

National Institute Of Technology, Hamirpur
Department Of Computer Science and Engineering
Sept-November 2020



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

PRACTICAL #1

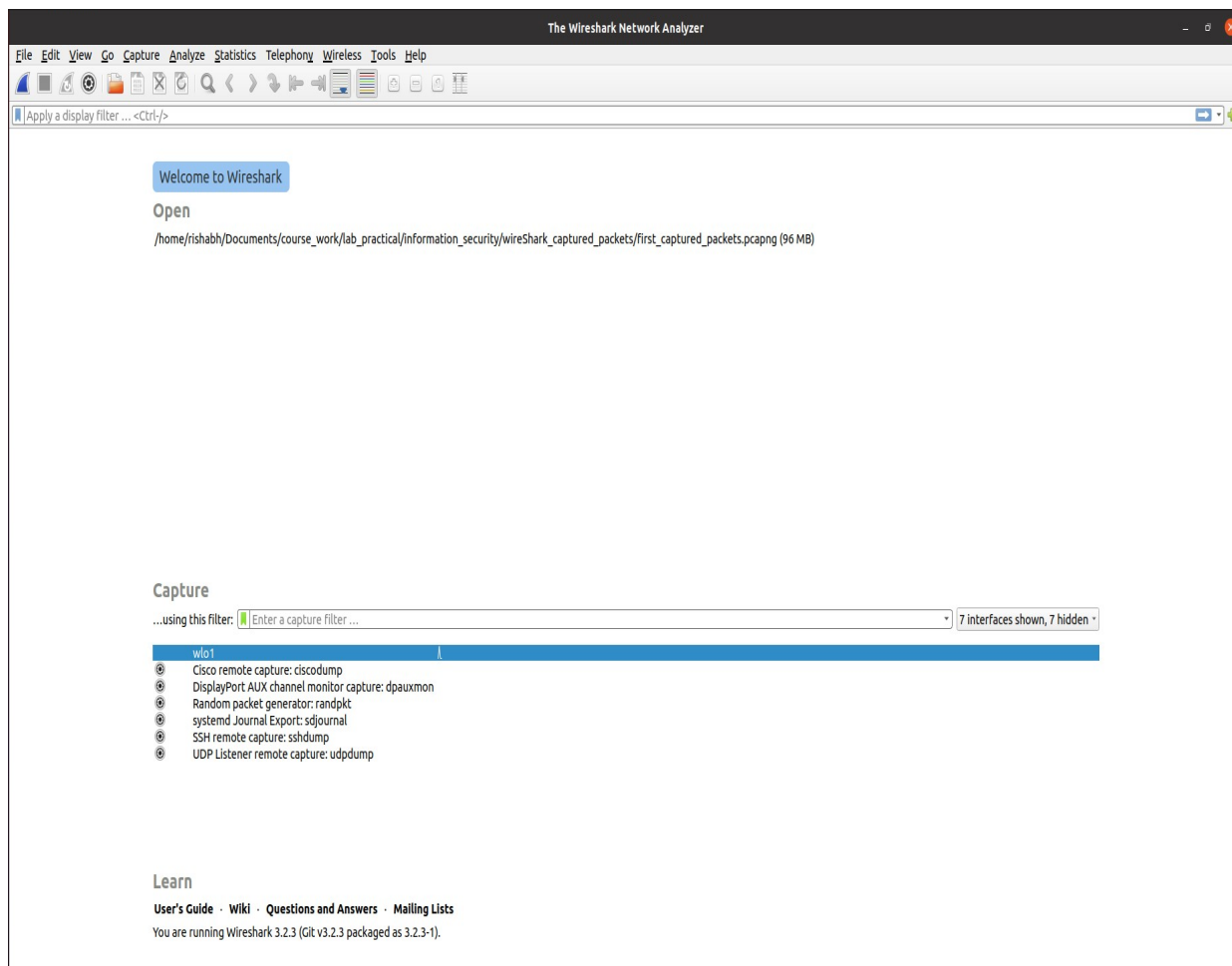
AIM : Introduction to Wireshark and implement Capture packets and Display packets in Wireshark.

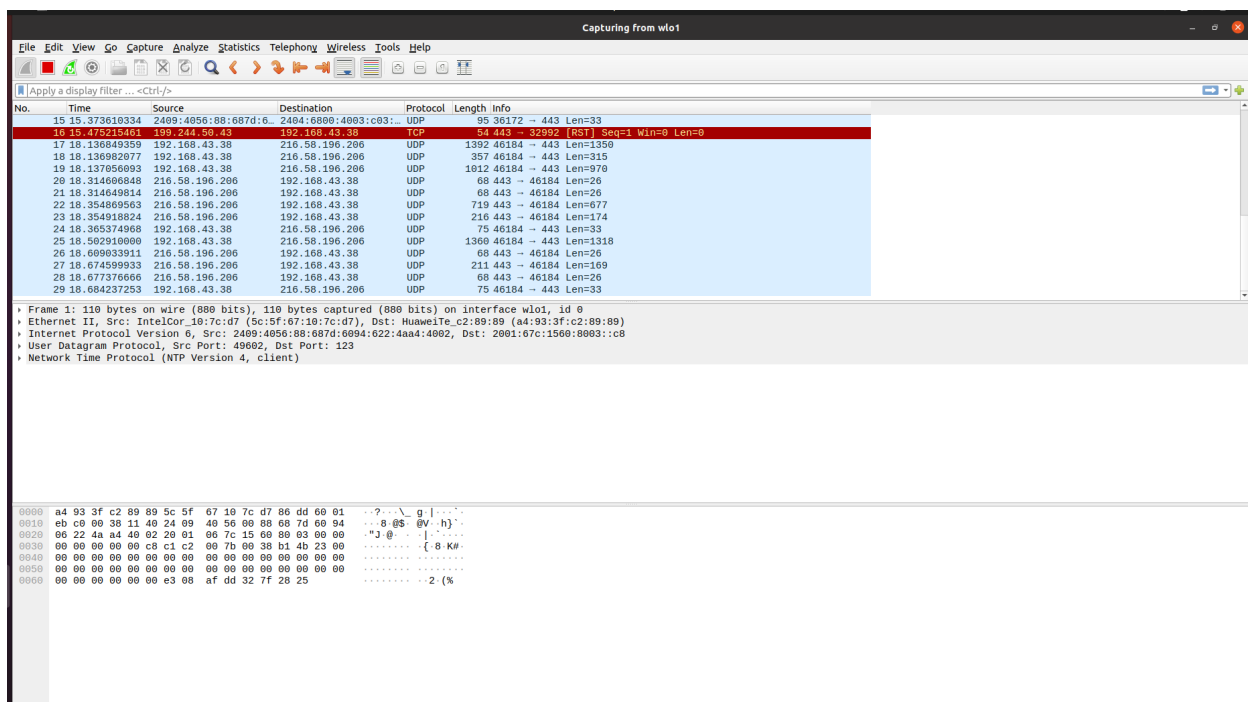
Theory:

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.

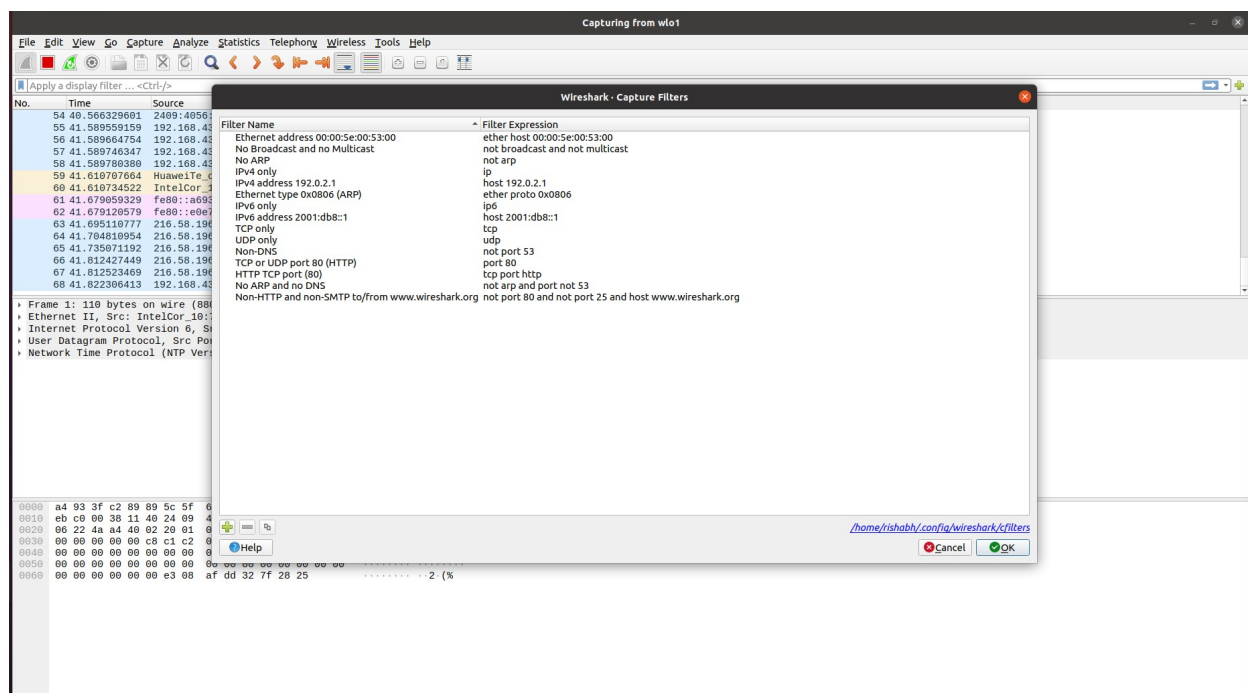
Images:

a. Interface of Wireshark:





Capture packets filters in Wireshark:



Display Filter :

Wireshark packet capture showing a TCP connection. The display filter is `tcp.flags.ack || (tcp.len >= 60)`. The packet list shows a sequence of TCP segments, including a SYN, ACK, and data segments. The packet details pane shows the structure of a TCP segment, and the packet bytes pane shows the raw data.

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=581 Len=0 TSval=3260128514
2	0.00019572	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::	2404:6800:4003:c02::	TCP	86	43952 → 5228 [ACK] Seq=1 Ack=1 Win=581 Len=0 TSval=1794005769...
4	2.209916285	2404:6800:4003:c02::	2409:4056:88:687d::	TCP	86	[TCP ACKed unseen segment] 5228 → 43952 [ACK] Seq=1 Ack=2 Win=...
5	12.118087193	13.35.221.201	192.168.43.38	TLSv1.2	165	[TCP ACKed unseen segment] , Application Data
6	12.118140015	13.35.221.201	192.168.43.38	TLSv1.2	90	[TCP ACKed unseen segment] , Application Data
7	12.118154241	13.35.221.201	192.168.43.38	TCP	66	[TCP ACKed unseen segment] 443 → 55840 [FIN, ACK] Seq=64 Ack=...
8	12.118164097	13.35.221.201	192.168.43.38	TCP	66	[TCP ACKed unseen segment] [TCP Out-Of-Order] 443 → 55840 [FI...
9	12.118163764	192.168.43.38	13.35.221.201	TCP	78	[TCP Previous segment not captured] 55840 → 443 [ACK] Seq=2 A...
10	12.118192205	192.168.43.38	13.35.221.201	TCP	66	55840 → 443 [FIN, ACK] Seq=2 Ack=50 Win=501 Len=0 TSval=32601...
11	12.1181409719	13.35.221.201	192.168.43.38	TCP	66	[TCP ACKed unseen segment] 443 → 55840 [ACK] Seq=65 Ack=3 Win=...
12	34.769402029	192.168.43.38	111.221.29.254	TCP	74	52372 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 ...
13	34.973201935	111.221.29.254	192.168.43.38	TCP	74	443 → 52372 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1376 WS...
14	34.973272011	192.168.43.38	111.221.29.254	TCP	66	52372 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=350650331...
15	34.973978018	192.168.43.38	111.221.29.254	TLSv1.2	583	Client Hello

Frame 11: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlo1, id 0
Ethernet II, Src: IntelCor_18:7c:d7 (5c:5f:67:10:7c:d7), Dst: HuaweiTe_c2:89:89 (a4:93:3f:c2:89:89)
Internet Protocol Version 4, Src: 192.168.43.38, Dst: 13.35.221.201
Transmission Control Protocol, Src Port: 55840, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000 a4 93 3f c2 89 89 5c 5f 67 10 7c d7 08 00 45 00 ...?...\ g |...E
0010 00 34 7d f4 49 00 40 06 e6 14 c9 a8 2b 20 0d 23 ...4) @ @ ...+ & #
0020 dd c9 da 20 01 b1 be 85 b3 11 d7 50 b1 02 02 10 ...P...
0030 01 f5 8e c7 00 00 01 01 08 ba c2 51 91 4a 0c 09Q J..
0040 8c da

Wireshark packet capture showing a UDP connection. The display filter is `udp.port == 443`. The packet list shows a sequence of UDP segments. The packet details pane shows the structure of a UDP segment, and the packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
1166	15.145879484	2404:6800:4002:80b::	2409:4056:88:687d::	UDP	176	443 → 54300 Len=108
1167	15.153544413	2409:4056:88:687d::	2404:6800:4002:80b::	UDP	95	54300 → 443 Len=33
1171	15.222632756	2409:4056:88:687d::	2404:6800:4002:811::	UDP	1392	45113 → 443 Len=1330
1172	15.306138323	2404:6800:4002:811::	2409:4056:88:687d::	UDP	104	443 → 45113 Len=42
1173	15.352602982	2404:6800:4002:811::	2409:4056:88:687d::	UDP	1392	443 → 45113 Len=1330
1174	15.353609701	2409:4056:88:687d::	2404:6800:4002:811::	UDP	95	45113 → 443 Len=33
1175	15.354150139	2409:4056:88:687d::	2404:6800:4002:811::	UDP	1392	45113 → 443 Len=1330
1176	15.354230176	2409:4056:88:687d::	2404:6800:4002:811::	UDP	1061	45113 → 443 Len=999
1177	15.422988610	2404:6800:4002:811::	2409:4056:88:687d::	UDP	67	443 → 45113 Len=25
1178	15.878676705	2404:6800:4002:811::	2409:4056:88:687d::	UDP	892	443 → 45113 Len=830
1179	15.878721215	2404:6800:4002:811::	2409:4056:88:687d::	UDP	277	443 → 45113 Len=215
1180	15.878744714	2404:6800:4002:811::	2409:4056:88:687d::	UDP	892	443 → 45113 Len=830
1181	15.878752392	2404:6800:4002:811::	2409:4056:88:687d::	UDP	67	443 → 45113 Len=25
1182	15.879297590	2409:4056:88:687d::	2404:6800:4002:811::	UDP	95	45113 → 443 Len=33
1183	15.879510300	2409:4056:88:687d::	2404:6800:4002:811::	UDP	95	45113 → 443 Len=33
1192	19.076745600	2409:4056:88:687d::	2404:6800:4002:80b::	UDP	1392	35432 → 443 Len=1330
1193	19.078204009	2404:6800:4002:80b::	2409:4056:88:687d::	UDP	104	443 → 35432 Len=42
1194	19.073876381	2404:6800:4002:80b::	2409:4056:88:687d::	UDP	1392	443 → 35432 Len=1330
1195	19.074801462	2409:4056:88:687d::	2404:6800:4002:80b::	UDP	95	35432 → 443 Len=33
1196	19.075476651	2409:4056:88:687d::	2404:6800:4002:80b::	UDP	1392	35432 → 443 Len=1330
1197	19.075536855	2409:4056:88:687d::	2404:6800:4002:80b::	UDP	1392	35432 → 443 Len=1330
1198	19.075564635	2409:4056:88:687d::	2404:6800:4002:80b::	UDP	265	35432 → 443 Len=203
1199	19.067810301	2404:6800:4002:80b::	2409:4056:88:687d::	UDP	87	443 → 35432 Len=25
1200	20.275120373	192.168.43.38	216.58.196.206	UDP	75	43430 → 443 Len=33
1203	20.315338467	2404:6800:4002:80b::	2409:4056:88:687d::	UDP	571	443 → 35432 Len=569
1204	20.315604428	2404:6800:4002:80b::	2409:4056:88:687d::	UDP	415	443 → 35432 Len=353
1205	20.315622217	2404:6800:4002:80b::	2409:4056:88:687d::	UDP	94	443 → 35432 Len=32
1206	20.315628520	2404:6800:4002:80b::	2409:4056:88:687d::	UDP	271	443 → 35432 Len=209
1207	20.315956248	2409:4056:88:687d::	2404:6800:4002:80b::	UDP	95	35432 → 443 Len=33
1208	20.316099556	2409:4056:88:687d::	2404:6800:4002:80b::	UDP	95	35432 → 443 Len=33
1210	20.368131886	216.58.196.206	192.168.43.38	UDP	67	443 → 43430 Len=25
1213	20.386130664	2404:6800:4002:80b::	2409:4056:88:687d::	UDP	571	443 → 35432 Len=569
1215	20.405659703	2409:4056:88:687d::	2404:6800:4002:80b::	UDP	95	35432 → 443 Len=33
1216	20.410221774	2409:4056:88:687d::	2001:4860:4802:38::	UDP	1392	49652 → 443 Len=1330
1217	20.492167105	2001:4860:4802:38::	2409:4056:88:687d::	UDP	104	443 → 49652 Len=42
1218	20.536654939	2001:4860:4802:38::	2409:4056:88:687d::	UDP	1392	443 → 49652 Len=1330
1219	20.537549215	2409:4056:88:687d::	2001:4860:4802:38::	UDP	95	49652 → 443 Len=33
1220	20.537900545	2409:4056:88:687d::	2001:4860:4802:38::	UDP	949	49652 → 443 Len=887
1221	20.622169530	2001:4860:4802:38::	2409:4056:88:687d::	UDP	87	443 → 49652 Len=25
1222	20.666710675	2001:4860:4802:38::	2409:4056:88:687d::	UDP	1095	443 → 49652 Len=1033
1223	20.668102425	2409:4056:88:687d::	2001:4860:4802:38::	UDP	111	49652 → 443 Len=49
1224	20.668449504	2001:4860:4802:38::	2409:4056:88:687d::	UDP	87	443 → 49652 Len=25
1225	20.694003420	2409:4056:88:687d::	2001:4860:4802:38::	UDP	95	49652 → 443 Len=33
1226	20.755067756	2001:4860:4802:38::	2409:4056:88:687d::	UDP	87	443 → 49652 Len=25
1227	24.024744219	2409:4056:88:687d::	2607:f8b0:4002:c03::	UDP	95	33899 → 443 Len=33
1228	24.685064616	2607:f8b0:4002:c03::	2409:4056:88:687d::	UDP	87	443 → 33899 Len=25

Frame 22: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface wlo1, id 0

Wireshark packet capture showing a UDP connection. The display filter is `udp.port == 443`. The packet list shows a sequence of UDP segments. The packet details pane shows the structure of a UDP segment, and the packet bytes pane shows the raw data.