MINOR PROJECT

NAME: Ankith Ram

EMAIL ID: ankitram951@gmail.com

INTERNSHIP PERIOD: FEB – MARCH (2023)

SMARTKNOWER STUDENT

CONTENTS

1. ABOUT PROJECT
2. Information Gathering on Websites
3. Penetration Testing on System
4. Malware Creation, Exploitation, and Mobile Hacking
5. Website Penetration Testing
6. Data Encryption, Decryption, and Hiding of Secret Messages

ABOUT PROJECT

Business Logic:

Nowadays, most companies are looking for penetration testers and ethical hackers to secure their networks and web applications from Black Hat Hackers. Most of the companies are doing projects on web applications and creating a network for start-ups. They perform penetration testing and hand over network reports to the client if the application or network is hacked. This helps the companies to understand the importance of cybersecurity and penetration testing.

Consideration/Scenario:

A web development company configured its network with many devices and started working on website development. They hired you as a penetration tester, and you need to perform penetration testing on all of their client's systems, mobiles, and websites. To test the systems' security, you must verify the system by creating a virus/trojans and injecting it into the system. This will help you analyze how the system is getting affected by the virus.

After these tests are completed, you also need to ensure that the information transferred through email by the employees of the organization is also safe. For that purpose, you need to perform data encryption and steganography techniques to hide the information. Make a report of all the tests and share it with the administrator to take further actions.

To start with the testing, we need to gather information about the website. To do so, perform the below tasks:

1. **Information Gathering on Websites**
    - Create a lab with Oracle Virtual Box or VMware with Kali Linux OS, Windows 7, and Windows XP.
    - Gather information about Instagram (website).

After information gathering, we need to test the company's security network as well. To do so, we will test their local system and its operating system (operating system). So, we need to perform enumeration and penetration testing on the company system.

2. **Penetration Testing on System**
    - Test the Windows security using the ProRat and get access to the key logs. Delete the files from desktop or C drive and execute the commands to create a new folder in desktop and upload any file from your system.

Now, after testing the system/network, we must test the antivirus in their system. To do so, we will create a virus and inject it in their system to determine/exploit the vulnerabilities of it.

3. **Malware Creation, Exploitation, and Mobile Hacking**
    - Create a virus using Tetrabit Virus Maker and execute the virus in the victim machine.

- Hack the mobile device using online tool MTF, gather the call list contacts, and access the camera.

After exploiting the system's vulnerabilities, we must also test and exploit the vulnerabilities of the client websites. To do so, we need to perform penetration testing and DOS injection attack on their websites.

4. **Website Penetration Testing**
    - Perform a DOS attack on windows 7 virtual machine using the LOIC tool and check the performance.
    - Test the website using BlindSQL to Bypass Admin panel Authentication manually for https://demo.testfire.net/ website.

After testing the systems and websites, one possibility that can steal sensitive information is from the communication medium, that is, email communications. We need to secure this transmission of messages by performing data encryption and hiding secret messages.

5. **Data Encryption, Decryption, and Hiding of Secret Messages**.
    - Hide the secret text file in the image using command prompts and SNOW tool.

Summary:

You will perform all the tests and create a report of the vulnerabilities found and provide it to the concerned department so that the loopholes can be fixed. Once this is done, you will help the company hide their secret information/conversations by encrypting the information and storing it in an image form.

Tools Covered in the Project:

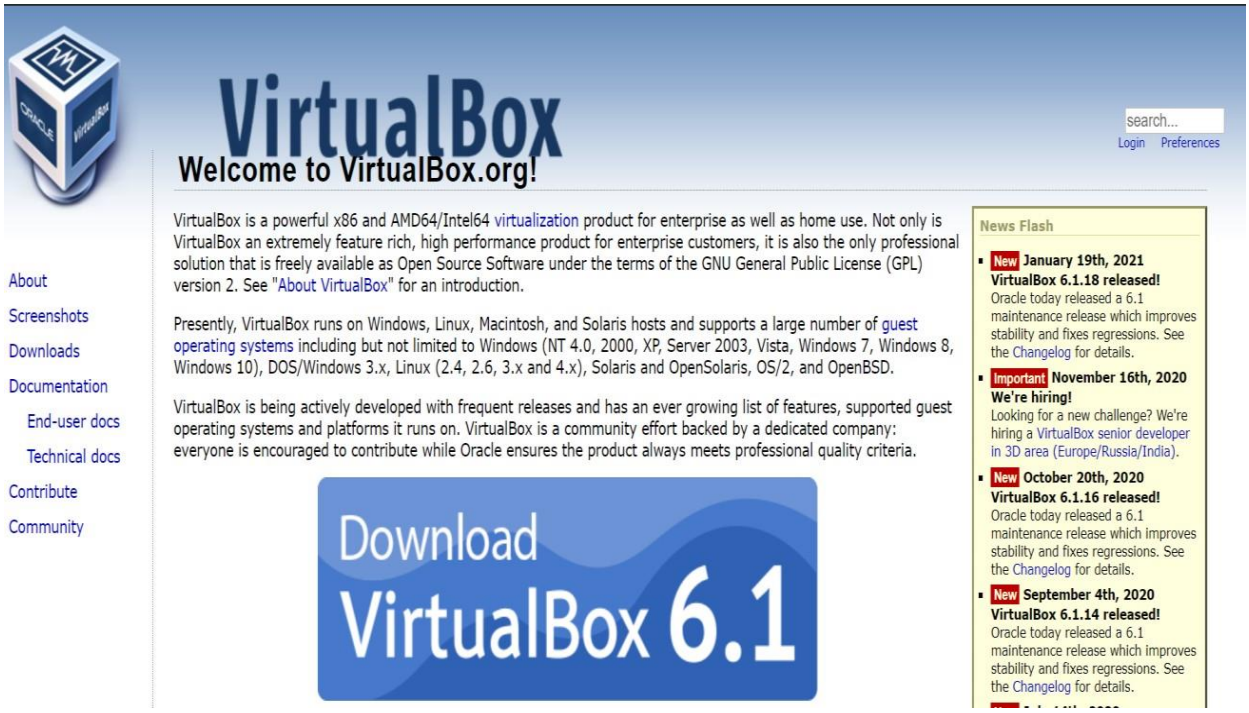
- ProRat
- Tetrabit Virus Maker
- LOIC Tool
- Mobile Tracker Free (MTF)
- SNOW Tool
- Manual Footprinting and BlindSQL Authentication Injection

LAB INSTALLING

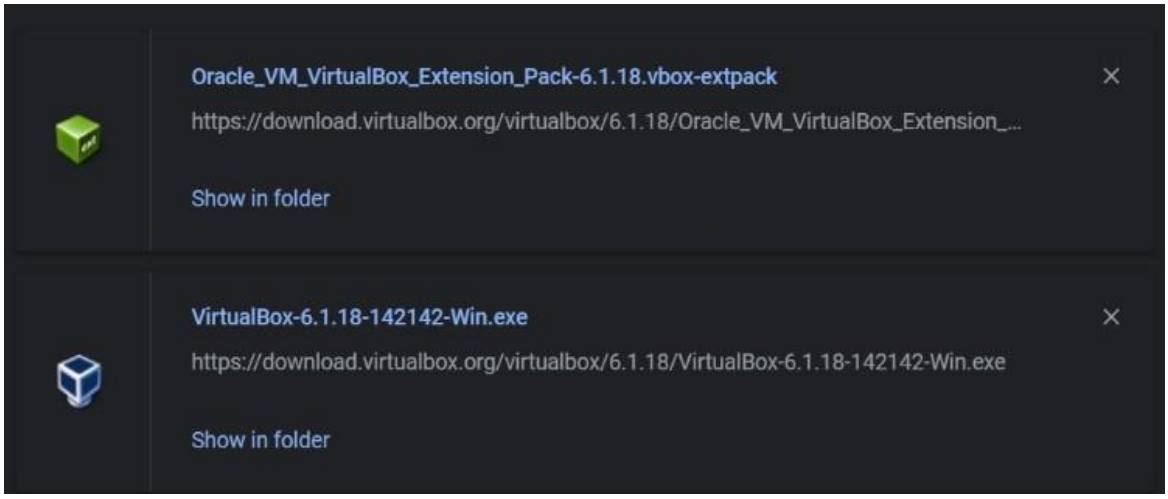
1. **Information Gathering on Websites**
   Create a lab with Oracle Virtual Box or VMware with Kali Linux OS, Windows 7, and Windows XP.

Oracle VM Virtual Machine Installation

Visit https://www.virtualbox.org/ and download Virtual box 6.1 (latest version).

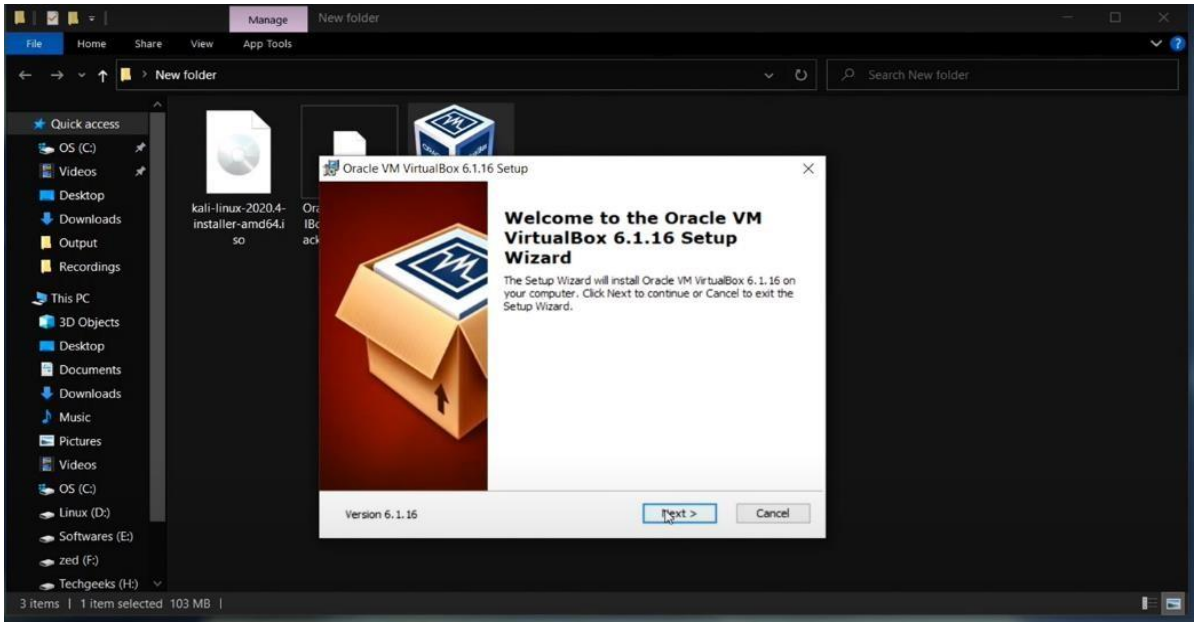


Open in folder and download its extension pack too.

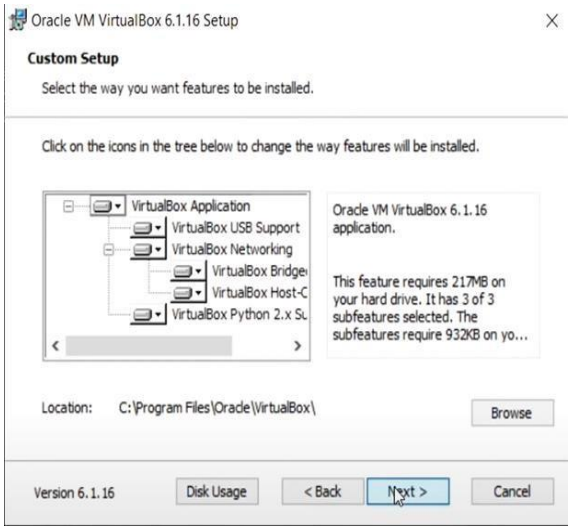


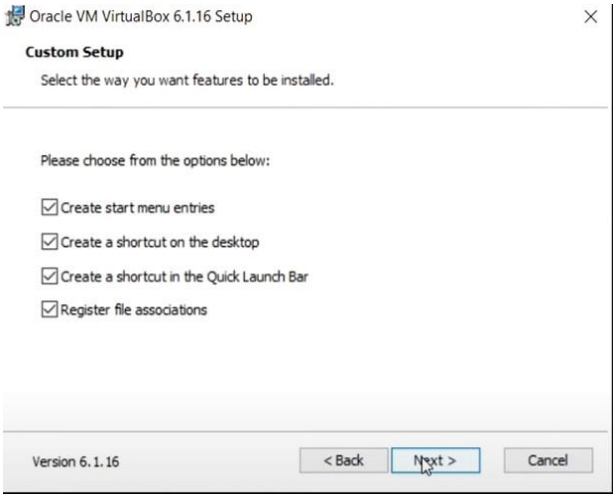
Start Installing.

Click on next.



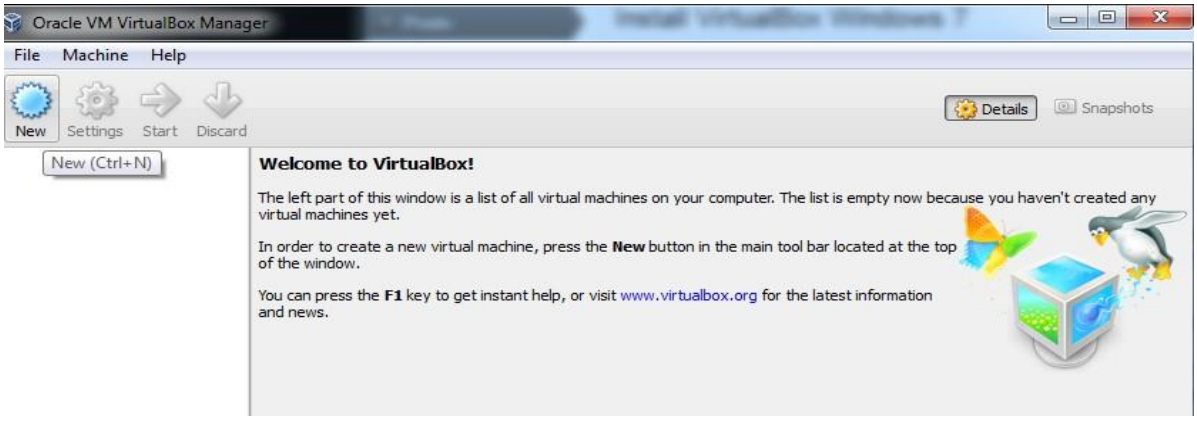
Click on next.





Click on install and finish.

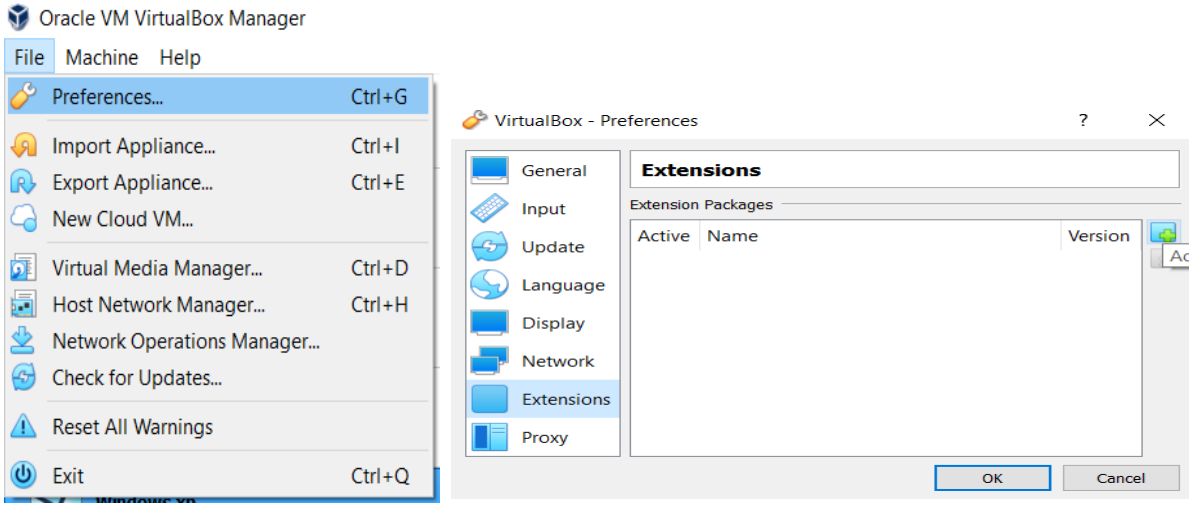
Here, Oracle VM Virtual Box is installed.



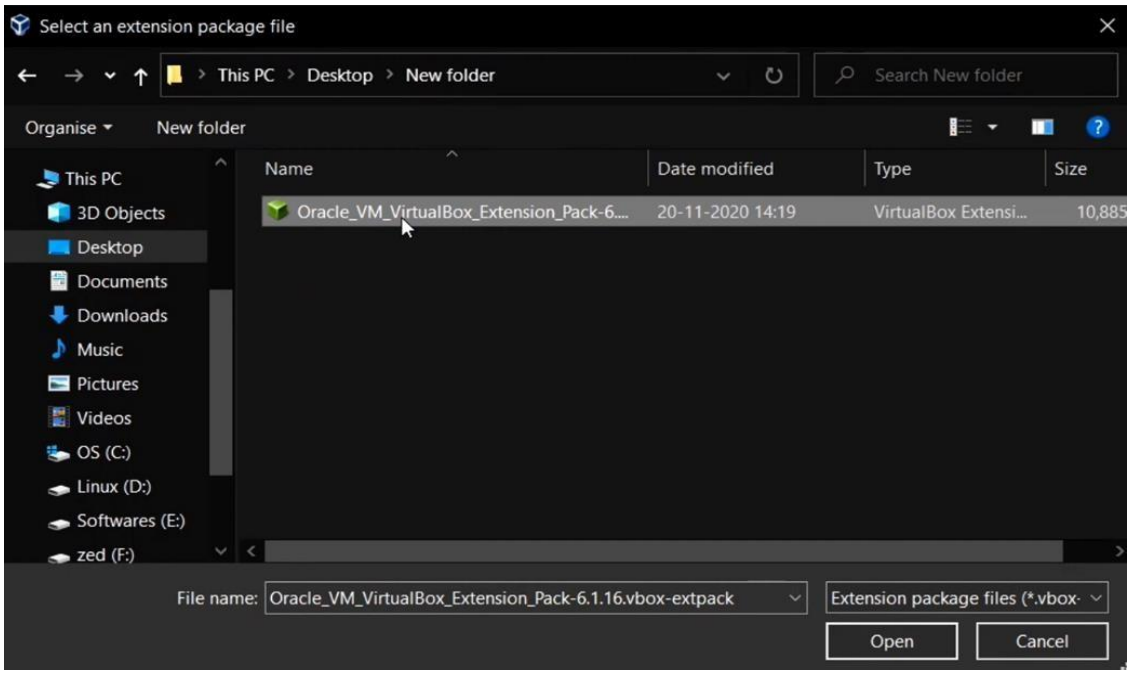
Now, let’s install the extension pack.

Click on **File** and select **Preferences**.

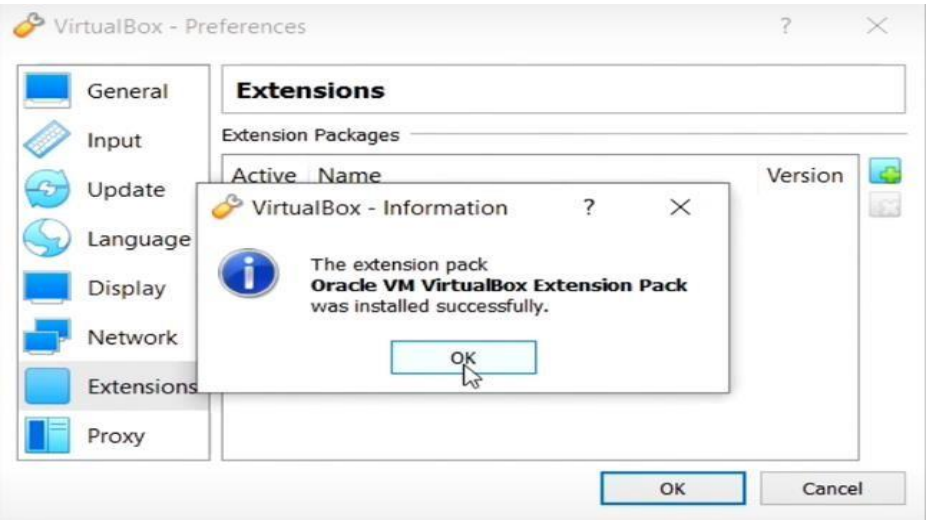
Click on **ADD** to activate the downloaded extension pack.



Select the file and open.

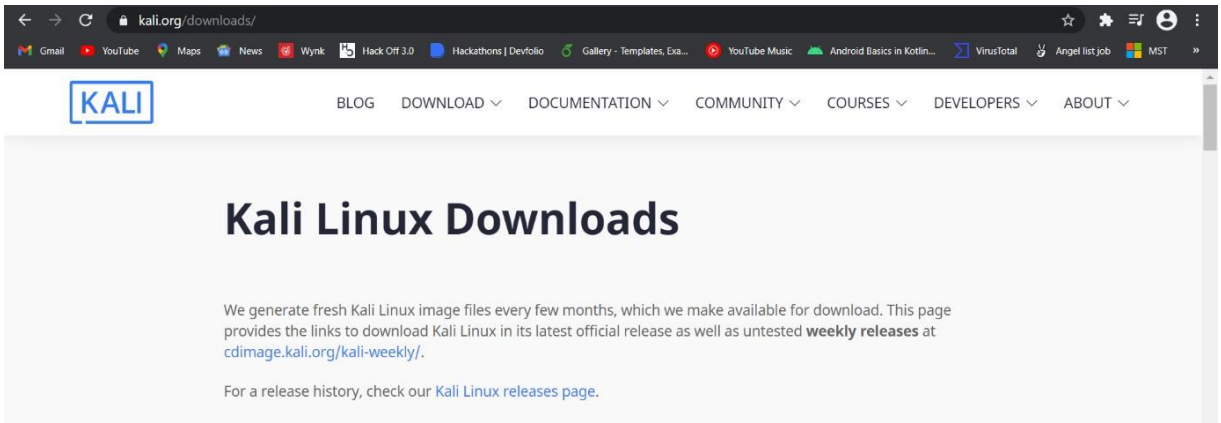


Click on install and activate.

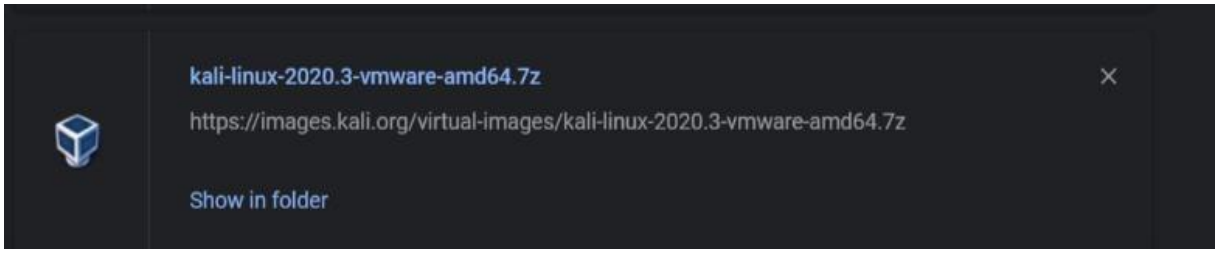


Kali Linux Installation

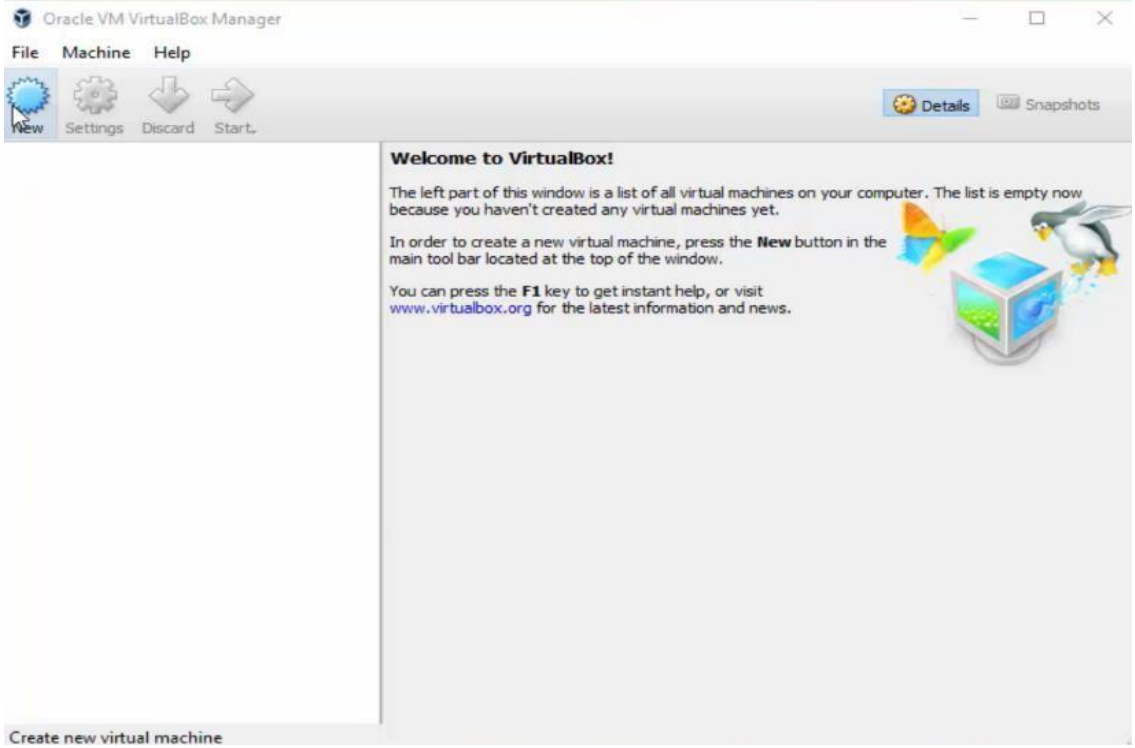
Visit https://www.kali.org/downloads/ and download Kali Linux latest version.



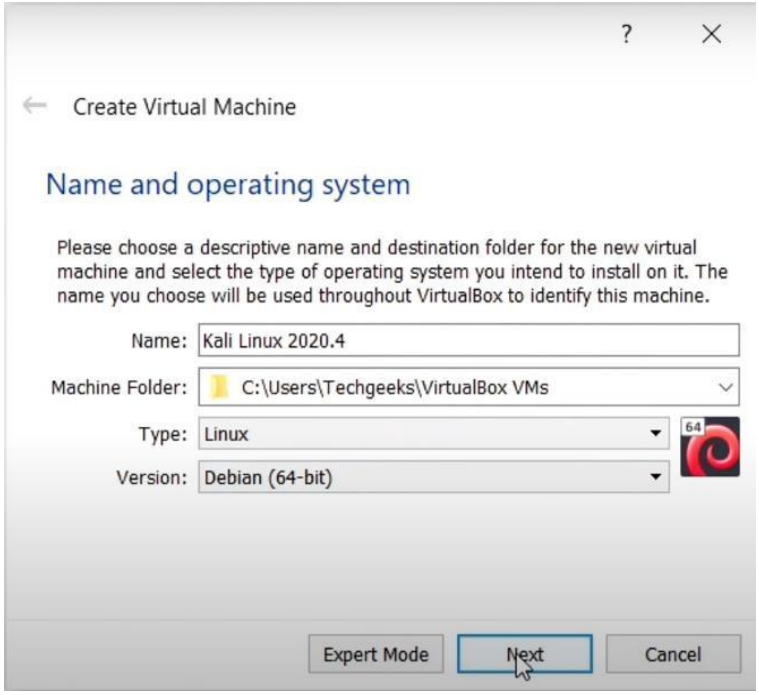
Open in folder.



To install new OS in virtual machine, click on **NEW.**

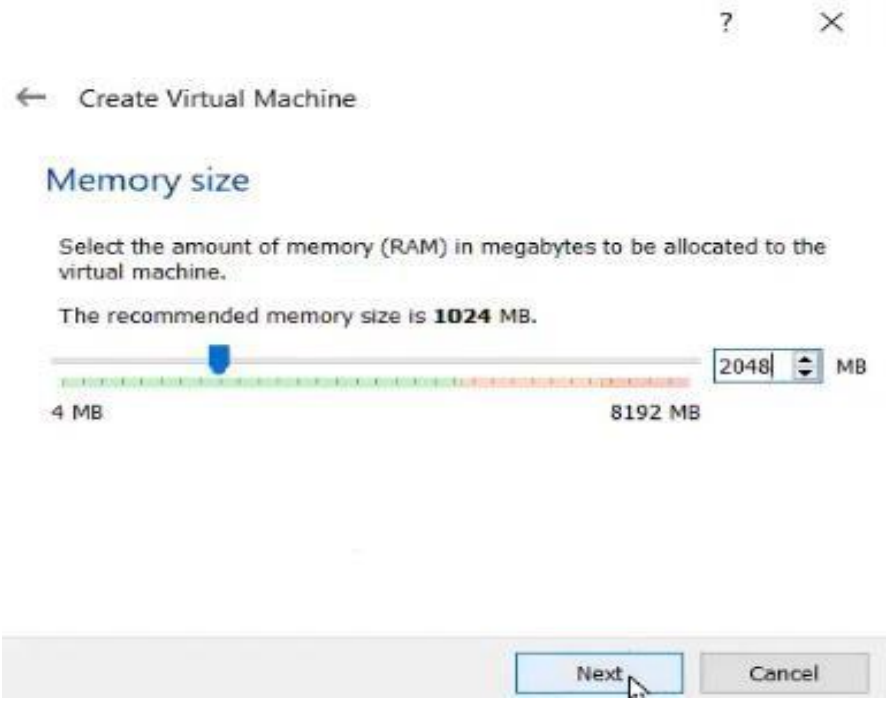


Write **“Kali Linux 2020.4”** in name (or whatever you wish to keep) and change the version to **Debian (64-bit)** and click on next.



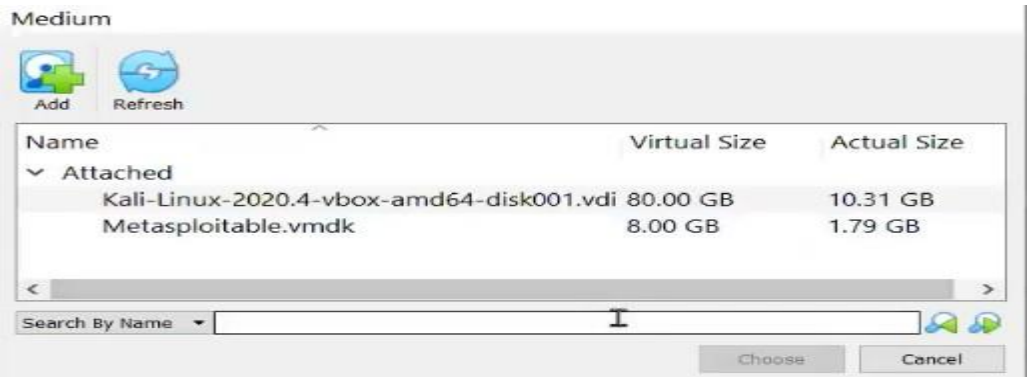
Allocate 2048 Mb (2 GB) memory size at least.

Click on next.

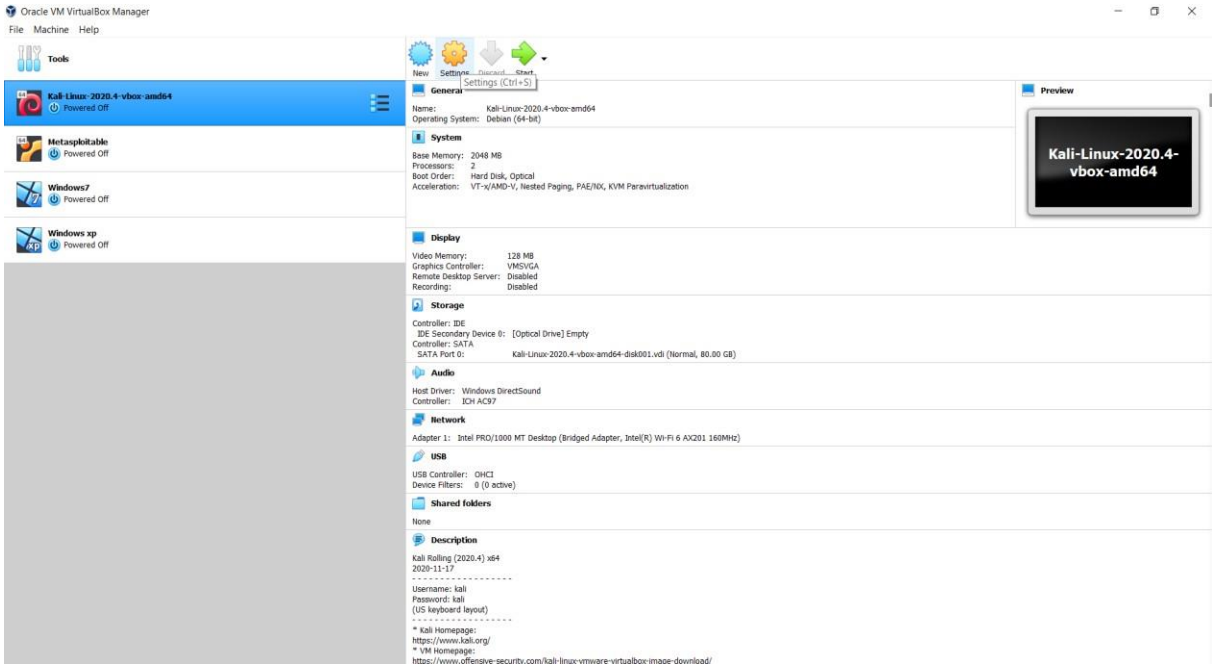


Select **“Use an existing virtual hard disk file”.**

Browse, select the downloaded file and create.

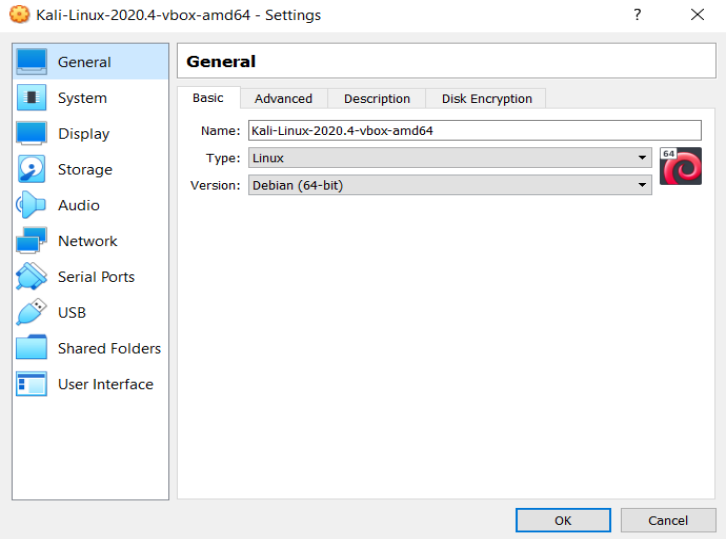


Now, Kali Linux OS is installed in our Virtual box. The window should look like this.

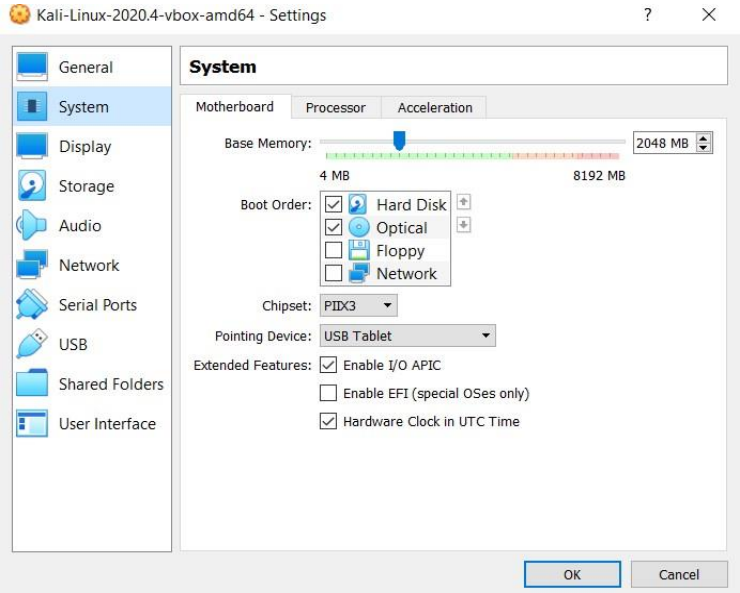


Now we will make some changes in its settings.

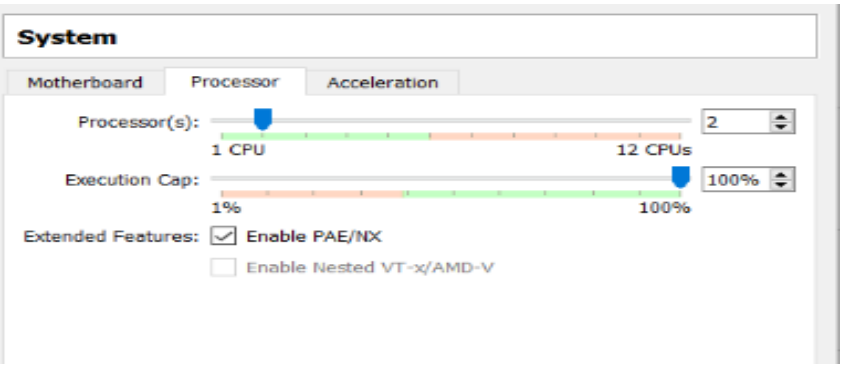
Select Linux and click on **settings.**



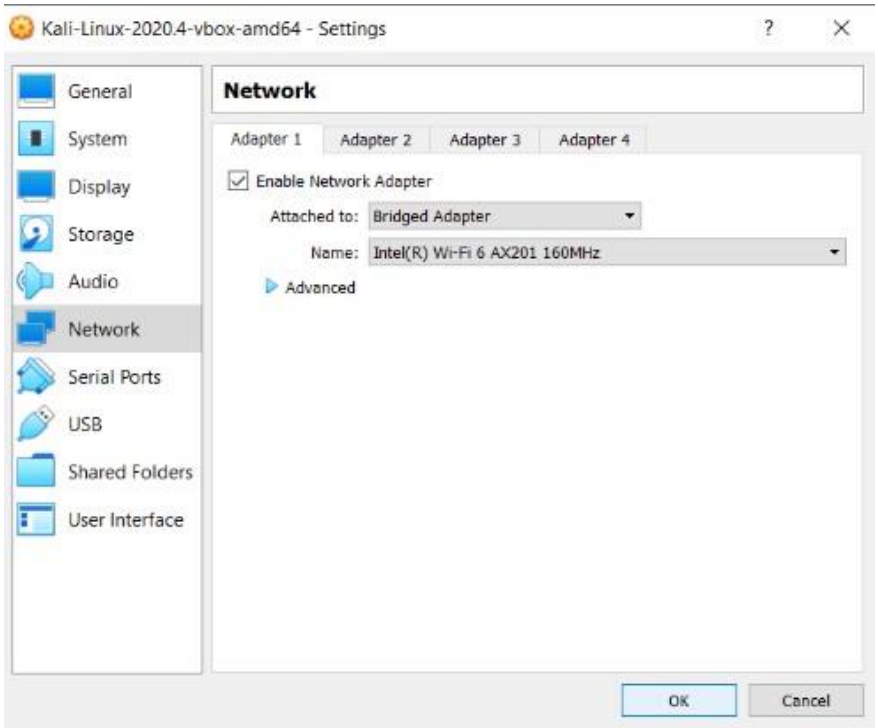
Uncheck **floppy** in **System** option.



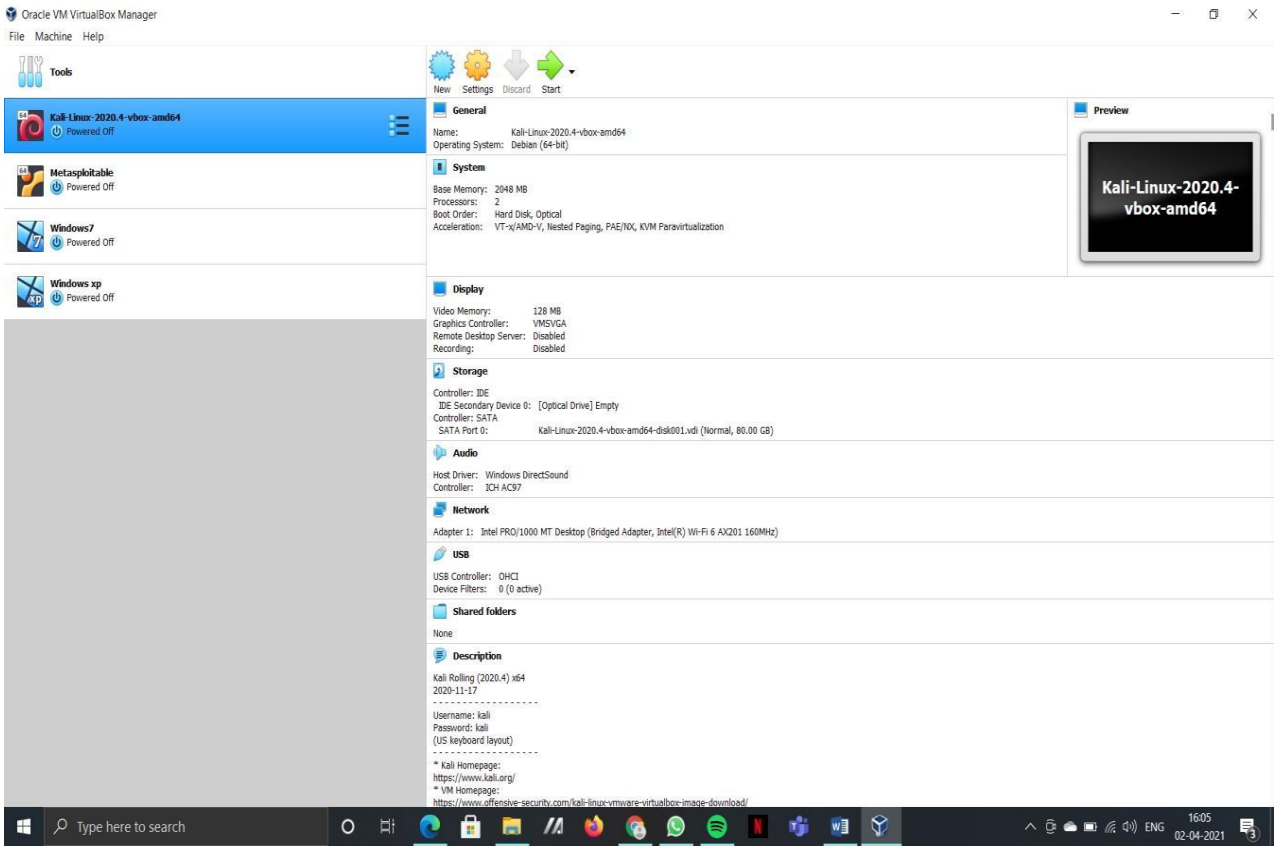
Click on additional option **Processor** and enable **PAE/NX.**



Select **Network** and change the attached to: from **NAT** to **Bridged Adapter** and click on OK.



Overview: The overall window will look like this.



Default Username: kali Username: root (which I'm using)

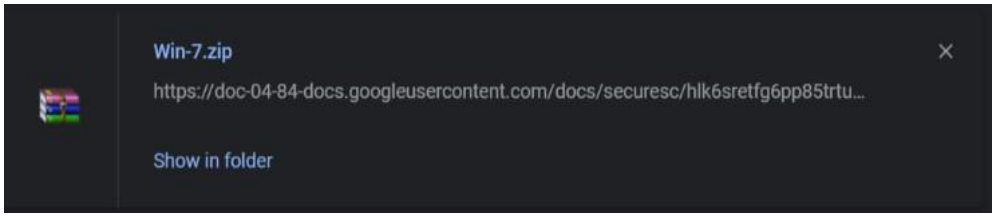
Password: kali Password: osboxes.org

Here, Our Kali Linux Virtual Machine is ready.

Windows 7 Installation

Visit https://o7planning.org/11883/install-windows-7-virtual-machine-in-virtualbox and download Windows 7 latest version Zip file.

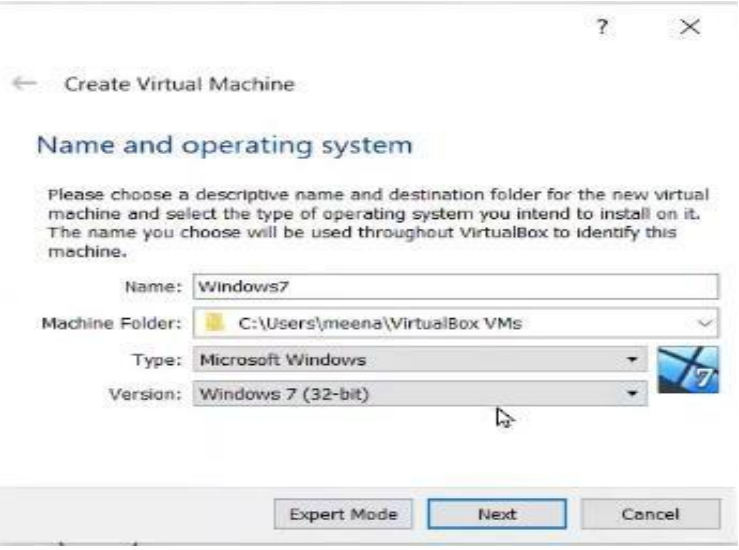
Open in folder.



Extracting files from Zip file.

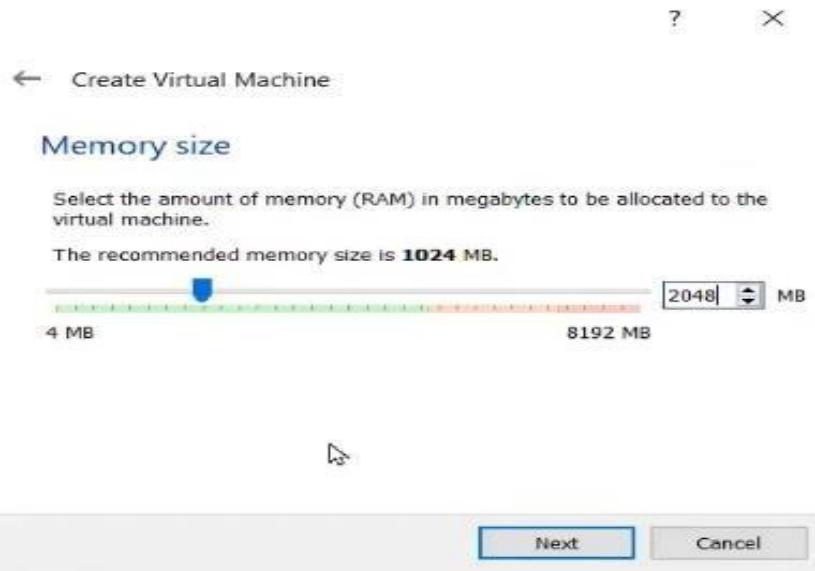
Open Virtual box and click on **NEW** to install Windows 7.

Write **"Windows 7"** in name (or whatever you wish to keep) and change the version from **Windows (64-bit)** to **Windows (32-bit)** and click on next.



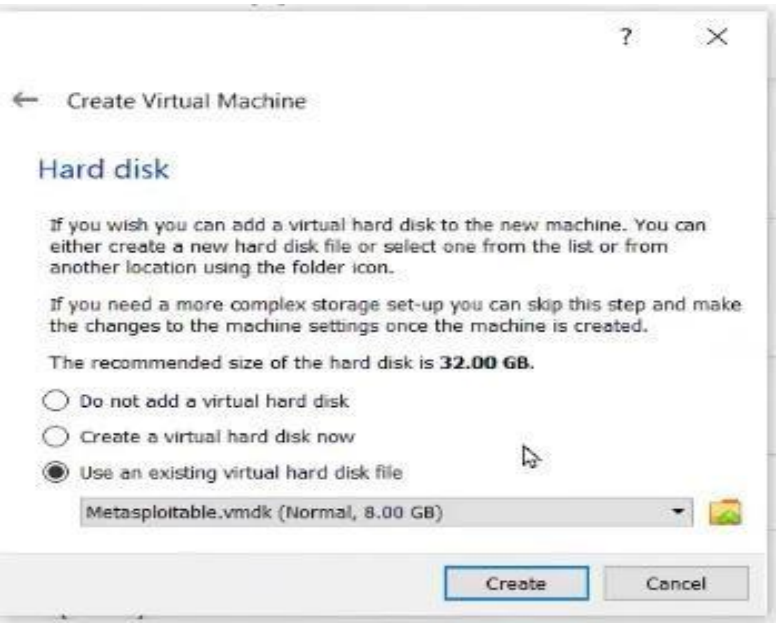
Allocate 2048 Mb (2 GB) memory size at least.

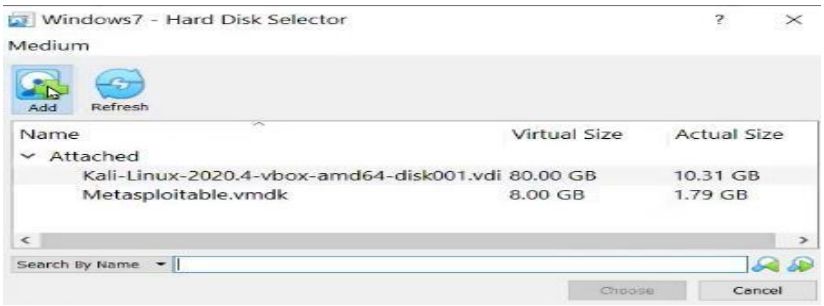
Click on next.



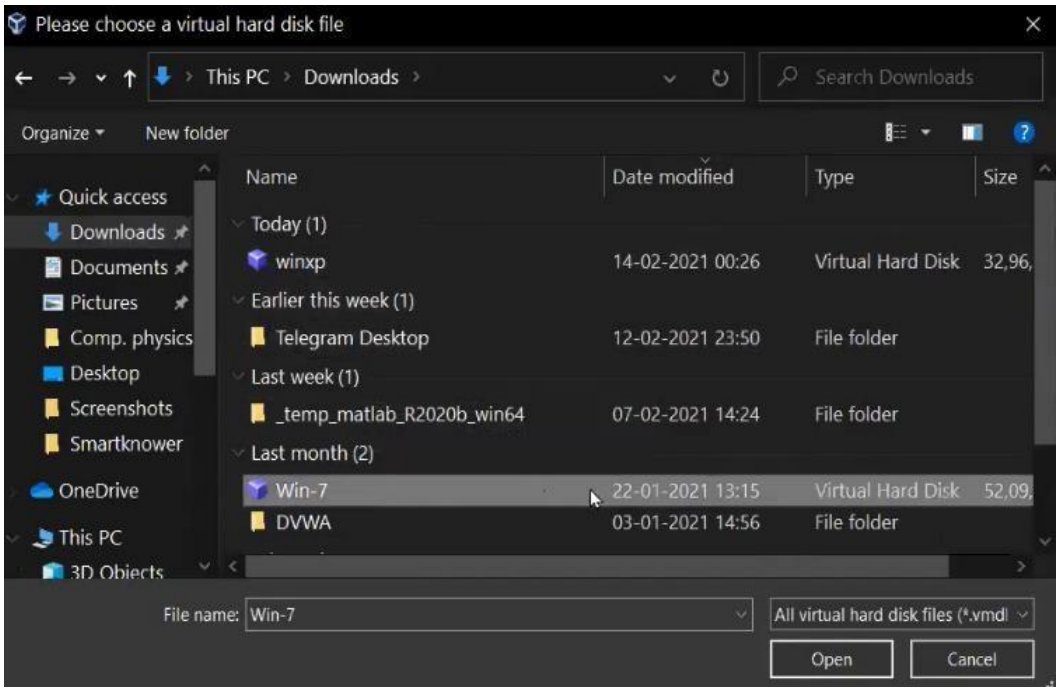
Select **"Use an existing virtual hard disk file".**

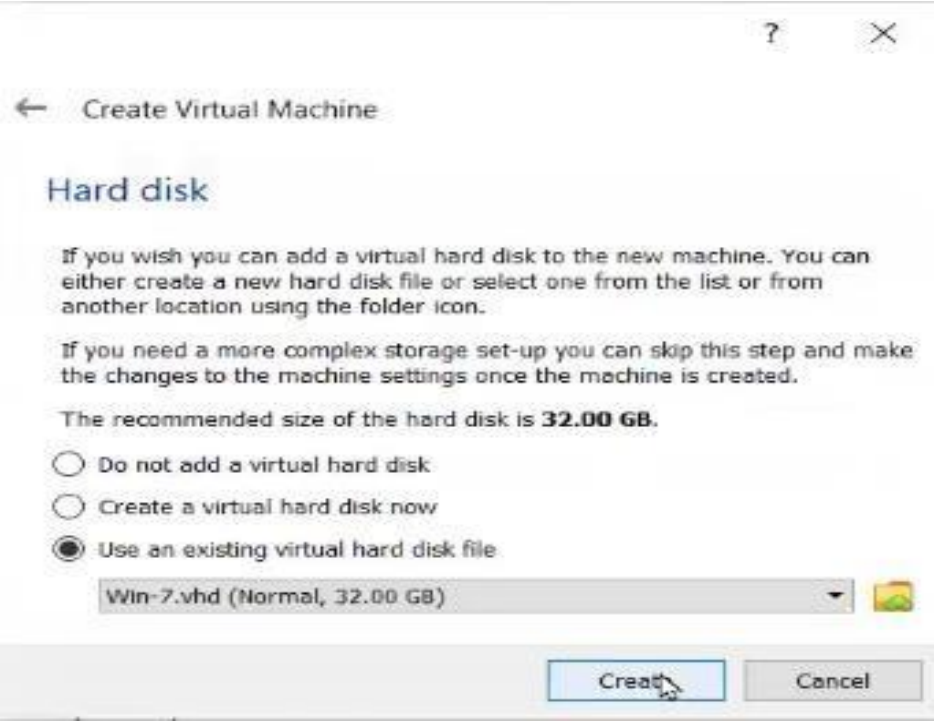
Browse for the Extracted file and ADD.



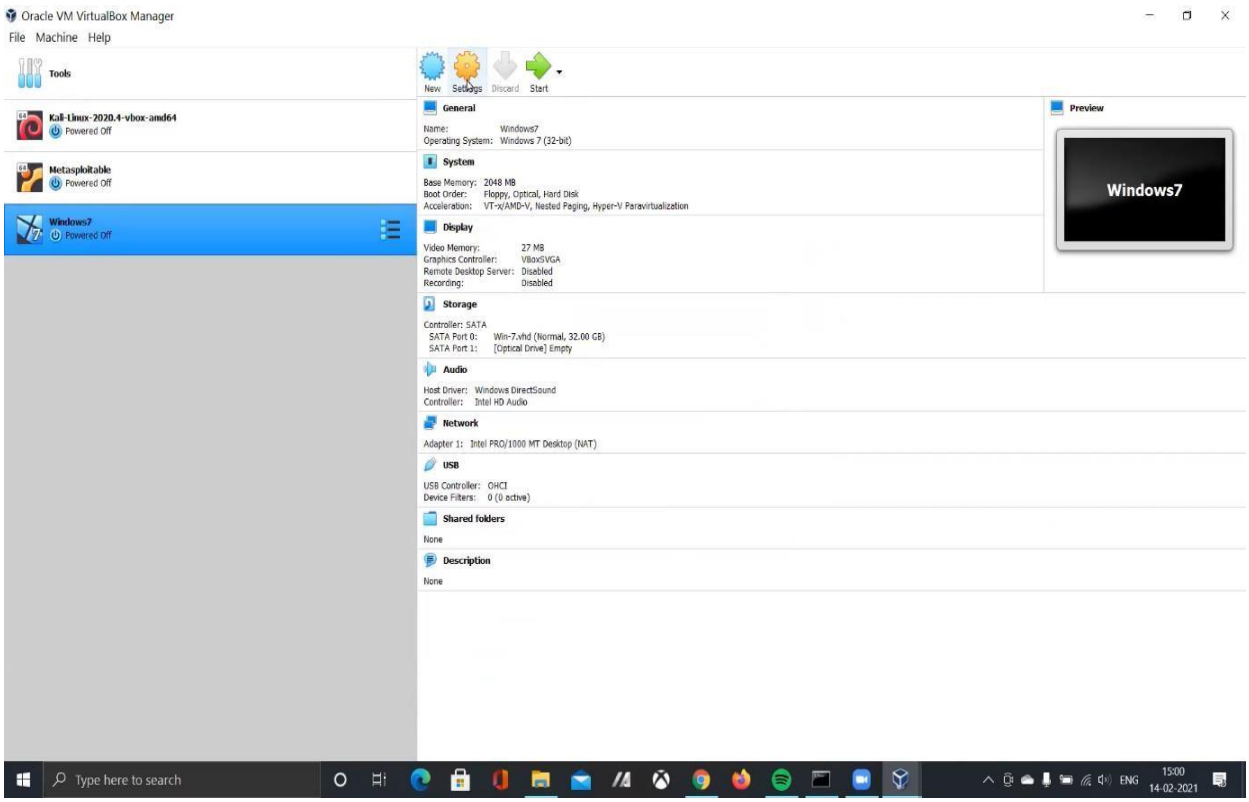


Select **Win 7** and click on create.



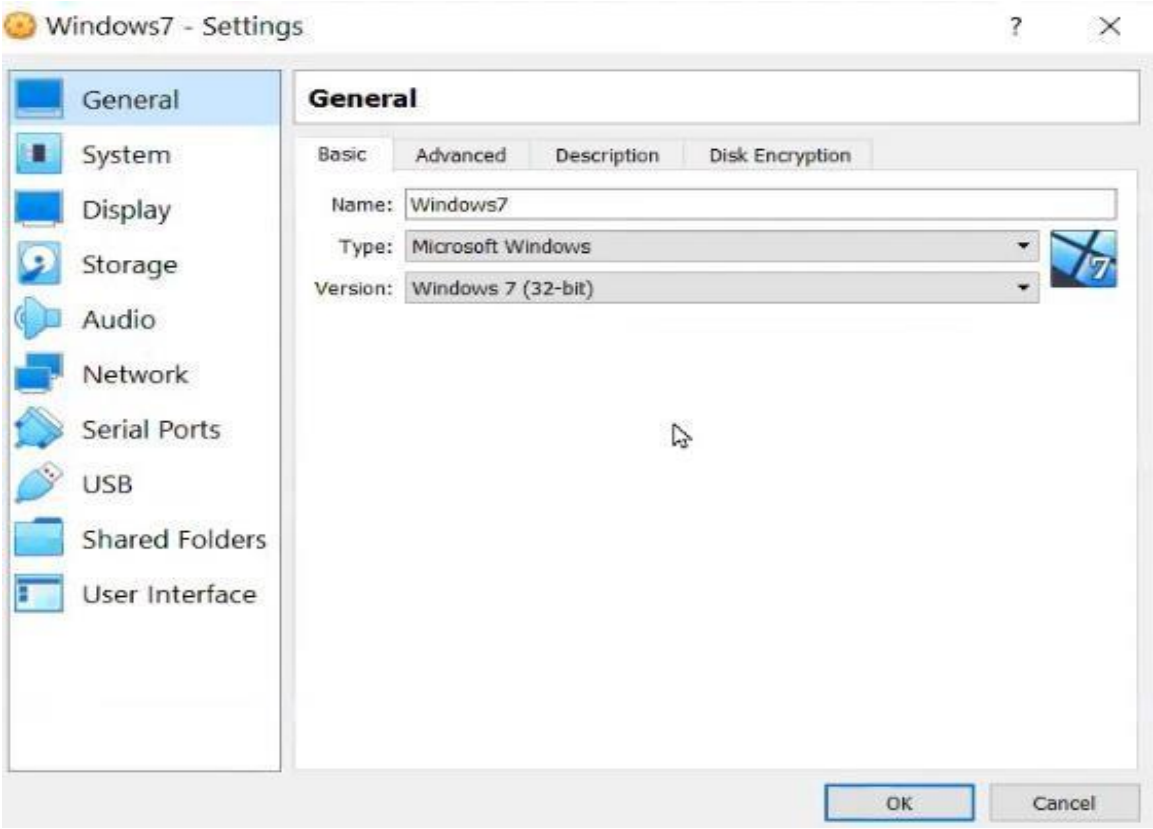


Now, Windows 7 OS is installed in our Virtual box. The window should look like this.

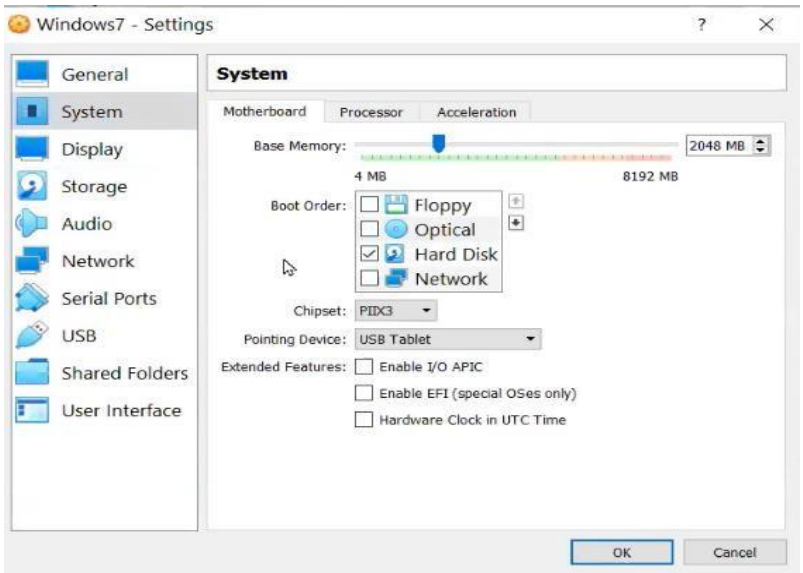


Now we will make some changes in its settings.

Select Windows 7 and click on **settings.**

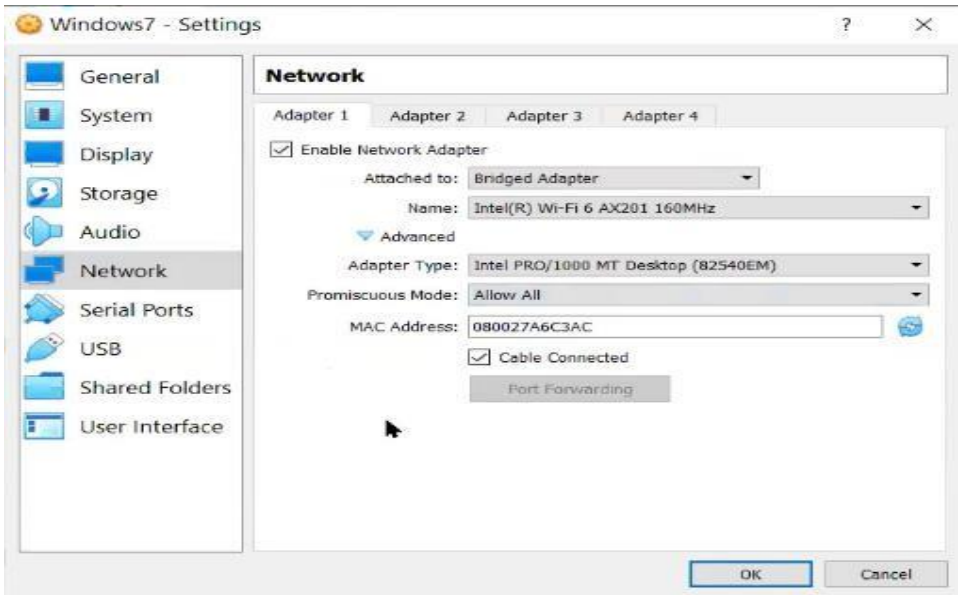


Uncheck **floppy** and **optical** in **System** option.

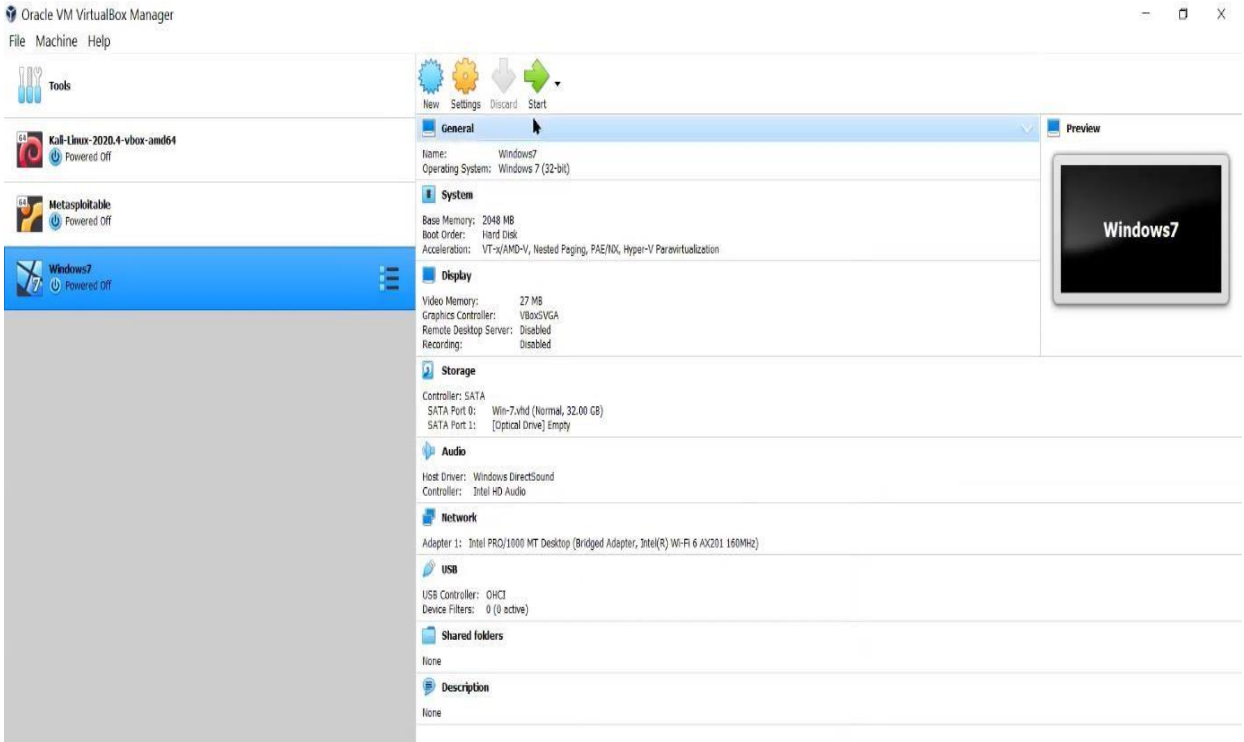


Click on additional option **Processor** and enable **PAE/NX.**

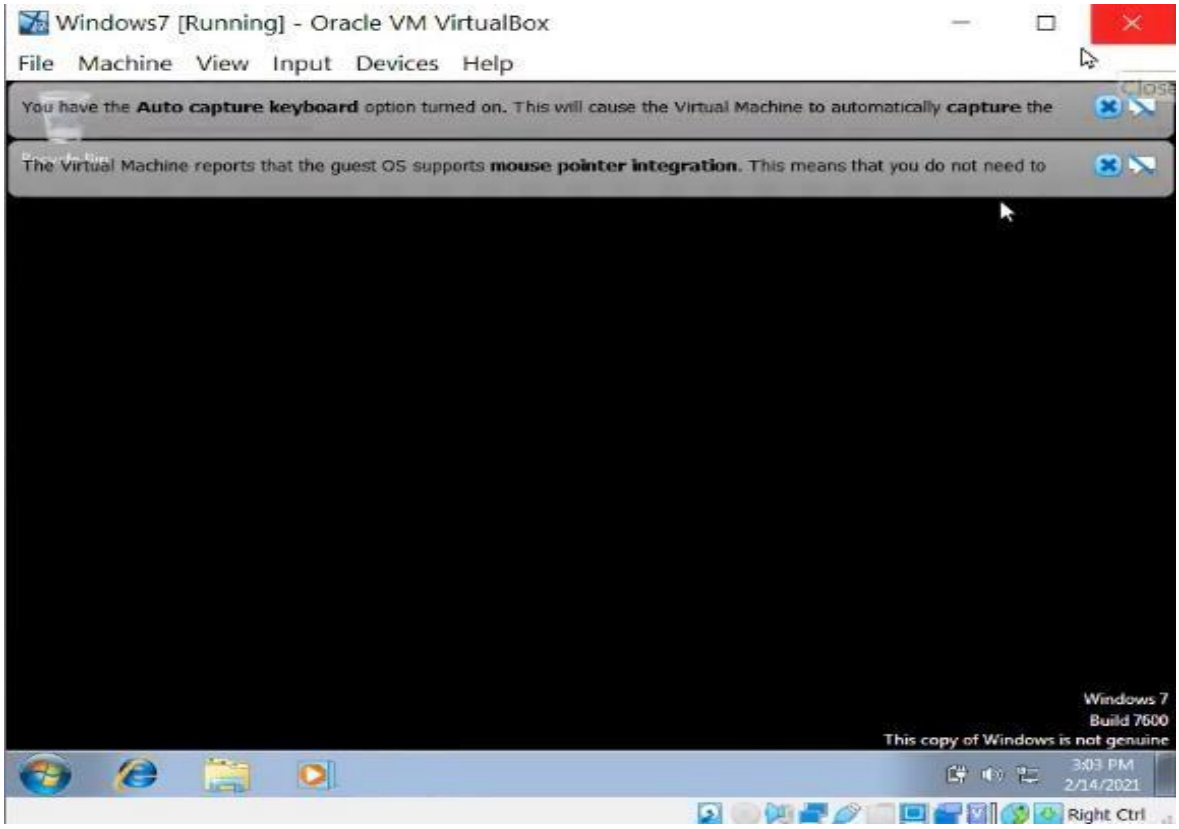
Select **Network** and change the attached to: from **NAT** to **Bridged Adapter** and Promiscuous mode from **deny** to **allow all** and click on OK.



Overview: The overall window will look like this.



It requires no login and password. On starting the machine, it will look like this.

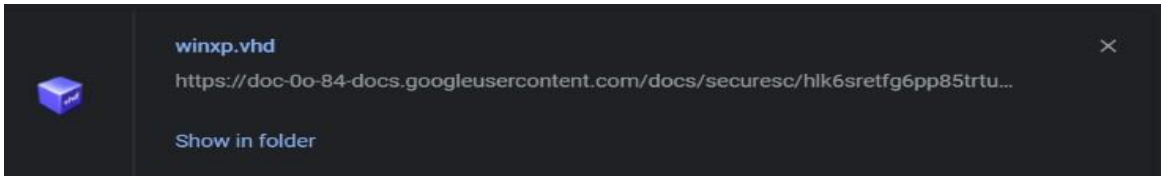


Here, Our Windows 7 Virtual Machine is ready.

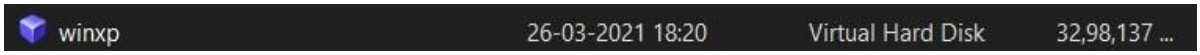
Windows XP Installation

Download Windows XP latest version Zip file.

Open in folder.



Extracting files from Zip file.

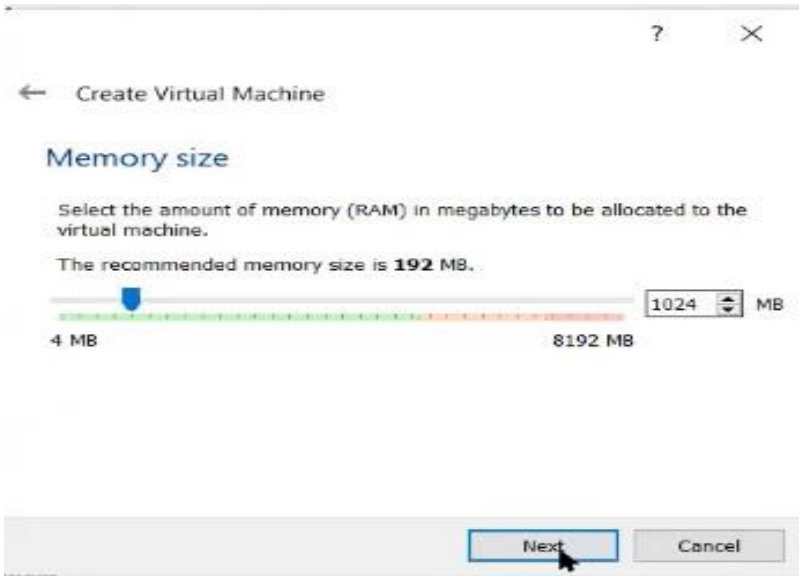


Open Virtual box and click on **NEW** to install Windows XP.

Write **"Windows XP"** in name (or whatever you wish to keep) and change the version from **Windows xp(64-bit)** to **Windows xp(32-bit)** and click on next.

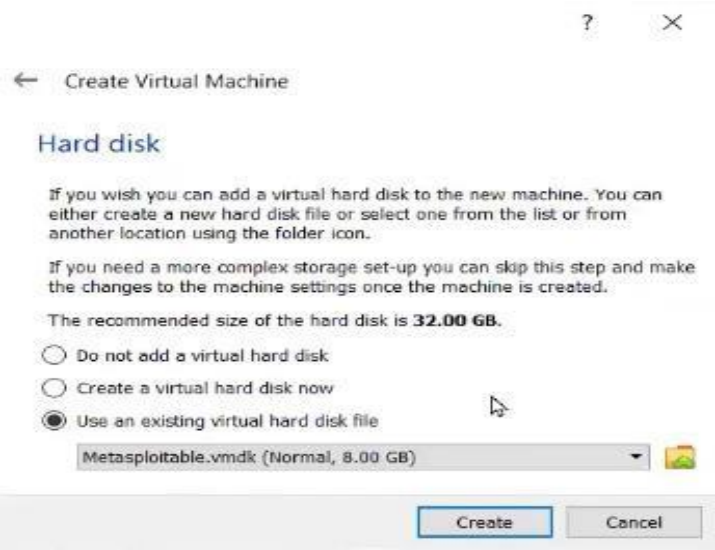
Allocate 1024 Mb (1 GB) memory size at least.

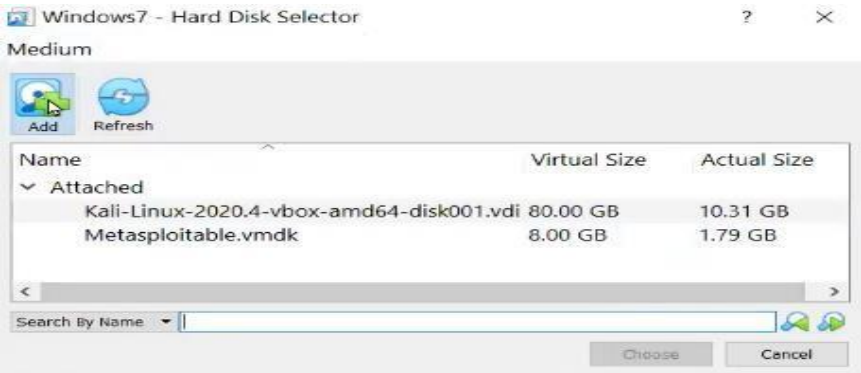
Click on next.



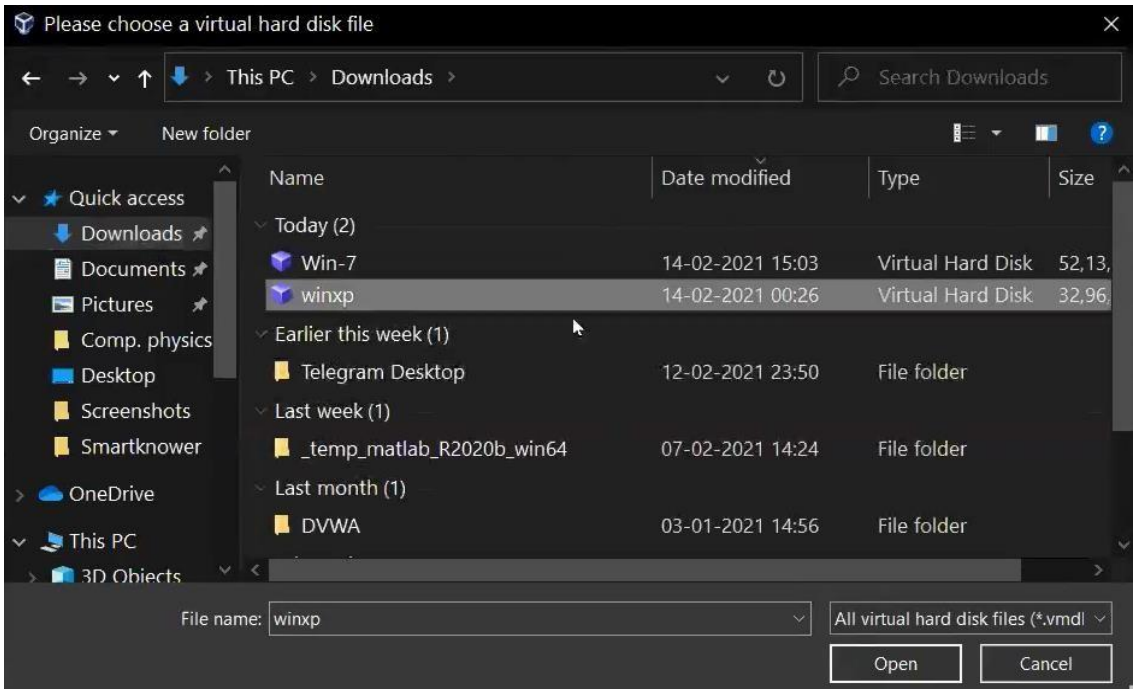
Select **"Use an existing virtual hard disk file".**

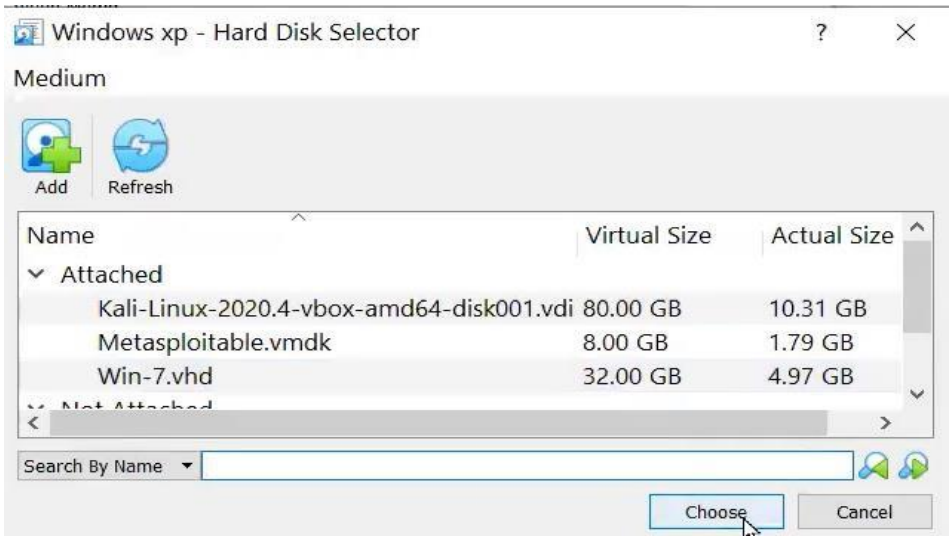
Browse for the Extracted file and ADD.





Select **Winxp** and click on open and create.

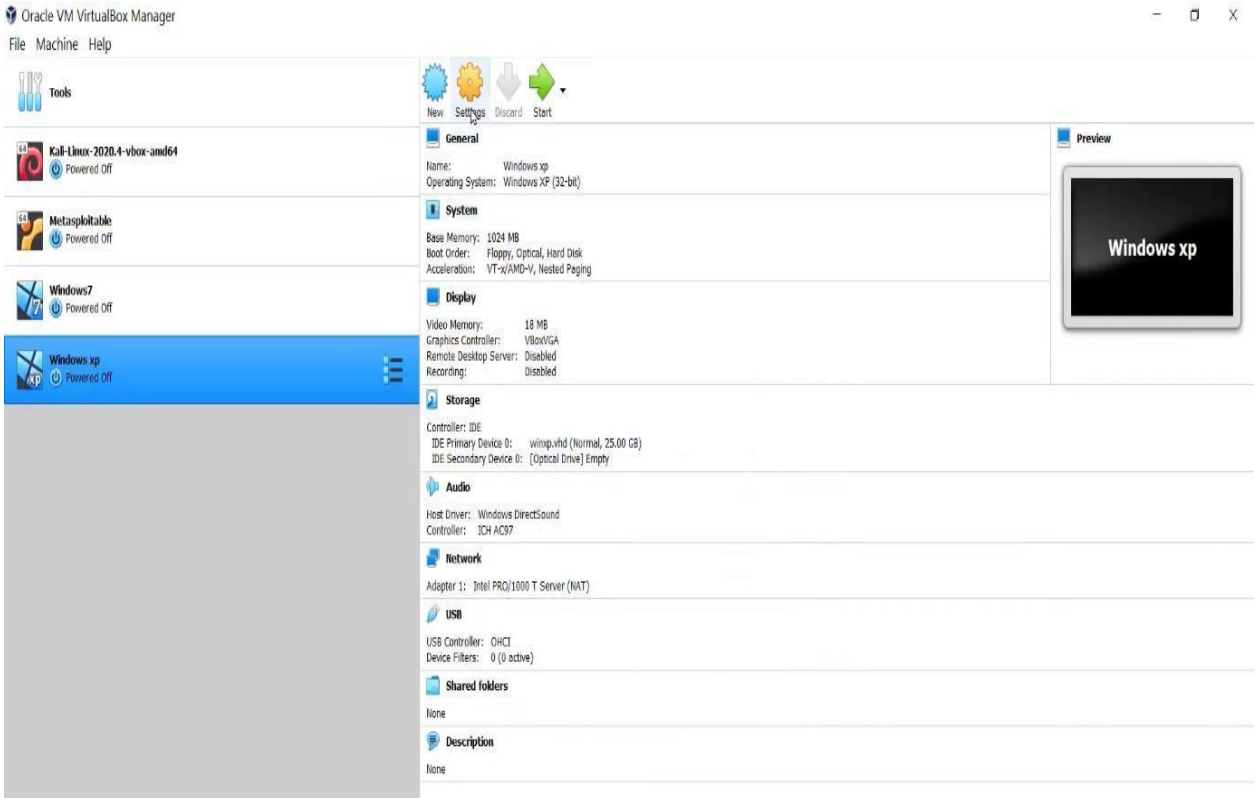




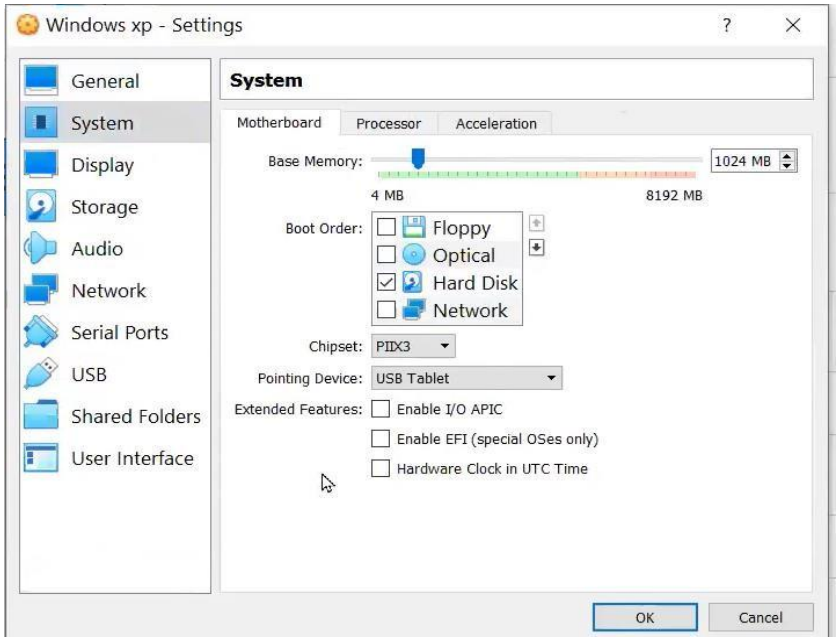
Now, Windows XP OS is installed in our Virtual box. The window should look like this.

Now we will make some changes in its settings.

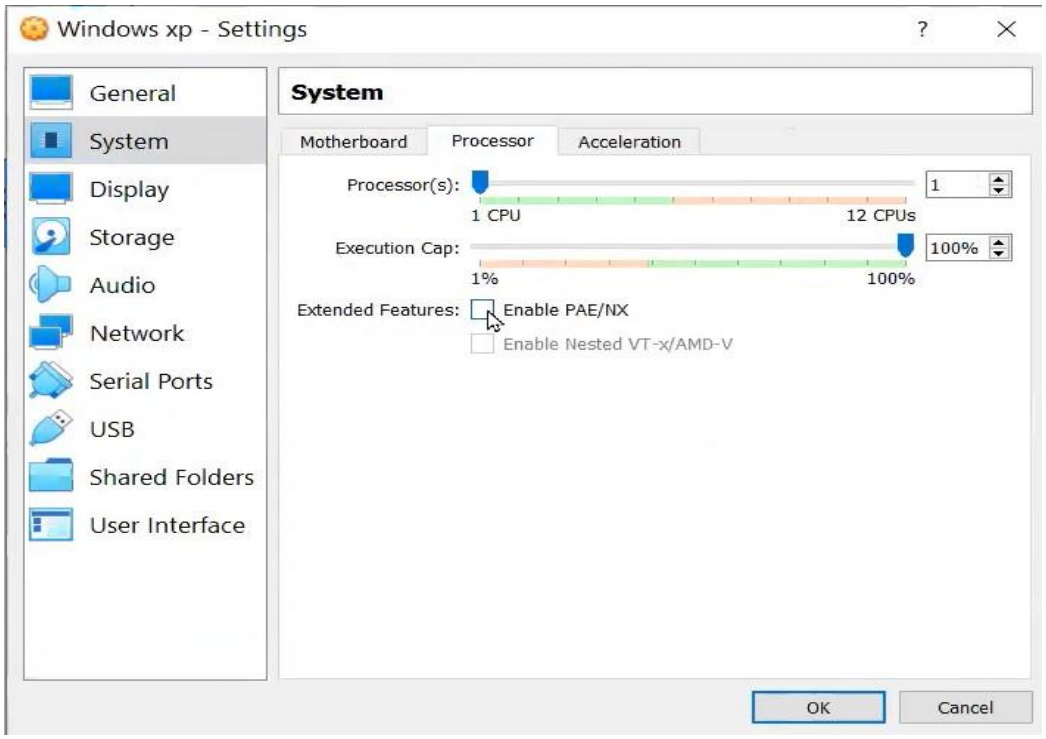
Select Windows 7 and click on **settings.**



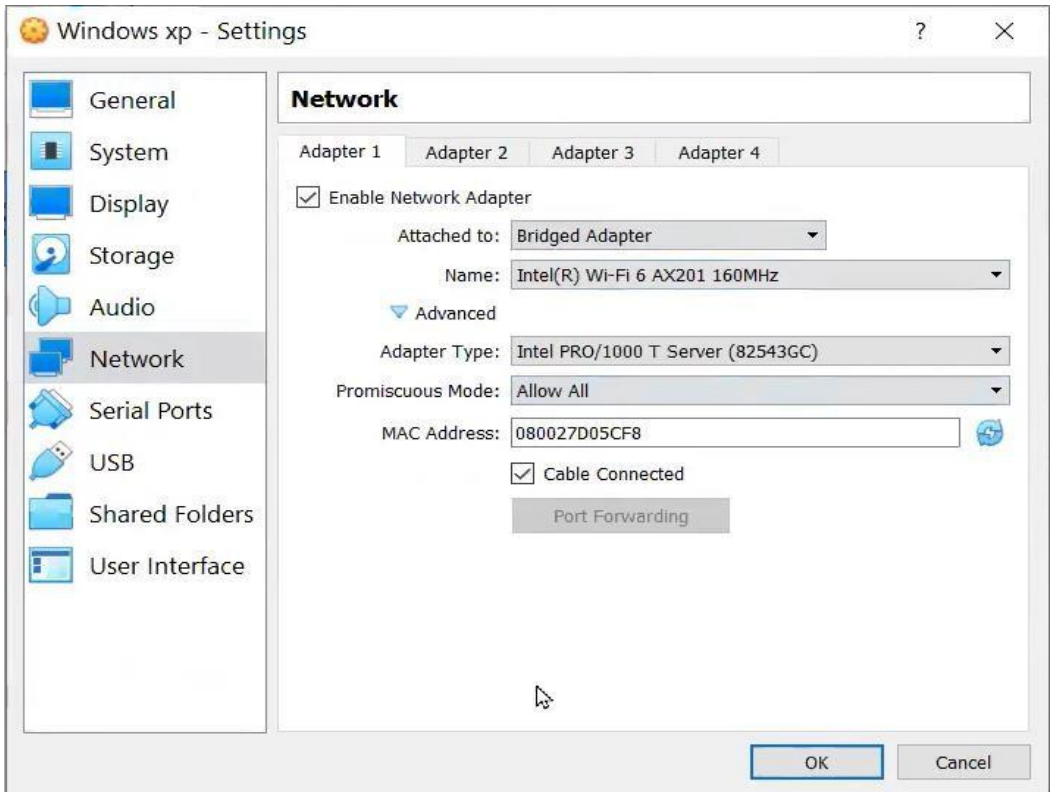
Uncheck **floppy** and **optical** in **System** option.



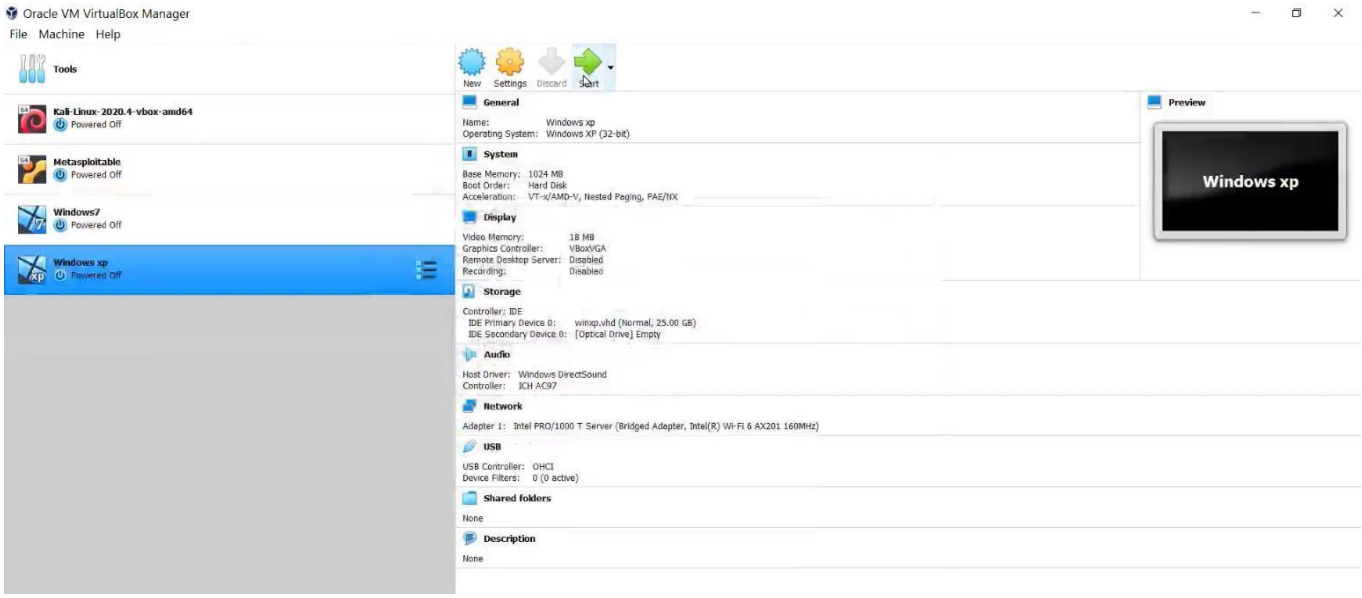
Click on additional option **Processor** and enable **PAE/NX.**



Select **Network** and change the attached to: from **NAT** to **Bridged Adapter** and Promiscuous mode from **deny** to **allow all** and click on OK.



Overview: The overall window will look like this.



Username: victim

Password: 123

Here, Our Windows XP Virtual Machine is ready.

Information Gathering (INSTAGRAM)

Gather information about Instagram (website)

HOST is live or not

```
Command Prompt
Microsoft Windows [Version 10.0.19042.868]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\meena>ping www.instagram.com

Pinging z-p42-instagram.c10r.facebook.com [2a03:2880:f2ff:e0:face:b00c:0:4420] with 32 bytes of data:
Reply from 2a03:2880:f2ff:e0:face:b00c:0:4420: time=36ms
Reply from 2a03:2880:f2ff:e0:face:b00c:0:4420: time=64ms
Reply from 2a03:2880:f2ff:e0:face:b00c:0:4420: time=61ms
Reply from 2a03:2880:f2ff:e0:face:b00c:0:4420: time=53ms

Ping statistics for 2a03:2880:f2ff:e0:face:b00c:0:4420:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 64ms, Average = 53ms
```

HOST IS LIVE

IP address

```
C:\Users\meena>nslookup www.instagram.com
Server:  UnKnown
Address:  192.168.43.253

Non-authoritative answer:
Name:    z-p42-instagram.c10r.facebook.com
Addresses:  2a03:2880:f2ff:e0:face:b00c:0:4420
          69.171.250.174
Aliases:  www.instagram.com
```

IP: 192.168.43.253

Route taken to reach www.instagram.com

```
C:\Users\meena>tracert www.instagram.com

Tracing route to z-p42-instagram.c10r.facebook.com [2a03:2880:f2ff:e0:face:b00c:0:4420]
over a maximum of 30 hops:

  1     2 ms     1 ms     2 ms  2401:4900:3058:76d2::96
  2    28 ms    17 ms    51 ms  2401:4900:3058:76d2:0:4b:3fc2:8c40
  3     *        *        *     Request timed out.
  4    84 ms    28 ms    35 ms  2401:4900:1c:408::102
  5    41 ms    47 ms    29 ms  2401:4900:1c:408::176
  6    81 ms    23 ms    45 ms  2401:4900:1c:408::166
  7    49 ms    28 ms    27 ms  2404:a800:1a00:601::5
  8    68 ms    52 ms    41 ms  2404:a800::207
  9    73 ms    49 ms    57 ms  ae20.pr04.del1.tfbnw.net [2620:0:1cff:dead:beee::bac]
 10    54 ms    61 ms    56 ms  po104.psw03.del1.tfbnw.net [2620:0:1cff:dead:bef0::469]
 11    72 ms    74 ms    75 ms  po3.msw1ad.02.del1.tfbnw.net [2a03:2880:f044:ffff::26f]
 12    70 ms    58 ms    57 ms  instagram-p426-shv-01-any2.fbcdn.net [2a03:2880:f2ff:e0:face:b00c:0:4420]

Trace complete.
```

Crossed 12 servers to reach www.instagram.com

Login link: https://www.instagram.com/accounts/login/?hl=en

Office locations:

- Gurgaon, India
- Menlo Park, CA
- Mumbai, India
- New York, NY
- Prineville, OR
- Remote, Contiguous US
- San Francisco, CA
- Singapore
- Tokyo, Japan

Teams:

- AR/VR
- Business Development & Partnerships
- Communications & Public Policy
- Data & Analytics
- Design & User Experience
- Facebook
- Infrastructure
- Legal, Finance, Facilities & Admin
- Research
- Sales & Marketing
- Security
- Technical Program Management

Funding via Crunchbase

Series B

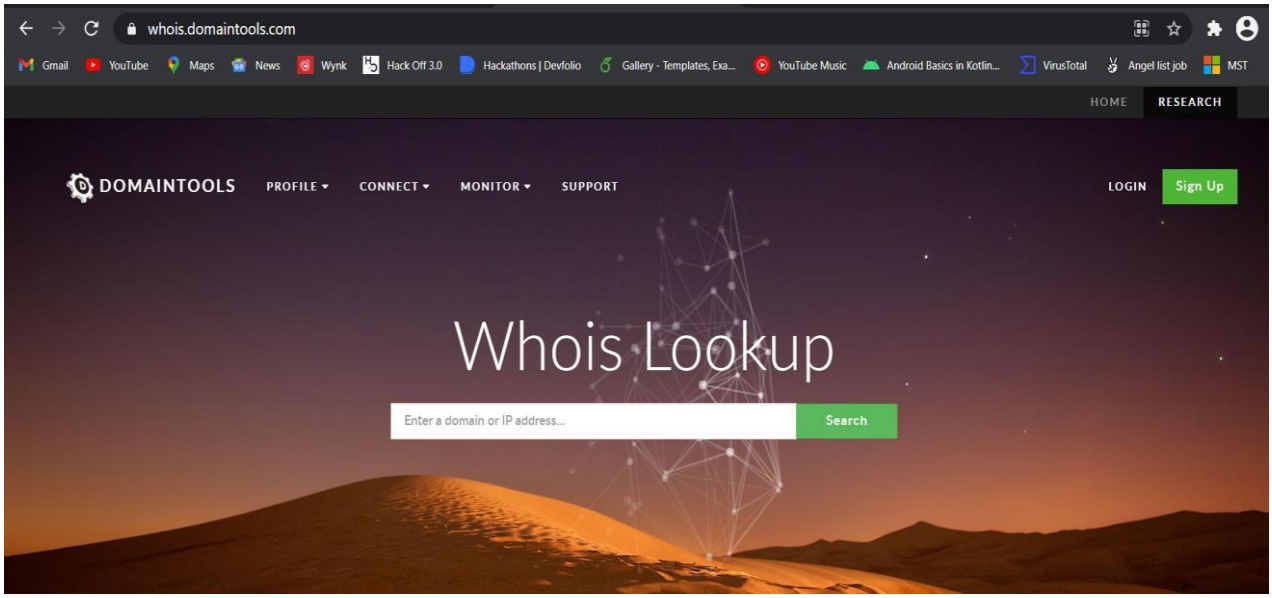
US$ 50M

Company Size: 10,001+ employees

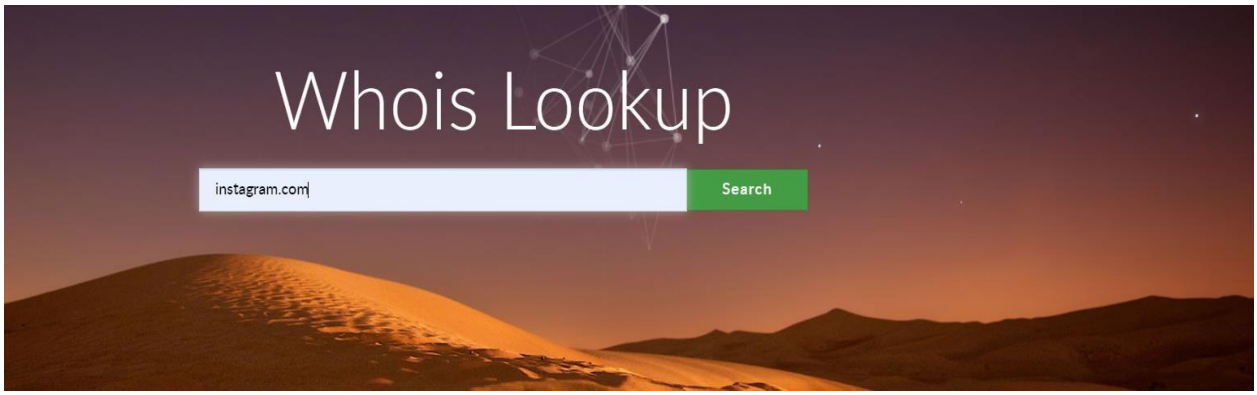
18,026 on LinkedIn Includes members with current employer listed as Instagram, including part-time roles.

Basic Details: instagram.com

Visit Site- https://whois.domaintools.com/ and you will find the following site.



Type www.instagram.com in the input area and click on search.



Below information gives us the results on Nameservers, Tech-contact Info, IP address, Location, IP History and Registrar History etc.

Whois Record for InstaGram.com

Registrant	REDACTED FOR PRIVACY (DT)
Registrant Org	Instagram LLC
Registrant Country	us
Registrar	RegistrarSafe, LLC IANA ID: 3237 URL: https://www.registrarsafe.com,http://www.registrarsafe.com

	Whois Server: whois.registrarsafe.com abusecomplaints@registrarsafe.com (p) 16503087004
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	6,133 days old Created on 2004-06-04 Expires on 2027-06-04 Updated on 2018-03-01
Name Servers	NS-1349.AWSDNS-40.ORG (has 36,537 domains) NS-2016.AWSDNS-60.CO.UK (has 436 domains) NS-384.AWSDNS-48.COM (has 6,446 domains) NS-868.AWSDNS-44.NET (has 244 domains)
Tech Contact	REDACTED FOR PRIVACY (DT) Instagram LLC 1601 Willow Rd, Menlo Park, CA, 94025, us (p)
IP Address	157.240.3.174 - 11 other sites hosted on this server
IP Location	- Washington - Seattle - Facebook Inc.
ASN	AS32934 FACEBOOK, US (registered Aug 24, 2004)
Domain Status	Registered And Active Website
IP History	392 changes on 392 unique IP addresses over 17 years
Registrar History	7 registrars with 1 drop
Hosting History	11 changes on 9 unique name servers over 17 years

Website

Website Title	None given.
Response Code	349

Whois Record (last updated on 2021-03-20)

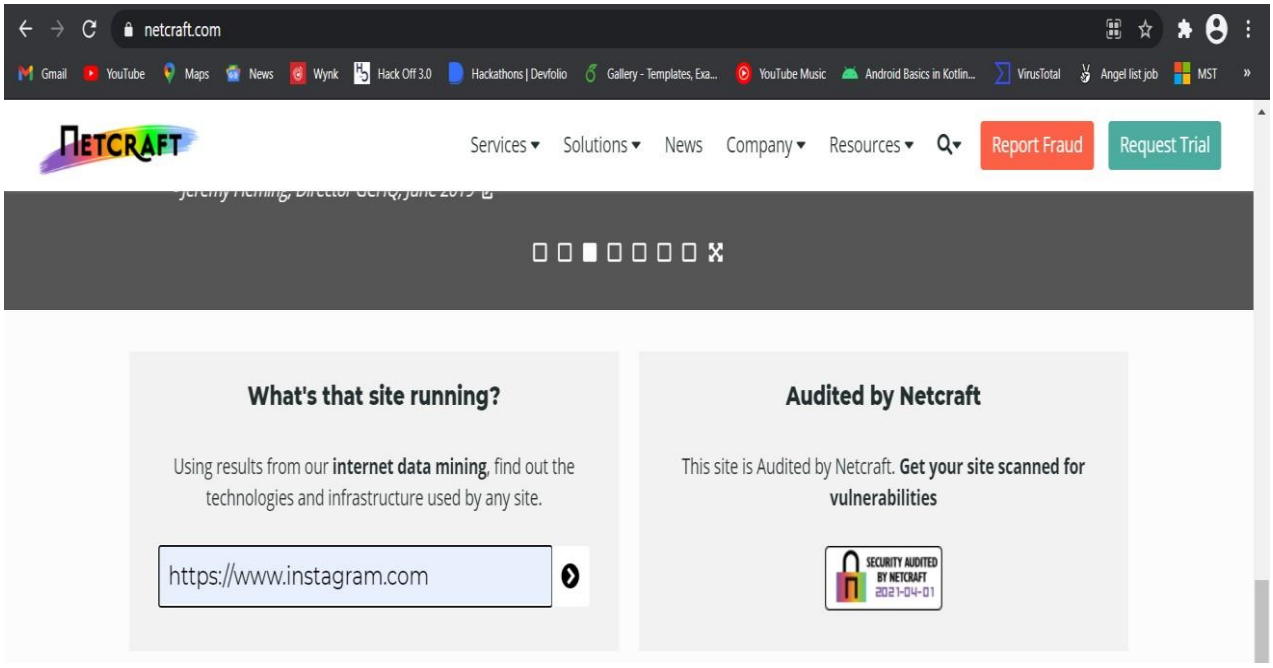
```
Domain Name: instagram.com
Registry Domain ID: 121748357_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
        http://www.registrarsafe.com
Updated Date: 2018-03-01T19:43:29+00:00
        2018-03-01
Creation Date: 2004-06-04T13:37:18+00:00
        2004-06-04
Registrar Registration Expiration Date: 2027-06-04T13:37:18+00:00
        2027-06-04
```

```
Registrar: RegistrarSafe, LLC
Sponsoring Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: 16503087004
Status:
        clientDeleteProhibited
        clientTransferProhibited
        clientUpdateProhibited
        serverDeleteProhibited
        serverTransferProhibited
        serverUpdateProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY (DT)
Registrant Organization: Instagram LLC
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: us
Registrant Phone: 16505434800
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: REDACTED FOR PRIVACY (DT)
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY (DT)
Admin Organization: Instagram LLC
Admin Street: 1601 Willow Rd
Admin City: Menlo Park
Admin State/Province: CA
Admin Postal Code: 94025
Admin Country: us
Admin Phone: REDACTED FOR PRIVACY (DT)
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: REDACTED FOR PRIVACY (DT)
Registry Tech ID:
Tech Name: REDACTED FOR PRIVACY (DT)
Tech Organization: Instagram LLC
Tech Street: 1601 Willow Rd
Tech City: Menlo Park
Tech State/Province: CA
Tech Postal Code: 94025
Tech Country: us
Tech Phone: REDACTED FOR PRIVACY (DT)
Tech Phone Ext:
Tech Fax:
```

```
Tech Fax Ext:
Tech Email: REDACTED FOR PRIVACY (DT)
Nameservers:
        ns-1349.awsdns-40.org
        ns-2016.awsdns-60.co.uk
        ns-384.awsdns-48.com
        ns-868.awsdns-44.net
DNSSEC: unsigned
```

Netcraft Results

Visit site - https://www.netcraft.com/ and search for the www.instagram.com



Results for target domain i.e. instagram.com

Below records gives us the info related to Network and results are on Company's history, IP history, DNS Admin, SSL/TLS, and Technology used etc.

Netcraft Records

Netblock Owner	**Facebook, Inc.**
Hosting company	Facebook

IPv6 address	2a03:2880:f258:e0:face:b00c:0:4420
IPv6 autonomous systems	AS32934
Reverse DNS	instagram-p42-shv-01-lhr8.fbcdn.net

SSL/TLS

SSL Certificate Information related to certificate name, issuer, validity, signature algorithm etc.

Validity period	From Mar 3 2021 to Jun 1 2021 (2 months, 4 weeks, 1 day)
Public key algorithm	rsaEncryption
Protocol version	TLSv1.3
Public key length	2048
Certificate check	ok
Signature algorithm	sha256WithRSAEncryption
Serial number	0x03534ca132574c1bdf79542948a8694b
Cipher	TLS_CHACHA20_POLY1305_SHA256
Version number	0x02

Hosting history

Hosting history along with IP address and OS, Webservers and last seen dates

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.221.174	Linux	unknown	1-Oct-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.1.174	Linux	unknown	15-Sep-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.221.174	Linux	unknown	8-Sep-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.1.174	Linux	unknown	24-Aug-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.221.174	Linux	unknown	16-Aug-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.1.174	Linux	unknown	27-Jul-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.221.174	Linux	unknown	20-Jul-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.1.174	Linux	unknown	6-Jun-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.221.174	Linux	unknown	3-Jun-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.1.174	Linux	unknown	20-May-2020

Site Technology (Server side and Client side)

Site Technology (fetched 20 days ago)

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Asynchronous Javascript	*No description*	www.primevideo.com, www.deepl.com, www.bloomberg.com
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	

TOTAL RESULTS

1,361

TOP COUNTRIES

United States	394
United Kingdom	157
Germany	126
Ireland	119
Singapore	84

TOP SERVICES

HTTPS	845
HTTP	374
HTTP (8080)	18
8081	14
587	10

TOP ORGANIZATIONS

Amazon Technologies Inc.	94
Amazon.com	84
DigitalOcean, LLC	84
Amazon Data Services UK	55
Amazon.com, Inc.	52

TOP PRODUCTS

nginx	393
Apache httpd	375
Microsoft IIS httpd	33
LiteSpeed httpd	23
Exim smtpd	14

Determining the OS, port & services using https://www.shodan.io/

104.26.7.72

City	**San Francisco**
Country	**United States**
Organization	**Cloudflare, Inc.**
ISP	**Cloudflare, Inc.**
Last Update	**2021-03-20T13:07:39.486989**
ASN	**AS13335**

Web Technologies

- Google Tag Manager
- jQuery
- MySQL
- PHP
- React
- reCAPTCHA
- WordPress

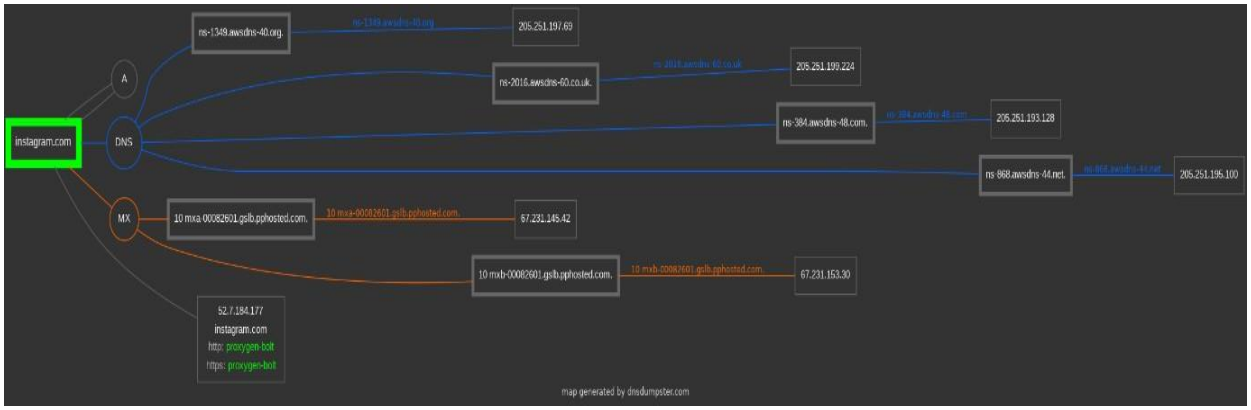
Ports

- 80
- 443
- 2082
- 2086
- 2087
- 8080
- 8443
- 8880

Certificate

http://cacerts.digicert.com/CloudflareIncECCCA-3.crt

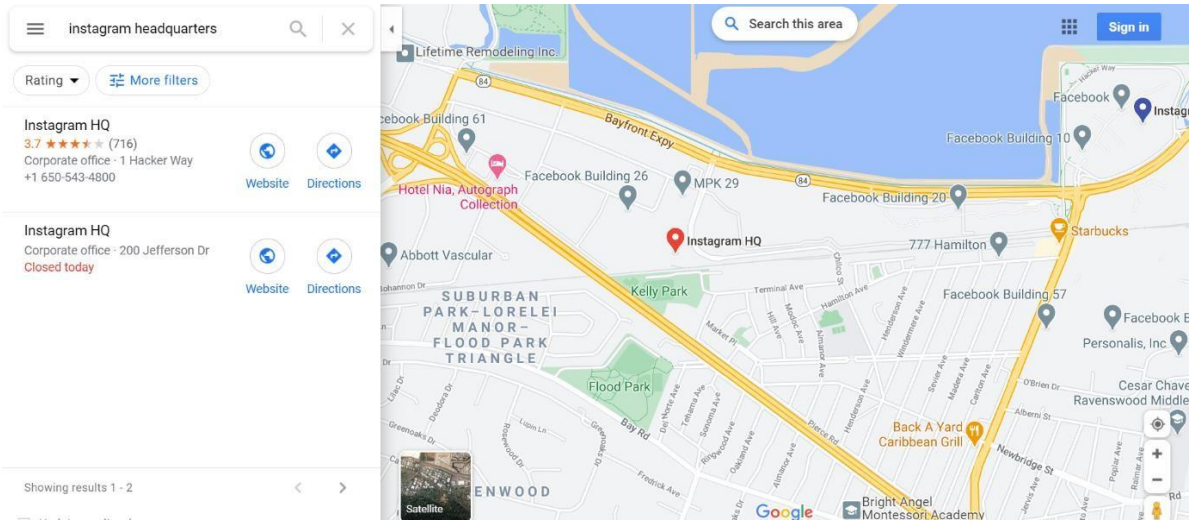
Mapping the domain



Extra Records (xlsx sheet)

	A	B	C	D	E	F	G	H	I
1	Hostname	IP Address	T	Reverse DNS	Netblock Owner	Country	Tech / Apps	HTTP / Title	HTTPS / Title
2	instagram.com	52.7.184.177	A	ec2-52-7-184-177.compute-1.amazonaws.com	AMAZON-AES	United States		proxygen-bolt	proxygen-bolt CN: .instagram.com O: Facebook Inc.
3	ns-1349.awsdns-40.org.	205.251.197.69	NS	ns-1349.awsdns-40.org	AMAZON-02	United States			
4	ns-2016.awsdns-60.co.uk.	205.251.199.224	NS	ns-2016.awsdns-60.co.uk	AMAZON-02	United States			
5	ns-384.awsdns-48.com.	205.251.193.128	NS	ns-384.awsdns-48.com	AMAZON-02	United States			
6	ns-868.awsdns-44.net.	205.251.195.100	NS	ns-868.awsdns-44.net	AMAZON-02	United States			
7	10 mxa-00082601.gslb.pphosted.com.	67.231.153.30	MX	mx0b-00082601.pphosted.com	PROOFPOINT-ASN-US-EAST	United States			
8	10 mxb-00082601.gslb.pphosted.com.	67.231.145.42	MX	mx0a-00082601.pphosted.com	PROOFPOINT-ASN-US-WEST	United States			

Physical Location



Penetration Testing

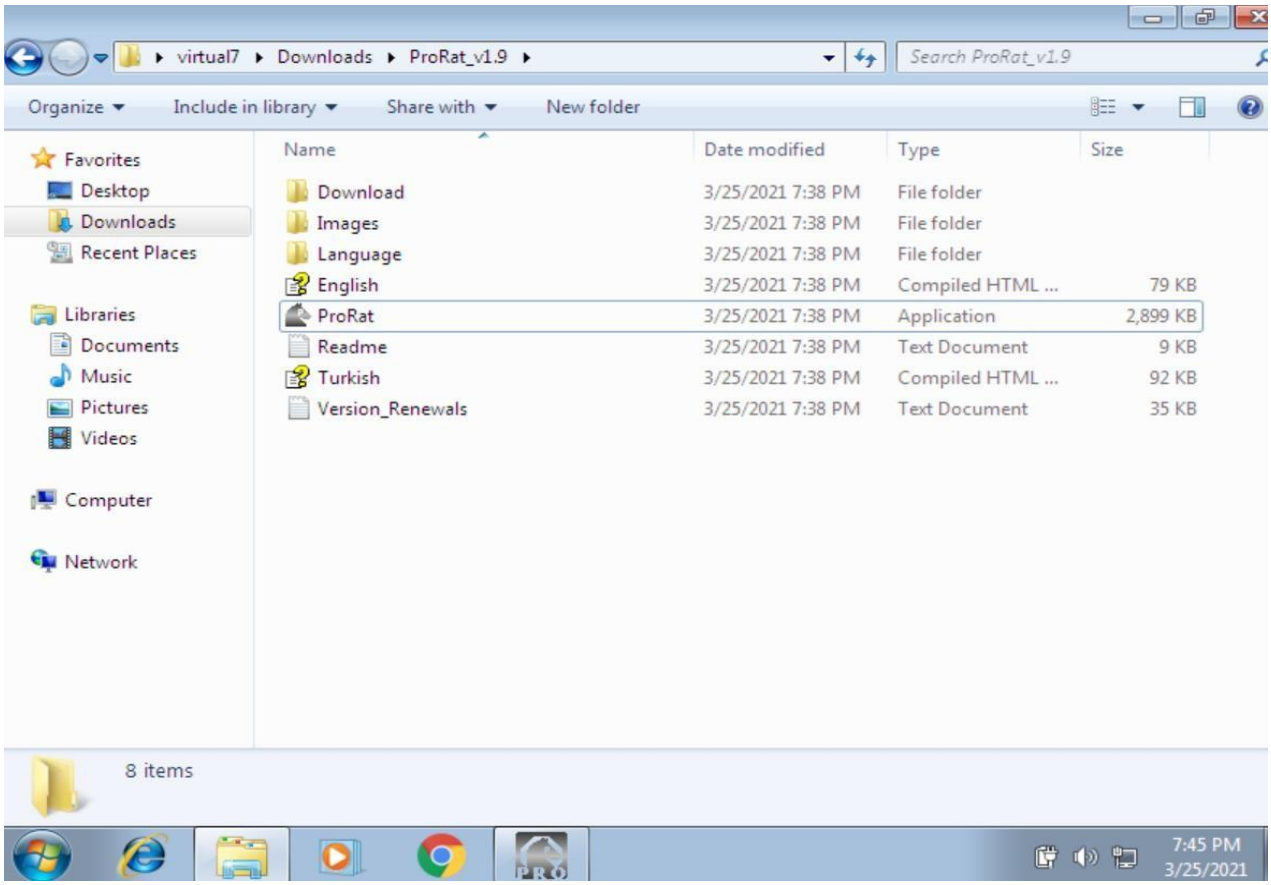
2. Penetration Testing on System

Test the Windows security using the ProRat and get access to the key logs. Delete the files from desktop or C drive and execute the commands to create a new folder in desktop and upload any file from your system.

- Testing the windows security using ProRat and access to the key logs.

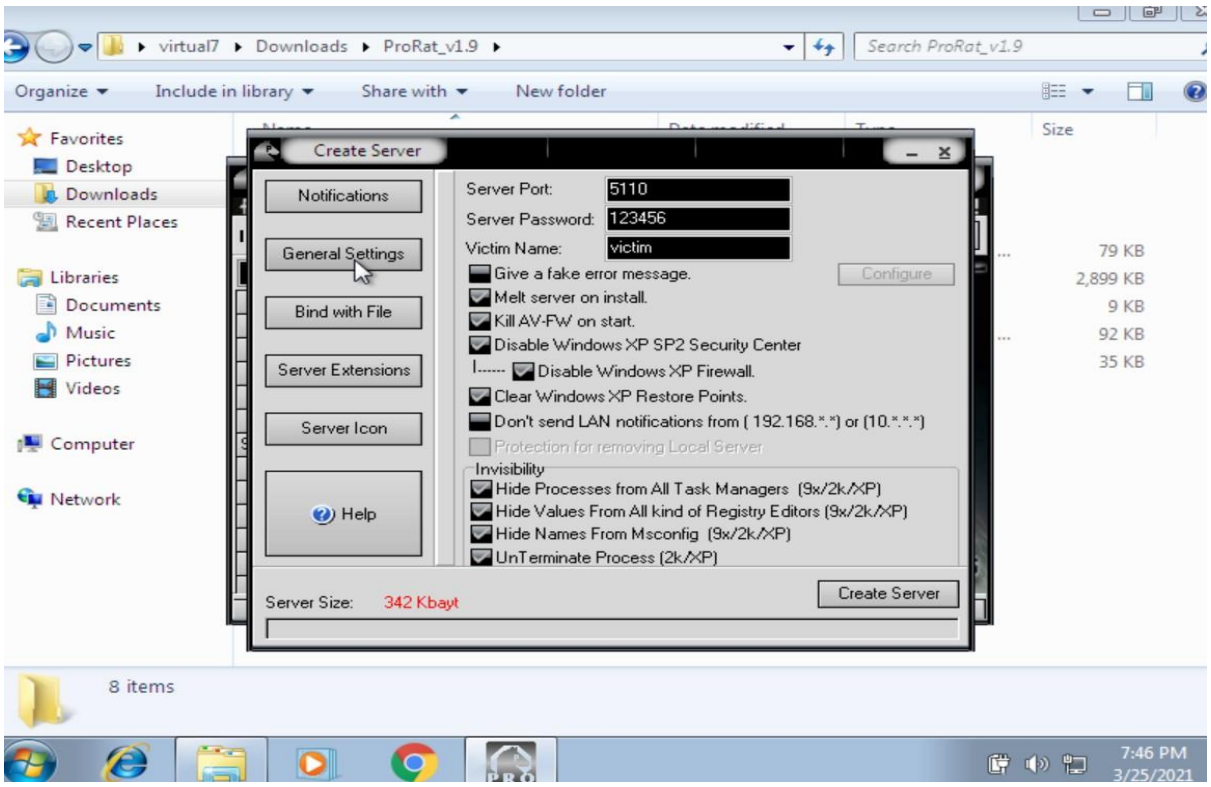
- Our **Victim machine is Windows XP** and **Hacker machine is Windows 7**.

- Here we have downloaded ProRat tool in our hacker machine so that we can create an undetected server.

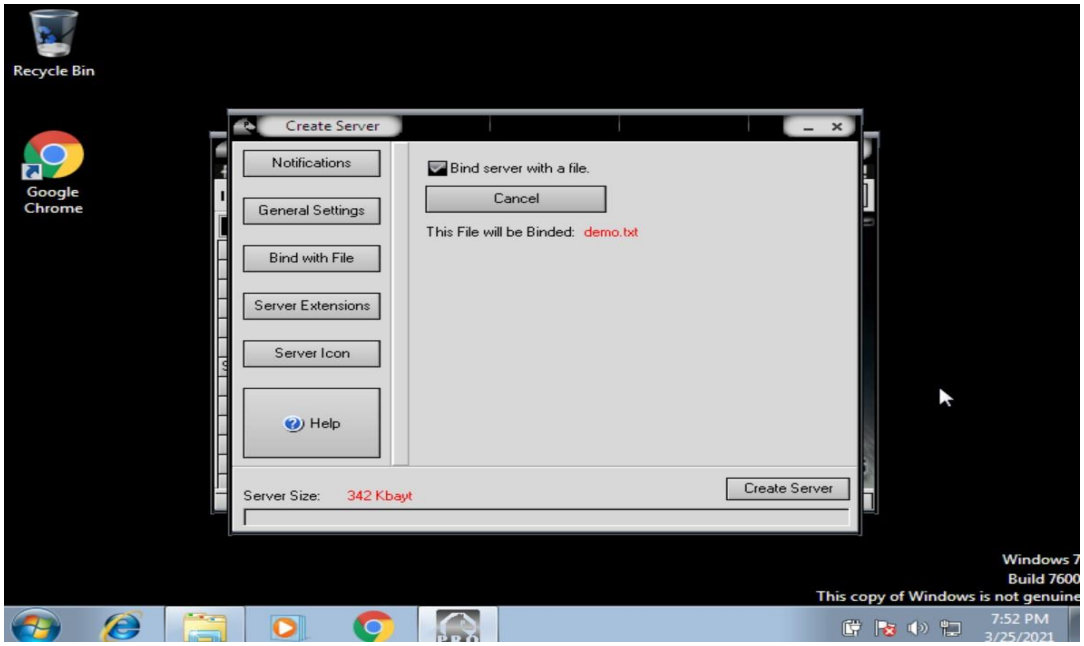


- Now, we will create a Trojan packet and the default port number is 5110.

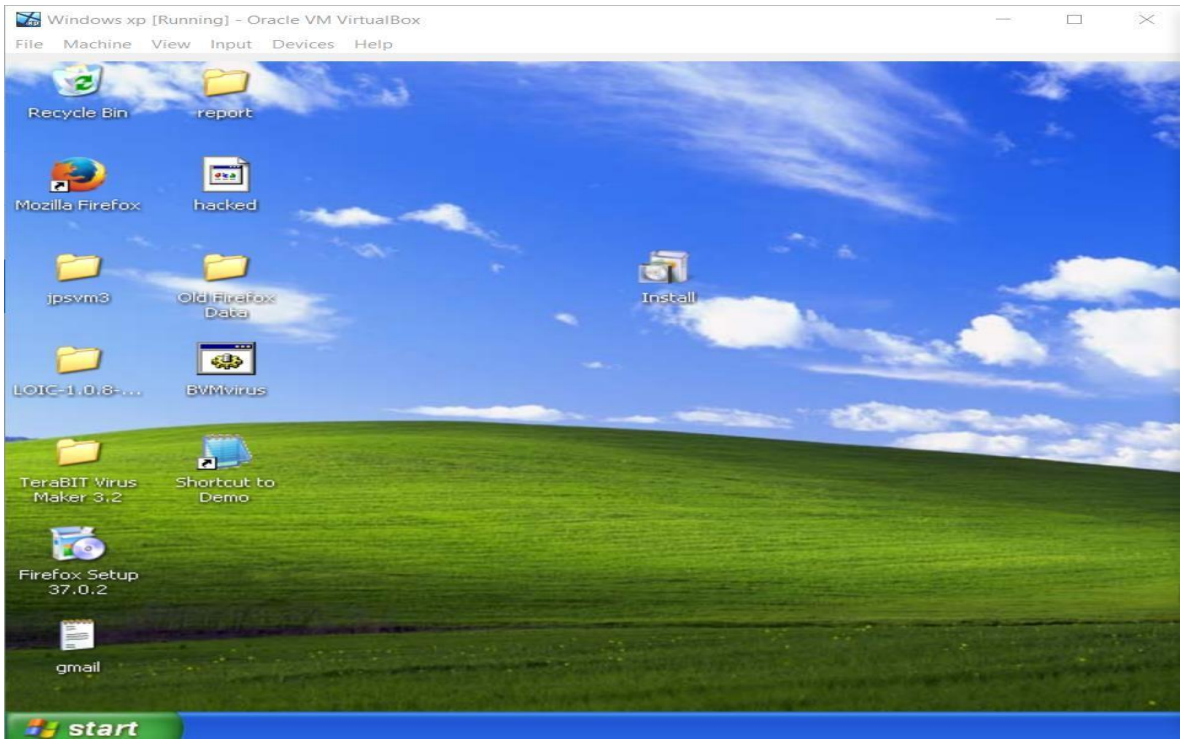
- Checking and unchecking all the boxes according to how we would like to set the settings of our packet.
- Setting the password (here I'm using 123456)



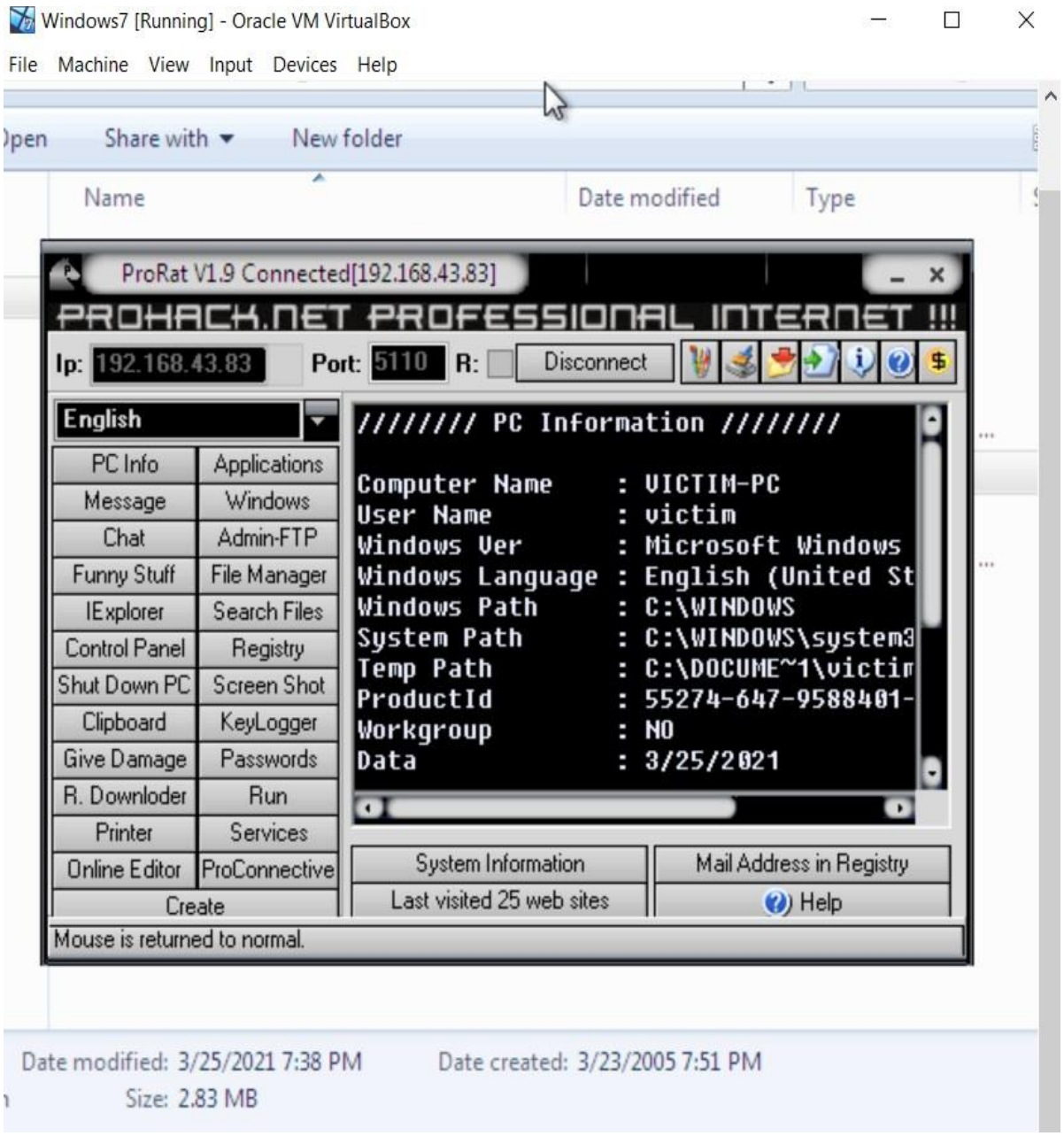
- After creating the package, we will bind it with a file which will act as a wrapper. In this case, demo.txt act as a wrapper with the server extension as .exe so that it looks like a genuine document.



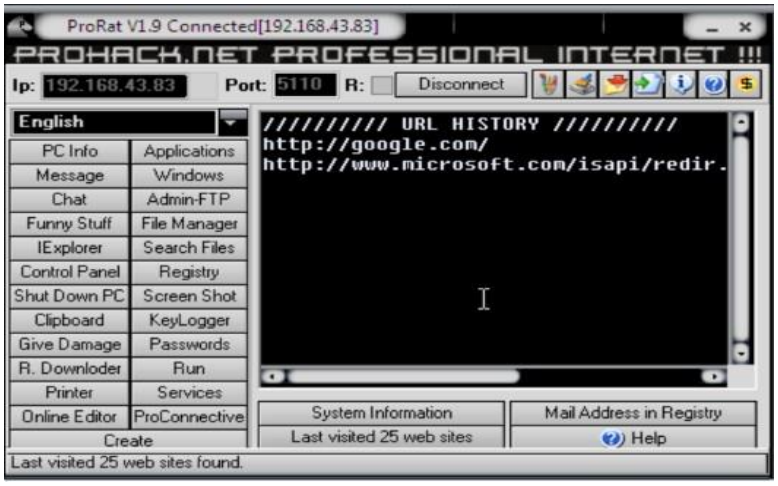
- Now we will send this packet/wrapper/Trojan to the victim machine through mail or any other means.
- Here, this is our victim machine windows XP and we have downloaded the document demo.txt over the desktop.



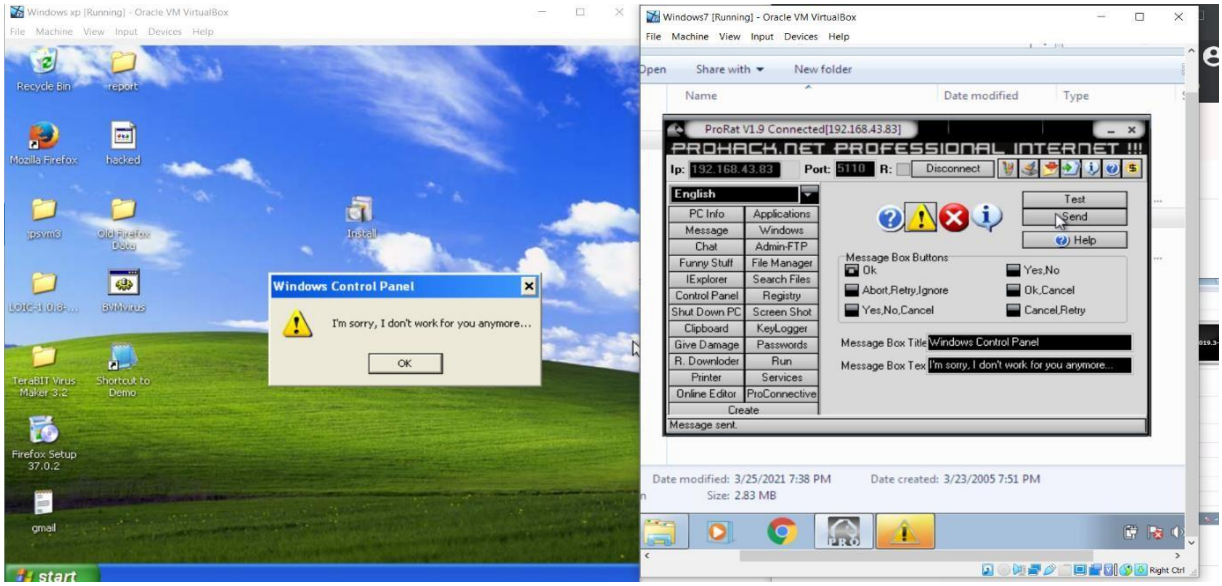
- The moment this text file was opened, our Trojan was executed without giving the machine any warning.
- On connecting the ProRat tool to the victim machine by using its IP address, it gave us the whole remote access to the machine including all the stuffs given below.
- We can check a lot of information regarding the victim machine like system information, last 25 sites visited by the host, ports running, services open etc.
- PC information is shown below.

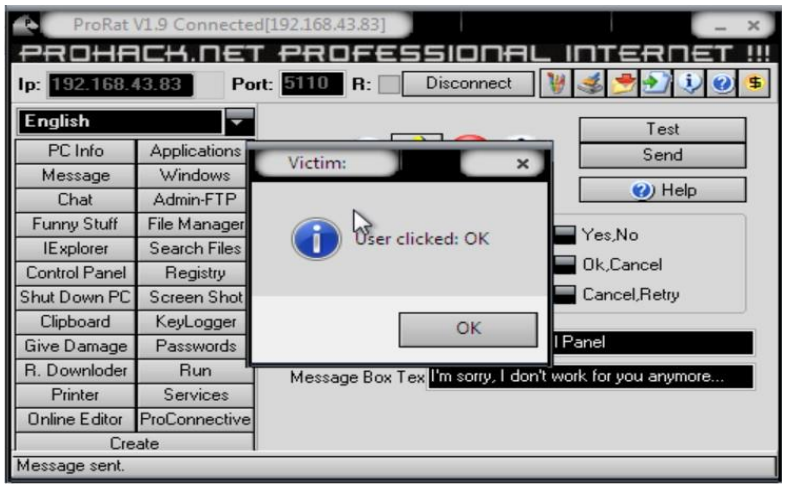


- Last visited websites information is shown below.

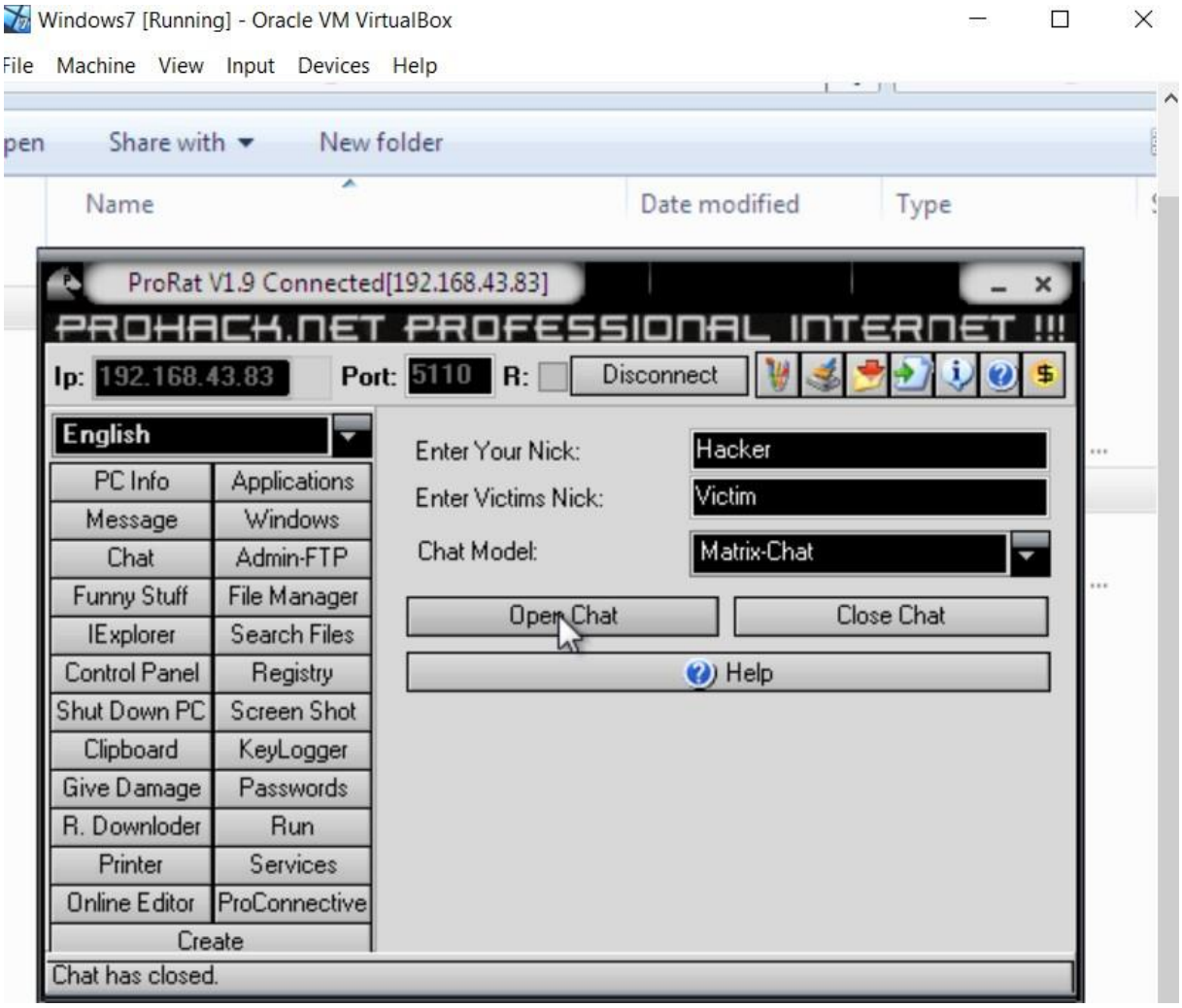


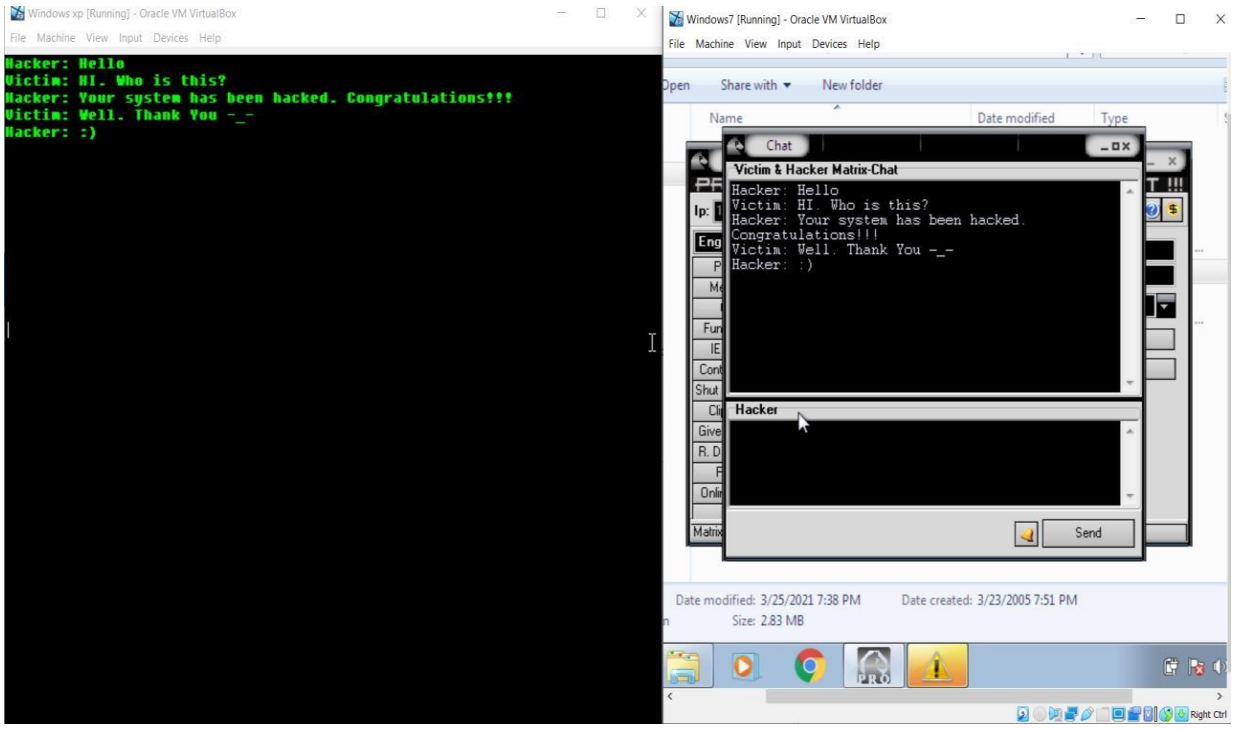
- We can even send a warning pop up like this and each activity of the victim machine can be monitored by the hacker without the knowing of victim.



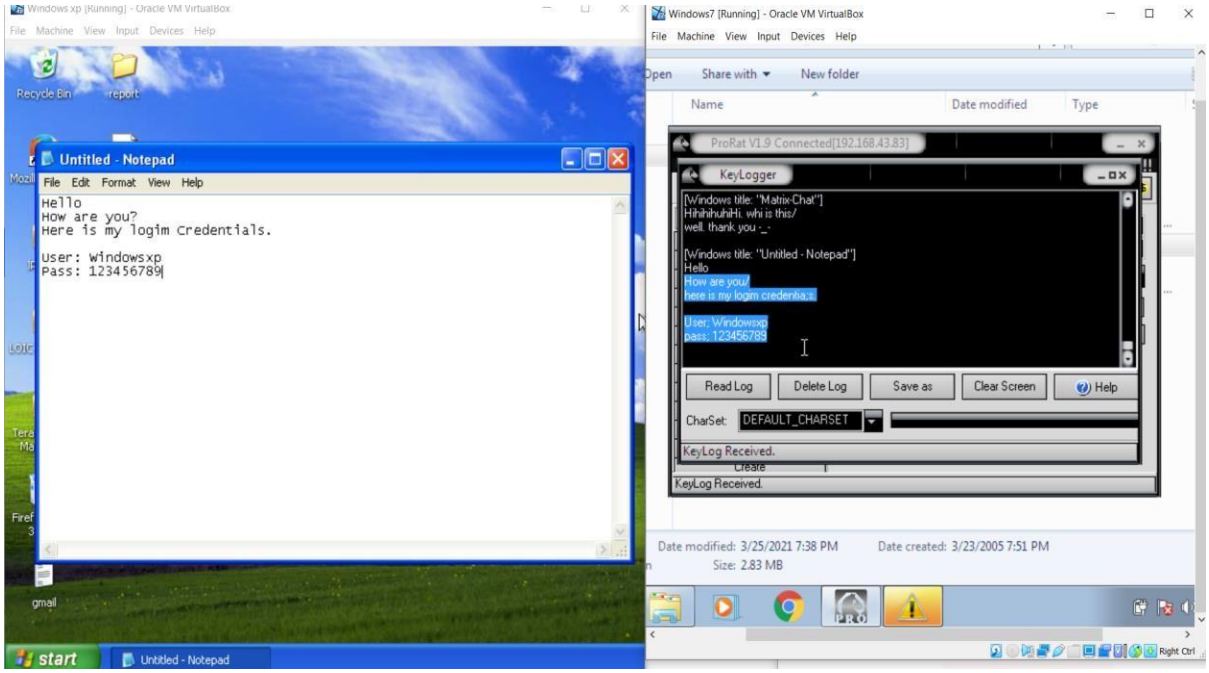


- We can also chat with the host by using this tool.

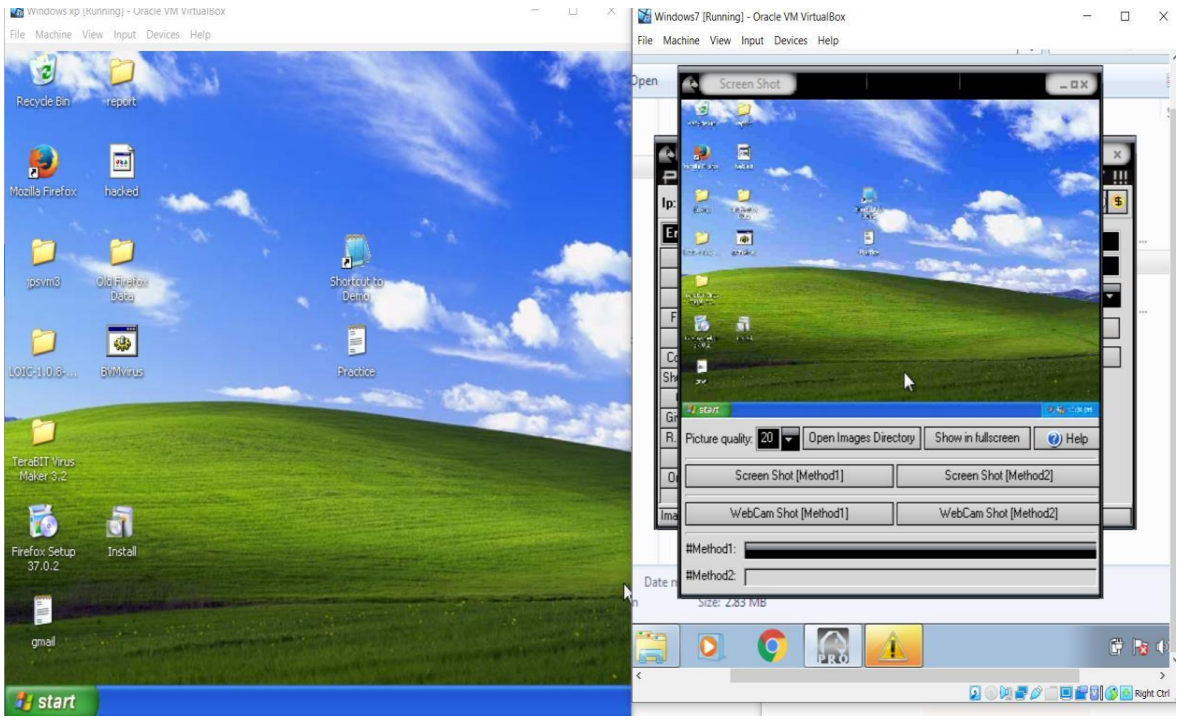




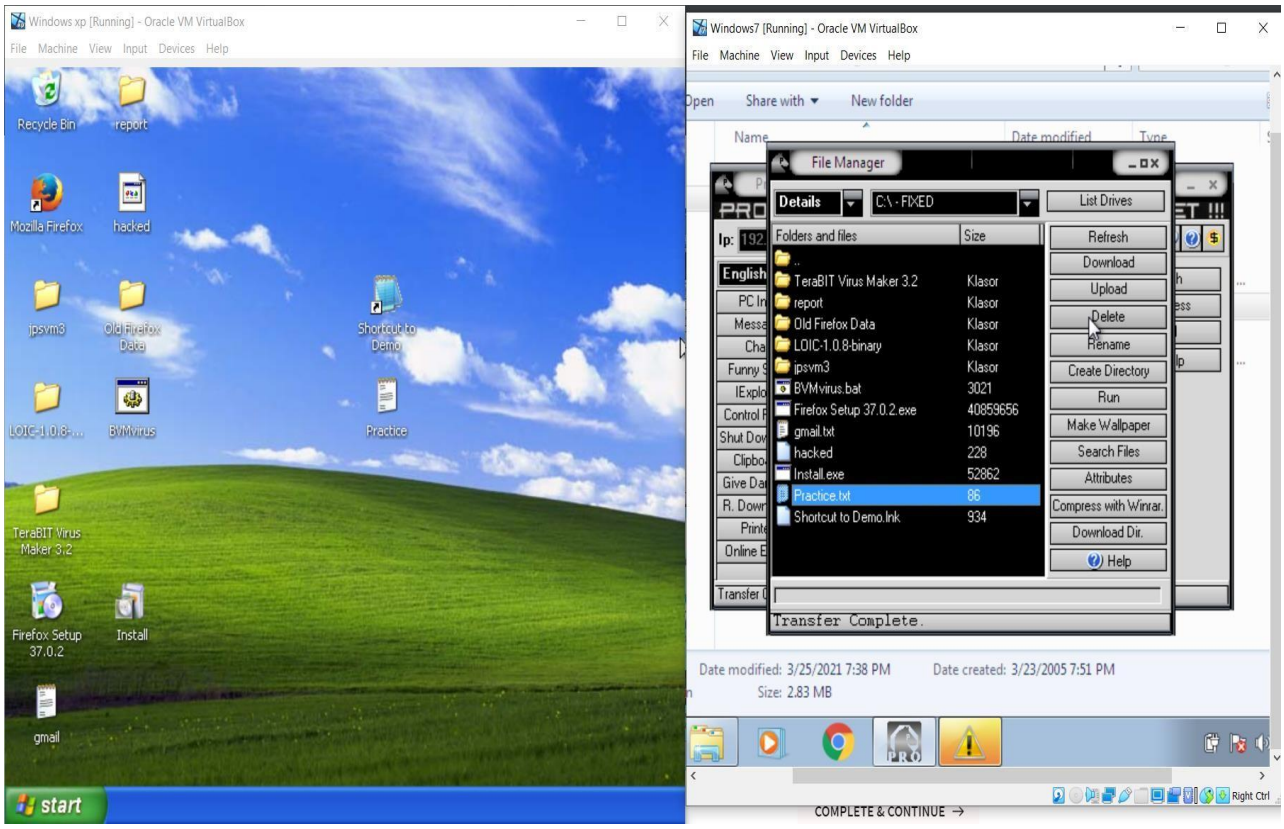
- We also have access to the key logs. User wrote his/her login credentials in an input area (here it being a notepad) and it can be accessed in the hacker machine like this.
- The file is being saved as Practice.txt .

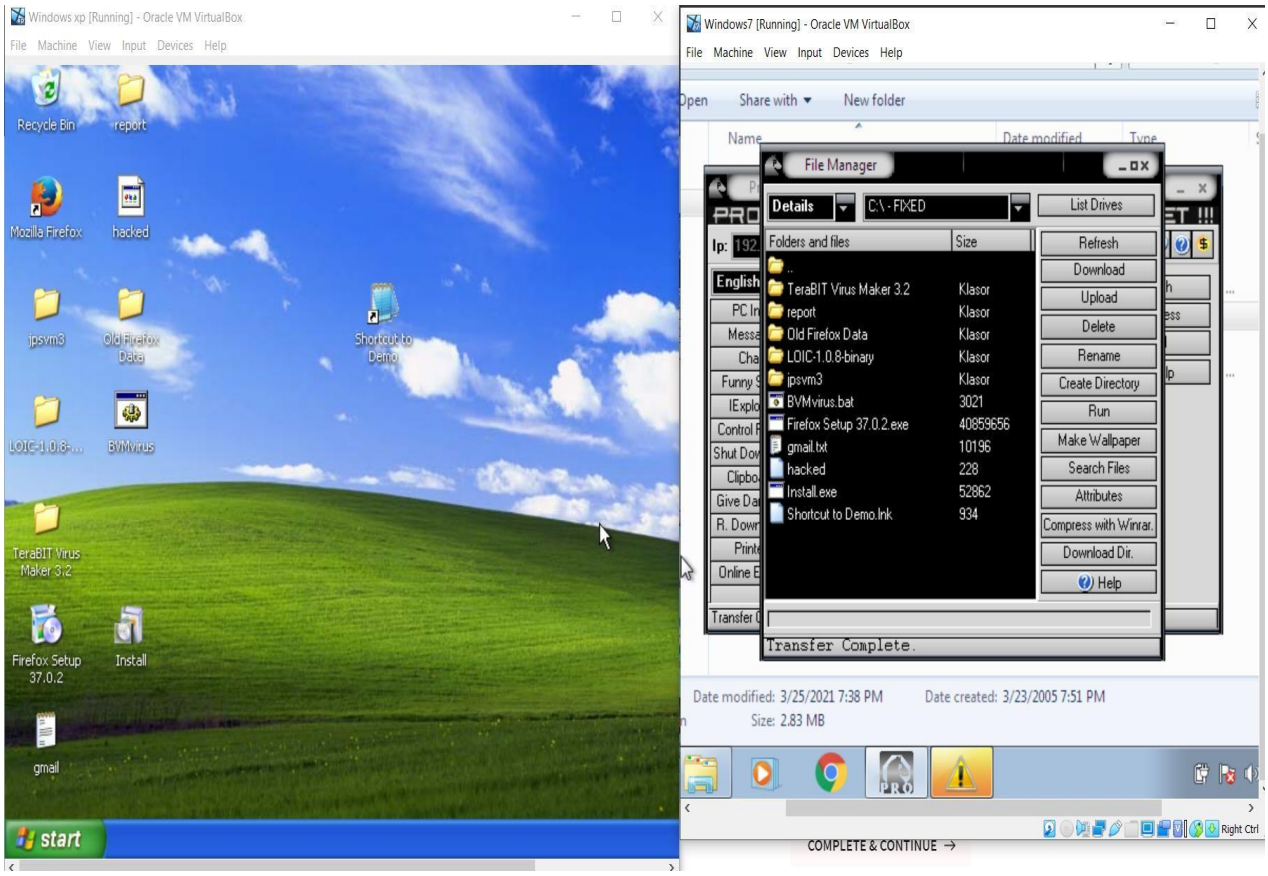


- We can check the site or file opened by the victim by taking a screenshot of its current activity. This stuff is done without the host knowing.

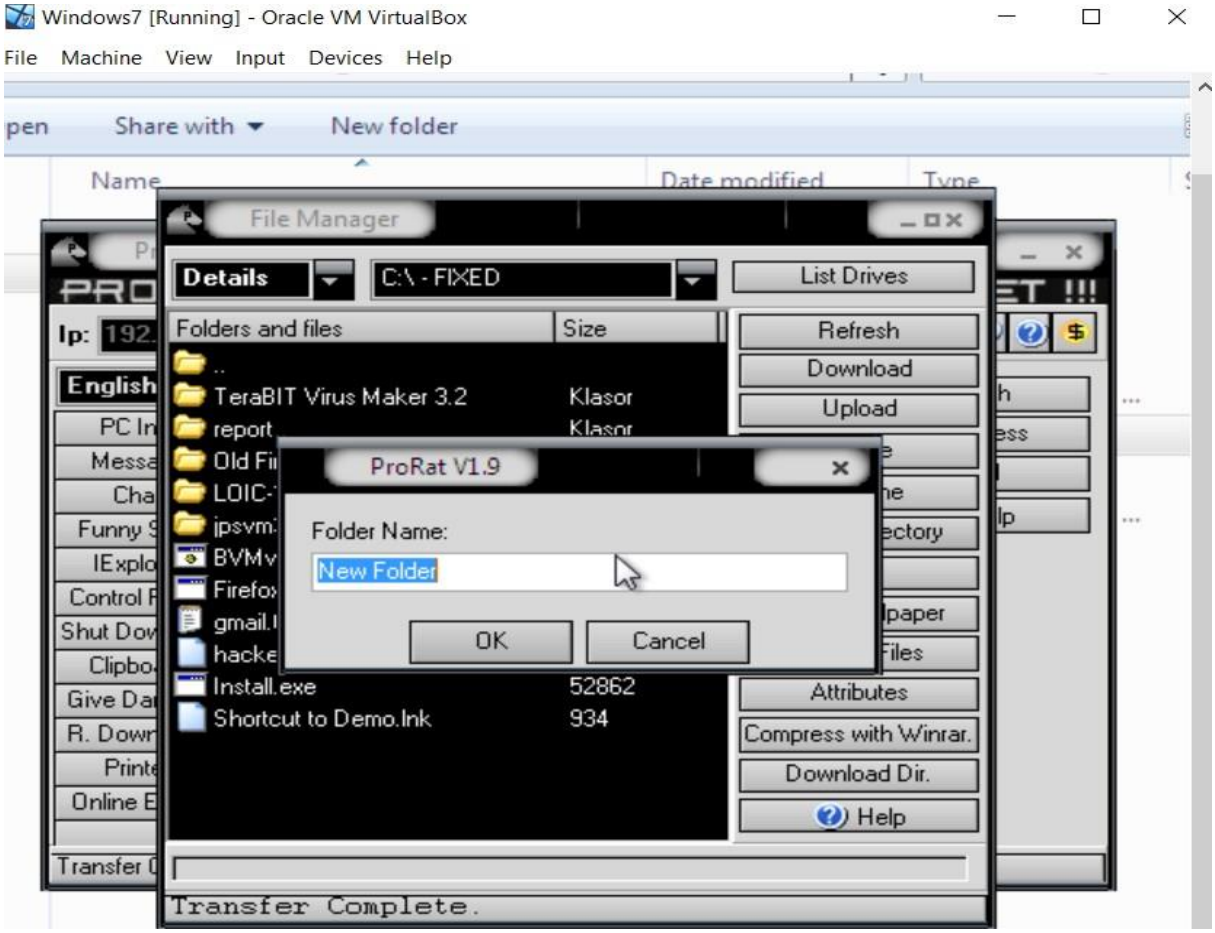


- We can delete any file or folder like this (here it being the Practice.txt from desktop).

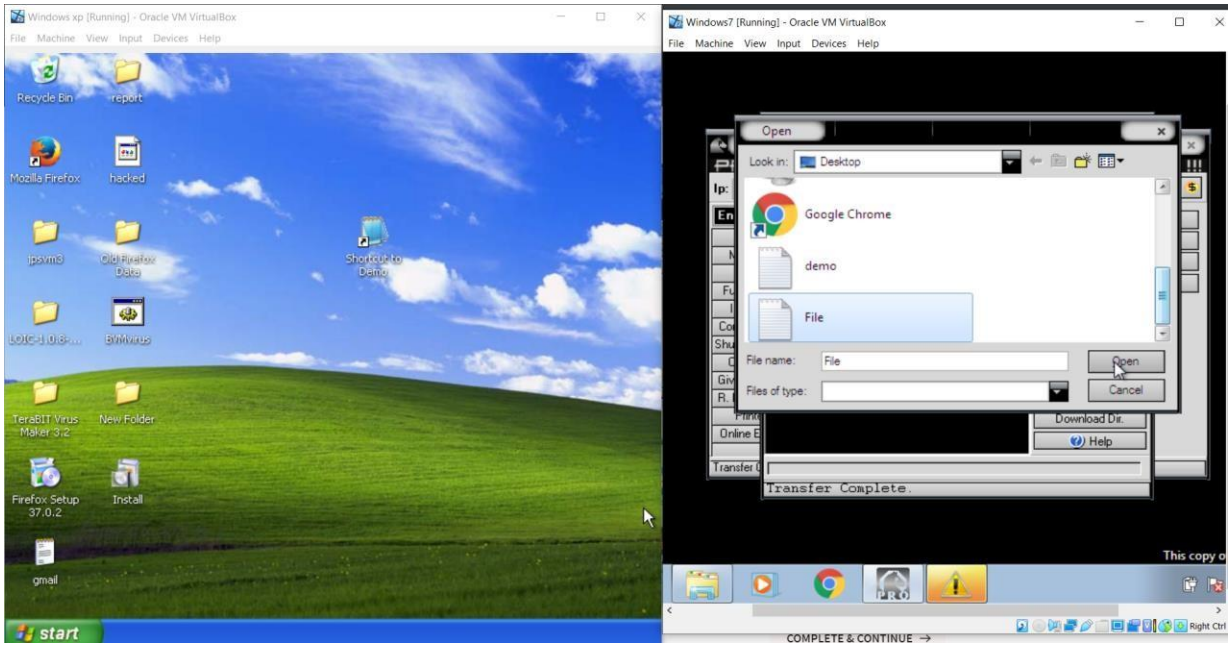


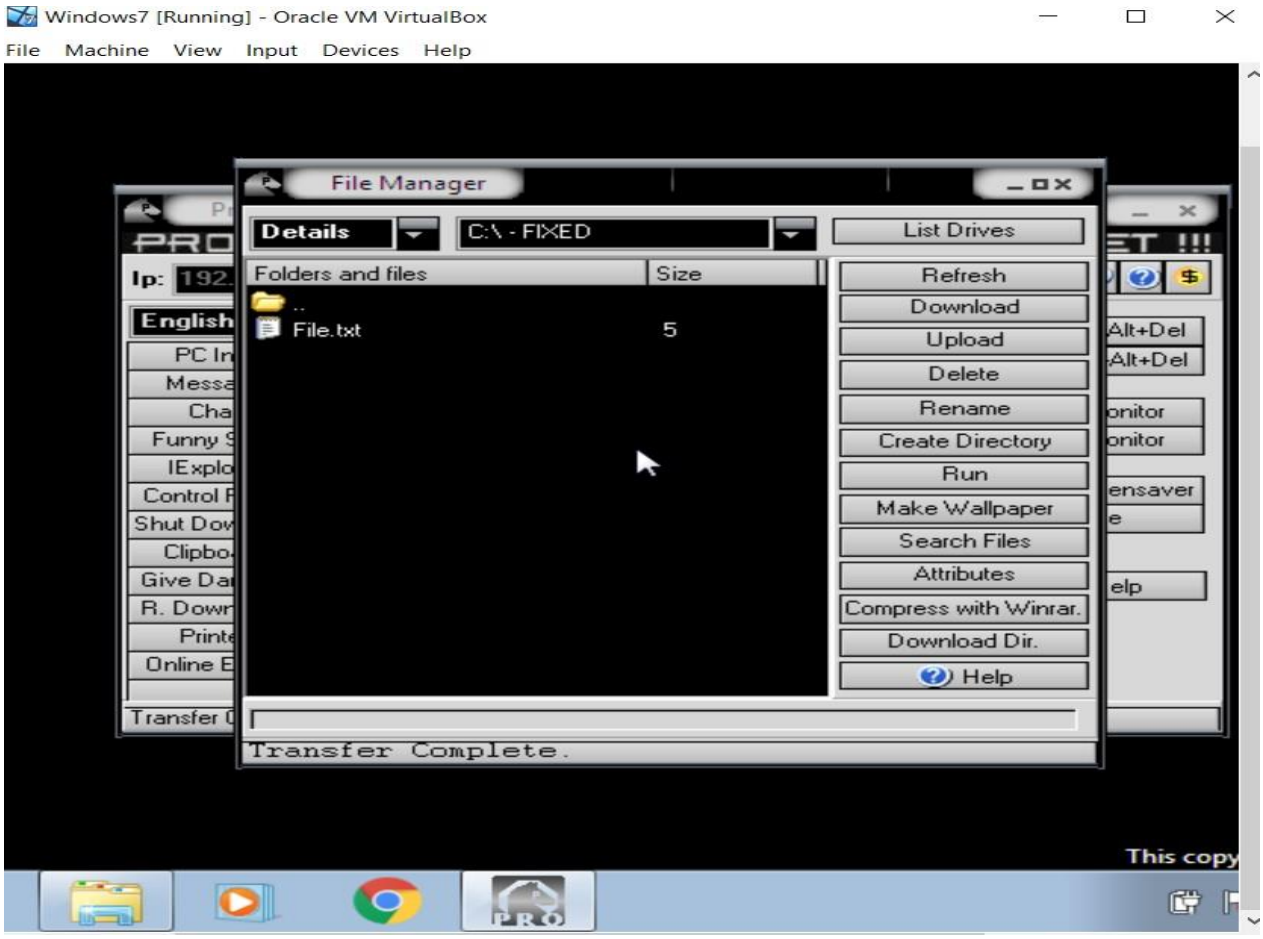


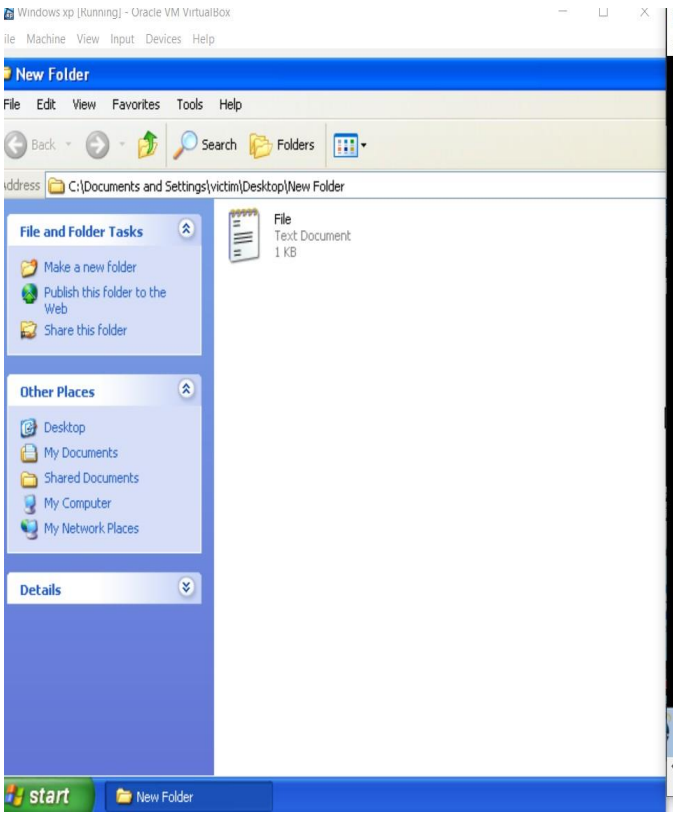
- New folder can also be created.

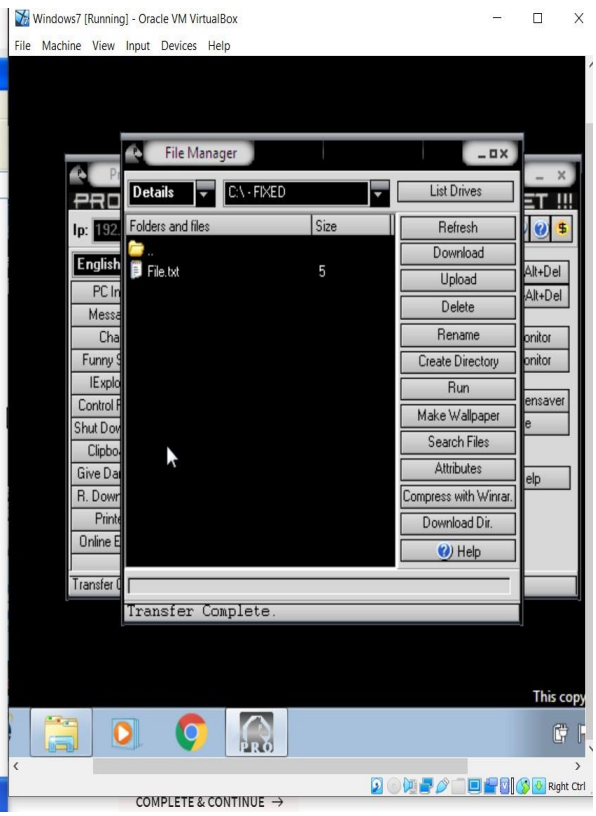


- Another file named File.txt has been uploaded on the victim machine in the newly created folder “New Folder” from the Hacker machine.




Windows7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Manager
Details
C:\ - FIXED
List Drives
Folders and files
Size
File.txt
5
Refresh
Download
Upload
Delete
Rename
Create Directory
Run
Make Wallpaper
Search Files
Attributes
Compress with Winrar.
Download Dir.
Help
Transfer Complete.
This copy


Windows xp [Running] - Oracle VM VirtualBox
New Folder
File Edit View Favorites Tools Help
Back
Search
Folders
C:\Documents and Settings\victim\Desktop\New Folder
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
Desktop
My Documents
Shared Documents
My Computer
My Network Places
Details
File
Text Document
1 KB
start
New Folder


Windows7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Manager
Details
C:\ - FIXED
List Drives
Folders and files
Size
File.txt
5
Refresh
Download
Upload
Delete
Rename
Create Directory
Run
Make Wallpaper
Search Files
Attributes
Compress with Winrar.
Download Dir.
Help
Transfer Complete.
This copy
COMPLETE & CONTINUE →

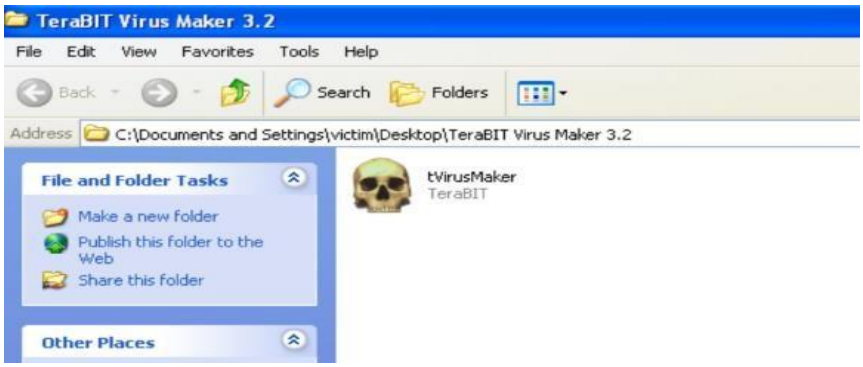
- Thank you!

Malware Creation

3. Malware Creation, Exploitation, and Mobile Hacking

Create a virus using Tetrabit Virus Maker and execute the virus in the victim machine.

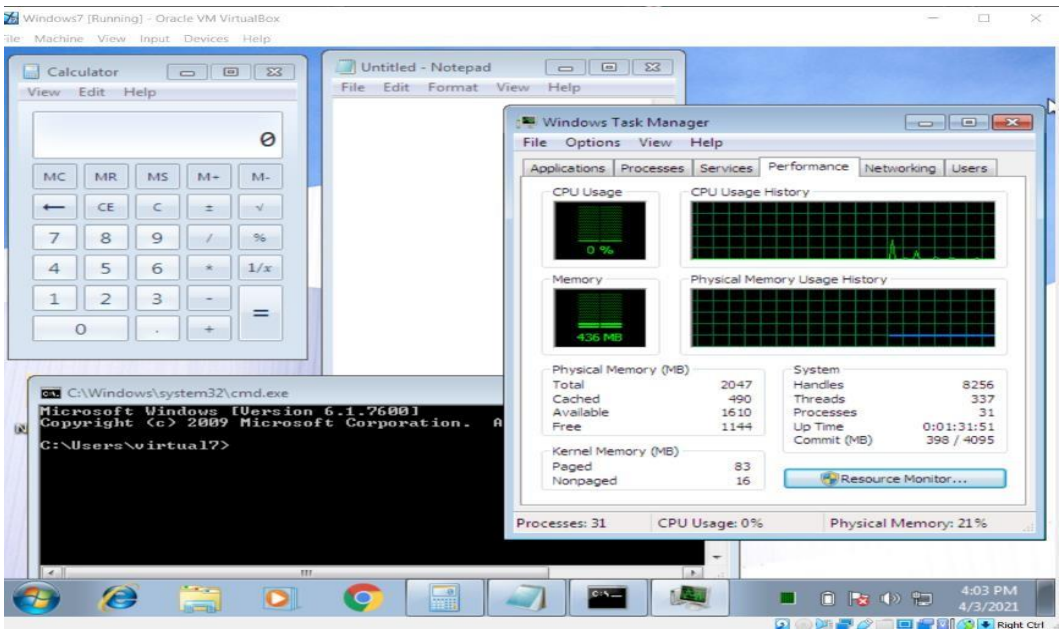
- To infect a system with a virus, first we need to create a virus.
- Here, we will create a virus of our own specifications by using Tetrabit Virus Maker tool.
- Here, our hacker machine is **Windows XP** and our victim machine is **Windows 7.**
- Let's first install and run the virus maker in our hacker machine.



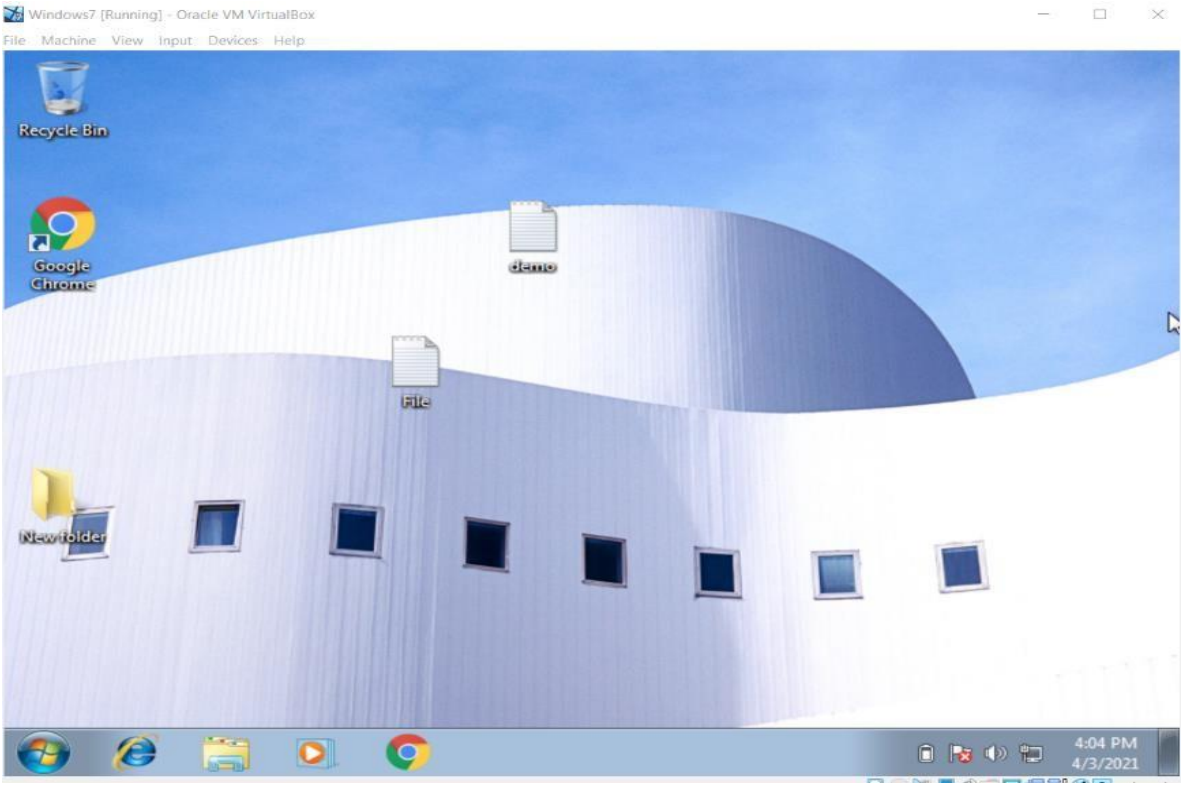
- The main window of this tool looks like this.

- Now, let’s give this tool the specifications we need to in our virus. For example: enabling avoid opening calculator, notepad, add 30 user accounts to windows, avoid opening Mozilla Firefox, always clean clipboard, disconnect from internet, disable command prompt, disable task manager, mute system volume, remove desktop wallpaper, remove windows clock etc.

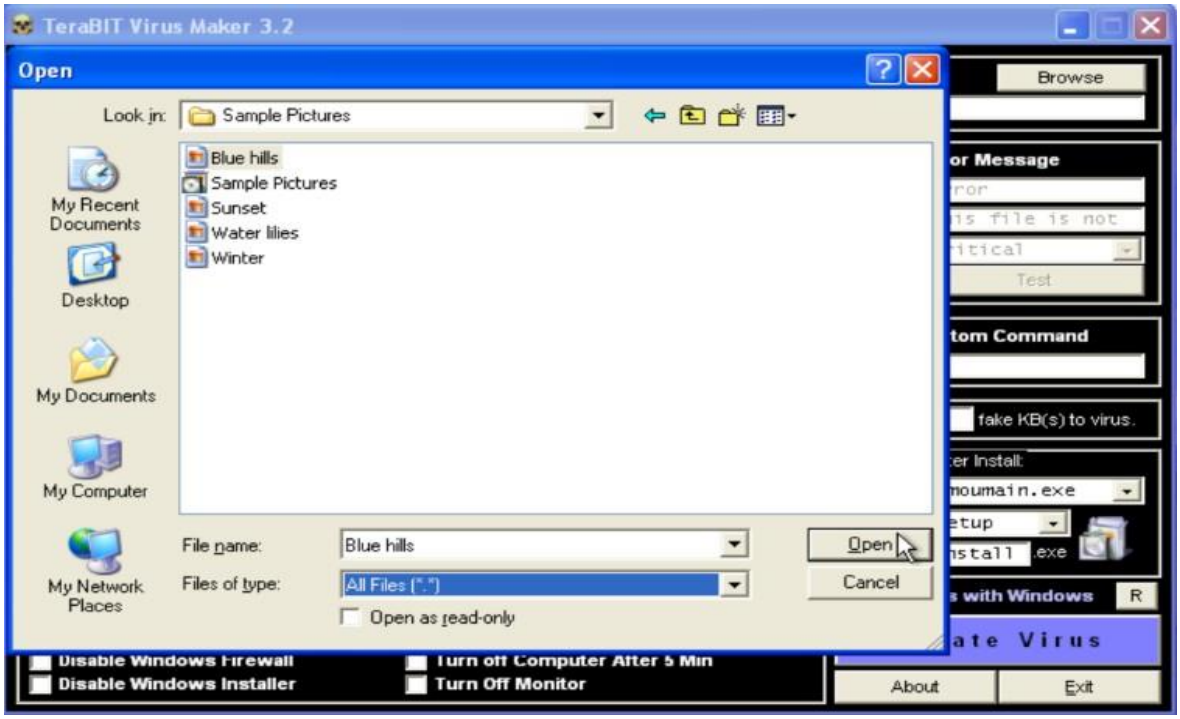
- Let’s also check the before virus infected condition of our victim machine i.e. Windows 7.
- We are able to open calculator, notepad, task manager etc.



- We are also able to see the internet connection enabled, windows clock time, wallpaper etc.



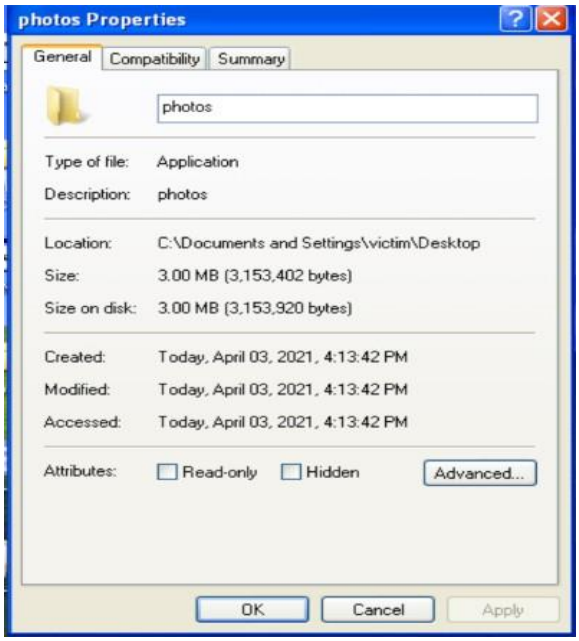
- Binder is also available so to make our virus file look genuine, we will bind it with a file (I'm taking an image file named **blue hills**). Browse and select.



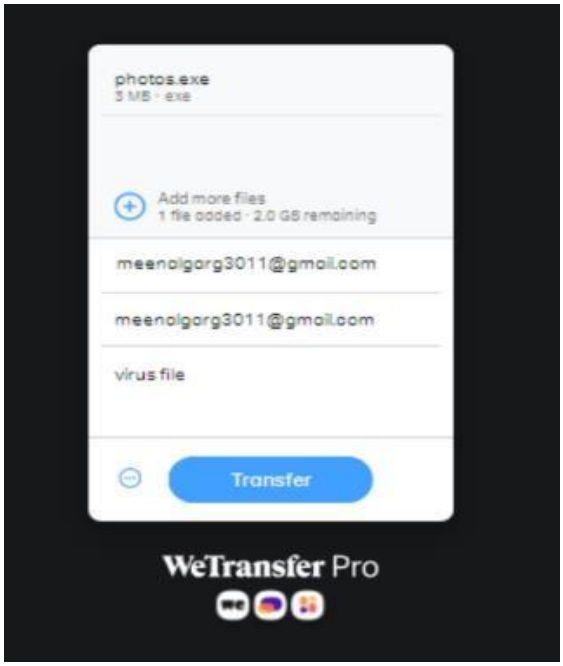
- We will set the fake kb size as **3000 KB** (3 MB), give it an **update.exe** extension, **folder** icon, name as **photos.**
- Click on create virus.

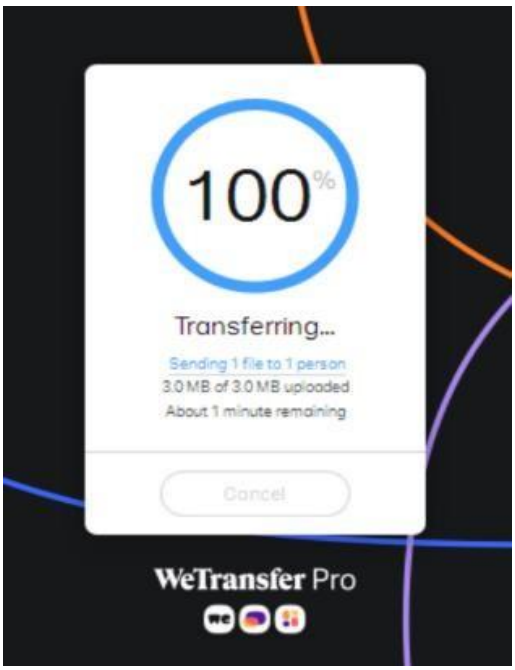
- Select the location and click on OK.

- We saved it on our hacker machine's desktop. We can see the specification we gave it in its properties.

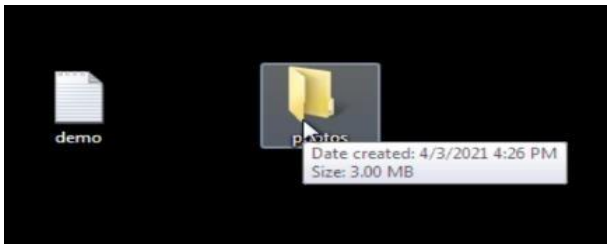


- To transfer our virus file to the victim machine, we will use https://wetransfer.com/ site.

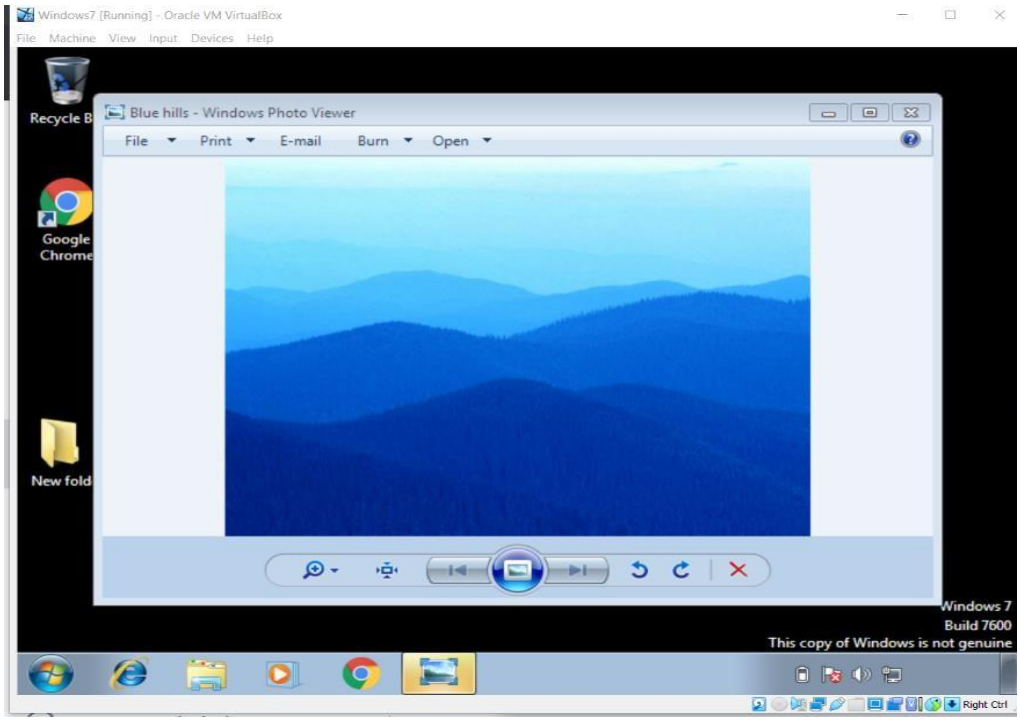




- We have downloaded our virus file in the victim machine with specifications remaining the same.

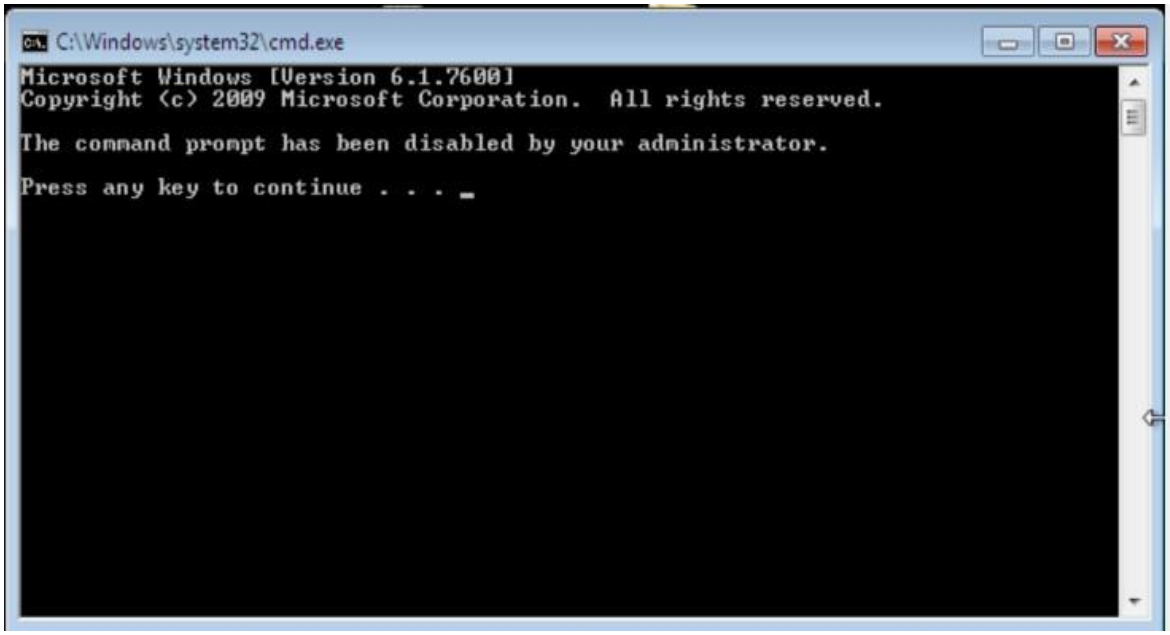


- The moment the file is opened, the virus gets executed destructing the system according to the hacker.

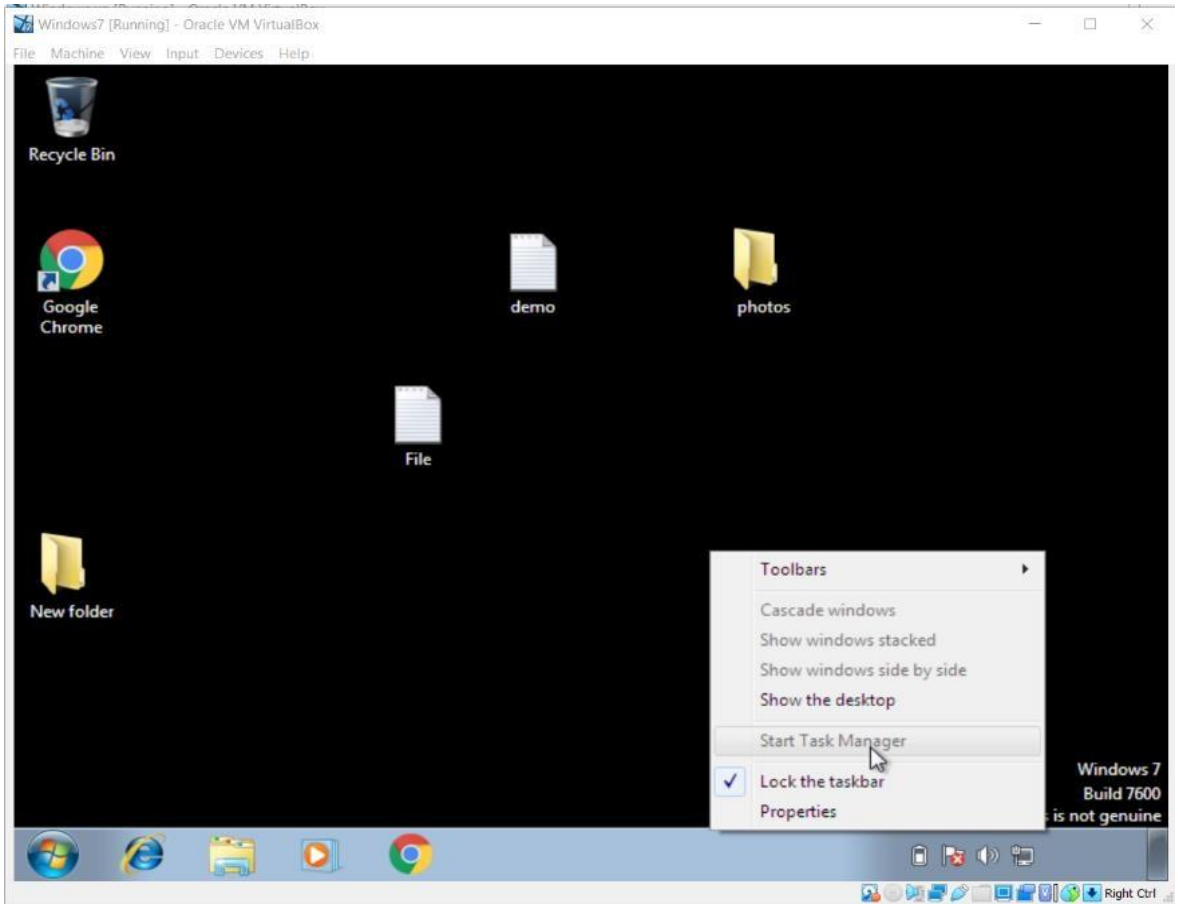


- Now, on clicking over calculator and notepad, they are not being opened.

- Command prompt shows that the access has been denied.

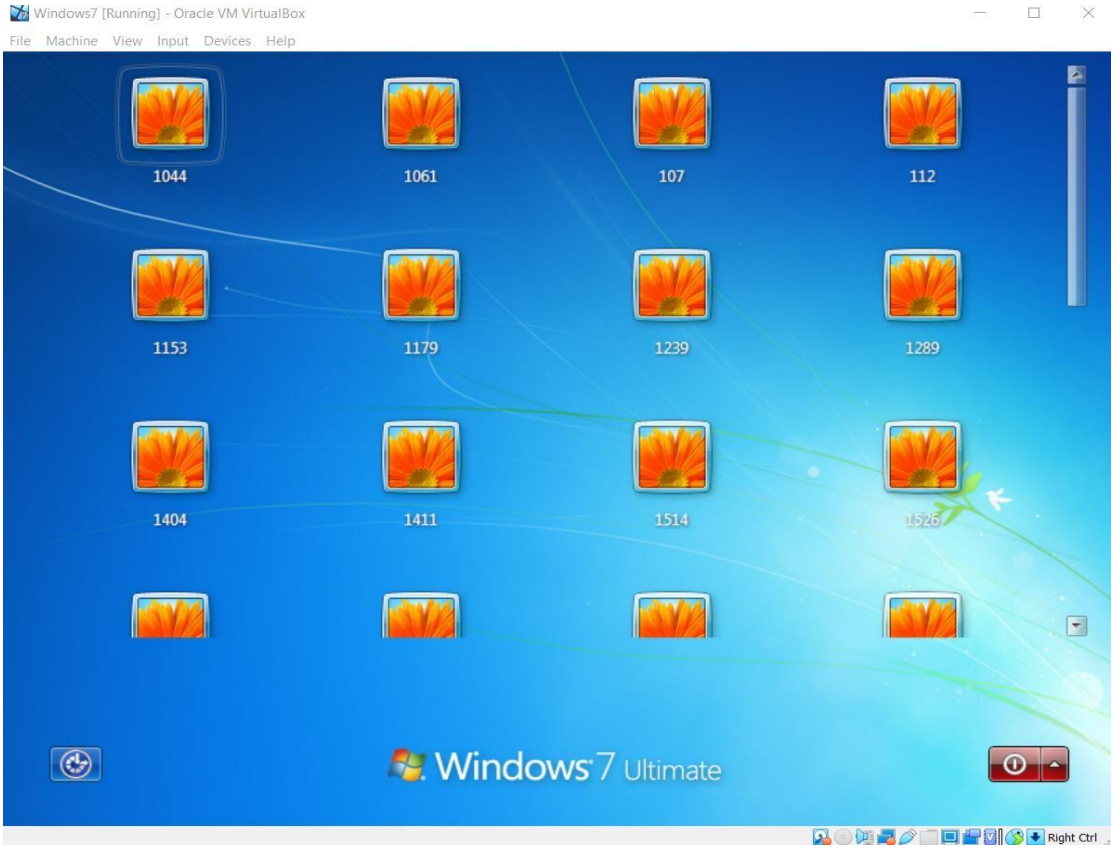


- Task bar option has been disabled. With this, clock has also disappeared, internet connection has been stopped etc.



- Let’s restart our victim machine.

- On restarting, there are 30 unknown user accounts shown.

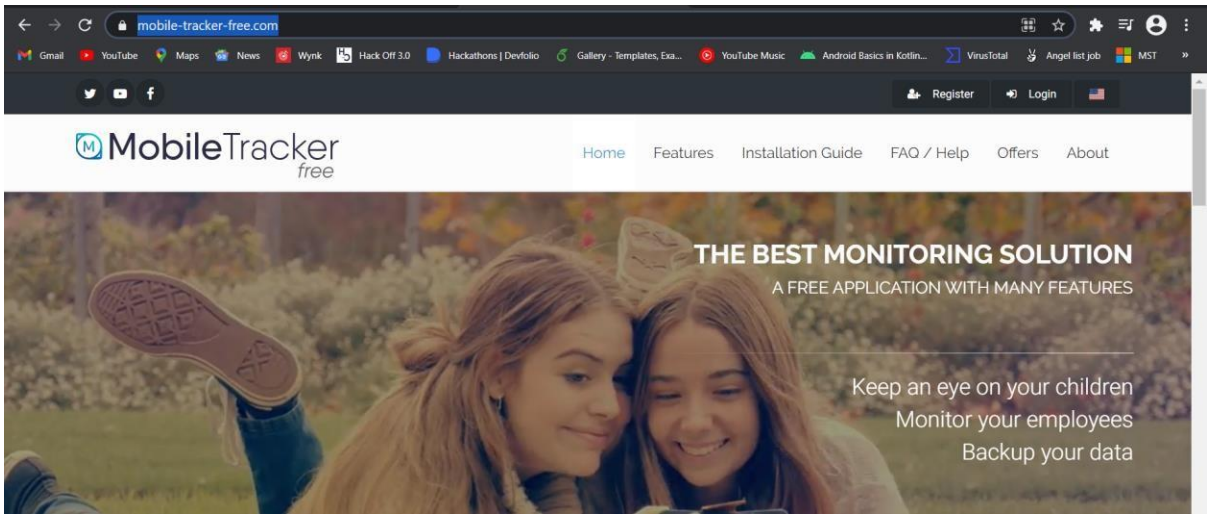


- These were some basic operations shown. We can also format/crash the whole system.
- Here, we are done with Virus.
- Thank you!

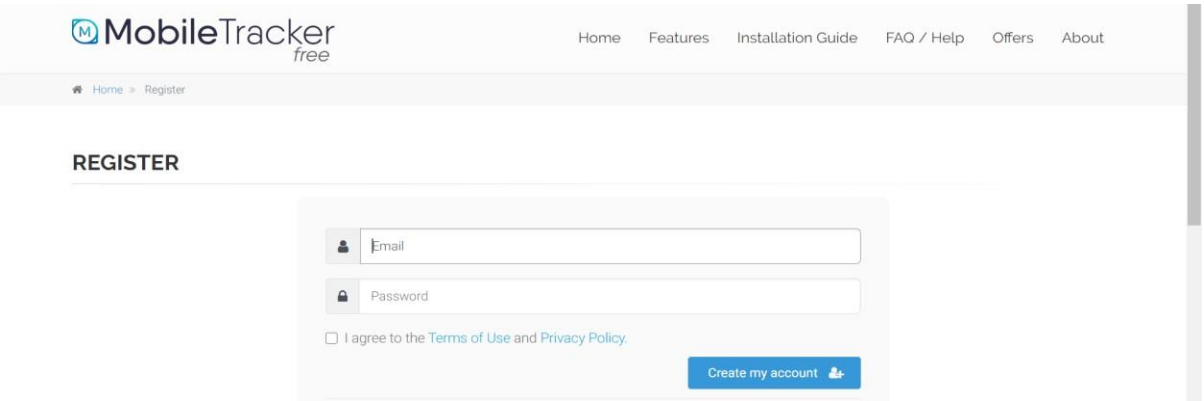
Mobile Hack

Hack the mobile device using online tool MTF, gather the call list contacts, and access the camera

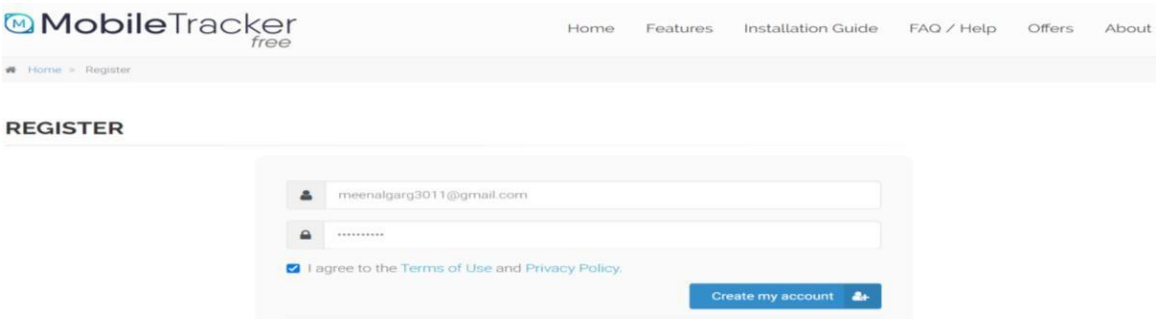
- Hacking mobile device using MTF tool (Mobile tracker free)
- Visit https://mobile-tracker-free.com/ site. For hacking a mobile device we need to make an account over this site.



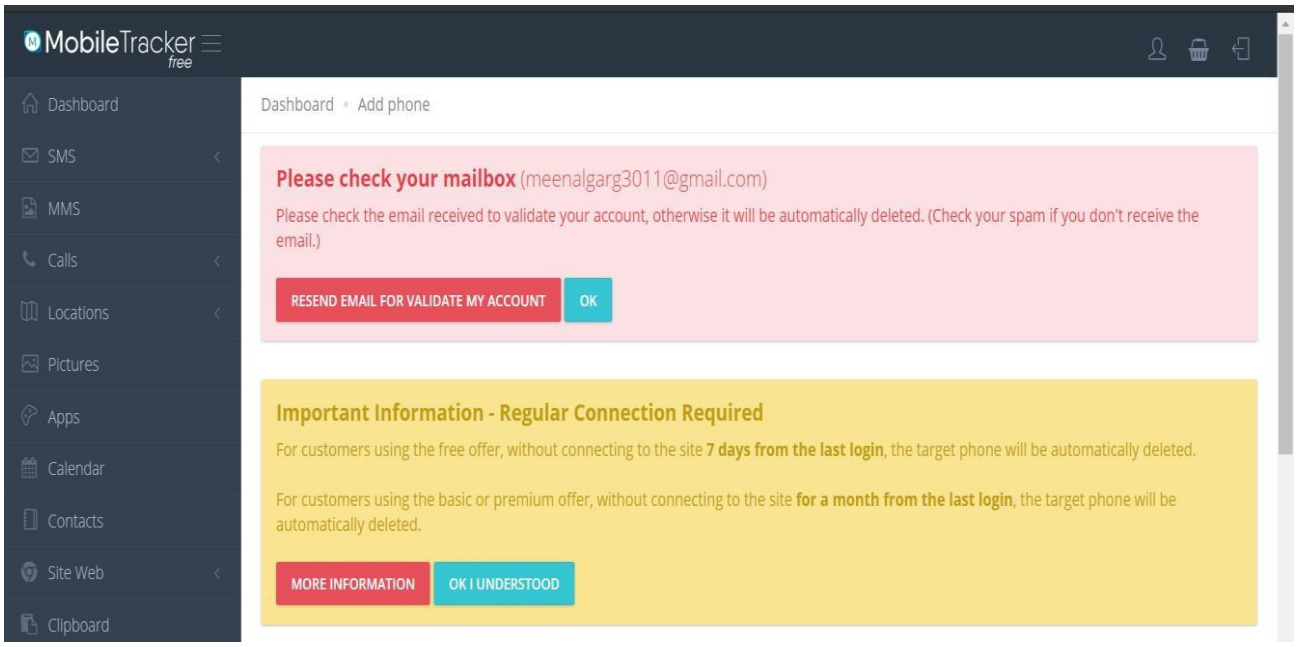
- Click on register.



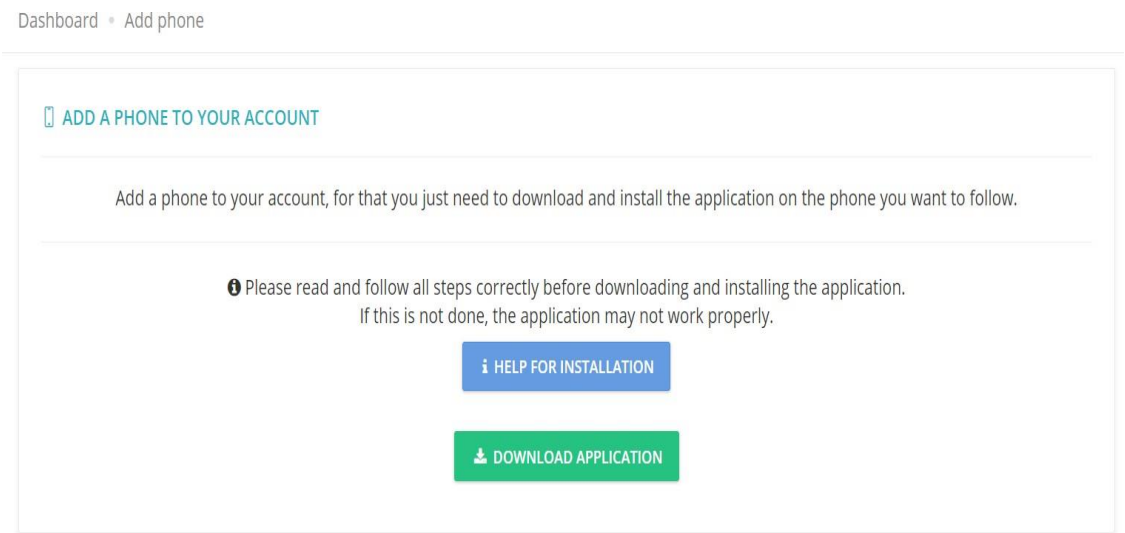
- Enter email id and set a password for this account.



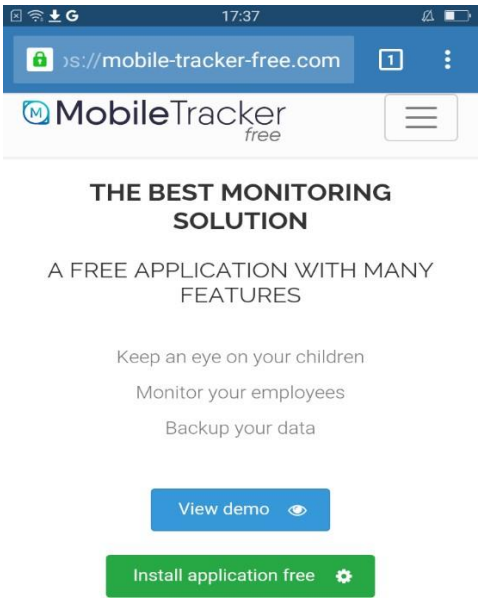
- Click on **“OK I UNDERSTOOD”** and verify your mail from your registered id.



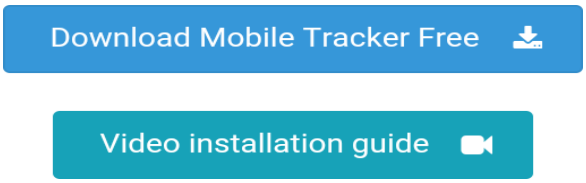
- After verifying, the window should look like this.
- Initially, no phone is added.



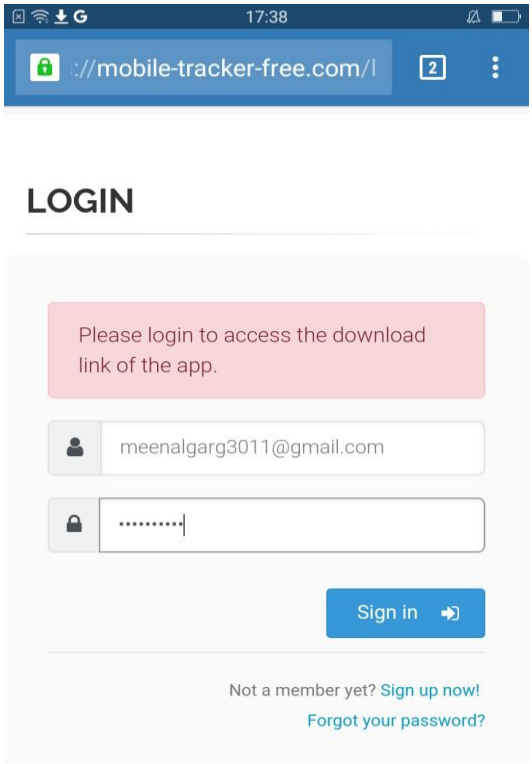
- Now, let’s move to our victim device i.e. mobile device.
- To get access of the device, we need to install MTF in the victim device. It is not available on playstore so we will download it from the https://mobile-tracker-free.com/ site.
- Open this site in google chrome or any other browser.
- Now, click on **Install application free.**



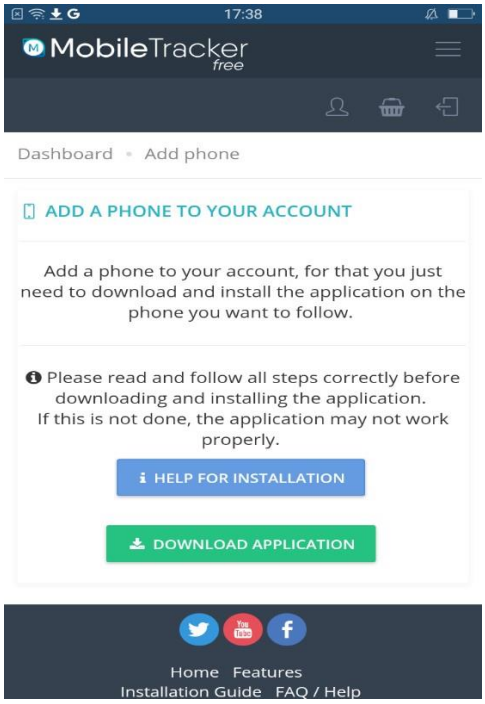
- Click on **Download Mobile Tracker Free.**

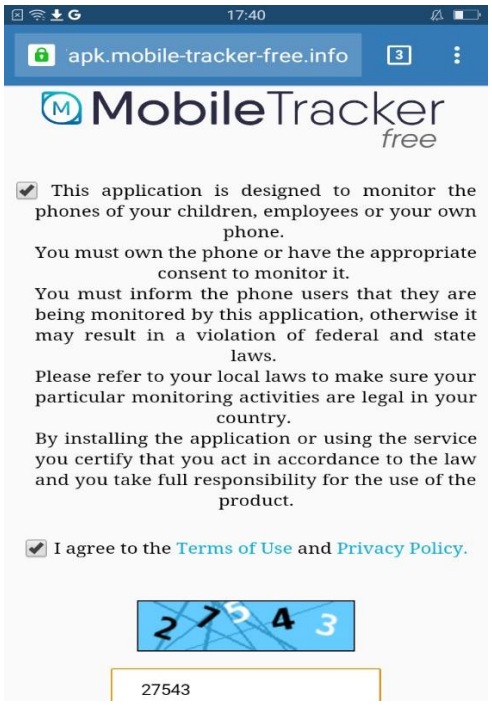


- Login using id and password we setted up on this site.



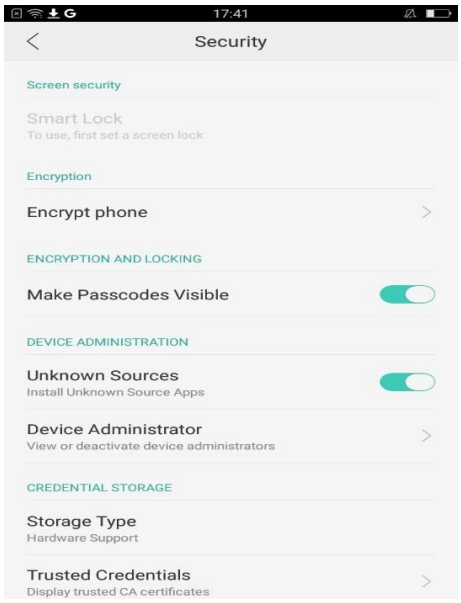
- Click on **DOWNLOAD APPLICATION.**
- Accept all the terms of use and privacy policies, enter the captha and **DOWNLOAD**.



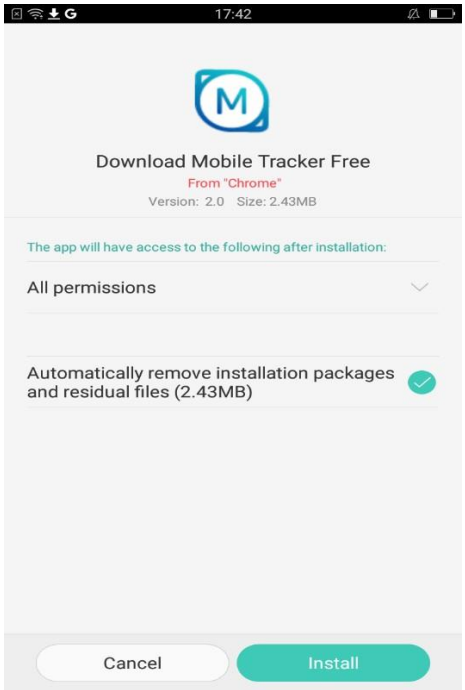


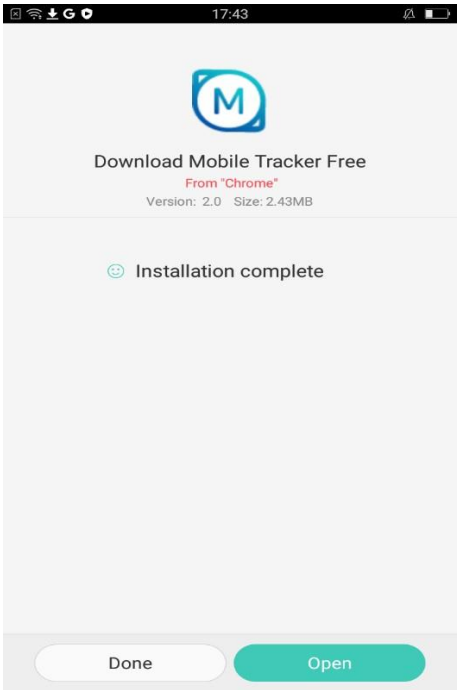
- Now, the APK file is downloaded. Click on **OPEN.**

- Open Settings and allow installation from unknown sources.
- Continue Installing.

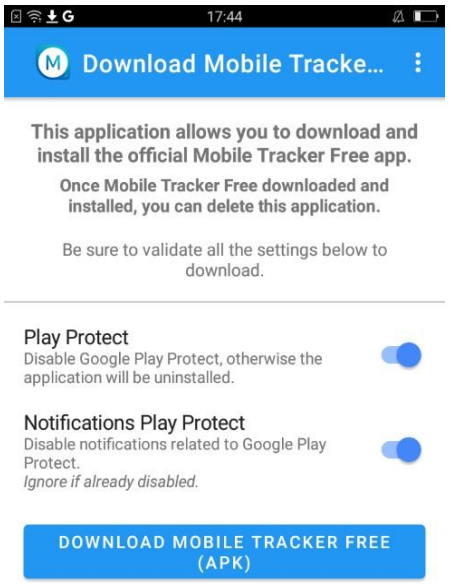


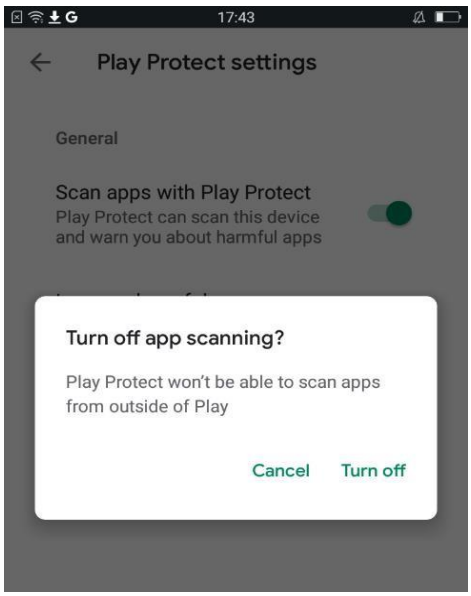
- Click on **Install** and **Open.**



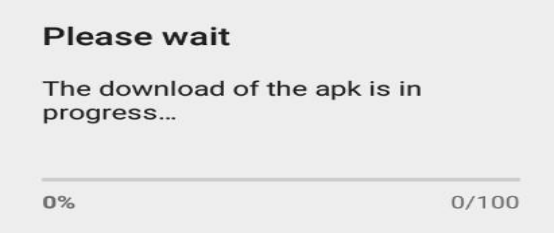


- To enable Play Protect, turn off App scanning in its settings.

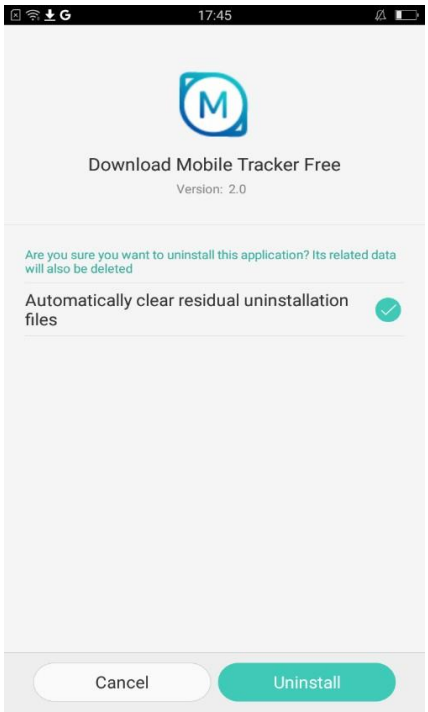




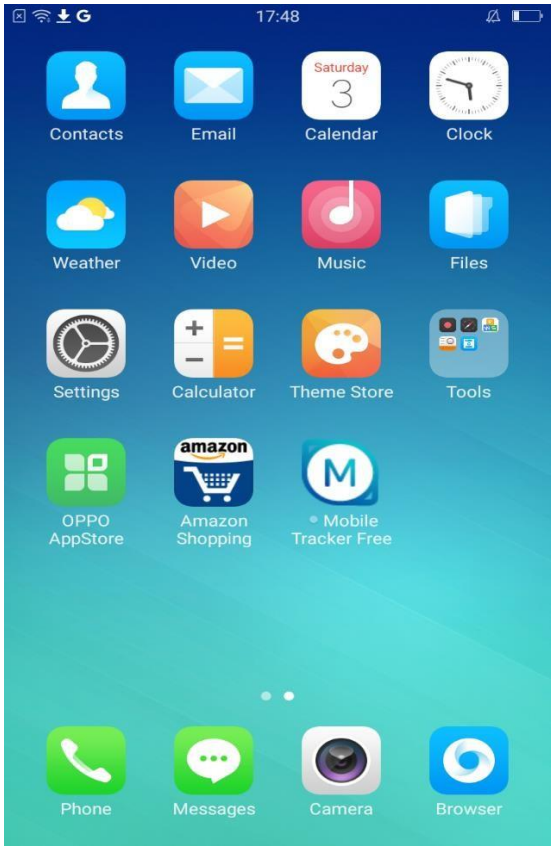
- Disable notifications related to Google Play Protect and the file starts downloading. Install mobile tracker free.



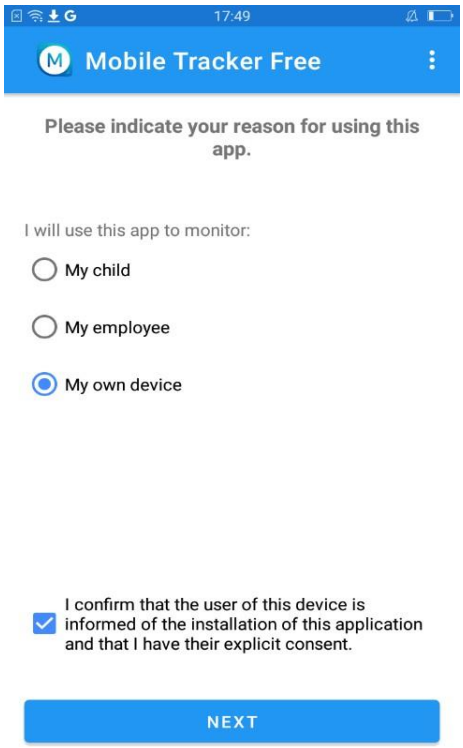
- Now, we will uninstall this app as it was only an agent to install the APK file in the victim machine.

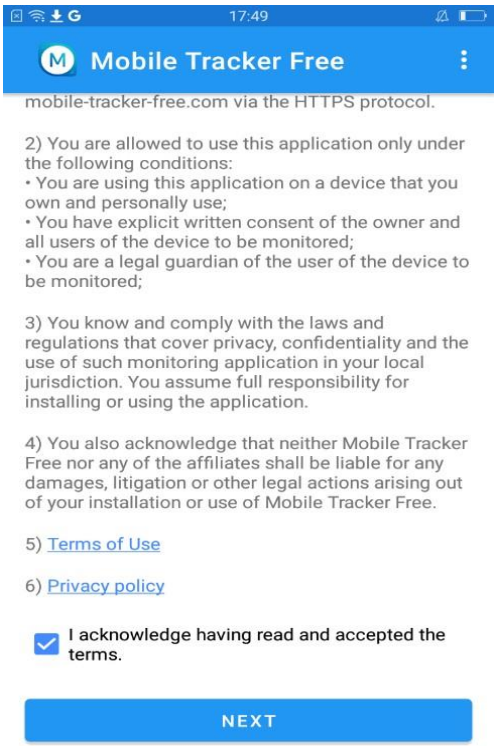


- Here we can see Mobile Tracker Free app on our device's home screen.

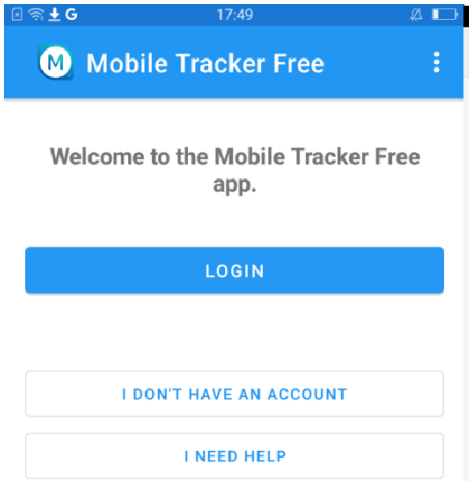


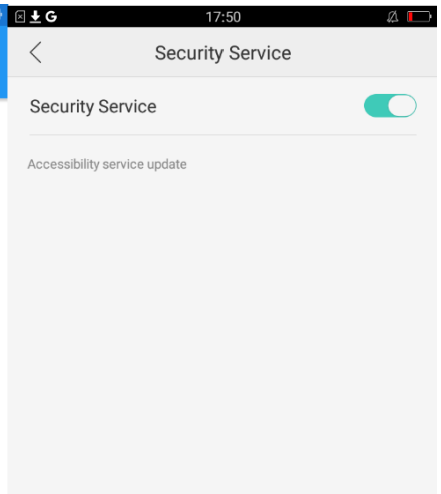
- Now, open this application and click on **My own device** and **next.** Accept all the terms and next.



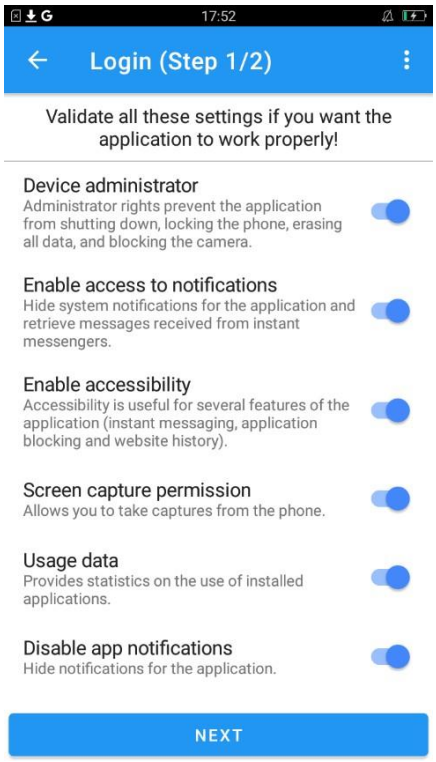


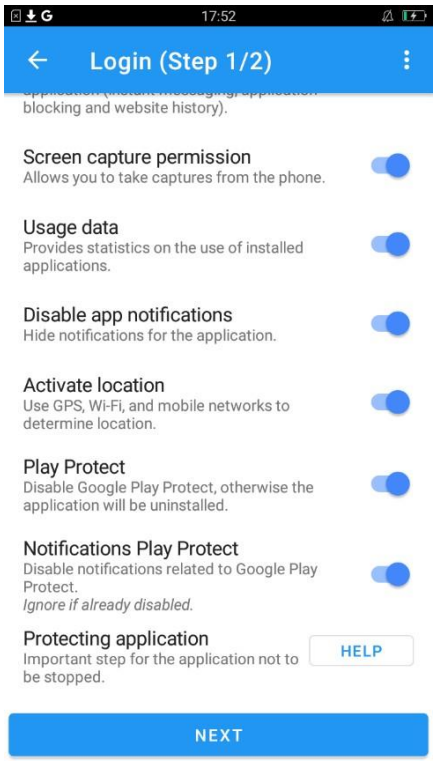
- Login using your email id and password.



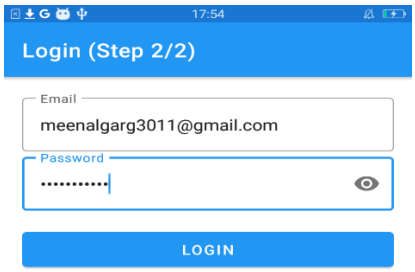


- Turn on the security service and proceed for enabling all the permissions like access to device administrator, screen capture permission, usage data, activate location, access to microphone, media, files, camera, etc.
- Click on **next.**

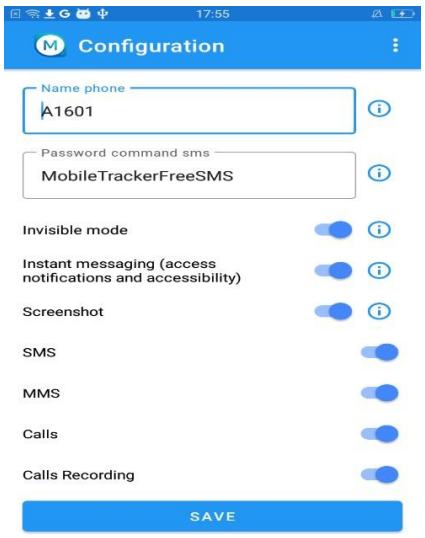


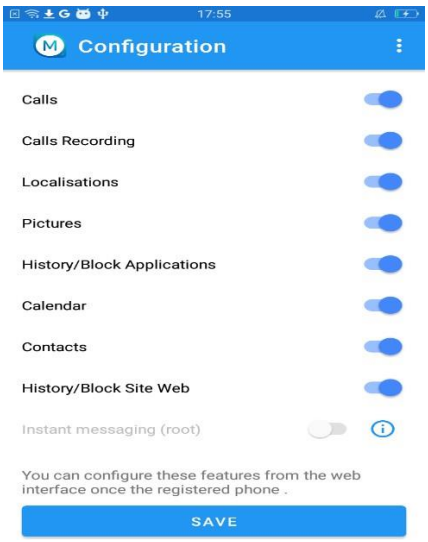


- Login once again.

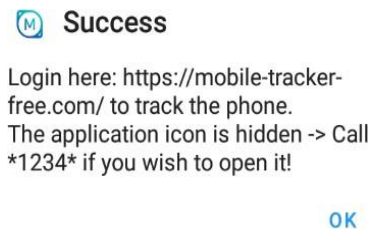


- Now, we can see the Name phone as **A1601** and enable everything. Click on **save.**

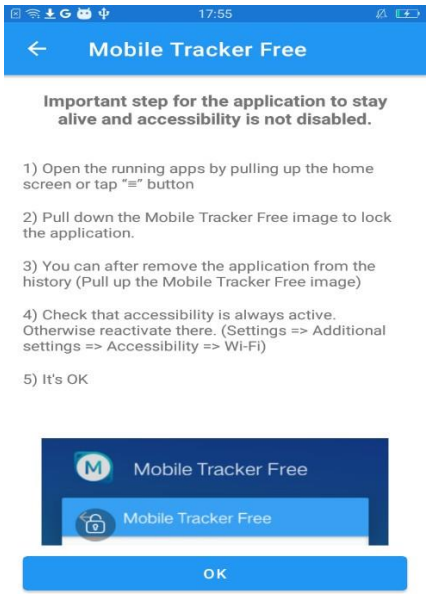




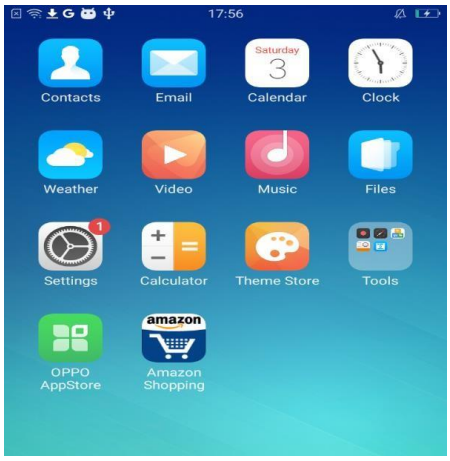
- A success message will be shown.

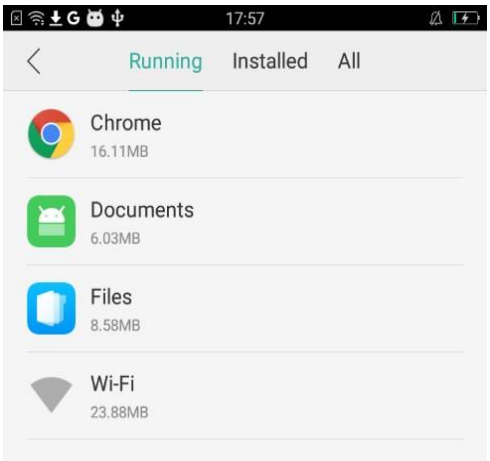


- Click on OK.

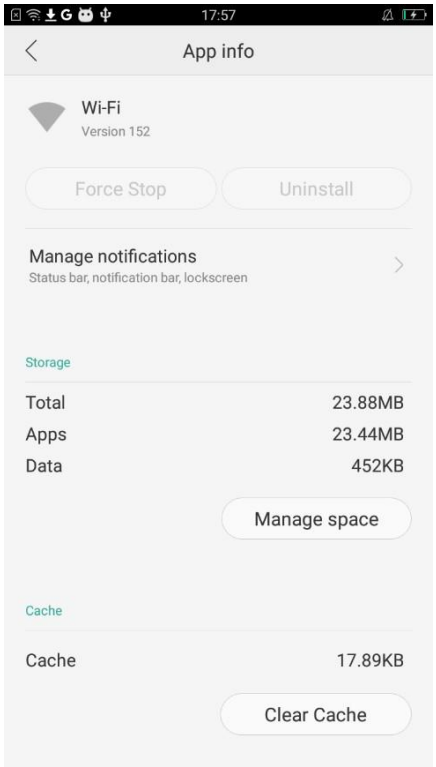


- Here, we are done with installing and enabling part.
- Now the app will get deleted automatically from the phone and the file name will be changed to Wi-Fi.
- The user cannot uninstall it even he/she finds it working in the background.

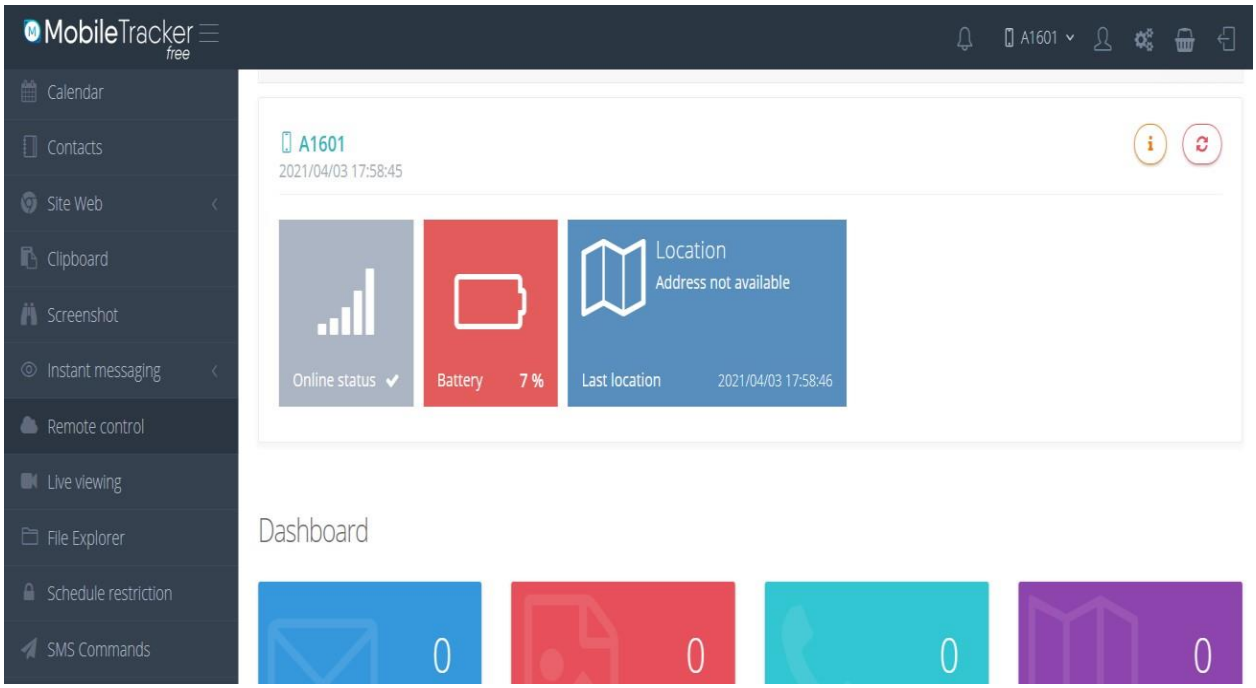




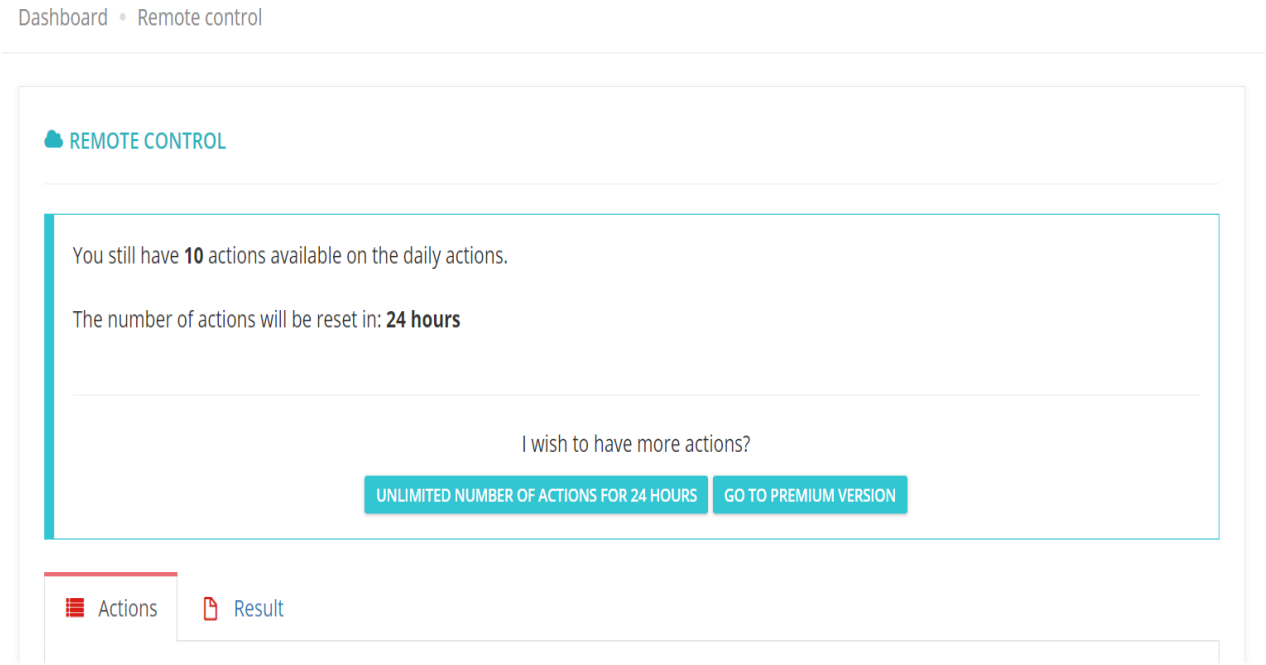
- No uninstalling option is available.



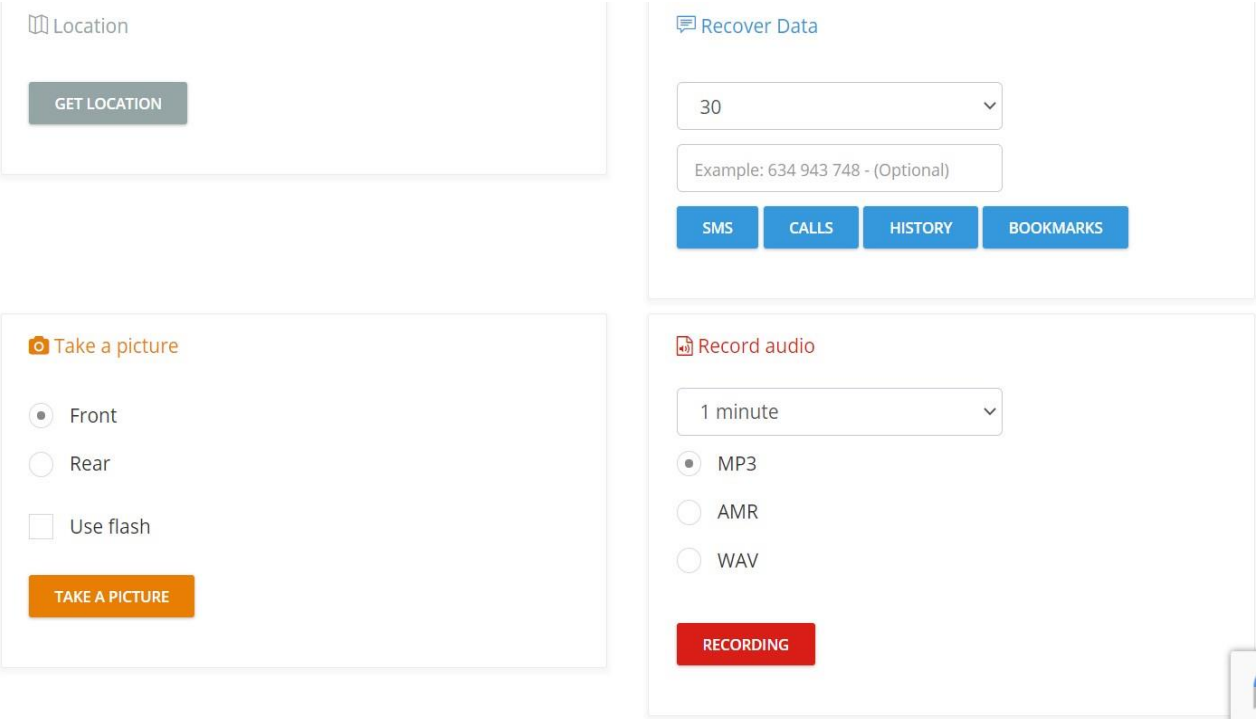
- Coming back to our PC, let’s refresh the site.
- We can see the device’s name being shown as A1601, battery percentage being 7%. We can also check the device’s location.
- From the left hand side, we can access the whole device.
- Let’s start with taking the remote control.



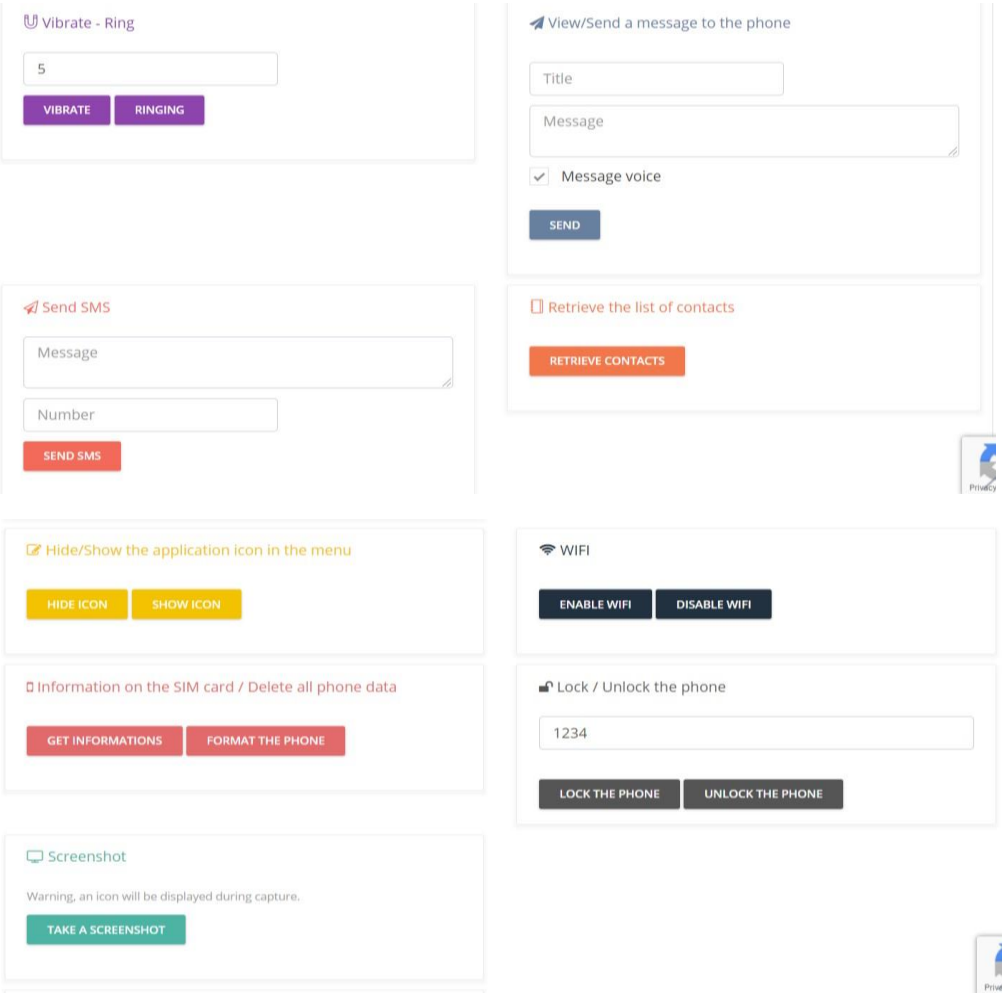
- As we have taken the free demo version, we can perform upto 10 actions.



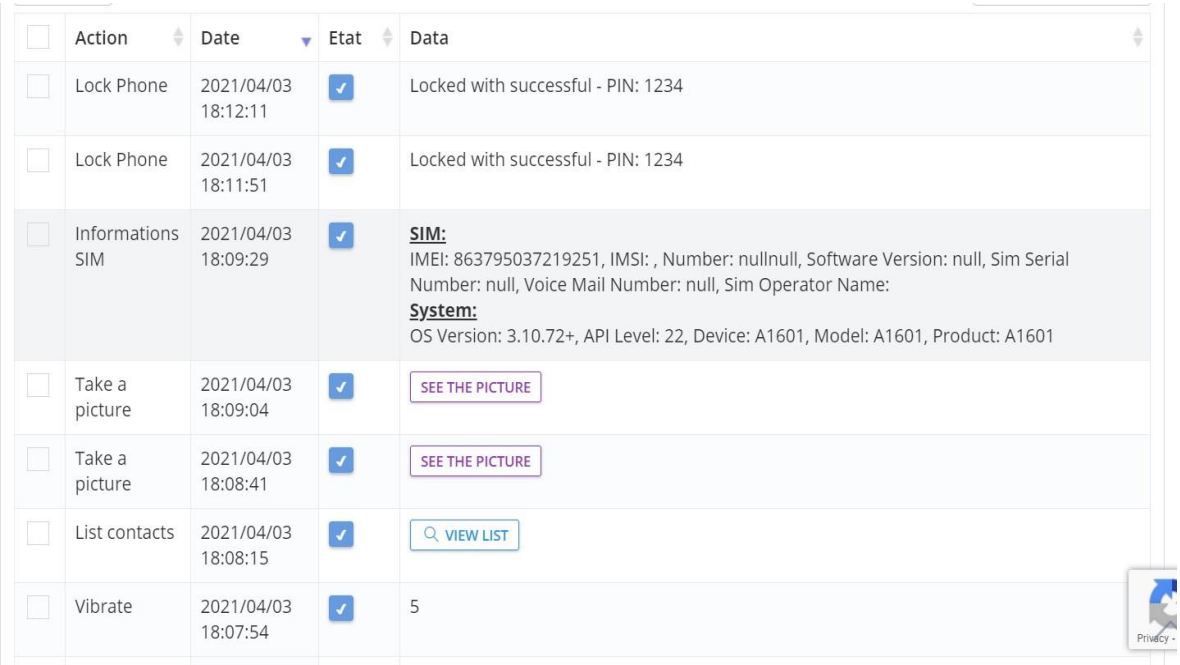
- We can access the location, recover data, click pictures, record audio/video, make the device ring/vibrate, send messages or make a call etc. without the knowing of the user.



- We can perform many more functions.

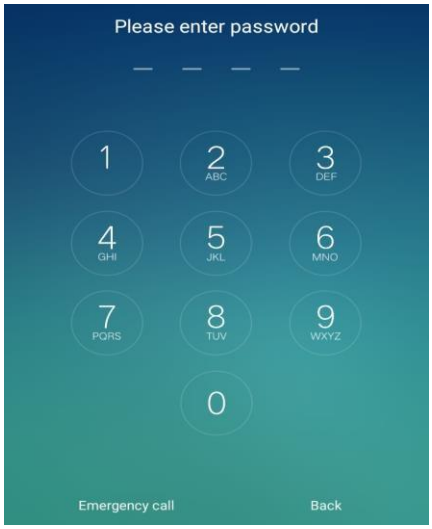


- After performing all the actions, we can check the results in the result section.

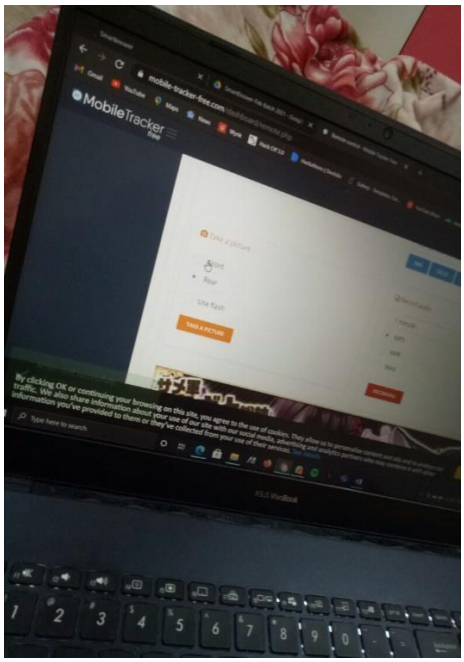


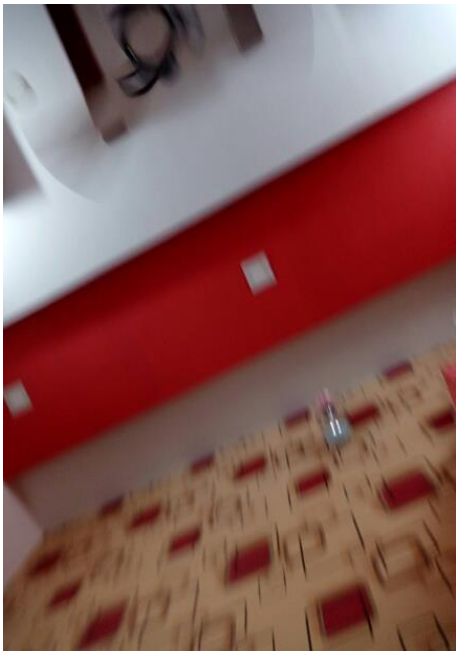
Action	Date	Etat	Data
Lock Phone	2021/04/03 18:12:11	✓	Locked with successful - PIN: 1234
Lock Phone	2021/04/03 18:11:51	✓	Locked with successful - PIN: 1234
Informations SIM	2021/04/03 18:09:29	✓	**SIM:** IMEI: 863795037219251, IMSI: , Number: nullnull, Software Version: null, Sim Serial Number: null, Voice Mail Number: null, Sim Operator Name: **System:** OS Version: 3.10.72+, API Level: 22, Device: A1601, Model: A1601, Product: A1601
Take a picture	2021/04/03 18:09:04	✓	SEE THE PICTURE
Take a picture	2021/04/03 18:08:41	✓	SEE THE PICTURE
List contacts	2021/04/03 18:08:15	✓	VIEW LIST
Vibrate	2021/04/03 18:07:54	✓	5

- We locked the device with the password: 1234.



- We took a rear and front picture.
- Rear picture. Front picture.



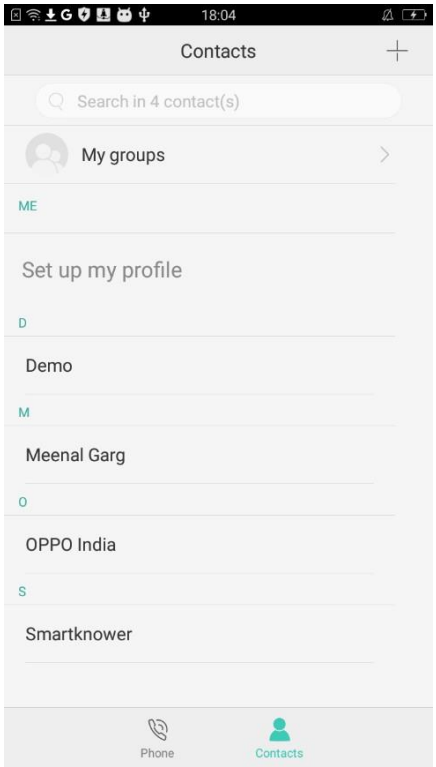


- Accessing the contacts.

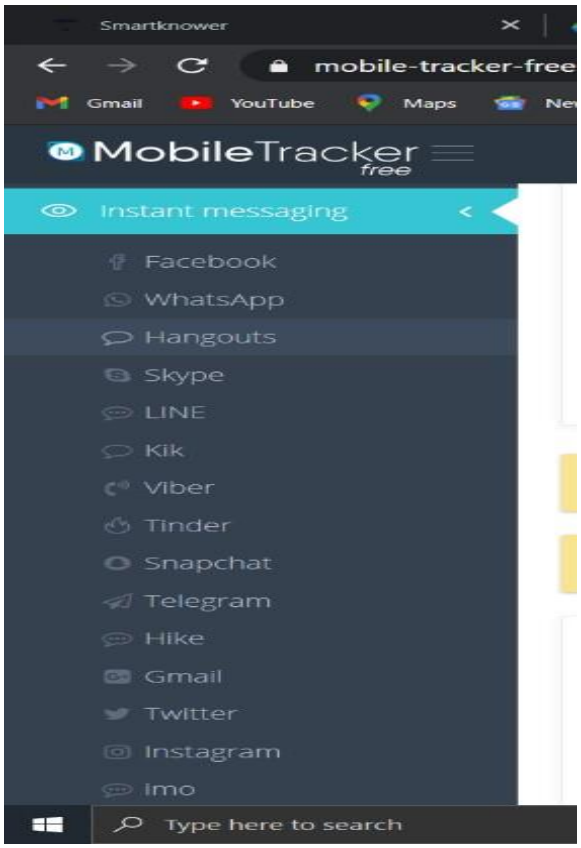
5 Search

ID	Name	Number
0	OPPO India	18001032777
1	Meenal Garg	1234567890
2	Demo	9512365478
3	Smartknower	9632587410

- Device screenshot of contacts to double check the information.



- We can also access all the applications and their insights.



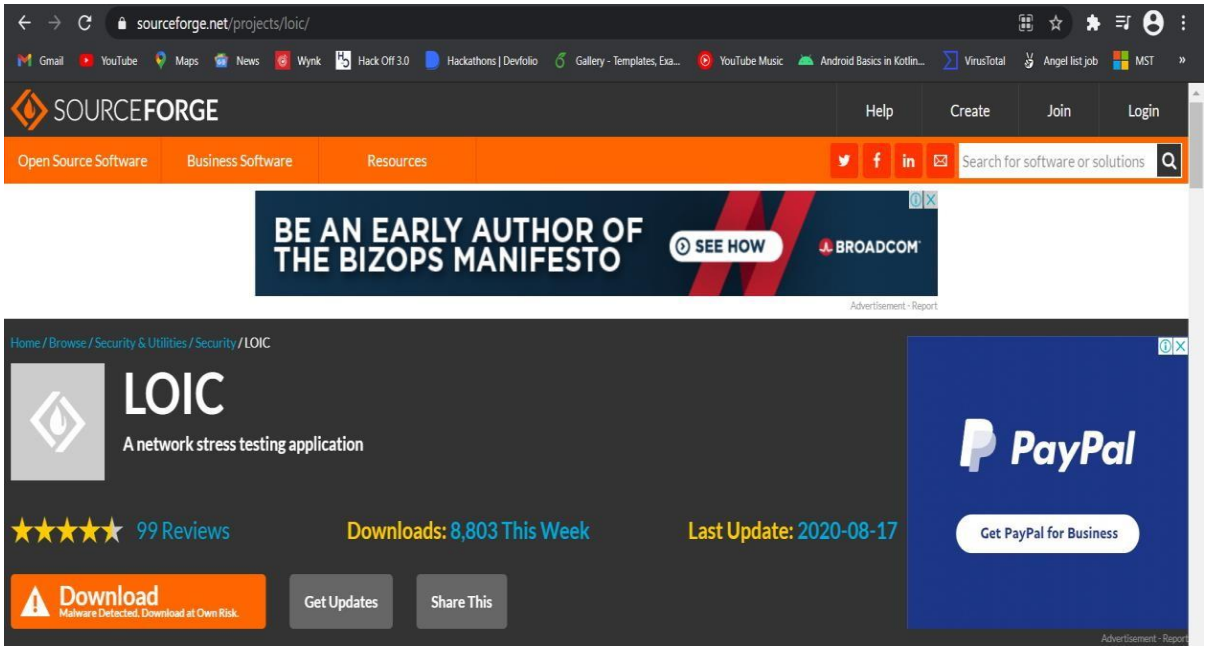
- Here, we are done with hacking the mobile device. Thank you!

DOS Attack

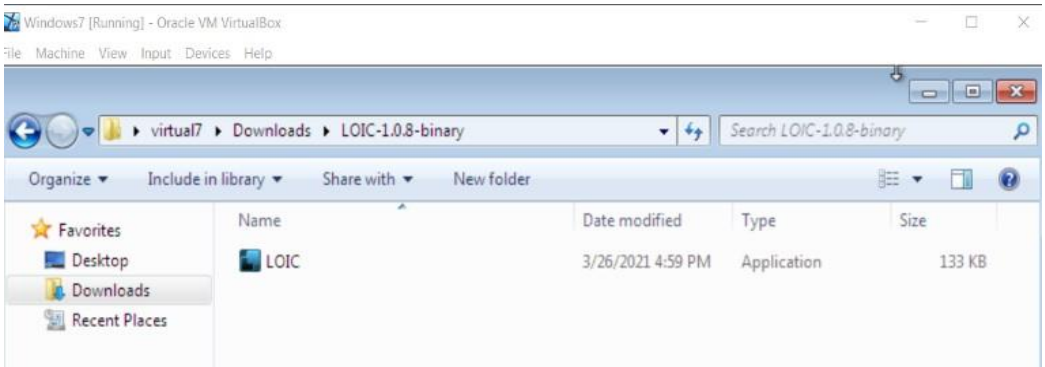
4. Website Penetration Testing

Perform a DOS attack on windows 7 virtual machine using the LOIC tool and check the performance.

- Performing DOS Attack on Windows 7 using LOIC Tool (Low orbit ion cannon).
- Our **Victim machine is Windows 7**.
- Firstly visit https://sourceforge.net/projects/loic/ site and download LOIC tool in our hacker machine.
- LOIC is a dangerous tool so be careful while installing it.

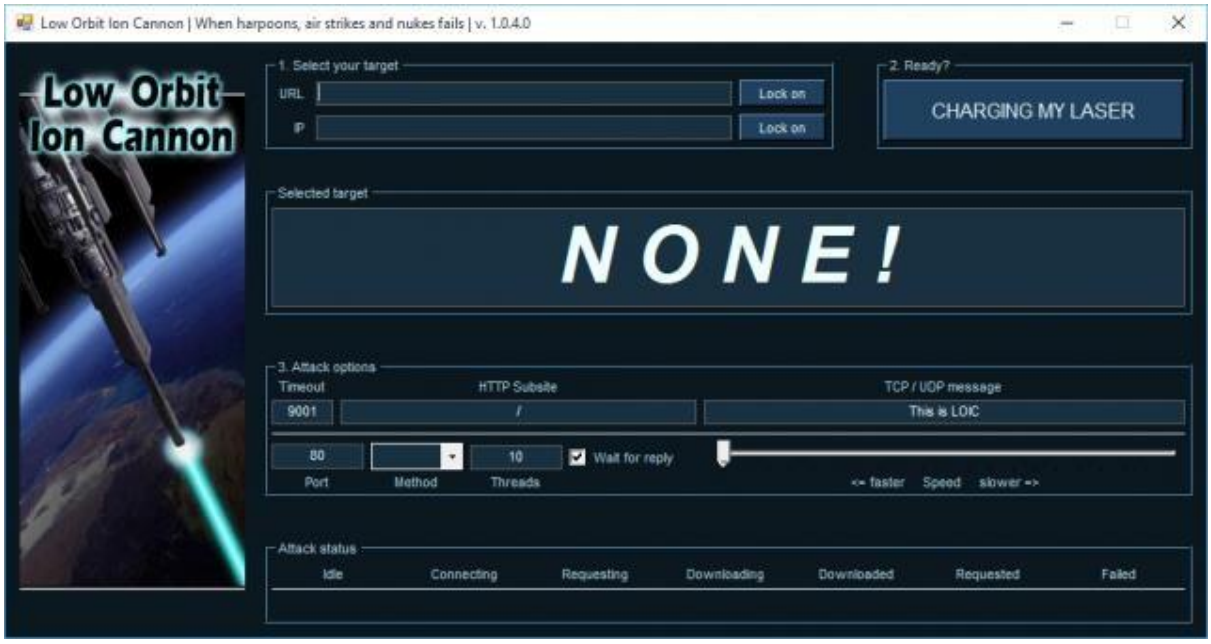


- Open in folder and extract files.

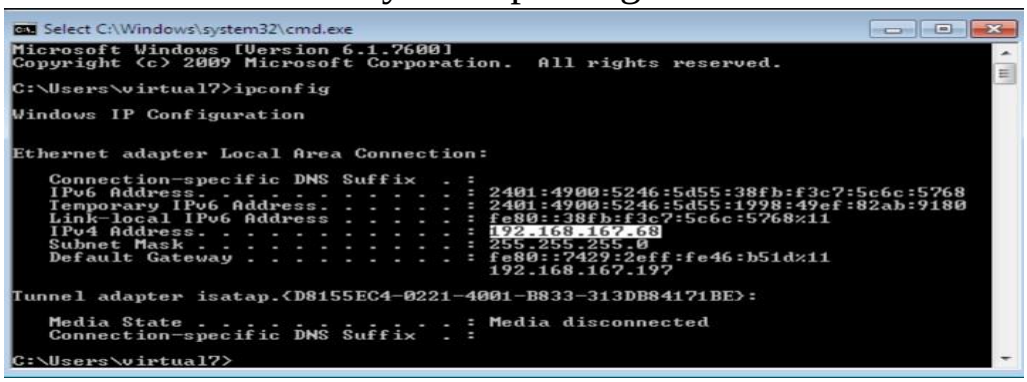


- Run the application.

- Main window of LOIC tool is shown below.
- Now, we have installed LOIC tool in our hacker machine.

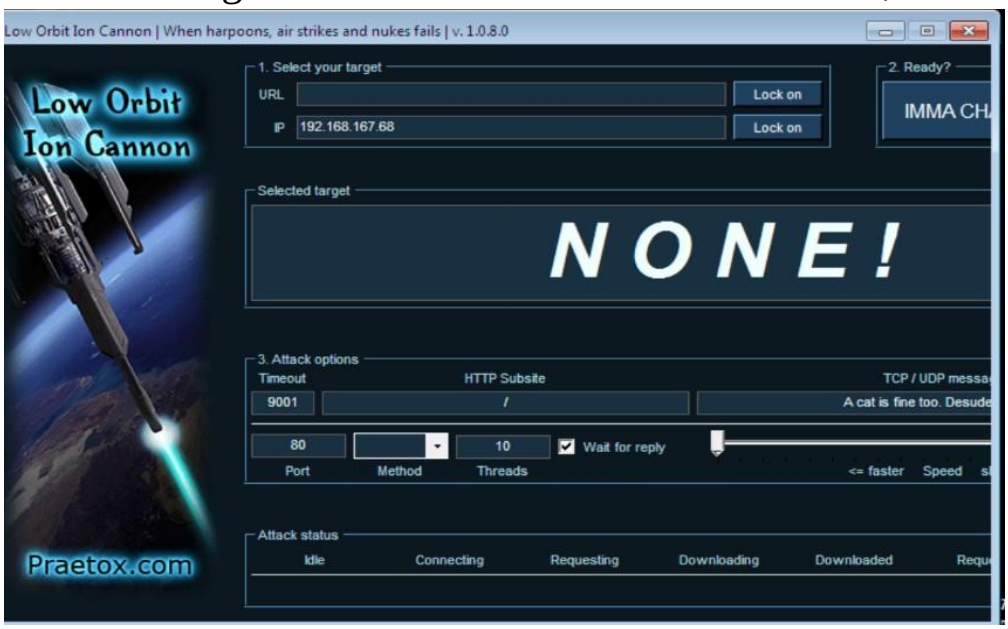


- To perform DOS attack using LOIC, we need IP address, open port number and protocol of victim machine i.e. Windows 7.
- Open command prompt in victim machine and write command for IP address. Syntax: ipconfig

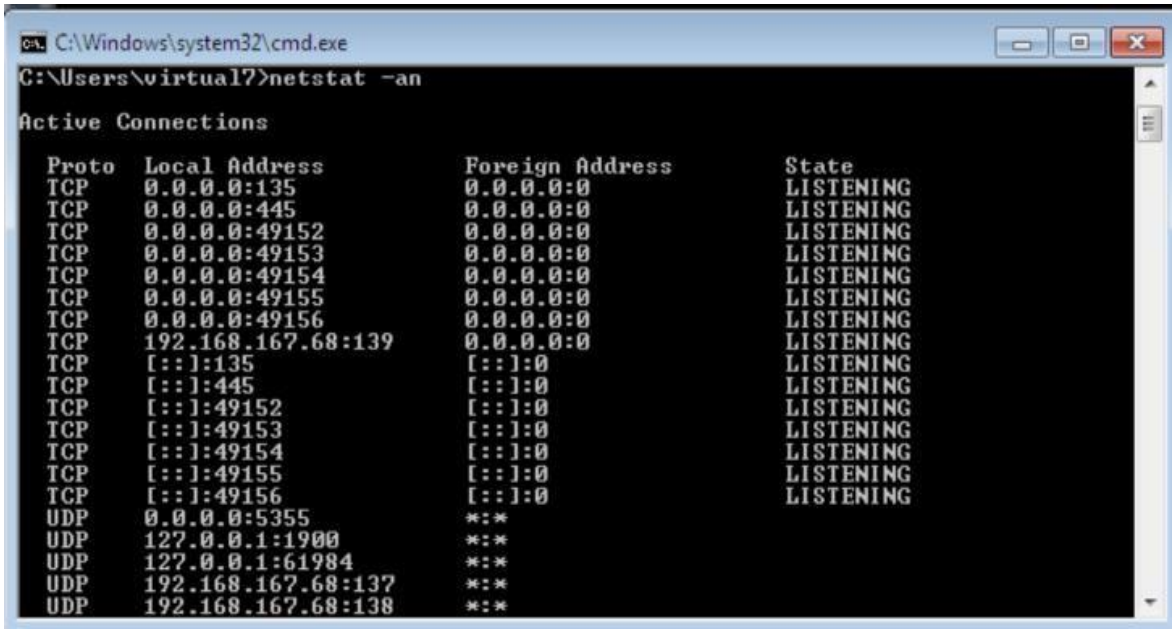


- IP address of victim machine is: 192.168.167.68

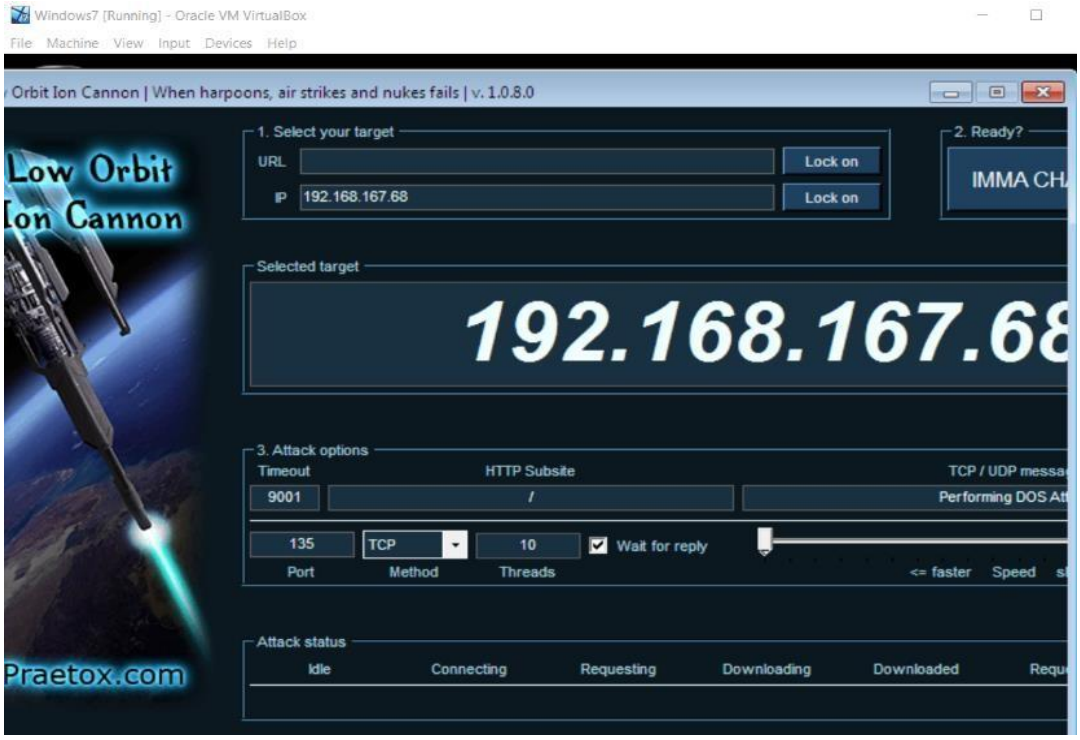
- Locking this IP in our tool on hacker machine, let's continue.



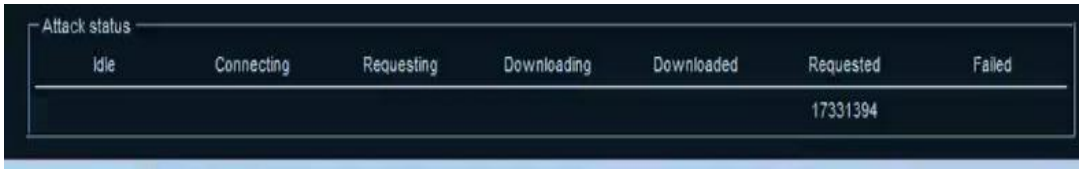
- Now for open ports and protocol of victim machine, open command prompt in victim machine and write command for information regarding ports. Syntax: netstat -an



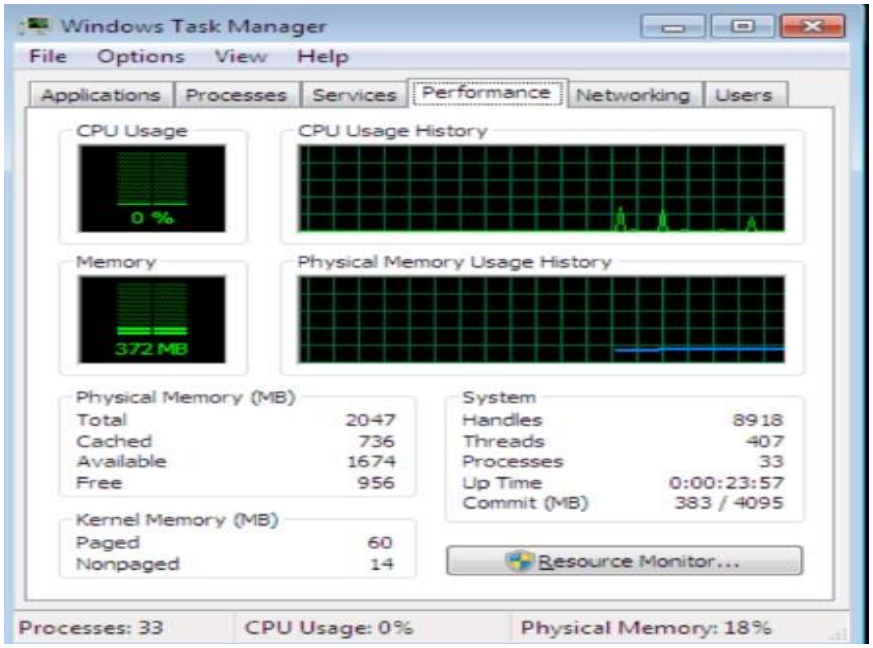
- Here, quite a few number of ports are open but we are going to take port number 135 with TCP protocol.
- Now, coming back to our hacker machine we will specify the port number as 135, protocol used as TCP, message (to be stored in firewall) as "Performing DOS Attack" and click on START.



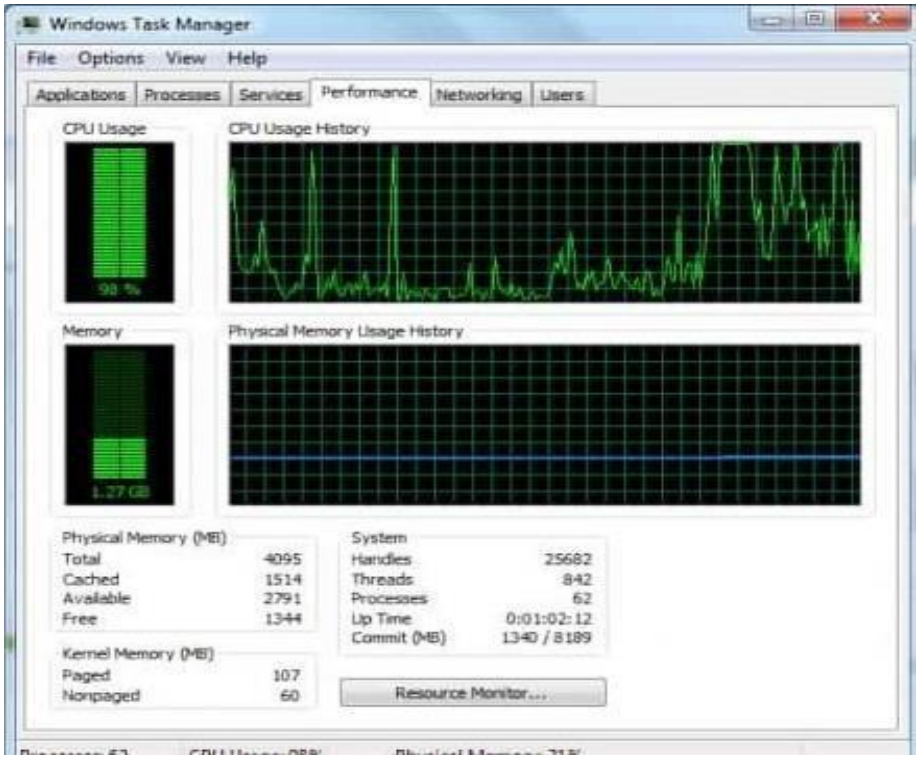
- Do check the requested status in the right bottom corner of the tool.



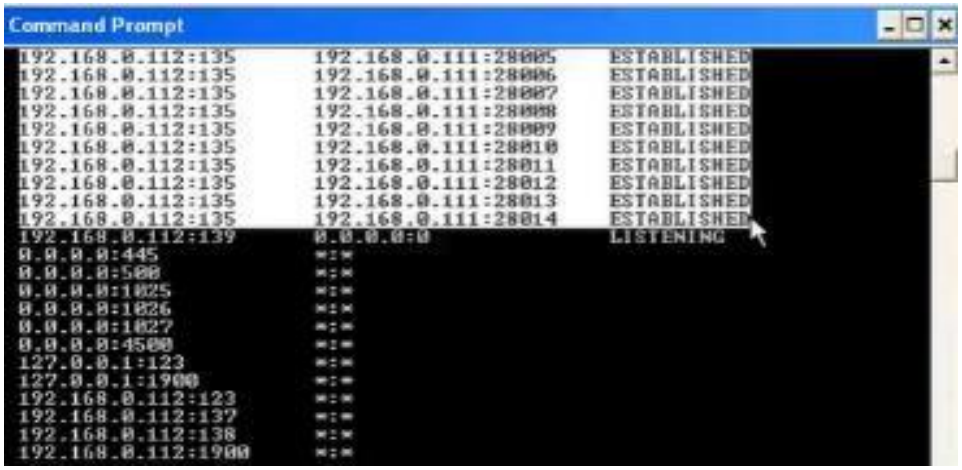
- Open Task Manager in victim machine and check it's status. It would look like this having no loads over CPU usage.



- Kindly note the changes in the CPU usage after starting the attack.
- Here, CPU usage shot up to 98% approx. slowing down the system creating denial of service. The graph has sharp points indicating the on/off of the attack.



- Again checking the port status in command prompt, it will show us the port status being changed to ESTABHLISHED from LISTENING. Also hacker's IP address will show.



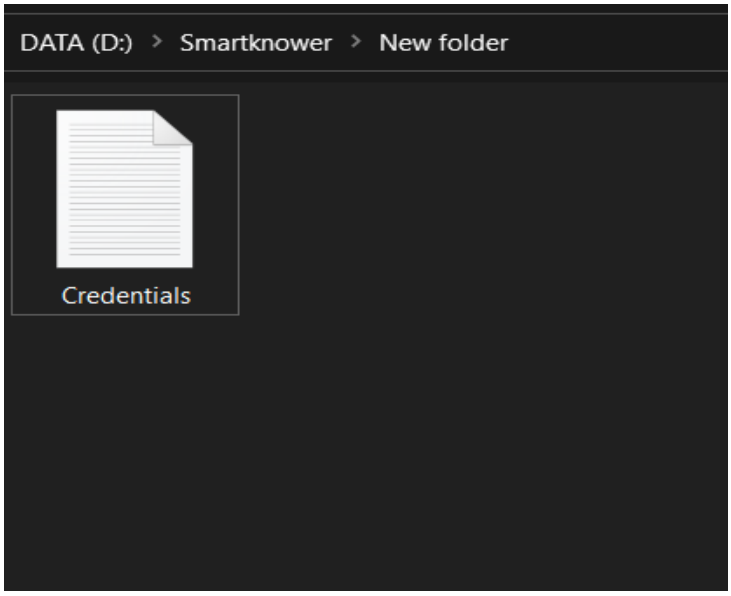
- Click on stop to stop the attack.
- Here, we are done with our DOS attack.

Steganography

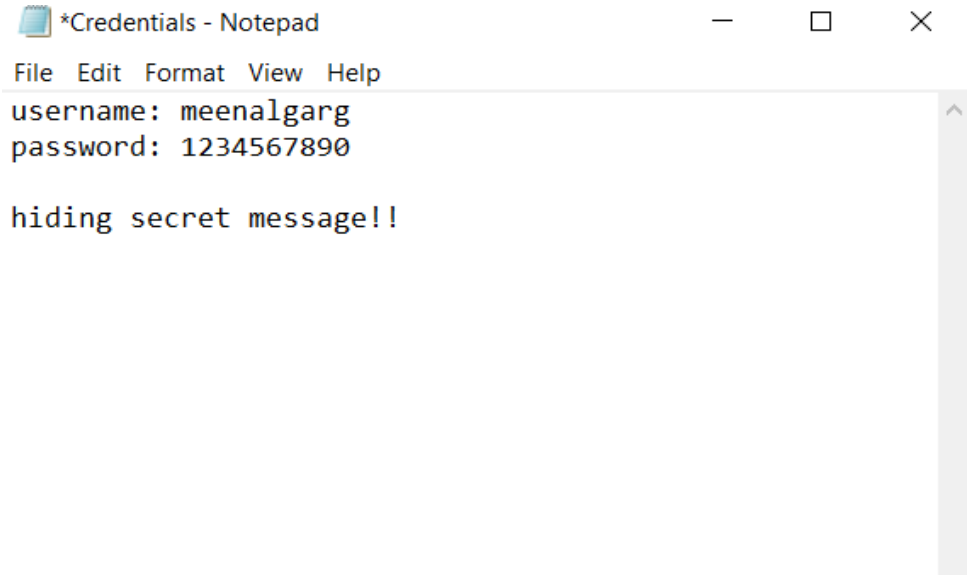
5. Data Encryption, Decryption, and Hiding of Secret Messages.

Hide the secret text file in the image using command prompts and SNOW tool.

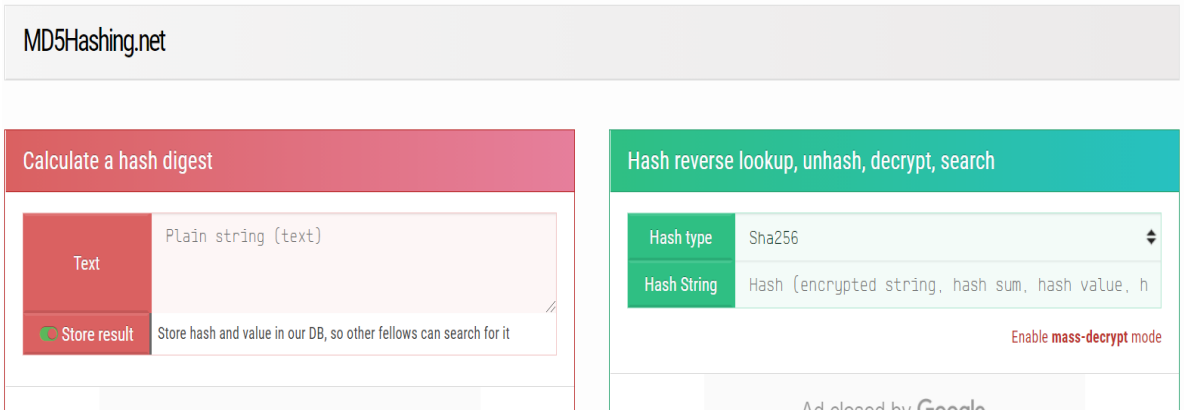
- Encrypting a text file with an image file.
- First, we will create a text file named **Credentials**.



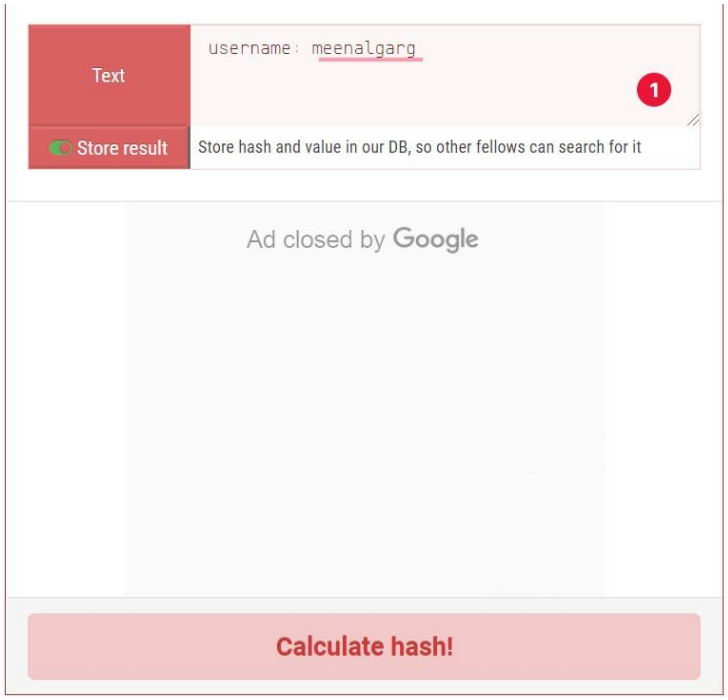
- Let's write our credentials in the file as an example.

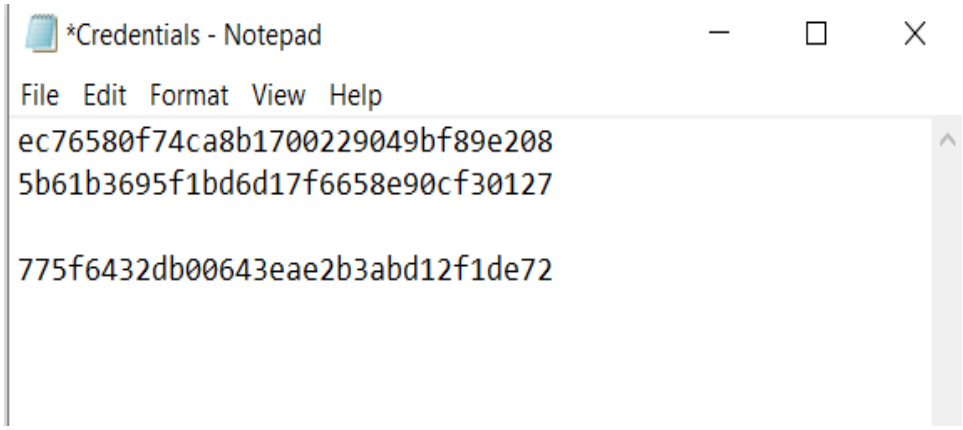


- Before saving, let's encrypt the data using MD5 algorithm from https://md5hashing.net/ site.



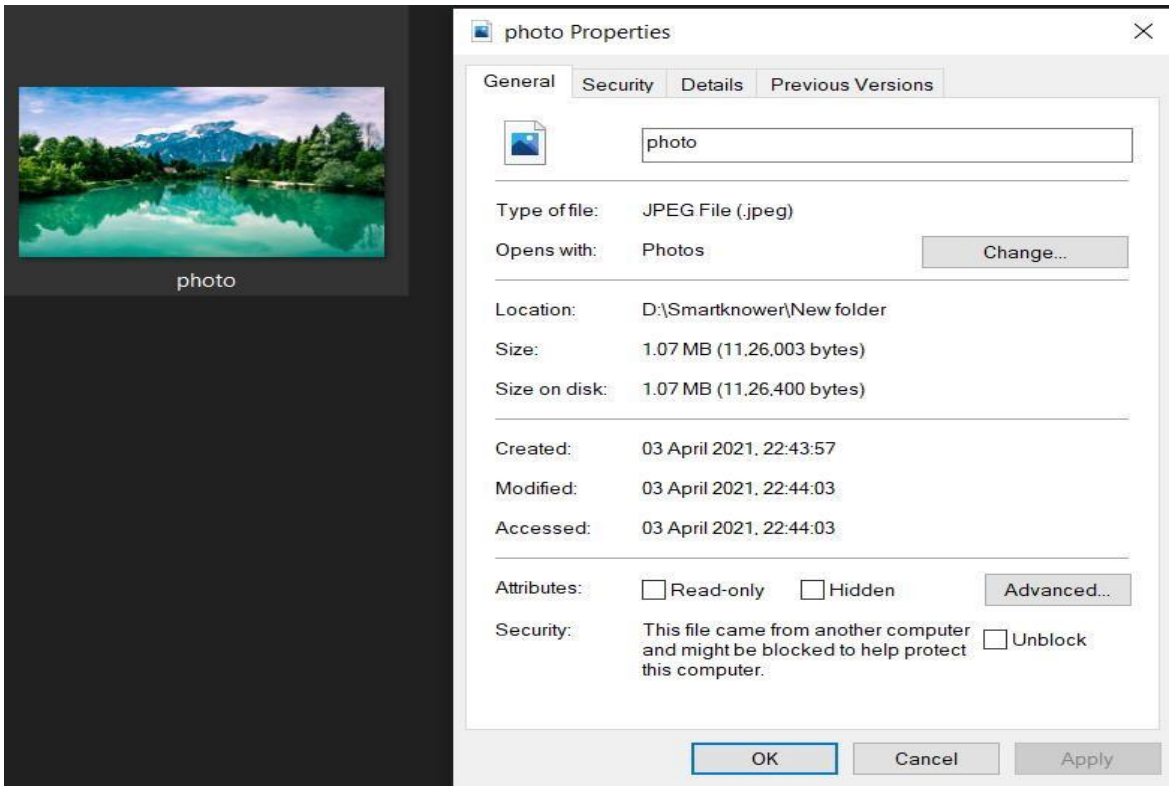
- Creating hashes of all the credential content written, we will save it.



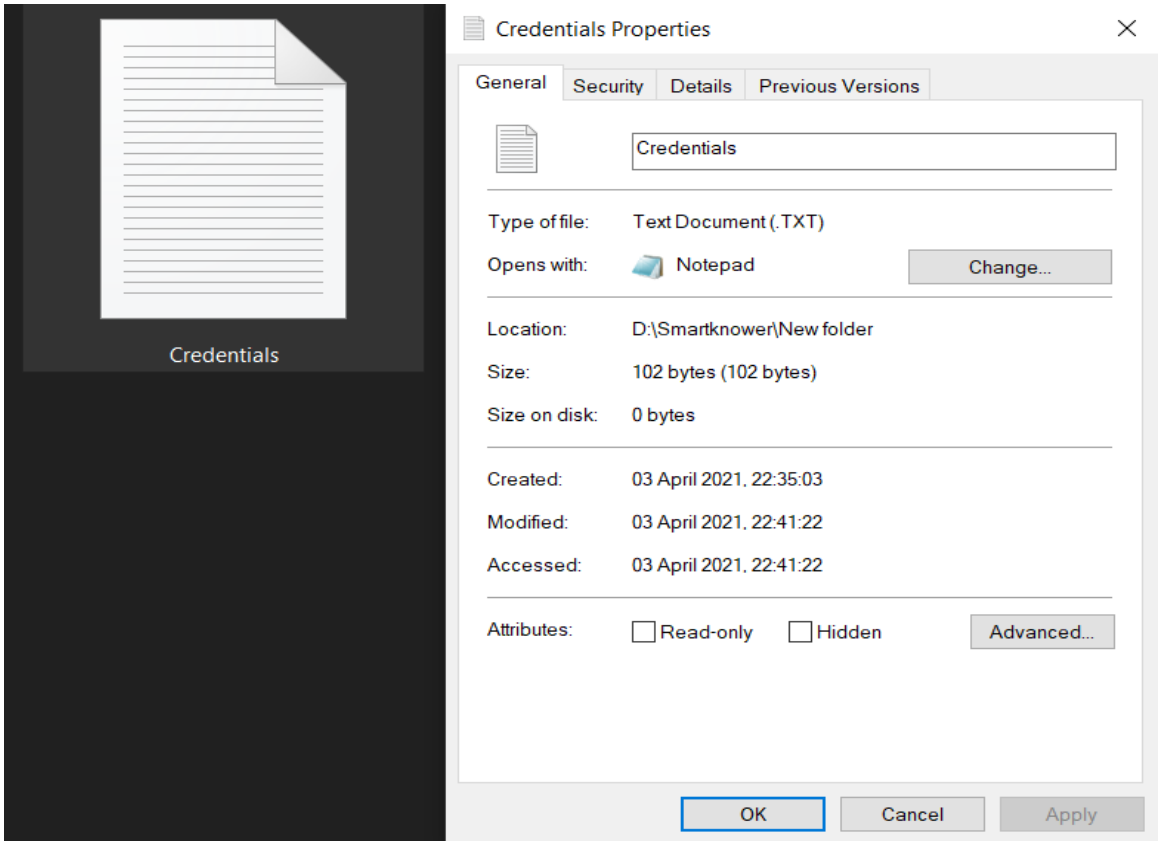


- Save our encrypted secret message in the text file.

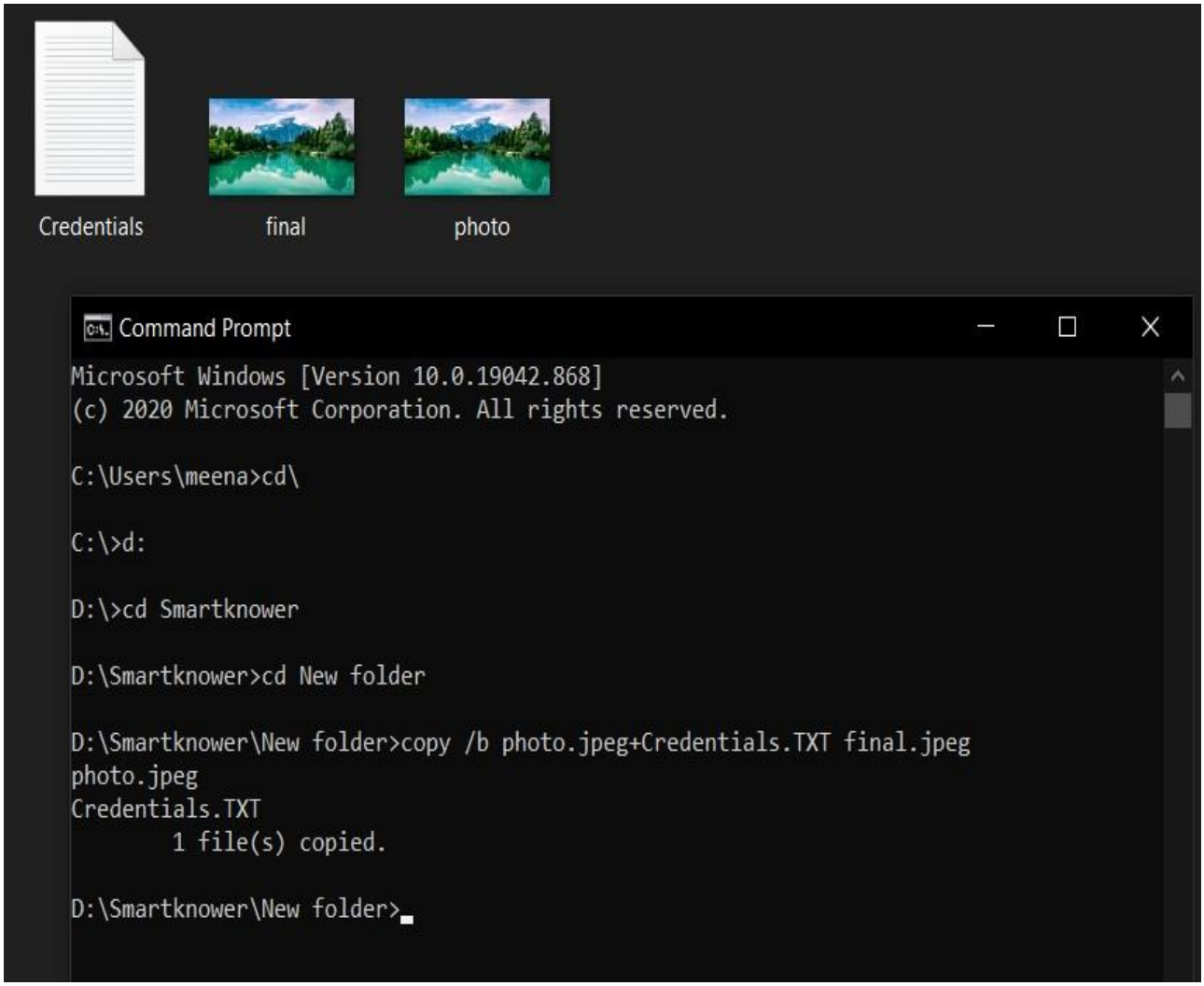
- Now, let's take an image file named **photo** with an extension **.jpeg** and size being 1.07 MB.



- Our text file has **.TXT** extension and size being 102 bytes.

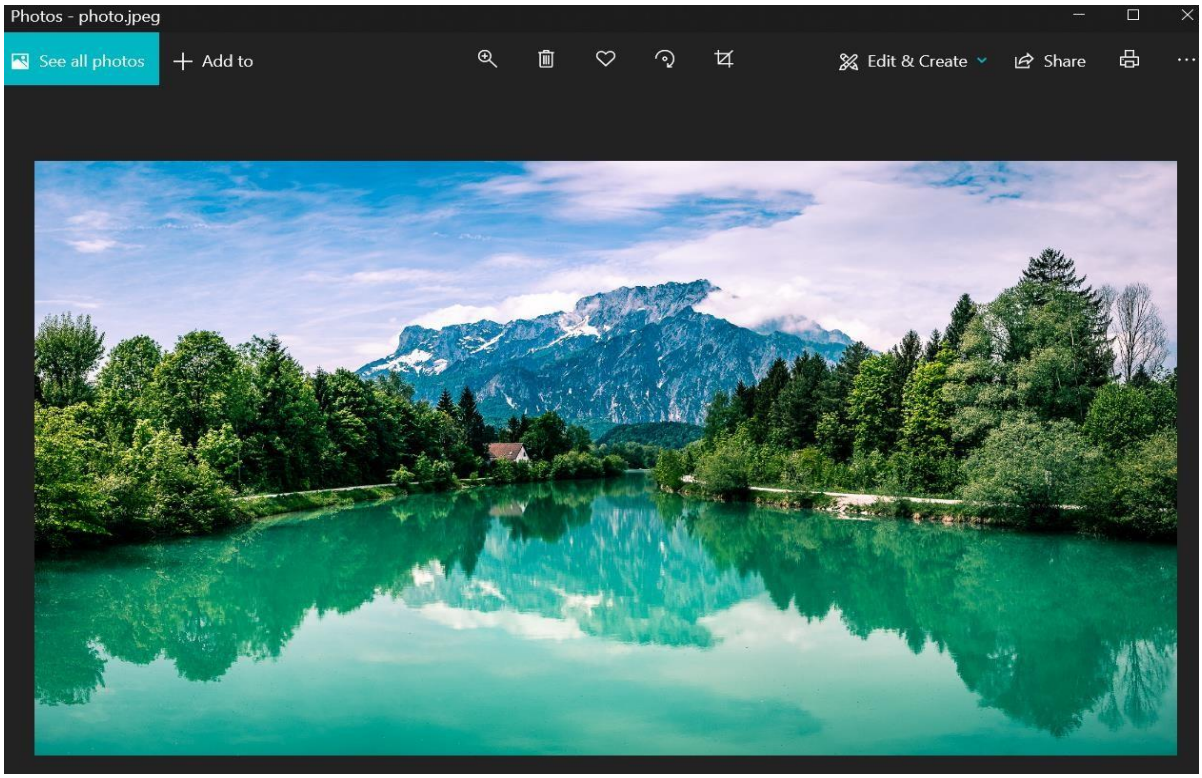


- We will use command prompt to bind our secret file with the image file.
- First, we will open our folder where both the files are stored.
- Location – D:\Smartknower\New folder

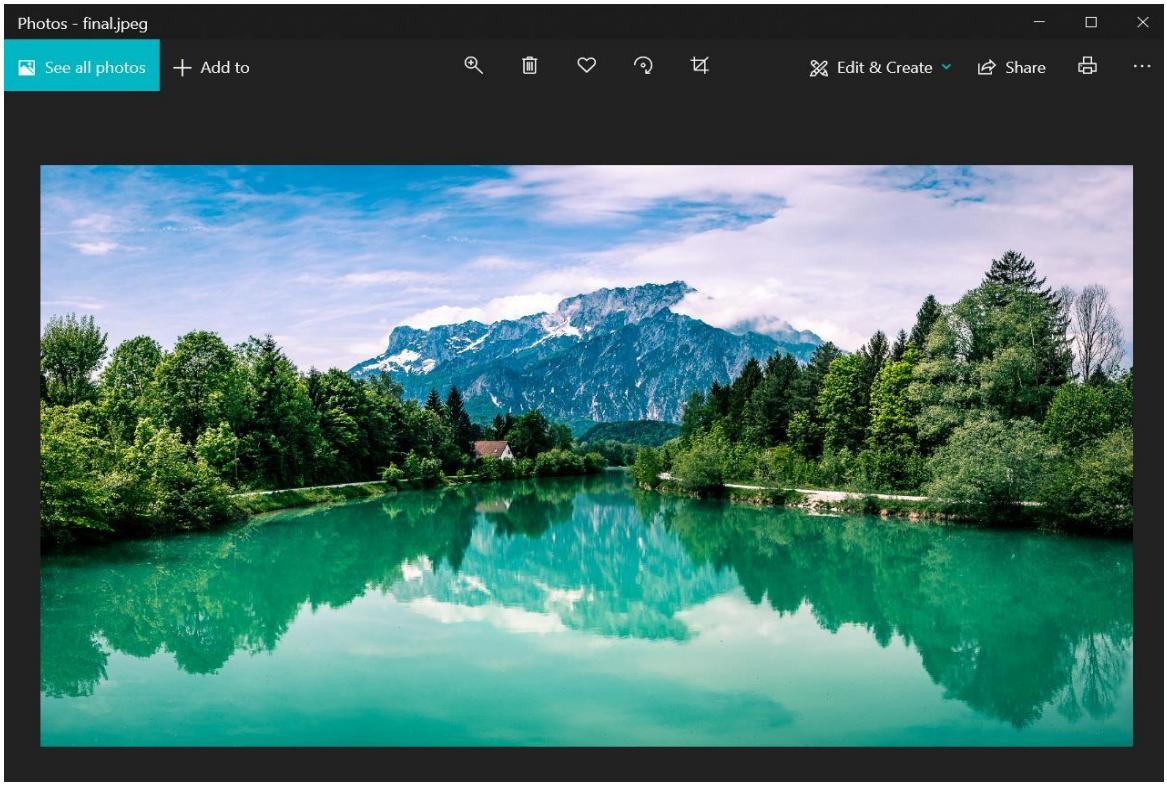


- To bind the files, we wrote the following command:
  copy /b photo.jpeg+Credentials.TXT final.jpeg
  copy: command syntax
  /b: to bind
  photo.jpeg: name of our image file
  +: to add/bind
  Credentials.TXT: name of our text file
  final.jpeg: name of our binded file
- Running this command will create a binded file named **final.jpeg**.

- No difference can be marked out by at least naked eye in the original and binded file.
- Photo.jpeg



- final.jpeg



- Opening the final.jpeg file in notepad, we will find the encrypted data at the bottom.
- We can decrypt it at the destination by using MD5 decryption.

- **<u>Thank you!</u>**