Computer Networks Laboratory

IT 3095

Lab instructions
On

Introduction to Wireshark Protocol Analyzer and exploring its features

Part- B

Objective: To explore various applications of HTTP protocols in getting, storing and modifying a file, and their analysis using Wireshark protocol analyzer.

Software Required: Wireshark Protocol Analyzer

Procedure:

GET request and response message in HTTP

- Close all web browsers and clear the cache first. Start any browser which you rarely used such as Firefox.
- Open Wireshark and start capturing packets on your Wi-Fi interface or Ethernet (if you are using wired LAN).
- Visit a few websites from your browser which is not using **https**. If a website uses https then http filter will not work. In this case, tls filter will work.
- Stop the capture.
- Notice that thousands of packets are captured. Apply a http filter to inspect the HTTP request and response.
- To see the http packest from your computer, in use **ip.addr = = your IP address && http** to display only the http packets going to and coming from your computer**.** For e.g., **ip.addr == 10.2.110.29 && http** will display only http packets going from and coming to **10.2.110.29.**
- Observer request message in terms of method, url, version, header line, and body.
- Observe response message in terms of version, status code, phrase, header lines, and body.

POST request and response message in HTTP

- Stop Wireshark. Now, clear the browser cache and close the browser.
- Open the Wireshark again. Capture the interface.
- Now open the browser again and search a few non https sites.
- Now open a google form and fill some details.
- Then stop the Wireshark.
- You can use the filter as done previously.
- Observe OCSP protocol and analyze the HTTP request and response in this case.
- Observer request message in terms of method, url, version, header line, and body.
- Observe response message in terms of version, status code, phrase, header lines, and body.

Observations: (Take Screen-shorts for putting Outputs in the Record)

- Take a screenshot of Wireshark for HTTP GET request showing all three panes.
- Take a screenshot of Wireshark for HTTP GET response showing all three panes.
- Take a screenshot of Wireshark for HTTP POST request (captured through **OCSP**) showing all three panes.
- Take a screenshot of Wireshark for HTTP POST response (captured through **OCSP**) showing all three panes.

Note: *Pane 3 can be viewed either in the* ***packet diagram*** *or* ***packet bytes*** *view.*

Conclusion: After the experiment, you must be able to write a conclusion in your own words. The conclusion may be based on the following observations: how to analyze HTTP protocols when accessing a file, modifying a file, etc. What is the different between request and response HTTP packets when accessing a file and when modifying a file?.

Outcomes:

- Students are now expected to be proficient with basic usage of Wireshark.
- They can demonstrate, in Wireshark, how to locate HTTP messages and header information in requests and responses.
- They must also be able to answer the difference between http and https.

***