EH mini project

-Done by

Tharun S.M.

tharuntech9840@gmail.com

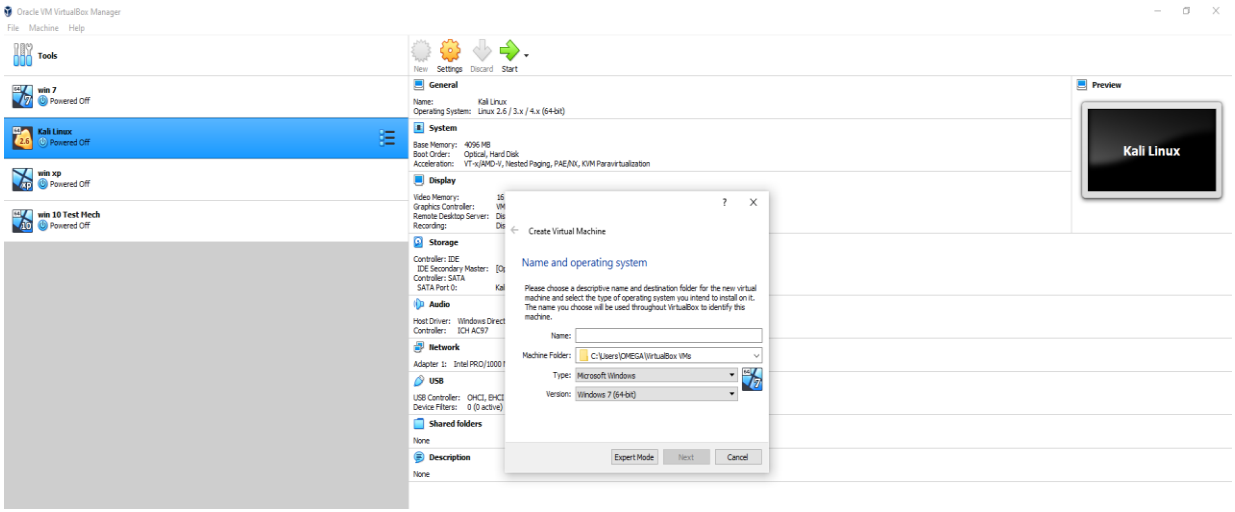
1. Information Gathering on Websites :

- **Create a lab with Oracle Virtual Box or VMware with Kali Linux OS, Windows 7, and Windows XP.**

  a. **First download and install Oracle virtual box from** https://www.virtualbox.org/wiki/Downloads

Click on Windows host and click on download to start Downloading after downloading click on install Oracle virtual Box to start the installation

b. Installing OS in virtual box



Click on the new tab and assign a name to your VM and choose the version in which it should run on

If you are installing windows 7 or windows XP OS

Select Type Windows and

Version windows 7 (64x) or the windows XP (64x)

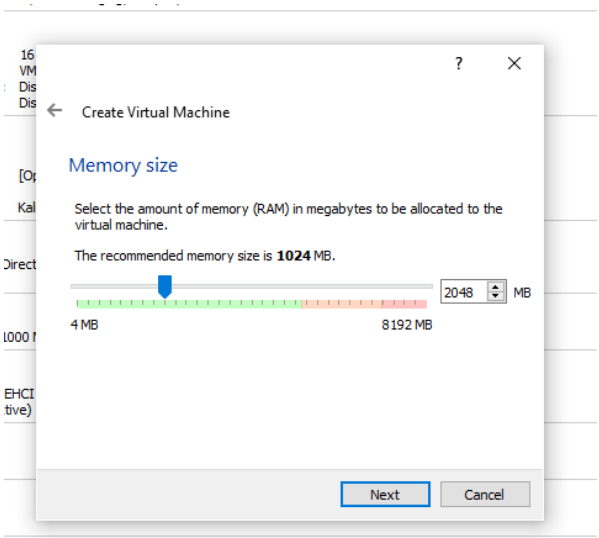
And if you want to install Kali Linus OS

Select Type linux and

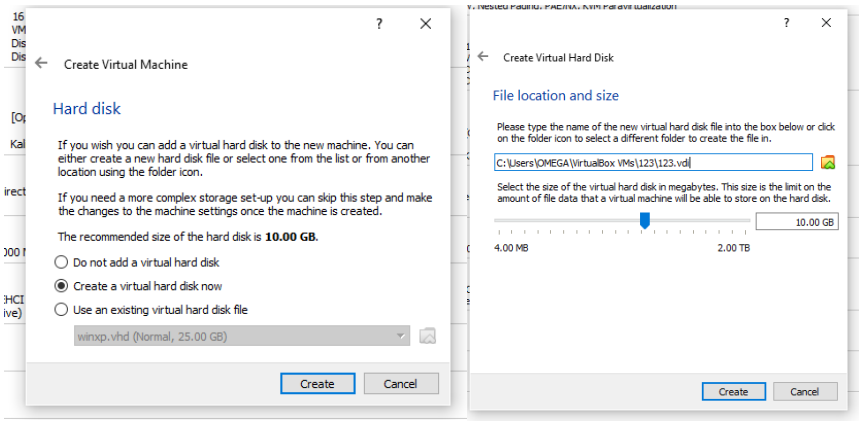
Version Ubuntu (64x)

And click 'Next'

c. Configuring settings for the OS

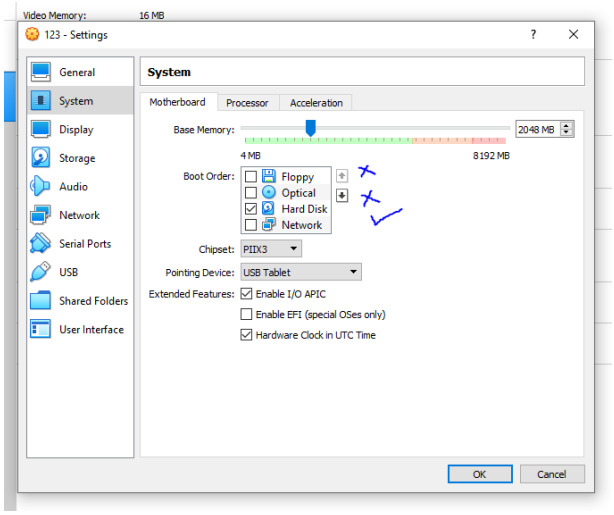


Assign appropriate RAM size for your OS (Win or Kali)



Assign Hard disk partition for your V box it might be a new partition or a pre-existing partition in the disk.
It is always recommended to have a minimum of 25GB or 30GB of storage space for your V box and all the applications in it.
And also choose a location and limit for the storage of your disk

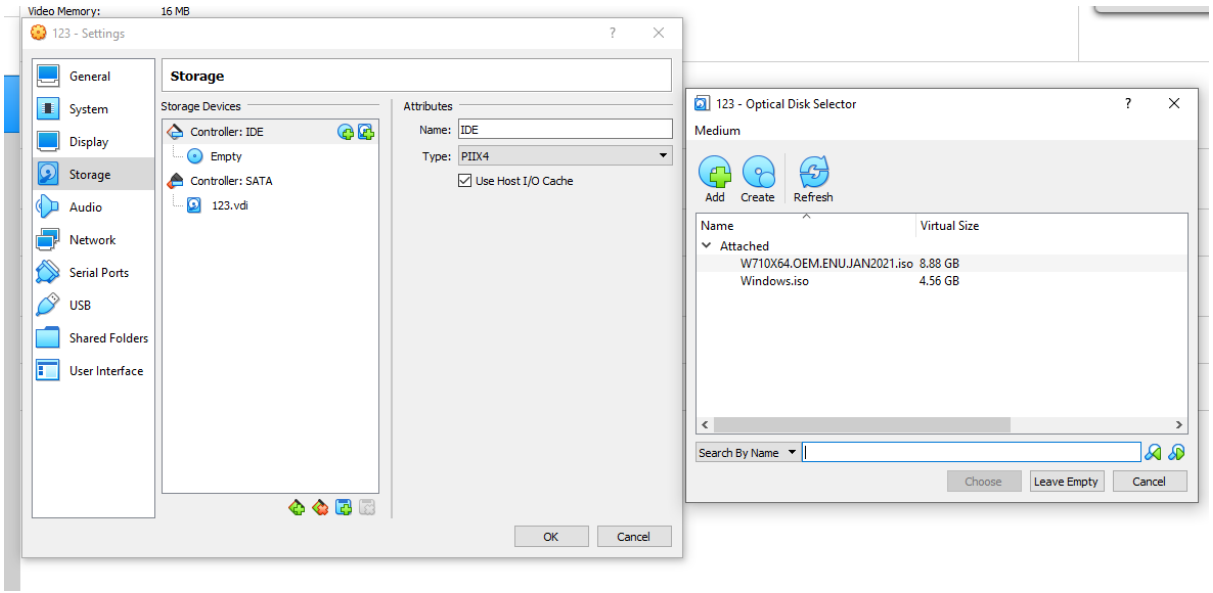
d. Setting up VM



Choose the OS (windows 7, windows XP or Kali Linux)

Click on the setting icon on the top left

Click on system and enable only hard disk in the boot order



Click on storage and add your OS file to your VM

NOW your VM is ready just click on the start icon to start your a specific Virtual Box OS

(VM can handle multiple OS at the same time , Because it only uses very less resources of your PC)

▪ **Gather information about Instagram (website).**

We have taken Instagram as our target Website to gather information

a. **Gathering information on the website using cmd/terminal**

Use command ping www.instagram.com to if the website is live or not

```
Command Prompt
Microsoft Windows [Version 10.0.19041.867]
(c) 2020 Microsoft Corporation. All rights reserved.

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

Pinging z-p42-instagram.c10r.facebook.com [31.13.79.174] with 32 bytes of data:
Reply from 31.13.79.174: bytes=32 time=26ms TTL=58
Reply from 31.13.79.174: bytes=32 time=25ms TTL=58
Reply from 31.13.79.174: bytes=32 time=26ms TTL=58
Reply from 31.13.79.174: bytes=32 time=26ms TTL=58

Ping statistics for 31.13.79.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 26ms, Average = 25ms

C:\Users\OMEGA>
```

From this we have found that the host website is responsive.

Use nslookup https://www.instagram.com/

To get the DNS or the IP of the Website

```
C:\Users\OMEGA>nslookup www.instagram.com
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    z-p42-instagram.c10r.facebook.com
Addresses:  2a03:2880:f22f:e5:face:b00c:0:4420
          31.13.79.174
Aliases:  www.instagram.com


C:\Users\OMEGA>
```

Use tracert www.instagram.com / traceroute www.instagram.com

To find the Nodes to which the packet travel to as the final destination

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

Tracing route to z-p42-instagram.c10r.facebook.com [157.240.16.174]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     5 ms     5 ms     5 ms  125.17.36.41
  3    25 ms    24 ms    24 ms  182.79.141.37
  4     *        *        *     Request timed out.
  5    28 ms    28 ms    27 ms  182.79.179.100
  6    24 ms    25 ms    24 ms  116.119.44.117
  7    29 ms    30 ms    29 ms  116.119.52.42
  8    26 ms    24 ms    25 ms  ae18.pr03.bom1.tfbnw.net [157.240.67.48]
  9    26 ms    28 ms    29 ms  po103.psw02.bom1.tfbnw.net [157.240.53.69]
 10    26 ms    26 ms    25 ms  157.240.38.135
 11    24 ms    23 ms    24 ms  instagram-p42-shv-01-bom1.fbcdn.net [157.240.16.174]

Trace complete.
```

This gives us all the information about the route and the ip address to which the connection is redirected to , To reach its final destination.

b. Gathering information on the website using Online FootPrinting

Gathering website Details using
https://whois.domaintools.com/

Whois Record for InstaGram.com

− Domain Profile

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	6,146 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 36,690 domains) NS-2016.AWSDNS-60.CO.UK (has 434 domains) NS-384.AWSDNS-48.COM (has 6,503 domains) NS-868.AWSDNS-44.NET (has 239 domains)
Tech Contact	REDACTED FOR PRIVACY (DT) Instagram LLC 1601 Willow Rd, Menlo Park, CA, 94025, us (p) REDACTED FOR PRIVACY (DT)
IP Address	157.240.3.174 - 12 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	390 changes on 390 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 2021-04-02)

```
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)
Registry Billing ID:
Billing Name:
Billing Organization:
Billing Street:
Billing City:
Billing State/Province:
Billing Postal Code:
Billing Country:
Billing Phone:
Billing Phone Ext:
Billing Fax:
Billing Fax Ext:
Billing Email:
Nameservers:
        ns-1349.awsdns-40.org
        ns-2016.awsdns-60.co.uk
        ns-384.awsdns-48.com
        ns-868.awsdns-44.net
DNSSEC: unsigned
```

Gathering information using

https://www.netcraft.com/internet-data-mining/

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Report Fraud Request Trial

Site report for https://www.instagram.com

▸ Look up another site?

Share:

Background

Site title	Login • Instagram	Date first seen	June 2014
Site rank	11	Netcraft Risk Rating	0/10
Description	Welcome back to Instagram. Sign in to check out what your friends, family & interests have been capturing & sharing around the world.	Primary language	Norwegian

Network

Site	https://www.instagram.com	Domain	instagram.com
Netblock Owner	Facebook, Inc.	Nameserver	ns-384.awsdns-48.com
Hosting company	Facebook	Domain registrar	registrarsafe.com
Hosting country	US	Nameserver organisation	whois.markmonitor.com
IPv4 address	157.240.221.174 (VirusTotal)	Organisation	Instagram LLC, 1601 Willow Rd, Menlo Park, 94025, United States
IPv4 autonomous systems	AS32934	DNS admin	awsdns-hostmaster@amazon.com
IPv6 address	2a03:2880:f258:e0:face:b00c:0:4420	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS32934	DNS Security Extensions	unknown
Reverse DNS	instagram-p42-shv-01-lhr8.fbcdn.net	Latest Performance	Performance Graph

IP delegation

IPv4 address (157.240.221.174)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 157.0.0.0-157.255.255.255	United States	NET157	Various Registries (Maintained by ARIN)
↳ 157.240.0.0-157.240.255.255	United States	THEFA-3	Facebook, Inc.
↳ 157.240.221.174	United States	THEFA-3	Facebook, Inc.

IPv6 address (2a03:2880:f258:e0:face:b00c:0:4420)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2a00::/11	European Union	EU-ZZ-2A00	RIPE NCC
↳ 2a00::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
↳ 2a03:2880::/29	Ireland	IE-FACEBOOK-201100822	Facebook Ireland Ltd
↳ 2a03:2880:f258:e0:face:b00c:0:4420	Ireland	IE-FACEBOOK-201100822	Facebook Ireland Ltd

SSL/TLS

Assurance	Organisation validation	Perfect Forward Secrecy	Yes
Common name	*.www.instagram.com	Supported TLS Extensions	RFC8446 supported versions, RFC8446 key share, RFC7301 application-layer protocol negotiation
Organisation	Facebook, Inc.	Application-Layer Protocol Negotiation	h2
State	California	Next Protocol Negotiation	Not Present
Country	US	Issuing organisation	DigiCert Inc
Organisational unit	Not Present	Issuer common name	DigiCert SHA2 High Assurance Server CA
Subject Alternative Name	*.www.instagram.com, www.instagram.com	Issuer unit	www.digicert.com
Validity period	From Mar 3 2021 to Jun 1 2021 (2 months, 4 weeks, 1 day)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	US
Server	Not Present	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation Lists	http://crl3.digicert.com/sha2-ha-server-g6.crl http://crl4.digicert.com/sha2-ha-server-g6.crl
Protocol version	TLSv1.3	Certificate Hash	GskBNGcTbPjCJ6QGGaBk9TY9oqQ
Public key length	2048	Public Key Hash	71c8f7aa2d8ebca3aa0c15293d58fd1d423ec523f8f8e2b3030239d50c146485
Certificate check	ok	OCSP servers	http://ocsp.digicert.com - *100% uptime in the past 24 hours*
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response	No response received
Serial number	0x03534ca132574c1bdf79542948a8694b		
Cipher	TLS_CHACHA20_POLY1305_SHA256		
Version number	0x02		

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Google Xenon 2021 fT7y+I//iFVoJMLAyp5SiXkrxQ54CX8uapdomX4i8Nc=	2021-03-03 02:56:05	Success
Certificate	DigiCert Yeti 2021 XNxDkv7mq0VEsV6a1FbmEDf71fpH3KFzlLJe5vbHDso=	2021-03-03 02:56:05	Success

Gathering information using https://www.shodan.io/

SHODAN www.instagram.com Explore Pricing Enterprise Access

Exploits Maps

TOTAL RESULTS

1,594

TOP COUNTRIES

United States	604
Germany	169
Brazil	111
Indonesia	104
France	79

TOP SERVICES

HTTPS	787
HTTP	293
8081	110
Synology	86
3001	64

TOP ORGANIZATIONS

Amazon Technologies Inc.	230
DigitalOcean, LLC	134
Amazon Data Services Ireland Limited	51
A100 ROW GmbH	48
Amazon Data Services NoVa	46

TOP PRODUCTS

Apache httpd	380
nginx	279
Microsoft IIS httpd	37
Apache Tomcat/Coyote JSP engine	16
LiteSpeed httpd	11

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

35.244.98.169
159.98.244.35.bc.googleusercontent.com
Google LLC
Added on 2021-04-03 05:00:11 GMT
Australia, Sydney
cloud

```
HTTP/1.1 200 OK
Date: Sat, 03 Apr 2021 05:00:11 GMT
Server: Apache/2.4.25 (Debian)
Set-Cookie: PHPSESSID=q0pb38okblts2qgicsco6tslbk; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Transfer-Encodin...
```

197.156.88.133
Hagbes
Added on 2021-04-03 05:08:44 GMT
Ethiopia, Addis Ababa

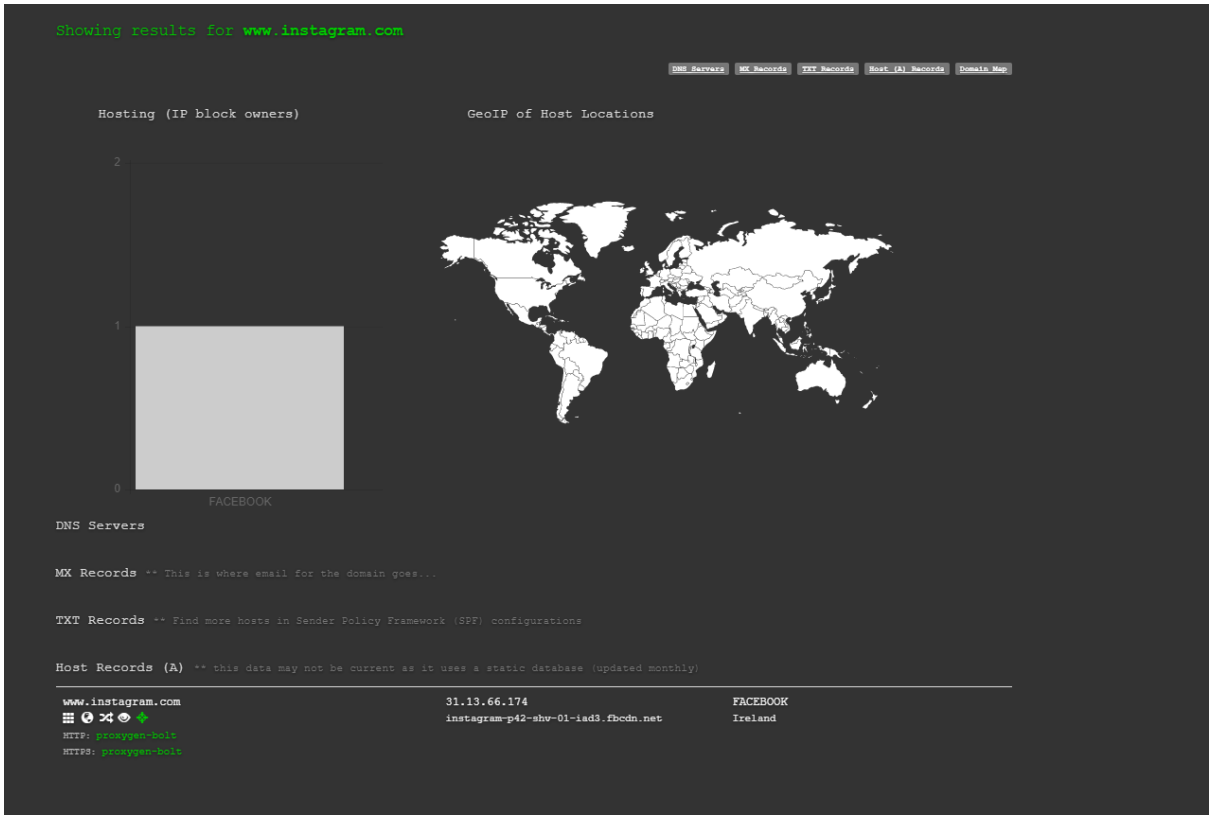
```
HTTP/1.1 200 OK
Date: Sat, 03 Apr 2021 05:08:43 GMT
Server: Apache/2.4.37 (Win64) OpenSSL/1.1.1a PHP/7.2.14
X-Powered-By: PHP/7.2.14
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

2507
<!DOCTYPE html>
        <head>
                <title>HAGBES - Portal System</title>
                <link rel="icon" h...
```

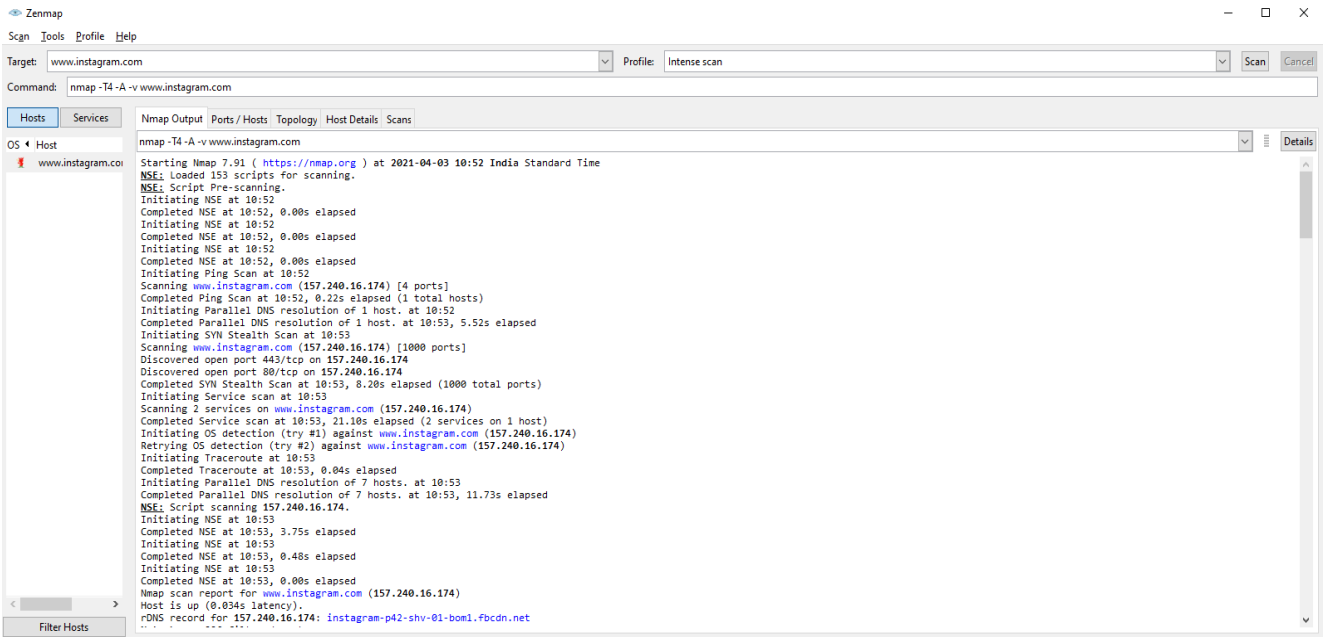
Tim News - Pagina inicial
52.7.217.248
ec2-52-7-217-248.compute-1.amazonaws.com
Amazon Technologies Inc.
Added on 2021-04-03 04:57:07 GMT
United States, Ashburn
Technologies: Nuxt.js
cloud

```
HTTP/1.1 200 OK
Date: Sat, 03 Apr 2021 04:57:06 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 189930
Connection: keep-alive
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Referrer-Policy: same-origin
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mo...
```

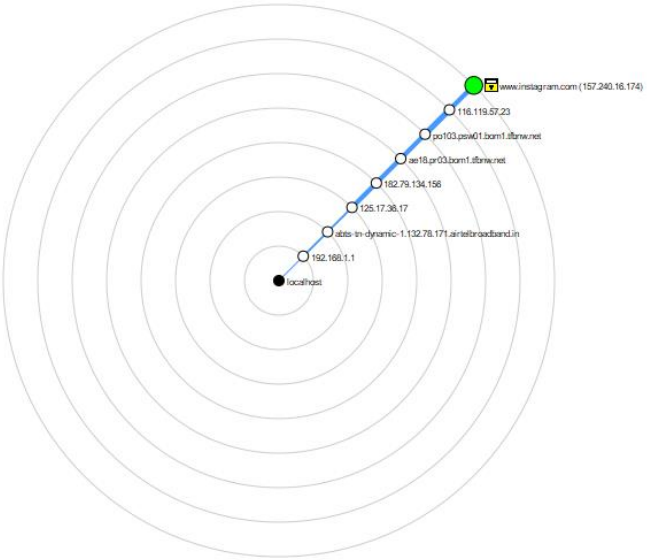
Gathering information using https://dnsdumpster.com/



c. Using nmap/zenmap to gather information on a website



Port	Protocol	State	Service	Version
80	tcp	open	http	proxygen-bolt
443	tcp	open	https	proxygen-bolt
843	tcp	closed	unknown	
5222	tcp	closed	xmpp-client	



www.instagram.com (157.240.16.174)

Host Status

State:	up
Open ports:	2
Filtered ports:	996
Closed ports:	2
Scanned ports:	1000
Up time:	19
Last boot:	Sat Apr 03 10:53:31 2021

Addresses

IPv4:	157.240.16.174
IPv6:	Not available
MAC:	Not available

Hostnames

Name - Type:	www.instagram.com - user
Name - Type:	instagram-p42-shv-01-bom1.fbcdn.net - PTR

Operating System

Name: FreeBSD 11.0-CURRENT

Accuracy: 87%

Ports used

OS Classes

TCP Sequence

IP ID Sequence

2. Penetration Testing on System

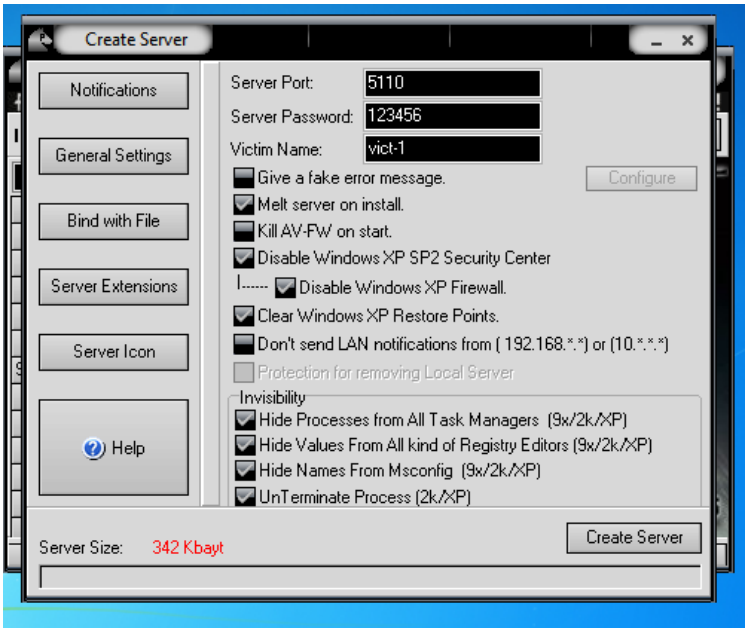
- **Test the Windows security using the ProRat and get access to the key logs. Delete the files from desktop or C drive and execute the commands to create a new folder in desktop and upload any file from your system.**

a) Download and Install ProRat in your Attacker PC (Attacker PC- windows 7 & Victim PC – windows XP)

Download Pro rat software from
https://prorat.software.informer.com/download/
And Install it in attacker PC
(Warning this software may contain virus and it is only safe to install it in VM)
Open ProRat after Installing it

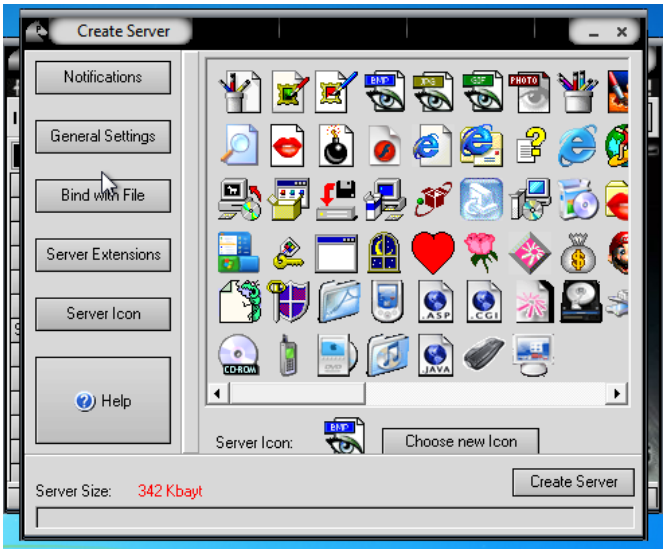
b) Creating a ProRat file

Click on 'Create' to create a new server



Then click on general setting and assign your victims name and server port and password

Also enable Melt server on install and make the server invisible



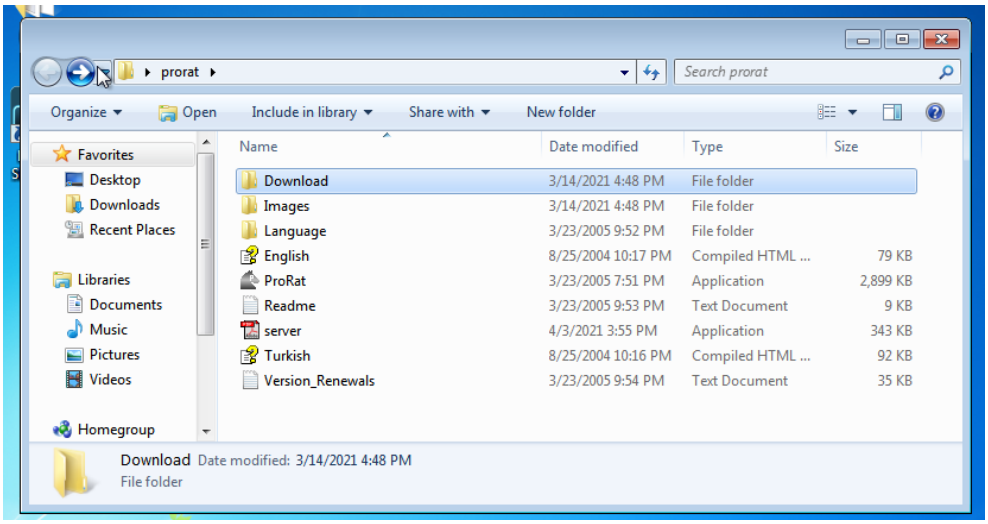
Assign the server with a genuine icon and name ,

So that the victim thinks it a legit file

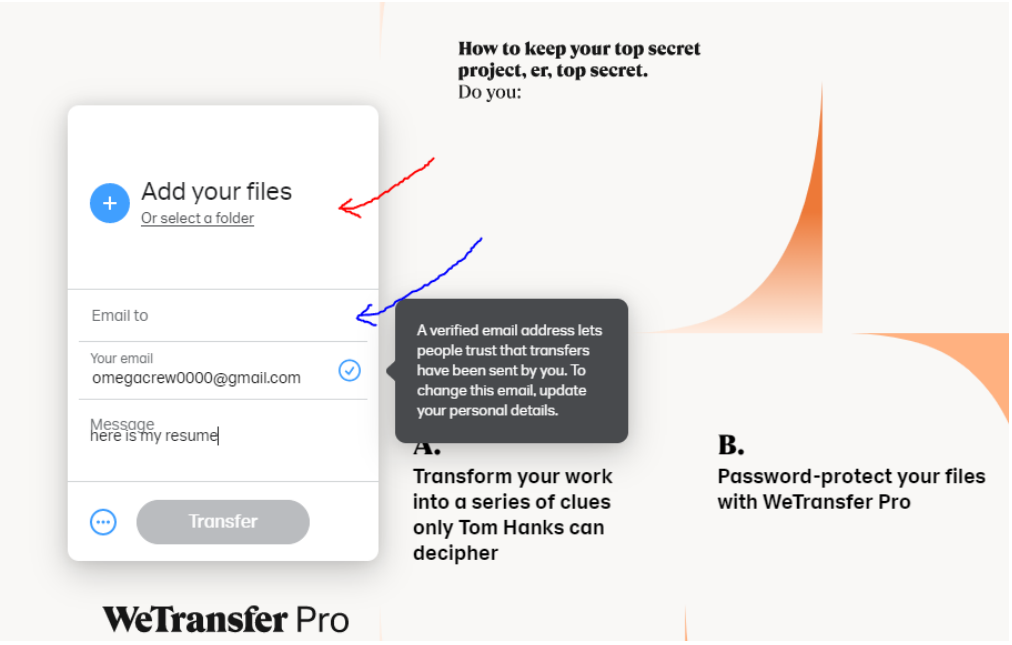
(I will be choosing the Pdf icon and naming the file my resume)

Next hit the create server

c) Sending the server file to the victim machine

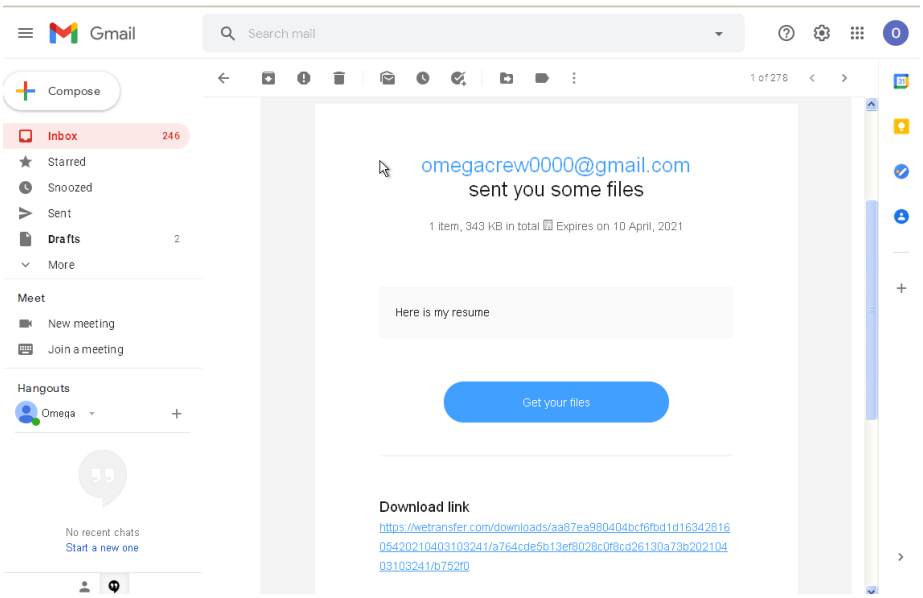


Now the server would have been created and will be available in the ProRat directory folder
Just rename the file according to your wish
And upload the file in https://wetransfer.com/

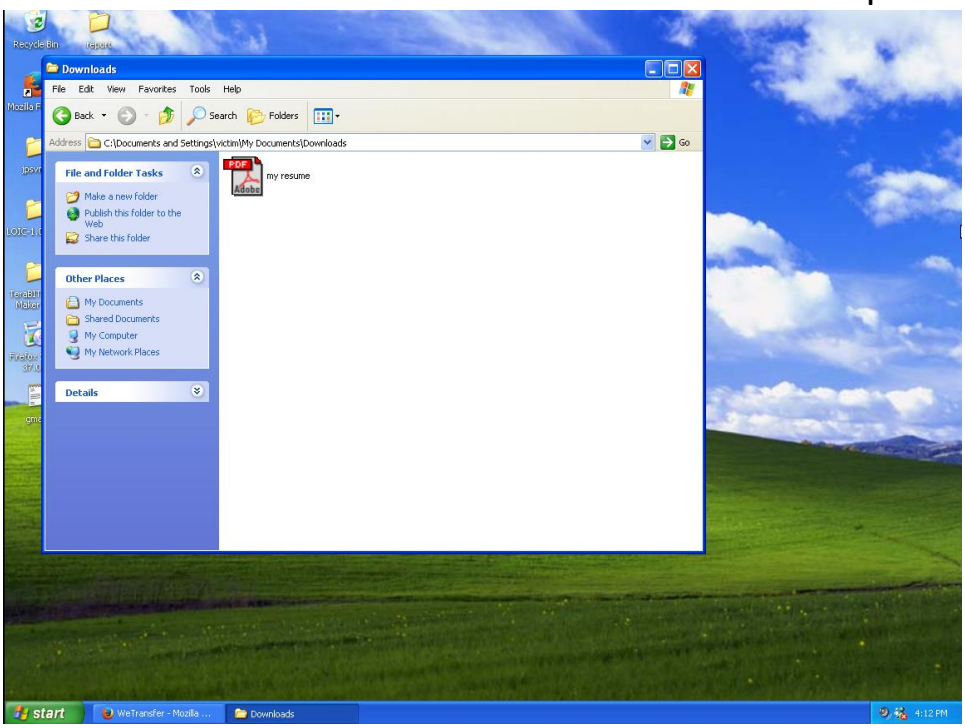


Upload your file and victims mail id here and hit transfer

Now we have to wait until the victim opens his mail and downloads the file we have sent



Once he has downloaded it all he has to do is to open the file



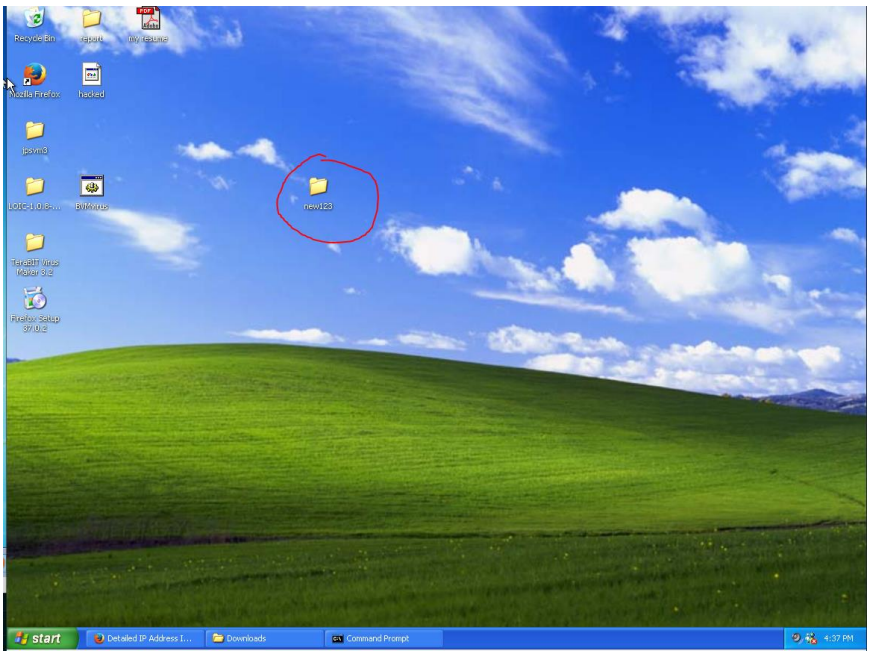
Now you can access Victims data by just typing the ip address of the victim and the password

d) Executing commands

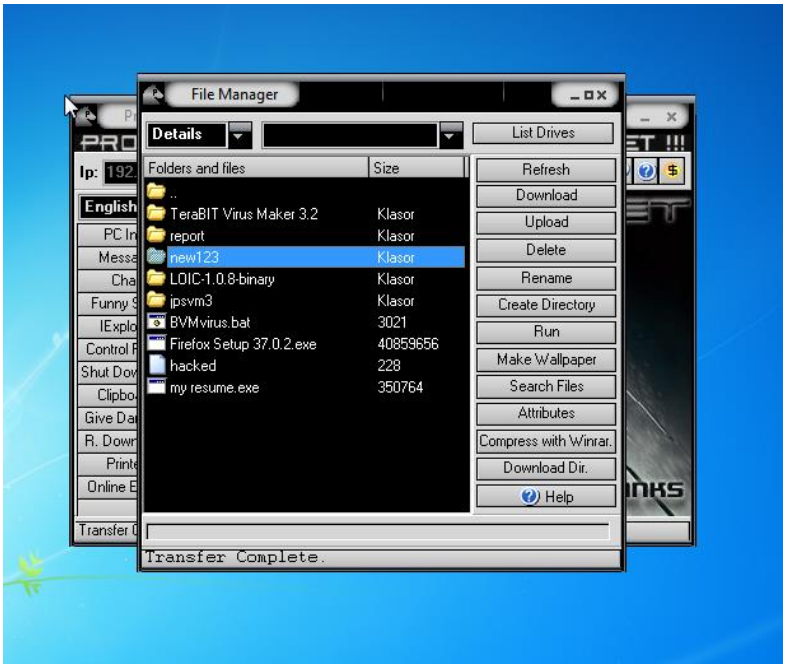
You can access the victims directory by clicking on 'File Manager'

And choosing destination where the file is present,

In my demo the file is present in the desktop and the name of the folder is 'new123'



Now to delete the file , choose the file and click delete from the options



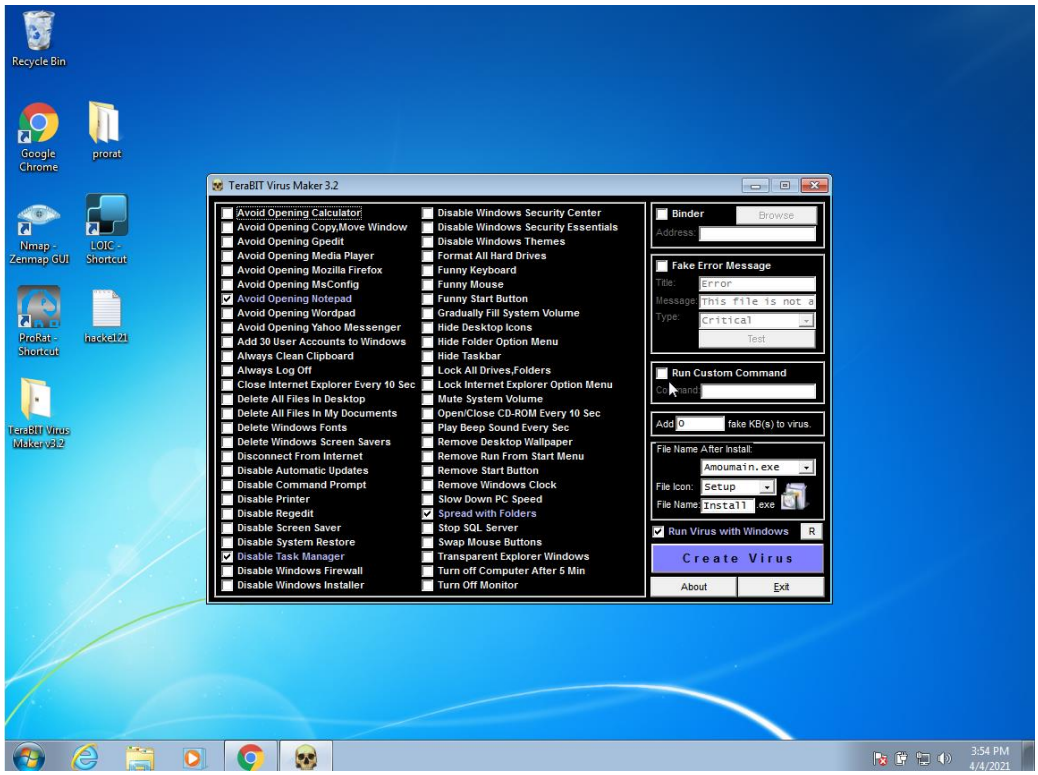
This will permanently delete the file from the Victims PC

3. Malware Creation, Exploitation, and Mobile Hacking

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

First download and extract Tetrabit virus maker in the attackers PC

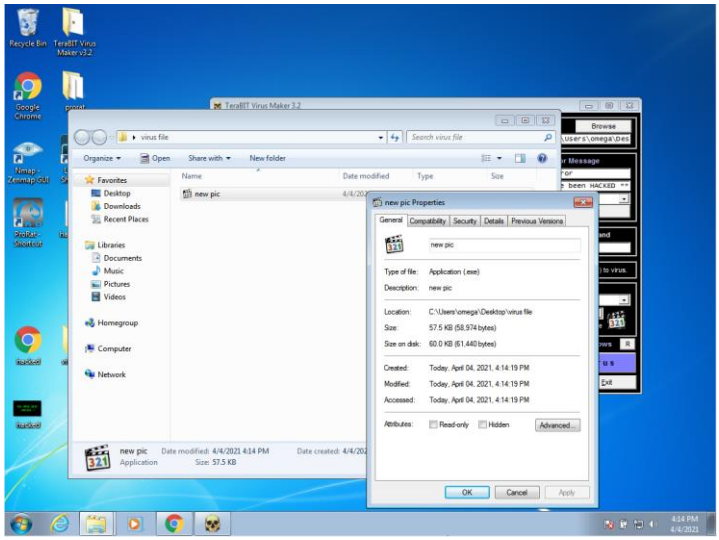
(I am using windows 7 as my attacker PC and windows XP as my victim PC)



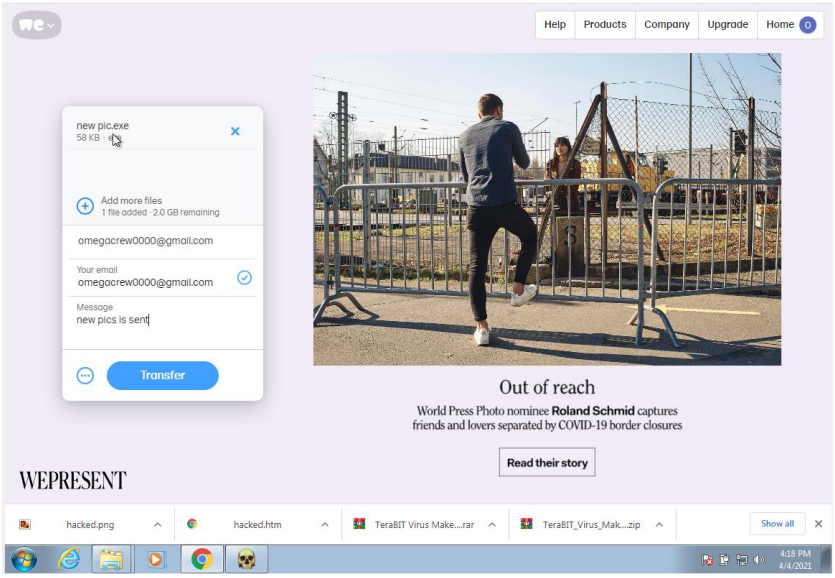
For demo I am going to use the Virus to disable the Calculator App and going to remove the start button and create a message saying ' YOU have been HACKED** '

I am also going to bind the virus file with a image file so that the victim does feel it as a suspicious file.

I am using wetransfer to send the virus file to the Victims PC



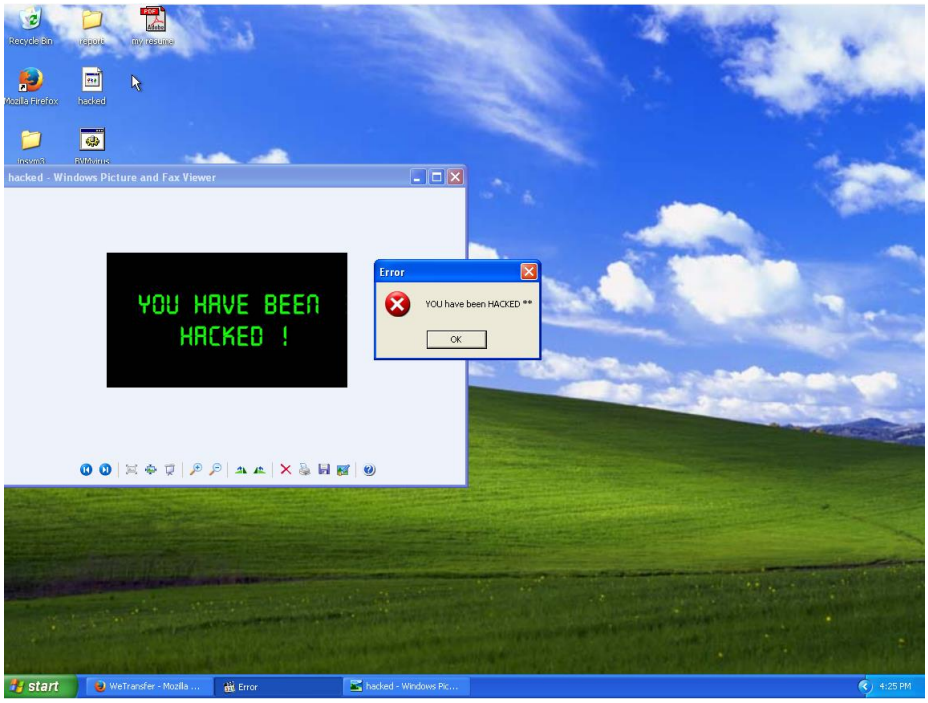
Virus has been successfully created and the file called as ‘new pic’



Once the file has been sent all the client has to do is to download and open the file

State of Windows XP machine before the attack

After opening the virus file calculator app does not open and there is no windows startup icon



This Virus cannot be detected or deleted by any anti-virus software

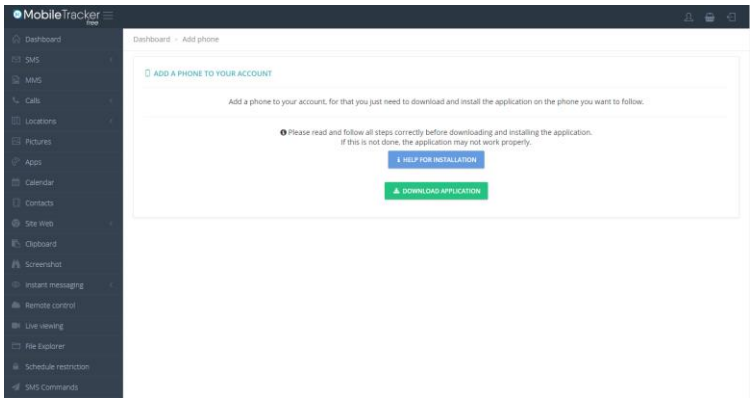
The victim should reinstall his OS to make his PC viable again

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

I could not do any real time attack because I did not have access to a VM *

But bellow I have shown how to setup and perform the attack

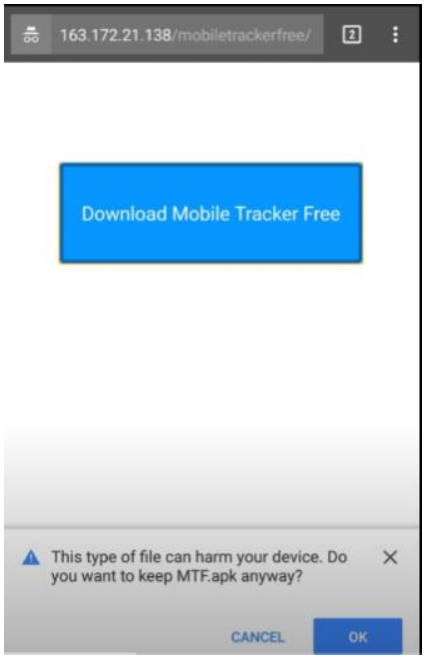
First create an account in mobile tracker free

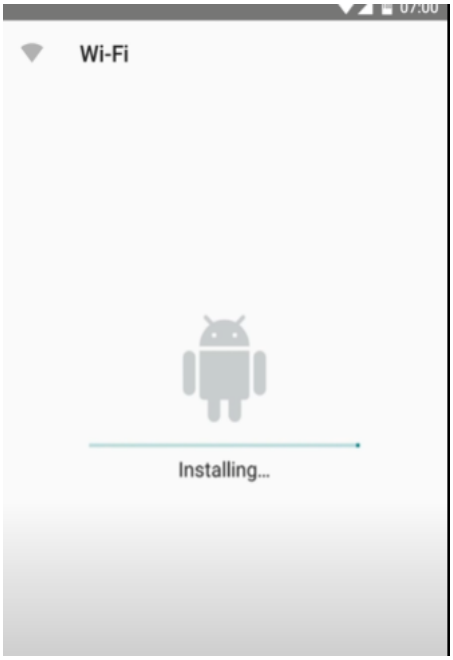


Next all you have to do is to download mobile tracker free app in the victims mobile and hide the app

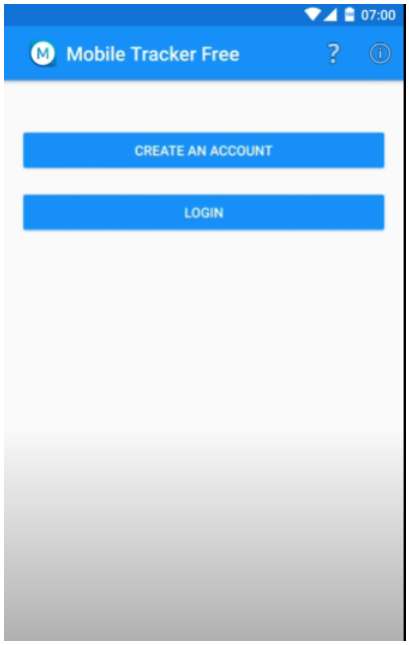
Once it is downloaded all the contact information and the device actions will be recorded and sent to the attacker

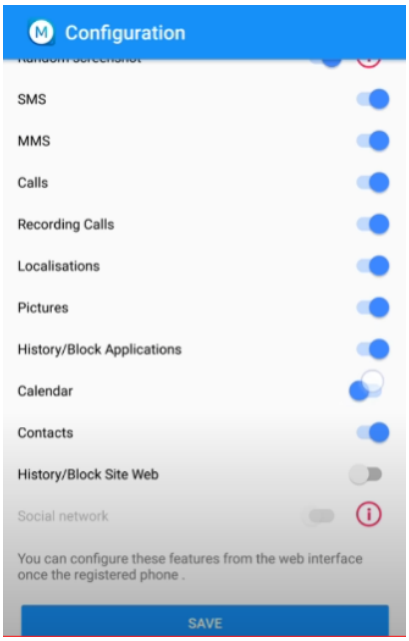
You can also track the victims mobile and also view the images and access the camera of the victim





These are some of the screenshots of a real time attack





4. Website Penetration Testing

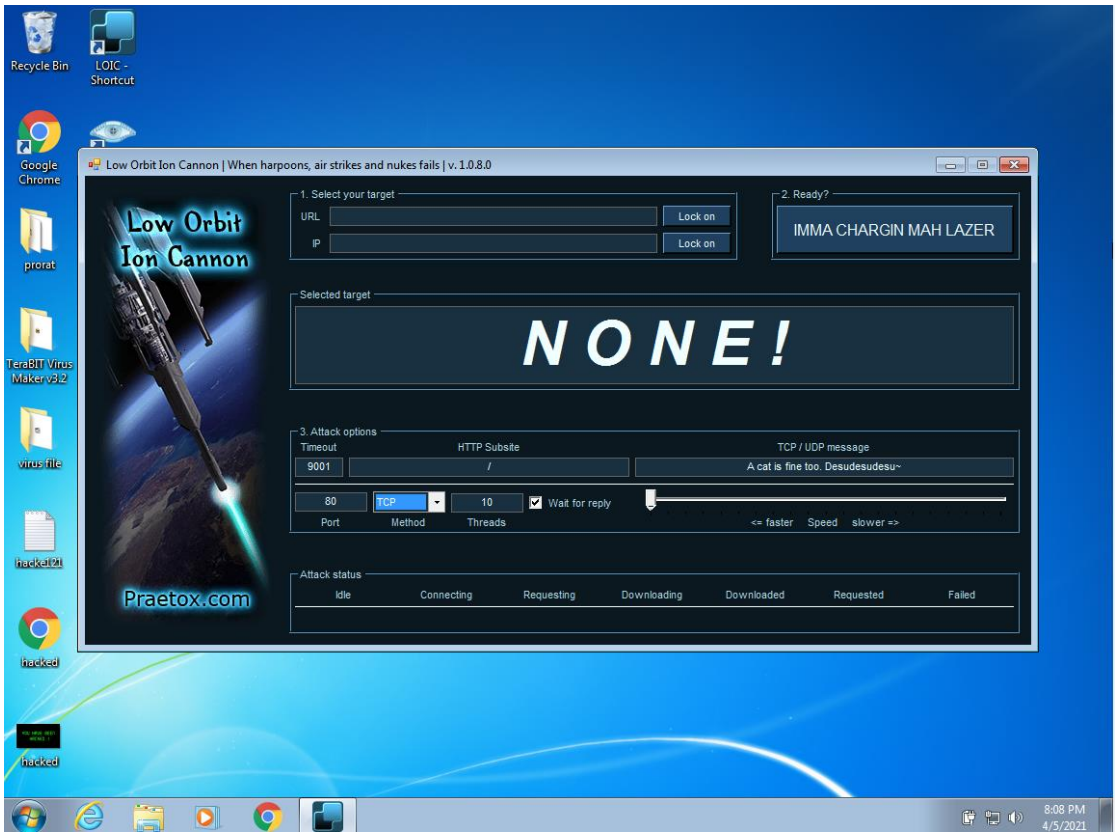
▪ Perform a DOS attack on windows 7 virtual machine using the LOIC tool and check the performance.

First Download and install the LOIC tool

In my demo I am going to use Windows 7 as my attacker PC and Windows XP as my Victim PC

Im going to use the victims ip address to do a dos attack

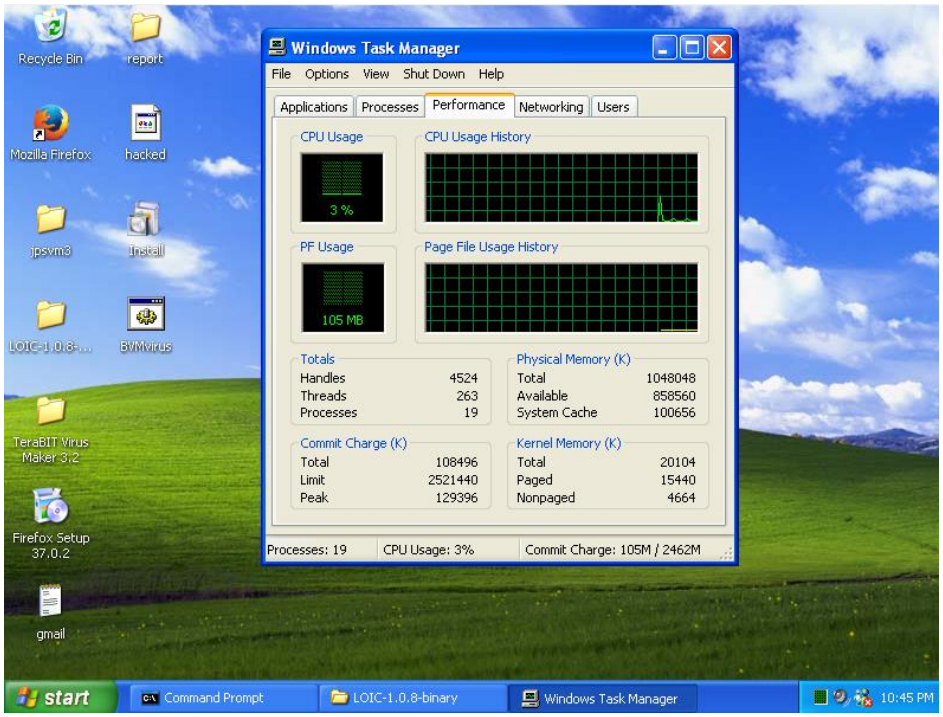
This attack can also be done on websites



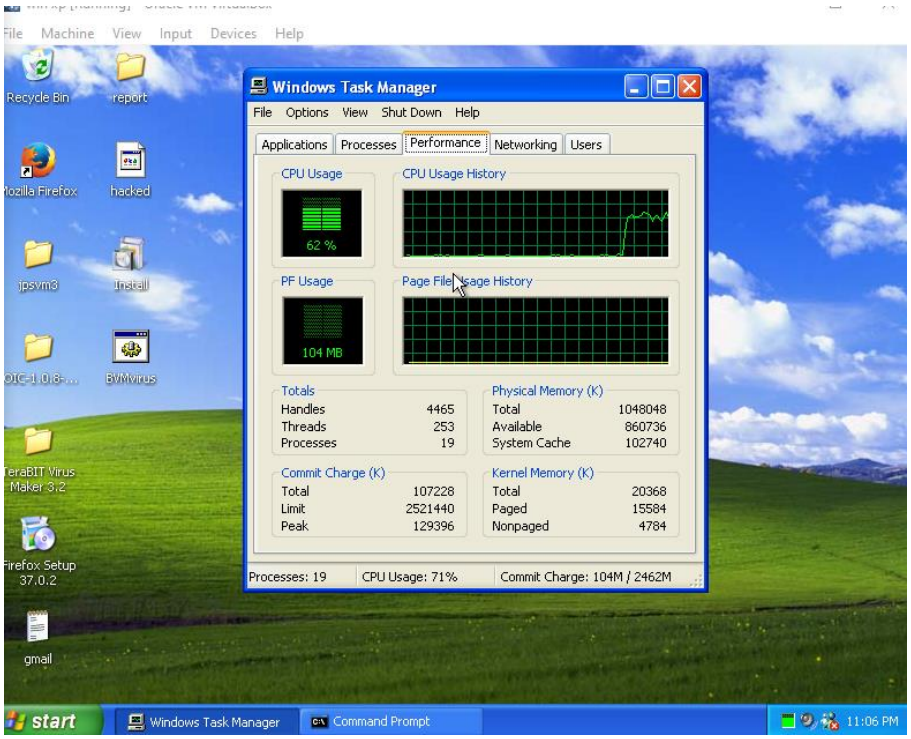
Victims Ip address is **192.168.1.10**

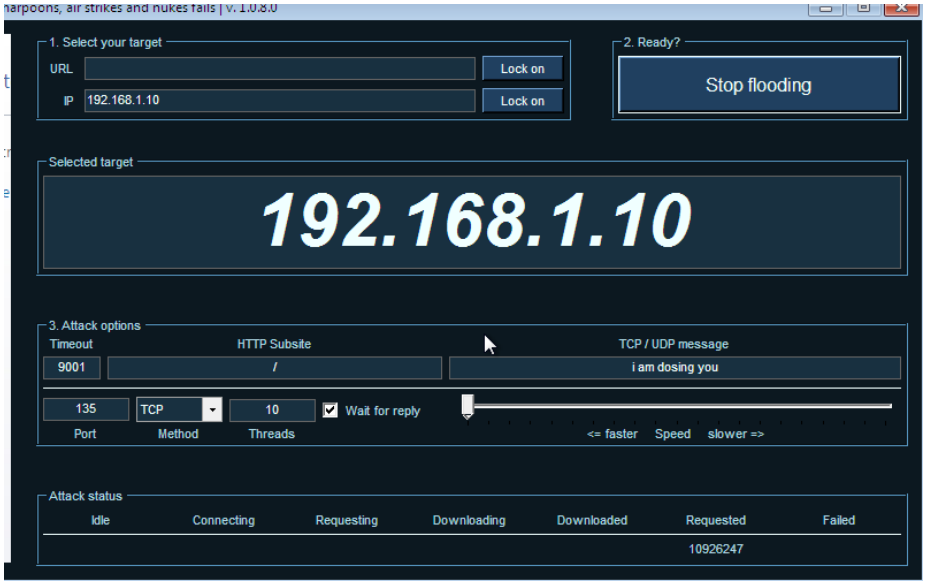
And the listening Port number is 135

Victim PC before Dos attack



After Dos attack

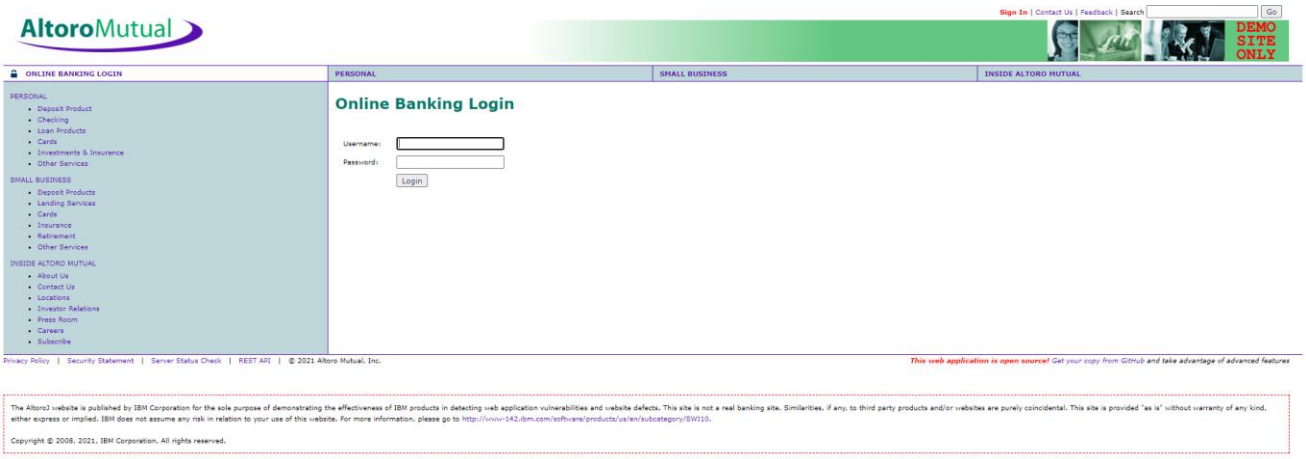




Request is continuously flooding to the ip's open port which cause drastic increase in CPU and RAM utilization of the Victims PC

- **Test the website using BlindSQL to Bypass Admin panel Authentication manually for https://demo.testfire.net/ website.**

First find empty login and password field in the website



As we are doing BlindSQL scripting to bypass the admin panel Authentication

We are not going to depend on error response instead we are going to check the response of the page according to our sql queries

For easy use I am using a cheat sheet to get some commonly used sql queries which exploits the website's Vulnerabilities

This list can be used by penetration testers when testing for SQL injection authentication bypass.A penetration tester can use it manually or through burp in order to automate the process.The creator of this list is Dr. Emin İslam Tatlıİf (OWASP Board Member).If you have any other suggestions please feel free to leave a comment in order to improve and expand the list.

```
or 1=1
or 1=1--
or 1=1#
or 1=1/*
admin' --
admin' #
admin'/*
admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'#
admin' or '1'='1'/*
admin'or 1=1 or ''='
admin' or 1=1
admin' or 1=1--
admin' or 1=1#
admin' or 1=1/*
admin') or ('1'='1
admin') or ('1'='1'--
admin') or ('1'='1'#
admin') or ('1'='1'/*
admin') or '1'='1
admin') or '1'='1'--
admin') or '1'='1'#
```

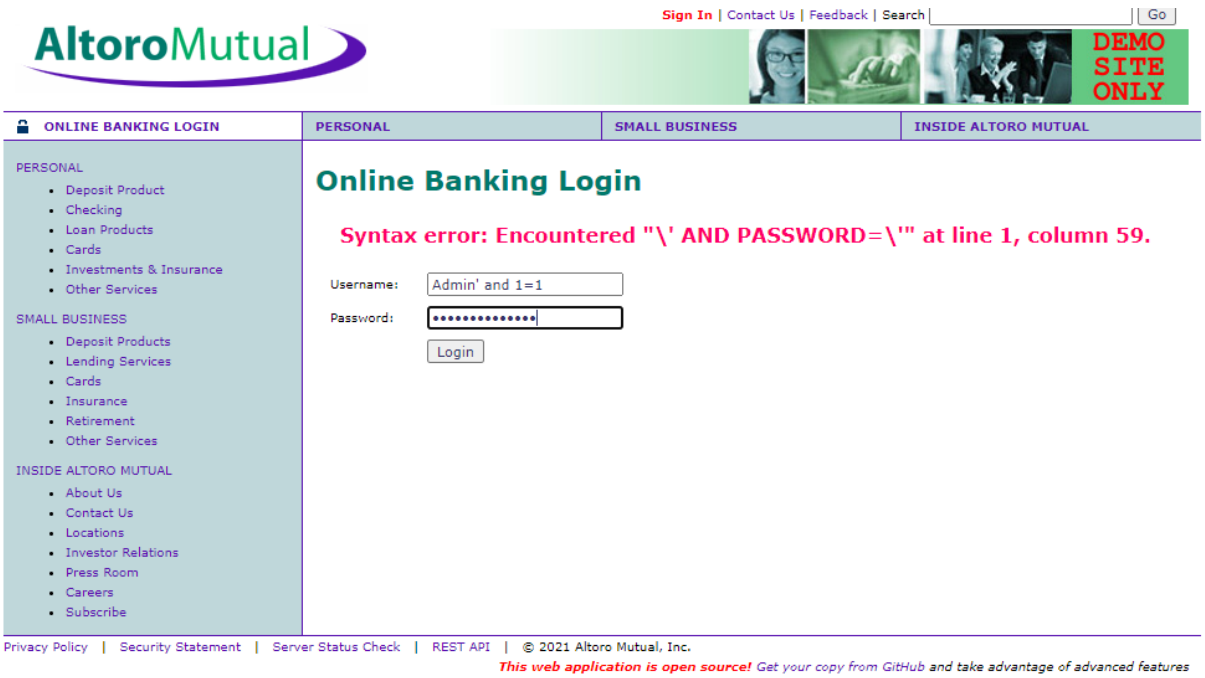
These are some of the common sql login commands used

We can use trial and error method to access the admin page but

As I am using BlindSQL method I am going to check the response of the page according to the input request .

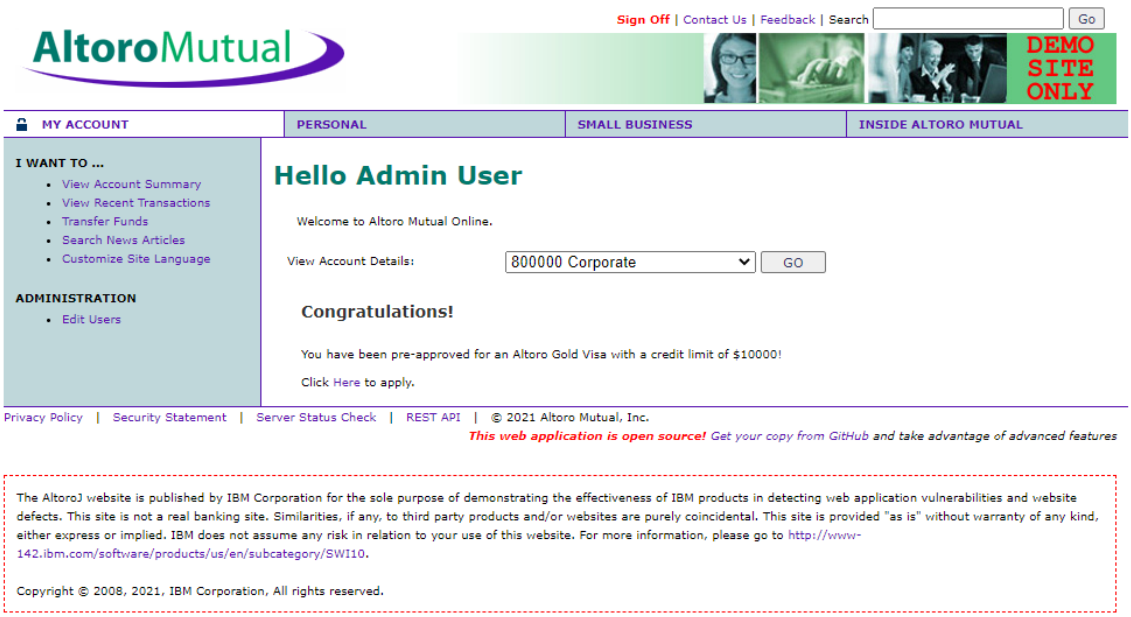
I am using commonly used Admin query

With a true conditional statement like 1=1



Error was encountered with "**\' And pwd=\'**"

So I used "**Admin' and '1'='1**"



And now I got access to the website

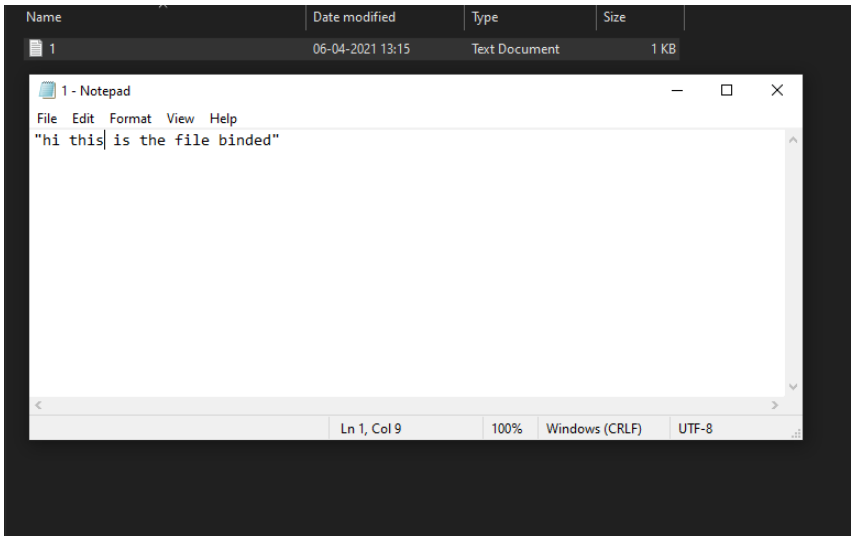
Now you can edit or upload any scripts in the web page as well as its server

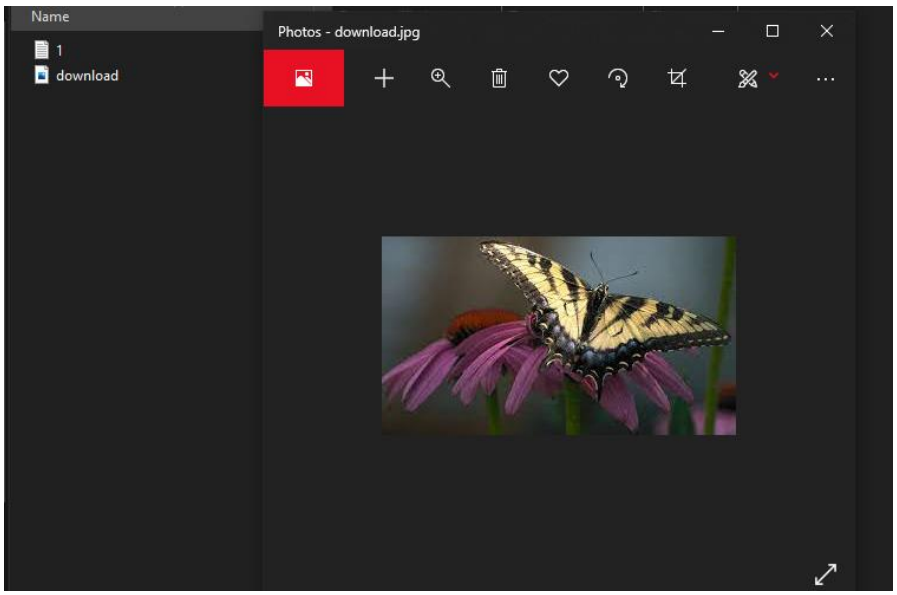
5. Data Encryption, Decryption, and Hiding of Secret Messages.

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

To bind a file with a image just put the file and image in the same folder

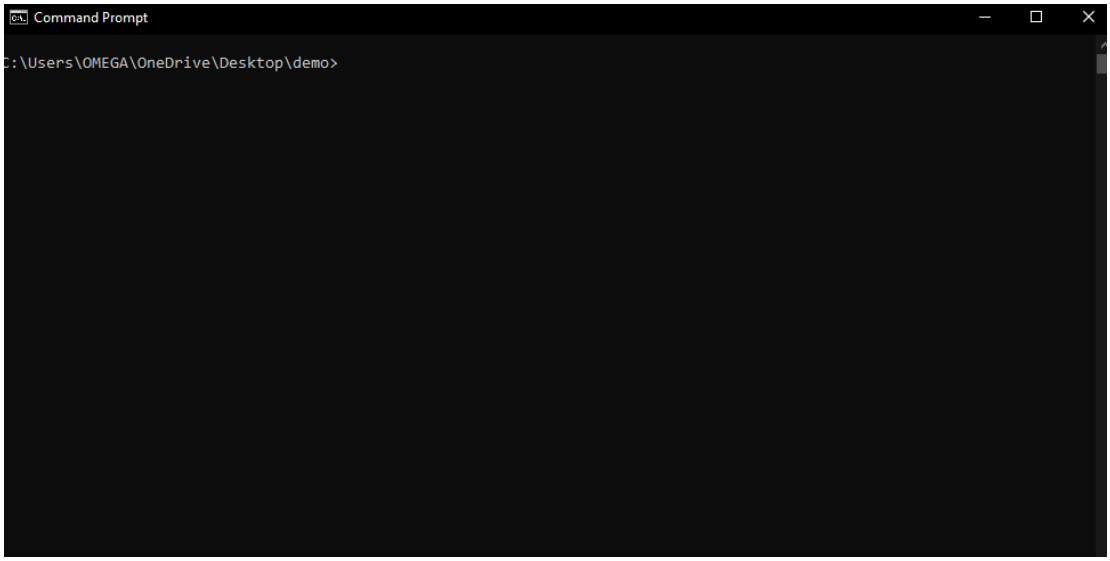
For demo purpose I am using a text file and binding it with a image file





Then encrypt the text file

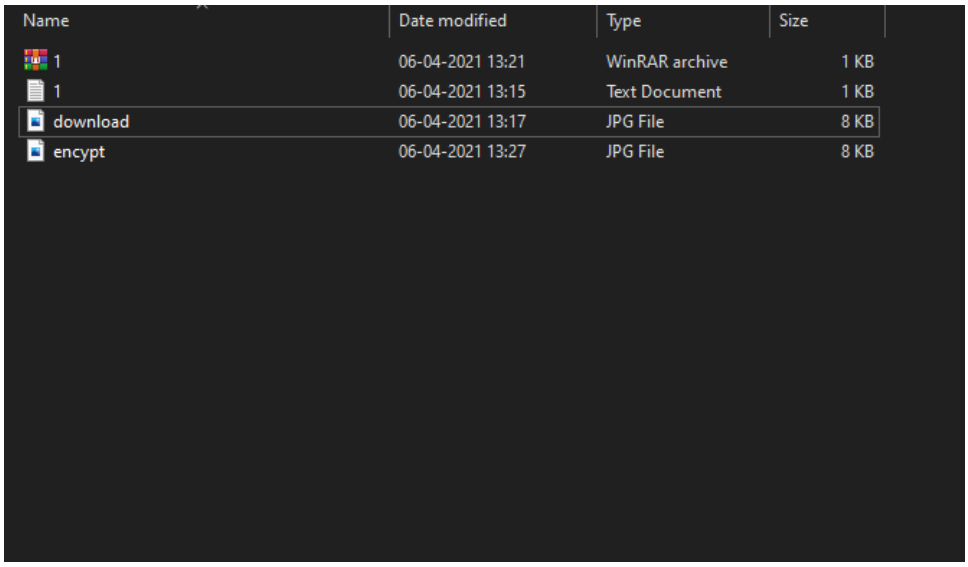
Open comand prompt and locate to the directory where these files are present



Now type the command

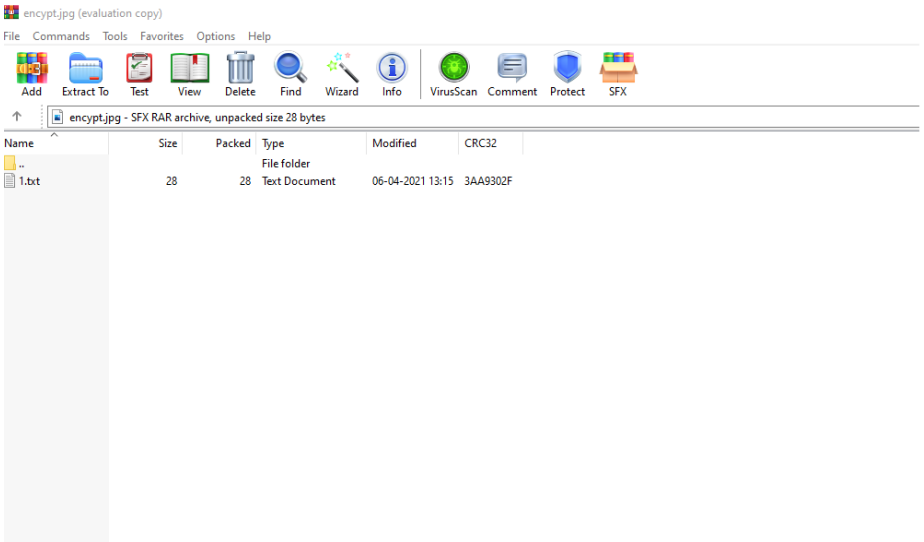
copy /b ‘image name’+ ’file name’ ‘output file’

Now the file has been created



Name	Date modified	Type	Size
1	06-04-2021 13:21	WinRAR archive	1 KB
1	06-04-2021 13:15	Text Document	1 KB
download	06-04-2021 13:17	JPG File	8 KB
encypt	06-04-2021 13:27	JPG File	8 KB

To view the file just open the image file using winrar



As you can see the text file is decrypted and available

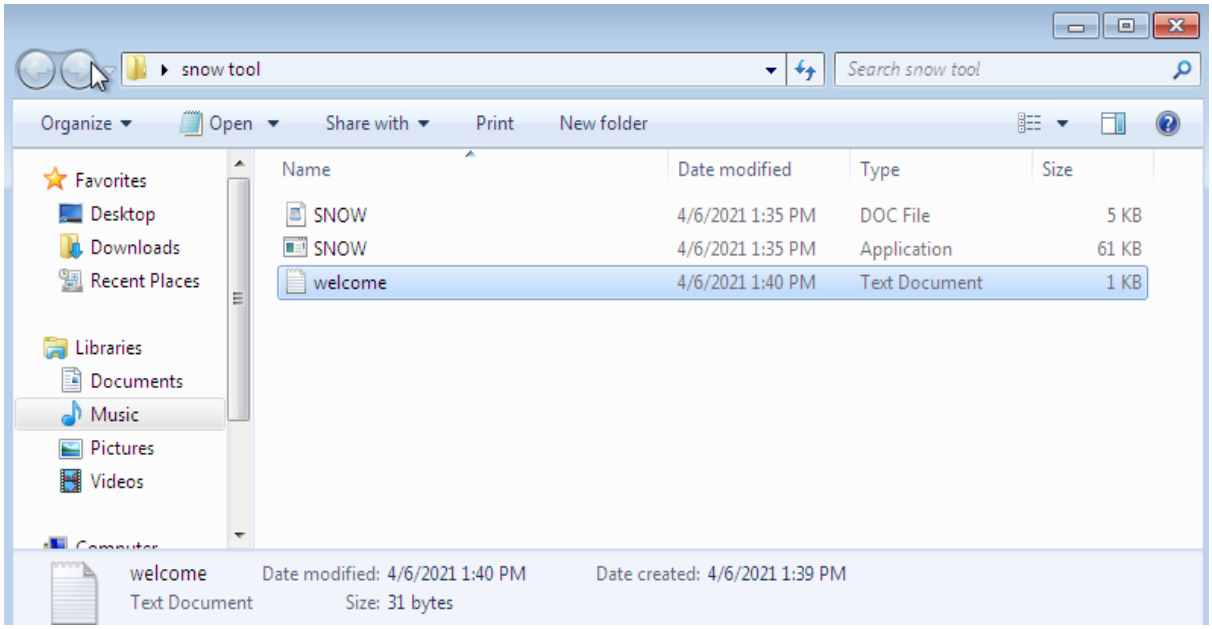
In this way we can also bing .exe like trojans and inject it into Victims PC

Similarly we can encrypt a secret message in a text files using snow tool

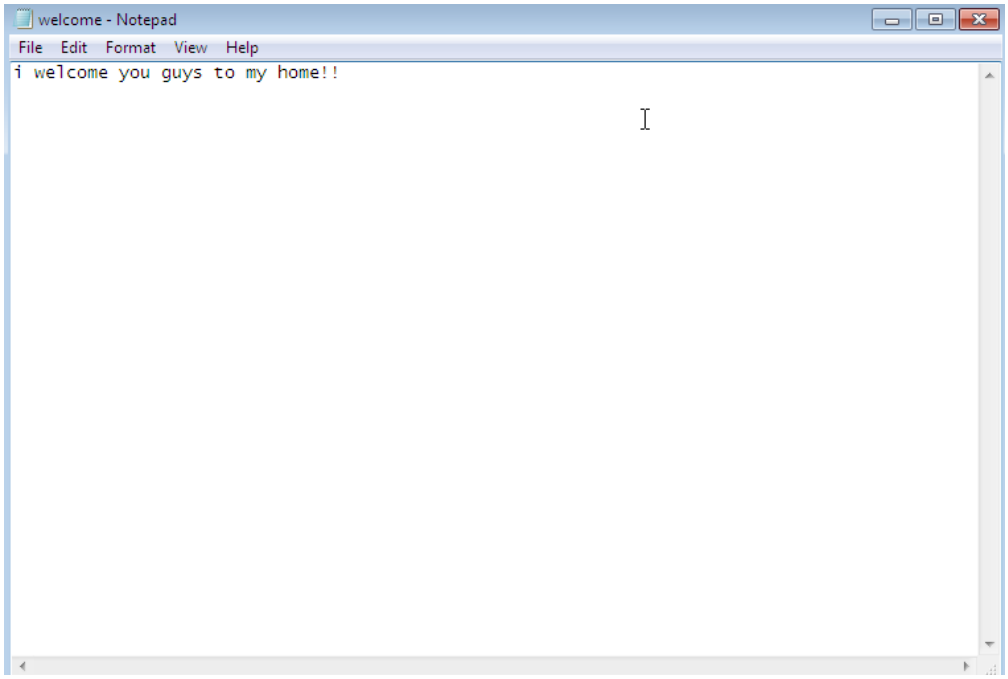
To use the snow just download the tool and use command prompt to open the dicrectory of the tool

Once the directory is open use this command to encrypt the message

Snow -C -m “encrypted message in quotes” -p “password” text_file_name New_text_file_name

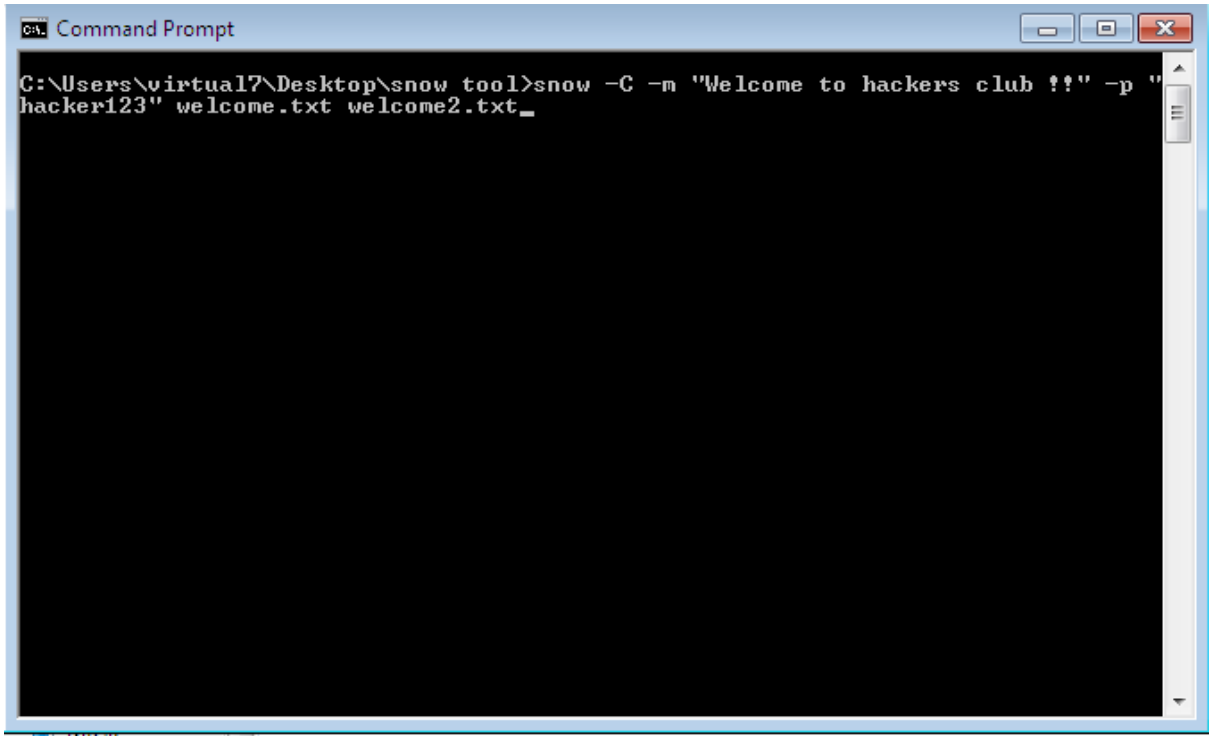


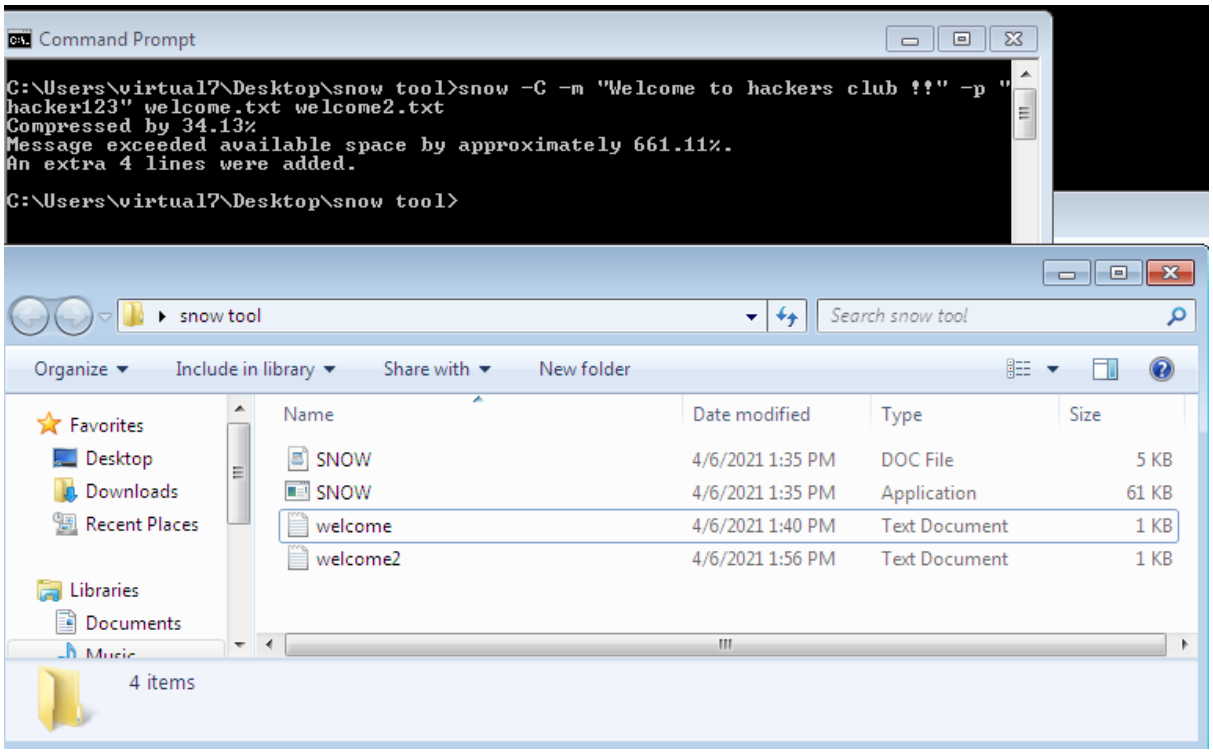
I have created a text file with name “welcome.txt”



This file is present in the same directory of the snow tool

Now use the command and encrypt the file

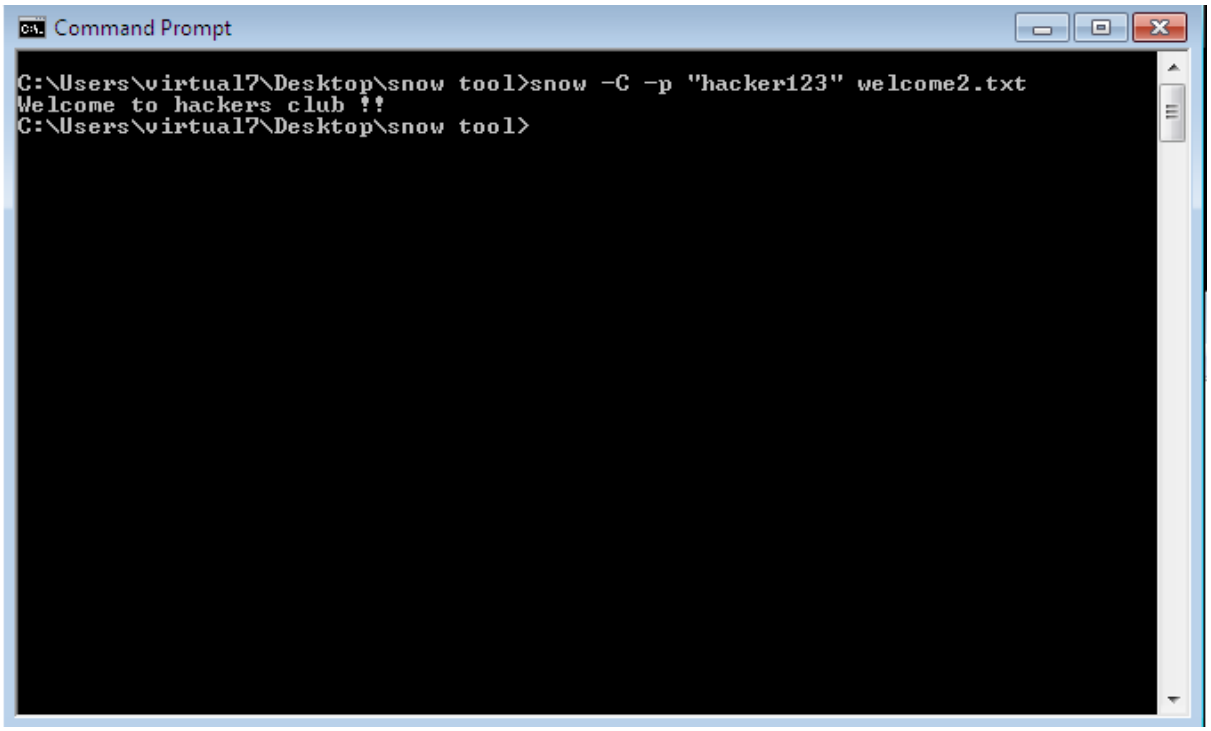




Now a new file called “welcome2.txt” has been created with the encrypted message

Now if you want to decrypt the message just type the command

snow -C -p “password” text_file_name



Now you can see that the hidden message has been decrypted

By this Steganography method hidden messages can be sent to anyone without getting noticed.