Ausama Askar
10/04-2018

Wireshark Introduction

Q1. My IP-adress is 10.22.10.24 while the website host's IP-adress is 130.243.105.49

Q2. It took about 0.094 seconds

Q3. The HTTP version being used is version 1.1

Basic HTTP Monitoring

Q1. The browser is running HTTP version 1.1

Q2. The accepted language indicated is en-SE, which should mean that it accepts english and swedish.

Q3. The host replies with status code 302 which means that the host has been moved temporarily

Q5. The alternative URL sent is : http://mro.oru.se/ (I think that there is a typo in the document, since Q3 is followed by Q5)

Q6. So we can conclude from the whole exchange that the host's URL has been moved from http://mrolab.eu to http://mro.oru.se/, There have been

some images loading on the website too which were tracked in the packet header. Lastly when the page finished loading images it gave a code 200: OK response.

Q7. My browser sent 25 GET requests to the internet addresses containing images that were being loaded on the host website “aass.oru.se”.

Q8. No, Objects in frames 3092, 638, 6195 and 639 were not retrieved

Q9. The server responded with the status code: 401 ; Unauthorized

Q10. The additional field is Authorization: Basic ….

Q11. The Authorization field included the credentials: “username::password”

Q12. The first GET request did not have the line “IF-MODIFIED-SINCE”

Q13. Yes, i can see that by clicking on the “Response in Frame” link which will lead me to the first GET request.

Q14. Yes i see the line, the information followed is the time the page had been modified; “Tue, 10 Apr 2018 5:59:01 GMT”

Q15. The returned response was the status code 304, Not Modified. And since the link of the “Response in frame” leads to our previous GET which included the line “IF-MODIFIED-SINCE”, we know that the server explicitly returned the contents of the file.

DNS Protocol

Q1. The name and IP of the default DNS server are;
anycast-resolver.bahnhof.net
213.80.98.2
Q2. The answer i got was non-authoritative

Q3. 4 name servers are listed

Q4. 3 queries

Q5. The transport protocol used was UDP

Q6. The DNS records requested are A and AAAA

Q7. The information sent through A is the Host Address while the AAAA contains the IPv6 Address

Q9. Removing the -nosearch option makes the nslookup perform a domain search.