



INSTITUTO TECNOLÓGICO DE LAS AMÉRICAS  
(ITLA)  
Tecnólogo en Informática Forense

**INFORME DE LEVANTAMIENTO:**

**DIRECCIÓN DEL LEVANTAMIENTO**

**NUMERO DE CASO**

Autopista Las Américas, km. 27, PCSD, La Caleta, Boca Chica, República Dominicana.	ITLA-1319
---	-----------

**NOMBRE DEL AGRAVIADO**

**TIPO DE HECHO**

Ángel Gabriel	Intento de acceso no autorizado y modificación de credenciales
---------------	---

**DETALLE DEL CASO**

**FECHA DE LLEGADA**

**TIEMPO DE LLEGADA**

Pedro Javier ingresó a la página web de sigeiacademico.itla.edu.do utilizando las credenciales de un estudiante con la intención de cambiar la contraseña de dicho estudiante sin autorización.	15-10-2024	09:15 AM
--	------------	----------

**ENC. DEL LEVANTAMIENTO EN EL TIEMPO DE  
LLEGADA**

**CONDICIÓN DE LA ESCENA**

Carlos Ernesto Mora	Aula donde imparten clases, mucha iluminación.
---------------------	--

**PERSONAL QUE PARTICIPO EN EL PROCESAMIENTO DE LA ESCENA**

<b>NOMBRE COMPLETO</b>	<b>FUNCIÓN</b>
Alan José Martínez Muñoz	Técnico de levantamiento
Pedro Navaja	Chofer
Julio José	Fotógrafo

## ANTECEDENTES

Siendo las 9:15 AM del día 15-10-2024, fue trasladada la unidad de levantamiento de evidencias electrónicas del departamento de informática forense de ForensicLab, solicitada por Edgar Emil, Rector del ITLA. Dicha unidad está compuesta por Alan José Martínez Muñoz (Técnico de levantamiento), Pedro Navaja (Chofer), Julio José (Fotógrafo).

El levantamiento se realizó en respuesta a la acción indebida cometida por Ángel Gabriel, quien habría ingresado al sitio web de [sigeiacademico.itla.edu.do](http://sigeiacademico.itla.edu.do) utilizando las credenciales de varios estudiantes de dicha institución, con la intención de modificar las contraseñas de estos sin su autorización.

La institución afectada, el Instituto Tecnológico de las Américas (ITLA), se dedica a la formación superior en tecnología y se encuentra ubicada en La Caleta, Boca Chica, República Dominicana. Al llegar al lugar a las 9:15 AM, fuimos recibidos por Edgar Emil, Rector de la institución, quien nos proporcionó acceso a la información necesaria para llevar a cabo el levantamiento de las evidencias.



Edificio 2



Aula 2-1C



dentro

## PROCEDIMIENTO TECNICO UTILIZADO

### Identificación:

- Se procedió a fotografiar la evidencia.
- Se verificó de manera física y lógica sus especificaciones, que componentes posee.
- Se verificó si está cifrado el dispositivo.

### Recolección:

- Se realizó un volcado de memoria RAM al dispositivo.

- Se verificó si hubo un acceso realmente en la herramienta Autopsy con el archivo generado por la herramienta de volcado.



#### Preservación:

- Redacción de cadena de custodia.
- Documentación de todos los procesos realizados
- Acceso limitado a la evidencia
- Valor hash de la evidencia

### HERRAMIENTAS UTILIZADOS

	<p>Encryption Disk Detector versión 3.1: Es una herramienta de línea de comandos que puede verificar de forma rápida y no intrusiva los volúmenes cifrados en un sistema informático durante la respuesta a incidentes.</p>
	<p>MWSNAP versión 3.0: Programa de captura de pantalla capaz de tomar tomas de escritorio completas, una ventana resaltada, un menú activo o un rectangular fijo</p>
	<p>Magnet RAM Capture versión 1.2: Es un programa gratuito de imágenes diseñado para capturar la memoria física de la computadora de un sospechoso</p>
	<p>MD5 Summer: Es una aplicación para Microsoft Windows 9x, NT, ME, 2000 y XP que genera. y verifica las sumas de comprobación MD5</p>
	<p>FTK Imager: Facilita el examen de archivos y carpetas dentro de imágenes forenses. Permite a los investigadores ver y extraer archivos individuales, incluidos archivos eliminados u ocultos, para un análisis en profundidad.</p>

## DISPOSITIVOS UTILIZADOS

	Fanxiang S101: Con sus especificaciones, sata ssd 1tb, internal state drive sata iii 6gb/s 2.5" sata ssd, up to 550mb/s, 1tb internal ssd.
	Data traveler exodia usb 3.2, color azul, almacenamiento 64 GB.

## METODOLOGIA O GUIA DE BUENA PRACTICA EMPLEADA

La metodología utilizada para realizar los procesos de adquisición, análisis y preservación de evidencias se basan en la norma ISO 27037:2012 (Tecnología de la información - Técnicas de seguridad - Guías para la identificación, recopilación, adquisición y preservación de evidencias digitales). Dicha norma tiene como principios, los siguientes:


- **Aplicación de métodos.** La evidencia digital debe ser adquirida del modo menos intrusivo posible, tratando de preservarla originalidad de la prueba y en la medida de lo posible obteniendo copias de respaldo.
- **Proceso auditable.** Los procedimientos seguidos y la documentación generada deben haber sido validados y contrastados por las buenas prácticas profesionales. Se deben proporcionar trazas y evidencias de lo realizado y sus resultados.
- **Proceso reproducible.** Los métodos y procedimientos aplicados deben de ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.
- **Proceso defendible.** Las herramientas utilizadas deben de ser mencionadas y éstas deben de haber sido validadas y contrastadas en su uso para el fin en el cual se utilizan en la actuación. Para cada tipología de dispositivo la norma divide la actuación o su tratamiento en tres procesos diferenciados como modelo genérico de tratamiento de las evidencias.
- **Identificación.** Es el proceso de la identificación de la evidencia y consiste en localizar e identificar las potenciales información eso elementos de prueba en sus dos posibles estados, el físico y el lógico, según sea el caso de cada evidencia.
- **Recolección y/o adquisición.** Este proceso se define como la recolección de los dispositivos y la documentación (incautación y secuestro de estos) que puedan contener la



evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos.

- **Conservación/preservación.** La evidencia ha de ser preservada para garantizar su utilidad, es decir, su originalidad para que a posteriori pueda ser ésta admisible como elemento de prueba original e íntegro, por lo tanto, las acciones de este proceso están claramente dirigidas a conservar la cadena de custodia, la integridad y la originalidad de la prueba.

ACTA DE ADQUISICIÓN DE EVIDENCIAS

FECHA	NUMERO DE CASO	NOTAS DEL CASO
15/10/2024	ITLA-1319	Las evidencias recolectadas serán enviadas al laboratorio su análisis detallado.

UBICACIÓN Y REGISTRO DE INDICIO				
NO.	FOTOGRAFIA	DESCRIPCION	UBICACION	LEVANTADO POR
1		Laptop Lenovo, color azul, modelo IdeaPad 3 15ADAD5, dispositivo encendido.	En la mesa dentro del Aula 2-1C	Alan José Martínez Muñoz – Técnico de Levantamiento

				
2.		Cargador Lenovo, modelo ADLX65CLGU2A, color negro.	Encima de la mesa del aula 2-1C, junto a laptop Lenovo.	Alan José Martínez Muñoz – Técnico de Levantamiento.



EVIDENCIA EVD-01X		
Tipo de Dispositivo:	<input type="checkbox"/> Ordenador de Sobremesa	<input type="checkbox"/> Ordenador Portátil
	<input type="checkbox"/> SmartPhone	<input type="checkbox"/> Tablet
	<input type="checkbox"/> Pendrive	<input type="checkbox"/> Otros(Especificar): Laptop
Tipo de Evidencia:	<input type="checkbox"/> Disco Duro (HDD) <input type="checkbox"/> RAID Nivel: <input type="checkbox"/> Memoria flash USB	<input type="checkbox"/> Disco Sólido (SDD) <input type="checkbox"/> Correo electrónico <i>(Indicar cuenta en Buzón de Correo)</i> <input type="checkbox"/> Memoria Flash Smartphone/Tablet
Fabricante:	Lenovo	
Modelo:	81W1	
Número de Serie:	PF2ELGQ8	
Fabricante del Dispositivo:	Lenovo	
Modelo de Dispositivo:	IdeaPad 3 15ADAD5	

IMEI de Dispositivo:	
Número de Serie de Dispositivo:	

EVIDENCIA EVD-02X	
Tipo de Dispositivo:	<input type="checkbox"/> Ordenador de Sobremesa <input type="checkbox"/> Ordenador Portátil <input type="checkbox"/> SmartPhone <input type="checkbox"/> Tablet <input type="checkbox"/> Pendrive <input type="checkbox"/> Otros (Especificar): Cargador
Tipo de Evidencia:	<input type="checkbox"/> Disco Duro (HDD) <input type="checkbox"/> RAID Nivel: <input type="checkbox"/> Memoria flash USB <input type="checkbox"/> Disco Sólido (SDD) <input type="checkbox"/> Correo electrónico <i>(Indicar cuenta en Buzón de Correo)</i> <input type="checkbox"/> Memoria Flash Smartphone/Tablet
Fabricante:	Lenovo
Modelo:	
Número de Serie:	SA10M42725
Fabricante del Dispositivo:	Lenovo
Modelo de Dispositivo:	ADLX65GLGU2A
IMEI de Dispositivo:	
Número de Serie de Dispositivo:	





## Cadena de Custodía

16/10/2024

Date

Case number: ITLA-1319

Reason evidence  
was obtained: Acceso ilícito y modificación de credenciales

Location from which the  
evidence was obtained: Instituto de Las Americas,  
Edificio 2, Aula 2-1C, encima  
de la mesa del docente

Date and time evidence  
was obtained: 15/10/2024

Item Number: 153628/125418

Quantity: 2

Description of item: Laptop Marca Lenovo, color azul, estado encendido . Recolectada junto a un cargador Marca Lenovo.


### Picked evidence from

Contact Name: Alan José Martínez Muñoz- Tecnico de Levantamiento Phone #: 800-000-0000

Company Name: ForensicxLabs Email: Martinezalan@forensicxlabs.com.do

Address: Calle D #159, Ensanche Naco

City: Santo Domingo

  
Signature

### Description of Evidence Item

Laptop marca Lenovo Modelo visible, IdeaPad 3 15ADAD5, Color azul, encontrada encendida. Serial visible, PF2ELHQ8

Cargador Marca Lenovo, Modelo visible: ADLX65CLGU2A. Color Negro.

### Observation

La evidencia fue recolectada para ser llevada al Laboratorio para su respectivo analisis.



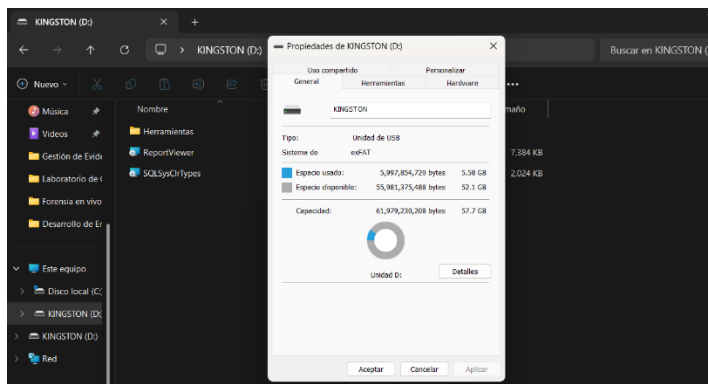
Received From  
Julio Alcantara- Encargado de Analisis

*ForensicxLabs*

Company  
ForensicxLabs

**CASO NÚMERO ITLA-1319**

Se procedió a montar el laboratorio lógico en la computadora para poder utilizar nuestras herramientas y poder hacer la identificación, recolección y preservamos la evidencia tanto de forma lógica como física. Nuestro laboratorio está almacenado en una Memoria USB Kingston.



Para identificar el dispositivo, fuimos a la siguiente ruta, D:\Herramientas\Herramientas Forenses (Live)\Herramientas Forenses (Live)\IDENTIFICACION\IR\_Tools. Donde tenemos un CMD portable y pondremos el siguiente código, systeminfo, con este código vamos a obtener la información de la evidencia que tenemos a mano.

```
D:\Herramientas\Herramienta x + v
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

D:\Herramientas\Herramientas Forenses (Live)\Herramientas Forenses (Live)\IDENTIFICACION\IR_Tools>systeminfo

Nombre de host: ALAAAANSITO
Nombre del sistema operativo: Microsoft Windows 11 Home
Versión del sistema operativo: 10.0.22631 N/D Compilación 22631
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: Alan Martinez
Organización registrada:
Id. del producto: 00325-81955-53577-AAOEM
Fecha de instalación original: 31/8/2024, 2:18:13 p. m.
Tiempo de arranque del sistema: 11/10/2024, 12:22:58 p. m.
Fabricante del sistema: LENOVO
Modelo el sistema: 81W1
Tipo de sistema: x64-based PC
Procesador(es): 1 Procesadores instalados.
[01]: AMD64 Family 23 Model 24 Stepping 1 AuthenticAMD ~2100 Mhz
Versión del BIOS: LENOVO E8CN34WW, 28/4/2022
Directorio de Windows: C:\Windows
Directorio de sistema: C:\Windows\system32
Dispositivo de arranque: \Device\HarddiskVolume1
Configuración regional del sistema: en-us;Inglés (Estados Unidos)
Idioma de entrada: es-mx;Español (México)
Zona horaria: (UTC-04:00) Georgetown, La Paz, Manaus, San Juan
Cantidad total de memoria física: 18,308 MB
Memoria física disponible: 11,490 MB
```

```
D:\Herramientas\Herramienta x + v
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio: WORKGROUP
Servidor de inicio de sesión: \\ALAAAANSITO
Revisión(es): 4 revisión(es) instaladas.
[01]: KB5044033
[02]: KB5027397
[03]: KB5044285
[04]: KB5046247

Tarjeta(s) de red: 3 Tarjetas de interfaz de red instaladas.
[01]: Bluetooth Device (Personal Area Network)
Nombre de conexión: Bluetooth Network Connection
Estado: Medios desconectados
[02]: Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
Nombre de conexión: Wi-Fi
DHCP habilitado: Sí
Servidor DHCP: 10.0.0.1
Direcciones IP
[01]: 10.0.0.3
[02]: fe80::1243:23e:2fb6:f92a
[03]: 2001:1308:248c:b400:add0:a3f2:2915:1fa3
[04]: 2001:1308:248c:b400:7cbf:7279:e7a2:33fb
[05]: 2001:1308:248c:b400:5012:8ef2:a80:c676
[06]: 2001:1308:248c:b400:1986:23a1:6227:a2be
[07]: 2001:1308:248c:b400:1112:6c00:4ee3:7f4b
[08]: 2001:1308:248c:b400:4bf:3fbc:c599:7149
[09]: 2001:1308:248c:b400:1d2f:23e2:dca8:f7ef
[10]: 2001:1308:248c:b400::1
[03]: VirtualBox Host-Only Ethernet Adapter
Nombre de conexión: Ethernet
DHCP habilitado: No
```

```
D:\Herramientas\Herramienta x + v
Tarjeta(s) de red:
[04]: KB5046247
3 Tarjetas de interfaz de red instaladas.
[01]: Bluetooth Device (Personal Area Network)
Nombre de conexión: Bluetooth Network Connection
Estado: Medios desconectados
[02]: Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
Nombre de conexión: Wi-Fi
DHCP habilitado: Sí
Servidor DHCP: 10.0.0.1
Direcciones IP
[01]: 10.0.0.3
[02]: fe80::1243:23e:2fb6:f92a
[03]: 2001:1308:248c:b400:ad0:a3f2:2915:1fa3
[04]: 2001:1308:248c:b400:7cbf:7279:e7a2:33fb
[05]: 2001:1308:248c:b400:5012:8ef2:a80:c676
[06]: 2001:1308:248c:b400:1986:23a1:6227:a2be
[07]: 2001:1308:248c:b400:1112:6c00:4ee3:7f4b
[08]: 2001:1308:248c:b400:4bf:3fbc:c599:7149
[09]: 2001:1308:248c:b400:1d2f:23e2:dca8:f7ef
[10]: 2001:1308:248c:b400::1
[03]: VirtualBox Host-Only Ethernet Adapter
Nombre de conexión: Ethernet
DHCP habilitado: No
Direcciones IP
[01]: 192.168.56.1
[02]: fe80::162a:db15:d539:969a
Requisitos Hyper-V: Se detectó un hipervisor. No se mostrarán las características necesarias para
Hyper-V.
D:\Herramientas\Herramientas Forenses (Live)\Herramientas Forenses (Live)\IDENTIFICACION\IR_Tools>
```

Se utilizó la herramienta encrypted disk detector, para identificar si la evidencia está cifrada, esta herramienta está localizada en la siguiente ruta: D:\Herramientas\Herramientas Forenses (Live)\Herramientas Forenses (Live)\IDENTIFICACION\Verificacion de encriptacion\Magnet encrypti\EDDv310.

```
D:\Herramientas\Herramientas Forenses (Live)\Herramientas Forenses (Live)\IDENTIFICACION\Verificacion de encriptacion\Magnet encrypti\EDDv310\EDDv310.exe
Copyright (c) 2009-2022 Magnet Forensics Inc.
http://www.magnetforensics.com
// By using this software from Magnet Forensics, you agree that your use is governed by the End User License Agreement available at www.magnetforensics.com/legal. //

* Checking physical drives on system... *

Checking PhysicalDrive0 - SKhynix_HFS001TE79X115N (1,024 GB) - Status: OK
Checking PhysicalDrive1 - Kingston DataTraveler 3.0 USB Device (62 GB) - Status: OK

* Completed checking physical drives on system. *

* Now checking logical volumes on system... *

Drive C: (PhysicalDrive0), Drive Type: Fixed, Filesystem: NTFS, Size: 1,023 GB, Free Space: 530 GB
Drive D: [Label: KINGSTON] (PhysicalDrive1), Drive Type: Removable, Filesystem: exFAT, Size: 62 GB, Free Space: 56 GB

* Completed checking logical volumes on system. *

* Running Secondary Bitlocker Check... *
* Completed Secondary Bitlocker Check... *

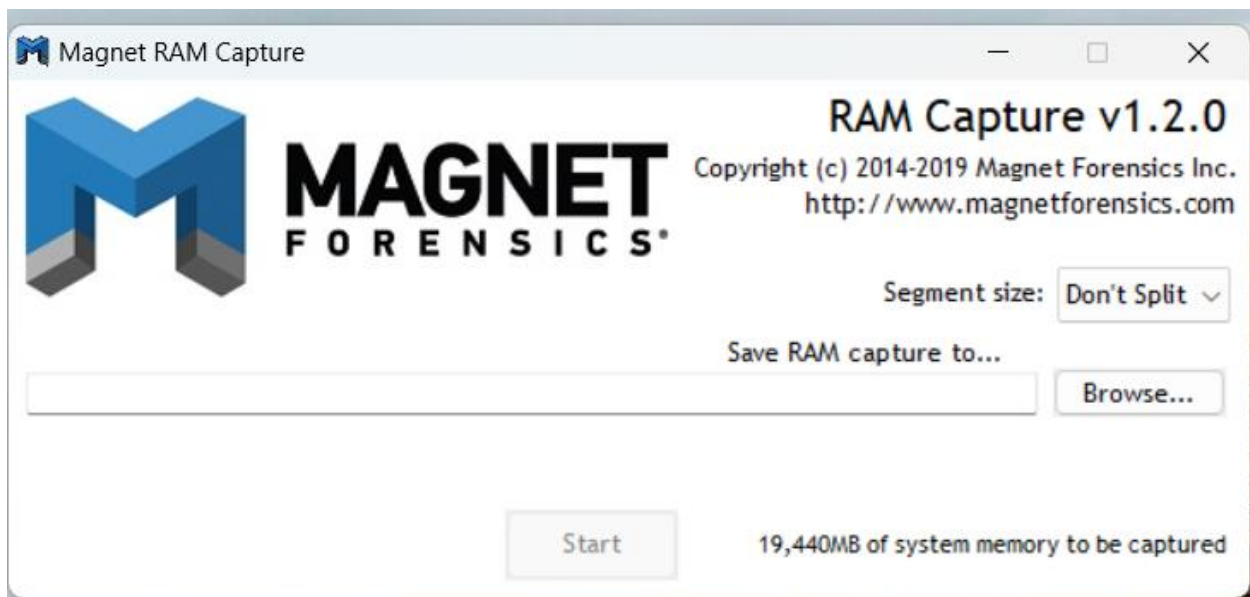
* Checking for running processes... *
* Completed checking running processes. *

*** No TrueCrypt, PGP, Bitlocker, VeraCrypt, SafeBoot, BestCrypt, Checkpoint, Sophos, or Symantec encrypted volumes detectable by EDD were found. ***

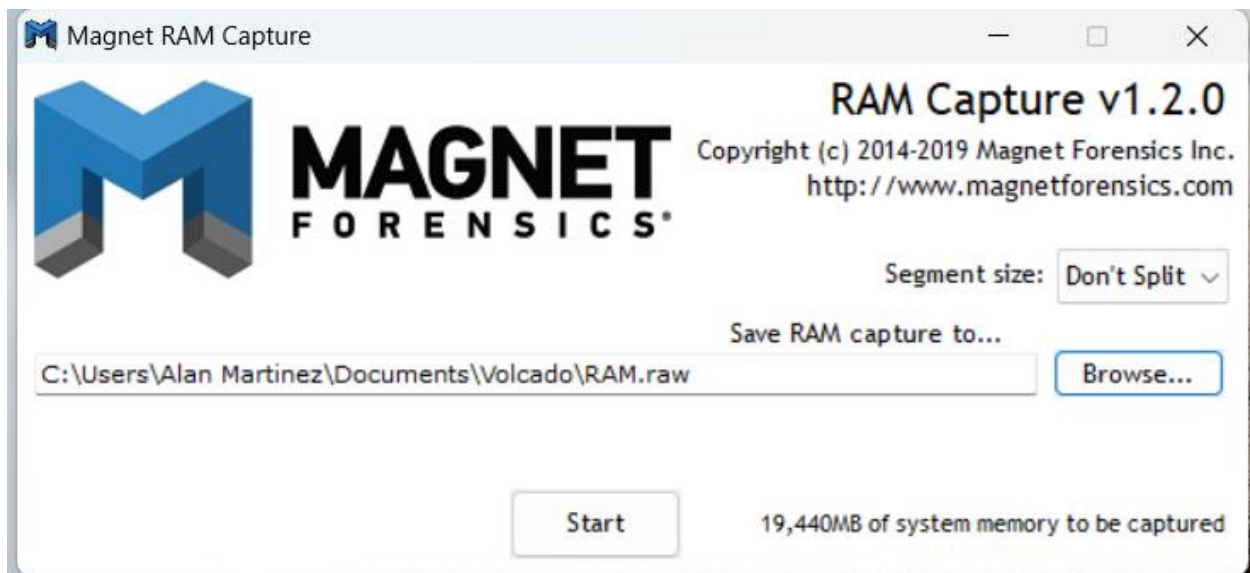
Press any key to continue...
(use 'EDD /batch' to bypass this prompt next time)
_
```

Se procedió a crear una carpeta llamada volcado en nuestro disco duro SSD externo. Esta carpeta nos servirá para almacenar el volcado de Memoria RAM que se le va a realizar al dispositivo, con la herramienta Magnet RAM Capture V1.2.0, dicha herramienta se encuentra localizada en la siguiente ruta: D:\Herramientas\Herramientas Forenses (Live)\Herramientas Forenses (Live)\RECOLECCION\Herramientas para Volcado\MagnetRamCapture.

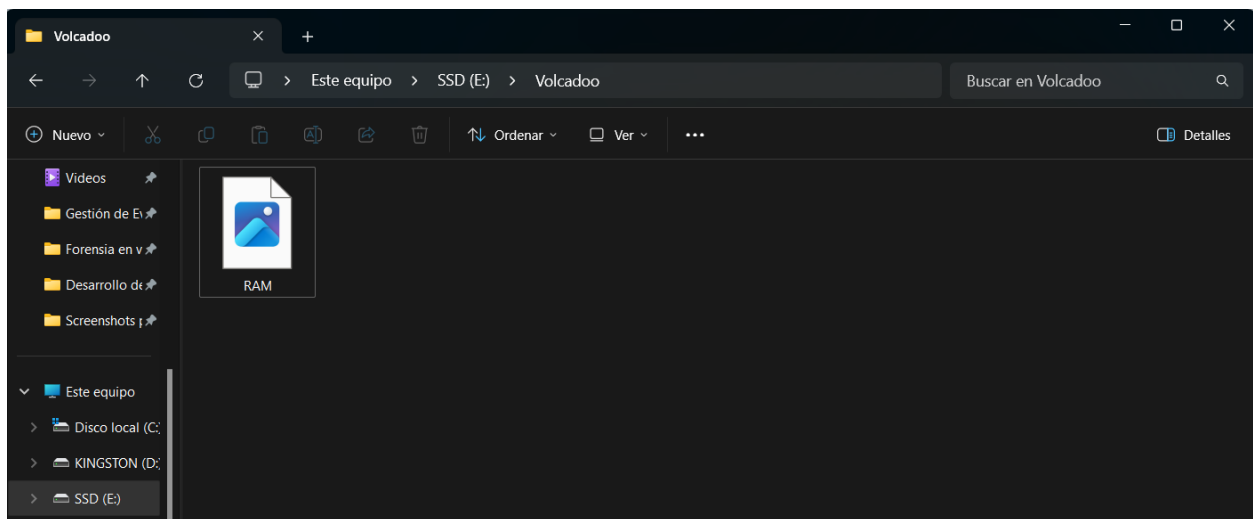
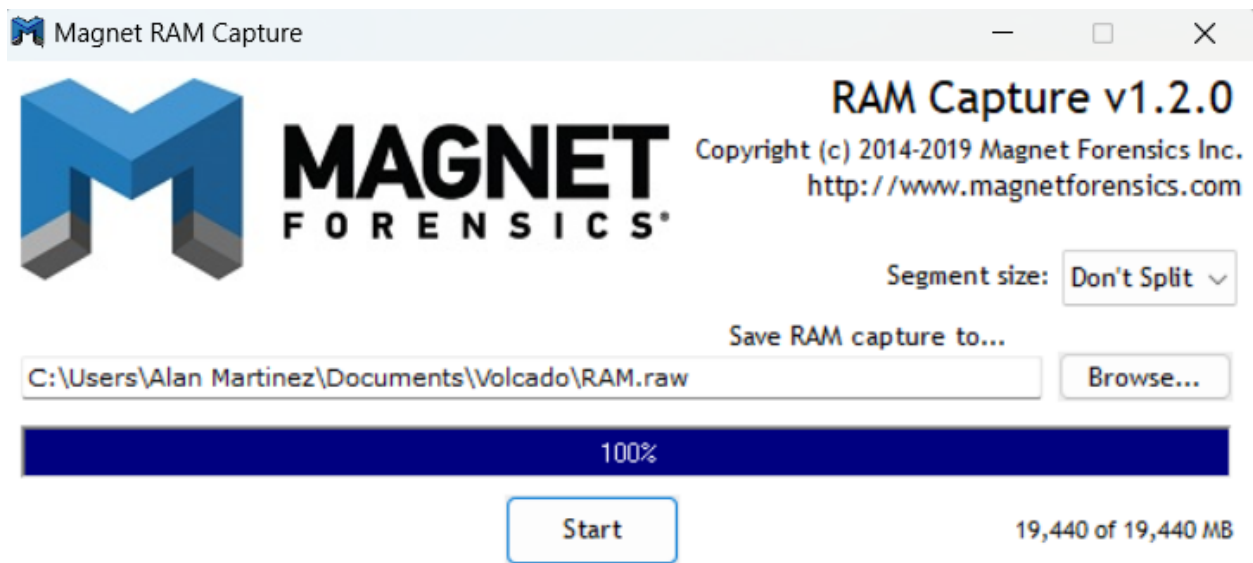
Abrimos la herramienta



Establecemos la ruta donde vamos a querer se almacene el archivo generado por la herramienta.



Archivo generado al 100% y ubicación del archivo: E:\Volcadoo

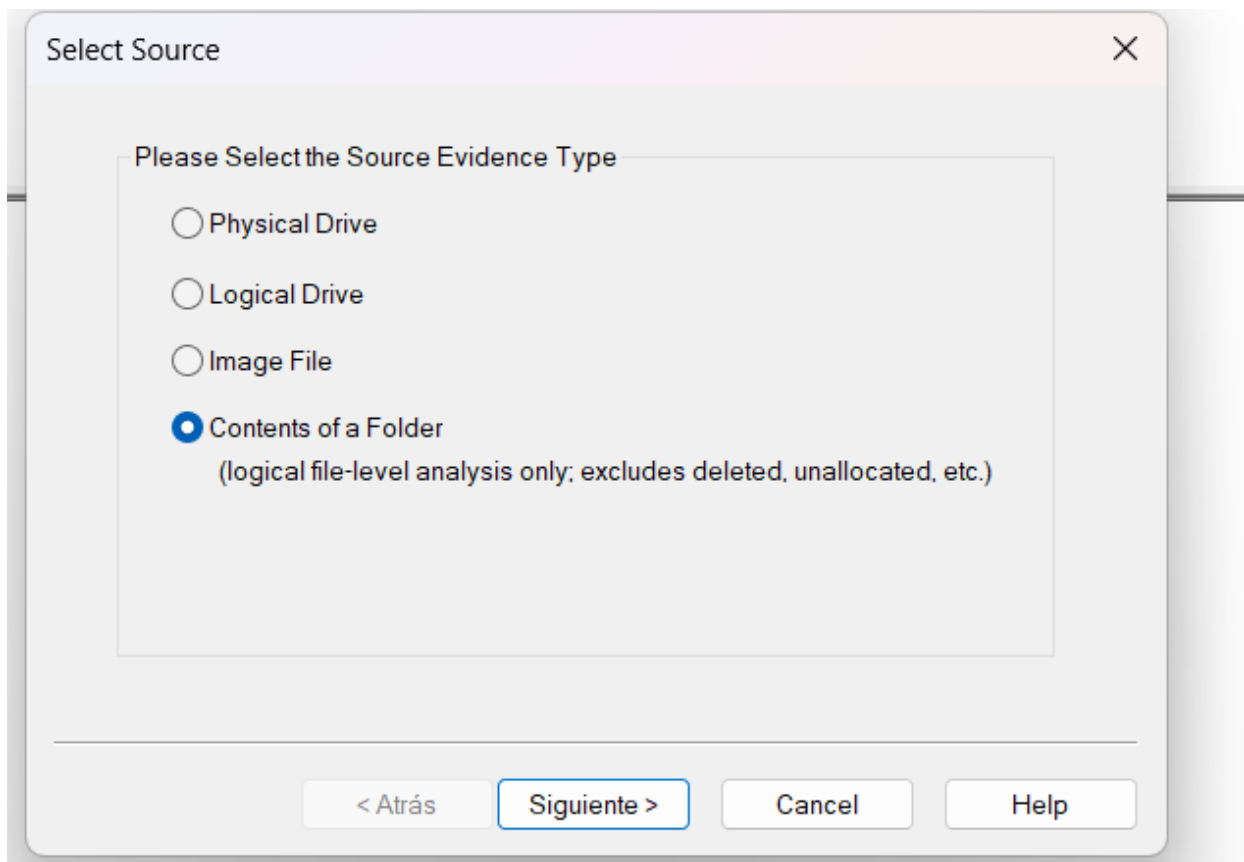


Realicé una copia a un archivo .xls para mantener su integridad, se utilizó la herramienta FTK Imager, y esta herramienta está ubicada en la siguiente ruta: D:\Herramientas\Herramientas Forenses (Live)\Herramientas Forenses (Live).

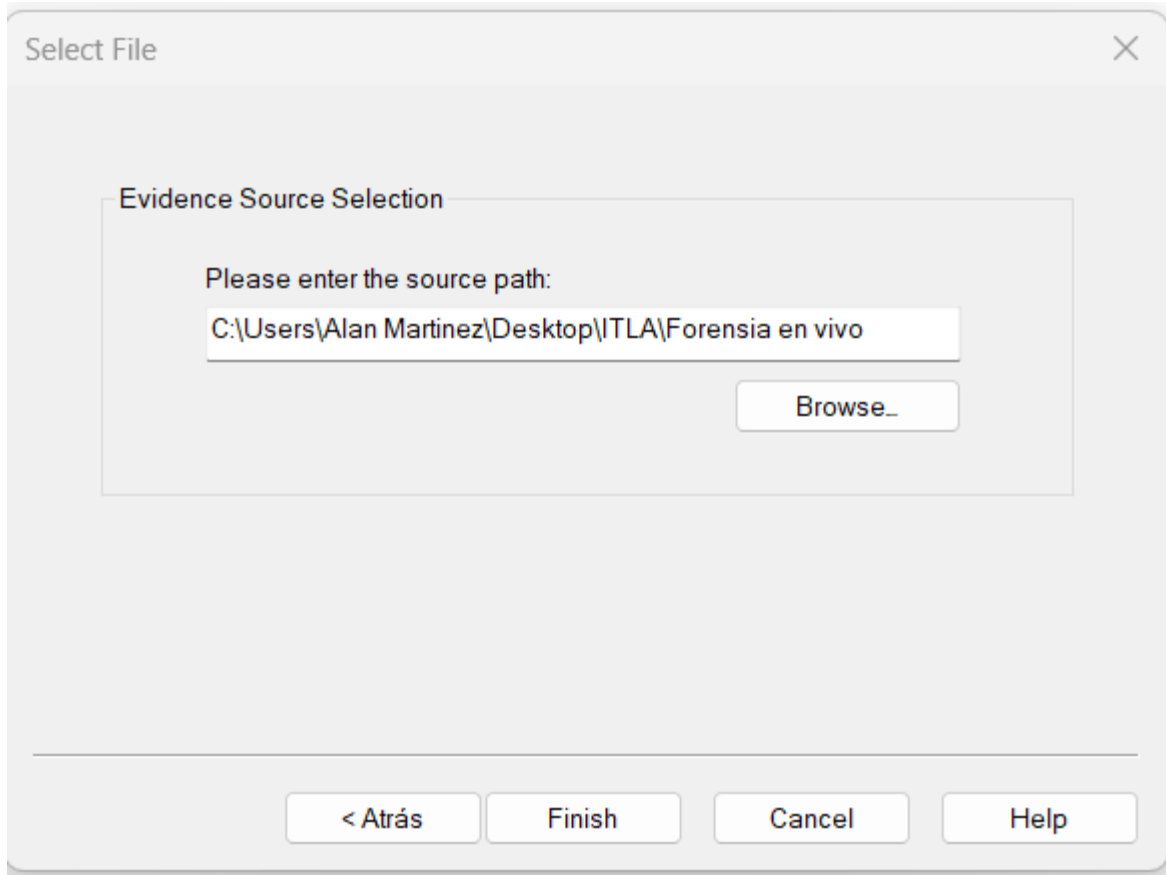
1- Seleccionaremos el primer icono debajo de file, que recibe su nombre de add evidence item



2-Seleccionaremos el tipo de evidencia, en nuestro caso es un archivo, por lo que vamos a seleccionar la 4ta opción.



3-Establecemos la ruta donde tenemos almacenada nuestra evidencia

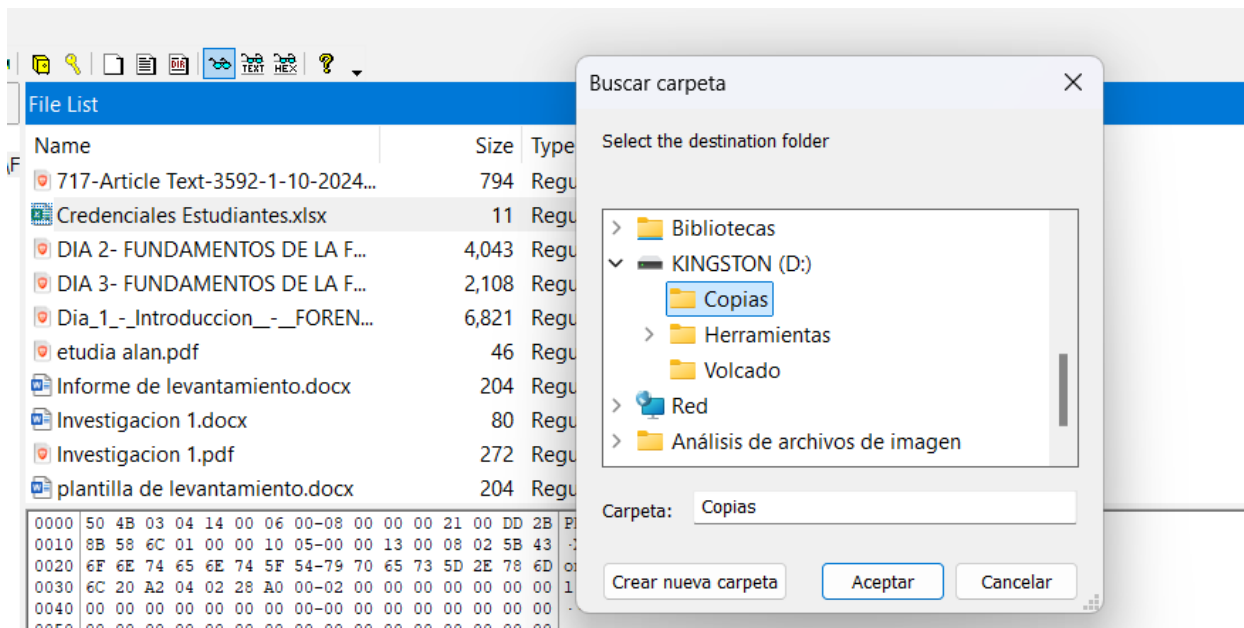


4-Identificamos nuestra evidencia a duplicar, en nuestro caso es el .xlsx

Evidence Tree		File List			
Forensia en vivo		Name	Size	Type	Date Modified
C:\Users\Alan Martinez\Desktop\ITLA\F		717-Article Text-3592-1-10-2024...	794	Regular File	17/9/2024 3:33:53 ...
		Credenciales Estudiantes.xlsx	11	Regular File	16/10/2024 2:57:37...
		DIA 2- FUNDAMENTOS DE LA F...	4,043	Regular File	16/9/2024 4:57:41 ...
		DIA 3- FUNDAMENTOS DE LA F...	2,108	Regular File	3/10/2024 11:01:04...
		Dia_1_-_Introduccion_-_FOREN...	6,821	Regular File	8/9/2024 4:07:26 p...
		etudia alan.pdf	46	Regular File	26/9/2024 7:19:48 ...
		Informe de levantamiento.docx	204	Regular File	11/10/2024 12:24:4...
		Investigacion 1.docx	80	Regular File	12/9/2024 12:46:37...
		Investigacion 1.pdf	272	Regular File	12/9/2024 12:46:56...
		plantilla de levantamiento.docx	204	Regular File	15/10/2024 3:49:40...

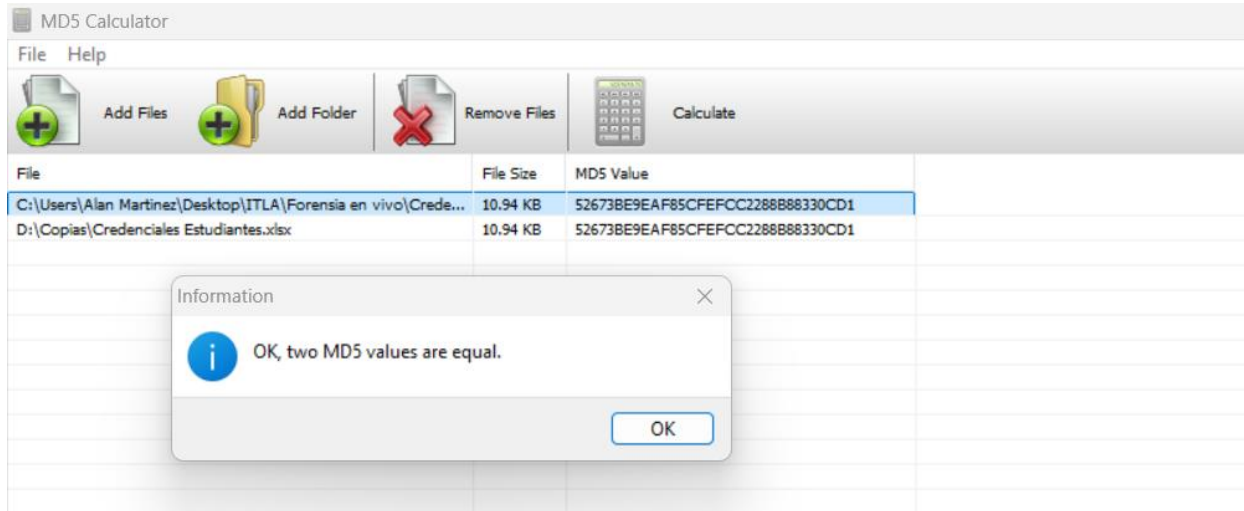
5-Seleccionaremos la ruta a donde vamos a guardar nuestra copia



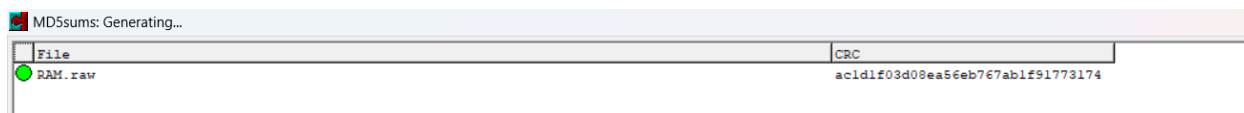


Se utilizó MD5 Calculator para sacarle el valor hash a dichas evidencias, esta herramienta está localizada en la siguiente ruta: D:\Herramientas\Herramientas Forenses (Live)\MD5 Calculator.

Se compararon los valores Hash del xls original y la copia que se le realizó.



Se calculó el valor hash de el archivo generado por la herramienta Magnet RAM capture, se utilizó la herramienta MD5Summary, esta herramienta está localizada en la siguiente ruta: D:\Herramientas\Herramientas Forenses (Live)\Herramientas Forenses (Live)\Herramientas Forenses (Live)\IDENTIFICACION\IR\_Tools.



## CONCLUSIONES

“Resumen de lo recolectado”

*FIRMA DE LOS TECNICOS DE LEVANTAMIENTO*

A handwritten signature in black ink, appearing to be 'Alan José Martínez Muñoz', written over a horizontal line.

---

Alan José Martínez Muñoz  
Técnico de Levantamiento  
Firma