

Linneuniversitetet Kalmar Växjö

Report

Assignment 1

Author: Yishu Yang Semester: Spring 2024

Email yy222cm@student.lnu.se



Linneuniversitetet Kalmar Växjö

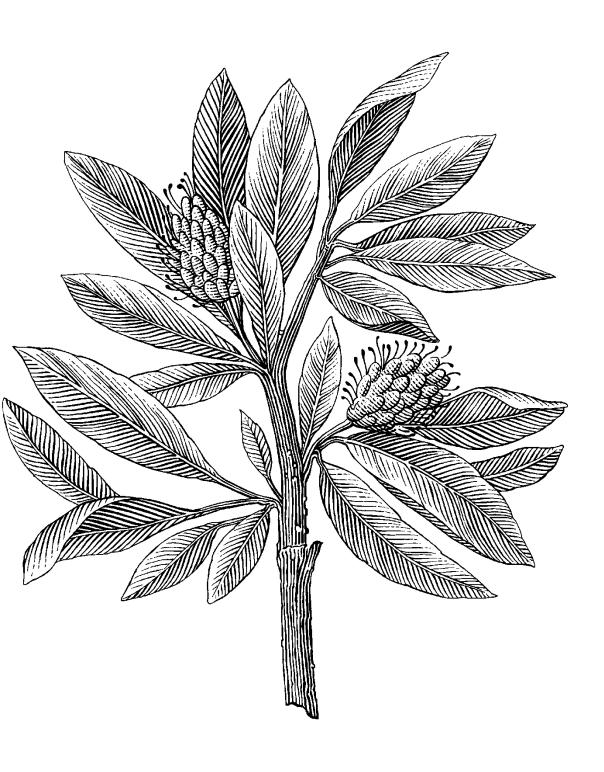


Table of Contents

1	Pro	blem 1	2				
	1.1	Discussion	2				
	1.2	T1-2	2				
	1.2	.1 Discussion	2				
	1.3	Discussion	2				
2	Pro	blem 2	2				
	2.1	Discussion	2				
	2.2	Discussion	3				
3	Pro	blem 3	3				
	3.1	Discussion	3				
4	Pro	blem 4	3				
	4.1	Discussion	3				
	4.2	Discussion	3				
	4.2	Discussion	3				
5	Pro	blem 5	3				
	5.1	Discussion	4				
6	Pro	blem 6	4				
	6.1	Discussion	4				
	6.2	Discussion	4				
	6.3	Discussion	4				
	6.4	Discussion	4				
	6.5	Discussion	4				
R	References						

1 Problem 1

143 5.526873	217.10.96.5	85.195.27.86	DNS	154 Standard query response 0xf96e A www.jd.com CNAME www.jd.com.gslb.qianxun.com CNAME jd-abroad.cdn20.com A 163.171.134.109
144 5.527573	85.195.27.86	163.171.134.109	TCP	66 65074 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
145 5.537830	163.171.134.109	85.195.27.86	TCP	66 80 → 65074 [SYN, ACK] Seq=0 Ack=1 Win=56940 Len=0 MSS=1460 SACK_PERM WS=128
146 5.537921	85.195.27.86	163.171.134.109	TCP	54 65074 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
147 5.537989	85.195.27.86	163.171.134.109	TCP	54 65074 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
148 5.551065	163.171.134.109	85.195.27.86	TCP	60 80 → 65074 [FIN, ACK] Seq=1 Ack=2 Win=56960 Len=0
149 5.551153	85.195.27.86	163.171.134.109	TCP	54 65074 → 80 [ACK] Seq=2 Ack=2 Win=131328 Len=0
150 5.568764	151.252.181.174	224.0.0.251	MDNS	123 Standard query 0x0000 ANY Android.local, "QU" question ANY Android.local, "QU" question A 151.252.181.174 AAAA fe80::5a20:59ff:
151 5.571804	119.28.35.248	85.195.27.86	TCP	60 443 → 65072 [ACK] Seq=151 Ack=758 Win=64128 Len=0
152 5.571804	119.28.35.248	85.195.27.86	TLSv1.2	123 Application Data

1.1 Discussion

Several protocols include DNS, TCP, MDNS, and TLSv1.2. 1. TCP, or Transmission Control Protocol, is a communication standard that enables application programs and computing devices to exchange messages over a network.[1] 2. TLSv1.2, or Transport Layer Security 1.2, is simply an upgraded form of TLS 1.1. TLS 1.2 offers improved security and is designed for high performance and reliability.[2] 3.DNS, or Domain Name System, is a hierarchical and distributed naming system for computers, services, and other resources on the Internet.[3] 4. MDNS, or multicast DNS, resolves hostnames to IP addresses within small networks that do not include a local name server.[4]

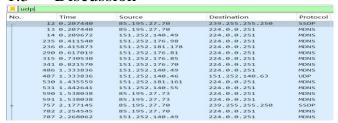
1.2 T1-2

The Socie	Definition	Free Jugil ris	i w				Da A das				
59359 5538	E.233.25	10 11 EM + 23 (60) (Section of College of Co	± k 1 k	Sauce	Seturin	trad leaf his	No.	Time	Source	Destination	Protocol Lengt Info
			1378 (5.290)	98: :39504e	SL 1902 (1)	DS K Stated per, 6699 Leed took, "Of pestin		86785 324.112758	85,195,27,86	8.8.8.8	DNS 83 Standard query Boble? A sladitor.oxi.office.net
			3378 45.398	146 (3954)4s	9, 102:03	IN A Social per (67); Leed		86/84 3/4,122413	85,195,27,85	217,36,96,5	UNS US Standard overv Deribe A minditor.osi.office.net
ESTATEM ESTATE	15.25.35.35	[6] SER -20 [0] Spill ANSER UNRER and SPRINGS SHORE.	330 10.188	980 0385436	au fifty stat	no Normani pary resto a red		BH502 568,055365	85.195.27.86	217.10.96.5	2015 70 Standard query Behalt: A way, jid.com.
BONNESSO ELGICE	D. 20.700 JE	TO 14 EDM + 20 (40) Explict A ref2/EDM LindSUBM (and	SE6 47.480	58: 0305430	all filtration	50 Surard pay rode and		80438 357,889408	85.195.27.86	217,18.96.5	005 73 Standard query Bridge A very taids, com
SSS NUSSES ELSIEN	28.28.25.29	SP STARTINELL	2008 (17.90)	(46) (31650) k	8L 182 (18	NO NO. and per, facts lead	- 1	97266 510,367667	85,195,27,86	217.10.06.5	265 78 Standard query Belli 87 A. y Englisystems
836 NJ 68% EC 12.00.4	38.85.50	80° 3219091901	2108 (0.100)	146 (31450) by	St. 1992 (I)	DS - X Stated yes, 6699 Described, "Off yestin	- 3	92484 337,485582	85.195.27.86	217.10.96.5	065 74 Standard query Bis/Feld A view-tacheo.com
ESCRIGOS ELICIDAD	20120	IDNO Shakedis Facility as 23.64.20	143K (C.H.E.)	58: :38:540:	3L 182 : 6	DG - R Starter By any 66900 A sack local, "Off practice	1	99776 334.616922	85,195,27,88	217.10.96.5	265 75 Standard query Bel624 A redictablysacion
ESPERIOS ELIQUAD	28.36.79	65 Street my 668 Pf Journal Majorial, No potini 68, pink patholical, 31 portini	200 65 850	580 (00544)	3L 182 : 6	DG K Started pery (e/R) Livert local, "Of parties	1	85871 321.075668	85.195.27.86	217.10.36.5	565 76 Standard query Belief LA statuspylogoccae
25930.689 E.GUNZ		\$5. Extraced are record \$600 RE with, to bold \$100, and fluid into Planchal RE, and fill		586 (\$650 b)	8L 182 cft	DS — Without pay 6690 Lestiloid, "Of patie	1	85352 315.831660	85.195.27.86	217.10.16.5	265 73 Standard quary Bebd2a A assets.min.co
E39 N/601 S/2 E2 E		No. Heinbele	3191 61.536	546 (58550)	8L 180 cca	NA A Started gray refer Lived		75248 249, 153458	85,195,27,86	217,10,16,5	905 93 Standard query 8x334 A extension fenetrics grammer
230 34 000 ELECTR		NGI (Deployee)	3432 45.8334	1961 (30) 5404 (6	9, 192 (23	BN N School per, 6639 Lond		75246 299.137458		217.10.96.5	365 90 Standard quary 0x648c A config.extension.grammarly.
ESCHOOL SCHOOL		DAL STRAIGHEAN	- 306 45 3023	96 (3950)	96, 982 (2.0)	IN A State of party for School and	1	71457 291,410501	85.195.27.86	217.10.16.5	365 86 Standard query 8x116x A statistics.s2-publishment
				Secretario	at 180 cost	per Richard and restricted	1	67993 283,459010	85.195.27.86	217.16.96.5	DNS 82 Standard quary Br85cd A diy-front.cdn.huya.com
238 M 6621 6.23 5/6	12.22.20.00	TO 15 EDR + 20 [40] Explict 4 (402500) alresting (and	283 93.500	Security Sta	a. fftz :ft	po 8 resired and restrict varieties of austin	- 1	67712 283.039371	85.195.27.88	217.10.96.5	265 73 Standard query Relica A ylog.hoya.com
ESPERIOR ENGINE	2167.2	16 13 E + 300 [24, 47] 36-21 40-32 tr-312 tr-4		-8: :34504x		DS X Societ any 6600 Seed load. "Of media	1	63647 272,73629E	85.195.27.85	217.10.96.5	DRS 70 Standard quary Bridgle A notric huya, com
ESSESSIONE \$1.0 FR.M.	8.682.6	Bid. Eleptionie in		-W-345Us		DS 18 Sept day, 6600 PS signal on majors, "No opcin-	1	60624 266.771973	85,195,27,86	217.10.96.5	DRS 76 Standard quary Bradf6 A vev. jd.com
838 NL683 E.SEE	D1.22.701.00	TO SEEDS AND TOO SENSE AND SENSE WAS SENSE OF SE		68 - 114 Ch		NAME OF TAXABLE PARTY AND ADDRESS OF TAXABLE PARTY.		54411 264 465925	85, 295, 27, 85	217.18.96.5	1805 Hr Standard mone Swittle & Dightstee, kniggs swidin com

1.2.1 Discussion

In the capture package of assignment1.2, we can see there are a total of 381516 frames (upper left screenshot of the last record) and 51 of them use IPv6 (upper middle screenshot by filter of IPv6), which means there are 427 IPv4 conversations and 3 IPv6 conversations. When we add the filter of DNS, a substantial amount of IP source address is 85.195.27.86, which is the IP address of the DNS server I am connected to. (upper right screenshot). Explain: Currently most DNS servers are still using IPv4 more than IPv6 because IPv6 is expensive and lacks compatibility. Additionally, people don't favor IPv6 because others don't favor it. The DNS server assigns me this IP address to help locate my computer with a virtual address.

1.3 Discussion



After adding the filter of UDP, some protocols like SSDP, MDNS, and UDP appear. From question 1-1 we have introduced the MDNS. So now: 1. SSDP, or Simple Service Discovery Protocol, is for advertisement, the discovery of network services, and present information.[5]

2. UDP, or User Datagram Protocol, sends messages (transported as datagrams in packets) to other hosts on an Internet Protocol (IP) network.

2 Problem 2

2.1 Discussion

The IP address of my machine is 85.195.27.86 and the IP address of the destination machine is 128.119.245.12. (Picture 1) I have observed that there are a total of 2 HTTP request messages when surfing that website and each of them has a response message, (Picture 2) where the second one is related to 404 Not Found.

per hose-55 KSZ Misor Ing							Status Code: 200 [Status Code Description: OK] Response Phrase: OK Date: Fri, 02 Feb 2024 00:10:20 GMT\r\n	Status Code: 404 [Status Code Description: Not Found]
No.	Time	Source	Destination	Protoc	ol Lengt Info	Consequent Machiner's (common of servy seets) payagement provide (Miny, has locally offers) Arrest: territory, angle first including high Testimorian (A.), (angle for finged high, haspidess), (Miny Arrest Conseque; at the Chiphyte (A. prepint), provide (A. president), (A. prepint), angle for fine (A. prepint), and (A	Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fip Last-Modified: Thu, 01 Feb 2024 06:59:02 GMT\r\n	
+	1771 68.226548	85.195.27.86	128,119,245,12	HTTP	573 GET /váreshark-labs/HTTP-váreshark-file1.html HTTP/1.1		ETag: "80-6104c87ceec5c"\r\n Accept-Ranges: bytes\r\n	Server: Apache/2.4.6 (CentOS) OpenSSL/1.6 V Content-Length: 209\r\n
	1921 68.683274	85.195.27.86	128.119.245.12	HTTP	519 GET /Favicon.ico HTTP/1.1		∨ Content-Length: 128\r\n [Content length: 128]	[Content length: 209]

2.2 Discussion

The first response message is no.1809, the status code is 200, the content length is 128 and the modified last time is Thu, 01 Feb 2024 06:59:02 GMT\r\n. The second response message is no.1953, status code is 404 representing not found, content length is 209 and no modified last time but the only date is Fri, 02 Feb 2024 00:10:20 GMT\r\n because of 404 not found. Status codes indicate whether a specific HTTP request has been completed.[6] The Content-Length indicates the size of the message body, in bytes, sent to the recipient.[7] The Last-Modified contains a date and time when the origin server believes the resource was last modified.[8]

3 Problem 3



3.1 Discussion

The connection of the GET request is kept alive and the response message has the same origin, where the last-modified can be traced back to 06 Feb 2024 and it has only an answer of OK. It means despite multiple downloads of this file, the server will send one complete copy only once due to IN-MODIFIED-SINCE in your HTTP GET request to the server, where Last-Modified does not change.

4 Problem 4



4.1 Discussion

There is only one request packet from the client to the server. But it is broken into 4 pieces of TCP segments and reassembled when the receiver receives the package. The first three segments have a length of 1460 and the last one has 481, hence the total length is 4861. This is because the Maximum Segment Size of TCP is 1460.

4.2 Discussion

When sending HTTP long files supported by TCP, TCP breaks the file into smaller segments, known as packets. These packets are then transmitted individually and reassembled by the receiving end.

4.2 Discussion

The 1st response package has status code 200 and the reason phrase "OK", which indicates that the request has succeeded. The 2nd response package has status code 404 and the reason phrase "Not Founded", which indicates the browser can communicate with a given server, but the server can't find what is requested.[9]

5 Problem 5

	11398 77.863365	user86.85-195-27.ne… gaia.cs.umass.edu HTTP	589 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
4	11425 77.967605	gaia.cs.umass.edu user86.85-195-27.ne HTTP	771 HTTP/1.1 401 Unauthorized (text/html)
	12018 94.920944	user86.85-195-27.ne gaia.cs.umass.edu HTTP	674 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
	12020 95.026242	gaia.cs.umass.edu user86.85-195-27.ne HTTP	544 HTTP/1.1 200 OK (text/html)
	12034 95.356077	user86.85-195-27.ne gaia.cs.umass.edu HTTP	535 GET /favicon.ico HTTP/1.1
	12044 95.457871	gaia.cs.umass.edu user86.85-195-27.ne HTTP	538 HTTP/1.1 404 Not Found (text/html)

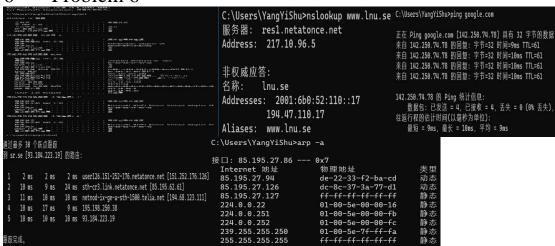
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n Credentials: wireshark-students:network

Upgrade-Insecure-Requests: 1\r\n

5.1 Discussion

Interesting observation: There are two consecutive requests for page contents and the response to the 1st one is "401 Unauthorized", whereas the 2nd one is "200 OK" for confirmation of correct username and password. Explanation: the client requests for the page contents. Since there are no valid authentication credentials yet for the requested resources, the server responds with "401 Unauthorized". Then the client requests again with input of valid credentials. After getting authorization by receiving the username and password, the server responds with "200 OK". Finally, the client asks for the image of the icon. Although the server received the request but did not find any icon, it replied with "404 Not Found". Problem: HTTP is not like HTTPS and isn't secure since if someone else uses Wireshark to capture the package of this HTTP transfer containing existing authorization of the credential data, he/she can get all the information of the username and password and access the website maliciously.

6 Problem 6



6.1 Discussion

The first command displays the full TCP/IP network configuration for all adapters. Here Windows IP and all network connections are shown, whereas all other networks are unconnected but only WLAN is connected. You can get all the information about the IPv4 address, DHCP server, default gateway, and DNS server.

6.2 Discussion

The second command displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Detailed information on www.lnu.se is about its server's name, network addresses, and aliases. This website is our university's website.

6.3 Discussion

The third command sends data to a specific IP address on the network, letting me know how long it takes to transmit the data and get a response. Here we ping www.google.com. There are four trials to connect to Google and send back the transmit time with an average of 10ms.

6.4 Discussion

The fourth command determines the path taken to a destination by sending ICMPv6 messages to the destination with incrementally TTL field values. Here the destination is sr.se and undergoes 5 routers to find the path.

6.5 Discussion

The last command displays the ARP cache tables for all interfaces. Here are 8 Internet addresses connected to my IP address with also physical addresses. Some are dynamic and some are static.

References

- 1. https://www.fortinet.com/resources/cyberglossary/tcp-ip#:~:text=Transmission%20Control%20Protocol%20(TCP)%20is,data%20and%20messages%2 Oover%20networks.
- 2. https://blog.gigamon.com/2021/07/14/what-is-tls-1-2-and-why-should-you-still-care/
- 3. https://en.wikipedia.org/wiki/Domain_Name_System
- $4. \qquad \underline{https://en.wikipedia.org/wiki/Multicast_DNS\#:\sim:text=In\%20computer\%20networking\%2}\\ C\%20the\%20multicast,Domain\%20Name\%20System\%20(DNS).$
- 5. https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol
- 6. https://developer.mozilla.org/en-US/docs/Web/HTTP/Status
- 7. <u>https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Length</u>
- 8. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Last-Modified
- 9. https://en.wikipedia.org/wiki/HTTP_404