

**CSE3052 - INFORMATION SECURITY  
MANAGEMENT**

**DIGITAL ASSIGNMENT-5**

**ALOKAM NIKHITHA**

**19BCE2555**

# Wireshark

## TITLE:

## Wireshark Captures

## AIM:

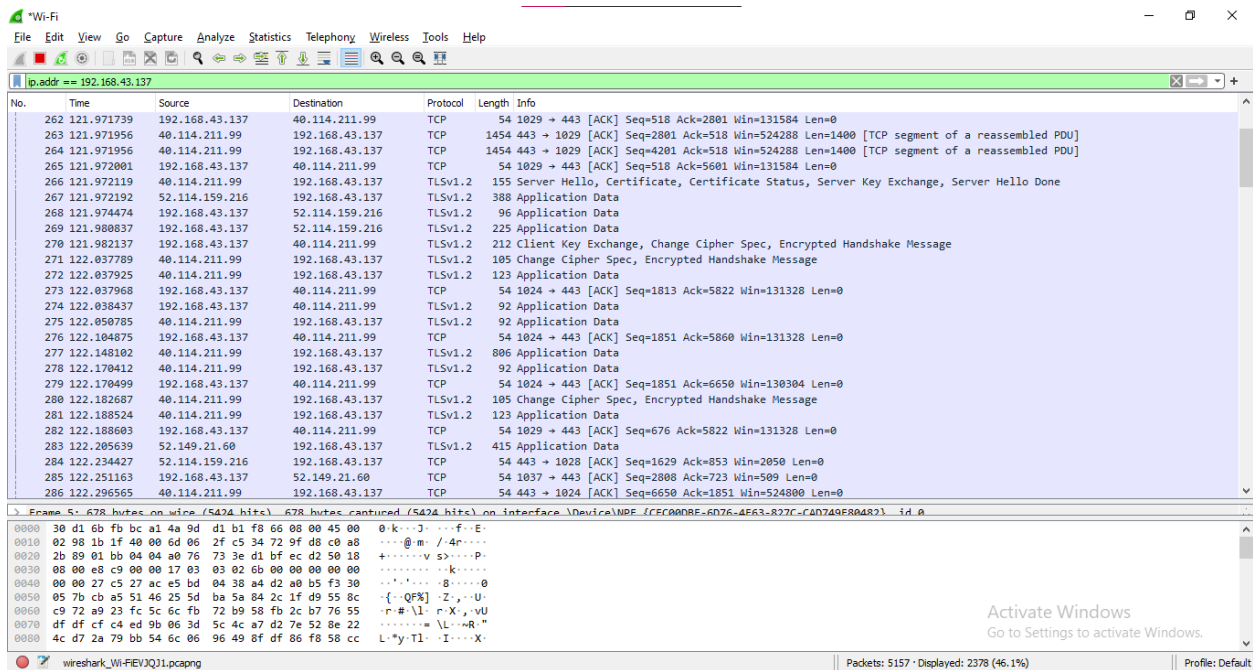
To capture packets with various filters in Wireshark

## PROCEDURE and Related Screen shots:

### 1. Filter traffic on specific IP address

It filters those traffic that have the specified IP address

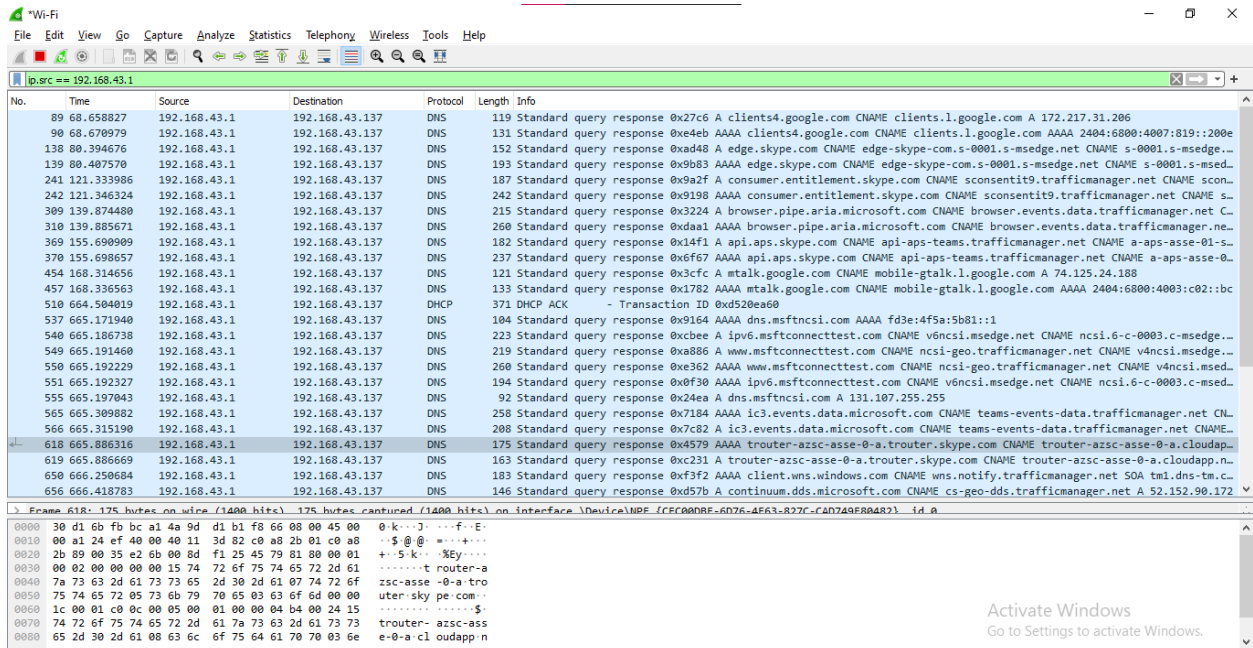
`ip.addr == 192.168.43.137`



## 2. Filter by source address

Displays all the packets that have the specified source address

ip.src == 192.168.43.1



The image shows 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. The filter bar at the top displays the active filter: `ip.src == 192.168.43.1`. The packet list pane shows a table of captured packets, with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are filtered to show only those from source IP 192.168.43.1. The packet details pane shows the selected packet (No. 618) as a DNS Standard query response. The packet bytes pane shows the raw data of the selected packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
89	68.658827	192.168.43.1	192.168.43.137	DNS	119	Standard query response 0x27c6 A clients4.google.com CNAME clients.l.google.com A 172.217.31.206
90	68.670979	192.168.43.1	192.168.43.137	DNS	131	Standard query response 0xe4eb AAAA clients4.google.com CNAME clients.l.google.com AAAA 2404:6800:4007:819::200e
138	80.394676	192.168.43.1	192.168.43.137	DNS	152	Standard query response 0xad48 A edge.skype.com CNAME edge-skype-com.s-0001.s-msedge.net CNAME s-0001.s-msedge...
139	80.407570	192.168.43.1	192.168.43.137	DNS	193	Standard query response 0x9b83 AAAA edge.skype.com CNAME edge-skype-com.s-0001.s-msedge.net CNAME s-0001.s-msed...
241	121.333986	192.168.43.1	192.168.43.137	DNS	187	Standard query response 0x9a2f A consumer.entitlement.skype.com CNAME sconsentit9.trafficmanager.net CNAME scons...
242	121.346324	192.168.43.1	192.168.43.137	DNS	242	Standard query response 0x9198 AAAA consumer.entitlement.skype.com CNAME sconsentit9.trafficmanager.net CNAME scons...
309	139.874480	192.168.43.1	192.168.43.137	DNS	215	Standard query response 0x3224 A browser.pipe.aria.microsoft.com CNAME browser.events.data.trafficmanager.net C...
310	139.885671	192.168.43.1	192.168.43.137	DNS	260	Standard query response 0xda1 AAAA browser.pipe.aria.microsoft.com CNAME browser.events.data.trafficmanager.net C...
369	155.690909	192.168.43.1	192.168.43.137	DNS	182	Standard query response 0x14f1 A api.aps.skype.com CNAME api-aps-teams.trafficmanager.net CNAME a-aps-asse-01-s...
370	155.690657	192.168.43.1	192.168.43.137	DNS	237	Standard query response 0x6f67 AAAA api.aps.skype.com CNAME api-aps-teams.trafficmanager.net CNAME a-aps-asse-0...
454	168.314656	192.168.43.1	192.168.43.137	DNS	121	Standard query response 0x3cfc A mtalk.google.com CNAME mobile-gtalk.l.google.com A 74.125.24.188
457	168.336563	192.168.43.1	192.168.43.137	DNS	133	Standard query response 0x1782 AAAA mtalk.google.com CNAME mobile-gtalk.l.google.com AAAA 2404:6800:4003:c02::bc
510	654.504819	192.168.43.1	192.168.43.137	DHCP	371	DHCP ACK - Transaction ID 0xd520ea60
537	665.171940	192.168.43.1	192.168.43.137	DNS	104	Standard query response 0x0164 AAAA dns.msftncsi.com AAAA fd3e4f5a:5b01::1
540	665.186738	192.168.43.1	192.168.43.137	DNS	223	Standard query response 0xcbee A ipv6.msftconnecttest.com CNAME v6ncsi.msedge.net CNAME ncsi.6-c-0003.c-msedge...
549	665.191468	192.168.43.1	192.168.43.137	DNS	219	Standard query response 0xa886 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME v4ncsi.msedge...
550	665.192229	192.168.43.1	192.168.43.137	DNS	260	Standard query response 0xe362 AAAA www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME v4ncsi.msed...
551	665.192327	192.168.43.1	192.168.43.137	DNS	194	Standard query response 0x0f30 AAAA ipv6.msftconnecttest.com CNAME v6ncsi.msedge.net CNAME ncsi.6-c-0003.c-msed...
555	665.197043	192.168.43.1	192.168.43.137	DNS	92	Standard query response 0x24ea A dns.msftncsi.com A 131.107.255.255
565	665.309882	192.168.43.1	192.168.43.137	DNS	258	Standard query response 0x7184 AAAA ic3.events.data.microsoft.com CNAME teams-events-data.trafficmanager.net CN...
566	665.315190	192.168.43.1	192.168.43.137	DNS	208	Standard query response 0x7c82 A ic3.events.data.microsoft.com CNAME teams-events-data.trafficmanager.net CNAME...
618	665.886316	192.168.43.1	192.168.43.137	DNS	175	Standard query response 0x4579 AAAA trouter-azsc-asse-0-a.trouter.skype.com CNAME trouter-azsc-asse-0-a.cloudapp.n...
619	665.886669	192.168.43.1	192.168.43.137	DNS	163	Standard query response 0xc231 A trouter-azsc-asse-0-a.trouter.skype.com CNAME trouter-azsc-asse-0-a.cloudapp.n...
650	666.250684	192.168.43.1	192.168.43.137	DNS	183	Standard query response 0xf3f2 AAAA client.wns.windows.com CNAME wns.notify.trafficmanager.net SOA tw1.dns-tm.c...
656	666.418783	192.168.43.1	192.168.43.137	DNS	146	Standard query response 0xd57b A continuum.dds.microsoft.com CNAME cs-geo-dds.trafficmanager.net A 52.152.90.172

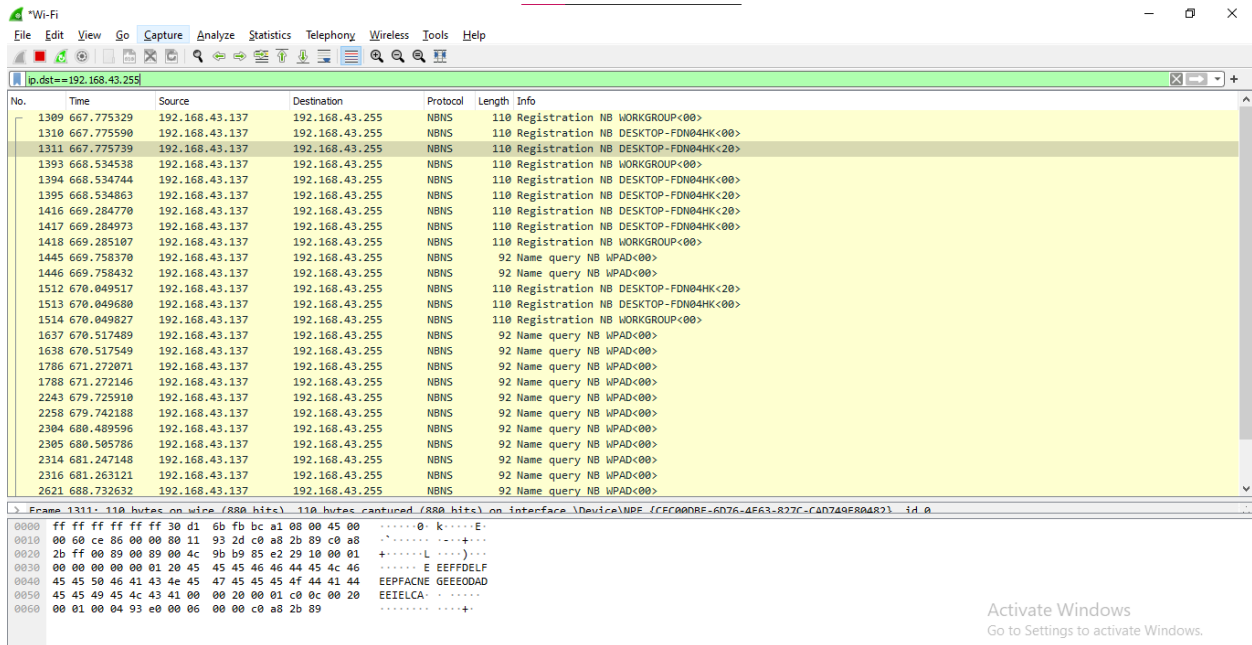
Frame 618: 175 bytes on wire (1400 bits) captured (1400 bits) on interface \Device\NPF{CEC000FE-6076-4F63-837C-C4D749F8A431} id 0

```
0000 30 d1 6b fb bc a1 4a 9d d1 b1 f8 66 00 00 45 00 00 k...f-E
0010 00 a1 24 ef 40 00 40 11 3d 82 c0 a8 2b 01 c0 a8 ..$@...+...
0020 2b 89 00 35 e2 6b 00 8d f1 25 45 79 81 80 00 01 +..5k...%Ey...
0030 00 02 00 00 00 00 15 74 72 6f 75 74 65 72 2d 61 .....t router-a
0040 7a 73 63 2d 61 73 73 65 2d 30 2d 61 07 74 72 6f zsc-asse-0-a.tro
0050 75 74 65 72 05 73 6b 79 70 65 03 63 6f 6d 00 00 uter-sky pe.com..
0060 1c 00 01 c0 0c 00 05 00 01 00 00 04 b4 00 24 15 .....$.
0070 74 72 6f 75 74 65 72 2d 61 7a 73 63 2d 61 73 73 trouter- azsc-asse
0080 65 2d 30 2d 61 08 63 6c 6f 75 64 61 70 70 03 6e e-0-a cl oudapp n
```

### 3. Filter by destination address

Displays all the packets that have the specified destination address

ip.dst==192.168.43.255



Wireshark packet capture window showing a list of packets filtered by destination IP 192.168.43.255. The list includes various protocols like NBNS and WPAD. A packet details pane is visible at the bottom showing the raw data of a selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1309	667.775329	192.168.43.137	192.168.43.255	NBNS	110	Registration NB WORKGROUP<00>
1310	667.775590	192.168.43.137	192.168.43.255	NBNS	110	Registration NB DESKTOP-FDN04HK<00>
1311	667.775739	192.168.43.137	192.168.43.255	NBNS	110	Registration NB DESKTOP-FDN04HK<20>
1393	668.534538	192.168.43.137	192.168.43.255	NBNS	110	Registration NB WORKGROUP<00>
1394	668.534744	192.168.43.137	192.168.43.255	NBNS	110	Registration NB DESKTOP-FDN04HK<00>
1395	668.534863	192.168.43.137	192.168.43.255	NBNS	110	Registration NB DESKTOP-FDN04HK<20>
1416	669.284770	192.168.43.137	192.168.43.255	NBNS	110	Registration NB DESKTOP-FDN04HK<20>
1417	669.284973	192.168.43.137	192.168.43.255	NBNS	110	Registration NB DESKTOP-FDN04HK<00>
1418	669.285107	192.168.43.137	192.168.43.255	NBNS	110	Registration NB WORKGROUP<00>
1445	669.758370	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
1446	669.758432	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
1512	670.049517	192.168.43.137	192.168.43.255	NBNS	110	Registration NB DESKTOP-FDN04HK<20>
1513	670.049680	192.168.43.137	192.168.43.255	NBNS	110	Registration NB DESKTOP-FDN04HK<00>
1514	670.049827	192.168.43.137	192.168.43.255	NBNS	110	Registration NB WORKGROUP<00>
1637	670.517489	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
1638	670.517549	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
1786	671.272071	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
1788	671.272146	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
2243	679.725910	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
2258	679.742188	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
2304	680.489596	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
2305	680.585706	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
2314	681.247148	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
2316	681.263121	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
2621	688.732632	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>

Frame 1311: 110 bytes on wire (880 bits) captured (880 bits) on interface \Device\NPF{CF600DE-6D76-4F63-R27C-CAD740E804R2} id 0

```
0000 ff ff ff ff ff 30 d1 6b fb bc a1 08 00 45 00 .....0.k....E
0010 00 60 ce 00 00 00 11 93 2d c0 a3 2b 89 c0 a8 .....-+...
0020 2b ff 00 89 00 89 00 4c 9b b9 85 e2 29 10 00 01 +.....L....)
0030 00 00 00 00 00 01 20 45 45 45 46 46 44 45 4c 46 .....E.EEFDL
0040 45 45 50 46 41 43 4e 45 47 45 45 45 4f 44 41 44 EEPFACNE GEEEOAD
0050 45 45 49 45 4c 43 41 00 00 20 00 01 c0 0c 00 20 EEIELCA .....
0060 00 01 00 04 93 e0 00 06 00 00 c0 a8 2b 89 .....+..
```

Activate Windows  
Go to Settings to activate Windows.

## 4. Filter by IP subnet

The mask does not need to match the local subnet mask since it is used to define the range. In order to display all the packet from 192.168.43.1, my display filter would be:

**ip.addr==192.168.43.1/24**

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane shows a list of captured packets, with the filter 'ip.addr==192.168.43.1/24' applied. The packet details pane shows the structure of the selected packet, and the packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1558	670.173629	192.168.43.137	224.0.0.252	LLMNR	64	Standard query 0x145d AAAA wpad
1559	670.173643	192.168.43.137	224.0.0.252	LLMNR	64	Standard query 0x5290 AAAA wpad
1560	670.173669	192.168.43.137	224.0.0.252	LLMNR	64	Standard query 0xe095 A wpad
1563	670.258872	192.168.43.137	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1564	670.272316	192.168.43.137	239.255.255.250	SSDP	223	M-SEARCH * HTTP/1.1
1576	670.322989	192.168.43.137	20.205.146.149	TCP	66	1042 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1588	670.324764	13.107.4.52	192.168.43.137	TCP	54	80 → 1040 [ACK] Seq=1 Ack=415 Win=4193792 Len=0
1603	670.329099	13.107.4.52	192.168.43.137	HTTP	574	HTTP/1.1 200 OK (text/plain)
1604	670.329223	52.149.21.60	192.168.43.137	TCP	66	443 → 1039 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM=1
1605	670.329275	192.168.43.137	52.149.21.60	TCP	54	1039 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
1606	670.329668	192.168.43.137	52.149.21.60	TLSv1.2	571	Client Hello
1607	670.370392	52.149.21.60	192.168.43.137	TCP	1454	443 → 1034 [ACK] Seq=1 Ack=518 Win=524288 Len=1400 [TCP segment of a reassembled PDU]
1608	670.371458	52.149.21.60	192.168.43.137	TCP	1454	443 → 1034 [ACK] Seq=1401 Ack=518 Win=524288 Len=1400 [TCP segment of a reassembled PDU]
1609	670.371491	192.168.43.137	52.149.21.60	TCP	54	1034 → 443 [ACK] Seq=518 Ack=2001 Win=131584 Len=0
1610	670.371843	52.149.21.60	192.168.43.137	TCP	1454	443 → 1034 [ACK] Seq=2001 Ack=518 Win=524288 Len=1400 [TCP segment of a reassembled PDU]
1612	670.377578	192.168.43.137	13.107.4.52	TCP	54	1040 → 80 [ACK] Seq=415 Ack=521 Win=131072 Len=0
1613	670.377631	52.149.21.60	192.168.43.137	TCP	1454	443 → 1034 [ACK] Seq=4201 Ack=518 Win=524288 Len=1400 [TCP segment of a reassembled PDU]
1614	670.377680	192.168.43.137	52.149.21.60	TCP	54	1034 → 443 [ACK] Seq=518 Ack=5601 Win=131584 Len=0
1615	670.377770	52.149.21.60	192.168.43.137	TLSv1.2	271	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
1620	670.387468	192.168.43.137	52.149.21.60	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1633	670.425680	20.205.146.149	192.168.43.137	TCP	66	443 → 1042 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=1 WS=128
1634	670.425736	192.168.43.137	20.205.146.149	TCP	54	1042 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
1635	670.426078	192.168.43.137	20.205.146.149	TLSv1.2	265	Client Hello
1637	670.517489	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>
1638	670.517549	192.168.43.137	192.168.43.255	NBNS	92	Name query NB WPAD<00>

Frame 1637: 92 bytes on wire (736 bits) captured (736 bits) on interface \Device\NPF{CFCA00FE-6D76-4F63-827C-CAD7A0F8A821} id 0

```
0000 ff ff ff ff ff ff 30 d1 6b fb bc a1 08 00 45 00 .....0 k-----E
0010 00 4e ce 92 00 00 00 11 93 33 c0 a8 2b 89 c0 a8 .....3-----N
0020 2b ff 00 89 00 00 00 3a 5e 3c 85 e4 01 10 00 01 .....^-----+
0030 00 00 00 00 00 00 20 46 48 46 41 45 42 45 45 43 .....F HFAEBEEC
0040 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 ACACACAC ACACACAC
0050 41 43 41 43 41 41 00 00 20 00 01 ACACAAA .....
```

Activate Windows  
Go to Settings to activate Windows.

## 5. Show all the packets

It shows all the packets that are being captured by Wireshark while net surfing.

## ALL PACKETS:

The screenshot displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets. The middle pane displays the details of the selected packet (No. 265), which is an Ethernet II frame. The bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
249	29.653383	2404:6800:4007:822::...	2401:4900:4dee:fa35::...	QUIC	912	Protected Payload (KP0)
250	29.653383	2404:6800:4007:822::...	2401:4900:4dee:fa35::...	QUIC	96	Protected Payload (KP0)
251	29.653383	2404:6800:4007:822::...	2401:4900:4dee:fa35::...	QUIC	201	Protected Payload (KP0)
252	29.653383	23.200.238.232	192.168.97.196	TLSv1.2	1398	Application Data
253	29.653405	192.168.97.196	23.200.238.232	TCP	54	7368 → 443 [ACK] Seq=1001 Ack=21350 Win=262144 Len=0
254	29.653513	192.168.97.132	192.168.97.196	DNS	174	Standard query response 0x3b67 AAAA ocsip.digicert.com CNAME cs9.wac.phicdn.net SOA ns1.edgecastcdn.net
255	29.653689	2401:4900:4dee:fa35::...	2404:6800:4007:822::...	QUIC	97	Protected Payload (KP0), DCID=2378094c85706029
256	29.653809	2401:4900:4dee:fa35::...	2404:6800:4007:822::...	QUIC	95	Protected Payload (KP0), DCID=2378094c85706029
257	29.653990	192.168.97.196	117.18.237.29	TCP	66	7371 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
258	29.779481	2404:6800:4007:822::...	2401:4900:4dee:fa35::...	QUIC	87	Protected Payload (KP0)
259	29.779481	23.200.238.232	192.168.97.196	TCP	54	443 → 7368 [ACK] Seq=21350 Ack=1001 Win=64128 Len=0
260	29.779481	52.84.6.120	192.168.97.196	TCP	66	80 → 7369 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=512
261	29.779481	117.18.237.29	192.168.97.196	TCP	66	80 → 7371 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=512
262	29.779481	2404:6800:4007:822::...	2401:4900:4dee:fa35::...	QUIC	87	Protected Payload (KP0)
263	29.779617	192.168.97.196	52.84.6.120	TCP	54	7369 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
264	29.779666	192.168.97.196	117.18.237.29	TCP	54	7371 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
265	29.779783	192.168.97.196	52.84.6.120	HTTP	274	GET //MEowS0B0MEQwQjA3BgUrDgKCGYuABBSLwZ6EW5gdYc9Ua5Eaal-jjETntkAQUv1X2830c7dH4b0N1Is3K0wG6p10CCQCNdkpWIK3fwL...
266	29.779711	192.168.97.196	117.18.237.29	HTTP	294	GET //MEFwTzBNMEswSTA3BetUrDeMVCgeUAB8050otx3ZfH0Zt1X28z8SIP17EWwxD10OUT1JUIB1V5uNu5e%2F6%2Bk570YX1zKCEAvpsXY8...

**Packet Details (No. 265):**

- Frame 265: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits) on interface \Device\NPF\_{CEC000BF-6D76-4E63-827C-CAD749E08482}, id 0
- Ethernet II, Src: LiteOnTe-fb:bca:1 (30:d1:6b:fb:bca:1), Dst: 8a:d3:5c:e7:28:f7 (8a:d3:5c:e7:28:f7)
- Internet Protocol Version 4, Src: 192.168.97.196, Dst: 52.84.6.120
- Transmission Control Protocol, Src Port: 7369, Dst Port: 80, Seq: 1, Ack: 1, Len: 220

**Packet Bytes:**

```
0000  8a d3 5c e7 28 f7 30 d1 6b fb bc a1 08 00 45 00  ...(\-0-k-----E-
0010  01 04 a0 ba 40 00 80 06 fc 00 c0 a8 61 c4 34 54  ...@.....a-4T
0020  06 78 1c c9 00 50 25 94 e1 86 a8 1c d5 fb 50 18  ...x...PX-----P-
0030  02 02 07 d5 00 00 47 45 54 20 2f 2f 4d 45 6f 77  ...---GE T //MEow
0040  53 44 42 47 4d 45 51 77 51 6a 41 4a 42 67 55 72  S0B0MEQw QjA3BgUr
0050  44 67 4d 43 47 67 55 41 42 42 53 4c 77 5a 36 45  DpKCGYuA BBSLwZ6E
0060  57 35 67 64 59 63 39 55 61 53 45 61 61 4c 6a 6a  W5gdYc9U a5Eaal-jj
0070  45 54 4e 74 6b 41 51 55 76 31 25 32 42 33 30 63  ETntkAQU v1X2830c
0080  37 64 48 34 62 30 57 31 57 73 33 4e 63 51 77 67  7dH4b0N1 W3NcQng
0090  36 70 69 4f 63 43 43 51 43 6e 44 6b 70 4d 4e 49  6pi0cCCQ CndkpWIK
00a0  4b 33 66 77 25 33 44 25 33 44 20 48 54 50 2f     K3fwK3D% 3D HTTP/
00b0  31 2e 31 00 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a  1.1-Connction:
00c0  20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63  Keep-Alive-Acc
```

Here we are collecting all the packets on starting the capture Here we haven't applied any filter. We can see that there are packets of different protocols which includes TCP (Transmission Control Protocol), HTTP (Hyper Text Transfer Protocol), OCSP (Online Certificate Status Protocol).

Here we are getting all are frames. We don't apply any filters and get this default screen as soon as we start capturing them.

We can see frames of different protocols which includes TCP (Transmission Control sProtocol), HTTP (Hyper Text Transfer Protocol), OCSP (Online Certificate Status Protocol).

Further we can see that all our TCP packets are acknowledged owing to the fact that TCP is a reliable protocol and deploys three-way handshaking rule to ensure that the packets are delivered at required destination.

In the snippet we can see that there are few TCP packets colored in black. These are incorrect transmissions. In the first transmission we can see the error message of incorrect acknowledgement. This implies that the TCP packet didn't satisfy the error check and control scheme. They seem to be a dirty read or incorrect checksum value while acknowledging the sequence number of that packet. Soon after we can see another black colored TCP packet. This packet is a retransmission packet as we need to re-send the packet which was not accepted by the receiver.

Next, we can see yet another TCP packet colored in black. This is a packet again being retransmitted because the sender didn't receive an acknowledgment of it while transmitting it.

## 6. TCP

[illegible]



No.	Time	Source	Destination	Protocol	Length	Info
13107	62.483480	35.161.149.12	192.168.97.141	TLSv1.2	92	Application Data
13108	62.483480	23.211.217.54	192.168.97.141	TLSv1.2	85	Encrypted Alert
13109	62.483480	2600:140f:2400:18f::...	2401:4900:4dee:fa35...	TLSv1.2	105	Encrypted Alert
13110	62.483480	2600:140f:2400:18f::...	2401:4900:4dee:fa35...	TCP	74	443 → 49721 [FIN, ACK] Seq=32 Ack=2 Win=503 Len=0
13111	62.483480	2600:140f:2400:18f::...	2401:4900:4dee:fa35...	TCP	74	[TCP Out-Of-Order] 443 → 49721 [FIN, ACK] Seq=32 Ack=2 Win=503 Len=0
13112	62.483480	99.83.135.170	192.168.97.141	TCP	54	443 → 25686 [ACK] Seq=8955 Ack=5027 Win=293888 Len=0
13113	62.483480	99.83.135.170	192.168.97.141	TCP	54	443 → 25686 [ACK] Seq=8955 Ack=5120 Win=293888 Len=0
13114	62.483480	23.211.217.54	192.168.97.141	TCP	54	443 → 49718 [FIN, ACK] Seq=32 Ack=2 Win=501 Len=0
13115	62.483480	2600:9000:2181:f000...	2401:4900:4dee:fa35...	TLSv1.3	1294	[TCP Fast Retransmission] , Continuation Data
13116	62.483480	99.83.135.170	192.168.97.141	TLSv1.2	129	Application Data
13117	62.483626	192.168.97.141	35.161.149.12	TCP	54	25680 → 443 [ACK] Seq=6396 Ack=9646 Win=65024 Len=0
13118	62.483671	192.168.97.141	23.211.217.54	TCP	54	49718 → 443 [ACK] Seq=2 Ack=32 Win=256 Len=0
13119	62.483770	192.168.97.141	23.211.217.54	TCP	54	49718 → 443 [RST, ACK] Seq=2 Ack=32 Win=0 Len=0
13120	62.483786	2401:4900:4dee:fa35...	2600:140f:2400:18f::...	TCP	74	49721 → 443 [RST, ACK] Seq=2 Ack=32 Win=0 Len=0
13121	62.485818	192.168.97.141	52.84.45.107	TLSv1.3	144	Application Data
13122	62.485885	192.168.97.141	52.84.45.107	TLSv1.3	1016	Application Data
13123	62.485975	23.211.217.54	192.168.97.141	TCP	54	[TCP Fast Retransmission] 443 → 49718 [FIN, ACK] Seq=32 Ack=2 Win=501 Len=0
13124	62.531500	192.168.97.141	99.83.135.170	TCP	54	25686 → 443 [ACK] Seq=5120 Ack=9030 Win=65024 Len=0
13125	62.531591	2401:4900:4dee:fa35...	2600:9000:2181:f000...	TCP	86	25675 → 443 [ACK] Seq=1069 Ack=3646387 Win=1058816 Len=0 SLE=3647607 SRE=3677114

> Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF\_{E727977E-8C51-48AA-883F-2048551768B5}, id 0  
 > Ethernet II, Src: IntelCor\_3f:c0:cd (ac:12:03:3f:c0:cd), Dst: 8a:d3:5c:e7:28:f7 (8a:d3:5c:e7:28:f7)  
 > Internet Protocol Version 4, Src: 192.168.97.141, Dst: 13.107.42.16  
 > Transmission Control Protocol, Src Port: 49800, Dst Port: 443, Seq: 1, Ack: 1, Len: 31  
 > Transport Layer Security

```

0000  8a d3 5c e7 28 f7 ac 12 03 3f c0 cd 08 00 45 00  --\ (---2---E-
0010  00 47 5f bf 40 00 80 06 00 00 c0 a8 61 8d 0d 6b  -G_@---a-k
0020  2a 10 c2 88 01 bb 33 d7 33 fe bf fe c4 4a 50 18  *-----3---JP
0030  01 01 59 ea 00 00 15 03 03 00 1a 00 00 00 00 00  -Y-----
0040  00 00 02 dc 56 c9 90 3a 43 93 c1 42 d4 a1 05 dc  ---V---C-B---
0050  0e af 5c 72 bd                                     --\n
  
```

Transmission Control Protocol: Protocol      Packets: 19899 · Displayed: 17238 (86.6%)      Profile: Default

Only TCP packets have been blocked in this case. We can see that [ACK] is used to acknowledge these packets once again. We also retrieve the length of each packet, which varies from 54 bytes to 1474 bytes in our case.

Many coloured TCP packets may be seen in our second screenshot. TCP out-of-order, TCP Fast Retransmission, and TCP Retransmission are some of the error messages we see.

1) TCP Out-of-Order: This refers to the fact that a frame was received in a different order than it was sent, i.e., it was acknowledged after a later packet was received first in sequence. It is not usually a problem; it indicates that there are numerous paths between the source and the destination, and one of them takes a longer route.

Here we applied tcp filter and we are able to collect all the tcp packets .

## 7. http

The image shows a Wireshark packet capture window with the filter 'http' applied. The packet list pane displays a list of captured packets, with the first 10 packets highlighted in green. The packet details pane shows the selected packet (No. 10) and its details, including the Ethernet II header, Internet Protocol Version 4 header, and Hypertext Transfer Protocol header. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
6152	858.384146	2600:140f:f400::173...	2401:4900:4dee:fa35...	HTTP	663	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
6154	858.386160	2401:4900:4dee:fa35...	2600:140f:f400::173...	HTTP	323	GET /c/msdownload/update/others/2022/03/36403572_18b87f890b365597cda6373f236dae625ecd415.cab HTTP/1.1
6158	858.450334	2600:140f:f400::173...	2401:4900:4dee:fa35...	HTTP	655	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
6160	858.452536	2401:4900:4dee:fa35...	2600:140f:f400::173...	HTTP	323	GET /c/msdownload/update/others/2022/03/36403571_667e0c8b3d3b2af1b7248f3eab9de29d7bb7761.cab HTTP/1.1
6167	858.577669	2600:140f:f400::173...	2401:4900:4dee:fa35...	HTTP	661	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
6247	861.589649	2401:4900:4dee:fa35...	2600:140f:f400::173...	HTTP	323	GET /c/msdownload/update/others/2022/03/36404270_a17e68965519bfb32593e0d332c069ff37a85ef2.cab HTTP/1.1
6254	861.676185	2600:140f:f400::173...	2401:4900:4dee:fa35...	HTTP	742	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
7028	889.869002	2401:4900:4dee:fa35...	2600:140f:f400::173...	HTTP	410	GET /d/msdownload/update/software/defu/2022/03/am_delta_patch_1.359.1921.0_c1806d9b1c28bac0941f37c3088ff411caa3...
7035	889.884509	2401:4900:4dee:fa35...	2600:140f:f400::173...	HTTP	410	GET /d/msdownload/update/software/defu/2022/03/am_delta_patch_1.359.1921.0_c1806d9b1c28bac0941f37c3088ff411caa3...
7037	889.926984	2600:140f:f400::173...	2401:4900:4dee:fa35...	HTTP	465	HTTP/1.1 206 Partial Content
7039	889.933746	2600:140f:f400::173...	2401:4900:4dee:fa35...	HTTP	465	HTTP/1.1 206 Partial Content
7040	889.945939	2401:4900:4dee:fa35...	2600:140f:f400::173...	HTTP	415	GET /d/msdownload/update/software/defu/2022/03/am_delta_patch_1.359.1921.0_c1806d9b1c28bac0941f37c3088ff411caa3...
7382	898.980253	2600:140f:f400::173...	2401:4900:4dee:fa35...	HTTP	1474	[TCP Fast Retransmission] HTTP/1.1 206 Partial Content
7432	891.509021	192.168.97.196	23.48.226.41	HTTP	407	GET /emdl/c/doc/ph/prod5/msdownload/update/software/defu/2022/03/1024/updateplatform_ec8a1f96ba65f834f24c5ba1b6...
7434	891.550549	23.48.226.41	192.168.97.196	HTTP/J...	1034	HTTP/1.1 200 OK , Javascript Object Notation (application/json)
7444	891.613340	2401:4900:4dee:fa35...	2600:140f:f400::173...	HTTP	397	GET /c/msdownload/update/software/defu/2022/03/updateplatform_ec8a1f96ba65f834f24c5ba1b660b4c10da59e3b.exe HTTP...
7447	891.618586	2401:4900:4dee:fa35...	2600:140f:f400::173...	HTTP	397	GET /c/msdownload/update/software/defu/2022/03/updateplatform_ec8a1f96ba65f834f24c5ba1b660b4c10da59e3b.exe HTTP...
7450	891.690520	2600:140f:f400::173...	2401:4900:4dee:fa35...	HTTP	467	HTTP/1.1 206 Partial Content

> Frame 265: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits) on interface \Device\NPF\_{CEC000BF-6076-4E63-827C-CAD749E80482}, id 0  
> Ethernet II, Src: LiteonTe\_fb:bcial (30:d1:6b:fb:bcial), Dst: 8a:d3:5c:e7:28:f7 (8a:d3:5c:e7:28:f7)  
> Internet Protocol Version 4, Src: 192.168.97.196, Dst: 52.84.6.120  
> Transmission Control Protocol, Src Port: 7369, Dst Port: 80, Seq: 1, Ack: 1, Len: 220

Here we applied http filter and we are able to collect all the http packets .

We've filtered out all of the packets that are part of the HTTP Protocol. Packet details such as source IP address, destination IP address, length, and information are visible.

The HTTP Status of Transmission can be found under the Information about Packets section. The status in our case is either 200 or 204.

1) HTTP 200 OK success code: The HTTP 200 OK success code indicates that the request was successful. By default, a 200 response can be cached.

2) HTTP 204 No content success: The HTTP 204 No content success status response code indicates that a request has been completed, but the client does not need to leave its

current page. This could be used, for example, when a wiki site's "save and continue editing" feature is implemented. The page would be saved using a PUT request, and the 204 No content response would be sent to signal that the editor should not be replaced by another page.

## **8. Filter traffic based on protocol**

### **DNS**

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol(IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
972	667.385478	192.168.43.1	192.168.43.137	DNS	187	Standard query response 0x2354 AAAA trouter2-azsc-krcce-5-b.trouter.teams.microsoft.com CNAME trouter2-azsc-krcce-
973	667.385478	192.168.43.1	192.168.43.137	DNS	230	Standard query response 0xb52 A teams.microsoft.com CNAME teams.office.com CNAME teams-mira-afd.trafficmanager-
974	667.385478	192.168.43.1	192.168.43.137	DNS	242	Standard query response 0xf2a4 AAAA teams.microsoft.com CNAME teams.office.com CNAME teams-mira-afd.trafficmana-
1370	668.042911	192.168.43.137	192.168.43.1	DNS	228	Standard query response 0xb9f7 A westus-prod-2.notifications.teams.microsoft.com CNAME westuscsn-prod-2.traffic-
1371	668.043218	192.168.43.137	192.168.43.1	DNS	86	Standard query 0xeded A licensing.mp.microsoft.com
1375	668.178216	192.168.43.1	192.168.43.137	DNS	86	Standard query 0xc89b AAAA licensing.mp.microsoft.com
1377	668.178500	192.168.43.1	192.168.43.137	DNS	266	Standard query response 0xeded A licensing.mp.microsoft.com CNAME consumer-licensing-aks2aks.md.mp.microsoft.co-
1449	669.758811	192.168.43.137	192.168.43.1	DNS	323	Standard query response 0xc89b AAAA licensing.mp.microsoft.com CNAME consumer-licensing-aks2aks.md.mp.microsoft-
1451	669.758998	192.168.43.137	192.168.43.1	DNS	81	Standard query 0x6ef3 A config.edge.skype.com
1452	669.759003	192.168.43.137	192.168.43.1	DNS	83	Standard query 0x9e10 A www.msftconnecttest.com
1453	669.759016	192.168.43.137	192.168.43.1	DNS	72	Standard query 0x62dc A www.bing.com
1456	669.759199	192.168.43.137	192.168.43.1	DNS	81	Standard query 0xa0c4 AAAA config.edge.skype.com
1457	669.759223	192.168.43.137	192.168.43.1	DNS	83	Standard query 0xb52 AAAA www.msftconnecttest.com
1472	669.788199	192.168.43.1	192.168.43.137	DNS	72	Standard query 0xb09c AAAA www.bing.com
1473	669.788610	192.168.43.1	192.168.43.137	DNS	246	Standard query response 0x9e10 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME v4ncsi.msedge...
1475	669.849688	192.168.43.1	192.168.43.137	DNS	230	Standard query response 0xb52 AAAA www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME v4ncsi.msed...
1476	669.849688	192.168.43.1	192.168.43.137	DNS	253	Standard query response 0xa0c4 AAAA config.edge.skype.com CNAME config.edge.skype.com.trafficmanager.net CNAME ...
1479	669.850713	192.168.43.1	192.168.43.137	DNS	216	Standard query response 0xb09c AAAA www.bing.com CNAME a-0001.a-afndentry.net.trafficmanager.net CNAME www-bing-
1480	669.850923	192.168.43.1	192.168.43.137	DNS	241	Standard query response 0x6f3 A config.edge.skype.com CNAME config.edge.skype.com.trafficmanager.net CNAME 1-0-
1500	670.003239	192.168.43.137	192.168.43.1	DNS	220	Standard query response 0x62dc A www.bing.com CNAME a-0001.a-afndentry.net.trafficmanager.net CNAME www-bing-com...
1501	670.003402	192.168.43.137	192.168.43.1	DNS	79	Standard query 0xa0a0 AAAA clients4.google.com
1543	670.094777	192.168.43.1	192.168.43.137	DNS	79	Standard query 0xa0a0 AAAA clients4.google.com
1544	670.096911	192.168.43.1	192.168.43.137	DNS	119	Standard query response 0xa0a0 A clients4.google.com CNAME clients.l.google.com A 142.250.182.14
1754	670.900874	192.168.43.137	192.168.43.1	DNS	131	Standard query response 0xa0a0 clients4.google.com CNAME clients.l.google.com AAAA 2404:6800:4007:809:200e...
1754	670.900874	192.168.43.137	192.168.43.1	DNS	82	Standard query 0x9e10 A client.wms.windows.com

Frame 1544: 131 bytes on wire (1048 bits) captured (1048 bits) on interface \Device\NPF{CEC000BF-6D76-4F63-B27C-CAD749F804R2} id 0

0000 30 d1 6b fb bc a1 4a 9d d1 b1 f8 66 00 00 45 00 0 k...J...f...E...  
0010 00 75 26 1f 40 00 40 11 3c 7e c0 a0 2b 01 c0 a8 u&@...<...+...  
0020 2b 89 00 35 e2 50 00 61 15 60 aa a0 81 00 00 01 +...5 P...a...  
0030 00 82 00 00 00 00 00 63 6c 69 65 6e 74 73 34 06 .....c lients4...  
0040 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 1c 00 01 c0 google.c om...  
0050 0c 00 05 00 01 00 00 49 00 0c 07 63 6c 69 65 .....nt: l...  
0060 6e 74 73 01 6c c0 15 c0 31 00 1c 00 01 00 00 01 nts l...  
0070 04 00 10 24 04 68 00 40 07 08 09 00 00 00 00 00 ..\$..h...  
0080 00 20 0e

## 9. http.request or http.response

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request or http.response

No.	Time	Source	Destination	Protocol	Length	Info
219	104.305239	192.168.43.137	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
220	105.311305	192.168.43.137	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
222	105.337989	192.168.43.137	239.255.255.250	SSDP	223	M-SEARCH * HTTP/1.1
224	106.322315	192.168.43.137	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
225	106.353486	192.168.43.137	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
229	107.336335	192.168.43.137	239.255.255.250	SSDP	223	M-SEARCH * HTTP/1.1
230	107.367330	192.168.43.137	239.255.255.250	SSDP	223	M-SEARCH * HTTP/1.1
231	108.381786	192.168.43.137	239.255.255.250	SSDP	223	M-SEARCH * HTTP/1.1
561	665.264645	192.168.43.137	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
568	665.336037	13.107.4.52	192.168.43.137	HTTP	593	HTTP/1.1 200 OK (text/plain)
596	665.704859	2401:4900:4de7:f4e0::2a01:111:2003::52	2401:4900:4de7:f4e0::2a01:111:2003::52	HTTP	186	GET /connecttest.txt HTTP/1.1
608	665.764584	2a01:111:2003::52	2401:4900:4de7:f4e0::2a01:111:2003::52	HTTP	613	HTTP/1.1 200 OK (text/plain)
910	667.263696	2401:4900:4de7:f4e0::2a01:111:2003::52	2401:4900:4de7:f4e0::2a01:111:2003::52	HTTP	229	GET /connecttest.txt HTTP/1.1
915	667.271353	192.168.43.137	13.107.4.52	HTTP	200	GET /connecttest.txt HTTP/1.1
961	667.385381	2a01:111:2003::52	2401:4900:4de7:f4e0::2a01:111:2003::52	HTTP	613	HTTP/1.1 200 OK (text/plain)
989	667.386238	13.107.4.52	192.168.43.137	HTTP	593	HTTP/1.1 200 OK (text/plain)
1551	670.103869	192.168.43.137	13.107.4.52	HTTP	468	GET /connecttest.txt?n=1649141992222 HTTP/1.1
1563	670.258872	192.168.43.137	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1564	670.272316	192.168.43.137	239.255.255.250	SSDP	223	M-SEARCH * HTTP/1.1
1603	670.329099	13.107.4.52	192.168.43.137	HTTP	574	HTTP/1.1 200 OK (text/plain)
1787	671.272114	192.168.43.137	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1789	671.286926	192.168.43.137	239.255.255.250	SSDP	223	M-SEARCH * HTTP/1.1
1846	672.278133	192.168.43.137	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1847	672.287964	192.168.43.137	239.255.255.250	SSDP	223	M-SEARCH * HTTP/1.1
1929	673.280993	192.168.43.137	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1

Frame 561: 165 bytes on wire (1320 bits) captured (1320 bits) on interface \Device\NPF{CEC000BF-6D76-4F63-B27C-CAD749F804R2} id 0

0000 4a 9d d1 b1 f8 66 30 d1 6b fb bc a1 00 00 45 00 J...f...k...E...  
0010 00 97 5a 98 40 00 00 06 a1 f8 c0 a0 2b 89 0d 6b +Z@...+...k...  
0020 04 34 04 14 00 50 d8 81 31 d6 d5 8b 7e 4f 50 18 4...P...1...xOP...  
0030 02 02 8d c1 00 00 47 45 54 20 2f 63 6f 6e 6e 65 .....GE T /conne...  
0040 63 74 74 65 73 74 2e 74 78 74 20 48 54 54 50 2f cttest: t HTTP/...  
0050 31 2e 31 0d 00 43 6f 6e 6e 65 63 74 69 6f 6e 3a 1..1..Con nection:...  
0060 20 43 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65 c lose: User-Age...  
0070 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 20 4e 43 nt: Micr osoft NC...  
0080 53 49 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 73 SI...Host : www.ms

Response: Boolean

Packets: 10987 · Displayed: 130 (1.2%)

Profile: Default

## 10. tcp.port==80 and ip.addr==192.168.43.137

The image shows a Wireshark packet capture analysis. The top toolbar includes options like File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main display area shows a list of captured packets, filtered by 'tcp.port==80 and ip.addr==192.168.43.137'. The list includes columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are numbered 552 to 995. The detailed view pane shows the selected packet (No. 561) with its raw data and protocol details. The raw data is displayed in hexadecimal and ASCII. The protocol details pane shows the packet structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
552	665.193704	192.168.43.137	13.107.4.52	TCP	66	1044 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
559	665.263944	13.107.4.52	192.168.43.137	TCP	66	80 → 1044 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM=1
560	665.264174	192.168.43.137	13.107.4.52	TCP	54	1044 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
561	665.264645	192.168.43.137	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
567	665.335910	13.107.4.52	192.168.43.137	TCP	54	80 → 1044 [ACK] Seq=1 Ack=112 Win=4194048 Len=0
568	665.336037	13.107.4.52	192.168.43.137	HTTP	593	HTTP/1.1 200 OK (text/plain)
569	665.336141	13.107.4.52	192.168.43.137	TCP	54	80 → 1044 [FIN, ACK] Seq=540 Ack=112 Win=4194048 Len=0
570	665.336197	192.168.43.137	13.107.4.52	TCP	54	1044 → 80 [ACK] Seq=112 Ack=541 Win=130816 Len=0
571	665.336269	192.168.43.137	13.107.4.52	TCP	54	1044 → 80 [FIN, ACK] Seq=112 Ack=541 Win=130816 Len=0
573	665.382863	13.107.4.52	192.168.43.137	TCP	54	80 → 1044 [ACK] Seq=541 Ack=113 Win=4194048 Len=0
798	667.207299	192.168.43.137	13.107.4.52	TCP	66	1035 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
913	667.272995	13.107.4.52	192.168.43.137	TCP	66	80 → 1035 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM=1
914	667.273046	192.168.43.137	13.107.4.52	TCP	54	1035 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
915	667.273153	192.168.43.137	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
988	667.386238	13.107.4.52	192.168.43.137	TCP	54	80 → 1035 [ACK] Seq=1 Ack=155 Win=4194048 Len=0
989	667.386238	13.107.4.52	192.168.43.137	HTTP	593	HTTP/1.1 200 OK (text/plain)
990	667.386238	13.107.4.52	192.168.43.137	TCP	54	80 → 1035 [FIN, ACK] Seq=540 Ack=155 Win=4194048 Len=0
993	667.386576	192.168.43.137	13.107.4.52	TCP	54	1035 → 80 [ACK] Seq=155 Ack=541 Win=130816 Len=0
995	667.387009	192.168.43.137	13.107.4.52	TCP	54	1035 → 80 [FIN, ACK] Seq=155 Ack=541 Win=130816 Len=0

> Frame 561: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on Interface \Device\NPF\_{CEC000BF-6076-4E63-827C-CAD749E80482}, Id 0  
> Ethernet II, Src: LiteonTe\_fb:bc:al (30:d1:6b:fb:bc:al), Dst: 4a:9d:d1:b1:f8:66 (4a:9d:d1:b1:f8:66)  
> Internet Protocol Version 4, Src: 192.168.43.137, Dst: 13.107.4.52  
> Transmission Control Protocol, Src Port: 1044, Dst Port: 80, Seq: 1, Ack: 111, Len: 111  
> Hypertext Transfer Protocol

0000 4a 9d d1 b1 f8 66 30 d1 6b fb bc a1 08 00 45 00 J....f0.k.....E  
0010 00 97 5a 98 40 00 80 06 a1 f8 c0 a8 2b 89 0d 6b ..Z.@.....+..k  
0020 04 34 04 14 00 50 d8 81 31 d6 d5 8b 7e 4f 50 18 .4...P...1....OP  
0030 02 82 8d c1 00 00 47 45 54 20 2f 63 6f 6e 6e 65 .....GE T /conne  
0040 63 74 74 65 73 74 2e 74 78 74 20 48 54 54 50 2f cttest.txt HTTP/  
0050 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 1.1' Con nection:  
0060 20 43 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65 Close User-Age  
0070 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 20 4e 43 nt: Micr osoft NC  
0080 53 49 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 73 SI...Host : www.ms

## Conclusion:

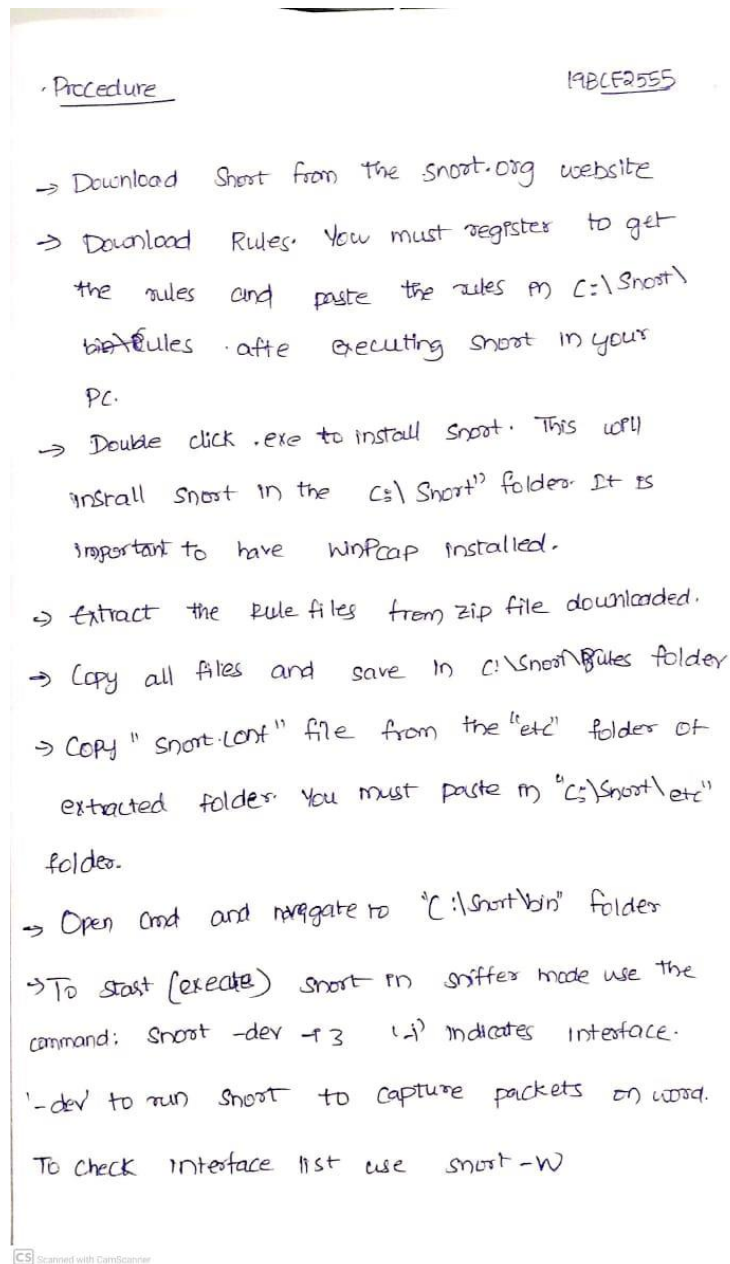
Here we have filtered all the packets and analysed different packets. We have summarized all the different errors we got during TCP transmission and also analysed various status states of HTTP.

# SNORT

## Aim:

## To Install and work with the SNORT Software

## Procedure:



## Moving to C:\Snort\bin directory in command prompt

```

C:\> Command Prompt - snort -dev -i 3
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\LENOVO>cd..

C:\Users>cd..

C:\>cd snort

C:\Snort>cd bin

```

## snort.exe for testing snort

```

C:\Snort\bin>snort.exe
Running in packet dump mode

    === Initializing Snort ===
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{ECE706EE-4EE9-49D6-BCBE-22AE47E5ABD4}".
Decoding Ethernet

    === Initialization Complete ===

    ,,_
o"  )~  -*> Snort! <*-
    '...'
Version 2.9.19-WIN64 GRE (Build 85)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Commencing packet processing (pid=14008)
*** Caught Int-Signal
=====
Run time for packet processing was 41.150000 seconds
Snort processed 0 packets.
Snort ran for 0 days 0 hours 0 minutes 41 seconds
Pkts/sec:          0
=====
Packet I/O Totals:
Received:          0
Analyzed:          0 ( 0.000%)
Dropped:           0 ( 0.000%)
Filtered:          0 ( 0.000%)
Outstanding:       0 ( 0.000%)
Injected:          0
=====

```



=====

Breakdown by protocol (includes rebuilt packets):

Eth:	0 ( 0.000%)
VLAN:	0 ( 0.000%)
IP4:	0 ( 0.000%)
Frag:	0 ( 0.000%)
ICMP:	0 ( 0.000%)
UDP:	0 ( 0.000%)
TCP:	0 ( 0.000%)
IP6:	0 ( 0.000%)
IP6 Ext:	0 ( 0.000%)
IP6 Opts:	0 ( 0.000%)
Frag6:	0 ( 0.000%)
ICMP6:	0 ( 0.000%)
UDP6:	0 ( 0.000%)
TCP6:	0 ( 0.000%)
Teredo:	0 ( 0.000%)
ICMP-IP:	0 ( 0.000%)
EAPOL:	0 ( 0.000%)
IP4/IP4:	0 ( 0.000%)
IP4/IP6:	0 ( 0.000%)
IP6/IP4:	0 ( 0.000%)
IP6/IP6:	0 ( 0.000%)
GRE:	0 ( 0.000%)
GRE Eth:	0 ( 0.000%)
GRE VLAN:	0 ( 0.000%)
GRE IP4:	0 ( 0.000%)
GRE IP6:	0 ( 0.000%)
GRE IP6 Ext:	0 ( 0.000%)
GRE PPTP:	0 ( 0.000%)
GRE ARP:	0 ( 0.000%)
GRE IPX:	0 ( 0.000%)
GRE Loop:	0 ( 0.000%)
MPLS:	0 ( 0.000%)
ARP:	0 ( 0.000%)

GRE Loop:	0 ( 0.000%)
MPLS:	0 ( 0.000%)
ARP:	0 ( 0.000%)
IPX:	0 ( 0.000%)
Eth Loop:	0 ( 0.000%)
Eth Disc:	0 ( 0.000%)
IP4 Disc:	0 ( 0.000%)
IP6 Disc:	0 ( 0.000%)
TCP Disc:	0 ( 0.000%)
UDP Disc:	0 ( 0.000%)
ICMP Disc:	0 ( 0.000%)
All Discard:	0 ( 0.000%)
Other:	0 ( 0.000%)
Bad Chk Sum:	0 ( 0.000%)
Bad TTL:	0 ( 0.000%)
S5 G 1:	0 ( 0.000%)
S5 G 2:	0 ( 0.000%)
Total:	0

=====

Memory Statistics for File at: Tue Apr 5 08:36:54 2022

Total buffers allocated:	0
Total buffers freed:	0
Total buffers released:	0
Total file mempool:	0
Total allocated file mempool:	0
Total freed file mempool:	0
Total released file mempool:	0

Heap Statistics of file:

Total Statistics:	
Memory in use:	0 bytes
No of allocs:	0
No of frees:	0

=====

Snort exiting



To check the interface list, use following command:  
**snort -W**

```
C:\Snort\bin>snort -W

-*) Snort! <*-
Version 2.9.19-WIN64 GRE (Build 85)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

-----
Index   Physical Address      IP Address      Device Name      Description
-----
1       00:00:00:00:00:00      disabled       \Device\NPF_{ECE706EE-4EE9-49D6-BCBE-22AE47E5A8D4}  WAN Miniport (Network Monitor)
2       00:00:00:00:00:00      disabled       \Device\NPF_{04111C3D-7002-4E4B-A7D7-02B560F8DB7C}  WAN Miniport (IPv6)
3       00:00:00:00:00:00      disabled       \Device\NPF_{F07AE100-36C8-4063-B0A1-78CE68C8FF7D}  WAN Miniport (IP)
4       30:D1:68:FB:BC:A2      0000:0000:fe80:0000:0000:c997:41d8 \Device\NPF_{CCE0FE47-D127-4F48-BD86-C7B7C751693F}  Bluetooth Device (Personal Area Network)
5       30:D1:68:FB:BC:A1      0000:0000:2401:4900:234b:b7ec:bc0a:7850 \Device\NPF_{CEC000BF-6D76-4E63-827C-CAD749E80482}  Qualcomm Atheros QCA9377 Wireless Network Adapter #2
6       42:D1:68:FB:BC:A1      0000:0000:fe80:0000:0000:e8b0:a6a1 \Device\NPF_{7354E09C-5621-4675-A32C-87F69382E94F}  Microsoft Wi-Fi Direct Virtual Adapter #2
7       32:D1:68:FB:BC:A1      0000:0000:fe80:0000:0000:0000:bca1:ee7f \Device\NPF_{D878D4CD-5ECD-4485-9625-BB3821B01501}  Microsoft Wi-Fi Direct Virtual Adapter
8       00:00:00:00:00:00      disabled       \Device\NPF_{Loopback} Adapter for loopback traffic capture
9       E8:6A:64:3D:57:F7      0000:0000:fe80:0000:0000:ec9b:89da \Device\NPF_{D8D11AE0-9913-4D2F-B431-53683A9F48A8}  Realtek PCIe GbE Family Controller
```

```
C:\Snort\bin>snort -i 1 -c c:\Snort\etc\snort.conf-T
Running in IDS mode

--- Initializing Snort ---
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf-T"
ERROR: c:\Snort\etc\snort.conf-T(0) Unable to open rules file "c:\Snort\etc\snort.conf-T": No such file or directory.

Fatal Error, Quitting..
Could not create the registry key.
```

To start (execute) snort in sniffer mode use following command:

**snort -dev -i 3**

-i indicates the interface number. You must pick the correct interface number. In my case, it is 3. -dev is used to run snort to capture packets on your network.

```

C:\Snort\bin>snort -dev -i 3
Running in packet dump mode

--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{F07AE100-36C8-4063-B0A1-78CE68C8FF7D}".
Decoding Ethernet

--== Initialization Complete ==--

_*> Snort! <*-
o"_)~ Version 2.9.19-WIN64 GRE (Build 85)
'...' By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using PCRE version: 8.10 2010-06-25
      Using ZLIB version: 1.2.11

Commencing packet processing (pid=17832)
*** Caught Int-Signal
=====
Run time for packet processing was 10130.399000 seconds
Snort processed 0 packets.
Snort ran for 0 days 2 hours 48 minutes 50 seconds
  Pkts/hr:      0
  Pkts/min:     0
  Pkts/sec:     0
=====
Packet I/O Totals:
  Received:      0
  Analyzed:      0 ( 0.000%)
  Dropped:       0 ( 0.000%)
  Filtered:      0 ( 0.000%)
  Outstanding:   0 ( 0.000%)
  Injected:      0
=====
Breakdown by protocol (includes rebuilt packets):
  Eth:           0 ( 0.000%)
  VLAN:          0 ( 0.000%)
  IP4:           0 ( 0.000%)
  Frag:          0 ( 0.000%)
  ICMP:          0 ( 0.000%)

```

Command Prompt

```
Frag: 0 ( 0.000%)
ICMP: 0 ( 0.000%)
UDP: 0 ( 0.000%)
TCP: 0 ( 0.000%)
IP6: 0 ( 0.000%)
IP6 Ext: 0 ( 0.000%)
IP6 Opts: 0 ( 0.000%)
Frag6: 0 ( 0.000%)
ICMP6: 0 ( 0.000%)
UDP6: 0 ( 0.000%)
TCP6: 0 ( 0.000%)
Teredo: 0 ( 0.000%)
ICMP-IP: 0 ( 0.000%)
EAPOL: 0 ( 0.000%)
IP4/IP4: 0 ( 0.000%)
IP4/IP6: 0 ( 0.000%)
IP6/IP4: 0 ( 0.000%)
IP6/IP6: 0 ( 0.000%)
GRE: 0 ( 0.000%)
GRE Eth: 0 ( 0.000%)
GRE VLAN: 0 ( 0.000%)
GRE IP4: 0 ( 0.000%)
GRE IP6: 0 ( 0.000%)
GRE IP6 Ext: 0 ( 0.000%)
GRE PPTP: 0 ( 0.000%)
GRE ARP: 0 ( 0.000%)
GRE IPX: 0 ( 0.000%)
GRE Loop: 0 ( 0.000%)
MPLS: 0 ( 0.000%)
ARP: 0 ( 0.000%)
IPX: 0 ( 0.000%)
Eth Loop: 0 ( 0.000%)
Eth Disc: 0 ( 0.000%)
IP4 Disc: 0 ( 0.000%)
IP6 Disc: 0 ( 0.000%)
TCP Disc: 0 ( 0.000%)
UDP Disc: 0 ( 0.000%)
ICMP Disc: 0 ( 0.000%)
All Discard: 0 ( 0.000%)
Other: 0 ( 0.000%)
Bad Chk Sum: 0 ( 0.000%)
Bad TTL: 0 ( 0.000%)
S5 G 1: 0 ( 0.000%)
S5 G 2: 0 ( 0.000%)
```

```
C:\ Command Prompt
GRE Loop:      0 ( 0.000%)
MPLS:          0 ( 0.000%)
ARP:           0 ( 0.000%)
IPX:           0 ( 0.000%)
Eth Loop:      0 ( 0.000%)
Eth Disc:      0 ( 0.000%)
IP4 Disc:      0 ( 0.000%)
IP6 Disc:      0 ( 0.000%)
TCP Disc:      0 ( 0.000%)
UDP Disc:      0 ( 0.000%)
ICMP Disc:     0 ( 0.000%)
All Discard:   0 ( 0.000%)
Other:         0 ( 0.000%)
Bad Chk Sum:   0 ( 0.000%)
Bad TTL:       0 ( 0.000%)
S5 G 1:        0 ( 0.000%)
S5 G 2:        0 ( 0.000%)
Total:         0

=====

Memory Statistics for File at:Tue Apr  5 12:07:11 2022

Total buffers allocated:      0
Total buffers freed:          0
Total buffers released:       0
Total file mempool:           0
Total allocated file mempool: 0
Total freed file mempool:     0
Total released file mempool:   0

Heap Statistics of file:
  Total Statistics:
    Memory in use:             0 bytes
    No of allocs:               0
    No of frees:                0

=====

Snort exiting

C:\Snort\bin>\
```

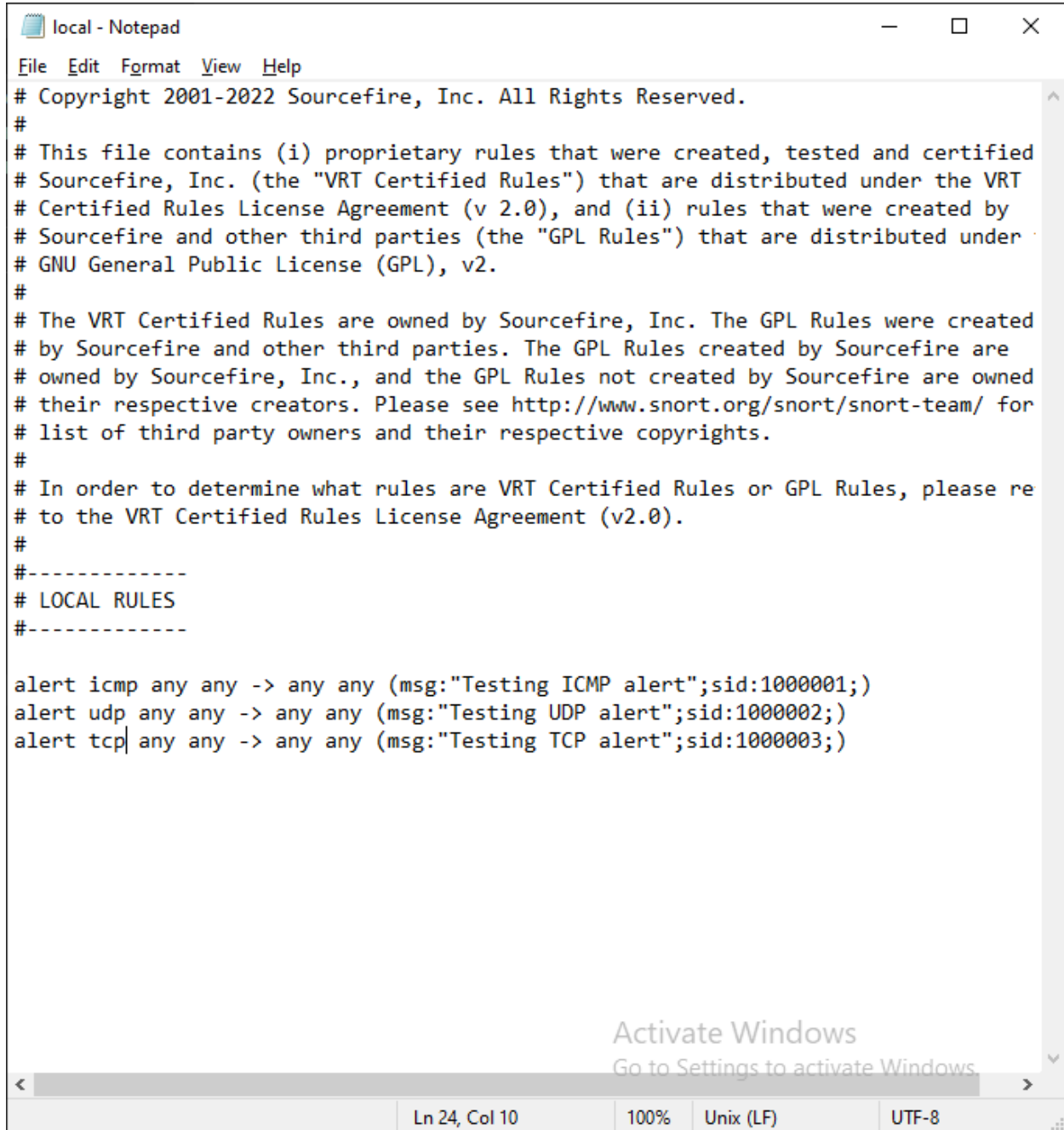
## To run:

```
C:\Snort\bin>snort -i 1 -c c:\Snort\etc\snort.conf-A console
Running in IDS mode

--- Initializing Snort ---
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf-A"
ERROR: c:\Snort\etc\snort.conf-A(0) Unable to open rules file "c:\Snort\etc\snort.conf-A": No such file or directory.

Fatal Error, Quitting..
Could not create the registry key.
C:\Snort\bin>
```

## Local Rules File:



```
local - Notepad
File Edit Format View Help
# Copyright 2001-2022 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
# Sourcefire and other third parties (the "GPL Rules") that are distributed under
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
# by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
# owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned
# their respective creators. Please see http://www.snort.org/snort/snort-team/ for
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules, please re
# to the VRT Certified Rules License Agreement (v2.0).
#
#-----
# LOCAL RULES
#-----

alert icmp any any -> any any (msg:"Testing ICMP alert";sid:1000001;)
alert udp any any -> any any (msg:"Testing UDP alert";sid:1000002;)
alert tcp any any -> any any (msg:"Testing TCP alert";sid:1000003;)

Activate Windows
Go to Settings to activate Windows.
Ln 24, Col 10 100% Unix (LF) UTF-8
```

We can add our own rules in the local file that is there in the `c:\snort\rules\` directory.

## On starting SNORT:

```
C:\Snort\bin>snort -v
Running in packet dump mode

--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{3F2BFF6B-91E4-4E81-8658-2376F920CF33}".
Decoding Ethernet

--== Initialization Complete ==--

_*> Snort! <*-
o" )~ Version 2.9.19-WIN64 GRE (Build 85)
' ' By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.
    Using PCRE version: 8.10 2010-06-25
    Using ZLIB version: 1.2.11

Commencing packet processing (pid=18564)
```

## On exiting (Ctrl+C)

```
Command Prompt
GRE IP6: 0 ( 0.000%)
GRE IP6 Ext: 0 ( 0.000%)
GRE PPTP: 0 ( 0.000%)
GRE ARP: 0 ( 0.000%)
GRE IPX: 0 ( 0.000%)
GRE Loop: 0 ( 0.000%)
MPLS: 0 ( 0.000%)
ARP: 0 ( 0.000%)
IPX: 0 ( 0.000%)
Eth Loop: 0 ( 0.000%)
Eth Disc: 0 ( 0.000%)
IP4 Disc: 0 ( 0.000%)
IP6 Disc: 0 ( 0.000%)
TCP Disc: 0 ( 0.000%)
UDP Disc: 0 ( 0.000%)
ICMP Disc: 0 ( 0.000%)
All Discard: 0 ( 0.000%)
Other: 0 ( 0.000%)
Bad Chk Sum: 0 ( 0.000%)
Bad TTL: 0 ( 0.000%)
SS G 1: 0 ( 0.000%)
SS G 2: 0 ( 0.000%)
Total: 0

=====

Memory Statistics for File at: Tue Apr 5 12:52:12 2022

Total buffers allocated: 0
Total buffers freed: 0
Total buffers released: 0
Total file mempool: 0
Total allocated file mempool: 0
Total freed file mempool: 0
Total released file mempool: 0

Heap Statistics of file:
Total Statistics:
Memory in use: 0 bytes
No of allocs: 0
No of frees: 0

=====
Snort exiting
```