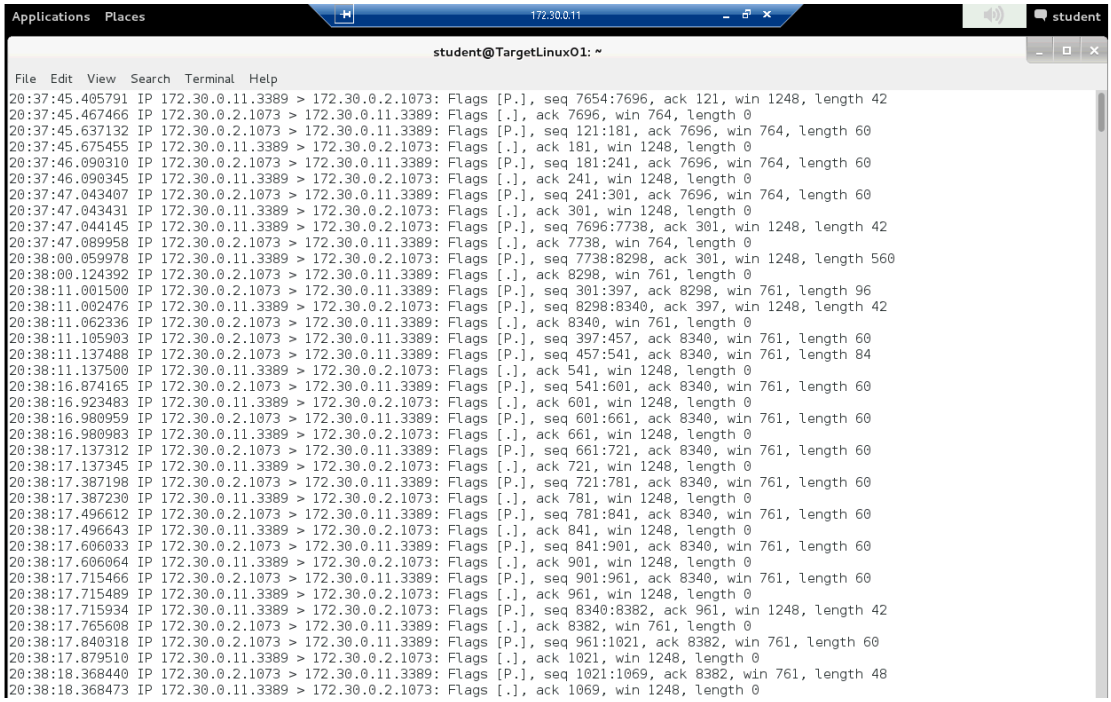
Lab Report

1. Result of tcpdump in Linux (Kali)

Figure 1. tcpdump results



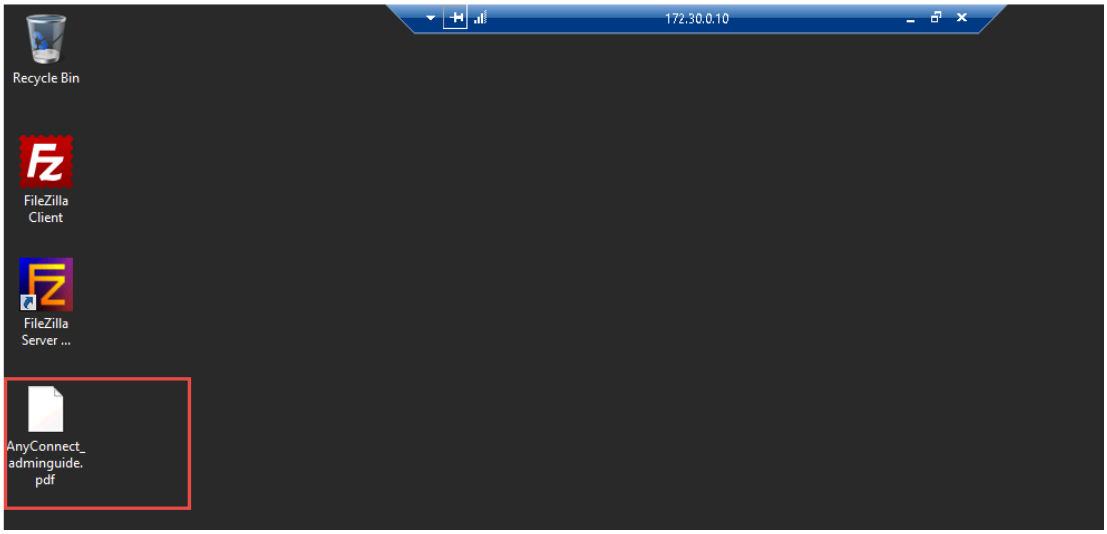
```
Applications  Places                                172.30.0.11                                  student
student@TargetLinuxO1: ~
File  Edit  View  Search  Terminal  Help
20:37:45.405791 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [P.], seq 7654:7696, ack 121, win 1248, length 42
20:37:45.467466 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [.], ack 7696, win 764, length 0
20:37:45.637132 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 121:181, ack 7696, win 764, length 60
20:37:45.675455 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 181, win 1248, length 0
20:37:46.090310 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 181:241, ack 7696, win 764, length 60
20:37:46.090345 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 241, win 1248, length 0
20:37:47.043407 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 241:301, ack 7696, win 764, length 60
20:37:47.043431 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 301, win 1248, length 0
20:37:47.044145 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [P.], seq 7696:7738, ack 301, win 1248, length 42
20:37:47.089958 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [.], ack 7738, win 764, length 0
20:38:00.059978 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [P.], seq 7738:8298, ack 301, win 1248, length 560
20:38:00.124392 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [.], ack 8298, win 761, length 0
20:38:11.001500 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 301:397, ack 8298, win 761, length 96
20:38:11.002476 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [P.], seq 8298:8340, ack 397, win 1248, length 42
20:38:11.062336 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [.], ack 8340, win 761, length 0
20:38:11.105903 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 397:457, ack 8340, win 761, length 60
20:38:11.137488 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 457:541, ack 8340, win 761, length 84
20:38:11.137500 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 541, win 1248, length 0
20:38:16.874165 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 541:601, ack 8340, win 761, length 60
20:38:16.923483 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 601, win 1248, length 0
20:38:16.980959 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 601:661, ack 8340, win 761, length 60
20:38:16.980983 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 661, win 1248, length 0
20:38:17.137312 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 661:721, ack 8340, win 761, length 60
20:38:17.137345 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 721, win 1248, length 0
20:38:17.387198 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 721:781, ack 8340, win 761, length 60
20:38:17.387230 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 781, win 1248, length 0
20:38:17.496612 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 781:841, ack 8340, win 761, length 60
20:38:17.496643 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 841, win 1248, length 0
20:38:17.606033 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 841:901, ack 8340, win 761, length 60
20:38:17.606064 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 901, win 1248, length 0
20:38:17.715466 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 901:961, ack 8340, win 761, length 60
20:38:17.715489 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 961, win 1248, length 0
20:38:17.715934 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [P.], seq 8340:8382, ack 961, win 1248, length 42
20:38:17.765608 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [.], ack 8382, win 761, length 0
20:38:17.840318 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 961:1021, ack 8382, win 761, length 60
20:38:17.879510 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 1021, win 1248, length 0
20:38:18.368440 IP 172.30.0.2.1073 > 172.30.0.11.3389: Flags [P.], seq 1021:1069, ack 8382, win 761, length 48
20:38:18.368473 IP 172.30.0.11.3389 > 172.30.0.2.1073: Flags [.], ack 1069, win 1248, length 0
```

Note: because the tcpdump scan result is too long, so here we just show the first part of the result.

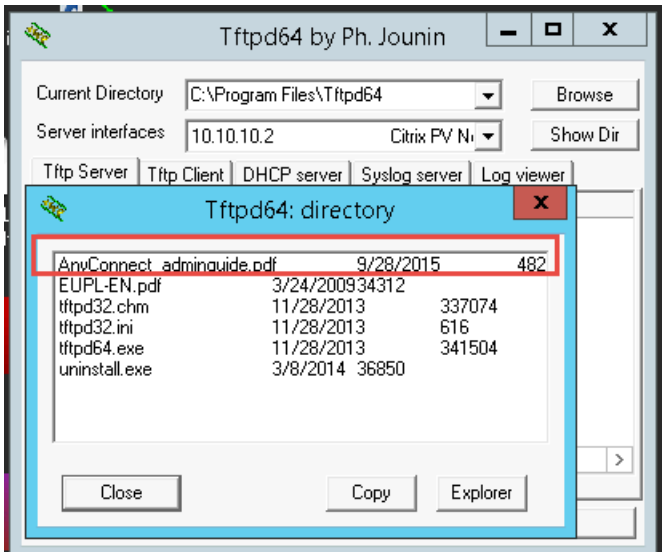
Explanation:

Tcpdump is a powerful tool provided by most of operating systems and it is used to capture packets over the network. We can use this tool to analyze potential threats and make information security baselines.

2. AnyConnect_adminguide.pdf on the targetWindows01 desktop



3. Transferred file in the Tftp64 directory



4. Protocol Hierarchy Statistics

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	26968	100.00 %	11869600	0.063	0	0	0.000
Ethernet	100.00 %	26968	100.00 %	11869600	0.063	0	0	0.000
Address Resolution Protocol	0.13 %	34	0.01 %	1464	0.000	34	1464	0.000
Internet Protocol Version 4	99.84 %	26926	99.98 %	11867316	0.063	0	0	0.000
Transmission Control Protocol	25.19 %	6793	47.20 %	5602831	0.030	3455	209294	0.001
Telnet	1.53 %	413	0.51 %	60090	0.000	413	60090	0.000
SSH Protocol	0.52 %	141	0.28 %	33686	0.000	38	21324	0.000
Malformed Packet	0.38 %	103	0.10 %	12362	0.000	103	12362	0.000
TPKT - ISO on TCP - RFC1006	4.36 %	1175	1.40 %	166658	0.001	1173	166484	0.001
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol	0.01 %	2	0.00 %	174	0.000	0	0	0.000
Malformed Packet	0.01 %	2	0.00 %	174	0.000	2	174	0.000
File Transfer Protocol (FTP)	0.30 %	80	0.06 %	6910	0.000	80	6910	0.000
FTP Data	5.67 %	1529	43.19 %	5126193	0.027	1529	5126193	0.027
User Datagram Protocol	74.64 %	20129	52.73 %	6264269	0.033	0	0	0.000
Domain Name Service	0.03 %	8	0.01 %	660	0.000	8	660	0.000
NetBIOS Name Service	0.08 %	21	0.02 %	1932	0.000	21	1932	0.000
NetBIOS Datagram Service	0.02 %	5	0.01 %	1134	0.000	0	0	0.000
SMB (Server Message Block Protocol)	0.02 %	5	0.01 %	1134	0.000	0	0	0.000
SMB MailSlot Protocol	0.02 %	5	0.01 %	1134	0.000	0	0	0.000
Microsoft Windows Browser Protocol	0.02 %	5	0.01 %	1134	0.000	5	1134	0.000
Data	4.59 %	1237	4.77 %	566153	0.003	1237	566153	0.003
Trivial File Transfer Protocol	69.93 %	18858	47.97 %	5694390	0.030	9430	433836	0.002
Data	34.96 %	9428	44.32 %	5260554	0.028	9428	5260554	0.028
Internet Group Management Protocol	0.01 %	4	0.00 %	216	0.000	4	216	0.000
Internet Protocol Version 6	0.03 %	8	0.01 %	820	0.000	0	0	0.000
User Datagram Protocol	0.03 %	8	0.01 %	820	0.000	0	0	0.000
Domain Name Service	0.03 %	8	0.01 %	820	0.000	8	820	0.000

Explanation:

This picture shows the overall protocol hierarchy and from it we can see that there are 11 protocols are used in all captured packets.

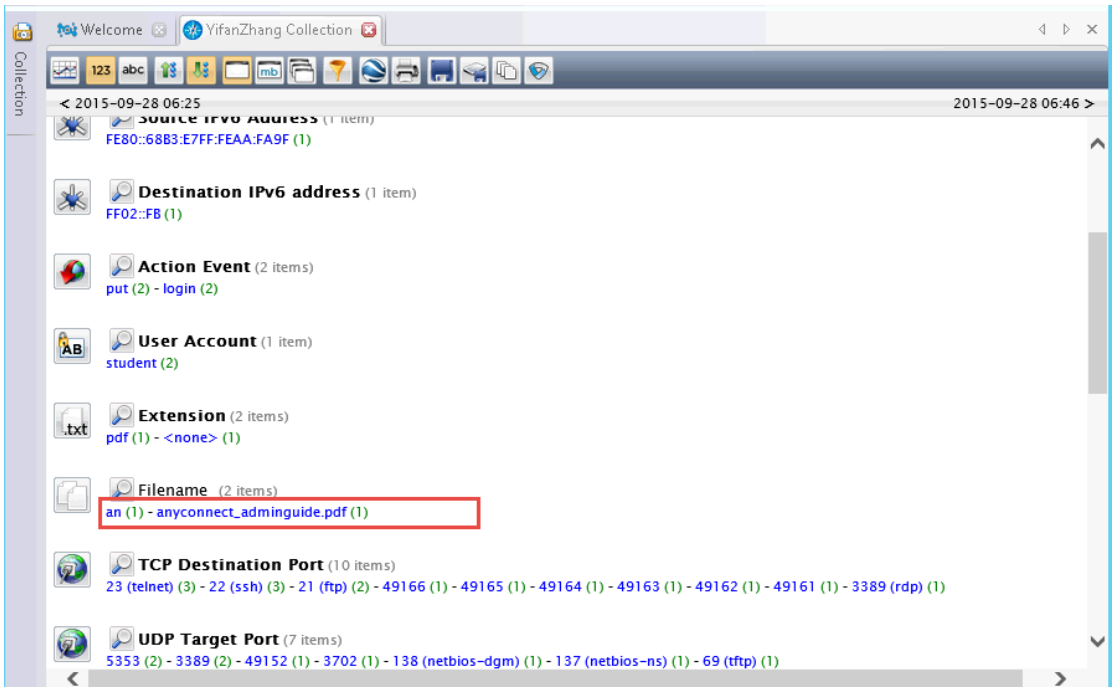
5. Packet Lengths distribution

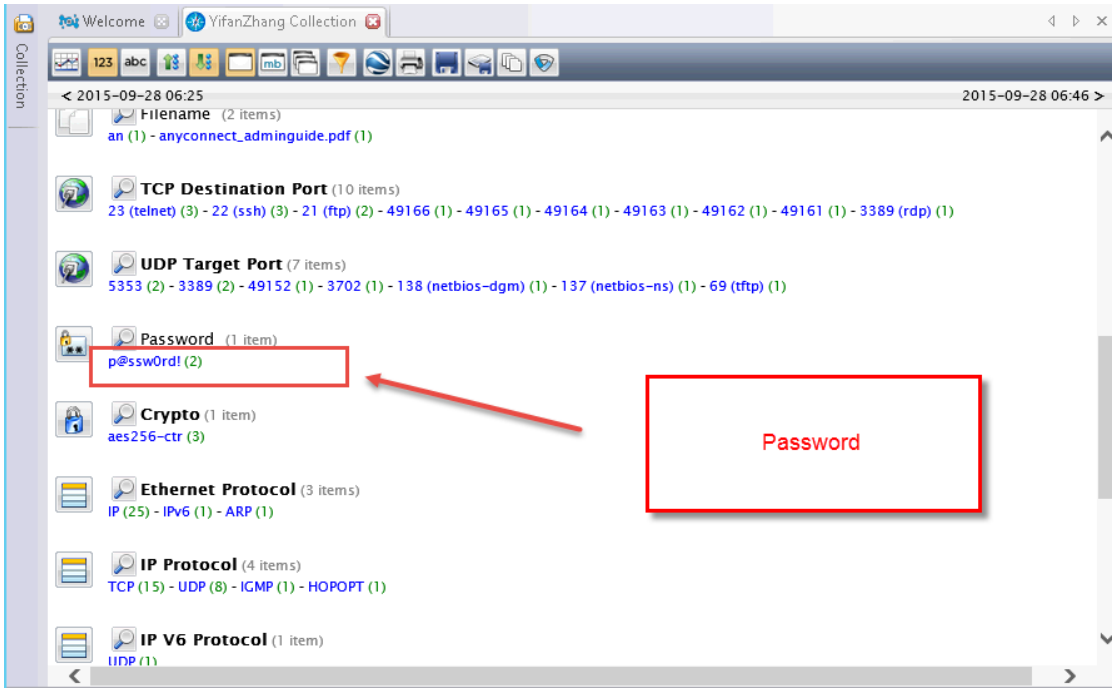
Packet Lengths with filter:

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	26968	0.017985	
0-19	0	0.000000	0.00%
20-39	0	0.000000	0.00%
40-79	13675	0.009120	50.71%
80-159	1651	0.001101	6.12%
160-319	149	0.000099	0.55%
320-639	9567	0.006380	35.48%
640-1279	400	0.000267	1.48%
1280-2559	306	0.000204	1.13%
2560-5119	1086	0.000724	4.03%
5120-4294967295	134	0.000089	0.50%

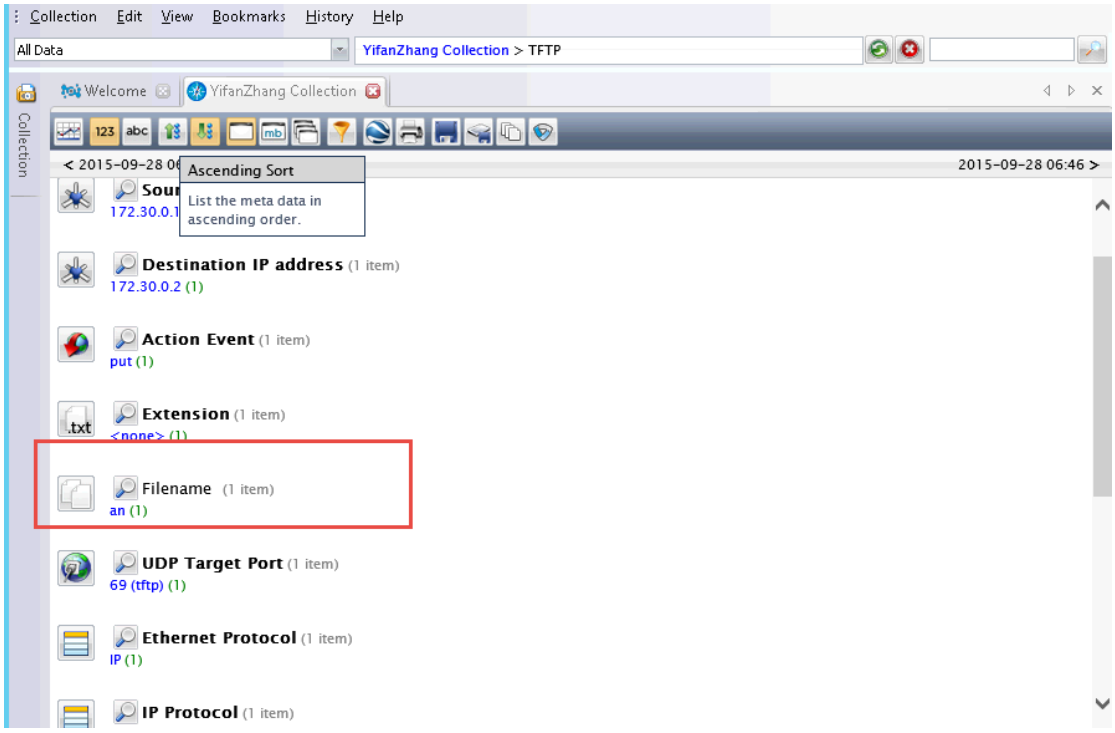
Close

6. Password and filename used in the FTP transfer

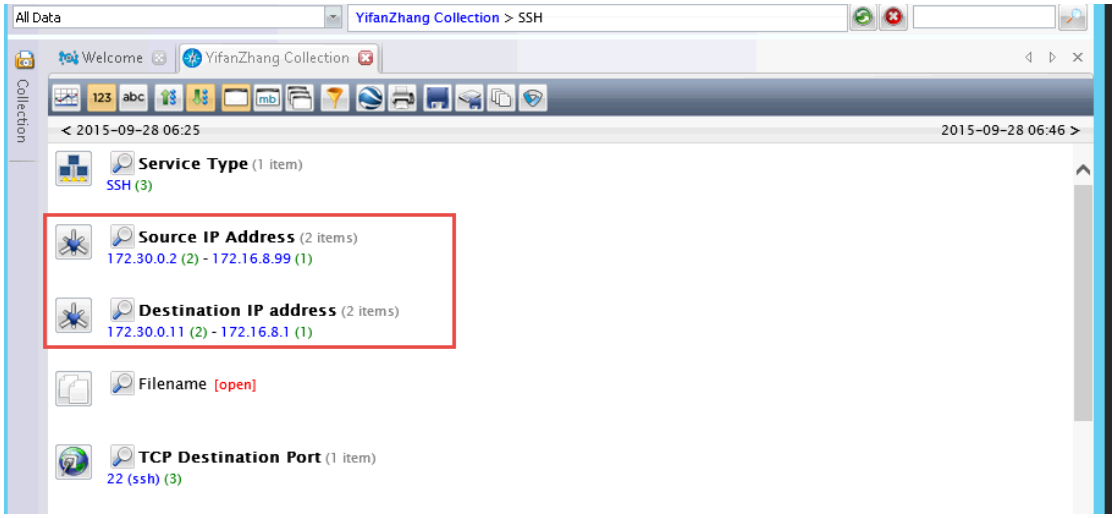


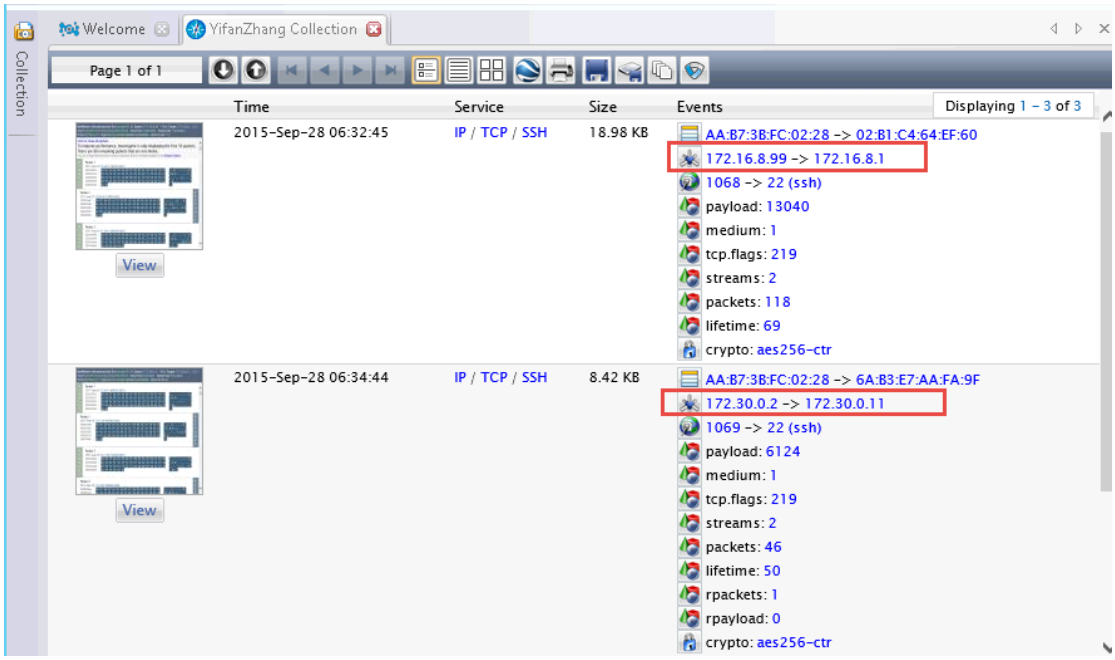


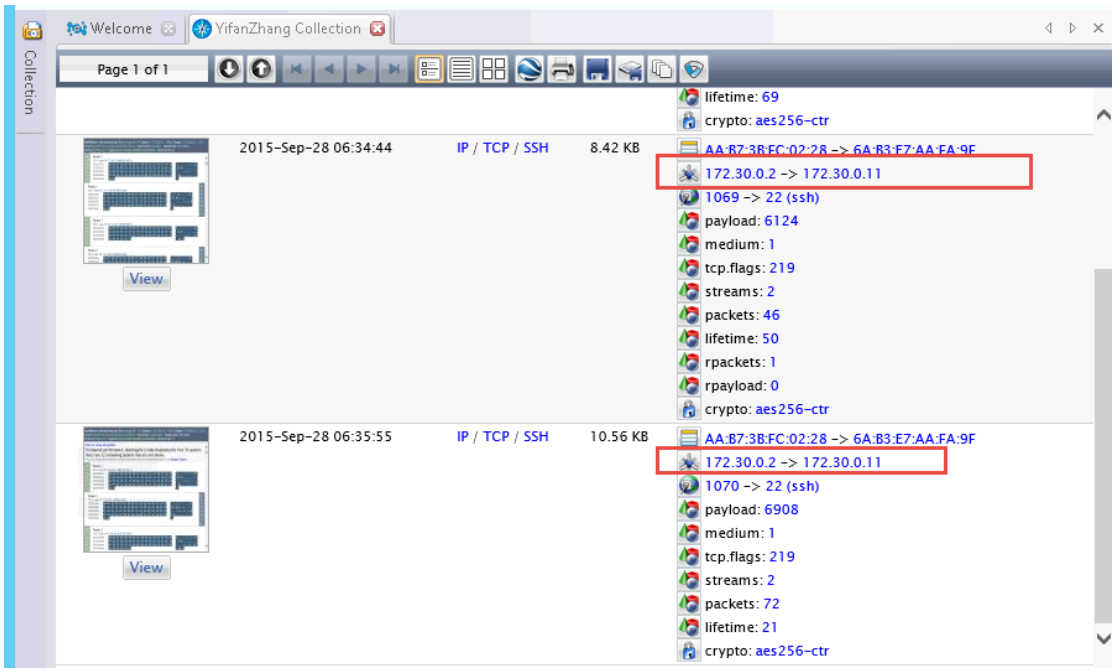
7. Filename used in the TFTP file transfer



8. IP addresses for the SSH sessions







Explanation:

From the above three pictures, we can see that there are total 3 ssh sessions and 4 IP addresses involved. Their IP addresses are 172.30.0.2, 172.30.0.11, 172.16.8.99 and 172.16.8.1.