CHANDIGARH UNIVERSITY

UNIVERSITY INSTITUTE OF ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Submitted By: Sandeep Kumar	**Submitted To: Renuka Ratten Maa'm**
Subject Name	WEB AND MOBILE SECURITY LAB
Subject Code	20CSP-338
Branch	CSE
Semester	5th

LAB INDEX

NAME: Lipakshi
UID: 20BCS5082
SECTION: 20BCS WM_607-B

SUBJECT NAME: Web and Mobile Security Lab
SUBJECT CODE: 20CSP-338

EXPERIMENT NO. 1

- **Aim:**

  Identity Http packet on Wireshark.

- **Objective:**

  To analyze Http traffic

- **Software/Hardware Requirements:**

  Windows 7 & above version.

- **Tools to be used:**

  1. Wireshark Packet Sniffer and Packet Capture Library
  2. Microsoft Word.
  3. Win Zip as necessary

- **Introduction:**

  Wireshark is a software tool used to monitor the network traffic through a network interface.It is the most widely used network monitoring tool today. Wireshark is loved equally by system administrators, network engineers, network enthusiasts, network security professionals and black hat hackers. The extent of its popularity is such, that experience with Wireshark is considered as a valuable/essential trait in a computer network in related professional.

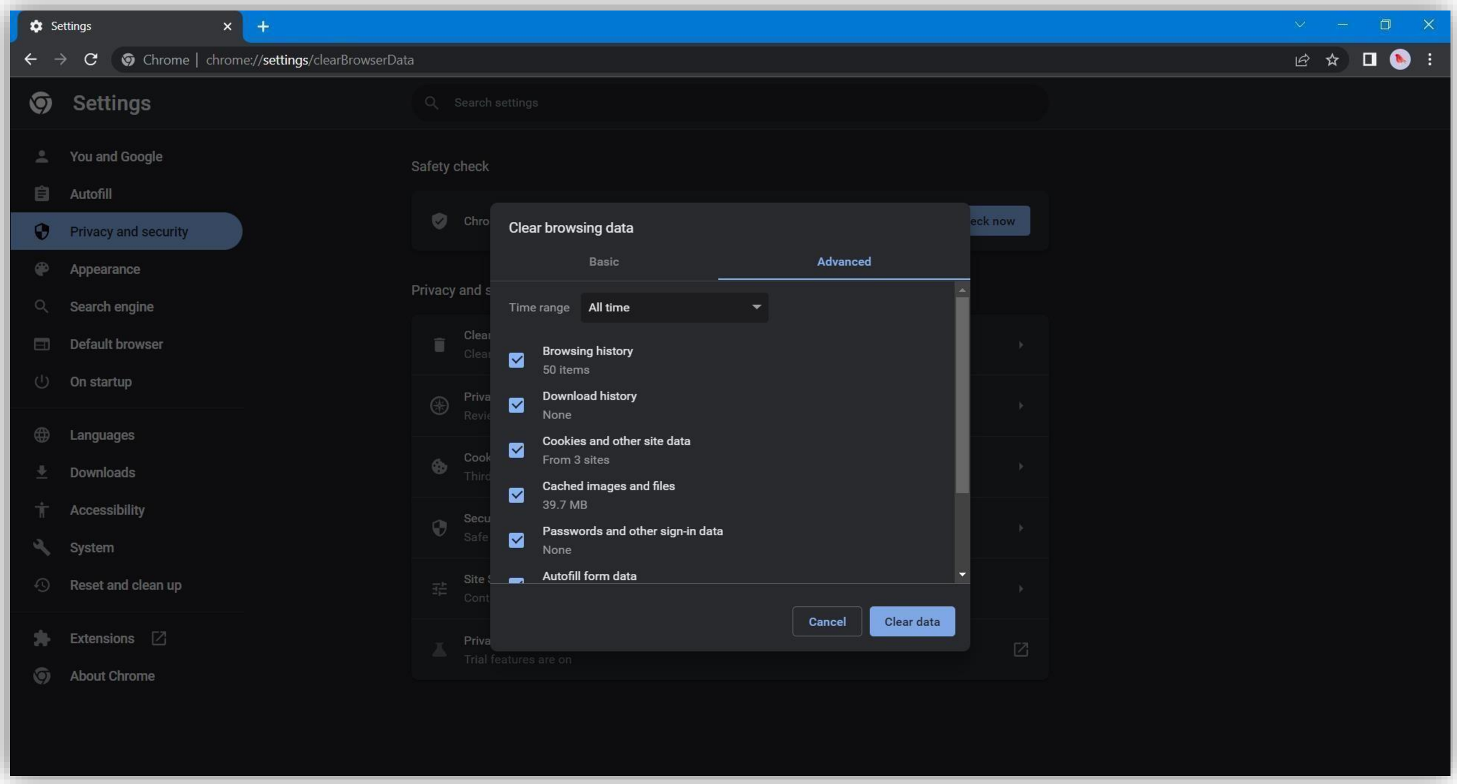
  There are many reasons why Wireshark is so popular:
  1. It has a great GUI as well as a conventional CLI(T Shark).
  2. It offers network monitoring on almost all types of network standards (ethernet, wlan, Bluetooth etc)
  3. It is open-source with a large community of backers and developers.
  4. All the necessary components for monitoring, analyzing and documenting the network traffic are present. It is free to use.

- **Steps/Method/Coding:**

  1. Install Wireshark.
  2. Open your Internet browser.
  3. Clear your browser cache.
  4. Open Wireshark
  5. Click on "Capture > Interfaces". A pop-up window will display.
  6. You'll want to capture traffic that goes through your ethernet driver. Click on the Start button to capture traffic via this interface.
  7. Visit the URL that you wanted to capture the traffic from.

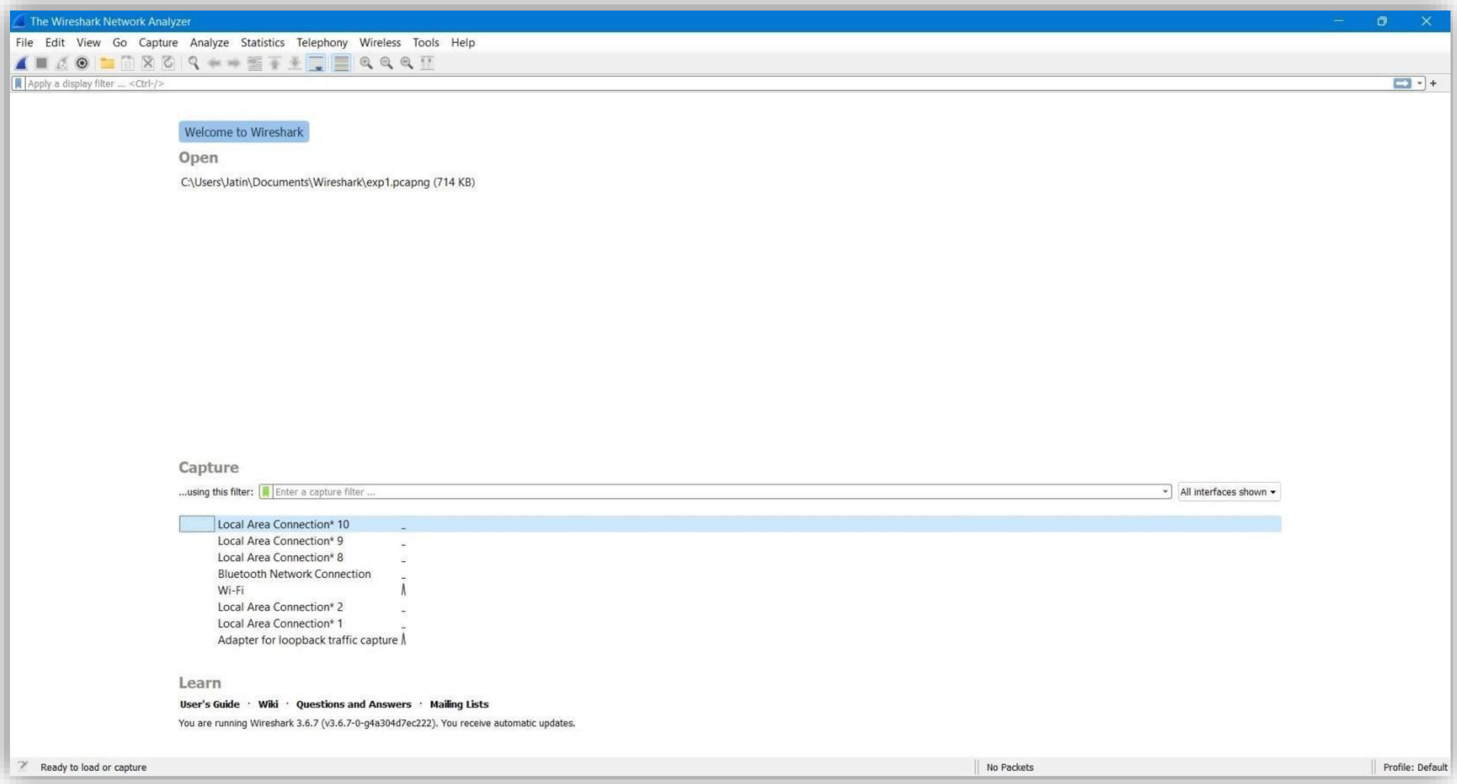
8. Go back to your Wireshark screen and press Ctrl + E to stop capturing.
9. After the traffic capture is stopped, please save the captured traffic into a *.pcap format file and attach it to your support ticket.

- **OUTPUT:**


Clear browsing data

Time range: All time

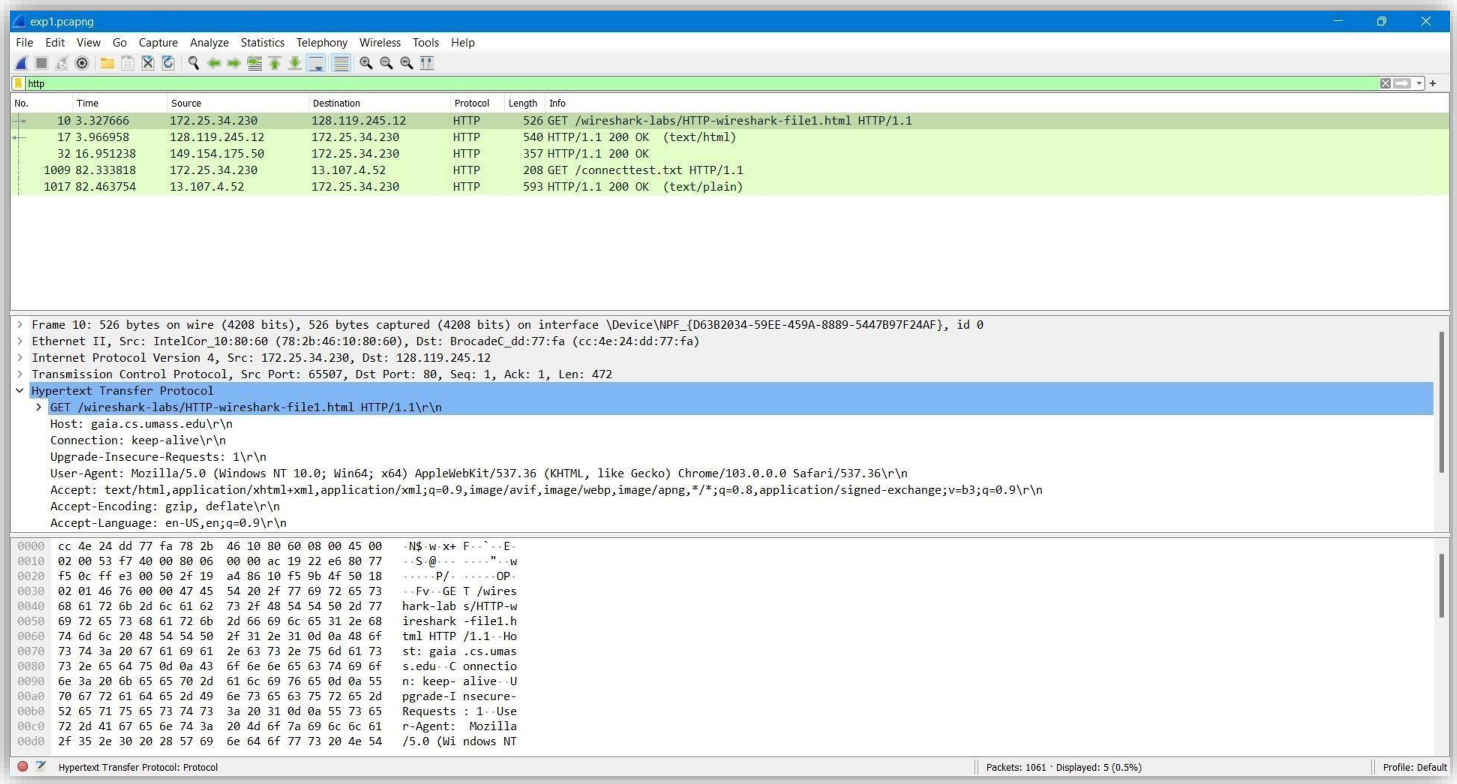
- [✓] Browsing history — 50 items
- [✓] Download history — None
- [✓] Cookies and other site data — From 3 sites
- [✓] Cached images and files — 39.7 MB
- [✓] Passwords and other sign-in data — None
- [✓] Autofill form data


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
Ready to load or capture
No Packets
Profile: Default

C:\Users\Jatin\Documents\Wireshark\exp1.pcapng (714 KB)

Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1
Adapter for loopback traffic capture

You are running Wireshark 3.6.7 (v3.6.7-0-g4a304d7ec222). You receive automatic updates.

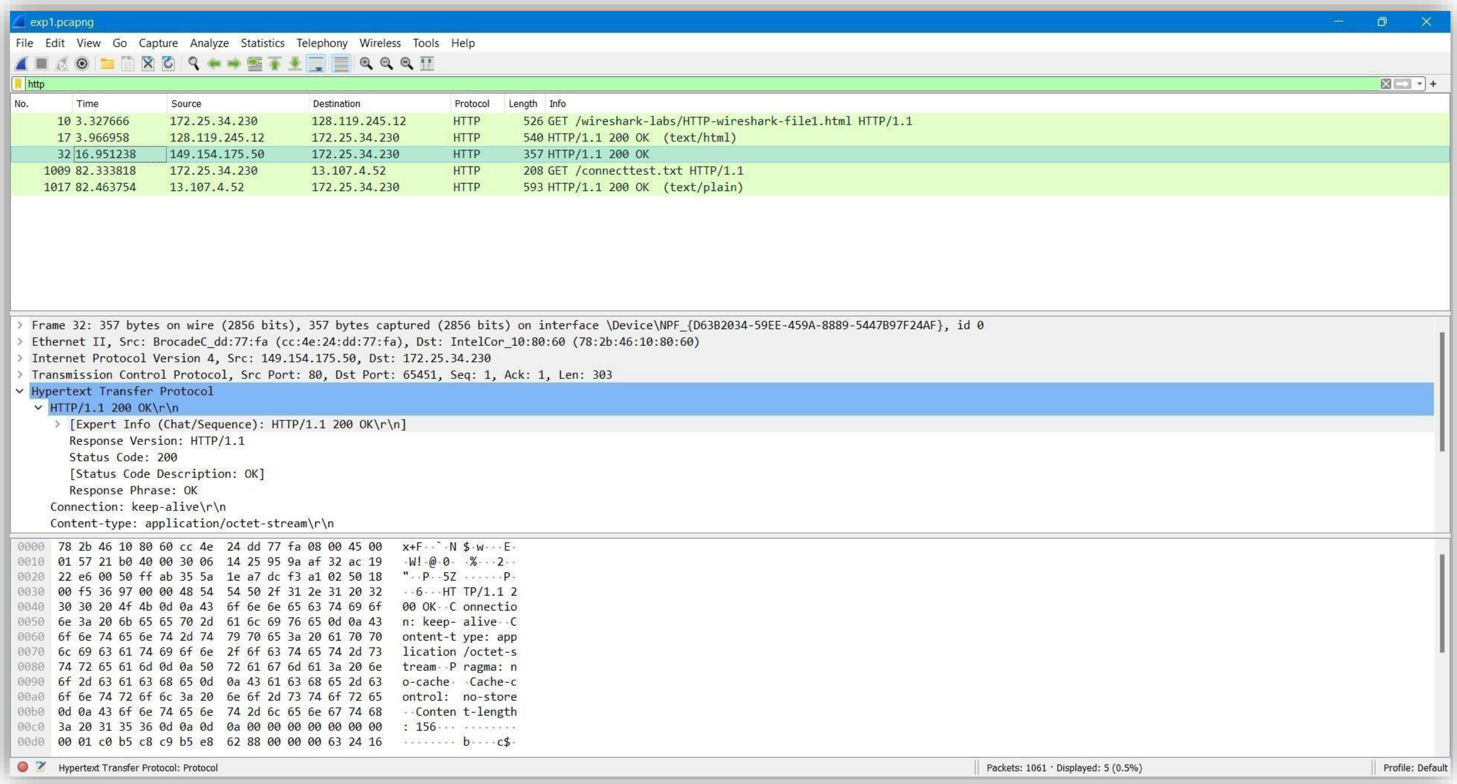

exp1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Packets: 1061 · Displayed: 5 (0.5%)
Profile: Default

```
No.    Time          Source            Destination       Protocol  Length  Info
  10 3.327666     172.25.34.230     128.119.245.12    HTTP      526 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  17 3.966958     128.119.245.12    172.25.34.230     HTTP      540 HTTP/1.1 200 OK  (text/html)
  32 16.951238    149.154.175.50    172.25.34.230     HTTP      357 HTTP/1.1 200 OK
1009 82.333818    172.25.34.230     13.107.4.52       HTTP      208 GET /connecttest.txt HTTP/1.1
1017 82.463754    13.107.4.52       172.25.34.230     HTTP      593 HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 10: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{D63B2034-59EE-459A-8889-5447B97F24AF}, id 0
> Ethernet II, Src: IntelCor_10:80:60 (78:2b:46:10:80:60), Dst: BrocadeC_dd:77:fa (cc:4e:24:dd:77:fa)
> Internet Protocol Version 4, Src: 172.25.34.230, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 65507, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\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/103.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
```

```
0000  cc 4e 24 dd 77 fa 78 2b  46 10 80 60 08 00 45 00   ·N$·w·x+ F··`··E·
0010  02 00 53 f7 40 00 80 06  00 00 ac 19 22 e6 80 77   ··S·@··· ····"··w
0020  f5 0c ff e3 00 50 2f 19  a4 86 10 f5 9b 4f 50 18   ·····P/· ·····OP·
0030  02 01 46 76 00 00 47 45  54 20 2f 77 69 72 65 73   ··Fv··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
```

Hypertext Transfer Protocol: Protocol



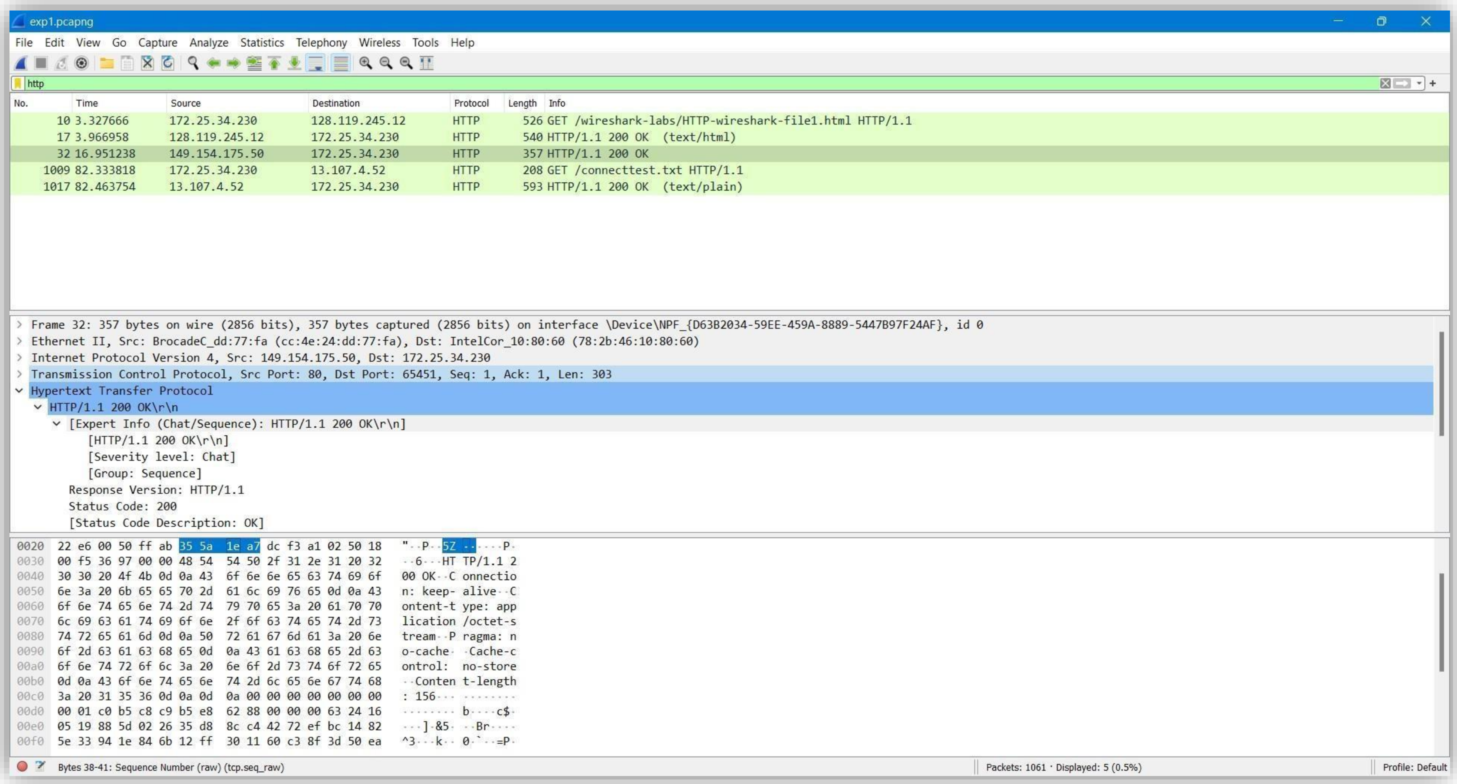
```
exp1.pcapng
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
http

No.   Time        Source           Destination      Protocol  Length  Info
   10 3.327666    172.25.34.230    128.119.245.12   HTTP      526 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   17 3.966958    128.119.245.12   172.25.34.230    HTTP      540 HTTP/1.1 200 OK  (text/html)
   32 16.951238   149.154.175.50   172.25.34.230    HTTP      357 HTTP/1.1 200 OK
 1009 82.333818   172.25.34.230    13.107.4.52      HTTP      208 GET /connecttest.txt HTTP/1.1
 1017 82.463754   13.107.4.52      172.25.34.230    HTTP      593 HTTP/1.1 200 OK  (text/plain)

> Frame 32: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface \Device\NPF_{D63B2034-59EE-459A-8889-5447B97F24AF}, id 0
> Ethernet II, Src: BrocadeC_dd:77:fa (cc:4e:24:dd:77:fa), Dst: IntelCor_10:80:60 (78:2b:46:10:80:60)
> Internet Protocol Version 4, Src: 149.154.175.50, Dst: 172.25.34.230
> Transmission Control Protocol, Src Port: 80, Dst Port: 65451, Seq: 1, Ack: 1, Len: 303
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Connection: keep-alive\r\n
    Content-type: application/octet-stream\r\n

0000  78 2b 46 10 80 60 cc 4e  24 dd 77 fa 08 00 45 00   x+F··`·N $·w···E·
0010  01 57 21 b0 40 00 30 06  14 25 95 9a af 32 ac 19   ·W!·@·0· ·%···2··
0020  22 e6 00 50 ff ab 35 5a  1e a7 dc f3 a1 02 50 18   "··P··5Z ······P·
0030  00 f5 36 97 00 00 48 54  54 50 2f 31 2e 31 20 32   ··6···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 6e 65 63 74 69 6f   00 OK··C onnectio
0050  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 43   n: keep- alive··C
0060  6f 6e 74 65 6e 74 2d 74  79 70 65 3a 20 61 70 70   ontent-t ype: app
0070  6c 69 63 61 74 69 6f 6e  2f 6f 63 74 65 74 2d 73   lication /octet-s
0080  74 72 65 61 6d 0d 0a 50  72 61 67 6d 61 3a 20 6e   tream··P ragma: n
0090  6f 2d 63 61 63 68 65 0d  0a 43 61 63 68 65 2d 63   o-cache· ·Cache-c
00a0  6f 6e 74 72 6f 6c 3a 20  6e 6f 2d 73 74 6f 72 65   ontrol:  no-store
00b0  0d 0a 43 6f 6e 74 65 6e  74 2d 6c 65 6e 67 74 68   ··Conten t-length
00c0  3a 20 31 35 36 0d 0a 0d  0a 00 00 00 00 00 00 00   : 156··· ········
00d0  00 01 c0 b5 c8 c9 b5 e8  62 88 00 00 00 63 24 16   ········ b····c$·

Hypertext Transfer Protocol: Protocol          Packets: 1061 · Displayed: 5 (0.5%)          Profile: Default
```



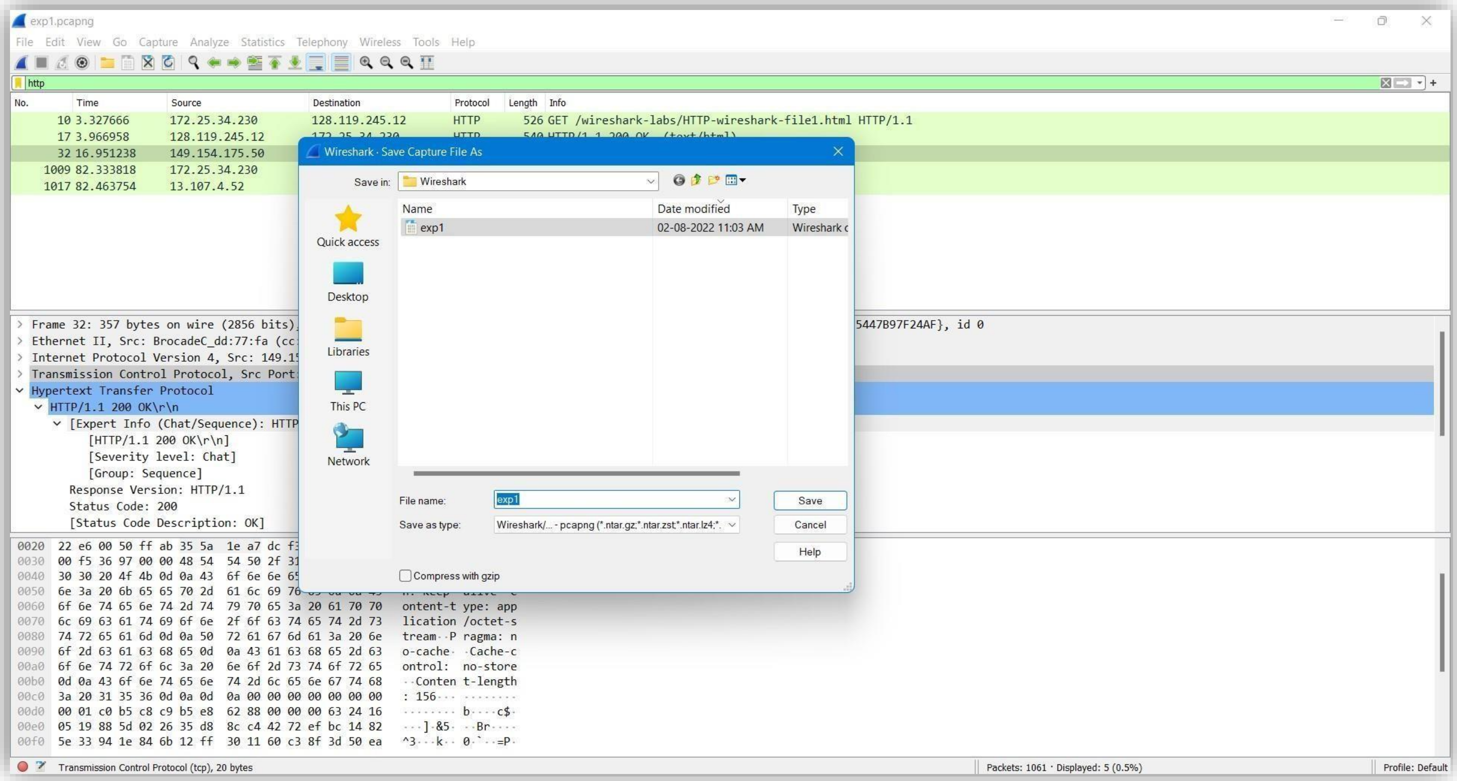
```
exp1.pcapng
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
http

No.   Time        Source           Destination      Protocol  Length  Info
   10 3.327666    172.25.34.230    128.119.245.12   HTTP      526 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   17 3.966958    128.119.245.12   172.25.34.230    HTTP      540 HTTP/1.1 200 OK  (text/html)
   32 16.951238   149.154.175.50   172.25.34.230    HTTP      357 HTTP/1.1 200 OK
 1009 82.333818   172.25.34.230    13.107.4.52      HTTP      208 GET /connecttest.txt HTTP/1.1
 1017 82.463754   13.107.4.52      172.25.34.230    HTTP      593 HTTP/1.1 200 OK  (text/plain)

> Frame 32: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface \Device\NPF_{D63B2034-59EE-459A-8889-5447B97F24AF}, id 0
> Ethernet II, Src: BrocadeC_dd:77:fa (cc:4e:24:dd:77:fa), Dst: IntelCor_10:80:60 (78:2b:46:10:80:60)
> Internet Protocol Version 4, Src: 149.154.175.50, Dst: 172.25.34.230
> Transmission Control Protocol, Src Port: 80, Dst Port: 65451, Seq: 1, Ack: 1, Len: 303
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [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]

0020  22 e6 00 50 ff ab 35 5a  1e a7 dc f3 a1 02 50 18   "··P··5Z ······P·
0030  00 f5 36 97 00 00 48 54  54 50 2f 31 2e 31 20 32   ··6···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 6e 65 63 74 69 6f   00 OK··C onnectio
0050  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 43   n: keep- alive··C
0060  6f 6e 74 65 6e 74 2d 74  79 70 65 3a 20 61 70 70   ontent-t ype: app
0070  6c 69 63 61 74 69 6f 6e  2f 6f 63 74 65 74 2d 73   lication /octet-s
0080  74 72 65 61 6d 0d 0a 50  72 61 67 6d 61 3a 20 6e   tream··P ragma: n
0090  6f 2d 63 61 63 68 65 0d  0a 43 61 63 68 65 2d 63   o-cache· ·Cache-c
00a0  6f 6e 74 72 6f 6c 3a 20  6e 6f 2d 73 74 6f 72 65   ontrol:  no-store
00b0  0d 0a 43 6f 6e 74 65 6e  74 2d 6c 65 6e 67 74 68   ··Conten t-length
00c0  3a 20 31 35 36 0d 0a 0d  0a 00 00 00 00 00 00 00   : 156··· ········
00d0  00 01 c0 b5 c8 c9 b5 e8  62 88 00 00 00 63 24 16   ········ b····c$·
00e0  05 19 88 5d 02 26 35 d8  8c c4 42 72 ef bc 14 82   ···]·&5· ··Br····
00f0  5e 33 94 1e 84 6b 12 ff  30 11 60 c3 8f 3d 50 ea   ^3···k·· 0·`··=P·

Bytes 38-41: Sequence Number (raw) (tcp.seq_raw)          Packets: 1061 · Displayed: 5 (0.5%)          Profile: Default
```


exp1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Save Capture File As
Save in: Wireshark
Quick access
Desktop
Libraries
This PC
Network
Save
Cancel
Help
Compress with gzip
Packets: 1061 · Displayed: 5 (0.5%)
Profile: Default

http

```
No.   Time        Source           Destination      Protocol  Length Info
   10 3.327666    172.25.34.230    128.119.245.12   HTTP      526 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   17 3.966958    128.119.245.12
   32 16.951238   149.154.175.50
 1009 82.333818   172.25.34.230
 1017 82.463754   13.107.4.52
```

Name	Date modified	Type
exp1	02-08-2022 11:03 AM	Wireshark c

File name: exp1

Save as type: Wireshark/... - pcapng (*.ntar.gz;*.ntar.zst;*.ntar.lz4;*.

```
> Frame 32: 357 bytes on wire (2856 bits)                 5447B97F24AF}, id 0
> Ethernet II, Src: BrocadeC_dd:77:fa (cc
> Internet Protocol Version 4, Src: 149.15
> Transmission Control Protocol, Src Port:
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
```

```
0020  22 e6 00 50 ff ab 35 5a  1e a7 dc f3
0030  00 f5 36 97 00 00 48 54  54 50 2f 31
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 6e 65
0050  6e 3a 20 6b 65 65 70 2d  61 6c 69 76
0060  6f 6e 74 65 6e 74 2d 74  79 70 65 3a 20 61 70 70   ontent-t ype: app
0070  6c 69 63 61 74 69 6f 6e  2f 6f 63 74 65 74 2d 73   lication /octet-s
0080  74 72 65 61 6d 0d 0a 50  72 61 67 6d 61 3a 20 6e   tream··P ragma: n
0090  6f 2d 63 61 63 68 65 0d  0a 43 61 63 68 65 2d 63   o-cache· ·Cache-c
00a0  6f 6e 74 72 6f 6c 3a 20  6e 6f 2d 73 74 6f 72 65   ontrol:  no-store
00b0  0d 0a 43 6f 6e 74 65 6e  74 2d 6c 65 6e 67 74 68   ··Conten t-length
00c0  3a 20 31 35 36 0d 0a 0d  0a 00 00 00 00 00 00 00   : 156··· ········
00d0  00 01 c0 b5 c8 c9 b5 e8  62 88 00 00 00 63 24 16   ········ b···c$·
00e0  05 19 88 5d 02 26 35 d8  8c c4 42 72 ef bc 14 82   ···]·&5· ··Br····
00f0  5e 33 94 1e 84 6b 12 ff  30 11 60 c3 8f 3d 50 ea   ^3···k·· 0·`··=P·
```

Transmission Control Protocol (tcp), 20 bytes

- **Learning Outcomes:**
  1. Identify requests (from client) and response packets.
  2. Find HTTP version, response code/phrase, requested file (including size).
  3. Observe single small file (e.g., simple html file) request/response behaviour and the request/response behaviour for a file that has already been received.
  4. Observe how a larger file is sent in multiple segments ‘
  5. Observe multi-file (e.g., web page with image) request/response behaviour. Observe request/response behaviour for a page that needs authentication.