Réseau - InterceptingImages - 50 points

Kévin DUVERGER

Table des matières

1 Résolution InterceptingImages : 2

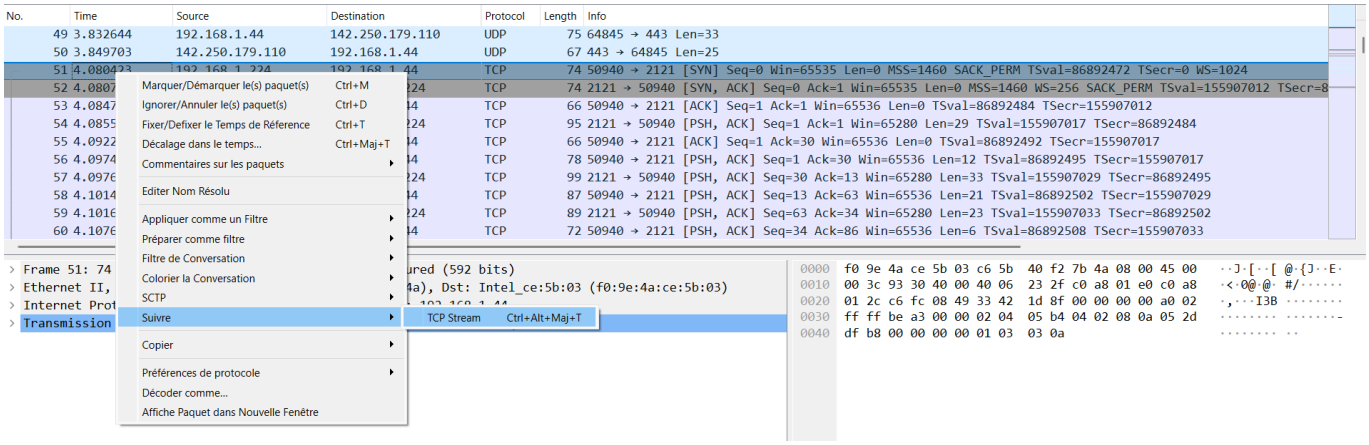
1 Résolution InterceptingImages :

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 :

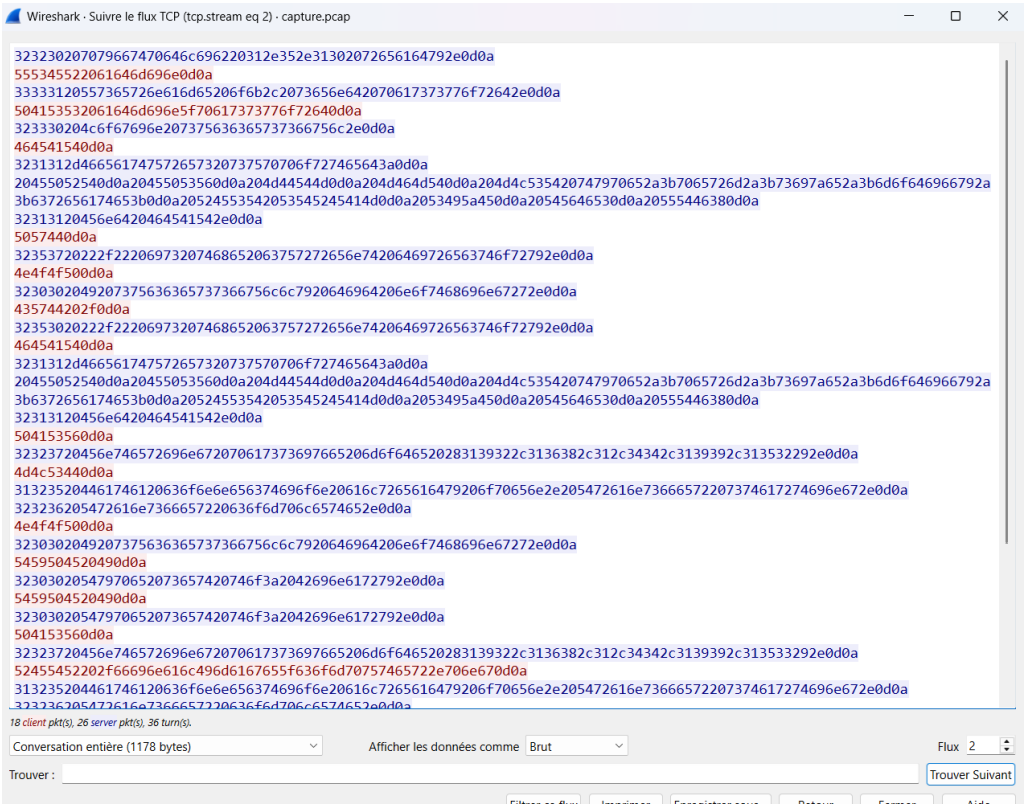
118	9.251268	192.168.1.44	142.250.178.138	UDP	71 53235 → 443 Len=29
119	9.276965	142.250.178.138	192.168.1.44	UDP	67 443 → 53235 Len=25
120	10.657564	146.59.227.136	192.168.1.44	TCP	82 9876 → 28097 [PSH, ACK] Seq=57 Ack=1 Win=491 Len=28
121	10.702205	192.168.1.44	146.59.227.136	TCP	54 28097 → 9876 [ACK] 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	11.806059	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 parasitaires, 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" :

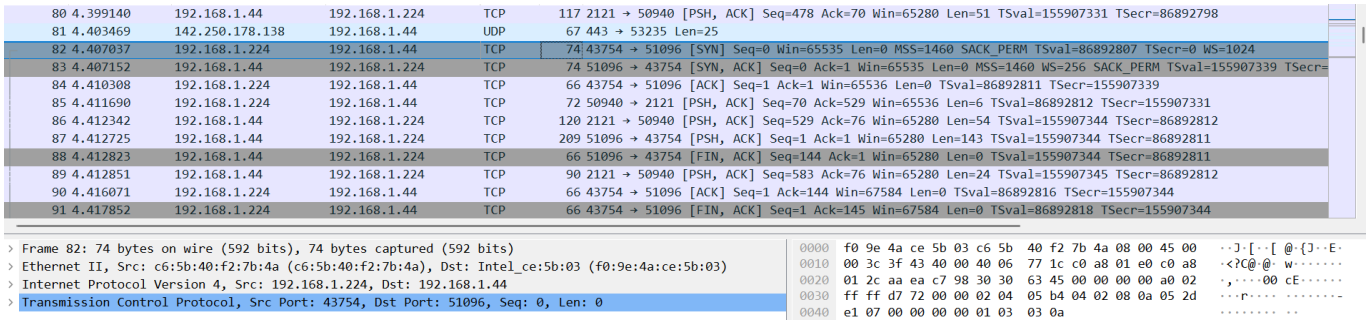


En faisant cela, nous obtenons la capture suivante :

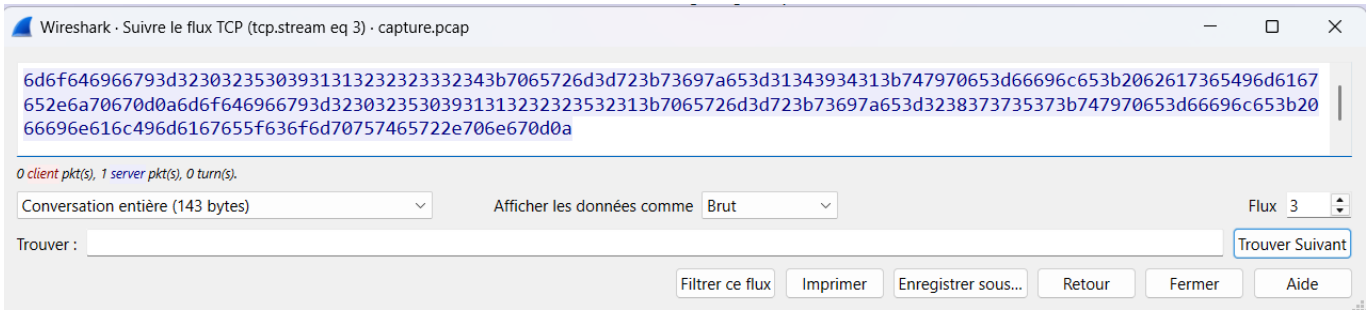


Et comme vous pouvez le voir il n'y a qu'environ 1200 octets qui semble plus être un échange de commandes entre le client et le serveur qu'une image (d'ailleurs les données échangées ici ne commencent même pas par la signature d'une image PNG / JPG).

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 éplucher la capture réseau, vous devriez remarquer que le paquet 82 a bien de nouveaux ports :

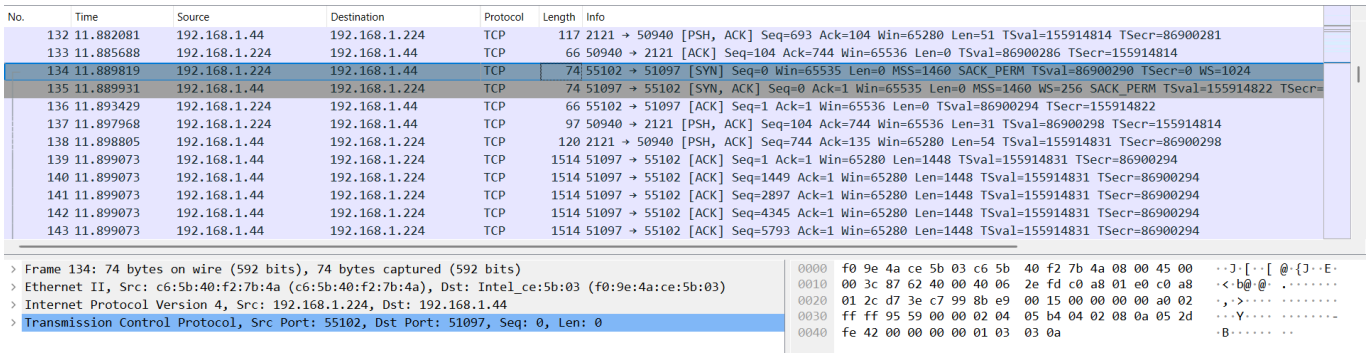


Nous pouvons une nouvelle fois suivre cette communication et voici ce que l'on obtient :

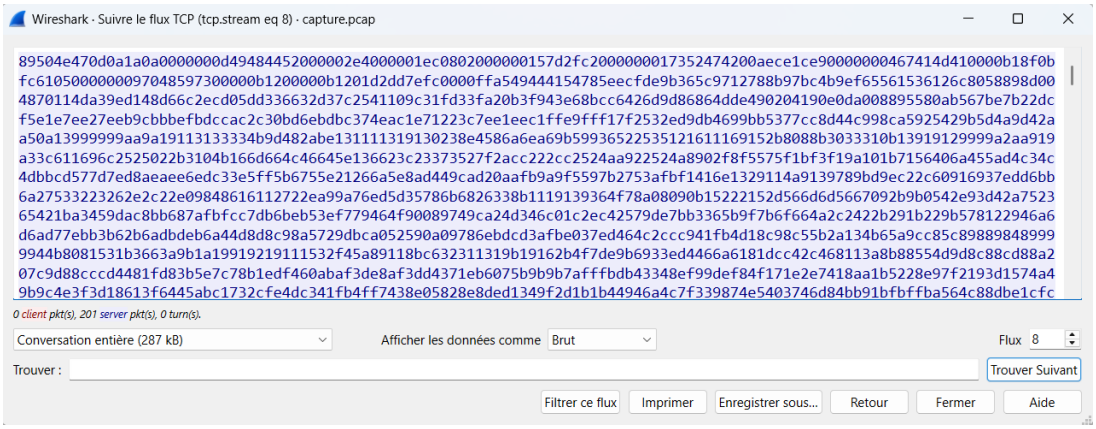


Malheureusement, cela ressemble très peu à une image, il faut continuer à chercher.

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



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



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