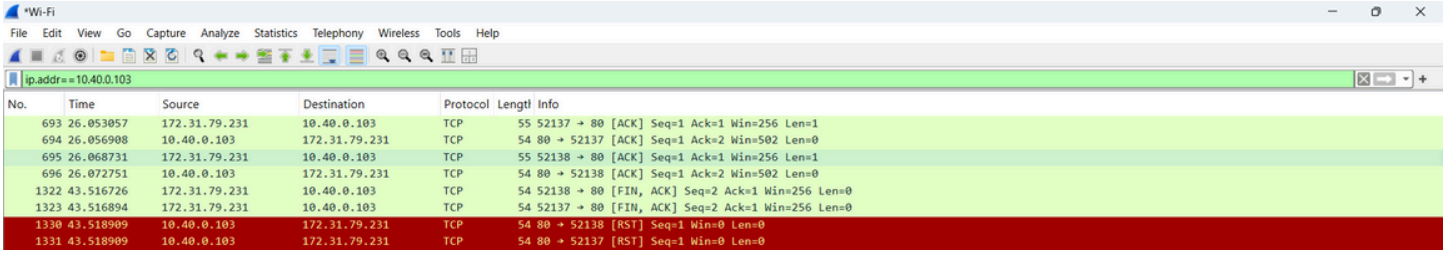
Lab Assignment 4 CyberSecurity

Name : Anubhav Tandon

Roll Number : B22CS013

Without http



No.	Time	Source	Destination	Protocol	Length	Info
693	26.053057	172.31.79.231	10.40.0.103	TCP	55	52137 → 80 [ACK] Seq=1 Ack=1 Win=256 Len=1
694	26.056908	10.40.0.103	172.31.79.231	TCP	54	80 → 52137 [ACK] Seq=1 Ack=2 Win=502 Len=0
695	26.068731	172.31.79.231	10.40.0.103	TCP	55	52138 → 80 [ACK] Seq=1 Ack=1 Win=256 Len=1
696	26.072751	10.40.0.103	172.31.79.231	TCP	54	80 → 52138 [ACK] Seq=1 Ack=2 Win=502 Len=0
1322	43.516726	172.31.79.231	10.40.0.103	TCP	54	52138 → 80 [FIN, ACK] Seq=2 Ack=1 Win=256 Len=0
1323	43.516894	172.31.79.231	10.40.0.103	TCP	54	52137 → 80 [FIN, ACK] Seq=2 Ack=1 Win=256 Len=0
1330	43.518909	10.40.0.103	172.31.79.231	TCP	54	80 → 52138 [RST] Seq=1 Win=0 Len=0
1331	43.518909	10.40.0.103	172.31.79.231	TCP	54	80 → 52137 [RST] Seq=1 Win=0 Len=0

with http

No.	Time	Source	Destination	Protocol	Length	Info
282	9.171973	172.31.79.231	10.40.0.103	HTTP	671	GET /login_process.html?username=test1&password=test1 HTTP/1.1
285	9.175745	10.40.0.103	172.31.79.231	HTTP	766	HTTP/1.1 200 OK (text/html)
375	9.468764	172.31.79.231	10.40.0.103	HTTP	673	GET /success.html HTTP/1.1
377	9.473502	10.40.0.103	172.31.79.231	HTTP	836	HTTP/1.1 200 OK (text/html)

With HTTPS

518	12.292759	172.31.79.231	142.250.194.42	TLSv1.3	93	Application Data
519	12.306104	142.250.194.42	172.31.79.231	TCP	54	443 → 52803 [ACK] Seq=27324 Ack=2831 Win=267520 Len=0
520	12.310053	104.18.36.252	172.31.79.231	TCP	54	443 → 50458 [ACK] Seq=25 Ack=29 Win=19 Len=0
521	12.342153	54.170.196.176	172.31.79.231	TCP	54	443 → 52800 [ACK] Seq=7097 Ack=4723 Win=38400 Len=0
522	12.389072	172.31.10.60	255.255.255.255	DB-LSP…	239	Dropbox LAN sync Discovery Protocol, JSON
523	12.389922	172.31.10.60	255.255.255.255	DB-LSP…	239	Dropbox LAN sync Discovery Protocol, JSON
524	12.389922	172.31.10.60	255.255.255.255	DB-LSP…	239	Dropbox LAN sync Discovery Protocol, JSON
525	12.389922	172.31.10.60	255.255.255.255	DB-LSP…	239	Dropbox LAN sync Discovery Protocol, JSON
526	12.389970	172.31.10.60	172.31.63.255	DB-LSP…	239	Dropbox LAN sync Discovery Protocol, JSON
527	12.391198	172.31.10.60	255.255.255.255	DB-LSP…	239	Dropbox LAN sync Discovery Protocol, JSON
528	12.423234	52.212.50.192	172.31.79.231	TCP	58	443 → 52809 [SYN, ACK] Seq=0 Ack=1 Win=35844 Len=0 MSS=1460
529	12.423381	172.31.79.231	52.212.50.192	TCP	54	52809 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
530	12.424139	172.31.79.231	52.212.50.192	TCP	1514	52809 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1460 [TCP PDU reassembled in 531]
531	12.424139	172.31.79.231	52.212.50.192	TLSv1.3	384	Client Hello (SNI=logs.netflix.com)
532	12.427243	52.212.50.192	172.31.79.231	TCP	54	443 → 52809 [ACK] Seq=1 Ack=1461 Win=65535 Len=0
533	12.478980	52.212.50.192	172.31.79.231	TCP	66	443 → 52809 [ACK] Seq=1 Ack=1791 Win=65535 Len=0 SLE=1 SRE=1791
534	12.492060	172.31.0.91	172.31.63.255	UDP	77	43133 → 15600 Len=35
535	12.594693	172.31.18.103	172.31.63.255	NBNS	92	Name query NB LAPTOP-1T3I76M6<1c>
536	12.594693	172.31.53.69	255.255.255.255	UDP	56	57880 → 3289 Len=14
537	12.594693	172.31.53.69	255.255.255.255	UDP	70	57876 → 22222 Len=28
538	12.594693	172.31.53.69	172.31.63.255	UDP	70	57873 → 22222 Len=28
539	12.594693	172.31.53.69	255.255.255.255	UDP	125	10004 → 10004 Len=83
540	12.594693	172.31.53.69	172.31.63.255	UDP	56	57881 → 3289 Len=14
541	12.594693	172.31.53.69	172.31.63.255	UDP	70	57877 → 22222 Len=28
542	12.594928	172.31.53.69	255.255.255.255	UDP	56	57882 → 3289 Len=14
543	12.594928	172.31.53.69	255.255.255.255	UDP	56	57883 → 3289 Len=14
544	12.594959	172.31.53.69	255.255.255.255	UDP	70	57874 → 22222 Len=28
545	12.594959	172.31.53.69	255.255.255.255	UDP	70	57875 → 22222 Len=28
546	12.594994	172.31.53.69	255.255.255.255	UDP	125	10004 → 10004 Len=83
547	12.594994	172.31.53.69	255.255.255.255	UDP	70	57878 → 22222 Len=28
548	12.596761	172.31.53.69	255.255.255.255	UDP	70	57879 → 22222 Len=28
549	12.596761	172.31.53.69	255.255.255.255	UDP	125	10004 → 10004 Len=83
550	12.596761	172.31.53.69	255.255.255.255	UDP	125	10004 → 10004 Len=83
551	12.596761	172.31.52.12	172.31.63.255	UDP	82	57621 → 57621 Len=40
552	12.602747	52.212.50.192	172.31.79.231	TLSv1.3	1514	Server Hello, Change Cipher Spec

The login credentials are not shared via plaintext in the packets when i log into **www.netflix.com** as can be seen in the screenshot. The username and password are encrypted in https requests to ensure security.

Credential Exposure in HTTP: The Wireshark capture shows that when logging into the HTTP server, the username (test1) and password (test1) are sent in plaintext within the URL. This makes it easy for attackers to intercept and steal credentials, which are test1 for username and password in this case.

TCP Communication and Connection Termination: The second screenshot displays TCP packets, including the handshake, data transfer, and connection termination. The presence of RST packets suggests an abrupt connection closure, which could indicate network issues or intentional termination.

2. The TCP handshake delay refers to the duration required for the three-way handshake process (SYN → SYN-ACK → ACK) to finalize before data transfer can commence. An extended handshake delay results in increased network latency, which can hinder communication and negatively impact real-time applications, web browsing, and overall system performance.

TCP Handshake Delay & Impact – The delay in completing the three-way handshake (SYN → SYN-ACK → ACK) increases network latency and slows communication.

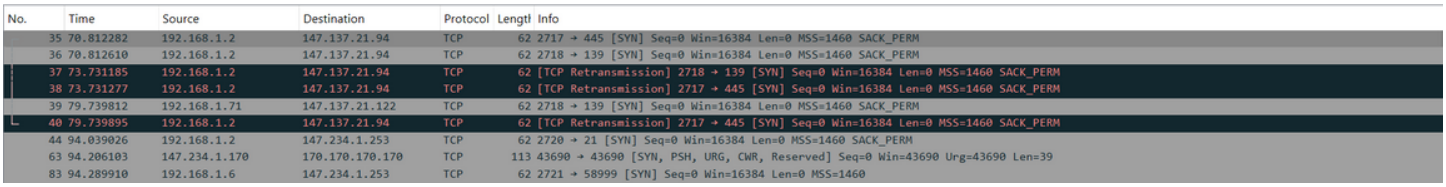
Measuring TCP Delay in Wireshark— Using filters like tcp.flags.syn == 1, measure time between SYN and SYN-ACK for network congestion, and SYN-ACK to ACK for client-side delay.

Analyzing Application Delays—Use http.request and || http.response for HTTP request-response time and DNS filter for DNS query-response time to diagnose slow performance.

Optimizing Performance—Reduce handshake delays with Keep-Alive, optimize HTTP with compression/CDNs, and speed up DNS with caching.

3 . <u>SYN Flood Detection</u>

tcp.flags.syn == 1 and tcp.flags.ack == 0

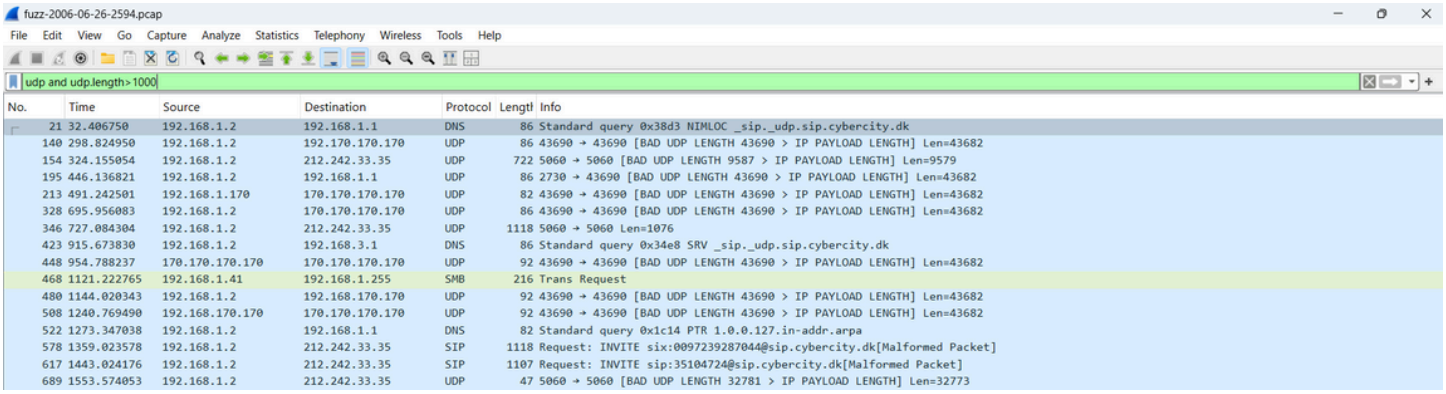


No.	Time	Source	Destination	Protocol	Length	Info
35	70.812282	192.168.1.2	147.137.21.94	TCP	62	2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
36	70.812610	192.168.1.2	147.137.21.94	TCP	62	2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
37	73.731185	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
38	73.731277	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
39	79.739812	192.168.1.71	147.137.21.122	TCP	62	2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
40	79.739895	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
44	94.039026	192.168.1.2	147.234.1.253	TCP	62	2720 → 21 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
63	94.206103	147.234.1.170	170.170.170.170	TCP	113	43690 → 43690 [SYN, PSH, URG, CWR, Reserved] Seq=0 Win=43690 Urg=43690 Len=39
83	94.289910	192.168.1.6	147.234.1.253	TCP	62	2721 → 58999 [SYN] Seq=0 Win=16384 Len=0 MSS=1460

Unusually high number of SYN packets without corresponding ACKs

<u>UDP Flood Detection</u>

udp and udp.length>1000



fuzz-2006-06-26-2594.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp and udp.length>1000

No.	Time	Source	Destination	Protocol	Length	Info
21	32.406750	192.168.1.2	192.168.1.1	DNS	86	Standard query 0x38d3 NIMLOC _sip._udp.sip.cybercity.dk
140	298.824950	192.168.1.2	192.170.170.170	UDP	86	43690 → 43690 [BAD UDP LENGTH 43690 > IP PAYLOAD LENGTH] Len=43682
154	324.155054	192.168.1.2	212.242.33.35	UDP	722	5060 → 5060 [BAD UDP LENGTH 9587 > IP PAYLOAD LENGTH] Len=9579
195	446.136821	192.168.1.2	192.168.1.1	UDP	86	2730 → 43690 [BAD UDP LENGTH 43690 > IP PAYLOAD LENGTH] Len=43682
213	491.242501	192.168.1.170	170.170.170.170	UDP	82	43690 → 43690 [BAD UDP LENGTH 43690 > IP PAYLOAD LENGTH] Len=43682
328	695.956083	192.168.1.2	170.170.170.170	UDP	86	43690 → 43690 [BAD UDP LENGTH 43690 > IP PAYLOAD LENGTH] Len=43682
346	727.084304	192.168.1.2	212.242.33.35	UDP	1118	5060 → 5060 Len=1076
423	915.673830	192.168.1.2	192.168.3.1	DNS	86	Standard query 0x34e8 SRV _sip._udp.sip.cybercity.dk
448	954.788237	170.170.170.170	170.170.170.170	UDP	92	43690 → 43690 [BAD UDP LENGTH 43690 > IP PAYLOAD LENGTH] Len=43682
468	1121.222765	192.168.1.41	192.168.1.255	SMB	216	Trans Request
480	1144.020343	192.168.1.2	192.168.170.170	UDP	92	43690 → 43690 [BAD UDP LENGTH 43690 > IP PAYLOAD LENGTH] Len=43682
508	1240.769490	192.168.170.170	170.170.170.170	UDP	92	43690 → 43690 [BAD UDP LENGTH 43690 > IP PAYLOAD LENGTH] Len=43682
522	1273.347038	192.168.1.2	192.168.1.1	DNS	82	Standard query 0x1c14 PTR 1.0.0.127.in-addr.arpa
578	1359.023578	192.168.1.2	212.242.33.35	SIP	1118	Request: INVITE sip:0097239287044@sip.cybercity.dk[Malformed Packet]
617	1443.024176	192.168.1.2	212.242.33.35	SIP	1107	Request: INVITE sip:35104724@sip.cybercity.dk[Malformed Packet]
689	1553.574053	192.168.1.2	212.242.33.35	UDP	47	5060 → 5060 [BAD UDP LENGTH 32781 > IP PAYLOAD LENGTH] Len=32773

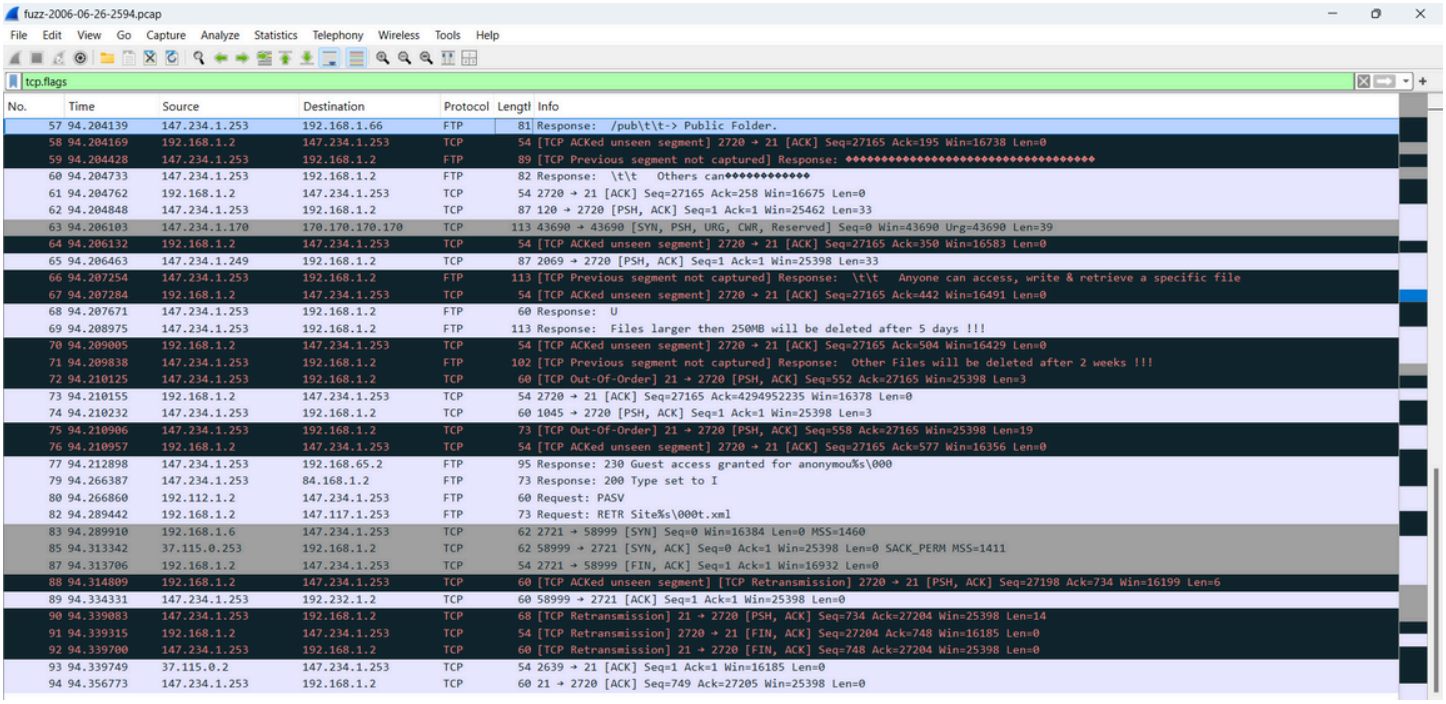
massive amounts of UDP packets to specific ports

ICMP Flood Detection

No icmp flood attack

Analyzing Attack Type

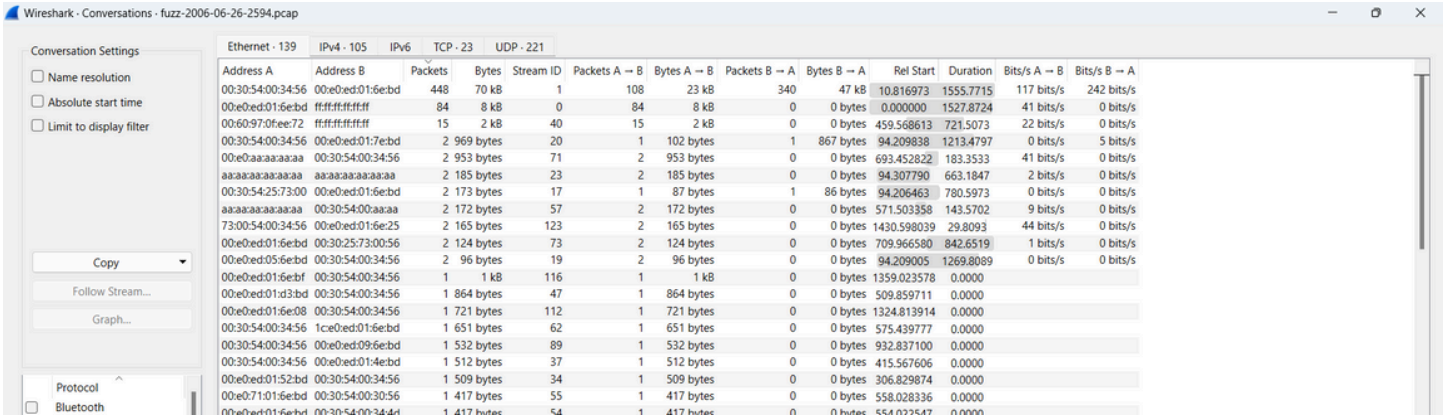
tcp.flags



Top talkers on the basis of number of packets

Address A : 00:30:54:00:34:56

Address B : 00:e0:ed:01:6e:bd



Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00:30:54:00:34:56	00:e0:ed:01:6e:bd	448	70 kB	1	108	23 kB	340	47 kB	10.816973	1555.7715	117 bits/s	242 bits/s
00:e0:ed:01:6e:bd	ff:ff:ff:ff:ff:ff	84	8 kB	0	84	8 kB	0	0 bytes	0.000000	1527.8724	41 bits/s	0 bits/s
00:60:97:0f:ee:72	ff:ff:ff:ff:ff:ff	15	2 kB	40	15	2 kB	0	0 bytes	459.568613	721.5073	22 bits/s	0 bits/s
00:30:54:00:34:56	00:e0:ed:01:7e:bd	2	969 bytes	20	1	102 bytes	1	867 bytes	94.209838	1213.4797	0 bits/s	5 bits/s
00:e0:aa:aa:aa:aa	00:30:54:00:34:56	2	953 bytes	71	2	953 bytes	0	0 bytes	693.452822	183.3533	41 bits/s	0 bits/s
aa:aa:aa:aa:aa:aa	aa:aa:aa:aa:aa:aa	2	185 bytes	23	2	185 bytes	0	0 bytes	94.307790	663.1847	2 bits/s	0 bits/s
00:30:54:25:73:00	00:e0:ed:01:6e:bd	2	173 bytes	17	1	87 bytes	1	86 bytes	94.206463	780.5973	0 bits/s	0 bits/s
aa:aa:aa:aa:aa:aa	00:30:54:00:aa:aa	2	172 bytes	57	2	172 bytes	0	0 bytes	571.503358	143.5702	9 bits/s	0 bits/s
73:00:54:00:34:56	00:e0:ed:01:6e:25	2	165 bytes	123	2	165 bytes	0	0 bytes	1430.598039	29.8093	44 bits/s	0 bits/s
00:e0:ed:01:6e:bd	00:30:25:73:00:56	2	124 bytes	73	2	124 bytes	0	0 bytes	709.966580	842.6519	1 bits/s	0 bits/s
00:e0:ed:05:6e:bd	00:30:54:00:34:56	2	96 bytes	19	2	96 bytes	0	0 bytes	94.209005	1269.8089	0 bits/s	0 bits/s
00:e0:ed:01:6e:bf	00:30:54:00:34:56	1	1 kB	116	1	1 kB	0	0 bytes	1359.023578	0.0000		
00:e0:ed:01:d3:bd	00:30:54:00:34:56	1	864 bytes	47	1	864 bytes	0	0 bytes	509.859711	0.0000		
00:e0:ed:01:6e:08	00:30:54:00:34:56	1	721 bytes	112	1	721 bytes	0	0 bytes	1324.813914	0.0000		
00:30:54:00:34:56	1c:e0:ed:01:6e:bd	1	651 bytes	62	1	651 bytes	0	0 bytes	575.439777	0.0000		
00:30:54:00:34:56	00:e0:ed:09:6e:bd	1	532 bytes	89	1	532 bytes	0	0 bytes	932.837100	0.0000		
00:30:54:00:34:56	00:e0:ed:01:4e:bd	1	512 bytes	37	1	512 bytes	0	0 bytes	415.567606	0.0000		
00:e0:ed:01:52:bd	00:30:54:00:34:56	1	509 bytes	34	1	509 bytes	0	0 bytes	306.829874	0.0000		
00:e0:71:01:6e:bd	00:30:54:00:30:56	1	417 bytes	55	1	417 bytes	0	0 bytes	558.028336	0.0000		
00:e0:ed:01:6e:bd	00:30:54:00:34:4d	1	417 bytes	54	1	417 bytes	0	0 bytes	554.023547	0.0000		

Top IP Addresses with unusally higher traffic are given below

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source IPv4 Addresses	606				0.0004	100%	0.3000	94.154
192.168.1.2	424				0.0003	69.97%	0.0900	94.154
192.168.1.1	49				0.0000	8.09%	0.0200	1238.569
212.242.33.35	30				0.0000	4.95%	0.0200	415.542
147.234.1.253	24				0.0000	3.96%	0.1900	94.154
192.168.1.41	13				0.0000	2.15%	0.0200	1125.479
170.170.170.170	8				0.0000	1.32%	0.0100	94.288
200.68.120.81	3				0.0000	0.50%	0.0100	510.566
200.168.1.2	2				0.0000	0.33%	0.0100	324.152

Destination IPv4 Addresses	606				0.0004	100%	0.3000	94.154
192.168.1.1	257				0.0002	42.41%	0.0200	525.361
192.168.1.2	103				0.0001	17.00%	0.1600	94.154
192.168.1.255	102				0.0001	16.83%	0.0200	1116.969
212.242.33.35	42				0.0000	6.93%	0.0100	32.005
147.234.1.253	18				0.0000	2.97%	0.0900	94.154
200.68.120.81	13				0.0000	2.15%	0.0100	508.350
170.170.170.170	12				0.0000	1.98%	0.0200	94.206
212.242.33.36	7				0.0000	1.16%	0.0600	1444.583

Impact Analysis:

response times:

tcp.time_delta > 1

No.	Time	Source	Destination	Protocol	Length	Info
37	73.731185	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
38	73.731277	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
40	79.739895	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM

connection timeouts:

tcp.analysis.retransmission

No.	Time	Source	Destination	Protocol	Length	Info
37	73.731185	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
38	73.731277	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
40	79.739895	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
47	94.153897	147.234.1.253	192.168.1.2	FTP	108	[TCP ACKed unseen segment] [TCP Spurious Retransmission] Response: 220 ProFTPD Server In ECI Telecom (ntp,ecitele.cCm)
88	94.314809	192.168.1.2	147.234.1.253	TCP	60	[TCP ACKed unseen segment] [TCP Retransmission] 2720 → 21 [PSH, ACK] Seq=27198 Ack=734 Win=16199 Len=6
90	94.339083	147.234.1.253	192.168.1.2	TCP	68	[TCP Retransmission] 21 → 2720 [PSH, ACK] Seq=734 Ack=27204 Win=25398 Len=14
91	94.339315	192.168.1.2	147.234.1.253	TCP	54	[TCP Retransmission] 2720 → 21 [FIN, ACK] Seq=27204 Ack=748 Win=16185 Len=0
92	94.339700	147.234.1.253	192.168.1.2	TCP	60	[TCP Retransmission] 21 → 2720 [FIN, ACK] Seq=748 Ack=27204 Win=25398 Len=0

Monitoring Packet Loss:

tcp.analysis.lost_segment

No.	Time	Source	Destination	Protocol	Length	Info
48	94.154372	192.168.1.2	147.234.1.253	FTP	70	[TCP Previous segment not captured] Request: ♦SER anonymous
52	94.187272	147.234.1.253	192.168.1.2	TCP	60	[TCP ACKed unseen segment] [TCP Previous segment not captured] 21 → 2720 [ACK] Seq=131 Ack=27165 Win=25398 Len=0
59	94.204428	147.234.1.253	192.168.1.2	FTP	89	[TCP Previous segment not captured] Response: ♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦
66	94.207254	147.234.1.253	192.168.1.2	FTP	113	[TCP Previous segment not captured] Response: \t\t Anyone can access, write & retrieve a specific file
71	94.209838	147.234.1.253	192.168.1.2	FTP	102	[TCP Previous segment not captured] Response: Other Files will be deleted after 2 weeks !!!

Legitimate Traffic:

tcp.flags.syn==1 and tcp.flags.ack==1

No.	Time	Source	Destination	Protocol	Length	Info
85	94.313342	37.115.0.253	192.168.1.2	TCP	62	58999 → 2721 [SYN, ACK] Seq=0 Ack=1 Win=25398 Len=0 SACK_PERM MSS=1411

Suspicious Traffic :

No.	Time	Source	Destination	Protocol	Length	Info
35	70.812282	192.168.1.2	147.137.21.94	TCP	62	2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
36	70.812610	192.168.1.2	147.137.21.94	TCP	62	2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
37	73.731185	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
38	73.731277	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
39	79.739812	192.168.1.71	147.137.21.122	TCP	62	2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
40	79.739895	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
44	94.039026	192.168.1.2	147.234.1.253	TCP	62	2720 → 21 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
63	94.206103	147.234.1.170	170.170.170.170	TCP	113	43690 → 43690 [SYN, PSH, URG, CWR, Reserved] Seq=0 Win=43690 Urg=43690 Len=39
83	94.289910	192.168.1.6	147.234.1.253	TCP	62	2721 → 58999 [SYN] Seq=0 Win=16384 Len=0 MSS=1460