



**Computer Engineering Department**  
**Engineering Department**

**Academic Year: 2021-2022**

**Class: S.Y.B.Tech Sem.: 4 Course: CCN**

<b>Name</b>	<b>Pratik Pujari</b>		
<b>UID no.</b>	<b>2020300054</b>	<b>Class:</b>	<b>Comps C Batch</b>
<b>Experiment No.</b>	<b>4</b>		

<b>AIM:</b>	To capture packet using WireShark application
<b>THEORY:</b>	<p><b>What is a network packet?</b></p> <p>A network packet is a small amount of data sent over Transmission Control Protocol/Internet Protocol (TCP/IP) networks. The packet size is around 1.5 kilobytes for Ethernet and 64 KB for IP payloads.</p> <p>A packet is the unit of data routed between an origin and a destination on the internet or other packet-switched network -- or networks that ship data around in small packets.</p> <p><b>What is a network packet?</b></p> <p>A network packet is a small amount of data sent over Transmission Control Protocol/Internet Protocol (TCP/IP) networks. The packet size is around 1.5 kilobytes for Ethernet and 64 KB for IP payloads.</p> <p>A packet is the unit of data routed between an origin and a destination on the internet or other packet-switched network -- or networks that ship data around in small packets.</p> <p><b>What are the parts of a network packet?</b></p> <p>Network packets are made up of three different parts: header, payload and trailer. Conceptually, they're like a postal package. In this scenario, the header is the box/envelope, the payload is content and the trailer is the signature.</p>



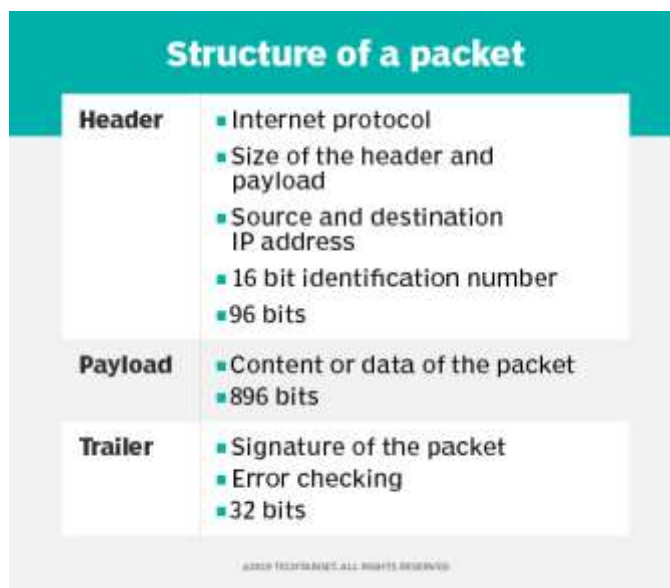
**Computer Engineering Department**  
**Engineering Department**

**Academic Year: 2021-2022**

**Class: S.Y.B.Tech Sem.: 4 Course: CCN**

The header contains instructions related to the data in the packet. These instructions can include the following:

- checksum, which detects errors;
- 16-bit identification number;
- flags to let a router know if it can fragment a packet;
- fragmentation offsets, which reconstruct fragmented packets;
- destination address;
- number of hops a packet can make;
- IP;
- length of the packet -- but not always, as some networks have fixed-length packets;
- size of the header and payload;
- time-to-live;
- originating address;
- packet number, in relation to the packet sequence;
- protocol or what type of packet is transmitted; and
- synchronization or the few bits that enable the packet to match up to the network.
- The payload is the data within the packet. This is the basic information that the packet delivers to the destination.





**Computer Engineering Department**  
**Engineering Department**

**Academic Year: 2021-2022**

**Class: S.Y.B.Tech Sem.: 4 Course: CCN**

## **What Is Wireshark?**

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

How to Install Wireshark on Linux

If you have a Linux system, you'd install Wireshark using the following sequence (notice that you'll need to have root permissions):

- \$ sudo apt-get install wireshark
- \$ sudo dpkg-reconfigure wireshark-common
- \$ sudo usermod -a -G wireshark \$USER
- \$ newgrp wireshark

Once you have completed the above steps, you then log out and log back in, and then start Wireshark:

- \$ wireshark &



**Computer Engineering Department**  
**Engineering Department**

**Academic Year: 2021-2022**

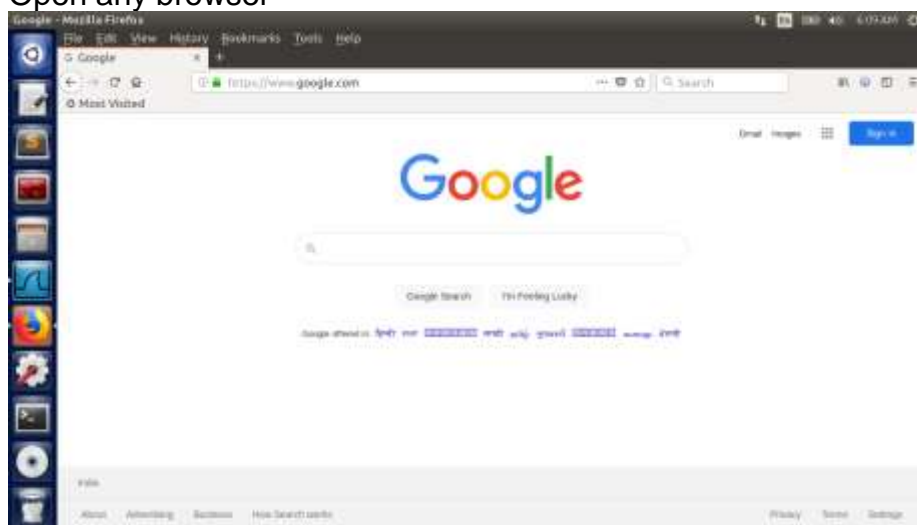
**Class: S.Y.B.Tech Sem.: 4 Course: CCN**

**EXPERIMENT 1**

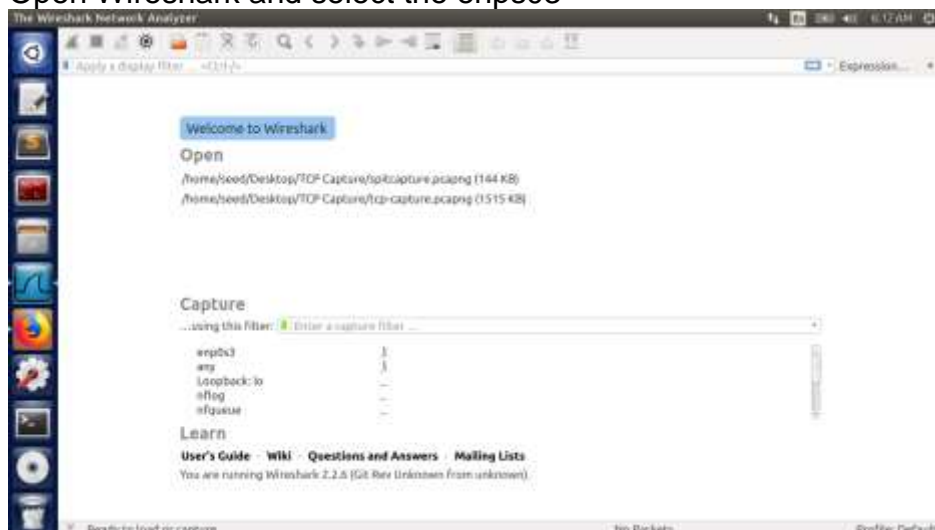
**STARTUP:**

Get Started in Wireshark

Open any browser



Open Wireshark and select the enps03



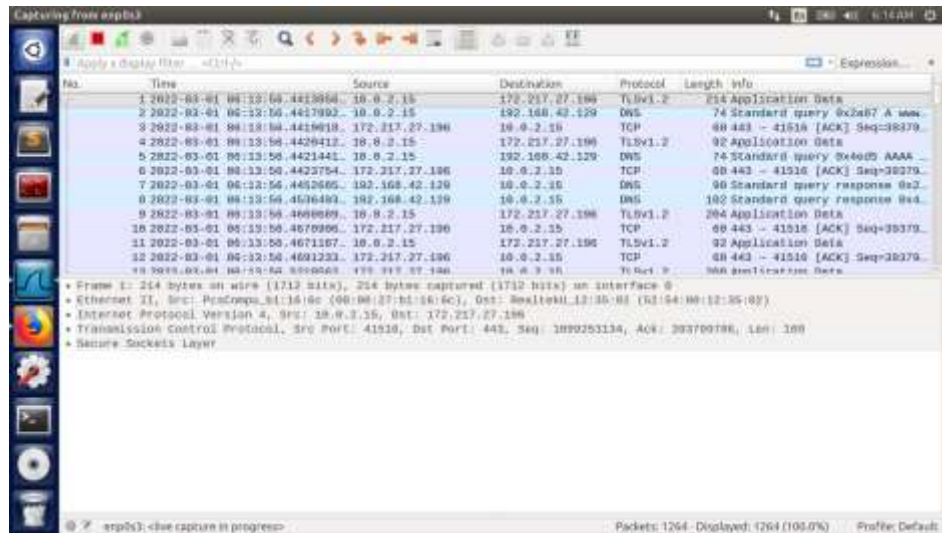
Load a website in the Browser in order to capture the packet in wireshark



**Computer Engineering Department**  
**Engineering Department**

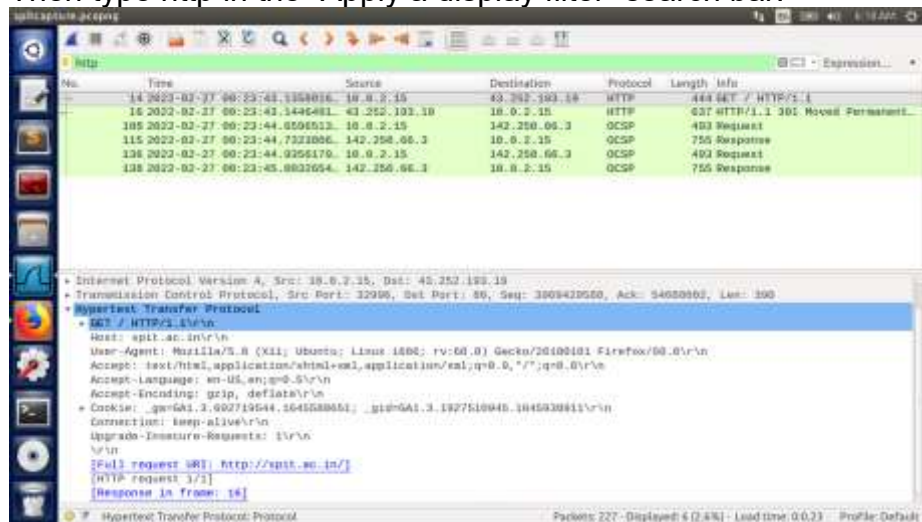
**Academic Year: 2021-2022**

**Class: S.Y.B.Tech Sem.: 4 Course: CCN**



You should get all the packet related info in the wireshark.

Then type http in the “Apply a display filter” search bar.



Here you can see all the Http get request and response

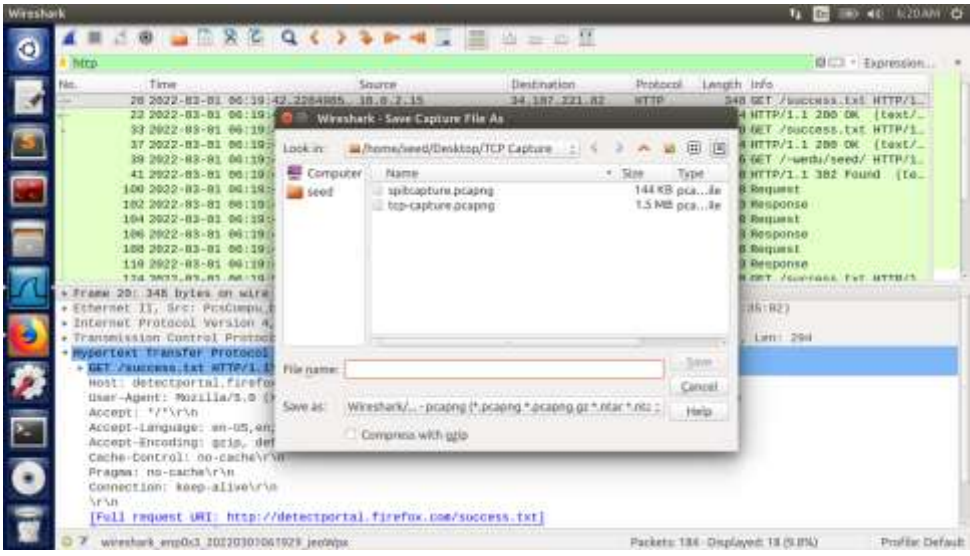
To save the captured packets click on the save capture file and save it



**Computer Engineering Department**  
**Engineering Department**

Academic Year: 2021-2022

Class: S.Y.B.Tech Sem.: 4 Course: CCN

	
<b>QUESTIONS:</b>	<ol style="list-style-type: none"><li><b>1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?</b> <pre>GET / HTTP/1.1\r\n Host: spit.ac.in\r\n User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n Accept-Encoding: gzip, deflate\r\n</pre><p>HTTP version:1.1</p></li><li><b>2. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?</b> <pre>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n Accept-Encoding: gzip, deflate\r\n</pre><p>Language used : English US</p></li><li><b>3. What is the IP address of your computer?</b> <pre>Source: 10.0.2.15 Destination: 43.252.193.19</pre><p>IP Address: 10. 0. 2.15</p></li></ol>





**Computer Engineering Department**  
**Engineering Department**

Academic Year: 2021-2022

Class: S.Y.B.Tech Sem.: 4 Course: CCN

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

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
Status Code: 200
```

**5. When was the HTML file that you are retrieving last modified at the server?**

```
Date: Tue, 01 Mar 2022 07:13:09 GMT\r\n
Etag: "621d0c7c-1d7"\r\n
Expires: Wed, 02 Mar 2022 19:02:53 GMT\r\n
Last-Modified: Mon, 28 Feb 2022 17:55:08 GMT\r\n
```

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

```
Location: https://spit.ac.in/\r\n
Content-Length: 227\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Total bytes captured: 227 bytes
```

**7. By inspecting the raw data in the "packet bytes" pane, do you see any http headers within the data that are not displayed in the "packet details" pane? If so, name one.**

No, there is no more headers below.

**8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?**



**Computer Engineering Department**  
**Engineering Department**

Academic Year: 2021-2022

Class: S.Y.B.Tech Sem.: 4 Course: CCN

```
- Hypertext Transfer Protocol
- GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
  [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
  [Severity Level: Chat]
  [Group: Sequence]
  Request Method: GET
  Request URI: /wireshark-labs/HTTP-wireshark-file1.html
  Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  If-Modified-Since: Tue, 01 Mar 2022 06:59:02 GMT\r\n
```

**9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**

Yes because we can see the contents in the Line-based text data field

**10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?**

**11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.**

→ Request Version: HTTP/1.1  
Status Code: 200  
Response Phrase: OK

The status code and phrase returned from the server is HTTP/1.1 200 OK. The server did return all the contents of the file since it was initially loaded into the browser

**12. How many HTTP GET request messages were sent by your browser?**





**Computer Engineering Department**  
**Engineering Department**

**Academic Year: 2021-2022**

**Class: S.Y.B.Tech Sem.: 4 Course: CCN**

```
14 2022-02-27 08:23:43.1358916 10.0.2.15 43.252.193.19 HTTP 444 GET / HTTP/1.1
16 2022-02-27 08:23:43.1448491 43.252.193.19 10.0.2.15 HTTP 657 HTTP/1.1 301 Moved P...
...
Frame 14: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface 0
Ethernet II, Src: PcsCompu, Dst: 08:00:37:01:30:06, Dst: RealtekU_32:06:02 (62:54:00:32:06:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 43.252.193.19
Transmission Control Protocol, Src Port: 32906, Dst Port: 80, Seq: 3060429588, Ack: 54800003, Len: 300
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: apit.ac.in\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux 680; rv:60.0) Gecko/20100101 Firefox/60.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Cookie: qm6A1.8.692719544.1645589891; _gid=6A1.8.3827518045.1645938911\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://apit.ac.in/]
[HTTP request 1/1]
[Response in frame 16]
```

There was 1 HTTP GET request message sent by my browser as seen in the screenshot.

**13.How many data-containing TCP segments were needed to carry the single HTTP response?**

```
126 2022-03-01 05:28:28.6343263 10.0.2.15 142.250.66.3 TCP 7456762 -> 80 [SYN] Seq...
127 2022-03-01 05:28:28.6478518 142.250.66.3 10.0.2.15 TCP 6088 -> 56762 [SYN, ACK...
128 2022-03-01 05:28:28.6479114 10.0.2.15 142.250.66.3 TCP 5456762 -> 80 [ACK] Seq...
```

Three TCP segments of length 74,60,54 were used.

**14.What is the status code and phrase associated with the response to the HTTP GET request?**

Status code : 200 OK

Status Code: 200  
Response Phrase: OK

**15.Is there any HTTP header information in the transmitted data associated with TCP segmentation?**

No

**16.How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?**

```
19 2022-03-01 05:37:55.8507981 10.0.2.15 34.107.221.82 HTTP 348 GET /success.txt HTTP/1...
21 2022-03-01 05:37:55.8719201 34.107.221.82 10.0.2.15 HTTP 274 HTTP/1.1 200 OK (text/...
59 2022-03-01 05:38:01.3637361 10.0.2.15 34.107.221.82 HTTP 348 GET /success.txt HTTP/1...
63 2022-03-01 05:38:01.3758453 34.107.221.82 10.0.2.15 HTTP 274 HTTP/1.1 200 OK (text/...
```



**Computer Engineering Department**  
**Engineering Department**

**Academic Year: 2021-2022**

**Class: S.Y.B.Tech Sem.: 4 Course: CCN**

	<p>There are 2 GET requests with the following source and destination addresses.</p> <p><b>17.Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.</b></p> <p>By checking the TCP ports we can see if our files were downloaded serially or in parallel. In this case the 2 images were transmitted over 2 TCP connections therefore they were downloaded serially.</p> <p><b>18.What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?</b></p> <p>Status code: 200 , Phrase: OK</p> <p><b>19.When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?</b></p> <pre>Server: nginx\r\n Content-Length: 8\r\n Via: 1.1 google\r\n Date: Mon, 28 Feb 2022 15:19:56 GMT\r\n Cache-Control: public, must-revalidate, max-age=0, s-maxage=86400\r\n Age: 69481\r\n Content-Type: text/plain\r\n</pre> <p>All the fields like Server, Content Length, Via, Date etc</p> <p><b>20.What does the "Connection: close" and "Connection: Keep-alive" header field imply in HTTP protocol? When should one be used over the other?</b></p> <pre>Connection: keep-alive\r\n Upgrade-Insecure-Requests: 1\r\n \r\n</pre> <p>The Connection general header controls whether the network connection stays open after the current transaction finishes. If the</p>
--	--



**Bharatiya Vidya Bhavan's**  
**Sardar Patel Institute of Technology**  
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India  
(Autonomous College Affiliated to University of Mumbai)

**Computer Engineering Department**  
**Engineering Department**

**Academic Year:** 2021-2022

**Class:** S.Y.B.Tech **Sem.:** 4 **Course:** CCN

	value sent is keep-alive, the connection is persistent and not closed, allowing for subsequent requests to the same server to be done.
<b>CONCLUSION:</b> Learnt how to use wireshark on capturing packets. I learnt how to find the http request and response. I understood how to assess the information relating to the http request given by a server.	