

# Unidad 7

## **Gestión de incidentes y Análisis Forense**

# ¿Qué es la forensia informática?

La **forensia informática** se ocupa del estudio de la adquisición, preservación, análisis y presentación de evidencias electrónicas procesadas y conservadas en un medio informático determinado.

# ¿Qué es un incidente de seguridad?

Un **incidente de seguridad** es:

- A) Un evento adverso en un entorno informático, que puede comprometer o compromete la confidencialidad, integridad o disponibilidad de la información.
- B) Una violación o inminente amenaza de violación de una política de seguridad de la información, política aceptable de uso o mejores prácticas de seguridad.

# Gestión de Incidentes

Consiste en la asignación oportuna de los recursos necesarios y su uso adecuado, con el objeto de prevenir, detectar y corregir incidentes que afectan la seguridad de la información.

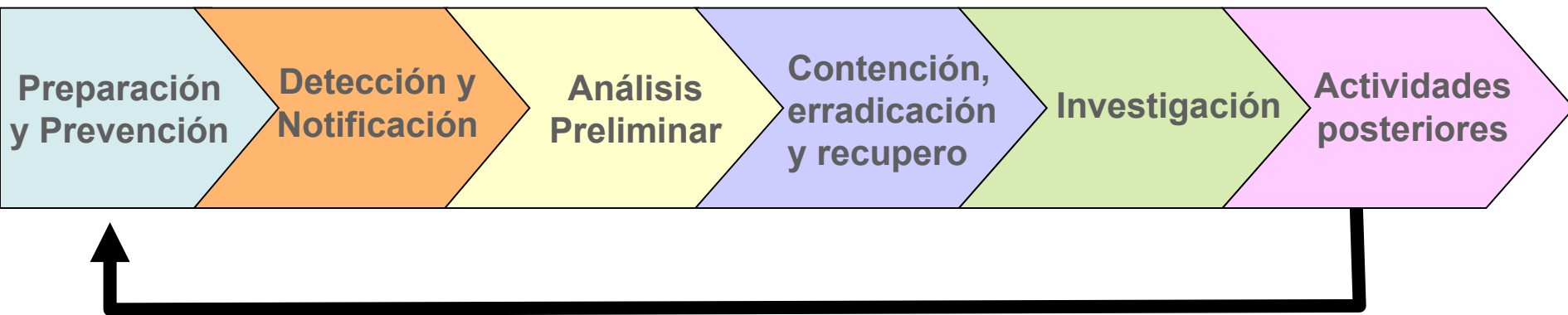
- ✓ Prevención de incidentes
- ✓ Detección y reporte del incidente
- ✓ Clasificación del incidente
- ✓ Análisis del incidente
- ✓ Respuesta al incidente
- ✓ Registro de incidentes
- ✓ Aprendizaje a partir de la experiencia
- ✓ Concientización y capacitación

# Algunos beneficios



- ✓ Responder a los incidentes en forma sistemática.
- ✓ Facilitar una recuperación rápida y eficiente de incidentes de seguridad, minimizando la pérdida de información e interrupción de servicios.
- ✓ Prevenir la ocurrencia reiterada de incidentes mediante el aprendizaje.
- ✓ Mejorar continuamente el marco de seguridad y el proceso de tratamiento de incidentes.
- ✓ Manejar correctamente los aspectos legales que pudieran surgir en el tratamiento de incidentes.

# Gestión de incidentes de seguridad



## Medidas de preparación

- Definir políticas, normas y procedimientos para la gestión de incidentes
- Definir criterios de clasificación y priorización de incidentes
- Preparar el CSIRT
- Entrenar al personal
- Documentar un mapa de la topología y arquitectura de la red
- Documentar la configuración del equipamiento
- Crear patrones de redes y sistemas
- Comprender el funcionamiento normal

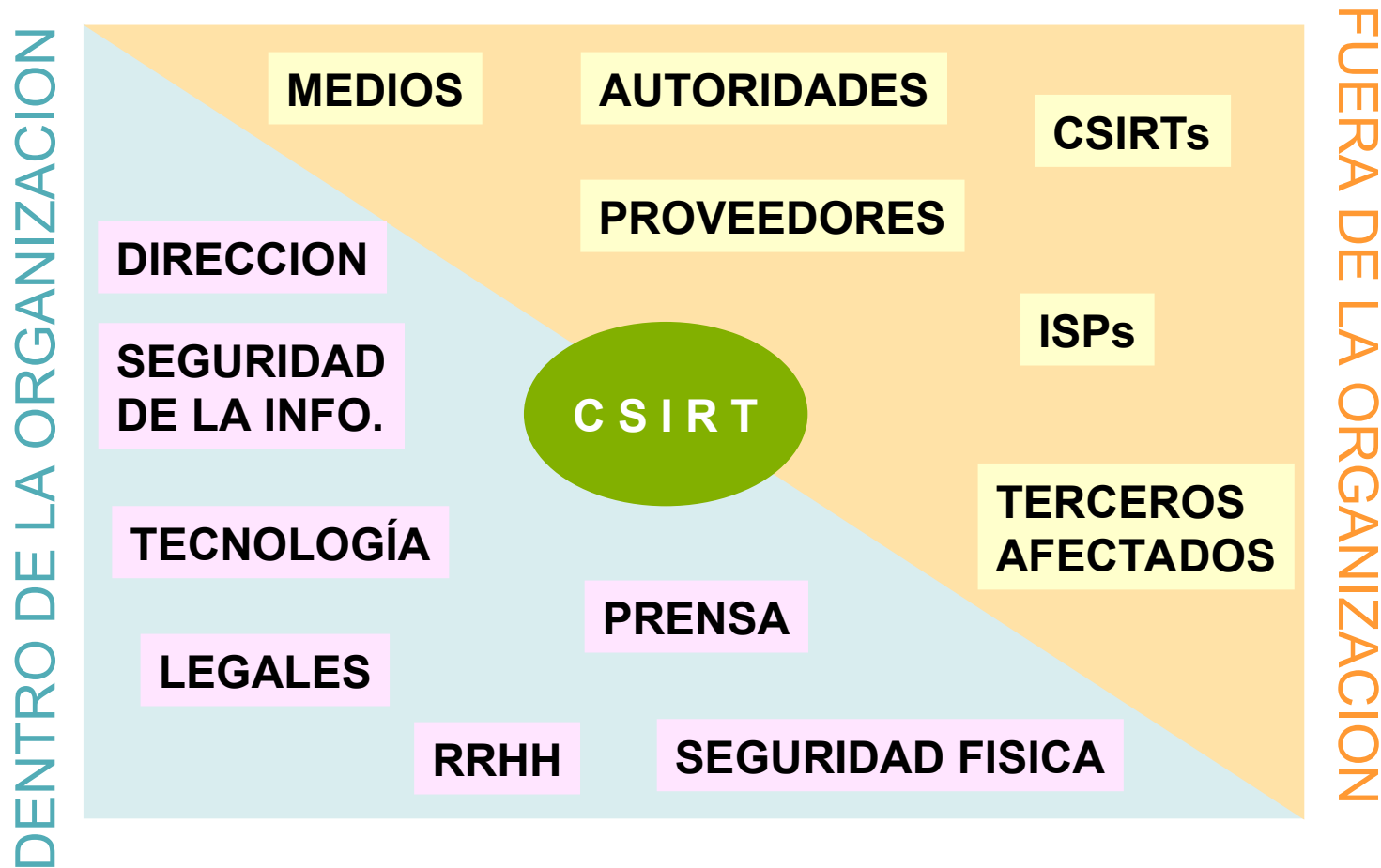
## Medidas de preparación

- Activar los logs en las diferentes plataformas y aplicaciones y en el equipamiento de comunicaciones
- Utilizar logging centralizado y crear una política de almacenamiento de logs
- Mantener los relojes de todos los equipos sincronizados
- Crear sumas de comprobación criptográficas (cryptographic checksums)
- Definir e implementar esquemas de resguardos de datos
- Contactos



# Preparación y Prevención

## Manejo de información con terceras partes



**Considerar la necesidad de utilizar herramientas para:**

- Detección de incidentes
- Monitoreo
- Análisis de incidentes – análisis forense
- Documentación de incidentes
- Etc.

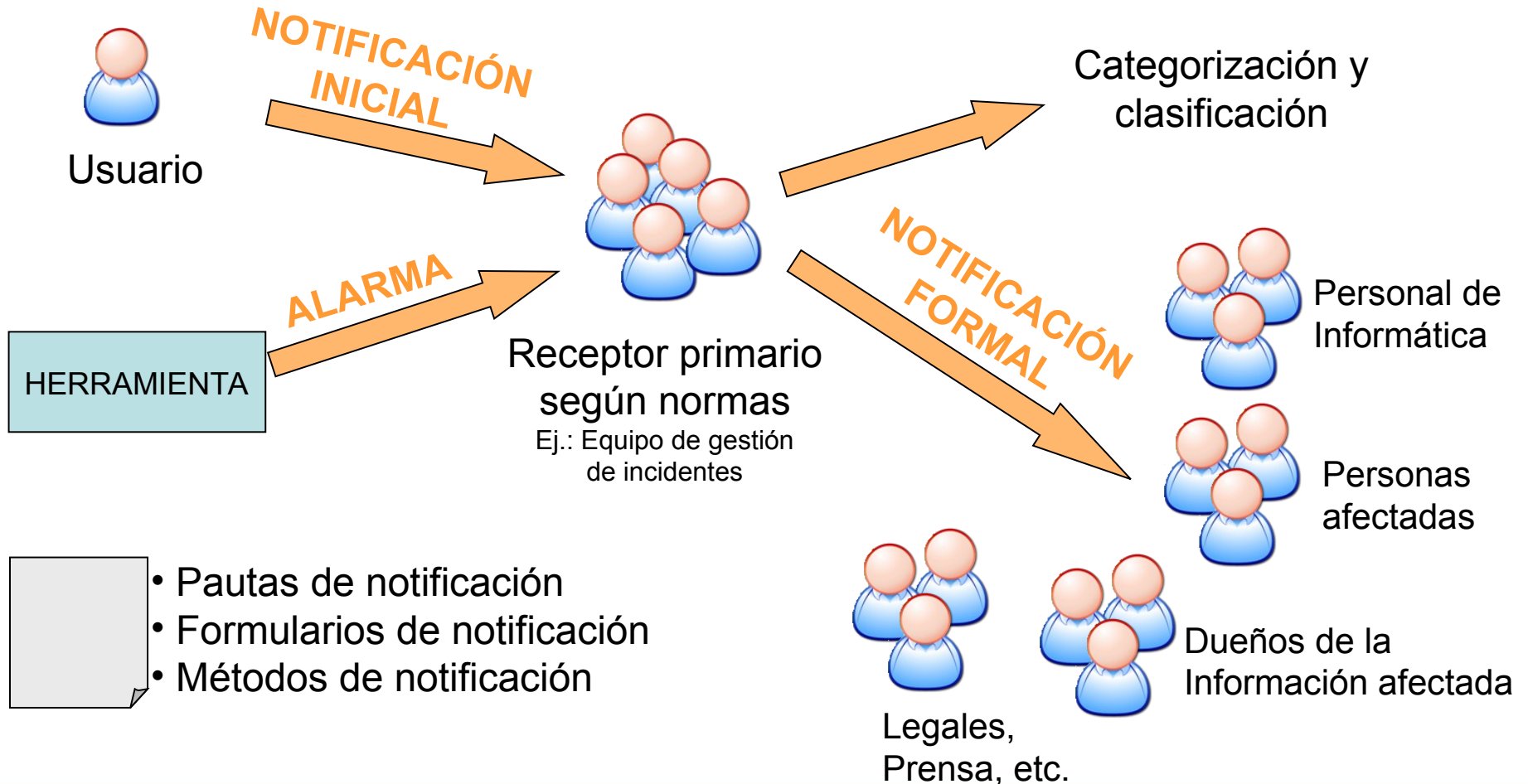
## Prevención de incidentes

- ✓ Análisis periódicos de riesgos
- ✓ Mejores prácticas de seguridad
- ✓ Auditorías periódicas
- ✓ Administración de actualizaciones
- ✓ Fortalecimiento de la seguridad de los equipos
- ✓ Seguridad en la red
- ✓ Prevención de código malicioso
- ✓ Concientización y capacitación de usuarios

## Detección de incidentes

- ✓ IDS - Sistemas de detección de intrusiones de red (NIDS) o de host (HIDS)
- ✓ Software antivirus
- ✓ Software de control de integridad de archivos
- ✓ Sistemas de monitoreo de red (NMS)
- ✓ Análisis de registros de auditoría (logs, SIEM)
- ✓ Información pública
- ✓ Usuarios de la organización
- ✓ Personas externas a la organización

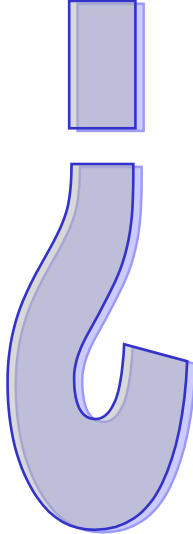

## Notificación de incidentes



## Recolección de información para analizar

- ✓ Alcance del incidente, es decir, qué redes, sistemas y aplicaciones afecta
- ✓ Qué originó el incidente
- ✓ Cómo ocurrió (o está ocurriendo) el incidente – métodos, herramientas utilizadas, vulnerabilidades explotadas, etc..
- ✓ El impacto potencial en las actividades de la organización

## Cómo determinar el alcance

- 
- ☐ ¿Cuántos equipos fueron comprometidos?
  - ☐ ¿Cuántas redes se vieron envueltas?
  - ☐ ¿Cuán dentro de la red logró penetrar el atacante?
  - ☐ ¿Qué nivel de privilegio logró el atacante?
  - ☐ ¿Qué es lo que está en riesgo? ¿Cómo impacta en las actividades de la organización el compromiso de los equipos? ¿Se encuentran en riesgo aplicaciones críticas?
  - ☐ ¿Quién sabe acerca del incidente y cómo puede afectar esto el impacto del mismo?
  - ☐ ¿Cuán conocida es la vulnerabilidad explotada por el atacante? ¿Hay otros equipos con la misma vulnerabilidad?
- 

## Métodos de recolección de información

### A C C I O N E S

- ☐ Indagación a los administradores de sistemas
- ☐ Personal de la organización
- ☐ Revisión de reportes de herramientas de detección de intrusiones
- ☐ Revisión de logs de comunicaciones, plataformas y sistemas
- ☐ Revisión de la topología de red y listas de acceso

### R E S U L T A D O S

- ☐ Obtener datos sobre sucesos anormales en los sistemas
- ☐ Obtener datos sobre sucesos anormales en las actividades cotidianas
- ☐ Conocer detalles del incidente
- ☐ Detectar actividades anormales
- ☐ Detectar posibles cambios no autorizados



# Contención, erradicación y recupero

## CONTENCIÓN

Evitar que el incidente siga produciendo daños.

## ERRADICACIÓN

Eliminar la causa del incidente y todo rastro de los daños.

## RECUPERO

Volver el entorno afectado a su estado original.

Incidente: infección con gusano

**Contención:** Desconexión del equipo afectado de la red.

**Erradicación:** detectar el código malicioso y eliminarlo del equipo. Instalar parches. Actualizar el software antivirus.

**Recupero:** Corrección de efectos producidos.  
Restauración del backup.

## Recolección de datos

### INFORMACIÓN BASADA EN HOST

- ✓ **Recolección en vivo** Ej.: Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la placa de red.
- ✓ **Duplicación Forense** Ej.: duplicación de discos rígidos, medios removibles, etc.

**INFORMACIÓN BASADA EN LA RED** Ej.: Logs de NIDSs, logs de monitoreo, información recolectada mediante sniffers, logs de routers, logs de firewalls, información de servidores de autenticación

**OTRA INFORMACIÓN** Ej.: Testimonio de personal

## Recolección de evidencia

### AUTENTICIDAD

Quien haya recolectado la evidencia debe poder probar que es auténtica

### CADENA DE CUSTODIA

Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuando la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.

### VALIDACION

Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

# Cadena de Custodia

Registro detallado de los movimientos de la evidencia durante su procesamiento judicial o extrajudicial.

Chain of Custody			
<i>From</i> <i>Location</i>	<i>Date</i>	<i>Reason</i>	<i>To</i> <i>Location</i>
<i>From</i> <i>Location</i>	<i>Date</i>	<i>Reason</i>	<i>To</i> <i>Location</i>
<i>From</i> <i>Location</i>	<i>Date</i>	<i>Reason</i>	<i>To</i> <i>Location</i>
<i>From</i> <i>Location</i>	<i>Date</i>	<i>Reason</i>	<i>To</i> <i>Location</i>
<i>From</i> <i>Location</i>	<i>Date</i>	<i>Reason</i>	<i>To</i> <i>Location</i>
<i>From</i> <i>Location</i>	<i>Date</i>	<i>Reason</i>	<i>To</i> <i>Location</i>
<i>Final Disposition of Evidence</i>		<i>Date</i>	

## Características:

- **Volatilidad**
- **Posibilidad de crear copias idénticas**
- **Copias no autorizadas sin dejar rastros**

Puede estar almacenada en una gran cantidad de dispositivos:

- RAM, discos rígidos, Pendrives
- Cámaras fotográficas digitales
- Reproductores de MP3
- smartphone
- Impresoras

2002: RFC 3227

Guidelines for Evidence Collection and Archiving

2004: Forensic Discovery

Dan Farmer y Wietse Venema

2006: NIST Special Publication 800-86

Guide to Integrating Forensic Techniques into Incident Response

Principio de Incertidumbre de Heisenberg



# Orden de volatilidad

## RFC 3227

- Registers, cache
- Network status
- Process information
- Main memory
- Temporary file systems
- Disk
- Remote logging and monitoring data that is relevant to the system in question
- Physical configuration, network topology
- Archival media

## Forensic Discovery

- Registers, peripheral memory, caches, etc.
- Main memory
- Network status
- Process information
- Disk
- Floppies, backup media, etc.
- CD-ROMs, printouts, etc.

## NIST SP 800-86

- Network status
- Login sessions
- Main memory
- Process information
- Open files
- Network configuration
- Operating system time

# Recolección en vivo – cosas a tener en cuenta

- **No apagar el equipo hasta que se realizaron las tareas de recolección en vivo, ni desloguearse del usuario. Utilizar runAs.**
- **No confiar en las herramientas del equipo. Utilizar herramientas de recolección desde medios protegidos (ej:cd-rom) y preferentemente linkeadas estáticamente.**
- **No utilizar programas que modifiquen los MAC times de los archivos (tar, winzip)**
- **Igualmente, la información recolectada puede ser falsa o se pueden estar ocultando cosas.**

# Recolección en vivo

## U N I X

**Hostname**

**df**

**date**

**Last**

**who**

**ifconfig**

**ps**

**lsof**

**Netstat**

**Arp**

**Nc**

**dd**

**TCT grave-robber**

## W I N D O W S

**Date**

**Psloggedon**

**Logonsessions**

**Openfiles**

**Netstat**

**Nbstat**

**Pstlist**

**Listdlls**

**Fport**

**Ipconfig**

**Pclip**

**autoruns**

# Herramienta automatizada para windows

## •Windows Forensic Toolchest (WFT)



Windows Forensic Toolchest™ (WFT) - Microsoft Internet Explorer -- Copyright © 2007 Monty McDougal

File Edit View Favorites Tools Help

**Fool Moon**  
Software & Security

**Windows Forensic Toolchest™ (WFT)**

Version 3.0.01

Main Log Config File Hashes Tools Security Resources About

**START**

START TIME

**MEMORY**

DD MEMORY DUMP  
DD STRINGS  
PCCLIP  
MEM P  
MEM D

**MAC TIME**

LAST ACCESSED S  
LAST CREATED S  
LAST MODIFIED S  
MAC S

**SYSTEM INFO**

PSINFO  
HOSTNAME  
UNAME  
OS VERSION  
ENVIRONMENT  
UPTIME  
UPTIME  
HISTORICAL  
PSUPTIME  
WHOAMI  
NET DOMAIN  
NET USER

Windows Forensic Toolchest™ (WFT)

NON-COMMERCIAL USE ONLY

**Main**

**Windows Forensic Toolchest™ (WFT)**

The Windows Forensic Toolchest™ (WFT) was written to provide an automated incident response [or even an audit] on a Windows system while collecting security-relevant information from the system. WFT is essentially a forensically enhanced batch processing shell, capable of running other security tools and producing HTML based reports in a forensically sound manner.

**System Information**

System Name: MONTY-LAPTOP  
Operating System: Microsoft Windows XP Workstation 5.1 Service Pack 2 (Build 2600)  
User Name: mmtcdoug  
Windows Directory: C:\WINDOWS  
System Directory: C:\WINDOWS\system32  
System Date/Time: 06/01/2007 15:10:53 (24h)

**Case Information**

Investigator Name: Monty  
Case ID: Test

System: MONTY-LAPTOP (mmtcdoug) (Monty) Date/Time: 06/01/2007 15:10:53 (24h)

Windows Forensic Toolchest™ (WFT) v3.0.01 Copyright © 2003-2007 Monty McDougal. All rights reserved.

# Modificación de la RAM

Action	% RAM unchanged	
	256 MB RAM	512 MB RAM
Start	100.0	100.0
Idle for 1 hour	90.4	96.7
Idle for 2 hours	79.7	96.1
run dd from Helix CD	76.9	89.8
Idle for 15 hours	74.8	85.6
run WFT from Helix CD	67.2	69.4

Fuente: <http://www.komoku.com/forensics/basic/bh-fed-07-walters-paper.pdf>

**Formato DD:** Copia bit a bit

**Formatos comerciales:** Incluyen metadata del caso, hashes, pueden marcar sectores defectuosos, partir la imagen en pedazos y comprimir, etc. Ej: Expert Witness Format

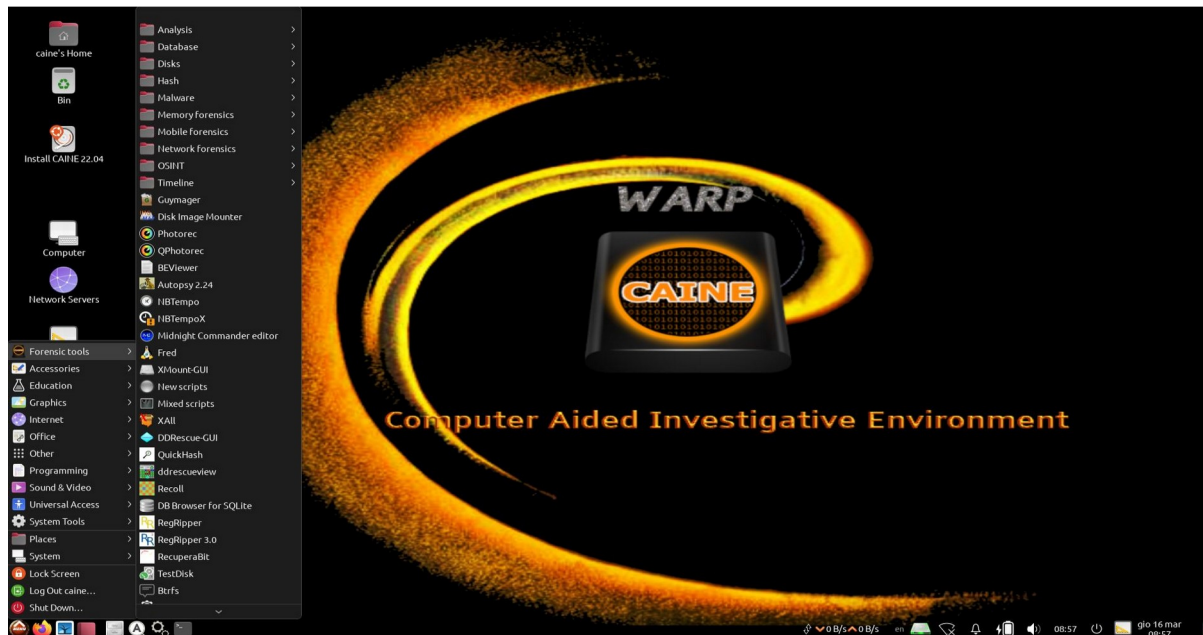
**AFF (Advanced Forensic Format):** Formato libre que brinda las funcionalidades de los formatos propietarios.

# LiveCDs para recolección y análisis

**CAINE** (<http://www.caine-live.net>)

**SIFT** (<https://digital-forensics.sans.org/community/downloads>)

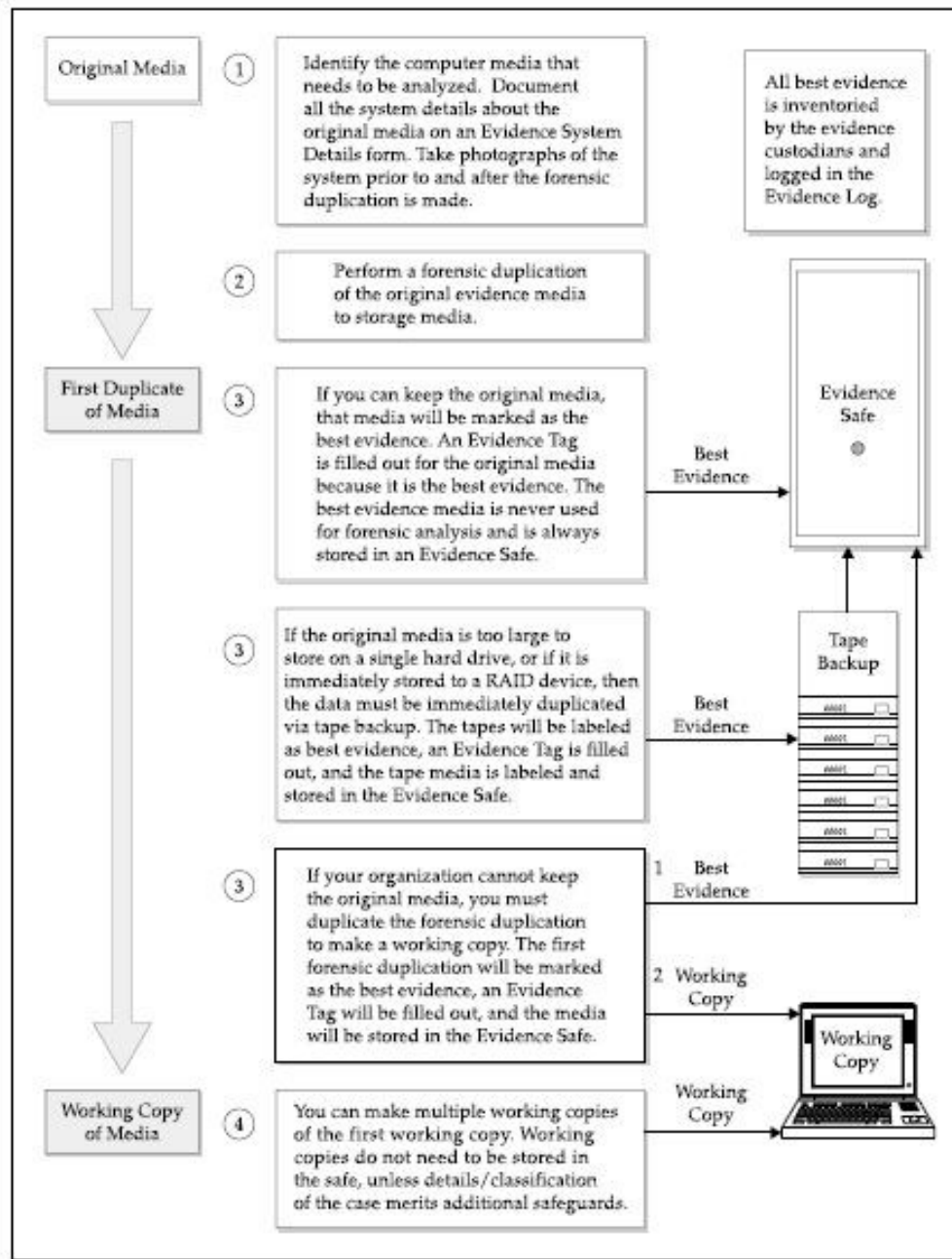
**TSURUGI** (<https://tsurugi-linux.org/>)



# Bloqueo de escritura de disco







**Fuente:**

Incident Response And Computer Forensics, 2<sup>nd</sup> edition, Mandia, Prosis, Pepe.

# Análisis

# Esto no es una pipa!



**“Forensic Discovery”**, Dan Farmer & Wietse Venema

<http://www.porcupine.org/forensics/forensic-discovery/>

**SEGURIDAD DE LA INFORMACION**

Se analiza información de los sistemas comprometidos.

¿Cómo sabemos que la información es confiable?  
¿Estamos viendo pistas de lo que realmente ocurrió, o estamos viendo pistas falsas puestas por el atacante?

# Busqueda de consistencia

```
May 25 10:12:46 spike telnetd[13626]: connect from hades
wietse ttyp1 hades Thu May 25 10:12 - 10:13 (00:00)
  hostname wietse ttyp1 0.00 secs Thu May 25 10:12
  sed wietse ttyp1 0.00 secs Thu May 25 10:12
  stty wietse ttyp1 0.00 secs Thu May 25 10:12
  mesg wietse ttyp1 0.00 secs Thu May 25 10:12
  . . . . .
  ls wietse ttyp1 0.00 secs Thu May 25 10:13
  w wietse ttyp1 0.00 secs Thu May 25 10:13
  csh wietse ttyp1 0.03 secs Thu May 25 10:12
  telnetd root __ 0.00 secs Thu May 25 10:12
wietse ttyp1 hades Thu May 25 10:12 - 10:13 (00:00)
```

**Atime** refiere a la última vez que un archivo o directorio fue accedido.

**Mtime** indica la fecha de modificación del contenido del archivo.

El atributo **Ctime** indica cuando se modifica el contenido o la información relacionada con permisos, dueño, grupo, etc.

Se pueden hacer líneas de tiempo para ver que archivos se accedieron, modificaron, etc.

# Actividad de acceso a archivos

	<b>www.things.org</b>	<b>www.fish.com</b>	<b>news.earthlink.net</b>
Over a year:	76.6 %	75.9 %	10.9 %
6 months-year:	7.6 %	18.6 %	7.2 %
1-6 months:	9.3 %	0.7 %	72.2 %
Day-month:	3.6 %	3.1 %	7.4 %
Within 24 hrs:	2.9 %	1.7 %	2.3 %

Porcentaje de archivos leídos o ejecutados recientemente por algunos servidores de internet.

Fuente: Forensic discovery

- **20 de Agosto de 2001:**
  - En Barney – equipo Linux – se encuentra un demonio SSH ejecutandose en un puerto inusual.
  - El administrador crea un backup de todo el sistema.
- **23 de Agosto de 2001:**
  - El equipo de seguridad pone a Barney en cuarentena.
  - Usa el Coroner's toolkit en el disco rígido



- Herramienta mactime (TCT) revela tiempos MAC
- Alternativamente se puede invocar la llamada a sistema lstat():

```
( $dev, $inode, $mode, $nlink, $uid, $gid, $rdev,  
  $size, $atime, $mtime, $ctime, $blksize, $blocks)  
    = lstat($filename);  
print "$filename (MAC): $mtime,$atime,$ctime\n";
```

# Historia de Barney: Salida MAC

Jul 19 2001

time	size	MAC	permissions	owner	file name
----	----	---	-----	-----	-----
16:47:47	655360	m..	-rw-r--r--	root	/usr/man/.s/sshdlinux.tar
16:48:13	655360	..c	-rw-r--r--	root	/usr/man/.s/sshdlinux.tar
16:48:16	395	..c	-rwxrw-r--	2002	/usr/man/.s/ssh.sh
	880	..c	-rw-r--r--	2002	/usr/man/.s/ssh_config
	537	..c	-rw-----	2002	/usr/man/.s/ssh_host_key
	341	..c	-rw-r--r--	2002	
/usr/man/.s/ssh_host_key.pub	1024	m.c	drwxr-xr-x	16:48:20	
root					/usr/man/.s
16:51:31	1024	m.c	drwxr-xr-x	root	/home
	1422	m.c	-rw-r--r--	sue	/home/sue/.Xdefaults
	24	m.c	-rw-r--r--	sue	/home/sue/.bash_logout
	230	m.c	-rw-r--r--	sue	/home/sue/.bash_profile
	124	m.c	-rw-r--r--	sue	/home/sue/.bashrc
16:57:57	1024	m.c	drwx-----	sue	/home/sue
	9	m.c	-rw-----	sue	/home/sue/.bash_history

## **19 de Julio de 2001:**

- Usuario con privilegios de root crea y desempaqueta un archivo tar.
- Los nombre de archivos indicarían que es un reemplazo del SSH.
- El archivo es ubicado en un directorio con un nombre sospechoso: “.s”
- El usuario Sue se desloguea.

- Se ordena la salida de mactime según la fecha de acceso.
- Los a-times se perdieron porque el backup que hizo el administrador cambió los valores al momento del backup.
- Hacer el backup fue una práctica forense pobre y destruyó evidencia.

- **Audit Record Generation and Utilization System (ARGUS) estaba corriendo.**
- **Se analizaron los logs de ARGUS**
  - Buscando conexiones al demonio SSH de Barney
    - TCP 33332
  - Mecanismo de transporte de archivo TAR

# Historia de Barney: log de ARGUS

Jul 19 2001

start	end	proto	source	destination
-------	-----	-------	--------	-------------

status

=====

=====

16:30:47-16:47:16	tcp	10.0.0.1.1023	192.168.0.1.33332	
-------------------	-----	---------------	-------------------	--

sSEfC

# Historia de Barney: log de ARGUS

Jul 19 2001

16:28:34-16:29:36 tcp 192.168.0.1.1466 10.0.1.1.21  
sSEfC

16:29:30-16:29:36 tcp 10.0.1.1.20 192.168.0.1.1467  
sSEfC

16:30:47-16:47:16 tcp 10.0.0.1.1023 192.168.0.1.33332  
sSEfC

- **Observaciones:**
  - La diferencia horaria entre Barney y los logs de ARGUS era de aprox. 17 minutos.
  - La dirección IP 10.0.1.1 es sospechosa
    - Buscar más entradas de esta dirección



# Historia de Barney: log de ARGUS

Jul 19 2001

16:25:32	tcp	10.0.0.1.44445	192.168.1.1.110	s
16:25:49	tcp	10.0.0.1.44445	192.168.0.1.110	sR
16:25:53-16:30:26	tcp	10.0.0.1.44445	192.168.0.1.21	sSEfR

- **Notar el uso de puertos inusuales**
- **La conexión no fue terminada correctamente.**
- **Buscar ese número de puerto**

# Historia de Barney: log de ARGUS

Aug 21-22 2000

23:59:55-00:29:48 tcp 10.0.3.1.1882 192.168.0.1.53  
sSEfR

Aug 22 2000

00:08:32-00:09:04 tcp 192.168.0.1.1027 10.0.2.1.21  
sSEfC

00:08:42-00:09:04 tcp 10.0.2.1.20 192.168.0.1.1028  
sSEfC

00:11:08-00:13:26 tcp 192.168.0.1.1029 10.0.2.1.21  
sSEfC

00:12:07-00:12:13 tcp 10.0.2.1.20 192.168.0.1.1030  
sSEfC

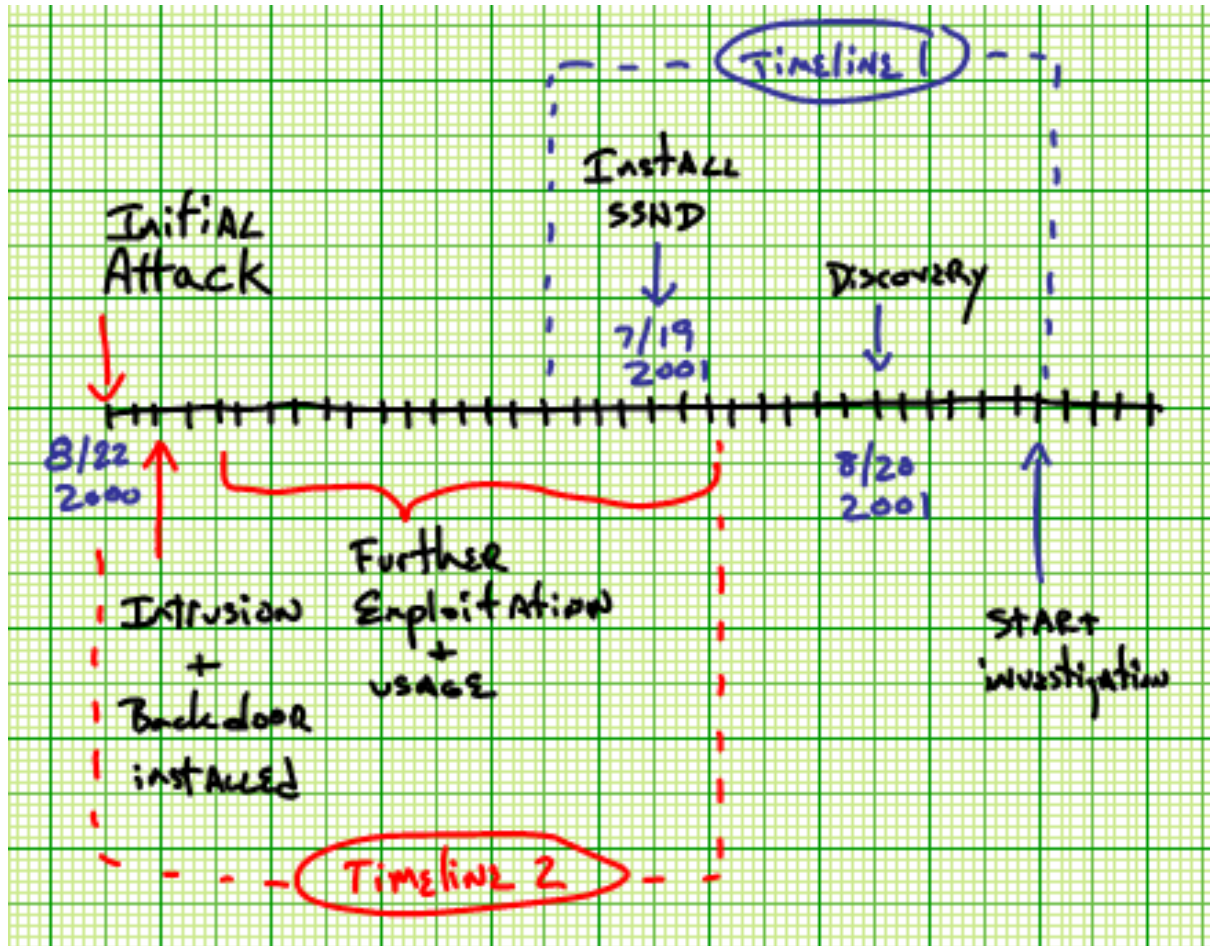
00:13:38-00:13:35 tcp 10.0.2.1.44445 192.168.0.1.21  
sSEfR

# Historia de Barney

- Aparentemente, el servidor de DNS de Barney fue atacado exitosamente desde 10.0.3.1
- El intruso uso ftp para instalar herramientas desde 10.0.2.1
- El intruso prueba un backdoor usando TCP/44445

- **Revisando nuevamente los tiempos MAC en Barney, este escenario fue confirmado.**
  - Aparentemente, Barney fue atacado exitosamente el 21 de agosto de 2000.
    - El atacante instaló un backdoor simple.
  - En Julio de 2001, se instaló un demonio SSH
  - El SSH es levantado en Agosto de 2001

# Historia de Barney



- Visualización de contenido de archivos, imágenes, emails, registro de windows, etc
- Búsqueda de cadenas
- OCR
- Historial de navegación
- Recuperación archivos borrados y File Carving
- Líneas de tiempo
- Identificación de archivos conocidos (<http://www.nsrl.nist.gov>)

**TCT (The Coroner's Toolkit, historico)**

**Sleuthkit & Autopsy**

**EnCase Forensics**

**FTK**

**Magnet Axion**

## Data Collection

### Network-Based Evidence

- Obtain IDS Logs
- Obtain Existing Router Logs
- Obtain Relevant Firewall Logs
- Obtain Remote Logs from a Centralized Host (SYSLOG)
- Perform Network Monitoring
- Obtain Backups

### Host-Based Evidence

- Obtain the Volatile Data during a Live Response
- Obtain the System Time
- Obtain the Time/Date Stamps for Every File on the Victim System
- Obtain all Relevant Files that Confirm or Dispel Allegation
- Obtain Backups

### Other Evidence

- Obtain Oral Testimony from Witnesses

## Analysis

1. Review the Volatile Data.
  - Review the Network Connections.
  - Identify Any Rogue Processes (Backdoors, Sniffers).
2. Analyze the Relevant Time/Date Stamps.
  - Identify Files Uploaded to the System by an Attacker.
  - Identify Files Downloaded or Taken from the System.
3. Review the Log Files.
4. Identify Unauthorized User Accounts.
5. Look for Unusual or Hidden Files.
6. Examine Jobs Run by the Scheduler Service.
7. Review the Registry.
8. Perform Keyword Searches.



# Bibliografía

