**Lab Manual**

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

**Exp No: 1**

**Aim:** Identity Http packet on Wireshark

**Objective:** To analyse 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 networking-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.

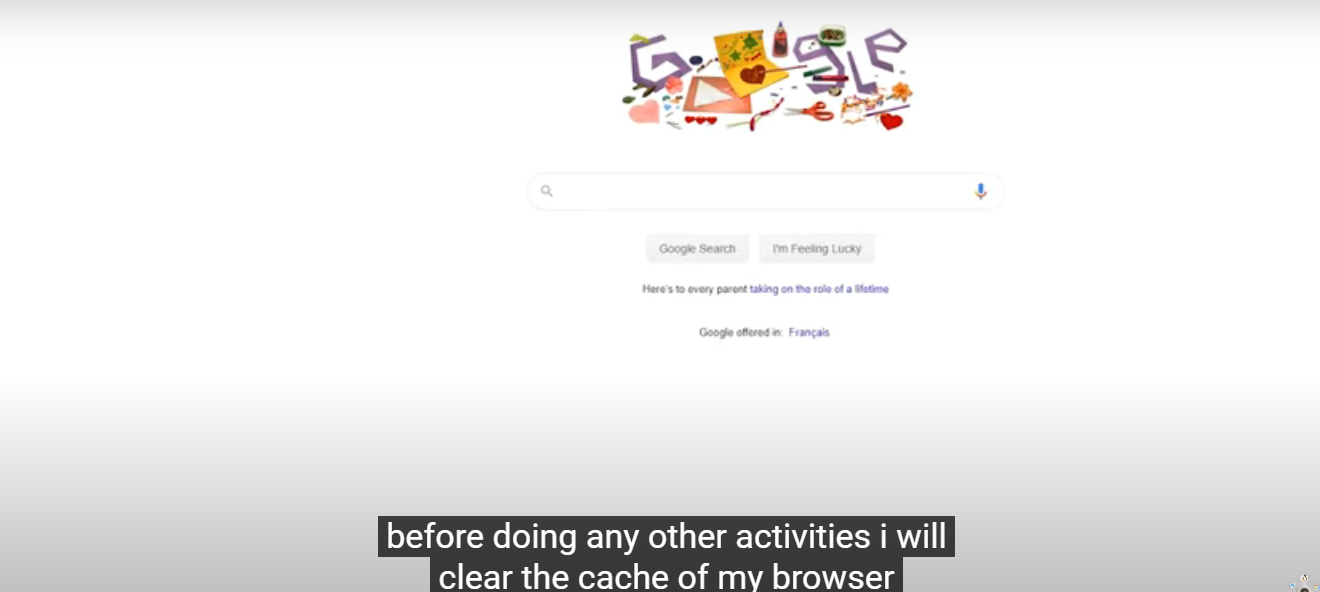
**Reading Material (add reference links along with material):** <https://www.slideshare.net/dgsweigert/wireshark-traffic-analysis>

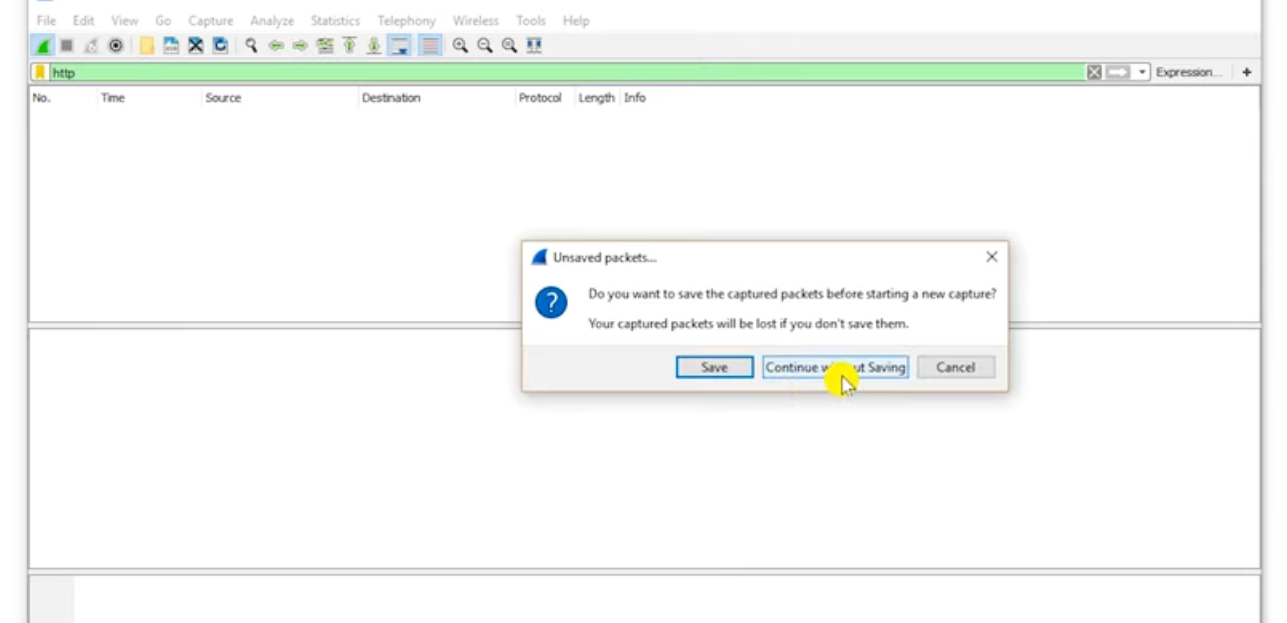
**Steps/Method/Coding:**

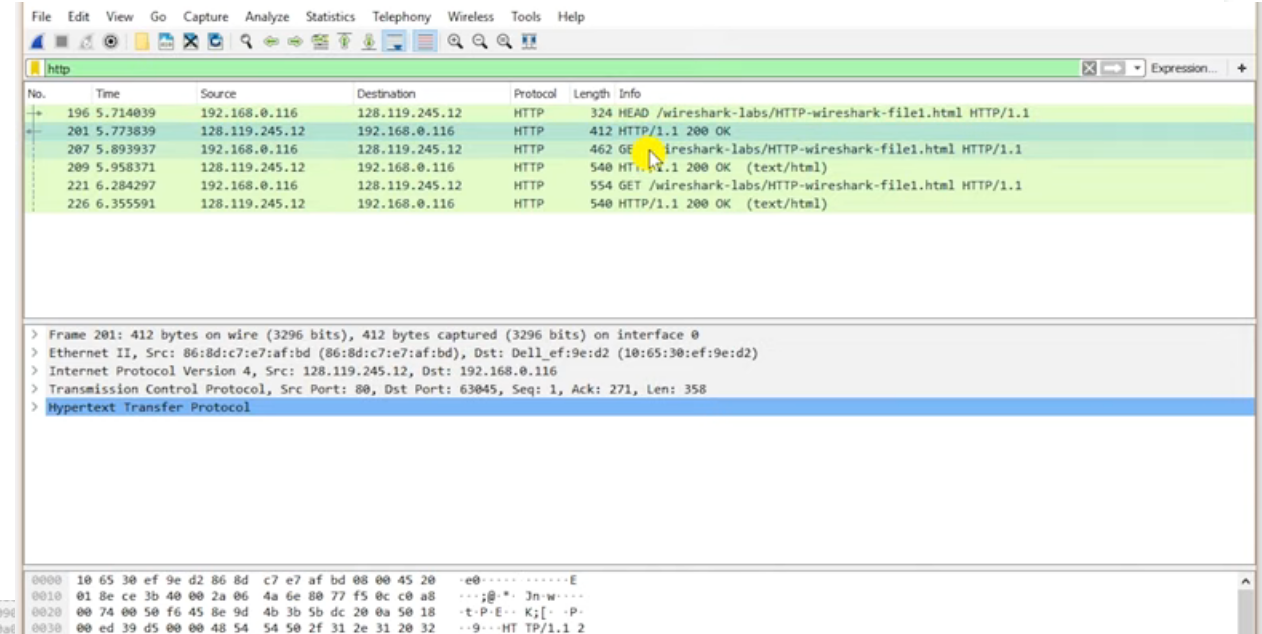
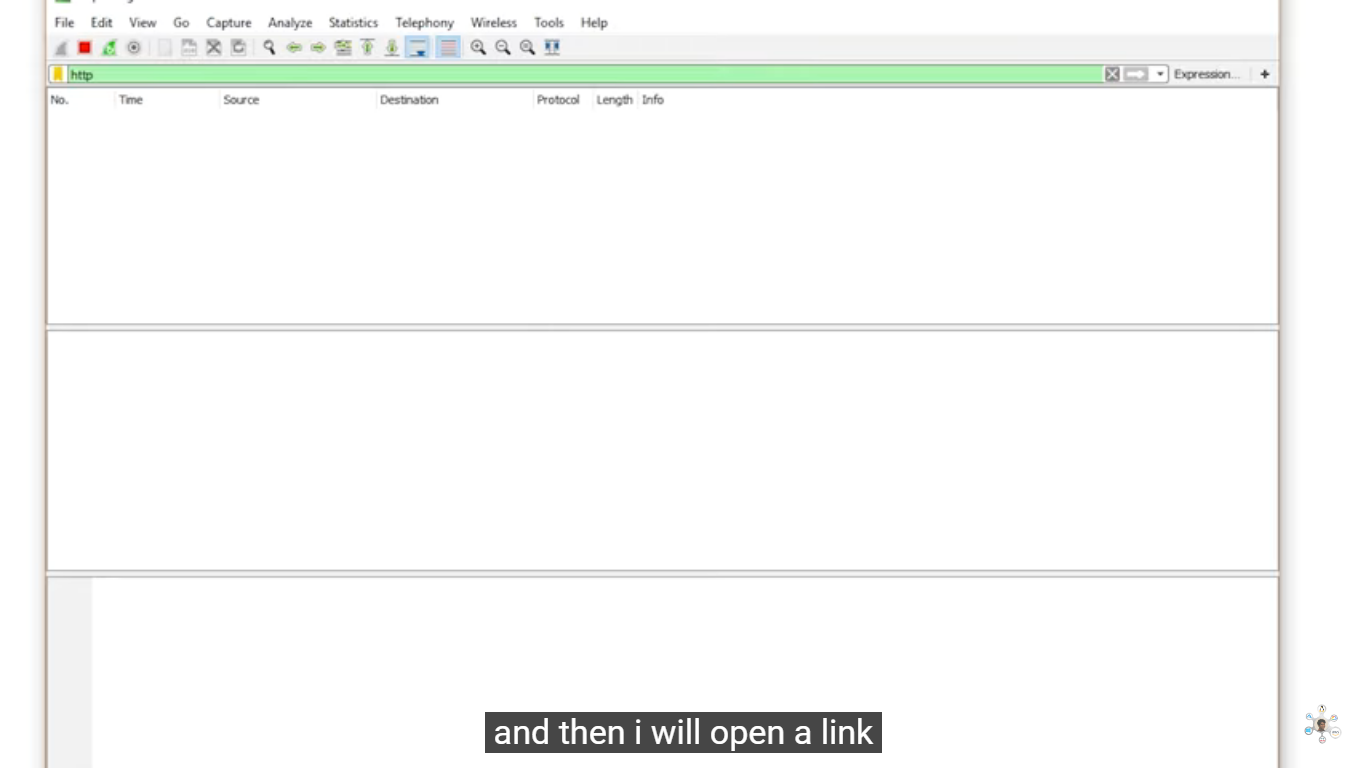
1. [Install Wireshark](http://www.wireshark.org/).
2. Open your Internet browser.
3. Clear your browser cache.
4. Open Wireshark
5. Click on "**Capture** > **Interfaces**". A pop-up window will display.
6. You'll want to capture traffic that goes through your ethernet driver. Click on the **Start** button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

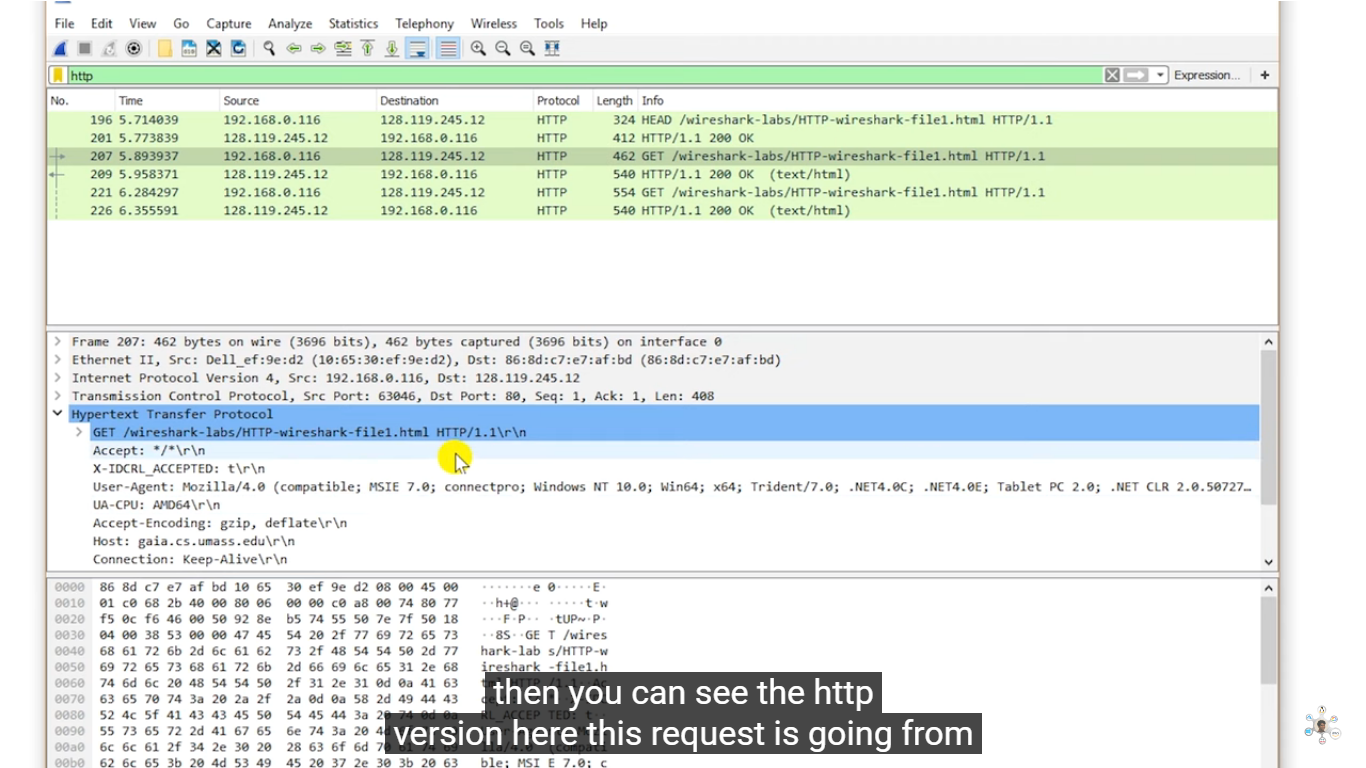
**Output screen +**

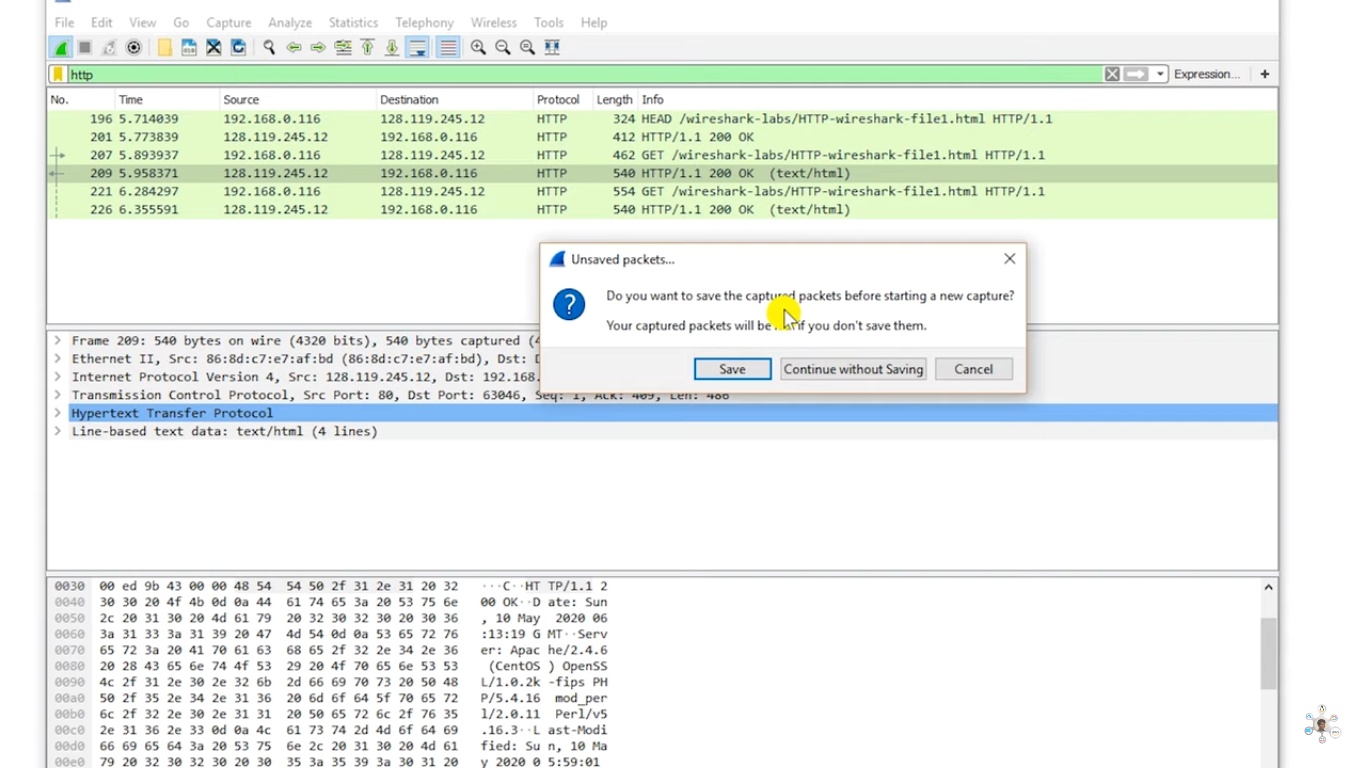
**shot:**

****

****

****

****

****

**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.