



Instituto Tecnológico de Las Américas

Tecnólogo Informática Forense

Forensia en Vivo

TIF-410

Informe de Análisis

Fecha: 31/10/2024

Caso: Acceso no autorizado

Numero de caso: 13466-5891

Antecedentes

El día 15 de octubre de 2024, a las 9:15 AM, Se desplazó la unidad de levantamiento de evidencias electrónicas del Departamento de Informática Forense de LabsForensicX en respuesta a una solicitud de Edgar Emil, Rector del Instituto Tecnológico de las Américas (ITLA), ubicado en La Caleta, Boca Chica, República Dominicana. La unidad de recolección estuvo conformada por Alan José Martínez Muñoz (Técnico de levantamiento), Pedro Navaja (Chofer) y Julio José (Fotógrafo).

El desplazamiento de la unidad se realizó debido a una posible acción ilícita cometida por un individuo identificado como Ángel Gabriel. Se sospecha que este accedió de manera no autorizada al sitio web sigeiacademico.itla.edu.do utilizando las credenciales de diversos estudiantes con la intención de modificar contraseñas sin su consentimiento.

Durante el levantamiento, el equipo de LabsForensicX recolectó una laptop marca Lenovo, color azul, modelo IdeaPad 3 15ADAD5. En la recolección de la evidencia, se realizó un volcado completo de la memoria RAM de dicho dispositivo, asegurando la preservación de datos volátiles para el análisis forense. Dicho volcado de memoria RAM, se encuentra almacenado en disco duro SSD marca Fanxiang, modelo S101, que lo portaba el técnico de levantamiento Alan José Martínez Muñoz.


Objetivo del levantamiento

Este proceso busca confirmar las acciones supuestamente realizadas por Ángel Gabriel y su intento de modificar credenciales de estudiantes en el sistema académico del ITLA. La institución afectada, dedicada a la formación tecnológica de nivel superior, quienes proporcionaron acceso a la información y a las instalaciones necesarias para la recolección de evidencia, colaborando en todo momento para aclarar los hechos.

Descripción del equipo o dispositivo

No.	Fotografía	Descripción
-----	------------	-------------

1		<p>Laptop Lenovo, color azul, modelo del dispositivo IdeaPad 3 15ADAD5, recolectado encendido, número de serie PF2ELGQ8.</p>
---	--	--

	<p>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.</p>

Procedimientos técnicos realizados

Preservación

- Se procedió a calcular el valor hash del volcado de memoria RAM, antes de su análisis y después del análisis.
- Se almacenó el volcado de la memoria RAM en un dispositivo de almacenamiento seguro, en este caso un SSD.
- Se utilizó la herramienta Magnet Capture RAM, para poder adquirir la información de la memoria RAM.

Análisis

- Se montó el volcado de memoria RAM en la herramienta de FTK Imager para su análisis.
- Se utilizó la técnica del uso de expresiones regulares para filtrar información y dar con lo sucedido.

Documentación

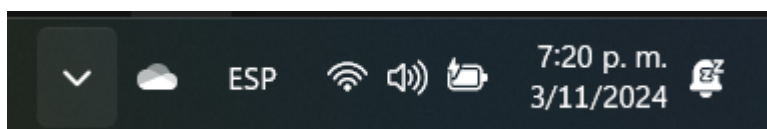
- Se procedió a documentar cada herramienta o cada comando utilizados durante el análisis.
- Se procedió a documentar lo encontrado durante el análisis.

Programas y software utilizados

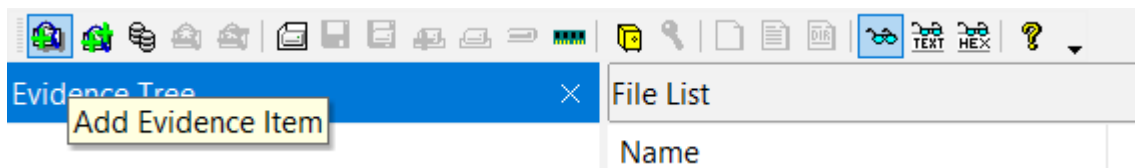
	<p>Software forense utilizado para crear copias exactas (imágenes) de discos duros y otros dispositivos de almacenamiento. Permite visualizar archivos y realizar análisis sin alterar la evidencia original, preservando su integridad.</p>
	<p>Herramienta de captura de pantalla que permite realizar capturas rápidas de cualquier área en la pantalla y editarlas o compartirlas fácilmente.</p>
	<p>Herramienta que genera hashes MD5 de archivos. Se usa comúnmente en informática forense para verificar la integridad de archivos y asegurar que no han sido modificados durante el análisis.</p>
	<p>Procesador de textos de Microsoft que permite redactar, editar y dar formato a documentos. Es ampliamente utilizado para crear informes y documentación, incluyendo reportes forenses</p>

Hallazgos

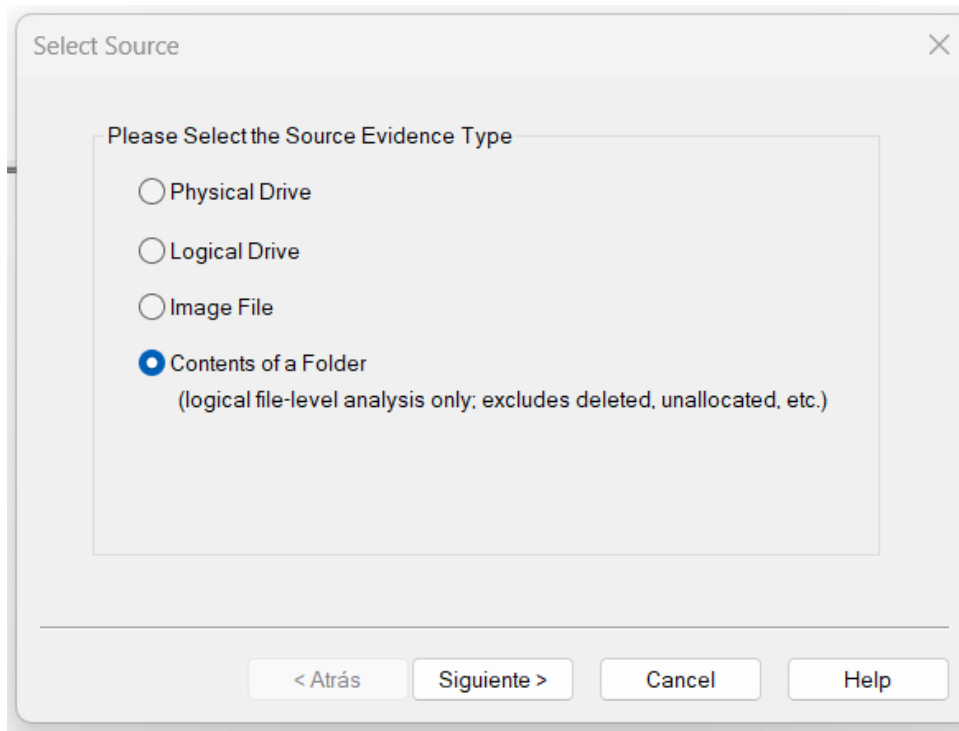
Se registró un intento de acceso a la plataforma virtual de la institución del ITLA, con una credencial de un estudiante 20231319@itla.edu.do. Donde también se intento un cambio de credenciales el cual no pudo ser exitoso.



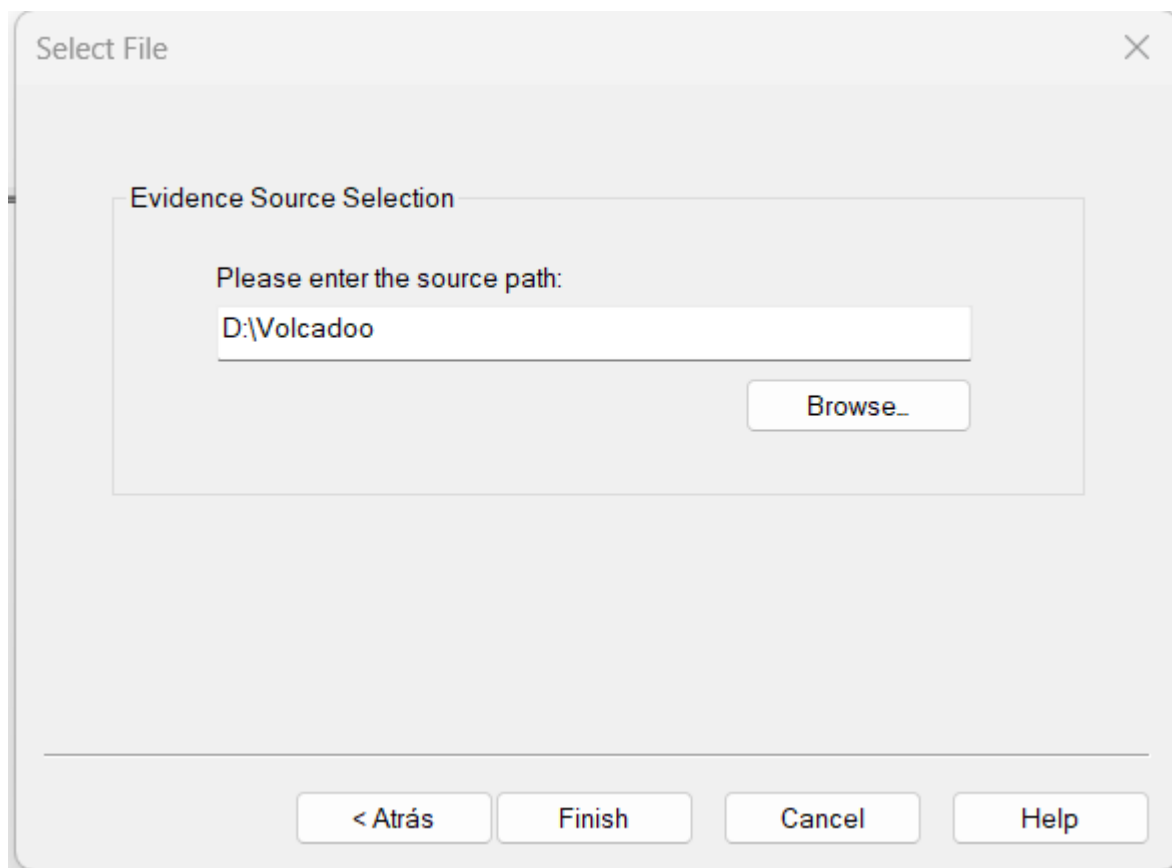
Seleccionamos el icono de añadir evidencia



Luego seleccionamos el tipo de evidencia



Seleccionamos la ruta donde tenemos almacenado nuestro volcado de memoria RAM.



Ya tenemos nuestro volcado de RAM montado en la herramienta FTK Imager.

Evidence Tree

Volcadoo

D:\Volcadoo

File List

Name	Size	Type	Date Modified
RAM.raw	19,906,560	Regular File	16/10/2024 7:15:26...

Custom Content Sources

Evidence:File System|Path|File

Options

New

Edit

Remove

Remove All

Create Image

Properties

Hex Value In...

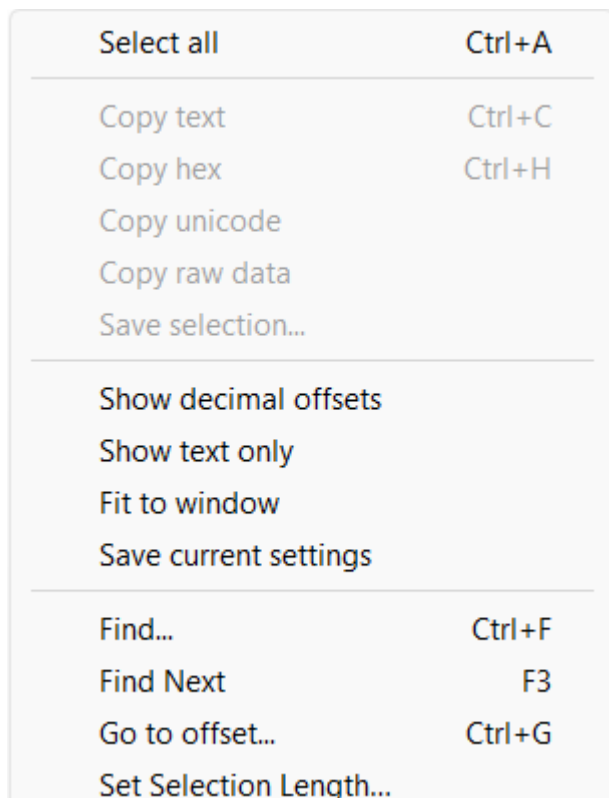
Custom Con...

00000000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000140	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000150	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000200	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000210	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000220	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000230	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000240	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000250	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

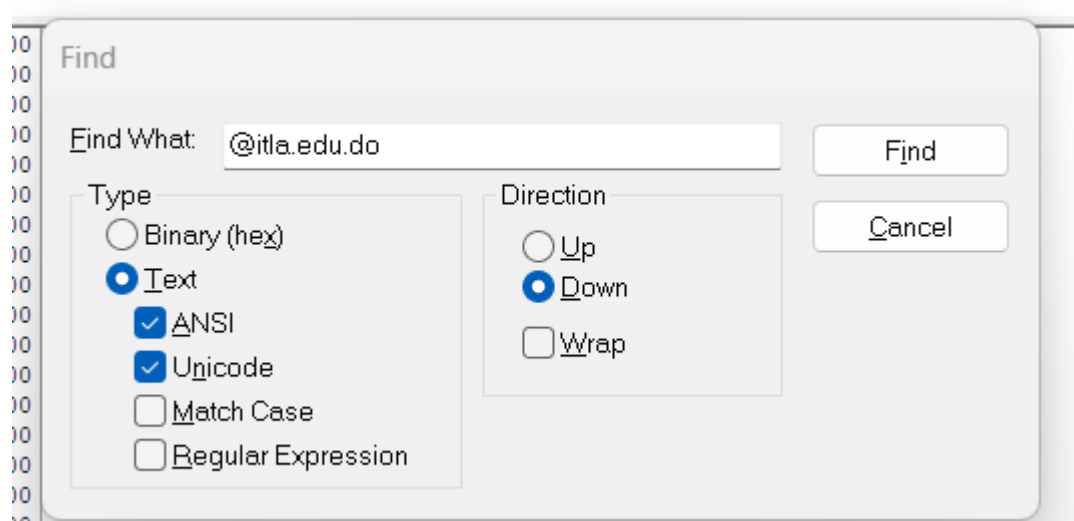
Cursor pos = 0

Listed: 1 Selected: 1 Volcadoo/D:\Volcadoo/RAM.raw

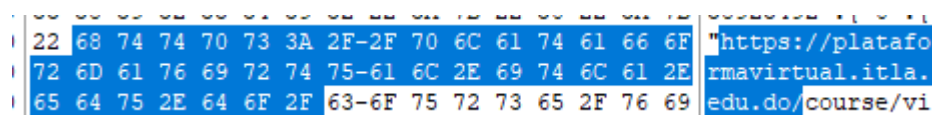
Seleccionamos la opción de Find, esto se hace haciendo un clic derecho en el recuadro de abajo.



Escribiremos los caracteres que deseamos filtrar en nuestro buscador



Se ingresó a la plataforma de la institución.



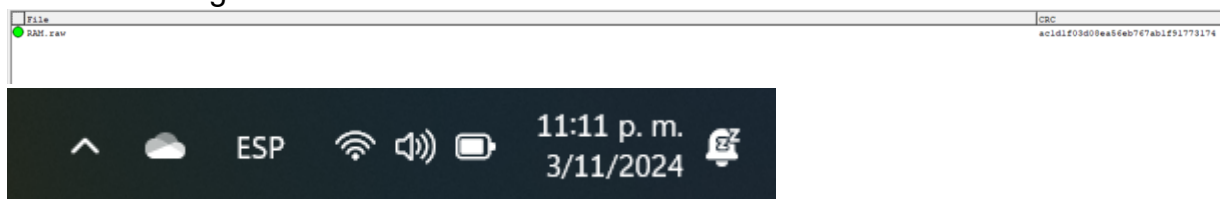
Podemos ver que se encontró la matriculación de un estudiante

001098dc0	00 73 00 65 00 72 00 5F-00 69 00 64 00 00 00 1F	-s-e-r-.i-d----
001098dd0	00 00 00 15 00 00 00 32-00 30 00 32 00 33 00 31	-----2-0-2-3-1
001098de0	00 33 00 31 00 39 00 40-00 69 00 74 00 6C 00 61	-3-1-9-@-i-t-l-a
001098df0	00 2E 00 65 00 64 00 75-00 2E 00 64 00 6F 00 00	-.e-d-u-.d-o--

Intento de modificación de contraseña

0002374d0	77 00 3E 72 03 73 73 0C-74 73 47 72 03 04 30 03	w-_results0110v1
0002374e0	65 77 00 43 68 61 6E 67-65 50 61 73 73 77 6F 72	ew-ChangePasswor
0002374f0	64 5F 43 68 61 6E 67 65-50 61 73 73 77 6F 72 64	c_ChangePassword
000237500	56 69 65 77 00 58 6D 6C-44 65 73 69 67 6E 65 72	View-XmlDesigner

Valor hash luego del análisis.



Conclusión

Tras el análisis del volcado de memoria, se ha confirmado que hubo acceso a la plataforma virtual del ITLA, se identificaron registros que indican el uso de credenciales de un correo electrónico que le pertenece a un estudiante de la institución. Por último, se encontró un intento de un cambio de contraseña.

Firma del encargado de Análisis

Nombre

Alan José Martínez Muñoz