**Evaluación Contínua 4 - Análisis Forense**

Alumno: Gonzalo Benito

Email: [gu4n4rt@gmail.com](mailto:gu4n4rt@gmail.com)

…..............................................................................................................................................................

**1. Explica en qué consiste la RFC 3227 y cuáles son sus fases, detallando cada una de ella. (1 punto)**

La RFC 3227 consiste en un documento con todas las guías y recomendaciones para la recopilación y posterior almacenamiento de información tras un incidente. El mismo detalla todo lo que se debe tener en cuenta, funcionando casi como un estándar para el análisis forense. Se puede dividir en la fase de recolección y la fase de almacenamiento:

Fase de recolección: recogemos toda la información posible, realizando copias sin modificar los datos. Se aconseja utilizar software o hardware especializado, siempre conociendo cómo funciona. Además de todo esto, es fundamental seguir el orden de recolección recomendado, siguiendo la regla de la volatilidad de la información, donde la información más volátil tendrá prioridad sobre la menos volátil.

Fase de almacenamiento: se siguen rigurosas medidas de seguridad para el almacenamiento, creando múltiples copias, tomando capturas del momento de la toma de la información para verificar la integridad y veracidad de los datos, mediante imágenes, hashes, etc. Además, debe almacenarse todo en un lugar seguro, y la custodia de los datos debe quedar en una persona, que se encargará de seguir estrictas reglas de rotulados y firmas para el acceso y manipulación de la información.

Durante todo el proceso debemos procurar mantener intacta la información, puesto que su modificación la invalidaría ante un juicio; e ir documentando todo, en todo momento.

**2. Ordena por volatilidad, de menos a más, las siguientes evidencias: (1 punto)**

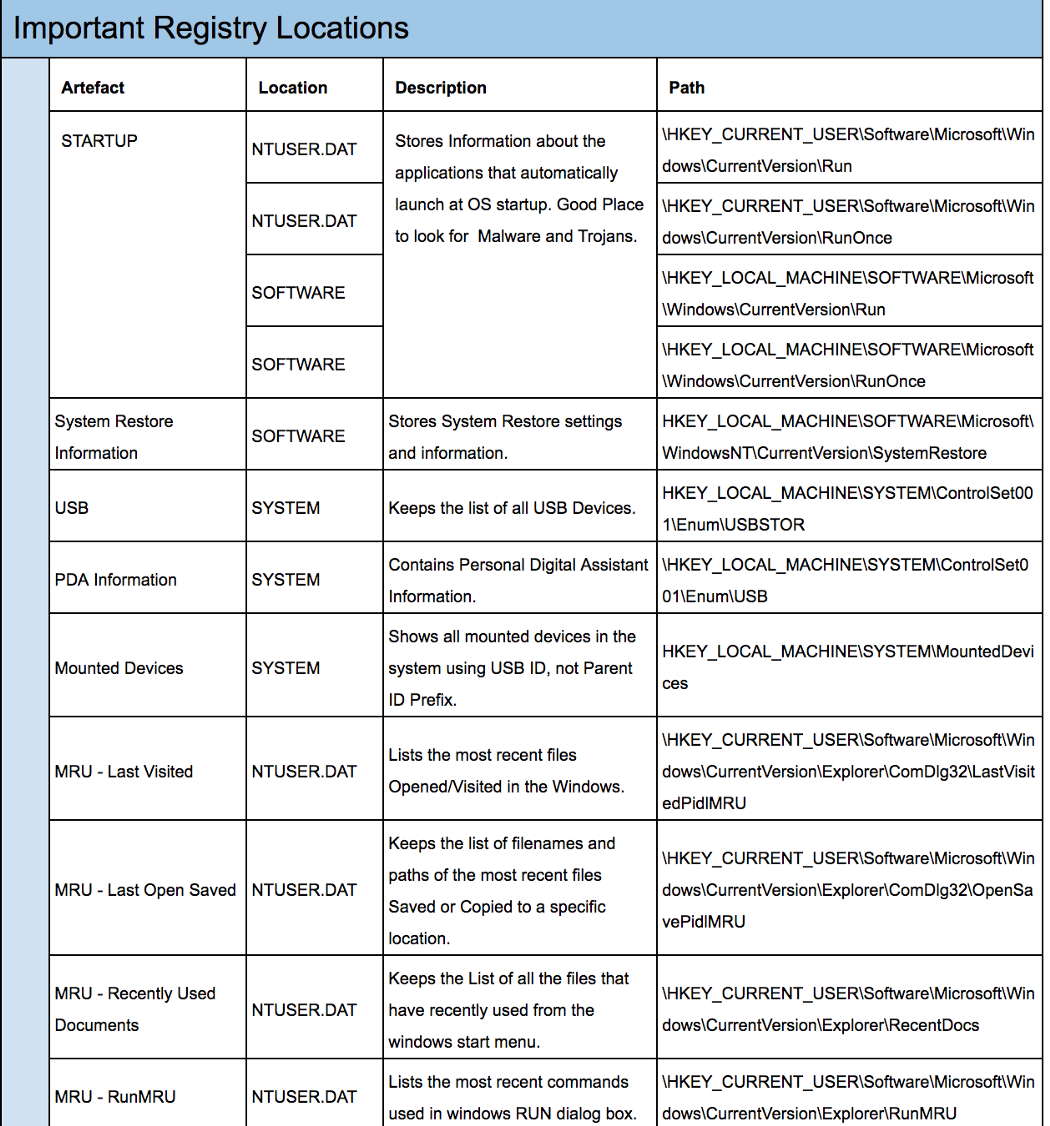
1. Valor del registro EIP
2. Información que se obtiene con el comando “arp -a”
3. Espacio de memoria de iexplorer.exe
4. Eventos de Windows
5. Ficheros almacenados en “Mis Documentos”

**3. Define, con tus propias palabras, y el máximo nivel de detalle, el concepto de Cadena de Custodia. (1 punto)**

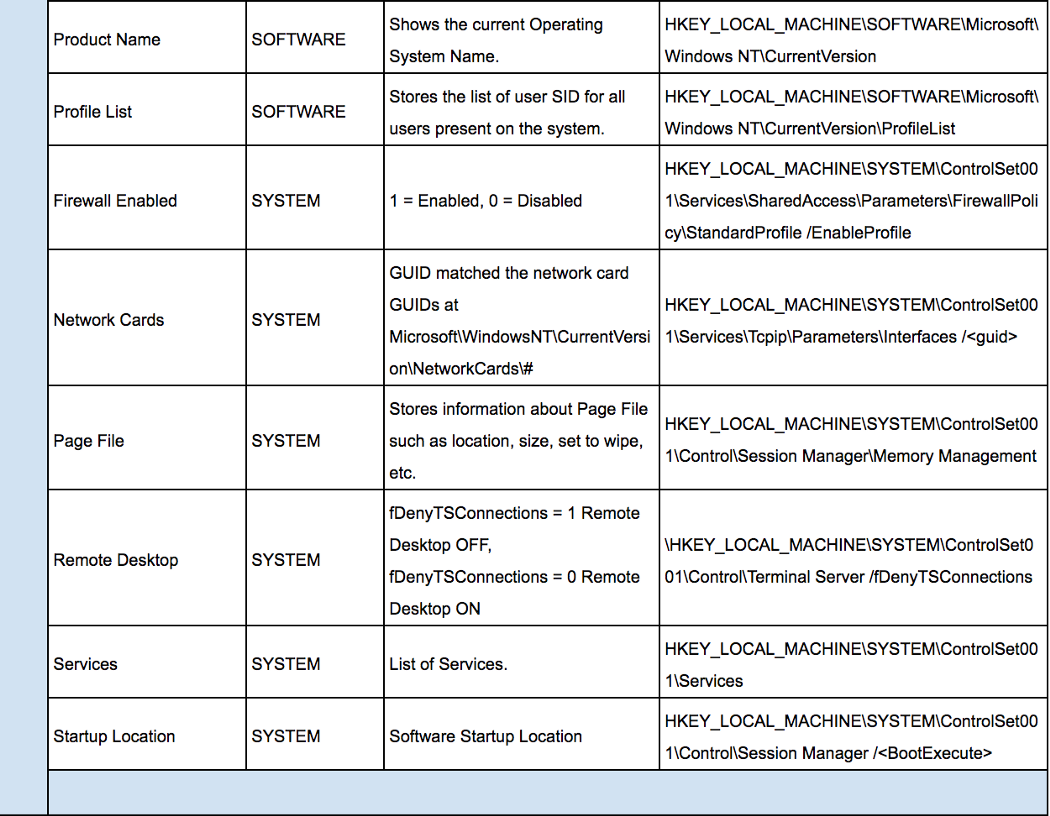
La cadena de custodia es el período durante el cual el perito forense mantiene contacto directo con la información, comenzando desde su primer contacto al entrar a la escena del crimen, y finalizando terminado un juicio, en caso de que lo haya. Durante todo este tiempo, el o los analistas deberán documentar todo lo que suceda sobre las evidencias, conservando la veracidad de las mismas.

**4. ¿Qué artefactos forenses componen el registro de Windows 7 y cuál es su localización? (1 punto)**

(No puedo responder esta consigna, pero adjunto información que encontré y que la responde)







*Fuente: https://medium.com/@lucideus/windows-registry-forensics-part-ii-2018-crucial-artefacts-lucideus-39c20a80ca16*

**5. Juan trabaja para una pequeña empresa, y últimamente se ha percatado que uno de los equipos de la oficina, que tiene instalado un Windows XP de 32 bits, con Service Pack 2, está funcionando de una forma un poco sospechosa. En ese momento decide llamarte para que le asesores, y te explica una serie de peculiaridades del equipo:**

* − Están utilizando ese equipo como servidor de producción
* − Se dispone de acceso físico al equipo
* − Dispone de puertos USB
* − Sólo se quiere saber el origen del posible problema, y en ningún momento de plantean llegar a juicio.

**Dada estas premisas, indica cual sería tu procedimiento de actuación, para determinar el origen de dicho comportamiento sospechoso. (1 puntos)**

Mi procedimiento de actuación consistiría en los siguientes pasos:

1. En primer lugar, pedir que me concedan el permiso, para comenzar el análisis. Como no se plantean llegar a juicio, el manejo de las evidencias o rastros será distinto (menos estricto).
   1. Teniendo en cuenta que el sistema operativo es antiguo, la cantidad de vulnerabilidades conocidas son enormes.
2. Intentaría hablar con Juan, para que me brinde toda la información posible, y determinar si lo que ocurrió fue un ataque, o simplemente otro problema.
3. Me haría y buscaría responder las preguntas básicas: ¿Qué? ¿Dónde? ¿Cuándo? ¿Por qué? ¿Quién? ¿Cómo?, haciendo menor énfasis en el quién.
4. Siguiendo las recomendaciones RFC, y según la información proporcionada (como que la máquina es el servidor de producción), recopilaría la información más volátil, como las conexiones IP entrantes y salientes (puertos y conexiones de red) de dicho servidor. Lo mismo con la caché ARP. Esto con la intención de ver si un atacante consiguió acceso al servidor remotamente explotando alguna vulnerabilidad, o por falta de controles y autenticación, por ejemplo.
   1. También identificaría y analizaría tráfico sospechoso en vivo, realizando una captura del tráfico de red.
   2. Analizaría los procesos y servicios en ejecución, en búsqueda de anomalías.
   3. Buscaría posibles vectores de ataque (los más críticos en primer lugar) que podría aprovechar un atacante. De esta forma, podría imaginar mejor los posibles escenarios.
   4. Buscaré logs de acceso a los servicios corriendo en el equipo (ej, servidor web, base de datos, etc)
5. Al disponerse de acceso físico, un atacante podría realizar una explotación local, o instalar cualquier tipo de malware, en caso que no se establezca un mínimo de seguridad. Esto sumado a que dispone puertos USB, facilita tanto la infección de malware como la escalada de privilegios, entre otras tantas cosas.
   1. Dado esto, revisaría los logs y artefactos de Windows en lugares clave, como lo es, en este caso, los registros sobre el uso de los puertos USB, por ejemplo.
6. Si luego de esto no encuentro evidencia de ningún tipo, se lo haría saber a Juan, presentando todos los análisis que he realizado y la información recolectada.