

Project Name: **Cybersecurity Club's Raspberry Pi Networking Project**

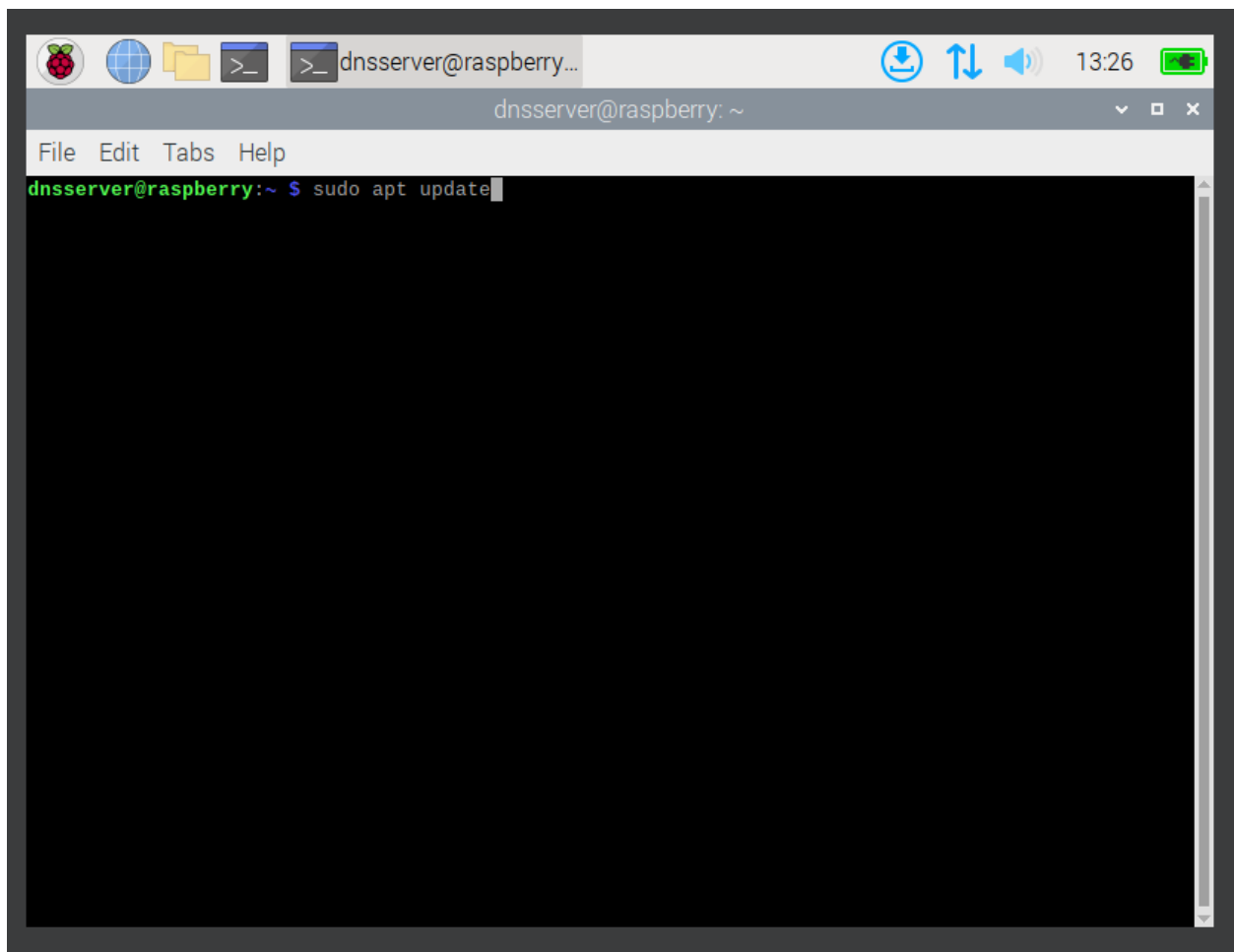
Date: **June 30, 2023**

Created by: **Jason Patrick Salerno**

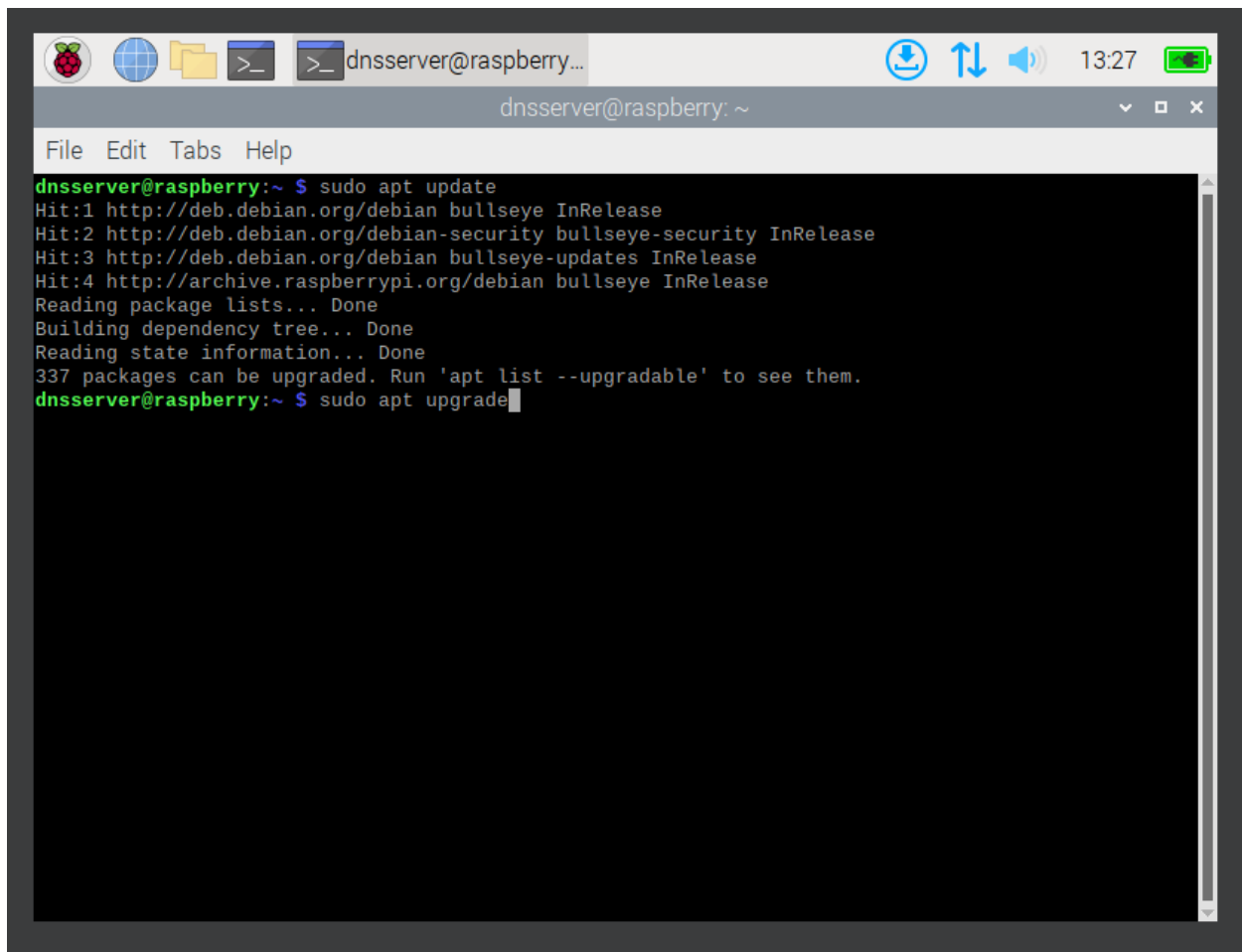
Purpose: **Documentation for the DNS Server**

Set up a Raspberry Pi as a DNS Server

1. I opened the Terminal, and typed the following: **sudo apt update**, this command will update the local package cache, refreshes package lists, and check for updates

A screenshot of a Raspberry Pi terminal window. The window has a title bar with icons for Raspberry Pi, a globe, a folder, and two terminal icons. The title text is 'dnsserver@raspberrypi...'. On the right side of the title bar are icons for a download arrow, a double-headed vertical arrow, a speaker, the time '13:26', and a battery icon. Below the title bar is a menu bar with 'File', 'Edit', 'Tabs', and 'Help'. The main area of the terminal is black with green text. The prompt is 'dnsserver@raspberrypi:~' followed by a blue '\$' symbol and the command 'sudo apt update' with a cursor at the end.

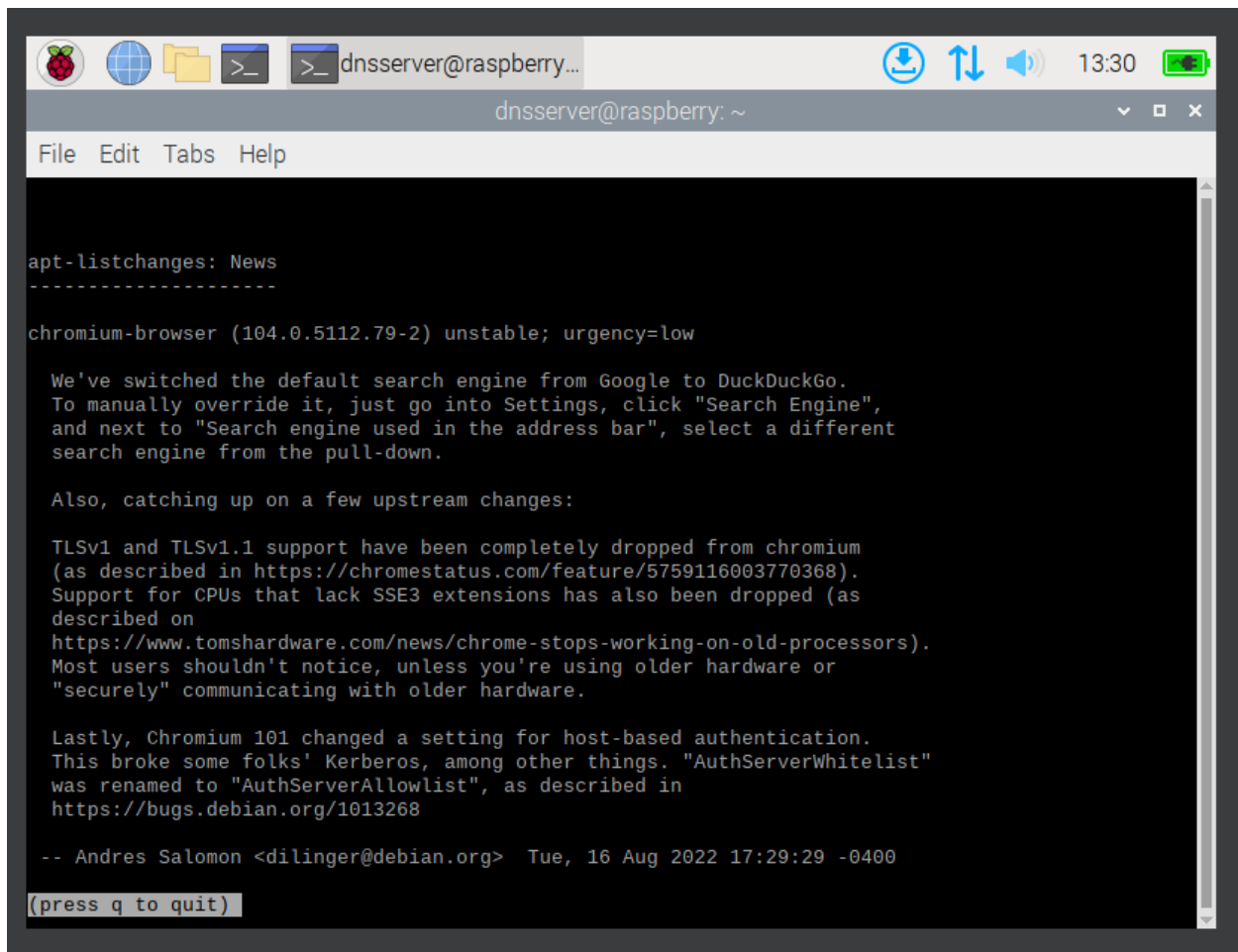
2. I typed the command: **sudo apt upgrade**, this command will upgrade/update the packages that are already installed on the raspberry pi OS.



The screenshot shows a terminal window titled 'dnsserver@raspberrypi: ~'. The window has a menu bar with 'File', 'Edit', 'Tabs', and 'Help'. The terminal output shows the command 'sudo apt update' being executed. The output indicates that four package lists were updated from various sources (deb.debian.org and archive.raspberrypi.org). It then shows the package lists being read and the dependency tree being built successfully. Finally, it states that 337 packages can be upgraded and suggests running 'apt list --upgradable' to see them. The prompt 'dnsserver@raspberrypi:~ \$' is followed by 'sudo apt upgrade'.

```
dnsserver@raspberrypi:~ $ sudo apt update
Hit:1 http://deb.debian.org/debian bullseye InRelease
Hit:2 http://deb.debian.org/debian-security bullseye-security InRelease
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease
Hit:4 http://archive.raspberrypi.org/debian bullseye InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
337 packages can be upgraded. Run 'apt list --upgradable' to see them.
dnsserver@raspberrypi:~ $ sudo apt upgrade
```

3. After the Installation is done, it will display the **apt-listchanges: News**, what changes have occurred.



```
dnsserver@raspberrypi: ~
File Edit Tabs Help

apt-listchanges: News
-----

chromium-browser (104.0.5112.79-2) unstable; urgency=low

We've switched the default search engine from Google to DuckDuckGo.
To manually override it, just go into Settings, click "Search Engine",
and next to "Search engine used in the address bar", select a different
search engine from the pull-down.

Also, catching up on a few upstream changes:

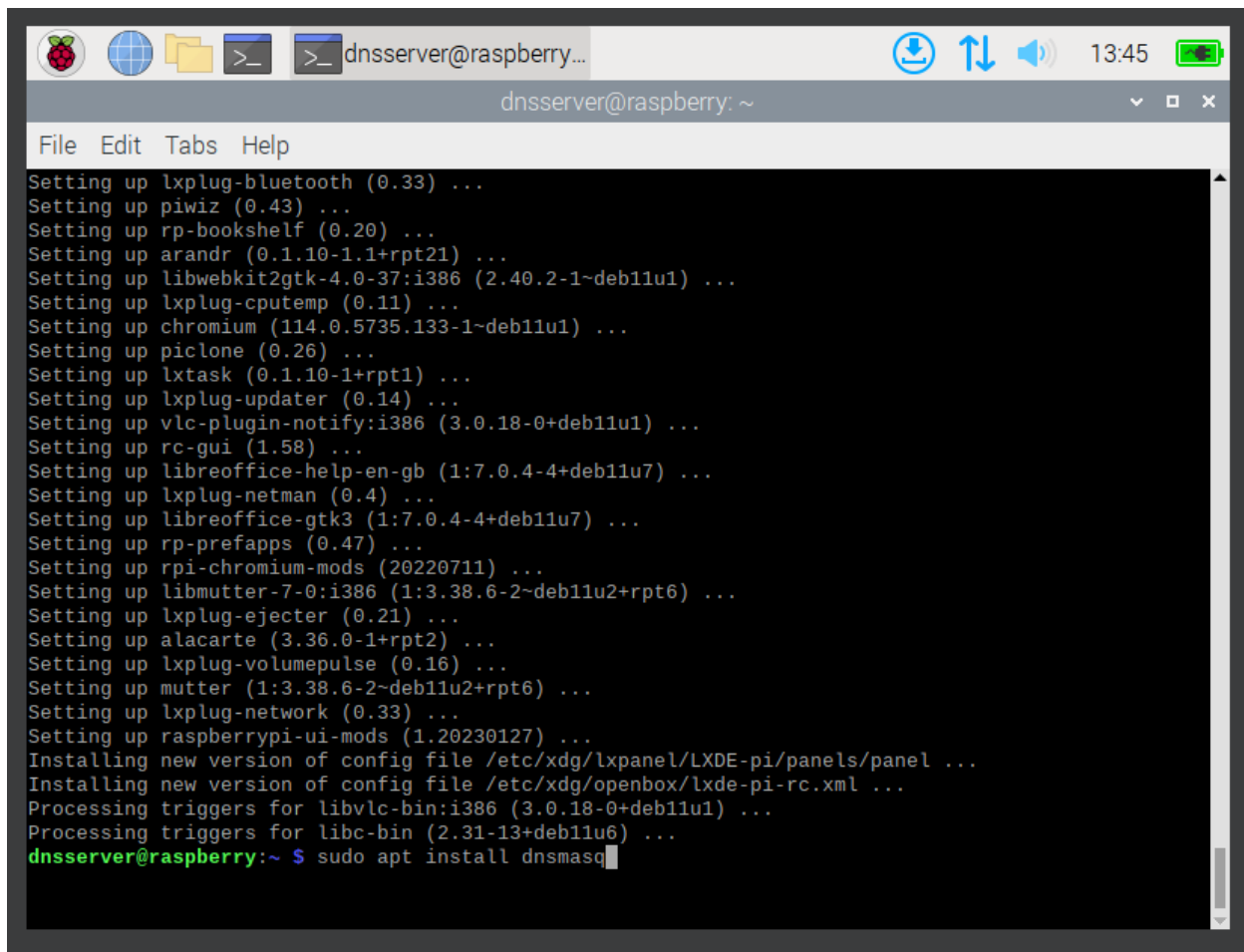
TLSv1 and TLSv1.1 support have been completely dropped from chromium
(as described in https://chromestatus.com/feature/5759116003770368).
Support for CPUs that lack SSE3 extensions has also been dropped (as
described on
https://www.tomshardware.com/news/chrome-stops-working-on-old-processors).
Most users shouldn't notice, unless you're using older hardware or
"securely" communicating with older hardware.

Lastly, Chromium 101 changed a setting for host-based authentication.
This broke some folks' Kerberos, among other things. "AuthServerWhitelist"
was renamed to "AuthServerAllowlist", as described in
https://bugs.debian.org/1013268

-- Andres Salomon <dilinger@debian.org> Tue, 16 Aug 2022 17:29:29 -0400

(press q to quit)
```

4. I've typed the following command: **sudo apt install dnsmasq**, this command will install the **dnsmasq** software package on our Raspberry Pi OS.



```
dnsserver@raspberrypi: ~
File Edit Tabs Help
Setting up lxplug-bluetooth (0.33) ...
Setting up piwiz (0.43) ...
Setting up rp-bookshelf (0.20) ...
Setting up arandr (0.1.10-1+rpt21) ...
Setting up libwebkit2gtk-4.0-37:i386 (2.40.2-1~deb11u1) ...
Setting up lxplug-cputemp (0.11) ...
Setting up chromium (114.0.5735.133-1~deb11u1) ...
Setting up piclone (0.26) ...
Setting up lxtask (0.1.10-1+rpt1) ...
Setting up lxplug-updater (0.14) ...
Setting up vlc-plugin-notify:i386 (3.0.18-0+deb11u1) ...
Setting up rc-gui (1.58) ...
Setting up libreoffice-help-en-gb (1:7.0.4-4+deb11u7) ...
Setting up lxplug-netman (0.4) ...
Setting up libreoffice-gtk3 (1:7.0.4-4+deb11u7) ...
Setting up rp-prefapps (0.47) ...
Setting up rpi-chromium-mods (20220711) ...
Setting up libmutter-7-0:i386 (1:3.38.6-2~deb11u2+rpt6) ...
Setting up lxplug-ejecter (0.21) ...
Setting up alacarte (3.36.0-1+rpt2) ...
Setting up lxplug-volumepulse (0.16) ...
Setting up mutter (1:3.38.6-2~deb11u2+rpt6) ...
Setting up lxplug-network (0.33) ...
Setting up raspberrypi-ui-mods (1.20230127) ...
Installing new version of config file /etc/xdg/lxpanel/LXDE-pi/panels/panel ...
Installing new version of config file /etc/xdg/openbox/lxde-pi-rc.xml ...
Processing triggers for libvlc-bin:i386 (3.0.18-0+deb11u1) ...
Processing triggers for libc-bin (2.31-13+deb11u6) ...
dnsserver@raspberrypi:~$ sudo apt install dnsmasq
```

5. I've Pressed Y and hit enter, to accept 1335 KB of additional disk space.

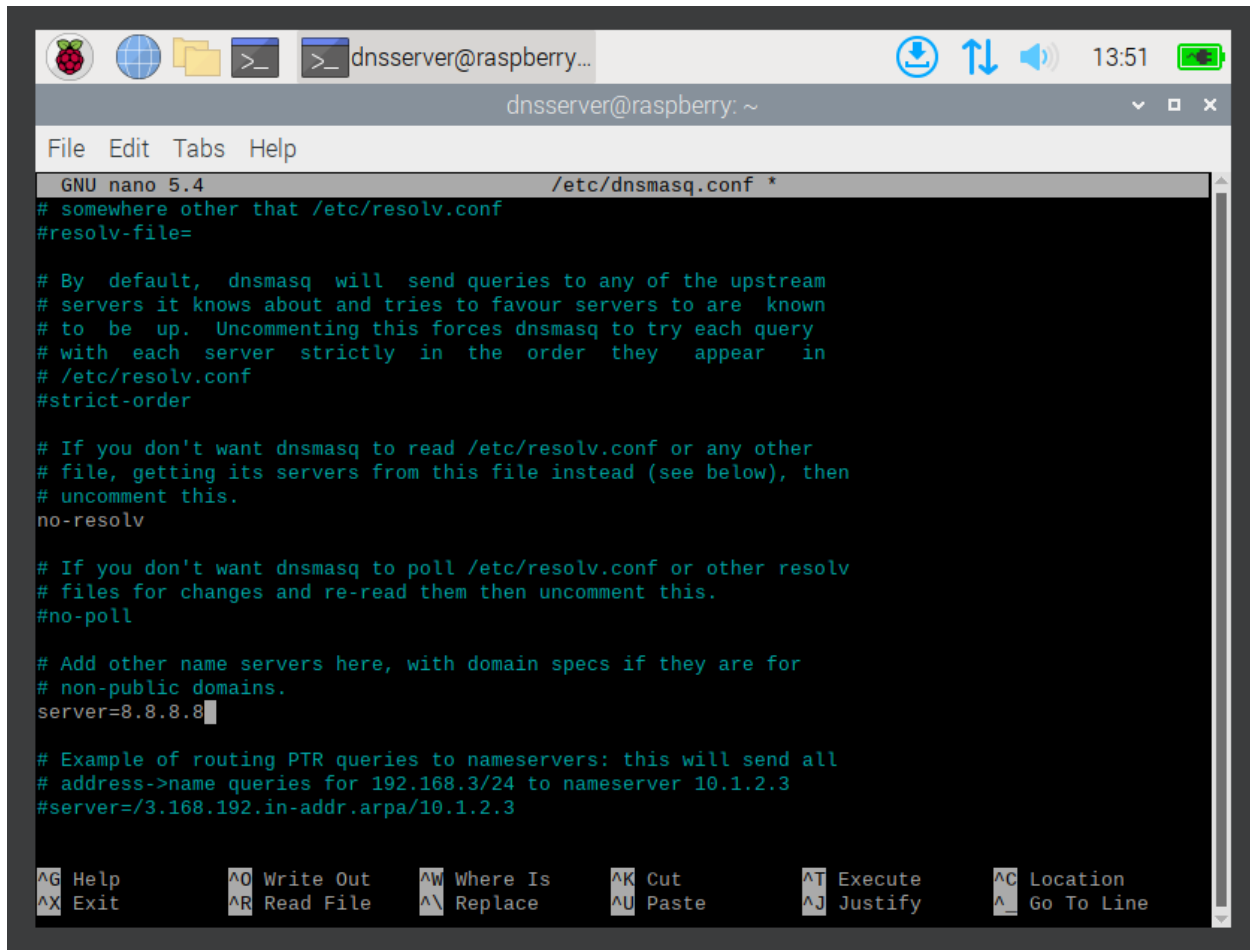
The screenshot shows a terminal window on a Raspberry Pi. The title bar indicates the user is 'dnsserver@raspberrypi...'. The terminal output shows the following sequence of events:

- Installation of several packages: libreoffice-help-en-gb, lxplug-netman, libreoffice-gtk3, rp-prefapps, rpi-chromium-mods, libmutter-7-0:i386, lxplug-ejecter, alacarte, lxplug-volumepulse, mutter, lxplug-network, and raspberrypi-ui-mods.
- Installation of configuration files for LXDE and Openbox.
- Processing of triggers for libvlc-bin and libc-bin.
- Execution of the command: `dnsserver@raspberrypi:~$ sudo apt install dnsmasq`
- Reading package lists and building the dependency tree.
- Reading state information.
- Notification that some packages (libopengl0, sse3-support) are no longer required.
- Notification that additional packages (dns-root-data, dnsmasq-base, libnetfilter-conntrack3, libnftnl) will be installed.
- Notification that new packages (dnsmasq, dnsmasq-base, libnetfilter-conntrack3, libnftnl) will be installed.
- Summary: 0 upgraded, 5 newly installed, 0 to remove, 1 not upgraded. Need to get 565 kB of archives.
- Notification that 1,335 kB of additional disk space will be used.
- Prompt: 'Do you want to continue? [Y/n] Y'

6. I modified the dnsmasq.conf file, through this command: **sudo nano /etc/dnsmasq.conf** , using the keys **CTRL+W** to find and uncomment the

following: **domain-needed**, **bogus-priv**, **no-resolv**. The next line to find is **#server=/localnet/192.168.0.1** , and removing it and replacing it with **server=8.8.8.8** and **server=8.8.4.4** next is finding

Note: adding **server=8.8.8.8**, **server=8.8.4.4** makes use of Google's DNS Servers for upstream nameservers.



```
GNU nano 5.4 /etc/dnsmasq.conf *
# somewhere other than /etc/resolv.conf
#resolv-file=

# By default, dnsmasq will send queries to any of the upstream
# servers it knows about and tries to favour servers to are known
# to be up. Uncommenting this forces dnsmasq to try each query
# with each server strictly in the order they appear in
# /etc/resolv.conf
#strict-order

# If you don't want dnsmasq to read /etc/resolv.conf or any other
# file, getting its servers from this file instead (see below), then
# uncomment this.
no-resolv

# If you don't want dnsmasq to poll /etc/resolv.conf or other resolv
# files for changes and re-read them then uncomment this.
#no-poll

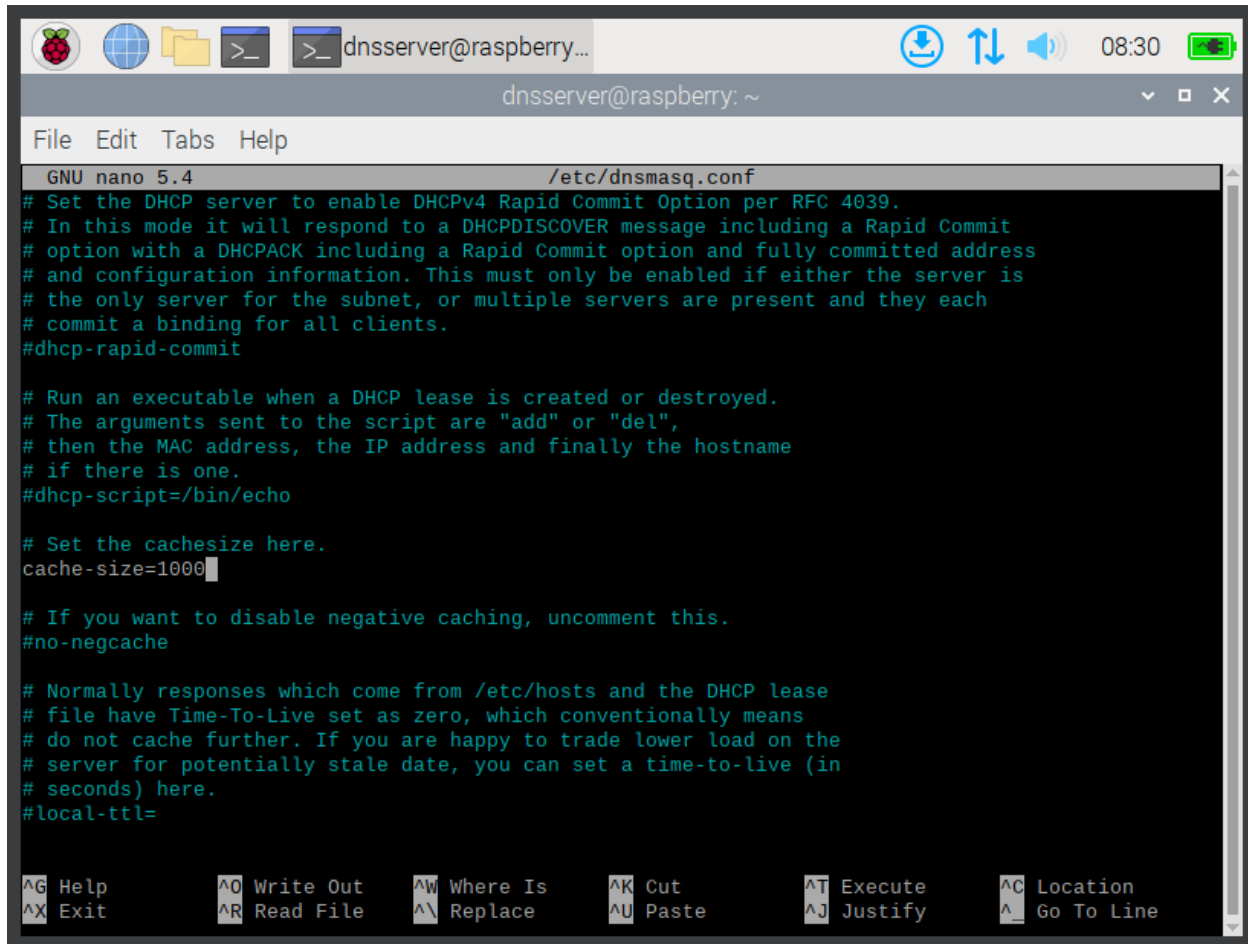
# Add other name servers here, with domain specs if they are for
# non-public domains.
server=8.8.8.8

# Example of routing PTR queries to nameservers: this will send all
# address->name queries for 192.168.3/24 to nameserver 10.1.2.3
#server=/3.168.192.in-addr.arpa/10.1.2.3

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

7. The next thing to change is by uncommenting **#cache-size=150** and changing the value from **150** to **1000**. I'd save the file using **CTRL+X** then pressing **Y** and hitting enter to keep the changes.

Note: More DNS queries are avoided by the DNSMasq cache when the cache size is increased. The DNS lookup time is decreased, which enhances network performance.



The screenshot shows a terminal window on a Raspberry Pi. The top bar displays the user 'dnsserver@raspberr...' and the time '08:30'. The terminal window title is 'dnsserver@raspberr: ~'. The editor is GNU nano 5.4, editing the file /etc/dnsmasq.conf. The file content includes comments about DHCPv4 Rapid Commit, DHCP script, cache size, and negative caching. The current line being edited is 'cache-size=1000'. The bottom status bar shows various keyboard shortcuts for nano editor.

```
GNU nano 5.4 /etc/dnsmasq.conf
# Set the DHCP server to enable DHCPv4 Rapid Commit Option per RFC 4039.
# In this mode it will respond to a DHCPDISCOVER message including a Rapid Commit
# option with a DHCPACK including a Rapid Commit option and fully committed address
# and configuration information. This must only be enabled if either the server is
# the only server for the subnet, or multiple servers are present and they each
# commit a binding for all clients.
#dhcp-rapid-commit

# Run an executable when a DHCP lease is created or destroyed.
# The arguments sent to the script are "add" or "del",
# then the MAC address, the IP address and finally the hostname
# if there is one.
#dhcp-script=/bin/echo

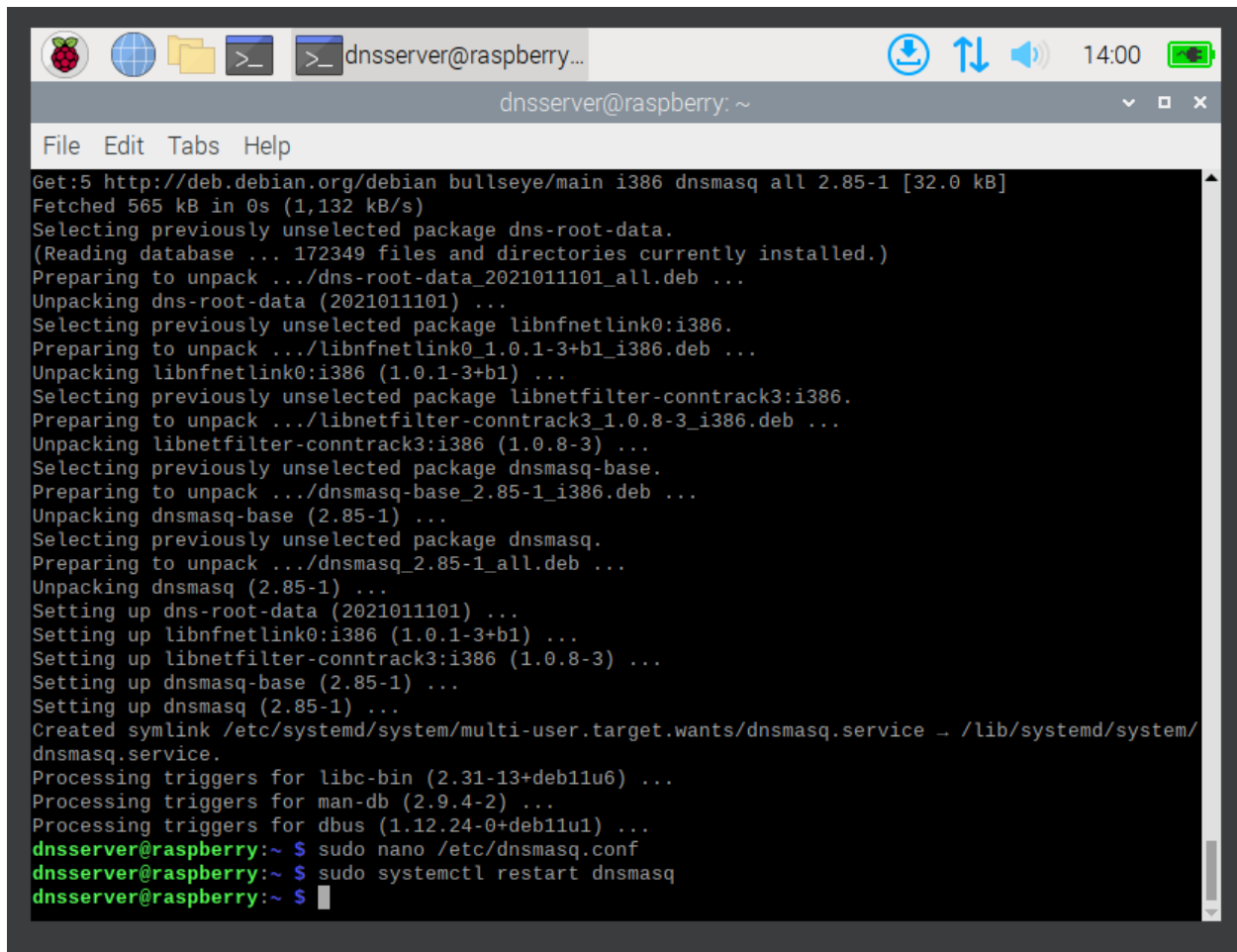
# Set the cachesize here.
cache-size=1000

# If you want to disable negative caching, uncomment this.
#no-negcache

# Normally responses which come from /etc/hosts and the DHCP lease
# file have Time-To-Live set as zero, which conventionally means
# do not cache further. If you are happy to trade lower load on the
# server for potentially stale data, you can set a time-to-live (in
# seconds) here.
#local-ttl=

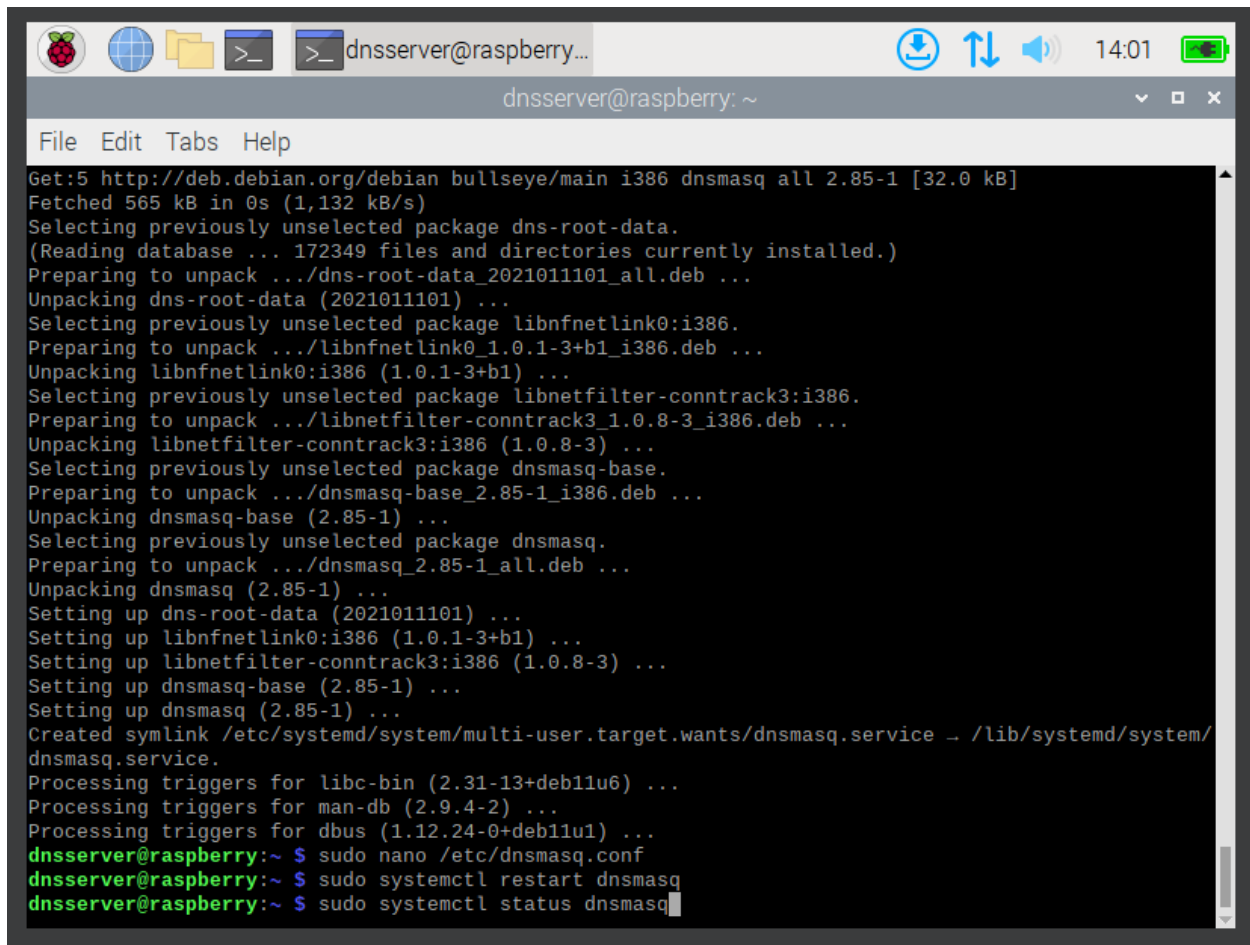
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

8. I had to restart the dnsmasq service to apply the changes, using the command:
sudo systemctl restart dnsmasq.



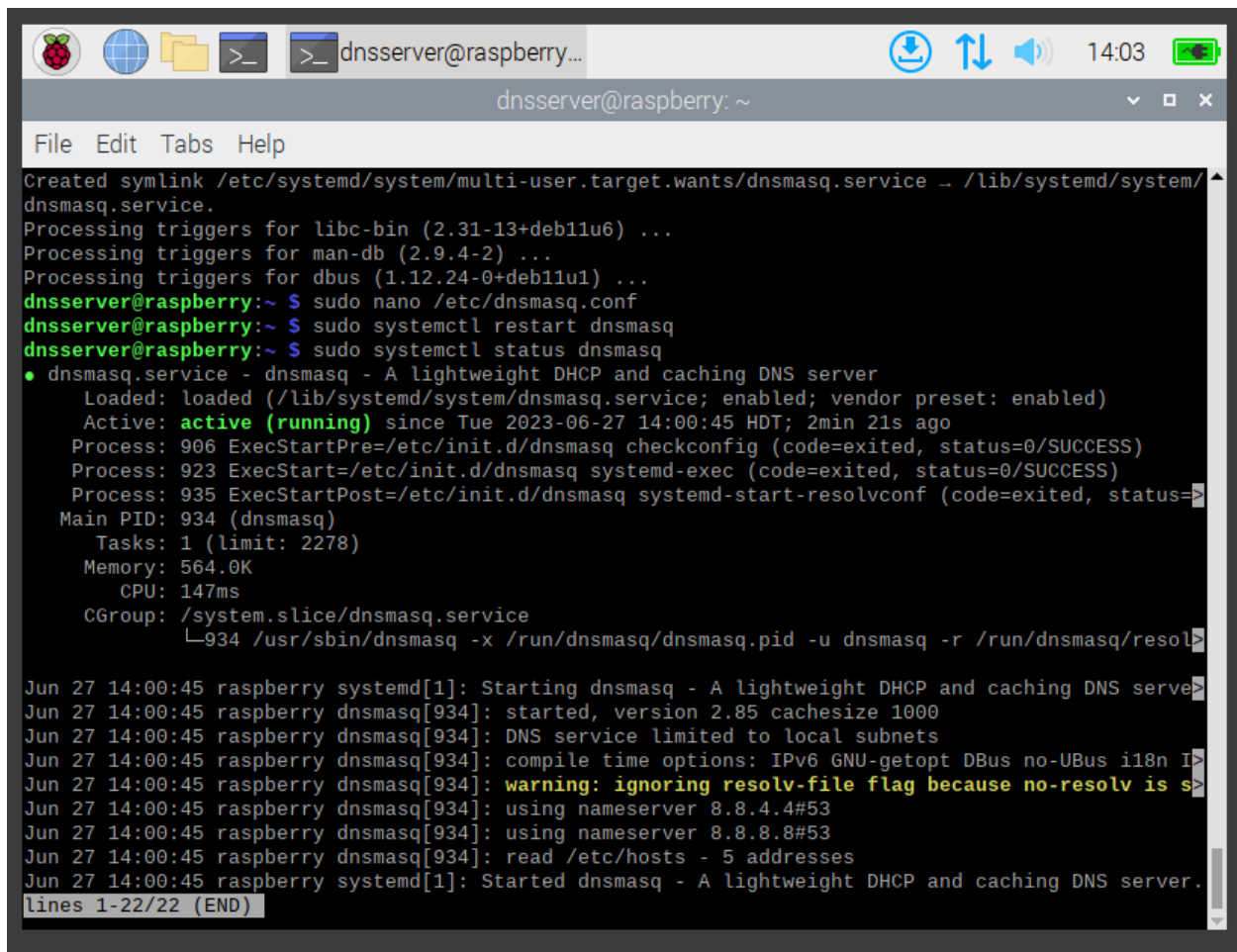
```
Get:5 http://deb.debian.org/debian bullseye/main i386 dnsmasq all 2.85-1 [32.0 kB]
Fetched 565 kB in 0s (1,132 kB/s)
Selecting previously unselected package dns-root-data.
(Reading database ... 172349 files and directories currently installed.)
Preparing to unpack .../dns-root-data_2021011101_all.deb ...
Unpacking dns-root-data (2021011101) ...
Selecting previously unselected package libnftnl:i386.
Preparing to unpack .../libnftnl_1.0.1-3+b1_i386.deb ...
Unpacking libnftnl:i386 (1.0.1-3+b1) ...
Selecting previously unselected package libnetfilter-conntrack3:i386.
Preparing to unpack .../libnetfilter-conntrack3_1.0.8-3_i386.deb ...
Unpacking libnetfilter-conntrack3:i386 (1.0.8-3) ...
Selecting previously unselected package dnsmasq-base.
Preparing to unpack .../dnsmasq-base_2.85-1_i386.deb ...
Unpacking dnsmasq-base (2.85-1) ...
Selecting previously unselected package dnsmasq.
Preparing to unpack .../dnsmasq_2.85-1_all.deb ...
Unpacking dnsmasq (2.85-1) ...
Setting up dns-root-data (2021011101) ...
Setting up libnftnl:i386 (1.0.1-3+b1) ...
Setting up libnetfilter-conntrack3:i386 (1.0.8-3) ...
Setting up dnsmasq-base (2.85-1) ...
Setting up dnsmasq (2.85-1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/dnsmasq.service → /lib/systemd/system/
dnsmasq.service.
Processing triggers for libc-bin (2.31-13+deb11u6) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for dbus (1.12.24-0+deb11u1) ...
dnsserver@raspberrypi:~ $ sudo nano /etc/dnsmasq.conf
dnsserver@raspberrypi:~ $ sudo systemctl restart dnsmasq
dnsserver@raspberrypi:~ $
```

9. Next is to check the status of dnsmasq service, by using the command: **sudo systemctl status dnsmasq**.



```
Get:5 http://deb.debian.org/debian bullseye/main i386 dnsmasq all 2.85-1 [32.0 kB]
Fetched 565 kB in 0s (1,132 kB/s)
Selecting previously unselected package dns-root-data.
(Reading database ... 172349 files and directories currently installed.)
Preparing to unpack .../dns-root-data_2021011101_all.deb ...
Unpacking dns-root-data (2021011101) ...
Selecting previously unselected package libnfnetwork0:i386.
Preparing to unpack .../libnfnetwork0_1.0.1-3+b1_i386.deb ...
Unpacking libnfnetwork0:i386 (1.0.1-3+b1) ...
Selecting previously unselected package libnetfilter-conntrack3:i386.
Preparing to unpack .../libnetfilter-conntrack3_1.0.8-3_i386.deb ...
Unpacking libnetfilter-conntrack3:i386 (1.0.8-3) ...
Selecting previously unselected package dnsmasq-base.
Preparing to unpack .../dnsmasq-base_2.85-1_i386.deb ...
Unpacking dnsmasq-base (2.85-1) ...
Selecting previously unselected package dnsmasq.
Preparing to unpack .../dnsmasq_2.85-1_all.deb ...
Unpacking dnsmasq (2.85-1) ...
Setting up dns-root-data (2021011101) ...
Setting up libnfnetwork0:i386 (1.0.1-3+b1) ...
Setting up libnetfilter-conntrack3:i386 (1.0.8-3) ...
Setting up dnsmasq-base (2.85-1) ...
Setting up dnsmasq (2.85-1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/dnsmasq.service → /lib/systemd/system/dnsmasq.service.
Processing triggers for libc-bin (2.31-13+deb11u6) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for dbus (1.12.24-0+deb11u1) ...
dnsserver@raspberrypi:~ $ sudo nano /etc/dnsmasq.conf
dnsserver@raspberrypi:~ $ sudo systemctl restart dnsmasq
dnsserver@raspberrypi:~ $ sudo systemctl status dnsmasq
```

10. As we can see from the dnsmasq service, it is **active (running)**, which indicates that our Raspberry Pi is running as a DNS server.

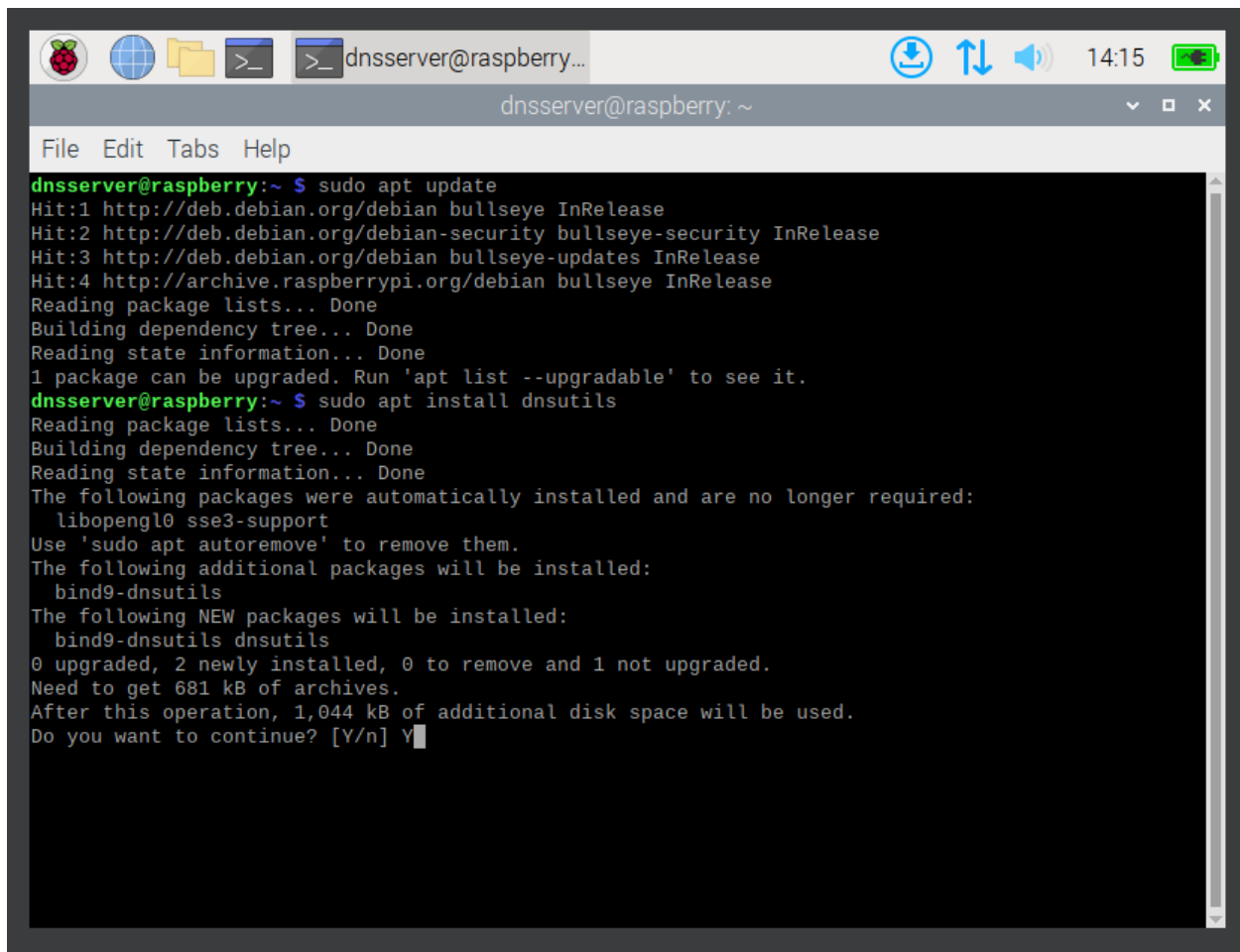


The screenshot shows a terminal window titled 'dnsserver@raspberrypi: ~'. The user has executed several commands to install and manage dnsmasq. The output shows that dnsmasq is now installed and running as a service. The status of the service is displayed, showing it is active and running. The user has also run 'sudo nano /etc/dnsmasq.conf' and 'sudo systemctl restart dnsmasq'. The terminal output includes the following lines:

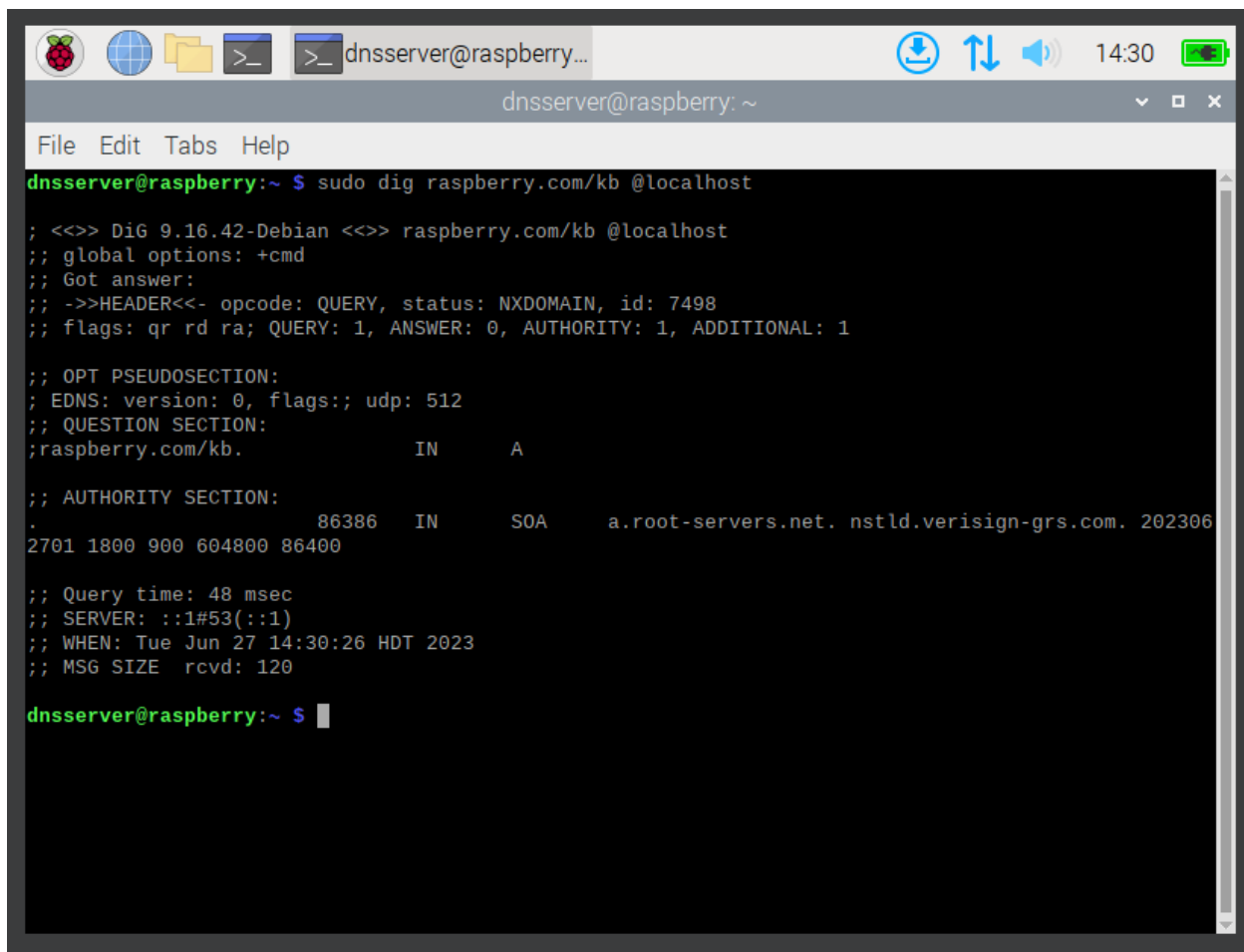
```
Created symlink /etc/systemd/system/multi-user.target.wants/dnsmasq.service → /lib/systemd/system/dnsmasq.service.
Processing triggers for libc-bin (2.31-13+deb11u6) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for dbus (1.12.24-0+deb11u1) ...
dnsserver@raspberrypi:~$ sudo nano /etc/dnsmasq.conf
dnsserver@raspberrypi:~$ sudo systemctl restart dnsmasq
dnsserver@raspberrypi:~$ sudo systemctl status dnsmasq
● dnsmasq.service - dnsmasq - A lightweight DHCP and caching DNS server
   Loaded: loaded (/lib/systemd/system/dnsmasq.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-06-27 14:00:45 HDT; 2min 21s ago
     Process: 906 ExecStartPre=/etc/init.d/dnsmasq checkconfig (code=exited, status=0/SUCCESS)
     Process: 923 ExecStart=/etc/init.d/dnsmasq systemd-exec (code=exited, status=0/SUCCESS)
     Process: 935 ExecStartPost=/etc/init.d/dnsmasq systemd-start-resolvconf (code=exited, status=0/SUCCESS)
    Main PID: 934 (dnsmasq)
       Tasks: 1 (limit: 2278)
      Memory: 564.0K
         CPU: 147ms
      CGroup: /system.slice/dnsmasq.service
              └─934 /usr/sbin/dnsmasq -x /run/dnsmasq/dnsmasq.pid -u dnsmasq -r /run/dnsmasq/resolvconf

Jun 27 14:00:45 raspberrypi systemd[1]: Starting dnsmasq - A lightweight DHCP and caching DNS server.
Jun 27 14:00:45 raspberrypi dnsmasq[934]: started, version 2.85 cachesize 1000
Jun 27 14:00:45 raspberrypi dnsmasq[934]: DNS service limited to local subnets
Jun 27 14:00:45 raspberrypi dnsmasq[934]: compile time options: IPv6 GNU-getopt DBus no-UBus i18n IDN2
Jun 27 14:00:45 raspberrypi dnsmasq[934]: warning: ignoring resolv-file flag because no-resolv is set
Jun 27 14:00:45 raspberrypi dnsmasq[934]: using nameserver 8.8.4.4#53
Jun 27 14:00:45 raspberrypi dnsmasq[934]: using nameserver 8.8.8.8#53
Jun 27 14:00:45 raspberrypi dnsmasq[934]: read /etc/hosts - 5 addresses
Jun 27 14:00:45 raspberrypi systemd[1]: Started dnsmasq - A lightweight DHCP and caching DNS server.
lines 1-22/22 (END)
```

11. The next command I was suppose to run was: **sudo dig raspberry.com/kb @localhost**, however when I runned that command it prompted me that there was no such command (**dig**)therefore I had to run the command: **sudo apt update** to update its packages and run the following command: **sudo apt install dnsutils** to install the necessary tools (**dig**).

A terminal window titled 'dnsserver@raspberrypi: ~' is shown. The window has a menu bar with 'File', 'Edit', 'Tabs', and 'Help'. The terminal output shows the execution of 'sudo apt update' and 'sudo apt install dnsutils'. The update process lists four sources and reports that one package can be upgraded. The install process lists additional packages to be installed (bind9-dnsutils) and new packages (bind9-dnsutils, dnsutils). It also shows disk space requirements and a confirmation prompt which has been answered 'Y'.

12. The next thing to do is finally test it by running the command: **sudo dig raspberry.com/kb @localhost** and as we can see the **query time is 48 msec**.



A terminal window titled "dnsserver@raspberr..." is shown. The window has a menu bar with "File", "Edit", "Tabs", and "Help". The terminal content shows a command being executed: `sudo dig raspberry.com/kb @localhost`. The output is a detailed DNS query result. It starts with a header indicating the query status as NXDOMAIN. The question section shows the query for `raspberry.com/kb.` in the `IN` class. The authority section shows the root servers. The query time is 48 msec. The window also shows a status bar at the top with system icons and a clock showing 14:30.

```
dnsserver@raspberr...
File Edit Tabs Help
dnsserver@raspberr:~ $ sudo dig raspberry.com/kb @localhost

; <<> DiG 9.16.42-Debian <<> raspberry.com/kb @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 7498
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;raspberry.com/kb.                IN      A

;; AUTHORITY SECTION:
.                86386   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 202306
2701 1800 900 604800 86400

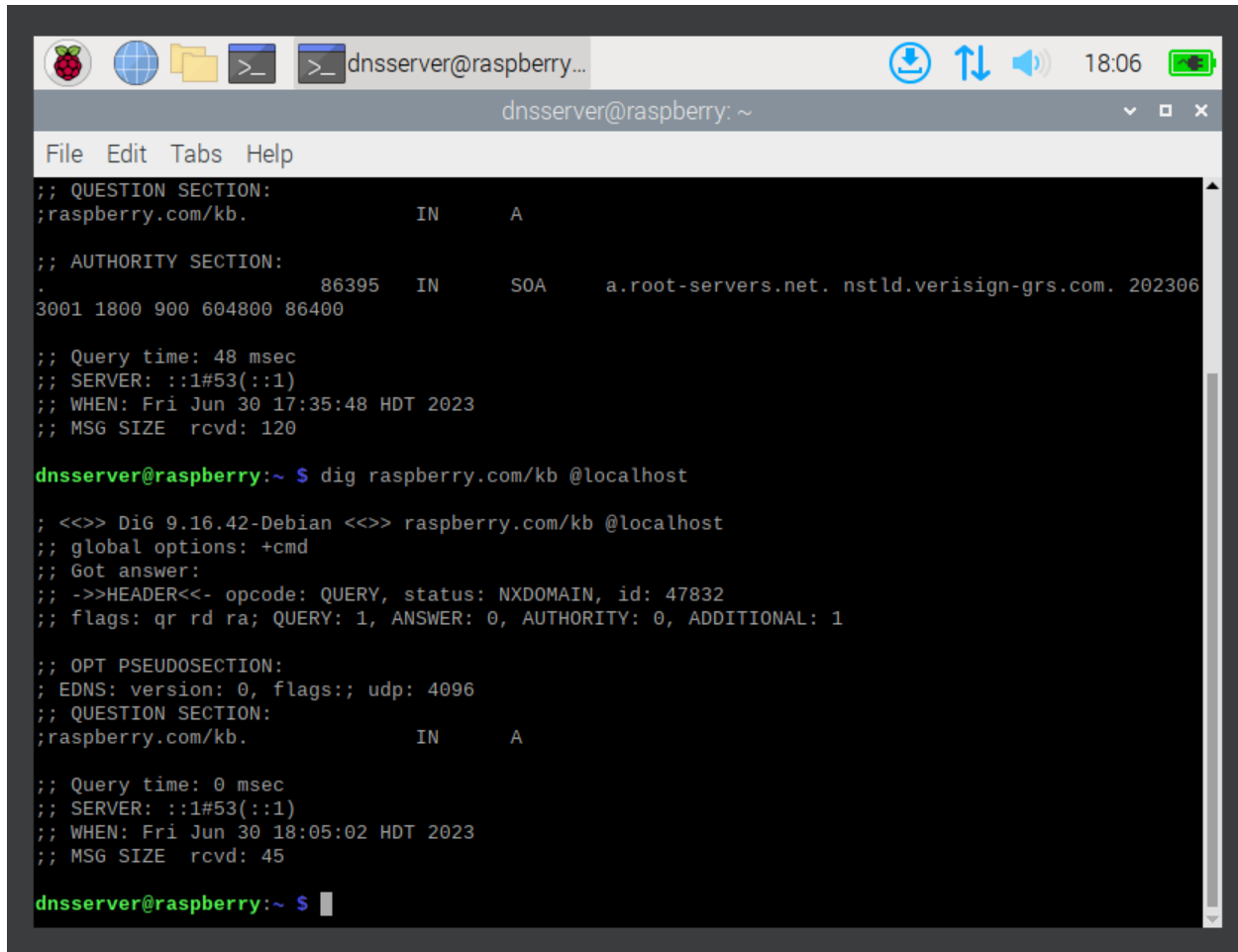
;; Query time: 48 msec
;; SERVER: ::1#53(::1)
;; WHEN: Tue Jun 27 14:30:26 HDT 2023
;; MSG SIZE rcvd: 120

dnsserver@raspberr:~ $
```

13. I want to test it once again to see if the query time has changed, and as it displays the query time has to **0 msec** we can verify that the address has been cached.

Note: the next step supposedly is to configure the endpoints/devices to use the Raspberry Pi as a DNS server however that is beyond this documentation.

References: <https://phoenixnap.com/kb/raspberry-pi-dns-server>

A screenshot of a terminal window on a Raspberry Pi. The window title is 'dnsserver@raspberrypi: ~'. The terminal shows the output of a 'dig' command. The first query shows a query time of 48 msec and a status of NXDOMAIN. The second query, after a cache refresh, shows a query time of 0 msec, indicating the result is cached. The terminal text is as follows:

```
dnsserver@raspberrypi:~$ dig raspberry.com/kb @localhost

; <<>> DiG 9.16.42-Debian <<>> raspberry.com/kb @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 47832
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;raspberry.com/kb.                IN      A

;; Query time: 48 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Jun 30 17:35:48 HDT 2023
;; MSG SIZE rcvd: 120

dnsserver@raspberrypi:~$ S dig raspberry.com/kb @localhost

; <<>> DiG 9.16.42-Debian <<>> raspberry.com/kb @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 47832
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

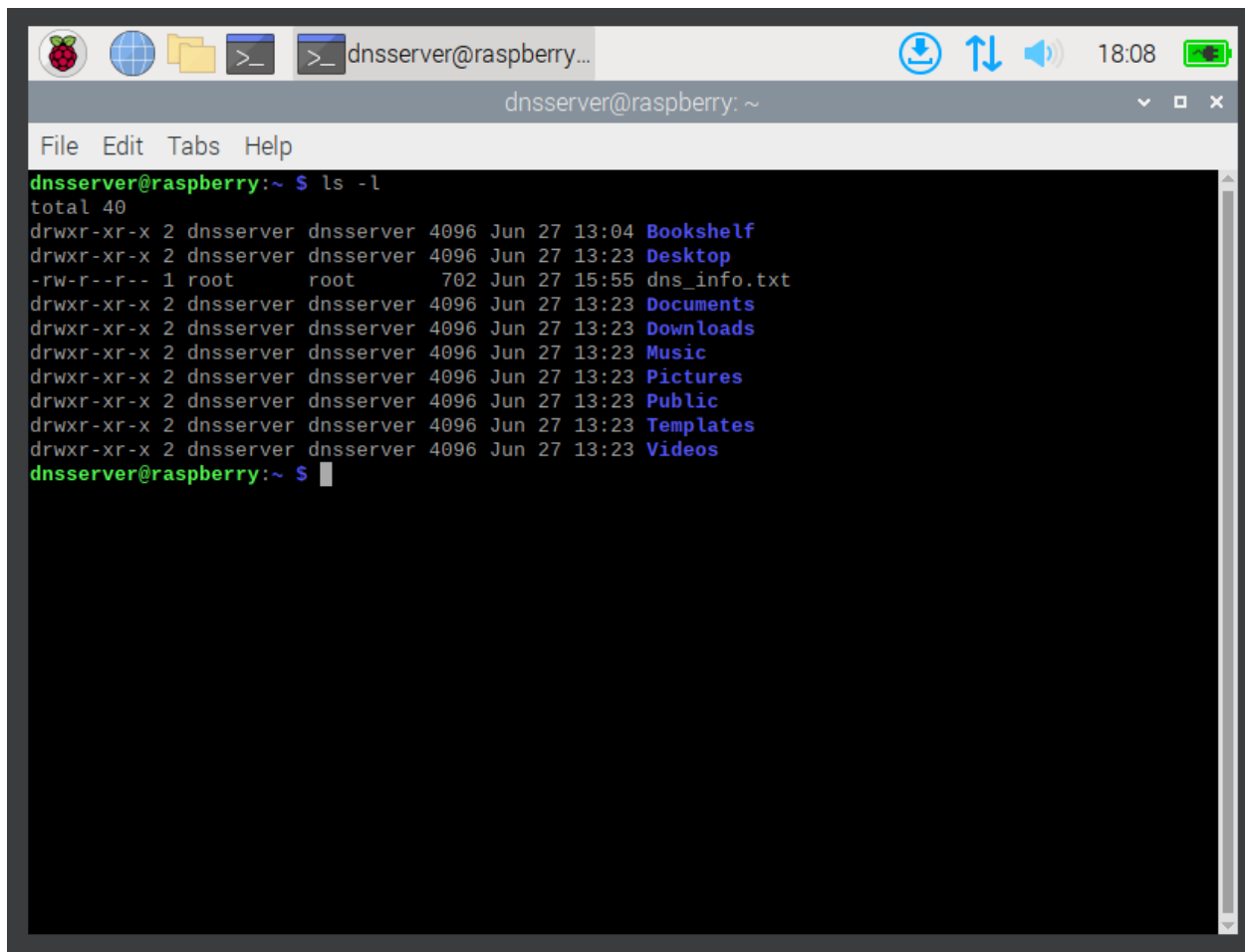
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;raspberry.com/kb.                IN      A

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Jun 30 18:05:02 HDT 2023
;; MSG SIZE rcvd: 45

dnsserver@raspberrypi:~$ S
```

14. As a bonus I added a text file called **dns_info.txt** so that if anyone wants to know the commands executed for the raspberry pi running as a DNS server, they

can read that file. It also states who executed the commands previously, since I added the command history there.



The image shows a terminal window titled "dnsserver@raspberrypi: ~". The window has a menu bar with "File", "Edit", "Tabs", and "Help". The terminal output shows the command "ls -l" and its results:

```
dnsserver@raspberrypi:~ $ ls -l
total 40
drwxr-xr-x 2 dnsserver dnsserver 4096 Jun 27 13:04 Bookshelf
drwxr-xr-x 2 dnsserver dnsserver 4096 Jun 27 13:23 Desktop
-rw-r--r-- 1 root      root      702 Jun 27 15:55 dns_info.txt
drwxr-xr-x 2 dnsserver dnsserver 4096 Jun 27 13:23 Documents
drwxr-xr-x 2 dnsserver dnsserver 4096 Jun 27 13:23 Downloads
drwxr-xr-x 2 dnsserver dnsserver 4096 Jun 27 13:23 Music
drwxr-xr-x 2 dnsserver dnsserver 4096 Jun 27 13:23 Pictures
drwxr-xr-x 2 dnsserver dnsserver 4096 Jun 27 13:23 Public
drwxr-xr-x 2 dnsserver dnsserver 4096 Jun 27 13:23 Templates
drwxr-xr-x 2 dnsserver dnsserver 4096 Jun 27 13:23 Videos
dnsserver@raspberrypi:~ $
```

The terminal window also shows a taskbar at the top with icons for a Raspberry Pi, a globe, a folder, and a terminal. The system clock shows 18:08 and a battery icon.