PRACTICAL 6

Aim: To perform network analysis using Wireshark in Ubuntu OS.

Software Used: Wireshark

Introduction:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education runs on Linux, OS X, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.

Features:

Wireshark is software that understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols, Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports.

- Data can be captured from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from a number of types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI or via the terminal (command line) version ofthe utility, TShark.
- Captured files can be programmatically edited or converted via command-line switches to the"editcap" program.
- Data display can be refined using a display filter.

Color coding:

The user typically sees packets highlighted in green, blue, and black. Wireshark uses colors to help the user identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic. Light blue is UDP traffic, and black identifies TCP packets with problems --for example, they could have been delivered out-of-order. Users can change existing rules for coloring packets, add new rules. Or remove rules.

Procedure:

Step 1: Installing Wireshark

```
sudo apt-get install wireshark
```

Step 2: Running Wireshark

```
sudowireshark
```

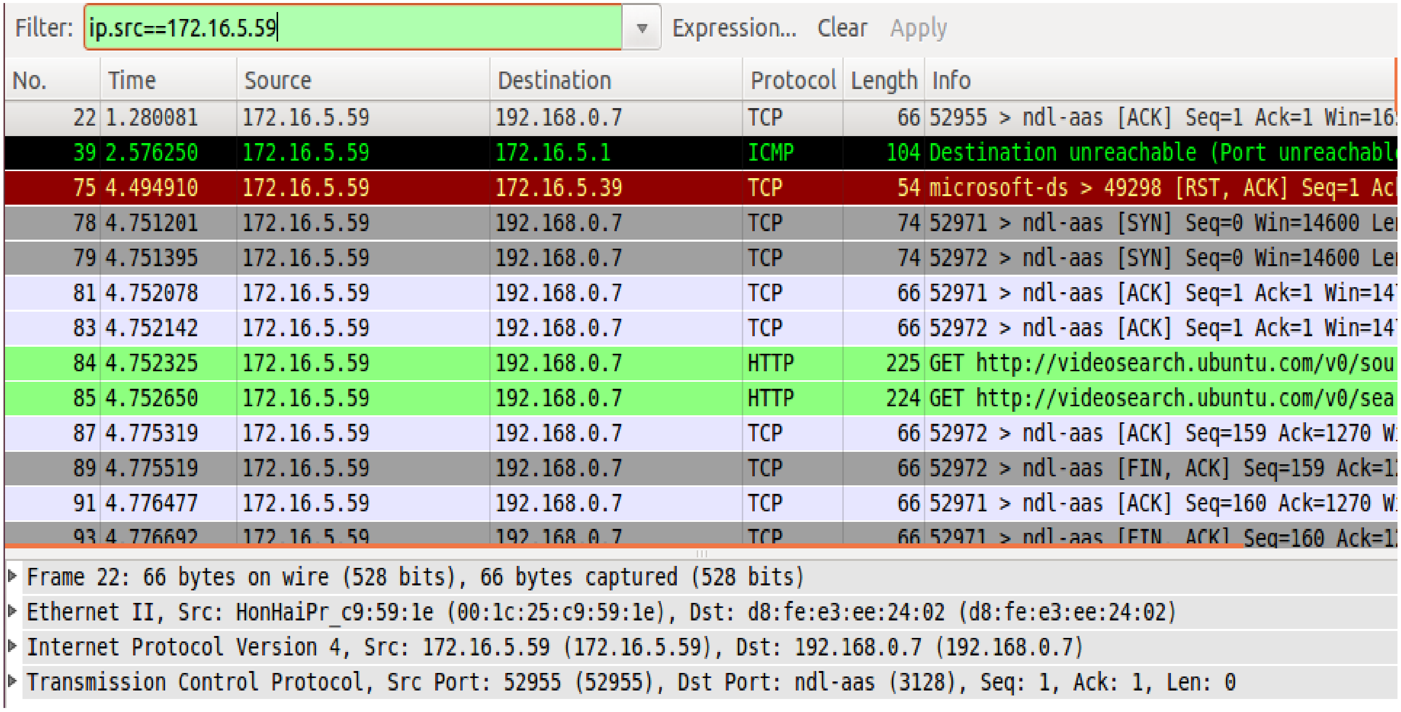
Step 3: Wireshark Configuration and Usage/Select an Interface and start the Capture

Step 4: Filtering (Write commands)

1) By Source IP Address
2) By Destination IP Address
3) By Ip Address
4) By Protocol
5) By PORT number

Results of filtering:

1. By Source IP Address: -

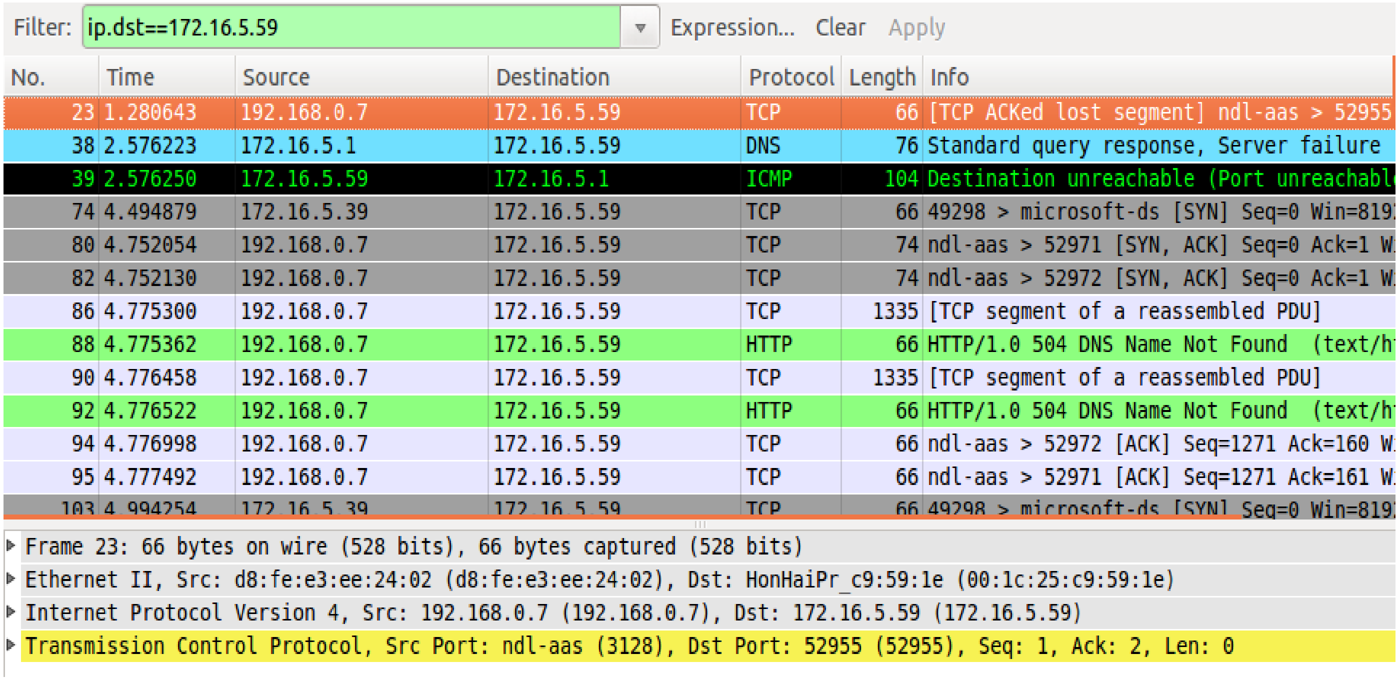


Filter: ip.src==172.16.5.59

No.	Time	Source	Destination	Protocol	Length	Info
22	1.280081	172.16.5.59	192.168.0.7	TCP	66	52955 > ndl-aas [ACK] Seq=1 Ack=1 Win=16
39	2.576250	172.16.5.59	172.16.5.1	ICMP	104	Destination unreachable (Port unreachabl
75	4.494910	172.16.5.59	172.16.5.39	TCP	54	microsoft-ds > 49298 [RST, ACK] Seq=1 Ac
78	4.751201	172.16.5.59	192.168.0.7	TCP	74	52971 > ndl-aas [SYN] Seq=0 Win=14600 Le
79	4.751395	172.16.5.59	192.168.0.7	TCP	74	52972 > ndl-aas [SYN] Seq=0 Win=14600 Le
81	4.752078	172.16.5.59	192.168.0.7	TCP	66	52971 > ndl-aas [ACK] Seq=1 Ack=1 Win=14
83	4.752142	172.16.5.59	192.168.0.7	TCP	66	52972 > ndl-aas [ACK] Seq=1 Ack=1 Win=14
84	4.752325	172.16.5.59	192.168.0.7	HTTP	225	GET http://videosearch.ubuntu.com/v0/sou
85	4.752650	172.16.5.59	192.168.0.7	HTTP	224	GET http://videosearch.ubuntu.com/v0/sea
87	4.775319	172.16.5.59	192.168.0.7	TCP	66	52972 > ndl-aas [ACK] Seq=159 Ack=1270 W
89	4.775519	172.16.5.59	192.168.0.7	TCP	66	52972 > ndl-aas [FIN, ACK] Seq=159 Ack=1
91	4.776477	172.16.5.59	192.168.0.7	TCP	66	52971 > ndl-aas [ACK] Seq=160 Ack=1270 W
93	4.776692	172.16.5.59	192.168.0.7	TCP	66	52971 > ndl-aas [FIN, ACK] Seq=160 Ack=1

```
▸ Frame 22: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: HonHaiPr_c9:59:1e (00:1c:25:c9:59:1e), Dst: d8:fe:e3:ee:24:02 (d8:fe:e3:ee:24:02)
▸ Internet Protocol Version 4, Src: 172.16.5.59 (172.16.5.59), Dst: 192.168.0.7 (192.168.0.7)
▸ Transmission Control Protocol, Src Port: 52955 (52955), Dst Port: ndl-aas (3128), Seq: 1, Ack: 1, Len: 0
```

2. By Destination IP Address: -

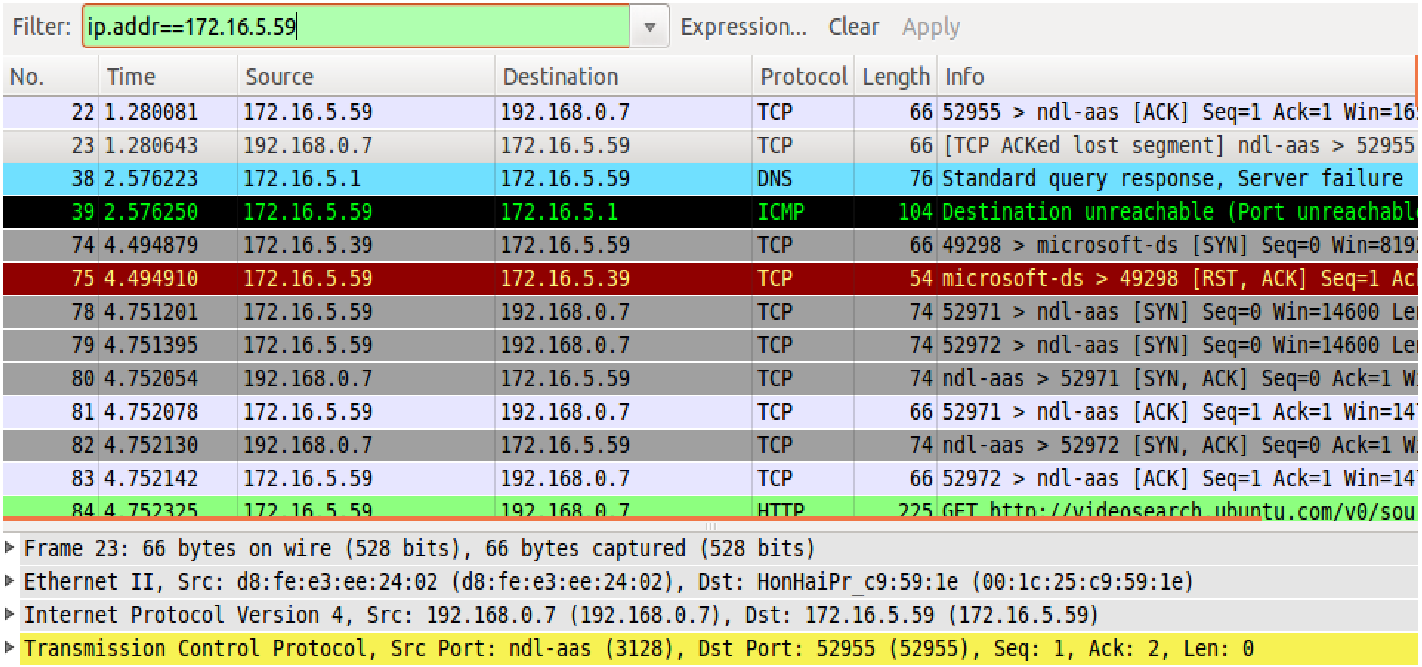


Filter: ip.dst==172.16.5.59

No.	Time	Source	Destination	Protocol	Length	Info
23	1.280643	192.168.0.7	172.16.5.59	TCP	66	[TCP ACKed lost segment] ndl-aas > 52955
38	2.576223	172.16.5.1	172.16.5.59	DNS	76	Standard query response, Server failure
39	2.576250	172.16.5.59	172.16.5.1	ICMP	104	Destination unreachable (Port unreachabl
74	4.494879	172.16.5.39	172.16.5.59	TCP	66	49298 > microsoft-ds [SYN] Seq=0 Win=819
80	4.752054	192.168.0.7	172.16.5.59	TCP	74	ndl-aas > 52971 [SYN, ACK] Seq=0 Ack=1 W
82	4.752130	192.168.0.7	172.16.5.59	TCP	74	ndl-aas > 52972 [SYN, ACK] Seq=0 Ack=1 W
86	4.775300	192.168.0.7	172.16.5.59	TCP	1335	[TCP segment of a reassembled PDU]
88	4.775362	192.168.0.7	172.16.5.59	HTTP	66	HTTP/1.0 504 DNS Name Not Found (text/h
90	4.776458	192.168.0.7	172.16.5.59	TCP	1335	[TCP segment of a reassembled PDU]
92	4.776522	192.168.0.7	172.16.5.59	HTTP	66	HTTP/1.0 504 DNS Name Not Found (text/h
94	4.776998	192.168.0.7	172.16.5.59	TCP	66	ndl-aas > 52972 [ACK] Seq=1271 Ack=160 W
95	4.777492	192.168.0.7	172.16.5.59	TCP	66	ndl-aas > 52971 [ACK] Seq=1271 Ack=161 W
103	4.994254	172.16.5.39	172.16.5.59	TCP	66	49298 > microsoft-ds [SYN] Seq=0 Win=819

```
▸ Frame 23: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: d8:fe:e3:ee:24:02 (d8:fe:e3:ee:24:02), Dst: HonHaiPr_c9:59:1e (00:1c:25:c9:59:1e)
▸ Internet Protocol Version 4, Src: 192.168.0.7 (192.168.0.7), Dst: 172.16.5.59 (172.16.5.59)
▸ Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: 52955 (52955), Seq: 1, Ack: 2, Len: 0
```

3. By Ip Address: -

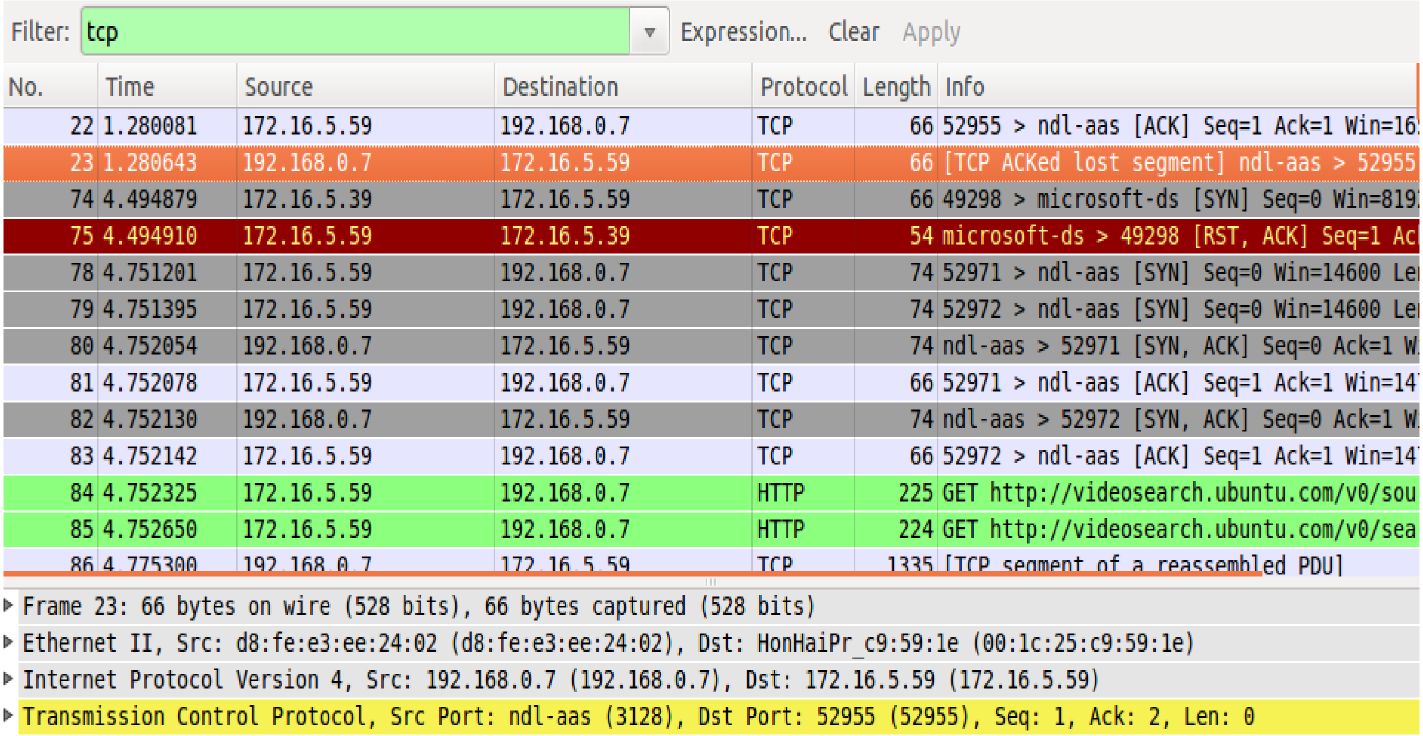


Filter: ip.addr==172.16.5.59

No.	Time	Source	Destination	Protocol	Length	Info
22	1.280081	172.16.5.59	192.168.0.7	TCP	66	52955 > ndl-aas [ACK] Seq=1 Ack=1 Win=16
23	1.280643	192.168.0.7	172.16.5.59	TCP	66	[TCP ACKed lost segment] ndl-aas > 52955
38	2.576223	172.16.5.1	172.16.5.59	DNS	76	Standard query response, Server failure
39	2.576250	172.16.5.59	172.16.5.1	ICMP	104	Destination unreachable (Port unreachabl
74	4.494879	172.16.5.39	172.16.5.59	TCP	66	49298 > microsoft-ds [SYN] Seq=0 Win=819
75	4.494910	172.16.5.59	172.16.5.39	TCP	54	microsoft-ds > 49298 [RST, ACK] Seq=1 Ac
78	4.751201	172.16.5.59	192.168.0.7	TCP	74	52971 > ndl-aas [SYN] Seq=0 Win=14600 Le
79	4.751395	172.16.5.59	192.168.0.7	TCP	74	52972 > ndl-aas [SYN] Seq=0 Win=14600 Le
80	4.752054	192.168.0.7	172.16.5.59	TCP	74	ndl-aas > 52971 [SYN, ACK] Seq=0 Ack=1 W
81	4.752078	172.16.5.59	192.168.0.7	TCP	66	52971 > ndl-aas [ACK] Seq=1 Ack=1 Win=14
82	4.752130	192.168.0.7	172.16.5.59	TCP	74	ndl-aas > 52972 [SYN, ACK] Seq=0 Ack=1 W
83	4.752142	172.16.5.59	192.168.0.7	TCP	66	52972 > ndl-aas [ACK] Seq=1 Ack=1 Win=14
84	4.752325	172.16.5.59	192.168.0.7	HTTP	225	GET http://videosearch.ubuntu.com/v0/sou

```
▸ Frame 23: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: d8:fe:e3:ee:24:02 (d8:fe:e3:ee:24:02), Dst: HonHaiPr_c9:59:1e (00:1c:25:c9:59:1e)
▸ Internet Protocol Version 4, Src: 192.168.0.7 (192.168.0.7), Dst: 172.16.5.59 (172.16.5.59)
▸ Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: 52955 (52955), Seq: 1, Ack: 2, Len: 0
```

4. By Protocol: -

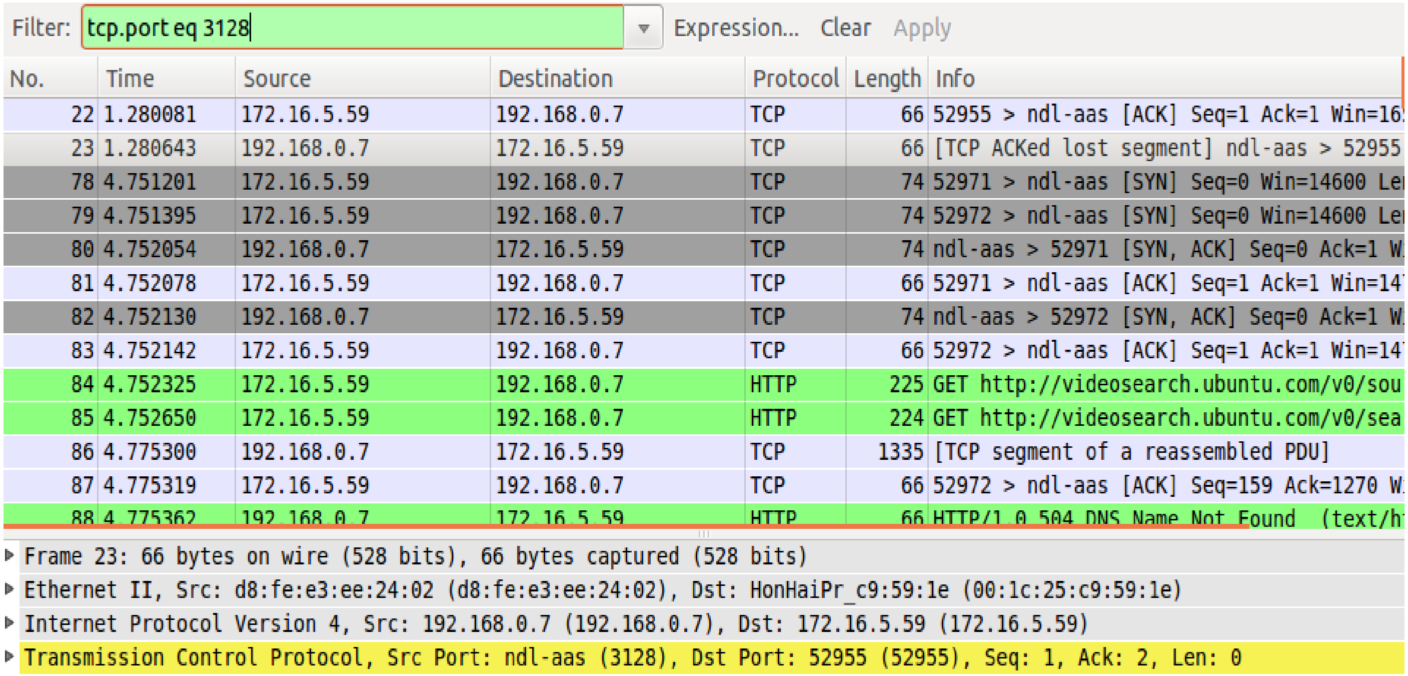


Filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
22	1.280081	172.16.5.59	192.168.0.7	TCP	66	52955 > ndl-aas [ACK] Seq=1 Ack=1 Win=16
23	1.280643	192.168.0.7	172.16.5.59	TCP	66	[TCP ACKed lost segment] ndl-aas > 52955
74	4.494879	172.16.5.39	172.16.5.59	TCP	66	49298 > microsoft-ds [SYN] Seq=0 Win=819
75	4.494910	172.16.5.59	172.16.5.39	TCP	54	microsoft-ds > 49298 [RST, ACK] Seq=1 Ac
78	4.751201	172.16.5.59	192.168.0.7	TCP	74	52971 > ndl-aas [SYN] Seq=0 Win=14600 Le
79	4.751395	172.16.5.59	192.168.0.7	TCP	74	52972 > ndl-aas [SYN] Seq=0 Win=14600 Le
80	4.752054	192.168.0.7	172.16.5.59	TCP	74	ndl-aas > 52971 [SYN, ACK] Seq=0 Ack=1 W
81	4.752078	172.16.5.59	192.168.0.7	TCP	66	52971 > ndl-aas [ACK] Seq=1 Ack=1 Win=14
82	4.752130	192.168.0.7	172.16.5.59	TCP	74	ndl-aas > 52972 [SYN, ACK] Seq=0 Ack=1 W
83	4.752142	172.16.5.59	192.168.0.7	TCP	66	52972 > ndl-aas [ACK] Seq=1 Ack=1 Win=14
84	4.752325	172.16.5.59	192.168.0.7	HTTP	225	GET http://videosearch.ubuntu.com/v0/sou
85	4.752650	172.16.5.59	192.168.0.7	HTTP	224	GET http://videosearch.ubuntu.com/v0/sea
86	4.775300	192.168.0.7	172.16.5.59	TCP	1335	[TCP segment of a reassembled PDU]

```
▸ Frame 23: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: d8:fe:e3:ee:24:02 (d8:fe:e3:ee:24:02), Dst: HonHaiPr_c9:59:1e (00:1c:25:c9:59:1e)
▸ Internet Protocol Version 4, Src: 192.168.0.7 (192.168.0.7), Dst: 172.16.5.59 (172.16.5.59)
▸ Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: 52955 (52955), Seq: 1, Ack: 2, Len: 0
```

5. By PORT number: -



Filter: tcp.port eq 3128

No.	Time	Source	Destination	Protocol	Length	Info
22	1.280081	172.16.5.59	192.168.0.7	TCP	66	52955 > ndl-aas [ACK] Seq=1 Ack=1 Win=16
23	1.280643	192.168.0.7	172.16.5.59	TCP	66	[TCP ACKed lost segment] ndl-aas > 52955
78	4.751201	172.16.5.59	192.168.0.7	TCP	74	52971 > ndl-aas [SYN] Seq=0 Win=14600 Le
79	4.751395	172.16.5.59	192.168.0.7	TCP	74	52972 > ndl-aas [SYN] Seq=0 Win=14600 Le
80	4.752054	192.168.0.7	172.16.5.59	TCP	74	ndl-aas > 52971 [SYN, ACK] Seq=0 Ack=1 W
81	4.752078	172.16.5.59	192.168.0.7	TCP	66	52971 > ndl-aas [ACK] Seq=1 Ack=1 Win=14
82	4.752130	192.168.0.7	172.16.5.59	TCP	74	ndl-aas > 52972 [SYN, ACK] Seq=0 Ack=1 W
83	4.752142	172.16.5.59	192.168.0.7	TCP	66	52972 > ndl-aas [ACK] Seq=1 Ack=1 Win=14
84	4.752325	172.16.5.59	192.168.0.7	HTTP	225	GET http://videosearch.ubuntu.com/v0/sou
85	4.752650	172.16.5.59	192.168.0.7	HTTP	224	GET http://videosearch.ubuntu.com/v0/sea
86	4.775300	192.168.0.7	172.16.5.59	TCP	1335	[TCP segment of a reassembled PDU]
87	4.775319	172.16.5.59	192.168.0.7	TCP	66	52972 > ndl-aas [ACK] Seq=159 Ack=1270 W
88	4.775362	192.168.0.7	172.16.5.59	HTTP	66	HTTP/1.0 504 DNS Name Not Found (text/h

```
▸ Frame 23: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: d8:fe:e3:ee:24:02 (d8:fe:e3:ee:24:02), Dst: HonHaiPr_c9:59:1e (00:1c:25:c9:59:1e)
▸ Internet Protocol Version 4, Src: 192.168.0.7 (192.168.0.7), Dst: 172.16.5.59 (172.16.5.59)
▸ Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: 52955 (52955), Seq: 1, Ack: 2, Len: 0
```

Conclusion: -

By performing this practical, we learnt that how to analysis network using Wireshark in Ubuntu OS.