Gestión de Incidentes - Análisis Forense

Gerardo Geis - LPIC1 y 2, CCNA, CCNA-Sec, JNCIA-SSL
Gabriel Silva – CCNA, CCNA Wireless

IBM - Agosto 2011

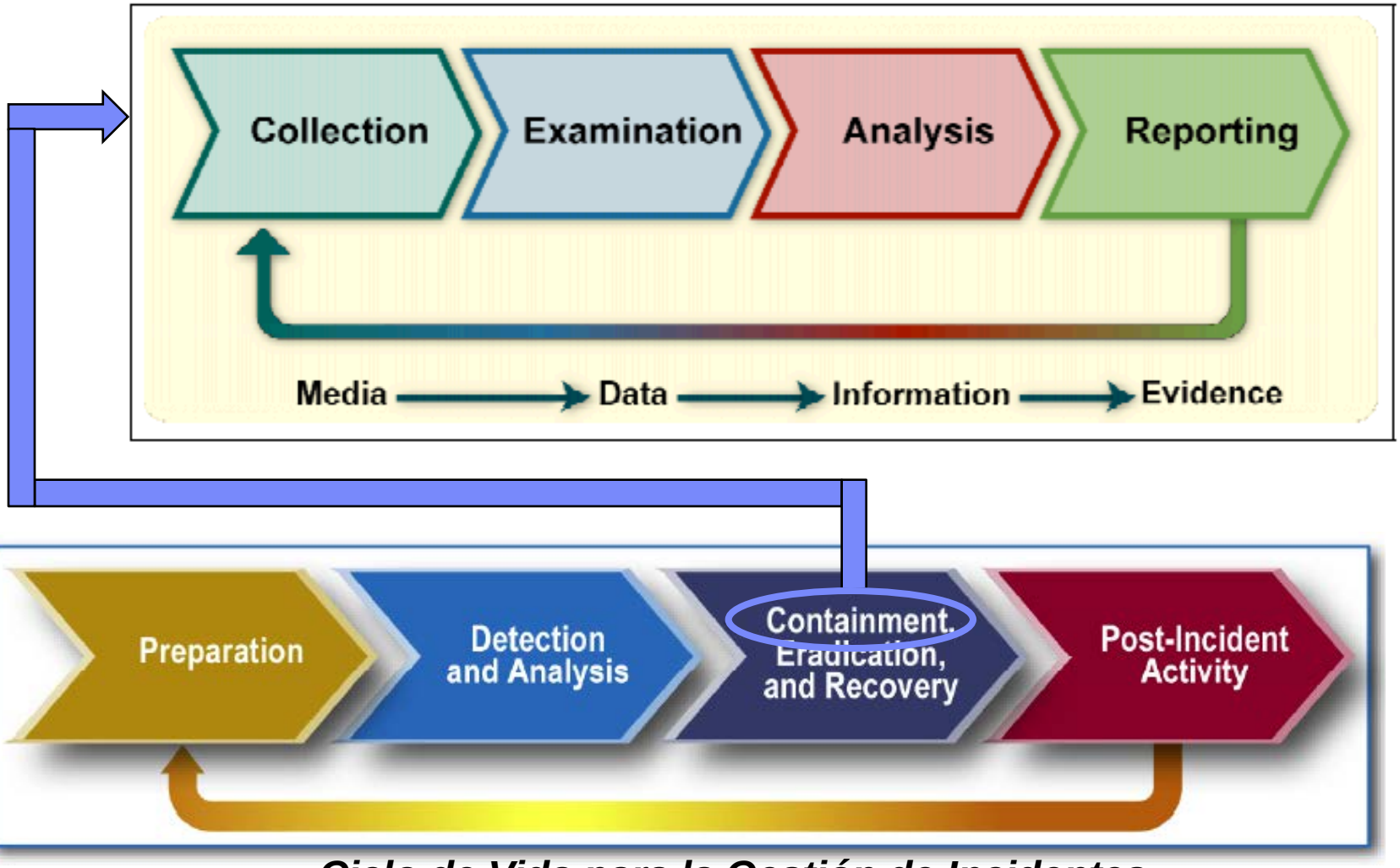
Agenda

Objetivo de la presentación:

- Ciclo de Vida de la Gestión de Incidentes
- Integración de Gestión de Incidentes con Análisis Forense
- Procesos para el Análisis Forense
- Demo

Integración de Gestión de Incidentes con Análisis Forense

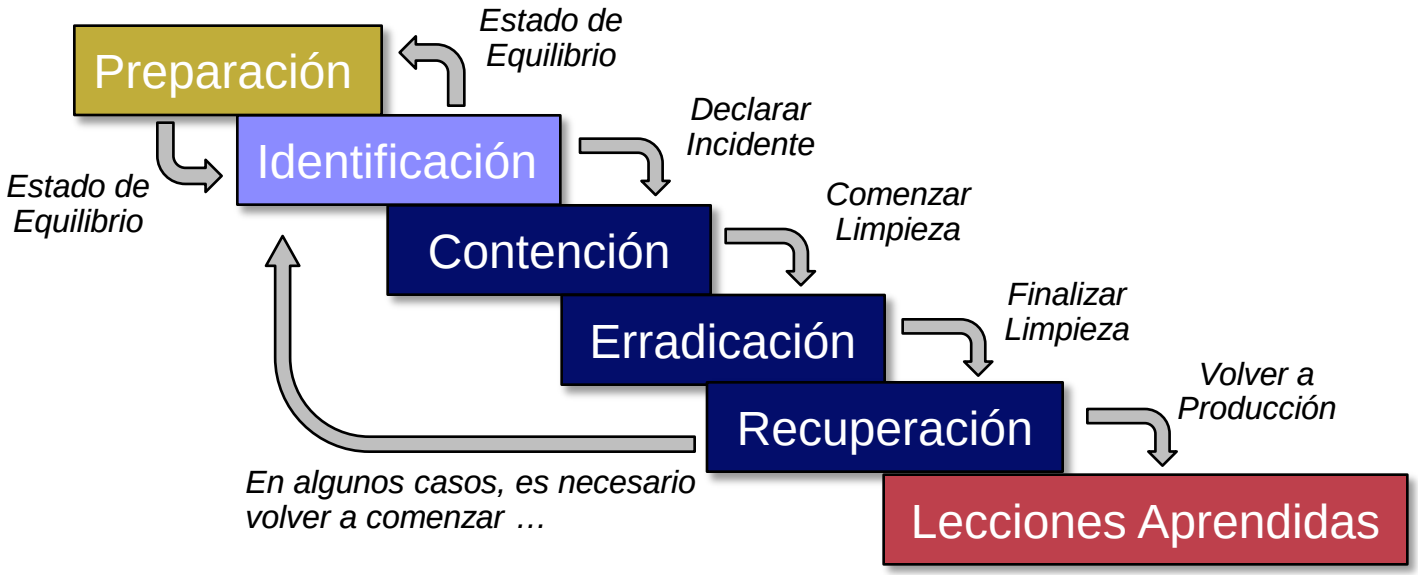
Ciclo de Vida para Análisis Forense

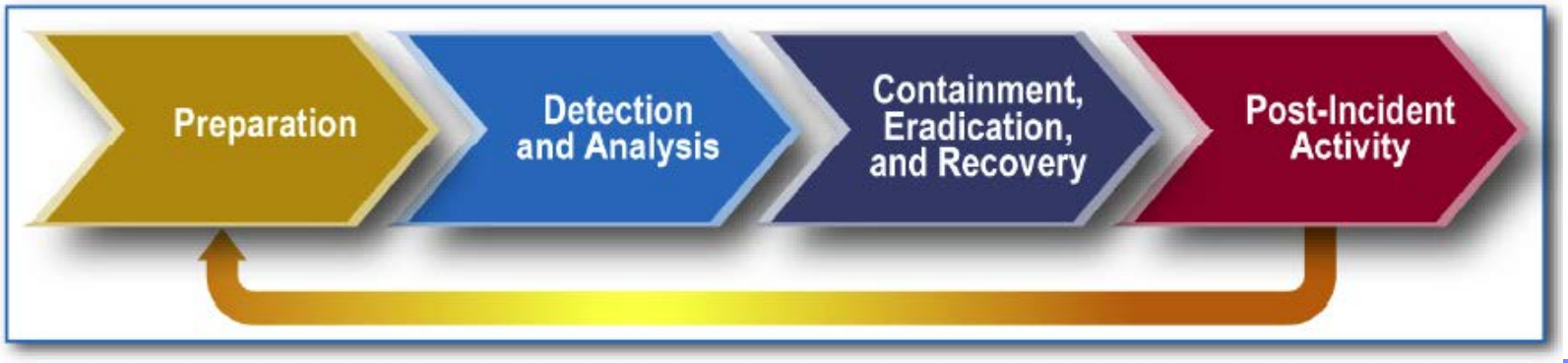


Ciclo de Vida para la Gestión de Incidentes

Gestión de Incidentes

Ciclo de Vida para la Gestión de Incidentes

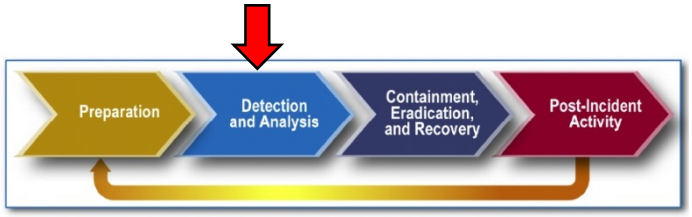




Gestión de Incidentes – Fase Preparación

- ***Organización / Gerencia***: Establecer una capacidad de respuesta a incidentes para que la organización esté preparada para responder a los incidentes.
- ***Marco:*** Establecer Políticas, Guías y Procedimientos de Gestión de Incidentes.
- ***Grupo de Trabajo***: conocimiento profundo, técnicos especializados y una amplia experiencia son necesarias para un análisis adecuado y eficiente de los datos relacionados con el incidente.
- ***Tiempo / SLA***: Establecer una línea base para el tiempo de respuesta
- ***Notificación***: establecer cómo se informa un incidente.
- ***Contacto***: Establecer un punto de contacto principal
- ***Indicadores/Métricas***: Publicar una lista de indicadores de un incidente.
- ***Comunicación***: relaciones con los administradores de sistemas, administradores de red y otras áreas.
- ***Arquitectura de Seguridad***: aseguran que los sistemas, redes y aplicaciones son lo suficientemente seguros.
- ***Herramientas***: adquirir herramientas y recursos que pueden ser de valor en el manejo de incidentes.

Gestión de Incidentes:
Fase Identicación (Detección y Análisis)



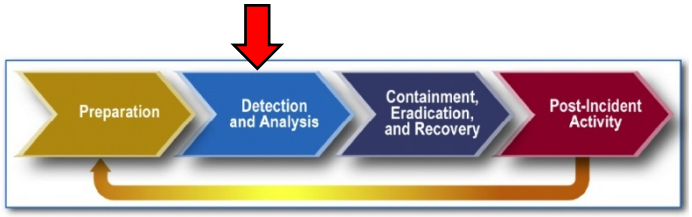
❑ ***Objetivo de la Fase de Identificación :*** consiste en recopilar hechos, analizarlos y determinar si se trata de un incidente. Detectar desviaciones e intentos de ataque.

❑ ***Preguntarse***:

- o ¿Cuánto daño podría ser causado?
- o ¿Cuál es el impacto si se explota la vulnerabilidad?
- o ¿Cuál es el valor de los sistemas afectados?
- o ¿Cuál es el valor de los datos en esos sistemas?
- o ¿Puede ser explota la vulnerabilidad en forma remota?
- o ¿Qué nivel de habilidad y requisitos previos son necesarios por un atacante para explotar la vulnerabilidad?
- o ¿Existe una solución para esta vulnerabilidad?
- o ¿Cuál es la fuente de información que podemos utilizar para el análisis?

❑ ***Responder:*** ¿Quién?, ¿Qué?, ¿Cuándo?, ¿Dónde?, ¿Por qué?, ¿Cómo?

Gestión de Incidentes:
Fase Identicación (Detección y Análisis)



❑ ***Fuente de Información***: eventos y logs generados por distintas fuentes (HIPS, NIPS, SIEM, antivirus, antispyware, chequeo de Integridad, firewalls, aplicaciones y SO), personal, terceros, anuncio vulnerabilidades, etc.

❑ ***Correlación de Eventos***: la recopilación de toda la información disponible de un incidente y validar si el incidente ocurrió.

❑ ***Relojes Sincronizados:*** importante para la correlación de eventos, análisis forense, troubleshooting.

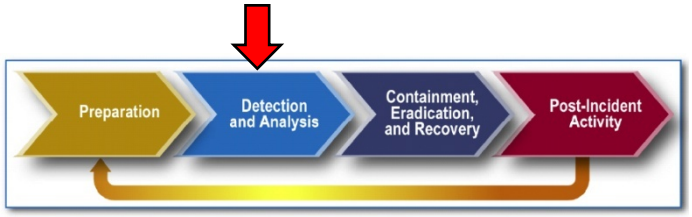
❑ ***Política de Retención de Logs***: implementar consolas centralizadas de eventos /logs y establecer el tiempo de retención de logs.

❑***Comportamiento normal de las redes, sistemas y aplicaciones :*** ayuda a detectar desviaciones de los niveles de actividad esperada.

❑ ***Base de Conocimiento*** : acceso rápido a la información pertinente para el análisis del incidente, como procedimientos, contactos, información histórica, instructivos de trabajo, etc.

❑ ***Matriz de diagnóstico:*** ayudar al personal en la determinación de qué tipo de incidente puede estar ocurriendo. Se enumeran las categorías de incidentes y los síntomas asociados con cada categoría.

Gestión de Incidentes: Fase Identicación (Detección y Análisis)



❑ ***Priorización de incidentes:*** Dar prioridad a los incidentes por el impacto en el negocio, tomando como base la criticidad de los recursos afectados y el efecto técnico del incidente.

Clasificación del Incidente

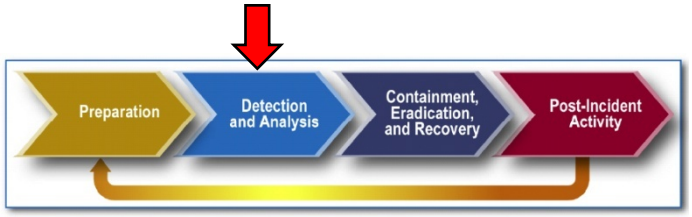
IMPACTO: determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados.

CRITICIDAD: Recursos Afectados

Nivel de Prioridad

URGENCIA: depende del tiempo máximo de demora aceptado por el negocio para la resolución del incidente.

Gestión de Incidentes:
Fase Identicación (Detección y Análisis)



❑ ***Declarar el Incidente:*** se deben establecer guías y procesos que describen la rapidez con que el equipo debe responder a los incidentes y las acciones que deberán llevarse a cabo, en función del impacto del incidente para el negocio.

❑***Tipo de Incidente***: Dado que hemos declarado un incidente, es necesario dejar constancia de su categoría y criticidad (en base a los conocimientos actuales).

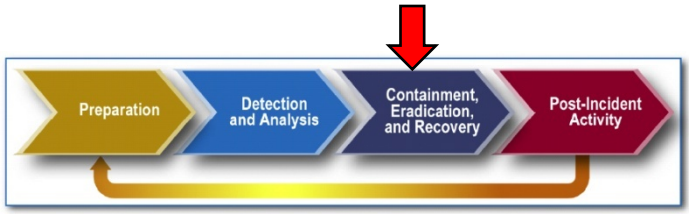
❑ ***Notificación de Incidentes***: las organizaciones deben especificar qué incidentes deben ser informados, cuándo y a quién.

❑ ***Notificación vertical y horizontal***: cuando se declara un incidente, notificar a la dirección y obtener apoyo para ayudar en el proceso de manejo de incidentes. Notificar las unidades de negocio afectadas.

❑ ***Documentación:*** registrar toda la información tan pronto como el equipo sospecha que ha ocurrido un incidente. Cada paso, desde el momento en que se detectó el incidente a su resolución final, deben ser documentados, especificando el tiempo.

❑ ***Proteger los Datos del Incidente***: el equipo debe asegurar que el acceso a los datos de los incidentes se restringe adecuadamente, tanto lógica como físicamente.

Gestión de Incidentes – Fase Contención

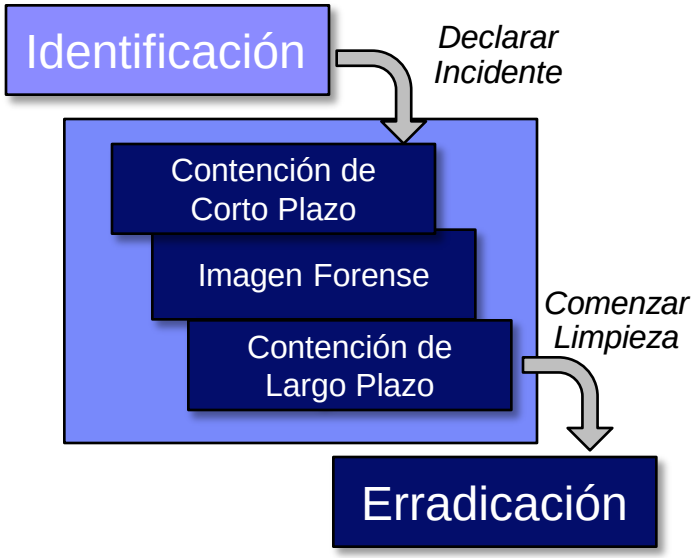


❑ ***Elegir una estrategia de contención:*** actuar rápido y con eficacia para limitar su impacto en el negocio. Las organizaciones deben definir un riesgo aceptable en la contención de los incidentes y desarrollar estrategias y procedimientos.

❑ ***Contención a Corto Plazo***: tratar de impedir que un atacante cause más daño, sin realizar ningún cambio en el sistema afectado .

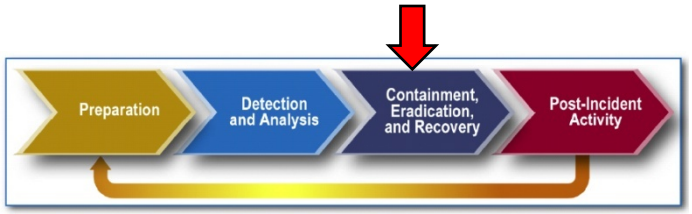
- o cambiar el equipo a otra vlan
- o uso de herramientas de gestión de red, (sniffers)
- o filtros en router o firewalls,
- o cambiar la configuración de DNS
- Notificar dueños de sistemas.

❑ ***Integración con Análisis Forense / Creación de Imágenes:*** crear 2 imágenes Bit a Bit , crear hashes criptográficos de la imagen original y las 2 copias (SHA-1, MD5).

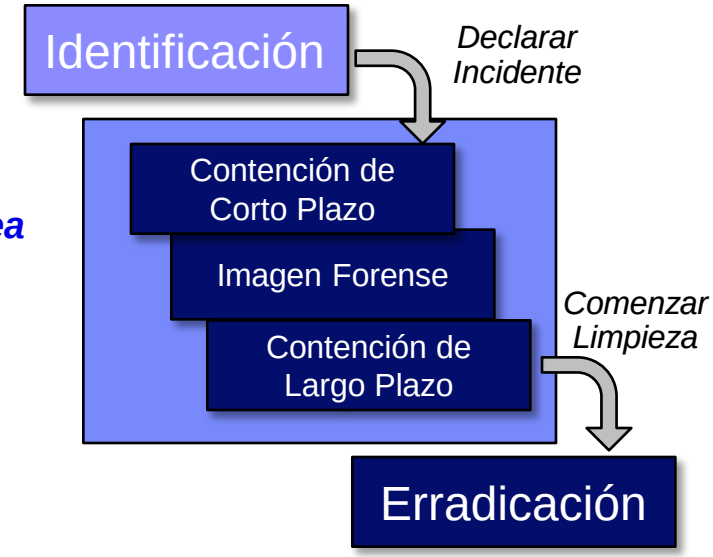


En la Fase CONTENCION se cruza un umbral en el que empezamos a MODIFICAR el sistema.

Gestión de Incidentes – Fase Contención



❑ ***Contención de Largo Plazo:*** una vez que tenemos la copia de seguridad para el análisis forense, podemos empezar a hacer cambios en el sistema.



Situación Ideal: si el sistema se puede mantener ***Fuera de Línea***

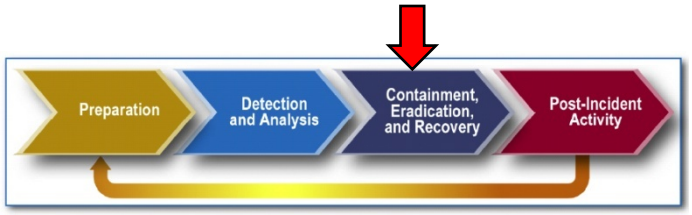
→ ***Fase Erradicación***

Menos Ideal: si el sistema debe ***Continuar en Producción***

→ ***Contención de Largo Plazo (Solución Temporal)***

- *Aplicar Parches*
- *Cambiar Passwords*
- *Aplicar ACLs en Routers y Firewalls*
- *Remover cuentas del atacante*
- *Bajar procesos relacionados con Backdoors.*

Gestión de Incidentes – Fases Erradicación y Recuperación



- ***Erradicación :*** Limpiar y Remover artefactos del Atacante
  - o Determinar la causa del incidente, encontrar el vector de la infección para prevenir una nueva ocurrencia.
  - o Remover código malicioso, cuentas del atacante, etc.
  - o Limpiar/Wiping/Zeroing
  - o Localizar la copia de seguridad limpia más reciente antes del incidente.
  - o Mejora de las defensas
  - o Análisis de Vulnerabilidad (sistema de red).

- ***Recuperación :*** Retornar a Producción
  - o Administradores restauran los sistemas
  - o Fortalecen medidas de seguridad / Hardening
  - o Restauración de los sistemas con backups limpios
  - o Reconstruir los sistemas desde cero
  - o Sustitución de los archivos comprometidos con versiones limpias
  - o Instalación de parches.
  - o Cambio de contraseñas
  - o Testing de servidor
  - o Decisión del dueño para vuelta a Producción
  - o Monitorear el sistema (logs, NIPS, HIPS, integridad de archivos, cuentas utilizadas, cambios en configuración, buscar procesos no autorizados, artefacto del atacante, etc)

Gestión de Incidentes: Post-Incidente

- ***Lecciones Aprendidas : documentar y mejora continua***

  Preguntas a ser respondidas:

  - ¿Exactamente lo que sucedió, y en qué momento?
  - ¿Qué tan bien se realizó la gestión del incidente? ¿Se siguieron los procedimientos documentados?
  - ¿Se tomaron las medidas o acciones adecuadas?
  - ¿Qué se podría realizar diferente?
  - ¿Qué medidas correctivas pueden evitar incidentes similares en el futuro?
  - ¿Qué herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro?

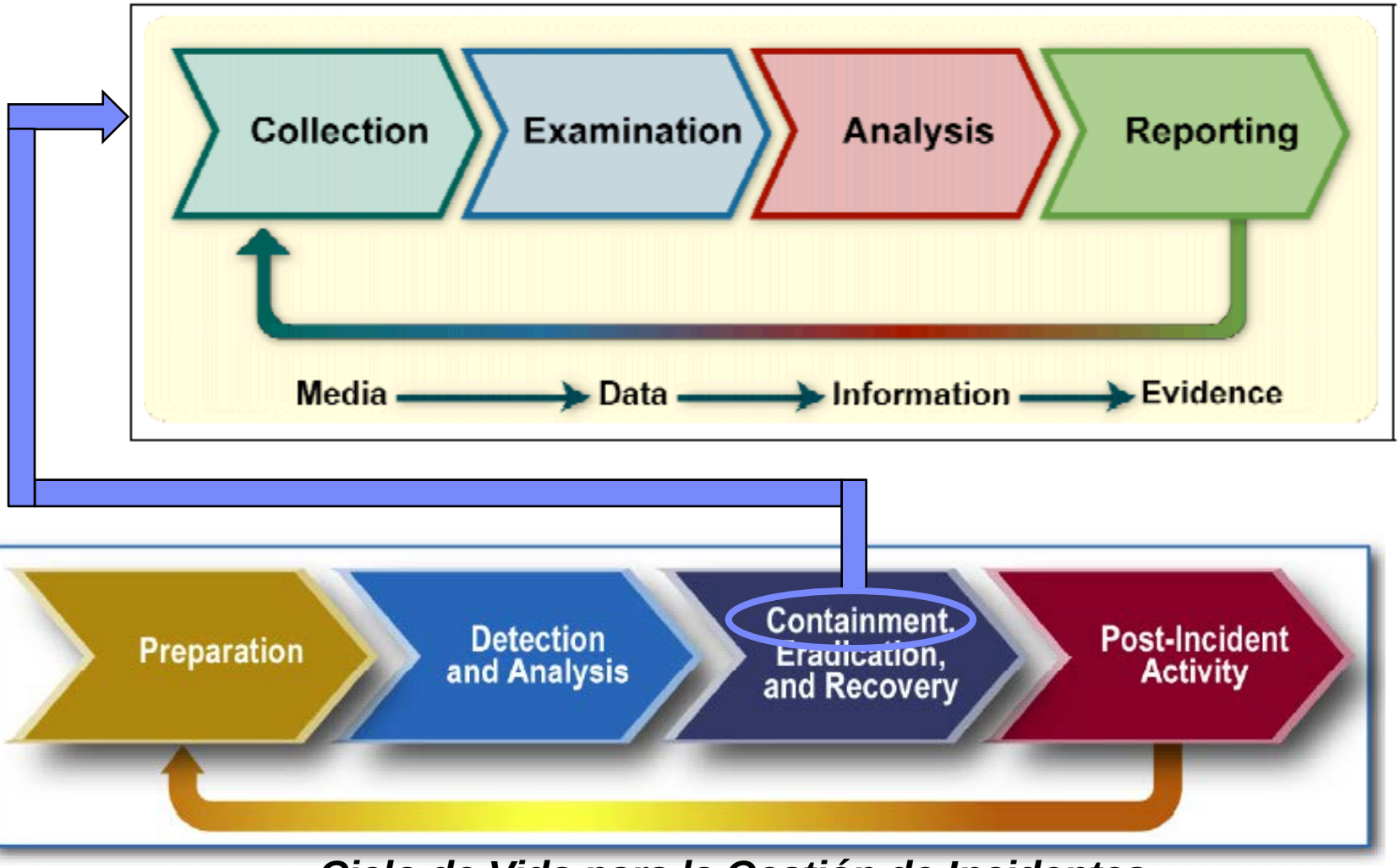
- ***Actualizar :*** políticas, procedimientos, guías, instructivos de trabajo.

- ***Métricas:***

  - Medir el éxito del grupo de respuesta a incidentes
  - Número de incidentes atendidos
  - Tiempo dedicado por Incidente

Integración de Gestión de Incidentes con Análisis Forense

Ciclo de Vida para Análisis Forense



Ciclo de Vida para la Gestión de Incidentes

Análisis Forense

Informática, Cómputo o Análisis Forense

- ***Objetivo:*** Identificar, asegurar, extraer, analizar y presentar pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.

- ***Tareas:*** Identificación de una actividad ilegal, obtención de evidencia, mantener cadena de custodia, preservación de la evidencia, investigación de la evidencia, presentación de resultados.

- ***Comunicación con otras áreas:***

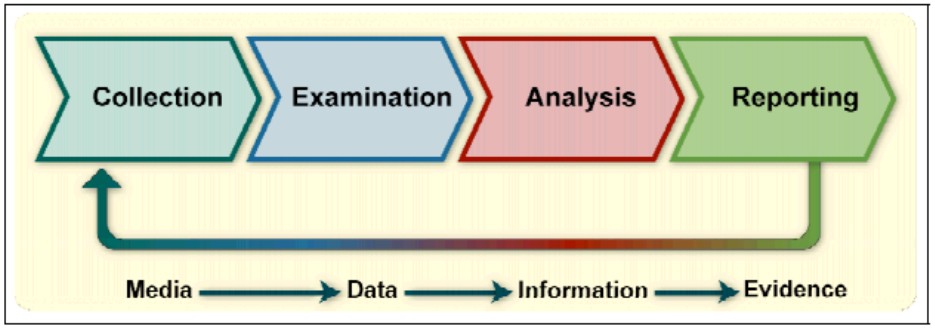
  - Administradores y Operadores de Sistemas
  - Departamento Legal
  - Departamento de Recursos Humanos
  - Auditores
  - Personal de seguridad física

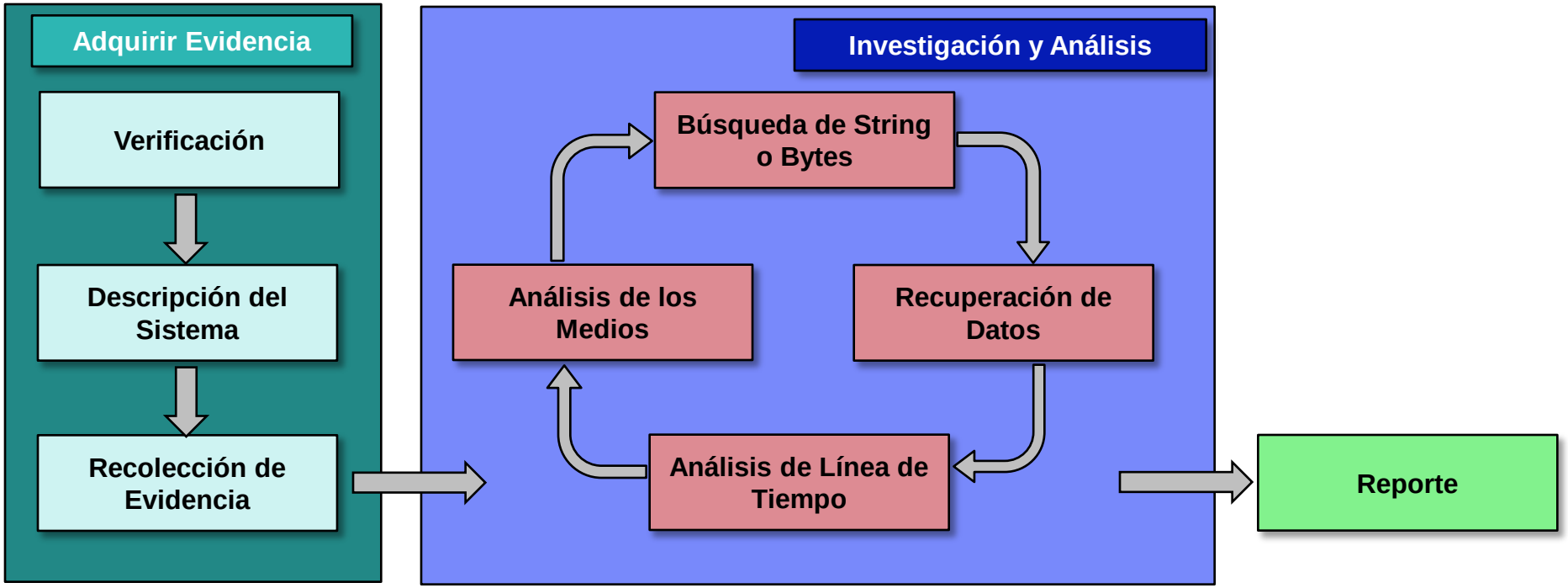
- ***Aplicabilidad :***

  - Operaciones / Troubleshooting
  - Monitoreo de Logs
  - Recuperación de Datos
  - Borrado de Información
  - Cumplimiento Regulatorio
  - Gestión de Incidentes

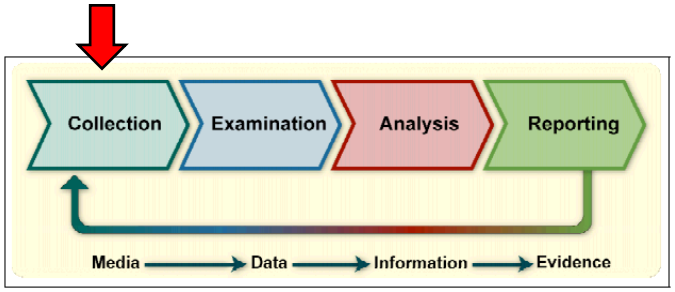
- ***Conocimiento Técnico***: Especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido.

Análisis Forense

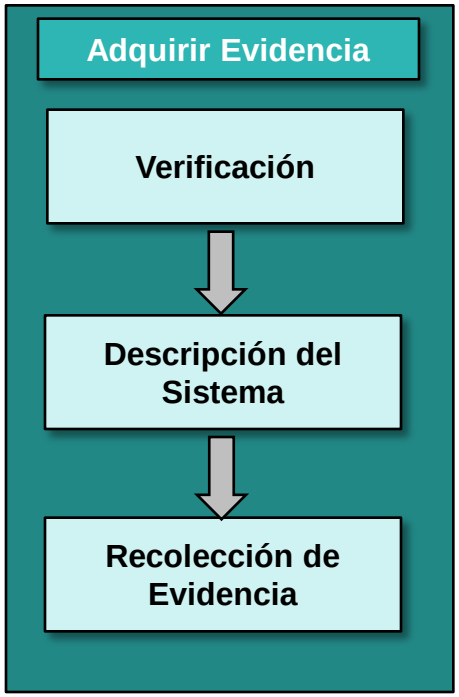




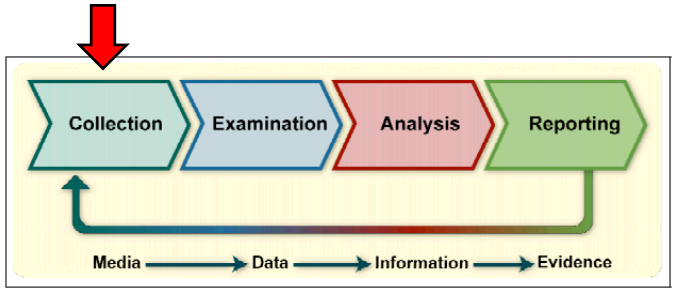
Análisis Forense – Adquirir Evidencia



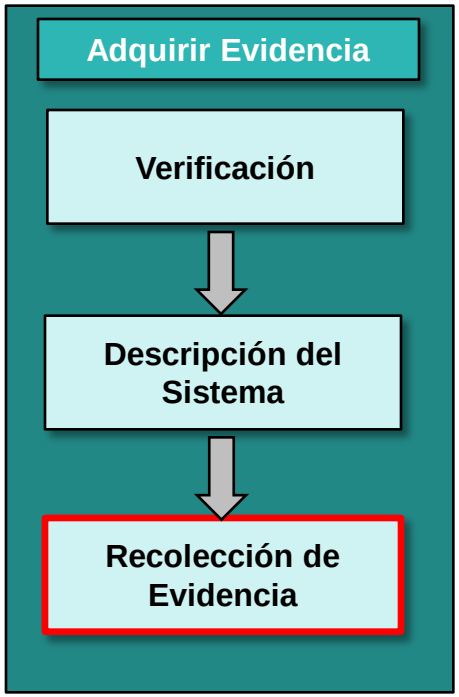
- ***Verificación:***
  - *Gestión de Incidentes: Fase Identificación*
  - Entrevistas con quienes trabajaron en etapas iniciales.
  - Estudio y revisión de información
  - Verificar la ocurrencia de un incidente
- ***Descripción del Sistema***:
  - Describir el sistema que se está analizando
  - Tipo de Sistema Operativo
  - Configuración del Sistema
  - Rol del sistema en la red



Análisis Forense – Adquirir Evidencia



- ***Integridad de la Evidencia***
  - Asegurar que la evidencia no fue alterada
  - Crear 2 copias/imágenes bit a bit
  - Guardar 1 copia en lugar seguro
  - Utilizar hashes criptográficos (SHA-1) para asegurar la integridad de la evidencia original y las copias.



- ***Orden de la volatilidad***: Cuando se colecta la evidencia, se debe proceder comenzando con la más volátil a la menos volátil. La siguiente lista es el orden de volatilidad de un sistema típico:
  - Memoria
  - Conexiones y Status de Red
  - Procesos Activos

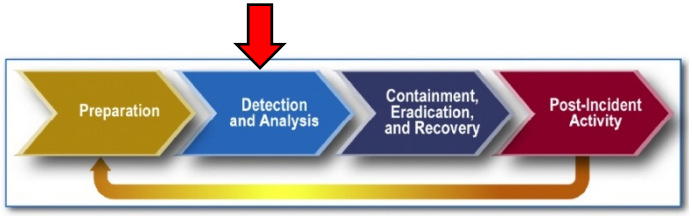
  Volátil: se pierde al apagar el sistema

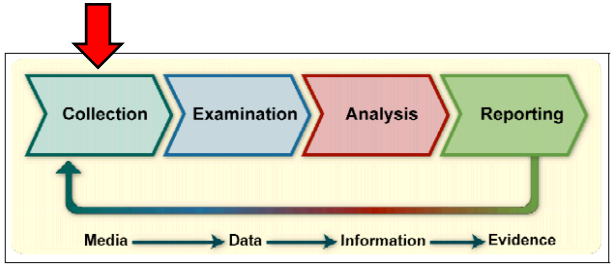
  - Discos Duros
  - Medios removibles

  No Volátil

EL ANÁLISIS NO DEBE SER CONDUCIDO SOBRE LA EVIDENCIA ORIGINAL.

Primera Línea de Actuación: Operador, Administrador de Sistemas y HelpDesk





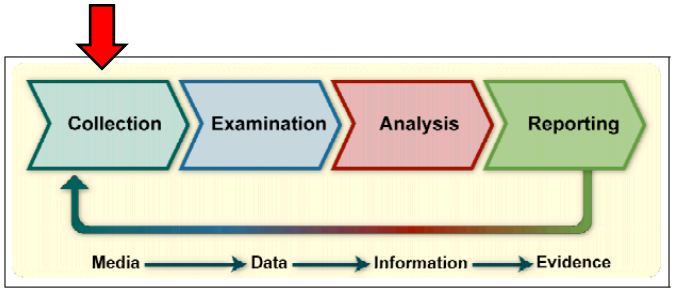
Las medidas adoptadas por el administrador del sistema después del descubrimiento de un potencial ataque al sistema, jugará un papel vital en la investigación.

Una vez que un incidente ha sido descubierto por un administrador del sistema, deben informar de ello de acuerdo a los procedimientos establecidos de notificación de incidentes de la organización.

Evitar trabajar en el equipo afectado, para no cambiar los datos (evidencia).

Tomar notas sobre la escena y documentar las acciones realizadas para luego ser entregados al Equipo Forense que atienda el caso.

Análisis Forense – Adquirir Evidencia



- ***Cadena de Custodia***

IBM Global Services Formulario - Cadena de Custodia

Formulario – Custodia de Evidencia

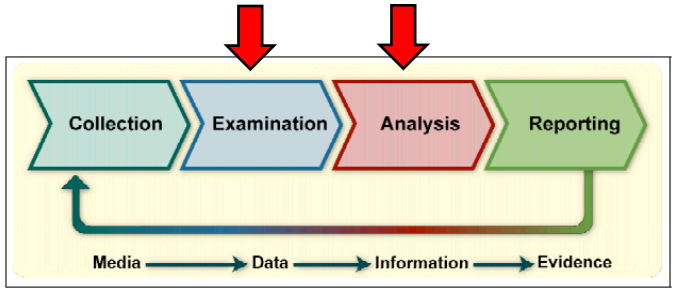
Labroatorio Forense

			Caso Forense #:
			Página: **de**
Item#:	**Descripción:**		
Marca:		**Modelo:**	**Serial#:**

Correo Registrado #	Fecha/Hora	Entregado Por	Recibido Por	Motivo
	Fecha/Hora	Nombre/Agencia/Organización	Nombre/Agencia/Organización	
	Hora	Firma	Firma	
	Fecha/Hora	Nombre/Agencia/Organización	Nombre/Agencia/Organización	
	Hora	Firma	Firma	

- Se debe seguir una cadena de custodia claramente definida para evitar acusaciones de mal manejo o manipulación de pruebas.
- Mantener un registro de cada persona que ha participado en la custodia de la evidencia.
- Documentar las acciones que se realizan en las pruebas y en qué momento
- Almacenar la evidencia en un lugar seguro cuando no se está utilizando,

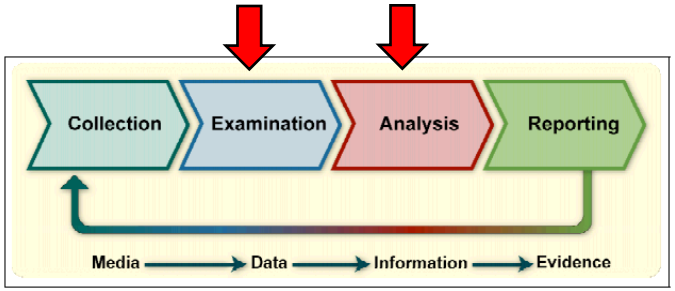
Análisis Forense – Examinar y Analizar

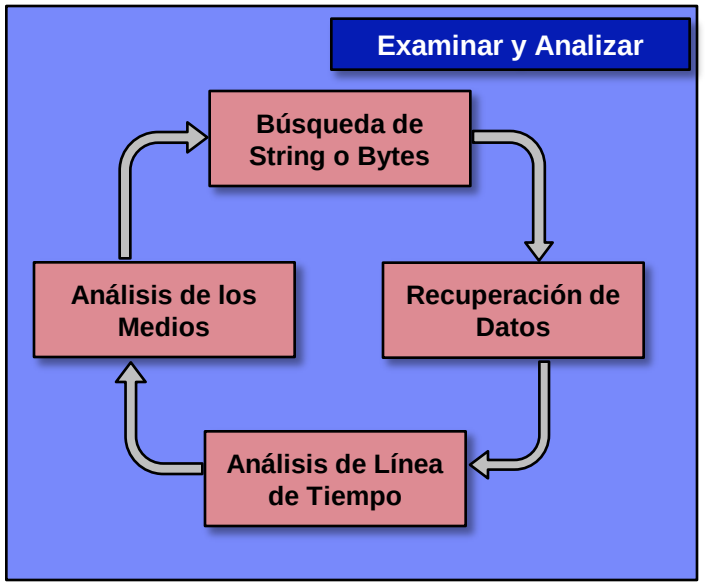


- Procesar gran cantidad de datos colectados para extraer datos relevantes y pertinentes.
- Utilización de técnicas y herramientas forenses.
- Analizar los resultados obtenidos de la extracción de datos.
- Los “datos” se transforman en “información” a través de análisis.
- Incluir la identificación de las personas, lugares, objetos, eventos, y la determinación de cómo estos elementos se relacionan de manera de llegar a una conclusión.
- Correlacionar datos de distintas fuentes (HIPS, NIPS, Antivirus, logs aplicaciones, sistemas operativos, base de datos, etc). Chequear “fidelidad” de la fuente.
- Comparar características de sistemas con su “baseline”.

Análisis Forense – Examinar y Analizar

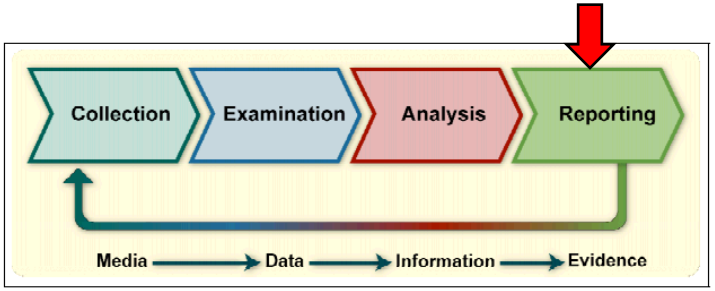
- ***Análisis de línea de Tiempo***
  - Archivos: modificación, creación, acceso
  - ¿Cuándo ha sido instalado el Sistema Operativo?
  - ¿Cuándo fueron realizadas las actualizaciones?
  - ¿Cuándo fue utilizado el sistema por última vez?
- ***Análisis de los Medios***
  - Examinar la imagen con herramientas forenses
  - Describir el análisis y las herramientas utilizadas
  - Mostrar que no se modifica la evidencia
  - Examinar el File System por modificaciones en OS o la configuración del sistema.
  - Buscar artefactos del atacante: rootkits, backdoors, sniffers, etc.
  - Examinar registros y/o procesos, archivos de inicio.
- ***Búsqueda de String o Bytes***
  - ¿Qué palabras/expresiones podría buscar?
  - ¿Por qué buscamos estas palabras/expresiones?



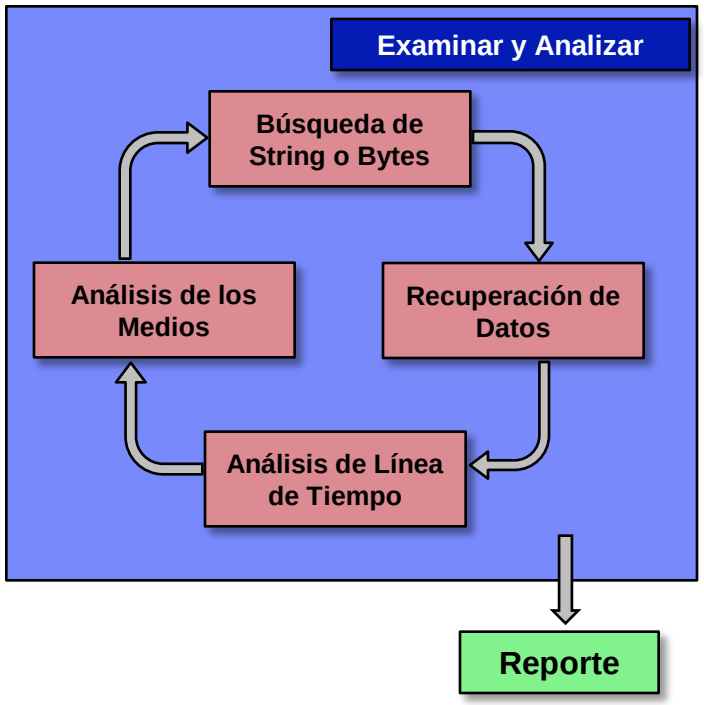


- ***Recuperación de Datos***
  - Recuperar archivos, datos borrados , artefactos del atacante
  - Identificar cúando fueron borrados los archivos
  - Recuperar archivos pertinentes
  - Documentar método utilizado.

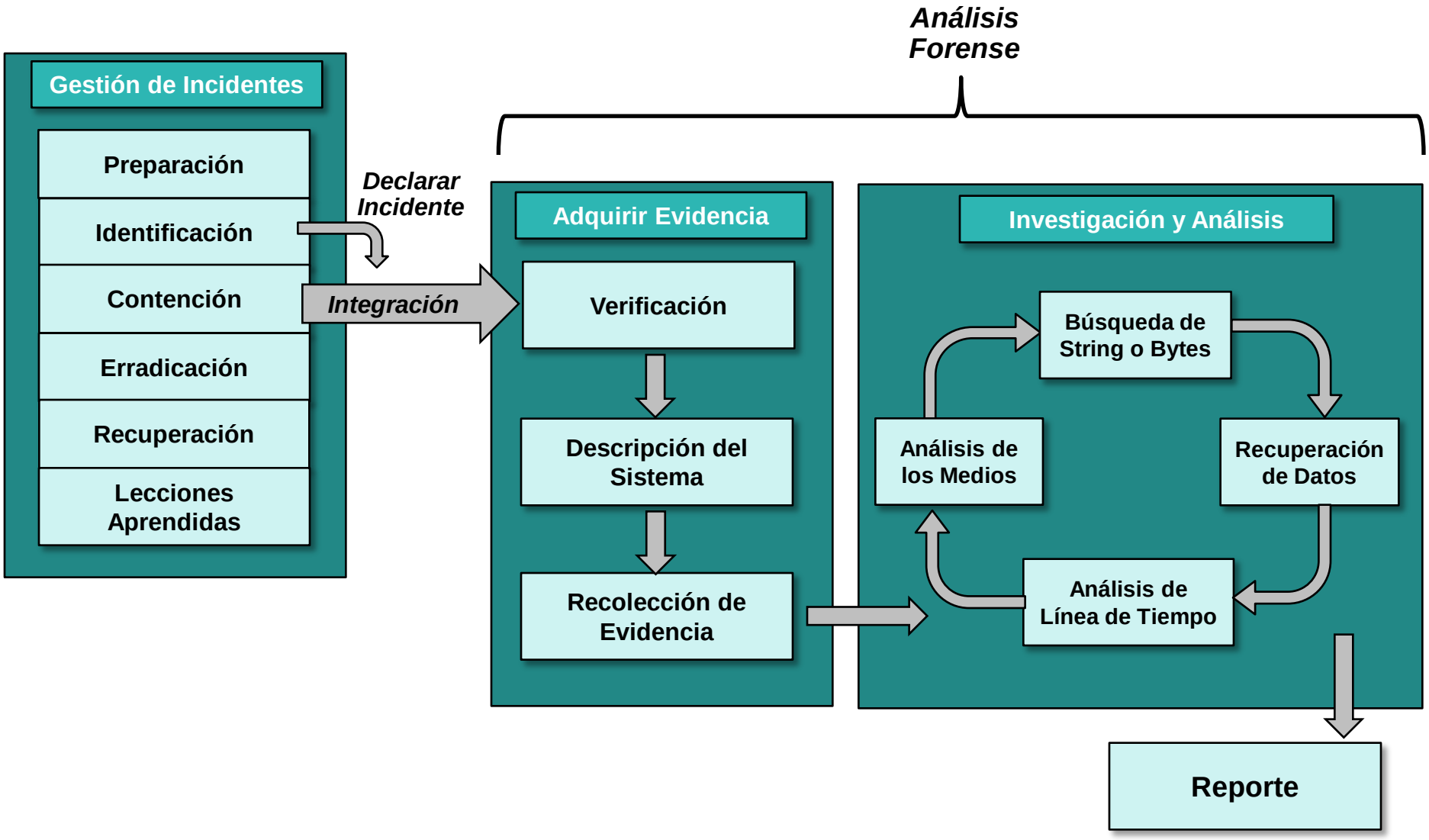
Análisis Forense – Fase Reportes



- Explicar claramente los resultados y la evidencia encontrada.
- Detallar hallazgos y conclusiones: archivos específicos relacionados con la solicitud y archivos borrados , cadena de búsquedas, búsquedas de palabras clave y búsquedas de cadenas de texto que apoyan las conclusiones.
- Informe básico incluye: ¿quién?, ¿qué?, ¿cuándo?, ¿dónde? y ¿cómo?
- Incluir en las notas: fechas, tiempos, las descripciones y resultados de las medidas adoptadas.
- Explicar las técnicas utilizadas y los detalles técnicos.
- Documentar irregularidades encontradas y las acciones adoptadas en relación con las irregularidades durante el análisis.
- Documentar los cambios realizados en el sistema o la red.
- Los analistas forenses deben utilizar un enfoque metódico para tratar de probar o refutar cada posible explicación que se propone.
- .Tener el cuenta el público objetivo
  - *Legal*: nivel alto de detalle. Copia de Evidencia
  - *Administrador de Sistemas*: análisis de información del sistema y de tráfico de red.
  - *Dirección*: alto nivel de lo sucedido.
- Medidas Correctivas: Identificar vulnerabilidades que deben ser corregidas.



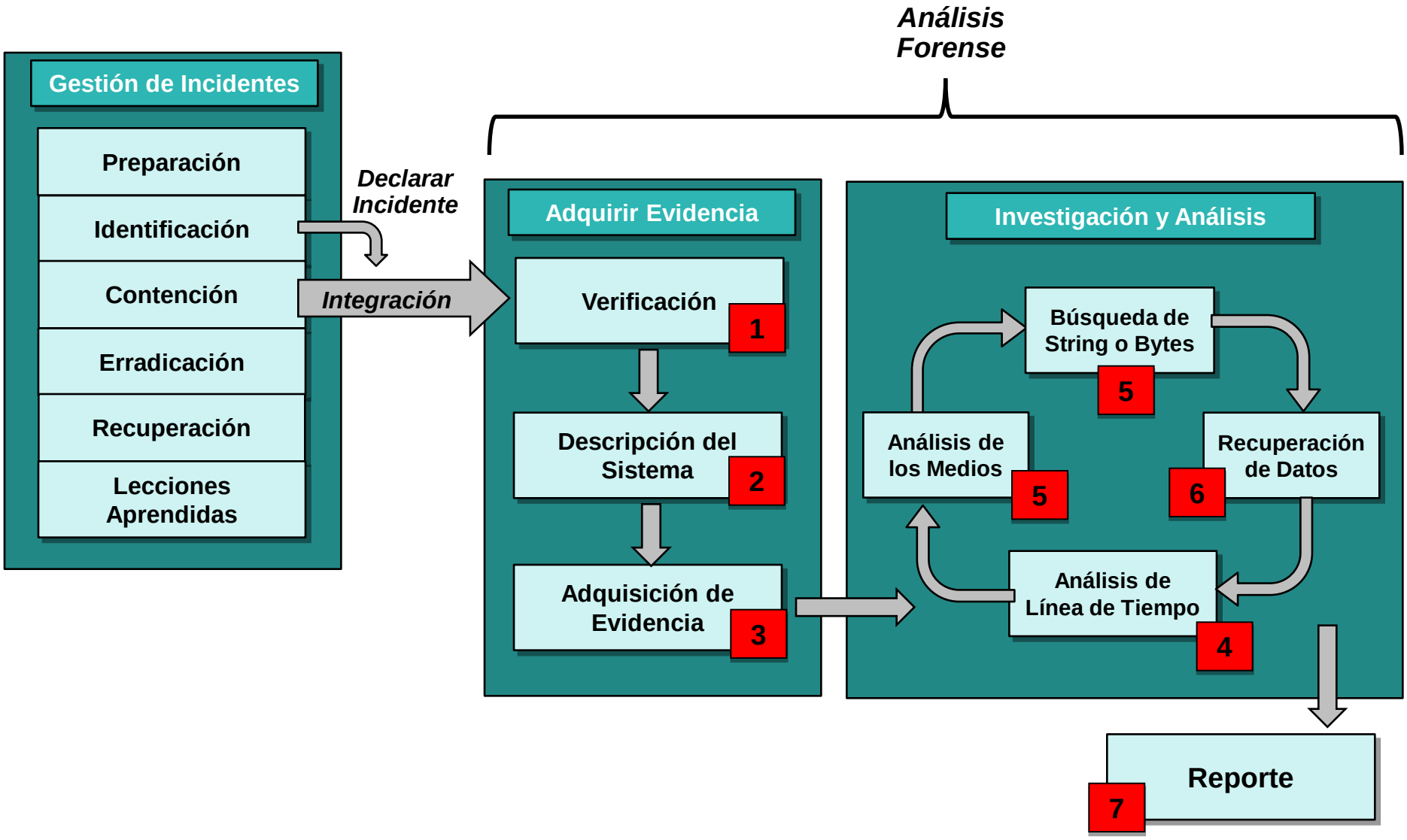
Ciclo de Vida para la Gestión de Incidentes y Análisis Forense



DEMO

Desafío - Análisis Forense

Ciclo de Vida para la Gestión de Incidentes y Análisis Forense



Desafío USB/Backdoor:

Metodología de Análisis:

Es lo efectivo de la recolección, examen, y reporte de nuestras acciones y resultados. La metodología ayudará el investigador a mantenerse en curso durante la investigación.

- Verificación: Verificar que ha ocurrido un incidente.
- Descripción del Sistema: Proveer una profunda descripción del Sistema.
- Adquisición de la Evidencia: Requiere que un investigador recolecte la evidencia.
- Investigación y Análisis: 4 fases -> de Tiempo, de Medios, Búsqueda, Recuperación.
- Reporte de Resultados: Detallará la investigación, la adquisición, el análisis paso a paso, y resultados concluyentes de análisis.

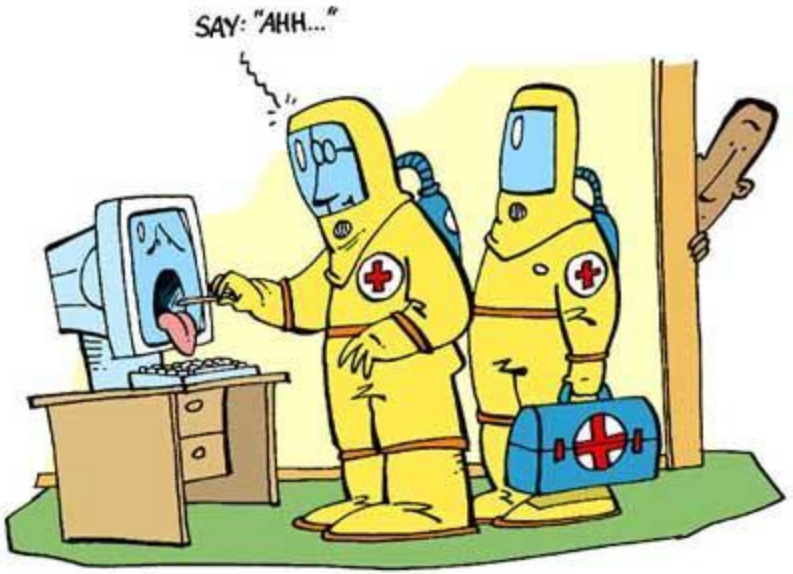
La adquisición de la evidencia generalmente ocurre durante la etapa de Contención del ciclo de vida para Gestión de Incidentes, donde debemos verificar el Incidente, pero también comenzar la recolección de la evidencia volátil y no volátil.

Desafío USB/Backdoor – (1) Verificación:

La información recabada por el equipo de análisis de eventos e incidentes e la siguiente:

- Los IPS han reportado tráfico no HTTP a través del puerto 80 TCP desde una estación de trabajo a una dirección pública el día Lunes 18/07/2011 a las 22:25 hs .
- Dirección IP y URL del destino de la conexión: IP 192.168.188.1 URL http://evil.server.com.
- Podríamos revisar bloqueo de las credenciales del usuario por parte de los Proxy de la empresa.

El Administrador del Centro de Gestión de Incidentes ha determinado la necesidad de dispara un análisis forense del la estación de trabajo previo a la etapa de contención de la amenaza, para confirmar la intrusión, si es posible que se haya comprometido información, y como se infectó el equipo.



Desafío USB/Backdoor – (2) Descripción del Sistema:

- **Describir el sistema que estamos analizando:**
  Donde fue adquirido.
  Para que es utilizado.
  Cual es la configuración del sistema: Red, OS, etc.
  Incluir cualquier otra información que creamos necesaria para realizar la investigación.
  Tomar notas puede ser de mucha ayuda durante la etapa de respuesta la incidente y recolección de información.

- **Caso de análisis USB/Backdoor:**
  Sistema Operativo: Microsoft Windows XP SP3, IE8, AV ESET.
  Hardware: P4 1.6 Ghz, 512 Mb RAM, 5Gb de disco.
  Red: DHCP.
  Uso: Estación de trabajo.
  Zona Horaria: GMT-3
  Info: La estación de trabajo es utilizada únicamente por el usuario “Usuario”, cuyo nombre de usuario en el sistema es “usuario”, tiene no RRCC configurados ni presta servicios.
  Log IDS: Proto Dirección local Dirección remota
  TCP 192.168.188.134:1030 192.168.188.1:80
  Notas: --

- **Donde realizar nuestra investigación:** Dado que el equipo donde se realice el análisis debe ser siempre un sistema limpio (de 0) usaremos una máquina virtual preparada para esta tarea.

Desafío USB/Backdoor – (3) Adquisición de la Evidencia:

Adquisición de la evidencia volátil:

win32dd.exe o win64dd.exe puede adquirir memoria física (RAM), solución open source:

(opción /s 0/1/2/3, 0=No hashing, 1=SHA1, 2=MD5, 3=SHA 256).

Se envía la evidencia volátil a una unidad USB:

win32dd.exe /s 2 /f E:\desafio/memory.img

Se envía la evidencia volátil a una unidad de red:

win32dd.exe /s 2 /f \\ip_address\desafio\memory.img

Adquisición de la evidencia no volátil:

dd.exe crea una imagen bit a bit del disco:

Se envía la evidencia no volátil a una unidad USB:

dd.exe if=\\.\C: of=E:\desafio/image.dd –cryptsum md5 –verify –cryptout E:\desafio/image.md5 –localwrt conv=noerror,sync

Se envía la evidencia no volátil a una unidad de red:

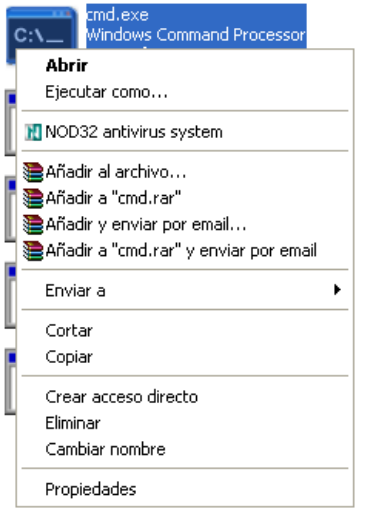
dd.exe if=\\.C: of=\\ip_address\desafio\image.dd –cryptsum md5 –verify –cryptout \\ip_address\desafio/image.md5 –localwrt conf=noerror,sync

Desafío USB/Backdoor – (3) Adquisición de la Evidencia:

Adquisición de la evidencia volátil:

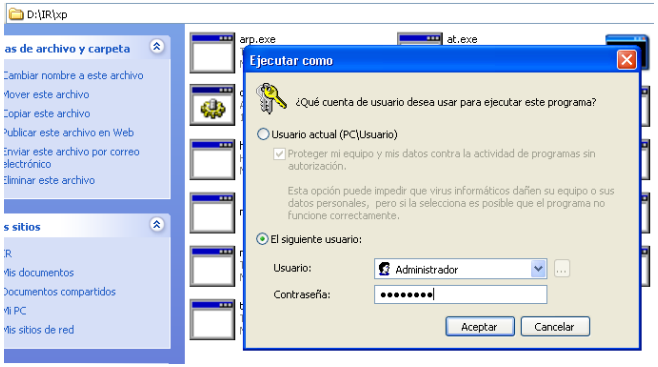
El primer paso para realizar esta tarea es abrir una shell en el sistema atacado con privilegios de administrador:

- En caso de estar logueado un usuario no administrador, podemos ejecutar el exe “cmd.exe.” con privilegios de administrador (“ejecutar como…”).
- Si el equipo está bloqueado o con protector de pantalla, no hay que deslogear al usuario; en este caso realizaremos la adquisición de la evidencia remotamente utilizando la herramienta de Microsoft “psexec”.



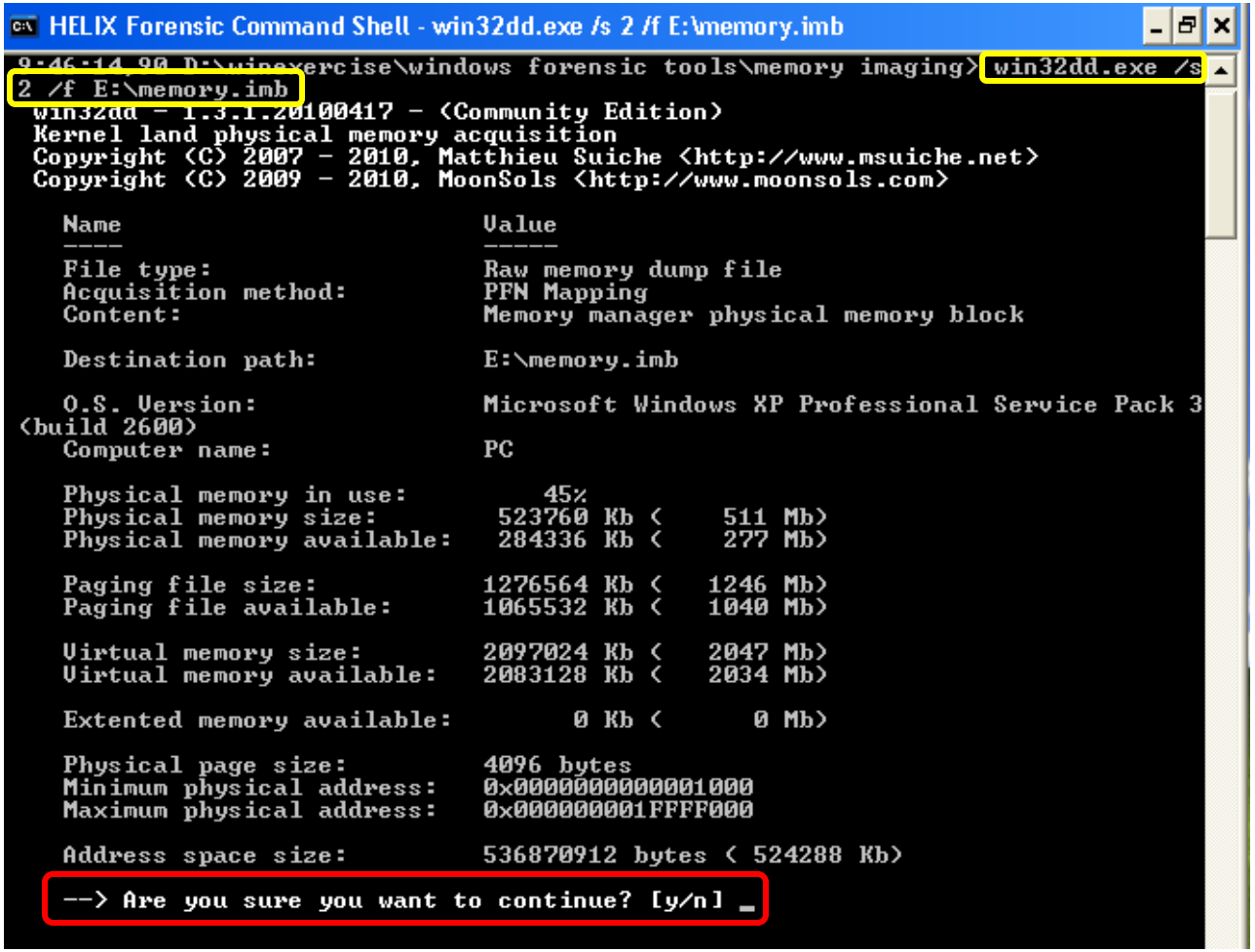
En nuestro escenario asumiremos que se encuentra logueado un usuario administrador y no tiene activado el protector de pantalla.

Ejecutamos nuestra versión de “cmd.exe” y luego nos cambiamos a un entorno controlado para no utilizar las herramientas del sistema. Esto tiene como fin el no dejar más huellas durante la etapa de recolección de evidencia. También aseguramos el uso de herramientas que no fueron alteradas por el atacante.



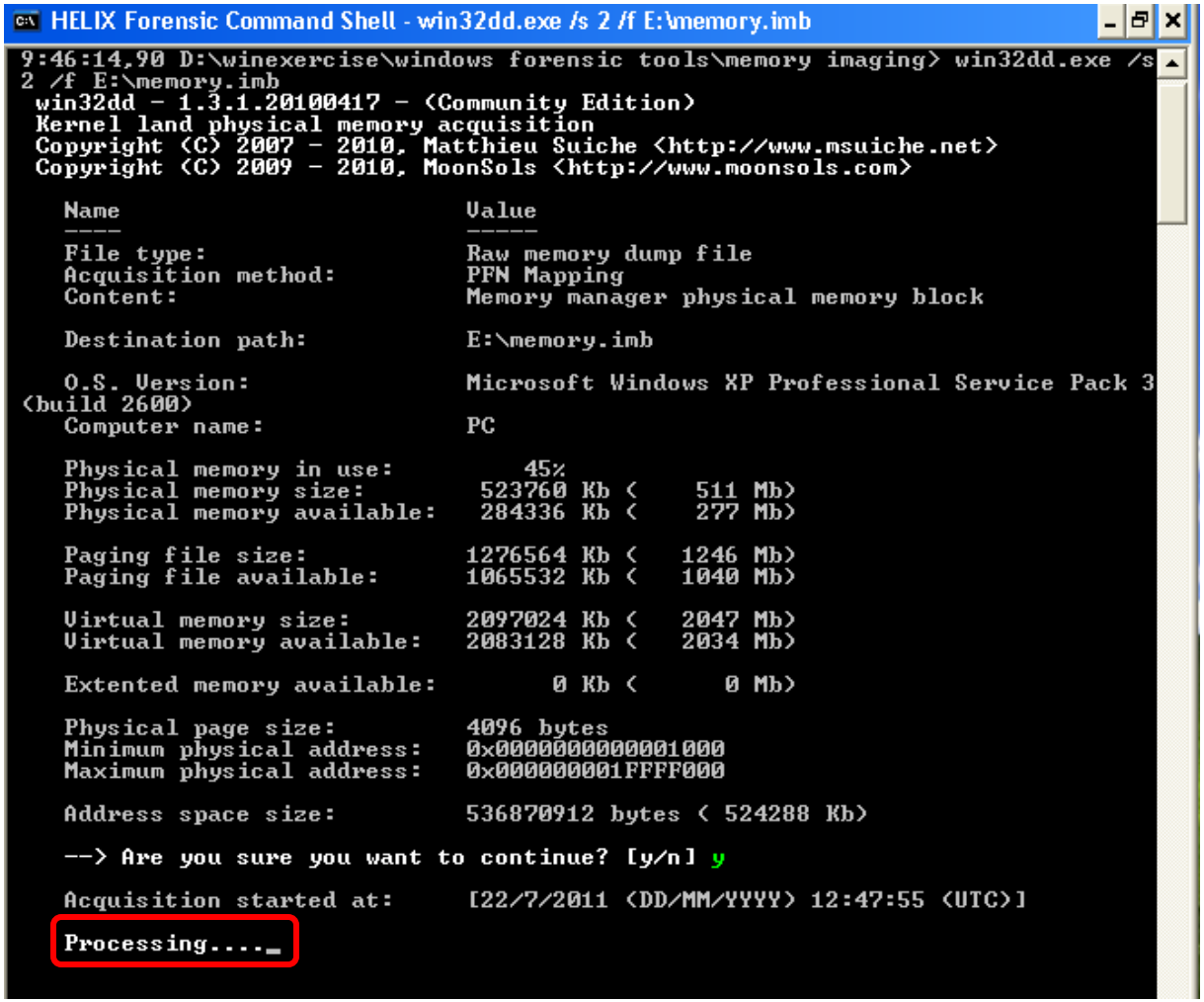
Desafío USB/Backdoor – (3) Adquisición de la Evidencia:

Adquisición de la evidencia volátil:



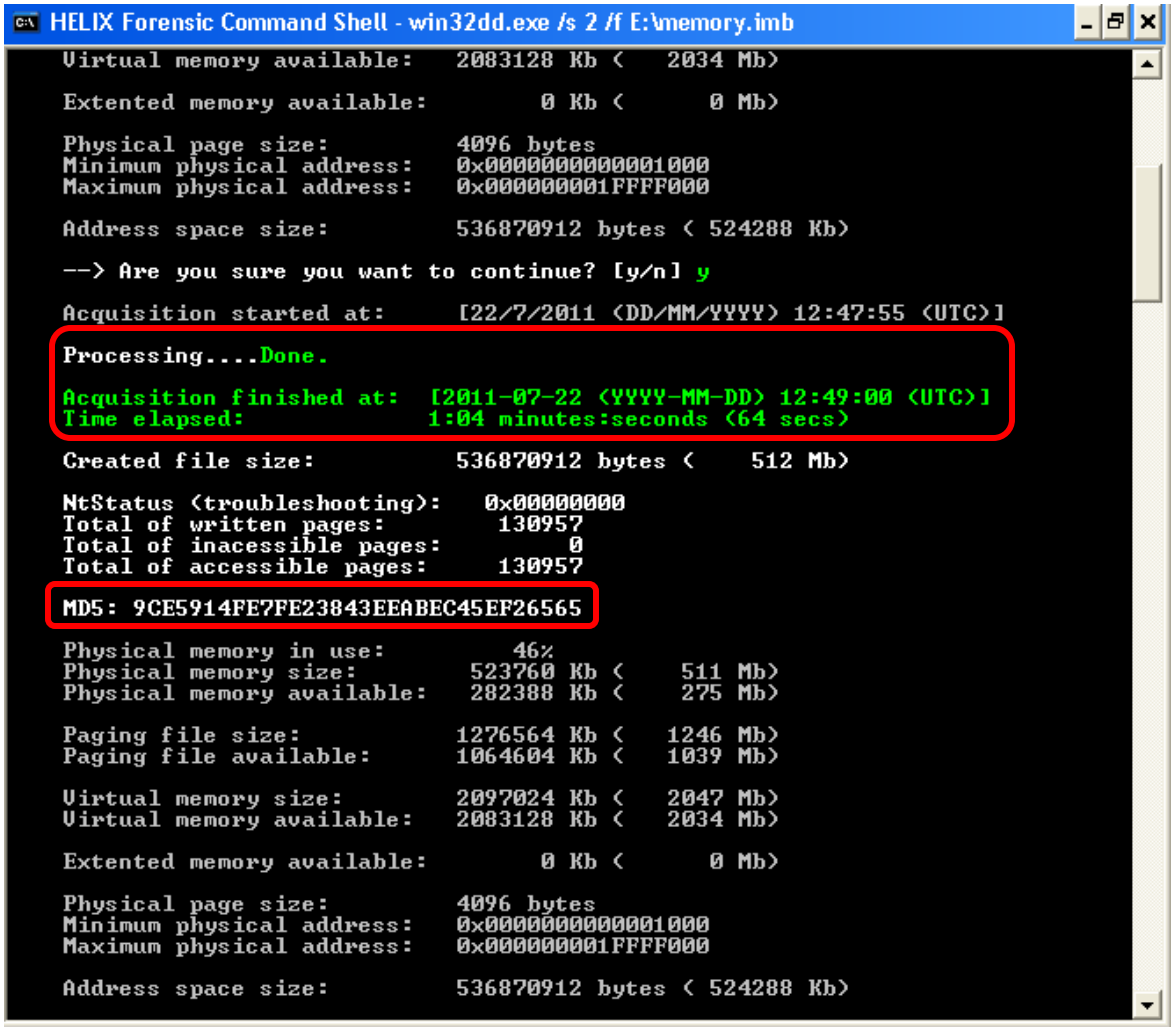
Desafío USB/Backdoor – (3) Adquisición de la Evidencia:

Adquisición de la evidencia volátil:



Desafío USB/Backdoor – (3) Adquisición de la Evidencia:

Adquisición de la evidencia volátil:



Desafío USB/Backdoor – (3) Adquisición de la Evidencia:

Adquisición de la evidencia no volátil:

Tres métodos de adquisición de la evidencia:

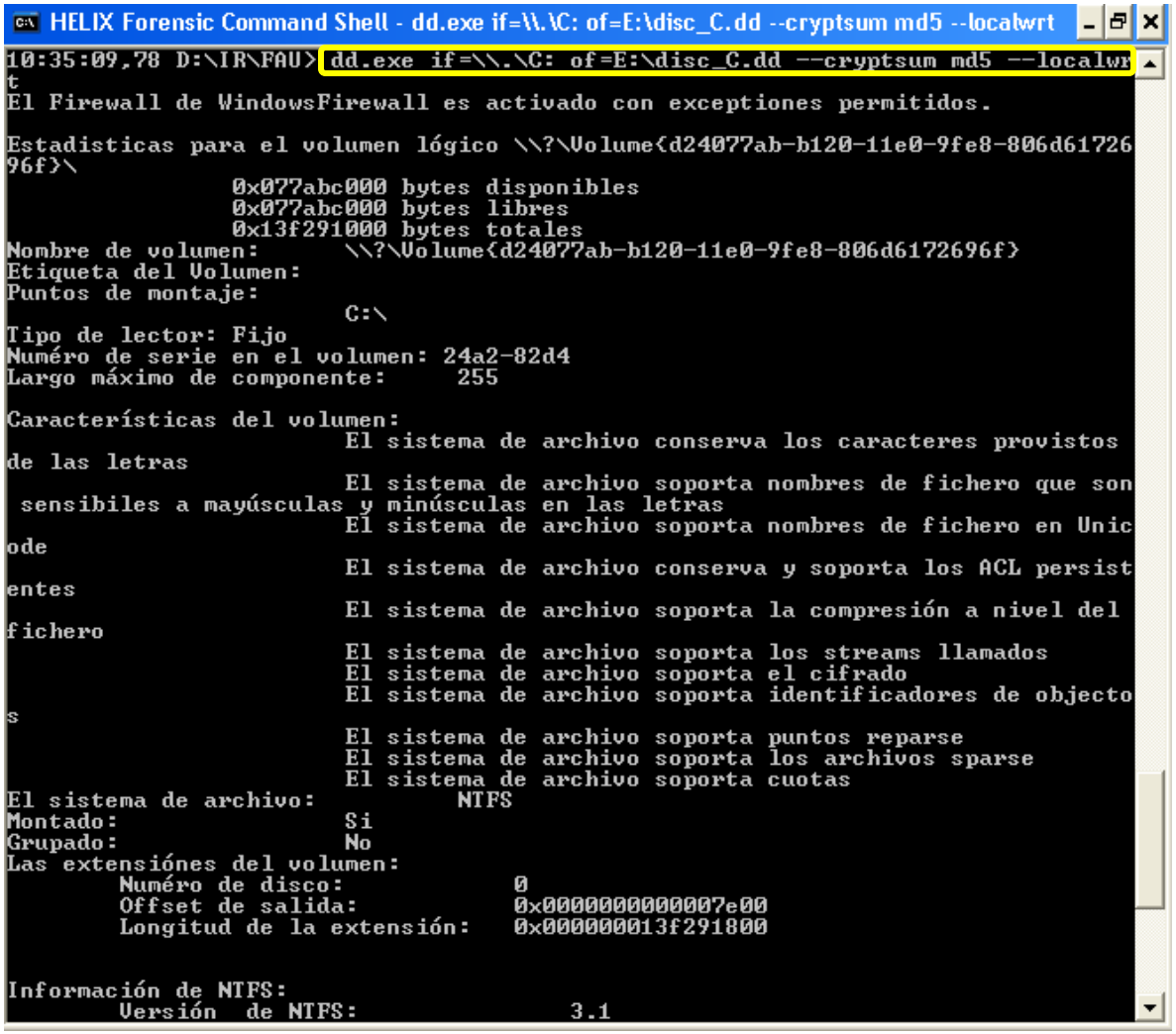
- Hardware: Remover el disco duro que contiene la evidencia y realizar una imagen disco a disco de la evidencia.
    * La evidencia no es modificada durante el proceso (bloqueadores de escritura).
    * La evidencia se mantiene estática.
    * Evidencia volátil no disponible.

- CD de Booteo (Helix3 Pro Evidence Adquisition): Iniciar sistema desde CD.
    * Evidencia volátil no disponible.
    * La evidencia no es modificada durante el proceso (mount ro).
    * La evidencia se mantiene estática.
    * Destino: USB/Firewire o Red (Cable cruzado + netcat).

- Live System: El sistema no es apagado o reiniciado.
    * Snapshot del sistema.
    * El sistema se mantiene encendido.
    * Evidencia volátil disponible.
    * Evidencia cambiará durante el proceso de imagen.
    * Destion: USB/Firewire o Red (netcat).

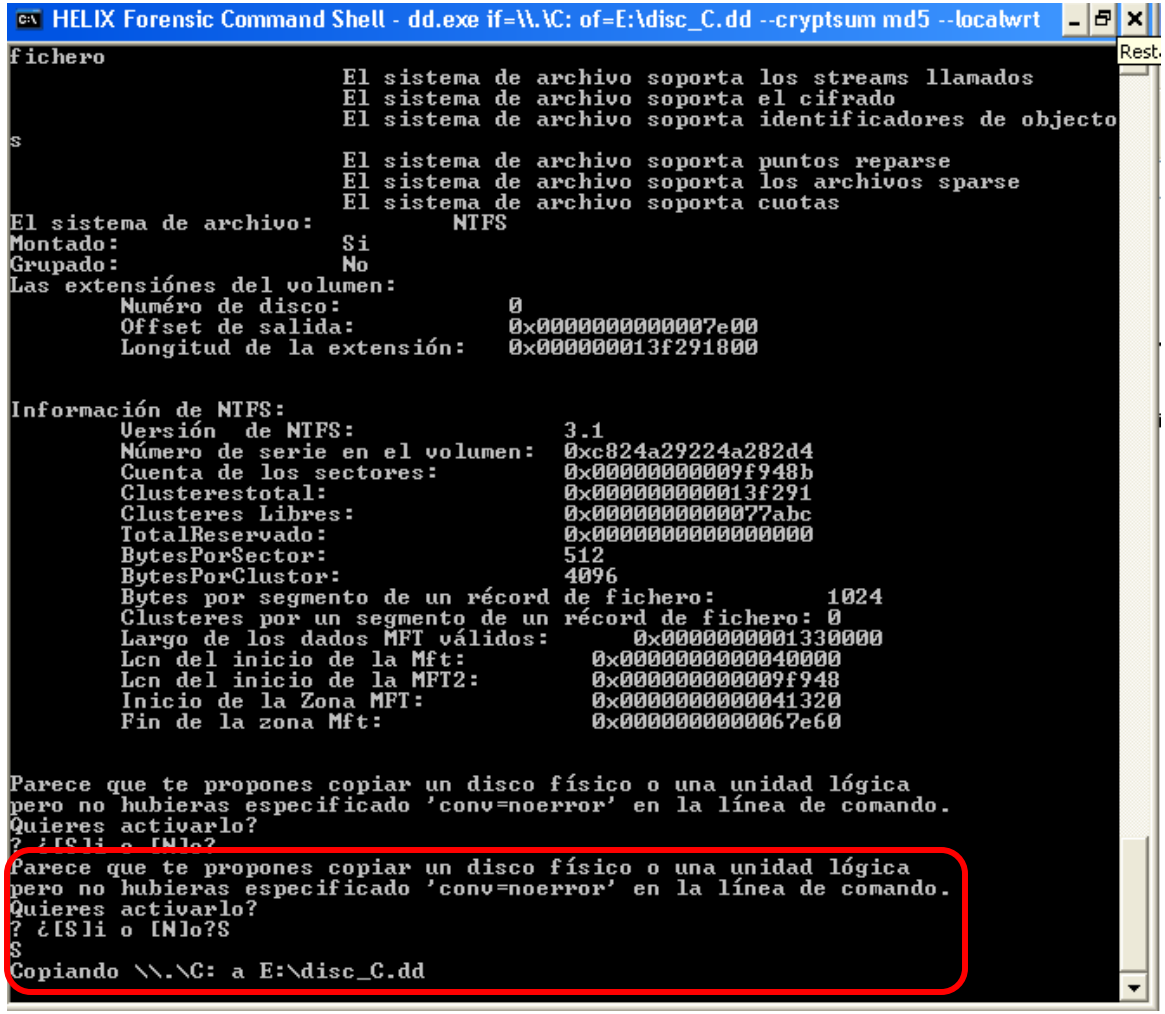
Desafío USB/Backdoor – (3) Adquisición de la Evidencia:

Adquisición de la evidencia no volátil: (Live System)



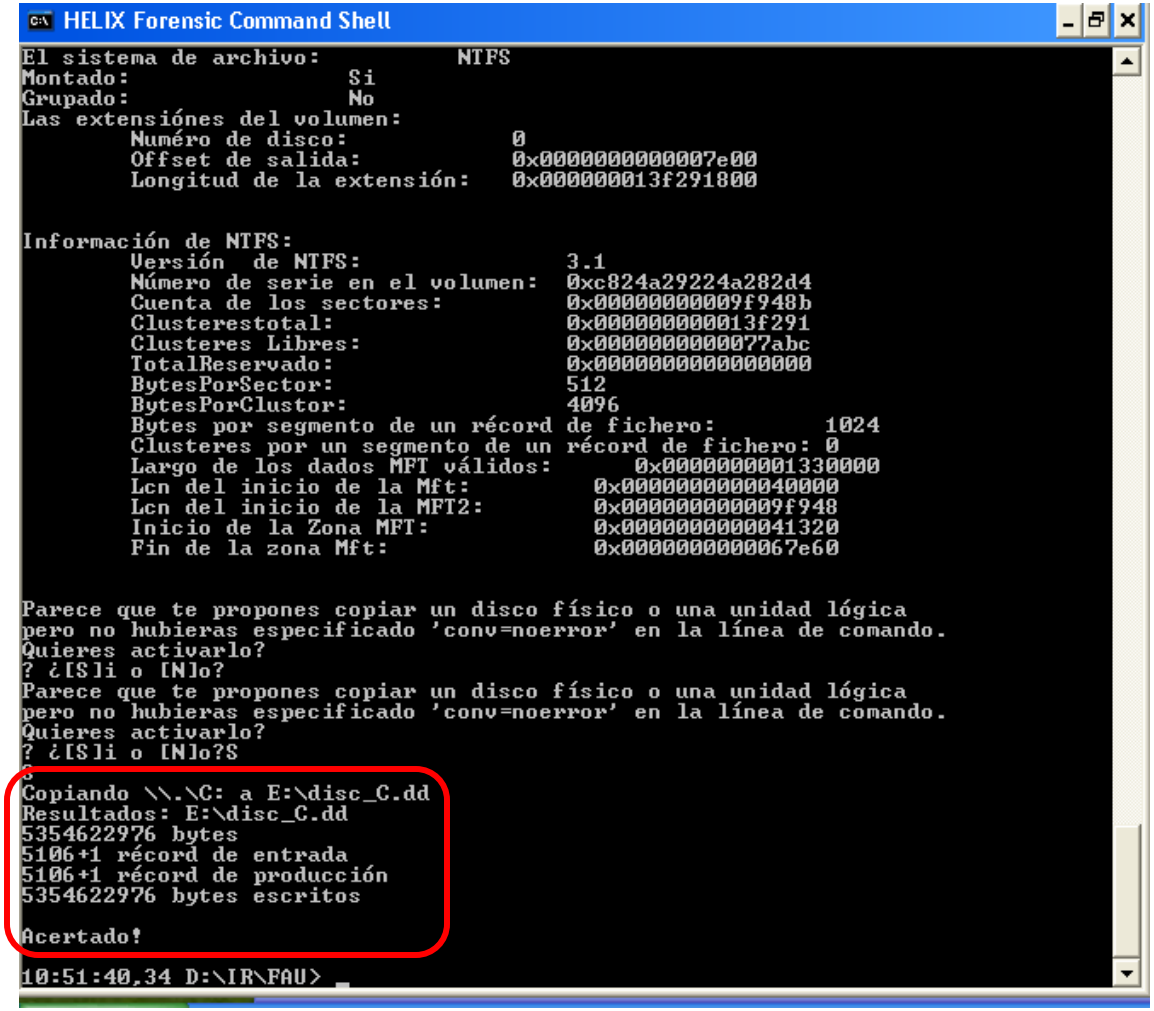
Desafío USB/Backdoor – (3) Adquisición de la Evidencia:

Adquisición de la evidencia no volátil: (Live System)



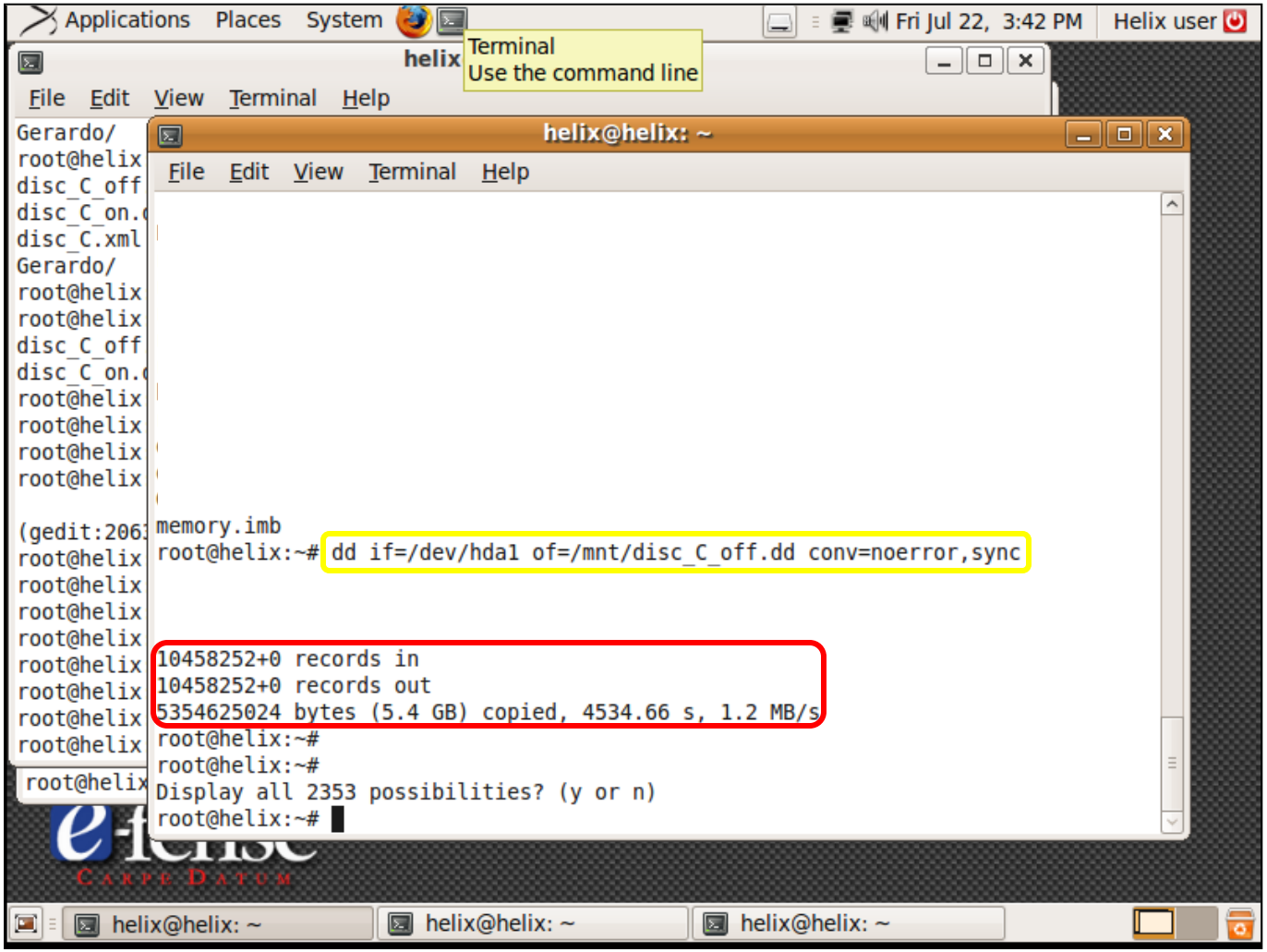
Desafío USB/Backdoor – (3) Adquisición de la Evidencia:

Adquisición de la evidencia no volátil: (Live System)



Desafío USB/Backdoor – (3) Adquisición de la Evidencia:

Adquisición de la evidencia no volátil: (Boot CD)

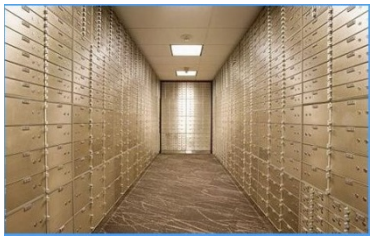


Desafío USB/Backdoor – (3) Adquisición de la Evidencia:

Cadena de Custodia de Evidencia:

El siguiente paso es completar el formulario de cadena de custodia.

El análisis forense es llevado a cabo con copias de la evidencia verificando su integridad.



IBM Global Services — Formulario - Cadena de Custodia

Formulario – Custodia de Evidencia

Labroatorio Forense

	Caso Forense #:
	Página: de

Item#:	**Descripción:**	
Marca:	**Modelo:**	**Serial#:**

Correo Registrado #	Fecha/Hora	Entregado Por	Recibido Por	Motivo
	Fecha/Hora	Nombre/Agencia/Organización	Nombre/Agencia/Organización	
	Hora	Firma	Firma	
	Fecha/Hora	Nombre/Agencia/Organización	Nombre/Agencia/Organización	
	Hora	Firma	Firma	

Capas del Sistema de Archivos – Persistencia de Datos:

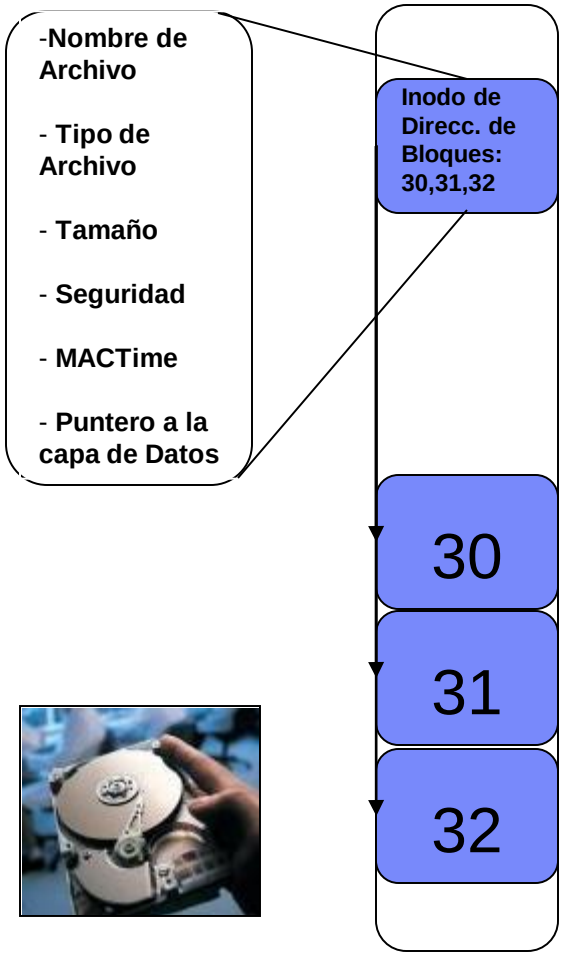
- **Capa Física:**
  El controlador.

- **Capa de Sistema de Archivos:**
  Información de Particionamiento.

- **Capa de Datos:**
  Donde los datos son almacenados (Bloques o Clusters).

- **Capa de Metadatos:**
  Información de la Estructura de archivos
  EXT2/3 - Inodo, Fat32 – Directorio de entrada FAT,
  NTFS – Entrada MFT):
  Asignados: (Block o Cluster Usado)
    Metadatos: GID, UID, MACTimes, Permisos, etc.
    Punteros a Bloques o Clusters.
  Sin Asignar: (Block o Cluster Libre)
    Metadatos: Pueden estar o no.
    Punteros a Bloques o Clusters pueden estar o no.

- **Capa de Nombre de Archivos:**
  Nombre del archivo.

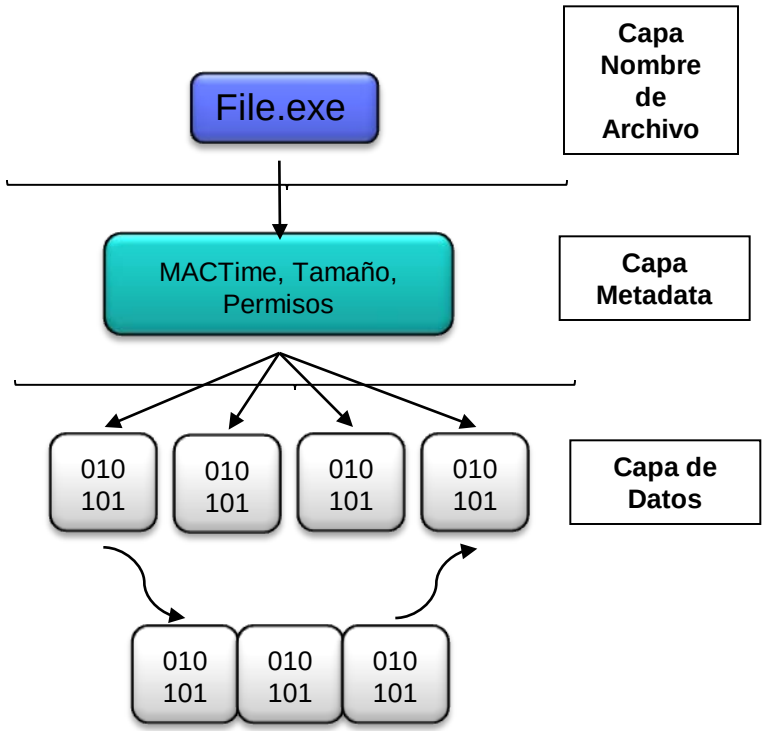


Capas del Sistema de Archivos – Herramientas:

Qué información aún existe luego de borrar un archivo?

- Generalmente tenemos éxito para recuperar datos borrados:
A no ser que alguien haya sobrescrito o wipeado los bloques de datos antes de borrar el archivo.
Un solo wipe es necesario para impedir que todas las herramientas forenses puedan recuperar los datos borrados. (NIST Guideline for Media Sanitization).

- Archivos Borrados:
Algunos OS borran los links entre el nombre y la metadata. Las distribuciones actuales borran además todos los punteros a los bloques de datos para borrar archivos (ext3/ext2). En Windows FAT: (file allocation table) en la capa nombre de archivo FAT12/16/32 remplaza la primer letra del nombre por 0xe5; en exFAT la entrada es marcada como inactivo. NTFS ($MFT master file table): la entrada del archivo es marcada como “borrado”.



Capas del Sistema de Archivos – Herramientas:

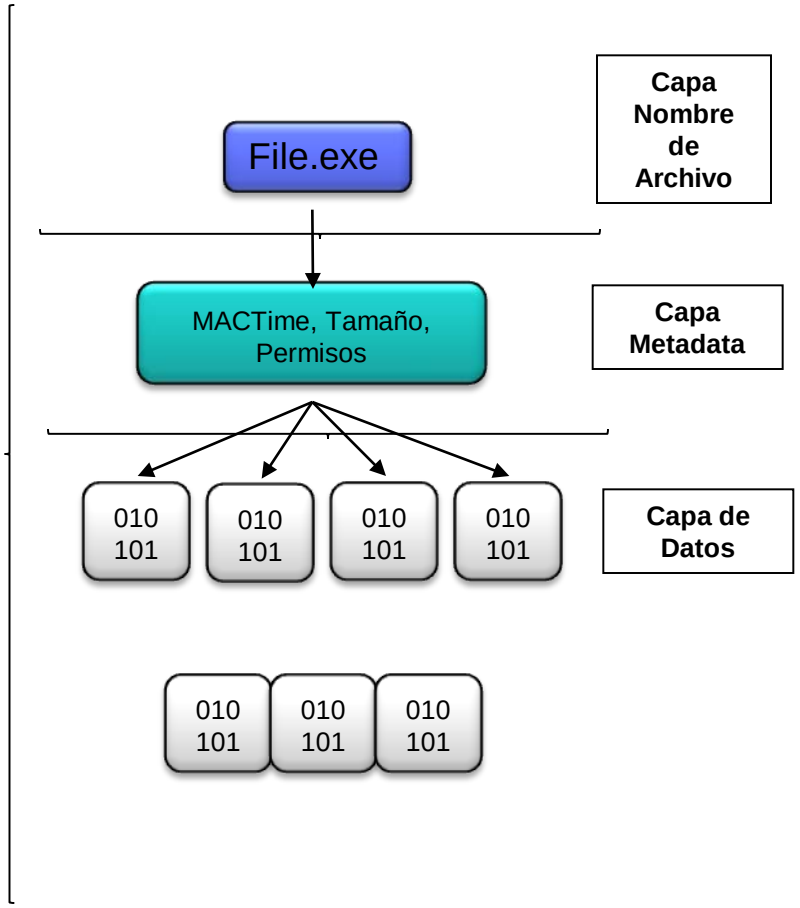
Qué información aún existe luego de borrar un archivo?

Ext2/3:

- Capa Nombre de Archivo:
Se preserva el nombre en la entrada del directorio. El número de inodo puede ser preservado si no es sobrescrito.

- Capa Metadata:
UID/GID son preservados.
Información MA- es preservada, --C cambia a la fecha de borrado.
Tipo de archivo, Permisos, Tamaño, y direccionamiento de bloques generalmente son preservados.

- Capa de Datos:
Los bloques serán marcados como “sin asignar”, pero los datos son preservados.



Capas del Sistema de Archivos – Herramientas:

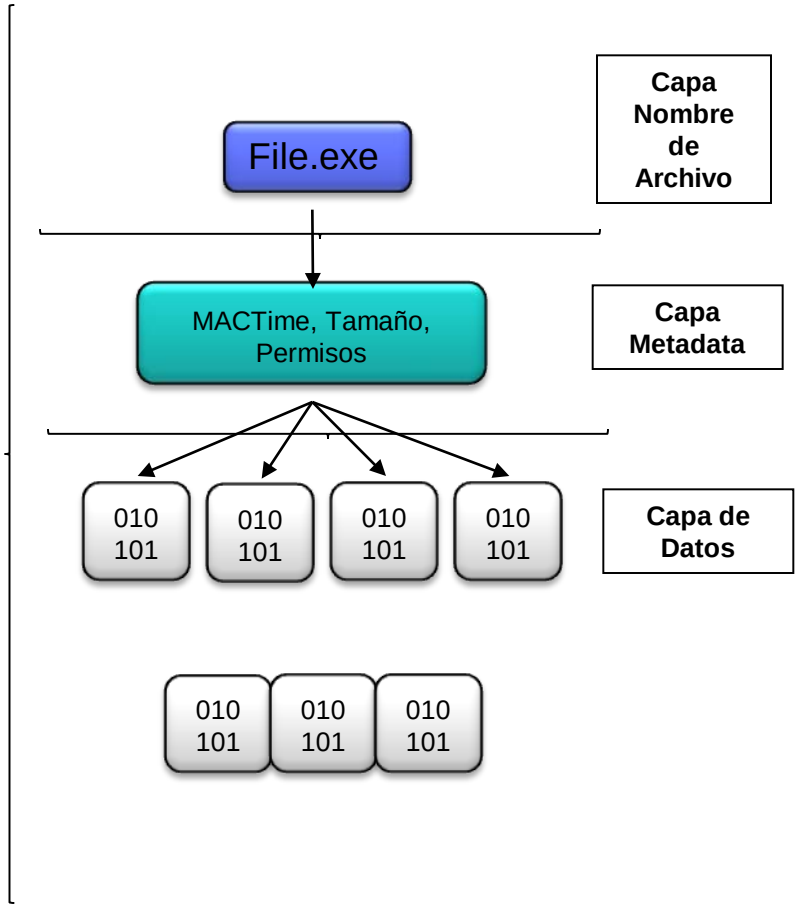
Qué información aún existe luego de borrar un archivo?

FAT12/16/32/exFAT y NTFS:

- Capa Nombre de Archivo:
Se preserva el nombre del archivo.

- Capa Metadata:
Información MAC es preservada. NTFS actualiza la hora --C- a la hora de borrado en la tabla MFT.
Los atributos del archivo son preservados.

- Capa de Datos:
Los cluster serán marcados como “sin asignar”, pero los datos son preservados en la localización de los clusters original.



Capas del Sistema de Archivos – Herramientas:

“Diferentes herramientas / Misma metodología: de OS a OS, de Sistema de Archivos a Sistema de Archivos.”

The Sleuth Kit Programs: (Resumen)

Open Source, Windows y Unix. Basadas en el modelo Unix de pequeñas herramientas especializadas.

- Capa de Sistema de Archivos:

  fsstat: despliega detalles del sistema de archivos.

- Capa de Datos:

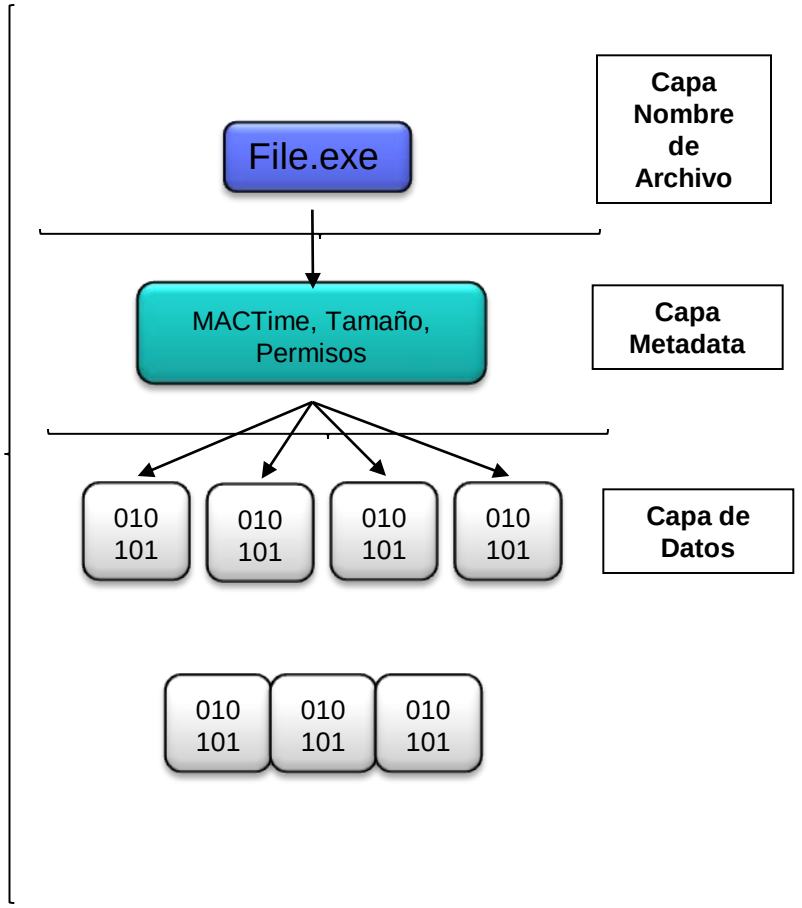
  blkcat: despliega el contenido de un bloque del disco.
  blkls: lista el contenido de bloques borrados del disco.
  blkcalc: mapea entra imagen y el resultado de blkls.
  blkstat: lista estadísticas asociadas a un bloque específico.

- Capa Metadatos:

  ils: despliega detalles del inodo.
  istat: despliega información sobre un nodo específico.
  icat: despliega el contenido de los bloques asignados a un inodo.
  ifind: determina que inodo tiene asignado un bloque.

- Capa Nombre de archivo:

  fls: despliega los archivos y directorios de una imagen.
  find: determina que archivos tienen asignados un inodo en la imagen.



Desafío USB/Backdoor – (4) Análisis de Tiempo:

Debemos crear un análisis de línea de tiempo para determinar el contexto cuando se dio el incidente:

La creación de la línea de tiempo consiste en dos pasos:

Crear un bodyflie: es un archivo generado con los datos de todos los archivos de la imagen (asignados, no asignados, borrados).

Crear un archivo legible por el humano ordenado por el timestamp de cada archivo de menor a mayor.

Crear bodyfile:

fls –m E: -r image.dd > image.bodyfile

Crear línea de tiempo:

mactime –b image.bodyfile –z EST5EDT > timeline.image.txt

Luego podemos editar el archivo resultante “timeline.image.txt” con cualquier editor de texto para determinar el contexto en el que se dio el incidente.
Reglas MACB/MACC:

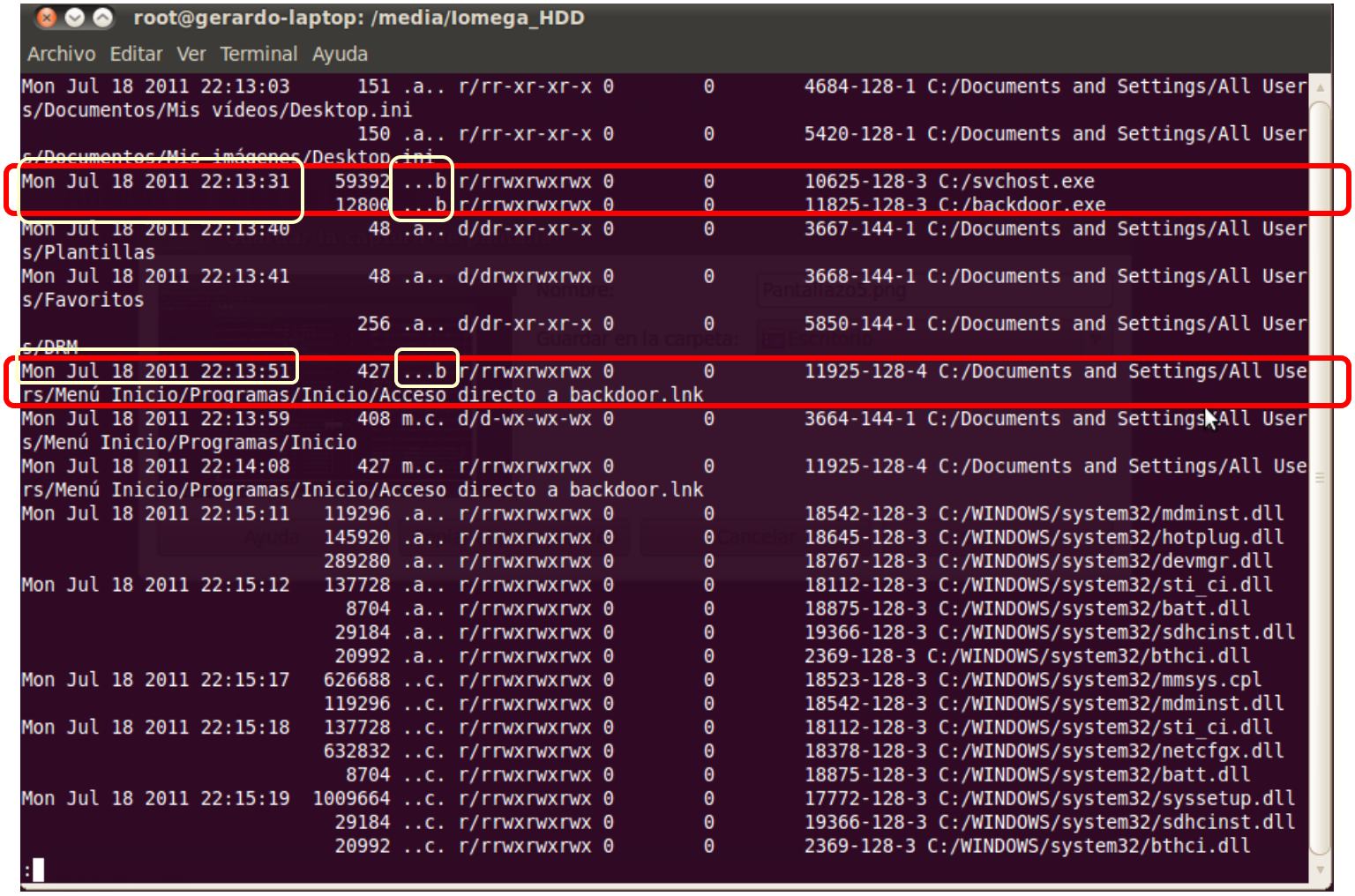
File System	Time Stored	Time Resolution	M	A	C	B
Ext2/3	Epoch	1 sec since Jan 1, 1970	Modified	Accessed	Inode Changed	
FAT	Local	Jan 1, 1980	Modified (2 sec)	Accessed Date (1 day)		Created (10 ms)
NTFS	UTC	100 ns since Jan 1, 1601	Modified	Accessed	MFT Modified	Created

Linux:
-Movimiento: --C
- Copiado: MAC
- Acceso: -A-
- Modificado: M-C
- Creado: MAC

Windows:
-Fecha de Modificación: se mantiene si el archivo es copiado o movido.
-Fecha de Creación: depende si fue copiado o movido.
NO Cambia si:
- Movido de C:\FAT a D:\NTFS
- Movido de C:\FAT a C:\FAT\subdir - Movido de D:\NTFS a D:\NTFS\subdir
Cambia si:
- Copiado de C:\FAT a D:\NTFS
- Copiado de C:\FAT a C:\FAT\subdir
- Copiado de D:\NTFS a D:\NTFS\subdir

Desafío USB/Backdoor – (4) Análisis de Tiempo:

Análisis de línea de tiempo:



Desafío USB/Backdoor – (5) Análisis de Medios/Búsqueda string/byte:

Análisis de la memoria RAM (Herramienta volatility):

volatility “opción” –f memory.img (https://www.volatilesystems.com/default/volatility; opciones: connscan, files, hibinfo, procdump, pslist, regobjkeys, sockets, sockscan)

volatility pslist –f memory.img
volatility sockets –f memory.img

Análisis de la línea de tiempo:

Lista de archivos copiados, creados, movidos a la hora de detección del incidente.

Descripción del Sistema:

Lista de palabras asociadas a archivos, procesos, o datos que pueden ser relevantes para la investigación.

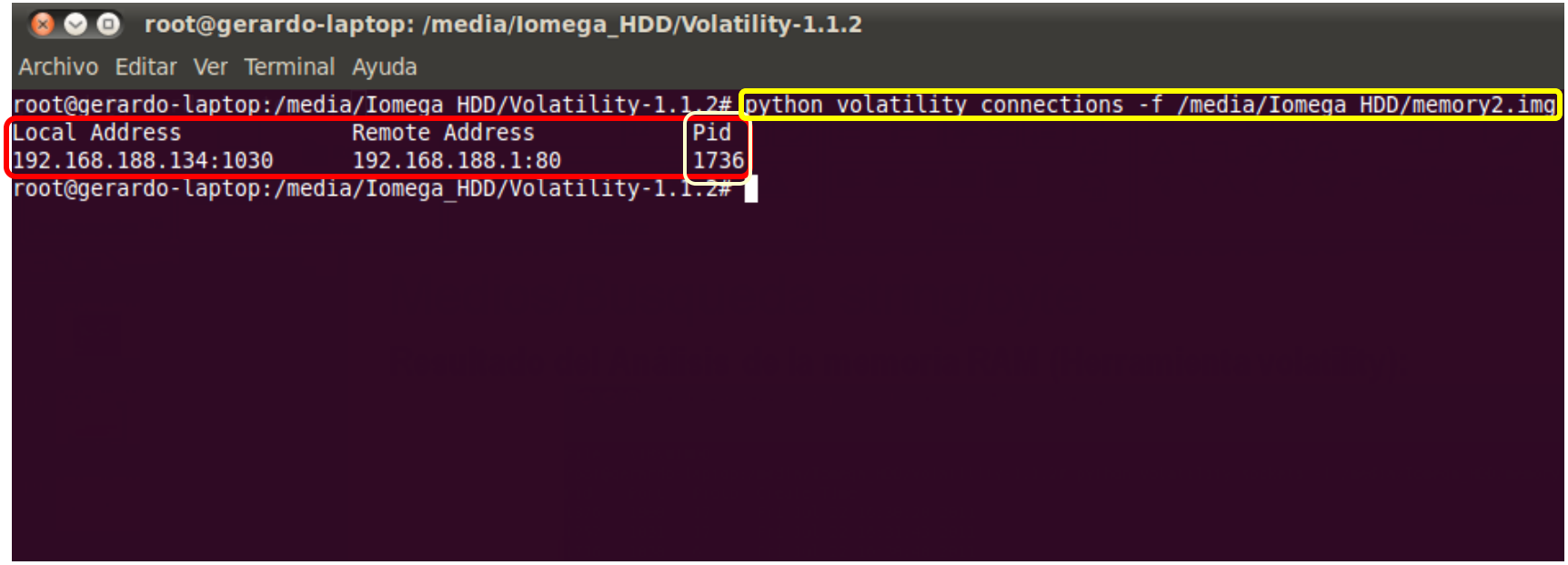
Armado de una lista de palabras a buscar referentes a programas o archivos a recuperar:

srch_strings “opción” image.dd
srch_strings –a -t –d image.img > lista_de_palabras.str
grep –i –f lista.txt lista_de_palabras.str

Desafío USB/Backdoor – (5) Análisis de Medios/Búsqueda string/byte:

Resultado del Análisis de la memoria RAM (Herramienta volatility):

Utilizando la opción “connections” encontramos una conexión establecida a la ip “192.168.188.1” puerto 80 por el proceso con ID “1736”.

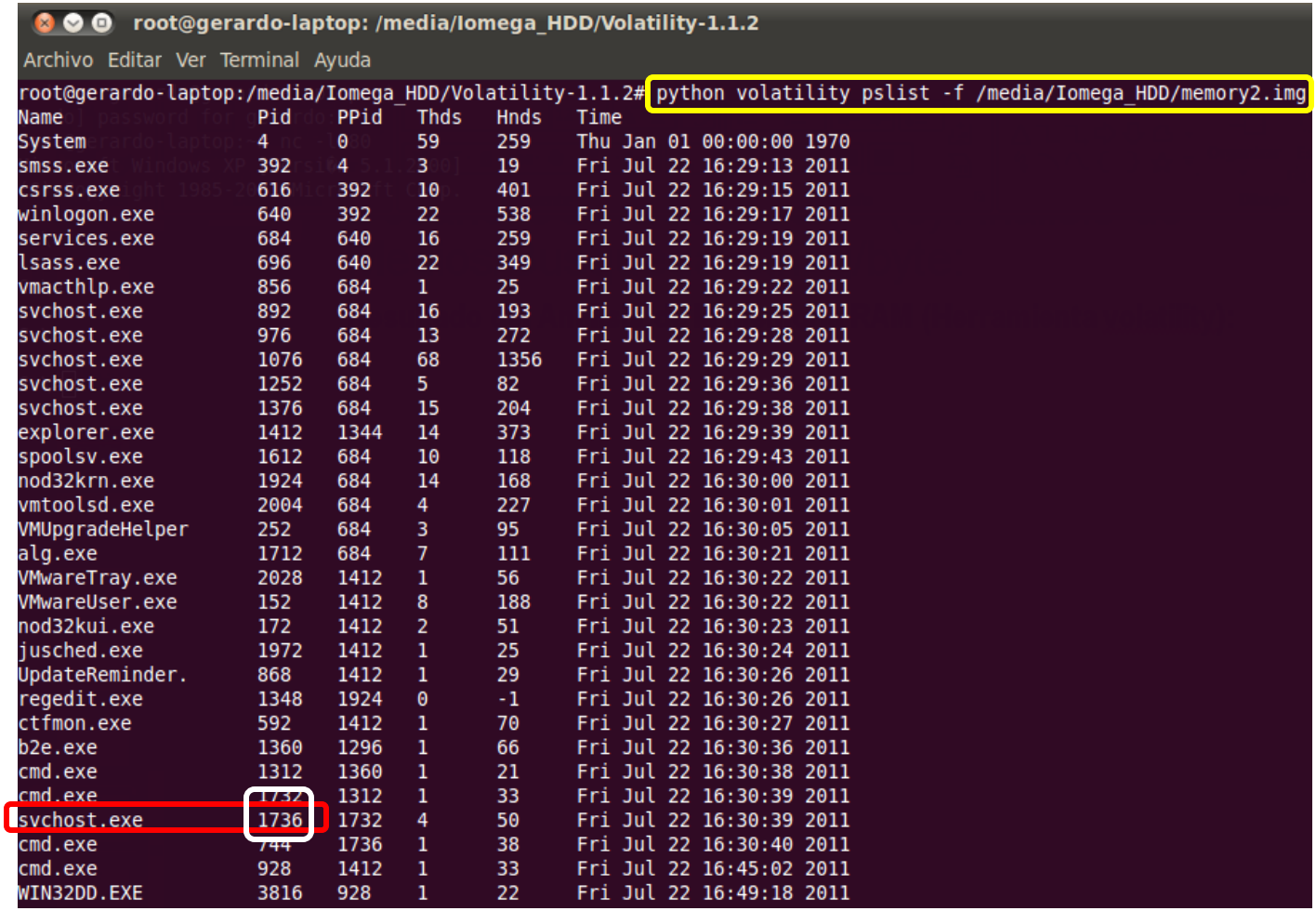


Desafío USB/Backdoor – (5) Análisis de Medios/Busqueda string/byte:

Resultado del Análisis de la memoria RAM (Herramienta volatility):

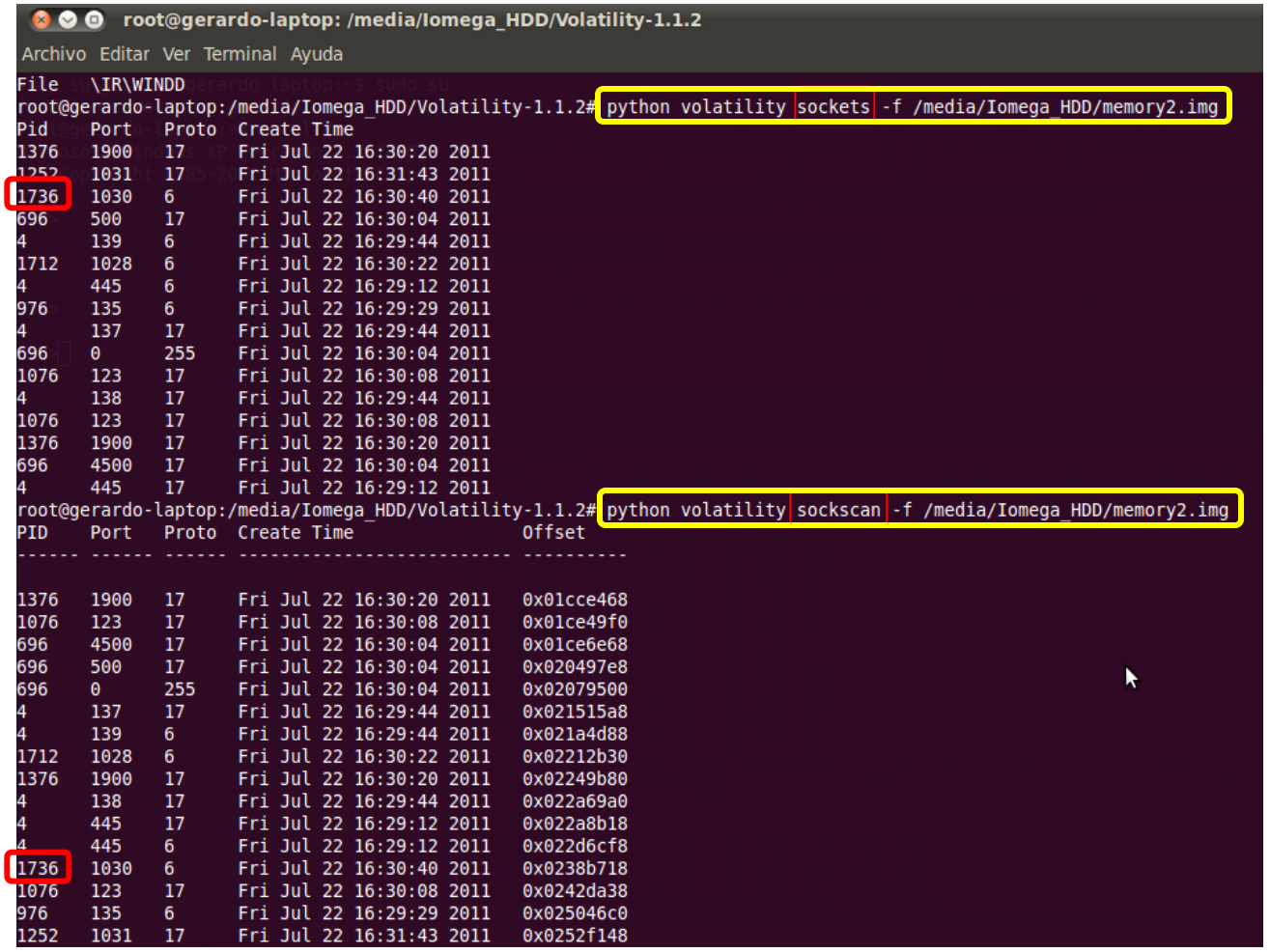
Uando la opción “pslist” obtenemos el proceso que tiene asignado el ID “1736”:

“svchost.exe”



Desafío USB/Backdoor – (5) Análisis de Medios/Búsqueda string/byte:

Resultado del Análisis de la memoria RAM (Herramienta volatility):



Desafío USB/Backdoor – (5) Análisis de Medios/Búsqueda string/byte:

Resultado del Análisis de la memoria RAM (Herramienta volatility):

Proceso svchost.exe tiene una conexión establecida a la ip “192.168.188.1” puerto 80.

Resultado del análisis de la línea de tiempo:

En torno a la hora de reportado el incidente los archivos “svchost.exe” y “backdoor.exe” fueron copiados al sistema (C:\) y se creo un acceso directo al directorio de “Inicio” del usuario “All users”.

Descripción del Sistema:

Durante la etapa de recolección de información se detectó la siguiente conexión activa:

Proto	Dirección local	Dirección remota
TCP	192.168.188.134:1030	192.168.188.1:80

Armado de una lista de palabras a buscar referentes a programas o archivos a recuperar:

srch_strings “opción” image.dd
srch_strings –a -t –d image.img > lista_de_palabras.str
grep –i –f lista.txt lista_de_palabras.str

Desafío USB/Backdoor – (5) Análisis de Medios/Búsqueda string/byte:

Armado de una lista de palabras a buscar referentes a programas o archivos a recuperar:

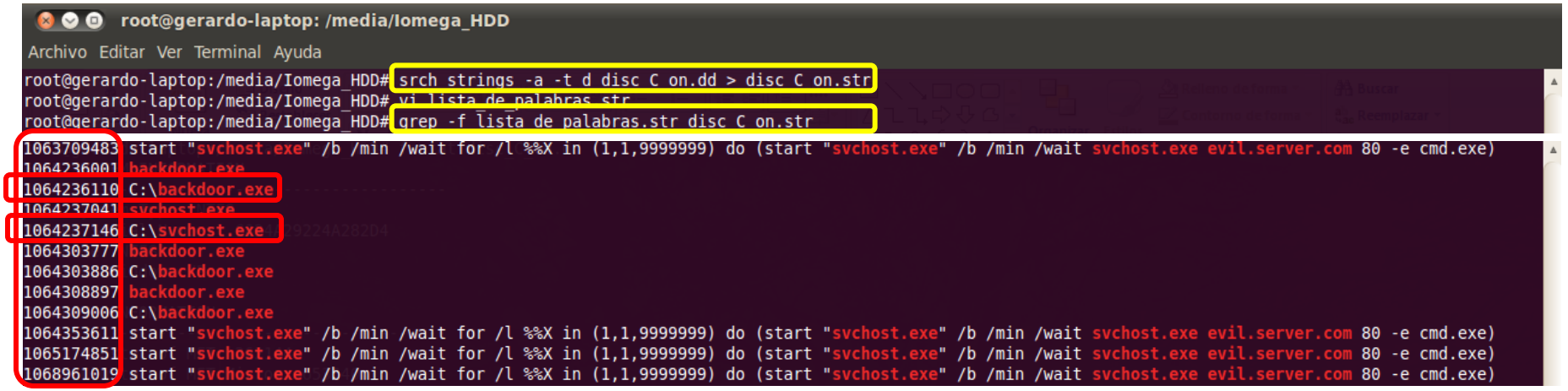
srch_strings “opción” image.dd opciones: (-a todo los strings, -t o/x/d base 8, 10 o 16; -e l/b litte endian/big endian).

srch_strings –a -t –d image.img > lista_de_palabras.str

Esto nos da como resultado el “byte offset” y a continuación el string.

grep –i –f lista.txt lista_de_palabras.str

Ej. Lsta_de_palabras.str: backdoor.exe, svchost.exe, evil.server.com



Desafío USB/Backdoor – (6) Recuperación de Datos:

Descripción de la capa "Sistema de Archivos" de la imagen del disco (copia de la evidencia):

Comando "fsstat":

- Nos muestra estadísticas de la capa sistema de archivos.

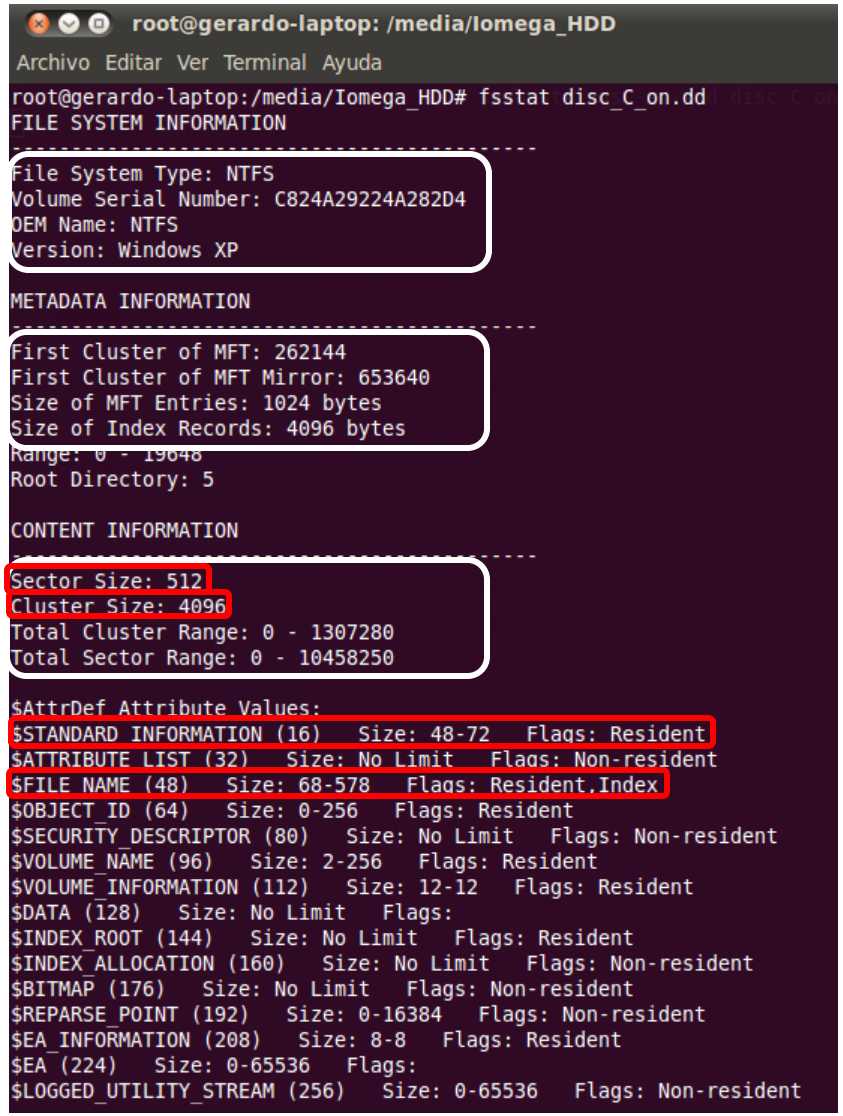
- **fsstat -f "*type*" "*imagefile.dd*"**

Byte Offset + Cluster Size:

Byte offset / Cluster Size = Número de Bloque.

1064236110 / 4096 = 259696

El bloque "259696" contiene el string que buscamos!!!



Desafío USB/Backdoor – (6) Recuperación de Datos:

Estado del Bloque: Asignado o Sin Asignar?

Herramienta "**blkstat**":

- Nos muestra estadísticas sobre un bloque de datos.

Busco el ínodo (metadatos):

Herramienta "**ifind**":

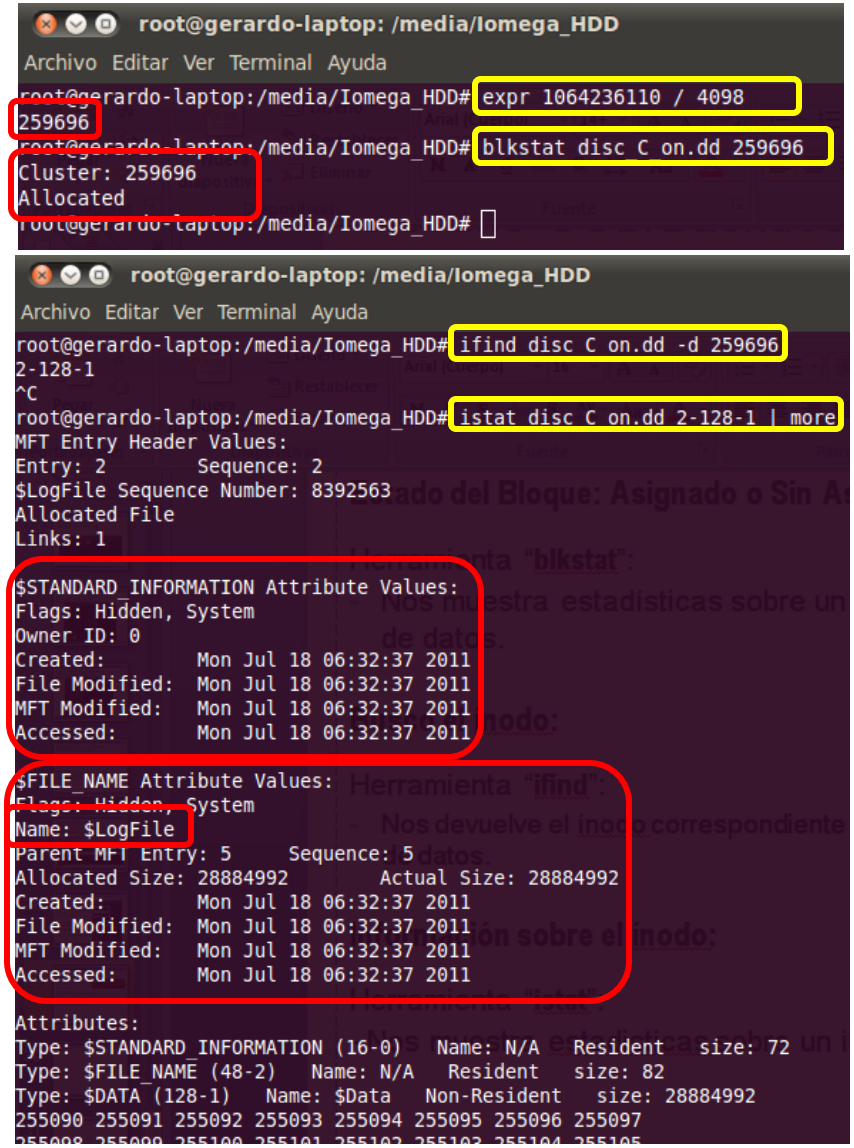
- Nos devuelve el ínodo correspondiente a el bloque de datos.

Información sobre el ínodo (metadatos):

Herramienta "**istat**":

- Nos muestra estadísticas sobre un inodo.

NO es nuestro archivo.



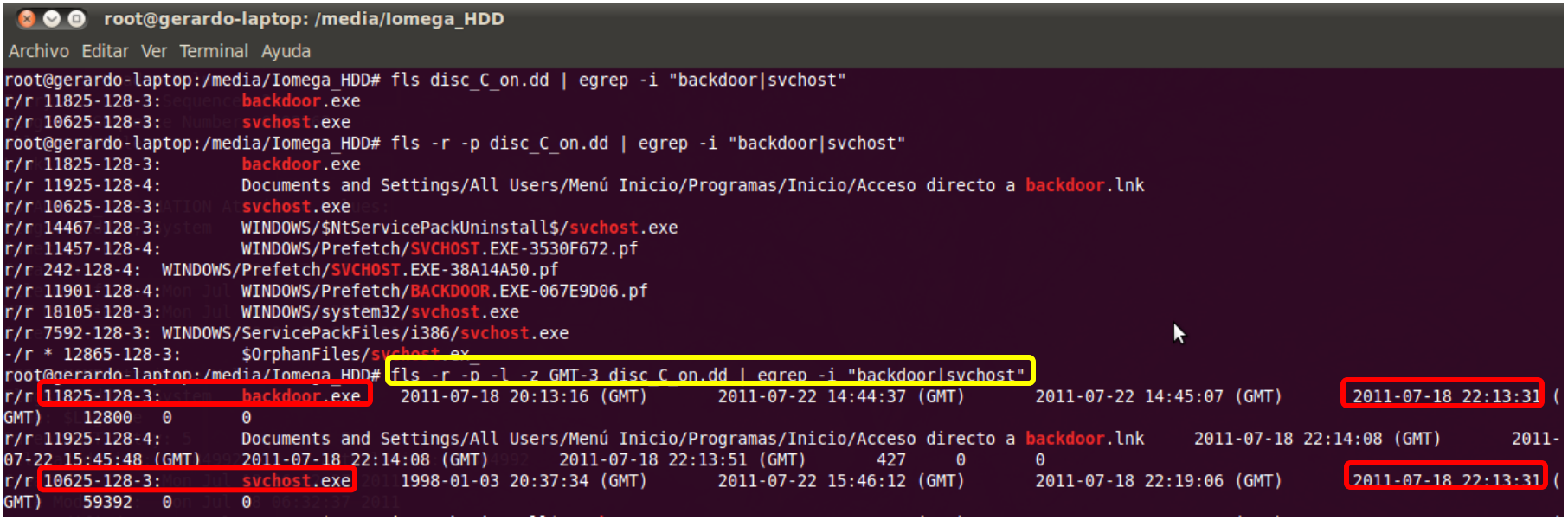
Desafío USB/Backdoor – (6) Recuperación de Datos:

Capa Sistema de Archivos:

Herramienta "**fls**":

- Nos permite interactuar con una imagen forense como si fuera un sistema de archivos normal.
- Toma el valor del inodo de un directorio, procesa el contenido, y despliega el nombre de los archivos en el directorio (incluídos los archivos borrados).

fls –r –p "*image.dd*" > image.fls



Desafío USB/Backdoor – (6) Recuperación de Datos:

Capa Metadatos:

Herramienta "**istat**":

```
root@gerardo-laptop: /media/Iomega_HDD
Archivo Editar Ver Terminal Ayuda
root@gerardo-laptop:/media/Iomega_HDD# icat -r disc_C_on.dd 11825-128-3 > backdoor.exe
root@gerardo-laptop:/media/Iomega_HDD# istat disc_C_on.dd 11825-128-3
MFT Entry Header Values:
Entry: 11825        Sequence: 25
$LogFile Sequence Number: 53620025
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Created:        Mon Jul 18 16:13:31 2011
File Modified:  Mon Jul 18 14:13:16 2011
MFT Modified:   Fri Jul 22 08:45:07 2011
Accessed:       Fri Jul 22 08:44:37 2011

$FILE_NAME Attribute Values:
Flags: Archive
Name: backdoor.exe
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 0       Actual Size: 0
Created:        Mon Jul 18 16:13:31 2011
File Modified:  Mon Jul 18 16:13:31 2011
MFT Modified:   Mon Jul 18 16:13:31 2011
Accessed:       Mon Jul 18 16:13:31 2011

$OBJECT_ID Attribute Values:
Object Id: 42aefd29-0c00-eaaf-11e0-b17211a6e214

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 90
Type: $OBJECT_ID (64-4)   Name: N/A   Resident   size: 16
Type: $DATA (128-3)   Name: $Data   Non-Resident   size: 12800
1179189 1179190 1179191 1179192
```

```
root@gerardo-laptop: /media/Iomega_HDD
Archivo Editar Ver Terminal Ayuda
Type: $OBJECT_ID (64-4)   Name: N/A   Resident   size: 16
Type: $DATA (128-3)   Name: $Data   Non-Resident   size: 59392
1186020 1186021 1186022 1186023 1186024 1186025 1186026 1186027
1186028 1186029 1186030 1186031 1186032 1186033 1186034
root@gerardo-laptop:/media/Iomega_HDD# istat disc_C_on.dd 10625-128-3
MFT Entry Header Values:
Entry: 10625        Sequence: 24
$LogFile Sequence Number: 54820069
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Created:        Mon Jul 18 16:13:31 2011
File Modified:  Sat Jan  3 14:37:34 1998
MFT Modified:   Mon Jul 18 16:19:06 2011
Accessed:       Fri Jul 22 09:46:12 2011

$FILE_NAME Attribute Values:
Flags: Archive
Name: svchost.exe
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 0       Actual Size: 0
Created:        Mon Jul 18 16:13:31 2011
File Modified:  Mon Jul 18 16:13:31 2011
MFT Modified:   Mon Jul 18 16:13:31 2011
Accessed:       Mon Jul 18 16:13:31 2011

$OBJECT_ID Attribute Values:
Object Id: 42aefd29-0c00-eaaf-11e0-b17211a6e215

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 88
Type: $OBJECT_ID (64-4)   Name: N/A   Resident   size: 16
Type: $DATA (128-3)   Name: $Data   Non-Resident   size: 59392
1186020 1186021 1186022 1186023 1186024 1186025 1186026 1186027
1186028 1186029 1186030 1186031 1186032 1186033 1186034
```

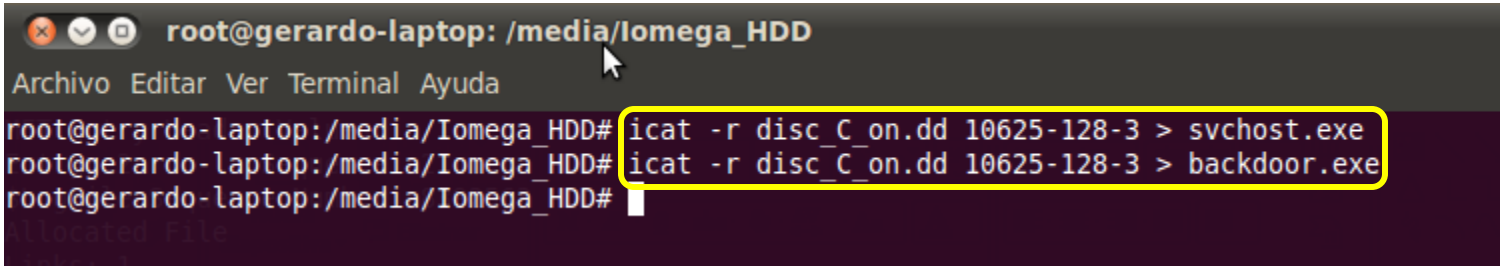
Desafío USB/Backdoor – (6) Recuperación de Datos:

Capa Metadatos:

Herramienta "**icat**":

- Copia archivos por inodo.
- Opera en disco e imágenes de discos.

icat –r "*image.dd*" "*numero*" > "*archivo.ext*"



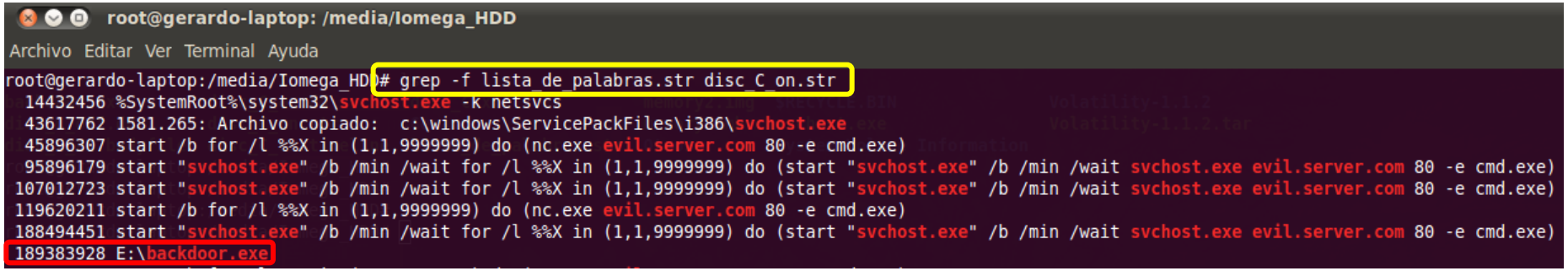
Recuperamos los archivos!: Ahora podemos analizar los archivos en un ambiente controlado. De ser necesario podemos remitir estos archivos a nuestro proveedor antivirus para que detecte el mismo en la siguiente definición de virus.

Desafío USB/Backdoor – (6) Recuperación de Datos:

Método de Infección:

- Correo electrónico: Ver logs de los servidores de correo, analizar pst.
- USB: Analizar el registro buscando indicios de conexión de un dispositivo USB.
- Internet: Analizar archivos del navegador: IE/FireFox/Chrome.

El resultado del la búsqueda de strings muestra que la infección pudo ingresar por dispositivo USB:



Desafío USB/Backdoor – (6) Recuperación de Datos:

Registro de Windows (repaso):

Registro de Windows:

- Colección de archivos de datos (HIVES) que guardan información del sistema y el usuario

  "%windows%\System32\Config":

  * SAM: todas las cuentas de usuarios y grupos (HKEY_LOCAL_MACHINE\SAM).

  * SECURITY: toda la información de seguridad usada por SAM y el sistema operativo, incluyendo políticas de contraseña, membrecía de grupos, etc. (HKEY_LOCAL_MACHINE\SECURITY).

  * SOFTWARE: toda la configuración de las aplicaciones. (HKEY_LOCAL_MACHINE\SOFTWARE).

  * SYSTEM: configuración del servicios y hardware. (HKEY_LOCAL_MACHINE\SYSTEM).

  * DEFAULT: (HKEY_LOCAL_MACHINE\DEFAULT).

- Cada usuario tiene su propio registro:

  *"C:\Documents and Settings*username*\NTUSER.dat" (HKEY_CURRENT_USER).
  *"C:\Users\username\NTUSER.dat" (solo vista): (HKEY_CURRENT_USER).

  Nos pueden mostrar detalles críticos para nuestra investigación relacionados al sistema y los usuarios individuales.

Desafío USB/Backdoor – (6) Recuperación de Datos:

Registro de Windows (repaso):

Registro de Windows:

- SYSTEM: configuración del servicios y hardware. (HKEY_LOCAL_MACHINE\SYSTEM).
  - Nombre del Equipo.
  - Zona Horaria.
  - Interfaces de Red y su configuración.
  - Redes Wireless a las que se ha conectado el equipo.
  - Programas de inicio automático.
  - Recursos Compartidos del sistema.
  - Fecha de ultimo apagado del equipo y número de veces que se apagó el equipo.
- NTUSER.dat: (HKEY_CURRENT_USER).
  - Historial de Búsqueda: NTUSER.dat\Software\Microsoft\Search Assistant\ACMru
  - URLs Tipeadas: NTUSER.dat\Software\Microsoft\Internet Explorer\TypedURLs
  - Documentos Recientes: NTUSER.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
  - Ventanas de Diálogos Open/Save:
    - Save: NTUSER.dat\Software\Microsoft\Windows\CurrentVersion\ComDlg32\OpenSavePIDIMRU
    - Open: NTUSER.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
  - Último comando ejecutado: NTUSER.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\RunRMU
  - Historial de Ejecución de Aplicaciones: NTUSER.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssis\{GUID}\count

Desafío USB/Backdoor – (6) Recuperación de Datos:

Claves del Registro vinculadas a dispositivos USB:

Windows XP:

- Determinar el Vendedor, Producto, Versión, y S/N:

  * “SYSTEM\CurrentControlSet\Enum\USBSTOR”

    Vendedor =
    Producto =
    Versión =
    S/N =

- Determinar el ID de Vendedor y el ID del Producto:

  * “SYSTEM\CurrentControlSet\Enum\USB” (buscamos por S/N).

    VID_XXXX =
    PID_YYYY =

- Determinar la letra asignada al dispositivo y GUID:

  * “SYSTEM\MountedDevices” (búsqueda por ID).

    Letra =
    GUID =

- Determinar el usuario que utilizó el dispositivo y la última vez que fue conectado:

  * “NTUSER.dat\Software\Mifrosoft\Windows\CurrentVersion\Explorer\MountPoint2” (buscamos por GUID).

    Usuario =
    Ultima vez que el dispositivo fue conectado =

Desafío USB/Backdoor – (6) Recuperación de Datos:

Analizando el registro con “RegRipper”:

- Montamos la copia de la imagen del disco:

```
mount -t ntfs-3g -o loop,ro,noexec,show_sys_files /media/Iomega_HDD/disc_C_off.dd  /media/WinXP_Infected/
```

- Usando la herramienta “regripper” analizamos el registro:

```
perl rip.pl -r /media/WinXP_Infected/WINDOWS/system32/config/system -f system > /media/Iomega_HDD/system.txt
perl rip.pl -r /media/WinXP_Infected/Documents\ and\ Settings/Usuario/NTUSER.DAT -f ntuser > /media/Iomega_HDD/ntuser.txt
```

- Determinar el ID de Vendedor y el ID del Producto:

Vendedor = Ven_Verbatim
Producto = Prod_STORE_N_GO
Versión = Rev_5.00
S/N = 078213A0000B
FriendlyName: Verbatim STORE N GO USB Device
ParentIdPrefix: 8&18eed44f&0
Letra = E:
GUID = 5e94e308-b147-11e0-afe3-000c29fdae42
Usuario = “Usuario” (5e94e308-b147-11e0-afe3-000c29fdae42)
Ultima vez que el dispositivo fue conectado = Mon Jul 18 22:12:01 2011 (UTC)

Desafío USB/Backdoor – (6) Recuperación de Datos:

Analizando el disco USB:

- Hacemos una copia de disco USB:

fdisk -l

Disco /dev/sdc: 4007 MB, 4007657472 bytes
16 cabezas, 32 sectores/pista, 15288 cilindros
Unidades = cilindros de 512 * 512 = 262144 bytes
Tamaño de sector (lógico / físico): 512 bytes / 512 bytes
Tamaño E/S (mínimo/óptimo): 512 bytes / 512 bytes
Identificador de disco: 0x73431463

Disposit.	Inicio	Comienzo	Fin	Bloques	Id	Sistema
/dev/sdc1		1	15288	3913712	b	W95 FAT32

dd if=/dev/sdc1 of=usb_image.dd conv=noerror,sync

md5sum usb_image.dd

```
root@gerardo-laptop: ~
Archivo  Editar  Ver  Terminal  Ayuda
root@gerardo-laptop:~# dd if=/dev/sdc1 of=/media/Iomega_HDD/usb_image.dd conv=noerror,sync
7827424+0 registros de entrada
7827424+0 registros de salida
4007641088 bytes (4,0 GB) copiados, 1081,41 s, 3,7 MB/s
root@gerardo-laptop:~# md5sum /media/Iomega_HDD/usb_image.dd
e93ed2f8ed824c85b47cd49344a9e2c3  /media/Iomega_HDD/usb_image.dd
root@gerardo-laptop:~#
```

Desafío USB/Backdoor – (6) Recuperación de Datos:

Analizando el disco USB:

- Usamos la herramienta “fls” para buscar los archivos sospechosos dentro del disco USB (esto es posible si la evidencia ya no fue sobrescrita por el uso o si el disco fue wipeado):

  fls –d –a –r –p –l –z GMT-3 usb_image.dd | grep lista_de_palabras.str

Los archivos fueron eliminados pero la capa “nombre de archivo” conserva la información ya que no ha sido sobrescrita. En caso de haber sido sobrescrita, podemos hacer una búsqueda de strings en todos los bloques de datos.

```
root@gerardo-laptop: ~
Archivo  Editar  Ver  Terminal  Ayuda
root@gerardo-laptop:~# fls -d -a -r -p -l -z GMT-3 /media/Iomega_HDD/usb_image.dd | grep -f /media/Iomega_HDD/lista_de_palabras.str
r/r * 3:        _ackdoor.exe    2011-07-18 14:13:16 (GMT)       2011-07-22 00:00:00 (GMT)       0000-00-00 00:00:00 (UTC)       2011-07-22 14:44:37 (GMT)   1
2800    0       0
r/r * 4:        _vchost.exe     1998-01-03 14:37:34 (GMT)       2011-07-22 00:00:00 (GMT)       0000-00-00 00:00:00 (UTC)       2011-07-22 14:44:37 (GMT    5
9392    0       0
r/r * 8:        Acceso directo a backdoor.lnk   2011-07-18 16:14:10 (GMT)       2011-07-22 14:44:37 (GMT)       0000-00-00 00:00:00 (UTC)       2011-07-22 14
:44:37 (GMT)    427     0       0
```

Desafío USB/Backdoor – (6) Recuperación de Datos:

Analizando el disco USB:

- Usamos la herramienta “istat” para ver la información de la capa “metadata”. Luego con la herramienta “icat” recuperamos los archivos borrados:

```
root@gerardo-laptop:~# istat /media/Iomega_HDD/usb_image.dd 3 | grep "Name:" -B 4
Directory Entry: 3
Not Allocated
File Attributes: File, Archive
Size: 12800
Name:   ackdoor.exe
root@gerardo-laptop:~# istat /media/Iomega_HDD/usb_image.dd 4 | grep "Name:" -B 4
Directory Entry: 4
Not Allocated
File Attributes: File, Archive
Size: 59392
Name:   vchost.exe
root@gerardo-laptop:~# istat /media/Iomega_HDD/usb_image.dd 8 | grep "Name:" -B 4
Directory Entry: 8
Not Allocated
File Attributes: File, Archive
Size: 427
Name:   CCESO~1.LNK
```

```
root@gerardo-laptop:~# icat /media/Iomega_HDD/usb_image.dd 3 > backdoor.exe
root@gerardo-laptop:~# icat /media/Iomega_HDD/usb_image.dd 4 > svchost.exe
root@gerardo-laptop:~# icat /media/Iomega_HDD/usb_image.dd 8 > backdoor.lnk
```

Desafío USB/Backdoor – (6) Recuperación de Datos:

Analizando el disco USB:

- Usamos la herramienta “md5sum” para verificar que los archivos recuperados del disco USB y de la imagen del equipo son el mismo archivo:

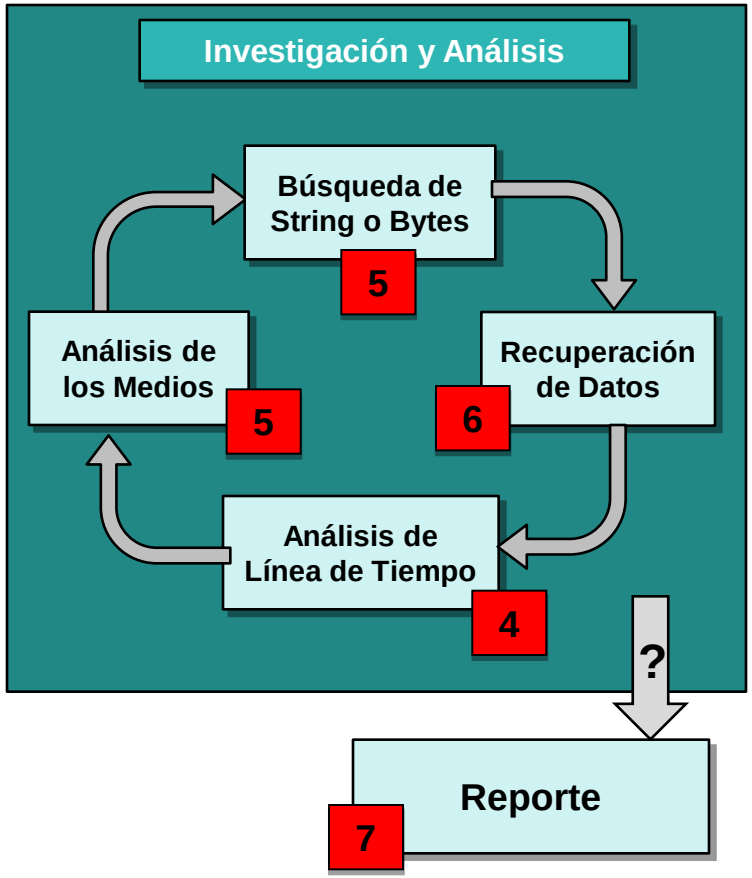
```
root@gerardo-laptop:/media/Iomega_HDD# md5sum usb_backdoor.exe
88b5fd06d2561588d6a55b59075743d3  usb_backdoor.exe
root@gerardo-laptop:/media/Iomega_HDD# md5sum backdoor.exe
88b5fd06d2561588d6a55b59075743d3  backdoor.exe
root@gerardo-laptop:/media/Iomega_HDD# md5sum usb_svchost.exe
e0fb946c00b140693e3cf5de258c22a1  usb_svchost.exe
root@gerardo-laptop:/media/Iomega_HDD# md5sum svchost.exe
e0fb946c00b140693e3cf5de258c22a1  svchost.exe
```

Conocemos el método de infección que a su vez vincula al usuario con la infección del equipo.

Ciclo de Vida para Análisis Forense

¿Finalizó la etapa de Investigación y Análisis?

- Debemos poder describir en detalle lo acontecido en el Incidente y detectar cualquier otro indicio de malware en el sistema para luego pasar a la etapa de Reporte.



Desafío USB/Backdoor – (7) Reporte:

Puntos a tener en cuenta para armar el Reporte:

- Hacer el reporte no es un aspecto técnico del análisis forense.
- La mayoría de los reportes son hechos para personas que no manejan aspectos técnicos de hardware, red, leyes criminales de computación.
- Debemos asegurarnos de que nuestro reporte explique claramente la evidencia encontrada, las técnicas utilizadas, y defina todo lo que es técnico.

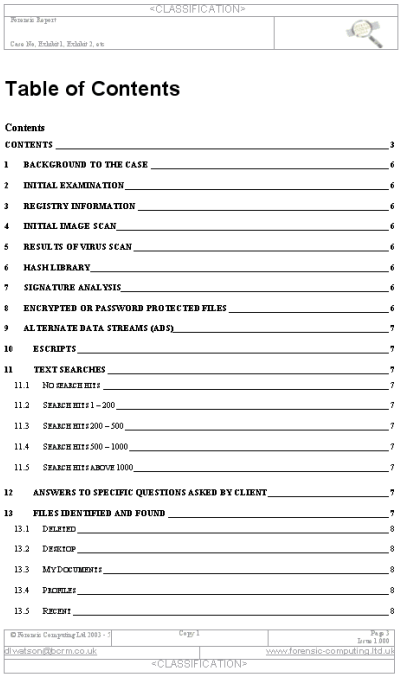
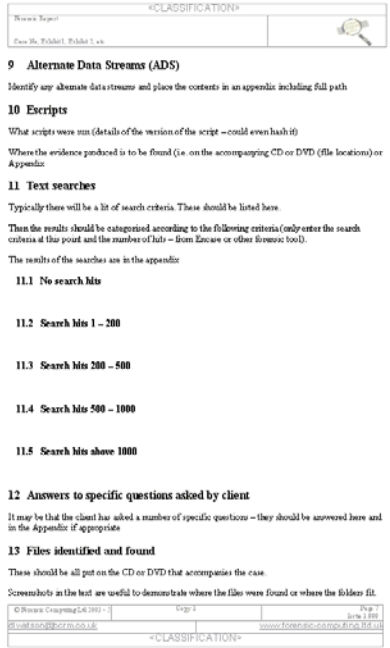


Table of Contents

Contents



9 Alternate Data Streams (ADS)

Identify any alternate data streams and place the contents in an appendix including full path

10 Escripts

What scripts were run (details of the version of the script – could even hash it)

Where the evidence produced is to be found (i.e. on the accompanying CD or DVD (file locations) or Appendix

11 Text searches

Typically there will be a lit of search criteria. These should be listed here.

Then the results should be categorised according to the following criteria (only enter the search criteria at this point and the number of hits – from Encase or other forensic tool).

The results of the searches are in the appendix

11.1 No search hits

11.2 Search hits 1 – 200

11.3 Search hits 200 – 500

11.4 Search hits 500 – 1000

11.5 Search hits above 1000

12 Answers to specific questions asked by client

It may be that the client has asked a number of specific questions – they should be answered here and in the Appendix if appropriate

13 Files identified and found

These should be all put on the CD or DVD that accompanies the case.

Screenshots in the text are useful to demonstrate where the files were found or where the folders fit.

Desafío USB/Backdoor

FIN