National Institute 0f Technology, Hamirpur

Department Of Computer Science and Engineering

Sept-November 2020

Subject Name: Information Security Lab	**Subject Code:** CSD – 415
Course: Information Security	**Semester:** 4th Year, 7th semester
Submitted By: Student Name: Rishabh Katna Roll No: 17MI552	**Submitted To:** Dr. Narottam Chand
Faculty Signature:	

PRACTICAL #1

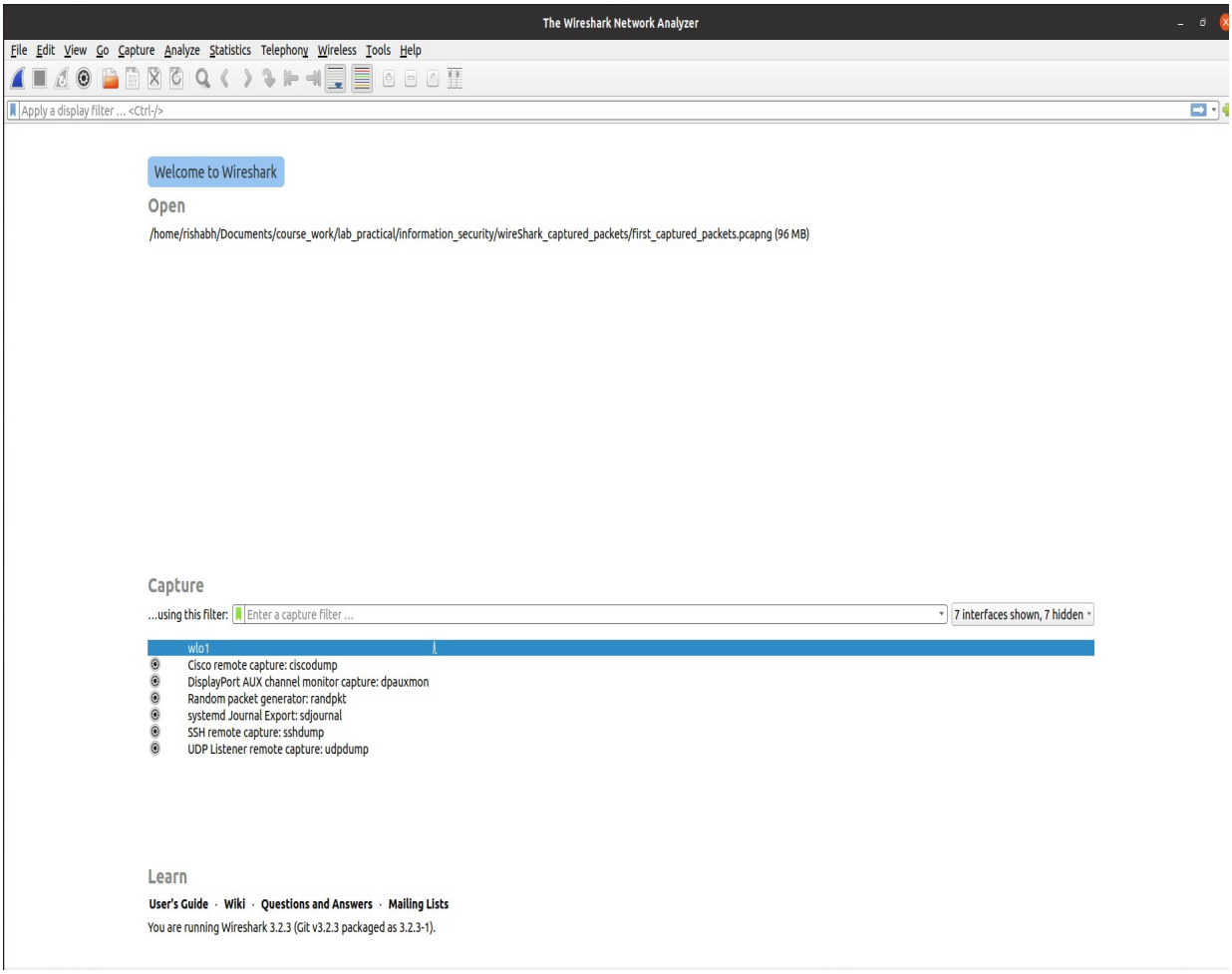
AIM : Introduction to Wireshark and implement Capture packets and Display packets in Wireshark.

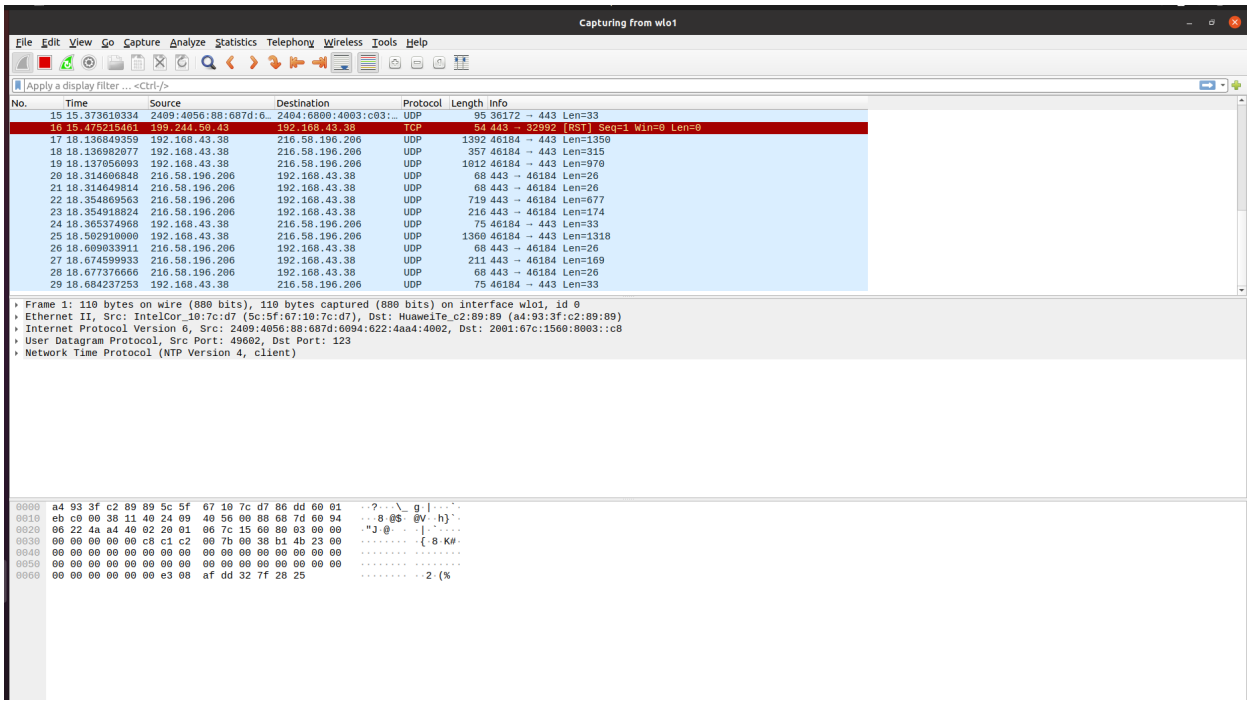
Theory:

Wireshark, formerly known as Ethereal, can be used to examine the details of traffic at a variety of levels ranging from connection-level information to the bits that make up a single packet. Packet capture can provide a network administrator with information about individual packets such as transmit time, source, destination, protocol type and header data. This information can be useful for evaluating security events and troubleshooting network security device issues.

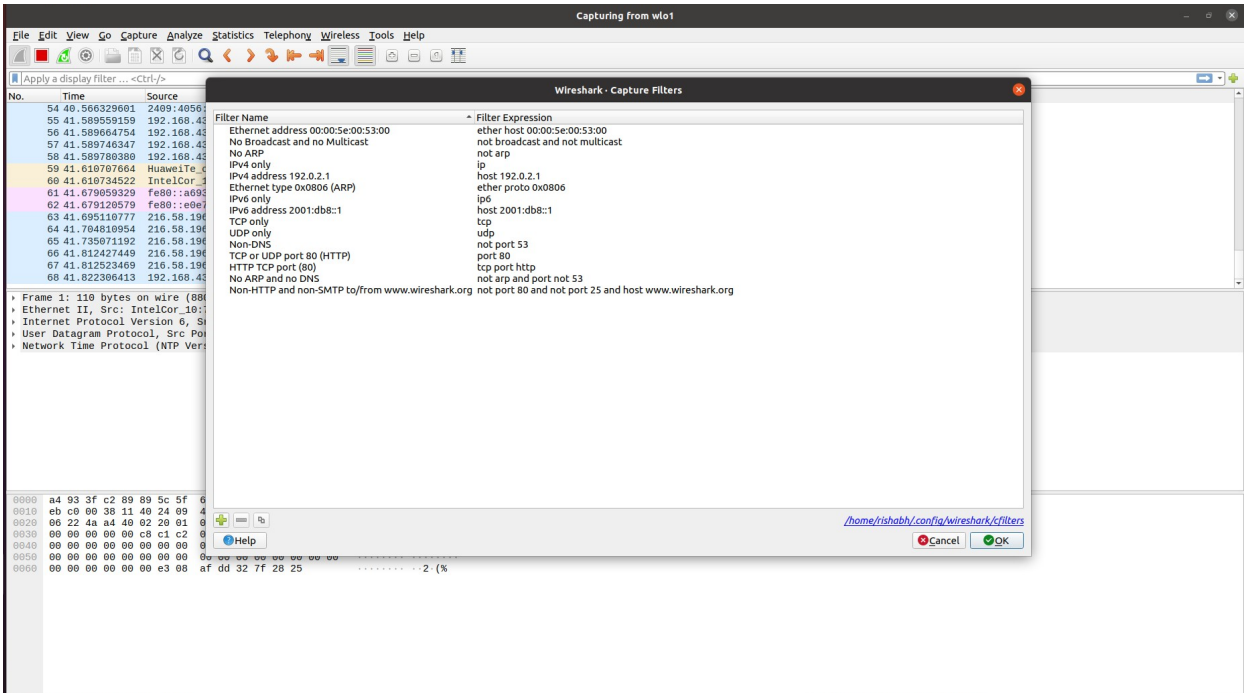
Images:

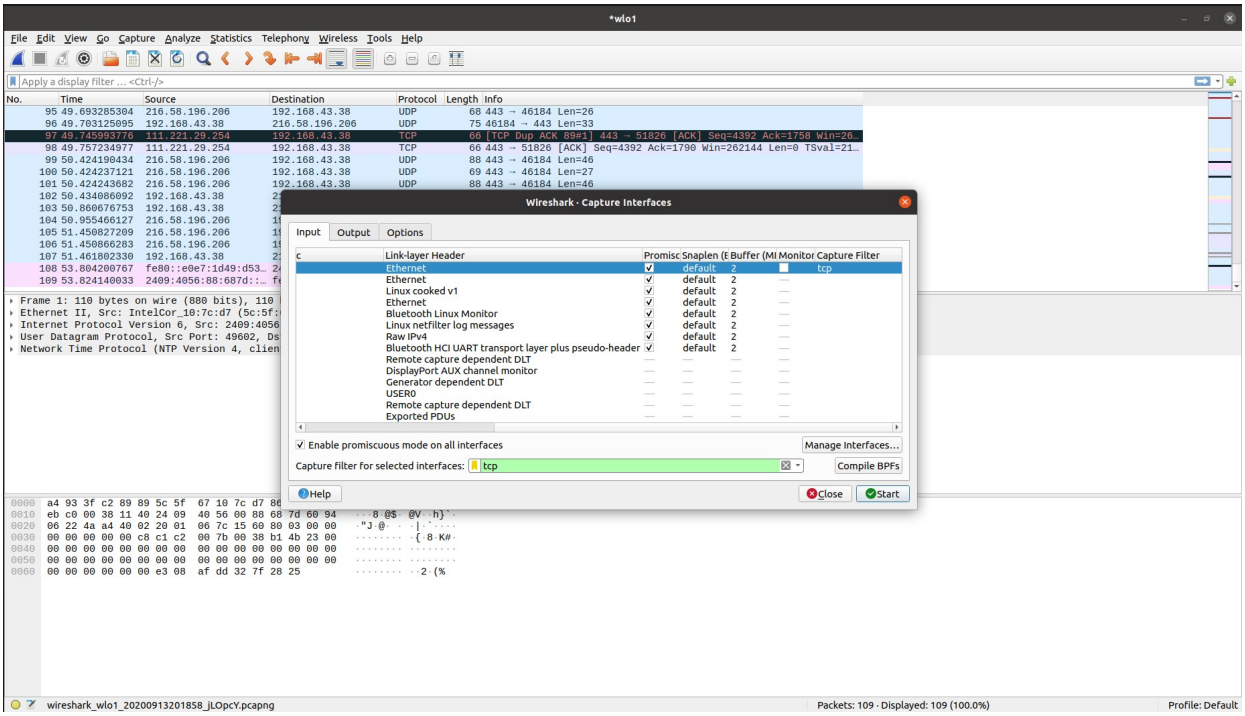
a. Interface of Wireshark:

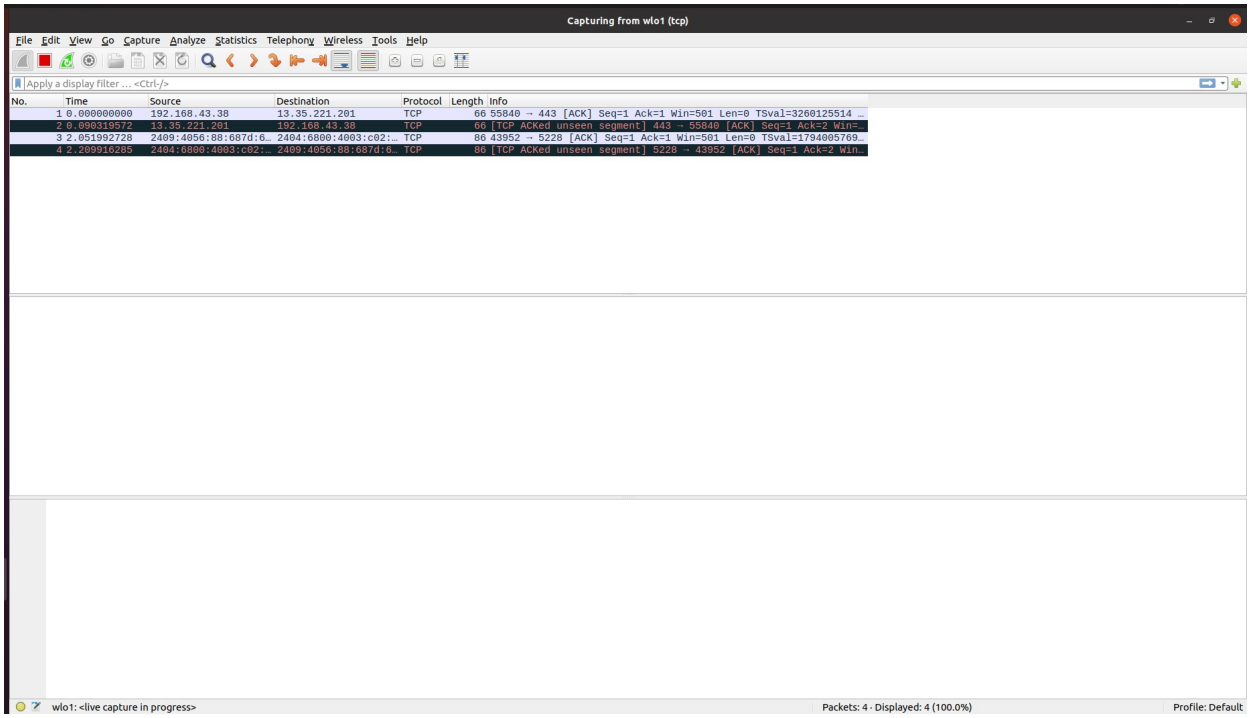




Capture packets filters in Wireshark:




*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
95 49.693285304 216.58.196.206 192.168.43.38 UDP 68 443 → 46184 Len=26
96 49.703125095 192.168.43.38 216.58.196.206 UDP 75 46184 → 443 Len=33
97 49.745993776 111.221.29.254 192.168.43.38 TCP 66 [TCP Dup ACK 89#1] 443 → 51826 [ACK] Seq=4392 Ack=1758 Win=26…
98 49.757234977 111.221.29.254 192.168.43.38 TCP 66 443 → 51826 [ACK] Seq=4392 Ack=1790 Win=262144 Len=0 TSval=21…
99 50.424190434 216.58.196.206 192.168.43.38 UDP 88 443 → 46184 Len=46
100 50.424237121 216.58.196.206 192.168.43.38 UDP 69 443 → 46184 Len=27
101 50.424243682 216.58.196.206 192.168.43.38 UDP 88 443 → 46184 Len=46
102 50.434086092 192.168.43.38 2
103 50.860676753 192.168.43.38 2
104 50.955466127 216.58.196.206 1
105 51.450827209 216.58.196.206 1
106 51.450866283 216.58.196.206 1
107 51.461802330 192.168.43.38 2
108 53.804200767 fe80::e0e7:1d49:d53… 2
109 53.824140033 2409:4056:88:687d::… f
Frame 1: 110 bytes on wire (880 bits), 110
Ethernet II, Src: IntelCor_10:7c:d7 (5c:5f:
Internet Protocol Version 6, Src: 2409:4056
User Datagram Protocol, Src Port: 49602, Ds
Network Time Protocol (NTP Version 4, clien
0000 a4 93 3f c2 89 89 5c 5f 67 10 7c d7 86
0010 eb c0 00 38 11 40 24 09 40 56 00 88 68 7d 60 94
0020 06 22 4a a4 40 02 20 01 06 7c 15 60 80 03 00 00
0030 00 00 00 00 00 c8 c1 c2 00 7b 00 38 b1 4b 23 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 e3 08 af dd 32 7f 28 25
wireshark_wlo1_20200913201858_jLOpcY.pcapng
Packets: 109 · Displayed: 109 (100.0%)
Profile: Default
Wireshark · Capture Interfaces
Input Output Options
c Link-layer Header Promisc Snaplen (E Buffer (MI Monitor Capture Filter
Ethernet default 2 tcp
Ethernet default 2
Linux cooked v1 default 2
Ethernet default 2
Bluetooth Linux Monitor default 2
Linux netfilter log messages default 2
Raw IPv4 default 2
Bluetooth HCI UART transport layer plus pseudo-header default 2
Remote capture dependent DLT
DisplayPort AUX channel monitor
Generator dependent DLT
USER0
Remote capture dependent DLT
Exported PDUs
Enable promiscuous mode on all interfaces
Manage Interfaces…
Capture filter for selected interfaces: tcp
Compile BPFs
Help
Close
Start


Capturing from wlo1 (tcp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.43.38 13.35.221.201 TCP 66 55840 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3260125514 …
2 0.098319572 13.35.221.201 192.168.43.38 TCP 66 [TCP ACKed unseen segment] 443 → 55840 [ACK] Seq=1 Ack=2 Win=…
3 2.051992728 2409:4056:88:687d:6… 2404:6800:4003:c02:… TCP 86 43952 → 5228 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1794005769…
4 2.209916285 2404:6800:4003:c02:… 2409:4056:88:687d:6… TCP 86 [TCP ACKed unseen segment] 5228 → 43952 [ACK] Seq=1 Ack=2 Win…
wlo1: <live capture in progress>
Packets: 4 · Displayed: 4 (100.0%)
Profile: Default

Display Filter :