

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.

No.	Time	Source	Destination	Protocol	Length	Info
4	11.452998213	192.168.1.7	192.168.1.1	DNS	88	Standard query 0x116a A contile.services.mozilla.com
5	11.453091934	192.168.1.7	192.168.1.1	DNS	88	Standard query 0x696b AAAA contile.services.mozilla.com
6	11.458149919	192.168.1.1	192.168.1.7	DNS	104	Standard query response 0x116a A contile.services.mozilla.com
7	11.482225898	192.168.1.1	192.168.1.7	DNS	169	Standard query response 0x696b AAAA contile.services.mozilla.com
8	11.484689616	192.168.1.1	192.168.1.7	DNS	169	Standard query response 0x696b AAAA contile.services.mozilla.com
9	11.484957377	192.168.1.7	192.168.1.1	ICMP	197	Destination unreachable (Port unreachable)
11	11.495000050	192.168.1.1	192.168.1.7	DNS	169	Standard query response 0x696b AAAA contile.services.mozilla.com
12	11.495017757	192.168.1.7	192.168.1.1	ICMP	197	Destination unreachable (Port unreachable)
21	11.619863394	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x5236 A spocs.getpocket.com
22	11.620059570	192.168.1.7	192.168.1.1	DNS	79	Standard query 0xf434 AAAA spocs.getpocket.com
23	11.628965105	192.168.1.1	192.168.1.7	DNS	145	Standard query response 0x5236 A spocs.getpocket.com CNAME pro
24	11.648920232	192.168.1.1	192.168.1.7	DNS	219	Standard query response 0xf434 AAAA spocs.getpocket.com CNAME
26	11.683702963	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x85f8 A r10.o.lencr.org
27	11.684003900	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x49f9 AAAA r10.o.lencr.org
28	11.691599728	192.168.1.1	192.168.1.7	DNS	174	Standard query response 0x85f8 A r10.o.lencr.org CNAME o.lencr
30	11.715753795	192.168.1.1	192.168.1.7	DNS	198	Standard query response 0x49f9 AAAA r10.o.lencr.org CNAME o.lencr
49	11.921135449	192.168.1.7	192.168.1.1	DNS	70	Standard query 0x6ec0 A o.pki.goog
50	11.921326487	192.168.1.7	192.168.1.1	DNS	70	Standard query 0xc5c1 AAAA o.pki.goog
52	11.924540935	192.168.1.7	192.168.1.1	DNS	95	Standard query 0x6211 A content-signature-2.cdn.mozilla.net
53	11.924647667	192.168.1.7	192.168.1.1	DNS	95	Standard query 0xf013 AAAA content-signature-2.cdn.mozilla.net

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.

1627	341.089651467	192.168.1.1	192.168.1.7	DNS	107	Standard query response 0xaa38 A forums.kali.org A 104.18.5.159 A 104.18.4.159
1642	354.768493542	192.168.1.7	192.168.1.1	DNS	72	Standard query 0x4e7f A facebook.com
1643	354.768659932	192.168.1.7	192.168.1.1	DNS	72	Standard query 0x097e AAAA facebook.com
1644	354.776871167	192.168.1.1	192.168.1.7	DNS	86	Standard query response 0x4e7f A facebook.com A 163.70.145.35
1645	354.803685079	192.168.1.1	192.168.1.7	DNS	100	Standard query response 0x097e AAAA facebook.com AAAA 2a03:2880:f18a:8a:face:b00
1657	355.109767157	192.168.1.7	192.168.1.1	DNS	77	Standard query 0xb394 A ocsp.digicert.com
1658	355.110025508	192.168.1.1	192.168.1.7	DNS	77	Standard query 0x6d95 AAAA ocsp.digicert.com
1659	355.115392446	192.168.1.7	192.168.1.1	DNS	198	Standard query response 0xb394 A ocsp.digicert.com CNAME ocsp.edge.digicert.com
1660	355.139287425	192.168.1.1	192.168.1.7	DNS	241	Standard query response 0x6d95 AAAA ocsp.digicert.com CNAME ocsp.edge.digicert.com
1682	355.446056179	192.168.1.7	192.168.1.1	DNS	76	Standard query 0x5498 A www.facebook.com
1683	355.447266908	192.168.1.7	192.168.1.1	DNS	76	Standard query 0x1e9a AAAA www.facebook.com

Frame 1642: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth9, id 0
 Ethernet II, Src: PCSSystemtec ce:22:38 (08:00:27:ce:22:38), Dst: zte_41:97:47 (b0:8b:92:41:97:47)
 Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.1
 User Datagram Protocol, Src Port: 47582, Dst Port: 53
 Domain Name System (query)

0000 b0 8b 92 41 97 47 08 00 27 c5 22 38 08 00 45
 0010 00 3a dd f0 40 00 40 11 49 69 c0 a8 01 07 c0
 0020 01 01 b9 de 00 35 00 26 83 99 4e 7f 01 00 00
 0030 00 00 00 00 00 00 00 61 63 05 62 6f 6f 6b
 0040 63 6f 6d 00 00 01 00 01

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

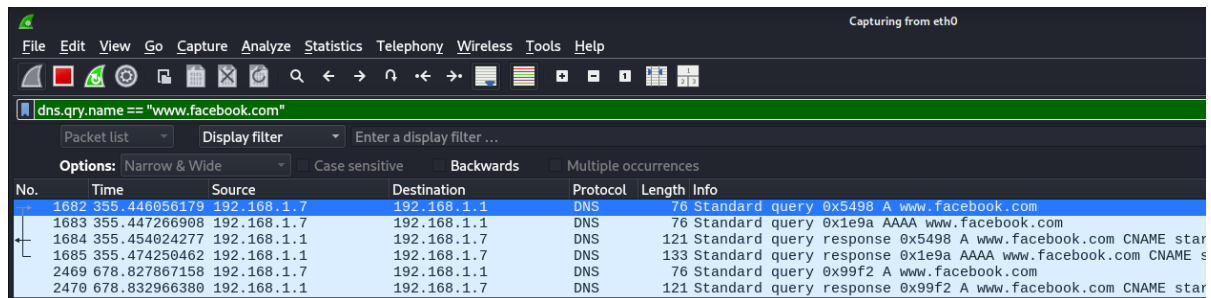
```

77 Standard query 0x6d95 AAAA ocsdp.digicert.com
198 Standard query response 0xb394 A ocsdp.digicert.com CNAME ocsdp.edge.digicert.com CNAME cac-ocsdp.digic
241 Standard query response 0x6d95 AAAA ocsdp.digicert.com CNAME ocsdp.edge.digicert.com CNAME cac-ocsdp.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.