

## Perform Network Analysis using Wireshark tool.

**Exercise 1:** Capture HTTP traffic using Wireshark to identify following information in the HTTP GET requests:

- a) Host
- b) User-Agent
- c) Source address and Destination address
- d) Source port and Destination port

### Method:

Step 1: Start Wireshark and begin capturing traffic on your network interface.

Step 2: Visit the websites that use HTTP; <http://naverssl.com>.

Step 3: Stop capturing after perform enough capturing.

Step 4: Apply the filter '**http**' to view only HTTP traffic.

Step 5: Identify the corresponding HTTP GET request and double click.

Step 6: Find out the required information.

**Exercise 2:** Analyse network traffic to identify any unencrypted data transfer in HTTP POST requests. Display the following information as out puts:

- a) Host
- b) User Agent
- c) Source address and Destination address
- d) User name
- e) Password

### Method:

Step 1: Start Wireshark and begin capturing traffic on your network interface.

Step 2: Visit the websites that use HTTP; <http://testphp.vulnweb.com>.

Step 3: Enter user name and password and click login button.

Step 4: Stop capturing.

Step 5: Apply the filter '**http**' to view only HTTP traffic.

Step 6: Identify the corresponding HTTP POST request and double click.

Step 6: Find out the required information.

**Exercise 3:** Create a new filter buttons with following display filters:

- a) tcp.port==80
- b) !(arp or stp or lldp or cdp)