Terna Engineering College

Computer Engineering Department

Program: Sem VII

Course: MOBILE COMMUNICATION & COMPUTING AND MOBILE APPLICATION DEVELOPMENT LAB (MCC & MAD Lab)

Experiment No. 07

PART B

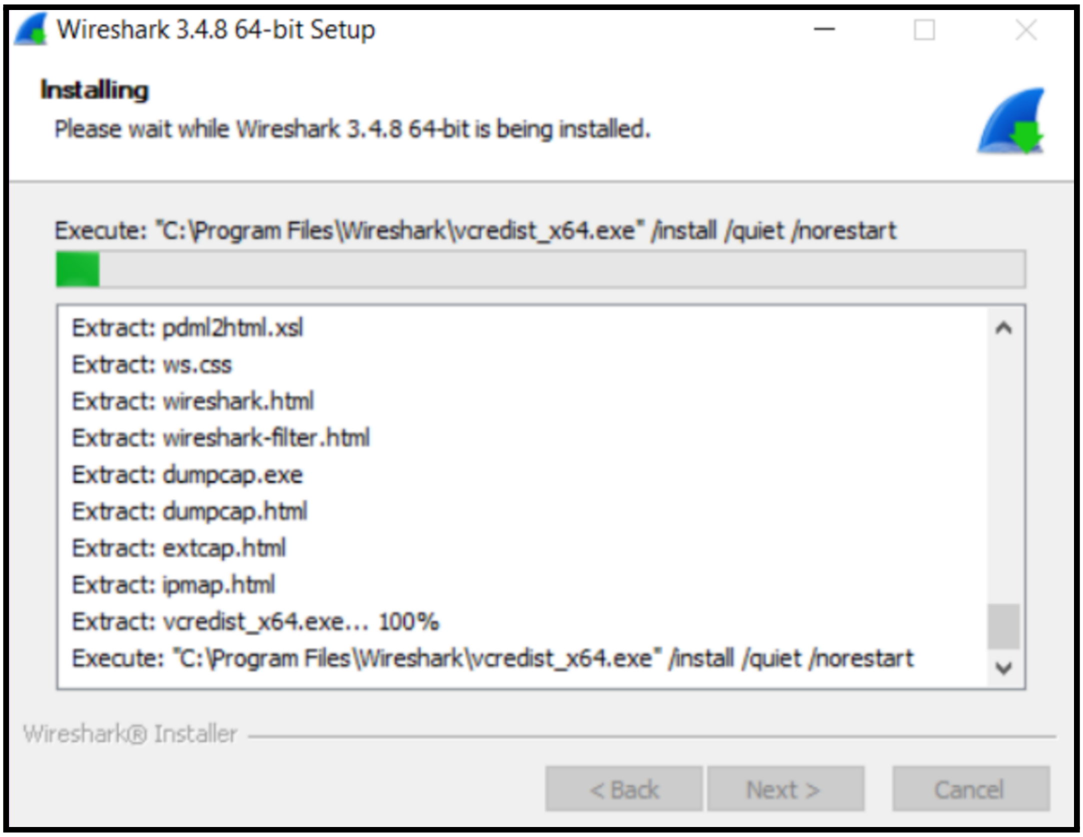
(PART B: TO BE COMPLETED BY STUDENTS)

(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.

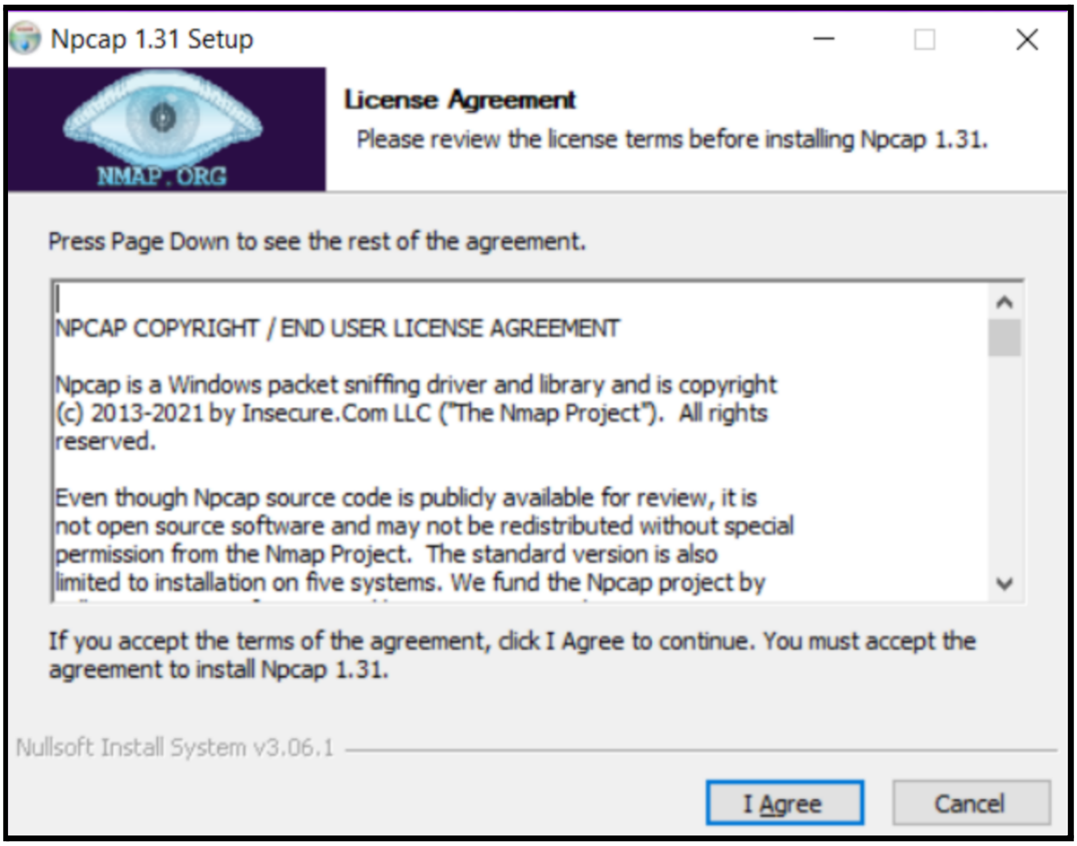
B.1 Installation Snapshots:


Wireshark 3.4.8 64-bit Setup
Installing
Please wait while Wireshark 3.4.8 64-bit is being installed.
Wireshark® Installer
< Back
Next >
Cancel

```
Execute: "C:\Program Files\Wireshark\vcredist_x64.exe" /install /quiet /norestart
```

```
Extract: pdml2html.xsl
Extract: ws.css
Extract: wireshark.html
Extract: wireshark-filter.html
Extract: dumpcap.exe
Extract: dumpcap.html
Extract: extcap.html
Extract: ipmap.html
Extract: vcredist_x64.exe... 100%
Execute: "C:\Program Files\Wireshark\vcredist_x64.exe" /install /quiet /norestart
```

Installing Npcap



Npcap 1.31 Setup

License Agreement

Please review the license terms before installing Npcap 1.31.

Press Page Down to see the rest of the agreement.

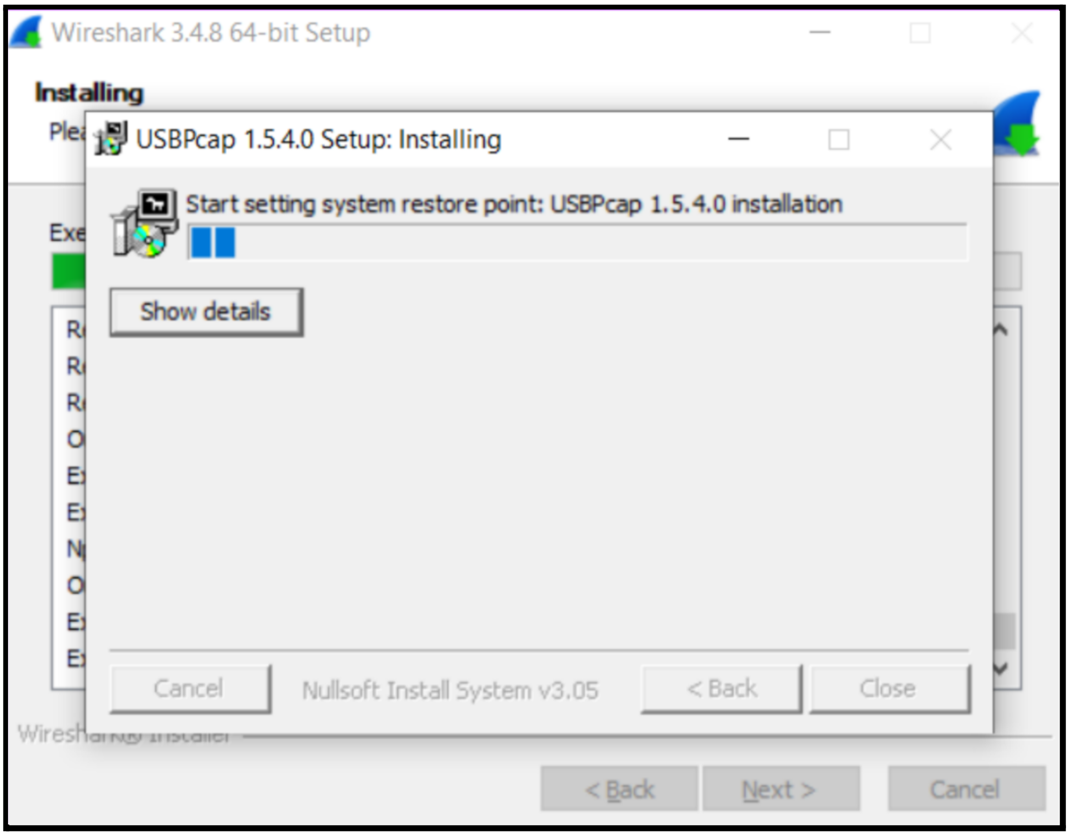
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT

Npcap is a Windows packet sniffing driver and library and is copyright (c) 2013-2021 by Insecure.Com LLC ("The Nmap Project"). All rights reserved.

Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed without special permission from the Nmap Project. The standard version is also limited to installation on five systems. We fund the Npcap project by

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 1.31.

Installing USBPcap



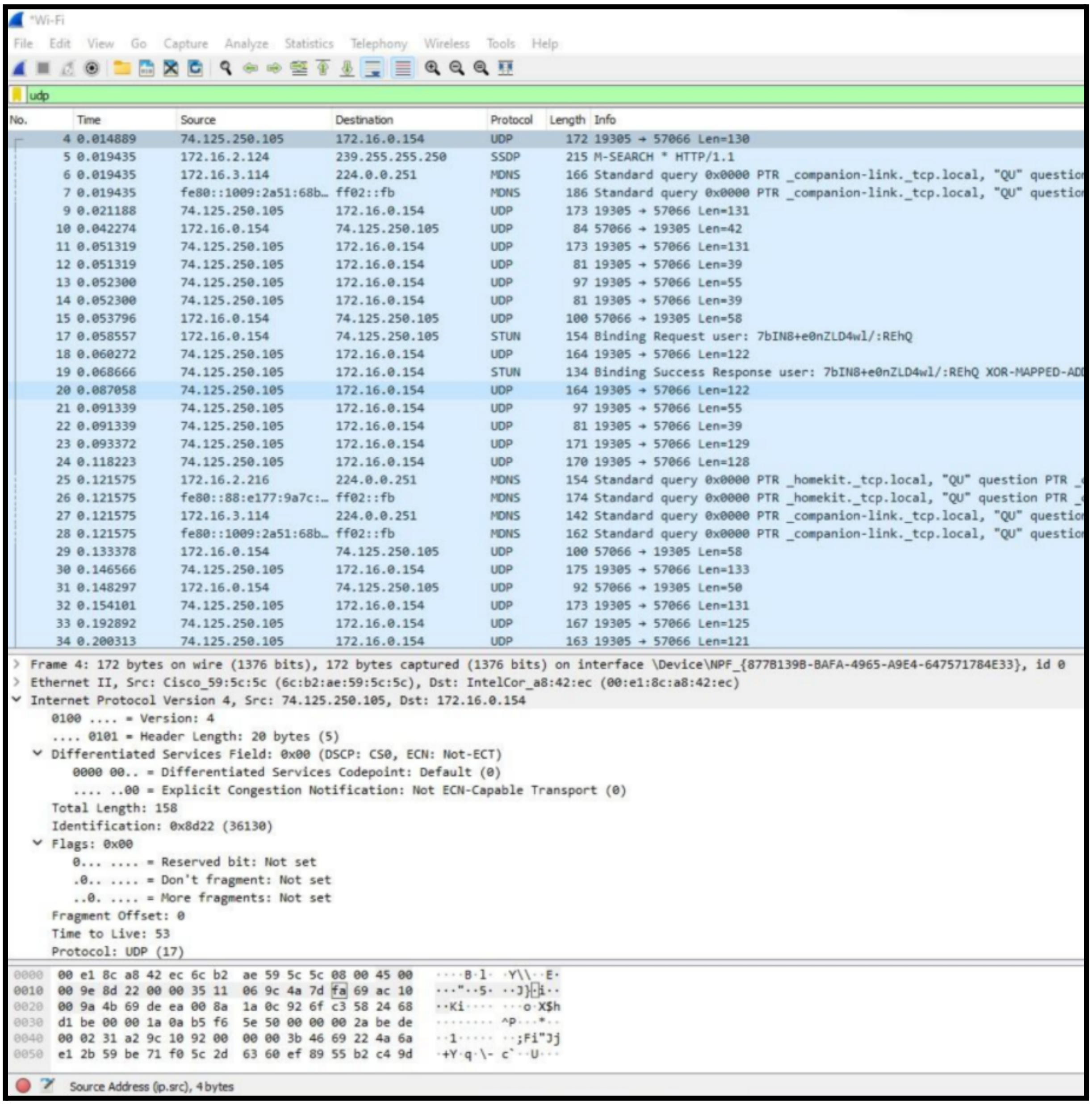
Wireshark 3.4.8 64-bit Setup

Installing

USBPcap 1.5.4.0 Setup: Installing

Start setting system restore point: USBPcap 1.5.4.0 installation

Apply different display filters to see specific protocol packets.



udp

```
No.    Time      Source                 Destination      Protocol Length Info
     4 0.014889  74.125.250.105         172.16.0.154     UDP      172 19305 → 57066 Len=130
     5 0.019435  172.16.2.124           239.255.255.250  SSDP     215 M-SEARCH * HTTP/1.1
     6 0.019435  172.16.3.114           224.0.0.251      MDNS     166 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" questio
     7 0.019435  fe80::1009:2a51:68b…   ff02::fb         MDNS     186 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" questio
     9 0.021188  74.125.250.105         172.16.0.154     UDP      173 19305 → 57066 Len=131
    10 0.042274  172.16.0.154           74.125.250.105   UDP       84 57066 → 19305 Len=42
    11 0.051319  74.125.250.105         172.16.0.154     UDP      173 19305 → 57066 Len=131
    12 0.051319  74.125.250.105         172.16.0.154     UDP       81 19305 → 57066 Len=39
    13 0.052300  74.125.250.105         172.16.0.154     UDP       97 19305 → 57066 Len=55
    14 0.052300  74.125.250.105         172.16.0.154     UDP       81 19305 → 57066 Len=39
    15 0.053796  172.16.0.154           74.125.250.105   UDP      100 57066 → 19305 Len=58
    17 0.058557  172.16.0.154           74.125.250.105   STUN     154 Binding Request user: 7bIN8+e0nZLD4wl/:REhQ
    18 0.060272  74.125.250.105         172.16.0.154     UDP      164 19305 → 57066 Len=122
    19 0.068666  74.125.250.105         172.16.0.154     STUN     134 Binding Success Response user: 7bIN8+e0nZLD4wl/:REhQ XOR-MAPPED-AD
    20 0.087058  74.125.250.105         172.16.0.154     UDP      164 19305 → 57066 Len=122
    21 0.091339  74.125.250.105         172.16.0.154     UDP       97 19305 → 57066 Len=55
    22 0.091339  74.125.250.105         172.16.0.154     UDP       81 19305 → 57066 Len=39
    23 0.093372  74.125.250.105         172.16.0.154     UDP      171 19305 → 57066 Len=129
    24 0.118223  74.125.250.105         172.16.0.154     UDP      170 19305 → 57066 Len=128
    25 0.121575  172.16.2.216           224.0.0.251      MDNS     154 Standard query 0x0000 PTR _homekit._tcp.local, "QU" question PTR _
    26 0.121575  fe80::88:e177:9a7c:…   ff02::fb         MDNS     174 Standard query 0x0000 PTR _homekit._tcp.local, "QU" question PTR _
    27 0.121575  172.16.3.114           224.0.0.251      MDNS     142 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" questio
    28 0.121575  fe80::1009:2a51:68b…   ff02::fb         MDNS     162 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" questio
    29 0.133378  172.16.0.154           74.125.250.105   UDP      100 57066 → 19305 Len=58
    30 0.146566  74.125.250.105         172.16.0.154     UDP      175 19305 → 57066 Len=133
    31 0.148297  172.16.0.154           74.125.250.105   UDP       92 57066 → 19305 Len=50
    32 0.154101  74.125.250.105         172.16.0.154     UDP      173 19305 → 57066 Len=131
    33 0.192892  74.125.250.105         172.16.0.154     UDP      167 19305 → 57066 Len=125
    34 0.200313  74.125.250.105         172.16.0.154     UDP      163 19305 → 57066 Len=121
```

```
> Frame 4: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface \Device\NPF_{877B139B-BAFA-4965-A9E4-647571784E33}, id 0
> Ethernet II, Src: Cisco_59:5c:5c (6c:b2:ae:59:5c:5c), Dst: IntelCor_a8:42:ec (00:e1:8c:a8:42:ec)
v Internet Protocol Version 4, Src: 74.125.250.105, Dst: 172.16.0.154
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 158
    Identification: 0x8d22 (36130)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 53
    Protocol: UDP (17)
```

```
0000  00 e1 8c a8 42 ec 6c b2  ae 59 5c 5c 08 00 45 00   ····B·l· ·Y\\··E·
0010  00 9e 8d 22 00 00 35 11  06 9c 4a 7d fa 69 ac 10   ···"··5· ··J}·i··
0020  00 9a 4b 69 de ea 00 8a  1a 0c 92 6f c3 58 24 68   ··Ki···· ···o·X$h
0030  d1 be 00 00 1a 0a b5 f6  5e 50 00 00 00 2a be de   ········ ^P···*··
0040  00 02 31 a2 9c 10 92 00  00 00 3b 46 69 22 4a 6a   ··1····· ··;Fi"Jj
0050  e1 2b 59 be 71 f0 5c 2d  63 60 ef 89 55 b2 c4 9d   ·+Y·q·\- c`··U···
```

Source Address (ip.src), 4 bytes

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.

2. 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).