**Networking Project**

**Phase 1**: *"I'd like to Teach the World to Ping"*

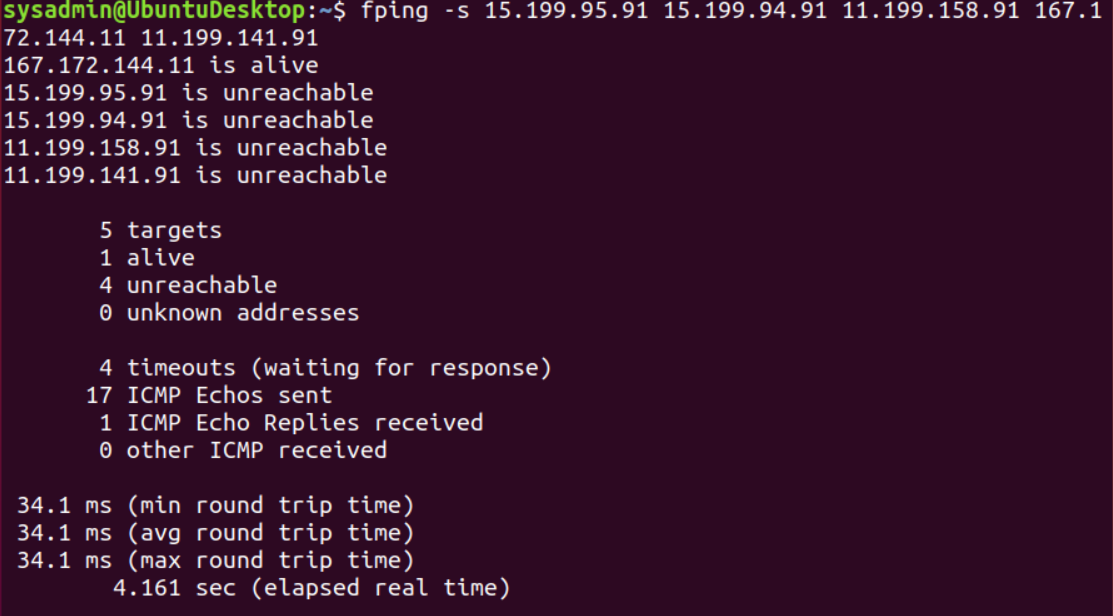
You have been provided a list of network assets belonging to RockStar Corp. Use fping to ping the network assets for only the Hollywood office.

* Determine the IPs for the Hollywood office and run fping against the IP ranges in order to determine which IP is accepting connections.

I used the following command to run fping for the Hollywood office IPs:

**fping -s 15.199.95.91 15.199.94.91 11.199.158.91 167.172.144.11 11.199.141.91**

* Create a summary file in a word document that lists out the fping command used, as well as a summary of the results.



* Your summary should determine which IPs are accepting connections: **167.172.144.11 is alive**

The following IPs are not accepting connections:

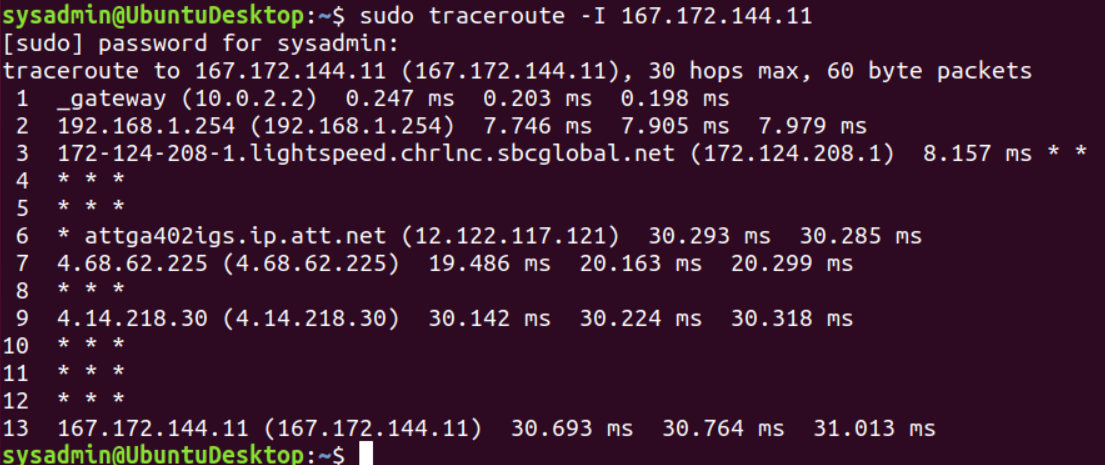
**15.199.95.91 is unreachable**

**15.199.94.91 is unreachable**

**11.199.158.91 is unreachable**

**11.199.141.91 is unreachable**

* Recommend to restrict allowing ICMP echo requests against IP **167.172.144.11**  to prevent successful responses from PING requests.



**Mitigations:**

Most ICMP attacks can be effectively reduced by deploying Firewalls at critical locations of a network to filter un-wanted traffic and from any destinations.

In addition, to keep a reasonable balance between services and security, you should configure your ICMP parameters in your network devices as follows:

Allow ping ICMP Echo-Request outbound and Echo-Reply messages inbound.

Allow traceroute TTL-Exceeded and Port-Unreachable messages inbound.

Allow path MTU ICMP Fragmentation-DF-Set messages inbound.

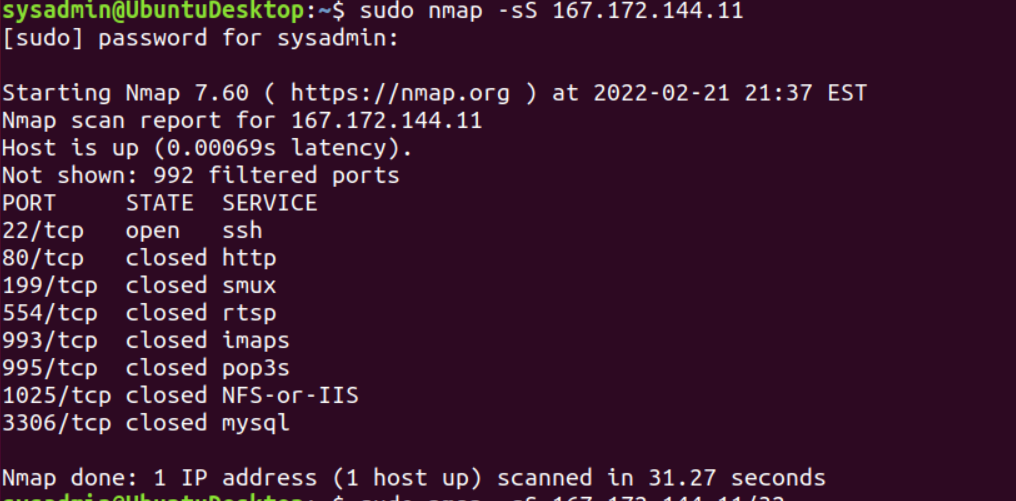
Blocking other types of ICMP traffic.

Source: *networkmitigations.blogspot.com*

* This occured on the network layer (layer 3) as Ping uses IP addresses and IPs are used on the Network Layer (layer 3)..

**Phase 2**: *"Some Syn for Nothin`"*

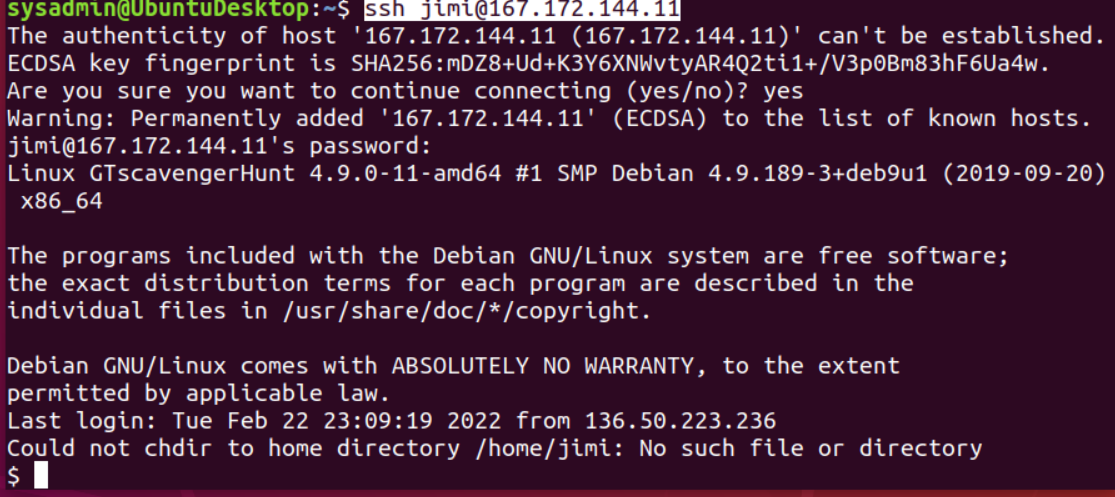
* **Command to run a SYN SCAN is: sudo nmap -sS 167.172.144.11**

****

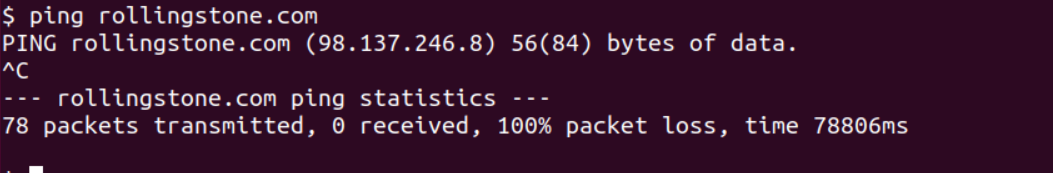
* The results show the port number TCP / UDP , the state of the port, and the service / protocol for the ports that are either open or filtered (stopped by a firewall): **port 22/tcp is open**
* The OSI layer is: **Transport (layer 4). Layer 4 key protocols include TCP in which port 22 is a tcp**.

**Phase 3: *"I Feel a DNS Change Comin' On"***

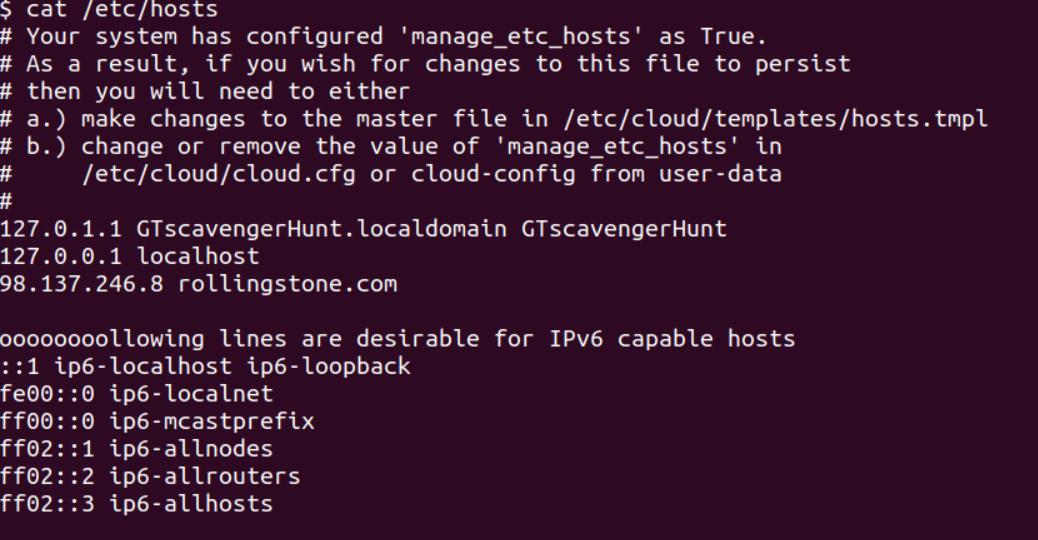
* Login: **ssh jimi@167.172.144.11**



* **Ping rollingstone.com**



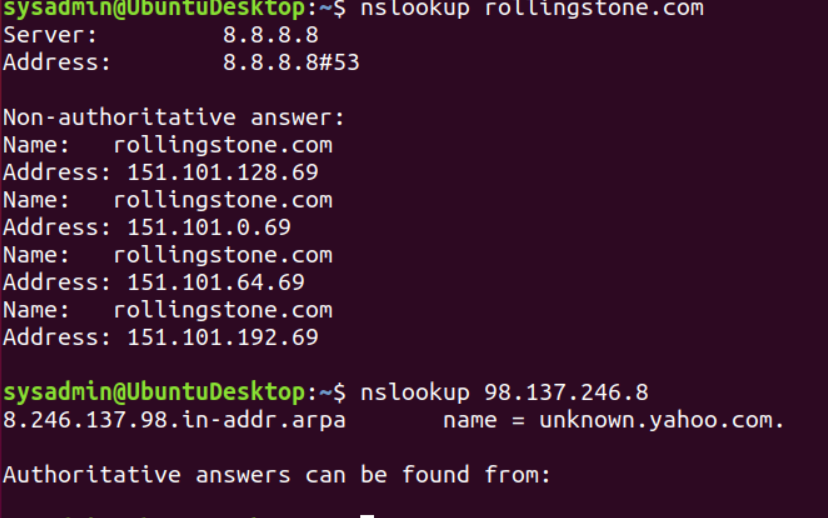
* **Cat /etc/hosts to check for any configurations. The IP address for rollingstone.com came up as 98.137.246.8.**

****

* Used the following commands: **nslookup rollingstone.com.** Then I tried

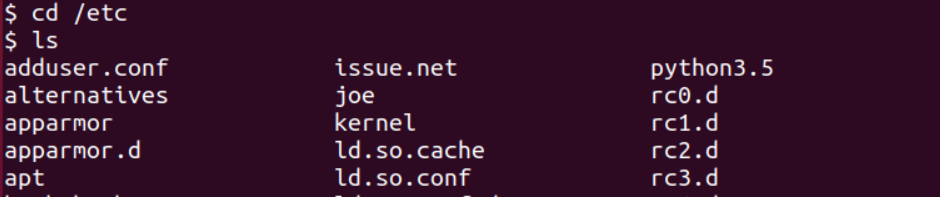
**nslookup 98.137.246.8**

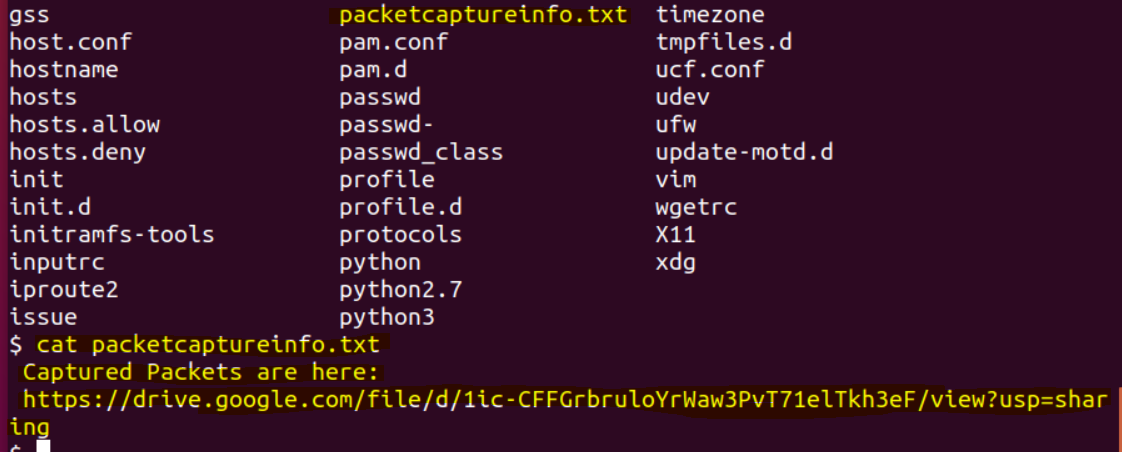
* The OSI layer: **Application (layer 7). Port 53 is DNS - For translating domains to IP addresses**.



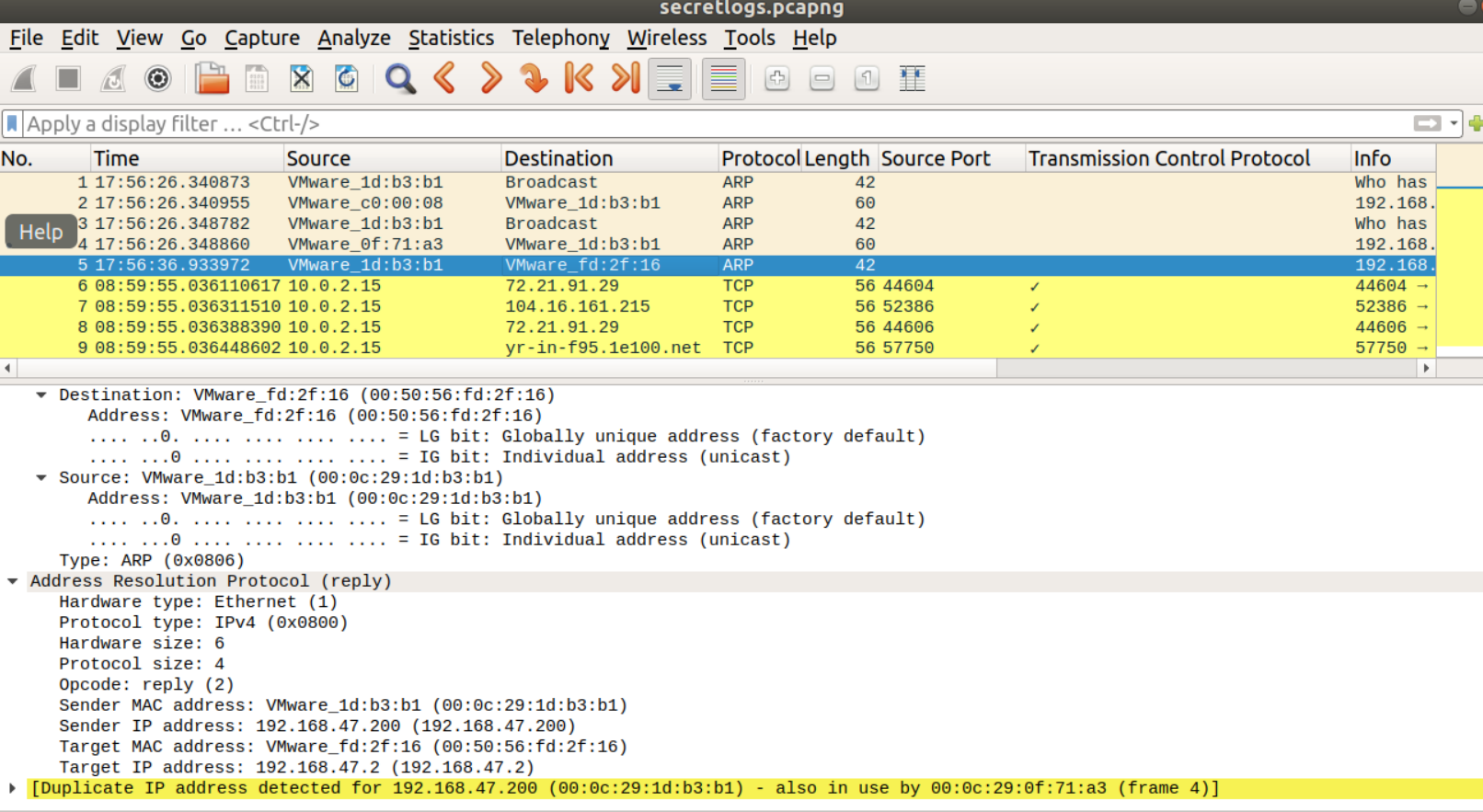
**Phase 4: "ShARP Dressed Man"**

* Login:  **ssh jimi@167.172.144.11**
* Then **cd /etc**
* **$ ls**

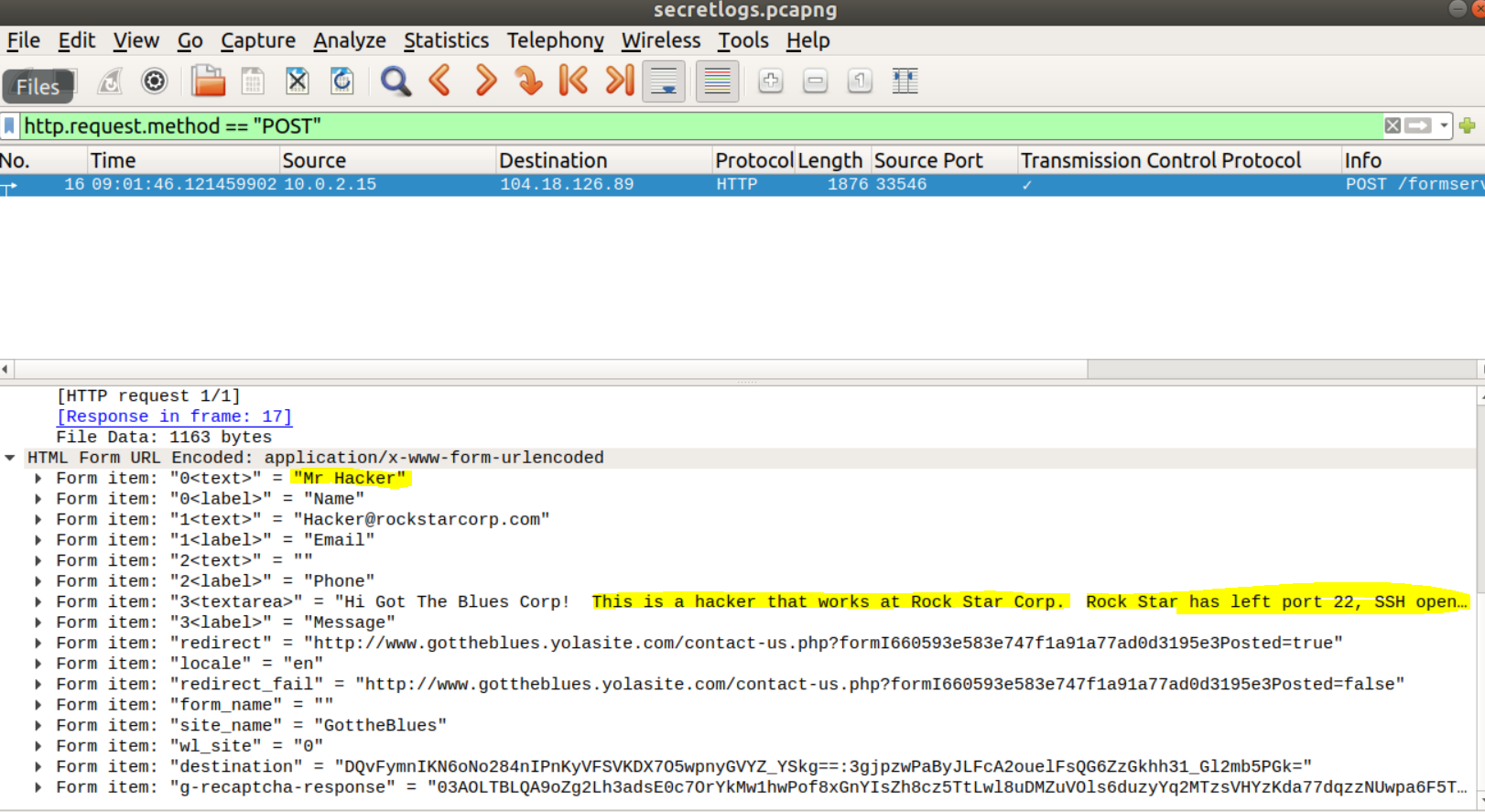




* The file left by the hacker is **packetcaptureinfo.txt.**
* Then I **cat packetcaptureinfo.txt.**
* Then I copied the link: [**https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing**](https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing) into Firefox web browser and discovered **secretlogs.pcapng** file.
* I opened **secretlongs**.pcapng using Wireshark.
* As I reviewed the traffic, I noticed in #5, the hacker interjected and duplicated the IP address and in #4 changed the MAC address. As shown below in the snippet—

****

* When I inputed the filter: http/request.method == “POST” I was able to see an email that stated the hacker workers for Rock Star Corp and informed that port 22 ssh is open.
* **This occured on the application layer (layer 7) as the input on the website is used on the Application Layer 7.**

****