CN LAB ASSIGNMENT : 2

PANCHAL GUNGUN PARESH
U21CS052

Que-1. Packet sniffer and its structure

When any data has to be transmitted over the computer network, it is broken down into smaller units at the sender's node called *data packets* and reassembled at receiver's node in original format. It is the *smallest unit* of communication over a computer network. It is also called a block, a segment, a datagram or a cell. The act of capturing data packet across the computer network is called **packet sniffing**. It is similar to as wire tapping to a telephone network. It is mostly used by *crackers and hackers* to collect information illegally about network. It is also used by *ISPs, advertisers and governments*. **ISPs** use packet sniffing to track all your activities such as:

-
    - what you looked on that website
    - downloads from a sitewho is receiver of your email
- what is content of that email
- what you download
- sites you visit
    - streaming events like video, audio, etc.

Advertising agencies or internet advertising agencies are paid according to:

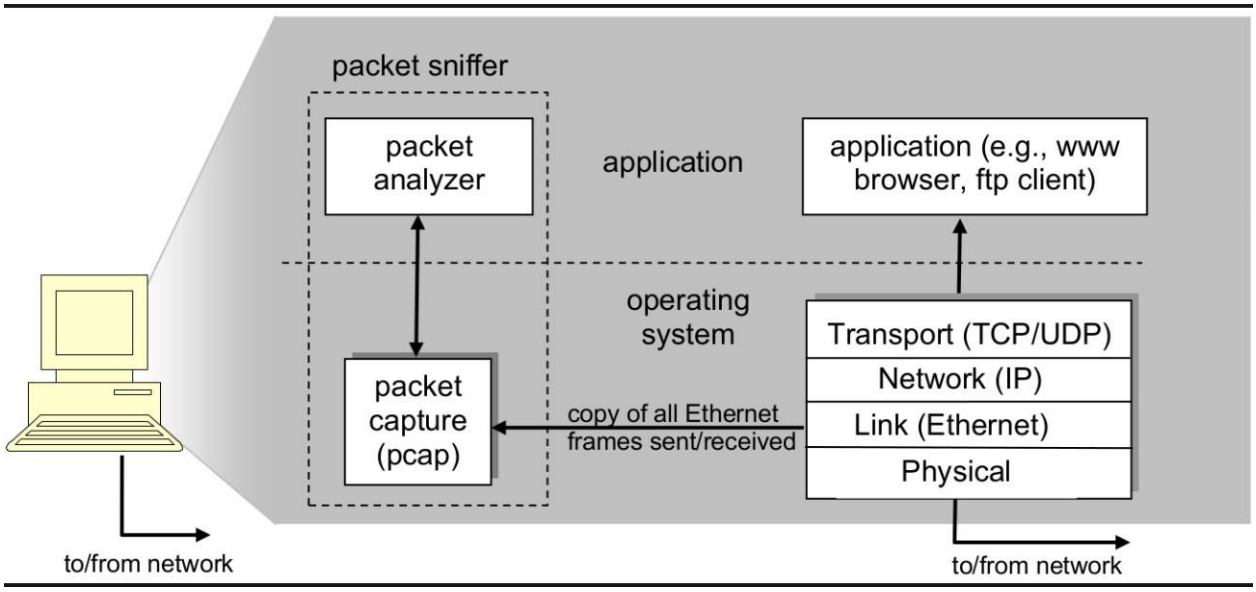
- number of ads shown by them.

- number of clicks on their ads also called PPC (pay per click).

To achieve this target, these agencies use packet sniffing to *inject advertisements* into the flowing packets. Most of the time these ads *contain malware*.

Government agencies use packet sniffing to:

- ensure security of data over the network.
- track an organisation's unencrypted data.

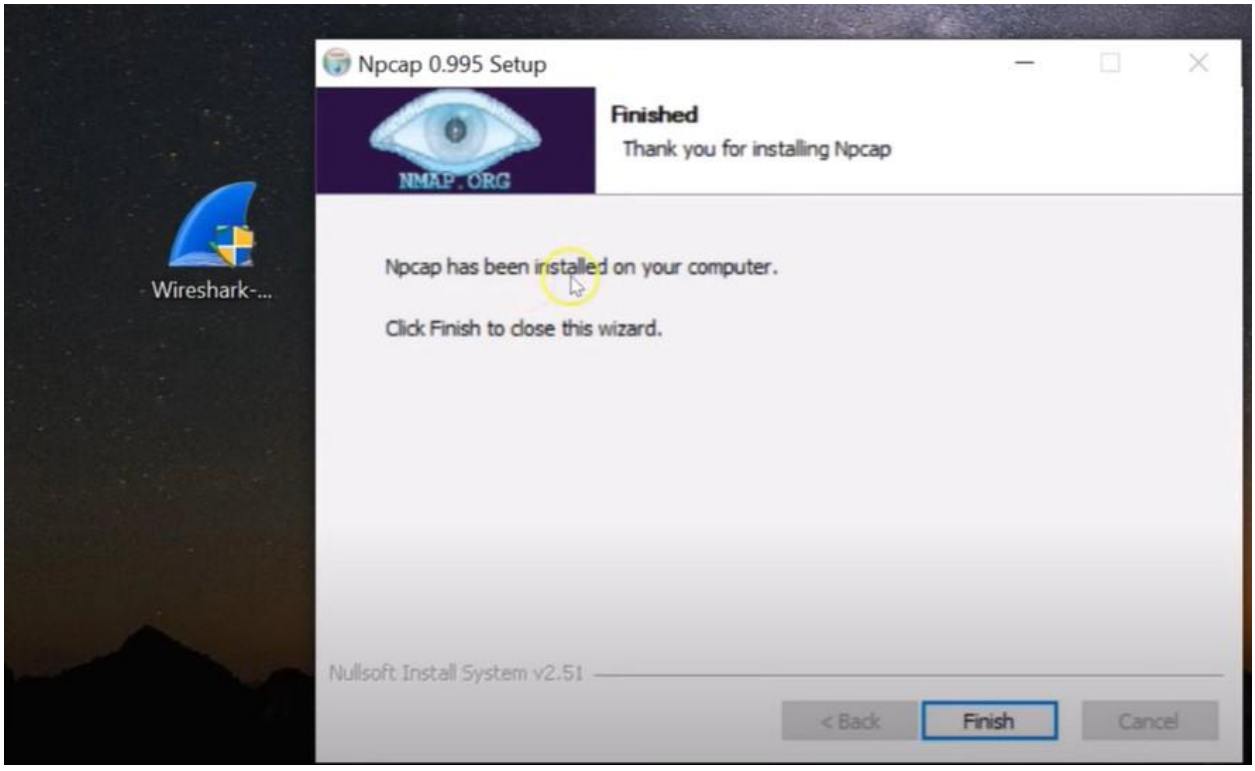


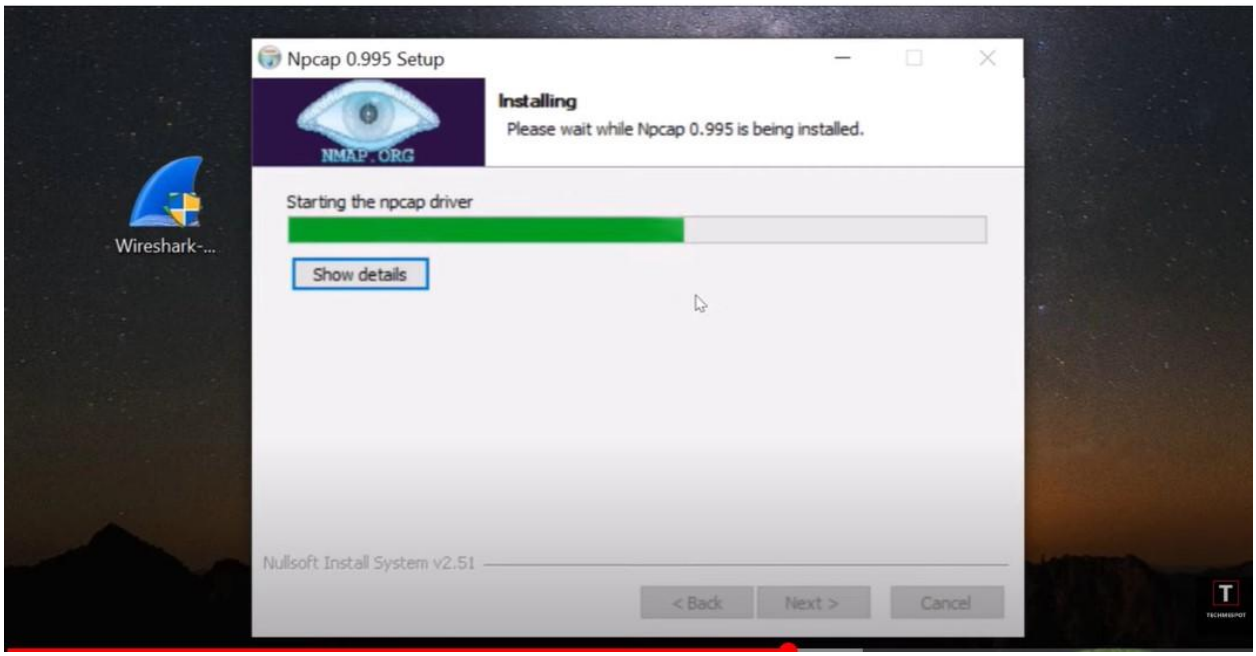
2. Steps involved in installation and running the wireshark with its components.

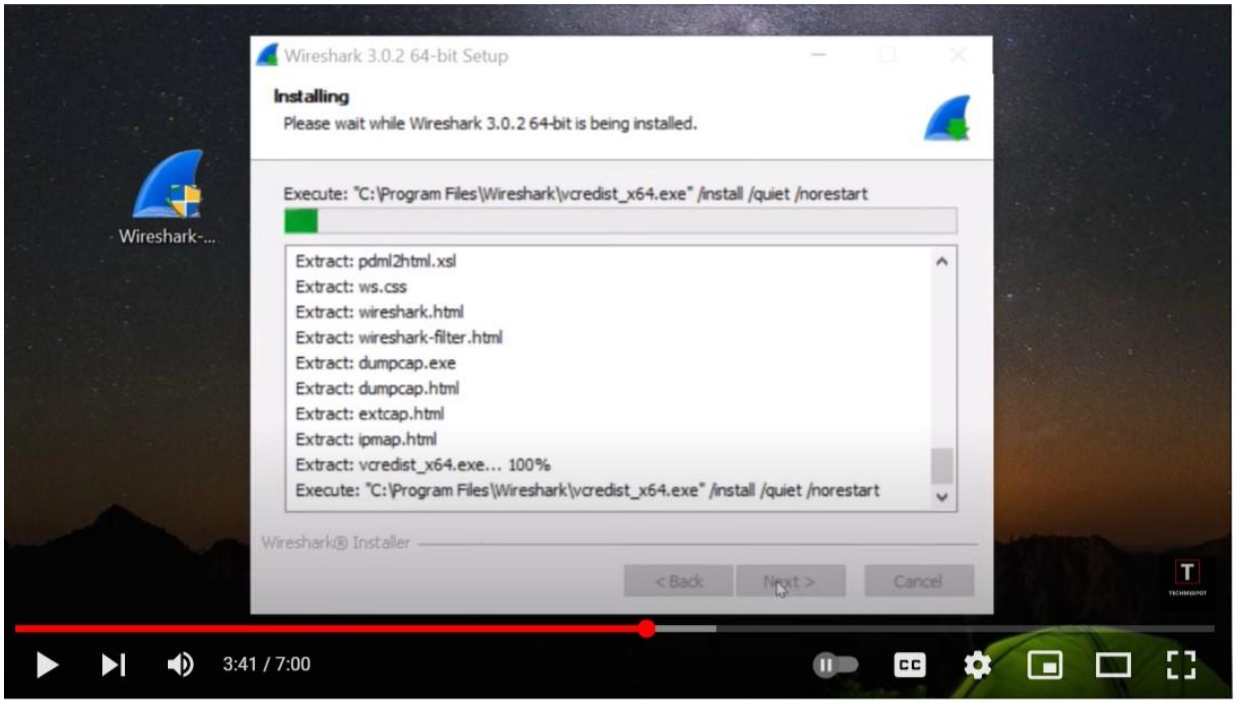
1. Go to the following website

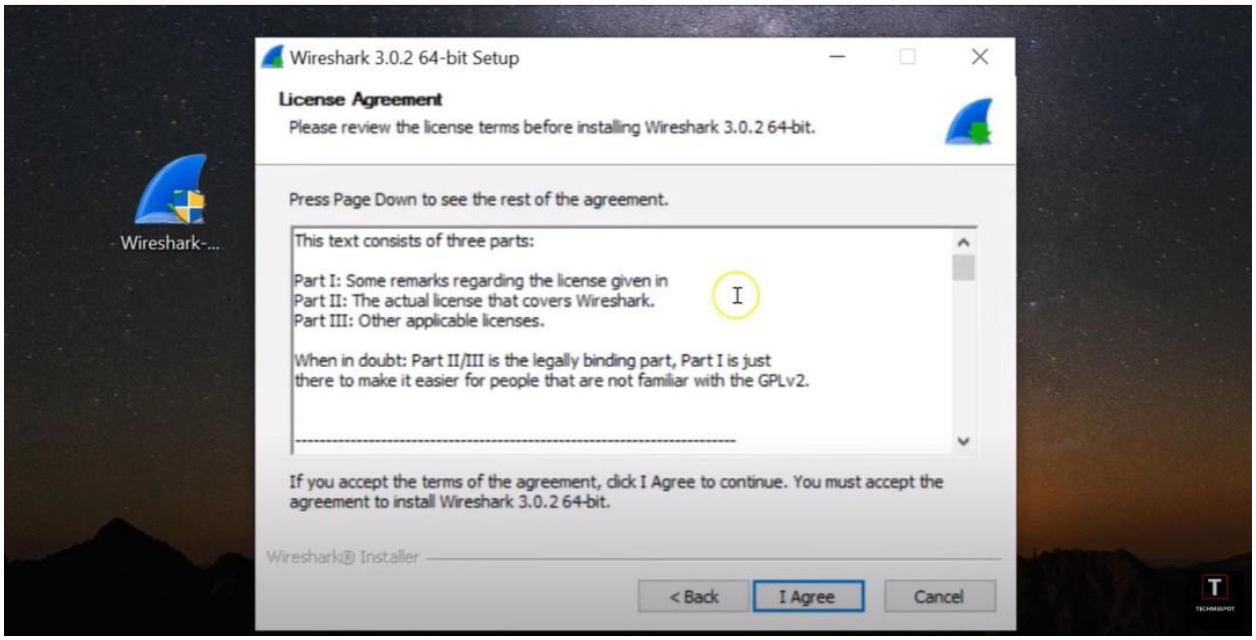
   https://www.wireshark.org/download.html

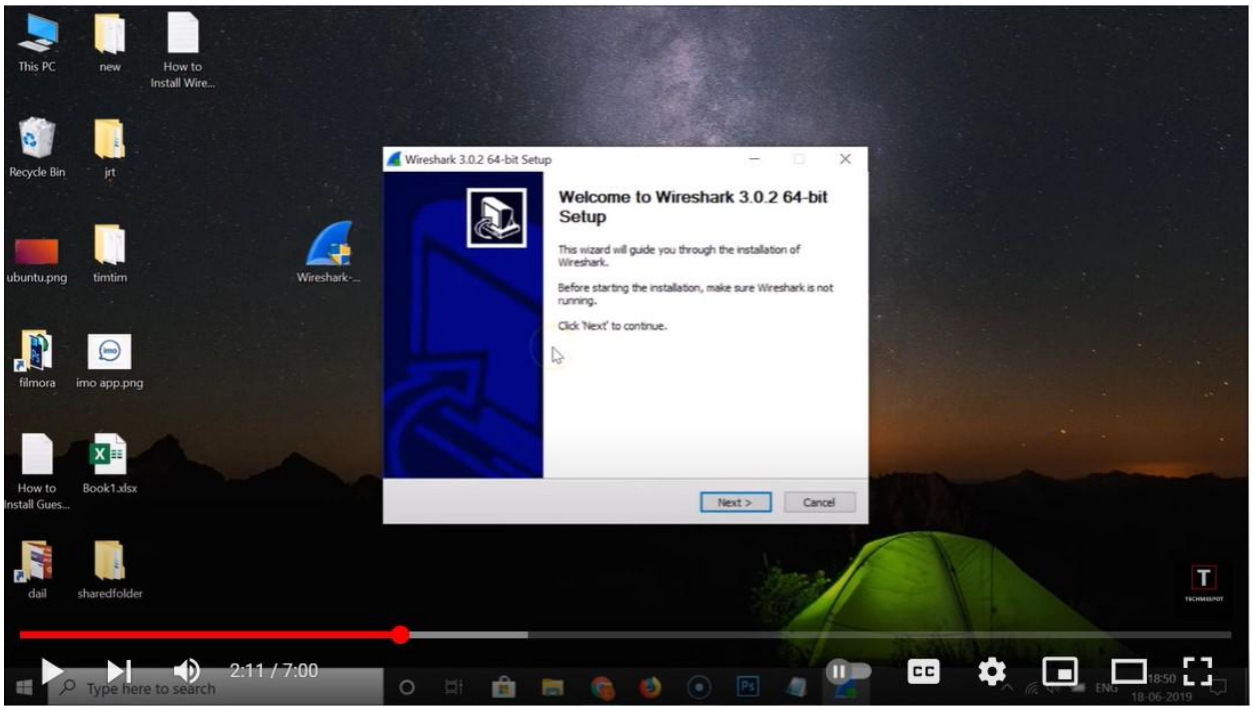
2. Choose the version according to your desktop specifications




Npcap 0.995 Setup
Installing
Please wait while Npcap 0.995 is being installed.
NMAP.ORG
Starting the npcap driver
Show details
Nullsoft Install System v2.51
< Back
Next >
Cancel
Wireshark-...


Wireshark 3.0.2 64-bit Setup
Installing
Please wait while Wireshark 3.0.2 64-bit is being installed.
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
Wireshark® Installer
< Back
Next >
Cancel
Wireshark-...
3:41 / 7:00


Wireshark 3.0.2 64-bit Setup
License Agreement
Please review the license terms before installing Wireshark 3.0.2 64-bit.
Press Page Down to see the rest of the agreement.
This text consists of three parts:
Part I: Some remarks regarding the license given in
Part II: The actual license that covers Wireshark.
Part III: Other applicable licenses.
When in doubt: Part II/III is the legally binding part, Part I is just
there to make it easier for people that are not familiar with the GPLv2.
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 3.0.2 64-bit.
Wireshark® Installer
< Back
I Agree
Cancel
Wireshark-...


This PC
new
How to Install Wire...
Recycle Bin
jrt
ubuntu.png
timtim
filmora
imo app.png
How to Install Gues...
Book1.xlsx
dail
sharedfolder
Wireshark-...
Wireshark 3.0.2 64-bit Setup
Welcome to Wireshark 3.0.2 64-bit Setup
This wizard will guide you through the installation of Wireshark.
Before starting the installation, make sure Wireshark is not running.
Click 'Next' to continue.
Next >
Cancel
2:11 / 7:00
Type here to search

3. Steps for capturing packets using URL given below:

http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

4. After your browser has displayed the INTRO-wireshark-file1.html page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. Type in "http" into the display filter specification window at the top of the main Wireshark window. Then select Apply or just hit return. Find the HTTP GET message that was sent from your computer to the gaia.cs.umass.edu HTTP server.

a) In the unfiltered packet-listing window in step above, list the three distinct protocols that are present in the protocol column

1. TCP
2. HTTP
3. SSDP

b) How long did it take between sending the HTTP GET message and receiving the HTTP OK response? (By default, the Time column in the packet listing window displays the duration of Wireshark tracing in seconds.Select the Wireshark View pull-down menu, then click Time Show Format, then click Time-of-day to display the Time field in time-of-day format.)

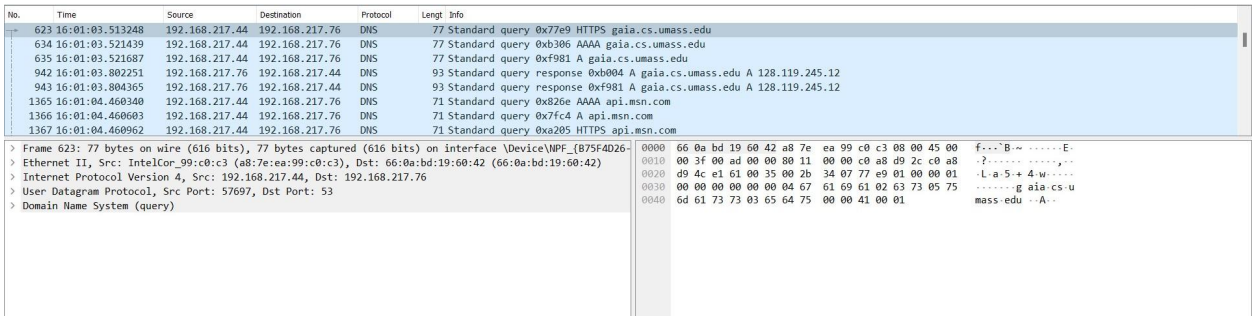
13301 15:42:16.687738 2409:40c1:10bf:926a:50d6:f19a:5bf4:b7ff 2600:140f:1c00::1740:8ca9 HTTP 186 GET /connecttest.txt HTTP/1.1

360 15:38:46.422844 2600:140f:1c00::1740:8ca9 2409:40c1:10bf:926a:50d6:f19a:5bf4:b7ff HTTP 261 HTTP/1.1 200 OK (text/plain)

Time difference = 00:03:30 (3 minutes and 30 seconds)

c) What is the Internet address of the gaia.cs.umass.edu (also known as www.net.cs.umass.edu)? What is the Internet address of your computer?

=> 192.168.217.44



- **The computer is going to have many ip addresses according the packets that are being accessed => so which one to chose**