ITU parte 3 - Angie Daniela Ruiz Alfonso.

Por qué es importante el Case Statement para el análisis forense?

Este documento permite que, al inicio de una investigación deduzcamos a través de ciertas preguntas si los elementos en la escena del crimen pueden constituir evidencia, debido a que este consta de: establecer los tiempos para buscar y analizar evidencia, así como el tiempo para reportar los hallazgos y determinar claramente lo que se busca reportar y el contexto, el cual ayuda a establecer posibles lugares iniciales donde buscar evidencia. Con estos dos puntos anteriores se determinan los elementos a investigar (hardware o software), logrando así que la investigación apunte a priorizar ciertos elementos, permitiendo así distinguir la especialización requerida para el investigador forense.

Fuente: Modulo 5 ITU.

Diseñe el contenido de un Registro de evidencia digital que incluya la cadena de custodia.

Basándome en FGN: https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf

Registro de Evidencia Digital

1. Código único del caso	Departamento + Municipio + Entidad + Unidad + Año + Consecutivo
2. Fecha y hora de recolección	DD/MM/AAAA y hora en formato militar
3. Descripción del elemento digital	
4. Tipo de dispositivo y cantidad	Celular, ordenador, tablet, cámara digital, otro
5. Marca del dispositivo	
6. Sistema operativo del dispositivo	
7. Tipo de memoria del dispositivo	
8. Modelo del dispositivo	
9. Capacidad del dispositivo	
10. Lugar de hallazgo del dispositivo	
11. Nombre completo de a quién se le encontró el elemento digital	
12. Cédula de a quién se le encontró el elemento digital	
13. Delito a investigar	
14. Nombre completo de quién halló el elemento digital	
15. Cédula de quién halló el elemento digital	
16. Entidad de quién halló el elemento digital	
17. Cargo de quién halló el elemento digital	
18. Firma de quién halló el elemento digital	
19. Nombre completo del recolector del elemento digital	
20. Cédula del recolector del elemento digital	
21. Entidad del recolector del elemento digital	
22. Cargo del recolector del elemento digital	
23. Firma del recolector del elemento digital	

24. Nombre completo de quién embaló el elemento digital	
25. Cédula de quién embaló el elemento digital	
26. Entidad de quién embaló el elemento digital	
27. Cargo de quién embaló el elemento digital	
28. Tipo de embalaje y cantidad	Bolsa plástica o de papel, frasco, caja, otro
29. Firma de quién embaló el elemento digital	
30. Ubicación del almacenamiento en la bodega	
31. Observaciones	

Durante la intervención policial se encontró a una persona operando una computadora conectada a internet a través de una red LAN cableado usando una conexión FTTH. De la evaluación inicial, el presunto delincuente se encontraría subiendo material ilegal a un sitio de internet de una red de explotación infantil internacional previamente identificada por la Interpol.

a) Describa las acciones que realizaría en la escena del crimen para la requisitoria de la evidencia

1. Como en este caso las fuerzas del orden son las llamadas a confiscar los elementos, deben contar con la orden del juez que indique los alcances de los elementos que pueden ser obtenidos producto del allanamiento y teniendo en cuenta lo anterior se procede a determinar un perímetro en la escena del crimen, donde solo el personal calificado pueda acceder a esta zona de interés y a sus equipos, y dentro del perímetro anterior deben identificar las fuentes de energía y switch principal para evitar cualquier corte o manipulación que puedan afectar a los equipos digitales, si es un escenario donde se cuenta con el apoyo de personal de Tecnologías de Información y personal de infraestructura se podrá entender mejor la interconexión de las fuentes de energía, si existen fuentes de backup, y si algunos equipos no pueden ser desconectar (por ejemplo, servidores en producción). Sin olvidar de tomar notas sobre lo encontrado al llegar a la escena.

2. Posteriormente deben cortar toda comunicación y energía hacia los equipos de interés desde el extremo más cercano (desconectar de la energía más no apagar), una vez toda información haya sido capturada para evitar pérdidas de información.

3. Luego revisan los equipos para detectar cualquier problema en ellos o cualquier distintivo que los identifique, se toman fotografías, y en caso de no contar con cámara se debe realizar un dibujo a mano alzada. Para con ello posteriormente hacer un mapa del perímetro con la ubicación de los distintos elementos dentro de él. Sin olvidar que al momento de confiscar los equipos a investigar debemos tomar notas sobre los tiempos, las personas en la escena, descripciones de la evidencia y como fue obtenida, sistemas operativos y procesos de red corriendo.

4. Cuando todos los elementos han sido etiquetados y documentación de las evidencias (junto con la cadena de custodia) se encuentran listos para su transporte, se llevan de la forma más segura a un lugar donde puedan ser almacenados y cuidados también de forma segura, teniendo en cuenta que, si los dispositivos estuvieran encendidos, se deben dejar enfriar antes de ser colocados en empaques debidamente sellados e identificados.

5. Cuando lleguen a su destino final, le harán copia digital de la memoria a los equipos y una vez hecha la imagen digital de estos, serán enviados a un lugar de almacenamiento donde permanecerán nuevamente sellados y fuera del contacto de personas ajenas al responsable de su cuidado.

b) Indique qué documentación debería producir en la escena del crimen para un mejor sustento del caso

La documentación a realizar al llegar a la escena del crimen es: Descripción de la escena, tipos de media encontrados y cables de red o WiFi, fotografía del etiquetado de los cables y puertos que estaban conectados, detalles de las personas que ocupan regularmente el espacio donde los equipos fueron encontrados, comentarios y notas de los usuarios de los equipos requisados (contraseñas, datos importantes sobre su uso, entre otros), acciones realizadas en la escena del crimen, incluyendo horas, acciones realizadas sobre la evidencia, detalles sobre cualquier otra evidencia no digital dentro de la escena del crimen (ejemplos: post-it con contraseñas, cuaderno de notas, entre otros) y formatos de Cadena de Custodia para cada elemento a requisar.

Fuente: Modulo 5 ITU.

Investigue acerca de los Software Autopsy EnCase como herramientas para el análisis de evidencias. Presente un comparativo de sus características, estableciendo sus ventajas y desventajas.

Herramienta	Ventajas	Desventajas
Autopsy	Compatible con Linux, su uso es gratuito, su descarga e instalación es muy sencilla, además viene incluida en Caine. Nos permite analizar una imagen forense, análisis de evidencia digital que se realiza con el fin de obtener información que pueda ser útil en una investigación, además de permitir la generación de reportes en diferentes formatos que son de gran utilidad a la hora de hallar evidencias y realizar su respectivo análisis. Es muy eficiente debido a sus diferentes tipos de análisis y su diseño estructural, el cual cuenta con distintos modos de configuración, funcionalidades que se pueden programar al momento de la creación del caso. Su interfaz gráfica es tipo browser lo cual la hace muy fácil de utilizar. Nos permite recuperar archivos borrados por medio de una imagen forense y la búsqueda de emails si lo requerimos. Soporta el análisis de diferentes sistemas de archivos tales como (NTFS, FAT, UFS1/2, Ext2/3). Nos permite buscar archivos profundamente en todo el sistema de archivos.	La mayoría de los manuales de uso están en inglés. No permite la creación de índices, a pesar del análisis profundo. No permite analizar actividad reciente en el equipo, únicamente análisis sobre la unidad o imagen a examinar.

Encase	Es reconocido como el estándar de la industria de software en informática forense y tiene mucha aceptación para forense móvil. Dispone de un abanico de aplicaciones internas muy potentes que lo diferencian de las herramientas libres y lo hace ideal para hallar elementos que permitan probar un delito informático Es utilizada por las fuerzas del orden y las organizaciones militares en todo el mundo, así como las empresas de seguridad corporativas y agencias de inteligencia. Puede realizar análisis forense en prácticamente cualquier sistema operativo y también tiene buenos informes integrados. Puede recuperar todos los archivos y meta-datos en un equipo, a pesar de los intentos de ocultación o borrado de datos y aunque el disco duro haya sido formateado. Verifica la firma para cada archivo contra una lista de firmas conocida de extensiones de archivos, en caso de que exista alguna discrepancia, como en el caso de que hayan escondido un archivo o simplemente lo hayan renombrado, el software detectará automáticamente la identidad del archivo, e incluirá en sus resultados un nuevo ítem con la bandera de firma descubierta, permitiendo al investigador darse cuenta de este detalle. Ofrece una vista completamente integrada que localiza automáticamente, extrae y despliega muchos archivos de imágenes como .gif y .jpg del disco. Permite montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos. Tiene una versión gratuita que se puede aplicar para la adquisición de información, la cual es muy simple de usar. Tiene soporte incorporado para casi todos los tipos de encriptación, incluidas buenas capacidades de búsqueda de palabras clave y funciones de scripting accesibles.	Es un software demasiado costoso. El procesamiento puede llevar mucho tiempo en caso de tener archivos muy grandes. Las versiones más recientes a veces no se ajustan a otras herramientas forenses.

Fuentes: http://notasinformaticaforense.blogspot.com/2014/11/herramientas-para-el-analisis-forense.html, http://eportafolioadrianamunoz.blogspot.com/2014/11/practica-1.html,

https://www.seabrookewindows.com/s/beneficios-encase-forensic/, http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442009000200025&script=sci_arttext, http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0187_IglesiasLF.pdf y https://ciberseguridad.com/servicios/analisis-forense/

Investigue y recomiende el índice del contenido de un reporte final de una investigación forense digital posteriormente un perfil profesional completo.

Recomiendo los siguientes lineamientos para un reporte final de una investigación forense digital teniendo en cuenta siempre al público que va dirigido el reporte:

- Agencia encargada de la investigación
- Número de caso/investigación
- Fecha y hora del inicio y fin de la investigación
- Nombre del examinador que realiza el reporte.
- Campo de especialización del examinador.
- Nombre de defendido/litigante.
- Resumen ejecutivo
- Antecedentes del caso
- Objetivos
- Preguntas relevantes del caso
- Búsqueda y captura de evidencia
- Acciones realizadas en la investigación, indicando el cómo y por qué fueron utilizadas las diferentes herramientas y procedimientos para recolectar y analizar la información.
- Declaración del examinador que indique la imparcialidad sobre la materia a investigar, limitándose a brindar solamente su conocimiento y profesionalismo.
- Declaración de que el reporte en toda su extensión refleja solamente la verdad de lo hallado por el examinador.
- Declaración de que no existen conflictos de intereses por parte del examinador.
- Delitos
- Brecha corporativa
- Limitaciones
- Análisis de los resultados obtenidos
- Conclusiones
- Material generado durante la investigación
- Firma

Fuente: Modulo 6 ITU, https://es.scribd.com/document/320907678/Ejemplo-Informe-de-Un-Analisis-Digital-Forense, https://buscandojusticia.es/wp-content/uploads/2019/03/DOC.CUATRO.1_2_Censurado-1.pdf y https://mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf.