Computación Forense

Fases de una Investigación Forense

S1V3

Profesor: Ing. Alex Araya Rojas, MT

CISSP, CISM

Fases de un Proceso Forense

Pre Investigación

- Aquí debemos preparar todo lo necesario para la práctica forense, por ejemplo:
  - ✓Laboratorio Forense
  - ✓Temas Legales
  - ✓Capacitación
  - ✓Definición de Alcance de la oficina

Investigación

- Fase Principal del proceso, vemos temas como:
  - ✓Acuerdos legales
  - ✓Definición clara del caso
  - ✓Selección de herramientas
  - ✓Aplicación metodología en la escena y para adquisición y análisis de evidencia

Post Investigación

- Aseguramiento de cumplimiento entre reporte y entregables con el alcance del caso o requerimientos de la investigación.

Fase Pre Investigación

Preparación

- Un elemento clave de esta fase es analizar la legislación vigente donde se va a realizar el proceso forense, de forma tal que no violemos leyes en nuestra actuación.

- La definición del tipo de casos que nuestro equipo forense va a atender es vital, esto para adquirir los equipos específicos como para preparar a nuestro personal.

- La adquisición y preparación del material que se utilizará tanto para la adquisición de evidencias como para el proceso de análisis deben contemplarse en esta fase, por ejemplo bolsas forenses, equipos de cómputo, adaptadores, cables, etc.

Fase Pre Investigación

Personal

- El personal designado para la atención de un caso debe tener claras responsabilidades, por ejemplo fotógrafo, líder técnico, secretario, técnico forense, etc.

- Las capacitaciones deben estar acorde con los roles definidos y estos pueden estar rotando si se considera necesario para que todo el personal experimente de forma integral el proceso forense.

- Las capacitaciones son importantes y el personal debe tener contante acceso a ellas, así como la aplicación de auditorías de calidad en todas las fases y las lecciones aprendidas.

Fase Investigación

Permisos Legales y Metodología

- En esta fase se pone en práctica todo lo aprendido en la etapa de preparación, uno de los elementos más importantes es contar con los acuerdos legales y/o administrativos que avalen la pericia forense que estamos por realizar.

- Otro elemento crítico es apegarse a la metodología de trabajo en cuanto al proceso de atención de un incidente, desde la declaración del incidente, la documentación de la escena, la adquisición de la evidencia y su traslado al centro de análisis.

- Un elemento fundamental es mantener la cadena de custodia claramente documentada para evitar problemas de admisibilidad de la evidencia.

Fase Investigación

Metodología y más Metodología

- Acostumbre de acuerdo con su metodología previamente establecida en la fase de preparación, respetar los acuerdos de etiquetado de la evidencia, la documentación de las entrevistas a testigos, los procesos de búsqueda y de retiro de evidencia.

- Cuídese de los errores burdos como apagar o encender equipos, así como de garantizar un adecuado traslado de los mismos.

- Siga las guías para recopilación de evidencia según sistema operativo y estado de los equipos.

Fase Investigación

Recolección y Análisis

- Enumere los archivos presentes así como los borrados y/o perdidos de las unidades de almacenamiento de interés.
- Utilice estrategias de recolección según el contexto de la investigación, casos de red, casos de redes sociales, casos in site, etc.
- Dedique suficiente tiempo para el análisis con herramientas reconocidas y apéguese al alcance y requerimientos de la investigación.
- Documente claramente y apegándose al permiso obtenido para la investigación.

Fase Post Investigación

Control de Calidad

- El informe generado durante la investigación puede verse influido por el calor de la misma, en esta etapa debe validar si el reporte está alineado con lo esperado y aprobado en el permiso.

- Realice sesiones de lecciones aprendidas y entrene formalmente al personal a cargo del proceso para ir depurando desviaciones del proceso.

- Todos los equipos y prácticas del equipo forense deben estarse revisando periódicamente para su validación o actualización según corresponda.

Gracias