Seguretat Informàtica (SI)

Tema 7. Análisis forense

Davide Careglio

Fuentes: Jordi Nin, "Network Security", Computer Security, 2014
Ton Rodriguez, "Anàlisi forense", Computer Security, 2018

Temario

- Tema 1. Introducción
- Tema 2. Criptografía
- Tema 3. Infraestructura PKI

- Tema 4. Seguridad en la red
- Tema 5. Seguridad en las aplicaciones

- Tema 6. Seguridad en los sistemas operativos
- Tema 7. Análisis forense

Temario

- Tema 1. Introducción
- Tema 2. Criptografía
- Tema 3. Infraestructura PKI

- Tema 4. Seguridad en la red
- Tema 5. Seguridad en las aplicaciones

- Tema 6. Seguridad en los sistemas operativos
- **Tema 7. Análisis forense**

Tema 7. Índice

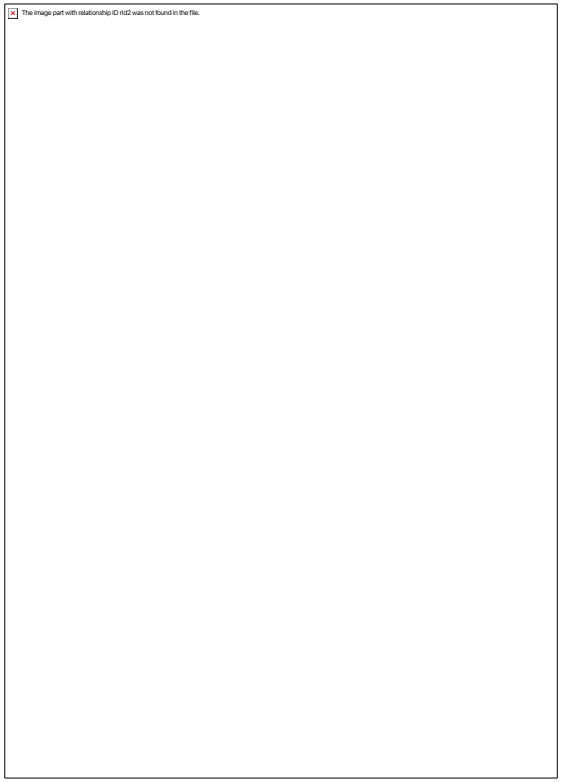
Tema 7. Índice

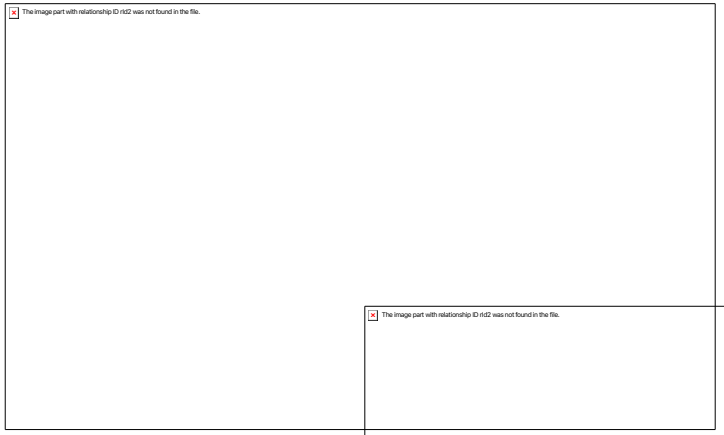
7.1 – Introducción

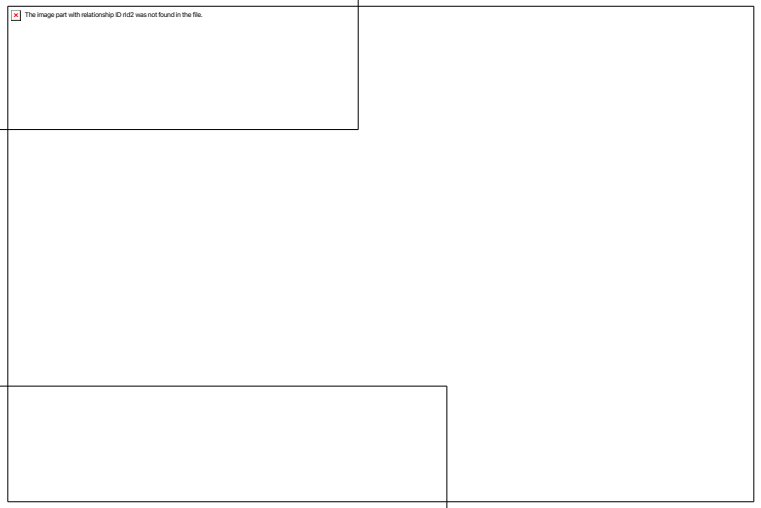
- Análisis forense…
- Significado?

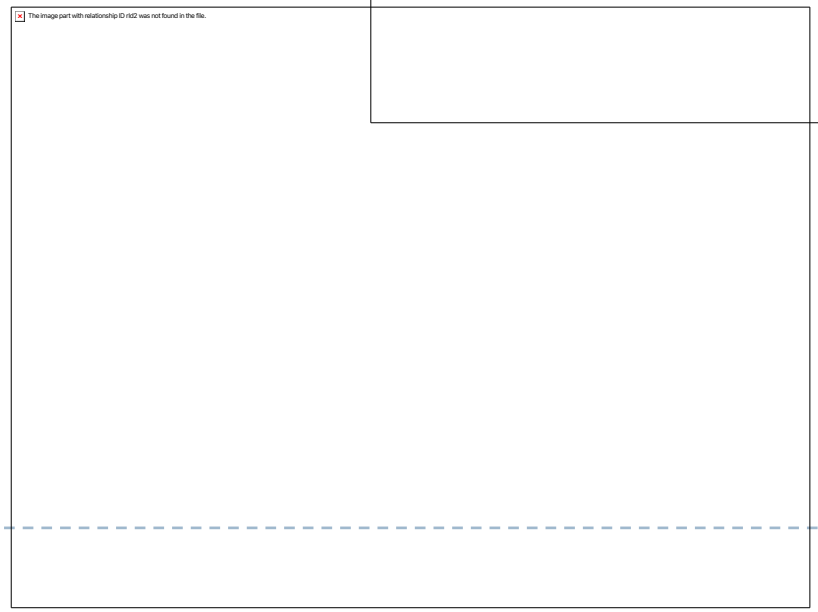
7.1 – Introducción

- Análisis forense…
- Significado?







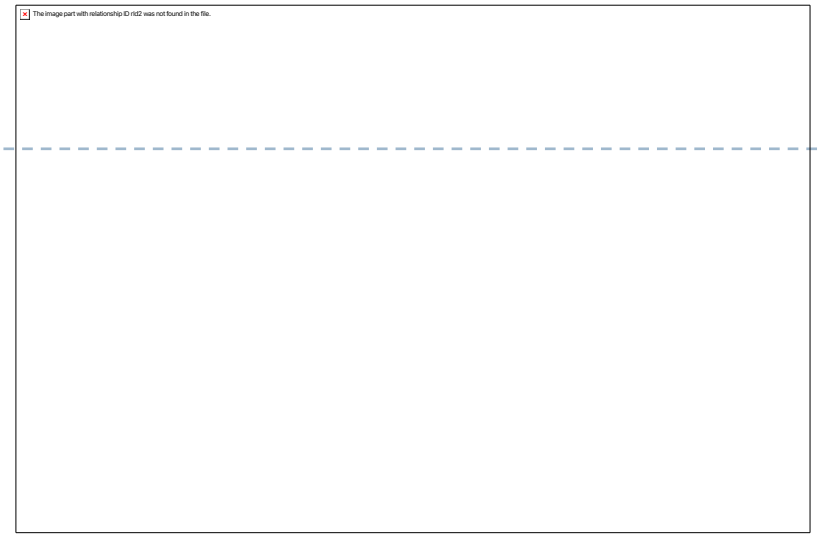


7.1 – Introducción

- Análisis forense…
- Significado?
- Y en ciberseguridad?

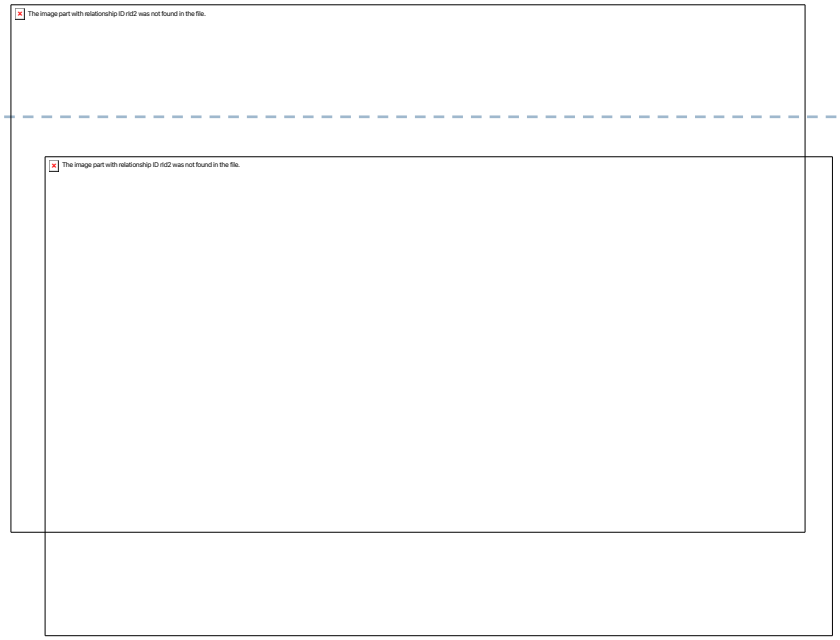
7.1 – Introducción

- Análisis forense…
- Significado?
- Y en ciberseguridad?



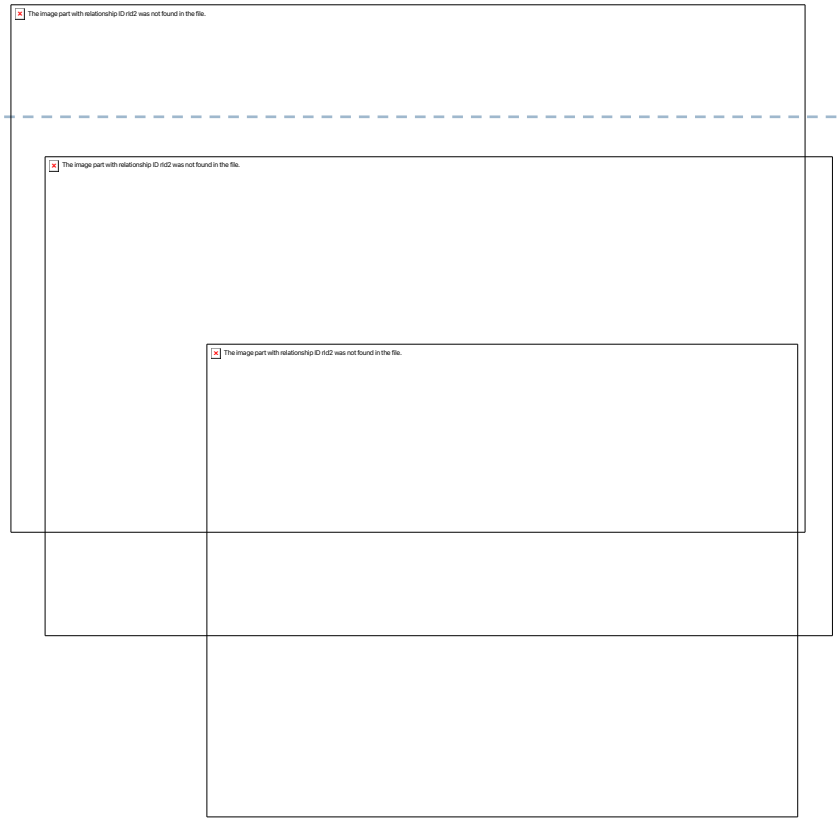
7.1 – Introducción

- Análisis forense…
- Significado?
- Y en ciberseguridad?
  - Análisis de hardware



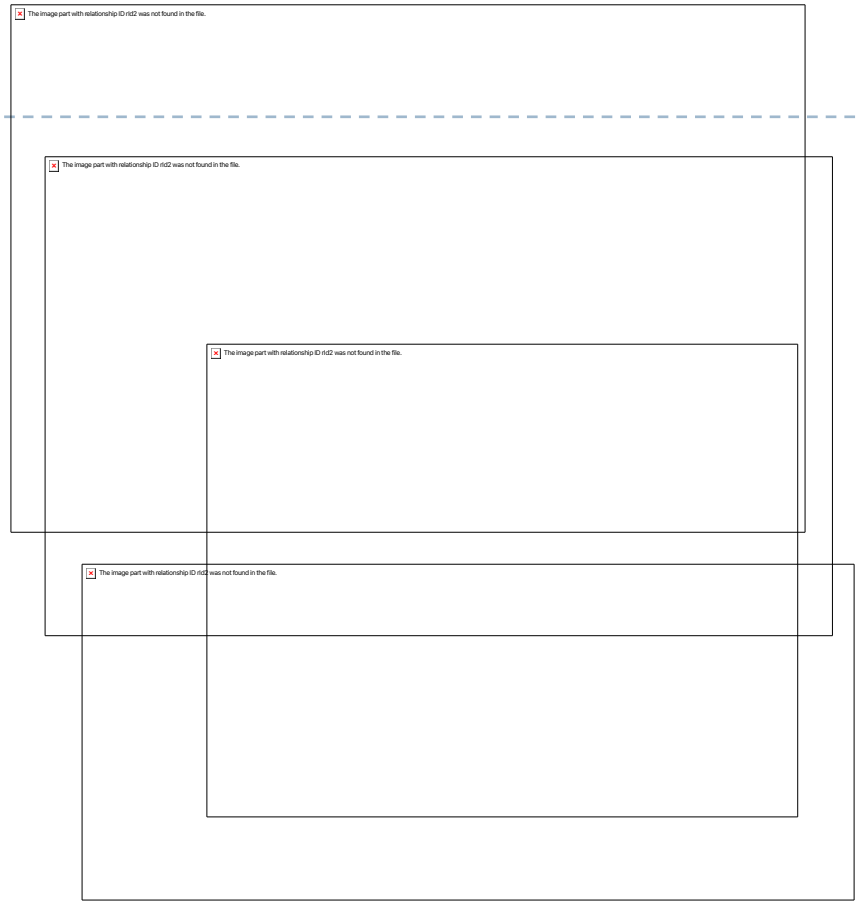
7.1 – Introducción

- Análisis forense…
- Significado?
- Y en ciberseguridad?
  - Análisis de hardware
  - Datos almacenados



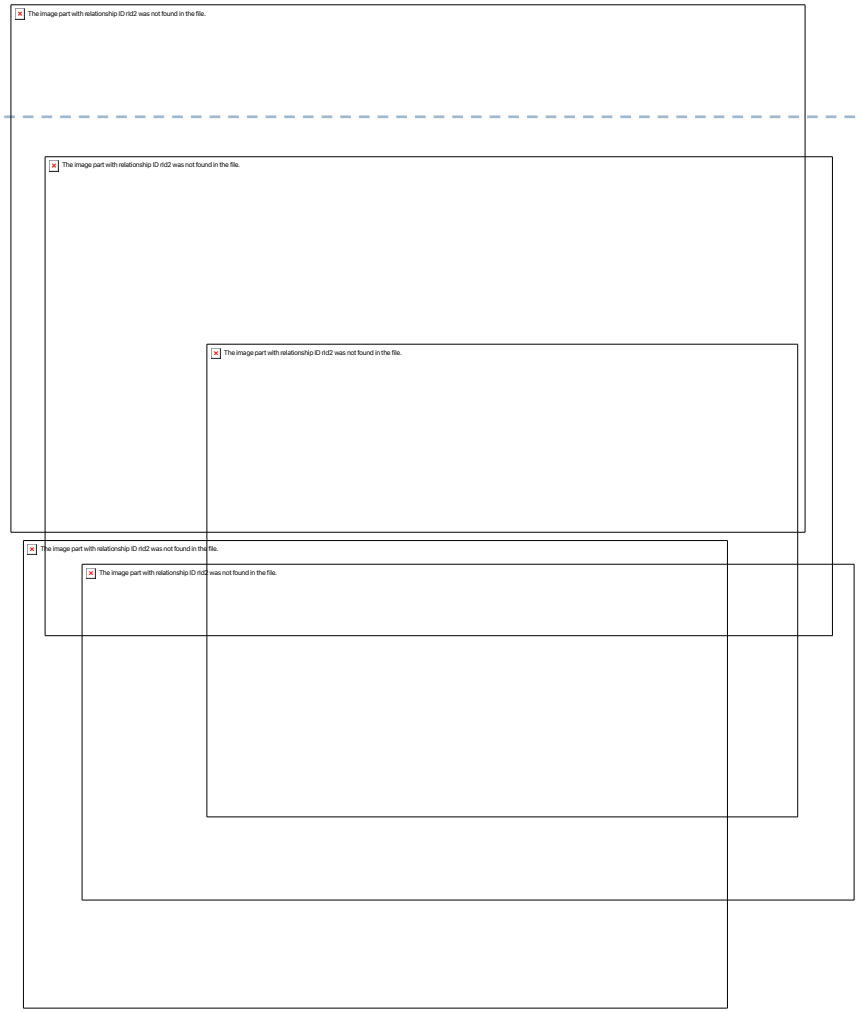
7.1 – Introducción

- Análisis forense…
- Significado?
- Y en ciberseguridad?
  - Análisis de hardware
  - Datos almacenados
  - Software



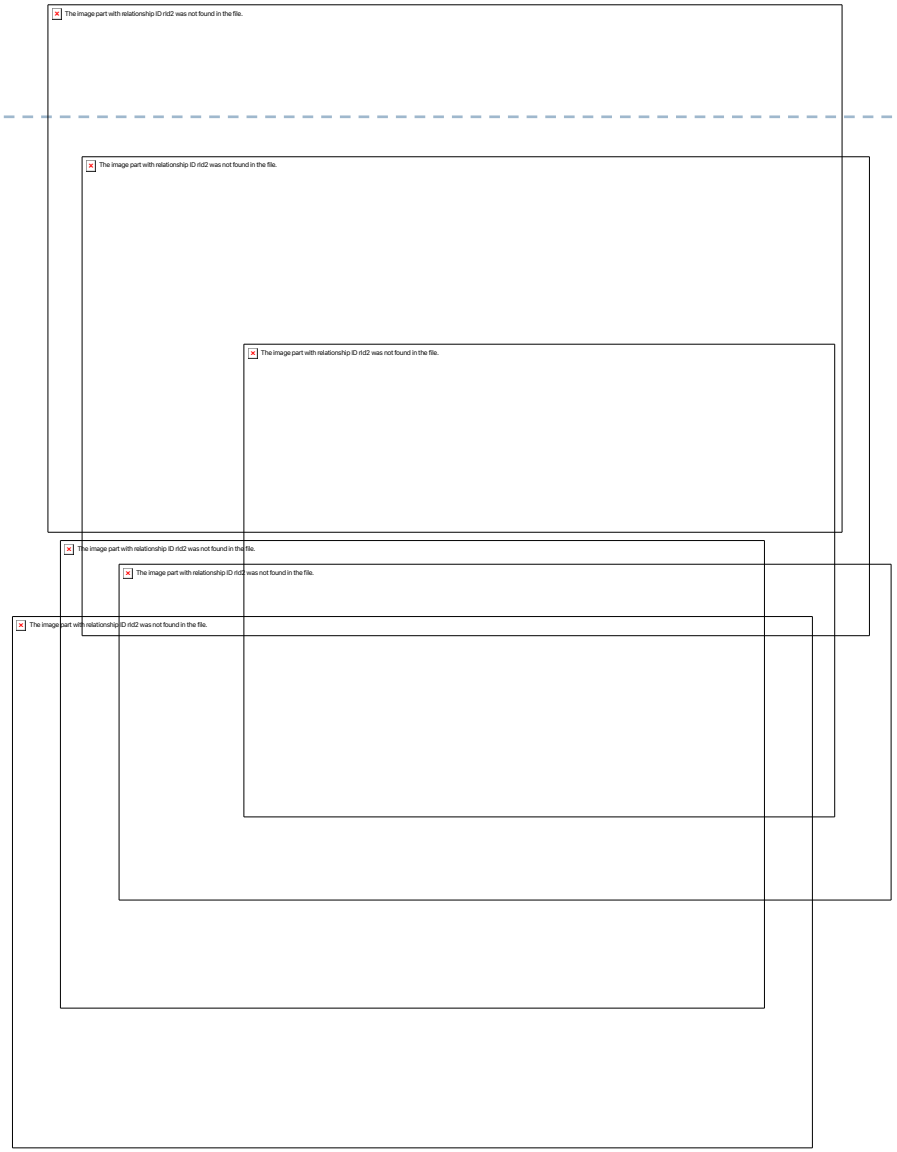
7.1 – Introducción

- Análisis forense…
- Significado?
- Y en ciberseguridad?
  - Análisis de hardware
  - Datos almacenados
  - Software
  - Leyes especificas



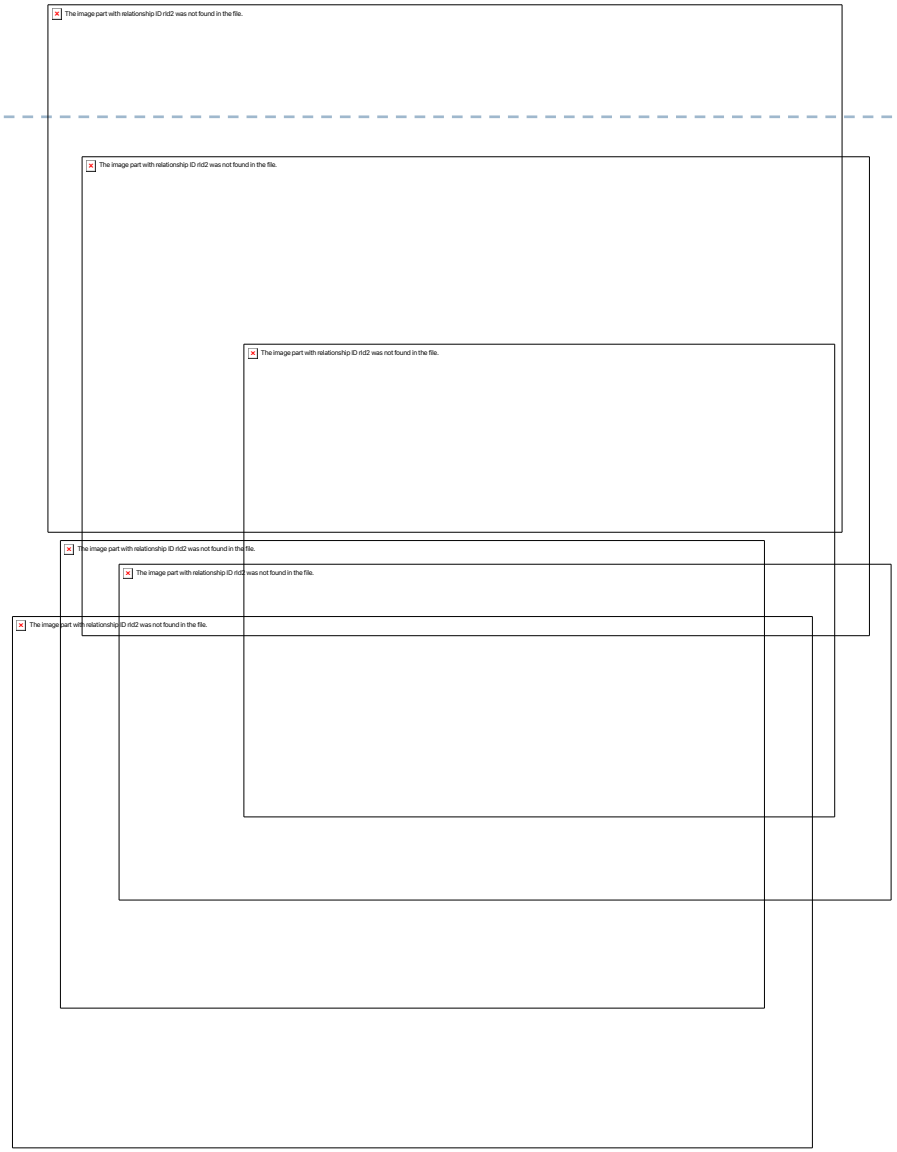
7.1 – Introducción

- Análisis forense…
- Significado?
- Y en ciberseguridad?
  - Análisis de hardware
  - Datos almacenados
  - Software
  - Leyes especificas
  - Rastrear huellas



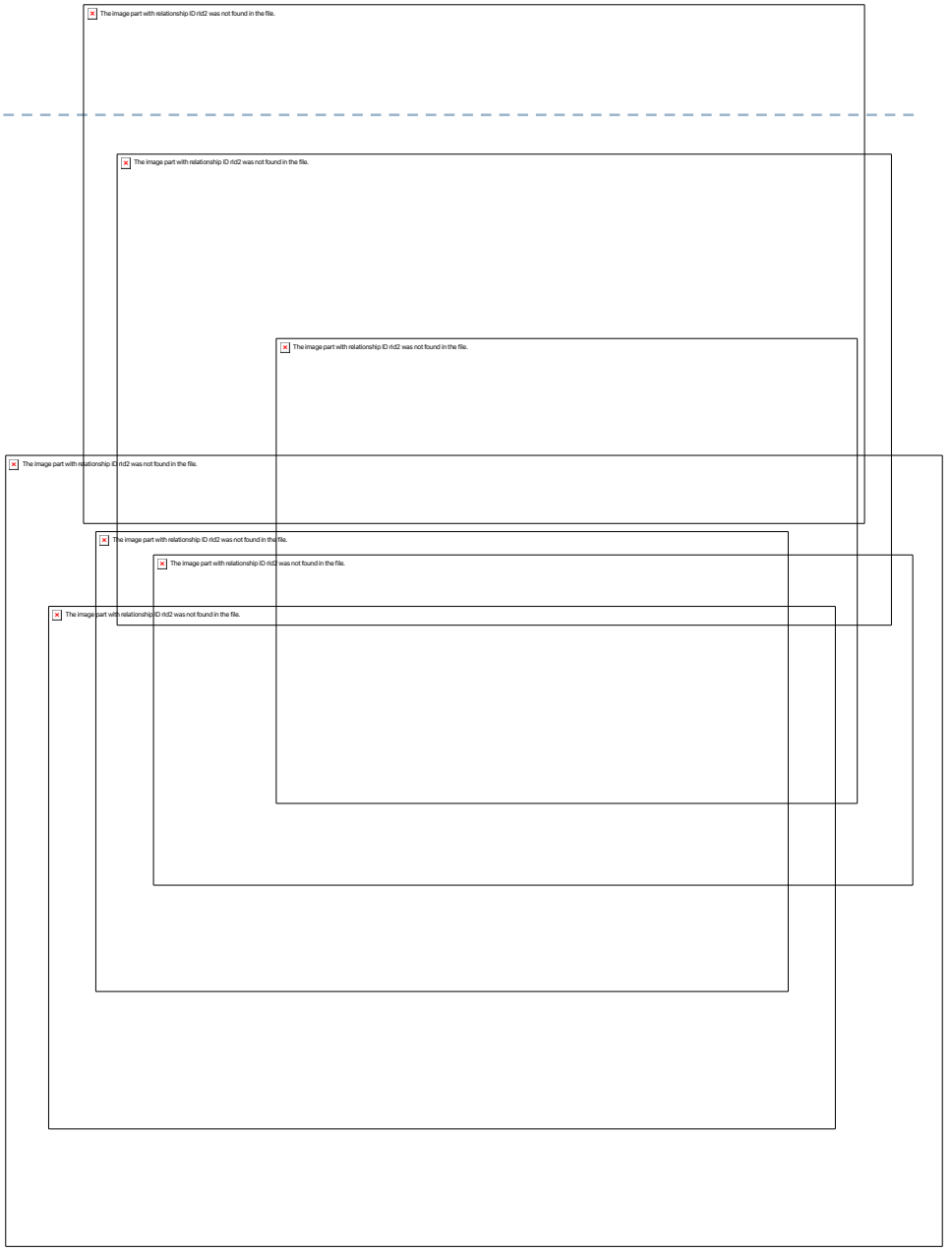
7.1 – Introducción

- Análisis forense…
- Significado?
- Y en ciberseguridad?
  - Análisis de hardware
  - Datos almacenados
  - Software
  - Leyes especificas
  - Rastrear huellas
  - Falta algo?



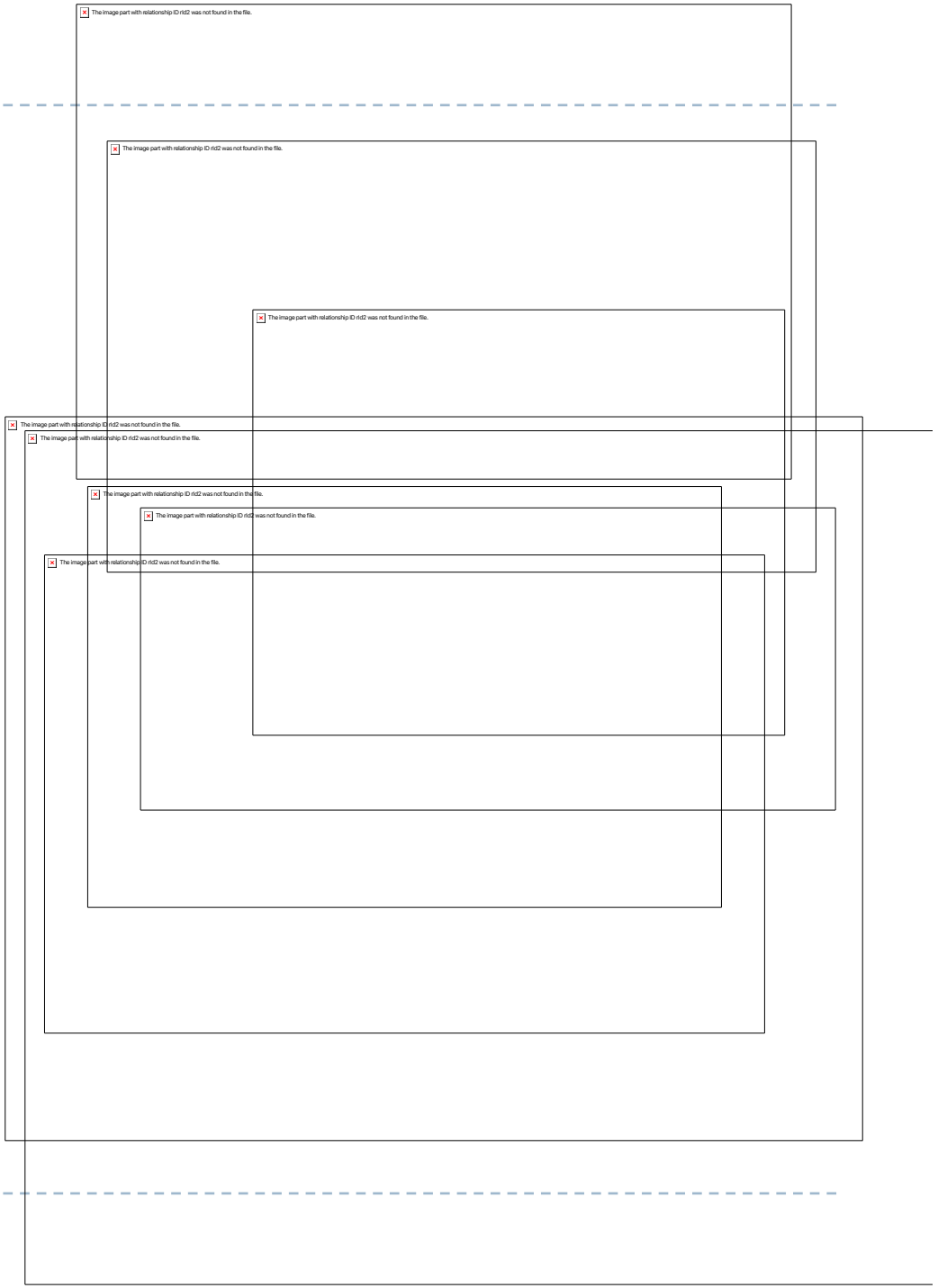
7.1 – Introducción

- Análisis forense…
- Significado?
- Y en ciberseguridad?
  - Análisis de hardware
  - Datos almacenados
  - Software
  - Leyes especificas
  - Rastrear huellas
  - Falta algo?
  - Reconocer que ha habido un crimen!!



7.1 – Introducción

- Análisis forense…
- Significado?
- Y en ciberseguridad?
  - Análisis de hardware
  - Datos almacenados
  - Software
  - Leyes especificas
  - Rastrear huellas
  - Falta algo?
  - Reconocer que ha habido un crimen!!
  - Encontrar evidencias del crimen



7.1 – Introducción

- La informática forense es la aplicación, en el ámbito IT, de técnicas científicas y analíticas especializadas para identificar, preservar, analizar y presentar datos que sean válidos en un proceso legal
- La "realización de un forense" se basa en la investigación de un incidente de seguridad donde interviene información digital
- Los principales retos de esta investigación son:
  - Las evidencias digitales son complejas
  - La objetividad y conocimiento de los peritos y jueces
  - La inexistente estandarización de herramientas
  - ¿Es un arte o es una ciencia?

7.1 – Introducción

- La informática forense es la aplicación, en el ámbito IT, de técnicas científicas y analíticas especializadas para identificar, preservar, analizar y presentar datos que sean válidos en un proceso legal
- La "realización de un forense" se basa en la investigación de un **incidente de seguridad** donde interviene información digital
- Los principales retos de esta investigación son:
  - Las evidencias digitales son complejas
  - La objetividad y conocimiento de los peritos y jueces
  - La inexistente estandarización de herramientas
  - ¿Es un arte o es una ciencia?

7.1 – Introducción
Incidente de seguridad

- Evento adverso en el que algún aspecto de la seguridad del ordenador puede estar amenazado
  - Pérdida de confidencialidad o integridad de los datos
  - Interrupción del sistema
  - Interrupción o denegación del servicio disponible
- Antiguamente: hackers o "chicos traviesos"
- Actualidad: mafias o cibercriminales
  - Ataques externos e internos
  - Robo de información
  - Espionaje (propiedad intelectual)
  - Denegación de servicio (competencia)
  - Troyanos, virus, phishing, etc.

7.1 – Introducción
El primer ataque

- En 1988 había unas 60.000 máquinas conectadas en Internet sin preocuparse demasiado por la seguridad
- El 2 de noviembre de 1988 aparece un gusano creado por el estudiante Robert T. Morris como un experimento que utilizaba un defecto del SO Unix para reproducirse hasta bloquear el ordenador
- La fiscalía argumentó que no se trataba de un error si no de un ataque contra el gobierno de los Estados Unidos
- Se le condenó a 3 años de libertad condicional, $14,000 de multa y 400 horas de servicio a la comunidad

7.1 – Introducción
Los primeros CERT

- En diciembre de 1988, a raíz del incidente con el gusano Morris, se crea Computer Emergency Response Team Coordination Center (CERT/CC) en la Carnegie Mellon, www.cert.org
- Team de expertos en seguridad informática con el objetivo de responder de forma óptima ante una incidencia donde intervenga información digital
- También se conocen como
  - Computer Emergency Readiness Team
  - Computer Security Incident Response Team (CSIRT)

7.1 – Introducción
Los primeros CERT

- En 1992 se crea el primer equipo de respuesta a incidentes europeo, el SURFnet-CERT holandés
- A finales de 1994, la UPC crea esCERT-UPC (ahora incluida en inLab)
- ¿En España?
  - En el 1995 se crea IRIS-CERT a la comunidad RedIRIS https://www.rediris.es/cert/
  - En el 2006, el CCN-CERT adscrito al CNI https://www.ccn-cert.cni.es
  - En el 2014, el INCIBE-CERT adscrito al Ministerio de Economía y Empresa https://www.incibe-cert.es

Tema 7. Índice

7.2 - Aspectos legales

- Se suele realizar un análisis forense para
  - Determinar actividades que se presumen delictivas o ilegítimas
  - Obtener pruebas simplemente a título informativo para conocimiento exclusivo del cliente
- Es importante conocer la legislación para evitar el rechazo de pruebas en un juicio por haber infringido la ley
  - Una prueba es el instrumento que tienen las partes para acreditar los hechos en los que basan sus pretensiones
  - El momento de presentación de las mismas depende de la jurisdicción
    - Civil, Laboral o Social, Penal, Contencioso Administrativa

7.2 – Aspectos legales
Jurisdicción civil

- Está regulada por la Ley de Enjuiciamiento Civil
  - https://www.boe.es/buscar/act.php?id=BOE-A-2000-323
- Pruebas periciales
  - De parte (se adjuntan a la demanda o contestación)
  - Judiciales (las pueden pedir las partes antes de la vista)
- Ámbitos mayoritarios de actuación
  - Demostración de daños en equipos informáticos
  - Demostración de competencia desleal
  - Identificación de sujetos que hayan cometido un ilícito civil
- Áreas especializadas
  - Mercantil/comercial
  - Familiar

7.2 – Aspectos legales
Jurisdicción laboral o social

- Está regulada por la Ley de Procedimiento Laboral
  - https://www.boe.es/buscar/act.php?id=BOE-A-1995-8758
- Ámbito de actuación
  - Obtención de información sobre el uso correcto o incorrecto por parte de los trabajadores de los medios telemáticos titularidad del empresario
- Áreas especializadas
  - Relaciones laborales entre las partes (denunciante y denunciada)
- Se limita la capacidad de control del empresario en favor de los derechos fundamentales de los trabajadores

7.2 – Aspectos legales
Empresarios vs trabajadores

- Obtención de pruebas:
  - El registro de equipos informáticos se realizará en horario laboral, dentro de los locales de la empresa y en presencia de un representante de los trabajadores

Art. 90.1 Ley de Procedimiento Laboral	Art. 20.3 Estatuto de los Trabajadores
Las partes podrán valerse de cuantos medios de prueba se encuentren regulados en la Ley, admitiéndose como tales los medios mecánicos de reproducción de la palabra, de la imagen y del sonido, salvo que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas.	El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso

7.2 – Aspectos legales
Jurisdicción penal

- Está regulada por la Ley de Enjuiciamiento Criminal
  - https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036
- Ámbito de actuación
  - Aportar pruebas sobre presuntos delitos o faltas
  - La validez de estas pruebas, requerirá en muchos casos la colaboración con órganos judiciales (jueces de instrucción) a la hora de obtener las evidencias
- Fases del procedimiento
  - Instrucción
  - Enjuiciamiento

7.2 – Aspectos legales
Jurisdicción penal

- Está regulada por la Ley de Enjuiciamiento Criminal
  - https://www.boe.es/buscar/act.php?id=BOE-A-**1882**-6036
- Ámbito de actuación
  - Aportar pruebas sobre presuntos delitos o faltas
  - La validez de estas pruebas, requerirá en muchos casos la colaboración con órganos judiciales (jueces de instrucción) a la hora de obtener las evidencias
- Fases del procedimiento
  - Instrucción
  - Enjuiciamiento

7.2 – Aspectos legales
Jurisdicción penal

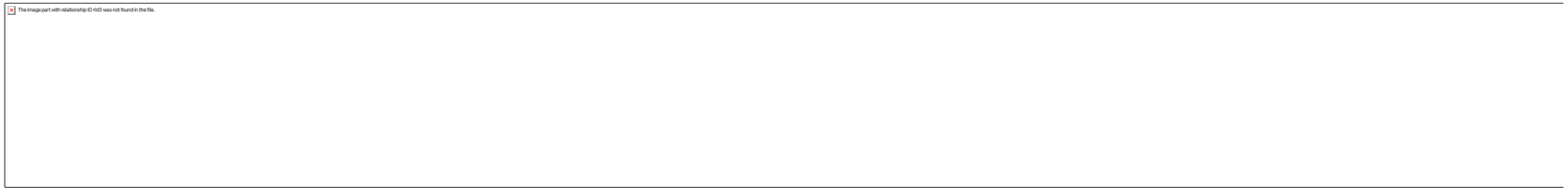
- Está regulada por la Ley de Enjuiciamiento Criminal
  - https://www.boe.es/buscar/act.php?id=BOE-A-**1882**-6036
- Ámbito de actuación
  - Aportar pruebas sobre presuntos delitos o faltas
  - La validez de estas pruebas, requerirá en muchos casos la colaboración con órganos judiciales (jueces de instrucción) a la hora de obtener las evidencias
- Fases del procedimiento
  - Instrucción
  - Enjuiciamiento

7.2 – Aspectos legales
Contenciosos administrativos

- Ámbito de actuación:
  - Litigios de particulares y empresas contra las Administraciones públicas (Estado, Comunidades Autónomas y Entidades Locales)
  - Toda clase de entes públicos (Agencia de protección de datos, Servicio de Salud de una Comunidad Autónoma, Universidades públicas, etcétera)

7.2 – Aspectos legales
Leyes especificas sobre SI

- Código de Derecho de la Ciberseguridad
  - https://www.boe.es/legislacion/codigos/codigo.php?id=173&modo=1&nota=0&tab=2

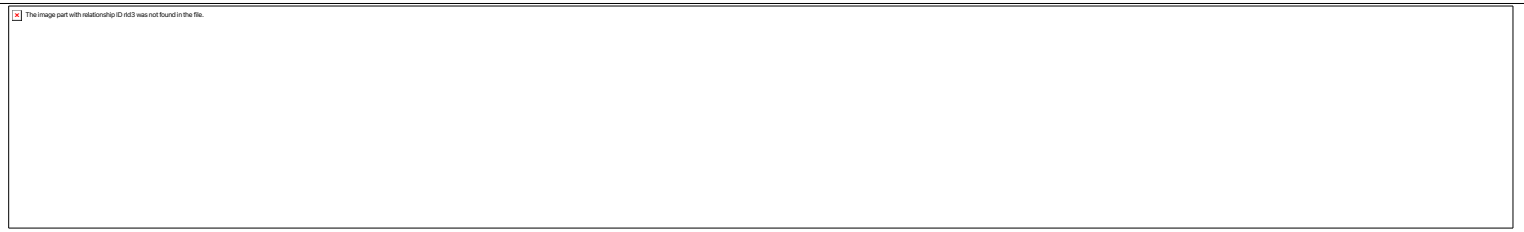


7.2 – Aspectos legales
Leyes especificas sobre SI

- Código de Derecho de la Ciberseguridad
  - https://www.boe.es/legislacion/codigos/codigo.php?id=173&modo=1&nota=0&tab=2

7.2 – Aspectos legales
Leyes especificas sobre SI

- Código de Derecho de la Ciberseguridad
  - https://www.boe.es/legislacion/codigos/codigo.php?id=173&modo=1&nota=0&tab=2



Tema 7. Índice

7.3 – Aspectos de una investigación
Como se inicia una investigación

- Las investigaciones forenses se suelen iniciar
  - A partir de una orden judicial cuando las fuerzas del orden tienen indicios de algún delito
    - Se necesita para que el juzgado admita las evidencias
  - Por aplicación de una política de seguridad de la empresa que permita que se realice
    - Banners, cursos de concienciación, entrega de documentos en papel de lectura obligada
    - Firma de la documentación conforme se ha sido informado sobre las consecuencias de incumplir la política de seguridad
- Si no es ninguno de los casos anteriores, se puede empezar previo consentimiento voluntario de las partes implicadas

7.3 – Aspectos de una investigación

Inicio de un proceso

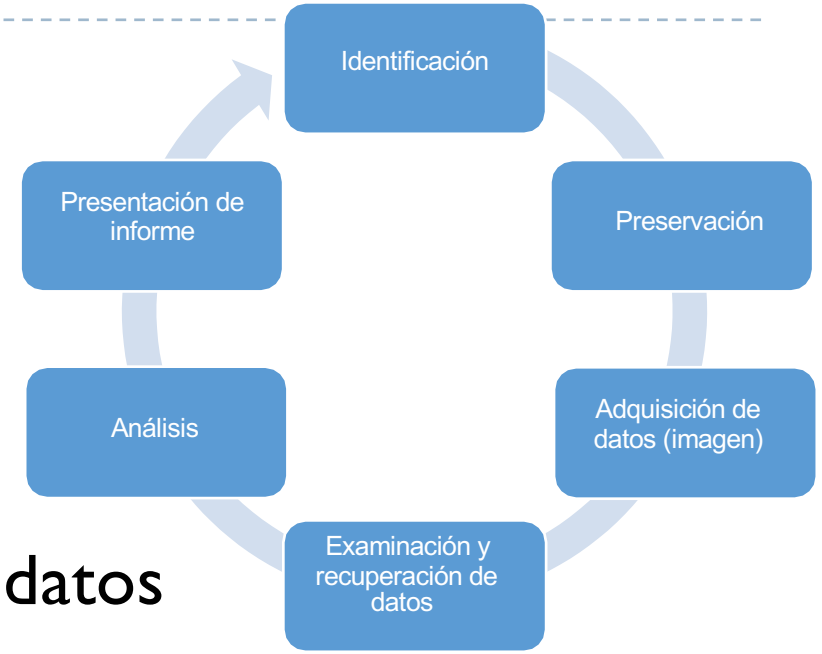
- Procedimientos civiles, mercantiles o laborales
  - Demanda
- Procedimientos penales (por delitos o faltas)
  - Denuncia
    - No tenemos porque ser víctimas
    - Se realiza de forma oral o escrita, ante la policía o el juzgado
  - Querella
    - Siempre somos la parte perjudicada
    - Se denuncia a una persona concreta
    - Se realiza por escrito en un juzgado
    - Se deben aportar pruebas que demuestren el hecho denunciado
    - Se necesita un abogado y un procurador
- "Diferencia entre demanda, denuncia y querella"

7.3 – Aspectos de una investigación
Buenas prácticas

- Documentación exhaustiva
  - Preservación de las evidencias
- Formación continua
  - Realización de cursos sobre análisis forense
  - Estudio de nuevas técnicas y herramientas
  - Recursos web y revistas especializadas
  - European Network of Forensic Science Institutes, http://enfsi.eu
- Conducta profesional
  - Integridad
  - Confidencialidad
  - Ética
  - Moral

7.3 – Aspectos de una investigación

Metodología: 6 fases



- **Identificación** del escenario
  - Evaluación del caso
- **Preservación**
  - Documentación y búsqueda de las evidencias
- **Adquisición** o recuperación de datos
- **Examinación**
  - Agregación y obtención de información relevante, ficheros eliminados, etc.
- **Análisis** en un entorno de laboratorio
- **Presentación**
  - Elaboración de un informe y presentación del mismo

7.3 – Aspectos de una investigación

Paso 1: Identificación del escenario

- La evaluación del caso implica acotar el entorno en el que se ha producido
  - Tipo de evidencia involucrada
  - Sistemas operativos y software involucrados
  - Formato de los sistemas de ficheros
  - Localización de la evidencia
  - Motivo de la sospecha
- Es muy importante
  - Tener profesionales con conocimientos adecuados
  - Disponer de un laboratorio forense
  - Disponer de materiales apropiados para recoger y procesar las evidencias

7.3 – Aspectos de una investigación

Paso 2: Preservación

- La metodología de recolección y preservación de las evidencias implica documentar exhaustivamente:
  - El escenario
  - El método de obtención de la evidencia
  - La cadena de custodia
  - El hardware y la configuración del sistema
  - La hora y fecha del sistema
  - Las fechas y horas clave de los sucesos
  - Etcétera

7.3 – Aspectos de una investigación

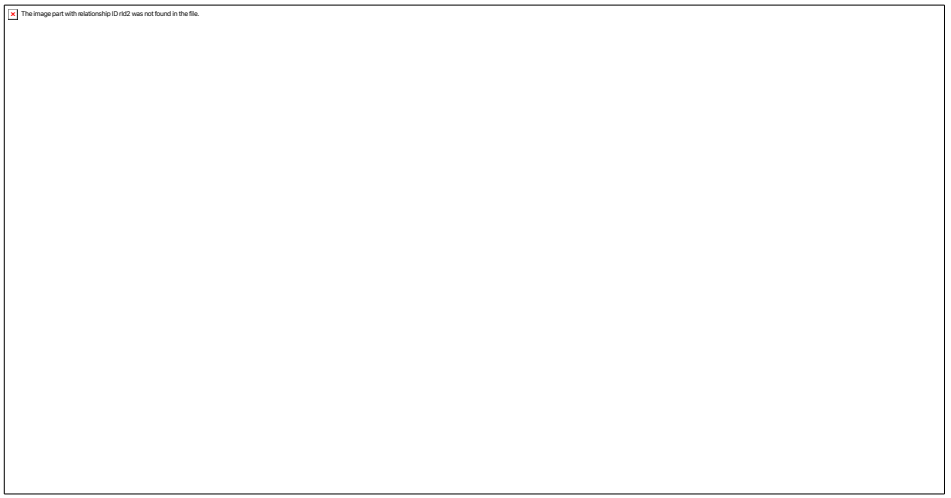
Paso 3: Adquisición

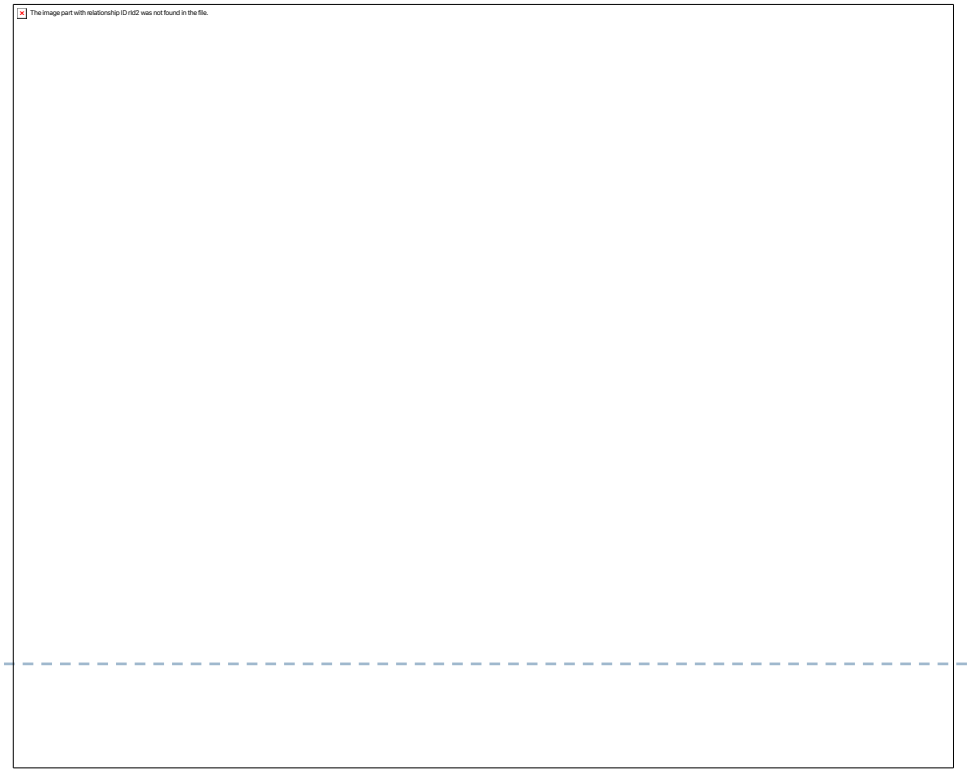
- "Una evidencia sin metodología no es una prueba”

1. Localizar la evidencia
2. Asegurar el escenario
3. Descubrir datos relevantes
4. Preparar el orden de volatilidad (de mayor a menor)
   - Ordenar la información según su disponibilidad en el tiempo
5. Recoger la evidencia
   - Recuperación de información borrada u oculta
   - Duplicado de la evidencia (bit a bit)
6. Preparar la cadena de custodia

7.3 – Aspectos de una investigación

Paso 3: Adquisición





7.3 – Aspectos de una investigación

Paso 4: Examinación

- Agregar la información relevante obtenida anteriormente
- Filtrar la información
  - Palabras clave
  - Información temporal
- Obtener los datos relevantes
  - De la información obtenida, sacar la parte importante para la investigación
  - Por ejemplo, extraer el buzón de un usuario de una base de datos

7.3 – Aspectos de una investigación

Paso 5: Análisis

- Análisis en un entorno de laboratorio
  - Se utiliza una copia de la evidencia
  - Utilización de herramientas forenses
- Analizar el conocimiento extraído de los datos ya procesados
  - Respetando la legalidad
  - Investigando únicamente aquello por lo que estamos autorizados

7.3 – Aspectos de una investigación

Paso 5: Análisis

- Análisis en un entorno de laboratorio
  - Se utiliza una copia de la evidencia
  - Utilización de herramientas forenses
- Analizar el conocimiento extraído de los datos ya procesados
  - Respetando la legalidad
  - Investigando únicamente aquello por lo que estamos autorizados

7.3 – Aspectos de una investigación

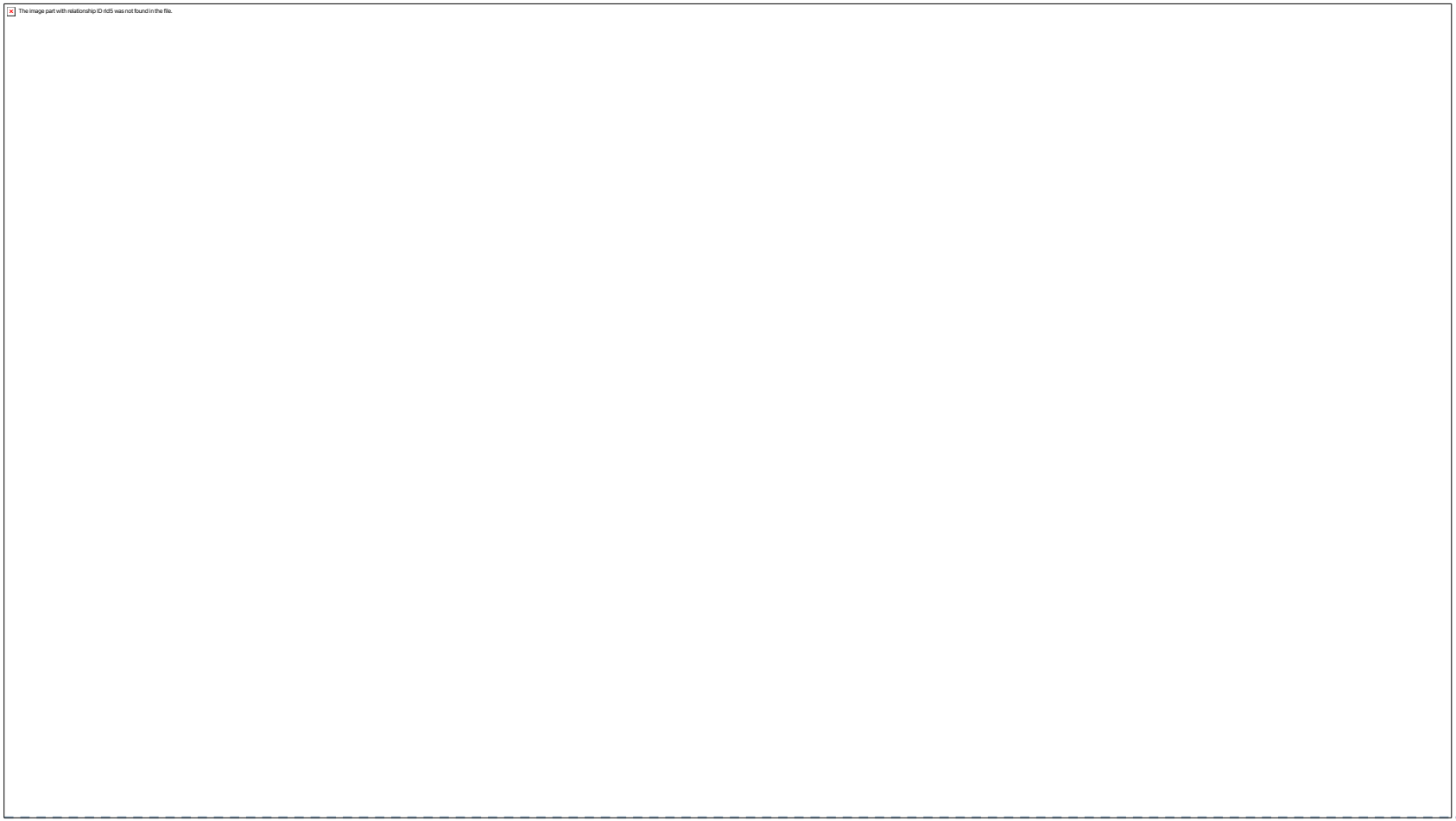
Paso 6: Presentación

- Expresar en un documento los hechos:
  - Contrastados
  - Relacionados con la investigación
- No incluir datos subjetivos
  - Si se expresa una hipótesis, comentarla claramente
- El informe debe incluir el trabajo realizado y los resultados obtenidos
  - Se incluirá el qué, cuándo, cómo y dónde
  - No se incluyó el porqué
  - Los hallazgos deben ser reproducibles

7.3 – Aspectos de una investigación

Resumen

- Video de Guidance Software
- https://www.youtube.com/watch?v=Xo6El8c3qrU



Tema 7. Índice

- Introducción
- Aspectos legales
- Aspectos de una investigación
- **Forensic Readiness**
- Adquisición de evidencias
  - Artefactos de Linux
  - Artefactos de Windows

7.4 – Forensic Readiness

- Investigación forense de una evidencia digital
  - Respuesta a un incidente de seguridad o crimen relacionado con ordenadores
  - Sería interesante tener la capacidad de
    - Leer/analizar datos constantemente para determinar si hay un ataque, se está cometiendo un crimen, se está haciendo un mal uso de los recursos, etc.
    - Saber preservar las evidencias digitales antes, durante y despues de la ocurrencia del incidente

7.4 – Forensic Readiness

- Definición
  - "Una organización debe tener un nivel apropiado de capacidad para poder preservar, recopilar, proteger y analizar evidencias digitales para que estas evidencias puedan ser utilizadas efectivamente: en cualquier asunto legal; en investigaciones de seguridad; en procedimientos disciplinarios; en un tribunal laboral; o en un tribunal de justicia."[1]
  - El uso de las evidencias digitales como defensa requiere
    - Monitorización de sistemas y usuarios: archivos de registro, correo electrónico, tráfico de red, llamadas telefónicas, etc.
    - Medios (técnicos, físicos y procedimentales) para asegurar los datos con los estándares de admisibilidad

[1] CESG Good Practice Guide No. 18, Forensic Readiness

7.4 – Forensic Readiness
Escenarios

- La recolección de evidencias debe estar preparada para una amplia gama de escenarios:
  - Amenazas y extorsión
  - Compromiso de la información
  - Accidentes y negligencias
  - Disputas comerciales
  - Desacuerdos, engaños y malas prácticas
  - Delincuencia económica (p.ej. Blanqueo de dinero)
  - Abuso de contenido
  - Invasión de la privacidad y robo de identidad
  - Cuestiones disciplinarias de los empleados
  - Etc.

7.4 – Forensic Readiness

Beneficios

- Posible defensa en una demanda judicial
- Elemento de disuasión de las amenazas internas
- Interrupción mínima del negocio
- Reducción de costes de investigación
- Reducción de costes de divulgación (por ejemplo, conformidad con la LPD)
- Muestra una diligencia corporativa ante los activos de información de la empresa
- Demuestra el cumplimiento de reglamentaciones
- Apoyo a posibles sanciones a trabajadores

7.4 – Forensic Readiness

Fuentes

- ¿Dónde se generan los datos?
- ¿En qué formato se encuentran almacenadas?
- ¿Cuánto tiempo se almacenan y por qué?
- ¿Cómo se gestionan, se controlan y protegen?
- ¿Quién tiene acceso a los datos?
- ¿Cuántas datos se producen?
- ¿Quién es responsable de estos datos?
- ¿Cómo podrían utilizarse en una investigación?
- ¿Contienen información personal?
- Etc.

7.4 – Forensic Readiness

Requerimientos

- Conocimiento de la seguridad del entorno
  - Inventario de activos
  - Avisos de vulnerabilidades
  - Análisis del riesgo
- Monitoreo
  - Paneles de control
  - Detección de intrusiones: NIDS (Snort) y HIDS (OSSEC)
  - Correlación de eventos: Security information and event management (OSSIM)
- Herramientas de gestión de incidentes
  - Correo electrónico y formularios
  - Filtrado y priorización
  - Base de datos de conocimiento

Tema 7. Índice

- Introducción
- Aspectos legales
- Aspectos de una investigación
- Forensic Readiness
- **Adquisición de evidencias**
  - Artefactos de Linux
  - Artefactos de Windows

7.5 – Adquisición de evidencias
Evaluación

- La evidencia digital debe ser evaluada en función del alcance de cada caso
  - Revisar el orden de registro u otra autorización legal
  - Discutir con el investigador principal que se puede o no descubrir mediante la realización del forense
  - Estudiar la posibilidad de obtener otras evidencias
    - P.ej. Envío de una orden de preservación de datos a un ISP
  - Considerar la relevancia de los periféricos al caso
    - P.ej. Robo o fraude: tarjetas de crédito en blanco, papel de cheques, impresoras, escáneres, etc.
  - Determinar si hay información adicional al caso
    - P.ej. Cuentas de correo, ISP, usuarios, ajustes de red, etc.

7.5 – Adquisición de evidencias
La “escena del crimen”

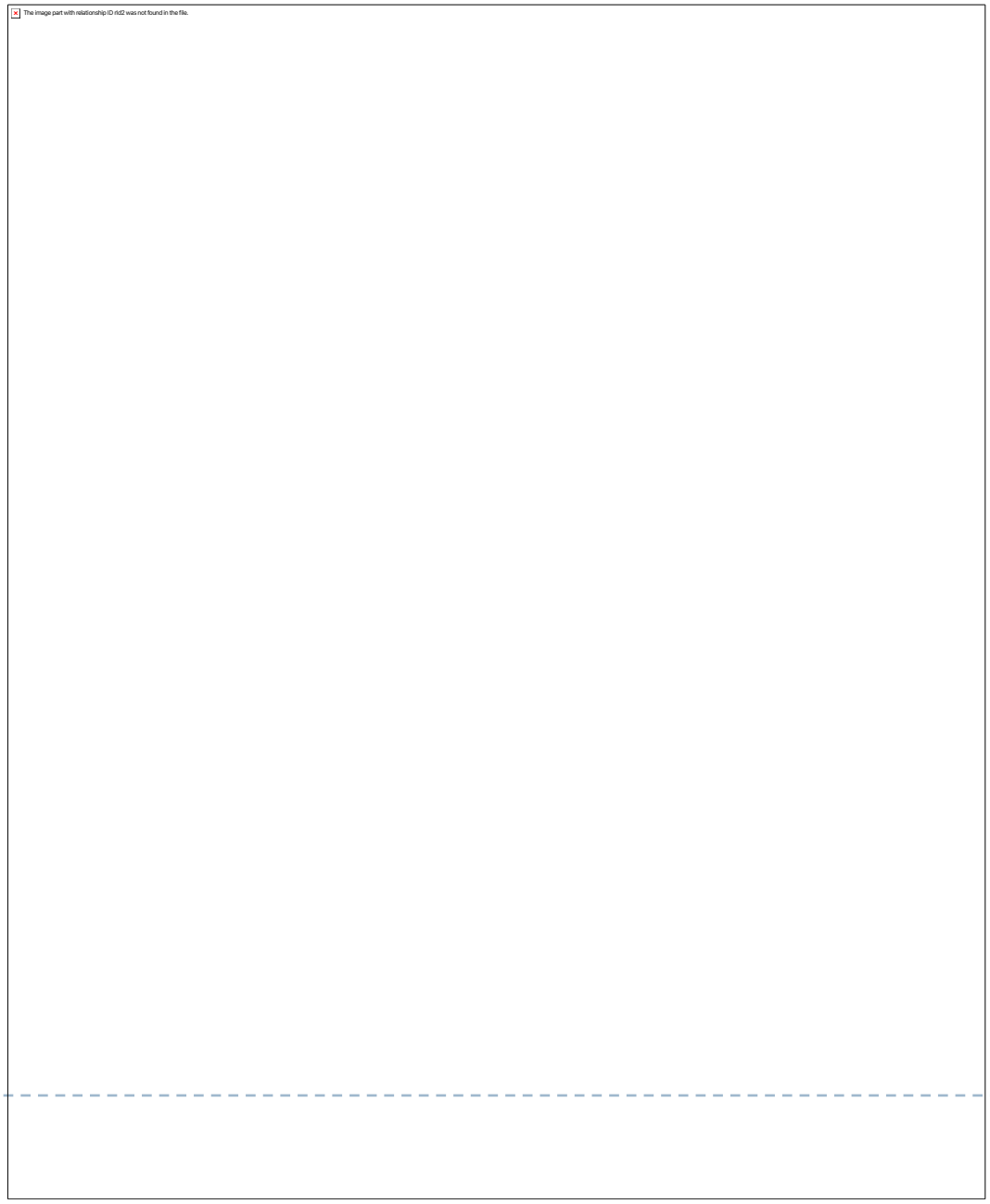
- Las siguientes acciones se realizan habitualmente mientras se investiga la "escena del crimen"
  - Identificar el número y tipo de ordenadores
  - Determinar si hay una red presente
  - Entrevistar al administrador de sistemas y los usuarios
  - Identificar y documentar los tipos y volúmenes de datos, incluyendo medios extraíbles
  - Identificar áreas de almacenamiento externo
  - Identificar software propietario
  - Etc.

7.5 – Adquisición de evidencias
Cadena de custodia

- Cada evidencia precisa de un documento de cadena de custodia
  - Evidencia inequívocamente identificada
  - Información sobre quién custodia la evidencia
  - Información sobre cada cambio de custodia (fecha, hora, personal involucrado)
- El documento de cadena de custodia debe estar siempre en el mismo lugar que la evidencia
- Este documento asegura la integridad de la evidencia como prueba ante procesos judiciales

7.5 – Adquisición de evidencias

Ejemplo de formulario



7.5 – Adquisición de evidencias
Orden de adquisición

- Basado en diferentes guías de recolección y archivo de evidencias electrónicas
  - RFC3227
- Orden de volatilidad
  - Registros y caché
  - Tabla de rutas y caché ARP
  - Memoria RAM de la máquina
  - Directorios temporales del sistema de archivos
  - Disco físico
  - Etc.
- La pregunta del millón: ¿cuándo hay que apagar una máquina?

7.5 – Adquisición de evidencias
Offline vs Live

- Adquisición de tipo "Offline"
  - Evita cambios debido al uso normal del equipo
    - Apagar el equipo, sacar el disco y colocarlo en una estación forense
  - Utilizar un dispositivo hardware / software para bloquear las escrituras (sólo lectura) antes de crear la imagen
- Adquisición de tipo "Live" (en caliente)
  - Cuando no se puede apagar el equipo, por ejemplo:
    - El equipo utiliza encriptación de disco y no se tiene acceso a las claves necesarias para descifrar
    - Se debe mantener el servicio por motivos de negocio
    - No se quiere apagar el equipo para no modificar el comportamiento de un proceso malicioso
    - No se quieren perder datos volatiles

7.5 – Adquisición de evidencias
Buenas prácticas en la preservación

- Documentar el hardware / software utilizados
- Abrir el ordenador para tener acceso físico a los discos
  - Protegerlos de electricidad estática y campos magnéticos
  - Documentar esta acción y realizarla ante testigos
- Identificar los dispositivos de almacenamiento (internos o externos) que es necesario adquirir
- Documentar los dispositivos de almacenamiento internos y la configuración hardware del equipo
  - Estado del disco (marca, modelo, geometría, interfaz, etc.)
  - Componentes internos (tarjetas de sonido, gráficas, de red, etc.)

7.5 – Adquisición de evidencias

Buenas prácticas en la preservación de los discos

- Comprobar si está encriptado antes de apagar el equipo (se recomienda adquirir en caliente, live)
- Desconectar para prevenir la destrucción o alteración de los datos
- Realizar la adquisición utilizando el equipo del examinador
- Es aconsejable el uso de dispositivos de protección de escritura para evitar modificar el disco original
- El disco destino debe estar "limpio" en términos forenses
  - Disco nuevo recién estrenado
  - Disco utilizado formateado indicando el procedimiento

7.5 – Adquisición de evidencias
Buenas prácticas en la preservación de los discos

- Es recomendable garantizar la integridad de la evidencia original antes de adquirirla
  - Cálculo de un hash del disco (p.ej. SHA1)
- Adquirir la evidencia utilizando software o hardware testeado y verificar la adquisición
  - Realizar la copia asegurando copiar los archivos borrados y los file slack
  - Comparación del hash original respecto al de la copia
- Cifrar las imágenes forenses para garantizar la confidencialidad y establecer la cadena de custodia correcta para la imagen
- Investigar **siempre** sobre las copias

7.5 – Adquisición de evidencias
Imagen de un disco (clon)

- Es una copia "bit a bit" de un disco completo o de una partición del mismo
  - Es una instantánea estática (snapshot) del contenido del disco en un momento determinado
  - No se copian ficheros, se copian bloques del disco
    - Ficheros accesibles actualmente
    - Espacio slack (espacio no utilizado de un clúster)
    - Espacio no asignado
      - Archivos borrados, fragmentos de ficheros, datos ocultos
  - Preservan el estado del disco en un momento determinado
    - Es importante utilizar correctamente las técnicas de adquisición para no invalidar la evidencia

7.5 – Adquisición de evidencias
Imagen forense

- Ficheros que contienen una imagen de disco
  - Ex, DD, ISO, RAW
  - Sin compresión: mismo tamaño que la fuente original
  - Compresas: para ahorrar espacio
  - Divididas (split imágenes): para facilitar el transporte
  - Empotradas: contienen metadatos sobre la imagen
    - Sello de tiempo con la fecha de creación de la imagen
    - Hash criptográfico que sirve como huella dactilar de la imagen
- No es lo mismo que un clon
  - Un clon es un duplicado exacto bit-a-bit en otro disco
  - Para realizar un clon se necesita
    - Mismo tipo de disco duro (tipo, tamaño, sectores, …)
    - Disco wipeado (todos los bits a 0 para evitar contaminaciones)

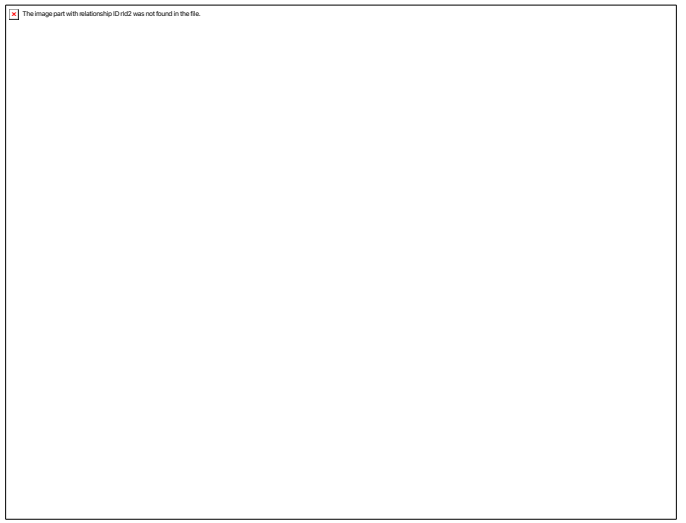
7.5 – Adquisición de evidencias
Laboratorio forense

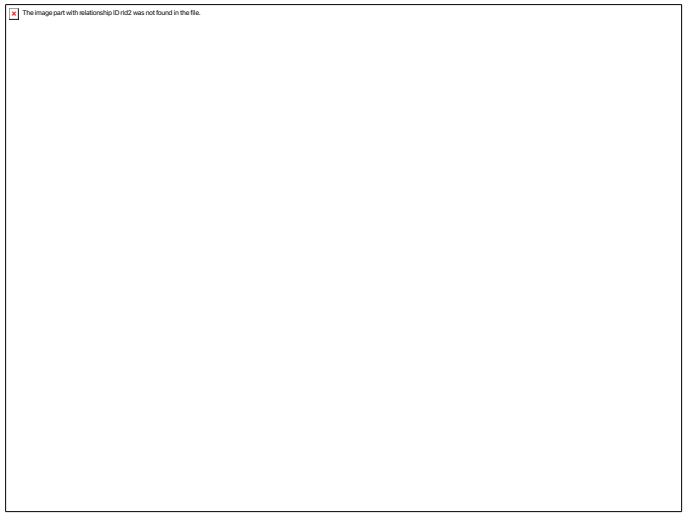
- Algunas de las características de un laboratorio forense son
  - Tamaño y ubicación en función del volumen de trabajo y el tipo de evidencias que se tratarán
  - Lugar seguro con vigilancia y, a ser posible, con una única entrada
    - Se registrarán los accesos al laboratorio, a las evidencias, el material informático que entra y sale, etc.
  - Sistemas de seguridad (cajas fuertes, alarmas, etc.), protección contra incendios y falta de electricidad (UPS)
  - Áreas de trabajo sin exposición al exterior (ventanas)
  - Estaciones de trabajo offline para análisis de evidencias
  - Estaciones de trabajo online para consulta de documentación

7.5 – Adquisición de evidencias

Material forense

- Hardware
  - Cables y discos duros
  - Tarjetas gráficas
  - Adaptadores o docks
  - Etc.
- Software
  - Diferentes SO
  - Software forense
    - Comercial: EnCase
    - Código abierto: SIFT, CAINE, etc.
  - Software ofimático (por informes)
  - Etc.





7.5 – Adquisición de evidencias
Requisitos de las herramientas

- Algunas de las características que debería cumplir una herramienta o entorno forense son:
  - Preservación de evidencias
    - Bloqueo lógico de escritura en los discos originales
    - Soporte de formatos RAW, Encase EWF, AFF, etc.
    - Trazabilidad (cadena de custodia)
    - Cálculo de hash criptográficos
  - Reducción y selección de datos rápida
    - Detección de firmas de archivos
    - Filtros avanzados y motor de búsqueda

7.5 – Adquisición de evidencias
Requisitos de las herramientas

- Reconstrucción de volúmenes y sistemas de archivos
  - Detección y montaje de particiones
  - Soporte de formato VMDK
  - Soporte de FAT12 / 16/32 (USB)
  - Soporte de NTFS con ADS y compresión (Windows)
  - Soporte de HFS, HFS + y HFSX (OS X, iPhone)
  - Soporte de Ext2 / 3/4 (GNU Linux, Android)
- Análisis multimedia
  - Visualización de galerías de fotografías
  - Extracción de miniaturas de vídeos
  - Extracción de metadatos EXIF

7.5 – Adquisición de evidencias
Requisitos de las herramientas

- Análisis de artefactos Linux/Windows
  - Ficheros
  - Archivos
  - Registros
  - Buzones (p.e., PST en Outlook)
- Análisis de memoria
  - http://www.primalsecurity.net/memory-forensics/
  - Volatility Framework, https://www.volatilityfoundation.org
  - Rekall, http://www.rekall-forensic.com
  - Reconstrucción gráfica de procesos: pstree, psxview,
  - Información de procesos: procdump
- Análisis de documentos
  - Visualizadores dedicados: PDF, Texto, Web, etc.
  - Extracción de metadatos, texto e imágenes en documentos ofimáticos

7.5 – Adquisición de evidencias
Forensic Live CD

- SIFT (SANS Investigative Forensic Toolkit)
  - https://digital-forensics.sans.org
  - v3.0 – Ubuntu 14.04 LTS x64
- CAINE (Computer Aided INvestigative Environment)
  - https://www.caine-live.net
  - v7.0 "DeepSpace" – Ubuntu 14.04.1 x64
- DEFT (Digital Evidence & Forensics Toolkit)
  - http://na.mirror.garr.it/mirrors/deft/
  - ZERO RC1 –Lubuntu 14.04.02 LTS
- WinFE (Windows Forensics Environment)
  - https://winfe.wordpress.com/
- BitCurator (University of North Carolina)
  - http://bitcurator.net
  - v1.5.12 – Ubuntu x64

Tema 7. Índice

7.5.1 – Artefactos Windows
Directorio del sistema

- La ubicación del directorio del sistema depende de la versión del SO
- Habitualmente el disco del sistema suele tener asignada la letra `c:` (variable `%HOMEDRIVE%`)

Directorio de Sistema	Sistema Operativo
`%HOMEDRIVE%\WINNT`	Windows NT Windows 2000
`%HOMEDRIVE%\Windows`	Windows 95/98/ME Windows XP/2003 Windows Vista Windows 7 Windows 2008 Windows 8/8.1 Windows 2012 Windows 10

7.5.1 – Artefactos Windows
Directorio del perfil del usuario

- La ubicación del directorio del perfil del usuario también depende de la versión del SO
- Variable `%USERPROFILE%`)

Directorio del perfil del usuario	**Sistema Operativo**
N/A	Windows 95/98/ME
%HOMEDRIVE%\WINNT\Profiles	Windows NT
%HOMEDRIVE%\Document and Settings	Windows 2000 Windows XP/2003
%HOMEDRIVE%\Users	Windows Vista Windows 7 Windows 2008 Windows 8/8.1 Windows 2012 Windows 10

7.5.1 – Artefactos Windows
User Shell Folders

- Directorios especiales para cada usuario (y maquina)
  - Habitualmente en el directorio del perfil del usuario
  - Se puede cambiar su ubicación, definida en el registro
    - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`
  - Se pueden utilizar atajos para acceder
  - Algunos de los más importantes son:
    - Escritorio
    - Documentos
    - Local AppData
    - Favoritos (Accesos directos de Internet Explorer)
    - Descargas
    - AppData (Itinerancia)

7.5.1 – Artefactos Windows
Directorios interesantes

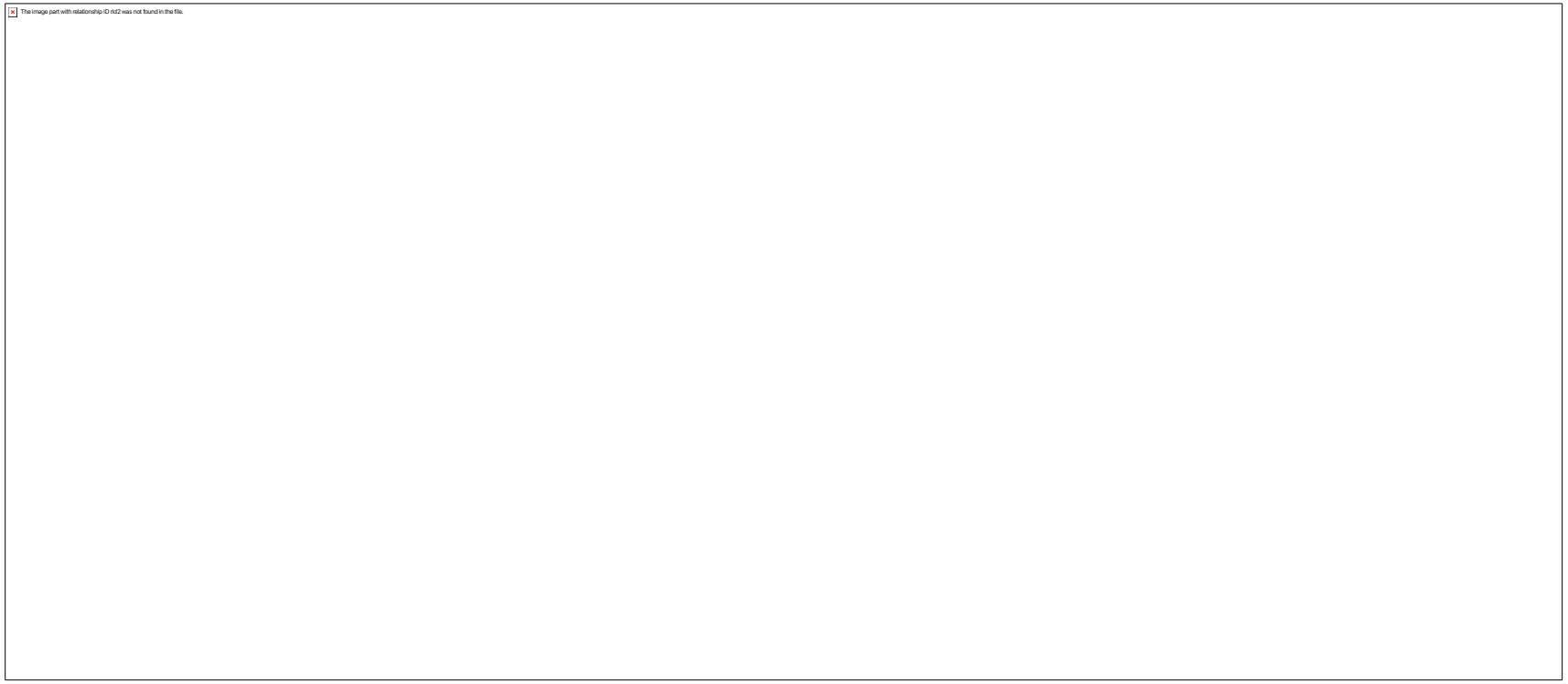
- Archivos recientes (Recent)
  - Cada vez que se abre un archivo, se crea un fichero LNK
    - `%APPDATA%\Microsoft\Windows\Recent`
- Directorio temporal
  - Utilizado por muchas aplicaciones e instaladores
  - Suelen quedar "restos" que se pueden analizar
    - `%LOCALAPPDATA%\Temp`
- Directorios utilizados por los browser
  - Preferidos
  - Histórico de navegación
  - Cookies
- Papelera

7.5.1 – Artefactos Windows
Accesos directos (LNK)

- File Shortcuts o Shell Links
  - Ficheros que apuntan a archivos locales o remotos
  - Creados por el usuario o instaladores (habitualmente)
  - Creados automáticamente al abrir un archivo
    - El listado de "archivos recientes" utiliza este tipo de enlaces
- Permiten conocer los detalles del archivo original
  - Carpeta original donde se encuentra el archivo
  - Fechas de acceso o marcas de tiempo
  - Información del volumen, número de serie, nombre NetBIOS y dirección MAC del ordenador donde se encuentra
  - Detalles de red si es un archivo remoto
  - Tamaño del archivo

7.5.1 – Artefactos Windows
Ejemplo de LNK

- Acceso reciente a documentos/ficheros
  - `%APPDATA%\Microsoft\Windows\Recent`
  - `C:\Users\<usuari>\AppData\Roaming`



7.5.1 – Artefactos Windows
Papelera

- Es el lugar donde se almacenan temporalmente los archivos eliminados
  - Es posible eliminar un archivo de forma "permanente" (sin que pase por la papelera de reciclaje) utilizando la combinación de teclas Mayús+Supr
  - Se puede configurar Windows para que no use la papelera de reciclaje
  - La ubicación real de la papelera depende de la versión de Windows que se está utilizando

Versión de Windows	**Ubicación**
Windows 95/98/ME (FAT32)	`X:\RECYCLED`
Windows NT/2000/XP (NTFS)	`X:\RECYCLER\%SID%`
Windows Vista/7+ (NTFS)	`X:\$Recycle.Bin\%SID%`

7.5.1 – Artefactos Windows
Papelera X:\RECYCLER (Windows NT/2000/XP)

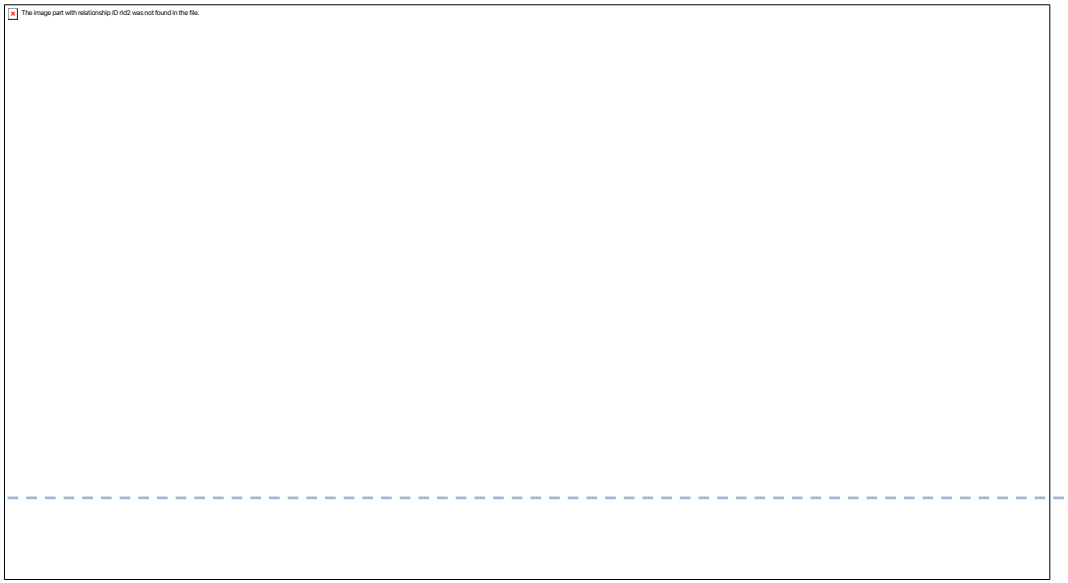
- Cuando se borra un archivo
  - Se borra la entrada correspondiente a la $MFT
    - Master File Table: descripción de todos los archivos en un volumen
  - Se crea una nueva entrada para la papelera a la $MFT
    - `D<letra><índice>.<Extensiónoriginal>`
  - Añade información del borrado al archivo INFO2
    - Nombre del fichero original (path)
    - Data y hora del borrado
    - Tamaño
    - Se puede analizar el contenido de INFO2 con programa específicos como Rifiuti2 de Intel/McAfee
- Cuando se recupera un archivo
  - La entrada de la $MFT de la papelera se marca como borrada
  - No se modifica INFO2. Se cambia el primer carácter a 00X

7.5.1 – Artefactos Windows
Papelera X:\RECYCLED (Windows 95/98/ME)

- Aunque permitía tener múltiples perfiles de usuario, todo era compartido entre todos
  - Cada usuario podía acceder a cualquier fichero
  - Incluido modificaciones de bajo nivel (boot sectors, hard drive, etc.)
- De forma que solo había una papelera compartida entre todos los perfiles
  - Parecido a Windows NT/2000/XP
  - Añade información del borrado al archivo INFO (versión anterior de INFO2)
    - Donde se almacena la información del fichero original para poder recuperarlo

7.5.1 – Artefactos Windows
Papelera $Recycle.Bin (Windows Vista)

- Cambio en la papelera a partir de Windows Vista
- Los ficheros de almacena en un directorio por usuario según su SID
  - X:\$Recycle.Bin\%SID%
- Se crean 2 ficheros para cada archivo eliminado
  - Los datos originales en un fichero $R<ID>
  - Los metadatos del archivo eliminado en un fichero $I<ID>



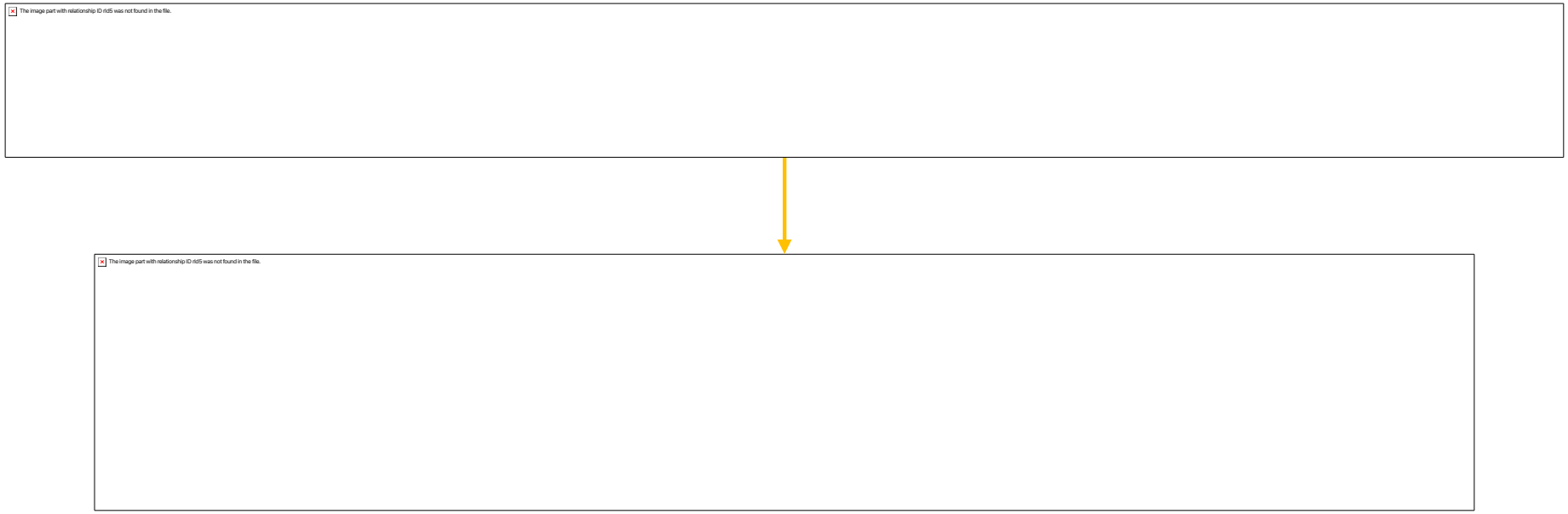
7.5.1 – Artefactos Windows
Ficheros Prefetch

- El prefetching de aplicaciones se utiliza para mejorar el rendimiento del SO desde Windows XP
- El sistema de monitorización de la cache de Windows escribe a disco ciertas características de las aplicaciones ejecutadas
  - Directorio protegido `%SystemRoot%\Prefetch`
  - Se crean ficheros con la nomenclatura
    - `<Nombredelbinario>-<hashruta>.pf`
  - Cada binario ejecutado desde rutas diferentes tendrá ficheros PF diferentes
  - Antiguamente el número de ficheros PF estaba limitado a 128
  - Se pueden utilizar para saber si se ha ejecutado un programa que ya no está instalado o ha sido borrado

7.5.1 – Artefactos Windows

Ficheros Prefetch

- Se puede analizar utilizando herramientas como
  - Windows File Analizer, http://mitec.cz/wfa.html
  - NirSoft WInPrefetchView, http://www.nirsoft.net/
  - TZWorks Windows Prefetch Parser, https://tzworks.net/prototypes.php



7.5.1 – Artefactos Windows
Cola de impresión

- Las tareas de impresión se guardan en el directorio
  - `%SystemRoot%\spool\PRINTERS`
- Dos archivos temporales para cada tarea:
  - Archivo * .shd (Shadow)
    - Usuario, impresora, archivo, modo de impresión
  - Archivo * .spl (Spool)
    - Información gráfica de la tarea a imprimir
- Modos de impresión: RAW, EMF (defecto)
  - EMF (Microsoft Enhanced Metafile)
  - Permite impresión avanzada (p.e., panfleto)
- SPLViewer
  - Visualiza, imprime y guarda archivos de la cola

7.5.1 – Artefactos Windows
Volume Shadow Copy (VSC)

- Tecnología de Microsoft que permite realizar copias de seguridad de archivos y volúmenes en uso
- Se incluye por defecto a partir de Windows Vista / 7
- Se realizan copias de tipo instantánea (snapshot):
  - Permite realizar copias totales o incrementales
  - Trabaja a nivel de bloque realizando una copia de seguridad si éste se verá modificado en una escritura
  - Es posible obtener versiones previas de un archivo, directorio o volumen a partir de una VSC
- Se pueden analizar
  - Online mediante el comando `vssadmin.exe`
  - Desde imágenes forenses utilizando herramientas especializadas

7.5.1 – Artefactos Windows
Registro de eventos

- Los registros de eventos son archivos locales en los que se registran los diferentes eventos que se producen en el sistema operativo
  - Se accede, se borra o se añade un archivo o una aplicación
  - Se modifica la fecha o se apaga el sistema
  - Se cambia la configuración del sistema
  - Etc.

7.5.1 – Artefactos Windows

Ficheros de registro de eventos

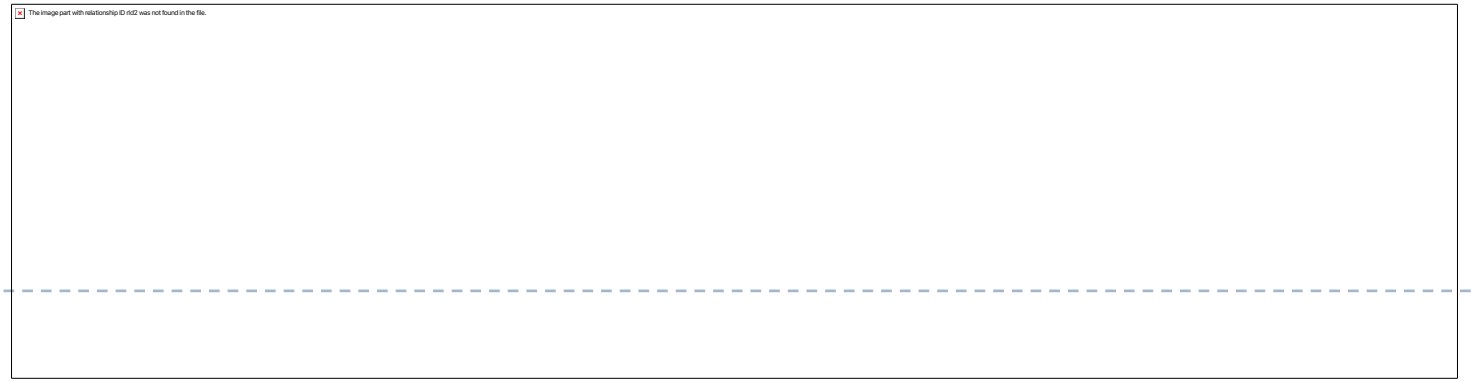
Antes de Windows Vista	Desde Windows Vista
`C:\Windows\System32\config`	`C:\Windows\System32\winevt\Logs`

- EventLog
  - Sistema
  - Seguridad
  - Aplicación
- Formato binario (*.evt)

- Windows EventLog
  - Sistema
  - Seguridad
  - Aplicación
  - + 200 archivos más
- Formato binario/XML (*.evtx)

7.5.1 – Artefactos Windows
Registro de Windows

- El registro es la evolución de los archivos * .ini y se introdujo por primera vez en Windows 95
- Se trata de una base de datos en la que las aplicaciones y componentes del sistema almacenan y recuperan datos de configuración
- Los datos almacenados en el registro varían según la versión de Windows
- Los datos se encuentras estructuradas en árbol
  - Cada nodo del árbol se denomina clave
  - Cada clave puede contener subclaves y datos, llamadas valores



7.5.1 – Artefactos Windows
Claves predefinidas

- El registro tiene 5 claves predefinidas

Handle	Descripción
`HKEY_CLASSES_ROOT`	Tipo (o clase) de documentos y las propiedades asociadas
`HKEY_CURRENT_CONFIG`	Información sobre el perfil de hardware actual del ordenador local. Es un alias de: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current`
`HKEY_CURRENT_USER`	Preferencias del usuario actual (que ha iniciado sesión). Es un alias de: `HKEY_USERS\<SID>`
`HKEY_LOCAL_MACHINE`	Define el estado físico del ordenador, memoria, software instalado, etc...
`HKEY_USERS`	Define la configuración por defecto para los usuarios (`HKEY_USERS\.DEFAULT`)

7.5.1 – Artefactos Windows

Claves de interés

- Nombre del ordenador
  - `SYSTEM\ControlSet00x\Control\ComputerName\ComputerName`
- BIOS (Fabricante, Modelo del equipo, versión, etc.)
  - `HARDWARE\DESCRIPTION\System\BIOS`
- Procesadores (Nombre, Fabricante, Velocidad, etc.)
  - `HARDWARE\DESCRIPTION\System\CentralProcessor`
- Hora del último cierre
  - `SYSTEM\ControlSet00x\Control\Windows`
    - Valor "ShutdownTime"
- Programas de inicio
  - `SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

7.5.1 – Artefactos Windows

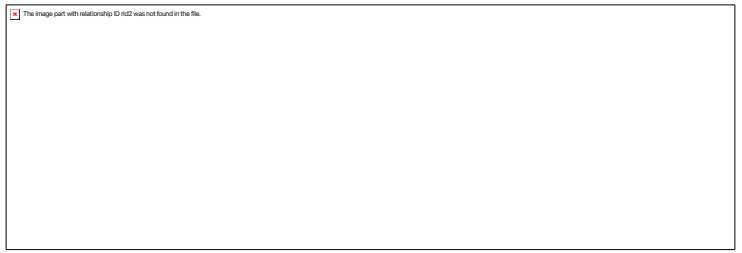
Claves de interés

- Aplicaciones registradas
  - `SOFTWARE\RegisteredApplications`
- Tarjetas de red
  - `SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkCards`
- Redes de la Intranet (a las que se ha connectado)
  - `SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Nla\Cache\Intranet`
- Redes Wireless (identificadores)
  - `SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Nla\Wireless`
- Perfiles de red (data de creación, conexión, etc.)
  - `SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles`

7.5.1 – Artefactos Windows

Claves de interés

- Impresoras
  - `SYSTEM\ControlSet001\Control\Print\Printers`
    - El valor "PrinterDriverData" tiene información sobre el modelo, el driver y la data de instalación
- Dispositivos USB
  - `SYSTEM\ControlSet001\Enum\USBSTOR`
    - Cada vez que se conecta un dispositivo USB se registra información que permite identificarlo de forma univoca (fabricante, ID producto, número de serie, etc.)



- Histórico
  - Clave "MRU", "Recent", etc. de diferentes programas
    - Lista de URL introducidas en Internet Explorer
    - Archivos reciente de Word, Excel, Acrobat, etc.
    - Unidad de red mapeadas recientemente
    - Comandos ejecutados recientemente, etc.

7.5.1 – Artefactos Windows
Otros ficheros de registro

- Windows guarda información en ficheros de registro que puede ser útil analizar

Fichero	Descripción
setupact.log	Acciones que se han producido durante la instalación del sistema: hardware, ficheros, etc.
setupapi.*.log	Instalaciones, actualizaciones y dispositivos conectados (USB, discos externos, etc.)
netsetup.log	Unión a un dominio o grupo de trabajo (Dominio, cuentas utilizadas, etc.)
pfirewall.log	Registro de paquetes aceptados/descartados por el firewall de Windows (es necesario tenerlo habilitado)
mrt.log	Registro de la herramienta Malicious Software Removal Tool (encargada de eliminar amenazas concretas)
cbs.log	Registro del gestor de paquetes de Windows

7.5.1 – Artefactos Windows
Fichero SAM

- SAM (Security Account Manager) es una base de datos con los hash de las contraseñas y los usuarios
  - LM Hash
  - NTLM Hash (a partir de NT 3.1)
- Se encuentra en `%windir%\System32\config`
- No se puede acceder al fichero SAM en un sistema en caliente, es necesario hacerlo offline
  - Utilizar `bkhive` para volcar la base de datos
    - `bkhive system /tmp/hive.txt`
  - Y `samdump2` para volcar los hash
    - `samdump2 SAM /tmp/hive.txt > /tmp/hash.txt`
  - Utilizar John the Ripper, https://www.openwall.com/john/
    - `john /tmp/hive.txt --users=Administrator`

7.5.1 – Artefactos Windows
NTFS ADS

- NTFS permite almacenar información adicional para cada fichero (metadatos)
  - A partir de NT 3.1 para proporcionar compatibilidad con el HFS (Hierarchical File System) de Apple
  - Se llama Alternate Data Stream (ADS)
  - Esta información adicional son ficheros ocultos enlazados con el archivo original (que no altera su formato o contenido)
- Características
  - No hay limitaciones de tamaño a los streams
  - Puede haber más de un stream enlazado a un archivo
  - Los ADS no son visibles en el Explorador o en el interprete de comandos
  - Los streams también se pueden enlazar a directorios y unidades de disco
  - El contenido puede ser binario (JPG, ejecutable, etc.)
  - No se pueden transferir utilizando protocolos de Internet (HTTP, SMTP, etc.)
  - Pero se pueden transferir a través de la LAN si el disco de destino se NTFS

7.5.1 – Artefactos Windows
¿Qué más buscar?

- Directorios con nombres que empiezan con un punto
  - Suelen ser directores que mantienen parámetros de configuración, información sobre la instalación
- Archivos modificados recientemente
- Archivos grandes

Tema 7. Índice

7.5.2 – Artefactos Linux

Jerarquía del sistema de ficheros

- FHS (Filesystem Hierarchy Standard)
  - https://wiki.linuxfoundation.org/lsb/fhs-30
  - 3.0 Juny 2015

Directorio	Uso
`/bin`	Binarios esenciales del sistema
`/boot`	Ficheros de arranque
`/dev`	Dispositivos
`/etc`	Ficheros de configuración
`/home`	Ficheros de usuarios
`/lib`	Librerías esenciales y módulos del kernel
`/media`	Montaje de dispositivos (automontaje)
`/mnt`	Puntos de montaje temporales (montaje manual)
`/opt`	Aplicaciones fuera de los paquetes de la distribución
`/root`	Home del usuario root
`/sbin`	Binarios del sistema
`/tmp`	Ficheros temporales
`/usr`	Compartición de información
`/var`	Datos variables, de administración, logs, etc...

7.5.2 – Artefactos Linux
Que se suele mirar

- `/etc`
  - Equivalente a `%SystemRoot%\System32\config`
  - Directorio principal de configuración del sistema
  - Archivos y directorios de configuración independientes para cada aplicación
- `/var/log`
  - Equivalente al Registro de Eventos de Windows
  - Registros de seguridad, aplicación, etc.
  - Los registros se guardan durante 4-5 semanas
- `/home/$USER`
- Equivalente a `%USERPROFILE%`
  - Los datos y la información de configuración del usuario

7.5.2 – Artefactos Linux

Información del sistema

Fichero	Información
`/etc/*-release`	Nombre de la distribución Linux y su versión
`/etc/hostname`	Nombre del ordenador (también se puede encontrar en los ficheros de `/var/log`)
`/etc/host`	Dirección IP (asignación estática)
`/var/lib/dhclient` `/var/log/*`	Dirección IP (DHCP)
`/etc/localtime`	Almacena datos de la zona horario por defecto • Ficheros binarios, hay que usar `zdump` • Buscar en `/usr/share/zoneinfo`
`/etc/passwd`	Información básica de los usuarios. Las cuentas con UID=0 tienen permisos de 'root'
`/etc/shadow`	Hash MD5 de las contraseñas (se puede usar John the Ripper)

7.5.2 – Artefactos Linux
Información del sistema

Fichero	Información
`/etc/sudoers`	Puede indicar los usuarios con permiso root
`/etc/group`	Pertenencia a grupos
`/var/log/wtmp`	Muestra información acerca del usuario, su origen, la hora y durada de una sesión. Hay que usar el comando `last` para verlo
`/var/log/btmp` `/var/log/faillog`	Información sobre los intentos fallados de acceso (`last -f /var/log/btmp | more`)
`/var/log/auth.log` `/var/log/secure`	Información de autorización del sistema, incluido los inicios de sesión de los usuarios, los que no han tenido éxito y el mecanismo de autentificación que se utiliza
`/var/log/daemon.log`	Mantiene información sobre los servicios en ejecución en background

7.5.2 – Artefactos Linux
Información del sistema

Fichero	Información
`/home/<user>`	La localización más común para las carpetas y ficheros de los usuarios
`/root`	El directorio del usuario root
`/home/.*`	Los ficheros y directorios "ocultos" empiezan por un punto • Contienen información de configuración específica de las aplicaciones • En algunos casos se ejecutan al iniciar sesión • Es un posible backdoor o mecanismo de persistencia

7.5.2 – Artefactos Linux
Navegadores en Linux

- Firefox y Chrome son los más comunes en Linux
- Los formatos de los ficheros son idénticos que en Windows
  - Base de datos en SQLite
- Los ficheros suelen estar en los directorios de los usuarios
  - Firefox: `$HOME/.mozilla/firefox/*.default`
  - Chrome: `$HOME/.config/chromium/Default`

7.5.2 – Artefactos Linux

Nautilus

- Es el explorador grafico de ficheros en Linux, similar a Explorer de Windows
- Miniaturas
  - `$HOME/.thumbnails`
- Ficheros recientes
  - `$HOME/.recently-used.xbel`

7.5.2 – Artefactos Linux

Históricos de comandos

- Los comandos ejecutadas por el usuario se guardan en `$HOME/.bash_history`
- Desafortunadamente, es un archivo sin marcas de tiempo
- Puede ser modificado o borrado por el propio usuario
- El histórico de comandos `sudo` se puede encontrar mirando los archivos
  - `/var/log/auth.log`
  - `/var/log/sudo.log`

7.5.2 – Artefactos Linux
Secure Shell

- SSH es un protocolo de red cifrado que permite iniciar sesión de forma remota y transferir ficheros
- Los ficheros más interesantes para investigar están en `$HOME/.ssh`
  - `known_hosts`: maquinas remotas a la que los usuarios se han conectados
  - `authorized_keys`: claves publicas para la conexión con maquinas remotas
  - `id_rsa`: claves privadas utilizadas para iniciar sesión en otras maquinas sin utilizar una contraseña

7.5.2 – Artefactos Linux
¿Qué más buscar?

- Archivos con el `setuid` activo
  - Permite a un usuario ejecutar un programa con permisos del propietario o del grupo
- Directorios con nombres que empiezan con un punto
- Archivos normales en el directorio `/dev`
- Archivos modificados recientemente
- Archivos grandes

Seguretat Informàtica (SI)

Tema 7. Análisis forense

Davide Careglio

Fuentes: Jordi Nin, "Network Security", Computer Security, 2014
Ton Rodriguez, "Anàlisi forense", Computer Security, 2018