Linnéuniversitetet
Kalmar Växjö

Report

Assignment 1

1DV701

Author: Yishu Yang
Semester: Spring 2024
Email yy222cm@student.lnu.se

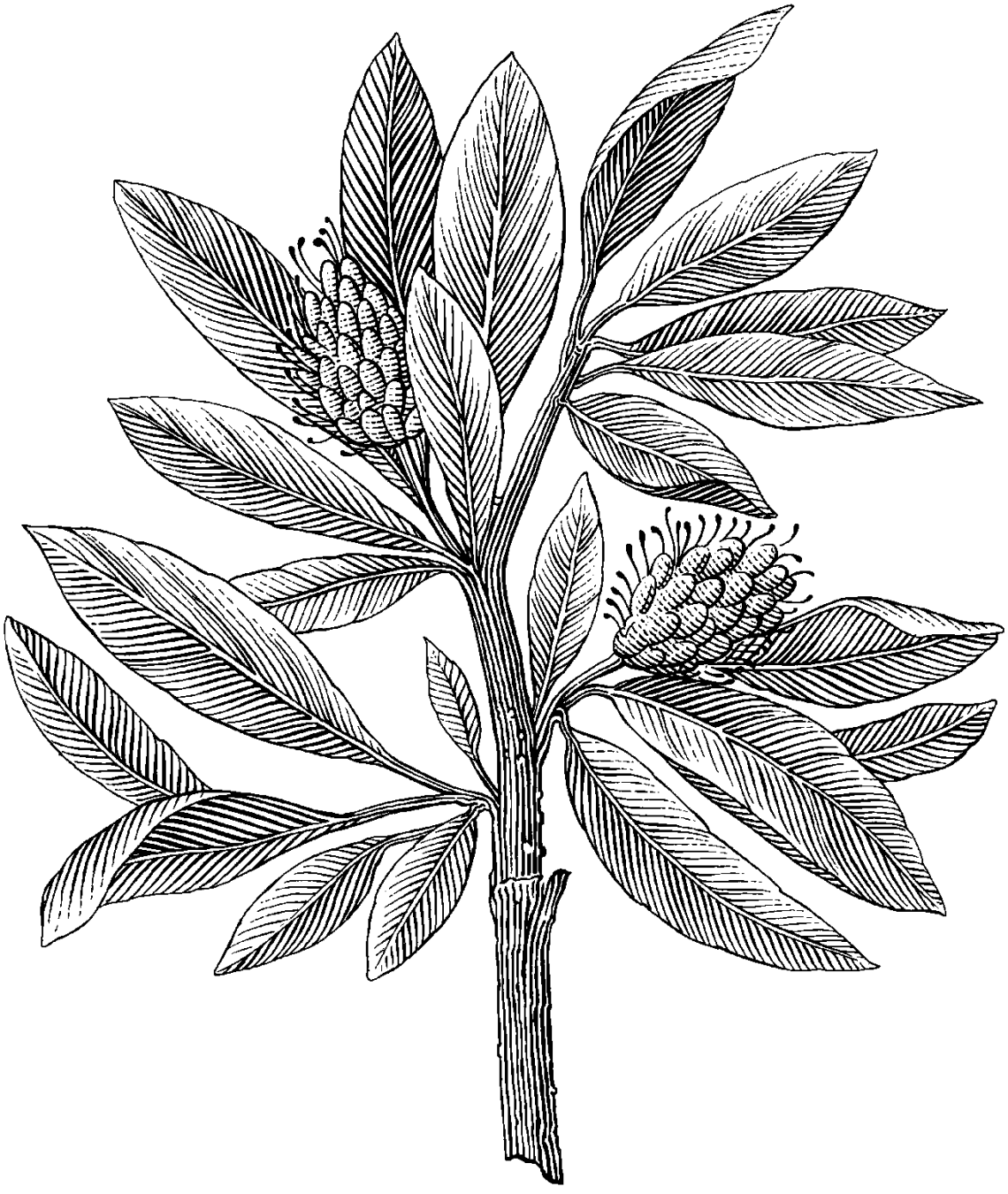


Table of Contents

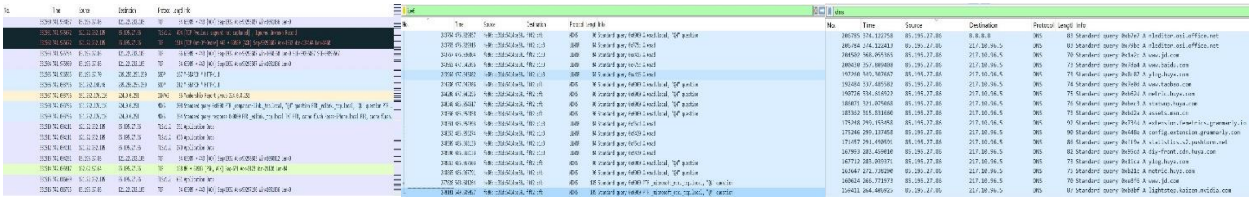
1 Problem 1

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



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

udp

No.	Time	Source	Destination	Protocol
12	0.207440	85.195.27.70	239.255.255.250	SSDP
13	0.207440	85.195.27.70	224.0.0.251	MDNS
14	0.209672	151.252.140.49	224.0.0.251	MDNS
235	0.411540	151.252.176.98	224.0.0.251	MDNS
236	0.415873	151.252.181.178	224.0.0.251	MDNS
290	0.617019	151.252.176.81	224.0.0.251	MDNS
315	0.730530	151.252.176.85	224.0.0.251	MDNS
341	0.821570	151.252.176.70	224.0.0.251	MDNS
486	1.333836	151.252.140.49	224.0.0.251	MDNS
487	1.333836	151.252.140.46	151.252.140.63	UDP
530	1.435559	151.252.181.161	224.0.0.251	MDNS
531	1.442641	151.252.140.55	224.0.0.251	MDNS
590	1.538038	85.195.27.73	224.0.0.251	MDNS
591	1.538038	85.195.27.73	224.0.0.251	MDNS
757	2.177145	85.195.27.70	239.255.255.250	SSDP
782	2.254545	85.195.27.70	224.0.0.251	MDNS
787	2.268062	151.252.140.49	224.0.0.251	MDNS

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. (Picture1) 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.

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

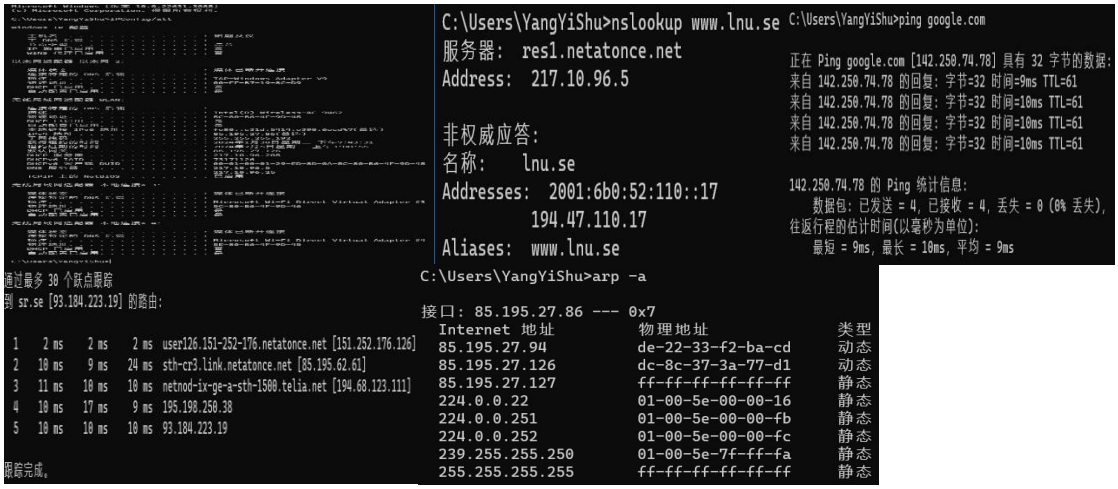
The 1st response package has status code 200 and the reason phrase “OK”, which indicates that the request has succeeded. The 2nd response package has status code 404 and the reason phrase “Not Founded”, which indicates the browser can communicate with a given server, but the server can’t find what is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

5 Problem 5

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%20over%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. https://en.wikipedia.org/wiki/Multicast_DNS#:~:text=In%20computer%20networking%2C%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. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Length
8. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Last-Modified
9. https://en.wikipedia.org/wiki/HTTP_404