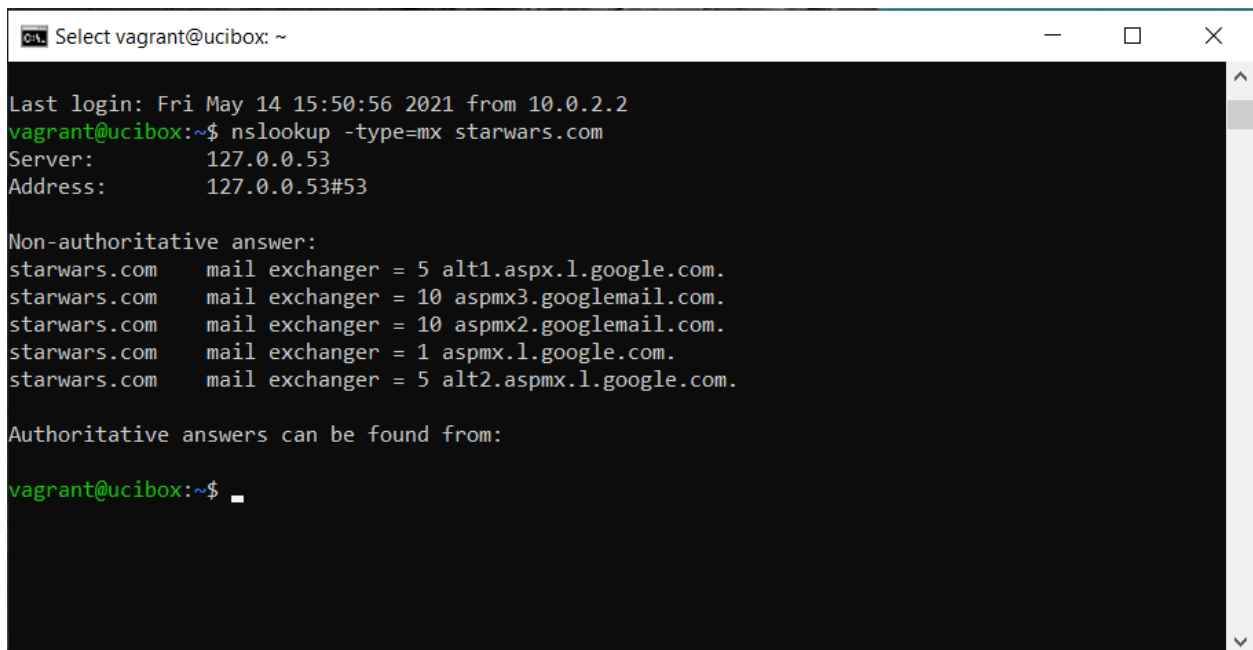


Mission 1

The new primary mail server is asltx.l.google.com and the secondary should be asltx.2.google.com.

nslookup -type=mx starwars.com



```

Select vagrant@ucibox: ~
Last login: Fri May 14 15:50:56 2021 from 10.0.2.2
vagrant@ucibox:~$ nslookup -type=mx starwars.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
starwars.com mail exchanger = 5 alt1.aspx.l.google.com.
starwars.com mail exchanger = 10 aspmx3.googlemail.com.
starwars.com mail exchanger = 10 aspmx2.googlemail.com.
starwars.com mail exchanger = 1 aspmx.l.google.com.
starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.

Authoritative answers can be found from:

vagrant@ucibox:~$
```

The resistance is not receiving any e-mail due to the incorrect mail exchange record.

Correct DNS record should be as follows:

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

starwars.com mail exchanger = 5 **asltx.2.google.com.**

starwars.com mail exchanger = 10 aspmx3.googlemail.com.

starwars.com mail exchanger = 10 aspmx2.googlemail.com.

starwars.com mail exchanger = 1 **asltx.l.google.com.**

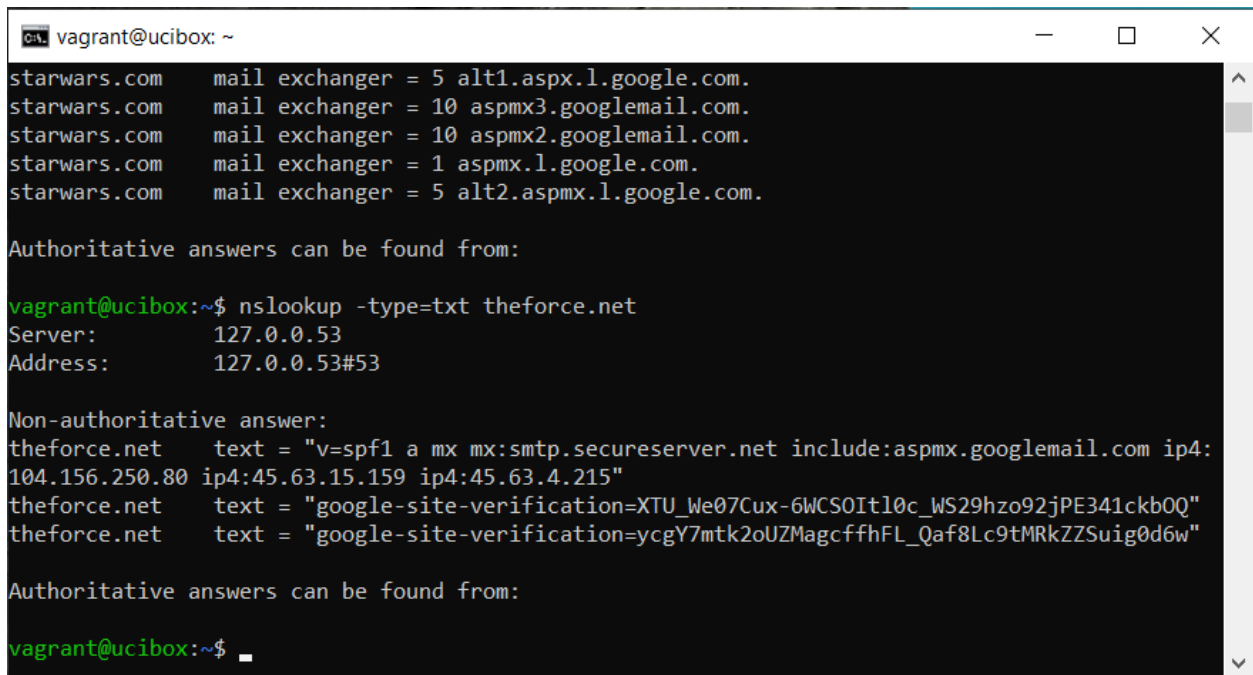
starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.

Authoritative answers can be found from:

Mission 2

theforce.net changed the IP address of their mail server to 45.23.176.21 while the network was down.

nslookup type=txt theforce.net

A screenshot of a terminal window titled 'vagrant@ucibox: ~'. The terminal shows the output of an nslookup command. It lists authoritative mail exchangers for starwars.com, then shows the authoritative answer for theforce.net (127.0.0.53). It then shows non-authoritative answers for theforce.net, including SPF and Google site verification records. The terminal ends with the prompt 'vagrant@ucibox:~\$' and a cursor.

```
vagrant@ucibox: ~
starwars.com mail exchanger = 5 alt1.aspx.l.google.com.
starwars.com mail exchanger = 10 aspmx3.googlemail.com.
starwars.com mail exchanger = 10 aspmx2.googlemail.com.
starwars.com mail exchanger = 1 aspmx.l.google.com.
starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.

Authoritative answers can be found from:

vagrant@ucibox:~$ nslookup -type=txt theforce.net
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
theforce.net text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"
theforce.net text = "google-site-verification=XTU_We07Cux-6WCS0It10c_WS29hzo92jPE341ckb0Q"
theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcfffhFL_Qaf8Lc9tMRkZZSuig0d6w"

Authoritative answers can be found from:

vagrant@ucibox:~$
```

The new IP address of 45.23.176.21 is not listed in the SPF record. Therefore it is being flagged as not coming from the theforce.net and as SPAM. The corrected record should be as follows:

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

theforce.net text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com
ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215 **ip4:45.23.176.21**"

theforce.net text = "google-site-verification=XTU_We07Cux-6WCSOI0c_WS29hzo92jPE341ckbOQ"

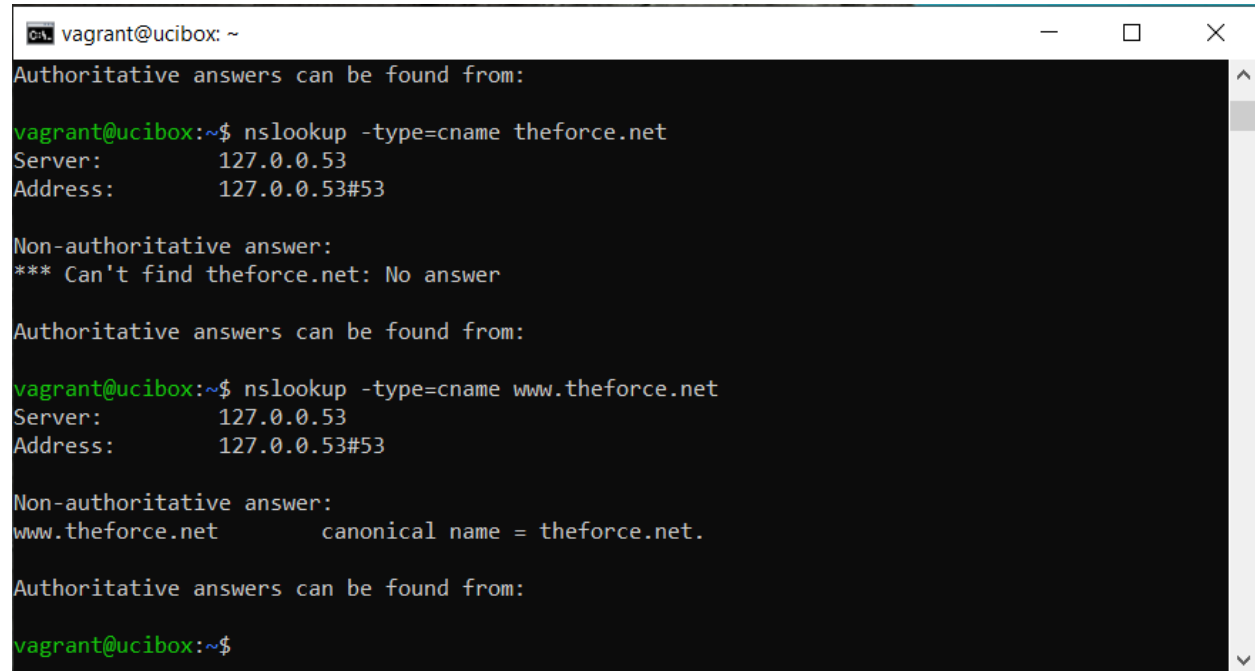
theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcfffhFL_Qaf8Lc9tMRkZZSuig0d6w"

Authoritative answers can be found from:

Mission 3

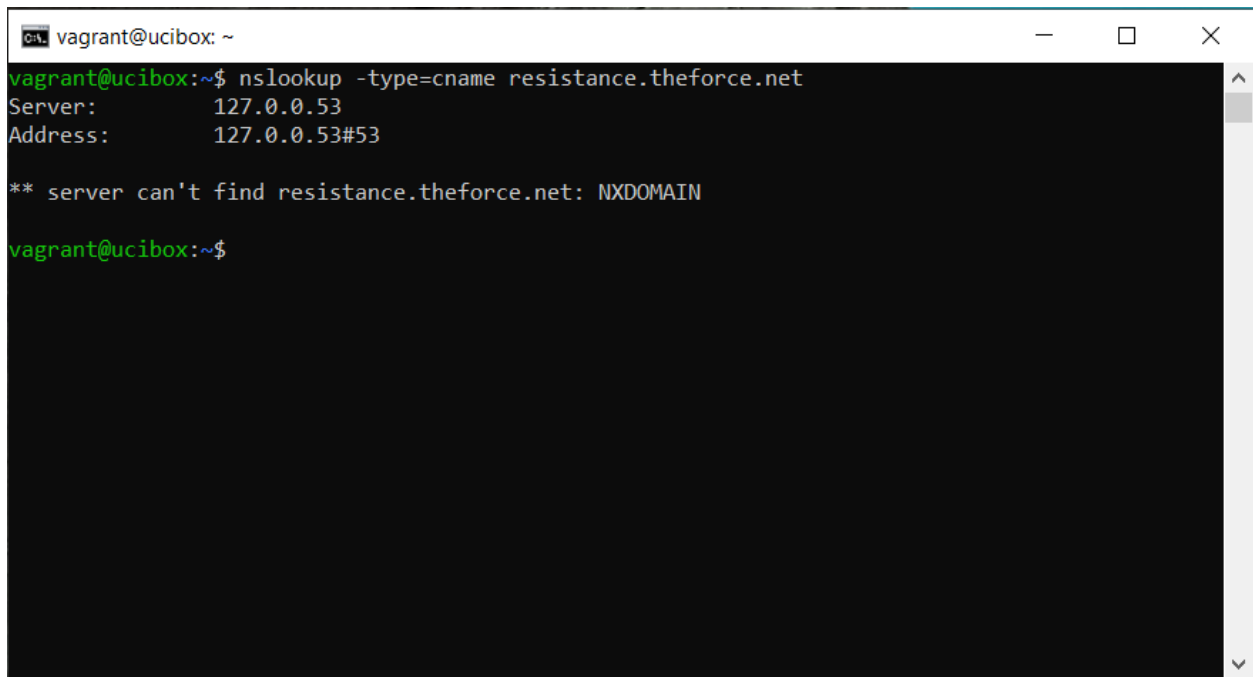
resistance.theforce.net is not re-directing to theforce.net.

nslookup type=cname ww.theforce.net



```
vagrant@ucibox: ~  
Authoritative answers can be found from:  
  
vagrant@ucibox:~$ nslookup -type=cname theforce.net  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
*** Can't find theforce.net: No answer  
  
Authoritative answers can be found from:  
  
vagrant@ucibox:~$ nslookup -type=cname www.theforce.net  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
www.theforce.net      canonical name = theforce.net.  
  
Authoritative answers can be found from:  
  
vagrant@ucibox:~$
```

nslookup -type=cname resistance.theforce.net shows there is no cname record for it.

A terminal window titled 'vagrant@ucibox: ~' with standard window controls. The terminal shows the command 'nslookup -type=cname resistance.theforce.net' and its output: 'Server: 127.0.0.53', 'Address: 127.0.0.53#53', and '** server can't find resistance.theforce.net: NXDOMAIN'. The prompt 'vagrant@ucibox:~\$' is visible at the bottom.

```
vagrant@ucibox: ~  
vagrant@ucibox:~$ nslookup -type=cname resistance.theforce.net  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
** server can't find resistance.theforce.net: NXDOMAIN  
  
vagrant@ucibox:~$
```

Corrected record should be as follows:

Server: 127.0.0.53

Address: 127.0.0.53#53

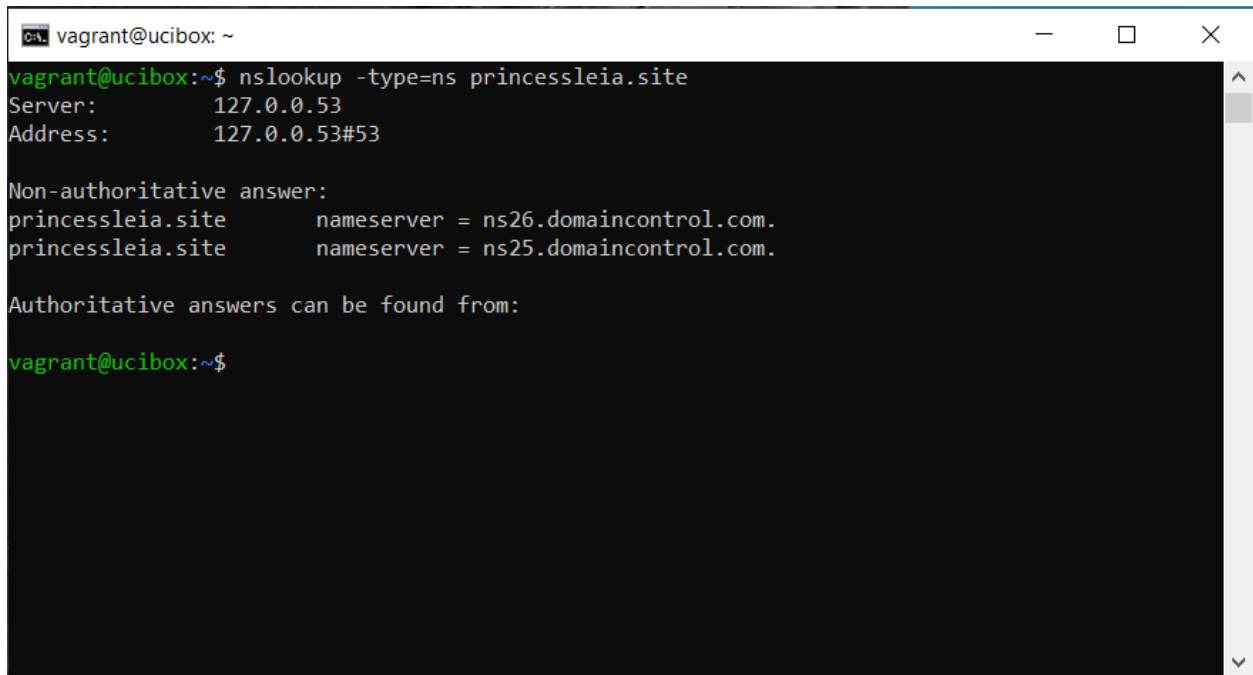
Non-authoritative answer:

resistance.theforce.net canonical name = theforce.net.

Authoritative answers can be found from:

Mission 4

`nslookup -type=ns princessleia.site` shows the backup DNS servers.

A terminal window titled 'vagrant@ucibox: ~' with standard window controls. The terminal shows the command 'nslookup -type=ns princessleia.site' and its output. The output includes the server address (127.0.0.53), a non-authoritative answer listing two nameservers (ns26.domaincontrol.com and ns25.domaincontrol.com), and a prompt for authoritative answers.

```
vagrant@ucibox: ~  
vagrant@ucibox:~$ nslookup -type=ns princessleia.site  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
princessleia.site    nameserver = ns26.domaincontrol.com.  
princessleia.site    nameserver = ns25.domaincontrol.com.  
  
Authoritative answers can be found from:  
vagrant@ucibox:~$
```

We need to add `ns2.galaxybackup.com` to the record to make sure backup server can be accessed.

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

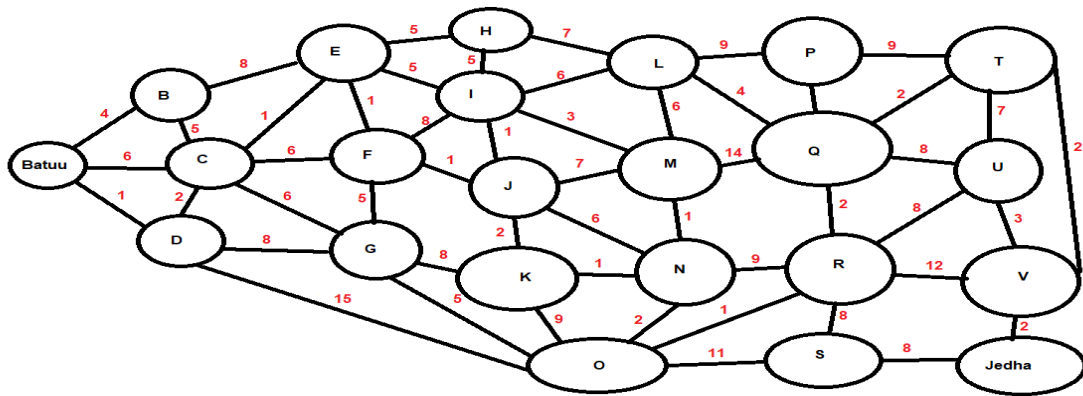
princessleia.site nameserver = ns26.domaincontrol.com.

princessleia.site nameserver = ns25.domaincontrol.com.

princessleia.site nameserver = ns2.galaxybackup.com.

Authoritative answers can be found from:

Mission 5



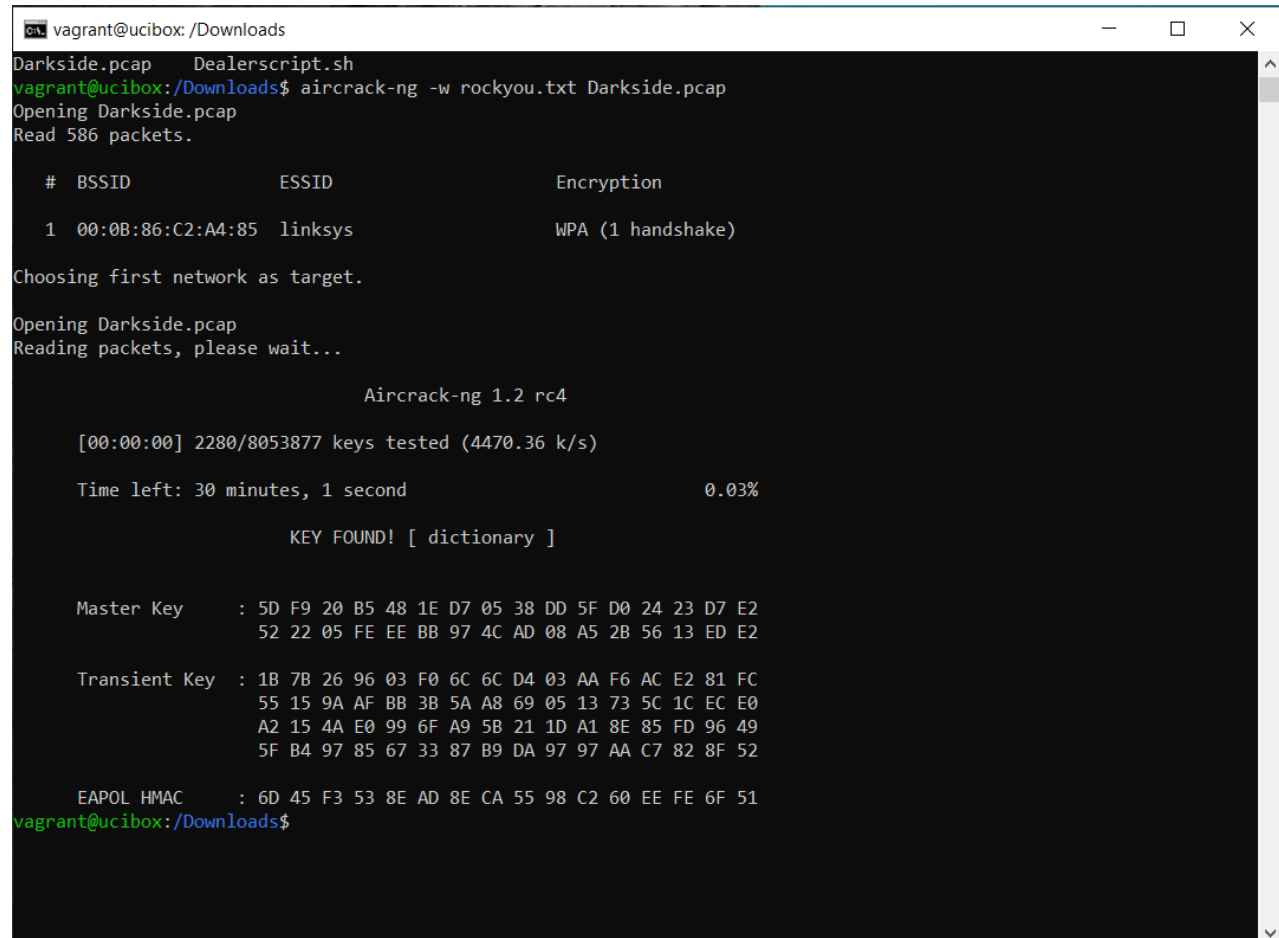
Batuu - C - E - I - L - Q - T - - - Jedha is the shortest path while not passing through planet N. Total trip is about 28ms.

Mission 6

Used aircrack-ng to crack password of captured Darkside.pcap file.

I placed necessary files in /Downloads/ in order to simplify the process

aircrack-ng -w rockyou.txt Darkside.pcap



```
vagrant@ucibox: /Downloads
Darkside.pcap Dealerscript.sh
vagrant@ucibox:/Downloads$ aircrack-ng -w rockyou.txt Darkside.pcap
Opening Darkside.pcap
Read 586 packets.

# BSSID          ESSID          Encryption
1 00:0B:86:C2:A4:85 linksys        WPA (1 handshake)

Choosing first network as target.

Opening Darkside.pcap
Reading packets, please wait...

Aircrack-ng 1.2 rc4

[00:00:00] 2280/8053877 keys tested (4470.36 k/s)

Time left: 30 minutes, 1 second          0.03%

KEY FOUND! [ dictionary ]

Master Key      : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
                  52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

Transient Key   : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC
                  55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0
                  A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49
                  5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52

EAPOL HMAC     : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51
vagrant@ucibox:/Downloads$
```

Key is 'dictionary'

I then inserted the key into Wireshark and decrypted the traffic and filtered by arp to see what MAC addresses have what IP addresses.

The screenshot shows the Wireshark interface with the file 'Darkside.pcap' open. The packet list is filtered for 'arp' and shows three packets. Packet 315 is selected, and its details are expanded, showing the 'Address Resolution Protocol (reply)' section. The packet bytes pane shows the raw data of the ARP reply, which includes the sender's MAC address (00:0f:66:e3:e4:01) and the target's IP address (172.16.0.1).

No.	Time	Source	Destination	Protocol	Length	Info
312	2006-05-03 19:32:09.421364	IntelCor_55:98:ef	Broadcast	ARP	80	Who has 172.16.0.1? Tell 172.16.0.101
314	2006-05-03 19:32:09.422968	IntelCor_55:98:ef	Broadcast	ARP	98	Who has 172.16.0.1? Tell 172.16.0.101
315	2006-05-03 19:32:09.423426	Cisco-Li_e3:e4:01	IntelCor_55:98:ef	ARP	98	172.16.0.1 is at 00:0f:66:e3:e4:01

Frame 315: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> IEEE 802.11 Data, Flags: .p....F.
> Logical-Link Control
> Address Resolution Protocol (reply)

```
0000  08 42 d4 00 00 13 ce 55 98 ef 00 0b 86 c2 a4 85  -B----U -  
0010  00 0f 66 e3 e4 01 70 0e 00 20 11 20 00 00 00 00  --f...p-  
0020  45 0b 5c 38 cc 56 d8 a0 3c 00 0e 45 fc 40 60 c7  E.\8-V- <...E.@`  
0030  42 1f dd 76 10 b5 82 8a 14 6a 86 33 0a ec a3 a0  B-v-...:j-3...  
0040  7c 92 ea 18 9a c2 13 bd 4d 04 93 d2 d1 ef 18 68  |.....M.....h  
0050  0e cc 36 3e 0f 7c a6 4b 0d fe 90 33 0c 84 1b 0a  --6>-|.K...3...  
0060  19 5e                                     .^
```

Frame (98 bytes) | Decrypted TKIP data (54 bytes)
Address Resolution Protocol: Protocol | Packets: 586 · Displayed: 3 (0.5%) | Profile: Default

Using this we can tell that 172.16.0.1 is at 00:0f:66:e3:e4:01

Mission 7

nslookup -type=txt princessleia.site

```
vagrant@ucibox: /Downloads
vagrant@ucibox:/Downloads$ nslookup -type=txt princessleia.site
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
princessleia.site      text = "Run the following in a command line: telnet towel.blinkenlights.nl or as
a backup access in a browser: www.asciimation.co.nz"

Authoritative answers can be found from:

vagrant@ucibox:/Downloads$
```

Tried running telnet towel.blinkenlights.nl but didn't work. Went to www.asciimation.co.nz

