VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

CSE3501 INFORMATION SECURITY ANALYSIS AND AUDIT
EXERCISE - 1

DATE: 16.07.2020

Implement the following in Wireshark:

1. Wireshark Download, Installation and Configuration
2. Wireshark Tool Functionality understanding
   a. Interfaces
   b. Packet capture – Browser instance
   c. Analysis
   d. Network Flow : TCP/UDP Stream follow
   e. Packet Filter
   f. Statistics – I/O Graph
   g. Color coding
3. Answer the following:
   a. If a packet is highlighted by black, what does it mean for the packet?
   b. What is the filter command for listing all outgoing http traffic?
   c. Why does DNS use Follow UDP Stream while HTTP use Follow TCP Stream?
   d. Differentiate http and https traffic.

Note :

- In a word document, mention step by step procedure and show the screen shot for each step output.
- The IP address of your machine has to appear (ipconfig command) in each screen shot (For reliability)