Linnéuniversitetet
Kalmar Växjö

Report

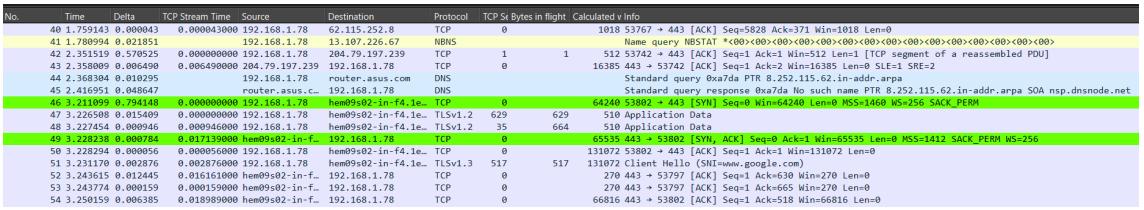
Assignment 1 - Wireshark

1DV701

Author: Benoit Dervieux
Semester: Spring 2024
[redacted]

Table of Contents

1 Problem 1 - Basic information about TCP/IP protocol



No.	Time	Delta	TCP Stream Time	Source	Destination	Protocol	TCP St	Bytes in flight	Calculated v	Info
40	1.759143	0.000043	0.000043000	192.168.1.78	62.115.252.8	TCP	0		1018	53767 → 443 [ACK] Seq=5828 Ack=371 Win=1018 Len=0
41	1.780994	0.021851		192.168.1.78	13.107.226.67	NBNS				Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
42	2.351519	0.570525	0.000000000	192.168.1.78	204.79.197.239	TCP	1	1	512	53742 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
43	2.358009	0.006490	0.006490000	204.79.197.239	192.168.1.78	TCP	0		16385	443 → 53742 [ACK] Seq=1 Ack=2 Win=16385 Len=0 SLE=1 SRE=2
44	2.368304	0.010295		192.168.1.78	router.asus.com	DNS				Standard query 0xa7da PTR 8.252.115.62.in-addr.arpa
45	2.416951	0.048647		router.asus.c…	192.168.1.78	DNS				Standard query response 0xa7da No such name PTR 8.252.115.62.in-addr.arpa SOA nsp.dnsnode.net
46	3.211099	0.794148	0.000000000	192.168.1.78	hem09s02-in-f4.1e…	TCP	0		64240	53802 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
47	3.226508	0.015409	0.000000000	192.168.1.78	hem09s02-in-f4.1e…	TLSv1.2	629	629	510	Application Data
48	3.227454	0.000946	0.000946000	192.168.1.78	hem09s02-in-f4.1e…	TLSv1.2	35	664	510	Application Data
49	3.228238	0.000784	0.017139000	hem09s02-in-f…	192.168.1.78	TCP	0		65535	443 → 53802 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
50	3.228294	0.000056	0.000056000	192.168.1.78	hem09s02-in-f4.1e…	TCP	0		131072	53802 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
51	3.231170	0.002876	0.002876000	192.168.1.78	hem09s02-in-f4.1e…	TLSv1.3	517	517	131072	Client Hello (SNI=www.google.com)
52	3.243615	0.012445	0.016161000	hem09s02-in-f…	192.168.1.78	TCP	0		270	443 → 53797 [ACK] Seq=1 Ack=630 Win=270 Len=0
53	3.243774	0.000159	0.000159000	hem09s02-in-f…	192.168.1.78	TCP	0		270	443 → 53797 [ACK] Seq=1 Ack=665 Win=270 Len=0
54	3.250159	0.006385	0.018989000	hem09s02-in-f…	192.168.1.78	TCP	0		66816	443 → 53802 [ACK] Seq=1 Ack=518 Win=66816 Len=0

1.1 Different protocols listed

The different protocols are: DNS, HTTP, LLMNR, MDNS, NBNS, SSDP, TCP, TLS. Here are some definitions:
DNS: Domain Name System, translates a domain name into an IP address to locate websites. Here, they are used as UDP packets. [1]
HTTP: Hypertext Transfer Protocol. Communication protocol to receive HTML pages. [2]
MDNS: Multicast DNS, gives special IP addresses to devices on the local network without registering them on DNS servers. [3]
TCP: Transmission Control Protocol. Communication protocol that allows the exchange of messages over a network. Ensures successful delivery of data transfer. [4]
TLS (v1.2 and v1.3): Transport Layer Security. Encrypts data securely over a network. Provide secure communication between two endpoints. [5]

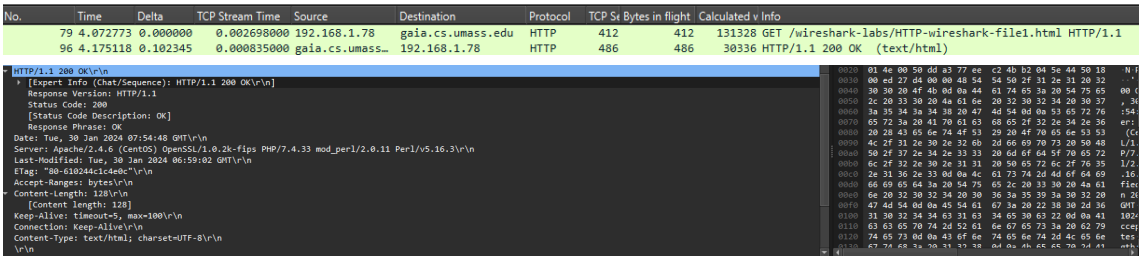
1.2 20 minutes of web browsing

Number of IPv4 conversations: 22. Number of IPv6 conversations: 1.
IPv4 of the DNS: 192.168.1.1
The reason why there is a fewer amount of IPv6 conversations compared to IPv4 is because IPv4 is still widely used in comparison to IPv6. [6]
The DNS server translates a domain name into an IP address to establish a conversation. [1]

1.3 UDP as a display filter

Protocol used for UDP: DNS, MDNS, NBNS, SSDP. They have in common that they are discovering services or names in networks and enable the communication from a domain name to a router and from a router to the world wide web. They allow fast and connectionless communication and improve the experience of accessing content on the web. [7]

2 Problem 2 - Basic information about HTTP



No.	Time	Delta	TCP Stream Time	Source	Destination	Protocol	TCP St	Bytes in flight	Calculated v	Info
79	4.072773	0.000000	0.002698000	192.168.1.78	gaia.cs.umass.edu	HTTP	412	412	131328	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
96	4.175118	0.102345	0.000835000	gaia.cs.umass…	192.168.1.78	HTTP	486	486	30336	HTTP/1.1 200 OK (text/html)

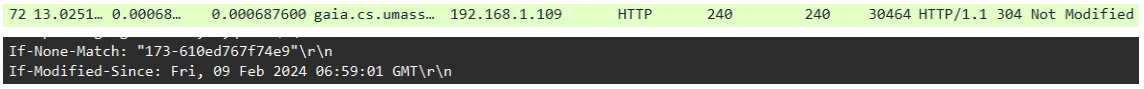
2.1 HTTP request message

My IP address : 192.168.1.78. Gaïa's IP address: 128.119.245.12
We can notice that the communication is between the website and my IP address. It uses a GET request to retrieve data from servers targeting a specific resource. [8]

2.2 HTTP response message

Status code: 200. Content length : 128. Last modified: Tue, 30 Jan 2024 06:59:02 GMT. This status code means that the server has accepted the request. The content length is the number of characters inside the document. Here, it concerns the number of characters. The last-modified section corresponds to the date and time when the requested resource was last modified on the server. [9][10][11]

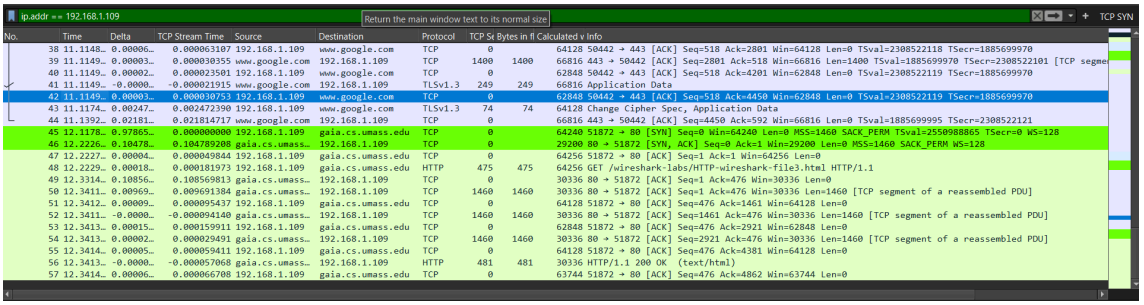
3 Problem 3 - GET request/response interaction



3.1 GET request and response message

Using Opera on Linux, there is an HTTP response of “304 Not modified” which indicates that the information inside the website wasn't modified since the last time that same request was made. The field “If-Modified-Since” replaced the last-modified field previously present.[12]

4 Problem 4 - Getting longer document



4.1 Request packets

Using Opera on Linux, we notice that the value of Maximum Segment Size of 1460 has been set up between IP addresses during the handshake. The client makes a GET request. The sender sends 3 packets of 1514 bytes and 1 of 481 bytes with an HTTP 200 OK response. The client sends an ACK back for every packet.

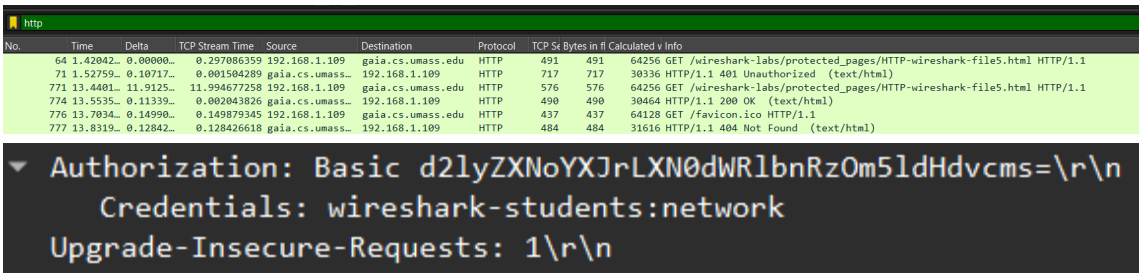
4.2 Understanding of HTTP long file

From my observations, the client first sends a GET request asking for the specific file. Then the server sends back package by package depending on the MSS. Here, it is 1514 as we have the Ethernet header (14 bytes), IP header (20 bytes), TCP header (20 bytes) and the payload/MSS (1460 bytes). The transaction finishes by an HTTP 200 OK response in charge of reassembling the different packages that have been sent. [13]

4.3 Status code

By analyzing the response, one can see that Wireshark displays the content of the document. This indicates that the entire document has been reassembled at reception using the packets corresponding to different frames. This is an interpretation made by Wireshark. [14]

5 Problem 5 - Getting a password over HTTP



5.1 Observations

The process: The client makes a GET request to the server. The server answers with an HTTP/1.1 401 unauthorized and a WWW-Authenticate: Basic is included. This means the client has to reformulate a new GET request with the credentials attached (Username and password) encoded in Basic64. The server responds with an HTTP response 200 by providing the content of the page. [15] [16]
The disturbing element here are the credentials. They are accessible in Wireshark. This pinpoints that this protocol is not secure and the information is not encrypted. The password can easily get caught by hackers.

6 Problem 6 - Basic network commands

6.1 IPConfig/all

The ipconfig/all command reveals and manages the IP addresses of the computer on the network such as: IP address, Mac address, IP address of the Gateway, the DHCP server's address, the subnet's Mask, the IP address of the DNS servers. [17] Results in appendix.

6.2 Nslookup

Nslookup helps discover IP addresses and DNS records. [18]
www.lnu.se sends back the address and name of the router that asks for the IPv4 and IPv6 addresses of www.lnu.se.
The results were: Addresses: 2001:6b0:52:110::17 and 194.47.110.17.

6.3 Ping

Ping is used to test a network connectivity from a client to a server. Ping (on windows) sends 4 packets and waits for a response in order to determine the connectivity. [19]
Writing "ping google.com" gave 4 replies with a 0% loss and an average response time of 17ms.

6.4 Tracert

Tracert (Traceroute) lists all the hops that separate a device's IP source to a website's IP destination. It also displays the time to access resources. [20] Screenshot in the appendix.

6.5 Arp -a

arp -a command displays the ARP table. It is a list of IP and MAC addresses that has recently communicated with the computer. Those entries have been registered after resolution of their IP address to their MAC address. [21]

Reference

1. What is DNS? How Domain Name System works : https://www.techtarget.com/searchnetworking/definition/domain-name-system
2. Definition of HTTP | PCMag : https://www.pcmag.com/encyclopedia/term/http
3. Definition of mDNS | PCMag : https://www.pcmag.com/encyclopedia/term/mdns
4. https://www.fortinet.com/resources/cyberglossary/tcp-ip : https://www.fortinet.com/resources/cyberglossary/tcp-ip
5. What is TLS & How Does it Work? - Internet Society : https://www.internetsociety.org/deploy360/tls/basics/
6. IPv4 vs IPv6: What's The Difference Between the Two Protocols? : https://kinsta.com/blog/ipv4-vs-ipv6/
7. What is the User Datagram Protocol (UDP)? | Cloudflare : https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/
8. 7 HTTP methods every web developer should know and how to test them : Assertible. : https://assertible.com/blog/7-http-methods-every-web-developer-should-know-and-how-to-test-them#:~:text=GET%20requests%20are%20the%20most,list%20of%20all%20available%20users
9. HTTP Status Code 200: What Is the 200 "OK" Response?. : https://www.clickminded.com/status-code-200/#:~:text=HTTP%20Status%20Code%20200%3A%20The,given%20the%20client%20the%20documents
10. Content-length header behavior in a streaming rewrite action : https://docs.netscaler.com/en-us/citrix-adc/current-release/appexpert/rewrite/content-length-header-behaviour.html#:~:text=Content-Length%20header%20is%20one,Chunked%20encoding
11. Last-Modified - HTTP | MDN : https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Last-Modified
12. HTTP 304 Not Modified, Explained in 500 Words or Less. : https://blog.hubspot.com/marketing/http-304-not-modified#:~:text=An%20HTTP%20304%20not%20modified%20status%20code%20means%20that%20the,repeatedly%20download%20the%20same%20information
13. MTU Troubleshooting on Cisco IOS : https://networklessons.com/cisco/ccie-routing-switching/pppoe-mtu-troubleshooting-cisco-ios
14. 7.8. Packet Reassembly : https://www.wireshark.org/docs/wsug_html_chunked/ChAdvReassemblySection.html
15. 401 Unauthorized Error: What It Is & How to Fix It. : https://www.dreamhost.com/blog/401-unauthorized-error/#:~:text=401%20errors%20occur%20when%20a,Outdated%20cookies%20or%20browser%20cache
16. HTTP authentication : https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication
17. Definition of IPCONFIG | PCMag : https://www.pcmag.com/encyclopedia/term/ipconfig
18. https://www.hostinger.com/tutorials/what-is-nslookup : https://www.hostinger.com/tutorials/what-is-nslookup
19. Ping - Definition and details : https://www.paessler.com/it-explained/ping
20. What is Traceroute: What Does it Do & How Does It Work? : https://www.fortinet.com/resources/cyberglossary/traceroutes
21. ARP Commands - javatpoint. : https://www.javatpoint.com/arp-commands#:~:text=arp%20-a%3A%20This%20command%20is,as%20the%20arp%20-a%20command

Appendix

Problem 6.1:

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : Laptop-de-Beubeu
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
```

Problem 6.4:

```
C:\Users\user>tracert sr.se

Tracing route to sr.se [93.184.223.19]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  router.asus.com [192.168.1.1]
  2     1 ms     1 ms     1 ms  gw5.A240.priv.bahnhof.se [79.136.15.1]
  3     *        *        *     Request timed out.
  4     3 ms     3 ms     1 ms  a240-wetternet-bahnhof-gw.bahnhof.net [46.59.118.48]
  5    30 ms     7 ms    10 ms  46.59.113.32
  6     8 ms     8 ms     7 ms  sto.cr4.sto1-p1.se.bahnhof.net [46.59.112.84]
  7     6 ms    10 ms     6 ms  sto5-er1.se.bahnhof.net [85.24.220.18]
  8    20 ms     6 ms    13 ms  ae-105.border1.skm.edgecastcdn.net [152.195.244.210]
  9    10 ms     7 ms     8 ms  ae-65.core1.ska.edgecastcdn.net [152.195.244.129]
 10    16 ms    15 ms     8 ms  93.184.223.19

Trace complete.
```

Problem 6.5:

```
Interface: 192.168.1.78 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           0c-9d-92-b1-34-cc     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```