Análisis Forense de Sistemas

Rafael Calzada Pradas

Universidad Carlos III de Madrid

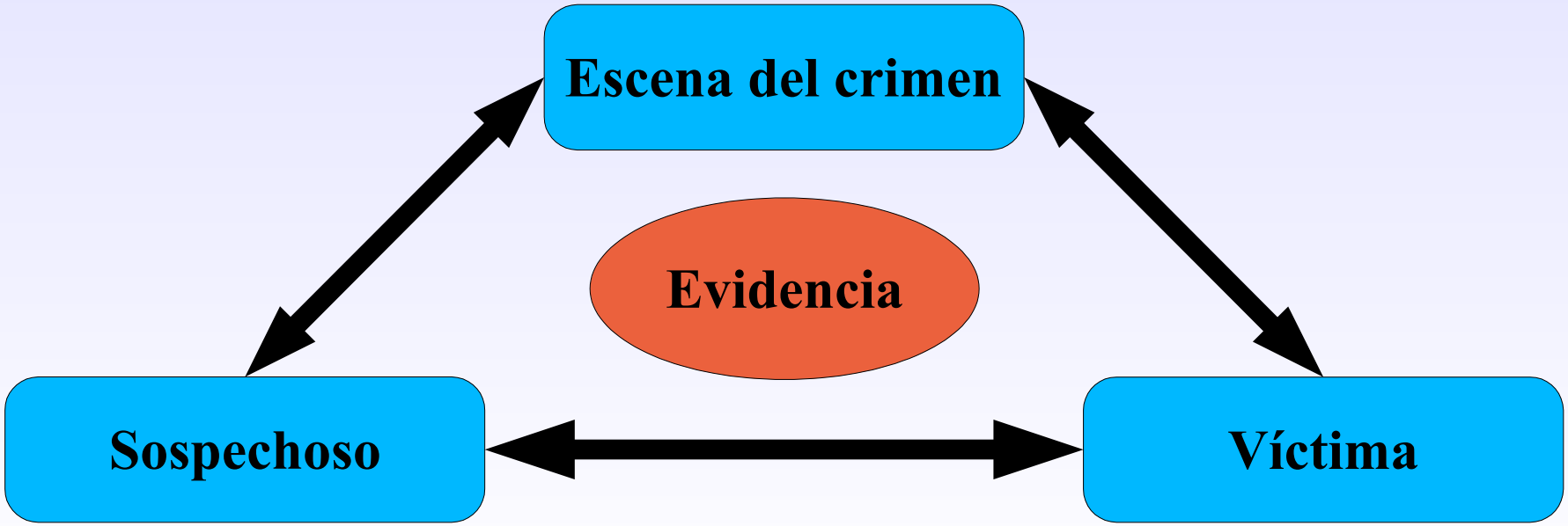
Agenda

- Introducción Teórica
- Aspectos Legales
- Preparación
- Análisis de un sistema Windows 2000
- Análisis de un sistema GNU/Linux
- Conclusiones
- Referencias

Introducción Teórica al Análisis Forense de Sistemas

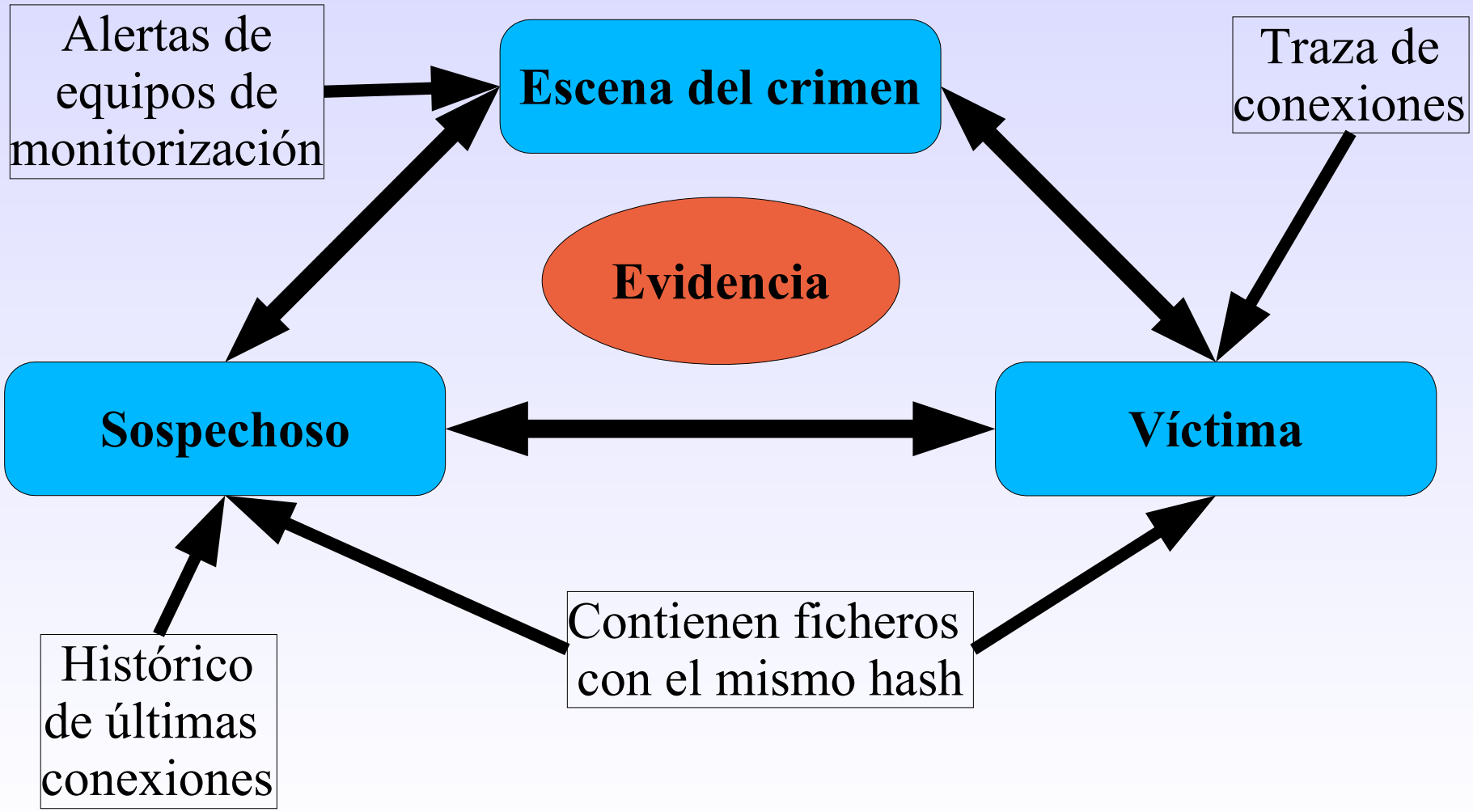
Introducción

- Ciencia aplicada para hallar/descubrir la verdad
- Principio de intercambio de Locard
  Cada contacto deja un rastro



Principio de Locard (versión digital)

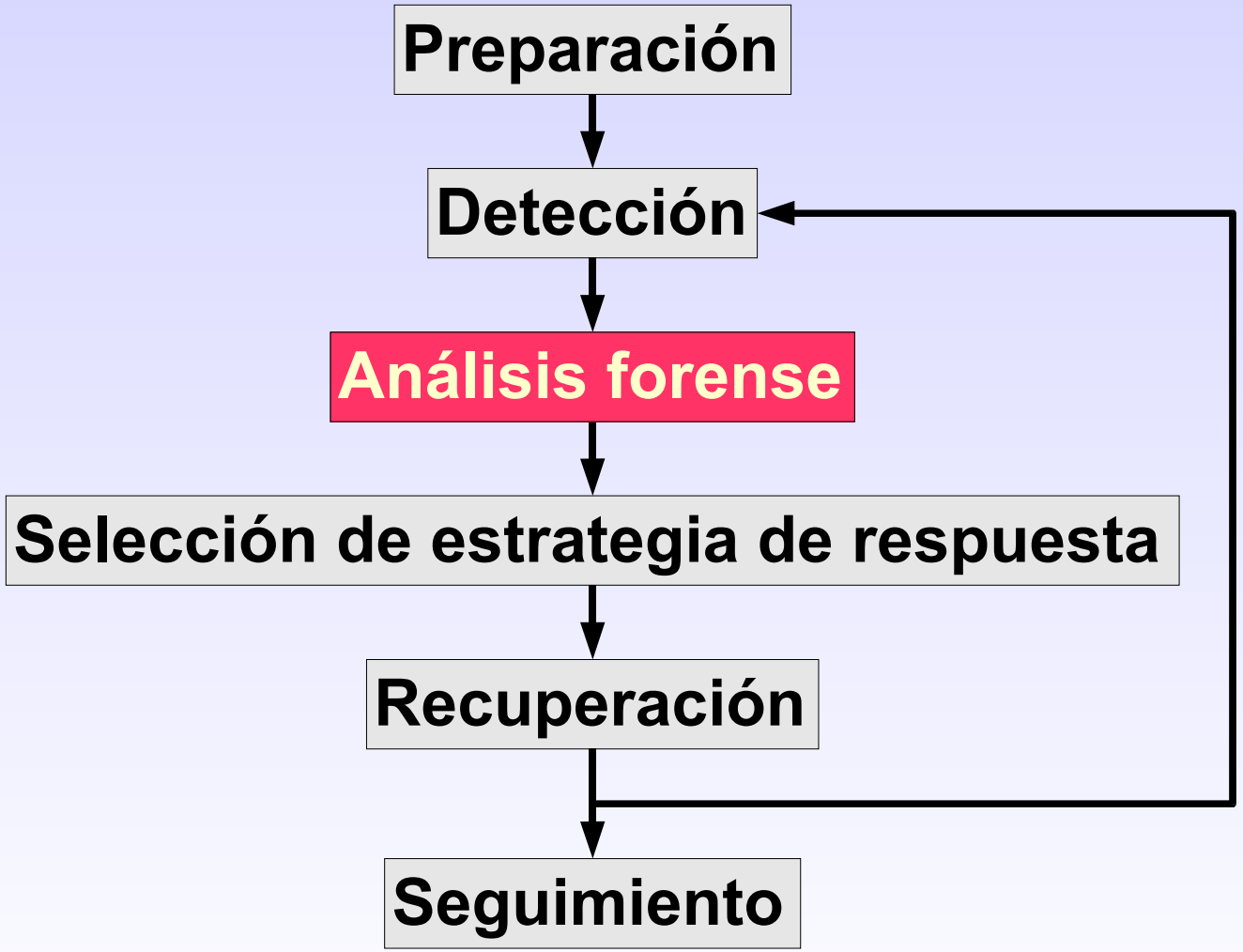
El intruso *sube* herramientas al equipo asaltado



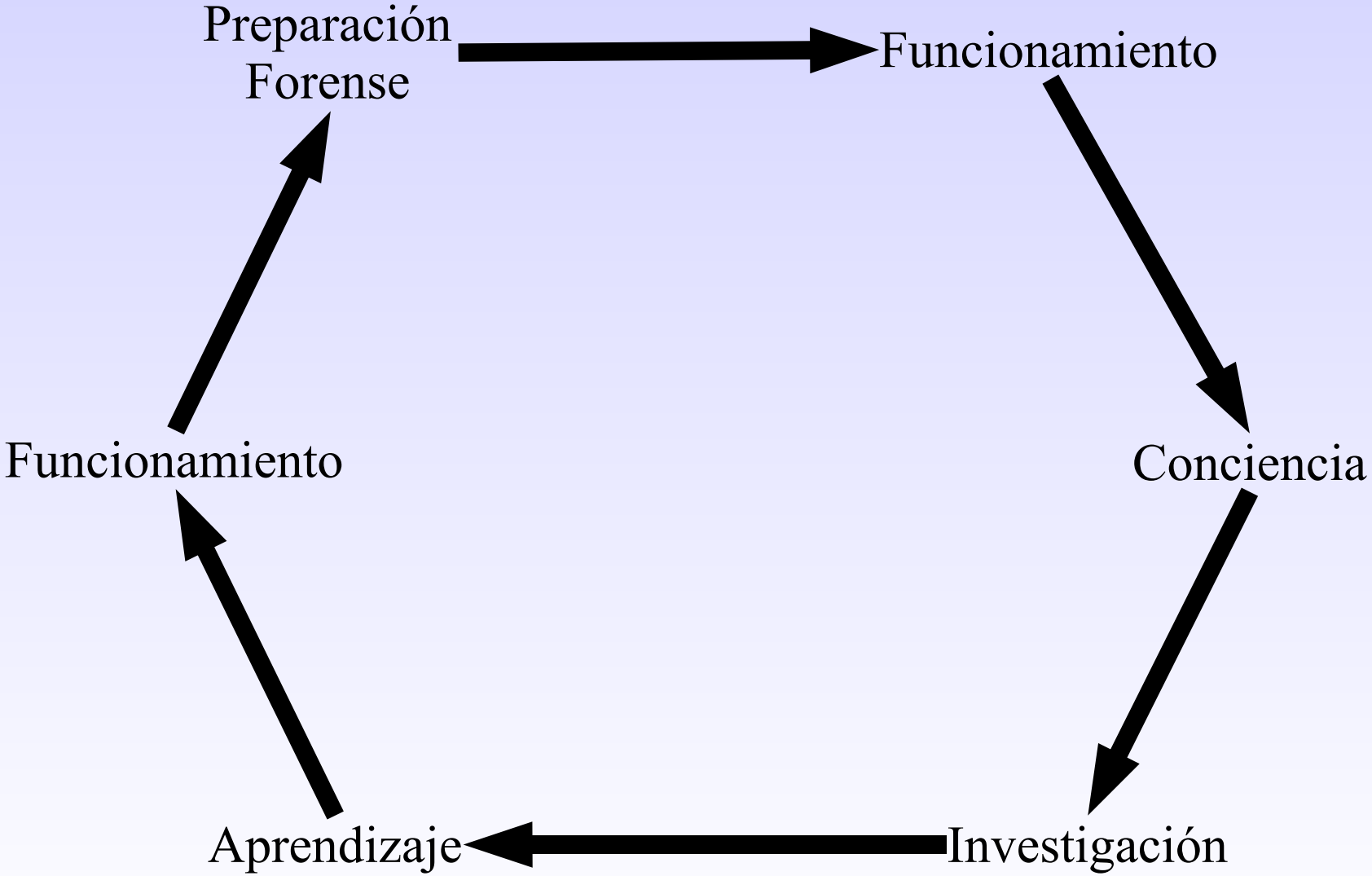
Análisis Forense (versión digital)

- Duplicación exacta de evidencias
- Comprobación de modificación/falsificación de evidencias
- Díficultad de borrado
- Posiblidad de disponer de varias copias de evidencias, para evitar destrucción.

Gestión de incidentes



Ciclo de vida de análisis forense de las evidencias



Objetivos

- Saber que ha sucedido
- Determinar la magnitud del incidente
- Determinar otras entidades implicadas
- Prevenir y mejorar la preparación para incidentes futuros
- Eliminar el riesgo y las posibles responsabilidades
- Si es necesario, denunciar

Fases del Análisis Forense

- Identificación
- Preservación de la evidencia
- Análisis
- Informe

Identificación

- ¿Quién puede recoger las evidencias?
  - Con evidencias físicas, sólo un experto autorizado
  - Con evidencias digitales...
- En España,
  - Hacer la recogida de evidencias de forma metódica
  - Hoja de identificación firmada por testigos, con checksum md5 o sha1
  - Si es caso se preve grave, avisar a las fuerzas del orden

Principio de indeterminación de Heisenberg

- No puedo obtener el estado de un sistema sin alterarlo
  - Tratar de obtener la mayor información posible con el mínimo impacto
- Normalmente el administrador detecta el incidente
  - Cambia contraseñas
  - Reinicia, actualiza, instala, etc
  - La mayor parte de las veces sin éxito
  - Preguntar y anotar todo lo realizado por el administrador

Cadena de confianza

- Los datos serán tan fiables como las herramientas utilizadas para obtenerlos
  - Rootkit no es el final del análisis
- Tener preparado CD y disquete con herramientas *fiables*
  - Permiten eludir rootkits de aplicación
- Nunca descartar rootkits de sistema
  - Pueden aparecer al analizar las evidencias

Sólo tendremos una oportunidad para recoger evidencias

- El responsable del equipo afectado quiere *recuperar* el sistema
- El responsable del servicio quiere *volver* a prestarlo
- El responsable de seguridad/análista necesita tiempo
- Hay que recoger las evidencias
  - Bien
  - A la primera

Aislar la escena

- TODOS son sospechosos
  - Especialmente si es un incidente interno
- Realizar la recogida de evidencias volátiles lo antes posible
  - Evitar que las acciones de terceros puedan alterar el estado del sistema
  - Etiquetar adecuadamente las evidencias

Cadena de custodia

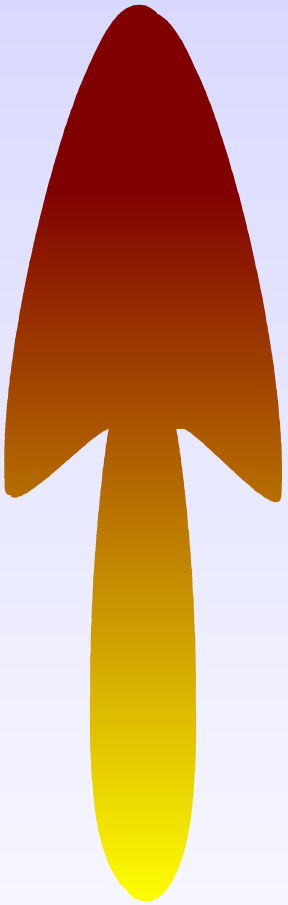
- Definir funciones y responsabilidad de cada miembro del equipo CSIRT
  - Para justificar los accesos a las evidencias
- Importante si el caso terminará en juicio
  - Cada evidencia debe estar etiquetada, incluyendo su checksum MD5 o SHA1
  - Registro de accesos
  - Red aislada para el equipo CSIRT
- Determinar las herramientas a emplear
- Mantener varias copias de las evidencias

Recolección de Evidencias

- No utilizar las herramientas del sistema
  - Podrían haber sido alteradas
- No ser intrusivo
  - Utilizar un CD o disquete con los ejecutables enlazados estáticamente
  - No alterar el contenido del disco
- No instalar programas, ni volcar salida de programas a disco duro
- Utilizar un disquete para almacenar la salida de los programas.

Clasificación de evidencias

- Registros CPU
- Memoria Cache
- Memoria
  - Módulos del SO
  - Controladores dispositivos
  - Programas en ejecución
  - Conexiones activas
- Disco



Volatilidad

Recolección de Evidencias

- Evidencias volátiles
  - Aquellas que se perderán al apagar el equipo
    - Hora del sistema y desfase horario
    - Contenido de la memoria
    - Procesos en ejecución:
      - Módulos/Controladores del Sistema Operativo
      - Programas en ejecución
    - Usuarios conectados
    - Configuración de red
      - Direcciones IP, tabla de rutas, cache arp, etc
      - Conexiones activas, puertos abiertos
    - Hacer checksum de todo, para evitar alteraciones

Recolección Evidencias

- Automatización = Fiabilidad y Rapidez
- Apagado del equipo afectado
  - Sincronizar los discos
  - Apagar *de botón*
    - Ficheros abiertos, pero borrados
    - Es posible que haya scripts para borrar huellas

Recolección Evidencias

- Evidencias no volátiles
  - Aquellas que permanecerán tras apagar el equipo
  - Copiarlas al equipo de análisis
    - De forma local o a través de la red
    - Hacer checksum
  - Nunca
    - Utilizar programas del sistema para hacer la copia
    - Montar los sistemas de ficheros en modo escritura
  - También logs de IDS/Cortafuegos externos

Análisis

El tiempo avanza y es nuestro amigo

- Tratar de correlar eventos
  - Logs del sistema
  - Tiempos MAC de los ficheros
    - Si no han sido alterados, información clave
- Reconstruir la secuencia de comandos ejecutados
- Analizar adecuadamente los programas en entornos seguros

Análisis

- ¿Dónde puede haber información?
  - Archivos normales
  - Archivos temporales
  - Archivos ocultos
  - Archivos borrados
  - Slack space
  - ¿Esteanografía?

Informe

- Características del análisis forense
  - Documentado
  - Reproducible
  - Resultados verificables
  - Independiente
    - Del investigador
    - De las herramientas empleadas
    - De la metodología

Aspectos Legales

Resumen

- *Análisis Forense:* Proceso para identificar, análizar y presentar evidencias digitales, de modo y forma que sean aceptadas en un tribunal
- Claves
  - Minimizar el tratamiento de los datos originales
  - Anotar cualquier cambio
  - Cumplir las reglas de gestión de las evidencias
  - No sobrepasar nuestros propios conocimientos

Admisibilidad de Evidencias Digitales

- Principios generales
  - Las evidencias tienen que ser recogidas de la forma y por el personal autorizados
  - Las evidencias deben ser recogidas de acuerdo a los requerimientos formales, para establecer su fiabilidad
  - Debe respetarse el derecho a la intimidad

Admisibilidad de Evidencias Digitales

- La integridad y autenticidad de las evidencias debe establecerse en el tribunal.
  - Utilizar técnicas y métodos estándarizados para recoger, almacenar y presentarlas
- Las evidencias digitales no son autoexplicativas
  - Es probable que sea necesario un experto para explicarlas

Legislación Aplicable

- Internacional
  - Carta de *Derechos Humanos*
  - Convención Europea sobre *Protección de los Individuos respecto al Tratamiento Automatizado de Datos Personales*
- Supranacional
  - Directiva 95/46EC sobre *Protección de los Individuos respecto al Tratamiento Automatizado de Datos Personales y movimiento de dichos datos*
  - Directiva 97/66EC sobre *Procesamiento de Datos Personales y Protección de la Privacidad en el Sector de las Telecomunicaciones*

Legislación Aplicable

- Nacional
  - Código Penal
    - Título X, Art 197, interceptación de comunicaciones, apropiación de ficheros, etc
- Por ello
  - Ser escrupulosos en los accesos a ficheros/directorios
  - No capturar los campos de datos
  - Contactar con los agentes de la autoridad si prevemos que el caso puede ser llevado a los tribunales
- Puede que los acusados seamos nosotros

Preparación para el Análisis Forense

Hardware (Do-it-yourself)

- Capacidad de proceso:
  - Procesador de última generación
  - 512MB o 1GB de RAM
- Almacenamiento:
  - Sistema (>10GB)
  - Trabajo (>60GB)
  - Grabadora CD/DVD
- Conexiones:
  - IDE
  - SCSI
  - USB
  - FireWire
  - Lectores de Tarjetas de Memoria
  - FastEthernet
- Portátil
  - Disco USB/FireWire

Hardware/Software (preinstalado)

- FREDDIE
  - $6,999.00

Software (Do-it-yourself)

- En la estación de análisis:
  - Linux
    - RAID, LV, loopback
    - ext2, fat, ntfs, etc
    - 802.1q e iptables
    - cloop
  - Autopsy
  - Vmware
  - runefs
- En equipo móvil
  - Linux
    - 2 ó 3 Ethernets
    - 802.1q, bridge e iptables
    - ext2, fat, ntfs, etc
  - Software
    - tcpdump/ethereal
    - FIRE

VMware

- Emulador de PC
  - Para plataformas Windows 2k, XP, 2k3 y Linux
  - Snapshot de discos
  - Multiples *equipos virtuales* simultáneos
  - Permite simular equipos afectados
    - Ejecución controlada de programas
    - Control de acceso a red
  - Precio razonable

@Stake Sleuth Kit (TASK) + Autopsy Forensic Browser

- Visualización de ficheros y directorios existentes y borrados
- Acceso a bajo nivel del sistema de ficheros
- Cronograma de actividad del sistema de ficheros
- Clasificación de ficheros
- Búsquedas utilizado expresiones regulares
- Búsquedas en NIST NSRL y Hash Keeper
- Notas del investigador
- Generador de informes
- Analiza imágenes creadas con dd
- Soporta fat, ntfs, ffs, ext2 y ext3
- Muestra los datos en Streams Alternativos de NTFS
- Permite importar eventos de otras herramientas
- Permite organizar los ficheros en función de su tipo

TASK + Autopsy: Limitaciones

- No incorpora duplicación hardware de discos
  - FIRE puede suplir esta limitación
- No soporta particiones swap, ni HFS/HFS+
- Poca capacidad para búsquedas en espacio no utilizado

foremost

- Permite analizar imágenes de discos para
  - Recuperar ficheros/partes de ficheros
  - Se basa en el formato de las cabeceras y finales de fichero
  -

runefs y bmap

- Permiten ocultar información en el sistema de ficheros
  - Runefs: Utiliza asignación de inodos
  - bmap: Utiliza slack-space

Forensic Incident Response Environment (FIRE)

- Distribución live basada en knoppix
  - Adaptada a tareas forenses
- Además incluye herramientas para captura de evidencias volátiles
  - Linux
  - Windows
  - Solaris

Recomendación

De lo que te cuenten
nada creas,
y sólo la mitad
de lo que veas

Análisis de un Sistema Windows 2000

Recogida de evidencias volátiles (FIRE)

- Psinfo
- net accounts
- net file
- net session
- net share
- net start
- net use
- net user
- net view
- arp -a
- netstat -anr
- psloggedon
- procinterrogate -list
- fport /p
- pslist -x
- nbtstat -c
- dir /s /a:h /t:a c:
- dir /s /a:h /t:a d:
- md5sum
  c:/*.*
  c:/winnt/*.*
  c:/winnt/system/*.*
  c:/winnt/system32/*.*
  d:/*.*
  d:/winnt/*.*
  d:/winnt/system/*.*
  d:/winnt/system32/*.*
- at

Recogida de evidencias no volátiles

1. Utilizar hdparm para optimizar acceso a disco
2. Hacer checksum de todas las particiones
3. Copia en equipo forense
    1. Necesitamos abrir el equipo afectado
    2. Necesitamos interfaces compatibles libres
4. Copia en equipo afectado
    1. Necesitamos utilizar un sistema operativo *limpio*
    2. Debe tener conectores para nuestro disco
    3. Nuestro disco debe tener la capacidad suficiente

Recogida de evidencias no volátiles

5. A través de la red
    1. Necesitaremos un sistema operativo *limpio*
        1. Con soporte para adaptador de red
    2. Mediante cable cruzado
    3. O a través de la red
        1. Utilizar cifrado
        2. Configurar ambos equipos en la misma VLAN

Importante hacer checksums de todas las particiones

Análisis

- Metodología espiral
  - Tomar nota de todo aquello que consideremos extraño
    - Servicios cuyo nombre no sea familiar
    - Servicios o controladores con descripción en idioma diferente del idioma del sistema operativo
    - Revisar las evidencias volátiles buscando puertos abiertos y/o procesos extraños
    - Nunca descartar nada
      - rootkit
      - Intruso interno

Ejemplo

- Esbozo de análisis de un sistema Windows 2000

Análisis de un sistema Debian GNU/Linux

Recogida de evidencias volátiles

- Desde un entorno *seguro*
  - FIRE (Forensic Incident Response Environment CD)
  - Discos de arranque, con programas enlazados estáticamente
  - Grabar la sesión, p.e. utilizar *script*

Recogida de evidencias volátiles (FIRE)

- hostname
- /proc/cpuinfo
- df -h
- fdisk -l
- /proc/version
- /proc/cmdline
- env
- who
- ps -efl
- ifconfig -a
- ifconfig -s
- arp -n
- /etc/hosts
- /etc/resolv.conf
- /etc/passwd
- /etc/shadow
- netstat -anp
- netstat -nr
- lsof -P -i -n
- lsof
- /proc/meminfo
- /proc/modules
- /proc/mounts
- /proc/swaps
- /etc/fstab
- /proc/*id_proceso*
- Listado /etc /bin /sbin /usr /var /dev /home /lib
- /dev/kcore debe copiarse de forma manual (cryptcat)
- Incluye chkrootkit

Recogida de evidencias no volátiles

- Igual que en un sistema Windows

Análisis

- Metodología espiral
  - Solicitar ayuda del administrador si no conocemos la distribución
    - Ubicación de logs
    - Aplicaciones/Parches instalados
  - Rootkits al orden del día
    - Muchos necesitan kernel modular
    - Pero otros no

Ejemplo

- Esbozo de análisis de un sistema Debian/GNU Linux