Edwin Sierra

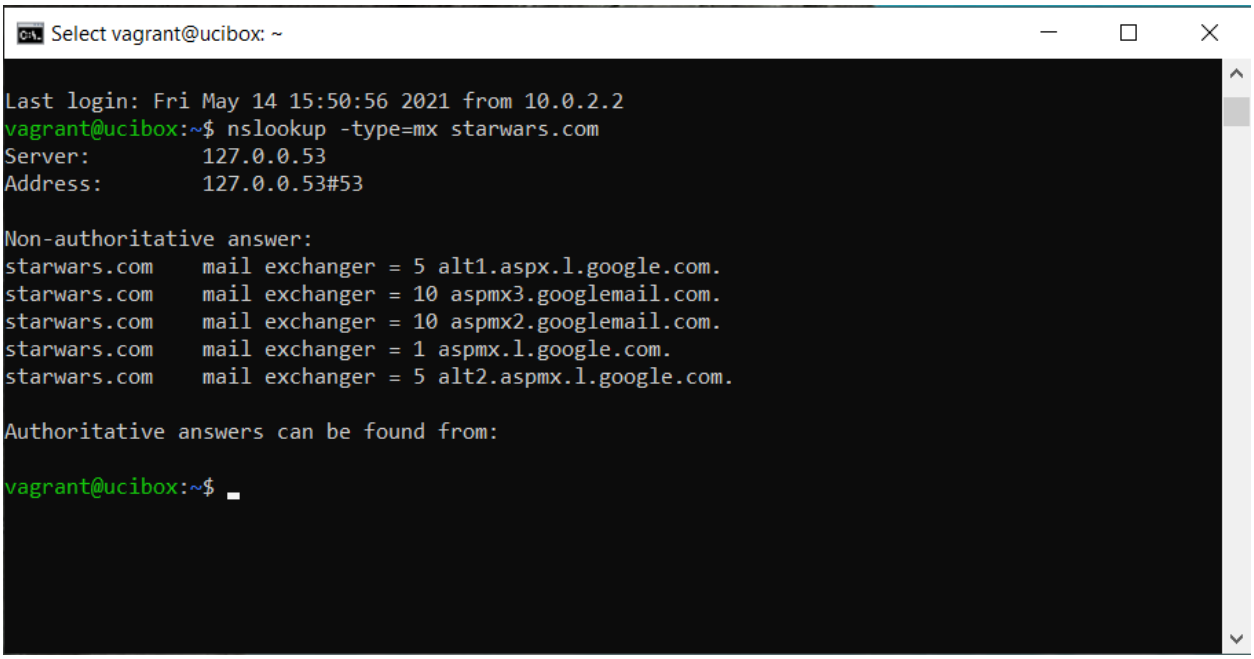
Homework #9

UCI Cybersecurity Bootcamp

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



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 alt1.aspx.1.google.com

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

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

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

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

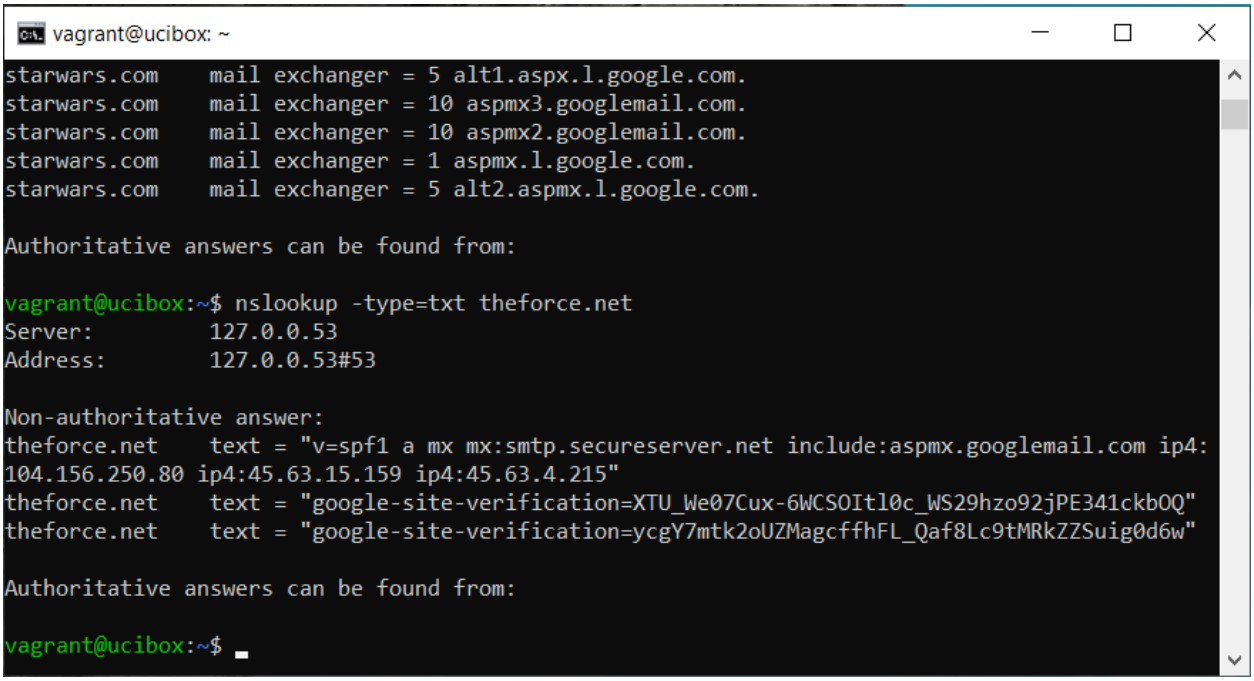
starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.

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



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-6WCSOItl0c_WS29hzo92jPE341ckbOQ"

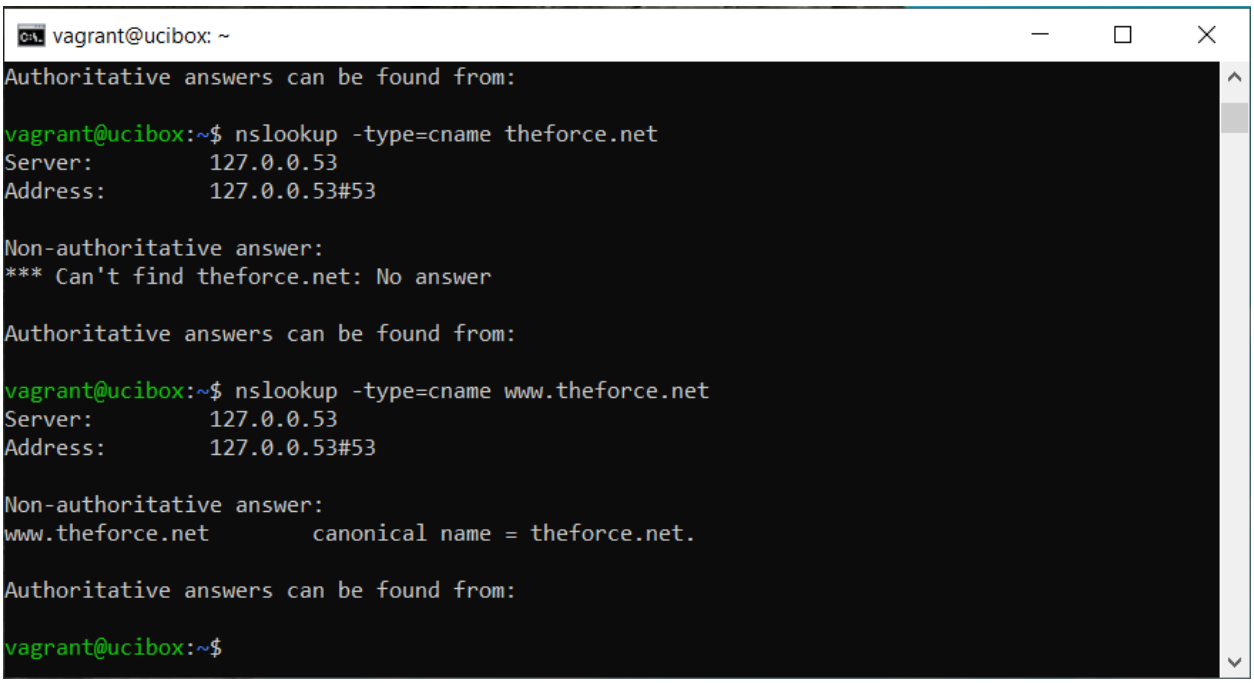
theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"

Authoritative answers can be found from:

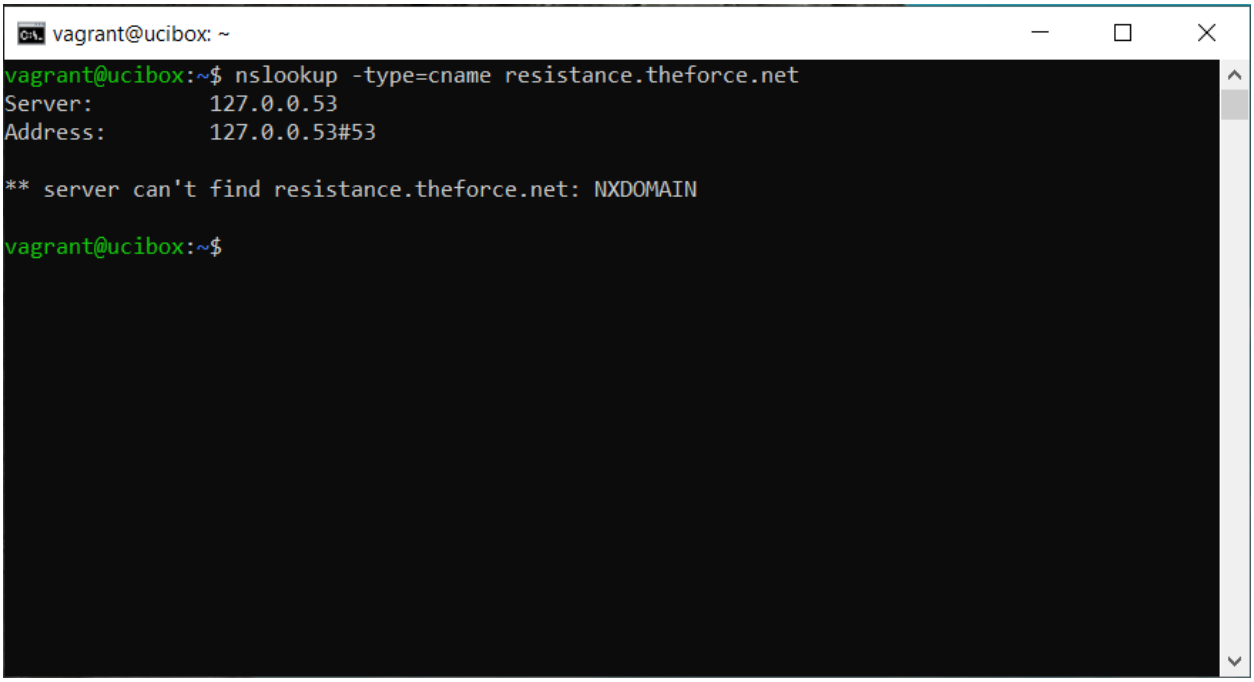
Mission 3

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

nslookup type=cname ww.theforce.net



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



Corrected record should be as follows:

Server: **127.0.0.53**

Address: **127.0.0.53#53**

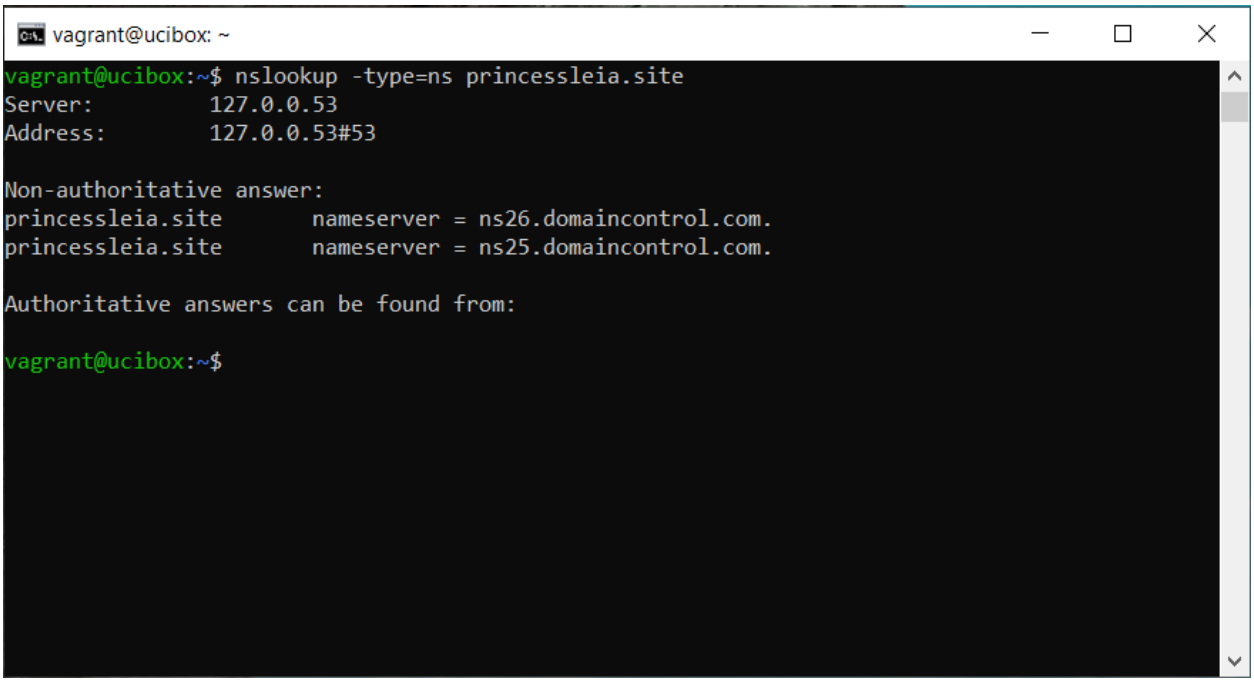
Non-authoritative answer:

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.



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:

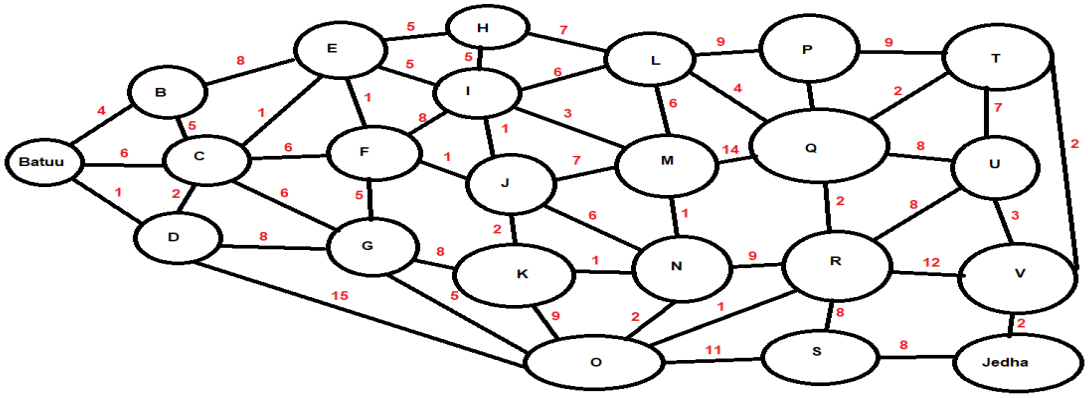
princessleia.site nameserver = ns26.domaincontrol.com.

princessleia.site nameserver = ns25.domaincontrol.com.

princessleia.site nameserver = ns2.galaxybackup.com.

Authoritative answers can be found from:

Mission 5



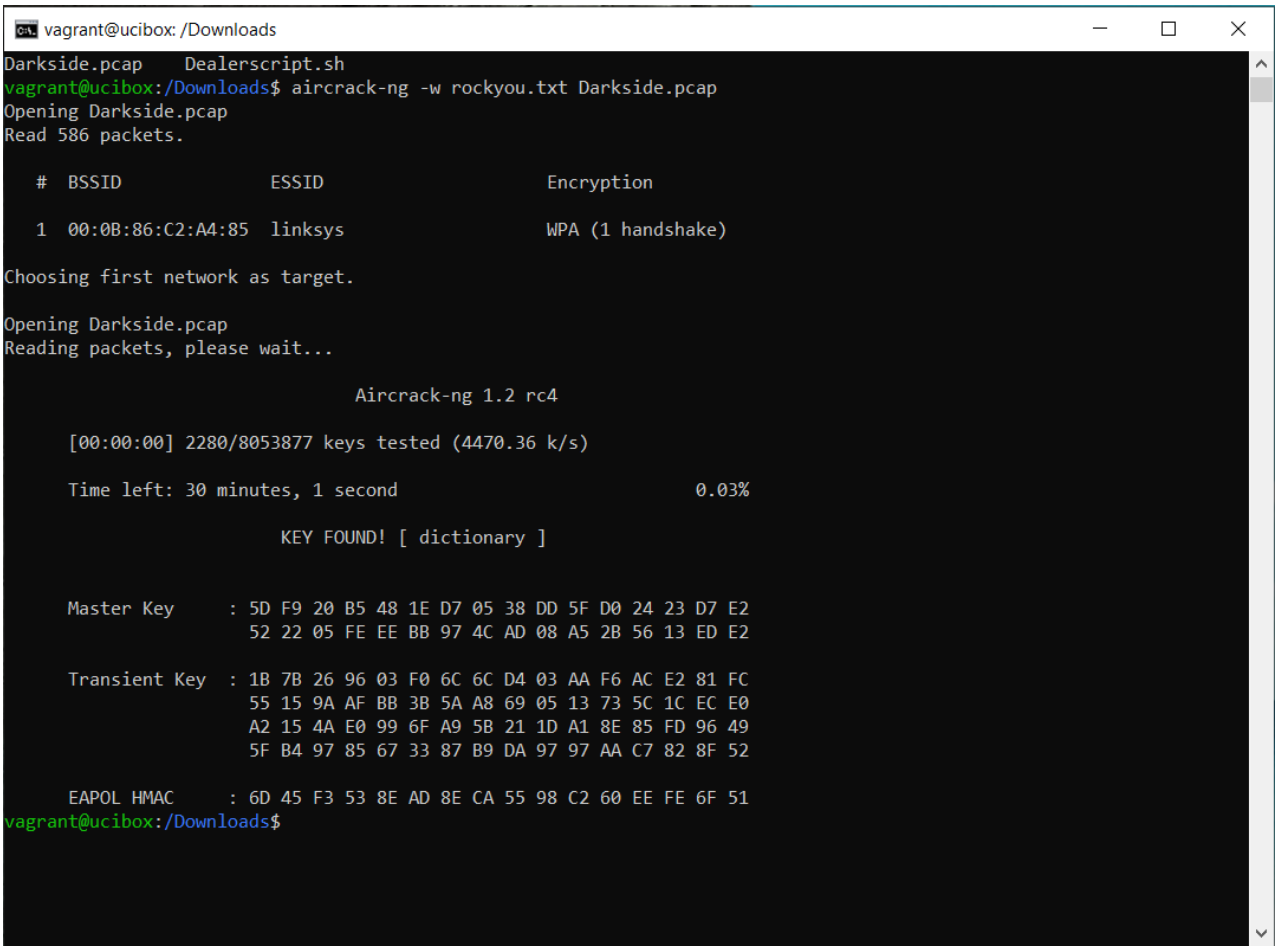
Batuu – D – C – E – F – J – I – L – Q – T – V - Jedha is the shortest path while not passing through planet N. Total trip is about 23ms.

Mission 6

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

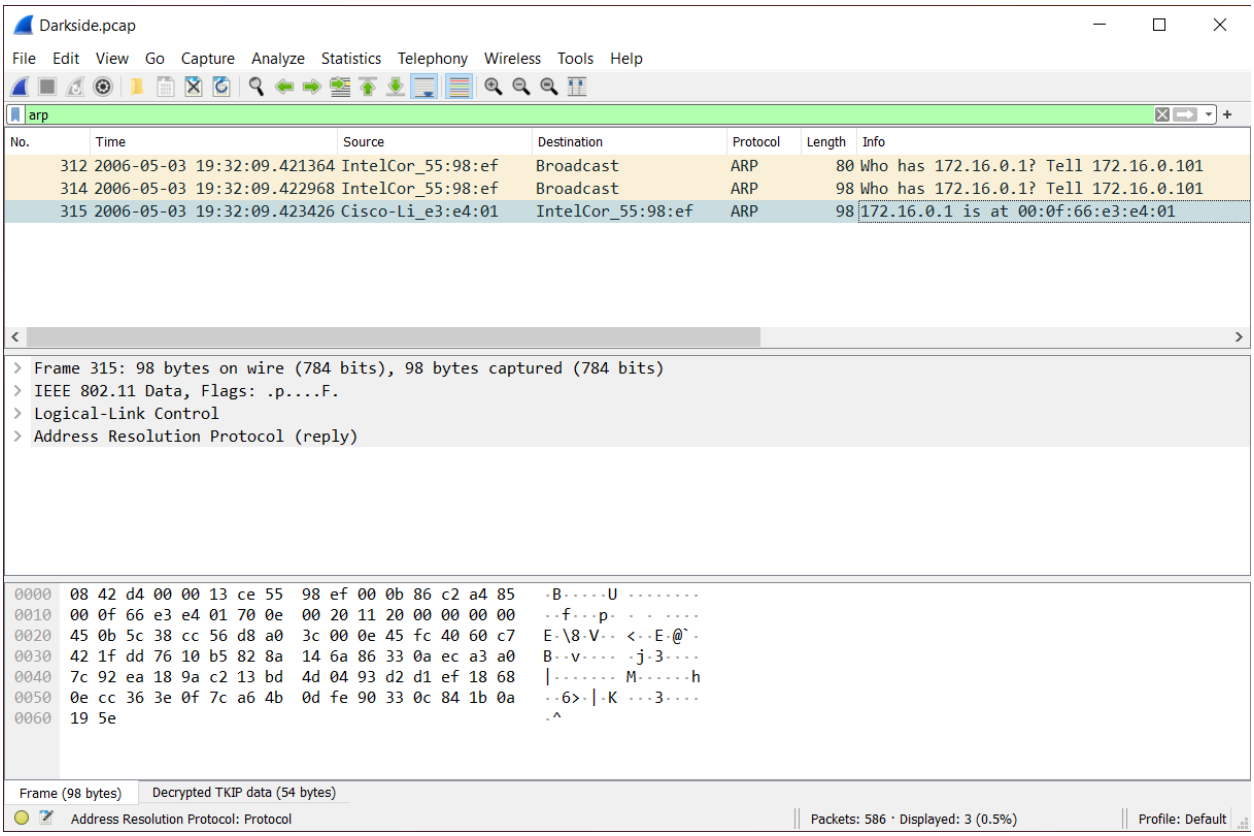
I placed necessary files in /Downloads/ in order to simplify the process

aircrack-ng -w rockyou.txt Darkside.pcap



Key is ‘dictionary’

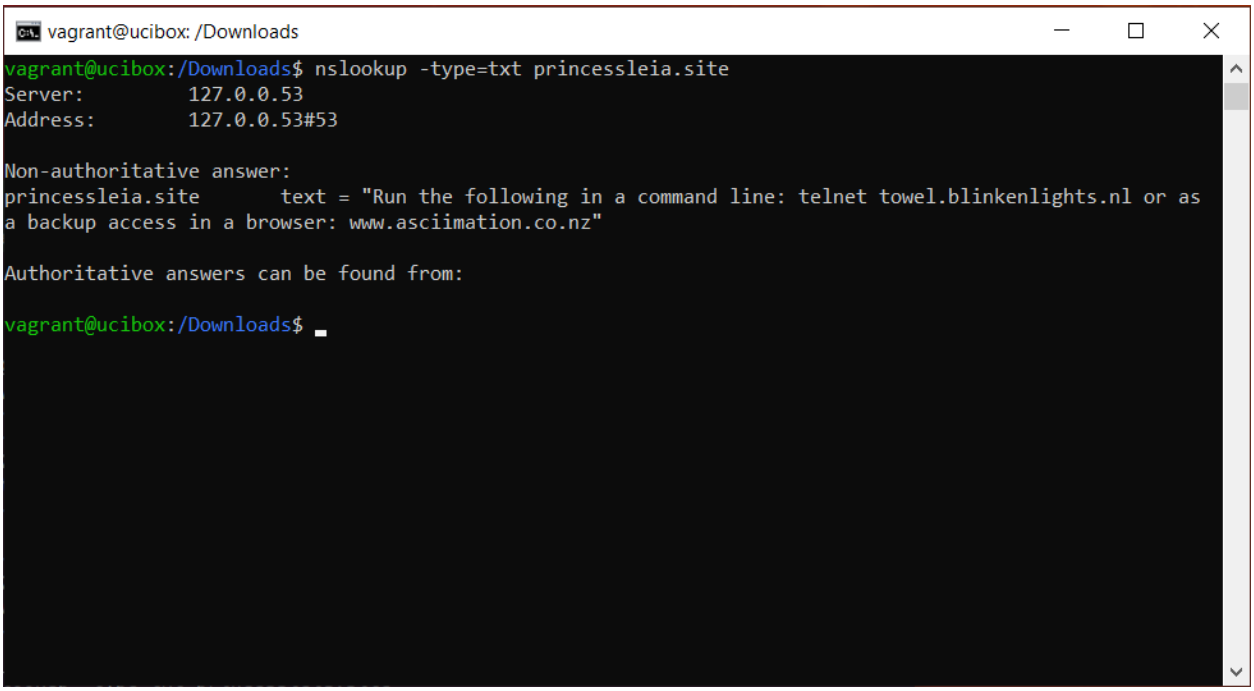
I then inserted the key into wireshark and decrypted the traffic and filtered by arp to see what mac addresses have what IP addresses.



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



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