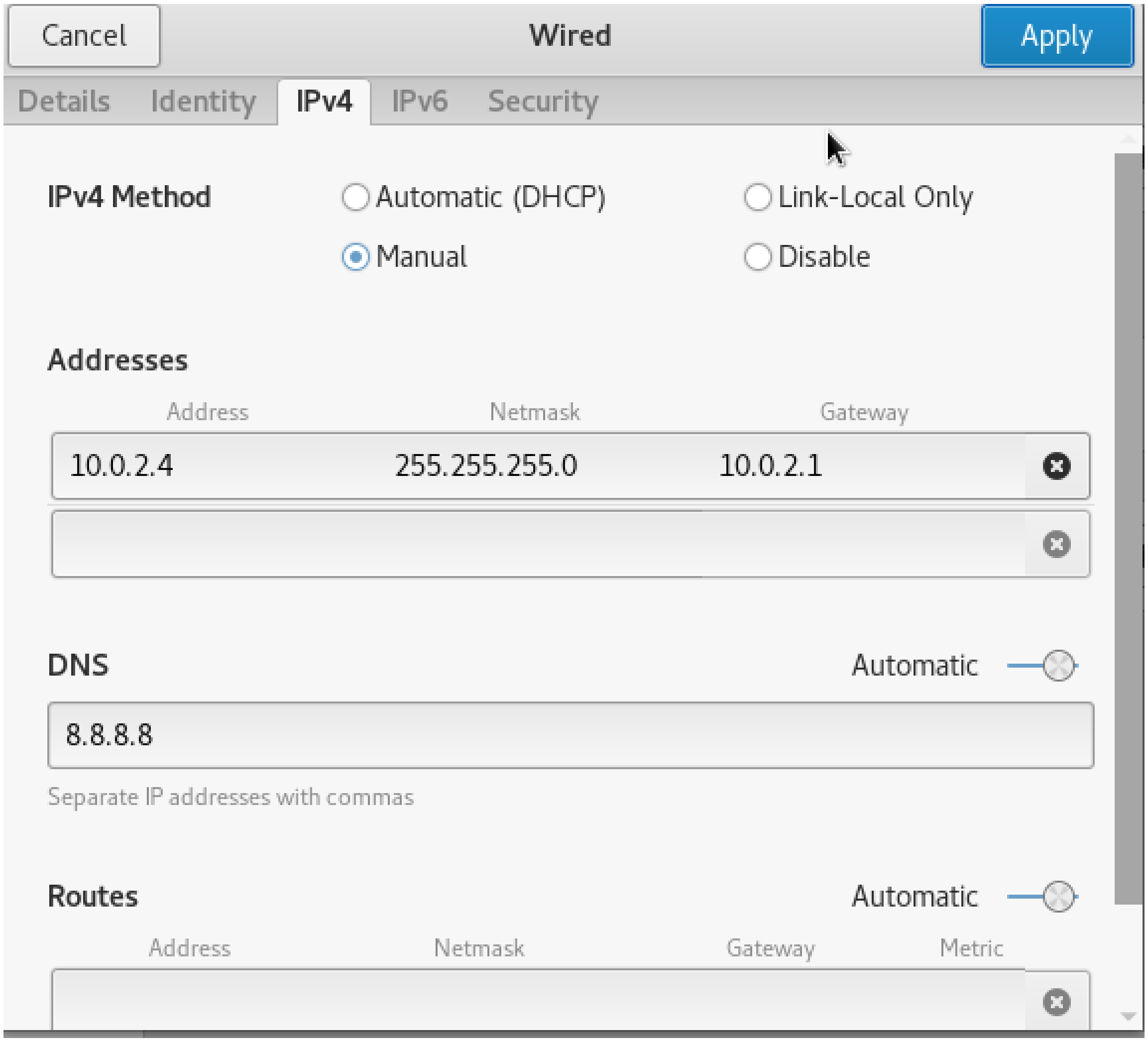
Joseph Shaffer

Shaffer.567

CSE 5473

Lab 3

VM A



IPv4 Method ○ Automatic (DHCP) ○ Link-Local Only
● Manual ○ Disable

Addresses

Address	Netmask	Gateway
10.0.2.4	255.255.255.0	10.0.2.1

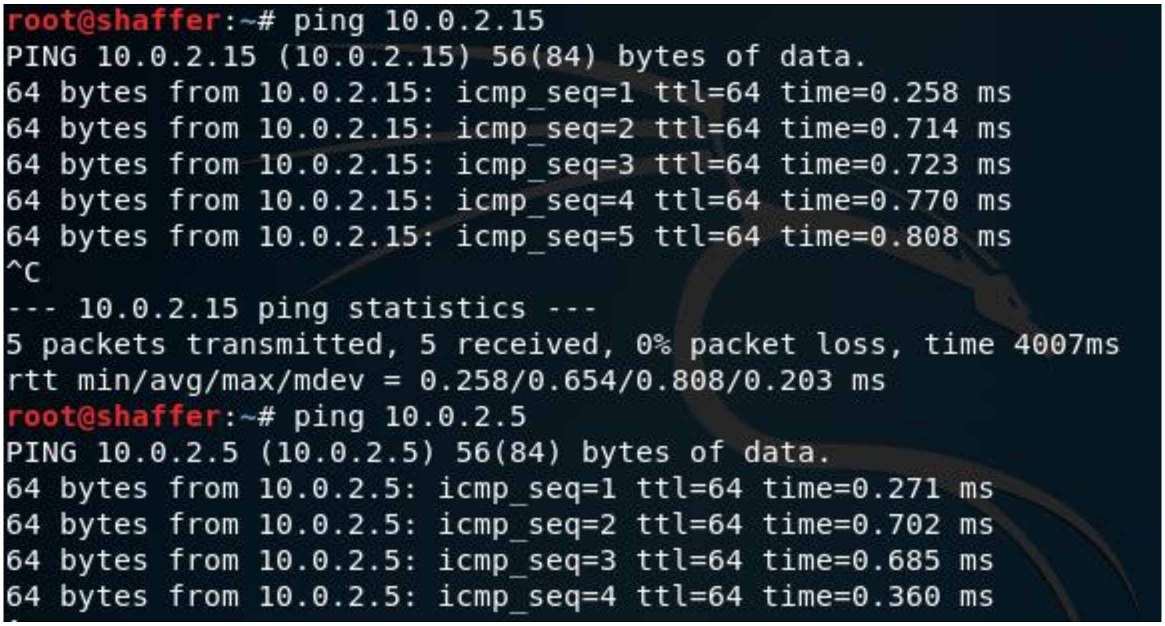
DNS Automatic

8.8.8.8

Separate IP addresses with commas

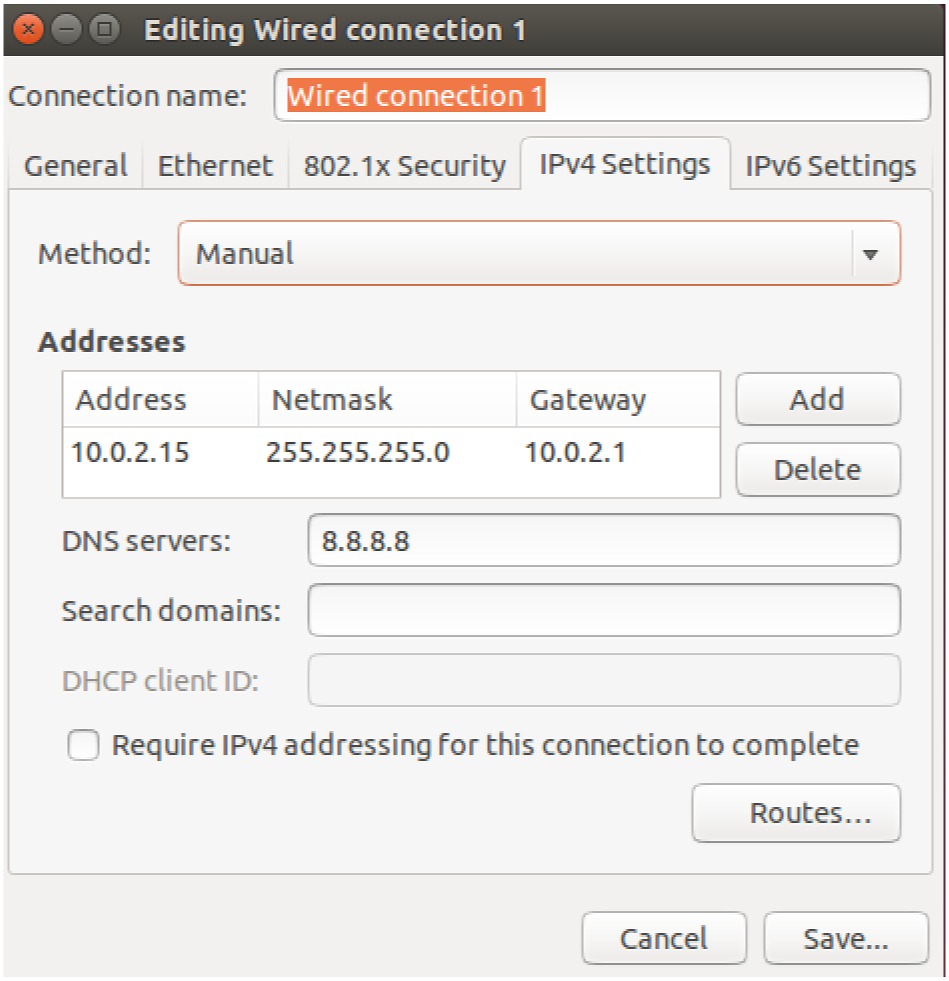
Routes Automatic

Address	Netmask	Gateway	Metric



```
root@shaffer:~# ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.258 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.714 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.723 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.770 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.808 ms
^C
--- 10.0.2.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.258/0.654/0.808/0.203 ms
root@shaffer:~# ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.271 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.702 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.685 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=0.360 ms
```

VM B



Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

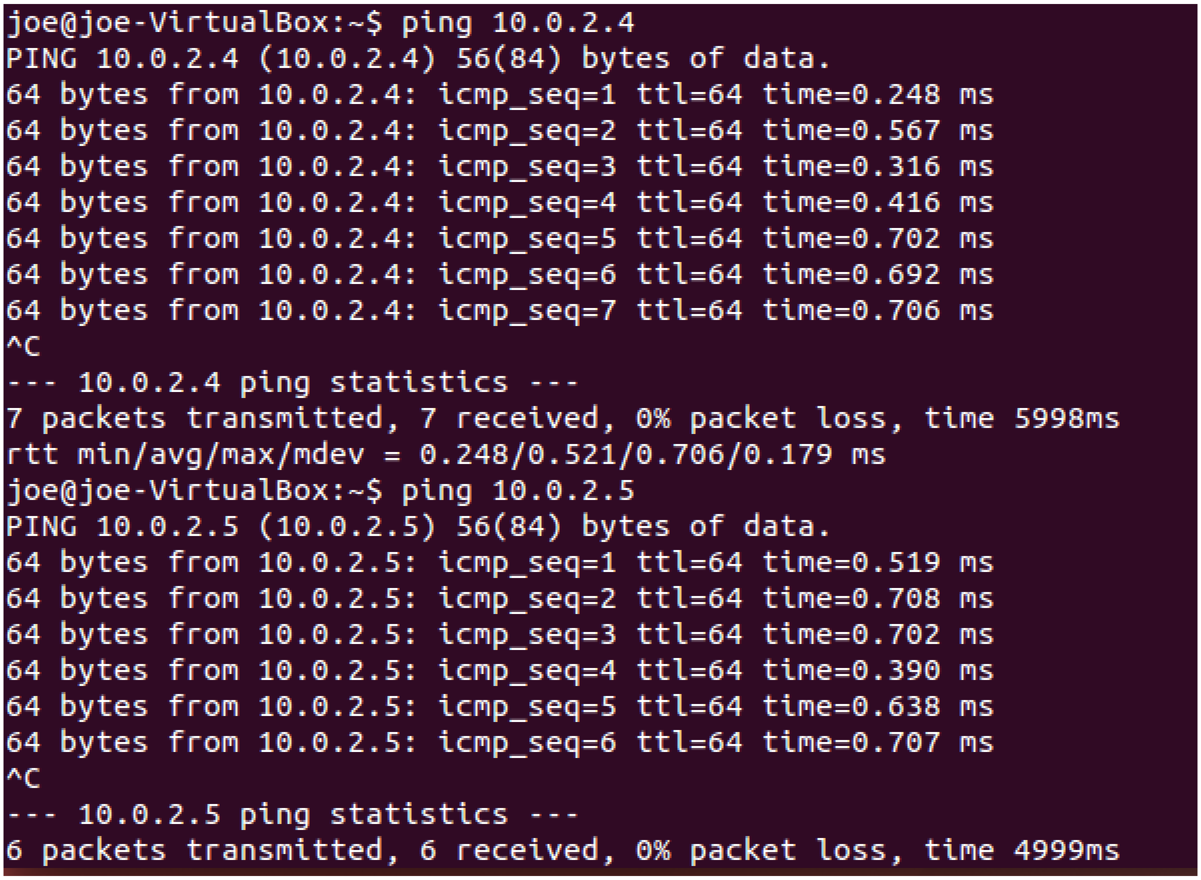
Address	Netmask	Gateway
10.0.2.15	255.255.255.0	10.0.2.1

DNS servers: 8.8.8.8

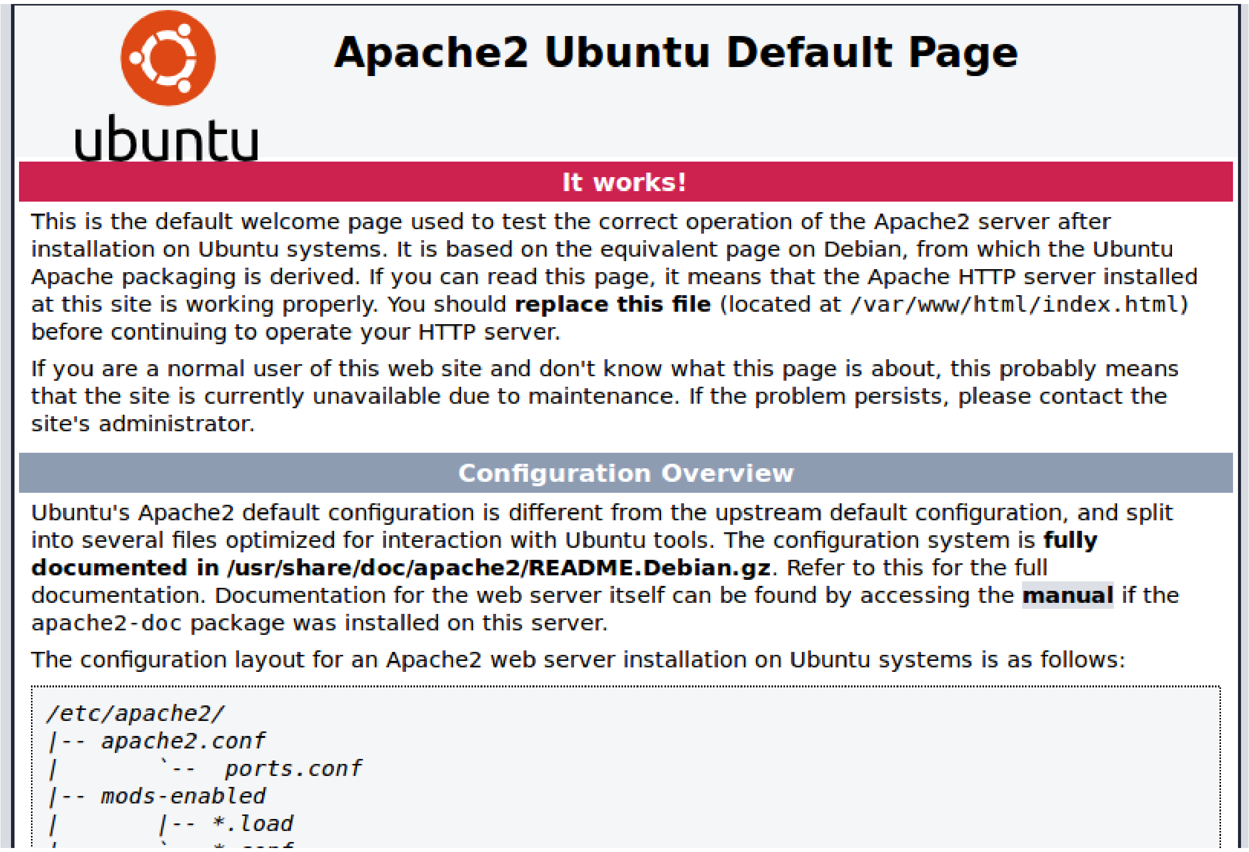
Search domains:

DHCP client ID:

□ Require IPv4 addressing for this connection to complete



```
joe@joe-VirtualBox:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.248 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.567 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.316 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.416 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.702 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=0.692 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=64 time=0.706 ms
^C
--- 10.0.2.4 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5998ms
rtt min/avg/max/mdev = 0.248/0.521/0.706/0.179 ms
joe@joe-VirtualBox:~$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.519 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.708 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.702 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=0.390 ms
64 bytes from 10.0.2.5: icmp_seq=5 ttl=64 time=0.638 ms
64 bytes from 10.0.2.5: icmp_seq=6 ttl=64 time=0.707 ms
^C
--- 10.0.2.5 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
```



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

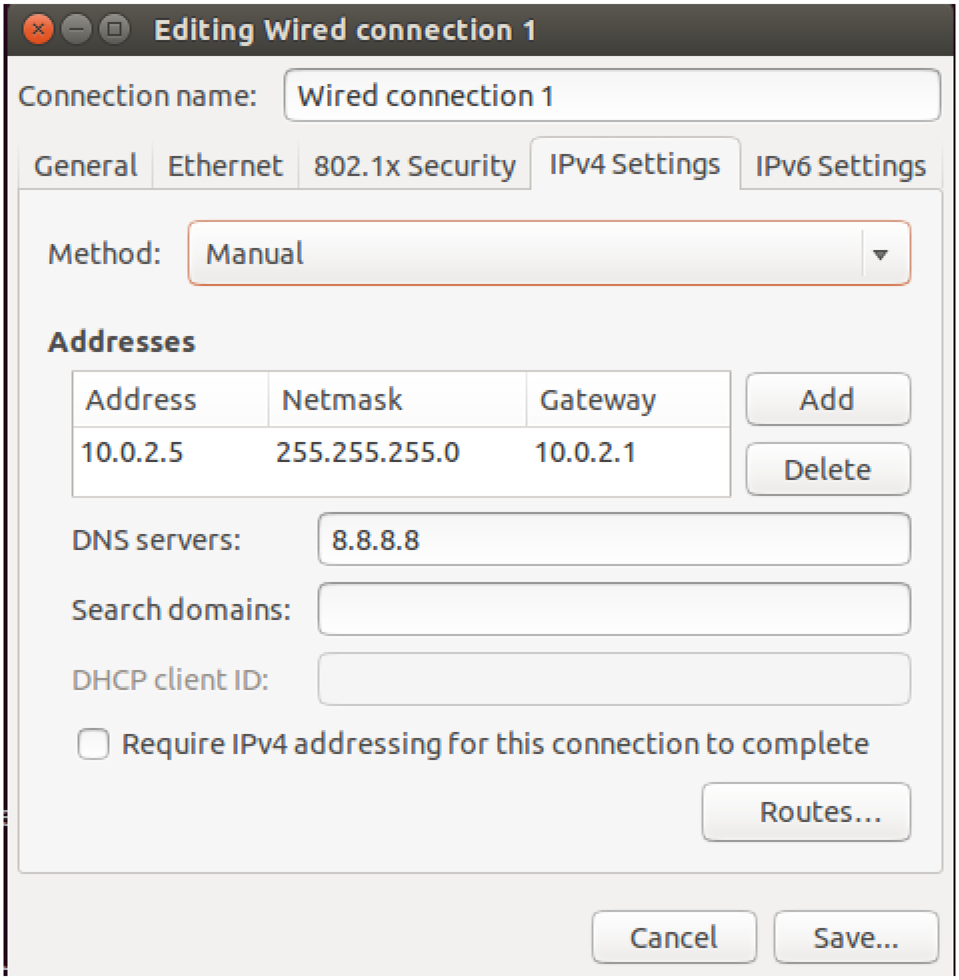
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
```

VM C



Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

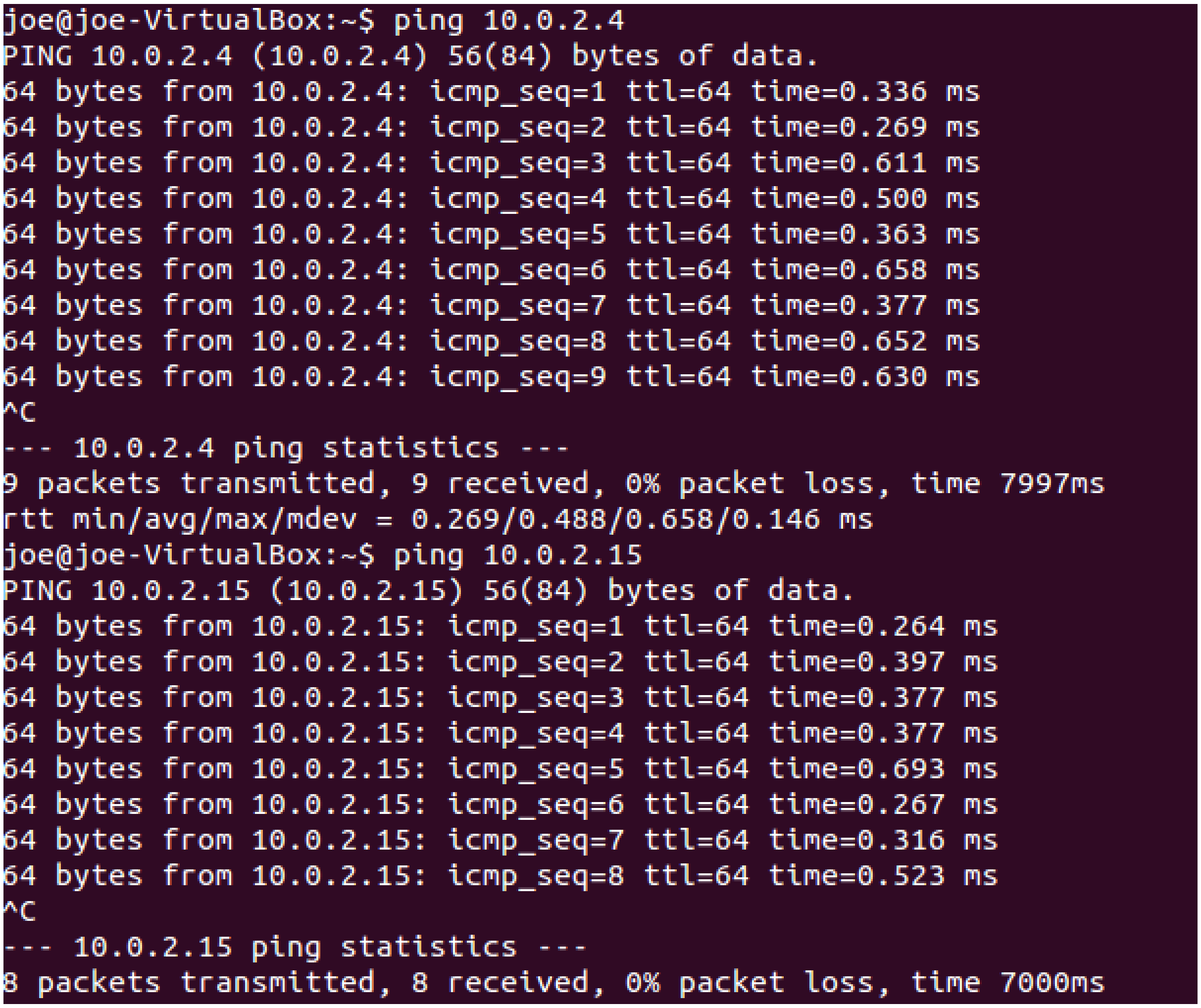
Address	Netmask	Gateway
10.0.2.5	255.255.255.0	10.0.2.1

DNS servers: 8.8.8.8

Search domains:

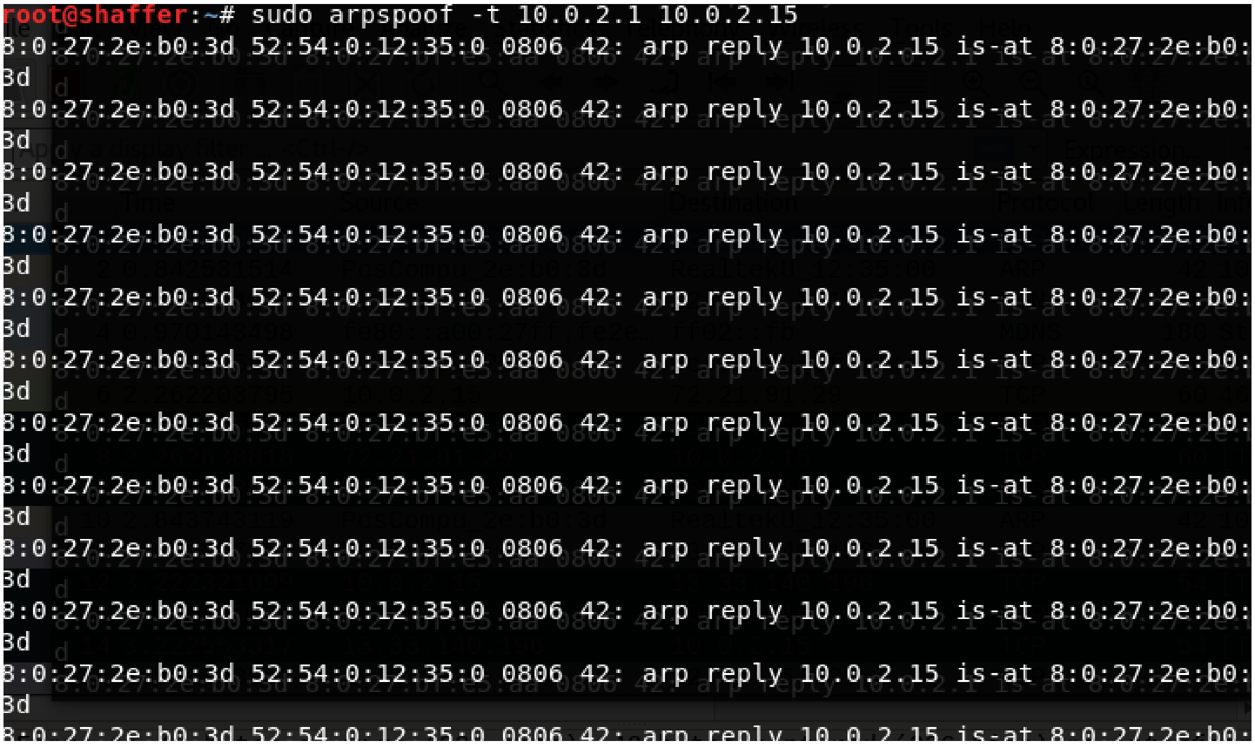
DHCP client ID:

□ Require IPv4 addressing for this connection to complete

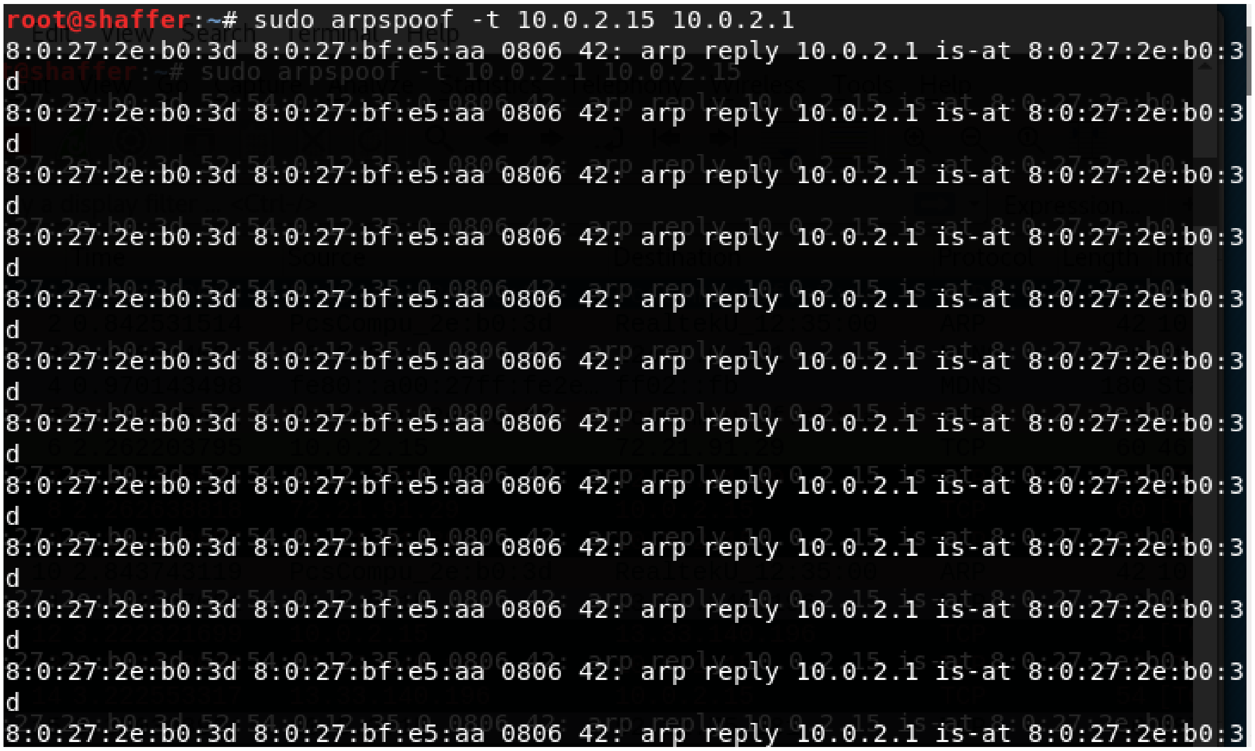


```
joe@joe-VirtualBox:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.336 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.269 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.611 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.500 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.363 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=0.658 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=64 time=0.377 ms
64 bytes from 10.0.2.4: icmp_seq=8 ttl=64 time=0.652 ms
64 bytes from 10.0.2.4: icmp_seq=9 ttl=64 time=0.630 ms
^C
--- 10.0.2.4 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 7997ms
rtt min/avg/max/mdev = 0.269/0.488/0.658/0.146 ms
joe@joe-VirtualBox:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.264 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.397 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.377 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.377 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.693 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.267 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.316 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.523 ms
^C
--- 10.0.2.15 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7000ms
```

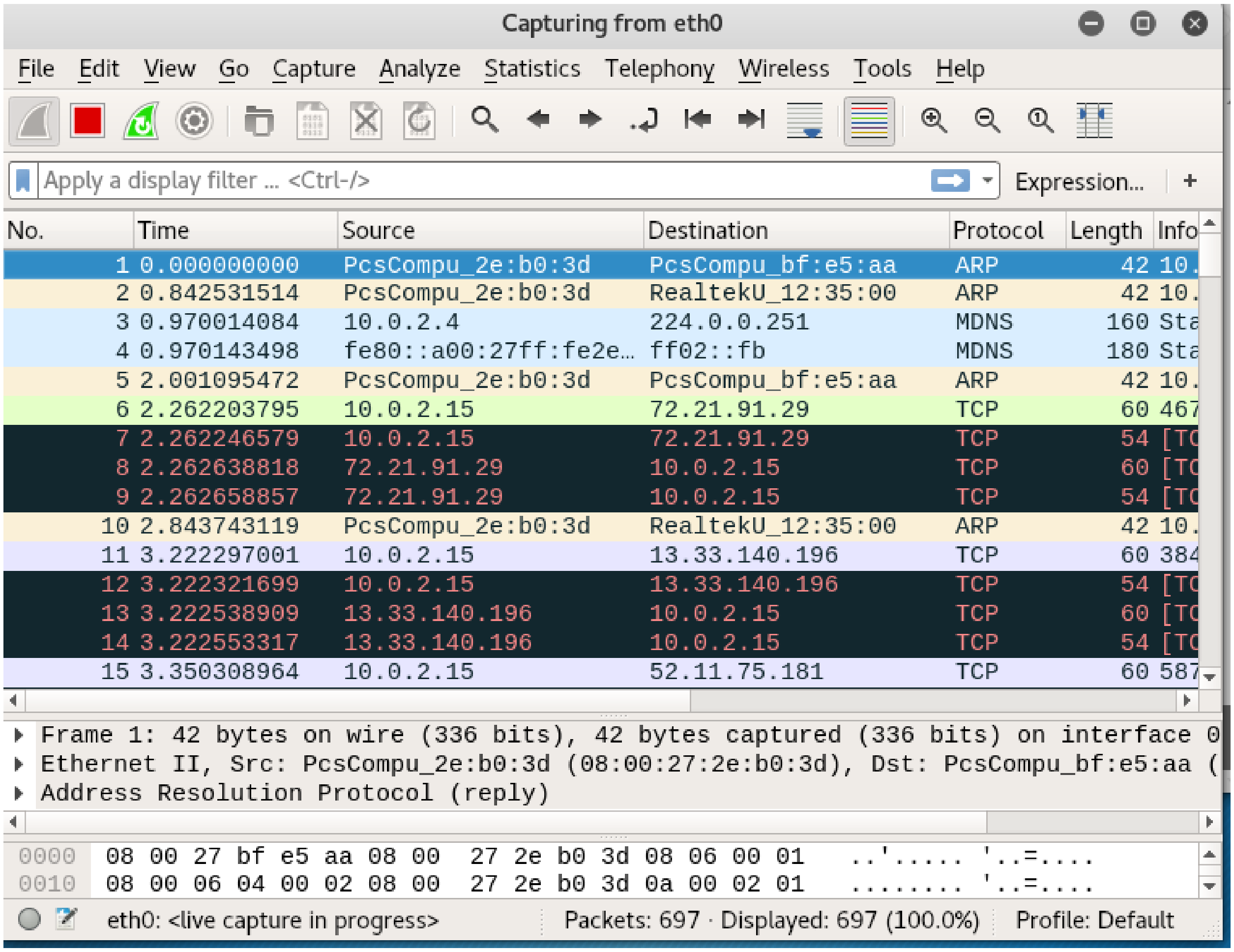
ARP Spoofing



```
root@shaffer:~# sudo arpspoof -t 10.0.2.1 10.0.2.15
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
3d
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
3d
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
3d
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
3d
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
3d
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
3d
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
3d
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
3d
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
3d
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
3d
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
3d
8:0:27:2e:b0:3d 52:54:0:12:35:0 0806 42: arp reply 10.0.2.15 is-at 8:0:27:2e:b0:
```



```
root@shaffer:~# sudo arpspoof -t 10.0.2.15 10.0.2.1
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
d
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
d
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
d
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
d
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
d
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
d
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
d
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
d
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
d
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
d
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
d
8:0:27:2e:b0:3d 8:0:27:bf:e5:aa 0806 42: arp reply 10.0.2.1 is-at 8:0:27:2e:b0:3
```

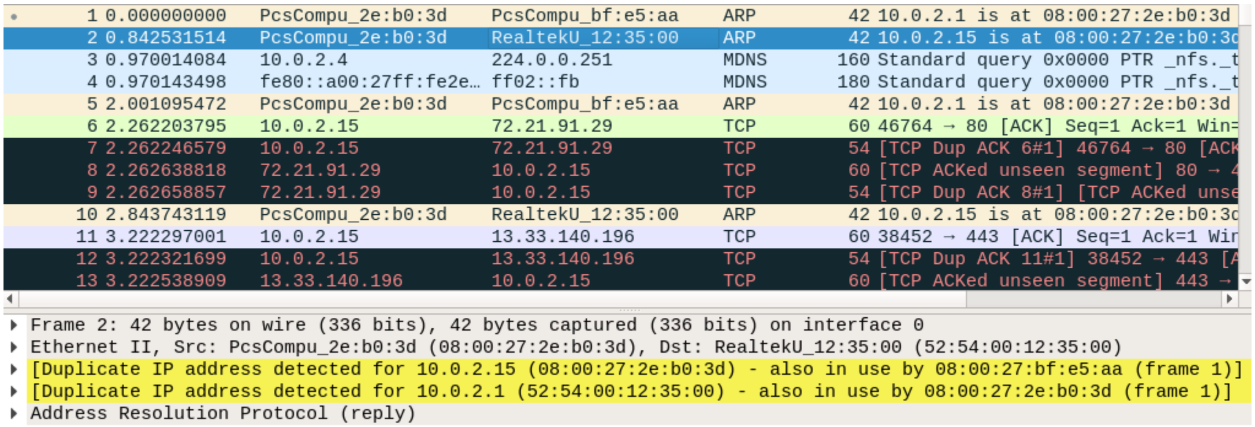

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.    Time          Source                   Destination          Protocol  Length  Info
     1 0.000000000   PcsCompu_2e:b0:3d        PcsCompu_bf:e5:aa    ARP           42  10.
     2 0.842531514   PcsCompu_2e:b0:3d        RealtekU_12:35:00    ARP           42  10.
     3 0.970014084   10.0.2.4                 224.0.0.251          MDNS         160  Sta
     4 0.970143498   fe80::a00:27ff:fe2e…     ff02::fb             MDNS         180  Sta
     5 2.001095472   PcsCompu_2e:b0:3d        PcsCompu_bf:e5:aa    ARP           42  10.
     6 2.262203795   10.0.2.15                72.21.91.29          TCP           60  467
     7 2.262246579   10.0.2.15                72.21.91.29          TCP           54  [TC
     8 2.262638818   72.21.91.29              10.0.2.15            TCP           60  [TC
     9 2.262658857   72.21.91.29              10.0.2.15            TCP           54  [TC
    10 2.843743119   PcsCompu_2e:b0:3d        RealtekU_12:35:00    ARP           42  10.
    11 3.222297001   10.0.2.15                13.33.140.196        TCP           60  384
    12 3.222321699   10.0.2.15                13.33.140.196        TCP           54  [TC
    13 3.222538909   13.33.140.196            10.0.2.15            TCP           60  [TC
    14 3.222553317   13.33.140.196            10.0.2.15            TCP           54  [TC
    15 3.350308964   10.0.2.15                52.11.75.181         TCP           60  587
```

```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_2e:b0:3d (08:00:27:2e:b0:3d), Dst: PcsCompu_bf:e5:aa (
▸ Address Resolution Protocol (reply)
```

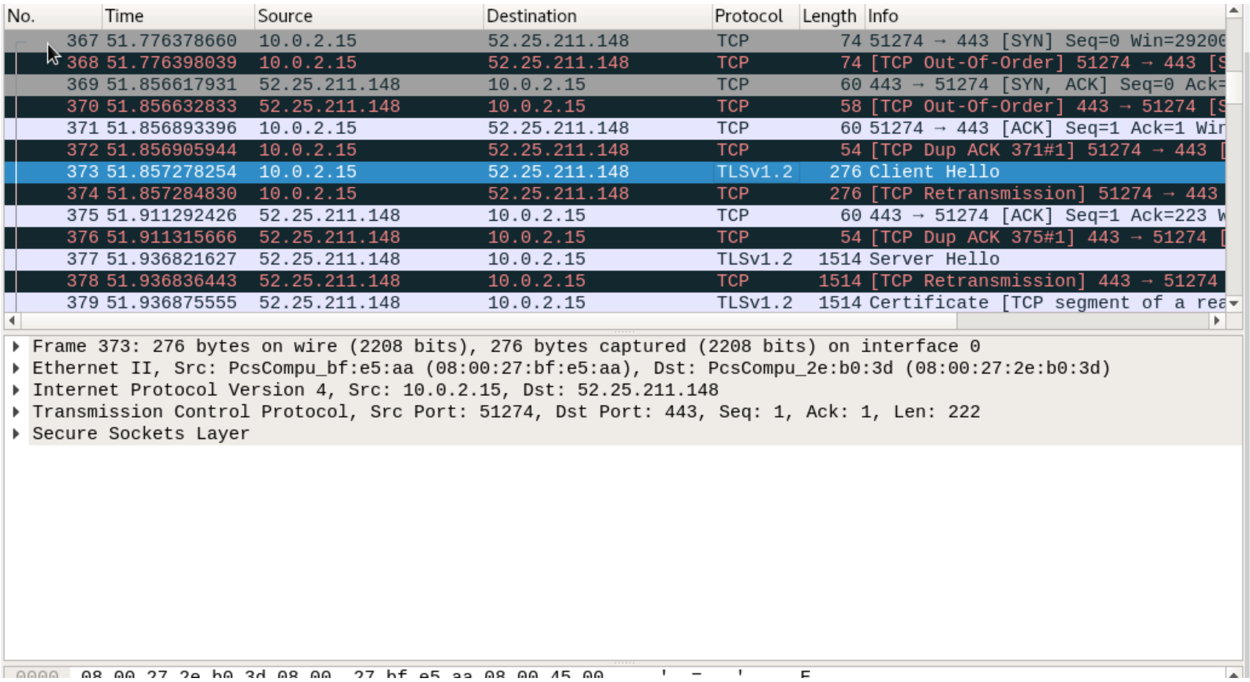
```
0000  08 00 27 bf e5 aa 08 00  27 2e b0 3d 08 06 00 01   ..'..... '..=....
0010  08 00 06 04 00 02 08 00  27 2e b0 3d 0a 00 02 01   ........ '..=....
```

eth0: <live capture in progress> Packets: 697 · Displayed: 697 (100.0%) Profile: Default



```
   1 0.000000000   PcsCompu_2e:b0:3d      PcsCompu_bf:e5:aa    ARP         42 10.0.2.1 is at 08:00:27:2e:b0:3d
   2 0.842531514   PcsCompu_2e:b0:3d      RealtekU_12:35:00    ARP         42 10.0.2.15 is at 08:00:27:2e:b0:3d
   3 0.970014084   10.0.2.4               224.0.0.251          MDNS       160 Standard query 0x0000 PTR _nfs._t
   4 0.970143498   fe80::a00:27ff:fe2e…   ff02::fb             MDNS       180 Standard query 0x0000 PTR _nfs._t
   5 2.001095472   PcsCompu_2e:b0:3d      PcsCompu_bf:e5:aa    ARP         42 10.0.2.1 is at 08:00:27:2e:b0:3d
   6 2.262203795   10.0.2.15              72.21.91.29          TCP         60 46764 → 80 [ACK] Seq=1 Ack=1 Win=
   7 2.262246579   10.0.2.15              72.21.91.29          TCP         54 [TCP Dup ACK 6#1] 46764 → 80 [ACK
   8 2.262638818   72.21.91.29            10.0.2.15            TCP         60 [TCP ACKed unseen segment] 80 → 4
   9 2.262658857   72.21.91.29            10.0.2.15            TCP         54 [TCP Dup ACK 8#1] [TCP ACKed unse
  10 2.843743119   PcsCompu_2e:b0:3d      RealtekU_12:35:00    ARP         42 10.0.2.15 is at 08:00:27:2e:b0:3c
  11 3.222297001   10.0.2.15              13.33.140.196        TCP         60 38452 → 443 [ACK] Seq=1 Ack=1 Wir
  12 3.222321699   10.0.2.15              13.33.140.196        TCP         54 [TCP Dup ACK 11#1] 38452 → 443 [A
  13 3.222538909   13.33.140.196          10.0.2.15            TCP         60 [TCP ACKed unseen segment] 443 →
```

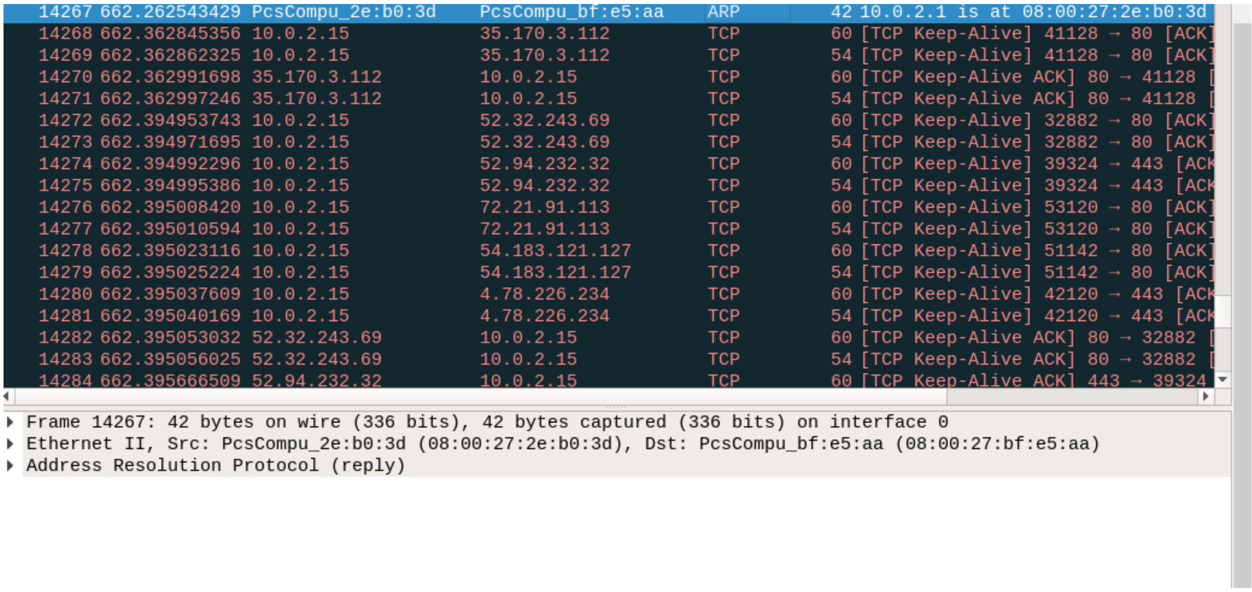
```
▸ Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_2e:b0:3d (08:00:27:2e:b0:3d), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▸ [Duplicate IP address detected for 10.0.2.15 (08:00:27:2e:b0:3d) - also in use by 08:00:27:bf:e5:aa (frame 1)]
▸ [Duplicate IP address detected for 10.0.2.1 (52:54:00:12:35:00) - also in use by 08:00:27:2e:b0:3d (frame 1)]
▸ Address Resolution Protocol (reply)
```



```
No.   Time             Source           Destination      Protocol  Length Info
  367 51.776378660  10.0.2.15        52.25.211.148    TCP          74 51274 → 443 [SYN] Seq=0 Win=29200
  368 51.776398039  10.0.2.15        52.25.211.148    TCP          74 [TCP Out-Of-Order] 51274 → 443 [S
  369 51.856617931  52.25.211.148    10.0.2.15        TCP          60 443 → 51274 [SYN, ACK] Seq=0 Ack=
  370 51.856632833  52.25.211.148    10.0.2.15        TCP          58 [TCP Out-Of-Order] 443 → 51274 [S
  371 51.856893396  10.0.2.15        52.25.211.148    TCP          60 51274 → 443 [ACK] Seq=1 Ack=1 Win
  372 51.856905944  10.0.2.15        52.25.211.148    TCP          54 [TCP Dup ACK 371#1] 51274 → 443 [
  373 51.857278254  10.0.2.15        52.25.211.148    TLSv1.2     276 Client Hello
  374 51.857284830  10.0.2.15        52.25.211.148    TCP         276 [TCP Retransmission] 51274 → 443
  375 51.911292426  52.25.211.148    10.0.2.15        TCP          60 443 → 51274 [ACK] Seq=1 Ack=223 W
  376 51.911315666  52.25.211.148    10.0.2.15        TCP          54 [TCP Dup ACK 375#1] 443 → 51274 [
  377 51.936821627  52.25.211.148    10.0.2.15        TLSv1.2    1514 Server Hello
  378 51.936836443  52.25.211.148    10.0.2.15        TCP        1514 [TCP Retransmission] 443 → 51274
  379 51.936875555  52.25.211.148    10.0.2.15        TLSv1.2    1514 Certificate [TCP segment of a rea
```

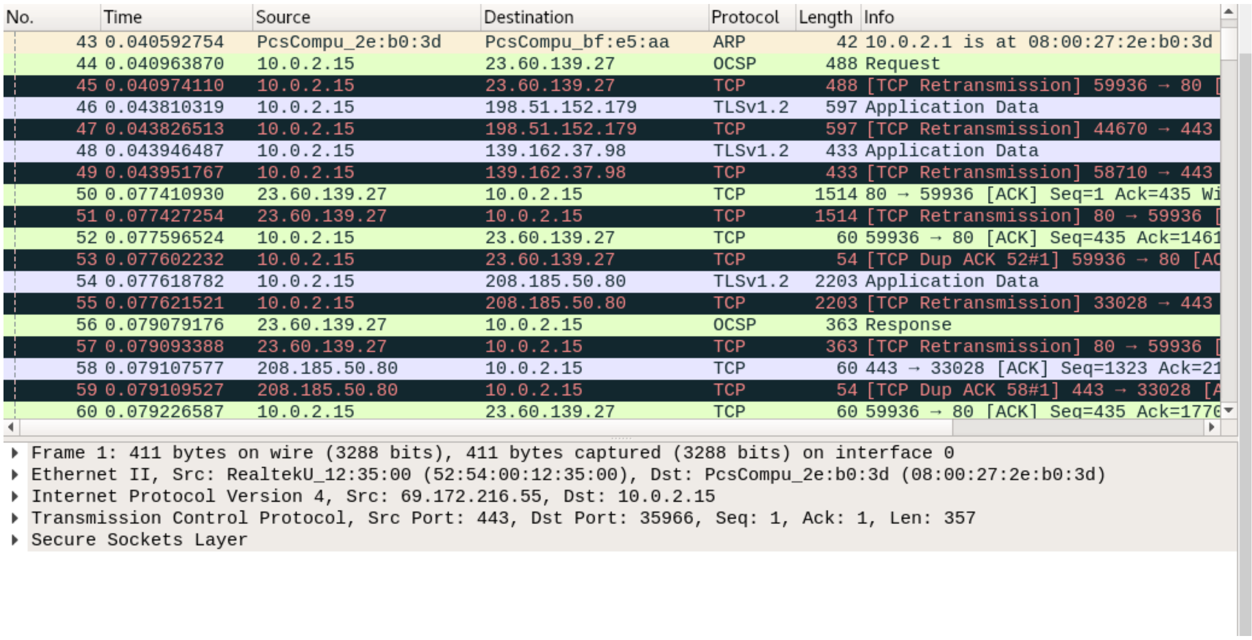
```
▸ Frame 373: 276 bytes on wire (2208 bits), 276 bytes captured (2208 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_bf:e5:aa (08:00:27:bf:e5:aa), Dst: PcsCompu_2e:b0:3d (08:00:27:2e:b0:3d)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 52.25.211.148
▸ Transmission Control Protocol, Src Port: 51274, Dst Port: 443, Seq: 1, Ack: 1, Len: 222
▸ Secure Sockets Layer
```

```
0000  08 00 27 2e b0 3d 08 00  27 bf e5 aa 08 00 45 00   ..'.=.. '.....E.
```



```
14267 662.262543429 PcsCompu_2e:b0:3d  PcsCompu_bf:e5:aa  ARP       42 10.0.2.1 is at 08:00:27:2e:b0:3d
14268 662.362845356 10.0.2.15          35.170.3.112       TCP       60 [TCP Keep-Alive] 41128 → 80 [ACK]
14269 662.362862325 10.0.2.15          35.170.3.112       TCP       54 [TCP Keep-Alive] 41128 → 80 [ACK]
14270 662.362991698 35.170.3.112       10.0.2.15          TCP       60 [TCP Keep-Alive ACK] 80 → 41128 [
14271 662.362997246 35.170.3.112       10.0.2.15          TCP       54 [TCP Keep-Alive ACK] 80 → 41128 [
14272 662.394953743 10.0.2.15          52.32.243.69       TCP       60 [TCP Keep-Alive] 32882 → 80 [ACK]
14273 662.394971695 10.0.2.15          52.32.243.69       TCP       54 [TCP Keep-Alive] 32882 → 80 [ACK]
14274 662.394992296 10.0.2.15          52.94.232.32       TCP       60 [TCP Keep-Alive] 39324 → 443 [ACK
14275 662.394995386 10.0.2.15          52.94.232.32       TCP       54 [TCP Keep-Alive] 39324 → 443 [ACK
14276 662.395008420 10.0.2.15          72.21.91.113       TCP       60 [TCP Keep-Alive] 53120 → 80 [ACK]
14277 662.395010594 10.0.2.15          72.21.91.113       TCP       54 [TCP Keep-Alive] 53120 → 80 [ACK]
14278 662.395023116 10.0.2.15          54.183.121.127     TCP       60 [TCP Keep-Alive] 51142 → 80 [ACK]
14279 662.395025224 10.0.2.15          54.183.121.127     TCP       54 [TCP Keep-Alive] 51142 → 80 [ACK]
14280 662.395037609 10.0.2.15          4.78.226.234       TCP       60 [TCP Keep-Alive] 42120 → 443 [ACK
14281 662.395040169 10.0.2.15          4.78.226.234       TCP       54 [TCP Keep-Alive] 42120 → 443 [ACK
14282 662.395053032 52.32.243.69       10.0.2.15          TCP       60 [TCP Keep-Alive ACK] 80 → 32882 [
14283 662.395056025 52.32.243.69       10.0.2.15          TCP       54 [TCP Keep-Alive ACK] 80 → 32882 [
14284 662.395666509 52.94.232.32       10.0.2.15          TCP       60 [TCP Keep-Alive ACK] 443 → 39324
```

```
▸ Frame 14267: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_2e:b0:3d (08:00:27:2e:b0:3d), Dst: PcsCompu_bf:e5:aa (08:00:27:bf:e5:aa)
▸ Address Resolution Protocol (reply)
```



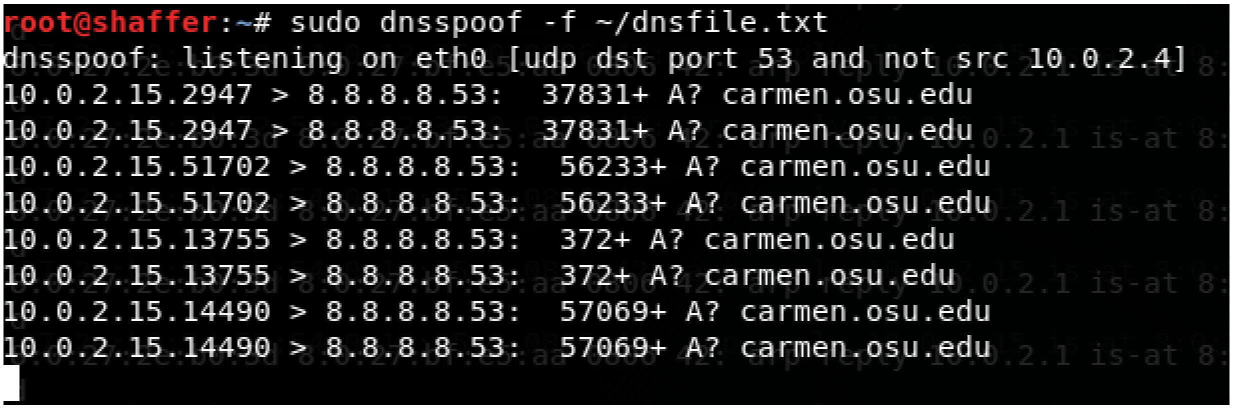
No.	Time	Source	Destination	Protocol	Length	Info
43	0.040592754	PcsCompu_2e:b0:3d	PcsCompu_bf:e5:aa	ARP	42	10.0.2.1 is at 08:00:27:2e:b0:3d
44	0.040963870	10.0.2.15	23.60.139.27	OCSP	488	Request
45	0.040974110	10.0.2.15	23.60.139.27	TCP	488	[TCP Retransmission] 59936 → 80 [
46	0.043810319	10.0.2.15	198.51.152.179	TLSv1.2	597	Application Data
47	0.043826513	10.0.2.15	198.51.152.179	TCP	597	[TCP Retransmission] 44670 → 443
48	0.043946487	10.0.2.15	139.162.37.98	TLSv1.2	433	Application Data
49	0.043951767	10.0.2.15	139.162.37.98	TCP	433	[TCP Retransmission] 58710 → 443
50	0.077410930	23.60.139.27	10.0.2.15	TCP	1514	80 → 59936 [ACK] Seq=1 Ack=435 Wi
51	0.077427254	23.60.139.27	10.0.2.15	TCP	1514	[TCP Retransmission] 80 → 59936 [
52	0.077596524	10.0.2.15	23.60.139.27	TCP	60	59936 → 80 [ACK] Seq=435 Ack=1461
53	0.077602232	10.0.2.15	23.60.139.27	TCP	54	[TCP Dup ACK 52#1] 59936 → 80 [AC
54	0.077618782	10.0.2.15	208.185.50.80	TLSv1.2	2203	Application Data
55	0.077621521	10.0.2.15	208.185.50.80	TCP	2203	[TCP Retransmission] 33028 → 443
56	0.079079176	23.60.139.27	10.0.2.15	OCSP	363	Response
57	0.079093388	23.60.139.27	10.0.2.15	TCP	363	[TCP Retransmission] 80 → 59936 [
58	0.079107577	208.185.50.80	10.0.2.15	TCP	60	443 → 33028 [ACK] Seq=1323 Ack=21
59	0.079109527	208.185.50.80	10.0.2.15	TCP	54	[TCP Dup ACK 58#1] 443 → 33028 [A
60	0.079226587	10.0.2.15	23.60.139.27	TCP	60	59936 → 80 [ACK] Seq=435 Ack=1776

```
▸ Frame 1: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on interface 0
▸ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_2e:b0:3d (08:00:27:2e:b0:3d)
▸ Internet Protocol Version 4, Src: 69.172.216.55, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 35966, Seq: 1, Ack: 1, Len: 357
▸ Secure Sockets Layer
```

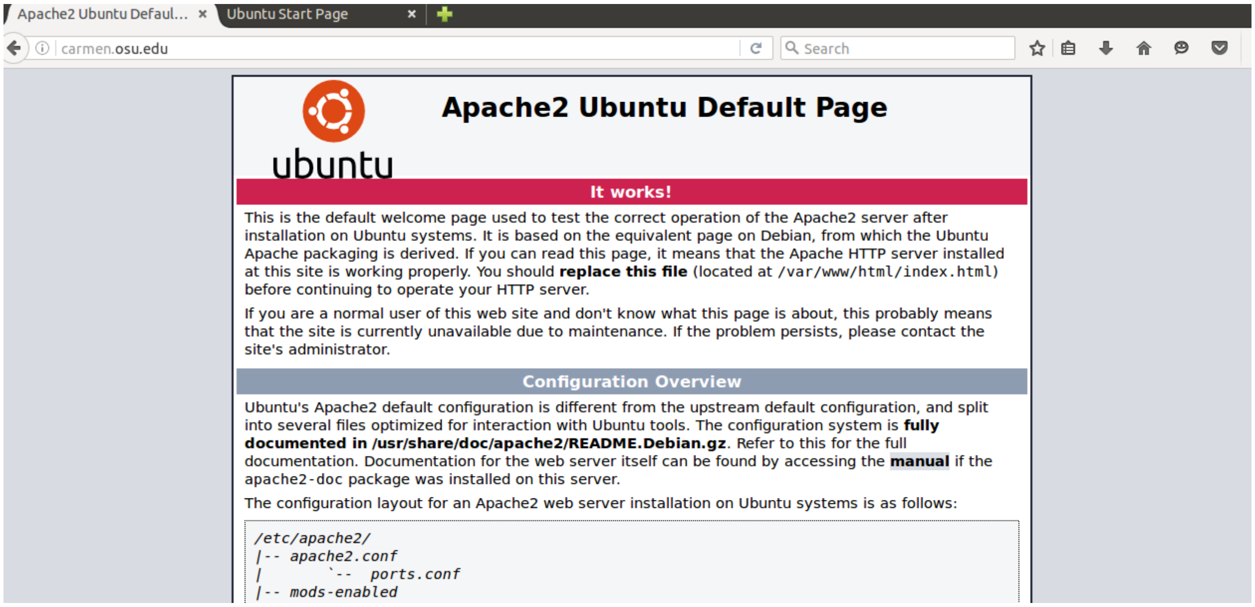
ARP spoofing is an attack where the attacker sends falsified ARP messages over a local area network, which can be seen in the screenshots above. This allows the attacker to associate it's MAC address with the IP address of the victim. By doing so, and from what can be seem above, any traffic meant for the victim was sent to the attacker instead. Furthermore, from the screenshots and wireshark analysis, all the traffic between the victim and the server/external web page can be seen by the attacker, such as the TCP handshake. The external webpage that was visited was http://www/bbc.com because it is not a https webpage and thus not encrypted. Thus, from the screenshots above, I can deduce that ARP spoofing allows attacker to see all the traffic between the victim and an external webpage.

This is done because ARP spoofing exploits the lack of authentication in the ARP protocol by sending spoofed ARP messages onto the LAN, which can also be seen in the screenshots. This means that any traffic meant for the victim will be sent to the attacker and the attacker can choose to look at those packets, as well as forwarding the traffic to victim to avoid discovery. The attacker can all send modified data to the victim instead.

DNS Spoofing



```
root@shaffer:~# sudo dnsspoof -f ~/dnsfile.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src 10.0.2.4]
10.0.2.15.2947 > 8.8.8.8.53:  37831+ A? carmen.osu.edu
10.0.2.15.2947 > 8.8.8.8.53:  37831+ A? carmen.osu.edu
10.0.2.15.51702 > 8.8.8.8.53:  56233+ A? carmen.osu.edu
10.0.2.15.51702 > 8.8.8.8.53:  56233+ A? carmen.osu.edu
10.0.2.15.13755 > 8.8.8.8.53:  372+ A? carmen.osu.edu
10.0.2.15.13755 > 8.8.8.8.53:  372+ A? carmen.osu.edu
10.0.2.15.14490 > 8.8.8.8.53:  57069+ A? carmen.osu.edu
10.0.2.15.14490 > 8.8.8.8.53:  57069+ A? carmen.osu.edu
```



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

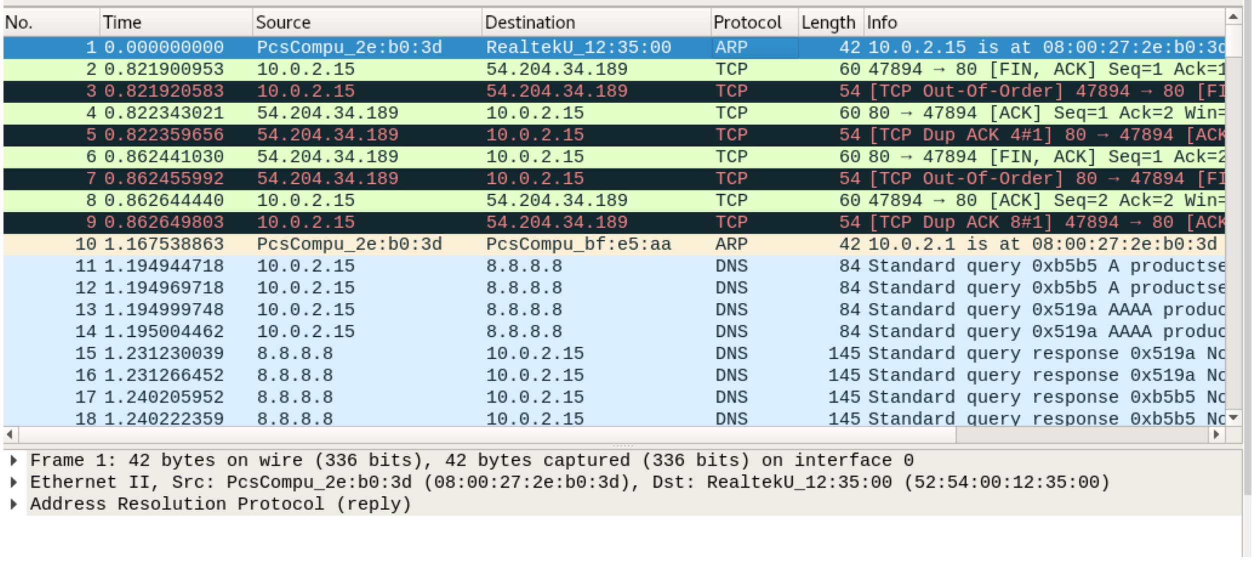
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

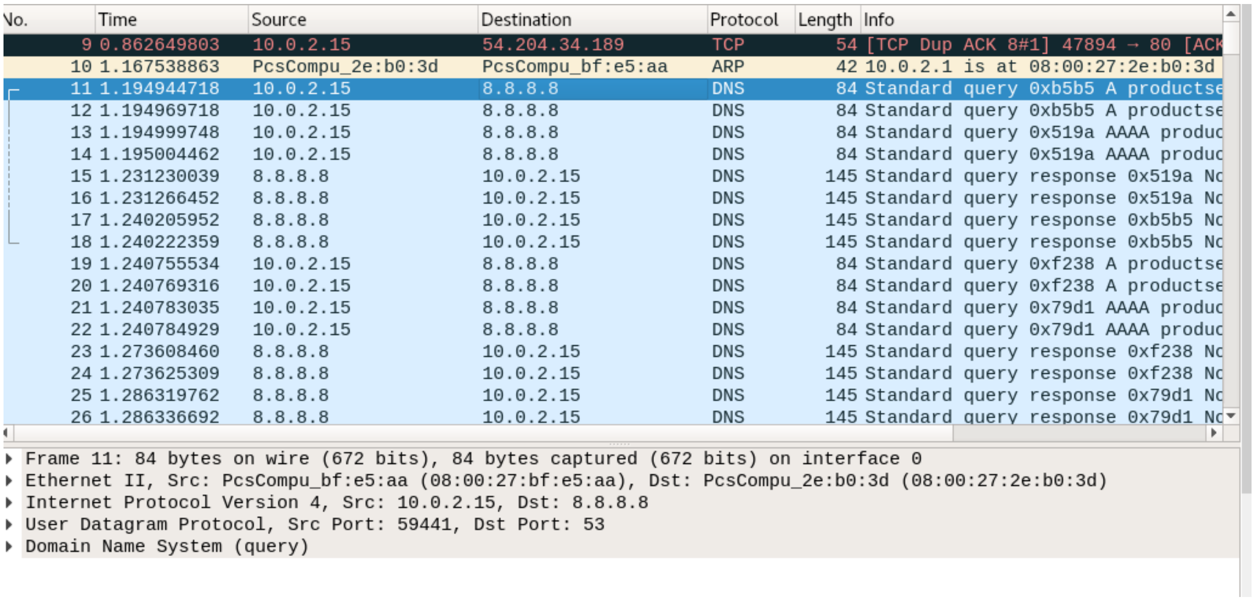
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
```



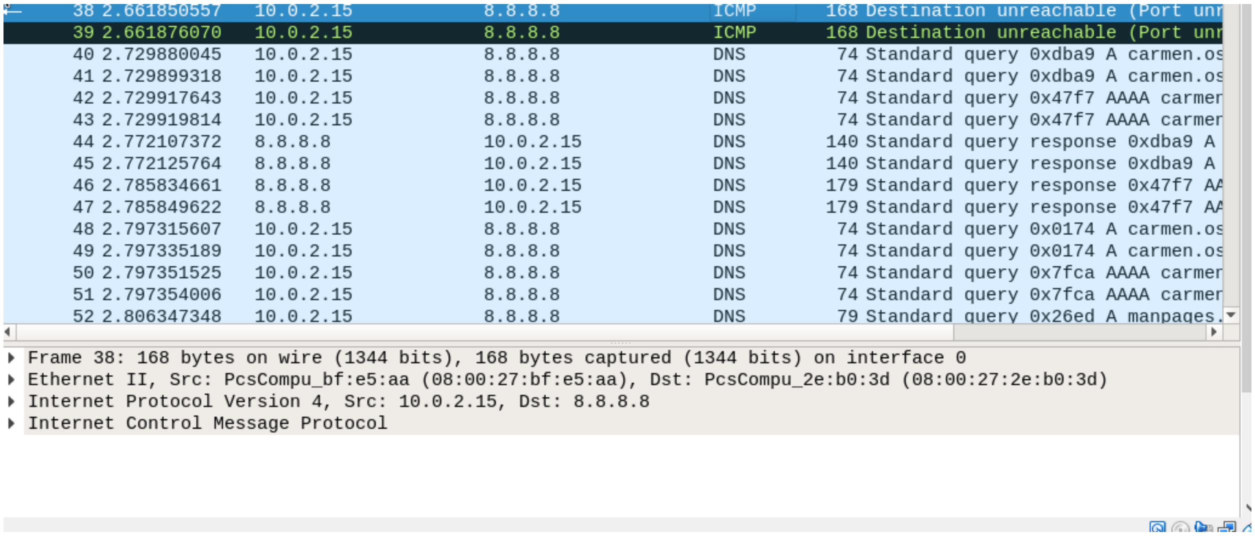
```
No.    Time           Source              Destination         Protocol  Length Info
     1 0.000000000    PcsCompu_2e:b0:3d   RealtekU_12:35:00   ARP          42 10.0.2.15 is at 08:00:27:2e:b0:3d
     2 0.821900953    10.0.2.15           54.204.34.189       TCP          60 47894 → 80 [FIN, ACK] Seq=1 Ack=1
     3 0.821920583    10.0.2.15           54.204.34.189       TCP          54 [TCP Out-Of-Order] 47894 → 80 [FI
     4 0.822343021    54.204.34.189       10.0.2.15           TCP          60 80 → 47894 [ACK] Seq=1 Ack=2 Win=
     5 0.822359656    54.204.34.189       10.0.2.15           TCP          54 [TCP Dup ACK 4#1] 80 → 47894 [ACK
     6 0.862441030    54.204.34.189       10.0.2.15           TCP          60 80 → 47894 [FIN, ACK] Seq=1 Ack=2
     7 0.862455992    54.204.34.189       10.0.2.15           TCP          54 [TCP Out-Of-Order] 80 → 47894 [FI
     8 0.862644440    10.0.2.15           54.204.34.189       TCP          60 47894 → 80 [ACK] Seq=2 Ack=2 Win=
     9 0.862649803    10.0.2.15           54.204.34.189       TCP          54 [TCP Dup ACK 8#1] 47894 → 80 [ACK
    10 1.167538863    PcsCompu_2e:b0:3d   PcsCompu_bf:e5:aa   ARP          42 10.0.2.1 is at 08:00:27:2e:b0:3d
    11 1.194944718    10.0.2.15           8.8.8.8             DNS          84 Standard query 0xb5b5 A productse
    12 1.194969718    10.0.2.15           8.8.8.8             DNS          84 Standard query 0xb5b5 A productse
    13 1.194999748    10.0.2.15           8.8.8.8             DNS          84 Standard query 0x519a AAAA produc
    14 1.195004462    10.0.2.15           8.8.8.8             DNS          84 Standard query 0x519a AAAA produc
    15 1.231230039    8.8.8.8             10.0.2.15           DNS         145 Standard query response 0x519a No
    16 1.231266452    8.8.8.8             10.0.2.15           DNS         145 Standard query response 0x519a No
    17 1.240205952    8.8.8.8             10.0.2.15           DNS         145 Standard query response 0xb5b5 No
    18 1.240222359    8.8.8.8             10.0.2.15           DNS         145 Standard query response 0xb5b5 No
```

```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_2e:b0:3d (08:00:27:2e:b0:3d), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▸ Address Resolution Protocol (reply)
```



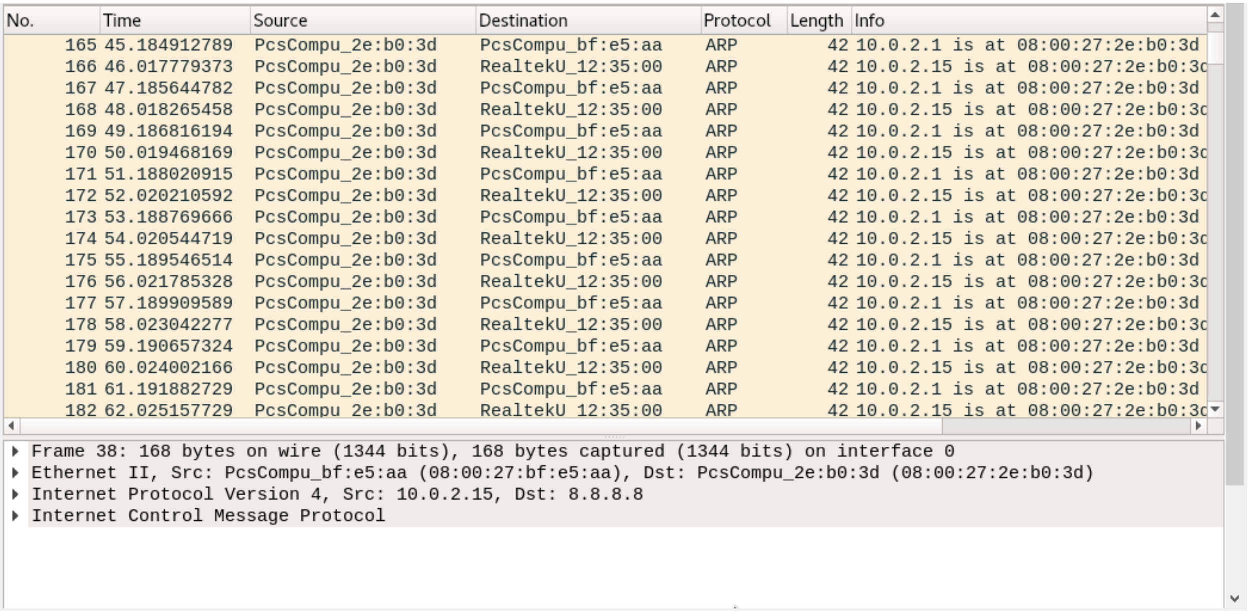
```
No.   Time         Source              Destination         Protocol  Length Info
    9 0.862649803  10.0.2.15           54.204.34.189       TCP          54 [TCP Dup ACK 8#1] 47894 → 80 [ACK
   10 1.167538863  PcsCompu_2e:b0:3d   PcsCompu_bf:e5:aa   ARP          42 10.0.2.1 is at 08:00:27:2e:b0:3d
   11 1.194944718  10.0.2.15           8.8.8.8             DNS          84 Standard query 0xb5b5 A productse
   12 1.194969718  10.0.2.15           8.8.8.8             DNS          84 Standard query 0xb5b5 A productse
   13 1.194999748  10.0.2.15           8.8.8.8             DNS          84 Standard query 0x519a AAAA produc
   14 1.195004462  10.0.2.15           8.8.8.8             DNS          84 Standard query 0x519a AAAA produc
   15 1.231230039  8.8.8.8             10.0.2.15           DNS         145 Standard query response 0x519a Nc
   16 1.231266452  8.8.8.8             10.0.2.15           DNS         145 Standard query response 0x519a Nc
   17 1.240205952  8.8.8.8             10.0.2.15           DNS         145 Standard query response 0xb5b5 Nc
   18 1.240222359  8.8.8.8             10.0.2.15           DNS         145 Standard query response 0xb5b5 Nc
   19 1.240755534  10.0.2.15           8.8.8.8             DNS          84 Standard query 0xf238 A productse
   20 1.240769316  10.0.2.15           8.8.8.8             DNS          84 Standard query 0xf238 A productse
   21 1.240783035  10.0.2.15           8.8.8.8             DNS          84 Standard query 0x79d1 AAAA produc
   22 1.240784929  10.0.2.15           8.8.8.8             DNS          84 Standard query 0x79d1 AAAA produc
   23 1.273608460  8.8.8.8             10.0.2.15           DNS         145 Standard query response 0xf238 Nc
   24 1.273625309  8.8.8.8             10.0.2.15           DNS         145 Standard query response 0xf238 Nc
   25 1.286319762  8.8.8.8             10.0.2.15           DNS         145 Standard query response 0x79d1 Nc
   26 1.286336692  8.8.8.8             10.0.2.15           DNS         145 Standard query response 0x79d1 Nc

▸ Frame 11: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_bf:e5:aa (08:00:27:bf:e5:aa), Dst: PcsCompu_2e:b0:3d (08:00:27:2e:b0:3d)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 59441, Dst Port: 53
▸ Domain Name System (query)
```



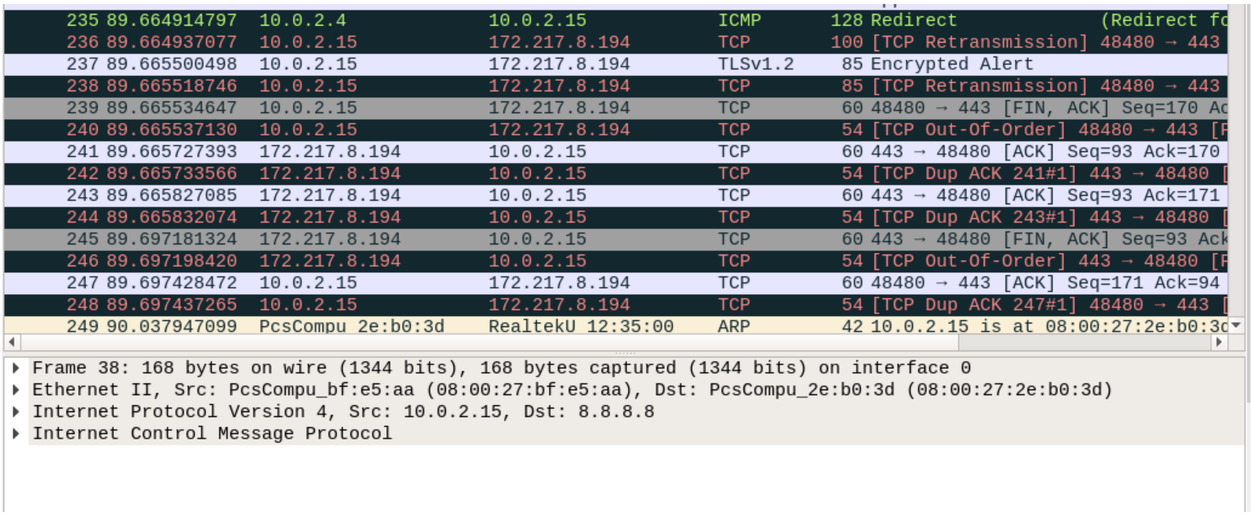
```
   38 2.661850557  10.0.2.15           8.8.8.8             ICMP        168 Destination unreachable (Port unr
   39 2.661876070  10.0.2.15           8.8.8.8             ICMP        168 Destination unreachable (Port unr
   40 2.729880045  10.0.2.15           8.8.8.8             DNS          74 Standard query 0xdba9 A carmen.os
   41 2.729899318  10.0.2.15           8.8.8.8             DNS          74 Standard query 0xdba9 A carmen.os
   42 2.729917643  10.0.2.15           8.8.8.8             DNS          74 Standard query 0x47f7 AAAA carmen
   43 2.729919814  10.0.2.15           8.8.8.8             DNS          74 Standard query 0x47f7 AAAA carmen
   44 2.772107372  8.8.8.8             10.0.2.15           DNS         140 Standard query response 0xdba9 A
   45 2.772125764  8.8.8.8             10.0.2.15           DNS         140 Standard query response 0xdba9 A
   46 2.785834661  8.8.8.8             10.0.2.15           DNS         179 Standard query response 0x47f7 AA
   47 2.785849622  8.8.8.8             10.0.2.15           DNS         179 Standard query response 0x47f7 AA
   48 2.797315607  10.0.2.15           8.8.8.8             DNS          74 Standard query 0x0174 A carmen.os
   49 2.797335189  10.0.2.15           8.8.8.8             DNS          74 Standard query 0x0174 A carmen.os
   50 2.797351525  10.0.2.15           8.8.8.8             DNS          74 Standard query 0x7fca AAAA carmen
   51 2.797354006  10.0.2.15           8.8.8.8             DNS          74 Standard query 0x7fca AAAA carmen
   52 2.806347348  10.0.2.15           8.8.8.8             DNS          79 Standard query 0x26ed A manpages.

▸ Frame 38: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_bf:e5:aa (08:00:27:bf:e5:aa), Dst: PcsCompu_2e:b0:3d (08:00:27:2e:b0:3d)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
▸ Internet Control Message Protocol
```



```
No.    Time          Source             Destination        Protocol  Length Info
   165 45.184912789  PcsCompu_2e:b0:3d  PcsCompu_bf:e5:aa  ARP           42 10.0.2.1 is at 08:00:27:2e:b0:3d
   166 46.017779373  PcsCompu_2e:b0:3d  RealtekU_12:35:00  ARP           42 10.0.2.15 is at 08:00:27:2e:b0:3c
   167 47.185644782  PcsCompu_2e:b0:3d  PcsCompu_bf:e5:aa  ARP           42 10.0.2.1 is at 08:00:27:2e:b0:3d
   168 48.018265458  PcsCompu_2e:b0:3d  RealtekU_12:35:00  ARP           42 10.0.2.15 is at 08:00:27:2e:b0:3c
   169 49.186816194  PcsCompu_2e:b0:3d  PcsCompu_bf:e5:aa  ARP           42 10.0.2.1 is at 08:00:27:2e:b0:3d
   170 50.019468169  PcsCompu_2e:b0:3d  RealtekU_12:35:00  ARP           42 10.0.2.15 is at 08:00:27:2e:b0:3c
   171 51.188020915  PcsCompu_2e:b0:3d  PcsCompu_bf:e5:aa  ARP           42 10.0.2.1 is at 08:00:27:2e:b0:3d
   172 52.020210592  PcsCompu_2e:b0:3d  RealtekU_12:35:00  ARP           42 10.0.2.15 is at 08:00:27:2e:b0:3c
   173 53.188769666  PcsCompu_2e:b0:3d  PcsCompu_bf:e5:aa  ARP           42 10.0.2.1 is at 08:00:27:2e:b0:3d
   174 54.020544719  PcsCompu_2e:b0:3d  RealtekU_12:35:00  ARP           42 10.0.2.15 is at 08:00:27:2e:b0:3c
   175 55.189546514  PcsCompu_2e:b0:3d  PcsCompu_bf:e5:aa  ARP           42 10.0.2.1 is at 08:00:27:2e:b0:3d
   176 56.021785328  PcsCompu_2e:b0:3d  RealtekU_12:35:00  ARP           42 10.0.2.15 is at 08:00:27:2e:b0:3c
   177 57.189909589  PcsCompu_2e:b0:3d  PcsCompu_bf:e5:aa  ARP           42 10.0.2.1 is at 08:00:27:2e:b0:3d
   178 58.023042277  PcsCompu_2e:b0:3d  RealtekU_12:35:00  ARP           42 10.0.2.15 is at 08:00:27:2e:b0:3c
   179 59.190657324  PcsCompu_2e:b0:3d  PcsCompu_bf:e5:aa  ARP           42 10.0.2.1 is at 08:00:27:2e:b0:3d
   180 60.024002166  PcsCompu_2e:b0:3d  RealtekU_12:35:00  ARP           42 10.0.2.15 is at 08:00:27:2e:b0:3c
   181 61.191882729  PcsCompu_2e:b0:3d  PcsCompu_bf:e5:aa  ARP           42 10.0.2.1 is at 08:00:27:2e:b0:3d
   182 62.025157729  PcsCompu_2e:b0:3d  RealtekU_12:35:00  ARP           42 10.0.2.15 is at 08:00:27:2e:b0:3c

▸ Frame 38: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_bf:e5:aa (08:00:27:bf:e5:aa), Dst: PcsCompu_2e:b0:3d (08:00:27:2e:b0:3d)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
▸ Internet Control Message Protocol
```



```
   235 89.664914797  10.0.2.4        10.0.2.15          ICMP      128 Redirect             (Redirect fc
   236 89.664937077  10.0.2.15       172.217.8.194      TCP       100 [TCP Retransmission] 48480 → 443
   237 89.665500498  10.0.2.15       172.217.8.194      TLSv1.2    85 Encrypted Alert
   238 89.665518746  10.0.2.15       172.217.8.194      TCP        85 [TCP Retransmission] 48480 → 443
   239 89.665534647  10.0.2.15       172.217.8.194      TCP        60 48480 → 443 [FIN, ACK] Seq=170 Ac
   240 89.665537130  10.0.2.15       172.217.8.194      TCP        54 [TCP Out-Of-Order] 48480 → 443 [F
   241 89.665727393  172.217.8.194   10.0.2.15          TCP        60 443 → 48480 [ACK] Seq=93 Ack=170
   242 89.665733566  172.217.8.194   10.0.2.15          TCP        54 [TCP Dup ACK 241#1] 443 → 48480 [
   243 89.665827085  172.217.8.194   10.0.2.15          TCP        60 443 → 48480 [ACK] Seq=93 Ack=171
   244 89.665832074  172.217.8.194   10.0.2.15          TCP        54 [TCP Dup ACK 243#1] 443 → 48480 [
   245 89.697181324  172.217.8.194   10.0.2.15          TCP        60 443 → 48480 [FIN, ACK] Seq=93 Ack
   246 89.697198420  172.217.8.194   10.0.2.15          TCP        54 [TCP Out-Of-Order] 443 → 48480 [F
   247 89.697428472  10.0.2.15       172.217.8.194      TCP        60 48480 → 443 [ACK] Seq=171 Ack=94
   248 89.697437265  10.0.2.15       172.217.8.194      TCP        54 [TCP Dup ACK 247#1] 48480 → 443 [
   249 90.037947099  PcsCompu_2e:b0:3d  RealtekU_12:35:00  ARP     42 10.0.2.15 is at 08:00:27:2e:b0:3c

▸ Frame 38: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_bf:e5:aa (08:00:27:bf:e5:aa), Dst: PcsCompu_2e:b0:3d (08:00:27:2e:b0:3d)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
▸ Internet Control Message Protocol
```

DNS spoofing is a way to corrupt the Domain Name System data that is introduced in the DNS resolver's cache, which causes the name server to return an incorrect IP address. The result of this is traffic is diverted to the attacker's computer. The attack can be used to redirect users from a website to another site of the attacker's choosing. It can be seen in the screenshots above that the attacker can see the traffic between the victim and an external web page, which in this case is www.carmen.edu. Furthermore, from the screenshots above that the victim is being redirected by the attacker to see the Ubuntu default page instead of the carmen website, which is a result of the DNS spoofing. Thus, the attacker is spoofing the IP address DNS entries for the carmen website on the given DNS server and replaces them with the IP address of a server under the attacker's control, which is the Ubuntu default page. The attacker can use DNS spoofing to create malicious files on the server under their control with names matching those on the target server, which means the victim could open those malicious files and receive computer worms or viruses for instance. Thus the victim who has referenced the wrong DNS server is tricked into accepting malicious content coming from a non-authentic server and downloads the malicious content. Furthermore, the attacker can create a fake version of the website that the victim is visiting to gain personal details from the victim such as bank account details. However this attack simply allows the attacker to see the traffic of the victim and redirects the victim to the external web page of the attacker’s choosing instead of the actual website the victim is trying to see.