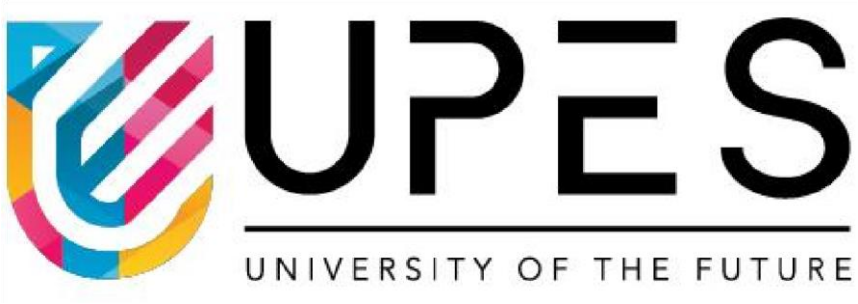


School of Computer Science

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
DEHRADUN, UTTARAKHAND

IT Network Security Lab File

5th Semester

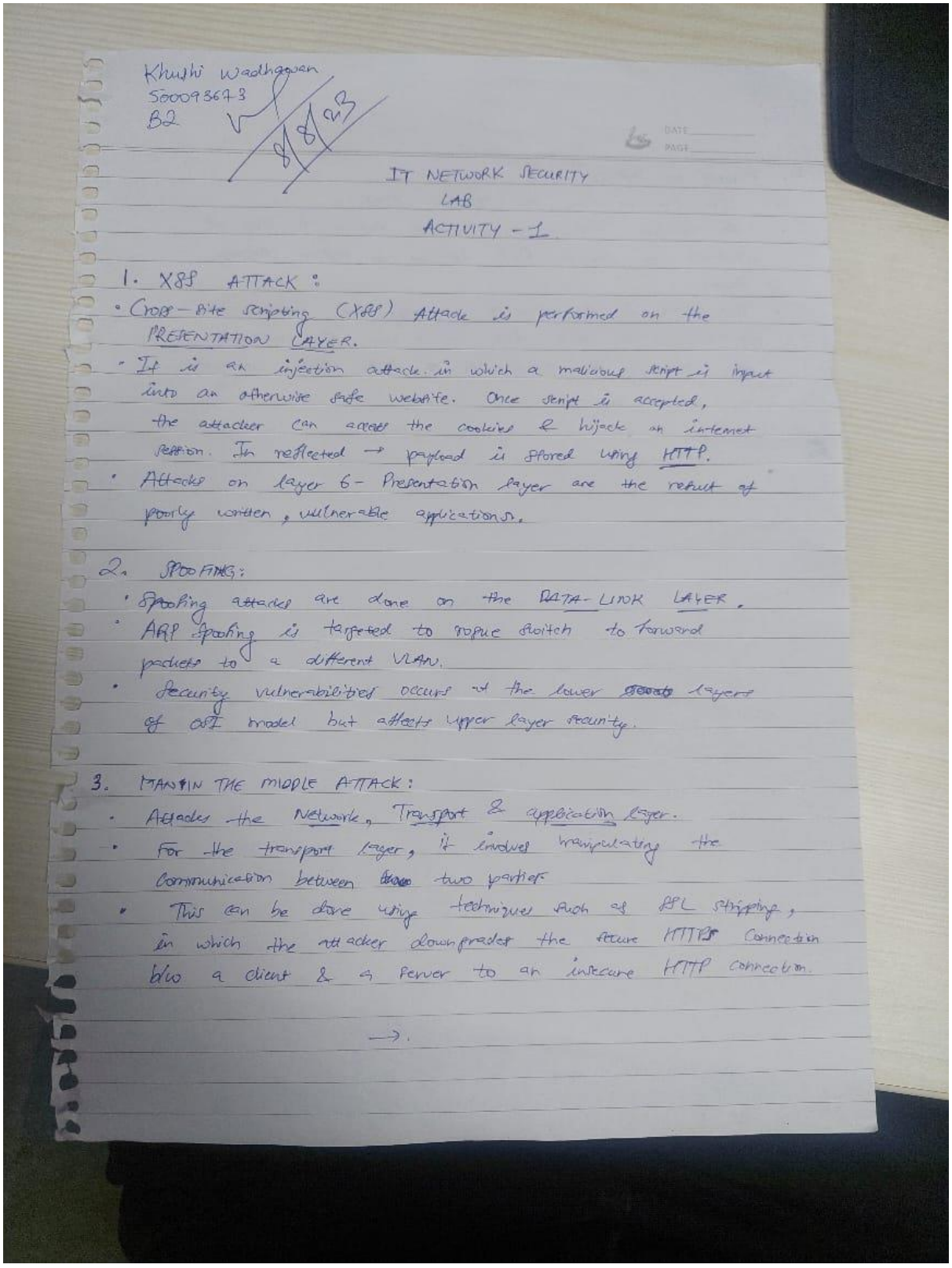
Submitted by:

Khushi Wadhawan
Sap id: 500093673
Btech CSE CSF
Batch: 2

Submitted to:

Mr. Keshav Sinha

EXPERIMENT 1



Khushi Wadhgaonkar
50009367-3
B2

DATE
PAGE

IT NETWORK SECURITY
LAB
ACTIVITY - 1

1. XSS ATTACK :
- Cross-Site Scripting (XSS) Attack is performed on the PRESENTATION LAYER.
- It is an injection attack in which a malicious script is input into an otherwise safe website. Once script is accepted, the attacker can access the cookies & hijack an internet session. In reflected → payload is stored using HTTP.
- Attacks on layer 6 - Presentation layer are the result of poorly written, vulnerable applications.

2. SPOOFING :
- Spoofing attacks are done on the DATA-LINK LAYER.
- ARP spoofing is targeted to rogue switch to forward packets to a different VLAN.
- Security vulnerabilities occurs at the lower layers of OSI model but affects upper layer security.

3. MAN IN THE MIDDLE ATTACK :
- Attacks the Network, Transport & application layer.
- For the transport layer, it involves manipulating the communication between two parties.
- This can be done using techniques such as SSL stripping, in which the attacker downgrades the secure HTTPS connection b/w a client & a server to an insecure HTTP connection.

→.

1) C:\> ipconfig /all

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-D9346HME
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : DDN.UPES.AC.IN

Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-15
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c8e6:d6bf:1e5d:d12d%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 1040842791
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-39-73-12-FC-34-97-96-92-9E
   NetBIOS over Tcpip. . . . . . . . : Enabled

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TAP-ProtonVPN Windows Adapter V9
   Physical Address. . . . . . . . . : 00-FF-43-58-8D-BA
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : DA-C0-A6-59-0B-65
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   Physical Address. . . . . . . . . : FA-C0-A6-59-0B-65
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:
```

```
C:\WINDOWS\system32\cmd.  X  +  v                                  -  □  X

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : DDN.UPES.AC.IN
   Description . . . . . . . . . . . : Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
   Physical Address. . . . . . . . . : D8-C0-A6-59-0B-65
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::84c0:b452:d779:fc55%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.12.29.181(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Lease Obtained. . . . . . . . . . : Tuesday, August 22, 2023 3:05:12 PM
   Lease Expires . . . . . . . . . . : Tuesday, August 29, 2023 3:05:28 PM
   Default Gateway . . . . . . . . . : 10.12.1.1
   DHCP Server . . . . . . . . . . . : 10.2.1.8
   DHCPv6 IAID . . . . . . . . . . . : 366526630
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-39-73-12-FC-34-97-96-92-9E
   DNS Servers . . . . . . . . . . . : 10.2.1.60
                                       10.2.1.61
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ddn.upes.ac.in
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : FC-34-97-96-92-9E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

2) C:\> Gpresult

```
GPRESULT [/S system [/U username [/P [password]]]] [/SCOPE scope]
         [/USER targetusername] [/R | /V | /Z]

Description:
    This command line tool displays the Resultant Set of Policy (RSoP)
    information for a target user and computer.

Parameter List:
    /S        system           Specifies the remote system to connect to.

    /U        [domain\]user    Specifies the user context under which the
                               command should run.
    /P        [password]       Specifies the password for the given user
                               context. Prompts for input if omitted.
    /SCOPE    scope            Specifies whether the user or the
                               computer settings need to be displayed.
                               Valid values: "USER", "COMPUTER".

    /USER     [domain\]user    Specifies the user name for which the
                               RSoP data is to be displayed.

    /R                         Displays RSoP summary data.

    /V                         Specifies that verbose information should
                               be displayed. Verbose information provides
                               additional detailed settings that have
                               been applied with a precedence of 1.

    /Z                         Specifies that the super-verbose
                               information should be displayed. Super-
                               verbose information provides additional
                               detailed settings that have been applied
                               with a precedence of 1 and higher. This
                               allows you to see if a setting was set in
                               multiple places. See the Group Policy
                               online help topic for more information.

    /?                         Displays this help message.

Examples:
    GPRESULT /R
    GPRESULT /USER targetusername /V
    GPRESULT /S system /USER targetusername /SCOPE COMPUTER /Z
    GPRESULT /S system /U username /P password /SCOPE USER /V
```

3) Ipconfig /flushdns

```
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

4) nbtstat -a <system name>

```
Ethernet 4:
Node IpAddress: [192.168.56.1] Scope Id: []

    Host not found.

Local Area Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

Wi-Fi:
Node IpAddress: [10.12.29.181] Scope Id: []

    Host not found.

Local Area Connection* 1:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

Local Area Connection* 12:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.
```

5) nbtstat -R

```
    Failed to Purge the NBT Remote Cache Table.
    Failed to Purge the NBT Remote Cache Table.
    Failed to Purge the NBT Remote Cache Table.
    Failed to Purge the NBT Remote Cache Table.
    Failed to Purge the NBT Remote Cache Table.
    Failed to Purge the NBT Remote Cache Table.
    Failed to Purge the NBT Remote Cache Table.
```

```
C:\Windows\System32>nbtstat -R
    Successful purge and preload of the NBT Remote Cache Name Table.
```

6) nbtstat -n

```
Ethernet 4:
Node IpAddress: [192.168.56.1] Scope Id: []

               NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    LAPTOP-D9346HME<20>  UNIQUE      Registered
    LAPTOP-D9346HME<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

Local Area Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Wi-Fi:
Node IpAddress: [10.12.29.181] Scope Id: []

               NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    LAPTOP-D9346HME<20>  UNIQUE      Registered
    LAPTOP-D9346HME<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

Local Area Connection* 1:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Local Area Connection* 12:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache
```

7) nbtstat -r

```
    NetBIOS Names Resolution and Registration Statistics
    ----------------------------------------------------

    Resolved By Broadcast     = 0
    Resolved By Name Server   = 0

    Registered By Broadcast   = 21
    Registered By Name Server = 0
```

8) nbtstat -ab

```
C:\Windows\System32>nbtstat -ab

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.
```

9) nbtstat -an

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1042           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1043           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5426           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9012           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9013           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9014           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:45906          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING
  TCP    10.12.29.181:139       0.0.0.0:0              LISTENING
  TCP    10.12.29.181:55773     20.198.118.190:443     CLOSE_WAIT
  TCP    10.12.29.181:55826     180.149.52.200:443     ESTABLISHED
  TCP    10.12.29.181:55866     180.149.52.217:443     CLOSE_WAIT
  TCP    10.12.29.181:55868     180.149.52.217:443     CLOSE_WAIT
  TCP    10.12.29.181:55869     180.149.52.217:443     CLOSE_WAIT
  TCP    10.12.29.181:55870     180.149.52.217:443     CLOSE_WAIT
  TCP    10.12.29.181:55877     180.149.52.217:443     CLOSE_WAIT
  TCP    10.12.29.181:55878     180.149.52.217:443     CLOSE_WAIT
  TCP    10.12.29.181:55879     180.149.52.217:443     CLOSE_WAIT
  TCP    10.12.29.181:55880     152.195.38.76:80       CLOSE_WAIT
  TCP    10.12.29.181:55884     204.79.197.222:443     ESTABLISHED
  TCP    10.12.29.181:55917     52.109.56.91:443       ESTABLISHED
  TCP    10.12.29.181:55938     20.198.119.143:443     TIME_WAIT
  TCP    10.12.29.181:55989     10.12.29.181:45906     TIME_WAIT
  TCP    10.12.29.181:55996     184.87.104.37:443      ESTABLISHED
  TCP    10.12.29.181:55997     173.223.89.166:443     ESTABLISHED
  TCP    10.12.29.181:55998     20.198.118.190:443     ESTABLISHED
  TCP    10.12.29.181:56003     173.223.89.166:443     ESTABLISHED
  TCP    10.12.29.181:56006     173.223.89.166:443     ESTABLISHED
  TCP    10.12.29.181:56007     173.223.89.166:443     ESTABLISHED
  TCP    10.12.29.181:56008     173.223.89.166:443     ESTABLISHED
  TCP    10.12.29.181:56011     13.78.111.198:443      ESTABLISHED
  TCP    10.12.29.181:56021     52.71.125.138:443      ESTABLISHED
  TCP    10.12.29.181:56024     20.197.103.14:443      SYN_SENT
  TCP    10.12.29.181:56025     40.74.98.194:443       ESTABLISHED
  TCP    10.12.29.181:56026     118.215.80.43:443      SYN_SENT
  TCP    10.12.29.181:56027     118.215.80.43:443      SYN_SENT
  TCP    127.0.0.1:1042         127.0.0.1:54982        ESTABLISHED
```

10) net use

```
New connections will be remembered.

There are no entries in the list.
```

11) net user

```
User accounts for \\LAPTOP-D9346HME

-------------------------------------------------------------------------------
Administrator            akshat kapil             DefaultAccount
Guest                    WDAGUtilityAccount
The command completed successfully.
```

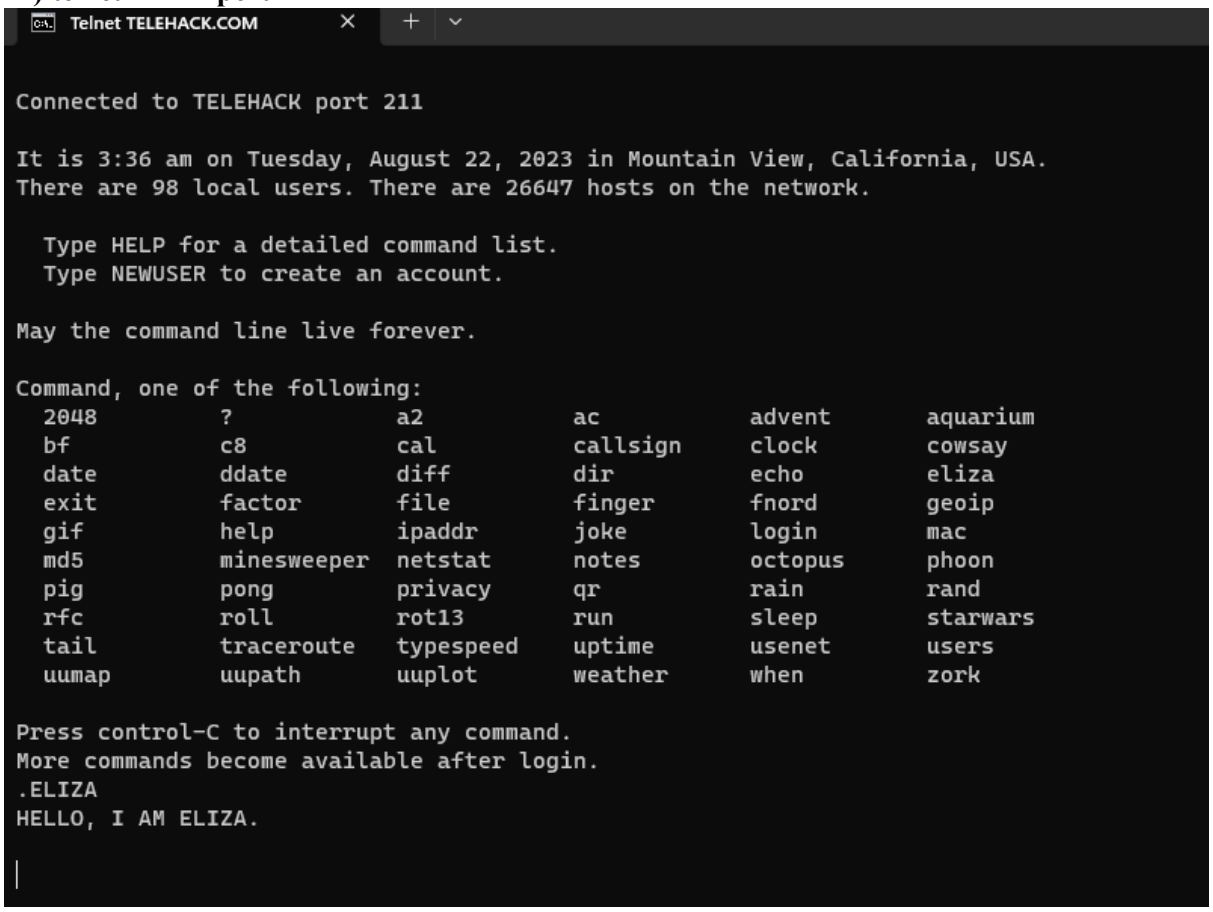
12) ping -a <IP address>

```
Pinging dsldevice.lan [192.168.1.1] with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=53ms TTL=64
Reply from 192.168.1.1: bytes=32 time=31ms TTL=64
Reply from 192.168.1.1: bytes=32 time=97ms TTL=64
Reply from 192.168.1.1: bytes=32 time=215ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 215ms, Average = 99ms
```

13) set L

```
LOGONSERVER=\\LAPTOP-D9346HME
```

14) telnet <IP> <port>



Create a batch file of the following commands and execute them on your VM.

1. Information Gathering done by Hacker Group 'Waterbug'

- Systeminfo
- net view
- net view /domain
- tasklist /v
- gpresult /z
- netstat –nao
- ipconfig /all
- arp –a
- net share
- net use
- net user administrator
- net user /domain
- net user administrator /domain
- tasklist /fi
- dir %systemdrive%\Users*.*
- dir %userprofile%\AppData\Roaming\Microsoft\Windows\Recent*.*
- dir %userprofile%\Desktop*.*

```
Host Name:                 LAPTOP-D9346HME
OS Name:                   Microsoft Windows 11 Home Single Language
OS Version:                10.0.22621 N/A Build 22621
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          akshat kapil
Registered Organization:   N/A
Product ID:                00327-36286-75987-AAOEM
Original Install Date:     2/13/2023, 10:22:32 AM
System Boot Time:          9/12/2023, 10:34:37 PM
System Manufacturer:       ASUSTeK COMPUTER INC.
System Model:              ASUS TUF Gaming A17 FA706IH_FA706IH
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 96 Stepping 1 AuthenticAMD ~3000 Mhz
BIOS Version:              American Megatrends Inc. FA706IH.316, 3/12/2021
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     7,599 MB
Available Physical Memory: 1,695 MB
Virtual Memory: Max Size:  20,911 MB
Virtual Memory: Available: 9,459 MB
Virtual Memory: In Use:    11,452 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-D9346HME
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB5028948
                           [02]: KB5029921
                           [03]: KB5012170
                           [04]: KB5030219
                           [05]: KB5028756
Network Card(s):           5 NIC(s) Installed.
                           [01]: TAP-ProtonVPN Windows Adapter V9
                                 Connection Name: Local Area Connection
                                 Status:          Media disconnected
                           [02]: Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
                                 Connection Name: Wi-Fi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.1.1
                                 IP address(es)
                                 [01]: 192.168.1.13
                                 [02]: fe80::84e0:b452:d779:fc55
                                 [03]: 2401:4900:1c62:845:3c8d:3718:e038:ba23
                                 [04]: 2401:4900:1c62:845:c7b0:7970:b886:b897
                           [03]: Realtek PCIe GbE Family Controller
```

C:\WINDOWS\system32\cmd.

```
========================= ======== ================ =========== ============ ============== ============================================ ============ ========================================================
====================
System Idle Process              0 Services                   0          8 K Unknown         NT AUTHORITY\SYSTEM                        162:10:48 N/A

System                           4 Services                   0      7,544 K Unknown         N/A                                          0:10:22 N/A

Registry                       180 Services                   0     50,724 K Unknown         N/A                                          0:00:02 N/A

smss.exe                       676 Services                   0      1,120 K Unknown         N/A                                          0:00:00 N/A

csrss.exe                      780 Services                   0      6,472 K Unknown         N/A                                          0:00:02 N/A

wininit.exe                   1168 Services                   0      7,004 K Unknown         N/A                                          0:00:00 N/A

services.exe                  1244 Services                   0     14,780 K Unknown         N/A                                          0:00:13 N/A

lsass.exe                     1328 Services                   0     28,820 K Unknown         N/A                                          0:00:37 N/A

svchost.exe                   1456 Services                   0     35,008 K Unknown         N/A                                          0:00:17 N/A

fontdrvhost.exe               1492 Services                   0      3,428 K Unknown         N/A                                          0:00:00 N/A

svchost.exe                   1600 Services                   0     27,096 K Unknown         N/A                                          0:00:49 N/A

svchost.exe                   1644 Services                   0      7,036 K Unknown         N/A                                          0:00:01 N/A

svchost.exe                   1812 Services                   0      6,848 K Unknown         N/A                                          0:00:00 N/A

svchost.exe                   1896 Services                   0      5,492 K Unknown         N/A                                          0:00:00 N/A

svchost.exe                   1908 Services                   0     11,836 K Unknown         N/A                                          0:00:03 N/A

svchost.exe                   1968 Services                   0     13,760 K Unknown         N/A                                          0:00:00 N/A

svchost.exe                   1980 Services                   0     11,960 K Unknown         N/A                                          0:00:00 N/A

svchost.exe                   1996 Services                   0      6,324 K Unknown         N/A                                          0:00:00 N/A

svchost.exe                   1192 Services                   0     16,208 K Unknown         N/A                                          0:00:01 N/A

svchost.exe                   2092 Services                   0     19,248 K Unknown         N/A                                          0:00:13 N/A

svchost.exe                   2184 Services                   0     20,228 K Unknown         N/A                                          0:00:04 N/A

svchost.exe                   2212 Services                   0     14,748 K Unknown         N/A                                          0:00:00 N/A

svchost.exe                   2484 Services                   0     19,588 K Unknown         N/A                                          0:00:23 N/A

svchost.exe                   2644 Services                   0     17,408 K Unknown         N/A                                          0:00:03 N/A

svchost.exe                   2676 Services                   0     14,020 K Unknown         N/A                                          0:00:00 N/A
```

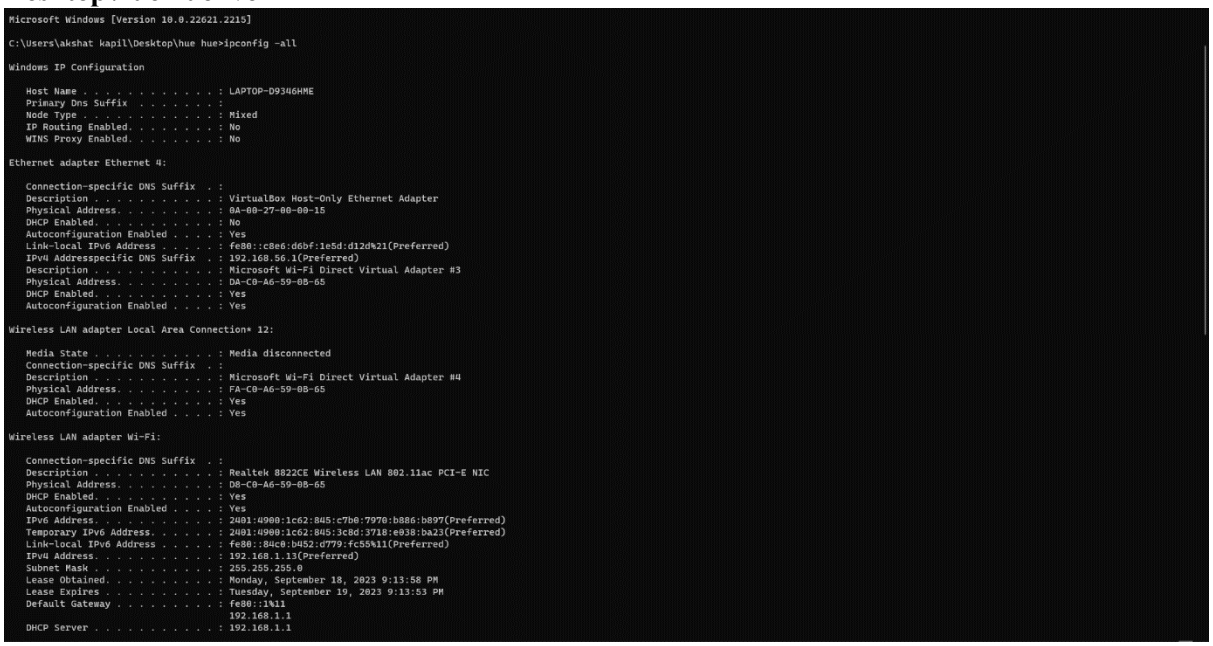
Documents>gpresult /z

```
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on  9/ 19/ 2023 at 12:23:15 AM


RSOP data for LAPTOP-D9346HME\akshat kapil on LAPTOP-D9346HME : Logging Mode
-----------------------------------------------------------------------------

OS Configuration:            Standalone Workstation
OS Version:                  10.0.22621
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\akshat kapil
Connected over a slow link?: No


USER SETTINGS
--------------

    Last time Group Policy was applied: 9/18/2023 at 9:13:53 PM
    Group Policy was applied from:      N/A
    Group Policy slow link threshold:   500 kbps
```

2. Information Gathering done by Hacker Group 'Appleworm/Lazarus'

- hostname
- whoami
- ver
- ipconfig -all
- ping www.google.com
- query user
- net user
- net view
- net view /domain
- reg query \"HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\"
- tasklist /svc
- netstat -ano | find \TCP\
- msdtc [IP] [port]

Desktop\hue hue>ver



```
Microsoft Windows [Version 10.0.22621.2215]

C:\Users\akshat kapil\Desktop\hue hue>ipconfig -all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-D9346HME
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-15
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c8e6:d6bf:1e5d:d12d%21(Preferred)
   IPv4 Addresspecific DNS Suffix  . : 192.168.56.1(Preferred)
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : DA-C0-A6-59-0B-65
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   Physical Address. . . . . . . . . : FA-C0-A6-59-0B-65
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
   Physical Address. . . . . . . . . : D8-C0-A6-59-0B-65
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2401:4900:1c62:845:c7b0:7970:b886:b897(Preferred)
   Temporary IPv6 Address. . . . . . : 2401:4900:1c62:845:3c8d:3718:e038:ba23(Preferred)
   Link-local IPv6 Address . . . . . : fe80::84c0:b452:d779:fc55%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.13(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, September 18, 2023 9:13:58 PM
   Lease Expires . . . . . . . . . . : Tuesday, September 19, 2023 9:13:53 PM
   Default Gateway . . . . . . . . . : fe80::1%11
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
```

Desktop\hue hue>ping www.google.com

```
Pinging www.google.com [2404:6800:4002:81e::2004] with 32 bytes of data:
Reply from 2404:6800:4002:81e::2004: time=19ms
Reply from 2404:6800:4002:81e::2004: time=32ms
Reply from 2404:6800:4002:81e::2004: time=22ms
Reply from 2404:6800:4002:81e::2004: time=40ms

Ping statistics for 2404:6800:4002:81e::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 40ms, Average = 28ms

C:\Users\akshat kapil\Desktop\hue hue>query user
'query' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\akshat kapil\Desktop\hue hue>net user

User accounts for \\LAPTOP-D9346HME

-------------------------------------------------------------------------------
Administrator            akshat kapil             DefaultAccount
Guest                    WDAGUtilityAccount
The command completed successfully.
```

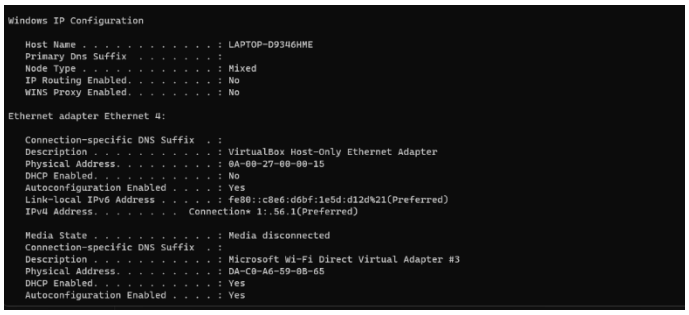
Desktop\hue hue>ner user

```
User accounts for \\LAPTOP-D9346HME

-------------------------------------------------------------------------------
Administrator            akshat kapil             DefaultAccount
Guest                    WDAGUtilityAccount
The command completed successfully.
```

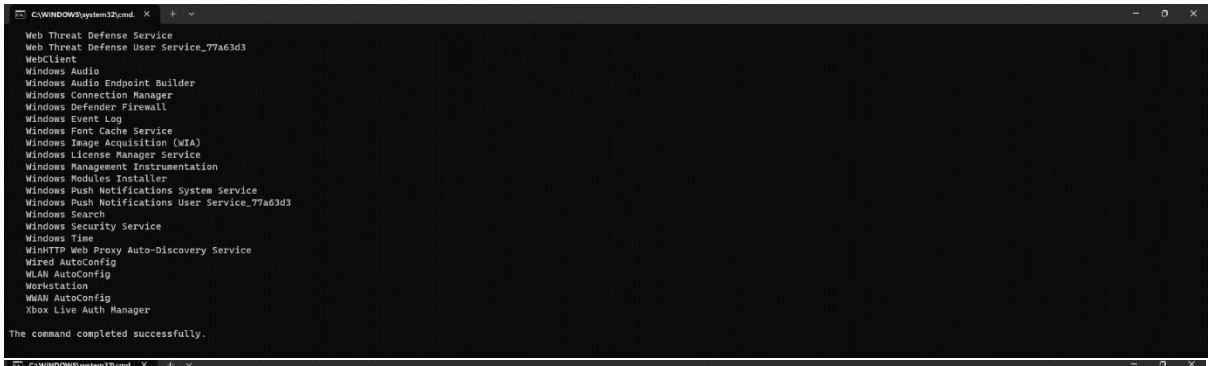
3. Information Gathering done by Hacker Group 'Billbug'

- net user
- ipconfig /all
- net start
- systeminfo
- gpresult

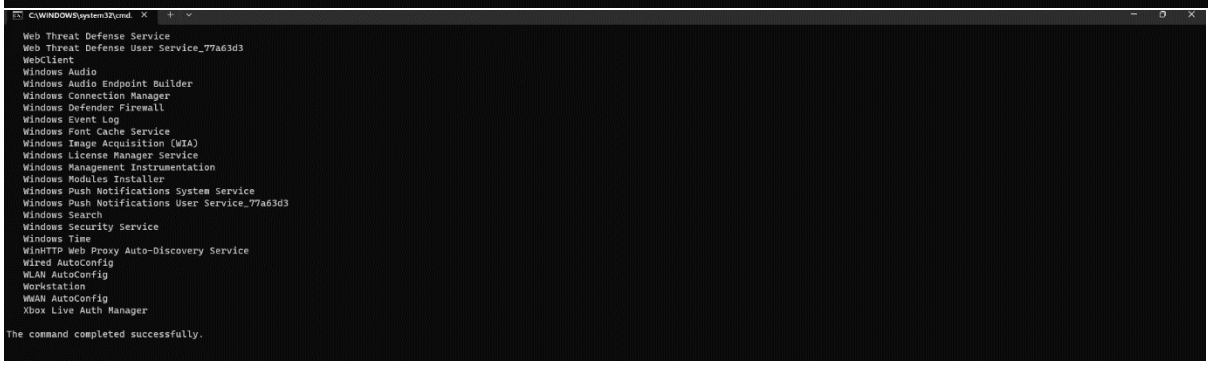
Desktop\hue hue>ipconfig /all



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-D9346HME
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-15
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c8e6:d6bf:1e5d:d12d%21(Preferred)
   IPv4 Address. . . . . . . . . . . : Connection* 1:.56.1(Preferred)

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : DA-C0-A6-59-0B-65
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```



```
C:\WINDOWS\system32\cmd.

   Web Threat Defense Service
   Web Threat Defense User Service_77a63d3
   WebClient
   Windows Audio
   Windows Audio Endpoint Builder
   Windows Connection Manager
   Windows Defender Firewall
   Windows Event Log
   Windows Font Cache Service
   Windows Image Acquisition (WIA)
   Windows License Manager Service
   Windows Management Instrumentation
   Windows Modules Installer
   Windows Push Notifications System Service
   Windows Push Notifications User Service_77a63d3
   Windows Search
   Windows Security Service
   Windows Time
   WinHTTP Web Proxy Auto-Discovery Service
   Wired AutoConfig
   WLAN AutoConfig
   Workstation
   WWAN AutoConfig
   Xbox Live Auth Manager

The command completed successfully.
```



```
C:\WINDOWS\system32\cmd.

   Web Threat Defense Service
   Web Threat Defense User Service_77a63d3
   WebClient
   Windows Audio
   Windows Audio Endpoint Builder
   Windows Connection Manager
   Windows Defender Firewall
   Windows Event Log
   Windows Font Cache Service
   Windows Image Acquisition (WIA)
   Windows License Manager Service
   Windows Management Instrumentation
   Windows Modules Installer
   Windows Push Notifications System Service
   Windows Push Notifications User Service_77a63d3
   Windows Search
   Windows Security Service
   Windows Time
   WinHTTP Web Proxy Auto-Discovery Service
   Wired AutoConfig
   WLAN AutoConfig
   Workstation
   WWAN AutoConfig
   Xbox Live Auth Manager

The command completed successfully.
```

EXPERIMENT 2

Khushi Wadhawan
50007373
B2

29/8/23

IT NETWORK SECURITY
LAB EXPERIMENT - 2 & 2

Q1.
Ans.
1. TCP
2. TLSv1.2
3. QUIC
4. DNS
5. TLSv1.3
6. OCSP
7. HTTP
8. ARP
9. ICMPv6
10. UDP

Q2.
Ans. HTTP GET - time : 86.696595749
HTTP OK - time : 87.102142223
Time taken - 87.102142223 - 86.696595749

Q3.
Ans. We can see in HTTP GET S.No 31 -
Source : 10.0.2.15 (My computer)
Destination : 44.228.249.3 (Website)

Q4.
Ans. Total no. of packets : 122

1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 9 above.

The following protocols appeared in the protocol column in the unfiltered packet listing window after downloading a webpage:

1. HTTP
2. UDP
3. TCP
4. DNS
5. DHCP
6. TCPv1.2
7. TCP V1.3
8. QUIC
9. SSDP
10. MDNS

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

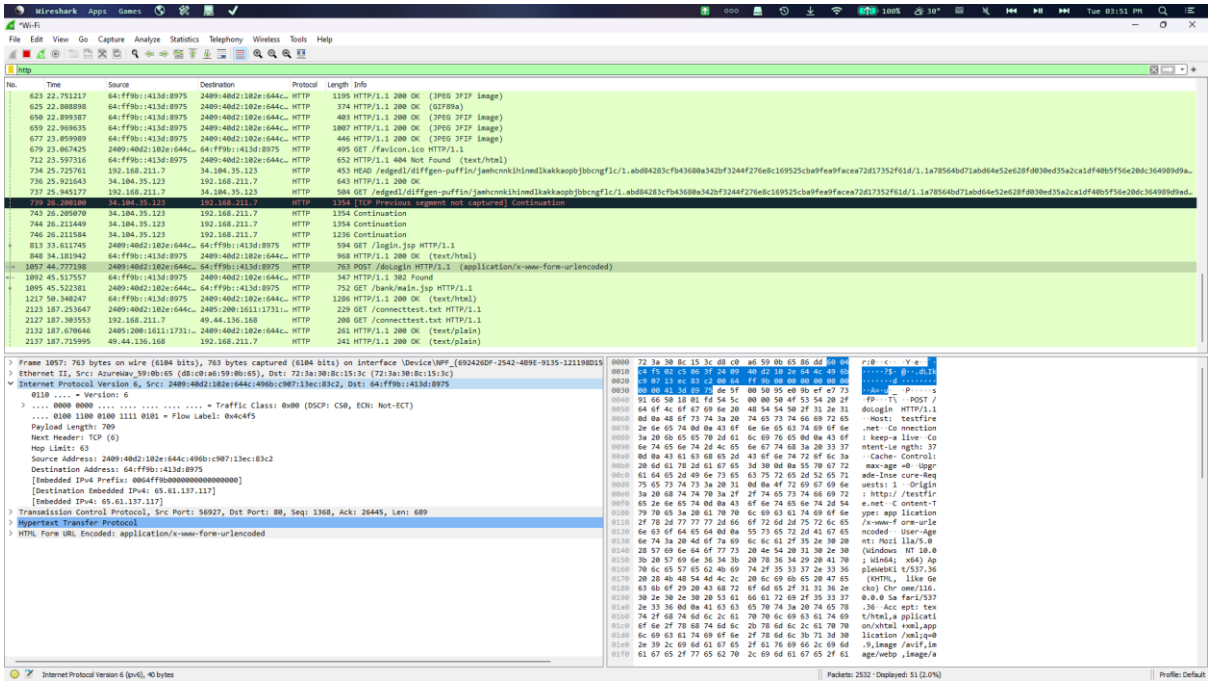
The time the GET packet arrived is 15:45:51.351103000

The same section for the HTTP OK shows an arrival time of 15:46:04.053117000

The difference of these 2 times gives 351103000 - 053117000 = **0.297986 seconds**

3. What is the Internet address (IP address) of the web site your accessed? What is the Internet address of your computer?

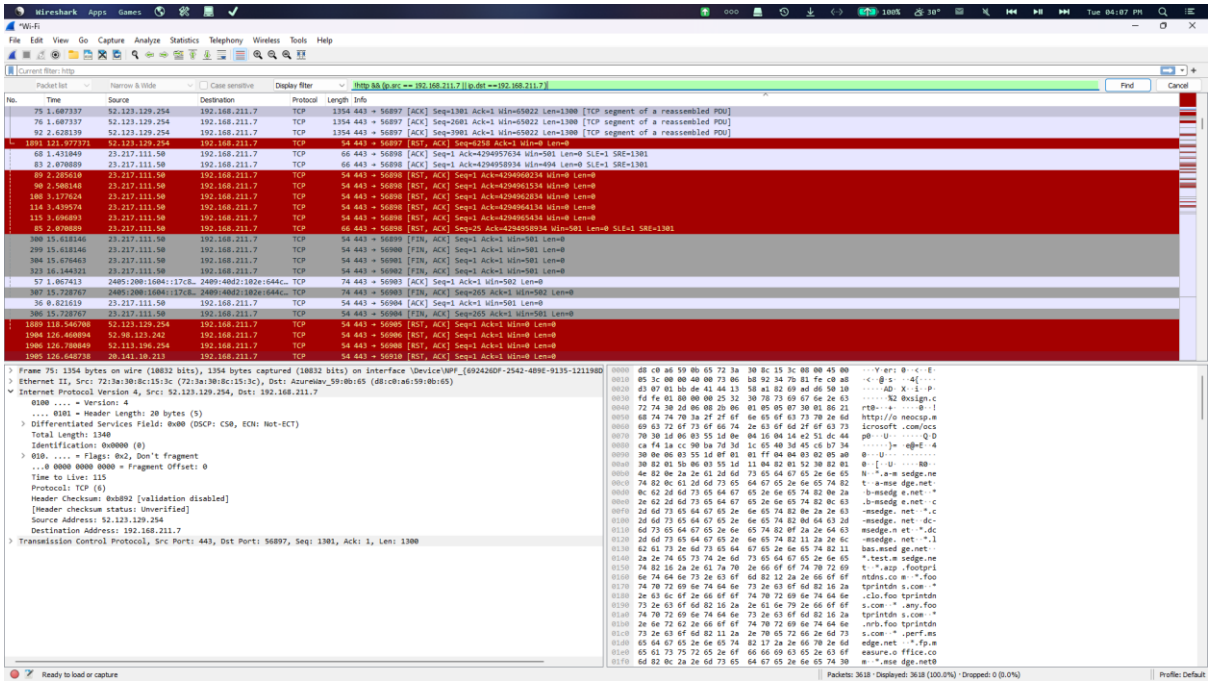
The IP Address of the website is 65.61.137.117
IP Address of my computer is 192.168.211.7



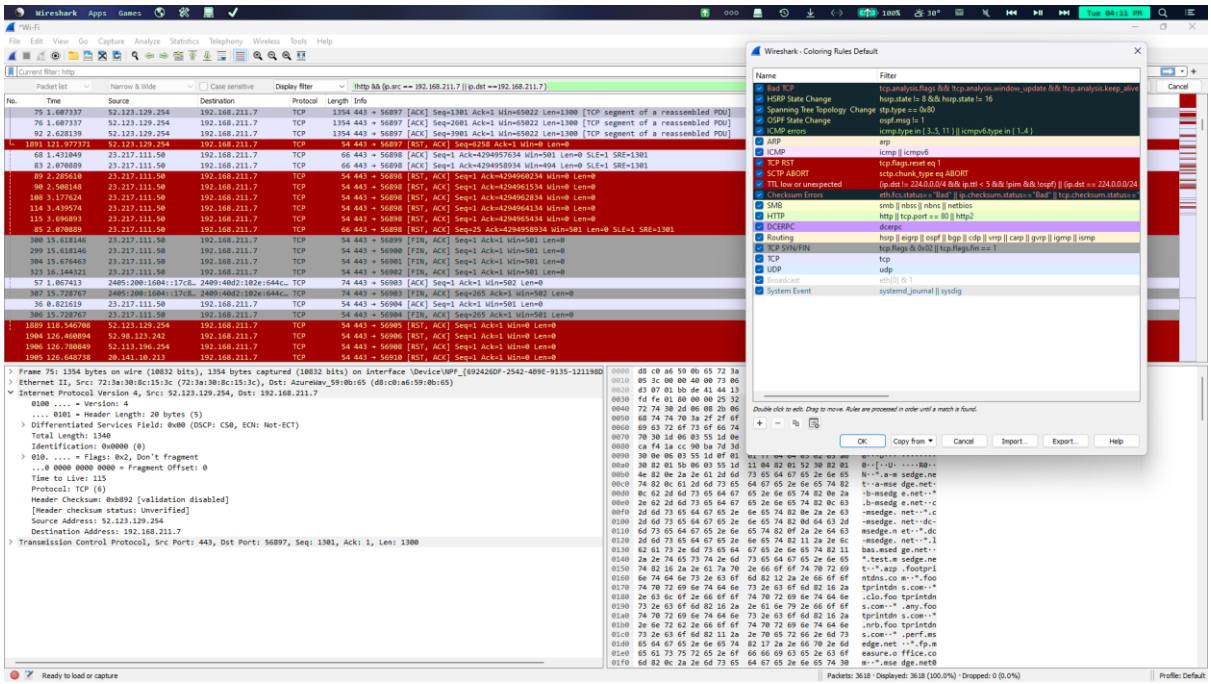
4. How many packets did you capture (total of all protocols, not just HTTP)?

3618 packets

5. What is this filter you used? Now, reverse the filter to determine how many packets don't contain your IP address. See any problems there?



7. What are the appropriate display filters to use? How does Wireshark warn you of such a problem?



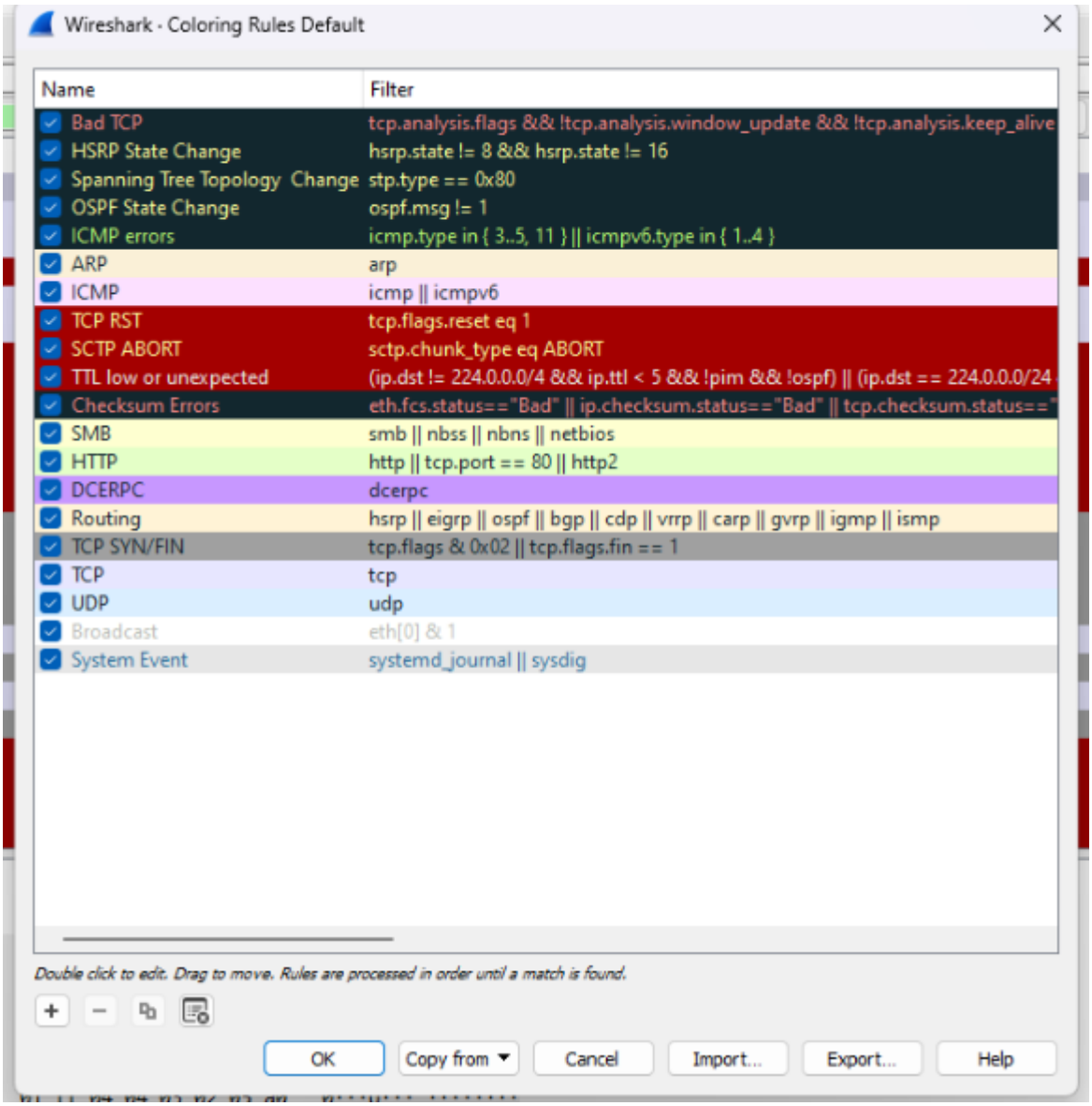
8. Use Wireshark skills to capture the process when your browser loads the front page of your favorite website. Ensure you examine the packet capture in detail, using appropriate Wireshark functionality.

• How many packets did you capture?

452

• Were all of them HTTP? Display them in RED color on Wireshark.

NO



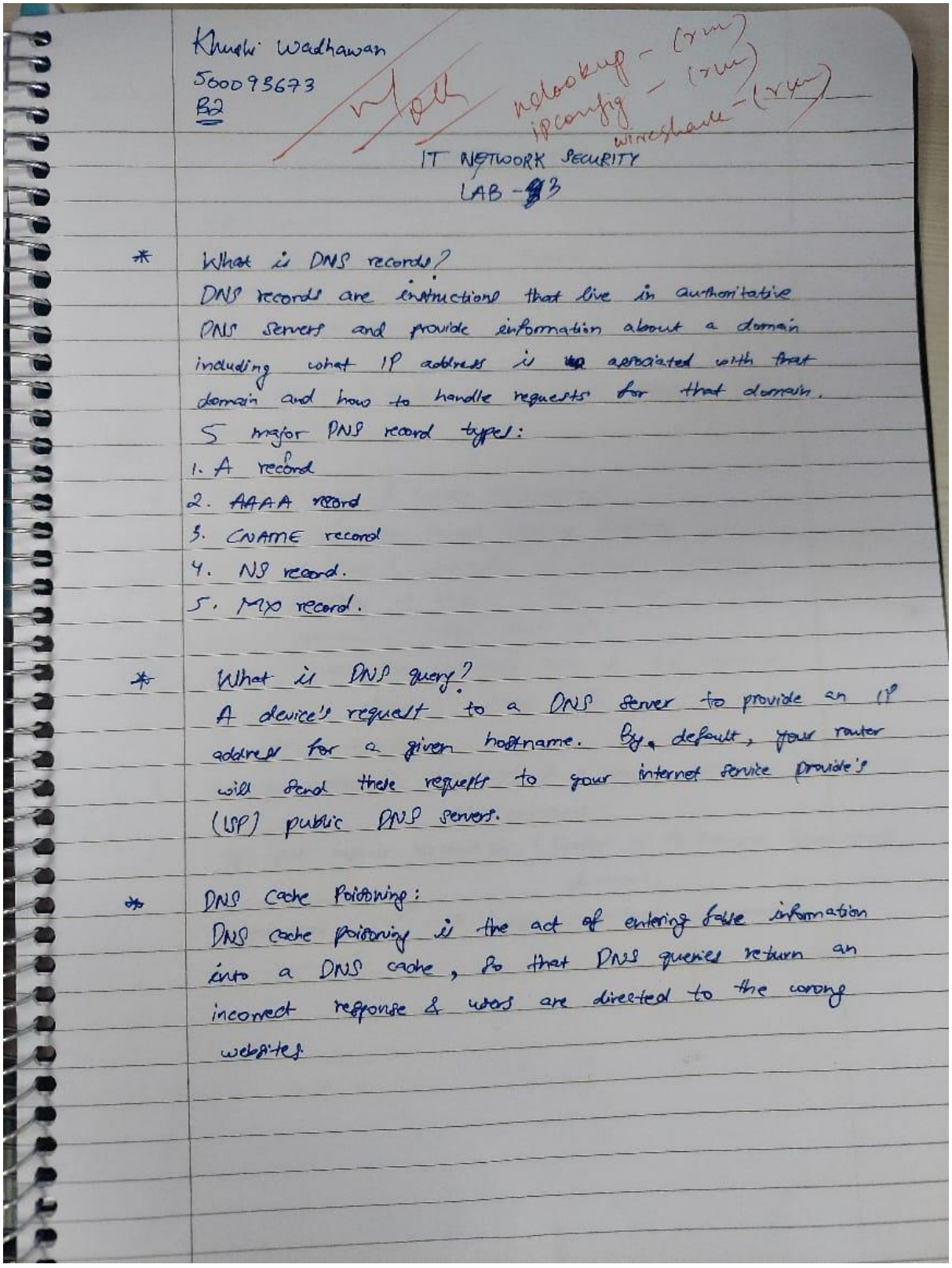
• How many HTTP requests did you make?

27

• Were all the replies "200 OK"?

No

EXPERIMENT 3



Khushi Wadhawan
500095673
B2

nslookup - (ryw)
ipconfig - (ryw)
Wireshark - (ryw)

IT NETWORK SECURITY
LAB - 3

* What is DNS records?
DNS records are instructions that live in authoritative DNS servers and provide information about a domain including what IP address is associated with that domain and how to handle requests for that domain.
5 major DNS record types:
1. A record
2. AAAA record
3. CNAME record
4. NS record.
5. MX record.

* What is DNS query?
A device's request to a DNS server to provide an IP address for a given hostname. By default, your router will send these requests to your internet service provide's (ISP) public DNS servers.

** DNS cache Poisoning:
DNS cache poisoning is the act of entering false information into a DNS cache, so that DNS queries return an incorrect response & users are directed to the wrong websites.

PART 1:

1.1

```
C:\Users\wadha>nslookup www.sdu.uk
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  10.2.1.60

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    www.sdu.uk
Address:  213.171.212.244
```

```
C:\Users\wadha>nslookup www.google.com
Server:  UnKnown
Address:  10.2.1.60

DNS request timed out.
    timeout was 2 seconds.
Name:    www.google.com
Address:  2404:6800:4002:818::2004
```

```
C:\Users\wadha>nslookup www.amazon.in
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  10.2.1.60

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Name:    d1elgm1ww0d6wo.cloudfront.net
Addresses:  2600:9000:256b:200:8:b109:e13:73e1
          2600:9000:256b:2000:8:b109:e13:73e1
          2600:9000:256b:2400:8:b109:e13:73e1
          2600:9000:256b:2600:8:b109:e13:73e1
          2600:9000:256b:3600:8:b109:e13:73e1
          2600:9000:256b:5200:8:b109:e13:73e1
          2600:9000:256b:6200:8:b109:e13:73e1
          2600:9000:256b:c800:8:b109:e13:73e1
Aliases:  www.amazon.in
          tp.c95e7e602-frontier.amazon.in
```

```
C:\Users\wadha>nslookup www.ajio.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  10.2.1.60

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    www.ajio.com
Address:  49.40.59.11
```

```
C:\Users\wadha>nslookup www.lenskart.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  10.2.1.60

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    www.lenskart.com
Addresses:  104.17.82.89
          104.17.83.89
```

Part 2

1.
2. Dynamic – DHCP enabled (yes)

```
Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 1A-CC-18-E9-B5-C9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

3. 10.2.1.60 (primary), 10.2.1.61

```
   Default Gateway . . . . . . . . . : 10.12.1.1
   DHCP Server . . . . . . . . . . . : 10.2.1.8
   DNS Servers . . . . . . . . . . . : 10.2.1.60
                                       10.2.1.61
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

4. ns1.google.com, ssl.gstatic.com, surfsharkstatus.com

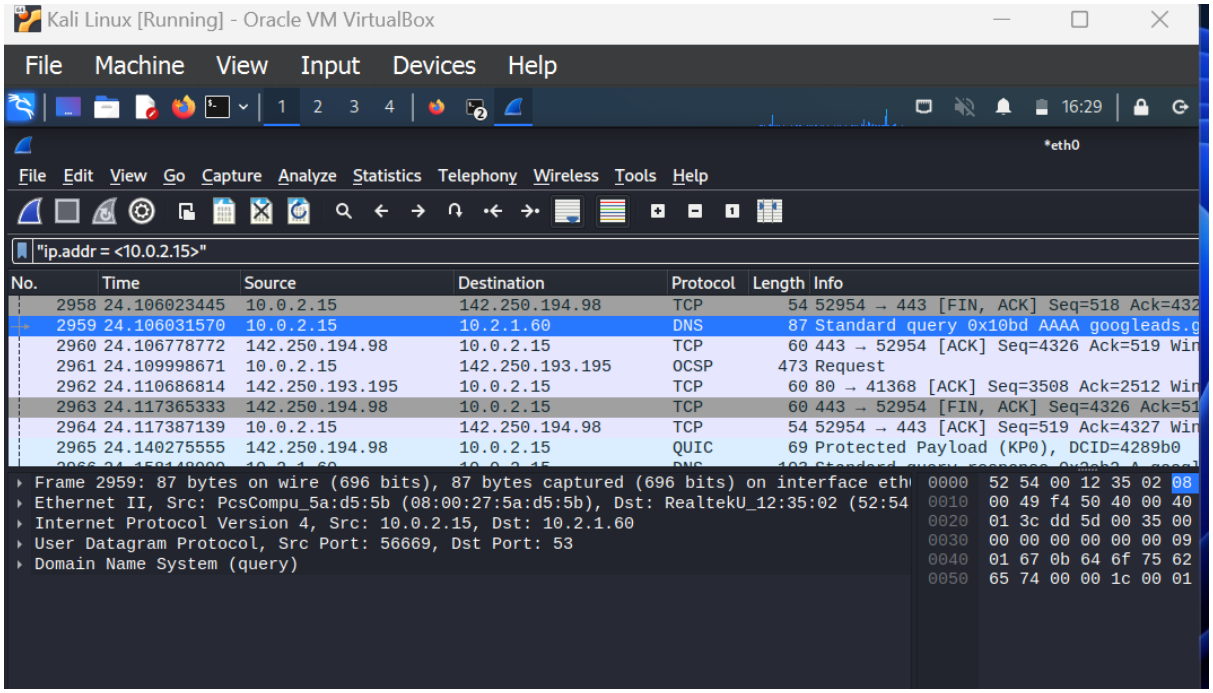
```
C:\Users\wadha>ipconfig /displaydns

Windows IP Configuration

    ns1.google.com
    ----------------------------------------
    Record Name . . . . . : ns1.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 65260
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 216.239.32.10


    ssl.gstatic.com
    ----------------------------------------
    Record Name . . . . . : ssl.gstatic.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 51
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 142.250.206.163


    surfsharkstatus.com
    ----------------------------------------
    Record Name . . . . . : surfsharkstatus.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 130
    Data Length . . . . . : 4
```

5.

```
C:\Users\wadha>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

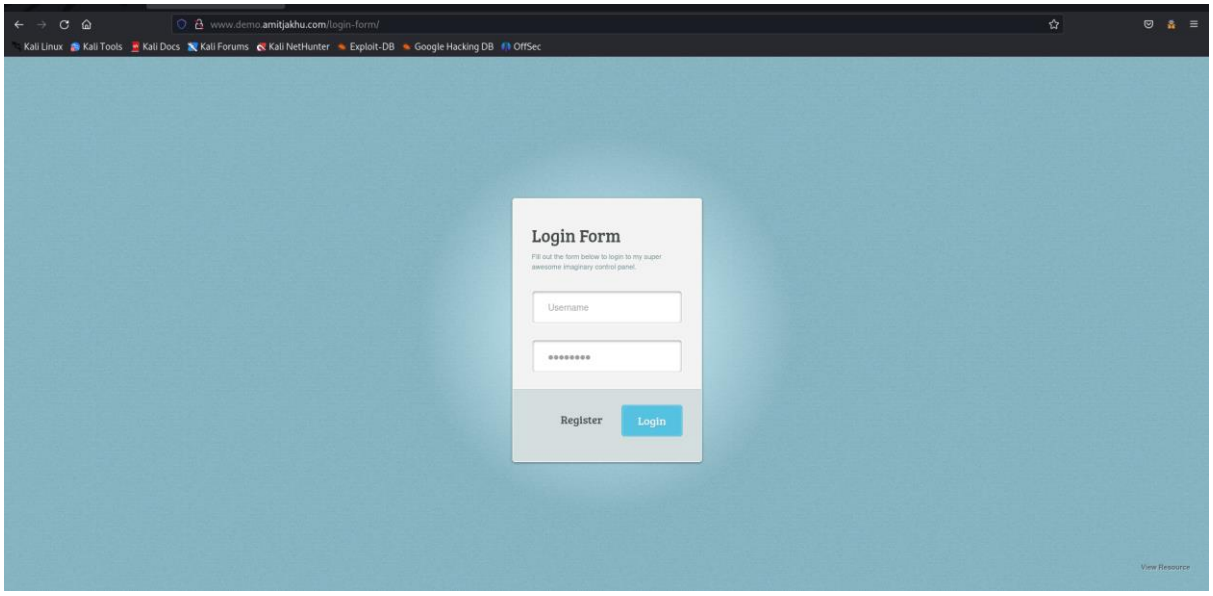
Part 3:

1. DNS query is sent over UDP



2. Source port – 56669, Destination port – 53
3. 10.2.1.60

EXPERIMENT 4



http

No.	Time	Source	Destination	Protocol	Length	Info
103	3.441950728	192.168.186.128	23.2.16.186	OCSP	467	Request
104	3.442056261	192.168.186.128	23.2.16.186	OCSP	467	Request
105	3.442206104	192.168.186.128	23.2.16.186	OCSP	467	Request
117	3.537696971	192.168.186.128	23.2.16.186	OCSP	467	Request
144	4.392296636	192.168.186.128	23.2.16.186	OCSP	467	Request
152	4.423378101	192.168.186.128	23.2.16.186	OCSP	467	Request
155	4.660824262	23.2.16.186	192.168.186.128	OCSP	942	Response
156	4.660824763	23.2.16.186	192.168.186.128	OCSP	942	Response
165	4.776134406	23.2.16.186	192.168.186.128	OCSP	942	Response
166	4.776135128	23.2.16.186	192.168.186.128	OCSP	942	Response
195	4.872277960	23.2.16.186	192.168.186.128	OCSP	943	Response
205	4.975306811	23.2.16.186	192.168.186.128	OCSP	942	Response
211	4.995373143	23.2.16.186	192.168.186.128	OCSP	943	Response
372	9.329681591	192.168.186.128	192.195.77.80	HTTP	454	GET /login-form HTTP/1.1
387	10.247678416	192.195.77.80	192.168.186.128	HTTP	557	HTTP/1.1 301 Moved Permanently (text/html)
389	10.258903508	192.168.186.128	192.195.77.80	HTTP	455	GET /login-form/ HTTP/1.1
412	13.087175760	192.195.77.80	192.168.186.128	HTTP	233	HTTP/1.1 200 OK (text/html)
414	13.315717169	192.168.186.128	192.195.77.80	HTTP	423	GET /login-form/css/style.css HTTP/1.1
426	14.415290633	192.168.186.128	23.2.16.219	OCSP	467	Request
427	14.415552279	192.168.186.128	23.2.16.219	OCSP	467	Request
455	15.796986042	192.195.77.80	192.168.186.128	HTTP	4480	HTTP/1.1 200 OK (text/css)
468	15.886856016	23.2.16.219	192.168.186.128	OCSP	943	Response
469	15.886856948	23.2.16.219	192.168.186.128	OCSP	943	Response
489	16.649260503	192.168.186.128	216.58.196.106	HTTP	406	GET /ajax/libs/jquery/1.2.6/jquery.min.js HTTP/1.1
519	18.097199869	192.168.186.128	142.250.193.10	HTTP	407	GET /css?family=Bree+Serif HTTP/1.1
528	19.056507744	216.58.196.106	192.168.186.128	HTTP	862	HTTP/1.1 200 OK (text/javascript)
534	20.038202099	142.250.193.10	192.168.186.128	HTTP	74	HTTP/1.1 200 OK (text/css)
536	20.126925280	192.168.186.128	192.195.77.80	HTTP	443	GET /login-form/images/bg.png HTTP/1.1
537	20.127186125	192.168.186.128	192.195.77.80	HTTP	450	GET /login-form/images/user-icon.png HTTP/1.1
560	20.962238270	192.168.186.128	192.195.77.80	HTTP	450	GET /login-form/images/pass-icon.png HTTP/1.1
562	20.970193177	192.195.77.80	192.168.186.128	HTTP	1457	HTTP/1.1 200 OK (PNG)
578	21.662010754	192.168.186.128	142.250.193.195	HTTP	516	GET /s/breeserif/v17/4UaHrEJCrhhnVA3DgluA96rp57F2IwM.woff2 HTTP/1.1
582	21.689270133	192.168.186.128	192.195.77.80	HTTP	417	GET /favicon.ico HTTP/1.1
586	21.866087581	192.195.77.80	192.168.186.128	HTTP	1410	HTTP/1.1 200 OK (PNG)
594	22.813382512	192.195.77.80	192.168.186.128	HTTP	14370	HTTP/1.1 200 OK (PNG)
603	24.121078656	192.195.77.80	192.168.186.128	HTTP	862	HTTP/1.1 404 Not Found (text/html)
653	30.741872378	142.250.193.195	192.168.186.128	HTTP	2694	HTTP/1.1 200 OK (font/woff2)

PART #1: By looking at the information in the HTTP GET and response messages, answer the following questions.

Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

HTTP version 1.1

What languages (if any) does your browser indicate that it can accept to the server?

Accept – Language: en-Us, en;q=0.5\r\n

```
Accept: text/html,application/xhtml+
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
```

What is the IP address of your computer and the web server?

Source address

```
Source Address: 192.168.186.128
Destination Address: 192.195.77.80
```

What is the status code returned from the server to your browser?

200

```
Status Code: 200
```

How many bytes of content are being returned to your browser?

```
Content-Length: 85\r\n
```

```
Content-Length: 503\r\n
```

By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No

PART #2

How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

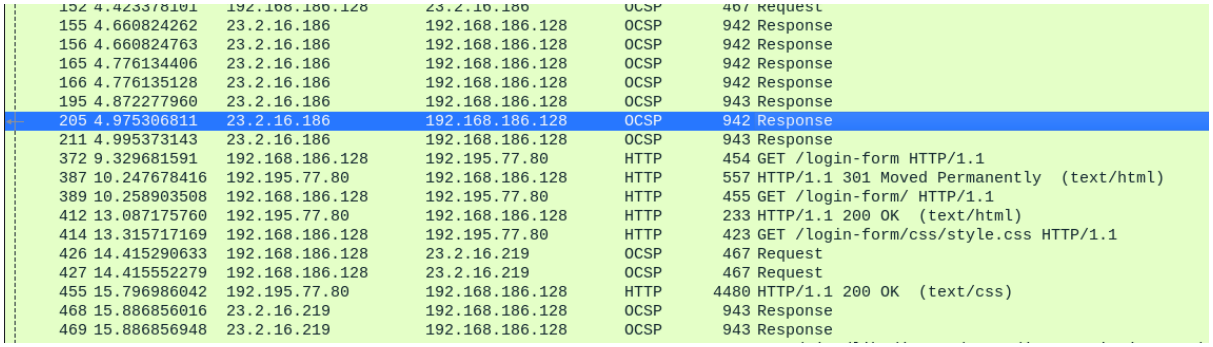
9

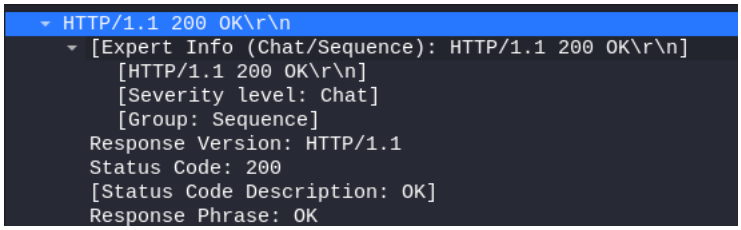
http

No.	Time	Source	Destination	Protocol	Length	Info
102	3.441755280	192.168.186.128	23.2.16.186	OCSP	467	Request
103	3.441950728	192.168.186.128	23.2.16.186	OCSP	467	Request
104	3.442056261	192.168.186.128	23.2.16.186	OCSP	467	Request
105	3.442206104	192.168.186.128	23.2.16.186	OCSP	467	Request
117	3.537696971	192.168.186.128	23.2.16.186	OCSP	467	Request
144	4.392296636	192.168.186.128	23.2.16.186	OCSP	467	Request
152	4.423378101	192.168.186.128	23.2.16.186	OCSP	467	Request
155	4.660824262	23.2.16.186	192.168.186.128	OCSP	942	Response
156	4.660824763	23.2.16.186	192.168.186.128	OCSP	942	Response
165	4.776134406	23.2.16.186	192.168.186.128	OCSP	942	Response
166	4.776135128	23.2.16.186	192.168.186.128	OCSP	942	Response
195	4.872277960	23.2.16.186	192.168.186.128	OCSP	943	Response
205	4.975306811	23.2.16.186	192.168.186.128	OCSP	942	Response
211	4.995373143	23.2.16.186	192.168.186.128	OCSP	943	Response
372	9.329681591	192.168.186.128	192.195.77.80	HTTP	454	GET /login-form HTTP/1.1
387	10.247678416	192.195.77.80	192.168.186.128	HTTP	557	HTTP/1.1 301 Moved Permanently (text/html)
389	10.258903508	192.168.186.128	192.195.77.80	HTTP	455	GET /login-form/ HTTP/1.1
412	13.087175760	192.195.77.80	192.168.186.128	HTTP	233	HTTP/1.1 200 OK (text/html)
414	13.315717169	192.168.186.128	192.195.77.80	HTTP	423	GET /login-form/css/style.css HTTP/1.1
426	14.415290633	192.168.186.128	23.2.16.219	OCSP	467	Request
427	14.415552279	192.168.186.128	23.2.16.219	OCSP	467	Request
455	15.796986042	192.195.77.80	192.168.186.128	HTTP	4480	HTTP/1.1 200 OK (text/css)
468	15.886856016	23.2.16.219	192.168.186.128	OCSP	943	Response
469	15.886856948	23.2.16.219	192.168.186.128	OCSP	943	Response
489	16.649260503	192.168.186.128	216.58.196.106	HTTP	406	GET /ajax/libs/jquery/1.2.6/jquery.min.js HTTP/1.1

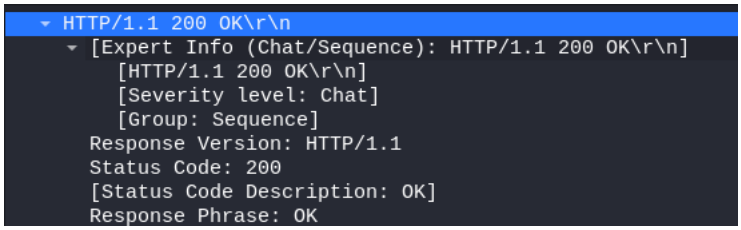
Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

9



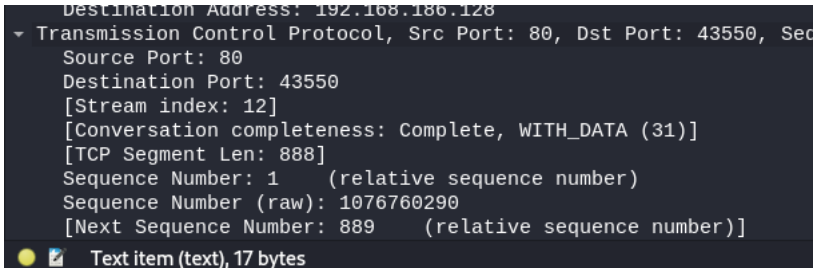


What is the status code and phrase in the response?



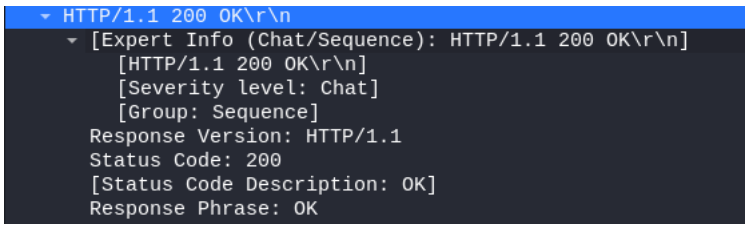
How many data-containing TCP segments were needed to carry the single HTTP response and the text of the book?

888



PART #3: Search for at least five WEB LOGIN based on HTTP (not HTTPS). Perform stapes in Part 3.

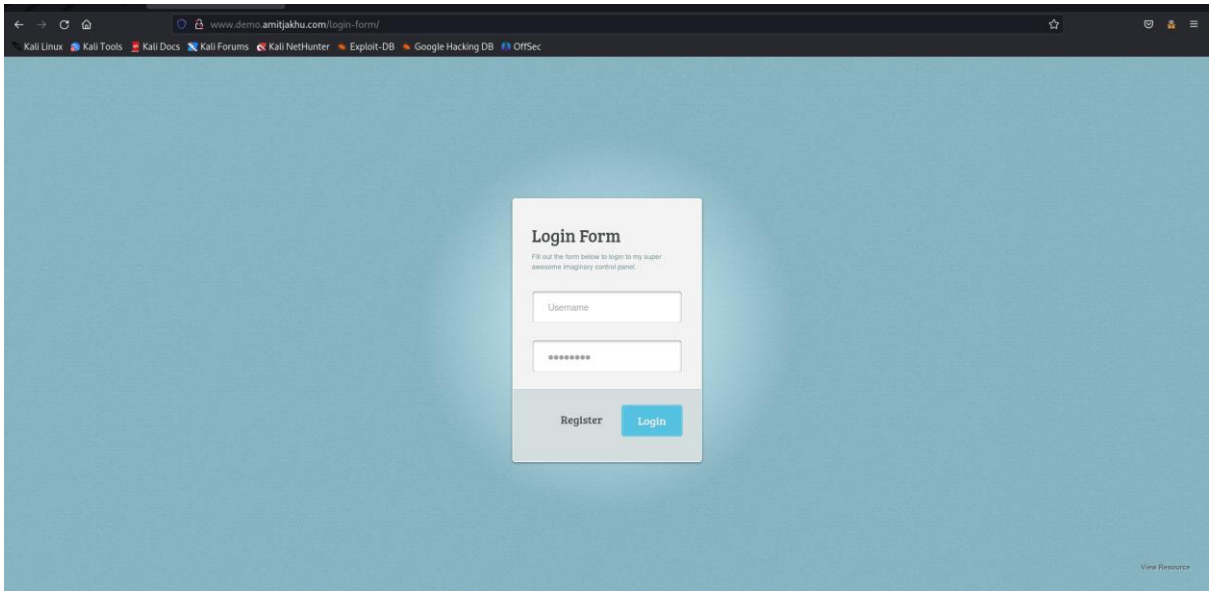
What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? Status code 200



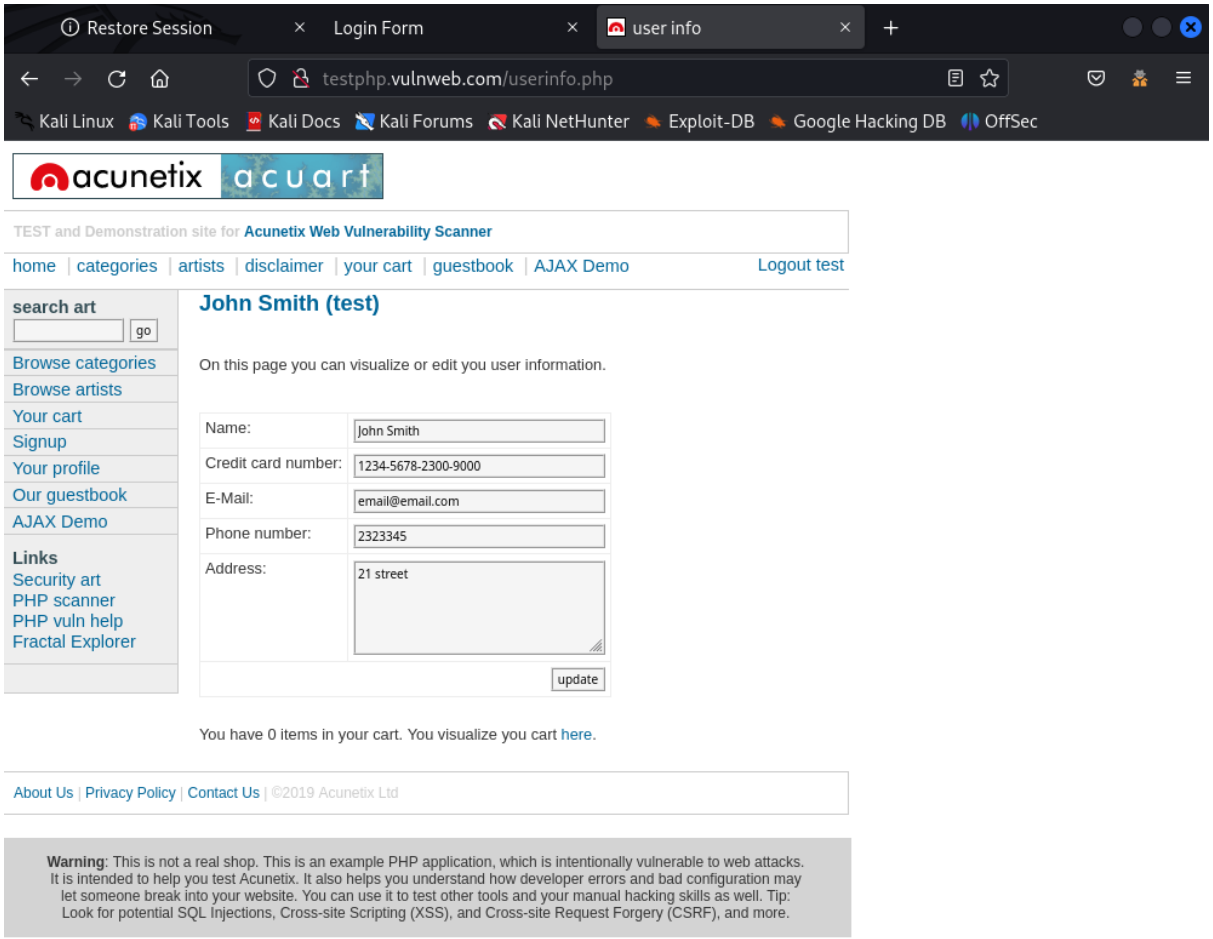
When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Content-Type: text/html\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  Keep-Alive: timeout=15\r\n
  Date: Mon, 18 Sep 2023 18:31:25 GMT\r\n
  Server: Apache\r\n
  Last-Modified: Sat, 15 Aug 2015 20:17:57 GMT\r\n
  ETag: W/"beb-51d5f43a79d35"\r\n
  Content-Encoding: gzip\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.338433999 seconds]
  [Request in frame: 110]
  [Request URI: http://www.demo.amitjakhu.com/login-form/]
  HTTP chunked response
  Content-encoded entity body (gzip): 1355 bytes -> 3051 bytes
  File Data: 3051 bytes
```

What is the User ID & Password that was captured?




```
  File Data: 51 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "username" = "hello123"
  Form item: "password" = "12345@123"
  Form item: "submit" = "Login"
```


Restore Session
Login Form
user info
testphp.vulnweb.com/userinfo.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
John Smith (test)
On this page you can visualize or edit you user information.
Name:
John Smith
Credit card number:
1234-5678-2300-9000
E-Mail:
email@email.com
Phone number:
2323345
Address:
21 street
update
You have 0 items in your cart. You visualize you cart here.
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.


File Data: 20 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "test"
Form item: "pass" = "test"

EXPERIMENT 5

__/__/__

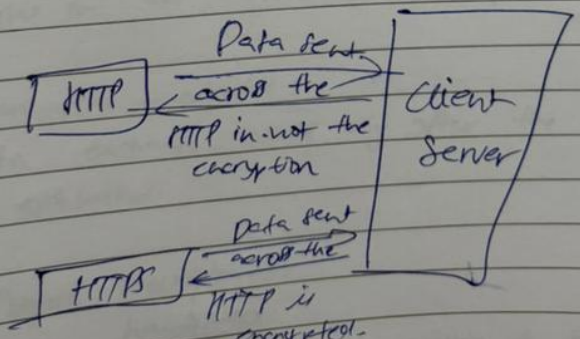
IT NETWORK SECURITY
LAB-5

Khushi Wadhawan
500093673
B2

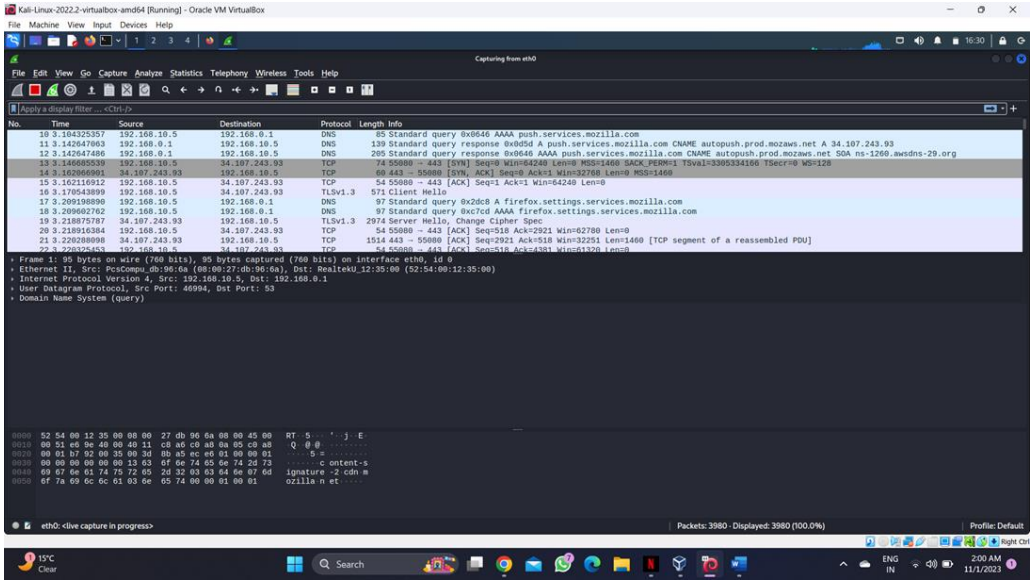
Q1.) HTTP packets are basically decrypted & provide confidential data whereas HTTPS uses encryption to hide the data.
HTTPS works on SSL / TLL encryption over the HTTP protocol.

Q2) Idea block size is 64 bits, 128 & 256 bits,
key size 128, 192, 256 bits
Asymmetric Key 1034 & 2048 bits SSL - 128 64 & 156 bit

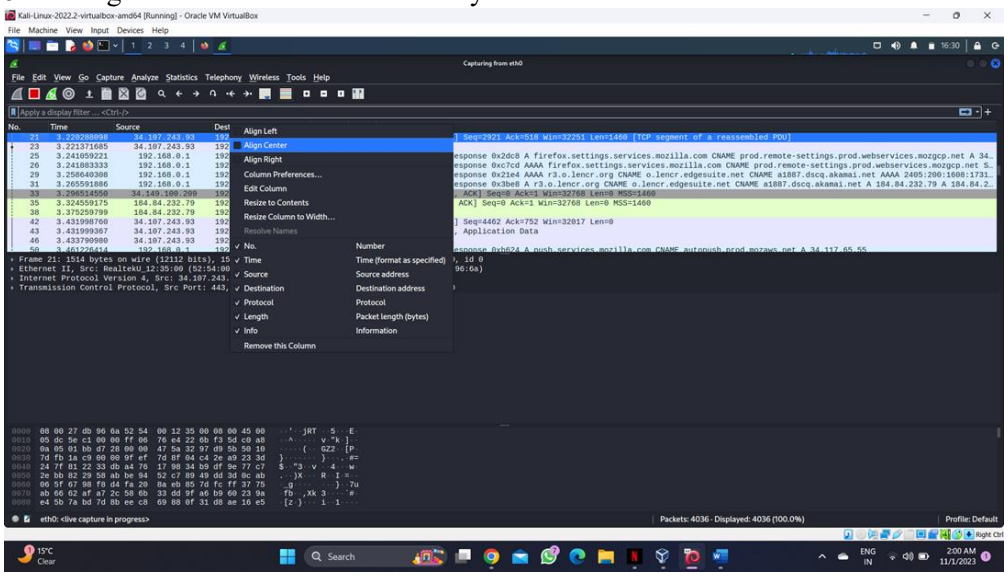
Q3.) HTTPS use TLL / SSL protocol to encrypt communication b/w client & server.

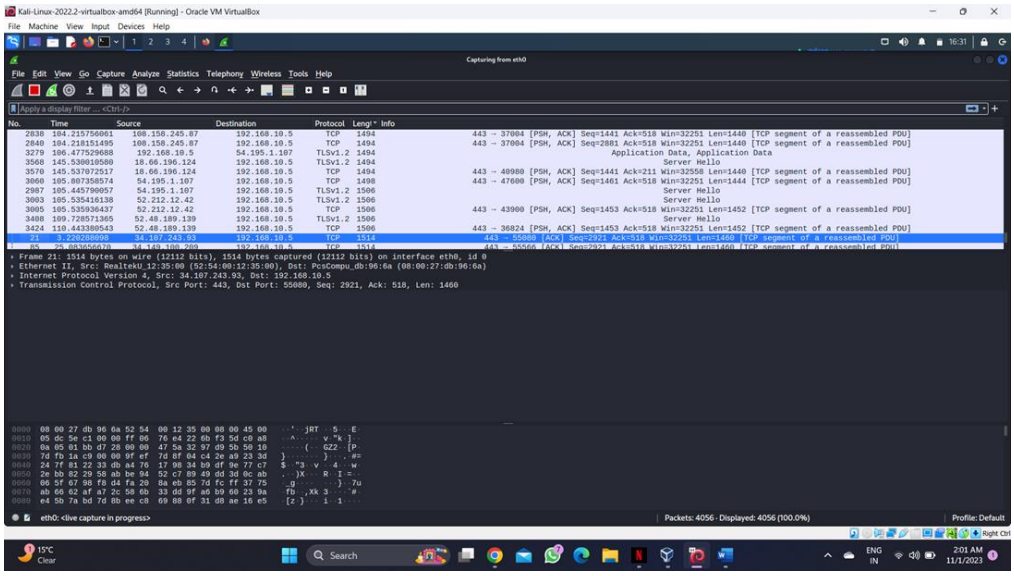


1. Use the ZIP (password: infected) with Keys in text file for this lab.
2. Open the PCAP in Wireshark
3. First open Wireshark à Preferences à Sort the columns and add one extra (number)
4. Now view the PCAP



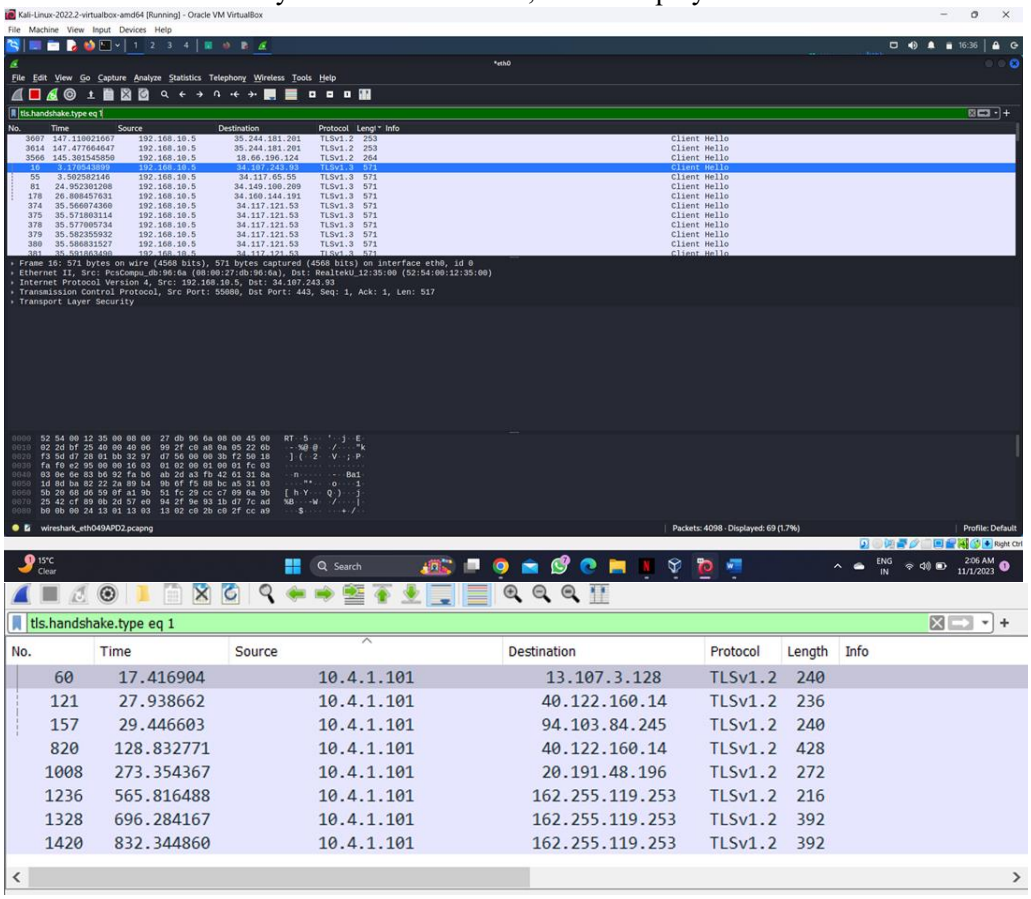
5. Align CENTER for better visibility





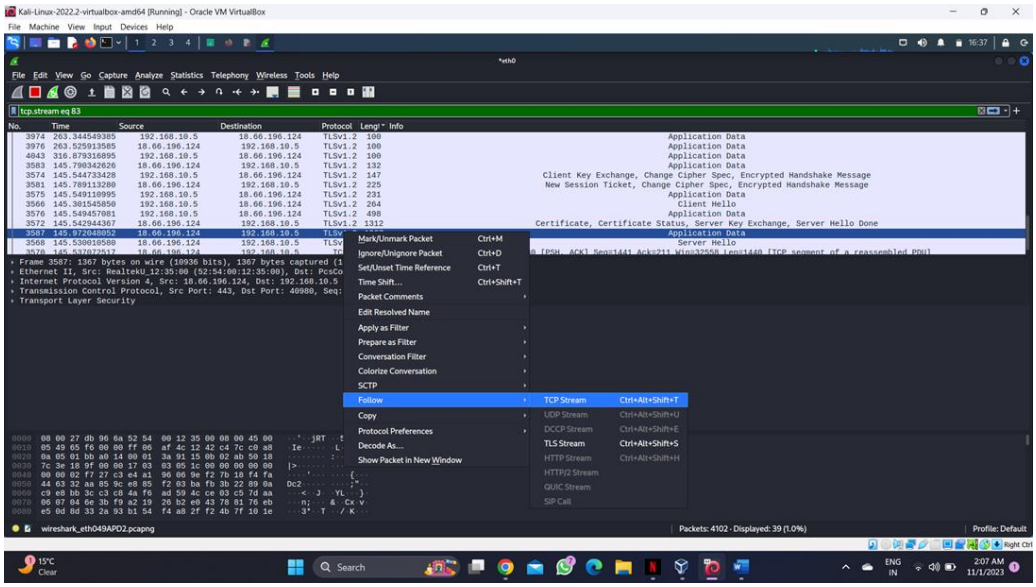
6. Our objective is to decrypt the communication between a particular system from the network dump and identify the infection and what has happened – typical Blue team operation

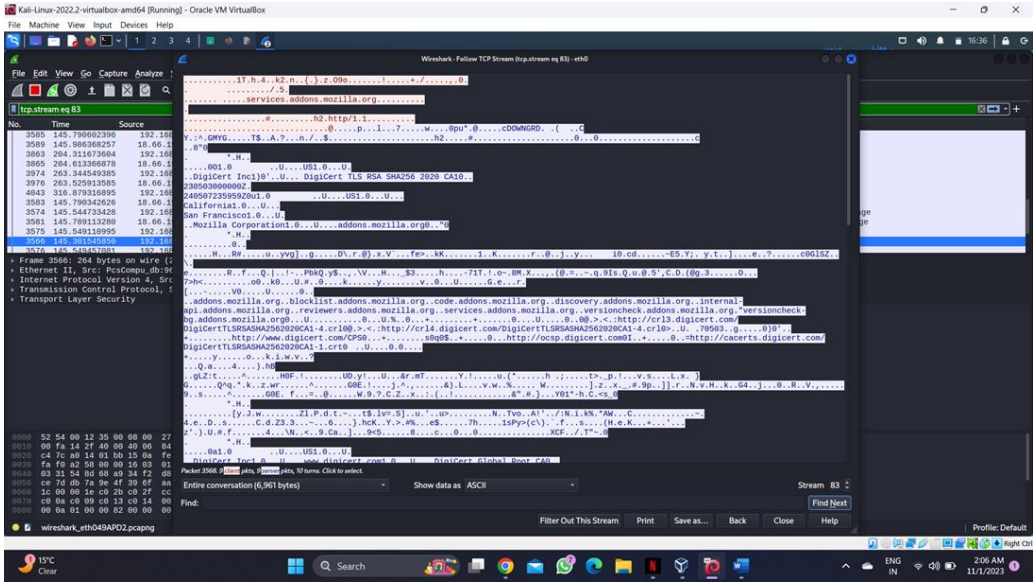
7. Filter TLS Handshake type equal to 1 for successful handshakes – this denotes client systems on the office LAN successfully accessed a TLS site, which displays TLS 1.2



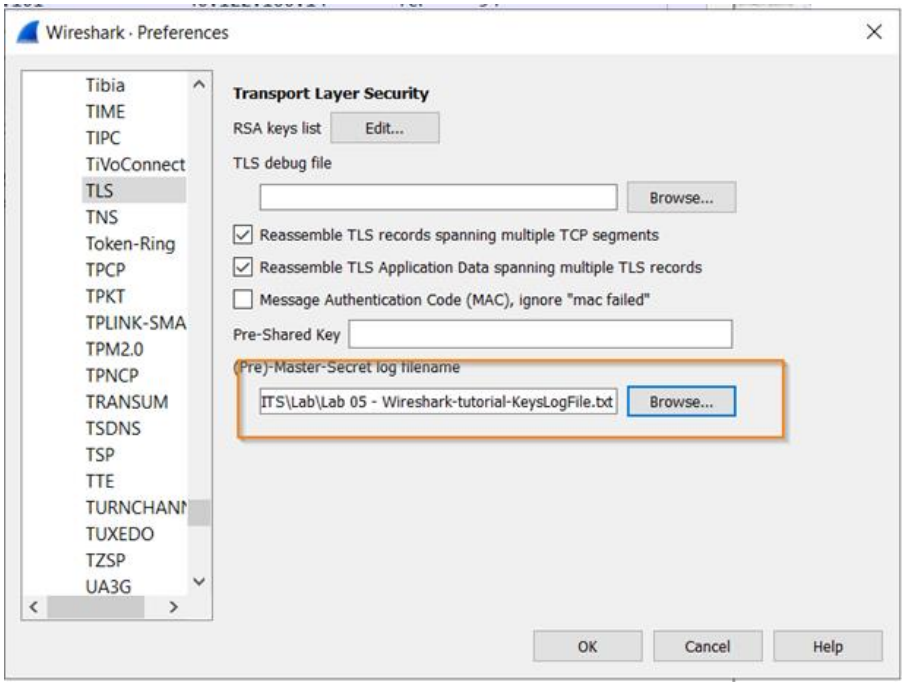
No.	Time	Source	Destination	Protocol	Length	Info
60	17.416904	10.4.1.101	13.107.3.128	TLSv1.2	240	
121	27.938662	10.4.1.101	40.122.160.14	TLSv1.2	236	
157	29.446603	10.4.1.101	94.103.84.245	TLSv1.2	240	
820	128.832771	10.4.1.101	40.122.160.14	TLSv1.2	428	
1008	273.354367	10.4.1.101	20.191.48.196	TLSv1.2	272	
1236	565.816488	10.4.1.101	162.255.119.253	TLSv1.2	216	
1328	696.284167	10.4.1.101	162.255.119.253	TLSv1.2	392	
1420	832.344860	10.4.1.101	162.255.119.253	TLSv1.2	392	

8. If we try to follow this packet – right click and select Follow à TCP Stream – all of that is encrypted because there is an SSL Certificate protecting these data packets

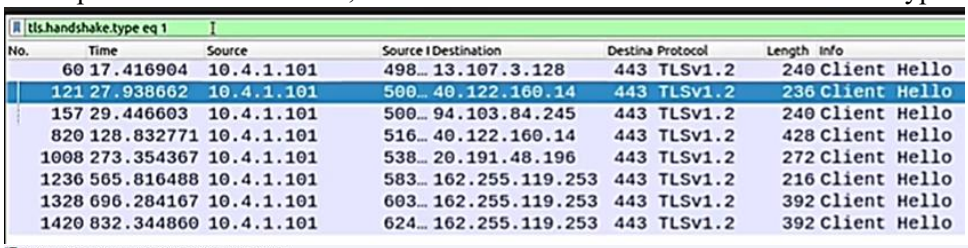


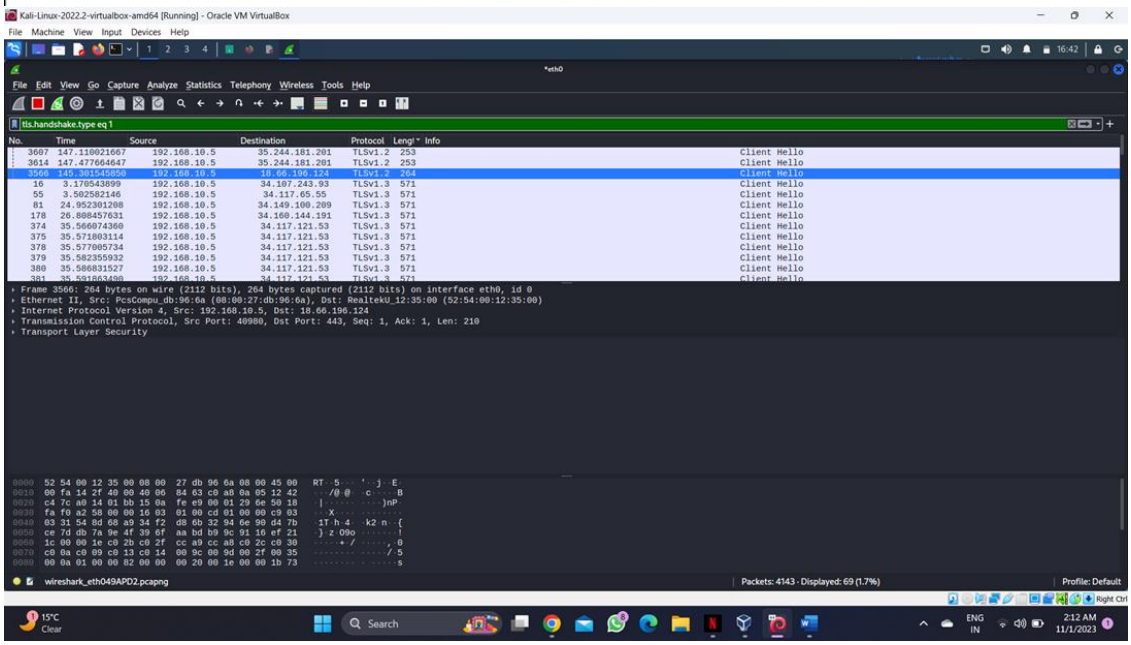


9. To decrypt these we need the SSL Keys, refer to the TEXT file with SSL Keys for this lab. Head over to Wireshark EDIT à Preferences à under Protocols à search for TLS à ‘Pre-Master’ secret log file upload option.

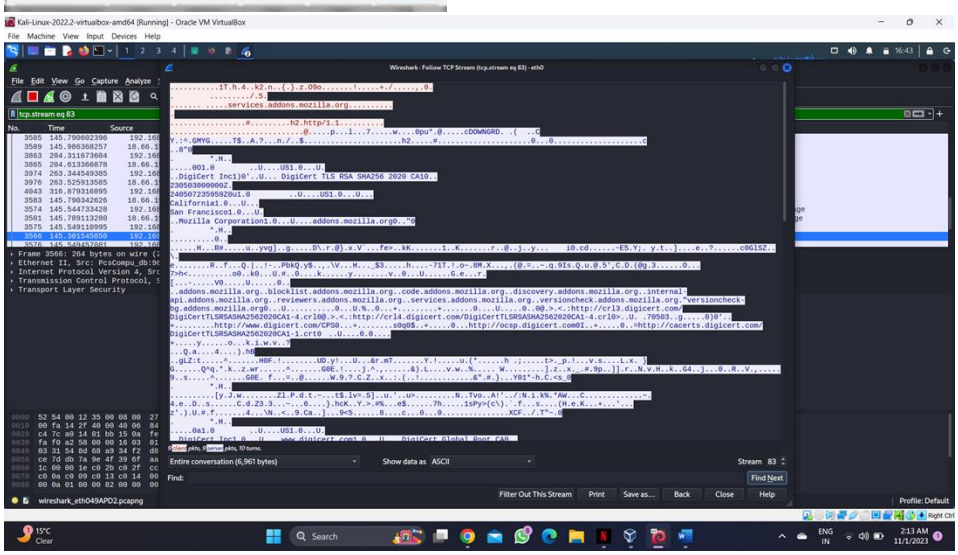


10. Upload the Text file here, remove the filter and now take a look at TLS.type eq 1

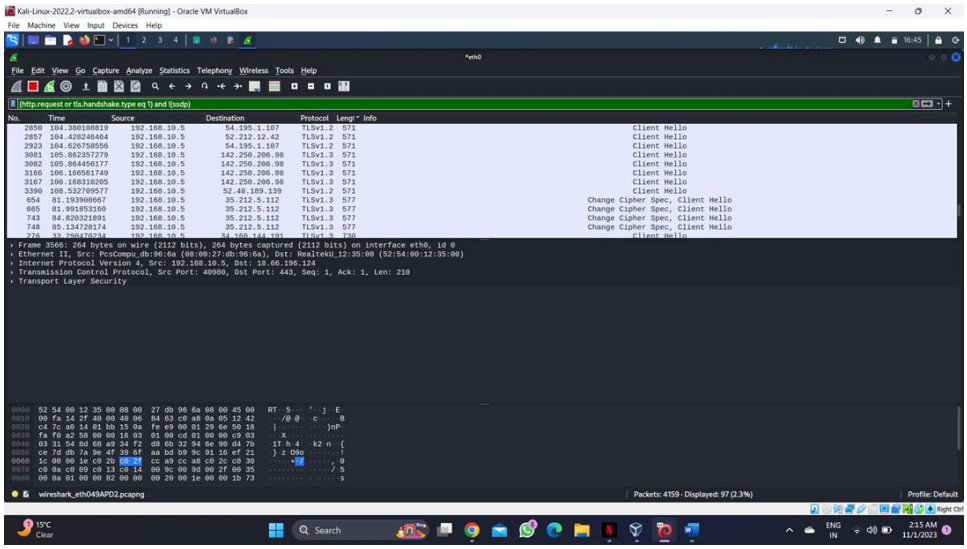


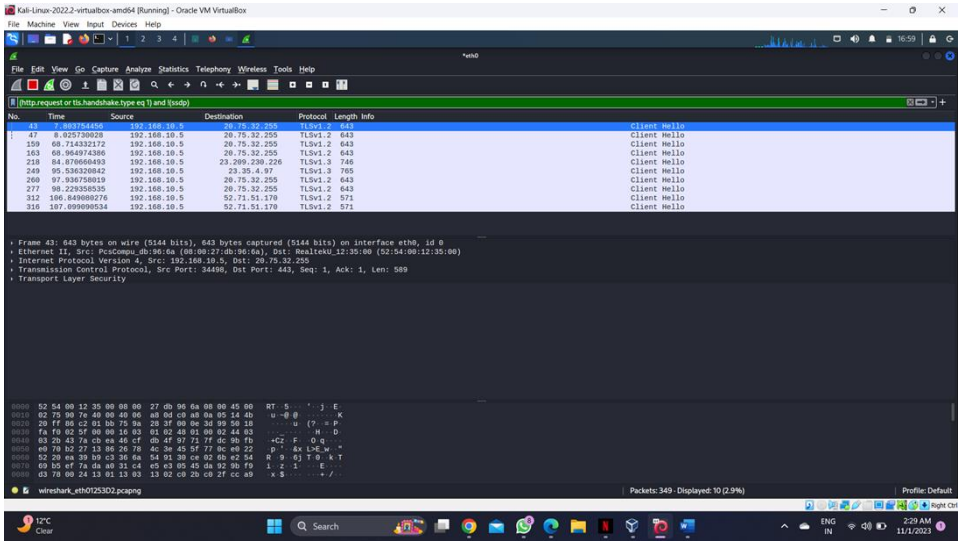


11. Now if we try to follow this packet – right click and select Follow à TCP is still encrypted but we can now view the TLS Stream
12. TSL stream displays clearly

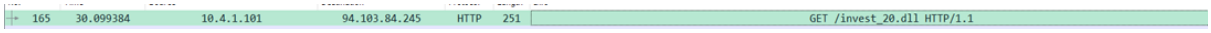


13. Let us try to find which system was infected or involved or which malware caused that infection. For this filter as http.request or tls.handshake.type eq 1 but exclude SSDP Protocol

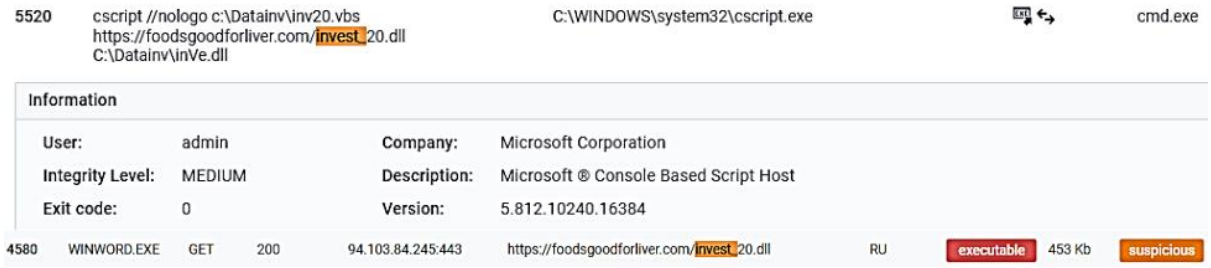




14. We see all HTTP requests – GET, POST, but one of the system on the office network is downloading a DLL file which is strange! Refer to packet number 165

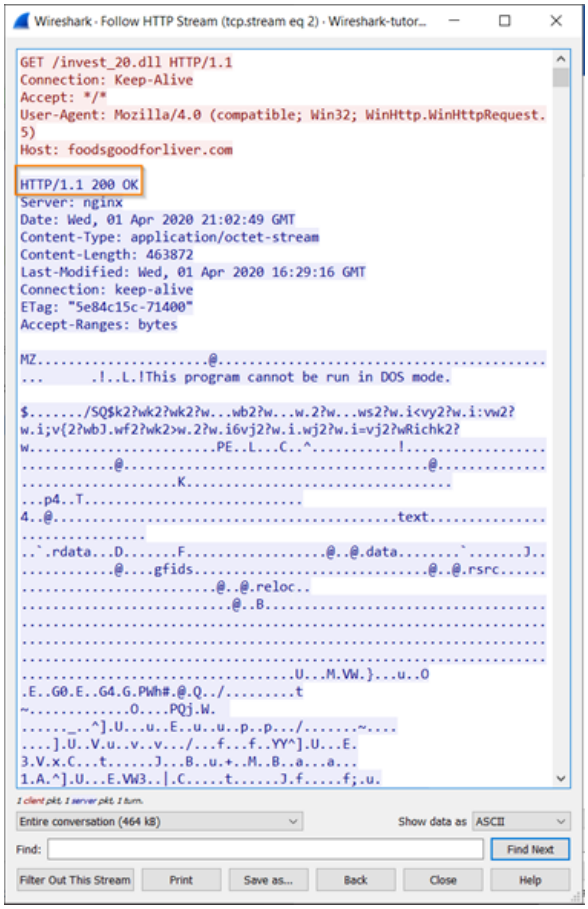


15. If we google to search about 'invest_20.dll' à Malware impacting financial institutions, hiding inside office spreadsheet documents using custom macros. It downloads specific utilities which download the final piece of malware

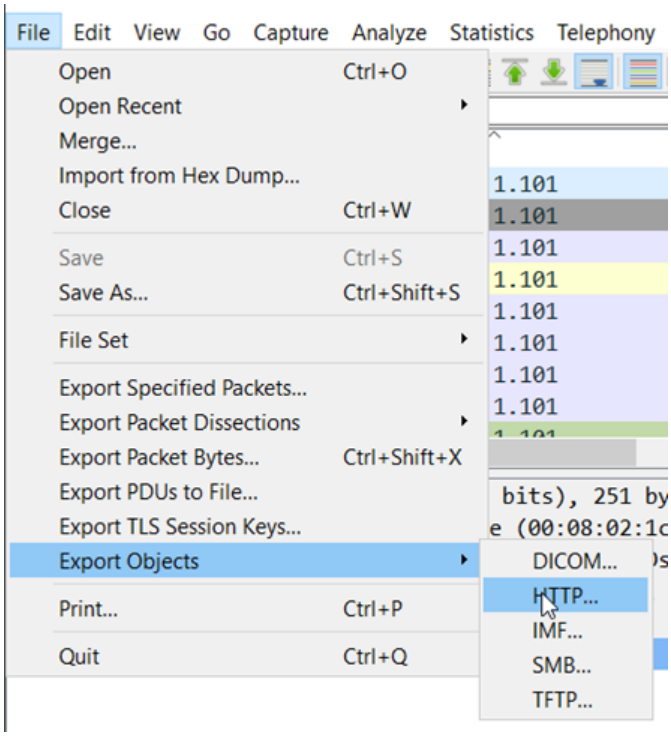


16. Since we have identified the DLL we can click and follow the HTTP Stream from this packet

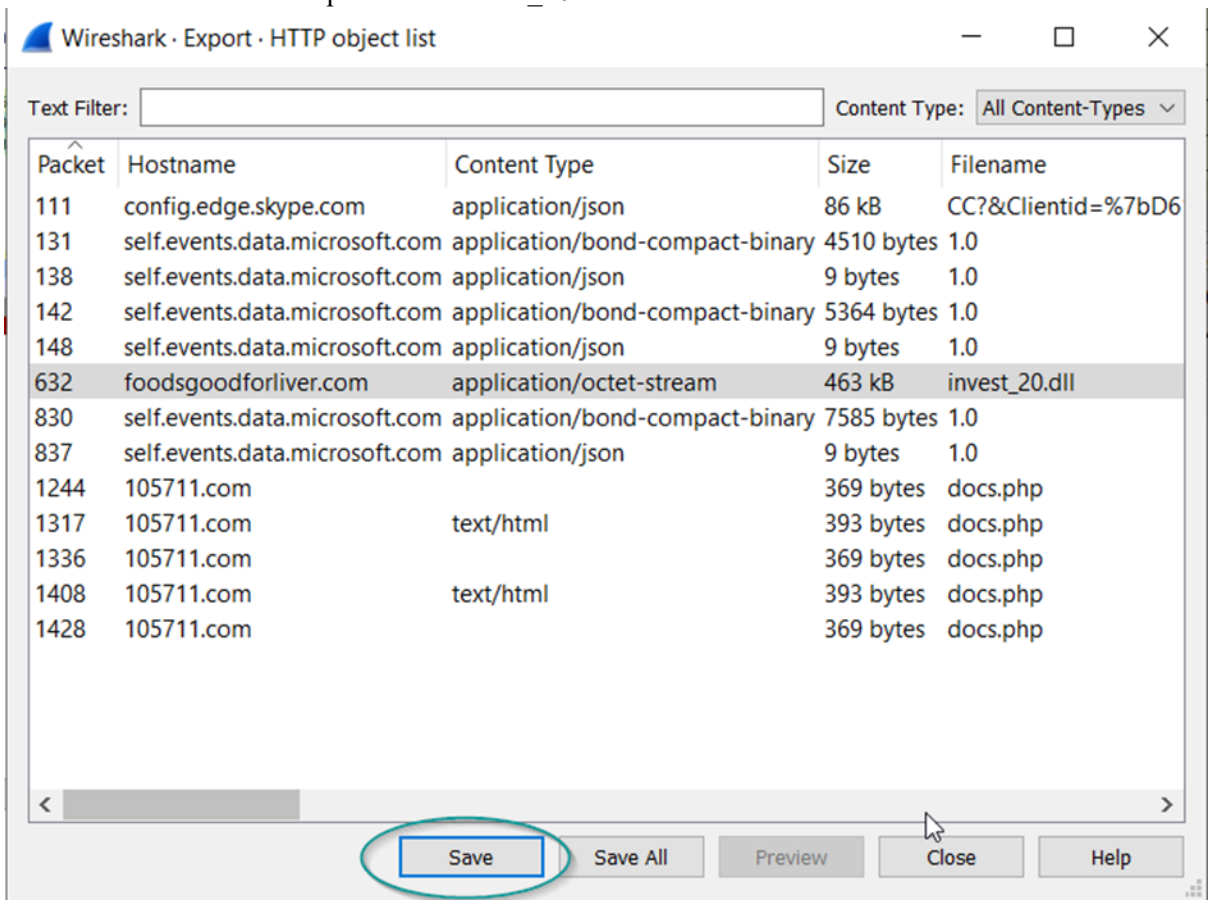
17. We can see that an internal system having IP10.4.1.101 did a GET request so from LAN that system contacted an external domain from 'foodsgoodforliver.com' having IP 94.103.84.245 to download that DLL file.
18. The server response is 200 OK – success and below encrypted info looks to be the actual DLL content



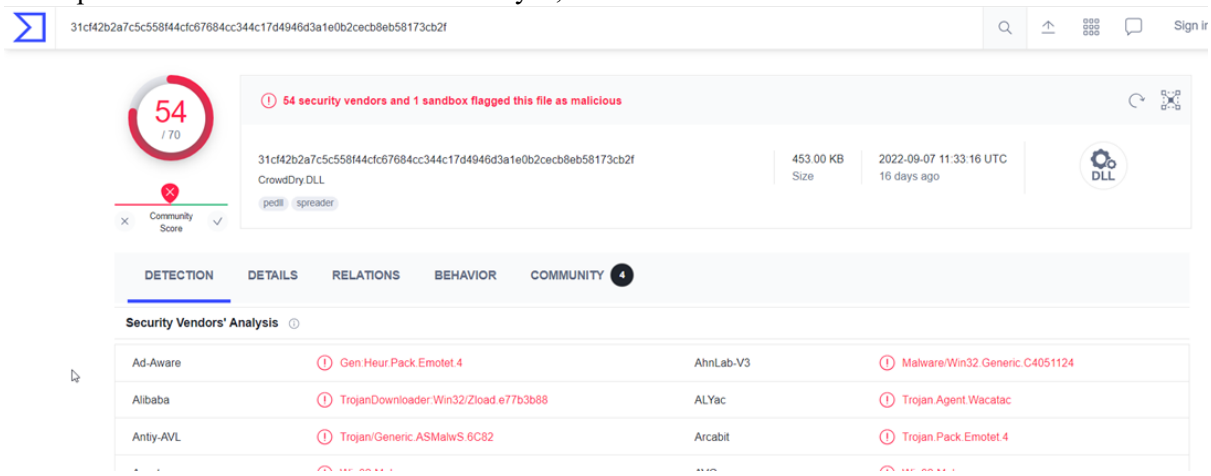
19. Malware hunters need to view the contents or the actual DLL to analyze the malware. We can either copy the contents to analyze on VirusTotal OR export the object from the network traffic dump.
20. Remove this filter to the initial filter and click FILE à Export Object à HTTP



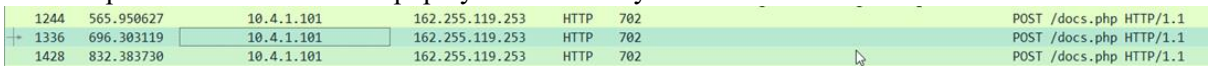
21. Save this on the desktop folder as invest_20.dll



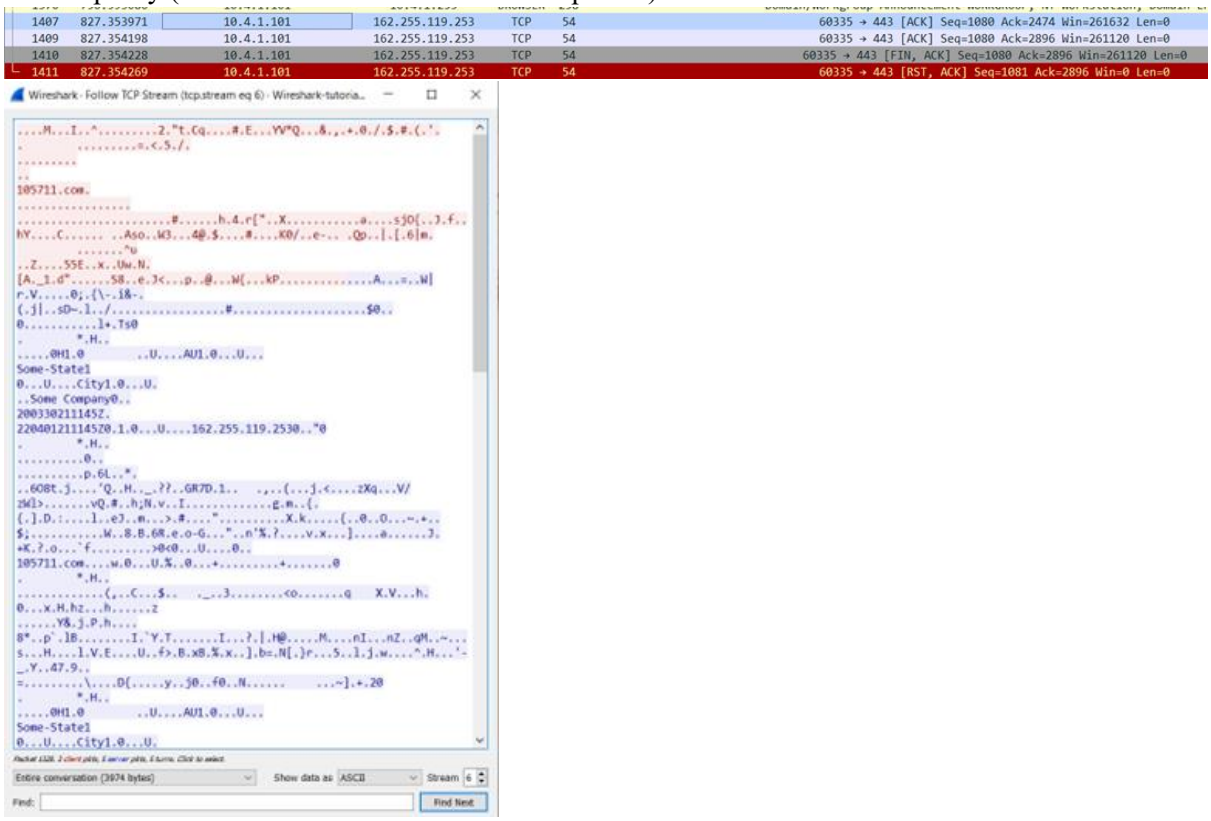
22. Upload the DLL to VirusTotal and analyze, which shows the malicious details



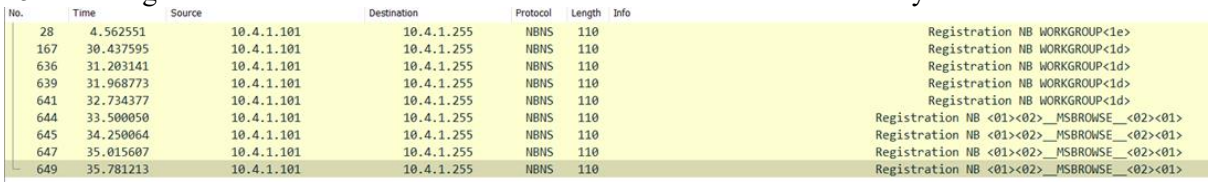
23. The user probably clicked a link OR email attachment (XLS) which then downloaded this DLL. The DLL further downloaded few tools and utilities for actual infection. There are POST requests to an unusual external port 60335 to send docs.php by the internal system at IP 10.4.1.101.



24. After the DLL the user system connected to the attacker's C2 system to send PHP using man-in-the-middle proxy (click Follow TCP stream for that packet)



25. Filtering the PACP for 'nbns' we can note the name of the infected user system



EXPERIMENT 6

Khushi Wadhewan
50009367 3
B2

17/10/23

IT NETWORK SECURITY

LAB6

Decrypt pdf / zip

Standard interchange format

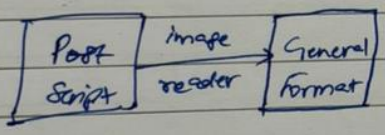
portable document format

Word - 1985 → First intro → Steve Jobs & John Warnock

H/W - 1990

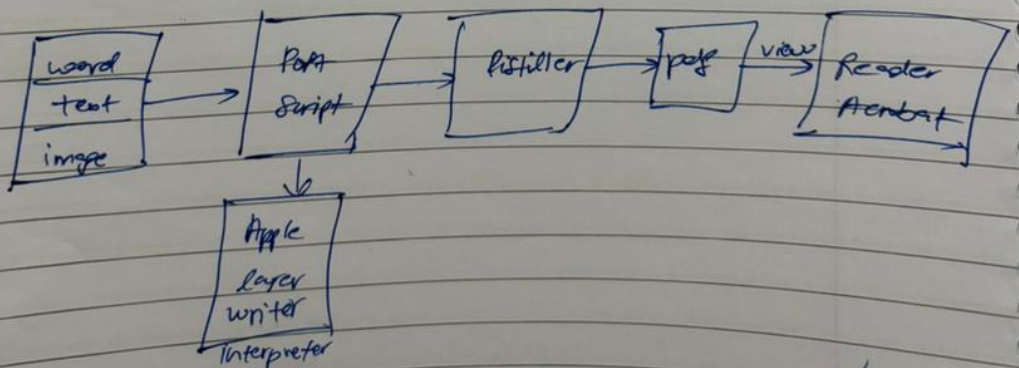
Computation - 1993 → Pdf + reader

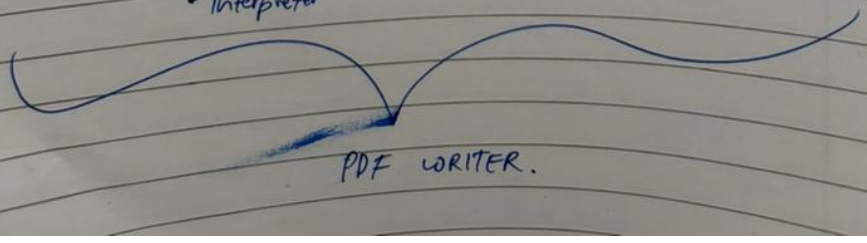
<< post script >> → to generate graphics



→ uses lossless compression

→ LZ or LZW compression technique used.



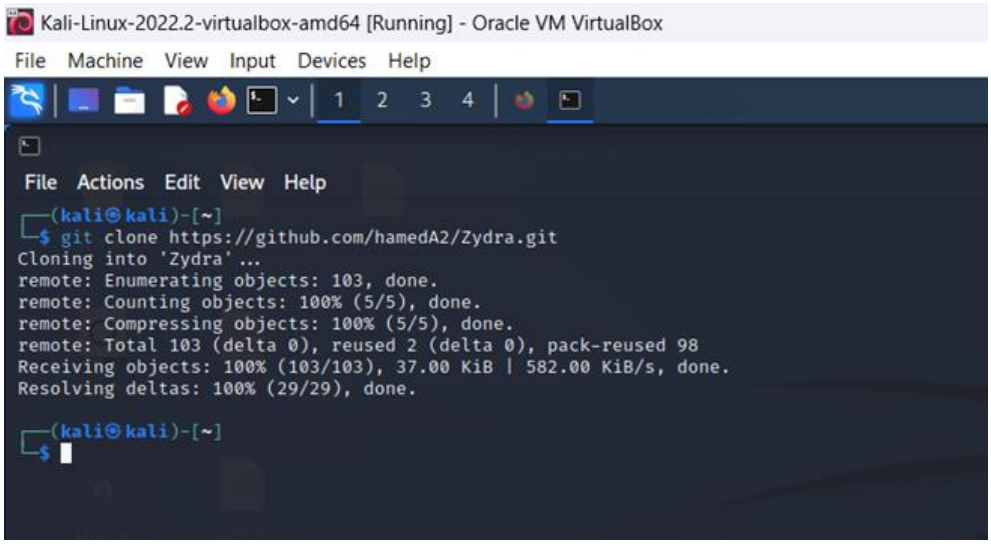


Crack Passwords of ZIP, RAR, PDF, Shadow files

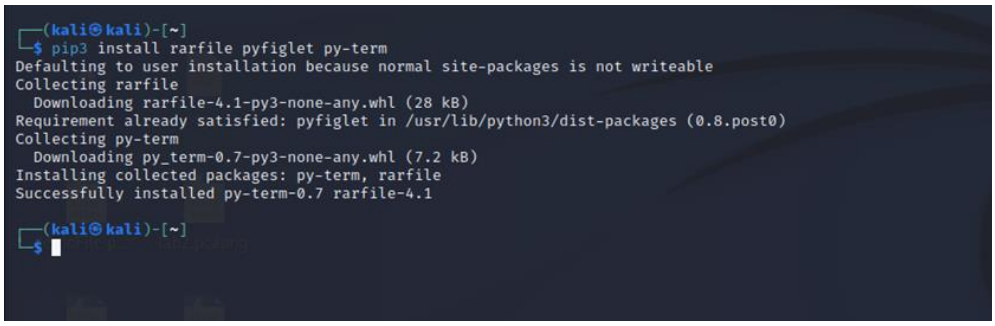
Everybody knows not to store sensitive information in unencrypted files, right? PDFs and ZIP files can often contain a treasure trove of information, such as network diagrams, IP addresses, and login credentials. Sometimes, even certain files that are encrypted aren't safe from attackers. That's where Zydra comes in — a tool for cracking RAR files, ZIP files, PDF files, and Linux shadow files.

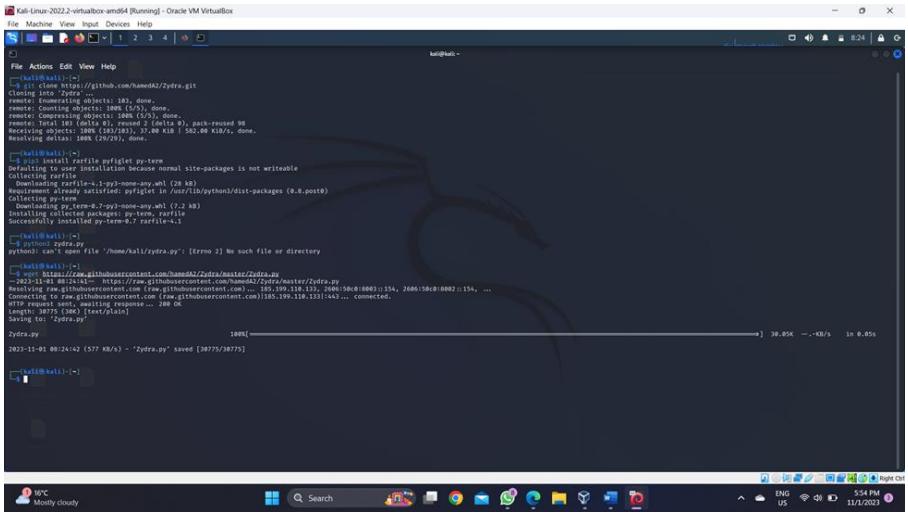
Depending on the program used and its version, these sorts of files could be password protected using various encryption algorithms. For example, the Linux command line zip utility uses the older PKZIP algorithm, which is insecure and easy to crack. Other programs, like WinZip and 7-Zip, use strong AES-256 encryption. Earlier versions of the RAR protocol use a proprietary encryption algorithm, while newer versions use AES. WinRAR and PeaZip, popular choices that can deal with RAR files, also use the AES standard.

Step 1: To begin, we need to download Zydra from GitHub — use the wget utility to grab the Python file right from the command line or clone as “git clone https://github.com/hamedA2/Zydra.git” or wget as

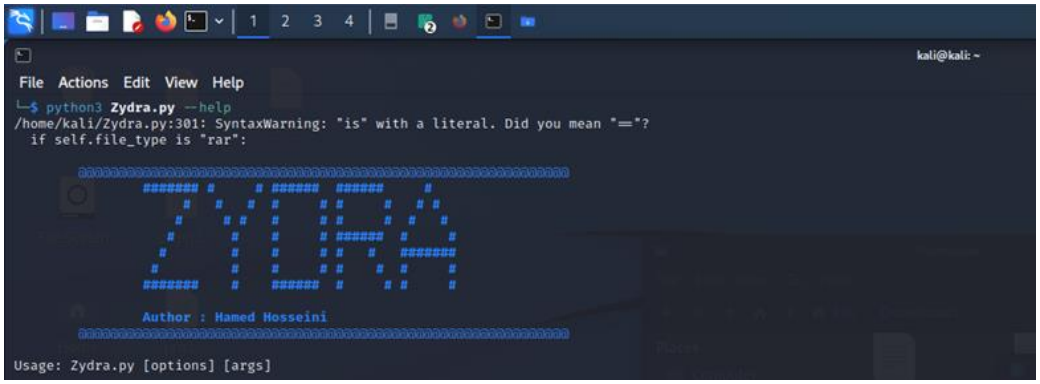


Step 2: install some dependencies for Zydra to work properly — it uses Python 3, so we can use pip3 to install the extra modules.





Step 3: Run Zydra using the python3 command.



Step 4: This gives us a nice little banner, a usage example, and options available.

Step 5: Now we need a suitable wordlist. I used wordlist from Github as https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/darkweb2017- top10.txt. You can download other wordlists you like.

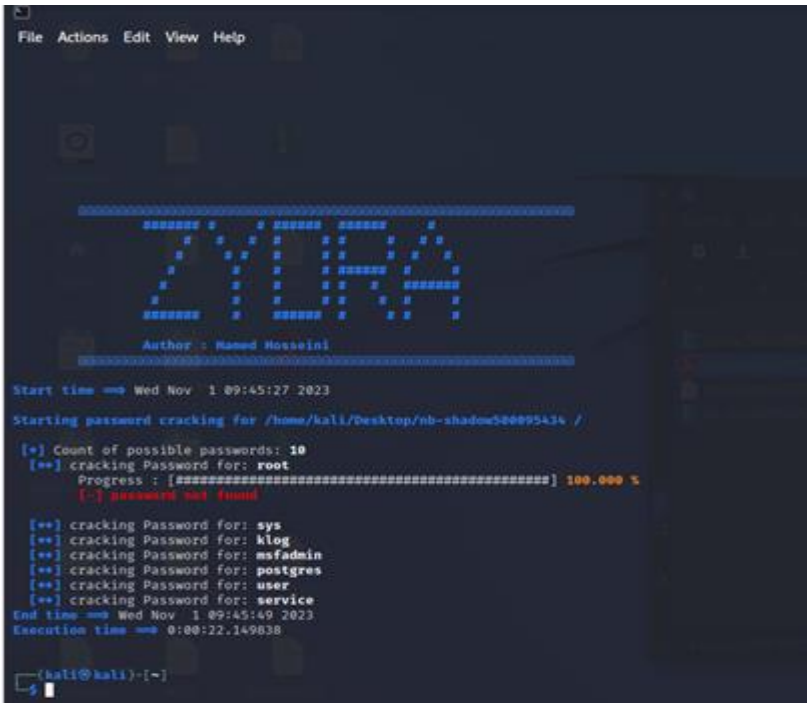
Step 6: Now we try to crack passwords of ZIP, RAR, PDF, Shadow files using Zydra.

Zip File:

PDF File:

RAR File:

Shadow File:



EXPERIMENT 7

__/__/__

IT NETWORK SECURITY
LAB 7

Khushi Wadhawan
500093673
B2

Q1). TCP :

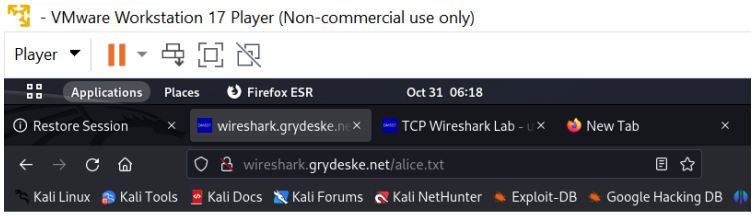
- Transmission Control Protocol
- Transport layer protocol that provides the transmission of packets from source to destination.
- Connection - oriented protocol
- takes the data from the app. layer, divides the data into several packets w/ a no. & then transmits them to dest.

Features of TCP:

i) Reliable :
- Follows flow & error control mechanism.
- works on an acknowledgement system.

ii) Connection - oriented :
- data exchange occurs only after the connection is established.

iii) Supports multiplexing:
- 3-way handshake
- multiple concurrent connections within a single network interface.



ALICE'S ADVENTURES IN WONDERLAND

Lewis Carroll

THE MILLENNIUM FULCRUM EDITION 3.0

CHAPTER I

Down the Rabbit-Hole

Alice was beginning to get very tired of sitting by her sister on the bank, and of having nothing to do: once or twice she had peeped into the book her sister was reading, but it had no pictures or conversations in it, `and what is the use of a book,' thought Alice `without pictures or conversation?'

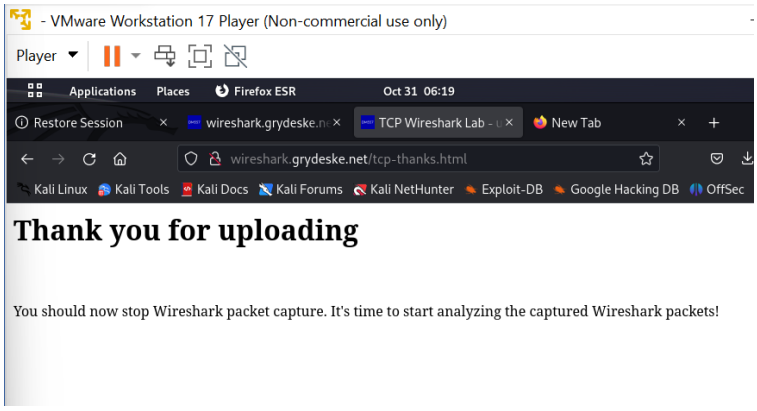
So she was considering in her own mind (as well as she could, for the hot day made her feel very sleepy and stupid), whether the pleasure of making a daisy-chain would be worth the trouble of getting up and picking the daisies, when suddenly a White Rabbit with pink eyes ran close by her.

There was nothing so VERY remarkable in that; nor did Alice think it so VERY much out of the way to hear the Rabbit say to itself, `Oh dear! Oh dear! I shall be late!' (when she thought it over afterwards, it occurred to her that she ought to have wondered at this, but at the time it all seemed quite natural); but when the Rabbit actually TOOK A WATCH OUT OF ITS WAISTCOAT-POCKET, and looked at it, and then hurried on, Alice started to her feet, for it flashed across her mind that she had never before seen a rabbit with either a waistcoat-pocket, or a watch to take out of it, and burning with curiosity, she ran across the field after it, and fortunately was just in time to see it pop down a large rabbit-hole under the hedge.

In another moment down went Alice after it, never once considering how in the world she was to get out again.

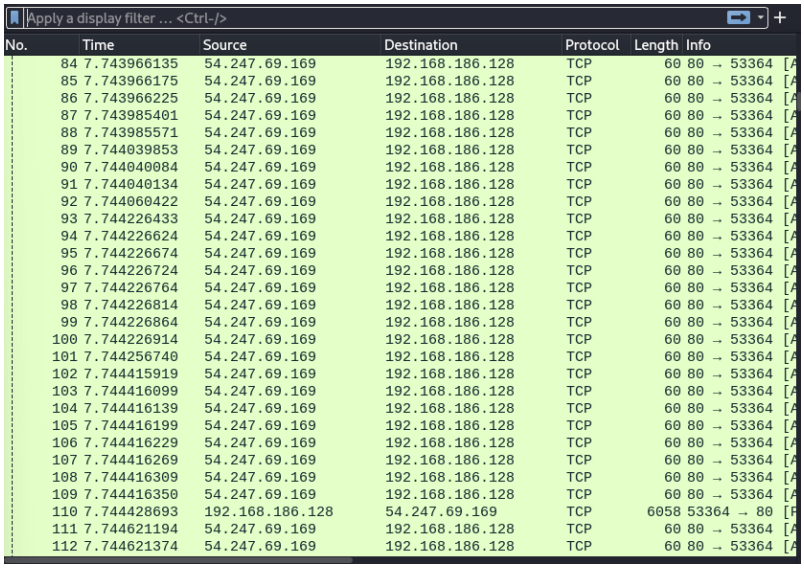
The rabbit-hole went straight on like a tunnel for some way, and then dipped suddenly down, so suddenly that Alice had not a moment to think about stopping herself before she found herself falling down a very deep well.

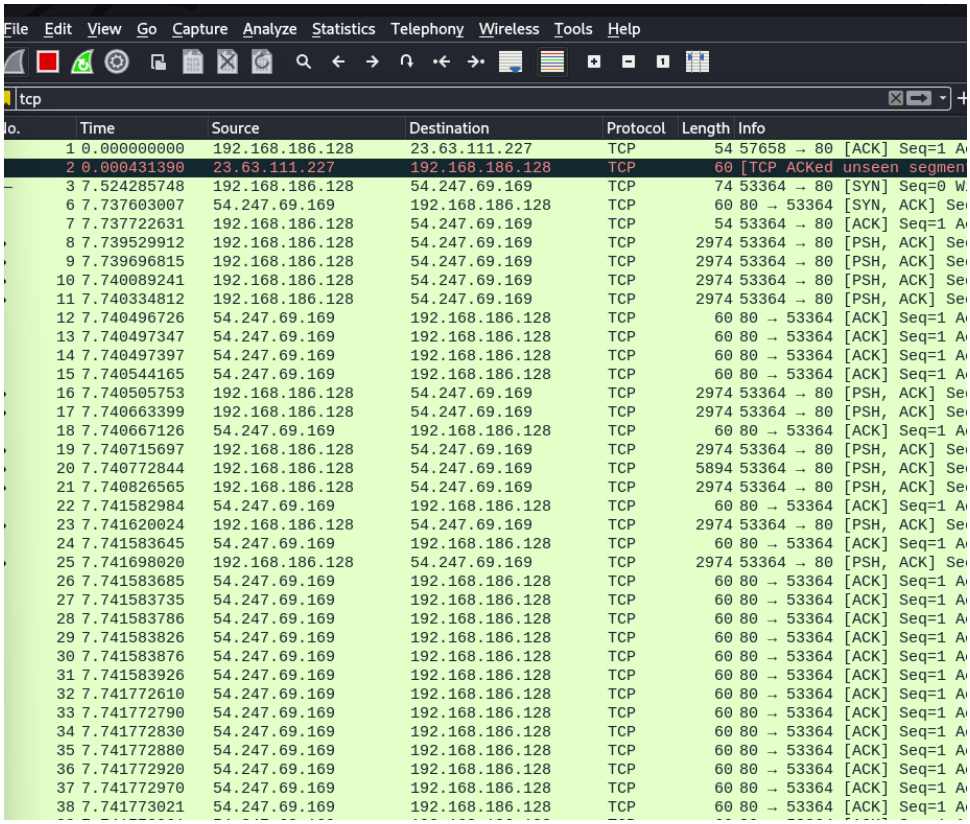
Either the well was very deep, or she fell very slowly, for she had plenty of time as she went down to look about her and to



Thank you for uploading

You should now stop Wireshark packet capture. It's time to start analyzing the captured Wireshark packets!


Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
84 7.743966135 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
85 7.743966175 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
86 7.743966225 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
87 7.743985401 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
88 7.743985571 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
89 7.744039853 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
90 7.744040084 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
91 7.744040134 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
92 7.744060422 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
93 7.744226433 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
94 7.744226624 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
95 7.744226674 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
96 7.744226724 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
97 7.744226764 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
98 7.744226814 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
99 7.744226864 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
100 7.744226914 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
101 7.744256740 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
102 7.744415919 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
103 7.744416099 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
104 7.744416139 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
105 7.744416199 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
106 7.744416229 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
107 7.744416269 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
108 7.744416309 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
109 7.744416350 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
110 7.744428693 192.168.186.128 54.247.69.169 TCP 6058 53364 → 80 [P
111 7.744621194 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A
112 7.744621374 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [A


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
lo. Time Source Destination Protocol Length Info
1 0.000000000 192.168.186.128 23.63.111.227 TCP 54 57658 → 80 [ACK] Seq=1 A
2 0.000431390 23.63.111.227 192.168.186.128 TCP 60 [TCP ACKed unseen segmen
3 7.524285748 192.168.186.128 54.247.69.169 TCP 74 53364 → 80 [SYN] Seq=0 W
6 7.737603007 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [SYN, ACK] Se
7 7.737722631 192.168.186.128 54.247.69.169 TCP 54 53364 → 80 [ACK] Seq=1 A
8 7.739529912 192.168.186.128 54.247.69.169 TCP 2974 53364 → 80 [PSH, ACK] Se
9 7.739696815 192.168.186.128 54.247.69.169 TCP 2974 53364 → 80 [PSH, ACK] Se
10 7.740089241 192.168.186.128 54.247.69.169 TCP 2974 53364 → 80 [PSH, ACK] Se
11 7.740334812 192.168.186.128 54.247.69.169 TCP 2974 53364 → 80 [PSH, ACK] Se
12 7.740496726 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
13 7.740497347 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
14 7.740497397 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
15 7.740544165 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
16 7.740505753 192.168.186.128 54.247.69.169 TCP 2974 53364 → 80 [PSH, ACK] Se
17 7.740663399 192.168.186.128 54.247.69.169 TCP 2974 53364 → 80 [PSH, ACK] Se
18 7.740667126 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
19 7.740715697 192.168.186.128 54.247.69.169 TCP 2974 53364 → 80 [PSH, ACK] Se
20 7.740772844 192.168.186.128 54.247.69.169 TCP 5894 53364 → 80 [PSH, ACK] Se
21 7.740826565 192.168.186.128 54.247.69.169 TCP 2974 53364 → 80 [PSH, ACK] Se
22 7.741582984 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
23 7.741620024 192.168.186.128 54.247.69.169 TCP 2974 53364 → 80 [PSH, ACK] Se
24 7.741583645 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
25 7.741698020 192.168.186.128 54.247.69.169 TCP 2974 53364 → 80 [PSH, ACK] Se
26 7.741583685 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
27 7.741583735 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
28 7.741583786 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
29 7.741583826 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
30 7.741583876 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
31 7.741583926 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
32 7.741772610 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
33 7.741772790 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
34 7.741772830 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
35 7.741772880 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
36 7.741772920 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
37 7.741772970 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A
38 7.741773021 54.247.69.169 192.168.186.128 TCP 60 80 → 53364 [ACK] Seq=1 A

```
POST /tcp-thanks.html HTTP/1.1
Host: wireshark.grydeske.net
User-Agent:  (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/
605.1.15 (KHTML, like Gecko) Version/15.4 Safari/605.1.15
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------234005332668943405511382139 88
Content-Length: 152357
Origin: http://wireshark.grydeske.net
DNT: 1
Connection: keep-alive
Referer: http://wireshark.grydeske.net/tcp-upload.html
Upgrade-Insecure-Requests: 1

-----------------------------234005332668943405511382139 88
Content-Disposition: form-data; name="file"; filename="alice.txt"
Content-Type: text/plain

                ALICE'S ADVENTURES IN WONDERLAND

                            Lewis Carroll

              THE MILLENNIUM FULCRUM EDITION 3.0



                        CHAPTER I

                    Down the Rabbit-Hole


  Alice was beginning to get very tired of sitting by her sister
on the bank, and of having nothing to do:  once or twice she had
peeped into the book her sister was reading, but it had no
pictures or conversations in it, `and what is the use of a book,'
thought Alice `without pictures or conversation?'

  So she was considering in her own mind (as well as she could,
for the hot day made her feel very sleepy and stupid), whether
```

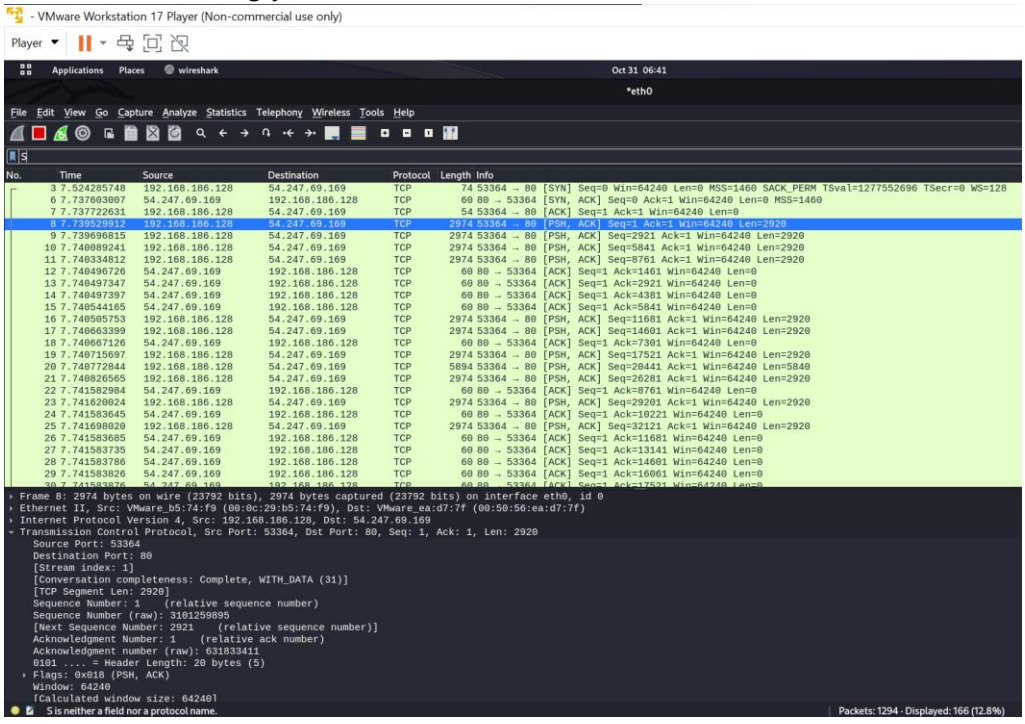
25 client pkts, 1 server pkt, 1 turn.

Entire conversation (154 kB) | Show data as ASCII | Stream 1

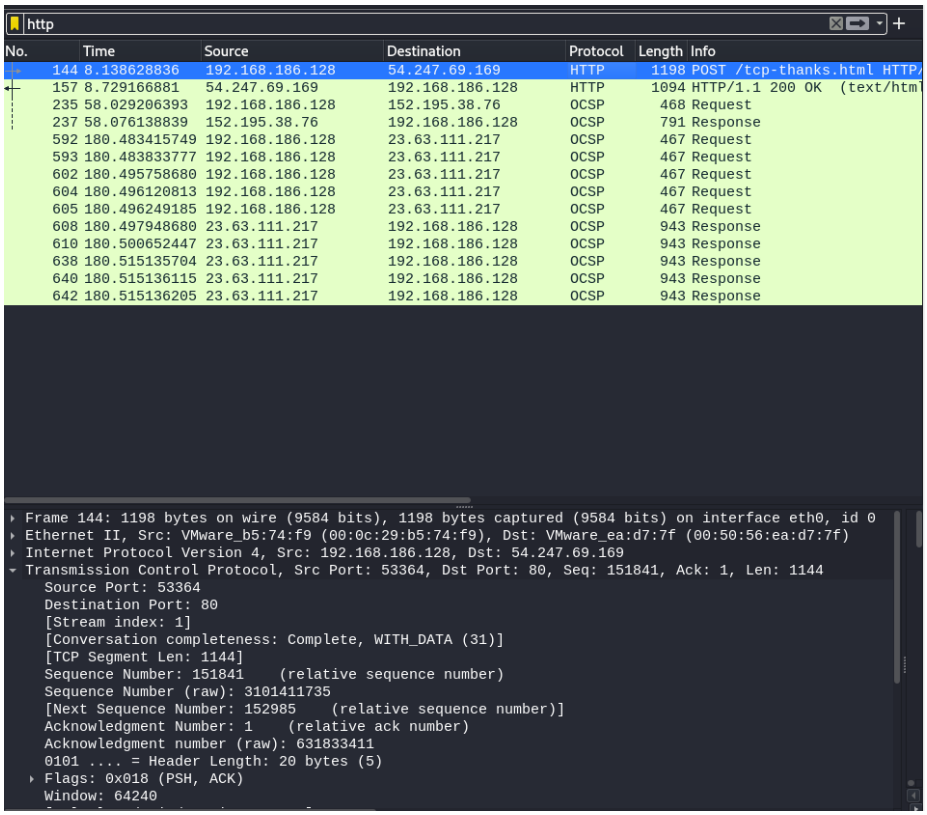
Find: | Find Next

Questions:

What is the IP address and TCP port number used by the client computer (source) that is transferring the file to wireshark.grydeske.net?

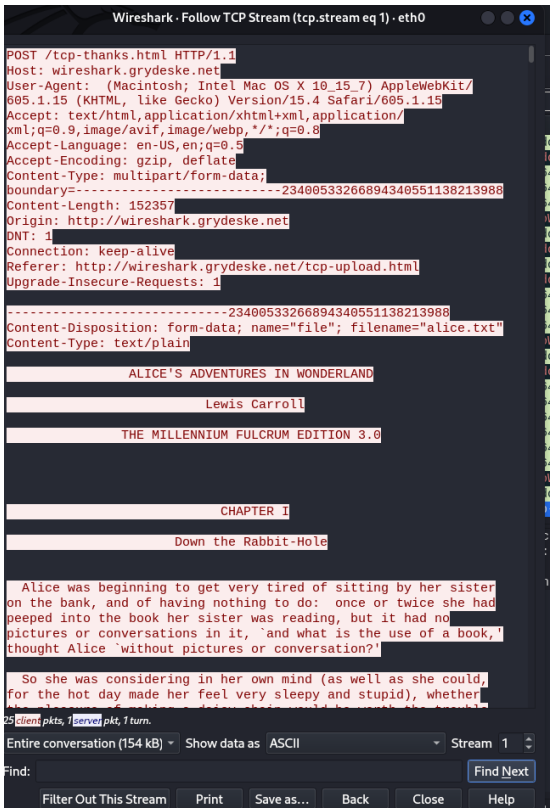


What do you see on filtering for ‘http’? Is there any POST?



What do you see on trying to view the ‘TCP Stream’ conversation?

Yes

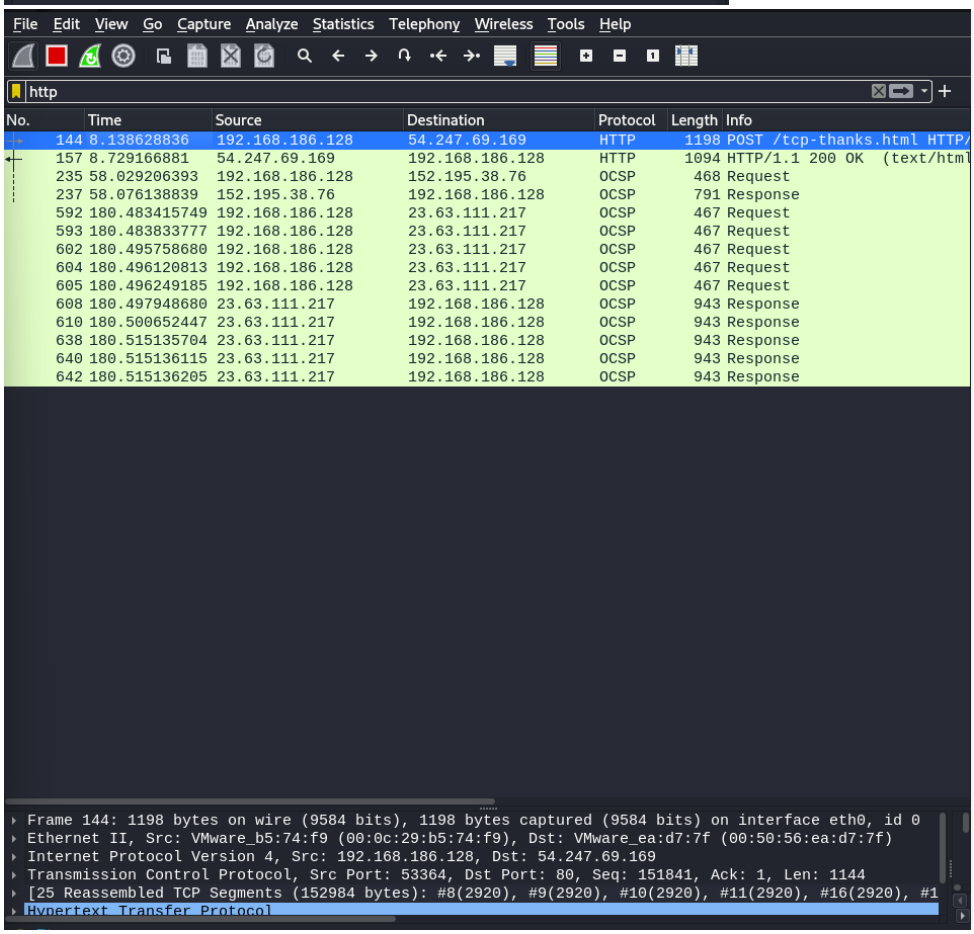


Check and find the user's OS and Web browser versions during the interaction.

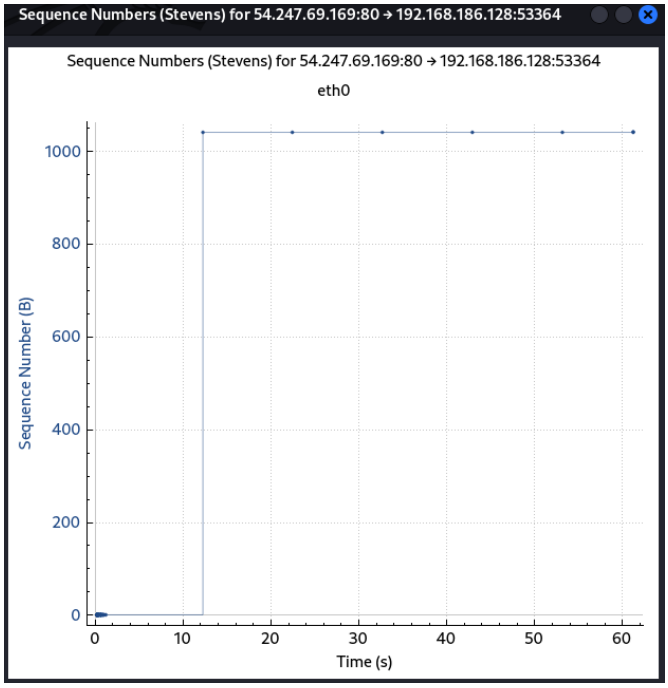
```
POST /tcp-thanks.html HTTP/1.1
Host: wireshark.grydeske.net
User-Agent:  (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/
605.1.15 (KHTML, like Gecko) Version/15.4 Safari/605.1.15
```

Check for Web server settings (language, encoding, site size, domain etc.)

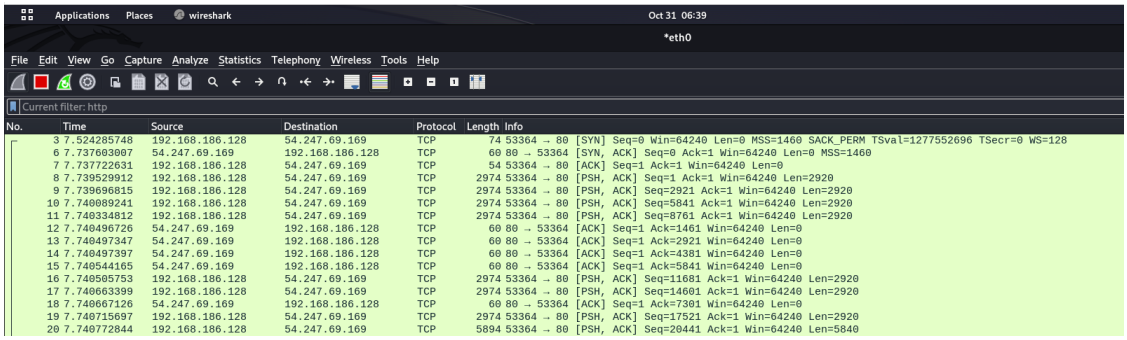
```
POST /tcp-thanks.html HTTP/1.1
Host: wireshark.grydeske.net
User-Agent:  (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/
605.1.15 (KHTML, like Gecko) Version/15.4 Safari/605.1.15
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------234005332668943405511382139 88
Content-Length: 152357
Origin: http://wireshark.grydeske.net
DNT: 1
Connection: keep-alive
Referer: http://wireshark.grydeske.net/tcp-upload.html
Upgrade-Insecure-Requests: 1

-----------------------------234005332668943405511382139 88
Content-Disposition: form-data; name="file"; filename="alice.txt"
Content-Type: text/plain
```



Analyze the TCP Segments by displaying a TCP graph.



Display three-way handshake between grydeske.net and the client computer (SYN-SYN-ACK-ACK)?



EXPERIMENT 8

__/__/____

IT NETWORK SECURITY

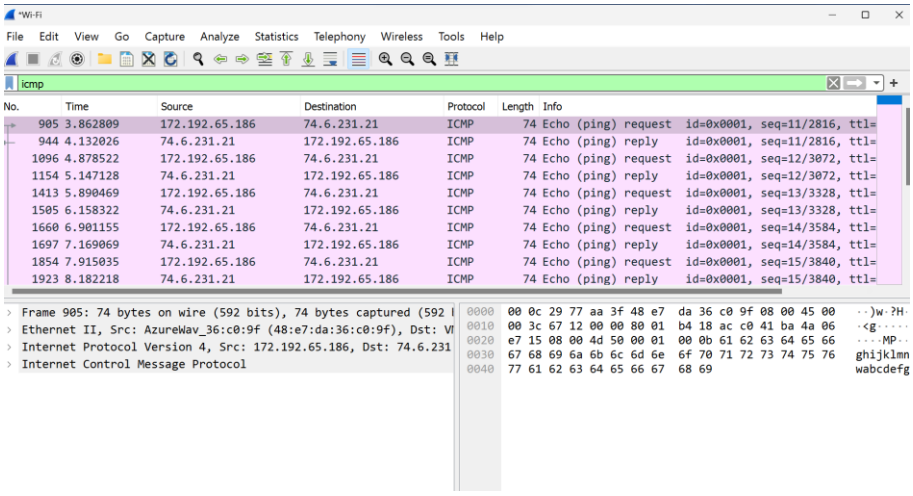
LAB - 8

Khushi Wadhawan
500093673
B2

A1.) ICMP operates within the TCP/IP suite & serves as a means of transmitting control messages & error reports b/w networked devices. These messages, encapsulated within IP packets contain information about network issues & diagnostics. ICMP utilizes type & code fields to specify the purpose & subtype of the message enabling function like "ping" requests to check the reachability of remote hosts & diagnose network problems. This protocol is indispensible for network administrators to troubleshoot issues & maintain efficient data transmission across the internet.

A2). It is primarily used for error reporting, allowing network devices to send messages to inform others of issues encountered during data transmission, like when a dest. is unreachable. ICMP is essential for network diagnostics or tools like "ping" using ICMP to check the responsiveness of remote hosts & diagnose connectivity problems. It also plays a role in detecting time - exceeding packets.

```
Pinging yahoo.com [74.6.231.21] with 32 bytes of data:
Reply from 74.6.231.21: bytes=32 time=269ms TTL=44
Reply from 74.6.231.21: bytes=32 time=268ms TTL=44
Reply from 74.6.231.21: bytes=32 time=268ms TTL=44
Reply from 74.6.231.21: bytes=32 time=268ms TTL=44
Reply from 74.6.231.21: bytes=32 time=267ms TTL=44
Reply from 74.6.231.21: bytes=32 time=267ms TTL=44
Reply from 74.6.231.21: bytes=32 time=268ms TTL=44
Reply from 74.6.231.21: bytes=32 time=269ms TTL=44
Reply from 74.6.231.21: bytes=32 time=269ms TTL=44
Reply from 74.6.231.21: bytes=32 time=273ms TTL=44

Ping statistics for 74.6.231.21:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 267ms, Maximum = 273ms, Average = 268ms
```

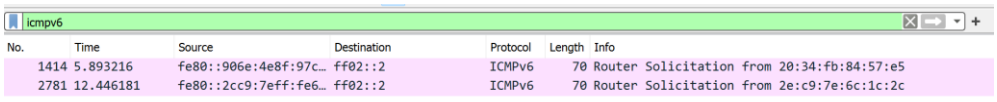


PART A:

• What is the IP address of your host?
Answer: 172.192.65.186

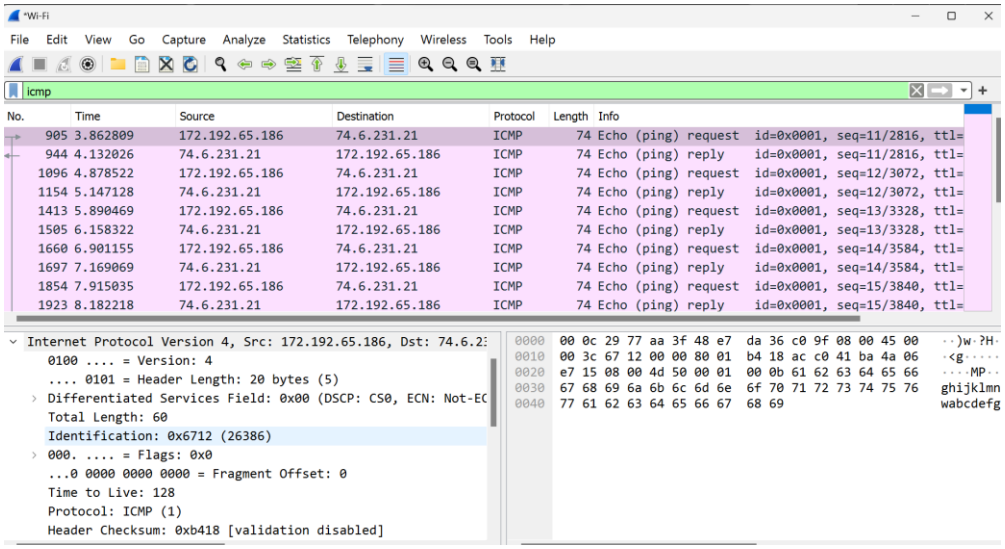
• What is the IP address of the destination host?
Answer: 74.6.231.21

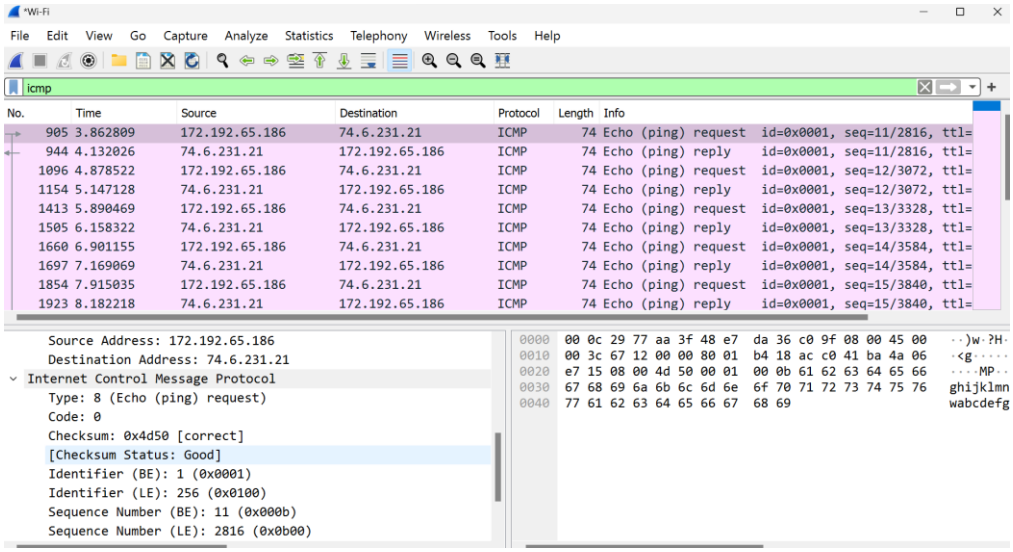
• Why is it that an ICMP packet does not have source and destination port numbers?
Answer:

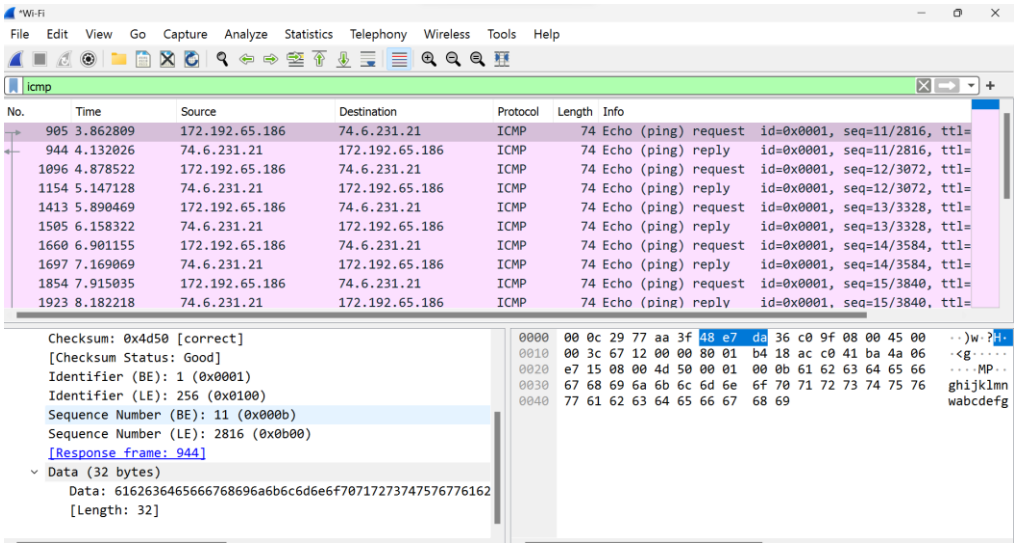


• Examine one of the ping request packets sent by your host - take a screenshot of wireshark with the ICMP packet expanded.

Answer:

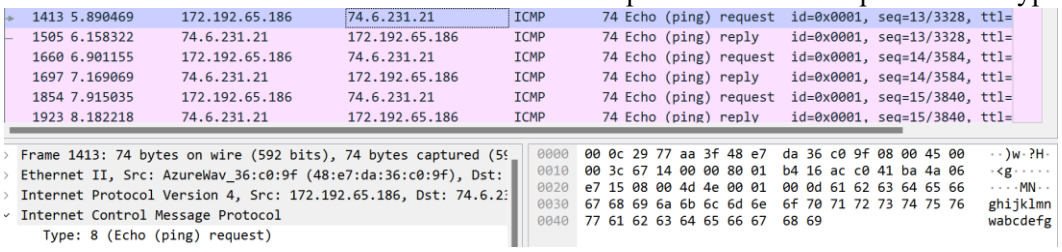




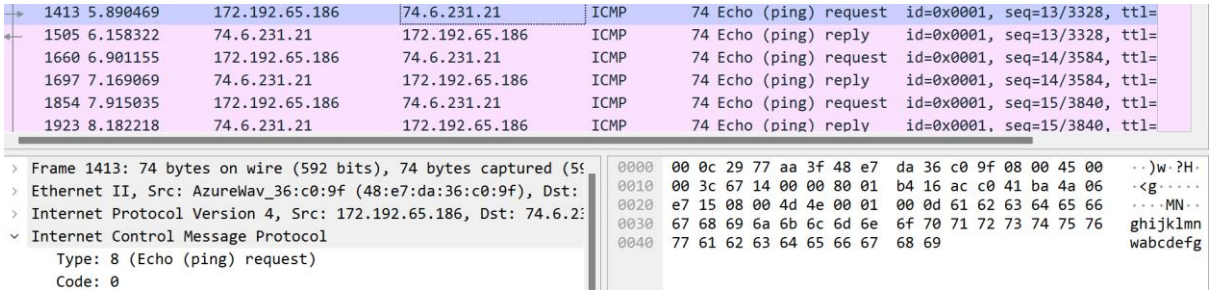


• What are the ICMP type number?

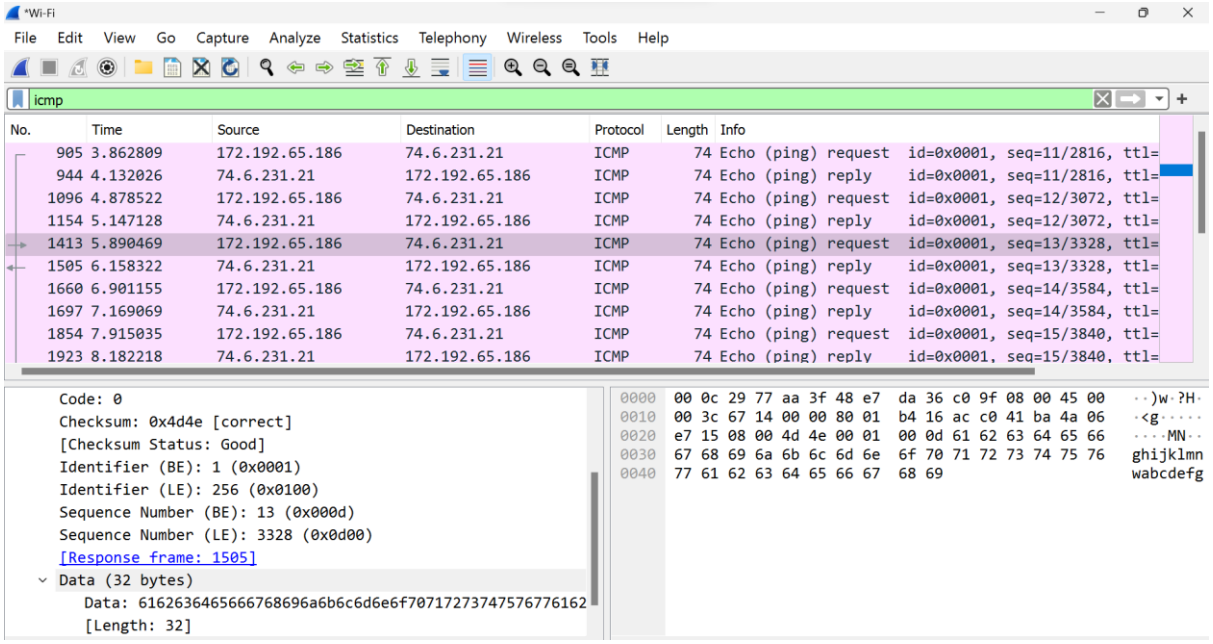
Answer: for echo request icmp type 8



• What are the ICMP code number?
Answer: for both echo request code is 0

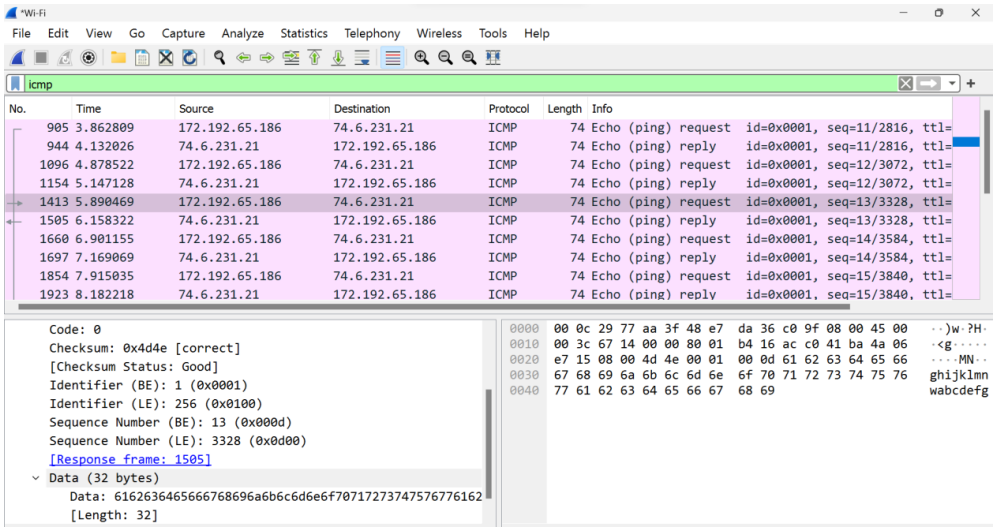


• What other fields does this ICMP packet have?
Answer:



Other fields like checksum, identifier, sequence number

• How many bytes are the checksum, sequence number and identifier fields?
Answer:



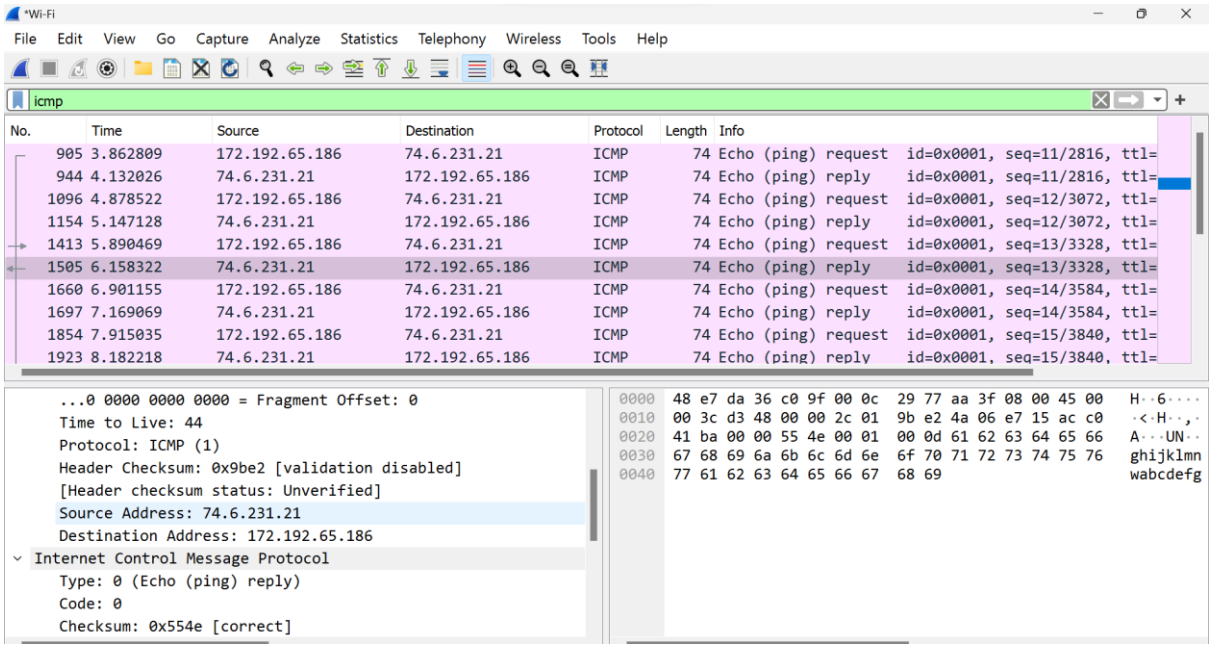
Checksum 2 bytes

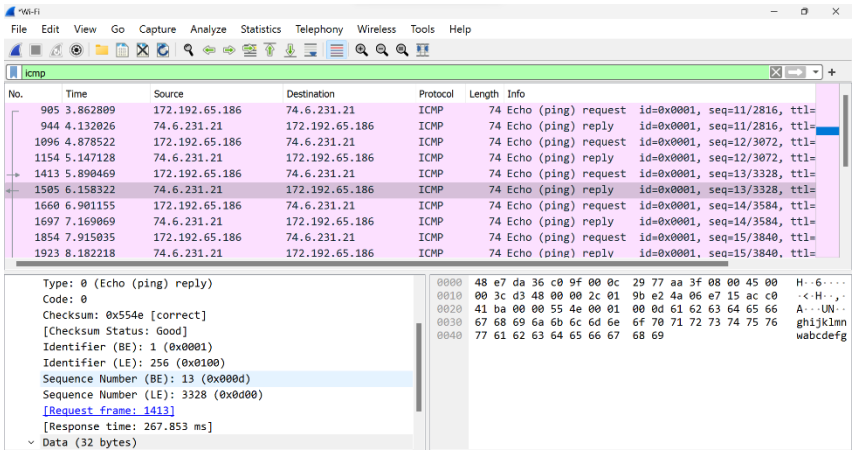
Identifier 2 bytes

Sequence number 2 bytes

• Examine the corresponding ping reply packet - take a screenshot of wireshark with the ICMP packet expanded.

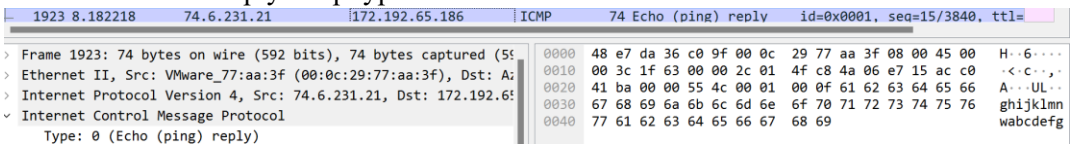
Answer:





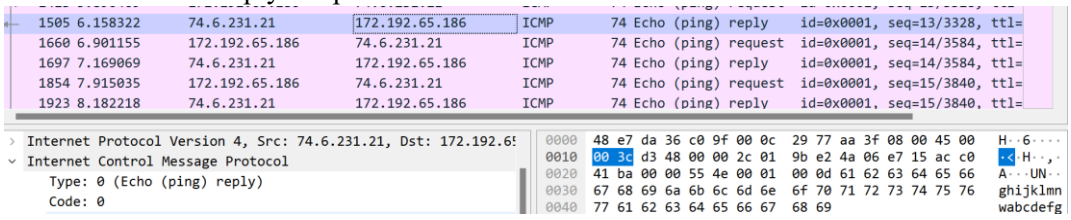
• What are the ICMP type number?

Answer: for echo reply icmp type 0



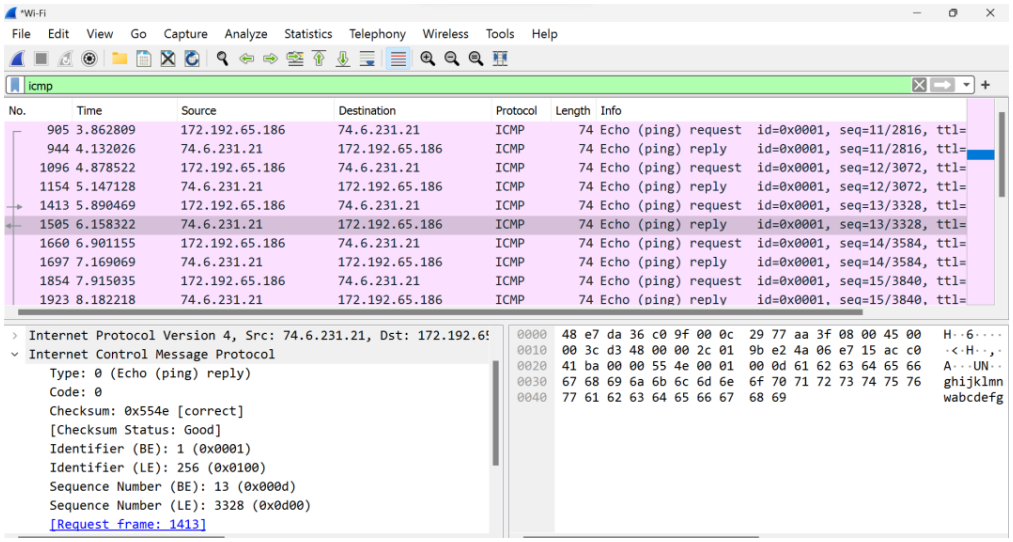
• What are the ICMP code number?

Answer: for echo reply icmp code number is 0



• What other fields does this ICMP packet have?

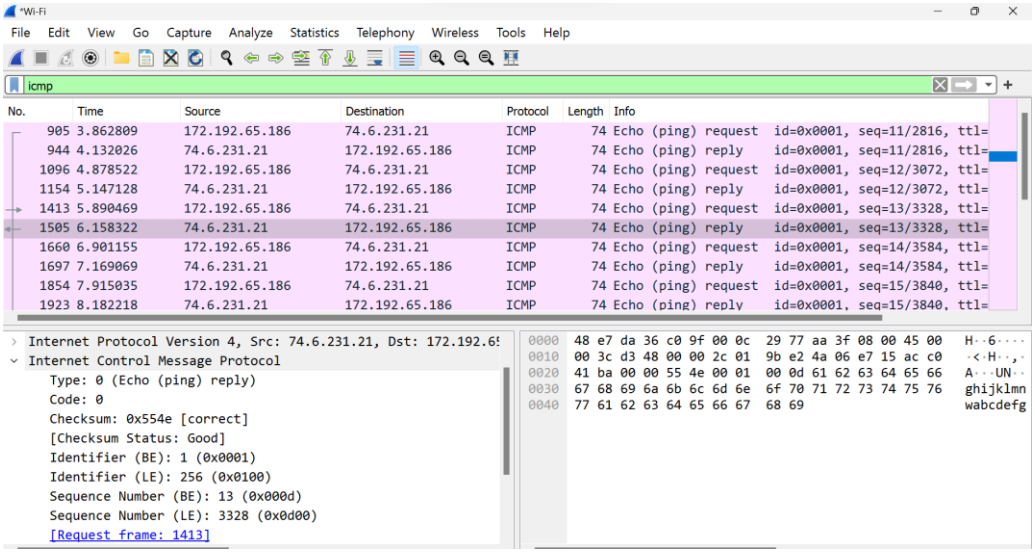
Answer:



Other fields like checksum, identifier , sequence number

• How many bytes are the checksum, sequence number and identifier fields?

Answer:

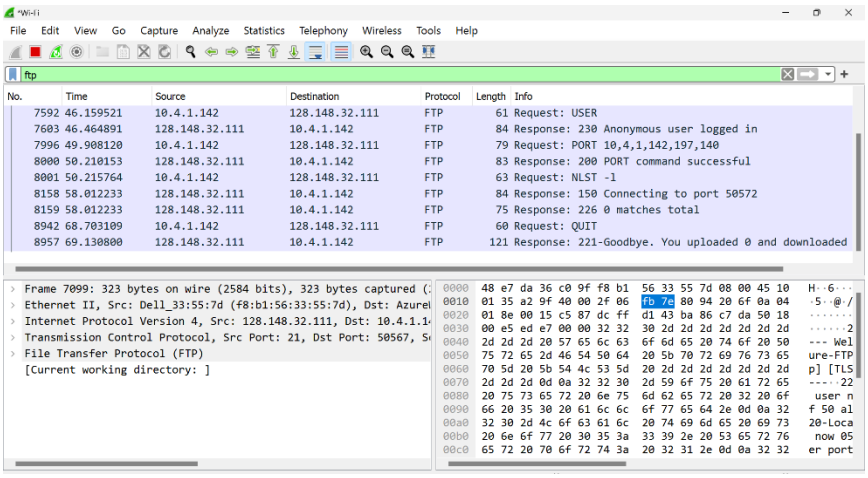


Checksum 2 bytes

Identifier 2 bytes

Sequence number 2 bytes

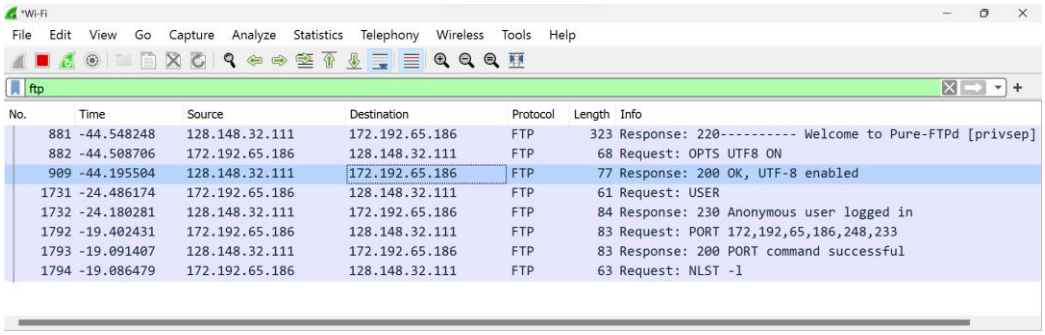
```
Connected to ftp.cs.brown.edu.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 2 of 50 allowed.
220-Local time is now 05:39. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
200 OK, UTF-8 enabled
User (ftp.cs.brown.edu:(none)):
230 Anonymous user logged in
ftp> ls -l
200 PORT command successful
150 Connecting to port 50572
226 0 matches total
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
```



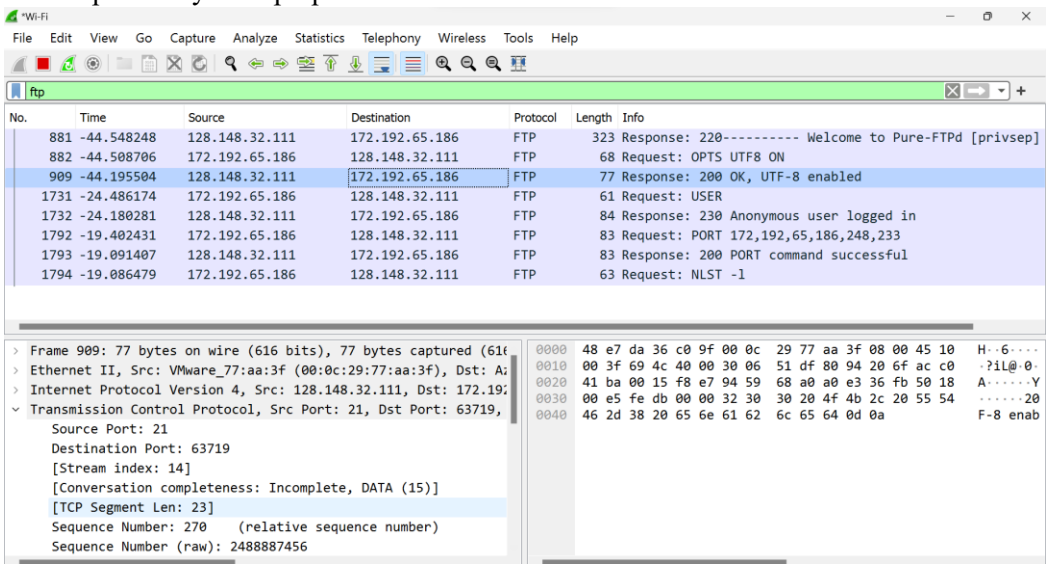
Part B

• What does FTP filter describe?
Answer: An FTP filter is a security feature that controls access to an FTP server. It can be used to allow or deny specific FTP commands, file name extensions, or IP addresses. FTP filters can be used to protect against unauthorized access, data theft, and malware attacks.
In short, an FTP filter is a way to control what can and cannot be done on an FTP server.

• What is the FTP Server IP Address?
Answer : 128.148.32.111



• What port did your laptop connect with the FTP Server?



Source port 21

EXPERIMENT 9

__/__/____

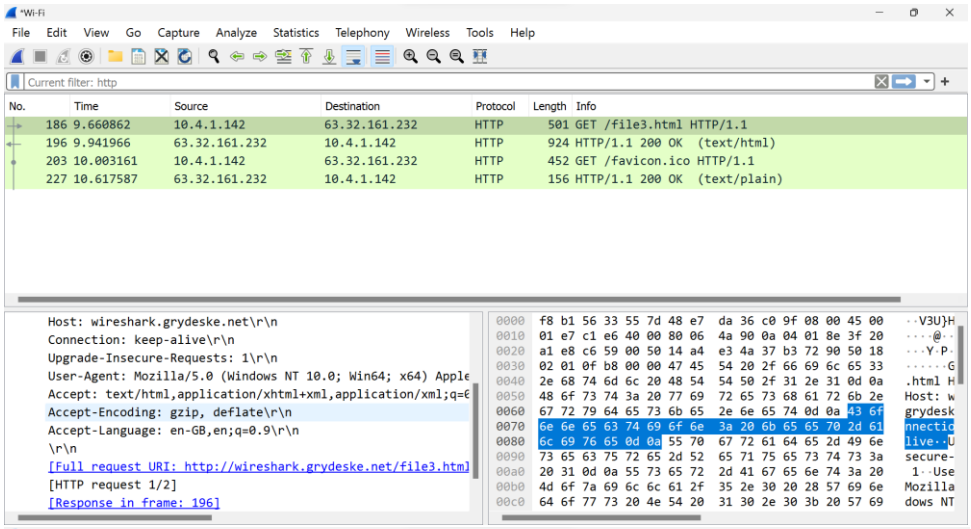
IT NETWORK SECURITY

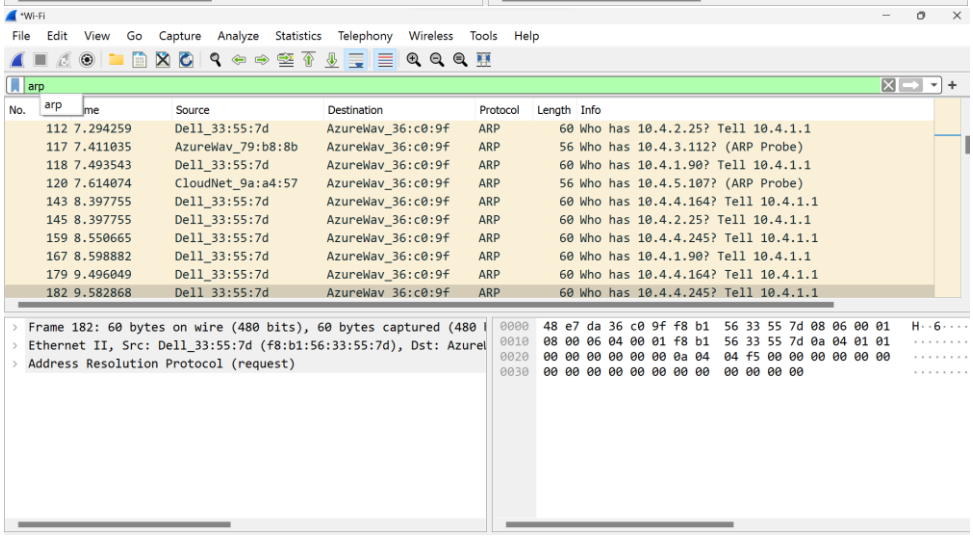
LAB 9

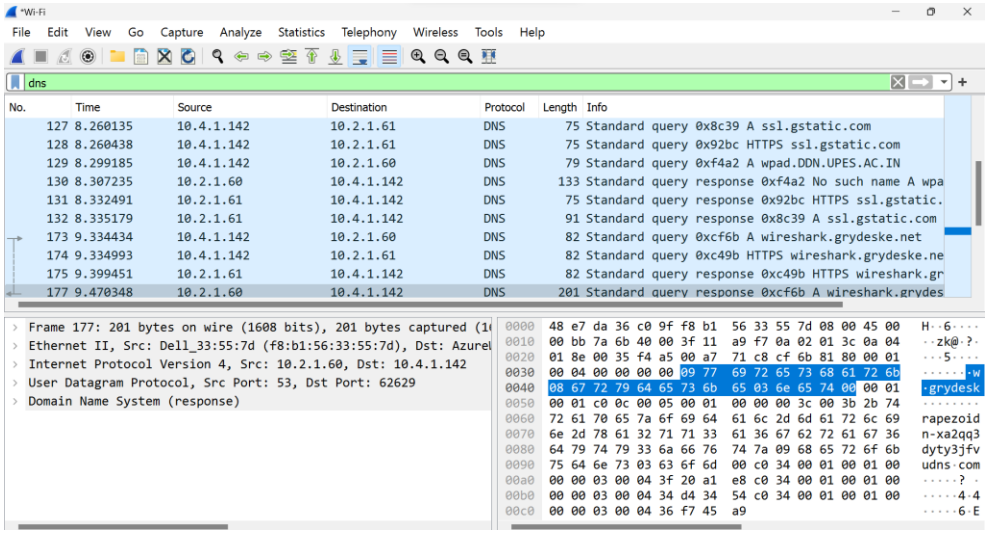
Khushi Wadhawan
F009367 3
B2.

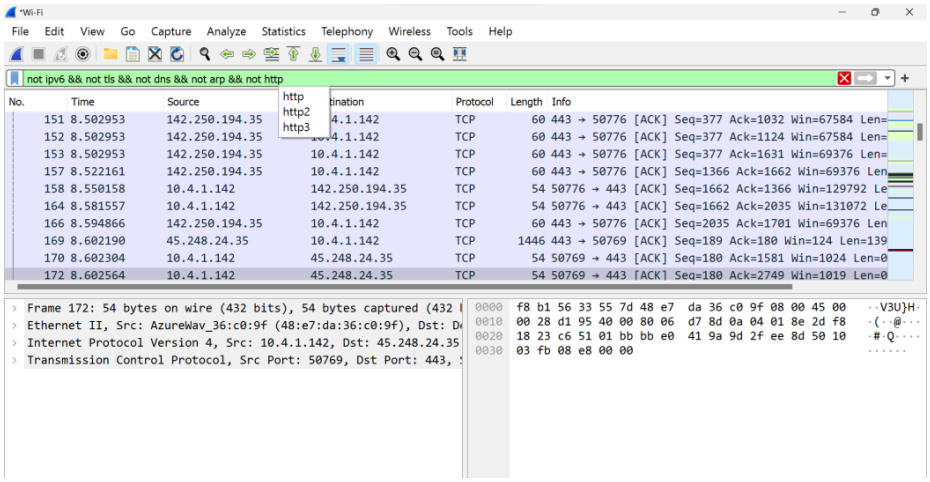
Q1.) HTTP GET filtering is a method used in web applications to request specific data from a server by including parameters in the URL of an HTTP GET request. These parameter act as a filter allowing users to refine the results they receive. For instance in an online store, you could use this technique to find electronic products with a price range. HTTP GET filtering is a vital component of web apps. & APIs, enhancing user interactions by tailoring the data returned from the server to meet specific criteria.

Q2.) A 32 bit IP Addres is a numerical label assigned to each device connected to a computer network that uses the internet protocol for communication. IPV4 addresses are typically represented as 4 sets of decimal numbers separated by periods (eg. 192.168.1.1). Each set consists of 8-bits, making a total of 32-bits for the entire address. IPv4 addresses are used to identify devices on a network & are essential for routing data across the internet.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http
No. Time Source Destination Protocol Length Info
186 9.660862 10.4.1.142 63.32.161.232 HTTP 501 GET /file3.html HTTP/1.1
196 9.941966 63.32.161.232 10.4.1.142 HTTP 924 HTTP/1.1 200 OK (text/html)
203 10.003161 10.4.1.142 63.32.161.232 HTTP 452 GET /favicon.ico HTTP/1.1
227 10.617587 63.32.161.232 10.4.1.142 HTTP 156 HTTP/1.1 200 OK (text/plain)
Host: wireshark.grydeske.net\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
Accept: text/html,application/xhtml+xml,application/xml;q=0
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en;q=0.9\r\n
\r\n
[Full request URI: http://wireshark.grydeske.net/file3.html]
[HTTP request 1/2]
[Response in frame: 196]
0000 f8 b1 56 33 55 7d 48 e7 da 36 c0 9f 08 00 45 00 ··V3U}H ··6····E·
0010 01 e7 c1 e6 40 00 80 06 4a 90 0a 04 01 8e 3f 20 ····@··· J·····?
0020 a1 e8 c6 59 00 50 14 a4 e3 4a 37 b3 72 90 50 18 ···Y·P·· ·J7·r·P·
0030 02 01 0f b8 00 00 47 45 54 20 2f 66 69 6c 65 33 ·····GE T /file3
0040 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1··
0050 48 6f 73 74 3a 20 77 69 72 65 73 68 61 72 6b 2e Host: wi reshark.
0060 67 72 79 64 65 73 6b 65 2e 6e 65 74 0d 0a 43 6f grydeske .net··Co
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection: keep-a
0080 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e live··Up grade-In
0090 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-R equests:
00a0 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 1··User- Agent:
00b0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla /5.0 (Win
00c0 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 dows NT 10.0; Wi

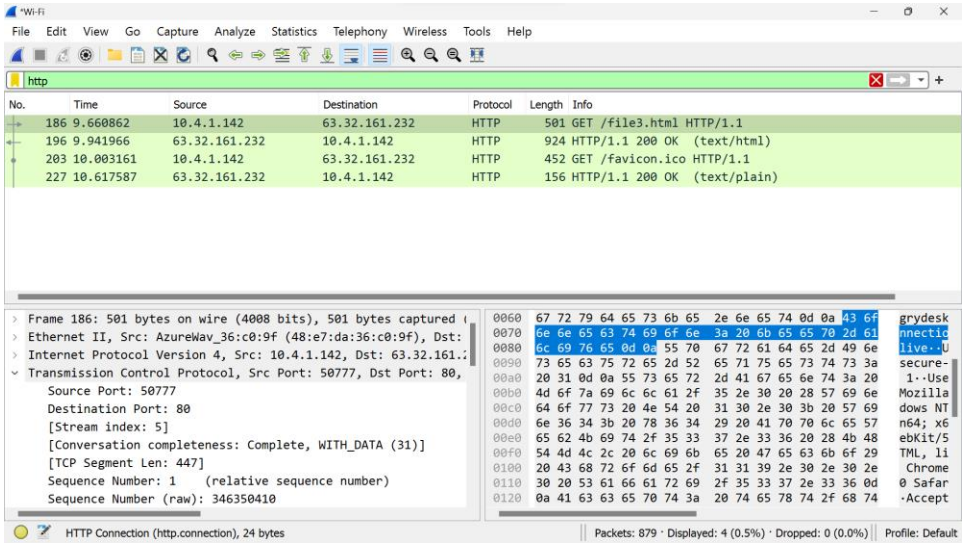

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
112 7.294259 Dell_33:55:7d AzureWav_36:c0:9f ARP 60 Who has 10.4.2.25? Tell 10.4.1.1
117 7.411035 AzureWav_79:b8:8b AzureWav_36:c0:9f ARP 56 Who has 10.4.3.112? (ARP Probe)
118 7.493543 Dell_33:55:7d AzureWav_36:c0:9f ARP 60 Who has 10.4.1.90? Tell 10.4.1.1
120 7.614074 CloudNet_9a:a4:57 AzureWav_36:c0:9f ARP 56 Who has 10.4.5.107? (ARP Probe)
143 8.397755 Dell_33:55:7d AzureWav_36:c0:9f ARP 60 Who has 10.4.4.164? Tell 10.4.1.1
145 8.397755 Dell_33:55:7d AzureWav_36:c0:9f ARP 60 Who has 10.4.2.25? Tell 10.4.1.1
159 8.550665 Dell_33:55:7d AzureWav_36:c0:9f ARP 60 Who has 10.4.4.245? Tell 10.4.1.1
167 8.598882 Dell_33:55:7d AzureWav_36:c0:9f ARP 60 Who has 10.4.1.90? Tell 10.4.1.1
179 9.496049 Dell_33:55:7d AzureWav_36:c0:9f ARP 60 Who has 10.4.4.164? Tell 10.4.1.1
182 9.582868 Dell_33:55:7d AzureWav_36:c0:9f ARP 60 Who has 10.4.4.245? Tell 10.4.1.1
Frame 182: 60 bytes on wire (480 bits), 60 bytes captured (480
Ethernet II, Src: Dell_33:55:7d (f8:b1:56:33:55:7d), Dst: Azurel
Address Resolution Protocol (request)
0000 48 e7 da 36 c0 9f f8 b1 56 33 55 7d 08 06 00 01 H··6···· V3U}····
0010 08 00 06 04 00 01 f8 b1 56 33 55 7d 0a 04 01 01 ····· V3U}····
0020 00 00 00 00 00 00 0a 04 04 f5 00 00 00 00 00 00 ····· ·····
0030 00 00 00 00 00 00 00 00 00 00 00 00 ····· ····

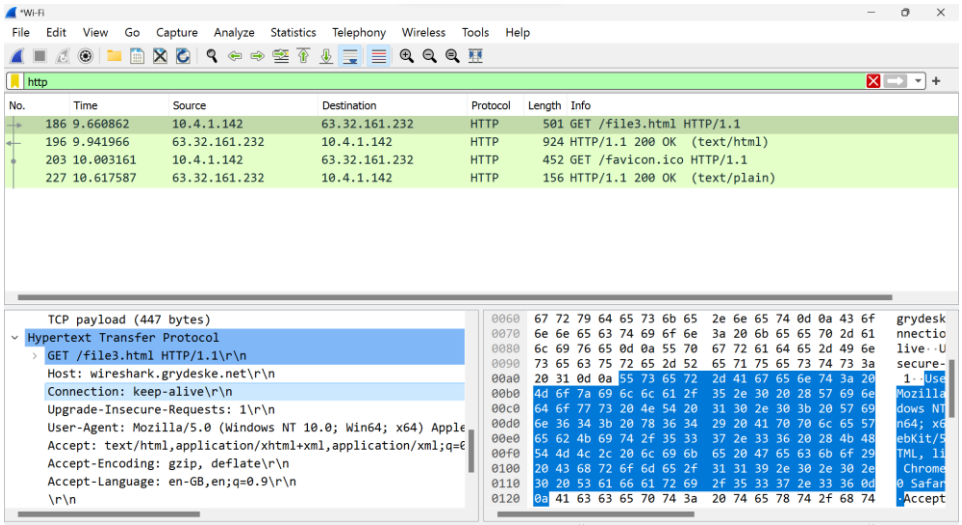

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
127 8.260135 10.4.1.142 10.2.1.61 DNS 75 Standard query 0x8c39 A ssl.gstatic.com
128 8.260438 10.4.1.142 10.2.1.61 DNS 75 Standard query 0x92bc HTTPS ssl.gstatic.com
129 8.299185 10.4.1.142 10.2.1.60 DNS 79 Standard query 0xf4a2 A wpad.DDN.UPES.AC.IN
130 8.307235 10.2.1.60 10.4.1.142 DNS 133 Standard query response 0xf4a2 No such name A wpa
131 8.332491 10.2.1.61 10.4.1.142 DNS 75 Standard query response 0x92bc HTTPS ssl.gstatic.
132 8.335179 10.2.1.61 10.4.1.142 DNS 91 Standard query response 0x8c39 A ssl.gstatic.com
173 9.334434 10.4.1.142 10.2.1.60 DNS 82 Standard query 0xcf6b A wireshark.grydeske.net
174 9.334993 10.4.1.142 10.2.1.61 DNS 82 Standard query 0xc49b HTTPS wireshark.grydeske.ne
175 9.399451 10.2.1.61 10.4.1.142 DNS 82 Standard query response 0xc49b HTTPS wireshark.gr
177 9.470348 10.2.1.60 10.4.1.142 DNS 201 Standard query response 0xcf6b A wireshark.grydes
Frame 177: 201 bytes on wire (1608 bits), 201 bytes captured (1
Ethernet II, Src: Dell_33:55:7d (f8:b1:56:33:55:7d), Dst: Azurel
Internet Protocol Version 4, Src: 10.2.1.60, Dst: 10.4.1.142
User Datagram Protocol, Src Port: 53, Dst Port: 62629
Domain Name System (response)
0000 48 e7 da 36 c0 9f f8 b1 56 33 55 7d 08 00 45 00 H··6···· V3U}··E·
0010 00 bb 7a 6b 40 00 3f 11 a9 f7 0a 02 01 3c 0a 04 ··zk@·?· ·····<··
0020 01 8e 00 35 f4 a5 00 a7 71 c8 cf 6b 81 80 00 01 ···5···· q··k····
0030 00 04 00 00 00 00 09 77 69 72 65 73 68 61 72 6b ·····w ireshark
0040 08 67 72 79 64 65 73 6b 65 03 6e 65 74 00 00 01 ·grydesk e·net···
0050 00 01 c0 0c 00 05 00 01 00 00 00 3c 00 3b 2b 74 ····· ····<·;+t
0060 72 61 70 65 7a 6f 69 64 61 6c 2d 6d 61 72 6c 69 rapezoid al-marli
0070 6e 2d 78 61 32 71 71 33 61 36 67 62 72 61 67 36 n-xa2qq3 a6gbrag6
0080 64 79 74 79 33 6a 66 76 74 7a 09 68 65 72 6f 6b dyty3jfv tz·herok
0090 75 64 6e 73 03 63 6f 6d 00 c0 34 00 01 00 01 00 udns·com ··4·····
00a0 00 00 03 00 04 3f 20 a1 e8 c0 34 00 01 00 01 00 ····· ? ····4·····
00b0 00 00 03 00 04 34 d4 34 54 c0 34 00 01 00 01 00 ····· 4·4T·4·····
00c0 00 00 03 00 04 36 f7 45 a9 ····· 6·E·



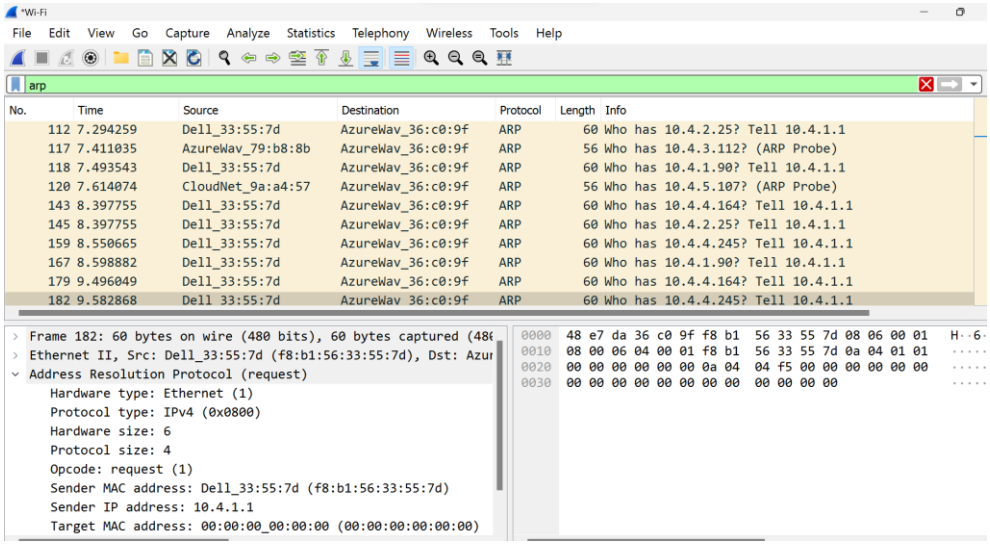
Explain what you found from HTTP GET filtering?

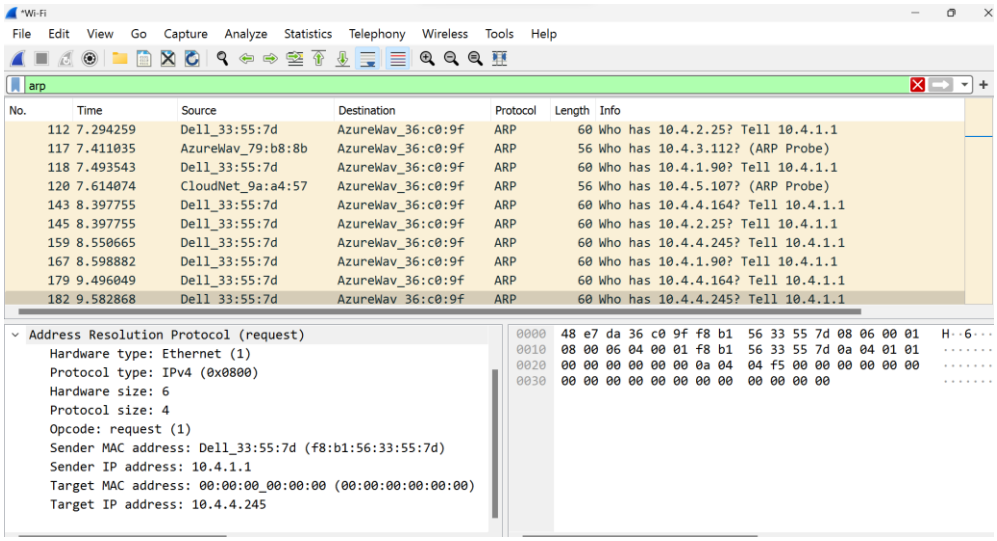
Answer:



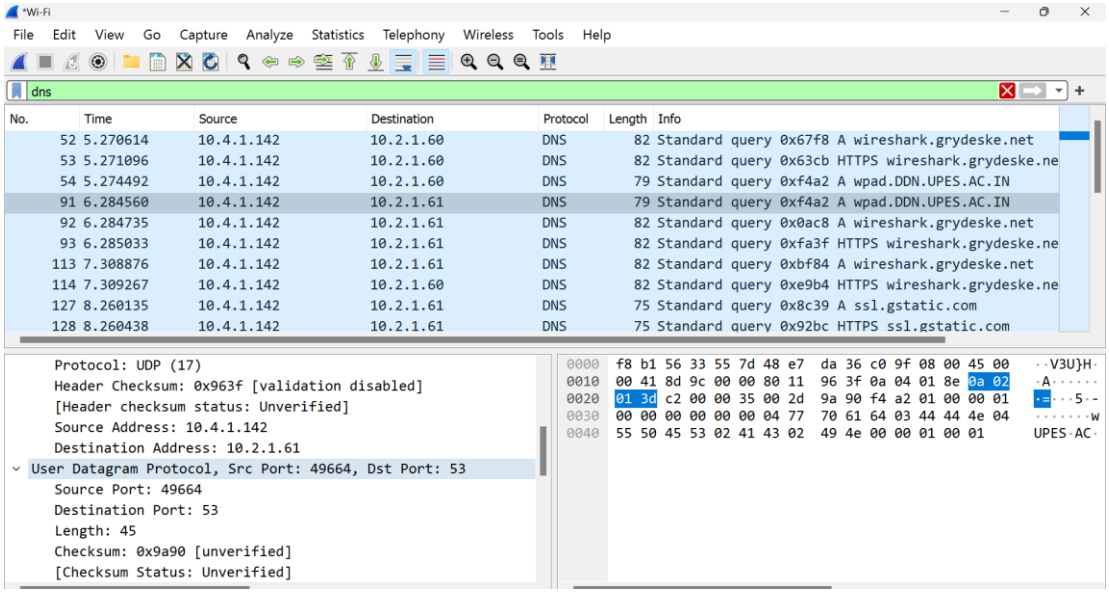


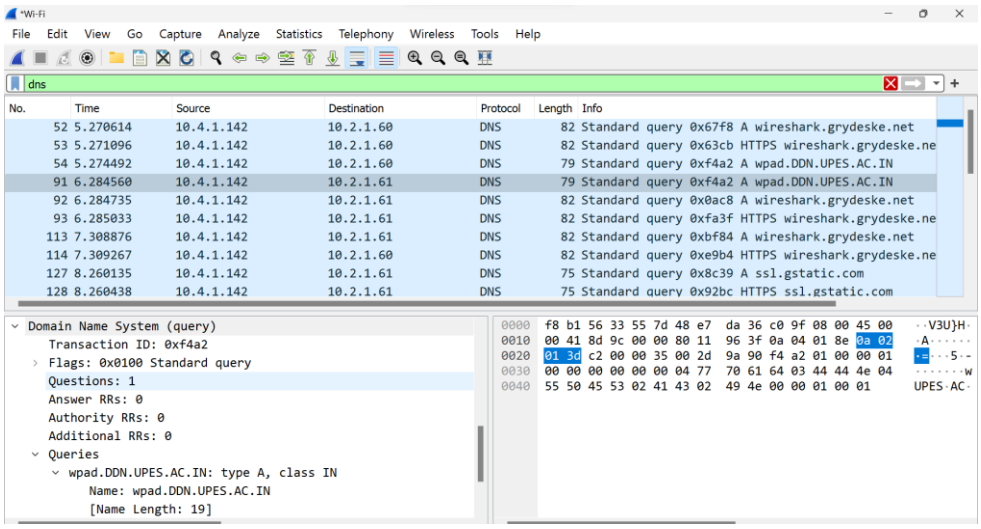
```
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
Accept: text/html,application/xhtml+xml,application/xml;q=0
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en;q=0.9\r\n
\r\n
[Full request URI: http://wireshark.grydeske.net/file3.html]
[HTTP request 1/2]
[Response in frame: 196]
[Next request in frame: 203]
```

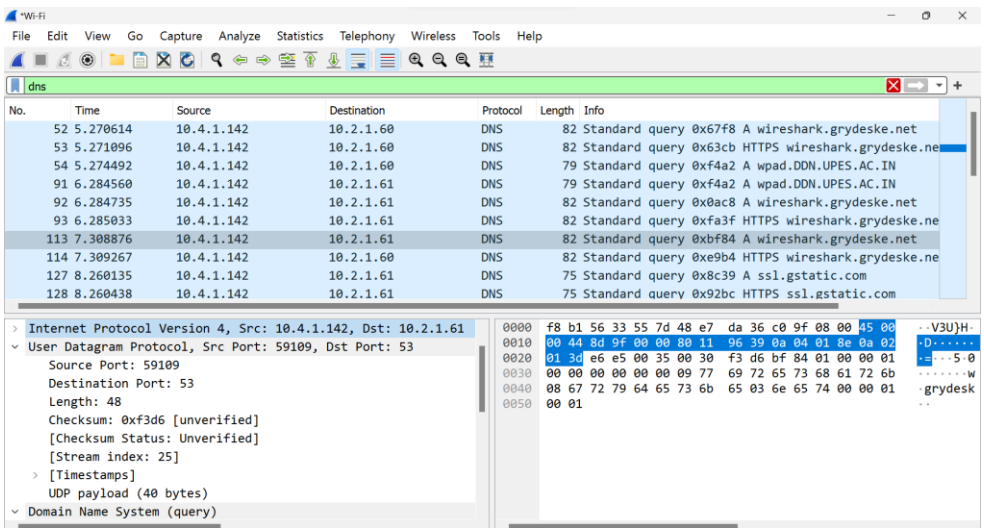


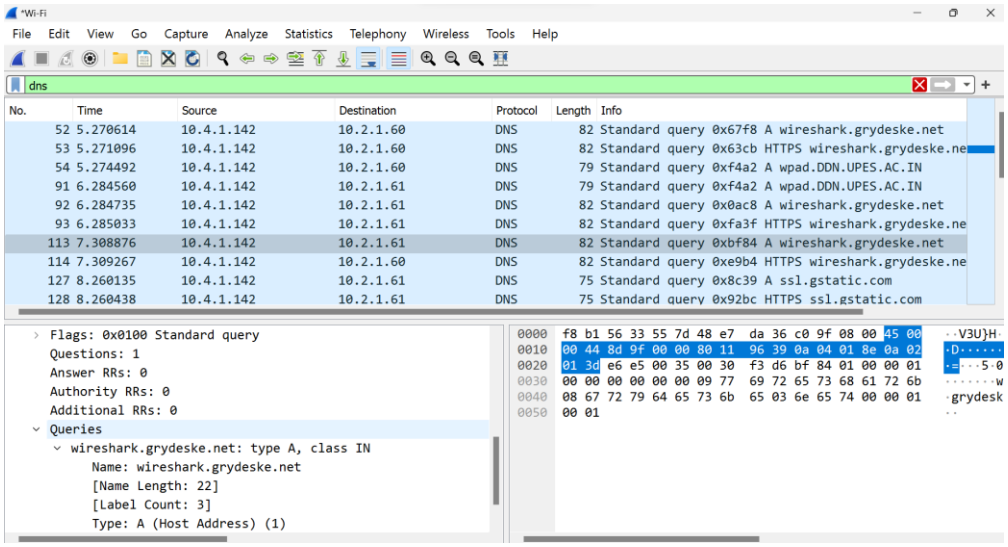


When filtering for DNS what is your local DNS & the domain you are trying to browse?
Answer:

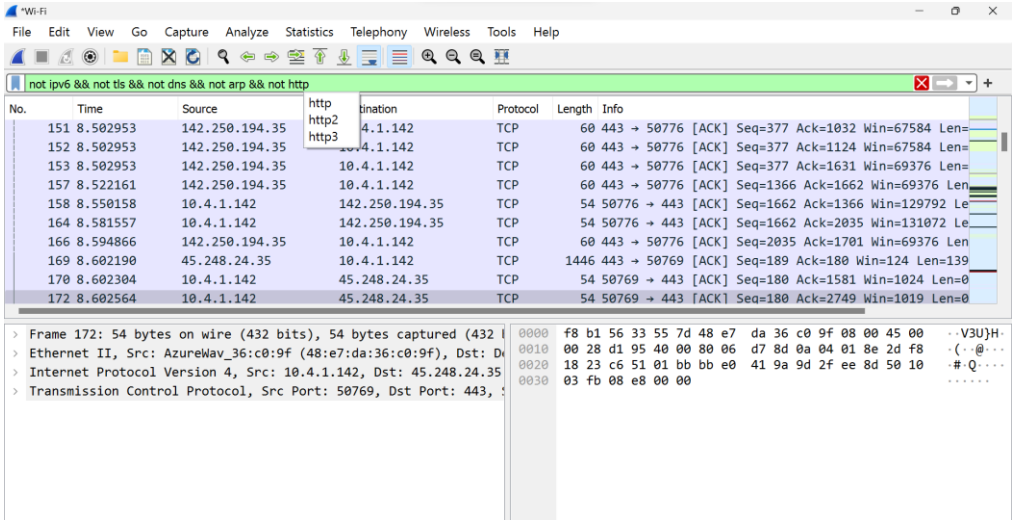




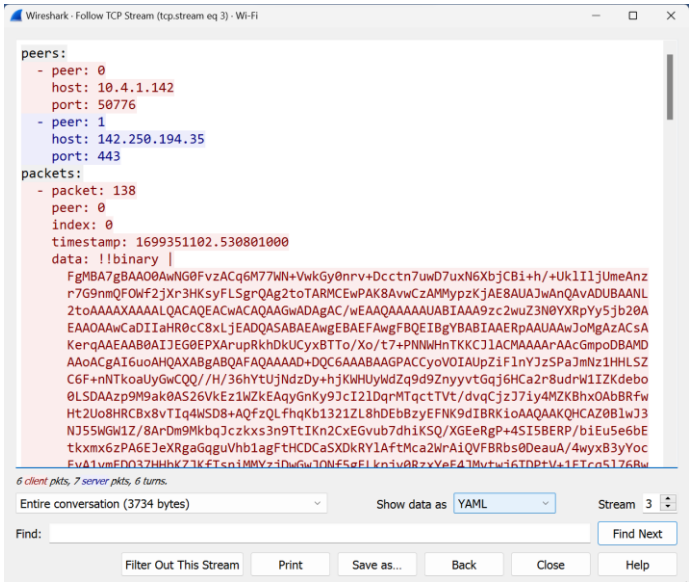




Filter only TCP packets, click and analyze TCP stream, what do you see?
Answer:

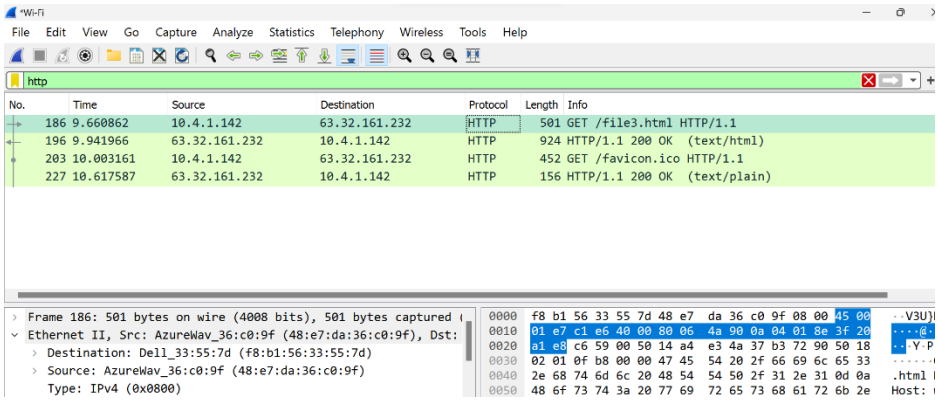


TCP stream



Select the Ethernet frame containing the HTTP GET message

Answer:



EXPERIMENT 10

__/__/____

IT NETWORK SEC.
LAB 10.

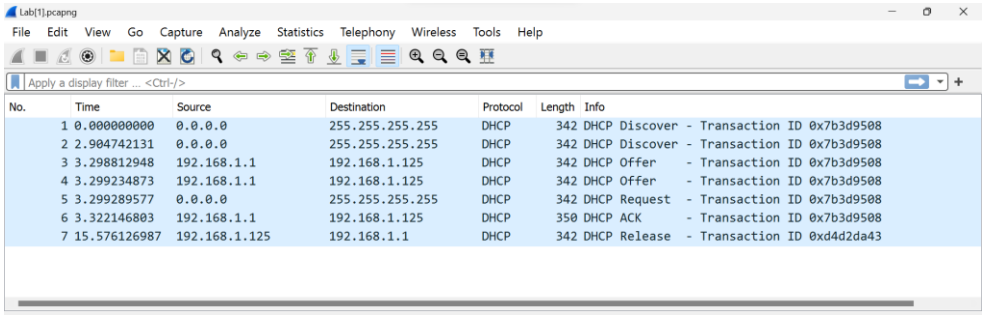
Khushi Wadhawan
500093673
B2

Q1.) DHCP or Dynamic Host Configuration Protocol is a fundamental network protocol that automates the assignment of IP addresses & other network configuration parameters to devices. When a device connects to a network, it sends DHCP request to a DHCP server. The server the selects an available IP address from a predefined pool & assigns it to the requesting device, along with details. Once assignment is complete, the device configures its network settings & can communicate on the network using the provided IP address.

Q2.) In DHCP, "DHCP Discovery" is the first step when a device seeks an IP address upon connecting to a network. The device sends a broadcast message request on IP address & network configuration. The DHCP server on the network responds with an offer initiating the process of an IP address assignment.

Q3.) A DHCP request is the third step in IP Address assignment. After receiving the offer from a DHCP server, the client server sends a request to accept the offered IP address & config.

```
Windows IP Configuration

No operation can be performed on Ethernet 2 while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

C:\Users\danveer>ipconfig/renew

Windows IP Configuration

No operation can be performed on Ethernet 2 while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x7b3d9508
2	2.904742131	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x7b3d9508
3	3.298812948	192.168.1.1	192.168.1.125	DHCP	342	DHCP Offer - Transaction ID 0x7b3d9508
4	3.299234873	192.168.1.1	192.168.1.125	DHCP	342	DHCP Offer - Transaction ID 0x7b3d9508
5	3.299289577	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x7b3d9508
6	3.322146803	192.168.1.1	192.168.1.125	DHCP	350	DHCP ACK - Transaction ID 0x7b3d9508
7	15.576126987	192.168.1.125	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xd4d2da43

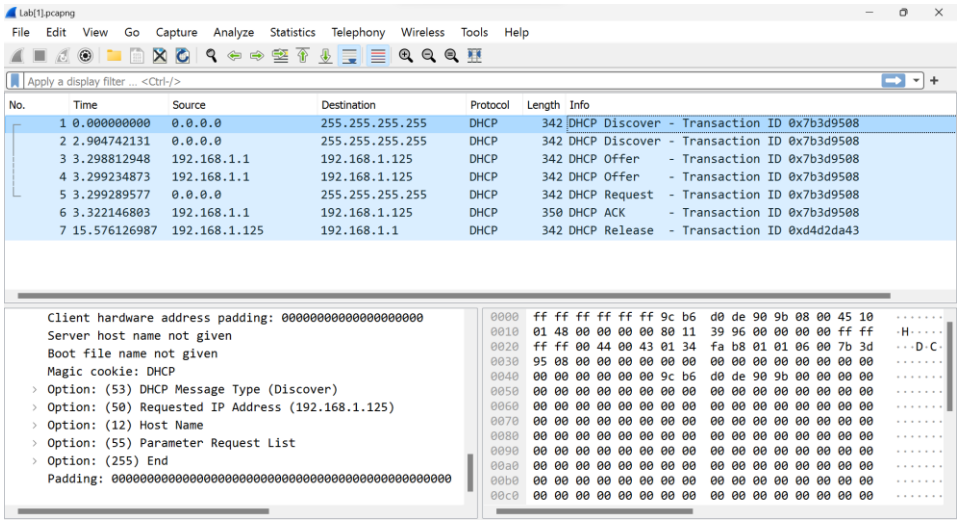
Are DHCP messages sent over UDP or TCP?

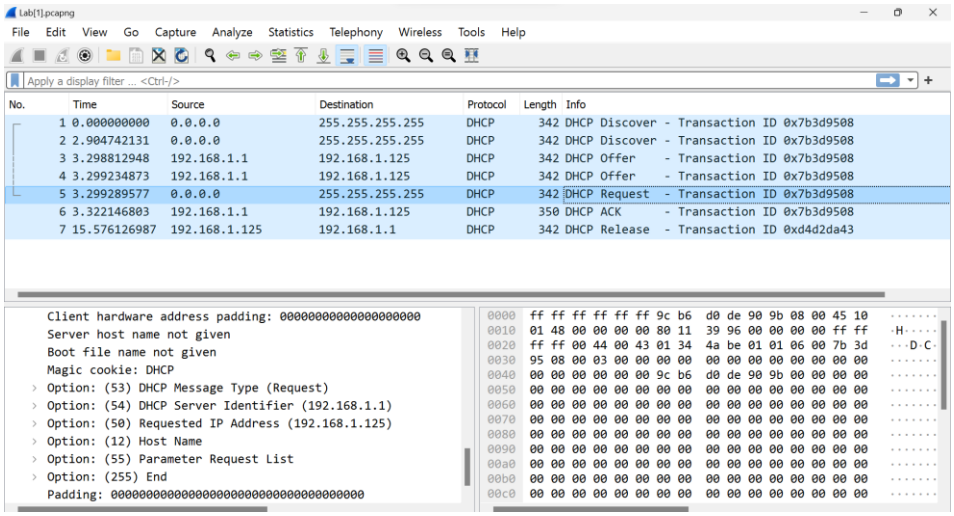
```
User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 308
    Checksum: 0x4abe [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
```

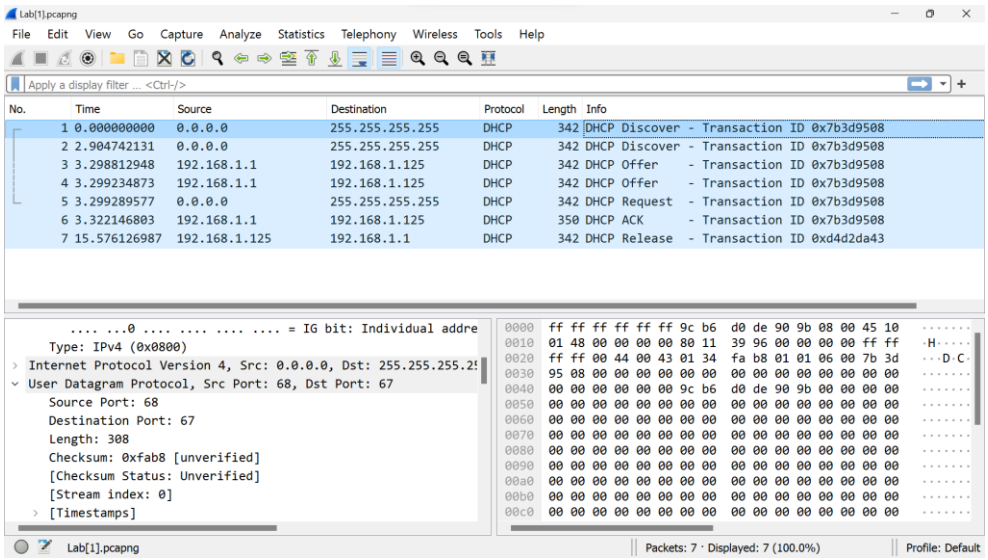
What is the link-layer (e.g., Ethernet) address of your host?
Answer: DHCP Message type and Request includes a server identifier fields

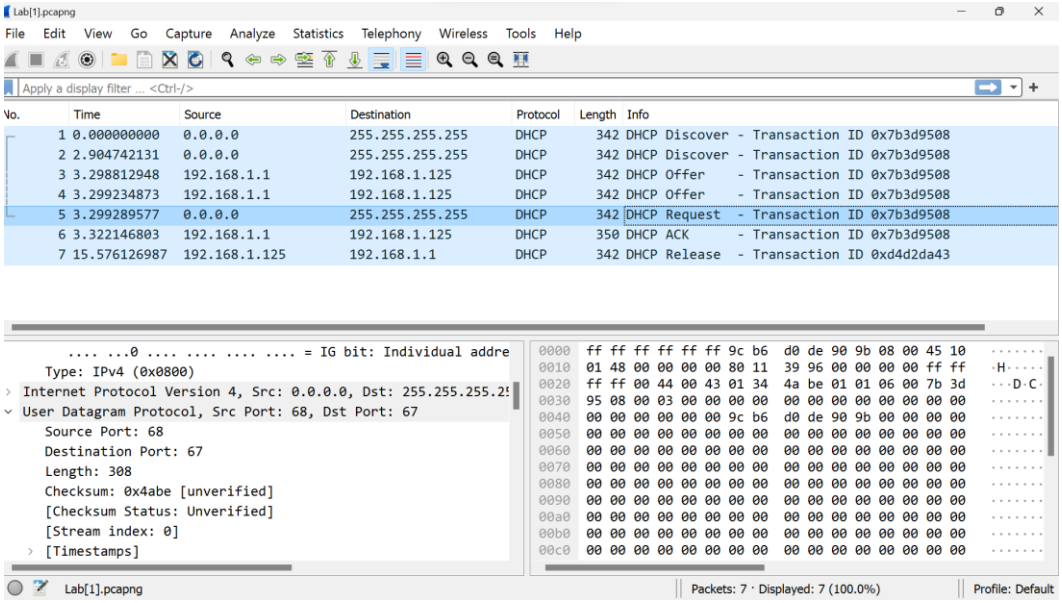
```
Ethernet II, Src: RivetNet_de:90:9b (9c:b6:d0:de:90:9b), Dst:
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administ
      .... ...1 .... .... .... .... = IG bit: Group address (m
  Source: RivetNet_de:90:9b (9c:b6:d0:de:90:9b)
      Address: RivetNet_de:90:9b (9c:b6:d0:de:90:9b)
      .... ..0. .... .... .... .... = LG bit: Globally unique
      .... ...0 .... .... .... .... = IG bit: Individual addre
    Type: IPv4 (0x0800)
```

What values in the DHCP discover message differentiate this message from the DHCP request message?


Lab[1].pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x7b3d9508
2 2.904742131 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x7b3d9508
3 3.298812948 192.168.1.1 192.168.1.125 DHCP 342 DHCP Offer - Transaction ID 0x7b3d9508
4 3.299234873 192.168.1.1 192.168.1.125 DHCP 342 DHCP Offer - Transaction ID 0x7b3d9508
5 3.299289577 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x7b3d9508
6 3.322146803 192.168.1.1 192.168.1.125 DHCP 350 DHCP ACK - Transaction ID 0x7b3d9508
7 15.576126987 192.168.1.125 192.168.1.1 DHCP 342 DHCP Release - Transaction ID 0xd4d2da43
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
Option: (50) Requested IP Address (192.168.1.125)
Option: (12) Host Name
Option: (55) Parameter Request List
Option: (255) End
Padding: 00000000000000000000000000000000000000000000000000
0000 ff ff ff ff ff ff 9c b6 d0 de 90 9b 08 00 45 10
0010 01 48 00 00 00 00 80 11 39 96 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 01 34 fa b8 01 01 06 00 7b 3d
0030 95 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 9c b6 d0 de 90 9b 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00


Lab[1].pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x7b3d9508
2 2.904742131 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x7b3d9508
3 3.298812948 192.168.1.1 192.168.1.125 DHCP 342 DHCP Offer - Transaction ID 0x7b3d9508
4 3.299234873 192.168.1.1 192.168.1.125 DHCP 342 DHCP Offer - Transaction ID 0x7b3d9508
5 3.299289577 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x7b3d9508
6 3.322146803 192.168.1.1 192.168.1.125 DHCP 350 DHCP ACK - Transaction ID 0x7b3d9508
7 15.576126987 192.168.1.125 192.168.1.1 DHCP 342 DHCP Release - Transaction ID 0xd4d2da43
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Request)
Option: (54) DHCP Server Identifier (192.168.1.1)
Option: (50) Requested IP Address (192.168.1.125)
Option: (12) Host Name
Option: (55) Parameter Request List
Option: (255) End
Padding: 00000000000000000000000000000000000000000000
0000 ff ff ff ff ff ff 9c b6 d0 de 90 9b 08 00 45 10
0010 01 48 00 00 00 00 80 11 39 96 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 01 34 4a be 01 01 06 00 7b 3d
0030 95 08 00 03 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 9c b6 d0 de 90 9b 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

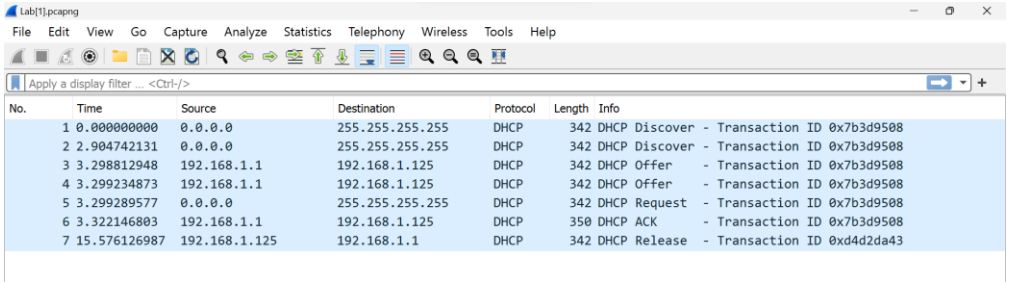

Lab[1].pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x7b3d9508
2 2.904742131 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x7b3d9508
3 3.298812948 192.168.1.1 192.168.1.125 DHCP 342 DHCP Offer - Transaction ID 0x7b3d9508
4 3.299234873 192.168.1.1 192.168.1.125 DHCP 342 DHCP Offer - Transaction ID 0x7b3d9508
5 3.299289577 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x7b3d9508
6 3.322146803 192.168.1.1 192.168.1.125 DHCP 350 DHCP ACK - Transaction ID 0x7b3d9508
7 15.576126987 192.168.1.125 192.168.1.1 DHCP 342 DHCP Release - Transaction ID 0xd4d2da43
....0 .... = IG bit: Individual addre
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.25
User Datagram Protocol, Src Port: 68, Dst Port: 67
Source Port: 68
Destination Port: 67
Length: 308
Checksum: 0xfab8 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
0000 ff ff ff ff ff ff 9c b6 d0 de 90 9b 08 00 45 10
0010 01 48 00 00 00 00 80 11 39 96 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 01 34 fa b8 01 01 06 00 7b 3d
0030 95 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 9c b6 d0 de 90 9b 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Lab[1].pcapng
Packets: 7 · Displayed: 7 (100.0%)
Profile: Default



A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.?
0.0.0.0/255.255.255.255 DHCP Discover
192.168.1.1/192.168.1.125 DHCP Offer
0.0.0.0/255.255.255.255 DHCP Request
192.168.1.1/192.168.1.125 DHCP ACK

What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address?
Answer: The DHCP server offer 192.168.1.1 as the ip address in the DHCP offer message

```
Option: (53) DHCP Message Type (Offer)
    Length: 1
    DHCP: Offer (2)
```



What is the IP address of the DHCP server?
Answer: 192.168.1.1

Explain the purpose of the lease time. How long is the lease time in your experiment?
Answer: The purpose of lease time is to tell the client how long they can use the specific IP address assigned by the server before they will have to be assigned a new one.The lease time in my experiment is 3600s seconds or 1 day

DHCP Server Identifier: 192.168.1.1

Option: (51) IP Address Lease Time

Length: 4

IP Address Lease Time: (3600s) 1 hour