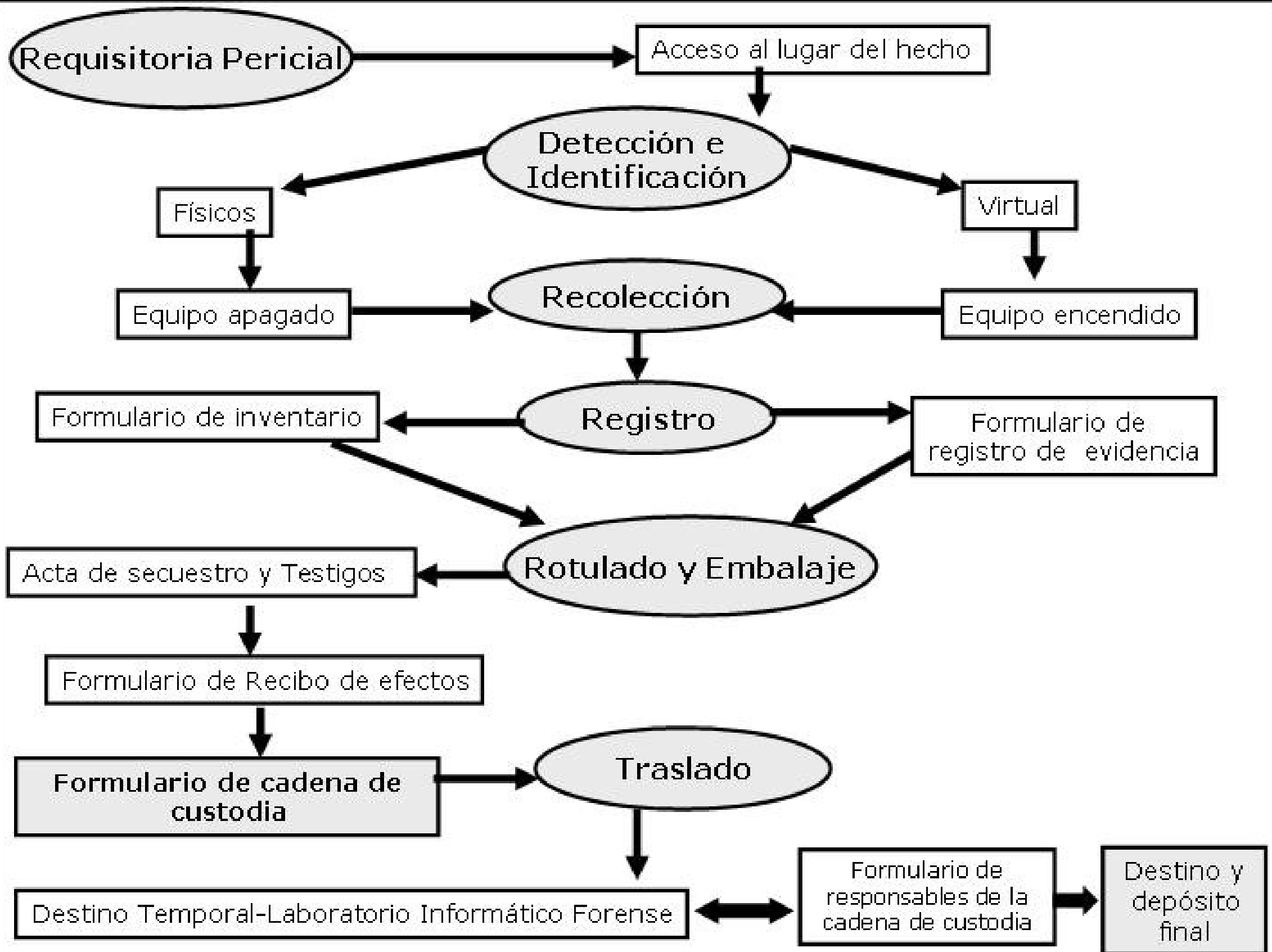


“El Proceso Forense Informático consiste en recolectar datos desde un medio para generar información que permita encontrar evidencia de un hecho en particular”





# Cadena de Custodia





# Guía de Recolección de Evidencia Digital

## (RFC3227) Order of volatility of digital evidence

- **Captura de datos volátiles**
  - ▶ **Procesos**
  - ▶ **Puertos y conexiones de red**
  - ▶ **Dumpeo de memoria**
- **Apagado del Sistema**
- **Elaboración de Imagen forense**





# Análisis Trafico de Red



## Símbolo del sistema

```
C:\Documents and Settings\Administrador>arp -a
```

```
Interfaz: 192.168.25.154 --- 0x2
Dirección IP          Dirección física      Tipo
192.168.25.2          00-50-56-f3-d1-26    dinámico
```

```
C:\Documents and Settings\Administrador>ipconfig
```

```
Configuración IP de Windows
```

```
Adaptador Ethernet Conexión de área local :

Sufijo de conexión específica DNS : localdomain
Dirección IP. . . . . : 192.168.25.154
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.25.2
```

```
C:\Documents and Settings\Administrador>arp -a
```

```
Interfaz: 192.168.25.154 --- 0x2
Dirección IP          Dirección física      Tipo
192.168.25.2          00-0c-29-c4-da-36    dinámico
192.168.25.155        00-0c-29-c4-da-36    dinámico
```

```
C:\Documents and Settings\Administrador>
```





# Análisis Trafico de Red

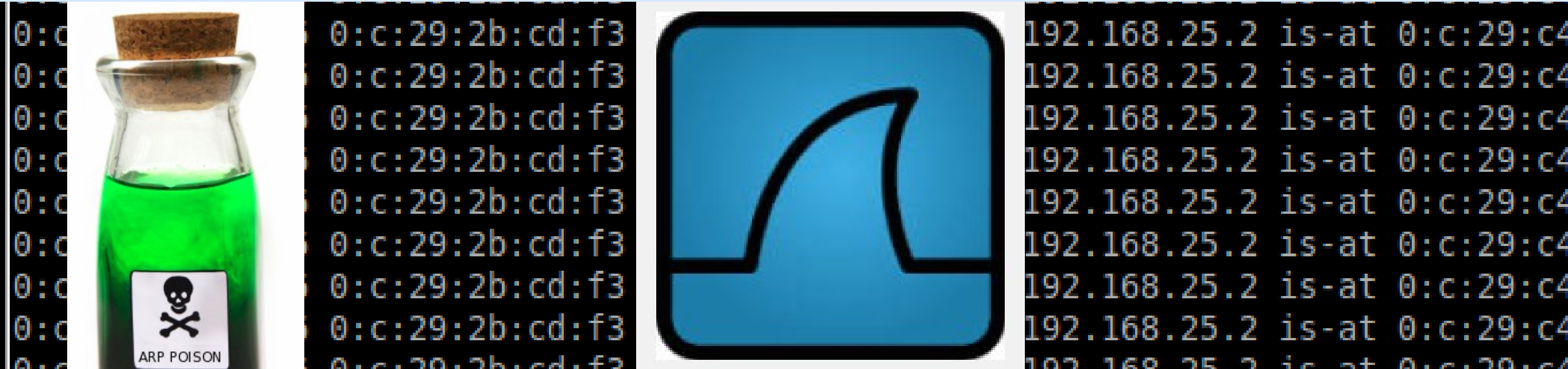
MITM\_SSLSTRIP\_CAP.pcapng [Wireshark 1.8.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help



Filter: arp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Vmware_94:ed:c3	Vmware_2b:cd:f3	ARP	60	192.168.25.2 is at 00:0c:29:9
2	2.000816000	Vmware_94:ed:c3	Vmware_2b:cd:f3	ARP	60	192.168.25.2 is at 00:0c:29:9
3	4.001671000	Vmware_94:ed:c3	Vmware_2b:cd:f3	ARP	60	192.168.25.2 is at 00:0c:29:9
4	6.002581000	Vmware_94:ed:c3	Vmware_2b:cd:f3	ARP	60	192.168.25.2 is at 00:0c:29:9
5	8.003288000	Vmware_94:ed:c3	Vmware_2b:cd:f3	ARP	60	192.168.25.2 is at 00:0c:29:9
6	10.004178000	Vmware_94:ed:c3	Vmware_2b:cd:f3	ARP	60	192.168.25.2 is at 00:0c:29:9
7	12.004987000	Vmware_94:ed:c3	Vmware_2b:cd:f3	ARP	60	192.168.25.2 is at 00:0c:29:9
8	14.005829000	Vmware_94:ed:c3	Vmware_2b:cd:f3	ARP	60	192.168.25.2 is at 00:0c:29:9
9	16.006614000	Vmware_94:ed:c3	Vmware_2b:cd:f3	ARP	60	192.168.25.2 is at 00:0c:29:9
10	18.007555000	Vmware_94:ed:c3	Vmware_2b:cd:f3	ARP	60	192.168.25.2 is at 00:0c:29:9





# Adquiriendo Evidencia Volátil

## DART2 (Digital Advanced Response Toolkit)

The screenshot shows a web browser window with the title "Package list | DEFT Linux - Computer Forensics liv". The address bar shows "www.deftlinux.net/package-list/". The website has a dark theme with the "deft" logo in a light gray font. A navigation bar contains links: Home, About », Download, Package list (highlighted), DEFT Manual, and Screenshot. The main content area displays the text "DART 2 2014 package list, in alphabetical order:" followed by a bulleted list of packages.

Package list | DEFT Linux - Computer Forensics liv

Iceweasel ▾ Package list | DEFT Linux - Co... +

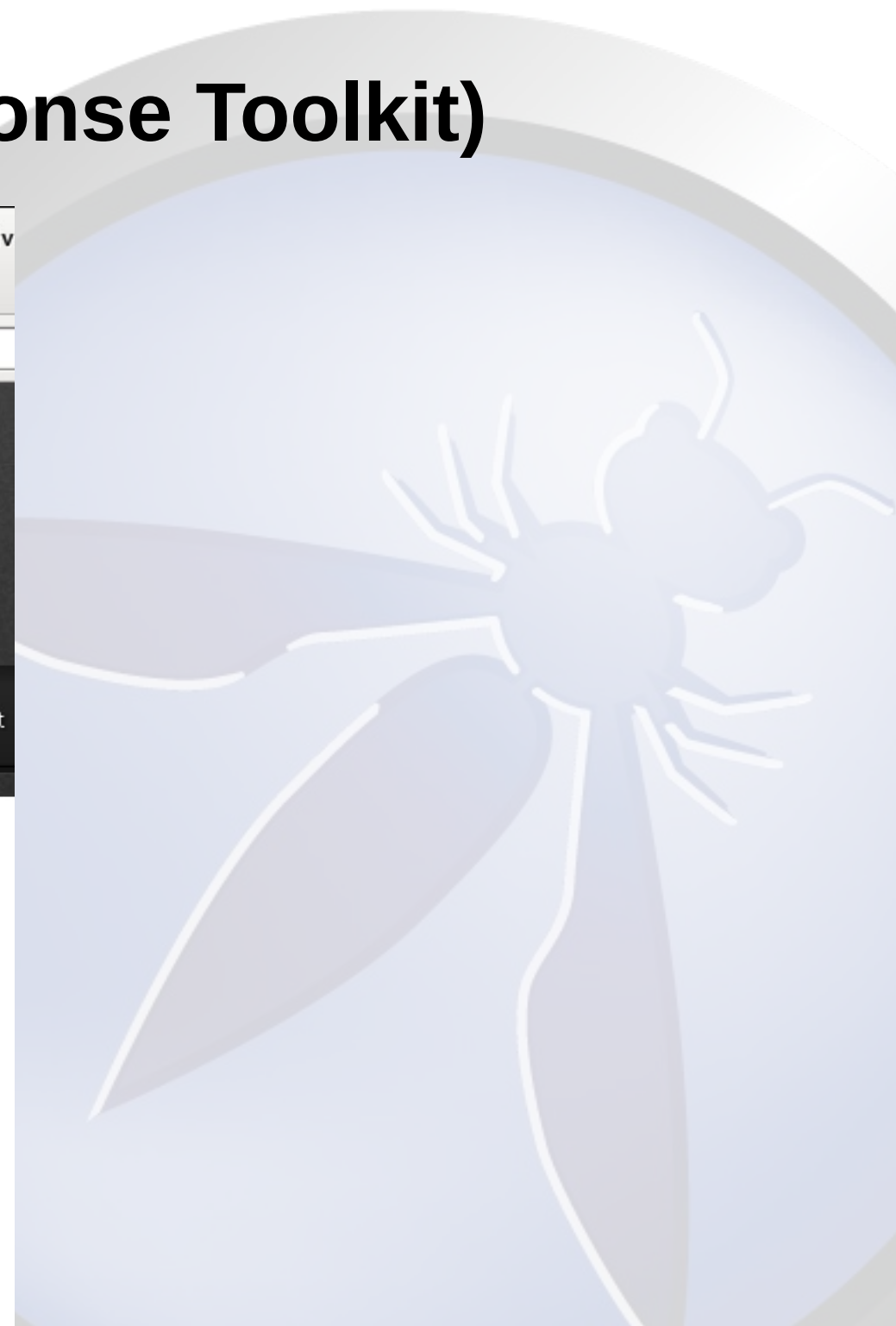
www.deftlinux.net/package-list/

deft

Home About » Download Package list DEFT Manual Screenshot

DART 2 2014 package list, in alphabetical order:


- Alert
- About
- Acquire
- Burn
- DeepBurner



# Adquiriendo Evidencia Volátil

## “tr3-collect.bat” Data Collection Script

code.google.com/p/jiir-resources/downloads/list



### jiir-resources

Journey Into Incident Response Blog Resources

[Project Home](#) **[Downloads](#)** [Wiki](#) [Issues](#) [Source](#)

Search  for

	Filename ▼	Summary + Labels
★ ↓	<a href="#">tr3_tool_kit_v2.zip</a>	tr3_data_collection
★ ↓	<a href="#">Microsoft_Office_Excel_MetaData_Changes.pdf</a>	Microsoft Office E
★ ↓	<a href="#">Microsoft_Office_Word_MetaData_Changes.pdf</a>	Microsoft Office W
★ ↓	<a href="#">general-info.bat</a>	regripper-general-os-info.bat script <b>Regripper Registry</b>
★ ↓	<a href="#">vsc-parser.zip</a>	vsc-parser <b>BatchScripting VSCs</b>

Equipo > HP16GB (E:) > Data-CASE003\_PCMURIZAR > WIN-RN58V

Organizar Compartir con Grabar Nueva carpeta

Favoritos

- Descargas
- Escritorio
- Sitios recientes

Bibliotecas

- Documentos
- Imágenes
- Música
- Videos

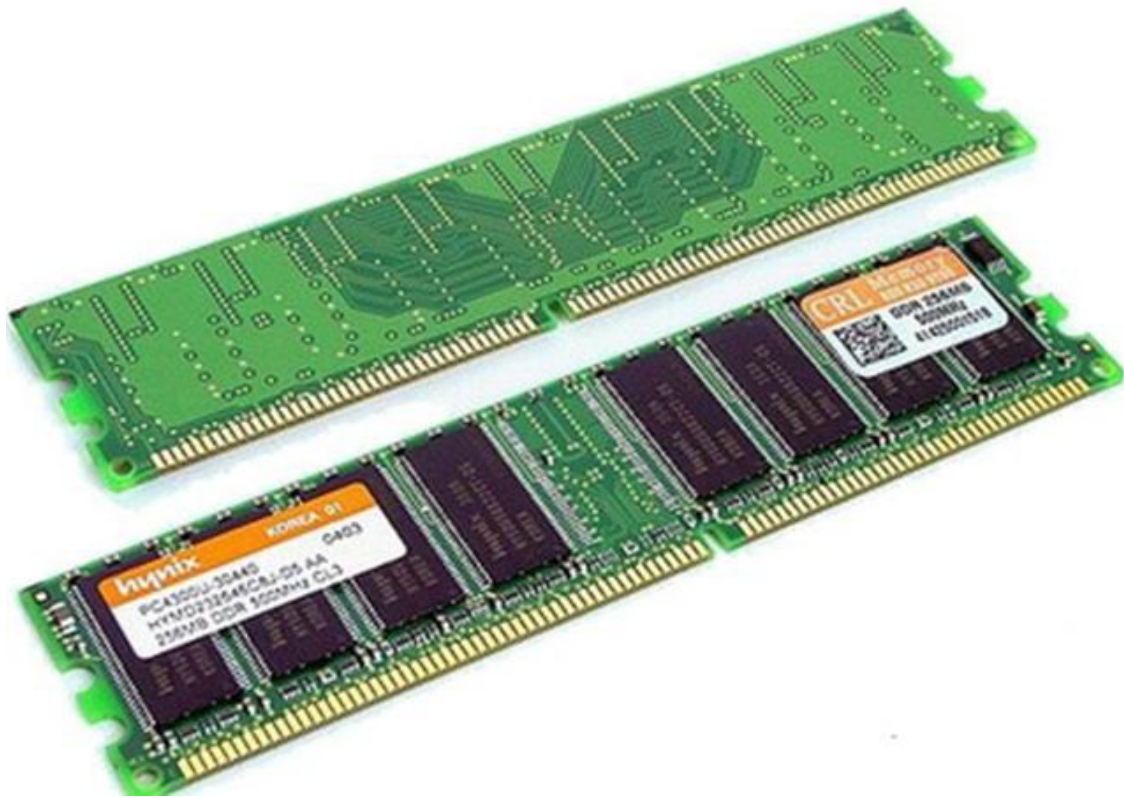
Equipo

- Disco local (C:)
- HP16GB (E:)
- Disco extraíble (F:)
- TOSHIBA EXT (G:)
- Red

Nombre	Fecha de
MiscInfo_1_clipboard-contents	24/05/2013
NetworkInfo_1_active-connections	24/05/2013
NetworkInfo_2_dns-queries-cache	24/05/2013
NetworkInfo_3_netbios-sessions	24/05/2013
NetworkInfo_4_netbios-cache	24/05/2013
NetworkInfo_5_file-transfer-over-netbios	24/05/2013
NetworkInfo_6_arp-cache	24/05/2013
NetworkInfo_7_routing-table	24/05/2013
NetworkInfo_8_port-to-process-mappin...	24/05/2013
NetworkInfo_8_port-to-process-mappin...	24/05/2013
OpenedFilesInfo_1_opened-files	24/05/2013
OpenedFilesInfo_2_remotely-opened-files	24/05/2013
ProcessInfo_1_running-processes	24/05/2013
ProcessInfo_1_running-processes-memo...	24/05/2013
ProcessInfo_2_process-to-exe-mapping	24/05/2013
ProcessInfo_3_process-to-user-mapping	24/05/2013
ProcessInfo_3_process-to-user-mapping...	24/05/2013
ProcessInfo_4_child-processes	24/05/2013
ProcessInfo_5_processe-file-handles	24/05/2013



# Adquiriendo Evidencia Volátil



Información proveniente del sistema operativo y medios de almacenamiento electrónicos que pierden los datos al ser apagados

```
Simbolo del sistema
E:\volatility\winpmem-1.4>winpmem_1.4.exe -1 image-mem-win.raw
Driver Unloaded.
Loaded Driver C:\DOCUME~1\ADMINI~1\CONFIG~1\Temp\pme23B.tmp.
Setting acquisition mode to 0
Will generate a RAW image
CR3: 0x0000331000
4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x00EFF000
Start 0x01000000 - Length 0x1EEF0000
Start 0x1FF00000 - Length 0x00100000
Padding from 0x00000000 to 0x00001000
```



# Analizando memoria RAM

## CONNSCAN

Lista conexiones de red para identificar equipos remotos conectados en el momento de la captura de la memoria RAM.

```
axon-virtual-machine ../volatility-2.3.1 % python vol.py -f /home/axon/Downloads/WINRAM
_malware01.img connsnscan
Volatility Foundation Volatility Framework 2.3.1
Offset(P)  Local Address          Remote Address          Pid
-----
0x0205ece0 192.168.157.10:1050      222.128.1.2:443        1672
0x020611f8 192.168.157.10:1053      218.85.133.23:89       796
0x032c01f8 192.168.157.10:1053      218.85.133.23:89       796
0x0337dce0 192.168.157.10:1050      222.128.1.2:443        1672
0x08a4ace0 192.168.157.10:1050      222.128.1.2:443        1672
0x18200ce0 192.168.157.10:1050      222.128.1.2:443        1672
axon-virtual-machine ../volatility-2.3.1 %
```



# Analizando memoria RAM

## DLLLIST

Lista los archivos “DLL” cargados de un proceso en particular

```
root:../volatility-2.3.1
File Edit Tabs Help
*****
iexplore.exe pid: 796
Command line : "C:\Program Files\Internet Explorer\iexplore.exe"
Service Pack 3

Base          Size  LoadCount Path
-----
0x00400000    0x9b000    0xffff C:\Program Files\Internet Explorer\iex
0x7c900000    0xaf000    0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000    0xffff C:\WINDOWS\system32\kernel32.dll
0x5d090000    0x9a000     0x1 C:\WINDOWS\system32\comctl32.dll
0x10000000    0x9000     0x1 C:\WINDOWS\system32\irykmmww.dll
0x78050000    0xd0000    0x2 C:\WINDOWS\system32\WININET.dll
```





# Analizando memoria RAM

## SCRIPT VERIFICA EN GOOGLE

```
# python check-dlls-google.py dlls.lst 0
Checking in google.com

=====
checking.....:wevtsvc.dll
checking.....:irykmmww.dll
This DLL already reported [6].....!!!!
checking.....:wiaservc.dll
checking.....:winrnr.dll
checking.....:winsatapi.dll
checking.....:wkssvc.dll
checking.....:wlansvc.dll
checking.....:wldap32.dll
```



# Analizando memoria RAM

## DLLDUMP

Extrae los DLL desde el espacio de memoria del proceso y lo descarga en el disco para el análisis.

```
axon-virtual-machine ../volatility-2.3.1 % python vol.py -f /home/axon/Downloads/WINRAM
_malware01.img dlldump --dump-dir ./dir-dump-dlls -p 796
Volatility Foundation Volatility Framework 2.3.1
```

Process(V) Name	Module Base	Module Name	Result
0x81dbdda0 iexplore.exe	0x000400000	iexplore.exe	OK: module.796.1fbdda0
.400000.dll			
0x81dbdda0 iexplore.exe	0x07c900000	ntdll.dll	OK: module.796.1fbdda0
.7c900000.dll			
0x81dbdda0 iexplore.exe	0x076b40000	WINMM.dll	OK: module.796.1fbdda0
.76b40000.dll			
0x81dbdda0 iexplore.exe	0x078130000	urlmon.dll	OK: module.796.1fbdda0
.78130000.dll			



# Analizando memoria RAM

Antivirus scan for d5dc32e16a4f36eb8de6a... 5 00:38:28 UTC - VirusTotal - Mozilla Firefox - +

File Edit View History Bookmarks Tools Help

Antivirus scan for d5dc32e16a... +

← https://www.virustotal.com/en/file/d5dc32e16a4f36eb... ☆ ↺ Google 🔍 ⬇️ 🏠 🌐

🏠 Community Statistics Documentation FAQ About English Join our community Sign in

## virustotal

SHA256: d5dc32e16a4f36eb8de6a1ebe172a05e077259c4005679cdd6af9ac14918054e

File name: module.796.1fbdda0.10000000.dll

Detection ratio: 33 / 50

Analysis date: 2014-03-05 00:38:28 UTC ( 2 months, 1 week ago )

Analysis File detail Additional information Comments 0 Votes

Antivirus	Result	Update
AVG	BackDoor.Generic17.ADXY	20140304
Ad-Aware	Gen:Trojan.Heur.LP.cu4@aOTEXGe	20140304
AhnLab-V3	Backdoor/Win32.PcClient	20140304
AntiVir	TR/Spy.Gen	20140304



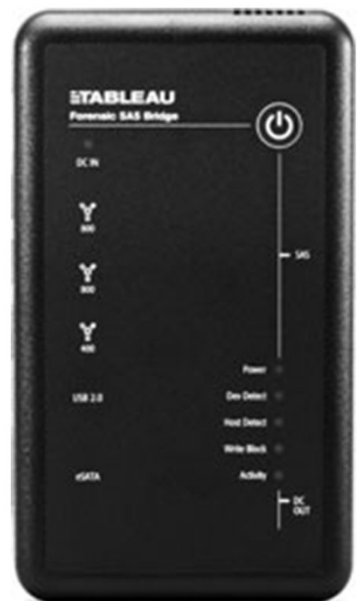
# Adquiriendo Evidencia Volátil

**Informacion proveniente de medios de almacenamiento electronicos o magneticos que no pierden los datos al quedarse sin energia**





# Utilizar “writeblockers” (si es posible)



Además de prevenir la escritura accidental en el origen, algunos de estos dispositivos pueden acelerar la transferencia de datos haciendo mas rápida la obtención de la imagen







# Adquisición Imagen Forense

**GUYMAGER**

Devices Misc Help

Rescan

Serial nr.	Linux device	Model	State	Size	Hidden Areas	Bad sector
01000000000000000001	/dev/sda				known	
	/dev/sdb				known	
20120426000540F	/dev/sdc				known	
	/dev/sdd				known	

Size 21,474,836,800  
Sector size 512  
Image file  
Info file  
Current speed  
Started  
Hash calculation  
Source verification  
Image verification

### Acquire image of /dev/sda

File format

☒ Linux dd raw image (file extension .dd or .xxx)  
☐ Expert Witness Format, sub-format Guymager (file extension .Exx)  
☐ Advanced forensic image (file extension .aff)

☐ Split image files  
Split size  MiB

Case number   
Evidence number   
Examiner   
Description   
Notes

Destination

Image directory   
Image filename (without extension)   
Info filename (without extension)

Hash calculation / verification

☒ Calculate MD5 ☒ Calculate SHA-256  
☒ Re-read source after acquisition for verification (takes twice as long)  
☒ Verify image after acquisition (takes twice as long)

Ok Cancel



# Cadena de Custodia...

Organismo	Formulario de registro de evidencia de servidores	IF-Nro.
-----------	---	---------

Caso Nro.	Juzgado	Litigante

Especificaciones de la computadora	
Marca	
Modelo	
Nro de Serie	
Garantía	
Placa Madre Marca/Modelo	
Microprocesador Mar- ca/Modelo/Velocidad	
Memoria Ram	
Memoria Cache	

Almacenamiento Secundario, Fijo y /o Removible				
Canti- dad	Tipo Disketera-CD-ROM- DVD-Disco Rígido- IDE-SCSI-USB-Zip- Jazz-PenDrive	Mar- ca/Modelo	Velocidad/ Capacidad	

Accesorios y Periféricos				
Canti- dad	Tipo Placa de red, mo- dem, cámara, tar- jeta de acceso, im- presora, etc.	Mar- ca/Modelo	Velocidad/ Capacidad	

Rótulos para las evidencias	
Nro.	
Caso	
Fecha	
Tipo	
Observaciones	
Firma	

Acta de traslado					
Cadena de Custodia de la Evidencia					
Nro Identificación de Caso:					
Nro Unico de Identificación	Ubicación Actual	Fecha	Razón de traslado	Sitio a donde se traslada	Observaciones
Entregado por:					Firma y Aclaración
Recibido por:					Firma y Aclaración
Lugar de depósito final de la evidencia:					Fecha:





# Esquema Tradicional

## **Analizar imagen con herramientas forenses**

- Examinar archivos conocidos de evidencias (NTUSER.DAT, SYSTEM, SOFTWARE, ETC..)
- Examinar fechas de archivos (timeline)
- Comprobar software malicioso en la RAM
- Examinar archivos eliminados
- Realizar búsquedas de cadenas (strings)
- Analizar encabezados archivos (file carving)



# Adquisición / Analizando Imagen Adquirida

**Add Data Source**

**Steps**

1. **Enter Data Source Information**
2. Configure Ingest Modules
3. Add Data Source

**Enter Data Source Information wizard (Step 1 of 3)**

**Enter Data Source Information:**

Select source type to add: Image File

Browse for an image file:

C:\Users\axon\Documents\CASO\_WINXP\_KEYLOGGER\imagenwindowsXPkeylogger.dd Browse

Please select the input timezone: (GMT-5:00) America/New\_York

☐ Ignore orphan files in FAT file systems  
(faster results, although some data will not be searched)

Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

< Back **Next >** Finish Cancel Help

- **Imagen Forense**
- **Disco Conectado**

# Analizando Imagen Adquirida

**Add Data Source**

**Steps**

1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source

**Enter Data Source Information wizard (Step 1 of 3)**

**Enter Data Source Information:**

Select source type to add: Image File

Browse for an image file:

C:\Users\axon\Documents\CASO\_WINXP\_KEYLOGGER\imagenwindowsXPkeylogger.dd Browse

Please select the input timezone: (GMT-5:00) America/New\_York

☐ Ignore orphan files in FAT file systems  
(faster results, although some data will not be searched)

Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

< Back Next > Finish Cancel Help

ntuser.dat

ch 1

	ID	Starting Sector	Length in Sectors	D
	1	0	2048	Ur
91)	2	2048	41938944	NT
943039)	3	41940992	2048	Ur

Hex View String View Result View Text View Media View

0x000000:	72	65	67	66	64	07	00	00	64	07	00	00	09	1A
0x000010:	7C	60	CF	01	01	00	00	00	05	00	00	00	00	00
0x000020:	01	00	00	00	20	00	00	00	00	F0	C8	00	01	00



# Analizando Registros (hives) de Windows

YU yaru - limited ver: 1.31; Copyright (c) TZWorks LLC - Demo use only

File View Options Reports Time Format

Registry Keys

Key/Value data

c:\users\axon\documents\autopsy\owasp01\archivos-extraídos\sam

SAM

Domains

Account

Aliases

Groups

Users

000001F4

000001F5

000003E8

000003E9

000003EA

Names

Administrator

axon

Guest

operador

pentester

(unnamed)

SAM\SAM\Domains\Account\Users\Names\pentester

Timestamp: 0x01cf2c454a36eca3 (02/18/2014 01:03:52.651 UTC)

owner sid [S-1-5-32-544]

group sid [S-1-5-18]

Discretionary Access Control List

access allowed Local System DELETE | READ\_CONTROL | WRITE\_DAC | WRITE\_OWNER  
access allowed Admins READ\_CONTROL | WRITE\_DAC

(unnamed)

unk:

0x000003ea





# Archivos Conocidos

# SANS

## Windows Artifact Analysis: Evidence of...

©2012 SANS - Created by Rick Lam and the SANS DFIR Faculty

### File Download

#### Open/Save MRU

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of files that have been opened or saved, along with the date and time of the last access.

#### E-mail Attachments

**How to find:** Windows Mail, Outlook, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of email attachments, along with the date and time of the last access.

#### Internet History

**How to find:** Internet Explorer, Firefox, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of internet history, along with the date and time of the last access.

#### Indexed/Placed on the

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of indexed/placed on the, along with the date and time of the last access.

#### Downloaded files

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of downloaded files, along with the date and time of the last access.

Created for FORTNIGHT - Windows Forensics - SANS Digital Forensics and Incident Response faculty created the "Evidence of..." categories to map a specific artifact to the analysis question that it will help to answer. Use this poster as a cheat-sheet to help you remember where you can discover key items to an activity for Microsoft Windows systems for intrusions, intellectual property theft, or common cyber-crimes.

### Program Execution

#### User Activity

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of user activity, along with the date and time of the last access.

#### Last Visited MRU

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of last visited MRU, along with the date and time of the last access.

#### Run MRU Start-to-Run

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of run MRU start-to-run, along with the date and time of the last access.

#### Application Compatibility Cache

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of application compatibility cache, along with the date and time of the last access.

#### Win7 Jump Lists

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of win7 jump lists, along with the date and time of the last access.

#### Prefetch

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of prefetch, along with the date and time of the last access.

#### Service Events

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of service events, along with the date and time of the last access.

### File Opening/Creation

#### Open/Save MRU

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of open/save MRU, along with the date and time of the last access.

#### Last Visited MRU

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of last visited MRU, along with the date and time of the last access.

#### Recent Files

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of recent files, along with the date and time of the last access.

#### Shell bags

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of shell bags, along with the date and time of the last access.

#### Shortcut (LNK) files

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of shortcut (LNK) files, along with the date and time of the last access.

#### Win7 Jump Lists

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of win7 jump lists, along with the date and time of the last access.

#### Prefetch

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of prefetch, along with the date and time of the last access.

#### Indexed/Placed on the

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of indexed/placed on the, along with the date and time of the last access.

### Deleted File or File Knowledge

#### XP Search - ADMRU

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of XP search - ADMRU, along with the date and time of the last access.

#### Win7 Search - WordWhisper Query

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of win7 search - WordWhisper Query, along with the date and time of the last access.

#### Last Visited MRU

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of last visited MRU, along with the date and time of the last access.

#### Thumbnail

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of thumbnail, along with the date and time of the last access.

#### Win7/Win7 Thumbnails

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of win7/win7 thumbnails, along with the date and time of the last access.

#### XP Recycle Bin

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of XP recycle bin, along with the date and time of the last access.

#### Win7 Recycle Bin

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of win7 recycle bin, along with the date and time of the last access.

#### Indexed/Placed on the

**How to find:** Windows Explorer, File History, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of indexed/placed on the, along with the date and time of the last access.

### Physical Location

#### Time zone

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of time zone, along with the date and time of the last access.

#### VISTA/Win7 Network History

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of VISTA/Win7 network history, along with the date and time of the last access.

#### Cookies

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of cookies, along with the date and time of the last access.

#### Browser Search Terms

**How to find:** Windows Task Manager, Windows Explorer, or the Windows Search index. The Windows Search index is the most reliable source for this data.

**How to use:** The Windows Search index is the most reliable source for this data. It contains a list of browser search terms, along with the date and time of the last access.

Proper digital forensic and incident response analysis is essential to successfully solving complex cases today. Each analyst should examine the artifacts and then analyze the activity that they describe to determine a clear picture of which user was involved, what the user was doing, when they were doing it, and why. The data here will aid you in finding multiple locations that can help substantiate facts related to your case work.



# Esquema Web

- Entender el flujo "normal" de la aplicación
- Archivos de registro (logs):
  - Servidor web
  - Servidor de Aplicaciones
  - Servidor de Base de Datos
  - Aplicación
- Archivos de configuración de la aplicación y servidor
- Identificar posibles anomalías:
  - Entradas maliciosas desde el cliente
  - Interrupciones de las tendencias normales de acceso a Internet
  - Cabeceras HTTP inusuales
  - Cambios a mitad de la sesión a los valores de cookie.



# OWASP

The Open Web Application Security Project

## OWASP Top 10 - 2013

Los diez riesgos más críticos en Aplicaciones Web

# A1

## Inyección

 Agentes de Amenaza	 Vectores de Ataque	 Debilidades de Seguridad		 Impactos Técnicos	 Impactos al negocio
Específico de la Aplicación	Explotabilidad FÁCIL	Prevalencia COMÚN	Detección PROMEDIO	Impacto SEVERO	Específico de la aplicación/negocio
Considere a cualquiera que pueda enviar información no confiable al sistema, incluyendo usuarios externos, usuarios internos y administradores.	El atacante envía ataques con cadenas simples de texto, los cuales explotan la sintaxis del interprete a vulnerar. Casi cualquier fuente de datos puede ser un vector de inyección, incluyendo las fuentes internas.	Las <u>fallas de inyección</u> ocurren cuando una aplicación envía información no confiable a un interprete. Estas fallas son muy comunes, particularmente en el código antiguo. Se encuentran, frecuentemente, en las consultas SQL, LDAP, Xpath o NoSQL; los comandos de SO, intérpretes de XML, encabezados de SMTP, argumentos de programas, etc. Estas fallas son fáciles de descubrir al examinar el código, pero difíciles de descubrir por medio de pruebas. Los analizadores y «fuzzers» pueden ayudar a los atacantes a encontrar fallas de inyección.		Una inyección puede causar pérdida o corrupción de datos, pérdida de responsabilidad, o negación de acceso. Algunas veces, una inyección puede llevar a el compromiso total de el servidor.	Considere el valor de negocio de los datos afectados y la plataforma sobre la que corre el intérprete. Todos los datos pueden ser robados, modificados o eliminados. ¿Podría ser dañada su reputación?



# Reporte

Firefox

ACME Co.

Autopsy Report for case OWASP001

+

file:///C:/Users/axon/Documents/AUTOPSY/OWASP001/Reports/OWASP001 04-26-2014-11-22-47/HTML Report/index.html

Google

Report Navigation

Case Summary

Bookmarks (84)

Cookies (510)

Devices Attached (0)

Downloads (0)

EXIF Metadata (0)

File Tags (2)

Hashset Hits (0)

Installed Programs (0)

Keyword Hits (3088)

Recent Documents (0)

Result Tags (0)

Web History (365)

Web Search Engine Queries (80)

Firefox

ACME Co.

Autopsy Report for case OWASP001

+

file:///C:/Users/axon/Documents/AUTOPSY/OWASP001/Reports/OWASP001 04-26-2014-11-22-47/HTML Report/index.html

Report Navigation

Case Summary

Bookmarks (84)

Cookies (510)

Devices Attached (0)

Downloads (0)

EXIF Metadata (0)

File Tags (2)

File Tags

Comment	File Name
	access.log
	access.log





# El proceso “standard” no siempre funciona



=



- Las aplicaciones web son a menudo críticas y el tiempo de inactividad para realizar la adquisición de una imagen **NO** es una opción desde **el punto de vista de el negocio.**
- Las aplicaciones web se distribuyen a menudo a través de múltiples servidores.
- Servidores de bases de datos por lo general tienen grandes arreglos de discos.



# Conclusiones



**Atacante**



**Servidor Web**

Card Type	Card Number	Issue	CV2	Address	PostCode
Visa (VISA)	492900000000006		123	88	412
MasterCard (MC)	54040000000000001		123	88	412
Visa Debit / Delta (DELTA)	44620000000000003		123	88	412
Solo (SOLO)	63349000000000005	1	123	88	412
UK Maestro / International Maestro (MAESTRO)	56418200000000005	01	123	88	412
American Express (AMEX)	300000000000000004	N/A	123	88	412
Visa Electron (UKE)	49173000000000008		123	88	412
JCB (JCB)	35699900000000009		123	88	412
Diner's Club (DINERS)	36000000000000008		123	88	412
Laser (LASER)	6304990000000000044		123	88	412





# OWASP

The Open Web Application Security Project

<http://www.owasp.org>

<http://www.owasp.org>

**PREGUNTAS Y/O  
COMENTARIOS**

**MauricioUrizar**



**murizar@open-sec.com**



**@MauricioUrizar**