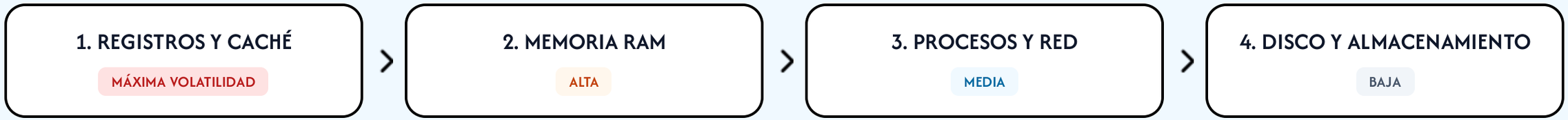
ORDEN DE VOLATILIDAD

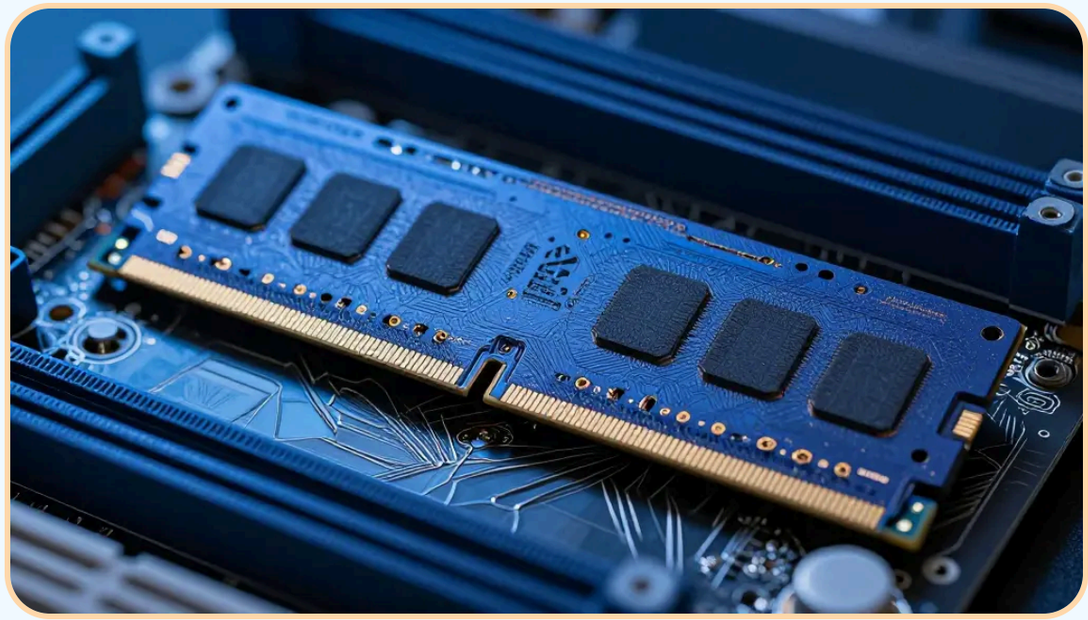


El orden de volatilidad se refiere a la susceptibilidad de los datos a cambiar o perderse dentro de un sistema de información. Este concepto es crucial tanto en el anólisis forense digital como en la respuesta a incidentes.

El orden de volatilidad clasifica los datos desde los mós susceptibles a perderse hasta aquellos que se mantienen estables. Al recolectar la evidencia se debe proceder en función de la volatilidad de los datos, es decir, de lo mós volótil a lo menos volótil. Para un sistema de información típico, el orden de recolección sería:

Altamente volátil

Altamente volátil: registros y caché. Son los más volótiles y pueden cambiar rópidamente mientras el sistema está en funcionamiento. La información obtenida de estas memorias suele tener poca utilidad, pero debe ser capturada como parte de la imagen de memoria del sistema.



Medianamente volátil

Medianamente volátil: memoria RAM, estadísticas del kernel, tablas de enrutamiento, caché ARP y tabla de procesos. Estas ubicaciones incluyen informoción sobre las actividades de la red y los procesos en ejecución.

Evidencias poco volátiles

Las siguientes se consideran evidencias poco volótiles:

l. Archivos temporales.

2. Almacenamiento en disco.

3 Ficheros de logs.

4. Configuración física, topología de red.

5. Almacenamiento externo.

Aplicación en ciberataque

El orden de volatilidad se tendró en cuenta, en el caso de un ciberataque, para analizar en primer lugar los datos volótiles, como la información del estado del sistema, que puede ser importante para la recuperación, y posteriormente los almacenados en disco, los cuales en caso de perderse se pueden restaurar a partir de copias de seguridad.

La guía RFC 3227 no incluye, a la hora de la preservación de los datos, la consideración de los datos en la nube, los cuales pueden ser muy volótiles en algunos casos.

Limitaciones de RFC 3227

RFC 3227

Guía estándar para preservación de evidencias digitales.

La nube

No incluye datos en la nube, que pueden ser altamente volátiles.

Existen una serie de recomendaciones que hay que tener en cuenta para evitar la contaminación de las evidencias. En algunos casos estas recomendaciones son contrarias dependiendo del tipo de evidencia que se quiera recopilar. Por ejemplo, ¿hay que apagar el equipo para recopilar las evidencias? Pues depende:

• **Modo de adquisición live:** se recomienda no apagar el equipo hasta que se haya completado la recopilación de los datos de almacenamiento volótil.

Modo de adquisición dead: se recomienda apagar el equipo, no de forma ordenada, para evitar esos procesos durante el apagado, sino desenchufando la fuente de alimentación (cable de corriente o batería); así se permite realizar una clonación exacta del estado del dispositivo, pues dejándolo encendido podría modificarse por las escrituras en disco.

Durante la adquisición se deben evitar ciertas acciones e intenciones:

- No apagar/encender innecesariamente hasta haber finalizado la recolección, ya sea *live* o *dead*.
- No confiar en los programas del sistema. Utilizar siempre programas externos de recolección de evidencias en medios adecuadamente protegidos.
- No ejecutar programas que modifiquen el tiempo de acceso de los archivos del sistema como tar o xcopy.

No apagar/encender innecesariamente hasta haber finalizado la recolección, ya sea live o dead.
Esta instrucción es fundamental en informática forense para preservar la integridad de la evidencia digital. Apagar un sistema vivo (live) borra la memoria volátil (RAM), perdiendo procesos activos y conexiones de red.

No confiar en los programas del sistema. Utilizar siempre programas externos de recolección de evidencias en medios adecuadamente protegidos. Los ejecutables nativos pueden estar infectados o modificados para ocultar evidencia.

No ejecutar programas que modifiquen el tiempo de acceso de los archivos del sistema como tar o xcopy.
Comandos como tar o xcopy alteran el tiempo de último acceso (atime) de archivos y directorios. Modificar estos metadatos destruye evidencia temporal crucial.

Capturar la memoria RAM durante un ciberataque como WannaCry es crucial para el análisis forense. La RAM contiene información volátil: procesos en ejecución, claves de cifrado utilizadas por el ransomware y conexiones de red activas. Analizar este volcado permite a los expertos comprender el comportamiento del malware, identificar indicadores de compromiso y desarrollar firmas para prevenir futuros ataques.

Ejemplo: WannaCry

Privacidad y confidencialidad en el análisis forense

La guía RFC 3227 también incluye una serie de consideraciones sobre la importancia de garantizar la privacidad y la confidencialidad durante el proceso de recopilación del análisis forense digital:

- Respetar las normas y directrices de privacidad de la empresa y su jurisdicción legal. Es decir, hay que garantizar que ninguna información recopilada junto con la evidencia que se está buscando sea accesible para personas no autorizadas. Por ejemplo, información confidencial de la empresa o datos personales.
- No recopilar información de áreas a las que normalmente no se tiene motivos para acceder, a menos que se tengan suficientes indicios de que en esas áreas existe un incidente real.
- Asegurarse de poseer un documento que acredite el respaldo de la empresa a realizar los procedimientos establecidos para la investigación del incidente.

EL CONTRATO NDA

Para evitar la difusión de secretos es habitual asociar un acuerdo de confidencialidad o **NDA**. Este contrato:

- Garantiza que ningún contenido analizado será divulgado a personas no autorizadas.
- Puede ser de carácter unilateral o bilateral.
- Establece sanciones en caso de incumplimiento.

AUTORIZACIONES ADICIONALES

También puede ser necesario obtener autorizaciones de:

- **De la empresa:** si el trabajo del investigador afecta a la disponibilidad de algunos servicios.
- **Del juez:** si se tiene una orden de registro para dispositivos móviles, pero no para la información en la nube.

En el caso de que las evidencias vayan a almacenarse para su posterior análisis, ya sea para conocer las causas que han originado el incidente o para que formen parte de un proceso judicial, es necesario conservarlas de manera segura, y para ello se deberá:

- Catalogar y rotular todos los elementos.
- Transportar con cuidado para que no les afecten características del entorno como la temperatura, la humedad o los campos electromagnéticos.
- Realizar, si es posible, al menos dos copias del original.

• Guardar en lugares asegurados contra accesos y manipulaciones no autorizadas (por ejemplo, cajas de seguridad) y contra otro tipo de accidentes (por ejemplo, armarios ignífugos). Además, es recomendable que se puedan detectar si se han producido accesos no autorizados.

• Documentar todos los accesos a la evidencia.

Si el fin de la investigación es presentar las evidencias a un tribunal, además será esencial mantener la cadena de custodia para no anular la validez de las pruebas.

- Almacenamiento seguro protege la información (integridad y confidencialidad).
  Cadena de custodia documenta cada transferencia del material (trazabilidad y autenticidad) para fines legales.

Volviendo a la guía RFC 3227, esta proporciona recomendaciones claras sobre el mantenimiento de la cadena de custodia de evidencias, indicando la importancia de documentar y describir detalladamente cada paso del proceso de manejo de evidencias, desde el descubrimiento hasta el examen:

- Dónde, cuándo y por quién fue descubierta y recopilada la evidencia, así como dónde, cuándo y por quién fue manipulada o examinada.

- Si la evidencia cambió de «manos» se deben incluir los detalles de cómo las pruebas cambiaron de custodia; quién ha tenido la custodia de las pruebas y durante qué período. Si se ha remitido por correo a otro lugar, incluir datos como el número de envío.
- En todo momento, tanto al recopilar, como al almacenar o transferir la prueba, es necesario indicar cómo se almacenó y cuándo.

Además, la guía recomienda generar códigos hash, así como firmar criptográficamente la evidencia recopilada. De esta manera es posible asegurar que la cadena de custodia ha sido sólida y demostrar que la evidencia no se ha alterado desde su recolección.

El proceso de copiado de un disco o de ficheros a otro dispositivo es crítico, por lo que se deben garantizar las siguientes condiciones:

- Si es posible, almacenar las evidencias en medios comunes.
- Las unidades donde se van a almacenar las copias deben haber sido formateadas de manera segura. Algunos estóndares recomiendan repetir un borrado seguro entre 3 y 35 veces.
- Las copias que se realicen de una evidencia deben ser idénticas a la original y entre ellas.

- Las copias que se realicen de una evidencia deben ser idénticas a la original y entre ellas.
- Trabajar sobre copias realizadas bit a bit.
- No alterar el origen de datos ni el destino paro evitar invalidar las evidencias obtenidas.
- El copiado debe ser completo, incluyendo el espacio libre y, en el caso de que los hubiere, los sectores defectuosos, ya que de ambos se puede obtener información a través de herramientas forenses especializadas.
- Aplicar funciones hash sobre la información recopilada para asegurar la integridad de las copias. Se suele utilizar el algoritmo MD5, y para evitar colisiones utilizar ademós el SHA- l.

Cuando se almacenen las evidencias es importante etiquetar, inventariar e incluso fotografiar de manera que se identifique:

- Marca, modelo, número de serie, tipo de conexión (USB, HDMI, etcétera).
- Persona responsable de la evidencia.
- Personal que trabaja con la evidencia (quiénes la han recopilado, almacenado, etiquetado, etcétera).
- Fechas relevantes.

Las herramientas de recopilación de evidencias son soluciones de software y hardware diseñadas para recuperar, almacenar y analizar datos electrónicos de diversas fuentes como unidades de disco, ficheros, registro, bases de datos, memoria RAM, correos electrónicos, imágenes, etcétera.

Una característica esencial de las herramientas de recolección de evidencias es que deben afectar al escenario lo mínimo posible. Por ejemplo, que no requieran mucha memoria que altere el estado del dispositivo que están analizando. Es por eso por lo que no se recomiendan aquellas que tengan interfaz gráfica.

Herramientas y comandos incluidos en los sistemas operativos habituales.

Cuando la investigación de los incidentes es realizada por los equipos de seguridad de la organización, y no por especialistas forenses, con el objetivo de dar respuesta al incidente, los comandos de los sistemas operativos de los propios sistemas son de gran utilidad:

dd: clonación y copias a bajo nivel. dc3dd es la versión forense.

showrev: información del sistema (ID host, versión, núcleo).

netstat: estado de red, protocolos y enrutamiento.

gpg: cifrado y descifrado de datos.

ps: listar y examinar procesos en ejecución.

ifconfig: información básica sobre interfaces de red.

shasum / md5sum: generación y verificación de hashes.

gcore y gdb: información sobre procesos en ejecución.

También es común emplear scripts para automatizar la recolección de datos, utilizando estas herramientas en el orden establecido según los objetivos de la investigación.

Herramientas para imágenes forenses.

Una de las acciones más habituales en una investigación forense es la recuperación de datos de discos duros, pendrives, tarjetas SD y otras unidades de almacenamiento, por lo que son imprescindibles herramientas que faciliten esta labor. Algunos ejemplos son EnCase Imager y FTK Imager.

Herramientas para el volcado de memoria.

Otro tipo de herramientas imprescindibles en el ámbito de la recolección de evidencias son las de volcado de memoria utilizadas para la adquisición de evidencias volátiles, es decir, datos que solo están presentes mientras el sistema está encendido y durante un tiempo limitado. Existen varias herramientas diseñadas para recopilar este tipo de datos, como Winpmem y AVML.

Además de las herramientas software, los investigadores forenses suelen preparar un kit completo para trabajar que contenga, entre otros elementos:

- Discos duros, pendrives, CD y DVD vírgenes.
- Pendrives de arranque de distintos sistemas operativos.
- Dispositivos USB y CD con distintas herramientas forenses preparadas para los distintos sistemas operativos que vayan a analizar. Se recomienda que estas herramientas estén en medios configurados para solo lectura, evitando así posibles infecciones o acciones antiforenses.
- Destornilladores para abrir dispositivos y acceder a su interior.
- Bolsitas específicas para guardar evidencias.
- Incluso jaulas de Faraday que anulen los campos electromagnéticos.