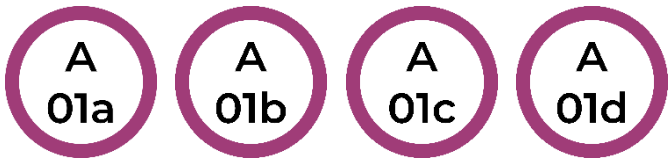


Answer Sheet
Assignment – A01

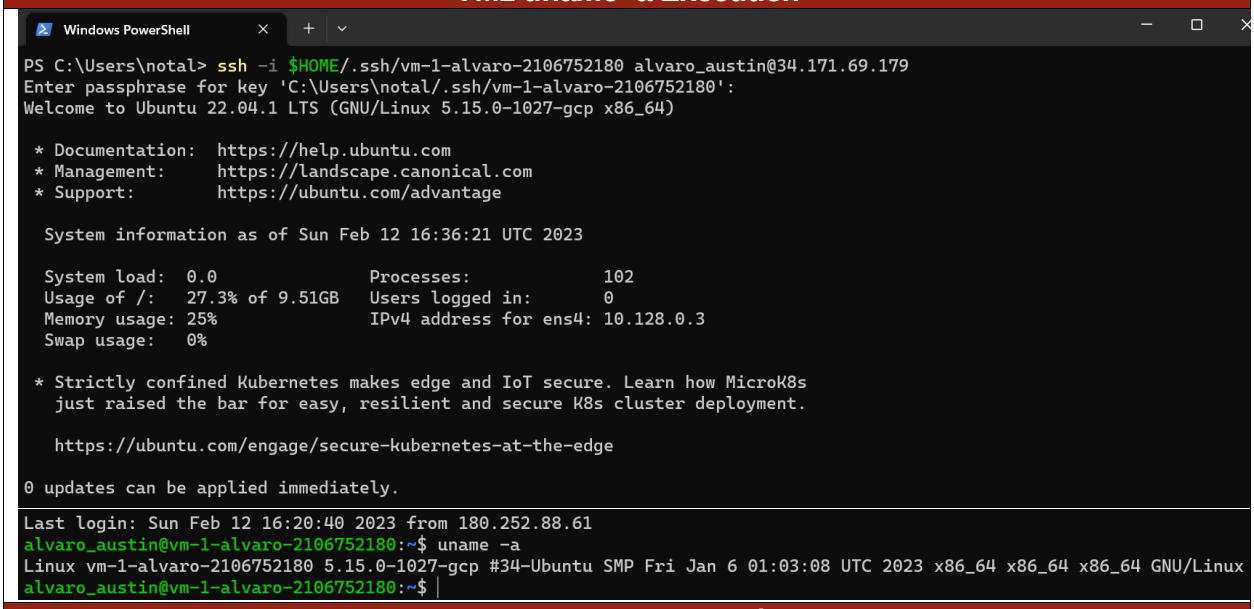
Introduction to Google Cloud Platform, Packet Tracer, Wireshark, and CLI Networking Tools

Name : Alvaro Austin
Student ID : 2106752180

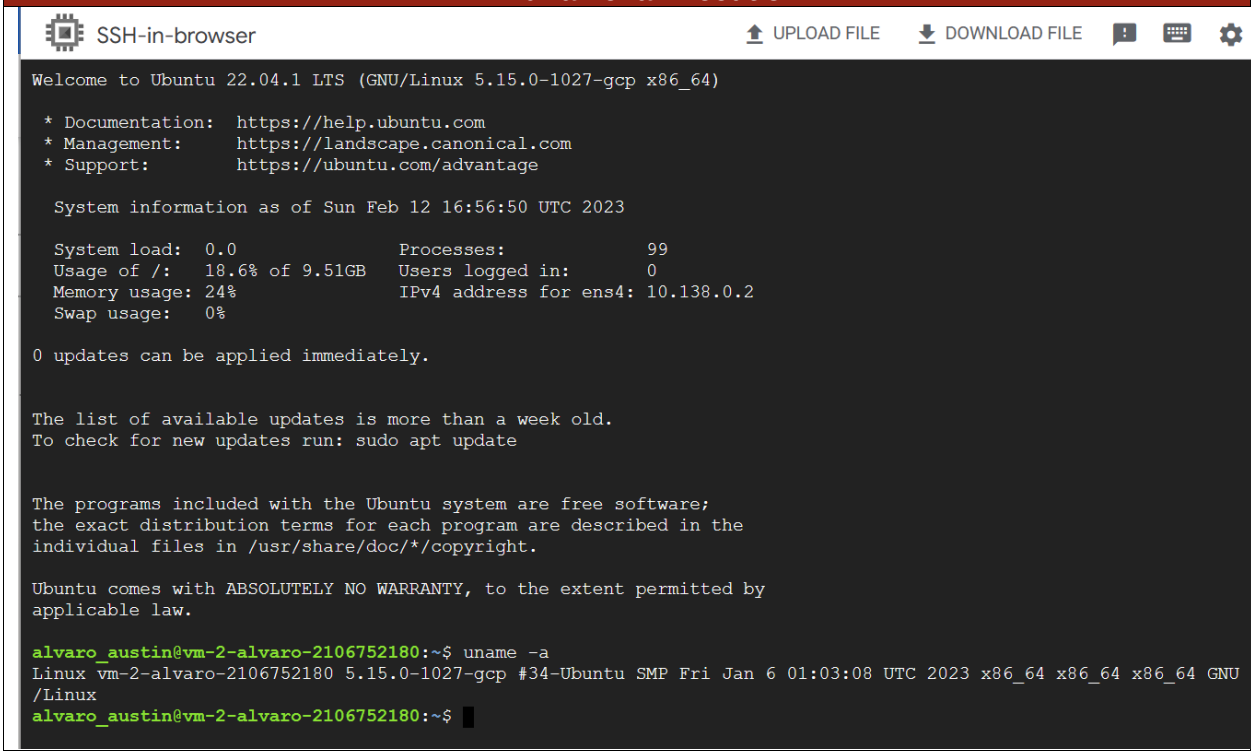
A01a – Introduction To Google Cloud Platform

[10 points] SSH Connection Establishment Proof

VM1 uname -a Execution



VM2 uname -a Execution



[10 points] Application Installation

VM1 which lynx Execution

```
alvaro_austin@vm-1-alvaro-2106752180:~$ which lynx
/usr/bin/lynx
alvaro_austin@vm-1-alvaro-2106752180:~$
```

VM2 which lynx Execution

```
alvaro_austin@vm-2-alvaro-2106752180:~$ which lynx
/usr/bin/lynx
alvaro_austin@vm-2-alvaro-2106752180:~$
```

[30 points] Firewall Rules Creation Proof

Firewall Rules Page

Filter Enter property name or value

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network
allow-dns	Ingress	allow-dns	IP ranges: 0.0.0.0/0	tcp:53 udp:53	Allow	1000	default
allow-unique	Ingress	allow-unique	IP ranges: 0.0.0.0/0	tcp:2180 udp:2180	Allow	1000	default
default-allow-http	Ingress	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000	default
default-allow-https	Ingress	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000	default
default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default
default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default
default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	default
default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default

[50 points] Virtual Machine Creation Proof

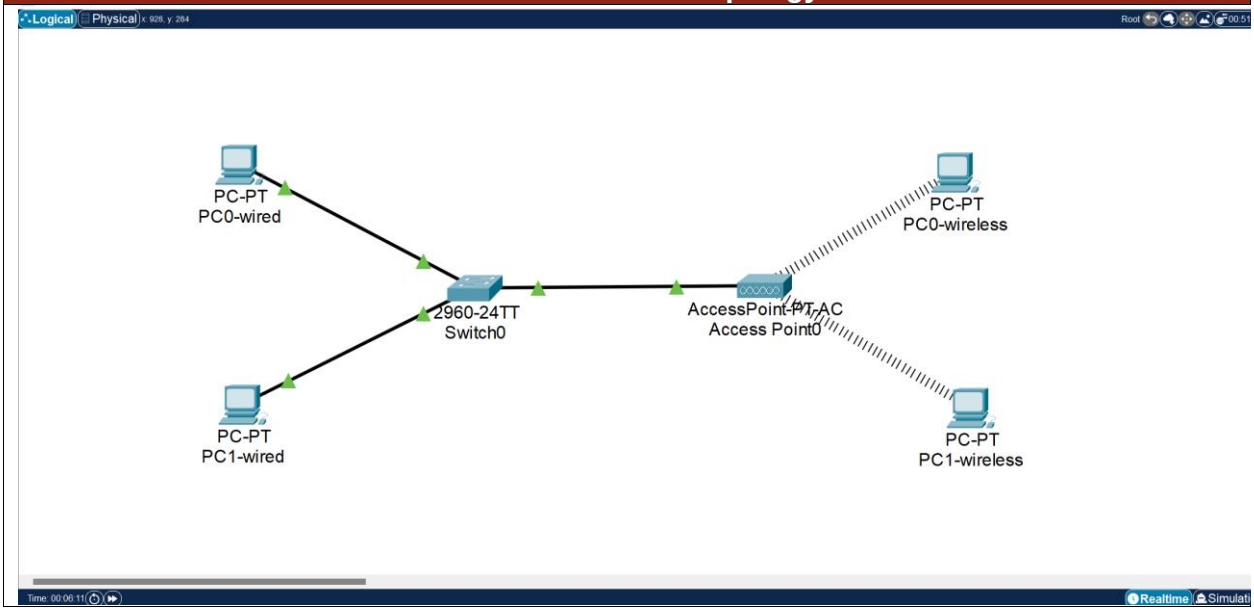
No answer is required for this component in this document. Please see the assignment document for explanation regarding the submission artifacts for this component.

Submitted the proof through SCELE.

A01b – Introduction to Packet Tracer

Create Topology

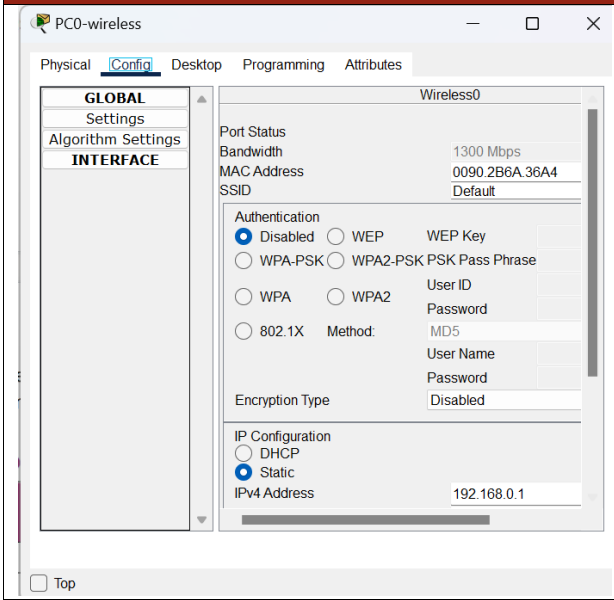
Screenshot of the Topology



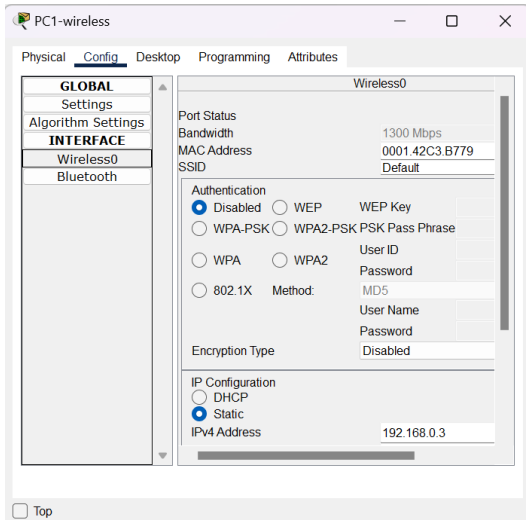
X

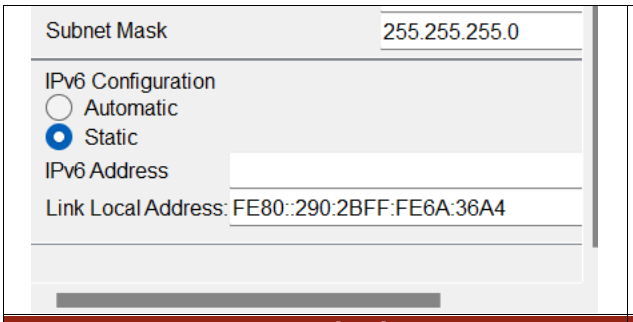
Configuration

PC0-wireless

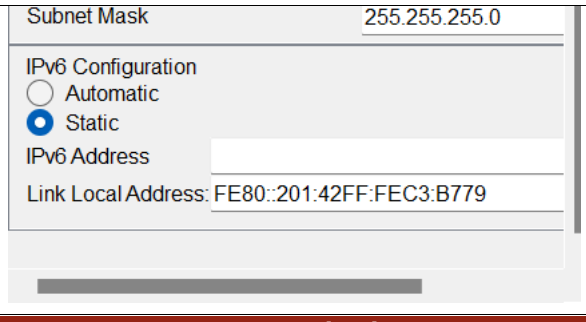


PC1-wireless

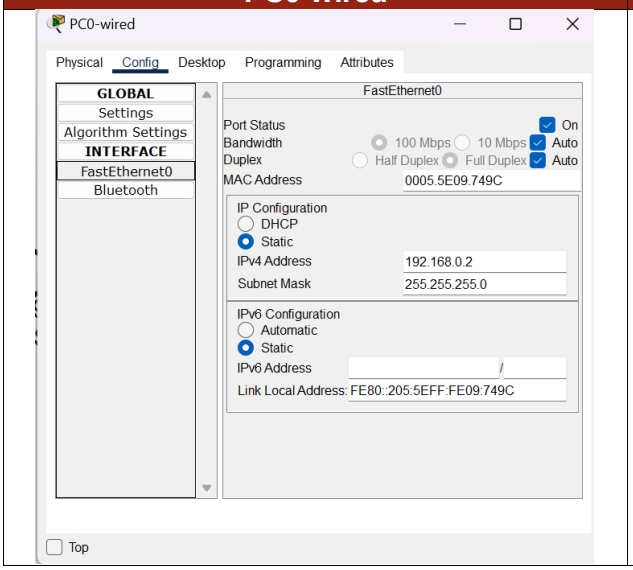


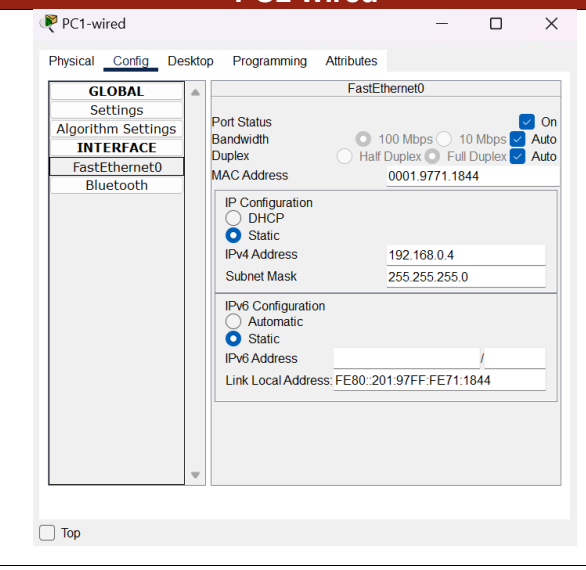


PC0-wired

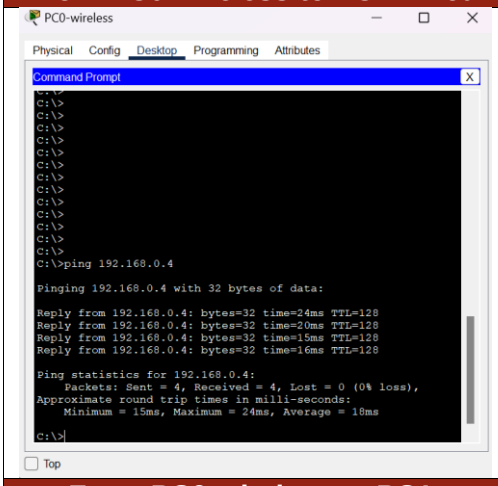
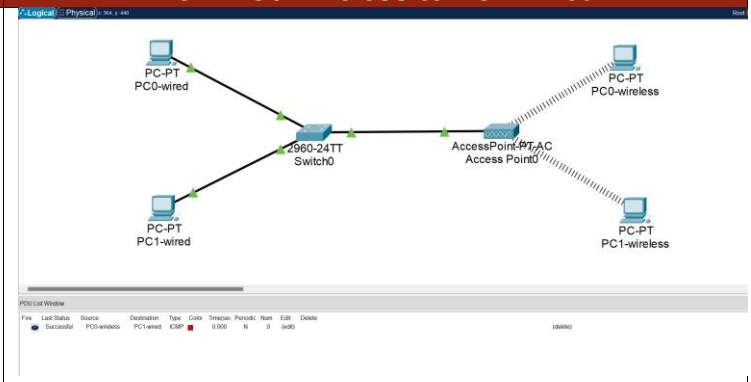


PC1-wired





Connectivity Test

Command Prompt – PING	Simple PDU
From PC0-wireless to PC1-wired	From PC0-wireless to PC1-wired
	
From PC0-wireless to PC1-wireless	From PC0-wireless to PC1-wireless

PC0-wireless

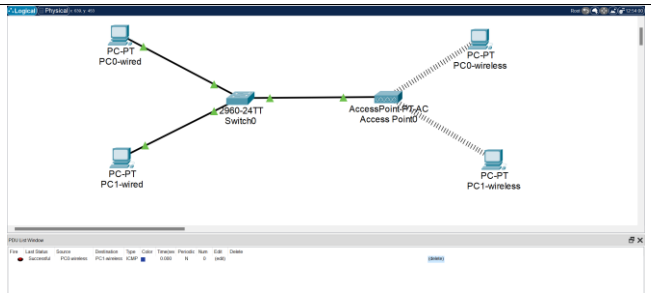
Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time=28ms TTL=128
Reply from 192.168.0.3: bytes=32 time=16ms TTL=128
Reply from 192.168.0.3: bytes=32 time=20ms TTL=128
Reply from 192.168.0.3: bytes=32 time=16ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 28ms, Average = 20ms

C:\>
```

Top

From PC0-wired to PC0-wireless



From PC0-wired to PC0-wireless

PC0-wired

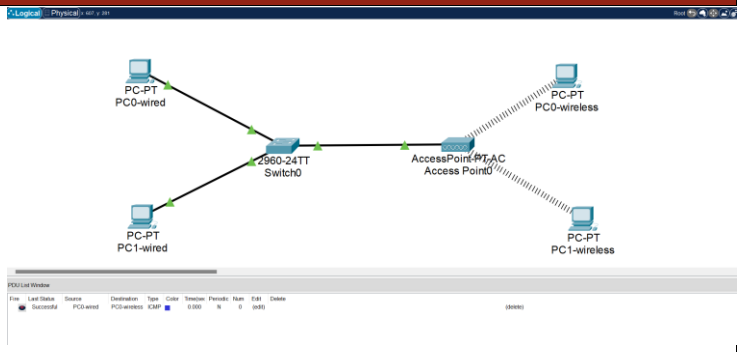
Physical Config Desktop Programming Attributes

Command Prompt

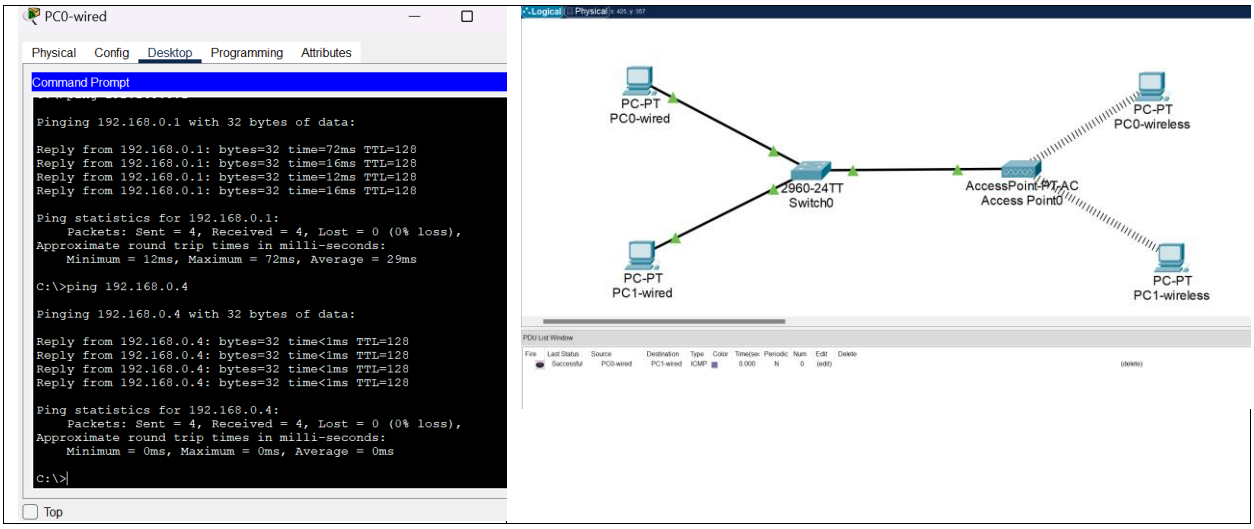
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=72ms TTL=128
Reply from 192.168.0.1: bytes=32 time=16ms TTL=128
Reply from 192.168.0.1: bytes=32 time=12ms TTL=128
Reply from 192.168.0.1: bytes=32 time=16ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% los
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 72ms, Average = 29ms

C:\>
```

Top

From PC0-wired to PC1-wired



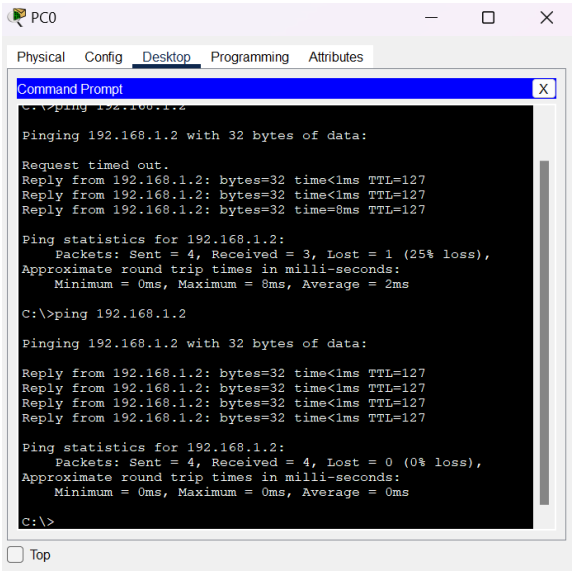
From PC0-wired to PC1-wired



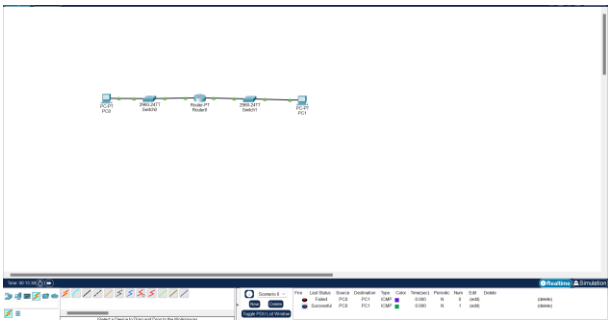
Connectivity Test with Simulation

Simulation 1

PING from PC0 to PC1



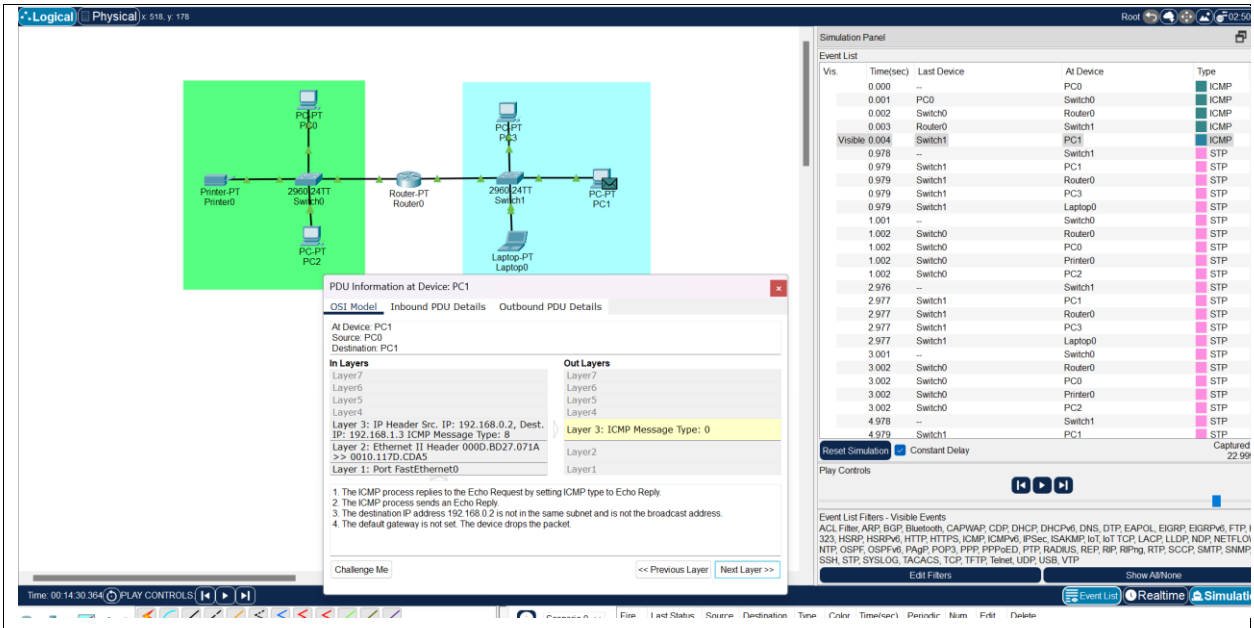
PDU from PC0 to PC1



Simulation 1 has the correct configuration. As you can see from PDU and PING test, the first time we tried to do connectivity test it failed but the second time we tried to do connectivity test it came out successful. From what I can infer, this is because network needs time to send data. Hence, the network came out fail but successful (need to time forward for this to work).

This is why simulation 1 has the correct configuration because the connectivity test ended up successful.

Simulation 2

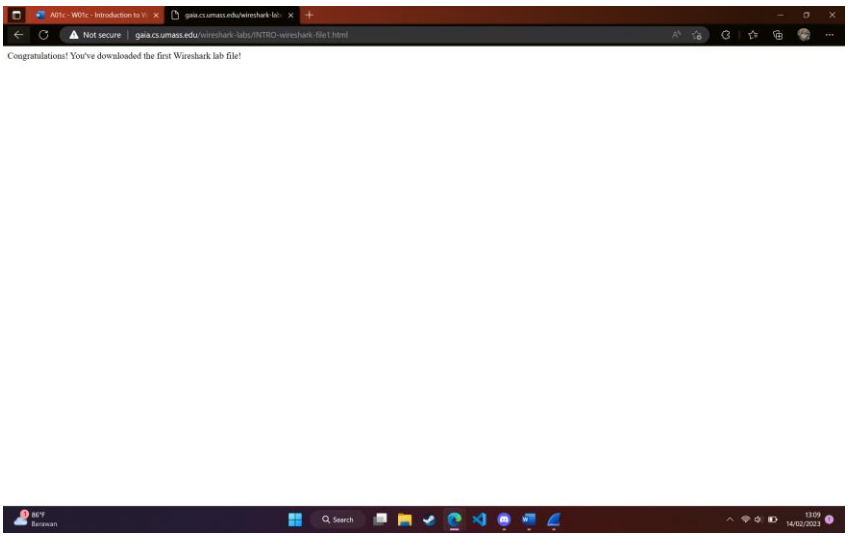


Simulation 2 ended up failing. This can be seen from PDU done in the example below. When we use simulation mode to find out about the problem, you can see that destination IP address of 192.166.0.2 is not in the same subnet and is not the broadcast address. This is the reason why the packet isn't successfully delivered.

A01c – Introduction to Wireshark

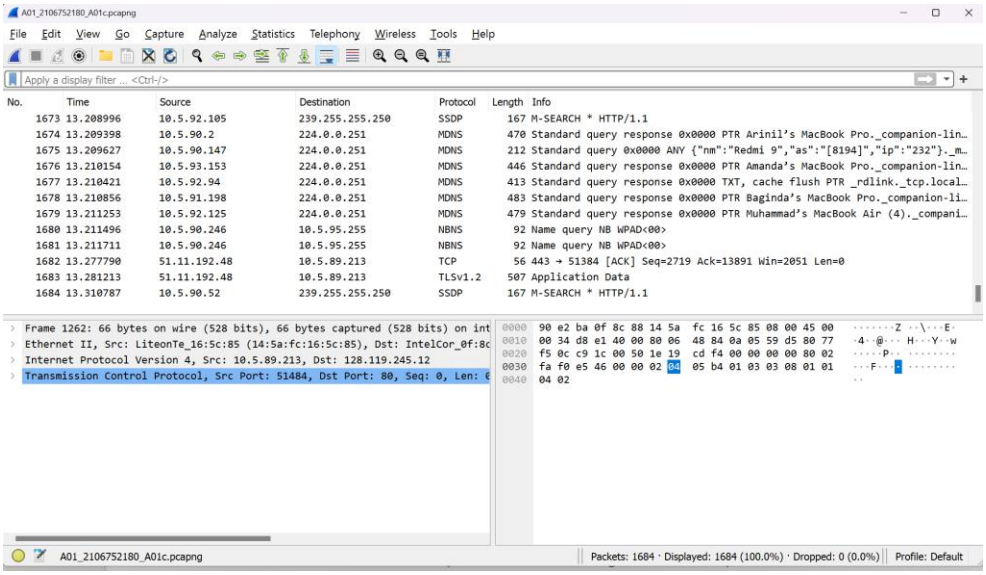
Simple Packet Capture

Screenshotted website:

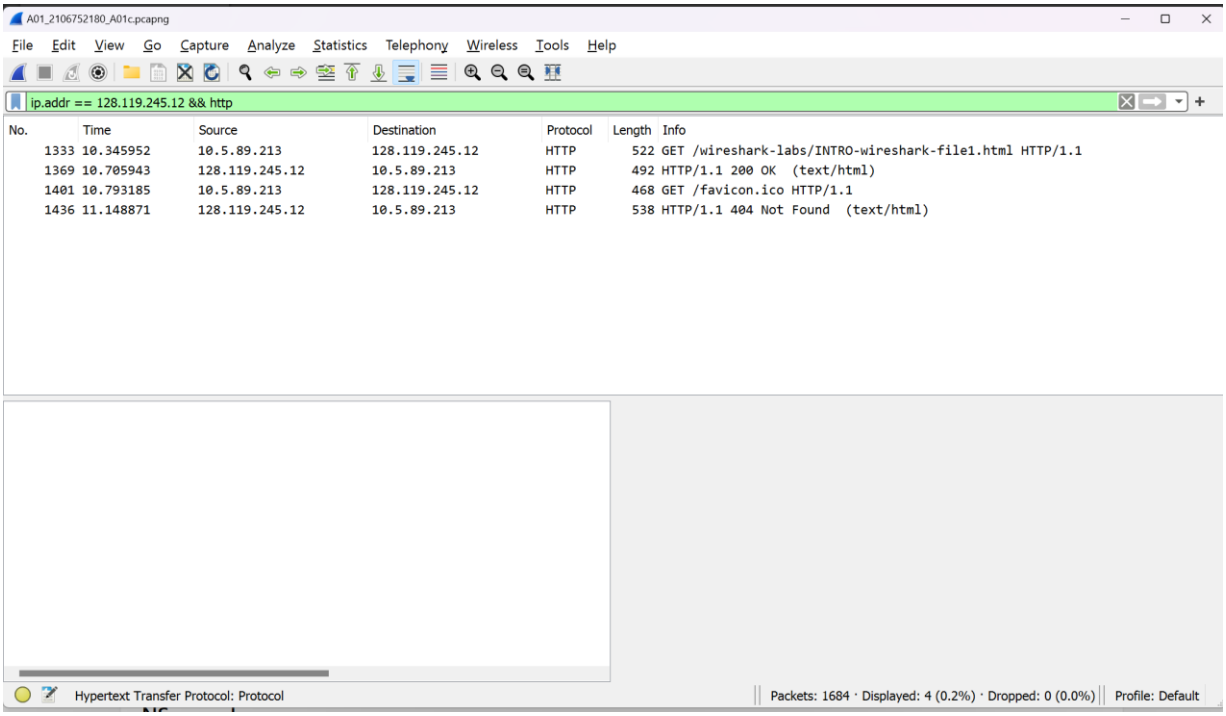


Simple Packet Filtering

Before Applying Filter



After Applying Filter



Simple Packet Analysis

IPv4 Address Screenshot

```
C:\Users\notal>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2788:71bd:5367:cbe3%9
   Autoconfiguration IPv4 Address. . : 169.254.59.232
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : ui.ac.id
   Link-local IPv6 Address . . . . . : fe80::4d39:a525:c40f:2b06%19
```

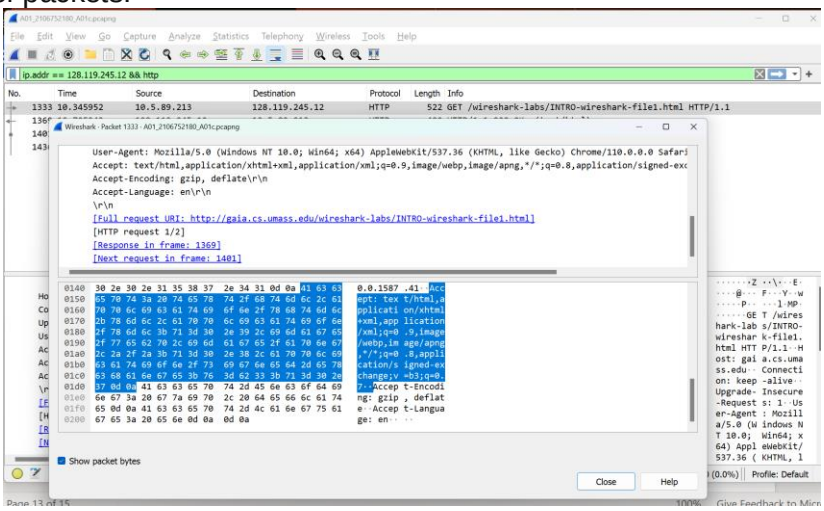
```
   IPv4 Address. . . . . . . . . . . : 10.5.89.213
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : 10.5.88.1

Ethernet adapter vEthernet (WSL):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::34c5:3071:3b6:46a9%47
   IPv4 Address. . . . . . . . . . . : 172.18.64.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

C:\Users\notal>
```

Packet Detail Screenshots

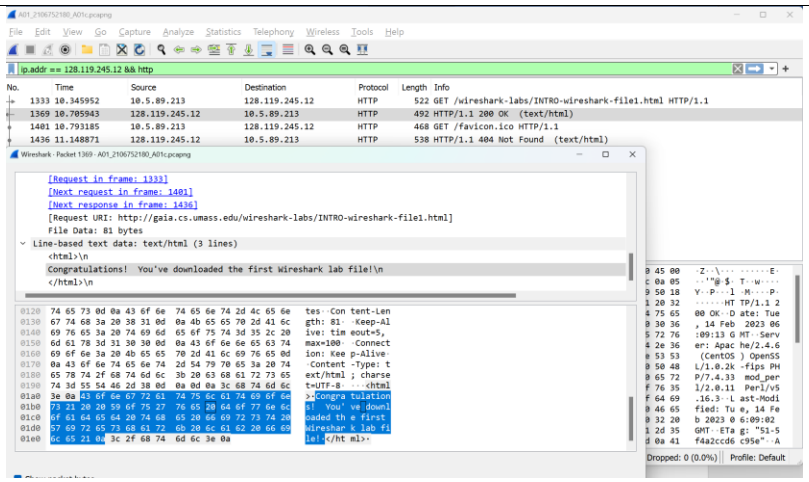
ip.addr == 128.119.245.12 && http

No.	Time	Source	Destination	Protocol	Length	Info
1333	10.345952	10.5.89.213	128.119.245.12	HTTP	522	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1369	10.705943	128.119.245.12	10.5.89.213	HTTP	492	HTTP/1.1 200 OK (text/html)
1401	10.793185	10.5.89.213	128.119.245.12	HTTP	468	GET /favicon.ico HTTP/1.1
1436	11.148871	128.119.245.12	10.5.89.213	HTTP	538	HTTP/1.1 404 Not Found (text/html)

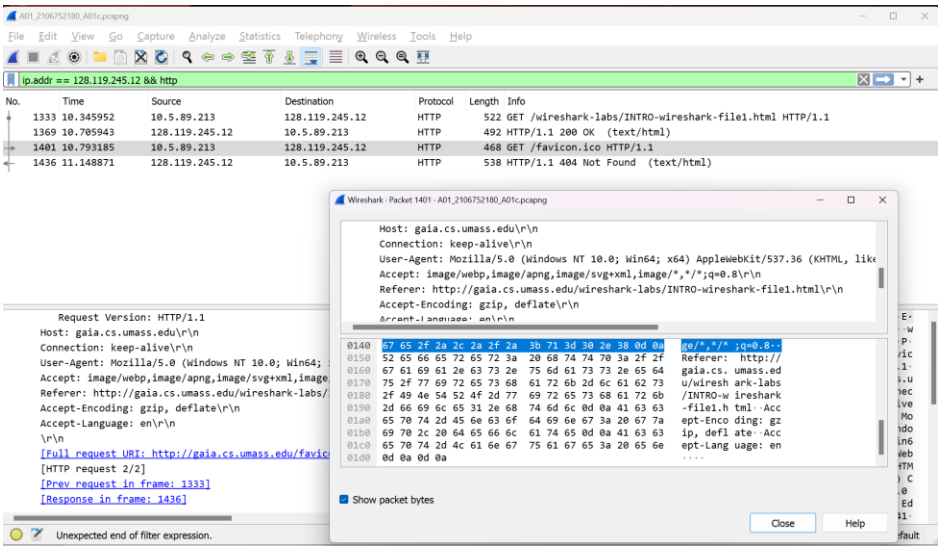
Detail of packets:

1. 

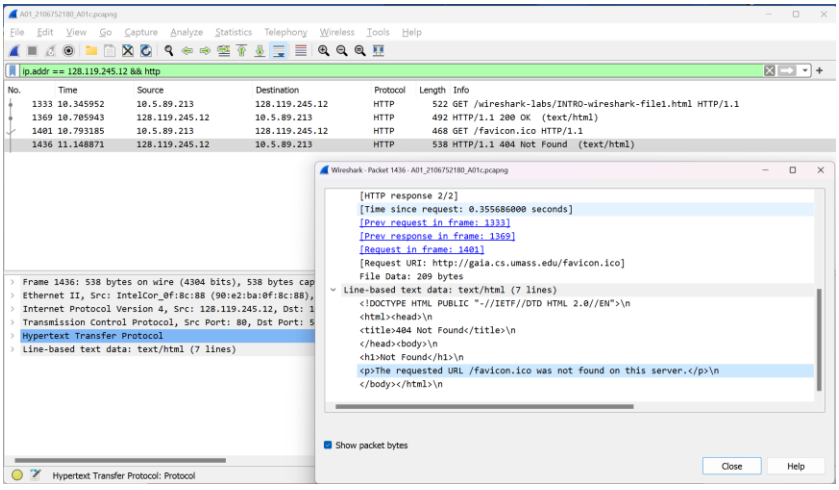
2.



3.



4.



Brief and Concise Explanation

I will explain what happened in the packet list step by step. Do note that http://gaia.cs.umass.edu/ has an IP address of 128.119.245.12 and my connection from Wireless LAN (ui.ac.id) is 10.5.89.213. Now that everything has been mentioned, I will explain:

1. My current connection (source = 10.5.89.213, IPV4 from Wireless LAN) request data from http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html (with IP address of 128.119.245.12). The data that were requested is the meta data of the website. In this case it is text/html.
2. Then http://gaia.cs.umass.edu/ return back a response of data that were requested to my connection (10.5.89.213) in the form of text/html (html data).
3. The next data that were requested (from my connection: 10.5.89.213) is favicon.ico which is the logo that is generated while opening the browser page (to http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html with IP of 128.119.245.12).
4. If we open http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html (with IP of 128.119.245.12), you could see that the website has no favicon.ico (seen as logo) hence it returned 404 error to us (10.5.89.213) means the requested data was not found.

A01d – Introduction to CLI Networking Tools

IP Config

Step 1: Local Device

```
C:\Users\notal>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2788:71bd:5367:cbe3%9
   Autoconfiguration IPv4 Address. . : 169.254.59.232
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : ui.ac.id
   Link-local IPv6 Address . . . . . : fe80::4d39:a525:c40f:2b06%19
   IPv4 Address. . . . . . . . . . . : 10.11.148.75
   Subnet Mask . . . . . . . . . . . : 255.255.224.0
   Default Gateway . . . . . . . . . : 10.11.128.1

Ethernet adapter vEthernet (WSL):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c3d6:a43a:3238:bc2e%54
   IPv4 Address. . . . . . . . . . . : 172.27.16.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

C:\Users\notal>
```

Step 2: GCP VM 1

```
alvaro_austin@vm-1-alvaro-2106752180:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 qdisc mq state UP group default qlen 1000
    link/ether 42:01:0a:80:00:03 brd ff:ff:ff:ff:ff:ff
    inet 10.128.0.3/32 metric 100 scope global dynamic ens4
       valid_lft 83553sec preferred_lft 83553sec
    inet6 fe80::4001:aff:fe80:3/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:b9:92:11:01 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:b9ff:fe92:1101/64 scope link
       valid_lft forever preferred_lft forever
5: veth34ff3f30@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group defau
lt
    link/ether fa:b8:a7:92:38:b7 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::f8b8:a7ff:fe92:38b7/64 scope link
       valid_lft forever preferred_lft forever
alvaro_austin@vm-1-alvaro-2106752180:~$
```

Step 2: GCP VM 2

```
alvaro_austin@vm-2-alvaro-2106752180:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 qdisc mq state UP group default qlen 1000
    link/ether 42:01:0a:8a:00:02 brd ff:ff:ff:ff:ff:ff
    inet 10.138.0.2/32 metric 100 scope global dynamic ens4
       valid_lft 83519sec preferred_lft 83519sec
    inet6 fe80::4001:aff:fe8a:2/64 scope link
       valid_lft forever preferred_lft forever
alvaro_austin@vm-2-alvaro-2106752180:~$
```

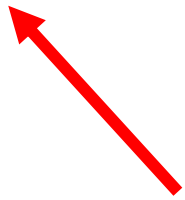
ARP

Step 1: Local Device

Command: **arp -av**

```
C:\Users\notal>arp -av

Interface: 127.0.0.1 --- 0x1
  Internet Address      Physical Address      Type
  224.0.0.2                                   static
  224.0.0.9                                   static
  224.0.0.22                                  static
  224.0.0.250                                 static
  224.0.0.253                                 static
  224.0.1.20                                  static
  224.0.1.60                                  static
  224.77.77.77                                static
  238.238.238.238                             static
  239.2.0.252                                 static
  239.192.152.143                             static
  239.242.6.7                                 static
  239.255.102.18                              static
  239.255.255.250                             static
  239.255.255.251                             static

Interface: 0.0.0.0 --- 0xffffffff
  Internet Address      Physical Address      Type
  224.0.0.9             01-00-5e-00-00-09     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.250           01-00-5e-00-00-fa     static
  224.0.0.253           01-00-5e-00-00-fd     static
  224.0.1.20            01-00-5e-00-01-14     static
  224.0.1.60            01-00-5e-00-01-3c     static
  224.77.77.77          01-00-5e-4d-4d-4d     static
  238.238.238.238       01-00-5e-6e-ee-ee     static
  239.2.0.252           01-00-5e-02-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.242.6.7           01-00-5e-72-06-07     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
```

```
Interface: 169.254.59.232 --- 0x9
  Internet Address      Physical Address      Type
  169.254.169.254       00-00-00-00-00-00     invalid
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.9             01-00-5e-00-00-09     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.250           01-00-5e-00-00-fa     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  224.0.1.20            01-00-5e-00-01-14     static
  224.0.1.60            01-00-5e-00-01-3c     static
  224.77.77.77          01-00-5e-4d-4d-4d     static
  238.238.238.238       01-00-5e-6e-ee-ee     static
  239.2.0.252           01-00-5e-02-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.242.6.7           01-00-5e-72-06-07     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 0.0.0.0 --- 0xffffffff
  Internet Address      Physical Address      Type
  224.0.0.9             01-00-5e-00-00-09     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.250           01-00-5e-00-00-fa     static
  224.0.0.253           01-00-5e-00-00-fd     static
  224.0.1.20            01-00-5e-00-01-14     static
  224.0.1.60            01-00-5e-00-01-3c     static
  224.77.77.77          01-00-5e-4d-4d-4d     static
  238.238.238.238       01-00-5e-6e-ee-ee     static
  239.2.0.252           01-00-5e-02-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.242.6.7           01-00-5e-72-06-07     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.251       01-00-5e-7f-ff-fb     static

Interface: 10.11.148.75 --- 0x13
  Internet Address      Physical Address      Type
  10.5.88.1             00-00-00-00-00-00     invalid
  10.5.89.117           00-00-00-00-00-00     invalid
  10.5.89.138           00-00-00-00-00-00     invalid
  10.5.89.249           00-00-00-00-00-00     invalid
  10.5.93.62            00-00-00-00-00-00     invalid
  10.5.95.224           00-00-00-00-00-00     invalid
  10.5.95.226           00-00-00-00-00-00     invalid
  10.11.128.1           90-e2-ba-0f-8c-88     dynamic
  192.168.100.129       00-00-00-00-00-00     invalid
  192.168.100.157       00-00-00-00-00-00     invalid
  192.168.100.173       00-00-00-00-00-00     invalid
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  224.0.1.20            01-00-5e-00-01-14     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.242.6.7           01-00-5e-72-06-07     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.27.16.1 --- 0x36
  Internet Address      Physical Address      Type
  172.27.16.95          00-15-5d-51-0f-71     dynamic
  172.27.31.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.250           01-00-5e-00-00-fa     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.253           01-00-5e-00-00-fd     static
  224.0.1.20            01-00-5e-00-01-14     static
  224.77.77.77          01-00-5e-4d-4d-4d     static
  238.238.238.238       01-00-5e-6e-ee-ee     static
  239.2.0.252           01-00-5e-02-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.242.6.7           01-00-5e-72-06-07     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
```



Primary Network Interface

Step 2: GCP VM 1

Command: **ip neigh show**

```
alvaro_austin@vm-1-alvaro-2106752180:~$ ip neigh show
172.17.0.2 dev docker0 lladdr 02:42:ac:11:00:02 STALE
10.128.0.1 dev ens4 lladdr 42:01:0a:80:00:01 REACHABLE
```

Step 2: GCP VM 2

Command: **ip neigh show**

```
alvaro_austin@vm-2-alvaro-2106752180:~$ ip neigh show
10.138.0.1 dev ens4 lladdr 42:01:0a:8a:00:01 REACHABLE
alvaro_austin@vm-2-alvaro-2106752180:~$
```

DiG

Step 1: GCP VM 1

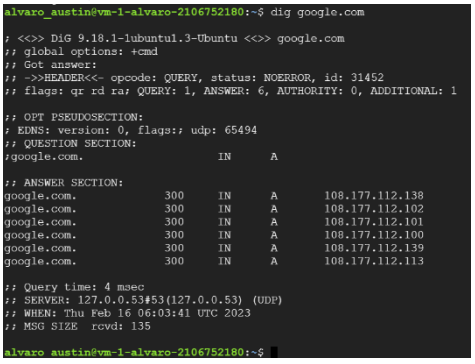
```
alvaro_austin@vm-1-alvaro-2106752180:~$ dig google.com

; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31452
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             300     IN      A       108.177.112.138
google.com.             300     IN      A       108.177.112.102
google.com.             300     IN      A       108.177.112.101
google.com.             300     IN      A       108.177.112.100
google.com.             300     IN      A       108.177.112.139
google.com.             300     IN      A       108.177.112.113

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Feb 16 06:03:41 UTC 2023
;; MSG SIZE  rcvd: 135

alvaro_austin@vm-1-alvaro-2106752180:~$
```

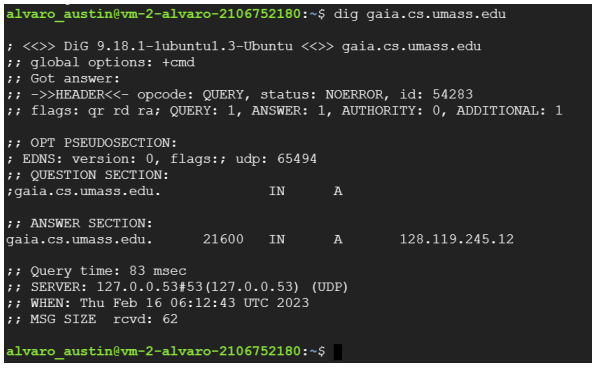
Step 1: GCP VM 2

```
alvaro_austin@vm-2-alvaro-2106752180:~$ dig gaia.cs.umass.edu

; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> gaia.cs.umass.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54283
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;gaia.cs.umass.edu.             IN      A

;; ANSWER SECTION:
gaia.cs.umass.edu.      21600   IN      A       128.119.245.12

;; Query time: 83 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Feb 16 06:12:43 UTC 2023
;; MSG SIZE  rcvd: 62

alvaro_austin@vm-2-alvaro-2106752180:~$
```

Step 2: Explanation

Side by side:





The output between dig on both VM is (VM 1 to google.com and VM2 to gaia.cs.umass.edu:

- Answer Section (IP Address): 6 (VM 1) to 1 (VM 2)
- Query time (in ms): 4 (VM1) to 83 (VM2) -> VM1 faster than VM2
- Message Size: 135 (VM1) to 62 (VM2)

The massive difference between 2 output is on the query time and the number of IP address assigned to google.com DNS. The reasoning between this difference based on what I could analyze is:

1. Google servers is all over the world. Meanwhile, gaia.cs.umass.edu is a server hosted in University of Massachusetts which located in eastern coast of US. In my VM1, the

server is hosted on us west, the geographical difference could be the main difference of query time.

2. The number of IP address give some good reasoning behind the speed. When we try to access a website, we tried to translate domain name's to IP address. Based on what I read on Internet, Google operates on it's own DNS server that is highly optimized. That's why there is 6 DNS record that **dig** found. This, most likely, increase the speed of DNS lookup. Meanwhile, gaia.cs.umass.edu might not operate on DNS server with the same speed or reliability as google.

Based on what I read, higher message size could means affect the speed and efficiency to be worse than smaller message size. Even though **dig google.com** gives higher message size, the speed that it delivers still much faster than **dig gaia.cs.umass.edu**. This means the factor above play a big role, such as number of IP address (affected the DNS lookup) and geographical location.

TCPDump

Step 3: TCPDump Terminal

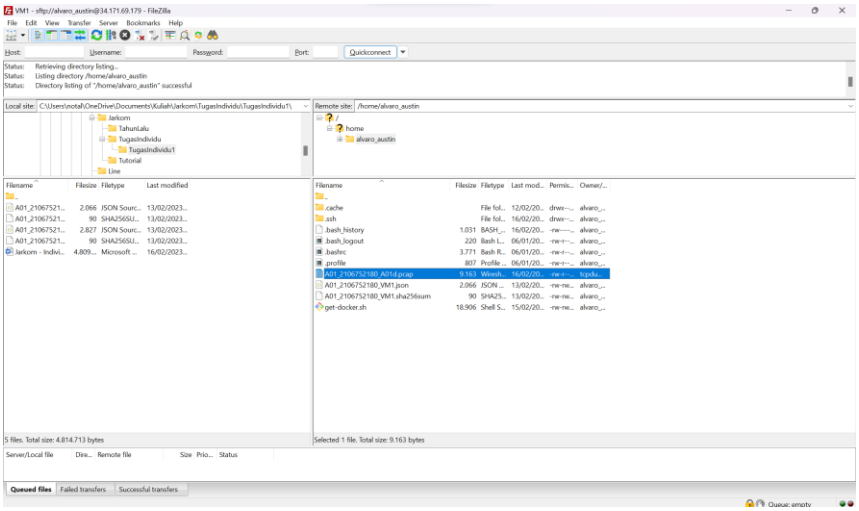
```
alvaro_austin@vm-1-alvaro-2106752180:~$ sudo tcpdump -i ens4 -w A01_2106752180_A01d.pcap port 80
tcpdump: listening on ens4, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C21 packets captured
21 packets received by filter
0 packets dropped by kernel
alvaro_austin@vm-1-alvaro-2106752180:~$
```

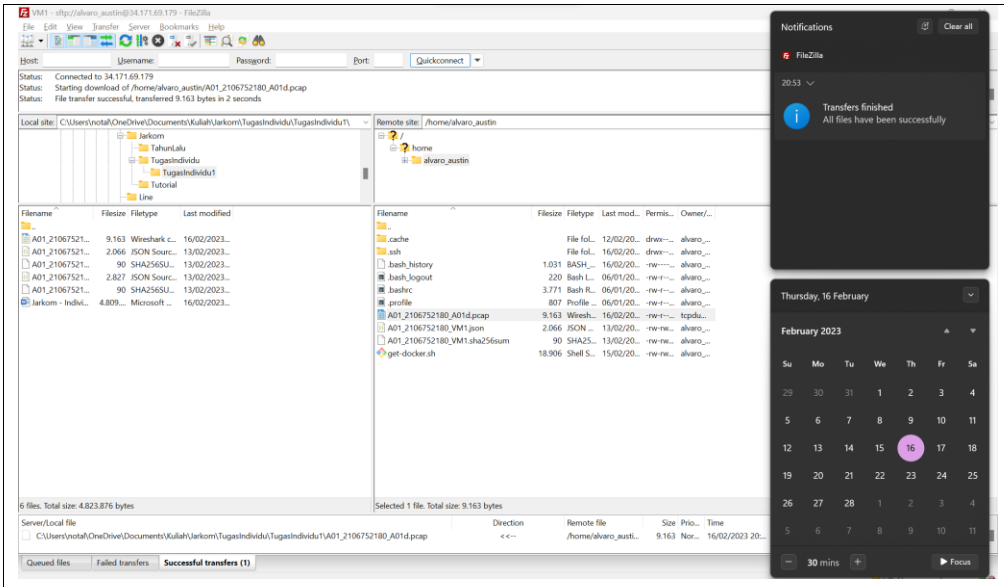
Step 3: Lynx Terminal

```
                                                                    ::Teori Bahasa dan Automata
                                    Web Kuliah Teori Bahasa dan Automata
                                          Fakultas Ilmu Komputer


   Please Login
   User ID:
     _______
   password:
     _______
      Reset OK
   lupa password?
   akun baru?
   Kuliah Lain
   SDA/DDP
   TBA Intern. Class
   Resources
   Petunjuk Umum (silakan klik, ada isian essay untuk mencoba submit saja)
   Regular Expression Utilities
   Download site JFlap 7.1
   Info Lain
   ** tidak ada **
   -->

   IFRAME: frame_detail




(NORMAL LINK) Use right-arrow or <return> to activate.
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

```
alvaro_austin@vm-1-alvaro-2106752180:~$ lynx http://aren.cs.ui.ac.id/tba/
alvaro_austin@vm-1-alvaro-2106752180:~$
```

Step 4: File Moved Verification

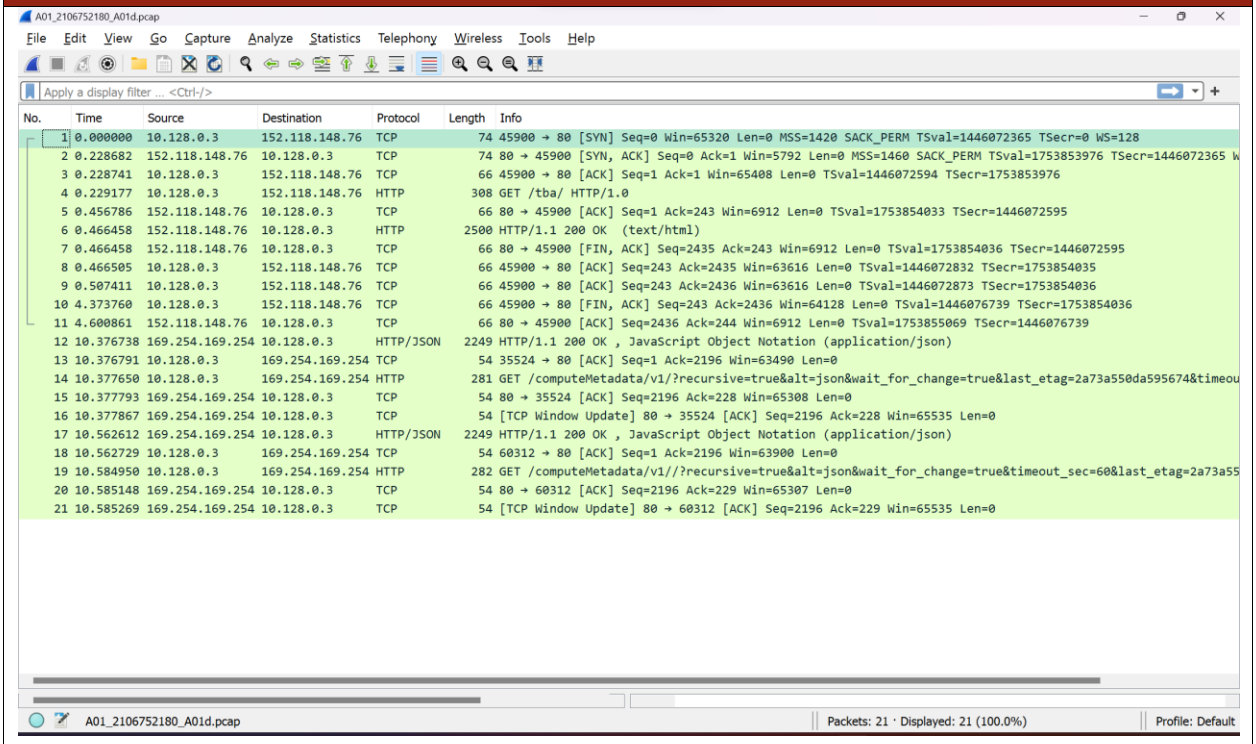




Step 6: Open Captured Data using TCPDump

```
alvaro_austin@vm-1-alvaro-2106752180:~$ sudo tcpdump -r A01_2106752180_A01d.pcap
reading from file A01_2106752180_A01d.pcap, link-type EN10MB (Ethernet), snapshot length 262144
13:39:41.574773 IP vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.45900 > aren.cs.ui.ac.id.http: Flags [S], seq 4088612188, win 65320, options [mss 1
420,sackOK,TS val 1446072365 ecr 0,nop,wscale 7], length 0
13:39:41.803455 IP aren.cs.ui.ac.id.http > vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.45900: Flags [S.], seq 1890340329, ack 4088612189, win 5792
, options [mss 1460,sackOK,TS val 1753853976 ecr 1446072365,nop,wscale 6], length 0
13:39:41.803514 IP vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.45900 > aren.cs.ui.ac.id.http: Flags [.], ack 1, win 511, options [nop,nop,TS val 1
446072594 ecr 1753853976], length 0
13:39:41.803950 IP vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.45900 > aren.cs.ui.ac.id.http: Flags [P.], seq 1:243, ack 1, win 511, options [nop,
nop,TS val 1446072595 ecr 1753853976], length 242: HTTP: GET /tba/ HTTP/1.0
13:39:42.031559 IP aren.cs.ui.ac.id.http > vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.45900: Flags [.], ack 243, win 108, options [nop,nop,TS val
 1753854033 ecr 1446072595], length 0
13:39:42.041231 IP aren.cs.ui.ac.id.http > vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.45900: Flags [P.], seq 1:2435, ack 243, win 108, options [n
op,nop,TS val 1753854035 ecr 1446072595], length 2434: HTTP: HTTP/1.1 200 OK
13:39:42.041231 IP aren.cs.ui.ac.id.http > vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.45900: Flags [F.], seq 2435, ack 243, win 108, options [nop
,nop,TS val 1753854036 ecr 1446072595], length 0
13:39:42.041278 IP vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.45900 > aren.cs.ui.ac.id.http: Flags [.], ack 2435, win 497, options [nop,nop,TS va
l 1446072832 ecr 1753854035], length 0
13:39:42.082184 IP vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.45900 > aren.cs.ui.ac.id.http: Flags [.], ack 2436, win 497, options [nop,nop,TS va
l 1446072873 ecr 1753854036], length 0
13:39:45.948533 IP vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.45900 > aren.cs.ui.ac.id.http: Flags [F.], seq 243, ack 2436, win 501, options [nop
,nop,TS val 1446076739 ecr 1753854036], length 0
13:39:46.175634 IP aren.cs.ui.ac.id.http > vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.45900: Flags [.], ack 244, win 108, options [nop,nop,TS val
 1753855069 ecr 1446076739], length 0
13:39:51.951511 IP metadata.google.internal.http > vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.35524: Flags [P.], seq 1561147367:1561149562, ack 9
31836665, win 65535, length 2195: HTTP: HTTP/1.1 200 OK
13:39:51.951564 IP vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.35524 > metadata.google.internal.http: Flags [.], ack 2195, win 63490, length 0
13:39:51.952423 IP vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.35524 > metadata.google.internal.http: Flags [P.], seq 1:228, ack 2195, win 63490,
length 227: HTTP: GET /computeMetadata/v1/?recursive=true&alt=json&wait_for_change=true&last_etag=2a73a550da595674&timeout_sec=60 HTTP/1.1
13:39:51.952566 IP metadata.google.internal.http > vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.35524: Flags [.], ack 228, win 65308, length 0
13:39:51.952640 IP metadata.google.internal.http > vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.35524: Flags [.], ack 228, win 65535, length 0
13:39:52.137385 IP metadata.google.internal.http > vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.60312: Flags [P.], seq 3762346621:3762348816, ack 2
580431099, win 65535, length 2195: HTTP: HTTP/1.1 200 OK
13:39:52.137502 IP vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.60312 > metadata.google.internal.http: Flags [.], ack 2195, win 63900, length 0
13:39:52.159723 IP vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.60312 > metadata.google.internal.http: Flags [P.], seq 1:229, ack 2195, win 63900,
length 228: HTTP: GET /computeMetadata/v1//?recursive=true&alt=json&wait_for_change=true&timeout_sec=60&last_etag=2a73a550da595674 HTTP/1.1
13:39:52.159921 IP metadata.google.internal.http > vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.60312: Flags [.], ack 229, win 65307, length 0
13:39:52.160042 IP metadata.google.internal.http > vm-1-alvaro-2106752180.c.jarkom-alvaro.internal.60312: Flags [.], ack 229, win 65535, length 0
alvaro_austin@vm-1-alvaro-2106752180:~$
```

Step 6: Open Captured Data using Wireshark



Step 7: Open Captured Data using TCPDump -n

```
alvaro_austin@vm-1-alvaro-2106752180:~$ sudo tcpdump -r A01_2106752180_A01d2.pcap -n
reading from file A01_2106752180_A01d2.pcap, link-type EN10MB (Ethernet), snapshot length 262144
14:46:53.118604 IP 169.254.169.254.80 > 10.128.0.3.35524: Flags [P.], seq 1561294432:1561296627, ack 931851874, win 65535, length 2195: HTTP: HTTP/1.1
 200 OK
14:46:53.118669 IP 10.128.0.3.35524 > 169.254.169.254.80: Flags [.], ack 2195, win 65535, length 0
14:46:53.119084 IP 10.128.0.3.35524 > 169.254.169.254.80: Flags [P.], seq 1:228, ack 2195, win 65535, length 227: HTTP: GET /computeMetadata/v1/?recur
sive=true&alt=json&wait_for_change=true&last_etag=2a73a550da595674&timeout_sec=60 HTTP/1.1
14:46:53.119257 IP 169.254.169.254.80 > 10.128.0.3.35524: Flags [.], ack 228, win 65308, length 0
14:46:53.119383 IP 169.254.169.254.80 > 10.128.0.3.35524: Flags [.], ack 228, win 65535, length 0
14:46:54.650494 IP 10.128.0.3.47876 > 152.118.148.76.80: Flags [S], seq 656445971, win 65320, options [mss 1420,sackOK,TS val 1450105441 ecr 0,nop,wsc
ale 7], length 0
14:46:54.800706 IP 169.254.169.254.80 > 10.128.0.3.60312: Flags [P.], seq 3762493686:3762495881, ack 2580446375, win 65535, length 2195: HTTP: HTTP/1.
1 200 OK
14:46:54.800756 IP 10.128.0.3.60312 > 169.254.169.254.80: Flags [.], ack 2195, win 65535, length 0
14:46:54.820873 IP 10.128.0.3.60312 > 169.254.169.254.80: Flags [P.], seq 1:229, ack 2195, win 65535, length 228: HTTP: GET /computeMetadata/v1//?recu
rsive=true&alt=json&wait_for_change=true&timeout_sec=60&last_etag=2a73a550da595674 HTTP/1.1
14:46:54.821071 IP 169.254.169.254.80 > 10.128.0.3.60312: Flags [.], ack 229, win 65307, length 0
14:46:54.821130 IP 169.254.169.254.80 > 10.128.0.3.60312: Flags [.], ack 229, win 65535, length 0
14:46:54.877159 IP 152.118.148.76.80 > 10.128.0.3.47876: Flags [S.], seq 126824891, ack 656445972, win 5792, options [mss 1460,sackOK,TS val 175486224
5 ecr 1450105441,nop,wscale 6], length 0
14:46:54.877233 IP 10.128.0.3.47876 > 152.118.148.76.80: Flags [.], ack 1, win 511, options [nop,nop,TS val 1450105668 ecr 1754862245], length 0
14:46:54.877651 IP 10.128.0.3.47876 > 152.118.148.76.80: Flags [P.], seq 1:243, ack 1, win 511, options [nop,nop,TS val 1450105668 ecr 1754862245], le
ngth 242: HTTP: GET /tba/ HTTP/1.0
14:46:55.103381 IP 152.118.148.76.80 > 10.128.0.3.47876: Flags [.], ack 243, win 108, options [nop,nop,TS val 1754862302 ecr 1450105668], length 0
14:46:55.113400 IP 152.118.148.76.80 > 10.128.0.3.47876: Flags [P.], seq 1:2435, ack 243, win 108, options [nop,nop,TS val 1754862304 ecr 1450105668],
 length 2434: HTTP: HTTP/1.1 200 OK
14:46:55.113400 IP 152.118.148.76.80 > 10.128.0.3.47876: Flags [F.], seq 2435, ack 243, win 108, options [nop,nop,TS val 1754862304 ecr 1450105668], l
ength 0
14:46:55.113449 IP 10.128.0.3.47876 > 152.118.148.76.80: Flags [.], ack 2435, win 497, options [nop,nop,TS val 1450105904 ecr 1754862304], length 0
14:46:55.154189 IP 10.128.0.3.47876 > 152.118.148.76.80: Flags [.], ack 2436, win 497, options [nop,nop,TS val 1450105945 ecr 1754862304], length 0
14:46:58.386208 IP 10.128.0.3.47876 > 152.118.148.76.80: Flags [F.], seq 243, ack 2436, win 501, options [nop,nop,TS val 1450109177 ecr 1754862304], l
ength 0
14:46:58.611462 IP 152.118.148.76.80 > 10.128.0.3.47876: Flags [.], ack 244, win 108, options [nop,nop,TS val 1754863179 ecr 1450109177], length 0
alvaro_austin@vm-1-alvaro-2106752180:~$
```

Step 8: Comparison Explanation

On step 6, without using -n parameter, it returns uses the name resolution for my machine and DNS for aren.cs.ui.ac.id. From what I read and analyze, without using -n basically converting IP addresses between my machine and target (aren.cs.ui.ac.id) to their domain name. This is great for human readability.

On step 7, as I mentioned previously, using -n gives the real output, the one without conversion of IP addresses to domain name. This increases output speed because we don't have to convert each time.

Netstat and ss

Step 1: Local Device

Command: **netstat -ano**

```
C:\Users\notal>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1724
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       9636
  TCP    0.0.0.0:5432           0.0.0.0:0              LISTENING       6552
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING       5288
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1448
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1280
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       3232
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       3756
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       4920
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       1356
  TCP    0.0.0.0:50128          0.0.0.0:0              LISTENING       4
  TCP    10.11.148.75:139       0.0.0.0:0              LISTENING       4
  TCP    10.11.148.75:49420     20.199.120.182:443     ESTABLISHED     5216
  TCP    10.11.148.75:49421     20.199.120.182:443     ESTABLISHED     5216
  TCP    10.11.148.75:55645     20.199.120.182:443     ESTABLISHED     16064
  TCP    10.11.148.75:55646     20.50.201.195:443      ESTABLISHED     16064
  TCP    10.11.148.75:55647     20.199.120.182:443     ESTABLISHED     20396
  TCP    10.11.148.75:61444     104.86.111.10:443      LAST_ACK        8652
  TCP    10.11.148.75:61451     2.18.66.163:443        LAST_ACK        8652
  TCP    10.11.148.75:61453     104.86.111.10:443      LAST_ACK        8652
  TCP    10.11.148.75:61454     2.18.66.163:443        LAST_ACK        8652
  TCP    10.11.148.75:61455     2.18.66.163:443        LAST_ACK        8652
  TCP    10.11.148.75:61456     2.18.66.163:443        LAST_ACK        8652
  TCP    10.11.148.75:61480     52.108.195.3:443       ESTABLISHED     17420
```

```
  TCP    10.11.148.75:63764     162.159.136.234:443    ESTABLISHED     5532
  TCP    10.11.148.75:64156     162.159.129.235:443    ESTABLISHED     5532
  TCP    10.11.148.75:64179     44.207.119.60:443      ESTABLISHED     2884
  TCP    10.11.148.75:64180     13.107.21.239:443      ESTABLISHED     16064
  TCP    10.11.148.75:64196     52.206.134.193:443     TIME_WAIT       0
  TCP    10.11.148.75:64200     20.189.173.10:443      TIME_WAIT       0
  TCP    10.11.148.75:64205     13.107.6.171:443       ESTABLISHED     16064
  TCP    10.11.148.75:64208     23.208.145.231:443     ESTABLISHED     16064
  TCP    10.11.148.75:64209     95.101.74.113:443      TIME_WAIT       0
  TCP    10.11.148.75:64212     52.111.233.3:443       ESTABLISHED     16064
  TCP    10.11.148.75:64213     52.111.233.3:443       ESTABLISHED     16064
  TCP    10.11.148.75:64214     40.126.35.87:443       ESTABLISHED     16064
  TCP    10.11.148.75:64215     40.126.35.87:443       ESTABLISHED     16064
  TCP    10.11.148.75:64217     40.126.35.87:443       ESTABLISHED     16064
  TCP    10.11.148.75:64218     13.107.6.171:443       ESTABLISHED     16064
  TCP    10.11.148.75:64219     104.18.32.68:80        TIME_WAIT       0
  TCP    10.11.148.75:64220     13.107.42.12:443       ESTABLISHED     17420
  TCP    10.11.148.75:64221     13.107.42.12:443       ESTABLISHED     17420
  TCP    10.11.148.75:64222     52.109.124.115:443     TIME_WAIT       0
  TCP    10.11.148.75:64223     13.107.237.59:443      ESTABLISHED     8652
  TCP    10.11.148.75:64224     2.18.66.163:443        ESTABLISHED     8652
  TCP    10.11.148.75:64225     13.107.18.254:443      ESTABLISHED     8652
  TCP    10.11.148.75:64226     52.109.68.101:443      ESTABLISHED     9916
  TCP    10.11.148.75:64227     13.107.226.59:443      ESTABLISHED     8652
  TCP    10.11.148.75:64228     2.18.66.163:443        ESTABLISHED     8652
  TCP    10.11.148.75:64229     2.18.66.163:443        ESTABLISHED     8652
  TCP    10.11.148.75:64230     2.18.66.163:443        ESTABLISHED     8652
  TCP    10.11.148.75:64231     204.79.197.222:443     ESTABLISHED     8652
  TCP    10.11.148.75:64232     152.199.43.62:443      ESTABLISHED     8652
  TCP    10.11.148.75:64233     52.98.33.130:443       ESTABLISHED     8652
  TCP    10.11.148.75:64234     104.86.111.10:443      ESTABLISHED     8652
  TCP    127.0.0.1:6463         0.0.0.0:0              LISTENING       18804
  TCP    127.0.0.1:53043        0.0.0.0:0              LISTENING       8356
  TCP    127.0.0.1:61424        127.0.0.1:61425        ESTABLISHED     2884
  TCP    127.0.0.1:61425        127.0.0.1:61424        ESTABLISHED     2884
  TCP    127.0.0.1:61426        127.0.0.1:61427        ESTABLISHED     2884
  TCP    127.0.0.1:61427        127.0.0.1:61426        ESTABLISHED     2884
  TCP    169.254.59.232:139     0.0.0.0:0              LISTENING       4
  TCP    172.27.16.1:139        0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       1724
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:5432              [::]:0                 LISTENING       6552
  TCP    [::]:49664             [::]:0                 LISTENING       1448
  TCP    [::]:49665             [::]:0                 LISTENING       1280
  TCP    [::]:49666             [::]:0                 LISTENING       3232
  TCP    [::]:49667             [::]:0                 LISTENING       3756
  TCP    [::]:49668             [::]:0                 LISTENING       4920
  TCP    [::]:49669             [::]:0                 LISTENING       1356
  TCP    [::]:50128             [::]:0                 LISTENING       4
  UDP    0.0.0.0:53             *:*                                    4556
  UDP    0.0.0.0:500            *:*                                    4844
  UDP    0.0.0.0:4500           *:*                                    4844
  UDP    0.0.0.0:5353           *:*                                    2656
  UDP    0.0.0.0:5353           *:*                                    2776
  UDP    0.0.0.0:5353           *:*                                    2776
  UDP    0.0.0.0:5353           *:*                                    2776
  UDP    0.0.0.0:5353           *:*                                    2776
  UDP    0.0.0.0:5353           *:*                                    2776
  UDP    0.0.0.0:5353           *:*                                    2776
  UDP    0.0.0.0:5355           *:*                                    2656
```

```
  UDP    0.0.0.0:50160          *:*                                    2656
  UDP    0.0.0.0:52407          *:*                                    2656
  UDP    0.0.0.0:57257          *:*                                    2656
  UDP    0.0.0.0:58623          *:*                                    2656
  UDP    0.0.0.0:59540          *:*                                    2656
  UDP    0.0.0.0:63885          *:*                                    4556
  UDP    0.0.0.0:63886          *:*                                    4556
  UDP    10.11.148.75:137       *:*                                    4
  UDP    10.11.148.75:138       *:*                                    4
  UDP    10.11.148.75:1900      *:*                                    13848
  UDP    10.11.148.75:64051     *:*                                    13848
  UDP    127.0.0.1:1900         *:*                                    13848
  UDP    127.0.0.1:10020        *:*                                    8356
  UDP    127.0.0.1:59521        *:*                                    14120
  UDP    127.0.0.1:63258        127.0.0.1:63258                        5188
  UDP    127.0.0.1:64052        *:*                                    13848
  UDP    169.254.59.232:137     *:*                                    4
  UDP    169.254.59.232:138     *:*                                    4
  UDP    169.254.59.232:1900    *:*                                    13848
  UDP    169.254.59.232:64050   *:*                                    13848
  UDP    172.27.16.1:137        *:*                                    4
  UDP    172.27.16.1:138        *:*                                    4
  UDP    172.27.16.1:1900       *:*                                    13848
  UDP    172.27.16.1:64053      *:*                                    13848
  UDP    [::]:500               *:*                                    4844
  UDP    [::]:4500              *:*                                    4844
  UDP    [::]:5353              *:*                                    2776
  UDP    [::]:5353              *:*                                    2776
  UDP    [::]:5353              *:*                                    2776
  UDP    [::]:5353              *:*                                    2656
  UDP    [::]:5355              *:*                                    2656
  UDP    [::]:50160             *:*                                    2656
  UDP    [::]:52407             *:*                                    2656
  UDP    [::]:57257             *:*                                    2656
  UDP    [::]:58623             *:*                                    2656
  UDP    [::]:59540             *:*                                    2656
  UDP    [::]:63887             *:*                                    4556
  UDP    [::1]:1900             *:*                                    13848
  UDP    [::1]:64048            *:*                                    13848
  UDP    [fe80::2788:71bd:5367:cbe3%9]:1900  *:*                       13848
  UDP    [fe80::2788:71bd:5367:cbe3%9]:64046  *:*                      13848
  UDP    [fe80::4d39:a525:c40f:2b06%19]:1900  *:*                      13848
  UDP    [fe80::4d39:a525:c40f:2b06%19]:64047  *:*                     13848
  UDP    [fe80::c3d6:a43a:3238:bc2e%54]:1900  *:*                      13848
  UDP    [fe80::c3d6:a43a:3238:bc2e%54]:64049  *:*                     13848

C:\Users\notal>
```

Step 2: GCP VM 1

Command: **ss -aetu**

```
alvaro_austin@vm-1-alvaro-2106752180:~$ ss -aetu
Netid     State         Recv-Q      Send-Q             Local Address:Port                Peer Address:Port
Process
udp       UNCONN        0           0                     127.0.0.1:323                      0.0.0.0:*
 ino:16640 sk:6d cgroup:/system.slice/chrony.service <->
udp       UNCONN        0           0                 127.0.0.53%lo:domain                   0.0.0.0:*
 uid:101 ino:16452 sk:6e cgroup:/system.slice/systemd-resolved.service <->
udp       UNCONN        0           0               10.128.0.3%ens4:bootpc                   0.0.0.0:*
 uid:100 ino:15629 sk:6f cgroup:/system.slice/systemd-networkd.service <->
udp       UNCONN        0           0                        [::1]:323                        [::]:*
 ino:16641 sk:70 cgroup:/system.slice/chrony.service v6only:1 <->
tcp       LISTEN        0           4096                  0.0.0.0:http                     0.0.0.0:*
 ino:17930 sk:71 cgroup:/system.slice/docker.service <->
tcp       LISTEN        0           4096              127.0.0.53%lo:domain                 0.0.0.0:*
 uid:101 ino:16453 sk:72 cgroup:/system.slice/systemd-resolved.service <->
tcp       LISTEN        0           128                   0.0.0.0:ssh                      0.0.0.0:*
 ino:17609 sk:73 cgroup:/system.slice/ssh.service <->
tcp       ESTAB         0           0                  10.128.0.3:33074          173.194.192.95:https
 timer:(keepalive,4.492ms,0) ino:38483 sk:68 cgroup:/system.slice/google-guest-agent.service <->
tcp       ESTAB         0           0                  10.128.0.3:45334          173.194.192.95:https
 timer:(keepalive,9.612ms,0) ino:38371 sk:69 cgroup:/system.slice/google-osconfig-agent.service <->
tcp       ESTAB         0           0                  10.128.0.3:ssh             35.235.244.33:42743
 timer:(keepalive,119min,0) ino:38517 sk:6a cgroup:/system.slice/ssh.service <->
tcp       ESTAB         0           0                  10.128.0.3:42142          169.254.169.254:http
 timer:(keepalive,18sec,0) ino:17597 sk:6b cgroup:/system.slice/google-guest-agent.service <->
tcp       TIME-WAIT     0           0                  10.128.0.3:39678          173.194.192.95:https
 timer:(timewait,8.288ms,0) ino:0 sk:74
tcp       ESTAB         0           0                  10.128.0.3:47472          169.254.169.254:http
 timer:(keepalive,18sec,0) ino:16679 sk:6c cgroup:/system.slice/google-osconfig-agent.service <->
tcp       LISTEN        0           4096                     [::]:http                        [::]:*
 ino:17933 sk:75 cgroup:/system.slice/docker.service v6only:1 <->
tcp       LISTEN        0           128                      [::]:ssh                         [::]:*
 ino:17611 sk:76 cgroup:/system.slice/ssh.service v6only:1 <->
alvaro_austin@vm-1-alvaro-2106752180:~$
```

Step 2: GCP VM 2

Command: **ss -aetu**

```
alvaro_austin@vm-2-alvaro-2106752180:~$ ss -aetu
Netid     State         Recv-Q      Send-Q             Local Address:Port                Peer Address:Port
Process
udp       UNCONN        0           0                 127.0.0.53%lo:domain                   0.0.0.0:*
 uid:101 ino:15324 sk:1 cgroup:/system.slice/systemd-resolved.service <->
udp       UNCONN        0           0               10.138.0.2%ens4:bootpc                   0.0.0.0:*
 uid:100 ino:15294 sk:2 cgroup:/system.slice/systemd-networkd.service <->
udp       UNCONN        0           0                     127.0.0.1:323                      0.0.0.0:*
 ino:15738 sk:3 cgroup:/system.slice/chrony.service <->
udp       UNCONN        0           0                        [::1]:323                        [::]:*
 ino:15739 sk:4 cgroup:/system.slice/chrony.service v6only:1 <->
tcp       LISTEN        0           4096              127.0.0.53%lo:domain                 0.0.0.0:*
 uid:101 ino:15325 sk:1001 cgroup:/system.slice/systemd-resolved.service <->
tcp       LISTEN        0           128                   0.0.0.0:ssh                      0.0.0.0:*
 ino:17238 sk:1002 cgroup:/system.slice/ssh.service <->
tcp       ESTAB         0           0                  10.138.0.2:45934          169.254.169.254:http
 timer:(keepalive,984ms,0) ino:17237 sk:1003 cgroup:/system.slice/google-guest-agent.service <->
tcp       TIME-WAIT     0           0                  10.138.0.2:60226           74.125.142.95:https
 timer:(timewait,344ms,0) ino:0 sk:1004
tcp       ESTAB         0           0                  10.138.0.2:36918          169.254.169.254:http
 timer:(keepalive,1.764ms,0) ino:28378 sk:1005 cgroup:/system.slice/google-guest-agent.service <->
tcp       ESTAB         0           0                  10.138.0.2:45892          169.254.169.254:http
 timer:(keepalive,968ms,0) ino:15789 sk:1006 cgroup:/system.slice/google-osconfig-agent.service <->
tcp       ESTAB         0           0                  10.138.0.2:48964           216.239.36.174:https
 timer:(keepalive,748ms,0) ino:28363 sk:1007 cgroup:/system.slice/google-osconfig-agent.service <->
tcp       ESTAB         0           0                  10.138.0.2:ssh             35.235.240.145:38691
 timer:(keepalive,119min,0) ino:28388 sk:1008 cgroup:/system.slice/ssh.service <->
tcp       ESTAB         0           0                  10.138.0.2:42238           216.239.34.174:https
 timer:(keepalive,7.148ms,0) ino:28841 sk:1009 cgroup:/system.slice/google-guest-agent.service <->
tcp       LISTEN        0           128                      [::]:ssh                         [::]:*
 ino:17240 sk:100a cgroup:/system.slice/ssh.service v6only:1 <->
alvaro_austin@vm-2-alvaro-2106752180:~$
```

Step 3: Explanation

Using **netstat -ano** and **ss -aetu** gives all active TCP and UDP connection. Both also gives local and Peer addresses. Not only that they also gives Port number (PID) that's really important if we want to use a port that is already been used by another process. Using those PID, we could kill the process corresponding to that port.

Ping and Tracert

Step 1: GCP VM 1

Ping VM1 to VM2(Internal IP = 10.138.0.2)

```
alvaro_austin@vm-1-alvaro-2106752180:~$ ping 10.138.0.2
PING 10.138.0.2 (10.138.0.2) 56(84) bytes of data.
64 bytes from 10.138.0.2: icmp_seq=1 ttl=64 time=33.3 ms
64 bytes from 10.138.0.2: icmp_seq=2 ttl=64 time=32.5 ms
64 bytes from 10.138.0.2: icmp_seq=3 ttl=64 time=32.3 ms
64 bytes from 10.138.0.2: icmp_seq=4 ttl=64 time=32.3 ms
64 bytes from 10.138.0.2: icmp_seq=5 ttl=64 time=32.2 ms
64 bytes from 10.138.0.2: icmp_seq=6 ttl=64 time=32.3 ms
64 bytes from 10.138.0.2: icmp_seq=7 ttl=64 time=32.8 ms
64 bytes from 10.138.0.2: icmp_seq=8 ttl=64 time=32.4 ms
64 bytes from 10.138.0.2: icmp_seq=9 ttl=64 time=32.2 ms
64 bytes from 10.138.0.2: icmp_seq=10 ttl=64 time=32.5 ms
64 bytes from 10.138.0.2: icmp_seq=11 ttl=64 time=32.2 ms
^C
--- 10.138.0.2 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10015ms
rtt min/avg/max/mdev = 32.189/32.455/33.283/0.308 ms
alvaro_austin@vm-1-alvaro-2106752180:~$
```

Traceroute VM 1 to VM 2 (Internal IP = 10.138.0.2)

```
alvaro_austin@vm-1-alvaro-2106752180:~$ traceroute 10.138.0.2
traceroute to 10.138.0.2 (10.138.0.2), 30 hops max, 60 byte packets
 1  vm-2-alvaro-2106752180.c.jarkom-alvaro.internal (10.138.0.2)  33.253 ms  33.166 ms *
alvaro_austin@vm-1-alvaro-2106752180:~$
```

Step 1: GCP VM 2

Ping VM2 to VM1(Internal IP = 10.138.0.3)

```
alvaro_austin@vm-2-alvaro-2106752180:~$ ping 10.128.0.3
PING 10.128.0.3 (10.128.0.3) 56(84) bytes of data.
64 bytes from 10.128.0.3: icmp_seq=1 ttl=64 time=33.5 ms
64 bytes from 10.128.0.3: icmp_seq=2 ttl=64 time=32.3 ms
64 bytes from 10.128.0.3: icmp_seq=3 ttl=64 time=32.4 ms
64 bytes from 10.128.0.3: icmp_seq=4 ttl=64 time=32.7 ms
64 bytes from 10.128.0.3: icmp_seq=5 ttl=64 time=32.5 ms
64 bytes from 10.128.0.3: icmp_seq=6 ttl=64 time=32.4 ms
64 bytes from 10.128.0.3: icmp_seq=7 ttl=64 time=32.7 ms
64 bytes from 10.128.0.3: icmp_seq=8 ttl=64 time=32.3 ms
64 bytes from 10.128.0.3: icmp_seq=9 ttl=64 time=32.1 ms
64 bytes from 10.128.0.3: icmp_seq=10 ttl=64 time=32.5 ms
64 bytes from 10.128.0.3: icmp_seq=11 ttl=64 time=32.4 ms
^C
--- 10.128.0.3 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10015ms
rtt min/avg/max/mdev = 32.124/32.519/33.523/0.354 ms
alvaro_austin@vm-2-alvaro-2106752180:~$
```

Traceroute VM 2 to VM1 (Internal IP = 10.138.0.3)

```
alvaro_austin@vm-2-alvaro-2106752180:~$ traceroute 10.128.0.3
traceroute to 10.128.0.3 (10.128.0.3), 30 hops max, 60 byte packets
 1  vm-1-alvaro-2106752180.c.jarkom-alvaro.internal (10.128.0.3)  33.577 ms *  33.370 ms
alvaro_austin@vm-2-alvaro-2106752180:~$
```

Step 2: Explanation

Based on what I could infer on the result, PING is used to test the reachability of a network host. It also counts the time it takes to react the network host. PING basically sends bytes of data then wait for response from the network host. If the data takes too long to be reached, then it will return time out. Meanwhile Traceroute is to trace path of the packets to reach the destination, in this case network hosts.