

Réseau - InterceptingImages - 50 points

Kévin DUVERGER

Table des matières

1 Résolution InterceptingImages :	2
--	----------

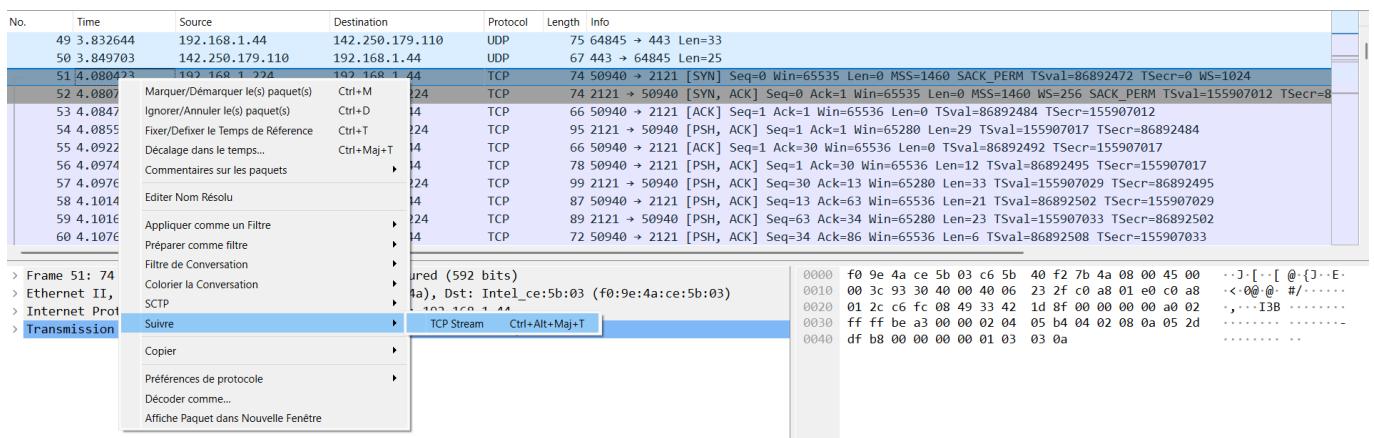
1 Résolution InterceptingImages :

Pour ce nouveau challenge, on nous donne un échange de données FTP et le but est de trouver l'image qui a été échangée entre un client et un serveur. La première chose que l'on peut faire est ouvrir la capture pour comprendre comment cela fonctionne :

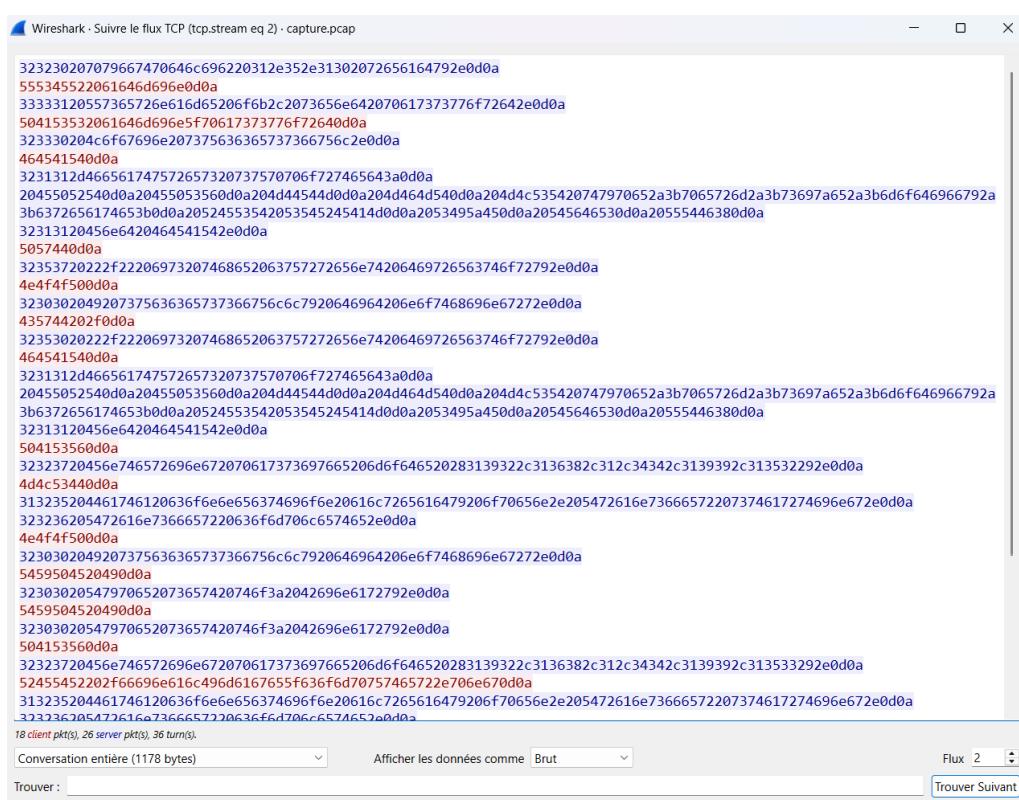
118 9.251268	192.168.1.44	142.250.178.138	UDP	71 53235 → 443 Len=29
119 9.276965	142.250.178.138	192.168.1.44	UDP	67 443 → 53235 Len=25
120 10.657564	146.59.227.136	192.168.1.44	TCP	82 9876 → 28097 [PSH, ACK] Seq=57 Ack=1 Win=491 Len=28
121 10.702205	192.168.1.44	146.59.227.136	TCP	54 28097 → 9876 [ACK] Seq=1 Ack=85 Win=253 Len=0
122 11.147686	146.59.227.136	192.168.1.44	TCP	82 9876 → 17648 [PSH, ACK] Seq=57 Ack=1 Win=501 Len=28
123 11.200097	192.168.1.44	146.59.227.136	TCP	54 17648 → 9876 [ACK] Seq=1 Ack=85 Win=251 Len=0
124 11.805842	192.168.1.224	192.168.1.44	TCP	72 50940 → 2121 [PSH, ACK] Seq=76 Ack=607 Win=65536 Len=6 TSval=86900192 TSecr=155907344
125 11.860659	192.168.1.44	192.168.1.224	TCP	100 2121 → 50940 [PSH, ACK] Seq=607 Ack=82 Win=65280 Len=34 TSval=155914738 TSecr=86900192
126 11.810400	192.168.1.224	192.168.1.44	TCP	74 50940 → 2121 [PSH, ACK] Seq=82 Ack=641 Win=65536 Len=8 TSval=86900211 TSecr=155914738
127 11.810559	192.168.1.44	192.168.1.224	TCP	92 2121 → 50940 [PSH, ACK] Seq=641 Ack=90 Win=65280 Len=26 TSval=155914742 TSecr=86900211
128 11.822578	192.168.1.224	192.168.1.44	TCP	74 50940 → 2121 [PSH, ACK] Seq=90 Ack=667 Win=65536 Len=8 TSval=86900223 TSecr=155914742
129 11.822744	192.168.1.44	192.168.1.224	TCP	92 2121 → 50940 [PSH, ACK] Seq=667 Ack=98 Win=65280 Len=26 TSval=155914755 TSecr=86900223

Comme vous pouvez le voir on ne voit jamais de FTP dans ce fichier et c'est probablement car Wireshark s'est arrêté à TCP. De plus, à part quelques échanges parasites, vous pouvez voir que la majorité des communications a lieu entre les IP 192.168.1.44 et 192.168.1.224, et ces sur ces dernières que nous allons nous concentrer.

On peut donc aller sur la première trame échangée entre ces 2 machines, la 51, faire un clic droit et aller vers "suivre" :



En faisant cela, nous obtenons la capture suivante :



Et comme vous pouvez le voir il n'y a qu'environ 1200 octets qui semble plus être un échange de commandes entre le client et le serveur qu'une image (d'ailleurs les données échangées ici ne commencent même pas par la signature d'une image PNG / JPG).

Pour comprendre pourquoi, il faut se souvenir du fonctionnement du protocole FTP : la connexion principale est utilisée pour l'échange de commandes entre le client et le serveur, et une autre connexion est créée pour échanger les données. La solution est donc de trouver l'autre stream TCP entre les 2 machines qui se produira probablement avec des ports différents de la première. En allant épucher la capture réseau, vous devriez remarquer que le paquet 82 a bien de nouveaux ports :

80 4.399140	192.168.1.44	192.168.1.224	TCP	117 2121 → 50940 [PSH, ACK] Seq=478 Ack=70 Win=65280 Len=51 TSval=155907331 TSecr=86892798
81 4.403469	142.250.178.138	192.168.1.44	UDP	67 443 → 53235 Len=25
82 4.407037	192.168.1.224	192.168.1.44	TCP	74 43754 → 51096 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=86892807 TSecr=0 WS=1024
83 4.407152	192.168.1.44	192.168.1.224	TCP	74 51096 → 43754 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM TSval=155907339 TSecr=
84 4.410308	192.168.1.224	192.168.1.44	TCP	66 43754 → 51096 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=86892811 TSecr=155907339
85 4.411690	192.168.1.224	192.168.1.44	TCP	72 50940 → 2121 [PSH, ACK] Seq=70 Ack=529 Win=65536 Len=6 TSval=86892812 TSecr=155907331
86 4.412342	192.168.1.44	192.168.1.224	TCP	120 2121 → 50940 [PSH, ACK] Seq=529 Ack=76 Win=65280 Len=54 TSval=155907344 TSecr=86892812
87 4.412725	192.168.1.44	192.168.1.224	TCP	209 51096 → 43754 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=143 TSval=155907344 TSecr=86892811
88 4.412823	192.168.1.44	192.168.1.224	TCP	66 51096 → 43754 [FIN, ACK] Seq=144 Ack=1 Win=65280 Len=0 TSval=155907344 TSecr=86892811
89 4.412851	192.168.1.44	192.168.1.224	TCP	90 2121 → 50940 [PSH, ACK] Seq=583 Ack=76 Win=65280 Len=24 TSval=155907345 TSecr=86892812
90 4.416071	192.168.1.224	192.168.1.44	TCP	66 43754 → 51096 [ACK] Seq=1 Ack=144 Win=67584 Len=0 TSval=86892816 TSecr=155907344
91 4.417852	192.168.1.224	192.168.1.44	TCP	66 43754 → 51096 [FIN, ACK] Seq=1 Ack=145 Win=67584 Len=0 TSval=86892816 TSecr=155907344

```
> Frame 82: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: c6:5b:40:f2:7b:4a (c6:5b:40:f2:7b:4a), Dst: Intel_ce:5b:03 (f0:9e:4a:ce:5b:03)
> Internet Protocol Version 4, Src: 192.168.1.224, Dst: 192.168.1.44
> Transmission Control Protocol, Src Port: 43754, Dst Port: 51096, Seq: 0, Len: 0
```

0000 f0 9e 4a ce 5b 03 c6 5b 40 f2 7b 4a 08 00 45 00	..J.[..[@ {]..E.
0010 00 3c 3f 43 40 00 40 06	..<?C@..w.....
0020 01 2c aa ea c7 98 30 30	,...00 cE.....
0030 ff ff d7 72 00 00 02 04	,...00 00 a0 02
0040 e1 07 00 00 00 00 01 03

Nous pouvons une nouvelle fois suivre cette communication et voici ce que l'on obtient :

Wireshark · Suivre le flux TCP (tcp.stream eq 3) · capture.pcap

6d6f646966793d32303235303931313232323332343b7065726d3d723b73697a653d31343934313b747970653d66696c653b2062617365496d1617
652e6a70670d0a6d6f646966793d32303235303931313232323532313b7065726d3d723b73697a653d323837373b747970653d66696c653b20
66696e616c496d6167655f636f6d70757465722e706e670d0a

0 client pkt(s), 1 server pkt(s), 0 turn(s).

Conversation entière (143 bytes)

Afficher les données comme Brut

Trouver :

Filtrer ce flux Imprimer Enregistrer sous... Retour Fermer Aide Trouver Suivant

Malheureusement, cela ressemble très peu à une image, il faut continuer à chercher.

Une autre connexion qui est différente des 2 autres commence au paquet 134 :

No.	Time	Source	Destination	Protocol	Length	Info
132 11.882081	192.168.1.44	192.168.1.224	TCP	117 2121 → 50940 [PSH, ACK] Seq=693 Ack=104 Win=65280 Len=51 TSval=155914814 TSecr=86900281		
133 11.885688	192.168.1.224	192.168.1.44	TCP	66 50940 → 2121 [ACK] Seq=104 Ack=744 Win=65536 Len=0 TSval=86900286 TSecr=155914814		
134 11.889819	192.168.1.224	192.168.1.44	TCP	74 55102 → 51097 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=86900290 TSecr=0 WS=1024		
135 11.889931	192.168.1.44	192.168.1.224	TCP	74 51097 → 55102 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM TSval=155914822 TSecr=		
136 11.893429	192.168.1.224	192.168.1.44	TCP	66 55102 → 51097 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=86900294 TSecr=155914822		
137 11.897968	192.168.1.224	192.168.1.44	TCP	97 50940 → 2121 [PSH, ACK] Seq=104 Ack=744 Win=65536 Len=31 TSval=86900298 TSecr=155914814		
138 11.898805	192.168.1.44	192.168.1.224	TCP	120 2121 → 50940 [PSH, ACK] Seq=744 Ack=135 Win=65280 Len=54 TSval=155914831 TSecr=86900298		
139 11.899073	192.168.1.44	192.168.1.224	TCP	1514 51097 → 55102 [ACK] Seq=1 Ack=1 Win=65280 Len=1448 TSval=155914831 TSecr=86900294		
140 11.899073	192.168.1.44	192.168.1.224	TCP	1514 51097 → 55102 [ACK] Seq=1449 Ack=1 Win=65280 Len=1448 TSval=155914831 TSecr=86900294		
141 11.899073	192.168.1.44	192.168.1.224	TCP	1514 51097 → 55102 [ACK] Seq=2897 Ack=1 Win=65280 Len=1448 TSval=155914831 TSecr=86900294		
142 11.899073	192.168.1.44	192.168.1.224	TCP	1514 51097 → 55102 [ACK] Seq=4345 Ack=1 Win=65280 Len=1448 TSval=155914831 TSecr=86900294		
143 11.899073	192.168.1.44	192.168.1.224	TCP	1514 51097 → 55102 [ACK] Seq=5793 Ack=1 Win=65280 Len=1448 TSval=155914831 TSecr=86900294		

```
> Frame 134: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: c6:5b:40:f2:7b:4a (c6:5b:40:f2:7b:4a), Dst: Intel_ce:5b:03 (f0:9e:4a:ce:5b:03)
> Internet Protocol Version 4, Src: 192.168.1.224, Dst: 192.168.1.44
> Transmission Control Protocol, Src Port: 55102, Dst Port: 51097, Seq: 0, Len: 0
```

0000 f0 9e 4a ce 5b 03 c6 5b 40 f2 7b 4a 08 00 45 00	..J.[..[@ {]..E.
0010 00 3c 3f 43 40 00 40 06	..<?C@..w.....
0020 01 2c aa ea c7 98 30 30	,...00 cE.....
0030 ff ff d7 72 00 00 02 04	,...00 00 a0 02
0040 e1 07 00 00 00 00 01 03

Nous pouvons encore suivre cette communication, ce qui nous donne :

Wireshark · Suivre le flux TCP (tcp.stream eq 8) · capture.pcap

89504e470d0a1a0a000000d49484452000002e4000001ec080200000157d2fc200000017352474200aece1ce9000000467414d410000b18f0b
fc610500000009704859730000b120000b1201d2dd7efc000fffa54944154785eeccfde9b365c9712788b97bc4b9ef65561536126c8058898d00
4870114da39ed148d662c2ed05d336632d37c2541109c31fd33fa20b3f943e68bcc6426d9d86864dde490204190e0da008895580ab567be7b22dc
f5e1e7ee27eb9cbbefbdccac2c30bd6ebdbc374eac1e71223c7ee1ecf9eff17f2532ed9db4699b5377cc8d44c998ca5925429b5d4a9d42a
a50a1399999aa9a19113133349bd482abe131111319130238e4586a6e69b5993652253121611169152b8088b3033310b1391929999aa9a19
a33c611696c2525022b3104b166d664c46645e136623c23373527f2acc222c2524a8902f8f575f1bf3f19a10b17156406a455ad4c34c
4dbbc577d7ed8aeaee6edc3e5ff5b6755e21266a5e8ad449cad20aaf9a5597b2753afbf1416e1329114a9139789bd9ec22c60916937edd6bb
6a27533223262e2c22e09848616112722ea99a76ed5d35786b6826338b119139364f78a08090b01522125d566d6d667092b5042e93d42a7523
65421ba3459dac8bb67afbfcc7db6bebde6a44d8b8c98a5729dbc052590a0978ebcd3afbe037ed464c2cc941fb4d18c98c55b2a134b65a9cc85c8988948999
9944b8081531b3663a9b1a19919219111532f45a89118bc6323113191b19162b4f7de9b6933ed4466a6181dc42c468113a8b88554d98c88d88a2
07c9d88cccd4481fd83b5e7c78b1edf460aba3de8af3dd4371eb6075b9b7afffbdb43348ef99def84f171e2e7418aa1b5228e97f2193d1574a4
9b9c4e3f3d18613f6445abc1732cfe4dc341fb4ff7438e05828e8ed1349f2d1b1b44946a4c7f33987e45403746d84bb91bfbbffba564c88dbe1fcf

0 client pkt(s), 201 server pkt(s), 0 turn(s).

Conversation entière (287 kB)

Afficher les données comme Brut

Trouver :

Filtrer ce flux Imprimer Enregistrer sous... Retour Fermer Aide Trouver Suivant

Et en cliquant sur "enregistrer" vers une image png, vous devriez obtenir ce que vous attendez :

