



VIT[®]

Vellore Institute of Technology

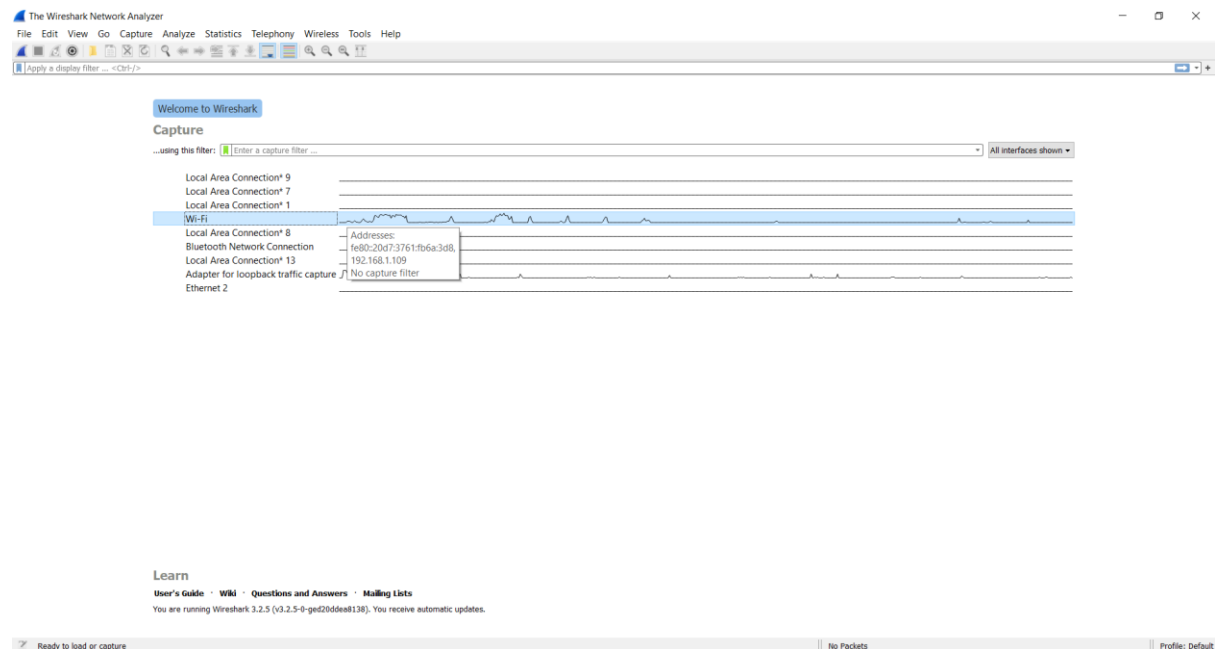
(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering
Lab Assessment-III, AUGUST 2020
B.Tech., Fall-2020-2021

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	CSE3501
COURSE NAME	INFORMATION SECURITY ANALYSIS & AUDIT
SLOT	L19+L20
FACULTY	Prof. THANDEESWARAN R.

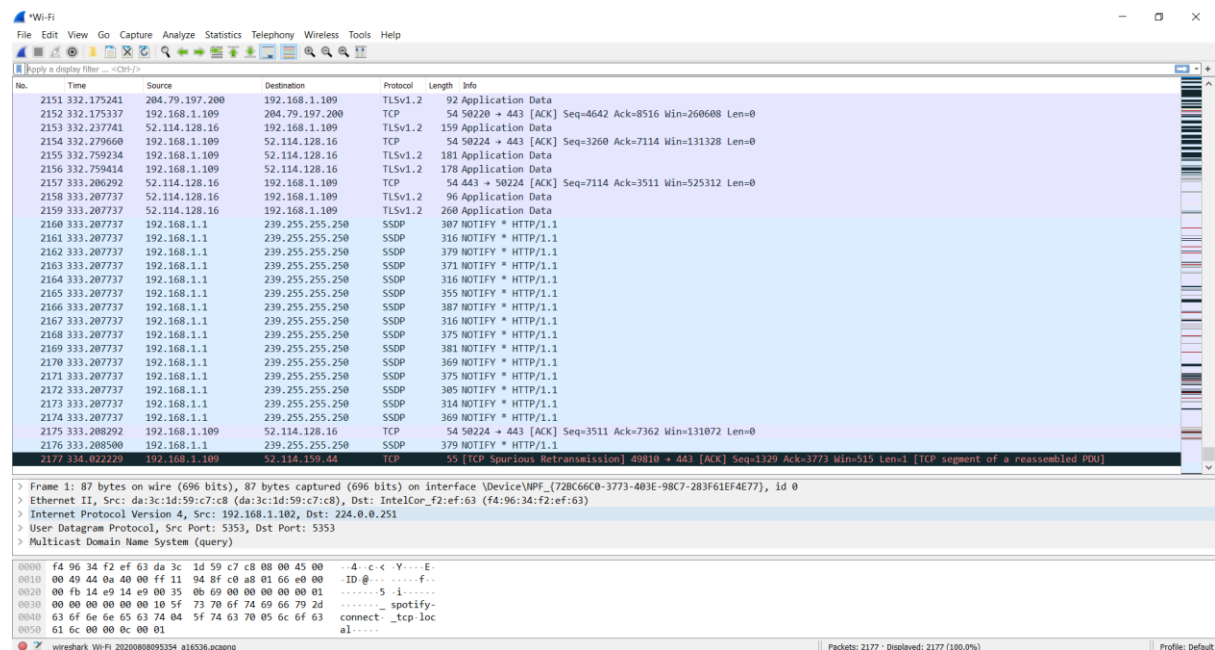
Using Wireshark, Capture live traffic, store it in a *.pcapng and perform the following tasks:

Wireshark Tool:



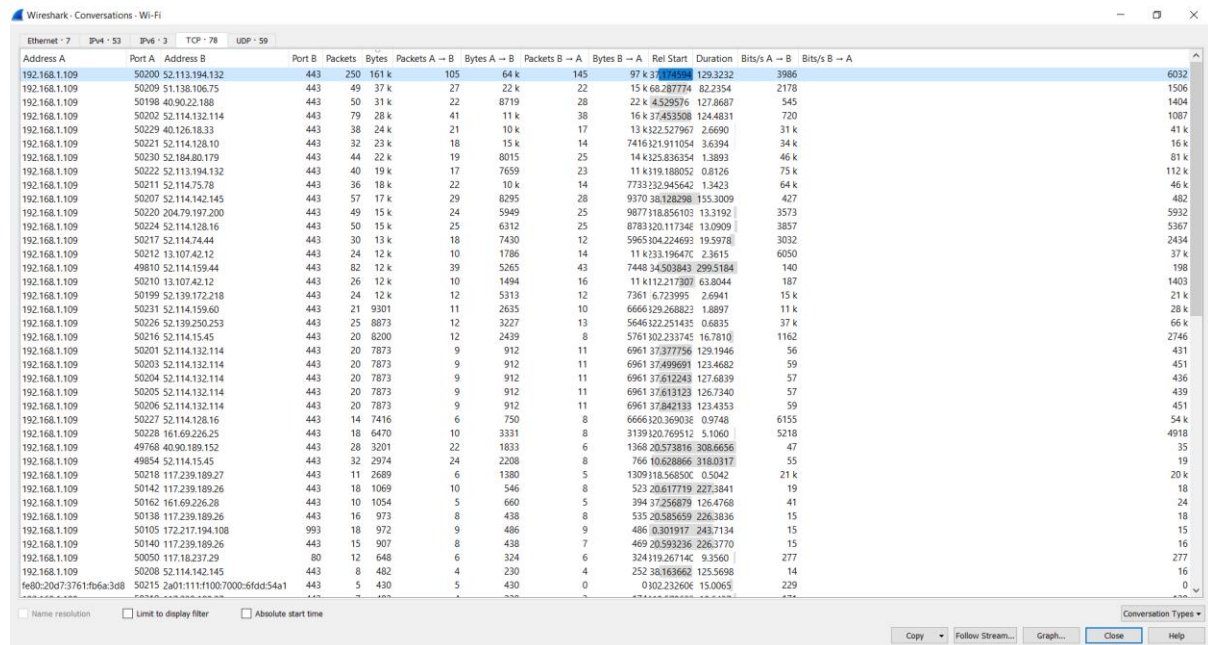
Wi-Fi:

isaa3.pcapng



1: Filter the most Active TCP connection.

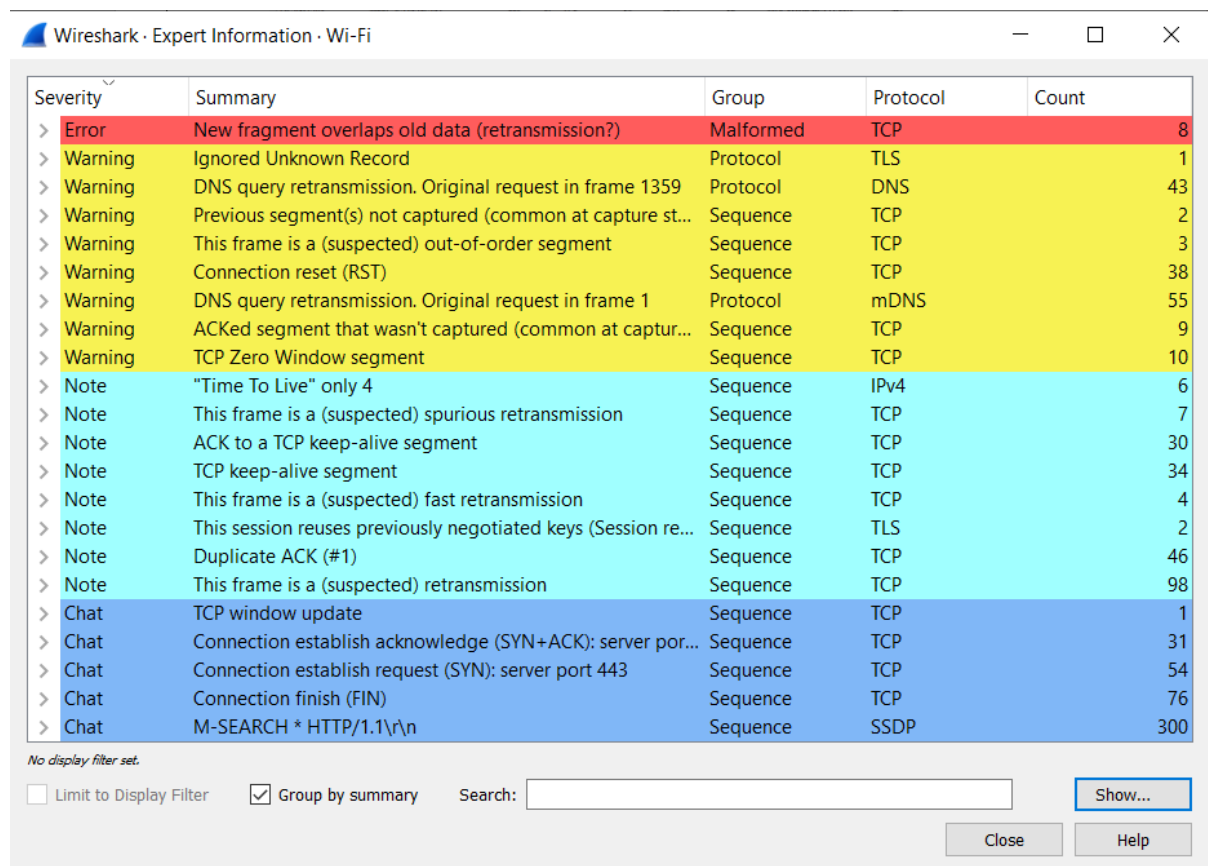
Go to **Statistics** → **Conversations** → **TCP**; then **sort by Bytes** in descending order
192.168.1.109 (Address A) has the most active TCP connection with 52.113.194.132 (Address B).



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.109	50200	52.113.194.132	443	250	161 k	105	64 k	145	97 k	37.177594	129.3232	3986	6032
192.168.1.109	50209	51.138.106.75	443	49	37 k	27	22 k	22	15 k	68.287774	82.2354	2178	1506
192.168.1.109	50198	40.90.22.188	443	50	31 k	22	8719	28	22 k	4.529576	127.8687	545	1404
192.168.1.109	50202	52.114.132.114	443	79	28 k	41	11 k	38	16 k	37.453598	124.4831	720	1087
192.168.1.109	50229	40.126.18.33	443	38	24 k	21	10 k	17	13 k	322.527967	2.6690	31 k	41 k
192.168.1.109	50221	52.114.128.10	443	32	23 k	18	15 k	14	7416	321.911054	3.6394	34 k	16 k
192.168.1.109	50230	52.184.80.179	443	44	22 k	19	8015	25	14 k	325.836354	1.3893	46 k	81 k
192.168.1.109	50222	52.113.194.132	443	40	19 k	17	7659	23	11 k	319.188052	0.8126	75 k	112 k
192.168.1.109	50211	52.114.75.78	443	36	18 k	22	10 k	14	7733	332.945642	1.3423	64 k	46 k
192.168.1.109	50209	52.114.142.145	443	57	17 k	29	8295	28	9370	38.128298	155.3009	427	482
192.168.1.109	50220	204.79.197.200	443	49	15 k	24	5949	25	9877	318.85103	13.3102	3573	5932
192.168.1.109	50224	52.114.128.16	443	50	15 k	25	6312	25	8783	320.117346	13.0909	3857	5367
192.168.1.109	50217	52.114.74.44	443	30	13 k	18	7430	12	5965	304.224693	19.5978	3032	2434
192.168.1.109	50212	13.107.42.12	443	24	12 k	10	1786	14	11 k	323.196470	2.3615	6050	37 k
192.168.1.109	49810	52.114.159.44	443	82	12 k	39	5265	43	7448	34.503843	299.5184	140	198
192.168.1.109	50210	13.107.42.12	443	26	12 k	10	1494	16	11 k	112.217307	63.8044	187	1403
192.168.1.109	50199	52.139.172.218	443	24	12 k	12	5313	12	7361	6.723995	2.6941	15 k	21 k
192.168.1.109	50231	52.114.159.60	443	21	9301	11	2635	10	6666	329.268022	1.8897	11 k	28 k
192.168.1.109	50226	52.139.250.253	443	25	8873	12	3227	13	5646	322.251435	0.6835	37 k	66 k
192.168.1.109	50216	52.114.15.45	443	20	8200	12	2439	8	5761	302.233745	16.7810	1162	2746
192.168.1.109	50201	52.114.132.114	443	20	7873	9	912	11	6961	37.377756	129.1946	56	431
192.168.1.109	50203	52.114.132.114	443	20	7873	9	912	11	6961	37.499691	123.4682	59	451
192.168.1.109	50204	52.114.132.114	443	20	7873	9	912	11	6961	37.612243	127.6839	57	436
192.168.1.109	50205	52.114.132.114	443	20	7873	9	912	11	6961	37.613123	126.7340	57	439
192.168.1.109	50206	52.114.132.114	443	20	7873	9	912	11	6961	37.842133	125.4353	59	451
192.168.1.109	50227	52.114.128.16	443	14	7416	6	750	8	6666	320.369036	0.9748	6155	54 k
192.168.1.109	50228	161.69.226.25	443	18	6470	10	3331	8	3139	320.769512	5.1060	5218	4918
192.168.1.109	49768	40.90.189.152	443	28	3201	22	1833	6	1368	20.573816	308.6656	47	35
192.168.1.109	49854	52.114.15.45	443	32	2974	24	2208	8	766	10.628866	318.0317	55	19
192.168.1.109	50218	117.239.189.27	443	11	2689	6	1380	5	1309	318.565500	0.5042	21 k	20 k
192.168.1.109	50142	117.239.189.26	443	18	1069	10	546	8	523	20.617719	227.3841	19	18
192.168.1.109	50162	161.69.236.28	443	10	1054	5	660	5	394	37.256879	126.4768	41	24
192.168.1.109	50138	117.239.189.26	443	16	973	8	438	8	535	20.585659	226.3836	15	18
192.168.1.109	50105	172.217.194.108	993	18	972	9	486	9	486	0.301917	243.7134	15	15
192.168.1.109	50140	117.239.189.26	443	15	907	8	438	7	469	20.593236	226.3770	15	16
192.168.1.109	50050	117.18.237.29	80	12	648	6	324	6	324	319.267140	9.3560	277	277
192.168.1.109	50208	52.114.142.145	443	8	482	4	230	4	252	38.163662	125.5698	14	16
fe80:20d7:3761fb6a:3d8	50215	2a01:1111:f100:7000:6fdd:54a1	443	5	430	5	430	0	0	102.232606	15.0065	229	229

2: Analyse TCP Errors and prepare a detailed report.

Go to **Analyse** → **Expert Information**



Severity	Summary	Group	Protocol	Count
Error	New fragment overlaps old data (retransmission?)	Malformed	TCP	8
Warning	Ignored Unknown Record	Protocol	TLS	1
Warning	DNS query retransmission. Original request in frame 1359	Protocol	DNS	43
Warning	Previous segment(s) not captured (common at capture st...	Sequence	TCP	2
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	3
Warning	Connection reset (RST)	Sequence	TCP	38
Warning	DNS query retransmission. Original request in frame 1	Protocol	mDNS	55
Warning	ACKed segment that wasn't captured (common at captur...	Sequence	TCP	9
Warning	TCP Zero Window segment	Sequence	TCP	10
Note	"Time To Live" only 4	Sequence	IPv4	6
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	7
Note	ACK to a TCP keep-alive segment	Sequence	TCP	30
Note	TCP keep-alive segment	Sequence	TCP	34
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	4
Note	This session reuses previously negotiated keys (Session re...	Sequence	TLS	2
Note	Duplicate ACK (#1)	Sequence	TCP	46
Note	This frame is a (suspected) retransmission	Sequence	TCP	98
Chat	TCP window update	Sequence	TCP	1
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	31
Chat	Connection establish request (SYN): server port 443	Sequence	TCP	54
Chat	Connection finish (FIN)	Sequence	TCP	76
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	300

3: Identify the user agents are being used on your network.

Filter: **http.user_agent**

Google Chrome is using the network.

The image shows a Wireshark packet capture window with the filter 'http.user_agent' applied. The packet list shows several HTTP GET requests from 192.168.1.109 to 103.138.234.220. The packet details pane shows the selected packet (No. 524) with the following information:

- Frame 167: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF... id 0
- Ethernet II, Src: IntelCor-f2:ef:63 (fa:96:34:f2:ef:63), Dst: IPvmcast-7f:ff:fa (01:00:5e:7f:ff:fa)
- Internet Protocol Version 4, Src: 192.168.1.109, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 57700, Dst Port: 1900
- Simple Service Discovery Protocol

The packet bytes pane shows the raw data of the packet, which is a SSDP message. The packet is identified as 'Google Chrome/8'.

4: Filter background network noise.

Filter: **!(amp or icmp or dns)**

The image shows a Wireshark packet capture window with the filter '!(amp or icmp or dns)' applied. The packet list shows various network traffic, including DNS queries, SSDP messages, and ICMP Echo (ping) requests. The packet details pane shows the selected packet (No. 1) with the following information:

- Frame 1: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF... id 0
- Ethernet II, Src: da:3c:1d:59:c7:c8 (da:3c:1d:59:c7:c8), Dst: IntelCor-f2:ef:63 (fa:96:34:f2:ef:63)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 224.0.0.251
- User Datagram Protocol, Src Port: 5353, Dst Port: 5353
- Multicast Domain Name System (query)

The packet bytes pane shows the raw data of the packet, which is a DNS query. The packet is identified as 'Standard query 0x0000 PTR _spotify-connect._tcp.local, "Q?" question'.

5: Detect Possible DDoS attacks.

Filter: **tcp.flags.syn == 1 and tcp.flags.ack == 0**

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like opening files, saving, and analyzing. The main pane is divided into three sections: the top section shows the packet list with columns for No., Time, Source, Destination, Protocol, Length, and Info; the middle section shows the packet details for the selected packet (No. 1521); and the bottom section shows the packet bytes in hexadecimal and ASCII. The filter bar at the top of the packet list shows the active filter: **tcp.flags.syn == 1 and tcp.flags.ack == 0**. The packet list contains numerous entries, mostly TCP SYN packets from source 192.168.1.109 to destination 52.114.132.114. Some packets are marked as retransmissions. The details pane for packet 1521 shows it is an ICMPv6 message of type 'Destination Unreachable' with code 'no route to destination'. The packet bytes pane shows the raw data of the selected packet.
