



The OWASP Foundation

<http://www.owasp.org>

Análisis Forense de un Ataque Web

Mauricio Urizar

murizar@open-sec.com



@MauricioUrizar



- Trabajando los últimos 07 años como parte del equipo de hacker éticos 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)

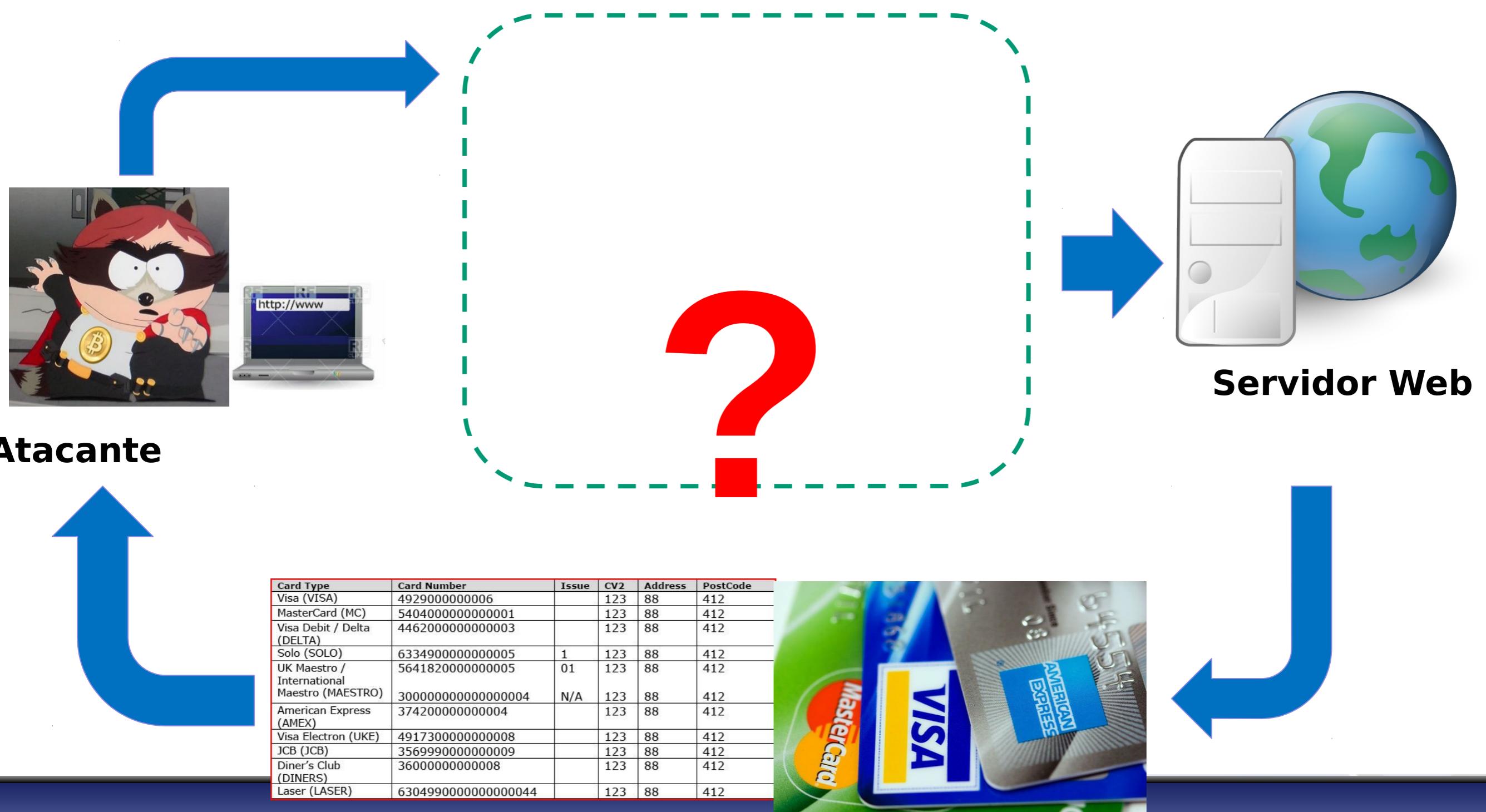


DESCARGO DE RESPONSABILIDADES

- 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





Que buscamos...

En busca de respuestas...

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





Investigación Forense



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

Definición de la Metodología

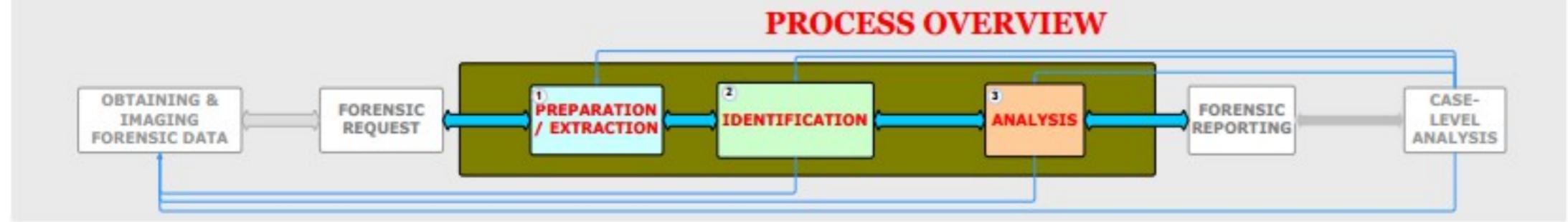
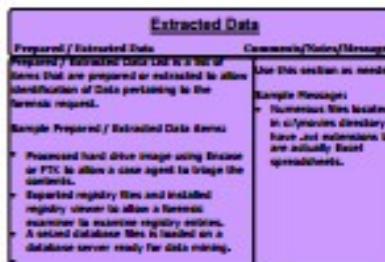
http://www.justice.gov/usa/o/eousa/foia_reading_room/usab5601.pdf



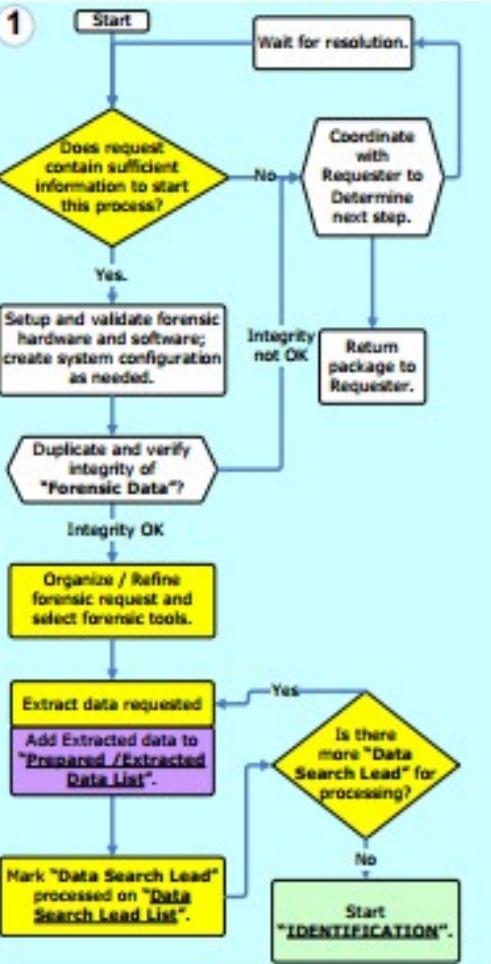
DIGITAL FORENSIC ANALYSIS METHODOLOGY



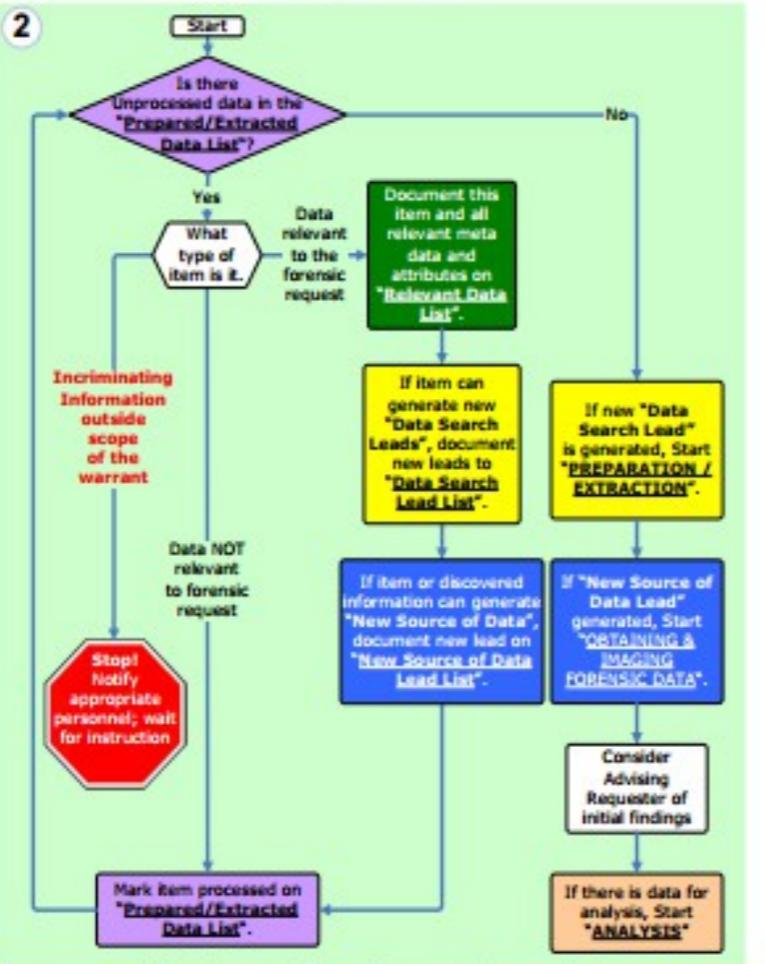
LISTS



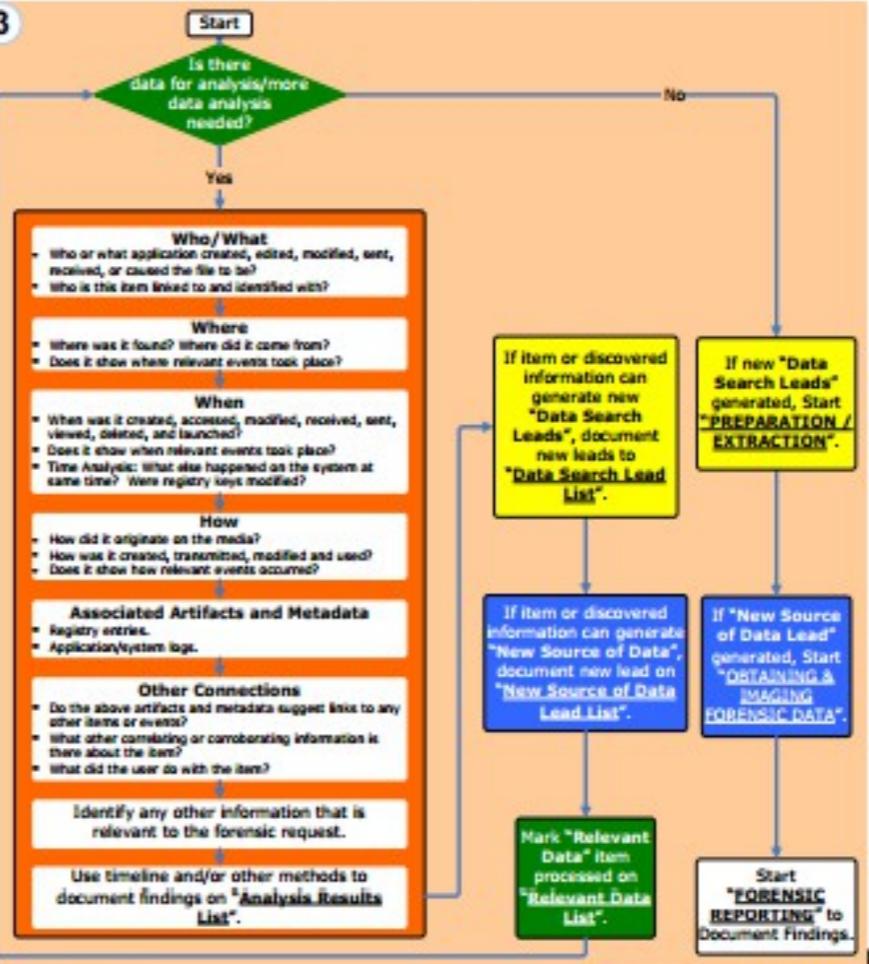
PREPARATION / EXTRACTION



IDENTIFICATION



ANALYSIS

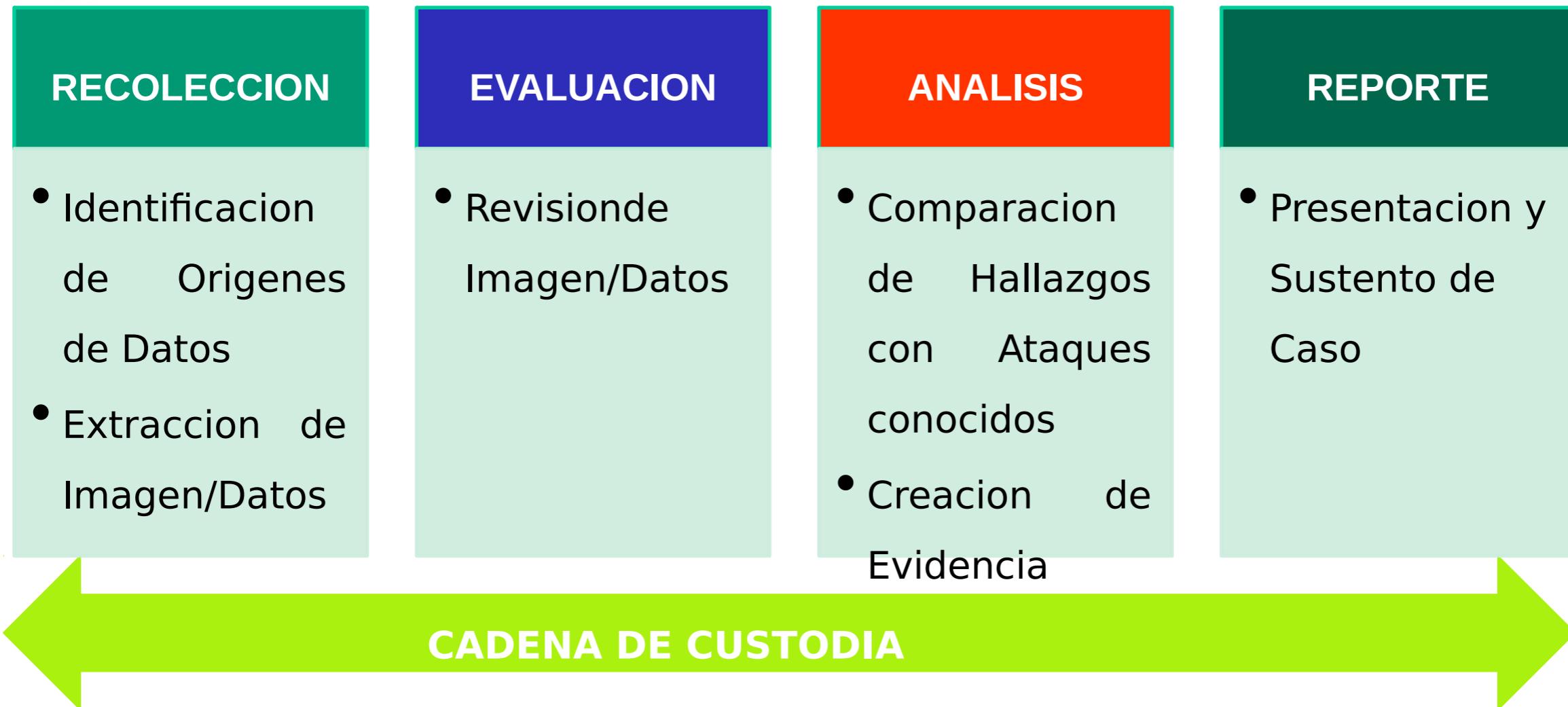


Return On Investment (determine when to stop this process. Typically, after enough evidence is obtained for prosecution, the value of additional forensic analysis diminishes.)

1000 1000 1000



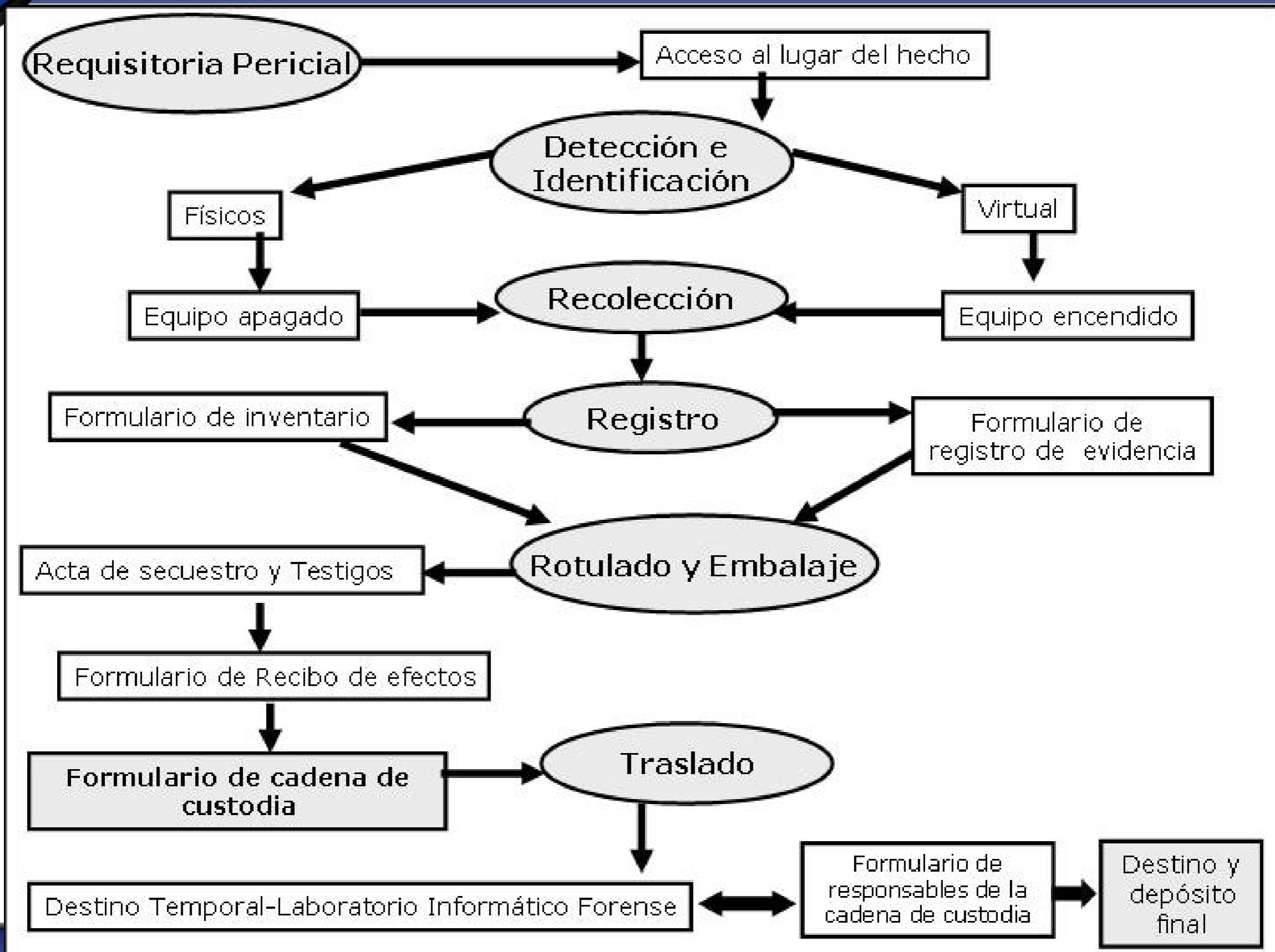
Proceso Forense Tradicional



“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



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

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)

Package list | DEFT Linux – Computer Forensics live

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

www.deftlinux.net/package-list/



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 Current downloads for

Filename	Summary + Label
tr3_tool_kit_v2.zip	tr3_data_collection
Microsoft_Office_Excel_MetaData_Changes.pdf	Microsoft Office E
Microsoft_Office_Word_MetaData_Changes.pdf	Microsoft Office W
general-info.bat	regripper-general-os-info.bat script
vsc-parser.zip	vsc-parser BatchScripting VSCs

Organizar Compartir con Grabar Nueva carpeta

Favoritos

- Descargas
- Escritorio
- Sitios recientes

Bibliotecas

- Documentos
- Imágenes
- Música
- Videos

Equipo

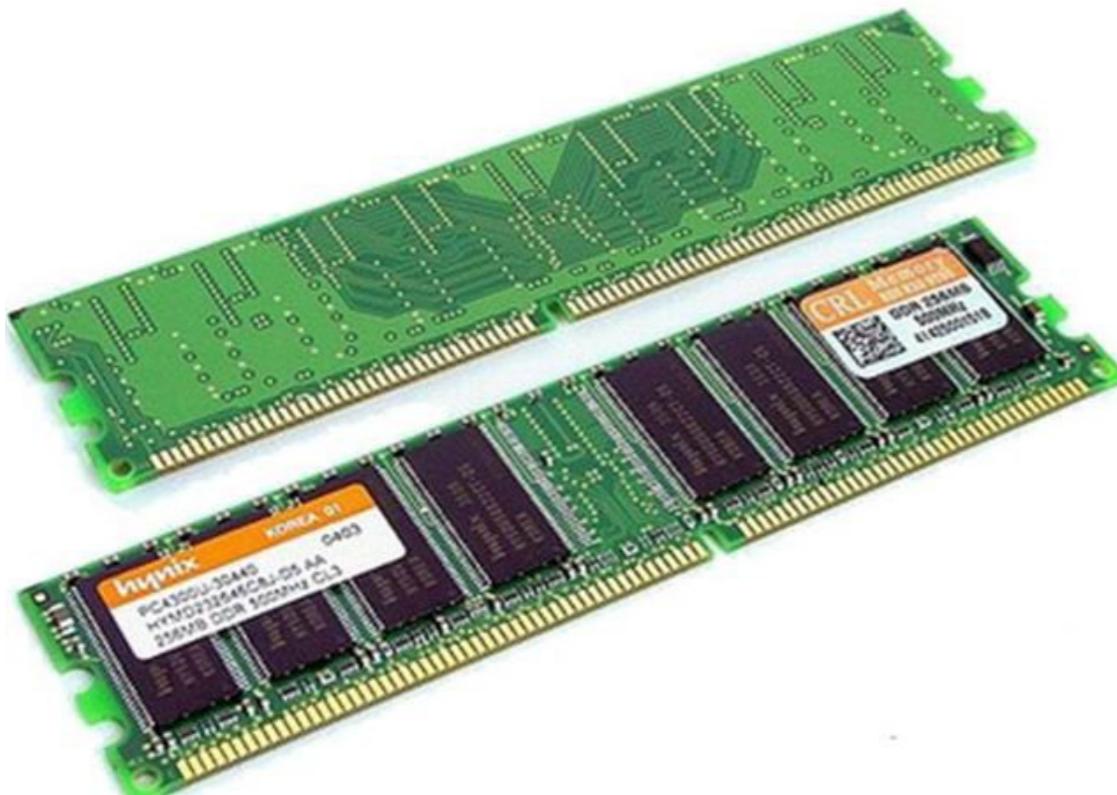
- Disco local (C:)
- HP16GB (E:)
- Disco extraíble (F:)
- TOSHIBA EXT (G:)

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-mapping	24/05/2013
NetworkInfo_8_port-to-process-mapping	24/05/2013
OpenedFileInfo_1_opened-files	24/05/2013
OpenedFileInfo_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_processes-file-handles	24/05/2013



Adquiriendo Evidencia Volátil



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

Símbolo del sistema

```
E:\volatility\winpmem-1.4>winpmem_1.4.exe -1 image-mem-win.raw
Driver Unloaded.
Loaded Driver C:\DOCUMENTOS\ADMINISTRACION\CONFIG\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 0x1EEP0000
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 connscan
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\iexplore.exe
0x7c900000  0xaf000  0xffff  C:\WINDOWS\system32\ntdll.dll
0x7c800000  0xf6000  0xffff  C:\WINDOWS\system32\kernel32.dll
0x5d090000  0x9a000  0x1    C:\WINDOWS\system32\comctl32.dll
0x100000000 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.....:widservc.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



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

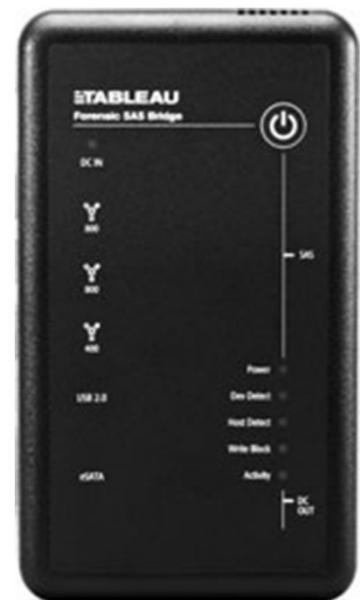


Informacion proveniente de medios de almacenamiento electronicos o magneticos que no pierden los datos al quedarse sin energia





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
010000000000000000000001	/dev/sda				known	
					known	
20120426000540F	/dev/sda				known	
					known	

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 2047 MiB

Case number

Evidence number

Examiner

Description

Notes

Destination

Image directory ... /mnt/toshiba/owasp-image/v2/

Image filename (without extension) win2008webserverowasp2014

Info filename (without extension) win2008webserverowasp2014

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	Lugar			
Especificaciones de la computadora					
Marca					
Modelo					
Nro. de Serie					
Garantía					
Placa Madre					
Marca/Modelo					
Microprocesador Marca/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	Marca/Modelo	Velocidad/ Capacidad		
Accesorios y Periféricos					
Canti-dad	Tipo Placa de red, mo- dem, cámara, tar- jeta de acceso, im- presora, etc.	Marca/Modelo	Velocidad/ Capacidad		
Rótulos para las evidencias					
Nro.					
Caso					
Fecha					
Tipo					
Observaciones					
Firm					
Acta de traslado					
Cadena de Custodia de la Evidencia					
Nro. Identificación de Caso:					
Nro. Único 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:

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

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**

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

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.

File System Tree:

- ProgramData (4)
- System Volume Information (4)
- Users (9)
- Windows (79)
- xampp (51)
- \$OrphanFiles (94)
- \$Unalloc (3)
- vol3 (Unallocated: 41940992-41943039)

Views

Results

- Extracted Content
 - Bookmarks (84)
 - Cookies (510)
 - Web History (387)
 - Downloads (0)
 - Recent Documents (0)

Hex View **String View** **Result View** **Text View** **Media View**

ID	Starting Sector	Length in Sectors	...
1	0	2048	Un
91	2048	41938944	NT
943039	41940992	2048	Un

Analizando Registros (hives) de Windows



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

File View Options Reports Time Format

Registry Keys

Key/Value data

Registry Keys

- c:\users\axon\documents\autopsy\owasp01\archivos-extraidos\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



Windows Artifact Analysis: Evidence of...

File
Download

Program Execution

File Opening / Creation

Deleted
File or File
Knowledge

Physical Location



Created for ICOntract – Windows Forensics – SAM43
Digital Forensics and Incident Response faculty
created this “Evidence of...” categories to map a
specific artifact to the analysis question that it
will help to answer. Use this poster as a chea-
sheet to help you remember where you can
discover key items to an activity for Microsoft
Windows systems for intrusions, intellect and
malware by file, or process or volume or item.



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 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

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)
- HashSet Hits (0)
- Installed Programs (0)
- Keyword Hits (3088)
- Recent Documents (0)
- Result Tags (0)
- Web History (365)
- Web Search Engine Queries (80)

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



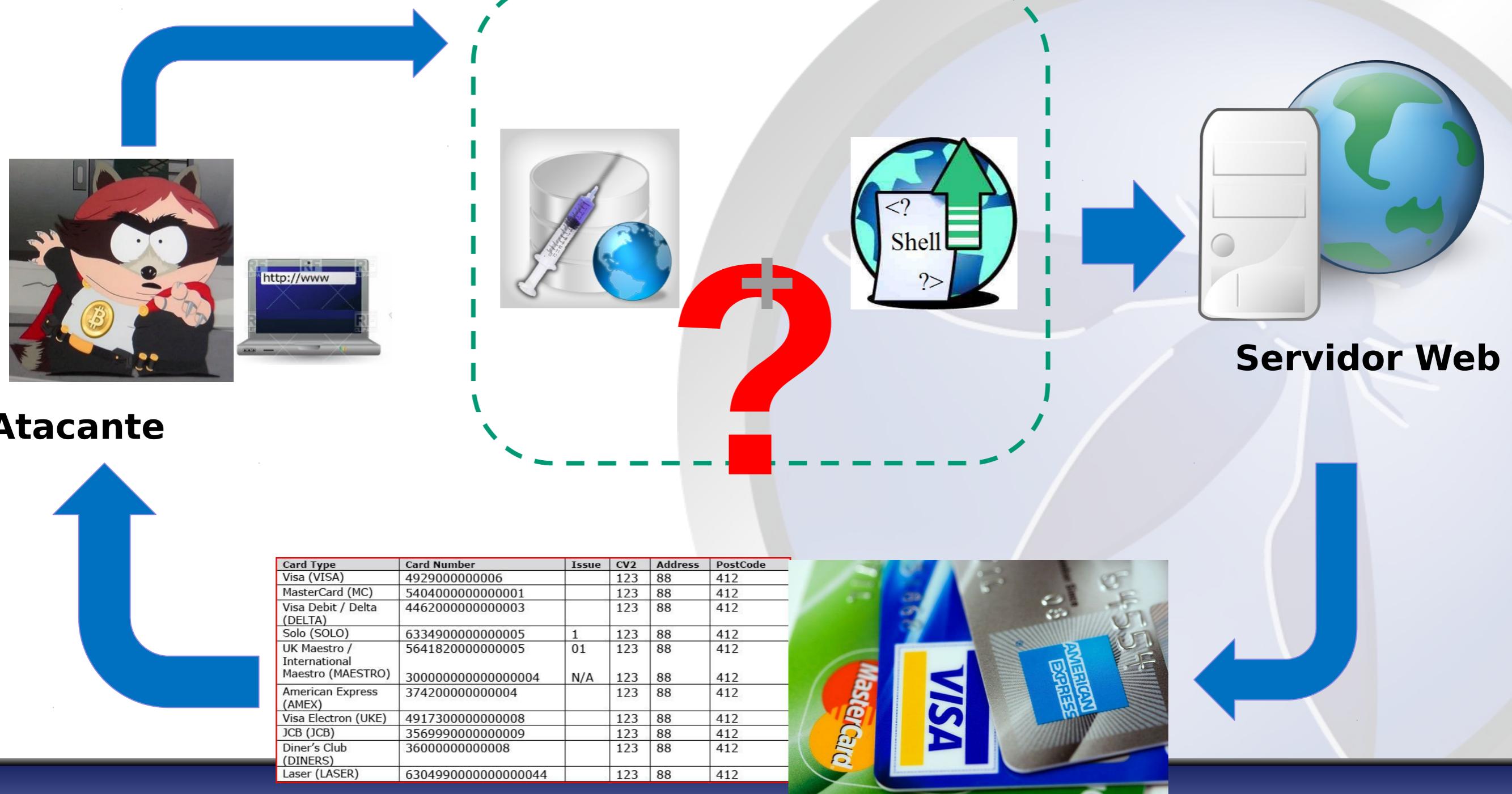
El proceso “standard” no siempre funciona



- 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 del 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





OWASP

The Open Web Application Security Project

<http://www.owasp.org>

**PREGUNTAS Y/O
COMENTARIOS**

MauricioUrizar



murizar@open-sec.com



@MauricioUrizar