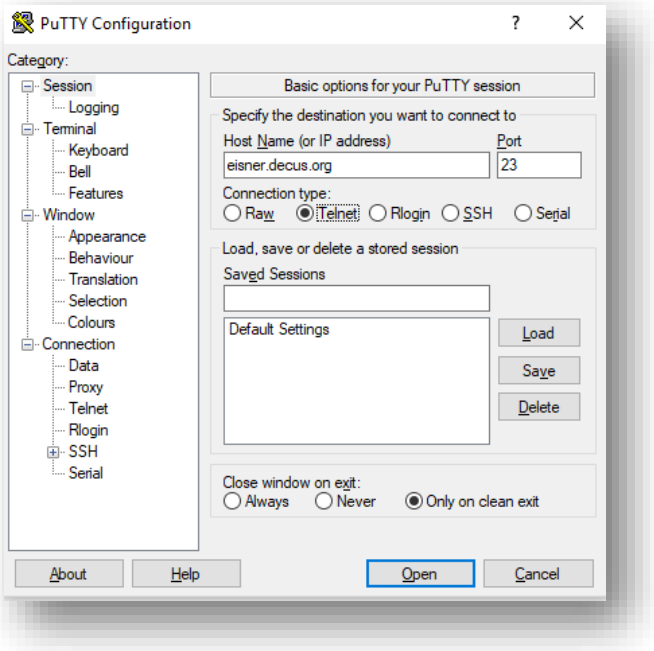
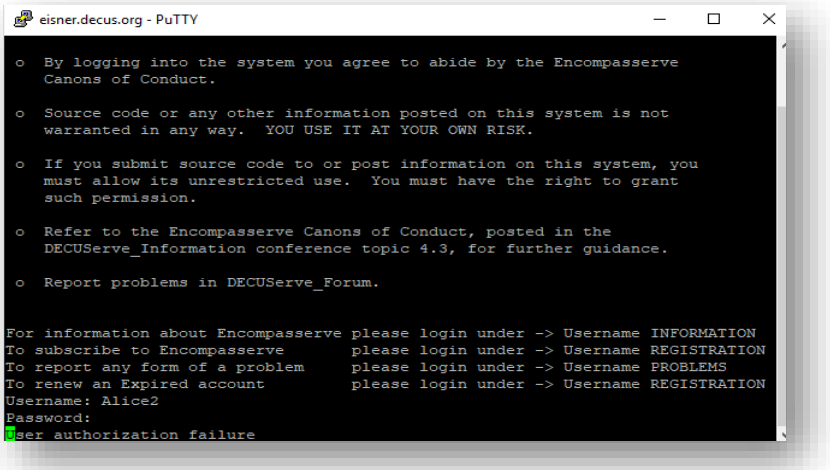
PROJECT 1 : PACKET EAVESDROPPING AND ANALYSIS

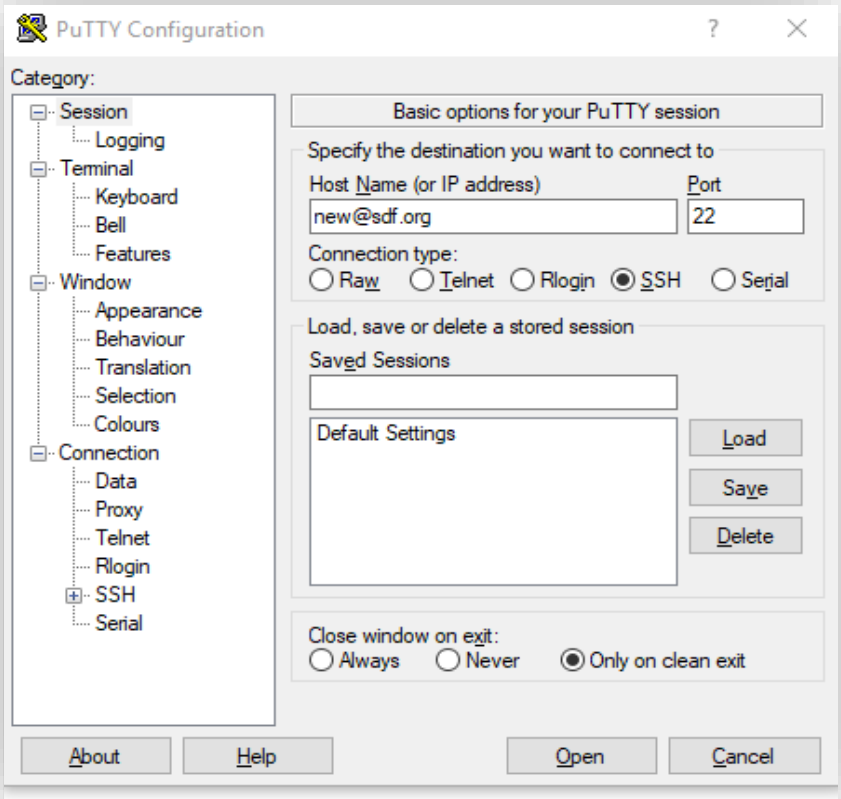
I followed all the steps given in the “Task” section of the Project 1. Following are some of the screenshots of the procedure.

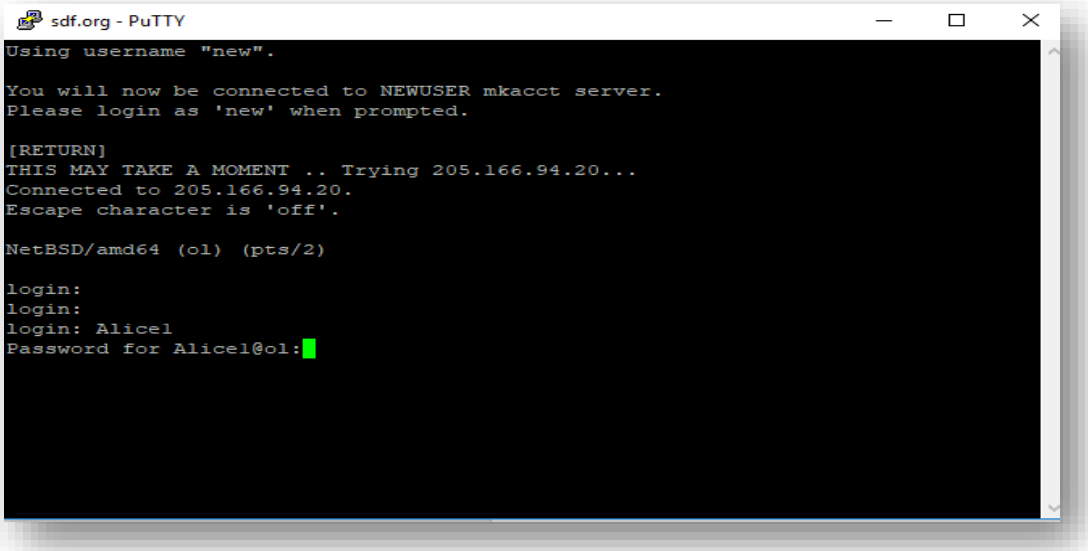
TELNET:





SSH:


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
new@sdf.org
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel


sdf.org - PuTTY
Using username "new".
You will now be connected to NEWUSER mkacct server.
Please login as 'new' when prompted.
[RETURN]
THIS MAY TAKE A MOMENT .. Trying 205.166.94.20...
Connected to 205.166.94.20.
Escape character is 'off'.
NetBSD/amd64 (ol) (pts/2)
login:
login:
login: Alicel
Password for Alicel@ol:

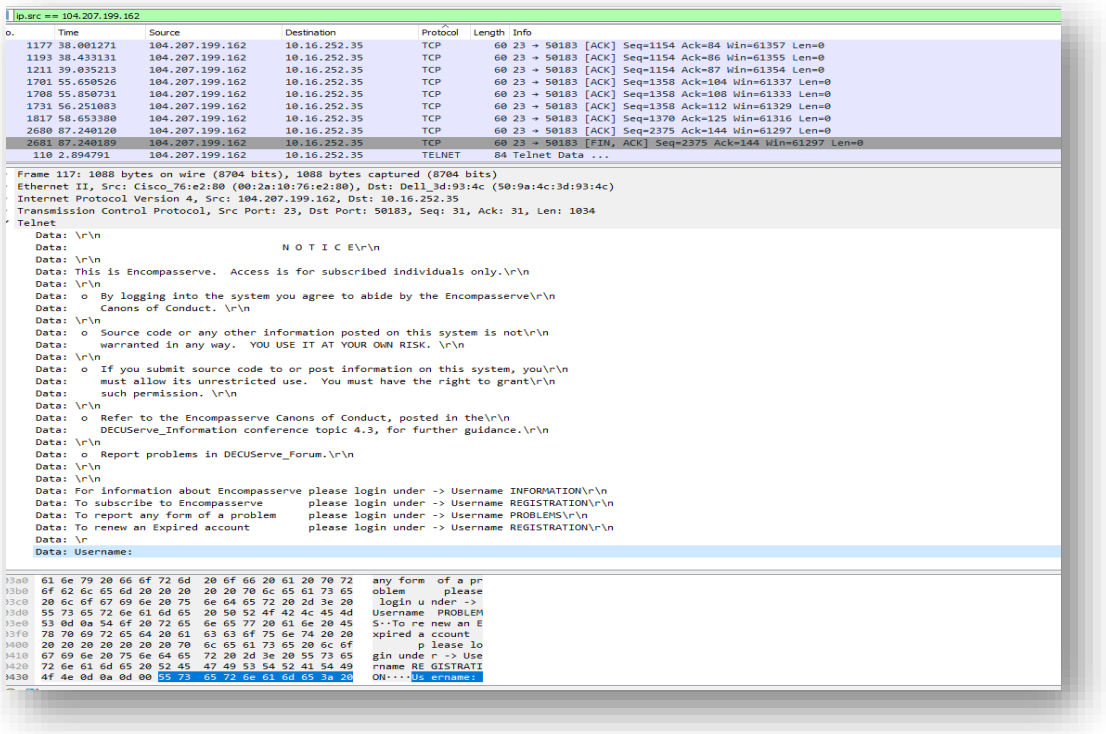
After performing the steps and analyzing the packet dumps, I came to the following conclusions for the Turn-in questions:

(A) What are the IP addresses of "eisner.decus.org" and "new@sdf.org"?

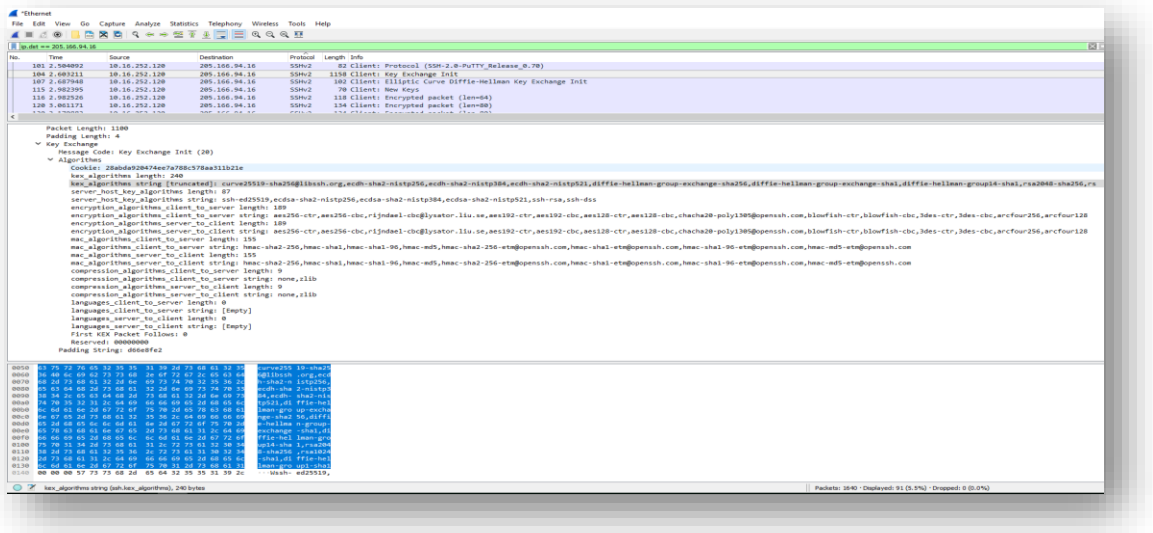
The IP address of eisner.decus.org used to connect via Telnet is 104.207.199.162 &
The IP address of sdf.org used to connect via SSH is 205.166.94.15

(B) Screenshots of the packet dump for the TELNET operation and the SSH operation. Please choose the packets with relatively large size so that we can see the data contents.

Screenshots of packet dump for TELNET:



Screenshot of packet dump for SSH:



(C) Please answer, which protocol does PuTTY use to establish encryption key with the SSH server?

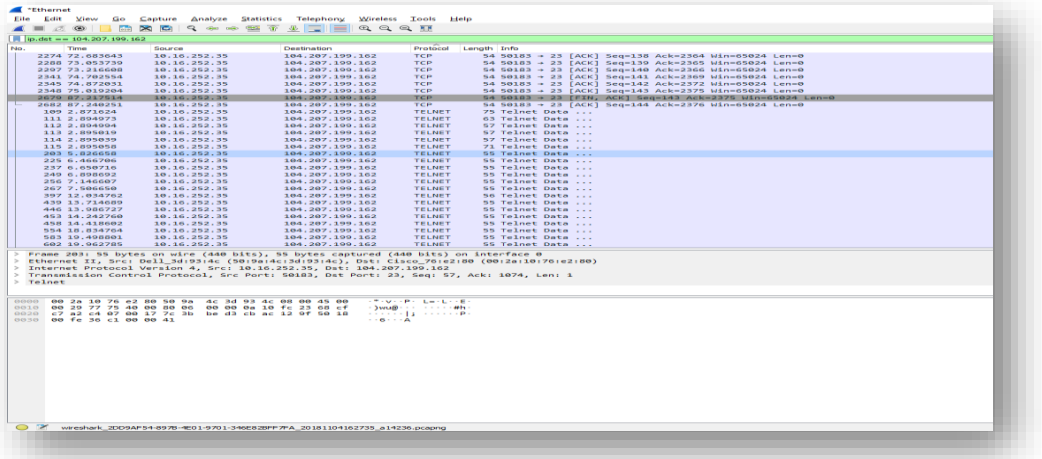
As seen in the above screenshot, PuTTY uses Deffie Hellman protocol to establish encryption key with the SSH server.

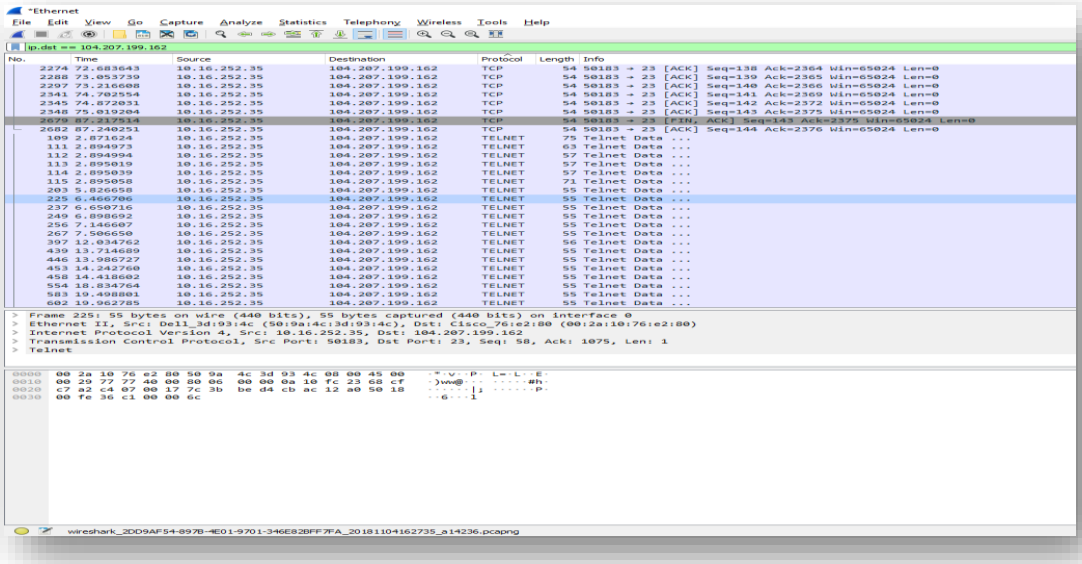
(D) Shortly analyze the packet dump out and explain why SSH is more secure than TELNET.

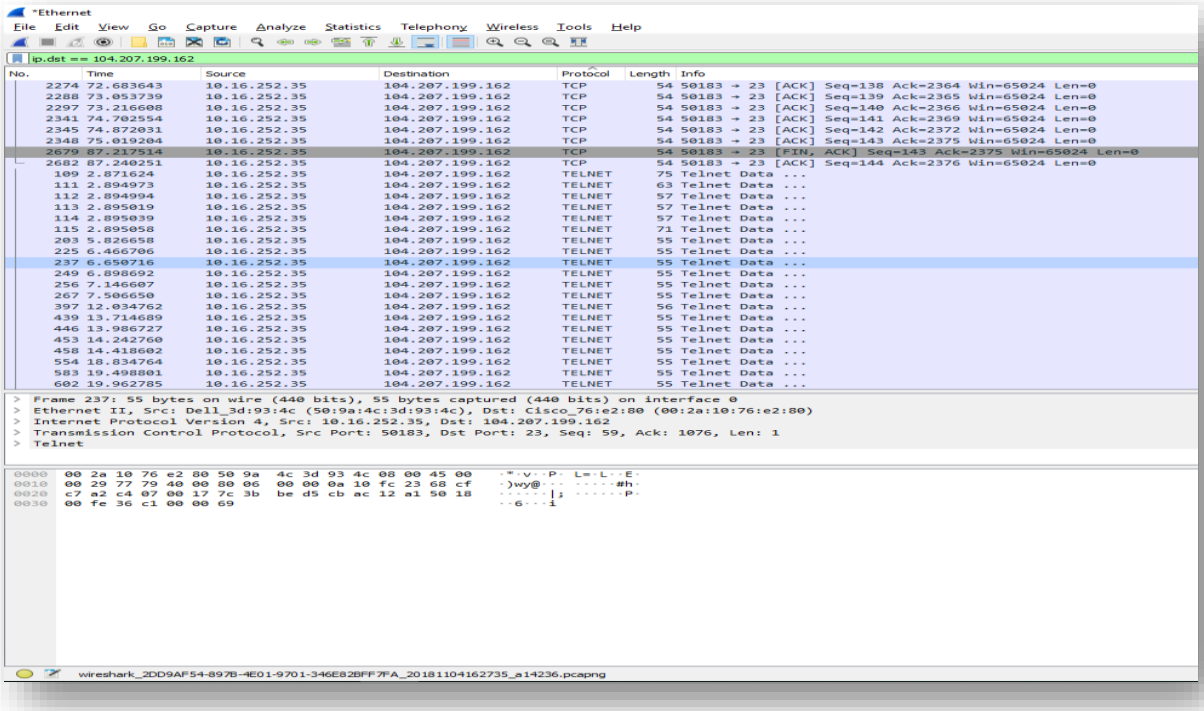
As seen in the screenshots below, it is seen that the usernames and passwords are sent over the communication channel in plaintext format in a Telnet communication. At the same time, the usernames and passwords are sent in a encrypted format in a SSH connection.

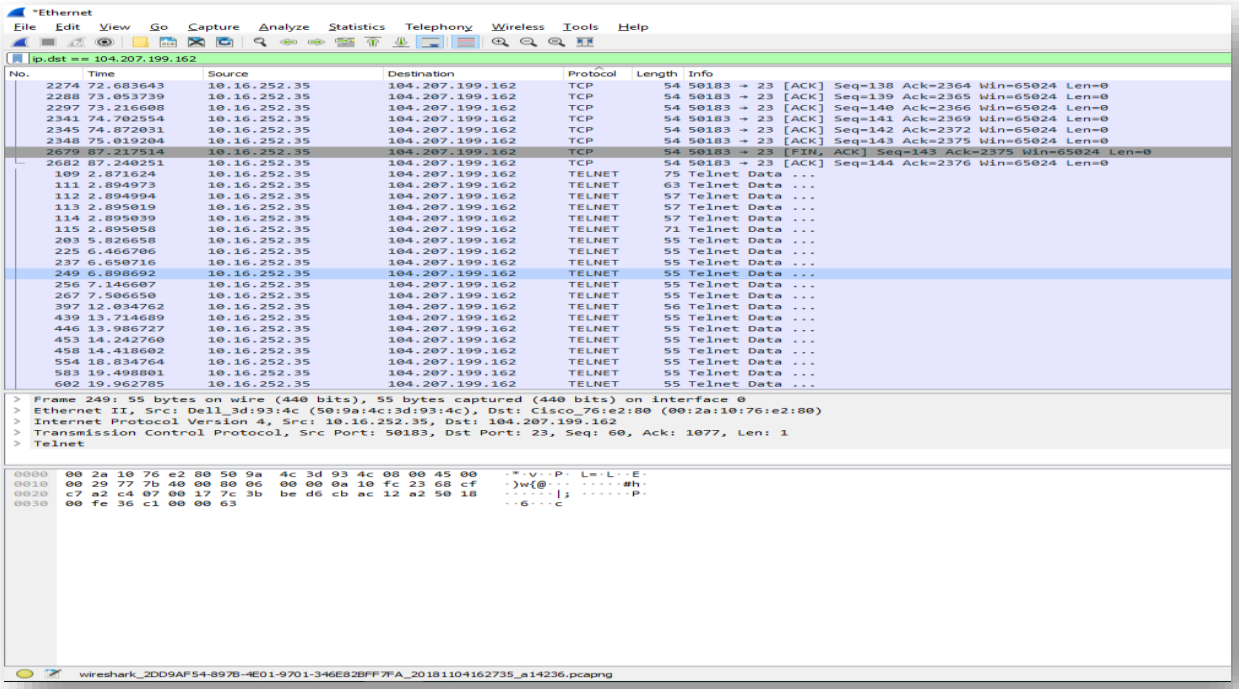
Telnet Packets:

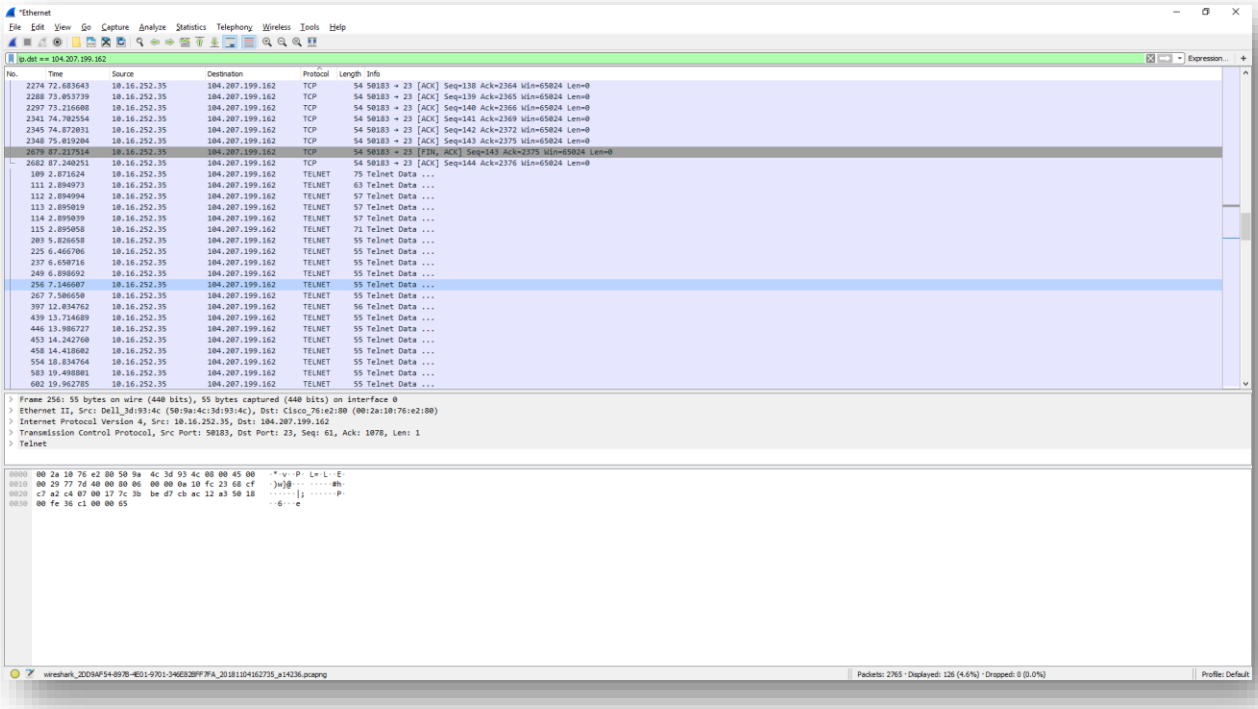
Username: Alice2 ; Password: p455ab

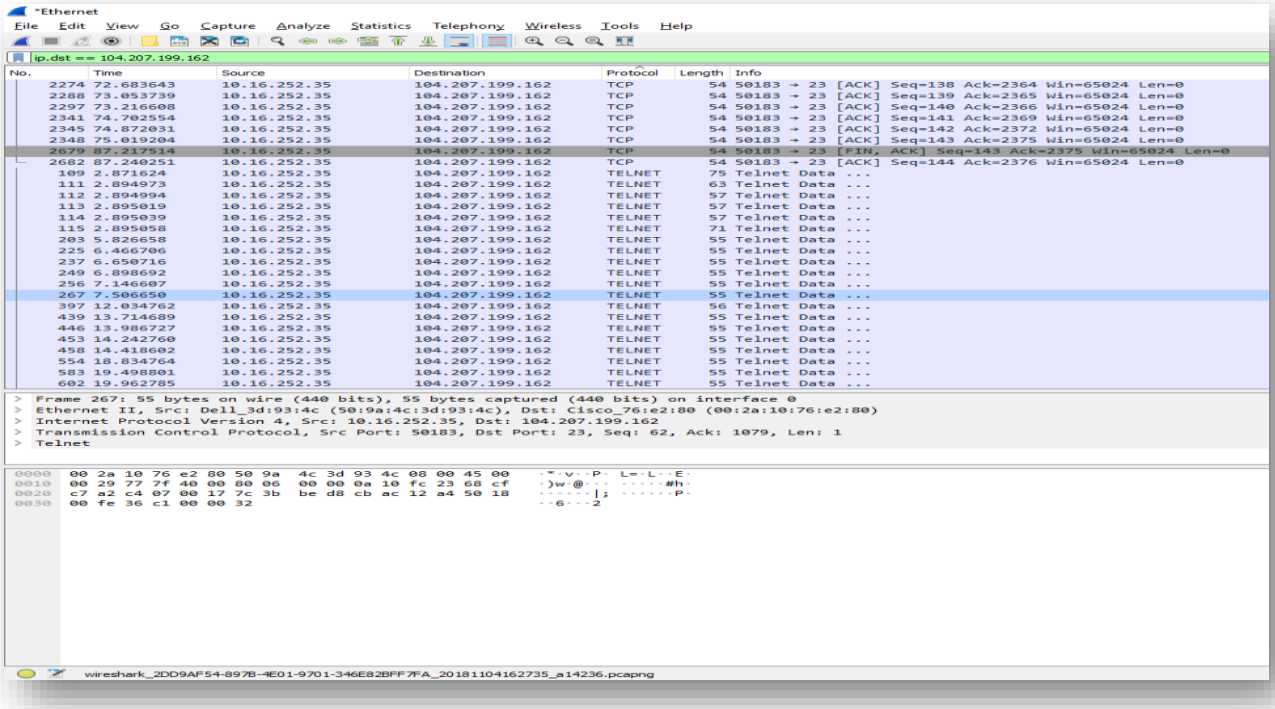


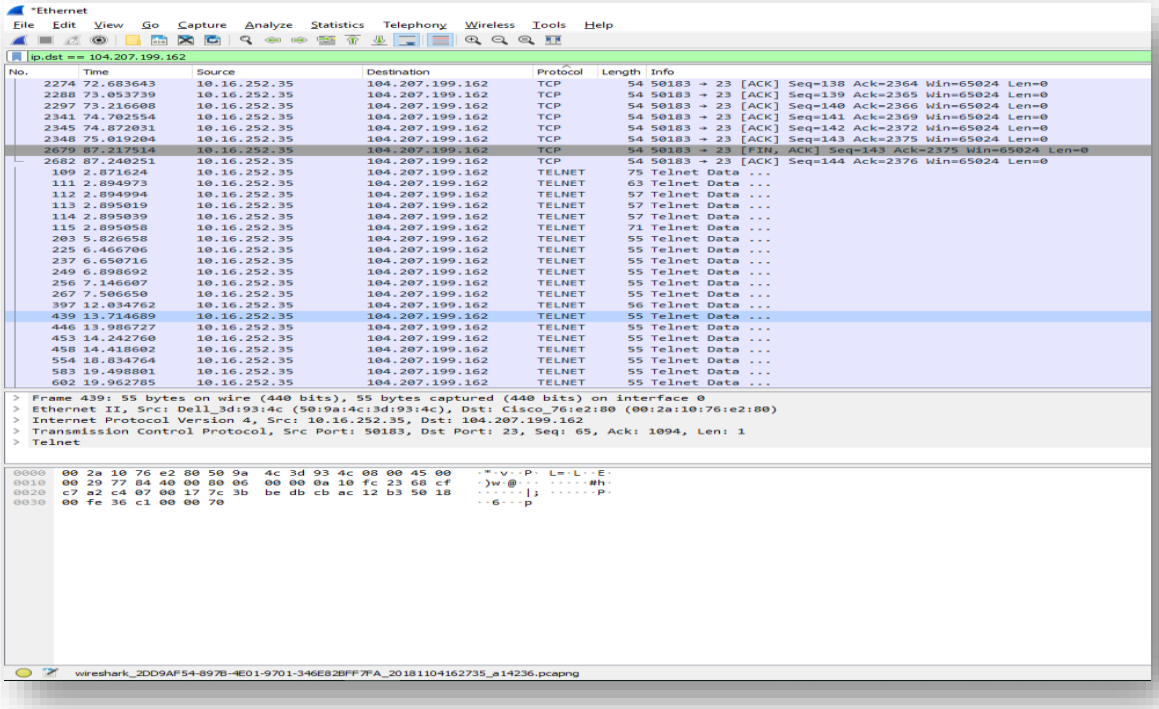

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 104.207.199.162
No. Time Source Destination Protocol Length Info
2274 72.683643 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=138 Ack=2364 Win=65024 Len=0
2288 73.053739 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=139 Ack=2365 Win=65024 Len=0
2297 73.216608 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=140 Ack=2366 Win=65024 Len=0
2341 74.702554 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=141 Ack=2369 Win=65024 Len=0
2345 74.872031 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=142 Ack=2372 Win=65024 Len=0
2348 75.019204 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=143 Ack=2375 Win=65024 Len=0
2679 87.217514 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [FIN, ACK] Seq=143 Ack=2375 Win=65024 Len=0
2682 87.240251 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=144 Ack=2376 Win=65024 Len=0
109 2.871624 10.16.252.35 104.207.199.162 TELNET 75 Telnet Data ...
111 2.894973 10.16.252.35 104.207.199.162 TELNET 63 Telnet Data ...
112 2.894994 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
113 2.895019 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
114 2.895039 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
115 2.895058 10.16.252.35 104.207.199.162 TELNET 71 Telnet Data ...
203 5.826658 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
225 6.466706 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
237 6.650716 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
249 6.898692 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
256 7.146607 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
267 7.506650 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
397 12.034762 10.16.252.35 104.207.199.162 TELNET 56 Telnet Data ...
439 13.714689 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
446 13.986727 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
453 14.242760 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
458 14.418602 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
554 18.834764 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
583 19.498801 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
602 19.962785 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
> Frame 225: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Dell_3d:93:4c (50:9a:4c:3d:93:4c), Dst: Cisco_76:e2:80 (00:2a:10:76:e2:80)
> Internet Protocol Version 4, Src: 10.16.252.35, Dst: 104.207.199.162
> Transmission Control Protocol, Src Port: 50183, Dst Port: 23, Seq: 58, Ack: 1075, Len: 1
> Telnet
0000 00 2a 10 76 e2 80 50 9a 4c 3d 93 4c 08 00 45 00 ·*·v··P· L=·L··E·
0010 00 29 77 77 40 00 80 06 00 00 0a 10 fc 23 68 cf ·)ww@··· ·····#h·
0020 c7 a2 c4 07 00 17 7c 3b be d4 cb ac 12 a0 50 18 ·····|; ·····P·
0030 00 fe 36 c1 00 00 6c ··6···l
wireshark_2DD9AF54-897B-4E01-9701-346E82BFF7FA_20181104162735_a14236.pcapng

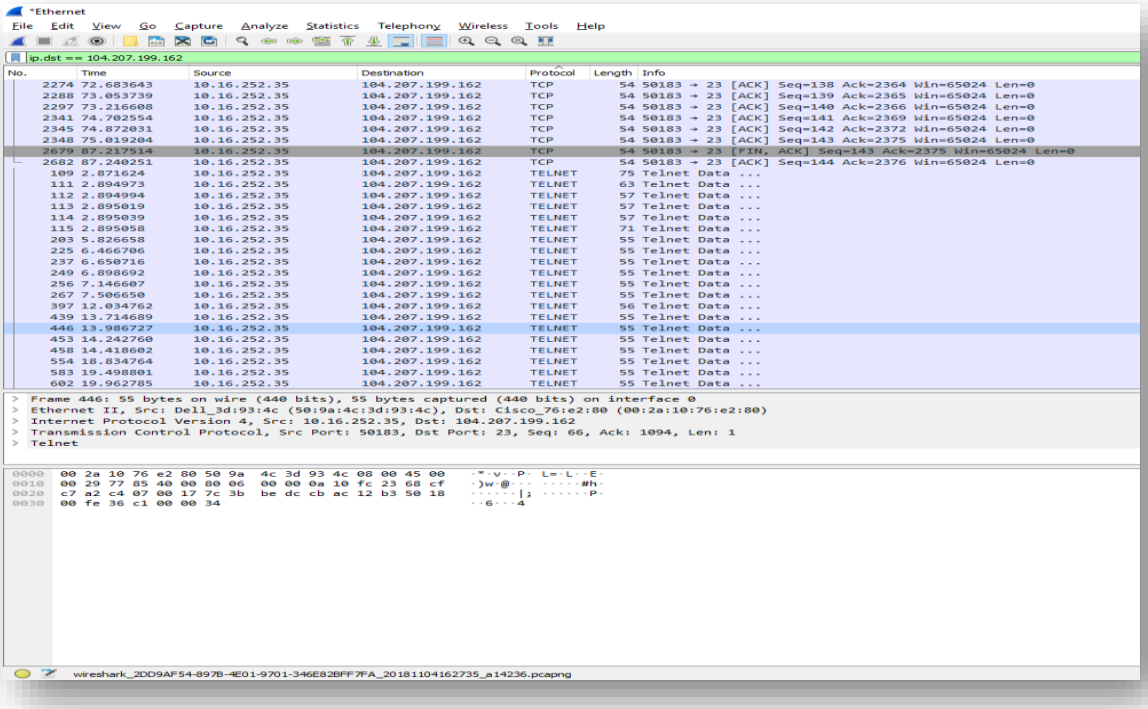

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 104.207.199.162
No. Time Source Destination Protocol Length Info
2274 72.683643 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=138 Ack=2364 Win=65024 Len=0
2288 73.053739 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=139 Ack=2365 Win=65024 Len=0
2297 73.216608 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=140 Ack=2366 Win=65024 Len=0
2341 74.702554 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=141 Ack=2369 Win=65024 Len=0
2345 74.872031 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=142 Ack=2372 Win=65024 Len=0
2348 75.019204 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=143 Ack=2375 Win=65024 Len=0
2679 87.217514 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [FIN, ACK] Seq=143 Ack=2375 Win=65024 Len=0
2682 87.240251 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=144 Ack=2376 Win=65024 Len=0
109 2.871624 10.16.252.35 104.207.199.162 TELNET 75 Telnet Data ...
111 2.894973 10.16.252.35 104.207.199.162 TELNET 63 Telnet Data ...
112 2.894994 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
113 2.895019 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
114 2.895039 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
115 2.895058 10.16.252.35 104.207.199.162 TELNET 71 Telnet Data ...
203 5.826658 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
225 6.466706 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
237 6.650716 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
249 6.898692 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
256 7.146607 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
267 7.506650 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
397 12.034762 10.16.252.35 104.207.199.162 TELNET 56 Telnet Data ...
439 13.714689 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
446 13.986727 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
453 14.242760 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
458 14.418602 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
554 18.834764 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
583 19.498801 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
602 19.962785 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
> Frame 237: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Dell_3d:93:4c (50:9a:4c:3d:93:4c), Dst: Cisco_76:e2:80 (00:2a:10:76:e2:80)
> Internet Protocol Version 4, Src: 10.16.252.35, Dst: 104.207.199.162
> Transmission Control Protocol, Src Port: 50183, Dst Port: 23, Seq: 59, Ack: 1076, Len: 1
> Telnet
0000 00 2a 10 76 e2 80 50 9a 4c 3d 93 4c 08 00 45 00 ·*·v··P· L=·L··E·
0010 00 29 77 79 40 00 80 06 00 00 0a 10 fc 23 68 cf ·)wy@··· ·····#h·
0020 c7 a2 c4 07 00 17 7c 3b be d5 cb ac 12 a1 50 18 ·····|; ·····P·
0030 00 fe 36 c1 00 00 69 ··6···i
wireshark_2DD9AF54-897B-4E01-9701-346E82BFF7FA_20181104162735_a14236.pcapng

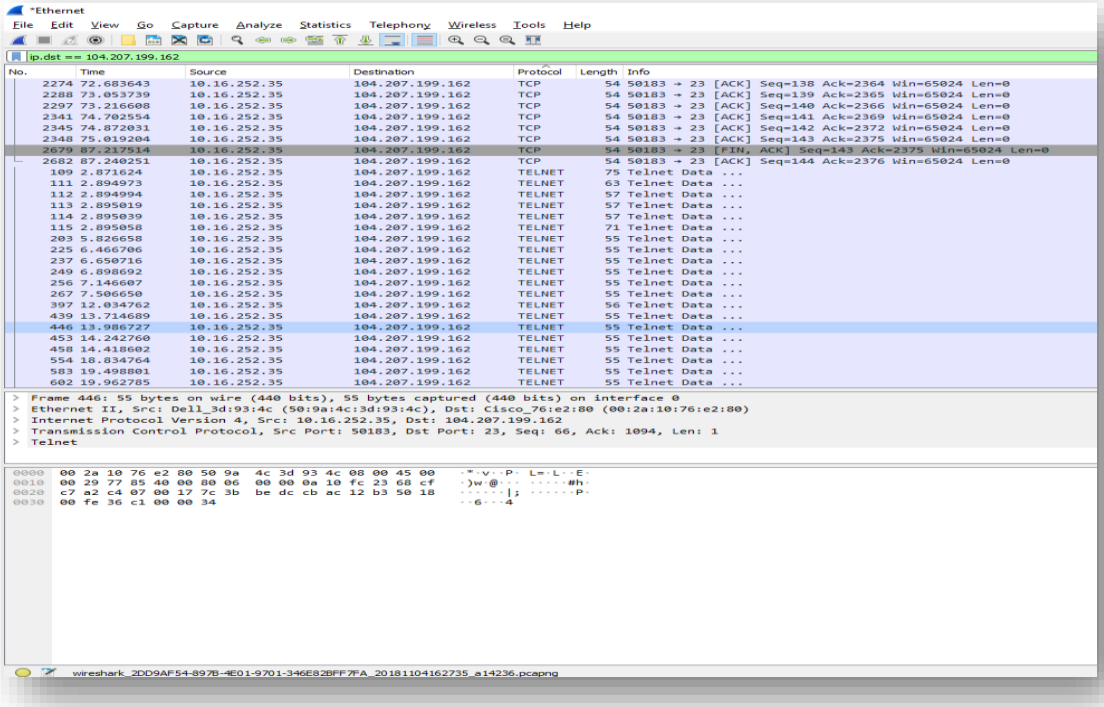

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 104.207.199.162
No. Time Source Destination Protocol Length Info
2274 72.683643 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=138 Ack=2364 Win=65024 Len=0
2288 73.053739 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=139 Ack=2365 Win=65024 Len=0
2297 73.216608 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=140 Ack=2366 Win=65024 Len=0
2341 74.702554 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=141 Ack=2369 Win=65024 Len=0
2345 74.872031 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=142 Ack=2372 Win=65024 Len=0
2348 75.019204 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=143 Ack=2375 Win=65024 Len=0
2679 87.217514 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [FIN, ACK] Seq=143 Ack=2375 Win=65024 Len=0
2682 87.240251 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=144 Ack=2376 Win=65024 Len=0
109 2.871624 10.16.252.35 104.207.199.162 TELNET 75 Telnet Data ...
111 2.894973 10.16.252.35 104.207.199.162 TELNET 63 Telnet Data ...
112 2.894994 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
113 2.895019 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
114 2.895039 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
115 2.895058 10.16.252.35 104.207.199.162 TELNET 71 Telnet Data ...
203 5.826658 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
225 6.466706 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
237 6.650716 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
249 6.898692 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
256 7.146607 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
267 7.506650 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
397 12.034762 10.16.252.35 104.207.199.162 TELNET 56 Telnet Data ...
439 13.714689 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
446 13.986727 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
453 14.242760 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
458 14.418602 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
554 18.834764 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
583 19.498801 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
602 19.962785 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
> Frame 249: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Dell_3d:93:4c (50:9a:4c:3d:93:4c), Dst: Cisco_76:e2:80 (00:2a:10:76:e2:80)
> Internet Protocol Version 4, Src: 10.16.252.35, Dst: 104.207.199.162
> Transmission Control Protocol, Src Port: 50183, Dst Port: 23, Seq: 60, Ack: 1077, Len: 1
> Telnet
0000 00 2a 10 76 e2 80 50 9a 4c 3d 93 4c 08 00 45 00 ·*·v··P· L=·L··E·
0010 00 29 77 7b 40 00 80 06 00 00 0a 10 fc 23 68 cf ·)w{@··· ·····#h·
0020 c7 a2 c4 07 00 17 7c 3b be d6 cb ac 12 a2 50 18 ·····|; ·····P·
0030 00 fe 36 c1 00 00 63 ··6···c
wireshark_2DD9AF54-897B-4E01-9701-346E82BFF7FA_20181104162735_a14236.pcapng

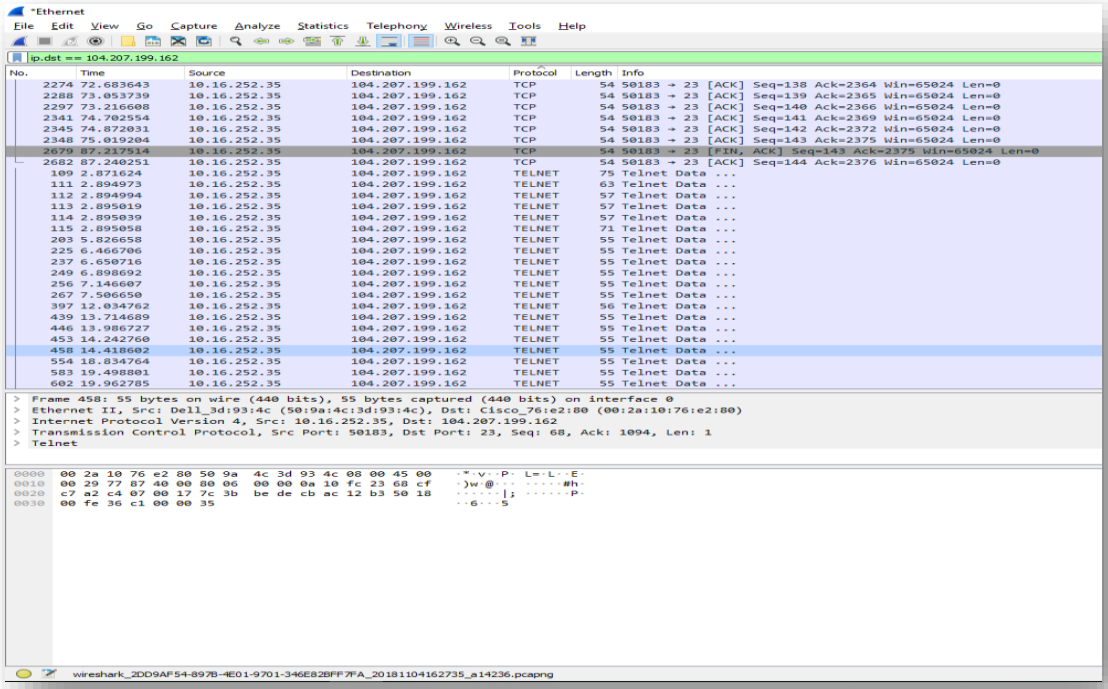

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 104.207.199.162
No. Time Source Destination Protocol Length Info
2274 72.683643 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=138 Ack=2364 Win=65024 Len=0
2288 73.053739 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=139 Ack=2365 Win=65024 Len=0
2297 73.216608 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=140 Ack=2366 Win=65024 Len=0
2341 74.702554 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=141 Ack=2369 Win=65024 Len=0
2345 74.872031 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=142 Ack=2372 Win=65024 Len=0
2348 75.019204 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=143 Ack=2375 Win=65024 Len=0
2679 87.217514 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [FIN, ACK] Seq=143 Ack=2375 Win=65024 Len=0
2682 87.240251 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=144 Ack=2376 Win=65024 Len=0
109 2.871624 10.16.252.35 104.207.199.162 TELNET 75 Telnet Data ...
111 2.894973 10.16.252.35 104.207.199.162 TELNET 63 Telnet Data ...
112 2.894994 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
113 2.895019 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
114 2.895039 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
115 2.895058 10.16.252.35 104.207.199.162 TELNET 71 Telnet Data ...
203 5.826658 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
225 6.466706 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
237 6.650716 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
249 6.898692 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
256 7.146607 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
267 7.506650 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
397 12.034762 10.16.252.35 104.207.199.162 TELNET 56 Telnet Data ...
439 13.714689 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
446 13.986727 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
453 14.242760 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
458 14.418602 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
554 18.834764 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
583 19.498801 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
602 19.962785 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
> Frame 256: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Dell_3d:93:4c (50:9a:4c:3d:93:4c), Dst: Cisco_76:e2:80 (00:2a:10:76:e2:80)
> Internet Protocol Version 4, Src: 10.16.252.35, Dst: 104.207.199.162
> Transmission Control Protocol, Src Port: 50183, Dst Port: 23, Seq: 61, Ack: 1078, Len: 1
> Telnet
0000 00 2a 10 76 e2 80 50 9a 4c 3d 93 4c 08 00 45 00 ·*·v··P· L=·L··E·
0010 00 29 77 7d 40 00 80 06 00 00 0a 10 fc 23 68 cf ·)w}@··· ·····#h·
0020 c7 a2 c4 07 00 17 7c 3b be d7 cb ac 12 a3 50 18 ·····|; ·····P·
0030 00 fe 36 c1 00 00 65 ··6···e
wireshark_2DD9AF54-897B-4E01-9701-346E82BFF7FA_20181104162735_a14236.pcapng
Packets: 2765 · Displayed: 126 (4.6%) · Dropped: 0 (0.0%)
Profile: Default

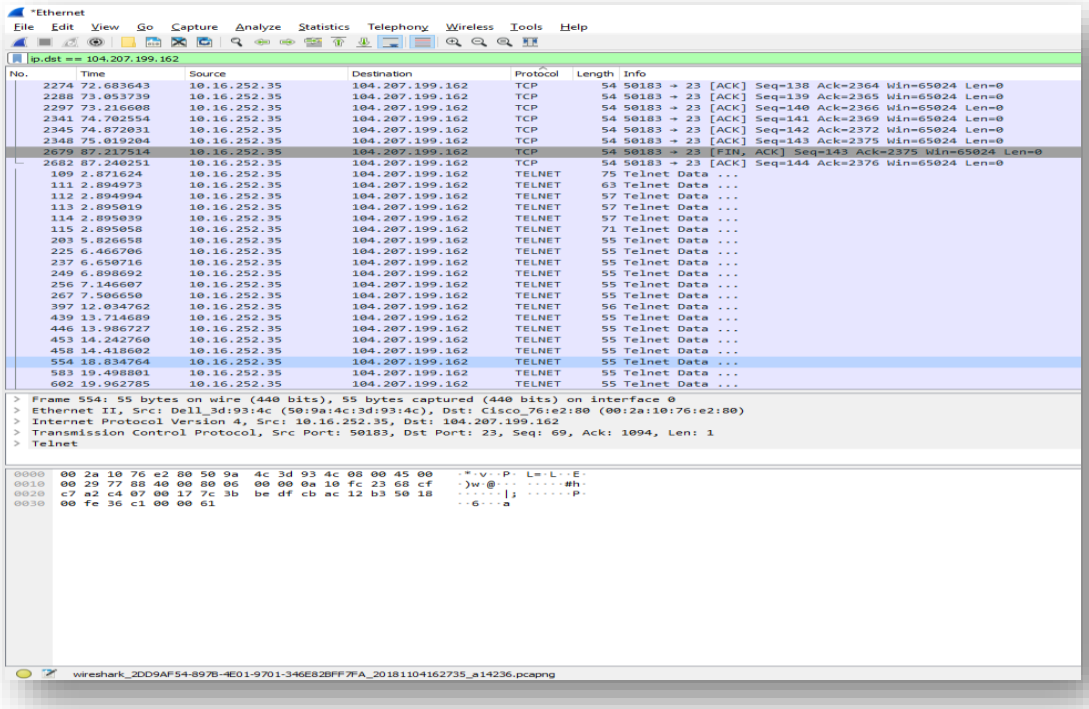

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 104.207.199.162
No. Time Source Destination Protocol Length Info
2274 72.683643 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=138 Ack=2364 Win=65024 Len=0
2288 73.053739 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=139 Ack=2365 Win=65024 Len=0
2297 73.216608 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=140 Ack=2366 Win=65024 Len=0
2341 74.702554 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=141 Ack=2369 Win=65024 Len=0
2345 74.872031 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=142 Ack=2372 Win=65024 Len=0
2348 75.019204 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=143 Ack=2375 Win=65024 Len=0
2679 87.217514 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [FIN, ACK] Seq=143 Ack=2375 Win=65024 Len=0
2682 87.240251 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=144 Ack=2376 Win=65024 Len=0
109 2.871624 10.16.252.35 104.207.199.162 TELNET 75 Telnet Data ...
111 2.894973 10.16.252.35 104.207.199.162 TELNET 63 Telnet Data ...
112 2.894994 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
113 2.895019 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
114 2.895039 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
115 2.895058 10.16.252.35 104.207.199.162 TELNET 71 Telnet Data ...
203 5.826658 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
225 6.466706 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
237 6.650716 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
249 6.898692 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
256 7.146607 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
267 7.506650 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
397 12.034762 10.16.252.35 104.207.199.162 TELNET 56 Telnet Data ...
439 13.714689 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
446 13.986727 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
453 14.242760 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
458 14.418602 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
554 18.834764 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
583 19.498801 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
602 19.962785 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
> Frame 267: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Dell_3d:93:4c (50:9a:4c:3d:93:4c), Dst: Cisco_76:e2:80 (00:2a:10:76:e2:80)
> Internet Protocol Version 4, Src: 10.16.252.35, Dst: 104.207.199.162
> Transmission Control Protocol, Src Port: 50183, Dst Port: 23, Seq: 62, Ack: 1079, Len: 1
> Telnet
0000 00 2a 10 76 e2 80 50 9a 4c 3d 93 4c 08 00 45 00
0010 00 29 77 7f 40 00 80 06 00 00 0a 10 fc 23 68 cf
0020 c7 a2 c4 07 00 17 7c 3b be d8 cb ac 12 a4 50 18
0030 00 fe 36 c1 00 00 32
wireshark_2DD9AF54-897B-4E01-9701-346E82BFF7FA_20181104162735_a14236.pcapng

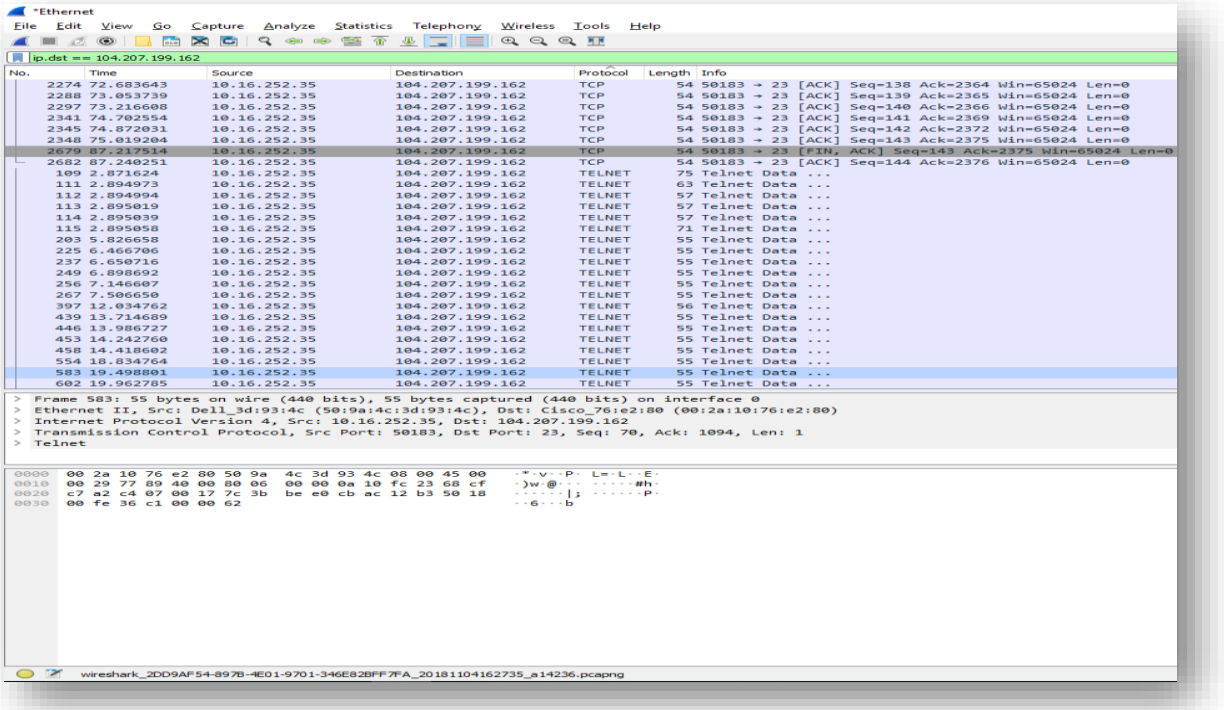

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 104.207.199.162
No. Time Source Destination Protocol Length Info
2274 72.683643 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=138 Ack=2364 Win=65024 Len=0
2288 73.053739 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=139 Ack=2365 Win=65024 Len=0
2297 73.216608 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=140 Ack=2366 Win=65024 Len=0
2341 74.702554 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=141 Ack=2369 Win=65024 Len=0
2345 74.872031 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=142 Ack=2372 Win=65024 Len=0
2348 75.019204 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=143 Ack=2375 Win=65024 Len=0
2679 87.217514 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [FIN, ACK] Seq=143 Ack=2375 Win=65024 Len=0
2682 87.240251 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=144 Ack=2376 Win=65024 Len=0
109 2.871624 10.16.252.35 104.207.199.162 TELNET 75 Telnet Data ...
111 2.894973 10.16.252.35 104.207.199.162 TELNET 63 Telnet Data ...
112 2.894994 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
113 2.895019 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
114 2.895039 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
115 2.895058 10.16.252.35 104.207.199.162 TELNET 71 Telnet Data ...
203 5.826658 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
225 6.466706 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
237 6.650716 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
249 6.898692 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
256 7.146607 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
267 7.506650 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
397 12.034762 10.16.252.35 104.207.199.162 TELNET 56 Telnet Data ...
439 13.714689 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
446 13.986727 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
453 14.242760 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
458 14.418602 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
554 18.834764 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
583 19.498801 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
602 19.962785 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
> Frame 439: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Dell_3d:93:4c (50:9a:4c:3d:93:4c), Dst: Cisco_76:e2:80 (00:2a:10:76:e2:80)
> Internet Protocol Version 4, Src: 10.16.252.35, Dst: 104.207.199.162
> Transmission Control Protocol, Src Port: 50183, Dst Port: 23, Seq: 65, Ack: 1094, Len: 1
> Telnet
0000 00 2a 10 76 e2 80 50 9a 4c 3d 93 4c 08 00 45 00
0010 00 29 77 84 40 00 80 06 00 00 0a 10 fc 23 68 cf
0020 c7 a2 c4 07 00 17 7c 3b be db cb ac 12 b3 50 18
0030 00 fe 36 c1 00 00 70
wireshark_2DD9AF54-897B-4E01-9701-346E82BFF7FA_20181104162735_a14236.pcapng


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 104.207.199.162
No. Time Source Destination Protocol Length Info
2274 72.683643 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=138 Ack=2364 Win=65024 Len=0
2288 73.053739 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=139 Ack=2365 Win=65024 Len=0
2297 73.216608 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=140 Ack=2366 Win=65024 Len=0
2341 74.702554 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=141 Ack=2369 Win=65024 Len=0
2345 74.872031 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=142 Ack=2372 Win=65024 Len=0
2348 75.019204 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=143 Ack=2375 Win=65024 Len=0
2679 87.217514 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [FIN, ACK] Seq=143 Ack=2375 Win=65024 Len=0
2682 87.240251 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=144 Ack=2376 Win=65024 Len=0
109 2.871624 10.16.252.35 104.207.199.162 TELNET 75 Telnet Data ...
111 2.894973 10.16.252.35 104.207.199.162 TELNET 63 Telnet Data ...
112 2.894994 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
113 2.895019 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
114 2.895039 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
115 2.895058 10.16.252.35 104.207.199.162 TELNET 71 Telnet Data ...
203 5.826658 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
225 6.466706 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
237 6.650716 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
249 6.898692 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
256 7.146607 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
267 7.506650 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
397 12.034762 10.16.252.35 104.207.199.162 TELNET 56 Telnet Data ...
439 13.714689 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
446 13.986727 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
453 14.242760 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
458 14.418602 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
554 18.834764 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
583 19.498801 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
602 19.962785 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
> Frame 446: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Dell_3d:93:4c (50:9a:4c:3d:93:4c), Dst: Cisco_76:e2:80 (00:2a:10:76:e2:80)
> Internet Protocol Version 4, Src: 10.16.252.35, Dst: 104.207.199.162
> Transmission Control Protocol, Src Port: 50183, Dst Port: 23, Seq: 66, Ack: 1094, Len: 1
> Telnet
0000 00 2a 10 76 e2 80 50 9a 4c 3d 93 4c 08 00 45 00
0010 00 29 77 85 40 00 80 06 00 00 0a 10 fc 23 68 cf
0020 c7 a2 c4 07 00 17 7c 3b be dc cb ac 12 b3 50 18
0030 00 fe 36 c1 00 00 34
wireshark_2DD9AF54-897B-4E01-9701-346E82BFF7FA_20181104162735_a14236.pcapng


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 104.207.199.162
No. Time Source Destination Protocol Length Info
2274 72.683643 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=138 Ack=2364 Win=65024 Len=0
2288 73.053739 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=139 Ack=2365 Win=65024 Len=0
2297 73.216608 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=140 Ack=2366 Win=65024 Len=0
2341 74.702554 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=141 Ack=2369 Win=65024 Len=0
2345 74.872031 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=142 Ack=2372 Win=65024 Len=0
2348 75.019204 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=143 Ack=2375 Win=65024 Len=0
2679 87.217514 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [FIN, ACK] Seq=143 Ack=2375 Win=65024 Len=0
2682 87.240251 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=144 Ack=2376 Win=65024 Len=0
109 2.871624 10.16.252.35 104.207.199.162 TELNET 75 Telnet Data ...
111 2.894973 10.16.252.35 104.207.199.162 TELNET 63 Telnet Data ...
112 2.894994 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
113 2.895019 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
114 2.895039 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
115 2.895058 10.16.252.35 104.207.199.162 TELNET 71 Telnet Data ...
203 5.826658 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
225 6.466706 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
237 6.650716 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
249 6.898692 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
256 7.146607 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
267 7.506650 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
397 12.034762 10.16.252.35 104.207.199.162 TELNET 56 Telnet Data ...
439 13.714689 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
446 13.986727 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
453 14.242760 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
458 14.418602 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
554 18.834764 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
583 19.498801 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
602 19.962785 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
> Frame 446: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Dell_3d:93:4c (50:9a:4c:3d:93:4c), Dst: Cisco_76:e2:80 (00:2a:10:76:e2:80)
> Internet Protocol Version 4, Src: 10.16.252.35, Dst: 104.207.199.162
> Transmission Control Protocol, Src Port: 50183, Dst Port: 23, Seq: 66, Ack: 1094, Len: 1
> Telnet
0000 00 2a 10 76 e2 80 50 9a 4c 3d 93 4c 08 00 45 00
0010 00 29 77 85 40 00 80 06 00 00 0a 10 fc 23 68 cf
0020 c7 a2 c4 07 00 17 7c 3b be dc cb ac 12 b3 50 18
0030 00 fe 36 c1 00 00 34
wireshark_2DD9AF54-897B-4E01-9701-346E82BFF7FA_20181104162735_a14236.pcapng

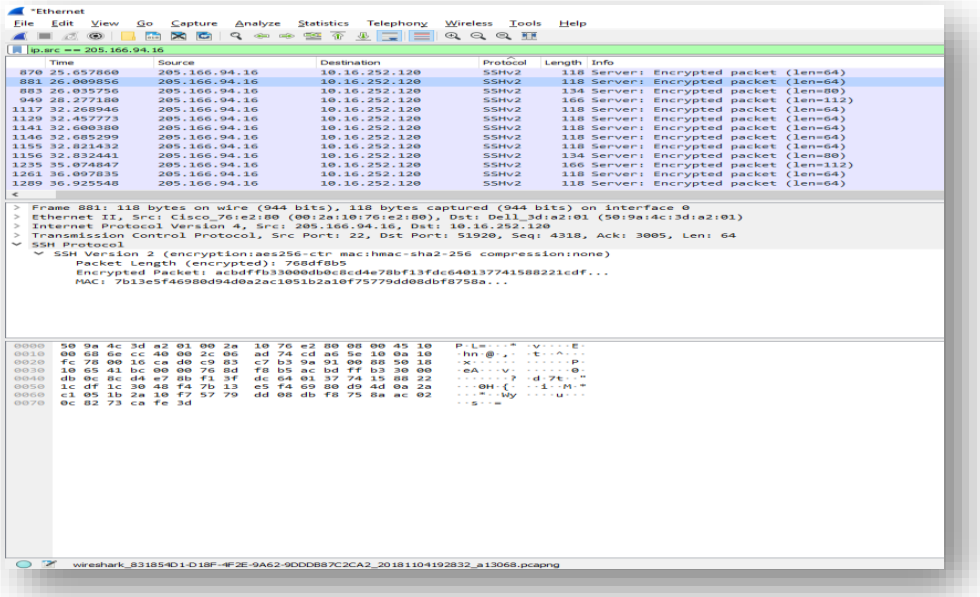

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 104.207.199.162
No. Time Source Destination Protocol Length Info
2274 72.683643 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=138 Ack=2364 Win=65024 Len=0
2288 73.053739 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=139 Ack=2365 Win=65024 Len=0
2297 73.216608 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=140 Ack=2366 Win=65024 Len=0
2341 74.702554 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=141 Ack=2369 Win=65024 Len=0
2345 74.872031 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=142 Ack=2372 Win=65024 Len=0
2348 75.019204 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=143 Ack=2375 Win=65024 Len=0
2679 87.217514 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [FIN, ACK] Seq=143 Ack=2375 Win=65024 Len=0
2682 87.240251 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=144 Ack=2376 Win=65024 Len=0
109 2.871624 10.16.252.35 104.207.199.162 TELNET 75 Telnet Data ...
111 2.894973 10.16.252.35 104.207.199.162 TELNET 63 Telnet Data ...
112 2.894994 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
113 2.895019 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
114 2.895039 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
115 2.895058 10.16.252.35 104.207.199.162 TELNET 71 Telnet Data ...
203 5.826658 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
225 6.466706 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
237 6.650716 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
249 6.898692 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
256 7.146607 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
267 7.506650 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
397 12.034762 10.16.252.35 104.207.199.162 TELNET 56 Telnet Data ...
439 13.714689 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
446 13.986727 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
453 14.242760 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
458 14.418602 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
554 18.834764 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
583 19.498801 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
602 19.962785 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
> Frame 458: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Dell_3d:93:4c (50:9a:4c:3d:93:4c), Dst: Cisco_76:e2:80 (00:2a:10:76:e2:80)
> Internet Protocol Version 4, Src: 10.16.252.35, Dst: 104.207.199.162
> Transmission Control Protocol, Src Port: 50183, Dst Port: 23, Seq: 68, Ack: 1094, Len: 1
> Telnet
0000 00 2a 10 76 e2 80 50 9a 4c 3d 93 4c 08 00 45 00 ·*·v··P· L=·L··E·
0010 00 29 77 87 40 00 80 06 00 00 0a 10 fc 23 68 cf ·)w·@··· ·····#h·
0020 c7 a2 c4 07 00 17 7c 3b be de cb ac 12 b3 50 18 ·····|; ·····P·
0030 00 fe 36 c1 00 00 35 ··6···5
wireshark_2DD9AF54-897B-4E01-9701-346E82BFF7FA_20181104162735_a14236.pcapng


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 104.207.199.162
No. Time Source Destination Protocol Length Info
2274 72.683643 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=138 Ack=2364 Win=65024 Len=0
2288 73.053739 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=139 Ack=2365 Win=65024 Len=0
2297 73.216608 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=140 Ack=2366 Win=65024 Len=0
2341 74.702554 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=141 Ack=2369 Win=65024 Len=0
2345 74.872031 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=142 Ack=2372 Win=65024 Len=0
2348 75.019204 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=143 Ack=2375 Win=65024 Len=0
2679 87.217514 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [FIN, ACK] Seq=143 Ack=2375 Win=65024 Len=0
2682 87.240251 10.16.252.35 104.207.199.162 TCP 54 50183 → 23 [ACK] Seq=144 Ack=2376 Win=65024 Len=0
109 2.871624 10.16.252.35 104.207.199.162 TELNET 75 Telnet Data ...
111 2.894973 10.16.252.35 104.207.199.162 TELNET 63 Telnet Data ...
112 2.894994 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
113 2.895019 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
114 2.895039 10.16.252.35 104.207.199.162 TELNET 57 Telnet Data ...
115 2.895058 10.16.252.35 104.207.199.162 TELNET 71 Telnet Data ...
203 5.826658 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
225 6.466706 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
237 6.650716 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
249 6.898692 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
256 7.146607 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
267 7.506650 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
397 12.034762 10.16.252.35 104.207.199.162 TELNET 56 Telnet Data ...
439 13.714689 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
446 13.986727 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
453 14.242760 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
458 14.418602 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
554 18.834764 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
583 19.498801 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
602 19.962785 10.16.252.35 104.207.199.162 TELNET 55 Telnet Data ...
> Frame 554: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Dell_3d:93:4c (50:9a:4c:3d:93:4c), Dst: Cisco_76:e2:80 (00:2a:10:76:e2:80)
> Internet Protocol Version 4, Src: 10.16.252.35, Dst: 104.207.199.162
> Transmission Control Protocol, Src Port: 50183, Dst Port: 23, Seq: 69, Ack: 1094, Len: 1
> Telnet
0000 00 2a 10 76 e2 80 50 9a 4c 3d 93 4c 08 00 45 00 ·*·v··P· L=·L··E·
0010 00 29 77 88 40 00 80 06 00 00 0a 10 fc 23 68 cf ·)w·@··· ·····#h·
0020 c7 a2 c4 07 00 17 7c 3b be df cb ac 12 b3 50 18 ·····|; ·····P·
0030 00 fe 36 c1 00 00 61 ··6···a
wireshark_2DD9AF54-897B-4E01-9701-346E82BFF7FA_20181104162735_a14236.pcapng



SSH Packets:

Username: Alice1 ; Password: p455abc

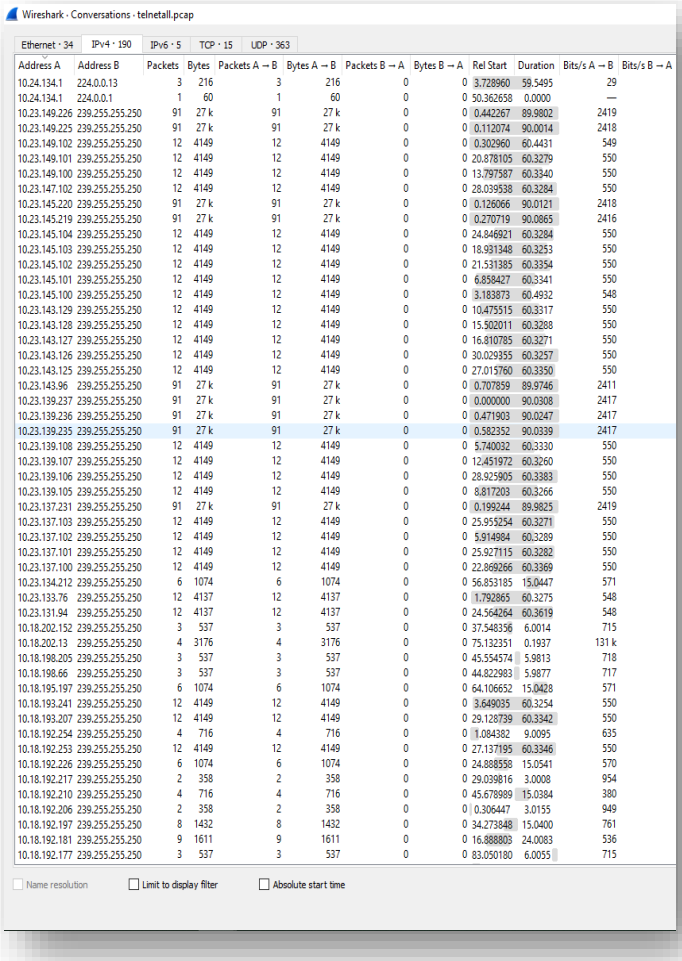


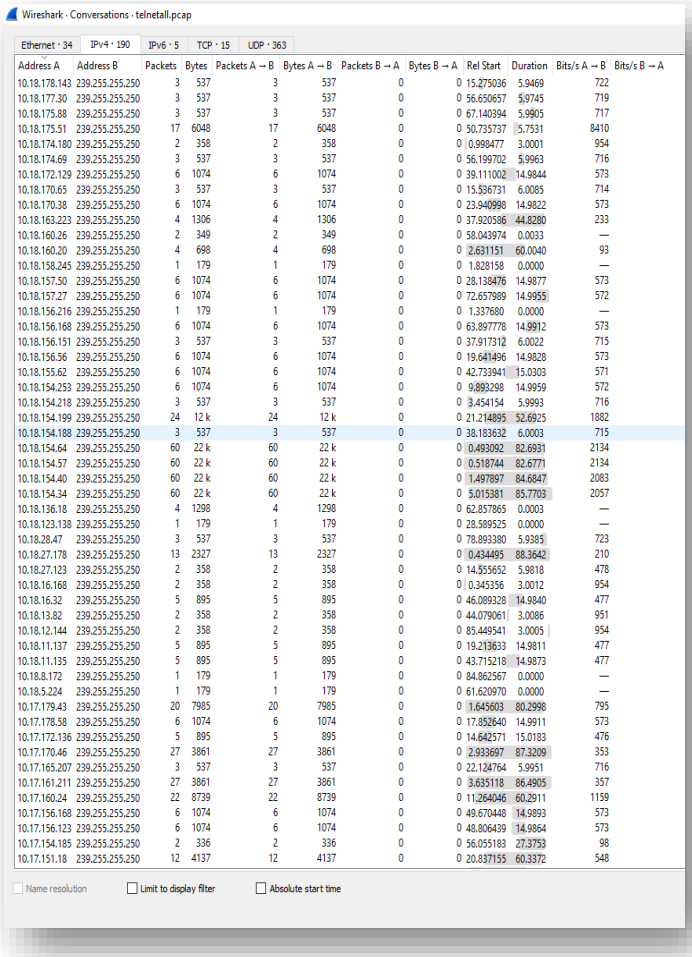
(E) Now open the packet capture for the TELNET operations again. You will notice that there are many other types of packets such as DNS, TCP, etc. Please answer:

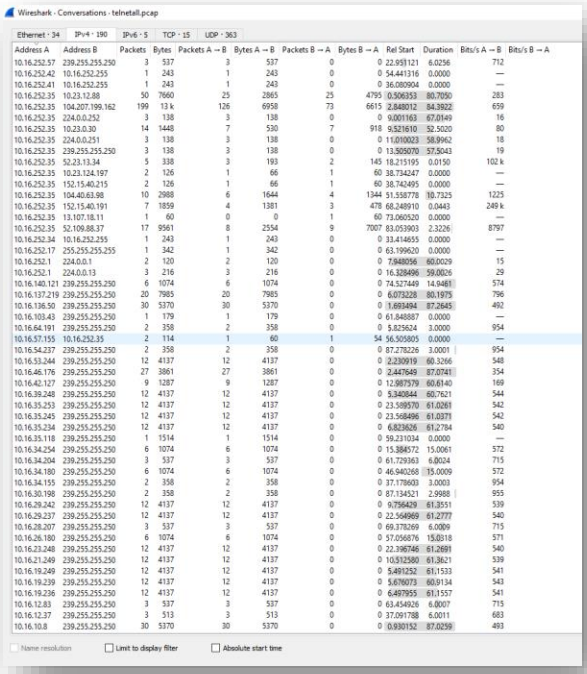
(1) List all different IP addresses that you see in these captured packets;

(2) List all TCP connections between the IP addresses that you capture. Please note that for a TCP connection, you need to provide (Source IP, Source PORT, Destination IP, Destination PORT)

(1) The list of all the IPs that I can see in these captured packets are in the screenshot below:







(2) A list of all TCP connections is give in the screenshots below: