UNIVERSIDAD AUTÓNOMA DE CHIAPAS

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
CAMPUS 1

ING. EN DESARROLLO Y TECNOLOGÍAS DE SOFTWARE

7 “M”

OPT.2 - ANÁLISIS DE VULNERABILIDADES

SUB1 - INTRODUCCIÓN AL PENTESTING

MALTEGO REALIZAR LA BASE DE CUALQUIER SITIO WEB

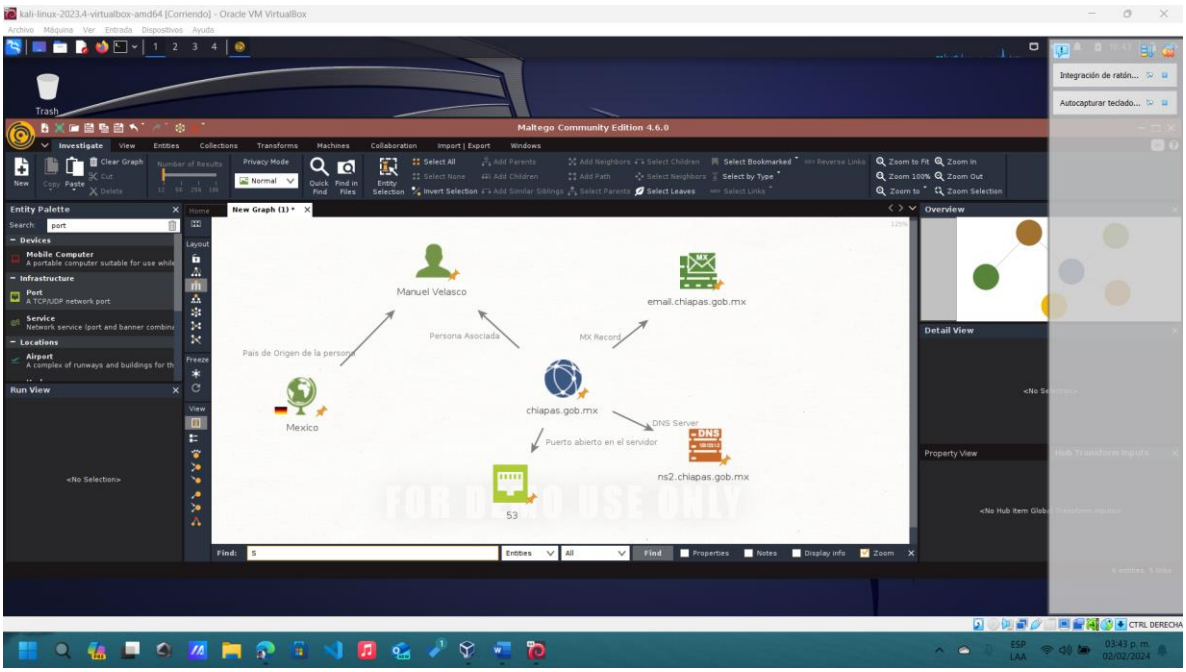
ALUMNOS:
LUIS EDUARDO GONZÁLEZ GUILLEN – A211397
MARCO ANTONIO ZÚÑIGA MORALES – A211121

DOCENTE: DR. LUIS GUTIÉRREZ ALFARO

TUXTLA GUTIÉRREZ, CHIAPAS
SÁBADO, 3 DE FEBRERO DE 2024

1. **Crearás un mapa de relación en Maltego similar al visto en clase donde añadirás las siguientes entidades:**

   - País de Origen
   - Dominio Central (Sitio Web, Compañía Fundadora, Industria, Certificado SSL) - Subdominios con sus respectivas direcciones IP
   - Registros DNS (NameServers - MX Records) con sus respectivas direcciones IP
   - Puertos Abiertos
   - Personas asociadas (Con sus detalles)



Para realizar esta primera parte del ejercicio utilizamos barias herramientas como las siguientes:

Para maltego las entidades en ingles para poder hacer el grafo

- Country
- Domain
- DNS Name y Mx Record
- Port
- Person

Para la obtención del dominio o DNS utilizamos DNSlytics https://dnslytics.com/ que ofrece búsquedas de DNS, dominios inversos, y más.

Para el puerto utilizamos Nmap Oline Scanner, que ofrece escaneos Nmao online sin necesidad de registrarse. https://nmap.online/

Para las personas asociadas utilizamos a Google donde buscamos las personas mas influyentes en el gobierno de Chiapas.

Y para el país de origen utilizamos https://www.ip2location.com/ que nos sirve para ver país, ciudad y región del servidor

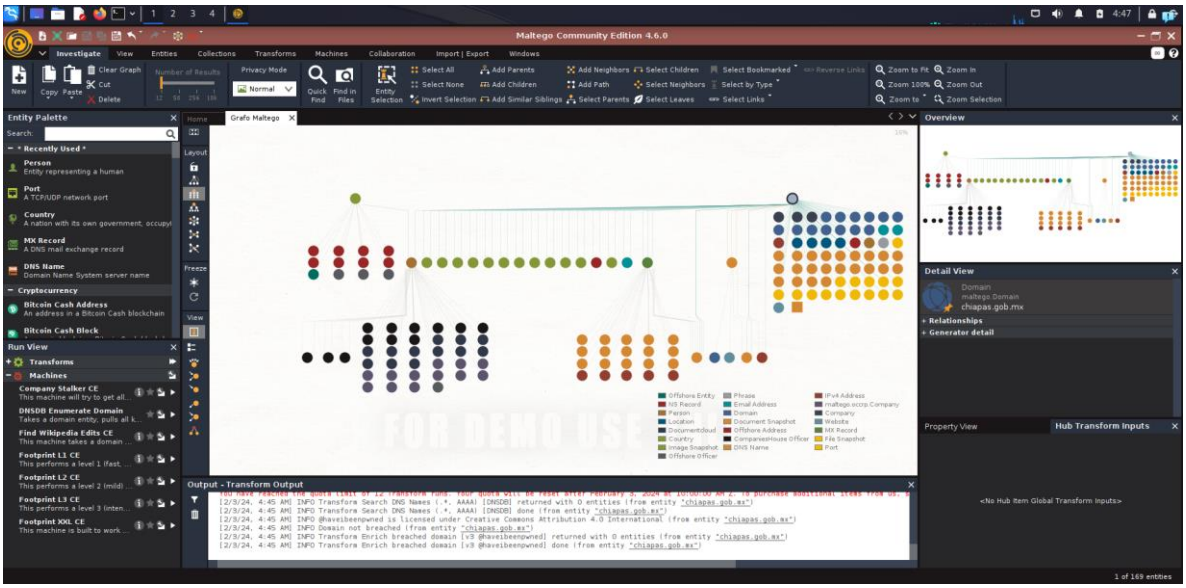
2. Después de tener tu mapa listo, correrás los transformadores que creas conveniente para complementar la investigación sobre el sitio web y en base a los resultados que tengas:

- Descartarás posibles falsos/positivos
- Complementarás y refinarás tu mapa anterior en base a los resultados que los transformadores te arrojen

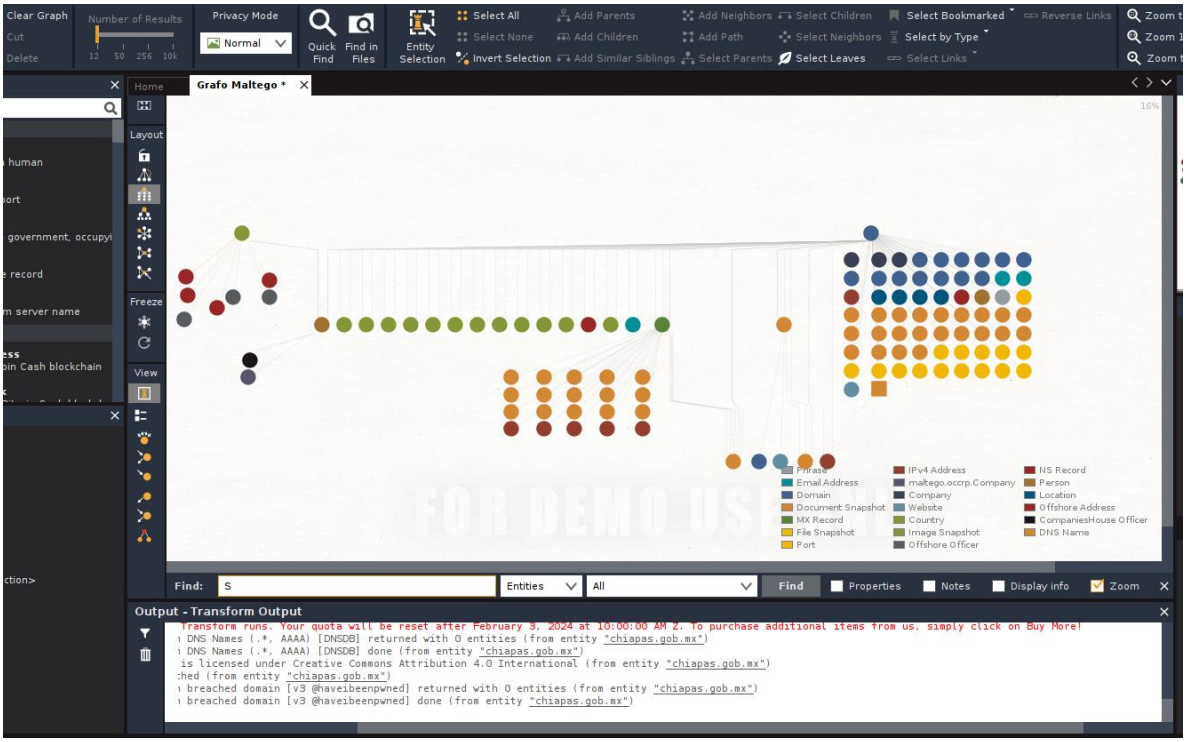
Los trasformadores que se instalaron en maltego para esta actividad fueron

- Have I been Pwned?
- Social Links CE
- Farsight DNSDB
- CaseFile Entities

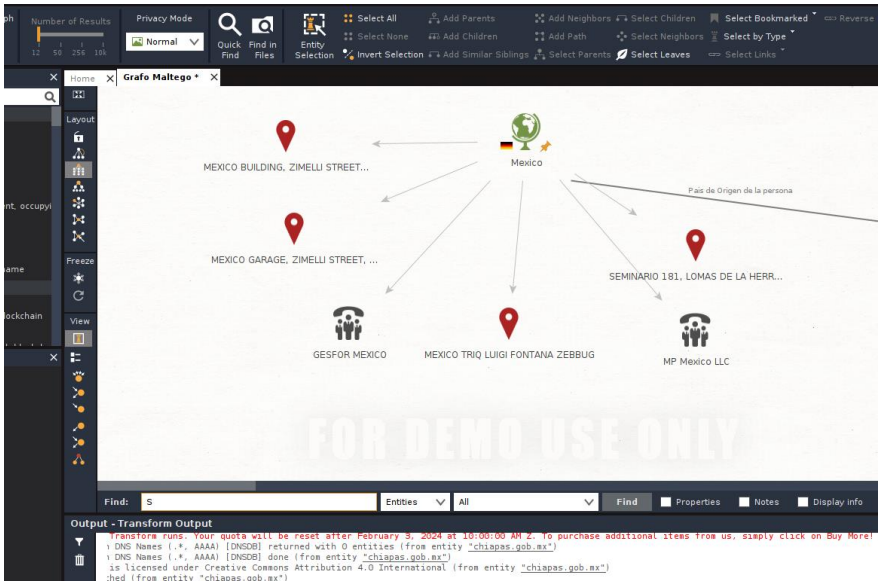
El programa maltego al correr los transformadores nos creó el siguiente grafo

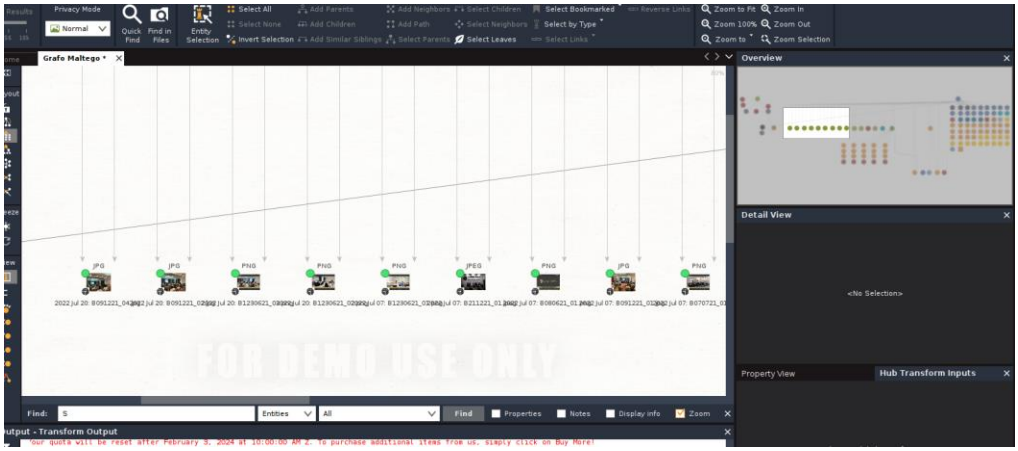


Descartando falsos positivos y examinando bien el grafo nos queda de la siguiente manera



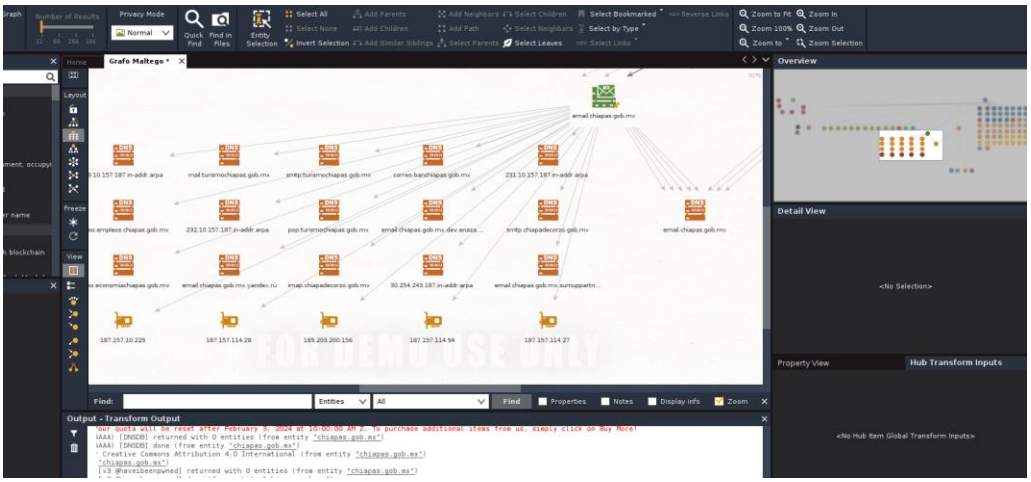
A continuación, las capturas de pantallas más cerca de estos datos



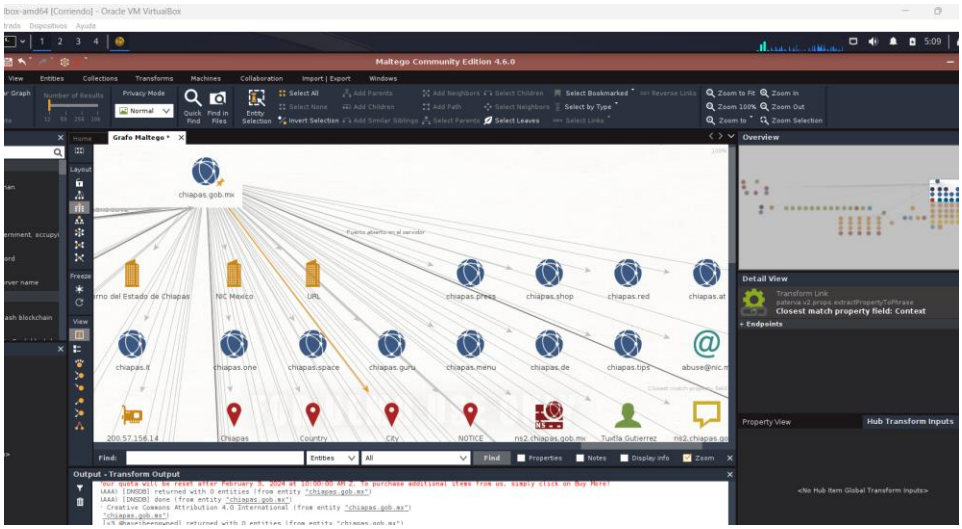


En esta captura de pantalla, nos muestra imágenes que tienen relación con el gobierno de Chiapas.

Aquí podemos visualizar claramente el logo del esta de Chiapas y una conferencia que algún día tuvo el gobierno de Chiapas.



Aquí nos muestra los DNS asociados al gobierno de Chiapas, incluso los DNS de otros municipios.



Y en esta captura podemos visualizar los diferentes dominios web que tiene el gobierno de Chiapas en sus diferentes áreas asignadas.

3. Conclusión

En conclusión, el inicio de esta actividad nos presentó ciertos desafíos, especialmente en la etapa inicial de establecer relaciones adecuadas para la construcción del grafo. No obstante, mediante la aplicación diligente y ética de herramientas especializadas, logramos extraer y analizar datos pertinentes para cada entidad requerida, tales como país de origen, dominio, registros DNS, puertos abiertos y personas asociadas. La selección cuidadosa de transformadores adecuados para cada tipo de entidad nos permitió alcanzar un nivel significativo de precisión en la información que integramos en el análisis.

Para esta actividad utilizamos instalamos los transformadores que se encuentran en maltego como: Have I been Pwned?, Standard Transforms CE, CaseFile Entities, Farsight DNSDB y Social Links CE. Estos transformadores nos fueron de ayuda para visualizar la información deseada que esperábamos.

Específicamente, enfocamos nuestro estudio en el dominio correspondiente al gobierno del estado de Chiapas, manteniendo un enfoque ético en todo momento. Este ejercicio nos permitió verificar la exactitud y relevancia de la información obtenida. Los resultados, evidenciados a través de capturas de pantalla incluidas en este documento, demostraron la eficacia de las transformaciones de Maltego en filtrar y clarificar los datos disponibles públicamente en Internet. Identificamos elementos visuales distintivos, como el logo del estado de Chiapas, así como datos valiosos en forma de fotografías de reuniones, direcciones y enlaces web que direccionan a recursos y municipios relacionados, junto con registros DNS específicos.

Esta experiencia subraya la importancia de las herramientas de inteligencia de fuentes abiertas (OSINT) como Maltego, no solo para la recopilación de datos sino también para su análisis en contextos investigativos. Trabajando en equipo, hemos podido superar los desafíos iniciales, lo que refleja la complementariedad de nuestras habilidades y la efectividad de nuestra colaboración. El éxito de esta actividad reafirma nuestro compromiso con la investigación ética y responsable, abriendo caminos para futuras indagaciones en el vasto dominio de la ciberseguridad y la inteligencia de información.