***TRABAJO PRÁCTICO***

***Un ataque por la red- lab#1***

***Materia***

Informática Forense

**Integrantes del Grupo:**

**Bernardo Napoleon Luscher**

**Turno: Noche**

**Docente: Antonio, Juan Manuel**

**Fecha de entrega:**

**Introducción**

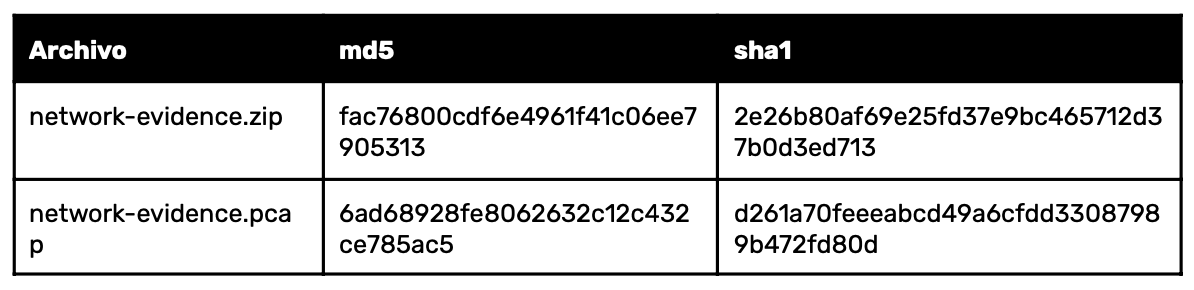
Se ha producido un ataque en un dispositivo de nuestra red y hemos logrado capturar los paquetes de red correspondientes para su posterior análisis.

Para resolver el presente laboratorio el alumno debe contar con el archivo de evidencia network-evidence.zip el cual puede ser bajado del aula virtual.

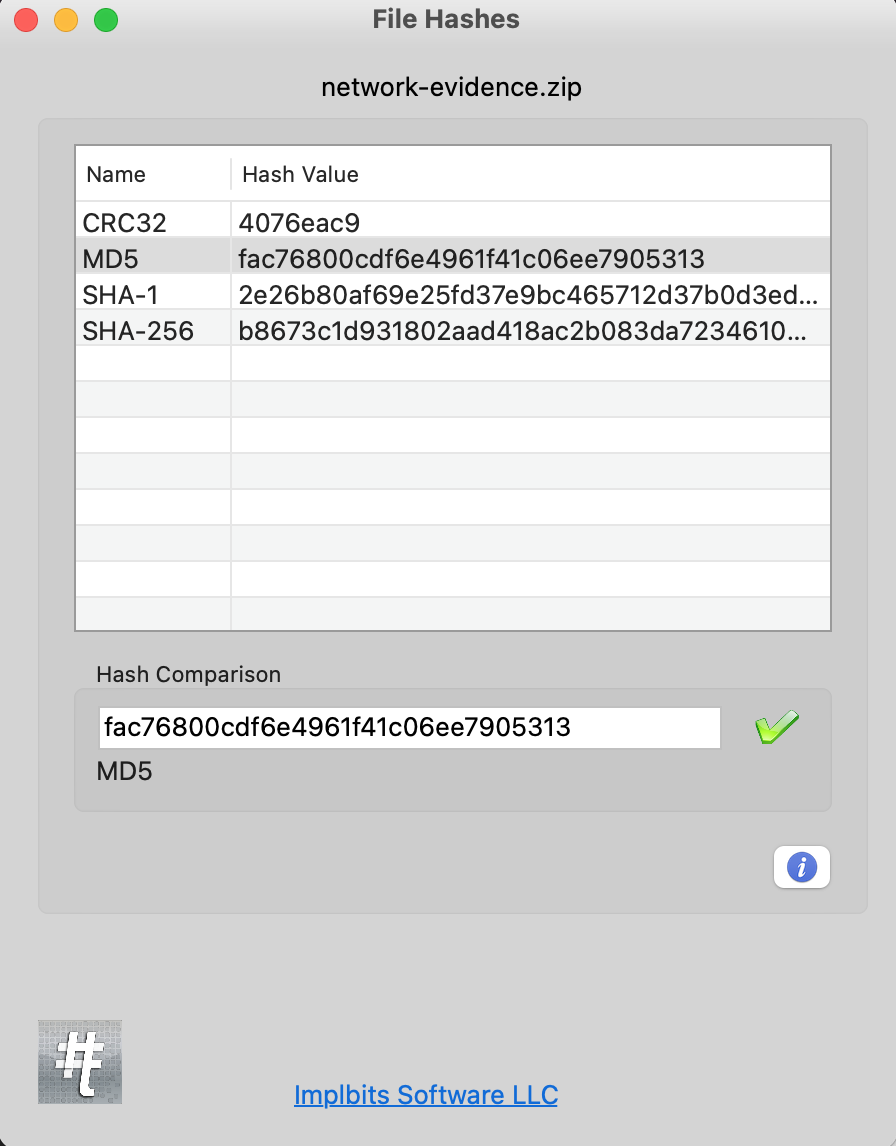
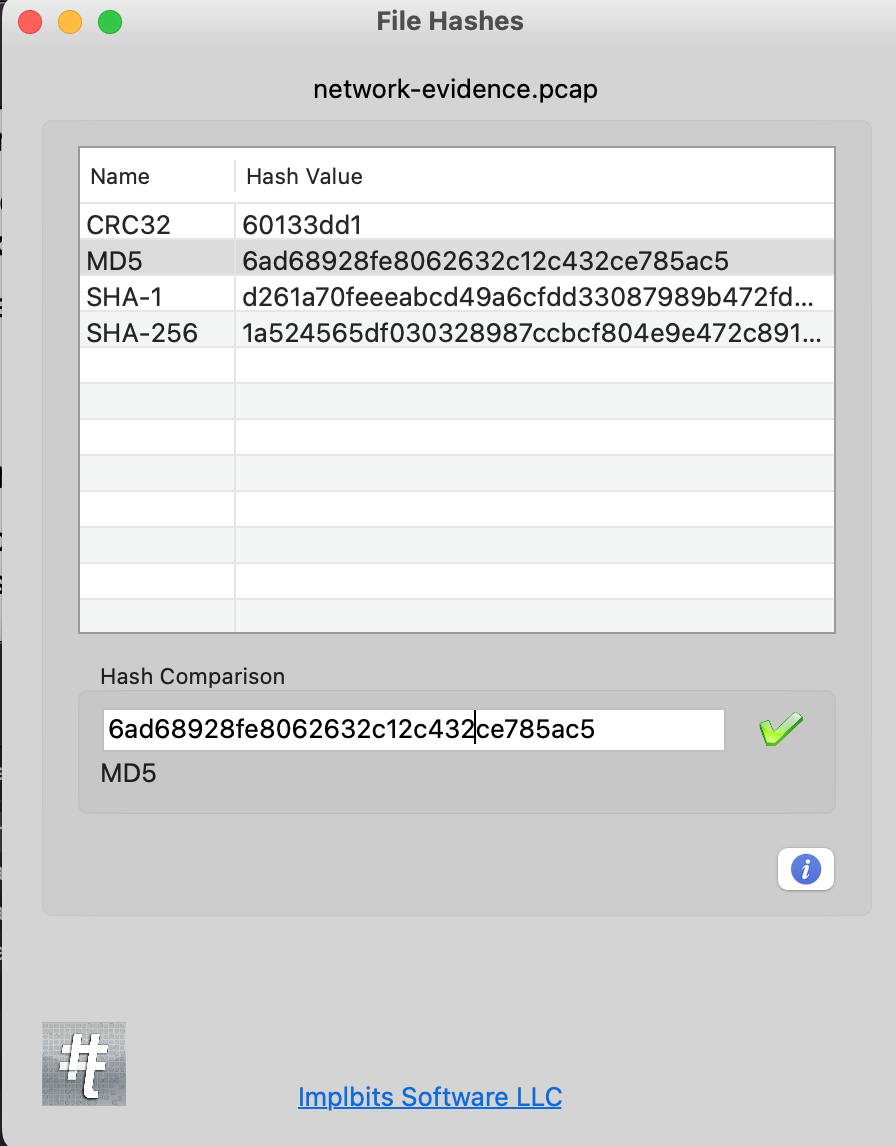
Dentro de este archivo encontraremos una captura de datos de la red de un sistema que ha sido atacado.

Para resolver el laboratorio, el alumno deberá responder las siguientes preguntas justificando en cada caso las respuestas y especificando las herramientas utilizadas:

1. Validar el hash de la evidencia. Continuar con las siguientes preguntas sólo en caso que la evidencia se encuentre validada.

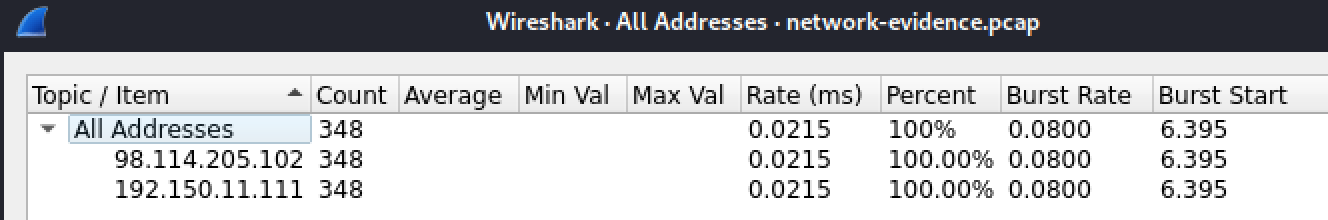


Solución: Se validó el hash de las evidencias mediante la herramienta *Hashtab version6.0*.El resultado fue que la evidencia descargada es consistente con la relevada. Dejemos la pruebas de la evaluación a continuación:

1. ¿Cuántos dispositivos se encuentran involucrados en la conversación?

Solución: 2 dispositivos [98.114.205.102 y 192.150.11.111]



1. ¿Cuántas sesiones TCP contiene la evidencia?
2. Identifique la dirección IP del atacante y la dirección IP de la víctima.
3. ¿Puede geolocalizar a la dirección IP del atacante? ¿Quién es el dueño de esa dirección IP?
4. ¿Qué sistema operativo tienen los dispositivos involucrados?
5. ¿Cuánto tiempo le llevó al atacante perpetrar el ataque?
6. ¿Cuál fue el servicio atacado?¿Cuál fue específicamente la vulnerabilidad que el atacante explotó?
7. Detallar y graficar las acciones que el atacante efectuó sobre la máquina víctima.
8. Determine la existencia de un malware. En caso afirmativo, especifique el nombre de dicho malware.
9. Determine si el ataque fue realizado de forma manual o automática y si tuvo éxito.