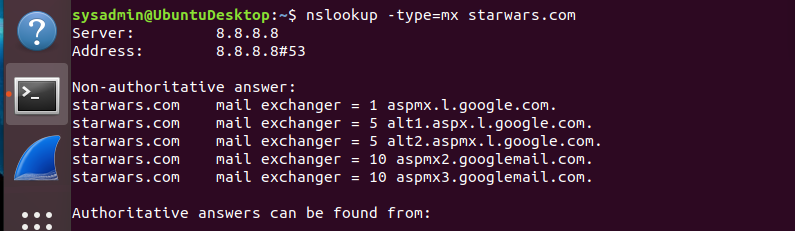
Mission 1:

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


Explain why the Resistance isn't receiving any emails.  
Asltx.l.google.com and asltx.2.google.com are not listed under non-authoritative.

Document what a corrected DNS record should be:

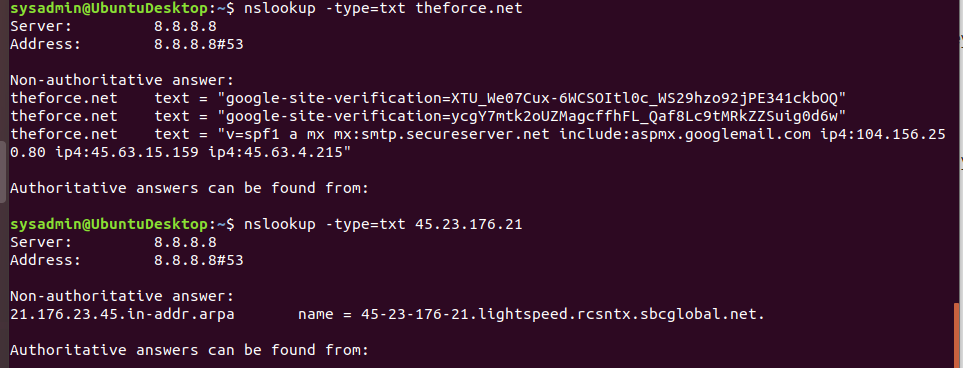
1 asltx.l.google.com

10 asltx.2.google.com

Mission 2:

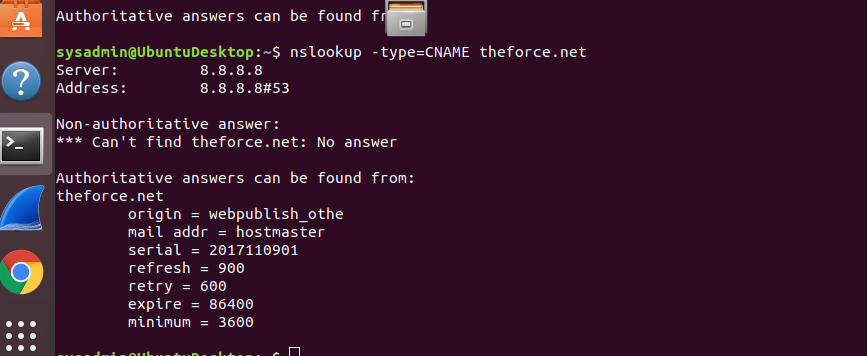
Your mission:

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



* Explain why the Force's emails are going to spam.  
  name = 45-23-176-21.lightspeed.rcsntx.sbcglobal.net needs to be added to SPF protocol.
* Document what a corrected DNS record should be:  
  "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:45-23-176-21.lightspeed.rcsntx.sbcglobal.net ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"

Mission 3:

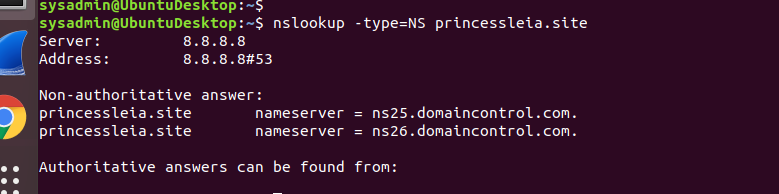
Document how a CNAME should look by viewing the CNAME of www.theforce.net using NSLOOKUP.  


Explain why the sub page of resistance.theforce.net isn't redirecting to theforce.net:  
Resistance.theforce.net isn’t redirecting to theforce.net because resistance.theforce.net isn’t listed.

Document what a corrected DNS record should be:

resistance.theforce.net canonical name = theforce.net  
[www.theforce.net](http://www.theforce.net) canonical name = theforce.net

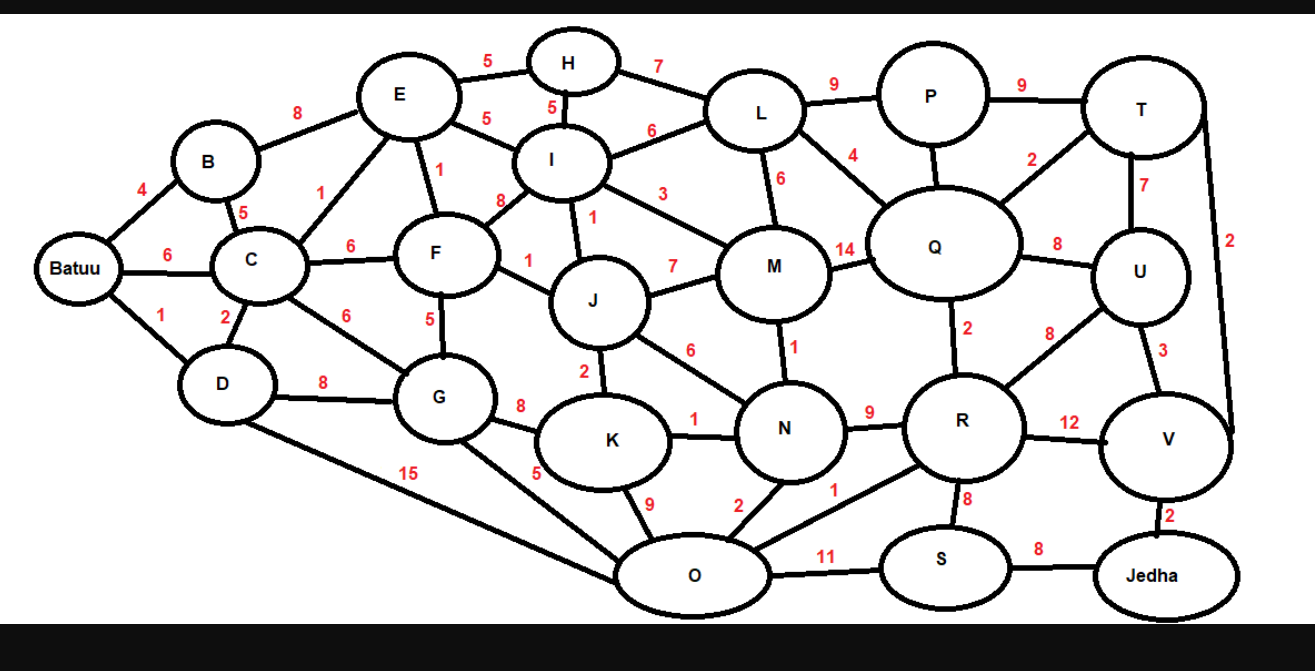
Mission 4:

Confirm the DNS records for princessleia.site:  


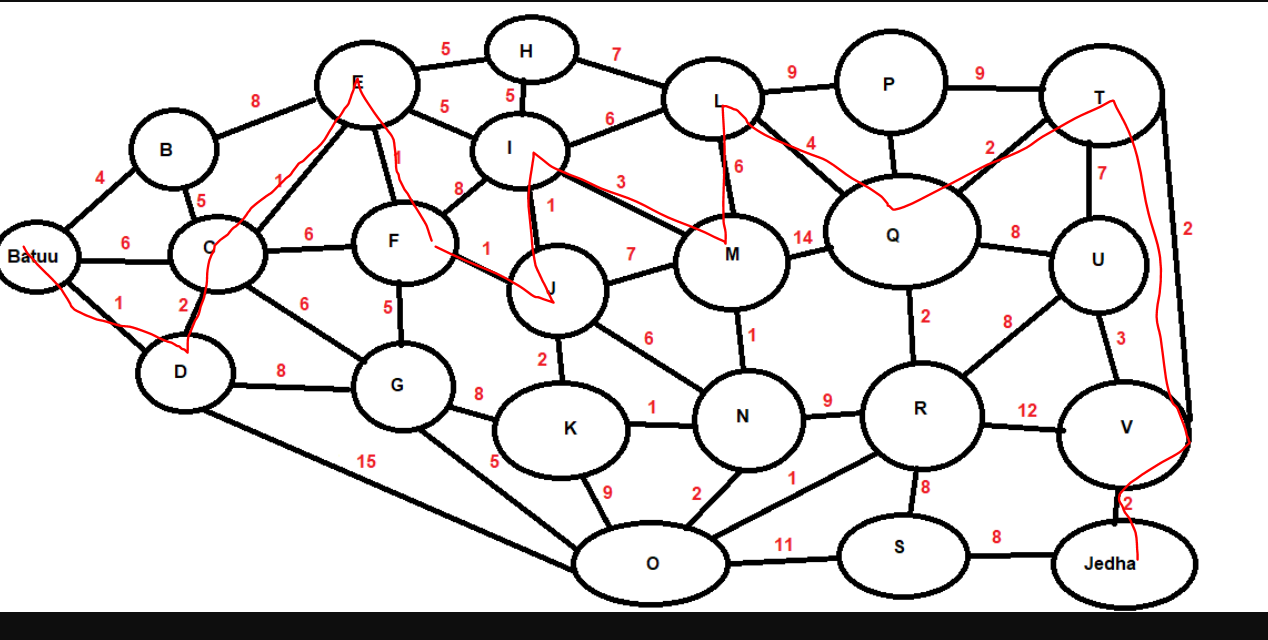
Document how you would fix the DNS record to prevent this issue from happening again:   
Update and add the following:  
Princessleia.site nameserver = ns2.galaxybackup.com

Mission 5:

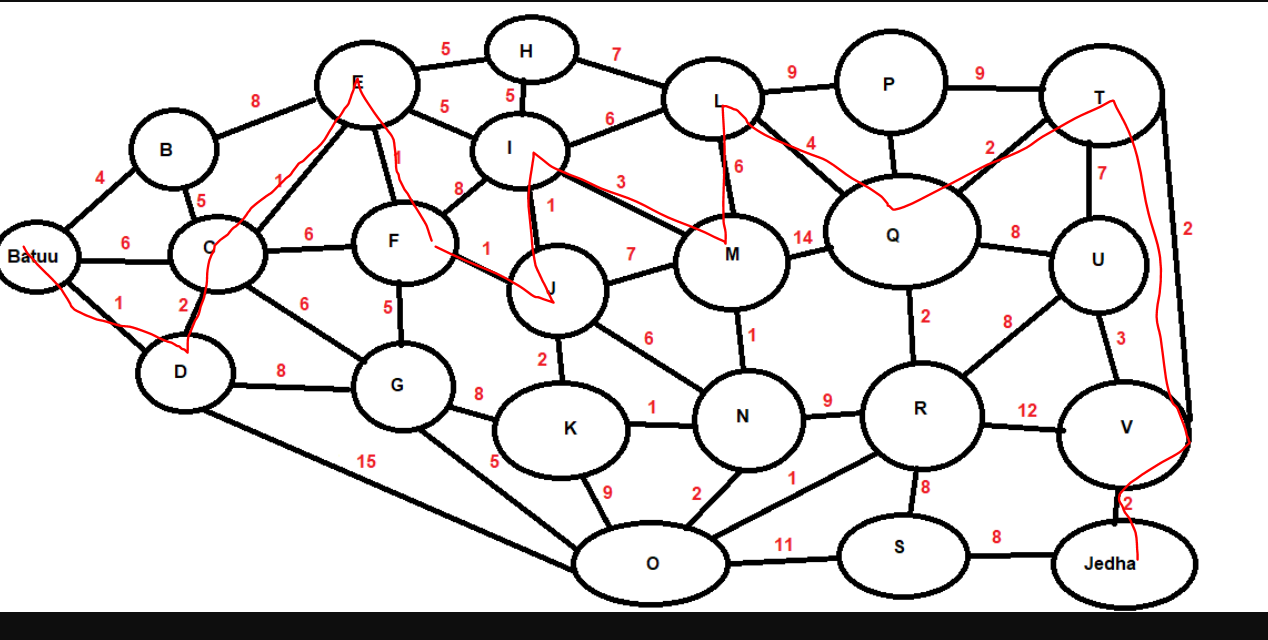
View the Galaxy Network Map and determine the OSPF shortest path from Batuu to Jedha:



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:



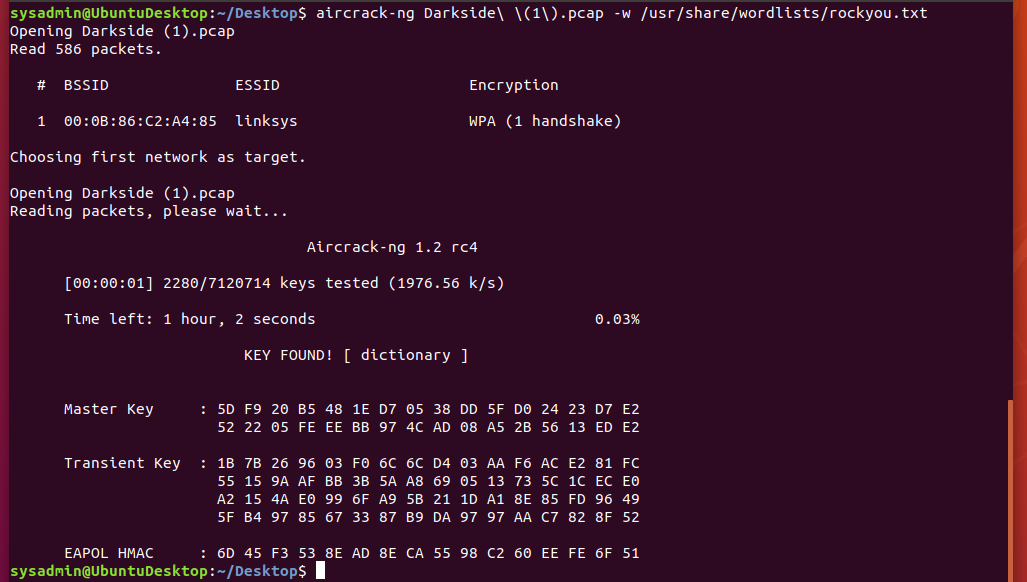
Mission 6:

Your Mission:

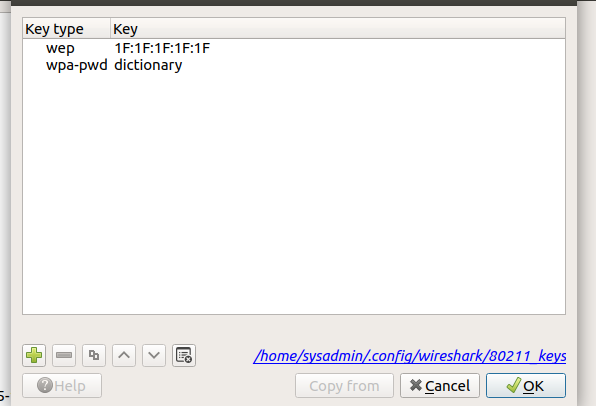
* Figure out the Dark Side's secret wireless key by using Aircrack-ng.  
    
   KEY FOUND! [ dictionary ]

5df920b5481ed70538dd5fd02423d7e2522205feeebb974cad08a52b5613ede2

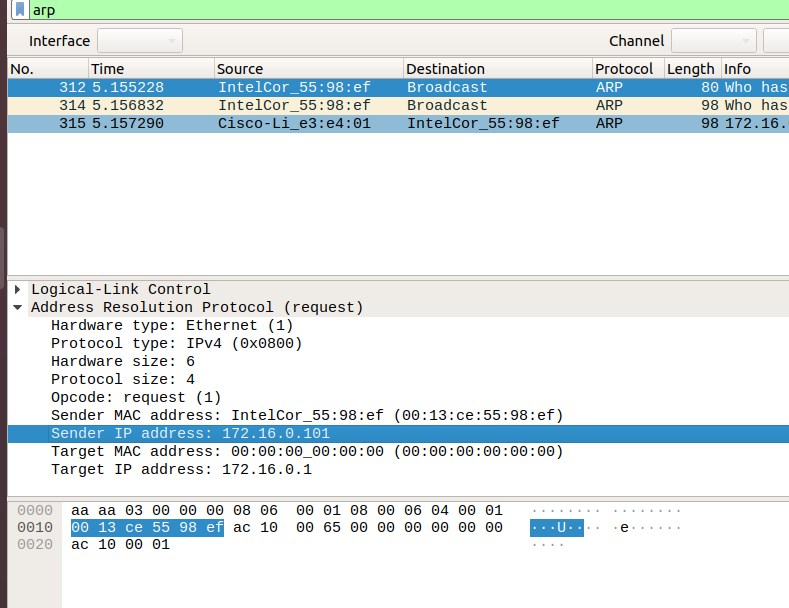
* + Hint: This is a more challenging encrypted wireless traffic using WPA.
  + In order to decrypt, you will need to use a wordlist (-w) such as rockyou.txt.



* Use the Dark Side's key to decrypt the wireless traffic in Wireshark.  
  + Hint: The format for the key to decrypt wireless is <Wireless\_key>:<SSID>

.

* 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.

MAC address: IntelCor\_55:98:ef (00:!3:ce:55:98:ef)

Ip address: arp.src.proto\_ipv4 == 172.16.0.101

Mission 7:

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.

