**Web and Mobile Security (CSP/ITP-338)**

**Exp No: 1**

**Aim:** Open any website on computer system and identify http packet on monitoring tool like Wireshark

**Objective:** To analyse Http traffic

**Introduction:** Wireshark is an open-source packet analyzer, which is used for **education, analysis, software development, communication protocol development, and network troubleshooting**.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a **sniffer, network protocol analyzer, and network analyzer**. It is also used by network security engineers to examine security problems.

Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

**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, 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.
5. Available for UNIX and Windows.
6. Capture live packet data from a network interface.
7. Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
8. Import packets from text files containing hex dumps of packet data.
9. Display packets with very detailed protocol information.

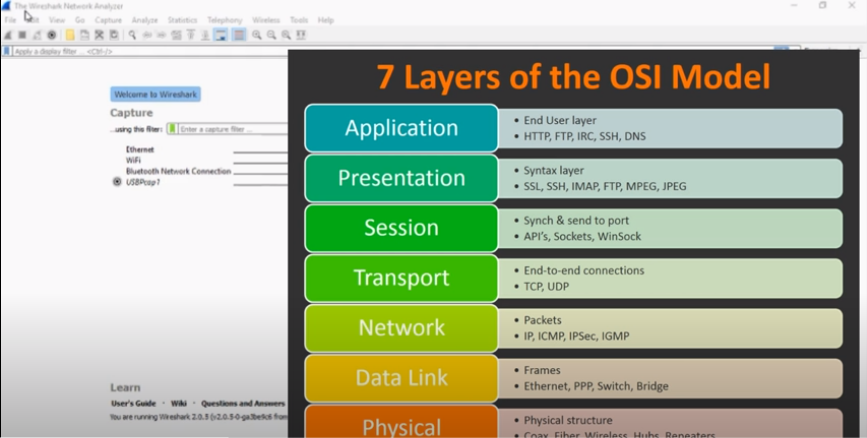
**Purposes**

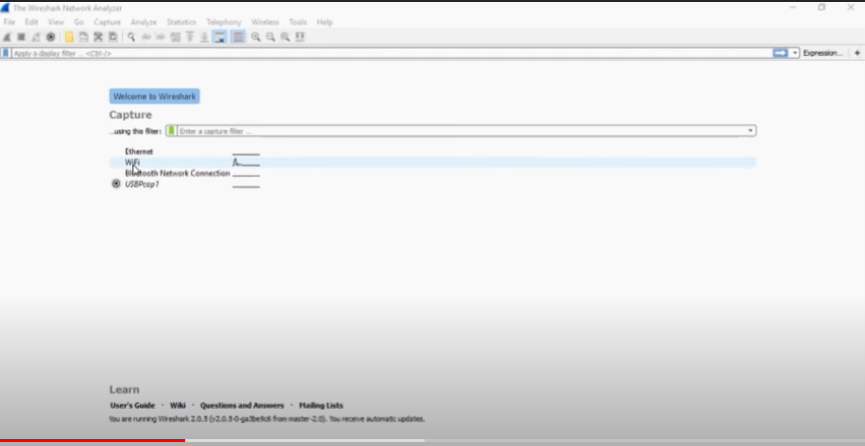
* Network administrators use it to *troubleshoot network problems*
* Network security engineers use it to *examine security problems*
* QA engineers use it to *verify network applications*
* Developers use it to *debug protocol implementations*
* People use it to *learn network protocol* internals

### What Wireshark is not

Here are some things Wireshark does not provide:

* Wireshark isn’t an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn’t allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
* Wireshark will not manipulate things on the network, it will only “measure” things from it. Wireshark doesn’t send packets on the network or do other active things (except domain name resolution, but that can be disabled).



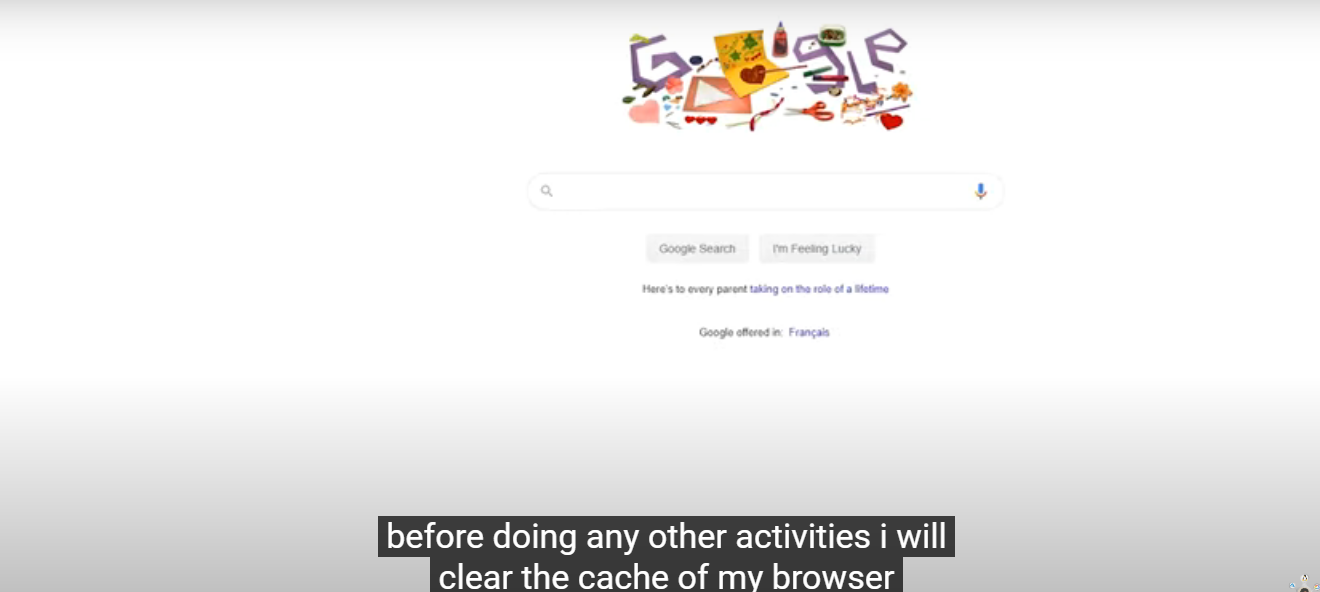


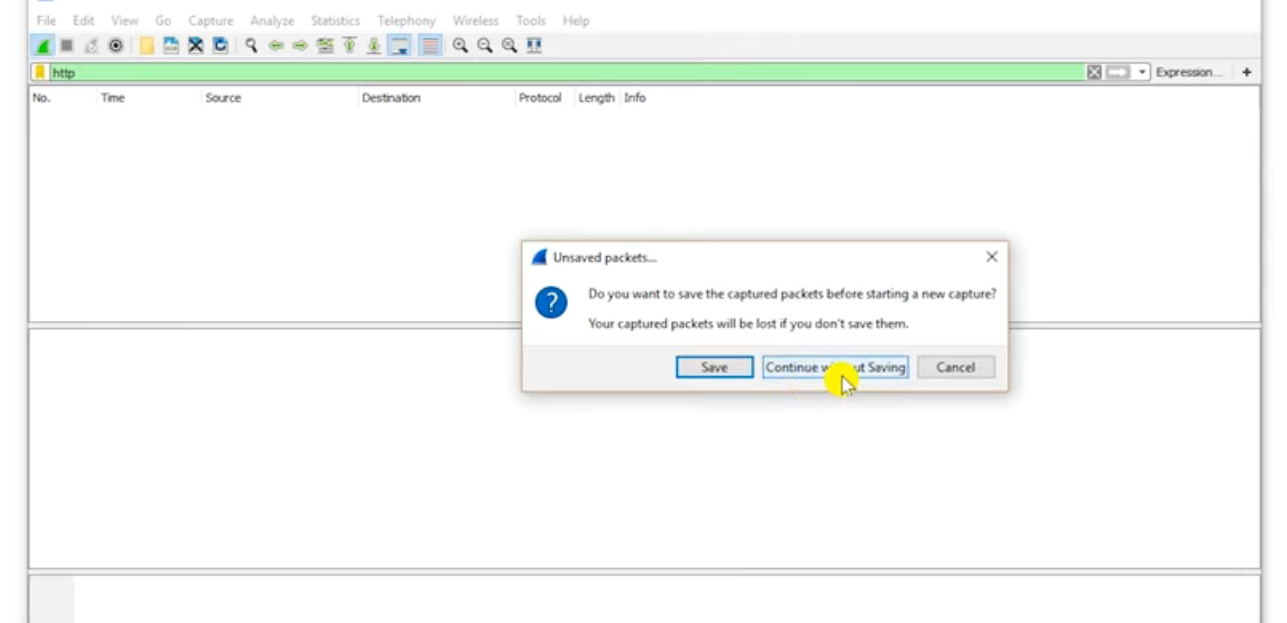
**Steps/Method/Coding:**

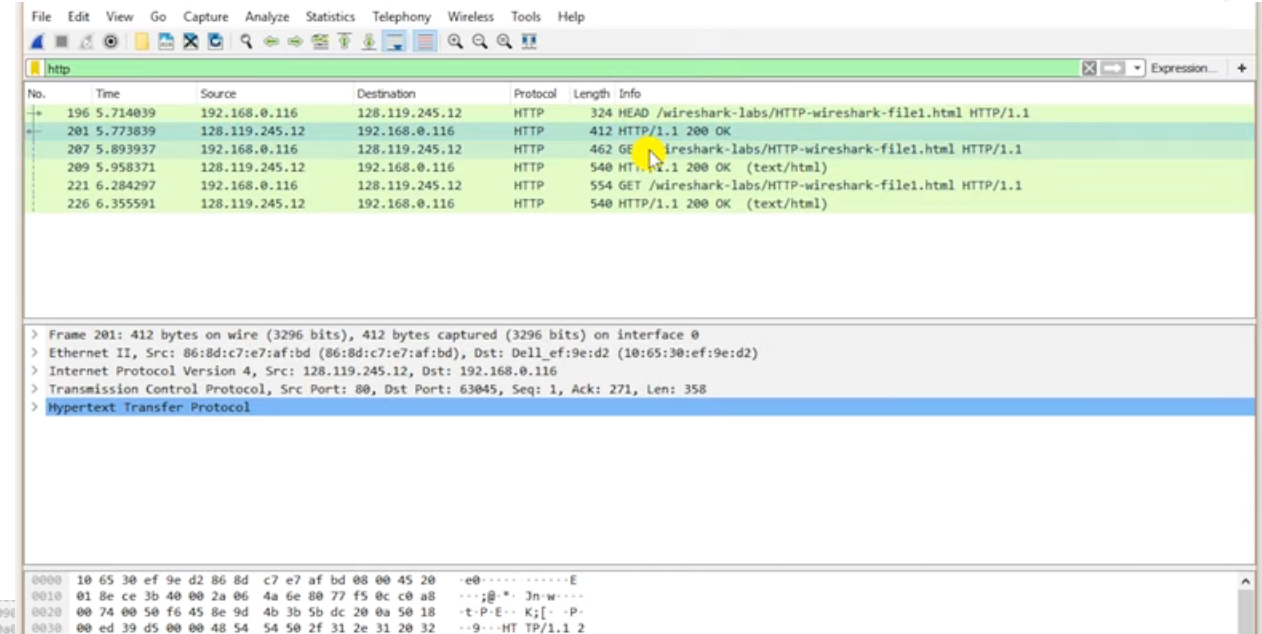
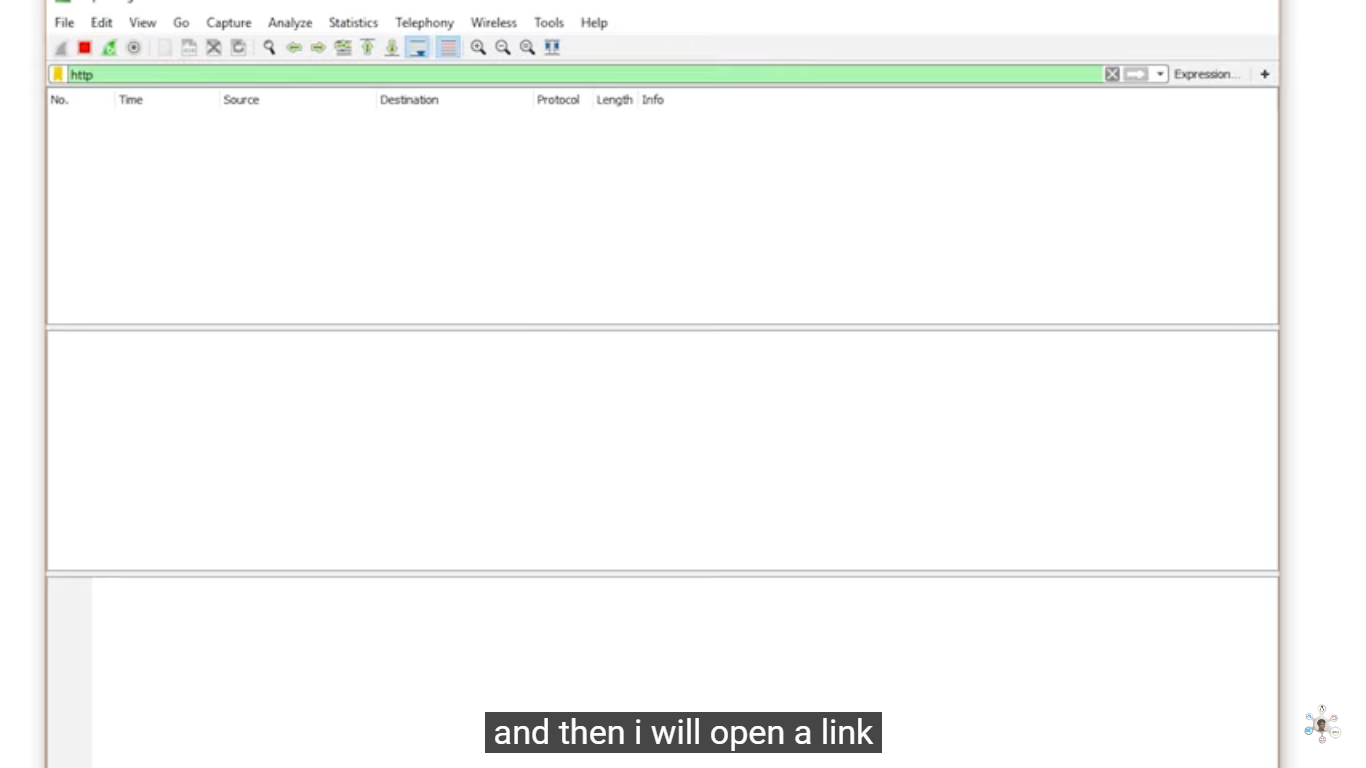
1. [Install Wireshark](http://www.wireshark.org/).
2. Open your Internet browser.
3. Clear your browser cache.
4. Open Wireshark
5. Click on "**Capture** > **Interfaces**". A pop-up window will display.
6. You'll want to capture traffic that goes through your ethernet driver. Click on the **Start** button 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.

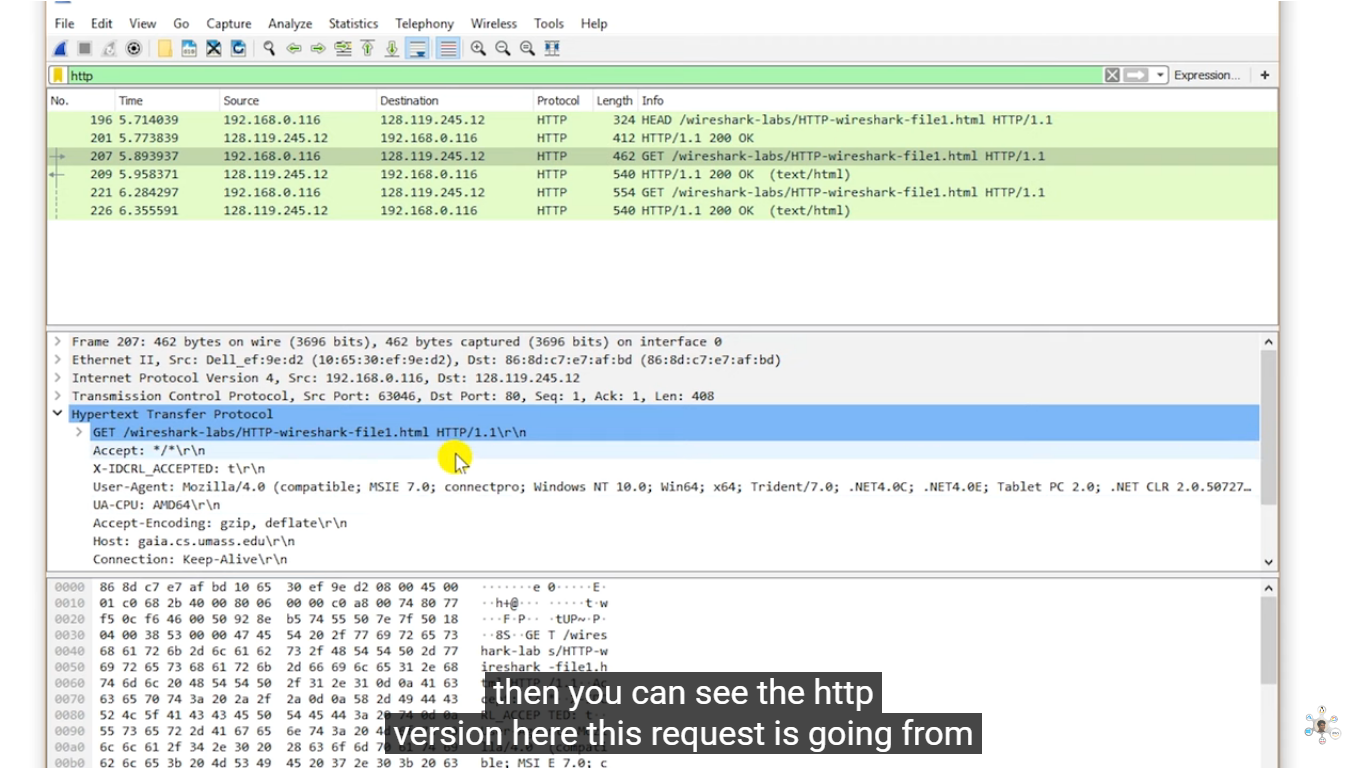
[**https://www.javatpoint.com/wireshark**](https://www.javatpoint.com/wireshark)

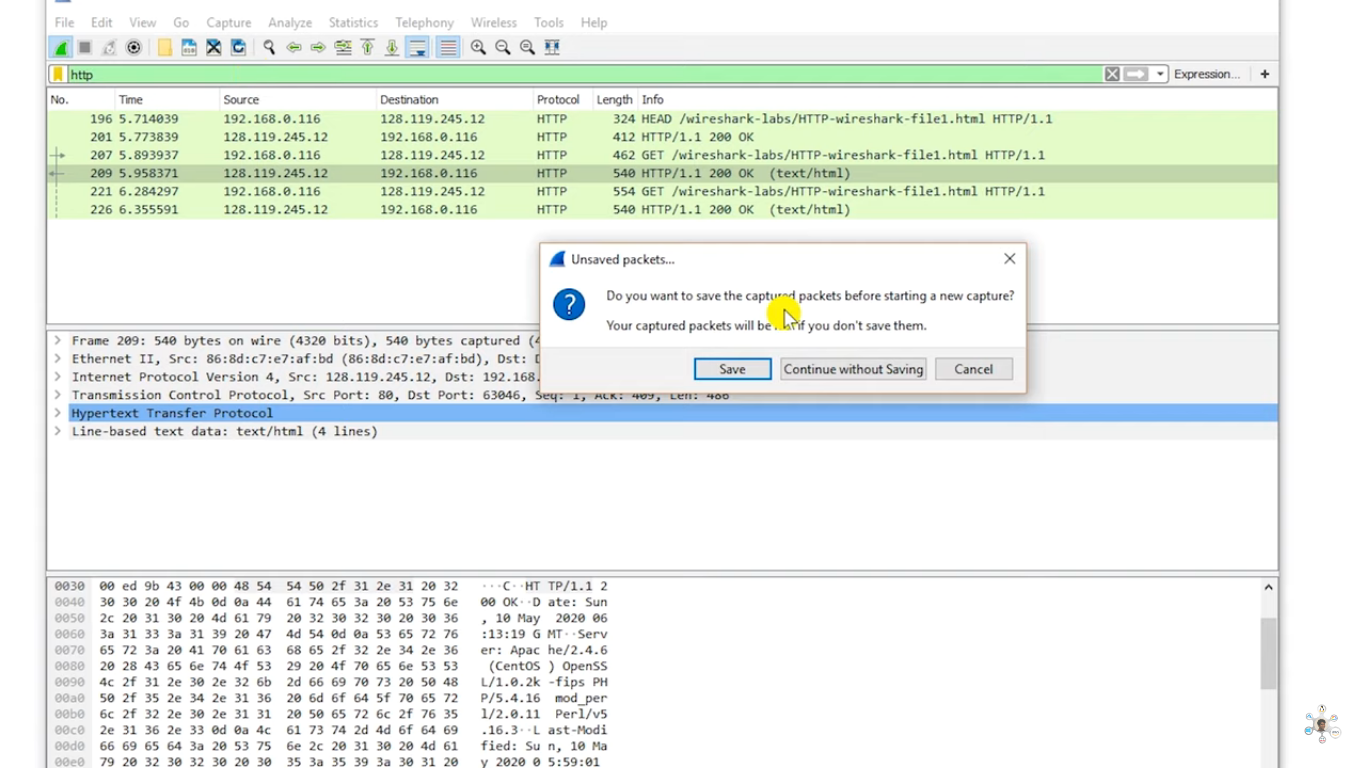
**Output screenshot:**

****

****

****

****

****

**Learning Outcomes:**

Identify requests (from client) and response packets. Find HTTP version, response code/phrase, requested file (including size). 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. Observe how a larger file is sent in multiple segments Observe multi-file (e.g., web page with image) request/response behaviour. Observe request/response behaviour for a page that needs authentication.