

# Adquisición de datos forenses

FIRST Technical Colloquium, Montevideo 2008

Ing. Santiago Paz, CISA, PMP, SSCP  
[santiago.paz@cert.uy](mailto:santiago.paz@cert.uy)  
[www.cert.uy](http://www.cert.uy)

## ¿Qué es CERTuy?

[www.cert.uy](http://www.cert.uy)

- Centro Nacional de Respuesta a Incidentes en Seguridad Informática
- Creado en la rendición de cuentas 2008, depende de AGESIC y tiene como cometido la protección de activos de información críticos del estado
- Es un Centro Coordinador de equipos de respuesta a incidentes en seguridad



# Agenda

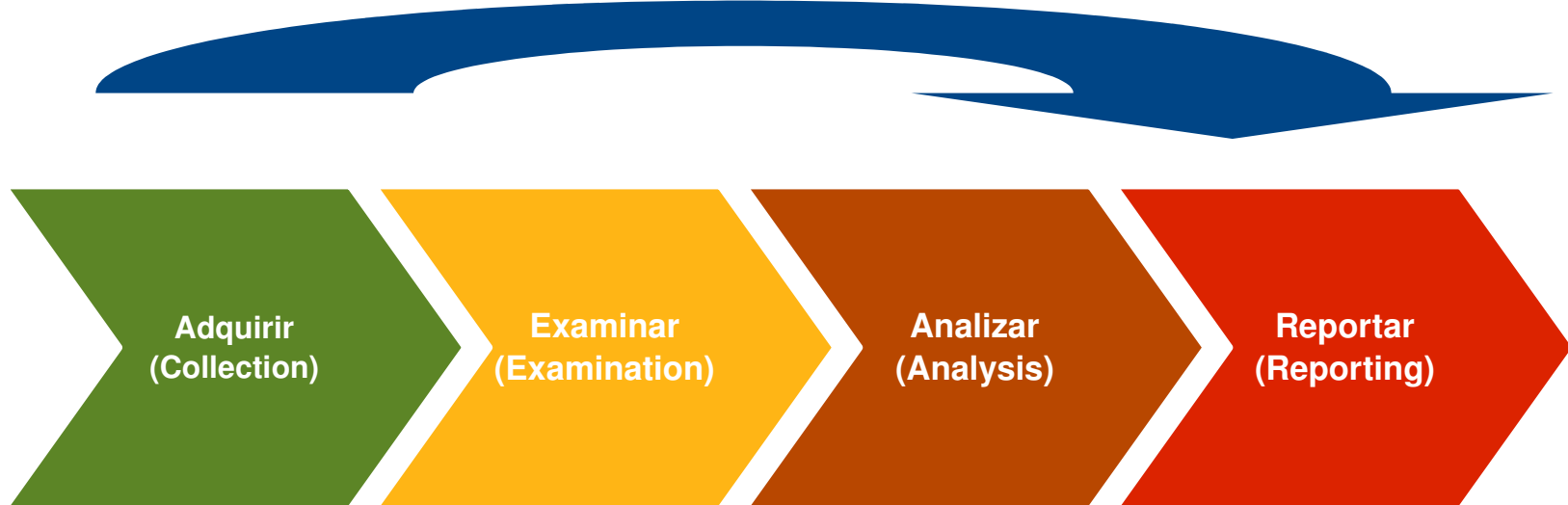
- Proceso forense
- Actividad forense de un CSIRT
- Adquisición de datos
- Casos de estudios
  - 1) Sistema off-line (post-mortem)
  - 2) Sistemas on-line (Vivo)

## nota:

- Esta presentación NO define un marco legal para la evidencia digital, son solo recomendaciones técnicas
- Esta presentación utiliza herramientas de uso libre, aunque existen también herramientas propietarias
- Las colecciones de datos de ejemplo NO son exhaustivas ni únicas, son simplemente recomendaciones
- Las herramientas presentadas NO fueron probadas en todos los ambientes, úsenlas a su propio riesgo

# Proceso Forense

Prepararse!



Sistema

Evidencia

# ¿Forénsica en un CSIRT?

- El equipo de respuesta a incidentes es de los primeros notificados del incidente, y trabaja en él hasta su solución
- Mitigación drástica vs. Preservación de la evidencia
- Procesos sistematizados, documentados y reproducibles
- La adquisición que se realice durante el incidente es MUY valiosa



# Documentación y custodia

- Buscar contra-partes para control
- Bitácora de actividades
- Fotografías
- Lacres
- Integridad y autenticidad
  - Firmas (digitales, autógrafas)
  - Hashes
- Formalizar la transferencia o custodia

```
spaz@linpolis:~/tmp/casol$ ls
Bicatoca_casol.odt  foto_fotointerna.jpg  foto_tracera.jpg
foto_adelante.jpg  foto_pantalla.jpg    imagen_sda_casol.dd
spaz@linpolis:~/tmp/casol$ shasum * | tee hashes_casol.shal
83f0aa17b3d261a261f0f7567959752bf6f0c500  Bicatoca_casol.odt
c4d07a3d3fa3fbe152564e02e019bc5441f53071  foto_adelante.jpg
e5fa44f2b31c1fb553b6021e7360d07d5d91ff5e  foto_fotointerna.jpg
02643953ae91930eff13ad13b639950a3f33ea9c  foto_pantalla.jpg
9e326868f078aede495af377c3f0f737827e6e7e  foto_tracera.jpg
d60ff6fcde8192ee5a25bac20579034e42d04487  imagen_sda_casol.dd
spaz@linpolis:~/tmp/casol$
```

**CERTuy**

**1 Técnicos asignados**

Técnico	Institución	Rol Asignado	contacto
<a href="#">Bruno Diaz</a>	Ciudad Gótica	<a href="#">Super héroe</a>	
<a href="#">John Rambo</a>	Army	Boina verde	

**2 Otros involucrados**

Persona	Institución	Contacto	Comentarios

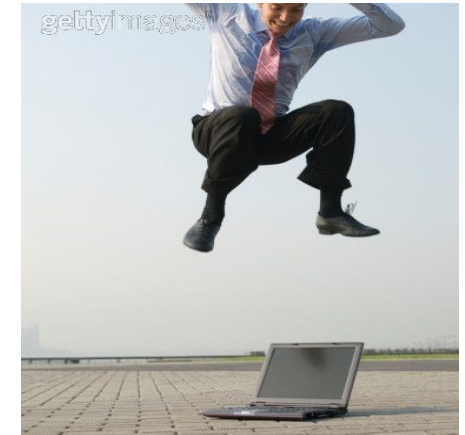


Adquirir  
(Collection)

# Adquisición de datos (RFC3227)

- Principios:

- Conseguir la imagen más fiel del sistema
- Minimizar los cambios en el sistema
- Documentar cada paso
- Colectar de lo más volátil a lo menos volátil
- Adherirse a las normas y políticas aplicables
- etc



- **NO HACER:**

- **Bajar o Reiniciar el sistema (hasta haber colectado)**
- **No confiar en el sistema comprometido**
- **No comprometer más sistemas por proteger la evidencia!!**

# Información a adquirir

- Por orden de volatilidad (RFC3227):

- Registros, cache
- Memoria, procesos, estado del kernel
- Información de red
- Filesystem temporal
- Discos
- Información remota (logs, remote file system)
- Información física (escena)

- **Sistema offline (post-mortem):**

- Archivos temporales
- Swap
- Discos
- Información remota
- Información física

- **Sistema on-line (vivo):**

- Cache, memoria
- Procesos, estadísticas
- Actividad de red
- Discos, swap, archivos temporales\*
- Información física

# Caso de estudio 1

Sistema offline (post-mortem)

# Sistema off-line (I)

- Verificar proceso de booteo
- Tomar fecha y hora
- Bootear con CD forense
- Tomar imagen del disco
- Apagar
- Lacrar

**Documentar!**

# Sistema off-line (herramientas)

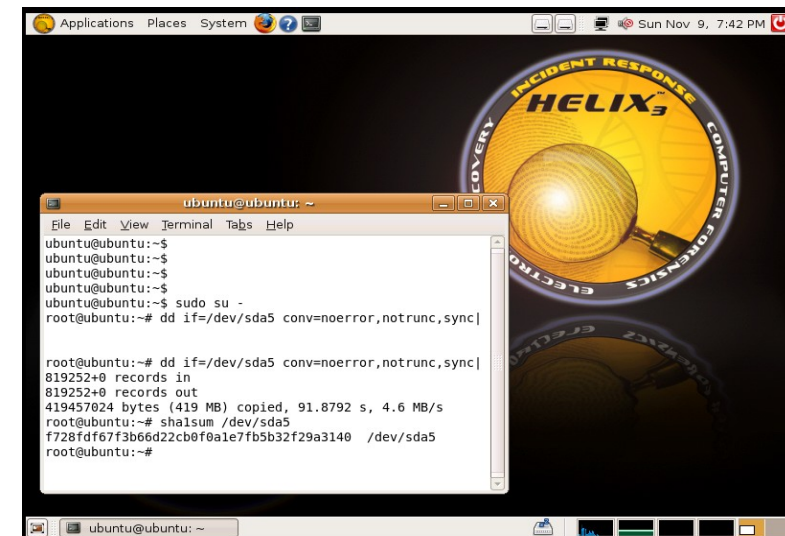
## • CD boteables

- Helix
- F.I.R.E
- Knoppix
- Pinguin-Sleuth

- No escribir en el HD del sistema (incluso swap)
- Tener drivers necesarios
- Tener herramientas necesarias

## • Herramientas de clonado

- dd, cat, win32dd, etc.
- nc, netcat, ssh
- df, fdisk, echo, etc
- md5sum, sha1sum, gpg



# Herramientas

## fdisk -l

- manipulador de tablas de particiones para linux. Con el modificador -l lista todas las tablas.

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	1	2306	18522913+	7	HPFS/NTFS
/dev/sda2		4935	9729	38515837+	b	W95 FAT32
/dev/sda3		2307	4934	21109410	5	Extended
/dev/sda5		2307	4819	20185641	83	Linux
/dev/sda6		4820	4934	923706	82	Linux swap

## sha1sum

- Realiza un calculo de hash SHA1 del contenido del archivo

## dd

- Herramienta para la generaci3n de imagenes. Realiza copias de bit-stream

## nc

- Netcat: herramienta para la manipulacion de conexiones de red. Funciona como cliente o como servidor

# Sistema off-line (ejemplo)

- Sistema analizado:

```
root@ubuntu:~#fdisk -l | nc 172.50.240.1 666 -w 3
```

```
root@ubuntu:~#sha1sum /dev/sda |nc 172.50.240.1 666 -w 3
```

```
root@ubuntu:~#dd if= /dev/sda conv=noerror,notrunc,sync | nc 172.50.240.1 666 -w 3
```

## Portable forense:

```
root@forense:~#nc -l -p 666 >>caso1_HD.txt
```

```
root@forense:~#nc -l -p 666 >>caso1_hashes
```

```
root@forense:~#nc -l -p 666 >caso1_HD_sda.dd
```

```
root@forense:~#sha1sum caso1_HD_sda.dd >>caso1_hashes
```

# Caso de estudio 2

Sistema on-line (Vivo)

# Información volátil (Linux)

- Carátula
  - **date, /proc/version, /proc/meminfo, hostname, ifconfig, uptime**
- Procesos en ejecución
  - **ps aux**
- Archivos abiertos
  - **lsof**
- Módulos cargados
  - **lsmod, /proc/modules**
- Usuarios logueados
  - **last, who, w**
- Tabla de enrutamiento
  - **netstat -nr**
- Firewall
  - **iptables -nvL, iptables-save**
- Cache arp
  - **arp -a**
- Conexiones de red
  - **netstat -punta**

# Información volátil Linux (II)

- Dump de memoria
  - **dd if=/dev/mem**
  - **dd /proc/kcore**
  - **memdump**
- Demo principio de incertidumbre

# Demo

Principio de incertidumbre

# Información volátil (windows)

- Carátula:
  - **date /t, time /t, hostname, ver.exe, uptime.exe, psinfo.exe,**
- Información de red
  - **Ipconfig /all, nbstat -c, promiscdetect.exe**
- Usuarios logueados
  - **PSloggedon.exe**
- Procesos en ejecución
  - **tlist.exe, pslist.exe, tasklist.exe**
- DLL cargadas
  - **ListDLLs.exe**
- Archivos abiertos
  - **Handle.exe**
- Tabla de enrutamiento
  - **netstat -nr**
- Cache arp
  - **arp.exe -a**
- Conexiones de red
  - **netstat.exe -ano**
- Dump de memoria
  - **dd.exe if=\\.\PhysicalMemory**

# Demo

Demo sistema on-line comprometido

# Herramientas

- Static Binaries
  - Helix
  - Sysinternals
  - gcc -static
  - LD\_LIBRARY\_PATH
- Considerar el uso de scripts
- Medio
  - CD/DVD
  - USB HW write protection
  - USB U3
  - Disco externo

# Conclusión

- Durante una respuesta a incidentes hay que tener en cuenta que luego el sistema puede ser necesarios para estudios forenses
- Hay que documentar bien cada paso
- La adquisición de datos on-line tiene mucha información útil que se pierde al apagar
- No hay que confiar en el sistema comprometido

# ¿Preguntas?

RFC 3227

<http://www.faqs.org/rfcs/rfc3227.html>

NIST 800-86

<http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>

Computer Forensics: Result of live response Inquiry vs. Memory image

<http://www.sei.cmu.edu/>

Manual de Peritaje informático

*Fundación de Cultura Universitaria, UY*

*Laboratorio Argentino*

<http://www.informaticapericial.com.ar>

HELIX

<http://www.e-fense.com/helix>