Universidad Tecnología de México

Docente: Roberto Corona Pizano

Maestría: Seguridad de Tecnología de Información

Materia: Inteligencia en Seguridad de TI

Integrantes:

Rodríguez Estrella Edgar Sebastián

Hernández Gálvez Jorge Luis Alfredo

Balanzario Martínez Daniel

Canuto Solis Emilio Israel

Ciclo: 25 - 1

Fecha de entrega: 19/11/2024

Actividad: Entregable 1° Sesión Presencial

Índice

Tabla de imágenes.

Introducción

Para la elaboración de la siguiente práctica, los alumnos por equipos realizarán el análisis de dos documentos previamente proporcionados por el docente durante la sesión presencial. Para ello haremos uso de dos herramientas: Autopsy y VirusTotal.

Autopsy

Es una plataforma de análisis forense digital ampliamente utilizada en investigaciones de ciberseguridad y criminalística digital. Esta herramienta permite:

- Examinar discos duros, tarjetas de memoria, teléfonos móviles y otros dispositivos de almacenamiento.
- Recuperar archivos eliminados y buscar archivos específicos por nombre, extensión o tamaño.
- Analizar registros de actividad del sistema, incluyendo el historial del usuario y accesos a dispositivos.
- Rastrear comunicaciones en redes sociales y examinar transacciones de correo electrónico.
- Obtenga información detallada sobre la actividad del sistema y posibles anomalías.

El objetivo inicial será hacer uso de Autopsy para analizar los documentos, extrayendo información clave como los **hashes** (valores únicos que identifican un archivo). Esto nos permitirá realizar una comparativa con los documentos originales para determinar si hay correlaciones o alteraciones, verificando así su autenticidad.

Posteriormente, con el apoyo de **VirusTotal**, se profundizará en el análisis de los hashes obtenidos. **VirusTotal** es una plataforma en línea que proporciona información sobre el contexto de amenazas cibernéticas, ayudando a identificar y clasificar elementos maliciosos mediante:

- Análisis de archivos, URLs, direcciones IP y dominios sospechosos.
- Proporcionar información sobre la reputación de archivos y su relación con amenazas conocidas.
- Detección de patrones de comportamiento malicioso basada en bases de datos colaborativas de seguridad.

Haciendo uso de VirusTotal podremos evaluar los hashes extraídos, determinando si alguno corresponde a archivos potencialmente maliciosos o que representan un riesgo de seguridad. Esta actividad nos permitirá clasificar y documentar los hallazgos, así podremos desarrollar una comprensión más detallada de los riesgos asociados y reforzar habilidades clave en ciberseguridad y análisis forense digital.

Desarrollo

En la presente practica se elaborará un análisis forense para varias imágenes proporcionadas por el profesor durante la clase. Para realizar lo anterior se utilizará el software Autopsy.

Se proporcionan dos imágenes para analizar, en las cuales se extraerán hashes para poder analizar estos y saber si son archivos maliciosos, estos hashes serian el “MD5” y el “SHA-256”.

En el marco de una simulación de investigación de cibercrimen, se cuenta con una imagen forense digital como evidencia clave. Esta imagen, se planteará como obtenida tras la incautación de un dispositivo en un operativo contra actividades ilícitas, contendrá una variedad de elementos para su análisis detallado. Entre los datos recuperados se encontrarán correos electrónicos con contenido sospechoso, fotografías relacionadas con actividades ilegales, documentos con patrones de comportamiento malicioso y rastros de posibles transacciones vinculadas al tráfico de drogas.

El objetivo de esta práctica será recrear un escenario realista en el que se apliquen técnicas forenses para identificar, clasificar y analizar la información contenida en la imagen. Con el uso de herramientas como Autopsy, se extraerán hashes de los archivos encontrados, aplicando algoritmos como MD5 y SHA-256 para verificar su autenticidad y detectar posibles alteraciones. Este proceso permitirá identificar elementos maliciosos y reconstruir una narrativa de las actividades realizadas en el dispositivo, aportando lecciones valiosas sobre el manejo de evidencia digital y destacando la importancia del análisis ético y preciso en investigaciones de ciberseguridad.

1. Apertura de caso con herramienta Autopsy.

Inicialización de Autopsy.

Iniciamos la aplicación de Autopsy y seleccionamos la opción de New case, para poder realizar un nuevo caso para analizar los archivos que agregaremos.

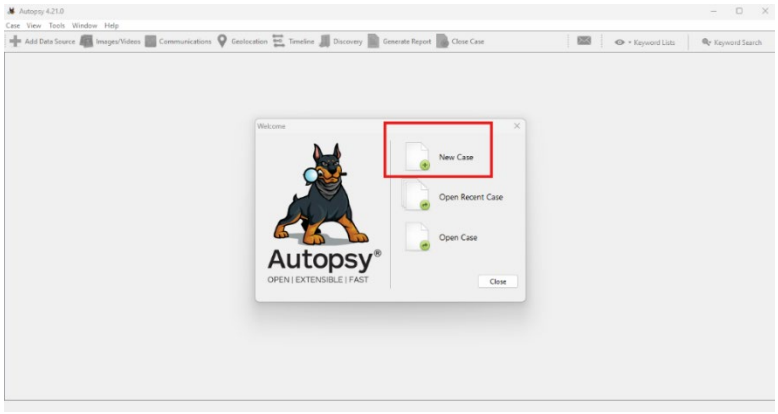

Imagen 1. Nuevo caso en Autopsy.

Información adicional para el caso.

A continuación, le damos un nombre a nuestro caso, para este caso será “Pracrica1” y la ruta en donde se guardar nuestro caso, esto para tener un orden y saber dónde se encuentran almacenados.

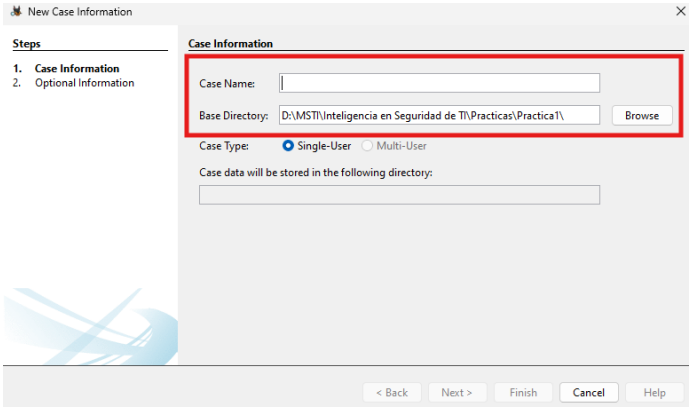

Imagen 2. Datos del caso.

De igual forma llenaremos un formulario con datos del personal que está llevando a cabo dicho caso, esto nos servirá para que nos genere un reporte con información del analista del caso.

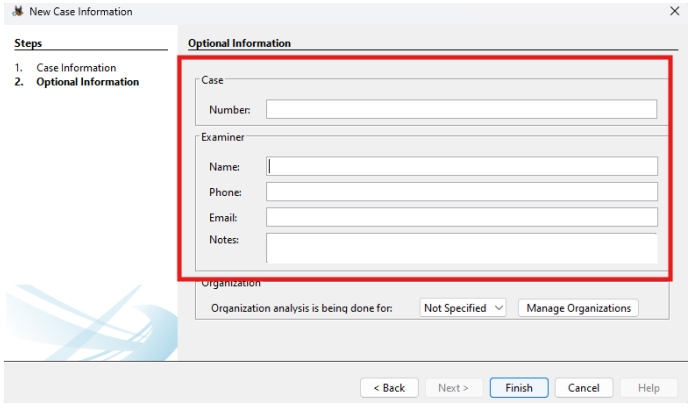

Imagen 3. Información adicional del caso.

Selección de datos.

A continuación, pasaremos a agregar los archivos que analizaremos para esta primera parte solo podremos analizar un primer archivo y cuando le demos a la opción de finish será el indicativo que ha terminado de analizar el primer archivo, posteriormente agregaremos el segundo archivo con las herramientas en la parte superior donde dice add data sourse y así podremos visualizar ambos archivos de nuestro caso.

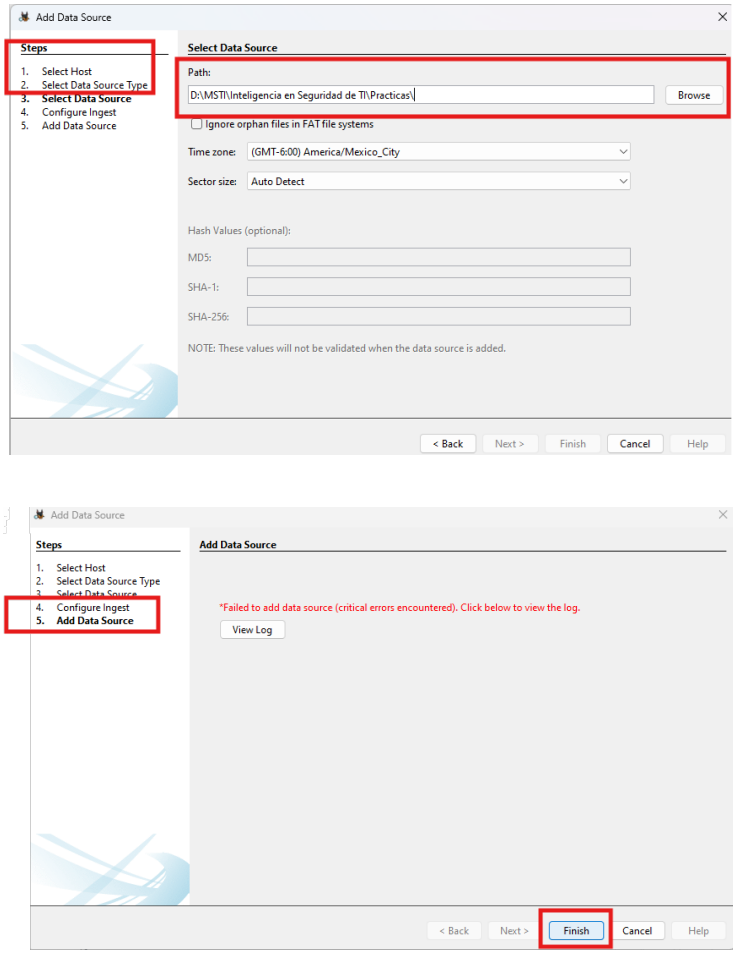

Imagen 4. Configuración de la imagen en Autopsy.

Visualización de archivos.

A continuación, podemos observar todos los archivos desplegados en el menú de lado izquierdo y podremos ir revisando uno a uno para conocer un poco más de su contenido, así como las rutas donde estos mismos se encuentran y algunos motores de búsqueda, en la parte inferior podemos obtener un resumen de los contenidos de los archivos con mayor detalle.

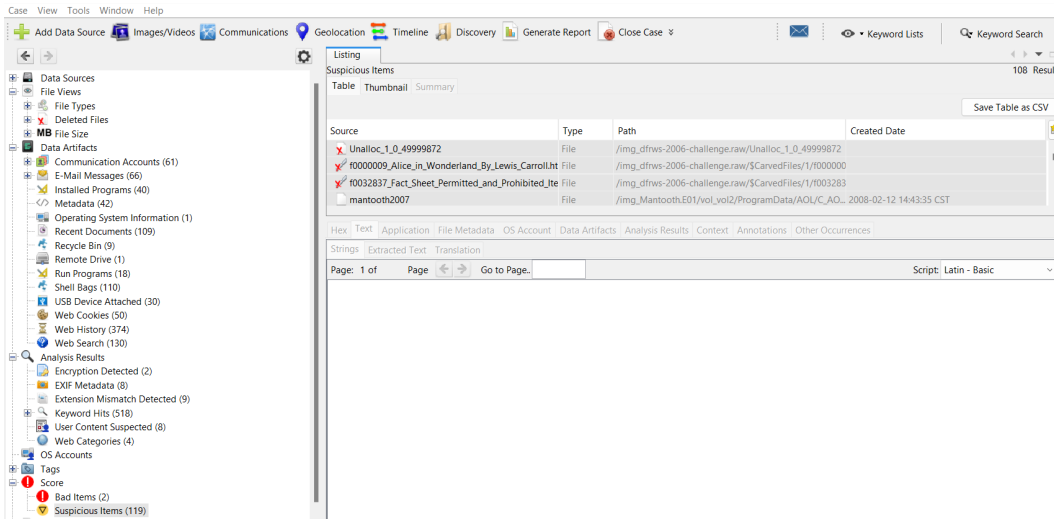

Imagen 5. Visualización de archivos de imagen.

2. Extracción de hashes con Autopsy.

Extracción de hashes

Para extraer hashes de los archivos que se consideran maliciosos, exportamos los archivos, para ello en el apartado de Results de lado derecho seleccionamos los archivos y dando click derecho escogemos la opción de extract file.

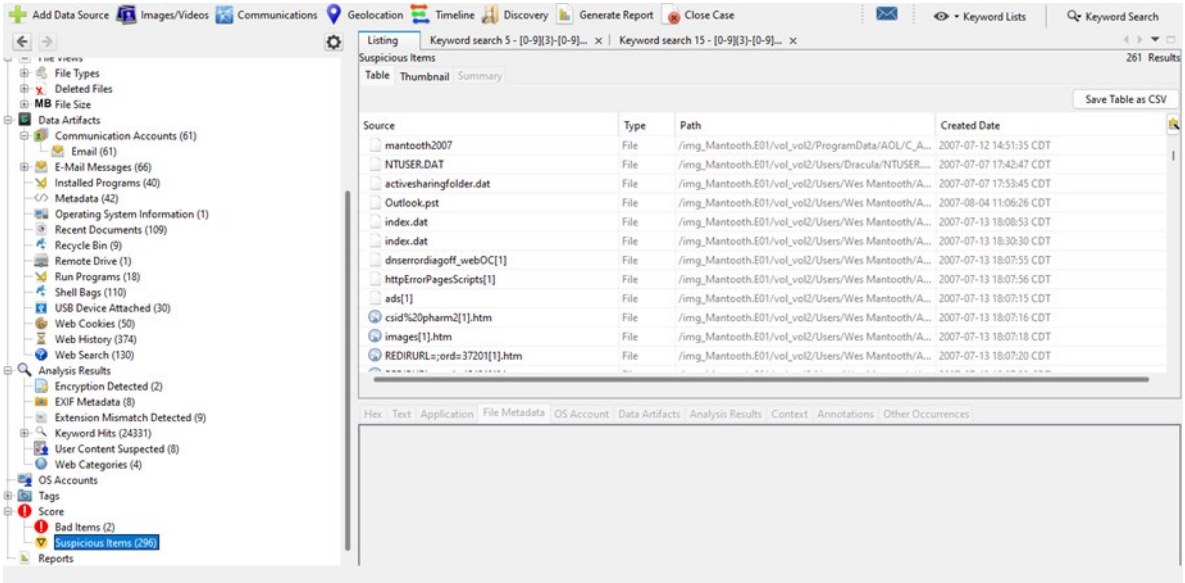

Imagen 6. Visualización de archivos sospechosos.

Los guardamos en una carpeta, dándole clic a Extract Files, para que estos archivos podamos guardarlos en una ubicación de nosotros deseemos en nuestro explorador de archivos ya que haremos uso de ellos más adelante para la comparación de Hashes.

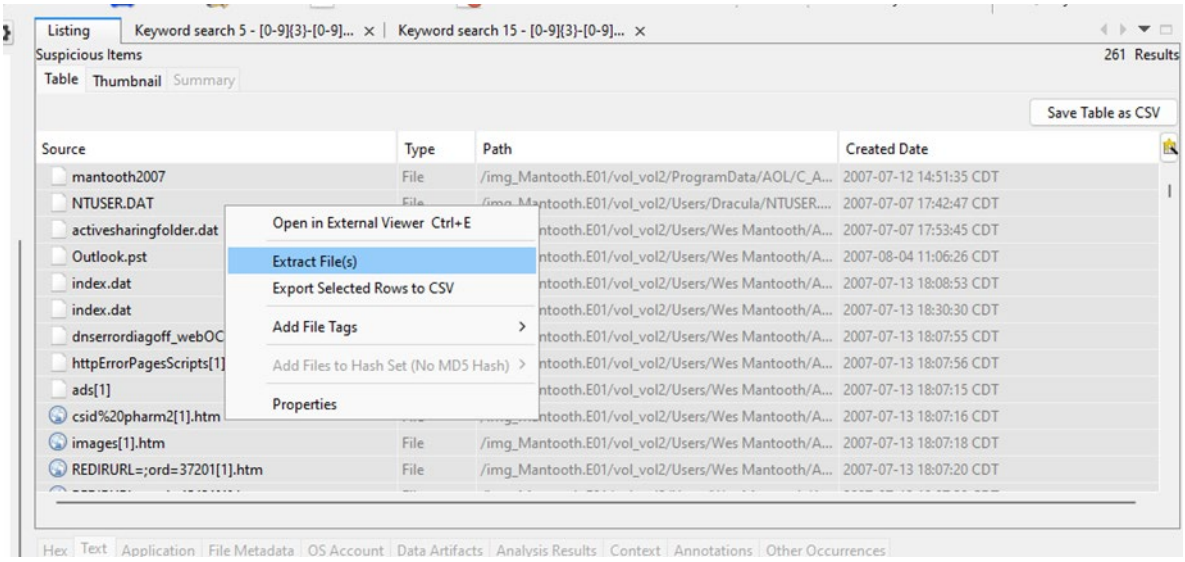

Imagen 7. Extracción de archivos.

Ya exportados en una carpeta en alguna carpeta que decidamos darle la ruta donde guardaremos dichos archivos exportados.

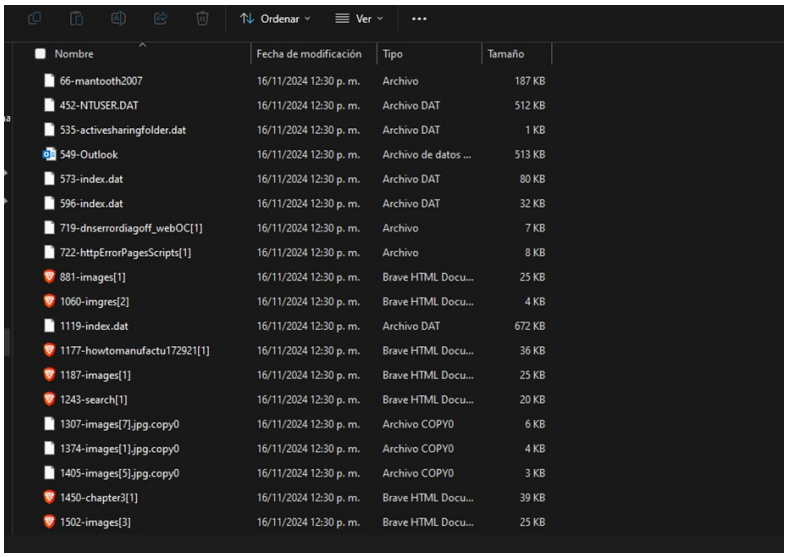

Imagen 8. Obtencion de archivos.

Para la obtención de Hash haremos uso de la siguiente página web, la cual nos ayuda a calcular los Hashes de los archivos que previamente extrajimos.

https://md5file.com/calculator

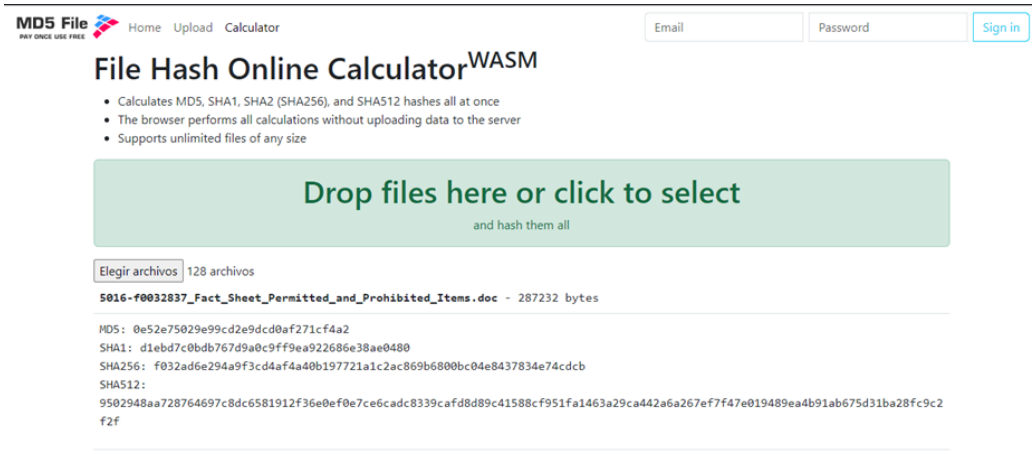

Imagen 9. Extracción de hashes.

Le damos en el apartado de Drop files para buscar en nuestro directorio los archivos que extrajimos, para poder cargarlos en la herramienta web para que nos ayude a calcular los Hashes de estos mismos archivos.

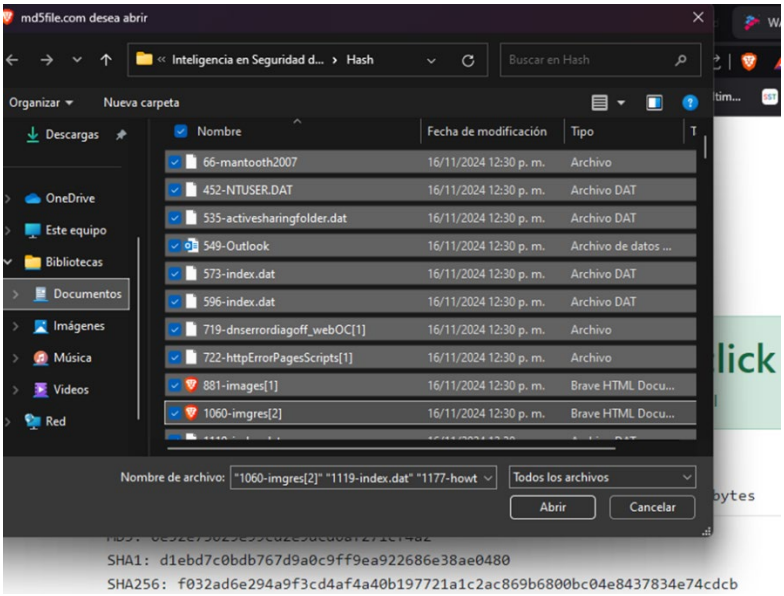

Imagen 10. Inserción de archivos.

Después del proceso de agregar los archivos, obtendremos los siguientes resultados con una serie de cadenas Hashes.

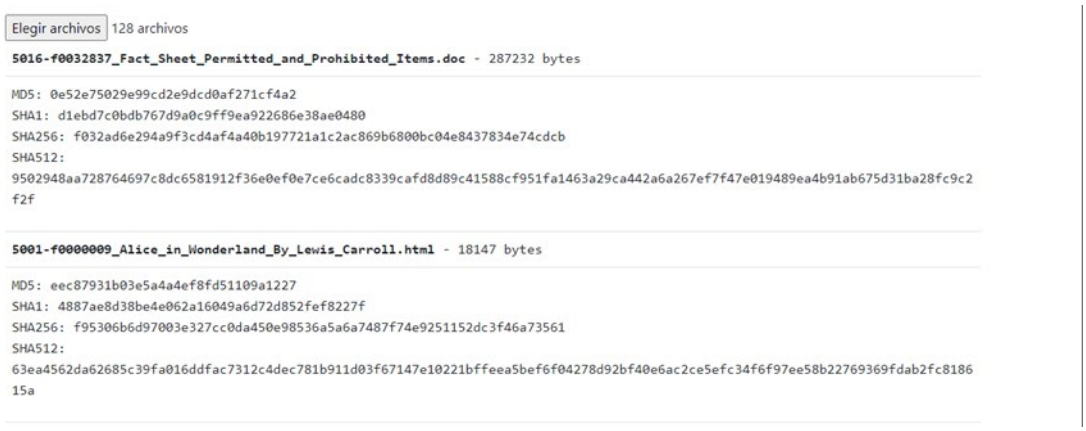

Imagen 11. Visualización de hashes

Pasamos a guardar el resultado de los Hashes obtenidos en un formato de txt para poder hacer uso de ellos con el código en Python que ejecutaremos en la máquina virtual de Kali.

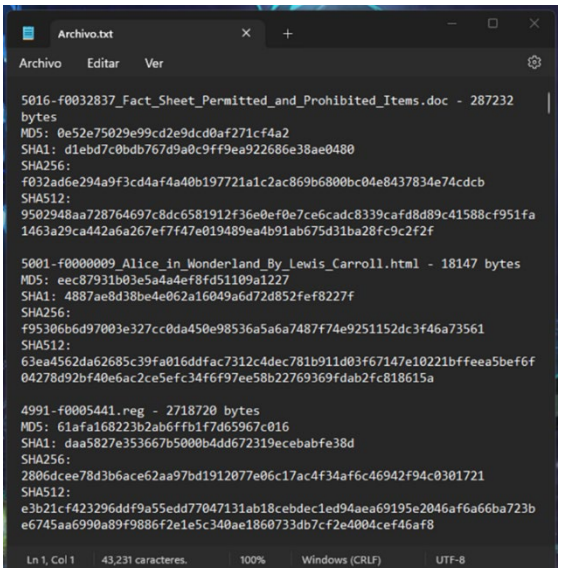

Imagen 12. Resultado de hashes.

Usamos el siguiente código para ordenar la información por columnas y convertirlo en .csv el cual es una hoja de cálculo como las que tiene Windows de Excel, pero en un software de Linux.

```
1  import re
2  import pandas as pd
3
4  # Archivo de entrada y salida
5  input_file = "Archivo.txt"  # Reemplaza con el nombre de tu archivo
6  output_file = "archivos_separados.csv"  # Usar .csv
7
8  # Leer el archivo de texto
9  with open(input_file, "r") as file:
10     lines = file.read().split("\n\n")  # Separar por bloques de
11 archivos
12
13 # Expresión regular para extraer datos
```

```
pattern = re.compile(
    r"^(.*) - (\d+ bytes)\nMD5: (.*)\nSHA1: (.*)\nSHA256:
(.*)\nSHA512: (.*)$"
)

# Procesar datos
data = []
for block in lines:
    match = pattern.match(block.strip())
    if match:
        data.append(match.groups())

# Crear un DataFrame y guardar en CSV
columns = ["Nombre del archivo", "Tamaño", "MD5", "SHA1", "SHA256",
"SHA512"]
df = pd.DataFrame(data, columns=columns)
df.to_csv(output_file, index=False)  # Guardar en formato CSV

print(f"Datos guardados en {output_file}")
```

Imagen 13. Código Python de ordenamiento de información

3. Análisis de hashes con código Python.

Dicho código en Python lo ejecutamos en una de las máquinas virtuales de Kali, con el objetivo de que hiciera el análisis de los Hashes y obtener el estatus de los mismo, si estos eran o no maliciosos o en todo caso un falso positivo.

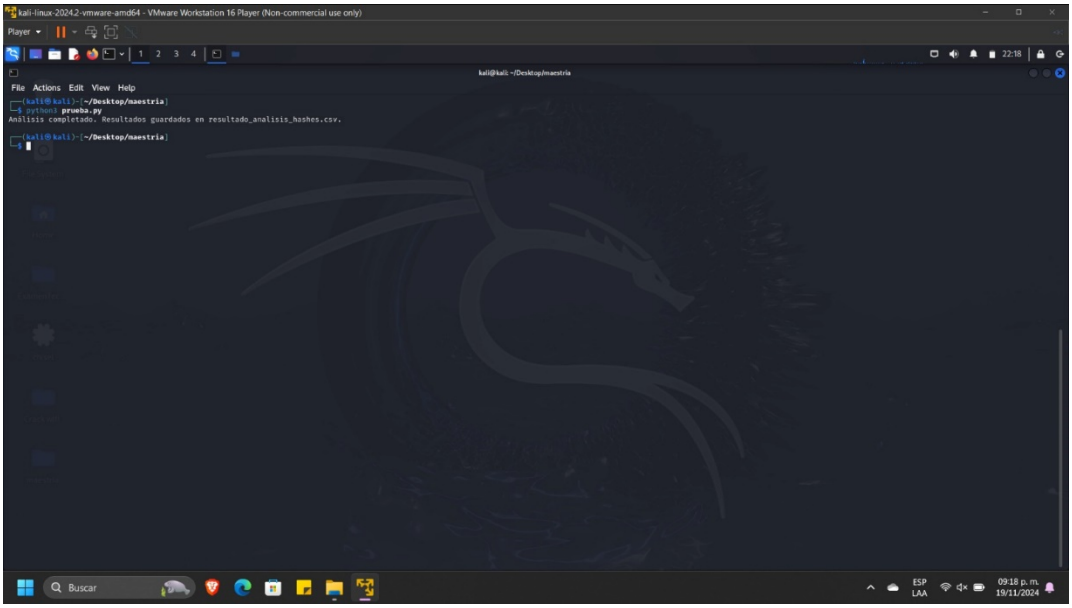

Imagen 14. Ejecución de análisis de hashes.

Posteriormente al terminar la ejecución de dicho código en Python nos arrojó los siguientes formatos, con los cuales pudimos generar las gráficas mediante la herramienta de Power BI.

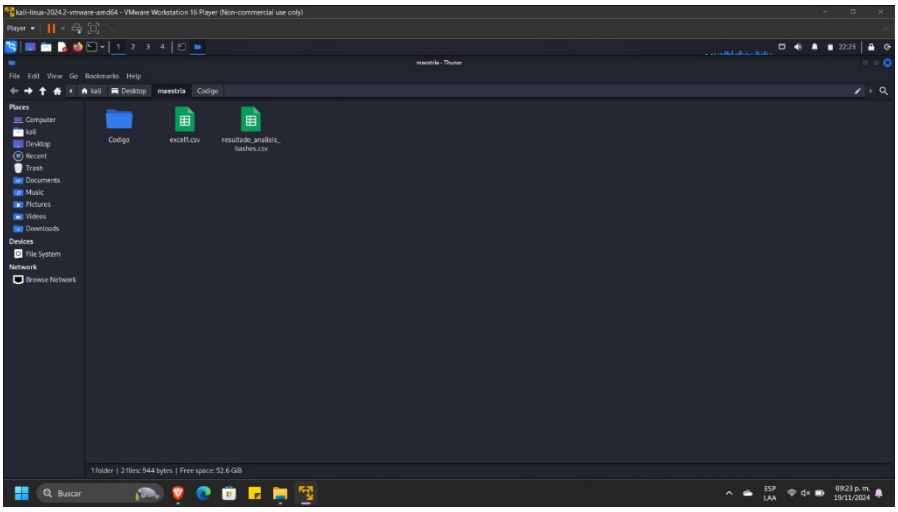

Imagen 15. Resultado de hashes.

Al momento de abrir el formato de Excel que nos generó el código en Python podremos pasar a la representación de los Hashes en un Dashboard para un mejor análisis de estos.

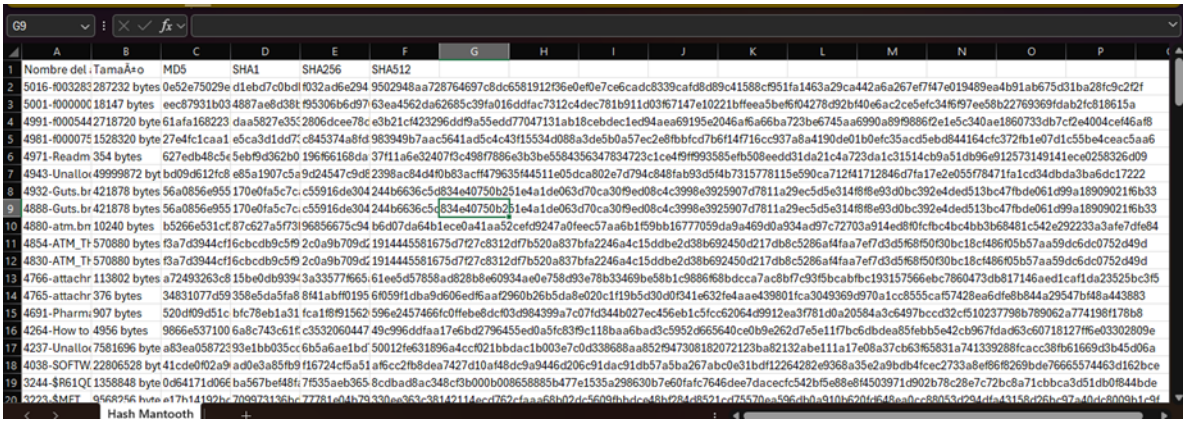

Imagen 16. Visualizacion de hashes obtenidos.

4. Visualización de resultados.

Representación de resultados (Dashboard).

Por último, paso, una vez obtenidos los resultados de los hashes, por medio de diferentes pasos anteriores, a continuación, podemos observar un pequeño dashboard acerca de lo que se logró, mostrando como resultado la evaluación de los hashes de las imágenes proporcionadas en la clase.

Se puede observar diferentes tipos de archivos dentro de las imágenes, con su respectiva evaluación de estos.

Mediante el análisis de los archivos .CSV en los que se encuentran toda la información necesaria para la evaluación de los hashes. Se puede observar en las imágenes siguientes los resultados de cada hash con su respectivo archivo. Dentro de los cuales se observa que algunos son y no maliciosos.

De acuerdo con los archivos mostrados, se desarrolla un breve dashboard, el cual representa la información obtenida de una forma mas gráfica y con mejor visualización de los resultados.

Name	MD5 Hash	SHA-256 Hash	TypeFile	Evaluacion de riesgo
f0000000.html	ec89111e45da8265b641655d0f68725e	66ab80041efaebe3f6f0b692fbb08b01820c3d9a94110724bdc89a616bbcead0	html	Hash no encontrado
f0000009_Alice_in_Wonderland_By_Lewis_Carroll.html	eec87931b03e5a4a4ef8fd51109a1227	f95306b6d97003e327cc0da450e98536a5a6a7487f74e9251152dc3f46a73561	html	0
f0003868.jpg	daf4205574abd6919b10ca8be92d17a3	4d09b003550f210dd77ada37c08026f92a2a6db522b8ba3726dea85e00ae5355	jpg	Hash no encontrado
f0004436_A_STUDY_IN_SCARLET_1_1.html	799ad2d2f2f1f17657338d98c97559c4	fecf4388a938104402b0f98b8a9a90c4fb9b60c89d3cf1b9c32019b5727d2a3e	html	Hash no encontrado
f0004456_1_Stave_1_Marley_s_Ghost.html	f4481ed348d3d59c5dad80afeb0341f9	a80826fae91e3bdfe8c148f240ab79b3a3989ad41d8bf582782d32310b744779	html	Hash no encontrado
f0007964_National_Park_Service.doc	8d2a9a284e078805ada47db191f35244	1b6a495892aac4826af72125b62b20c82bfc519087870aeb03ae8d5bd378c7f2	doc	Hash no encontrado
f0008285.jpg	4efc6c572683878efd8f3404ddaded7b	8e036fa838def99d95aea2e5780df34cd1b2b28302a010e60c8a030377c45919	jpg	Hash no encontrado
f0012222.jpg	b070beae1606f67a342bc5f78c29c743	da8bd3d361bf4844c47a39453fbe2338def0571aee2b839b8de3a276ea061533	jpg	Hash no encontrado
f0027496_Comedy_of_Errors_Entire_Play.html	76e51ff4adcaaa7b64da061636e532f3	c405e7d6d79d98afa78bd268efeef63e8fc57376efcd2f987eaea9bea5e5bd26	html	Hash no encontrado
f0027607.jpg	fe7e7ac67709f2d9c2483aa98c681b99	e30ec1bf9236dcaa920da5a1dc4ec00219b344929e1caf0c6089e4dbdbd76fab	jpg	Hash no encontrado
f0027978.html	8593b9c26ec20d90660b369ca59a5904	001f314742ac697659705b7799eb72c8c7b2643e1f8a6fb7a2079ec62b46c05e	html	Hash no encontrado
f0028244_Chapter_cxxxiv_THE_CHASE_SECOND_DAY.html	bffb62273976ca98240d4bb74abb50f5	610c682f3de6d1769f32a1caefd7dbad014f799142b5ee9f453ab669294dfabc	html	Hash no encontrado
f0028307.html	7a03dee0e5b82b89c1a81ff6a97c8f82	b7751ed2a8f3cd4f2b99f2c6819496a40b5d834363e63940f7c2d60dcce7332e	html	Hash no encontrado
f0028439_4n6rodeo3_fix_copy.zip	ebabde39ba44d38888dd82606980498a	12480cd0b022b38e970880202989 31b8ffb19c2aaedbc4da0647aa42fef9f41d	zip	Hash no encontrado
f0028729_file1.zip	9a4c2d3a9bd203eb39c9f954a3c997e4	54349e4a2c394acf1b8fec361b82caee21d8b10aaea55aecc9e9c6aa3f6b3e2d	zip	Hash no encontrado
f0029529_The_Tempest_Entire_Play.html	158496c522d97b7389c9907cae777ac1	5a4edb7c73289897196e3f6dd1564f890a0d65a0240f0081a233384f0c6ce3d4	html	Hash no encontrado
f0032837_Fact_Sheet_Permitted_and_Prohibited_Items.doc	0e52e75029e99cd2e9dcd0af271cf4a2	f032ad6e294a9f3cd4af4a40b197721a1c2ac869b6800bc04e8437834e74cdcb	doc	0
f0036292.jpg	2fae8770cc013d22e9ea1c070f2f509b	5b4425d3de9a334be3edde1600d0ac77fd228d9153e0d759a330d4fbf60d4b29	jpg	Hash no encontrado
f0041611.jpg	7cce072e518fd72484c97adb1b4be08e	50872aa2c45802ddd86705e0fe4a4de3f04fbe0d1899b140af0a4aa3b01b6bdf	jpg	Hash no encontrado
f0043434.jpg	c0da37b3f1a07af790e6e9171cedc4d2	2c0ab159dabd04349d80105dc005c0b0ebe0e2f18ec6e7410856d488c1dbf465	jpg	Hash no encontrado
f0045566.jpg	2320fe9c41eaddb864a56c2ddc4dd186	503bec56f2d2a02273496f79857d3a915b833ec5268a76c178769cabedb1f141	jpg	Hash no encontrado
f0045964_Statements_of_Financial_Condition.doc	109284cc5abddc83879a29785795fd75	8751b4cf9e1b3d3b8a72f6578fdd1f88a6fa763cafa162768920d37f972941ea	doc	0
f0046910.jpg	db32b271506b2f49747919576 27c61cc	f49edfe8e6919bcf85feb07786dcef46cceec51e462c1faf18ece912bc2c26de	jpg	Hash no encontrado

Name	MD5	SHA256	TypeFile	Evaluacion de riesgo
5016-f0032837_Fact_Sheet_Permitted_and_Prohibited_Items.doc	0e52e75029e99cd2e9dcd0af271c	f032ad6e294a9f3cd4af4a40b197721a	doc	0
5001-f0000009_Alice_in_Wonderland_By_Lewis_Carroll.html	eec87931b03e5a4a4ef8fd51109a	f95306b6d97003e327cc0da450e98536	html	0
4991-f0005441.reg	61afa168223b2ab6ffb1f7d65967	2806dcee78d3b6ace62aa97bd191207	Archivo de registros	0
4981-f0000757.reg	27e4fc1caa1a891f0	aedecdf79602	c845374a8fd37a95b604db99d0f9d57(	Archivo de registros	Hash no encontrado
4971-Readme.txt	627edb48c5eb4c22891bafba5fb8	196f66168daf1455b53923e7c9e1bfa4f	txt	Hash no encontrado
4943-Unalloc_4942_0_49999872	bd09d612fc8b3f92662b98f9456f2	9d24547c9d8a17602ee5a8ecf960ff8c	Desconocido	0
4932-Guts.bmp	56a0856e955784f8332a8affd1a2	c55916de30497742c02bf88b4e7d5ad	Desconocido	Hash no encontrado
4888-Guts.bmp	56a0856e955784f8332a8affd1a2	c55916de30497742c02bf88b4e7d5ad	Desconocido	Hash no encontrado
4880-atm.bmp	b5266e531cf285832e486ed6625b	96856675c94f3c57860dddfe779d8de6	Desconocido	Hash no encontrado
4854-ATM_THEFTS1.ppt	f3a7d3944cf180492662b98ecc51	2c0a9b709d2bcbe481feeefb942ff949	Archivo de Powepoint	0
4830-ATM_THEFTS1.ppt	f3a7d3944cf180492662b98ecc51	2c0a9b709d2bcbe481feeefb942ff949	Archivo de Powepoint	0
4766-attachment1917156117	a72493263c83b0fff8f9101af4204f	3a33577f665a58465cdb78d480d984b	Desconocido	Hash no encontrado
4765-attachment1701374899	34831077d596b1de38f51ee1d148	8f41abff0195910ee7c2e9cdbb067159	Desconocido	Hash no encontrado
4691-Pharmacy.vcs	520df09d51cdb6a3bb773678d04	fca1f8f915620efa023545434d20be7e7	Desconocido	Hash no encontrado
4264-How to Steal Cars.txt	9866e5371005b1e536b7a16d8fb5	c3532060447502f1a4def9ed8396369d	txt	0
4237-Unalloc_4236_3267072_106657792	a83ea058723b2140c1e6ac2e3dc	6b5a6ae1bd7df140d2af06415177239(	Desconocido	0
4038-SOFTWARE	41cde0f02a96746c316eb4e83e84	f16724cf5a5142dd3c2279d95e60dc4b	Desconocido	Hash no encontrado
3244-$R61QDFF.exe	0d64171d0669dacac2c694829e7	7f535aeb3654aab46d6e35aad8a4e7a	ejecutable	26
3223-$MFT	e17b14192bd7225fd20086bc72e	77781e04b79f2ddb5e660fe8f66de99c	Desconocido	Hash no encontrado
3187-NTUSER.DAT	9c0eceb64682cf23835933e21f7f9	71d210d3e4683bf9eac45a3e75571a8	Archivo de datos	0
3119-ntuser.dat.LOG1	217a4a60e65119c343de998361d	258033696a92f9652f5e3d91e9da49f6	Archivo de registros	0
3022-My Sharing Folders.lnk	339f212afd3270c08c80e1c8f544	21965bc1158aa47fd3f76de0ffa2a5e1	Desconocido	Hash no encontrado
3018-My poem.txt_HARDCORE.JPG	e16fffc19575863c840e4f5f1b18cb	45c30206ffad970850f7fbefdc7288773	jpg	0
3007-trout.exe	5ff79967b2e097e938312983 9fba9	cce2942f226c565476a0190603b58eba	ejecutable	1
3004-Revelation.exe	5fbc923249818c4b0489b85c1abf	462b67c7754ae423681755f58d5293bc	ejecutable	45
3002-readme.txt	4f13601b5dfe6b56672fed5fdc206	7113913dd1adfbb166412e132d84fbfe	txt	0
2996-getopt.c	b5a16a384b5a7489c2a2aa60f15	bee37fe66d6fce912ca377be55c0f6b7	Archivo de código fuente C	0
2950-secring.skr	66f6ba488735faa2073036fe65cb4	fcf8ca6009b21be35a2a320f29f6c532e	Desconocido	Hash no encontrado
2948-pubring.pkr	cfe3ab7c21734e795e1c7f9674d0	730733140baed9324eafa11c9a1cfcb9	Desconocido	Hash no encontrado
2931-165183.html	e8f5280b4fa2e352abac1a2322db	d2ee016fcc9f40c0aa7a2719de498e8e	html	Hash no encontrado
2896-Google Image Result for http--glossary_ippaper_com-image	7462e0cac61ee18deb6b6e83a71	c41d305e735b5a504a4ccf257125ee7f	Desconocido	0
2858-readthis.txt_pfah603.jpg	45211e60c4e02e64961dc242efaf	43c2bee19c1c4b5da91080dbc384e62	jpg	Hash no encontrado
2855-readthis.txt	94d1af666b1a813cd05d452cb33	3a2d6563f426acabb245990d63845f26	txt	0
2821-Pharmacy.vcs	520df09d51cdb6a3bb773678d04	fca1f8f915620efa023545434d20be7e7	Desconocido	Hash no encontrado
2819-junction.exe	e387f3de8362c7d9b45e801622cf	e5cce9bb6af1b467f73ca7e42f43ed24	ejecutable	0
2817-How to create and manipulate NTFS junction points.mht	367891bd6d9b441b9a87e492f55	dcb0e04202516d9dd607d0c363bc4b8	Archivo de mail	0
2768-PGPlog4.txt	6b12795e745e639052763ec414ec	19c318a1f271261405fc6c048ada3796	txt	Hash no encontrado
2766-PGPlog3.txt	6fffe02a6e8b7e1cd4d256d4ec69	1c10a4aefb6e1b046f3d190464fa0881	txt	Hash no encontrado
2748-history.dat	fc51fb51fbd361b709bf9dd95dbe	adc61350696e298425618c080d76af27	Archivo de datos	Hash no encontrado
2737-search.rdf	939dcfba9fa92f86bcacb487df9d	451c4475c6c285da263f91049224c87c	Desconocido	0

Imagen 17. Evaluación de hashes.

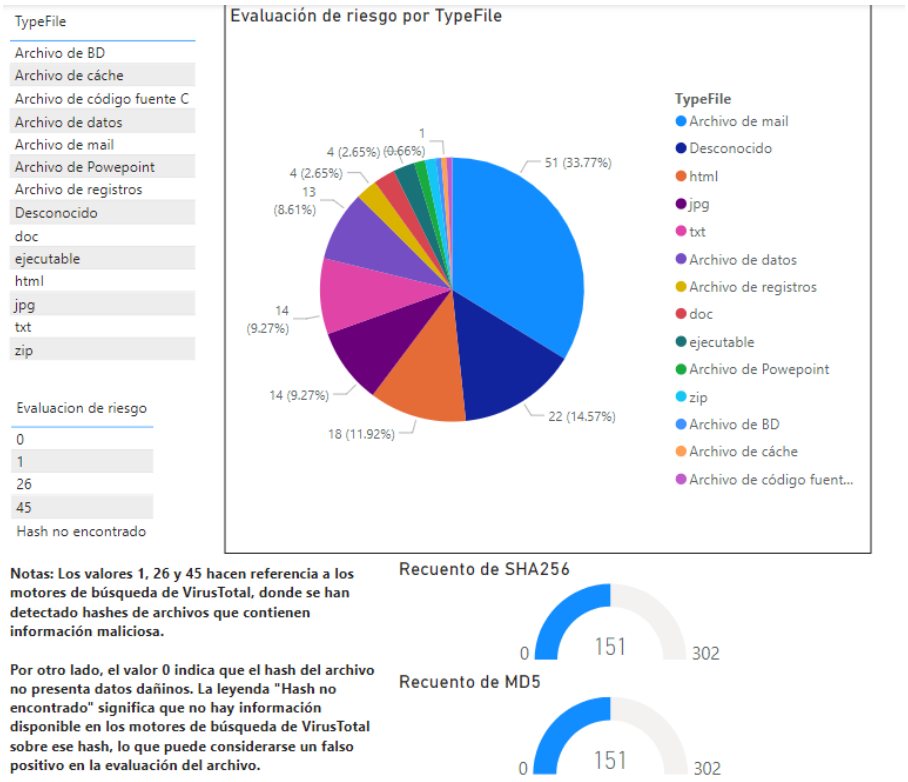

Imagen 18. Dashboard de resultados.

Para poder visualizar el dashboard a detalle se deja el enlace siguiente:

https://myunitecedu-my.sharepoint.com/:u:/g/personal/edgar_rodrigueze_my_unitec_edu_mx/EYzbmjSAMd9LitGTvl743dkBCTXjx084AG4G3lGBD6SPuA?e=edd1KC

Para visualizar todo lo que se realizó para esta práctica proporcionamos el repositorio en Git donde subimos todos nuestros materiales y pruebas realizadas:

https://github.com/Luis-hg14/Reportepractica1.git

Conclusión General

La actividad realizada permitió explorar y aplicar herramientas fundamentales en el análisis forense digital, como Autopsy y VirusTotal, para evaluar la integridad y posibles amenazas de archivos proporcionados. A lo largo del proceso, el equipo desarrolló habilidades esenciales para identificar, analizar y documentar archivos sospechosos, destacando la importancia del trabajo colaborativo y la organización. Esta experiencia no solo reforzó competencias técnicas, sino también la capacidad de gestionar información crítica en

contextos reales. La práctica subrayó la relevancia de mantenerse actualizados en ciberseguridad, ya que las amenazas evolucionan constantemente, y el dominio de estas herramientas es indispensable para enfrentar desafíos en entornos profesionales.

Conclusiones Individuales:

Daniel Balanzario Martínez:

En resumen, la práctica realizada nos sumió en herramientas esenciales del análisis de informática forense, como Autopsy y VirusTotal. Esto nos permitió adquirir habilidades clave en la identificación y evaluación de archivos sospechosos. Sin embargo, a lo largo de toda esta práctica no solo reforzamos nuestras capacidades técnicas, sino que también fortalecimos el trabajo en equipo y la habilidad de documentar efectivamente la información encontrada.

Desde mi punto de vista, estas experiencias refuerzan la necesidad de mantenernos actualizados en el campo de la ciberseguridad, ya que las amenazas evolucionan constantemente. Dominar estas herramientas proporciona la experiencia necesaria para enfrentar casos reales, donde el trabajo colaborativo y la precisión son fundamentales. Además, estas prácticas no solo amplían nuestras competencias técnicas, sino que también nos llevan a reflexionar sobre la ética y el profesionalismo que debemos tener como responsables de la seguridad de la información.

Emilio Israel Canuto Solis:

Esta actividad me ayudo a conocer diversas herramientas que se emplean para el análisis de archivos y así mismo conocer la autenticidad de estos, esto nos permitirá conocer quiénes y que se le ha modificado a un archivo, así mismo conocer el contenido que pudo albergar estos almacenamientos, ya que en ocasiones es necesario conocer la información que estos albergan si se trata de un asuntó de seguridad, ya sea personal o a nivel institucional.

También nos permite conocer si estos mismos archivos pueden ser maliciosos y posiblemente puedan causar un mal mayor a la integridad de las personas o instituciones, es bueno tener un conocimiento en el uso de estas herramientas si nuestro objetivo es enforcarnos en el área de ciberseguridad de manera profesional, ya que nos abrirá más nuestro panorama.

Jorge Luis Alfredo Hernández Gálvez:

Desde mi perspectiva, la actividad representó una oportunidad valiosa e importante para reforzar los conocimientos que tenía sobre el tema, también me ayudo a adquirir conocimientos sobre el uso de herramientas de análisis forense, que vienen siendo fundamentales en el campo de la ciberseguridad y ciberinteligencia. A través del uso de Autopsy y VirusTotal, no solo aprendí a analizar y evaluar archivos, sino también a identificar patrones que podrían indicar alteraciones o riesgos potenciales en los archivos y datos de una empresa, que esto es algo esencial para garantizar la integridad de la información.

Al estar realizando el análisis de los archivos que nos arrojó Autopsy también me di cuenta que es muy importante llevar a cabo un análisis más profundo y buscar adicionalmente más archivos comprometido que no están en la parte de Item Maliciosos, se debe de ser preciso y tener ética al manejar información sensible, ya que estos elementos son indispensables para la confiabilidad de los análisis realizados. Además, comprendí que el dominio de estas herramientas no solo amplía nuestras competencias técnicas, sino que también nos prepara para enfrentar escenarios reales en los que el trabajo en equipo y la toma de decisiones fundamentadas son cruciales.

Por otro lado, esta práctica subrayó la necesidad de mantenerse actualizado en un campo tan dinámico como la seguridad de TI, donde las amenazas evolucionan rápidamente y exigen soluciones innovadoras y efectivas. En este sentido, la actividad me inspiró a seguir profundizando en el conocimiento técnico y a fortalecer habilidades que me permitan contribuir de manera significativa al ámbito profesional.

Edgar Sebastián Rodríguez Estrella

En la presente actividad, se llevó a cabo un análisis forense básico utilizando diversas herramientas de inteligencia de seguridad, tanto a través de software especializado como de recursos disponibles en línea. A lo largo de esta práctica, tuvimos la oportunidad de verificar la integridad de los archivos de imagen proporcionados durante la clase. Esto se logró mediante la obtención de los hashes de cada archivo, lo que no solo nos permitió confirmar la integridad de los datos, sino también detectar posibles amenazas, como malware o virus informáticos. El uso de herramientas como Autopsy, junto con máquinas virtuales de Linux y scripts en Python, fue fundamental para llevar a cabo este análisis. Estas tecnologías nos brindaron un entorno seguro y eficiente para explorar y evaluar los archivos en cuestión.

Desde mi perspectiva, esta actividad no solo amplía nuestro conocimiento sobre el análisis forense digital, sino que también refuerza la importancia de la ciberseguridad en el manejo de información. Aprender a identificar y mitigar riesgos potenciales es una habilidad crucial en el mundo actual, donde las amenazas cibernéticas son cada vez más sofisticadas. Esta experiencia práctica nos prepara mejor para enfrentar desafíos reales en el ámbito de la seguridad informática.