

## PRÁCTICA 06

“LA INTELIGENCIA CONSISTE NO SÓLO EN EL CONOCIMIENTO, SINO TAMBIÉN EN LA DESTREZA DE APlicar LOS CONOCIMIENTOS EN LA PRÁCTICA”

### ANÁLISIS FORENSE DE ATAQUES WEB

**REFERENCIAS:** hash del archivo entregado.

Archivo entregado: **Evidencias.iso**

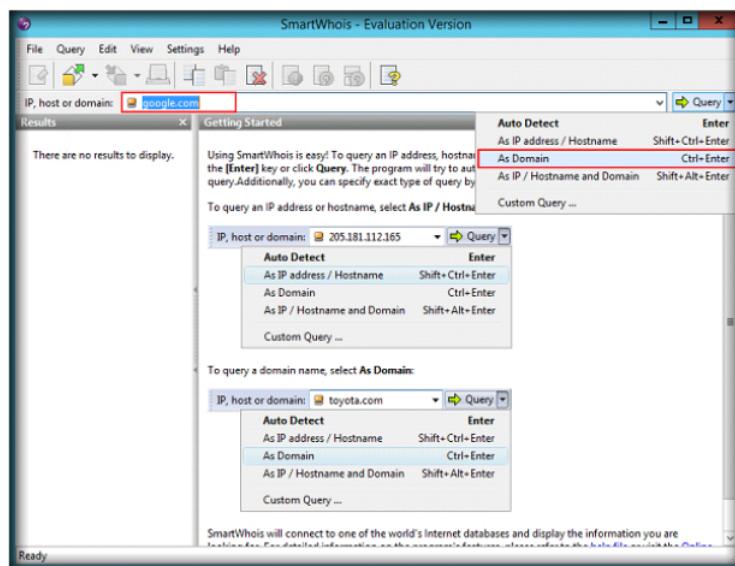
**HASH**

**MD5 E283AE481719A194B2F3A01F95C8252B**

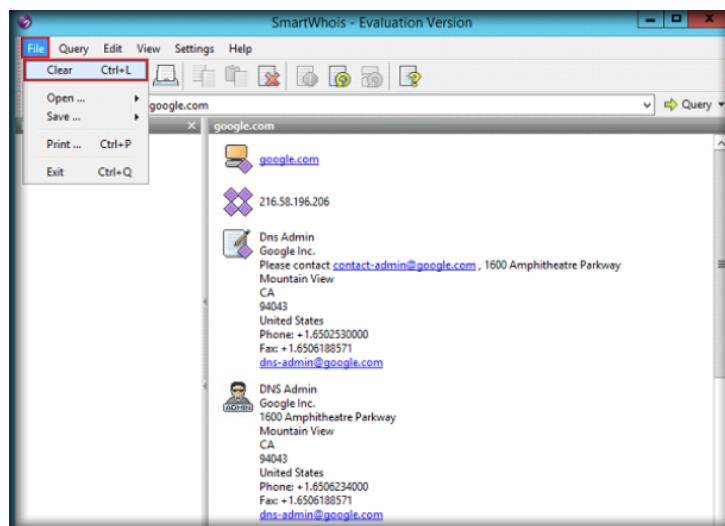
#### EJERCICIO 01 – Análisis un Dominio e IP

Utilizando la herramienta **SmartWhois** y utilizando su navegador de Internet que prefiera implementar:

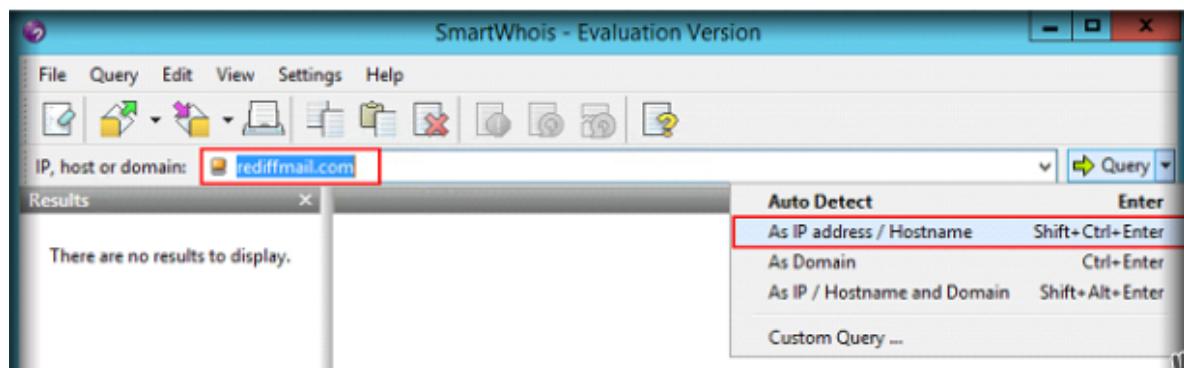
Busquemos información del dominio **google.com** y consultamos **As Domain**:



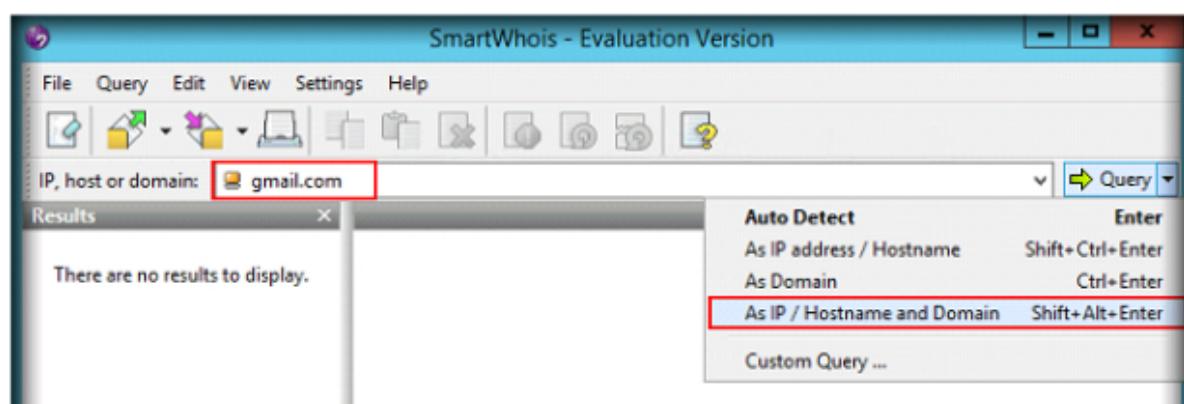
Y mostrará el resultado de la consulta, luego de ver el contenido limpiar el mismo y realizar otra consulta:



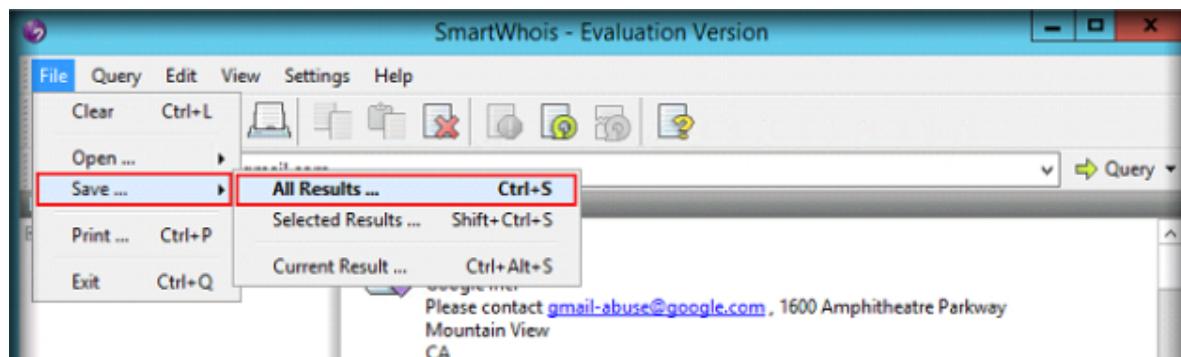
Busque información de [www.rediffmail.com](http://www.rediffmail.com):



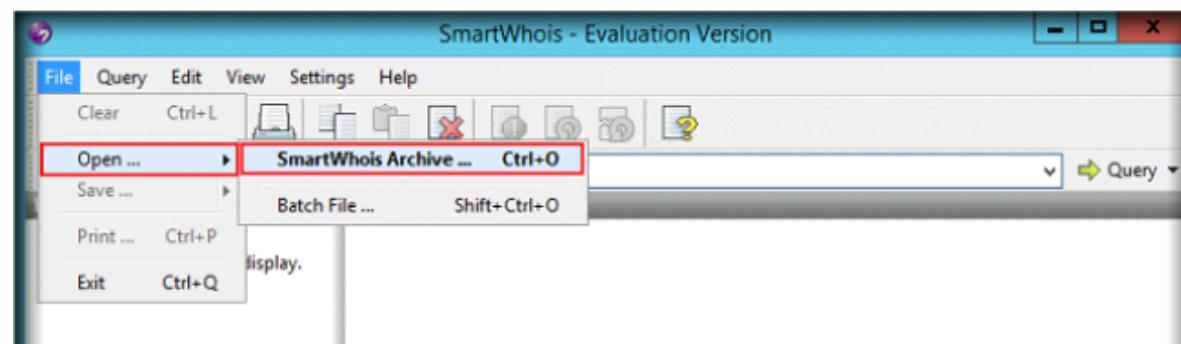
También puede hacer la búsqueda por **IP Address** y **Hostname**, por ejemplo realice la siguiente búsqueda sobre gmail.com:



Y vea sus resultados... Puede también guardar todos sus resultados:



Y luego consultar su archivo de almacenamiento:

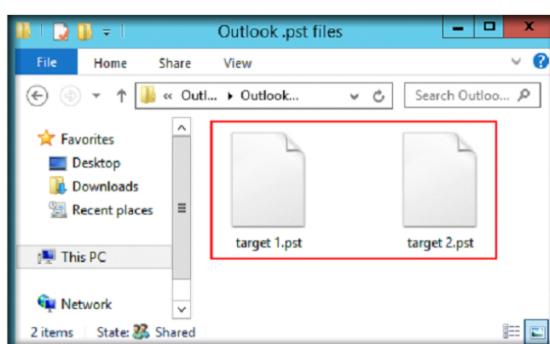


Para más información sobre el WHOIS y su uso, puede consultar:

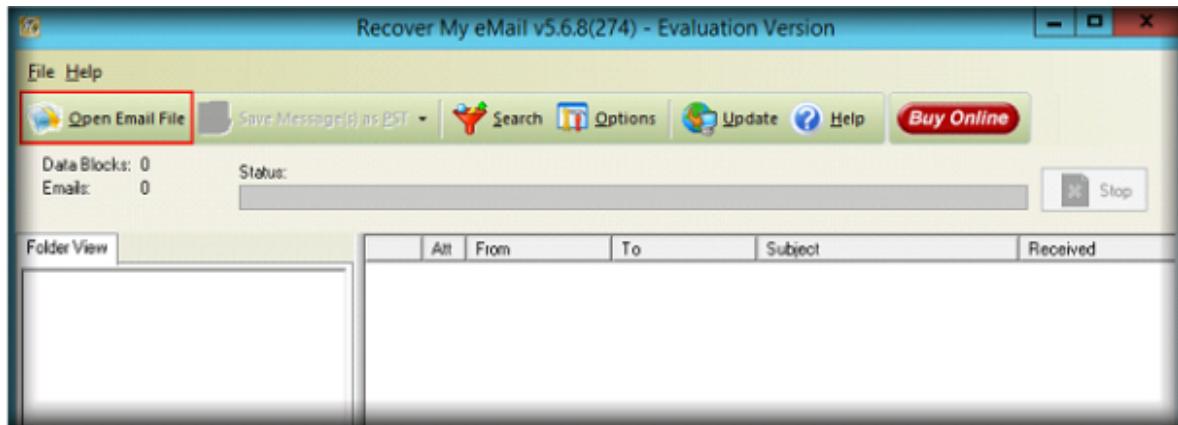
<https://www.lacnic.net/1002/1/lacnic/whois>

## EJERCICIO 02 – Recuperando correos electrónicos borrados

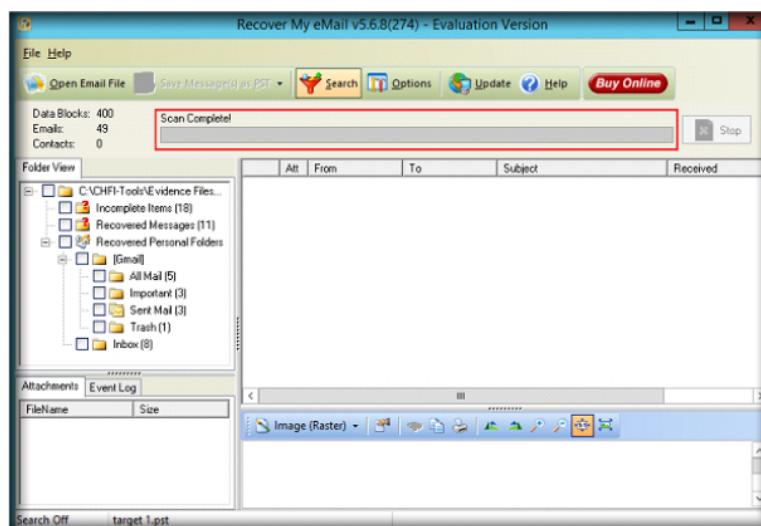
Vamos a utilizar las siguiente evidencias:



Utilizando la herramienta **Recover my Email (RecoverMyEmail-Setup.exe)**, abrimos el archivo “target1.pst”:

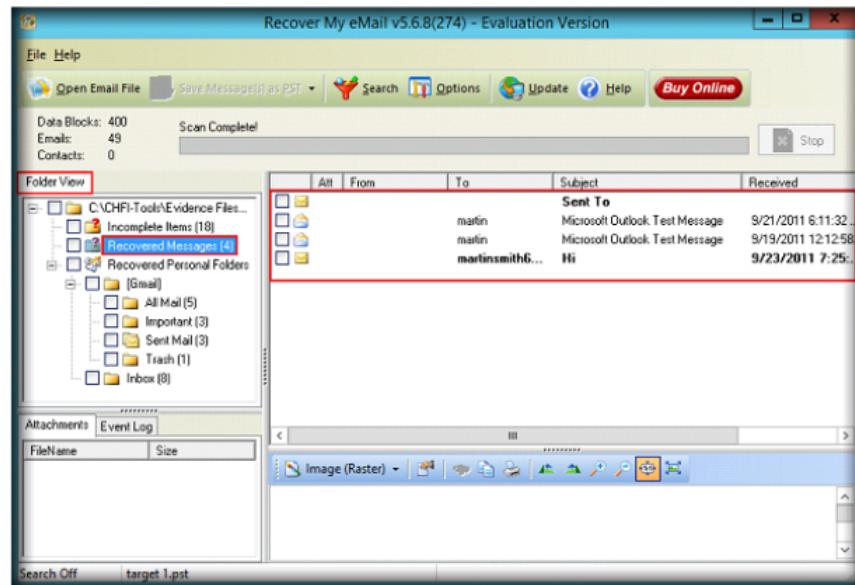


cargará el archivo, lo escaneará y luego veremos algo como lo siguiente:

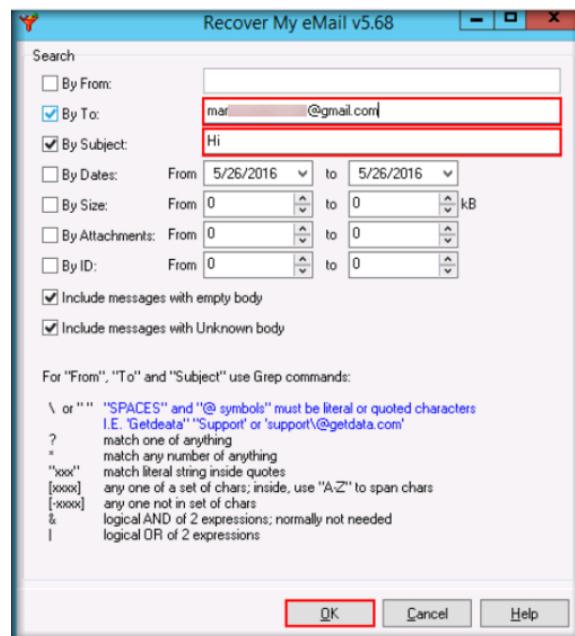


Podemos ver la vista de

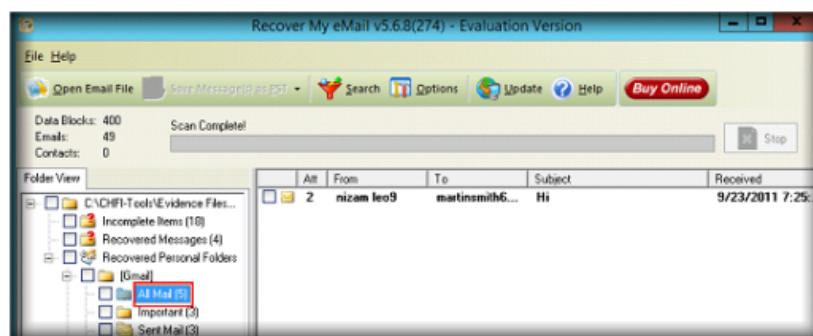
“Recovered Messages”:



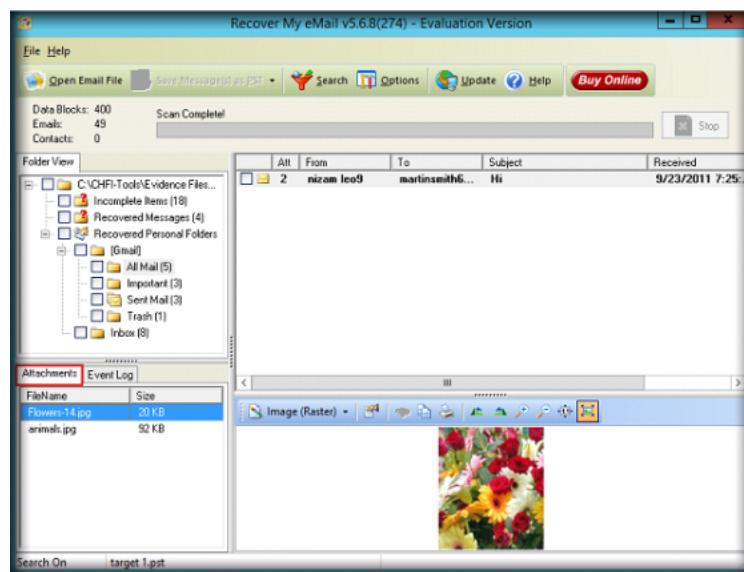
Podemos hacer búsquedas específicas como las siguientes:



y tener resultados:



También podemos ver los archivos adjuntos:

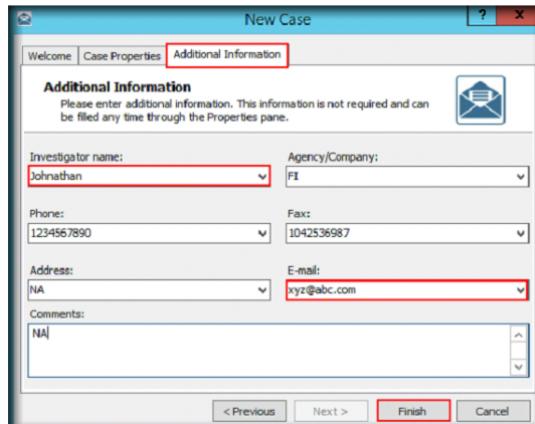
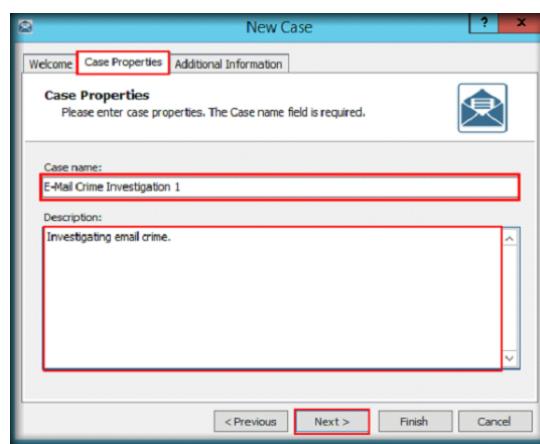
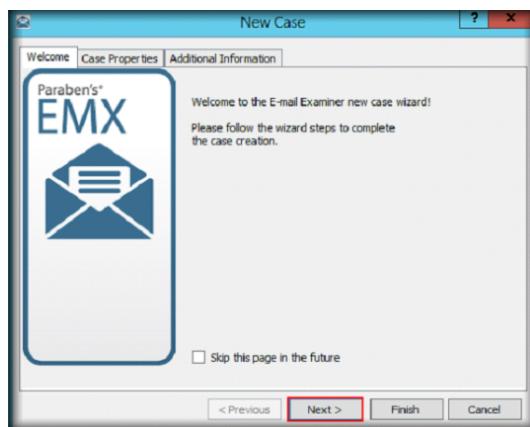


### EJERCICIO 03 – Investigando crímenes por medio del correo electrónico

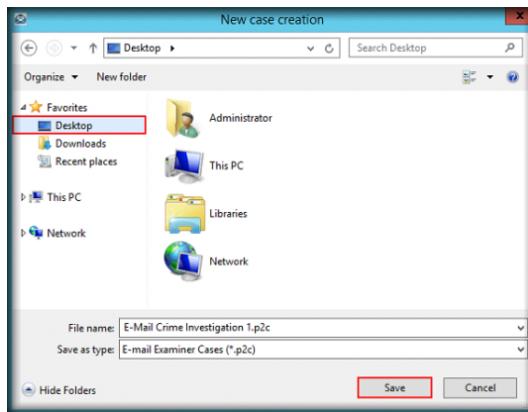
Vamos a utilizar la herramienta Paraben's Email Examiner (emx-demo.exe) y creamos un nuevo caso:



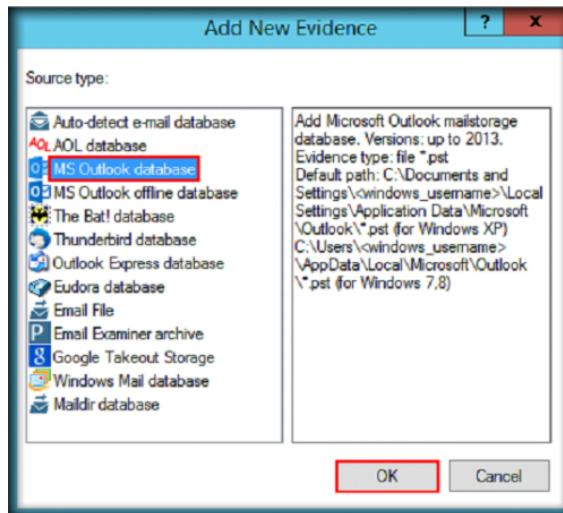
y seguimos los pasos:



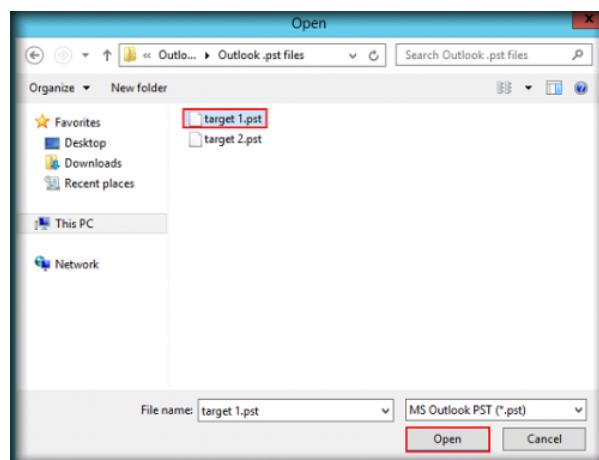
Y grabamos el caso en el escritorio de nuestra sesión de trabajo:



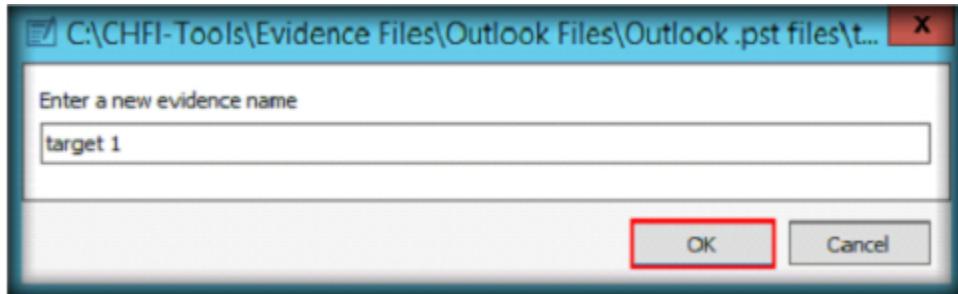
Agreguemos nueva evidencia:



y seleccionamos el archivo “**target1.pst**”:



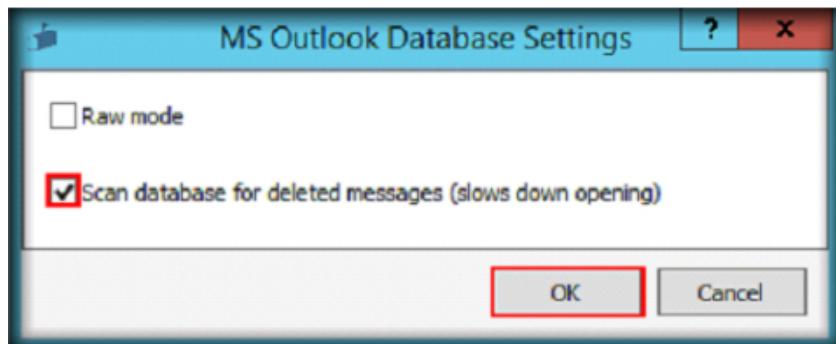
Aparecerá una ventana y le dejamos el mismo nombre:



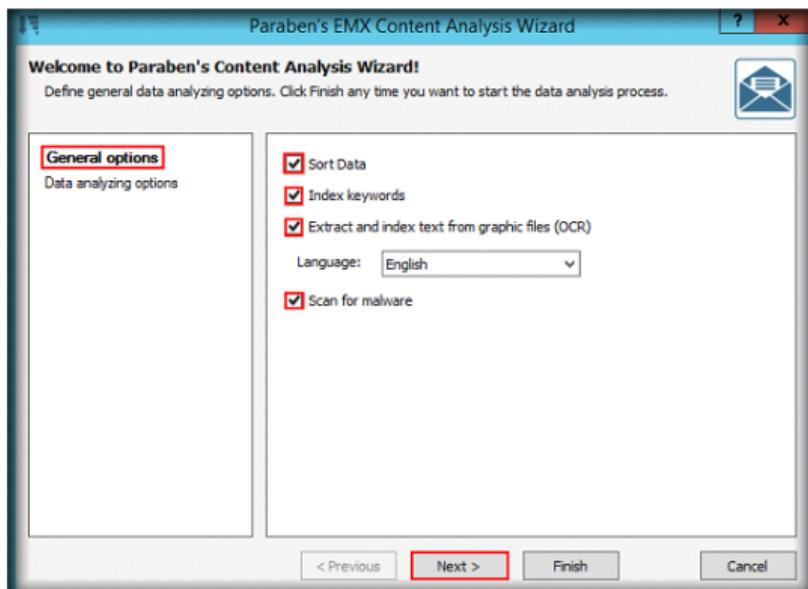
Aparecerá una solicitud de escoger qué método utilizaremos:

- **Raw Mode:** Despliega todo el contenido de la base de datos, incluyendo: sistema, información huérfana y elementos borrados.
- **Scan database for deleted messages (slows down opening):** seleccione esta opción para encontrar y recuperar mensajes borrados en la base de datos. Esta opción puede tomar tiempo.

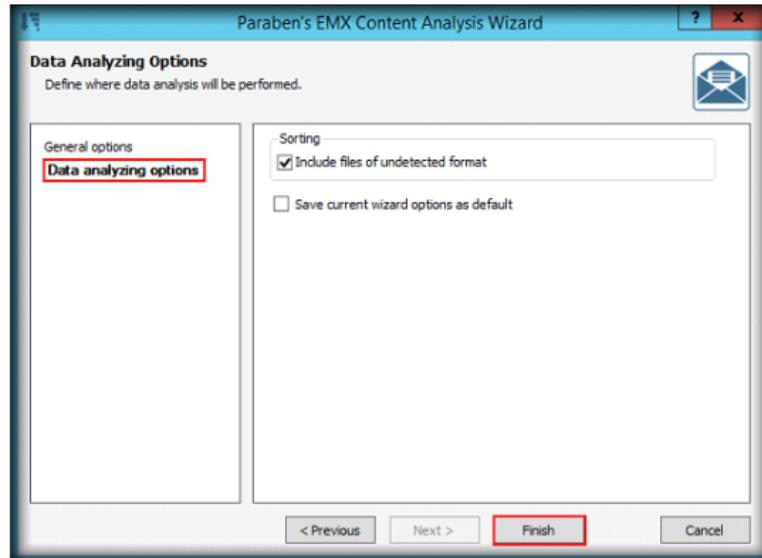
Y realice la siguiente selección:



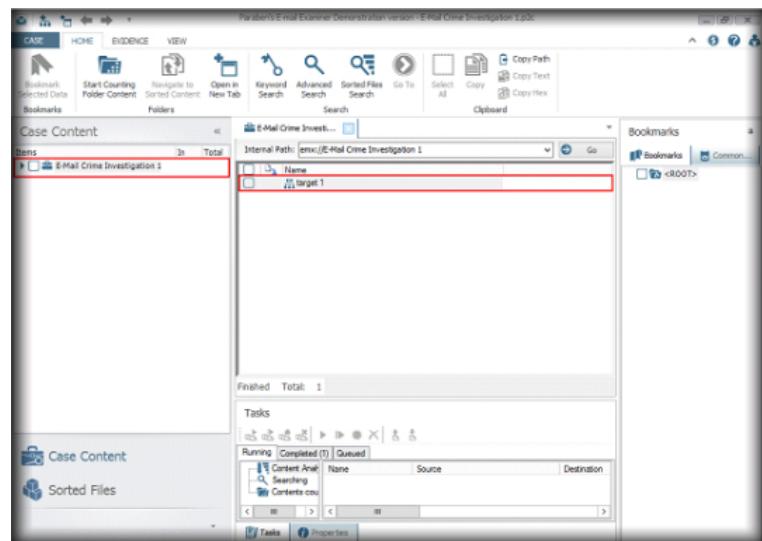
y realizamos las siguientes selecciones:



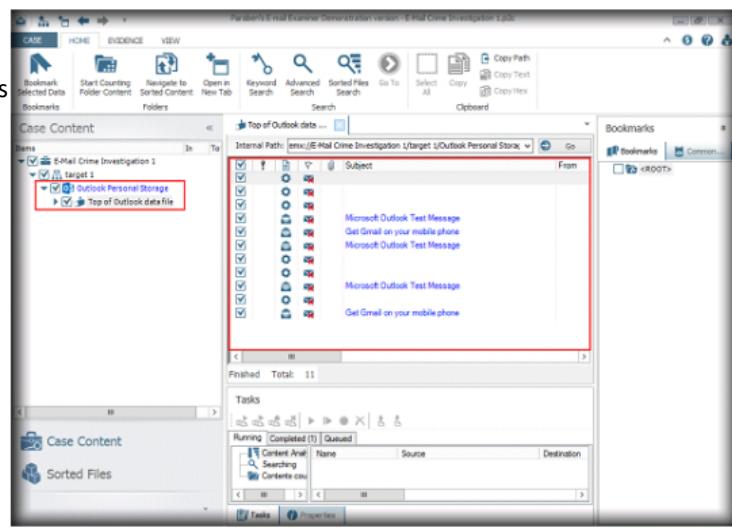
y luego seleccionamos:



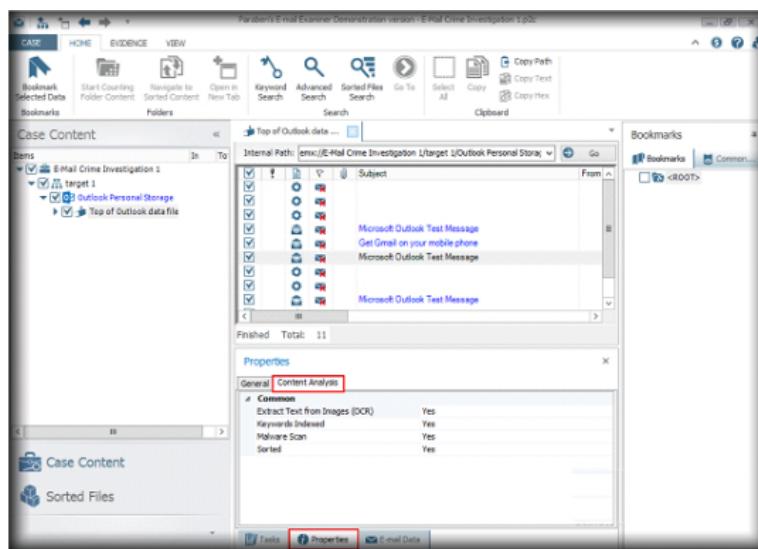
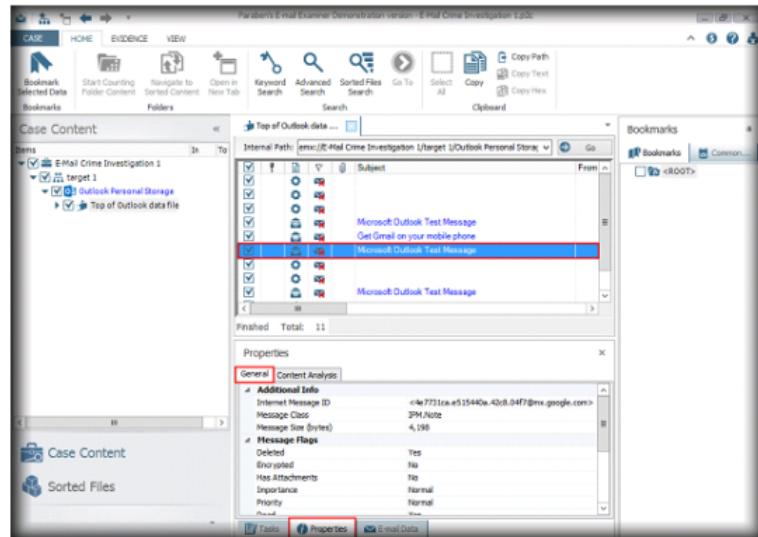
Y después de realizar el análisis la herramienta se mostrará lo siguiente:



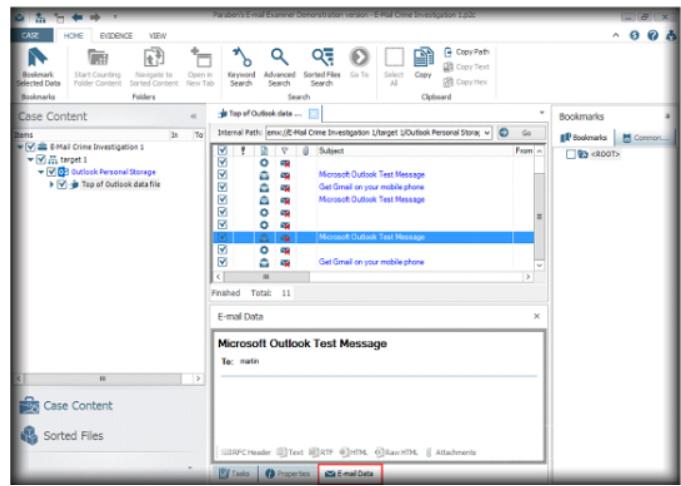
Luego investigamos lo obtenido:



Seguimos inspeccionando:



Y bueno, en la versión no nos deja ver el contenido del mensaje, pero ya con este recorrido nos damos cuenta que tan profundo es el análisis que puede llegar a realizar la herramienta:



**Evaluación:**

La evaluación de esta práctica se basará en los siguientes criterios:

- La capacidad de los estudiantes para utilizar las herramientas y técnicas forenses aplicadas de forma correcta.
- La capacidad de los estudiantes para comprender como se implementa un análisis forense.
- La capacidad de los estudiantes para responder a las preguntas de reflexión de forma crítica y reflexiva.
- La capacidad de brindar un relato claro en la introducción de la tarea entregada, así como brindar conclusiones y recomendaciones efectivas sobre los distintos ejercicios realizados.

**Nota:** Esta práctica es solo para fines educativos. No se debe utilizar para realizar actividades ilegales.

**ENTREGABLE:** Implementar un Informe Académico que debe cumplir con el siguiente alcance:

- **Introducción:** Describir el reto que significó hacer esta tarea, describir por punto como lo resolvieron.
- **Resultados:**
  - EJERCICIO
    - Realizar por cada archivo que contiene la imagen ISO (también analizar el archivo ISO) el análisis de evidencia y presentar la tabulación respectiva basado en el documento llamado “FORMATO.ANALISIS.EVIDENCIAS.xlsx”.
    - Cumplir con lo solicitado a desarrollar por cada ejercicio.
    - Por cada apartado donde aparece una imagen a implementar una operación, siempre agregar un párrafo que explique lo que se está realizando, y cuando aplique, dar un comentario oportuno sobre algún hallazgo o dato/explicación concluyente.
- **CONCLUSIONES:** sobre cada herramienta utilizada, hallazgos y capacidades de análisis, así como del manejo de la evidencia y uso de comandos con adecuado criterio experto.