**1.What types of traffic (HTTP, DNS, FTP, etc.) are present?**

The capture includes traffic using both TCP and UDP protocols.

- DNS and mDNS uses UDP
- HTTP use TCP

There's no FTP or other protocols observed in this capture.

**2.How many DNS queries were made in total?**

There were 357 DNS queries made in total to different websites and 1 mDNS query.

**3.What types of DNS queries were made?**

The number along with the type of DNS queries is listed below

1. A (IPv4 address) - 143
2. AAAA(IPv6 address) - 141
3. HTTPS - 72
4. PTR(reverse DNS lookback) - 1

**4.What is a Loopback Interface?**

A Loopback Interface is a virtual network interface used to communicate with the same device and manage systems internally. It's commonly used for testing and uses the IP address 127.0.0.1.

**5.How many .txt files were requested? List their names.**

Three .txt files were requested:

- decoy1.txt
- decoy2.txt
- encoded.txt

**6.One .txt file contains base64-encoded content. Identify and decode it. What does it contain?**

The file encoded.txt contains base64-encoded content and it says FLAG{spid3r_network_master} when decoded.

**7.Was any attempt made to distract the analyst using decoy files? Explain.**

Yes, the attempt was made to distract the analyst. The files contained plain text of one line each and TCP exchange happening locally shows that this was just to distract the analyst.

**8.Are there any known ports being used for uncommon services?**

Yes, the port 8000 is used multiple times for the http service. The standard port for the http services is 80, here port 8000 is used for the same purpose.

**9.How many HTTP GET requests are visible in the capture?**

There are 3 GET requests visible in the capture.

**10.What User-Agent was used to make the HTTP requests?**

The User-Agent string was:curl/8.5.0. Thus curl was used to make the http requests.