Experiment-9

AIM: To capture and analyze DNS (Domain Name System) queries and understand how domain names are resolved to IP addresses.

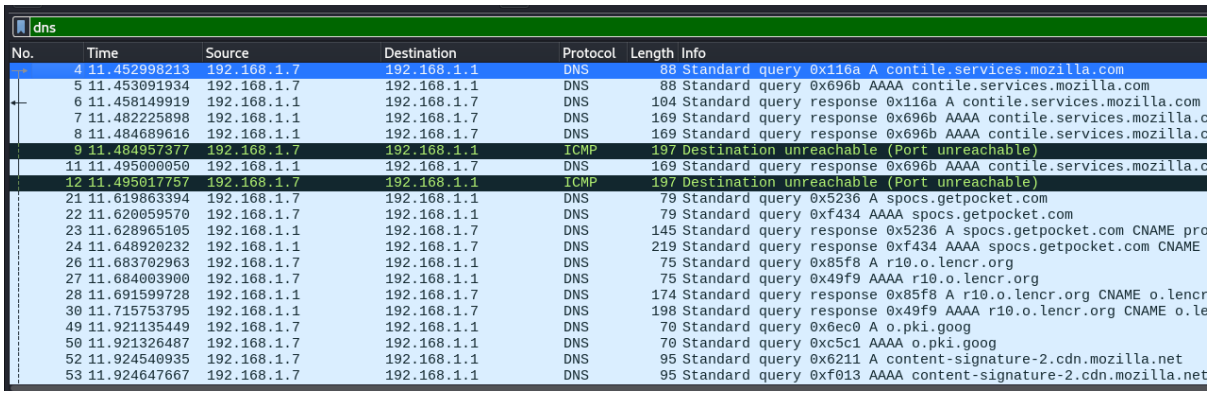
Objective: Monitor the DNS queries generated when accessing websites and analyze how the DNS resolution process works.

Theory: When you enter a website address (e.g., www.facebook.com) in your browser, a DNS query is made to resolve the domain name to its corresponding IP address. DNS servers respond with the IP address, allowing the browser to connect to the server.

Used **Commands** in Wireshark:

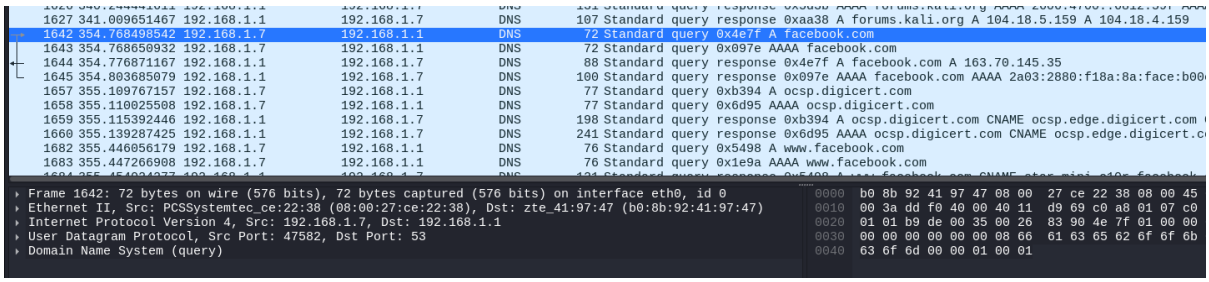
1. Capture DNS Traffic:

- Start capturing packets and use the display filter dns to capture only DNS packets.



2. Filter DNS Queries:

- Look for DNS query packets that contain requests like A www.facebook.com, which indicates a request for the IP address of the domain www.facebook.com.



3. Analyze DNS Response:

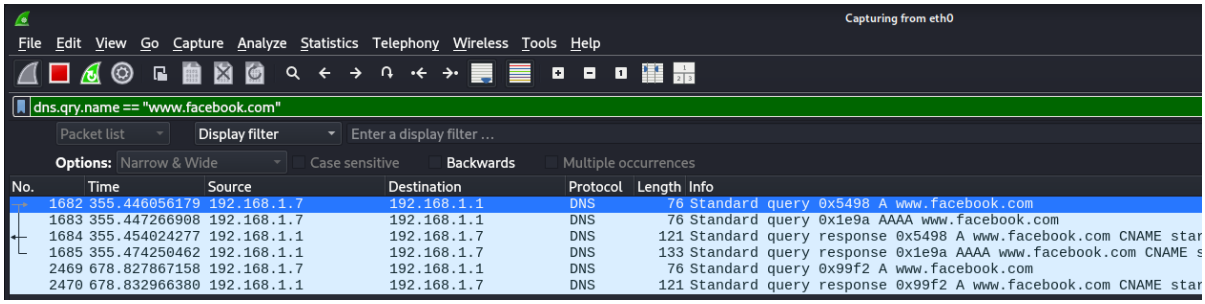
- Look for DNS response packets that will provide the IP address for the requested domain name,

e.g., www.facebook.com -> 163.70.145.35

```
 77 Standard query 0x6d95 AAAA ocsp.digicert.com
198 Standard query response 0xb394 A ocsp.digicert.com CNAME ocsp.edge.digicert.com CNAME cac-ocsp.digic
241 Standard query response 0x6d95 AAAA ocsp.digicert.com CNAME ocsp.edge.digicert.com CNAME cac-ocsp.di
 76 Standard query 0x5498 A www.facebook.com
 76 Standard query 0x1e9a AAAA www.facebook.com
121 Standard query response 0x5498 A www.facebook.com CNAME star-mini.c10r.facebook.com A 163.70.145.35
133 Standard query response 0x1e9a AAAA www.facebook.com CNAME star-mini.c10r.facebook.com AAAA 2a03:288
 79 Standard query 0x5b18 A static.xx.fbcdn.net
 79 Standard query 0x411e AAAA static.xx.fbcdn.net
```

4. Filter by DNS Query:

- Use a filter like dns.qry.name == "www.facebook.com" to see the DNS query for a specific domain.



Conclusion: In this experiment, we successfully captured and analyzed DNS (Domain Name System) traffic using Wireshark to understand how domain names are resolved to IP addresses. By monitoring DNS queries and responses, we gained insights into the DNS resolution process, which is a fundamental part of how the internet operates