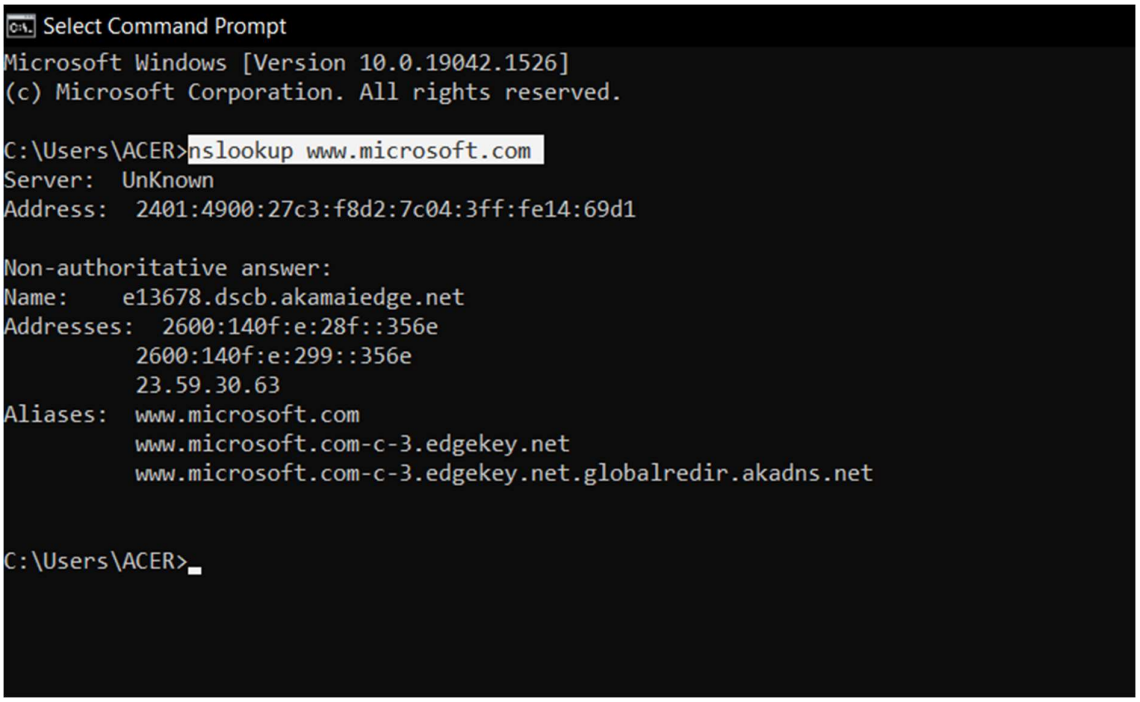
MINOR PROJECT

FOOT-PRINTING

STEPS TO REPRODUCE :

1) Go to CMD Prompt and run the following command To get internet domain and server name.
   Command = "**nslookup www.microsoft.com**"



We get the following details :

Server: UnKnown

Address: 2401:4900:27c3:f8d2:7c04:3ff:fe14:69d1

Non-authoritative answer:

Name: e13678.dscb.akamaiedge.net

Addresses: 2600:140f:e:28f::356e

2600:140f:e:299::356e

23.59.30.63

Aliases:

www.microsoft.com

www.microsoft.com-c-3.edgekey.net

www.microsoft.com3.edgekey.net.globalredir.akadns.net

2) To see the path that the signal took as it travelled around the internet to the website.
Command = "**tracert www.microsft.com**"

```
C:\Users\ACER>tracert www.microsoft.com

Tracing route to e13678.dscb.akamaiedge.net [2600:140f:e:28f::356e]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  2401:4900:27c3:f8d2:7c04:3ff:fe14:69d1
  2    31 ms    52 ms    42 ms  2401:4900:27c3:f8d2:0:45:8215:eb40
  3     *        *        *     Request timed out.
  4    38 ms    33 ms    28 ms  2401:4900:0:c000::16
  5   288 ms   308 ms   190 ms  2404:a800:3a00:2::ba
  6    97 ms    57 ms    53 ms  2404:a800:3a00:2::b9
  7     *      235 ms   163 ms  2404:a800::78
  8   424 ms   196 ms    41 ms  g2600-140f-000e-028f-0000-0000-0000-356e.deploy.static.akamaitechnologies.com [2600:140f:e:28f::356e]

Trace complete.

C:\Users\ACER>
```

Tracing route to e13678.dscb.akamaiedge.net [2600:140f:e:28f::356e]

over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 2401:4900:27c3:f8d2:7c04:3ff:fe14:69d1

2 31 ms 52 ms 42 ms 2401:4900:27c3:f8d2:0:45:8215:eb40

3 * * * Request timed out.

4 38 ms 33 ms 28 ms 2401:4900:0:c000::16

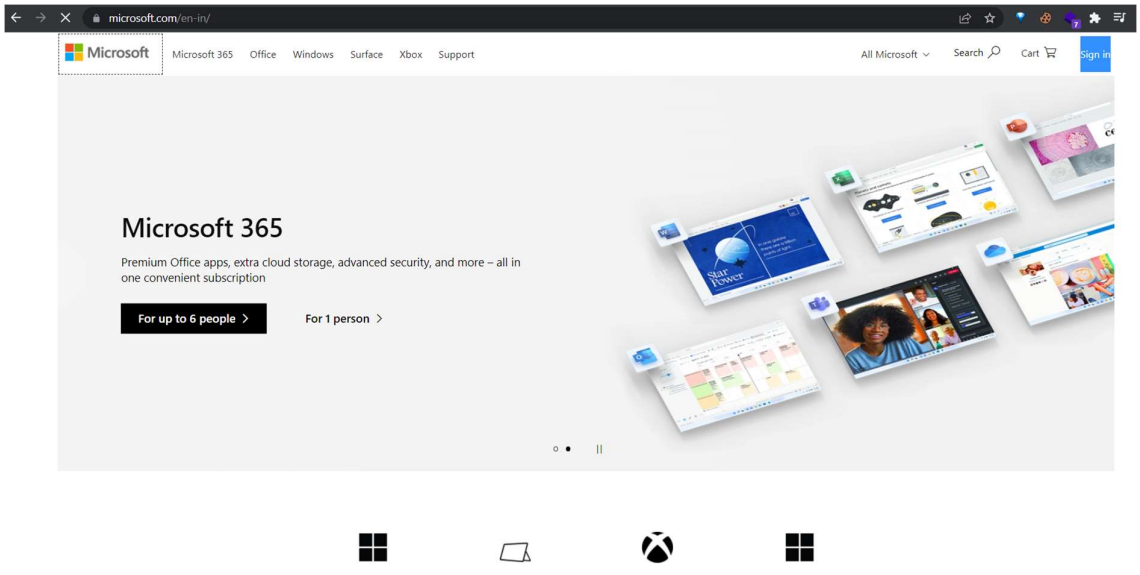
5 288 ms 308 ms 190 ms 2404:a800:3a00:2::ba

6 97 ms 57 ms 53 ms 2404:a800:3a00:2::b9

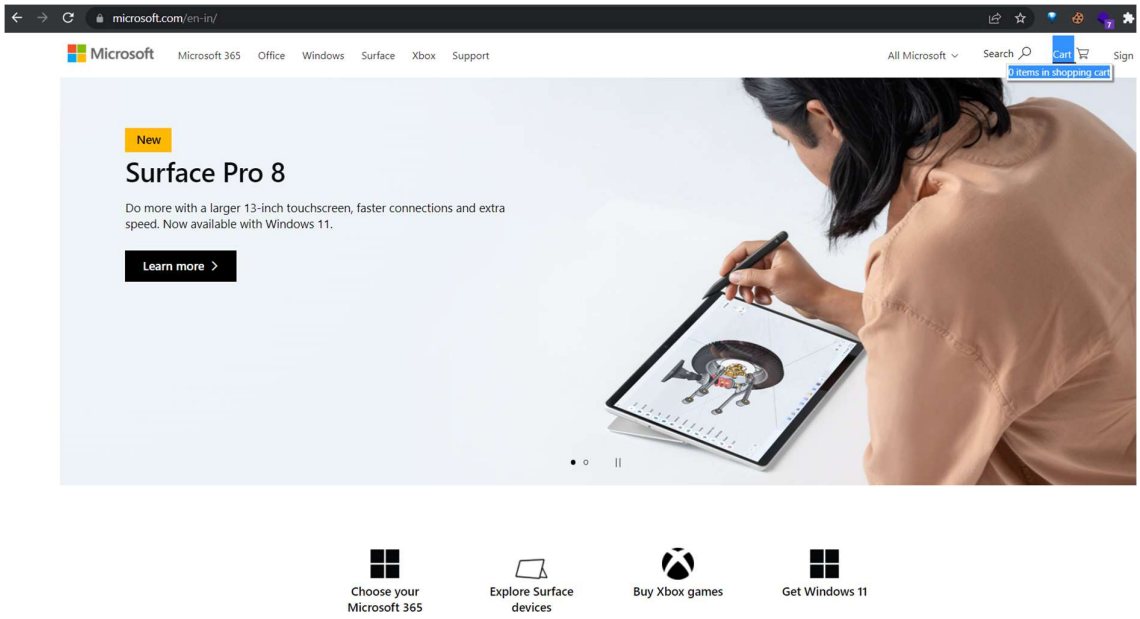
7 * 235 ms 163 ms 2404:a800::78

3) Directly from the website we can find the following information.

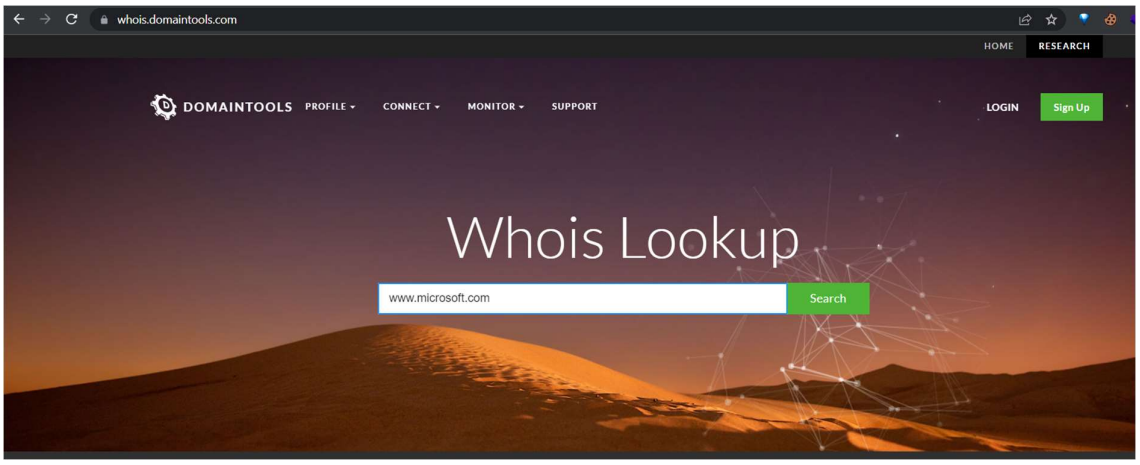
a) Login page



b) Ecommerce website (shopping cart)



4) getting information from who is domain tool https://whois.domaintools.com/



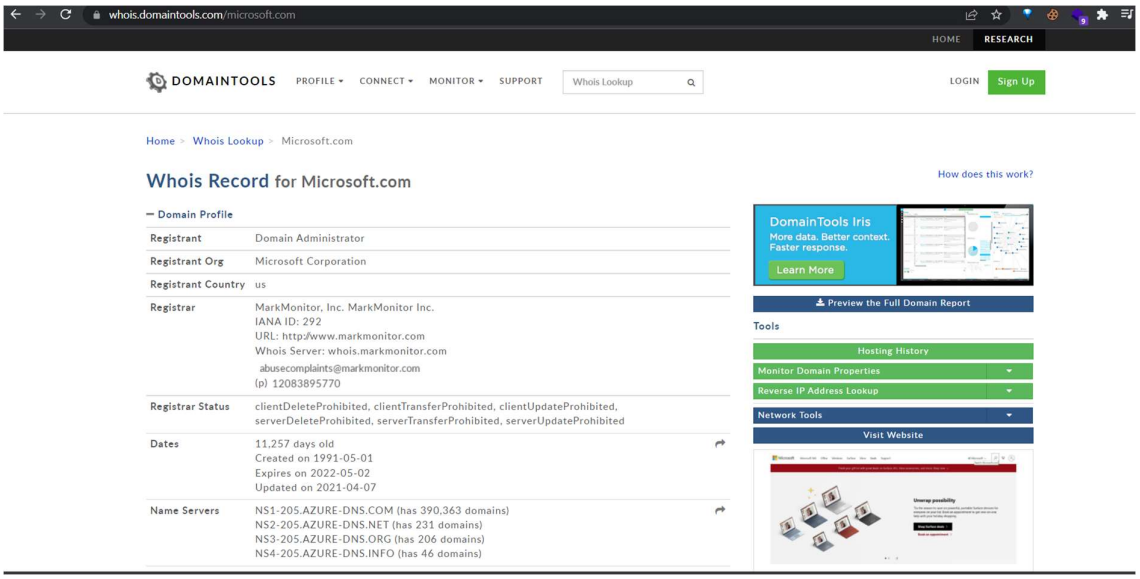
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292

	URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com

Dates	11,257 days old Created on 1991-05-01 Expires on 2022-05-02 Updated on 2021-04-07

Dates	11,257 days old Created on 1991-05-01 Expires on 2022-05-02 Updated on 2021-04-07

IP Address	23.216.81.152 - 15 other sites hosted on this server
IP Location	- Washington - Seattle - Akamai Technologies Inc.
IP History	258 changes on 258 unique IP addresses over 18 years
Hosting History	3 changes on 4 unique name servers over 2 years



	NS4-205.AZURE-DNS.INFO (has 46 domains)
Tech Contact	MSN Hostmaster Microsoft Corporation One Microsoft Way,, Redmond, WA, 98052, us msnhst@microsoft.com (p) 14258828080 (f) 14259367329
IP Address	23.216.81.152 - 15 other sites hosted on this server
IP Location	- Washington - Seattle - Akamai Technologies Inc.
ASN	AS16625 AKAMAI-AS, US (registered May 30, 2000)
Domain Status	Registered And Active Website
IP History	258 changes on 258 unique IP addresses over 18 years
Registrar History	4 registrars with 1 drop
Hosting History	3 changes on 4 unique name servers over 2 years

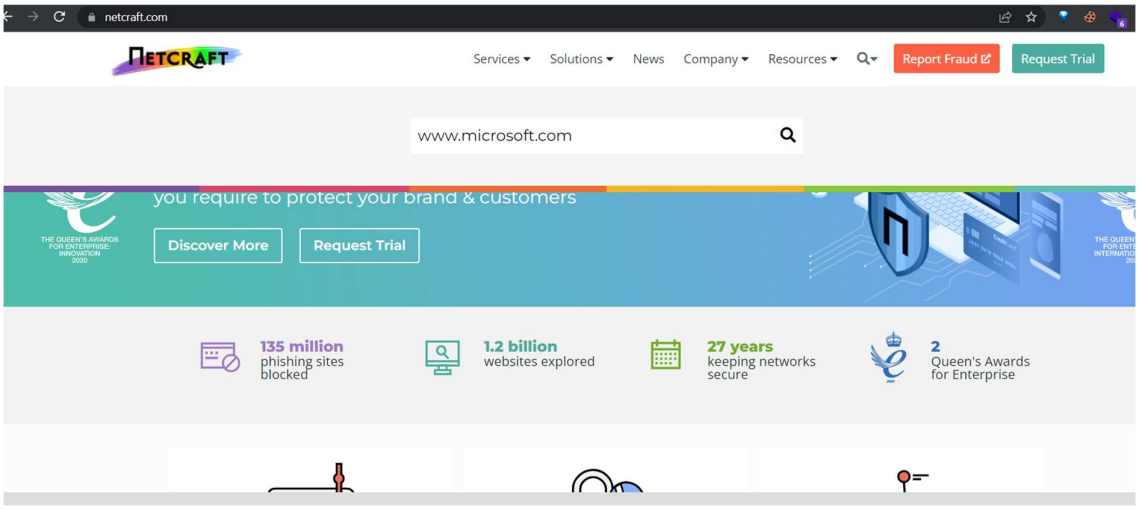
– Website

Website Title	Microsoft – Cloud, Computers, Apps & Gaming
Response Code	200
Terms	633 (Unique: 305, Linked: 271)
Images	24 (Alt tags missing: 10)
Links	124 (Internal: 111, Outbound: 13)

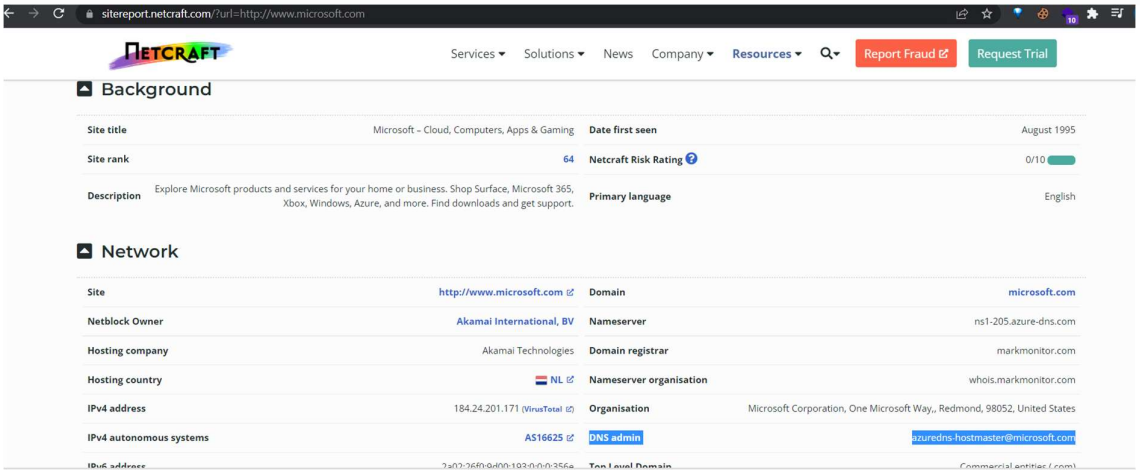
Whois Record (last updated on 20220224)

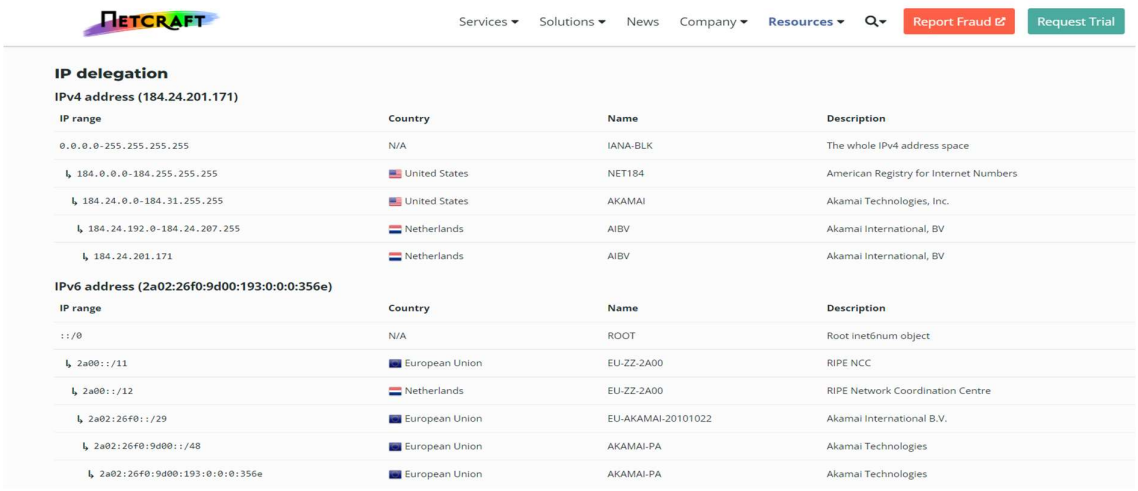
```
Domain Name: microsoft.com
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2021-04-07T19:58:15+0000
Creation Date: 1991-05-02T04:00:00+0000
Registrar Registration Expiration Date: 2022-05-02T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: admin@domains.microsoft
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Microsoft Corporation
Admin Street: One Microsoft Way,
Admin City: Redmond
Admin State/Province: WA
```

5) Getting information using Netcraft
https://www.netcraft.com/



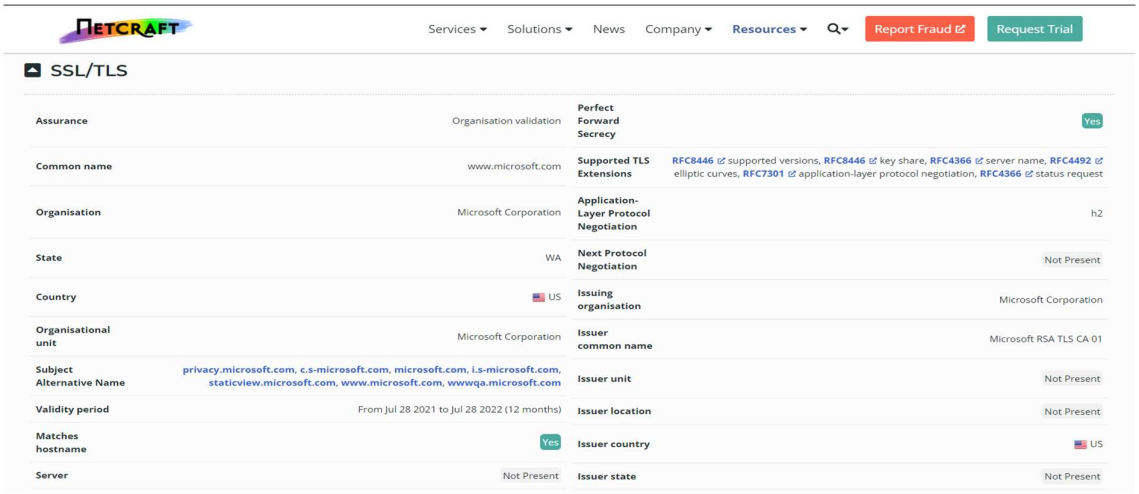
Site rank	64
IPv4 address	184.24.201.171
DNS admin	azuredns-hostmaster@microsoft.com



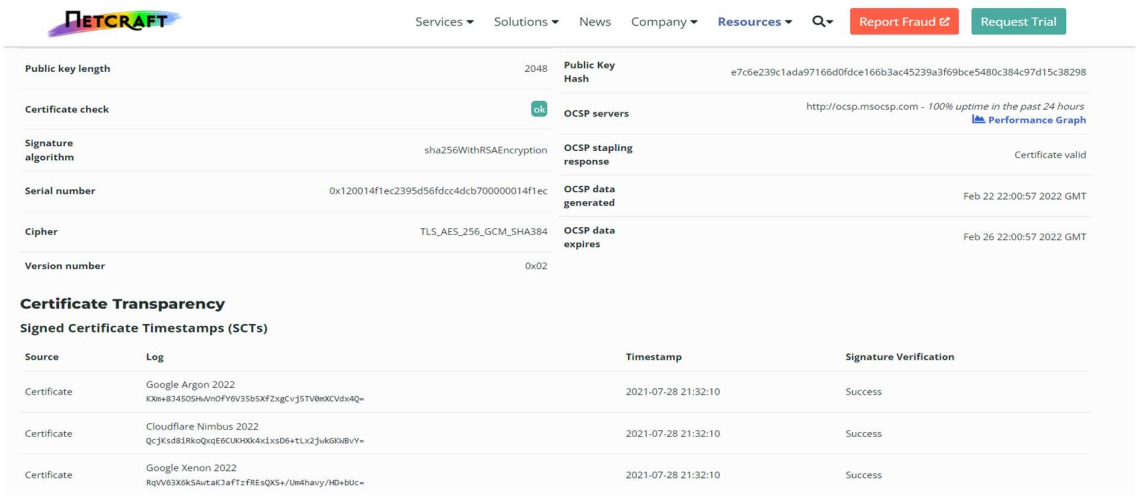


SSL/TLS information

Public key algorithm	rsaEncryption
Subject Alternative Name	privacy.microsoft.com, c.s-microsoft.com, microsoft.com, i.s-microsoft.com, staticview.microsoft.com, www.microsoft.com, wwwqa.microsoft.com
Signature algorithm	sha256WithRSAEncryption
Serial number	0x120014f1ec2395d56fdcc4dcb700000014f1ec



Source	Log	Timestamp
Certificate	Google Argon 2022 KXm+8J45OSHwVnOfY6V35b5XfZxgCvj5TV0mXCVdx4Q=	2021-07-28 21:32:10
Certificate	Cloudflare Nimbus 2022 QcjKsd8iRkoQxqE6CUKHXk4xixsD6+tLx2jwkGKWBvY=	2021-07-28 21:32:10
Certificate	Google Xenon 2022 RqVV63X6kSAwtaKJafTzfREsQXS+/Um4havy/HD+bUc=	2021-07-28 21:32:10

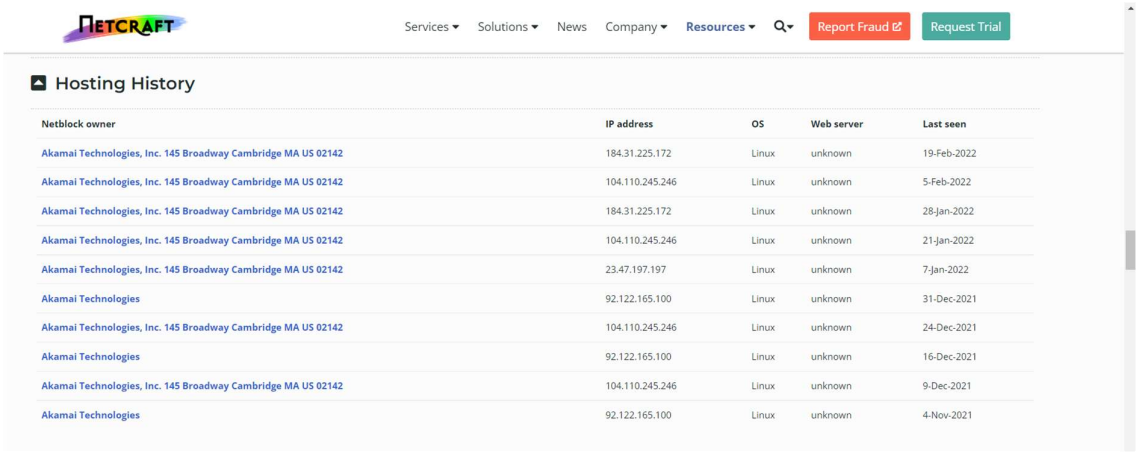


Organisational unit	CyberTrust
Validity period	From 2000-05-12 to 2025-05-12

SSL Certificate Chain

Common name	Baltimore CyberTrust Root
Organisational unit	CyberTrust
Organisation	Baltimore
Validity period	From 2000-05-12 to 2025-05-12
Common name	Microsoft RSA TLS CA 01
Organisational unit	Not Present
Organisation	Microsoft Corporation
Validity period	From 2020-07-21 to 2024-10-08

HOSTING HISTORY



Netblock owner	IP address	OS	Web server	Last seen
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	184.31.225.172	Linux	unknown	19-Feb-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	5-Feb-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	184.31.225.172	Linux	unknown	28-Jan-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	21-Jan-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	23.47.197.197	Linux	unknown	7-Jan-2022
Akamai Technologies	92.122.165.100	Linux	unknown	31-Dec-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	24-Dec-2021
Akamai Technologies	92.122.165.100	Linux	unknown	16-Dec-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	9-Dec-2021
Akamai Technologies	92.122.165.100	Linux	unknown	4-Nov-2021

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	www.linkedin.com, outlook.office.com, l.facebook.com
Document Compatibility Mode	A meta-tag used in Internet Explorer 8 to enable compatibility mode	docs.microsoft.com, outlook.live.com, teams.microsoft.com
X-Content-Type-Options	Browser MIME type sniffing is disabled	en.wikipedia.org, login.microsoftonline.com, mail.google.com
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	www.google.com, mail-redir.mention.com
X-XSS-Protection Block	Block pages on which cross-site scripting is detected	www.bbc.co.uk, www.startpage.com, mail.protonmail.com

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	discord.com, web.whatsapp.com

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	

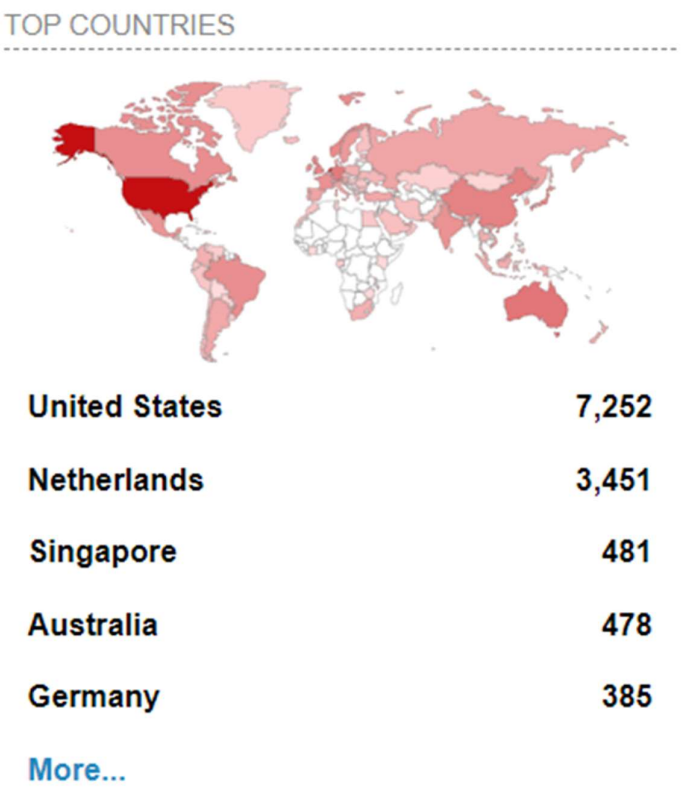
CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.msn.com, www.instagram.com, www.baidu.com
CSS Media Query	*No description*	www.paypal.com, www.canva.com, www.w3schools.com

6) Gathering information through shodan
   https://www.shodan.io/

It gives all the information of the servers.



TOTAL RESULTS

15,573

TOP COUNTRIES

- **United States 7,252**
- **Netherlands 3,451**
- **Singapore 481**
- **Australia 478**
- **Germany 385**

TOP PORTS

- **443 8,165**
- **8443 3,239**
- **4443 2,511**
- **80 521**
- **8081 265**

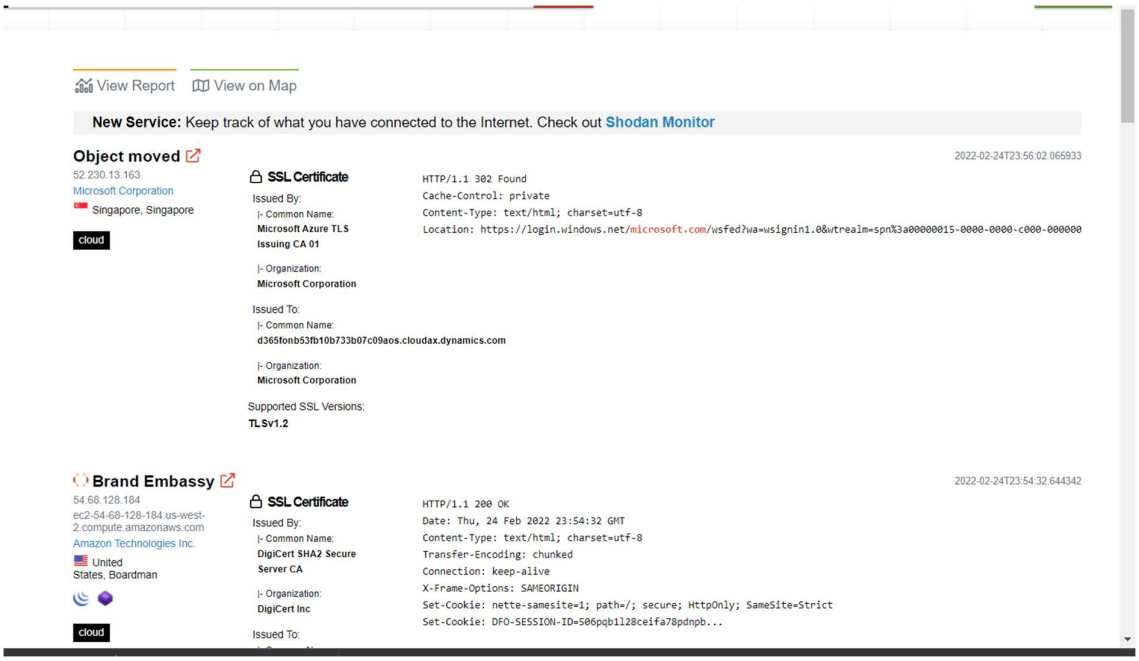
TOP ORGANIZATIONS

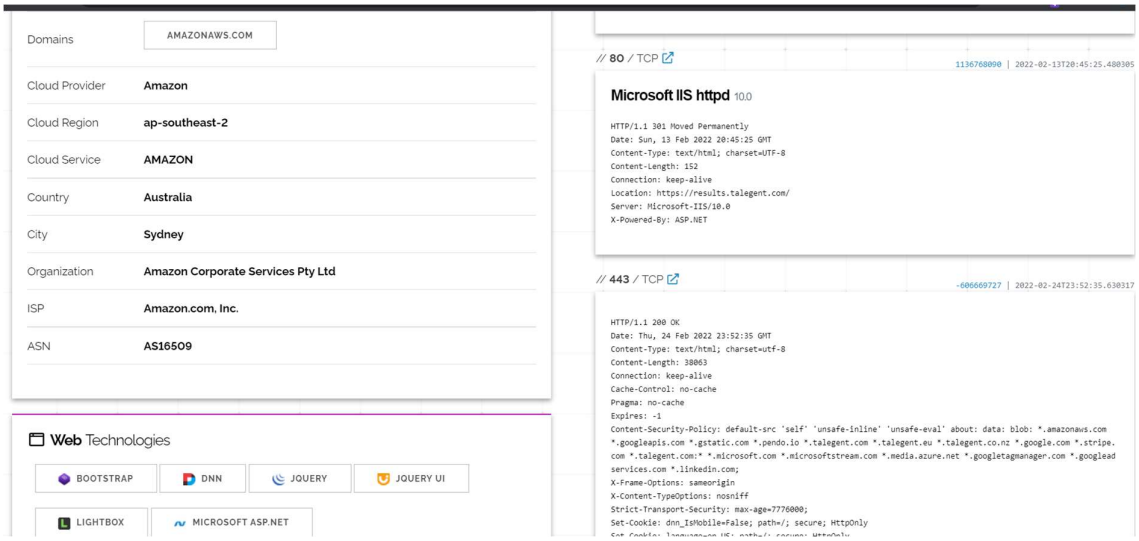
- **Microsoft Corporation 7,590**
- **Microsoft Corp 861**
- **Microsoft Limited UK 843**
- **Akamai Technologies, Inc. 614**
- **Amazon Technologies Inc. 442**

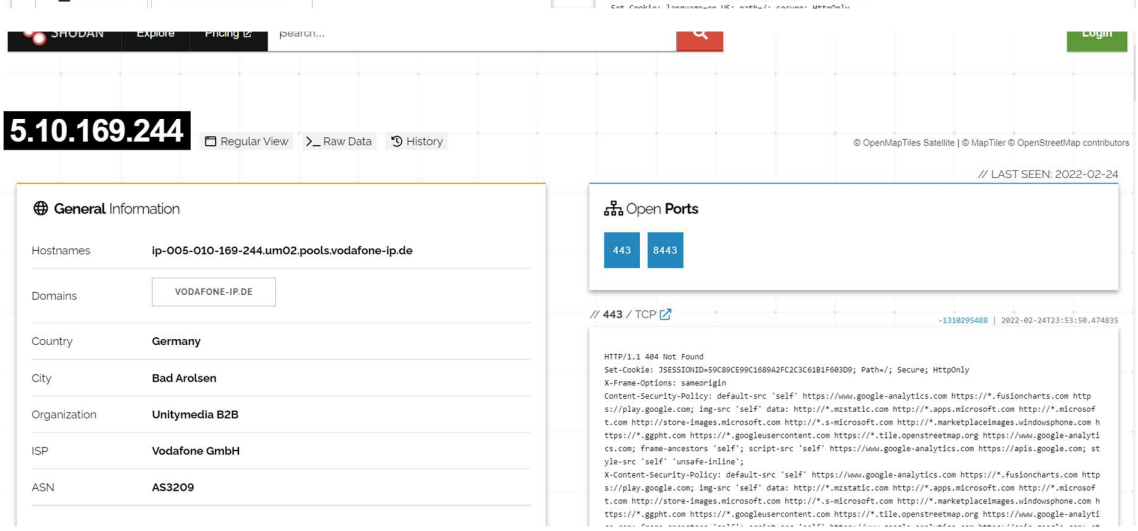
TOP PRODUCTS

- **Apache httpd 2,033**
- **Microsoft IIS httpd 1,145**
- **nginx 466**
- **Apache Tomcat/Coyote JSP engine 46**
- **Exim smtpd 20**

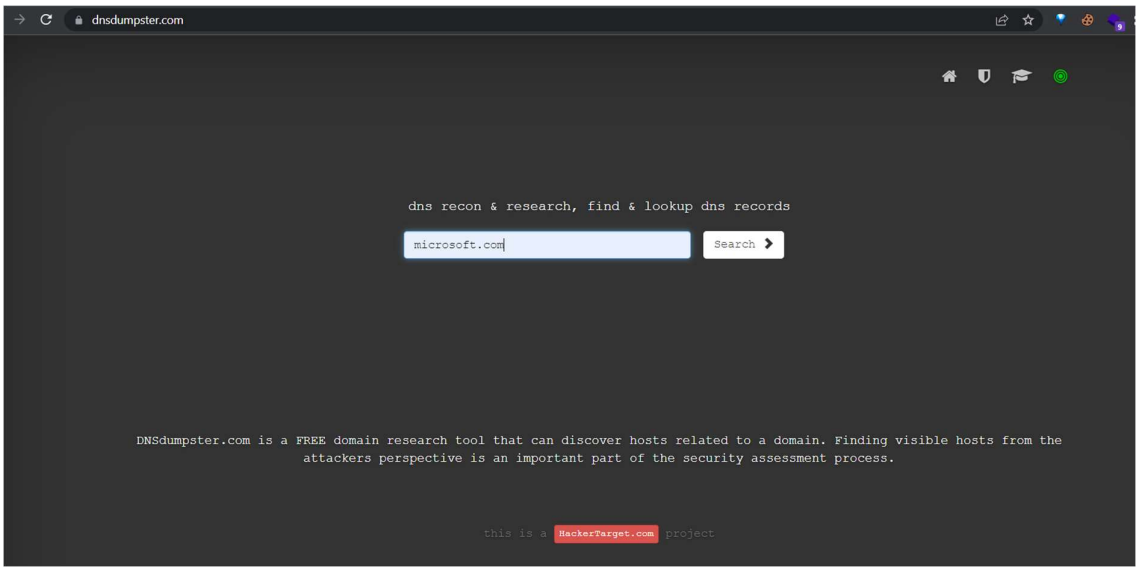
By clicking on the server available we can all the information like how many ports are open vulnerability solved etc.,


View Report
View on Map
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
Object moved
2022-02-24T23:56:02.065933
52.230.13.163
Microsoft Corporation
Singapore, Singapore
cloud
SSL Certificate
Issued By:
|- Common Name:
Microsoft Azure TLS Issuing CA 01
|- Organization:
Microsoft Corporation
Issued To:
|- Common Name:
d365fonb53fb10b733b07c09aos.cloudax.dynamics.com
|- Organization:
Microsoft Corporation
Supported SSL Versions:
TLSv1.2
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: https://login.windows.net/microsoft.com/wsfed?wa=wsignin1.0&wtrealm=spn%3a00000015-0000-0000-c000-000000
Brand Embassy
2022-02-24T23:54:32.644342
54.68.128.184
ec2-54-68-128-184.us-west-2.compute.amazonaws.com
Amazon Technologies Inc.
United States, Boardman
cloud
SSL Certificate
Issued By:
|- Common Name:
DigiCert SHA2 Secure Server CA
|- Organization:
DigiCert Inc
Issued To:
HTTP/1.1 200 OK
Date: Thu, 24 Feb 2022 23:54:32 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Set-Cookie: nette-samesite=1; path=/; secure; HttpOnly; SameSite=Strict
Set-Cookie: DFO-SESSION-ID=506pqb1128ceifa78pdnpb...


Domains
AMAZONAWS.COM
Cloud Provider
Amazon
Cloud Region
ap-southeast-2
Cloud Service
AMAZON
Country
Australia
City
Sydney
Organization
Amazon Corporate Services Pty Ltd
ISP
Amazon.com, Inc.
ASN
AS16509
Web Technologies
BOOTSTRAP
DNN
JQUERY
JQUERY UI
LIGHTBOX
MICROSOFT ASP.NET
// 80 / TCP
1136768090 | 2022-02-13T20:45:25.480305
Microsoft IIS httpd 10.0
HTTP/1.1 301 Moved Permanently
Date: Sun, 13 Feb 2022 20:45:25 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 152
Connection: keep-alive
Location: https://results.talegent.com/
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
// 443 / TCP
-606669727 | 2022-02-24T23:52:35.630317
HTTP/1.1 200 OK
Date: Thu, 24 Feb 2022 23:52:35 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 38063
Connection: keep-alive
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
X-Frame-Options: sameorigin
X-Content-TypeOptions: nosniff
Strict-Transport-Security: max-age=7776000;
Set-Cookie: dnn_IsMobile=False; path=/; secure; HttpOnly

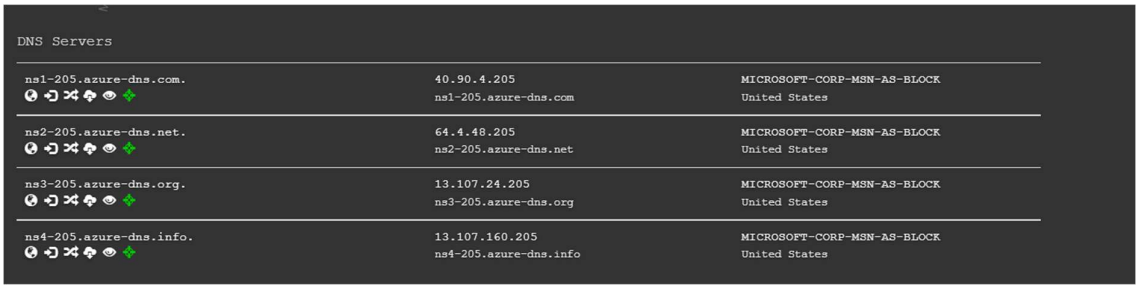

SHODAN
Explore
Pricing
Search...
Login
5.10.169.244
Regular View
Raw Data
History
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors
// LAST SEEN: 2022-02-24
General Information
Hostnames
ip-005-010-169-244.um02.pools.vodafone-ip.de
Domains
VODAFONE-IP.DE
Country
Germany
City
Bad Arolsen
Organization
Unitymedia B2B
ISP
Vodafone GmbH
ASN
AS3209
Open Ports
443
8443
// 443 / TCP
-1310295488 | 2022-02-24T23:53:50.474835
HTTP/1.1 404 Not Found
Set-Cookie: JSESSIONID=59C89CE99C16B9A2FC2C3C61B1F603D9; Path=/; Secure; HttpOnly
X-Frame-Options: sameorigin
Content-Security-Policy: default-src 'self' https://www.google-analytics.com https://*.fusioncharts.com http
s://play.google.com; img-src 'self' data: http://*.mzstatic.com http://*.apps.microsoft.com http://*.microsof
t.com http://store-images.microsoft.com http://*.s-microsoft.com http://*.marketplaceimages.windowsphone.com h
ttps://*.ggpht.com https://*.googleusercontent.com https://*.tile.openstreetmap.org https://www.google-analyti
cs.com; frame-ancestors 'self'; script-src 'self' https://www.google-analytics.com https://apis.google.com; st
yle-src 'self' 'unsafe-inline';
X-Content-Security-Policy: default-src 'self' https://www.google-analytics.com https://*.fusioncharts.com http
s://play.google.com; img-src 'self' data: http://*.mzstatic.com http://*.apps.microsoft.com http://*.microsof
t.com http://store-images.microsoft.com http://*.s-microsoft.com http://*.marketplaceimages.windowsphone.com h
ttps://*.ggpht.com https://*.googleusercontent.com https://*.tile.openstreetmap.org https://www.google-analyti

7) Gathering information from dnsdumpster
https://dnsdumpster.com/



Hosting (IP block owners)

Name DNS server name with IP address and which country is maintaining the server.



DNS Servers

ns1-205.azure-dns.com.	40.90.4.205 ns1-205.azure-dns.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns2-205.azure-dns.net.	64.4.48.205 ns2-205.azure-dns.net	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns3-205.azure-dns.org.	13.107.24.205 ns3-205.azure-dns.org	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns4-205.azure-dns.info.	13.107.160.205 ns4-205.azure-dns.info	MICROSOFT-CORP-MSN-AS-BLOCK United States

MX Records →This is where email for the domain goes…

10 microsoft-com.mail.protection.outlook.com.	40.93.212.0	MICROSOFT-CORP-MSN-AS-BLOCK United States

TXT Records →Find more hosts in sender policy framework (SPF) configurations.

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"docusign=d5a3737c-c23c-4bd0-9095-d2ff621f2840"

"v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com include:_spf1-meo.microsoft.com -all"

"adobe-sign-verification=c1fea9b4cdd4df0d5778517f29e0934"

"docusign=52998482-393d-46f7-95d4-15ac6509bfdd"

"adobe-idp-site-verification=8aa35c528af5d72beb19b1bd3ed9b86d87ea7f24b2ba3c99ffcd00c27e9d809c"

"d365mktkey=4d8bnycx40fy3581petta4gsf"

"8RPDXjBzBS9tu7Pbysu7qCACrwXPoDV8ZtLfthTnC4y9VJFLd84it5sQlEITg8LJ4KOIA8pBZxmyvPujuUvhOg=="

"google-site-verification=1TeK8q0OziFl4T1tF-QR65JkzHZ1rcdgNccDFp78iTk"

"d365mktkey=3uc1cf82cpv750lzk70v9bvf2"

"facebook-domain-verification=fwzwhbbzwmg5fzgotc2go51olc3566"

"apple-domain-verification=0gMeaYyYy6GLViGo"

"google-site-verification=pjPOauSPcrfXOZS9jnPPa5axowcHGCDAl1_86dCqFpk"

"fg2t0gov9424p2tdcuo94goe9j"

"t7sebee51jrj7vm932k531hipa"

"google-site-verification=M--CVfn_YwsV-2FGbCp_HFaEj23BmT0cTF418hXgpvM"

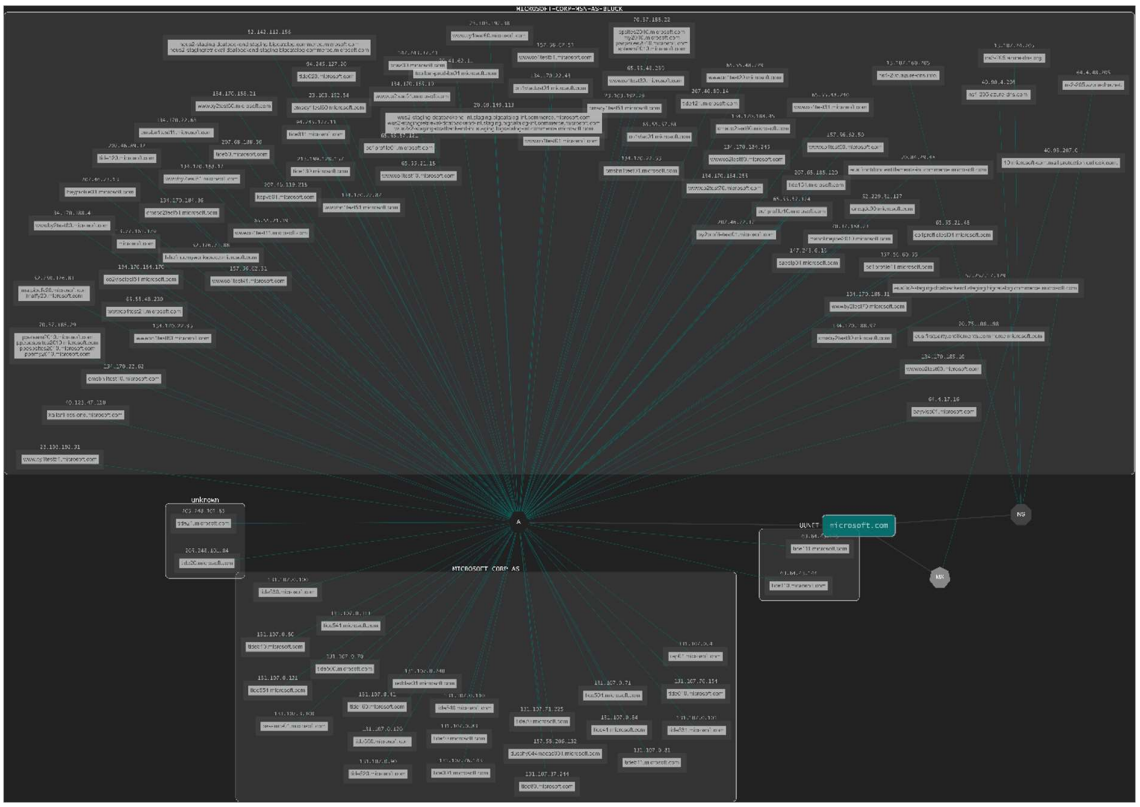
"pbcpcw84sfk7w4nhm7dwyg2k3gx0t4xr"

Host Records

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

microsoft.com HTTP: Kestrel HTTPS: Kestrel	13.77.161.179	MICROSOFT-CORP-MSN-AS-BLOCK United States
wwwcoltest10.microsoft.com	65.55.21.18 wwwcoltest10.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide620.microsoft.com	94.245.127.20 tide620.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK Ireland
wwwcoltest21.microsoft.com	65.55.48.230 wwwcoltest21.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
kailani-ess.one.microsoft.com HTTPS: Microsoft-IIS/10.0 HTTPS TECH: IIS,10.0	40.123.47.110	MICROSOFT-CORP-MSN-AS-BLOCK United States
wus2-staging-dcatbackend-int.staging.bigcatalog-int.commerce.microsoft.com	20.69.149.113	MICROSOFT-CORP-MSN-AS-BLOCK United States
colprofile11.microsoft.com	157.56.60.55 colprofile11.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
ppeteam2010.microsoft.com	70.37.188.29 ppe2010my.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide550.microsoft.com	131.107.0.120 tide550.microsoft.com	MICROSOFT-CORP-AS United States
tide541.microsoft.com	131.107.0.111 tide541.microsoft.com	MICROSOFT-CORP-AS United States
wwwcoltest30.microsoft.com	65.55.48.239	MICROSOFT-CORP-MSN-AS-BLOCK

Infrastructure of the website



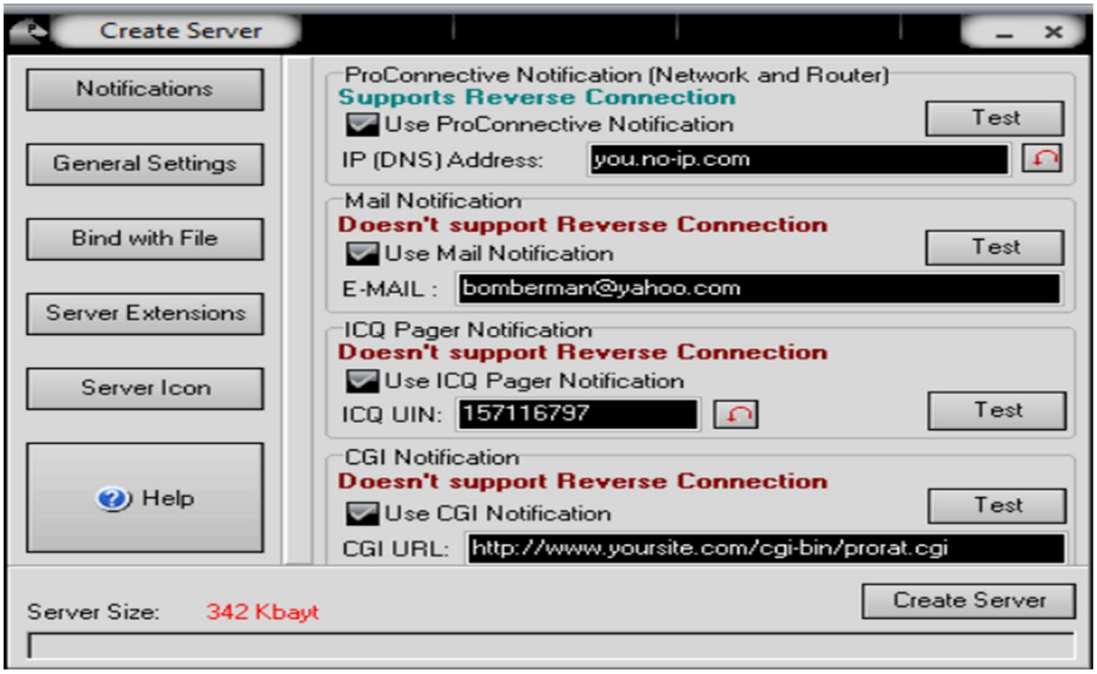
Foot printing countermeasures:-

a) Limit employee access to social networking sites via the organization's network
b) Setup web servers to prevent data leakage.
c) Teach employees how to utilize pseudonyms in blogs, discussion groups, and forums.
d) Don't expose sensitive information in press releases, yearly reports, or other public documents.
e) Keep the amount of information you share with the public to a minimum.
f) Apply the same foot printing procedures to find and remove any sensitive information that is publicly accessible.
g) Use anonymous registration services to prevent search engines from caching a webpage.
h) In the web servers, disable directory listing.
i) Use the who-is lookup database's privacy services.
j) Protect sensitive information by encrypting it and using a password.

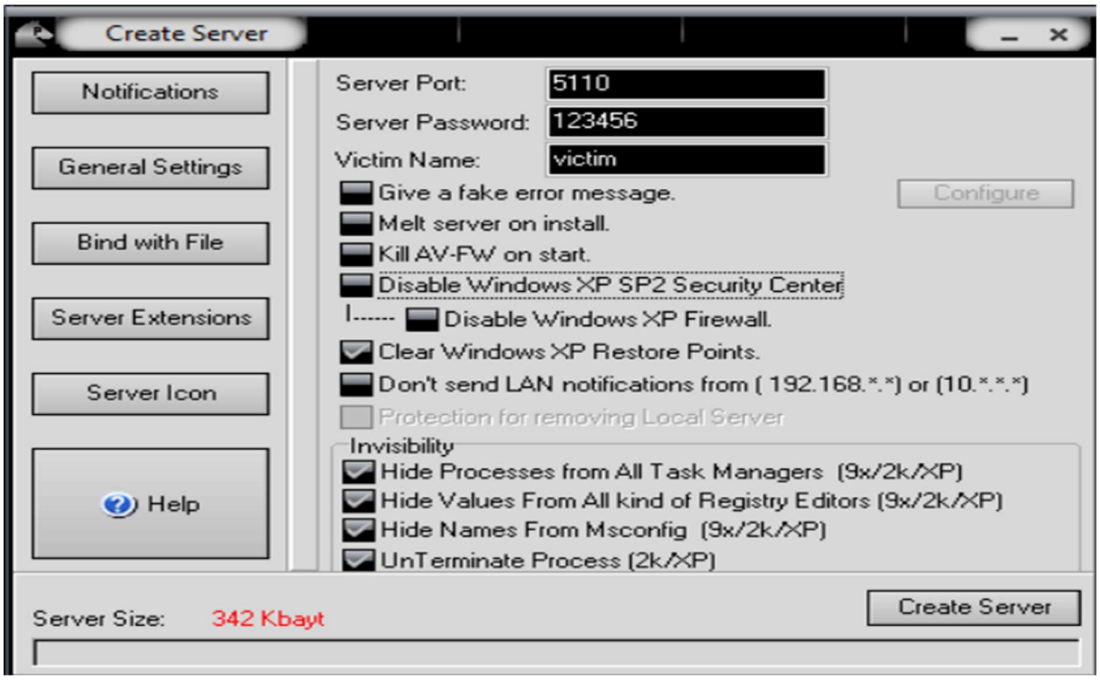
PRORATE TOOL

1) Download and install the Prorat Tool.
2) Download any image or file so that we can bind the malicious file into it.

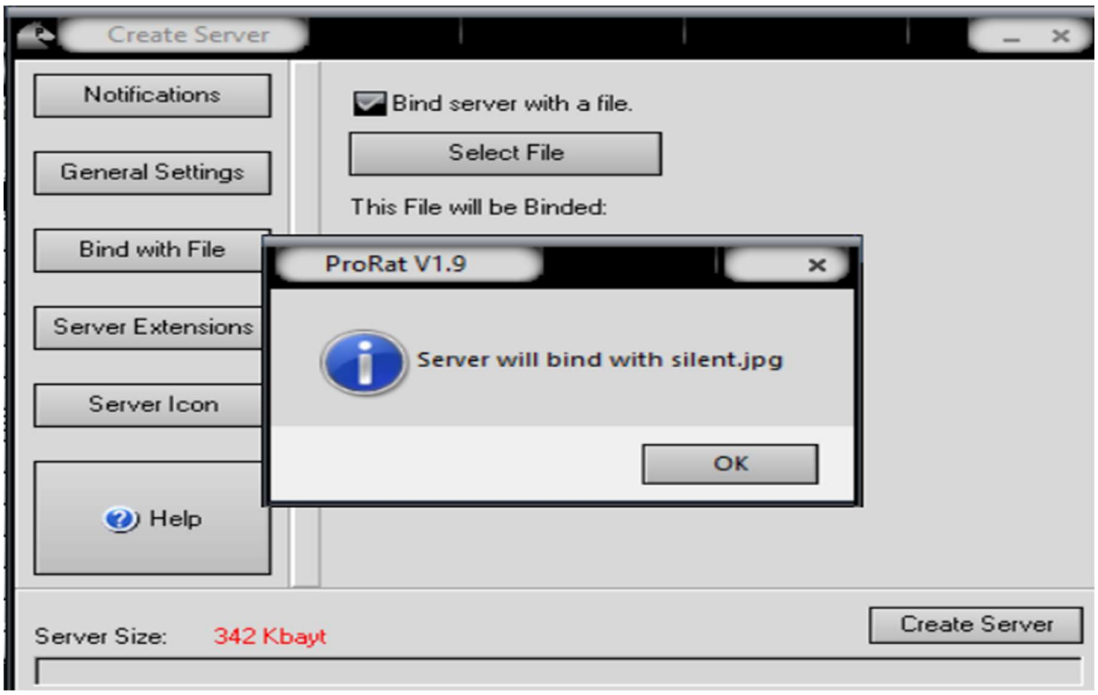
3) Now create a malicious file from the prorate tool as shown in the below image.



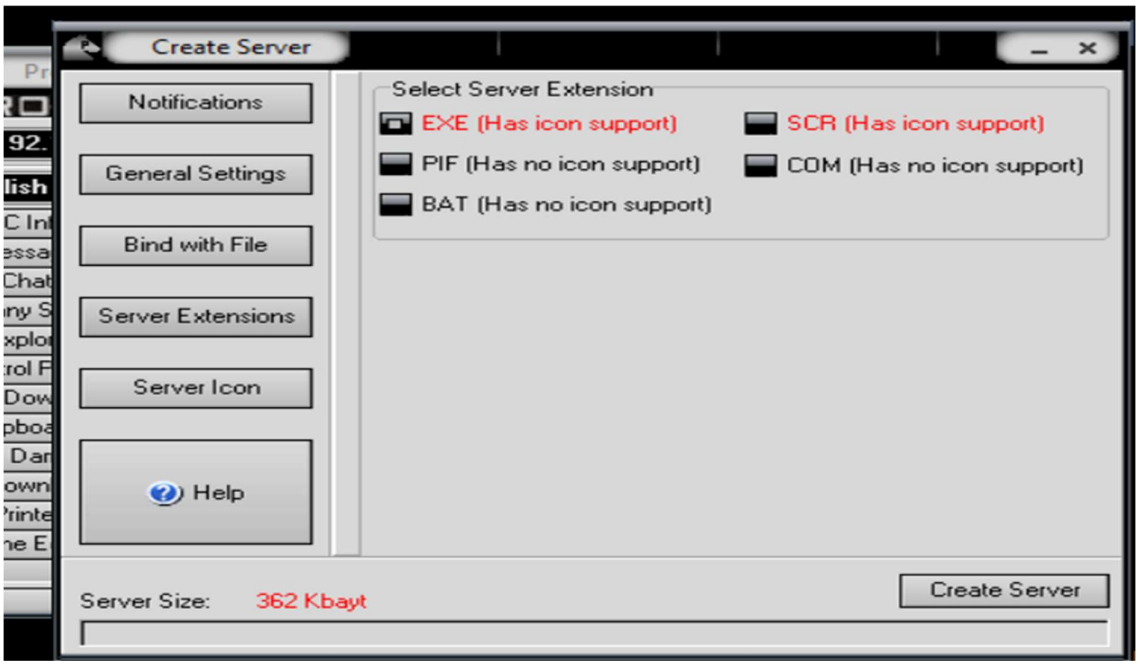
4) Now create a server port and password with a victim name and disable all the settings as per necessary.



5) Now select a file or image which is need to bind and bind it with a malicious code.

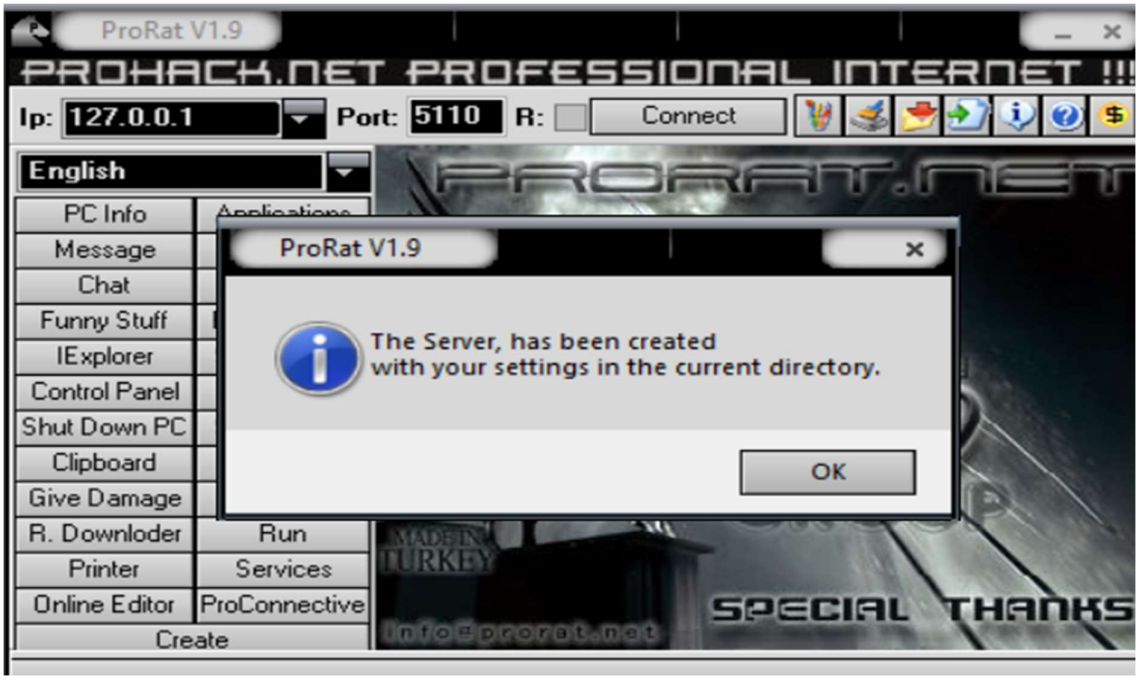


6) Check the server Extension make sure that the file extension is .exe file.

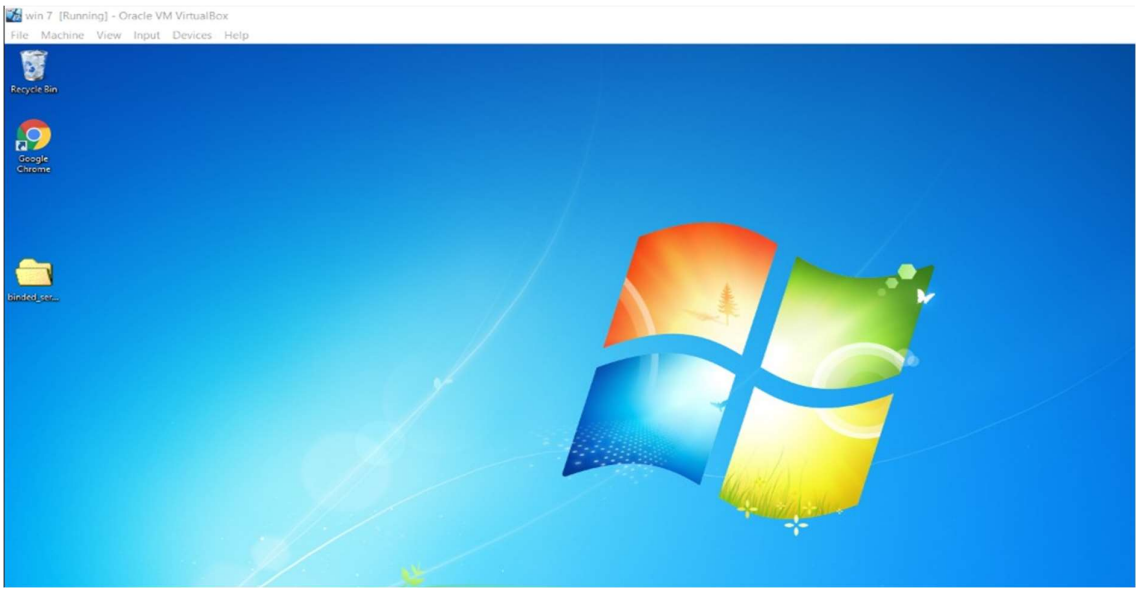


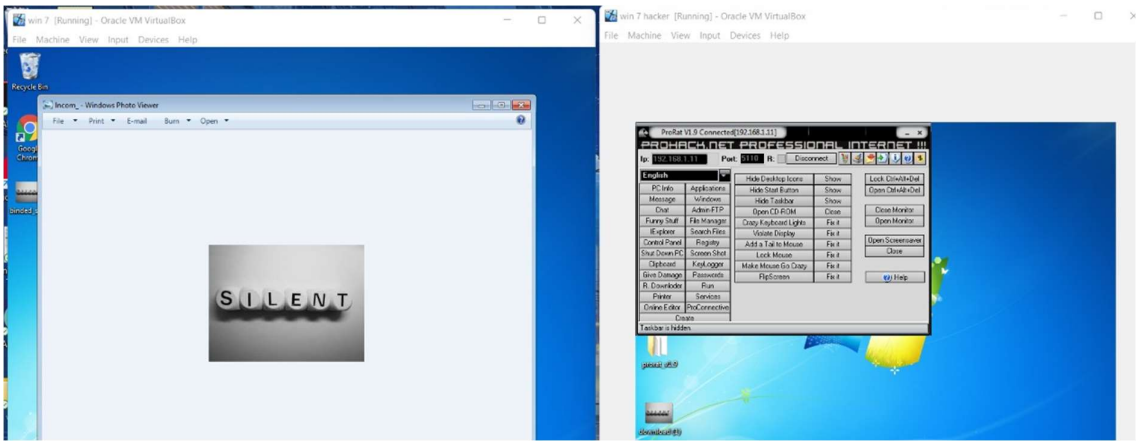
7) Now select the file icon as per your choice and on create server.

8) Now we can that the malicious image /file is created and share the folder with victim system.

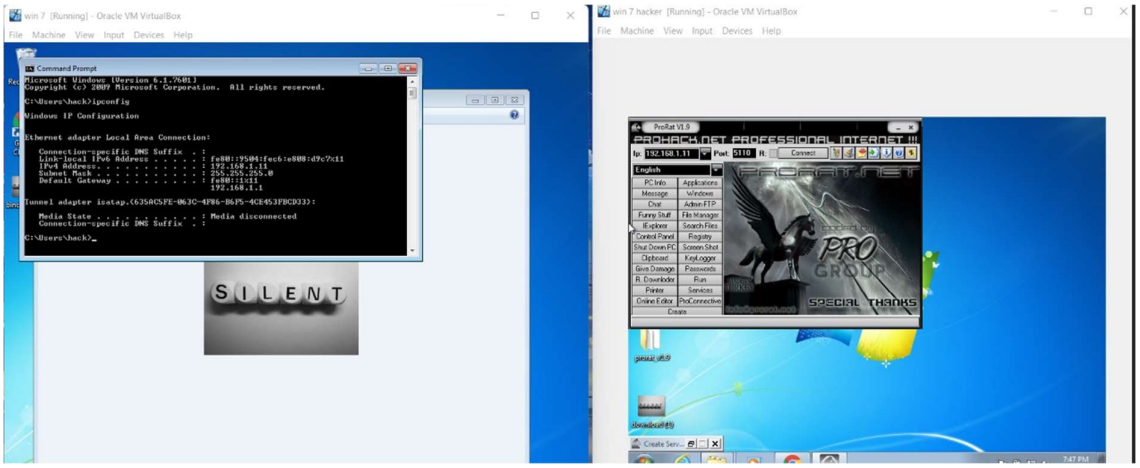


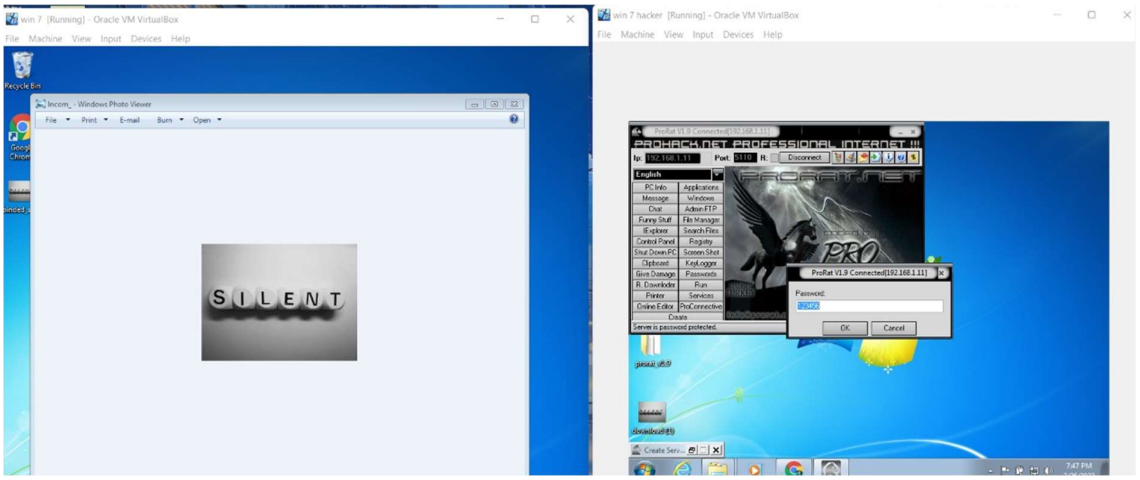
9) We can see the folder in victim system, when victim try to open the folder we get access of the victim system.



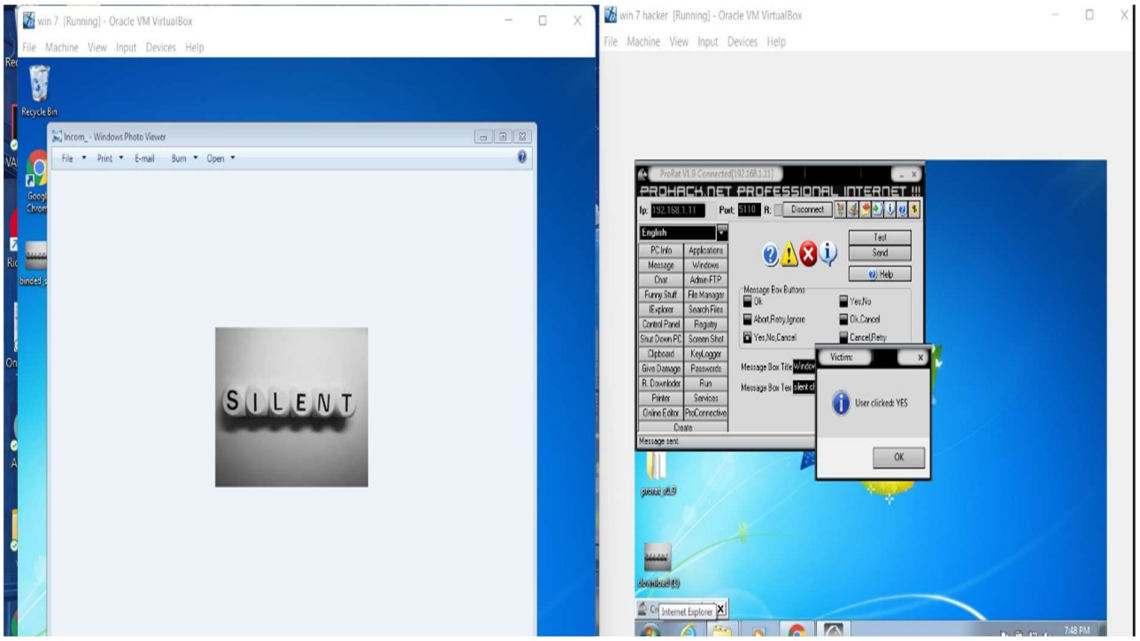


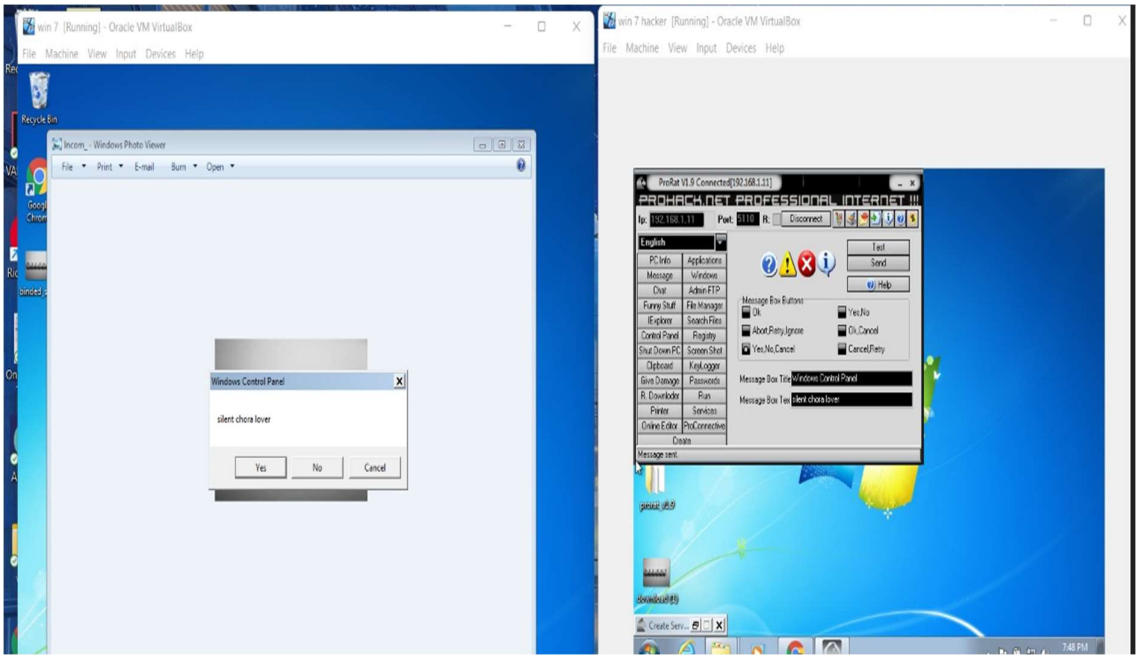
10) Now get the victim IP address and the type in the prorat tool with correct port number and try to connect it.



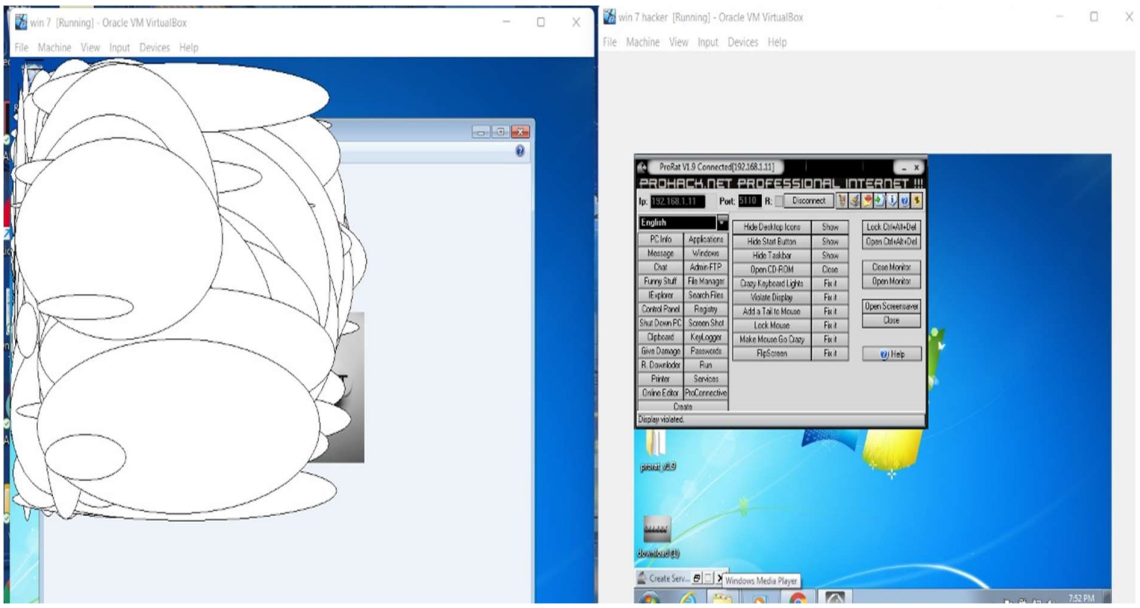


11) We can send pop up messages and funny alert messages.

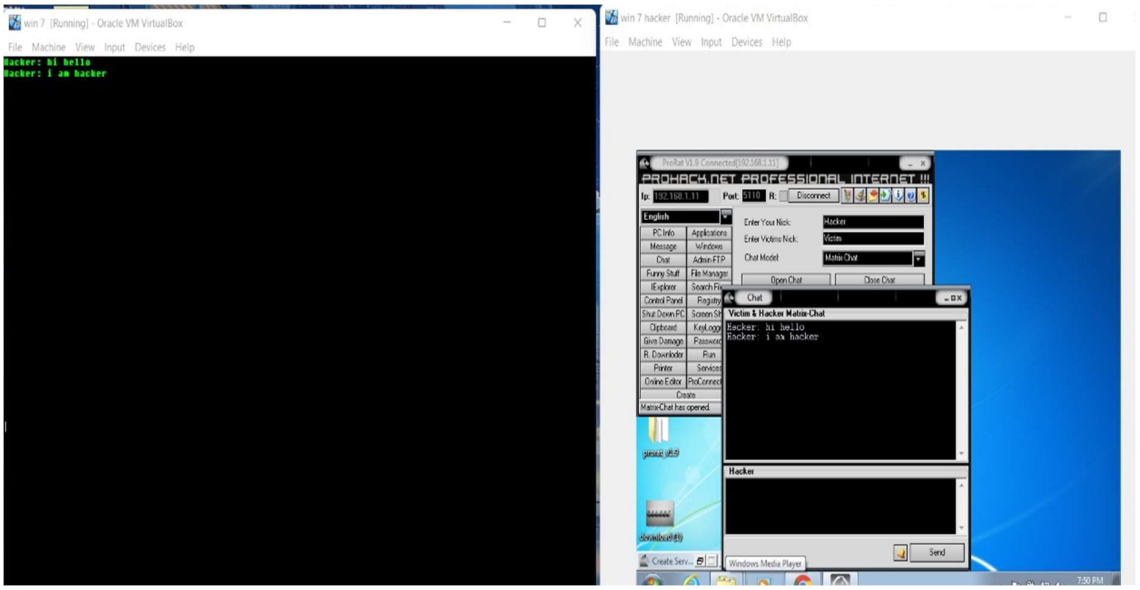


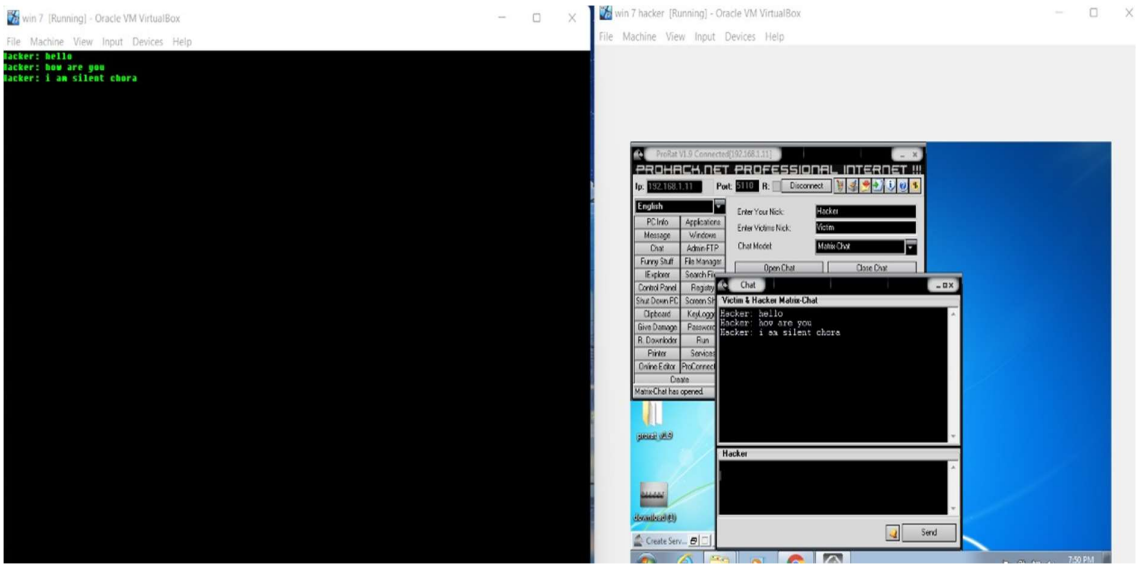


12) We can send scrambled images funny stuffs.

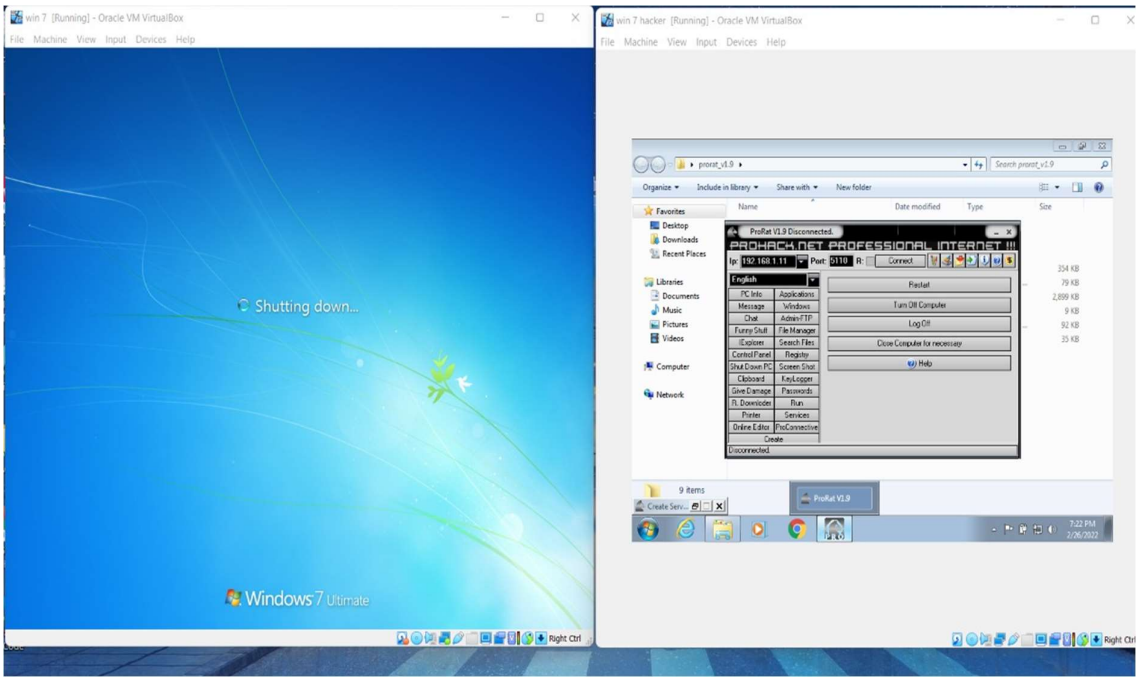


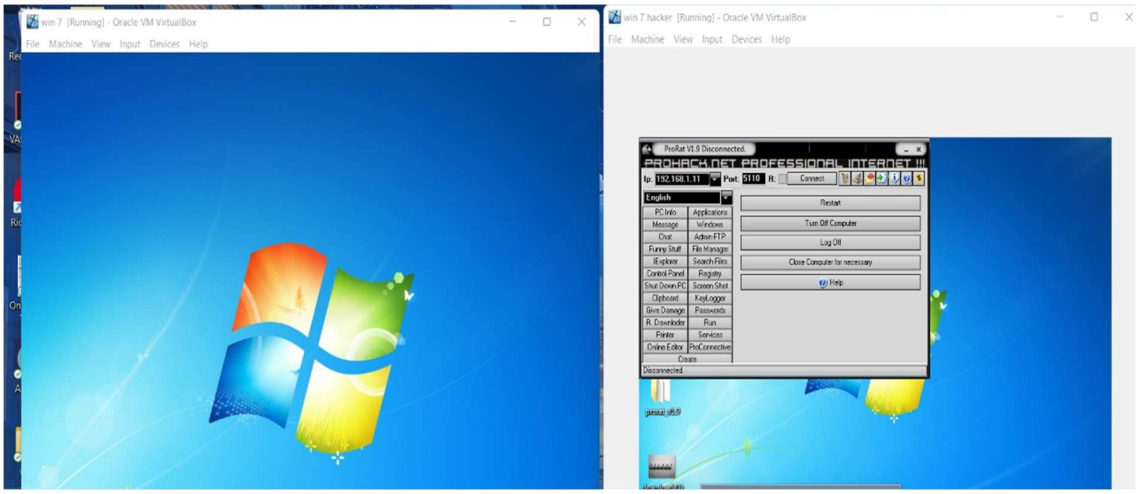
13) We can do matrix chatting and funny chatting.





14) We can access the victim computer and shutdown or restart the system.





How to avoid these type of attacks:

1) Never install or download software from a source you don't totally trust.

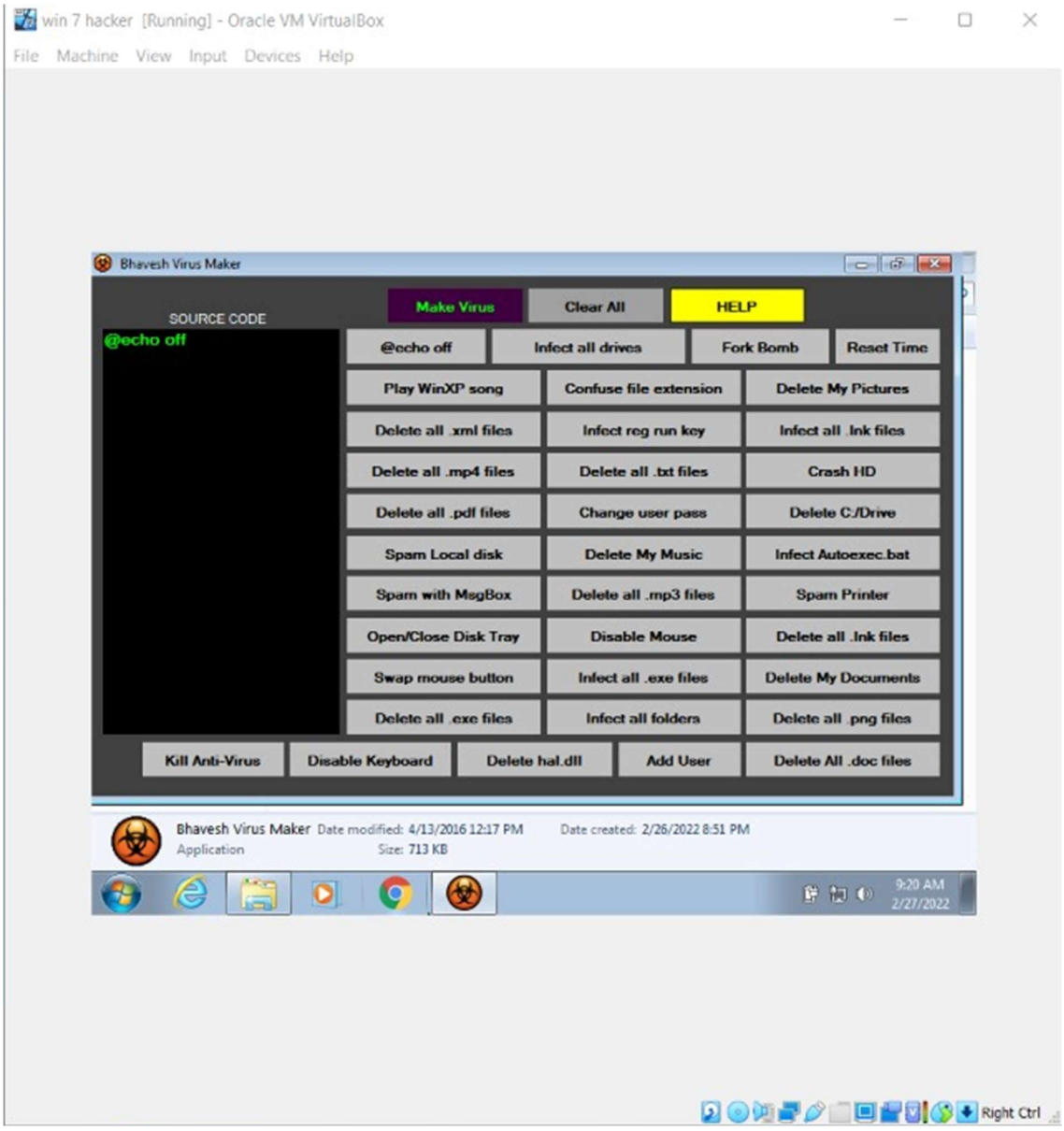
2) Never open an attachment or launch a programme supplied to you by an unknown sender in an email.

3) Keep all of your computer's software up to date with the most recent fixes.

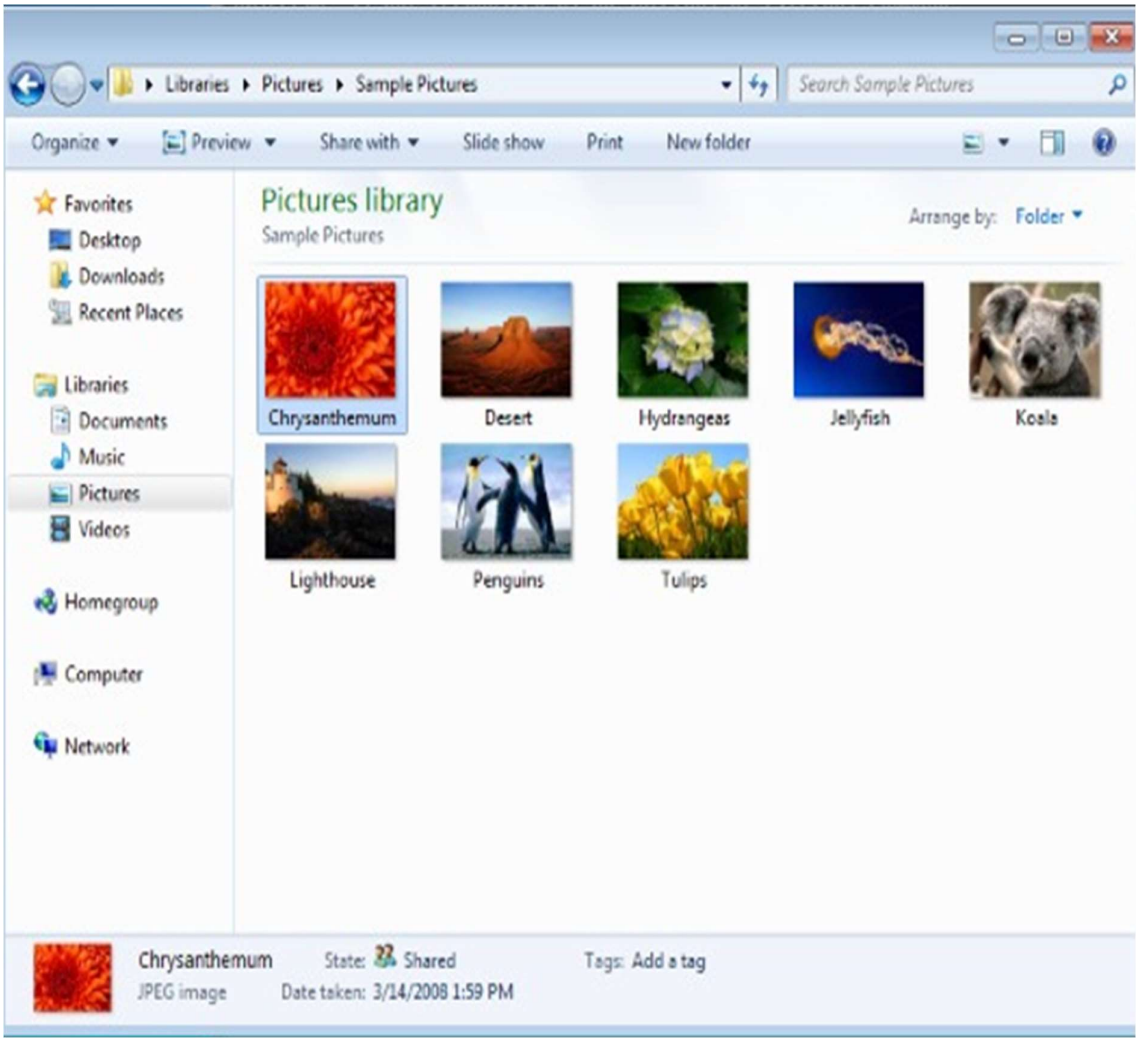
4) Make sure your machine has a trojan antivirus programme installed and functioning.

BVM TOOL

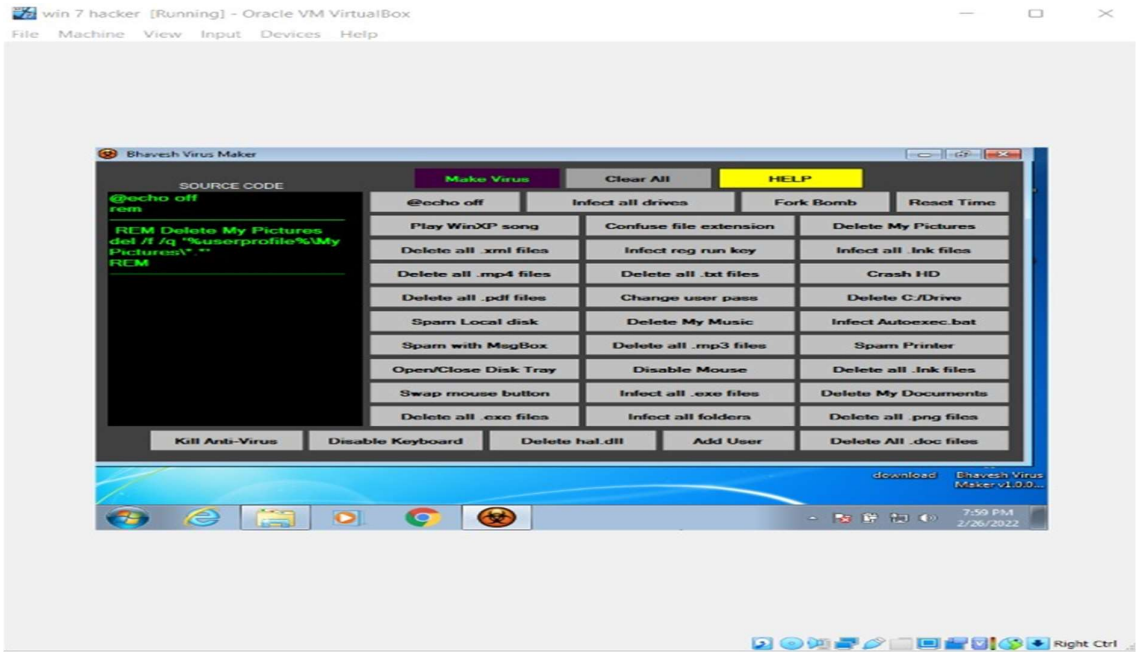
1) Firstly download and install BVM (Bhavesh virus Maker) tool from the given link.
https://sourceforge.net/projects/bhavesh-virus-maker/

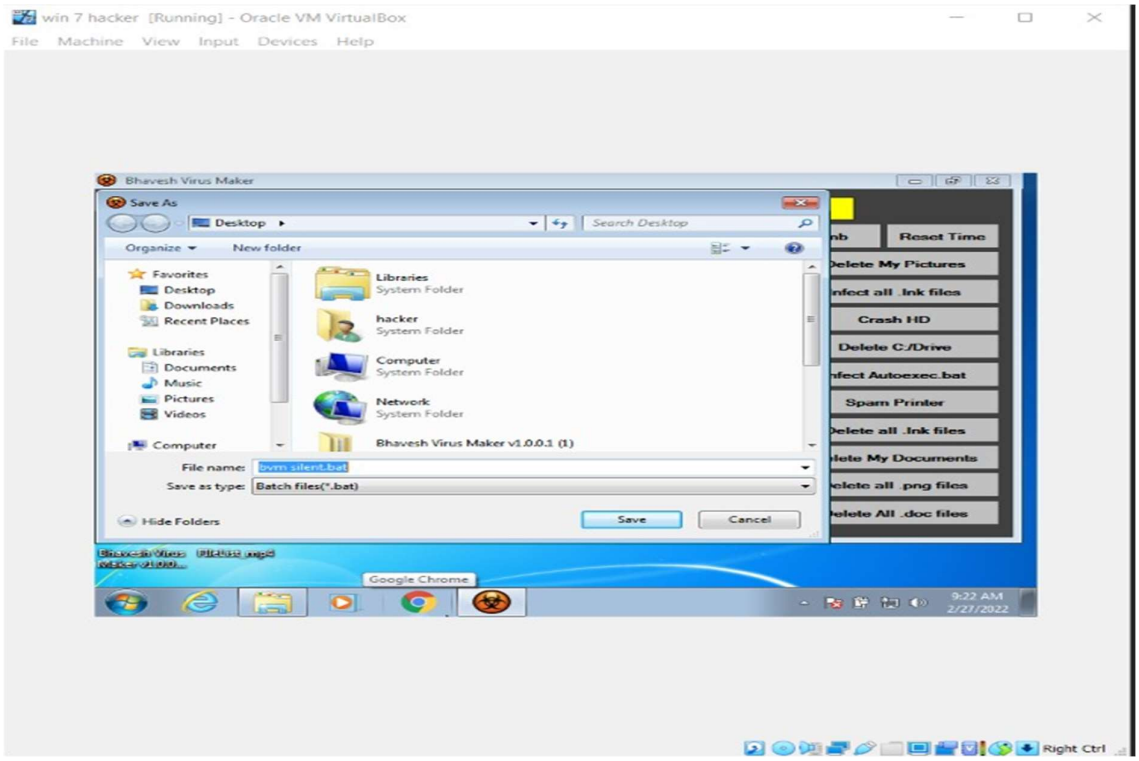


2) We can see pictures in the system before the attack to delete all the files we here create a virus using BVM tool.

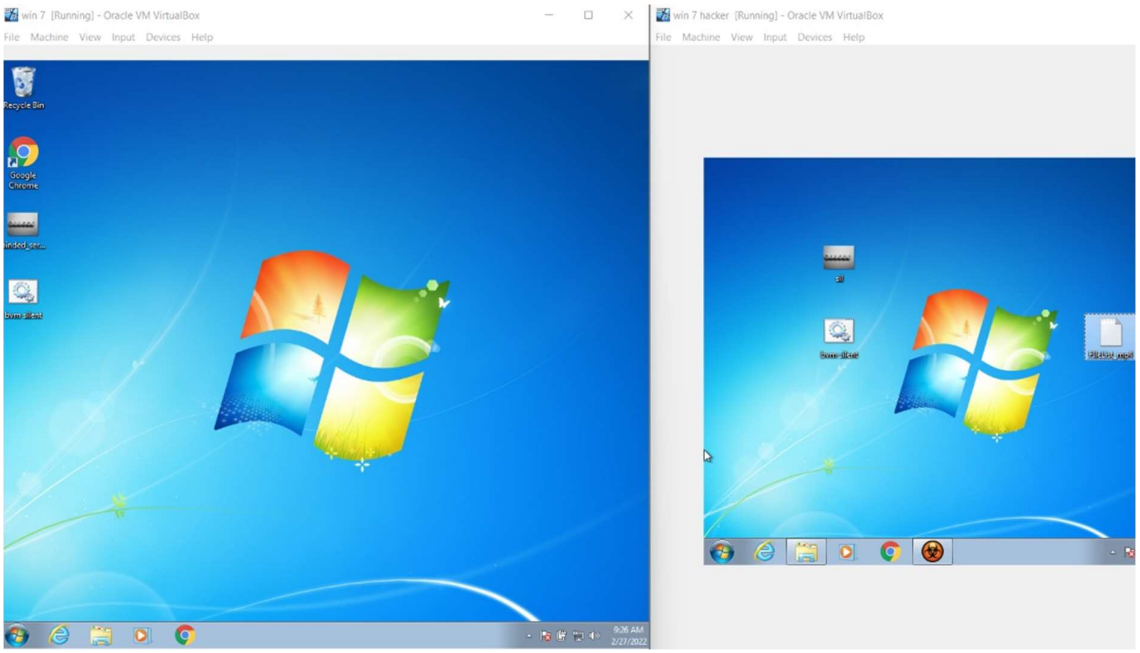


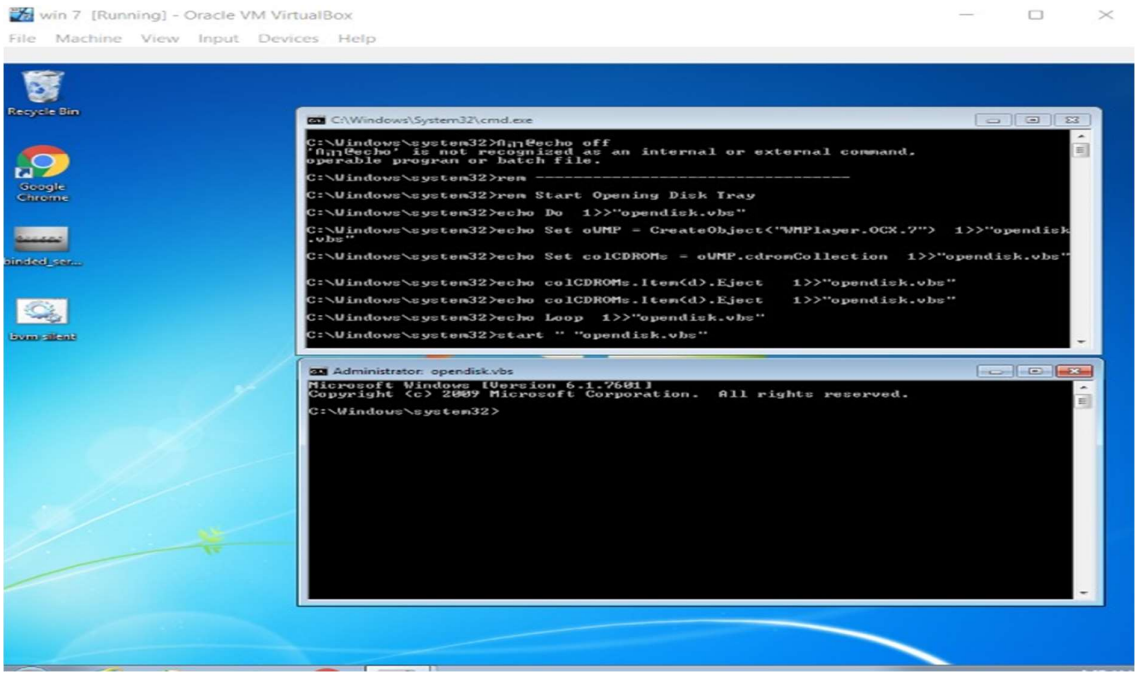
3) Now create a virus by click on delete my pictures and download a virus file and share with victim.



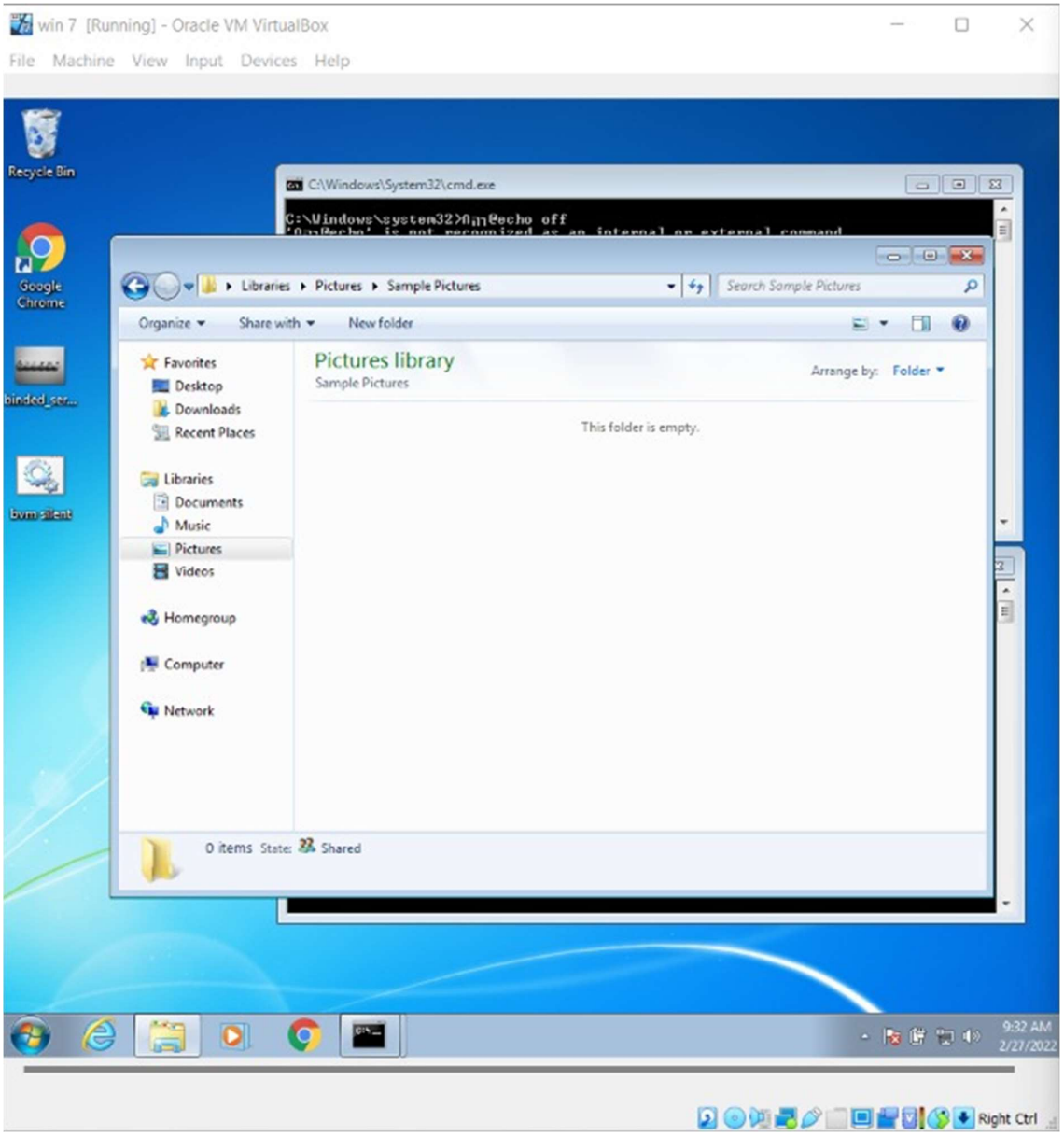


4) We can see that the virus file is shared with victim system.





5) We can see that all the images in the victim file are deleted.



6) We can do so many attacks and delete the files c-drive folder, crash the system or spam folder or file.

The preventive measures to avoid this malware affect:

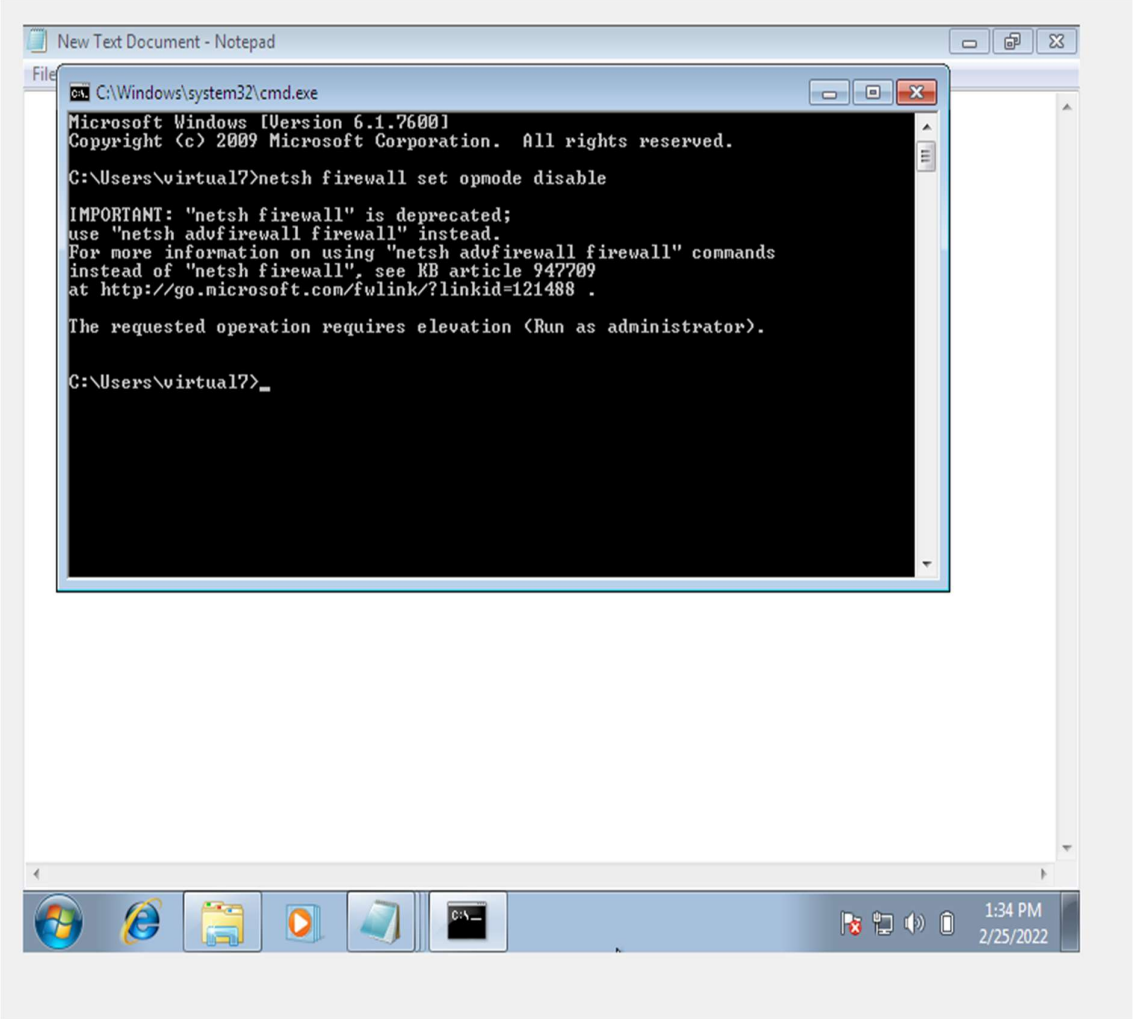
1) Anti-virus software should be installed.
2) Update your software on a regular basis.
3) Apps should only be purchased from reputable sources.
4) Don't open attachments from unfamiliar sources or click on dodgy websites.
5) Set up a firewall.
6) Backup your files on a regular basis.

BATCH PROGRAM

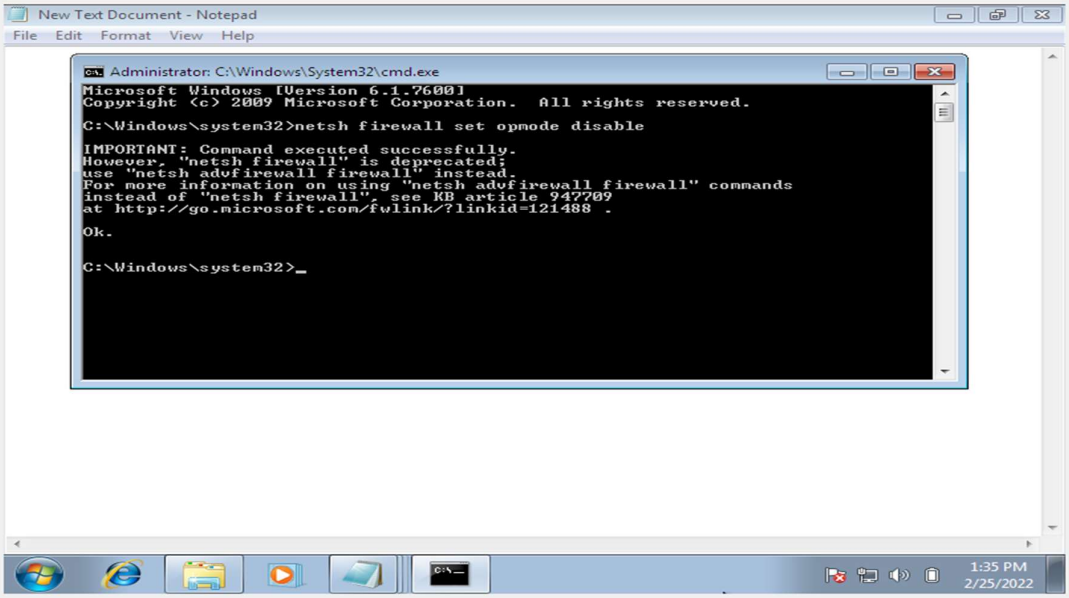
1) To disable firewall using CMD Prompt

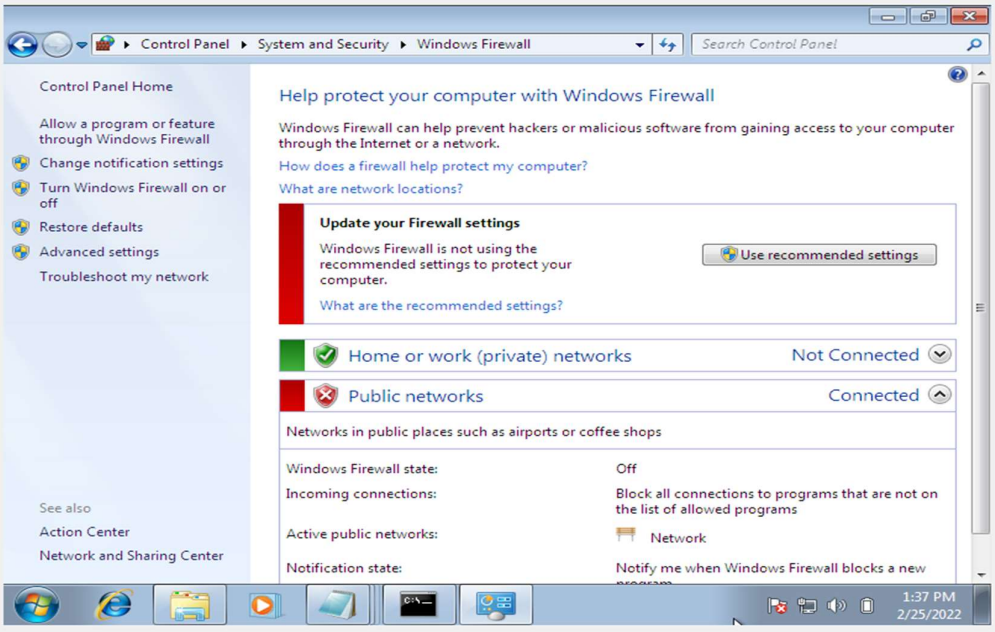
netsh firewall set opmode disable

Here we can see that it is asking for administrator.

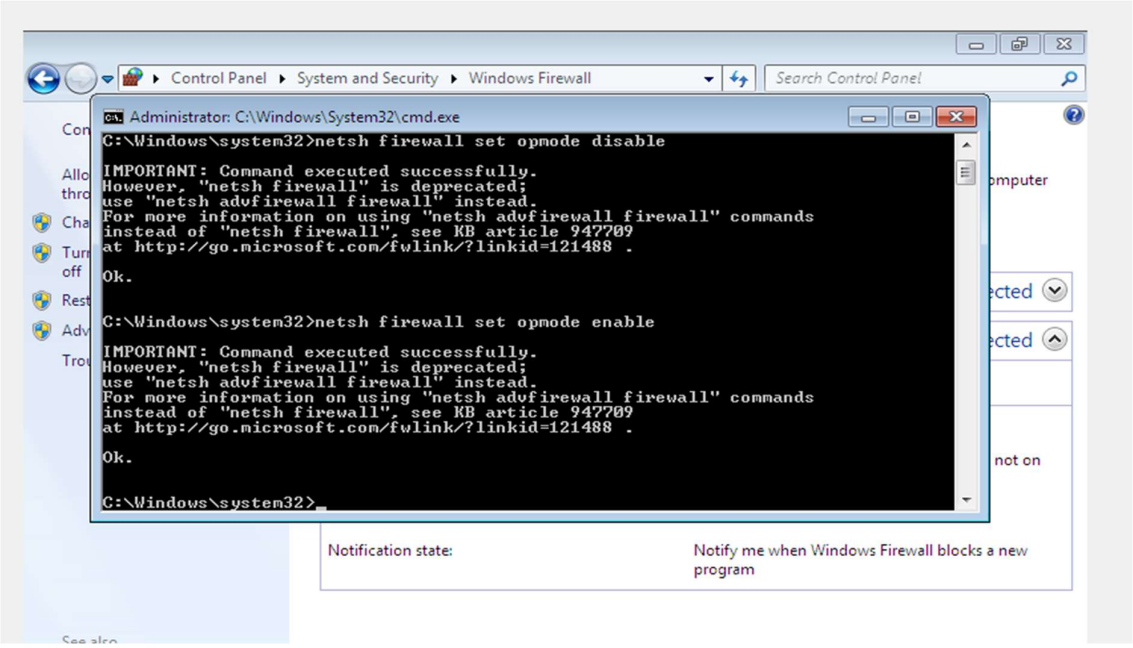


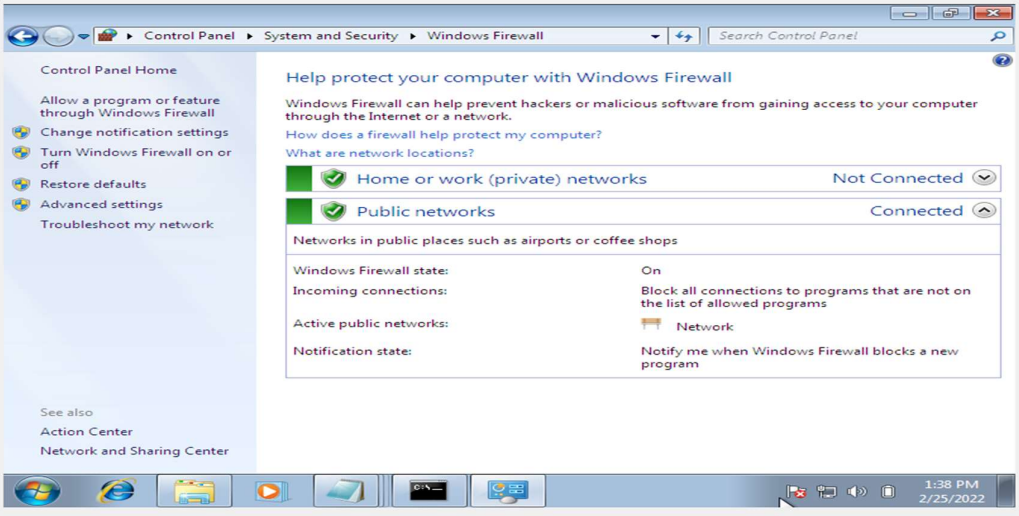
2) After running with administrator, the firewall is disabled.



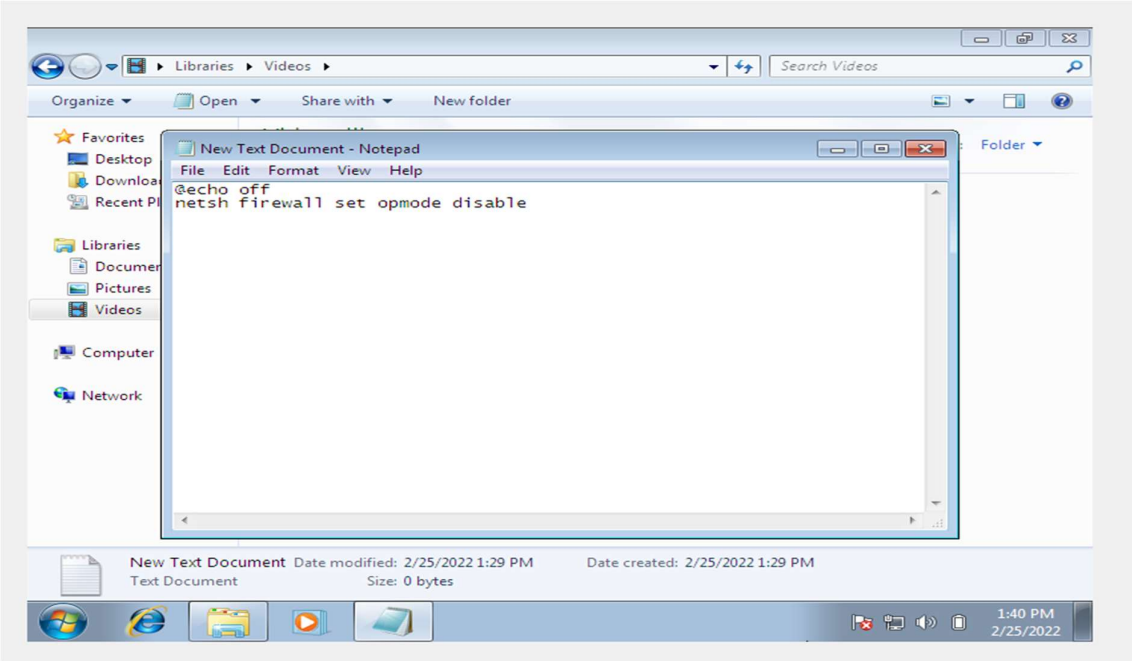


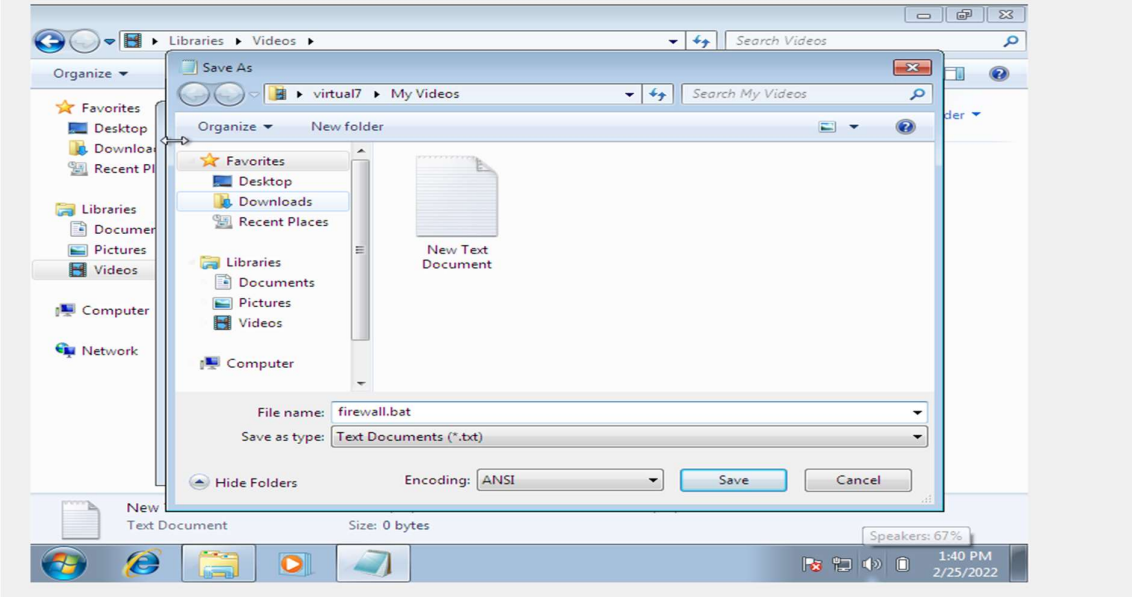
3) To enable the firewall use the following command
netsh firewall set opmode enable



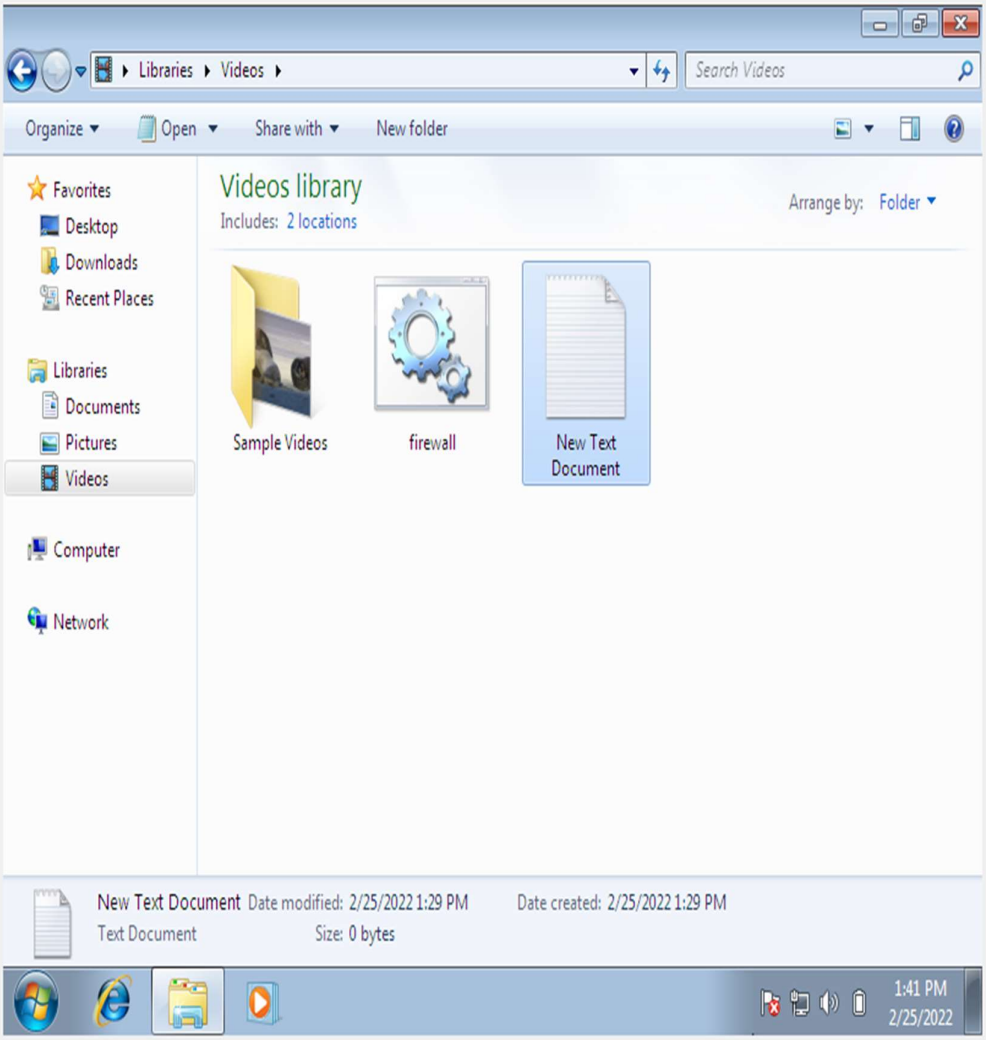


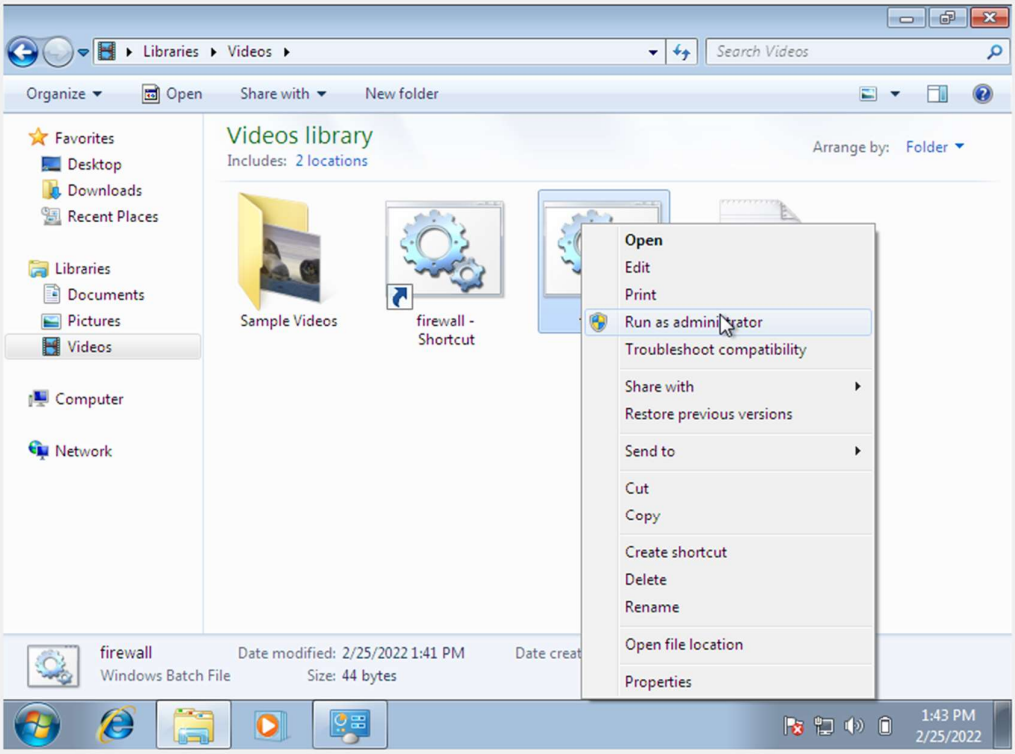
4) Disabling Firewall of victim computer using Batch program with .bat extension.
5) Firstly create a text and write the command and save it with .bat extension.

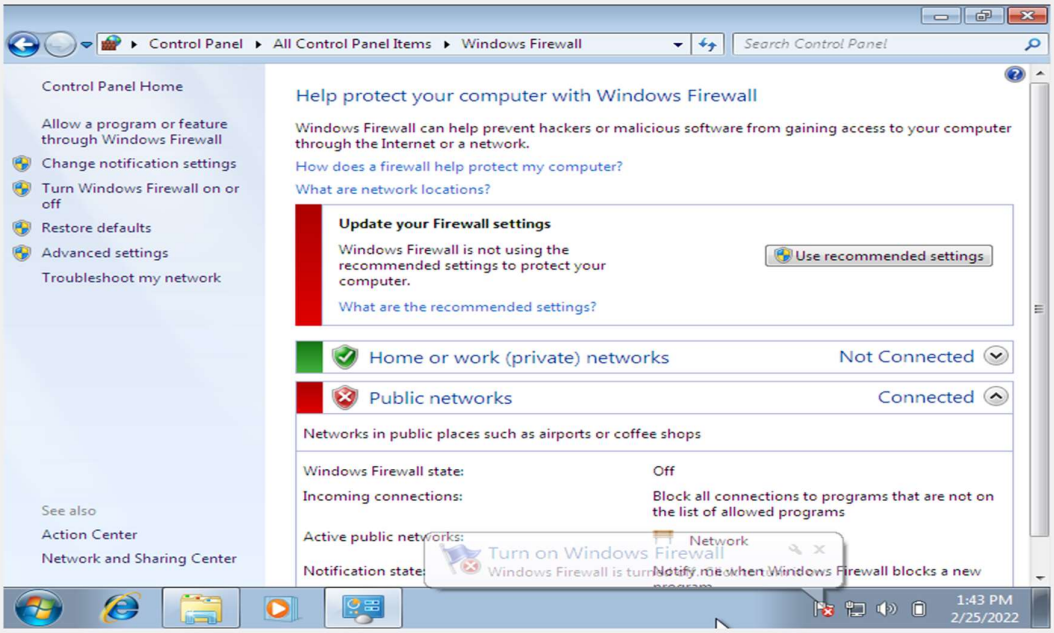




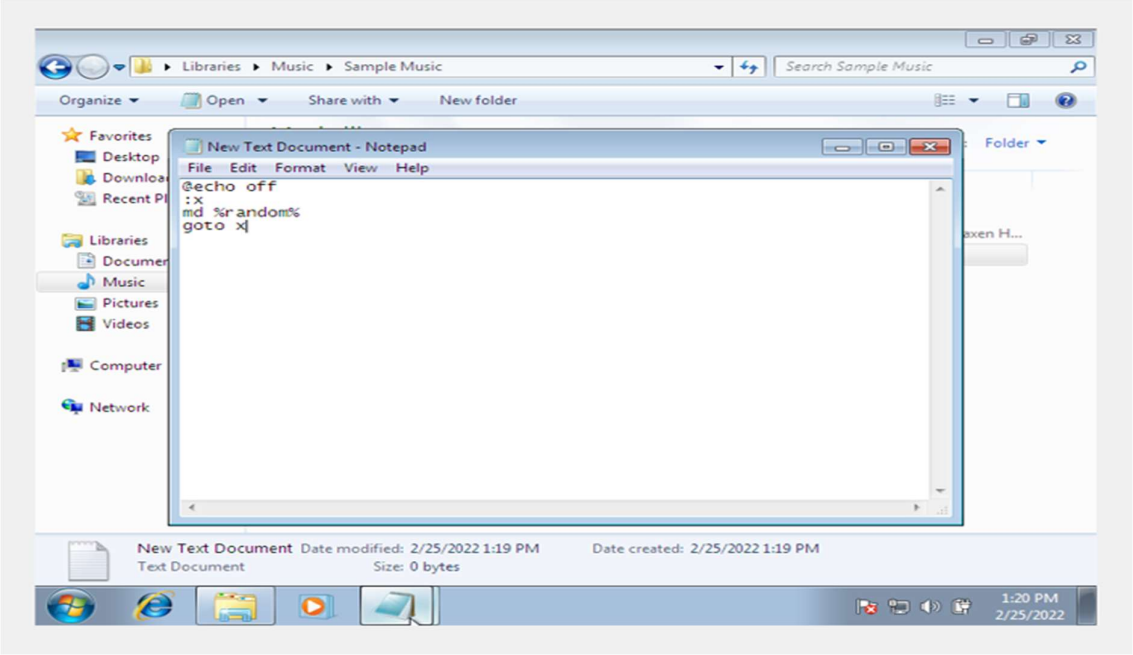
6) We can see .bat extension file share this file to victim.
7) When victim open the file the firewall of the system automatically disable.



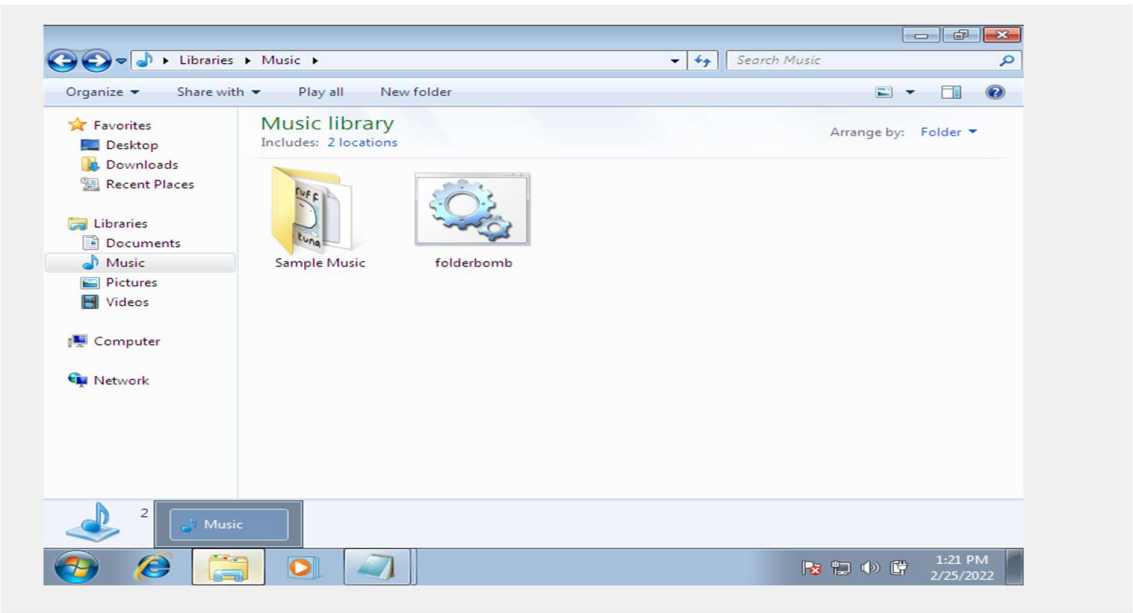

Libraries ▸ Videos ▸
Search Videos
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Pictures
Videos
Computer
Network
Videos library
Includes: 2 locations
Arrange by: Folder
Sample Videos
firewall - Shortcut
Open
Edit
Print
Run as administrator
Troubleshoot compatibility
Share with
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Open file location
Properties
firewall
Windows Batch File
Date modified: 2/25/2022 1:41 PM
Size: 44 bytes
1:43 PM
2/25/2022


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Help protect your computer with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
Update your Firewall settings
Windows Firewall is not using the recommended settings to protect your computer.
What are the recommended settings?
Use recommended settings
Home or work (private) networks
Not Connected
Public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state:
Off
Incoming connections:
Block all connections to programs that are not on the list of allowed programs
Active public networks:
Network
Notification state:
Notify me when Windows Firewall blocks a new
Turn on Windows Firewall
Windows Firewall is turn
1:43 PM
2/25/2022

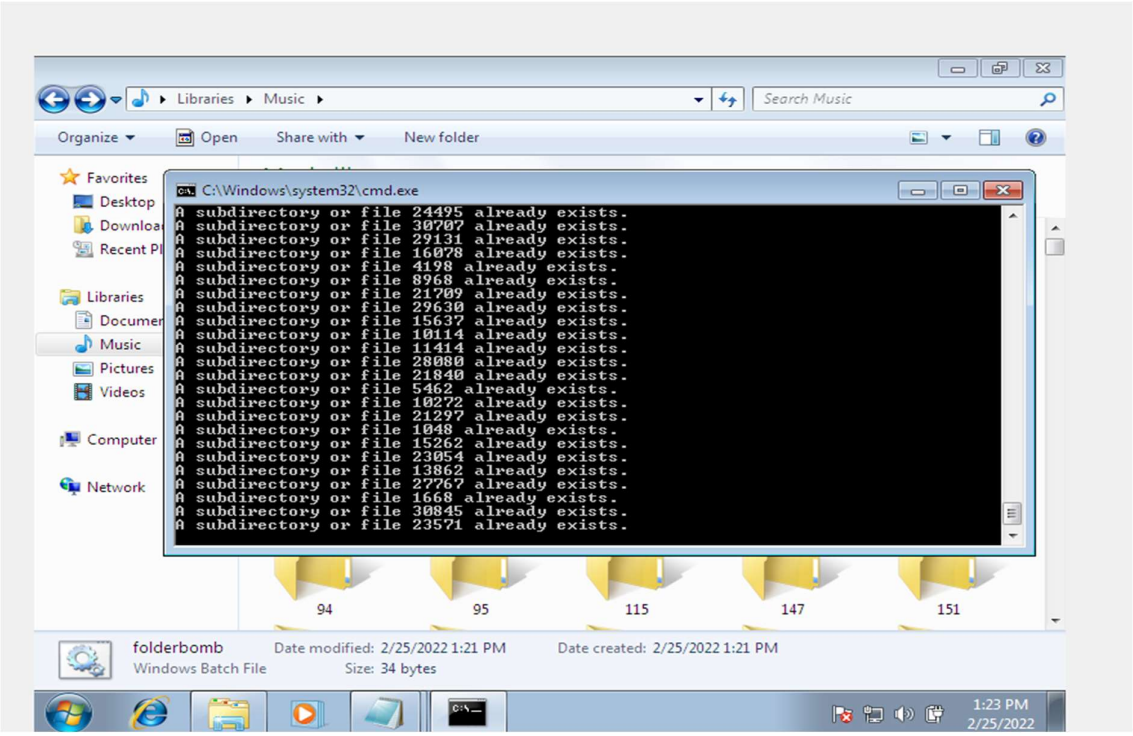
8) Creating infinite folders in victim system.
9) Firstly write a command in text file and save it with .bat extension file.

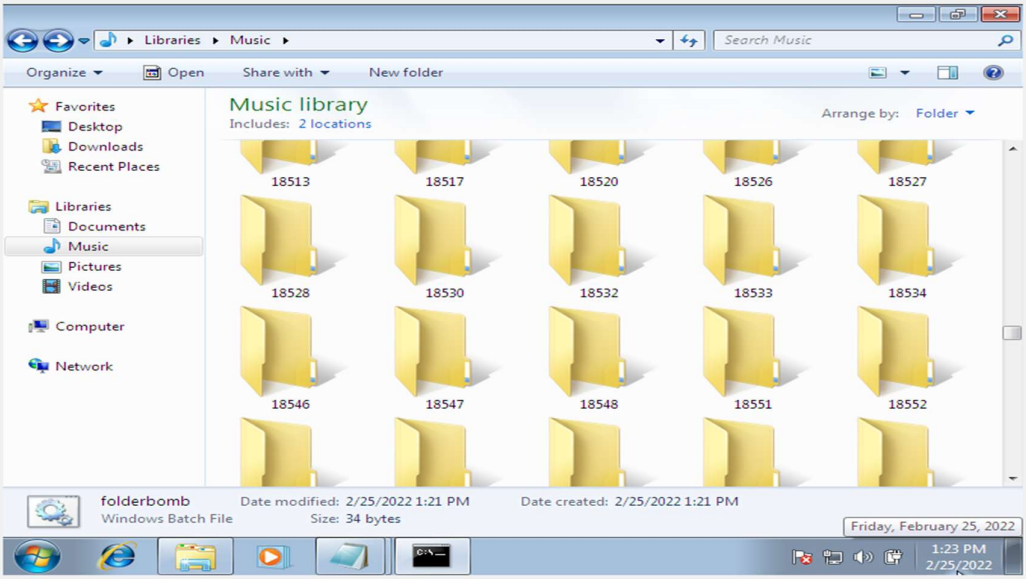


10) We can see the .bat extension file in music folder.

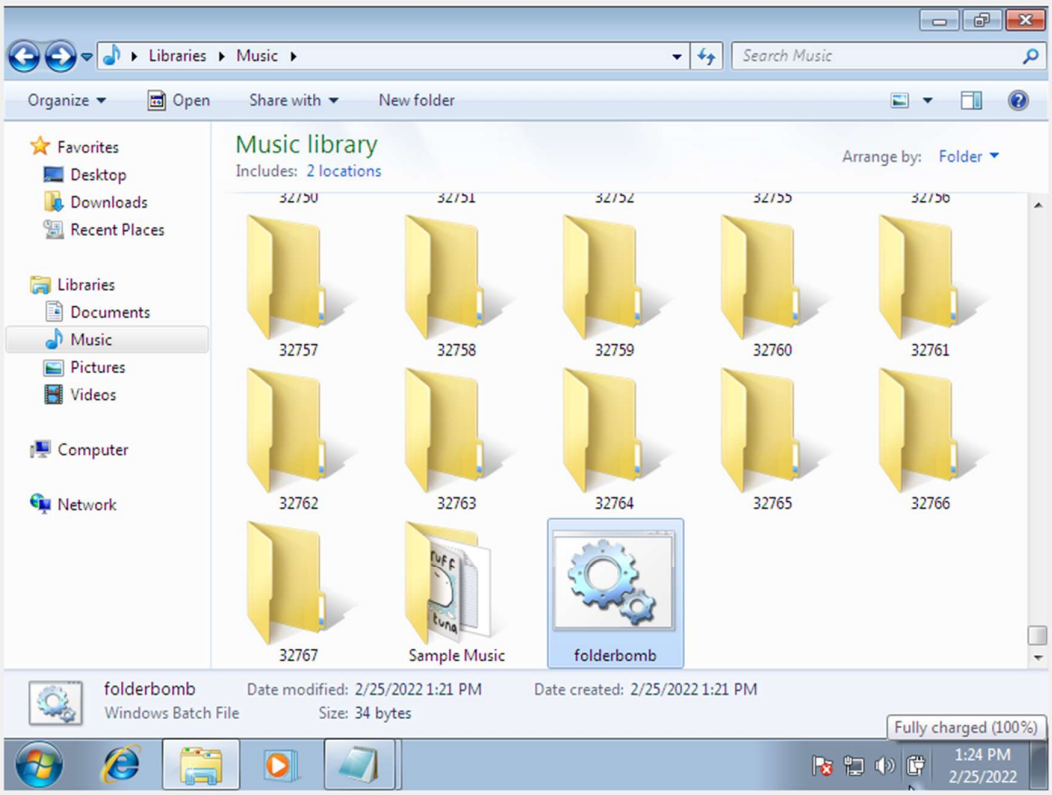


11) Send the file to victim if victim opens the file then he will receive infinite folders.





12) When he closes the CMD prompt then its stop.

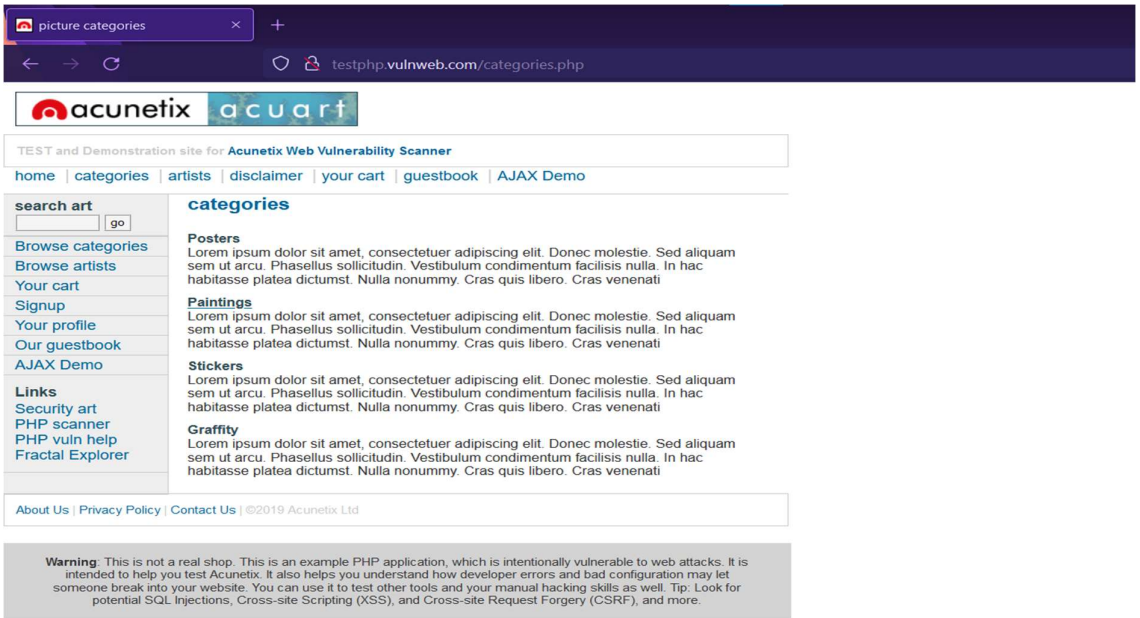


HAVJI TOOL (SQL INJECTION)

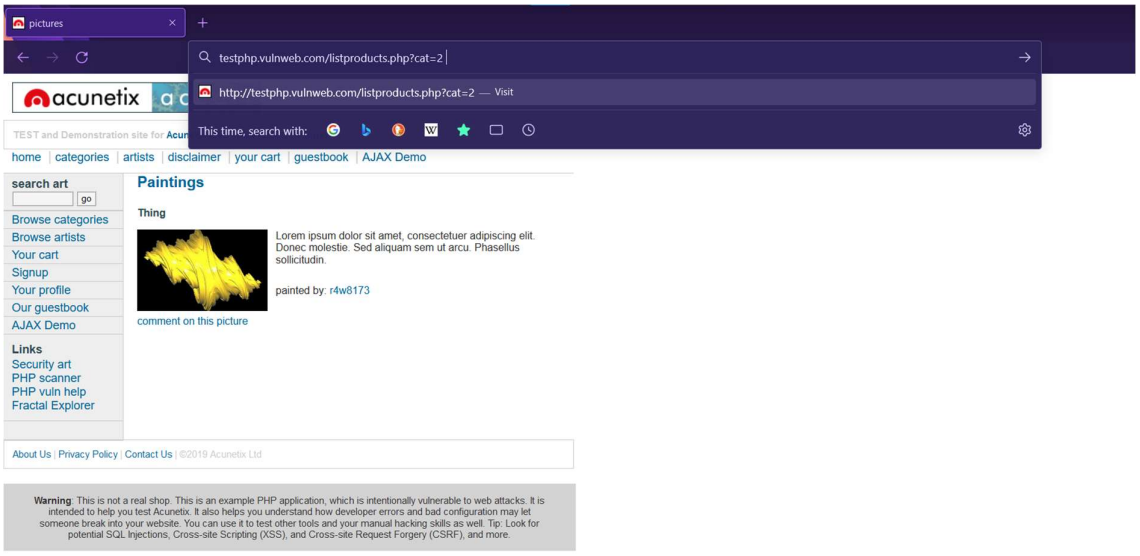
Path used to Download it:
https://www.mediafire.com/file/r6q3duastpl9x43/Havij-1.12-Free-Download.zip/file

STEPS TO REPRODUCE :

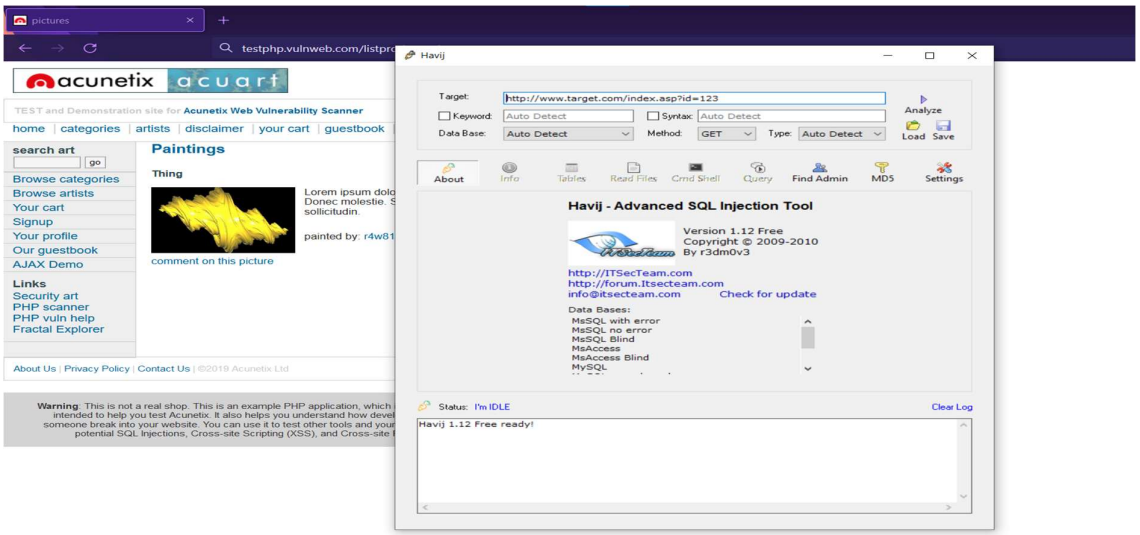
1) Download and install the Wireshark tool from the above link.
2) Open the demo website in the browser http://testphp.vulnweb.com/login.php

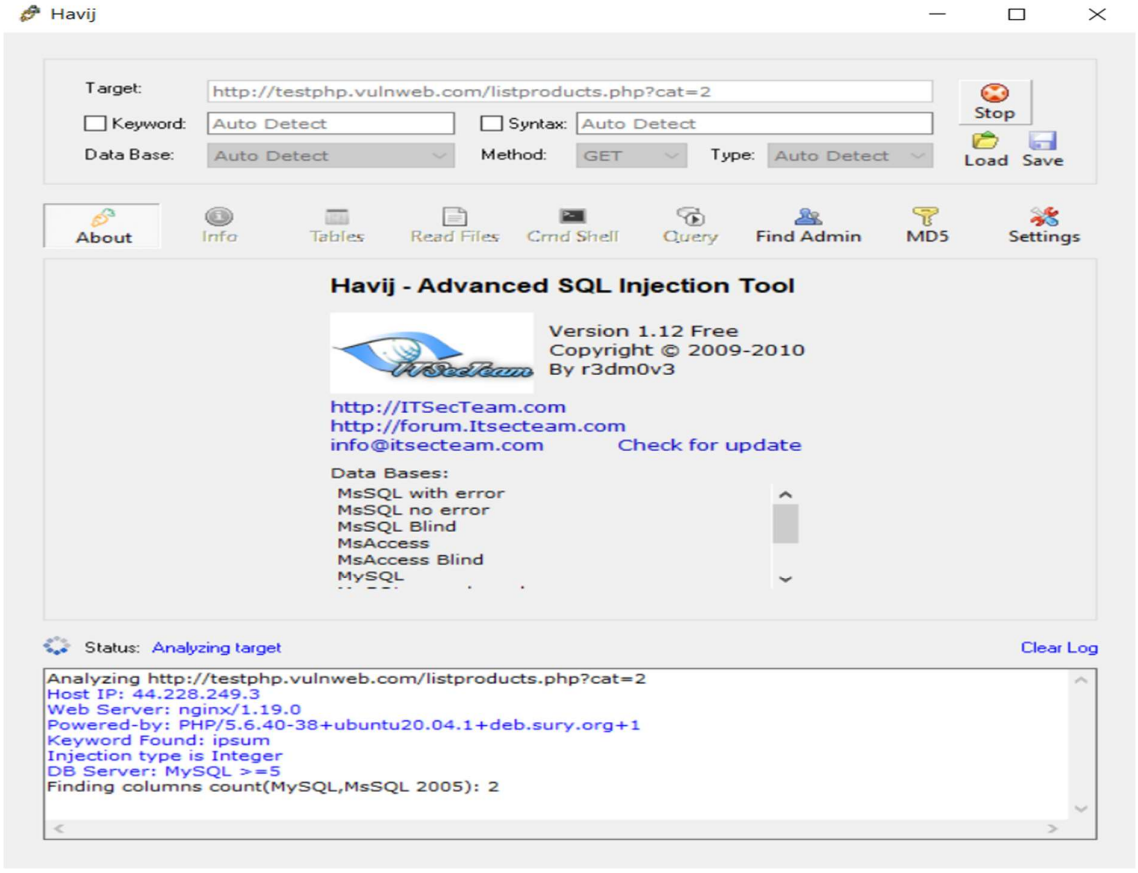


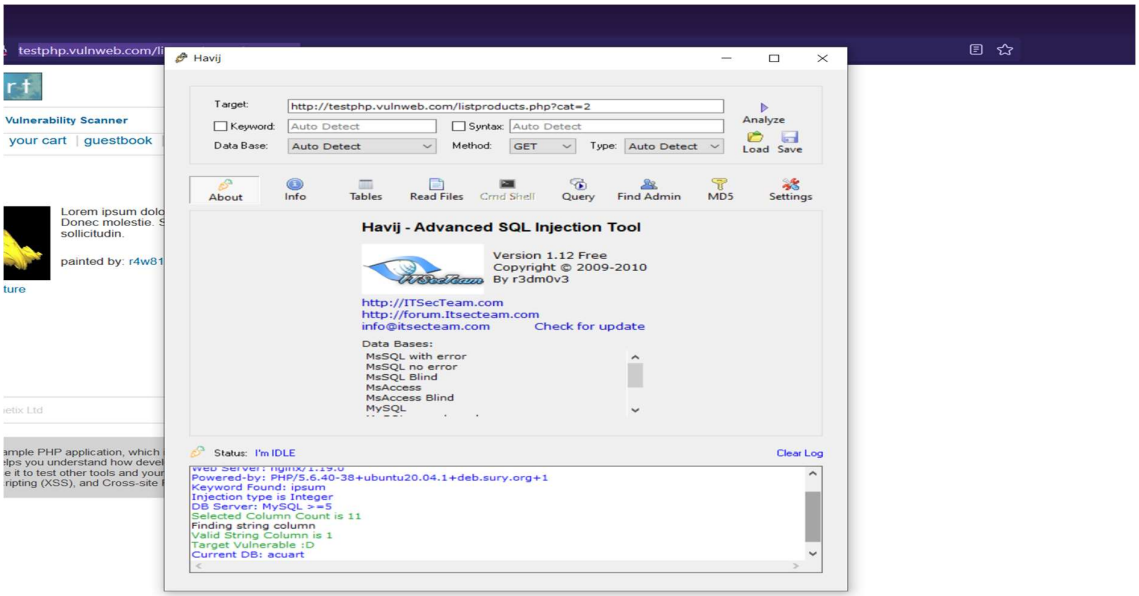
3) In the website check in the link where it is "= any number" http://testphp.vulnweb.com/listproducts.php?cat=2



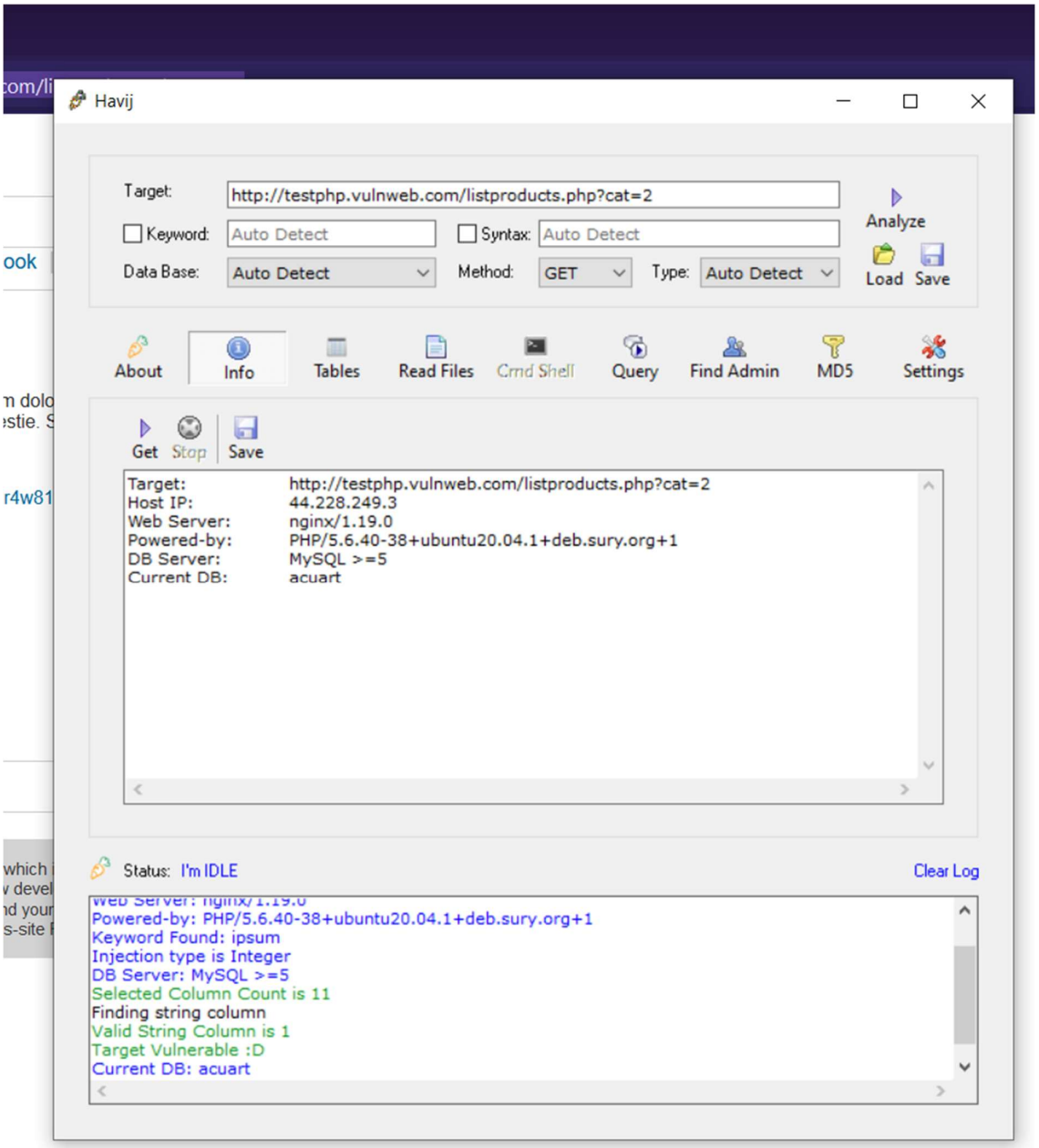
4) Open the link in the Havij tool and start analyse it.



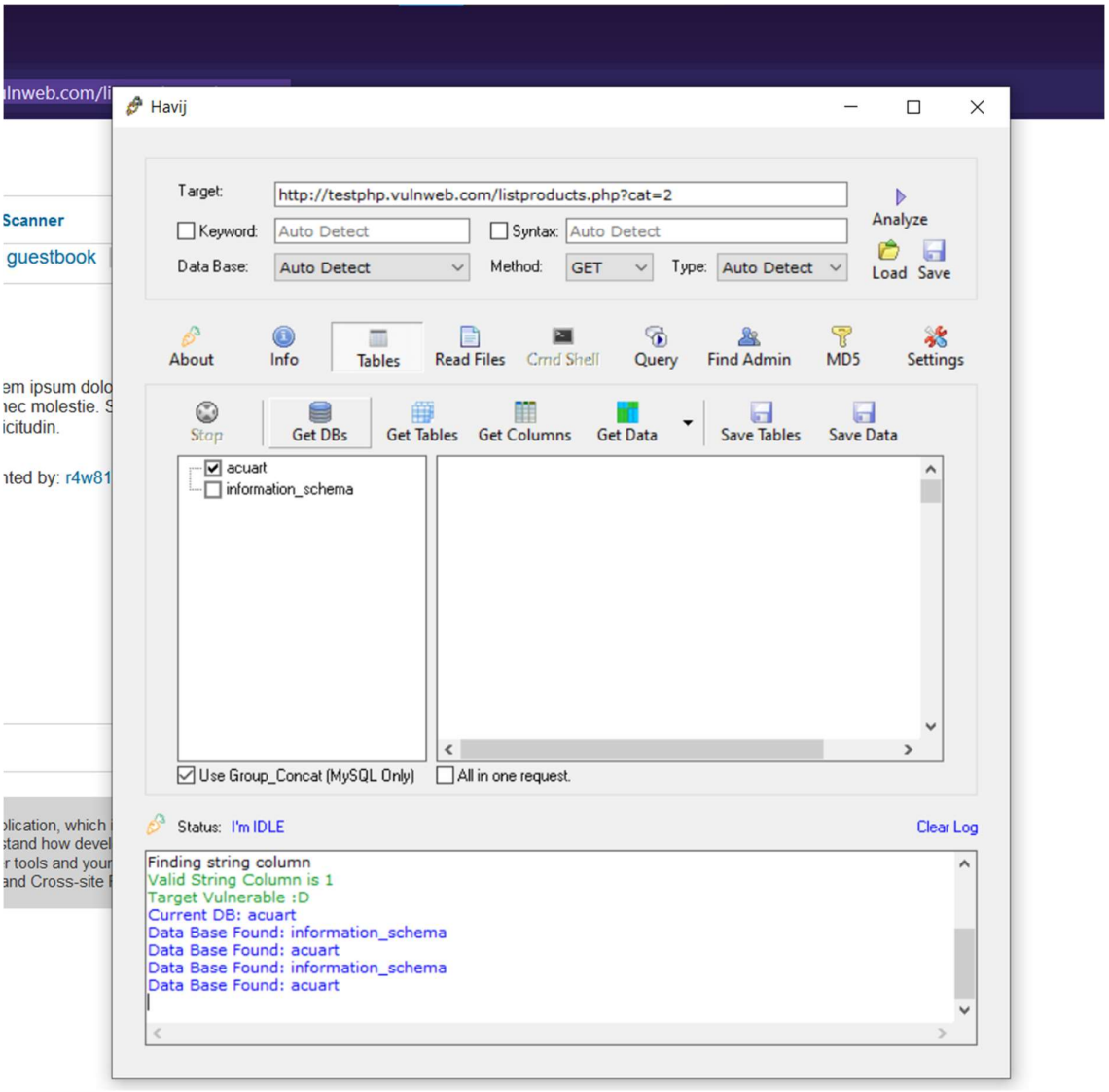

Havij
Target:
http://testphp.vulnweb.com/listproducts.php?cat=2
Keyword:
Auto Detect
Syntax:
Auto Detect
Data Base:
Auto Detect
Method:
GET
Type:
Auto Detect
Stop
Load
Save
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Havij - Advanced SQL Injection Tool
Version 1.12 Free
Copyright © 2009-2010
By r3dm0v3
http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com
Check for update
Data Bases:
MsSQL with error
MsSQL no error
MsSQL Blind
MsAccess
MsAccess Blind
MySQL
Status: Analyzing target
Clear Log
Analyzing http://testphp.vulnweb.com/listproducts.php?cat=2
Host IP: 44.228.249.3
Web Server: nginx/1.19.0
Powered-by: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Keyword Found: ipsum
Injection type is Integer
DB Server: MySQL >=5
Finding columns count(MySQL,MsSQL 2005): 2


testphp.vulnweb.com/li
Vulnerability Scanner
your cart
guestbook
Lorem ipsum dolo
Donec molestie.
sollicitudin.
painted by: r4w81
ture
Havij
Target:
http://testphp.vulnweb.com/listproducts.php?cat=2
Keyword:
Auto Detect
Syntax:
Auto Detect
Data Base:
Auto Detect
Method:
GET
Type:
Auto Detect
Analyze
Load
Save
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Havij - Advanced SQL Injection Tool
Version 1.12 Free
Copyright © 2009-2010
By r3dm0v3
http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com
Check for update
Data Bases:
MsSQL with error
MsSQL no error
MsSQL Blind
MsAccess
MsAccess Blind
MySQL
Status: I'm IDLE
Clear Log
Powered-by: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Keyword Found: ipsum
Injection type is Integer
DB Server: MySQL >=5
Selected Column Count is 11
Finding string column
Valid String Column is 1
Target Vulnerable :D
Current DB: acuart

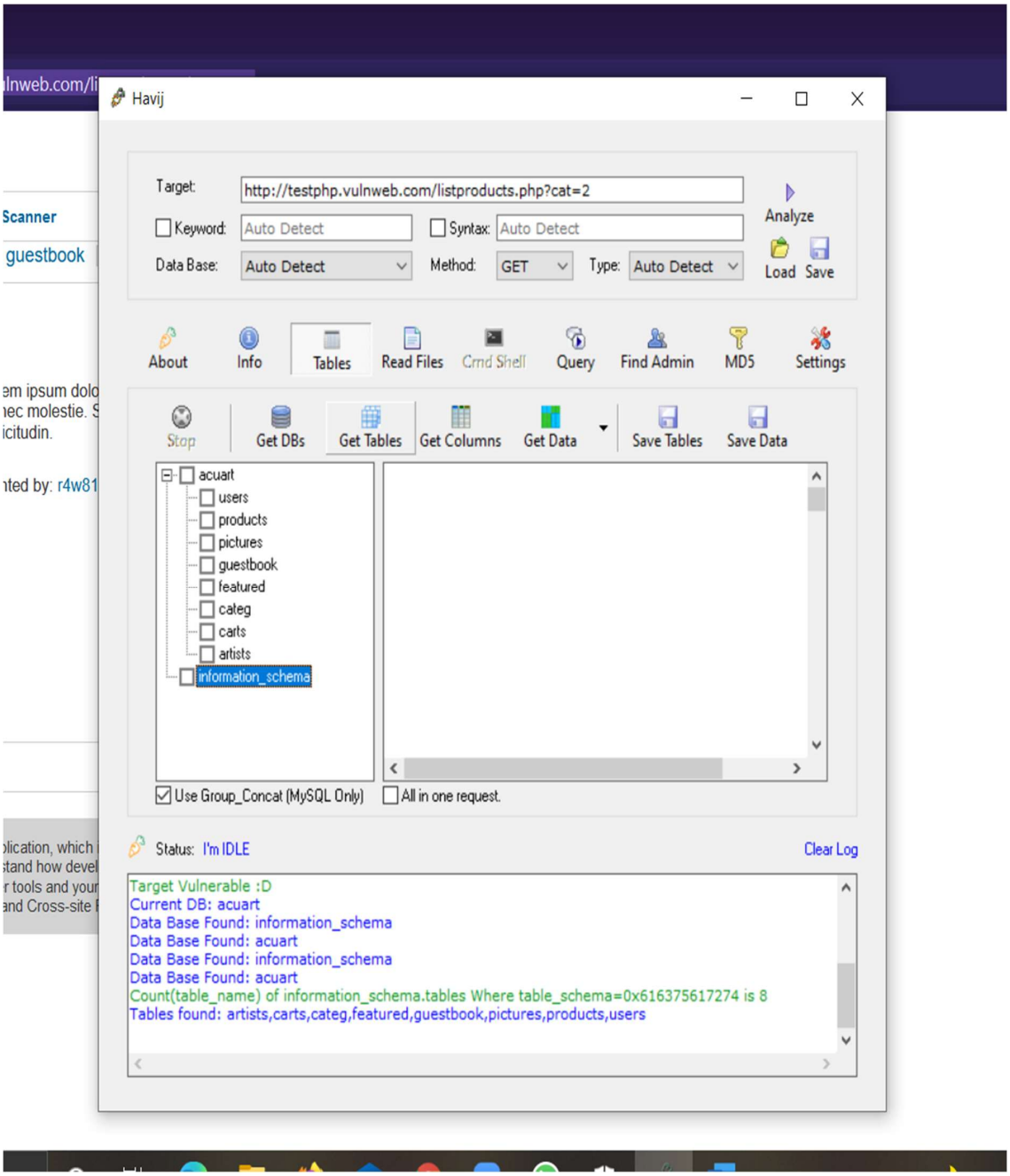
5) Go to info we can see some details of website like host Ip , webserver used etc.,



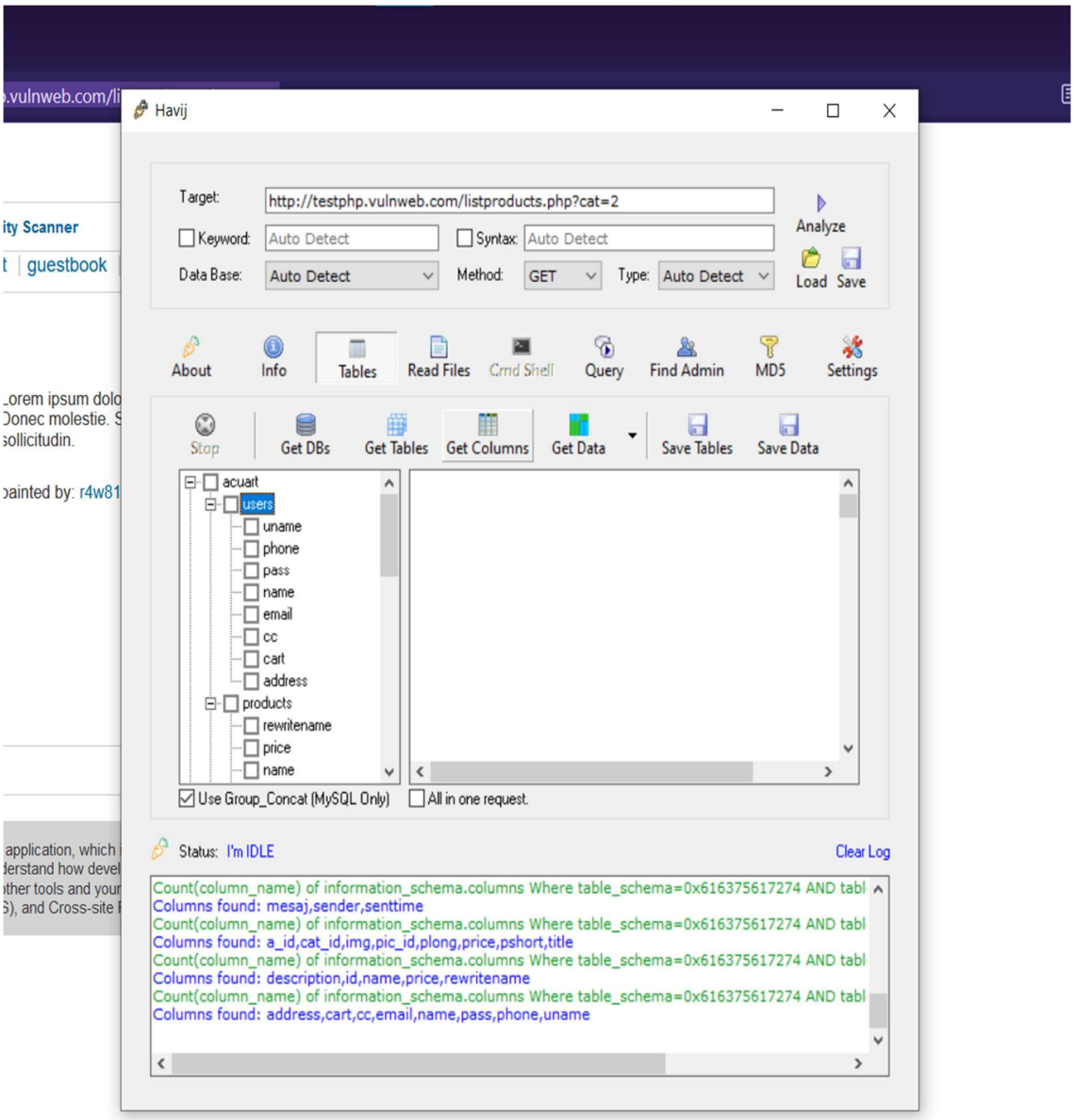
6) Go to tables and get the database. Here we found information schema.



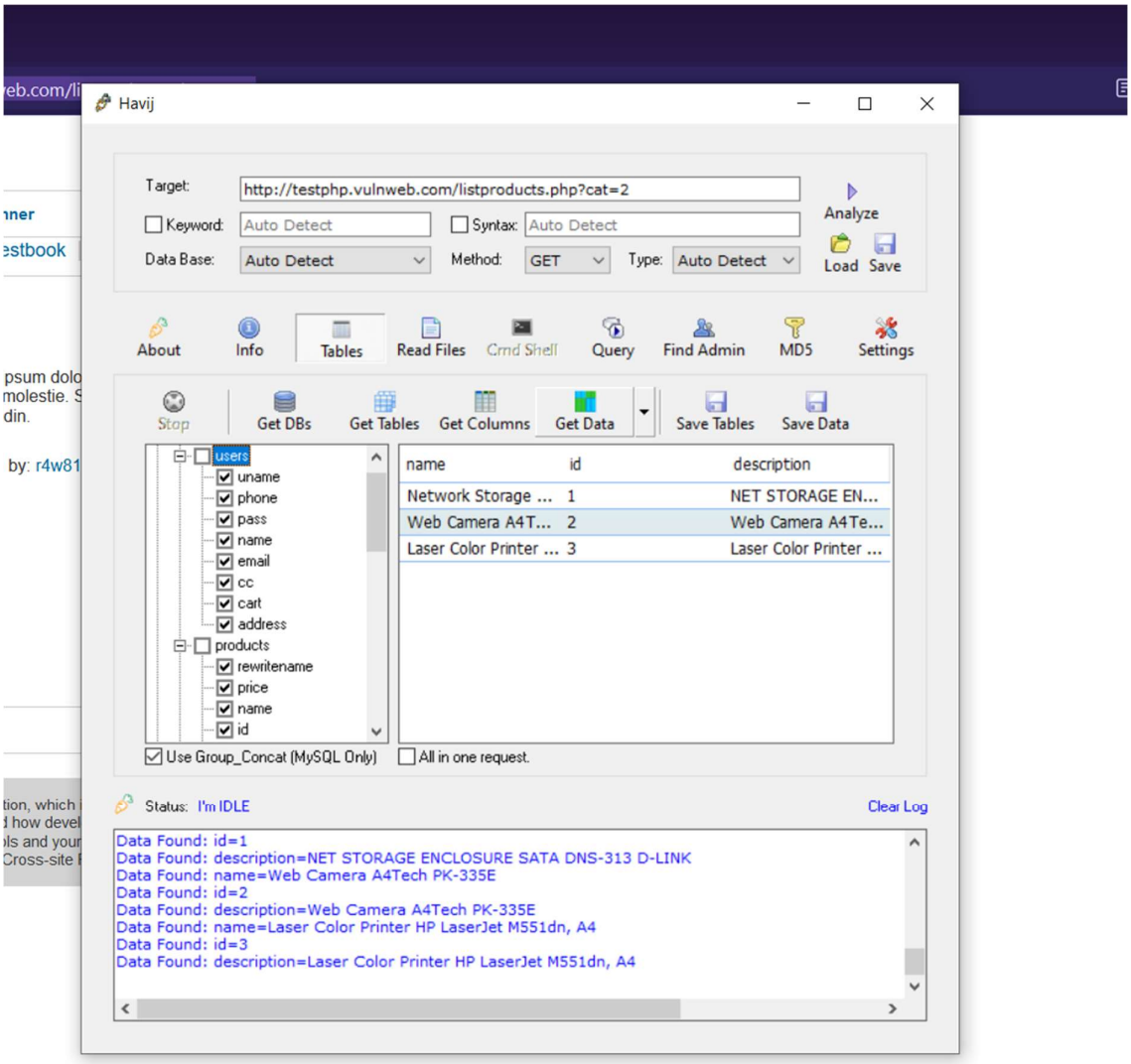
7) Click on information schema and click on get tables.



8) Now select all the tables and get colums.



9) Then select all the columns and the Data inside it.



10) Now try the same procedure for the given following links which found in the given websites.

a) http://testphp.vulnweb.com/artists.php?artist=1
b) http://testphp.vulnweb.com/listproducts.php?artist=1
c) http://testphp.vulnweb.com/artists.php?artist=2

d) http://testphp.vulnweb.com/listproducts.php?artist=2
e) http://testphp.vulnweb.com/artists.php?artist=3
f) http://testphp.vulnweb.com/listproducts.php?artist=3

Steps to Prevent SQL Injection: -

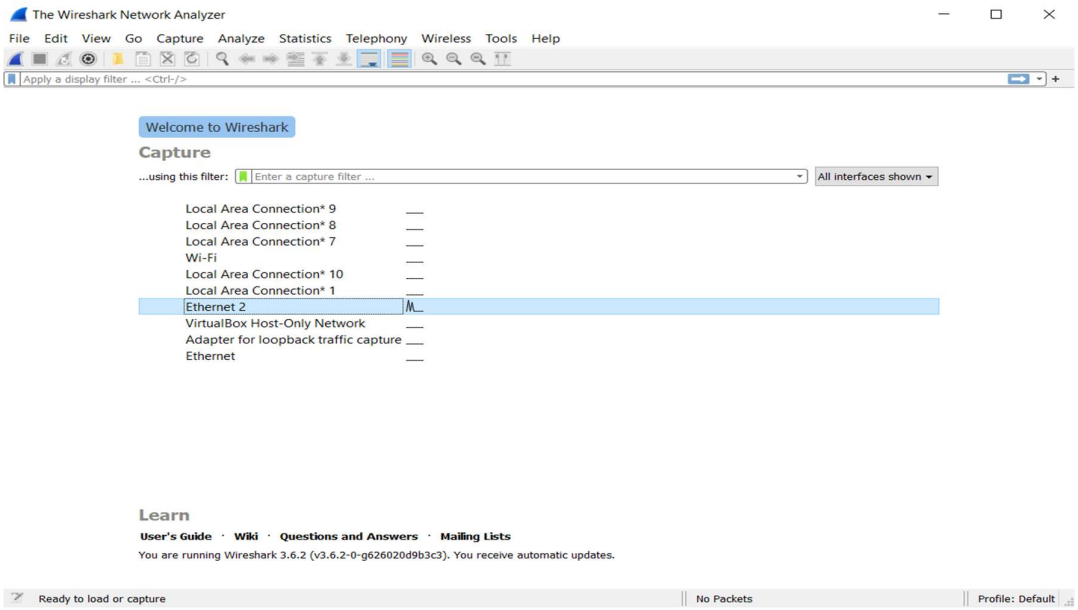
1) Verify the user's inputs.
2) Limit special characters in data to keep it clean.
3) Make sure prepared statements and parameterization are enforced.
4) Make use of database stored procedures.
5) Keep track of fixes and updates.
6) Increase the number of virtual or physical firewalls.
7) Harden your operating system and applications.
8) Make your assault surface smaller.
9) Assign proper permissions and restrict access.
10) Restrict read-only access.
11) Encryption: Keep your secrets hidden via encryption.
12) Extensive URLs are not allowed.
13) In error messages, don't reveal more information than is really necessary.
14) There are no shared databases or accounts.
15) Adhere to best practises when it comes to account and password policies.
16) SQL statements are constantly monitored.
17) Auditing and penetration testing should be done on a regular basis.
18) Better software and code development.

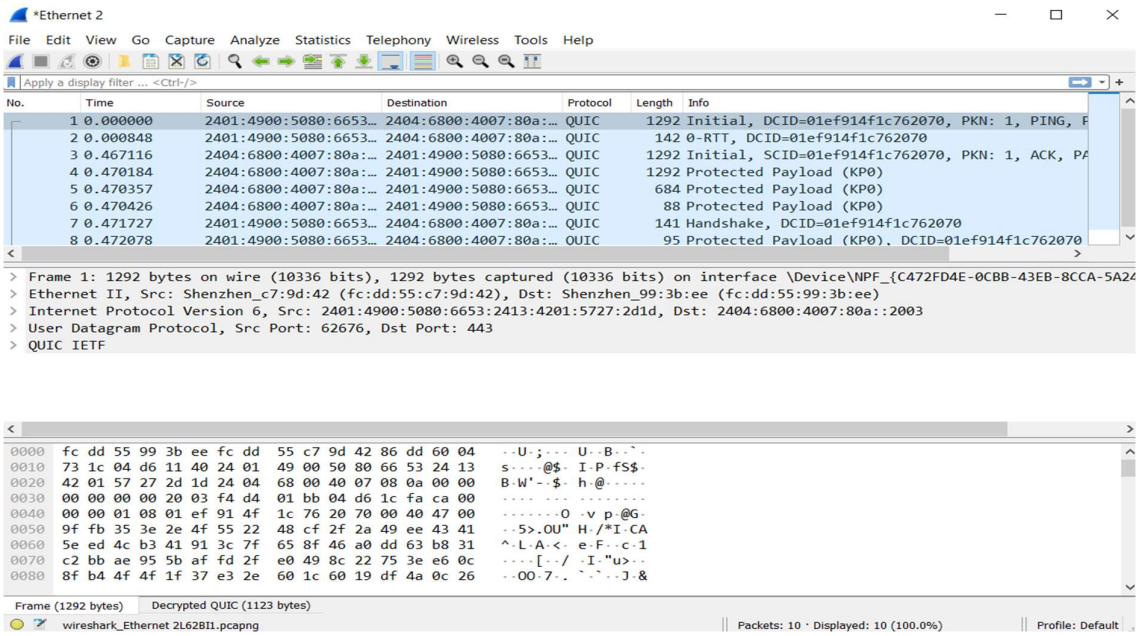
USING THE WIRESHARK TOOL SNIFFING THE DATA AND GETTING USER ID AND PASSWORD

Path used to Download it: https://www.wireshark.org/

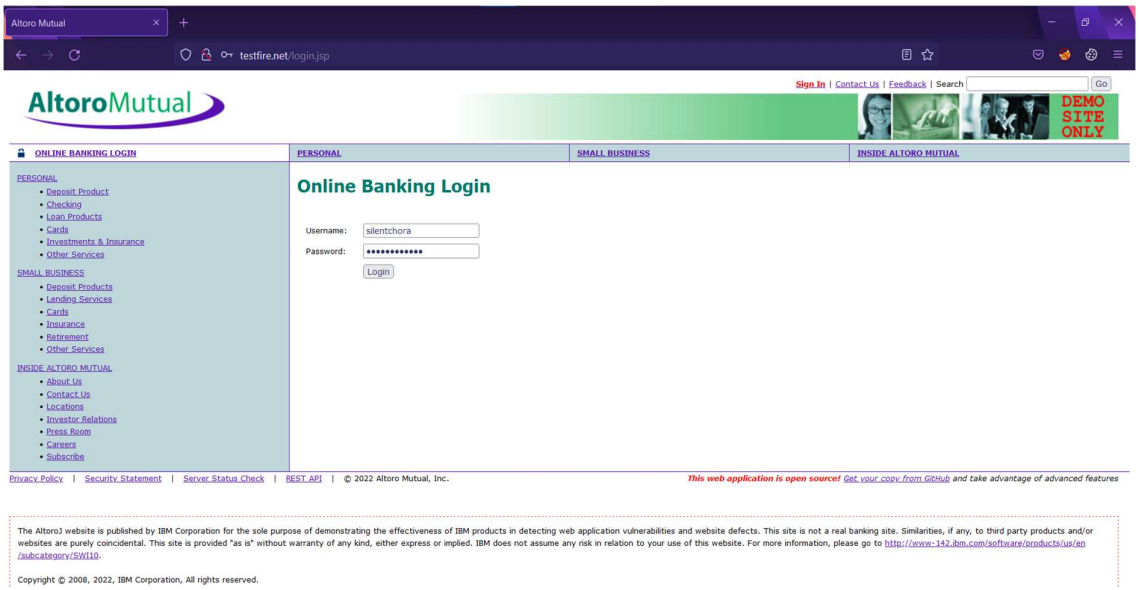
STEPS TO REPRODUCE :

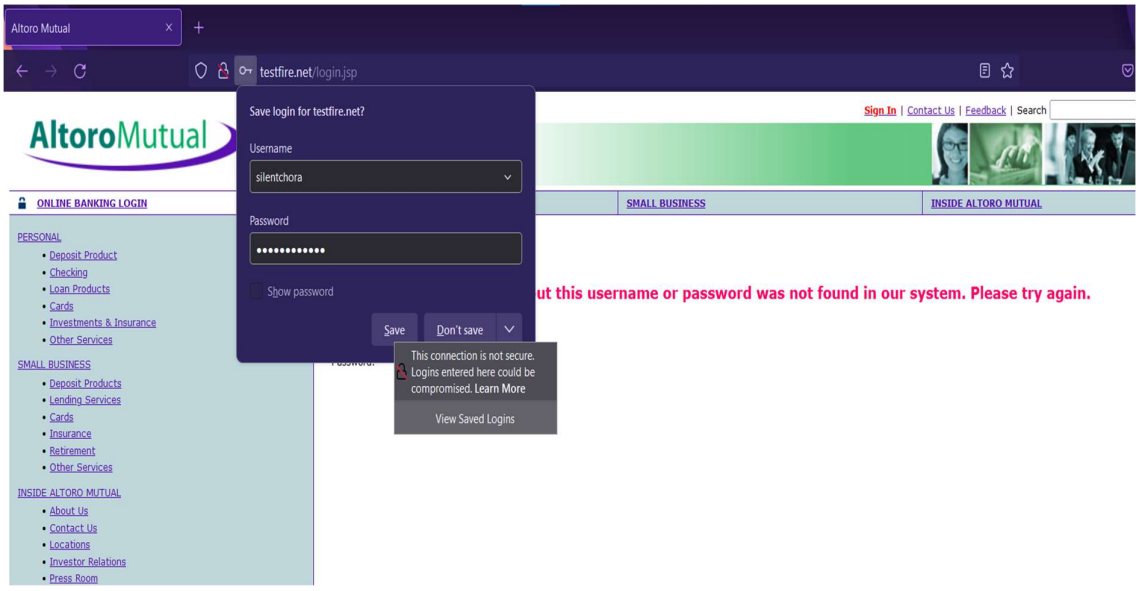
1) Download and install the Wireshark tool from the above link.
2) Select the network (Ether2) and open it.



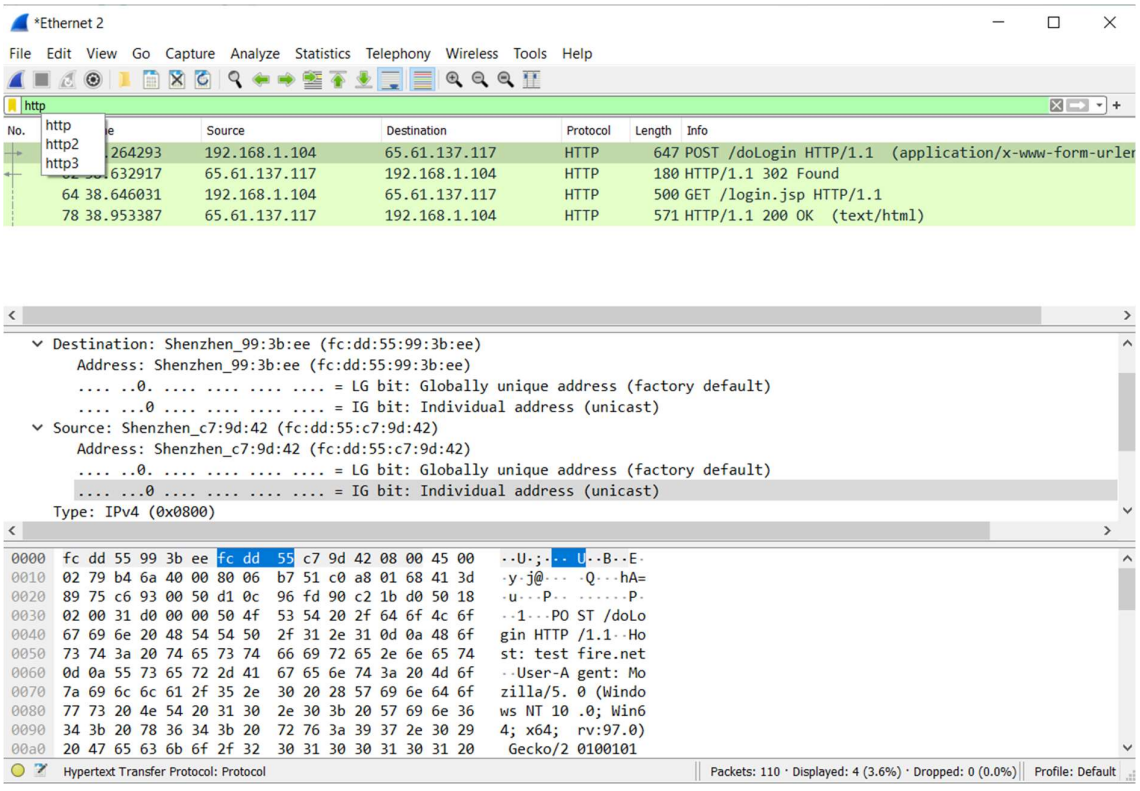


3) Open the demo website in the browser http://testfire.net/login.jsp and to login it.

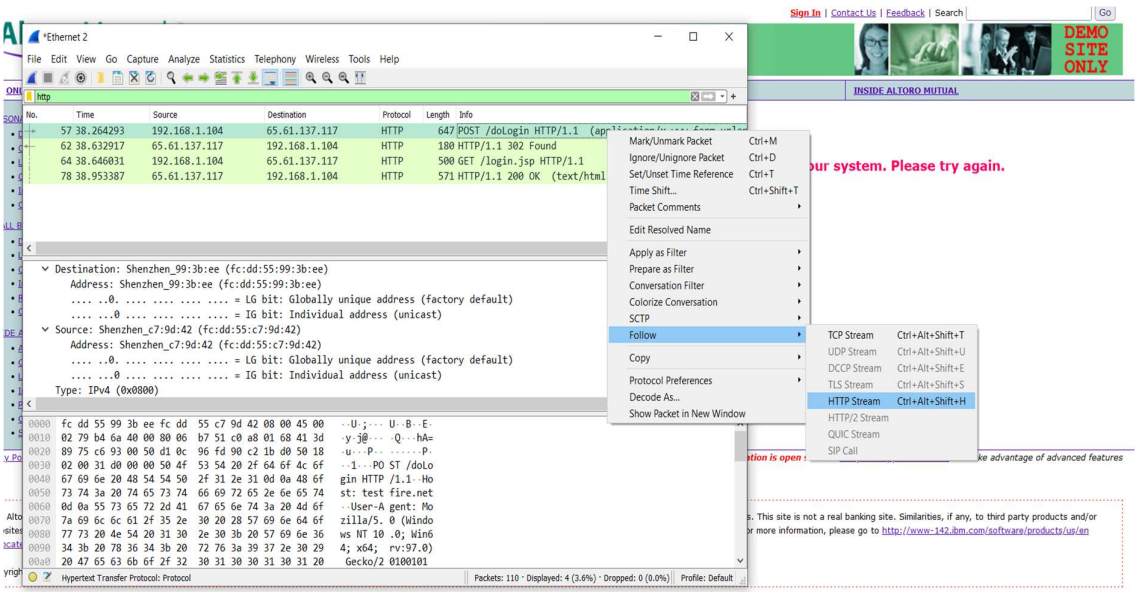




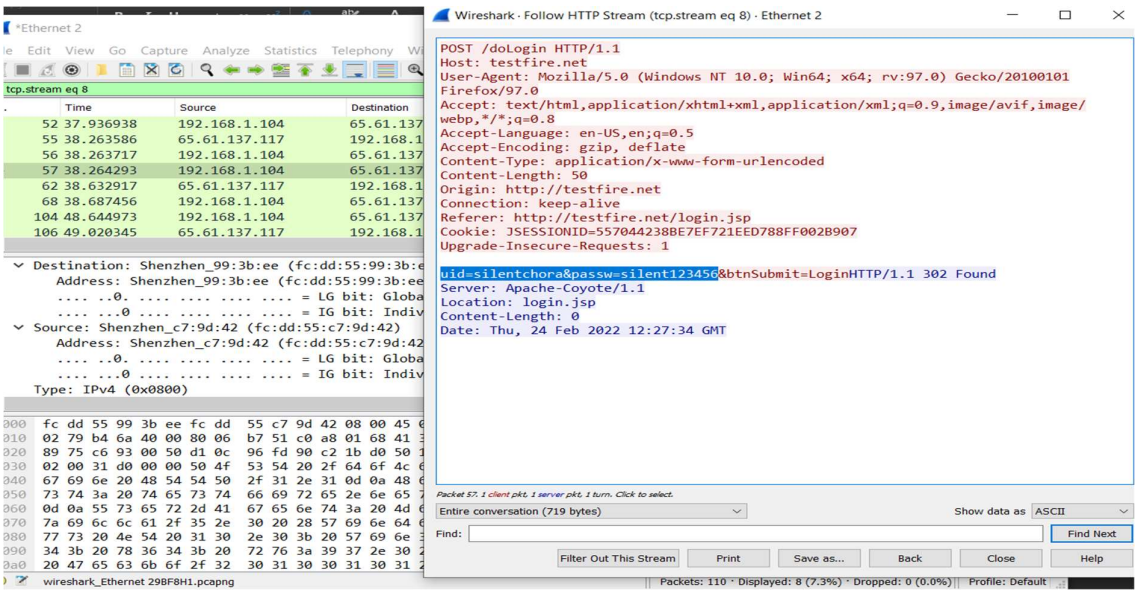
4) Now capture the request in Wireshark.



5) In the above search box search for HTTP.



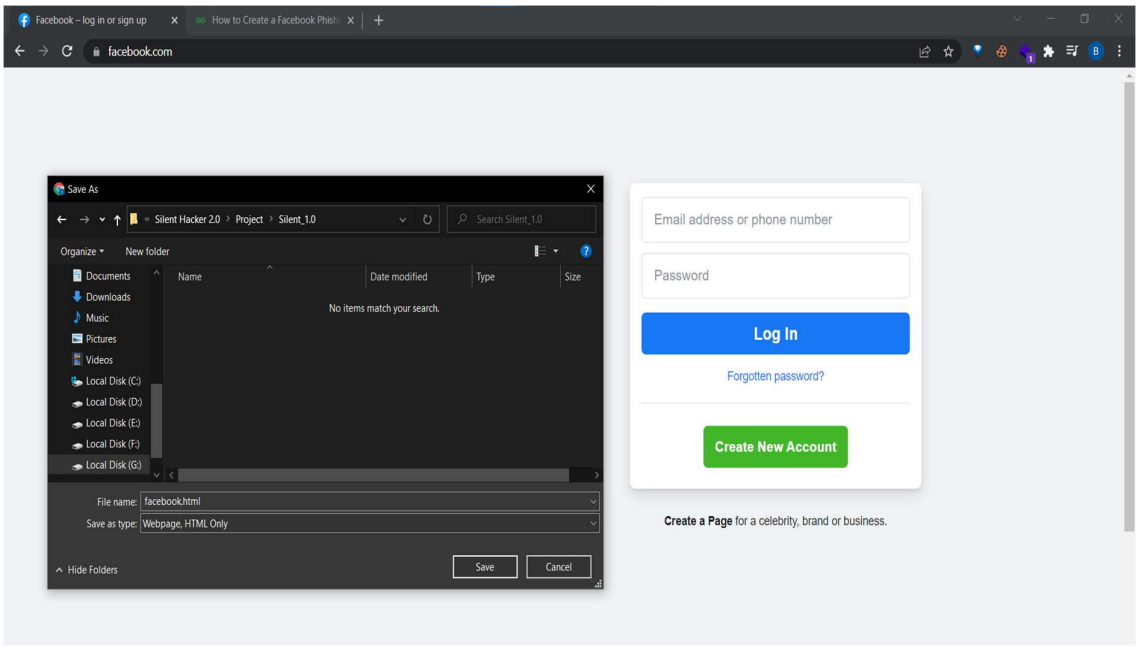
6) In the HTTP Stream we can find the User ID and password which we entered to login the website.



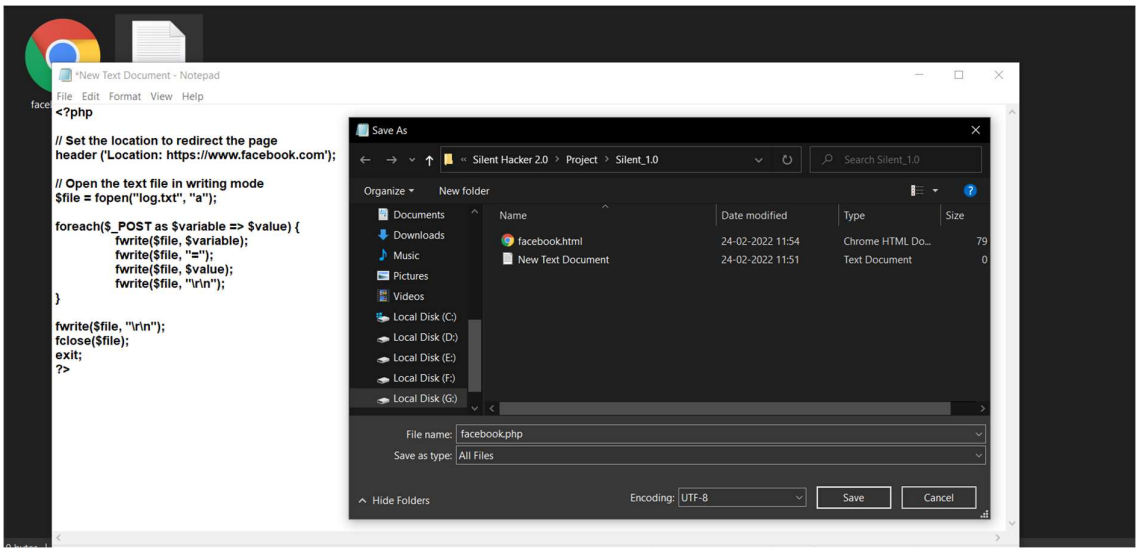
PHISHING ATTACK

STEPS TO REPRODUCE :

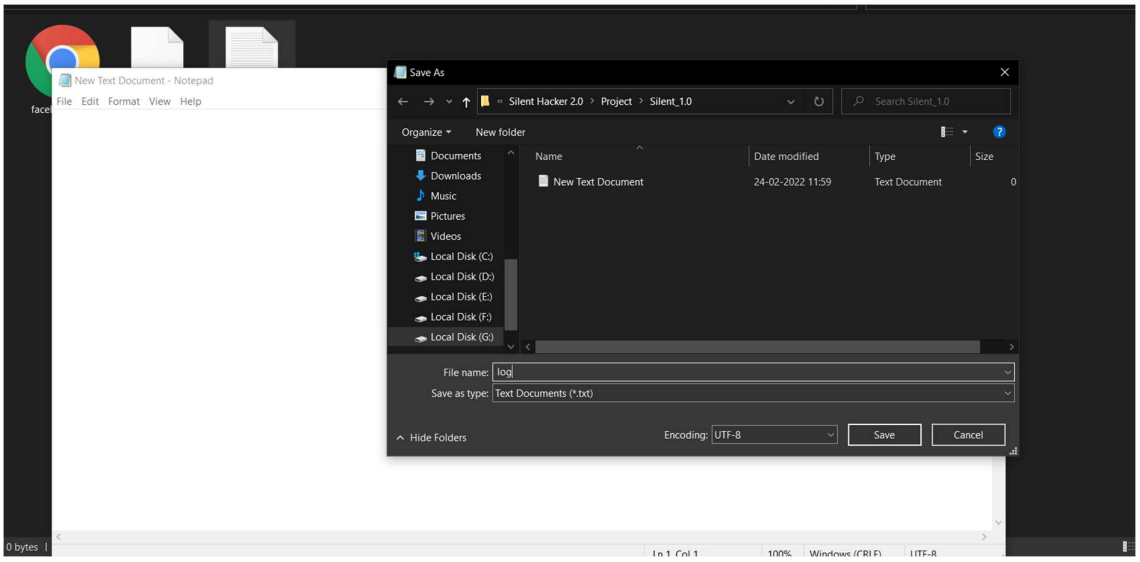
1) Three files are required for doing a phishing attack.
2) First file HTML-file which looks like genuine login page.
3) Second file is PHP-file which contains malicious code for capturing user ID and password.
4) Third file is Empty TEXT-file to save user ID and Password of victim.
5) Now clone the login page of the website by clicking right click and save the page.



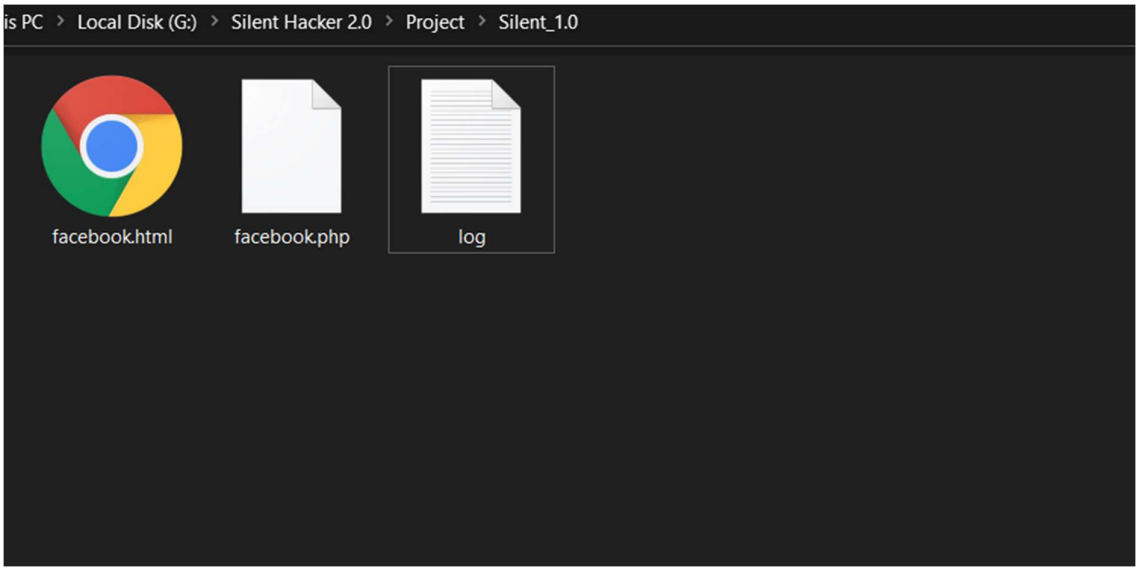
6) Create a PHP file with malicious code to capture details.
7) Get the php phishing script from google or we can type if we know it.



8) Create an empty text file with name log.

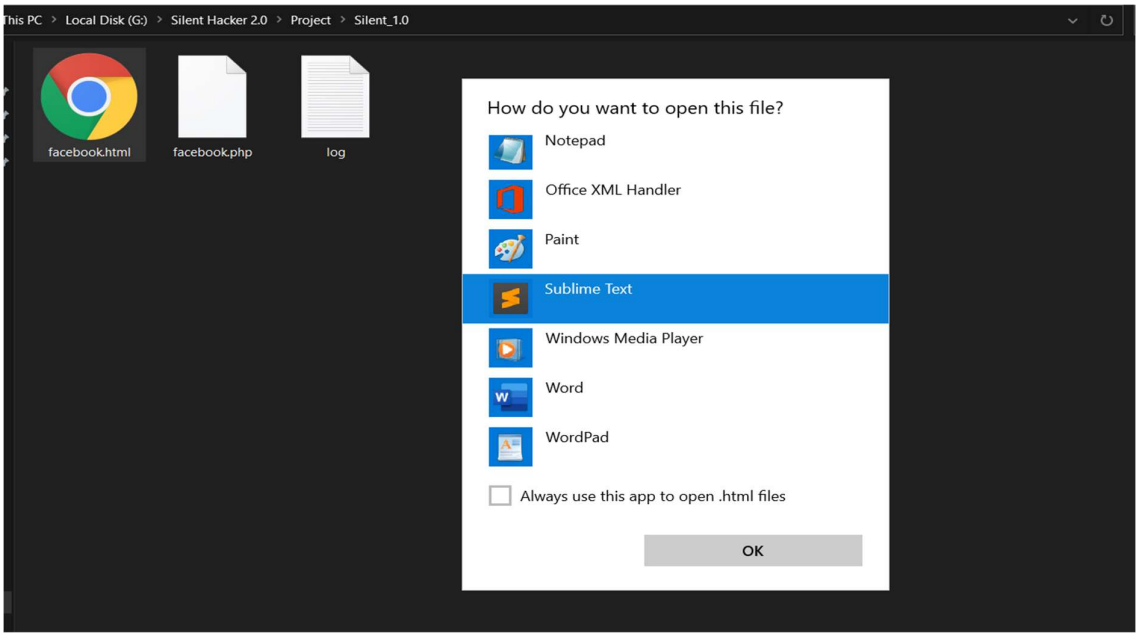


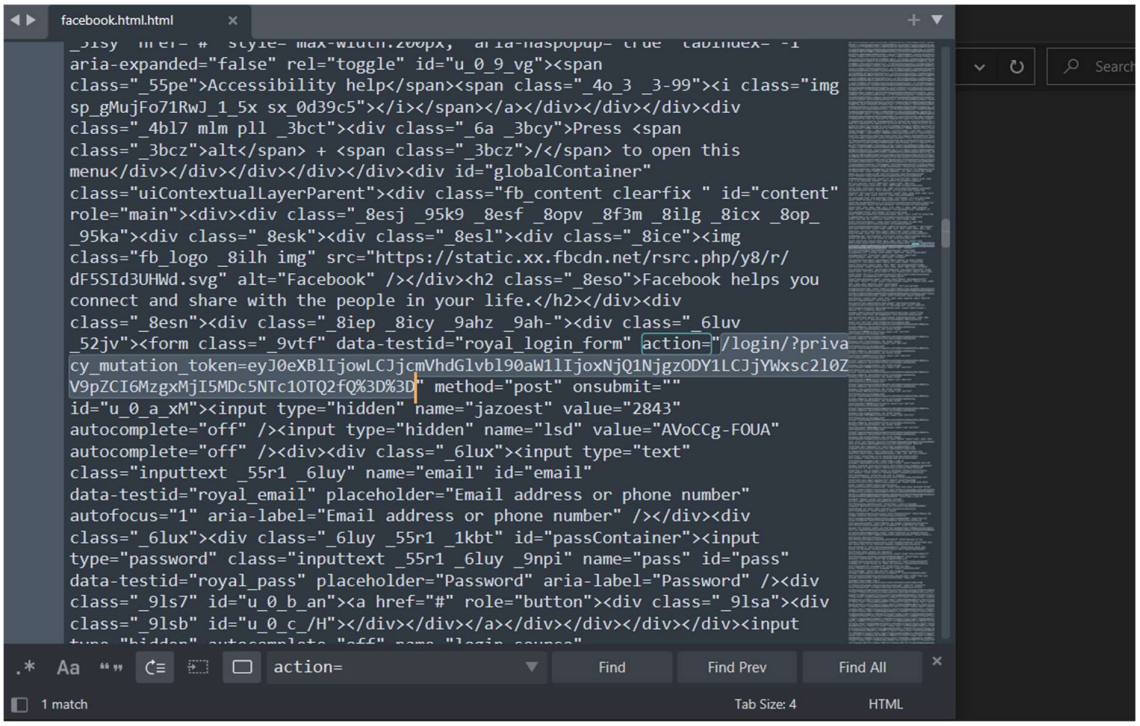
9) We can see all the three files.

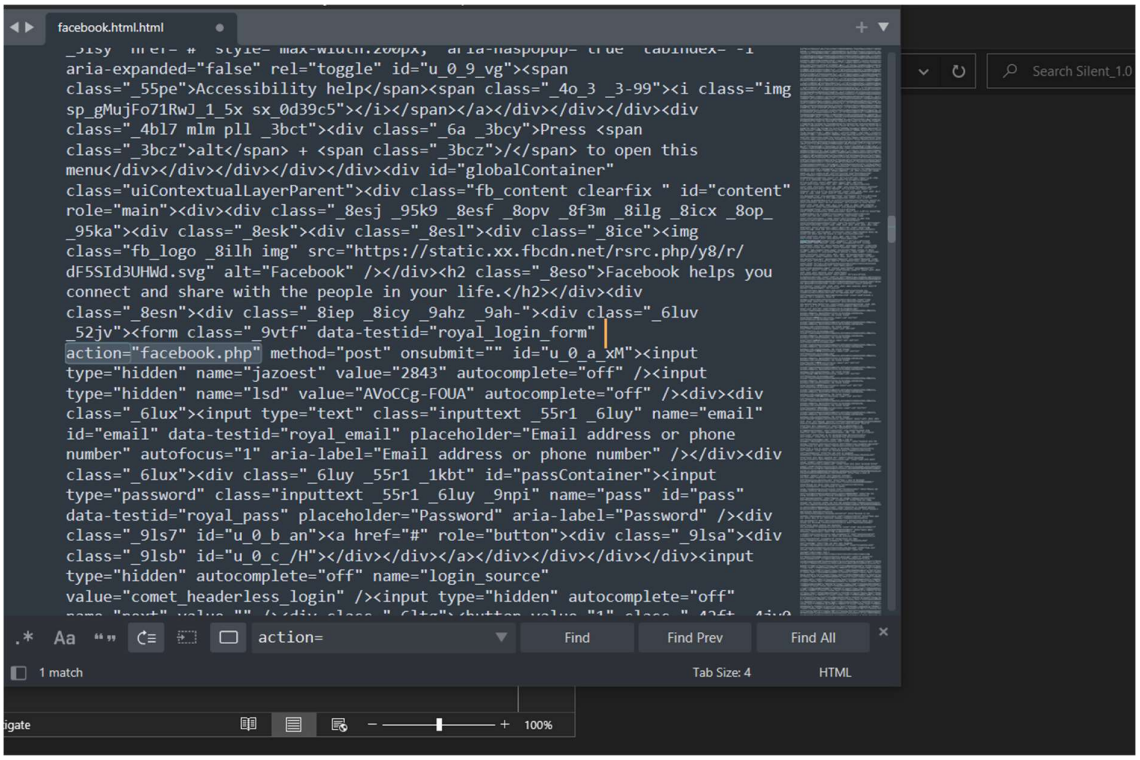


10) Now edit the HTML file with notepad(sublime text / Notepad++) and search for the keyword called "**action="**

11) Replace the original link with php file name (facebook.php)

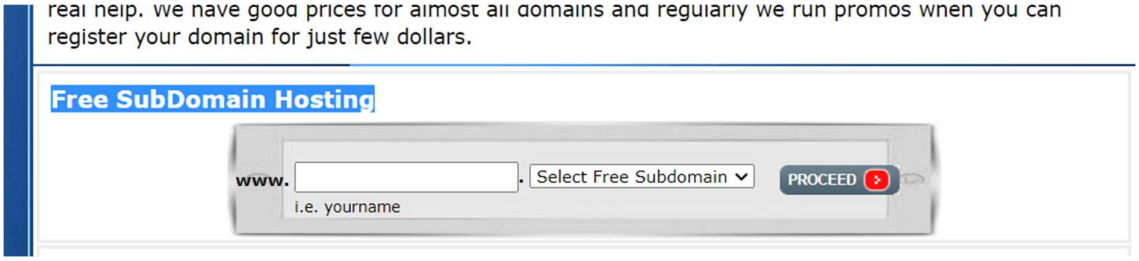


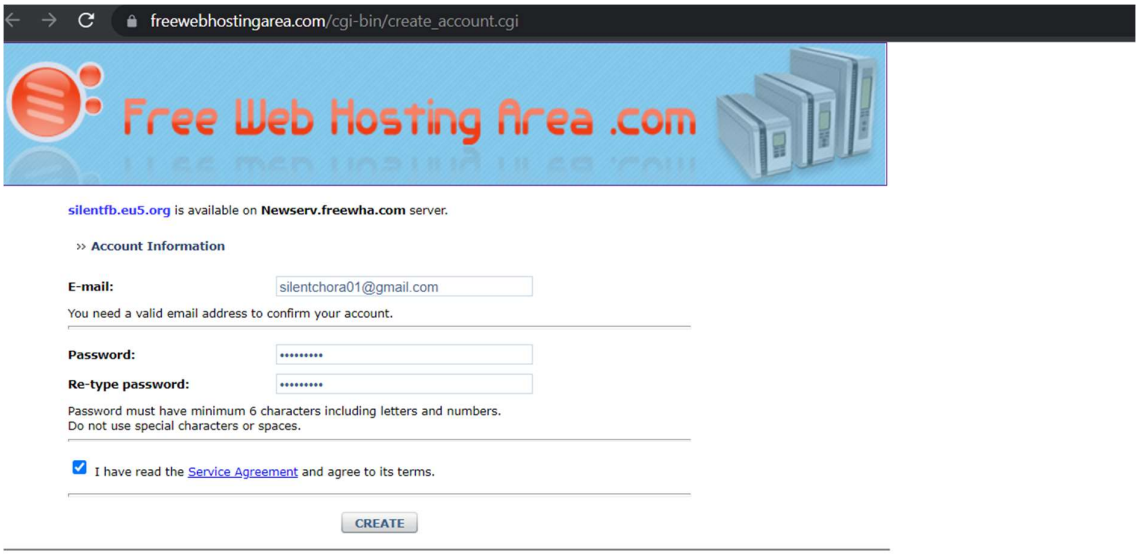

facebook.html.html
aria-expanded="false" rel="toggle" id="u_0_9_vg"><span
class="_55pe">Accessibility help<i class="img
sp_gMujFo71RwJ_1_5x sx_0d39c5"></i> <div
class="_4bl7 mlm pll _3bct"> Press <span
class="_3bcz">alt + / to open this
menu <div id="globalContainer"
class="uiContextualLayerParent"><div class="fb_content clearfix " id="content"
role="main"> <div class="_8esj _95k9 _8esf _8opv _8f3m _8ilg _8icx _8op_
_95ka"> <img
class="fb_logo _8ilh img" src="https://static.xx.fbcdn.net/rsrc.php/y8/r/
dF5SId3UHWd.svg" alt="Facebook" /> <h2 class="_8eso">Facebook helps you
connect and share with the people in your life.</h2> <div
class="_8esn"> <div class="_6luv
_52jv"><form class="_9vtf" data-testid="royal_login_form" action="/login/?priva
cy_mutation_token=eyJ0eXBlIjowLCJjcmVhdGlvbl90aW1lIjoxNjQ1NjgzODY1LCJjYWxsc2l0Z
V9pZCI6MzgxMjI5MDc5NTc1OTQ2fQ%3D%3D" method="post" onsubmit=""
id="u_0_a_xM"><input type="hidden" name="jazoest" value="2843"
autocomplete="off" /><input type="hidden" name="lsd" value="AVoCCg-FOUA"
autocomplete="off" /> <input type="text"
class="inputtext _55r1 _6luy" name="email" id="email"
data-testid="royal_email" placeholder="Email address or phone number"
autofocus="1" aria-label="Email address or phone number" /> <div
class="_6lux"> <input
type="password" class="inputtext _55r1 _6luy _9npi" name="pass" id="pass"
data-testid="royal_pass" placeholder="Password" aria-label="Password" /><div
class="_9ls7" id="u_0_b_an"> <div
class="_9lsb" id="u_0_c_/H"> <input
action=
Find
Find Prev
Find All
1 match
Tab Size: 4
HTML


facebook.html.html
aria-expanded="false" rel="toggle" id="u_0_9_vg"><span
class="_55pe">Accessibility help<i class="img
sp_gMujFo71RwJ_1_5x sx_0d39c5"></i> <div
class="_4bl7 mlm pll _3bct"> Press <span
class="_3bcz">alt + / to open this
menu <div id="globalContainer"
class="uiContextualLayerParent"><div class="fb_content clearfix " id="content"
role="main"> <div class="_8esj _95k9 _8esf _8opv _8f3m _8ilg _8icx _8op_
_95ka"> <img
class="fb_logo _8ilh img" src="https://static.xx.fbcdn.net/rsrc.php/y8/r/
dF5SId3UHWd.svg" alt="Facebook" /> <h2 class="_8eso">Facebook helps you
connect and share with the people in your life.</h2> <div
class="_8esn"> <div class="_6luv
_52jv"><form class="_9vtf" data-testid="royal_login_form"
action="facebook.php" method="post" onsubmit="" id="u_0_a_xM"><input
type="hidden" name="jazoest" value="2843" autocomplete="off" /><input
type="hidden" name="lsd" value="AVoCCg-FOUA" autocomplete="off" /> <div
class="_6lux"><input type="text" class="inputtext _55r1 _6luy" name="email"
id="email" data-testid="royal_email" placeholder="Email address or phone
number" autofocus="1" aria-label="Email address or phone number" /> <div
class="_6lux"> <input
type="password" class="inputtext _55r1 _6luy _9npi" name="pass" id="pass"
data-testid="royal_pass" placeholder="Password" aria-label="Password" /><div
class="_9ls7" id="u_0_b_an"> <div
class="_9lsb" id="u_0_c_/H"> <input
type="hidden" autocomplete="off" name="login_source"
value="comet_headerless_login" /><input type="hidden" autocomplete="off"
action=
Find
Find Prev
Find All
1 match
Tab Size: 4
HTML
100%

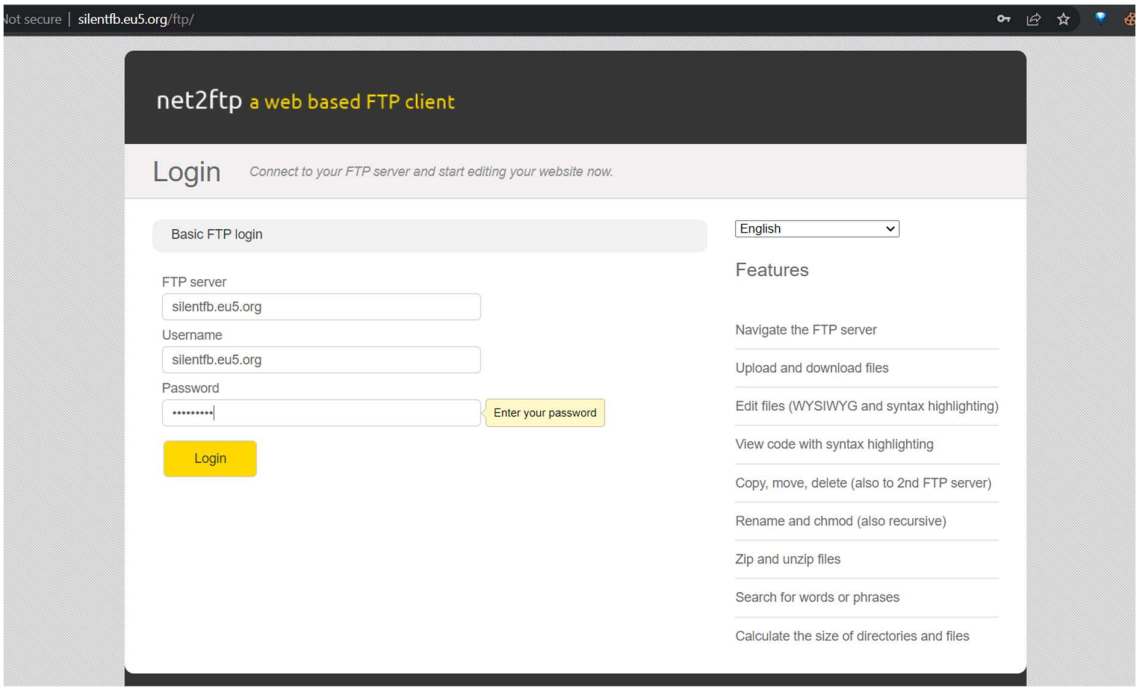
12) Now we need a website hosting page to upload these three files into in to online.

13) Free website hosting domain link https://www.freewebhostingarea.com/

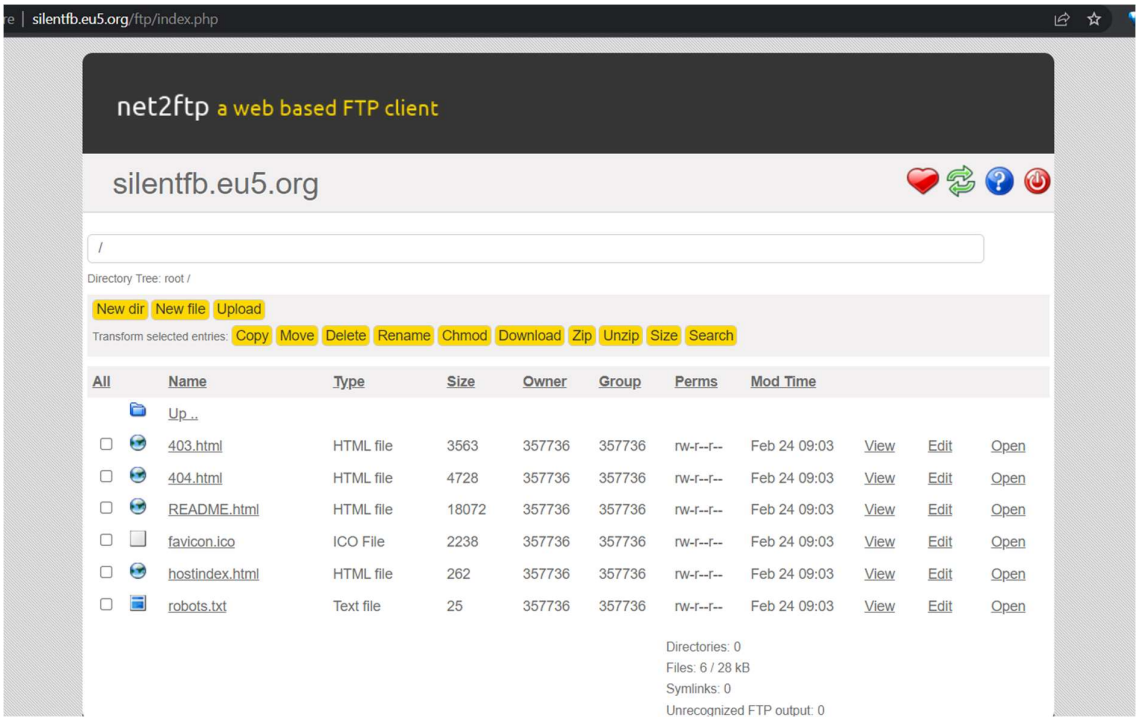


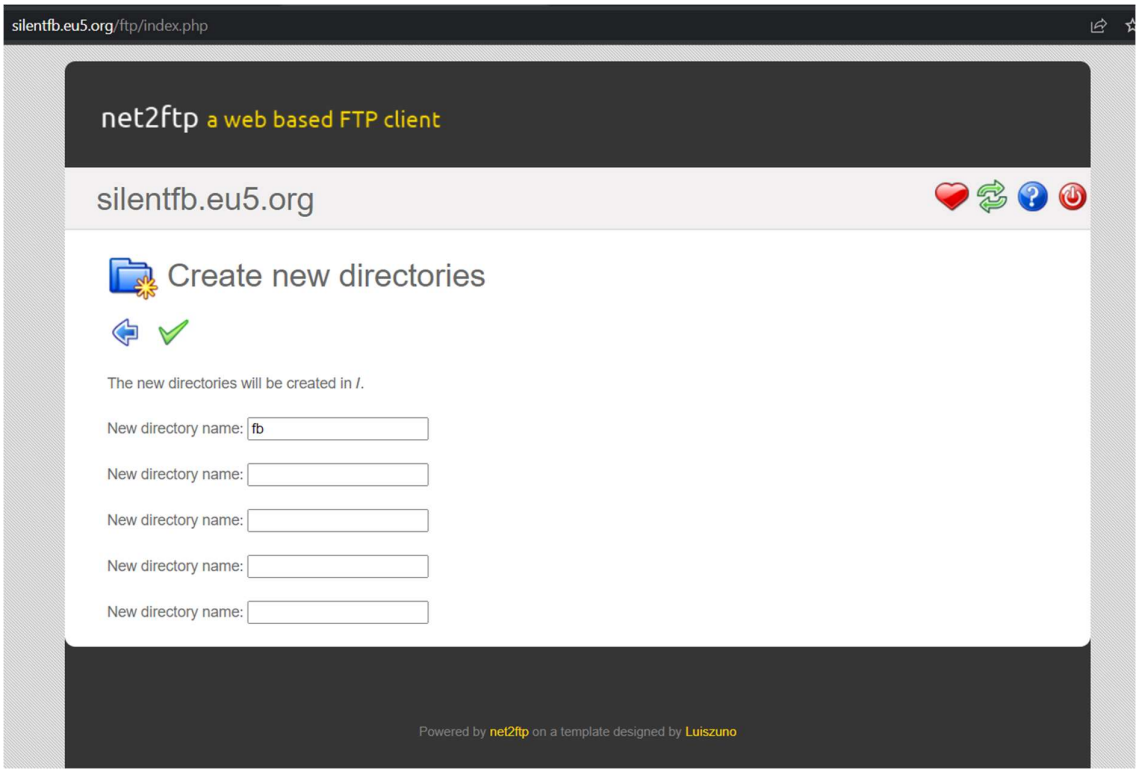


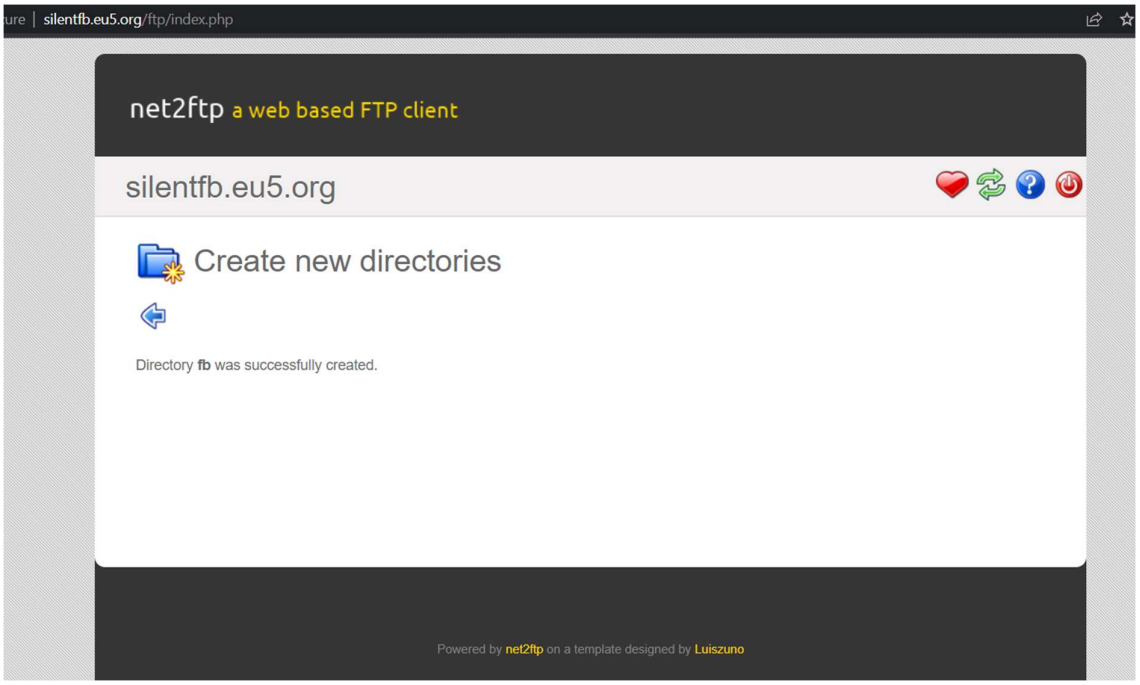
14) Open the new link generated and login with ftp(file transfer protocol) to upload all three files.

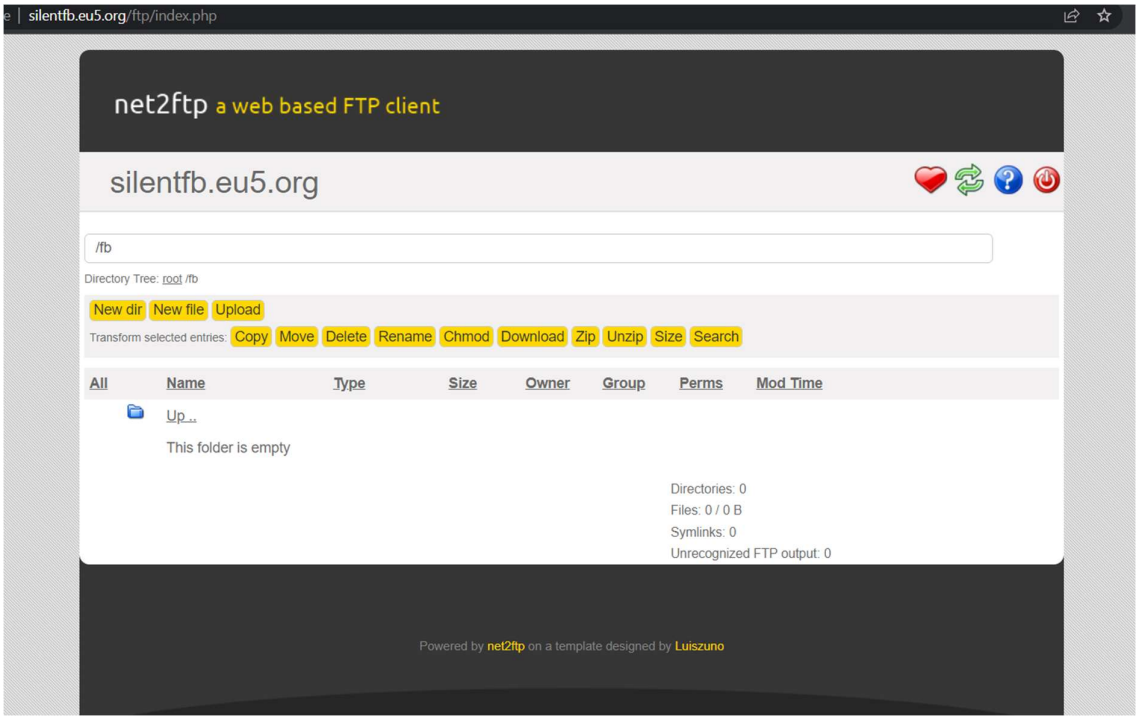


15) Create a new folder after login into ftp website.

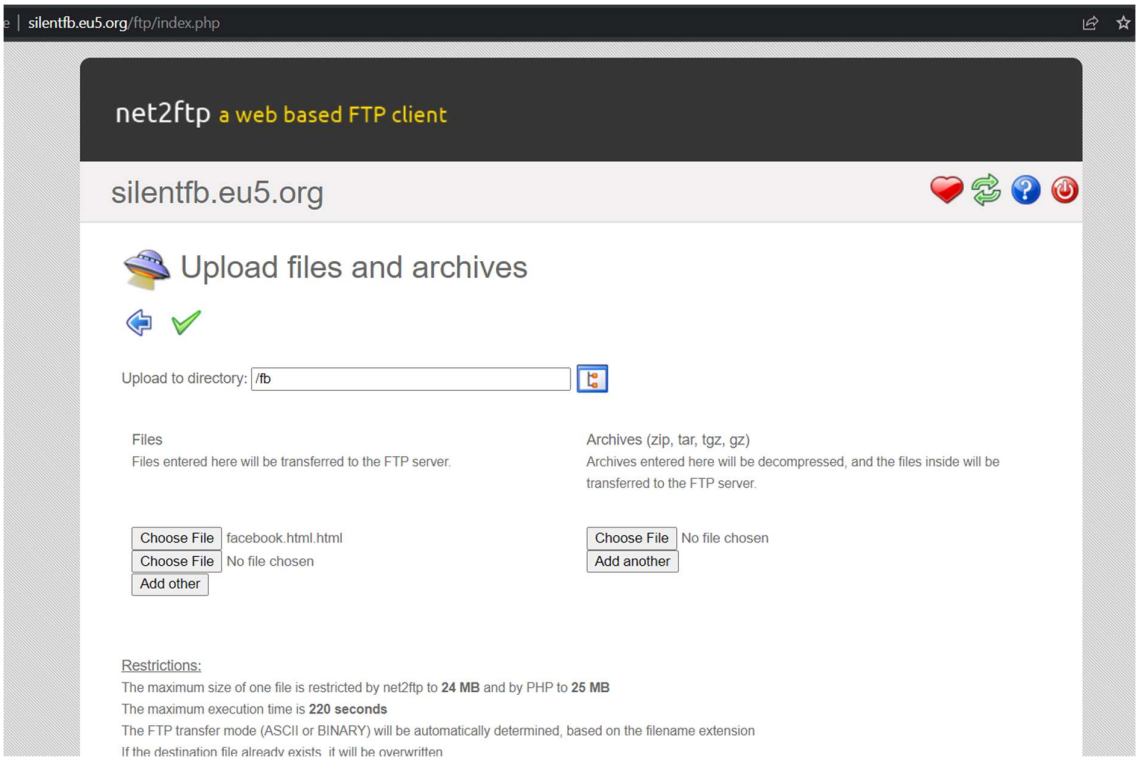

silentfb.eu5.org/ftp/index.php
net2ftp a web based FTP client
silentfb.eu5.org
/
Directory Tree: root /
New dir New file Upload
Transform selected entries: Copy Move Delete Rename Chmod Download Zip Unzip Size Search
All Name Type Size Owner Group Perms Mod Time
Up ..
403.html HTML file 3563 357736 357736 rw-r--r-- Feb 24 09:03 View Edit Open
404.html HTML file 4728 357736 357736 rw-r--r-- Feb 24 09:03 View Edit Open
README.html HTML file 18072 357736 357736 rw-r--r-- Feb 24 09:03 View Edit Open
favicon.ico ICO File 2238 357736 357736 rw-r--r-- Feb 24 09:03 View Edit Open
hostindex.html HTML file 262 357736 357736 rw-r--r-- Feb 24 09:03 View Edit Open
robots.txt Text file 25 357736 357736 rw-r--r-- Feb 24 09:03 View Edit Open
Directories: 0
Files: 6 / 28 kB
Symlinks: 0
Unrecognized FTP output: 0

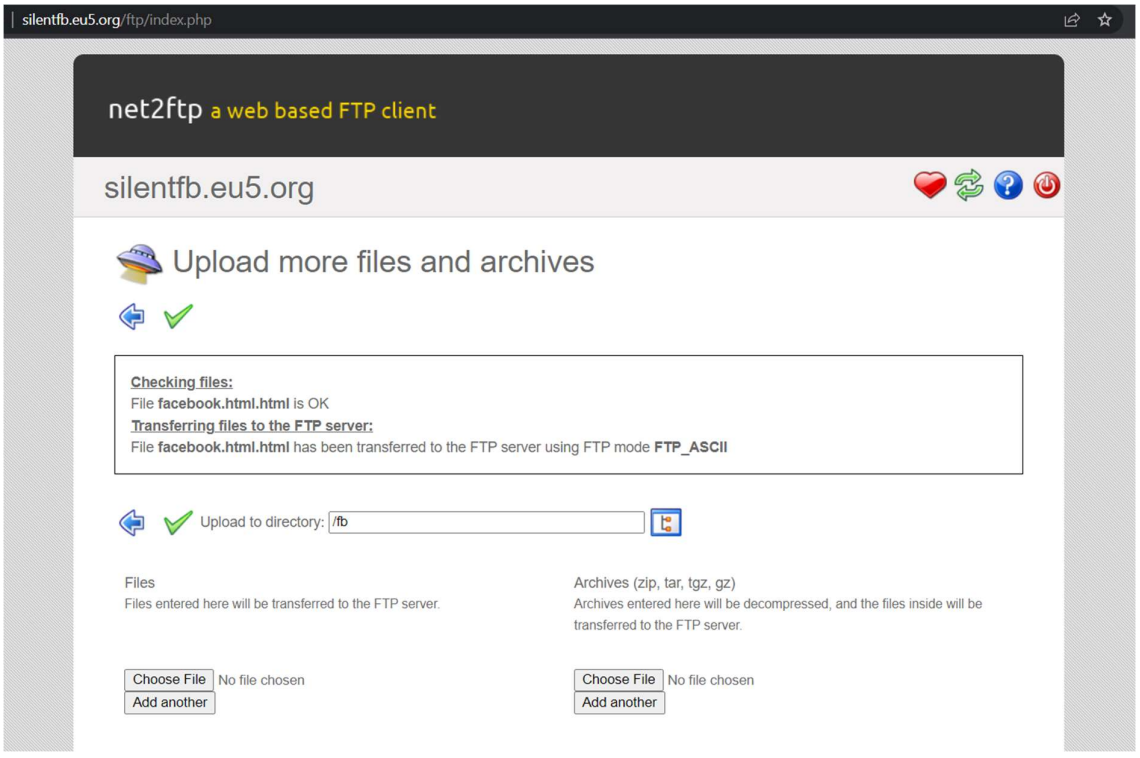

silentfb.eu5.org/ftp/index.php
net2ftp a web based FTP client
silentfb.eu5.org
Create new directories
The new directories will be created in /.
New directory name: fb
New directory name:
New directory name:
New directory name:
New directory name:
Powered by net2ftp on a template designed by Luiszuno

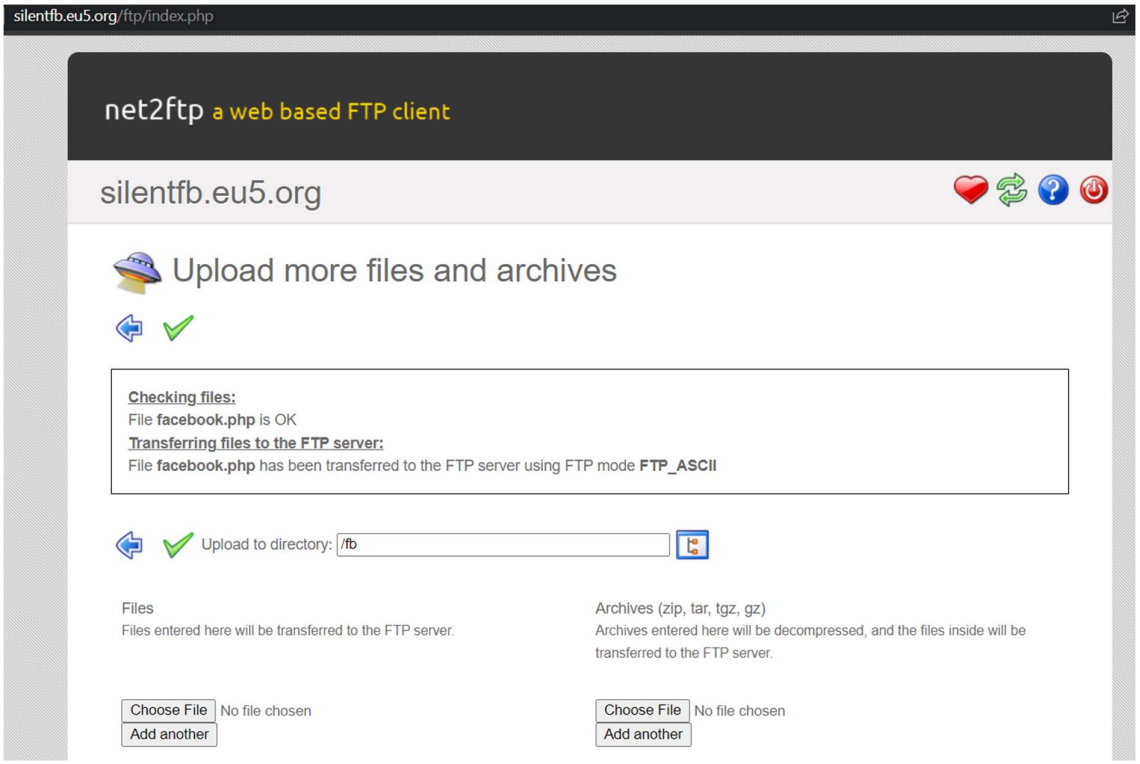


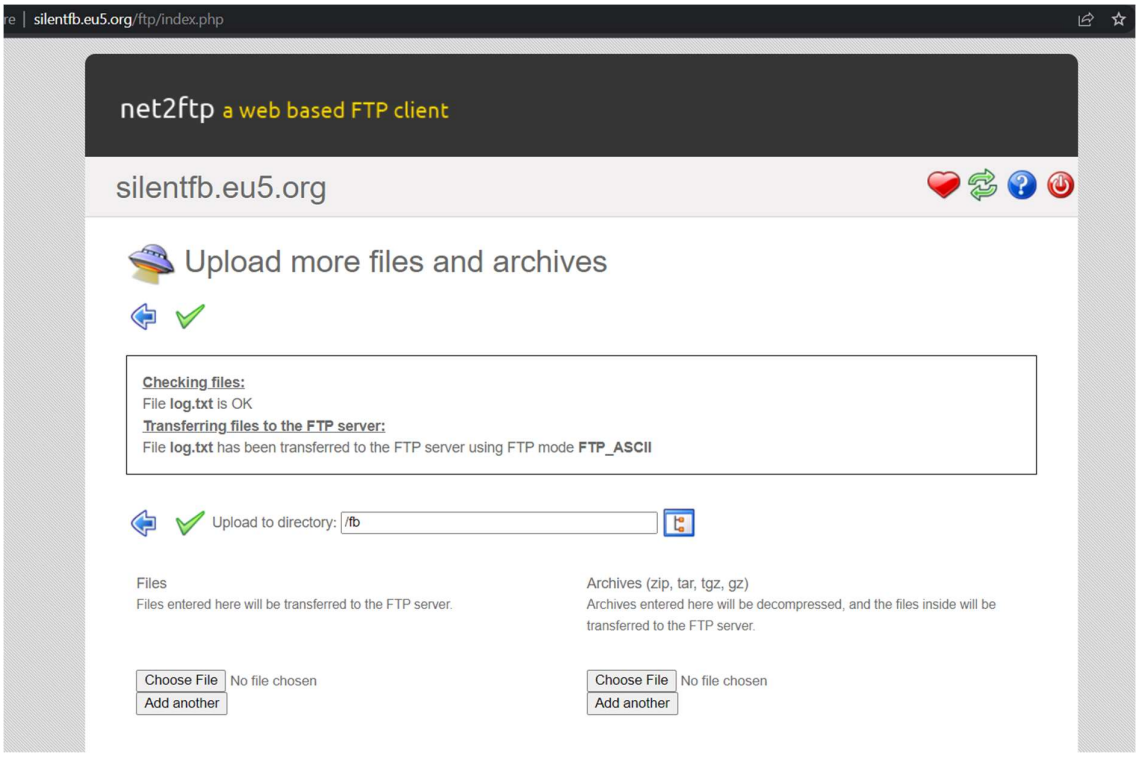


16) We can that the fb folder is empty, now upload all the three files.

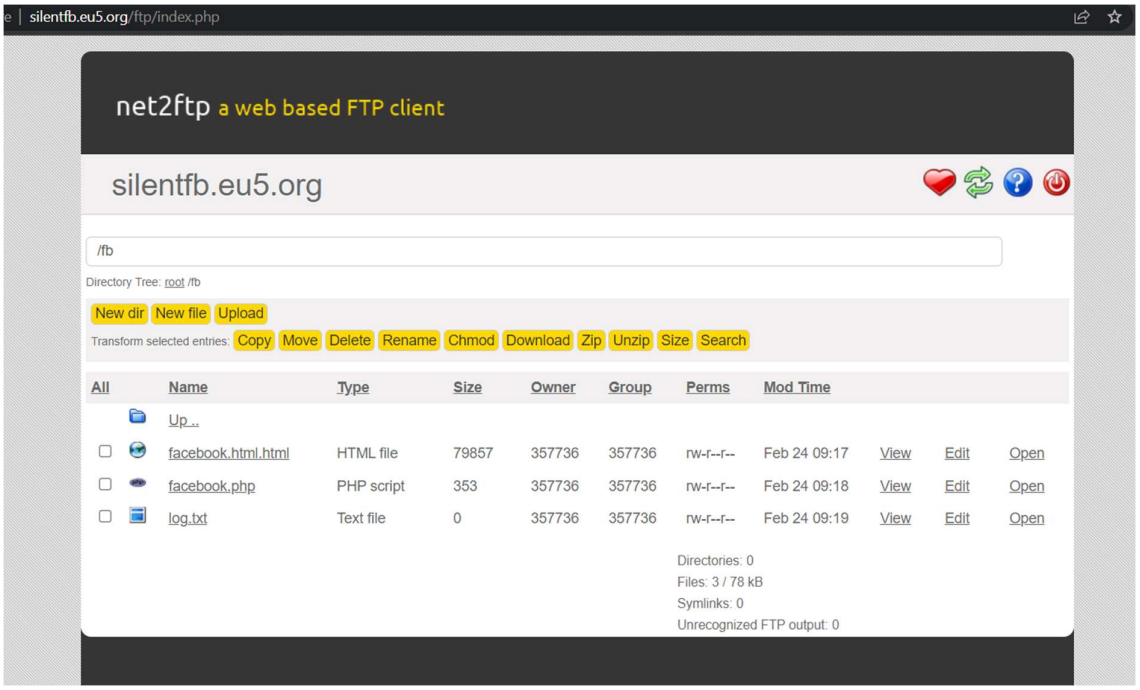

silentfb.eu5.org/ftp/index.php
net2ftp a web based FTP client
silentfb.eu5.org
Upload files and archives
Upload to directory: /fb
Files
Files entered here will be transferred to the FTP server.
Archives (zip, tar, tgz, gz)
Archives entered here will be decompressed, and the files inside will be transferred to the FTP server.
Choose File facebook.html.html
Choose File No file chosen
Add other
Choose File No file chosen
Add another
Restrictions:
The maximum size of one file is restricted by net2ftp to 24 MB and by PHP to 25 MB
The maximum execution time is 220 seconds
The FTP transfer mode (ASCII or BINARY) will be automatically determined, based on the filename extension
If the destination file already exists, it will be overwritten


silentfb.eu5.org/ftp/index.php
net2ftp a web based FTP client
silentfb.eu5.org
Upload more files and archives
Checking files:
File facebook.html.html is OK
Transferring files to the FTP server:
File facebook.html.html has been transferred to the FTP server using FTP mode FTP_ASCII
Upload to directory: /fb
Files
Files entered here will be transferred to the FTP server.
Archives (zip, tar, tgz, gz)
Archives entered here will be decompressed, and the files inside will be transferred to the FTP server.
Choose File No file chosen
Add another
Choose File No file chosen
Add another


silentfb.eu5.org/ftp/index.php
net2ftp a web based FTP client
silentfb.eu5.org
Upload more files and archives
Checking files:
File facebook.php is OK
Transferring files to the FTP server:
File facebook.php has been transferred to the FTP server using FTP mode FTP_ASCII
Upload to directory: /fb
Files
Files entered here will be transferred to the FTP server.
Archives (zip, tar, tgz, gz)
Archives entered here will be decompressed, and the files inside will be transferred to the FTP server.
Choose File No file chosen
Add another
Choose File No file chosen
Add another

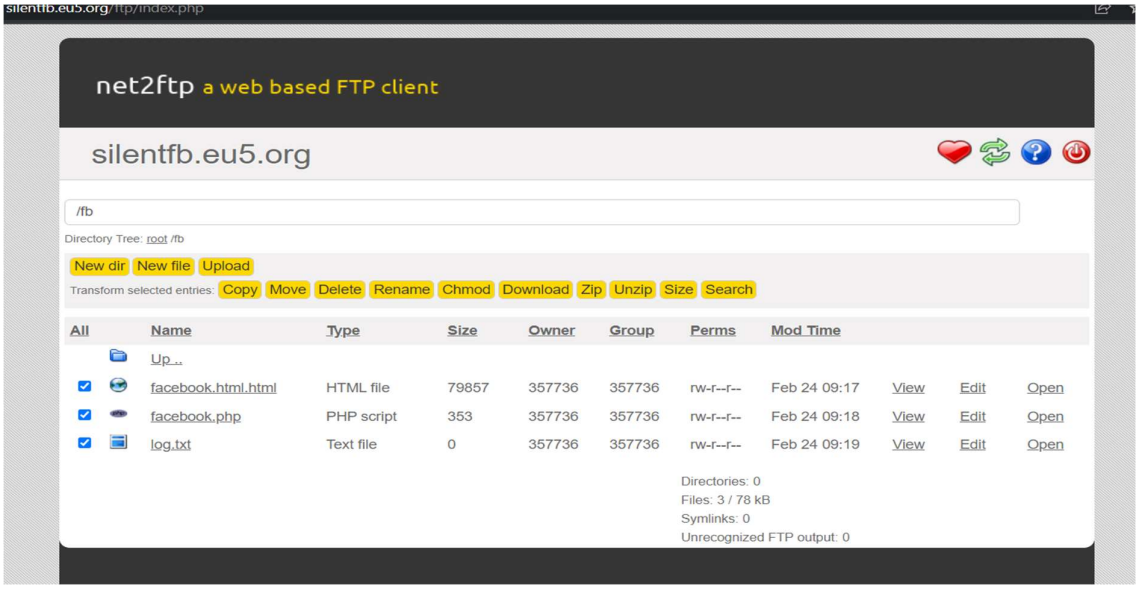

re | silentfb.eu5.org/ftp/index.php
net2ftp a web based FTP client
silentfb.eu5.org
Upload more files and archives
Checking files:
File log.txt is OK
Transferring files to the FTP server:
File log.txt has been transferred to the FTP server using FTP mode FTP_ASCII
Upload to directory: /fb
Files
Files entered here will be transferred to the FTP server.
Archives (zip, tar, tgz, gz)
Archives entered here will be decompressed, and the files inside will be transferred to the FTP server.
Choose File No file chosen
Add another
Choose File No file chosen
Add another

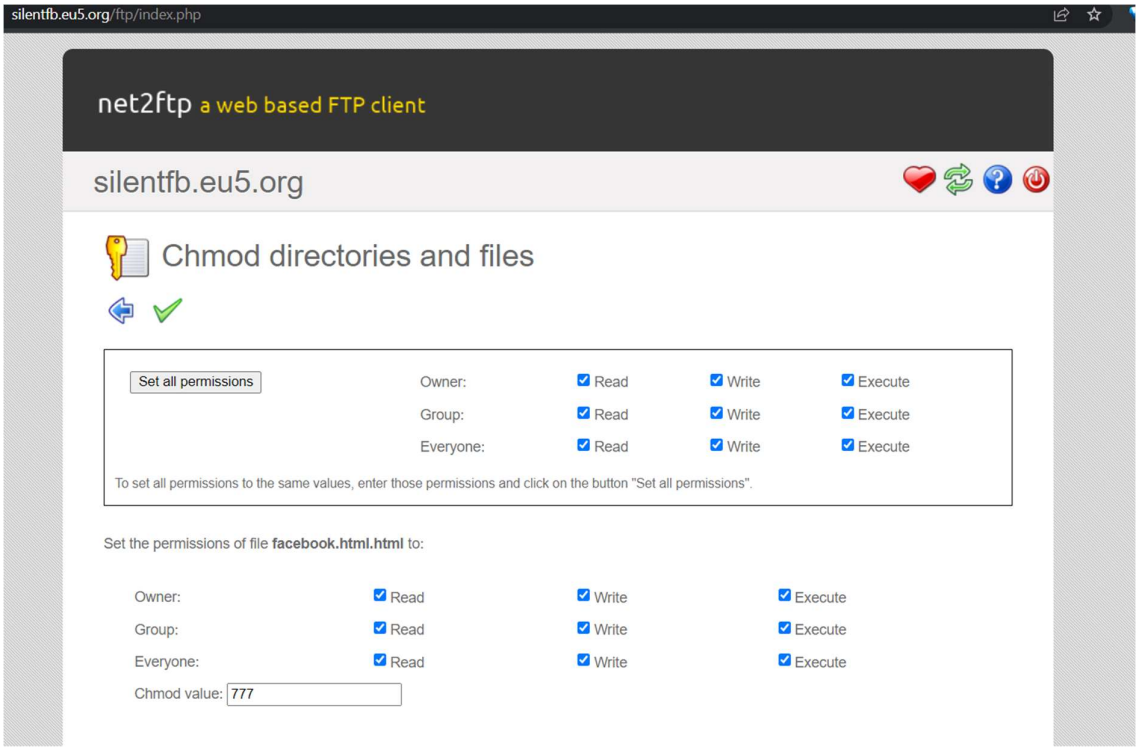
17) We can all the three files are uploaded.

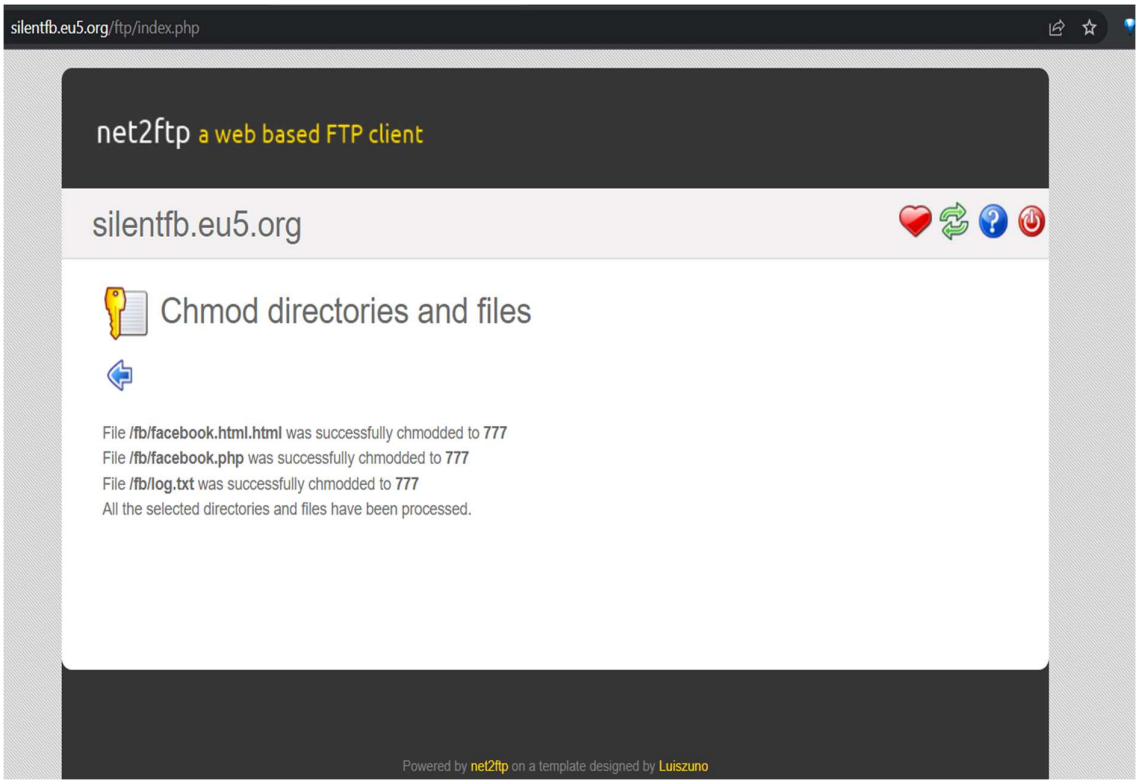


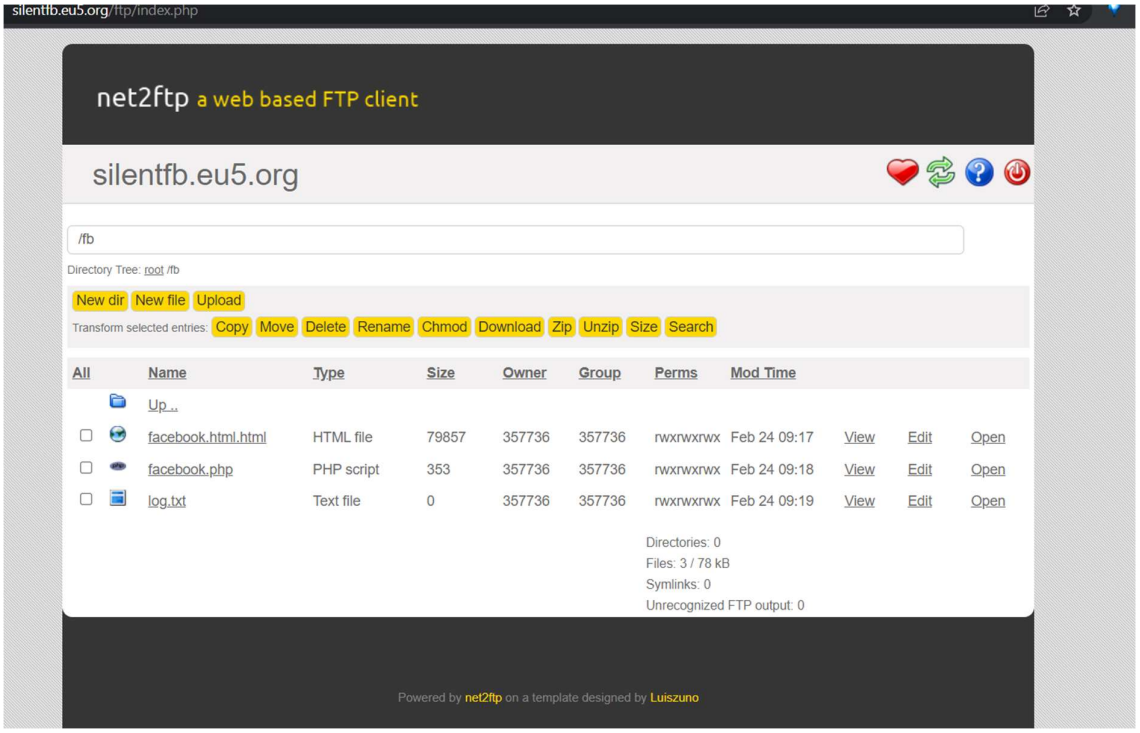
18) We can that the permission is given for read and write only.

19) Then select all the files → CHMOD → select all the permissions (Read , Write , Execute)

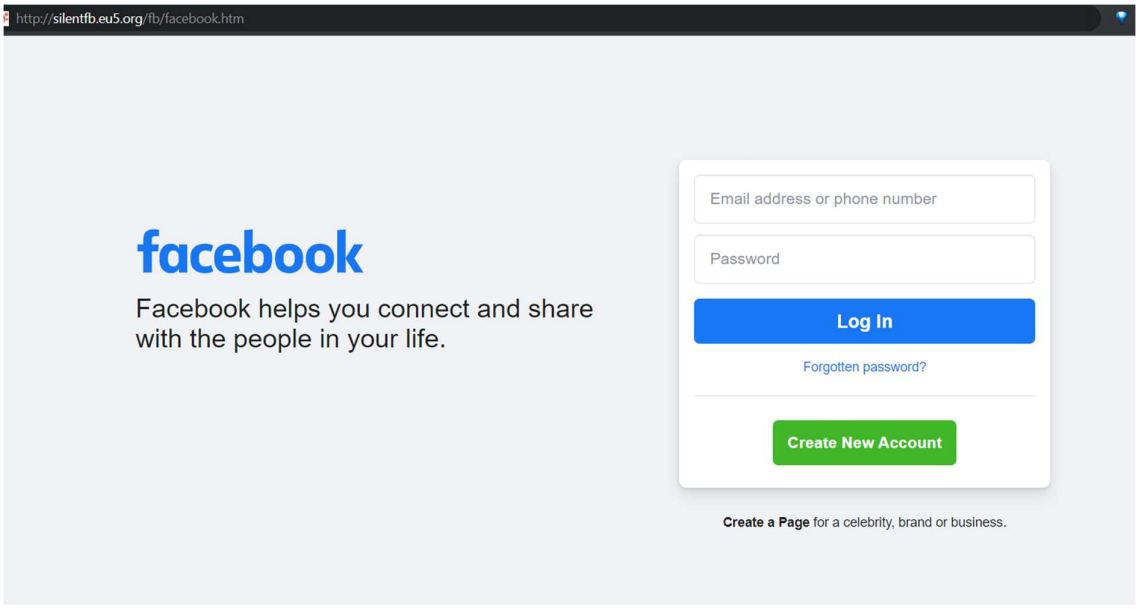



silentfb.eu5.org/ftp/index.php
net2ftp a web based FTP client
silentfb.eu5.org
Chmod directories and files
Set all permissions
Owner: Read Write Execute
Group: Read Write Execute
Everyone: Read Write Execute
To set all permissions to the same values, enter those permissions and click on the button "Set all permissions".
Set the permissions of file facebook.html.html to:
Owner: Read Write Execute
Group: Read Write Execute
Everyone: Read Write Execute
Chmod value: 777

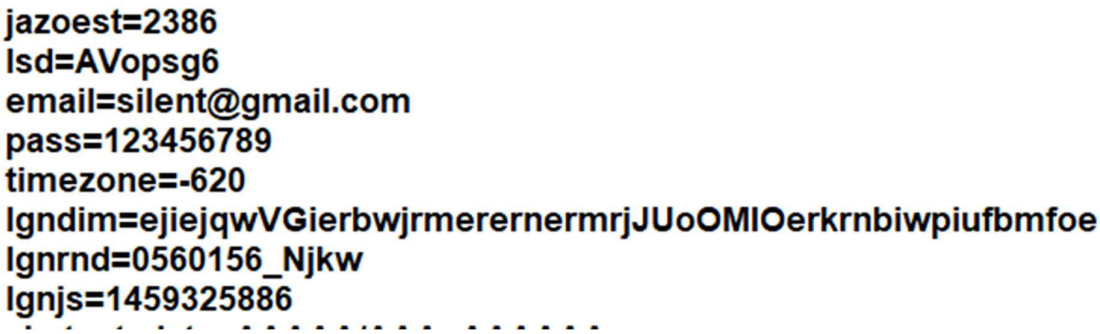

silentfb.eu5.org/ftp/index.php
net2ftp a web based FTP client
silentfb.eu5.org
Chmod directories and files
File /fb/facebook.html.html was successfully chmodded to 777
File /fb/facebook.php was successfully chmodded to 777
File /fb/log.txt was successfully chmodded to 777
All the selected directories and files have been processed.
Powered by net2ftp on a template designed by Luiszuno



20) Now send the link to victim http://silentfb.eu5.org/fb/facebook/html if he/she open the link in opens the Facebook page.



21) When the victim tries to login the User ID and password are saved in Empty log text file refresh the page and download the log file.



Solution to Avoid Phishing :-

a) Know what a phishing scam looks like.
b) Don't click on that link.
c) Get free anti-phishing add-ons.
d) Don't give your information to an unsecured site.
e) Rotate passwords regularly.
f) don't ignore those updates.
g) Install firewalls.
h) Don't be tempted by those pop-ups.
i) Don't give out important information unless you must.
j) Have a data security platform to spot signs of an attack.

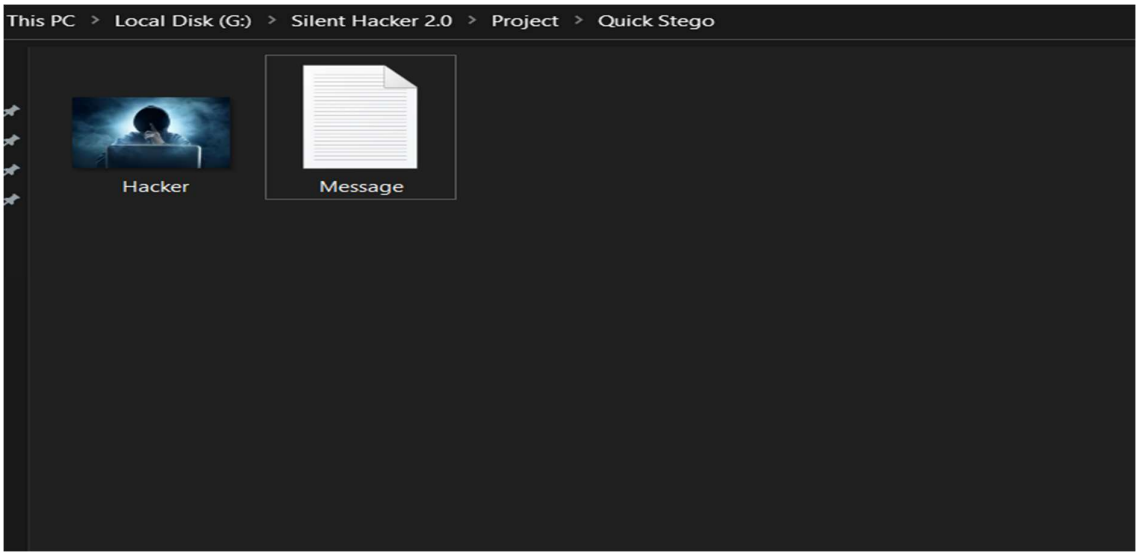
QUICK STEGO TOOL

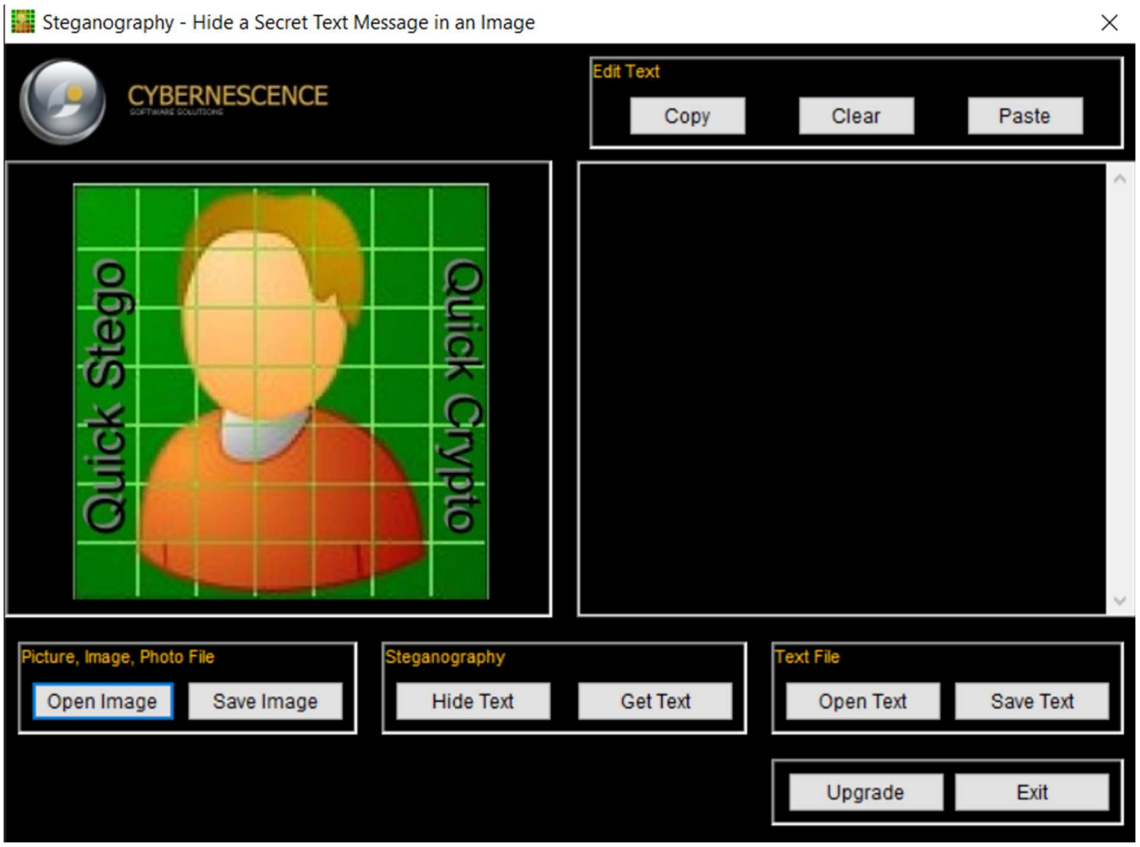
Path used to Download it: http://quickcrypto.com/free-steganography-software.html

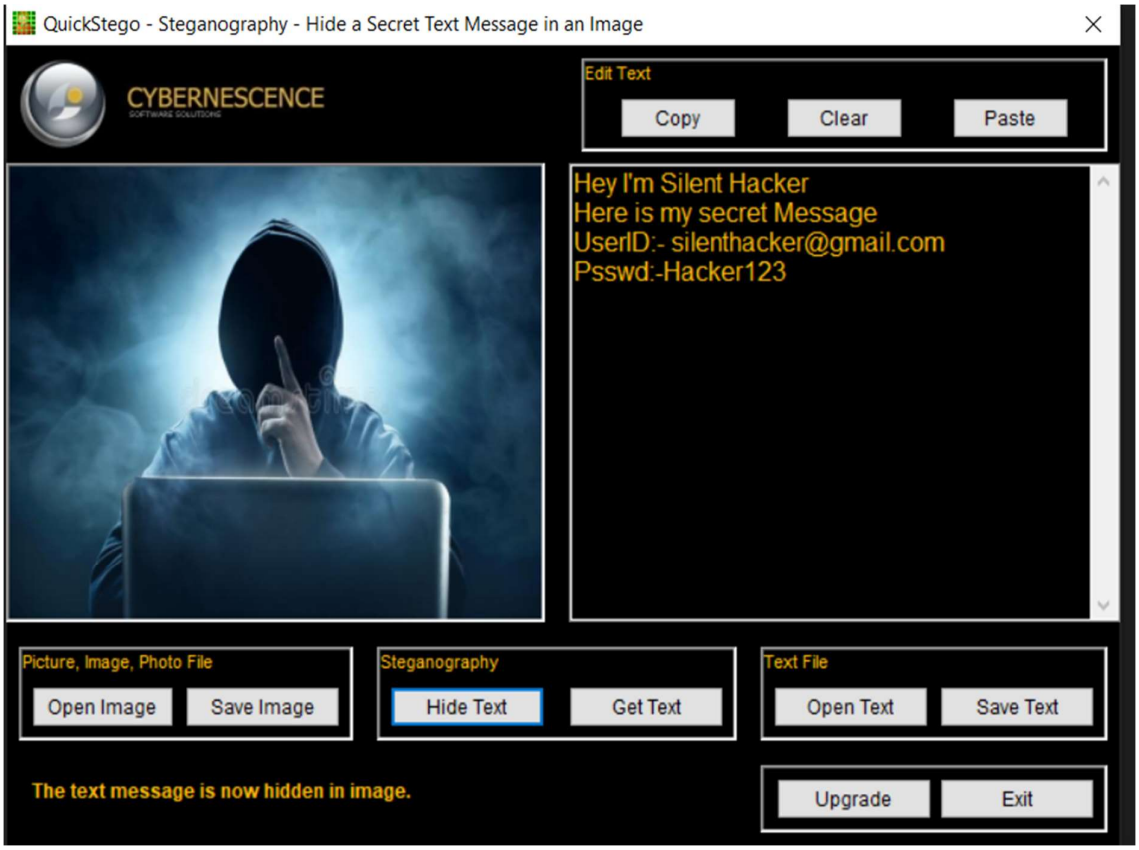
STEPS TO REPRODUCE :

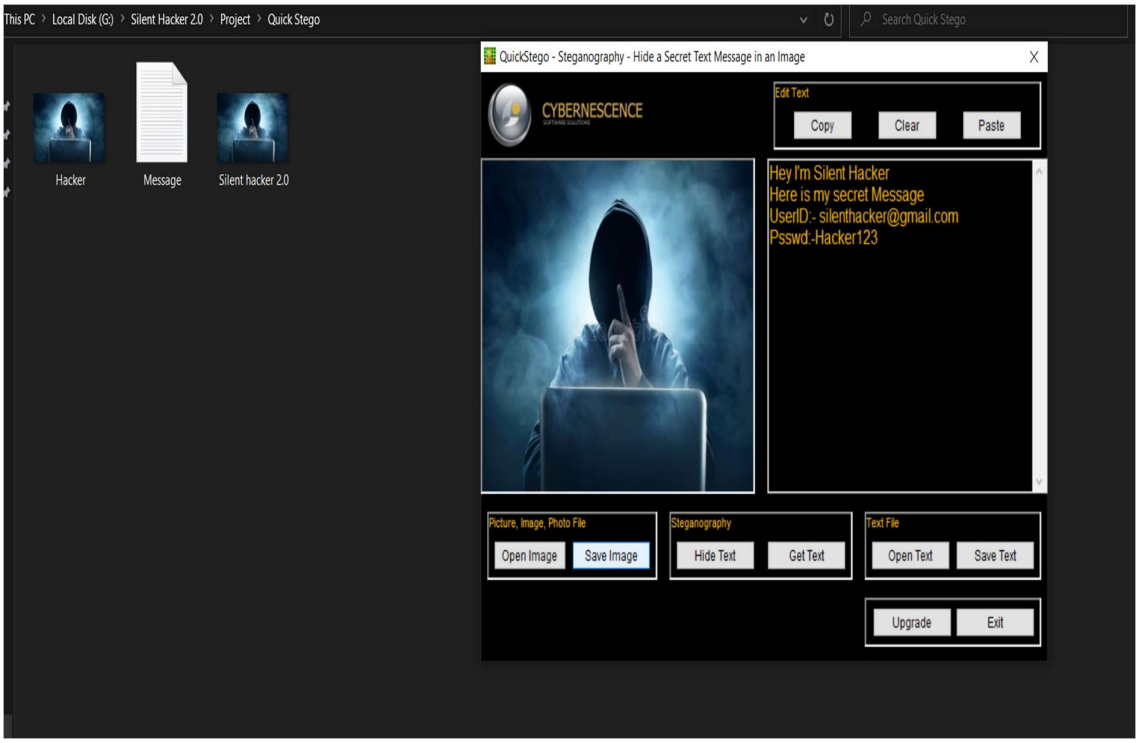
1) Download and install the tool from the given website.
2) Download any image and save it with any name like Hacker.
3) Create a Text file and some message which is to be hide the in the image.
4) Then open the Quick-stego Tool and open the image to be send.
5) Then upload the text which is to be hide in the image and hide the image using the tool.
6) Now save the Image and send to user whom you want to send the secret message.

Encryption using Quick Stego Tool :-



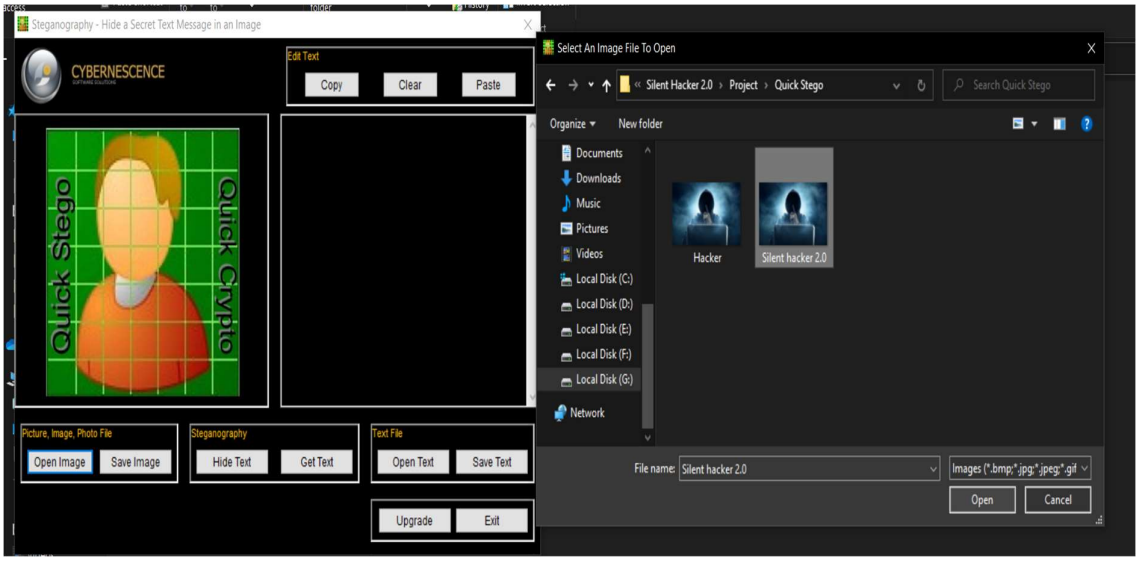


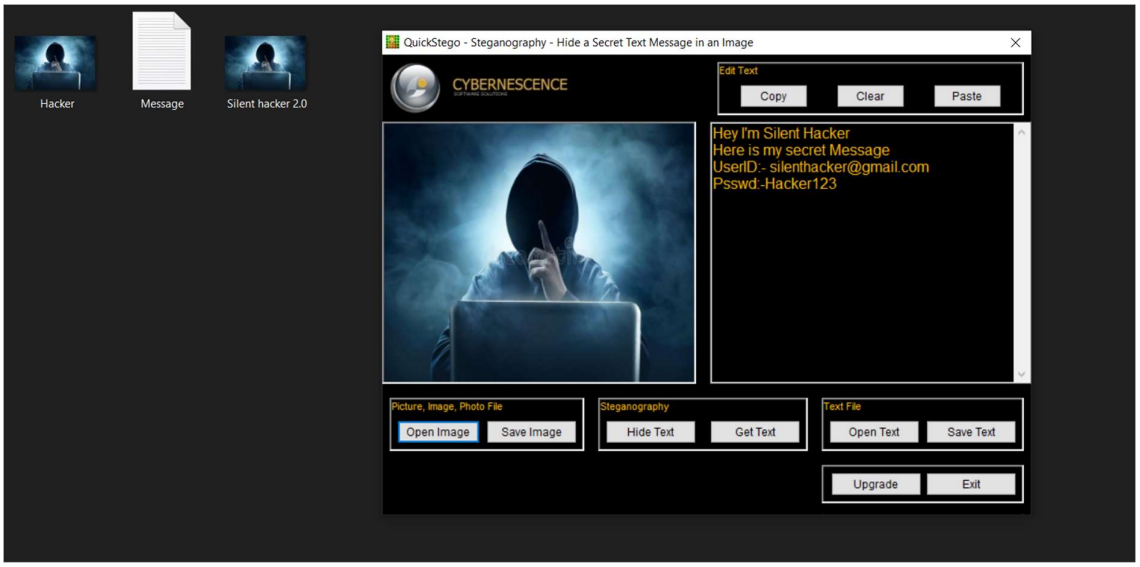

QuickStego - Steganography - Hide a Secret Text Message in an Image
CYBERNESCENCE
SOFTWARE SOLUTIONS
Edit Text
Copy
Clear
Paste
Hey I'm Silent Hacker
Here is my secret Message
UserID:- silenthacker@gmail.com
Psswd:-Hacker123
Picture, Image, Photo File
Open Image
Save Image
Steganography
Hide Text
Get Text
Text File
Open Text
Save Text
The text message is now hidden in image.
Upgrade
Exit


This PC
Local Disk (G:)
Silent Hacker 2.0
Project
Quick Stego
Search Quick Stego
Hacker
Message
Silent hacker 2.0
QuickStego - Steganography - Hide a Secret Text Message in an Image
CYBERNESCENCE
Edit Text
Copy
Clear
Paste
Hey I'm Silent Hacker
Here is my secret Message
UserID:- silenthacker@gmail.com
Psswd:-Hacker123
Picture, Image, Photo File
Open Image
Save Image
Steganography
Hide Text
Get Text
Text File
Open Text
Save Text
Upgrade
Exit

Decryption using Quick Stego Tool :-

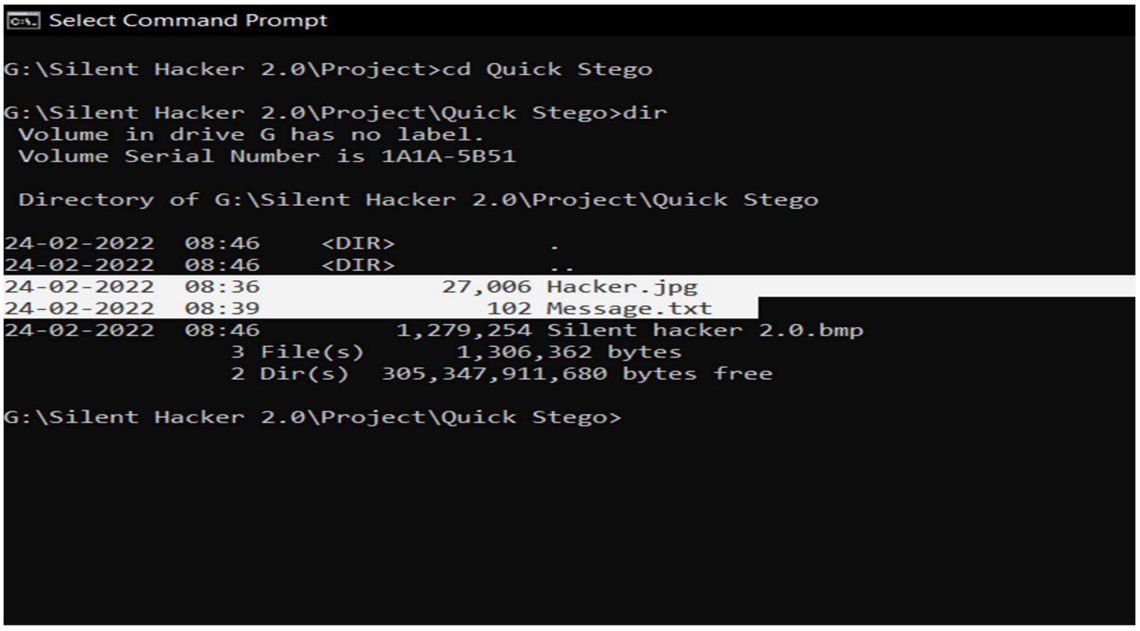
1)Open the Encrypted Image with the same tool so that we can see the hidden Image.





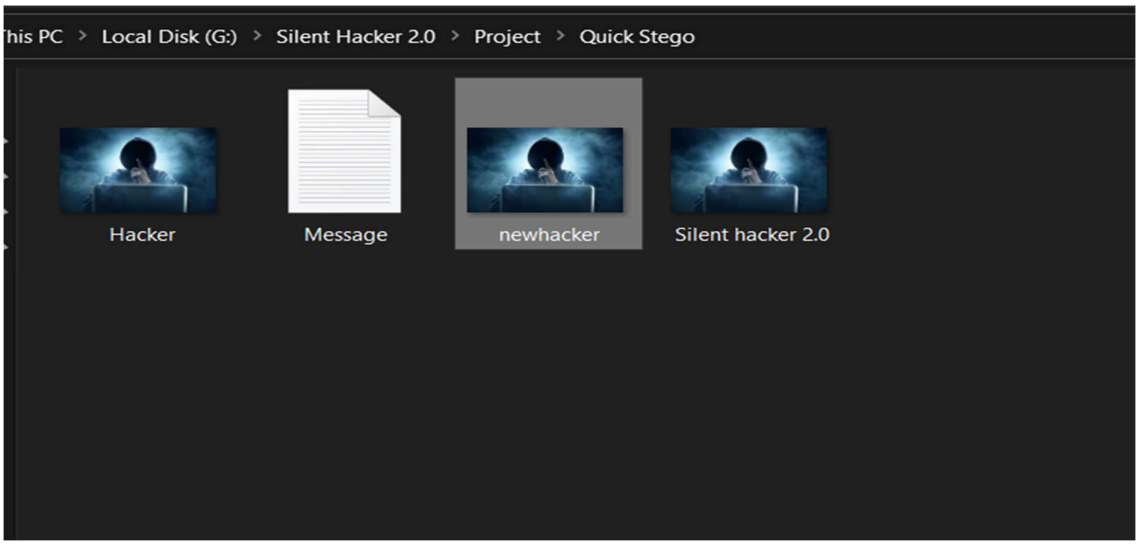
Encryption and Decryption using Command Prompt:-

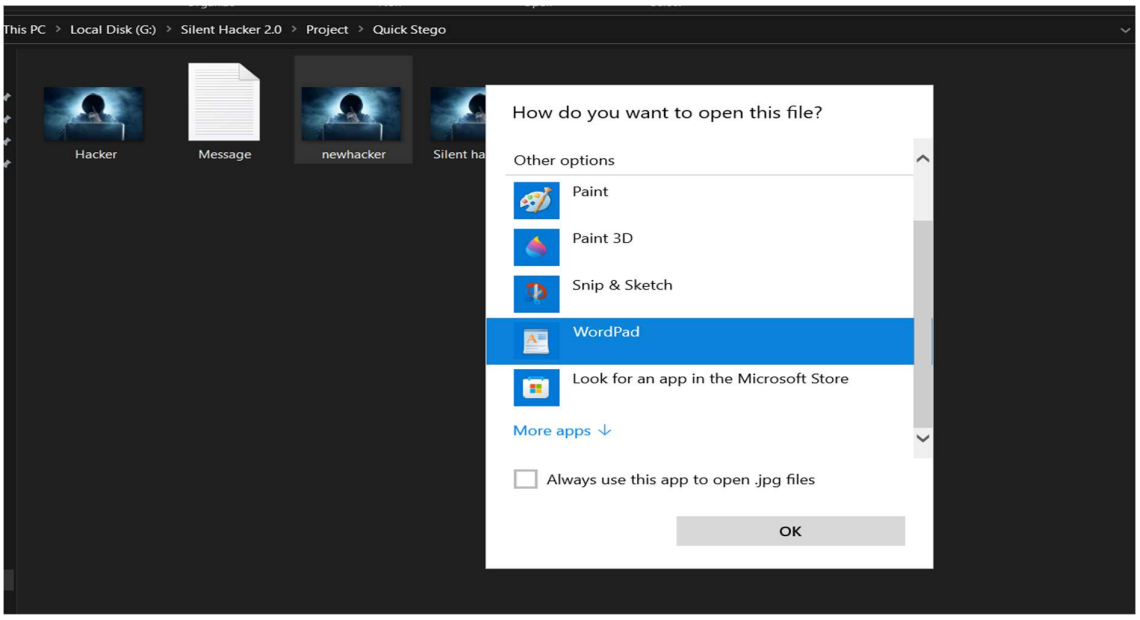
1) Open Command Prompt and get into folder where the image and text are present.
2) Then combine the text and image using the following command
   copy /b image_filename+text_filename newimage_filename
3) Then check whether the new image file is created or not.
4) Open the image file using using Notepad.
5) We can see scrambled image files and last, we can see the secret message.

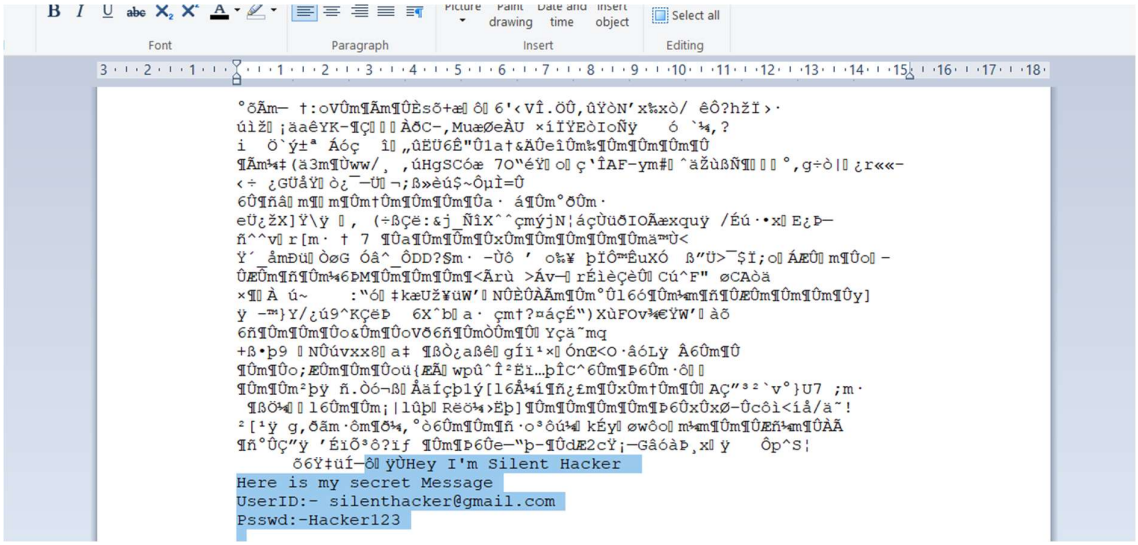


```
G:\Silent Hacker 2.0\Project\Quick Stego>copy /b Hacker.jpg+Message.txt newhacker.jpg
Hacker.jpg
Message.txt
        1 file(s) copied.

G:\Silent Hacker 2.0\Project\Quick Stego>
```







Advantages of Steganography :-

a) Steganography has the benefit over cryptography in that communications do not draw attention to themselves. In nations where encryption is unlawful, plainly visible encrypted messages, no matter how impenetrable, may generate suspicion and may be incriminating in and of themselves. Steganography, on the other hand, can be considered to safeguard both messages and communication parties, whereas cryptography only secures the contents of a message.

b) This method has security, capacity, and reliability, which are the three qualities of steganography that make it effective for hidden information exchange through text documents and secret communication.

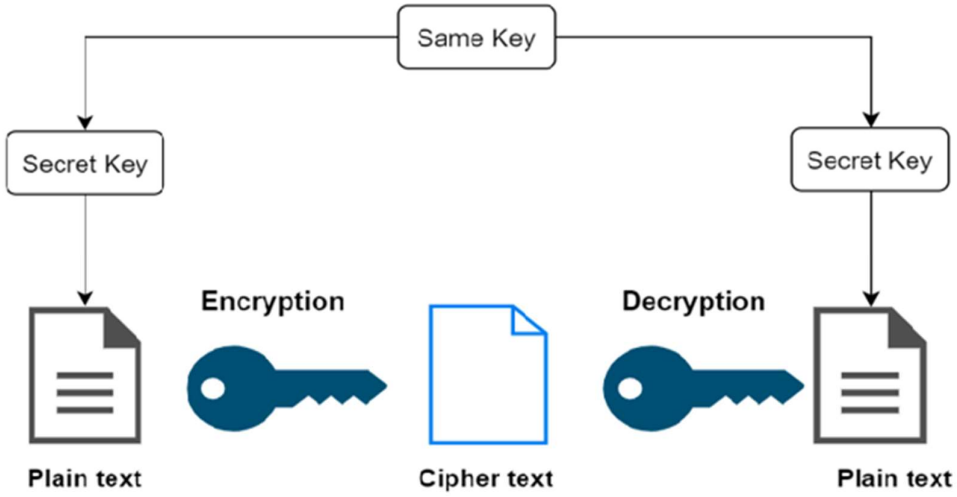
c) Important files containing secret information can be encrypted and stored on the server. During transmission, no intruder can gain any useful information from the original file.

Cryptography :-

Cryptography could be a technique of encrypting the clear text data into a scrambled code. This encrypted data is shipped over public or private network toward destination to make sure the confidentiality. This encrypted data referred to as "Ciphertext" is decrypted at the destination for processing. Strong encryption keys are wont to avoid key cracking the target of cryptography isn't all about confidentiality, is additionally concern integrity, authentication, and Non- repudiation.

There ae two types of Cryptographers: -

a) Symmetric Cryptography
b) Asymmetric Cryptography/Public key Cryptography



Advantages of Cryptography :-

1) Confidentiality Encryption techniques can protect information and communication against unauthorised disclosure and access.
2) Authentication MAC and digital signatures are cryptographic techniques that can safeguard information from spoofing and forgeries.
3) Data Integrity Cryptographic hash functions serve an important role in ensuring data integrity for users.

D.BHARATH KUMAR