TITLE

Rajdeep Gill 7934493

COURSE CODE SECTION

January 17, 2025

Contents

1 Wireshark Lab: Getting Started

3

1 Wireshark Lab: Getting Started

- 1. The different protocols that appear in the protocol column in the unfiltered packet-listing window are:
 - UDP, TCP, DNS, HTTP, ICMPv6, TLSv1.2, LLC, TLSv1.3,

Some of these packets can be see in Figure 1.

No.	Time ^	Source	Destination	Protocol	Length	Info
Г	1 0.000000	140.193.68.180	142.251.211.228	UDP	123	52636 → 443 Len=81
	2 0.084035	142.251.211.228	140.193.68.180	UDP	68	443 → 52636 Len=26
	3 0.126978	142.251.211.228	140.193.68.180	UDP	1287	443 → 52636 Len=1245
	4 0.126981	142.251.211.228	140.193.68.180	UDP	184	443 → 52636 Len=142
	5 0.129657	142.251.211.228	140.193.68.180	UDP	69	443 → 52636 Len=27
	6 0.129659	142.251.211.228	140.193.68.180	UDP	117	443 → 52636 Len=75
	7 0.143903	140.193.68.180	142.251.211.228	UDP	80	52636 → 443 Len=38
L	8 0.223775	142.251.211.228	140.193.68.180	UDP	68	443 → 52636 Len=26
	9 0.948648	140.193.68.180	130.179.3.145	DNS	77	q, g
	10 0.948802	140.193.68.180	130.179.3.145	DNS	77	Standard query 0xbeeb HTTPS gaia.cs.u
		130.179.3.145	140.193.68.180	DNS		Standard query response 0xbeeb HTTPS
		130.179.3.145	140.193.68.180	DNS		Standard query response 0x0cc6 A gaia
		140.193.68.180	128.119.245.12	TCP		53371 → 80 [SYN] Seq=0 Win=65535 Len=
	14 0.998911	128.119.245.12	140.193.68.180	TCP	66	80 → 53371 [SYN, ACK] Seq=0 Ack=1 Win
	15 0.999101	140.193.68.180	128.119.245.12	TCP		53371 → 80 [ACK] Seq=1 Ack=1 Win=2621
	16 0.999235	140.193.68.180	128.119.245.12	HTTP		GET /wireshark-labs/INTRO-wireshark-f
		128.119.245.12	140.193.68.180	TCP		$80 \rightarrow 53371 [ACK] Seq=1 Ack=591 Win=30$
		128.119.245.12	140.193.68.180	HTTP		HTTP/1.1 304 Not Modified
		140.193.68.180	128.119.245.12	TCP		53371 → 80 [ACK] Seq=591 Ack=240 Win=
	20 1.496157		ff02::1	ICMPv6		Neighbor Advertisement fe80::6011:a72
	21 2.623408	142.251.167.109	140.193.68.180	TCP		993 → 53178 [FIN, ACK] Seq=1 Ack=1 Wi
	22 2.623687		142.251.167.109	TCP		53178 → 993 [ACK] Seq=1 Ack=2 Win=204
	23 2.688968		34.224.149.186	TCP		53359 → 443 [SYN] Seq=0 Win=65535 Len
	24 2.946150	140.193.68.180	34.224.149.186	TCP	78	53360 → 443 [SYN] Seq=0 Win=65535 Len

Figure 1: Packet-listing window

2. The time taken for when the HTTP GET message was sent to when the HTTP OK reply was recieved was 0.04264 seconds. This was calculated by subtracting the time the HTTP GET message was sent from the time the HTTP OK reply was recieved. This can be seen in Figure 2.

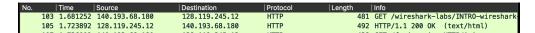


Figure 2: Time taken for HTTP GET message to HTTP OK reply

3. The Internet address of the gaia.cs.umass.edu is 128.119.245.12 and the Internet address of my computer is 140.193.68.100. These addresses are seen in Figure 2.