

LAB 09

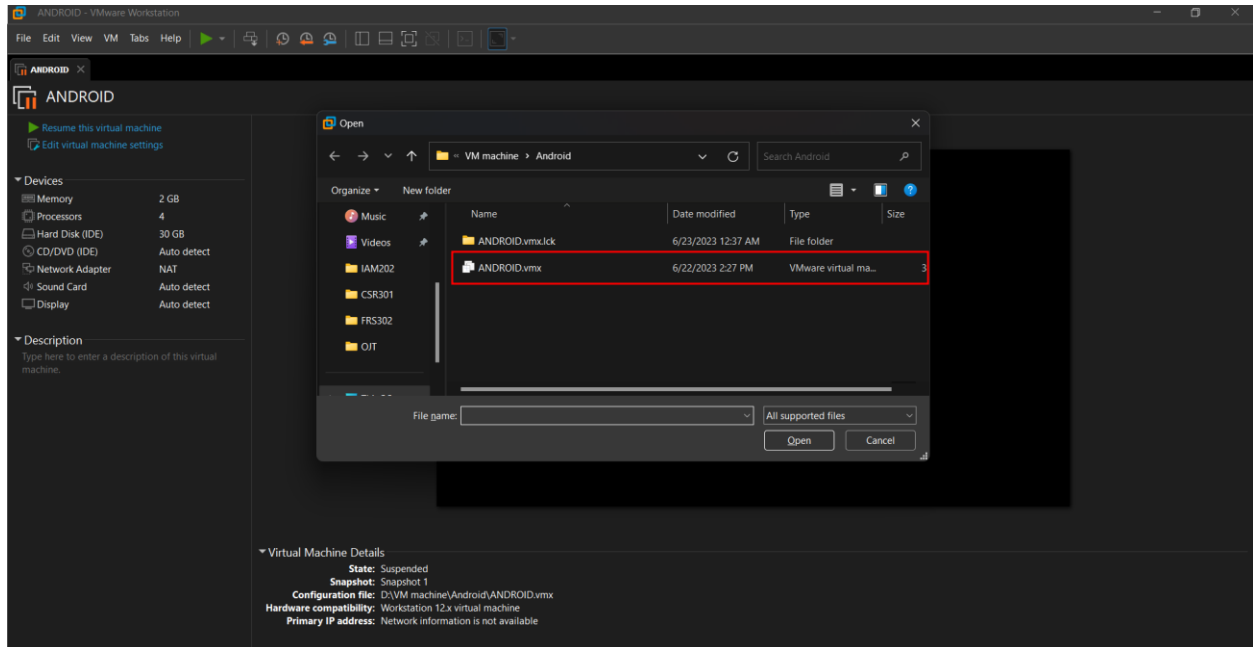
Thầy Mai Hoàng Đình
Trường đại học FPT

Người thực hiện
Đặng Hoàng Nguyên

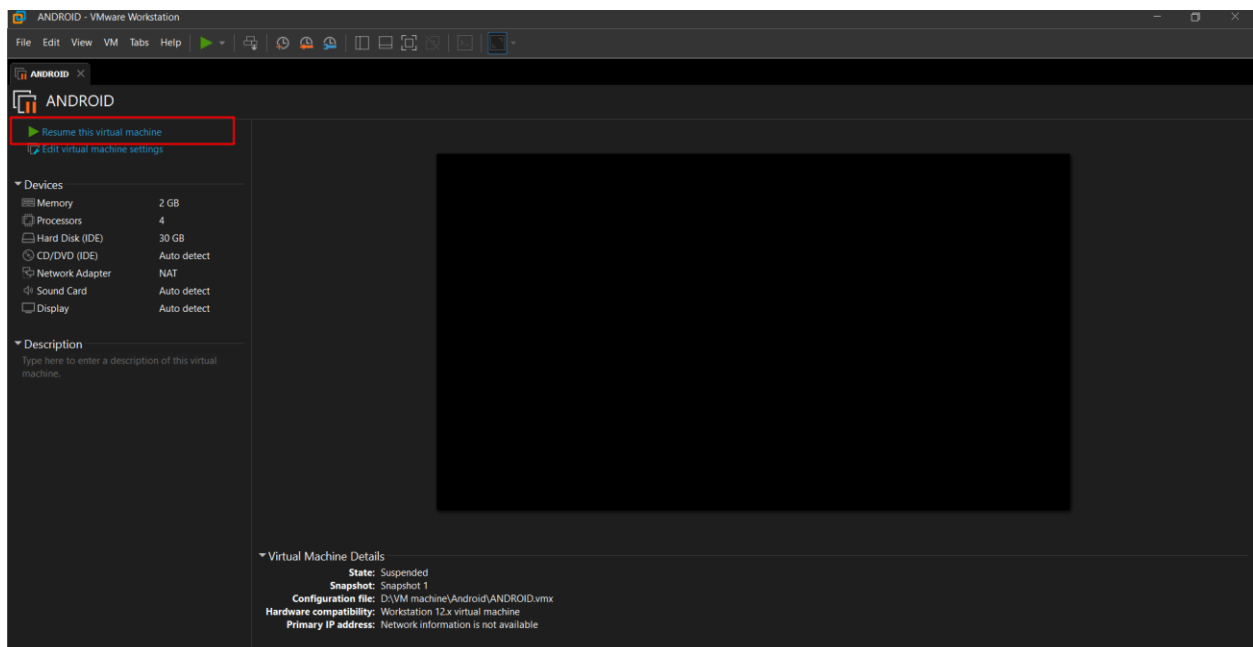
Acquiring a Forensic Image of an Android Phone

Creating an Android Virtual Machine

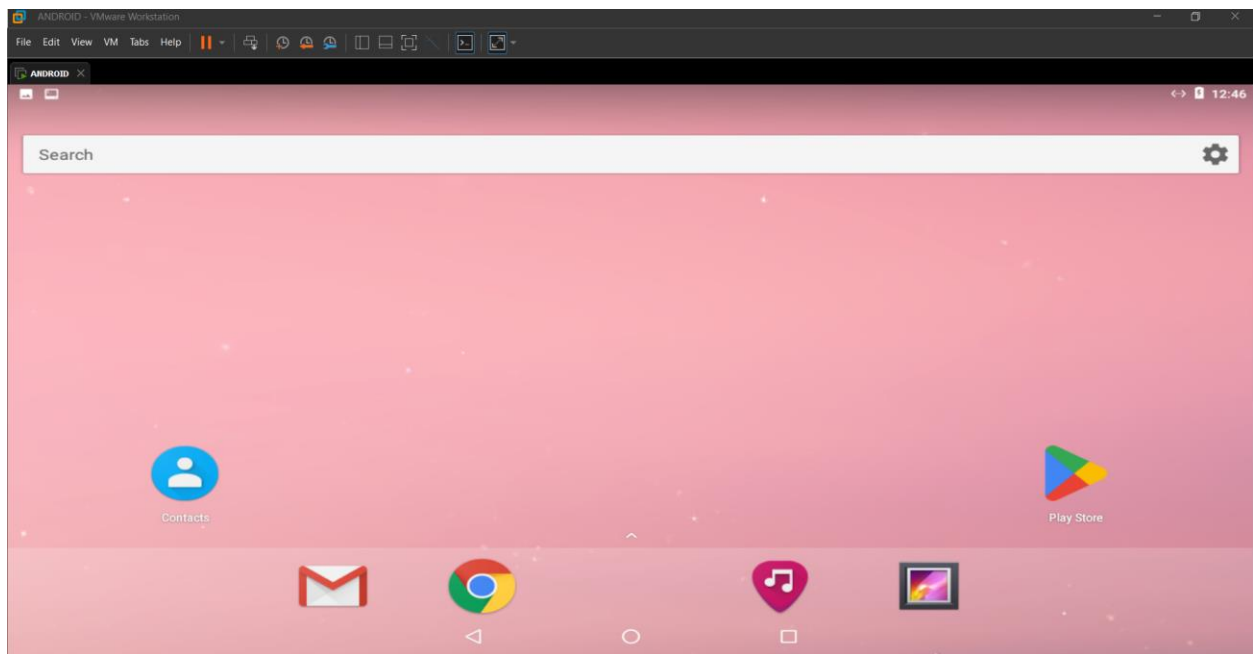
Ở bước này ta sẽ import file máy ảo android vào bên trong máy VMware của chúng ta bằng cách sử dụng đuôi file vmx. Chỉ cần click đúp vào bên trong hoặc nhấn tổ hợp Ctrl + O rồi sau đó lựa chọn file máy ảo cho phù hợp.



Sau khi import vào rồi ta sẽ có giao diện như hình dưới đây. Sau đó chỉ cần mở máy lên và vì nếu là lần đầu chạy file máy android này nên có thể VMware sẽ phải load một khoảng thời gian lâu.



Và đây là giao diện khi VMware đã load được file máy ảo Android vào bên trong máy:



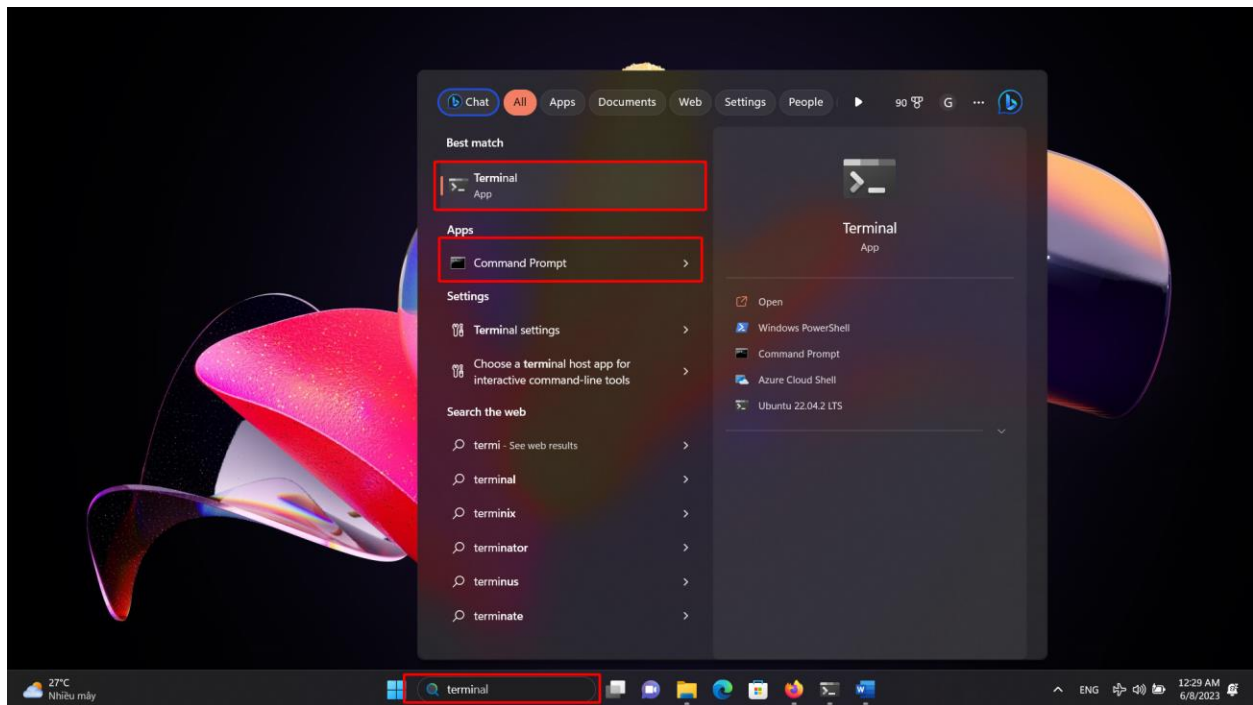
Task 2: Installing Android Studio

Downloading Android Studio

Trước khi cài đặt Android Studio, chúng ta phải check xem rằng máy của chúng ta đã có java chưa. Để kiểm tra rằng máy mình đã có java, thì chúng ta chỉ cần bật **CMD** hoặc **Terminal** lên bằng cách vào search và gõ **CMD** hoặc **Terminal**

Trong trường hợp này em sẽ dùng terminal vì tính tiện lợi của nó , vì có thể thực hiện nhiều câu lệnh giống trong môi trường linux

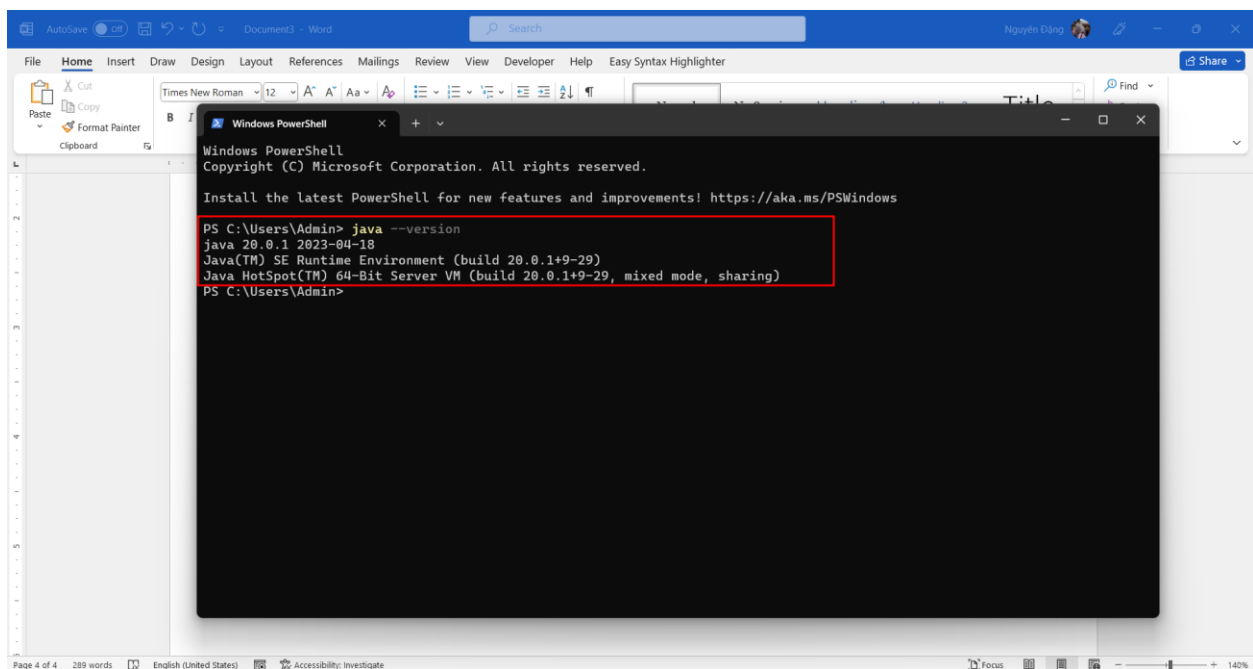
Nếu chưa có Terminal, ta có thể tải thông qua **Microsoft Store**, chỉ cần đơn giản tải search Terminal và phần việc còn lại để cho máy tự cài đặt



Sau đó ta sẽ khởi chạy câu lệnh

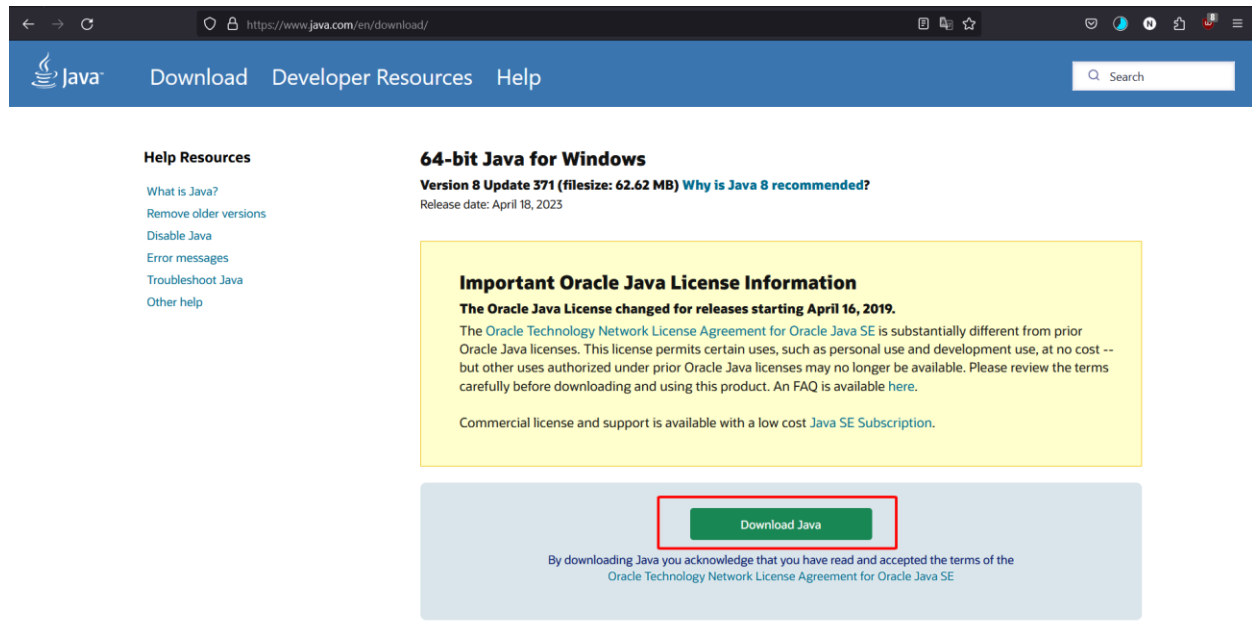
- Java -version

Câu lệnh trên giúp chúng ta kiểm tra xem bên trong máy của chúng ta đã cài các gói hỗ trợ của Java chưa



Như ta đã thấy hình trên thì máy tính này đã cài đặt Java.

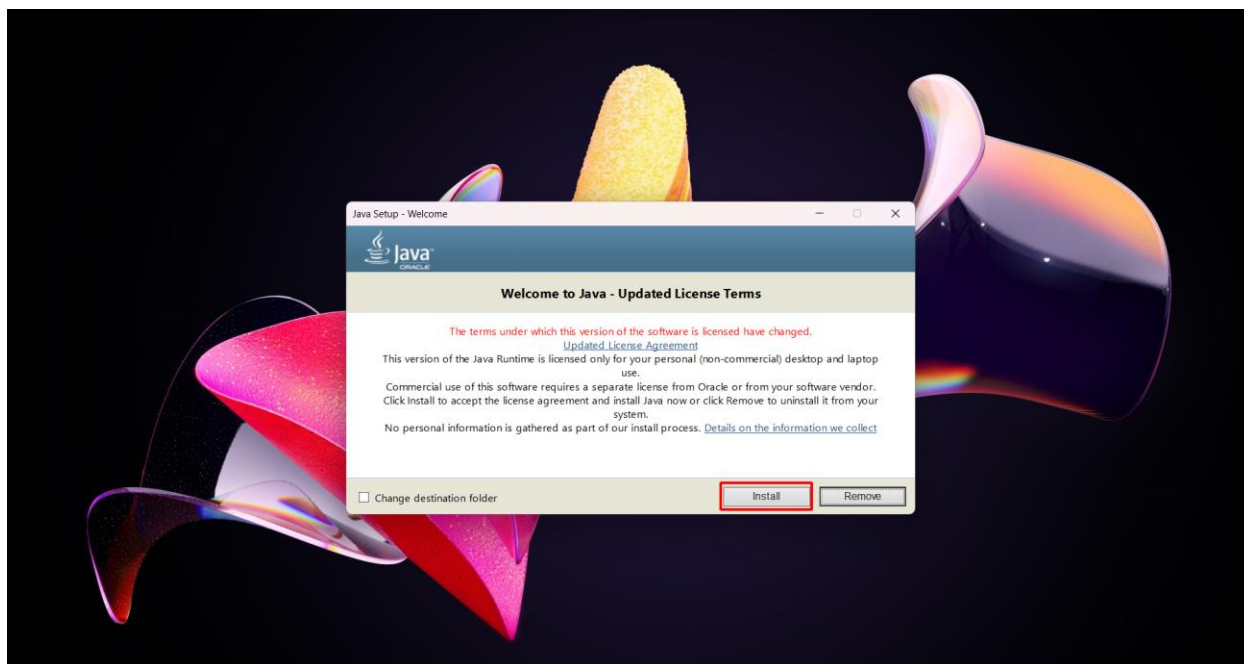
Trong trường hợp máy chưa có phần mềm Java thì chúng ta sẽ cần cài đặt thông qua đường link hướng dẫn sau: <https://www.java.com/en/download/>



Sau khi download xong, chúng ta chỉ cần chạy file đã download xuống. Trong trường hợp này nó nằm ở trong htuw mục Download của user:



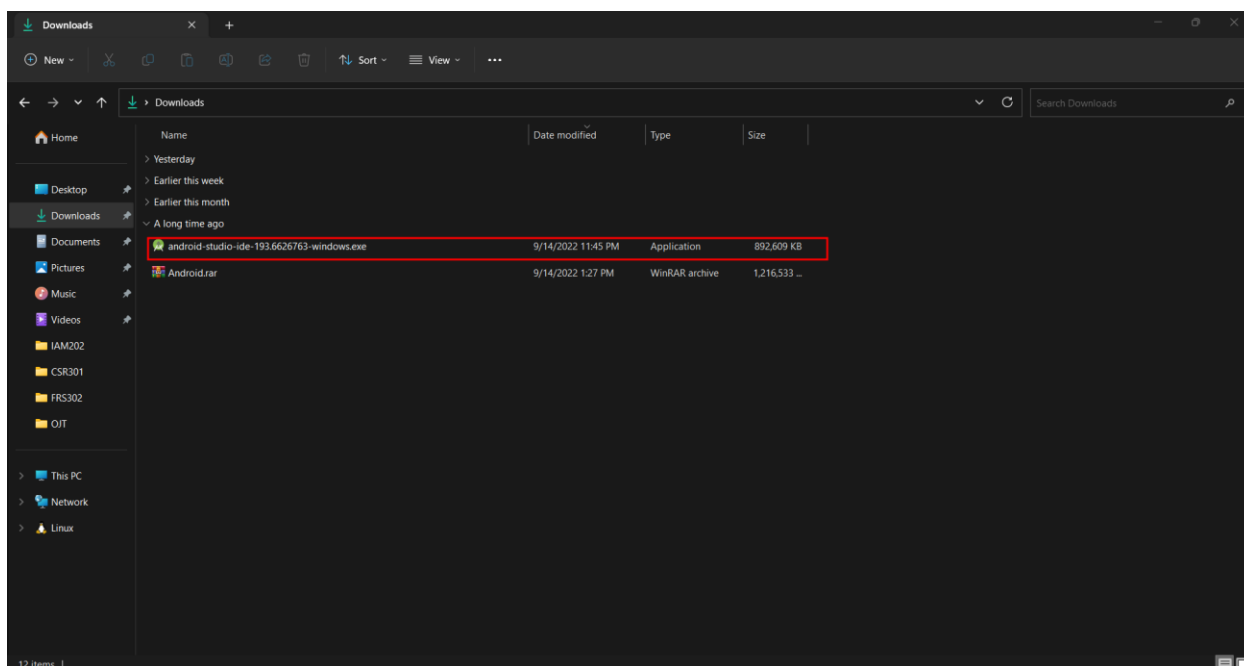
Sau khi nhấn cài đặt, chúng ta chỉ cần việc nhấn **Install** và để cho quá trình cài đặt JRE được tiến hành một cách tự động



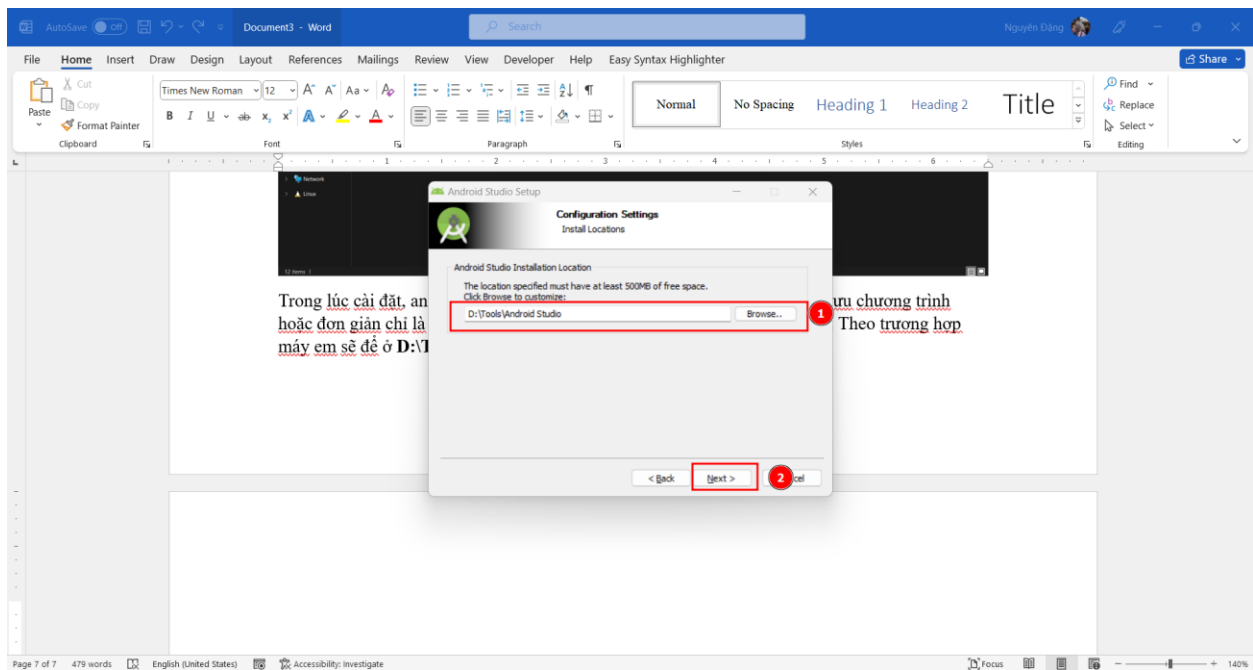
Sau khi cài đặt java xong, chúng ta sẽ bắt đầu cài đặt Android Studio bằng đường link sau:

- <https://developer.android.com/studio>

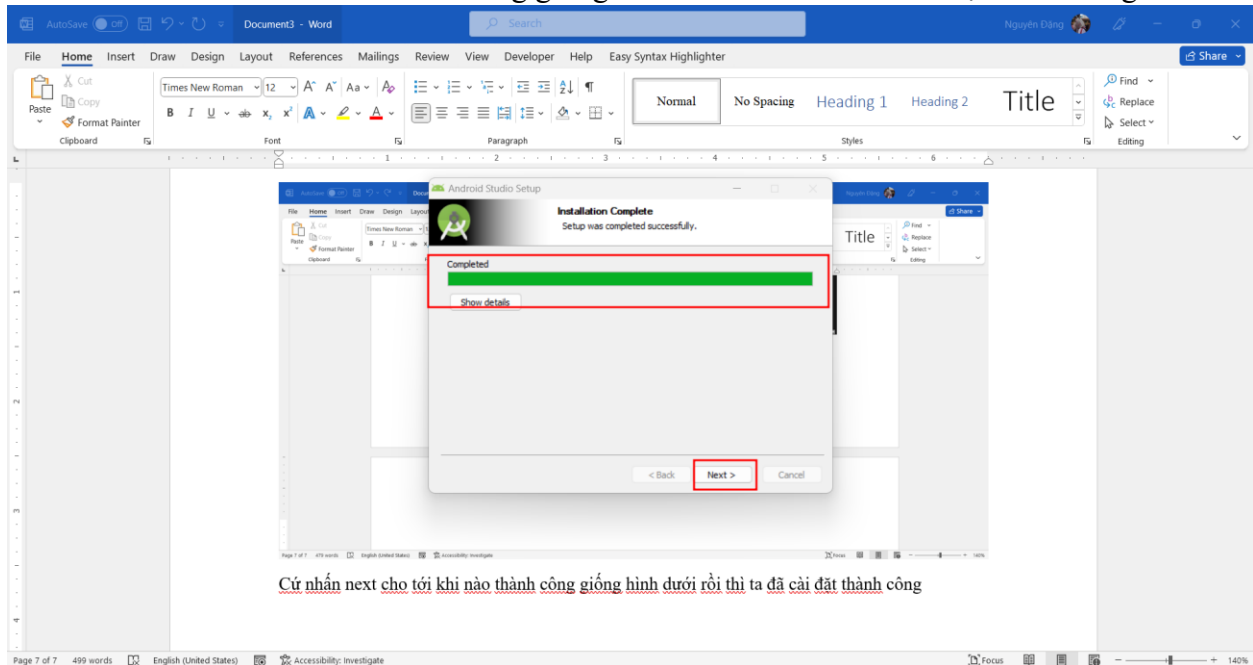
Sau khi tải xong thì ta sẽ vào thư mục mà đã download file. Trong trường hợp này là ở Downloads, click đúp vào file và sau đó khởi chạy cài đặt



Trong lúc cài đặt, android studio sẽ hỏi nơi lưu trữ, ta chỉ cần việc điền nơi lưu chương trình hoặc đơn giản chỉ là nhấn next nếu để theo vị trí mặc định của chương trình. Theo trường hợp máy em sẽ để ở **D:\Tools\Android Studio**



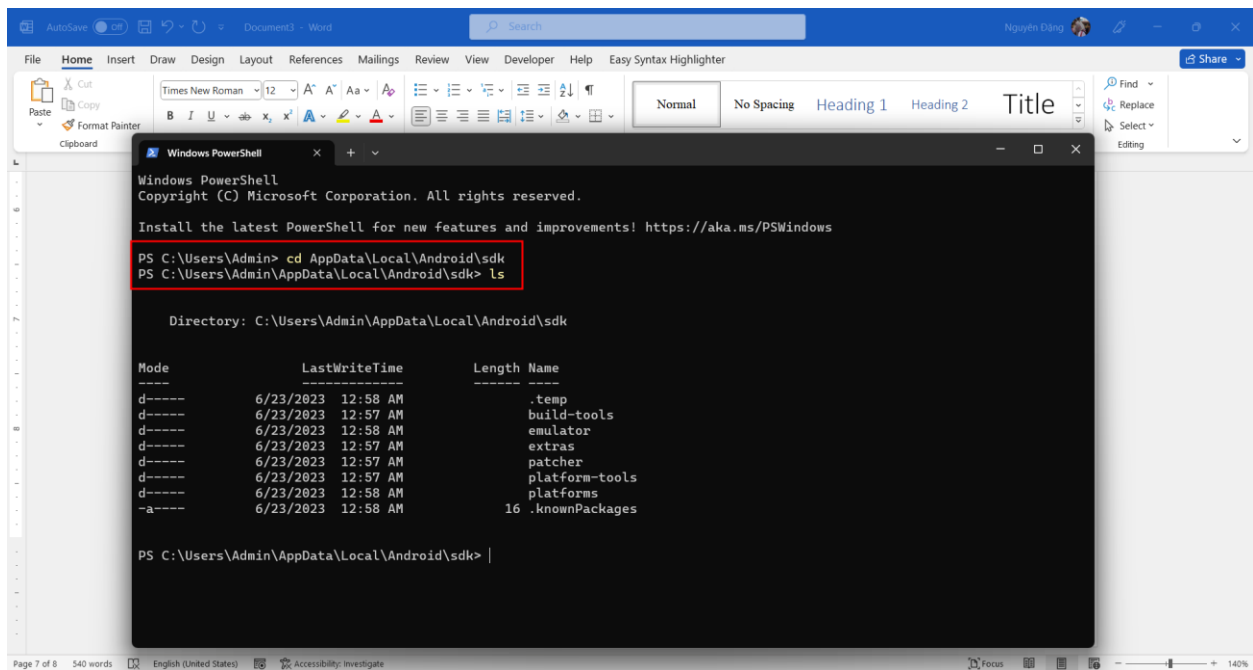
Cứ nhấn next cho tới khi nào thành công giống hình dưới rồi thì ta đã cài đặt thành công



Finding the SDK Path

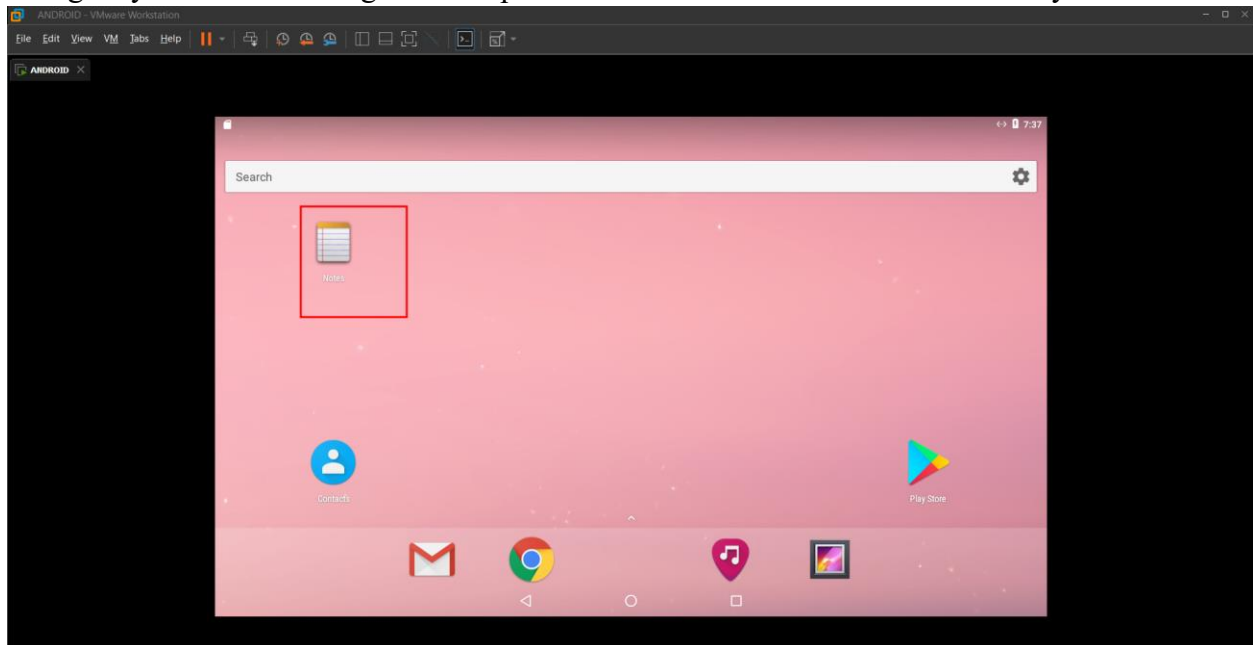
Bây giờ chúng ta phải tìm xem nơi lưu trữ SDK của chúng ta ở đâu bằng cách mở Terminal lên và di chuyển đến thư mục AppData\Local\Android\sdk và thực hiện câu lệnh ls

- cd AppData\Local\Android\sdk
- ls

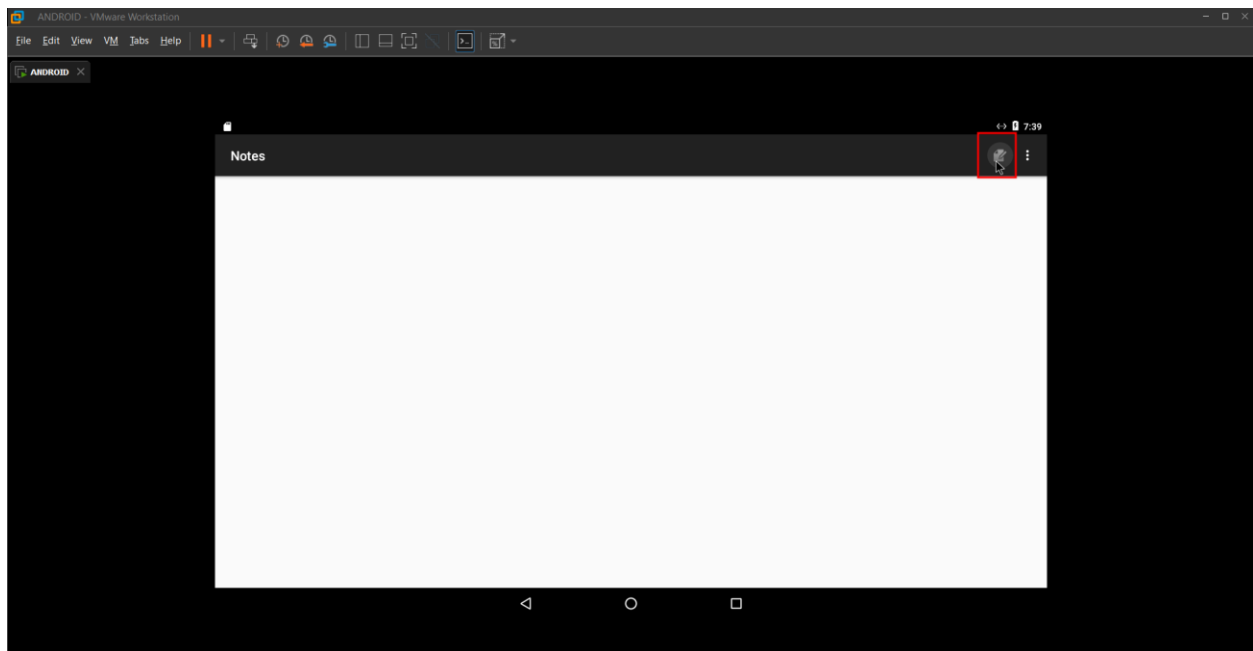


Task 3: Creating Evidence on the Android VM

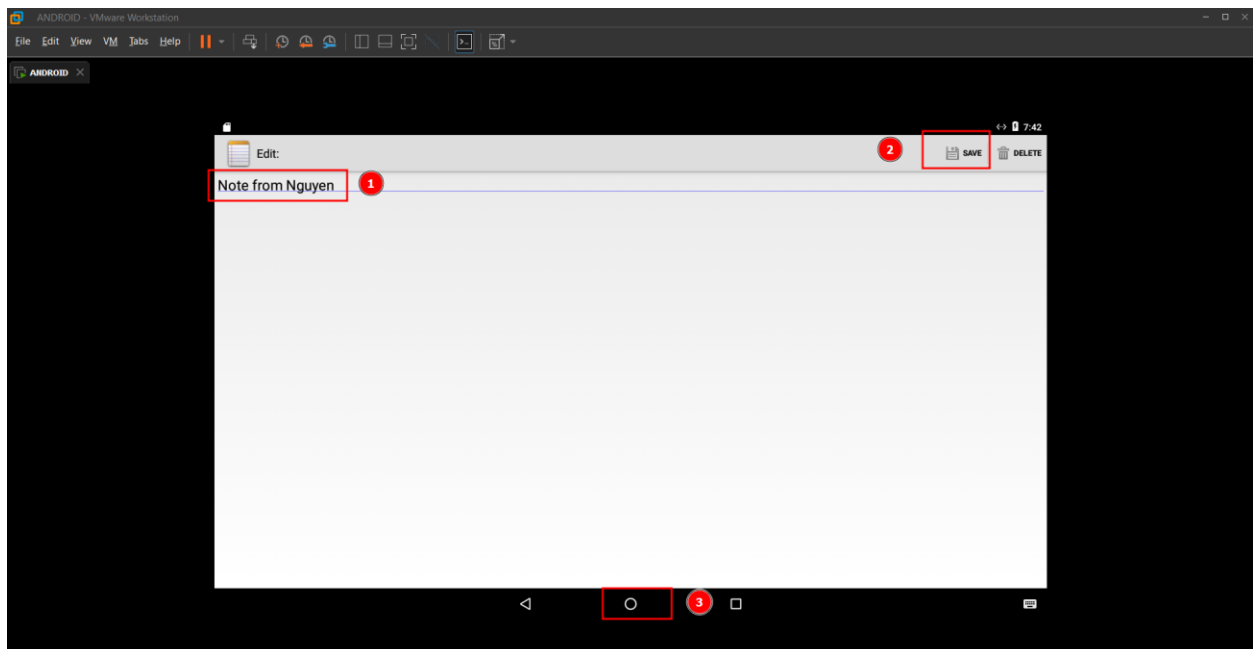
Trong máy ảo android chúng ta sẽ mở phần Note bên trên màn hình chính của máy.



Sau đó vào bên trong đó phía trên phải của màn hình và chọn New để có thể ghi Note



Sau đó ghi một cái gì đó lên trên note để lát nữa kiểm tra chuỗi ở bên trong máy. Trong trường hợp này ta sẽ ghi là: **“Note from Nguyen”**. Lưu lại và sau đó thoát ra màn hình chính và không tắt luôn ứng dụng note

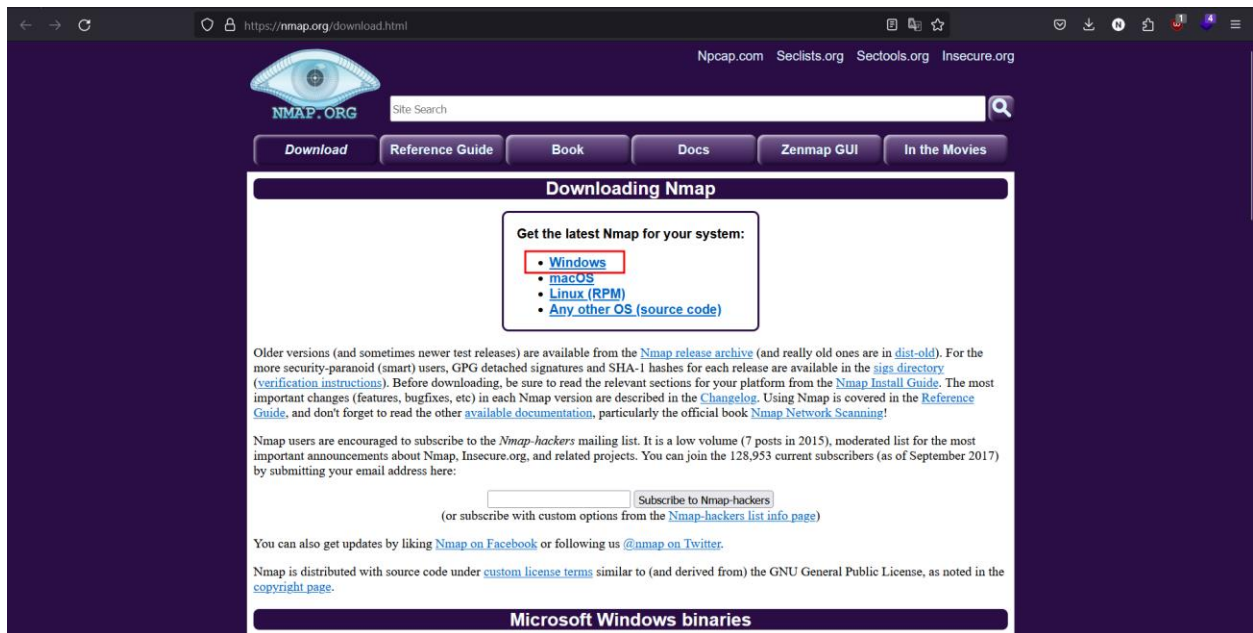


Task 4: Capturing a Live Image

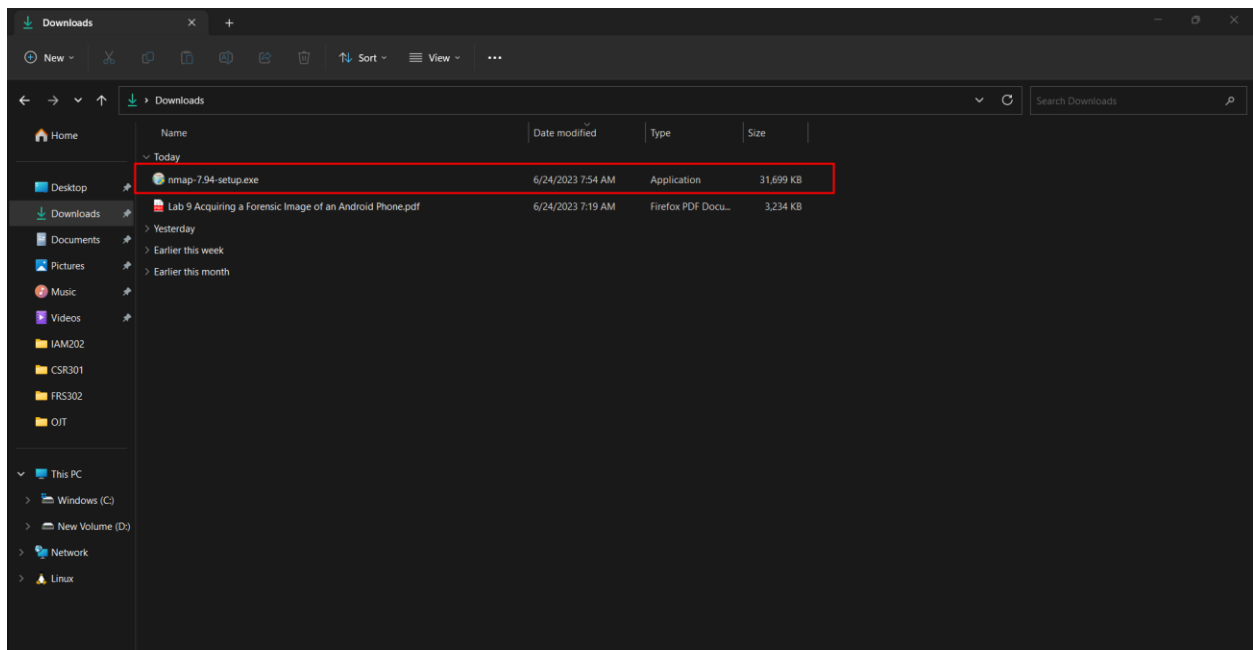
Ở bước này ta sẽ tiến hành cài công cụ nmap – một công cụ khá là hữu dụng tron việc dò port của một địa chỉ ip. Tại máy window chúng ta sẽ cài nmap để sử dụng command nc. Nó giống với câu lệnh nc (netcat) giống với linux.

Trên trình duyệt, chúng ta sẽ download nmap tại web chính thức của nhà phát hành:

- <https://nmap.org/download.html>



Vào trong thư mục đã Download và trong trường hợp này nmap đã được download ở folder Downloads. Double click vào chương trình và sau đó thì cho nó chạy cài đặt với chế độ mặc định để phù hợp với việc sử dụng trong bài lab dễ hơn



Sau đó chúng ta check thử xem máy đã sử dụng được netcat chưa thông qua Terminal. Bật Terminal lên và sử dụng netcat thử xem đã có chưa

- `ncat --help`

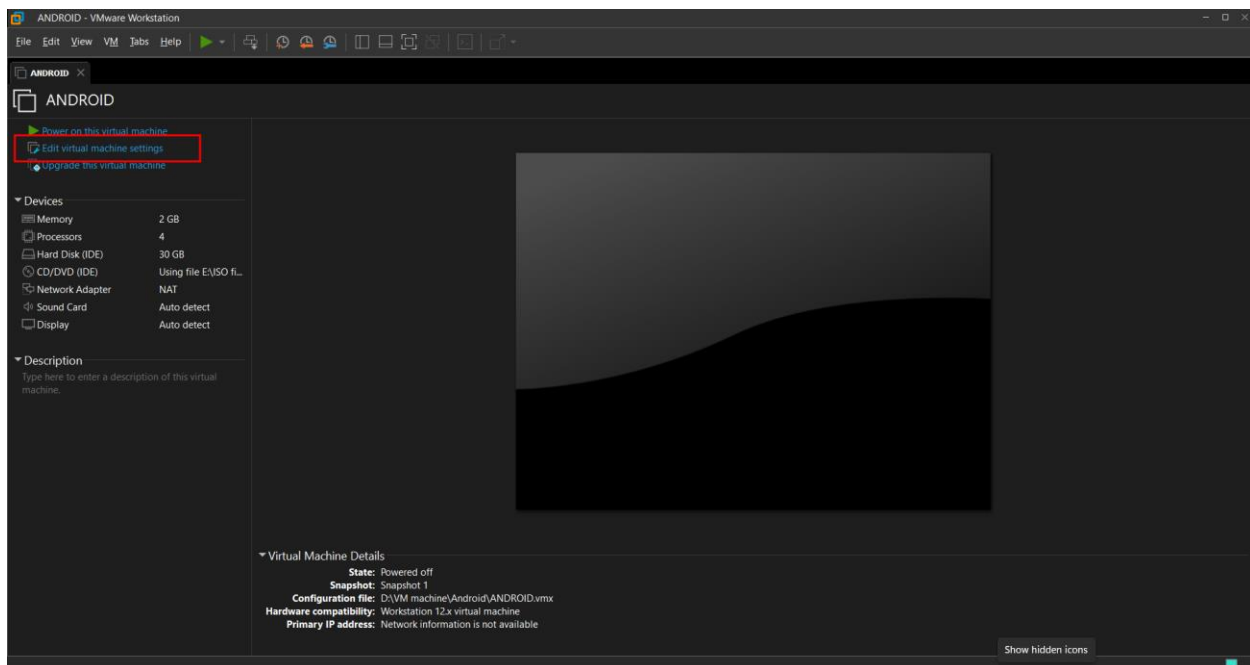
```
Windows PowerShell
PS C:\Users\Admin> ncat --help
Ncat 7.94 ( https://nmap.org/ncat )
Usage: ncat [options] [hostname] [port]

Options taking a time assume seconds. Append 'ms' for milliseconds,
's' for seconds, 'm' for minutes, or 'h' for hours (e.g. 500ms).
  -4                               Use IPv4 only
  -6                               Use IPv6 only
  -C, --crlf                       Use CRLF for EOL sequence
  -c, --sh-exec <command>         Executes the given command via /bin/sh
  -e, --exec <command>            Executes the given command
  --lua-exec <filename>           Executes the given Lua script
  -g hop1[,hop2,...]              Loose source routing hop points (8 max)
  -G <n>                           Loose source routing hop pointer (4, 8, 12, ...)
  -m, --max-conns <n>             Maximum <n> simultaneous connections
  -h, --help                       Display this help screen
  -d, --delay <time>              Wait between read/writes
  -o, --output <filename>         Dump session data to a file
  -x, --hex-dump <filename>       Dump session data as hex to a file
  -i, --idle-timeout <time>       Idle read/write timeout
  -p, --source-port port           Specify source port to use
  -s, --source addr               Specify source address to use (doesn't affect -l)
  -l, --listen                     Bind and listen for incoming connections
  -k, --keep-open                 Accept multiple connections in listen mode
  -n, --nodns                     Do not resolve hostnames via DNS
  -t, --telnet                     Answer Telnet negotiations
  -u, --udp                       Use UDP instead of default TCP
  --sctp                          Use SCTP instead of default TCP
  -v, --verbose                   Set verbosity level (can be used several times)
  -w, --wait <time>              Connect timeout
```

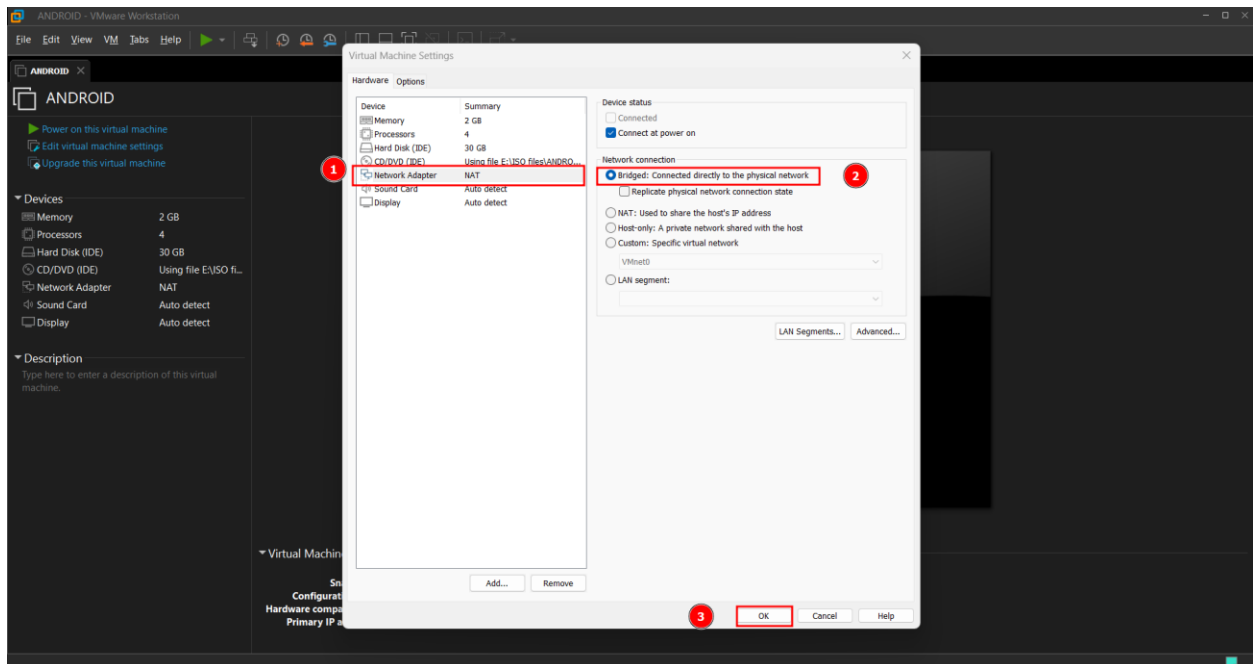
Configuring Bridged Networking

Vào trong máy Android, chúng ta sẽ mở ứng dụng Android Terminal lên như hình dưới đây

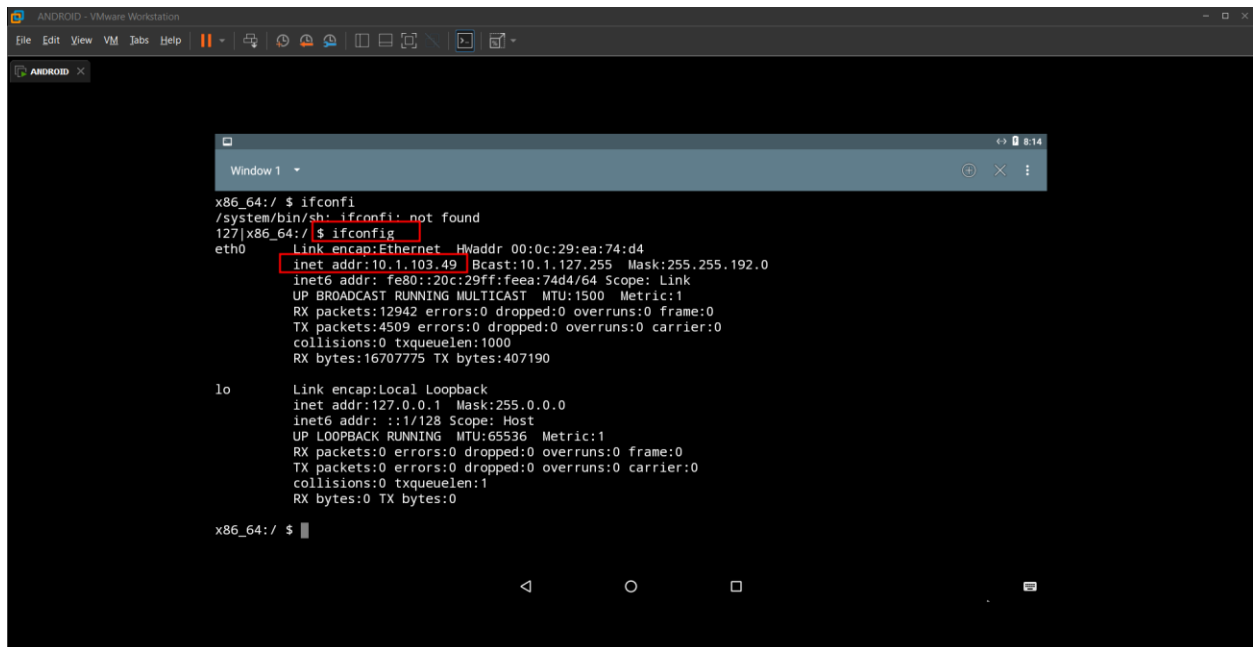
Bây giờ chúng ta sẽ tiến hành cài đặt card mạng bridged bằng cách shutdown máy trên VMWare bằng cách nhấn tổ hợp Ctrl + E và hiển thị như hình bên dưới. Sau đó nhấn vào phần “Edit virtual machine settings”



Sau đó vào phần Network Adapter và vào phần Netwrk Connection, chuyển từ NAT chúng ta sẽ chuyển đổi về Bridged và nhấn OK.



Sau đó chúng ta sẽ khởi động lại máy Android của chúng ta và test lại câu lệnh “ifconfig” bên trong Android Terminal. Ta thấy rằng địa chỉ ip lúc này đang là 10.1.103.49



Connecting to the Android Device with Android Debug Bridge (ADB)

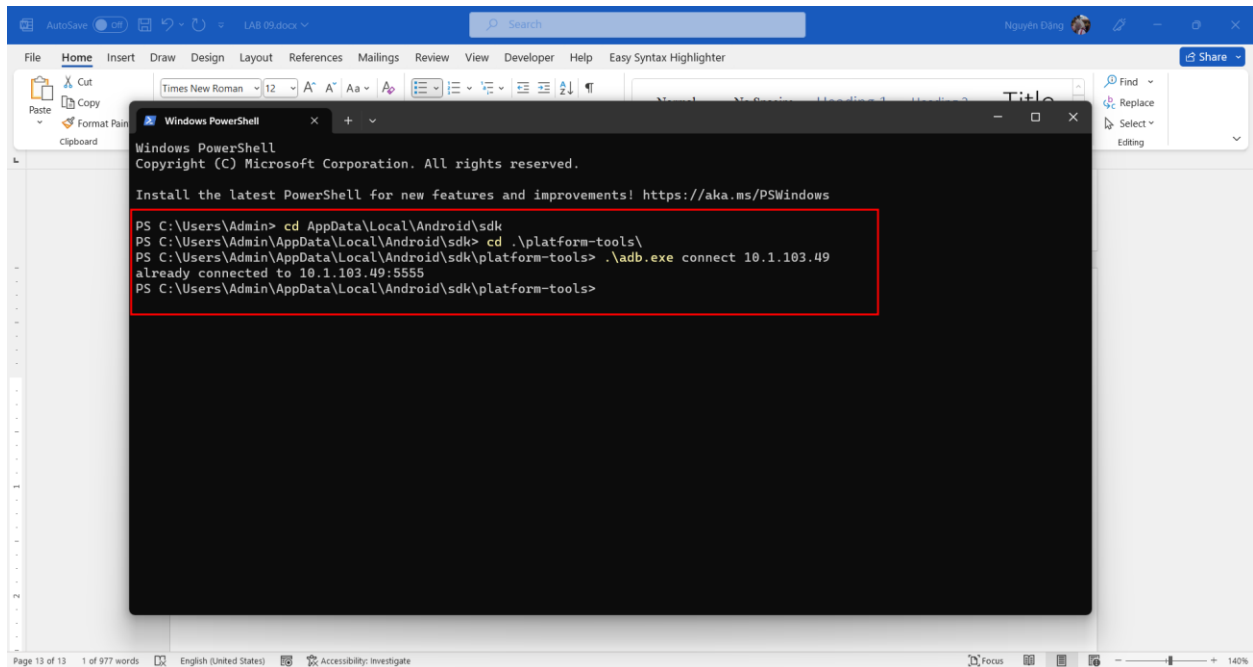
Trên máy chính của chúng ta, chúng ta sẽ vào trong terminal và đến nơi chứa đường dẫn SDK mà chúng ta đã cài đặt từ trước đó. Trong trường hợp đường dẫn mặc định của chúng sẽ theo đường dẫn sau:

- AppData\Local\Android\sdk

Thực hiện các câu lệnh sau theo tuần tự:

- `cd AppData\Local\Android\sdk`
- `cd platform-tools`
- `.\adb.exe connect <ip máy android>`

Như ta thấy vậy là chúng ta đã connect thành công vào máy android



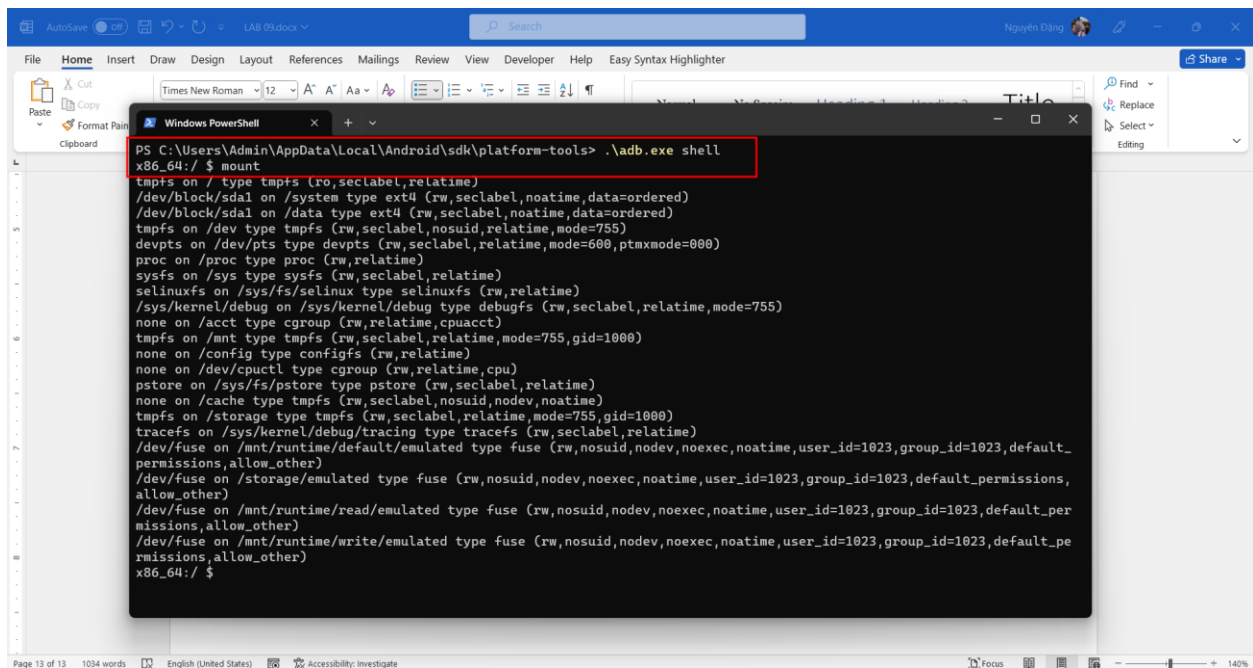
The screenshot shows a Windows PowerShell window with the following commands and output:

```
PS C:\Users\Admin> cd AppData\Local\Android\sdk
PS C:\Users\Admin\AppData\Local\Android\sdk> cd .\platform-tools\
PS C:\Users\Admin\AppData\Local\Android\sdk\platform-tools> .\adb.exe connect 10.1.103.49
already connected to 10.1.103.49:5555
PS C:\Users\Admin\AppData\Local\Android\sdk\platform-tools>
```

Examining the Filesystem of the Android Device

Sau khi kết nối thành công tới máy android chúng ta sẽ thực hiện câu lệnh sau:

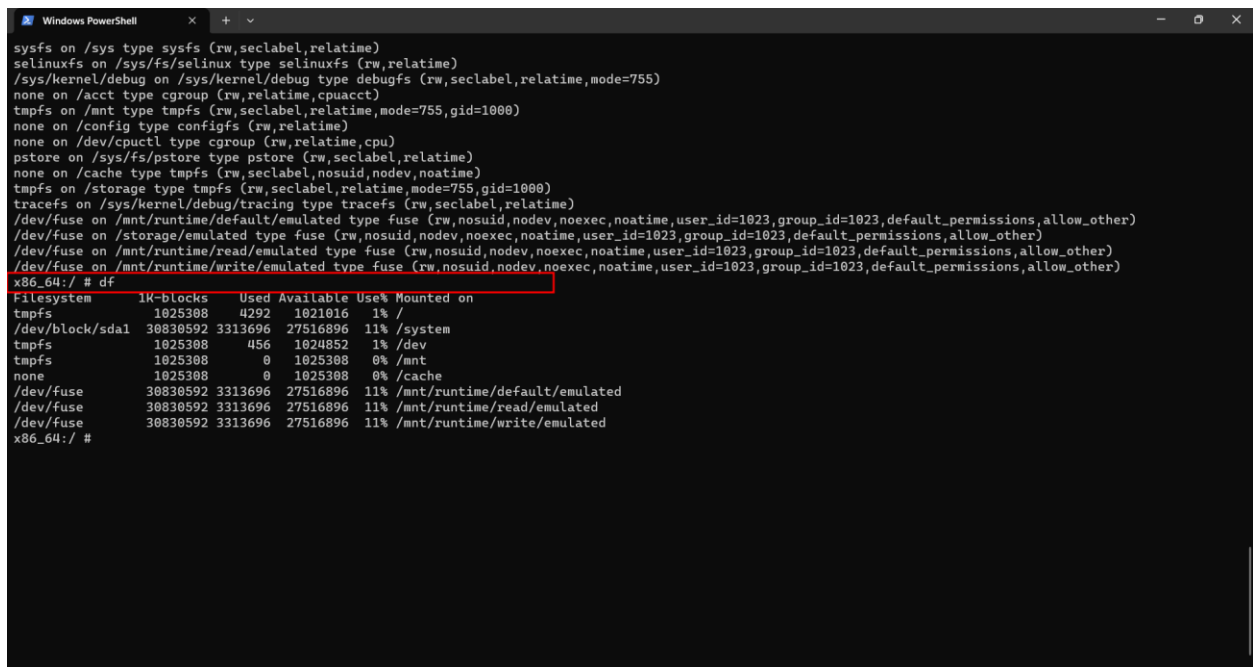
- `.\adb.exe shell`
 - Câu lệnh giúp chúng ta có thể vào bên trong shell của con android
- `Mount`
 - Câu lệnh giúp chúng ta có thể xem tất cả các ổ đĩa đang có bên trong máy android



Android cũng được xem như là một hệ điều hành Linux, ta cũng sẽ thấy rằng phần data của thẻ Android ccauas trúc nó cũng được lưu dưới dạng dev/block/sda1

Sau đó sử dụng câu lệnh sau đây:

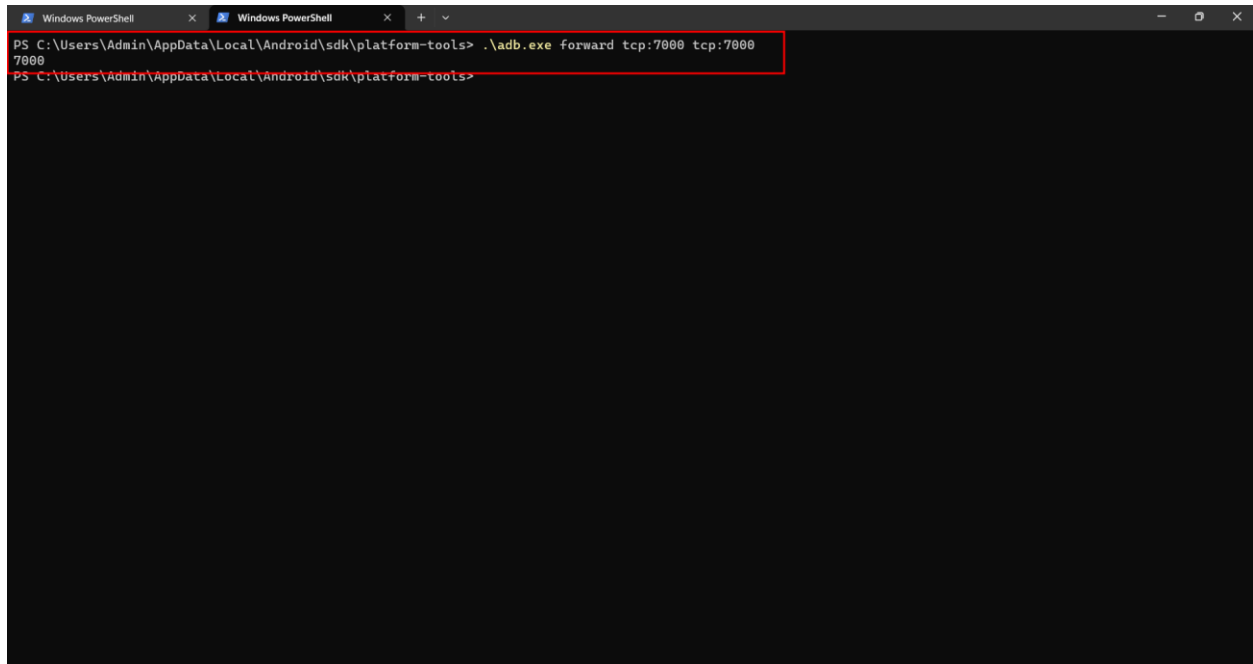
- Df
 - Câu lệnh này cho phép chúng ta xem dung lượng ổ đĩa trên android



Configuring Port Forwarding

Bây giờ trên Terminal chúng ta mở thêm một cửa sổ Terminal khác và vào bên trong `AppData\Local\Android\sdk` và chúng ta sẽ forward tcp thông qua câu lệnh sau:

- `.\adb.exe forward tcp:7000 tcp:7000`
 - Đây là câu lệnh giúp chúng ta có thể forward gói tin đến với máy chính thông qua port 7000

A screenshot of a Windows PowerShell terminal window. The window has a title bar with "Windows PowerShell" and standard minimize, maximize, and close buttons. The terminal content shows the command `.\adb.exe forward tcp:7000 tcp:7000` being entered at the prompt `PS C:\Users\Admin\AppData\Local\Android\sdk\platform-tools>`. The command is highlighted with a red rectangular box. The prompt for the next line is `PS C:\Users\Admin\AppData\Local\Android\sdk\platform-tools>`.

Performing a Network Acquisition

Tiếp theo đó bên trong powershell ban đầu, chúng ta sẽ bắt đầu thực hiện vào quyền su (root) và bắt máy Android sẽ phải listen trên cổng 7000 và gửi image đến coonrgd đã được kết nối

- `su`
- `dd if=/dev/block/sda1 | busybox nc -l -p 7000`

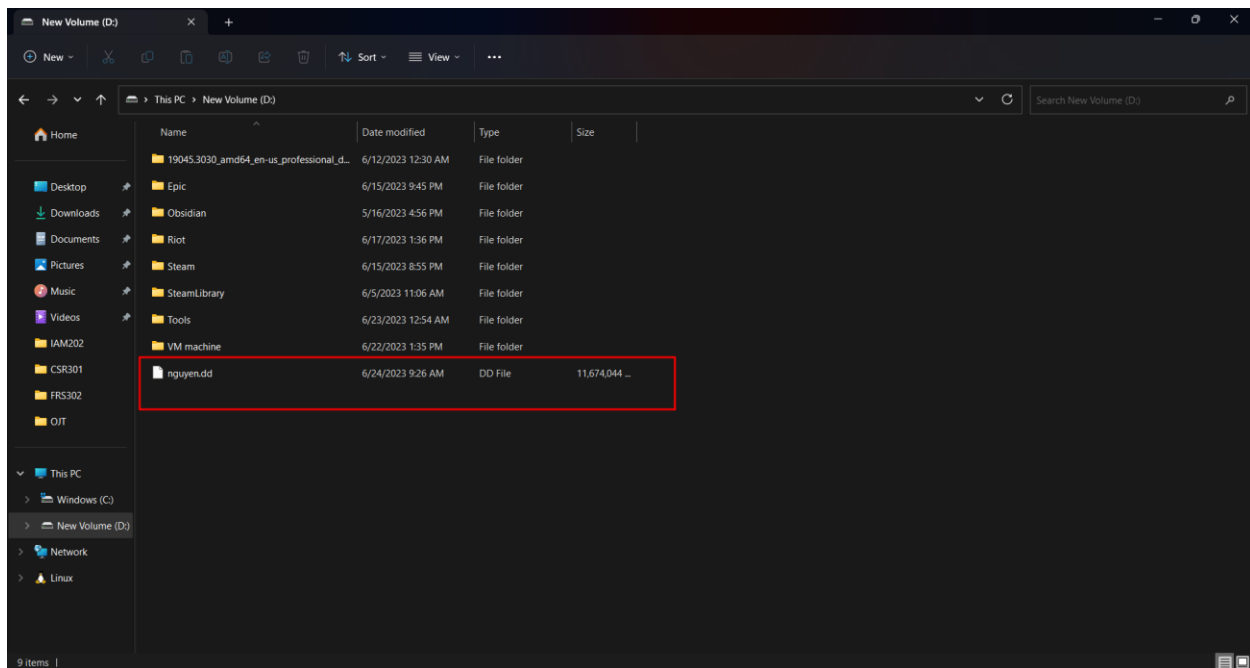
Bây giờ chúng ta sẽ chạy cmd dưới quyền admin và thực hiện câu lệnh sau::

- `ncat 127.0.0.1 7000 > D:/nguyen.dd`

```
Windows PowerShell x Windows PowerShell x + v
x86_64:/ # dd if=/dev/block/sda1 | busybox ncat -l -p 7000
ncat: applet not found
1|x86_64:/ # dd if=/dev/block/sda1 | busybox nc -l -p 7000
62910477+0 records in
62910477+0 records out
32210164224 bytes transferred in 2276.979 secs (14146088 bytes/sec)
x86_64:/ #
```

```
Administrator: Command Prompt - ncat 127.0.0.1 7000
C:\Windows\System32>ncat 127.0.0.1 7000 > D:/nguyen.dd
nc
C:\Windows\System32>ncat 127.0.0.1 7000 > D:/nguyen.dd
```

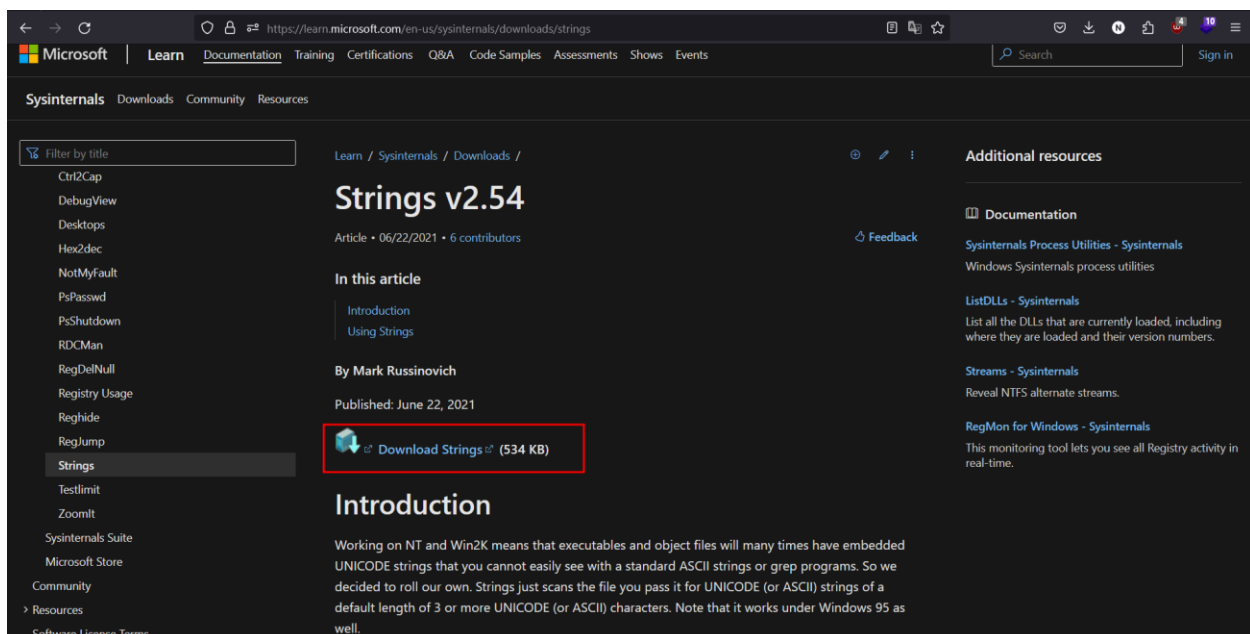
Như ta có thể thấy rằng file đã được dump thành công. Vào check bên trong thư mục chúng ta vừa tải xuống đó chính là ổ D với tên là nguyen.dd



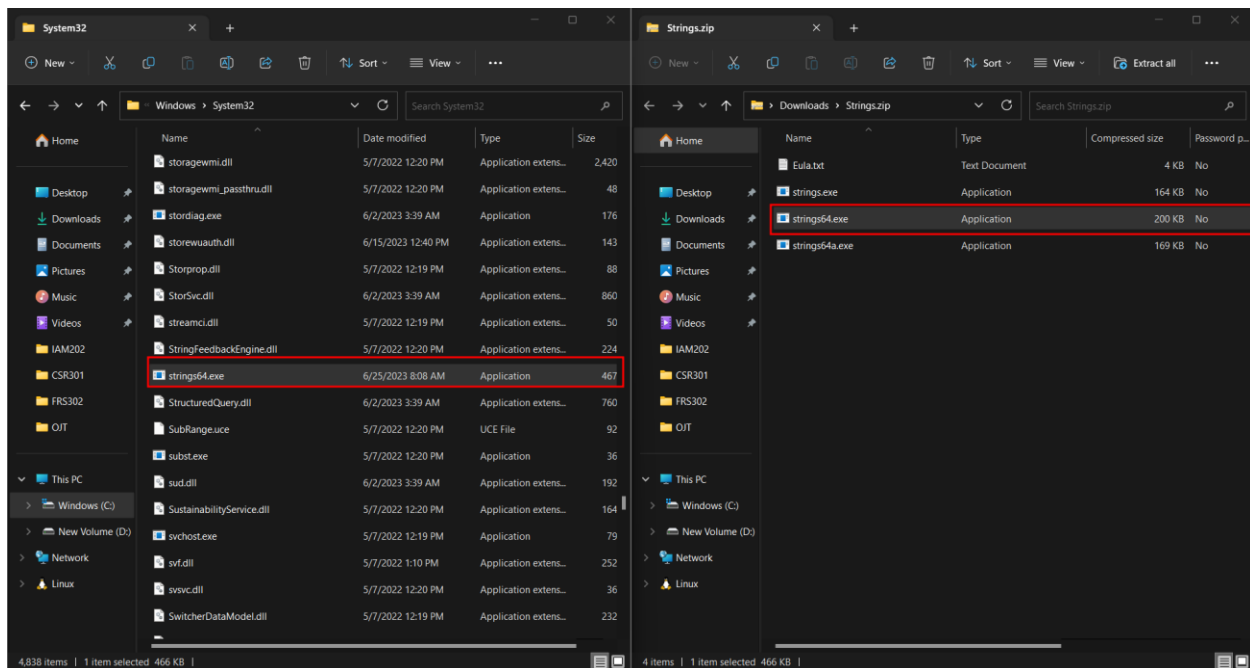
Installing Strings

Bây giờ chúng ta sẽ bắt đầu phân tích thông qua strings, bây giờ chúng ta sẽ lên trang web sau đây để có thể lưu file về.

- <https://technet.microsoft.com/en-us/sysinternals/bb897439>



Sau khi tải xong, chúng ta cần phải giải nén và để trong thư mục C:\\Windows\\System32. Bên trong folder có 3 file exe, một file dành cho 32bit và 2 file dành cho máy 64bit. Vì là máy 64bit nên chúng ta sẽ chọn file 64bit



Sau khi hoàn tất, mở terminal lên và thử câu lệnh với cú pháp sau đây để test rằng câu lệnh hoạt động một cách đúng đắn. Như ta thấy hình bên dưới thì câu lệnh đã thực hiện thành công

```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>
C:\Users\Admin>strings

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: strings [-a] [-f offset] [-b bytes] [-n length] [-o] [-s] [-u] <file or directory>
-a      Ascii-only search (Unicode and Ascii is default)
-b      Bytes of file to scan
-f      File offset at which to start scanning.
-o      Print offset in file string was located
-n      Minimum string length (default is 3)
-r      Recurse subdirectories
-u      Unicode-only search (Unicode and Ascii is default)
-nobanner
        Do not display the startup banner and copyright message.

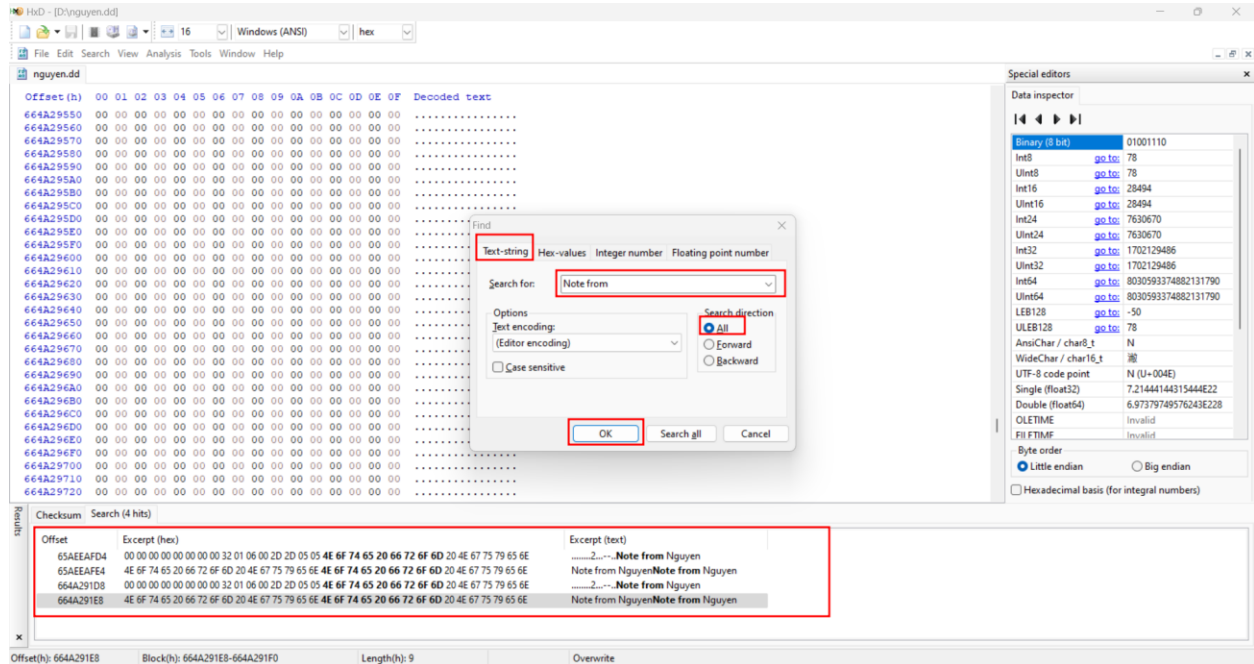
C:\Users\Admin>
```

Bây giờ chúng ta sẽ vào bên trong thư mục chứa file android và kiểm tra xem note của chúng ta có bên trong file disk ổ đĩa không. Trong trường hợp này file android đang ở bên trong ổ D nên ta sẽ cd vào ổ D và tìm strings với câu lệnh sau:

- strings nguyen.dd | findstr "Note from Nguyen"

- Câu lệnh này giúp chúng ta tìm những ascii có trong Nguyen.dd và sau đó tìm chuỗi Note from Nguyen, tương tự như câu lệnh grep bên trong linux

Hoặc cách thứ hai có thể làm là load ổ đĩa vào bên trong HxD, sau khi load xong, ta nhấn tổ hợp Ctrl F và chọn “text string” và trong mục “search for” và tìm chữ “Note form”. Quá trình có thể diễn ra chậm do file tận 20gb. Và kết quả được hiển thị như hình bên dưới:



Vậy là chúng ta đã phân tích ổ đĩa đơn giản một cách thành công