

**Faculty of Engineering and Technology**

**Electrical and Computer Engineering Department**

**ENEE3320**

**COURSE PROJECT**

**SOCKET PROGRAMMING**

Prepared by:

**Heba Mustafa 1221916 section 1**

**Maysam Habbash 1220075 section 1**

Instructor: Dr. Ahmad Shawahneh

Date: 22/11/2024

[1. Theory: 3](#_Toc183279866)

[1.1. Network commands and Wireshark: 3](#_Toc183279867)

[1.2. Web Server: 7](#_Toc183279868)

[1.3. UDP Socket Programming 11](#_Toc183279869)

[2. Results and Discussion 12](#_Toc183279870)

[2.1. Task 1 – Network Commands and Wireshark 12](#_Toc183279871)

[2.2. Task 2 – Web Server 17](#_Toc183279872)

[2.3. Task 3 – UDP Client-Server Trivia Game Using Socket Programming 17](#_Toc183279873)

[References: 18](#_Toc183279874)

# Theory:

## Network commands and Wireshark:

The network is like an infrastructure which allows many different clients to connect to one another in order to send and receive data. The network core is a bunch of interconnected routers connected to one another enabling us to reach almost anywhere in the world. In order to be able to send this data over the network we use packet switching, which is essentially breaking up the application layer messages into packets. The Network then goes ahead and forward these packets from one router to another until it reaches the desired location.

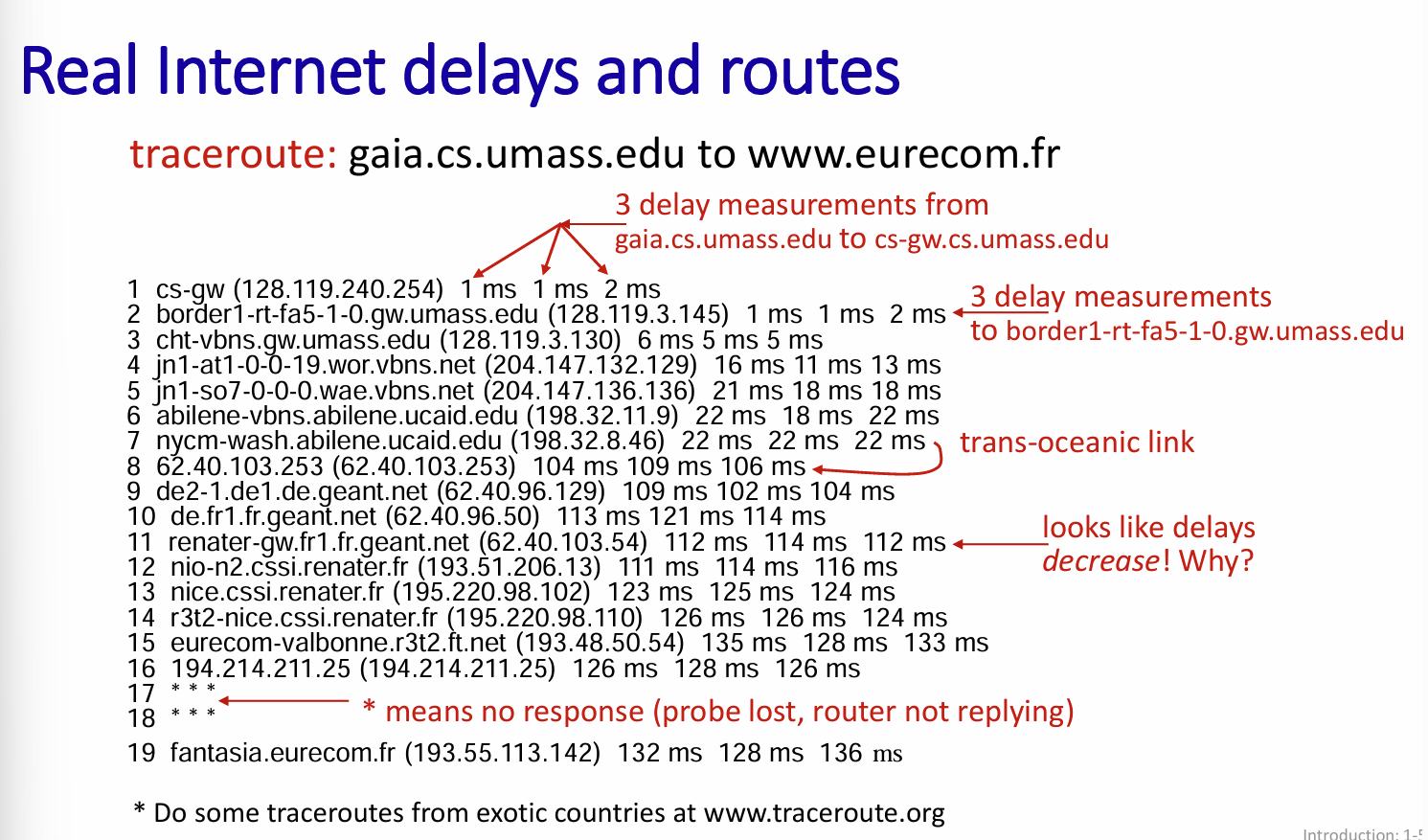


Figure .: Traceroute program [1]

Programs like traceroute allow us to measure end-end internet path delay along transition over the network. Figure 1.1 gives three delay measurements when tracing the route from gaia.cs to eurecom.fr [1]

### Message Segmentation:

We use message segmentation (cutting the data into packets) in order to reduce the delay and if an error occurs we only need to re-send the part with the error not all the message. Additionally it will cause smaller packets to have to wait for a large queue after sending a full message. [1]

### Network Hops:

The message sent from one end to the other doesn’t just go there through a straight line. Passing the message goes through a number of routers and switches each one forwarding the message to another, we call this hops (Figure 1.2). When routing to the destination, we try to go through the path of the least hops (shortest path about all the time). The Tracert command, talked about later, is a way we can view these hops [5].

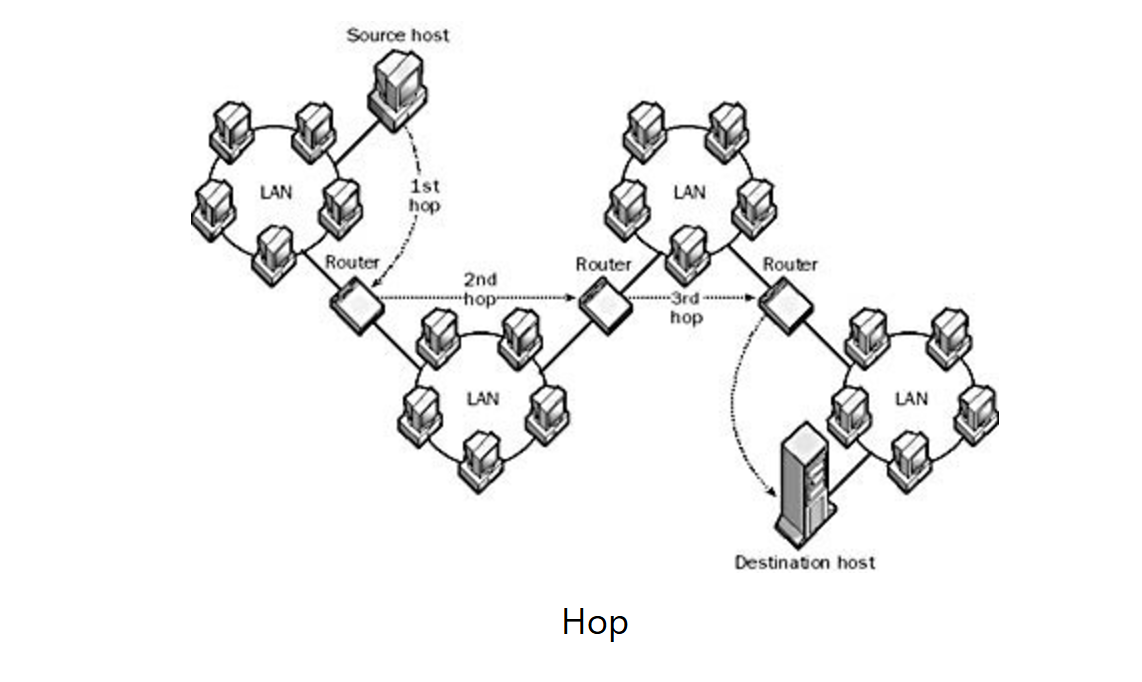


Figure .: Network hops [5]

### IP Address (Internet Protocol Address)

Every device needs a unique number as an identifier for the network to be able to connect and tell the devices apart from one another. For that reason we have a unique address for each device and we call this the IP address. These numbers, in the IPV4, range from 0.0.0.0 to 255.255.255.255 (Figure 1.3).

We have a lot more devices than addresses so in order to solve this problem a lot of devices are using the same address and hiding behind a local network. So that means a local WIFI will only be consuming one public IP and will use a whole bunch of local IPS behind the router [2] [1].

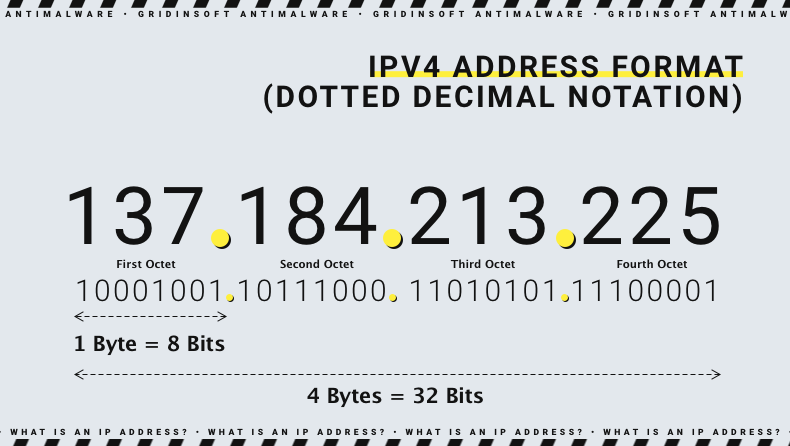


Figure .: IP Address [2]

### WireShark:

Wireshark is a network packet capture tool. It allows you to see the traffic on the internet and see thousands of packets. We can filter these packets so that we only get the information that we want. It is used to troubleshoot network problems and performance issues [3] [1] [4].

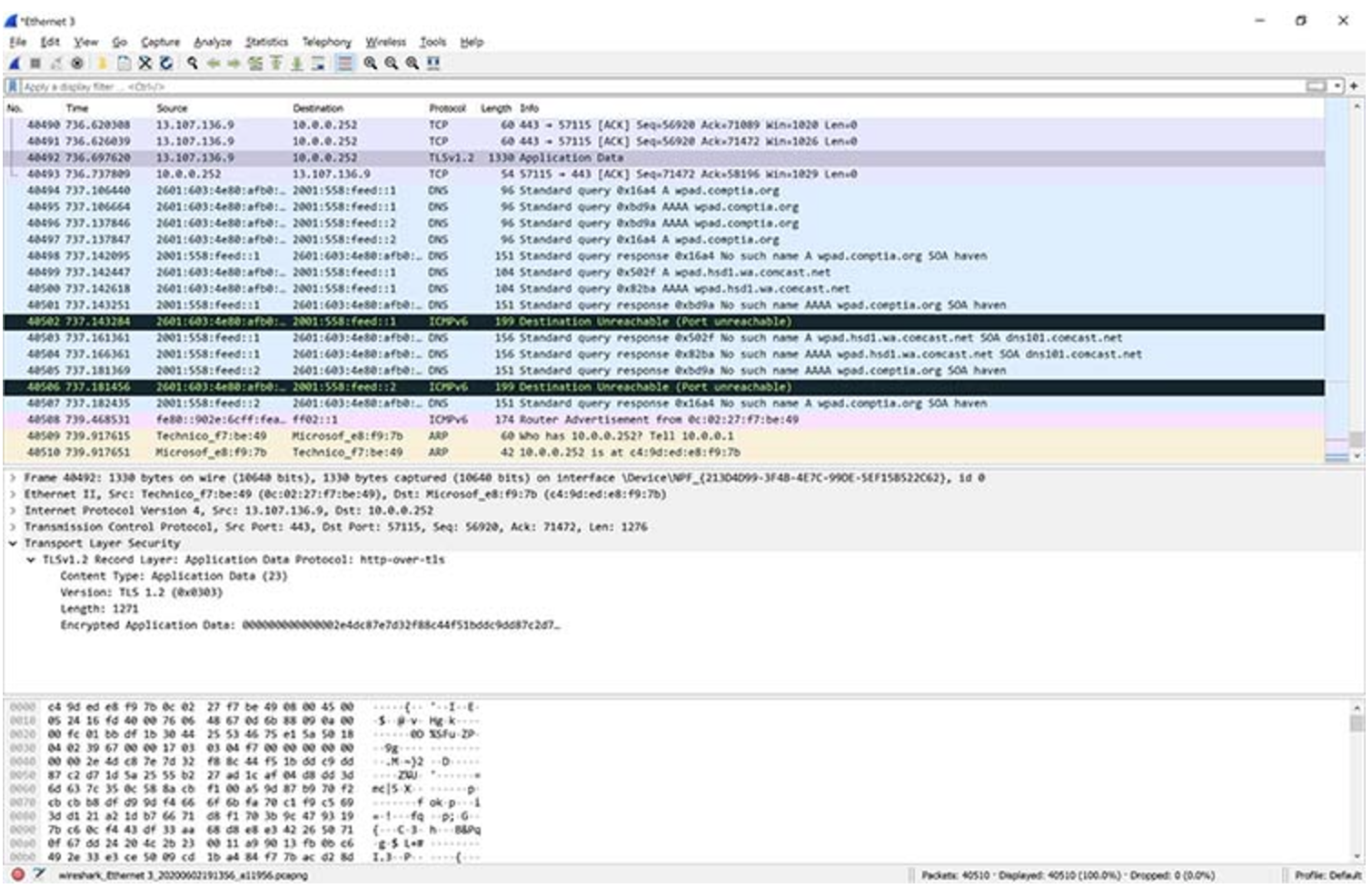


Figure .: Identifying Problems in wireShark [3]

As you can see in figure 1.4, there is a problem with sending some packets the destination was unreachable Wireshark highlighted these in black [3].

### Network Commands:

Another important skill that can be used to troubleshoot network problems is using the network commands that can be run on CMD or a Terminal. Some of these commands include:

1. **Ping:**

Ping is a command that is used to test whether a host is reachable on an Internet Protocol network. It can also help determine whether a specific IP is accessible and it also measures the round trip time from the local host to the host we want to access. It provides information about network routes and the time it takes to reach them.

1. **NetStat:**

It displays information about the active network connections with their status.

1. **IP CONFIG:**

It gives us the IP address of the current device, subnet mask, default gateway and other configurations of the IP address of a windows machine.

1. **NsLookup:**

NsLookup is used to query Domain Name System DNS to get the domain name and IP address mapping, and other records of DNS.

1. **Tracert:**

Another word for Traceroute, it is used to display the packets that are being sent and received, it shows the number of hops required to reach their destination [6].

## Web Server:

A web server is a program that processes incoming requests of web content and delivers it. To run the web server software, a physical machine (server) that provides the processing units, storage units, and network connectivity is needed to handle requests and deliver responses [7].

A web server facilitates the exchange of web content over the internet. To standardize communication between clients and the server, a protocol is needed to specify how requests and responses are transmitted over the network. Such a protocol is the HTTP, where it plays a key role in the client-server model by processing requests from user agents, such as web browsers. When a user enters a URL, the browser sends an HTTP request to the web server, which responds with the requested web page, other resources (images and resources), or an error message.

### HTML web pages

HTML (HyperText Markup Language) is the fundamental component of the Web, outlining the structure and meaning of web content. To enhance the appearance and functionality of a web page, other technologies like CSS (for styling), JavaScript (for behavior) are typically used.

While JavaScript is essential for client-side interactivity and real-time updates, Python is generally used for server-side development, handling tasks like data processing, database management, and generating dynamic content. The term "Hypertext" refers to the links that connect web pages, either within the same site or across different websites. These links are essential to the Web's structure.

### HTTP Protocol

HTTP (HyperText Transfer Protocol) is a protocol used to transfer data over the World Wide Web (www). It is a set of rules that explains how data is sent between a client (like your web browser) and a server. It allows the browser to ask the server for things like web pages, images, or other files. The server then sends back the requested content or an error message if something goes wrong.

HTTP transaction, illustrated in figure 1.5, is applied in a way where the client sends an HTTP request (Figure 1.6) to the server, which typically includes a method (like GET or POST), a URL identifying the resource, and additional headers with metadata (such as content type or authorization details). The server then processes the request and returns an HTTP response, which includes a status code (indicating whether the request was successful or failed), headers with additional information, and the requested content, such as HTML, a video, or an image.

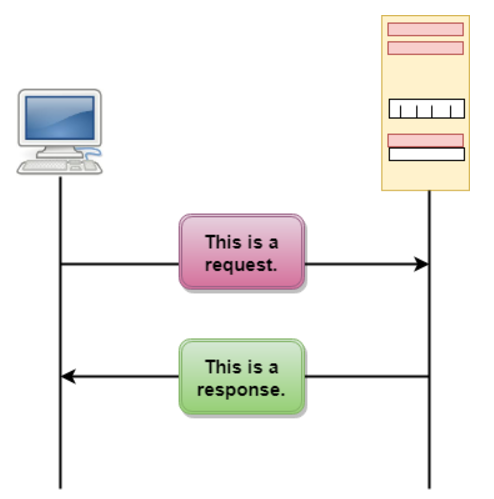


Figure .: HTTP transactions [8]

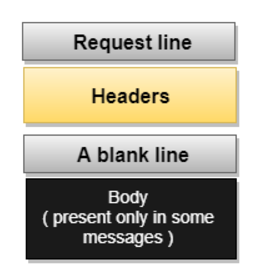
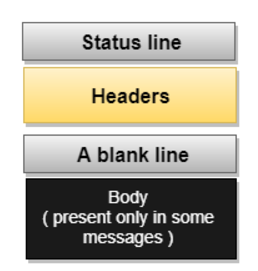
 

Figure .: HTTP request message format [8] Figure .: HTTP response message format [8]

A Uniform Resource Locator (URL) is a standard way to specify the address of information on the internet, enabling clients to access documents. It consists of four main parts: the **method**, which defines the protocol used to retrieve the document (e.g., HTTP), the **host**, which is the server where the information is stored (often with an alias like "www"), the **port**, which is optional and indicates the server's port number if specified; and the **path**, which represents the location of the file on the server, using slashes to separate directories, subdirectories, and files [8].



Figure .: URL Format [8]

#### **HTTP Features**

HTTP is a **connectionless** protocol, that is, the client initiates a request, waits for a server response, and then disconnects after receiving it. The connection exists only during the request and response. It is also **media independent**, as data can be transmitted in any format, as long as both the client and server know how to handle the content, with the content type specified in the content-type header [8].

#### **HTTP Methods**

HTTP methods are a set of operations that define the actions a client can perform on a resource stored on a server. These methods are part of the HTTP request, as discussed before, and determine what kind of operation is being requested. The most common HTTP methods are:

1. **GET:** used to request data from a server without making any changes to the resource, such as retrieving a web page or an image.
2. **PUT:** used to update or replace an existing resource on the server with new data, like updating a user profile or modifying a document.
3. **POST:** used to send data to the server to create or update a resource, commonly used when submitting form data or uploading a file.
4. **HEAD:** similar to **GET**, but it only retrieves the headers of a resource without downloading the body, often used to check metadata like content type or last-modified date.

#### **HTTP Status Codes**

HTTP response status codes indicate whether a specific HTTP request has been successfully completed or not. Response status codes are categorized into five classes [9]:

1. **Informational Responses (100 - 199)**
2. **Successful Responses (200 - 299):**

Most common response is 200 OK, which indicates that the request was successful and requested data is being sent by server.

1. **Redirection Messages (300 - 399):**

Status code 307 (Temporary Redirect) indicates that the requested resource has been temporarily moved to a different URL, and the client should continue using the original URL for future requests.

1. **Client-Error Responses (400 - 499):**

Most common responses are 404 (Not Found), which indicates that the requested resource could not be found on the server, and 403 (Forbidden), where the client does not have permission to access the resource.

1. **Server-Error Responses (500 - 599):**

#### **HTTP Headers**

HTTP headers are key-value pairs sent in both HTTP requests and responses, providing essential metadata about the request or the response. **Request headers**, included in an HTTP request provide information about the request, the client, and the desired content. They can specify details like the type of data the client can accept (Accept), the client's identity (User-Agent), and any authentication credentials (Authorization). R**esponse headers**, sent by the server, include information about the content type (Content-Type), the length of the response body (Content-Length), and instructions for caching or redirection (Cache-Control, Location).

### Socket Programming

## UDP Socket Programming

# Results and Discussion

## Task 1 – Network Commands and Wireshark

**a. In your own words, provide a brief (two-sentence maximum) explanation of each of the following commands: (i) ipconfig, (ii) ping, (iii) tracert, (iv) telnet, and (v) nslookup.**

\*\*ipconfig/all command: It gives info about the devices configuration, like the IP address Subnet, Default gateway, DNS address and more.

Ping:



e IP address: 192.168.88.11

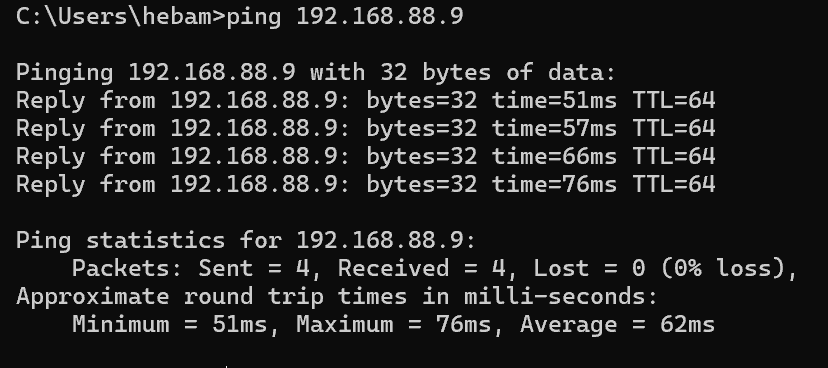
subnet mask 255.255.255.0

, default gateway, 192.168.88.1

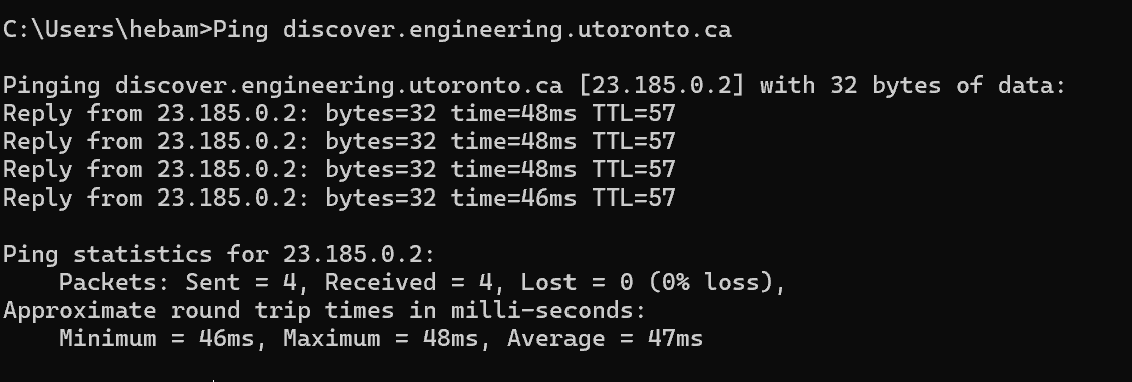
and Domain Name System (DNS) server addresses 192.168.88.1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ping a device within your local network (e.g., from your laptop to a smartphone on the same Wi-Fi network).

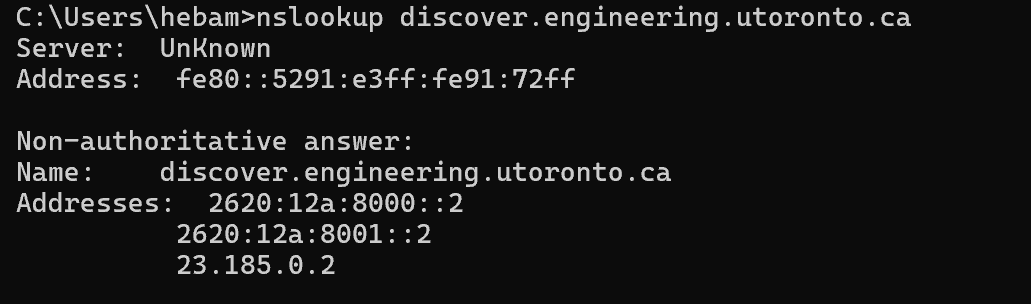
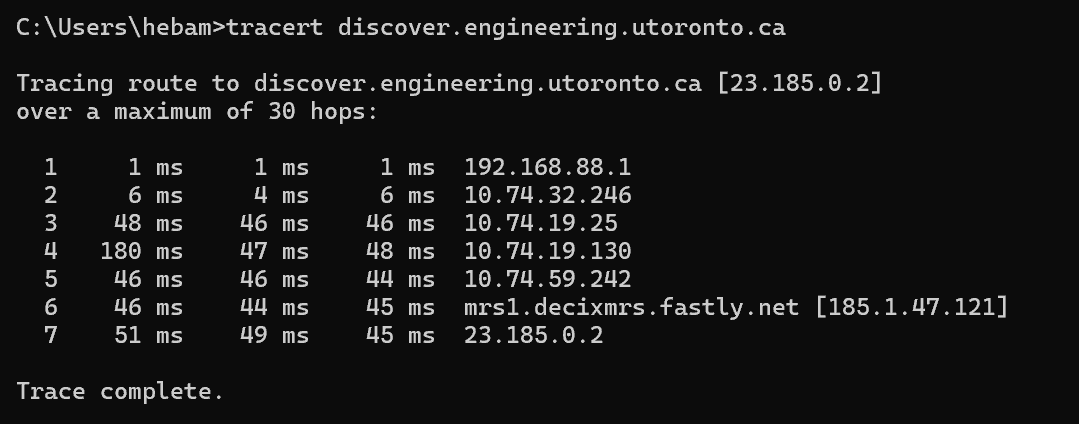
Ping discover.engineering.utoronto.ca. Based on the results, briefly explain whether you believe the response originates from Canada.

–No from the IP address its clear its located in California

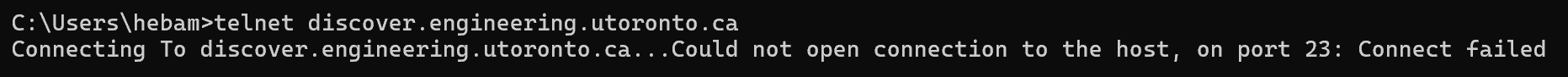


Run tracert on discover.engineering.utoronto.ca.

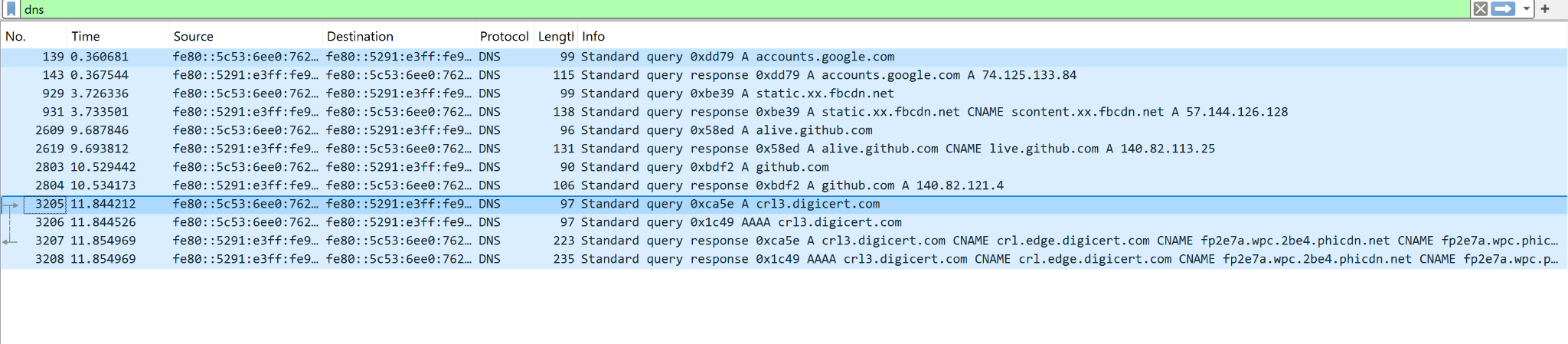
Use nslookup to retrieve the DNS information for discover.engineering.utoronto.ca.

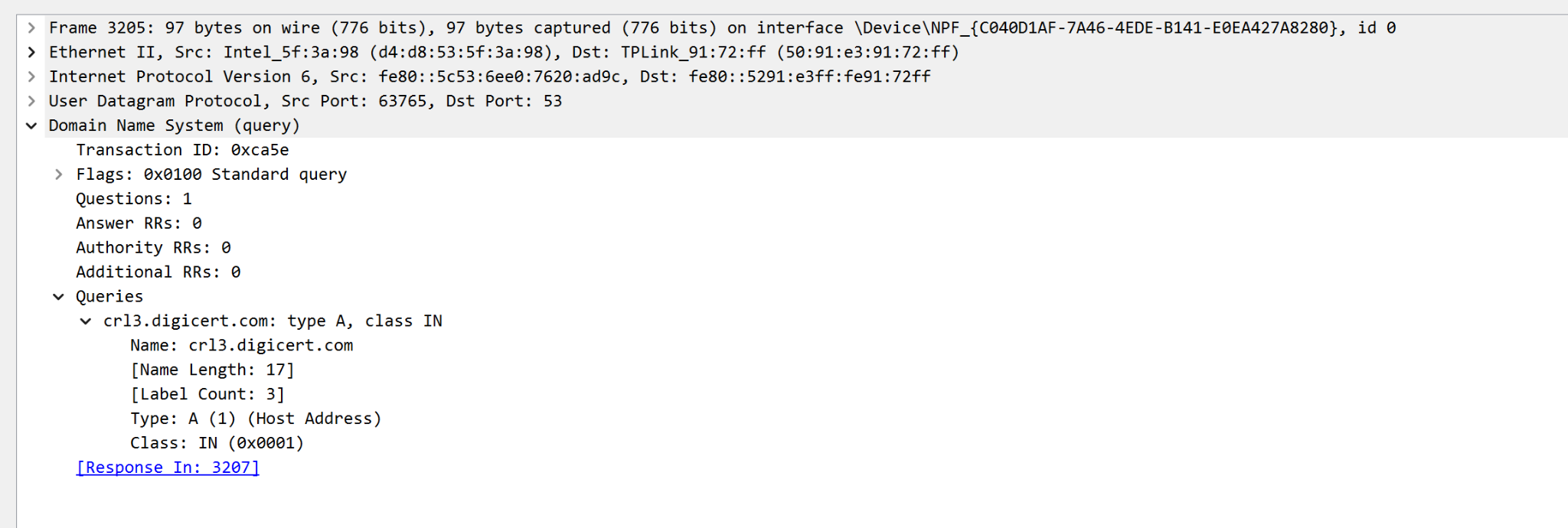


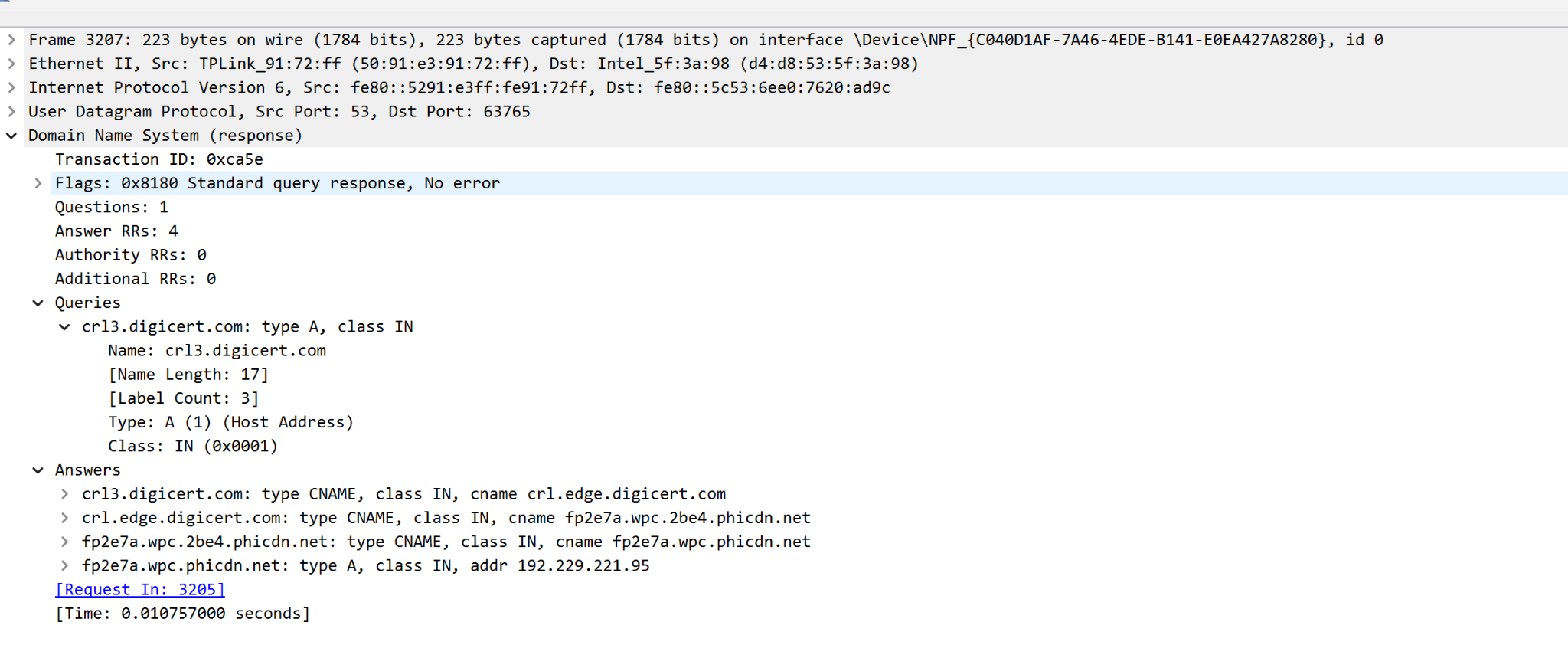
Telnet



Wireshark







## Task 2 – Web Server

## Task 3 – UDP Client-Server Trivia Game Using Socket Programming

# References:

[1]: PowerPoint slides referencing the textbook used in Birzeit University for the Computer Networking course (ENCS3320): Computer Networking: A Top-Down Approach 8th edition Jim Kurose, Keith Ross Pearson, 2020.

[2]: What is an IP address (Gridinsoft)[What is an IP address - Definition and Explanation | Gridinsoft](https://gridinsoft.com/ip-address)

[3]: What is wireshark? [What Is Wireshark and How to Use It | Cybersecurity | CompTIA](https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it)

[4]: How wireShark works [Chapter 7. How Wireshark Works](https://www.wireshark.org/docs/wsdg_html_chunked/ChapterWorks.html)

[5]: Hop Networking [Understanding Network Hops: The Journey of Data Packets - NETWORK ENCYCLOPEDIA](https://networkencyclopedia.com/hop-networking/)

[6]: Networking commands [Top 12 Networking Commands Every Windows Admin Should Use - Practically Networked](https://www.practicallynetworked.com/networking-commands/)

[7]: Web servers [What is a web server? - Learn web development | MDN](https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/What_is_a_web_server)

[8]: HTTP [HTTP - HyperText Transfer Protocol - javatpoint](https://www.javatpoint.com/computer-network-http)

[9]: HTTP status codes [HTTP response status codes - HTTP | MDN](https://developer.mozilla.org/en-US/docs/Web/HTTP/Status)

[10]: Socket Programming [Socket Programming in Python (Guide) – Real Python](https://realpython.com/python-sockets/)