ANÀLISI FORENSE : Pendrive + Cadena de custòdia

L’anàlisi forense i la cadena de custòdia són pràctiques fonamentals per obtenir proves, per garantir-ne la validesa en un context legal i per assegurar que les dades s'examinen de manera rigorosa i fiable.

Anàlisi Forense d'un pendrive

Implica l'examen detallat del dispositiu per recuperar dades i identificar possibles proves d'activitats il·legals o no autoritzades. El procés inclou:

1. Recollida: El pendrive s'ha de recollir de manera segura, evitant qualsevol alteració.
2. Imatge Forense: Es crea una còpia exacta del contingut del pendrive mitjançant eines d'anàlisi forense, assegurant que la còpia és intacta i que la informació original no es modifica.
3. Anàlisi: Es revisa el contingut de la imatge, incloent fitxers, documents, registres d'activitat i metadades per identificar informació rellevant.
4. Informe: Es documenta tot el procés i les troballes en un informe que pot ser utilitzat en procediments legals.

Cadena de Custòdia

És el registre documentat que segueix el camí de les proves des de la seva recollida fins a la seva presentació en un tribunal. Inclou:

1. Documentació Inicial: Detalls sobre la recollida del pendrive, incloent qui el va recollir, quan i on.
2. Identificació: Cada prova ha de tenir un identificador únic (número de prova) per garantir la seva traçabilitat.
3. Transparència: Cada transferència de custòdia ha d'estar documentada, incloent les signatures de les persones que controlen la prova.
4. Integritat: La prova ha de ser mantinguda en un entorn segur, amb un registre que demostri que no ha estat alterada o compromesa en cap moment.

ACTIVITATS

Passos a seguir per realitzar l'activitat:

1. Recollida de la prova
1.1. Omplir la cadena de custòdia
2. Generació de la imatge forense de la prova
3. Retorn de la prova
3.1. Omplir la cadena de custòdia
4. Anàlisi de la imatge forense
4.1. Redactar informe

1. Cerca de proves i documentació.

Et trobes en un local on hi ha indicis que s'hi realitzaven pràctiques fraudulentes. Concretament els propietaris del local són sospitosos d'extorsió i estafes electròniques fent-se passar per reconegudes entitats bancàries i organismes públics.

Número identificador del cas forense: 123

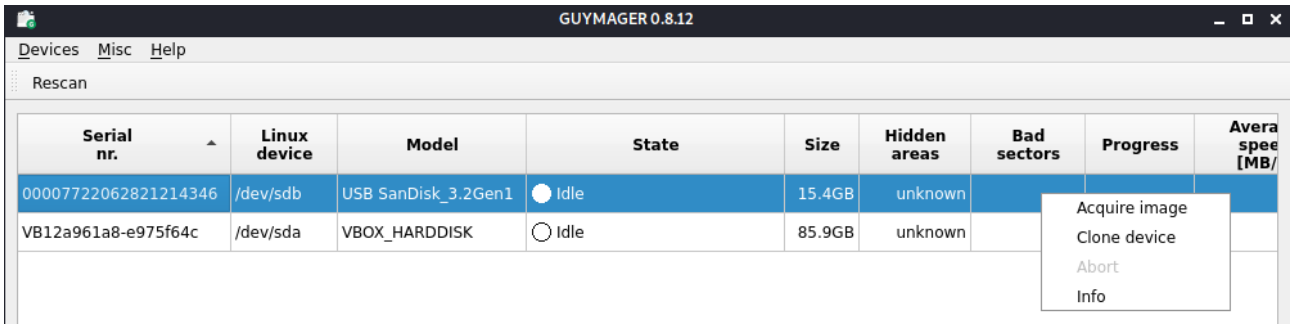
Amb l'objectiu d'obtenir dades rellevants per la investigació, se t'entrega un pendrive aparentment buit, extreu-ne les evidències ocultes i analitza-les.
Número identificador del pendrive com a possible font de proves: 0001

Per aquesta pràctica hauràs d'utilitzar les següents eines open source:

- **Guymager:** Generació d'imatges forenses.
- **Autopsy:** Anàlisi forense de sistemes i fitxers.

Pots instal·lar-los a la teva màquina virtual o usar Kali Linux que els incorpora com a part de la seva suite forense.
Per poder treballar amb el pendrive hauràs d'habilitar-ne l'accés USB a la teva VM per tal que així el capturi.

Primerament hem d’obtenir una imatge del pendrive per tal d’evitar treballar directament sobre el dispositiu en la recerca de proves.
Per això obrim Guymager com a root.
Generem una imatge del pendrive usant "Aquire image".

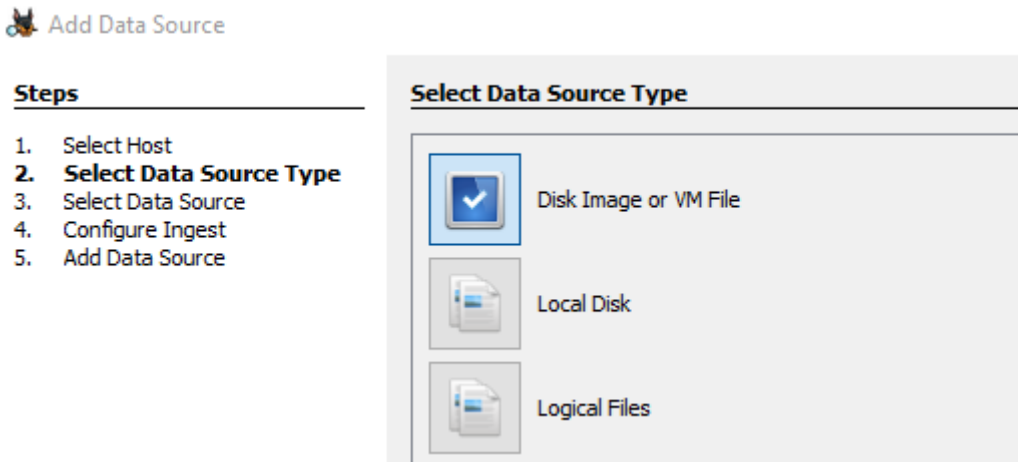


Per defecte, particionarà la imatge en fitxers d'extensió .EXX per cada bloc de 2047MB de dades. Per aquesta pràctica li serà suficient amb un arxiu.

Així que n’obtingueu l’imatge de treball i anoteu les característiques del pendrive l’heu de guardar en un lloc segur perquè no sigui alterat. En una investigació convencional, com a mesura de seguretat, s’hauria de fer una còpia de la imatge extreta, però per aquest exercici no serà necessari.

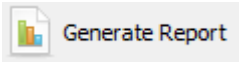
Versió i detalls de l’eina usada a través de "Help/About GUYMAGER".

Usant Autopsy extraurem el contingut de la imatge anteriorment creada.



Analitza els arxius recuperats.
Juntament amb aquest informe adjunta comprimits els arxius que consideris indicatius de delicte o que puguin aportar informació rellevant. Per cada arxiu omple un document com el de la «Figura 2».

Pots obtenir informació del programa generant-ne un informe.



Redacta un informe omplint un document com el de la «Figura 1» amb les dades del cas i el dispositiu electrònic.

<table>
<tr><td colspan="3">Codi del cas:</td><td colspan="3">Data:</td></tr>
<tr><td colspan="6">Dispositiu d’origen</td></tr>
<tr><td colspan="3" rowspan="3">Fotografia i descripció del dispositiu</td><td colspan="3">Codi:</td></tr>
<tr><td colspan="3">Tipus:</td></tr>
<tr><td colspan="2">Marca:</td><td colspan="2">Model:</td></tr>
<tr><td colspan="2">Sistema operatiu / Sistema de fitxers:</td><td colspan="2">Tipus de memòria:</td><td colspan="2">Capacitat (MB):</td></tr>
<tr><td colspan="6">Mitjà de recuperació del contingut del dispositiu</td></tr>
<tr><td colspan="3">Tipus:</td><td colspan="2" rowspan="2">Hash:</td><td rowspan="2">Tipus de hash:</td></tr>
<tr><td colspan="2">Data creació:</td><td colspan="2">Mida (MB):</td></tr>
<tr><td colspan="6">Programari usat:</td></tr>
<tr><td colspan="6">Malware detectat</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">Observacions</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">Responsable peritatge</td></tr>
<tr><td colspan="3">Encarregat:</td><td colspan="3" rowspan="3">Firma:</td></tr>
<tr><td colspan="3">Identificació:</td></tr>
<tr><td colspan="3">Càrrec:</td></tr>
</table>

Figura 1. Registre dispositiu digital

Codi assignat a l'evidència:		
Nom:	Extensió:	Mida (MB):
Tipus:	Data de creació:	Data de modificació:
Ruta i estat original (esborrada, malmesa, etc):	Propietari:	Permisos:

Figura 2. Registre d'evidència digital

Codi cas: 123		Codi prova: 0001	Codi etiquetatge:
Descripció prova: Pendrive			
1	Nom i firma de qui entrega la prova:	Nom i firma de qui recull la prova:	Data entrega: Observacions:
2	Nom i firma de qui entrega la prova:	Nom i firma de qui recull la prova:	Data entrega: Observacions:

Figura 3. Cadena de custòdia (Impressió)