

# Ingeniería en Sistemas de Información

## Ciberseguridad

Docente: Ing. Gabriela Nicolao

Ayudantes: Ing. Luciano Sebastianelli, Matías  
Baghdassarian

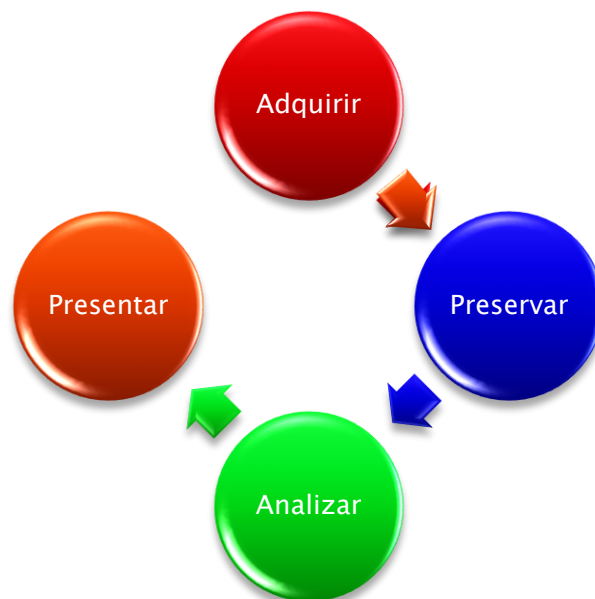


# Análisis Forense



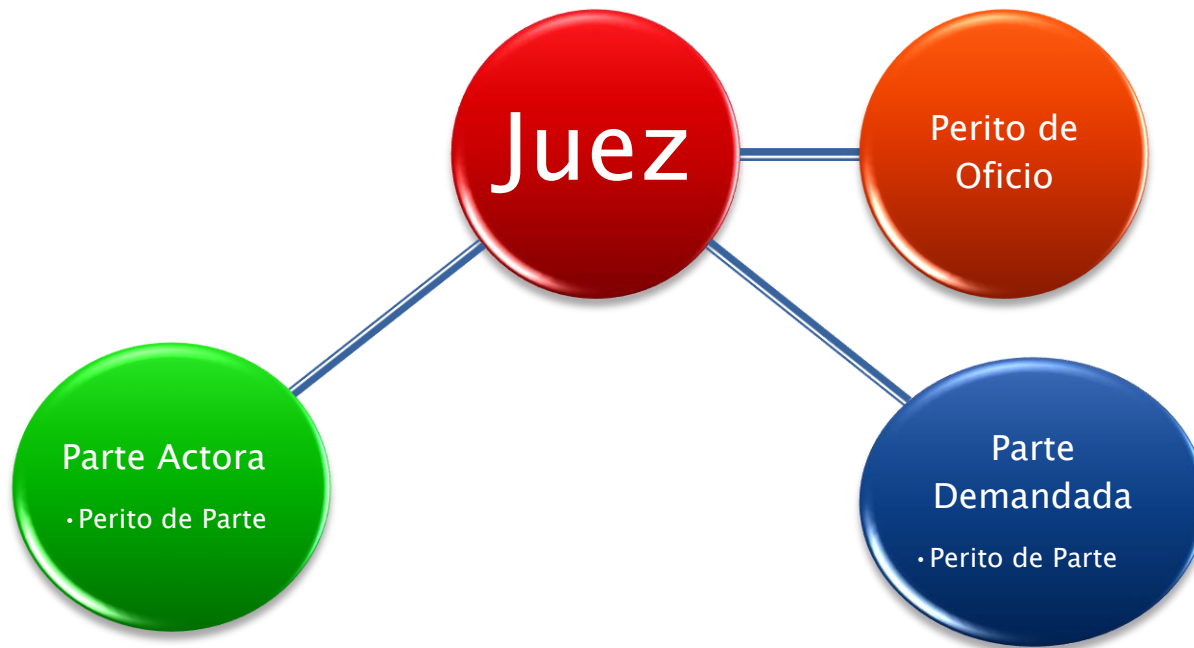
# Introducción Análisis Forense

- ▶ Es la ciencia de adquirir, preservar, analizar y presentar datos que han sido procesados electrónicamente y almacenados en medios informáticos.



- ▶ Esta relacionado con delitos informáticos o delitos donde se utiliza la tecnología como medio para llevar a cabo el delito.

- ▶ El análisis forense se puede realizar en el marco de la justicia o en el marco corporativo.
- ▶ Para el caso de la justicia los involucrados son:



- ▶ El juez solicita al perito de oficio los puntos de pericia.
- ▶ El perito de oficio los revisa e informa si hay algún punto que no puede ser contestado porque puede **no ser de su competencia**.
- ▶ En caso que tenga algún punto que **no sea de su especialidad debe contestarlo de igual manera**.
- ▶ El perito puede **no aceptar el caso por ser pariente directo** de una de las partes o tener algún tipo de **interés directo** con la parte actora o demandada.
- ▶ El resto de los puntos debe generar un informe y contestar cada uno de ellos con las evidencias correspondientes.

## Repetible

- Puede ser duplicado de manera exacta.

## Integra

- Se puede verificar si ha sido modificada.

## Recuperable

- En muchos casos es posible recuperarla aún borrada.

## Metadatos

- Contiene datos relativos a la evidencia en cuestión.



# Manejo de la evidencia

Las acciones no deben  
cambiar la evidencia

Solo debe tener acceso  
el profesional forense

Toda actividad debe ser  
documentada,  
preservada y disponible  
para revisión

Se debe mantener la  
cadena de custodia

# Cadena de custodia



- ▶ Nombre de la persona y fecha de contacto con la evidencia.
- ▶ Registro del pasaje de una persona a otra.
- ▶ Registro del pasaje de una ubicación física a otra.
- ▶ Tareas realizadas durante la posesión.
- ▶ Sellado de la evidencia al finalizar la posesión.
- ▶ Registro de testigos.





# Ocultamiento de la evidencia

- ▶ Renombrado del tipo de archivo.
- ▶ Alteración de la ubicación de archivos.
- ▶ Compactado.
- ▶ Encriptado/Cifrado.
- ▶ Esteganografía.

# Regla de exclusión de la evidencia

- ▶ La evidencia obtenida en violación de cualquier procedimiento técnico-legal, es Inadmisibile.
- ▶ Todas las conclusiones que se obtengan a partir de esa evidencia serán anuladas.

- ▶ Es el más rápido pero requiere de un bloqueador de escritura.

Pasos a seguir:

1. Extraer disco de la PC.
2. Montar disco en la PC del Investigador.
3. Adquirir imagen.
4. Reinstalar disco en PC del sospechoso.

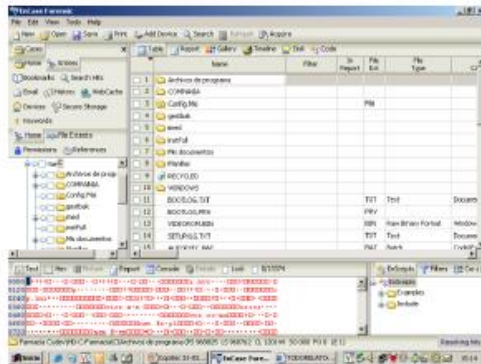
# Bloqueadores de escritura forense



# Plataforma para adquisición directa



**Adquisición DOS /Windows/  
Linux**



**PC del Investigador**



**Write Blocker para Windows o  
adquisición directa para DOS ó  
Linux modificados**

**Almacenamiento adicional**



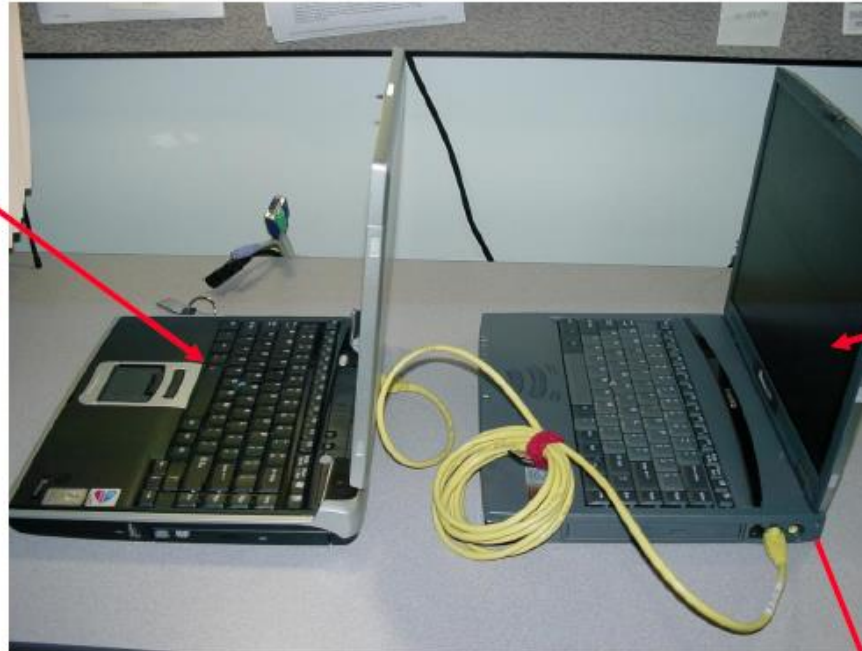
- ▶ Permite adquirir sin apertura. Es un método más lento que el Directo.
  
- ▶ Pasos a seguir:
  1. Lograr conectividad equipo de adquisición.
  2. Correr herramienta en modo Server en la PC sospechosa.
  3. Adquirir imagen.



# Plataforma para adquisición indirecta

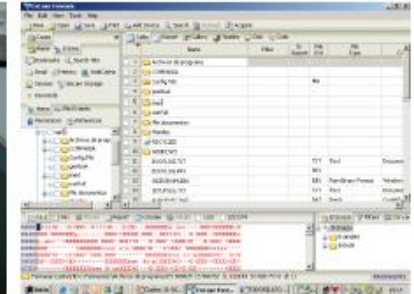


**Adquisición DOS /  
Windows/ Linux**



**Sospechoso**


**Investigador**



**Almacenamiento adicional  
USB**



1. Organizar el caso y crear una planilla para el informe final.
2. Examinar la documentación relacionada con la evidencia.
3. Controlar la cadena de custodia previa a tomar contacto con la evidencia.
4. Determinar la mejor alternativa de adquisición.
5. Verificar secuencia de boot – Verificar la fecha/hora.
6. Realizar la adquisición y mantener copias de resguardo.

7. Ingresar la evidencia en el software de análisis y verificar su integridad.
  8. Ajustar la zona de tiempos del software de análisis para poder correlacionar eventos de tiempo.
  9. Geometría de las unidades. Determinar la totalidad de sectores en el dispositivo y verificar que los mismos estén asignados a particiones de la unidad , de lo contrario realizar una recuperación y montar las eventuales particiones eliminadas.
  10. Realizar una búsqueda de posibles carpetas eliminadas en todas las unidades del caso.
- 

## 11. Ejecutar un análisis de firmas: Determinar la existencia de posibles archivos renombrados.

Nombre	Signature/Header	Header	Extension	Heder/Extension	Resultado	
Foto.jpg	FF D8 FF E0	conocido	conocido	iguales	<b>MATCH</b>	
Foto.dll	FF D8 FF E0	conocido	conocido	distintos	<b>*ALIAS JPG</b>	
Foto.zzz	FF D6 FF E0	desconocido	desconocido		<b>Unknown</b>	
Foto.jpg	D8 D8 FF E0	desconocido	conocido		<b>Bad Signature</b>	

**Foto.jpg**



**Foto.dll**



**Foto.zzz**



**Foto.jpg**



# Procedimiento Forense en Windows

## 12. Ejecutar un análisis de índices: Identificar archivos “notables”.

The screenshot displays the EnCase Forensic interface. The 'Hash Sets' menu is open, showing options like 'New', 'Update', 'Change Root Path...', 'Import Hashkeeper...', 'Import NSRL...', 'Rebuild Library...', 'Set Category...', 'New Folder...', 'Expand/Contract', 'Expand All', 'Contract All', 'Set Included Folders', 'Include Sub Folders', and 'Include Single Folder'. The main window shows a table of files with columns for Name, Count, and Category. The 'Category' column has two entries circled in red: 'Notable' for 'Fotos Pen drive secuestro 22-05' and 'Notable' for 'Imágenes Causa IPP873-92'.

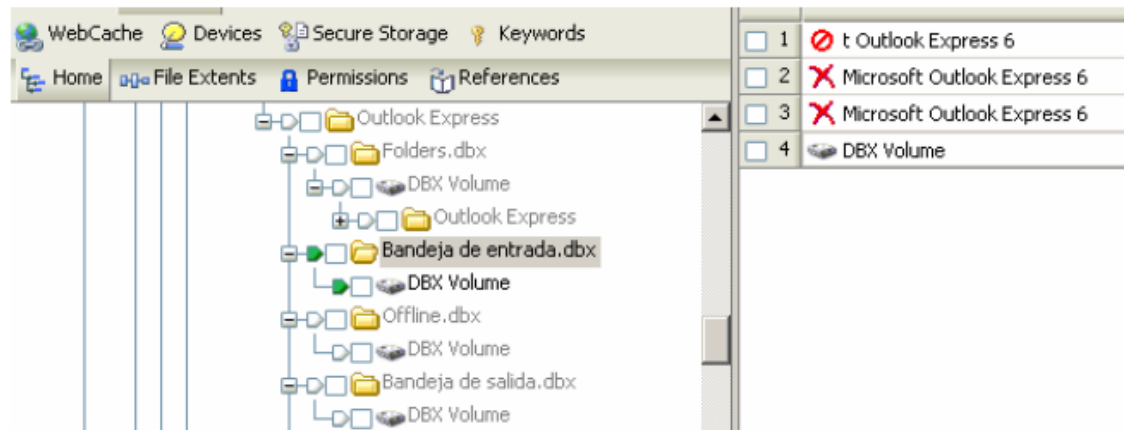
	Name	Count	Category
<input type="checkbox"/> 1	Fotos Pen drive secuestro 22-05		Notable
<input type="checkbox"/> 2	Imágenes Causa IPP873-92		Notable
<input type="checkbox"/> 3	FrontPage 98 November, 1997_1851	2456	
<input type="checkbox"/> 4	Exchange 50 SP1 August, 1997_1871	1042	
<input type="checkbox"/> 5	MatLab 5.2Mar1998Rel10_2433	1054	
<input type="checkbox"/> 6	Netscape Navigator 3.03_2066	66	
<input type="checkbox"/> 7	Office 97 Pro SR1, Project 97_1790	6308	
<input type="checkbox"/> 8	Office 97_1783	6509	
<input type="checkbox"/> 9	Office 97_1784	5998	
<input type="checkbox"/> 10	Office 97_1786	6093	
<input type="checkbox"/> 11	Office 97_1815	6753	
<input type="checkbox"/> 12	Office Standard2000 NL_2318	9062	
<input type="checkbox"/> 13	Project - International Releases 95_...	2893	
<input type="checkbox"/> 14	...	...	...

# Procedimiento Forense en Windows

13. Determinar si la unidad tiene algún tipo de cifrado de datos.

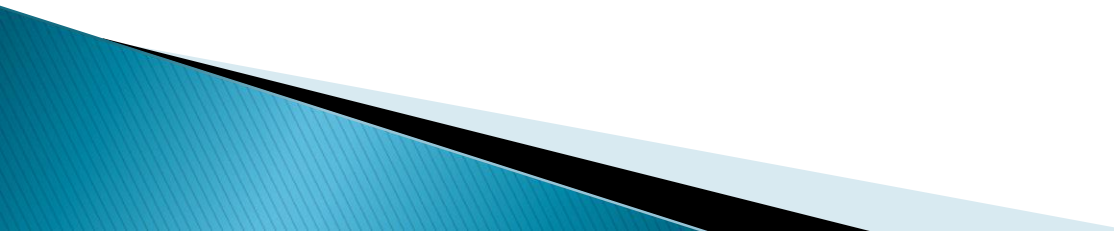
14. Identificar los tipos de clientes de correo electrónico utilizados.

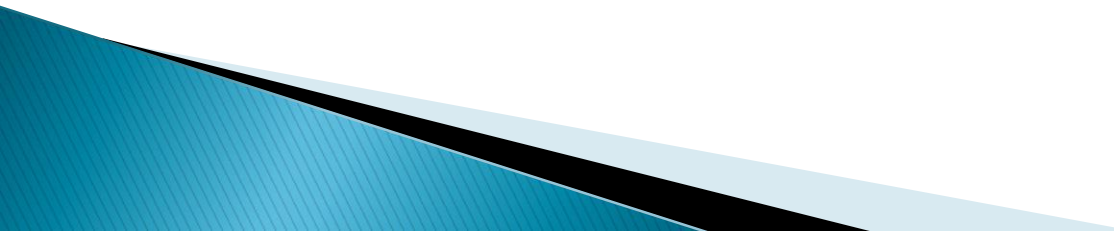
15. Realizar una búsqueda y posterior montaje de archivos compuestos (PST , DBX , ZIP , etc...):





16. Examinar la estructura de programas instalados en busca de algo vinculado con el objetivo de la investigación.
17. Si lo amerita, conducir un análisis antivirus/antispyware sobre la evidencia.
18. Determinar la ubicación de los archivos temporarios, temporarios de internet, historial y caché de internet.
19. Procesar el registro de Windows para determinar los últimos programas ejecutados. En caso de encontrar alguno de interés, analizarlo.
20. Realizar búsquedas de palabras y frases. Refinar la búsqueda en función de resultados parciales.
21. Realizar un análisis de los archivos LNK.

- 22. Realizar una búsqueda genérica de imágenes.
  - 23. Identificar unidades removibles o de red.
  - 24. Procesar la papelera de reciclaje: Determinar fechas de borrado y usuarios.
  - 25. Procesar la cola de impresión en búsqueda de impresiones realizadas.
  - 26. Determinar la existencia de mensajeros instantáneos y procesar artefactos del mismo.
  - 27. Determinar la utilización de software de intercambio P2P y procesar artefactos del mismo.
- 

28. Analizar el caché de internet en búsqueda de patrones y páginas visitadas.
  29. Realizar una verificación de la evidencia.
  30. Completar el informe y guardar todo el material procesado para una eventual ampliación posterior.
- 

# PREGUNTAS?

