Networks Fundamentals II Homework: In a Network Far, Far Away!

Mission 1

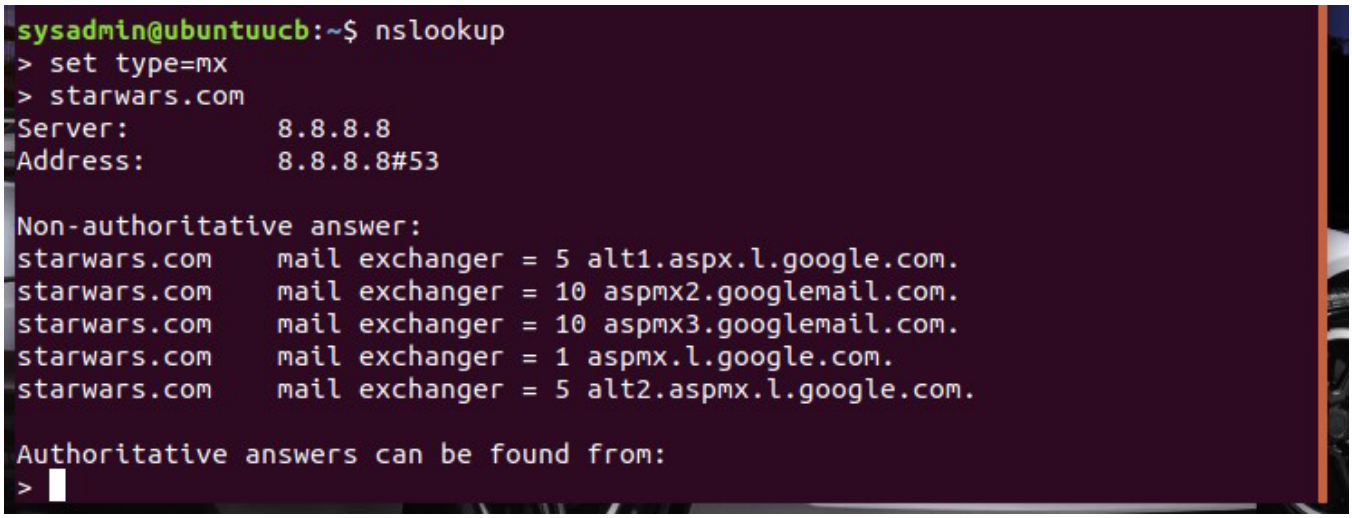
Issue: Due to the DoS attack, the Empire took down the Resistance's DNS and primary email servers.

The Resistance's network team was able to build and deploy a new DNS server and mail server.

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

The Resistance (***starwars.com***) is able to send emails but unable to receive any.

Your Mission:
-Determine and document the mail servers for starwars.com using ***NSLOOKUP.***
-Explain why the Resistance isn't receiving any emails.
-Document what a corrected DNS record should be.



The above are the current mail servers for starwars.com using NSLOOKUP.

Since neither of the the new primary server ***asltx.l.google.com*** and secondary server ***asltx.2.google.com*** are listed as any of the mail exchangers, none of the emails would be directed at all, thus the Resistance wouldn't receive any emails.

The corrected DNS record for the mail exchanger should be as follows:

```
starwars.com      mail exchanger = 1 asltx.l.google.com.
starwars.com      mail exchanger = 5 asltx.2.google.com.
starwars.com      mail exchanger = 10 aspmx.l.google.com.
starwars.com      mail exchanger = 15 alt1.aspx.l.google.com.
starwars.com      mail exchanger = 15 alt2.aspx.l.google.com.
starwars.com      mail exchanger = 20 aspmx2.googlemail.com.
starwars.com      mail exchanger = 20 aspmx3.googlemail.com.
```

Mission 2

Issue: Now that you've addressed the mail servers, all emails are coming through. However, users are still reporting that they haven't received mail from the ***theforce.net*** alert bulletins.

Many of the alert bulletins are being blocked or going into spam folders.

This is probably due to the fact that ***theforce.net*** changed the IP address of their mail server to ***45.23.176.21*** while your network was down.

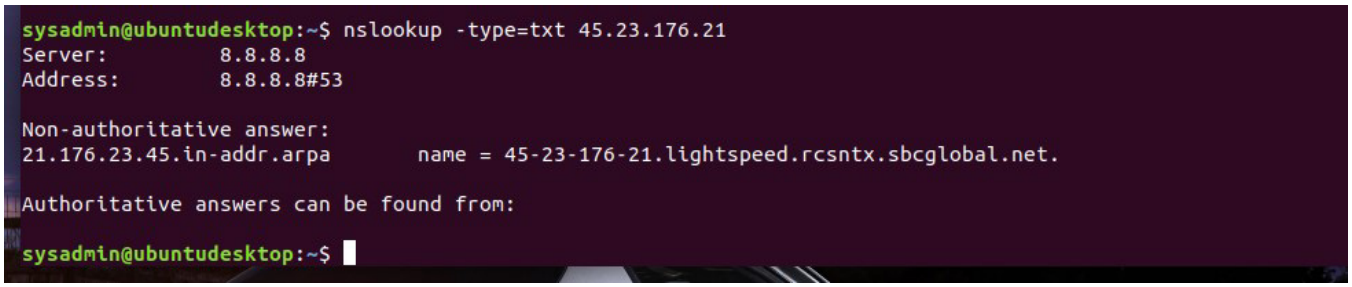
These alerts are critical to identify pending attacks from the Empire.

Your Mission:
-Determine and document the SPF for theforce.net using NSLOOKUP.
-Explain why the Force's emails are going to spam.
-Document what a corrected DNS record should be.

The Sender Policy Framework txt records show that the email server is set to the] following:

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"

Since the IP of their mail server is supposed to be 45.23.176.21, it is likely not updated yet with the new IP address for their DNS records so emails go to spam.



The updated/ corrected DNS record should be as follows:

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 include:45-23-176-21.lightspeed.rcsntx.sbcglobal.net"

Mission 3

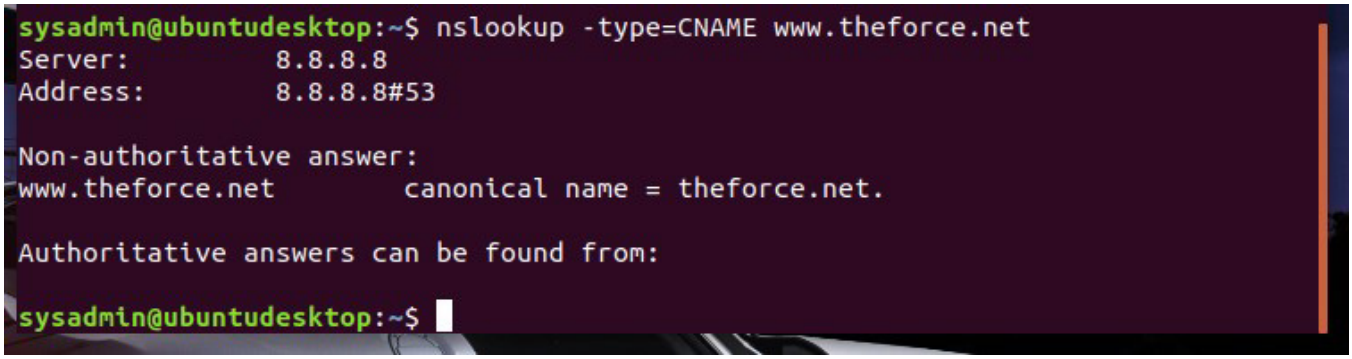
Issue: You have successfully resolved all email issues and the resistance can now receive alert bulletins. However, the Resistance is unable to easily read the details of alert bulletins online.

They are supposed to be automatically redirected from their sub page of ***resistance.theforce.net*** to ***theforce.net*** .

Your mission:
Document how a CNAME should look by viewing the CNAME of ***www.theforce.net*** using NSLOOKUP.

Explain why the sub page of ***resistance.theforce.net*** isn't redirecting to ***theforce.net*** .

Document what a corrected DNS record should be.



The above the current CNAME record for www.theforce.net

Since there is no CNAME record for the subdomain resistance.theforce.net, then the ones trying to access it is unable to see the page from theforce.net

The proper CNAME record should be added for the subdomain to the root domain:

```
NAME TYPE VALUE
---------------
resistance.theforce.net. CNAME theforce.net.
www.theforce.net.        CNAME theforce.net.
```

or

```
resistance.theforce.net    canonical name = theforce.net
www.theforce.net           canonical name = theforce.net
```

Mission 4

Issue: During the attack, it was determined that the Empire also took down the primary DNS server of ***princessleia.site***.

Fortunately, the DNS server for princessleia.site is backed up and functioning.

However, the Resistance was unable to access this important site during the attacks and now they need you to prevent this from happening again.

The Resistance's networking team provided you with a backup DNS server of: ***ns2.galaxybackup.com***.

Your Mission:
-Confirm the DNS records for ***princessleia.site***.
-Document how you would fix the DNS record to prevent this issue from happening again.

```
sysadmin@ubuntudesktop:~$ nslookup -type=ns princessleia.site
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
princessleia.site       nameserver = ns26.domaincontrol.com.
princessleia.site       nameserver = ns25.domaincontrol.com.

Authoritative answers can be found from:

sysadmin@ubuntudesktop:~$
```

The above are the current name servers for princessleia.site.

In order to fix it so that the backup name server can be used in case the primary and secondary are down again, you would add the third one to the list of name servers since a site can usually use up to a maximum of 3 name servers as follows:

```
princessleia.site       nameserver = ns26.domaincontrol.com.
princessleia.site       nameserver = ns25.domaincontrol.com.
princessleia.site       nameserver = ns2.galaxybackup.com.
```

Mission 5

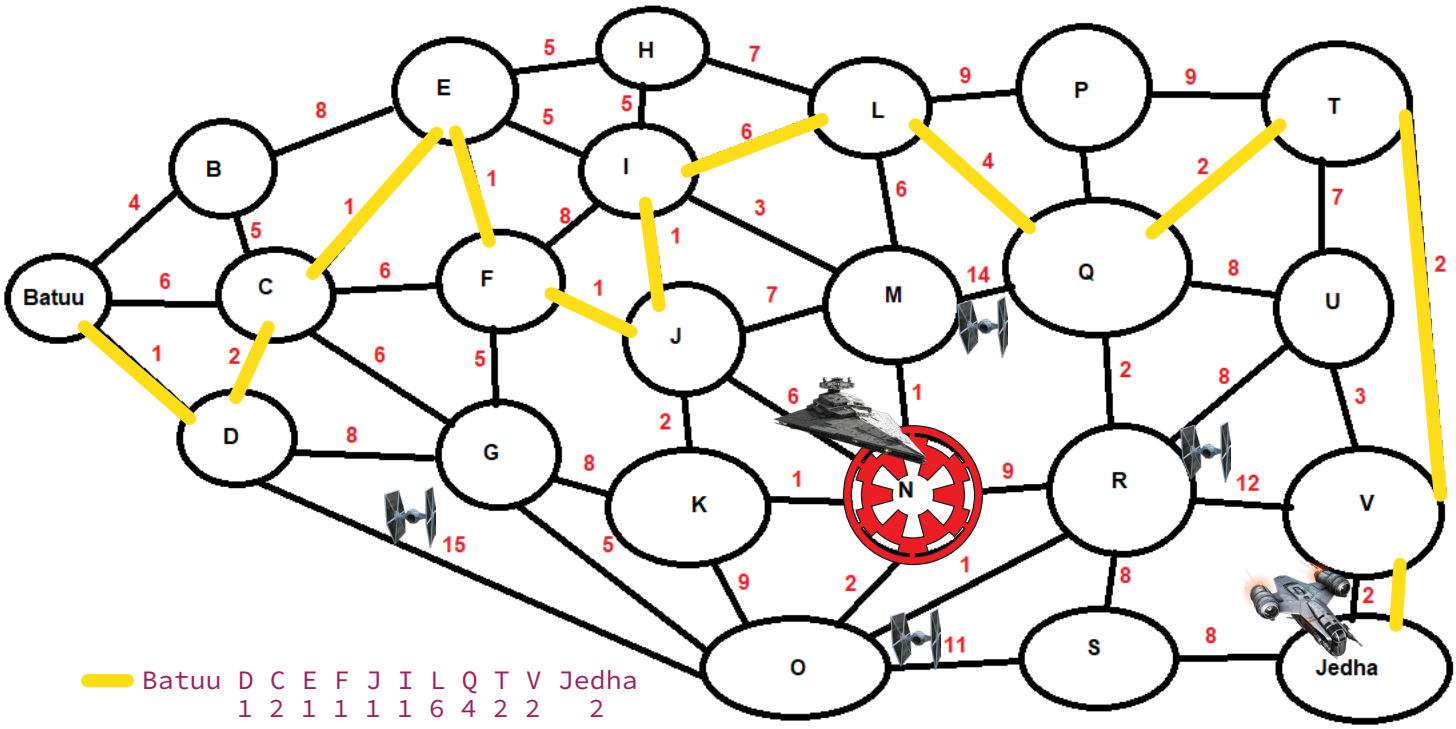
Issue: The network traffic from the planet of ***Batuu*** to the planet of ***Jedha*** is very slow.

You have been provided a network map with a list of planets connected between ***Batuu*** and ***Jedha***.

It has been determined that the slowness is due to the Empire attacking ***Planet N***.

Your Mission:
-View the ***Galaxy Network Map*** and determine the ***OSPF*** shortest path from ***Batuu*** to ***Jedha***.
-Confirm your path doesn't include ***Planet N*** in its route.
-Document this shortest path so it can be used by the Resistance to develop a static route to improve the traffic.

The Open Shortest Path First (OSPF) from Batuu to Jedha is the Yellow path indicated below. There is a total of 11 hops to go from both locations with a total response time of 23, avoiding the Galactic Empire and staying as far as possible along the way.



Mission 6

Issue: Due to all these attacks, the Resistance is determined to seek revenge for the damage the Empire has caused.

You are tasked with gathering secret information from the Dark Side network servers that can be used to launch network attacks against the Empire.

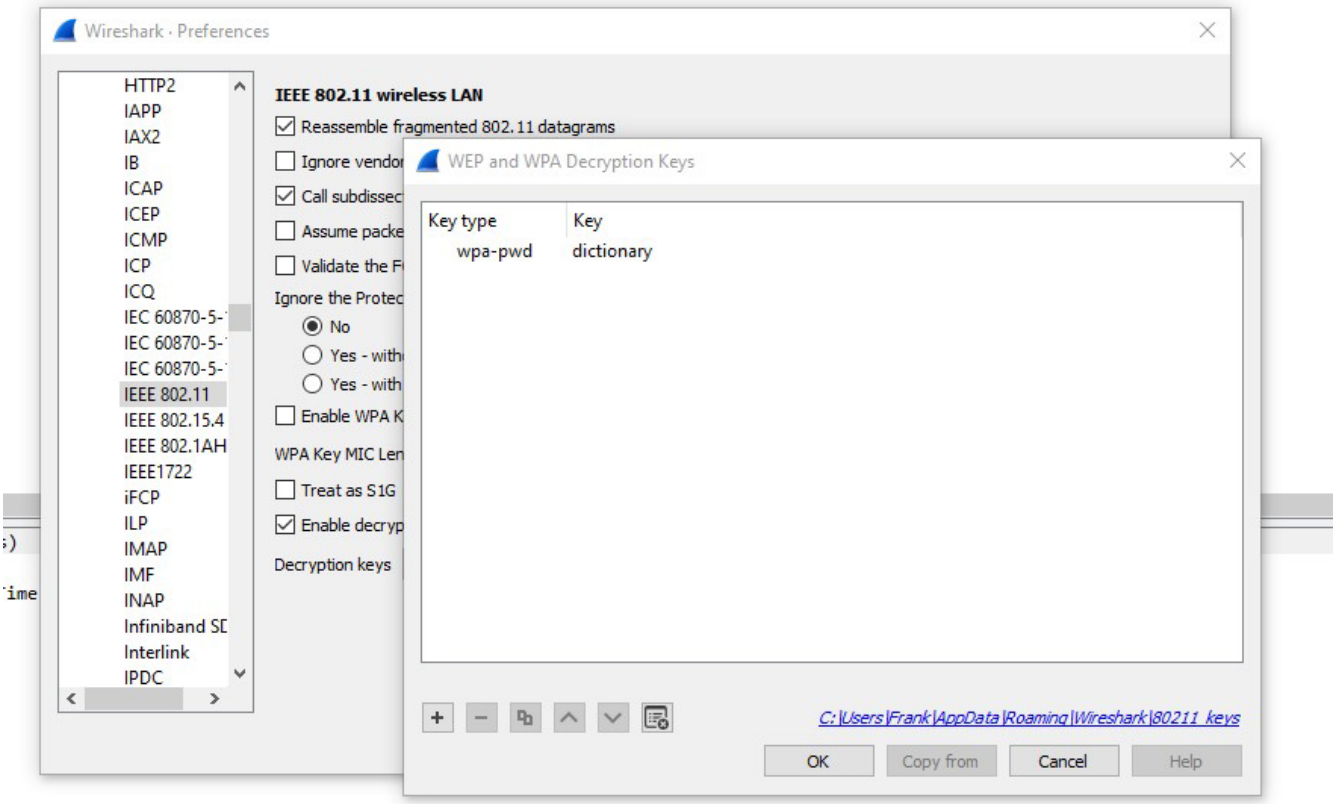
You have captured some of the Dark Side's encrypted wireless internet traffic in the following ***pcap: Darkside.pcap***.

Your Mission:
Figure out the Dark Side's secret wireless key by using ***Aircrack-ng***.
-Hint: This is a more challenging encrypted wireless traffic using WPA.
-In order to decrypt, you will need to use a ***wordlist (-w)*** such as ***rockyou.txt.***

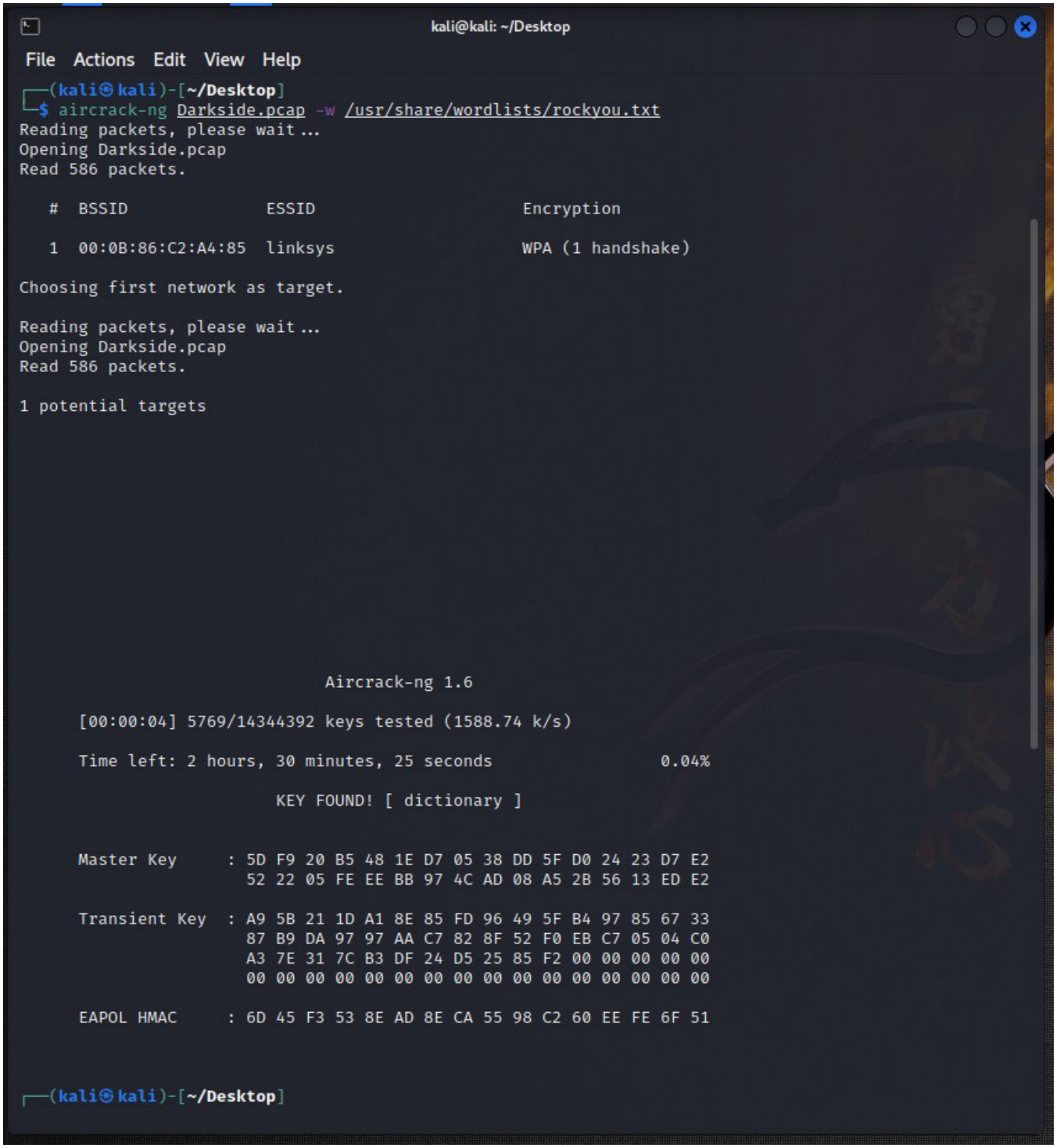
Use the Dark Side's key to decrypt the wireless traffic in Wireshark.
-Hint: The format for they key to decrypt wireless is <***Wireless_key***>:<***SSID***>.
Correction: <Wireless_key only>

Once you have decrypted the traffic, figure out the following Dark Side information:
-Host IP Addresses and MAC Addresses by looking at the decrypted ***ARP*** traffic.
-Document these IP and MAC Addresses, as the resistance will use these IP addresses to launch a retaliatory attack.

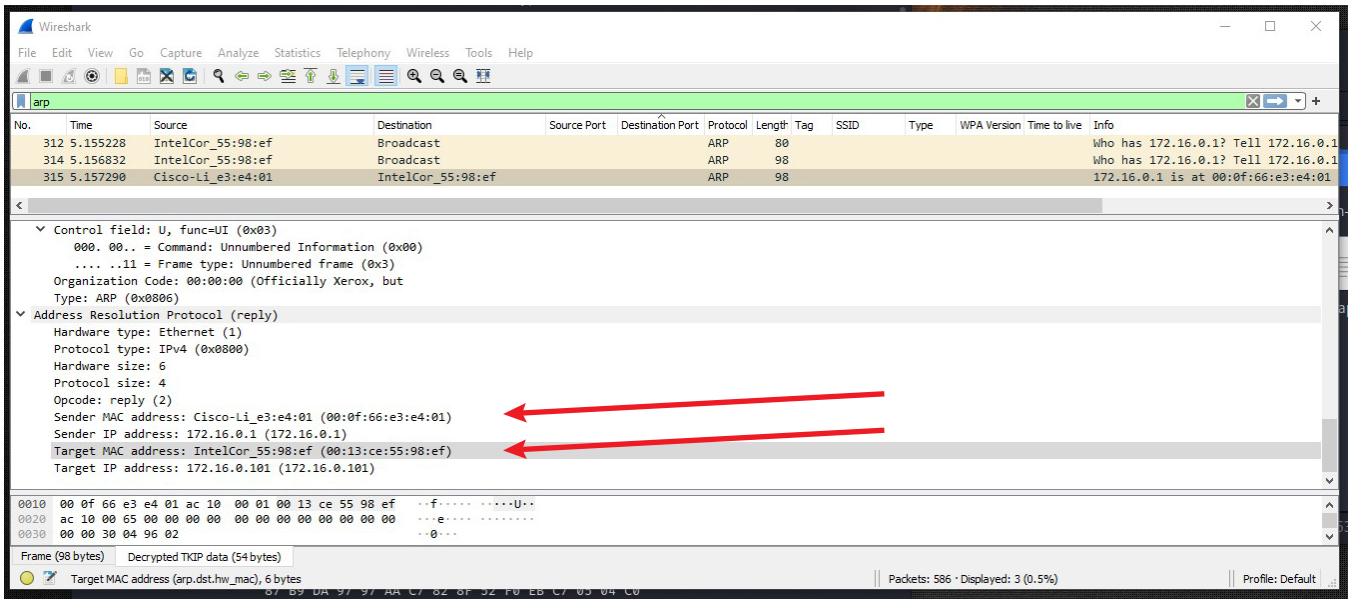
Used the aircrack-ng program inside my Kali Linux since the wordlist was already available inside the OS. Copied over the Darkside.pcap file to Desktop and used the wordlist option to find out Dark Side's secret wireless key.



Results of the aircrack-ng program.
SSID: linksys
Key found: dictionary



Filtered the decrypted traffic file for ARP packets only:



The IP and MAC addresses are as follows:

Sender’s MAC address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
Sender’s IP address: 172.16.0.101

Target’s MAC address: Cisco-Li_e3:e4:01 (00:0f:66:e3:e4:01)
Target’s IP address: 172.16.0.1

Mission 7

As a thank you for saving the galaxy, the Resistance wants to send you a secret message!

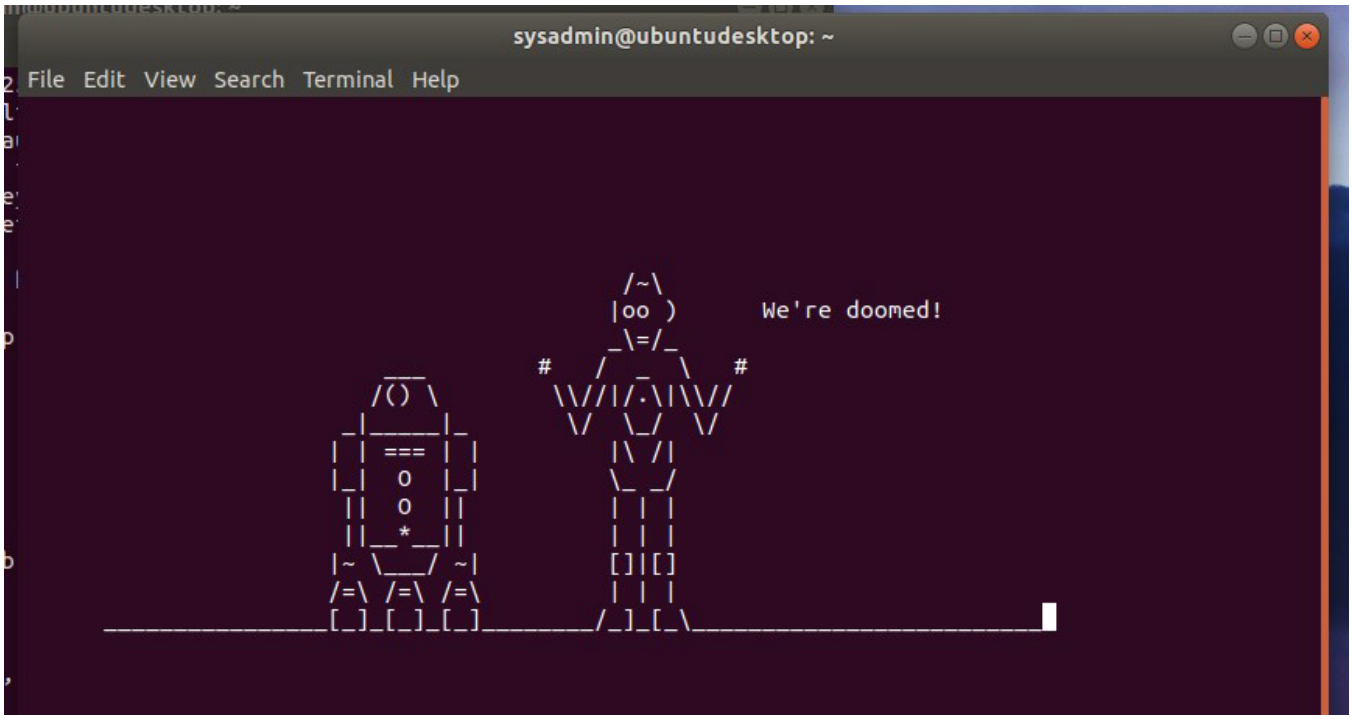
Your Mission:
View the DNS record from Mission #4.

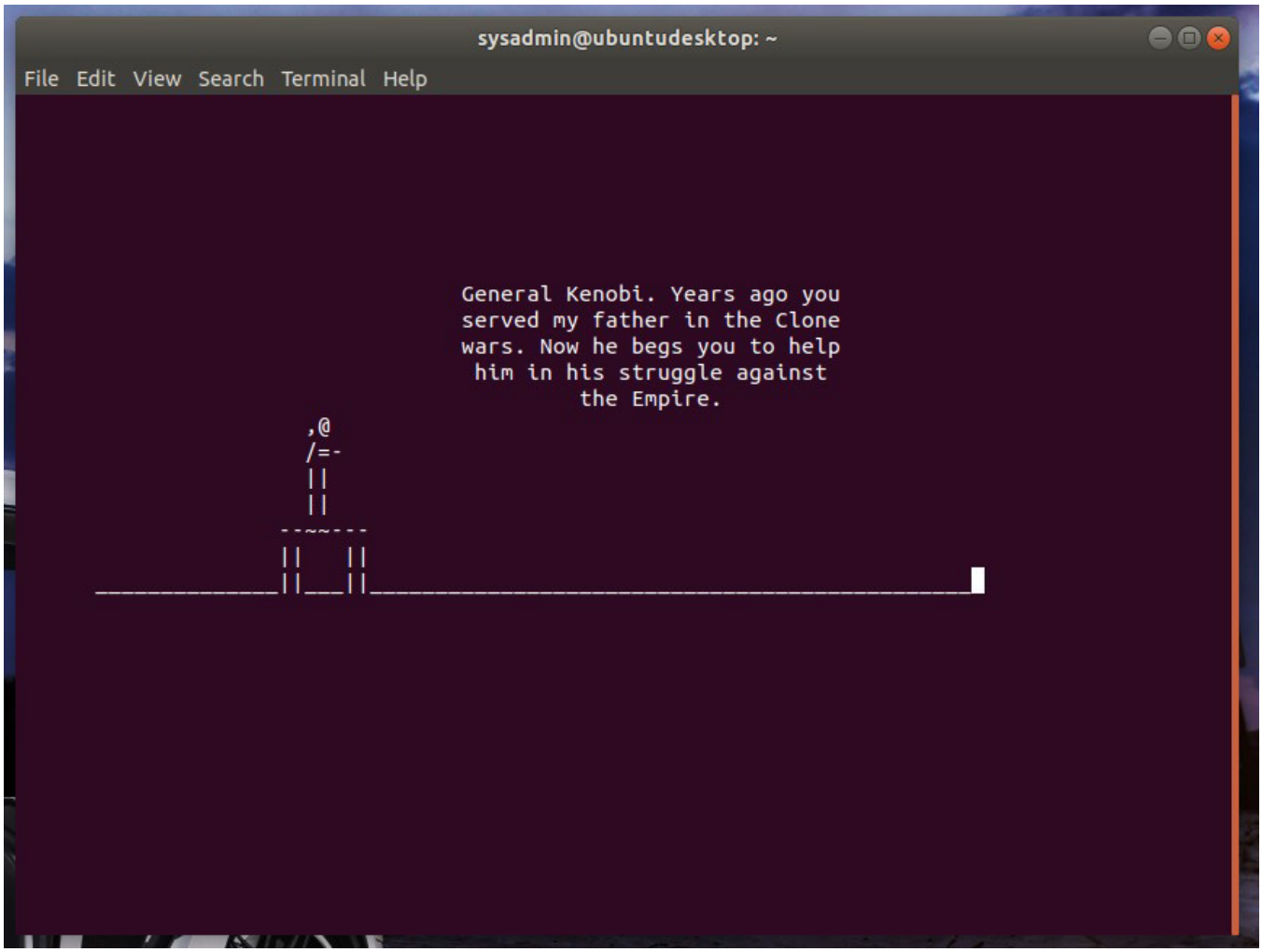
The Resistance provided you with a hidden message in the TXT record, with several steps to follow.

Follow the steps from the ***TXT*** record.
-Note: A backup option is provided in the ***TXT*** record (as a website) in case the main telnet site is unavailable

Take a screen shot of the results.


```
telnet towel.blinkenlights.nl
```




sysadmin@ubuntudesktop: ~
File Edit View Search Terminal Help
General Kenobi. Years ago you
served my father in the Clone
wars. Now he begs you to help
him in his struggle against
the Empire.
,@
/=-
||
||
--~~---
|| ||
_____||__||_____