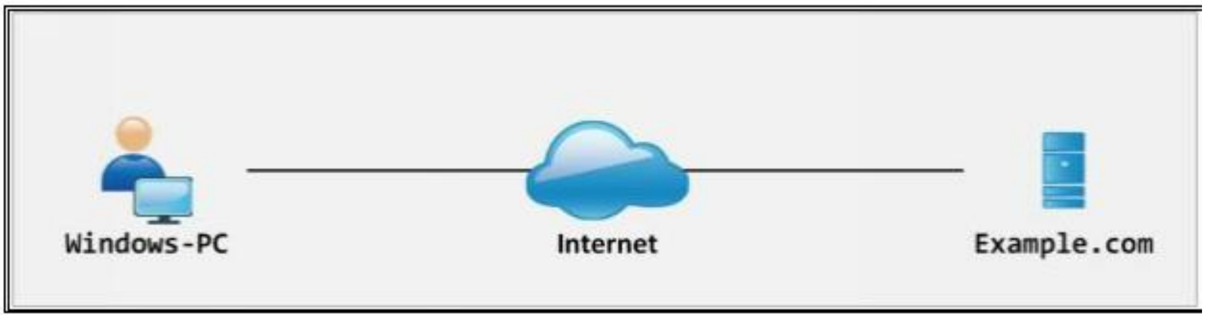
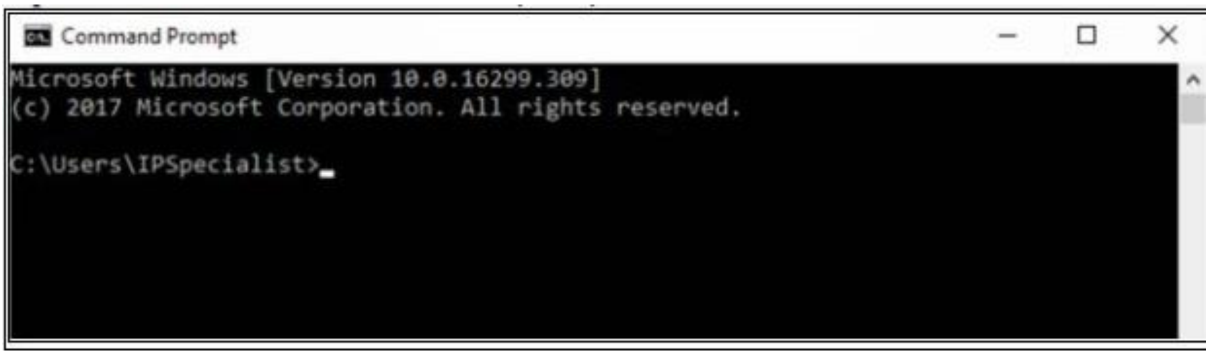
Practical No 1: Windows Command Line Utilities Ping.

Consider a network where you have access to a Windows PC connected to the Internet. Using Windows-based tools, let's gather some information about the target. You can assume any target domain or IP address, in our case, we are using **example.com** as a target.

Topology Diagram:

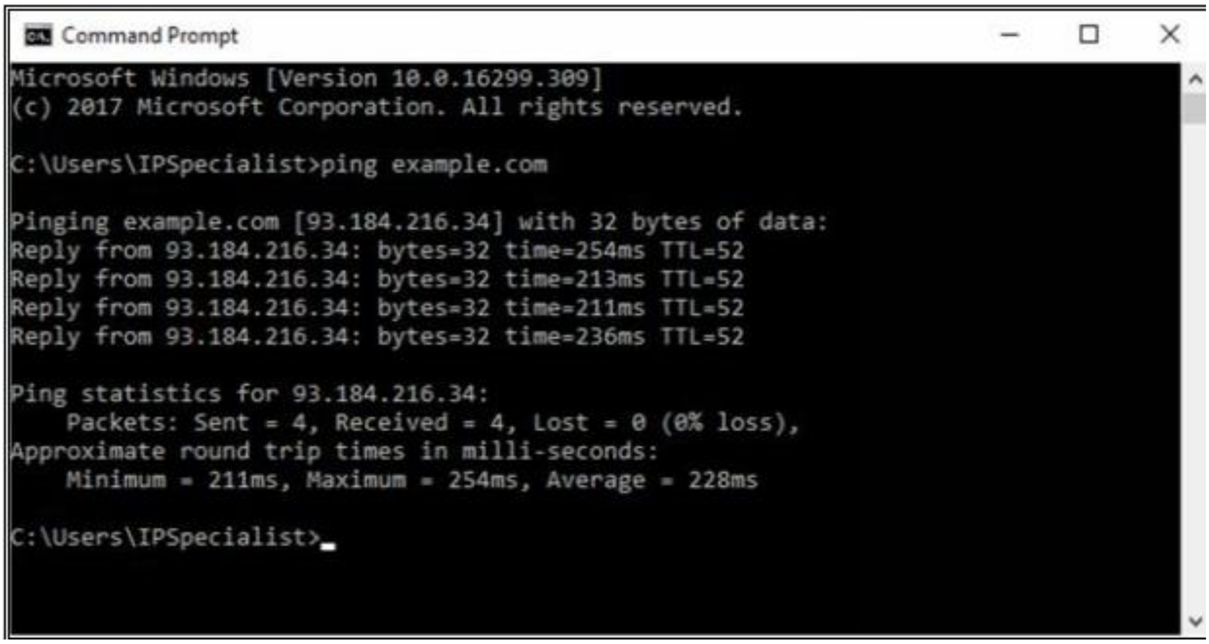


1- Open Windows Command Line (cmd) from Windows PC



```
Microsoft Windows [Version 10.0.16299.309]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\IPSpecialist>_
```

2 -Enter the command “ **Ping example.com** ” to ping.



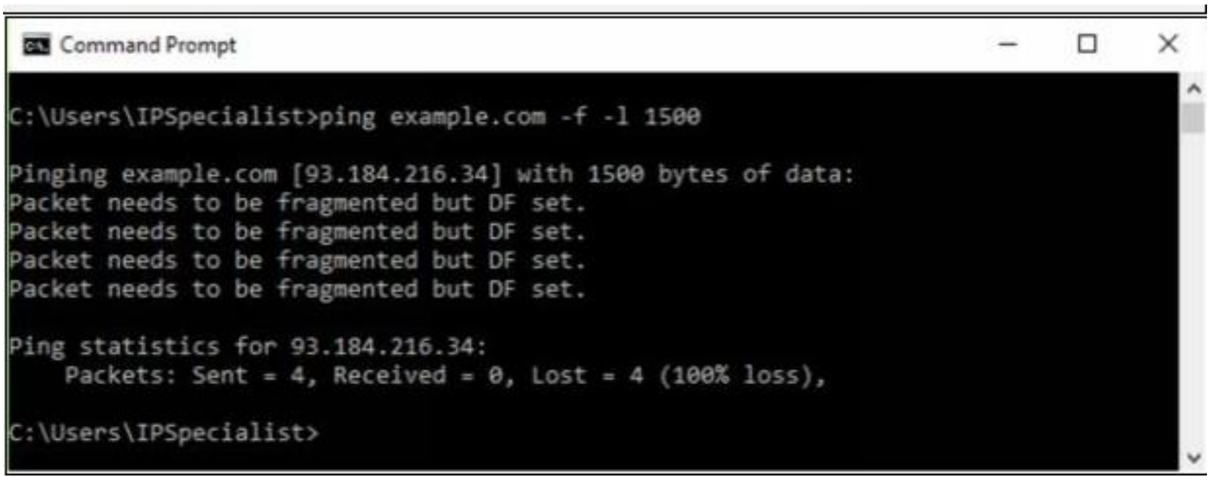
```
Microsoft Windows [Version 10.0.16299.309]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\IPSpecialist>ping example.com

Pinging example.com [93.184.216.34] with 32 bytes of data:
Reply from 93.184.216.34: bytes=32 time=254ms TTL=52
Reply from 93.184.216.34: bytes=32 time=213ms TTL=52
Reply from 93.184.216.34: bytes=32 time=211ms TTL=52
Reply from 93.184.216.34: bytes=32 time=236ms TTL=52

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 211ms, Maximum = 254ms, Average = 228ms

C:\Users\IPSpecialist>_
```

From the output, you can observe and extract the following information:

- Example.com is live
- IP address of example.com.

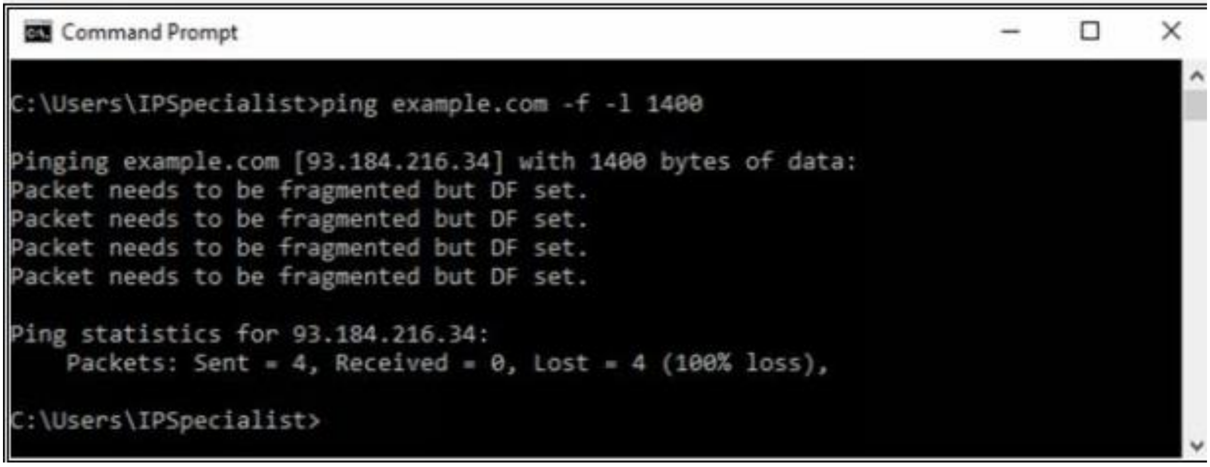
- Round Trip Time
- TTL value
- Packet loss statistics

3- Now, Enter the command “ Ping example.com –f –l 1500 ” to check the value of fragmentation.



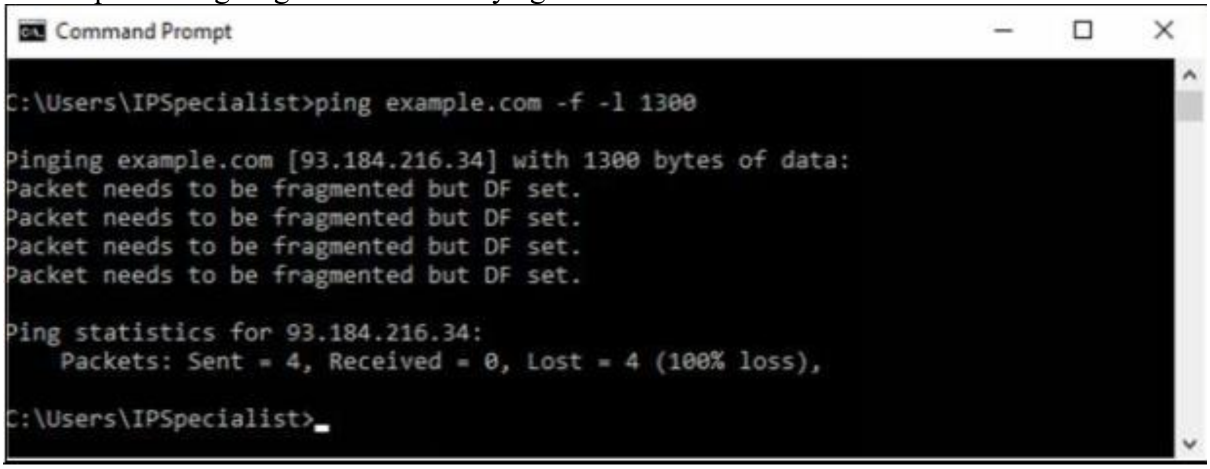
```
C:\Users\IPSpecialist>ping example.com -f -l 1500

Pinging example.com [93.184.216.34] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\IPSpecialist>
```

The output shows “ **Packet needs to be fragmented but DF set** ” which means 150o bits will require being fragmented. Let’s try again with smaller value:



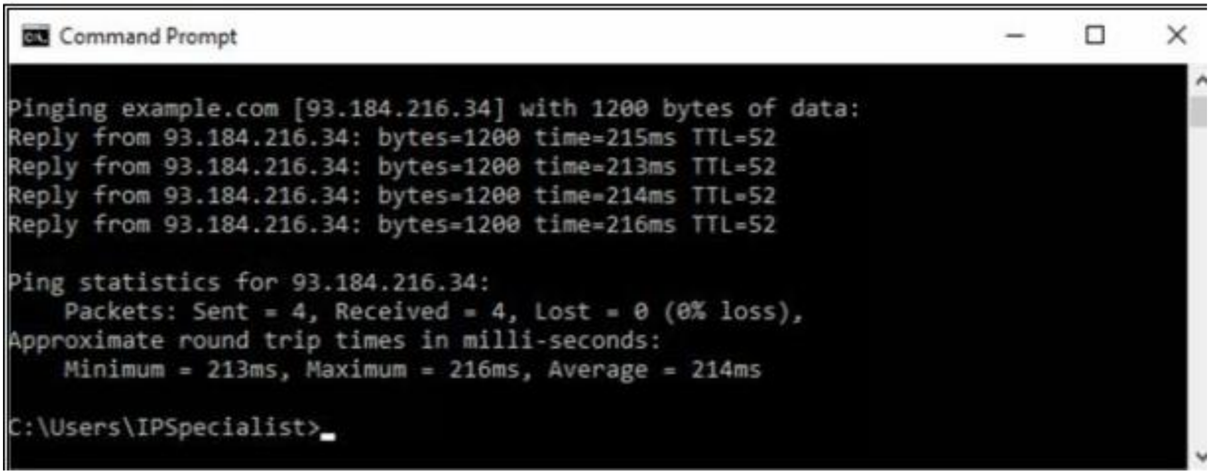
```
C:\Users\IPSpecialist>ping example.com -f -l 1400

Pinging example.com [93.184.216.34] with 1400 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\IPSpecialist>
```

Output again shows “ **Packet needs to be fragmented but DF set** ” which means 140o bits will require being fragmented. Let’s try again with smaller value:



```
C:\Users\IPSpecialist>ping example.com -f -l 1300

Pinging example.com [93.184.216.34] with 1300 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\IPSpecialist>_
```

Output again shows “ **Packet needs to be fragmented but DF set** ” which means 130o bits will require being fragmented. Let’s try again with smaller value:

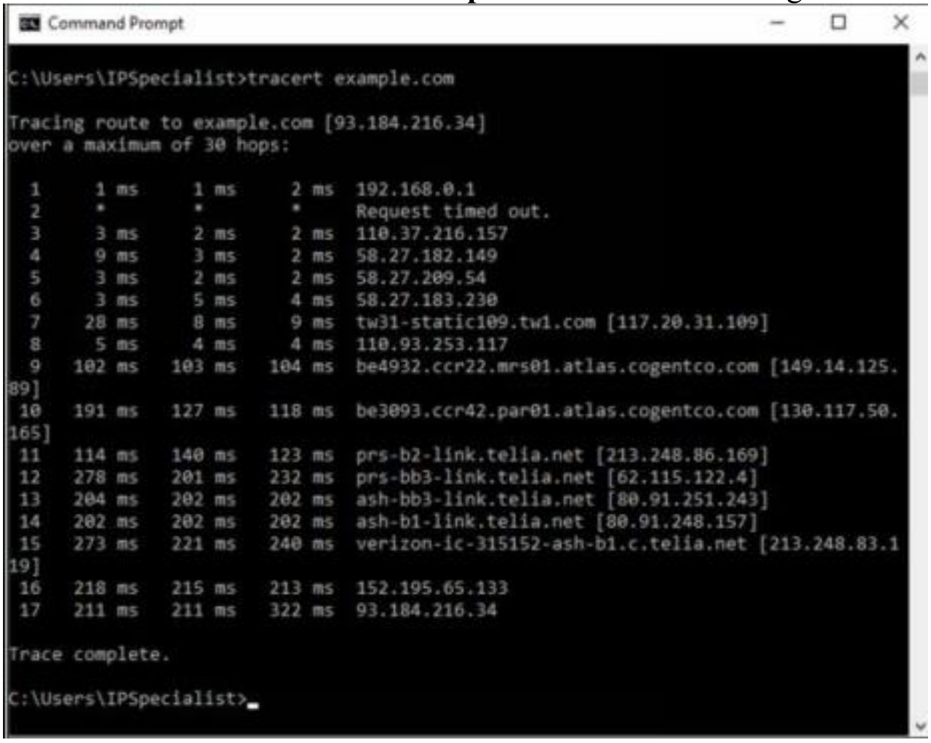


```
Pinging example.com [93.184.216.34] with 1200 bytes of data:
Reply from 93.184.216.34: bytes=1200 time=215ms TTL=52
Reply from 93.184.216.34: bytes=1200 time=213ms TTL=52
Reply from 93.184.216.34: bytes=1200 time=214ms TTL=52
Reply from 93.184.216.34: bytes=1200 time=216ms TTL=52

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 213ms, Maximum = 216ms, Average = 214ms

C:\Users\IPSpecialist>_
```

The output shows the reply now, which means 120o bits will not require being fragmented. You can try again to get the more appropriate fragment value.

Practical No 2: Windows Command Line Utilities Tracert Using Ping.

Enter the command “ **Tracert example.com** ” to trace the target.

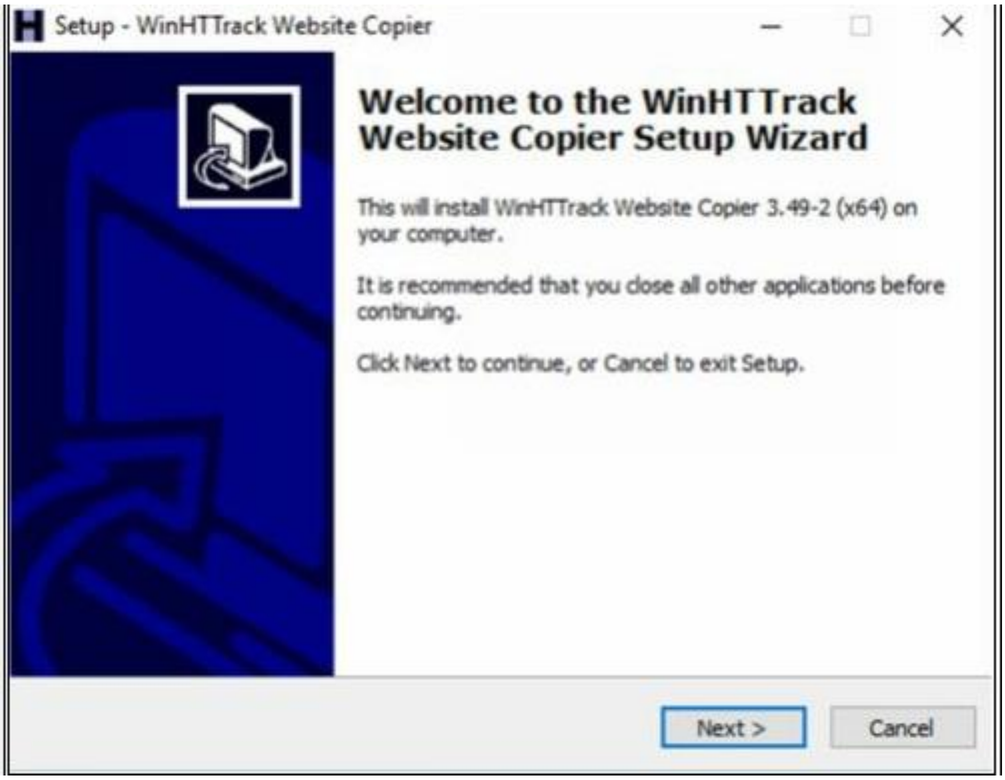


```
C:\Users\IPSpecialist>tracert example.com

Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1     1 ms     1 ms     2 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     3 ms     2 ms     2 ms  110.37.216.157
  4     9 ms     3 ms     2 ms  58.27.182.149
  5     3 ms     2 ms     2 ms  58.27.209.54
  6     3 ms     5 ms     4 ms  58.27.183.230
  7    28 ms     8 ms     9 ms  tw31-static109.tw1.com [117.20.31.109]
  8     5 ms     4 ms     4 ms  110.93.253.117
  9   102 ms   103 ms   104 ms  be4932.ccr22.mrs01.atlas.cogentco.com [149.14.125.
89]
 10   191 ms   127 ms   118 ms  be3093.ccr42.par01.atlas.cogentco.com [130.117.50.
165]
 11   114 ms   140 ms   123 ms  prs-b2-link.telia.net [213.248.86.169]
 12   278 ms   201 ms   232 ms  prs-bb3-link.telia.net [62.115.122.4]
 13   204 ms   202 ms   202 ms  ash-bb3-link.telia.net [80.91.251.243]
 14   202 ms   202 ms   202 ms  ash-b1-link.telia.net [80.91.248.157]
 15   273 ms   221 ms   240 ms  verizon-ic-315152-ash-b1.c.telia.net [213.248.83.1
19]
 16   218 ms   215 ms   213 ms  152.195.65.133
 17   211 ms   211 ms   322 ms  93.184.216.34

Trace complete.

C:\Users\IPSpecialist>_
```

From the output, you can get the information about hops between the source (your PC) and the destination (example.com), response times and other information.

Practical No 3: Website Copier Tool (Httrack)

1- Download and Install the WinHTTrack Website Copier Tool from the website **http://www.httrack.com**. You can check the compatibility of HTTrack Website copier tool on different platforms such as Windows, Linux, and Android from the website.



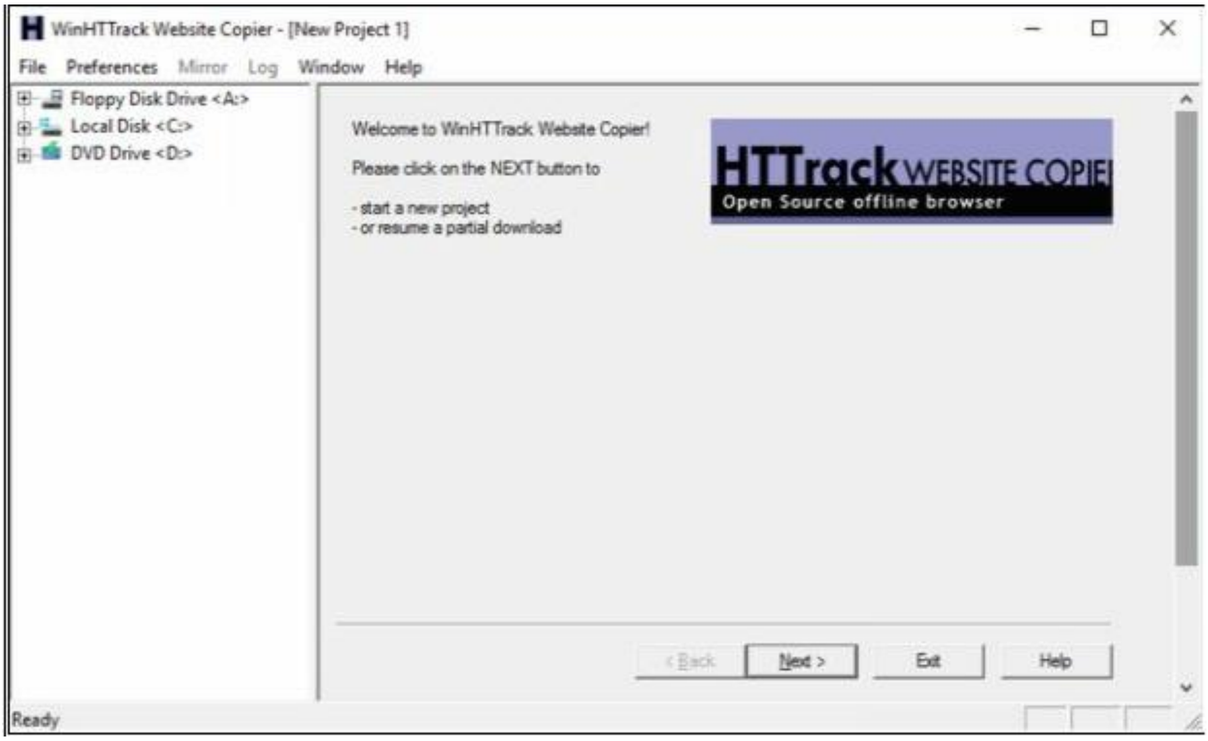
Welcome to the WinHTTrack Website Copier Setup Wizard

This will install WinHTTrack Website Copier 3.49-2 (x64) on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

2-HTTrack Website Copier tool installation

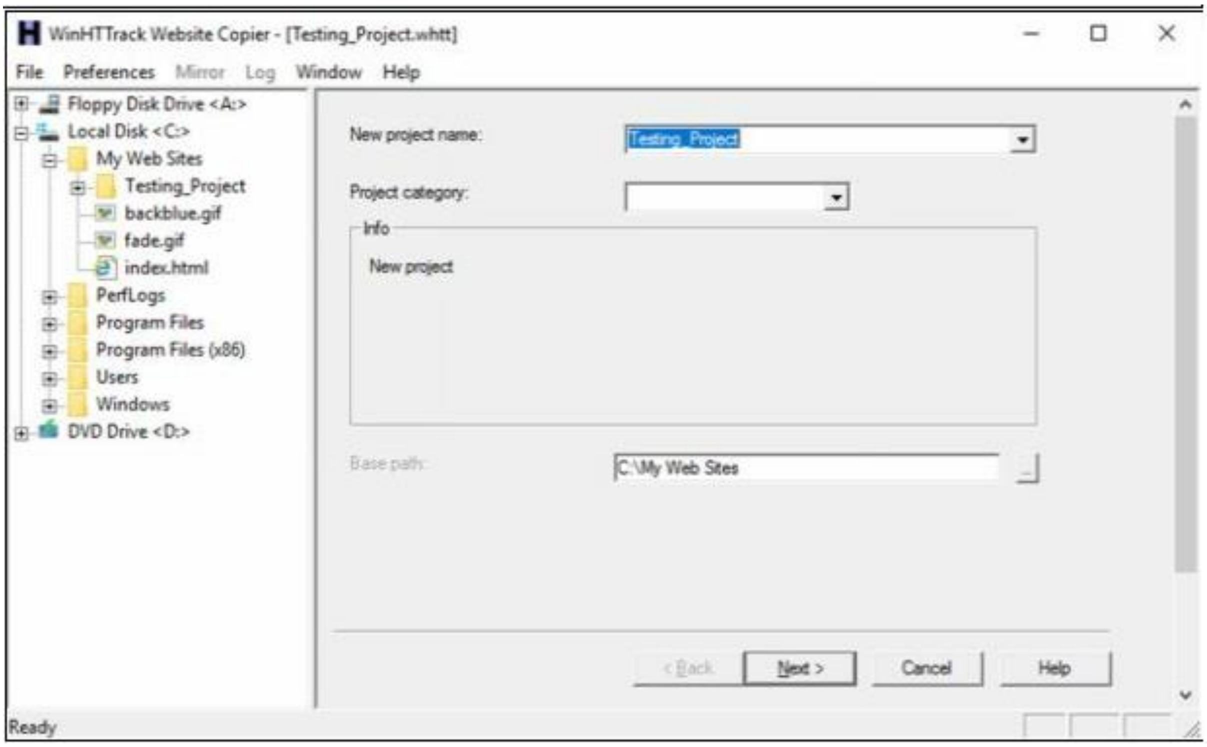

WinHTTrack Website Copier - [New Project 1]
File Preferences Mirror Log Window Help
Floppy Disk Drive <A:>
Local Disk <C:>
DVD Drive <D:>
HTTrack WEBSITE COPIER
Open Source offline browser
< Back
Next >
Exit
Help
Ready

Welcome to WinHTTrack Website Copier!

Please click on the NEXT button to

- start a new project
- or resume a partial download

3-Click Next



New project name: Testing_Project

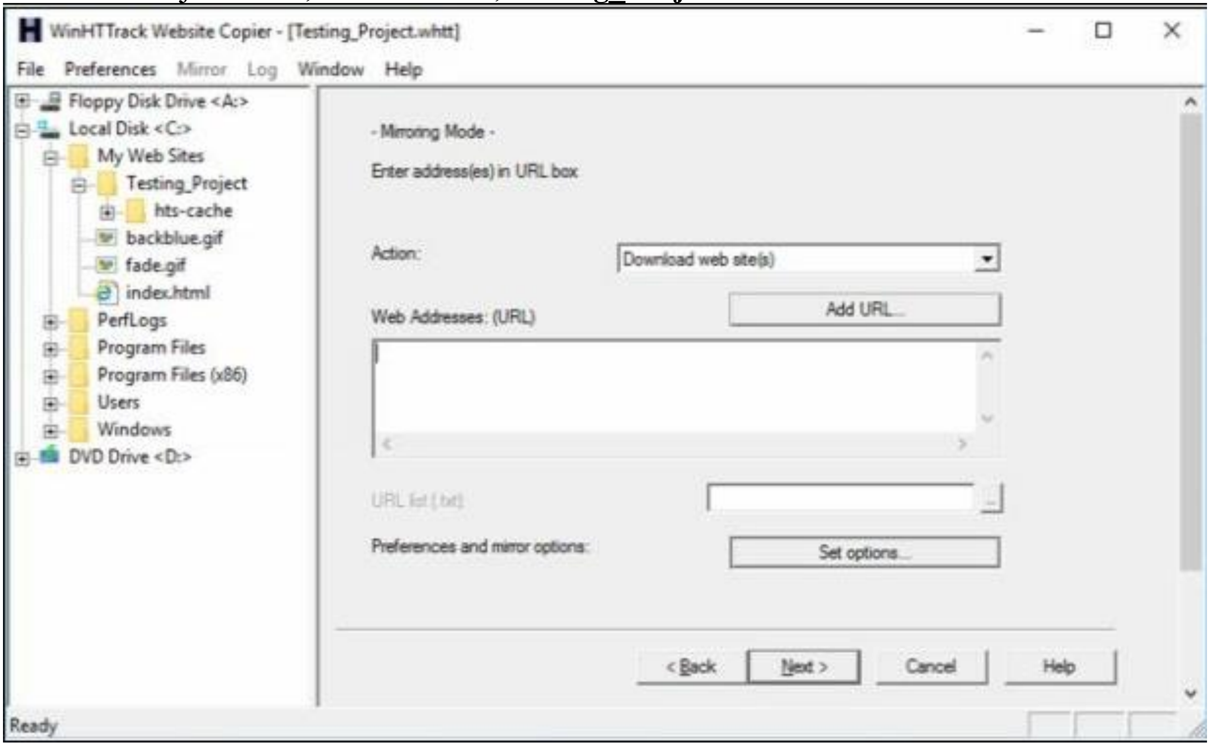
Project category:

Info

New project

Base path: C:\My Web Sites

4- Enter a Project name, as in our case, **Testing_Project.**



- Mirroring Mode -

Enter address(es) in URL box

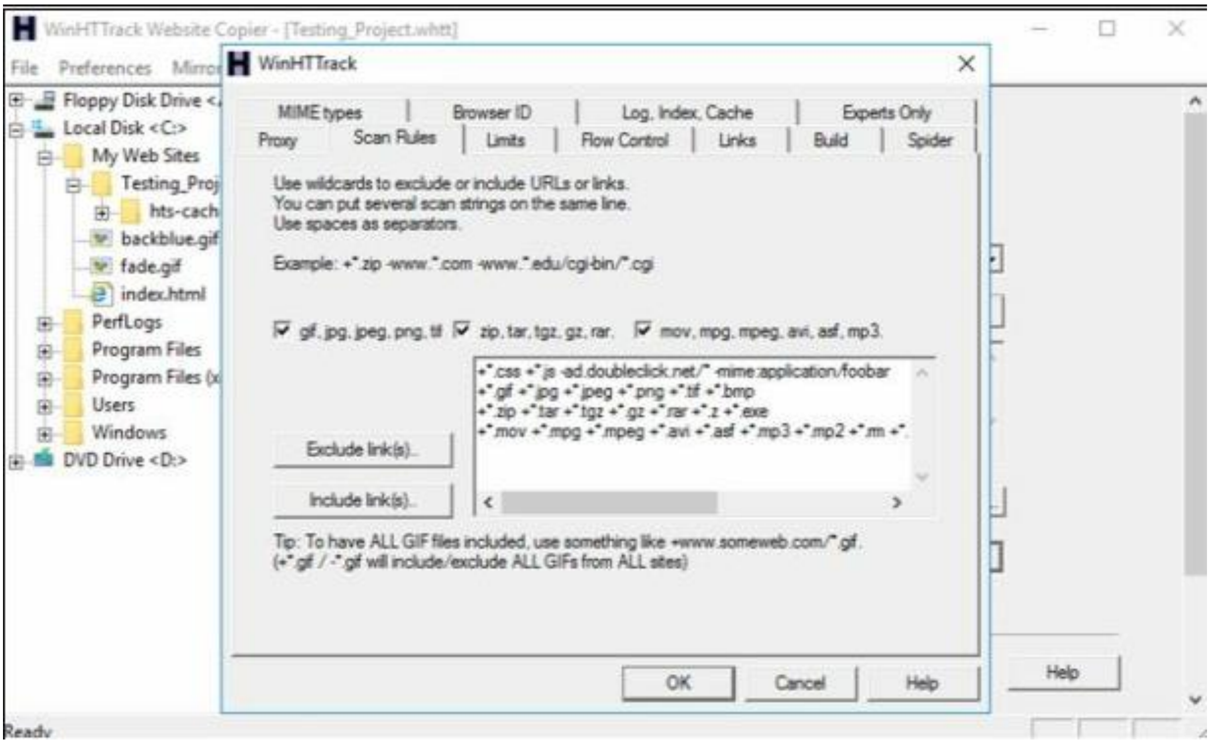
Action: Download web site(s)

Web Addresses: (URL)

URL list (.txt):

Preferences and mirror options:

5- Click on **Set Options** button.



Use wildcards to exclude or include URLs or links.
You can put several scan strings on the same line.
Use spaces as separators.

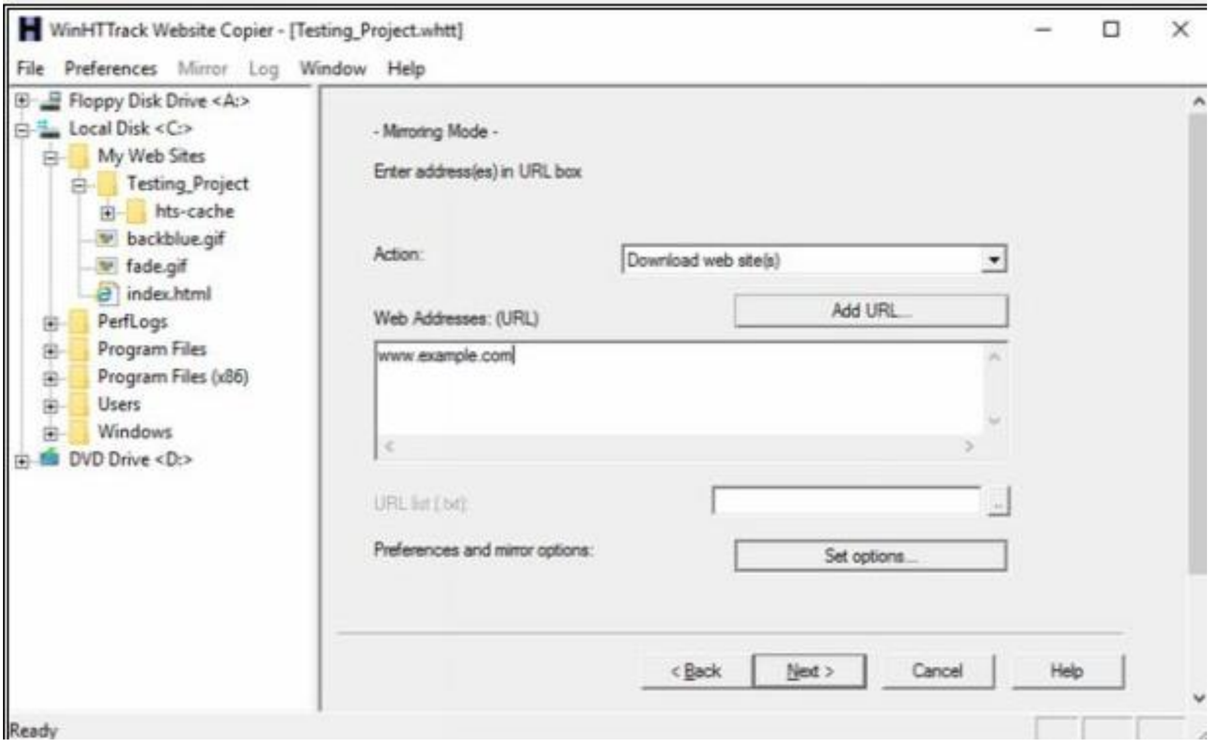
Example: +*.zip -www.*.com -www.*.edu/cgi-bin/*.cgi

☑ gif, jpg, jpeg, png, tif ☑ zip, tar, tgz, gz, rar, ☑ mov, mpg, mpeg, avi, asf, mp3,

```
+*.css +*.js -ad.doubleclick.net/* -mime:application/foobar
+*.gif +*.jpg +*.jpeg +*.png +*.tif +*.bmp
+*.zip +*.tar +*.tgz +*.gz +*.rar +*.z +*.exe
+*.mov +*.mpg +*.mpeg +*.avi +*.asf +*.mp3 +*.mp2 +*.rm +*.
```

Tip: To have ALL GIF files included, use something like +www.someweb.com/*.gif.
(+*.gif / -*.gif will include/exclude ALL GIFs from ALL sites)

6- Go to **Scan Rules** Tab and Select options as required.



- Mirroring Mode -

Enter address(es) in URL box

Action: Download web site(s)

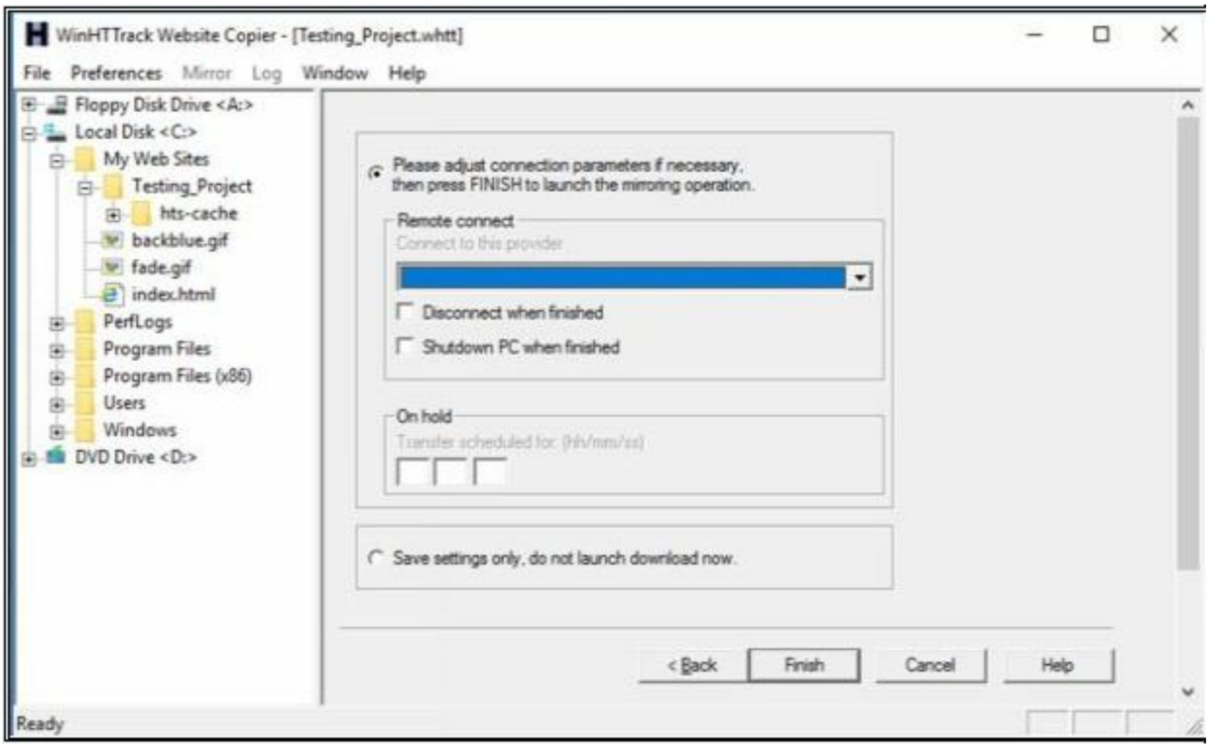
Web Addresses: (URL)

www.example.com

URL list (.txt):

Preferences and mirror options:

7- Enter the Web Address in the field and Click Next.



● Please adjust connection parameters if necessary,
then press FINISH to launch the mirroring operation.

Remote connect

Connect to this provider

□ Disconnect when finished

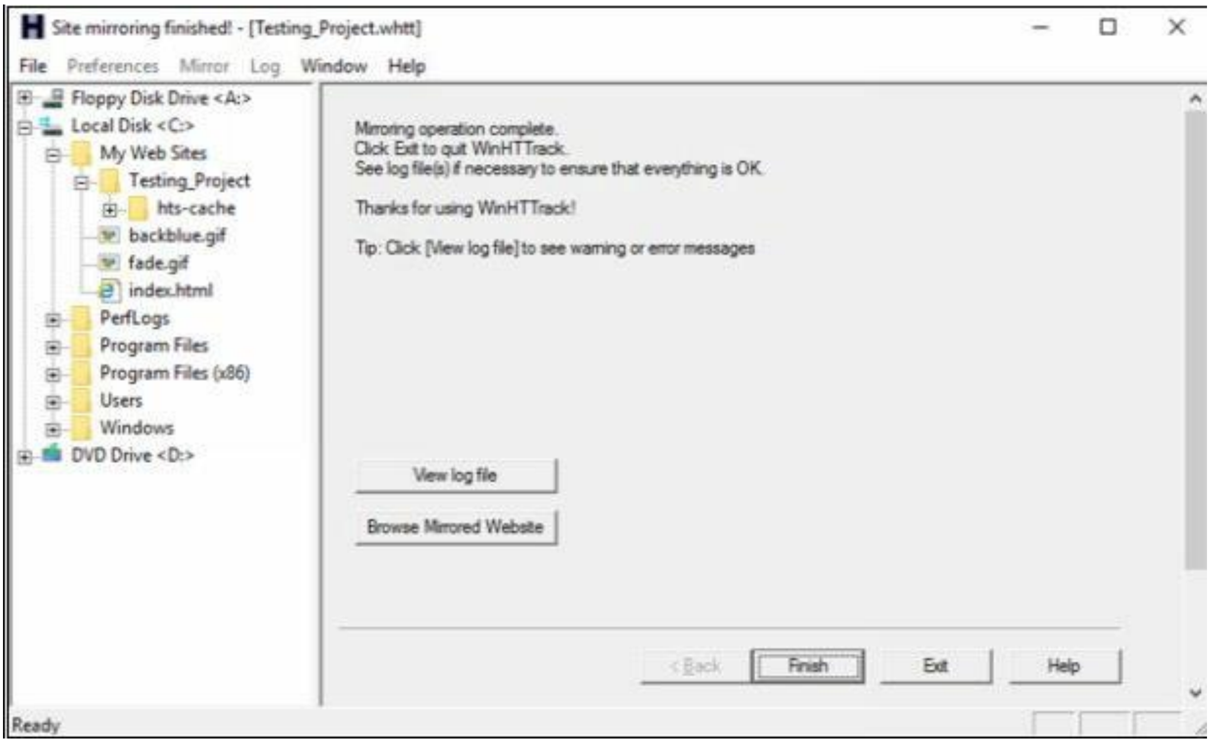
□ Shutdown PC when finished

On hold

Transfer scheduled for: (hh/mm/ss)

○ Save settings only, do not launch download now.

8- Click Next.

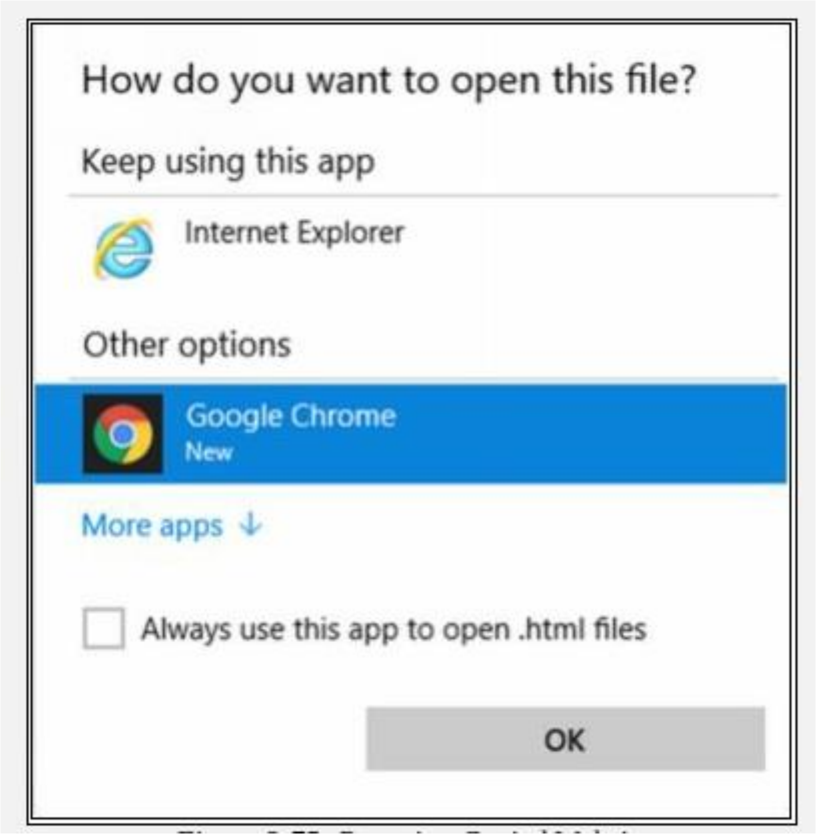


Mirroring operation complete.
Click Exit to quit WinHTTrack.
See log file(s) if necessary to ensure that everything is OK.

Thanks for using WinHTTrack!

Tip: Click [View log file] to see warning or error messages

9- Click **Browse Mirrored Website**.



How do you want to open this file?

Keep using this app

Internet Explorer

Other options

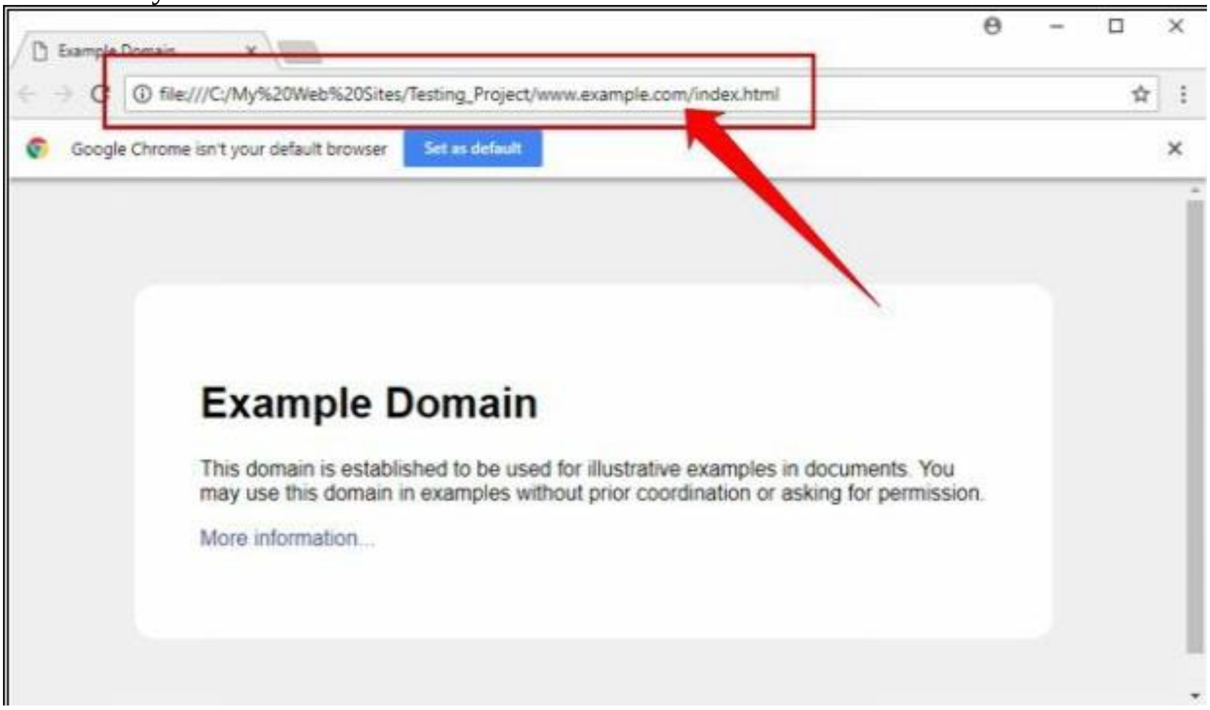
Google Chrome
New

More apps ↓

□ Always use this app to open .html files

OK

10- Select your favorite web browser.



Example Domain

file:///C:/My%20Web%20Sites/Testing_Project/www.example.com/index.html

Google Chrome isn't your default browser

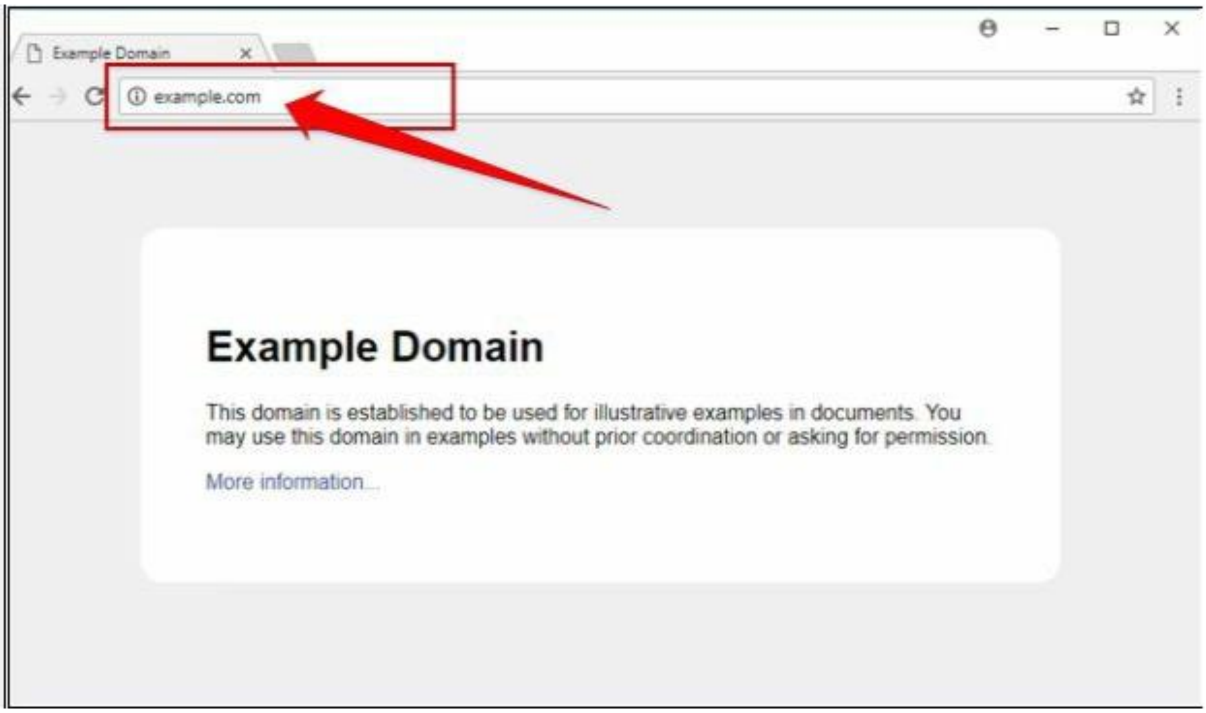
Set as default

Example Domain

This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.

More information...

Observed the above output. Example.com website is copied into a local directory and browsed from there. Now you can explore the website in an offline environment for the structure of the website and other parameters.



Example Domain

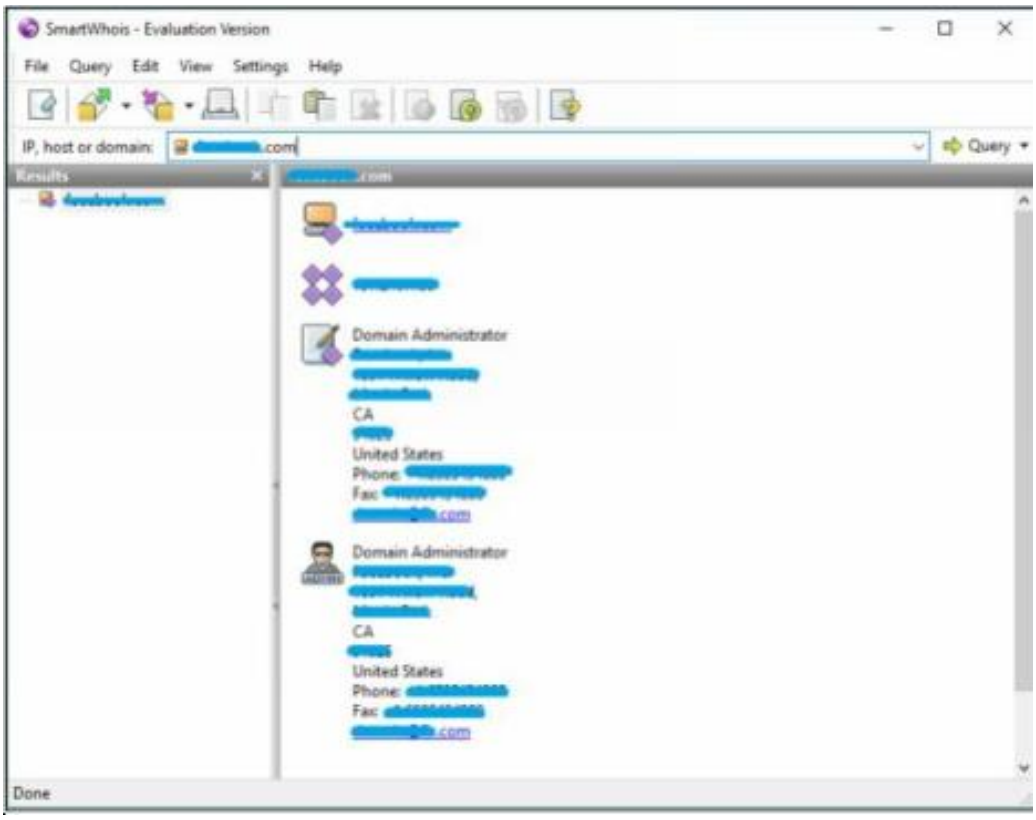
This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.

More information...

To make sure, compare the website to the original example.com website. Open a new tab and go to URL example.com.

Practical No 4: Smart Whois

You can download software "***SmartWhois***" from ***www.tamos.com*** for Whois lookup as shown in the figure below: -



IP, host or domain: [redacted].com

[redacted].com

[redacted]

[redacted]

Domain Administrator
[redacted]
CA
[redacted]
United States
Phone: [redacted]
Fax: [redacted]
[redacted].com

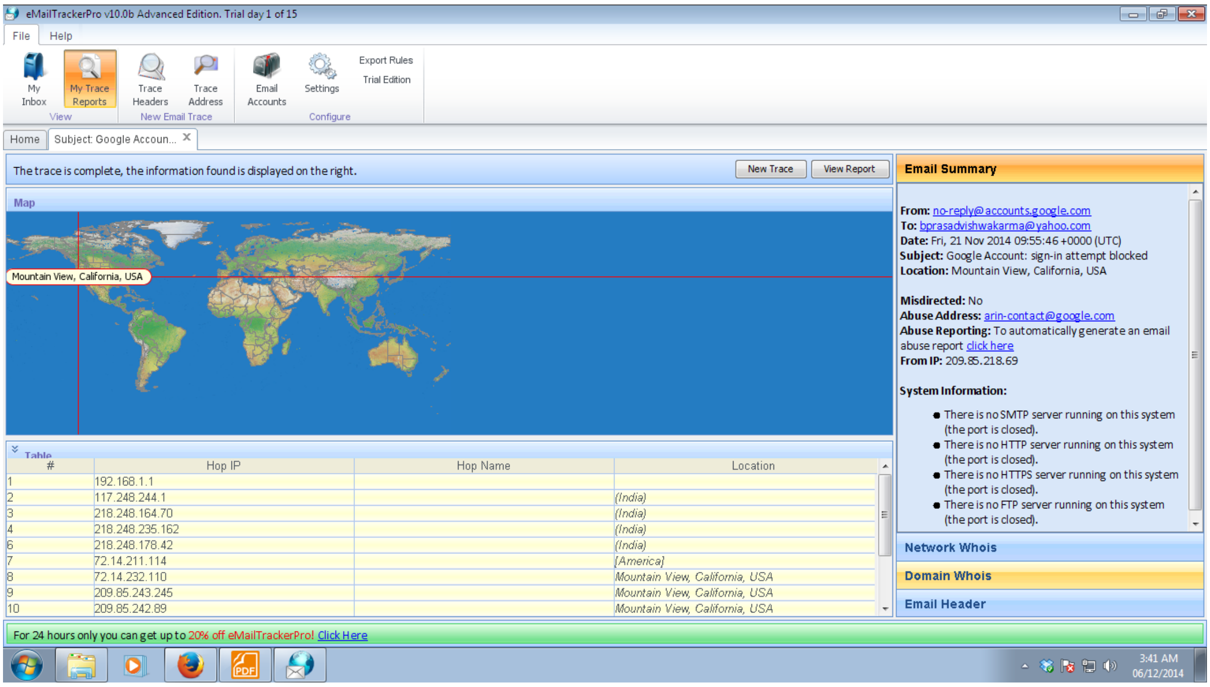
Domain Administrator
[redacted]
CA
[redacted]
United States
Phone: [redacted]
Fax: [redacted]
[redacted].com

Done

Practical No 5: Emailtracker Pro

eMailTrackerPro is **a Windows based email tracker that can be used to monitor employees, senders and recipients**. This powerful tool can be used in conjunction with other programs such as Windows Nuke (also known as Spamwasher) to quickly identify where a computer has been and how it has been used.

Click on Trace Headers/Trace email address and enter the Message Header and click Okay. The Status of the Trace will be shown inside Trace Reports



The trace is complete, the information found is displayed on the right.

#	Hop IP	Hop Name	Location
1	192.168.1.1		
2	117.248.244.1		*(India)*
3	218.248.164.70		*(India)*
4	218.248.235.162		*(India)*
6	218.248.178.42		*(India)*
7	72.14.211.114		*[America]*
8	72.14.232.110		*Mountain View, California, USA*
9	209.85.243.245		*Mountain View, California, USA*
10	209.85.242.89		*Mountain View, California, USA*

Email Summary

From: no-reply@accounts.google.com
To: bprasadvishwakarma@yahoo.com
Date: Fri, 21 Nov 2014 09:55:46 +0000 (UTC)
Subject: Google Account: sign-in attempt blocked
Location: Mountain View, California, USA

Misdirected: No
Abuse Address: arin-contact@google.com
Abuse Reporting: To automatically generate an email abuse report click here
From IP: 209.85.218.69

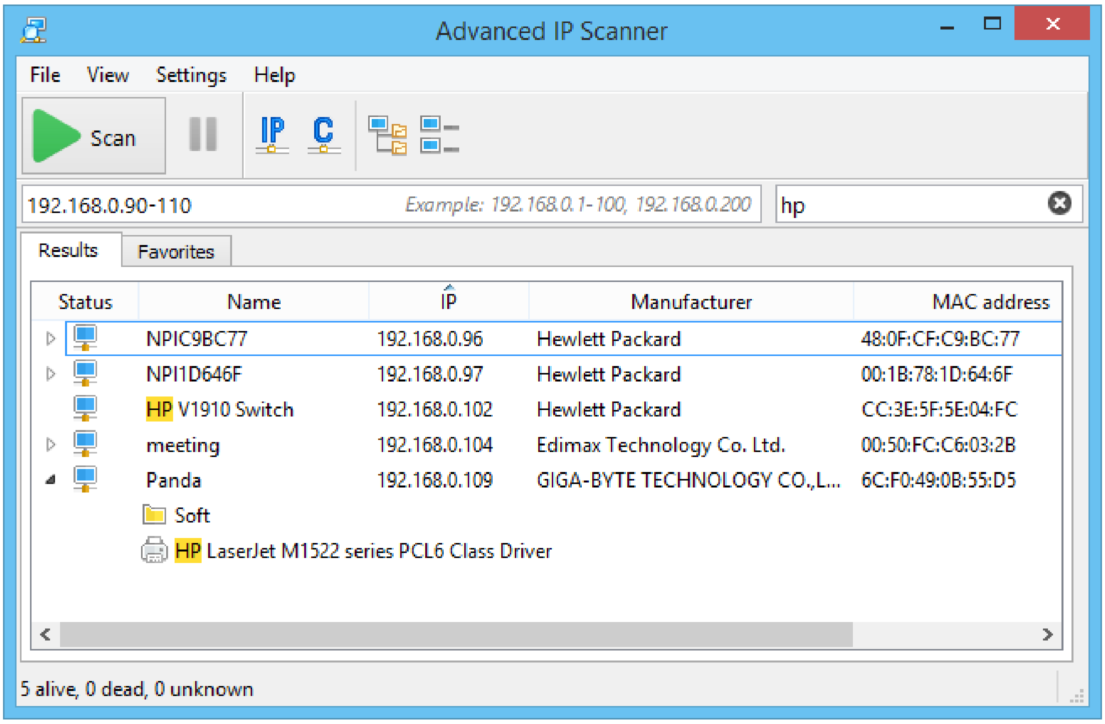
System Information:

- There is no SMTP server running on this system (the port is closed).
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

For 24 hours only you can get up to 20% off eMailTrackerPro! Click Here

Practical No 6: Scan The Network Using The Advanced IP Scanner.

Advanced IP Scanner is **a fast and powerful network scanner with a user-friendly interface**. In seconds, Advanced IP Scanner can locate all computers on your wired or wireless local network and scan their ports. The program provides easy access to various network resources such as HTTP, HTTPS, FTP, and shared folders.



192.168.0.90-110 *Example: 192.168.0.1-100, 192.168.0.200*

hp

Status	Name	IP	Manufacturer	MAC address
▷	NPIC9BC77	192.168.0.96	Hewlett Packard	48:0F:CF:C9:BC:77
▷	NPI1D646F	192.168.0.97	Hewlett Packard	00:1B:78:1D:64:6F
	HP V1910 Switch	192.168.0.102	Hewlett Packard	CC:3E:5F:5E:04:FC
▷	meeting	192.168.0.104	Edimax Technology Co. Ltd.	00:50:FC:C6:03:2B
◢	Panda	192.168.0.109	GIGA-BYTE TECHNOLOGY CO.,L...	6C:F0:49:0B:55:D5
	Soft			
	HP LaserJet M1522 series PCL6 Class Driver			

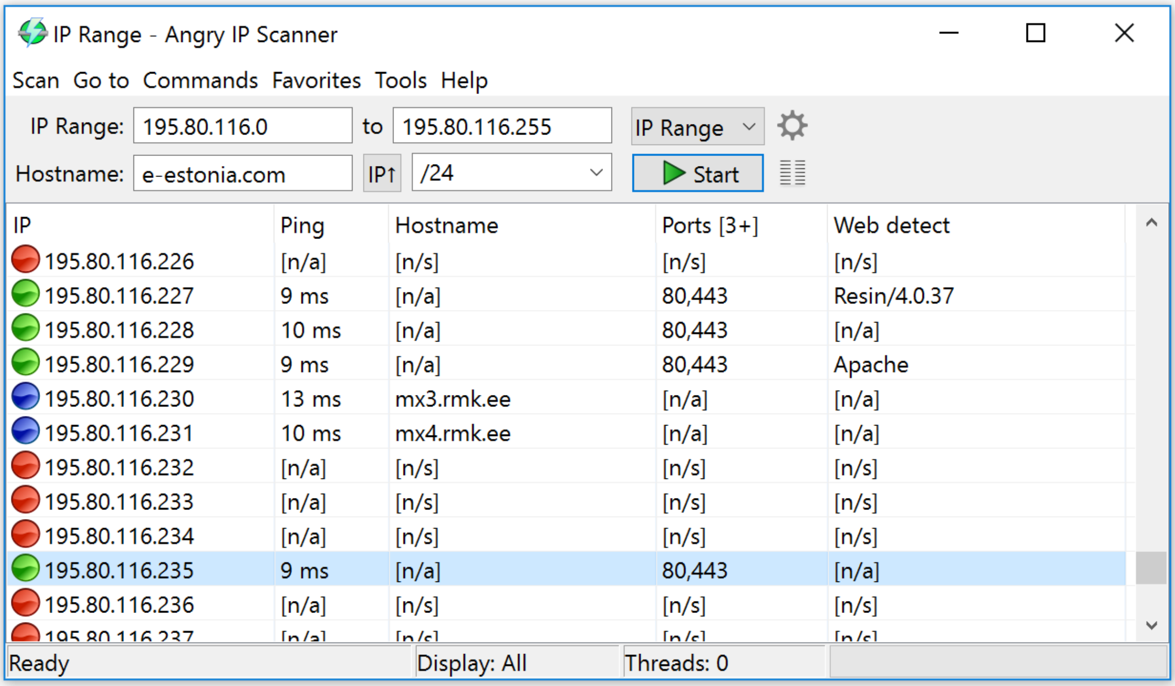
5 alive, 0 dead, 0 unknown

Practical No 7: Angry IP Scanner

Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has many other features.

It is widely used by network administrators and just curious users around the world, including large and small enterprises, banks, and government agencies.

It runs on Linux, Windows, and Mac OS X, possibly supporting other platforms as well.


IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range
IP↑
Start

IP Range: 195.80.116.0 to 195.80.116.255

Hostname: e-estonia.com /24

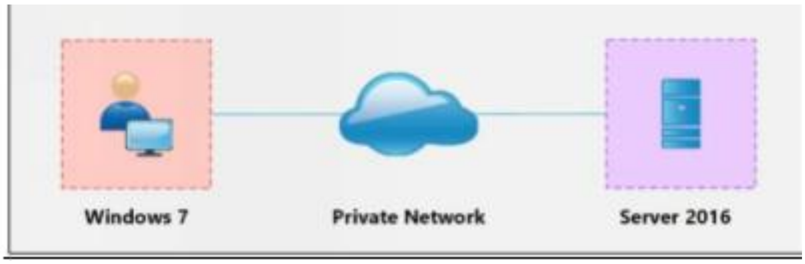
IP	Ping	Hostname	Ports [3+]	Web detect
🔴 195.80.116.226	[n/a]	[n/s]	[n/s]	[n/s]
🟢 195.80.116.227	9 ms	[n/a]	80,443	Resin/4.0.37
🟢 195.80.116.228	10 ms	[n/a]	80,443	[n/a]
🟢 195.80.116.229	9 ms	[n/a]	80,443	Apache
🔵 195.80.116.230	13 ms	mx3.rmk.ee	[n/a]	[n/a]
🔵 195.80.116.231	10 ms	mx4.rmk.ee	[n/a]	[n/a]
🔴 195.80.116.232	[n/a]	[n/s]	[n/s]	[n/s]
🔴 195.80.116.233	[n/a]	[n/s]	[n/s]	[n/s]
🔴 195.80.116.234	[n/a]	[n/s]	[n/s]	[n/s]
🟢 195.80.116.235	9 ms	[n/a]	80,443	[n/a]
🔴 195.80.116.236	[n/a]	[n/s]	[n/s]	[n/s]
🔴 195.80.116.237	[n/a]	[n/s]	[n/s]	[n/s]

Ready Display: All Threads: 0

Practical No 8: Currports

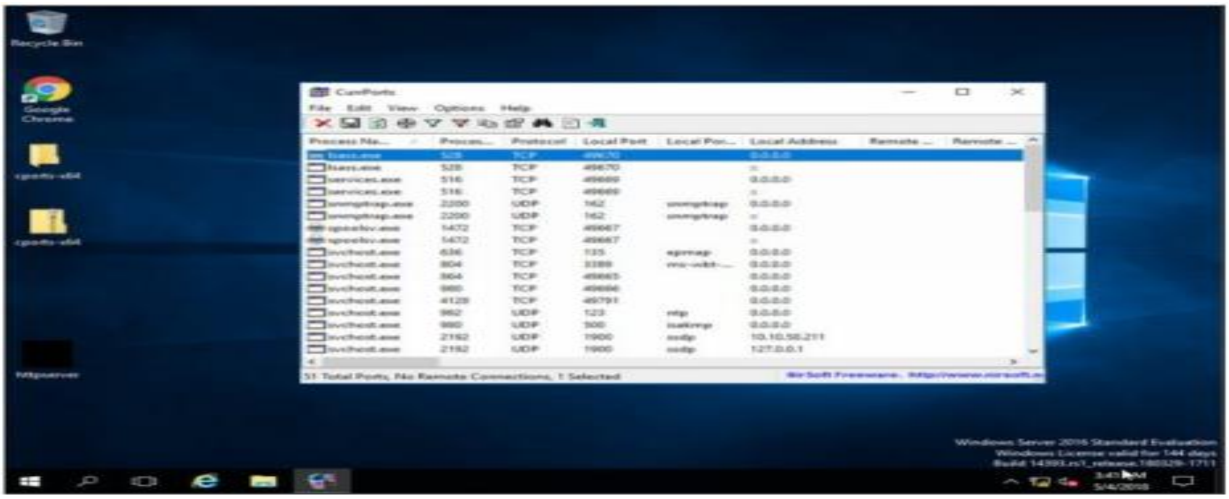
Case Study: Using the Previous lab, we are going to re-execute HTTP Remote Access Trojan (RAT) on Windows 12 machine (10.10.50.211) and observed the TCP/IP connections to detect and kill the connection.

Topology:



Configuration:

1. Run the application **Currports** on Windows Server 2016 and observe theprocesses.

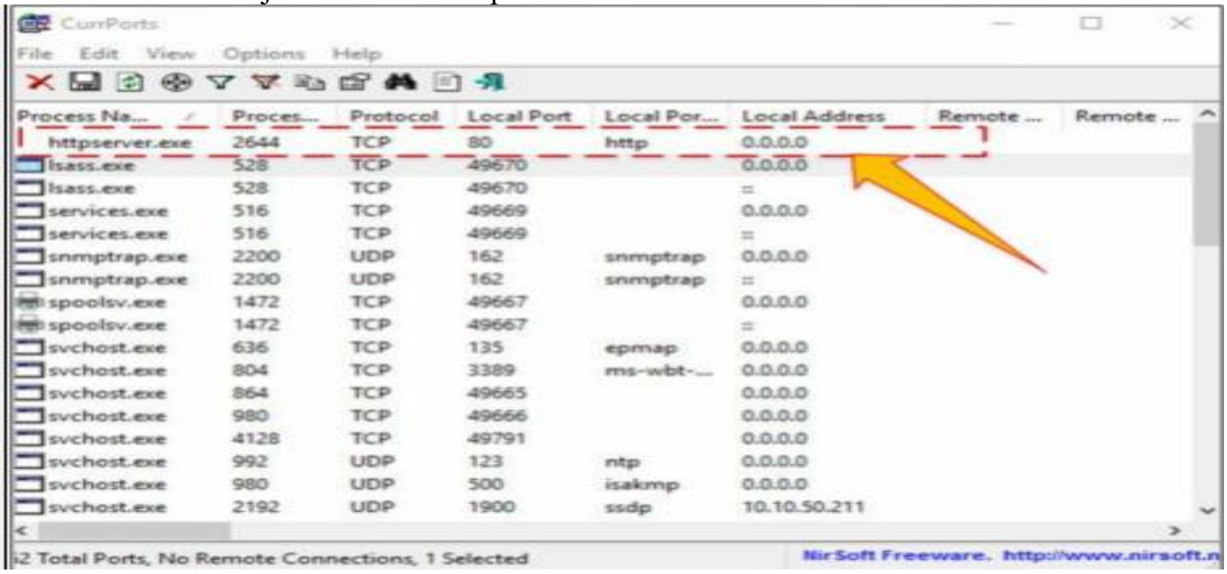


Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...
lsass.exe	528	TCP	49670		0.0.0.0		
lsass.exe	528	TCP	49670		::		
services.exe	516	TCP	49669		0.0.0.0		
services.exe	516	TCP	49669		::		
snmptrap.exe	2200	UDP	162	snmptrap	0.0.0.0		
snmptrap.exe	2200	UDP	162	snmptrap	::		
spoolsv.exe	1472	TCP	49667		0.0.0.0		
spoolsv.exe	1472	TCP	49667		::		
svchost.exe	636	TCP	135	epmap	0.0.0.0		
svchost.exe	804	TCP	3389	ms-wbt-...	0.0.0.0		
svchost.exe	864	TCP	49665		0.0.0.0		
svchost.exe	980	TCP	49666		0.0.0.0		
svchost.exe	4128	TCP	49791		0.0.0.0		
svchost.exe	992	UDP	123	ntp	0.0.0.0		
svchost.exe	980	UDP	500	isakmp	0.0.0.0		
svchost.exe	2192	UDP	1900	ssdp	10.10.50.211		
svchost.exe	2192	UDP	1900	ssdp	127.0.0.1		

51 Total Ports, No Remote Connections, 1 Selected

NirSoft Freeware. http://www.nirsoft.n

2.Run the HTTP Trojan created in the previous lab

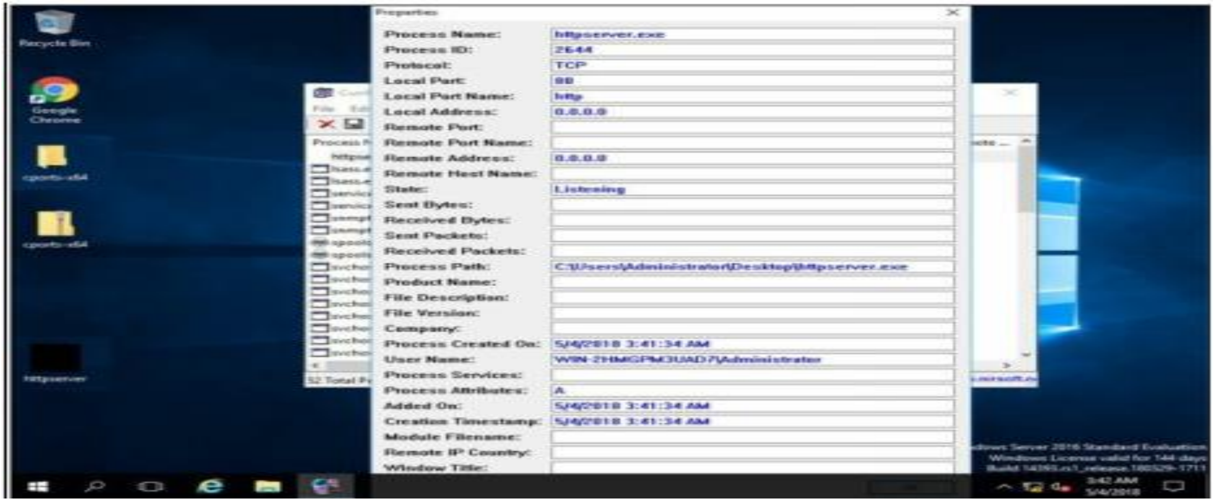


Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...
httpserver.exe	2644	TCP	80	http	0.0.0.0		
lsass.exe	528	TCP	49670		0.0.0.0		
lsass.exe	528	TCP	49670		::		
services.exe	516	TCP	49669		0.0.0.0		
services.exe	516	TCP	49669		::		
snmptrap.exe	2200	UDP	162	snmptrap	0.0.0.0		
snmptrap.exe	2200	UDP	162	snmptrap	::		
spoolsv.exe	1472	TCP	49667		0.0.0.0		
spoolsv.exe	1472	TCP	49667		::		
svchost.exe	636	TCP	135	epmap	0.0.0.0		
svchost.exe	804	TCP	3389	ms-wbt-...	0.0.0.0		
svchost.exe	864	TCP	49665		0.0.0.0		
svchost.exe	980	TCP	49666		0.0.0.0		
svchost.exe	4128	TCP	49791		0.0.0.0		
svchost.exe	992	UDP	123	ntp	0.0.0.0		
svchost.exe	980	UDP	500	isakmp	0.0.0.0		
svchost.exe	2192	UDP	1900	ssdp	10.10.50.211		

i2 Total Ports, No Remote Connections, 1 Selected

NirSoft Freeware. http://www.nirsoft.n

The new process is added to the list.
You can observe the process name, Protocol, Local and remote port and IP address information.
3. For more detail, right click on httpserver.exe and go to properties

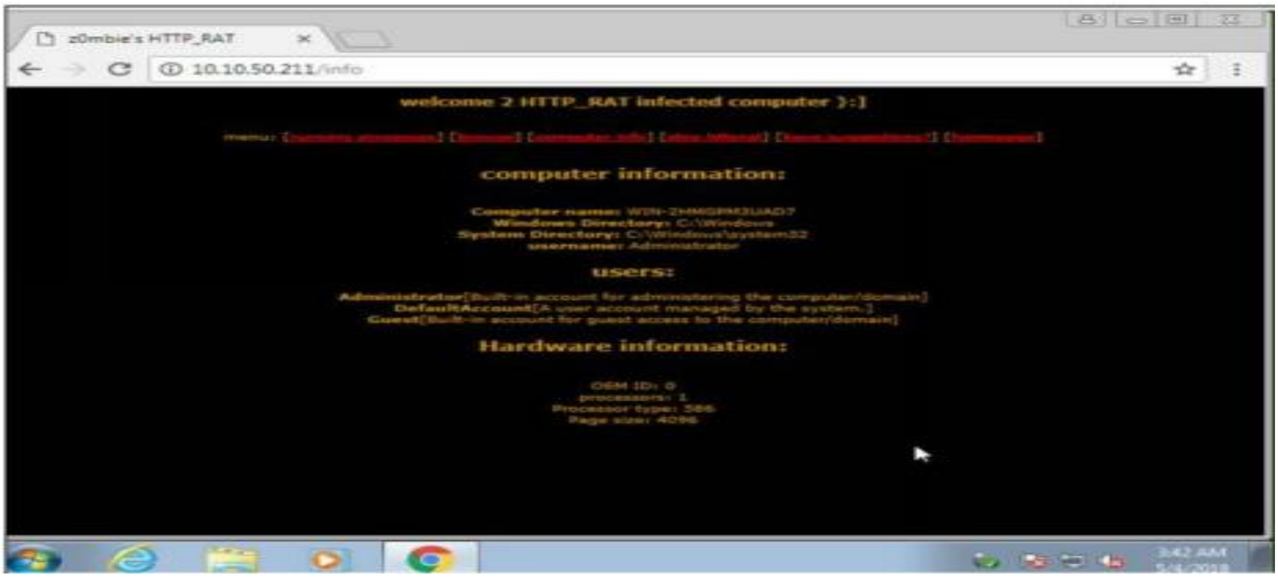


Properties

Process Name: httpserver.exe
Process ID: 2644
Protocol: TCP
Local Port: 80
Local Port Name: http
Local Address: 0.0.0.0
Remote Port:
Remote Port Name:
Remote Address: 0.0.0.0
Remote Host Name:
State: Listening
Sent Bytes:
Received Bytes:
Sent Packets:
Received Packets:
Process Path: C:\Users\Administrator\Desktop\httpserver.exe
Product Name:
File Description:
File Version:
Company:
Process Created On: 5/4/2018 3:41:34 AM
User Name: WIN-2HMGPM3UAD7\Administrator
Process Services:
Process Attributes: A
Added On: 5/4/2018 3:41:34 AM
Creation Timestamp: 5/4/2018 3:41:34 AM
Module Filename:
Remote IP Country:
Window Title:

Recycle Bin
Google Chrome
cports-x64
cports-x64
httpserver
Windows Server 2016 Standard Evaluation
Windows License valid for 144 days
Build 14393.rs1_release.180329-1711
3:42 AM
5/4/2018

Properties are showing more details about tcp connection.
4. Go to Windows 7 machine and initiate the connection as mentioned in the previous lab using a web browser.



welcome 2 HTTP_RAT infected computer }:]

menu: [illegible]

computer information:

Computer name: WIN-2HMGPM3UAD7
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
username: Administrator

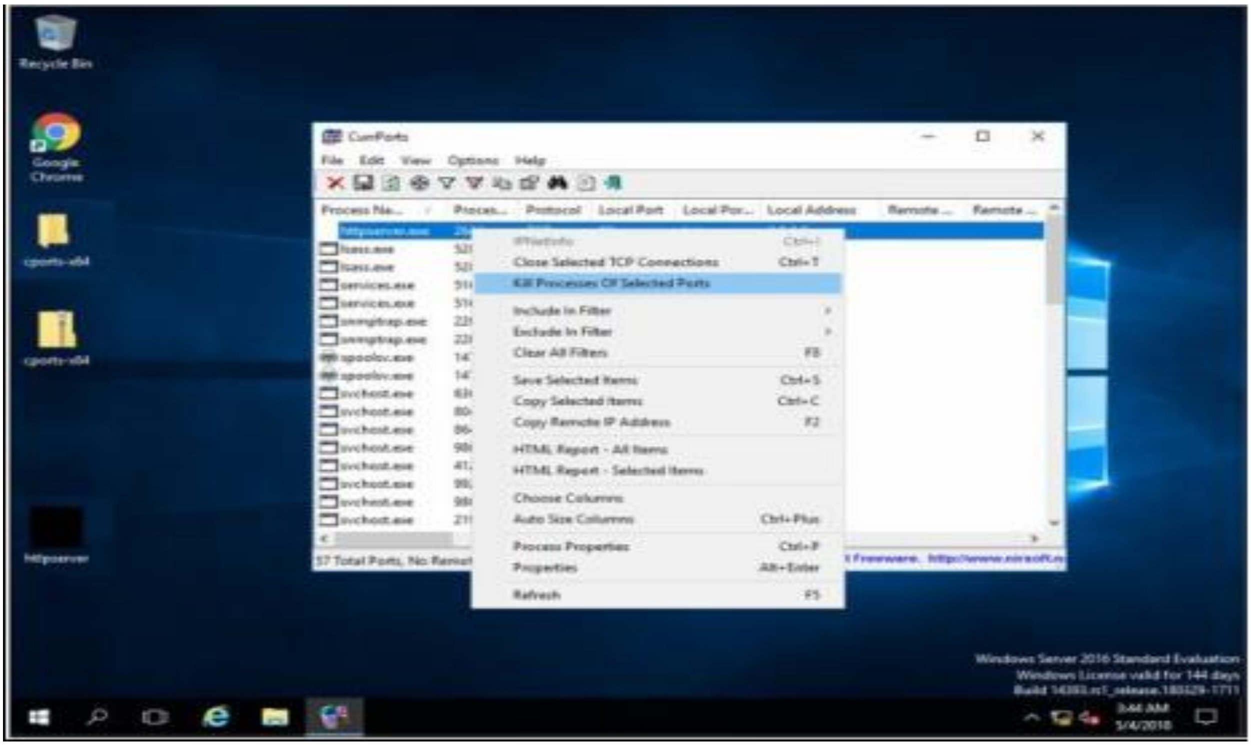
users:

Administrator[Built-in account for administering the computer/domain]
DefaultAccount[A user account managed by the system.]
Guest[Built-in account for guest access to the computer/domain]

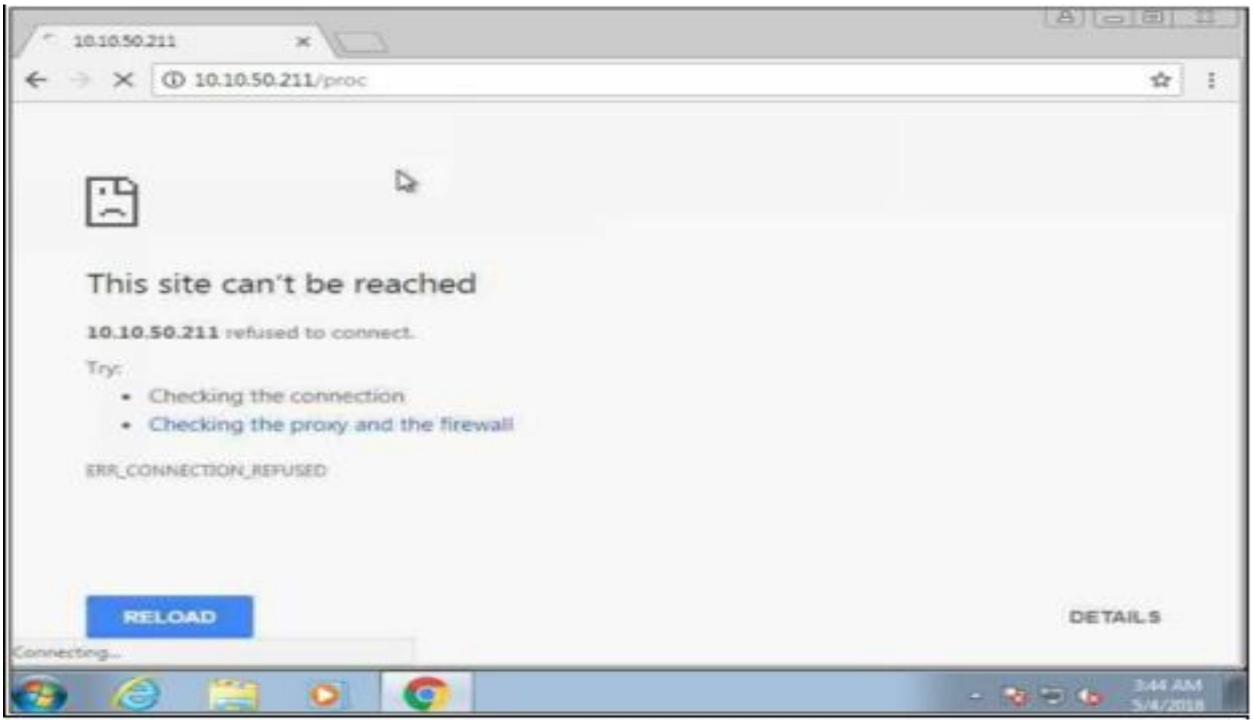
Hardware information:

OEM ID: 0
processors: 1
Processor type: 586
Page size: 4096

Connection successfully established.
5. Back to Windows Server 2016, Kill the connection


CurrPorts
File Edit View Options Help
Process Na... Proces... Protocol Local Port Local Por... Local Address Remote ... Remote ...
httpserver.exe
lsass.exe
services.exe
snmptrap.exe
spoolsv.exe
svchost.exe
IPNetInfo Ctrl+I
Close Selected TCP Connections Ctrl+T
Kill Processes Of Selected Ports
Include In Filter
Exclude In Filter
Clear All Filters F8
Save Selected Items Ctrl+S
Copy Selected Items Ctrl+C
Copy Remote IP Address F2
HTML Report - All Items
HTML Report - Selected Items
Choose Columns
Auto Size Columns Ctrl+Plus
Process Properties Ctrl+P
Properties Alt+Enter
Refresh F5
57 Total Ports, No Remot
Recycle Bin
Google Chrome
cports-x64
httpserver
Windows Server 2016 Standard Evaluation
3:44 AM
5/4/2018

6. To verify, retry to establish the connection from windows 7.



10.10.50.211/proc

This site can't be reached

10.10.50.211 refused to connect.

Try:

- Checking the connection
- Checking the proxy and the firewall

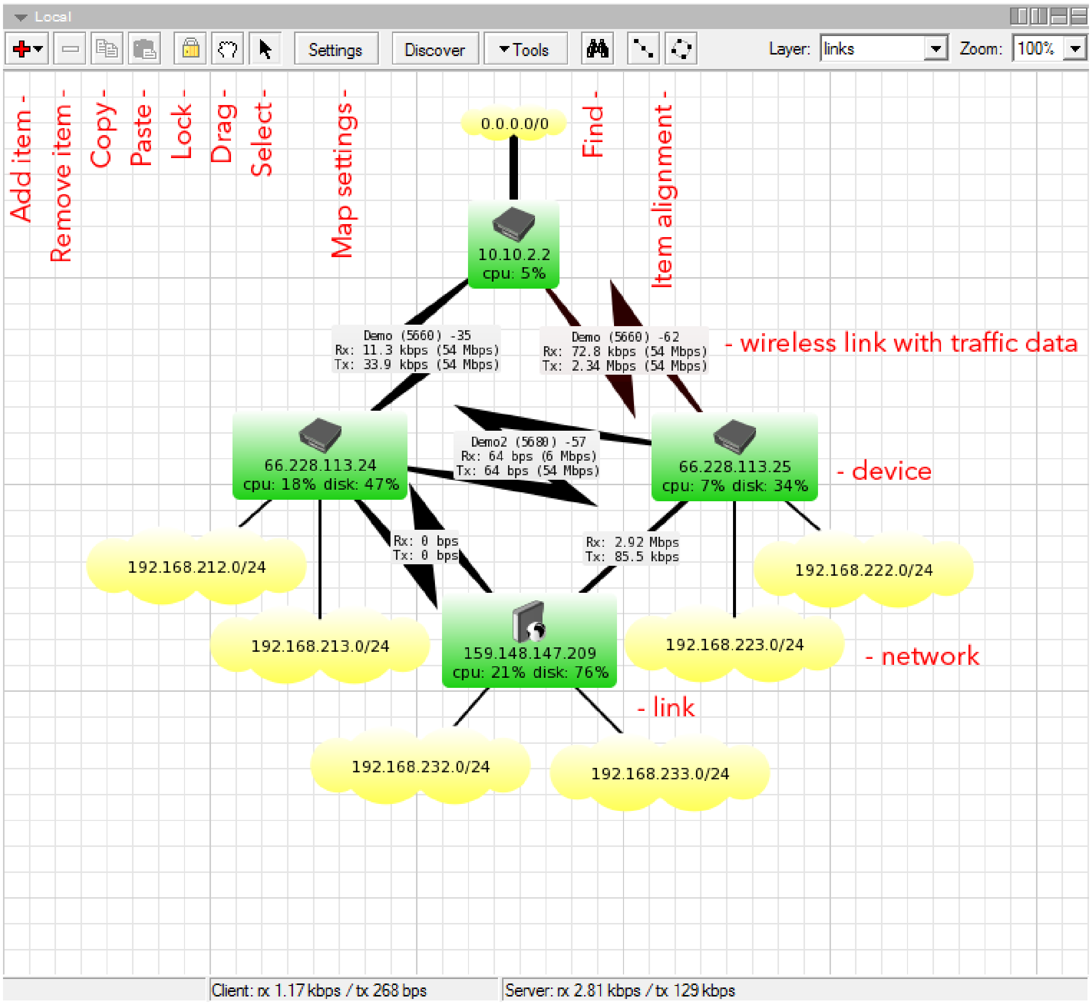
ERR_CONNECTION_REFUSED

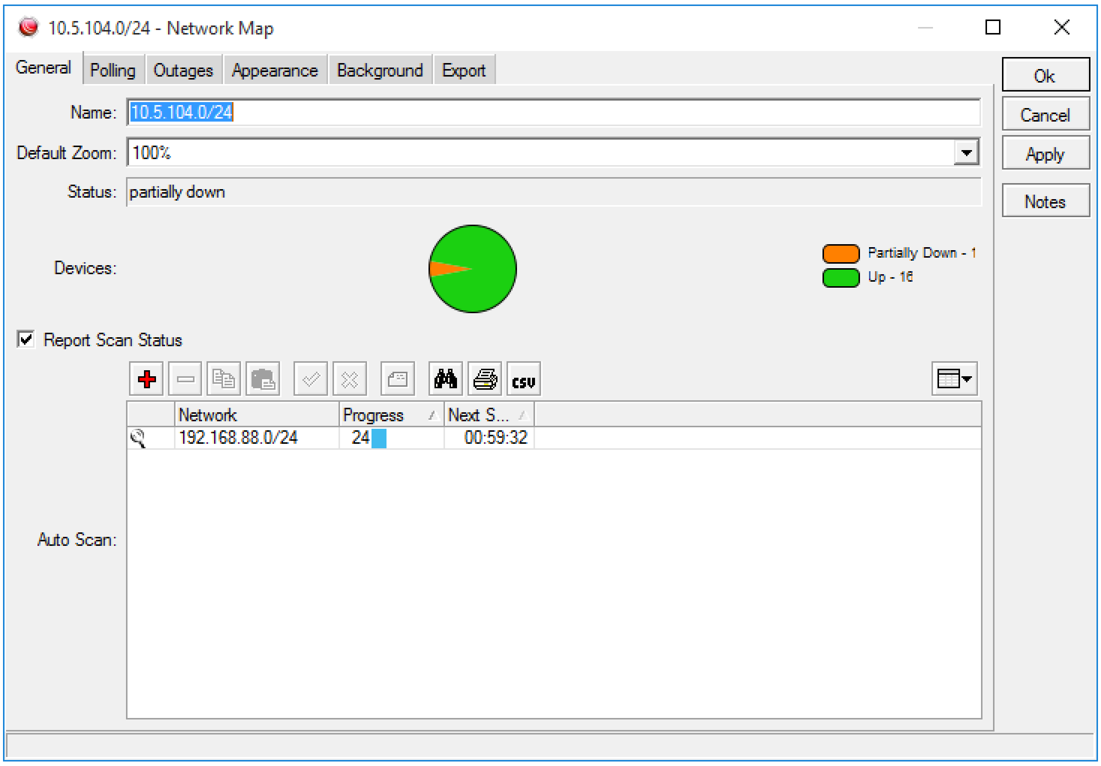
Practical No 9: The Dude

The Dude network monitor is a new application by MikroTik which can dramatically improve the way you manage your network environment. It will automatically scan all devices within specified subnets, draw and layout a map of your networks, monitor services of your devices and alert you in case some service has problems.

Main Features:

- Auto network discovery and layout
- Discovers any type or brand of device
- Device, Link monitoring, and notifications
- Includes SVG icons for devices, and supports custom icons and backgrounds
- Easy installation and usage
- Allows you to draw your own maps and add custom devices
- Supports SNMP, ICMP, DNS and TCP monitoring for devices that support it
- Individual Link usage monitoring and graphs
- Direct access to remote control tools for device management
- Supports remote Dude server and local client





Name: 10.5.104.0/24

Default Zoom: 100%

Status: partially down

Devices:

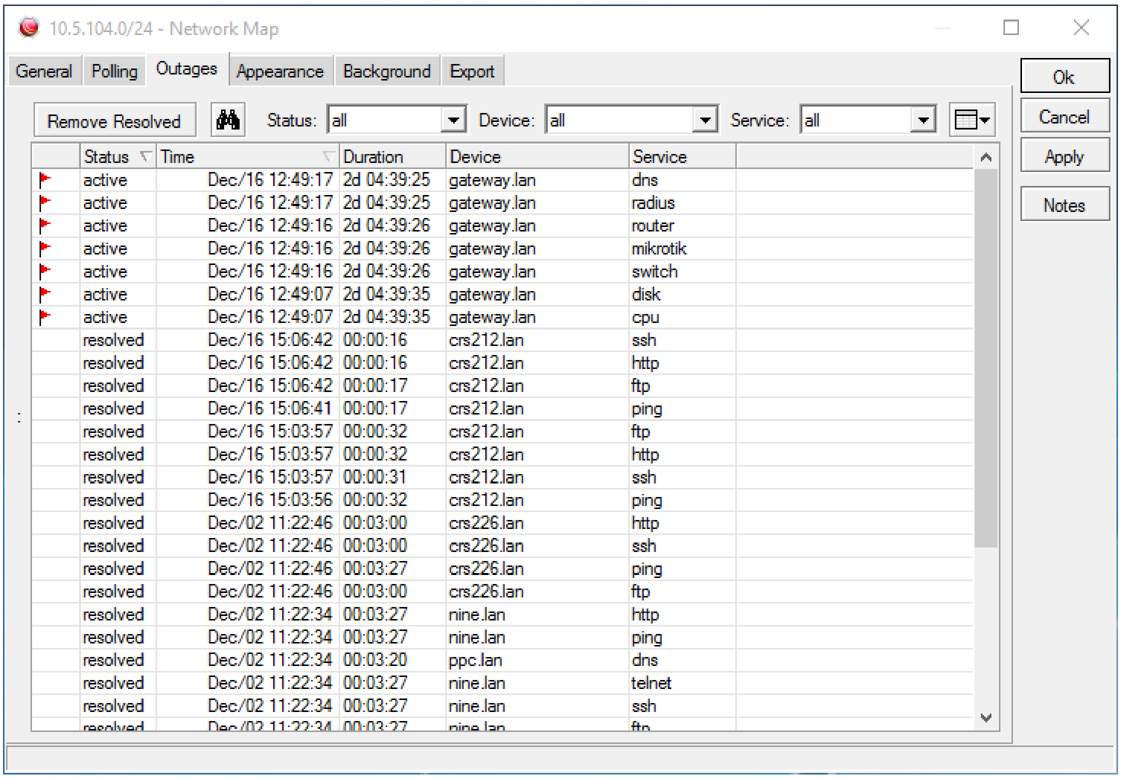
🟧 Partially Down - 1

🟩 Up - 16

☑ Report Scan Status

Auto Scan:

Network	Progress	Next S...
192.168.88.0/24	24	00:59:32

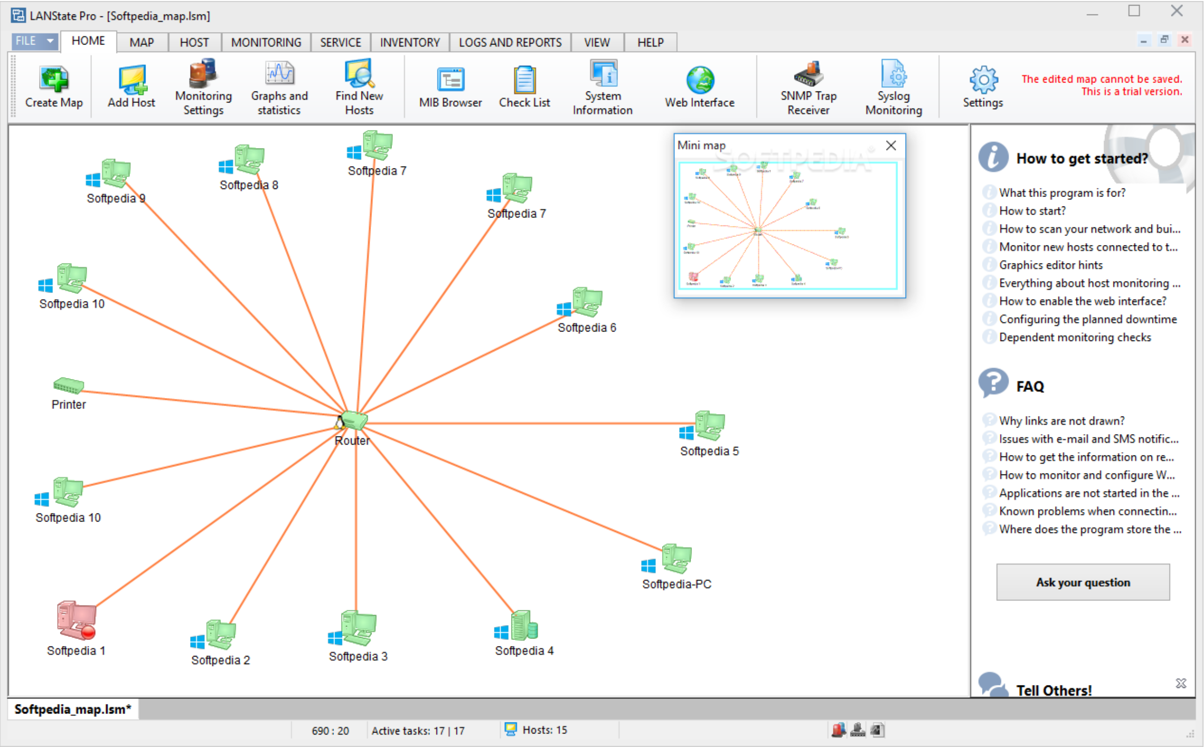


Status: all Device: all Service: all

Status	Time	Duration	Device	Service
active	Dec/16 12:49:17	2d 04:39:25	gateway.lan	dns
active	Dec/16 12:49:17	2d 04:39:25	gateway.lan	radius
active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	router
active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	mikrotik
active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	switch
active	Dec/16 12:49:07	2d 04:39:35	gateway.lan	disk
active	Dec/16 12:49:07	2d 04:39:35	gateway.lan	cpu
resolved	Dec/16 15:06:42	00:00:16	crs212.lan	ssh
resolved	Dec/16 15:06:42	00:00:16	crs212.lan	http
resolved	Dec/16 15:06:42	00:00:17	crs212.lan	ftp
resolved	Dec/16 15:06:41	00:00:17	crs212.lan	ping
resolved	Dec/16 15:03:57	00:00:32	crs212.lan	ftp
resolved	Dec/16 15:03:57	00:00:32	crs212.lan	http
resolved	Dec/16 15:03:57	00:00:31	crs212.lan	ssh
resolved	Dec/16 15:03:56	00:00:32	crs212.lan	ping
resolved	Dec/02 11:22:46	00:03:00	crs226.lan	http
resolved	Dec/02 11:22:46	00:03:00	crs226.lan	ssh
resolved	Dec/02 11:22:46	00:03:27	crs226.lan	ping
resolved	Dec/02 11:22:46	00:03:00	crs226.lan	ftp
resolved	Dec/02 11:22:34	00:03:27	nine.lan	http
resolved	Dec/02 11:22:34	00:03:27	nine.lan	ping
resolved	Dec/02 11:22:34	00:03:20	ppc.lan	dns
resolved	Dec/02 11:22:34	00:03:27	nine.lan	telnet
resolved	Dec/02 11:22:34	00:03:27	nine.lan	ssh
resolved	Dec/02 11:22:34	00:03:27	nine.lan	ftp

Practical No 10: Perform Network Discovery Using The LANState Pro

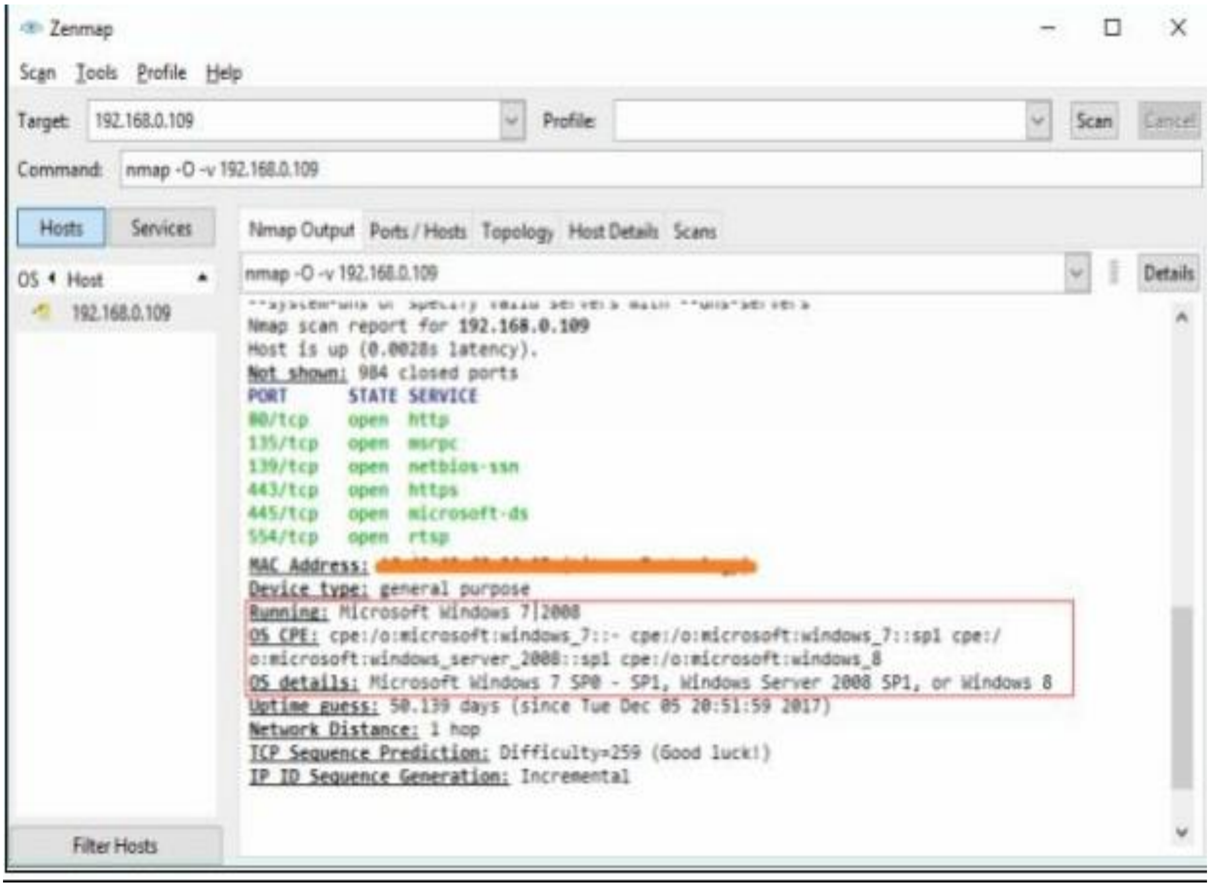
LANState is **a simple network topology mapping, host monitoring, and management program**. Monitor the service availability. Manage servers, computers, switches, and other devices easier using the graphic map. Access devices' properties, RDP, web UI faster.



The edited map cannot be saved. This is a trial version.

Practical No 11: Perform Enumeration Using The Nmap.

NMAP, as we know, is a powerful networking tool which supports many features and commands. Operating System detection capability allows to send TCP and UDP packet and observe the response from the targeted host. A detailed assessment of this response bring some clues regarding nature of an operating system disclosing the type an OS. To perform OS detection with nmap perform the following: nmap -O<ip address>



Target: 192.168.0.109

Profile:

Command: nmap -O -v 192.168.0.109

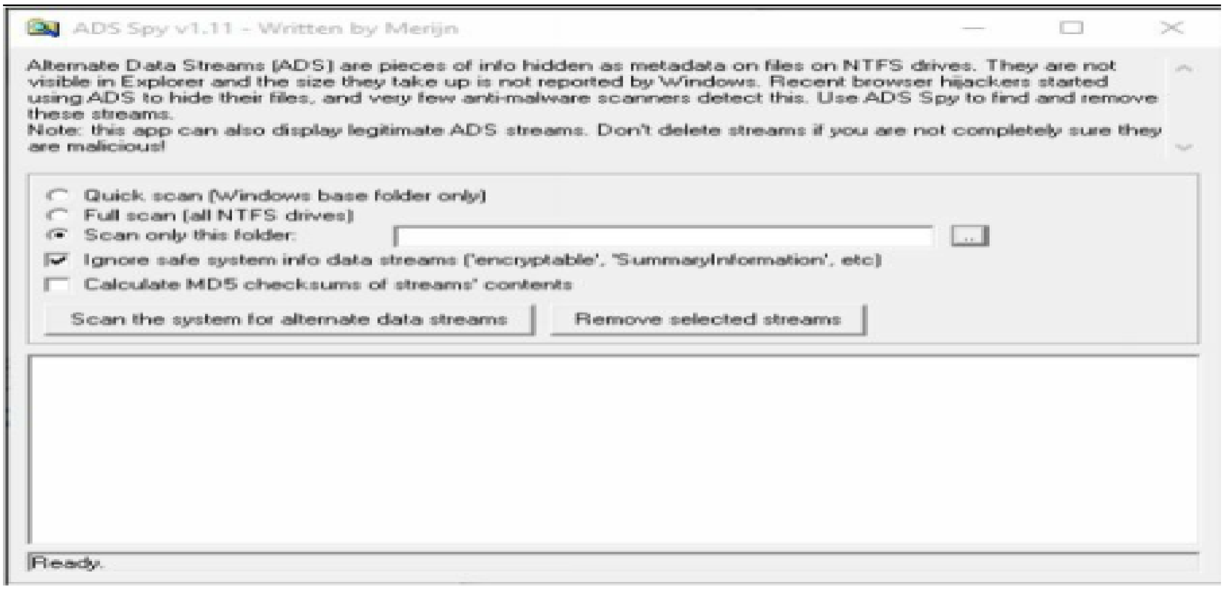
192.168.0.109

```
nmap -O -v 192.168.0.109
--system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.109
Host is up (0.0028s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
MAC Address: [redacted]
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/
o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Uptime guess: 50.139 days (since Tue Dec 05 20:51:59 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
```

Practical No 12: Perform The System Hacking Using The ADS Spy.

AdSpy offers the most search options of any Ad Intelligence Tool, so you can find the data you want, how you want. Search in the usual way: ad text, URL, page name. Search true data from user reactions in advert comments. Be as rigorous as you need to: search or filter by affiliate network, affiliate ID, Offer ID, landing page technologies - whatever helps you find the information you can work with. Open ADS Spy application and select the option if you want to:

- Quick Scan
- Full Scan
- Scan Specific Folder



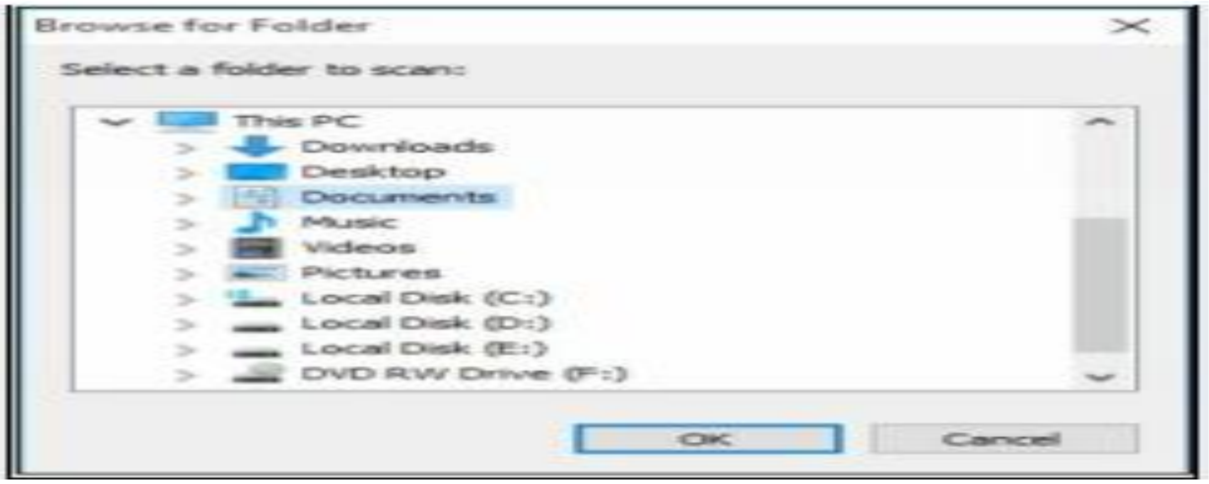
ADS Spy v1.11 - Written by Merijn

Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

○ Quick scan (Windows base folder only)
○ Full scan (all NTFS drives)
● Scan only this folder:
☑ Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
☐ Calculate MD5 checksums of streams' contents

Ready.

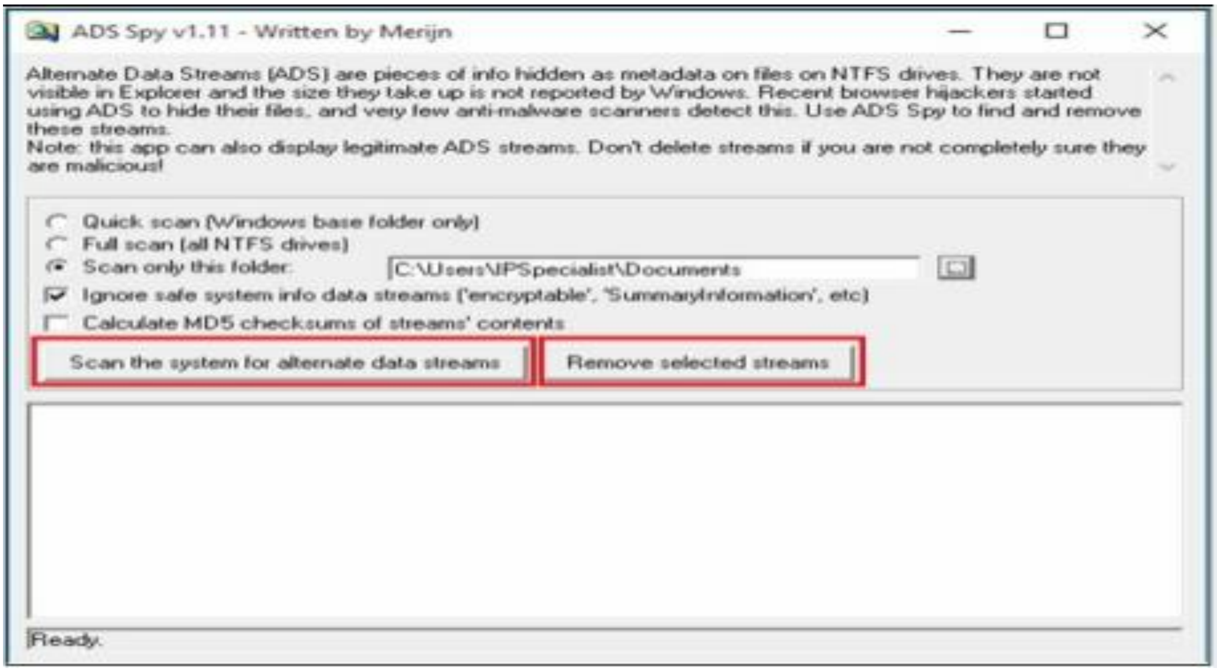
As we store the file in the Document folder, Selecting Document folder to scan particular folder only.



Browse for Folder

Select a folder to scan:

Select an Option, if you want to scan for ADS, click "**Scan the system for ADS**"/ or click **removes** button to remove the file



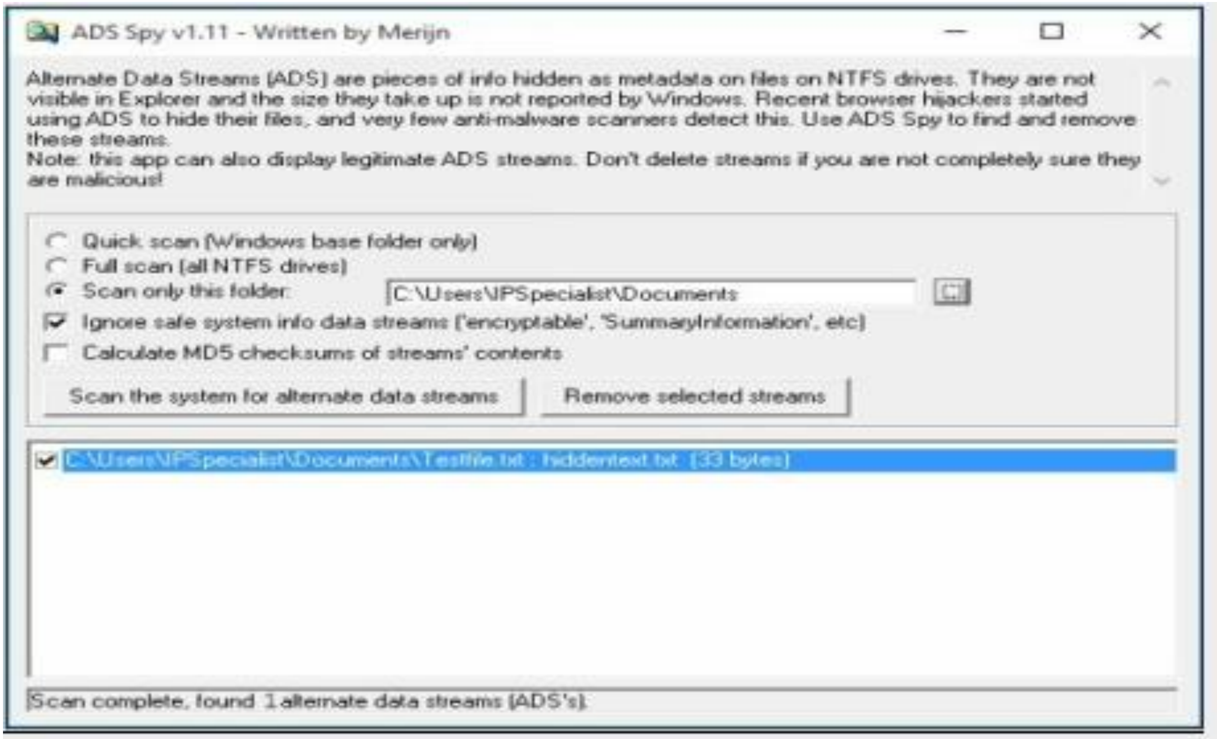
ADS Spy v1.11 - Written by Merijn

Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

○ Quick scan (Windows base folder only)
○ Full scan (all NTFS drives)
● Scan only this folder: C:\Users\IPSpecialist\Documents
☑ Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
□ Calculate MD5 checksums of streams' contents

Ready.

As shown in the figure below, ADS Spy has detected the **Testfile.txt:hidden.txt** file from the directory.



ADS Spy v1.11 - Written by Merijn

Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

○ Quick scan (Windows base folder only)
○ Full scan (all NTFS drives)
● Scan only this folder: C:\Users\IPSpecialist\Documents
☑ Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
□ Calculate MD5 checksums of streams' contents

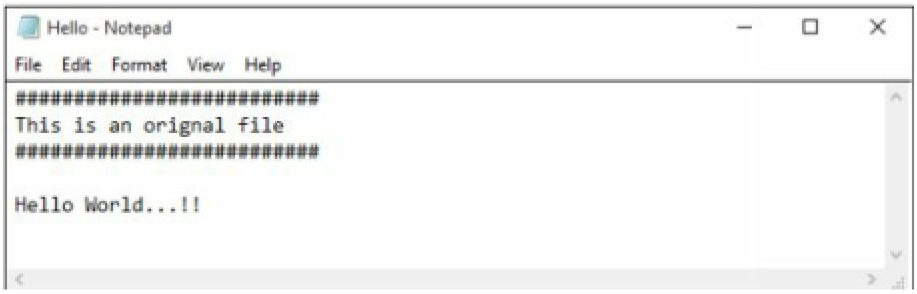
☑ C:\Users\IPSpecialist\Documents\Testfile.txt : hiddentext.txt (33 bytes)

Scan complete, found 1 alternate data streams (ADS's)

Figure 6-50 ADS Detection

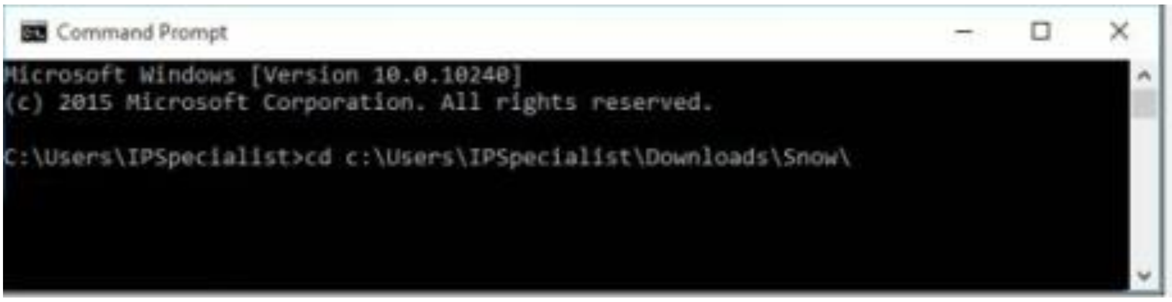
Practical No 13: Perform The System Hacking Using The Snow.

Create a text file with some data in the same directory where Snow Tool is installed.



```
###########################
This is an orignal file
###########################

Hello World...!!
```

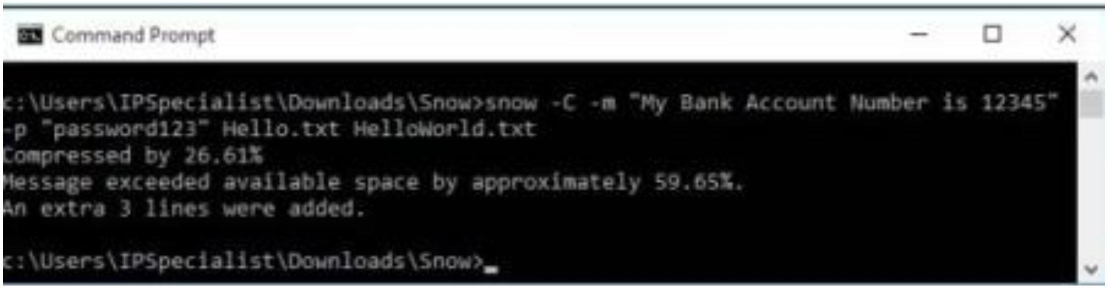
Go to Command Prompt
Change the directory to run Snow tool



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\IPSpecialist>cd c:\Users\IPSpecialist\Downloads\Snow\
```

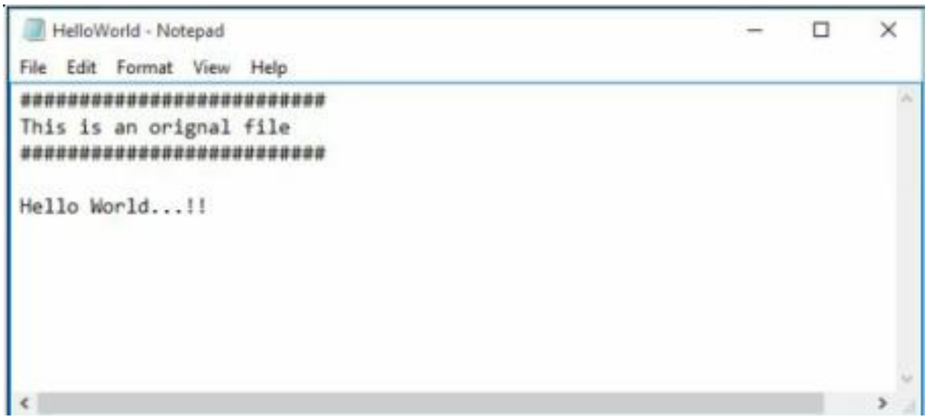
Type the command
Snow –C –m “text to be hide” –p “password” <Sourcefile> <Destinationfile>

The source file is a Hello.txt file as shown above. Destination file will be the exact copy of source file containing hidden information.



```
c:\Users\IPSpecialist\Downloads\Snow>snow -C -m "My Bank Account Number is 12345"
-p "password123" Hello.txt HelloWorld.txt
Compressed by 26.61%
Message exceeded available space by approximately 59.65%.
An extra 3 lines were added.

c:\Users\IPSpecialist\Downloads\Snow>_
```

Go to the directory; you will a new file **HelloWorld.txt**. Open the File

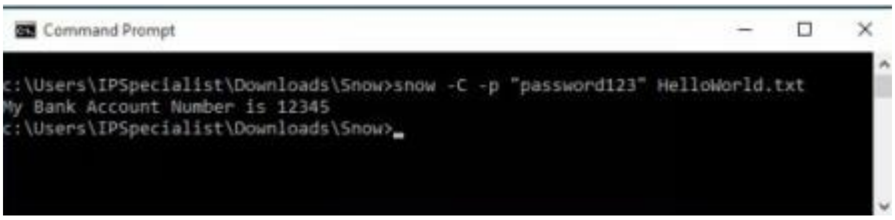


```
###########################
This is an orignal file
###########################

Hello World...!!
```

New File has the same text as an original file without any hidden information. This file can be sent to the target.

Recovering Hidden Information

On destination, Receiver can reveal information by using the command **Snow –C –p "password123" HelloWorld.txt**



```
:\Users\IPSpecialist\Downloads\Snow>snow -C -p "password123" HelloWorld.txt
y Bank Account Number is 12345
:\Users\IPSpecialist\Downloads\Snow>_
```

As shown in the above figure, File decrypted, showing hidden information encrypted in the previous section.

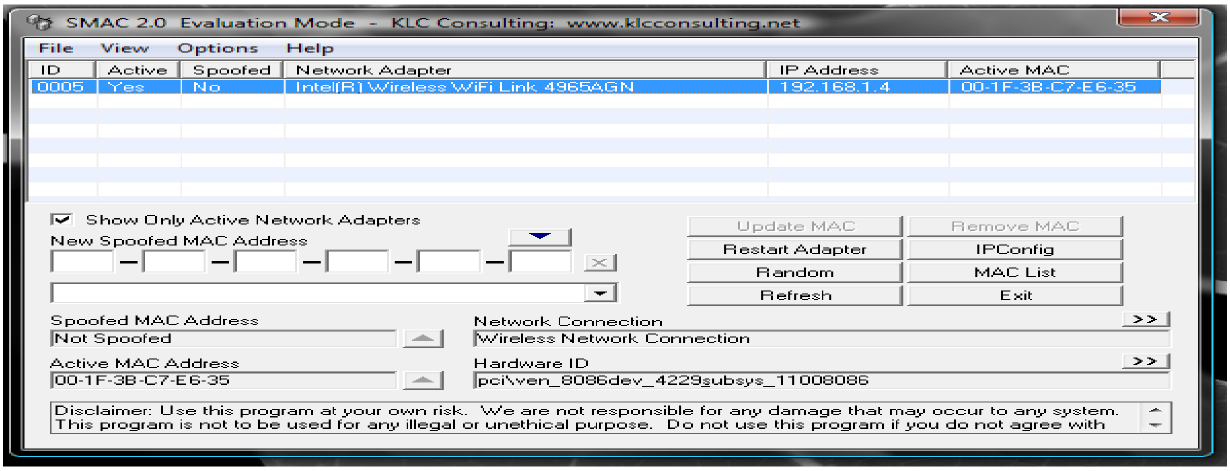
Practical No 14: Use SMAC For MAC Spoofing.

SMAC is a MAC address changer that has a simple-to-use graphical interface that enables the less experienced user all the way up to the guru to change a piece of hardware's MAC address. The less experienced user will appreciate the random generator whereas the guru will appreciate the ability to hand enter a new MAC address.

Once it is installed, you will find the application launcher in a Start Menu subdirectory called KLC. Click on that folder and you will see SMAC 2.0. Click on that launcher and the SMAC main window (**Figure A**) will open.

Using SMAC can be very simple, depending on how you want to use it. The simplest way to use SMAC is to assign a random MAC address to a piece of hardware. Before we actually assign a new address, let's take a look at the other hardware on the machine. In the main window there is a check box that tells SMAC to show only active hardware. This checkbox is checked by default. Uncheck that box and your listing will grow, depending on the hardware on your machine. Take a look at **Figure B** to see how much the listing grows on my laptop that includes wireless, wired, and dial-up connections.

Figure A



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0005	Yes	No	Intel(R) Wireless WiFi Link 4965AGN	192.168.1.4	00-1F-3B-C7-E6-35

☑ Show Only Active Network Adapters

New Spoofed MAC Address

Spoofed MAC Address: Not Spoofed

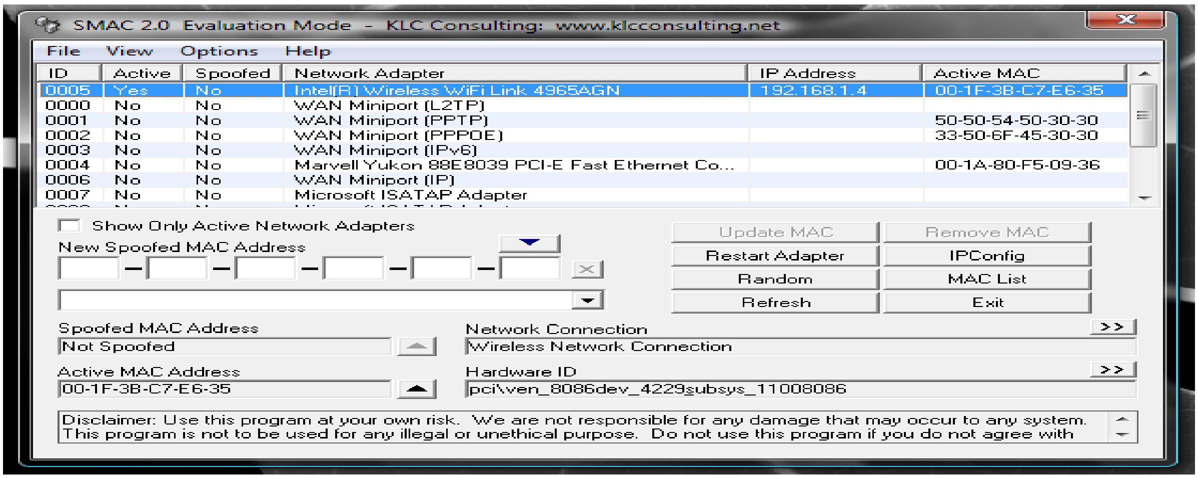
Active MAC Address: 00-1F-3B-C7-E6-35

Network Connection: Wireless Network Connection

Hardware ID: pci\ven_8086dev_4229subsys_11008086

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

Figure B



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0005	Yes	No	Intel(R) Wireless WiFi Link 4965AGN	192.168.1.4	00-1F-3B-C7-E6-35
0000	No	No	WAN Miniport (L2TP)		
0001	No	No	WAN Miniport (PPTP)		50-50-54-50-30-30
0002	No	No	WAN Miniport (PPPOE)		33-50-6F-45-30-30
0003	No	No	WAN Miniport (IPv6)		
0004	No	No	Marvell Yukon 88E8039 PCI-E Fast Ethernet Co...		00-1A-80-F5-09-36
0006	No	No	WAN Miniport (IP)		
0007	No	No	Microsoft ISATAP Adapter		

☐ Show Only Active Network Adapters

New Spoofed MAC Address

Spoofed MAC Address: Not Spoofed

Active MAC Address: 00-1F-3B-C7-E6-35

Network Connection: Wireless Network Connection

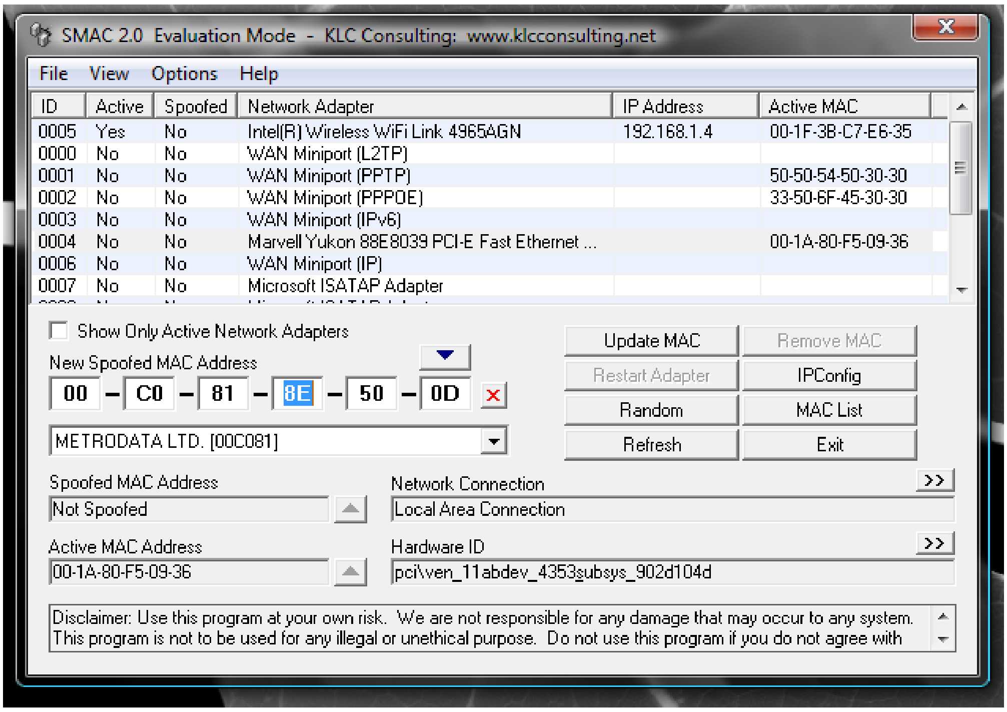
Hardware ID: pci\ven_8086dev_4229subsys_11008086

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

When you click on a different listing, the information about that hardware will be displayed below.

Let's change the MAC address of the Wired Marvell Yukon PCI-E Faster Ethernet Controller. To do this, select that entry from the list and click the Random button. As you can see in **Figure C**, the new, random MAC address is displayed in the New Spoofed MAC Address section.

Figure C



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0005	Yes	No	Intel(R) Wireless WiFi Link 4965AGN	192.168.1.4	00-1F-3B-C7-E6-35
0000	No	No	WAN Miniport (L2TP)		
0001	No	No	WAN Miniport (PPTP)		50-50-54-50-30-30
0002	No	No	WAN Miniport (PPPOE)		33-50-6F-45-30-30
0003	No	No	WAN Miniport (IPv6)		
0004	No	No	Marvell Yukon 88E8039 PCI-E Fast Ethernet ...		00-1A-80-F5-09-36
0006	No	No	WAN Miniport (IP)		
0007	No	No	Microsoft ISATAP Adapter		

☐ Show Only Active Network Adapters

New Spoofed MAC Address: 00 – C0 – 81 – 8E – 50 – 0D

METRODATA LTD. [00C081]

Spoofed MAC Address: Not Spoofed

Network Connection: Local Area Connection

Active MAC Address: 00-1A-80-F5-09-36

Hardware ID: pci\ven_11abdev_4353subsys_902d104d

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

The address listed will correspond to a manufacturer list that you can choose from.

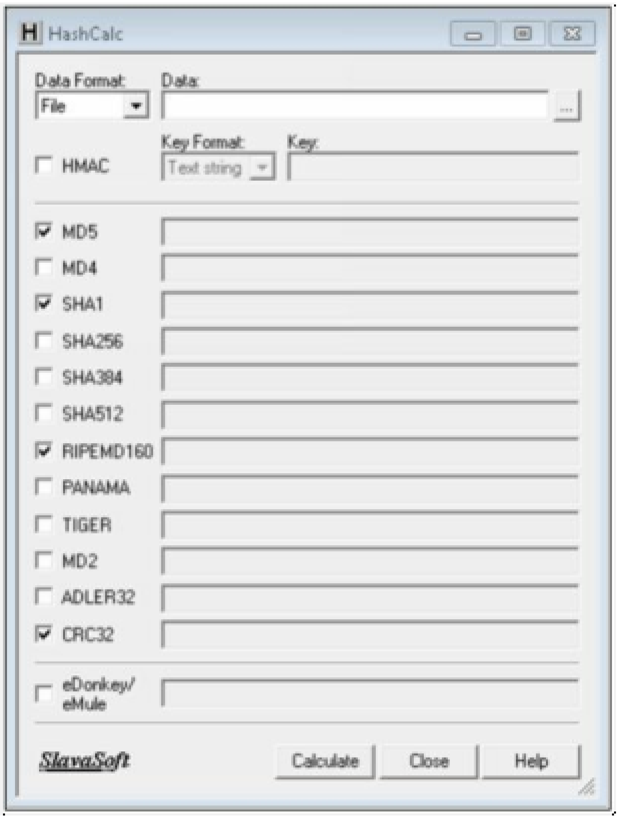
If you know you want to spoof your MAC address to that of a specific manufacturer you can select a different manufacturer from the drop-down list. When you make this selection, the address listed will change. You can keep hitting Random until you get an address you like (or you can just take the first random address you get).

Once you have your address, select the Options menu and make sure Automatically Restart Adapter is checked. Once that is checked, hit the Update MAC Address button and the new MAC address will be applied.

Practical No 15: Use The Following Tools For Cryptography Hashcale.

Calculating MD5 value using HashCalc

1. Open HashCalc tool.

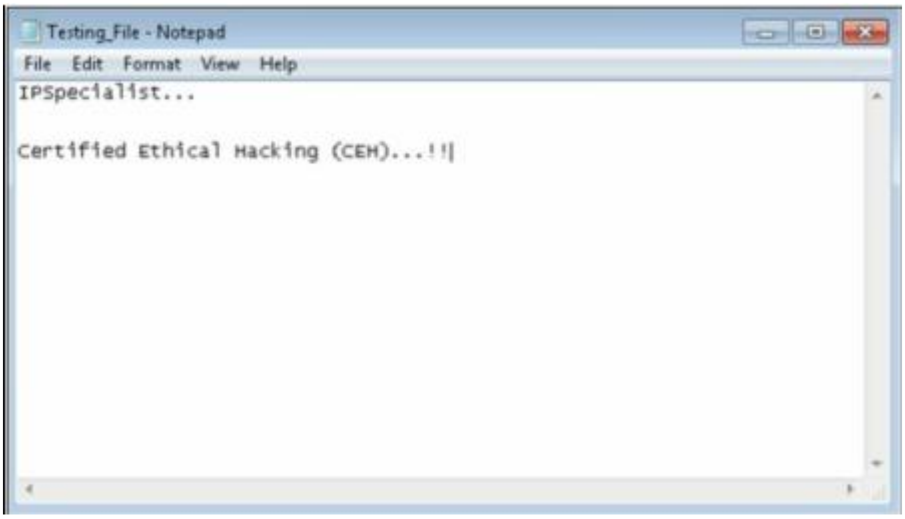


Data Format: File

☐ HMAC

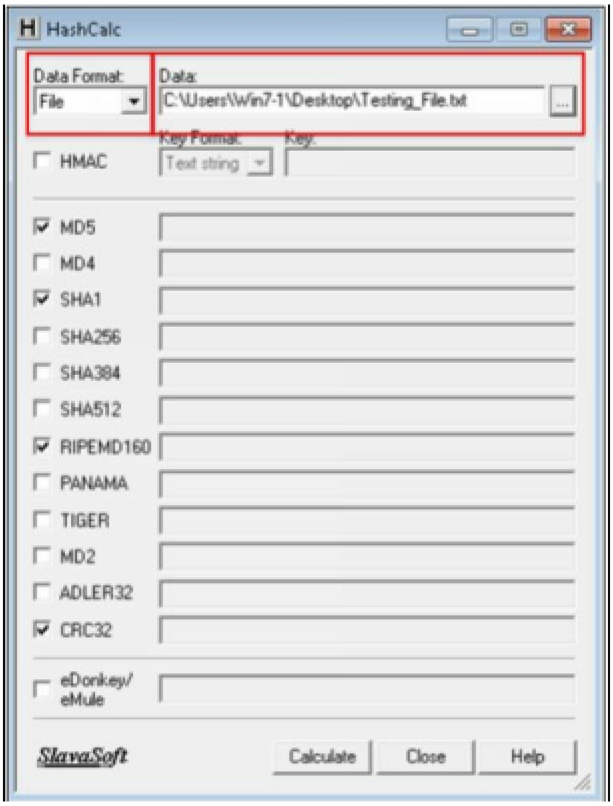
☑ MD5
☐ MD4
☑ SHA1
☐ SHA256
☐ SHA384
☐ SHA512
☑ RIPEMD160
☐ PANAMA
☐ TIGER
☐ MD2
☐ ADLER32
☑ CRC32
☐ eDonkey/ eMule

2. Create a new file with some content in it as shown below.



```
IPSpecialist...

Certified Ethical Hacking (CEH)...!!
```

3. Select Data Format as “File” and upload your file



Data Format: File

Data: C:\Users\Win7-1\Desktop\Testing_File.txt

□ HMAC Key Format: Text string Key:

☑ MD5

□ MD4

☑ SHA1

□ SHA256

□ SHA384

□ SHA512

☑ RIPEMD160

□ PANAMA

□ TIGER

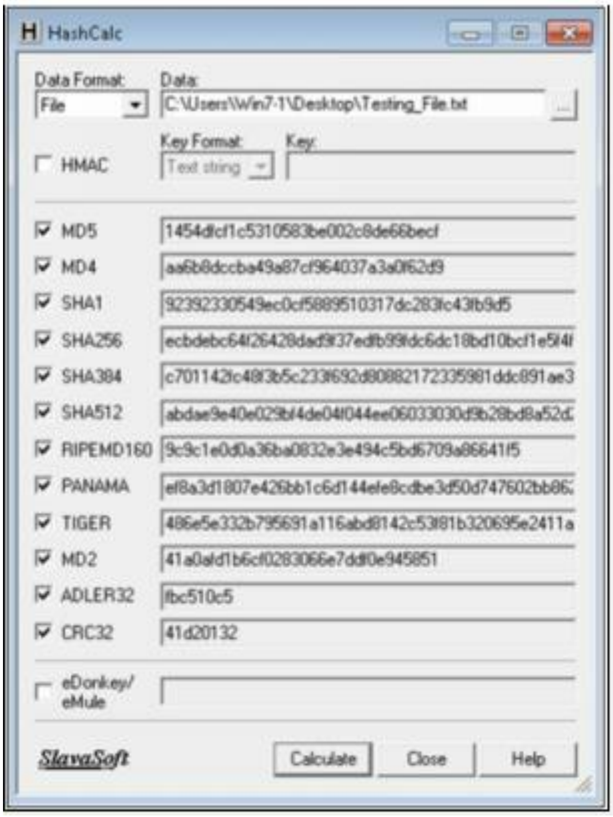
□ MD2

□ ADLER32

☑ CRC32

□ eDonkey/ eMule

4. Select Hashing Algorithm and Click Calculate



Data Format: File

Data: C:\Users\Win7-1\Desktop\Testing_File.txt

□ HMAC Key Format: Text string Key:

☑ MD5 1454dfcf1c5310583be002c8de66becf

☑ MD4 aa6b8dccba49a87cf964037a3a0f62d9

☑ SHA1 92392330f549ec0cf5889510317dc283fc43fb9d5

☑ SHA256 ecbdebc64f26428dadf9f37edfb99fdc6dc18bd10bcf1e5f4f

☑ SHA384 c701142fc48f3b5c233f692d80882172335981ddc891ae3

☑ SHA512 abdae9e40e029bf4de04f044ee06033030d9b28bd8a52d

☑ RIPEMD160 9c9c1e0d0a36ba0832e3e494c5bd6709a86641f5

☑ PANAMA ef8a3d1807e426bb1c6d144efe8cdbe3d50d747602bb86

☑ TIGER 486e5e332b795691a116abd8142c53f81b320695e2411a

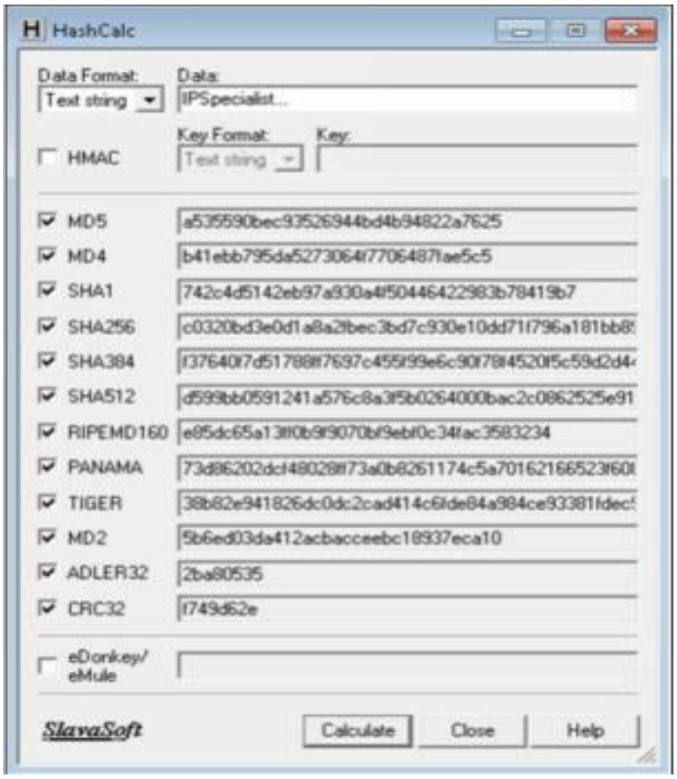
☑ MD2 41a0afd1b6cf0283066e7ddf0e945851

☑ ADLER32 fbc510c5

☑ CRC32 41d20132

□ eDonkey/ eMule

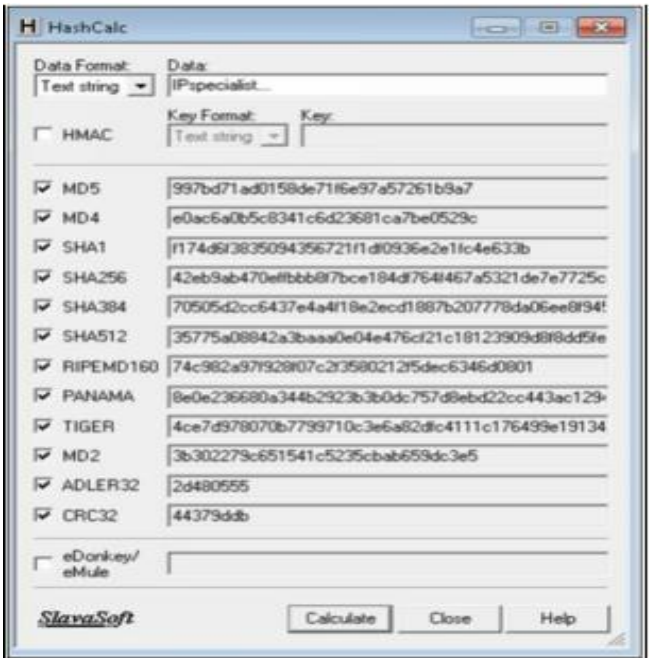
5. Now Select the Data Format to “**Text String**” and Type “**IPSpecialist…**” into Data filed and calculated MD5.



Data Format: Text string
Data: IPSpecialist...
□ HMAC Key Format: Text string Key:
☑ MD5 a535590bec93526944bd4b94822a7625
☑ MD4 b41ebb795da5273064f77064871ae5c5
☑ SHA1 742c4d5142eb97a930a4f50446422983b78419b7
☑ SHA256 c0320bd3e0d1a8a2fbec3bd7c930e10dd71f796a181bb8
☑ SHA384 f37640f7d51788ff7697c455f99e6c90f78f4520f5c59d2d4
☑ SHA512 d599bb0591241a576c8a3f5b0264000bac2c0862525e91
☑ RIPEMD160 e85dc65a13ff0b9f9070bf9ebf0c34fac3583234
☑ PANAMA 73d86202dcf48028ff73a0b8261174c5a70162166523f60
☑ TIGER 38b82e941826dc0dc2cad414c6fde84a984ce93381fdec
☑ MD2 5b6ed03da412acbacceebc18937eca10
☑ ADLER32 2ba80535
☑ CRC32 f749d62e
□ eDonkey/ eMule

MD5 Calculated for the text string “**IPSpecialist…**” is “**a535590bec93526944bd4b94822a7625**”

6. Now, let's see how MD5 value is changed from minor change.

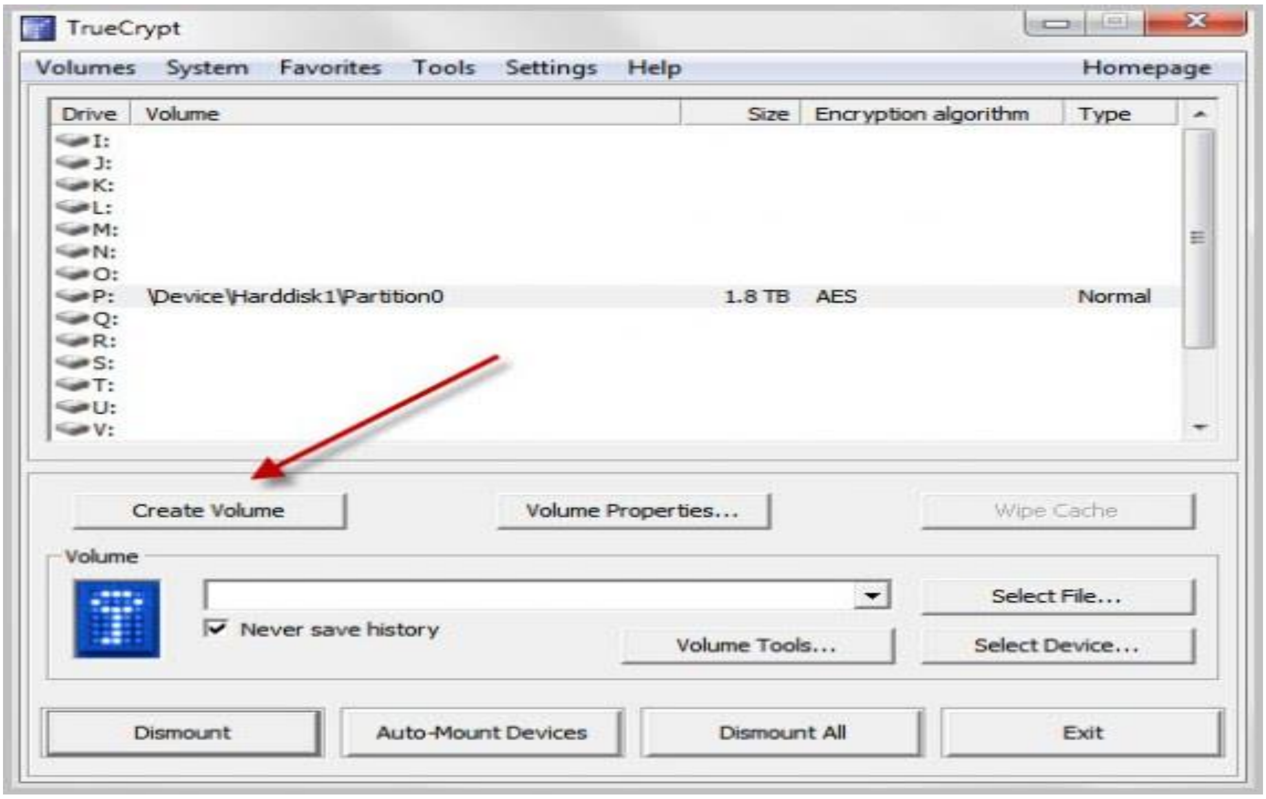


Data Format: Text string
Data: IPspecialist...
□ HMAC Key Format: Text string Key:
☑ MD5 997bd71ad0158de71f6e97a57261b9a7
☑ MD4 e0ac6a0b5c8341c6d23681ca7be0529c
☑ SHA1 f174d6f3835094356721f1df0936e2e1fc4e633b
☑ SHA256 42eb9ab470effbbb8f7bce184df764f467a5321de7e7725c
☑ SHA384 70505d2cc6437e4a4f18e2ecd1887b207778da06ee8f94
☑ SHA512 35775a08842a3baaa0e04e476cf21c18123909d8f8dd5fe
☑ RIPEMD160 74c982a97f928f07c2f3580212f5dec6346d0801
☑ PANAMA 8e0e236680a344b2923b3b0dc757d8ebd22cc443ac129
☑ TIGER 4ce7d978070b7799710c3e6a82dfc4111c176499e19134
☑ MD2 3b302279c651541c5235cbab659dc3e5
☑ ADLER32 2d480555
☑ CRC32 44379ddb
□ eDonkey/ eMule

Just lowering the case of single alphabet changes entire hashing value. MD5 Calculated for the text string “**IPspecialist…**” is “**997bd71ad0158de71f6e97a57261b9a7”**

Practical No 16: Use The Following Tools For Cryptography Truecrypt.

TrueCrypt is a leading disk encryption software program that lets you secure disk partitions on your Windows computer. There are times when your hard drive is accessible by other people, such as in an office setting, while travelling, or at home. The data you have on the PC may be vulnerable to attack and compromise your privacy. However, in these moments of risk, **TrueCrypt may just be the tool to protect your data.**



Click Next two times on the following screens to create an encrypted file container with a standard TrueCrypt volume (those are the default options). Click Select File and browse to a location where you want to create the new container. **Make sure it is not in the Dropbox folder if Dropbox is running.** You can name the container anyway you want, e.g. holiday2010.avi.

Click Next on the encryption options page unless you want to change the encryption algorithm or hash algorithm. Select the volume size on the next screen. I suggest you keep it at a few hundred Megabytes tops.

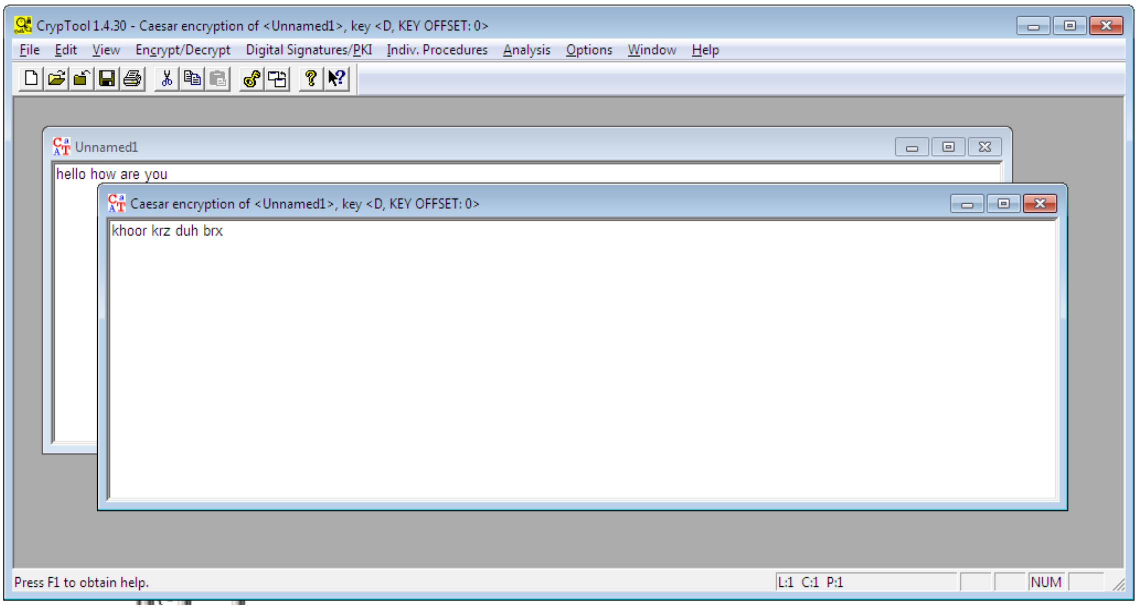
You need to enter a secure password on the next screen. It is suggested to use as many characters as possible (24+) with upper and lower letters, numbers and special characters. The maximum length of a True Crypt password is 64 characters.

Now it is time to select the volume format on the next screen. If you only use Windows computers you may want to select NTFS as the file system. If you use others you may be better of with FAT. Juggle the mouse around a bit and click on format once you are done with that.

Congratulations, the new True Crypt volume has been created.

Practical No 17: Use The Following Tools For Cryptography Cryptool.

Cryptool is a free e-learning tool to illustrate the concepts of cryptography. Try Various Encryption/Decryption algorithms.



CrypTool 1.4.30 - Caesar encryption of <Unnamed1>, key <D, KEY OFFSET: 0>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed1

hello how are you

Caesar encryption of <Unnamed1>, key <D, KEY OFFSET: 0>

khoor krz duh brx

Press F1 to obtain help.
L:1 C:1 P:1
NUM