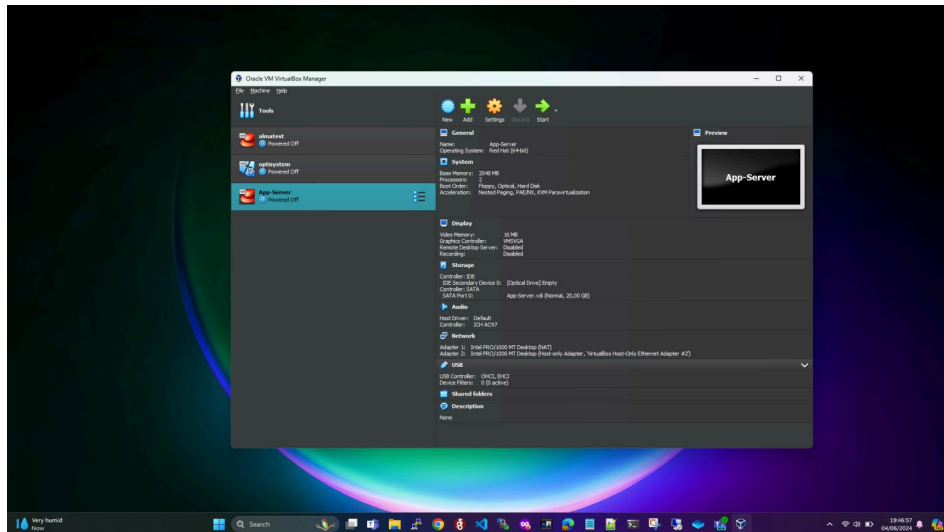
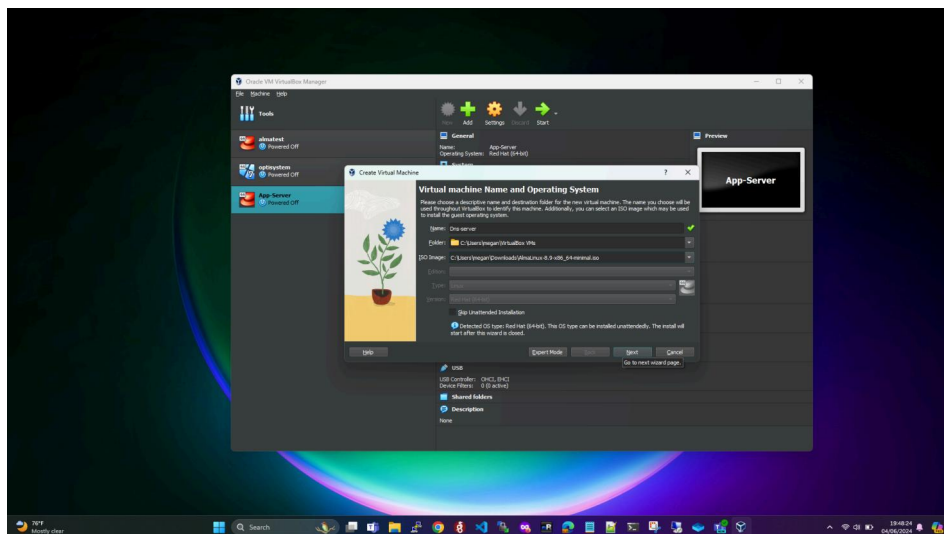


## INSTALL NEW VM ON VIRTUALBOX (configure web server dan dns server)

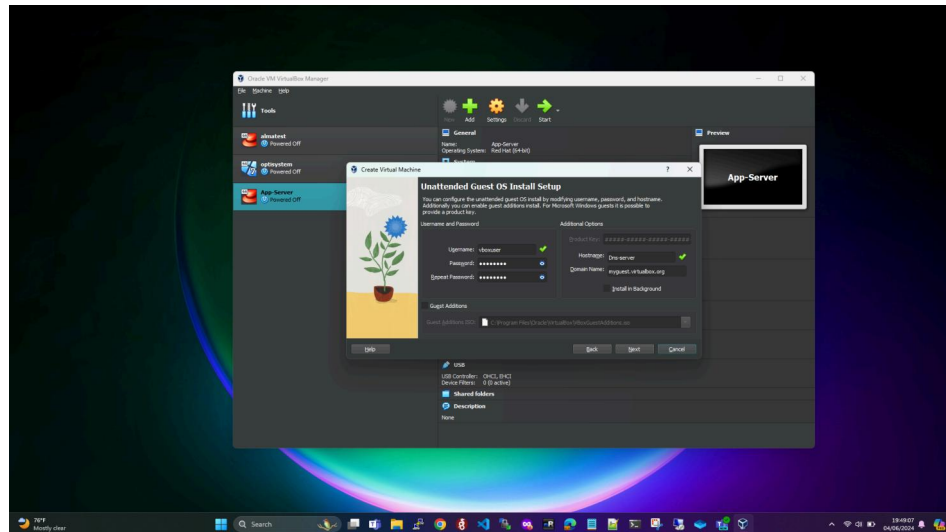
1. Pertama untuk membuat VM baru buka aplikasi VirtualBox kemudian klik new



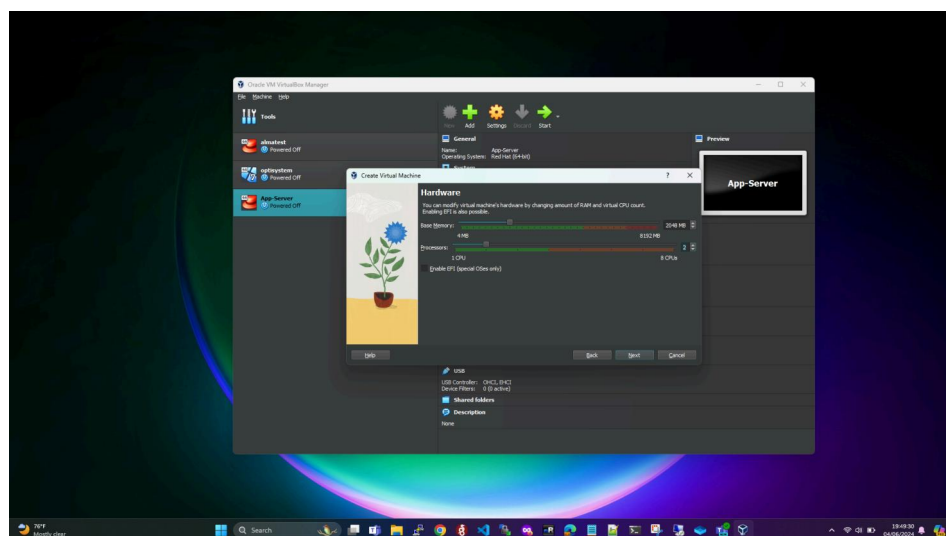
2. Ketika muncul box pada saat create new vm isikan nama vm, directory vm dan file iso yang akan digunakan



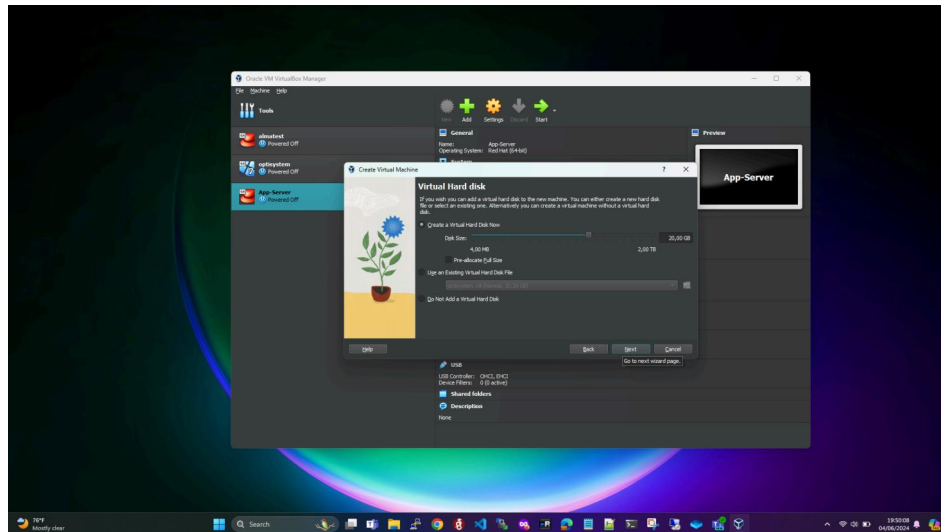
3. Kemudian pilih next dan isikan hostname user dan password guest user



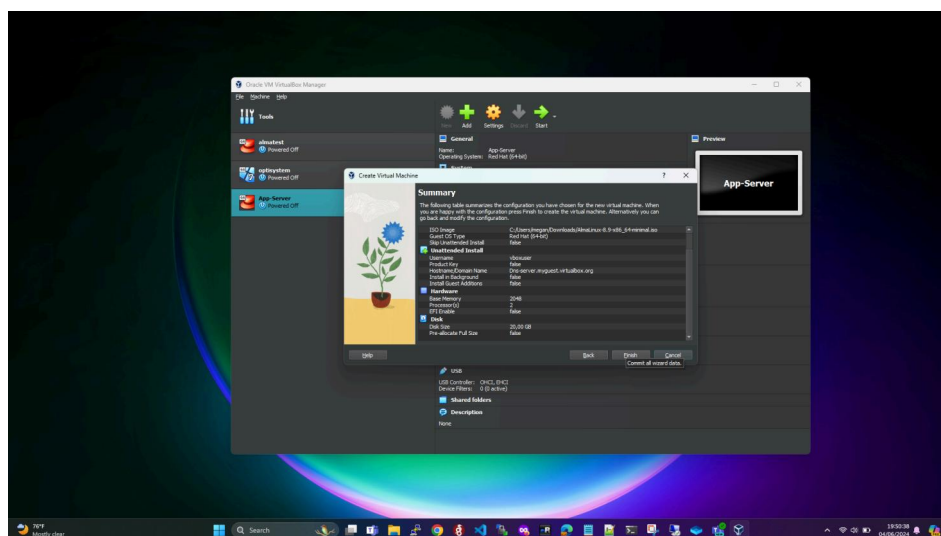
4. Kemudian klik next dan isikan jumlah memory dan cpu yang akan dialokasikan untuk VM nya



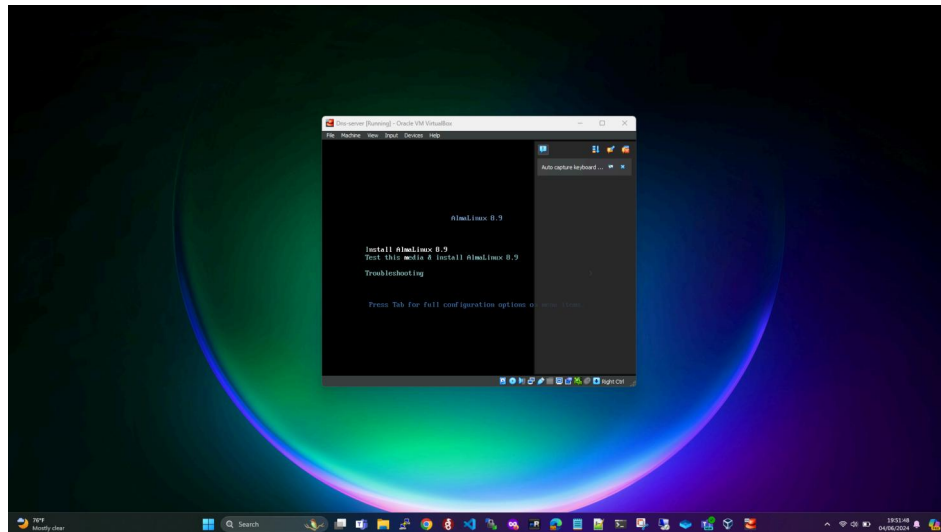
5. Step selanjutnya adalah memasukkan alokasi untuk disk yang akan digunakan



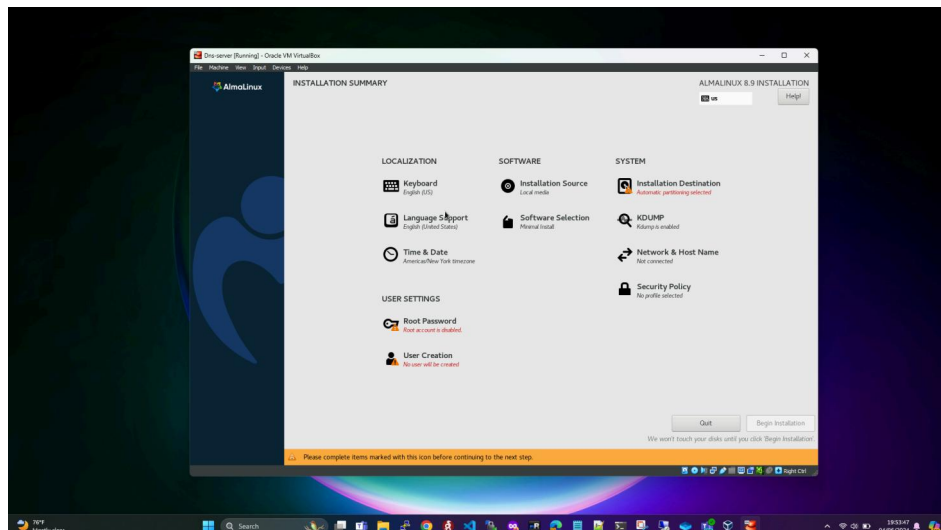
6. Klik finish untuk membuat vm pada virtual box



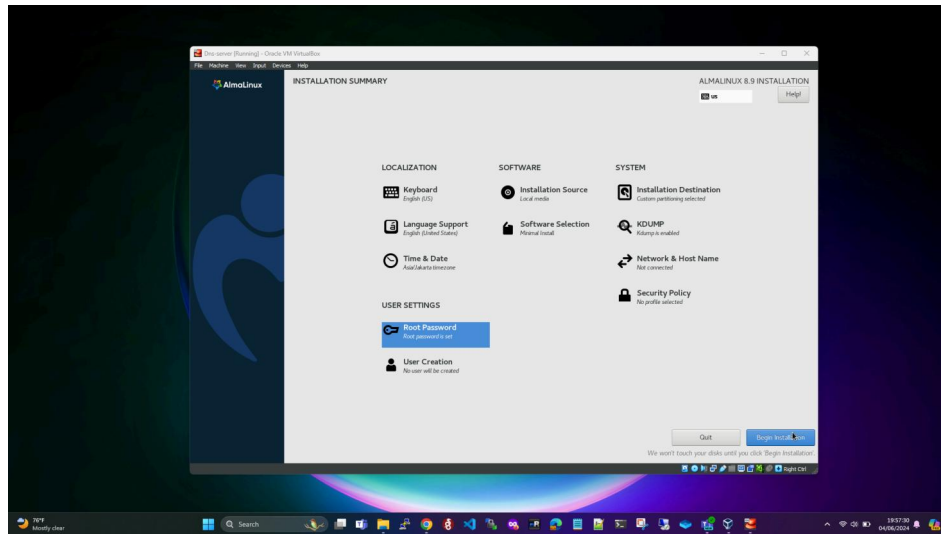
7. Start vm yang sudah berhasil dibuat dan lakukan instalasi OS pada VM tersebut pada step ini saya menggunakan OS Alma Linux



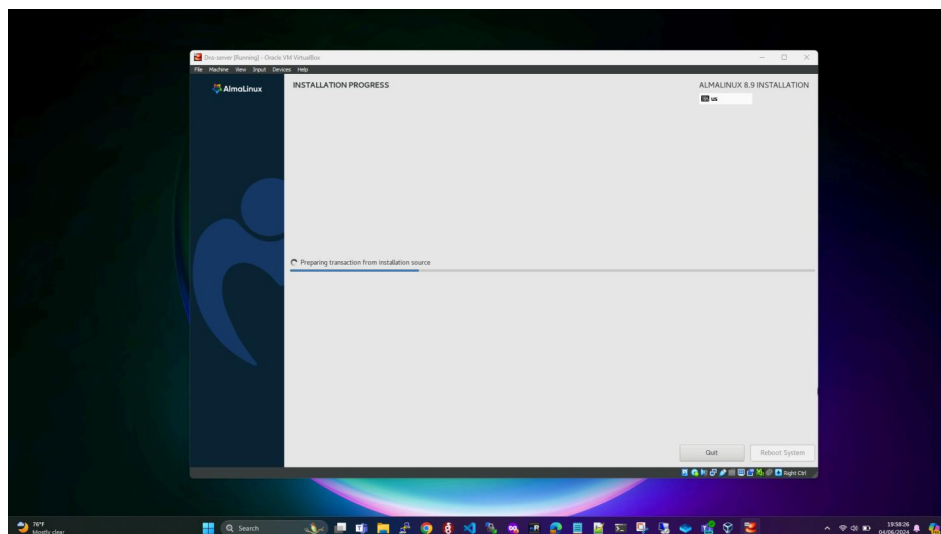
8. Pada step ini sesuaikan time, installation destination, user dan password



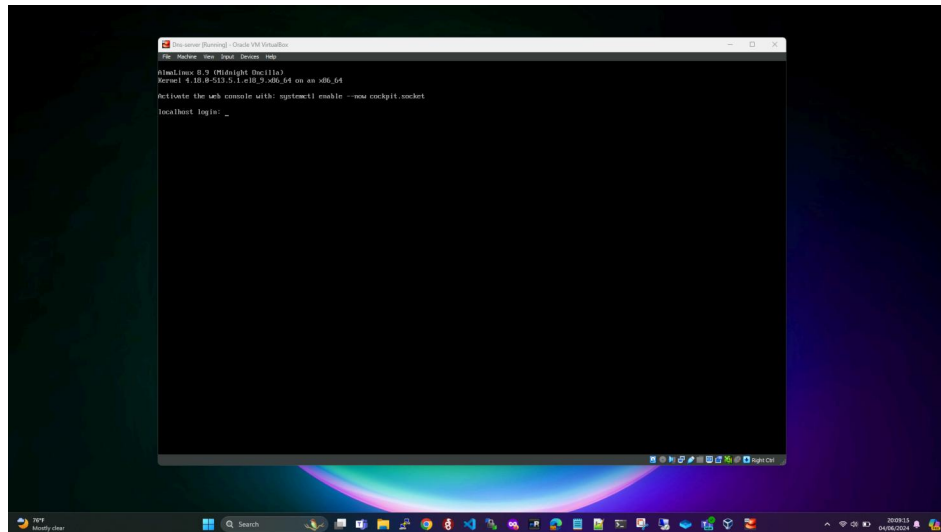
9. Kemudian klik begin installation untuk melakukan instalasi pada OS VM tersebut



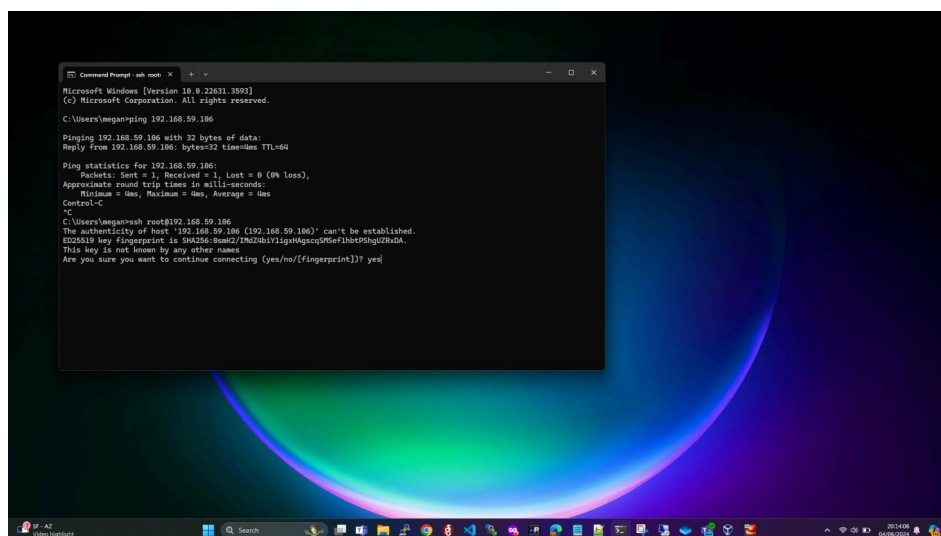
10. Proses instalasi OS sedang berjalan tunggu hingga proses selesai



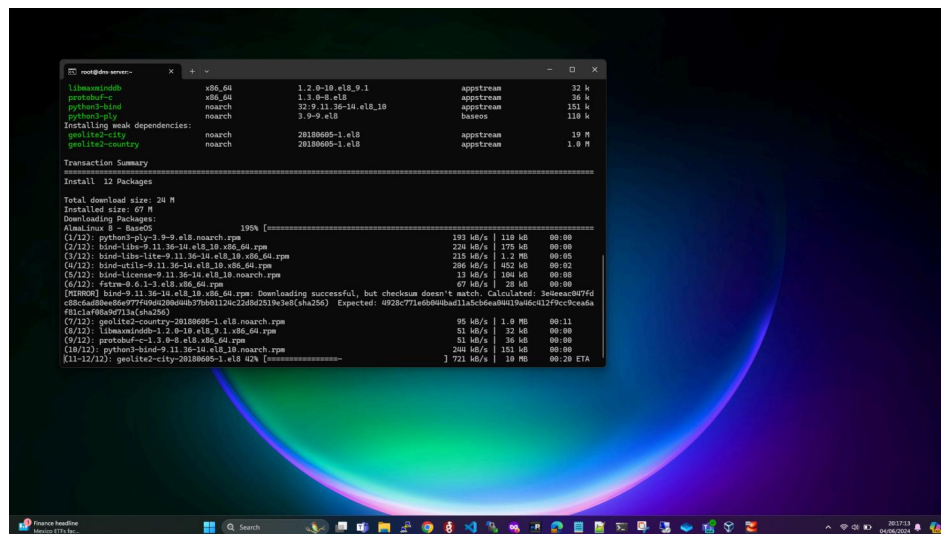
## 11. VM sudah berhasil terinstall os



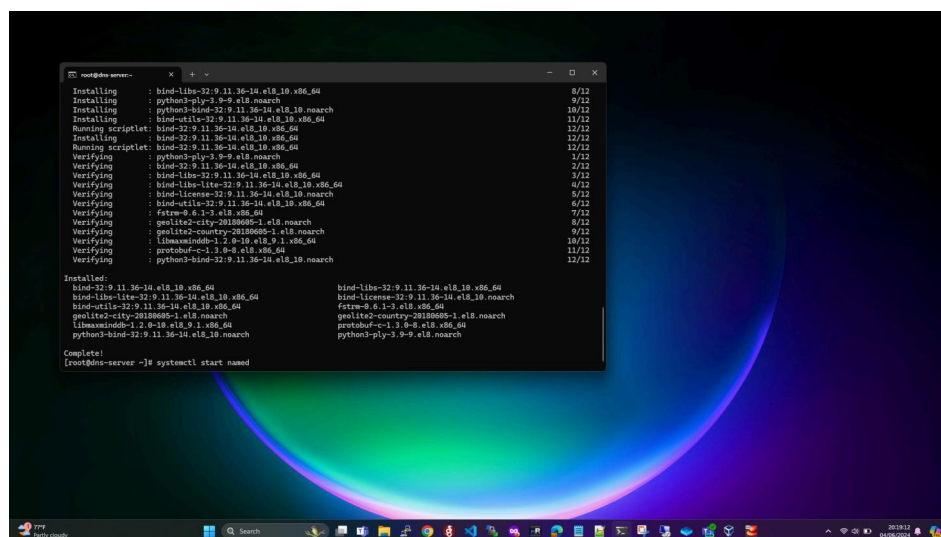
## 12. Lakukan testing remote server dengan ssh



13. Setelah VM berhasil terinstall lakukan instalasi service dns pada step ini saya menggunakan service bind



14. Setelah service named berhasil terinstall kemudian start service named





15. Kemudian lakukan enable service named agar ketika server atau vm restart service otomatis start

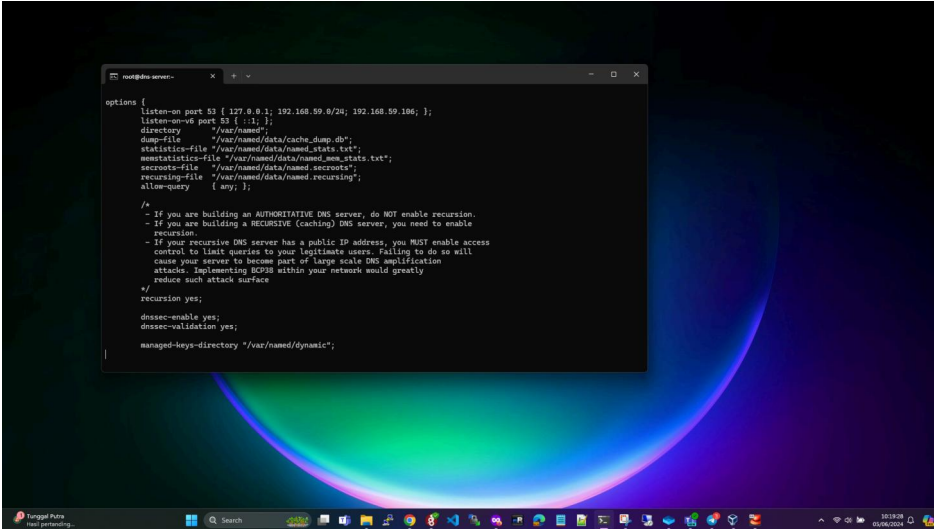
```
Complete!  
[root@dns-server ~]# systemctl start named  
[root@dns-server ~]# systemctl status named  
named.service - Berkeley Internet Name Domain (DNS)  
Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; vendor preset: disabled)  
Active: active (running) since Tue 2024-06-04 20:19:36 WIB; 5s ago  
Process: 18264 ExecStartPre=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)  
Process: 18268 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" = "yes" ]; then /usr/sbin/named-checkconf -f  
Main PID: 18271 (named)  
Tasks: 7 (limit: 11051)  
Memory: 16.5M  
CGroup: /system.slice/named.service  
--18271 /usr/sbin/named -u named -c /etc/named.conf  
  
Jun 04 20:19:39 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/5/IN: 199.7.91.13853  
Jun 04 20:19:40 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/DNSKEY/IN: 192.5.5.241853  
Jun 04 20:19:40 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/5/IN: 193.0.14.129853  
Jun 04 20:19:40 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/5/IN: 192.5.5.241853  
Jun 04 20:19:40 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/DNSKEY/IN: 199.7.83.42853  
Jun 04 20:19:41 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/DNSKEY/IN: 198.41.0.4853  
Jun 04 20:19:41 dns-server named[18271]: managed-keys-zone: Unable to fetch DNSKEY set '': failure  
Jun 04 20:19:41 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/5/IN: 198.41.0.4853  
Jun 04 20:19:41 dns-server named[18271]: resolver priming query complete  
  
[root@dns-server ~]#  
[root@dns-server ~]# systemctl enable named  
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /usr/lib/systemd/system/named.service.  
[root@dns-server ~]#
```

16. Enable service dns pada firewall

```
Complete!  
[root@dns-server ~]# systemctl start named  
[root@dns-server ~]# systemctl status named  
named.service - Berkeley Internet Name Domain (DNS)  
Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; vendor preset: disabled)  
Active: active (running) since Tue 2024-06-04 20:19:36 WIB; 5s ago  
Process: 18264 ExecStartPre=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)  
Process: 18268 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" = "yes" ]; then /usr/sbin/named-checkconf -f  
Main PID: 18271 (named)  
Tasks: 7 (limit: 11051)  
Memory: 16.5M  
CGroup: /system.slice/named.service  
--18271 /usr/sbin/named -u named -c /etc/named.conf  
  
Jun 04 20:19:39 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/5/IN: 199.7.91.13853  
Jun 04 20:19:40 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/DNSKEY/IN: 192.5.5.241853  
Jun 04 20:19:40 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/5/IN: 193.0.14.129853  
Jun 04 20:19:40 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/5/IN: 192.5.5.241853  
Jun 04 20:19:40 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/DNSKEY/IN: 199.7.83.42853  
Jun 04 20:19:41 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/DNSKEY/IN: 198.41.0.4853  
Jun 04 20:19:41 dns-server named[18271]: managed-keys-zone: Unable to fetch DNSKEY set '': failure  
Jun 04 20:19:41 dns-server named[18271]: REFUSED unexpected RCODE resolving .:/5/IN: 198.41.0.4853  
Jun 04 20:19:41 dns-server named[18271]: resolver priming query complete  
  
[root@dns-server ~]#  
[root@dns-server ~]# systemctl enable named  
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /usr/lib/systemd/system/named.service.  
[root@dns-server ~]# firewall-cmd --permanent --add-service=dns
```



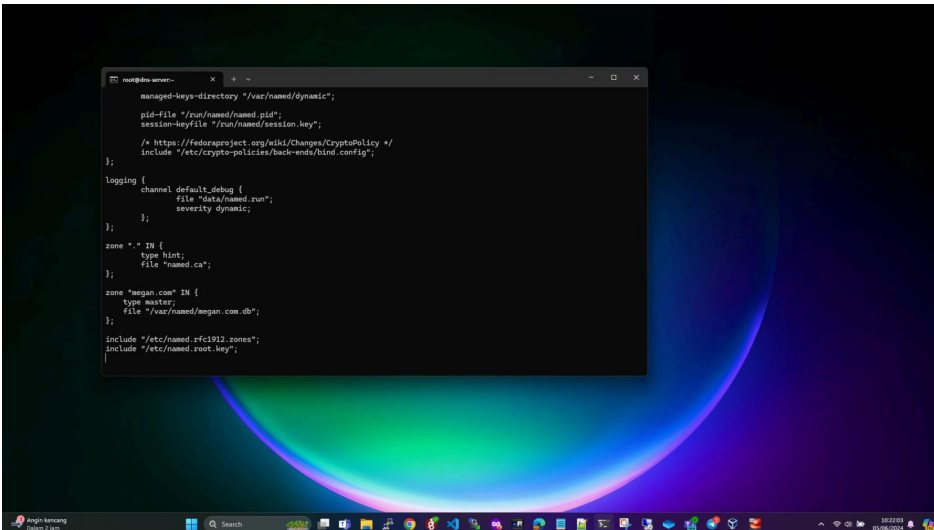
17. Kemudian lakukan konfigurasi DNS server kemudian edit file di folder /etc/named.conf tambahkan conf berikut



```
options {
    listen-on port 53 { 127.0.0.1; 192.168.59.0/24; 192.168.59.106; };
    listen-on-v6 port 53 { ::1; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    nonstatistics-file "/var/named/data/named_non_stats.txt";
    secrets-file "/var/named/data/named.secrets";
    recursion-file "/var/named/data/named.recursion";
    allow-query { any; };
}

/*
- If you are building an AUTHORITY DNS server, do NOT enable recursion.
- If you are building a RECURSIVE (caching) DNS server, you need to enable
  recursion.
- If your recursive DNS server has a public IP address, you MUST enable access
  control to limit queries to your legitimate users. Failing to do so will
  cause your server to become part of large scale DNS amplification
  attacks. Implementing RPZs within your network would greatly
  reduce such attack surface
*/
recursion yes;
dnsec-enable yes;
dnsec-validation yes;
managed-keys-directory "/var/named/dynamic";
```

18. Tambahkan juga zone baru pada conf named.conf nya seperti berikut



```
managed-keys-directory "/var/named/dynamic";
pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";
/* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
include "/etc/crypto-policies/back-ends/bins.config";
};

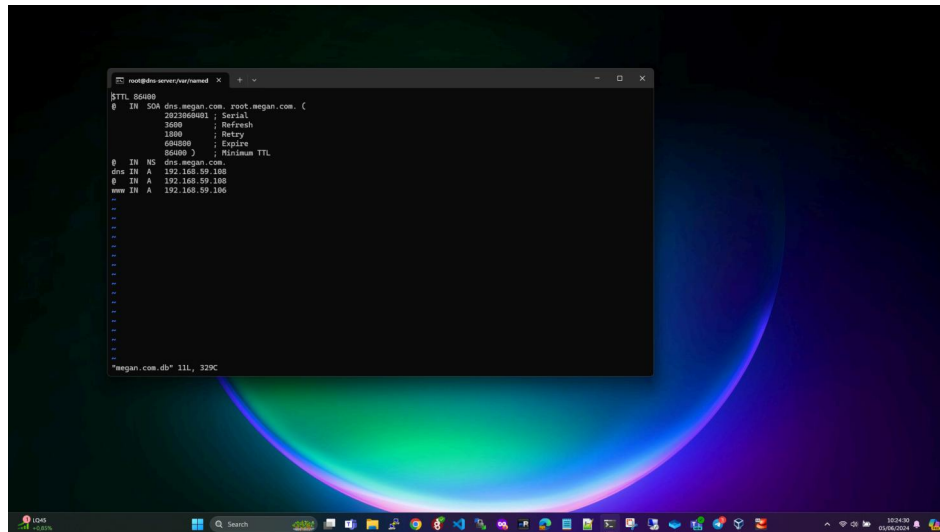
logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "megan.com" IN {
    type master;
    file "/var/named/megan.com.db";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

19. Kemudian buat file untuk zone megan.com di var/named/ seperti berikut

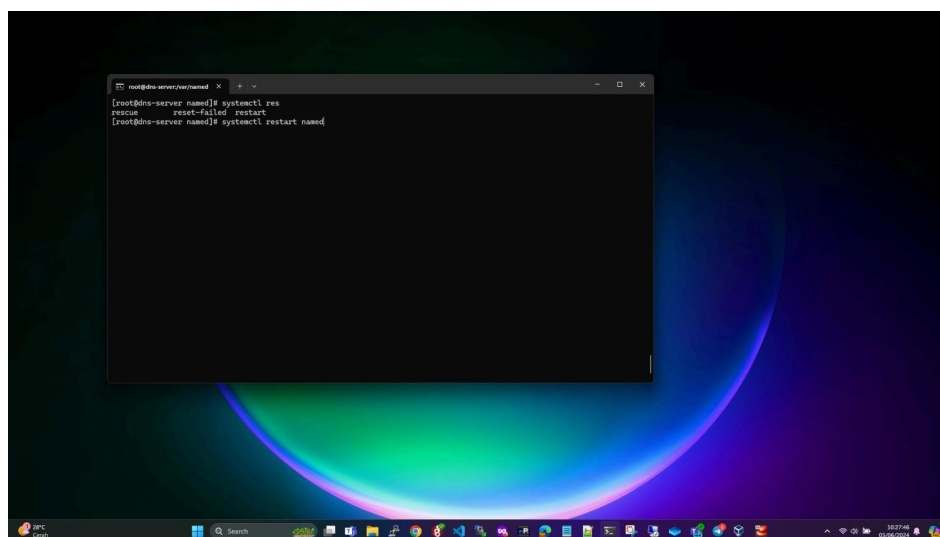


```
root@dns-server:/var/named # cat megan.com.db
$TTL 86400
$ORIGIN dns.megan.com.
$SOA dns.megan.com. root.megan.com. (
    2023060401 ; Serial
    3600      ; Refresh
    1800      ; Retry
    604800    ; Expire
    86400     ; Minimum TTL
)

$INCLUDE megan.com.db

$TTL 3600
dns IN A 192.168.59.100
www IN A 192.168.59.100
```

20. Setelah itu lakukan check pada conf namednya dengan menjalankan perintah “named-checkconf” dan “named-checkzone megan.com /var/named/megan.com.db” dan lakukan restart pada service named



```
root@dns-server:/var/named # named-checkconf
[root@dns-server named]# systemctl res
rescue root@dns-server:~# named-checkzone megan.com /var/named/megan.com.db
[root@dns-server named]# systemctl restart named
```

21. Lakukan pengujian pada dns server untuk lookup domain megan.com atau bisa dengan menggunakan dig dan megan.com sudah berhasil resolved ke endpoint server app dengan ip 192.168.59.108

```
root@dns-server:~# dig @127.0.0.1 megan.com

;<>> DIG 9.11.36-RedHat-9.11.36-14.el8_18 <>> @127.0.0.1 megan.com
;; (1 server found)
;; global options: +cmd
;; >>>HEADER<<< opcode: QUERY, status: NOERROR, id: 14860
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: 0, udp: 1232
; COOKIE: 6d4c7f3b6e7d20151cfc7cab665fdb01e7f0bede175ebbd (good)
;; QUESTION SECTION:
; megan.com.                IN      A
;; ANSWER SECTION:
megan.com.                  60408   IN      A      192.168.59.108
;; AUTHORITY SECTION:
megan.com.                  60408   IN      NS      dns.megan.com.
;; ADDITIONAL SECTION:
dns.megan.com.              60408   IN      A      192.168.59.108

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Jun 05 18:36:24 WIB 2024
;; MSG SIZE  rcv=116

[root@dns-server:~# nslookup megan.com 192.168.59.108
Server:
192.168.59.108
Address:
192.168.59.108453

Name:   megan.com
Address: 192.168.59.108
```

22. Konfigurasi web server dengan menggunakan apache pertama lakukan instalasi apache servernya

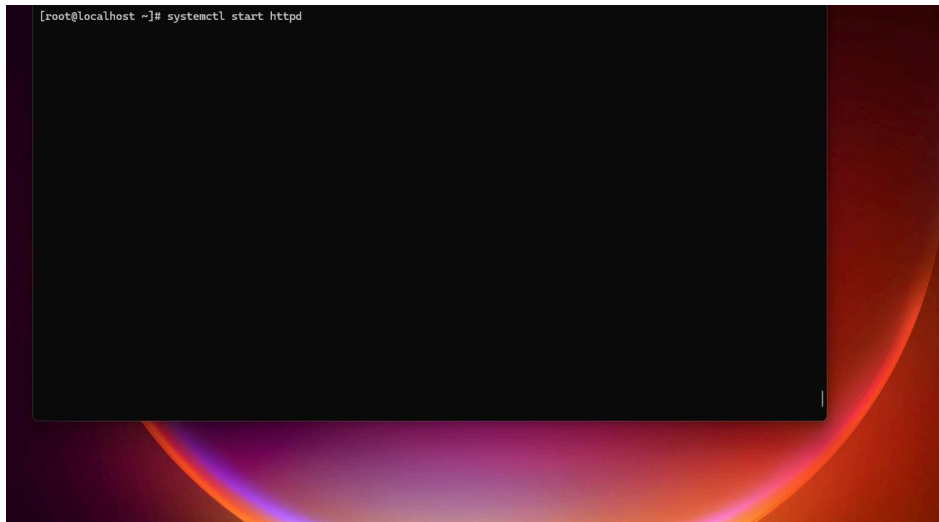
```
root@localhost:~# dnf install httpd -y

fsfw-0.6.1-3.el8.x86_64
geolite2-city-20180605-1.el8.noarch
grub2-tools-efi-1:2.02-156.el8.almalinux1.x86_64
kernel-core-4.10.0-553.el8_10.x86_64
libX11-1.6.8-8.el8.x86_64
libXau-1.0.9-3.el8.x86_64
libXrender-0.9.10-7.el8.x86_64
libxsimd-1.2.0-10.el8_9.1.x86_64
libsoup-2.62.3-5.el8.x86_64
libsss_sudo-2.9.4-3.el8_10.x86_64
libweb-1.12.1-1.el8.x86_64
memtrack-0.2.5-2.el8.x86_64
pixman-0.38.4-4.el8.x86_64
policycoreutils-python-utils-2.9-25.el8.noarch
python3-audit-3.1.2-1.el8.x86_64
python3-cairo-1.16.3-6.el8.x86_64
python3-gobject-3.28.3-2.el8.x86_64
python3-libnl2-2.9.7-18.el8_9.x86_64
python3-ply-3.9-9.el8.noarch
python3-psutil-5.4.3-11.el8.x86_64
python3-pydbus-0.6.0-5.el8.noarch
python3-tracer-1.1-1.el8.noarch
rpm-plugin-systemd-inhibit-4.14.3-31.el8.x86_64
setroubleshoot-server-3.3.26-6.el8.x86_64
sssd-nfs-idmap-2.9.4-3.el8_10.x86_64
tracer-common-1.1-1.el8.noarch
xkeyboard-config-2.28-1.el8.noarch

gdk-pixbuf2-2.36.12-6.el8_10.x86_64
geolite2-country-20180605-1.el8.noarch
kernel-4.10.0-553.el8_10.x86_64
kernel-modules-4.10.0-553.el8_10.x86_64
libX11-common-1.6.8-8.el8.noarch
libXext-1.3.4-1.el8.x86_64
libappstream-glib-0.7.16-3.el8.x86_64
libffi-devel-3.3-39.el8.x86_64
libss_autofs-2.9.4-3.el8_10.x86_64
libstemmer-0-10.505svn.el8.x86_64
libtdcommon-0.9.1-1.el8.x86_64
pigz-2.4-4.el8.x86_64
platform-python-pip-9.0.3-24.el8.noarch
protobuf-c-1.3.0-8.el8.x86_64
python3-bind-32.9.11.36-14.el8_10.noarch
python3-libsm-1.4.0-2.module.el8_9.0+3700+efeb9fd.noarch
python3-libsm-1.4.0-2.module.el8_9.0+3700+efeb9fd.noarch
python3-pexpect-4.3.1-3.el8.noarch
python3-policycoreutils-2.9-25.el8.noarch
python3-ptyprocess-0.5.2-4.el8.noarch
python3-setools-4.3.0-5.el8.x86_64
python3-unbound-1.16.2-5.el8_9.6.x86_64
setroubleshoot-plugins-3.3.14-1.el8.noarch
sscp-3.0.0-7.el8.x86_64
sssd-proxy-2.9.4-3.el8_10.x86_64
unbound-libs-1.16.2-5.el8_9.6.x86_64

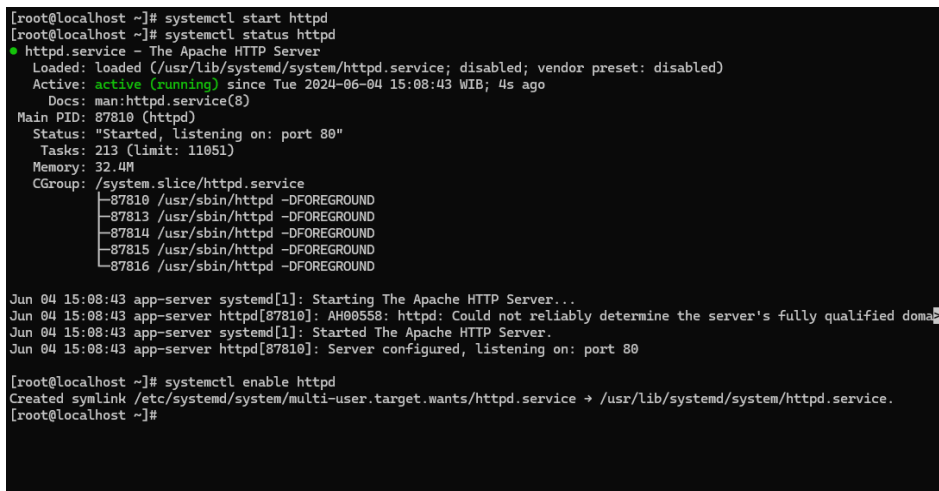
Complete!
[root@localhost ~]# dnf install httpd -y
```

23. Setelah service apache terinstall kemudian lakukan start pada service apache seperti berikut

A terminal window with a dark background and a colorful, abstract, glowing background image. The terminal shows the command `[root@localhost ~]# systemctl start httpd` being entered at the prompt.

```
[root@localhost ~]# systemctl start httpd
```

24. Setelah service apache berhasil start lakukan enable pada service apache agar ketika reboot vm atau server service apache otomatis start

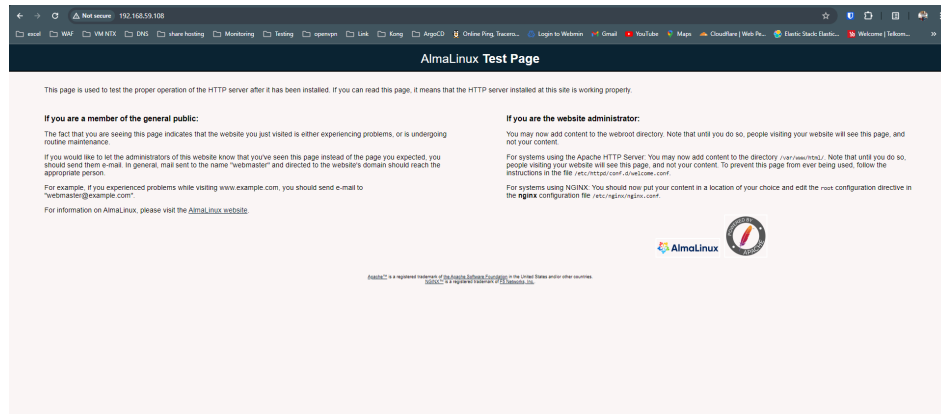
A terminal window showing the status of the httpd service and the command to enable it. The output of `systemctl status httpd` is displayed, showing the service is active and running. Then, the command `systemctl enable httpd` is entered, and the output shows that a symlink has been created to enable the service at boot.

```
[root@localhost ~]# systemctl start httpd
[root@localhost ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2024-06-04 15:08:43 WIB; 4s ago
     Docs: man:httpd.service(8)
  Main PID: 87810 (httpd)
   Status: "Started, listening on: port 80"
    Tasks: 213 (limit: 11051)
   Memory: 32.4M
   CGroup: /system.slice/httpd.service
           └─87810 /usr/sbin/httpd -DFOREGROUND
             └─87813 /usr/sbin/httpd -DFOREGROUND
               └─87814 /usr/sbin/httpd -DFOREGROUND
                 └─87815 /usr/sbin/httpd -DFOREGROUND
                   └─87816 /usr/sbin/httpd -DFOREGROUND

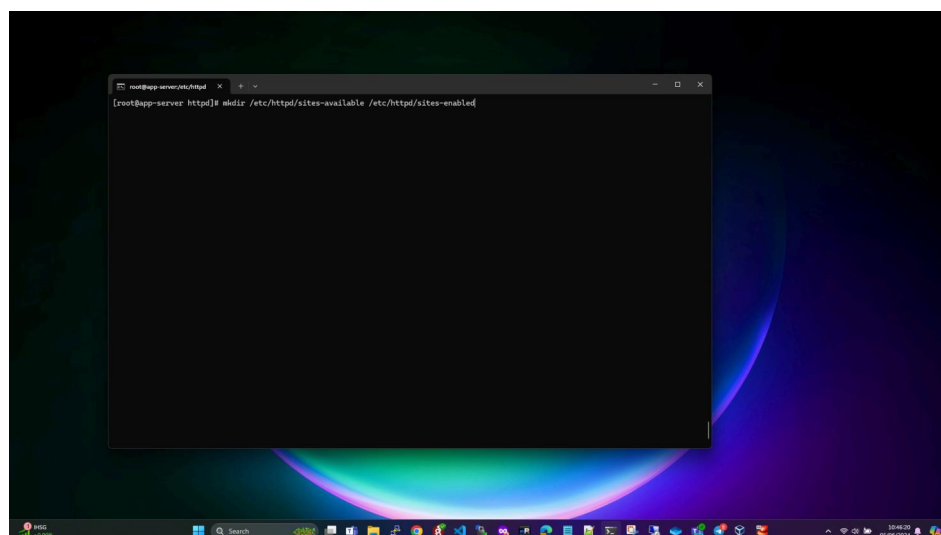
Jun 04 15:08:43 app-server systemd[1]: Starting The Apache HTTP Server...
Jun 04 15:08:43 app-server httpd[87810]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1:80 for ServerName
Jun 04 15:08:43 app-server systemd[1]: Started The Apache HTTP Server.
Jun 04 15:08:43 app-server httpd[87810]: Server configured, listening on: port 80

[root@localhost ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@localhost ~]#
```

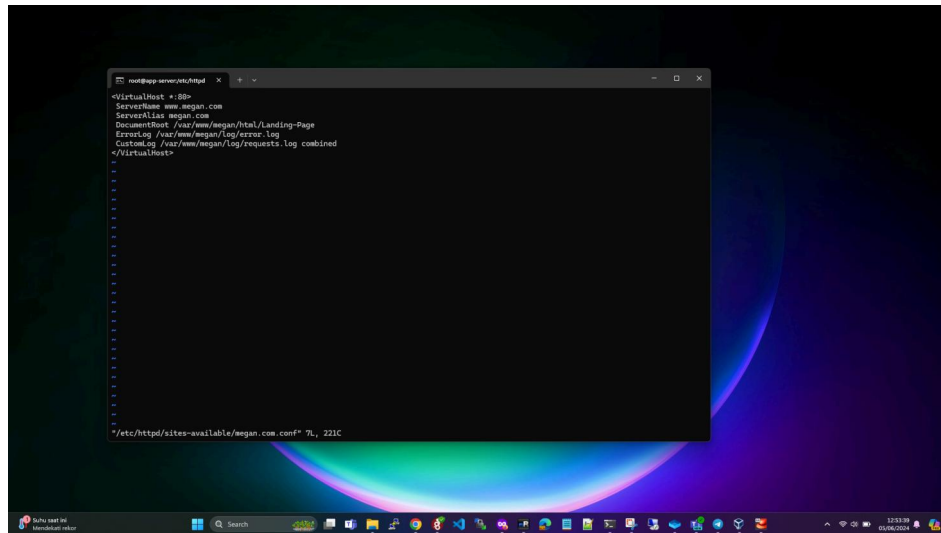
25. Lakukan testing untuk service apache jalan atau tidak dengan mengakses ip vm yang di install service apache



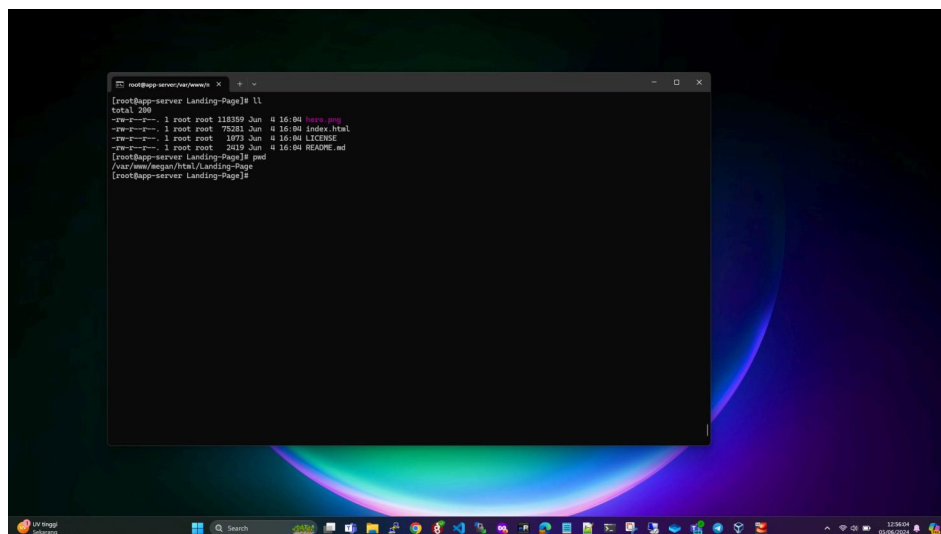
26. Setelah service apache berhasil berjalan lakukan create domain kita dimana pertama kita membuat folder site-available dan site-enabled



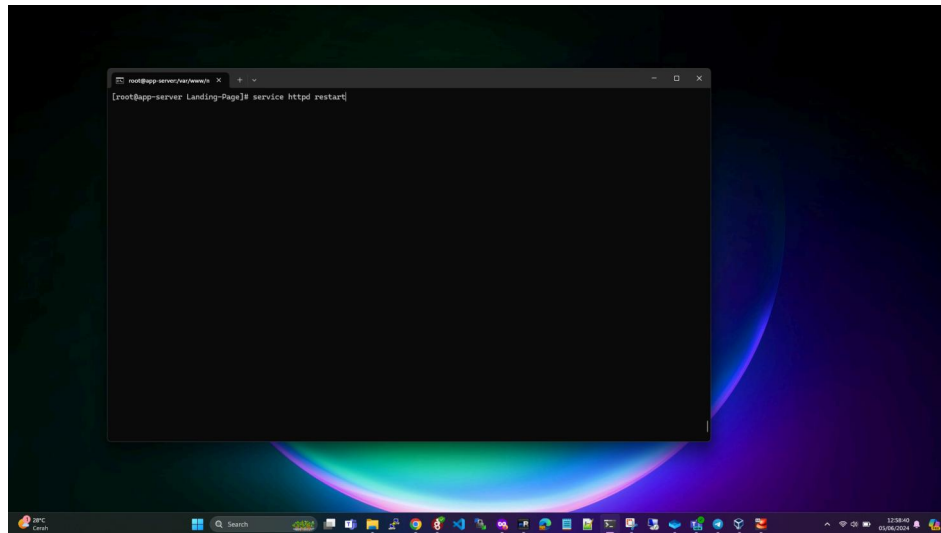
27. Buat konfigurasi untuk web kita seperti berikut sesuaikan nama domain dan folder yang akan digunakan



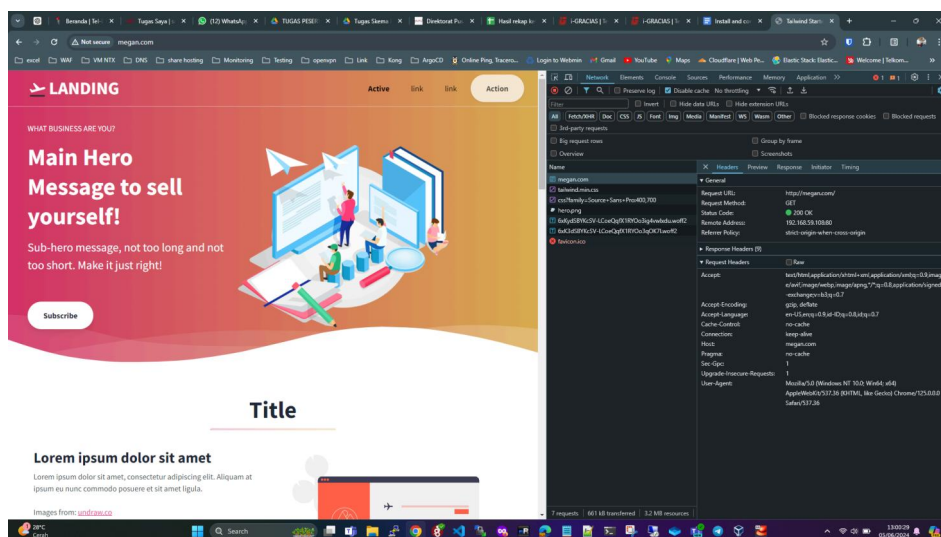
28. Pada folder document root web isikan file website kita disini menggunakan html saja terlihat seperti berikut



29. Setelah selesai kemudian melakukan restart pada service apache agar konfigurasi bisa ter apply



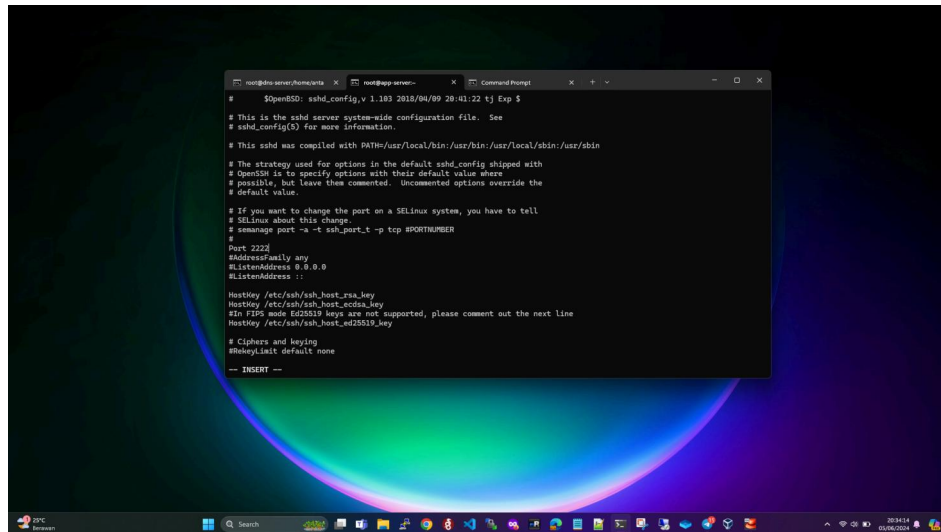
30. Cek domain yang sudah kita buat sebelumnya apakah sudah running atau belum, dan berikut web yang kita sudah berhasil berjalan dengan benar.



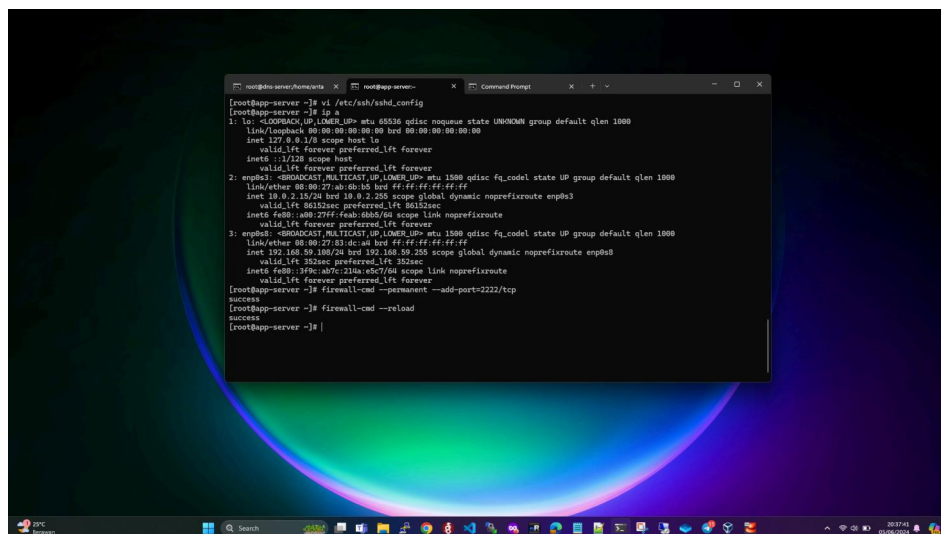


## PERANCANGAN KEAMANAN SERVER

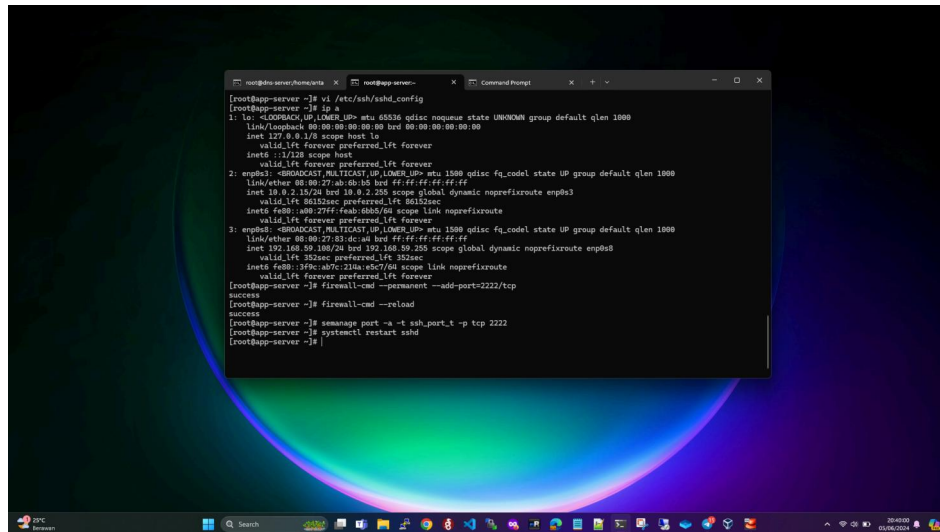
1. Selalu menggunakan remote server dengan ssh dan merubah port standar ssh berikut adalah conf untuk mengubah port standar ssh dari port 22 menjadi 2222



2. Kemudian tambahkan port baru ssh pada firewalld seperti berikut

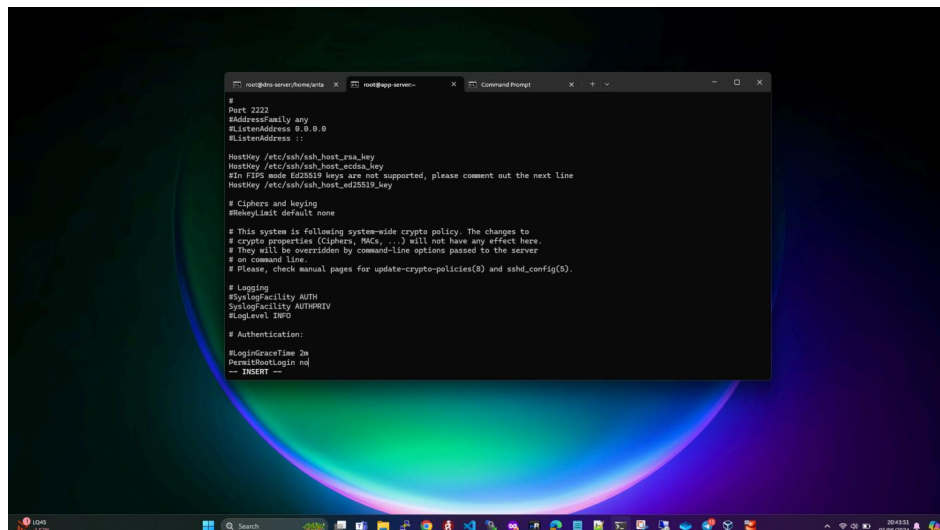


3. Tambahkan port 2222 pada selinux dan restart service sshd dan setting untuk merubah default port sudah berhasil



```
[root@server:~#] vi /etc/ssh/sshd_config
[Root@server:~#] ls a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
     valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
     valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:ab:0b:b5 brd ff:ff:ff:ff:ff:ff
   inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
     valid_lft 86152sec preferred_lft 86152sec
   inet6 fe80::a00:27ff:feab:0b05/64 scope link noprefixroute
     valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:03:00:00 brd ff:ff:ff:ff:ff:ff
   inet 192.168.59.100/24 brd 192.168.59.255 scope global dynamic noprefixroute enp0s8
     valid_lft 352sec preferred_lft 352sec
   inet6 fe80::390:a07c:21ba:c6c7/64 scope link noprefixroute
     valid_lft forever preferred_lft forever
[Root@server:~#] firewall-cmd --permanent --add-port=2222/tcp
success
[Root@server:~#] firewall-cmd --reload
success
[Root@server:~#] semanage port -a -t ssh_port_t -p tcp 2222
[Root@server:~#] systemctl restart sshd
[Root@server:~#]
```

4. Kemudian untuk hardening yang lain bisa dengan menonaktifkan root user login pada ssh dengan cara disable Permit Login dengan root user



```
#
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
# HostKey /etc/ssh/ssh_host_ed25519_key

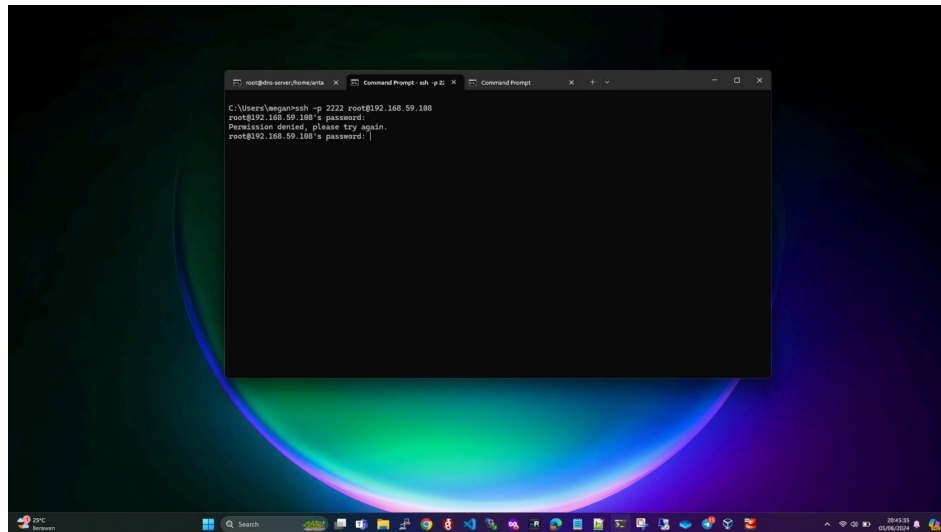
# Ciphers and keying
#RekeyInterval default none

# This system is following system-wide crypto policy. The changes to
# crypto properties (Ciphers, MACs, ...) will not have any effect here.
# They will be overridden by command-line options passed to the server
# on command line.
# Please, check manual pages for update-crypto-policies(8) and sshd_config(8).

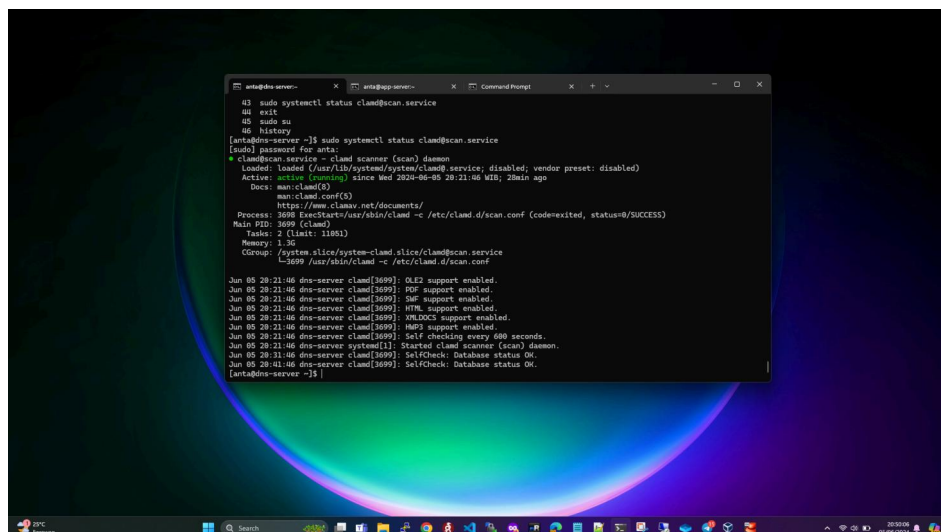
# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
#LoginGraceTime 3m
PermitRootLogin no
-- INSERT --
```

5. Ketika sudah menonaktifkan root user login maka ketika kita melakukan access ssh ke server maka akan tidak bisa dan tampil seperti berikut

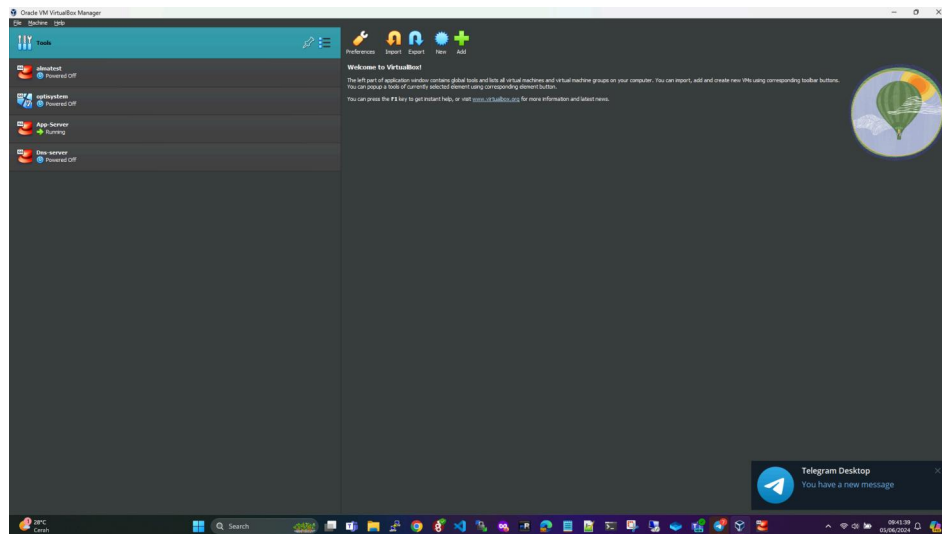


6. Selain itu kita juga bisa melakukan hardening dengan melakukan install antivirus berikut saya melakukan instalasi clamav

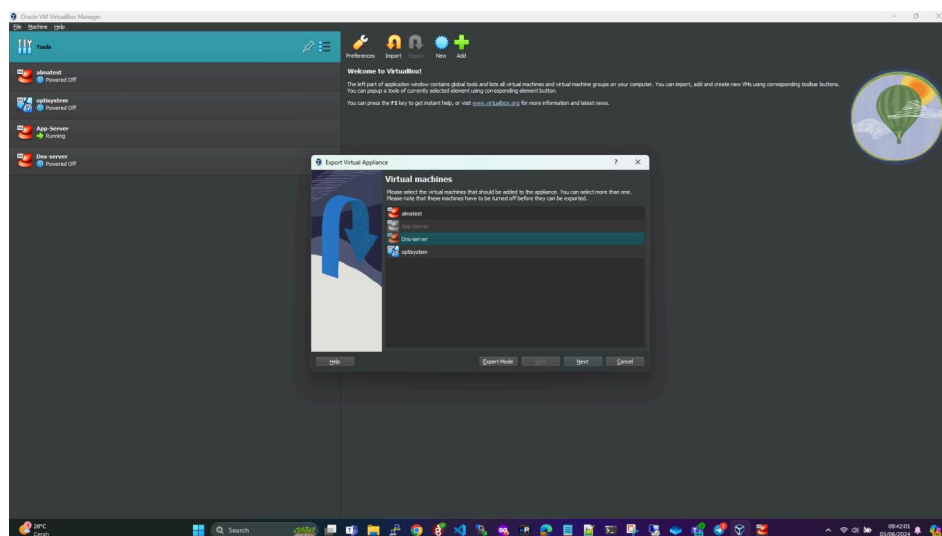


## BACKUP AND RESTORE VM

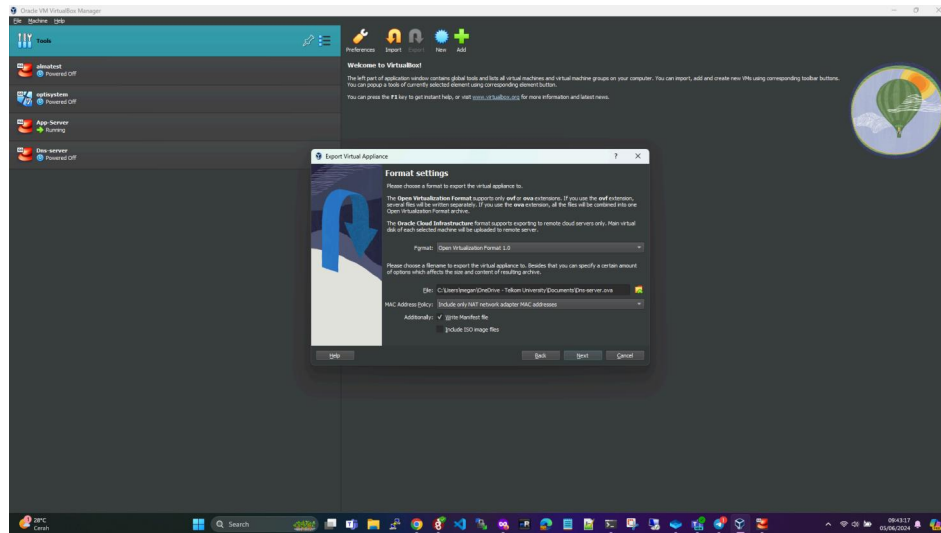
1. Untuk melakukan backup vm pada virtualbox pertama masuk ke virtualbox



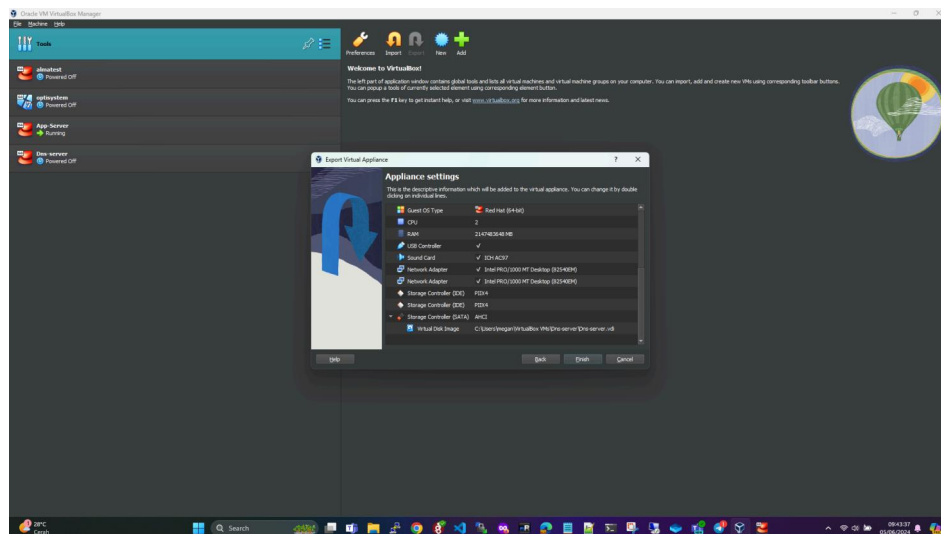
2. Kemudian klik export dan pilih vm mana yang akan di backup pada saat ini saya pilih dns-server kemudian klik next



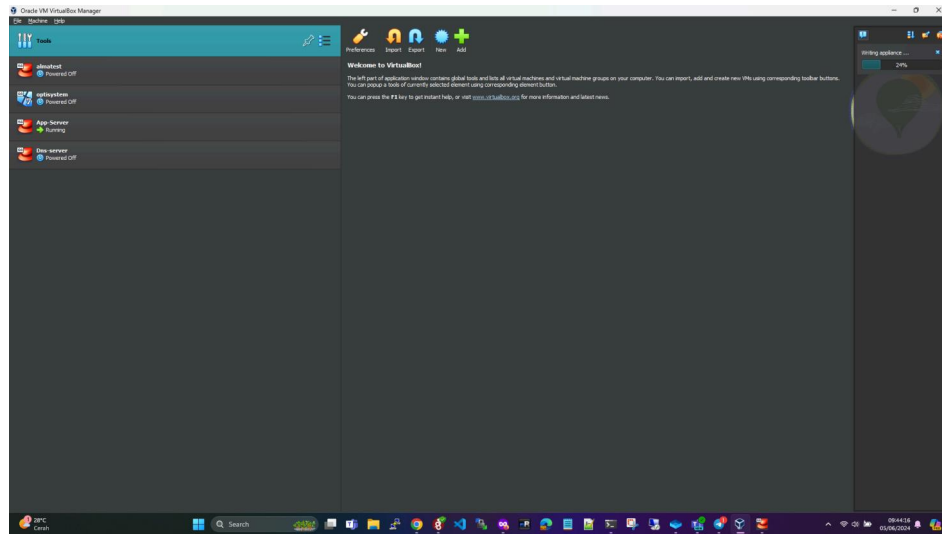
3. Kemudian tentukan format, lokasi vm untuk di export, dan mac address policy yang digunakan



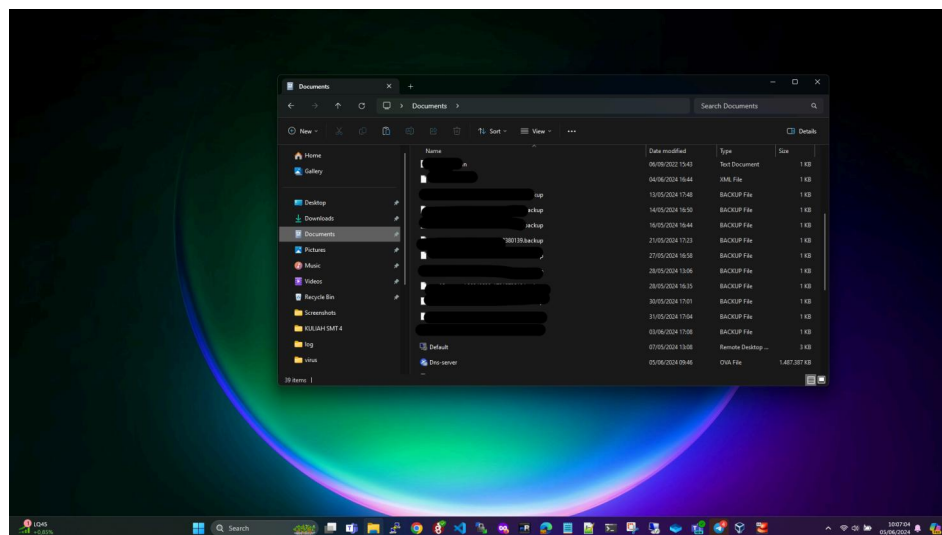
4. Klik finish untuk mulai melakukan backup/export vm



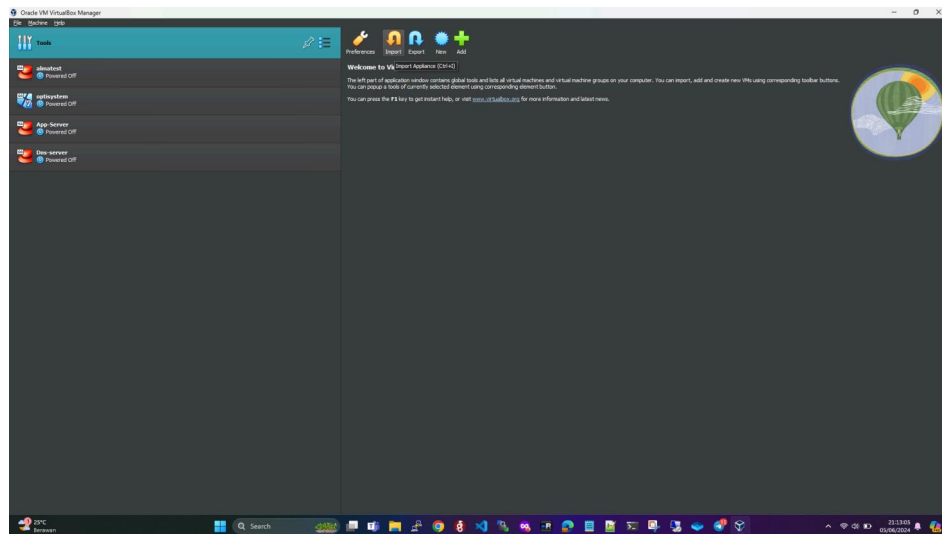
5. Proses backup masih berjalan dan tunggu hingga proses selesai



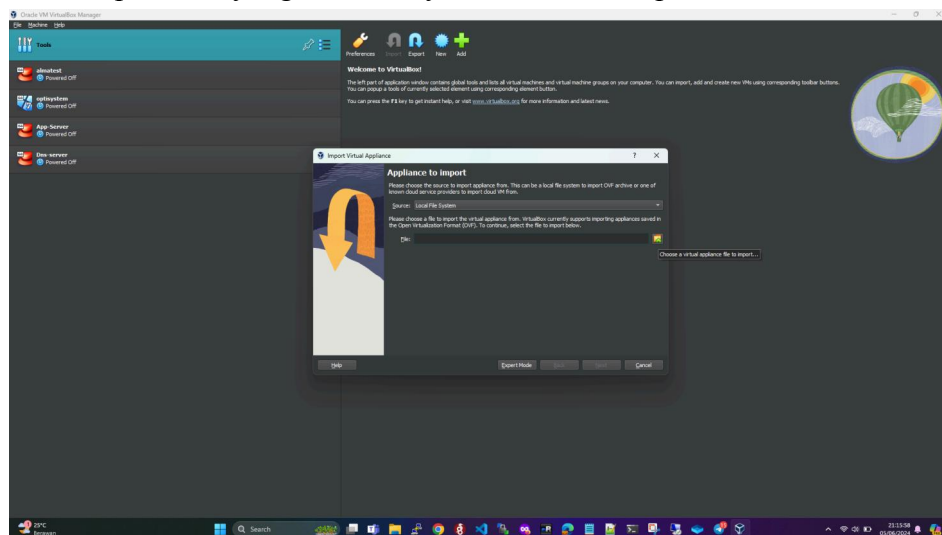
6. Berikut adalah hasil untuk backup VMnya



7. Setelah berhasil melakukan backup kita akan melakukan simulasi restore pada VM yang sudah di backup, pertama masuk pada virtual box kemudian pilih import

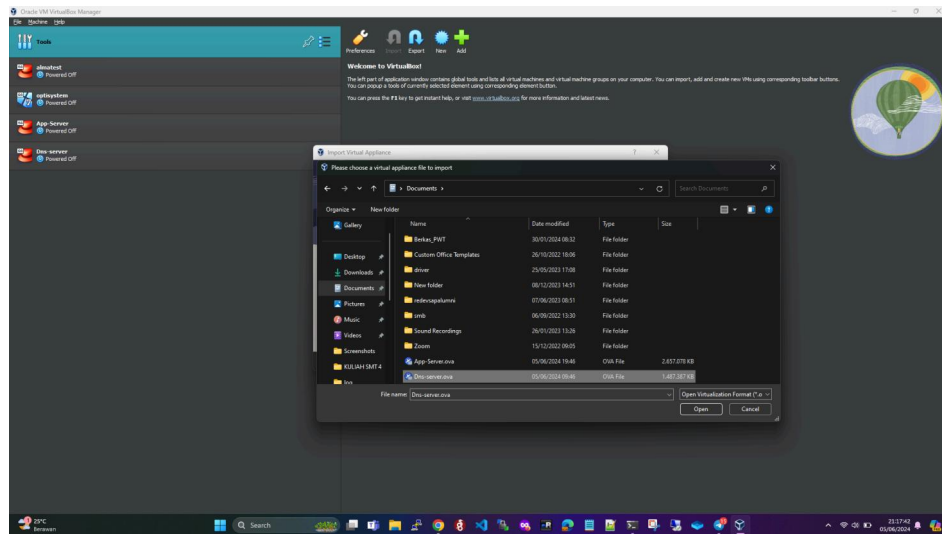


8. Kemudian pilih file yang sebelumnya sudah di backup

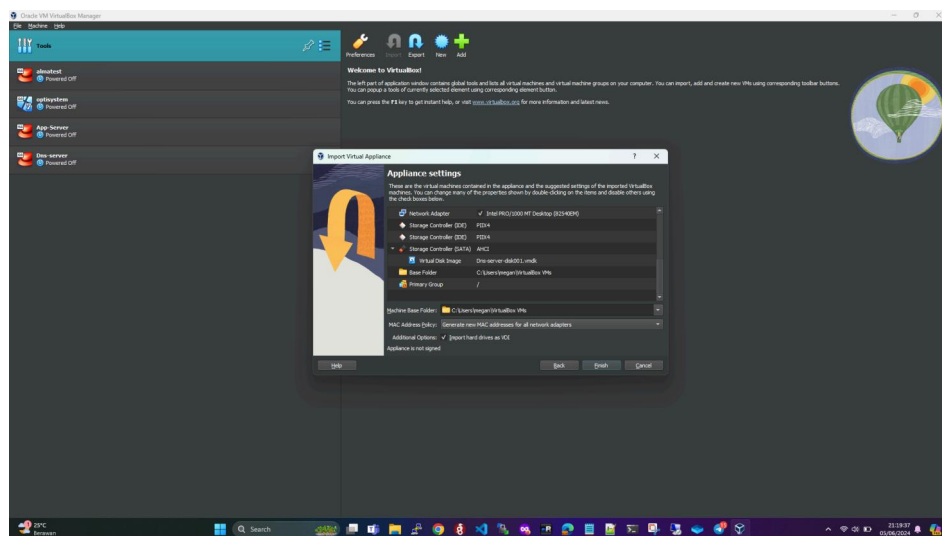




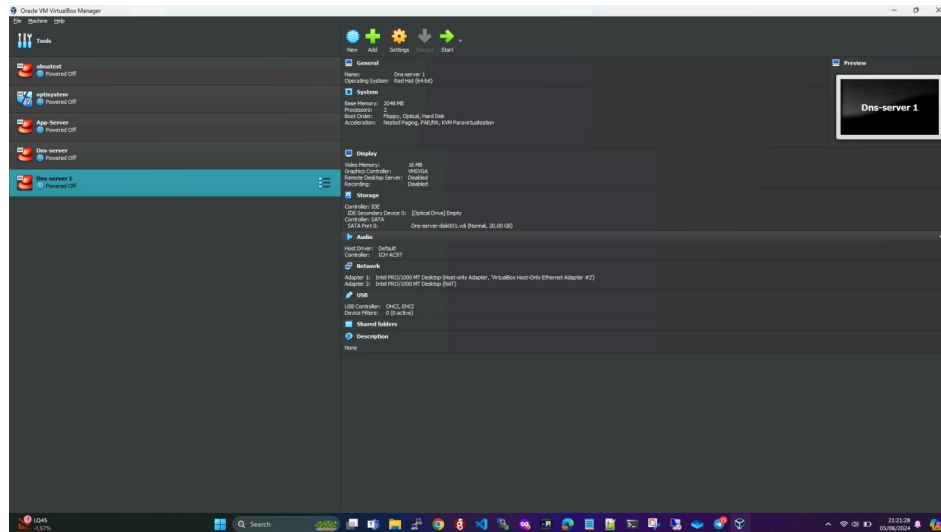
## 9. Pilih file dengan ekstensi .ova



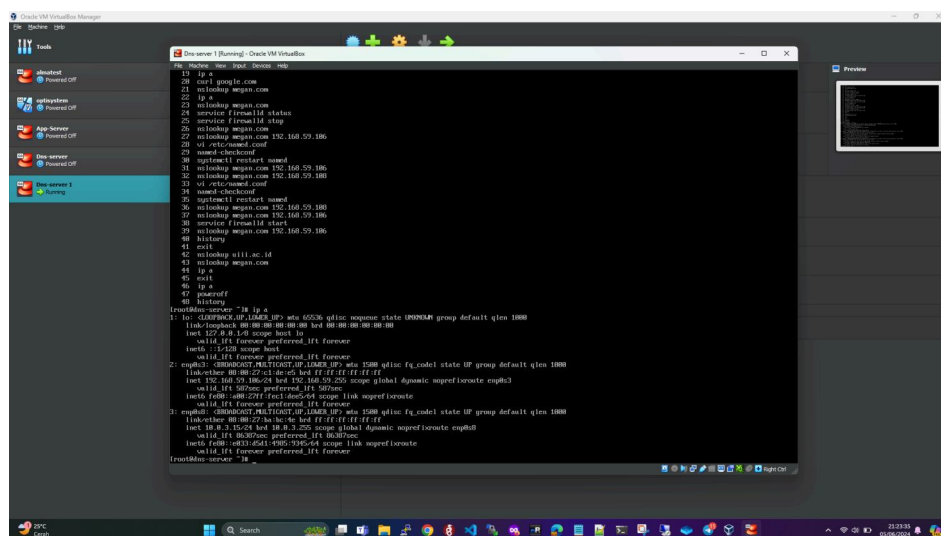
## 10. Kemudian klik finish



## 11. VM berhasil di restore dengan baik

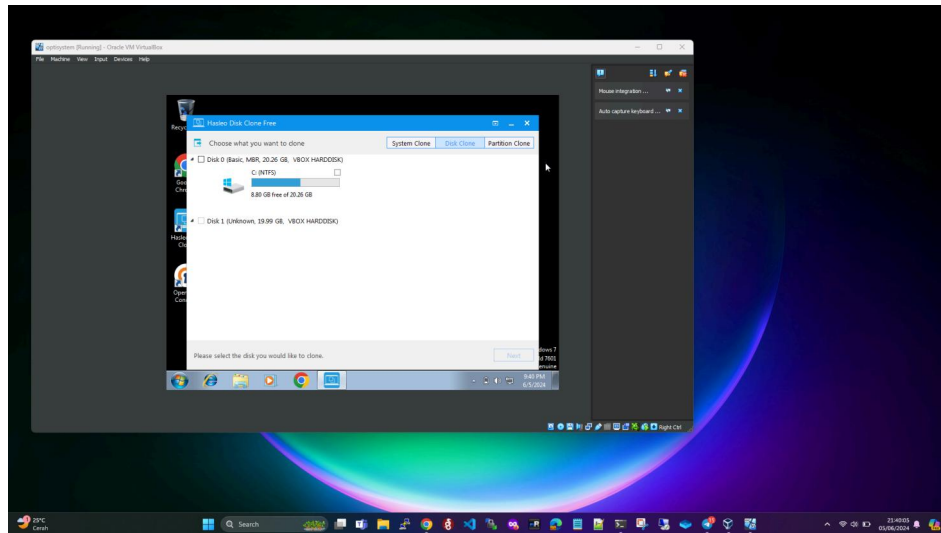


## 12. Lakukan testing dengan menyalakan vm dan data dan history kita masih ada sesuai dengan terakhir kita backup

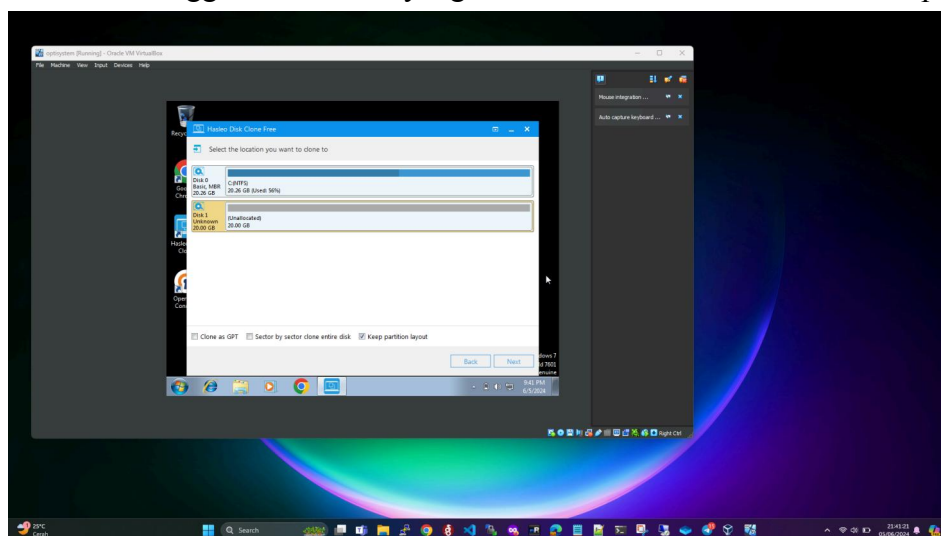


## SIMULASI MIGRASI

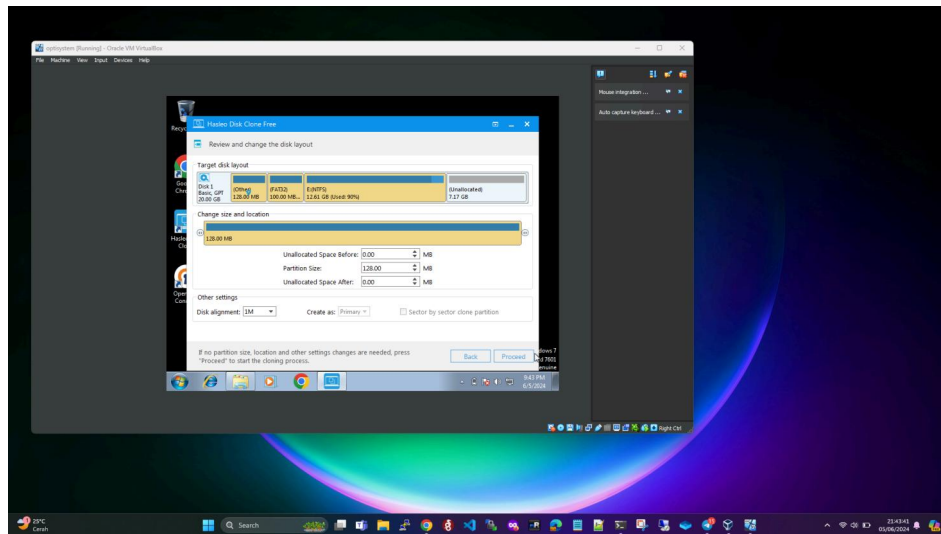
1. Buka aplikasi hasleo yang akan digunakan untuk cloning disk keperluan migrasi



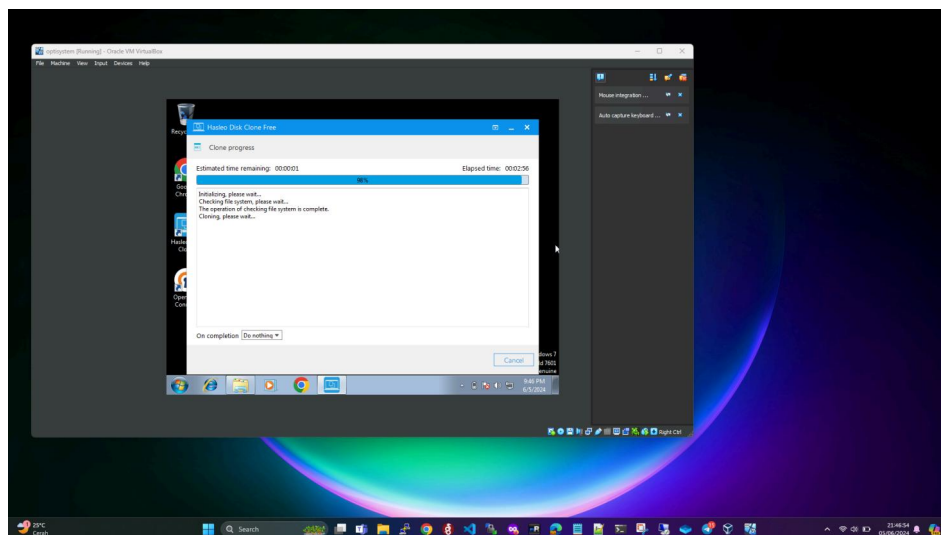
2. Pilih disk yang akan di clone dan tujuan atau disk destination untuk kloningnya dimana kita menggunakan disk 0 yang akan di clone dan disk 1 untuk tempat clone



- Pilih settingan untuk alokasi disknya kemudian klik finish



- Tunggu hingga proses kloning selesai



## 5. Proses kloning pada disk kita sudah berhasil

