

Computer Networks Laboratory

UE20CS255

Name: Naman Choudhary

SRN: PES2UG20CS209

Section: D

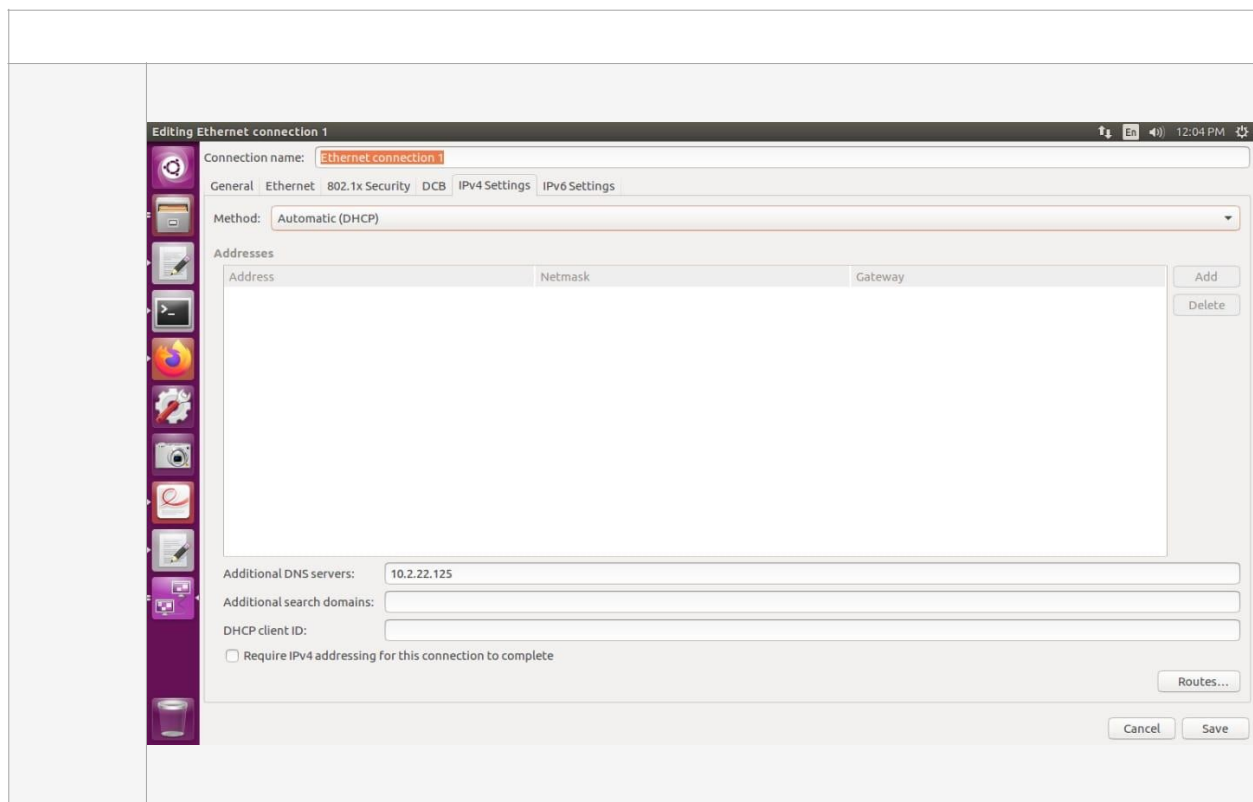
Week 5

Implementation of a Local DNS Server

Task 1: Setting Up a Local DNS Server

```
isfcr@isfcr-H110M-H:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
[sudo] password for isfcr:
isfcr@isfcr-H110M-H:~$ sudo cat /etc/resolvconf/resolv.conf.d/head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.2.22.184
isfcr@isfcr-H110M-H:~$ sudo resolvconf -u
isfcr@isfcr-H110M-H:~$
```

Also, add 10.2.22.184 in 'Additional DNS servers' field in IPv4 settings of client machine.



Task 2:

```

root@PESU: ~
64 bytes from 163.53.78.110: icmp_seq=23 ttl=54 time=10.3 ms
64 bytes from 163.53.78.110: icmp_seq=24 ttl=54 time=10.5 ms
64 bytes from 163.53.78.110: icmp_seq=25 ttl=54 time=10.5 ms
64 bytes from 163.53.78.110: icmp_seq=26 ttl=54 time=10.4 ms
64 bytes from 163.53.78.110: icmp_seq=27 ttl=54 time=10.4 ms
64 bytes from 163.53.78.110: icmp_seq=28 ttl=54 time=10.4 ms
64 bytes from 163.53.78.110: icmp_seq=29 ttl=54 time=10.3 ms
64 bytes from 163.53.78.110: icmp_seq=30 ttl=54 time=10.5 ms
64 bytes from 163.53.78.110: icmp_seq=31 ttl=54 time=10.5 ms
64 bytes from 163.53.78.110: icmp_seq=32 ttl=54 time=10.3 ms
64 bytes from 163.53.78.110: icmp_seq=33 ttl=54 time=10.4 ms
64 bytes from 163.53.78.110: icmp_seq=34 ttl=54 time=10.4 ms
^C
--- flipkart.com ping statistics ---
34 packets transmitted, 34 received, 0% packet loss, time 37114ms
rtt min/avg/max/mdev = 10.311/10.569/13.057/0.453 ms

```

*enp2s8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
71	7.714261715	10.1.10.109	10.2.22.125	DNS	74	Standard query 0x137c A www.google.com
72	7.714284467	10.1.10.109	10.2.22.125	DNS	74	Standard query 0xa353 AAAA www.google.com
89	9.336944714	10.1.10.109	10.2.22.125	DNS	74	Standard query 0x23e9 A www.google.com
90	9.336978899	10.1.10.109	10.2.22.125	DNS	74	Standard query 0x0368 AAAA www.google.com
103	10.719713390	10.1.10.1	10.1.10.109	ICMP	102	Destination unreachable (Host unreachable)
112	11.991093963	10.1.10.109	10.2.22.125	DNS	83	Standard query 0x733e A flipkart.pesuec.pes.edu
113	11.991123613	10.1.10.109	10.2.22.125	DNS	83	Standard query 0xe338 AAAA flipkart.pesuec.pes.edu
123	12.716509141	10.1.10.109	192.168.3.2	DNS	74	Standard query 0x84e4 A www.google.com
124	12.716548123	10.1.10.109	8.8.8.8	DNS	74	Standard query 0x84e4 A www.google.com
125	12.716674084	10.1.10.109	192.168.3.2	DNS	74	Standard query 0x8881 AAAA www.google.com

Frame 71: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: Micro-St_79:54:5a (00:19:db:79:54:5a), Dst: HewlettP_0b:39:80 (2c:59:e5:0b:39:80)
 Internet Protocol Version 4, Src: 10.1.10.109, Dst: 10.2.22.125
 User Datagram Protocol, Src Port: 35602, Dst Port: 53
 Domain Name System (query)

2c 59 e5 0b 39 80 00 19 db 79 54 5a 08 00 45 00 ,Y 9... yTZ E
 00 3c cd f9 40 00 40 11 37 cb 0a 01 0a 6d 0a 02 < @ 7... m
 16 7d 8b 12 00 35 00 28 9d 46 13 7c 01 00 00 01 }... 5 (F |...
 00 00 00 00 00 00 03 77 77 77 06 6f 6f 6f 6cw ww googl
 65 03 63 6f 6d 00 00 01 00 01 e.com...

Domain Name System: Protocol Packets: 3785 - Displayed: 257 (6.8%) Profile: Default

Task 3: Set Up a Local DNS Server

STEP 1:

```
GNU nano 2.5.3      File: /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    dump-file "/var/cache/bind/dump.db";
}
```

STEP 2:

```
pesit@PESU-23: ~
pesit@PESU-23:~$ sudo nautilus
[sudo] password for pesit:

(nautilus:7151): Gtk-WARNING **: Failed to register client: GDBus.Error:org.freedesktop.DBus.E
nager was not provided by any .service files

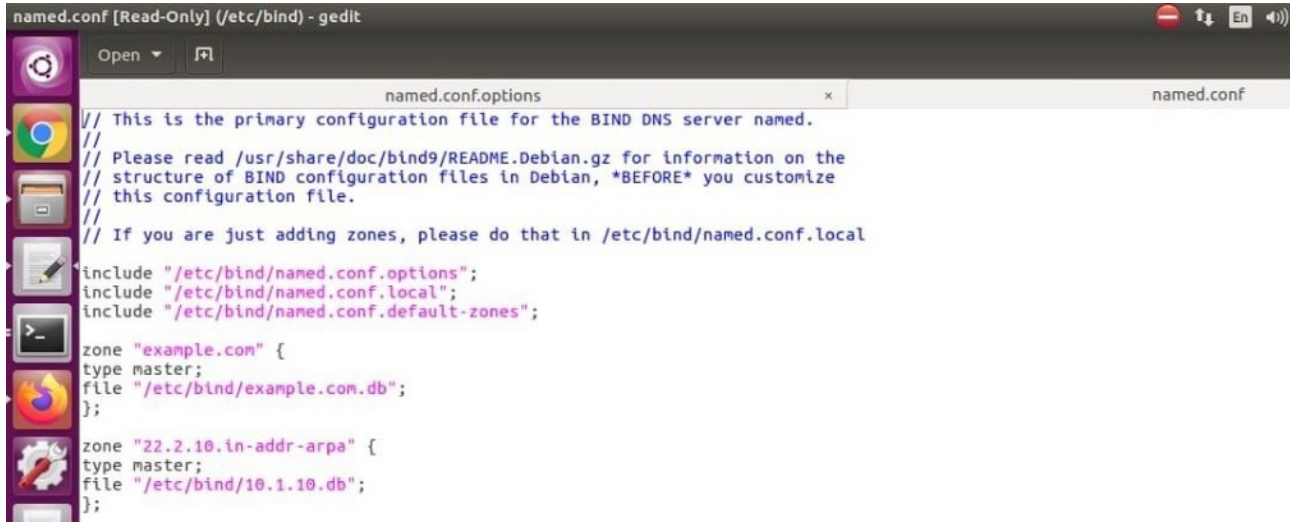
** (nautilus:7151): CRITICAL **: Another desktop manager in use; desktop window won't be creat
Nautilus-Shares-Messag: Called "net usershare info" but it failed: 'net usershare' returned er
ectory /var/lib/samba/usershares. Error No such file or directory
Please ask your system administrator to enable user sharing.

^Z
[1]+  Stopped                  sudo nautilus
pesit@PESU-23:~$ sudo service bind9 restart
pesit@PESU-23:~$
```

```
34 packets transmitted, 34 received, 0% packet loss, time 37114ms
rtt min/avg/max/mdev = 10.311/10.569/13.057/0.453 ms
root@PESU:~# sudo rndc dumpdb -cache
No command 'sudu' found, did you mean:
  Command 'tudu' from package 'tudu' (universe)
  Command 'sudo' from package 'sudo' (main)
  Command 'sudo' from package 'sudo-ldap' (universe)
sudu: command not found
root@PESU:~# sudo rndc dumpdb -cache
root@PESU:~#
```

Task 4: Host a Zone in the Local DNS server.

STEP 1:



```
named.conf [Read-Only] (/etc/bind) - gedit
named.conf.options
named.conf

// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "example.com" {
    type master;
    file "/etc/bind/example.com.db";
};

zone "22.2.10.in-addr-arpa" {
    type master;
    file "/etc/bind/10.1.10.db";
};
```

STEP 2:

```
$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.

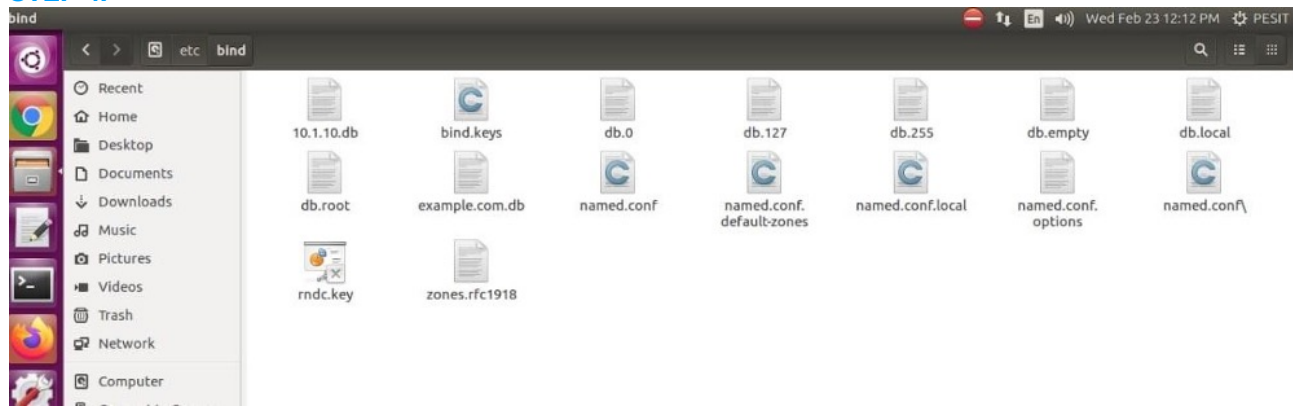
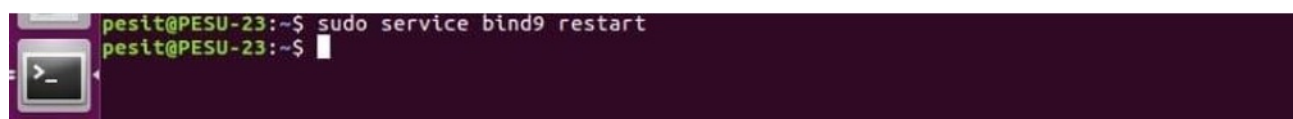
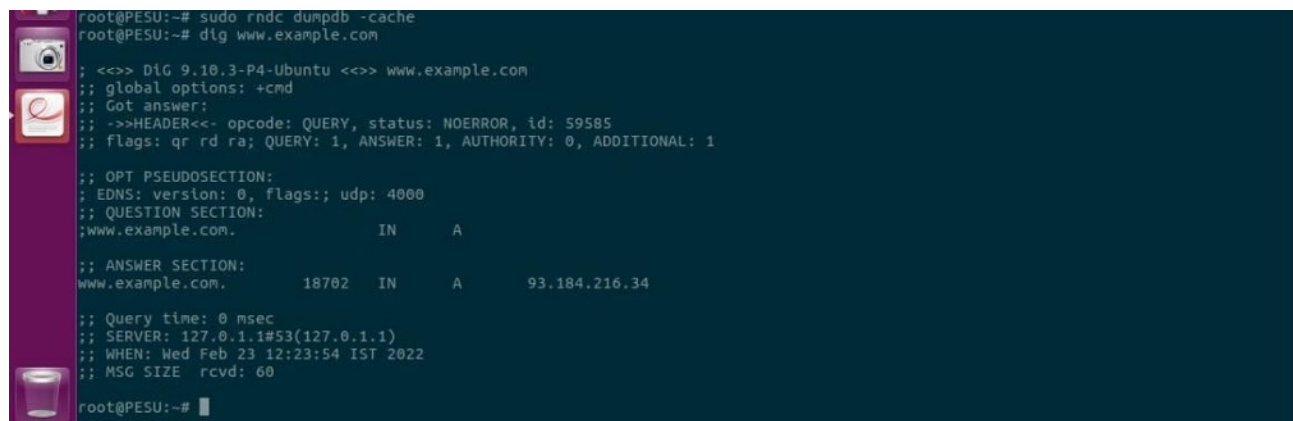
www    IN      A    10.2.22.101
mail   IN      A    10.2.22.102
ns     IN      A    10.2.22.10
*.example.com. IN  A  10.2.22.100
```

STEP 3:

```
$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.
```


STEP 4:**Task 5: Restart the BIND server and test****STEP 1:****STEP 2:****STEP 3:**

1 0.00000000	Azurewav_56:b7:ed	ARP	62 Who has 10.2.22.101? Tell 10.2.22.171
2 1.00000000	Azurewav_56:b7:ed	ARP	62 Who has 10.2.22.161? Tell 10.2.22.171
3 8.029680511	::1	UDP	65 42520 → 42520 Len=1
4 8.029707882	10.2.22.195	DNS	88 Standard query 0x1624 A www.example.com OPT
5 8.030388651	10.2.22.184	DNS	137 Standard query response 0x1624 A www.example.com A 10.2.22.101 NS ns.example.com A 10.2.22.10 OPT
6 9.120902499	Azurewav_56:b7:ed	ARP	62 Who has 10.2.22.161? Tell 10.2.22.171
7 9.999525402	Azurewav_56:b7:ed	ARP	62 Who has 10.2.22.161? Tell 10.2.22.171
8 10.999577685	Azurewav_56:b7:ed	ARP	62 Who has 10.2.22.161? Tell 10.2.22.171
9 13.040903664	Giga-Byt_dc:e3:e9	ARP	62 Who has 10.2.22.195? Tell 10.2.22.184
10 13.040932978	Giga-Byt_76:0c:f5	ARP	44 10.2.22.195 is at e0:d5:5e:76:0c:f5
11 19.156379156	Azurewav_56:b7:ed	ARP	62 Who has 10.2.22.161? Tell 10.2.22.171
12 20.000032310	Azurewav_56:b7:ed	ARP	62 Who has 10.2.22.161? Tell 10.2.22.171

STEP 4:

The screenshot shows a Linux desktop environment with a purple-themed desktop background. The top panel displays the system clock at 12:41 PM. The main workspace contains two windows: Wireshark and Mozilla Firefox.

Wireshark Window:

- File:** FBtGUSzH05mLL9Aq.pdf
- Filter:** dns
- Packet List:**
 - 438 66.373164959 10.1.10.159 10.2.22.184 DNS 71 Standard query 0x5604 A e.edim.co
 - 439 66.373193784 10.1.10.159 10.2.22.184 DNS 71 Standard query 0x86bc AAAA e.edim.co
 - 464 71.374958221 127.0.0.1 127.0.1.1 DNS 71 Standard query 0x5604 A e.edim.co
 - 465 71.374993727 127.0.0.1 127.0.1.1 DNS 71 Standard query 0x86bc AAAA e.edim.co
 - 466 71.375077284 10.1.10.159 192.168.3.2 DNS 71 Standard query 0x48c5 A e.edim.co
 - 467 71.375098721 10.1.10.159 8.8.8.8 DNS 71 Standard query 0x48c5 A e.edim.co
 - 468 71.375111978 10.1.10.159 10.2.22.184 DNS 71 Standard query 0x48c5 A e.edim.co
 - 469 71.375152186 10.1.10.159 8.8.8.8 DNS 71 Standard query 0x2c62 AAAA e.edim.co
 - 470 71.375806626 192.168.3.2 10.1.10.159 DNS 178 Standard query response 0x48c5 A e.edim.co CNAME d269ufzyv97j...
 - 471 71.375899329 127.0.1.1 127.0.0.1 DNS 178 Standard query response 0x5604 A e.edim.co CNAME d269ufzyv97j...
- Packet Details (Packet 468):**
 - Frame 468: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
 - Linux cooked capture
 - Internet Protocol Version 4, Src: 10.1.10.159, Dst: 10.2.22.184
 - User Datagram Protocol, Src Port: 48424, Dst Port: 53
 - Domain Name System (query)
- Packet Bytes:**

```

0000 00 04 00 01 00 00 00 19 db 78 1f 45 00 08 00 00 .....x-E....
0010 45 00 00 37 a0 a8 40 00 40 11 64 b4 0a 01 0a 9f E-7-@-@-d-
0020 0a 02 16 b8 9d e8 00 35 00 23 a5 c5 48 c5 01 00 .....5-#-H-
0030 00 01 00 00 00 00 00 00 01 65 04 65 64 69 6d 02 .....e.edim-
0040 63 6f 00 00 01 00 01 co.....

```

Mozilla Firefox Window:

- Address Bar:** You are here
- Page Title:** Wireshark - Packet 1233 - any
- Content:**
 - Recursion desired: Do query recursively
 - Recursion available: Server can do recursive queries
 - 0 = Z: reserved (0)
 - 0 = Answer authenticated: Answer/authority portion was not authenticated by the serv...
 - 0 = Non-authenticated data: Unacceptable
 - 0000 = Reply code: No error (0)
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries:
 - example.org: type A, class IN
 - Answers:
 - example.org: type A, class IN, addr 93.184.216.34
 - Name: example.org
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 8067
 - Data length: 4
 - Address: 93.184.216.34

Packet Bytes (Wireshark):

```

0000 00 00 03 04 00 00 00 00 00 00 00 40 00 08 00 .....@-
0010 45 00 00 49 31 7f 40 00 40 11 0a 23 7f 00 01 01 E-11@-@-#-
0020 7f 00 00 01 00 35 a8 52 00 35 ff 48 c6 49 01 00 ...-5-R-5-H-1-
0030 00 01 00 01 00 00 00 00 07 65 78 61 6d 70 6c 65 .....example
0040 03 6f 72 67 00 00 01 00 01 c0 0c 00 01 00 01 00 ...org.....
0050 00 1f 83 00 04 5d b8 d8 22 .....}..

```

Packet List (Wireshark):

- 468 71.375111978 10.1.10.159 10.2.22.184 DNS 71 Standard query 0x48c5 A e.edim.co
- 469 71.375152186 10.1.10.159 8.8.8.8 DNS 71 Standard query 0x2c62 AAAA e.edim.co
- 470 71.375806626 192.168.3.2 10.1.10.159 DNS 178 Standard query response 0x48c5 A e.edim.co CNAME d269ufzyv97j...
- 471 71.375899329 127.0.1.1 127.0.0.1 DNS 178 Standard query response 0x5604 A e.edim.co CNAME d269ufzyv97j...

Packet Details (Wireshark):

- Frame 468: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
- Linux cooked capture
- Internet Protocol Version 4, Src: 10.1.10.159, Dst: 10.2.22.184
- User Datagram Protocol, Src Port: 48424, Dst Port: 53
- Domain Name System (query)

Packet Bytes (Wireshark):

```

0000 00 04 00 01 00 00 00 19 db 78 1f 45 00 08 00 00 .....x-E....
0010 45 00 00 37 a0 a8 40 00 40 11 64 b4 0a 01 0a 9f E-7-@-@-d-
0020 0a 02 16 b8 9d e8 00 35 00 23 a5 c5 48 c5 01 00 .....5-#-H-
0030 00 01 00 00 00 00 00 00 01 65 04 65 64 69 6d 02 .....e.edim-
0040 63 6f 00 00 01 00 01 co.....

```

```
root@PESU:~# sudo rndc dumpdb -cache
root@PESU:~#
```