Cyber Security Workshop

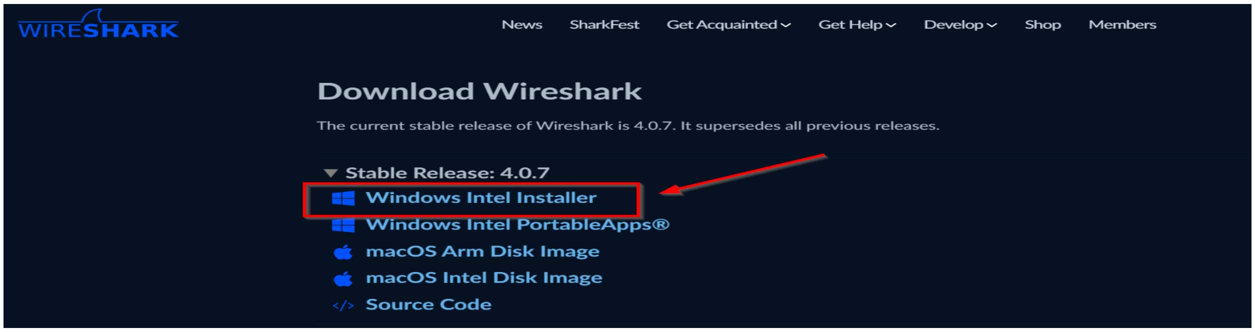
Introduction to Wireshark

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course)

Downloading Steps:

1. Your first step is to head to the **Wireshark download page** and locate the Windows installer.



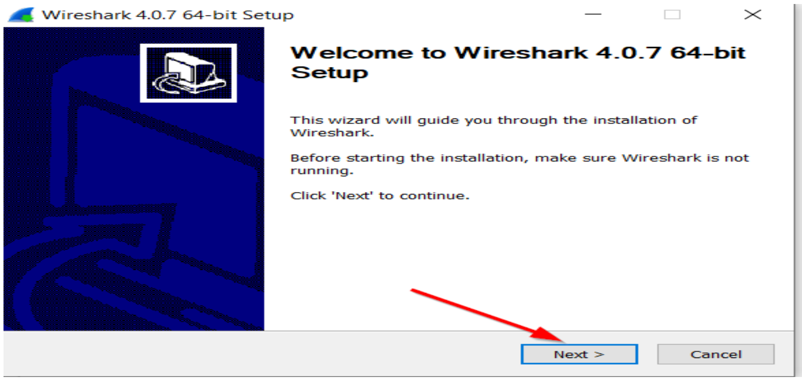
Download Wireshark

The current stable release of Wireshark is 4.0.7. It supersedes all previous releases.

Stable Release: 4.0.7
- Windows Intel Installer
- Windows Intel PortableApps®
- macOS Arm Disk Image
- macOS Intel Disk Image
- Source Code

Once your file is downloaded, you can open the file from your Download folder.

2. You will be presented with the Wireshark wizard to guide you through the installation. Click "Next."



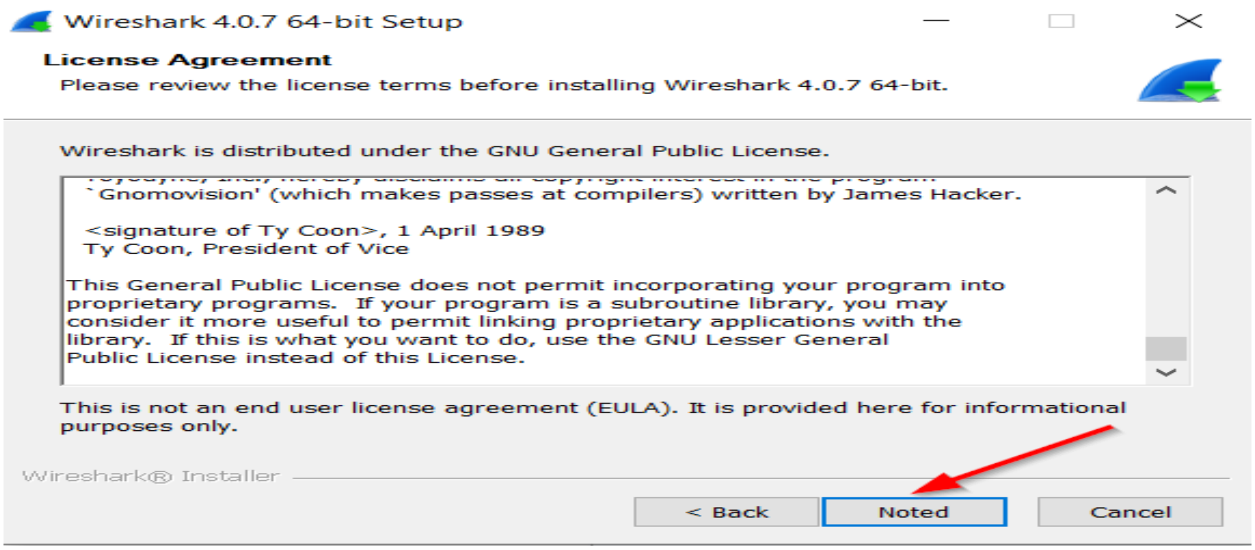
Welcome to Wireshark 4.0.7 64-bit Setup

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

3. Next, you can review, agree to the license agreement, and click "Noted" to continue.


Wireshark 4.0.7 64-bit Setup

License Agreement

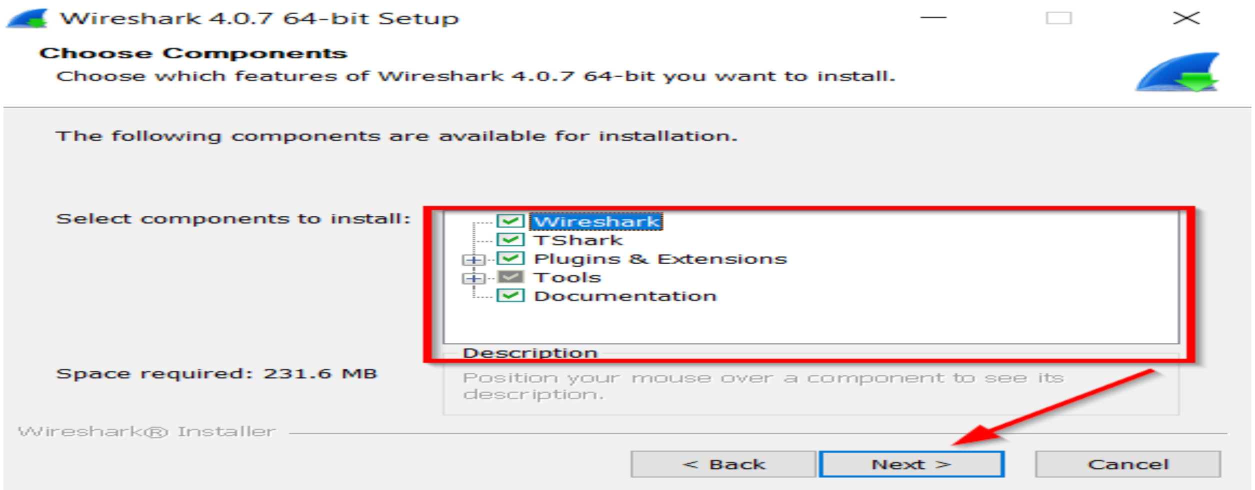
Please review the license terms before installing Wireshark 4.0.7 64-bit.

Wireshark is distributed under the GNU General Public License.

```
 `Gnomovision' (which makes passes at compilers) written by James Hacker.

 <signature of Ty Coon>, 1 April 1989
 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs.  If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library.  If this is what you want to do, use the GNU Lesser General
Public License instead of this License.
```

This is not an end user license agreement (EULA). It is provided here for informational purposes only.

4. The next screen will ask if you want to donate to the Wireshark Foundation to help support Wireshark and Sharkfest at **https://wiresharkfoundation.org/**. Click “Next” when finished.
5. Next, you will be asked what components you want to install. You can make your choice and then click “Next.”


Wireshark 4.0.7 64-bit Setup

Choose Components

Choose which features of Wireshark 4.0.7 64-bit you want to install.

The following components are available for installation.

Select components to install:

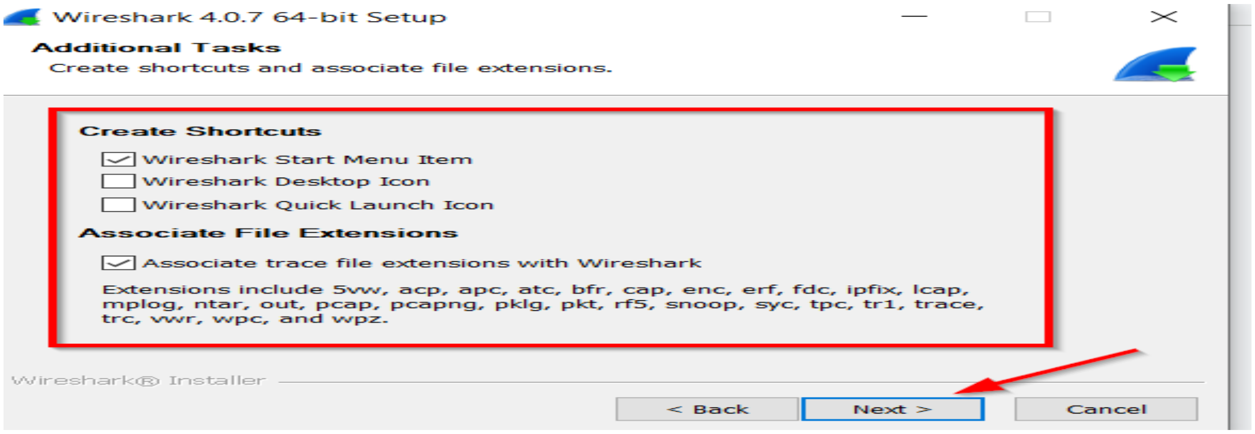
- ☑ Wireshark
- ☑ TShark
- ☑ Plugins & Extensions
- ☑ Tools
- ☑ Documentation

Space required: 231.6 MB

Description

Position your mouse over a component to see its description.

6. The following screen will ask if you want to create any shortcuts and if you want to associate trace file extensions with Wireshark (recommended).


Wireshark 4.0.7 64-bit Setup

Additional Tasks

Create shortcuts and associate file extensions.

Create Shortcuts

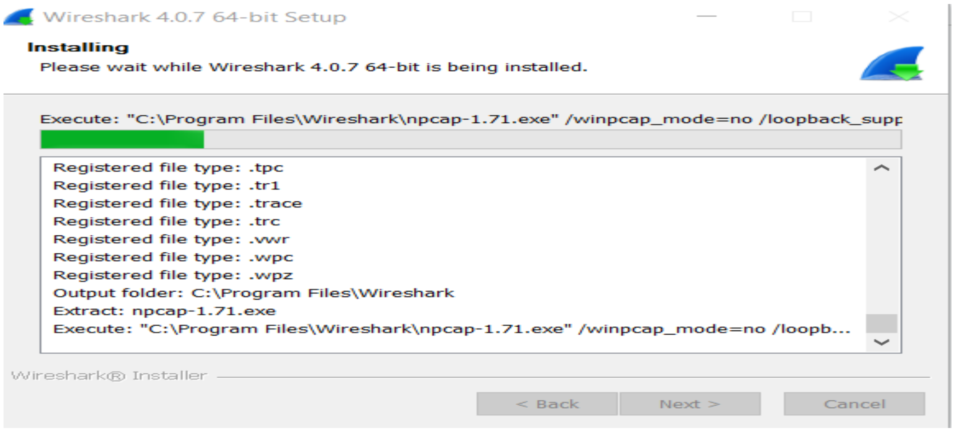
- ☑ Wireshark Start Menu Item
- ☐ Wireshark Desktop Icon
- ☐ Wireshark Quick Launch Icon

Associate File Extensions

- ☑ Associate trace file extensions with Wireshark

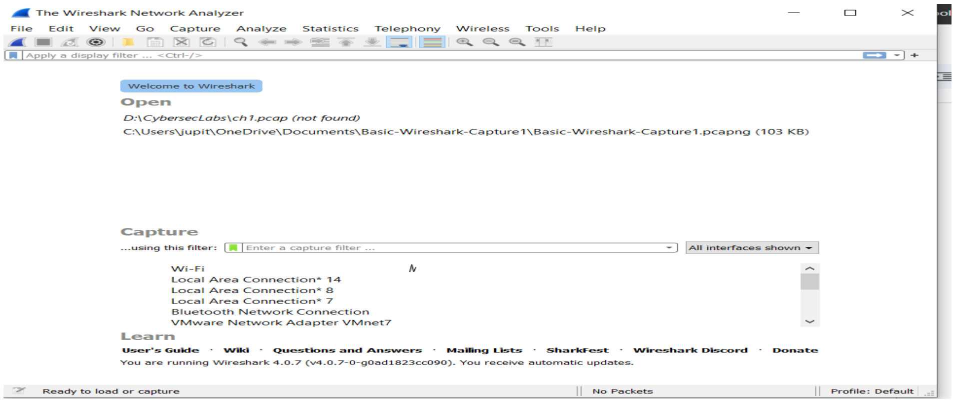
Extensions include 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, lcap, mplog, ntar, out, pcap, pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, and wpz.

7. Now you must install Ncap (an open-source library for packet capture and network analysis). It's a library allowing Wireshark to capture and analyze network traffic effectively. It enhances Wireshark's capabilities by providing optimized packet capture.
8. Wireshark will now begin the installation process.


Wireshark 4.0.7 64-bit Setup
Installing
Please wait while Wireshark 4.0.7 64-bit is being installed.
Wireshark® Installer
< Back
Next >
Cancel

```
Execute: "C:\Program Files\Wireshark\npcap-1.71.exe" /winpcap_mode=no /loopback_supp
```

```
Registered file type: .tpc
Registered file type: .tr1
Registered file type: .trace
Registered file type: .trc
Registered file type: .vwr
Registered file type: .wpc
Registered file type: .wpz
Output folder: C:\Program Files\Wireshark
Extract: npcap-1.71.exe
Execute: "C:\Program Files\Wireshark\npcap-1.71.exe" /winpcap_mode=no /loopb...
```


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Ready to load or capture
No Packets
Profile: Default

```
D:\CybersecLabs\ch1.pcap (not found)
C:\Users\jupit\OneDrive\Documents\Basic-Wireshark-Capture1\Basic-Wireshark-Capture1.pcapng (103 KB)
```

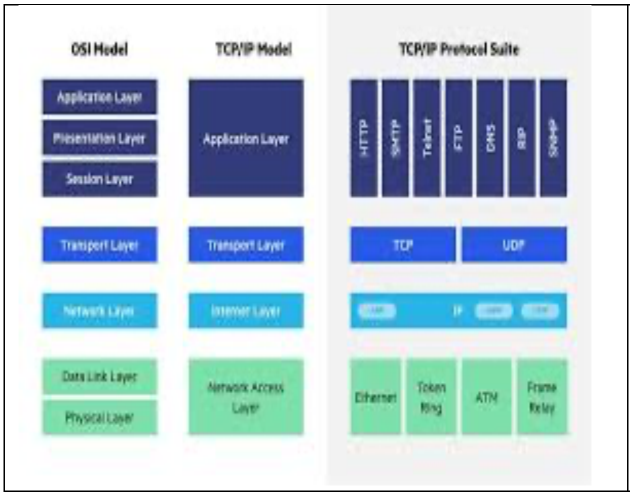
```
Wi-Fi
Local Area Connection* 14
Local Area Connection* 8
Local Area Connection* 7
Bluetooth Network Connection
VMware Network Adapter VMnet7
```

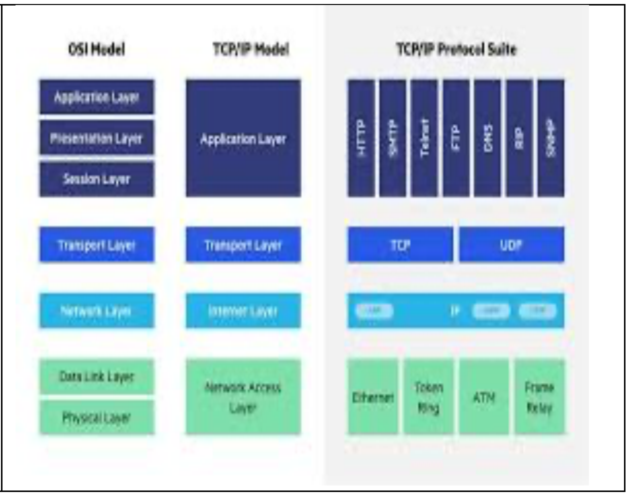
You are running Wireshark 4.0.7 (v4.0.7-0-g0ad1823cc090). You receive automatic updates.

Objective 1:
Basic Packet Inspection: Capture network traffic using Wire shark and analyze basic protocols like HTTP, DNS, and SMTP to understand how data is transmitted and received.
Tool Used: Wireshark

Protocols used in different OSI Layers:

SENDER/ BROWSER	RECEIVER/SERVER

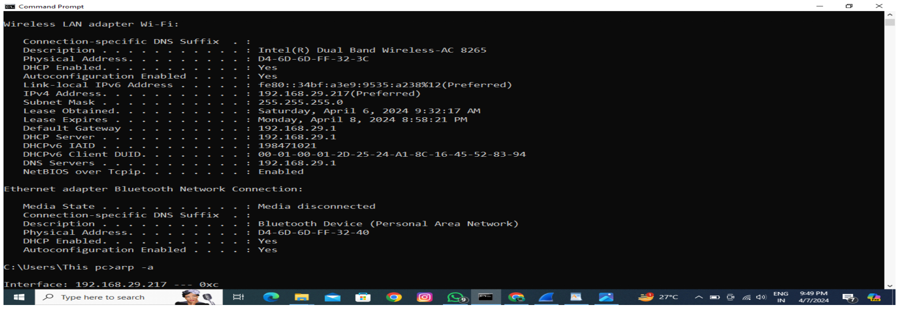




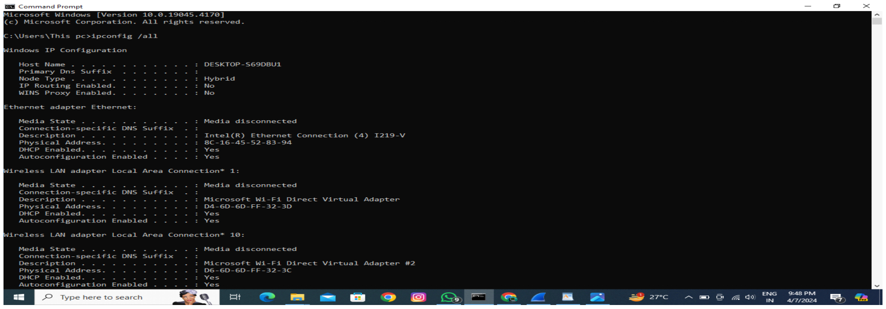
Commands used for making Reference Table:

- Ipconfig   /all (for getting information of local host)
- arp -a (for getting MAC address of Gateway)
- ping httpforever.com for capturing http packets

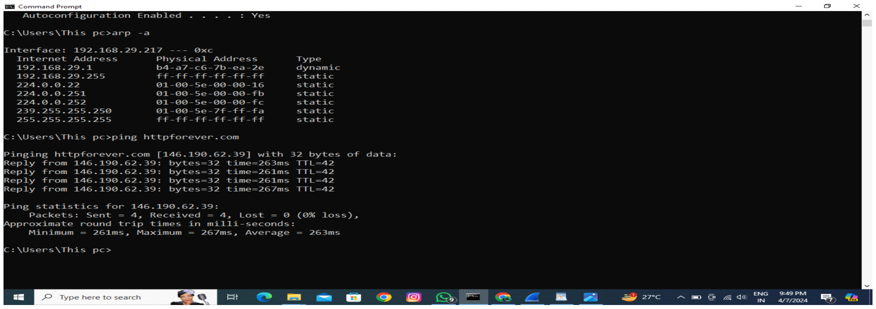
Parameter	Value
Your Machine IP Address	192.168.29.217
Your Machine MAC	D4-6D-6D-FF-32-3c
Default Gateway MAC	b4-a7-c6-7b-ea-2e
Website URL	httpforever.com
Website IP Address	146.190.62.39



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : D4-6D-6D-FF-32-3C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::34bf:a3e9:9535:a238%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.29.217(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, April 6, 2024 9:32:17 AM
   Lease Expires . . . . . . . . . . : Monday, April 8, 2024 8:58:21 PM
   Default Gateway . . . . . . . . . : 192.168.29.1
   DHCP Server . . . . . . . . . . . : 192.168.29.1
   DHCPv6 IAID . . . . . . . . . . . : 198471021
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-25-24-A1-8C-16-45-52-83-94
   DNS Servers . . . . . . . . . . . : 192.168.29.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : D4-6D-6D-FF-32-40
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Users\This pc>arp -a

Interface: 192.168.29.217 --- 0xc
```



```
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\This pc>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-S69DBU1
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (4) I219-V
   Physical Address. . . . . . . . . : 8C-16-45-52-83-94
   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
   Physical Address. . . . . . . . . : D4-6D-6D-FF-32-3D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : D6-6D-6D-FF-32-3C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```



```
   Autoconfiguration Enabled . . . . : Yes

C:\Users\This pc>arp -a

Interface: 192.168.29.217 --- 0xc
  Internet Address      Physical Address      Type
  192.168.29.1          b4-a7-c6-7b-ea-2e     dynamic
  192.168.29.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\This pc>ping httpforever.com

Pinging httpforever.com [146.190.62.39] with 32 bytes of data:
Reply from 146.190.62.39: bytes=32 time=263ms TTL=42
Reply from 146.190.62.39: bytes=32 time=261ms TTL=42
Reply from 146.190.62.39: bytes=32 time=261ms TTL=42
Reply from 146.190.62.39: bytes=32 time=267ms TTL=42

Ping statistics for 146.190.62.39:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 261ms, Maximum = 267ms, Average = 263ms

C:\Users\This pc>
```

1. Steps to Analyse HTTP protocol

Step 1: Open ether/wifi adapter in wireshark

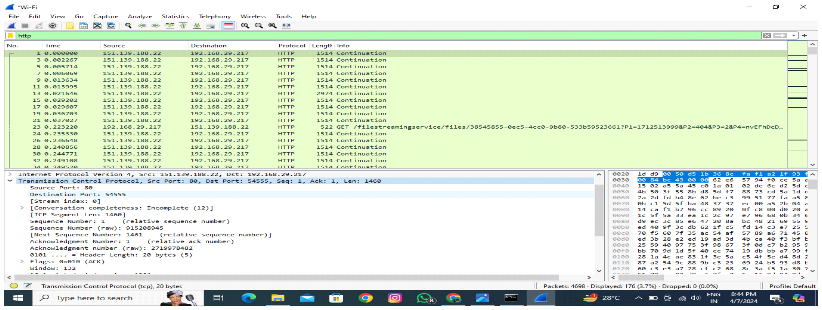
Step2: Apply http filter as given below:

Step 3: Start Capturing

Step 4: open httpforever.com in the browser

Step 5: Analyse the TCP data (source port, destination port), source Mac, Destination Mac, Source Ip etc. and compare it with the reference table

Step 6: check 3way handshaking befor establishing http connection by using the filter tcp.port==56368*



http

```
No.   Time        Source            Destination       Protocol Length Info
    1 0.000000    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
    3 0.002267    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
    5 0.005714    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
    7 0.006069    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
    9 0.013634    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
   11 0.013995    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
   13 0.021646    151.139.188.22    192.168.29.217    HTTP     2974 Continuation
   15 0.029202    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
   17 0.029607    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
   19 0.036703    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
   21 0.037027    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
   23 0.223220    192.168.29.217    151.139.188.22    HTTP      522 GET /filestreamingservice/files/38545855-0ec5-4cc0-9b80-533b59523661?P1=1712513999&P2=404&P3=2&P4=nvEFhDcD…
   24 0.235330    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
   26 0.236648    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
   28 0.240856    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
   30 0.244771    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
   32 0.249108    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
   34 0.249520    151.139.188.22    192.168.29.217    HTTP     1514 Continuation
```

```
> Internet Protocol Version 4, Src: 151.139.188.22, Dst: 192.168.29.217
v Transmission Control Protocol, Src Port: 80, Dst Port: 54555, Seq: 1, Ack: 1, Len: 1460
    Source Port: 80
    Destination Port: 54555
    [Stream index: 0]
  > [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 1460]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 915208945
    [Next Sequence Number: 1461    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2719978482
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 132
```

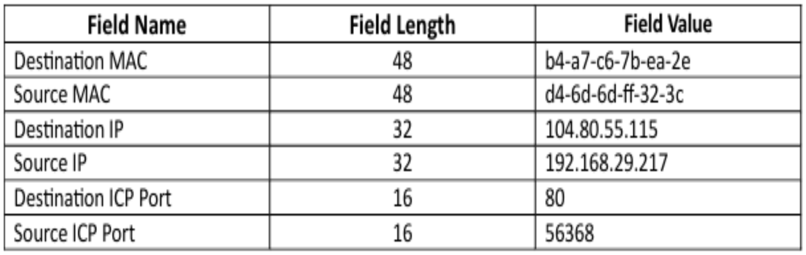
```
0020  1d d9 00 50 d5 1b 36 8c  fa f1 a2 1f 93
0030  00 84 bc 43 00 00 62 e6  57 94 f0 ce 5a
0040  15 02 a5 5a 45 c0 1a 01  02 de 6c d2 5d
0050  4b 50 3f 55 8b d8 5d f7  88 73 cd 5a 1d
0060  2a 2d fd b4 8e 62 be c3  99 51 77 fa a5
0070  0b c1 5d 5f ba 48 37 37  ec 00 a5 2b 04
0080  14 ca f1 b7 96 cc 89 20  0f c8 00 d0 20
0090  1c 5f 5a 33 ea 1c 2c 97  e7 96 68 0b 34
00a0  d9 ec 3c 85 e6 47 20 8a  bc 48 21 69 55
00b0  ed 40 9f 3c db 62 1f c5  fd 14 c3 e7 25
00c0  70 f5 60 7f 35 ac 54 af  57 89 a6 71 45
00d0  ed 3b 28 e2 ed 19 ad 3d  4b ca 40 f3 bf
00e0  25 59 40 97 75 3f 98 67  3f 0d c7 b2 95
00f0  bb 70 9d 1d 5f 40 cc 74  19 db bb a7 99
0100  28 1a 4c ae 83 1f 3e 5a  c5 4f 5e d4 8d
0110  87 a2 54 9c 88 9b c3 23  69 24 b5 93 d8
0120  60 c3 e3 a7 28 cf c2 68  8c 3a f5 1a 30
```

Transmission Control Protocol (tcp), 20 bytes

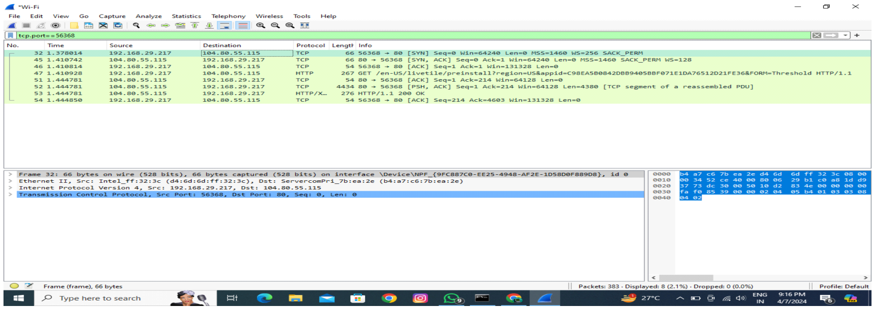
Packets: 4698 · Displayed: 176 (3.7%) · Dropped: 0 (0.0%)

Profile: Default

Type here to search
28°C
ENG IN
8:44 PM
4/7/2024

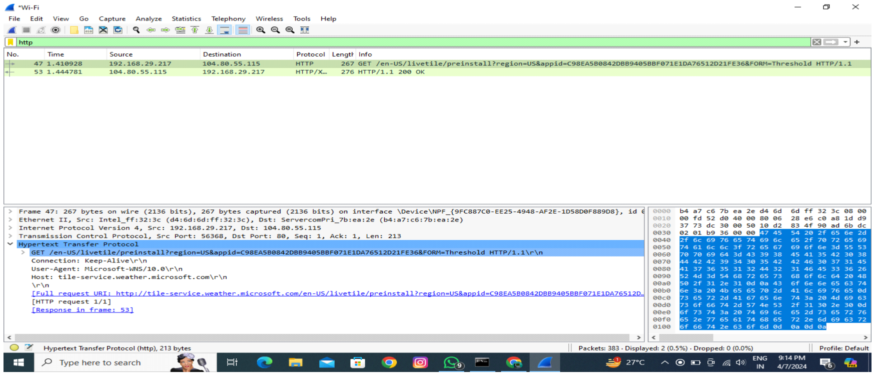


Field Name	Field Length	Field Value
Destination MAC	48	b4-a7-c6-7b-ea-2e
Source MAC	48	d4-6d-6d-ff-32-3c
Destination IP	32	104.80.55.115
Source IP	32	192.168.29.217
Destination ICP Port	16	80
Source ICP Port	16	56368


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

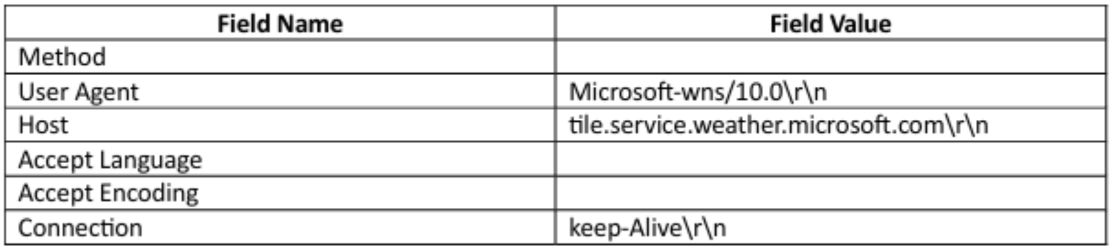
```
tcp.port==56368
No.  Time      Source          Destination     Protocol Length Info
  32 1.378014  192.168.29.217  104.80.55.115   TCP        66 56368 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  45 1.410742  104.80.55.115   192.168.29.217  TCP        66 80 → 56368 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
  46 1.410814  192.168.29.217  104.80.55.115   TCP        54 56368 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  47 1.410928  192.168.29.217  104.80.55.115   HTTP      267 GET /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
  51 1.444781  104.80.55.115   192.168.29.217  TCP        54 80 → 56368 [ACK] Seq=1 Ack=214 Win=64128 Len=0
  52 1.444781  104.80.55.115   192.168.29.217  TCP      4434 80 → 56368 [PSH, ACK] Seq=1 Ack=214 Win=64128 Len=4380 [TCP segment of a reassembled PDU]
  53 1.444781  104.80.55.115   192.168.29.217  HTTP/X…   276 HTTP/1.1 200 OK
  54 1.444850  192.168.29.217  104.80.55.115   TCP        54 56368 → 80 [ACK] Seq=214 Ack=4603 Win=131328 Len=0

> Frame 32: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{9FC887C0-EE25-4948-AF2E-1D58D0F889D8}, id 0
> Ethernet II, Src: Intel_ff:32:3c (d4:6d:6d:ff:32:3c), Dst: ServercomPri_7b:ea:2e (b4:a7:c6:7b:ea:2e)
> Internet Protocol Version 4, Src: 192.168.29.217, Dst: 104.80.55.115
> Transmission Control Protocol, Src Port: 56368, Dst Port: 80, Seq: 0, Len: 0

0000  b4 a7 c6 7b ea 2e d4 6d  6d ff 32 3c 08 00
0010  00 34 52 ce 40 00 80 06  29 b1 c0 a8 1d d9
0020  37 73 dc 30 00 50 10 d2  83 4e 00 00 00 00
0030  fa f0 85 39 00 00 02 04  05 b4 01 03 03 08
0040  04 02

Frame (frame), 66 bytes    Packets: 383 · Displayed: 8 (2.1%) · Dropped: 0 (0.0%)    Profile: Default
```

Step 7: Now finally record the data for http header in the table given below:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

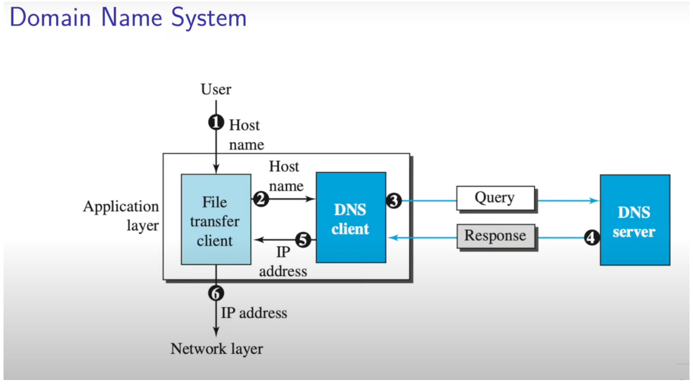
```
http
No.  Time      Source          Destination     Protocol Length Info
  47 1.410928  192.168.29.217  104.80.55.115   HTTP      267 GET /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
  53 1.444781  104.80.55.115   192.168.29.217  HTTP/X…   276 HTTP/1.1 200 OK

> Frame 47: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface \Device\NPF_{9FC887C0-EE25-4948-AF2E-1D58D0F889D8}, id 0
> Ethernet II, Src: Intel_ff:32:3c (d4:6d:6d:ff:32:3c), Dst: ServercomPri_7b:ea:2e (b4:a7:c6:7b:ea:2e)
> Internet Protocol Version 4, Src: 192.168.29.217, Dst: 104.80.55.115
> Transmission Control Protocol, Src Port: 56368, Dst Port: 80, Seq: 1, Ack: 1, Len: 213
v Hypertext Transfer Protocol
  > GET /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1\r\n
    Connection: Keep-Alive\r\n
    User-Agent: Microsoft-WNS/10.0\r\n
    Host: tile-service.weather.microsoft.com\r\n
    \r\n
    [Full request URI: http://tile-service.weather.microsoft.com/en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D…
    [HTTP request 1/1]
    [Response in frame: 53]

0000  b4 a7 c6 7b ea 2e d4 6d  6d ff 32 3c 08 00
0010  00 fd 52 d0 40 00 80 06  28 e6 c0 a8 1d d9
0020  37 73 dc 30 00 50 10 d2  83 4f 90 ad 6b dc
0030  02 01 b9 36 00 00 47 45  54 20 2f 65 6e 2d
0040  2f 6c 69 76 65 74 69 6c  65 2f 70 72 65 69
0050  74 61 6c 6c 3f 72 65 67  69 6f 6e 3d 55 53
0060  70 70 69 64 3d 43 39 38  45 41 35 42 30 38
0070  44 42 42 39 34 30 35 42  42 46 30 37 31 45
0080  41 37 36 35 31 32 44 32  31 46 45 33 36 26
0090  52 4d 3d 54 68 72 65 73  68 6f 6c 64 20 48
00a0  50 2f 31 2e 31 0d 0a 43  6f 6e 6e 65 63 74
00b0  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d
00c0  73 65 72 2d 41 67 65 6e  74 3a 20 4d 69 63
00d0  73 6f 66 74 2d 57 4e 53  2f 31 30 2e 30 0d
00e0  6f 73 74 3a 20 74 69 6c  65 2d 73 65 72 76
00f0  65 2e 77 65 61 74 68 65  72 2e 6d 69 63 72
0100  6f 66 74 2e 63 6f 6d 0d  0a 0d 0a

Hypertext Transfer Protocol (http), 213 bytes    Packets: 383 · Displayed: 2 (0.5%) · Dropped: 0 (0.0%)    Profile: Default
```

2. Steps to analyse DNS protocol



Field Name	Field Value
Method	
User Agent	Microsoft-wns/10.0\r\n
Host	tile.service.weather.microsoft.com\r\n
Accept Language	
Accept Encoding	
Connection	keep-Alive\r\n

DNS:

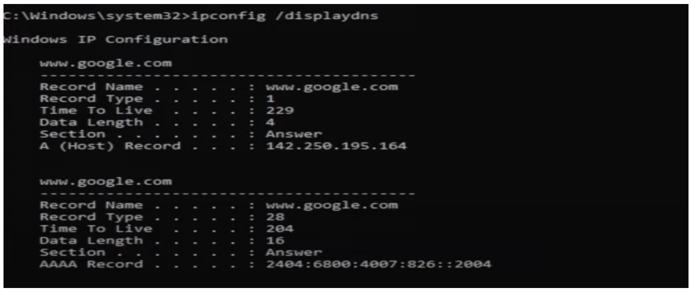


Domain Name System

Command for cmd:

ipconfig /displaydns

ipconfig /flushdns



```
C:\Windows\system32>ipconfig /displaydns

Windows IP Configuration

    www.google.com
    ----------------------------------------
    Record Name . . . . . : www.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 229
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 142.250.195.164


    www.google.com
    ----------------------------------------
    Record Name . . . . . : www.google.com
    Record Type . . . . . : 28
    Time To Live  . . . . : 204
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    AAAA Record . . . . . : 2404:6800:4007:826::2004
```

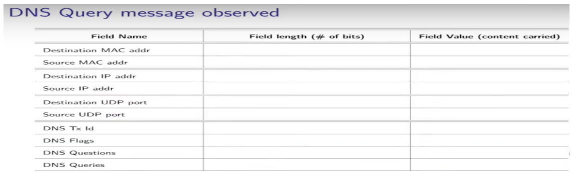
DNS observation

Step 1: Start capturing via Wireshark

Step 2: ping nptel.ac.in (command prompt)

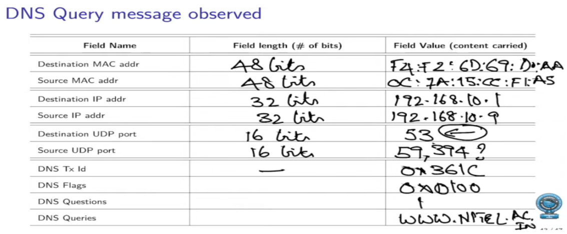
Step 3: Apply dns protocol filter in wireshark

Step 4: Observe the data in the given table:



DNS Query message observed

Field Name	Field length (# of bits)	Field Value (content carried)
Destination MAC addr		
Source MAC addr		
Destination IP addr		
Source IP addr		
Destination UDP port		
Source UDP port		
DNS Tx Id		
DNS Flags		
DNS Questions		
DNS Queries		



DNS Query message observed

Field Name	Field length (# of bits)	Field Value (content carried)
Destination MAC addr	48 bits	F4:F2:6D:69:D0:AA
Source MAC addr	48 bits	0C:7A:15:CC:F1:A5
Destination IP addr	32 bits	192.168.10.1
Source IP addr	32 bits	192.168.10.9
Destination UDP port	16 bits	53 ←
Source UDP port	16 bits	59,394 ?
DNS Tx Id	—	0x361C
DNS Flags		0x0100
DNS Questions		1
DNS Queries		WWW.NPTEL.AC.IN

3. Step to analyse SMTP protocol

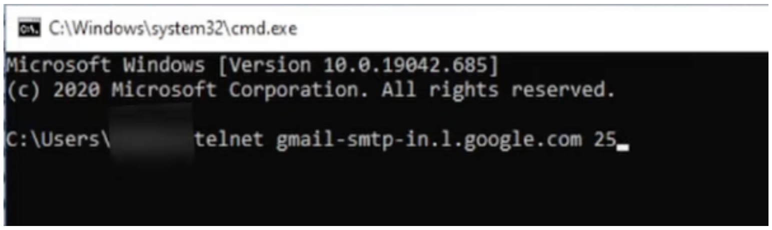
Step 1: Start capturing via Wireshark

Step 2: Enable the telnet feature by usin windows feature service

Step 3: telnet gmail-smtp-in.l.google.com 25 (command prompt)

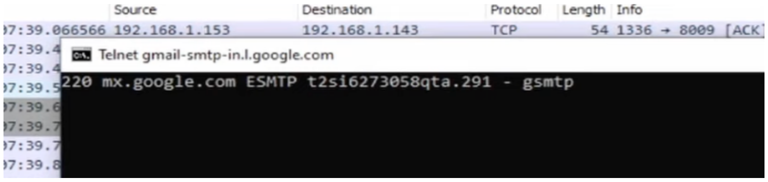
Helo sahil

quit



C:\Windows\system32\cmd.exe

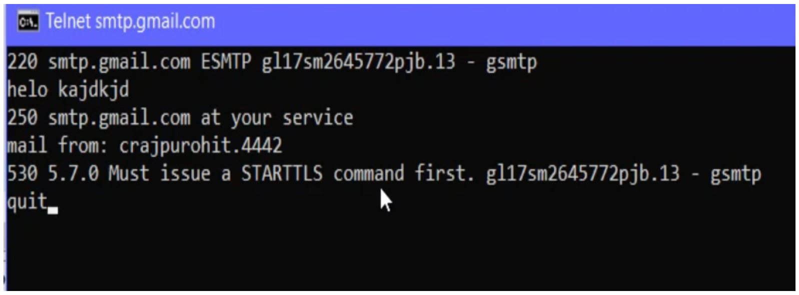
```
Microsoft Windows [Version 10.0.19042.685]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\[redacted]telnet gmail-smtp-in.l.google.com 25
```



```
                Source            Destination       Protocol  Length  Info
)7:39.066566  192.168.1.153     192.168.1.143       TCP          54  1336 → 8009 [ACK]
```

```
220 mx.google.com ESMTP t2si6273058qta.291 - gsmtp
```

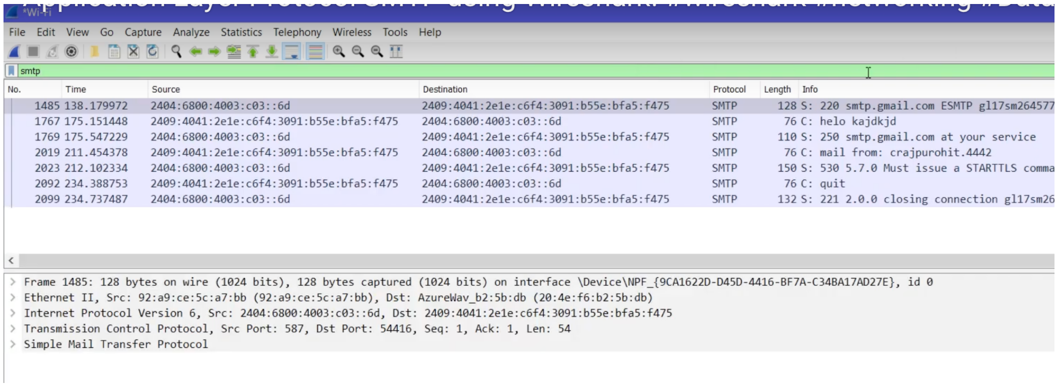
Commands to use:



```
220 smtp.gmail.com ESMTP gl17sm2645772pjb.13 - gsmtp
helo kajdkjd
250 smtp.gmail.com at your service
mail from: crajpurohit.4442
530 5.7.0 Must issue a STARTTLS command first. gl17sm2645772pjb.13 - gsmtp
quit
```

Step 3: Apply smtp protocol filter in wireshark

Step 4: Observe the data in SMTP:



```
No.     Time        Source                                 Destination                            Protocol  Length  Info
   1485 138.179972  2404:6800:4003:c03::6d                 2409:4041:2e1e:c6f4:3091:b55e:bfa5:f475  SMTP    128 S: 220 smtp.gmail.com ESMTP gl17sm264577
   1767 175.151448  2409:4041:2e1e:c6f4:3091:b55e:bfa5:f475  2404:6800:4003:c03::6d                 SMTP     76 C: helo kajdkjd
   1769 175.547229  2404:6800:4003:c03::6d                 2409:4041:2e1e:c6f4:3091:b55e:bfa5:f475  SMTP    110 S: 250 smtp.gmail.com at your service
   2019 211.454378  2409:4041:2e1e:c6f4:3091:b55e:bfa5:f475  2404:6800:4003:c03::6d                 SMTP     76 C: mail from: crajpurohit.4442
   2023 212.102334  2404:6800:4003:c03::6d                 2409:4041:2e1e:c6f4:3091:b55e:bfa5:f475  SMTP    150 S: 530 5.7.0 Must issue a STARTTLS comma
   2092 234.388753  2409:4041:2e1e:c6f4:3091:b55e:bfa5:f475  2404:6800:4003:c03::6d                 SMTP     76 C: quit
   2099 234.737487  2404:6800:4003:c03::6d                 2409:4041:2e1e:c6f4:3091:b55e:bfa5:f475  SMTP    132 S: 221 2.0.0 closing connection gl17sm26
```

```
> Frame 1485: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface \Device\NPF_{9CA1622D-D45D-4416-BF7A-C34BA17AD27E}, id 0
> Ethernet II, Src: 92:a9:ce:5c:a7:bb (92:a9:ce:5c:a7:bb), Dst: AzureWav_b2:5b:db (20:4e:f6:b2:5b:db)
> Internet Protocol Version 6, Src: 2404:6800:4003:c03::6d, Dst: 2409:4041:2e1e:c6f4:3091:b55e:bfa5:f475
> Transmission Control Protocol, Src Port: 587, Dst Port: 54416, Seq: 1, Ack: 1, Len: 54
> Simple Mail Transfer Protocol
```