www.eysglobal.com

CURSO DE INFORMÁTICA FORENSE

Instructor: Juan Esteban Tapias

MÓDULO 3
PARTE
1
RECUPERACIÓN DE EVIDENCIA

EVIDENCIAS DIGITALES

INFORMÁTICA FORENSE

Propiedades de la evidencia digital

A principios del siglo XXI, más de la mitad de los casos penales involucró un dispositivo informático de alguna descripción, y la tendencia ha continuado y es probable que aumente.

INFORMÁTICA FORENSE

Propiedades de la evidencia digital

- *Definir evidencia digital y su uso*
- *Explicar las propiedades especiales de la evidencia digital, incluido su tiempo y metadatos de ubicación y características del archivo*
- *Resaltar las complejidades técnicas de la evidencia digital y los desafíos para análisis de sonido*
- *Explicar los requisitos para determinar la admisibilidad de evidencia digital.*

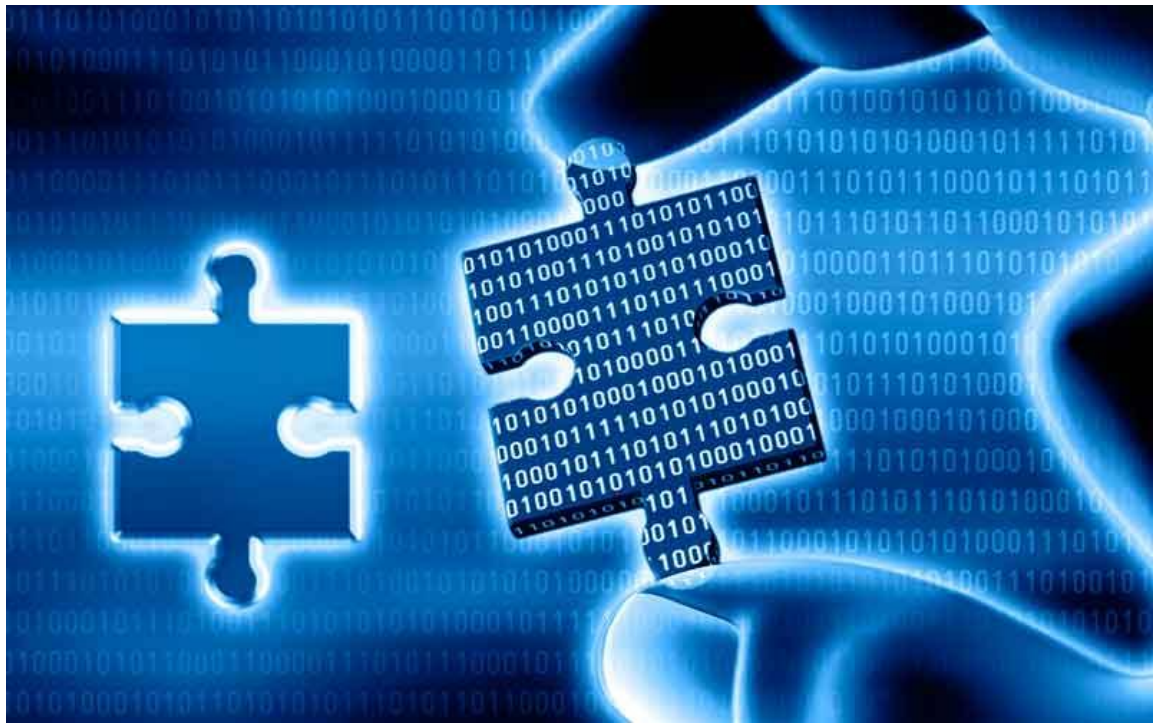
INFORMÁTICA FORENSE

Definición de evidencia digital

La evidencia digital es información en forma digital que se encuentra en una amplia gama de dispositivos; de hecho, es cualquier cosa que tenga un microchip o haya sido procesada por una y luego se almacena en otros medios.

INFORMÁTICA FORENSE

Definición de evidencia digital



Las pruebas presentadas en casos legales, como juicios penales, se clasifican como testigos.
testimonio o evidencia directa, o evidencia indirecta en la forma de un objeto, tal
como documentos físicos, la propiedad de personas, etc.

INFORMÁTICA FORENSE

El uso de evidencia digital

La evidencia en casos legales se usa para probar (o refutar) hechos que también están en disputa como prueba de la plausibilidad de los mismos, en particular, la evidencia circunstancial o evidencia indirecta.

INFORMÁTICA FORENSE

El uso de evidencia digital

La evidencia digital puede tomar muchas formas dependiendo de las circunstancias de cada caso y los dispositivos de los que se recuperan las pruebas.

INFORMÁTICA FORENSE

El uso de evidencia digital

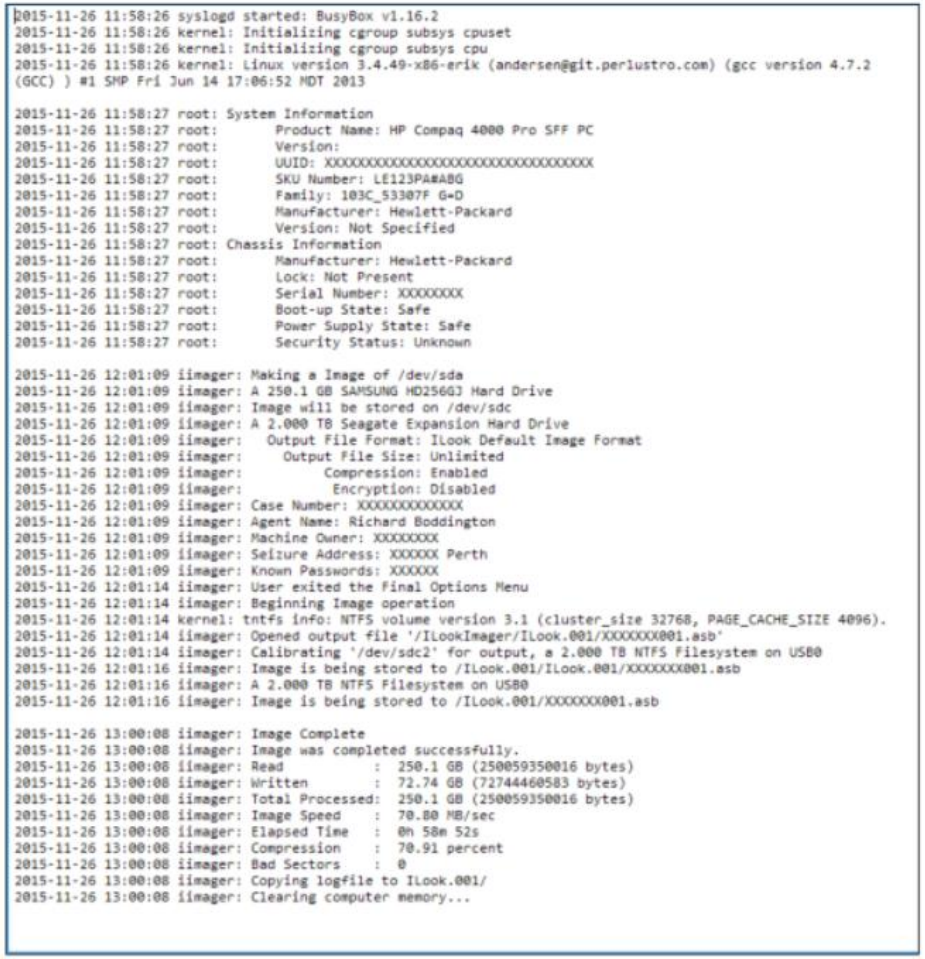
Name	Date modified	Type	Size
Suspect	26/11/2015 10:12 ...	Text Document	90 KB
Suspect001.asb	26/11/2015 10:12 ...	ASB File	154,327,10...

El proceso de obtención de imágenes está destinado a copiar todos los bloques de datos del sospechoso al el dispositivo objetivo. Esto a veces se denomina copia física de todos los datos, a diferencia de una copia lógica, que solo copiará lo que un usuario normalmente ve. La siguiente captura de pantalla muestra un contenedor de imágenes forenses .ASB producido por IXImager, que contiene un registro cifrado y un archivo de imagen.

INFORMÁTICA FORENSE

El uso de evidencia digital

La ventaja de poder hacer una copia exacta de los datos es que se pueden copiar y el dispositivo original puede devolverse al propietario o almacenarse para su prueba sin normalmente tiene que ser examinado repetidamente

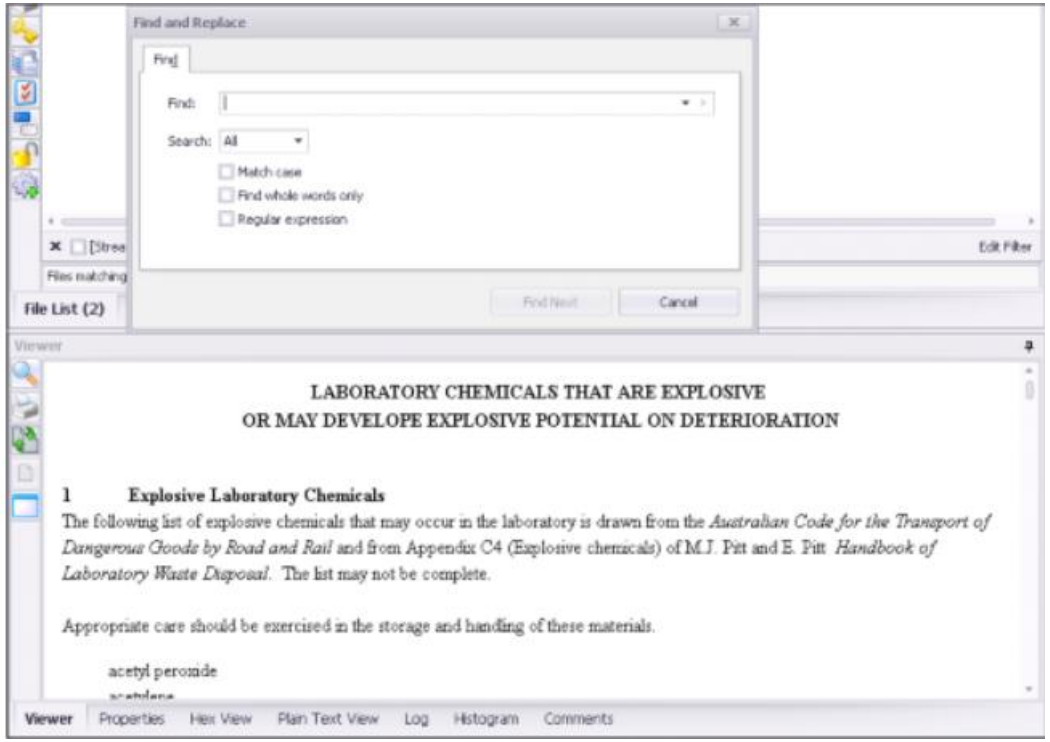


```
2015-11-26 11:58:26 syslogd started: BusyBox v1.16.2
2015-11-26 11:58:26 kernel: Initializing cgroup subsys cpuset
2015-11-26 11:58:26 kernel: Initializing cgroup subsys cpu
2015-11-26 11:58:26 kernel: Linux version 3.4.49-x86-erik (andersen@git.perlustro.com) (gcc version 4.7.2
(GCC) ) #1 SMP Fri Jun 14 17:06:52 MDT 2013

2015-11-26 11:58:27 root: System Information
2015-11-26 11:58:27 root:       Product Name: HP Compaq 4000 Pro SFF PC
2015-11-26 11:58:27 root:       Version:
2015-11-26 11:58:27 root:       UUID: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
2015-11-26 11:58:27 root:       SKU Number: LE123PA#ABG
2015-11-26 11:58:27 root:       Family: 103C_53307F G=D
2015-11-26 11:58:27 root:       Manufacturer: Hewlett-Packard
2015-11-26 11:58:27 root:       Version: Not Specified
2015-11-26 11:58:27 root: Chassis Information
2015-11-26 11:58:27 root:       Manufacturer: Hewlett-Packard
2015-11-26 11:58:27 root:       Lock: Not Present
2015-11-26 11:58:27 root:       Serial Number: XXXXXXXX
2015-11-26 11:58:27 root:       Boot-up State: Safe
2015-11-26 11:58:27 root:       Power Supply State: Safe
2015-11-26 11:58:27 root:       Security Status: Unknown

2015-11-26 12:01:09 iimager: Making a Image of /dev/sda
2015-11-26 12:01:09 iimager: A 250.1 GB SAMSUNG HD256GJ Hard Drive
2015-11-26 12:01:09 iimager: Image will be stored on /dev/sdc
2015-11-26 12:01:09 iimager: A 2.000 TB Seagate Expansion Hard Drive
2015-11-26 12:01:09 iimager:   Output File Format: ILook Default Image Format
2015-11-26 12:01:09 iimager:     Output File Size: Unlimited
2015-11-26 12:01:09 iimager:          Compression: Enabled
2015-11-26 12:01:09 iimager:           Encryption: Disabled
2015-11-26 12:01:09 iimager: Case Number: XXXXXXXXXXXX
2015-11-26 12:01:09 iimager: Agent Name: Richard Boddington
2015-11-26 12:01:09 iimager: Machine Owner: XXXXXXXX
2015-11-26 12:01:09 iimager: Seizure Address: XXXXXX Perth
2015-11-26 12:01:09 iimager: Known Passwords: XXXXXX
2015-11-26 12:01:14 iimager: User exited the Final Options Menu
2015-11-26 12:01:14 iimager: Beginning Image operation
2015-11-26 12:01:14 kernel: tntfs info: NTFS volume version 3.1 (cluster_size 32768, PAGE_CACHE_SIZE 4096).
2015-11-26 12:01:14 iimager: Opened output file '/ILookImager/ILook.001/XXXXXX001.asb'
2015-11-26 12:01:14 iimager: Calibrating '/dev/sdc2' for output, a 2.000 TB NTFS Filesystem on USB0
2015-11-26 12:01:16 iimager: Image is being stored to /ILook.001/ILook.001/XXXXXX001.asb
2015-11-26 12:01:16 iimager: A 2.000 TB NTFS Filesystem on USB0
2015-11-26 12:01:16 iimager: Image is being stored to /ILook.001/XXXXXX001.asb

2015-11-26 13:00:08 iimager: Image Complete
2015-11-26 13:00:08 iimager: Image was completed successfully.
2015-11-26 13:00:08 iimager: Read           :  250.1 GB (250059350016 bytes)
2015-11-26 13:00:08 iimager: Written        :  72.74 GB (72744460583 bytes)
2015-11-26 13:00:08 iimager: Total Processed:  250.1 GB (250059350016 bytes)
2015-11-26 13:00:08 iimager: Image Speed    :  70.80 MB/sec
2015-11-26 13:00:08 iimager: Elapsed Time   :  0h 58m 52s
2015-11-26 13:00:08 iimager: Compression    :  70.91 percent
2015-11-26 13:00:08 iimager: Bad Sectors    :  0
2015-11-26 13:00:08 iimager: Copying logfile to ILook.001/
2015-11-26 13:00:08 iimager: Clearing computer memory...
```

INFORMÁTICA FORENSE

El uso de evidencia digital

Se requieren herramientas forenses especiales para abrir y examinar los datos contenidos en una imagen, y lo hacen sin alterar la imagen y contaminar la evidencia, como una práctica forense sólida



INFORMÁTICA FORENSE

El uso de evidencia digital