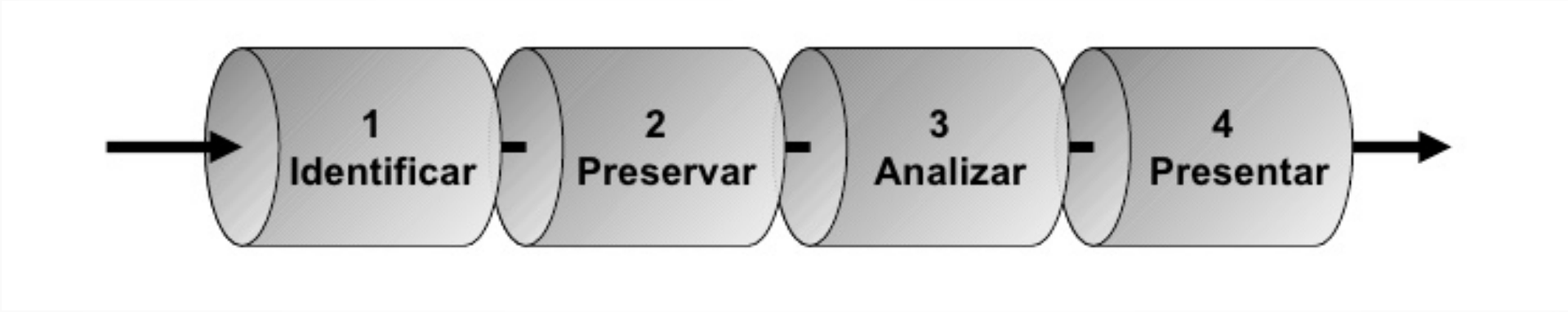
Metodologías de Análisis Forense

- El análisis Forense de un sistema informático nos permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad.

- “Es el proceso de identificar, preservar, analizar y presentar evidencia digital, de manera que esta sea legalmetne aceptable”



Identificación de la Evidencia

Principio de Locard

"Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto"

- Del mismo modo se cumple el principio de locard a la hora de realizar el propio análisis forense digital por lo que ser especialmente cuidadoso para que el sistema se vea afectado en la menor medida posible y que las evidencias asquiridas no se vean alteradas.

Tipos de análisis forense

- Análisis Forense de Sitemas (Sistema Operativos Windows, OSX, GNU/Linux,…)
- Análsis forense de redes
- Análisis forense de sistemas embebidos
- Análisis forense de memoria volátil.

Características

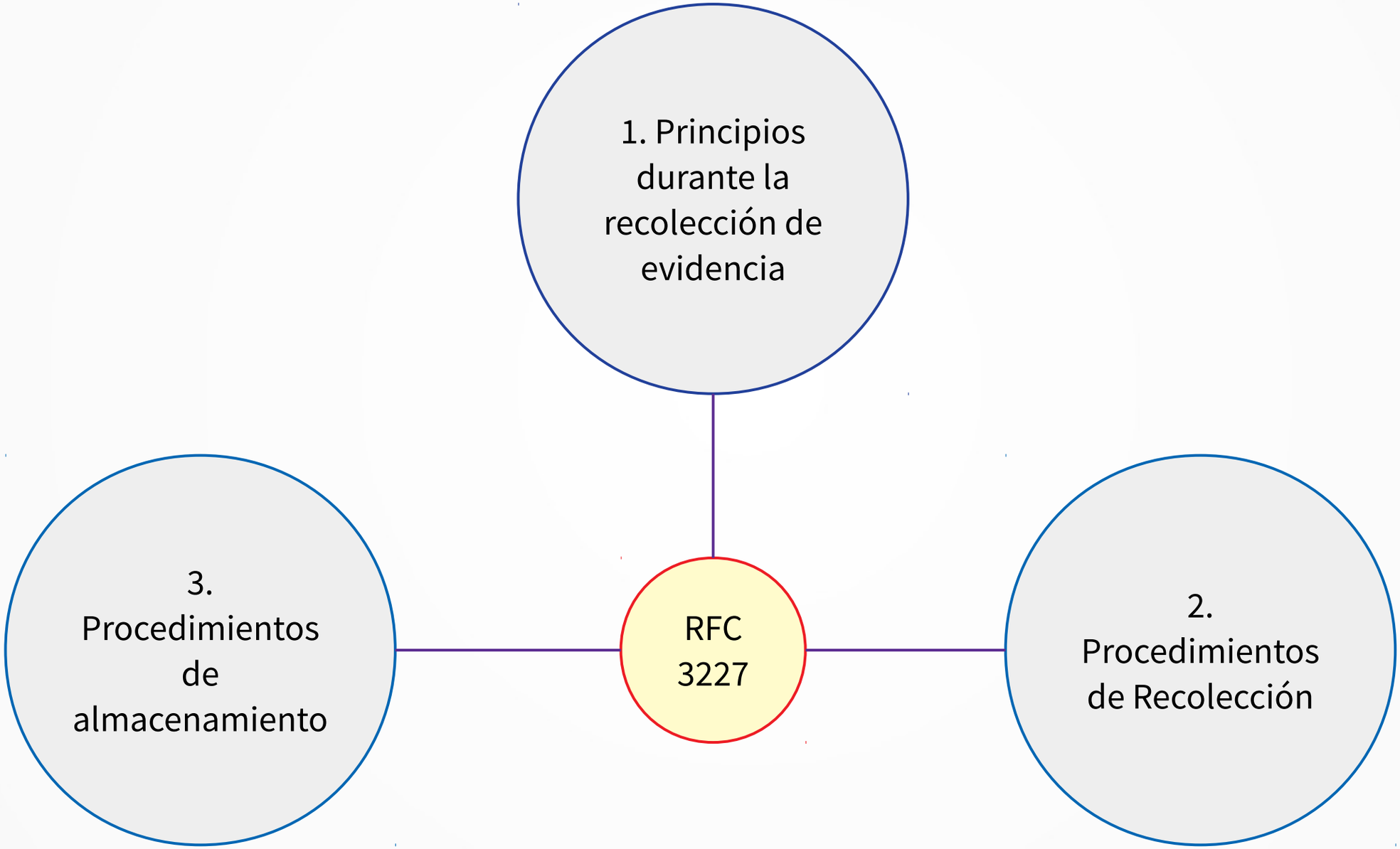
- El procedimiento de análisis forense debe poseer las siguietnes características:
  - Verificable
  - Reproducible
  - Documentado
  - Independiente

Incidentes de seguridad informática

- Un incidente de seguridad es cualquier acción fuera de la ley o no autorizada.
- Existe una gran cantidad de incidentes relacionados con la seguiridad informática.

Directrices para la recolección de evidencias y su almacenamiento

- El RFC-3227 es un documento que recoge las “directrices para la recopilación de evidencias y su almacenamiento” y puede llegar a servir como estándar de facto para la recopilación de información en incidentes de seguridad.


1. Principios durante la recolección de evidencia
3. Procedimientos de almacenamiento
RFC 3227
2. Procedimientos de Recolección

Principios durante la recolección de evidencias

1) Orden de volatilidad
2) Acciones que deben evitarse
3) Consideraciones de privacidad
4) Consideraciones legales

- Capturar una imagen del sistema tan precisa como sea posible.
- Realizar notas detalladas, incluyendo fechas horas indicando si se utiliza horario local o UTC
- Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo
- En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis
- Recoger la información según el orden de voaltilidad (de mayor a menor)
- Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.

Procedimiento de recolección

- Transparentes y reproducibles
- Colección de Pasos

Procedimiento de almacenamiento

- Cadena de custodia
- Dónde y cómo almacenarlo

Inicio del Proceso

- Comenzar etiquetando, inventariando y fotografiando todos los dispositivos que se van a analizar.
- Se procede a la recopilación de las evidencias:
  - Se puede clasificar por tipo de información:
    - Volátil
    - No volátil
- También se peude hacer un análsisis en caliente de un sistema en funcionamiento, o análisis en frio de un sistema que está apagado.

Preservación

- En esta segunda fase, procedemos a ejecutar los 3 pasos para adquirir la evidencia sin alterarla o dañarla, se autentica que la información de la evidencia sea igual a la original.

- Se debe definir los equipos y herramientas determinadas para llevar a cabo la investigación. Lograr un entorno de trabajo adecuado para el análisis y la investigación.

Iniciar una Bitácora, que nos permita documentar de manera precisa identificar y autenticar los datos que se recogen, tipo:

- ¿Quién realiza la acción y por qué lo hicieron.
- ¿Qué estaban tratando de lograr?
- ¿Cómo se realiza la acción, incluidas las herramientas que utilizaban y los procedimientos que siguieron.
- Cuando se realizó la acción (fecha y hora) y los resultados.

De igual forma, se toman otras fuentes de información de los sistemas vivos, los datos volátiles como:

- Cache del Sistema
- Archivos temporales
- Registros de sucesos.
- Registros de internos y externos que los dispositivos de red, tales como firewalls, routers, servidores proxy,etc.
- Logs del sistema, Aplicaciones.
- Tablas de enrutamiento (arp, cache de Netbios, lista de procesos, información de la memoria y el kernel)
- Registros remotos e información de monitoreo relevante

- Realizar copia imagen de los dispositivos (bit a bit), con una herramienta apropiada, Y firmar su contenido con un hash de MD5 o SHA1, generando así el segundo original, a partir de este se generaran las copias para el Análisis de datos, cada copia debe ser comprobada con firmas digitales nuevamente de MD5 o SHA1.

- Documente la evidencia con el documento del embalaje (y cadena de custodia) que puedan garantizar que se incluye información acerca de sus configuraciones. Por ejemplo, anote el fabricante y modelo, configuración de los puentes, y el tamaño del dispositivo. Además, tenga en cuenta el tipo de interfaz y de la condición de la unidad.

Importante considerar las buenas practicas para conservar la información y la evidencia.

Buenas practicas para conservar la información y la evidencia

- Asegurar de manera física un lugar para almacenar los datos, evitando su manipulación. No olvide documentarlo.
- Proteger los equipos de almacenamiento de los campos magnéticos (estática).
- Realice mínimo el segundo original y una copia del segundo original para el análisis y almacene el segundo original en un sitio seguro

Buenas practicas para conservar la información y la evidencia

- Asegurar que la evidencia está protegido digital y físicamente (por ejemplo, en una caja fuerte, asignar una contraseña a los medios de almacenamiento).

  Nuevamente, no olvide actualizar el documento de Cadena de custodia (incluye información como el nombre de la persona que examina la evidencia, la fecha exacta y el tiempo que echa un vistazo a las pruebas, y la fecha exacta y hora en que lo devuelva).

Buenas practicas para conservar la información y la evidencia

- Se pretende que esta información sea:
  - Autentica
  - Correcta
  - Completa
  - Convincente

ANÁLISIS DE DATOS:

- Análisis de Datos de la Red
- Análisis de los Datos del Host
- Análisis de los Medios de Almacenamiento

Análisis de Datos de la Red:

Para nuestra investigación nos centraremos en identificar los dispositivos de comunicación y de defensa perimetral (Servidores Web, Firewall, IDS’s, IPS’s, Proxys, Filtros de Contenido, Analizadores de Red, Servidores de Logs, etc) que están en la Red, con la finalidad de recuperar los logs que se han tomado como parte de la gestión de red.

Análisis de los Datos del Host:

- Generalmente se logra con la información obtenida de los sistemas vivos, de la lectura de las Aplicaciones y los Sistemas Operativos.
- Debemos de limitarnos a tratar de recuperar estos archivos de la evidencia en procesos de Data Carving o Recuperación de Datos, y definir criterios adecuados de búsqueda, debido a que lo mas probable es que encontremos una gran cantidad de información que nos puede complicar o facilitar el análisis de datos, dependiendo de nuestros objetivos de búsqueda Posteriormente definiremos a que archivos le realizaremos la búsqueda.

Análisis de los Medios de Almacenamiento:

- Igual que el punto anterior debemos definir criterios de búsqueda con objetivos claros, debido a la gran cantidad de información disponible, que nos puede desviar la atención o sencillamente complicar el proceso de análisis de la información

Análisis de los Medios de Almacenamiento

Tengamos en cuenta las siguientes buenas practicas:

- No olvidemos, que se debe utilizar la copia del segundo original, a su vez el segundo original preservarlo manteniendo un buen uso de la cadena de custodia.
- Determinar si los archivos no tienen algún tipo de cifrado (varias claves del registro no lo pueden determinar).
- Preferiblemente descomprimir los archivos con sistemas de compresión

Análisis de los Medios de Almacenamiento

Tengamos en cuenta las siguientes buenas practicas:

- Crear una estructura de Directorios y Archivos recuperados.
- Identificar y recuperar los archivos objetivo (determinados por algunos criterios, ejemplo aquellos que han sido afectados por el incidente). Y se puede comparar su hash (archivos del sistema operativo y aplicaciones) con los hash de archivos que nos facilita la http://www.nsrl.nist.gov/, o sitios como: http://www.processlibrary.com/
- Analizar archivos de Booteo y configuración del sistema, el registro del sistema

Análisis de los Medios de Almacenamiento

Tengamos en cuenta las siguientes buenas practicas:

- Información de Login / Logout del sistema, nombres de usuario e información del AD (Directorio Activo)
- Software instalado, actualizaciones y parches.
- Buscar archivos con NTFS ADS (Alterna Data Stream)
- 10. Estudio de las Metadata (en especial identificar las marcas de tiempo, creación, actualización, acceso, modificación,etc).
- 11. La evidencia debe ser cargada de solo lectura, para evitar daños o alteraciones sobre las copias del segundo original.

PREPARACIÓN DEL INFORME

Es la fase final y la mas delicada e importante la cual sera el documento que sustentara una prueba en un proceso legal, básicamente tener en cuenta estos dos pasos:

- Organización de la Información
- Escribir el Informe Final

Organización de la Información:

1. Retomemos toda la documentación generada en las fases de la metodología e igual cualquier información anexa como notas, antecedentes o informe policial.

2. Identifiquemos lo mas importante y pertinente de la investigación

3. Realizar conclusiones (tenga en cuenta los hechos) y crear una lista de las pruebas para presentar en el informe.

Escribir el Informe Final

- Debe ser claro, conciso y escrito en un lenguaje entendible para gente común (no tan técnico).
- Debe contener como mínimo:
- Propósito del Informe. Explicar claramente el objetivo del informe, el público objetivo, y por qué se preparó el informe.
- Autor del informe. Todos los autores y co-autores del informe, incluyendo sus posiciones, las responsabilidades durante la investigación, y datos de contacto.

Escribir el Informe Final

- Resumen de Incidentes. Introducir el incidente y explicar su impacto. El resumen deberá estar escrito de manera que una persona no técnica, como un juez o jurado sería capaz de entender lo que ocurrió y cómo ocurrió.
- Pruebas. Proporcionar una descripción de las pruebas de que fue adquirido durante la investigación. Cuando el estado de la evidencia que describen la forma en que fue adquirida, cuándo y quién lo adquirió.

Escribir el Informe Final

- Detalles. Proporcionar una descripción detallada de lo que la evidencia se analizó y los métodos de análisis que se utilizaron. Explicar los resultados del análisis. Lista de los procedimientos que se siguieron durante la investigación y de las técnicas de análisis que se utilizaron. Incluir una prueba de sus resultados, tales como los informes de servicios públicos y las entradas de registro. Justificar cada conclusión que se extrae del análisis.

Escribir el Informe Final

- ...Detalles.

  Sello documentos de apoyo, el número de cada página, y se refieren a ellos por el nombre de la etiqueta cuando se examinan en el análisis. Por ejemplo, “registro de Firewall de servidor, documento de apoyo D.” Además, proporcionan información sobre aquellos individuos que realizaron o participaron en la investigación. Si procede, proporcione una lista de testigos.

Escribir el Informe Final

- Conclusión. Resumir los resultados de la investigación. La conclusión debe ser específica de los resultados de la investigación. Citar pruebas concretas para demostrar la conclusión, pero no dar excesivos detalles acerca de cómo se obtuvieron las pruebas (tal información debe estar en la sección “Detalles”). Incluir una justificación para su conclusión, junto con las pruebas y la documentación. La conclusión debe ser lo más clara y sin ambigüedades como sea posible. En muchos casos, se declaró cerca del comienzo del informe, porque representa la información procesable.

Escribir el Informe Final

- Los documentos justificativos. Incluya cualquier información de antecedentes a que se refiere en todo el informe, tales como diagramas de red, los documentos que describen los procedimientos de investigación de equipos usados, y un panorama general de las tecnologías que intervienen en la investigación. Es importante que los documentos justificativos proporcionen información suficiente para que el lector del informe pueda comprender el incidente tan completamente como sea posible.

Otros modelos de análisis forense

- Modelo de Casey (2000)
  - Identificación
  - La conservación, adquisisción y documentación
  - La clasificación, comparación y la individualización
  - La reconstrucción

Otros modelos de análisis forense

- Modelo publicado por el U.S. Dep.
  - Identificación
  - Conservación
  - Análisis
  - Presentación

Otros modelos de análisis forense

- Modelo de Lee (2001)
  - Reconocimiento
  - Identificación
  - Individualización
  - Reconstrucción

Otros modelos de análisis forense

- Modelo de DFRWS (2001)
  - Identificación
  - Preservación
  - Colección
  - Exámen
  - Análisis
  - Presentación
  - Decisión

Otros modelos de análisis forense

- Modelo de Reith, Carr y Gunsch(2002)
  - Identificación
  - Prepración
  - Estrategia de acercamiento
  - Preservación
  - Colección
  - Examen
  - Análisis
  - Presentación
  - Devolución de la evidencia