**Intel Report**

**The Resistance Corp.**

**HW 9.0 December 3, 2020**

### **PREPARED FOR**

**The Resistance Corp.**

**Milky Way Division**

### **PREPARED BY**

**Sean James**

**Network Jedi**

**December 3, 2020**

### **The Resistance**

### **Milky Way Galaxy Section**

**Re: Summary of Findings**

**The Sith Empire recently carried out a DoS attack, taking out the Resistance's core network infrastructure, including its DNS servers.  
This attack destroyed the Resistance's ability to communicate via email and retrieve other crucial information about each others' operations. The Empire has taken advantage of this compromised availability by ambushing numerous Resistance outposts, all vulnerable because they can no longer call for help.**

**The questions posed to me are high-lighted in BABY YODA’s favorite puke green color. With the following findings and recommendations, you can restore the Resistance's core DNS infrastructure. Thank you for allowing me to help!**

**Sean James**

**Network Jedi**

**The Resistance Corp.**

**450.555.555**

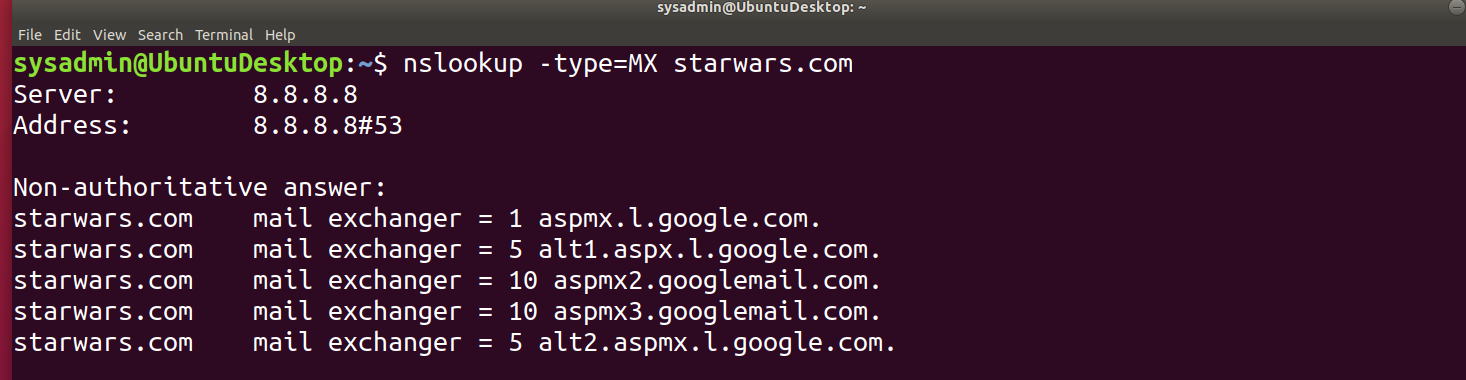
**Information Reported**

**The Sith Empire recently carried out a DoS attack, taking out the Resistance's core network infrastructure, including its DNS servers.**

**This attack destroyed the Resistance's ability to communicate via email and retrieve other crucial information about each other’s' operations. The Empire has taken advantage of this compromised availability by ambushing numerous Resistance outposts, all vulnerable because they can no longer call for help.**

**Mission 1**

**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.**

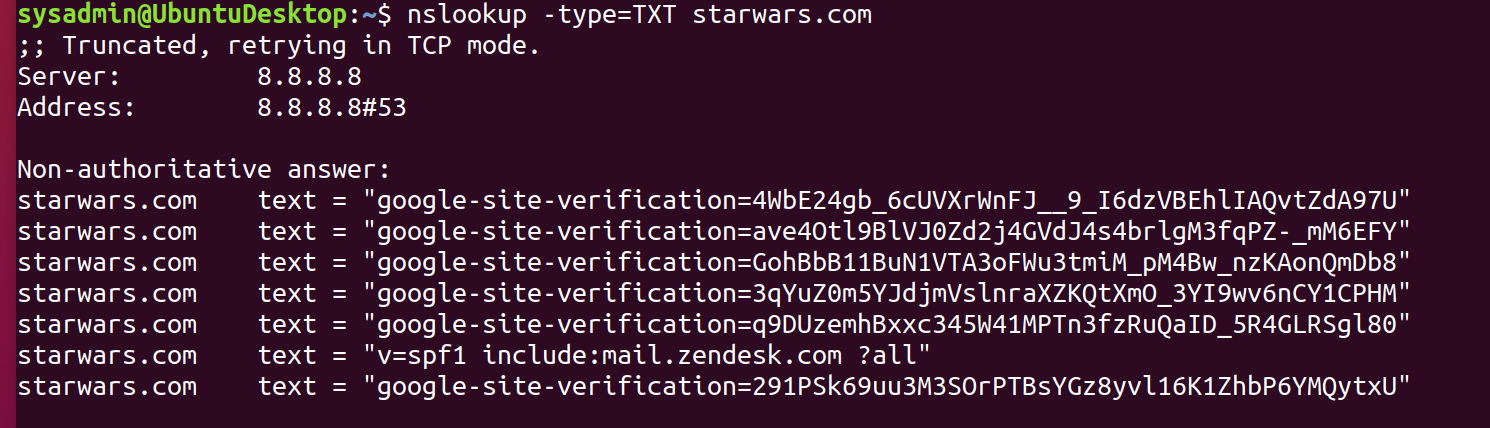


**The above screenshot was taken after I searched for the available email servers for starwars.com. I used <nslookup -type=MX starwars.com> to accomplish this. The results reveal (5) servers that are used for email exchange. They are used in order of the weight, or number to the right of the < = > sign. The lowest number is used first, with similar numbers used in a round-robin fashion.**

**The new servers that The Resistance has created need to be added, and the firewall settings should be adjusted and enabled to keep ports secured. The corrected DNS record should be something like:**

**< starwars.com mail exchanger = 1 asltx.l.google.com >**

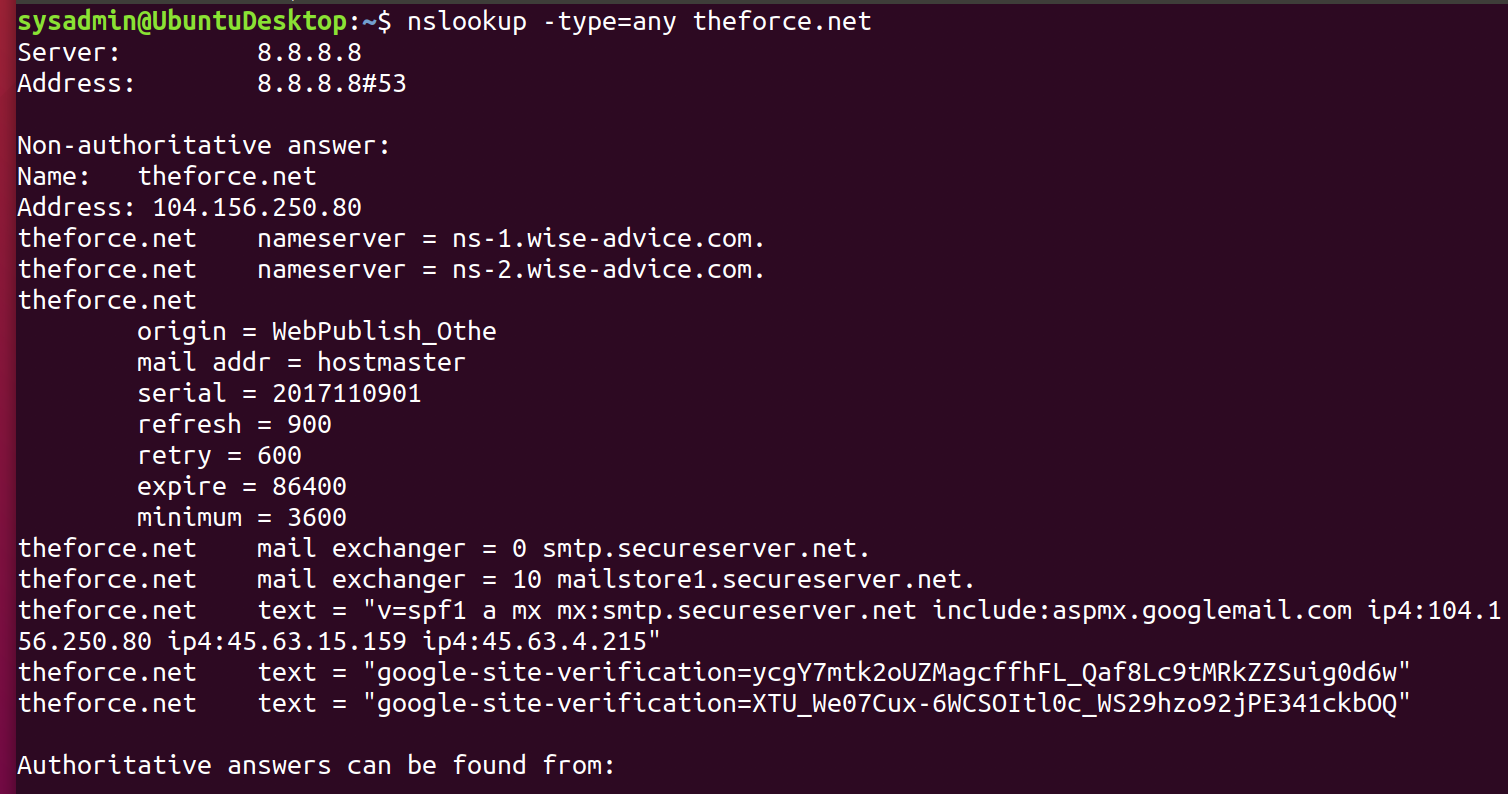
**< starwars.com mail exchanger = 5 asltx.2.google.com >**

****

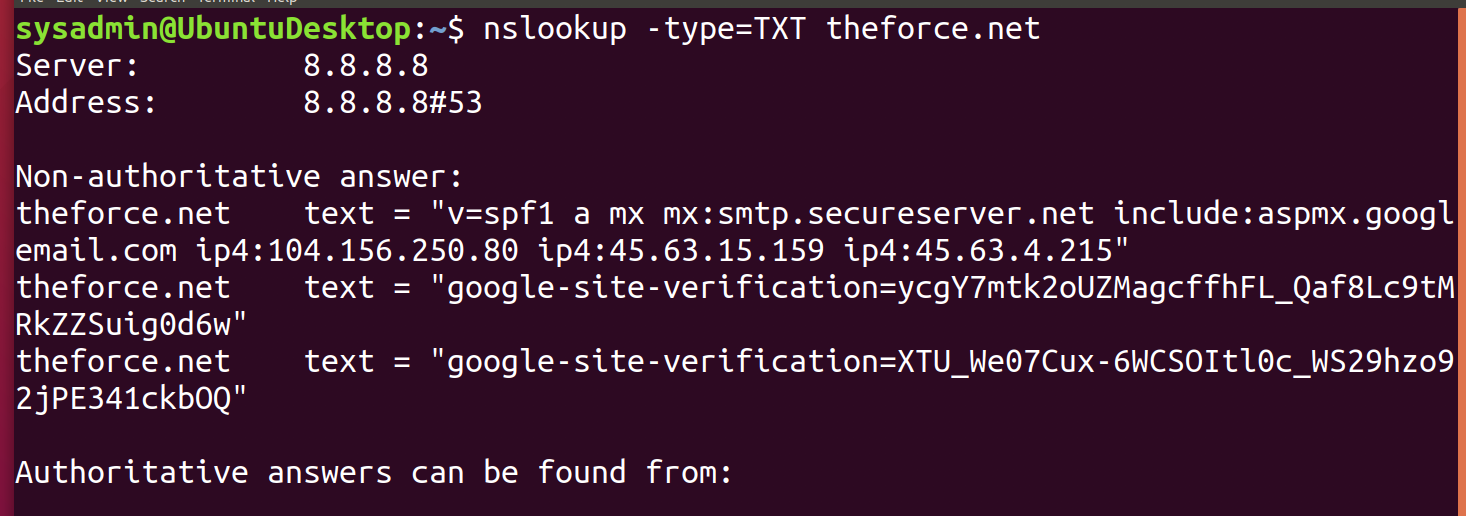
**Also, I was able to see the SPF re-routing location as pictured above.**

**Mission 2**

**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.**

****

**I initially used the -type=SPF and did not receive results. I then used the more generic -type=any and received a list of the servers that The Force uses. That uncovered the SPF file from within and the two Resistance mail servers that are being controlled by The Force.**

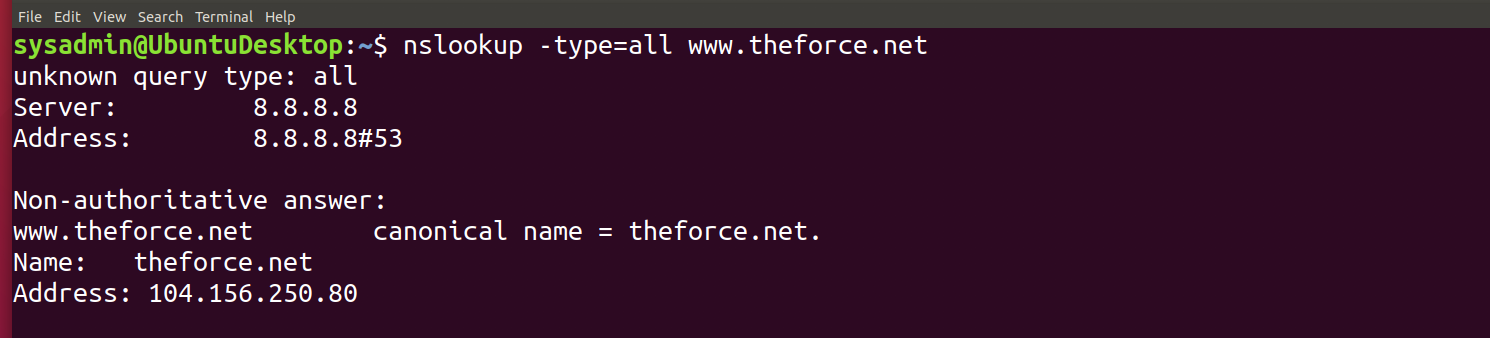
****

**According to the SPF record above, the IP address of <45.23.176.21> is not listed. Therefore, the emails are going to go to spam. This IP address needs to be added to the SPF record for it to work correctly. It should appear as:**

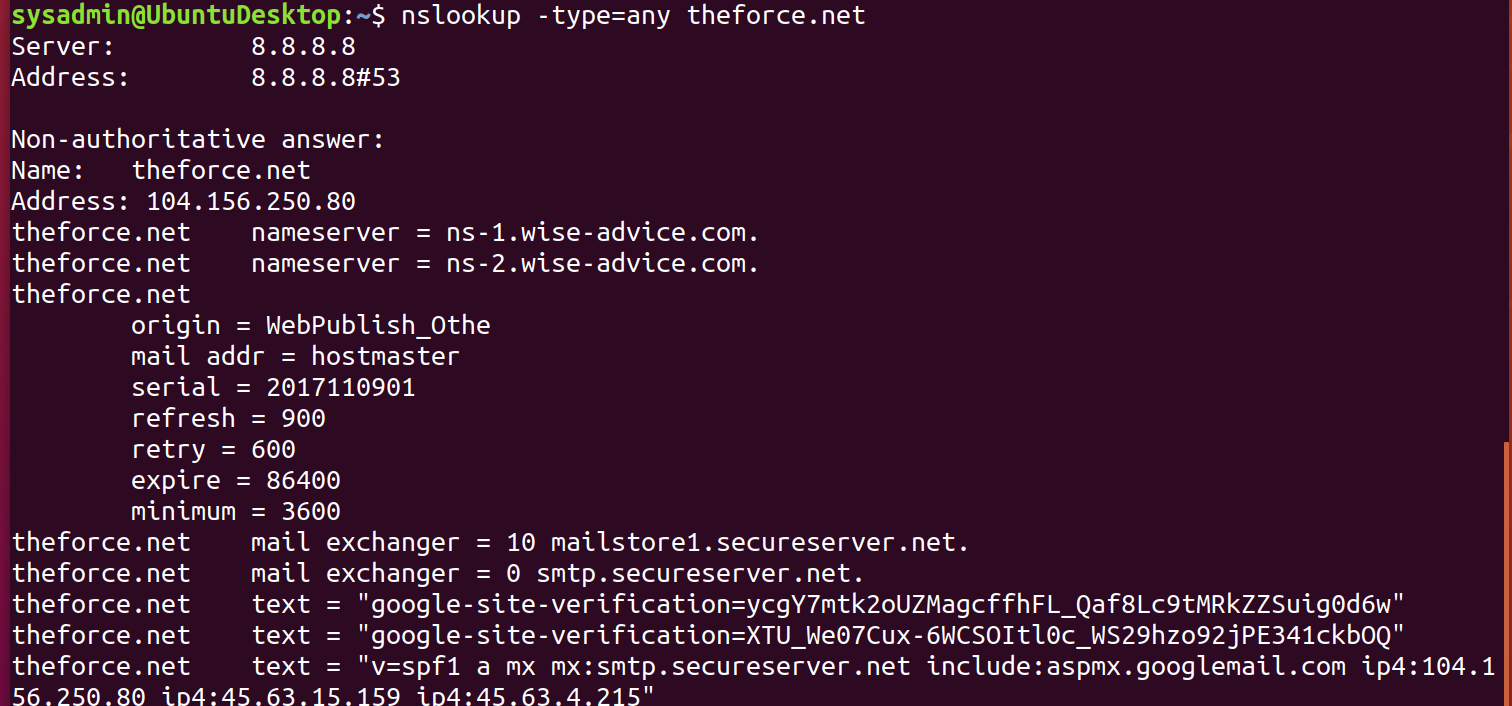
**theforce.net text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215 ip4:45.23.176.21"**

**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.  
Document what a corrected DNS record should be.**



**The CNAME, or canonical name can be verified by using the above search of <nslookup -type=all www.theforce.net>.**



**The reason that the subpage <resistance.theforce.net> is not redirecting to <theforce.net> is due to the DNS record is not a valid domain, and it is not within the SPF record. I suggest that the domain name and IP be created and redirected with a CNAME entry. A corrected version of this would look like:**

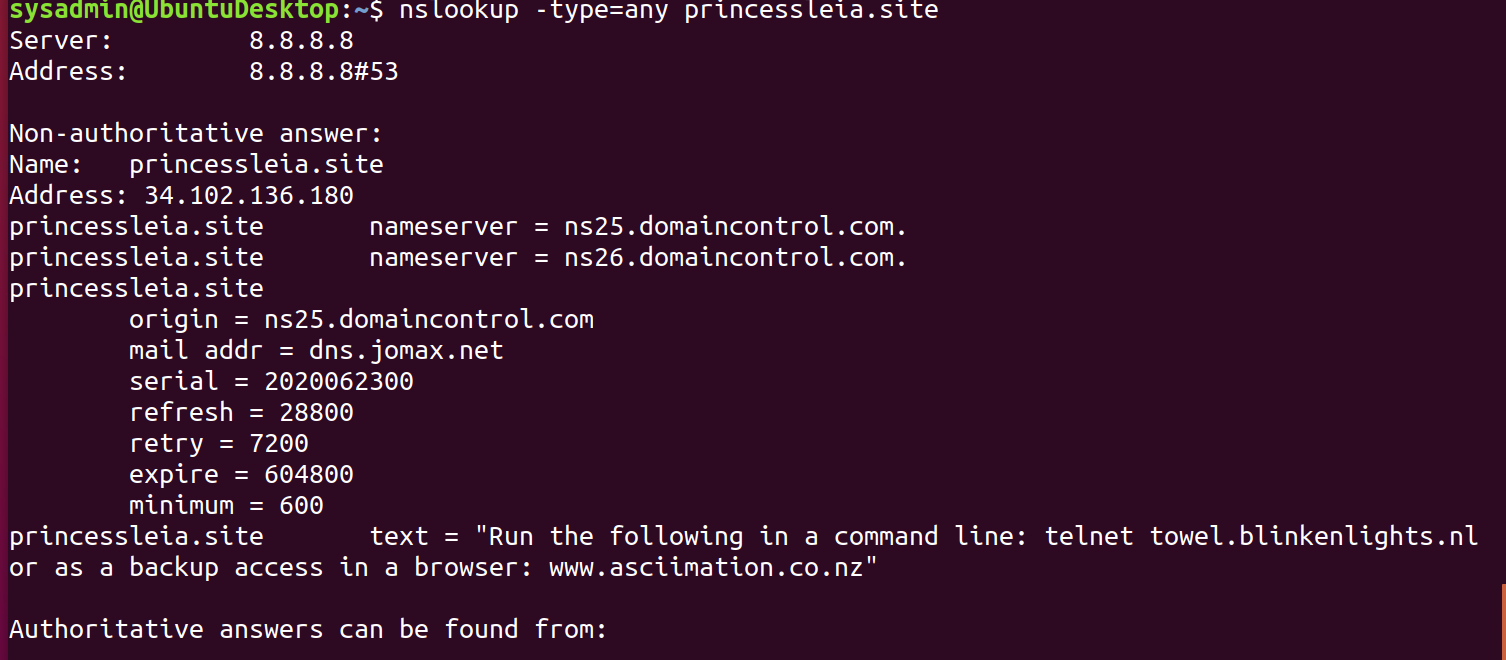
**Non-authoritative answer:**

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

**Name: resistance.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.**



**I was able to confirm the DNS records for the <princessleia.site> domain name as noted above. The backup server <ns2.galaxybackup.com> should be added to the nameserver list. It should appear as the following entry:**

**<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.**

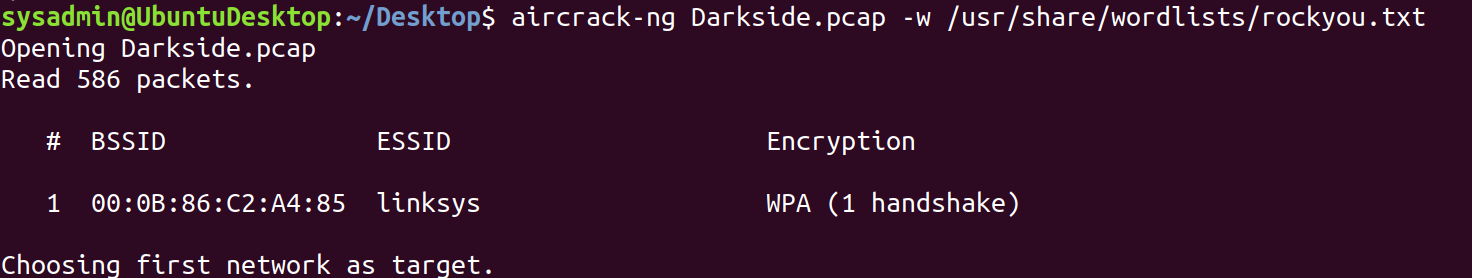
**Document this shortest path so it can be used by the Resistance to develop a static route to improve the traffic.**

**The shortest path from Batuu to Jedha without passing through planet N is the following sequence: Batuu >DCEFJILQTV> Jedha = 23**

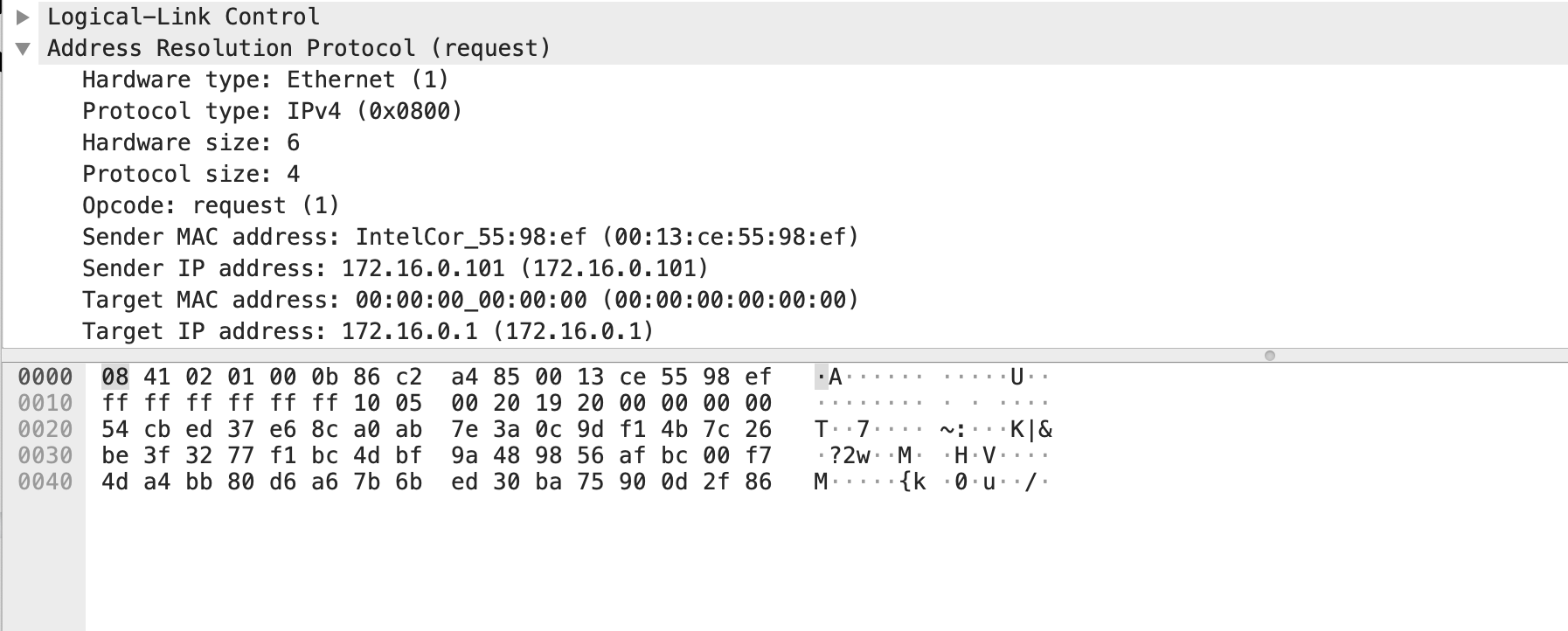
**Mission 6**

**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.  
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.**



**I ran the above <aircrack-ng Darkside.pcap -w /usr/share/wordlists/rockyou.txt> to gain the key of <dictionary>**

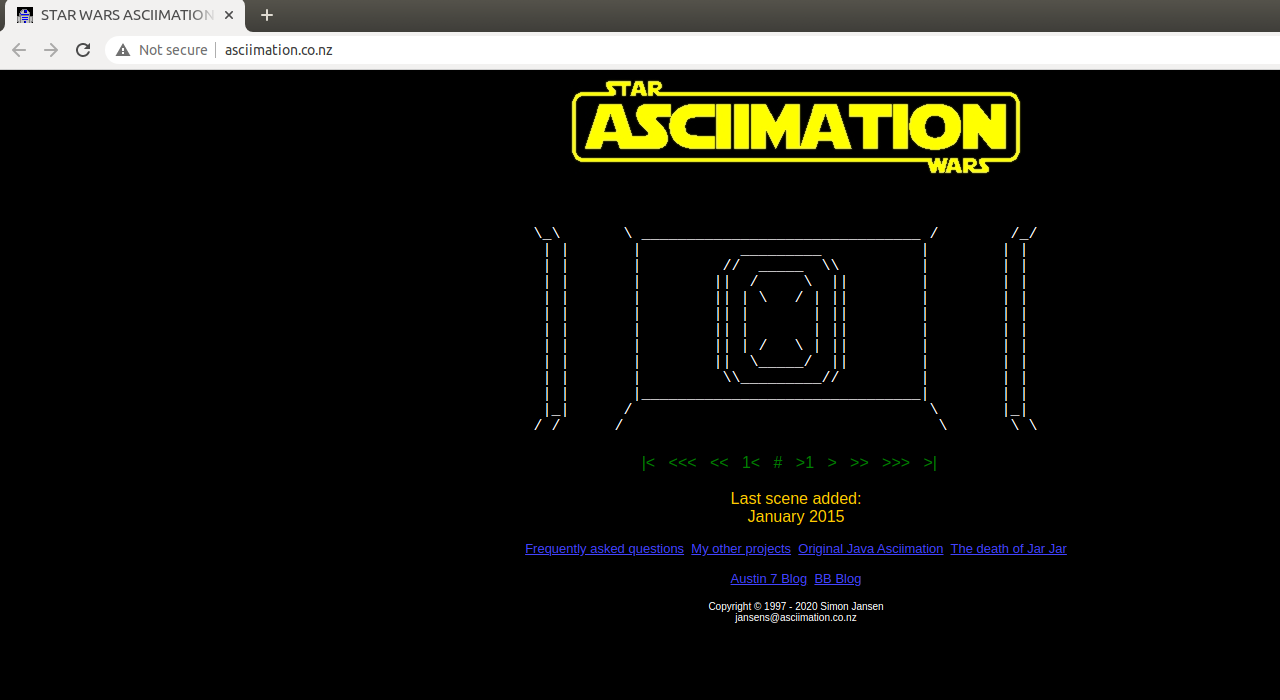


**Once that was gained, I changed the settings within Wireshark under preferences>Protocols>IEEE 802.11 to allow for the key to be added of <dictionary:linksys>. I then filtered ARP traffic within Wireshark and mined down into the Address Resolution Protocol to see the host IP and MAC address as pictured above. The sender MAC address <InterCor\_55:98:ef (00:13:ce:55:98:ef)> and IP Address <172.16.0.101 (172.16.0.101)> were captured.**

**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. 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.**

****

**The above is the screenshot taken from the link given in Mission 4.**