



**EKOPARTY
HACKADEMY**

DOCENTE: Ing. Pablo A. Rodriguez Romeo

MATERIA: Computer Forensics

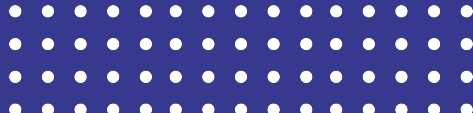


Hola!

SOY Pablo Rodriguez Romeo

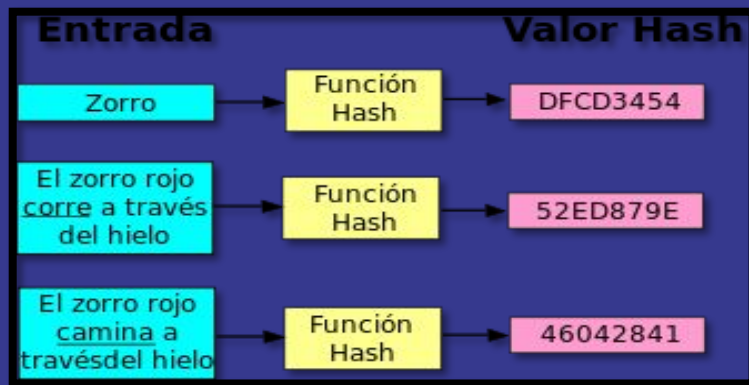
I am here because I love to give presentations.
You can find me at @username

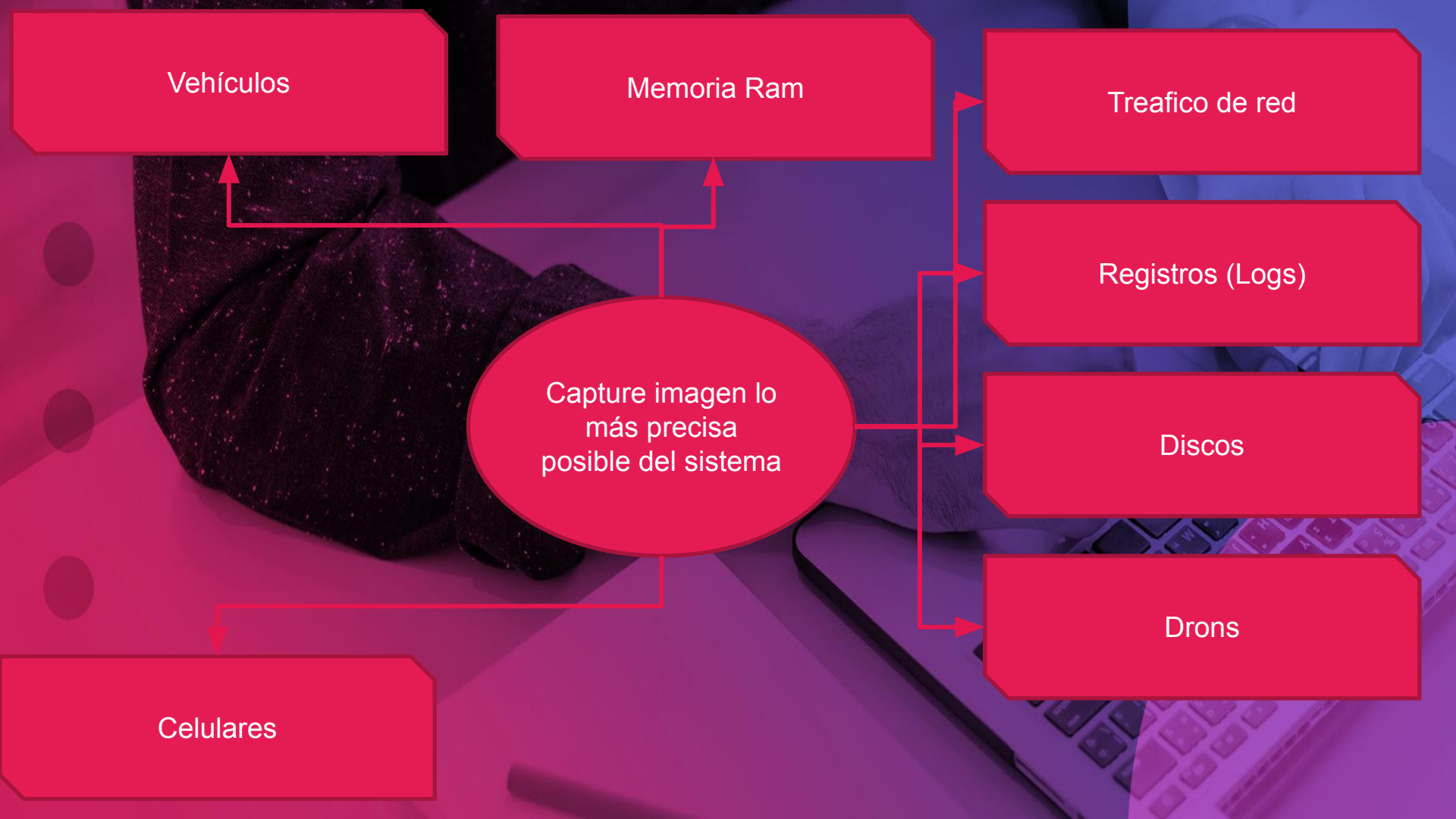
Metodología para la recolección de prueba digital



Hash o funciones resumen

Es una función que tiene como entrada, un conjunto de datos y como salida un numero finito, al cambiar el conjunto de datos de entrada el numero finito de salida cambia





Vehículos

Memoria Ram

Treafico de red

Registros (Logs)

Discos

Drons

Capture imagen lo
más precisa
posible del sistema

Celulares

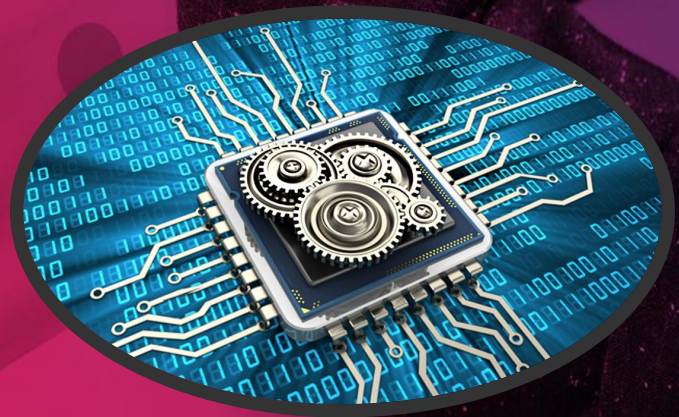


EKOPARTY
HACKADEMY

Metodología para la recolección de prueba digital

La calidad de la prueba digital, es un aspecto fundamental en cualquier disputa legal o extrajudicial esencialmente dentro de un delito donde esté involucrado directa o indirectamente un equipo informático, porque aporta valor probatorio a la investigación.

Se entiende por prueba digital, los datos generados por un equipo informático, si se considera un disco duro, la información queda registrada incluso luego de que haya sido formateado, es decir los datos almacenados en el disco pueden ser recuperados y procesados de forma correcta para que sean presentados como prueba dentro de un proceso legal.



Metodología para la recolección de prueba digital

En caso de no seguir con los procedimientos adecuados en la recolección de la prueba digital, en muchas ocasiones no se va a obtener la evidencia probatoria válida para presentar ante un juez, y por ende el delito informáticos no van a poder ser resueltos, o en otros casos no van a ser válido lo recolectado como prueba digital.





EKOPARTY
HACKADEMY

Metodología para la recolección de prueba digital

Características de la prueba digital:

Prueba Constante - Prueba Volátil

Ser muy Frágil:

Tiene la gran posibilidad de ser eliminada o modificada con facilidad.

Ser reproducible:

Tiene la gran posibilidad de ser copiada sin rastros.

Ser anónima:

No se puede saber con exactitud si realmente lo que se extrajo pertenece a un individuo en particular.

Preservación de la Prueba

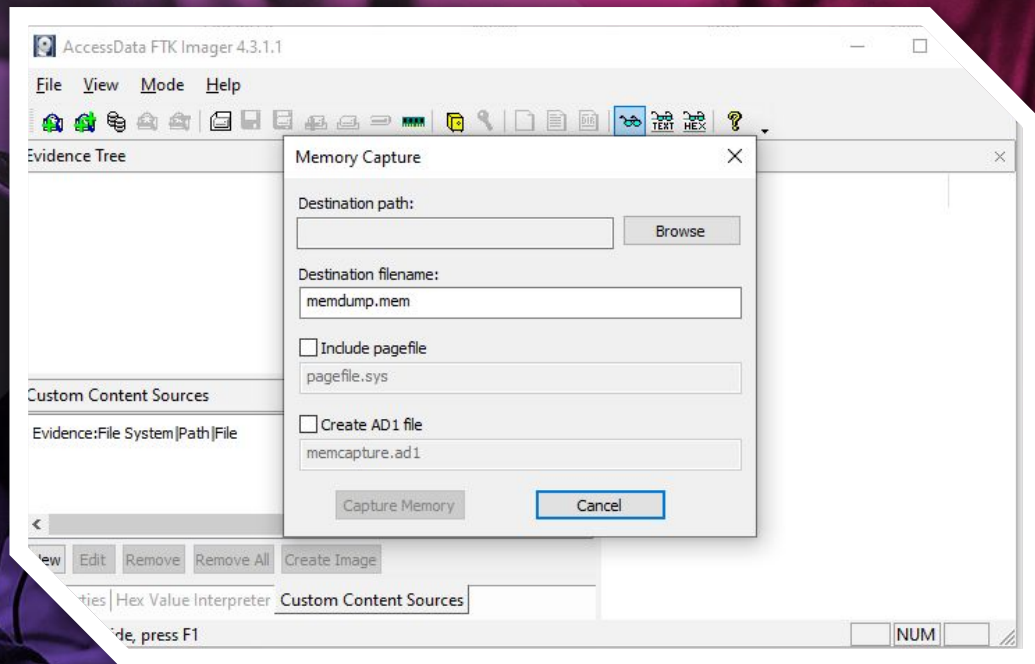
Cadena de Custodia

- Obtención de Imágenes digitales
- Imagen de un medio magnético
- Utilización de software que duplique bit a bit
- Validación de las copias mediante un algoritmo matemático (hash)
- Reproducción de estudios

Preservación de la Prueba

Capture imagen lo
más precisa
posible del sistema

Memoria Ram





Preservación de la Prueba

IgorWare Hasher

Options Help

File Text

C:\Users\Pablo\Documents\Downloads\memdump.mem Browse

Verification data

SHA-1: Verification file not found ...

MD5: Verification file not found ...

CRC32: Verification file not found ...

Hash Result

☒ SHA-1: 65f2c271ac4931475dd50395d8e4569e2ec7a7cb

☒ MD5: 21b4dc9f2d490305856e0f724658208f ☐ CRC32: Copy Save

Calculation done! Calculate

Preservación de la Prueba

En la recolección de Prueba digital, considera las buenas prácticas basados en el RFC 3227 pautas para la colección de evidencias y su resguardo en el que se destaca en principio el orden con el que debe ser recolectada, iniciando con la información más volátil hasta finalizar recolectando la información menos volátil.

Preservación de la Prueba

La prueba digital para que sea válida en procesos judicial, debe ser preservada en su autenticidad, confiabilidad, integridad y tiene que ser repetible. La prueba debe tener las siguientes características:

Admisibilidad: Debe cumplir las normas legales del país.

Auténtico: Debe comprobar que la prueba es genuina.

Fiable: No debe haber duda de su legitimidad y autenticidad.

Creíble: Debería entenderse y ser fidedigna para el tribunal

Cadena de custodia

Permite conocer la trazabilidad de la prueba en la cual debe contar con:

- Nombre de la persona y fecha de contacto con la prueba
- 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 prueba al finalizar la posesión
- Registro de testigos
- Fotografías de la prueba en las tareas realizadas
- Log de actividades durante la posesión



Cadena de custodia

Puntos a tener en cuenta en la cadena de custodia.

- La prueba debe estar correctamente lacrado, todos sus accesos (puertos, enchufes, botones y tapas)
- Si esta en una caja o sobre, deben estar correctamente cerrado y sus fajas sin roturas.

Descripción detallada de que se hizo en cada momento (comúnmente se ve reflejado en un acta)

Metodología para la recolección de evidencia digital



Capture imagen lo
más precisa
posible del sistema

TODA LA EVIDENCIA	181											
RESULTADOS REFINADOS	19											
Identificadores: Dispositivo	8											
Identificadores: Personas	3											
Archivos y carpetas de acceso local	8											
WEB RELACIONADA	101											
Contenido de Edge/Internet Explorer 10-11	5											
Historial principal de Edge/Internet Explorer 10-11	8											
Google Maps	9											
Actividad posible de navegador	78											
Historial web del navegador de WebKit (tallado)	1											
MEDIOS	27											
Google WebP Images	8											
Imágenes	19											
CORREO ELECTRÓNICO	1											
Archivos EML (X)	1											
SISTEMA OPERATIVO	32											
Archivos LNK	28											
Registros de eventos de Windows	4											
PERSONALIZAR	1											
Carved Archives (content not searched)	1											
		Identifica...	Nombre de co...	Artefacto	ID. d...	Fuente	Mét...	Fuen...	Ubicación	Número...		
		AA6F405F	Volume Serial Number	LNK Files	4	memdump.mem			File Offset 25516992	memdump.mem		
		B4:2E99:4EA3:4E	MAC Address	LNK Files	4	memdump.mem			File Offset 25516992	memdump.mem		
		B070E279	Volume Serial Number	LNK Files	17	memdump.mem			File Offset 21492800	memdump.mem		
		Causas	Volume Name	LNK Files	17	memdump.mem			File Offset 21492800	memdump.mem		
		0A6D2CC9	Volume Serial Number	LNK Files	31	memdump.mem			File Offset 30644288	memdump.mem		
		FTI	Volume Name	LNK Files	31	memdump.mem			File Offset 30644288	memdump.mem		
		02:01:00:00:00:00	MAC Address	LNK Files	107	memdump.mem			File Offset 56472064	memdump.mem		
		PC-Destino	Computer	Windows Event Logs	123	memdump.mem			File Offset 104524016	memdump.mem		

Gracias



CYSI

Informática Forense



CYSI

Informática Forense