

Universidad Alcalá de Henares

Práctica 2

Análisis Forense Avanzado

Paula Daniela Sanchez Rodriguez
Enrique García Cuadrado

Contenido

1.	Forense en Windows.....	2
1.1.	Hora y fecha del sistema al inicio del análisis.....	2
1.2.	Listado de conexiones activas.....	2
1.3.	Relación de aplicación y puertos abiertos.....	3
1.4.	Caché DNS.....	4
1.5.	Caché ARP.....	5
1.6.	Tráfico por proceso.....	6
1.7.	Estadística de las conexiones actuales.....	6
1.8.	Hora y fecha de fin	7
1.9.	Análisis de evidencias.....	8
a.	Caché ARP (arp -a).....	8
b.	Relación de Aplicaciones y Puertos Abiertos (netstat -bano)	8
2.	Forense en Email.....	10
2.1.	Nombre del cliente de correo electrónico	10
2.2.	¿Cuál es la dirección de e-mail origen del envío?	10
2.3.	¿Cuál es la dirección de e-mail destino?	11
2.4.	¿Qué sistema operativo alberga el servicio SMTP?	11
2.5.	¿Cuál es el nombre del software usa el servicio SMTP?.....	12
2.6.	¿Qué puerto de origen y destino aparece en la parte de TCP de la trama nº20? ...	12
2.7.	¿Cuál es la dirección IP origen y destino de la trama nº9?	13
2.8.	¿Qué servidor (nombre) está involucrado en la petición http de esta captura?	13
2.9.	¿Cuál es el puerto origen y destino de la trama nº 6?	14
2.10.	Indique la siguiente información de la trama nº4 y cómo la ha conseguido:	14
2.11.	Compruebe el filtro http.cookie en esta captura e indique la información que obtenemos y para qué puede servir en nuestro dictamen.....	15
2.12.	¿Qué direcciones IP origen y destino tiene la trama nº 78?	16
2.13.	Explique la trama nº17 con toda la información que pueda exponer	16

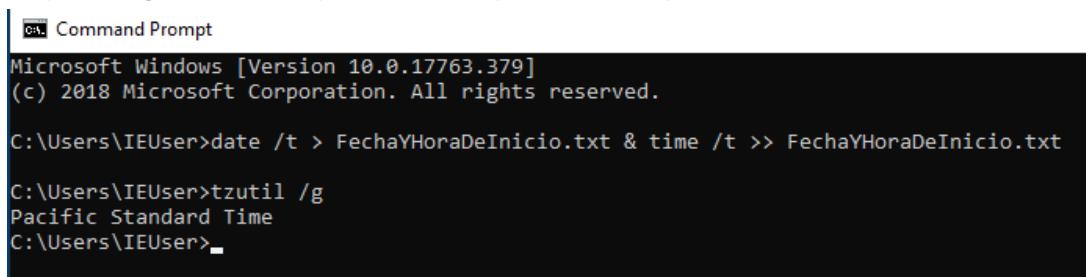
El análisis forense digital es una disciplina clave en la investigación de incidentes de seguridad, ya que permite la recolección y análisis de evidencias digitales para comprender el alcance de un ataque y determinar la responsabilidad de los implicados. En este informe se presentan los hallazgos obtenidos en un análisis forense llevado a cabo sobre un sistema comprometido.

1. Forense en Windows

El proceso de recolección de evidencias se realizó siguiendo el principio de orden de volatilidad, priorizando aquella información que puede desaparecer rápidamente. Cada conjunto de evidencias se acompañó con su correspondiente hash SHA-256 para garantizar la integridad de los datos.

1.1. Hora y fecha del sistema al inicio del análisis

Se debe establecer una línea temporal desde que se empieza a recolectar las evidencias hasta que se finaliza este proceso. En primer lugar, se recoge la fecha y hora de inicio del comienzo del análisis forense. Como se observa en la figura 1, el ordenador está en la zona Pacific Standard Time y en la figura 2 la fecha y la hora en la que se inició el proceso.



```
Command Prompt
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>date /t > FechaYHoraDeInicio.txt & time /t >> FechaYHoraDeInicio.txt

C:\Users\IEUser>tzutil /g
Pacific Standard Time
C:\Users\IEUser>
```

Figura 1. Obtención de tiempo en UTC

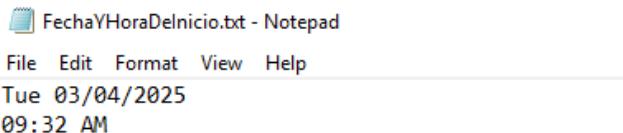
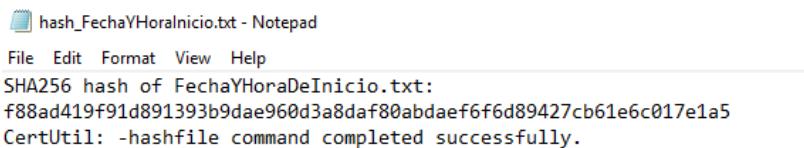


Figura 2. Hora de inicio análisis



```
hash_FechaYHoraDeInicio.txt - Notepad
File Edit Format View Help
SHA256 hash of FechaYHoraDeInicio.txt:
f88ad419f91d891393b9dae960d3a8daf80abdaef6f6d89427cb61e6c017e1a5
CertUtil: -hashfile command completed successfully.
```

Figura 3. Hash evidencia hora de inicio

1.2. Listado de conexiones activas.

El comando **netstat -an** muestra todas las conexiones de red activas en el sistema, incluyendo direcciones IP y puertos en uso. Su análisis es clave para detectar conexiones sospechosas con servidores externos o actividades maliciosas en la red.

```
C:\Users\IEUser>netstat -an >> conexiones_activas.txt
C:\Users\IEUser>certutil -hashfile conexiones_activas.txt SHA256 > hash_conexiones_activas.txt
C:\Users\IEUser>
```

Figura 4. Netstat -an

Proto	Dirección local	Dirección remota	Estado
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49672	0.0.0.0:0	LISTENING
TCP	10.0.2.15:139	0.0.0.0:0	LISTENING
TCP	10.0.2.15:49680	20.93.72.182:443	ESTABLISHED
TCP	10.0.2.15:49762	4.207.247.137:443	ESTABLISHED
TCP	10.0.2.15:50167	104.83.13.150:80	ESTABLISHED
TCP	10.0.2.15:50168	2.23.28.64:443	ESTABLISHED
TCP	10.0.2.15:50169	2.20.253.189:443	ESTABLISHED
TCP	10.0.2.15:50170	2.20.253.189:443	ESTABLISHED
TCP	10.0.2.15:50171	2.20.253.189:443	ESTABLISHED
TCP	10.0.2.15:50172	23.223.88.103:80	ESTABLISHED
TCP	10.0.2.15:50173	77.209.227.80:443	ESTABLISHED
TCP	10.0.2.15:50174	204.79.197.222:443	ESTABLISHED
TCP	10.0.2.15:50175	2.20.253.140:443	ESTABLISHED
TCP	10.0.2.15:50176	20.140.56.69:443	ESTABLISHED
TCP	10.0.2.15:50177	184.24.0.227:80	ESTABLISHED
TCP	10.0.2.15:50178	52.113.196.254:443	ESTABLISHED
TCP	10.0.2.15:50179	13.107.3.254:443	ESTABLISHED
TCP	[::]:135	[::]:0	LISTENING
TCP	[::]:445	[::]:0	LISTENING
TCP	[::]:5985	[::]:0	LISTENING
TCP	[::]:7680	[::]:0	LISTENING
TCP	[::]:47001	[::]:0	LISTENING
TCP	[::]:49664	[::]:0	LISTENING
TCP	[::]:49665	[::]:0	LISTENING

Figura 5. Listado de conexiones activas

```
hash_conexiones_activas.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
SHA256 hash de aplicaciones_puertos.txt:
6d7ebc7bbb7a40ab3f65669458106d07cc7f71a63bd390297b5182173b56369b
CertUtil: -hashfile comando completado correctamente.
```

Figura 6. Hash documento conexiones activas

1.3. Relación de aplicación y puertos abiertos.

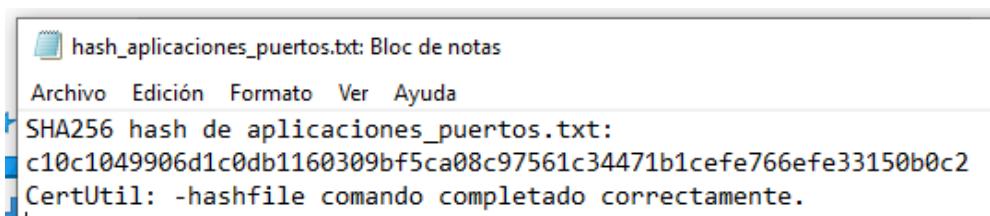
El comando **netstat -bano** permite analizar qué aplicaciones están utilizando puertos abiertos en el sistema. Esta información es esencial para detectar procesos maliciosos que pudieran estar estableciendo conexiones con servidores externos.

```
C:\Users\IEUser>netstat -bano >> aplicaciones_puertos.txt
C:\Users\IEUser>certutil -hashfile aplicaciones_puertos.txt SHA256 > hash_aplicaciones_puertos.txt
```

Figura 7. Netstat -bano

Conexiones activas					
Proto	Dirección local	Dirección remota	Estado	PID	
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	788	RpcSs
[svchost.exe]					
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4	No se puede obtener información de propiedad
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	4016	CDPSSvc
[svchost.exe]					
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4	No se puede obtener información de propiedad
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING	6924	No se puede obtener información de propiedad
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4	No se puede obtener información de propiedad
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	456	No se puede obtener información de propiedad
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	884	EventLog
[svchost.exe]					
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1168	Schedule
[svchost.exe]					
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1984	[spoolsv.exe]
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	548	No se puede obtener información de propiedad
TCP	0.0.0.0:49672	0.0.0.0:0	LISTENING	556	[lsass.exe]
TCP	10.0.2.15:139	0.0.0.0:0	LISTENING	4	No se puede obtener información de propiedad
TCP	10.0.2.15:50225	13.107.253.254:443	ESTABLISHED	4480	[SearchUI.exe]
TCP	10.0.2.15:50229	2.20.253.189:443	ESTABLISHED	4480	[SearchUI.exe]
TCP	10.0.2.15:50230	2.20.253.189:443	ESTABLISHED	4480	[SearchUI.exe]
TCP	10.0.2.15:50232	20.141.12.34:443	ESTABLISHED	4480	[SearchUI.exe]
TCP	10.0.2.15:50235	13.107.226.254:443	ESTABLISHED	4480	[SearchUI.exe]
TCP	10.0.2.15:50344	4.207.247.138:443	ESTABLISHED	2348	WpnService
[svchost.exe]					
TCP	[::]:135	[::]:0	LISTENING	788	RpcSs
[svchost.exe]					

Figura 8. Listado de puertos abiertos



```
hash_aplicaciones_puertos.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
SHA256 hash de aplicaciones_puertos.txt:
c10c1049906d1c0db1160309bf5ca08c97561c34471b1cefef766efe33150b0c2
CertUtil: -hashfile comando completado correctamente.
```

Figura 9. Hash Aplicaciones_puertos

1.4. Caché DNS.

El comando **ipconfig /displaydns** muestra las entradas almacenadas en la caché DNS del sistema, lo que permite analizar los dominios recientemente resueltos. Esta información es útil en el análisis forense para detectar comunicaciones con dominios sospechosos o maliciosos.

```
C:\Users\IEUser>ipconfig /displaydns >>cache_dns.txt
C:\Users\IEUser>certutil -hashfile cache_dns.txt SHA256 > hash_dns.txt
```

Figura 10. Ipconfig /displaydns

```

Configuraci n IP de Windows
array615.prod.do.dsp.mp.microsoft.com
-----
Nombre de registro . . : array615.prod.do.dsp.mp.microsoft.com
Tipo de registro . . : 1
Per odo de vida . . . : 2827
Longitud de datos . . : 4
Secci n . . . . . : respuesta
Un registro (host). . . : 40.69.74.84

array603.prod.do.dsp.mp.microsoft.com
-----
Nombre de registro . . : array603.prod.do.dsp.mp.microsoft.com
Tipo de registro . . : 1
Per odo de vida . . . : 2256
Longitud de datos . . : 4
Secci n . . . . . : respuesta
Un registro (host). . . : 13.74.138.254

array619.prod.do.dsp.mp.microsoft.com
-----
Nombre de registro . . : array619.prod.do.dsp.mp.microsoft.com
Tipo de registro . . : 1
Per odo de vida . . . : 2684
Longitud de datos . . : 4
Secci n . . . . . : respuesta
Un registro (host). . . : 13.74.187.43

```

Figura 11. Listado de cache DNS

```

hash_dns.txt: Bloc de notas
Archivo Edici n Formato Ver Ayuda
SHA256 hash de cache_dns.txt:
d61a30eaf21fb99d3fffc42d5cee7dc8503fd69102e3dcc2918de03e03cccd3a8
CertUtil: -hashfile comando completado correctamente.

```

Figura 12. Hash cache DNS

1.5. Cach  ARP.

La cach  ARP permite analizar la correspondencia entre direcciones IP y MAC en una red local. Su an lisis es crucial en la detecci n de ataques de suplantaci n de identidad (ARP Spoofing), que pueden ser utilizados en ataques de tipo Man-in-the-Middle (MITM).

```

C:\Users\IEUser>arp -a >> cache_arp.txt
C:\Users\IEUser>certutil -hashfile cache_arp.txt SHA256 > hash_cache_arp.txt

```

Figura 13. arp -a

Interfaz: 10.0.2.15 --- 0x5	Direcci�n de Internet	Direcci�n f�sica	Tipo
10.0.2.2	52-55-0a-00-02-02	din mico	
10.0.2.3	52-55-0a-00-02-03	din mico	
10.0.2.255	ff-ff-ff-ff-ff-ff	est tico	
224.0.0.22	01-00-5e-00-00-16	est tico	
224.0.0.251	01-00-5e-00-00-fb	est tico	
224.0.0.252	01-00-5e-00-00-fc	est tico	
239.255.255.250	01-00-5e-7f-ff-fa	est tico	
255.255.255.255	ff-ff-ff-ff-ff-ff	est tico	

Figura 14. Listado direcciones ip/MAC

```

hash_cache_arp.txt: Bloc de notas
Archivo Edici n Formato Ver Ayuda
SHA256 hash de cache_arp.txt:
4c59a7a4671a54f932bdef92338b080b771b2c5935f92eeaeef5a20eec5c9751
CertUtil: -hashfile comando completado correctamente.

```

Figura 15. Hash cache ARP

1.6. Tráfico por proceso.

El comando **tasklist /v** proporciona una lista detallada de los procesos en ejecución en el sistema, incluyendo el identificador de proceso (PID), el nombre de la imagen, el estado del proceso y más información sobre los recursos que están siendo utilizados. Este comando es fundamental en un análisis forense para identificar procesos sospechosos o maliciosos.

```
C:\Users\IEUser>tasklist /v >> trafico_por_proceso.txt  
C:\Users\IEUser>certutil -hashfile trafico_por_proceso.txt SHA256 > hash_trafico_por_proceso.txt
```

Figura 16. Tasklist /v

Nombre de imagen	PID	Nombre de sesión	Nº	Em. de ses	Uso de memor	Estado	Nombre de usuario	Tiempo de CP	Ti;tu:
System Idle Process	0	Services	0		8 KB	Unknown	NT AUTHORITY\SYSTEM	5:35:05 N/D	
System	4	Services	0		24 KB	Unknown	N/D	0:03:32 N/D	
Registry	68	Services	0		23.880 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:04 N/D	
sms.exe	292	Services	0		356 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
cssss.exe	388	Services	0		1.752 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
wininit.exe	456	Services	0		896 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
cssss.exe	464	Console	1		2.212 KB	Running	NT AUTHORITY\SYSTEM	0:00:01 N/D	
winlogon.exe	524	Console	1		4.308 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
services.exe	548	Services	0		5.560 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:05 N/D	
lsass.exe	558	Services	0		10.620 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:06 N/D	
fontdrvhost.exe	672	Console	1		1.820 KB	Unknown	Fon Driver Host\UMFD-1	0:00:00 N/D	
fontdrvhost.exe	680	Services	0		1.092 KB	Unknown	Fon Driver Host\UMFD-0	0:00:00 N/D	
svchost.exe	688	Services	0		988 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
svchost.exe	748	Services	0		16.900 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:10 N/D	
svchost.exe	788	Services	0		9.876 KB	Unknown	NT AUTHORITY\NETWORK SERVICE	0:00:17 N/D	
svchost.exe	832	Services	0		3.168 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
dwm.exe	896	Console	1		55.892 KB	Running	Window Manager\DIM-1	0:00:06 DWM I	
svchost.exe	980	Services	0		2.068 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/D	
svchost.exe	320	Services	0		4.748 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/D	
svchost.exe	236	Services	0		4.788 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
svchost.exe	884	Services	0		9.488 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:01 N/D	
svchost.exe	1044	Services	0		4.692 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/D	
svchost.exe	1064	Services	0		3.680 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/D	
svchost.exe	1124	Services	0		6.672 KB	Unknown	NT AUTHORITY\NETWORK SERVICE	0:00:00 N/D	
svchost.exe	1148	Services	0		4.152 KB	Unknown	NT AUTHORITY\NETWORK SERVICE	0:00:01 N/D	
svchost.exe	1168	Services	0		8.616 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:02 N/D	
\BoxService.exe	1260	Services	0		3.564 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:05 N/D	
svchost.exe	1320	Services	0		5.020 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
svchost.exe	1336	Services	0		4.152 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/D	
svchost.exe	1356	Services	0		54.156 KB	Unknown	NT AUTHORITY\SYSTEM	0:01:28 N/D	
svchost.exe	1388	Services	0		1.444 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
svchost.exe	1508	Services	0		5.888 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:01 N/D	
svchost.exe	1516	Services	0		5.188 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
Memory Compression	1528	Services	0		100.020 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:03 N/D	
svchost.exe	1598	Services	0		2.184 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
svchost.exe	1616	Services	0		2.956 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/D	
svchost.exe	1742	Services	0		3.432 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/D	
svchost.exe	1804	Services	0		4.692 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:01 N/D	
svchost.exe	1812	Services	0		1.880 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/D	
svchost.exe	1824	Services	0		5.488 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/D	
svchost.exe	1888	Services	0		3.748 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/D	
svchost.exe	1928	Services	0		2.532 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
spoolsv.exe	1994	Services	0		2.332 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	
svchost.exe	2016	Services	0		11.260 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:00 N/D	
svchost.exe	2024	Services	0		2.238 KB	Unknown	NT AUTHORITY\NETWORK SERVICE	0:00:00 N/D	
svchost.exe	2176	Services	0		25.776 KB	Unknown	NT AUTHORITY\NETWORK SERVICE	0:00:04 N/D	
svchost.exe	2188	Services	0		20.668 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:03 N/D	
svchost.exe	2204	Services	0		20.924 KB	Unknown	NT AUTHORITY\LOCAL SERVICE	0:00:05 N/D	
svchost.exe	2216	Services	0		12.760 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:16 N/D	
svchost.exe	2228	Services	0		3.336 KB	Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/D	

Figura 17. Listado procesos

```
hash_trafico_por_proceso.txt: Bloc de notas  
Archivo Edición Formato Ver Ayuda  
SHA256 hash de trafico_por_proceso.txt:  
58cd6df84bf2eb8f9aa20888d32ba7768162fa35337c05bb2a990ca78f1189f8a  
CertUtil: -hashfile comando completado correctamente.
```

Figura 18. Hash listado procesos

1.7. Estadística de las conexiones actuales.

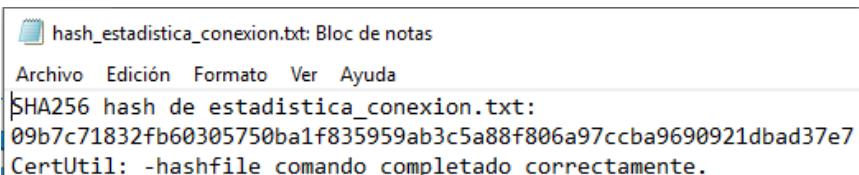
El comando **netstat -e** muestra estadísticas relacionadas con las conexiones de red, incluyendo la cantidad de paquetes enviados y recibidos, los errores, y las colisiones. Este tipo de información es útil para evaluar la salud general de la red, así como para detectar actividad anómala.

```
C:\Users\IEUser>netstat -e >> estadisticaConexion.txt  
C:\Users\IEUser>certutil -hashfile estadisticaConexion.txt SHA256 > hash_EstadisticaConexion.txt
```

Figura 19. Netstat -e

Estadísticas de interfaz		
	Recibidos	Enviados
Bytes	860058024	12623216
Paquetes de unidifusión	638012	99188
Paquetes no de unidifusión	164	1980
Descartados	0	0
Errores	0	0
Protocolos desconocidos	0	

Figura 20. Estadística de conexiones activas



hash_EstadisticaConexion.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
SHA256 hash de estadisticaConexion.txt:
09b7c71832fb60305750ba1f835959ab3c5a88f806a97ccba9690921dbad37e7
CertUtil: -hashfile comando completado correctamente.

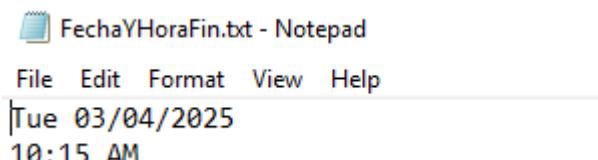
Figura 21. Hash Estadística de conexiones

1.8. Hora y fecha de fin

Tras adquirir todas las evidencias, se debe registrar la hora y fecha final para cerrar la línea de tiempo de adquisición.

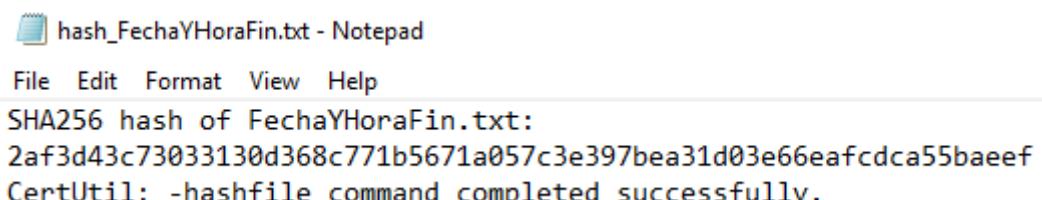
```
C:\Users\IEUser>date /t > FechaYHoraFin.txt & time /t >> FechaYHoraFin.txt  
C:\Users\IEUser>certutil -hashfile FechaYHoraFin.txt SHA256 > hash_FechaYHoraFin.txt
```

Figura 22. Registro de hora y fecha fin



FechaYHoraFin.txt - Notepad
File Edit Format View Help
Tue 03/04/2025
10:15 AM

Figura 23. Hora y fecha fin



hash_FechaYHoraFin.txt - Notepad
File Edit Format View Help
SHA256 hash of FechaYHoraFin.txt:
2af3d43c73033130d368c771b5671a057c3e397bea31d03e66eafcdca55baeeff
CertUtil: -hashfile command completed successfully.

Figura 24. Hash fecha y hora fin

1.9. Análisis de evidencias

a. Caché ARP (arp -a)

❖ ¿Qué información proporciona esta orden?

El comando arp -a muestra la caché ARP del sistema, que contiene la relación entre direcciones IP y direcciones MAC en la red local. Esta información es esencial para analizar cómo un equipo ha estado comunicándose con otros dispositivos en la misma red.

❖ ¿Para qué se usa en análisis forense?

El análisis de la caché ARP es útil para detectar ataques de *ARP Spoofing*, una técnica en la que un atacante falsifica la dirección MAC de otro dispositivo para interceptar tráfico de red o redirigir conexiones.

❖ Ejemplo de Incidente: Ataque Man-in-the-Middle (MITM) usando ARP Spoofing

Un usuario reporta que su sesión en un sistema de banca en línea ha sido comprometida a pesar de haber iniciado sesión desde una red supuestamente segura. El análisis forense mediante este comando revela que la dirección IP del router legítimo (192.168.1.1) ha sido suplantada por una dirección MAC desconocida.

Salida sospechosa del comando arp -a en un equipo comprometido:

Interfaz: 192.168.1.100

Dirección IP	Dirección física	Tipo
192.168.1.1	00-14-22-01-23-45	Dinámico
192.168.1.1	54-52-00-1A-2B-3C	Dinámico

En este caso, hay dos direcciones MAC asociadas a la misma IP del router, lo cual es un claro indicio de ARP Spoofing. Un atacante ha suplantado la dirección del gateway para redirigir el tráfico a su propio dispositivo, permitiéndole interceptar credenciales bancarias o cualquier otro tráfico sensible.

El análisis de la caché ARP puede ayudar a identificar un ataque Man-in-the-Middle (MITM) en tiempo real, permitiendo tomar medidas correctivas como el uso de IP estáticas y la implementación de protecciones ARP en los switches de la red.

b. Relación de Aplicaciones y Puertos Abiertos (netstat -ban)

❖ ¿Qué información proporciona esta orden?

El comando netstat -ban muestra qué procesos están utilizando qué puertos en el sistema, incluyendo:

- PID (Process ID) del programa.
- Dirección remota con la que está estableciendo conexión.
- Estado de la conexión (LISTENING, ESTABLISHED, TIME_WAIT).
- Ruta del ejecutable que está usando la conexión.

❖ ¿Para qué se usa en análisis forense?

Este comando es fundamental para detectar procesos *maliciosos* que han establecido conexiones no autorizadas con servidores externos. Es clave en la detección de malware, troyanos, puertas traseras y botnets.

❖ **Ejemplo de Incidente: Un Malware con Conexión a un Servidor de Comando y Control (C2)**

Un usuario reporta que su equipo se ha vuelto lento y muestra un uso elevado de red sin ninguna aplicación abierta. Al ejecutar netstat -ban, se observa lo siguiente:

Protocolo	Dirección local	Dirección Remota	Estado	PID
Tcp	192.168.1.100	185.220.101.6:443	ESTABLISHED	4321

[malware.exe]

Análisis Forense:

- Se detecta que el proceso malware.exe está manteniendo una conexión establecida con 185.220.101.6 en el puerto 443.
- Una búsqueda en bases de datos de amenazas revela que 185.220.101.6 está asociada a un servidor de Comando y Control (C2) utilizado en botnets.
- Se confirma que el equipo está infectado con un troyano que está recibiendo instrucciones desde el atacante.

Gracias al uso de netstat -ban, se puede identificar una conexión maliciosa establecida por un malware que estaba operando de manera oculta en el sistema.

2. Forense en Email

2.1. Nombre del cliente de correo electrónico

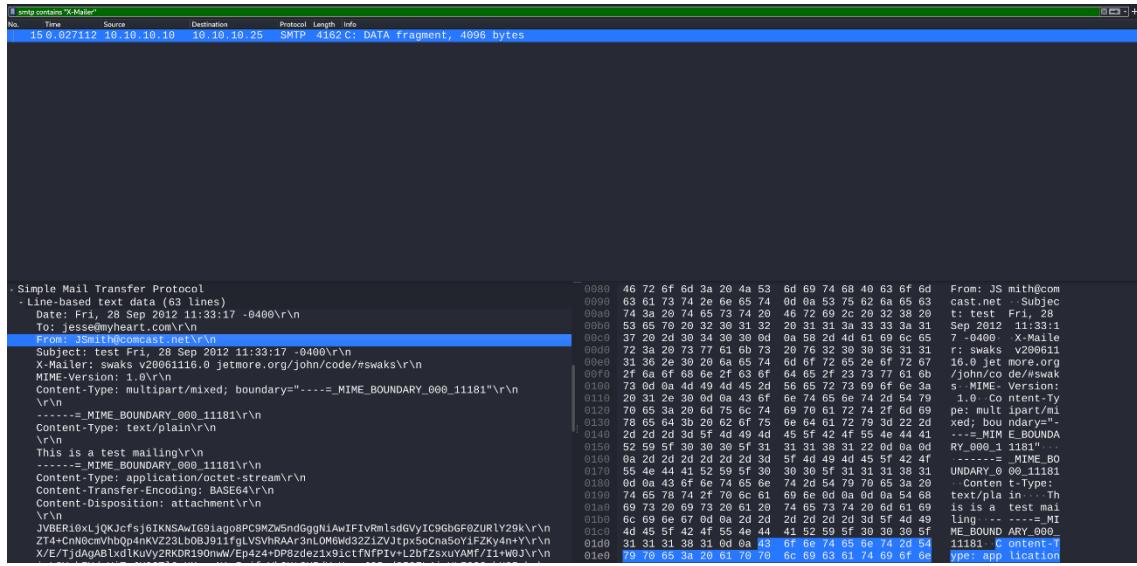


Figura 25. Captura de Wireshark con el filtro smtp y el operador contains

Filtro: smtp contains "X-Mailer"

El primer paso ha sido aplicar un filtro en Wireshark, para identificar la línea en la que nos dice el cliente de correo que se usa, que en este caso es Swaks, una herramienta usada para hacer pruebas de servidores de correo SMTP.

Para explicar este filtro X-Mailer es un campo estándar en los correos que contiene el nombre del software que se utilizó para enviar el mensaje, por lo que el filtro nos da solo los elementos que han pasado por el protocolo SMTP y que contengan esta cabecera.

2.2. ¿Cuál es la dirección de e-mail origen del envío?

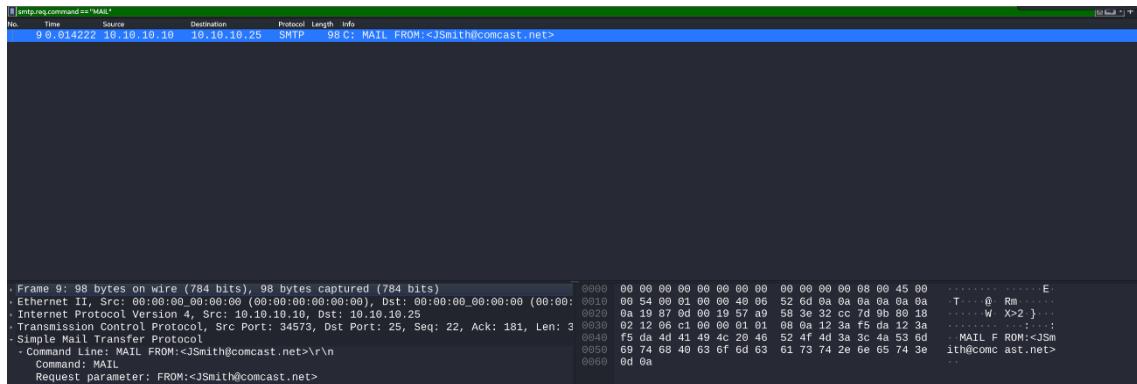


Figura 26. Captura de Wireshark con el filtro smtp.req.command

Filtro: smtp.req.command == "MAIL"

Para este ejercicio hemos usado un filtro que permite obtener la información relevante sobre el remitente del correo electrónico desde el tráfico SMTP. Este filtro en concreto permite aislar específicamente el comando MAIL, que es utilizado en el protocolo SMTP para indicar el inicio de la transferencia de un correo y como se puede ver en el "MAIL FROM" se especifica la dirección de correo electrónico de origen, que en este caso es JSmith@comcast.net.

2.3. ¿Cuál es la dirección de e-mail destino?

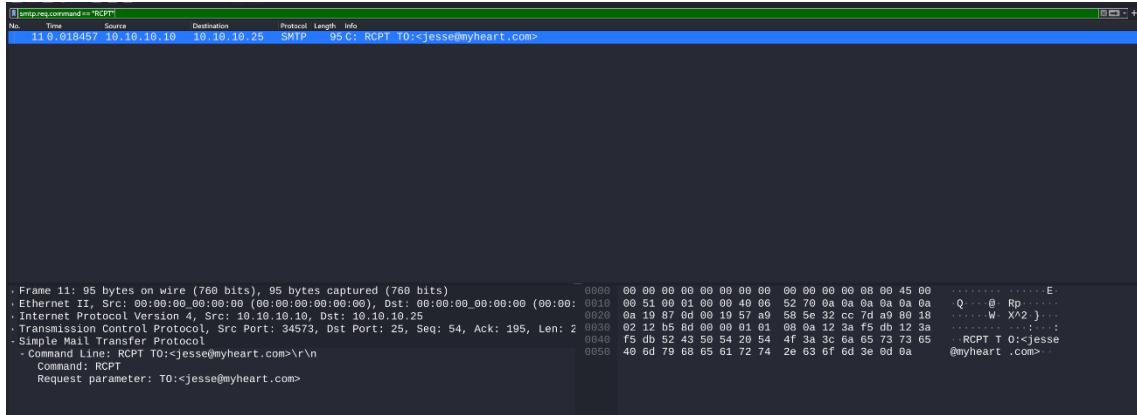


Figura 27. Wireshark con el filtro smtp.req.command

Filtro: smtp.req.command == "RCPT"

Este filtro es utilizado en el protocolo SMTP para especificar el destinatario del correo, permite ver los paquetes relacionados con el comando RCPT que es el que indica a qué dirección de correo electrónico se está enviando el mensaje.

El campo RCPT TO especifica la dirección de correo electrónico del destinatario. En este caso, la dirección de correo electrónico de destino es jesse@myheart.com.

2.4. ¿Qué sistema operativo alberga el servicio SMTP?

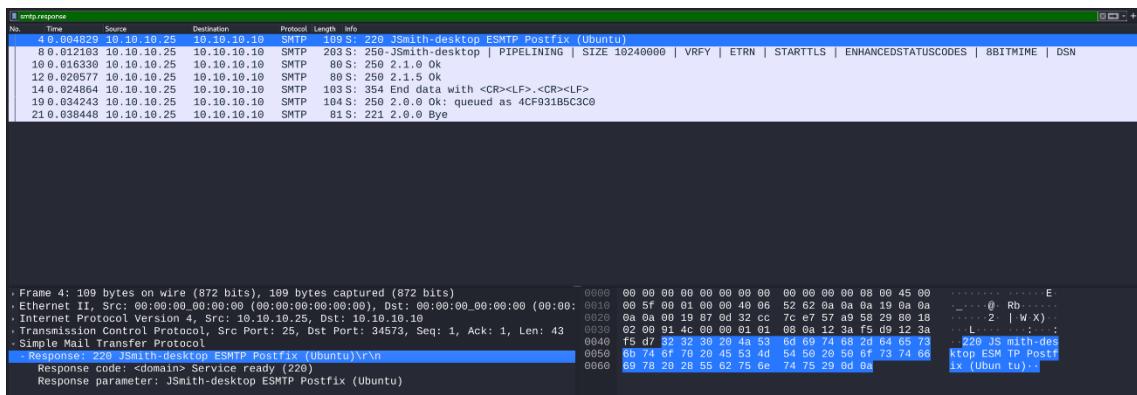


Figura 28. Wireshark con el filtro smtp.response

Filtro: smtp.response

Muchas veces el servidor SMTP responde con un banner que contiene información sobre el sistema operativo utilizado, en este caso se puede ver: 220 JSmith-desktop ESMTP Postfix

(Ubuntu). Postfix sería el servidor de correo que se está utilizando lo cual ya nos da una pista de que puede ser un sistema Linux, pero esto se confirma al ver Ubuntu y con esto sabemos exactamente la distribución que tiene de Linux.

2.5. ¿Cuál es el nombre del software usa el servicio SMTP?

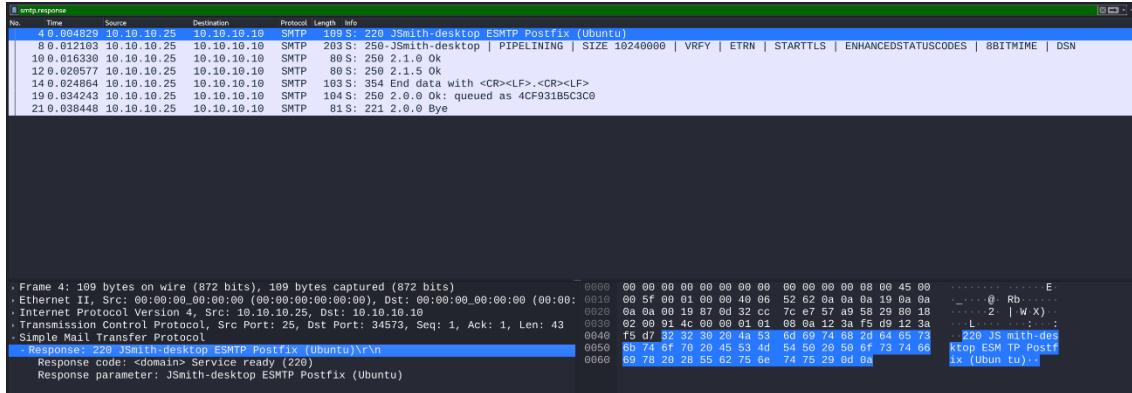


Figura 29. Wireshark con el filtro smtp.response

Filtro: smtp.response

Esta pregunta ya está resuelta con el anterior apartado, se sabe con el mismo filtro y se encuentra la información en la misma línea. En este caso el software utilizado es Postfix que es un servidor de correo electrónico de código abierto para gestionar el correo electrónico en sistemas Linux. Es uno de los servidores de correo más famosos debido a su rendimiento y enfoque en la seguridad. Como dato curioso acerca de la seguridad de este software, soporta la autenticación de correo electrónico SASL lo que lo hace más seguro que otros.

2.6. ¿Qué puerto de origen y destino aparece en la parte de TCP de la trama nº20?

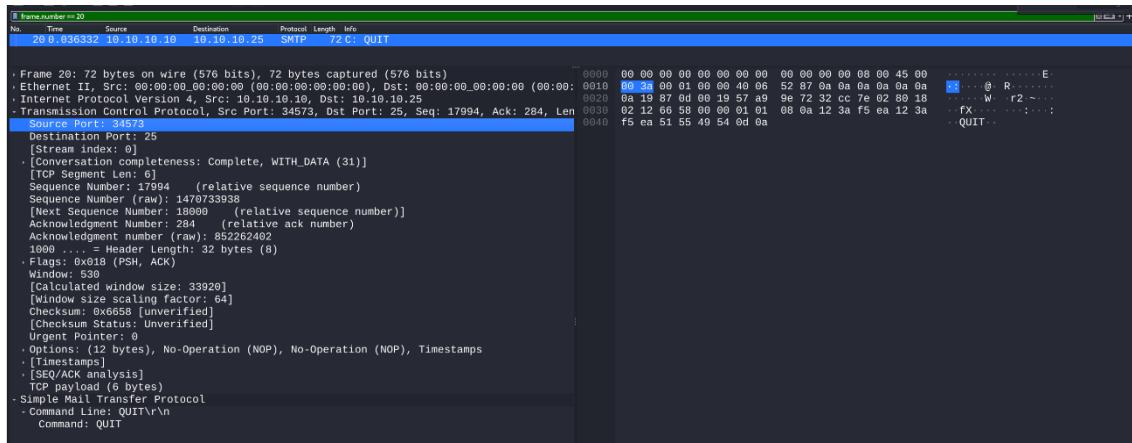


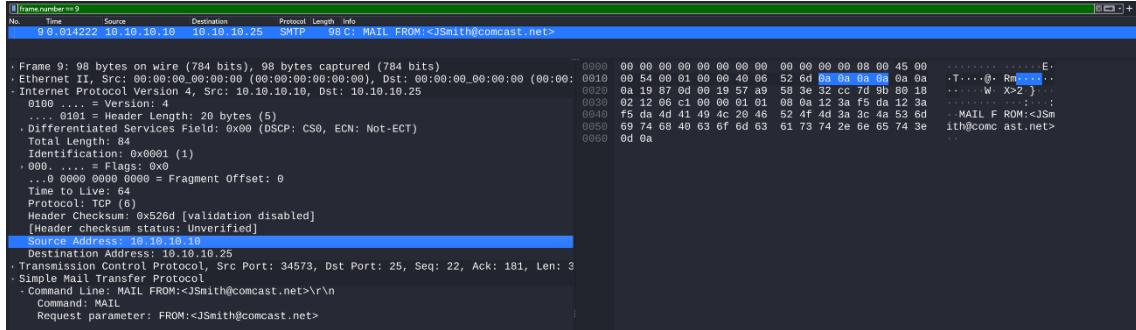
Figura 30. Wireshark con el filtro frame.number

Filtro: frame.number == 20

Con este filtro podemos ver la información detallada del tráfico TCP en la trama SMTP (nº20). Aquí se encuentra la información sobre los puertos de origen y destino utilizados. En este caso el puerto de origen es el 34573 y es el puerto desde el cual se inicia la conexión en el lado del cliente

para establecer la comunicación con el servidor SMTP. El puerto de destino es el 25, que es el puerto estándar utilizado por el protocolo SMTP.

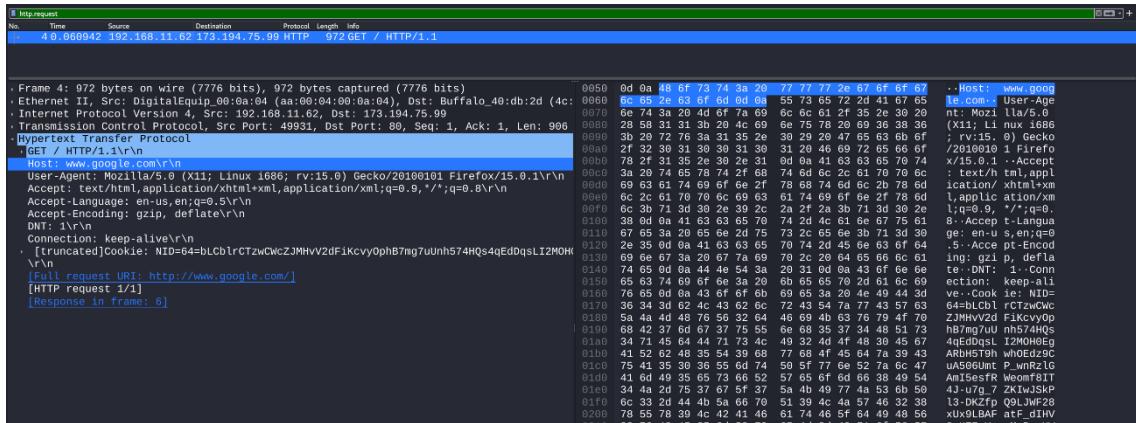
2.7. ¿Cuál es la dirección IP origen y destino de la trama nº9?



Filtro: frame.number == 9

En esta captura vemos que la dirección IP de origen está indicada como 10.10.10.10. Esta es la dirección del dispositivo que está enviando la solicitud SMTP. Y la dirección IP de destino es la 10.10.10.25 que es la dirección del servidor que recibe la solicitud SMTP.

2.8. ¿Qué servidor (nombre) está involucrado en la petición http de esta captura?



Filtro: http.request

En este apartado hemos analizado el segundo archivo .pcap aplicando un filtro nos deja ver el tráfico HTTP. Aquí se puede ver que está siendo procesado y podemos ver el servidor involucrado en la petición al revisar los detalles del encabezado en la solicitud. El valor del campo host nos dice que el servidor al que se está realizando la solicitud es www.google.com.

2.9. ¿Cuál es el puerto origen y destino de la trama nº 6?

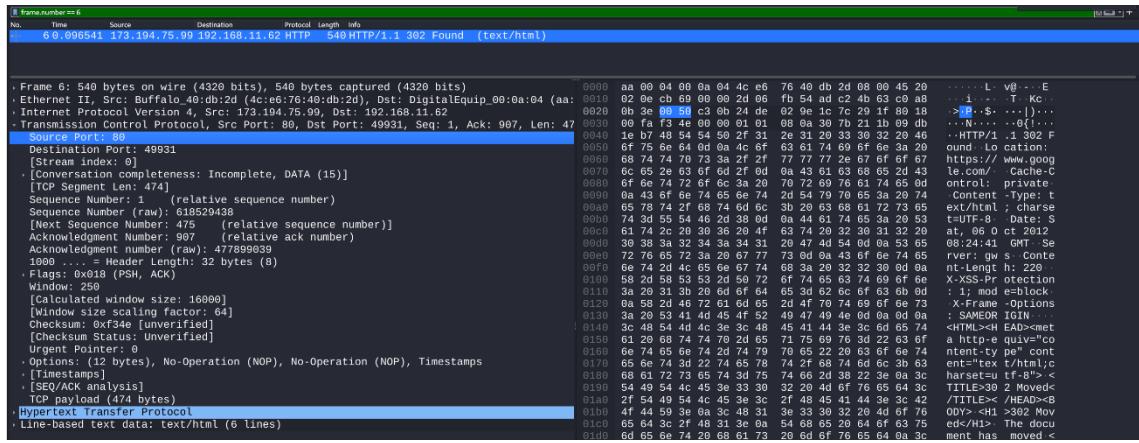


Figura 33. Wireshark con el filtro frame.number

Filtro: frame.number == 6

Al igual que en uno de los apartados anteriores, mediante este filtro podemos ver que en la sección de la trama TCP, el puerto de origen, es decir el puerto desde el cual se inicia la conexión en el lado del cliente para comunicarse con el servidor HTTP, es el 49931 y el puerto de destino es el 80, que es el puerto estándar utilizado por el protocolo HTTP.

2.10. Indique la siguiente información de la trama nº4 y cómo la ha conseguido:

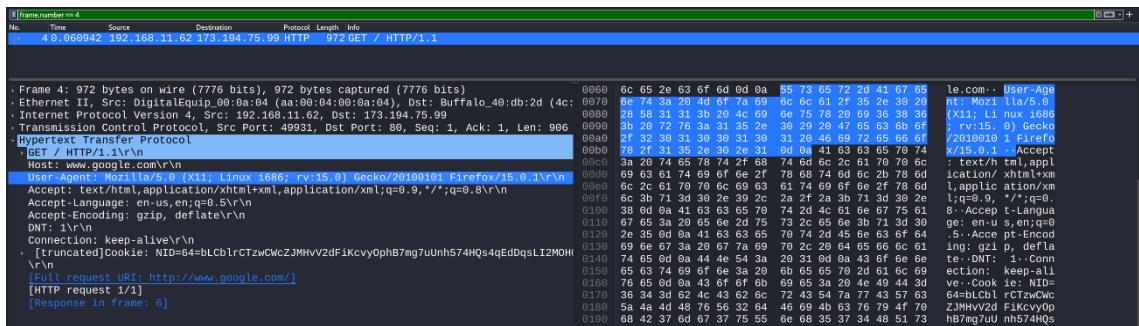


Figura 34. Wireshark con el filtro frame.number

Las solicitudes HTTP contienen varios encabezados relevantes que nos dicen el navegador, sistema operativo y host que se han utilizado. Utilizando el filtro de frame.number, pero con la trama número 4 podemos responder a las siguientes preguntas.

¿Qué navegador ha hecho la petición? ¿Qué versión?

El campo User-Agent contiene información sobre el navegador y la versión. El encabezado relevante es:

User-Agent: Mozilla/5.0 (X11; Linux i686; rv:15.0) Gecko/20100101 Firefox/15.0.1

Con esto sabemos que el navegador que ha hecho la petición es Firefox en su versión 15.0.1.

¿Qué sistema operativo?

En el mismo campo se puede ver que el sistema operativo utilizado es Linux (específicamente una versión para arquitectura i686, que corresponde a una arquitectura de 32 bits).

¿A qué host se ha solicitado la petición?

El campo Host en la solicitud HTTP se ve la dirección del servidor al que se ha enviado la petición. En este caso es www.google.com

2.11. Compruebe el filtro http.cookie en esta captura e indique la información que obtenemos y para qué puede servir en nuestro dictamen.

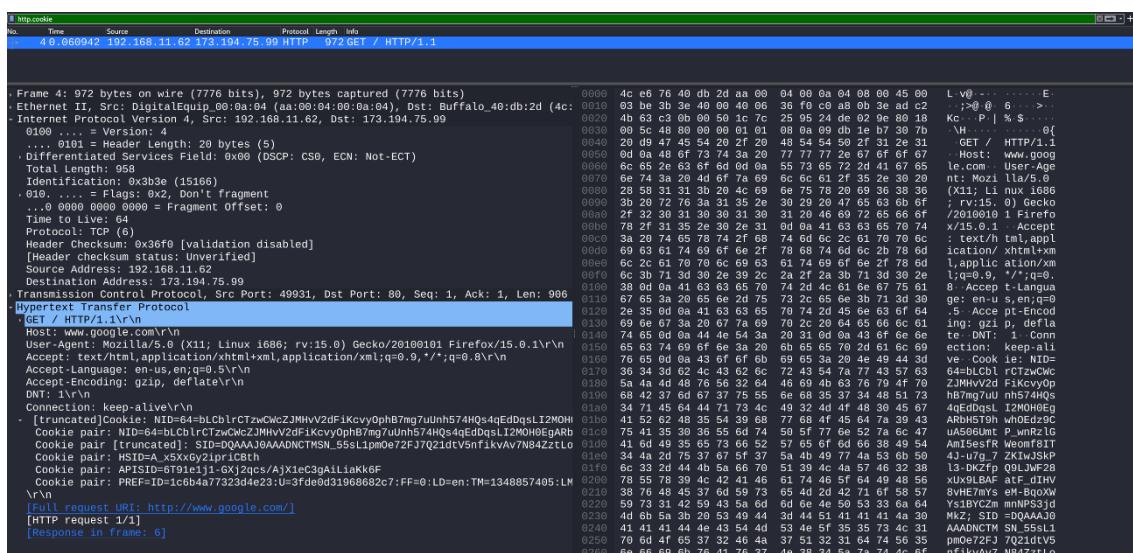


Figura 35. Wireshark con el filtro http.cookie

Filtro: http.cookie

Este filtro nos deja ver las cookies enviadas por el cliente en las solicitudes HTTP.

En este caso la cookie que se envía es Cookie: NID=64=LbCbrCTzCWCZJMHvV2dF... donde NID=64 es la clave de la cookie que está asociada a un identificador único utilizado para almacenar información sobre las preferencias del usuario. El resto representa un identificador único relacionado con la actividad del usuario en el sitio web.

Esto es muy relevante en un análisis forense para seguir la pista de actividades en un sitio web. Si hay una sospecha de un acceso no autorizado o de actividad maliciosa, las cookies pueden ayudar a identificar si la sesión fue iniciada por un usuario legítimo o no. Además, las cookies también se utilizan para mantener sesiones activas, lo que es útil para las investigaciones para ayudar a recuperar información sobre el estado de la sesión de un usuario en el momento en que ocurrió un incidente de seguridad.

2.12. ¿Qué direcciones IP origen y destino tiene la trama nº 78?

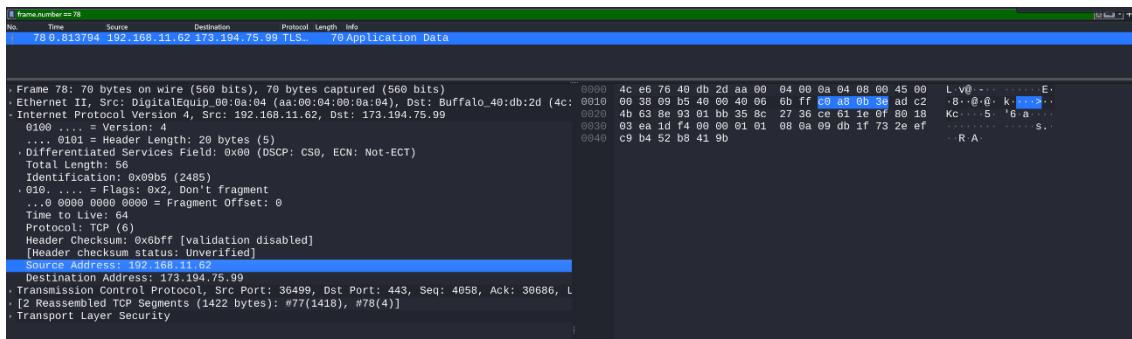


Figura 36. Wireshark con el filtro frame.number

Filtro: frame.number == 78

Mediante este filtro podemos ver que la dirección IP de origen es la 192.168.11.62 y la dirección IP de destino es la 173.194.75.99.

¿Cuál de las dos corresponde con el servidor en internet?

La primera dirección, la de origen, corresponde a una IP interna, es decir, de una red local. Las direcciones IP que comienzan con 192.168.x.x están reservadas para redes las privadas.

La segunda dirección, la de destino, es una IP pública ya que está en el rango de direcciones públicas, por lo que se puede deducir que corresponde al servidor en internet al que se realizó la solicitud y parece ser una dirección de Google al ver su registro whois.

IP Whois	
NetRange:	173.194.0.0 - 173.194.255.255
CIDR:	173.194.0.0/16
NetName:	GOOGLE
NetHandle:	NET-173-194-0-0-1
Parent:	NET173 (NET-173-0-0-0-0)
NetType:	Direct Allocation
OriginAS:	AS15169
Organization:	Google LLC (GOGL)
RegDate:	2009-08-17
Updated:	2012-02-24
Ref:	https://rdap.arin.net/registry/ip/173.194.0.0

Figura 37. Consulta WHOIS de la dirección IP pública

2.13. Explique la trama nº17 con toda la información que pueda exponer



Figura 38. Wireshark con el filtro frame.number

Filtro: frame.number == 17

En esta trama se observa una solicitud de Client Hello dentro del protocolo TLSv1 (Transport Layer Security versión 1). Este es el primer paso para establecer una conexión segura con el

servidor, en este caso, www.google.com y el propósito de este mensaje es permitir que el cliente y el servidor negocien los parámetros de la conexión segura, como los algoritmos de cifrado y la versión de TLS que se utilizará.

En esta solicitud también se incluye el parámetro SNI (Server Name Indication), el cual le indica al servidor qué dominio está solicitando el cliente. Esto es útil cuando varios dominios están alojados en el mismo servidor o dirección IP, como es común en los servicios de Google. El SNI permite que el servidor seleccione el certificado SSL/TLS correcto para la conexión.

La dirección IP origen de esta trama es 192.168.11.62, lo que indica que la solicitud proviene de una máquina en una red local, y la dirección IP destino es 173.194.75.99, una dirección asociada con Google, que indica que la solicitud está siendo enviada a un servidor en Internet.