CSE3052 - INFORMATION SECURITY MANAGEMENT

DIGITAL ASSIGNMENT-5

ALOKAM NIKHITHA

19BCE2555

Wireshark

TITLE:

Wireshark Captures

AIM:

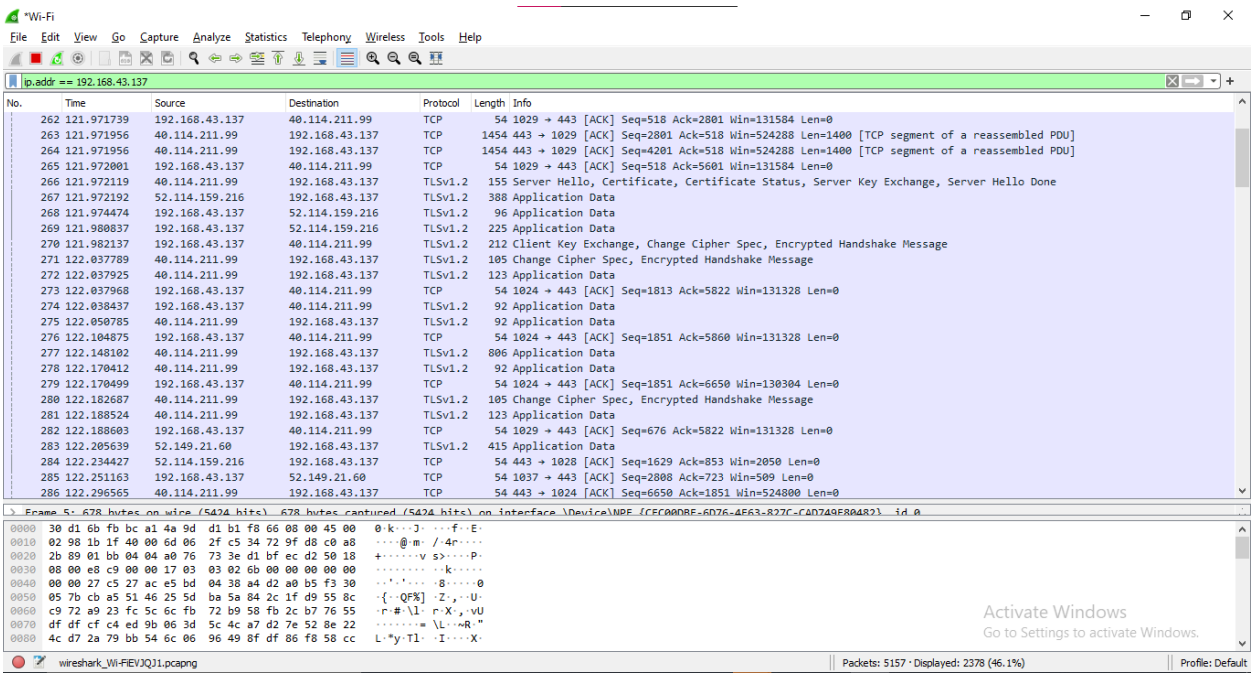
To capture packets with various filters in Wireshark

PROCEDURE and Related Screen shots:

1. Filter traffic on specific IP address

It filters those traffic that have the specified IP address

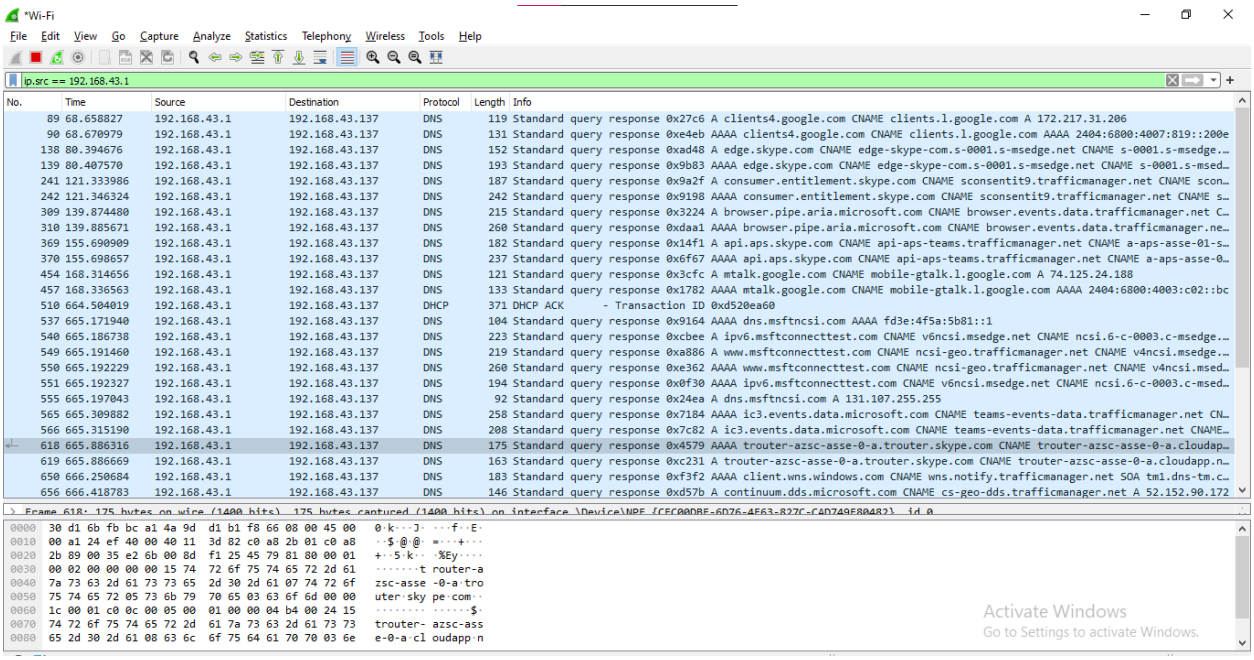
ip.addr == 192.168.43.137



2. Filter by source address

Displays all the packets that have the specified source address

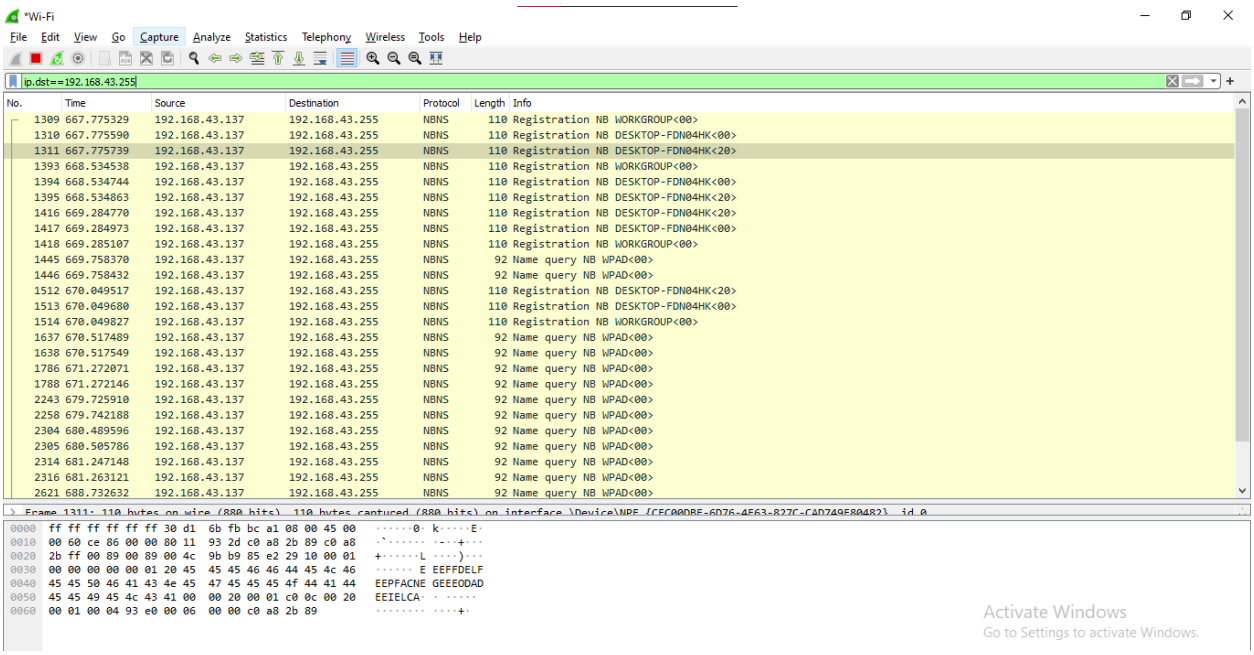
ip.src == 192.168.43.1



3. Filter by destination address

Displays all the packets that have the specified destination address

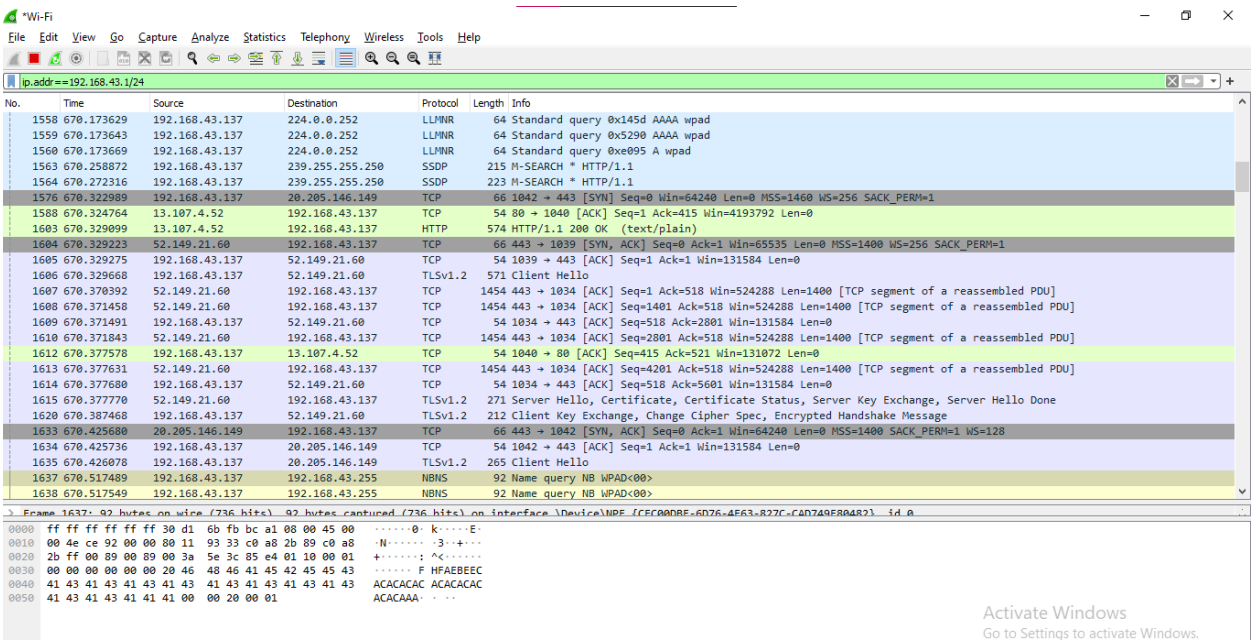
ip.dst==192.168.43.255



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:

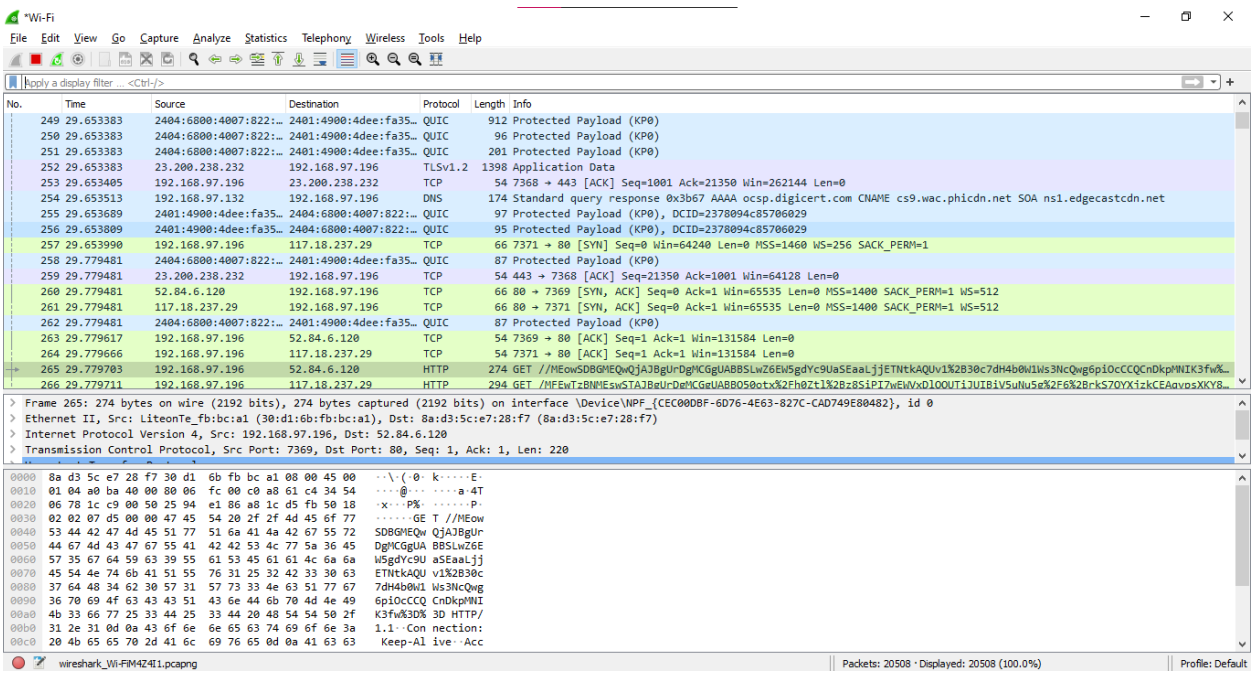
ip.addr==192.168.43.1/24

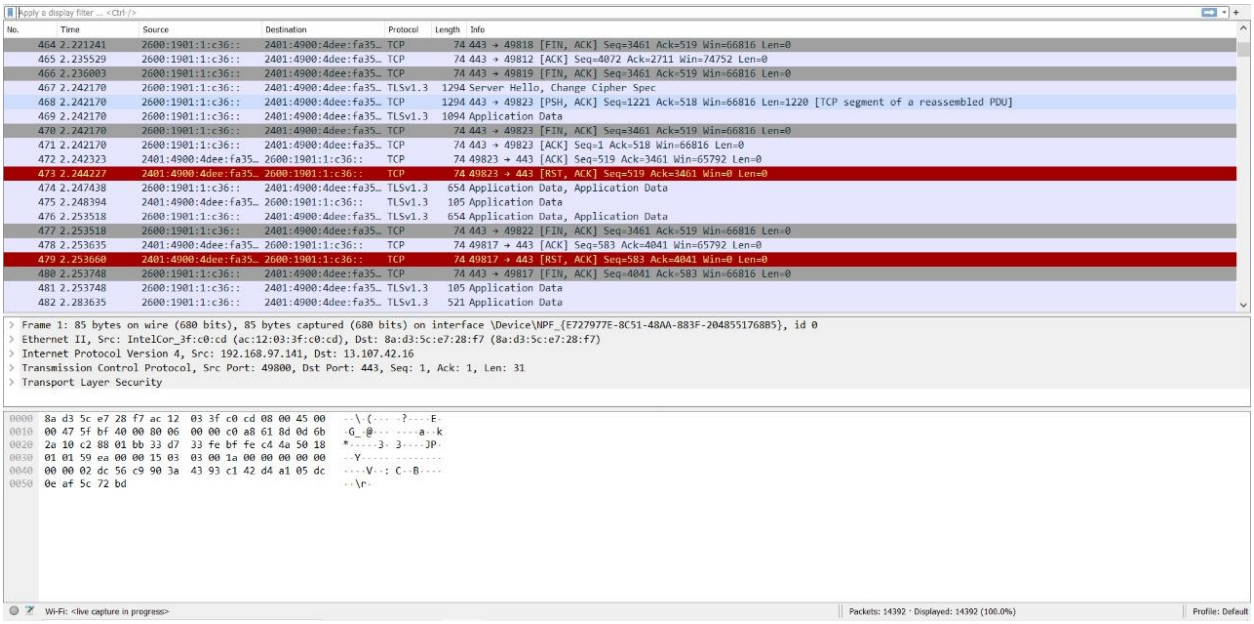


5. Show all the packets

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

ALL PACKETS:





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.

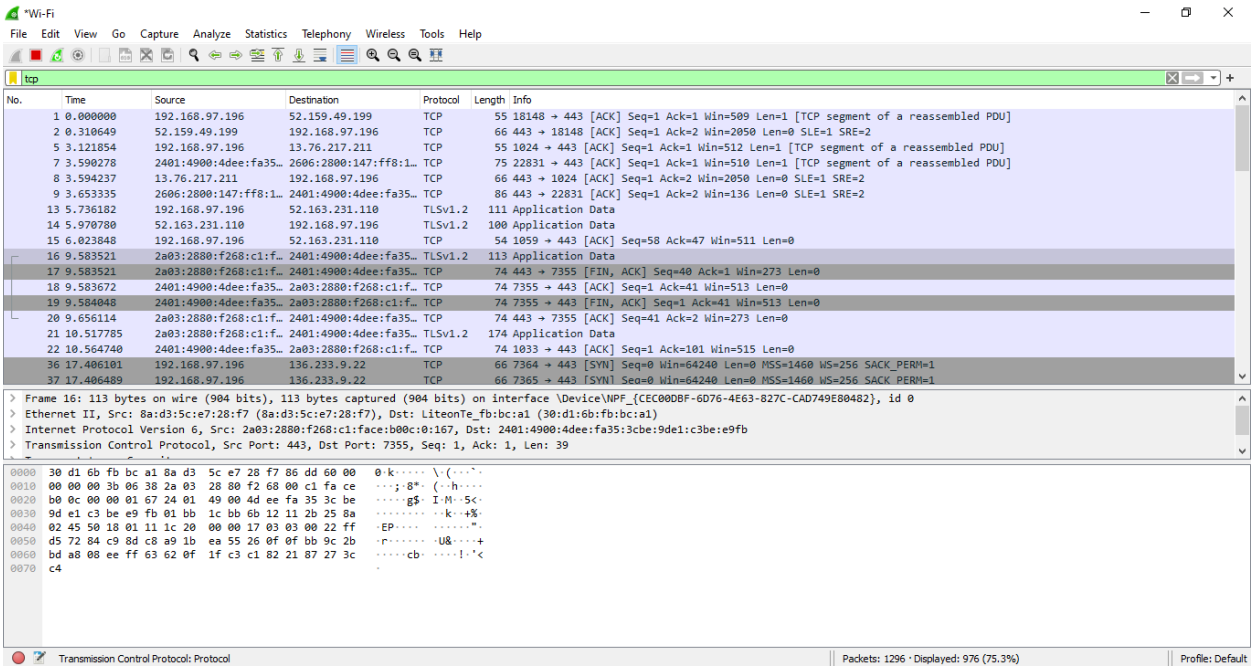
In the snippet we can see that there are few TCP packets colored in black. These are incorrect transmissions. In the first transmission we can see the error message of incorrect acknowledgement. This implies that the TCP packet didn't satisfy the error check and control scheme. They seem to be a dirty 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.

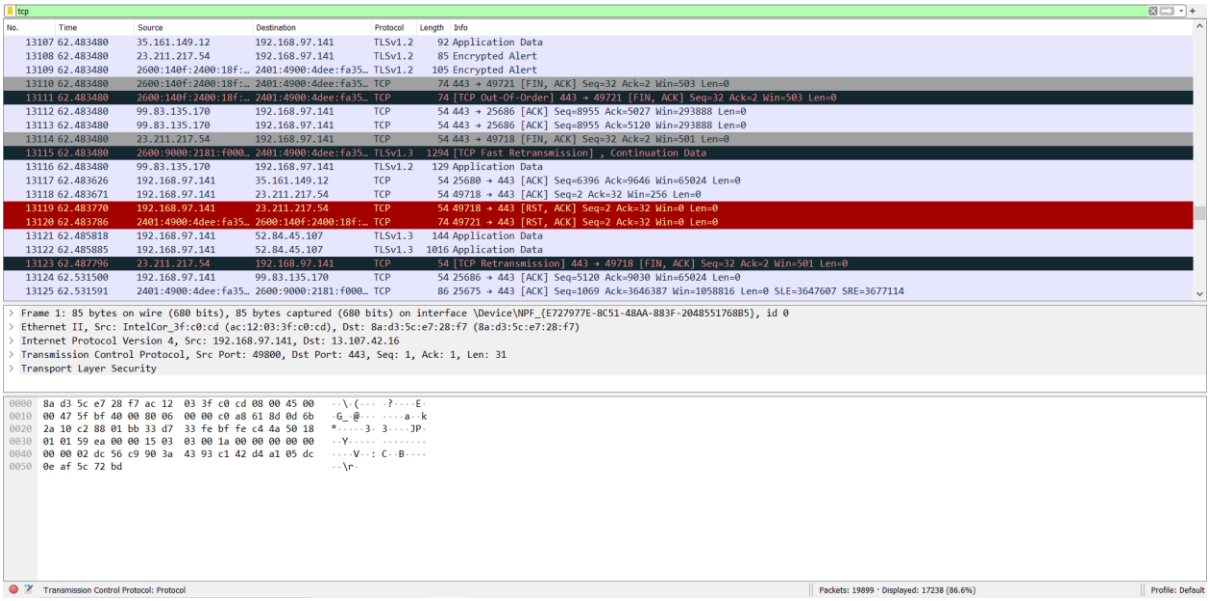
Next, we can see yet another TCP packet colored in black. This is a packet again being retransmitted because the sender didn't receive an acknowledgment of it while transmitting it.

In our second screenshot we can see that two of the TCP packets are colored in red. The message here is [RST, ACK]. This implies that the connection is being reset and being halted. It ends a TCP session. The packet is acknowledging the previous packet stream and RST is used to reset the connection.

6. TCP

TCP stands for Transmission Control Protocol. It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP.





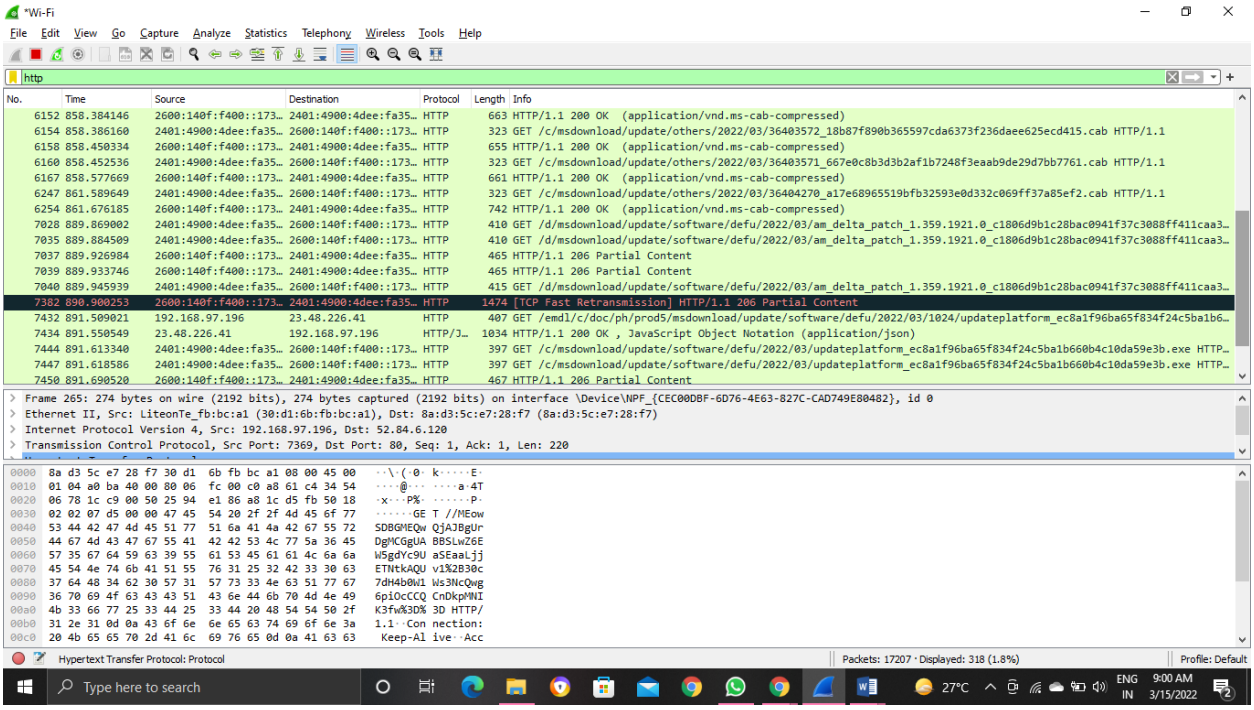
Only TCP packets have been blocked in this case. We can see that [ACK] is used to acknowledge these packets once again. We also retrieve the length of each packet, which varies from 54 bytes to 1474 bytes in our case.

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



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 HTT 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

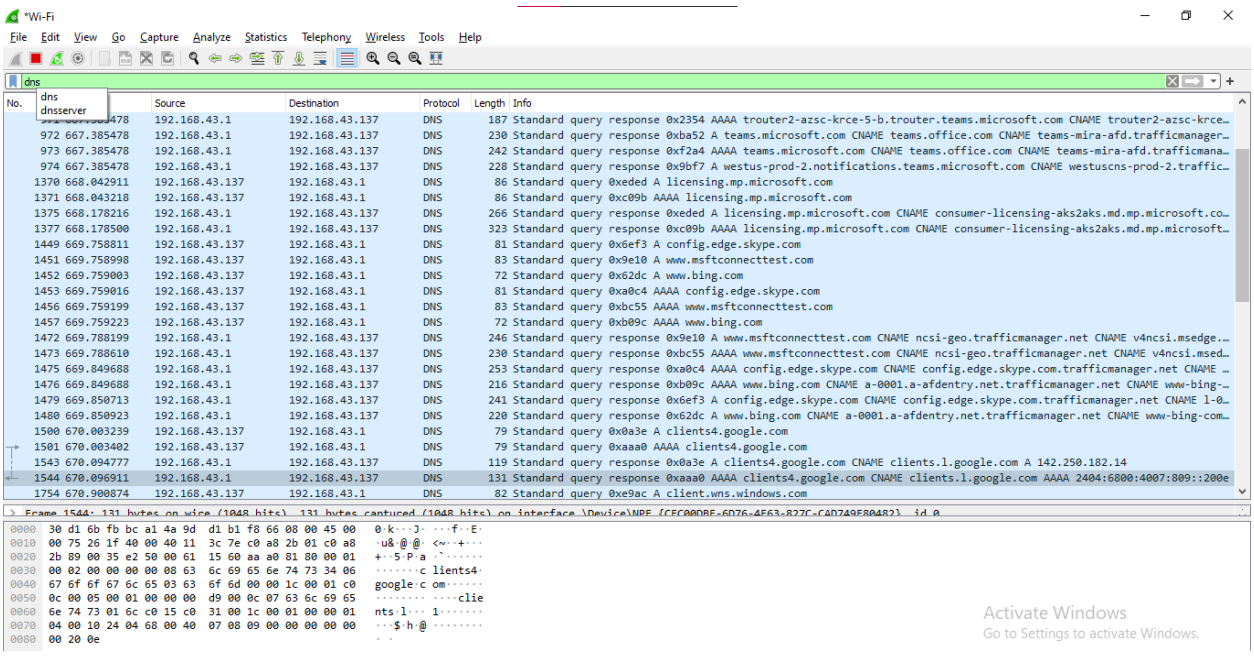
current page.This could be used, for example, when a wiki site's "save and continue editing" feature is implemented. The page would be saved using a PUT request, and the 204 No content response would be sent to signal that the editor should not be replaced by another page.

8. Filter traffic based on protocol

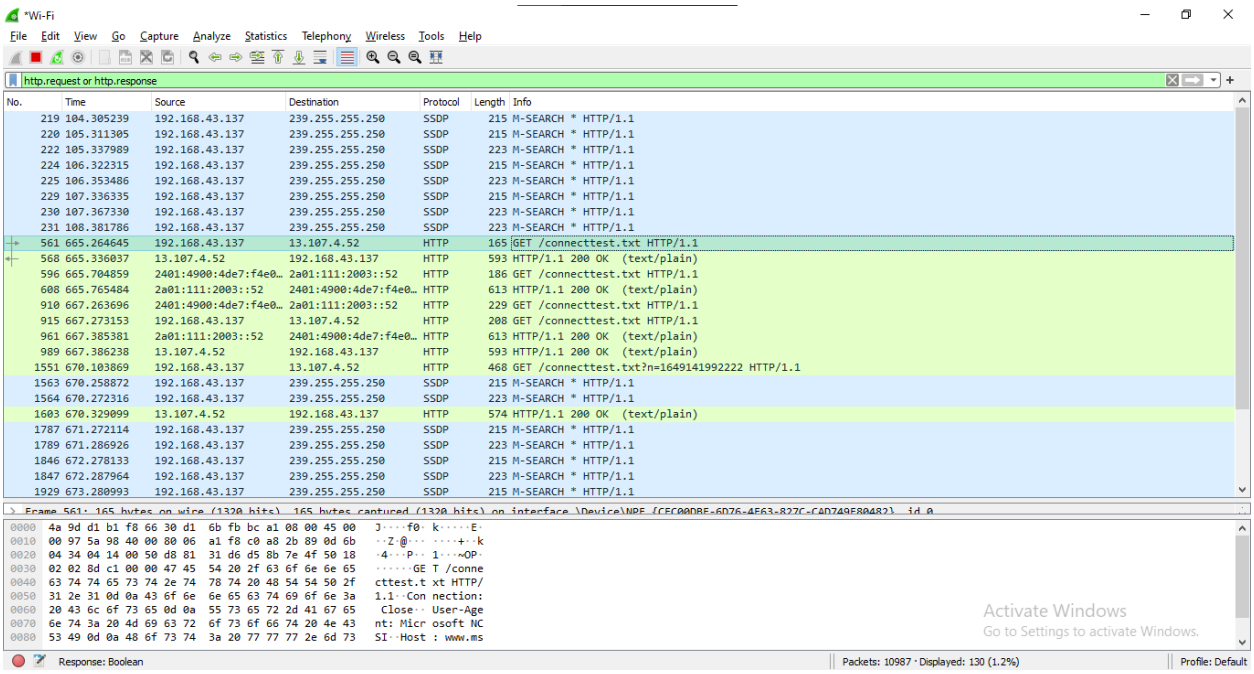
DNS

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.

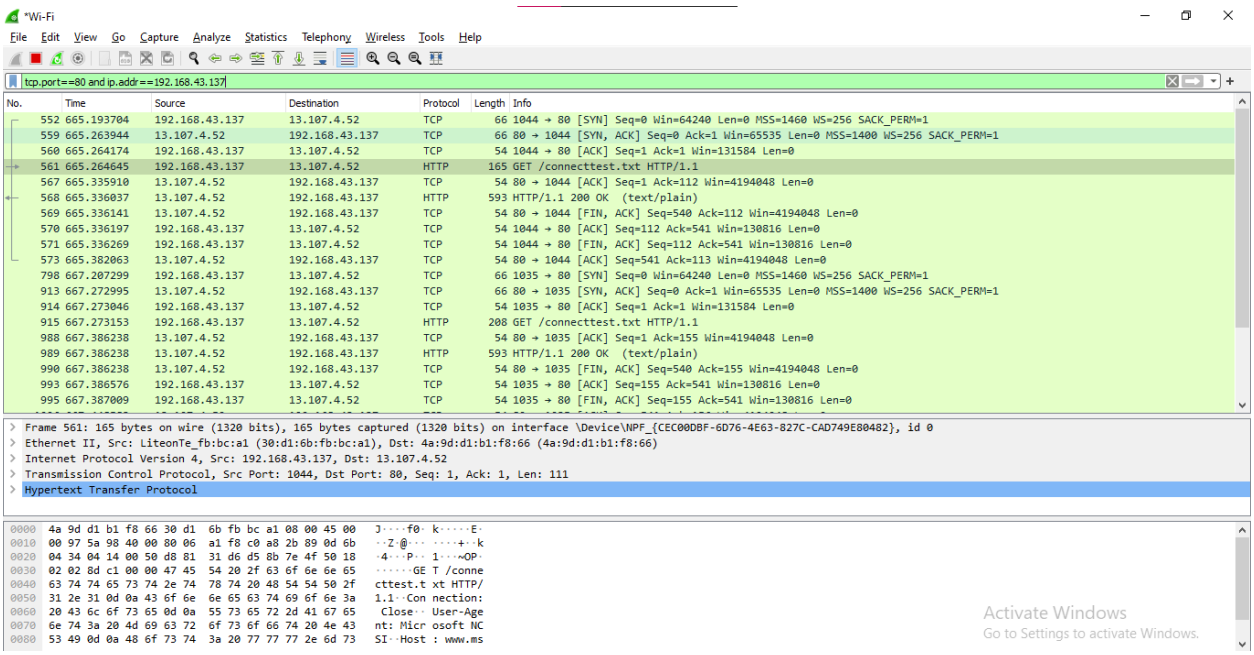
Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).



9. http.request or http.response



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



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:

· Procedure 19BCE2555

→ Download Short from the snort.org website

→ Download Rules. You must register to get the rules and paste the rules in C:\Snort\~~bin~~\Rules · afte executing snort in your PC.

→ Double click .exe to install snort. This will install snort in the C:\ Snort" folder. It is important to have WinPcap installed.

→ Extract the Rule files from zip file downloaded.

→ Copy all files and save in C:\Snort\Rules folder

→ Copy " snort.conf" file from the "etc" folder of extracted folder. You must paste in "C:\Snort\etc" folder.

→ Open cmd and navigate to "C:\Snort\bin" folder

→ To start (execute) snort in sniffer mode use the command: snort -dev -i 3 '-i' indicates interface. '-dev' to run snort to capture packets on word.

To check interface list use snort -W

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

```
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

```
Command Prompt - snort  -dev -i 3

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 ==--

   ,,_     -*> 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=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! <*-
  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

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{ECE706EE-4EE9-49D6-BCBE-22AE47E5ABD4}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{D41A1C3D-7D02-4E4B-A7D7-02B560FBDB7C}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{F07AE100-36C8-4063-B0A1-78CE68C8FF7D}      WAN Miniport (IP)
    4   30:D1:6B:FB:BC:A2       0000:0000:fe80:0000:0000:0000:c997:41d8 \Device\NPF_{C6E0FE47-D127-4F48-BD86-C7B7C751693F}      Bluetooth Device (Personal Area Network)

    5   30:D1:6B:FB:BC:A1       0000:0000:2401:4900:234b:b7ec:bc0a:7858 \Device\NPF_{CEC00DBF-6D76-4E63-827C-CAD749E80482}      Qualcomm Atheros QCA9377 Wireless Networ
k Adapter
    6   42:D1:6B:FB:BC:A1       0000:0000:fe80:0000:0000:0000:e8b0:a6a1 \Device\NPF_{7354E09C-5621-4675-A32C-87F69382E94F}      Microsoft Wi-Fi Direct Virtual Adapter #
2
    7   32:D1:6B: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:fe80:0000:0000:0000: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.

Command Prompt

```
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%)
```

```
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;)
```


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%)
     S5 G 1:            0 (  0.000%)
     S5 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
```