Phase #1

- **fping -s** command was used to determine availability of IP connection ranges of 15.199.95.91, 15.199.94.91, 11.199.158.91, 167.172.144.11, and 11.199.141.91.

- **15.199.95.91 is unreachable**

```
   1 targets
   0 alive
   1 unreachable
   0 unknown addresses
   1 timeouts (waiting for response)
   4 ICMP Echos sent
   0 ICMP Echo Replies received
   0 other ICMP received
0.00 ms (min round trip time)
0.00 ms (avg round trip time)
0.00 ms (max round trip time)
    4.079 sec (elapsed real time)
```

- **15.199.94.91 is unreachable**

```
   1 targets
   0 alive
   1 unreachable
   0 unknown addresses
   1 timeouts (waiting for response)
   4 ICMP Echos sent
   0 ICMP Echo Replies received
   0 other ICMP received
0.00 ms (min round trip time)
0.00 ms (avg round trip time)
0.00 ms (max round trip time)
    4.144 sec (elapsed real time)
```

- **11.199.158.91 is unreachable**

```
   1 targets
   0 alive
   1 unreachable
```

```
       0 unknown addresses
       1 timeouts (waiting for response)
       4 ICMP Echos sent
       0 ICMP Echo Replies received
       0 other ICMP received
    0.00 ms (min round trip time)
    0.00 ms (avg round trip time)
    0.00 ms (max round trip time)
        4.078 sec (elapsed real time)
```

- **167.172.144.11 is alive**

```
       1 targets
       1 alive
       0 unreachable
       0 unknown addresses
       0 timeouts (waiting for response)
       1 ICMP Echos sent
       1 ICMP Echo Replies received
       0 other ICMP received
    41.8 ms (min round trip time)
    41.8 ms (avg round trip time)
    41.8 ms (max round trip time)
        0.042 sec (elapsed real time)
```

- **11.199.141.91 is unreachable**

```
       1 targets
       0 alive
       1 unreachable
       0 unknown addresses
       1 timeouts (waiting for response)
       4 ICMP Echos sent
       0 ICMP Echo Replies received
       0 other ICMP received
    0.00 ms (min round trip time)
    0.00 ms (avg round trip time)
    0.00 ms (max round trip time)
        4.097 sec (elapsed real time)
```

- Test determined that 167.172.144.11 is alive making it a possible vulnerability.

- Recommend to restrict allowing ICMP echo requests to 167.172.144.11 to prevent successful responses from ping requests as full disabling may cause networking issues.

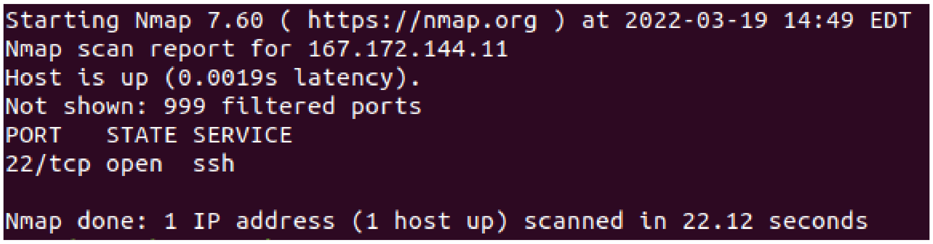
- **sudo traceroute -I**

```
“traceroute to 167.172.144.11 (167.172.144.11), 30 hops max, 60 byte packets.”
1  _gateway (10.0.2.2)  0.217 ms  0.263 ms  0.259 ms
 2  192.168.254.254 (192.168.254.254)  4.447 ms  4.464 ms  4.555 ms
 3  h2.84.134.40.dynamic.ip.windstream.net (40.134.84.2)  14.179 ms  14.273 ms  15.931 ms
 4  ae1-0.agr02.cmrc01-ga.us.windstream.net (40.128.251.102)  15.965 ms  16.011 ms  16.233 ms
 5  * * *
 6  * * *
 7  ae5.cr02.asbn07-va.us.windstream.net (40.132.59.34)  33.836 ms  33.297 ms  33.415 ms
 8  ae21-0.cr01.nycm01-ny.us.windstream.net (169.130.193.206)  40.366 ms  40.390 ms  41.060 ms
 9  ae10-0.cr02.nycm01-ny.us.windstream.net (40.129.35.249)  40.416 ms  40.597 ms  41.065 ms
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  167.172.144.11 (167.172.144.11)  41.560 ms  41.540 ms  40.132 ms
```

- This occurred on the network layer as PING uses IP addresses and IPs are used on **Network Layer 3.**

Phase #2

- **sudo nmap -sS 167.172.144.11**



```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-19 14:49 EDT
Nmap scan report for 167.172.144.11
Host is up (0.0019s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 22.12 seconds
```

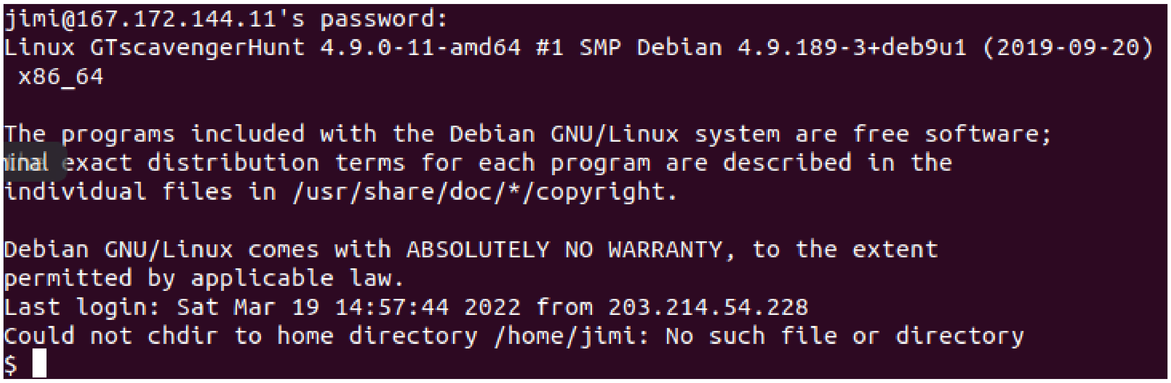
- Recommend closing of any unused ports and adjusting any firewalls in place to allow only specific transmission protocols.

- Port 22 is an open connection.

- This occurred on the transport layer as SYN uses TCP which is connection based on **Transport Layer 4**.

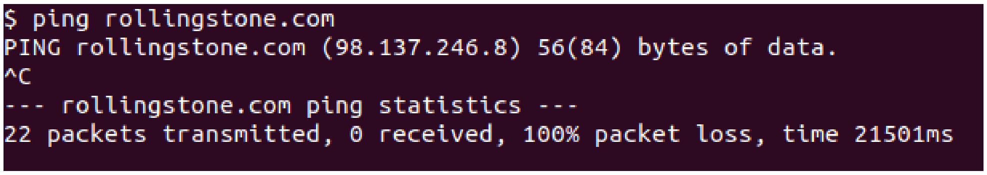
Phase #3

- **ssh jimi@167.172.144.11 -22**



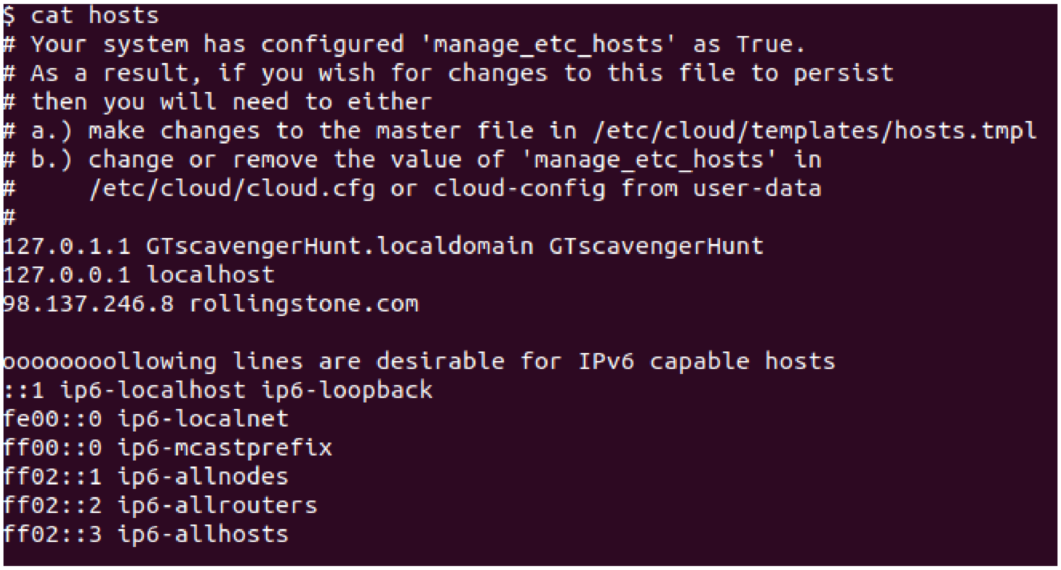
```
jimi@167.172.144.11's password:
Linux GTscavengerHunt 4.9.0-11-amd64 #1 SMP Debian 4.9.189-3+deb9u1 (2019-09-20)
 x86_64

The programs included with the Debian GNU/Linux system are free software;
inal exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Mar 19 14:57:44 2022 from 203.214.54.228
Could not chdir to home directory /home/jimi: No such file or directory
$ 
```

- **ping** rollingstone.com.



```
$ ping rollingstone.com
PING rollingstone.com (98.137.246.8) 56(84) bytes of data.
^C
--- rollingstone.com ping statistics ---
22 packets transmitted, 0 received, 100% packet loss, time 21501ms
```

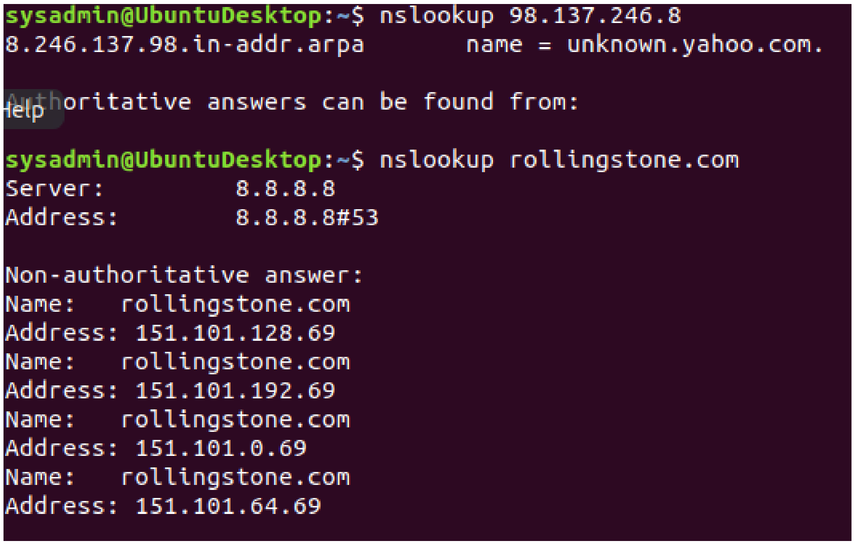
- **cd** etc folder then **cat** the hosts file to see any changes to configuration.



```
$ cat hosts
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
#     /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt
127.0.0.1 localhost
98.137.246.8 rollingstone.com

ooooooooollowing lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

- **Ctrl + D** out of the ssh then applied the 98.137.246.8 rollingstone.com to nslookup.

- **nslookup** 98.137.246.8



```
sysadmin@UbuntuDesktop:~$ nslookup 98.137.246.8
8.246.137.98.in-addr.arpa       name = unknown.yahoo.com.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$ nslookup rollingstone.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   rollingstone.com
Address: 151.101.128.69
Name:   rollingstone.com
Address: 151.101.192.69
Name:   rollingstone.com
Address: 151.101.0.69
Name:   rollingstone.com
Address: 151.101.64.69
```

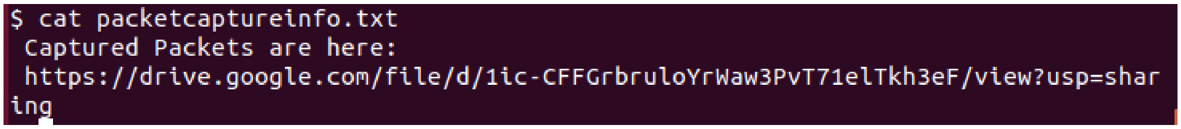
- Would recommend restricting critical access to domain/name servers as to prevent spoofing of addresses. Additional measures put in place as well to prevent cache poisoning if compromised.

- This occurs on the **Application Layer 7** of the OSI model as DNS and HTTP run side by side.

PHASE #4

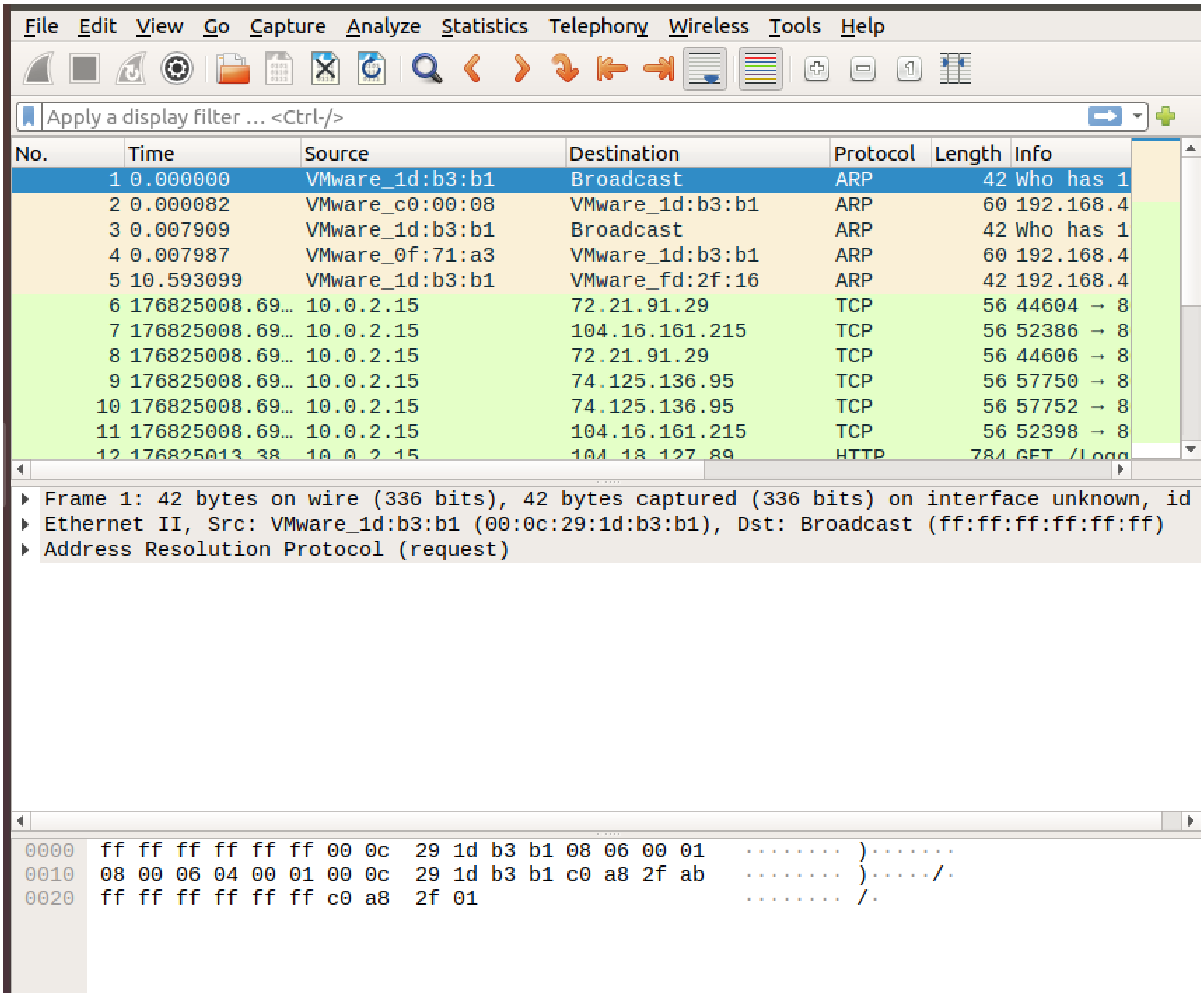
The file, like the hosts config, was also within the etc folder titled ***packetcaptureinfo.txt.***

- **cat** *packetcaptureinfo.txt.*



```
$ cat packetcaptureinfo.txt
 Captured Packets are here:
 https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=shar
ing
```

- Use the link above to open with Wireshark.

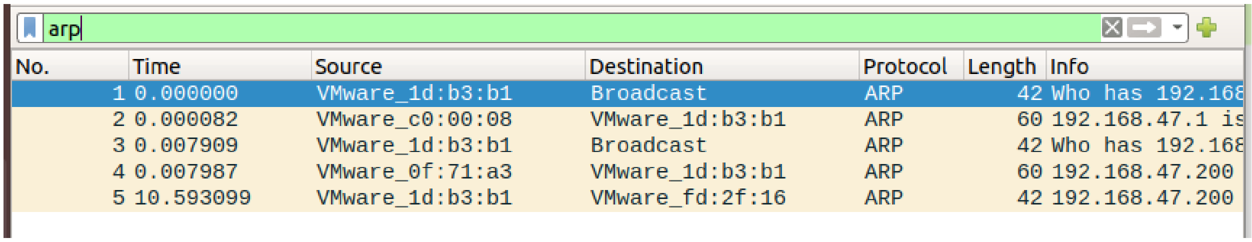

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	VMware_1d:b3:b1	Broadcast	ARP	42	Who has 1
2	0.000082	VMware_c0:00:08	VMware_1d:b3:b1	ARP	60	192.168.4
3	0.007909	VMware_1d:b3:b1	Broadcast	ARP	42	Who has 1
4	0.007987	VMware_0f:71:a3	VMware_1d:b3:b1	ARP	60	192.168.4
5	10.593099	VMware_1d:b3:b1	VMware_fd:2f:16	ARP	42	192.168.4
6	176825008.69…	10.0.2.15	72.21.91.29	TCP	56	44604 → 8
7	176825008.69…	10.0.2.15	104.16.161.215	TCP	56	52386 → 8
8	176825008.69…	10.0.2.15	72.21.91.29	TCP	56	44606 → 8
9	176825008.69…	10.0.2.15	74.125.136.95	TCP	56	57750 → 8
10	176825008.69…	10.0.2.15	74.125.136.95	TCP	56	57752 → 8
11	176825008.69…	10.0.2.15	104.16.161.215	TCP	56	52398 → 8
12	176825013.38	10.0.2.15	104.18.127.89	HTTP	784	GET /Logg

```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id
▸ Ethernet II, Src: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)
```

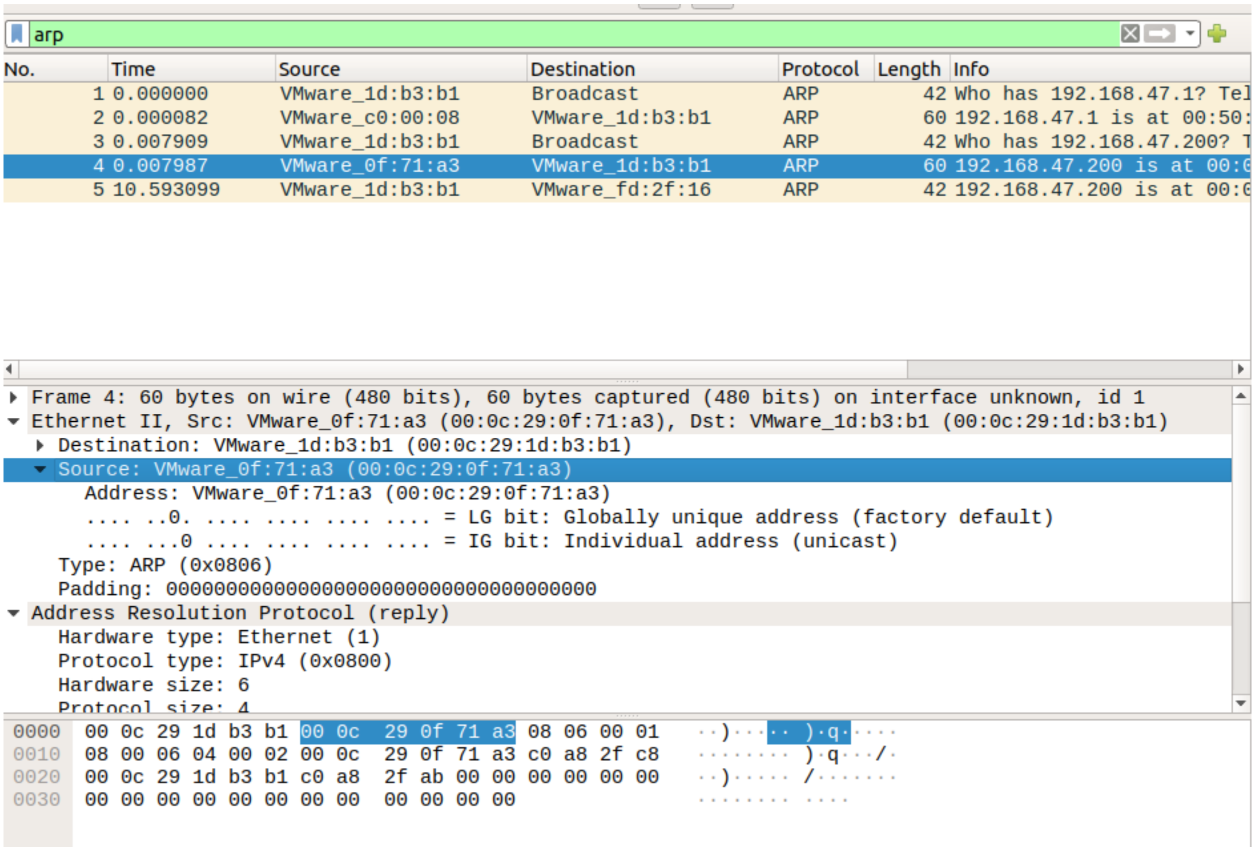
```
0000  ff ff ff ff ff ff 00 0c  29 1d b3 b1 08 06 00 01   ········ )·······
0010  08 00 06 04 00 01 00 0c  29 1d b3 b1 c0 a8 2f ab   ········ )·····/·
0020  ff ff ff ff ff ff c0 a8  2f 01                     ········ /·
```

- Filter the ARP.



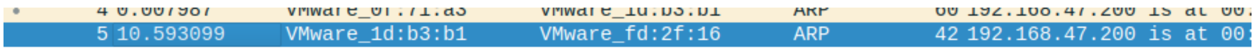
```
arp
No.  Time       Source             Destination        Protocol Length Info
   1 0.000000   VMware_1d:b3:b1    Broadcast          ARP          42 Who has 192.168
   2 0.000082   VMware_c0:00:08    VMware_1d:b3:b1    ARP          60 192.168.47.1 is
   3 0.007909   VMware_1d:b3:b1    Broadcast          ARP          42 Who has 192.168
   4 0.007987   VMware_0f:71:a3    VMware_1d:b3:b1    ARP          60 192.168.47.200
   5 10.593099  VMware_1d:b3:b1    VMware_fd:2f:16    ARP          42 192.168.47.200
```

- With the ARP filtered you can see the *192.168.47.1* request on line 1 matches the given MAC address of *00:0c:29:0f:71:a3* that is on line 4.

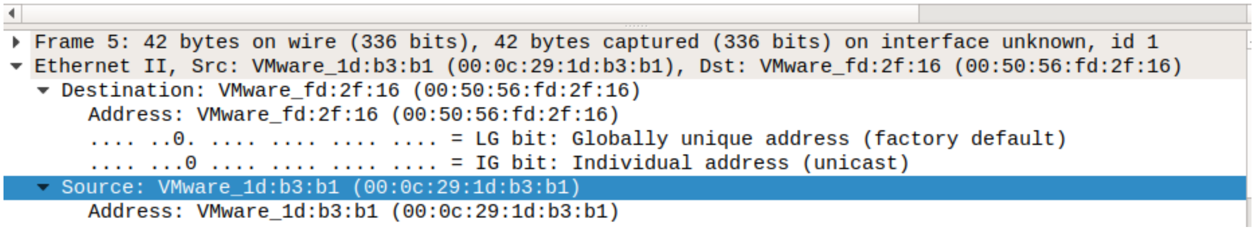


```
arp
No.  Time       Source             Destination        Protocol Length Info
   1 0.000000   VMware_1d:b3:b1    Broadcast          ARP          42 Who has 192.168.47.1? Tel
   2 0.000082   VMware_c0:00:08    VMware_1d:b3:b1    ARP          60 192.168.47.1 is at 00:50:
   3 0.007909   VMware_1d:b3:b1    Broadcast          ARP          42 Who has 192.168.47.200? T
   4 0.007987   VMware_0f:71:a3    VMware_1d:b3:b1    ARP          60 192.168.47.200 is at 00:0
   5 10.593099  VMware_1d:b3:b1    VMware_fd:2f:16    ARP          42 192.168.47.200 is at 00:0

▸ Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface unknown, id 1
▾ Ethernet II, Src: VMware_0f:71:a3 (00:0c:29:0f:71:a3), Dst: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)
  ▸ Destination: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)
  ▾ Source: VMware_0f:71:a3 (00:0c:29:0f:71:a3)
      Address: VMware_0f:71:a3 (00:0c:29:0f:71:a3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4

0000  00 0c 29 1d b3 b1 00 0c  29 0f 71 a3 08 06 00 01   ··)····· )·q·····
0010  08 00 06 04 00 02 00 0c  29 0f 71 a3 c0 a8 2f c8   ········ )·q···/·
0020  00 0c 29 1d b3 b1 c0 a8  2f ab 00 00 00 00 00 00   ··)····· /·······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

- But, on line 5 you will see that an adversary has provided a poisoned MAC address of *00:0c:29:1d:b3:b1* which is used to gain access.



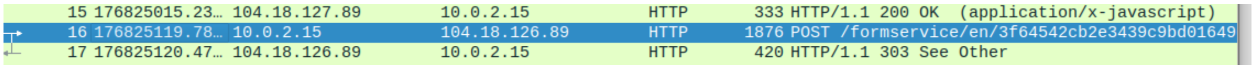
```
    4 0.007987     VMware_0f:71:a3    VMware_1d:b3:b1    ARP        60 192.168.47.200 is at 00:
    5 10.593099    VMware_1d:b3:b1    VMware_fd:2f:16    ARP        42 192.168.47.200 is at 00:
```



```
▸ Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id 1
▾ Ethernet II, Src: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1), Dst: VMware_fd:2f:16 (00:50:56:fd:2f:16)
  ▾ Destination: VMware_fd:2f:16 (00:50:56:fd:2f:16)
      Address: VMware_fd:2f:16 (00:50:56:fd:2f:16)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)
      Address: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)
```

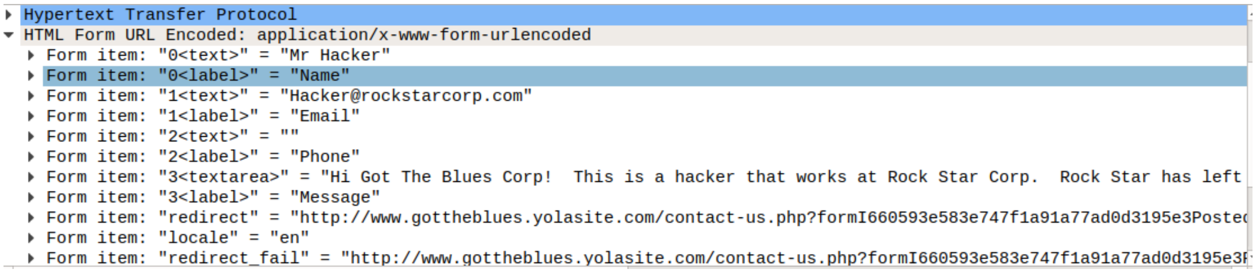
- Next, filtered out the HTTP.

- Upon reviewing the traffic information, you'll notice that on line 16 the adversary had POST to a website.



```
   15 176825015.23… 104.18.127.89     10.0.2.15         HTTP       333 HTTP/1.1 200 OK  (application/x-javascript)
   16 176825119.78… 10.0.2.15         104.18.126.89     HTTP      1876 POST /formservice/en/3f64542cb2e3439c9bd01649
   17 176825120.47… 104.18.126.89     10.0.2.15         HTTP       420 HTTP/1.1 303 See Other
```

- Upon expanding on the given detail, Mr Hacker should probably not quit his day job or at least find a better alias. 😉



```
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "0<text>" = "Mr Hacker"
  ▸ Form item: "0<label>" = "Name"
  ▸ Form item: "1<text>" = "Hacker@rockstarcorp.com"
  ▸ Form item: "1<label>" = "Email"
  ▸ Form item: "2<text>" = ""
  ▸ Form item: "2<label>" = "Phone"
  ▸ Form item: "3<textarea>" = "Hi Got The Blues Corp!  This is a hacker that works at Rock Star Corp.  Rock Star has left
  ▸ Form item: "3<label>" = "Message"
  ▸ Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Postec
  ▸ Form item: "locale" = "en"
  ▸ Form item: "redirect_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3F
```

- Recommend filtering of all web traffic through a firewall to prohibit unauthorized access. Additional measures put in place as well to prevent cache poisoning if compromised.

- This all happened within the **Application Layer 7** of the OSI model as website data ruins through this layer.