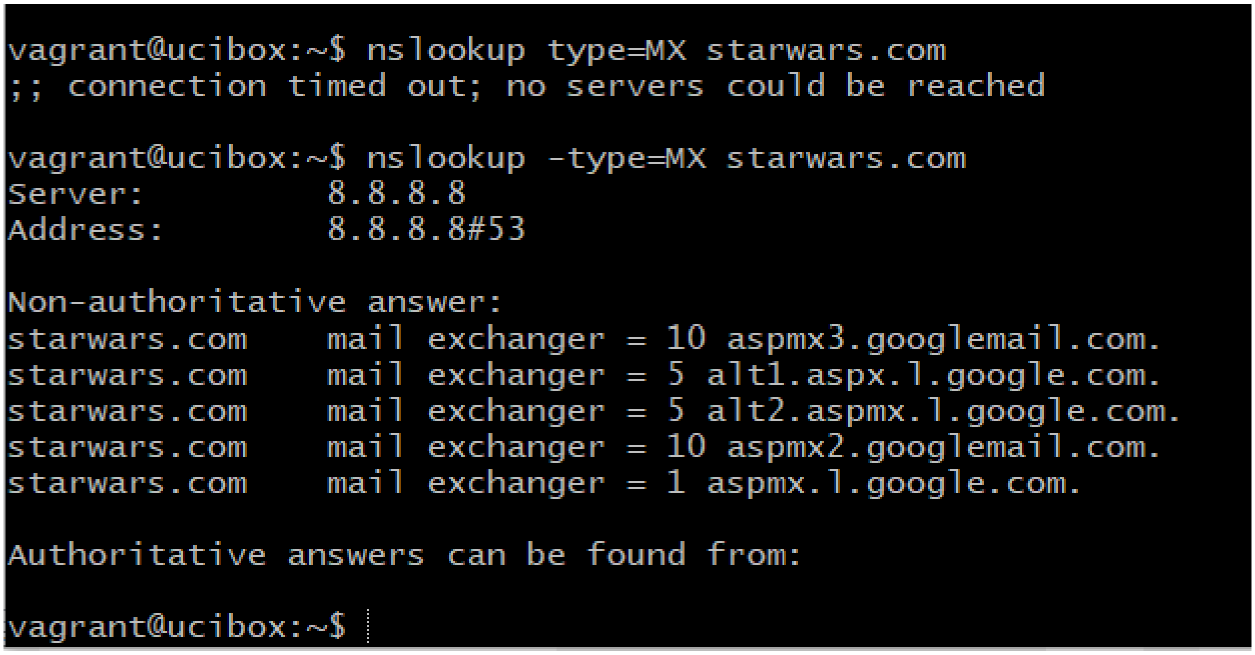
Networks Fundamentals II Homework: *In a Network Far, Far Away!*

Mission 1

- Nslookup -type=MX starwars.com

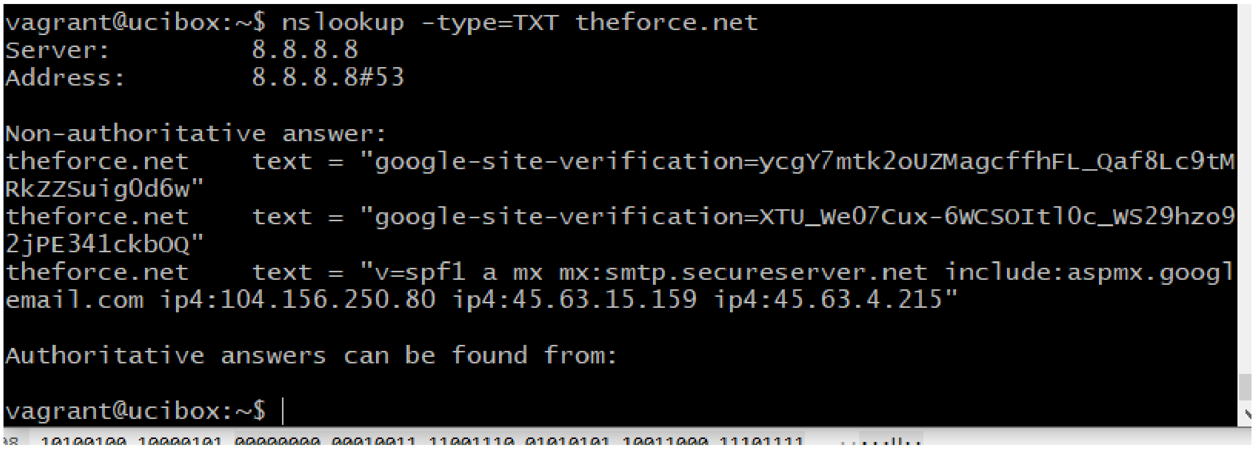


```
vagrant@ucibox:~$ nslookup type=MX starwars.com
;; connection timed out; no servers could be reached

vagrant@ucibox:~$ nslookup -type=MX starwars.com
Server:         8.8.8.8
Address:        8.8.8.8#53

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

Authoritative answers can be found from:

vagrant@ucibox:~$
```

- The current mail servers for starwars.com do not match what the network team had built and deployed. Hence they cannot receive any emails because the domain names are not associated with the mail servers deployed by the network team. The mail servers displayed above are not the servers the network team deployed.
- The correct servers should be asltx.1.google.com as primary and asltx.2.google.com as secondary
    - Starwars.com mail exchanger = 1 asltx.1.google.com
    - Starwars.com mail exchanger = 2 asltx.2.google.com

Mission 2

- Nslookup -type=TXT theforce.net

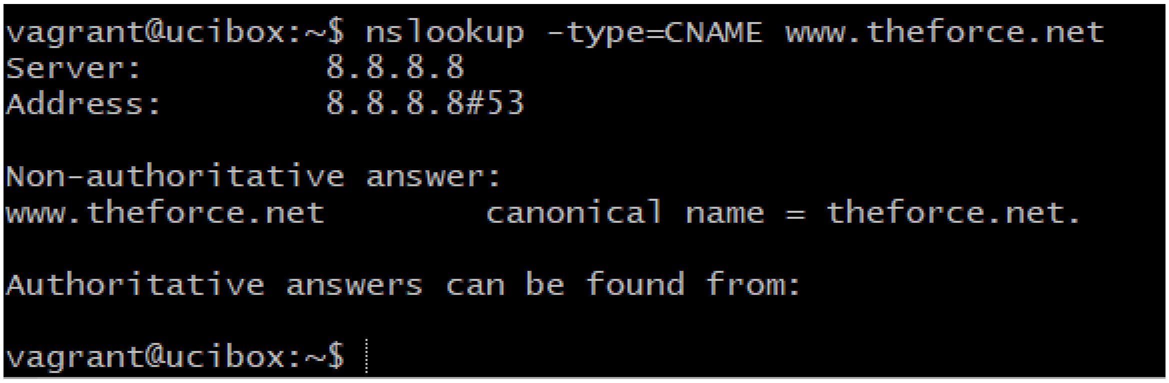


```
vagrant@ucibox:~$ nslookup -type=TXT theforce.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
theforce.net    text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tM
RkZZSuig0d6w"
theforce.net    text = "google-site-verification=XTU_We07Cux-6WCSOItl0c_WS29hzo9
2jPE341ckbOQ"
theforce.net    text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googl
email.com ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"

Authoritative answers can be found from:

vagrant@ucibox:~$ |
 10100100 10000101 00000000 00010011 11001110 01010101 10011000 11101111
```

- Emails from theforce.net are going to spam is due to the change in IP address not being included in the DNS records. The absence of theforce.net IP address is due to the DNS record not updating to to be align with the SPF records.
- The correct DNS should include the new IP address for theforce.net
  - Ip4: 45.23.176.21

Mission 3

- Nslookup -type=CNAME www.theforce.net

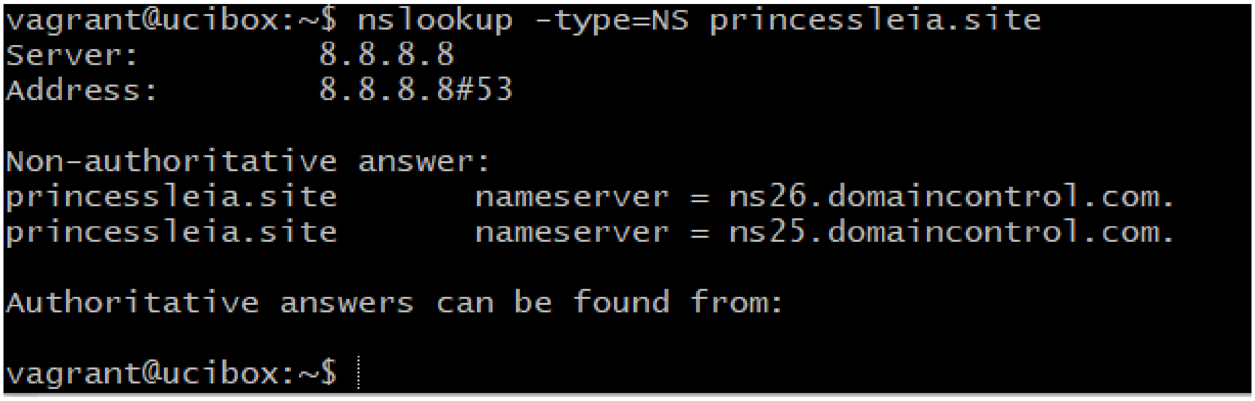


```
vagrant@ucibox:~$ nslookup -type=CNAME www.theforce.net
Server:         8.8.8.8
Address:        8.8.8.8#53

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

Authoritative answers can be found from:

vagrant@ucibox:~$
```

- As seen above, resistance.theforce.net is not a documented canonical name for www.theforce.net cname records.
- The correct DNS record should have and show:
  - www.theforce.net   canonical name = resistance.theforce.net

Mission 4

- Nslookup -type=NS princessleia.site



```
vagrant@ucibox:~$ 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:

vagrant@ucibox:~$
```

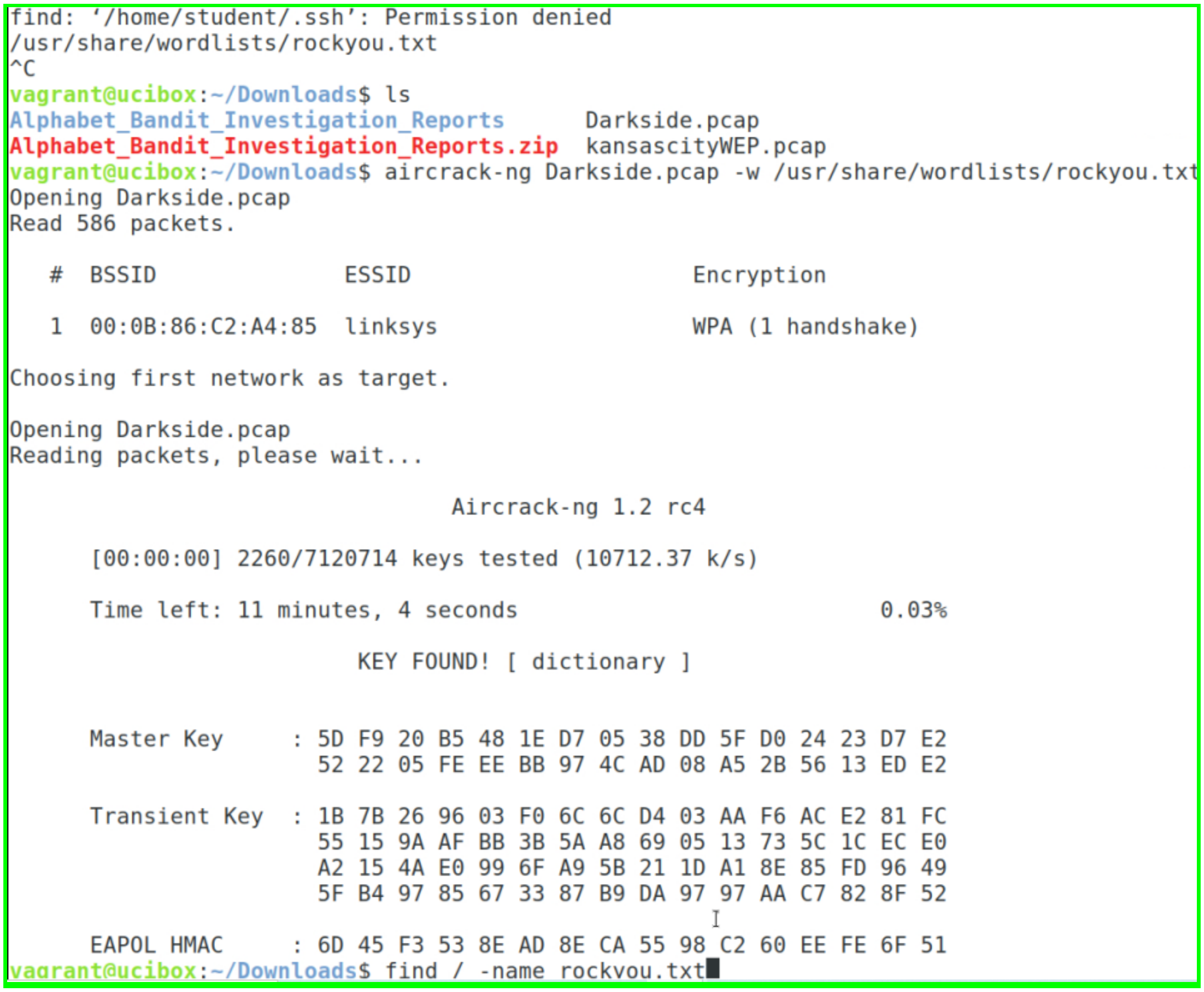
- Add the following the NS records
    - Princessleia.site   nameserver = ns2.galaxybackup.com

Mission 5

- Batuu > D > C > E > F > J > K > O > R > Q > T > V > Jedha

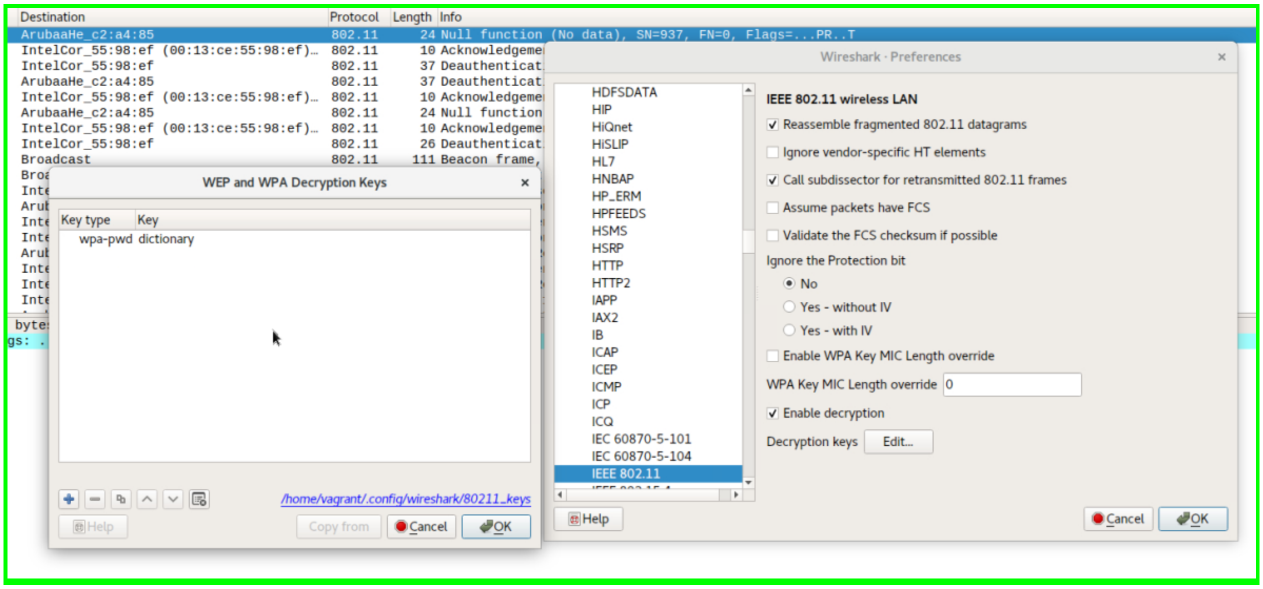
Mission 6

- Find / -name rockyou.txt
- Aircrack-ng Darkside.pcap -w /usr/share/wordlists/rockyou.txt



```
find: ‘/home/student/.ssh’: Permission denied
/usr/share/wordlists/rockyou.txt
^C
vagrant@ucibox:~/Downloads$ ls
Alphabet_Bandit_Investigation_Reports      Darkside.pcap
Alphabet_Bandit_Investigation_Reports.zip  kansascityWEP.pcap
vagrant@ucibox:~/Downloads$ aircrack-ng Darkside.pcap -w /usr/share/wordlists/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...

                                 Aircrack-ng 1.2 rc4

      [00:00:00] 2260/7120714 keys tested (10712.37 k/s)

      Time left: 11 minutes, 4 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
vagrant@ucibox:~/Downloads$ find / -name rockyou.txt
```

- Key Found! : dictionary



```
Destination                               Protocol Length Info
ArubaaHe_c2:a4:85                         802.11       24 Null function (No data), SN=937, FN=0, Flags=...PR..T
IntelCor_55:98:ef (00:13:ce:55:98:ef)…    802.11       10 Acknowledgeme
IntelCor_55:98:ef                         802.11       37 Deauthenticat
ArubaaHe_c2:a4:85                         802.11       37 Deauthenticat
IntelCor_55:98:ef (00:13:ce:55:98:ef)…    802.11       10 Acknowledgeme
ArubaaHe_c2:a4:85                         802.11       24 Null function
IntelCor_55:98:ef (00:13:ce:55:98:ef)…    802.11       10 Acknowledgeme
IntelCor_55:98:ef                         802.11       26 Deauthenticat
Broadcast                                 802.11      111 Beacon frame,
```

WEP and WPA Decryption Keys

Key type	Key
wpa-pwd	dictionary

/home/vagrant/.config/wireshark/80211_keys

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

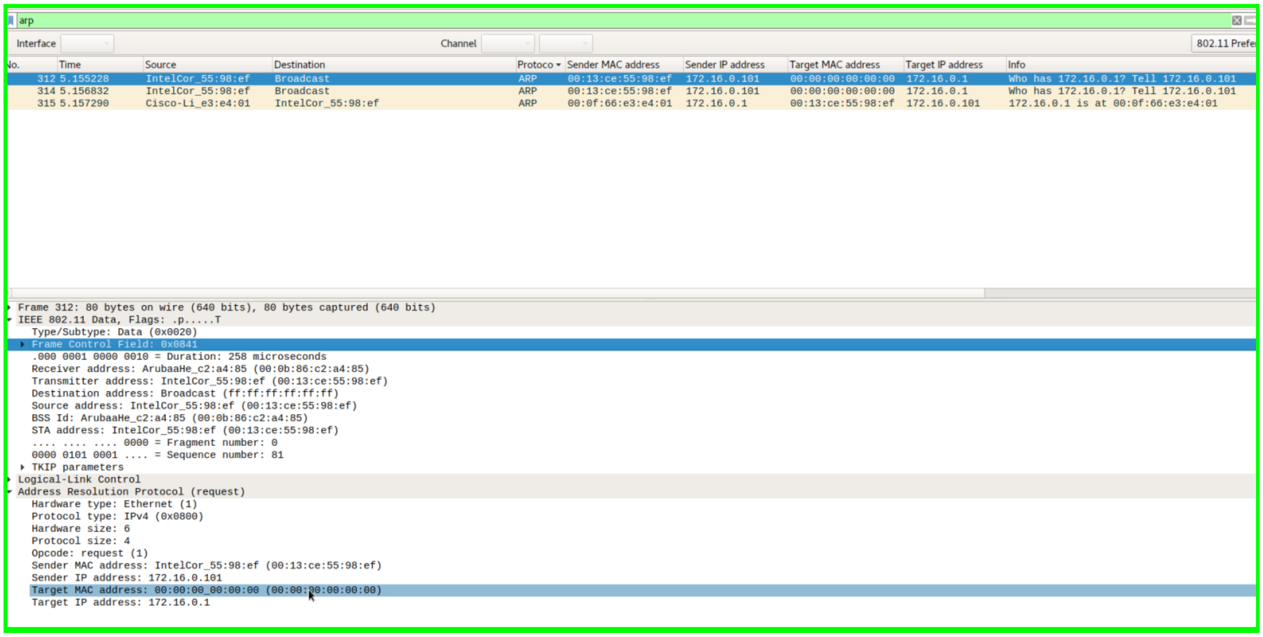
○ Yes - with IV

☐ Enable WPA Key MIC Length override

WPA Key MIC Length override 0

☑ Enable decryption

Decryption keys Edit...



arp

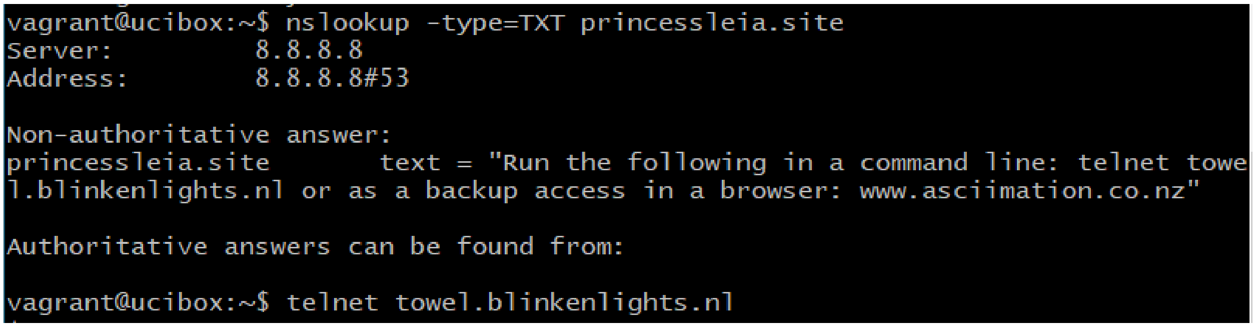
```
No.  Time     Source            Destination       Protoco Sender MAC address Sender IP address Target MAC address Target IP address Info
 312 5.155228 IntelCor_55:98:ef Broadcast         ARP     00:13:ce:55:98:ef  172.16.0.101      00:00:00:00:00:00  172.16.0.1        Who has 172.16.0.1? Tell 172.16.0.101
 314 5.156832 IntelCor_55:98:ef Broadcast         ARP     00:13:ce:55:98:ef  172.16.0.101      00:00:00:00:00:00  172.16.0.1        Who has 172.16.0.1? Tell 172.16.0.101
 315 5.157290 Cisco-Li_e3:e4:01 IntelCor_55:98:ef ARP     00:0f:66:e3:e4:01  172.16.0.1        00:13:ce:55:98:ef  172.16.0.101      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
    Type/Subtype: Data (0x0020)
  ▸ Frame Control Field: 0x0841
    .000 0001 0000 0010 = Duration: 258 microseconds
    Receiver address: ArubaaHe_c2:a4:85 (00:0b:86:c2:a4:85)
    Transmitter address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
    BSS Id: ArubaaHe_c2:a4:85 (00:0b:86:c2:a4:85)
    STA address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
    .... .... .... 0000 = Fragment number: 0
    0000 0101 0001 .... = Sequence number: 81
  ▸ TKIP parameters
▸ Logical-Link Control
▾ 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
```

- Addresses of interest
  - IP:
    - 172.16.0.101
    - 172.16.0.1
  - MAC:
    - 00:13ce:55:98:ef
    - 00:0f:66:e3:e4:01

Mission 7

- Nslookup -type=TXT princessleia.txt
- Telnet towel.blinkenlights.nl



```
vagrant@ucibox:~$ 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 towe
l.blinkenlights.nl or as a backup access in a browser: www.asciimation.co.nz"

Authoritative answers can be found from:

vagrant@ucibox:~$ telnet towel.blinkenlights.nl
```

- ITS A STAR WARS MINI MOVIE!!!! I LOVE IT