**Integrantes del equipo:**

|  |  |
| --- | --- |
| **Nombre del alumno** | **Numero de Matricula** |
| Jose Luis Solis Sosa | 03483370 |
| Víctor Manuel Vázquez Jiménez | 01411637 |
| Brandon Alejandro Castillo Gallardo | 15165340 |
| Raul Olivares Rodrigue | 19469262 |

Nombre del Profesor: **Roberto Corona Pizano**

Nombre del Curso: **Inteligencia en Seguridad de TI**

Actividad: **Actividad en Clase 1 - Autopsy**

Fecha: **18 de noviembre del 2024**

Contenido

[Introducción 3](#_Toc182948766)

[Desarrollo: 4](#_Toc182948767)

[Palabra Drugs 4](#_Toc182948768)

[Palabra Special K 5](#_Toc182948769)

[Tabla dinámica con información: 6](#_Toc182948770)

[Repositorio de archivos en Github: 9](#_Toc182948771)

[Conclusiones 9](#_Toc182948772)

[Bibliografía: 11](#_Toc182948773)

# Introducción

El análisis forense digital es una herramienta fundamental para examinar y recolectar evidencia almacenada en dispositivos electrónicos. Esta técnica es ampliamente utilizada en investigaciones legales y de ciberseguridad para identificar actividades sospechosas, rastrear comportamientos específicos o esclarecer posibles delitos.

En este proyecto, utilizaremos el software Autopsy, una herramienta especializada en análisis forense digital, para estudiar dos imágenes forenses. Estas imágenes contienen datos que serán analizados con el fin de buscar información relevante relacionada con las palabras clave "drugs" y "special k". Estas palabras podrían estar vinculadas a actividades de interés para la investigación y nos permitirán identificar patrones, conexiones o contenidos relacionados con estos términos.

Una vez recopilados los resultados, organizaremos la información en una tabla dinámica. Esta herramienta nos ayudará a clasificar y analizar los datos de manera estructurada, facilitando la interpretación de los hallazgos y permitiendo generar conclusiones claras y comprensibles. El objetivo de este trabajo es mostrar cómo el análisis forense puede contribuir a desentrañar información clave en investigaciones electrónicas y cómo su aplicación puede ser comprensible para cualquier lector interesado en este campo.

# Desarrollo:

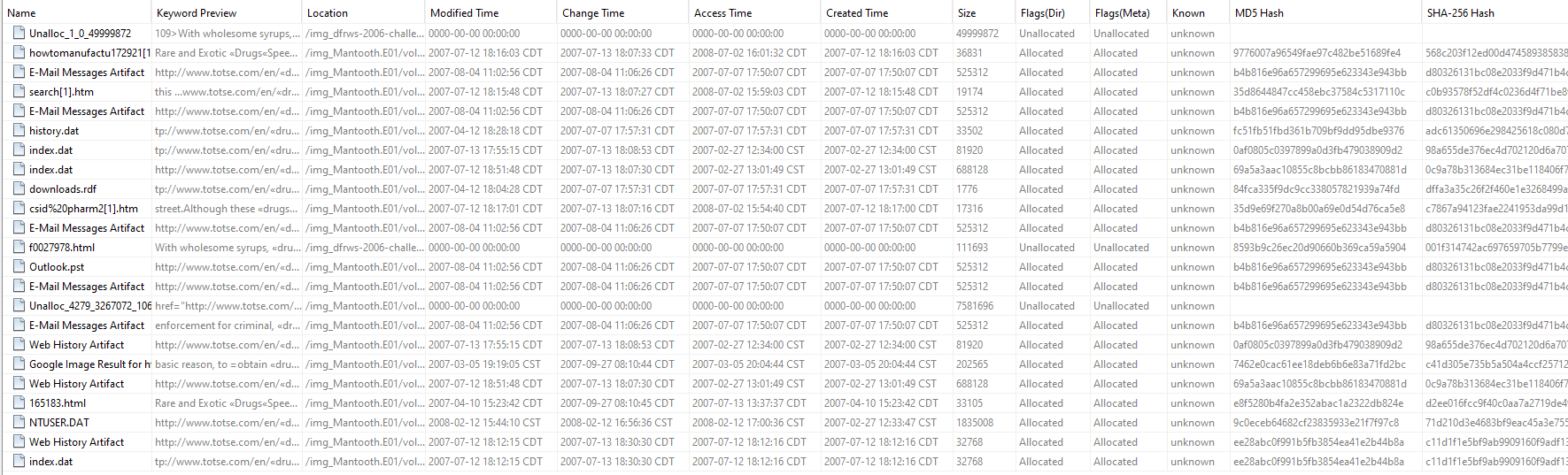
Con base a estas dos imágenes será que se llevará a cabo todo el proceso de búsqueda y análisis de información:



Del contenido encontrado obtendremos los hashes que nos da la aplicación y los pasaremos por la página <https://www.virustotal.com/> para validar si continúen virus o código malicioso que se haya detectado con anterioridad, analizaremos también esta información.

## Palabra Drugs

Se llevo a cabo la búsqueda de información que contuviera la palabra ‘Drugs’ obteniendo los siguientes resultados:



En resumen, la información encontrada fue la siguiente:

El texto detalla conversaciones y actividades ilícitas relacionadas con la manipulación de recetas médicas, adquisición de sustancias controladas como ketamina y métodos fraudulentos para alterar documentos y realizar esquemas de estafa financiera.

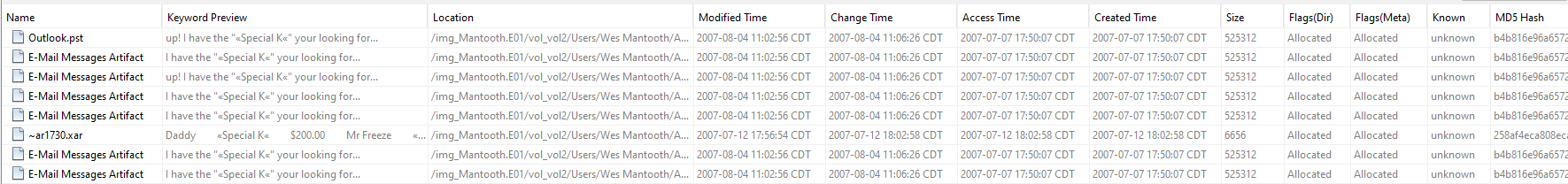
Se abordan sustancias como benzodiacepinas, anfetaminas y metanfetaminas, junto con los efectos y riesgos asociados.

También se menciona un taller sobre inteligencia aplicada a fuerzas del orden en EE.UU. UU., que cubre temas como terrorismo y narcotráfico, y una referencia a una obra de Shakespeare.

Además, incluye definiciones técnicas como la de sistemas de archivos y metanfetaminas.

## Palabra Special K

Se llevo a cabo la búsqueda de información que contuviera la palabra ‘Special K’ obteniendo los siguientes resultados:

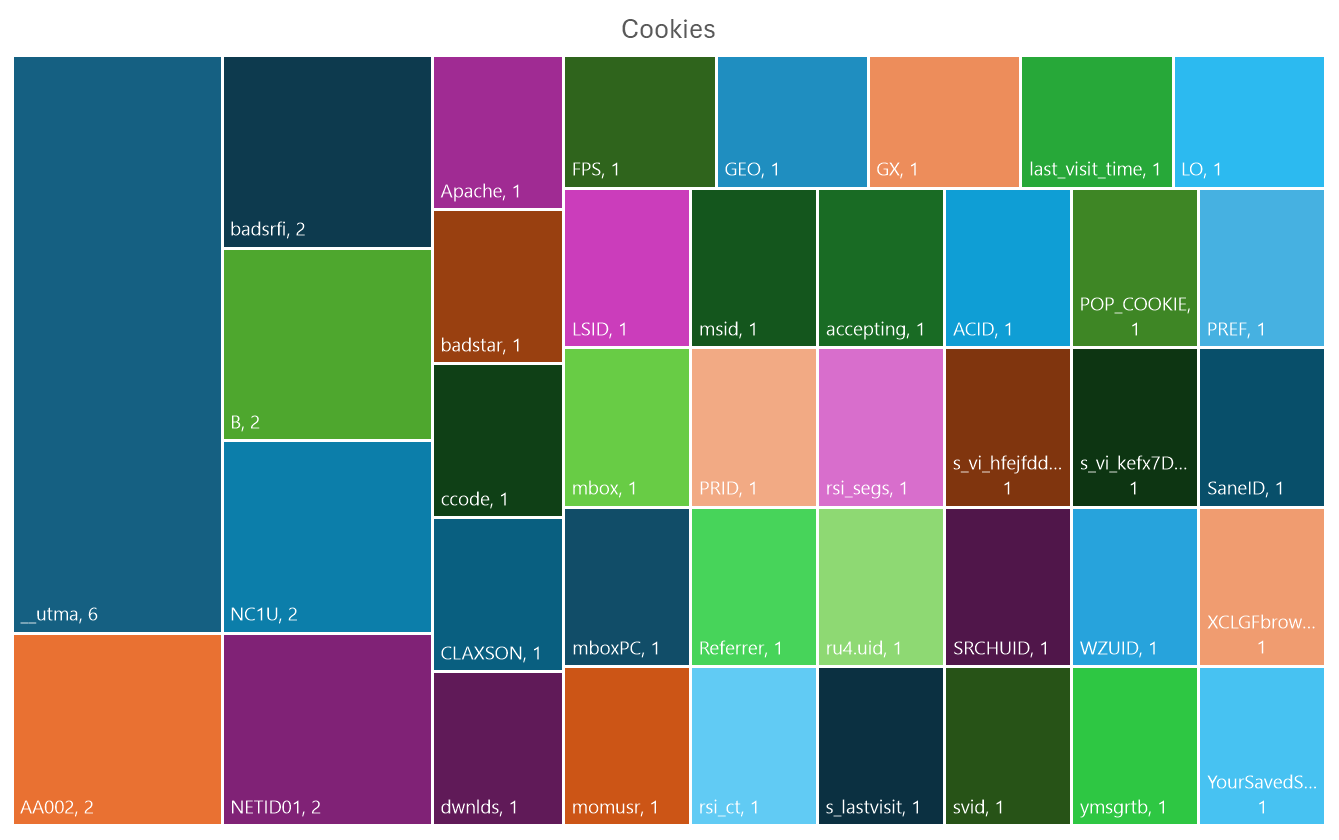


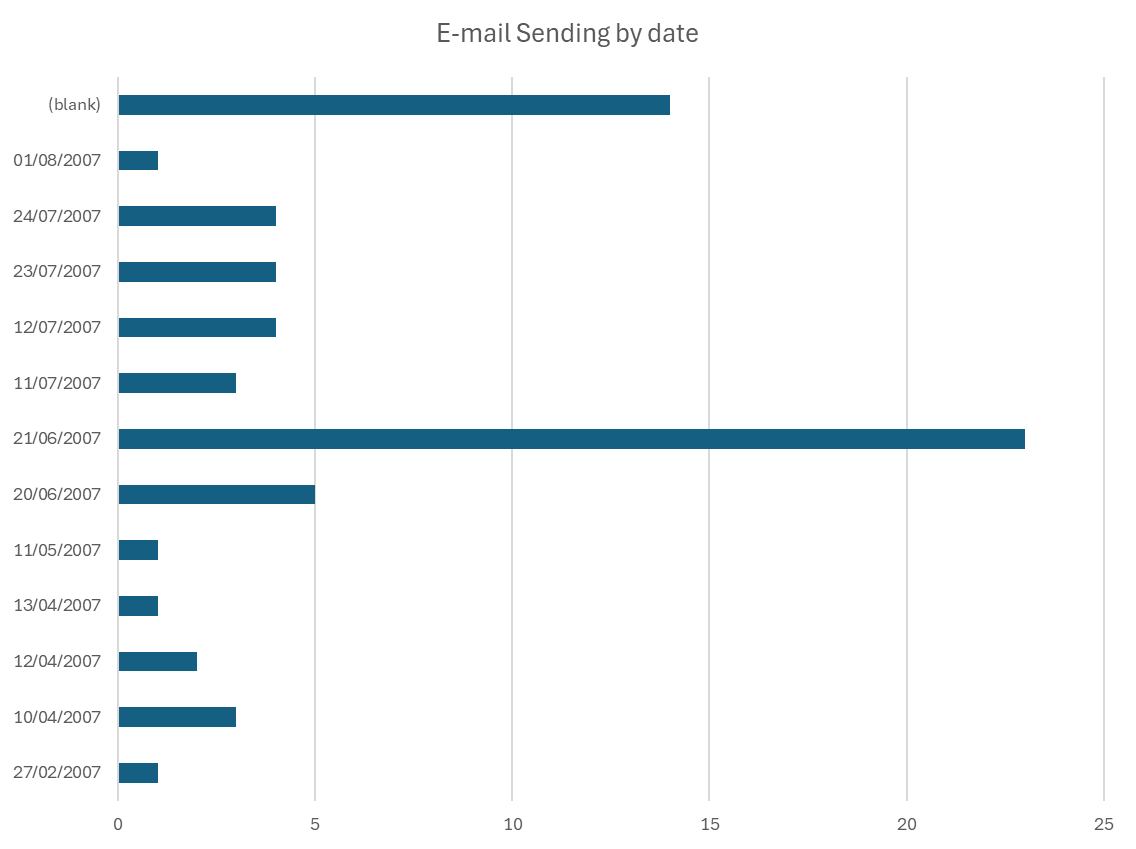
En resumen, la información encontrada fue la siguiente:

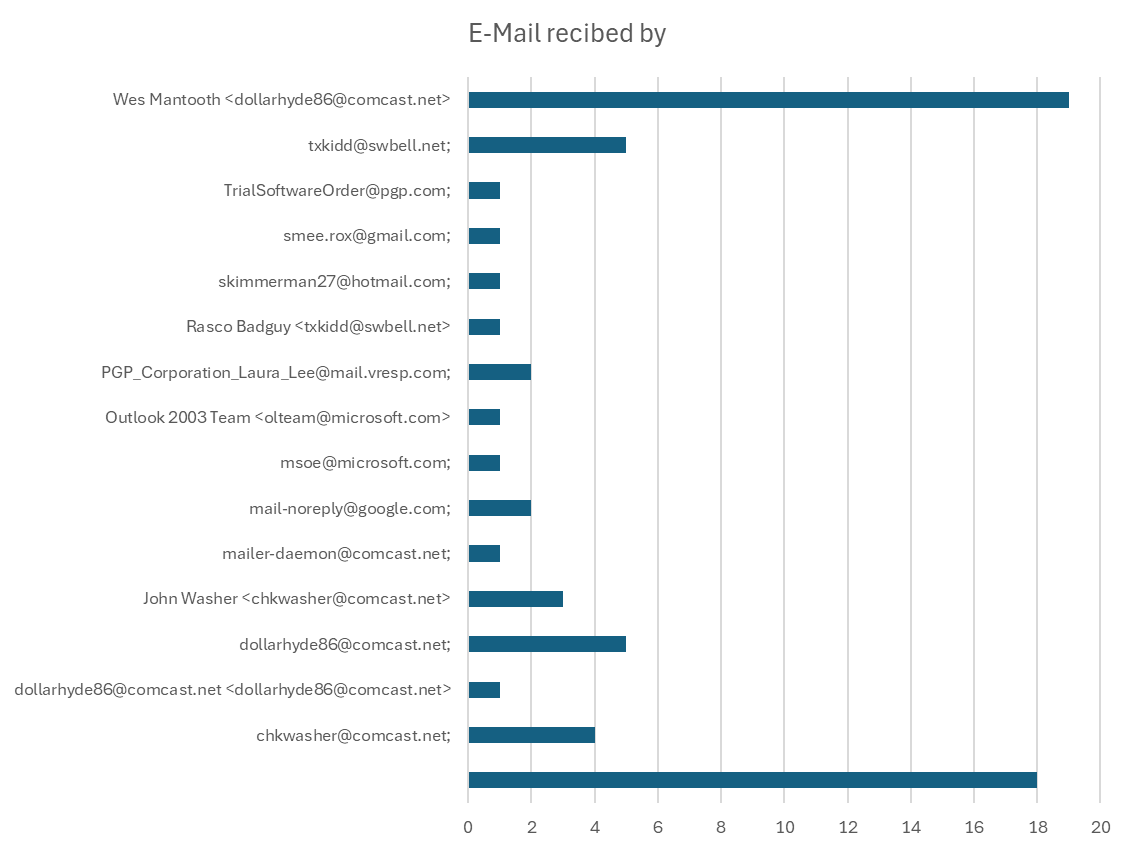
Si bien, después de analizar todos los archivos mediante la página Virus total ninguno demostró tener algún score alto o algún reporte por algún vendor, al validar la información que contienen cada uno de los archivos logramos detectar que se habla de fraudes de diferentes tipos:

* Fraude económico mediante transferencias duplicadas.
* Extracción de Special K de forma ilegal, aprovechando los huecos de seguridad que los demás empleados tienen al dejar recetas olvidadas, siendo aprovechadas para usarlas y surtir esta sustancia de forma ilegal.
* De igual forma se encontró una lista con contactos para el tráfico de metanfetaminas, y robo de cheques.
* Se detecto en un archivo que posiblemente pueda ser una tabla de Excel información de contactos con ‘adeudos’ sobre Special K, Metanfetaminas y Marijuana, lo cual deja al descubierto una red de tráfico dentro de la organización.

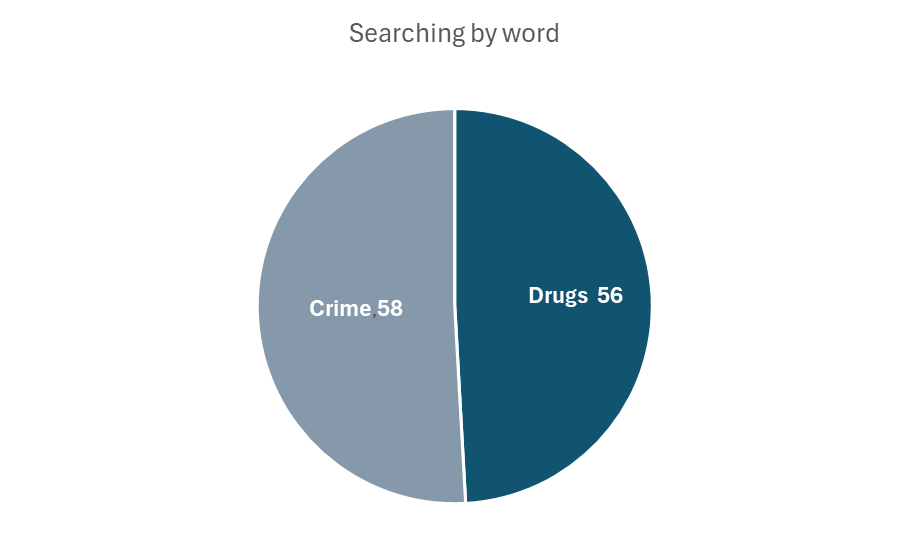
## Tabla dinámica con información:

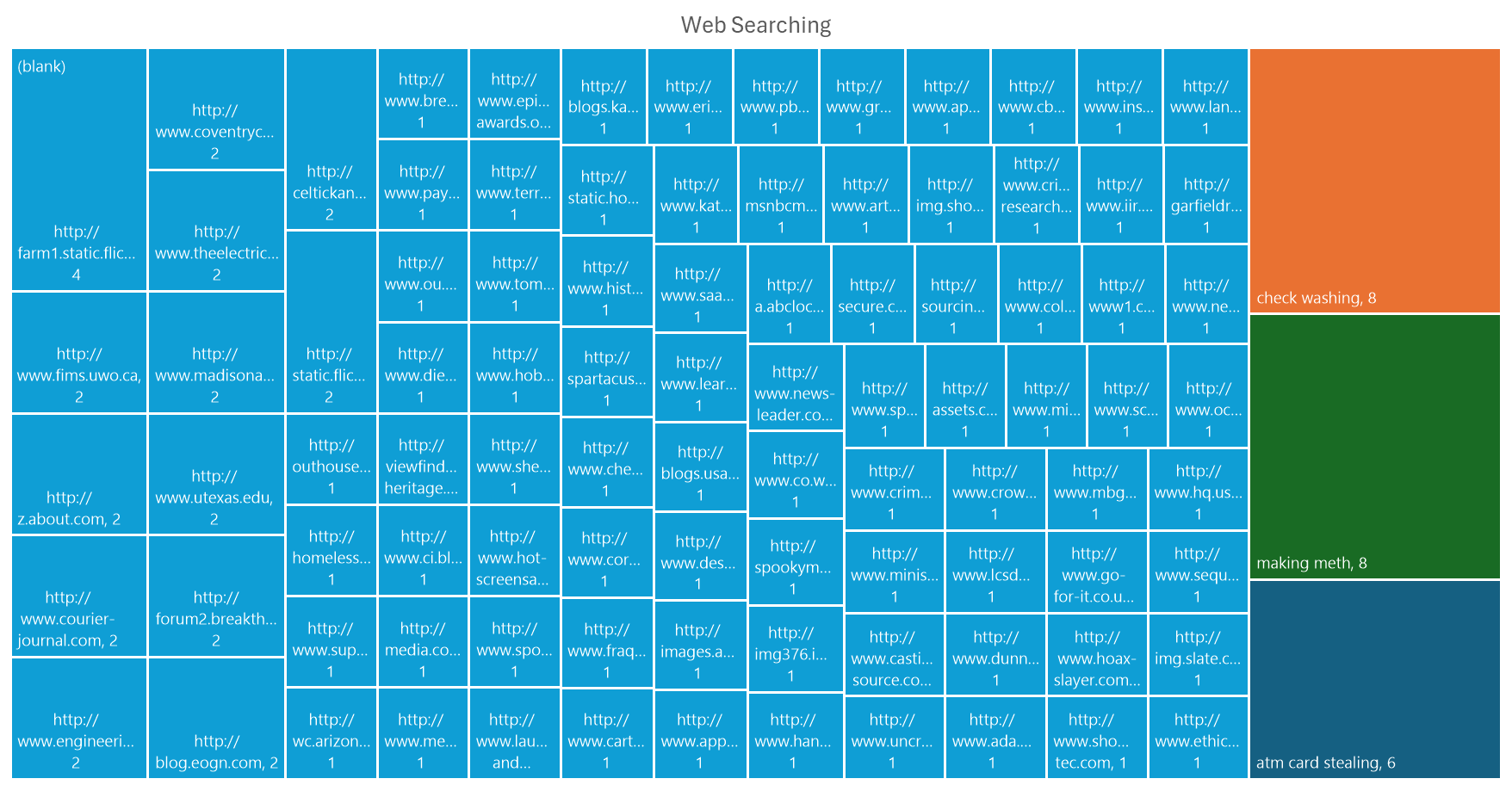












# Repositorio de archivos en Github:

Se adjuntan los archivos utilizados como insumos para el presente entregable dentro del siguiente repositorio de Github:

<https://github.com/LuisSolis-74/Actividad_en_Clase_2>

# Conclusiones

# Bibliografía:

1. Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley Professional.
2. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3ª ed.). Academic Press.
3. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*, S64-S73.
4. Autopsy. (n.d.). *Autopsy User Documentation*. Retrieved from https://www.sleuthkit.org/autopsy/
5. Kruse, W. G., & Heiser, J. G. (2002). *Computer Forensics: Incident Response Essentials*. Addison-Wesley.