

Date: 30 /8 /2024

Lab Practical #08:

Study Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

Practical Assignment #08:

1. Explain usage of Wireshark tool.

Wireshark is a powerful network protocol analyzer used for capturing and analyzing network traffic in real-time. It helps in troubleshooting network issues, monitoring network activity, and ensuring security by inspecting the data packets transmitted over a network.

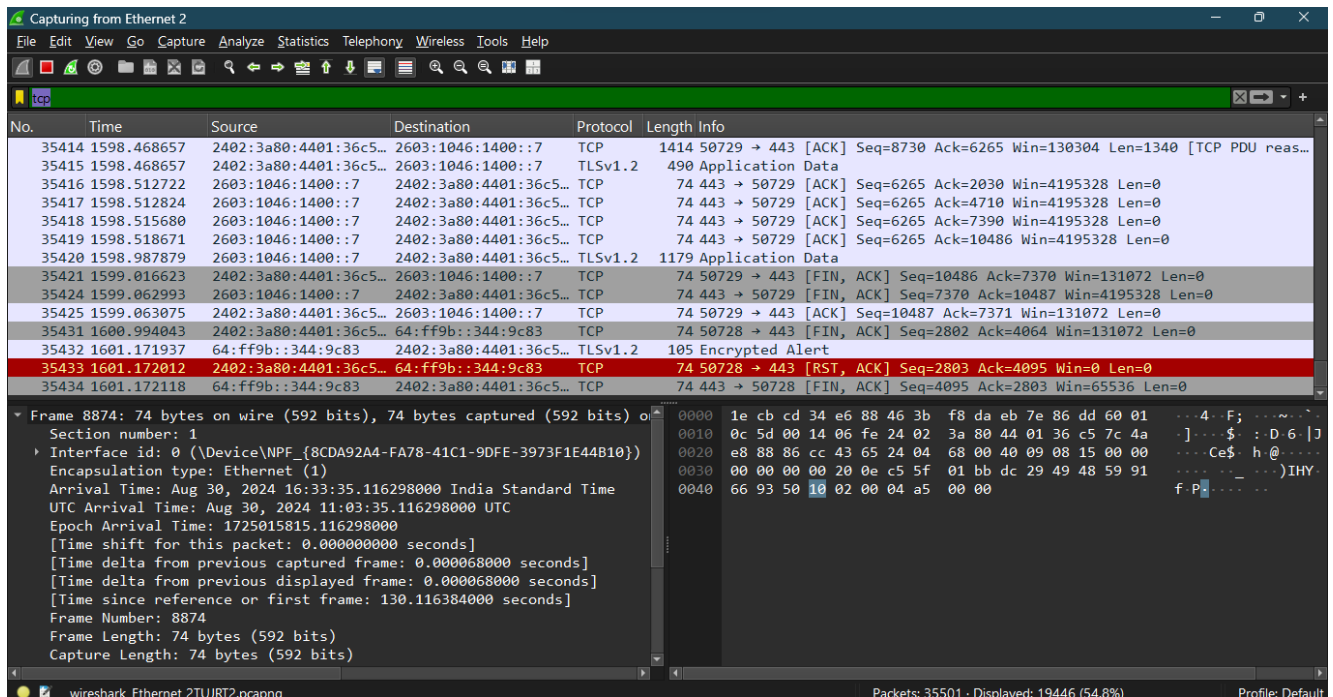
Key Uses:

1. Network Troubleshooting: Identifying bottlenecks, dropped packets, or misconfigurations.
2. Security Analysis: Detecting malicious traffic, network intrusions, or unauthorized access.
3. Protocol Analysis: Analyzing network protocols such as TCP/IP, HTTP, DNS, etc.
4. Performance Monitoring: Measuring network performance and bandwidth utilization.
5. Learning & Research: Understanding how data flows in a network for educational purposes.

Wireshark provides detailed packet-level information, making it invaluable for network administrators and security professionals.

2. Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

TCP



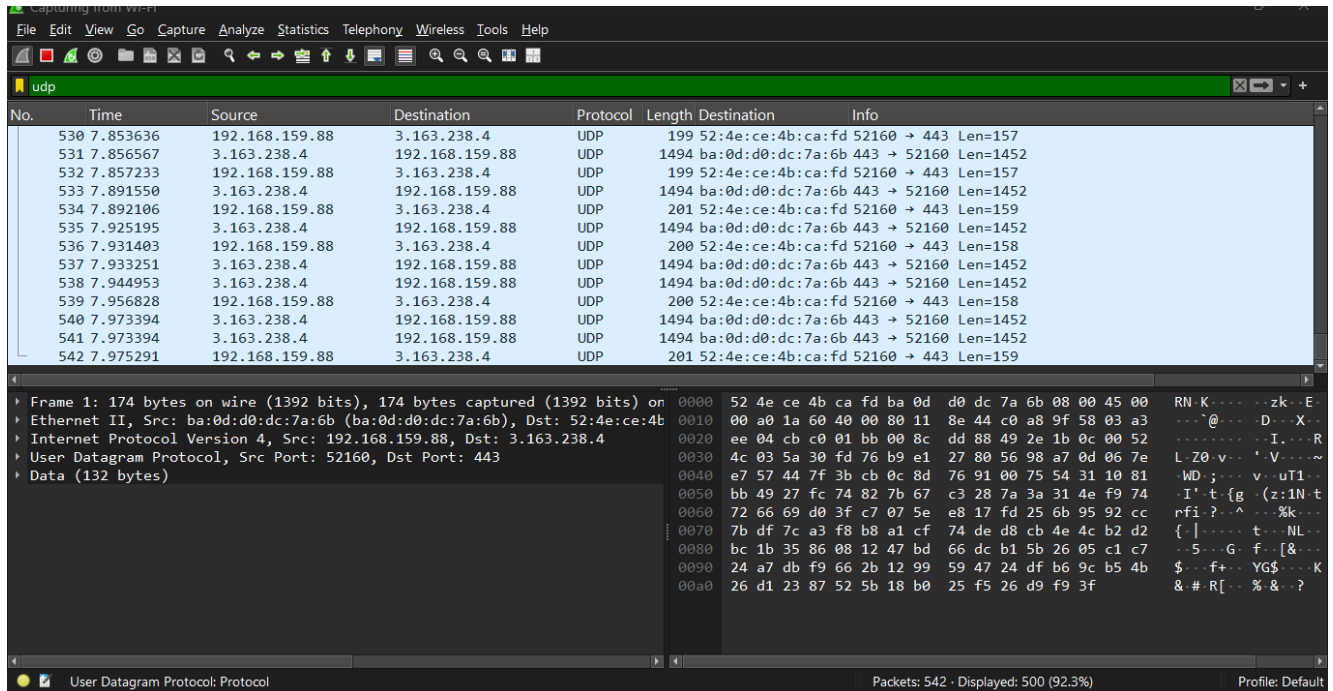


DARSHAN INSTITUTE OF ENGINEERING & TECHNOLOGY

Semester 5th | Practical Assignment | Computer Networks (2101CS501)

Date: 30 /8 /2024

UDP



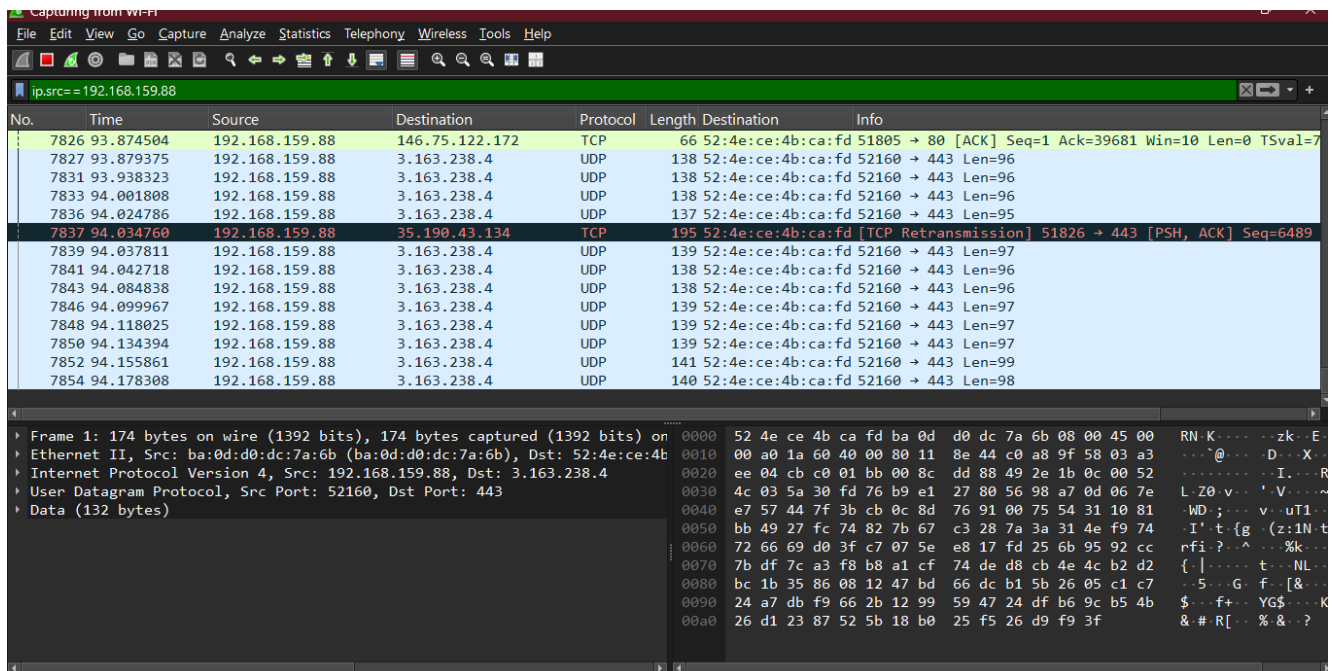
Wireshark capture of UDP traffic. The packet list shows 14 UDP packets from 192.168.159.88 to 3.163.238.4. The packet details pane shows the structure of a UDP packet: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (Src Port: 52160, Dst Port: 443). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Destination	Info
530	7.853636	192.168.159.88	3.163.238.4	UDP	199	52:4e:ce:4b:ca:fd	52160 → 443 Len=157
531	7.856567	3.163.238.4	192.168.159.88	UDP	1494	ba:0d:d0:dc:7a:6b	443 → 52160 Len=1452
532	7.857233	192.168.159.88	3.163.238.4	UDP	199	52:4e:ce:4b:ca:fd	52160 → 443 Len=157
533	7.891550	3.163.238.4	192.168.159.88	UDP	1494	ba:0d:d0:dc:7a:6b	443 → 52160 Len=1452
534	7.892106	192.168.159.88	3.163.238.4	UDP	201	52:4e:ce:4b:ca:fd	52160 → 443 Len=159
535	7.925195	3.163.238.4	192.168.159.88	UDP	1494	ba:0d:d0:dc:7a:6b	443 → 52160 Len=1452
536	7.931403	192.168.159.88	3.163.238.4	UDP	200	52:4e:ce:4b:ca:fd	52160 → 443 Len=158
537	7.933251	3.163.238.4	192.168.159.88	UDP	1494	ba:0d:d0:dc:7a:6b	443 → 52160 Len=1452
538	7.944953	3.163.238.4	192.168.159.88	UDP	1494	ba:0d:d0:dc:7a:6b	443 → 52160 Len=1452
539	7.956828	192.168.159.88	3.163.238.4	UDP	200	52:4e:ce:4b:ca:fd	52160 → 443 Len=158
540	7.973394	3.163.238.4	192.168.159.88	UDP	1494	ba:0d:d0:dc:7a:6b	443 → 52160 Len=1452
541	7.973394	3.163.238.4	192.168.159.88	UDP	1494	ba:0d:d0:dc:7a:6b	443 → 52160 Len=1452
542	7.975291	192.168.159.88	3.163.238.4	UDP	201	52:4e:ce:4b:ca:fd	52160 → 443 Len=159

Frame 1: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on
Ethernet II, Src: ba:0d:d0:dc:7a:6b (ba:0d:d0:dc:7a:6b), Dst: 52:4e:ce:4b:ca:fd
Internet Protocol Version 4, Src: 192.168.159.88, Dst: 3.163.238.4
User Datagram Protocol, Src Port: 52160, Dst Port: 443
Data (132 bytes)

Packets: 542 - Displayed: 500 (92.3%) Profile: Default

IP



Wireshark capture of IP traffic. The packet list shows 14 IP packets from 192.168.159.88 to 3.163.238.4. The packet details pane shows the structure of an IP packet: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (Src Port: 52160, Dst Port: 443). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Destination	Info
7826	93.874504	192.168.159.88	146.75.122.172	TCP	66	52:4e:ce:4b:ca:fd	51805 → 80 [ACK] Seq=1 Ack=39681 Win=10 Len=0 TSval=7
7827	93.879375	192.168.159.88	3.163.238.4	UDP	138	52:4e:ce:4b:ca:fd	52160 → 443 Len=96
7831	93.938323	192.168.159.88	3.163.238.4	UDP	138	52:4e:ce:4b:ca:fd	52160 → 443 Len=96
7833	94.001808	192.168.159.88	3.163.238.4	UDP	138	52:4e:ce:4b:ca:fd	52160 → 443 Len=96
7836	94.024786	192.168.159.88	3.163.238.4	UDP	137	52:4e:ce:4b:ca:fd	52160 → 443 Len=95
7837	94.034760	192.168.159.88	35.190.43.134	TCP	195	52:4e:ce:4b:ca:fd	[TCP Retransmission] 51826 → 443 [PSH, ACK] Seq=6489
7839	94.037811	192.168.159.88	3.163.238.4	UDP	139	52:4e:ce:4b:ca:fd	52160 → 443 Len=97
7841	94.042718	192.168.159.88	3.163.238.4	UDP	138	52:4e:ce:4b:ca:fd	52160 → 443 Len=96
7843	94.084838	192.168.159.88	3.163.238.4	UDP	138	52:4e:ce:4b:ca:fd	52160 → 443 Len=96
7846	94.099967	192.168.159.88	3.163.238.4	UDP	139	52:4e:ce:4b:ca:fd	52160 → 443 Len=97
7848	94.118025	192.168.159.88	3.163.238.4	UDP	139	52:4e:ce:4b:ca:fd	52160 → 443 Len=97
7850	94.134394	192.168.159.88	3.163.238.4	UDP	139	52:4e:ce:4b:ca:fd	52160 → 443 Len=97
7852	94.155861	192.168.159.88	3.163.238.4	UDP	141	52:4e:ce:4b:ca:fd	52160 → 443 Len=99
7854	94.178308	192.168.159.88	3.163.238.4	UDP	140	52:4e:ce:4b:ca:fd	52160 → 443 Len=98

Frame 1: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on
Ethernet II, Src: ba:0d:d0:dc:7a:6b (ba:0d:d0:dc:7a:6b), Dst: 52:4e:ce:4b:ca:fd
Internet Protocol Version 4, Src: 192.168.159.88, Dst: 3.163.238.4
User Datagram Protocol, Src Port: 52160, Dst Port: 443
Data (132 bytes)



DARSHAN INSTITUTE OF ENGINEERING & TECHNOLOGY

Semester 5th | Practical Assignment | Computer Networks (2101CS501)

Date: 30 /8 /2024

HTTP

No.	Time	Source	Destination	Protocol	Length	Destination	Info
1346	0.031513	111.119.15.128	192.168.159.88	TCP	1346	ba:0d:d0:dc:7a:6b 80 → 51752 [ACK] Seq=34561 Ack=1 Win=32363 Len=1280	TCP Reset, Seq=34561, Win=32363, Len=1280
492	0.031513	192.168.159.88	111.119.15.0	HTTP	492	52:4e:ce:4b:ca:fd GET /filestreamingservice/files/ec3f42ff-db07-4960-b5	GET /filestreamingservice/files/ec3f42ff-db07-4960-b5
977	0.031513	111.119.15.0	192.168.159.88	HTTP	977	ba:0d:d0:dc:7a:6b HTTP/1.1 206 Partial Content (application/x-chrome-e	HTTP/1.1 206 Partial Content (application/x-chrome-e
492	0.031513	192.168.159.88	111.119.15.0	HTTP	492	52:4e:ce:4b:ca:fd GET /filestreamingservice/files/ec3f42ff-db07-4960-b5	GET /filestreamingservice/files/ec3f42ff-db07-4960-b5
1001	0.031513	111.119.15.0	192.168.159.88	HTTP	1001	ba:0d:d0:dc:7a:6b HTTP/1.1 206 Partial Content (application/x-chrome-e	HTTP/1.1 206 Partial Content (application/x-chrome-e
492	0.031513	192.168.159.88	111.119.15.0	HTTP	492	52:4e:ce:4b:ca:fd GET /filestreamingservice/files/ec3f42ff-db07-4960-b5	GET /filestreamingservice/files/ec3f42ff-db07-4960-b5
1001	0.031513	111.119.15.0	192.168.159.88	HTTP	1001	ba:0d:d0:dc:7a:6b HTTP/1.1 206 Partial Content (application/x-chrome-e	HTTP/1.1 206 Partial Content (application/x-chrome-e
492	0.031513	192.168.159.88	111.119.15.0	HTTP	492	52:4e:ce:4b:ca:fd GET /filestreamingservice/files/ec3f42ff-db07-4960-b5	GET /filestreamingservice/files/ec3f42ff-db07-4960-b5
1001	0.031513	111.119.15.0	192.168.159.88	HTTP	1001	ba:0d:d0:dc:7a:6b HTTP/1.1 206 Partial Content (application/x-chrome-e	HTTP/1.1 206 Partial Content (application/x-chrome-e
492	0.031513	192.168.159.88	111.119.15.0	HTTP	492	52:4e:ce:4b:ca:fd GET /filestreamingservice/files/ec3f42ff-db07-4960-b5	GET /filestreamingservice/files/ec3f42ff-db07-4960-b5
959	0.031513	111.119.15.0	192.168.159.88	HTTP	959	ba:0d:d0:dc:7a:6b HTTP/1.1 206 Partial Content (application/x-chrome-e	HTTP/1.1 206 Partial Content (application/x-chrome-e
492	0.031513	192.168.159.88	111.119.15.0	HTTP	492	52:4e:ce:4b:ca:fd GET /filestreamingservice/files/ec3f42ff-db07-4960-b5	GET /filestreamingservice/files/ec3f42ff-db07-4960-b5
598	0.031513	192.168.159.88	142.250.193.35	HTTP	598	52:4e:ce:4b:ca:fd GET /chrome-variations/seed?osname=win&channel=stable	GET /chrome-variations/seed?osname=win&channel=stable
492	0.031513	192.168.159.88	111.119.15.0	HTTP	492	52:4e:ce:4b:ca:fd GET /filestreamingservice/files/ec3f42ff-db07-4960-b5	GET /filestreamingservice/files/ec3f42ff-db07-4960-b5

Frame 508: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: ba:0d:d0:dc:7a:6b (ba:0d:d0:dc:7a:6b), Dst: 52:4e:ce:4b:ca:fd (52:4e:ce:4b:ca:fd)
Internet Protocol Version 4, Src: 192.168.159.88, Dst: 111.119.15.0
Transmission Control Protocol, Src Port: 51752, Dst Port: 80, Seq: 1, Ack: 1, Win: 0, Len: 0
Hypertext Transfer Protocol