**COMPUTER NETWORKING**

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

Ans) Types of traffic present are HTTP and DNS which are transmitted via the HTTP, UDP and TCP protocols.

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

Ans) 714 , out of the 764 queries made, were DNS.

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

Ans) The different types of DNS queries made were A records , AAAA records and HTTPS records.

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

Ans) A Loopback Interface is a virtual network interface used primarily for testing local servers like databases , APIs or websites and for internal communication within a host machine.

Usually the destination IP address is 127.0.0.1.

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

Ans) 3 .txt files were requested. Their names are decoy1.txt , encoded.txt and decoy2.txt.

**6. One .txt file contains base64-encoded content. Identify and decode it.**

**What does it contain?**

Ans) FLAG{spid3r\_network\_master}

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

Ans) Decoy files are files that look important but contain harmless, misleading or junk content. They are used to distract analysts from real data or to waste their time. The decoy files here are decoy1.txt and decoy2.txt as they contain no base64 , no structured content , or no useful data.

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

Ans) Yes, HTTP traffic was observed on port 8000, which is a known port but not the default for HTTP. This is a mildly uncommon usage, but not necessarily malicious.

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

Ans) 3 HTTP GET requests are visible in the capture.

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

Ams) curl/8.5.0 was used where curl is a command-line tool used to make HTTP requests and 8.5.0 is the version of curl used.