Table of Contents

Question 1.

	command	description	example	rationale/obs
1	`whois`	Searches a database for information about the owners of a server	`whois google.ca`	To validate the authenticity of a server
2	`ping`	Sends internet requests to a server	`ping google.ca`	To see if a server is available, and how fast you can connect
3	`traceroute`	Prints the hops of a packet during the sending of a packet	`traceroute google.ca`	See how long a packet takes to get to its destination
4	`nslookup`	Looks up DNS information about a server	`nslookup google.ca`	To get the IP address of a domain
5	`nmap`	Scans ports of a server	`nmap -p- google.ca`	To find security vulernibilities and holes in a network
6	`tcpdump`	Captures packets coming from or to a network interface	`tcpdump --interface eth0`	To monitor network traffic
7	`ssh`	Login to a remote machine securely to run commands	`ssh utorid@iits-b473-13 .utsc-labs.utoronto.ca`	To run or deploy applicatinos on another machine
8	`arp`	Maniuplate and show the ARP cache	`arp -d 10.0.0.2`	To check what IP's goes to what hardware address

Question 2.

(2.1)
TCP, and HTTP

(2.2)
0.040223931 seconds (0.334008437 - 0.293784506)

(2.3)
The internet address of `gaia.cs.umass.edu` is 128.119.245.15.
The internet address of my computer is 192.168.1.15

(2.4)
Firefox/117.0

(2.5)
80

(2.6)

GET Request:

```
15 1.779065577 192.168.1.15 128.119.245.12 HTTP 436 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 15: 436 bytes on wire (3488 bits), 436 bytes captured (3488 bits) on interface wlp6s0, id 0
Ethernet II, Src: Tp-LinkT_19:7c:3f (18:d6:c7:19:7c:3f), Dst: KasdaNet_c8:a1:6c (00:0e:f4:c8:a1:6c)
Internet Protocol Version 4, Src: 192.168.1.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 36996, Dst Port: 80, Seq: 1, Ack: 1, Len: 382
    Source Port: 36996
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 382]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1766915886
    [Next Sequence Number: 383    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 806556979
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0x9331 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (382 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/117.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 17]
    [Next request in frame: 19]
```

OK Response:

```
17 1.819752288 128.119.245.12 192.168.1.15 HTTP 492 HTTP/1.1 200 OK  (text/html)
Frame 17: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface wlp6s0, id 0
Ethernet II, Src: KasdaNet_c8:a1:6c (00:0e:f4:c8:a1:6c), Dst: Tp-LinkT_19:7c:3f (18:d6:c7:19:7c:3f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.15
Transmission Control Protocol, Src Port: 80, Dst Port: 36996, Seq: 1, Ack: 383, Len: 438
    Source Port: 80
    Destination Port: 36996
    [Stream index: 0]
    [Conversation completeness: Incomplete, DATA (15)]
```

```
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 806556979
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 383    (relative ack number)
    Acknowledgment number (raw): 1766916268
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xc9b0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sat, 09 Sep 2023 04:57:13 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 08 Sep 2023 05:59:02 GMT\r\n
    ETag: "51-604d2ac658c62"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.040686711 seconds]
    [Request in frame: 15]
    [Next requ{\fontsize{3.3mm}{3.3mm}\selectfontest in frame: 19]
    [Next response in frame: 20]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```