Review each network issue in the missions below.

Document each DNS record type found.

Take note of the DNS records that can explain the reasons for the existing network issue.

Provide recommended fixes to save the Galaxy!

Mission 1

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

Using nslookup -type=MX starwars my results were:

```
Server:     8.8.8.8
Address:    8.8.8.8#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 = 1 aspmx.l.google.com.
starwars.com  mail exchanger = 5 alt2.aspmx.l.google.com.
starwars.com  mail exchanger = 10 aspmx2.googlemail.com.
```

Explain why the Resistance isn't receiving any emails.

The new primary mail server is *asltx.1.google.com* and the secondary should be *asltx.2.google.com* however the results of the search show that the mail servers are as follows:

- Alt1.aspx.l.google.com
- Aspmx3.googlemail.com
- Aspmx.l.google.com
- Alt2.aspmx.l.google.com
- aspmx2.googlemail.com

Therefore they are misconfigured, since they do not match the new primary and secondary mail servers.

Document what a corrected DNS record should be

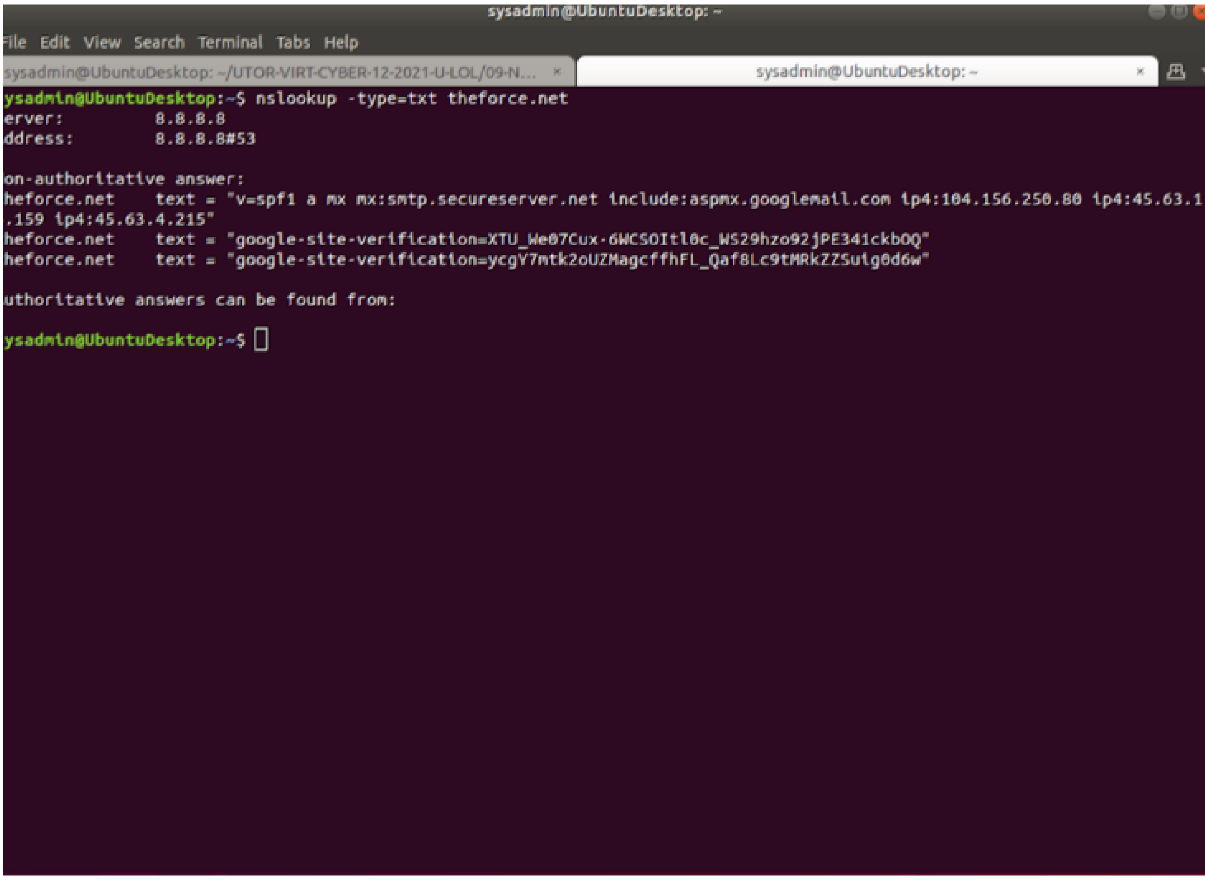
- starwars.com mail exchanger = 1 *Asltx.1.google.com*
- starwars.com mail exchanger = 5*asltx.2.google.com*

Mission 2

Determine and document the SPF for theforce.net using NSLOOKUP.

- Nslookup -type=txt theforce.net

- 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"



sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Tabs Help
sysadmin@UbuntuDesktop: ~/UTOR-VIRT-CYBER-12-2021-U-LOL/09-N...
sysadmin@UbuntuDesktop: ~

```
ysadmin@UbuntuDesktop:~$ nslookup -type=txt theforce.net
erver:          8.8.8.8
ddress:         8.8.8.8#53

on-authoritative answer:
heforce.net     text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80 ip4:45.63.1
.159 ip4:45.63.4.215"
heforce.net     text = "google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckbOQ"
heforce.net     text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"

uthoritative answers can be found from:

ysadmin@UbuntuDesktop:~$ 
```

Explain why the Force's emails are going to spam.

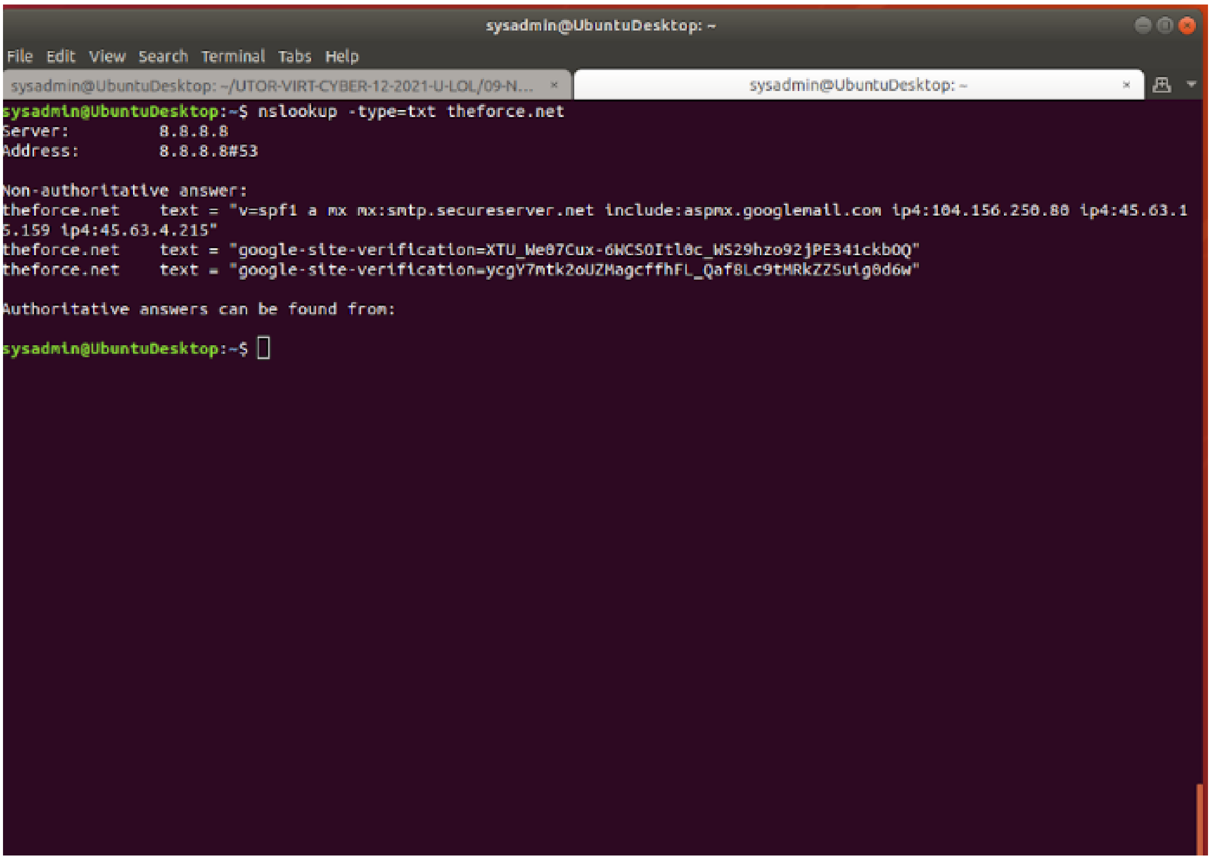
Theforce.net changed the IP address of their mail server to 45.23.176.21 whereas the current listed SPF for the force.net is :

- ip4:104.156.250.80

- ip4:45.63.15.159 ip4:45.63.4.215

Document what a corrected DNS record should be.

- Ip4: 45.23.176.21 should be a corrected DNS

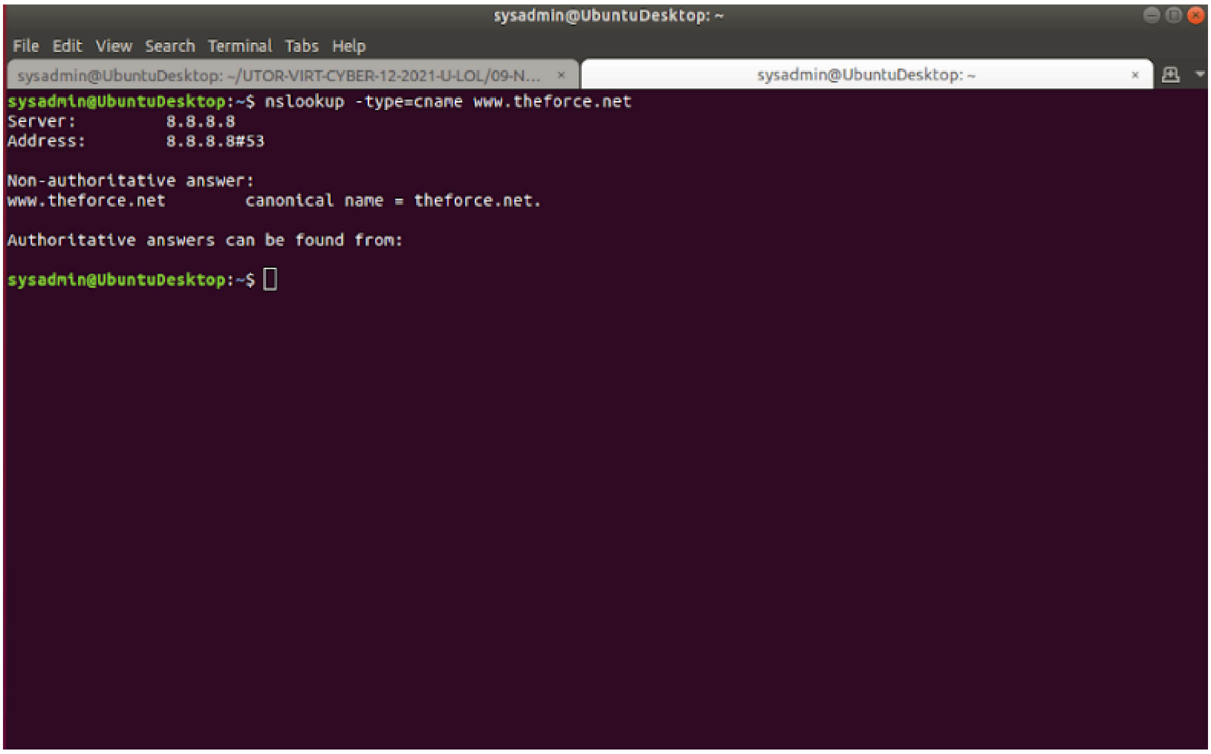

sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Tabs Help
sysadmin@UbuntuDesktop: ~/UTOR-VIRT-CYBER-12-2021-U-LOL/09-N...
sysadmin@UbuntuDesktop: ~

```
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.googlemail.com ip4:104.156.250.80 ip4:45.63.1
5.159 ip4:45.63.4.215"
theforce.net    text = "google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo92jPE341ckbOQ"
theforce.net    text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$ 
```

Mission 3

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

- Nslookup -type=cname www.theforce.net



sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Tabs Help
sysadmin@UbuntuDesktop: ~/UTOR-VIRT-CYBER-12-2021-U-LOL/09-N...
sysadmin@UbuntuDesktop: ~

```
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:

sysadmin@UbuntuDesktop:~$ 
```

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

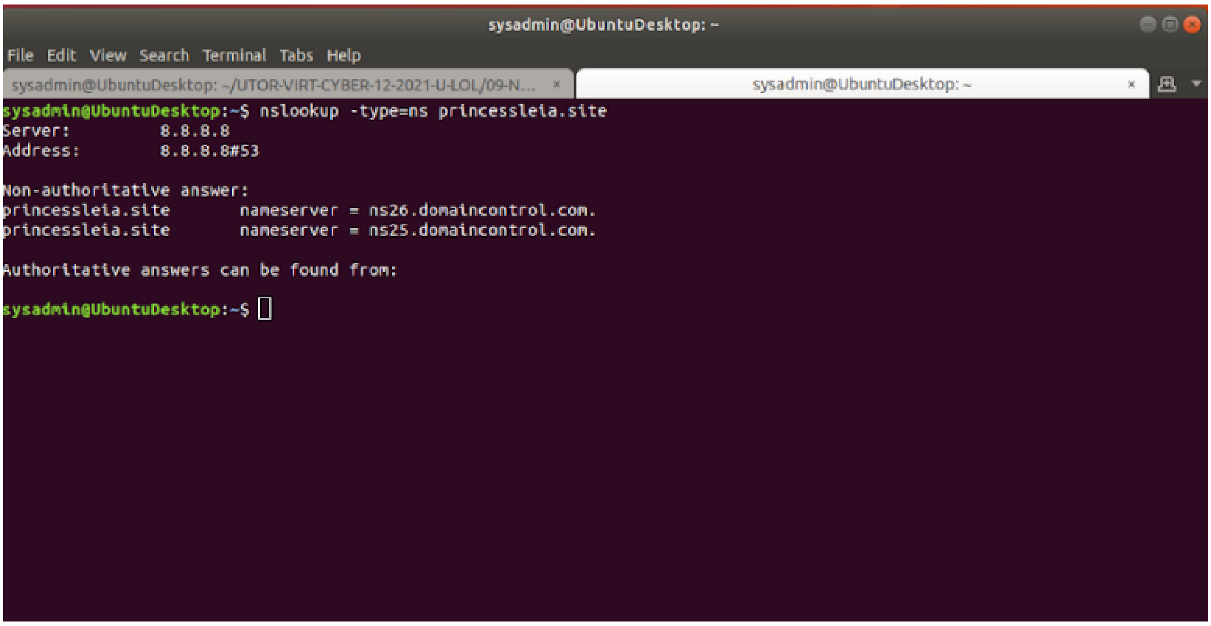
As shown above, the canonical name (cname) is listed as theforce.net whereas it should be listed as resistance.theforce.net

Document what a corrected DNS record should be.

The corrected DNS record (cname) should be resistance.theforce.net

Mission 4

Confirm the DNS records for princessleia.site.



sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Tabs Help
sysadmin@UbuntuDesktop: ~/UTOR-VIRT-CYBER-12-2021-U-LOL/09-N...
sysadmin@UbuntuDesktop: ~

```
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:~$ 
```

Document how you would fix the DNS record to prevent this issue from happening again.

The backup DNA server ns2.galaxybackup.com should be added to the NS list on the server

To fix this you would add a tertiary server :
Princessleia.site   nameserver = ns2.galaxybackup.com

Mission 5

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.

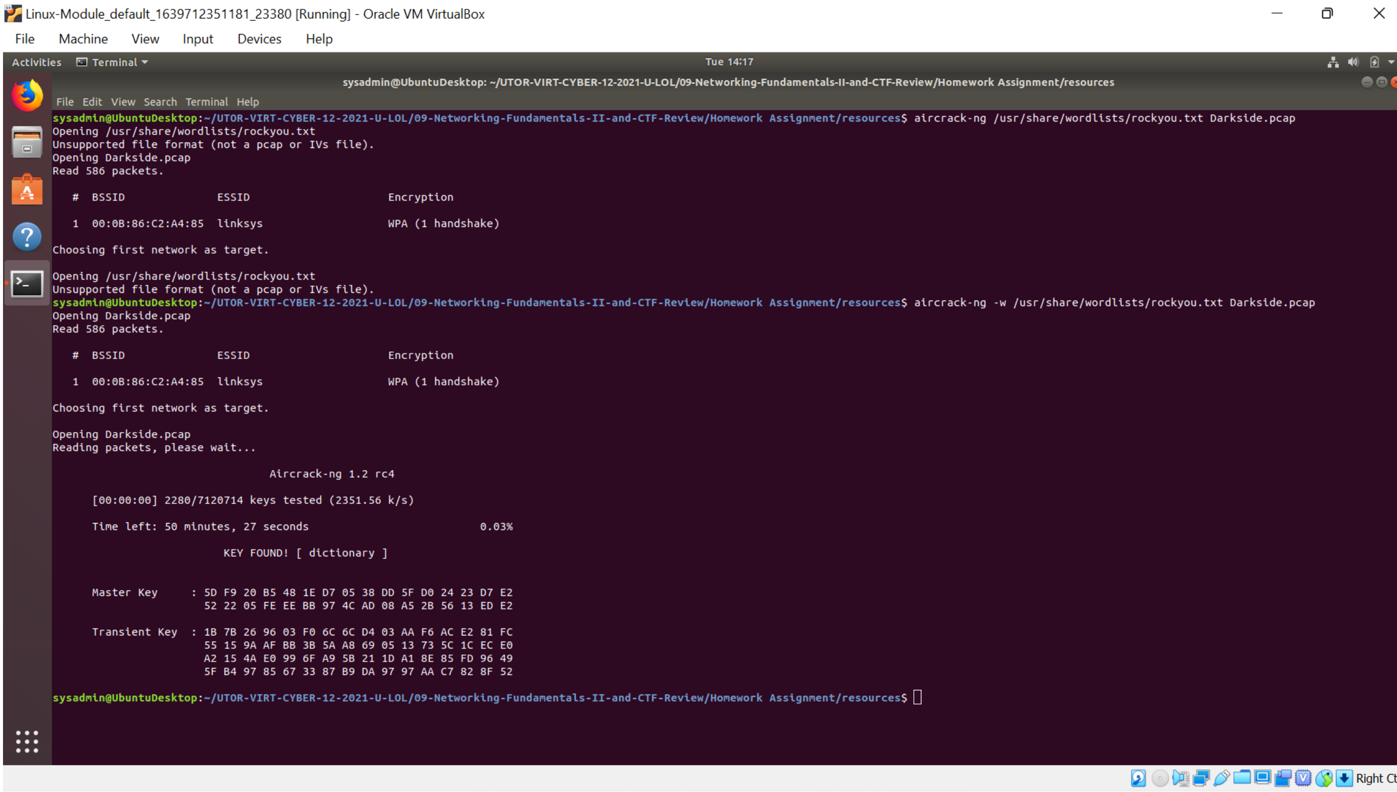
D-C-E-F--J-I-L-Q-T-V-Jedha

Mission 6

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.

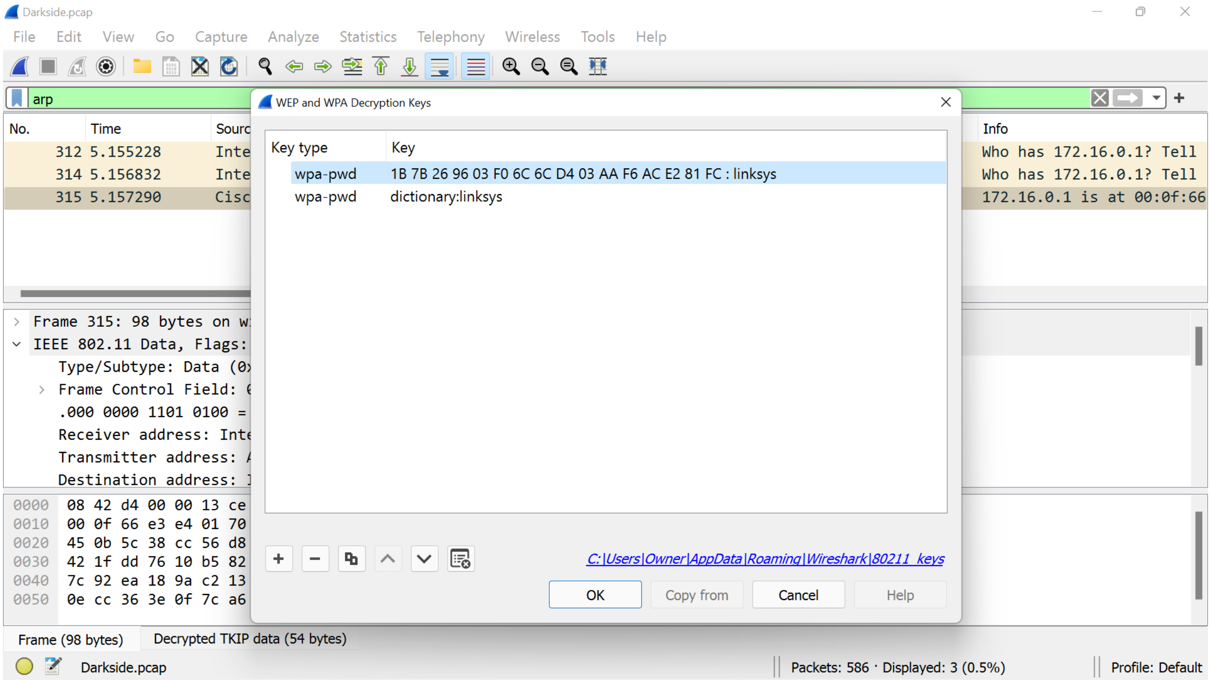


Linux-Module_default_1639712351181_23380 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Tue 14:17
sysadmin@UbuntuDesktop: ~/UTOR-VIRT-CYBER-12-2021-U-LOL/09-Networking-Fundamentals-II-and-CTF-Review/Homework Assignment/resources
File Edit View Search Terminal Help
Right Ct

```
sysadmin@UbuntuDesktop:~/UTOR-VIRT-CYBER-12-2021-U-LOL/09-Networking-Fundamentals-II-and-CTF-Review/Homework Assignment/resources$ aircrack-ng /usr/share/wordlists/rockyou.txt Darkside.pcap
Opening /usr/share/wordlists/rockyou.txt
Unsupported file format (not a pcap or IVs file).
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 /usr/share/wordlists/rockyou.txt
Unsupported file format (not a pcap or IVs file).
sysadmin@UbuntuDesktop:~/UTOR-VIRT-CYBER-12-2021-U-LOL/09-Networking-Fundamentals-II-and-CTF-Review/Homework Assignment/resources$ aircrack-ng -w /usr/share/wordlists/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] 2280/7120714 keys tested (2351.56 k/s)

      Time left: 50 minutes, 27 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

sysadmin@UbuntuDesktop:~/UTOR-VIRT-CYBER-12-2021-U-LOL/09-Networking-Fundamentals-II-and-CTF-Review/Homework Assignment/resources$ 
```

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>.


Darkside.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
WEP and WPA Decryption Keys
C:\Users\Owner\AppData\Roaming\Wireshark\80211_keys
OK
Copy from
Cancel
Help
Frame (98 bytes)
Decrypted TKIP data (54 bytes)
Darkside.pcap
Packets: 586 · Displayed: 3 (0.5%)
Profile: Default

arp

```
No.   Time       Sourc     Info
312 5.155228    Inte      Who has 172.16.0.1? Tell
314 5.156832    Inte      Who has 172.16.0.1? Tell
315 5.157290    Cisc      172.16.0.1 is at 00:0f:66
```

Key type	Key
wpa-pwd	1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC : linksys
wpa-pwd	dictionary:linksys

```
> Frame 315: 98 bytes on w
v IEEE 802.11 Data, Flags:
    Type/Subtype: Data (0x
  > Frame Control Field: 0
    .000 0000 1101 0100 =
    Receiver address: Inte
    Transmitter address: A
    Destination address: I
```

```
0000  08 42 d4 00 00 13 ce
0010  00 0f 66 e3 e4 01 70
0020  45 0b 5c 38 cc 56 d8
0030  42 1f dd 76 10 b5 82
0040  7c 92 ea 18 9a c2 13
0050  0e cc 36 3e 0f 7c a6
```

Once you have decrypted the traffic, figure out the following Dark Side information:

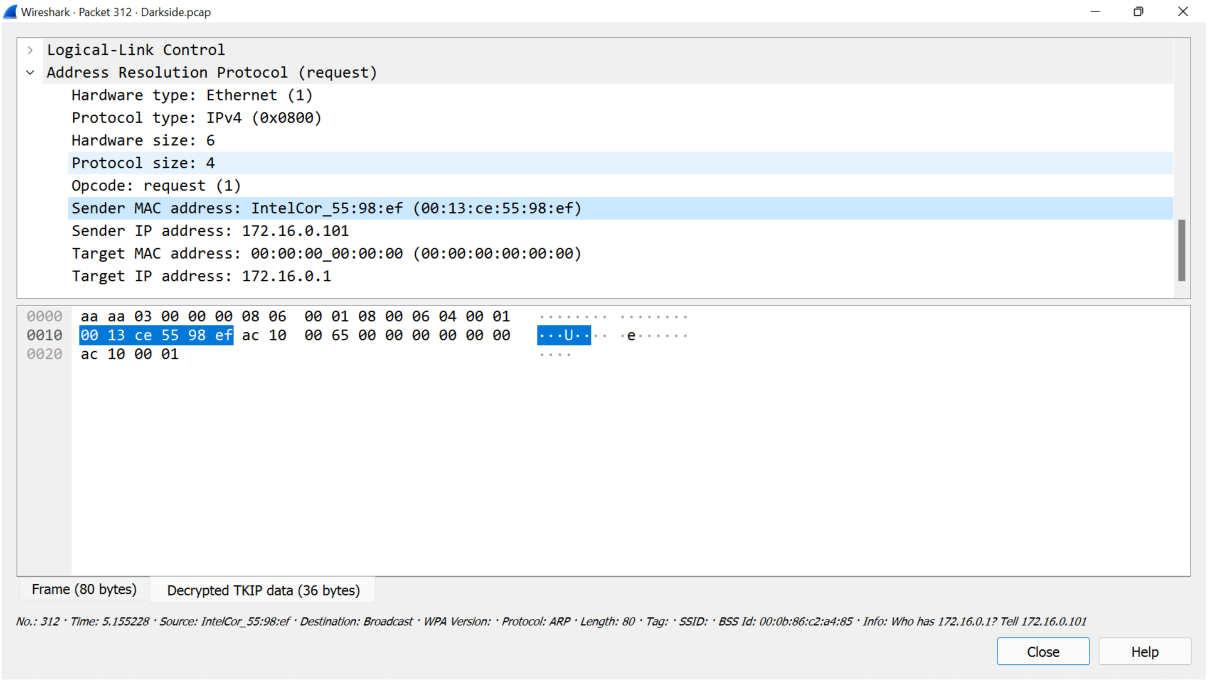
- Host IP Addresses and MAC Addresses by looking at the decrypted ARP traffic.

Host: Cisco-Li_e3:e4:01 (00:0f:66:e3:e4:01)

Sender's IP: 172.16.0.1

Target's MAC: IntelCor_55:98:ef (00:13:ce:55:98:ef)

Target's ip: 172.16.0.101

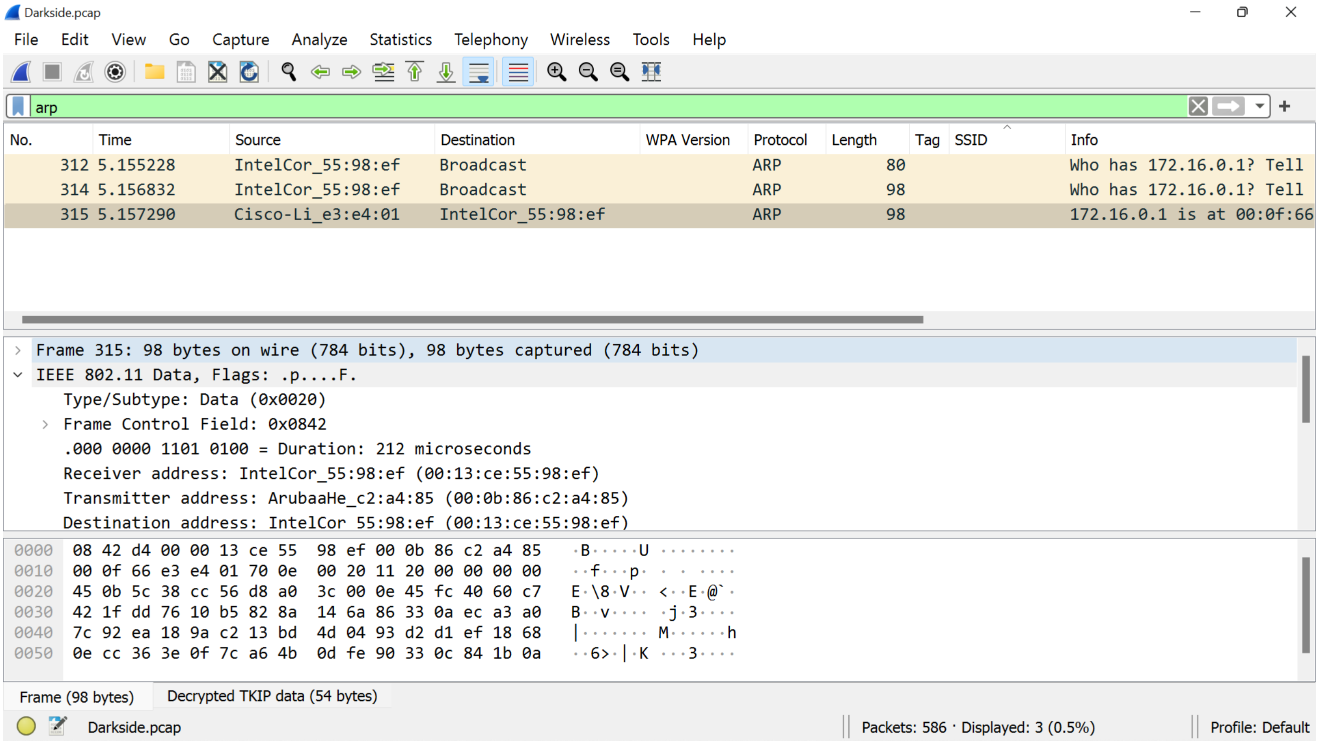


```
> Logical-Link Control
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
    Sender IP address: 172.16.0.101
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.16.0.1
```

```
0000  aa aa 03 00 00 00 08 06  00 01 08 00 06 04 00 01   ········ ········
0010  00 13 ce 55 98 ef ac 10  00 65 00 00 00 00 00 00   ···U···· ·e······
0020  ac 10 00 01                                        ····
```

No.: 312 · Time: 5.155228 · Source: IntelCor_55:98:ef · Destination: Broadcast · WPA Version: · Protocol: ARP · Length: 80 · Tag: · SSID: · BSS Id: 00:0b:86:c2:a4:85 · Info: Who has 172.16.0.1? Tell 172.16.0.101

- Document these IP and MAC Addresses, as the resistance will use these IP addresses to launch a retaliatory attack.



arp

No.	Time	Source	Destination	WPA Version	Protocol	Length	Tag	SSID	Info
312	5.155228	IntelCor_55:98:ef	Broadcast		ARP	80			Who has 172.16.0.1? Tell
314	5.156832	IntelCor_55:98:ef	Broadcast		ARP	98			Who has 172.16.0.1? Tell
315	5.157290	Cisco-Li_e3:e4:01	IntelCor_55:98:ef		ARP	98			172.16.0.1 is at 00:0f:66

```
> Frame 315: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
v IEEE 802.11 Data, Flags: .p....F.
    Type/Subtype: Data (0x0020)
  > Frame Control Field: 0x0842
    .000 0000 1101 0100 = Duration: 212 microseconds
    Receiver address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
    Transmitter address: ArubaaHe_c2:a4:85 (00:0b:86:c2:a4:85)
    Destination address: IntelCor 55:98:ef (00:13:ce:55:98:ef)
```

```
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····
```

Packets: 586 · Displayed: 3 (0.5%)

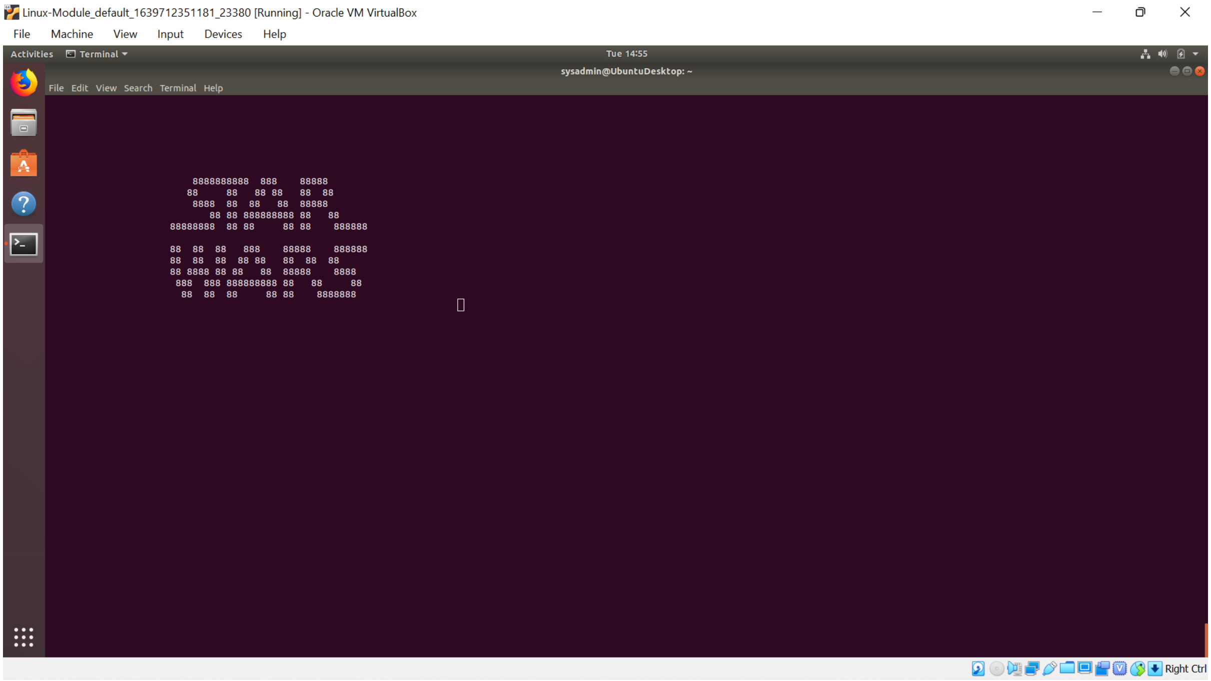
Profile: Default

Mission 7

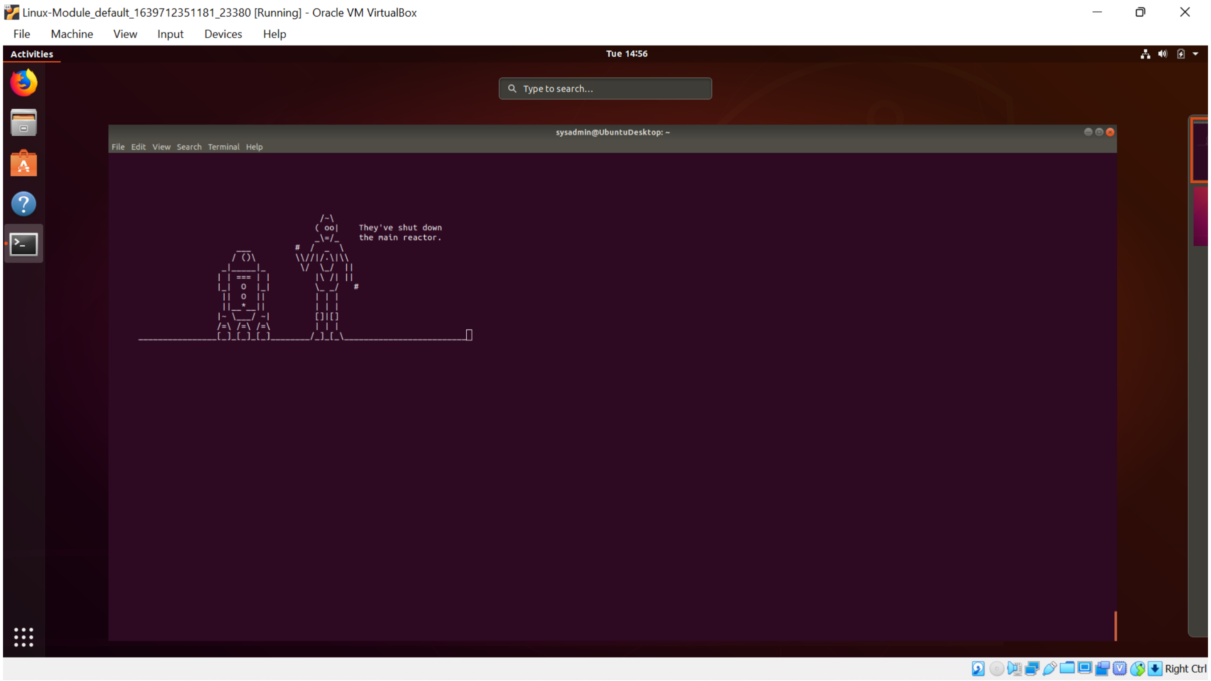
View the DNS record from Mission #4.

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

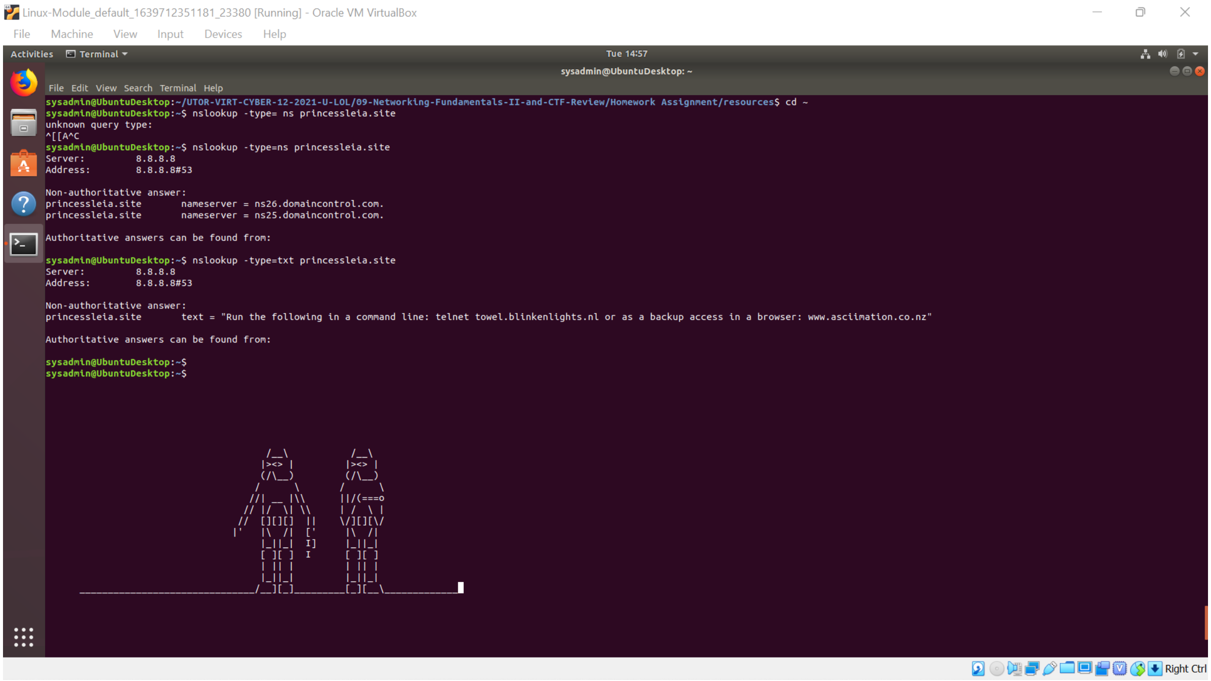
The message was:
Run the following in a command line: telnet towel.blinkenlights.nl
When I did, I received the Star Wars film ! (see screenshots below)


Linux-Module_default_1639712351181_23380 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Tue 14:55
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Right Ctrl

```
    8888888888  888    88888
   88     88   88 88   88  88
    8888  88  88   88  88888
       88 88 888888888 88   88
88888888  88 88     88 88    888888

88  88  88   888    88888    888888
88  88  88  88 88   88  88  88
88 8888 88 88   88  88888    8888
 888  888 888888888 88   88     88
  88  88  88     88 88    8888888
```


Linux-Module_default_1639712351181_23380 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Tue 14:56
Type to search…
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Right Ctrl

```
                                     /~\
                                    ( oo|    They've shut down
                                    _\=/_    the main reactor.
                    ___         #  /  _  \
                   / ()\        \\//|/.\|\\
                 _|_____|_       \/  \_/  ||
                | | === | |         |\ /| ||
                |_|  O  |_|         \_ _/   #
                 ||  O  ||          | | |
                 ||__*__||          | | |
                |~ \___/ ~|         []|[]
                /=\ /=\ /=\         | | |
________________[_]_[_]_[_]________/_]_[_\_________________________
```


Linux-Module_default_1639712351181_23380 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Tue 14:57
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Right Ctrl

```
sysadmin@UbuntuDesktop:~/UTOR-VIRT-CYBER-12-2021-U-LOL/09-Networking-Fundamentals-II-and-CTF-Review/Homework Assignment/resources$ cd ~
sysadmin@UbuntuDesktop:~$ nslookup -type= ns princessleia.site
unknown query type:
^[[A^C
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:~$ 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 towel.blinkenlights.nl or as a backup access in a browser: www.asciimation.co.nz"

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$
sysadmin@UbuntuDesktop:~$




                                       /__\           /__\
                                      |><> |         |><> |
                                      (/\__)         (/\__)
                                     /      \       /      \
                                    //| __ |\\      ||/(===o
                                   // |/  \| \\     | /  \ |
                                  //  [][][]  ||    \/][][\/
                                 |'   |\  /|  ['     |\  /|
                                      |_||_|  I]     |_||_|
                                      [ ][ ]  I      [ ][ ]
                                      | || |         | || |
                                      |_||_|         |_||_|
      _______________________________/__][_]_________[_][__\______________
```