

Week #4

NAME	SIRI S SNEHA P
SRN	PES1UG19CS485 PES1UG19CS490
SECTION	H
SUBJECT	COMPUTER NETWORKS LABORATORY

Implementation of a Local DNS Server:

DNS (Domain Name System) is the Internet's phone book; it translates hostnames to IP addresses (and vice versa). This translation is through DNS resolution, which happens behind the scenes.

Lab Setup

DNS Server: 10.1.10.41

User/Client: 10.1.10.74

TASK-1

First Test:

Ping a computer such as www.example.com. Please use Wireshark to show the DNS query triggered by your ping command and DNS response. Describe your observation. (Take a screenshot).

The screenshot shows a Wireshark capture of network traffic. The packet list on the left shows several DNS queries and responses, followed by an ICMP 'Destination unreachable' message. The packet details pane for packet 49 (a DNS query) is expanded, showing the query for 'www.example.com'. The packet bytes pane at the bottom shows the raw data of the DNS query, including the domain name 'www.example.com' in ASCII and hexadecimal.

No.	Time	Source	Destination	Protocol	Length	Info
49	8.079590539	10.1.10.74	10.1.10.41	DNS	77	Standard query 0xbc87 A www.example.com
66	13.084718874	127.0.0.1	127.0.1.1	DNS	77	Standard query 0xbc87 A www.example.com
67	13.084808452	10.1.10.74	192.168.3.5	DNS	77	Standard query 0x170f A www.example.com
68	13.084817378	10.1.10.74	4.2.2.2	DNS	77	Standard query 0x170f A www.example.com
69	13.084820760	10.1.10.74	202.138.96.2	DNS	77	Standard query 0x170f A www.example.com
70	13.084824347	10.1.10.74	202.138.103.100	DNS	77	Standard query 0x170f A www.example.com
71	13.085250529	192.168.3.5	10.1.10.74	DNS	93	Standard query response 0x170f A www.examp...
72	13.085335186	127.0.1.1	127.0.0.1	DNS	93	Standard query response 0xbc87 A www.examp...
76	13.226042573	4.2.2.2	10.1.10.74	DNS	93	Standard query response 0x170f A www.examp...
78	13.231566787	202.138.96.2	10.1.10.74	DNS	229	Standard query response 0x170f A www.examp...
79	13.278553844	202.138.103.100	10.1.10.74	DNS	229	Standard query response 0x170f A www.examp...
81	13.959993149	10.1.10.41	10.1.10.74	DNS	229	Standard query response 0xbc87 A www.examp...
82	13.960020230	10.1.10.74	10.1.10.41	ICMP	257	Destination unreachable (Port unreachable)

Frame 49: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.1.10.74, Dst: 10.1.10.41
User Datagram Protocol, Src Port: 60670, Dst Port: 53
Domain Name System (query)

0000 00 04 00 01 00 06 b8 ae ed a5 a5 e3 01 30 08 000..
0010 45 00 00 3d 61 69 40 00 40 11 b0 d2 0a 01 0a 4a E...=ai@. @.....J
0020 0a 01 0a 29 ec fe 00 35 00 29 e3 0f bc 87 01 00 ...).5.).....
0030 00 01 00 00 00 00 00 03 77 77 77 07 65 78 61www-exa

wireshark_any_20210216141642_LtyhN2.pcapng Packets: 168 · Displayed: 13 (7.7%) Profile: Default

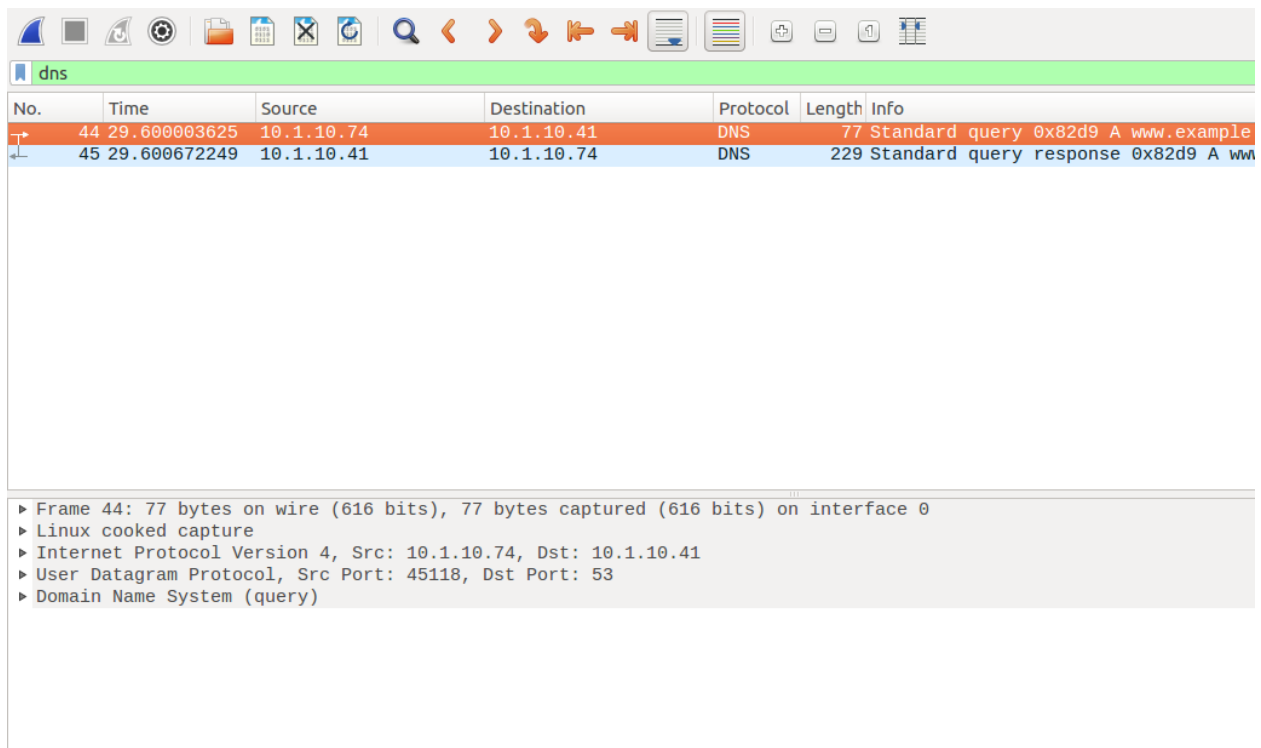
TASK-2

Set Up a Local DNS Server:

Configure and start a local DNS server.

```
student@CSELAB:~$ sudo rndc dumpdb -cache
student@CSELAB:~$ sudo rndc flush
student@CSELAB:~$
```

Now, go back to your user machine (10.2.22.195), and ping a computer such as www.flipkart.com and describe your observation. Please use Wireshark to show the DNS query triggered by your ping command. Please also indicate when the DNS cache is used. (Take a screenshot).



TASK-3

Host a Zone in the Local DNS server.

```
dump.db [Read-Only] (/var/cache/bind) - gedit
: Start view _default
:
: Cache dump of view '_default' (cache _default)
:
$DATE 20210216091904
; secure
516124 IN NS a.root-servers.net.
516124 IN NS b.root-servers.net.
516124 IN NS c.root-servers.net.
516124 IN NS d.root-servers.net.
516124 IN NS e.root-servers.net.
516124 IN NS f.root-servers.net.
516124 IN NS g.root-servers.net.
516124 IN NS h.root-servers.net.
516124 IN NS i.root-servers.net.
516124 IN NS j.root-servers.net.
516124 IN NS k.root-servers.net.
516124 IN NS l.root-servers.net.
516124 IN NS m.root-servers.net.
; secure
516146 RRSIG NS 8 0 518400 (
20210301050000 20210216040000 42351 .
b/vMCz4Qqazgyra/qDhuU4iQSn/HKnsMmhKV
dDtrPLlj82x6w6kVAoVX1MHY6baunAHT+LM1
Tzr1LwEEhGbMD5t6DDeZMmk5aPCrIa5a5fi/
StPE3INZPhQPIrHtwHLeFGydogmbccn21tn/
mtYXk2W2Pzvt14WpqaX61HakV0EqTNRJXA+
G50bRffTn7WbcXzVK5ZgbYxSHzc2x8Z7uLNT
09fUHSdaIjktjITo0otsybyqYr3QoFVv2dEst
kZbkKn0gs3H8uKDxjt3npNb1h8zF08LRE8JQ
XYoLrZ7BhVP5Ydu1xTQ5nMmWxUwJdQL/dTpo
TeP8xCH/KvfyxgRRYw== )
; secure
170523 DNSKEY 256 3 8 (
AwEAAbKGKkqc1VAvQr48iPf9Nd39f337Mitg
gxFOAB9kLKRNSuq9Jo0EPC/R6PD/4LTzUms8
U9oP+aLF0rVC2rGOKSd0LxPHRLA3ameMFTZ/
3bmVCFsRsn03IVTdNSVUJfCz1n1nA0t9NM7b
```

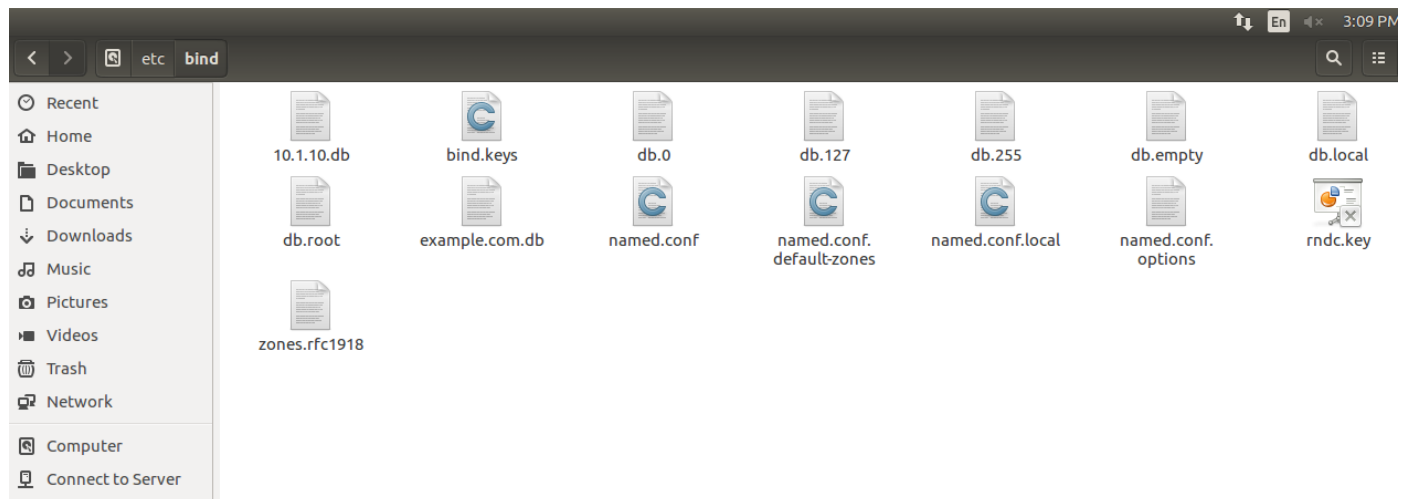
Setup the forward lookup zone file

```
example.com.db (/etc/bind) - gedit
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
2008111001
8H
2H
4W
1D)
@ IN NS ns.example.com.
@ IN MX 10 mail.example.com.
www IN A 10.1.10.101
mail IN A 10.1.10.102
ns IN A 10.1.10.10
*.example.com. IN A .100|
```

Setup the reverse lookup zone file

```
10.1.10.db (/etc/bind) - gedit
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
2008111001
8H
2H
4W
1D)
@ IN NS ns.example.com.
101 IN PTR www.example.com.
102 IN PTR mail.example.com.
10 IN PTR ns.example.com.
```

Copy the above files into /etc/bind location.



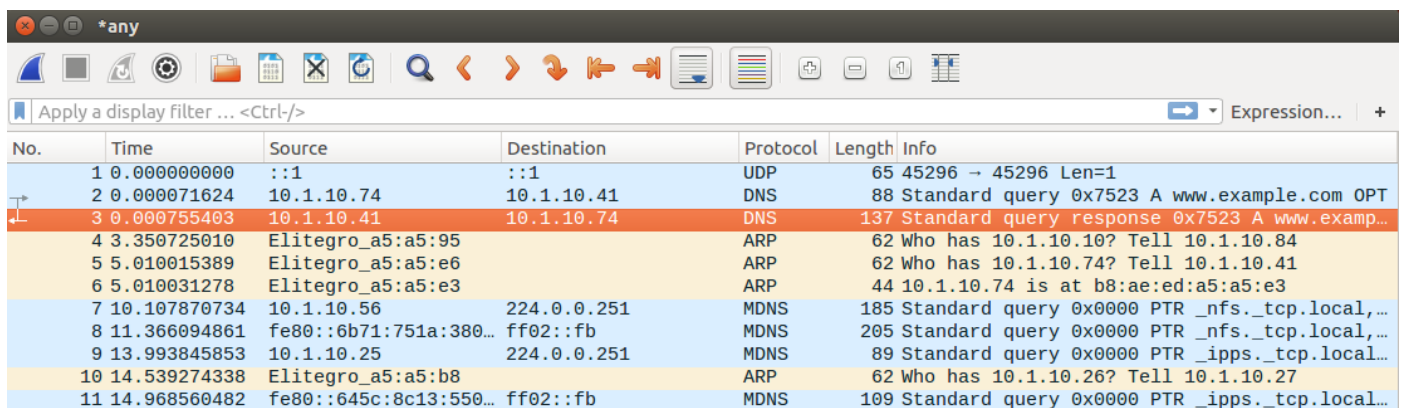
TASK-4

Restart the BIND server and test

Now, go back to the client machine and ask the local DNS server for the IP address of `www.example.com` using the `dig` command.

```
student@CSELAB: ~  
student@CSELAB:~$ dig www.example.com  
  
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43220  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;www.example.com.                IN      A  
  
;; ANSWER SECTION:  
www.example.com.                259200  IN      A      10.1.10.101  
  
;; AUTHORITY SECTION:  
example.com.                    259200  IN      NS      ns.example.com.  
  
;; ADDITIONAL SECTION:  
ns.example.com.                 259200  IN      A      10.1.10.10  
  
;; Query time: 0 msec  
;; SERVER: 10.1.10.41#53(10.1.10.41)  
;; WHEN: Tue Feb 16 15:16:57 IST 2021  
;; MSG SIZE rcvd: 93  
  
student@CSELAB:~$
```

Observe the results in Wireshark capture.



The image shows a Wireshark network capture with a toolbar at the top and a packet list table below. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The third packet (No. 3) is highlighted in orange, showing a DNS Standard query response from 10.1.10.41 to 10.1.10.74 for www.example.com. Other packets include ARP requests and MDNS queries.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	::1	::1	UDP	65	45296 → 45296 Len=1
2	0.000071624	10.1.10.74	10.1.10.41	DNS	88	Standard query 0x7523 A www.example.com OPT
3	0.000755403	10.1.10.41	10.1.10.74	DNS	137	Standard query response 0x7523 A www.examp...
4	3.350725010	Elitegro_a5:a5:95		ARP	62	Who has 10.1.10.10? Tell 10.1.10.84
5	5.010015389	Elitegro_a5:a5:e6		ARP	62	Who has 10.1.10.74? Tell 10.1.10.41
6	5.010031278	Elitegro_a5:a5:e3		ARP	44	10.1.10.74 is at b8:ae:ed:a5:a5:e3
7	10.107870734	10.1.10.56	224.0.0.251	MDNS	185	Standard query 0x0000 PTR _nfs._tcp.local,...
8	11.366094861	fe80::6b71:751a:380...	ff02::fb	MDNS	205	Standard query 0x0000 PTR _nfs._tcp.local,...
9	13.993845853	10.1.10.25	224.0.0.251	MDNS	89	Standard query 0x0000 PTR _ipps._tcp.local...
10	14.539274338	Elitegro_a5:a5:b8		ARP	62	Who has 10.1.10.26? Tell 10.1.10.27
11	14.968560482	fe80::645c:8c13:550...	ff02::fb	MDNS	109	Standard query 0x0000 PTR _ipps._tcp.local...

Packet 3 · any

▶ Frame 3: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0

▶ Linux cooked capture

▶ Internet Protocol Version 4, Src: 10.1.10.41, Dst: 10.1.10.74

▶ User Datagram Protocol, Src Port: 53, Dst Port: 48952

▼ Domain Name System (response)

Transaction ID: 0x7523

▶ Flags: 0x8580 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 1

Additional RRs: 2

▶ Queries

▼ Answers

▼ www.example.com: type A, class IN, addr 192.168.0.101

Name: www.example.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 259200

Data length: 4

Address: 10.1.10.101

▼ Authoritative nameservers

▼ example.com: type NS, class IN, ns ns.example.com

Name: example.com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 259200

Data length: 5

Name Server: ns.example.com

▼ Additional records

▼ ns.example.com: type A, class IN, addr 192.168.0.10

Name: ns.example.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 259200

Data length: 4

Address: 10.1.10.10

▼ <Root>: type OPT

Name: <Root>

Type: OPT (41)

UDP payload size: 4096

Higher bits in extended RCODE: 0x00

EDNS0 version: 0

▶ Z: 0x0000

Data length: 0

[\[Request In: 2\]](#)

[Time: 0.000683779 seconds]