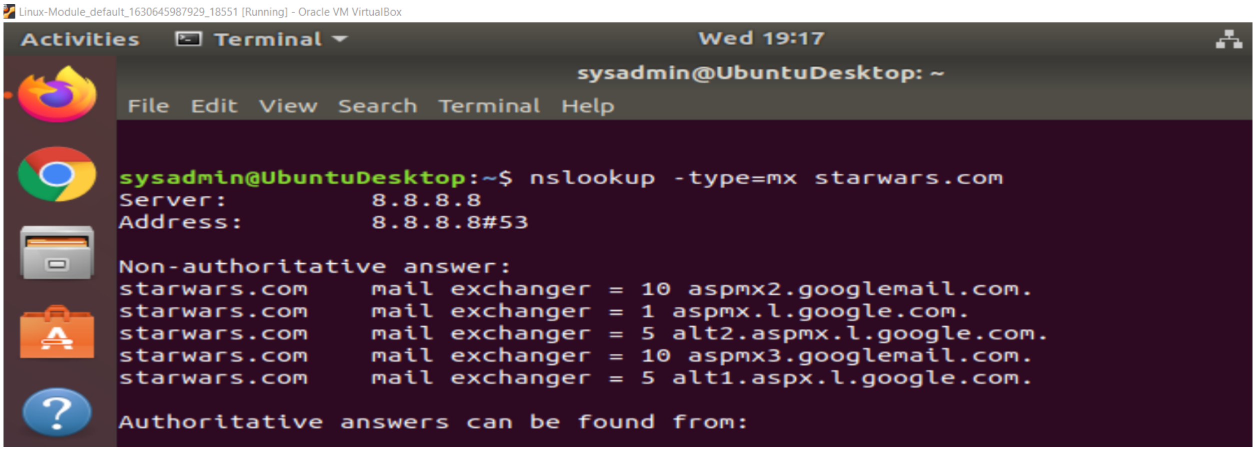
Networking Fundamentals II

Mission 1:

nslookup type: (MX: Specifies the mail exchanger)

1.a: Determine and document the mail servers for starwars.com using NSLOOKUP:

For this task I used **nslookup -type=mx starwars.com** in order to look at the **satarwars.com** mail serves list.



Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Wed 19:17
sysadmin@UbuntuDesktop: ~
File
Edit
View
Search
Terminal
Help

```
sysadmin@UbuntuDesktop:~$ nslookup -type=mx starwars.com
Server:         8.8.8.8
Address:        8.8.8.8#53

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

Authoritative answers can be found from:
```

1b: Explain why the Resistance isn't receiving any emails:

The resistance is able to send out emails, but unable to receive any is because the mail servers **asltx.l.google.com** and **asltx.2.google.com** are not listed in the **starwars.com** mail servers authorized DNS record list.

1c: Document what a corrected DNS record should be:

A corrected DNS record should include in its list:

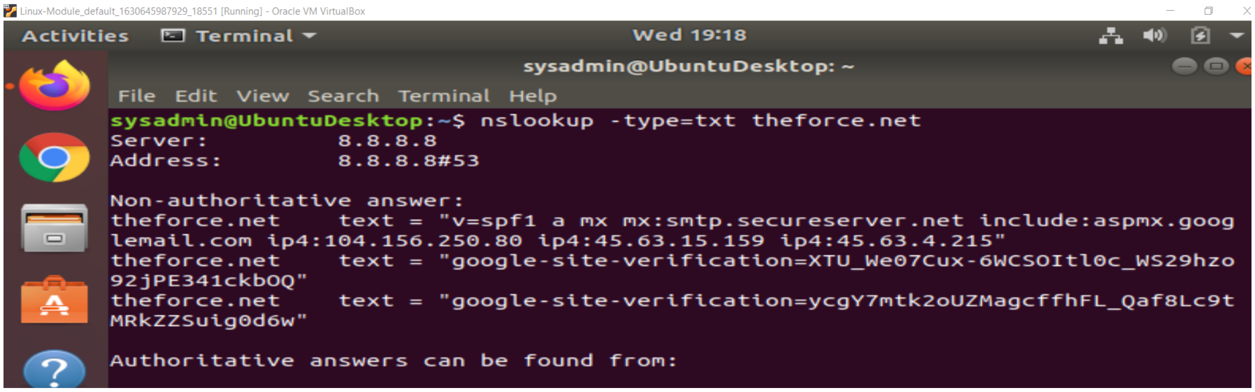
starwars.com MX preference= 1 mail exchanger = asltx.l.google.com
starwars.com MX preference= 5 mail exchanger = asltx.2.google.com

Mission 2:

nslookup type: (TXT: Specifies the user identifier)

2a: Determine and document the SPF for theforce.net using NSLOOKUP:

For this task, I used **nslookup -type=txt theforce.net** in order to look at available mail servers IP addresses for **theforce.net.**



Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Wed 19:18
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
sysadmin@UbuntuDesktop:~$ nslookup -type=txt theforce.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
theforce.net    text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.goog
lemail.com ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"
theforce.net    text = "google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo
92jPE341ckbOQ"
theforce.net    text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9t
MRkZZSuig0d6w"

Authoritative answers can be found from:
```

2b: Explain why the Force's emails are going to spam:

The reason **theforce.net** alert bulletins emails are going to spam, is because **theforce.net** mail server IP address of **45.23.176.21**, was removed from the list.

2c: Document what a corrected DNS record should be:

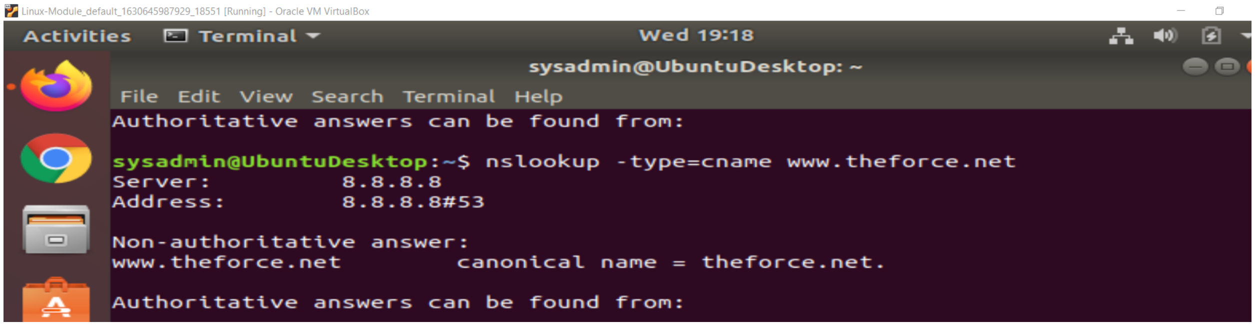
A corrected DNS record should include the IP address **45.23.176.21** in its list. doing so, the alert bulletins should be received by the intended recipients, and shouldn't end up in the spam.

Mission 3:

nslookup type: (CNAME:Specifies a canonical name for an alias)

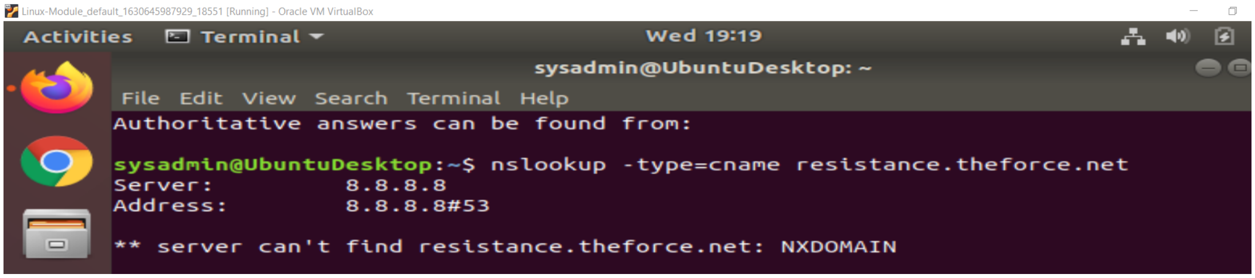
3a: Document how a CNAME should look by viewing the CNAME of www.theforce.net using NSLOOKUP:

For this task, I performed a two step process.
First, I used **nslookup -type=CNAME www.theforce.net,** in order to find the **www.theforce.net** canonical name.
canonical name= theforce.net.


Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Wed 19:18
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$ nslookup -type=cname www.theforce.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.theforce.net        canonical name = theforce.net.

Authoritative answers can be found from:
```

Second, I used **nslookup -type=CNAME resistance.theforce.net,** in order to find the **resistance.theforce.net** canonical name.


Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Wed 19:19
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$ nslookup -type=cname resistance.theforce.net
Server:         8.8.8.8
Address:        8.8.8.8#53

** server can't find resistance.theforce.net: NXDOMAIN
```

3b: Explain why the sub page of resistance.theforce.net isn't redirecting to theforce.net:

The reason the resistance is not able to redirect the alert bulletins emails from the sub page of **resistance.theforce.net** to **theforce.net,** is because the **theforce.net (Alias)** does not hold any canonical name of **resistance.theforce.net** in the DNS records.

3c: Document what a corrected DNS record should be:

A corrected DNS record should reflect the following:

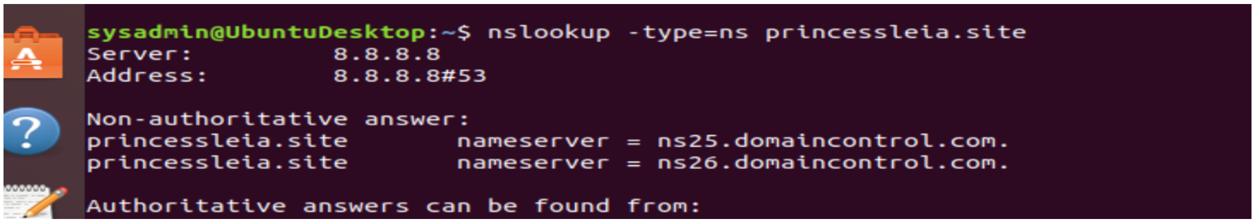
theforce.net   canonical name = resistance.theforce.net

Mission 4:

nslookup type: (NS: Specifies name server for the named zone)

4a: Confirm the DNS records for princessleia.site:

for this task. **I used nslookup -type=ns princessleia.site,** in order to find princessleia.site access servers list.



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

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

Authoritative answers can be found from:
```

4b: Document how you would fix the DNS record to prevent this issue from happening again:

In order to provide the resistance access to the site **princessleia.site** via the backup server, we need to add the backup server **ns2.galaxybackup.com** to the DNS servers list available/accessible to **princessleia.site**.

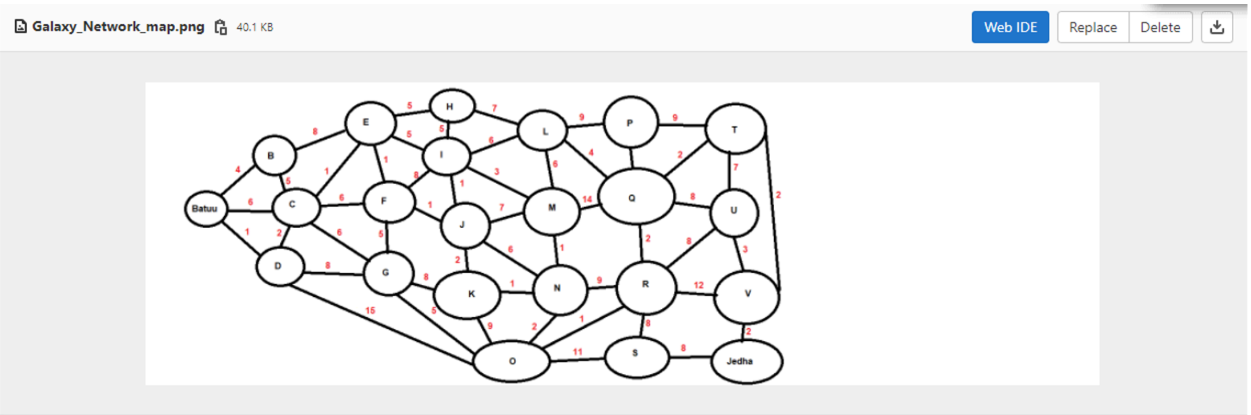
The added server will look as follow:

princessleia.site   nameserver = ns2.galaxybackup.com

Mission 5:

5a: View the Galaxy Network Map and determine the OSPF shortest path from Batuu to Jedha:

Answer: Batuu>D>C>E>F>J>I>L>Q>T>V>Jedha = 23



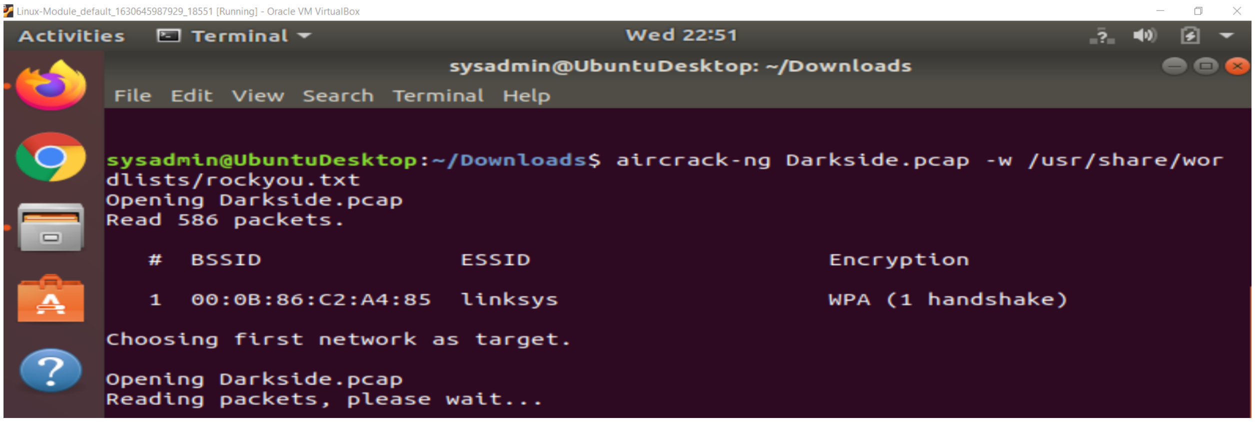
Mission 6:

6a: Figure out the Dark Side's secret wireless key by using Aircrack-ng:

In the VM, I found the file named **rockyou.txt,** which contains the secret wireless key that can decrypt the darkside's wireless internet traffic.The path that the file rockyou.txt was found in: **/usr/share/wordlists/rockyou.txt**.
I used **aircrack-ng** to find the decryption key with the following command: -------->

```
aircrack-ng Darkside.pcap -w /usr/share/wordlists/rockyou.txt
```

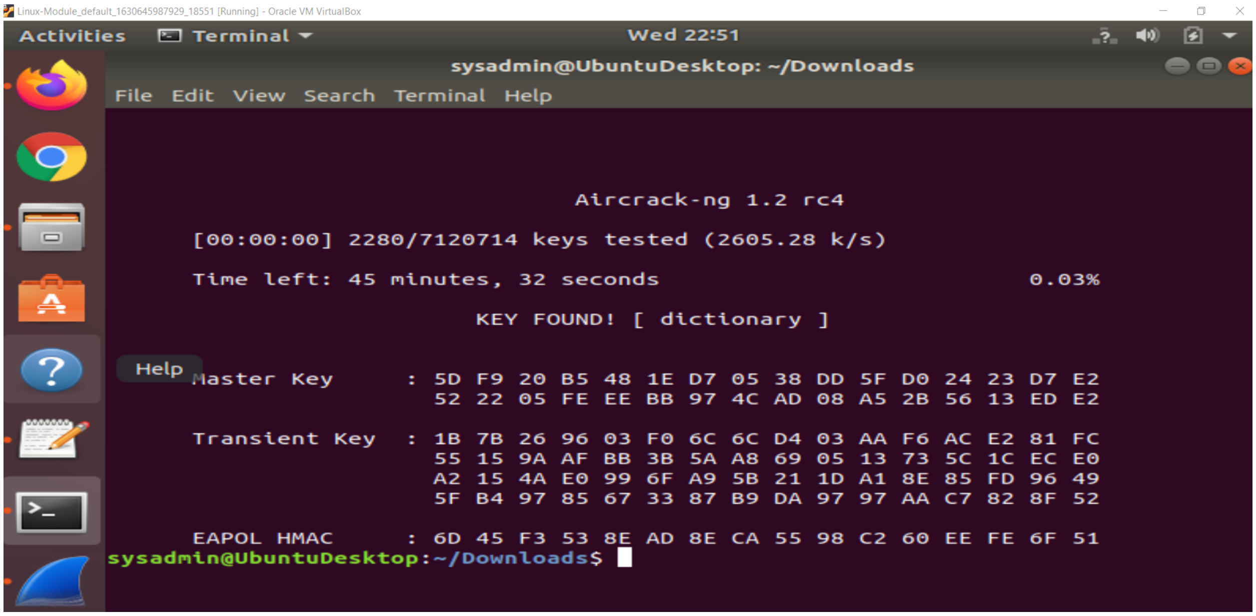
(Top part of screen of the result)



Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Wed 22:51
sysadmin@UbuntuDesktop: ~/Downloads
File Edit View Search Terminal Help

```
sysadmin@UbuntuDesktop:~/Downloads$ aircrack-ng Darkside.pcap -w /usr/share/wor
dlists/rockyou.txt
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...
```

(Bottom part of screen of the result)



Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Wed 22:51
sysadmin@UbuntuDesktop: ~/Downloads
File Edit View Search Terminal Help
Help

```
                              Aircrack-ng 1.2 rc4

      [00:00:00] 2280/7120714 keys tested (2605.28 k/s)

      Time left: 45 minutes, 32 seconds                          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
sysadmin@UbuntuDesktop:~/Downloads$ 
```

6b: The key to decrypt Darkside's wireless internet traffic was found. in the picture above.

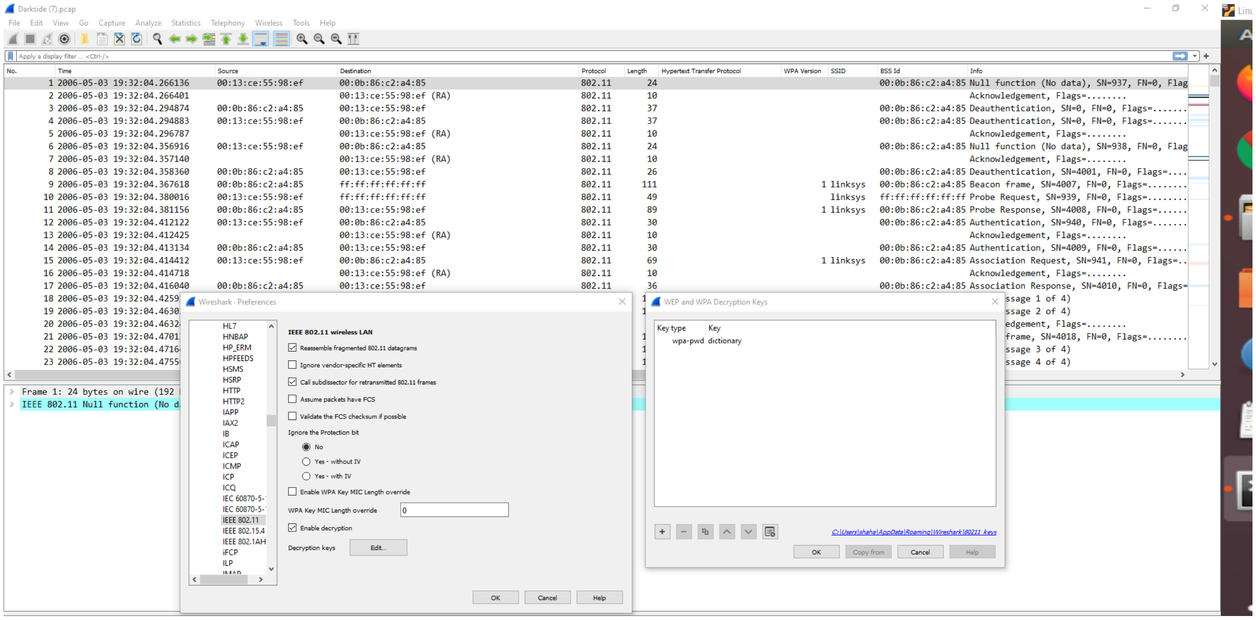
key found! (dictionary)

6c: Use the Dark Side's key to decrypt the wireless traffic in Wireshark:

once we got the key **(dictionary)**, we need to put the key in the wireshark in order to decrypt Darkside's wireless internet traffic.

Instruction adding the decryption key:

1. Go to **edit.**
2. Press on the **preferences.**
3. Double click on **protocols.**
4. Go down the menu and choose **IEEE 802.11** From the list.
5. go to the Decryption keys **Edit** box, and click.
6. Add the decryption key **dictionary** to list (press + to add)



Darkside (7).pcap

```
No.   Time                        Source              Destination              Protocol  Length  Hypertext Transfer Protocol  WPA Version  SSID       BSS Id             Info
    1 2006-05-03 19:32:04.266136  00:13:ce:55:98:ef   00:0b:86:c2:a4:85        802.11        24                                                      00:0b:86:c2:a4:85 Null function (No data), SN=937, FN=0, Flag
    2 2006-05-03 19:32:04.266401                      00:13:ce:55:98:ef (RA)   802.11        10                                                                        Acknowledgement, Flags=........
    3 2006-05-03 19:32:04.294874  00:0b:86:c2:a4:85   00:13:ce:55:98:ef        802.11        37                                                      00:0b:86:c2:a4:85 Deauthentication, SN=0, FN=0, Flags=.......
    4 2006-05-03 19:32:04.294883  00:13:ce:55:98:ef   00:0b:86:c2:a4:85        802.11        37                                                      00:0b:86:c2:a4:85 Deauthentication, SN=0, FN=0, Flags=.......
    5 2006-05-03 19:32:04.296787                      00:13:ce:55:98:ef (RA)   802.11        10                                                                        Acknowledgement, Flags=........
    6 2006-05-03 19:32:04.356916  00:13:ce:55:98:ef   00:0b:86:c2:a4:85        802.11        24                                                      00:0b:86:c2:a4:85 Null function (No data), SN=938, FN=0, Flag
    7 2006-05-03 19:32:04.357140                      00:13:ce:55:98:ef (RA)   802.11        10                                                                        Acknowledgement, Flags=........
    8 2006-05-03 19:32:04.358360  00:0b:86:c2:a4:85   00:13:ce:55:98:ef        802.11        26                                                      00:0b:86:c2:a4:85 Deauthentication, SN=4001, FN=0, Flags=....
    9 2006-05-03 19:32:04.367618  00:0b:86:c2:a4:85   ff:ff:ff:ff:ff:ff        802.11       111                                          1 linksys   00:0b:86:c2:a4:85 Beacon frame, SN=4007, FN=0, Flags=........
   10 2006-05-03 19:32:04.380016  00:13:ce:55:98:ef   ff:ff:ff:ff:ff:ff        802.11        49                                            linksys   ff:ff:ff:ff:ff:ff Probe Request, SN=939, FN=0, Flags=........
   11 2006-05-03 19:32:04.381156  00:0b:86:c2:a4:85   00:13:ce:55:98:ef        802.11        89                                          1 linksys   00:0b:86:c2:a4:85 Probe Response, SN=4008, FN=0, Flags=......
   12 2006-05-03 19:32:04.412122  00:13:ce:55:98:ef   00:0b:86:c2:a4:85        802.11        30                                                      00:0b:86:c2:a4:85 Authentication, SN=940, FN=0, Flags=.......
   13 2006-05-03 19:32:04.412425                      00:13:ce:55:98:ef (RA)   802.11        10                                                                        Acknowledgement, Flags=........
   14 2006-05-03 19:32:04.413134  00:0b:86:c2:a4:85   00:13:ce:55:98:ef        802.11        30                                                      00:0b:86:c2:a4:85 Authentication, SN=4009, FN=0, Flags=......
   15 2006-05-03 19:32:04.414412  00:13:ce:55:98:ef   00:0b:86:c2:a4:85        802.11        69                                          1 linksys   00:0b:86:c2:a4:85 Association Request, SN=941, FN=0, Flags=..
   16 2006-05-03 19:32:04.414718                      00:13:ce:55:98:ef (RA)   802.11        10                                                                        Acknowledgement, Flags=........
   17 2006-05-03 19:32:04.416040  00:0b:86:c2:a4:85   00:13:ce:55:98:ef        802.11        36                                                      00:0b:86:c2:a4:85 Association Response, SN=4010, FN=0, Flags=
   18 2006-05-03 19:32:04.4259                                                  1                                                                      ssage 1 of 4)
   19 2006-05-03 19:32:04.4630                                                  1                                                                      ssage 2 of 4)
   20 2006-05-03 19:32:04.4632                                                                                                                         edgement, Flags=........
   21 2006-05-03 19:32:04.4701                                                  1                                                                      frame, SN=4018, FN=0, Flags=........
   22 2006-05-03 19:32:04.4716                                                  1                                                                      ssage 3 of 4)
   23 2006-05-03 19:32:04.4755                                                  1                                                                      ssage 4 of 4)

> Frame 1: 24 bytes on wire (192
> IEEE 802.11 Null function (No d
```

Wireshark · Preferences

IEEE 802.11 wireless LAN

☑ Reassemble fragmented 802.11 datagrams

☐ Ignore vendor-specific HT elements

☑ Call subdissector for retransmitted 802.11 frames

☐ Assume packets have FCS

☐ Validate the FCS checksum if possible

Ignore the Protection bit

● No

○ Yes - without IV

○ Yes - with IV

☐ Enable WPA Key MIC Length override

WPA Key MIC Length override: 0

☑ Enable decryption

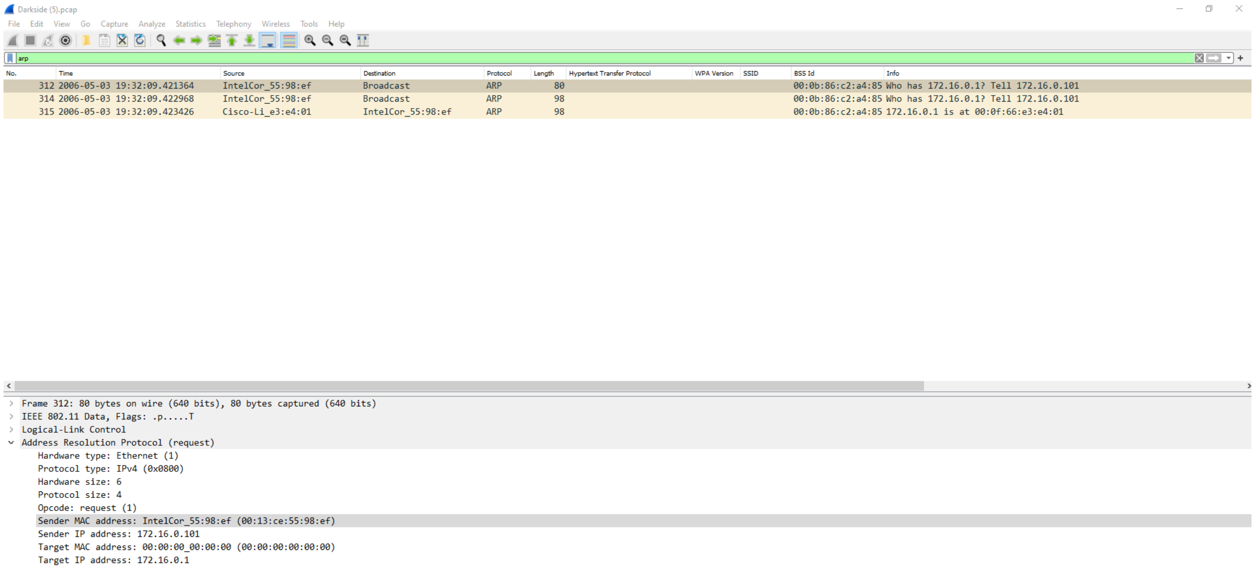
Decryption keys: Edit...

WEP and WPA Decryption Keys

Key type	Key
wpa-pwd	dictionary

6d: Host IP Addresses and MAC Addresses by looking at the decrypted ARP traffic:

once you are done adding the decryption key, type **arp** in the filter bar, and press enter to activate the filter.
press on the first line (no.312), and then go to the list at the bottom.
Double click on **Addresses Resolution Protocol (request) >**
to open the list.
The Host IP address is: **172.16.0.101**
The Host mac addresses is: **00:13:ce:55:987:ef**


Darkside (5).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	WPA Version	SSID	BSS Id	Info
312	2006-05-03 19:32:09.421364	IntelCor_55:98:ef	Broadcast	ARP	80				00:0b:86:c2:a4:85	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				00:0b:86:c2:a4:85	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				00:0b:86:c2:a4:85	172.16.0.1 is at 00:0f:66:e3:e4:01

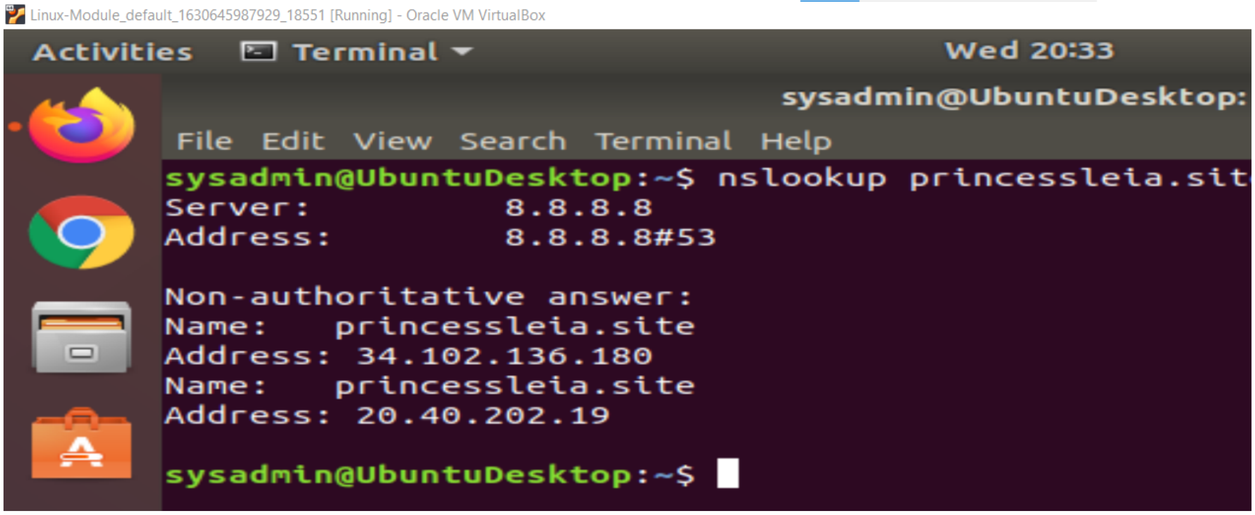
```
> Frame 312: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
> IEEE 802.11 Data, Flags: .p.....T
> Logical-Link Control
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
    Sender IP address: 172.16.0.101
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.16.0.1
```

Mission 7:

nslookup type: (TXT: Specifies the user identifier)

7a: View the DNS record from Mission #4:

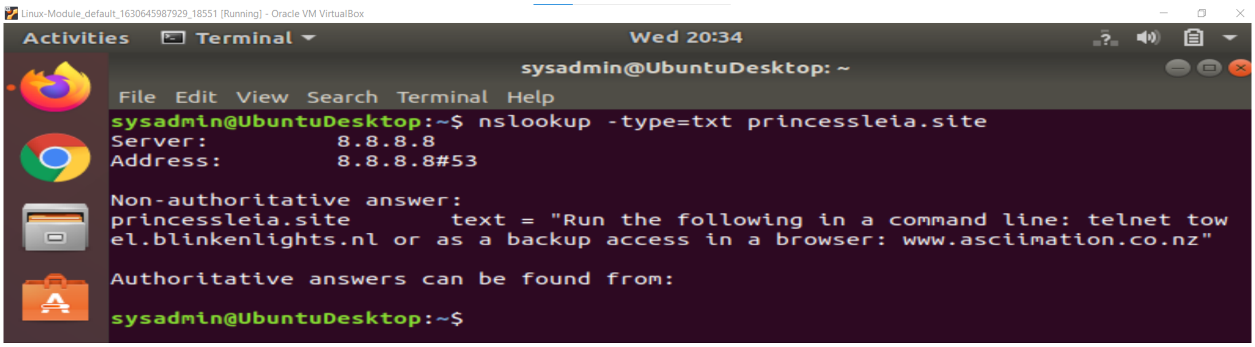
In this task I used **nslookup** with **princessleia.site** that was used in step 4, to look at the record for **princessleia.site**.


Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Wed 20:33
sysadmin@UbuntuDesktop:
File Edit View Search Terminal Help

```
sysadmin@UbuntuDesktop:~$ nslookup princessleia.sit
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   princessleia.site
Address: 34.102.136.180
Name:   princessleia.site
Address: 20.40.202.19

sysadmin@UbuntuDesktop:~$ 
```

7b: The Resistance provided you with a hidden message in the TXT record, with several steps to follow:

In this task, I used **nslookup -type=txt princessleia.site**, to look up the hidden txt message in the DNS record in **princessleia.site.**



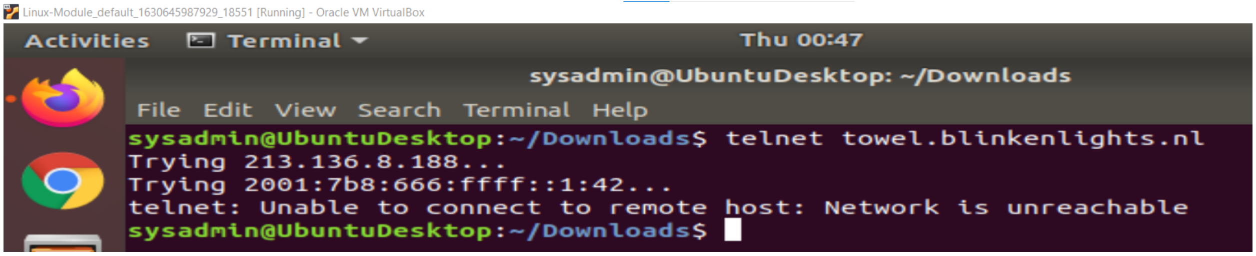
Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Wed 20:34
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

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

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

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$
```

7c: Follow the steps from the TXT record:

text= "Run the following in the command line: **telnet towel.blinkenlights.nl** or as a backup access in a browser: **www.asiimation.co.nz**"

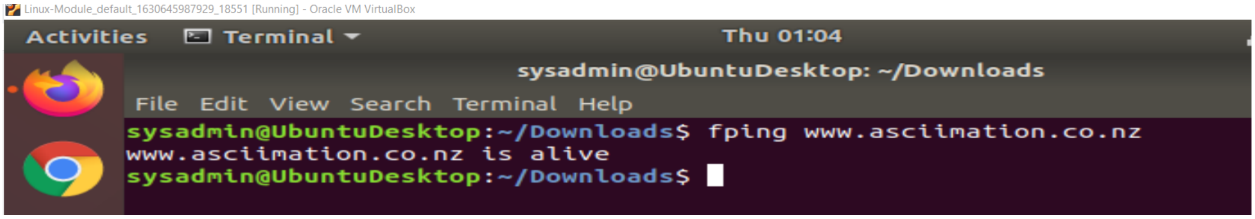
I ran the command **telnet towel.blinkenlights.nl** that was provided in the hidden message txt, and it looks like the main site is unavailable/unreachable.



Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Thu 00:47
sysadmin@UbuntuDesktop: ~/Downloads
File Edit View Search Terminal Help

```
sysadmin@UbuntuDesktop:~/Downloads$ telnet towel.blinkenlights.nl
Trying 213.136.8.188...
Trying 2001:7b8:666:ffff::1:42...
telnet: Unable to connect to remote host: Network is unreachable
sysadmin@UbuntuDesktop:~/Downloads$
```

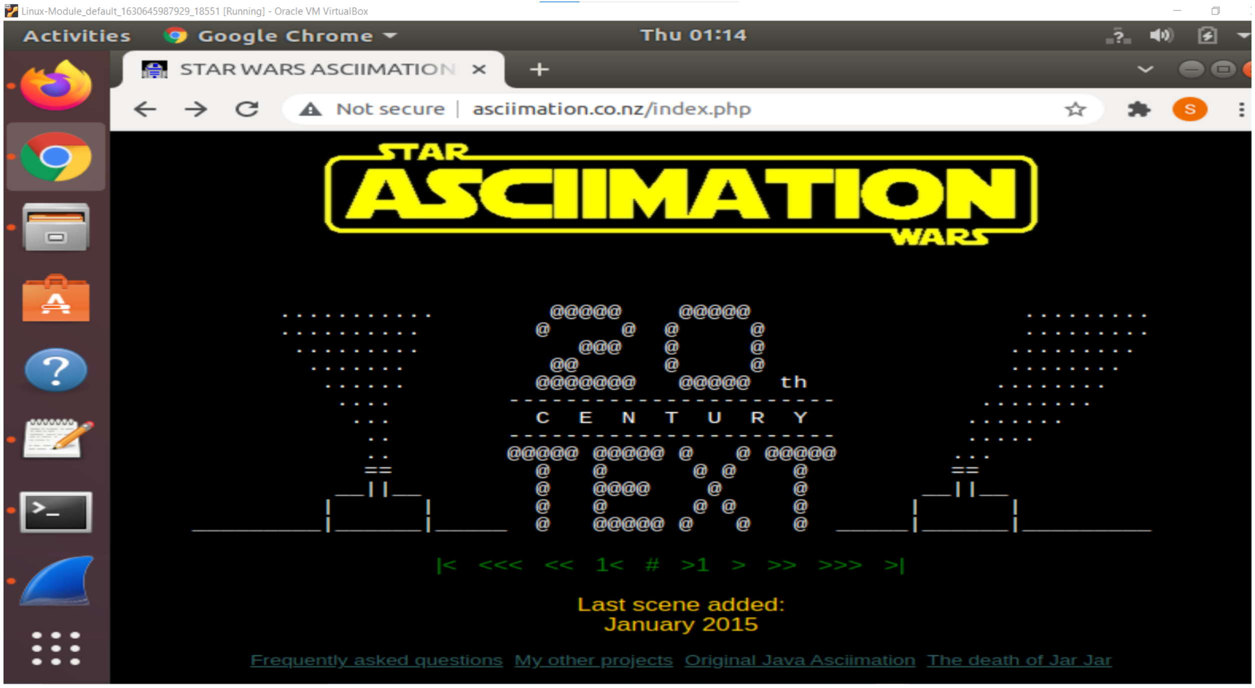
The website **www.asiimation.co.nz** was provided in the hidden txt as a backup, in case the main telnet site is unavailable (see screenshot above). The website provided is **alive**.



Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Thu 01:04
sysadmin@UbuntuDesktop: ~/Downloads
File Edit View Search Terminal Help

```
sysadmin@UbuntuDesktop:~/Downloads$ fping www.asciimation.co.nz
www.asciimation.co.nz is alive
sysadmin@UbuntuDesktop:~/Downloads$
```

7d: In order to open the link to **www.asiimation.co.nz**, I right click on it, and then pressed **open link** with google chrome.



Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox

Not secure | asciimation.co.nz/index.php

Last scene added:
January 2015