

**UNIVERSITY INSTITUTE OF ENGINEERING**

**Department of Computer Science & Engineering**

**Subject Name:** Web and Mobile Security Lab

**Subject Code:** 20CSP-338

**Submitted to: Submitted by:**

Er. Himanshi Name: Sahil Kaundal

UID: 21BCS8197

Section: 616

Group: A

**INDEX**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ex. No** | **List of Experiments** | **Conduct (MM: 12)** | **Viva**  **(MM: 10)** | **Record (MM: 8)** | **Total**  **(MM: 30)** | **Remarks/Signature** |
| 1.1 | Open any website on computer system and identify http packet on monitoring tool like Wireshark. |  |  |  |  |  |
| 1.2 |  |  |  |  |  |  |
| 1.3 |  |  |  |  |  |  |
| 2.1 |  |  |  |  |  |  |
| 2.2 |  |  |  |  |  |  |
| 2.3 |  |  |  |  |  |  |
| 2.4 |  |  |  |  |  |  |
| 3.1 |  |  |  |  |  |  |
| 3.2 |  |  |  |  |  |  |
| 3.3 |  |  |  |  |  |  |

**Experiment 1.1**

**Student Name:** Sahil Kaundal **UID:** 21BCS8197

**Branch:** BE CSE (Lateral Entry) **Section/Group:** 616/A

**Semester:** 5th **Date of Performance:** 22/08/2022

**Subject Name:** WMS Lab **Subject Code:** 20CSP-338

1. **Aim/Overview of the practical:**

Open any website on computer system and identify http packet on monitoring tool like Wireshark.

1. **Task to be done/ Which logistics used:**

To analyze Http traffic.

**3. Apparatus / Simulator Used:**

* Windows 7 & above version.

**Tools to be used:**

* Wireshark Packet Sniffer and Packet Capture Library
* Microsoft Word.
* 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 network in related professional.

**There are many reasons why Wireshark is so popular:**

* It has a great GUI as well as a conventional CLI (T Shark).
* It offers network monitoring on almost all types of network standards (ethernet, W-LAN, Bluetooth etc.)
* It is open-source with a large community of backers and developers.
* All the necessary components for monitoring, analyzing and documenting the network traffic are present. It is free to use.
* Available for UNIX and Windows.
* Capture live packet data from a network interface.
* Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
* Import packets from text files containing hex dumps of packet data.
* 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

* 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).

**4. Program/ Steps/ Method:**

1. Install Wireshark.

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.

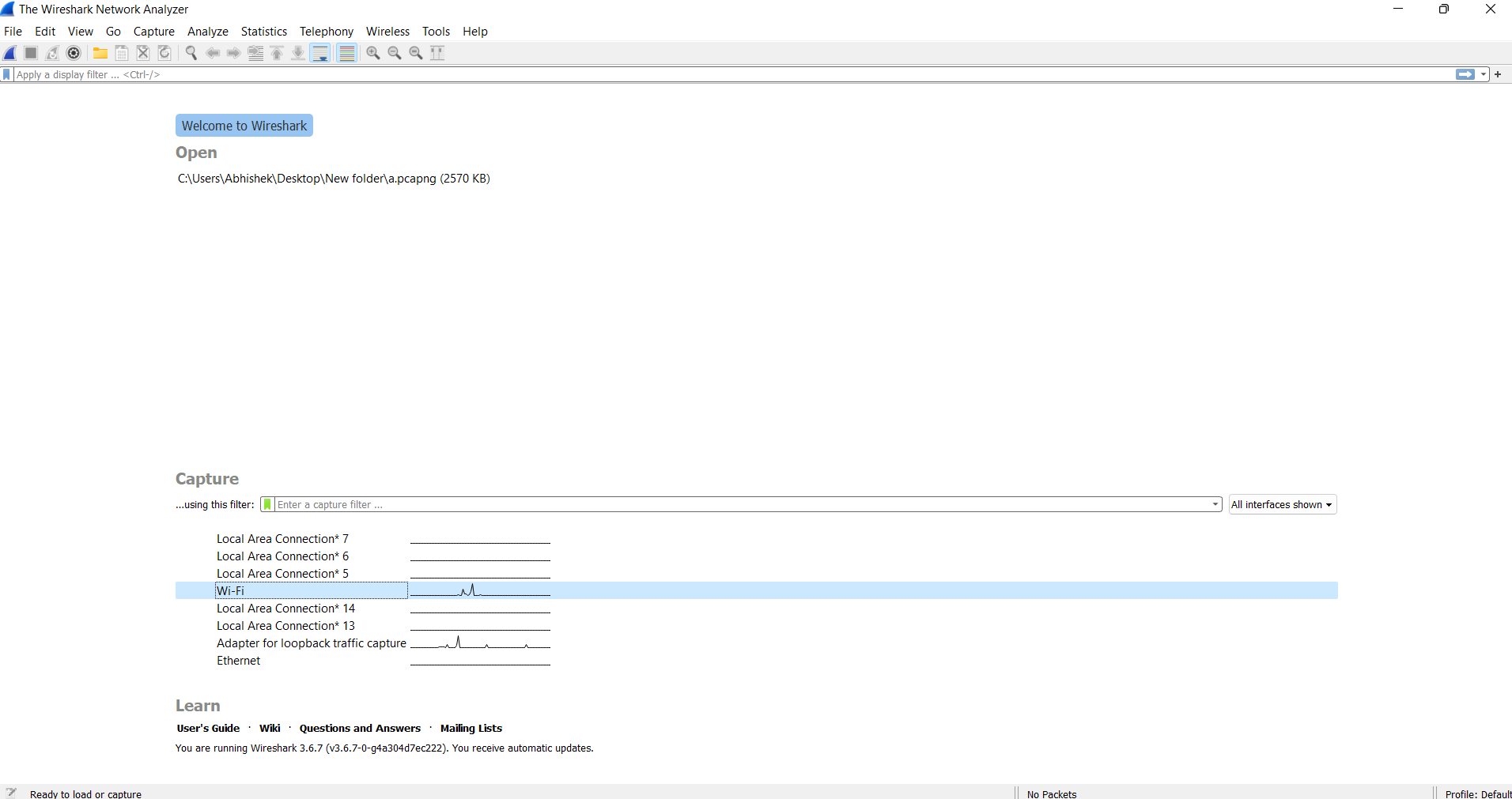
7. Visit the URL that you wanted to capture the traffic from.

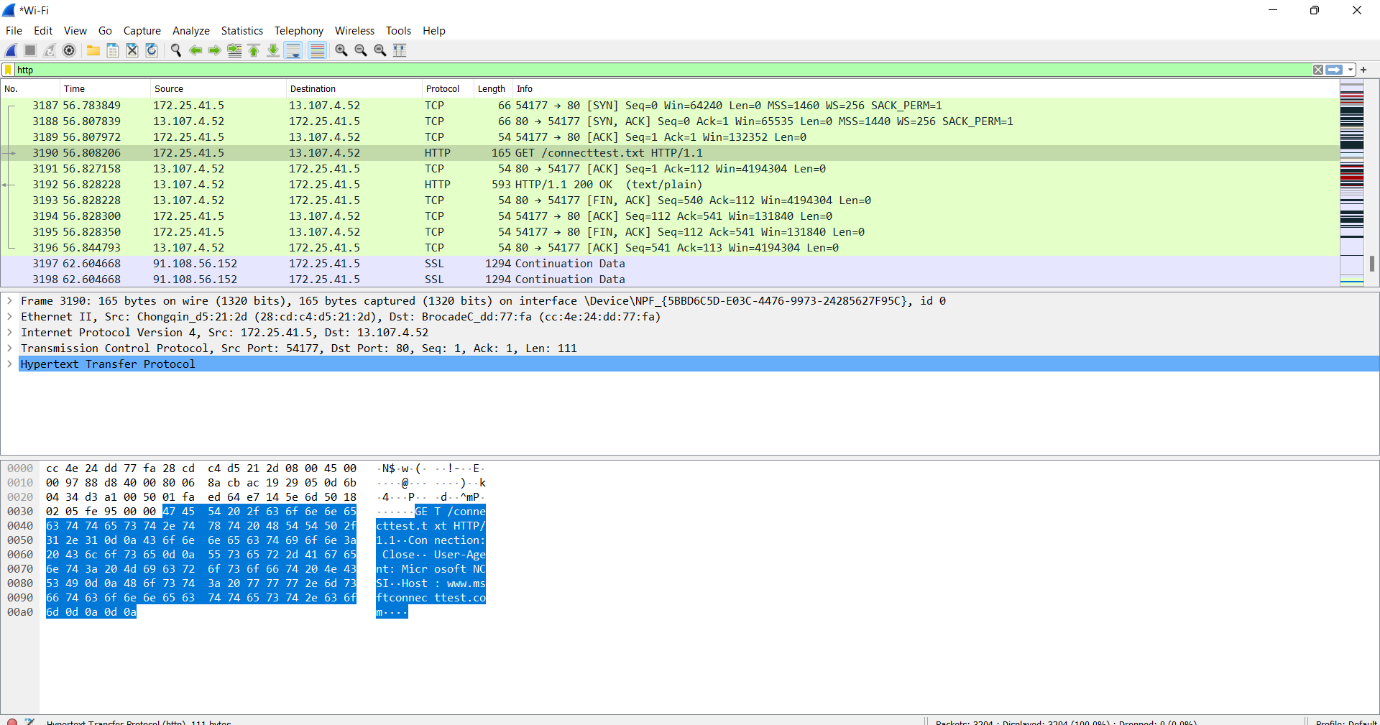
8. Go back to your Wireshark screen and press Ctrl + E to stop capturing.

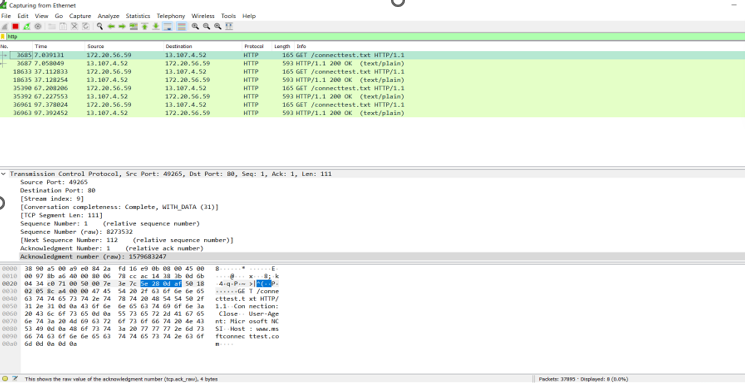
9. After the traffic capture is stopped, please save the captured traffic into

a \*.pcap format file and attach it to your support ticket.

**5. DBMS script/Result/Output/Writing Summary:**





****

**Learning outcomes (What I have learnt):**

1. Open any website on computer system and identify http packet on monitoring tool like Wireshark.
2. 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.

**Evaluation Grid (To be created as per the SOP and Assessment guidelines by the faculty):**

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No. | Parameters | Marks Obtained | Maximum Marks |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
|  |  |  |  |