1.1.1

http

No.	Time	Source	Destination	Protocol	Length	Info
97	3.943785	192.168.1.83	130.243.109.196	HTTP	515	GET /Research/MRO/gasbot/gallery.html HTTP/1.1
101	3.957137	130.243.109.196	192.168.1.83	HTTP	594	HTTP/1.1 307 Temporary Redirect (text/html)
106	3.981635	192.168.1.83	130.243.105.49	HTTP	493	GET /Research/MRO/gasbot/images/GB_08b_small.jpg HTTP/1.1
109	3.993408	130.243.105.49	192.168.1.83	HTTP	1304	HTTP/1.1 404 Not Found (text/html)
118	4.040413	192.168.1.83	130.243.105.49	HTTP	495	GET /Research/MRO/gasbot/images/L0EntryArrowDark.gif HTTP/1.1
119	4.051778	130.243.105.49	192.168.1.83	HTTP	1303	HTTP/1.1 404 Not Found (text/html)

598	18.595093	192.168.1.83	130.243.109.196	HTTP	515	GET /Research/MRO/gasbot/gallery.html HTTP/1.1
602	18.607266	130.243.109.196	192.168.1.83	HTTP	594	HTTP/1.1 307 Temporary Redirect (text/html)
606	18.617068	192.168.1.83	130.243.105.49	HTTP	518	GET /Research/MRO/gasbot/gallery.html HTTP/1.1
612	18.637894	130.243.105.49	192.168.1.83	HTTP	105	HTTP/1.1 200 OK (text/html)
614	18.652919	192.168.1.83	130.243.105.49	HTTP	369	GET /Research/MRO/gasbot/styles.css HTTP/1.1
625	18.667231	192.168.1.83	130.243.105.49	HTTP	415	GET /Research/MRO/gasbot/lsl.js HTTP/1.1
632	18.678255	130.243.105.49	192.168.1.83	HTTP	832	HTTP/1.1 200 OK (text/css)
634	18.679080	192.168.1.83	130.243.105.49	HTTP	494	GET /Research/MRO/gasbot/images/RAGD_indoor_1.JPG HTTP/1.1
748	18.798673	130.243.105.49	192.168.1.83	HTTP	80	HTTP/1.1 200 OK (application/x-javascript)
752	18.799980	192.168.1.83	130.243.105.49	HTTP	501	GET /Research/MRO/gasbot/images/RAGD_outdoor_1_small.JPG HTTP/1.1
797	18.868757	192.168.1.83	130.243.105.49	HTTP	492	GET /Research/MRO/gasbot/images/GB_07_small.jpg HTTP/1.1
804	18.868939	192.168.1.83	130.243.105.49	HTTP	492	GET /Research/MRO/gasbot/images/GB_08_small.jpg HTTP/1.1
805	18.868964	192.168.1.83	130.243.105.49	HTTP	492	GET /Research/MRO/gasbot/images/GB_09_small.jpg HTTP/1.1
806	18.868987	192.168.1.83	130.243.105.49	HTTP	492	GET /Research/MRO/gasbot/images/GB_10_small.jpg HTTP/1.1
1658	19.645419	130.243.105.49	192.168.1.83	HTTP	1102	HTTP/1.1 200 OK (JPEG JFIF image)
1659	19.645737	192.168.1.83	130.243.105.49	HTTP	492	GET /Research/MRO/gasbot/images/GB_06_small.jpg HTTP/1.1
2341	20.207917	130.243.105.49	192.168.1.83	HTTP	908	HTTP/1.1 200 OK (JPEG JFIF image)
2343	20.208234	192.168.1.83	130.243.105.49	HTTP	492	GET /Research/MRO/gasbot/images/GB_04_small.jpg HTTP/1.1
2450	20.342259	130.243.105.49	192.168.1.83	HTTP	60	HTTP/1.1 200 OK (JPEG JFIF image)
2452	20.342591	192.168.1.83	130.243.105.49	HTTP	492	GET /Research/MRO/gasbot/images/GB_14_small.jpg HTTP/1.1
2514	20.378322	192.168.1.83	130.243.105.49	HTTP	493	GET /Research/MRO/gasbot/images/GB_08b_small.jpg HTTP/1.1
2552	20.405385	130.243.105.49	192.168.1.83	HTTP	250	HTTP/1.1 200 OK (JPEG JFIF image)
2554	20.405650	192.168.1.83	130.243.105.49	HTTP	501	GET /Research/MRO/gasbot/images/RAGD_outdoor_2_small.JPG HTTP/1.1
2633	20.479788	130.243.105.49	192.168.1.83	HTTP	1303	HTTP/1.1 404 Not Found (text/html)
2634	20.480377	192.168.1.83	130.243.105.49	HTTP	501	GET /Research/MRO/gasbot/images/RAGD_outdoor_3_small.JPG HTTP/1.1
2795	20.603778	130.243.105.49	192.168.1.83	HTTP	600	HTTP/1.1 200 OK (JPEG JFIF image)
2796	20.604102	192.168.1.83	130.243.105.49	HTTP	492	GET /Research/MRO/gasbot/images/GB_01_small.png HTTP/1.1
3603	21.297997	192.168.1.83	130.243.105.49	HTTP	492	GET /Research/MRO/gasbot/images/GB_02_small.jpg HTTP/1.1
3956	21.586094	192.168.1.83	130.243.105.49	HTTP	486	GET /Research/MRO/gasbot/images/GB_13.png HTTP/1.1
4572	22.159913	192.168.1.83	130.243.105.49	HTTP	492	GET /Research/MRO/gasbot/images/GB_15_small.jpg HTTP/1.1
4579	22.163736	192.168.1.83	130.243.105.49	HTTP	492	GET /Research/MRO/gasbot/images/GB_16_small.jpg HTTP/1.1
4597	22.176455	130.243.105.49	192.168.1.83	HTTP	258	HTTP/1.1 200 OK (JPEG JFIF image)
4923	22.456191	130.243.105.49	192.168.1.83	HTTP	1288	HTTP/1.1 200 OK (JPEG JFIF image)
5330	22.751437	130.243.105.49	192.168.1.83	HTTP	1351	HTTP/1.1 200 OK (JPEG JFIF image)
5723	23.123188	130.243.105.49	192.168.1.83	HTTP	810	HTTP/1.1 200 OK (PNG)
5809	23.185267	130.243.105.49	192.168.1.83	HTTP	1299	HTTP/1.1 200 OK (JPEG JFIF image)
6138	23.305868	130.243.105.49	192.168.1.83	HTTP	712	HTTP/1.1 200 OK (PNG)
6139	23.311033	192.168.1.83	130.243.105.49	HTTP	489	GET /Research/MRO/gasbot/images/aass_oru.png HTTP/1.1
6140	23.311129	192.168.1.83	130.243.105.49	HTTP	498	GET /Research/MRO/gasbot/images/headerGasbot_title.jpeg HTTP/1.1
6141	23.311157	192.168.1.83	130.243.105.49	HTTP	489	GET /Research/MRO/gasbot/images/2px_99AACC.gif HTTP/1.1
6142	23.311202	192.168.1.83	130.243.105.49	HTTP	495	GET /Research/MRO/gasbot/images/L0EntryArrowDark.gif HTTP/1.1
6143	23.320503	192.168.1.83	130.243.105.49	HTTP	461	GET /favicon.ico HTTP/1.1
6190	23.348336	130.243.105.49	192.168.1.83	HTTP	450	HTTP/1.1 200 OK (GIF89a)
6200	23.356544	130.243.105.49	192.168.1.83	HTTP	1166	HTTP/1.1 200 OK (PNG)
6232	23.410204	130.243.105.49	192.168.1.83	HTTP	401	HTTP/1.1 200 OK (text/plain)
6253	23.426835	130.243.105.49	192.168.1.83	HTTP	1303	HTTP/1.1 404 Not Found (text/html)
6689	23.893698	130.243.105.49	192.168.1.83	HTTP	300	HTTP/1.1 200 OK (JPEG JFIF image)

Q1: My local machine ip can be seen in the source of the first packet which is 192.168.1.83 and the servers public ip is 130.243.109.196, though the first server seems to redirect to another servers public ip which is 130.243.105.49 which is also the final domain we end up with in the browser.

Q2: We can see that it takes 4 packets before we receive a 200 Ok from the GET request.

Q3: The protocol used between the client and host is HTTP/1.1

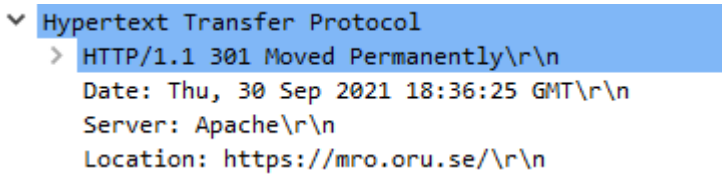
2.2.1

Q1: The version used is HTTP/1.1

Q2: The language that the browser indicated is en-US (English US).

Q3: The first packet responds with the code 301 Moved Permanently.

Q4:



The url sent in the response is the following: https://mro.oru.se/

Q5: By looking at the packets we can easily tell that the website has been moved to another server and domain or the protocol has been upgraded to HTTPS, but in this case the server responds with a new domain which also has a TLS/SSL certificate which makes the domain use https instead of http.

2.2.2

Q8: Theres 2 requests that come back with a 404 not found fails to load a gif called “L0EntryArrowDark.gif” which gets requested from the following link: http://130.243.105.49/Research/MRO/gasbot/images/L0EntryArrowDark.gif

The second one fails to load an image called “GB_14_small.jpg” which gets requested from the following link: http://130.243.105.49/Research/MRO/gasbot/images/GB_14_small.jpg

Which is a filepath (URL) on the server which cant be found.

2.2.3

Q9: The first response is 401 Unauthorized

Q10: The field that appears in the second GET request is the “Authorization” field.

Q11: Credentials, username and password.

2.2.4

Q12: There is no IF-MODIFIED-SINCE in the first get request.

Q13: Since we get a file size back and content type indicate that we have downloaded the html file in the first response.

Q14: The second request includes an if-modified-since header which has the value of the last date the site was modified.

Q15: “304 Not modified”, No because it used the cached version of the site since it has not been modified since we last visited it.

2.3.1

Q1:

```
PS C:\Users\an_de> nslookup -nosearch www.oru.se
Server:  raspberrypi
Address:  192.168.1.4

Non-authoritative answer:
Name:    www.oru.se
Addresses:  2001:6b0:2b:2057::233
          130.243.98.233
```

The name is www.oru.se and the ipv4 ip is 130.243.98.233

Q2:

```
PS C:\Users\an_de> nslookup -nosearch -type=NS oru.se
Server:  raspberrypi
Address:  192.168.1.4

Non-authoritative answer:
oru.se  nameserver = ns3.oru.se
oru.se  nameserver = ns1.oru.se
oru.se  nameserver = ns2.oru.se
```

Non-Authoritative

Q3: There are 3 nameservers listed.

2.3.2

Q4:

4 requests

Q5:

```
Protocol: UDP (17)
```

The protocol used is UDP.

Q6:

```
▼ Queries
    > www.nfl.com: type A, class IN

Queries
  > www.nfl.com: type AAAA, class IN
```

The type of DNS records requested is type A and AAAA

Q7: The A record points to an IPv4 address while the AAAA records points to an IPv6

Q9: When the nosearch option is removed it sends a request to each dns record until it finds one that answers.

161	2.114542	192.168.1.83	192.168.1.4	DNS	84	Standard query 0x0001 PTR 4.1.168.192.in-addr.arpa
162	2.115272	192.168.1.4	192.168.1.83	DNS	109	Standard query response 0x0001 PTR 4.1.168.192.in-addr.arpa PTR raspberrypi
163	2.115726	192.168.1.83	192.168.1.4	DNS	75	Standard query 0x0002 A www.nfl.com.lan
164	2.123660	192.168.1.4	192.168.1.83	DNS	150	Standard query response 0x0002 No such name A www.nfl.com.lan SOA a.root-servers.net
165	2.123777	192.168.1.83	192.168.1.4	DNS	75	Standard query 0x0003 AAAA www.nfl.com.lan
166	2.129874	192.168.1.4	192.168.1.83	DNS	150	Standard query response 0x0003 No such name AAAA www.nfl.com.lan SOA a.root-servers.net
167	2.129989	192.168.1.83	192.168.1.4	DNS	71	Standard query 0x0004 A www.nfl.com
176	2.200565	192.168.1.4	192.168.1.83	DNS	174	Standard query response 0x0004 A www.nfl.com CNAME global.nfl.map.fastly.net A 151.101.1.153 A 151.101.65.153 A 151.101.129.153 A 151.101.193.153
177	2.202740	192.168.1.83	192.168.1.4	DNS	71	Standard query 0x0005 AAAA www.nfl.com
185	2.285783	192.168.1.4	192.168.1.83	DNS	168	Standard query response 0x0005 AAAA www.nfl.com CNAME global.nfl.map.fastly.net SOA ns1.fastly.net