NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Network Lab (CL3001)
Lab Session 04

Objective:

- Implementation & understanding of HTTP/HTTPS.
- Network traffic analysis of HTTP/S 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 (HTTPS) 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. Thesecertificates 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.

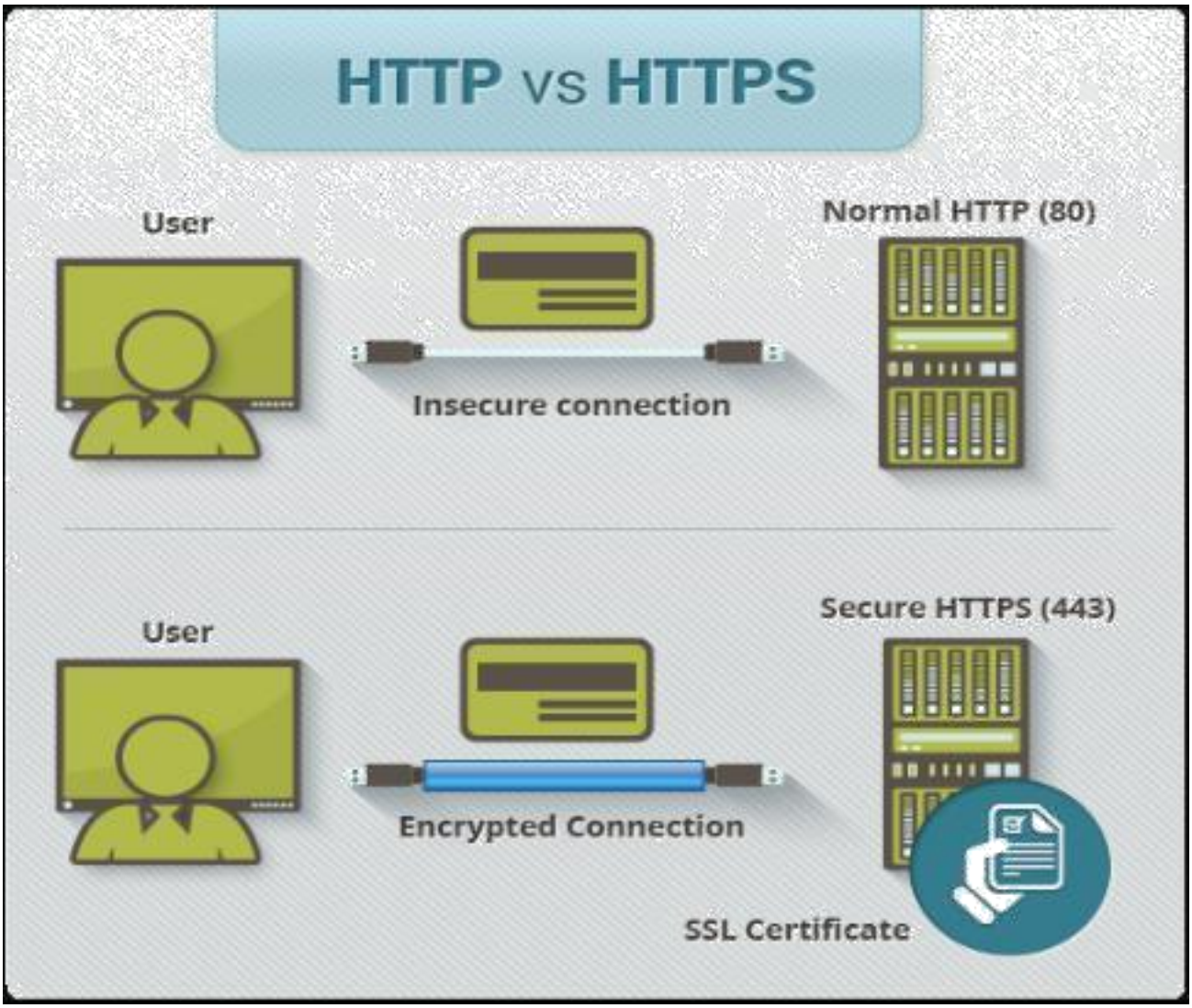

Fig-1: HTTP & HTTPS difference

3. HTTP & HTTPS Differences:

Here are some major difference 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 required

4a. Client Error:

The 4xx class of status code is intended for cases in which the client seems to have erred. Exceptwhen 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 tobe 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 hasfailed 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 accessauthentication 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. Theclient 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 andno 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.

5. Implementation:

Design the given topology shown in figure 2. Assign IP address to PC using static through as done in pervious lab.

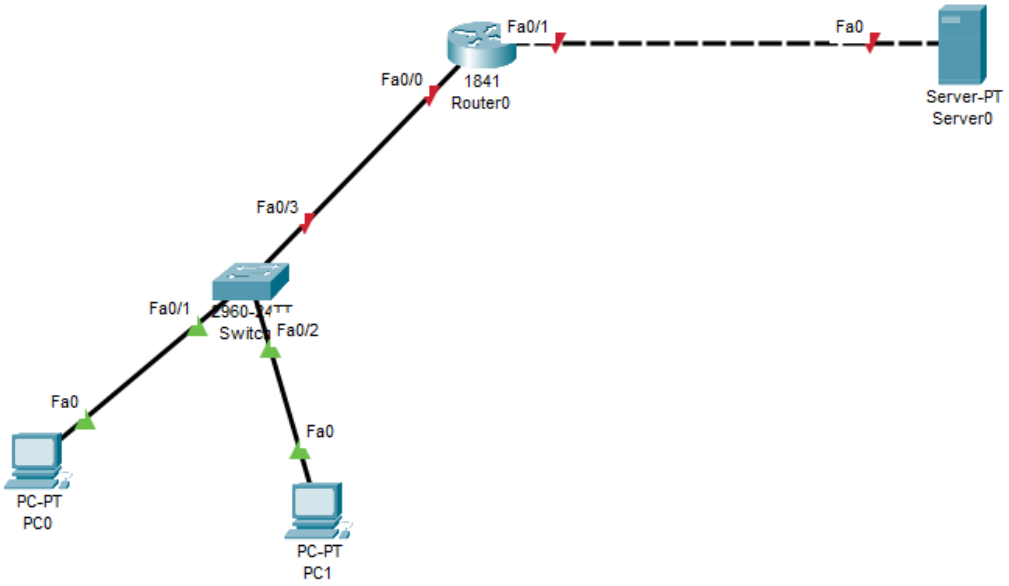

Fig-2: Lab 4 network topology

The above topology configured as “one server room”, “one IT room: and “Lab#01 environment having three systems”. On our server we have enabled web services as well as DNS services. Click on the web server, go to config --->services—HTTP
Here you can see HTTP & HTTPS services are on.

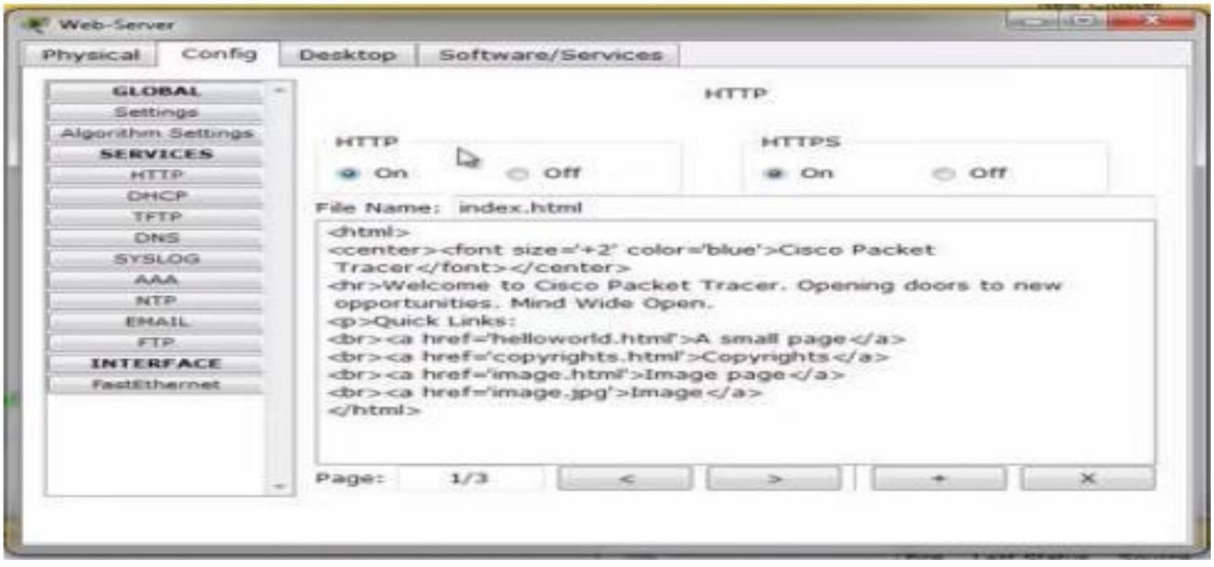

Fig-3: HTTP services on server interface in Packet Tracer

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.

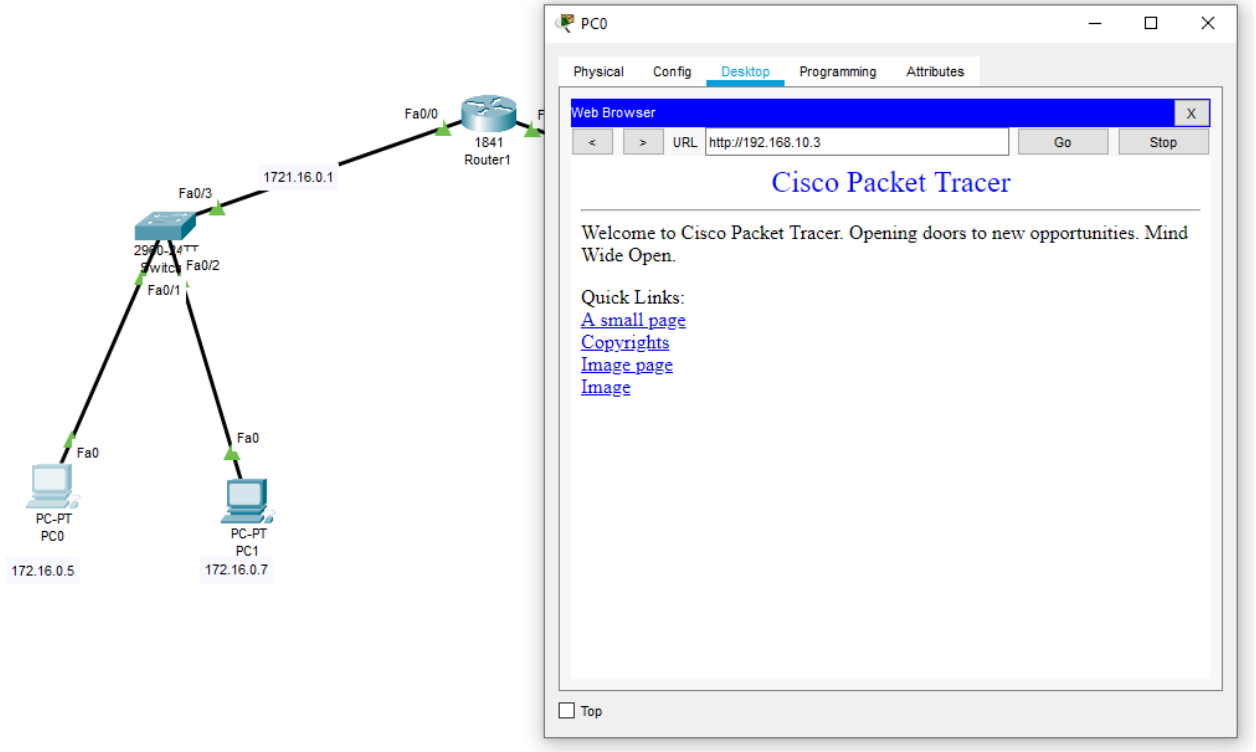

Fig-4: HTTP services on server interface in Packet Tracer

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

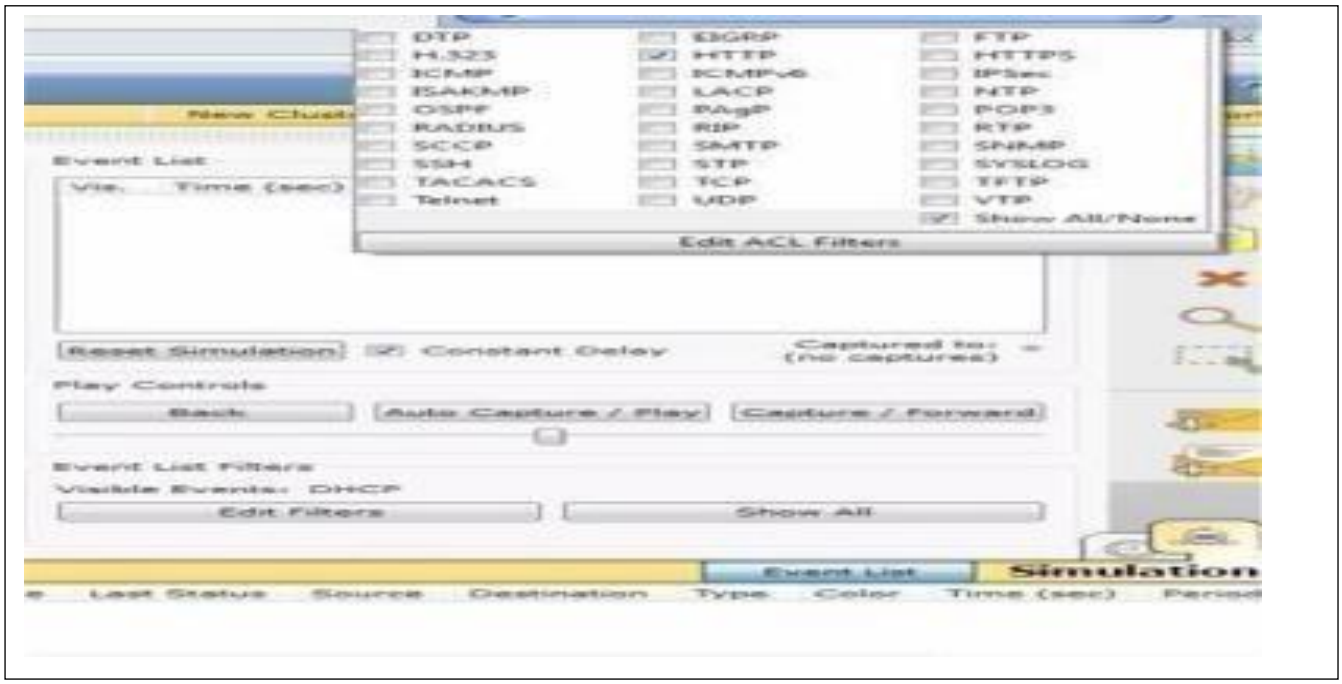

Fig-5: Packet Tracer Simulation Mode Interface

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

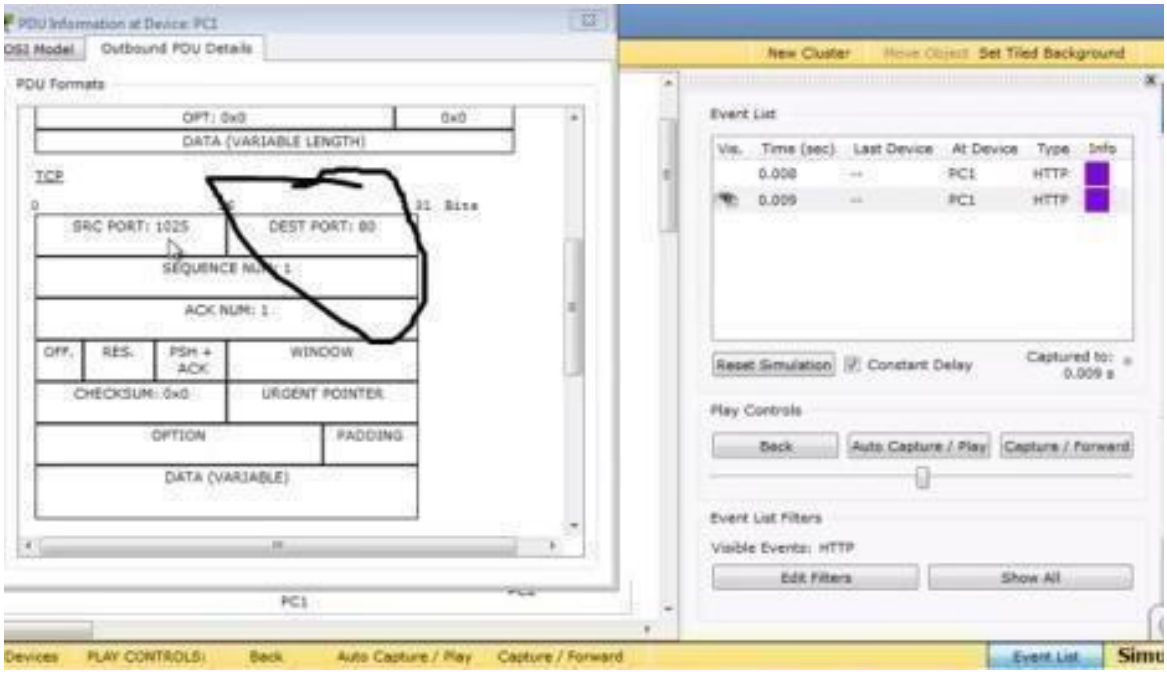

Fig-6: HTTP PDU in Packet Tracer

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

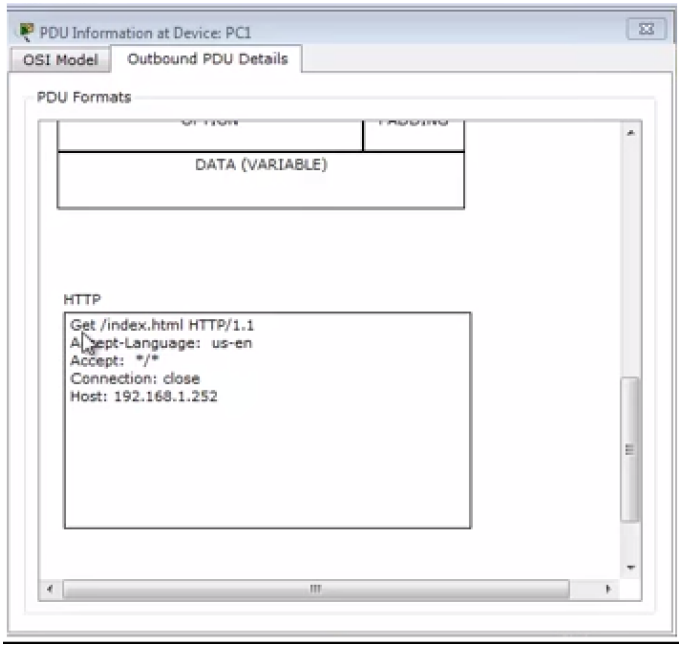

Fig-7: HTTP details in PDU

For HTTPS:

Now click on PC and go to Desktop---- >Web Browser. Now type web-server IP 192.168.1.252

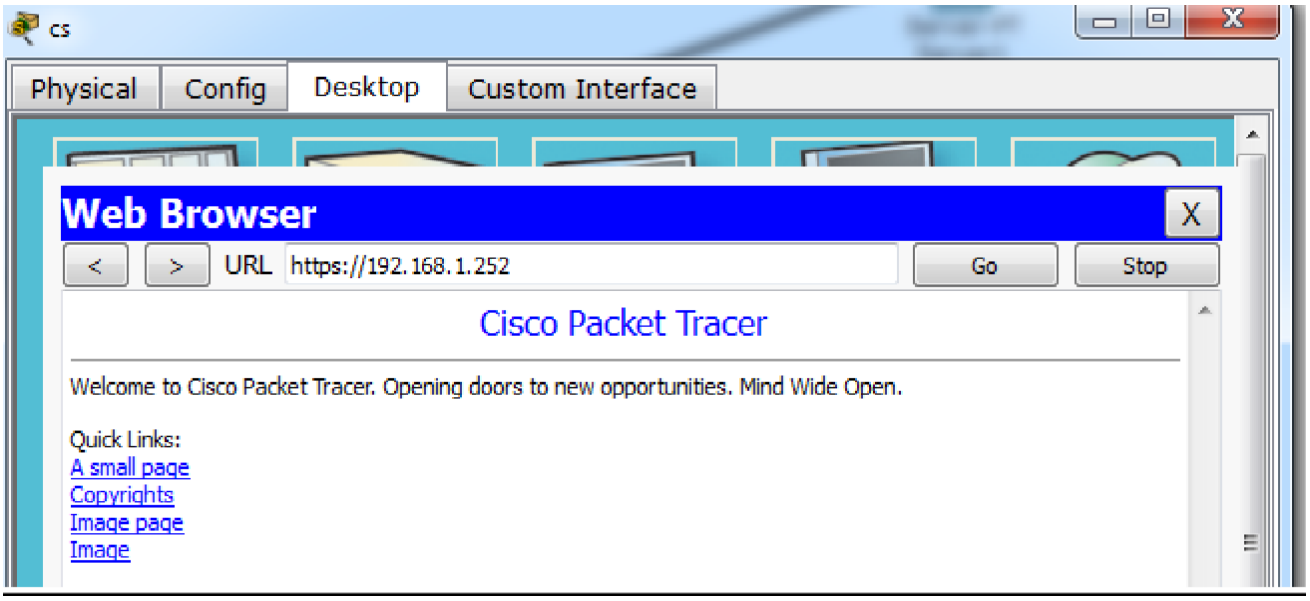

Fig-8: Web page using HTTPS

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.

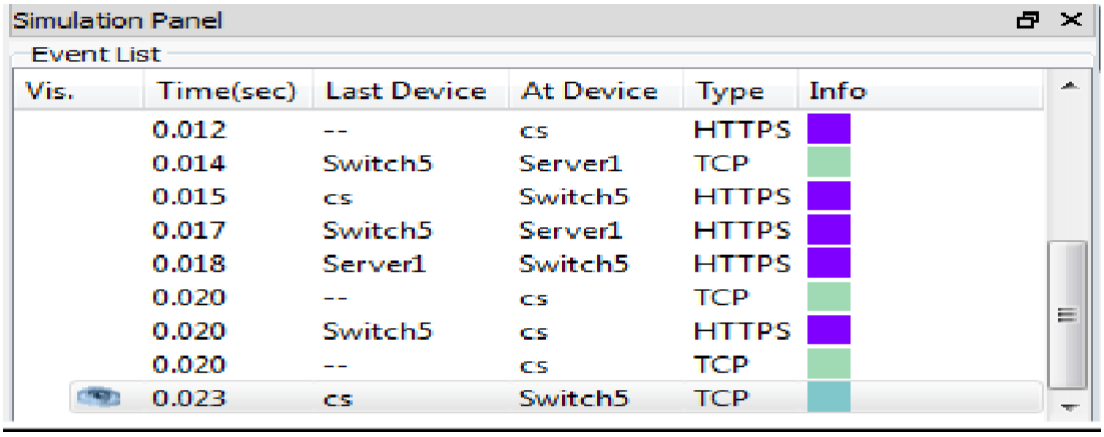

Fig-9: Packets flow in simulation

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

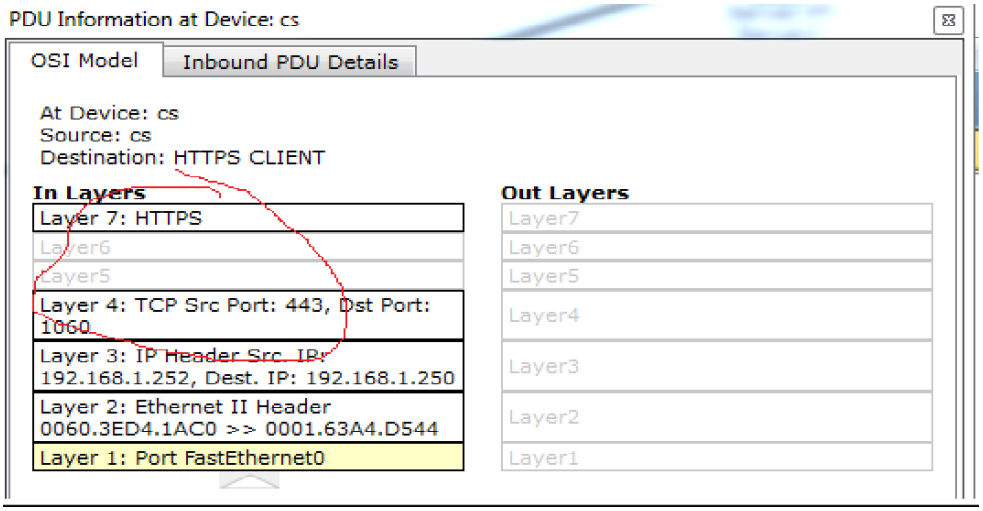

Fig-10: Packet information

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

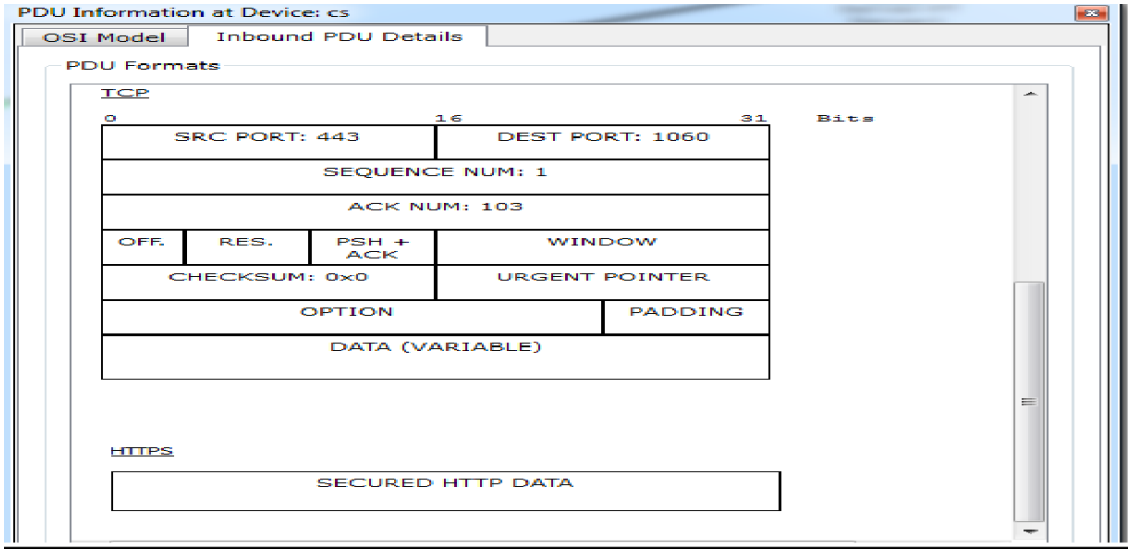

Fig-11: HTTPs PDU details

5. Lab Exercise:

Q1) In caching, what is the difference between the age header and expires?
Q2) What are the four groupings of HTTP headers?

What is Wireshark?

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

Figure 12 Wireshark

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.

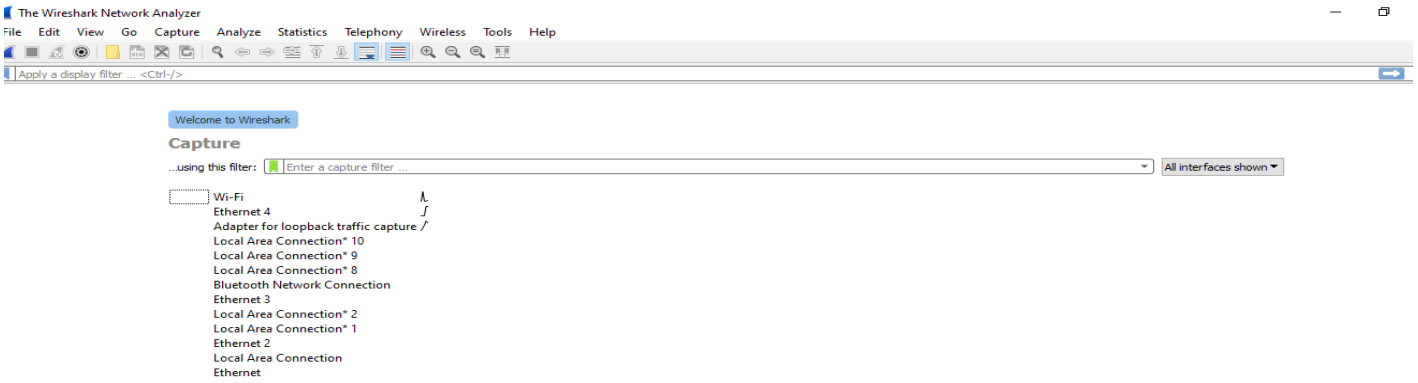

Figure 13 1Wireshark workspace

Open Wireshark

Figure 13 2 Wireshark logo

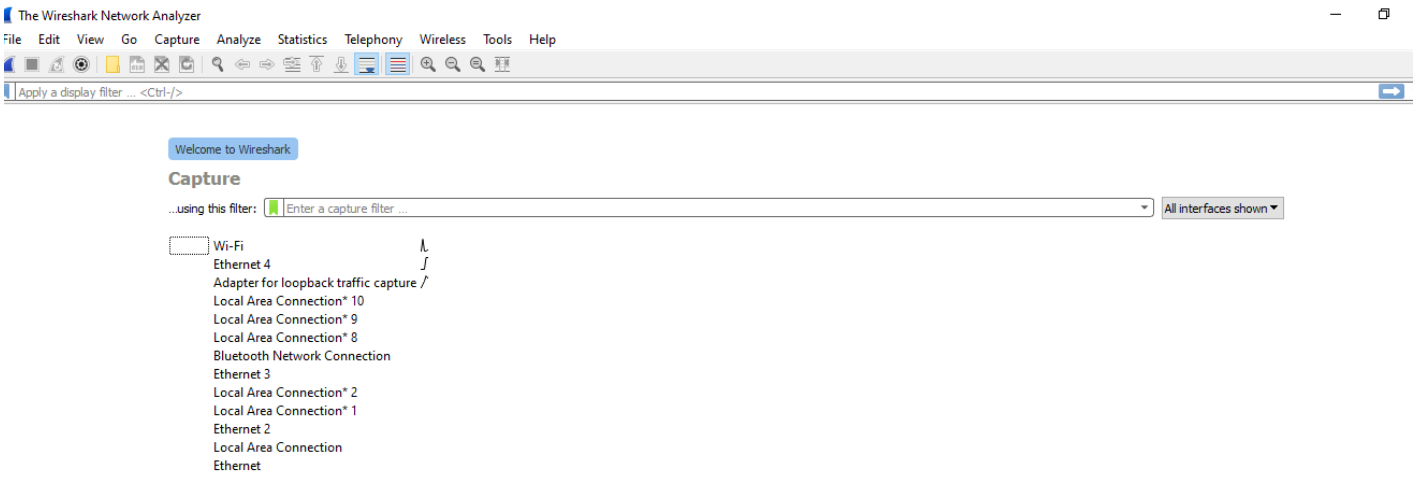

Figure 13 3 Select connected Network

Select the technology you used for packet analysis

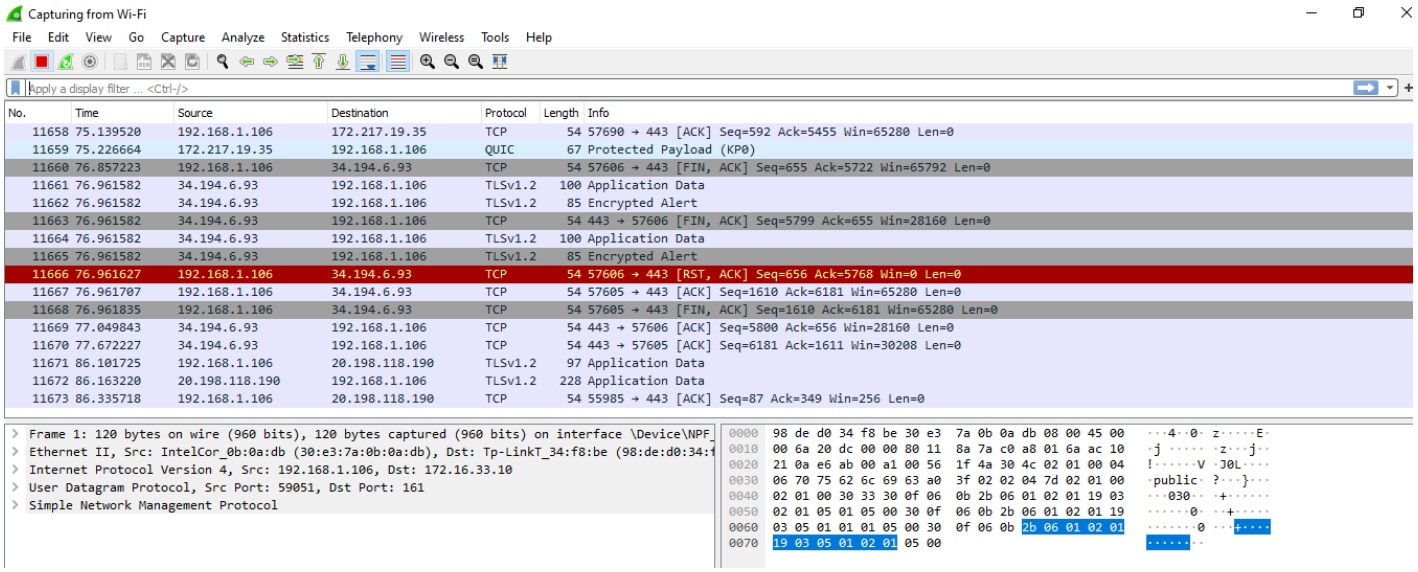

Figure 13 4 Use filter Http for observation

6. Lab Exercise:

TASKs

Goto website below:
http://testphp.vulnweb.com/login.php
Username: your name
Password: you roll number
Take Snapshot of each Step, and Submit in Docx file/pdf with one line answer, what you understand here?

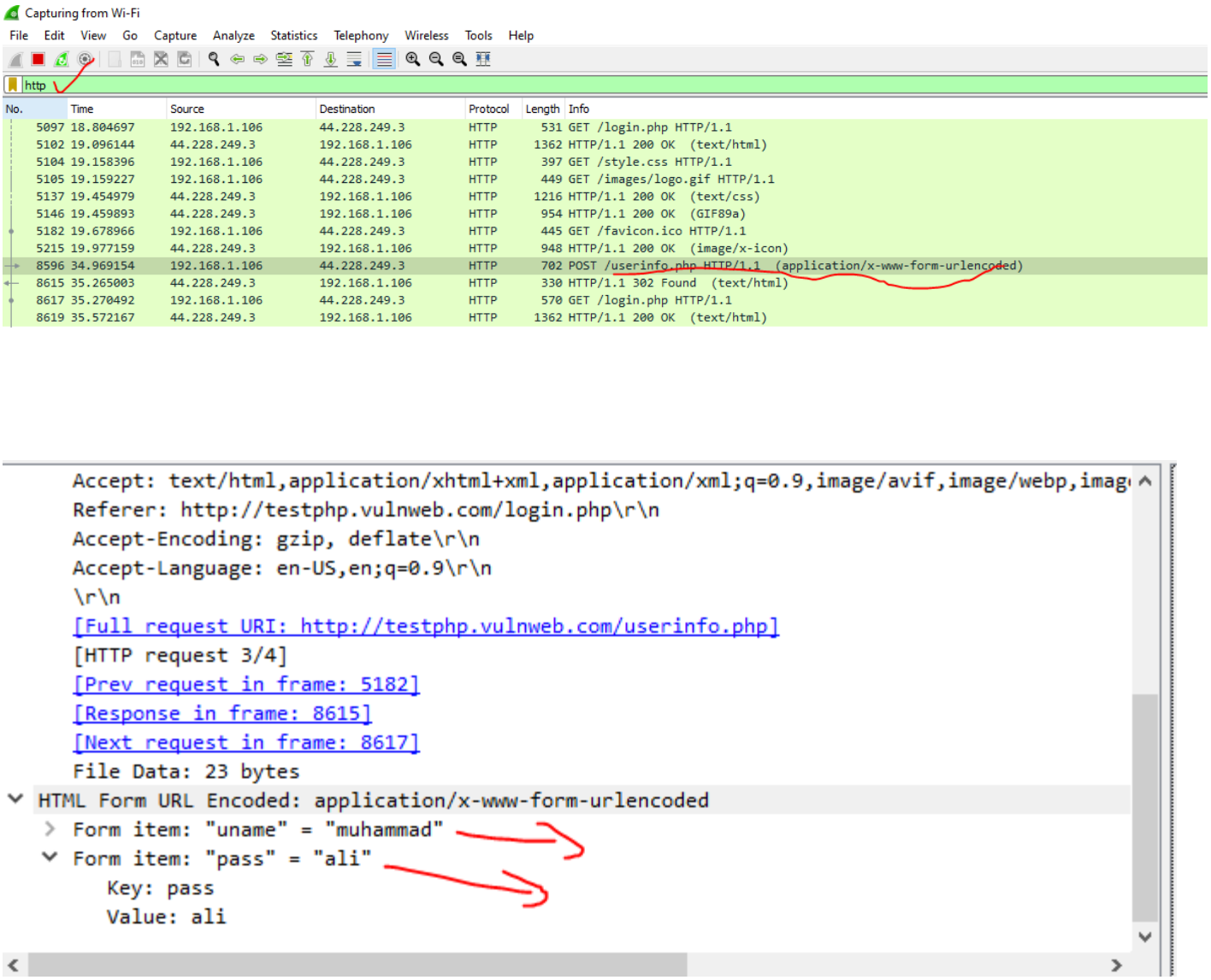

Figure 13 5find the username and password via Wireshark

7. Lab Exercise:

TASK

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?