Terna Engineering College

Computer Engineering Department

Program: Sem V

Course: Computer Network Lab

Faculty: Umesh B Mantale, D V Thombre and Ramesh Shahabade

LAB Manual

PART A

(PART A: TO BE REFERRED BY STUDENTS)

Experiment No. 4

A.1 Objective:

Demonstration, identification and analysis of different types of protocols used and packets transmitted in TCP/IP by using wireshark.

A.2 Prerequisite:

Knowledge of OSI and TCP/IP model.

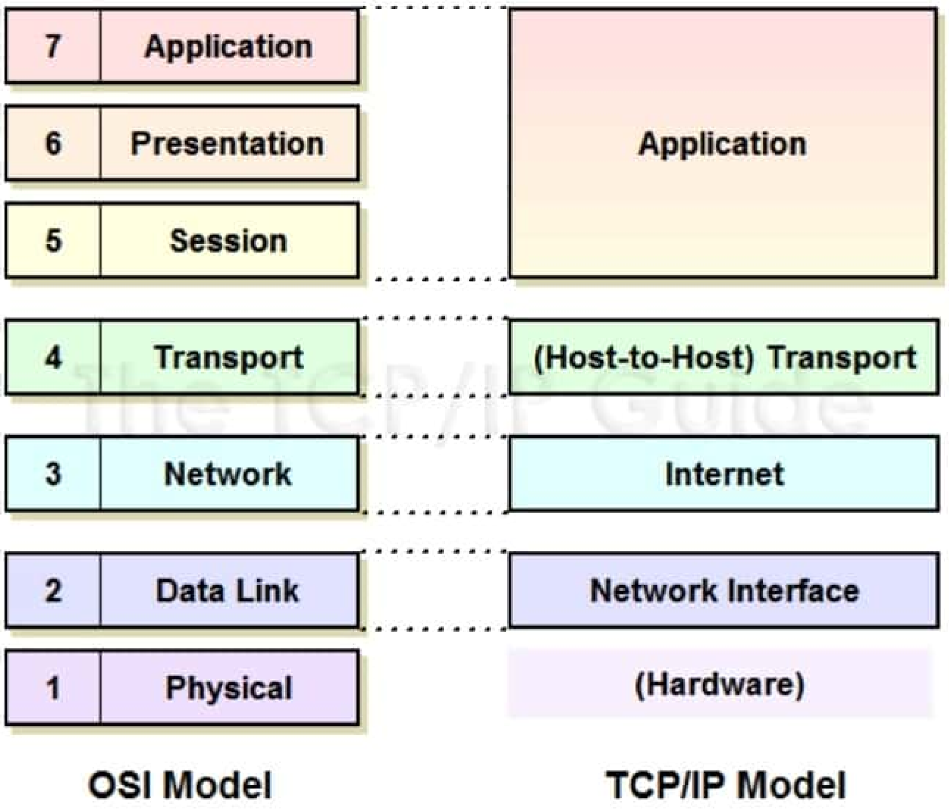
A.3 Outcome:

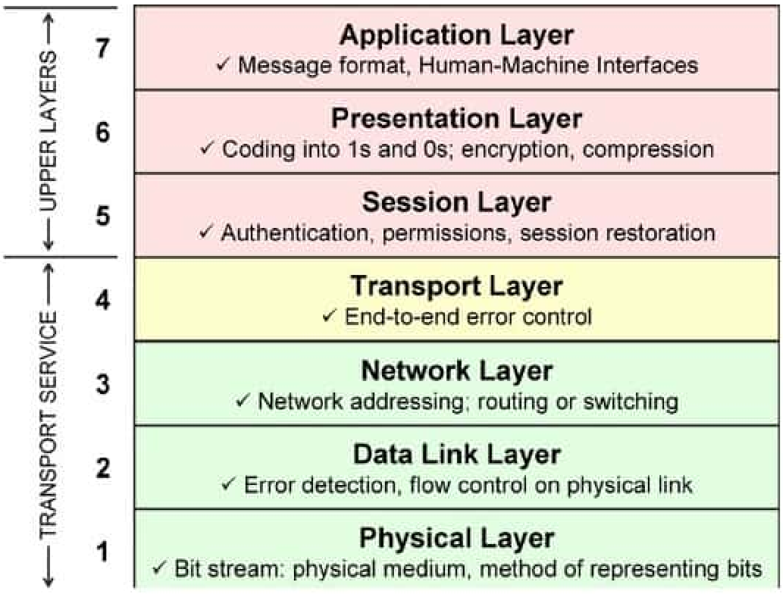
After successful completion of this experiment students will be able to

- Demonstration of a network packet analyzer and presentation of captured packet data in as much detail as possible.
- Ability to use network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

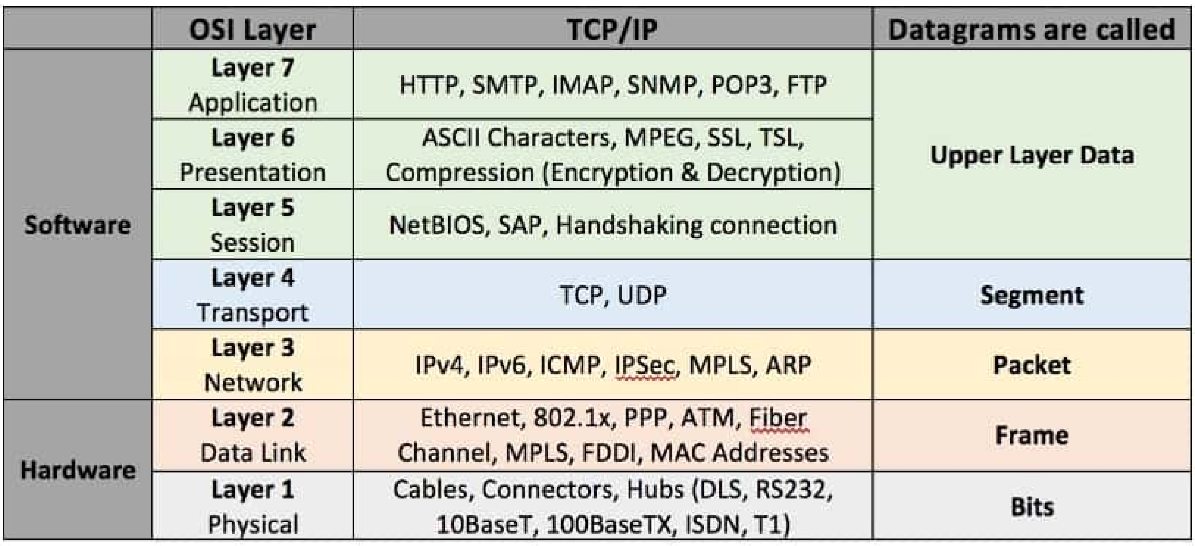
A.4 Theory:

OSI MODEL & TCP/IP MODEL





UPPER LAYERS	7	**Application Layer** ✓ Message format, Human-Machine Interfaces
	6	**Presentation Layer** ✓ Coding into 1s and 0s; encryption, compression
	5	**Session Layer** ✓ Authentication, permissions, session restoration
TRANSPORT SERVICE	4	**Transport Layer** ✓ End-to-end error control
	3	**Network Layer** ✓ Network addressing; routing or switching
	2	**Data Link Layer** ✓ Error detection, flow control on physical link
	1	**Physical Layer** ✓ Bit stream: physical medium, method of representing bits



	OSI Layer	TCP/IP	Datagrams are called
Software	**Layer 7** Application	HTTP, SMTP, IMAP, SNMP, POP3, FTP	**Upper Layer Data**
	Layer 6 Presentation	ASCII Characters, MPEG, SSL, TSL, Compression (Encryption & Decryption)	
	Layer 5 Session	NetBIOS, SAP, Handshaking connection	
	Layer 4 Transport	TCP, UDP	**Segment**
	Layer 3 Network	IPv4, IPv6, ICMP, IPSec, MPLS, ARP	**Packet**
Hardware	**Layer 2** Data Link	Ethernet, 802.1x, PPP, ATM, Fiber Channel, MPLS, FDDI, MAC Addresses	**Frame**
	Layer 1 Physical	Cables, Connectors, Hubs (DLS, RS232, 10BaseT, 100BaseTX, ISDN, T1)	**Bits**

1.1. What is Wireshark?

- Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.
- You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).
- In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

1.1.1. Some intended purposes

Here are some reasons people use Wireshark:

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- QA engineers use it to verify network applications
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

Wireshark can also be helpful in many other situations.

1.1.2. Features

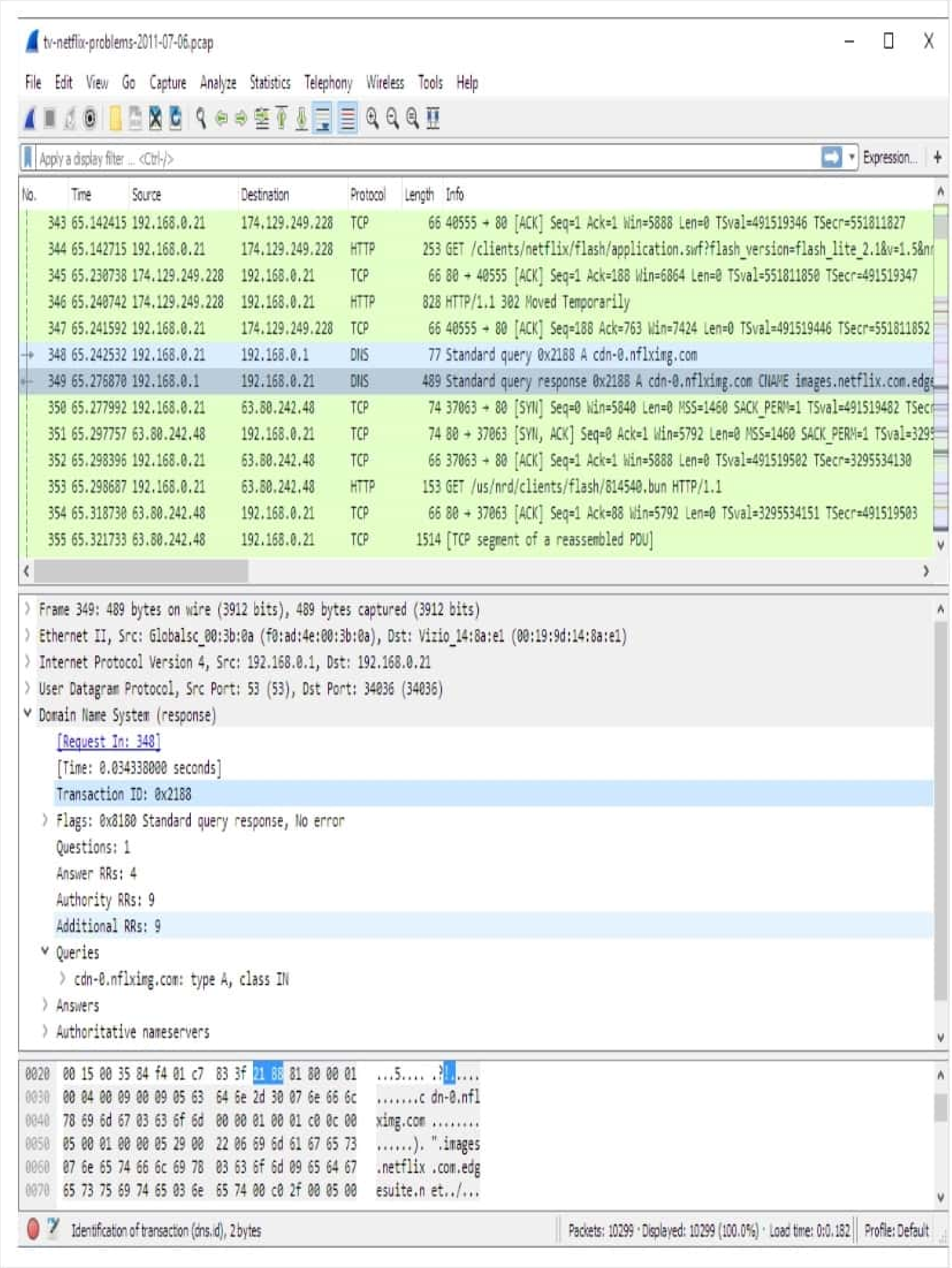
The following are some of the many features Wireshark provides:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Save packet data captured.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet displays based on filters.
- Create various statistics.
- ...and a lot more!

However, to really appreciate its power you have to start using it.

Figure 1.1, "Wireshark captures packets and lets you examine their contents." shows Wireshark having captured some packets and waiting for you to examine them.

Figure 1.1. Wireshark captures packets and lets you examine their contents.


tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time       Source           Destination      Protocol Length Info
 343 65.142415 192.168.0.21     174.129.249.228  TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
 344 65.142715 192.168.0.21     174.129.249.228  HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
 345 65.230738 174.129.249.228  192.168.0.21     TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
 346 65.240742 174.129.249.228  192.168.0.21     HTTP      828 HTTP/1.1 302 Moved Temporarily
 347 65.241592 192.168.0.21     174.129.249.228  TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
 348 65.242532 192.168.0.21     192.168.0.1      DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
 349 65.276870 192.168.0.1      192.168.0.21     DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
 350 65.277992 192.168.0.21     63.80.242.48     TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
 351 65.297757 63.80.242.48     192.168.0.21     TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
 352 65.298396 192.168.0.21     63.80.242.48     TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
 353 65.298687 192.168.0.21     63.80.242.48     HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
 354 65.318730 63.80.242.48     192.168.0.21     TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
 355 65.321733 63.80.242.48     192.168.0.21     TCP      1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes

Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

1.1.3. Live capture from many different network media

Wireshark can capture traffic from many different network media types, including Ethernet, Wireless LAN, Bluetooth, USB, and more. The specific media types supported may be limited by several factors, including your hardware and operating system. An overview of the supported media types can be found at https://wiki.wireshark.org/CaptureSetup/NetworkMedia.

1.1.4. Import files from many other capture programs

Wireshark can open packet captures from a large number of capture programs. For a list of input formats see Section 5.2.2, "Input File Formats".

1.1.5. Export files for many other capture programs

Wireshark can save captured packets in many formats, including those used by other capture programs. For a list of output formats see Section 5.3.2, "Output File Formats".

1.1.6. Many protocol dissectors

There are protocol dissectors (or decoders, as they are known in other products) for a great many protocols: see Appendix C, Protocols and Protocol Fields.

1.1.7. Open Source Software

Wireshark is an open source software project, and is released under the GNU General Public License (GPL). You can freely use Wireshark on any number of computers you like, without worrying about license keys or fees or such. In addition, all source code is freely available under the GPL. Because of that, it is very easy for people to add new protocols to Wireshark, either as plugins, or built into the source, and they often do!

1.1.8. What Wireshark is not

Here are some things Wireshark does not provide:

- Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

- Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except domain name resolution, but that can be disabled).

Refer:

1. https://www.wireshark.org/docs/wsug_html_chunked/ChCustCommandLine.html
2. https://www.javatpoint.com/wireshark
3. (https://www.youtube.com/watch?v=TkCSr30UojM)

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

(Students must submit the soft copy as per 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 the there is no Black board access available)

Roll No. 50	Name: Amey Thakur
Class: TE-Comps B	Batch: B3
Date of Experiment: 06/08/2020	Date of Submission: 06/08/2020
Grade :	

B.1 Document created by the student:

(Write the answers to the questions given in section 5.1 during the 2 hours of practical in the lab here)

Refer B.5

B.3 Observations and learning:

(Students are expected to understand the selected topic. Have to list out the components & functionality. Prepare a flow of the algorithm defined in the paper. List the performance metrics that is used)

We have studied demonstration, identification and analysis of different types of protocols used and packets transmitted in TCP/IP by using wireshark.

B.4 Conclusion:

(Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.3)

We conclude that using wireshark we identify and analyse different types of protocols used and packets transmitted in TCP/IP

Computer Networks Laboratory Experiment - 4

Amey Thakur D.O.E. - 06.08.2020

TE-Comps B-50 D.O.S. - 06.08.2020

B3

Q.1. Briefly explain why there are two layered protocols in networking, TCP/IP four layered and OSI seven layered?

Ans:

- In networking, there are two layered protocols for abstraction and specialization.
  Layers provide a division of the work done by a network. Networks are set up with a protocol hierarchy that divides the communication task into several layers. A protocol is a set of rules for communication within a layer. A service is what the layer provides to the layer above it through an interface.
- OSI has seven layers whereas TCP/IP has 4 layers
- OSI model is a generic model that is based upon functionalities of each layer. TCP/IP model is a protocol oriented standard.
- OSI model distinguishes three concepts -
  ① Services, ② Interfaces, ③ Protocol.
  TCP/IP does not have a clear distinction between these three
- OSI follows vertical approach whereas TCP/IP follows horizontal approach.
- In OSI, Data link layer and physical layer are separate layers whereas in TCP/IP these layers are combined.
- There is no session and presentation layer in TCP/IP model

Q.2. What is wireshark & mention the uses of wireshark.

Ans:

- Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.
- You could think of a network packet analyzer as a measuring device for examining what's h. happening inside a network cable.
- Wireshark is the world's leading network traffic analyzer, and an essential tool for any security professional or system administrator. This free software lets you analyze network traffic in real time and is often the best tool for troubleshooting issues on your network.

Uses:

① Capturing and analyzing packets on NICs

② Ability to negotiate multiple protocols on each OSI layer.

③ Capturing NIC for many layer 2 protocols like PPP, Ethernet, HDLC, etc. as well as ARP requests and routing protocol Hello message, etc.

④ Ability to capture different media traffic like USB, VOIP calls, application layer, protocol streams

⑤ Ability to see the data (best one available).

Q.3. A. Which layer of TCP/IP 4 layer model this address belongs to.

B. State the protocol appropriate to this address and any special characteristic for this address within the appropriate protocol.

The addresses are

① 136.206.1.4

② 192.168.1.10

③ 127.0.0.1

④ 0C : 5F : 56 : C0 : DD : 08

⑤ Port 80

⑥ Port 2000

Ans:

① 136.206.1.4

A. Internet Layer

B. IPv4 Public IP

② 192.168.1.10

A. Internet Layer

B. IPv4 Private IP

③ 127.0.0.1

A. Internet Layer

B. IPv4 Loopback

④ 0C : 5F : 56 : C0 : DD : 08

A. Link Layer

B. Mac Address

⑤ Port 80

A. Application Layer

B. HTTP, ip address 80, example - 192.168.126.132:80

⑥ Port 2000

A. SCCP / Skinny protocol

B. Transport Layer

Q.4. Port numbers belong to which layer ?

Ans:

Port numbers belong to Session Layer.

Q.5. What is a packet ? In which layer it is created ?

Ans:

- A packet is a small amount of data sent over a network.
- Packet refers to protocol data unit which is created in layer 3.

Q.6. What is color coding in Wireshark ?

Ans:

- In wireshark, there are packets highlighted in a variety of different colors.
- Wireshark uses colors to help identify the type of traffic at a glance.
- By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors.

Q.7. Write the features of Wireshark ?

Ans:

Features.

① Deep inspection of hundreads of protocols with more being added all the time.

② Live capture and offline analysis.

③ standard three - pane packet browser.

④ Multi platform

⑤ Captured network data can be browse by GUI. TTY mode TShark utility

6. The most powerful display filters in the industry
7. Rich VoIP Analysis
8. Read / Write many different capture file format
9. Capture file compressed with gzip can be decompressed on the fly
10. Live data can be read from various platforms

Q.8. Write the filters used in wireshark?

Ans:

- Wireshark has two filtering languages.
  1. Capture filters
  2. Display filters
- Capture filters are used for filtering when capturing packets
- Display filters are used for filtering which packets are displayed.

This filter displays packet based on

→ protocol
→ The presence of a field
→ The values of field
→ The comparison between fields

Q.9. What is packet snifting?

Ans:

- Packet snifting is the practice of gathering, collecting and logging some or all packets that pass through a computer network regardless of how the packet is addressed.
- In this way every packet or a defined subset of packets may be gathered for analysis.