Lab1 Report
Wireshark (HTTP & DNS)

Albin Zahnér
Bingcheng Chen
Christian Lind

January 31, 2023

Chalmers University of Technology
Computer communication - EDA344

1 Task 1

(a) The IP-address of the computer used was 10.0.68.177 and the IP-address for the server was 129.119.245.12

(b) The http version used to download the HTML file was http/1.1. The status code that was returned was 200 with the phrase "ok".

(c) Looking at the accepted languages, the browser sends "sv,en;q=0.9,en-GB;q=0.8,en-US;q=0.7". What this means is that the computer accepts languages in Swedish and English for the US and Great Britain. For another student we instead got "en,zh-CN;q=0.9,zh;q=0.8,sv;q=0.7". Here the difference is that the computer also accepts Chinese. The last time the file was modified is Fri, 27 Jan 2023 06:59:01 GMT and the size of the file is 128 bytes.

2 Task 2

(a) The If-Modified-Since HTTP header indicates the time for which a browser first downloaded a resource from the server. Since the browser hasn't downloaded a resource, thus there isn't an If-Modified-Since header line in the first HTTP GET request.

(b) The server explicitly returned the content of the file, as we can see in figure 1, the response received from the server contains all the content list in the browser.

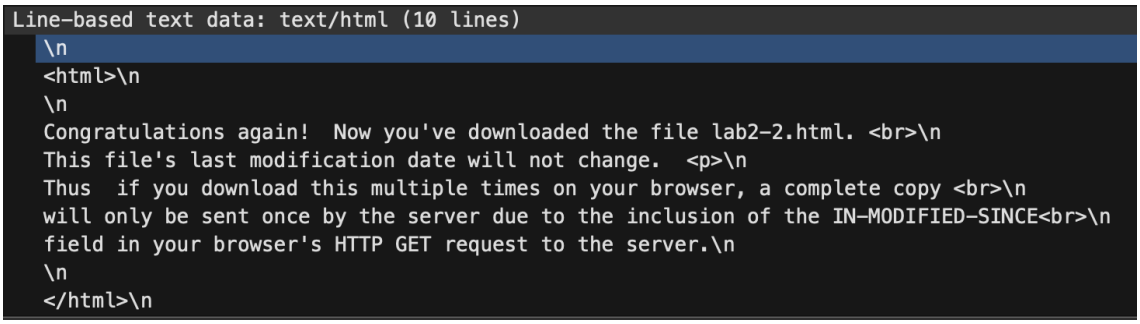

Figure 1: Line-based text data of the HTTP response from the server

(c) There is an If-Modified-Since header line in the HTTP GET message in the content of the second HTTP GET request. the information follows the If-Modified-Since header is "Fri, 27 Jan 2023 06:59:01 GMT\r\n".

Figure 2: If-Modified-Since header line in the second HTTP GET message

(d) The If-Modified-Since header determines if the resource has changed since last accessed. In our case, the file we access from the server will not change, resulting in a "304 Not

Modified" HTTP status code and phrase, indicating that the file has not changed and there is no need to download it again to improve efficiency.

3 Task 3

(a) The browser sends three GET requests. The first two are sent to the server containing the HTML file as well as the first image (128.119.245.12). The third request is sent to another server that contains the second image (178.79.137.164).

No.	Time	Source	Destination	Protocol	Length	Info
189	23:40:04.291422	192.168.0.176	128.119.245.12	HTTP	562	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
194	23:40:04.488575	128.119.245.12	192.168.0.176	HTTP	1367	HTTP/1.1 200 OK (text/html)
197	23:40:04.511319	192.168.0.176	128.119.245.12	HTTP	508	GET /pearson.png HTTP/1.1
204	23:40:04.553459	192.168.0.176	178.79.137.164	HTTP	475	GET /8E_cover_small.jpg HTTP/1.1
206	23:40:04.579696	178.79.137.164	192.168.0.176	HTTP	237	HTTP/1.1 301 Moved Permanently
221	23:40:04.629001	128.119.245.12	192.168.0.176	HTTP	781	HTTP/1.1 200 OK (PNG)

Figure 3

(b) From figure 3, we can see that the client requested for the second image before it finished download the first image, thus we got the conclusion, the two image were downloaded from the two web servers in parallel.

4 Task 4

(a) Using NSlookup on the website gov.za (the South African government website) we get the IP-address 163.195.1.225.

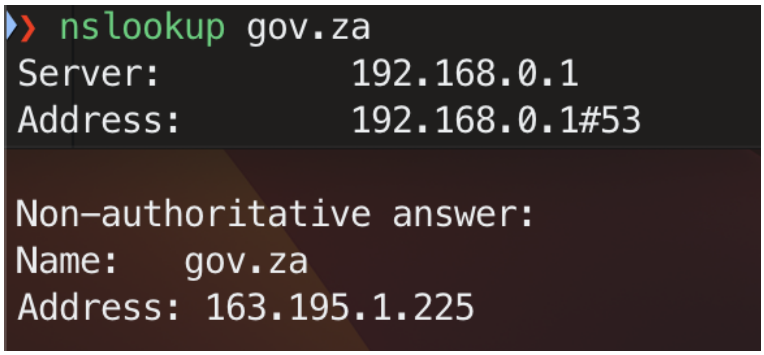

Figure 4: nslookup command for a Web server in Africa

(b) For the mail-server we found the address "unicamp.br" belonging to the State University of Campinas in Brazil.

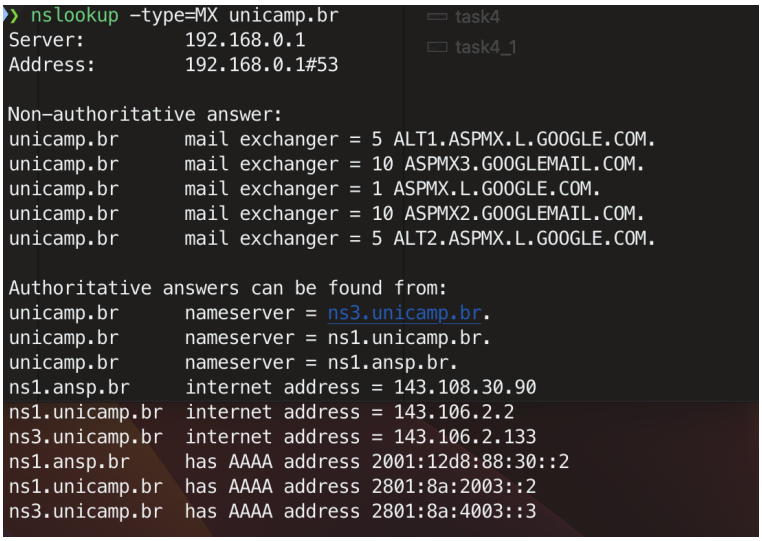

Figure 5: mail servers for the State University of Campinas in Brazil

(c) A nameserver responsible for svt.se is "nsa.dnsnode.net".

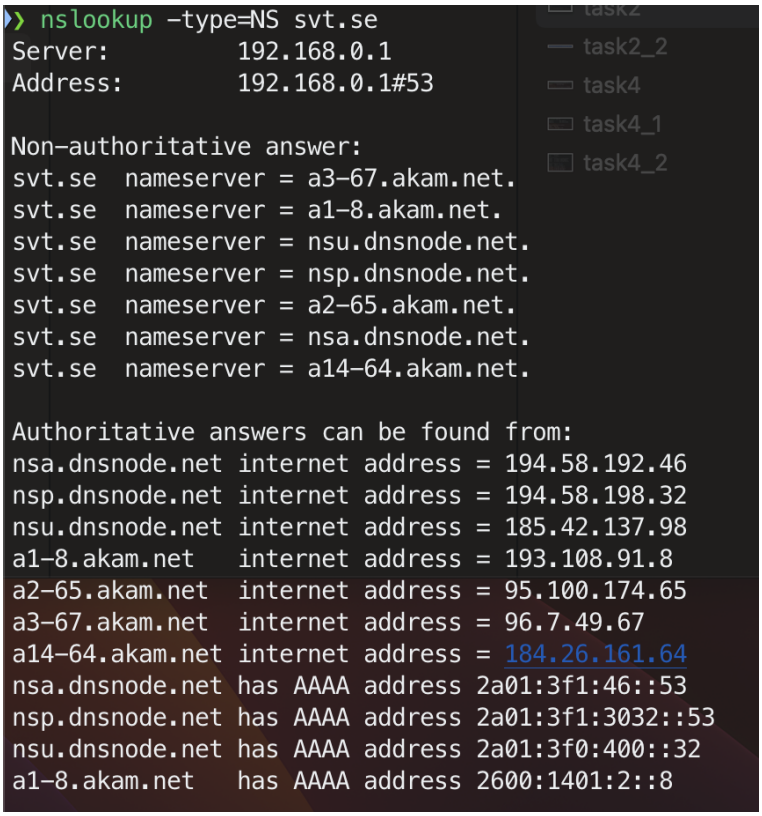

Figure 6: Name servers in charge of svt.se.

(d) NSlookup returns with the response "server can't find amazon.com: REFUSED". This is because the DNS contains no records on what ip-address amazon.com has.

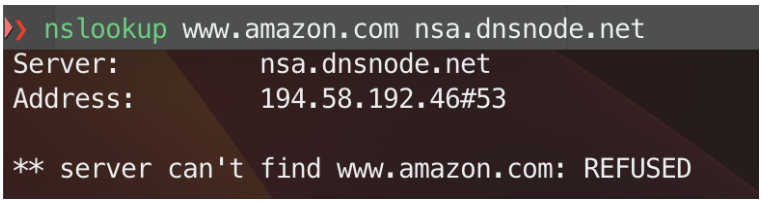

Figure 7: Query 'www.amazon.com' on a nameserver in charge of 'svt.se'

5 Task 5

(a) nslookup -type=NS gov.za 192.36.148.17

(b) nslookup -type=NS gov.za 204.61.216.55

(c) nslookup -type=NS gov.za 163.195.128.13

(d) nslookup gov.za 163.195.1.153

6 Task 6

(a) The filter applied is "dns && ip.addr==192.168.0.176"

(b)
- The DNS query and response messages are transported using UDP. This is because UDP is much faster, and also DNS requests are tiny in size and fit well within UDP segments, despite UDPs lack of reliability. Reliability can be added at the application layer with a timeout and resend mechanism.
- The destination port for the DNS query message is 53, the source port of DNS response message is 53 too.
- The IP address the DNS query message sent is '192.168.0.1'. This is the ip address of local DNS server.

(c) DNS query and response messages have the same format, they both consists of a 12 bytes header section (which contains Identity, Flags, Questions, Answer RRs, Authority RRs, Additional RRs). For DNS query messages, it contains Queries section, For DNS response messages, it contains Queries, Answer, Authoritative nameservers and Additional records section, and some sections may be empty.

The "type" of DNS query used here is "A".

(d) The host's DNS client didn't issue new DNS queries, since the image's domain is the same as the web page domain.

(e) When the page is reloaded, Wireshark cannot capture new DNS messages due to the IP address being stored in DNS cache after the initial query, eliminating the need for a second DNS query for the hostname's IP address.

7 Task 7

(a) The canonical name for "www.tue.nl" is "web.w3.tue.nl.", the IP addresses returned is 49.12.16.43.

The DNS response message contains 5 sections. The first 12 bytes is the **header section**, it contains Identity(identify the query, help matching the received responses with corresponding queries), Flags(Attributes of the message), Questions, Answer RRs, Authority RRs, Additional RRs respectively indicate the number of occurrences of the four sections after the header section.
The **Queries section** contains the information about the query.
The **Answers section** contains the resource records for the name that was originally queried.
The **Authoritative nameservers** section contains records of other authoritative servers.
The **Additional records section** contains other helpful records.

```
❯ nslookup www.tue.nl
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
www.tue.nl      canonical name = web.w3.tue.nl.
Name:   web.w3.tue.nl
Address: 49.12.16.43
```

Figure 8: nslookup command

```
▾ Domain Name System (response)
    Transaction ID: 0xe8a6
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 4
    Additional RRs: 8
  ▾ Queries
    › www.tue.nl: type A, class IN
  ▾ Answers
    › www.tue.nl: type CNAME, class IN, cname web.w3.tue.nl
    › web.w3.tue.nl: type A, class IN, addr 49.12.16.43
  ▾ Authoritative nameservers
    › w3.tue.nl: type NS, class IN, ns ns-424.awsdns-53.com
    › w3.tue.nl: type NS, class IN, ns ns-550.awsdns-04.net
    › w3.tue.nl: type NS, class IN, ns ns-1464.awsdns-55.org
    › w3.tue.nl: type NS, class IN, ns ns-1853.awsdns-39.co.uk
  ▾ Additional records
    › ns-424.awsdns-53.com: type A, class IN, addr 205.251.193.168
    › ns-550.awsdns-04.net: type A, class IN, addr 205.251.194.38
    › ns-1464.awsdns-55.org: type A, class IN, addr 205.251.197.184
    › ns-1853.awsdns-39.co.uk: type A, class IN, addr 205.251.199.61
    › ns-424.awsdns-53.com: type AAAA, class IN, addr 2600:9000:5301:a800::1
    › ns-550.awsdns-04.net: type AAAA, class IN, addr 2600:9000:5302:2600::1
    › ns-1464.awsdns-55.org: type AAAA, class IN, addr 2600:9000:5305:b800::1
    › ns-1853.awsdns-39.co.uk: type AAAA, class IN, addr 2600:9000:5307:3d00::1
    [Request In: 211]
    [Time: 0.021393000 seconds]
```

Figure 9: Captured DNS response message

(b) Three name servers were returned, and their IP addresses were contained in the Additional records section.

```
❯ nslookup -type=NS tue.nl
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
tue.nl  nameserver = ns3.tue.nl.
tue.nl  nameserver = ns1.tue.nl.
tue.nl  nameserver = ns2.tue.nl.

Authoritative answers can be found from:
ns1.tue.nl      internet address = 131.155.2.3
ns2.tue.nl      internet address = 131.155.3.3
ns3.tue.nl      internet address = 130.89.2.7
ns1.tue.nl      has AAAA address 2001:610:1108:2::3
ns2.tue.nl      has AAAA address 2001:610:1108:3::3
```

Figure 10: nslookup command

```
Domain Name System (response)
    Transaction ID: 0x0c85
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 5
  v Queries
    > tue.nl: type NS, class IN
  v Answers
    > tue.nl: type NS, class IN, ns ns3.tue.nl
    > tue.nl: type NS, class IN, ns ns1.tue.nl
    > tue.nl: type NS, class IN, ns ns2.tue.nl
  v Additional records
    > ns1.tue.nl: type A, class IN, addr 131.155.2.3
    > ns2.tue.nl: type A, class IN, addr 131.155.3.3
    > ns3.tue.nl: type A, class IN, addr 130.89.2.7
    > ns1.tue.nl: type AAAA, class IN, addr 2001:610:1108:2::3
    > ns2.tue.nl: type AAAA, class IN, addr 2001:610:1108:3::3
    [Request In: 18]
    [Time: 0.025569000 seconds]
```

Figure 11: Captured DNS response message

(c) The command-line used is "nslookup www.tue.nl ns1.tue.nl", and the name server returned the canonical name of "www.tue.nl" as "web.w3.tue.nl"

```
❯ nslookup www.tue.nl ns1.tue.nl
Server:         ns1.tue.nl
Address:        131.155.2.3#53

www.tue.nl      canonical name = web.w3.tue.nl.
```

Figure 12: nslookup for www.tue.nl to a name server on tue.nl's domain

(d) One name server "ns-550.awsdns-04.net" is actually responsible for "web.w3.tue.nl",

and it belong to two Top-Level Domains (TLD), the primary name server is "ns-550.awsdns-04.net", the other is responsible authority's mailbox: "awsdns-hostmaster.amazon.com".

```
❯ nslookup -type=NS web.w3.tue.nl
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
*** Can't find web.w3.tue.nl: No answer

Authoritative answers can be found from:
w3.tue.nl
        origin = ns-550.awsdns-04.net
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400
```

Figure 13: nslookup for web.w3.tue.nl

(e) The command-line used here is "nslookup web.w3.tue.nl ns-550.awsdns-04.net", and the IP address received is identical to the one obtained in (a).

```
❯ nslookup web.w3.tue.nl ns-550.awsdns-04.net
Server:         ns-550.awsdns-04.net
Address:        205.251.194.38#53

Name:   web.w3.tue.nl
Address: 49.12.16.43
```

Figure 14: nslookup for web.w3.tue.nl