Computer Networking

Rollno: 107124064

1) DNS, TCP, HTTP, MDNS, are the types of traffic present in given PCAP file.

2) Totally there are 357 DNS queries were made in total

3) Types of queries

* PTR - 1
* HTTPS - 72
* AAAA - 141
* A - 143

4) * Loopback Interface is a virtual network interface used for communication within the same device

* It allows applications to talk to themselves over network protocols.

5) three types of .txt files were requested they are

→ decoy2.txt
→ encoded.txt
→ decoy1.txt

6) After decoding it contains 'Malformed input....'

7) decoy1.txt → This is just a decoy
decoy2.txt → Nothing to see here

No attempt made to distract the analyst using decoy files.

8) Port is 8000 and not officially reserved and commonly used as alternative HTTP port.

9) Totally there are 3 HTTP GET requests visible in capture.

10)
153 GET / decoy1.txt HTTP/1.1
154 GET / encoded.txt HTTP/1.1 .
153 GET / decoy1.txt HTTP/1.1