



Mawlana Bhashani Science and Technology University

Lab-Report

Report No: 04

Course code: ICT-4202

Course title: Wireless and Mobile Communication Lab

Date of Performance: 11.09.2020

Date of Submission: 18.09.2020

Submitted by

Name: Wahia Tasnim

ID:IT-16029

4th year 2nd semester

Session: 2015-2016

Dept. of ICT

MBSTU.

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Experiment N0: 04

Experiment Name : Protocol Analysis with Wireshark

Objective :

At the end of this activity, we will be able to:

1. Define protocol analysis.
2. Capture protocols at each TCP/IP Layer.
3. Capture, and identify a TCP connection including handshake and tear down.
4. Identify a DNS request/response session.
5. Generate and record protocol hierarchy statistics for a session.

Defining protocol analysis:

Protocol analysis describes the process of capturing and interpreting live data as it flows across a network in order to better understand what is happening on that network.

Protocol analysis can help us understand network characteristics, learn who is on a network, determine who or what is utilizing available bandwidth, identify peak network usage times, identify possible attacks or malicious activity, and find unsecured and bloated applications.

Capturing protocols at each TCP/IP Layer:

The image displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for various functions. The main window is divided into three panes:

- Packet List Pane:** Shows a list of captured packets. The first packet (No. 1) is selected, showing its details in the packet details pane.
- Packet Details Pane:** Displays the hierarchical structure of the selected packet. It shows the Ethernet II layer, Internet Protocol Version 4 layer, and Transmission Control Protocol layer.
- Packet Bytes Pane:** Shows the raw data of the selected packet in hexadecimal and ASCII format.

The selected packet (No. 1) is a TCP segment of a reassembled PDU. The details pane shows the following information:

- Ethernet II:** Src: HonHaiPr-f8:4a:e9 (60:6d:c7:f8:4a:e9), Dst: Tp-LinkT_99:3e:7e (d8:07:b6:99:3e:7e)
- Internet Protocol Version 4:** Src: 192.168.0.105, Dst: 69.173.159.63
- Transmission Control Protocol:** Src Port: 55197, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

The packet bytes pane shows the raw data of the selected packet, including the Ethernet II header, IP header, and TCP header.

Identifying a TCP connection including handshake:

61	76.368864	192.168.0.105	69.173.159.63	TCP	54	55202 → 443 [ACK] Seq=3 Ack=2 Win=64811 Len=0
62	76.374698	172.217.31.206	192.168.0.105	TCP	66	443 → 55222 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1360 SACK_PERM=1 WS=256
63	76.374786	192.168.0.105	172.217.31.206	TCP	54	55222 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0

Identifying a DNS request/response session:

No.	Time	Source	Destination	Protocol	Length	Info
54	76.279909	192.168.0.105	192.168.0.1	DNS	75	Standard query 0xd267 A www.youtube.com
55	76.318902	192.168.0.105	192.168.0.1	DNS	75	Standard query 0xd267 A www.youtube.com
56	76.348864	192.168.0.1	192.168.0.105	DNS	269	Standard query response 0xd267 A www.youtube.com CNAME youtube-ui.1.google.com A 172.217.31.206 A 172.217.160.1...
57	76.348210	192.168.0.1	192.168.0.105	DNS	269	Standard query response 0xd267 A www.youtube.com CNAME youtube-ui.1.google.com A 172.217.31.206 A 172.217.160.1...
58	76.348713	192.168.0.105	172.217.31.206	TCP	66	55222 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
59	76.368523	69.173.159.63	192.168.0.105	TCP	54	443 → 55202 [ACK] Seq=1 Ack=3 Win=47880 Len=0
60	76.368832	69.173.159.63	192.168.0.105	TCP	54	443 → 55202 [FIN, ACK] Seq=1 Ack=3 Win=47880 Len=0
61	76.368864	192.168.0.105	69.173.159.63	TCP	54	55202 → 443 [ACK] Seq=3 Ack=2 Win=64811 Len=0
62	76.374698	172.217.31.206	192.168.0.105	TCP	66	443 → 55222 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1360 SACK_PERM=1 WS=256
63	76.374786	192.168.0.105	172.217.31.206	TCP	54	55222 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
64	76.375146	192.168.0.105	172.217.31.206	TCP	54	55222 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
Domain Name System (response)						
Transaction ID: 0xd267						
Flags: 0x8100 Standard query response, No error						
Questions: 1						
Answer RRs: 11						
Authority RRs: 0						
Additional RRs: 0						
Queries						
Answers						
[Request In: 54]						
[Time: 0.068155000 seconds]						

Generating protocol hierarchy statistics for a session:

Wireshark · Protocol Hierarchy Statistics · Wi-Fi								
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	547	100.0	158081	7687	0	0	0
Ethernet	100.0	547	4.8	7658	372	0	0	0
Internet Protocol Version 6	1.3	7	0.2	280	13	0	0	0
User Datagram Protocol	1.3	7	0.0	56	2	0	0	0
DHCPv6	1.3	7	0.4	574	27	7	574	27
Internet Protocol Version 4	97.6	534	6.8	10692	519	0	0	0
User Datagram Protocol	10.6	58	0.3	464	22	0	0	0
Simple Service Discovery Protocol	6.6	36	7.6	11950	581	36	11950	581
Domain Name System	4.0	22	0.9	1467	71	22	1467	71
Transmission Control Protocol	86.5	473	78.9	124720	6064	245	25706	1250
Transport Layer Security	41.7	228	74.6	117936	5734	224	104394	5076
Data	0.7	4	0.0	4	0	4	4	0
Internet Group Management Protocol	0.5	3	0.0	52	2	3	52	2
Address Resolution Protocol	1.1	6	0.1	168	8	6	168	8

Conclusion:

In this lab, we learned about protocol analysis with Wireshark. For this we first start capturing data with Wireshark. After that we identify a TCP connection including handshake and also identify a DNS request. At last we generate the protocol hierarchy statistics for this session.