Linnéuniversitetet
Kalmar Växjö

Report

Assignment 1

1DV701

Author: Melat Haile
Semester: Spring 2021
Email: mh225ic@student.lnu.se

Linnéuniversitetet
Kalmar Växjö

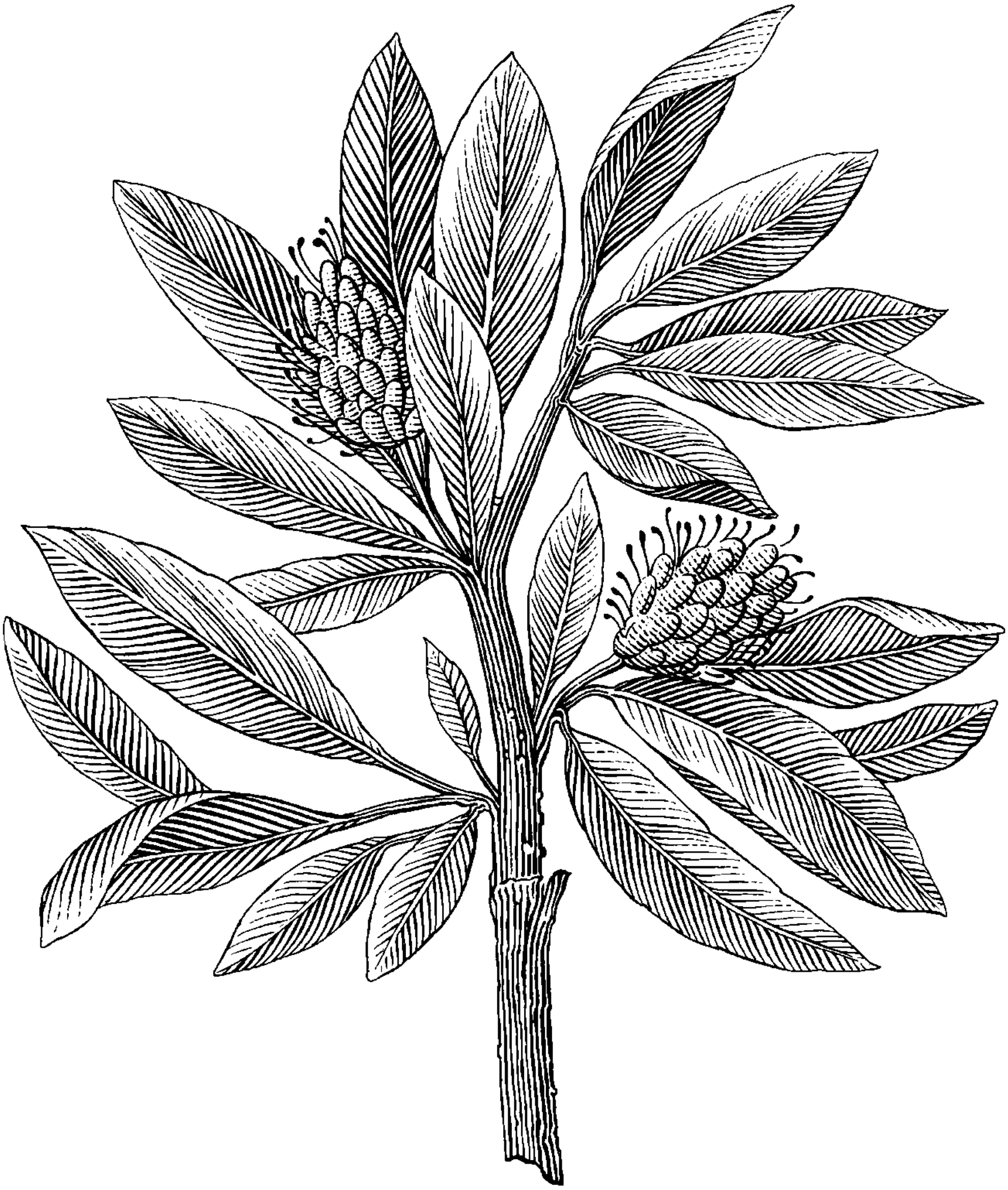
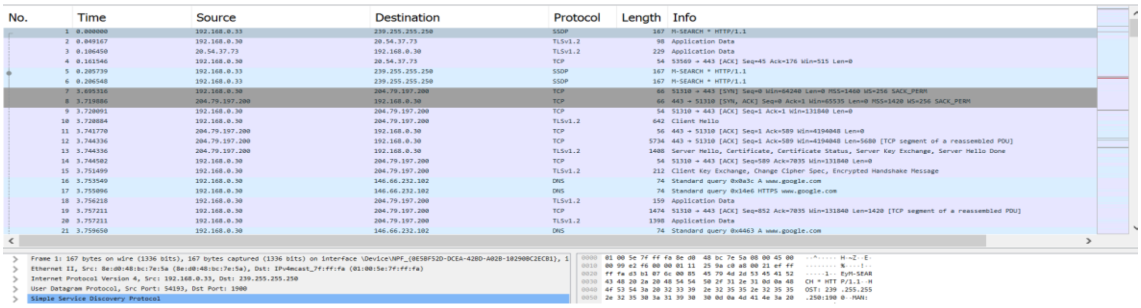


Table of Contents

Problem 1

T1-1



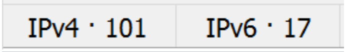
```
No.  Time      Source          Destination      Protocol  Length  Info
  1  0.000000  192.168.0.33    239.255.255.250  SSDP         167  M-SEARCH * HTTP/1.1
  2  0.049167  192.168.0.30    20.54.37.73      TLSv1.2       98  Application Data
  3  0.106450  20.54.37.73     192.168.0.30     TLSv1.2      229  Application Data
  4  0.161546  192.168.0.30    20.54.37.73      TCP           54  53569 → 443 [ACK] Seq=45 Ack=176 Win=515 Len=0
  5  0.205739  192.168.0.33    239.255.255.250  SSDP         167  M-SEARCH * HTTP/1.1
  6  0.206548  192.168.0.33    239.255.255.250  SSDP         167  M-SEARCH * HTTP/1.1
  7  3.695316  192.168.0.30    204.79.197.200   TCP           66  51310 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  8  3.719886  204.79.197.200  192.168.0.30     TCP           66  443 → 51310 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 WS=256 SACK_PERM
  9  3.720091  192.168.0.30    204.79.197.200   TCP           54  51310 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
 10  3.720884  192.168.0.30    204.79.197.200   TLSv1.2      642  Client Hello
 11  3.741770  204.79.197.200  192.168.0.30     TCP           56  443 → 51310 [ACK] Seq=1 Ack=589 Win=4194048 Len=0
 12  3.744336  204.79.197.200  192.168.0.30     TCP         5734  443 → 51310 [ACK] Seq=1 Ack=589 Win=4194048 Len=5680 [TCP segment of a reassembled PDU]
 13  3.744336  204.79.197.200  192.168.0.30     TLSv1.2     1408  Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
 14  3.744502  192.168.0.30    204.79.197.200   TCP           54  51310 → 443 [ACK] Seq=589 Ack=7035 Win=131840 Len=0
 15  3.751499  192.168.0.30    204.79.197.200   TLSv1.2      212  Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 16  3.753549  192.168.0.30    146.66.232.102   DNS           74  Standard query 0x0a3c A www.google.com
 17  3.755096  192.168.0.30    146.66.232.102   DNS           74  Standard query 0x14e6 HTTPS www.google.com
 18  3.756218  192.168.0.30    204.79.197.200   TLSv1.2      159  Application Data
 19  3.757211  192.168.0.30    204.79.197.200   TCP         1474  51310 → 443 [ACK] Seq=852 Ack=7035 Win=131840 Len=1420 [TCP segment of a reassembled PDU]
 20  3.757211  192.168.0.30    204.79.197.200   TLSv1.2     1398  Application Data
 21  3.759650  192.168.0.30    146.66.232.102   DNS           74  Standard query 0x4463 A www.google.com
```

```
> Frame 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF_{0E5BF52D-DCEA-428D-A02B-102908C2ECB1}, 1
> Ethernet II, Src: 8e:d0:48:bc:7e:5a (8e:d0:48:bc:7e:5a), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.0.33, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 54193, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 8e d0  48 bc 7e 5a 08 00 45 00   ··^····· H·~Z··E·
0010  00 99 e2 f6 00 00 01 11  25 9a c0 a8 00 21 ef ff   ········ %····!··
0020  ff fa d3 b1 07 6c 00 85  45 79 4d 2d 53 45 41 52   ·····l·· EyM-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN: 
```

SSDP advertises and discovers network services and presence information. **TLSv1.2** is the latest version of the SSL protocol, featuring new cipher suites using the SHA-256 algorithm. **TCP** is a reliable delivery and connection protocol for applications at the transport layer. **DNS** maps host names to IP addresses in a client-server model.

T1-2



IPv4 · 101 IPv6 · 17

In this experiment, the DNS server used has IP address 192.168.0.30. This server is utilized because modern routers often act as caching name servers for local networks. The IP address, 192.168.0.30, is the internal address of the client's router, which will either forward the DNS queries to the DNS server configured by the client's ISP or resolve it from the router's cache.

There are currently more IPv4 conversations compared to IPv6 because IPv4 has been around since the early days of the Internet, and has been widely adopted and deployed. It has a much larger address space and has proven to be a reliable and flexible protocol.

On the other hand, IPv6 is a newer protocol that was introduced to address the depletion of IPv4 addresses. While it offers many benefits over IPv4, such as a much larger address space, improved security, and enhanced mobility, it has not yet been widely adopted. This is due to several factors, including the cost and complexity of upgrading existing networks, compatibility issues with older devices and systems, and the lack of incentives for organizations to upgrade.

T1-3

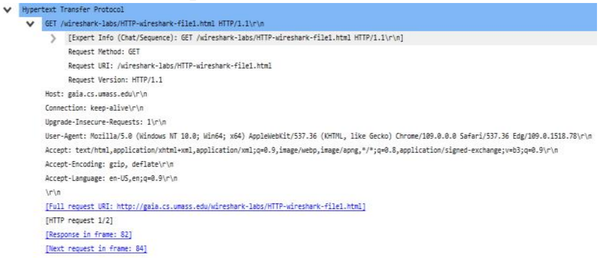
After searching for the term "udp," various protocols were identified that use the User Datagram Protocol (UDP). These include:

- DNS, used for converting domain names to IP addresses.
- QUIC, a fast and secure internet transport protocol.
- MDNS, for name resolution in local networks
- SSDP, for discovering UPnP devices.
- DHCPv6, for assigning IP addresses and network configurations.
- LLMNR, for name resolution in local networks.
- NBNS, for name resolution in Windows-based networks.
- DHCP, for assigning IP addresses and network configurations.
- ICMP, used to send error and status messages and to test network connectivity.

Problem 2

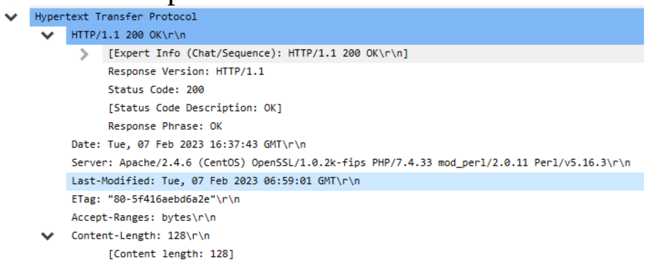
IP Address of the machine: **192.168.0.30**
IP Address of the destination: **128.119.245.12**

HTTP Get Request



```
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    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 Edg/109.0.1518.78\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 82]
    [Next request in frame: 84]
```

HTTP Response



```
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Tue, 07 Feb 2023 16:37:43 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 07 Feb 2023 06:59:01 GMT\r\n
    ETag: "80-5f416aebd6a2e"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
        [Content length: 128]
```

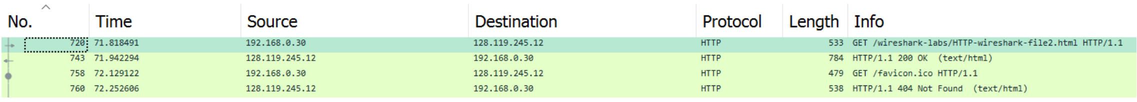
T2-1

A request message was observed with the following details: the request method was a "GET," the request URL was "/wireshark-labs/HTTP-wireshark-file1.html," the request version was "HTTP/1.1," the host was "gaia.cs.umass.edu," and the user-agent was identified as "Mozilla/5.0."

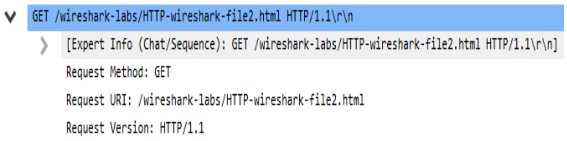
T2-2

Response Version: HTTP/1.1, Status Code: 200, Status Code Description: OK, Response Phrase: OK
The response version indicates the protocol version, which is "HTTP/1.1"; the content-length value of "128 bytes" denotes the length of the message for the receiver; and the last adjustment time and date is "Tue, 07 Feb 2023 06:59:01 GMT," according to the origin server.

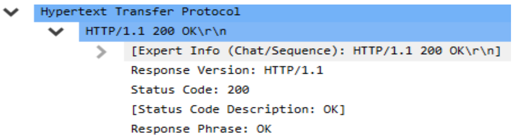
Problem 3



No.	Time	Source	Destination	Protocol	Length	Info
720	71.818491	192.168.0.30	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
743	71.942294	128.119.245.12	192.168.0.30	HTTP	784	HTTP/1.1 200 OK (text/html)
758	72.129122	192.168.0.30	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
760	72.252606	128.119.245.12	192.168.0.30	HTTP	538	HTTP/1.1 404 Not Found (text/html)



```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
```

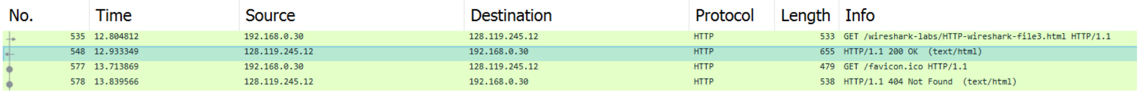


```
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
```

T3-1

A GET request was sent to a web address with the target webpage and the protocol version "HTTP/1.1". The "HOST" is listed as "http://gaia.cs.umass.edu" and the "User-Agent" specifies information about the browser and system being used. The response from the server indicated a successful conversation with the "Response Version" as "HTTP/1.1" and a "Status Code" of 200. Communication between a client (browser) and server involves a request and response process. It was noted that the content length in this instance was 371 bytes, larger than what was seen in task 2.

Problem 4



No.	Time	Source	Destination	Protocol	Length	Info
535	12.804812	192.168.0.30	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
548	12.933349	128.119.245.12	192.168.0.30	HTTP	655	HTTP/1.1 200 OK (text/html)
577	13.713869	192.168.0.30	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
578	13.839566	128.119.245.12	192.168.0.30	HTTP	538	HTTP/1.1 404 Not Found (text/html)

T4-1

During the observation, two request packet was sent from the client to the server. There were 4 reassembled TCP segments, due to the document being larger than the MTU of 1500 bytes in the experimental environment. The header size was observed to be 20 bytes, meaning the data payload must have been less than 1500 bytes at 1363 bytes. Based on the initial observation, the size of the original document was determined to be 4805, which equals 1363 * 3 + 716. This confirms the accuracy of the above observations.

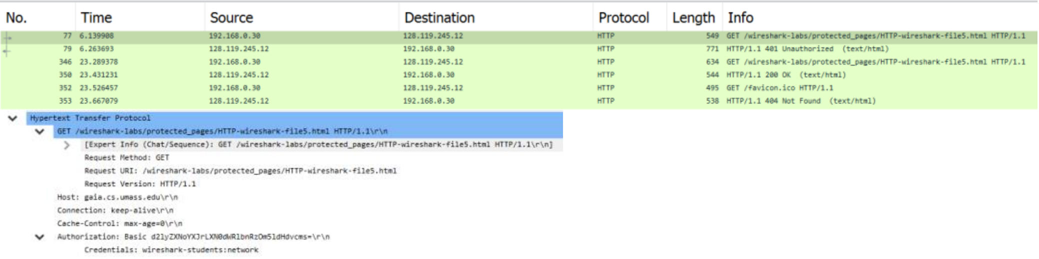
T4-2

HTTP and TCP work together to support the transfer of large files. HTTP sends requests for files, while TCP provides a reliable connection to transfer the file in small packets. The packets are guaranteed to be received in the correct order and any lost packets are retransmitted to ensure a successful transfer. This process enables HTTP to support large files.

T4-3

In this observation, a GET request was made and the response was "200 OK", indicating that the requested resource was successfully retrieved and included in the message body. However, another request returned a "404 NOT FOUND" response, indicating that the server couldn't find the requested resource.

Problem 5



No.	Time	Source	Destination	Protocol	Length	Info
77	6.139908	192.168.0.30	128.119.245.12	HTTP	549	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
79	6.263693	128.119.245.12	192.168.0.30	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
346	23.289378	192.168.0.30	128.119.245.12	HTTP	634	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
350	23.431231	128.119.245.12	192.168.0.30	HTTP	544	HTTP/1.1 200 OK (text/html)
352	23.526457	192.168.0.30	128.119.245.12	HTTP	495	GET /favicon.ico HTTP/1.1
353	23.667079	128.119.245.12	192.168.0.30	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
        Credentials: wireshark-students:network
```

T5-1

During this observation, the client tried to access a password-protected website and was initially denied access with a "401 Unauthorized" response from the server. After entering the correct username and password, the client was granted access with a "200 OK" response from the server.

However, the website's security was found to be lacking as it used the HTTP protocol instead of the more secure HTTPS protocol and sent sensitive information like the username and password in the GET request, which is not encrypted and visible to anyone monitoring the conversation. This practice is dangerous and not recommended for sensitive data.