DEFENCE CYBER MAIN DIRECTORATE

Assignment of CTI

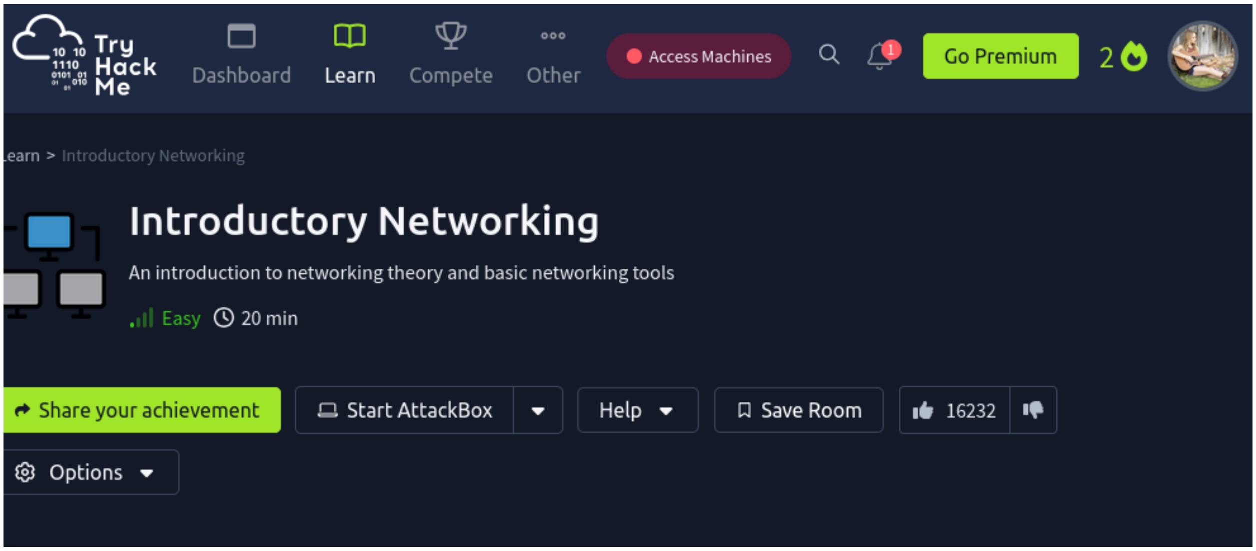
Group's Name and Their Id Number		
Rank	ID Number	Full Name
Cap.	00755597	Markos Matewos
Cap.	01387097	Birhane H/Mariam
2nd Lt.	00788107	Kahasi G/Silase
Serj.	00789207	Tezibt Gashaw
Ls Corp.	18333814	Dereje Solomon
Ls Corp.	01910813	Gashaw Erkyhun
Pt.	00591516	Tesfaye Wako
Pt.	00952516	Dagim Tesfaye
Pt.	01005416	Abebe Getu

Submitted to: Cap. Sisay D

Submission Date:Mar 19,2025

Answers

After you login to your account of THM account's tap on the learn link button and search for Introductory Networking, then join the room and start your journey with tasks. It looks like the below screenshot.



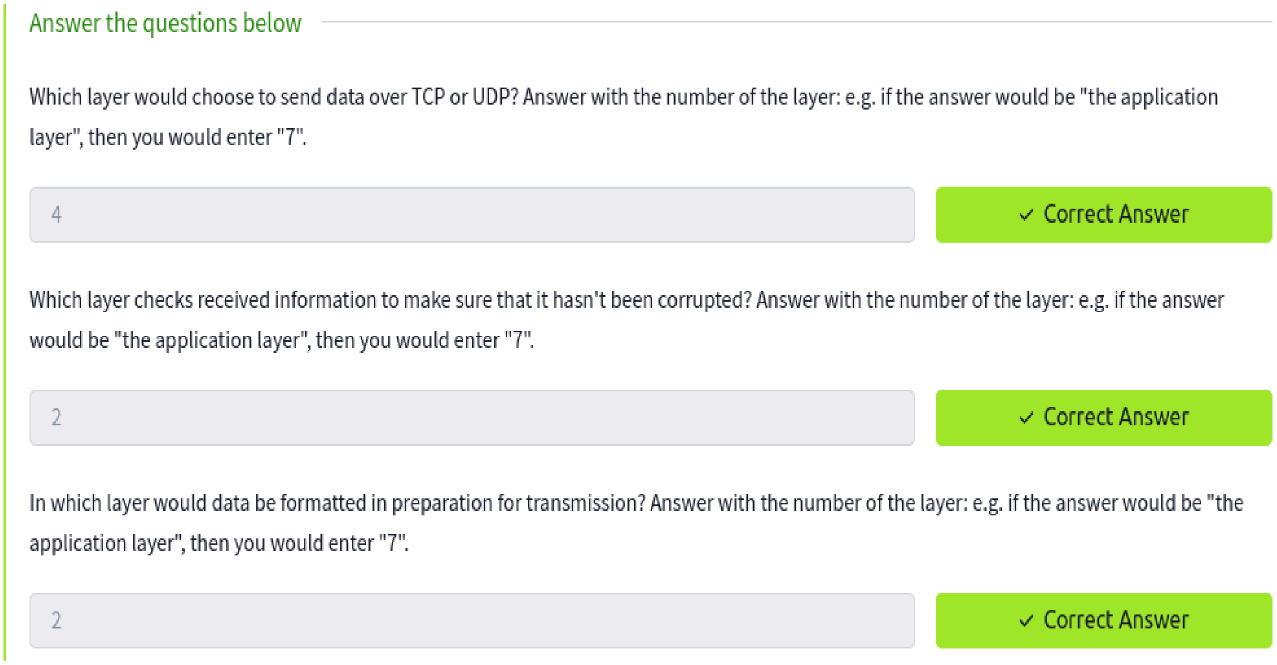
Introductory Networking

An introduction to networking theory and basic networking tools

The topics that we're going to cover are:

- □ The OSI Model
- □ The TCP/IP Model
- □ How these models look in practice
- □ An introduction to basic networking tools

Task 2



Answer the questions below

Which layer would choose to send data over TCP or UDP? Answer with the number of the layer: e.g. if the answer would be "the application layer", then you would enter "7".

4

✓ Correct Answer

Which layer checks received information to make sure that it hasn't been corrupted? Answer with the number of the layer: e.g. if the answer would be "the application layer", then you would enter "7".

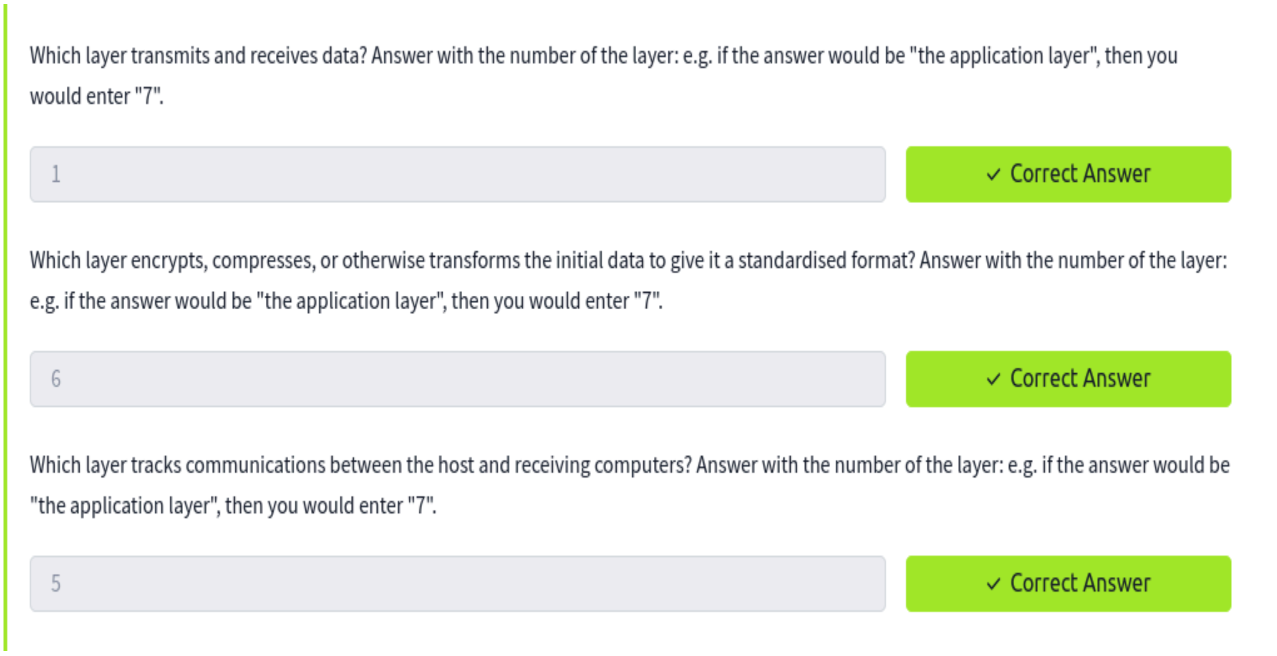
2

✓ Correct Answer

In which layer would data be formatted in preparation for transmission? Answer with the number of the layer: e.g. if the answer would be "the application layer", then you would enter "7".

2

✓ Correct Answer



Which layer transmits and receives data? Answer with the number of the layer: e.g. if the answer would be "the application layer", then you would enter "7".

1

✓ Correct Answer

Which layer encrypts, compresses, or otherwise transforms the initial data to give it a standardised format? Answer with the number of the layer: e.g. if the answer would be "the application layer", then you would enter "7".

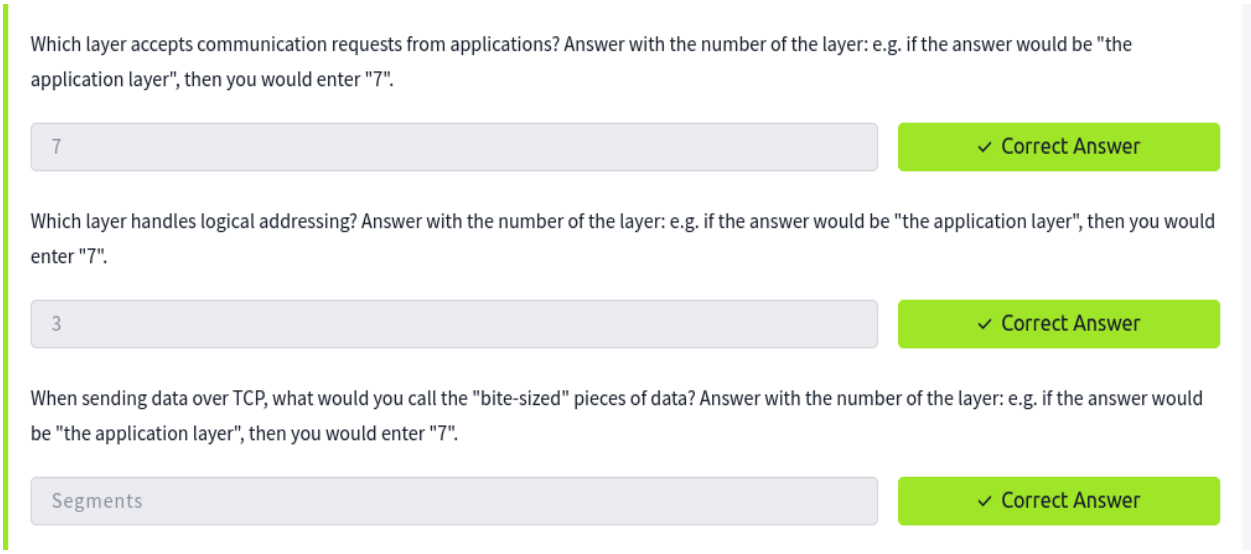
6

✓ Correct Answer

Which layer tracks communications between the host and receiving computers? Answer with the number of the layer: e.g. if the answer would be "the application layer", then you would enter "7".

5

✓ Correct Answer



Which layer accepts communication requests from applications? Answer with the number of the layer: e.g. if the answer would be "the application layer", then you would enter "7".

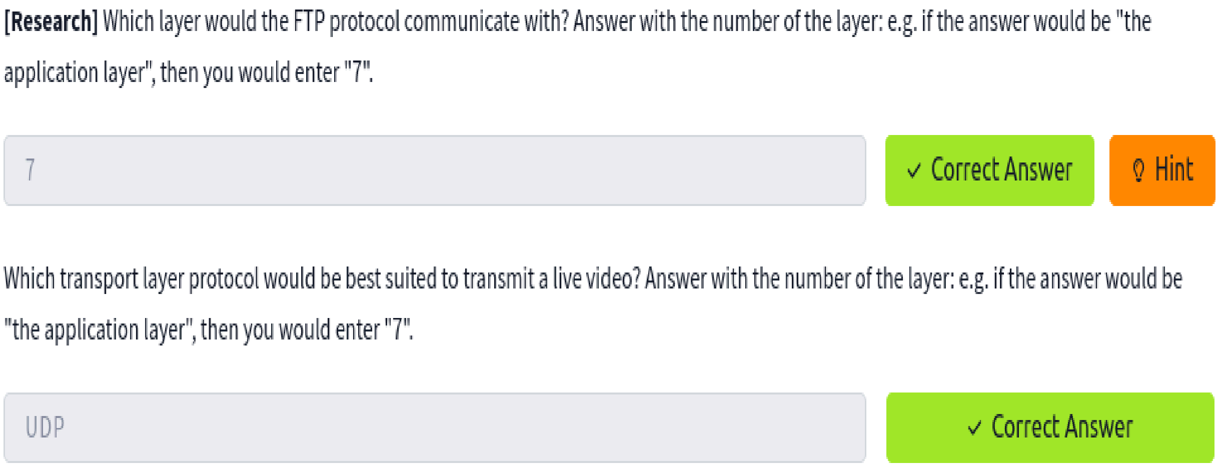
7

Which layer handles logical addressing? Answer with the number of the layer: e.g. if the answer would be "the application layer", then you would enter "7".

3

When sending data over TCP, what would you call the "bite-sized" pieces of data? Answer with the number of the layer: e.g. if the answer would be "the application layer", then you would enter "7".

Segments



[Research] Which layer would the FTP protocol communicate with? Answer with the number of the layer: e.g. if the answer would be "the application layer", then you would enter "7".

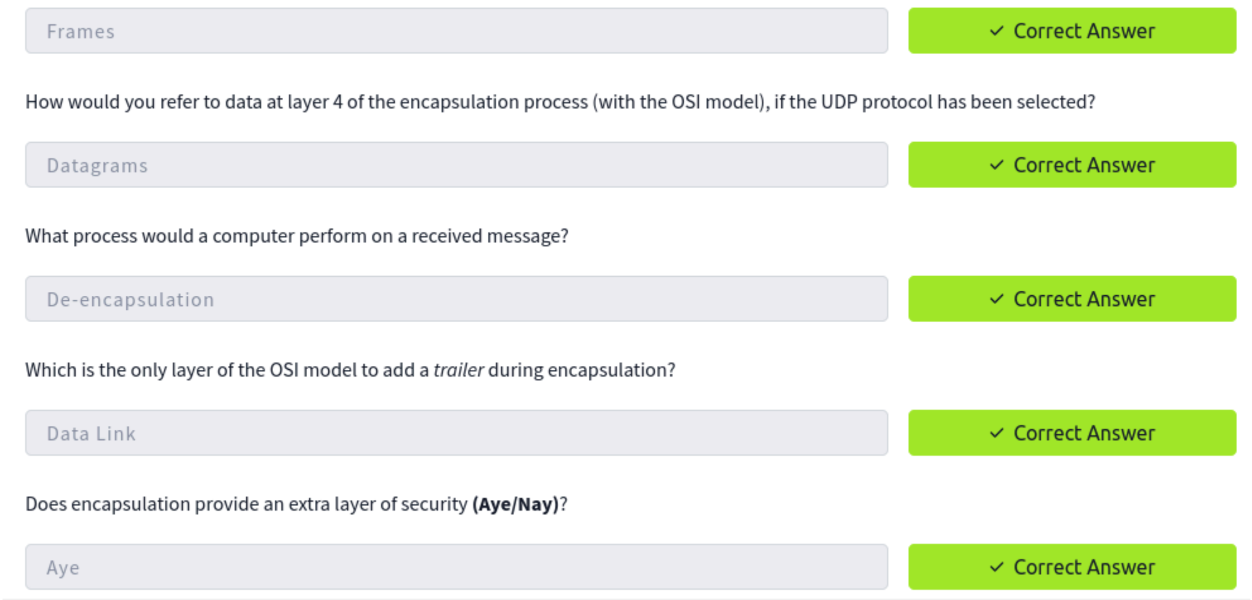
7

Which transport layer protocol would be best suited to transmit a live video? Answer with the number of the layer: e.g. if the answer would be "the application layer", then you would enter "7".

UDP

Task 3

How would you refer to data at layer 2 of the encapsulation process (with the OSI model)?



Frames

How would you refer to data at layer 4 of the encapsulation process (with the OSI model), if the UDP protocol has been selected?

Datagrams

What process would a computer perform on a received message?

De-encapsulation

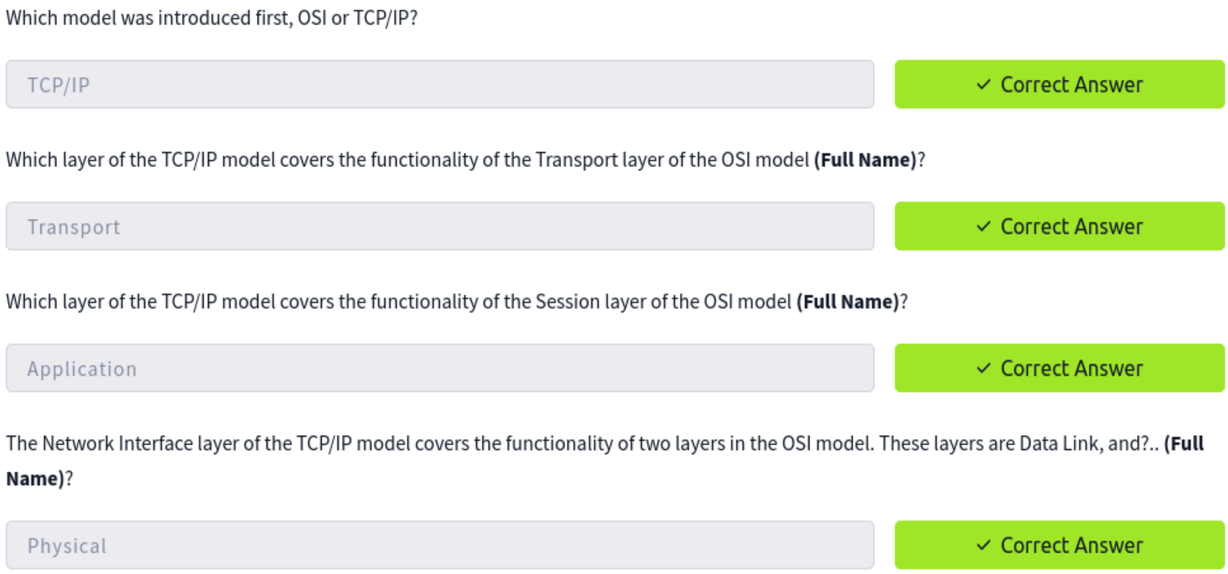
Which is the only layer of the OSI model to add a *trailer* during encapsulation?

Data Link

Does encapsulation provide an extra layer of security **(Aye/Nay)**?

Aye

Task 4



Which model was introduced first, OSI or TCP/IP?

TCP/IP

Which layer of the TCP/IP model covers the functionality of the Transport layer of the OSI model **(Full Name)**?

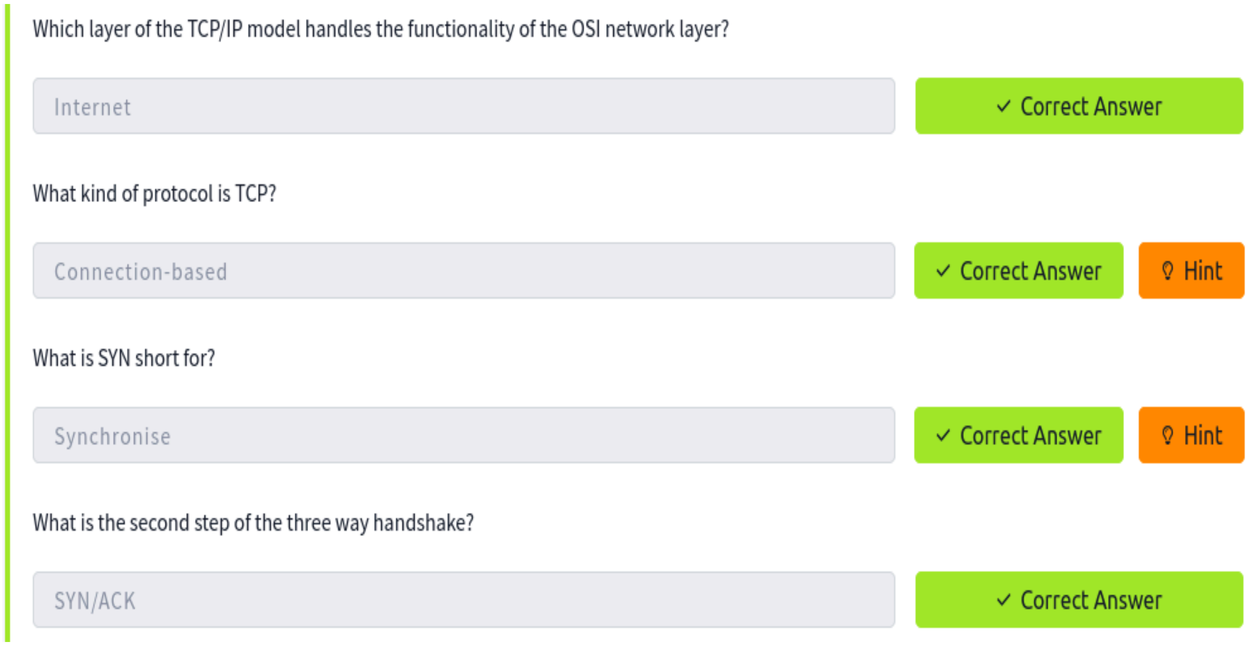
Transport

Which layer of the TCP/IP model covers the functionality of the Session layer of the OSI model **(Full Name)**?

Application

The Network Interface layer of the TCP/IP model covers the functionality of two layers in the OSI model. These layers are Data Link, and?.. **(Full Name)**?

Physical



Which layer of the TCP/IP model handles the functionality of the OSI network layer?

Internet

What kind of protocol is TCP?

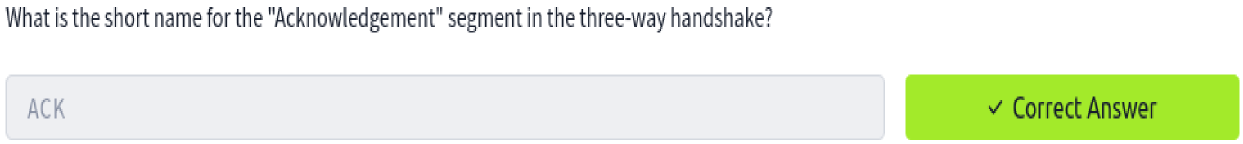
Connection-based

What is SYN short for?

Synchronise

What is the second step of the three way handshake?

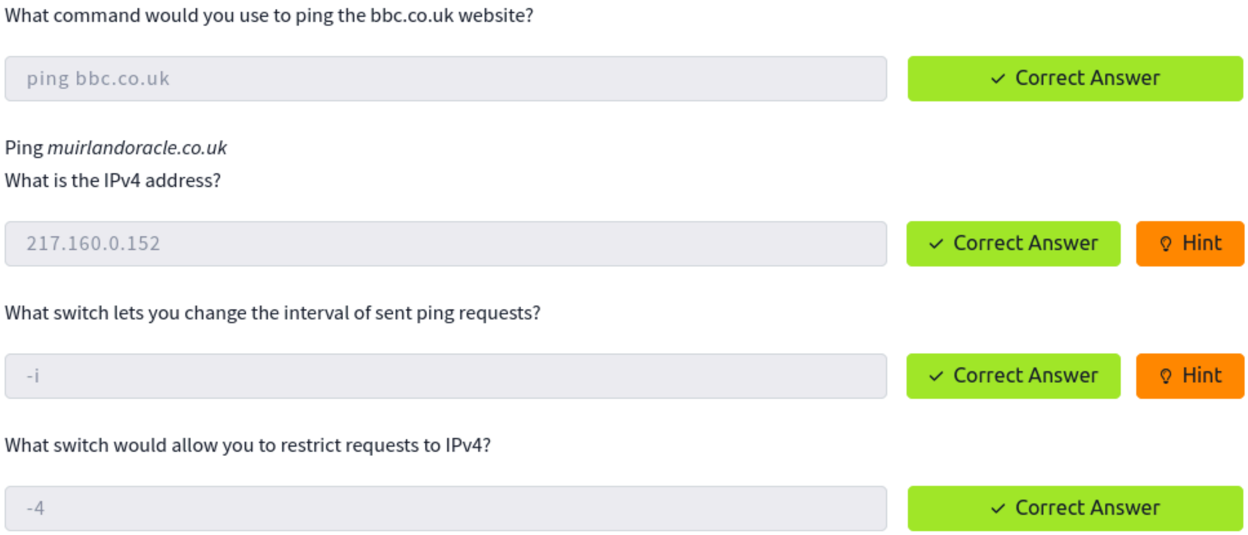
SYN/ACK



What is the short name for the "Acknowledgement" segment in the three-way handshake?

ACK

Task 5



What command would you use to ping the bbc.co.uk website?

ping bbc.co.uk

Ping *muirlandoracle.co.uk*
What is the IPv4 address?

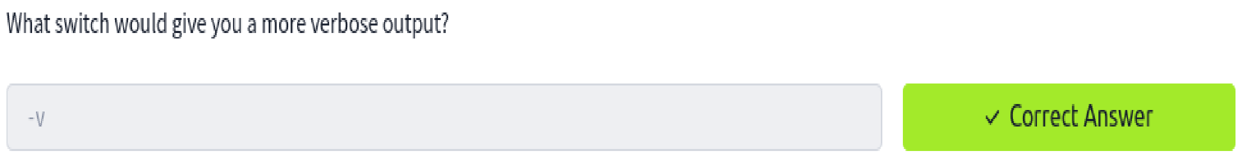
217.160.0.152

What switch lets you change the interval of sent ping requests?

-i

What switch would allow you to restrict requests to IPv4?

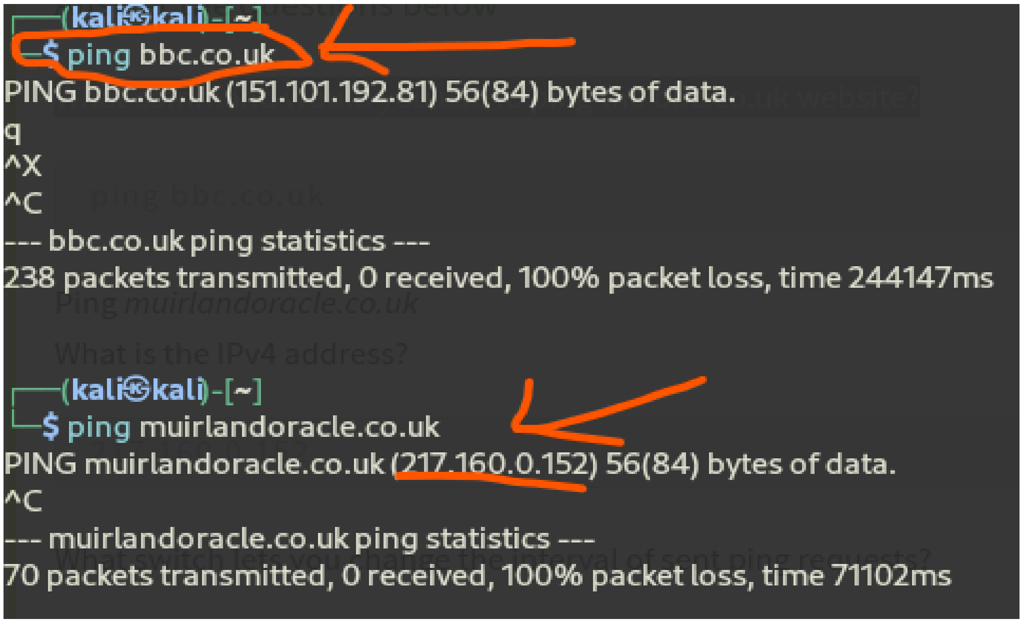
-4



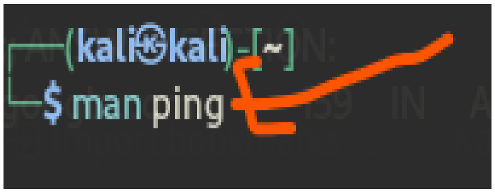
What switch would give you a more verbose output?

```
-v
```

Also we used the kali terminal to get the correct answers of those above challenges. Like IPv4, switch commands like –i,-v, etc.

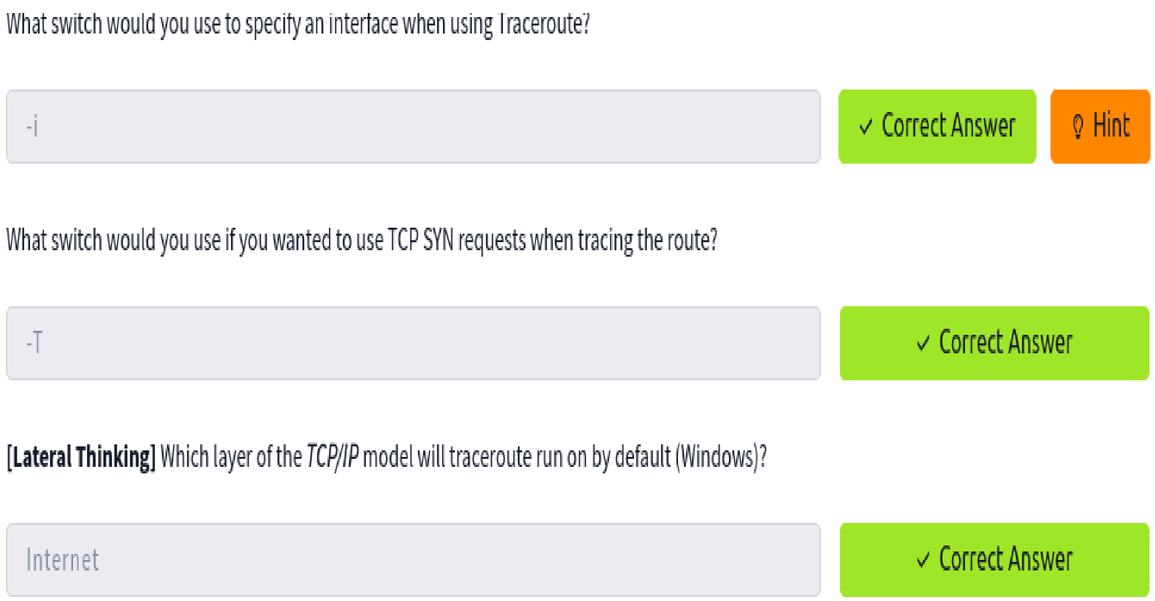


```
┌──(kali㉿kali)-[~]
└─$ ping bbc.co.uk
PING bbc.co.uk (151.101.192.81) 56(84) bytes of data.
q
^X
^C
--- bbc.co.uk ping statistics ---
238 packets transmitted, 0 received, 100% packet loss, time 244147ms

┌──(kali㉿kali)-[~]
└─$ ping muirlandoracle.co.uk
PING muirlandoracle.co.uk (217.160.0.152) 56(84) bytes of data.
^C
--- muirlandoracle.co.uk ping statistics ---
70 packets transmitted, 0 received, 100% packet loss, time 71102ms
```



```
┌──(kali㉿kali)-[~]
└─$ man ping
```

Task 6



What switch would you use to specify an interface when using Traceroute?

-i

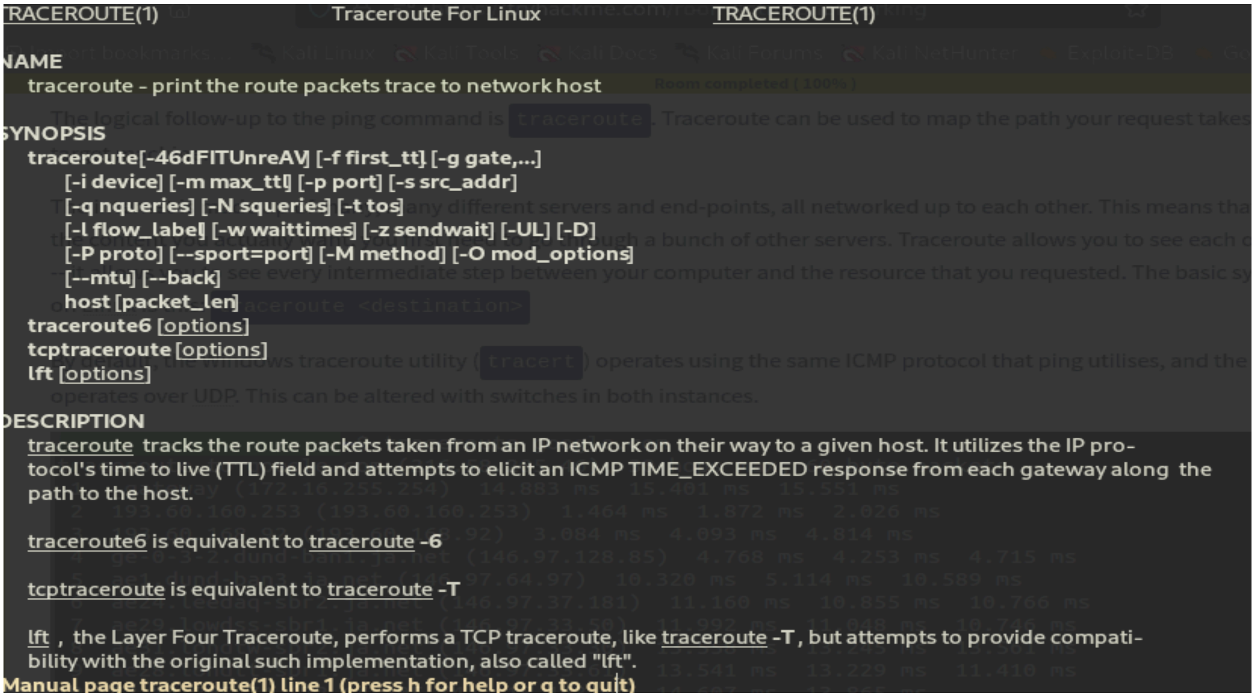
What switch would you use if you wanted to use TCP SYN requests when tracing the route?

-T

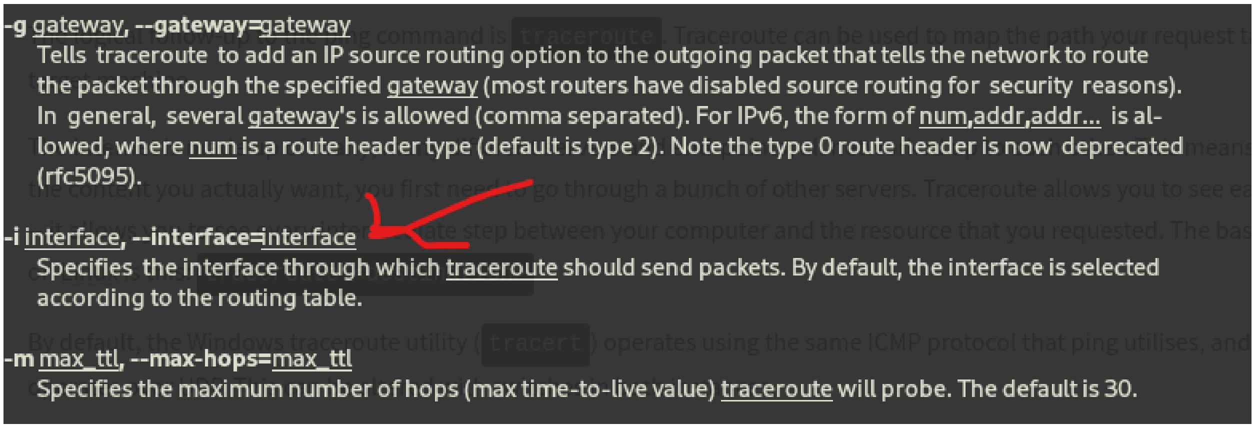
[Lateral Thinking] Which layer of the *TCP/IP* model will traceroute run on by default (Windows)?

Internet

A Man Command is to help us to get switch commands to specify an interface and TCP SYN requests on kali Linux .

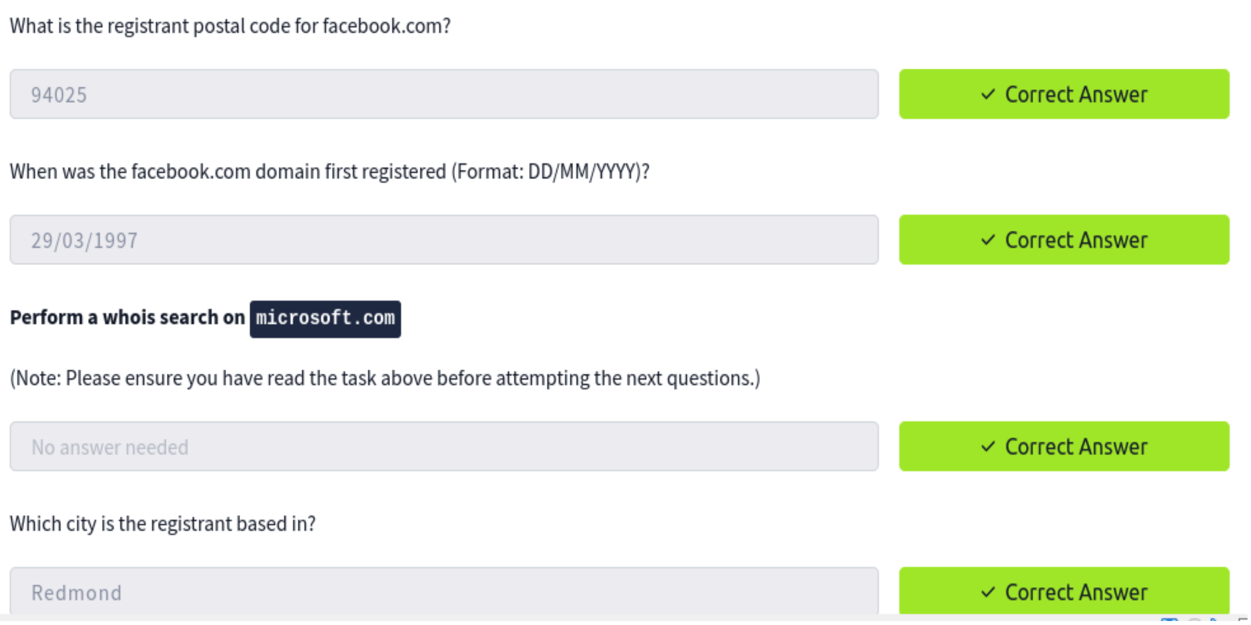


```
TRACEROUTE(1)              Traceroute For Linux              TRACEROUTE(1)

NAME
   traceroute - print the route packets trace to network host

SYNOPSIS
   traceroute[-46dFITUnreAV] [-f first_ttl] [-g gate,...]
      [-i device] [-m max_ttl] [-p port] [-s src_addr]
      [-q nqueries] [-N squeries] [-t tos]
      [-l flow_label] [-w waittimes] [-z sendwait] [-UL] [-D]
      [-P proto] [--sport=port] [-M method] [-O mod_options]
      [--mtu] [--back]
      host [packet_len]
   traceroute6 [options]
   tcptraceroute [options]
   lft [options]

DESCRIPTION
   traceroute  tracks the route packets taken from an IP network on their way to a given host. It utilizes the IP pro-
   tocol's time to live (TTL) field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along  the
   path to the host.

   traceroute6 is equivalent to traceroute -6

   tcptraceroute is equivalent to traceroute -T

   lft  ,  the Layer Four Traceroute, performs a TCP traceroute, like traceroute -T , but attempts to provide compati-
   bility with the original such implementation, also called "lft".
Manual page traceroute(1) line 1 (press h for help or q to quit)
```



```
-g gateway, --gateway=gateway
    Tells  traceroute  to add an IP source routing option to the outgoing packet that tells the network to route
    the packet through the specified gateway (most routers have disabled source routing for  security  reasons).
    In  general,  several gateway's is allowed (comma separated). For IPv6, the form of num,addr,addr...  is al-
    lowed, where num is a route header type (default is type 2). Note the type 0 route header is now  deprecated
    (rfc5095).

-i interface, --interface=interface
    Specifies  the interface through which traceroute should send packets. By default, the interface is selected
    according to the routing table.

-m max_ttl, --max-hops=max_ttl
    Specifies the maximum number of hops (max time-to-live value) traceroute will probe. The default is 30.
```

Task 7



What is the registrant postal code for facebook.com?

94025 | ✓ Correct Answer

When was the facebook.com domain first registered (Format: DD/MM/YYYY)?

29/03/1997 | ✓ Correct Answer

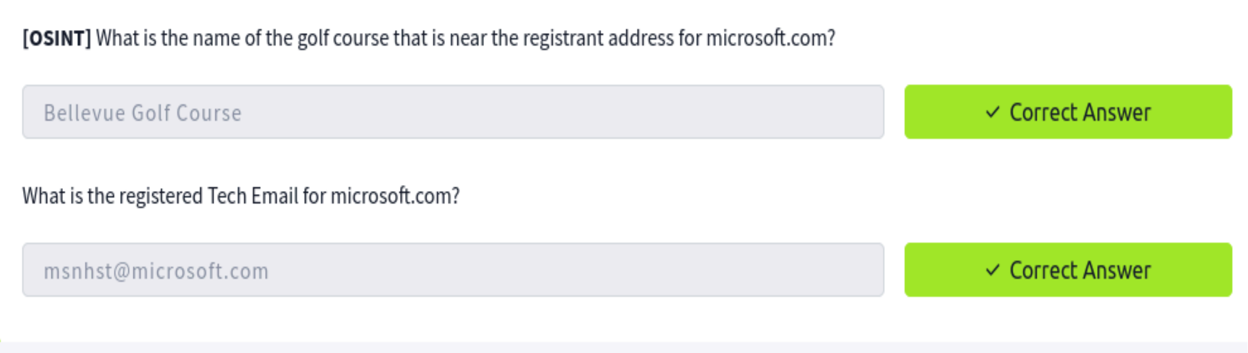
Perform a whois search on `microsoft.com`

(Note: Please ensure you have read the task above before attempting the next questions.)

No answer needed | ✓ Correct Answer

Which city is the registrant based in?

Redmond | ✓ Correct Answer



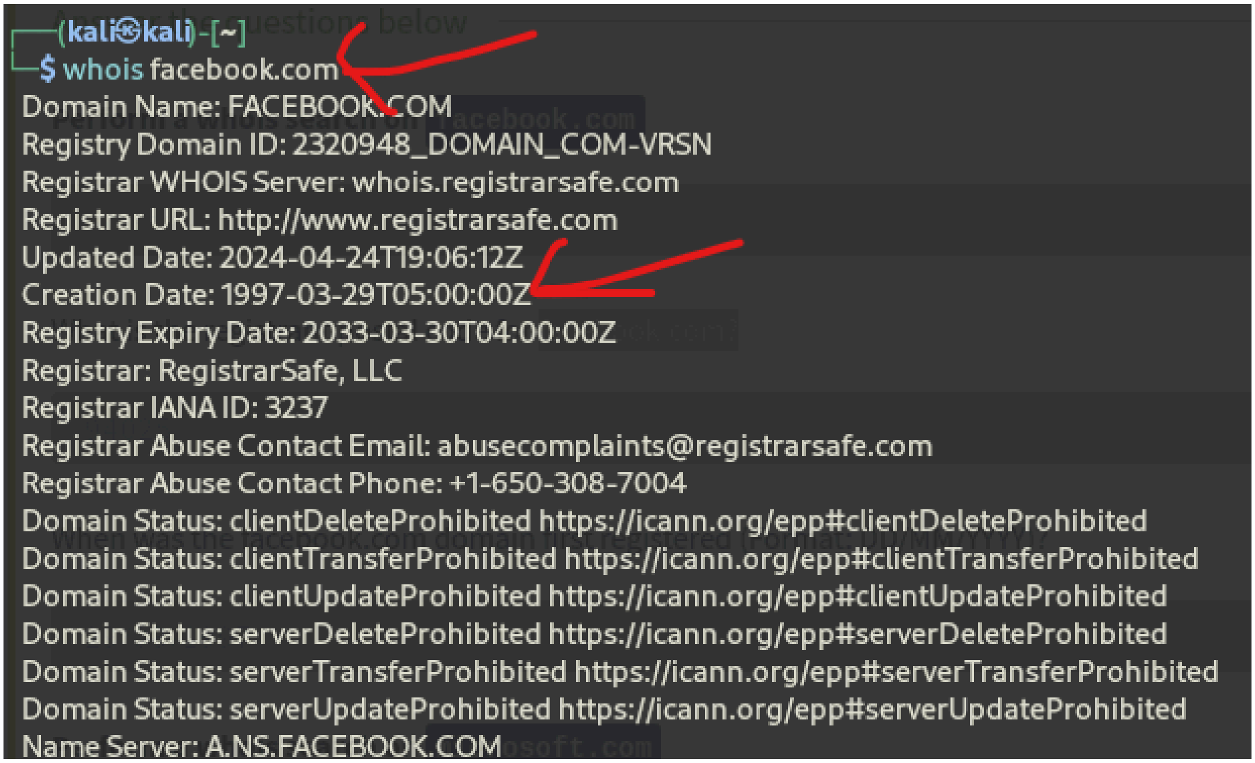
[OSINT] What is the name of the golf course that is near the registrant address for microsoft.com?

Bellevue Golf Course | ✓ Correct Answer

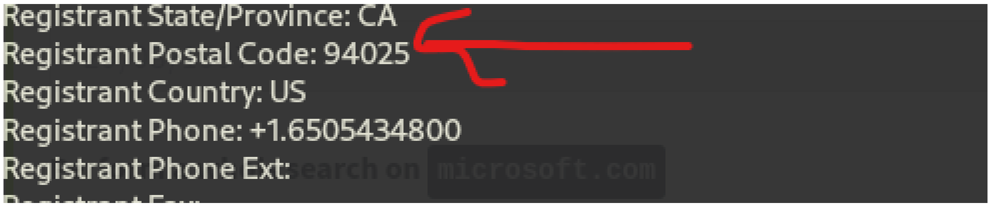
What is the registered Tech Email for microsoft.com?

msnhst@microsoft.com | ✓ Correct Answer

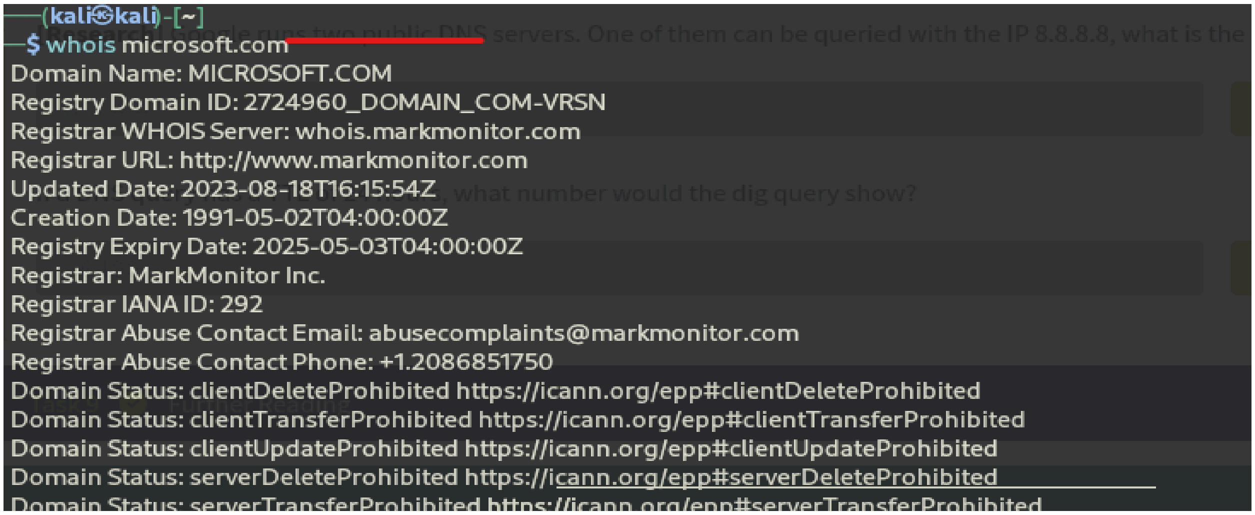
Also for task 7 we should have used some kali commands on the terminal to get the answers for those questions.



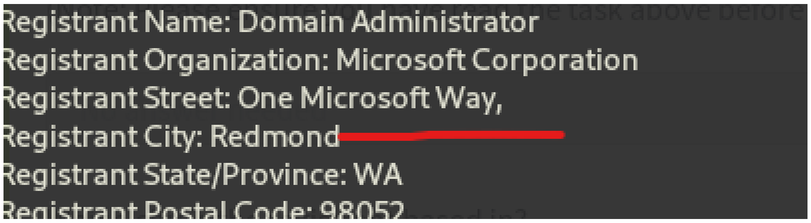
```
┌──(kali㉿kali)-[~]
└─$ whois facebook.com
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2024-04-24T19:06:12Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2033-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: A.NS.FACEBOOK.COM
```



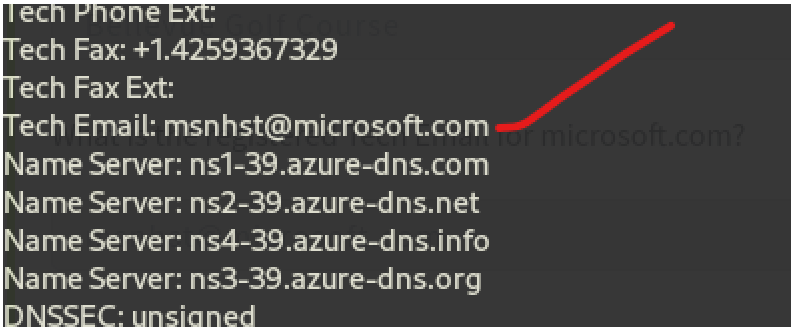
```
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax:
```



```
──(kali㉿kali)-[~]
└─$ whois microsoft.com
Domain Name: MICROSOFT.COM
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-08-18T16:15:54Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2025-05-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
```

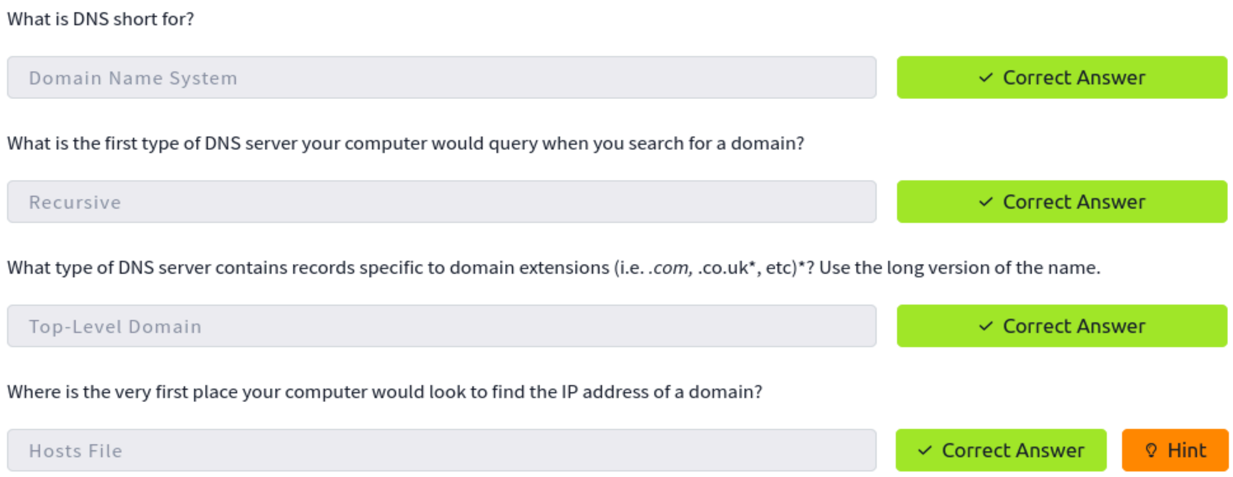


```
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
```



```
Tech Phone Ext:
Tech Fax: +1.4259367329
Tech Fax Ext:
Tech Email: msnhst@microsoft.com
Name Server: ns1-39.azure-dns.com
Name Server: ns2-39.azure-dns.net
Name Server: ns4-39.azure-dns.info
Name Server: ns3-39.azure-dns.org
DNSSEC: unsigned
```

Task 8



What is DNS short for?

Domain Name System

What is the first type of DNS server your computer would query when you search for a domain?

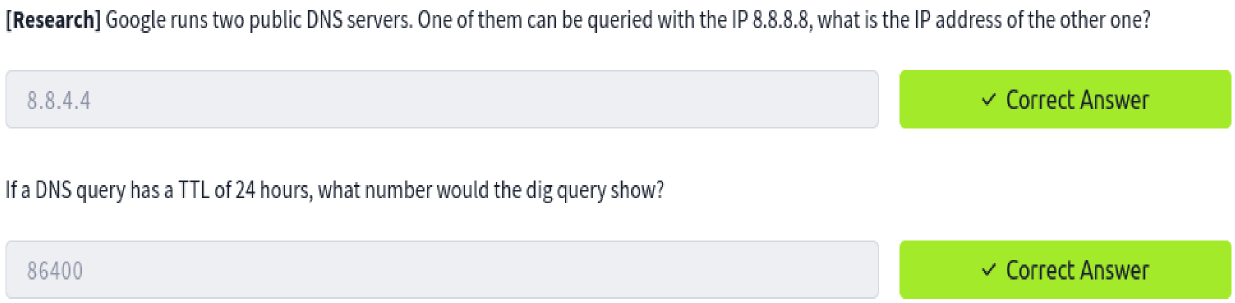
Recursive

What type of DNS server contains records specific to domain extensions (i.e. *.com*, .co.uk*, etc)*? Use the long version of the name.

Top-Level Domain

Where is the very first place your computer would look to find the IP address of a domain?

Hosts File



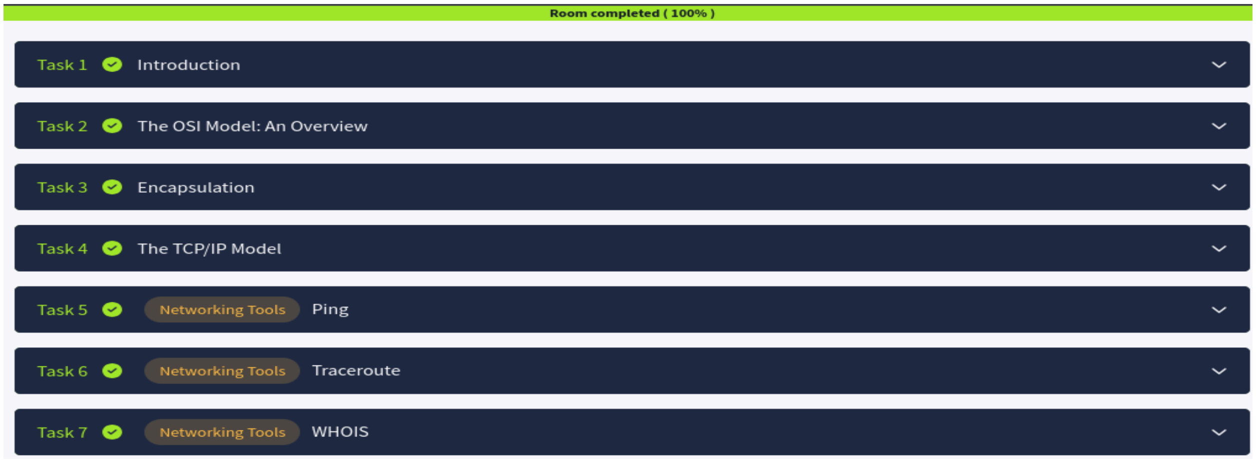
[Research] Google runs two public DNS servers. One of them can be queried with the IP 8.8.8.8, what is the IP address of the other one?

8.8.4.4

If a DNS query has a TTL of 24 hours, what number would the dig query show?

86400

After completing the progress the task looks like this and the congratulation message is popped.



Room completed (100%)

Task 1 Introduction

Task 2 The OSI Model: An Overview

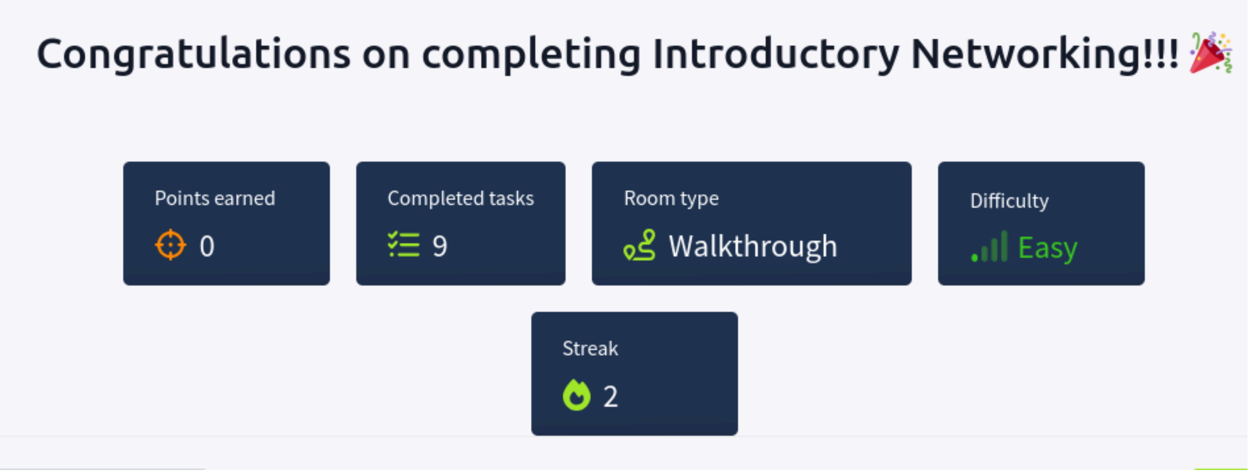
Task 3 Encapsulation

Task 4 The TCP/IP Model

Task 5 Ping

Task 6 Traceroute

Task 7 WHOIS



Congratulations on completing Introductory Networking!!! 🎉

Points earned
0

Completed tasks
9

Room type
Walkthrough

Difficulty
Easy

Streak
2