CyberDefenders

RESOLUCIÓN DE LABORATORIO

Caso: PacketMaze (CyberDefenders)

Documentación técnica y resolución paso a paso de un escenario de Network Forensics basado en la captura de tráfico (PCAP) de una posible amenaza interna.

Sebastian David
Torres Reyes

Escenario:

El servidor interno de una empresa ha sido detectado por actividad de red inusual, con múltiples conexiones salientes a una IP externa desconocida. El análisis inicial sugiere una posible exfiltración de datos. Investigue los registros de red proporcionados para determinar el origen y el método de la vulneración.

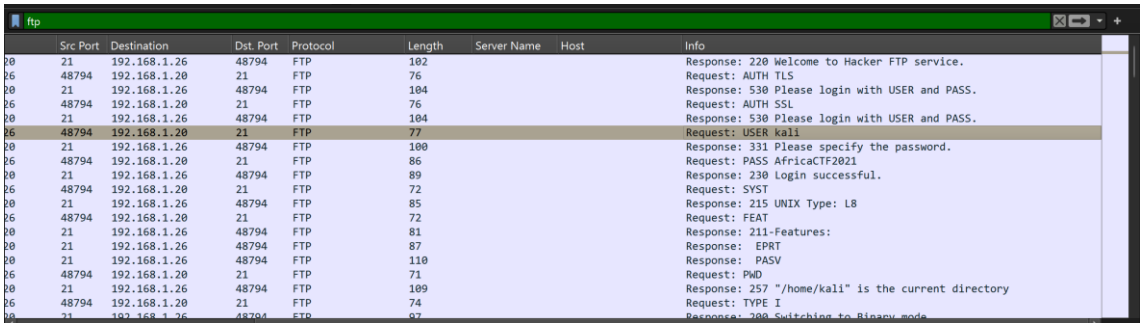
Herramientas utilizadas:

- Wireshark

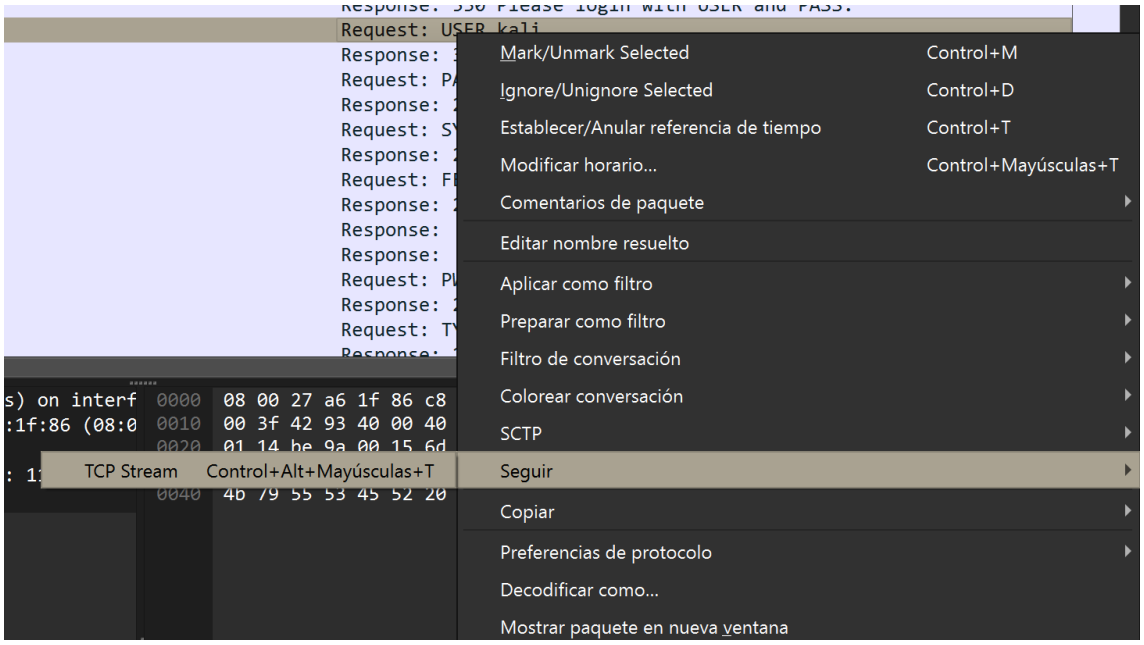
P1: ¿Cuál es la contraseña FTP?

R: AfricaCTF2021

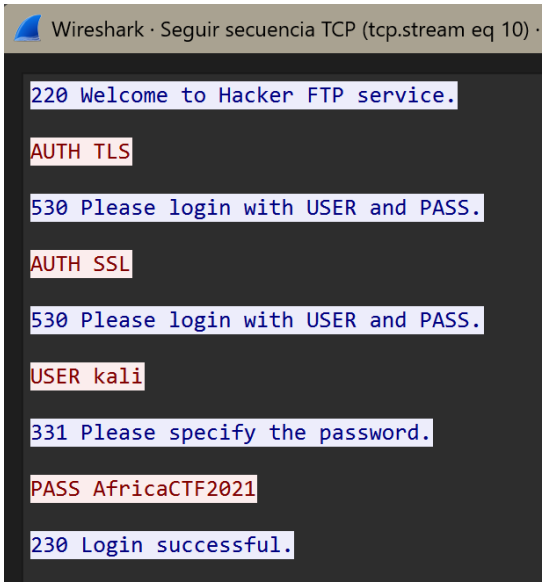
Para visualizar solamente paquetes FTP se aplicó el filtro “ftp” y se pudo verificar la información de cada paquete.



Se pudo ver en orden las solicitudes y respuesta entre el cliente y el servidor donde se realiza la autenticación, entonces se hizo el seguimiento del flujo TCP.



Se puede ver la comunicación del servidor y cliente en el paquete seleccionado, entonces después de que el cliente ingrese la contraseña el servidor emitirá un mensaje “230 Login successful”. Con esto se concluyó que la contraseña del servidor FTP es “AfricaCTF2021”

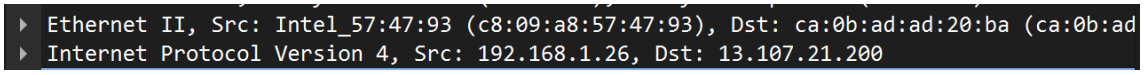


P2: ¿Cuál es la dirección IPv6 del servidor DNS utilizado por 192.168.1.26?

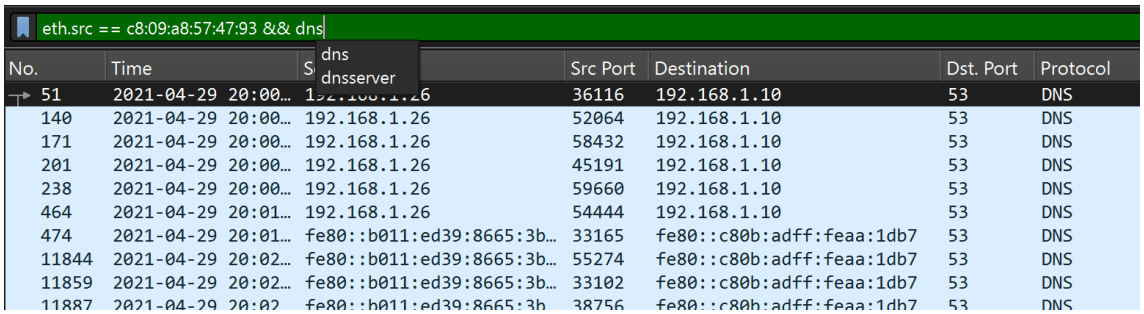
R: fe80::c80b:adff:feaa:1db7

Para saber la dirección IPv6 del servidor DNS usado por la dirección IPv4 192.168.1.26 primero se debe saber cuál es la dirección IPv6 asociada a esta

dirección IPv4 entonces se usó el filtro “ip.addr == 192.168.1.26” para esto se usó la dirección física, MAC, la cual es “c8:09:a8:57:47:93”.



Sabiendo esto, se pudo filtrar por la dirección MAC para estar seguro de cual es la dirección IPv6; también se necesitó ver solamente los paquetes DNS con el filtro “eth.src == c8:09:a8:57:47:93 && dns”, el proceso para saber la dirección IPv6 asociada no es necesario si se tiene acceso al host.

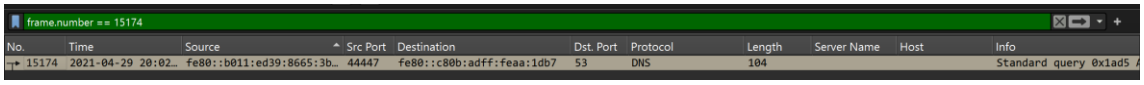


Como se puede observar, hay una dirección IPv4 y otra dirección IPv6 asociada a la dirección MAC, entonces si se selecciona cualquier PDU de la dirección IPv6 se puede observar la dirección IPv6 del servidor DNS en la columna de “Destination” que sería “fe80::c80b:adff:feaa:1db7”.

P3: ¿Qué dominio está buscando el usuario en el paquete 15174?

R: www.7-zip.org

Para situarse solamente en el paquete 15174 se aplicó el filtro “frame.number == 15174”.



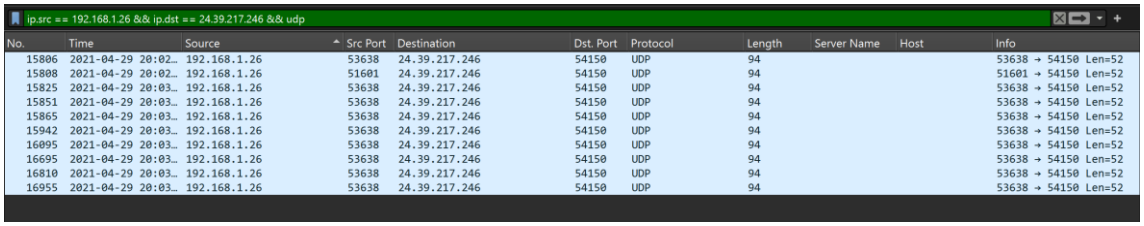
Luego en la información de la solicitud DNS se encontró el dominio que el usuario buscó el cual sería “www.7-zip.org”

```
▸ Ethernet II, Src: Intel_57:47:93 (c8:09:a8:57:47:93), Dst: ca:0b:ad:ad:20:ba (ca:0b:
▸ Internet Protocol Version 6, Src: fe80::b011:ed39:8665:3b0a, Dst: fe80::c80b:adff:fe
▸ User Datagram Protocol, Src Port: 44447, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x1ad5
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ www.7-zip.org: type A, class IN
        Name: www.7-zip.org
        [Name Length: 13]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ▸ Additional records
    [Response In: 15190]
```

P4: ¿Cuántos paquetes UDP se enviaron desde 192.168.1.26 a 24.39.217.246?

R: 10

Para saber el número de paquetes UDP que se enviaron desde la dirección IP 192.168.1.26 a la dirección IP 24.39.217.246 se aplicó el filtro “ip.src == 192.168.1.26 && ip.dst == 24.39.217.246 && udp” resultando en 10 paquetes.

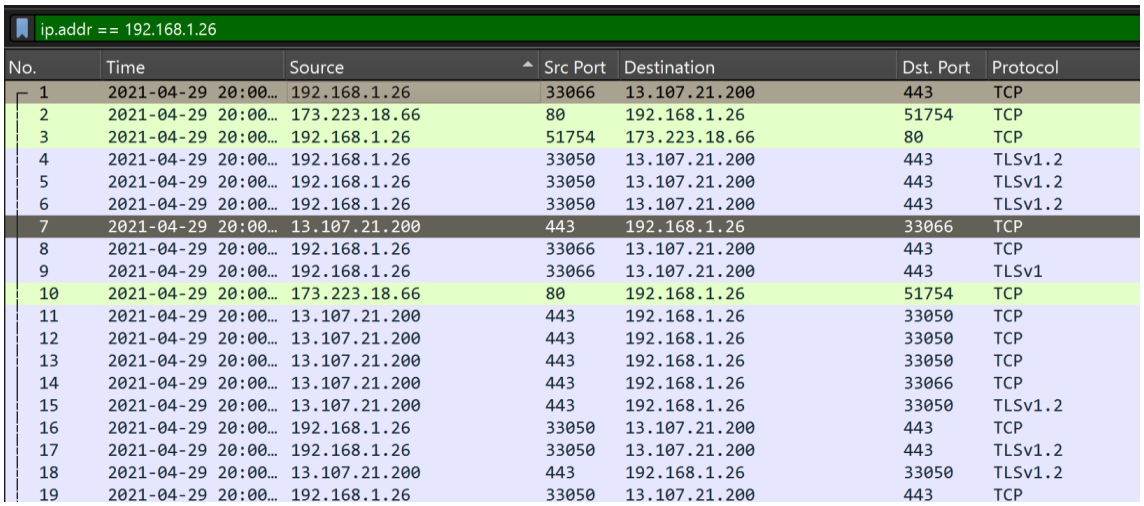

ip.src == 192.168.1.26 && ip.dst == 24.39.217.246 && udp

No.	Time	Source	Src Port	Destination	Dst. Port	Protocol	Length	Server Name	Host	Info
15806	2021-04-29 20:02…	192.168.1.26	53638	24.39.217.246	54150	UDP	94			53638 → 54150 Len=52
15808	2021-04-29 20:02…	192.168.1.26	51601	24.39.217.246	54150	UDP	94			51601 → 54150 Len=52
15825	2021-04-29 20:03…	192.168.1.26	53638	24.39.217.246	54150	UDP	94			53638 → 54150 Len=52
15851	2021-04-29 20:03…	192.168.1.26	53638	24.39.217.246	54150	UDP	94			53638 → 54150 Len=52
15865	2021-04-29 20:03…	192.168.1.26	53638	24.39.217.246	54150	UDP	94			53638 → 54150 Len=52
15942	2021-04-29 20:03…	192.168.1.26	53638	24.39.217.246	54150	UDP	94			53638 → 54150 Len=52
16095	2021-04-29 20:03…	192.168.1.26	53638	24.39.217.246	54150	UDP	94			53638 → 54150 Len=52
16695	2021-04-29 20:03…	192.168.1.26	53638	24.39.217.246	54150	UDP	94			53638 → 54150 Len=52
16810	2021-04-29 20:03…	192.168.1.26	53638	24.39.217.246	54150	UDP	94			53638 → 54150 Len=52
16955	2021-04-29 20:03…	192.168.1.26	53638	24.39.217.246	54150	UDP	94			53638 → 54150 Len=52

P5: ¿Cuál es la dirección MAC del sistema bajo investigación en el archivo PCAP?

R: c8:09:a8:57:47:93

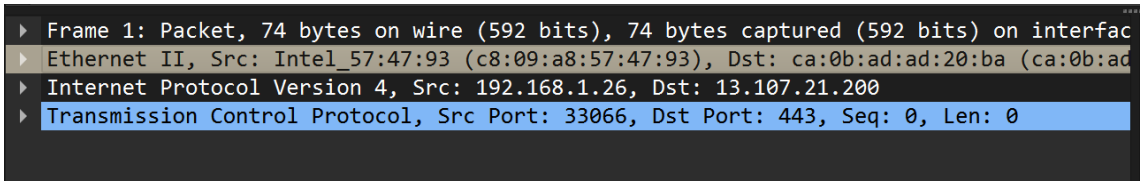
La dirección IPv4 del sistema bajo investigación es 192.168.1.26 entonces se aplicó el filtro “ip.addr == 192.168.1.26”.



ip.addr == 192.168.1.26

No.	Time	Source	Src Port	Destination	Dst. Port	Protocol
1	2021-04-29 20:00…	192.168.1.26	33066	13.107.21.200	443	TCP
2	2021-04-29 20:00…	173.223.18.66	80	192.168.1.26	51754	TCP
3	2021-04-29 20:00…	192.168.1.26	51754	173.223.18.66	80	TCP
4	2021-04-29 20:00…	192.168.1.26	33050	13.107.21.200	443	TLSv1.2
5	2021-04-29 20:00…	192.168.1.26	33050	13.107.21.200	443	TLSv1.2
6	2021-04-29 20:00…	192.168.1.26	33050	13.107.21.200	443	TLSv1.2
7	2021-04-29 20:00…	13.107.21.200	443	192.168.1.26	33066	TCP
8	2021-04-29 20:00…	192.168.1.26	33066	13.107.21.200	443	TCP
9	2021-04-29 20:00…	192.168.1.26	33066	13.107.21.200	443	TLSv1
10	2021-04-29 20:00…	173.223.18.66	80	192.168.1.26	51754	TCP
11	2021-04-29 20:00…	13.107.21.200	443	192.168.1.26	33050	TCP
12	2021-04-29 20:00…	13.107.21.200	443	192.168.1.26	33050	TCP
13	2021-04-29 20:00…	13.107.21.200	443	192.168.1.26	33050	TCP
14	2021-04-29 20:00…	13.107.21.200	443	192.168.1.26	33066	TCP
15	2021-04-29 20:00…	13.107.21.200	443	192.168.1.26	33050	TLSv1.2
16	2021-04-29 20:00…	192.168.1.26	33050	13.107.21.200	443	TCP
17	2021-04-29 20:00…	192.168.1.26	33050	13.107.21.200	443	TLSv1.2
18	2021-04-29 20:00…	13.107.21.200	443	192.168.1.26	33050	TLSv1.2
19	2021-04-29 20:00…	192.168.1.26	33050	13.107.21.200	443	TCP

Luego, en el panel de detalles se pudo visualizar la dirección MAC del sistema siendo este “c8:09:a8:57:47:93”

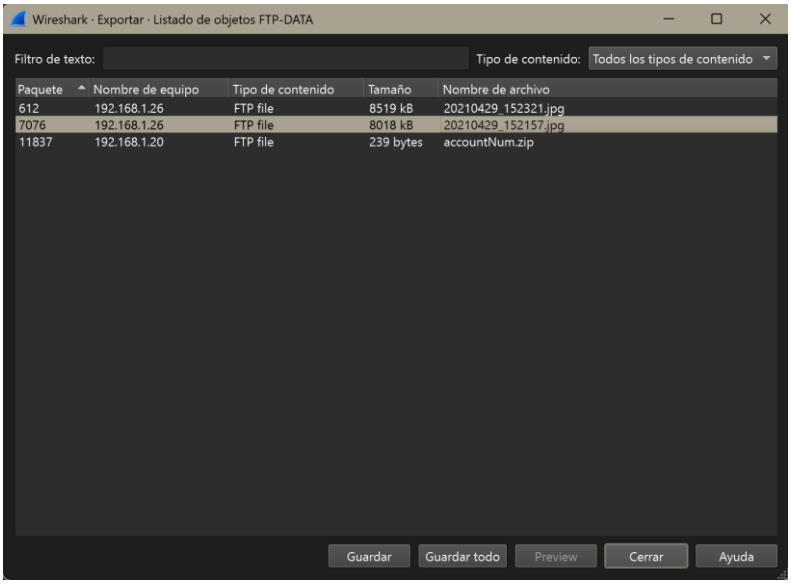


```
Frame 1: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interfac
Ethernet II, Src: Intel_57:47:93 (c8:09:a8:57:47:93), Dst: ca:0b:ad:ad:20:ba (ca:0b:ad
Internet Protocol Version 4, Src: 192.168.1.26, Dst: 13.107.21.200
Transmission Control Protocol, Src Port: 33066, Dst Port: 443, Seq: 0, Len: 0
```

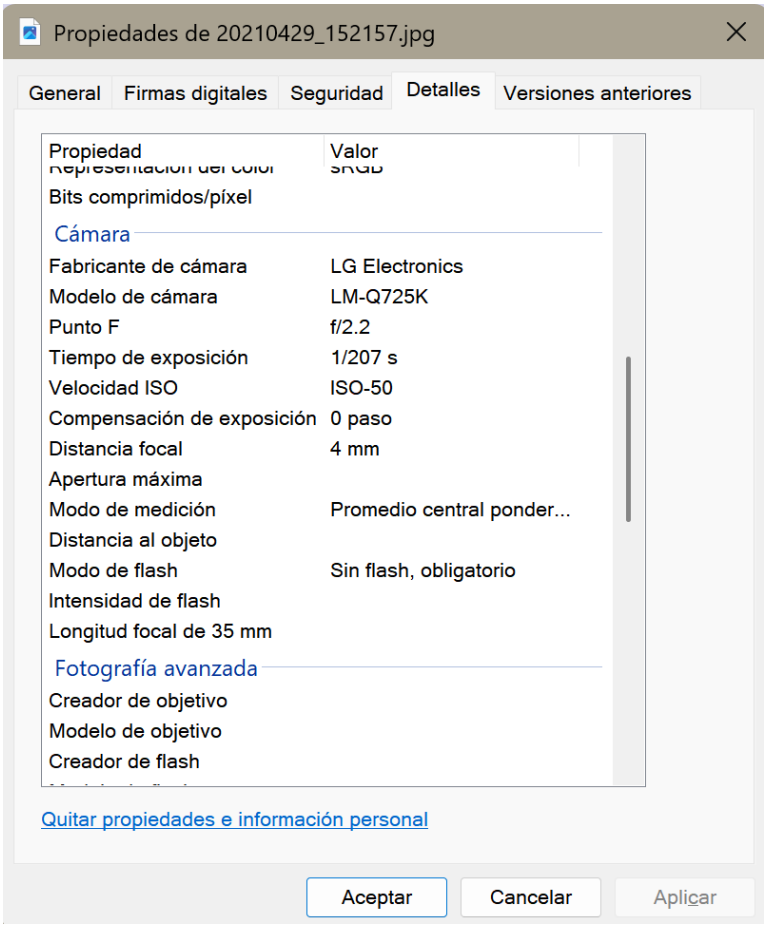
P6: ¿Cuál era el nombre del modelo de cámara utilizado para tomar la fotografía 20210429_152157.jpg?

R: LM-Q725K

Se exportó el archivo jpg para ver los detalles y saber el modelo de la cámara que se usó para tomar esta foto.



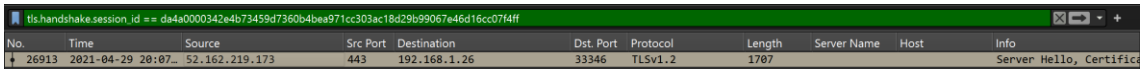
Luego en las propiedades del archivo se pudo hallar el modelo de la cámara que es LM-Q725K.



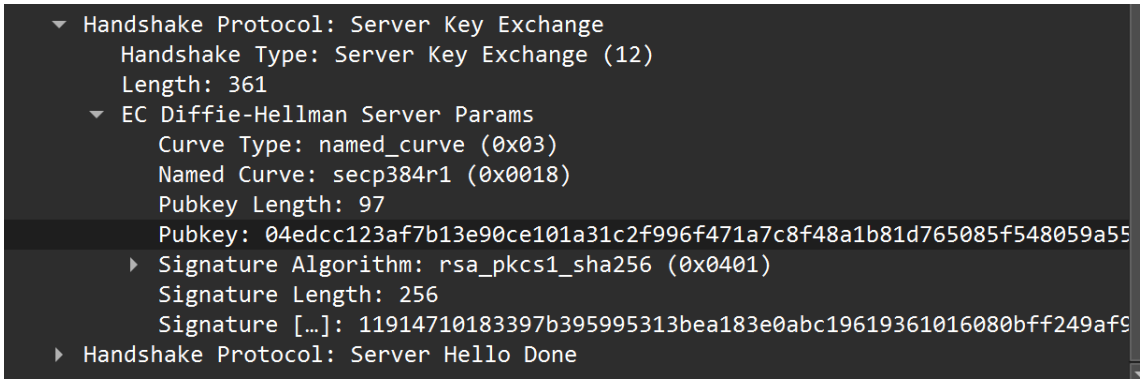
P7: ¿Cuál es la clave pública efímera proporcionada por el servidor durante el protocolo de enlace TLS en la sesión con el ID de sesión: da4a0000342e4b73459d7360b4bea971cc303ac18d29b99067e46d16cc07f4ff?

R:
04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f62ca1f0e8f74d727053074a37bceb2cbdc7ce2a8994dcd76dd6834eefc5438c3b6da929321f3a1366bd14c877cc83e5d0731b7f80a6b80916efd4a23a4d

Se aplico el filtro "tls.handshake.session_id == da4a0000342e4b73459d7360b4bea971cc303ac18d29b99067e46d16cc07f4ff" para poder visualizar solo el paquete TLS durante el handshake con el sesión ID investigado.



Luego en el panel de detalles se pudo visualizar la llave pública proporcionada por el servidor que es "04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f62ca1f0e8f74d727053074a37bceb2cbdc7ce2a8994dcd76dd6834eefc5438c3b6da929321f3a1366bd14c877cc83e5d0731b7f80a6b80916efd4a23a4d"

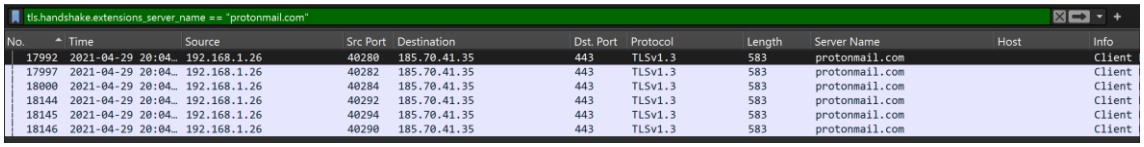


P8: ¿Cuál es el primer cliente TLS 1.3 aleatorio que se utilizó para establecer una conexión con protonmail.com?

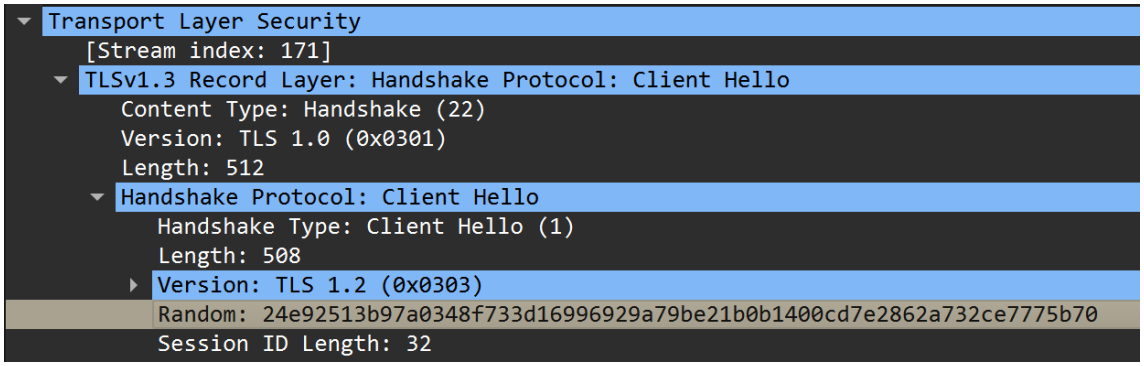
R:
24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70

Se supo que dentro del paquete TLS existe la extensión Server Name Indication (SNI), en este apartado se puede visualizar el dominio al que se quizo ingresar en texto plano antes de que se cifre la conexión. Se aplicó el filtro

‘tls.handshake.extensions_server_name == "protonmail.com”’ para especificar el paquete donde se estableció conexión con el dominio protonmail.com.



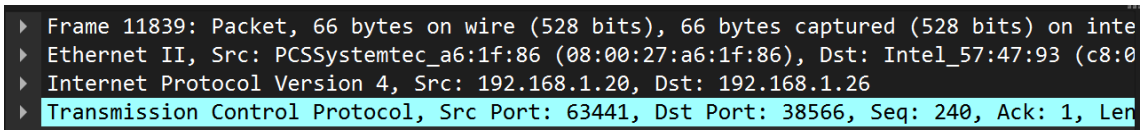
El valor random del primer cliente fue “24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70”



P9: ¿En qué país está registrado el fabricante de la dirección MAC del servidor FTP?

R: United States

La dirección IPv4 del servidor FTP es “192.168.1.20”; se seleccionó cualquier paquete donde el servidor FTP este presente y se pudo saber la dirección MAC perteneciente que es “08:00:27:a6:1f:86”



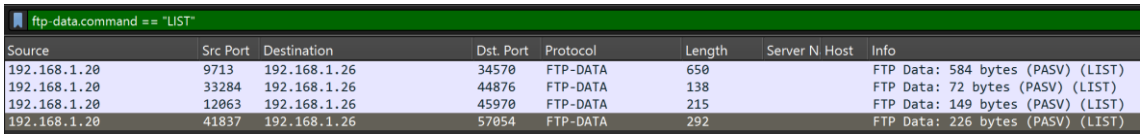
Para poder saber el país del fabricante me centré en el OUI que vendrían a ser los primeros 24 bits de la dirección MAC, es decir, “08:00:27”. Luego con la ayuda de una página externa se encontró el país del fabricante que es United States.

MAC Address	08:00:27
Vendor	PCS Systemtechnik GmbH
Address	600 Suffold St Lowell MA 01854 US
Block Size	MA-L
Block Range	08:00:27:00:00:00 - 08:00:27:FF:FF:FF
Virtual Machine	Oracle VirtualBox

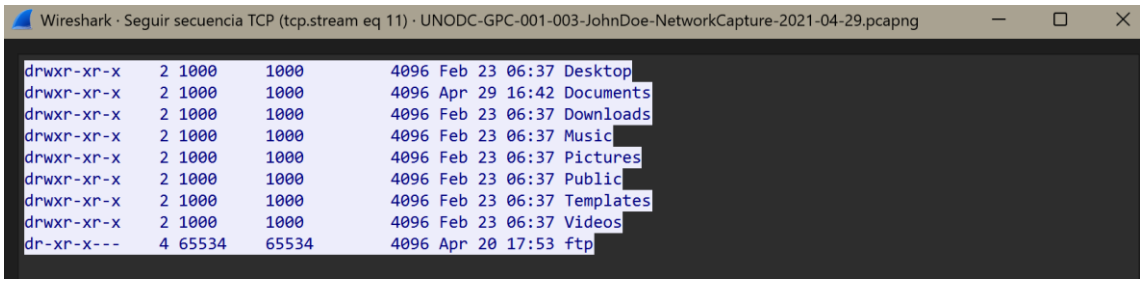
P10: ¿A qué hora se creó una carpeta no estándar en el servidor FTP el 20 de abril?

R: 17:53

Para enfocarme en la transferencia real de los archivos en el servidor FTP se aplicó el filtro “ftp-data” y me centré en los paquetes donde se ejecutaron comandos LIST, para un mejor análisis también se pudo aplicar el filtro ‘ftp-data.command == "LIST"’.



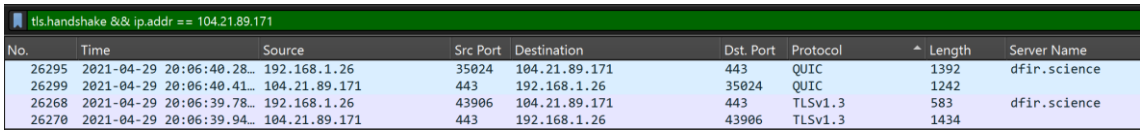
Se realizó un seguimiento TCP del paquete 530 y se pudo hallar la hora de creación del folder no estándar el día 20 de Abril, siendo este a las 17:53 horas.



P11: ¿Qué URL fue visitada por el usuario y se conectó a la dirección IP 104.21.89.171?

R: http://dfir.science/

Para poder centrarnos en el dominio al que el usuario ingresó se filtró los paquetes TLS en el proceso del handshake y se fijó en la extensión SNI. Luego, para tener una mejor visualización se añadió esta extensión como columna. También se necesitó filtrar los paquetes donde el usuario se conectó a la dirección IP 104.21.89.17, con esto dicho, se aplicó el filtro “tls.handshake && ip.addr == 104.21.89.171” donde finalmente se dedujo la URL visitada siendo este “http://dfir.science/”.


tls.handshake && ip.addr == 104.21.89.171

No.	Time	Source	Src Port	Destination	Dst. Port	Protocol	Length	Server Name
26295	2021-04-29 20:06:40.28…	192.168.1.26	35024	104.21.89.171	443	QUIC	1392	dfir.science
26299	2021-04-29 20:06:40.41…	104.21.89.171	443	192.168.1.26	35024	QUIC	1242	
26268	2021-04-29 20:06:39.78…	192.168.1.26	43906	104.21.89.171	443	TLSv1.3	583	dfir.science
26270	2021-04-29 20:06:39.94…	104.21.89.171	443	192.168.1.26	43906	TLSv1.3	1434	