HABILIDADES DE ANÁLISIS FORENSE INFORMÁTICO

Esquema para complementar la presentación de diapositivas. El presente esquema no sigue exactamente el orden de las diapositivas.

1. Orden del día

   - ¿Qué es el análisis forense informático?
   - Dónde encontrar evidencia informática.
   - Obtención de imágenes forenses.
   - Análisis forense informático.

2. ¿Qué es el "análisis forense informático"?

   - Es la conservación, identificación, extracción, análisis e interpretación de información digital con la expectativa de que los hallazgos se utilicen en la corte.

3. Habilidades

   - Revela evidencia directa en la máquina.
   - Asocia a una máquina con la información.
   - Proporciona pistas para la investigación.
   - Muestra evidencia que corrobora o refuta alegatos o coartadas.
   - Deja al descubierto evidencia conductual.

4. Relación entre el agente del caso y el analista forense.

   - El agente del caso y el analista forense deben trabajar en equipo
   - El agente del caso
     - Involucra al analista forense desde un inicio.
     - Explica el aso-
     - Proporciona solicitudes específicas.
   - El analista forense
     - Educa y aconseja al investigador.
     - Explica los resultados y sus limitaciones.

5. Dónde encontrar evidencia informática.

   - Confiscar artículos que se detallan en la orden de cateo.
     - Computadoras, laptops, equipo de red (conectores e interruptores).
     - Periféricos: CDR, DVD-R, cámara digitales, PDA.
     - Medios externos: CD, diskettes, memorias USB.
     - Notas en papel, documentos y manuales, notas autoadheribles.
   - Antes de moverlo, documente el equipo y los periféricos.
     - Fotografías digitales, diagramas.

6. ¿Qué es la obtención de imágenes forenses?

- Se obtiene mediante un método que, bajo ninguna circunstancia, altere la información en la unidad de almacenamiento que se está duplicando.
- El duplicado debe contener una copia de cada bit, byte y sector de la unidad de almacenamiento original.
- El duplicado no contendrá ninguna información distinta a la que se copió de la fuente original, exceptuando los caracteres de llenado (para áreas dañadas).
- Fiel, verificable, reproducible.

7. La importancia de las imágenes forenses

- Las imágenes forenses y aquellas que se obtienen en el momento en que se responde al incidente son el paso más importante de toda la investigación electrónica.
- Si falla, ésta puede invalidar o hacer inadmisible toda la información que se obtenga de evidencia digital.

8. El proceso de la imagen

9. Bloqueos físicos contra escritura.

- Dispositivo físico que evita que se escriba sobre la unidad de almacenamiento de evidencia.
- Es el mejor método para obtener imágenes.

10. Conectar un bloqueo contra escritura.

11. Hardware para obtener imágenes

12. Software para obtener imágenes

- CD o diskettes de reinicio.
- Controla la computadora de tal manera que sólo envíe comandos para leer la unidad y nunca para escribir en ella.
- Ejemplos:
- FTK Imager
- EnCase
- DD
- Ghost
- Otros

13. Físico vs. lógico

- La estructura física de los datos se refiere a la organización de los mismos en una unidad de almacenamiento. La obtención física de imágenes consigue tantos ceros y unos como sea posible del dispositivo.
- La estructura lógica de los datos se refiere a cómo aparece la información en cierto programa o para un usuario, tal como se ve a través del sistema operativo. La obtención lógica de imágenes pasa por alto la información que se encuentra en áreas que no ve el sistema operativo.

14. ¿Qué puede encontrar el analista?

- Archivos borrados.
- Fragmentos de texto.
- Meta archivos mejorados (archivos que se imprimieron).
- Meta datos mejorados (información insertada).
- Información en el registro de hora y fecha
- Mensajes de correo electrónico e historiales de conversación.
- Información sobre el uso del Internet (historial).
- Ficheros archivados y archivos comprimidos (zip).
- Archivos codificados adjuntos a mensajes de correo electrónico.
- Imágenes (activas y borradas)
- Y más…

15. Cómo puede solicitar un análisis forense.

- Ejemplo: El secuestro de Heather Miller.
    - Evidencia que involucraba a la acusada con sustracción de menores.
    - Búsqueda del nombre de la víctima.
    - Fotografías de la víctima.
    - Evidencia de una carta de amenaza que se le envió a la víctima.
    - Evidencia de referencias a drogas para violación.
    - Evidencia de un conspirador.
    - Actividad en la computadora al momento del delito.
    - Relacionado con el usuario.

16. Cómo empezar

- Búsquedas de palabras clave
- Inconvenientes de las búsquedas de palabras clave.
    - Documentos Adobe PDF.
    - Faxes.
    - Excel
    - Registro.
    - Archivos compuestos / comprimidos.
    - Varios otros.

17. Revisión de las gráficas.

17. Revisión del correo electrónico.

18. Encabezados del correo electrónico

19. Tipos de metadatos del correo electrónico

- Cuándo se creó
- Cómo se creó
- Cuándo se envió
- Cuándo se recibió
- Quién lo envió / recibió
- Ruta
- Correo electrónico de respuesta

20. Análisis temporal

21. Análisis gráfico

22. Historial de las aplicaciones

23. Caché de Internet

24. Historiales de conversación

25. Meta datos

26. Usando buscadores en línea

27. Historial web

- Identificar la sesión de navegación web
- ¿Cuándo / dónde se abrió el navegador?
- ¿Cómo llegaron al hallazgo relevante?
- Correo web
- ¿Otras actividades?
- Todo tiene que ver con relacionar al usuario.

28. Resumen

- La evidencia electrónica está en todas partes.
- Los agentes del caso deben trabajar en conjunto con los analistas.
- Los analistas forenses deben de ver más allá del “archivo”.
- Los metadatos pueden ser cruciales para establecer una relación con el usuario.

- Incluso si se ha destruido o borrado la propia evidencia se pueden encontrar varios artefactos.

Fin