National Institute of Technology, Rourkela

DCCN Lab (CS3072)

2024 Spring Sem

Lab 3

Answer the following questions for captured file dns1.pcap (DNS Protocol)

1. Locate the DNS query and response messages. Are they sent over UDP or TCP?
2. What is the destination port for the DNS query message? What is the source port of DNS response message?
3. To what IP address is the DNS query message sent? Use nm-tool command to determine the IP address of your local DNS server. Are these two IP addresses the same?
4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
5. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Use the command: nslookup –type=NS mit.edu (Use dns2.pcap file)

8. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
9. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
10. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?