

Computer Networks Lab 04

Course: Computer Networks (CL3001)
Instructor: Waseem Rauf

Semester: Spring 2024
T.A: N/A

Note:

- Maintain discipline during the lab.
 - Listen and follow the instructions as they are given.
 - Just raise hand if you have any problem.
 - Completing all tasks of each lab is compulsory.
 - Get your lab checked at the end of the session.
-

Lab Objective

- Implementation & understanding of HTTP/HTTPS.
- Network traffic analysis of HTTP/HTTPS protocol headers, cookies using Wireshark.

HTTP/HTTPS

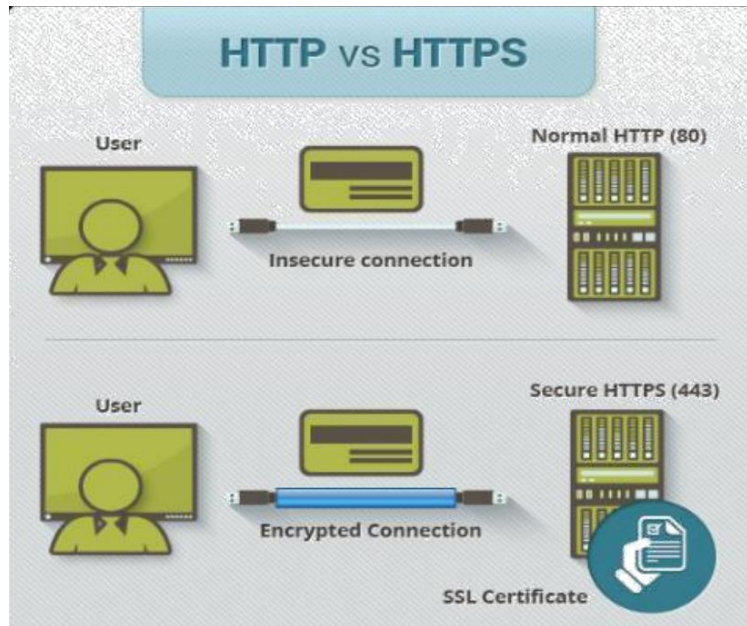
1. Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) is a protocol used in networking. When you type any web address in your web browser, your browser acts as a client, and the computer having the requested information acts as a server. When client requests for any information from the server, it uses HTTP protocol to do so. The server responds back to the client after the request completes. The response comes in the form of web page which you see just after typing the web address and press “Enter”.

2. Hypertext Transfer Protocol Secure (HTTPS)

Hypertext Transfer Protocol Secure (HTTPS) is a combination of two different protocols. It is more secure way to access the web. It is combination of Hypertext Transfer Protocol (HTTP) and SSL/TLS protocol. It is more secure way to sending request to server from a client, also the communication is purely encrypted which means no one can know what you are looking for. This kind of communication is used for accessing those websites where security is required. Banking websites, payment gateway, emails (Gmail offers HTTPS by default in Chrome browser), and corporate sector websites are some great examples where HTTPS protocols are used.

For HTTPS connection, public key trusted and signed certificate is required for the server. These certificates come either free or it costs few dollars depends on the signing authority. There is one other method for distributing certificates. Site admin creates certificates and loads in the browser of users. Now when user requests information to the web server, his identity can be verified easily.



3. Difference between HTTP & HTTPS

Below given are some major differences between HTTP & HTTPS:

HTTP	HTTPS
URL begins with “http://”	URL begins with “https://”
It uses port 80 for communication.	It uses port 443 for communication.
Unsecured.	Secured.
Operates at Application Layer.	Operates at Transport Layer.
No encryption.	Encryption is present.
No certificates required.	Certificates are required.

4a. Client Error

The 4xx class of status code is intended for cases in which the client seems to have erred. Except when responding to a HEAD request, the server should include an entity containing an explanation of the error situation, and whether it is a temporary or permanent condition. These status codes are applicable to any request method. User agents should display any included entity to the user.

400 Bad Request

The server cannot or will not process the request due to something that is perceived to be a client error (e.g., malformed request syntax, invalid request message framing, or deceptive request routing).

401 Unauthorized (RFC 7235)

Similar to 403 Forbidden, but specifically for use when authentication is required and has failed or has not yet been provided. The response must include a WWW-Authenticate header field containing a challenge applicable to the requested resource. See Basic access authentication and Digest access authentication.

403 Forbidden

The request was a valid request, but the server is refusing to respond to it. Unlike a 401 unauthorized response, authenticating will make no difference.

404 Not Found

The requested resource could not be found but may be available again in the future. Subsequent requests by the client are permissible.

408 Request Timeout

The server timed out waiting for the request. According to HTTP specifications: "The client did not produce a request within the time that the server was prepared to wait. The client may repeat the request without modifications at any later time."

4b. Server Error

The server failed to fulfill an apparently valid request.

Response status codes beginning with the digit "5" indicate cases in which the server is aware that it has encountered an error or is otherwise incapable of performing the request. Except when responding to a HEAD request, the server should include an entity containing an explanation of the error situation, and indicate whether it is a temporary or permanent condition. Likewise, user agents should display any included entity to the user. These response codes are applicable to any request method.

500 Internal Server Error

A generic error message, given when an unexpected condition was encountered and no more specific message is suitable.

501 Not Implemented

The server either does not recognize the request method, or it lacks the ability to fulfil the request. Usually this implies future availability (e.g., a new feature of a web-service API).

502 Bad Gateway

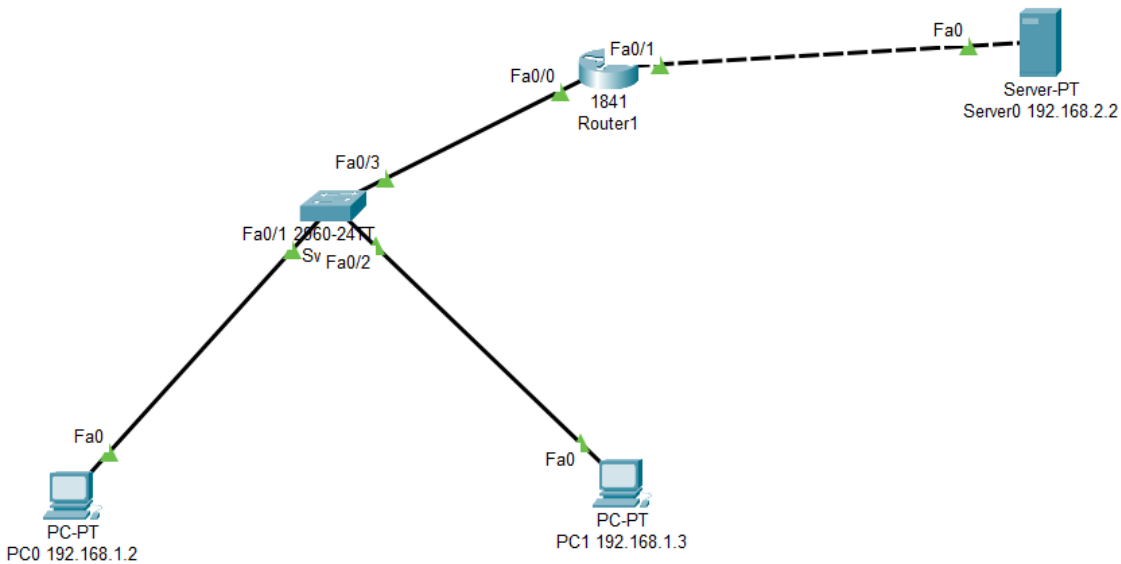
The server was acting as a gateway or proxy and received an invalid response from the upstream server.

503 Service Unavailable

The server is currently unavailable (because it is overloaded or down for maintenance). Generally, this is a temporary state.

5a. Implementation for HTTP

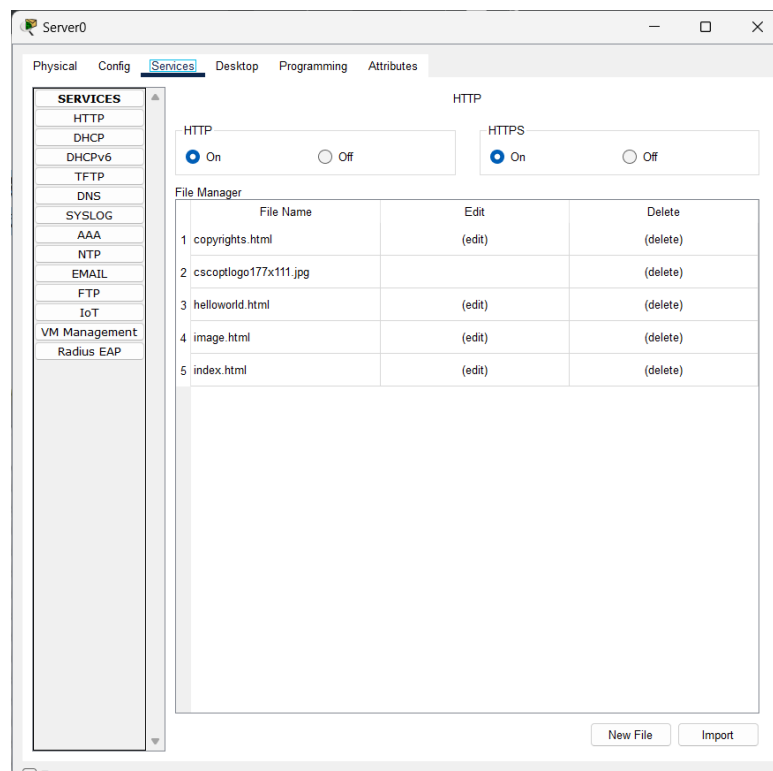
Design the given topology shown below. Assign IP address to PC using static through as done in pervious lab.



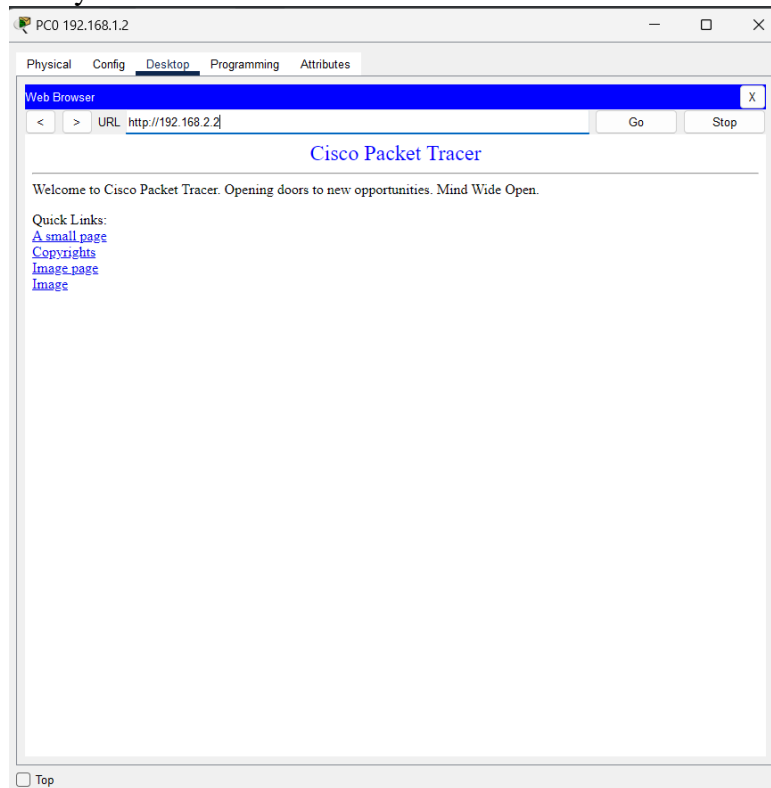
The above topology configured as “one server room”, “one IT room: and “Lab#01 environment having two systems”. On our server we have enabled web services as well as DNS services.

Click on the web server, go to services tab—HTTP

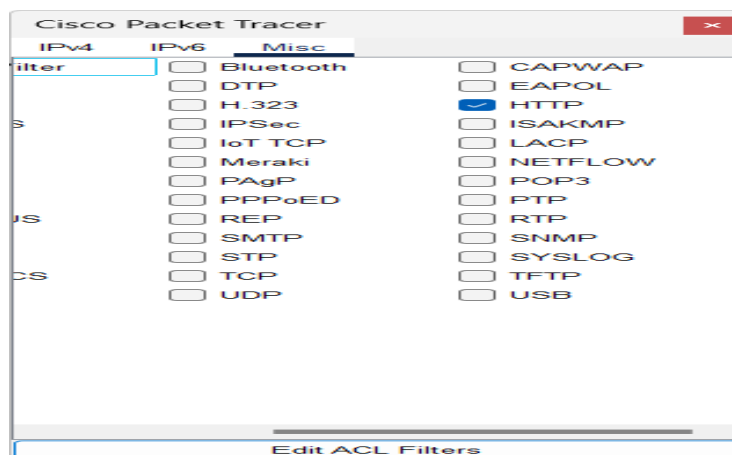
Here you can see HTTP & HTTPS services are on (turn them on if they are previously turned off).



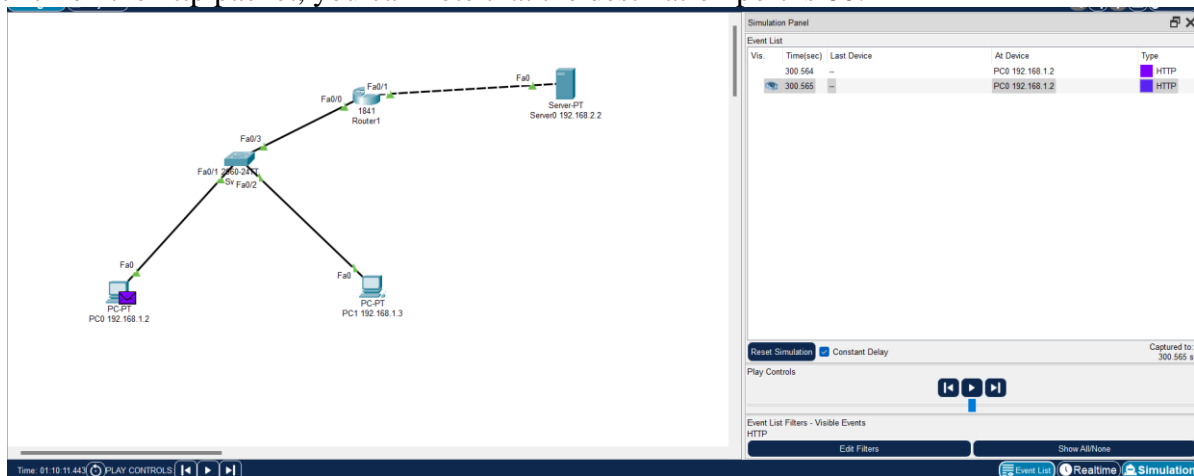
Now click on PC0 and go to Desktop -> Web Browser. Now type web-server IP which you have assign or the website name which you have store in the DNS server record.



To note the http header format information, go to simulation mode edit filters and click on http check box then click on capture/forward button.



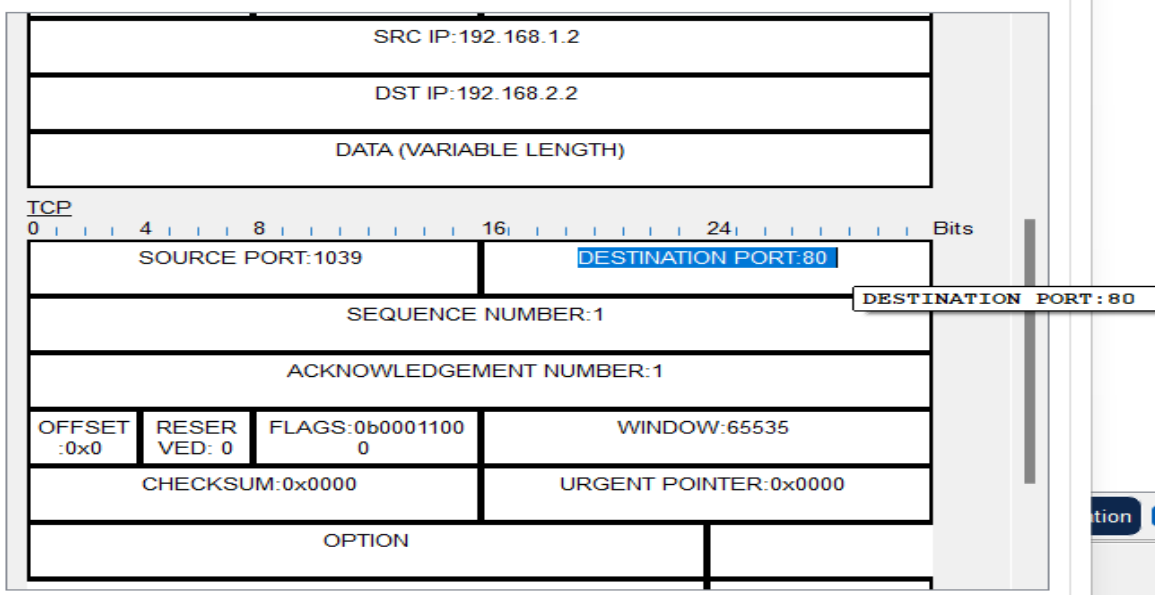
Now click on the http packet, you can note that the destination port is 80.



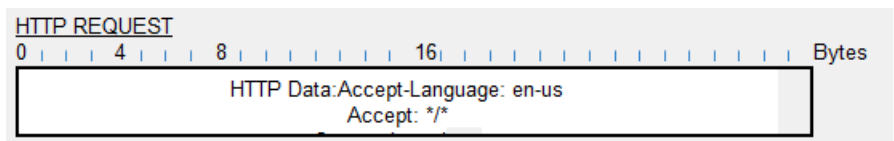
PDU Information at Device: PC0 192.168.1.2

OSI Model Outbound PDU Details

PDU Formats

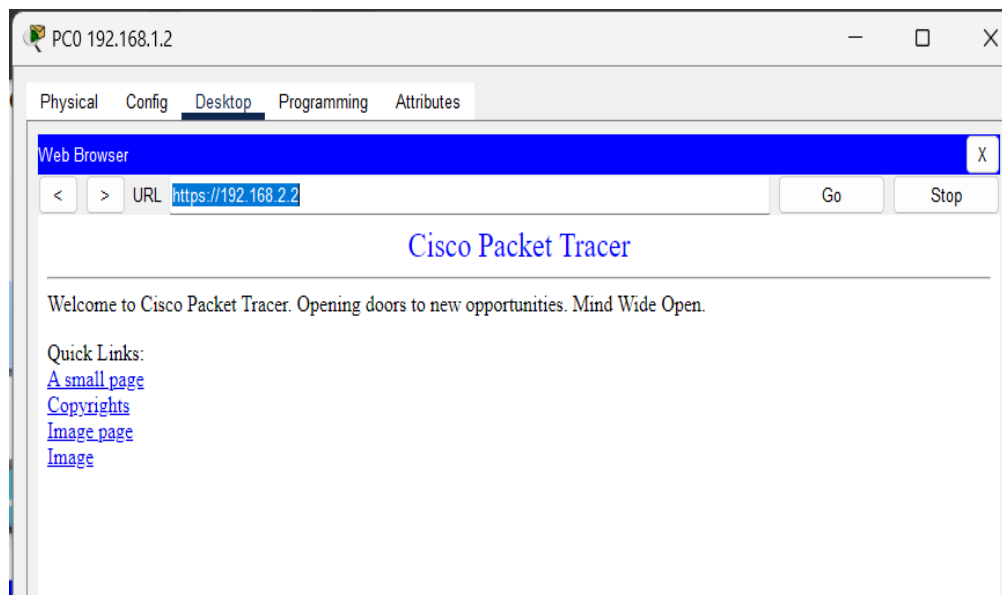


Now scroll the Outbound PDU Details, you can see the http protocol information.

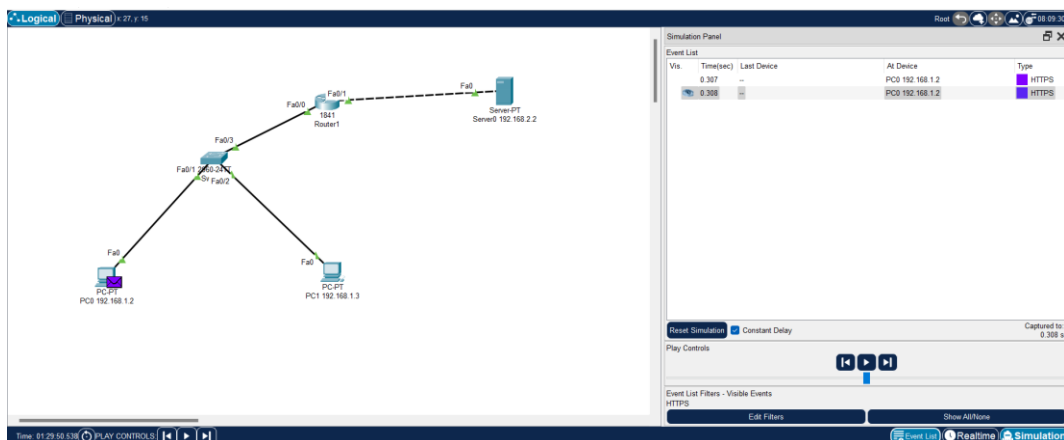
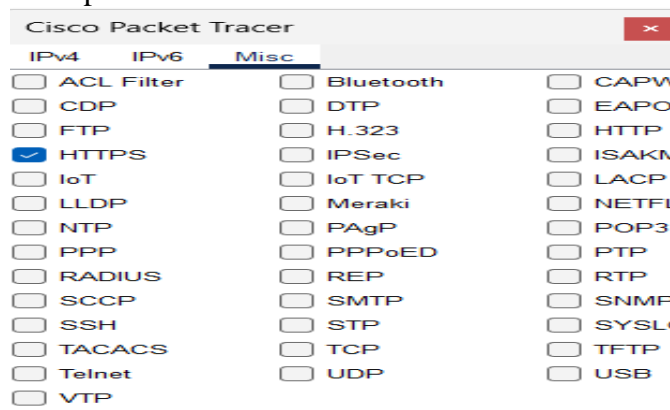


5b. Implementation for HTTPS

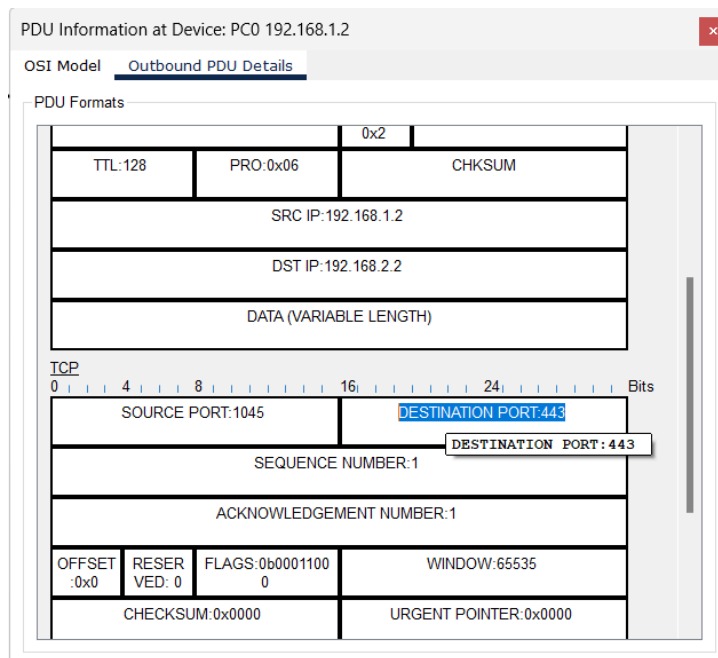
Now click on PC and go to Desktop---->Web Browser. Now type web-server IP 192.168.2.2



Now to note the https header format information go to simulation mode -----> editfilters and click on https check box then click on capture/forward button.



Now click on the https packet, you can note that the destination port is 443.



Now scroll the Outbound PDU Details, you can see the https PDU.

Lab Exercise

1. In caching, what is the difference between the age header and expires?
2. What are the four groupings of HTTP headers?

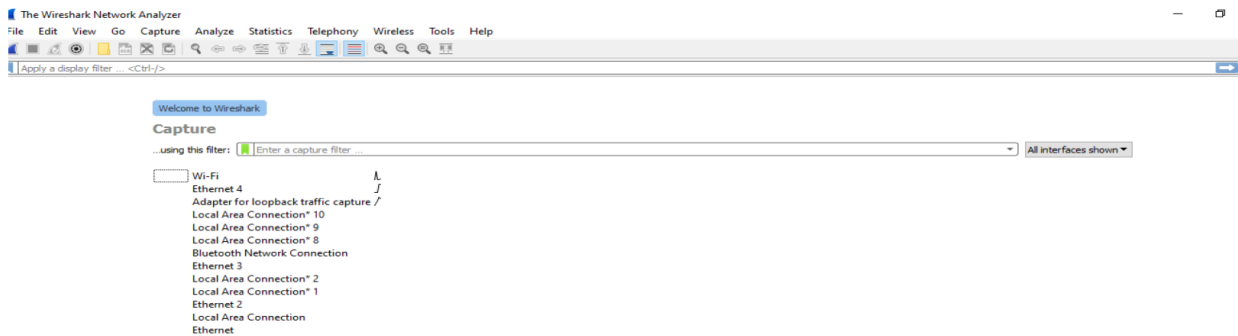
WIRESHARK

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.



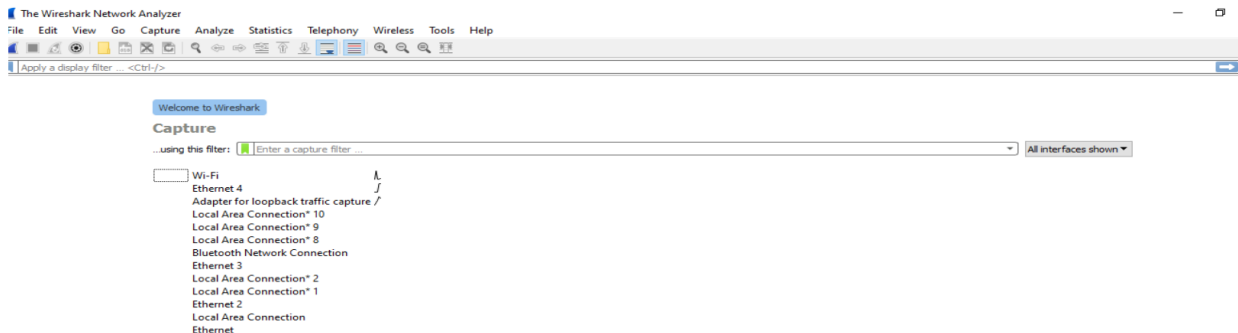
Why we use Wireshark?

Wireshark has many uses, including troubleshooting networks that have performance issues. Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic.

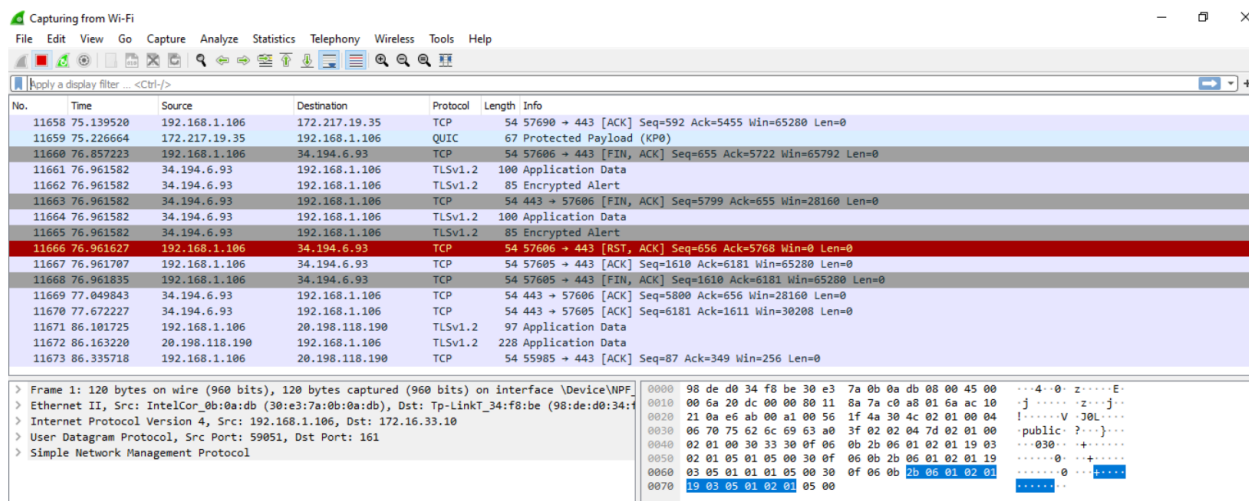


Open Wireshark





Select the technology you used for packet analysis



Lab Exercise

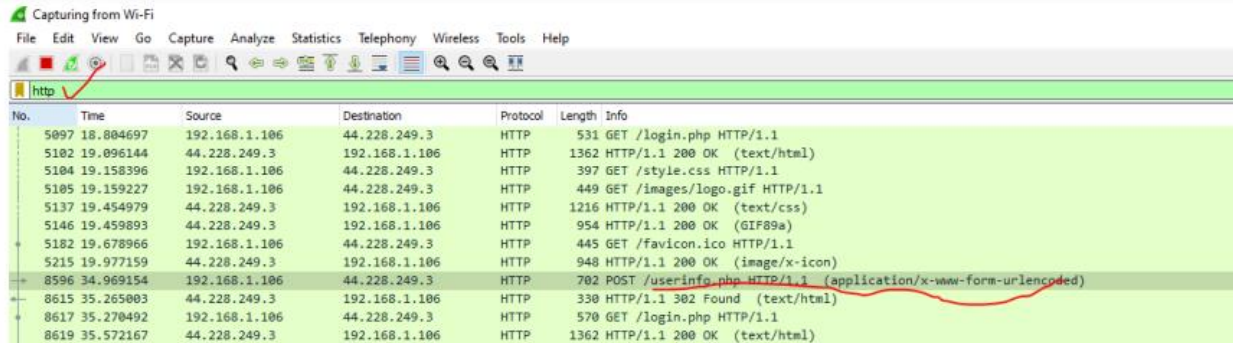
1. Goto website below:

<http://testphp.vulnweb.com/login.php>


Username: test

Password: test

Take Snapshot of each Step, and Submit in Docx file/pdf with one line answer, what you understand here?



No.	Time	Source	Destination	Protocol	Length	Info
5097	18.804697	192.168.1.106	44.228.249.3	HTTP	531	GET /login.php HTTP/1.1
5102	19.096144	44.228.249.3	192.168.1.106	HTTP	1362	HTTP/1.1 200 OK (text/html)
5104	19.158396	192.168.1.106	44.228.249.3	HTTP	397	GET /style.css HTTP/1.1
5105	19.159227	192.168.1.106	44.228.249.3	HTTP	449	GET /images/logo.gif HTTP/1.1
5137	19.454979	44.228.249.3	192.168.1.106	HTTP	1216	HTTP/1.1 200 OK (text/css)
5146	19.459893	44.228.249.3	192.168.1.106	HTTP	954	HTTP/1.1 200 OK (GIF89a)
5182	19.678966	192.168.1.106	44.228.249.3	HTTP	445	GET /favicon.ico HTTP/1.1
5215	19.977159	44.228.249.3	192.168.1.106	HTTP	948	HTTP/1.1 200 OK (image/x-icon)
8596	34.969154	192.168.1.106	44.228.249.3	HTTP	702	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
8615	35.265003	44.228.249.3	192.168.1.106	HTTP	330	HTTP/1.1 302 Found (text/html)
8617	35.270492	192.168.1.106	44.228.249.3	HTTP	570	GET /login.php HTTP/1.1
8619	35.572167	44.228.249.3	192.168.1.106	HTTP	1362	HTTP/1.1 200 OK (text/html)



```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image ^
Referer: http://testphp.vulnweb.com/login.php\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
[HTTP request 3/4]
[Prev request in frame: 5182]
[Response in frame: 8615]
[Next request in frame: 8617]
File Data: 23 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "uname" = "muhammad"
  > Form item: "pass" = "ali"
      Key: pass
      Value: ali
```

2. Follow the above step for HTTPS

Take Snapshot of each Step, and Submit in Docx file/pdf with one line answer, what you understand here?

Observe the difference between HTTP and HTTPS and answer in one line with proper snapshots?