Linnéuniversitetet
Kalmar Växjö

Report

Assignment 1

1DV701

Author: Katarina Simakina
Semester: Spring 2023
Email es225hi@student.lnu.se

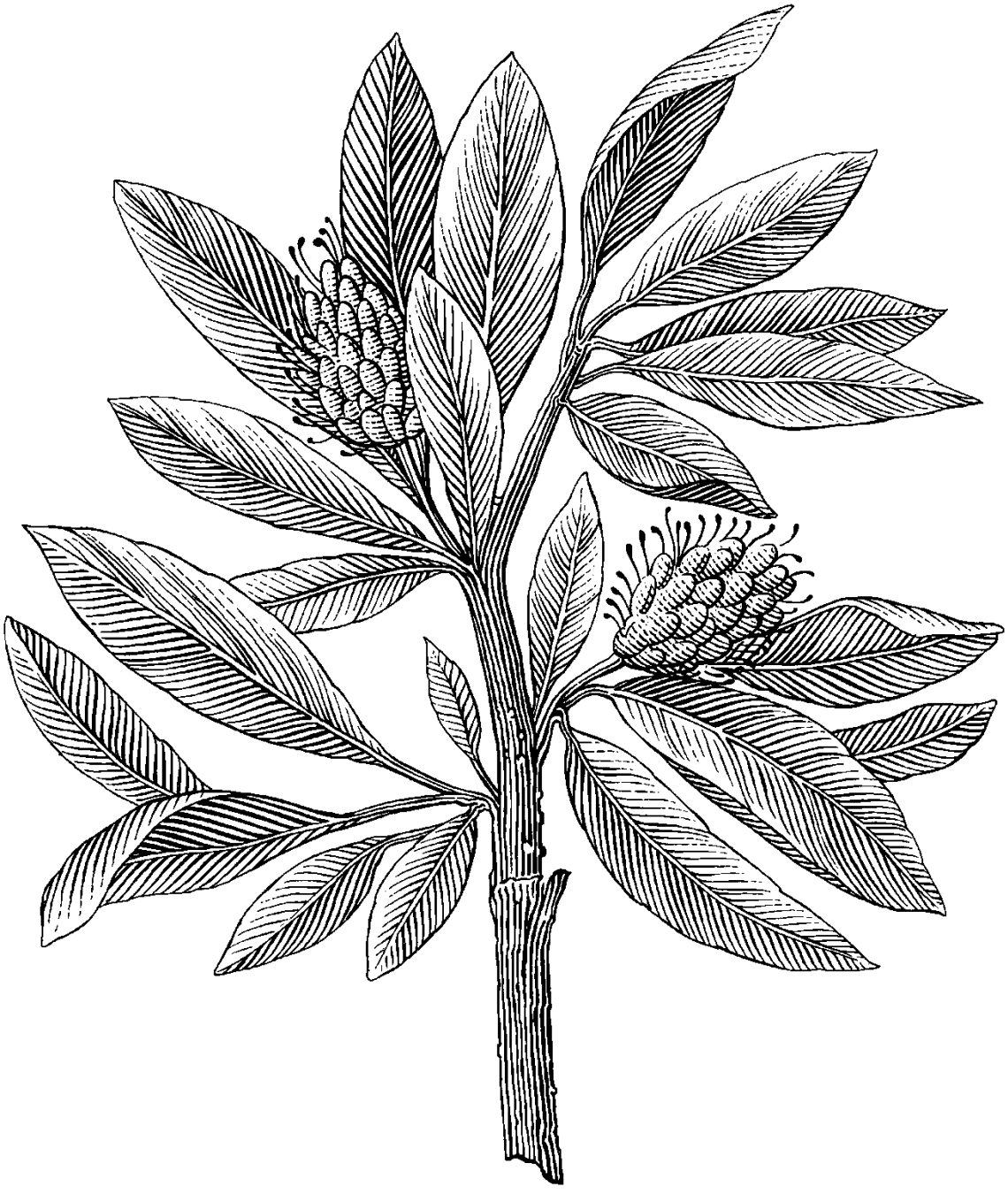


Table of Contents

Problem 1 2
- 1.1 Discussion 2
- 1.2 Discussion 2
- 1.3 Discussion 2

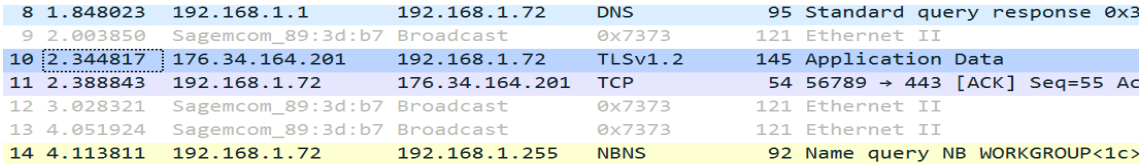
Problem 2 3
- 2.1 Discussion 3
- 2.2 Discussion 3

Problem 3 3
- 3.1 Discussion 3

Problem 4 4
- 4.1 Discussion 4
- 4.2 Discussion 4
- 4.3. Discussion 4

Problem 5 4
- 5.1 Discussion 4

1 Problem 1



8	1.848023	192.168.1.1	192.168.1.72	DNS	95	Standard query response 0x3
9	2.003850	Sagemcom_89:3d:b7	Broadcast	0x7373	121	Ethernet II
10	2.344817	176.34.164.201	192.168.1.72	TLSv1.2	145	Application Data
11	2.388843	192.168.1.72	176.34.164.201	TCP	54	56789 → 443 [ACK] Seq=55 Ac
12	3.028321	Sagemcom_89:3d:b7	Broadcast	0x7373	121	Ethernet II
13	4.051924	Sagemcom_89:3d:b7	Broadcast	0x7373	121	Ethernet II
14	4.113811	192.168.1.72	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1c>

1.1 Discussion

T1-1

The following protocol listed in the protocol window in my system:

TCP (Transmission Control Protocol) is a connection-oriented protocol for communications. It is located between application and Network Layers. Using this protocol delivery service is reliable. This protocol helps in the exchange of messages (data) between different devices over a network.

DNS (Domain Network System) is a standard protocol which allows users to access websites using human-readable addresses. DNS allows users to enter the address of a website and automatically determine its IP address, that is, the unique identifier of a particular device (server) in a computer network.

TLSv1.2 (Transport Layer Security (TLS) 1.2) is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet. TLS ensures that each message is sent with Message Authentication Code.

NBNS (NetBIOS Name Service NBNS) is a protocol which translates human-readable names into IP addresses, can only provide IPv4 addresses and it does not support IPv6. It can work over several different network protocols (example IP, IPX, ...).

0x7373 is a protocol used by the device manufacturer or an ISP for periodic broadcast traffic. For example, ISP's specialists can access special parts of the device management interface via a special application or a Manufacturer uses this protocol to prevent their proprietary control, discovery, etc. traffic from being mixed with client traffic.

1.2 Discussion

T1-2

I got more IPv4 than IPv6. IPv4 is approx. 110, IPv6 is approx. 12, total is 122. DNS is 192.168.1.72

There is a different amount of IPv4 and IPv6 conversations. Firstly, in 2011 the Internet officially ran out of IPv4 addresses, so IPv6 was created. Secondly, IPv4 showed up reason is application of NAT technology in IPv4. IPv6 does not support NAT which allows to use one IP address on thousands of devices. In top of it, ISPs don't want to switch to a new protocol as IPv4 can manage with tasks as well old user devices also do not support IPv6.

DNS server is used as when a user enters the name of a site in the browser's address bar for example google.com, then the computer requests the IP address of this site on a special DNS server, after receiving the correct answer, it opens the site. A DNS server is a specialized computer (or group) that stores the IP addresses of websites. That is DNS server is used to match website hostnames to their suitable IP addresses.

1.3 Discussion

T1-3

The following protocols after typing "udp":

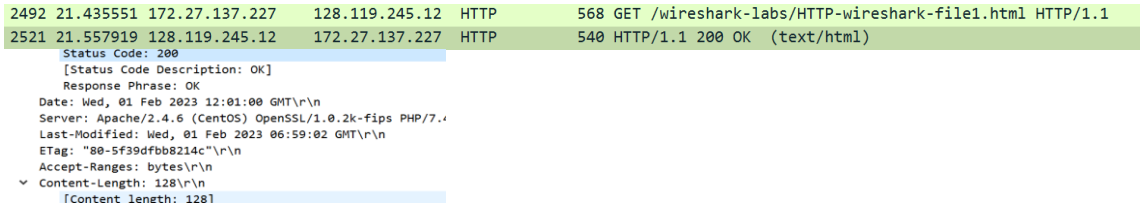
DNS (Domain Network System). It finds websites using hostnames instead using numeric IP addresses.

SSDP (Simple Service Discovery Protocol). It is used in in small networks. It discovers Plug & Play devices.

ICMP (Internet Control Message Protocol) helps determine if a packet can reach its destination within a specified time frame. It is used to diagnose network connectivity problems.

MDNS protocol converts hostnames to IP addresses on small networks.

2 Problem 2



2.1 Discussion

T2-1

IP address of my machine 172.27.137.227 and the destination machine 128.119.245.12

I have observed in the HTTP request message the following things: there is an exchange of data between the client and the server. That is, the client sends a request to trigger an action on the server, and the server sends a response.

2.2 Discussion

T2-2

The following details of the HTTP response message:

Status code: 200 (successful). Status code shows HTTP request has been done successfully or not, it gives some informational responses (100 – 199) Successful responses (200 – 299) Redirection messages (300 – 399) Client error responses (400 – 499).

Content length: 128. Content length indicates the size of entity-body in decimal and sent it to the recipient. Briefly, it is the number of bytes of data in the body of the request or response.

Modified last time: Wed, 01 Feb 2023 06:59:02 GMT. It is a date which refers to the last time a document or media file was modified.

3 Problem 3

3.1 Discussion

T3-1

HTTP GET request is sent to the server and here are the important fields in the packet.

Request Method: GET. It means that the packet is a HTTP GET. Request URI: /wireshark-labs/HTTP-wireshark-file2.html It means that the client . That it the client is asking the file HTTP-wireshark-file2.html User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 That it is client side browser type.

Response message: version of the protocol is HTTP/1.1 It has status code: 200. It means successful message. Status message (code description) is OK. Last modified: Wed, 01 Feb 2023

06:59:02 GMT, it is the date when file has been modified. As well the server returned the contents of the file as the contents of the message in the Line-based text data.
Communication between clients and servers is going by exchanging individual messages. The Client sends the message via Web browser, it is request. Server gives answer, it is response.

4 Problem 4

```
3141 8.603835  172.27.137.227   128.119.245.12  HTTP        568 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
3170 8.722035  128.119.245.12   172.27.137.227  HTTP        826 HTTP/1.1 200 OK  (text/html)
```

4.1 Discussion

T4-1

My browser sent 1 request packet.
The packet length defines the size of the whole packet: header, trailer, the data the packet length is the size of the captured frame.

4.2 Discussion

T4-2

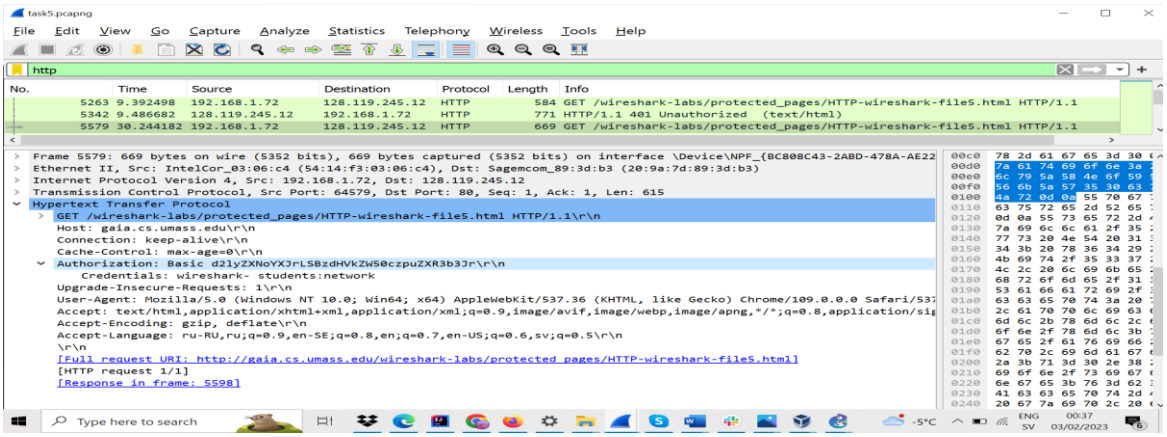
All HTTP communications take place using TCP/IP. TCP provides HTTP with a reliable bit channel (bytes inserted into one side of a TCP connection come out from the other side in the correct order). HTTP transmits a message over a TCP connection. TCP receives the data, cuts the data in segments and sends in IP packets over the Internet.

4.3 Discussion

T4-3

In HTTP-response contains status code is a number and response phrase. In my case is Packet 3170; status code: 200; response phrase: OK. Status code gives information how HTTP request has been done (for example 200-299 successful response, 300 -399 redirection response etc); response phrase is status but in text which gives conclusion of the status code. For example, “method not allowed” or “OK” etc.

5 Problem 5



5.1 Discussion

T5-1

Entering username and password didn’t allow me to open this data (file) as my connection to this site is not private. On my request to open HTTP-wireshark-file5.html I got response where it was status code: 401. It means that client error responses my request has not been completed as no valid authentication credentials. Response phrase: Unauthorized It means, I need to authenticate itself to get the requested response.
There are problems with the password protection. Username and password are not encrypted. (They are encoded in a format (Base64) but not encrypted).