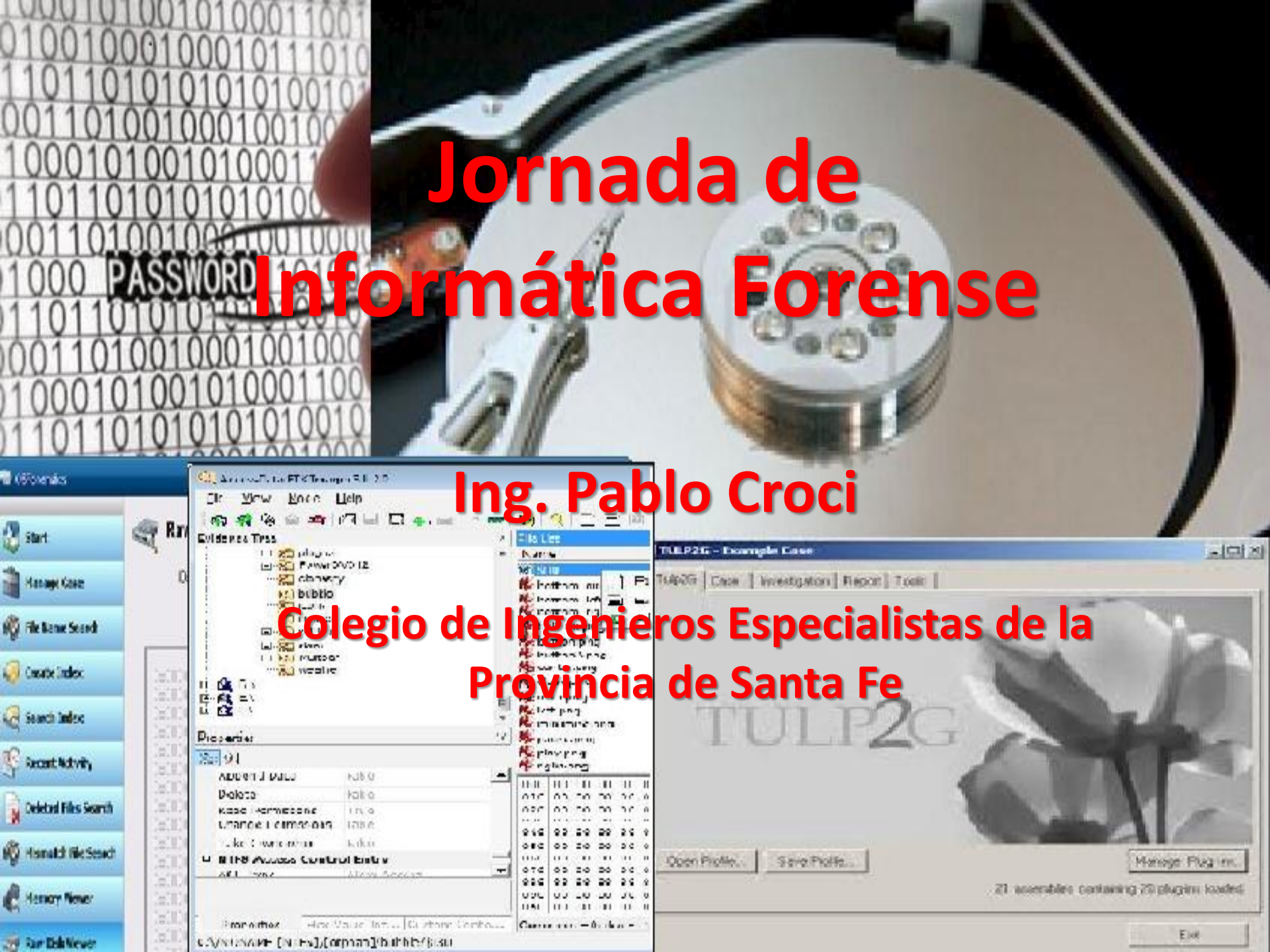


Jornada de Informática Forense

Ing. Pablo Croci

Colegio de Ingenieros Especialistas de la Provincia de Santa Fe

Presentación

- Pablo Croci. Ing. Electrónico (UBA). Especialista en Criptografía y Seguridad Teleinformática (EST Ejercito Argentino)
- 15 de experiencia en Informática Forense. Desempeño en tribunales penales federales. Perito de parte. Consultor Técnico Judicial. Investigación de Fraude
- Capacitación de Peritos Informáticos COPITEC (parte técnica). Parte de la Comisión de Peritos
- Laboratorio de Forensia Informática de la Especialización de Criptologia y Seguridad Teleinformática EST

Presentación

- Cursos y conocimientos de productos Guidance, Tableau, Nuix, UFED Cellebrite, Oxigen Detective Forensic
- Conocimientos en Tecnologías Open Source destinadas a Informática Forense, Analisis de Malware y Pruebas de Penetración

Módulos a ver en la Jornada

- **Introducción:** Conceptos básicos como proceder con la evidencia en Informática Forense. Breve mención de la ISO 27.037. Imagen Forense. Tipos de Imágenes Forenses. Concepto de Hash. El porqué del Hash para Resguardo de Evidencias. Métodos de bloqueos contra escritura de la evidencia. ¿Por qué Distribuciones Linux para Informática Forense?
- **Ejemplo:** Creación de Imagen Forense con Caine. Consideraciones a Tener en cuenta
- **Ejemplo:** Puntos de pericias mas comúnmente solicitados: mails, artefactos de internet (historiales, temporales de navegación), últimos archivos abiertos. Autopsy en Linux y Windows
- **Ejemplo:** Tratamiento de archivos borrados, concepto de análisis de borrados en papelera de reciclaje, borrado definitivo. Recuperación por Carving. (Windows)

Informática Forense

- Conjunto de métodos, procedimientos y normas internacionales de buenas costumbres, tendientes a efectuar investigaciones judiciales o privadas en medios tecnológicos, con el principio de conservación de la evidencia
- ¿Donde están esas normas de buena conducta o mejores prácticas?
  - RFC 3227 - Guidelines for Evidence Collection and Archiving (año 2002)
  - ISO/IEC 27037 Guidelines for identification, collection, acquisition, and preservation of digital evidence (año 2012)

Otros estándares ISO que trata el análisis de la evidencia recolectada

- **ISO/IEC 27041** offers guidance on the *assurance* aspects of digital forensics *e.g.* ensuring that the appropriate methods and tools are used properly.
- **ISO/IEC 27042** covers what happens *after* digital evidence has been collected *i.e.* its analysis and interpretation.
- **ISO/IEC 27050** (in 4 parts) concerns *electronic discovery* ... which is pretty much what the other standards cover.

Conceptos Básicos de la 27037

- **Relevancia de la Evidencia**: la evidencia digital debe estar unívocamente relacionada con los hechos a investigar
- **Confiabilidad y Repetitibilidad:** la evidencia: tiene que ser confiable, y debe aportar los mismos resultados por distintos investigadores, en las instancias que sean
- **Suficiencia**: los elementos adquiridos deben ser suficientes para el hecho a investigar

Conceptos Básicos de la 27037

- Metodología acorde a lo que se venia tratando hasta 2012, y desde épocas de la RFC 3227 :
  - Identificación
  - Recolección
  - Adquisición
  - Preservación

ISO 27037

- La norma no especifica si las cuatro etapas deben ser realizadas por el/los perito/s
- Tampoco especifica si todas las etapas deben realizarse en la escena del hecho.
- Todo dependerá de lo que ordene el “oficio judicial”
- Algunas etapas pueden ser en la escena, otras en el laboratorio

Etapa de Identificación y Recolección

- Obviamente identificar los elementos de la escena y nomenclarlos. Los mismos pueden estar descriptos o no en el oficio. Así mismo se debe documentar el estado de situación de cada elemento hallado.
- Se debe nomenclar utilizando descripciones simples, **ej PC-01**, y documentando las características constitutivas del elemento
- Se debe documentar en acta marca, modelo y números de serie de dispositivos de almacenamiento masivo (magnético. Electrónico y óptico)
- Si el paso posterior es traslado a Laboratorio, entonces se deberá almacenar convenientemente, revestir con bolsas antiestáticas y anti ruido EM sobre todo para el caso de equipos móviles (bolsa de faraday)

Etapas de Adquisición

- Se denomina así ya que hay que es la etapa en donde se adquiere la copia más fiel que se puede tener de las evidencias recolectadas e inidentificadas.
- A esa copia fiel, la denominaremos de ahora en más la llamaremos “Copia Forense o Imagen Forense”
- Una imagen forense, es una copia “bit a bit” de la evidencia a adquirir, sin importar, la estructura de datos y sistema de archivos a copiar

Tipos de Imágenes Forenses

- Imagen tipo DD, efectuada con el viejo comando de copia dd, es el denominado plano, y ocupa el mismo espacio que el original. Su extensión es archivo.dd
- Imagen tipo EWF, es el formato propietario de Encase, que ya es un estándar libre hoy. Se particiona en varios archivos. Comprime y puede ser encriptado. Archivo.E01, Archivo.E02, etc
- Imagen tipo AWF, similar al anterior. Siempre fue estándar abierto. Prácticamente en desuso

¿Qué condición debe tener la evidencia original en el momento de la adquisición?

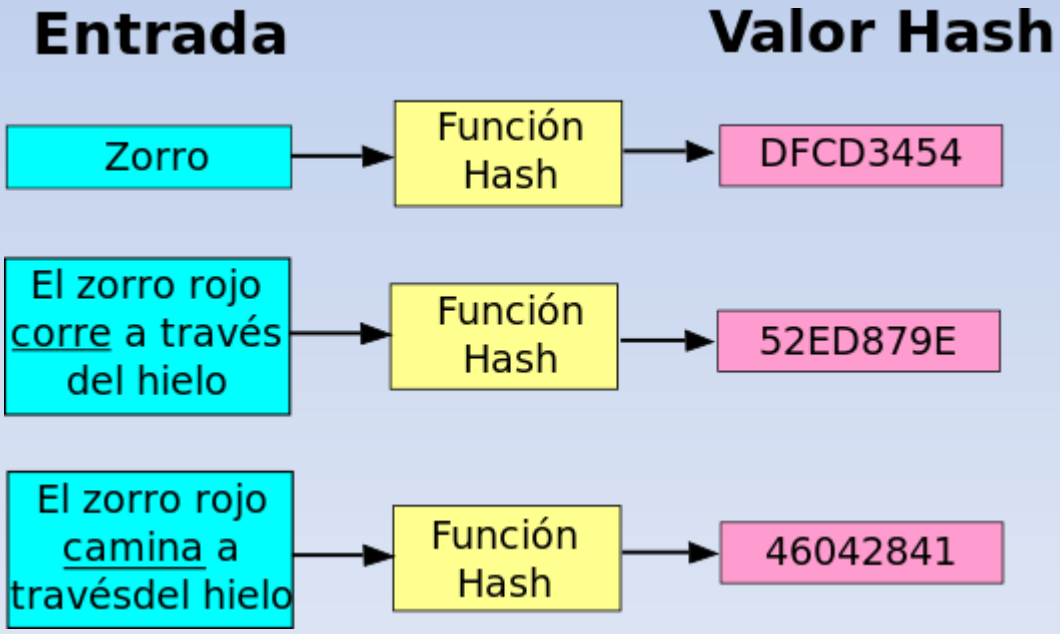
- La evidencia original debe mantenerse "**inalterable**". Entonces en el momento que vayamos a hacer la "imagen forense", la misma **no debe ser alterada por el Sistema Operativo** en dónde hagamos la tarea
- Por ende se debe bloquear contra escritura
  - **Bloqueo por Hard = Bloqueadores y Duplicadores Forenses**
  - **Bloqueo por Soft = Bloqueo de USB en Windows o Distro de Linux Forense**

Etapa de preservación

- Etapa mas que importante, ya que da aval técnico y jurídico a las anetriores
- ¿Qué se tiene que preservar?
  - Evidencias Originales (embalar, bolsas faraday, etc)
  - Evidencias de las imágenes realizadas
- ¿Qué es lo que preserva a las imágenes forenses?
  - **El calculo del Hash**

Concepto de Hash

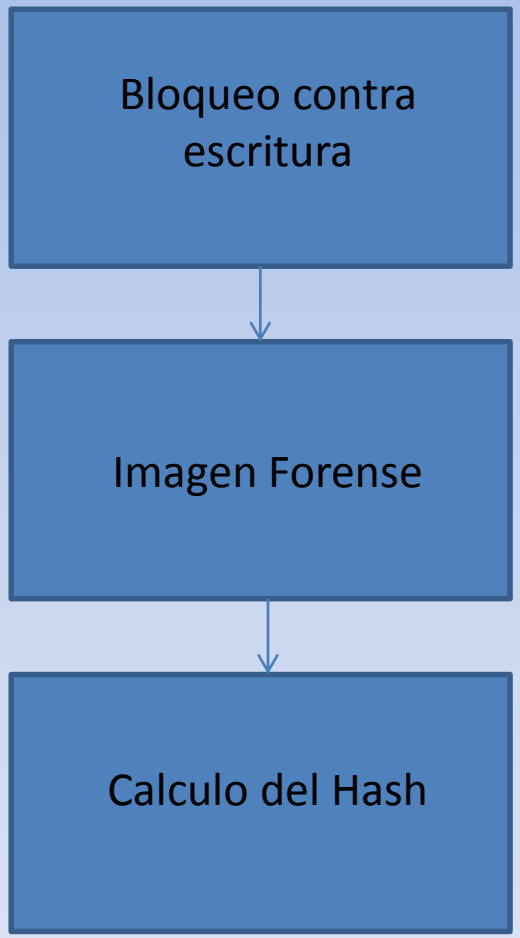
- Es una función matemática de criptografía. Dado un archivo digital, si aplicamos la función hash a dicho archivo, obtenemos como resultado un numero finito de bits, que es univoco a dicho archivo. Si el archivo no se modifica, el calculo del valor hash dará siempre el mismo resultado



Conclusión

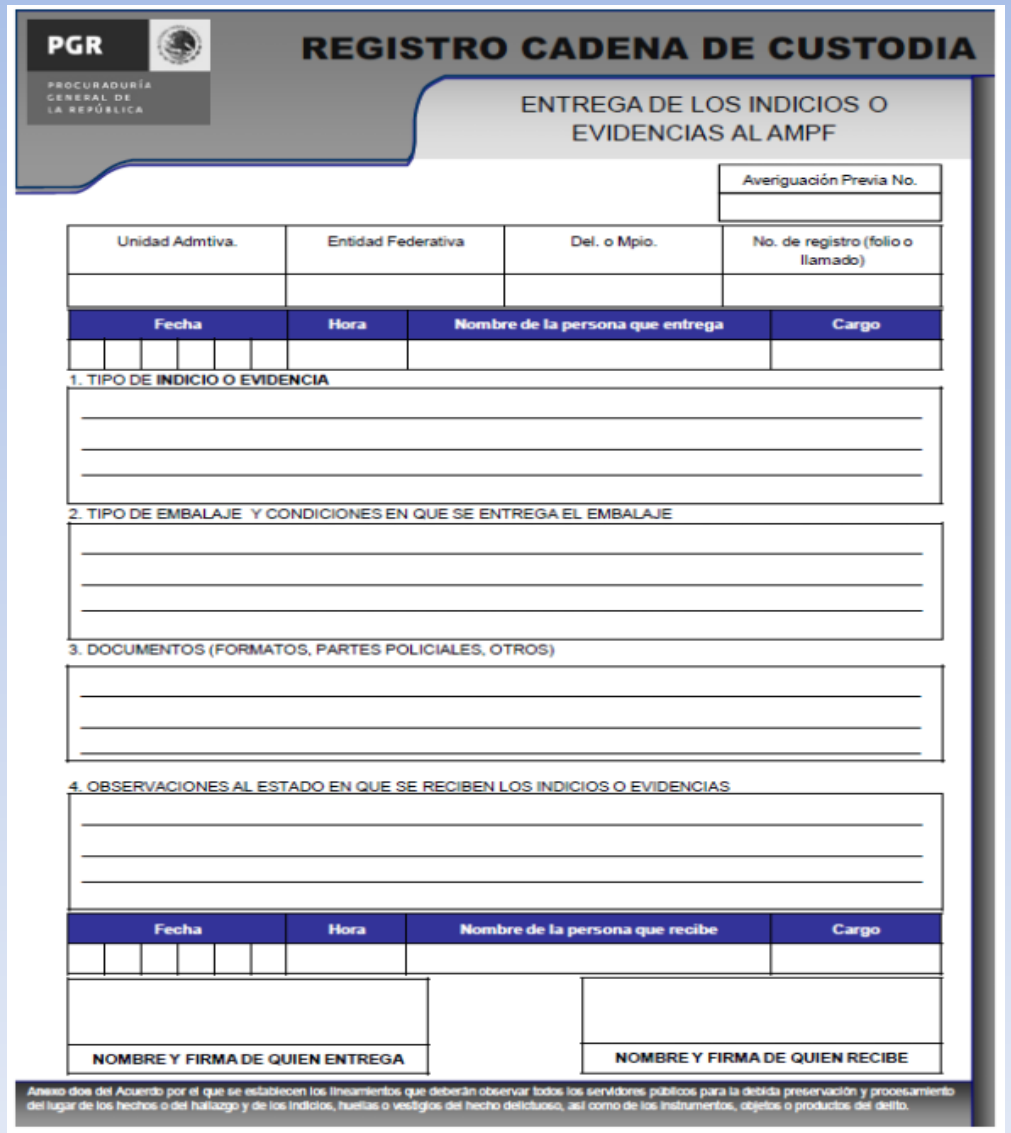
- Luego de adquisición de cada imagen forense, se deberá efectuar un hash a la evidencia original, y a la imagen forense efectuada. Si ambos hashes resultan coincidentes, entonces la copia forense es “integra”, y la evidencia será preservada

Etapa de Adquisición, por cada Evidencia a Tratar



Obligatoriedad de la cadena de Custodia

- La cadena de custodia refleja el estado en todo el proceso pericial, de las evidencias y los peritos intervinientes den las diferentes etapas



PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

REGISTRO CADENA DE CUSTODIA

ENTREGA DE LOS INDICIOS O EVIDENCIAS AL AMPF

Averiguación Previa No.

Unidad Admtiva.	Entidad Federativa	Del. o Mpio.	No. de registro (folio o llamado)

Fecha	Hora	Nombre de la persona que entrega	Cargo

1. TIPO DE **INDICIO O EVIDENCIA**

2. TIPO DE EMBALAJE Y CONDICIONES EN QUE SE ENTREGA EL EMBALAJE

3. DOCUMENTOS (FORMATOS, PARTES POLICIALES, OTROS)

4. OBSERVACIONES AL ESTADO EN QUE SE RECIBEN LOS INDICIOS O EVIDENCIAS

Fecha	Hora	Nombre de la persona que recibe	Cargo

NOMBRE Y FIRMA DE QUIEN ENTREGA	NOMBRE Y FIRMA DE QUIEN RECIBE

Anexo dos del Acuerdo por el que se establecen los lineamientos que deberán observar todos los servidores públicos para la debida preservación y procesamiento del lugar de los hechos o del hallazgo y de los indicios, huellas o vestigios del hecho delictuoso, así como de los instrumentos, objetos o productos del delito.

Procedimientos con computadoras

- Extracción de los discos duros Existentes
- Nomenclar los discos correlativamente respecto a lo efectuado con cada CPU, ej PC01-HD01
- Inserción de cada disco en la CPU examinadora
- O Inserción de cada disco en un duplicador forense
- O para el caso de notebooks, se podra arrancar con boot USB/DVD forensic

Procedimientos con los distintos elementos de Tecnología

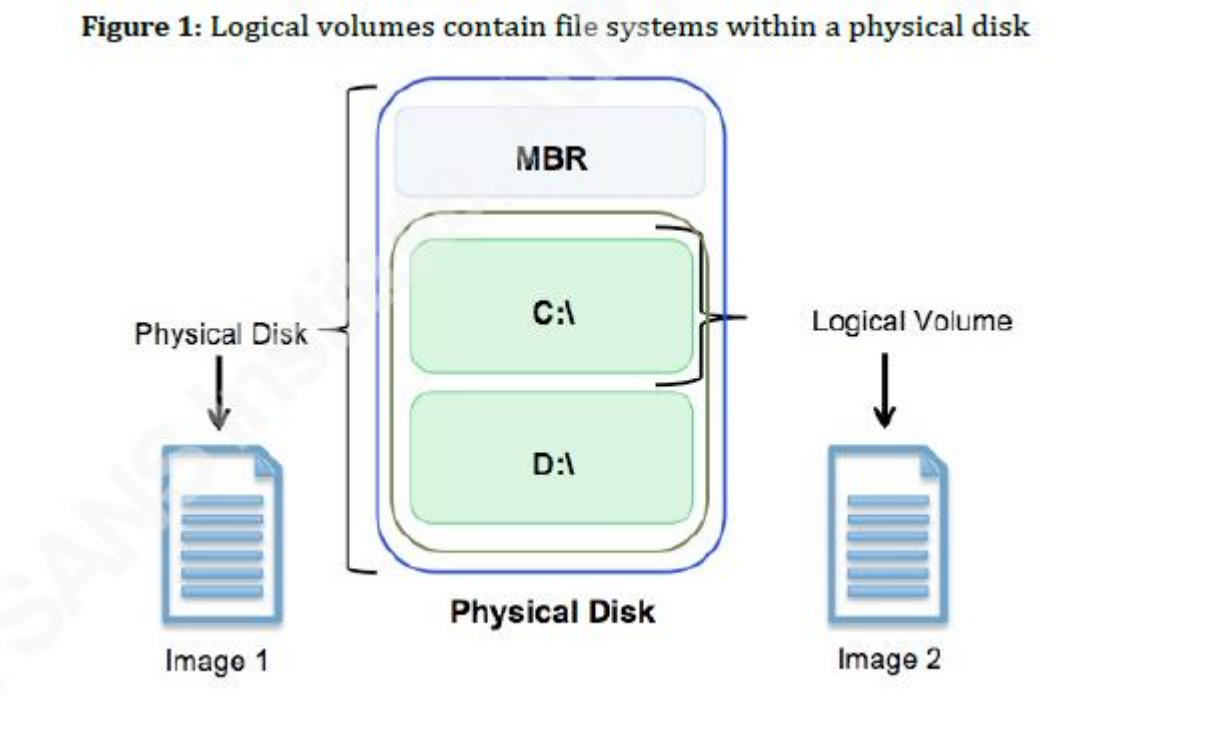
- CPU que se encuentra apagada , **“NO SE ENCIENDE”**
- CPU que se encuentra encendida **“NO SE APAGA”.** Se debe adquirir memoria “**RAM**”, y luego proceder a su desconexión eléctrica.
- Servidores de disponibilidad crítica, corresponde archivo de “**EVIDENCIA LOGICA**”, esto es tomar imagen en vivo del contenedor o carpeta que corresponda
- Servidores con sistema RAID, imagen forense de cada disco. Luego en el análisis se deberá rearmar el volumen lógico
- Memorias, usar **adaptadores USB** y bloqueando dicho puerto contra escritura para su posterior adquisición
- Elemento móvil, **bolsa de Faraday** o “**Modo Avión**” aunque es cuestionable

Antes de Adquirir

- Asegurar el bloqueo contra escritura, esto implica
  - **Bloqueo por Hard o Soft en sistemas Windows**
  - **Usar Duplicadores Forenses (Nos despreocupamos de bloquear por escritura)**
  - **Usar Linux Live CDs para adquirir evidencias, Helix, CAINE o DEFT**

Es importante **tener en cuenta el tamaño de discos a adquirir y el disco destino** en donde se alojaran dichas imágenes forenses. Otra buena práctica es la Sanitización de los discos destinos, es decir efectuar un borrado seguro sobre el/los mismos

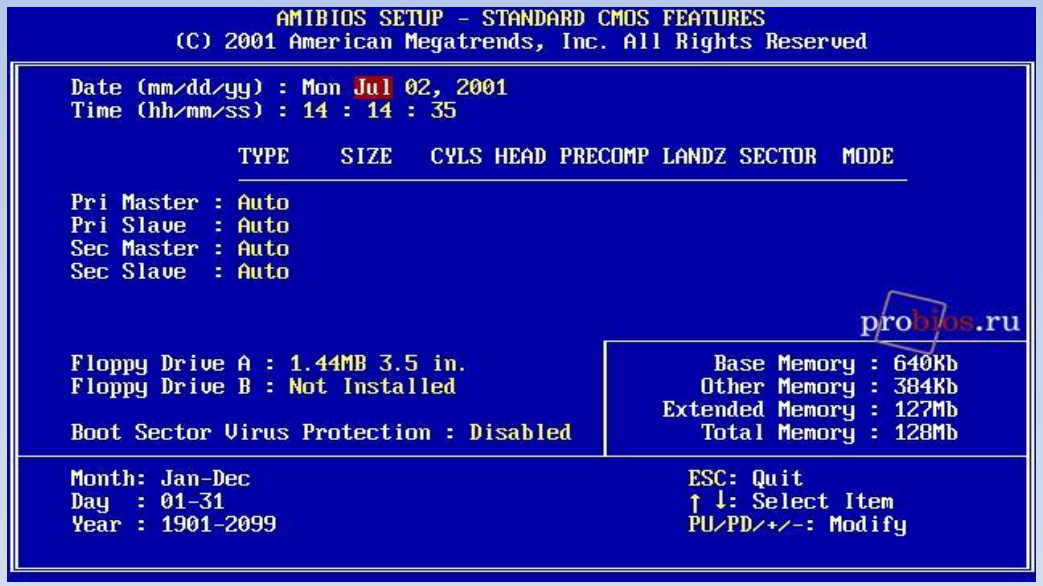
Imágenes Forenses a Realizar



Las buenas costumbres de la informática forense indican adquisición de **Disco Físico**. Si por oficio se solicita solo volumen lógico, carpetas o contenedores, se debe asentar en acta que así fue ordenado, y el perito en su informe puede hacer un descargo de que es lo que se pierde al no realizar imagen del disco en su totalidad

Otras tareas ineludibles

- Recabar horas y fechas en BIOS en CPUs evidencias (..obviamente se deben retirar los discos evidencias..)



- Seteo de la hora y fecha de la CPU en donde se adquieren las imágenes forenses. O sea en la CPU examinadora

Forensia en móviles

- **No existe el concepto de imagen forense**, ya que se examina el sistema en vivo. Con lo cual hablamos del concepto de "**extracción lógica**" de los datos de la **SIM+Sistema Operativo**
- Antes de la extracción lógica se debe usar **bolsas de faraday** para confinar el equipo dentro, para aislar de señales EM entrantes y salientes, que puedan contaminar la evidencia
- Pocas plataformas Open Source, **NEOSECURE** para Android, **Paladin** para IPHONE (es pago), salvo Autopsy 4.1.1 que analiza o **parsea** un sistema Android
- **UFED-Cellebrite, XRY Forensic** (fuerzas de la ley), **Oxigen Suite Forensic**, **MobileEdit Forensic**, son algunos de los programas mas usados

Proceso pericial Completo (no contemplado en su totalidad por la ISO 27037)

Etapa de evaluación: se debe evaluar las pruebas digitales a fondo con respecto al ámbito de aplicación del caso para determinar el curso de acción tomar.

Etapa de Adquisición: Las pruebas originales deberán ser adquiridas de manera de proteger y preservar la integridad de las mismas.

Etapa de Análisis: Investigación de los puntos de pericia solicitados por oficio. Lo mejor que nos puede pasar es que los puntos vengan bien detallados. Saben llegar oficios generalizados

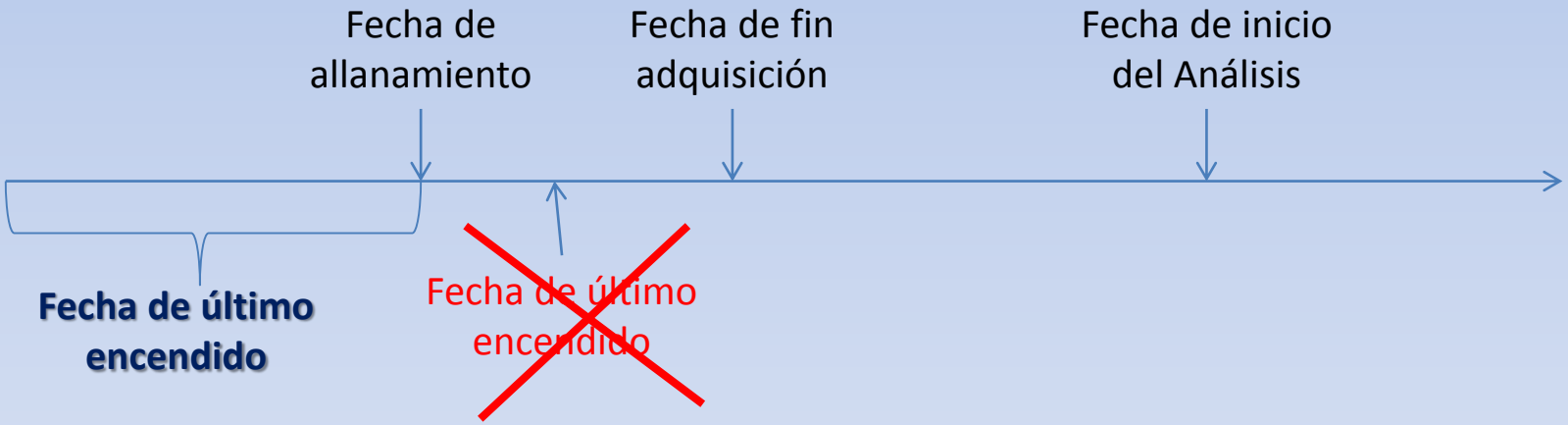
Documentación y reporte: Las acciones anteriores deben ser debidamente documentadas. Se debe concluir con un informe escrito de lo efectuado, en el ámbito judicial cuidando las formas. En el ámbito interno con un Escribano que de fe a las actas generadas; el paso posterior puede se la presentación de las pruebas en la justicia.

Análisis Forense

- Parte del proceso en donde se efectúa el análisis de los puntos solicitados, los más comúnmente pedidos son:
- Mails: tanto configurados en clientes como en Webmails (problemática actual)
- Búsqueda de palabras claves, Keyword Search
- Recuperación de información borrada
- Trazas de la información: metadatos de fechas de una acción dada
- Metadatos sobre determinados archivos: últimos archivos abiertos, fecha de ultimo encendido de equipos

¿Qué debería verificar el perito?

- Antes de iniciar el análisis, si el perito no actuó en el allanamiento, debería verificar la última fecha de encendido del equipo



- O sea la fecha de último encendido debe ser menor o igual a la fecha de allanamiento, nunca posterior. De verificar esto, el perito debe reportear que se ha roto la cadena de custodia

Software para análisis forense

- **Licenciados**: Encase Forensic, Access FTK, Nuix Investigator, IEF Mangent , Belkasoft Evidence Center
- **Open Source y Freeware**: Autopsy (Windows y Linux). DFF. Builk Extractor. Set de herramientas de DEFT o CAINE, tanto lado Windows como lado Linux. FTK imager y herramientas auxiliares.
- **Análisis de Malware**: Volatility, RED LINE, REMNux (distro forense)
- **Virtualización de Imágenes Forenses**: Live View en combinación con Vmware Workstation

Informe o Dictamen Forense

- Primeras foja/s: explicación de lo realizado en cada punto de pericia. Se debe explicar en forma concisa y guardando las formas
- Anexos: por cada punto de pericia se tendrá que efectuar un informe detallado, con todos los aspectos técnicos exportados, explicando el origen y reporteando los logs
- El perito puede considerar el envío el formato digital de la información, pasadas las 50 fojas útiles (Resolución Nº 3.909/2010 CSJN)

Muchas Gracias por su atención

- ¿Preguntas? ¿Dudas?

- ppc@sisbaires.com.ar
- @pablocroci
- https://www.facebook.com/periciasinformaticasdeparte/
- www.linkedin.com/in/pablo-croci