**Terna Engineering College**

**Computer Engineering Department**

Program: Sem VII

[**Course: MOBILE COMMUNICATION & COMPUTING AND MOBILE APPLICATION DEVELOPMENT LAB (MCC & MAD Lab)**](https://github.com/Amey-Thakur/MOBILE-COMMUNICATION-AND-COMPUTING-AND-MOBILE-APPLICATION-DEVELOPMENT-LAB)

**Experiment No. 07**

**PART B**

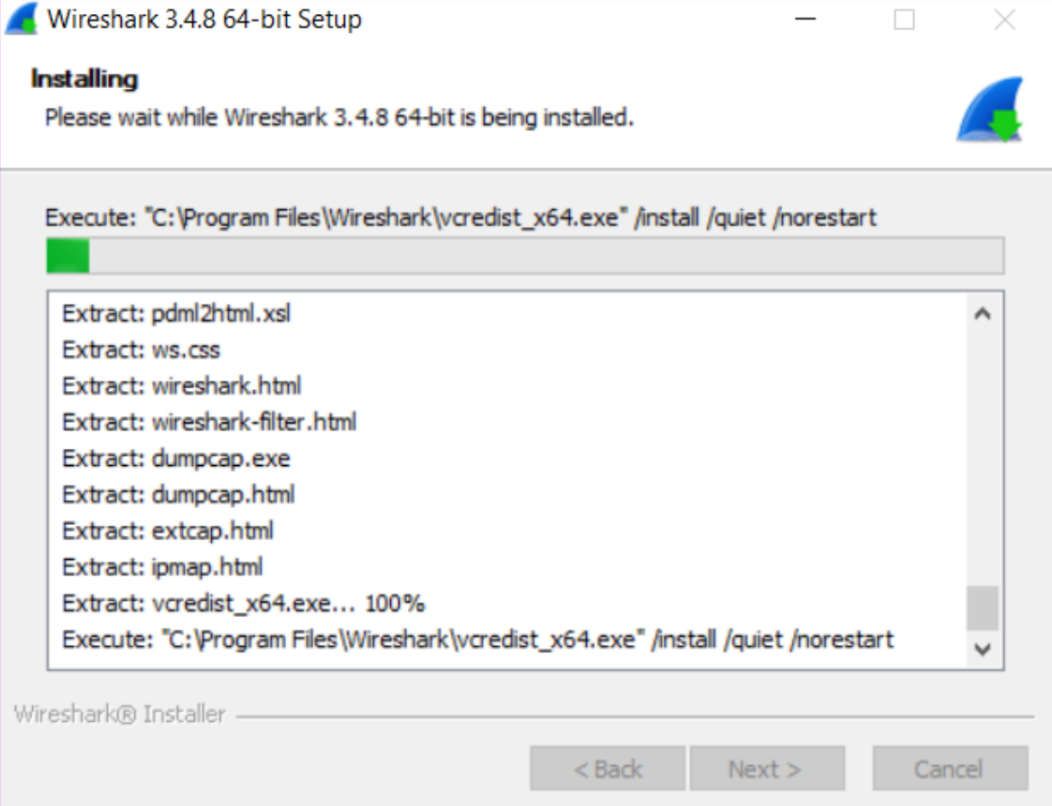
**(PART B: TO BE COMPLETED BY STUDENTS)**

***(Students must submit the soft copy as per the following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case there is no Blackboard access available)***

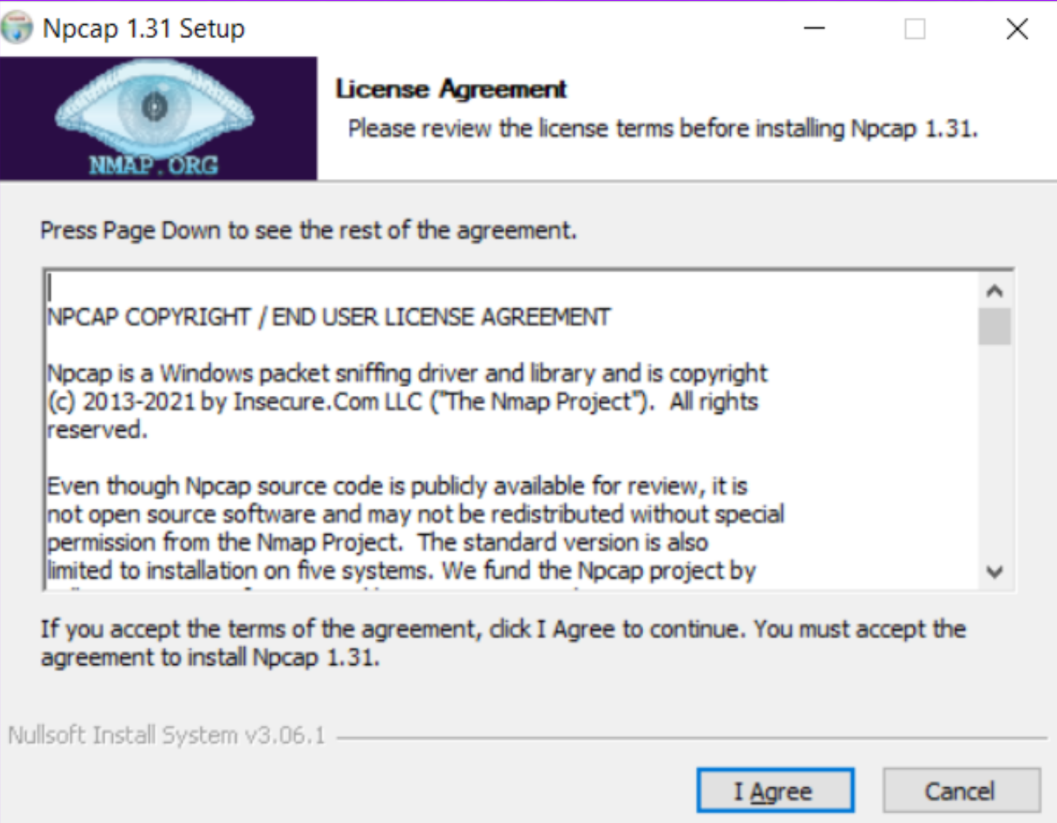
| Roll No. 50 | Name: AMEY THAKUR |
| --- | --- |
| Class: BE-COMPS-50 | Batch: B3 |
| Date of Experiment: 17-09-2021 | Date of Submission: 17-09-2021 |
| Grade : |  |

**Aim:** Analyze packets using Wireshark.

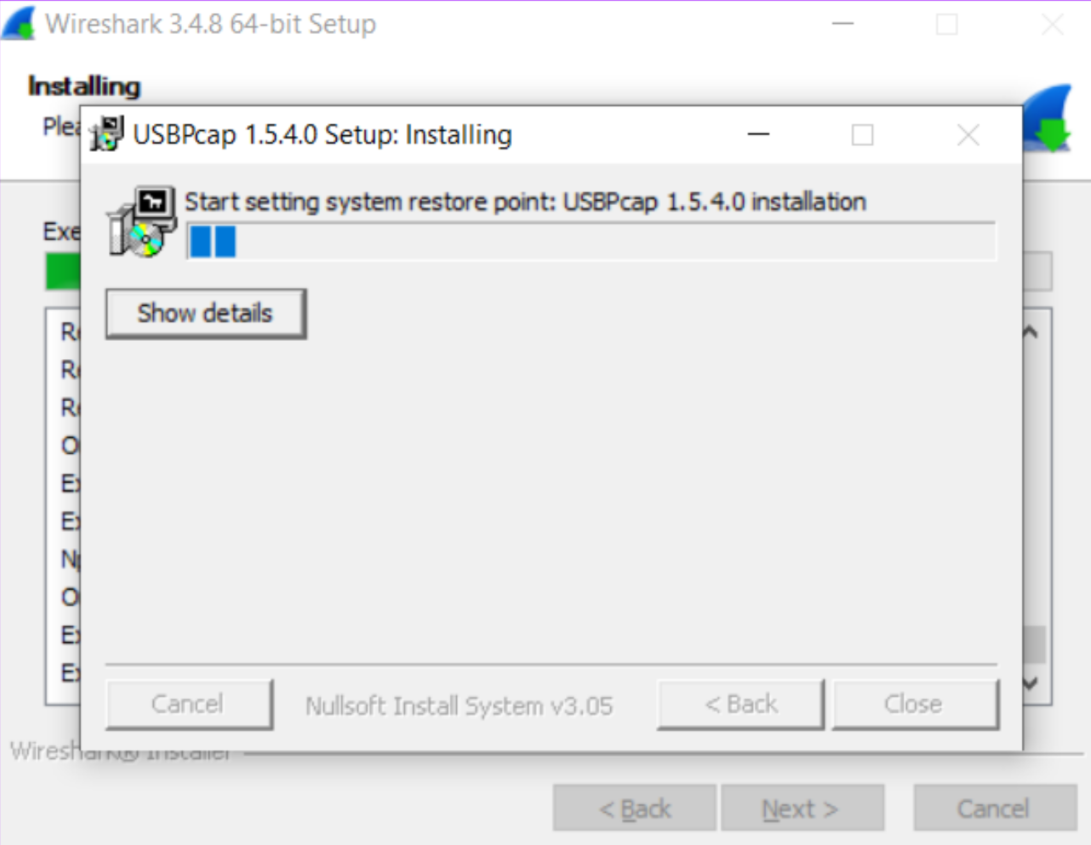
**B.1 Installation Snapshots:**



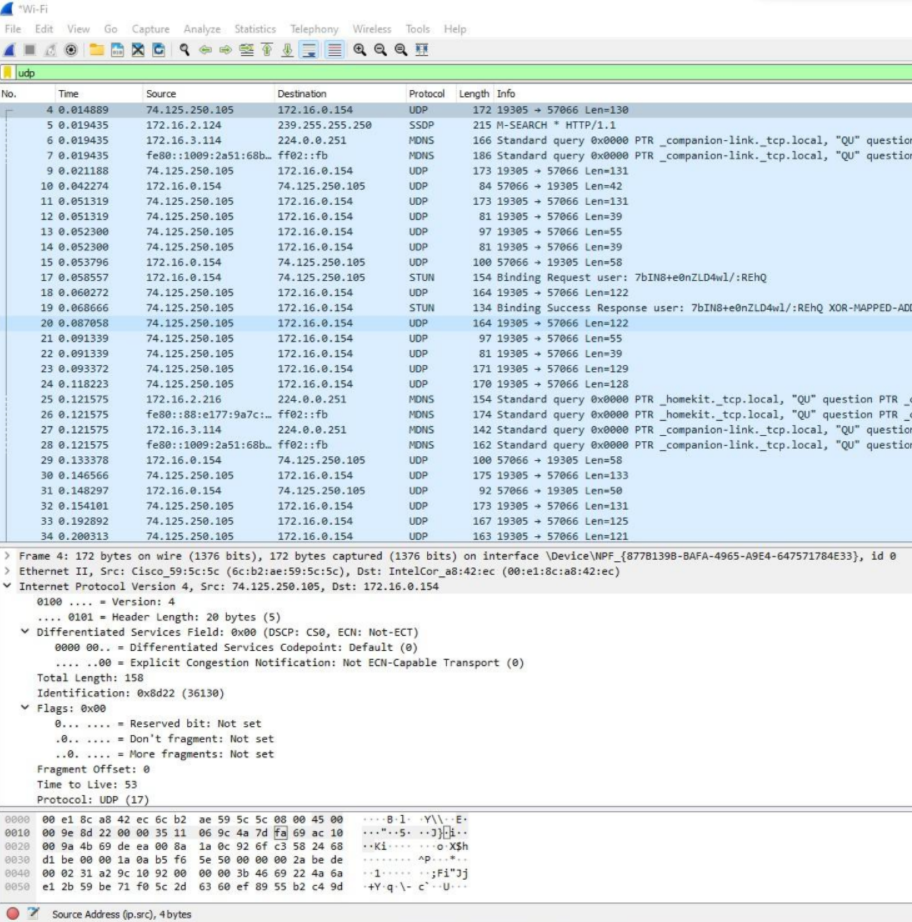
**Installing Npcap**

****

**Installing USBPcap**

****

**Apply different display filters to see specific protocol packets.**

****

**B.2 Conclusion**

Hence we’ve successfully installed Wireshark and analyzed various packets.

**B.3 Question of Curiosity**

1. Explain the procedure to capture packets.

Ans:

* When you open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor. You also have a capture filter field, so you only capture the network traffic you want to see.
* You can select one or more of the network interfaces using “shift left-click.” Once you have the network interface selected, you can start the capture, and there are several ways to do that.
* Click the first button on the toolbar, titled “Start Capturing Packets.”
* You can select the menu item Capture -> Start.
* During the capture, Wireshark will show you the packets that it captures in real-time.
* Once you have captured all the packets you need, you use the same buttons or menu options to stop the capture.

1. Which types of filters did you apply in Wireshark, explain in detail?

Ans:

* One of the best features of Wireshark is the Wireshark Capture Filters and Wireshark Display Filters. Filters allow you to view the capture the way you need to see it so you can troubleshoot the issues at hand.
* Wireshark Capture Filters:

Capture filters limit the captured packets by the filter. Meaning if the packets don’t match the filter, Wireshark won’t save them.

Example: port 53: capture traffic on port 53 only.

* Wireshark Display Filters:

Wireshark Display Filters change the view of the capture during analysis. After you have stopped the packet capture, you use display filters to narrow down the packets in the Packet List so you can troubleshoot your issue.

Example: ip.src==IP-address and ip.dst==IP-address

This filter shows you packets from one computer (ip.src) to another (ip.dst).