Madhav Institute of Technology & Science
Gwalior

PRACTICAL FILE

Network &Web LAB (BCSL 605)

COMPUTER SCIENCE & ENGINEERING

Session: 2016-2020

Submitted To:

Prof. Santosh Sahu

Kesharvani

Submitted By:

Name: Shubham

Roll No: 090CS161112

Course: B.E (CSE)

Semester: VI

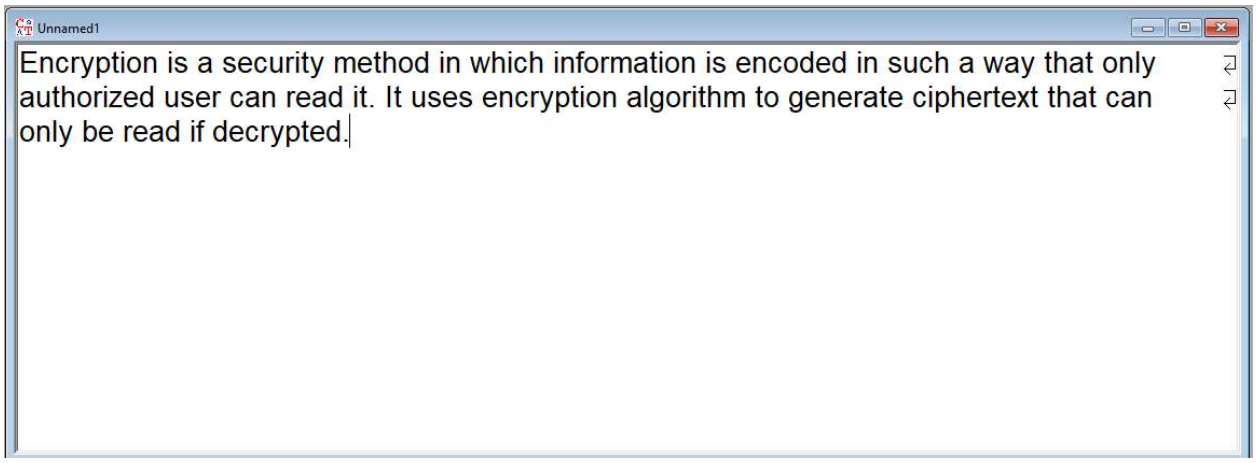
S . No.	Experiment	Date	Sign.
1	Footprinting using footprintingtools(Open Source & Free)(ex-nslookup,ARIN,Whois,Google Earth etc.)		
2	Scanning for vulnerabilities using (Angry IP,HPing2,IPScanner,GlobalNetwork,InventoryScanner,Net Tools Suite Pack etc.)		
3	NetBIOS Enumeration Using NetViewTool,Nbtstat Enumeration Tool(Open Source)		
4	Steganography using tools : Merge Streams,ImageHide,StealthFiles,Blindside,Stools,Steghide,Steganos,Pretty Good Envelop,Stegdetect		
5	Steganalysis – Stego Watch – Stego Detection Tool,StegSpy		
6	How to Detect Trojans by using – Netstat,fPort,TCPView,CurrPortsTool,Process Viewer		
7	Lan Scanner using look@LAN,wireshark		
8	Understanding DoS Attack Tools –Jolt2,Bubonic.c,Land and LaTierra,Targa,Nemesy Blast,Panther2,Crazy Pinger,SomeTrouble,UDPFlood,FSMax.		

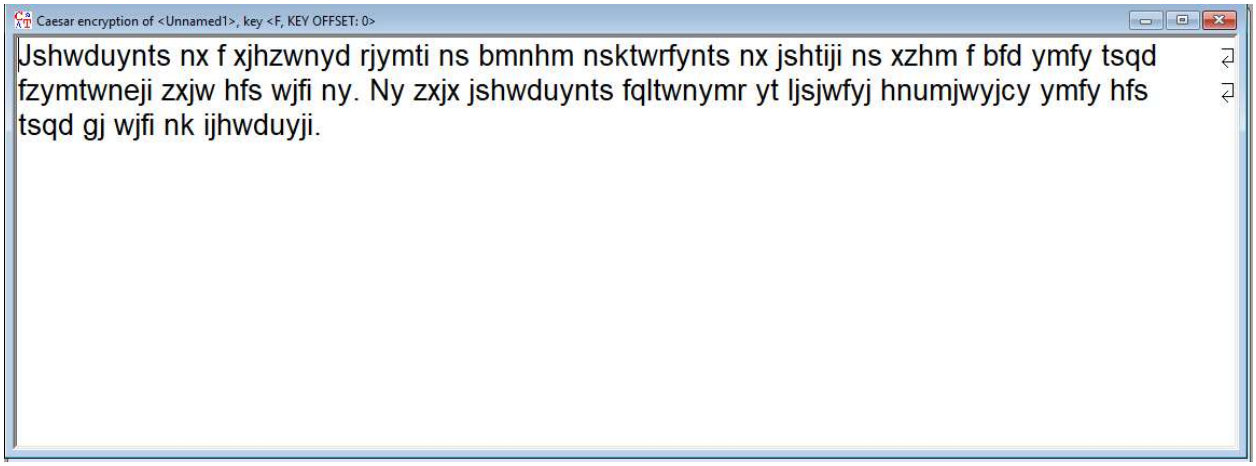
Experiment-1

Objective :-Encryption and Decryption using cryptography .

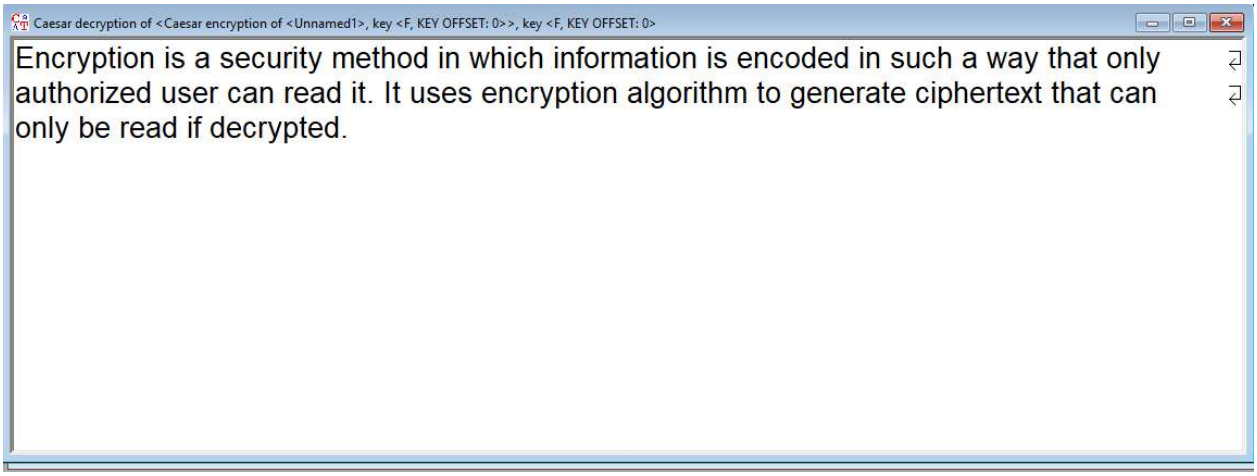
Ans : -

1. **Encryption : -**Encryption is a security method in which information is encoded in such a way that only authorized user can read it. It uses encryption algorithm to generate ciphertext that can only be read if decrypted.





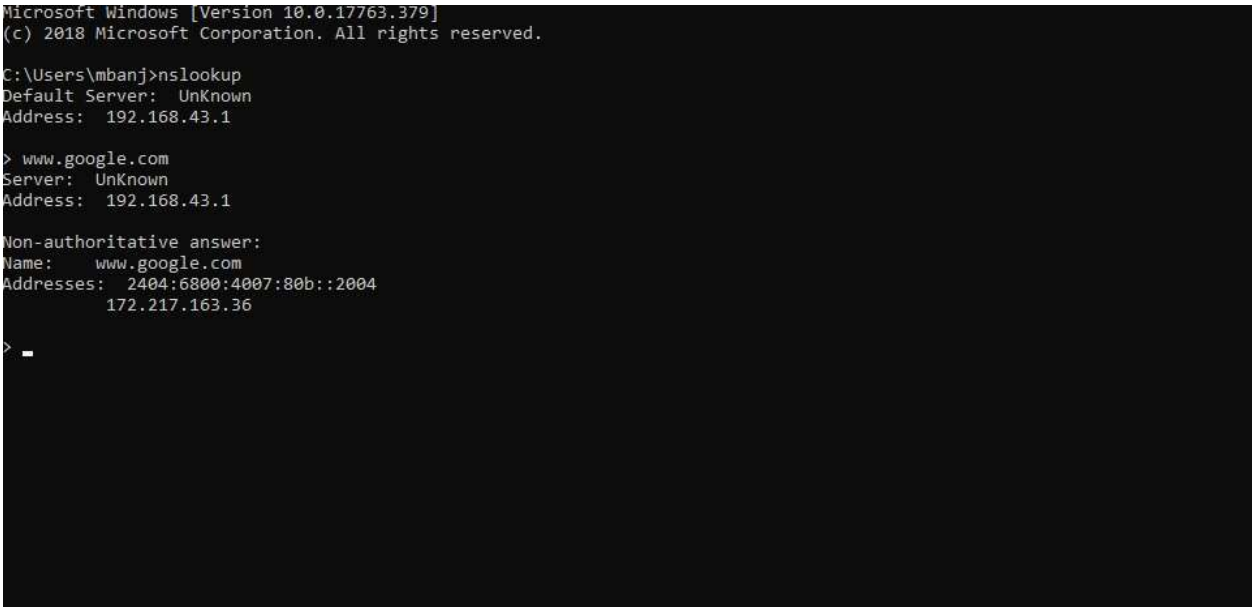
2. **Decryption : -**The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

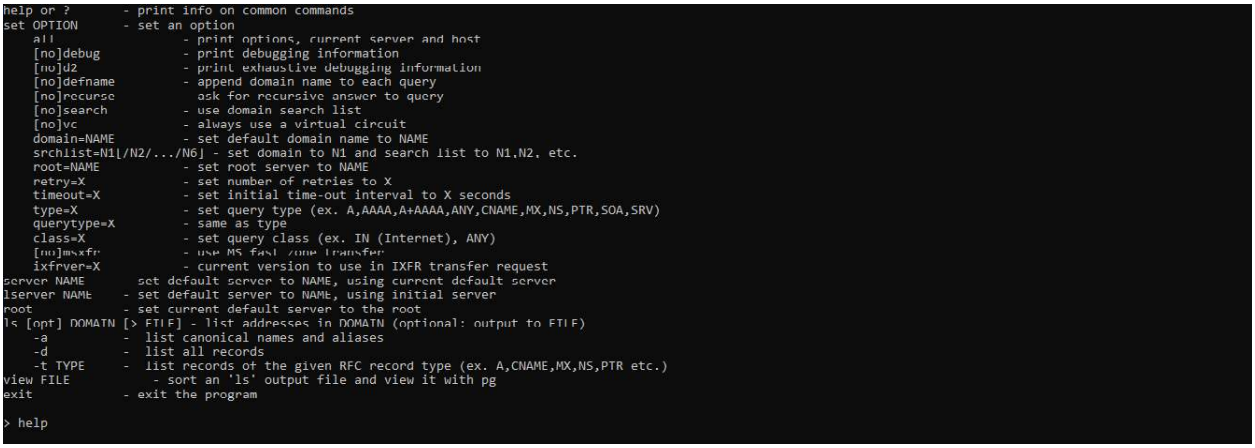


Experimet-2

Objective : Footprinting using footprinting tools :

1 . ex – nslookup : -NsLookup is a tool included in many operating systems that can look up IP addresses and perform other searches on DNS domains and servers. This resource is housed in a utility called nslookup.exe. NsLookup is a basic way to get fundamental DNS information quickly and easily.





2.ARIN :-ARIN is a Regional Internet Registry (RIR) incorporated in the Commonwealth of Virginia, USA. There are five RIRs covering the globe, and each RIR:

- Provides services related to the technical coordination and management of Internet number resources in its respective service region;
- Participates in the global Internet community;
- Facilitates the development of policy decisions made by its members and any other interested Internet citizens;
- Is a nonprofit, membership organization;
- Is governed by an executive board elected by its membership.

3 .WHOIS : -Whois is an Internet service and protocol that searches and displays information pertaining to a domain name from repositories of domain name registrars worldwide.

Whois service is a free Internet service that enables a user to search a specific domain name's availability and, in the case that it's registered, the assigned entity/person to whom it is registered. Whois was first conceived in 1982 as an enhancement to the Nickname protocol that was developed by ARPANET.

Whois Record for Google.com

Domain Profile

Registrant Org	Google LLC
Registrant Country	US
Registrar	MarkMonitor, Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895740
Registrar Status	clientUpdateProhibited, clientTransferProhibited, clientDeleteProhibited, serverUpdateProhibited, serverTransferProhibited, serverDeleteProhibited
Dates	7,850 days old Created on 1997-09-15 Expires on 2020-09-13 Updated on 2018-02-21
Name Servers	NS1.GOOGLE.COM (has 14,357 domains) NS2.GOOGLE.COM (has 14,357 domains) NS3.GOOGLE.COM (has 14,357 domains) NS4.GOOGLE.COM (has 14,357 domains)
Tech Contact	—
IP Address	172.217.3.164 - 106 other sites hosted on this server
IP Location	- California - Mountain View - Google Llc
ASN	AS15169 GOOGLE - Google LLC, US (registered Mar 30, 2000)
IP History	328 changes on 328 unique IP addresses over 15 years
Registrar History	3 registrars with 1 drop

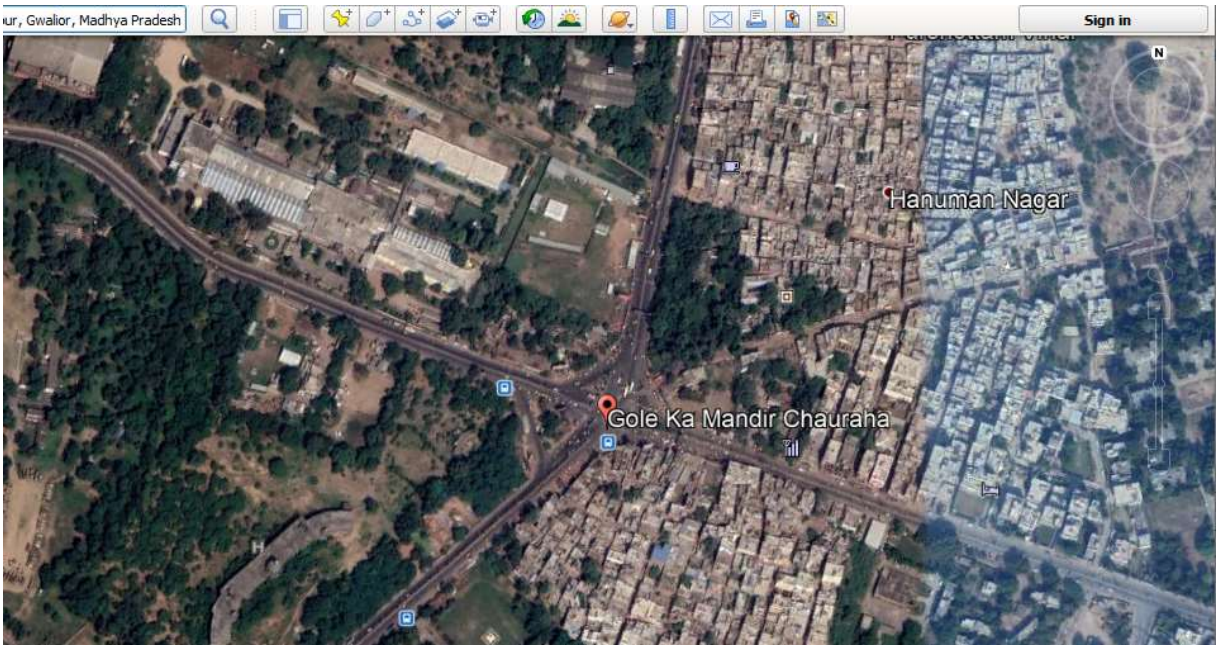
Website

Website Title	Google
Server Type	Gws
Response Code	200
Terms	5,867 (Unique: 1,208, Linked: 32)
Images	1 (Alt tags missing: 0)
Links	19 (Internal: 16, Outbound: 0)

Whois Record (last updated on 2019-03-14)

4 .Google Earth : - Google gets images for Google Earth from satellite photos, which are stitched together to make a larger image. The images themselves are of varying quality.

Google Earth is a beefed-up map of the world. Instead of the normal 2D, click-and-drag map you're perhaps used to, Google Earth mimics the globe with a spherical map and stunning graphics so that you can zoom and glide over the oceans and cities of the world.



Experiment-3

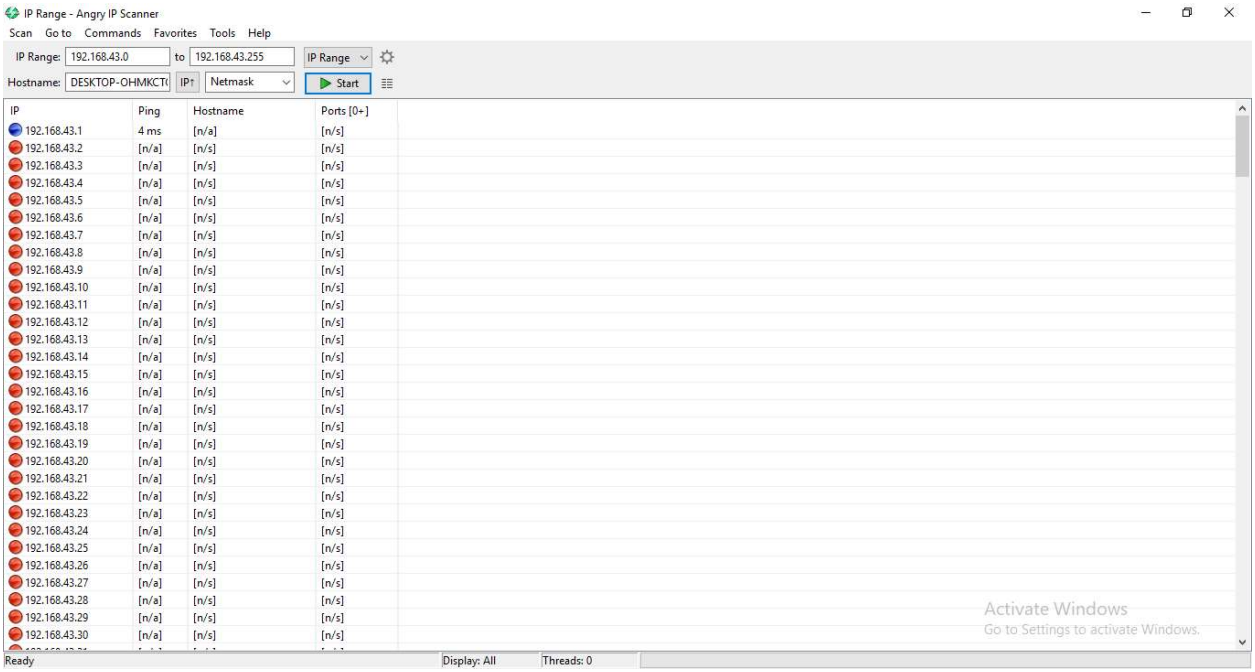
Objective : Scanning for vulnerabilities using :

1. **Angry ip : -**Angry IP scanner is a very fast IP address and port scanner.

It can scan IP addresses in any range as well as any their ports. It is cross-platform and lightweight. Not requiring any installations, it can be freely copied and used anywhere.

Angry IP scanner simply pings each IP address to check if it's alive, then optionally it is resolving its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be extended with plugins.

It also has additional features, like NetBIOS information (computer name, workgroup name, and currently logged in Windows user), favorite IP address ranges, web server detection, customizable openers, etc.



2 . HPing2 : -Hping2 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping do with ICMP replies. Hping2 handles

fragmentation, arbitrary packet body and size and can be used in order to transfer files under supported protocols.

Hping2 can be used, among other things to:

- Test firewall rules,
- [spoofed] port scanning,
- Test net performance using differents protocols, packet size, TOS (type of service) and fragmentation,
- Path MTU discovery,
- Files transfering even between really fascist firewall rules,
- Traceroute like under different protocols,
- Firewalk like usage,
- Remote OS fingerprint,
- TCP/IP stack auditing

It's also really a good didactic tool to learn TCP/IP.

hping2 rc3 --scan mode output example:

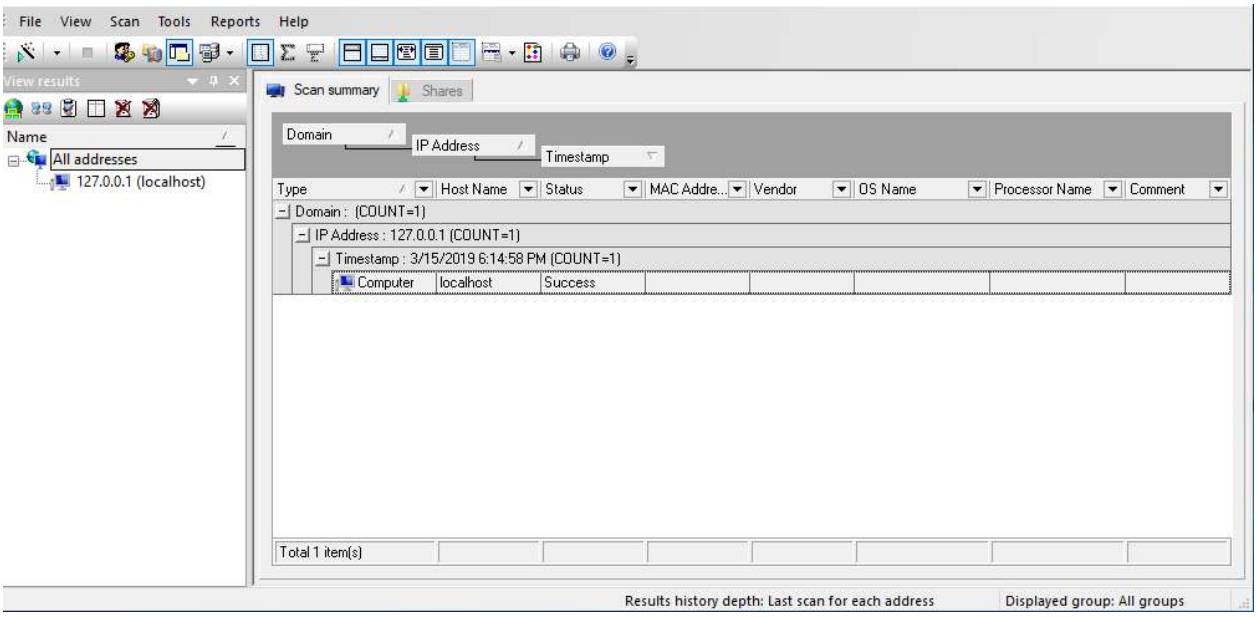
```
# hping2 --scan known 1.2.3.4

Scanning 1.2.3.4 (1.2.3.4), port known
245 ports to scan, use -V to see all the replies
+----+----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+----------+---------+---+-----+-----+-----+
    9 discard    : .S..A...  64     0 32767    44
   13 daytime    : .S..A...  64     0 32767    44
   21 ftp        : .S..A...  64     0 32767    44
   22 ssh        : .S..A...  64     0 32767    44
   25 smtp       : .S..A...  64     0 32767    44
   37 time       : .S..A...  64     0 32767    44
   80 www        : .S..A...  64     0 32767    44
  111 sunrpc     : .S..A...  64     0 32767    44
  113 auth       : .S..A...  64     0 32767    44
  631 ipp        : .S..A...  64     0 32767    44
 3306 mysql      : .S..A...  64     0 32767    44
 6000 x11        : .S..A...  64     0 32767    44
 6667 ircd       : .S..A...  64     0  3072    44
All replies received. Done.
Not responding ports:
```

3. **IPScanner : -**IP Scanner is a tool that is quite useful in the field of networking. The IP Scanner is, as its name indicates, a scanner that scans for IP addresses and various other information of the devices on your network. So, in short, the IP scanner scans your network for devices and information relevant to them.

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-15 06:30 UTC

Nmap scan report for 27.57.199.80

Host is up.



PORT     STATE    SERVICE

21/tcp   filtered ftp

22/tcp   filtered ssh

23/tcp   filtered telnet

80/tcp   filtered http

110/tcp  filtered pop3

143/tcp  filtered imap

443/tcp  filtered https

3389/tcp filtered ms-wbt-server
```

```
Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
```

4. **Global Network Inventory : - Global Network Inventory** is a powerful and flexible software and hardware inventory system that can be used as an audit scanner in an agent-free and zero deployment environments. If used as an audit scanner, it only requires full administrator rights to the remote computers you wish to scan. Global Network Inventory can audit remote computers and even network appliances, including switches, network printers, document centers, etc.



Experiment-4

Objective :Open source :

1. **NetBIOS Enumeration Using NetView Tool : -**NetBIOS stands for Network Basic Input Output System. It Allows computer communication over a LAN and allows them to share files and printers.

NetBIOS names are used to identify network devices over TCP/IP (Windows). It must be unique on a network, limited to 16 characters where 15 characters are used for the device name and the 16th character is reserved for identifying the type of service running or name record type.

Attackers use the NetBIOS enumeration to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts on the network
- Policies and passwords

```
nbtscan 172.16.1.102
Doing NBT name scan for addresses from 172.16.1.102

IP address       NetBIOS Name     Server    User             MAC
address
------------------------------------------------------------------------
--------
172.16.1.102     METASPLOITABLE   <server>  METASPLOITABLE
00:00:00:00:00:00
```

```
nbtscan 172.16.1.102 -v
Doing NBT name scan for addresses from 172.16.1.102

NetBIOS Name Table for Host 172.16.1.102:

Incomplete packet, 335 bytes long.
Name             Service          Type
---------------------------------------
METASPLOITABLE   <00>             UNIQUE
METASPLOITABLE   <03>             UNIQUE
METASPLOITABLE   <20>             UNIQUE
METASPLOITABLE   <00>             UNIQUE
```

```
METASPLOITABLE   <03>            UNIQUE
METASPLOITABLE   <20>            UNIQUE
__MSBROWSE__  <01>              GROUP
WORKGROUP        <00>              GROUP
WORKGROUP        <1d>            UNIQUE
WORKGROUP        <1e>              GROUP
WORKGROUP        <00>              GROUP
WORKGROUP        <1d>            UNIQUE
WORKGROUP        <1e>              GROUP

Adapter address: 00:00:00:00:00:00
----------------------------------------
```

```
nbtscan 172.16.1.102 -vh
Doing NBT name scan for addresses from 172.16.1.102

NetBIOS Name Table for Host 172.16.1.102:

Incomplete packet, 335 bytes long.
Name             Service          Type
----------------------------------------
METASPLOITABLE   Workstation Service
METASPLOITABLE   Messenger Service
METASPLOITABLE   File Server Service
METASPLOITABLE   Workstation Service
METASPLOITABLE   Messenger Service
METASPLOITABLE   File Server Service
__MSBROWSE__  Master Browser
WORKGROUP        Domain Name
WORKGROUP        Master Browser
WORKGROUP        Browser Service Elections
WORKGROUP        Domain Name
WORKGROUP        Master Browser
WORKGROUP        Browser Service Elections

Adapter address: 00:00:00:00:00:00
----------------------------------------
```

2. **Nbtstat Enumeration Tool : -**Displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. **nbtstat** allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Used without parameters, **nbtstat** displays help.

Syntax
Copy

```
nbtstat [/a <remoteName>] [/A <IPaddress>] [/c] [/n] [/r] [/R]
[/RR] [/s] [/S] [<Interval>
```

```
nbtscan
NBTscan version 1.5.1. Copyright (C) 1999-2003 Alla Bezroutchko.
This is a free software and it comes with absolutely no warranty.
You can use, distribute and modify it under terms of GNU GPL.

Usage:
nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s
separator] [-m retransmits] (-f filename)|(<scan_range>)
       -v            verbose output. Print all names received
                     from each host
       -d            dump packets. Print whole packet contents.
       -e            Format output in /etc/hosts format.
       -l            Format output in lmhosts format.
                     Cannot be used with -v, -s or -h options.
       -t timeout    wait timeout milliseconds for response.
                     Default 1000.
       -b bandwidth  Output throttling. Slow down output
                     so that it uses no more that bandwidth bps.
                     Useful on slow links, so that ougoing queries
                     don't get dropped.
       -r            use local port 137 for scans. Win95 boxes
                     respond to this only.
                     You need to be root to use this option on Unix.
       -q            Suppress banners and error messages,
       -s separator  Script-friendly output. Don't print
                     column and record headers, separate fields with
separator.
       -h            Print human-readable names for services.
                     Can only be used with -v option.
       -m retransmits       Number of retransmits. Default 0.
       -f filename   Take IP addresses to scan from file filename.
```

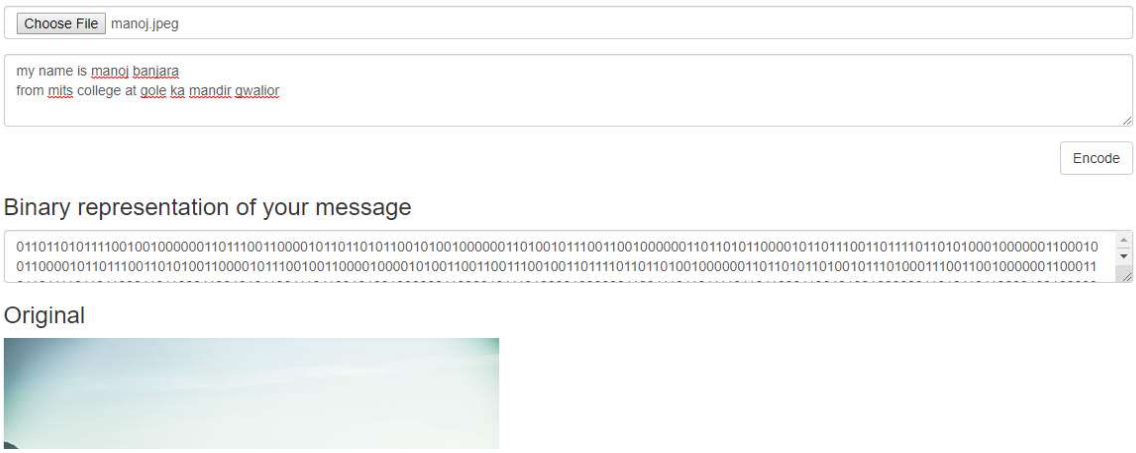
```
                    -f - makes nbtscan take IP addresses from stdin.
      <scan_range>  what to scan. Can either be single IP
                    like 192.168.1.1 or
                    range of addresses in one of two forms:
                    xxx.xxx.xxx.xxx/xx or xxx.xxx.xxx.xxx-xxx.
Examples:
      nbtscan -r 192.168.1.0/24
            Scans the whole C-class network.
      nbtscan 192.168.1.25-137
            Scans a range from 192.168.1.25 to 192.168.1.137
      nbtscan -v -s : 192.168.1.0/24
            Scans C-class network. Prints results in script-friendly
            format using colon as field separator.
            Produces output like that:
            192.168.0.1:NT_SERVER:00U
            192.168.0.1:MY_DOMAIN:00G
            192.168.0.1:ADMINISTRATOR:03U
            192.168.0.2:OTHER_BOX:00U
            ...
      nbtscan -f iplist
            Scans IP addresses specified in file iplist.
```

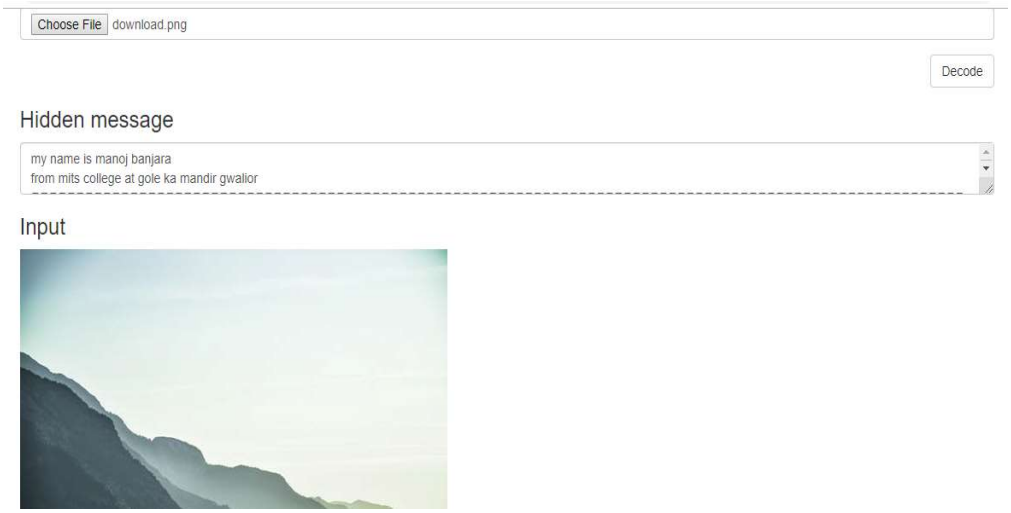
Experiment-5

Objective :Stagnography Using Tools :

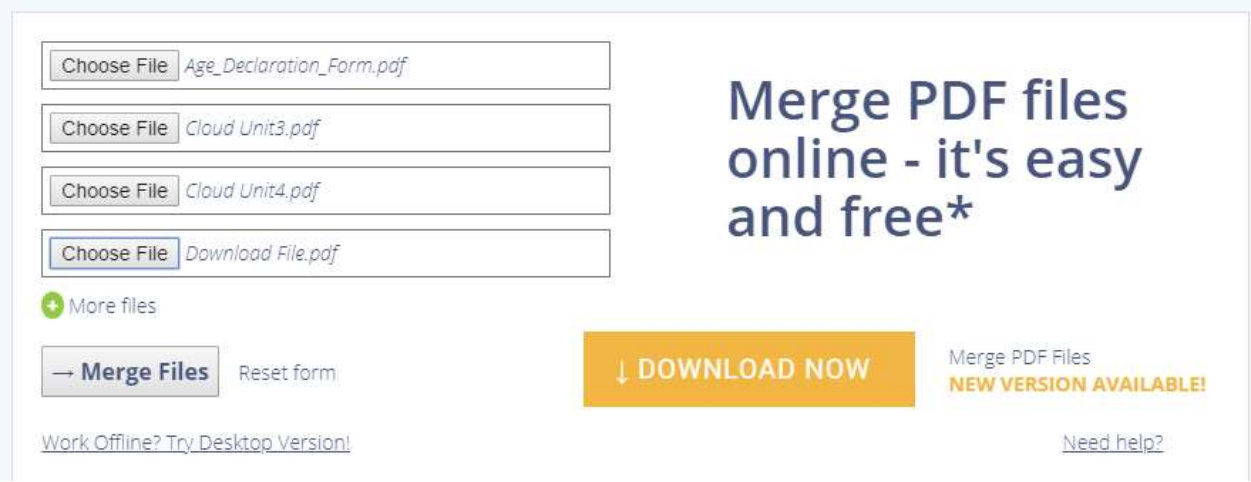
1. **Stagnography : -** Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.

   Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.



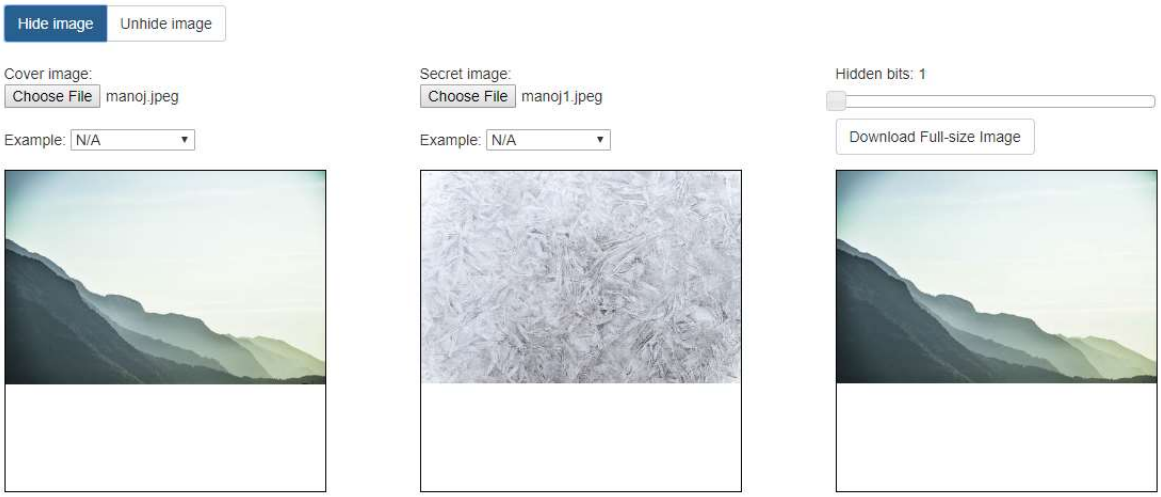


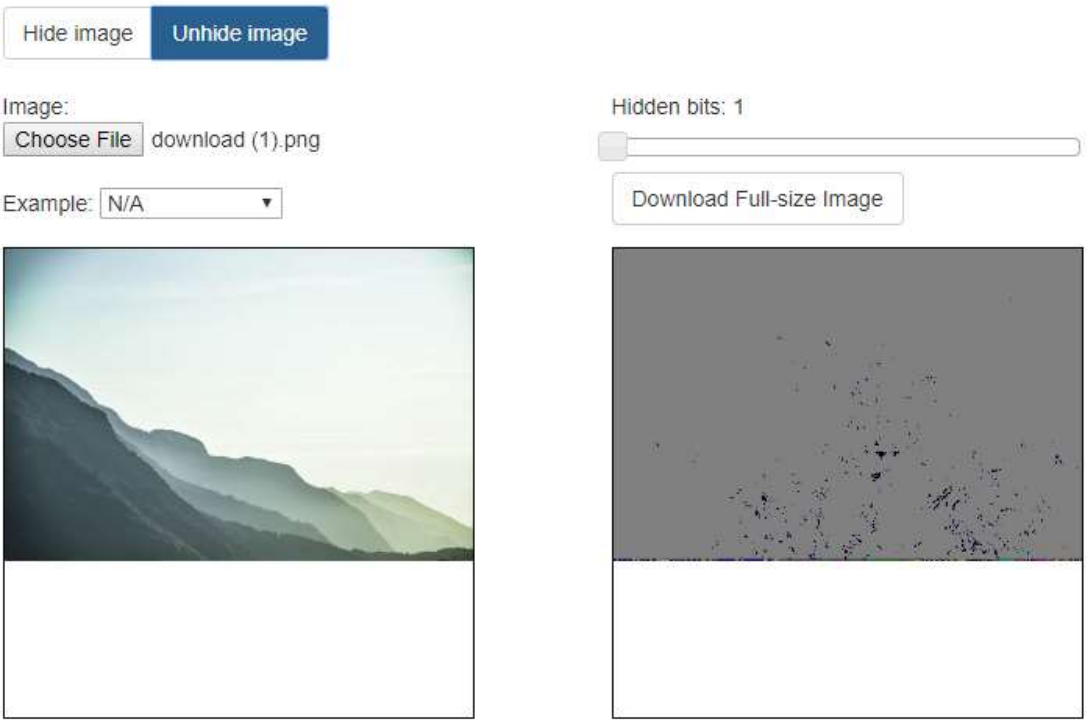
2. **Merge Streams : -** One of the utilities that is included in your Wireshark distribution is a command line tool called 'mergecap'. We use this tool to merge multiple captures generated, let's say, from a ring buffer capture (you can see how to do ring buffer captures using T-Shark here).



3. **Image Hide : -**This is a client-side Javascript tool to steganographically hide images inside the lower "bits" of other images.

Select either "Hide image" or "Unhide image". Play with the **example** images (all 200x200 px) to get a feel for it.





4. **Stealth Files : -**Stealth Files hides any type of file in almost any other type of file. This is called steganography. This is a way of encrypting data so that it is hard to find. You can not decrypt something unless you know what to decrypt. Using steganography, Stealth Files compresses, encrypts, and then hides any type of file inside many other types of files, including EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI, WAV, DOC, BMP, and most other types of video, image, and executable files. You will still be able to view, open, and run these files without and problems. If you want to, you can also use a password to encrypt the hidden files.

Experiment-6

Objective :Steganalysis :

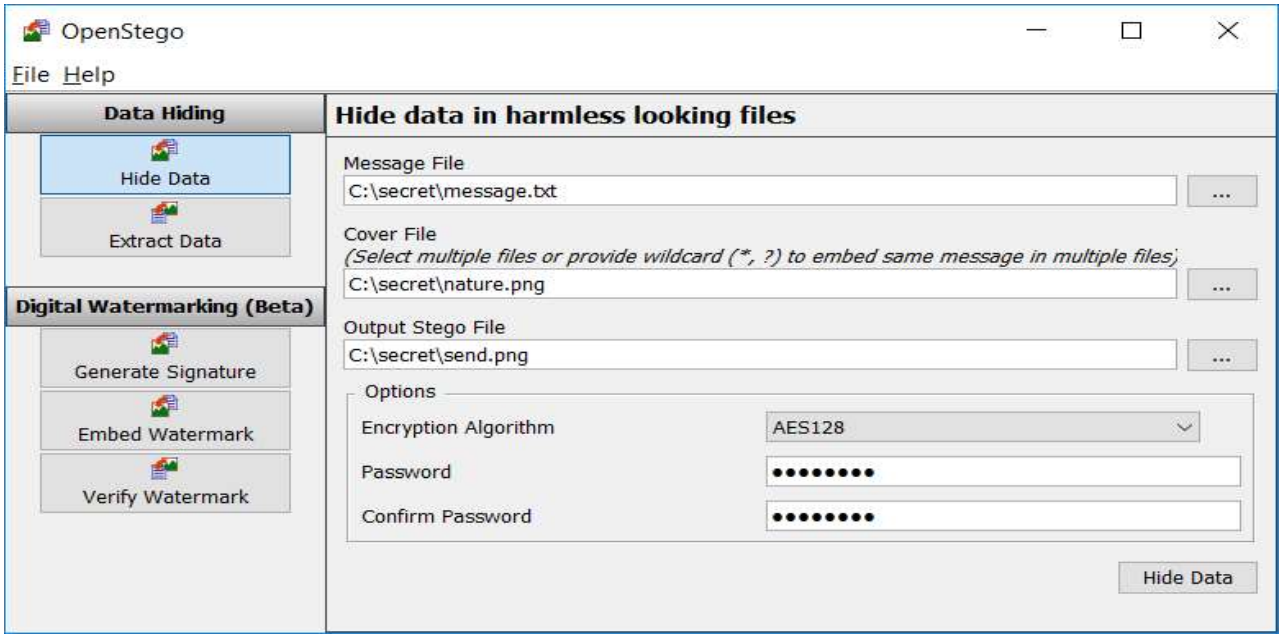
1. **Stego Watch : -**Welcome to the homepage of OpenStego, the free steganography solution.

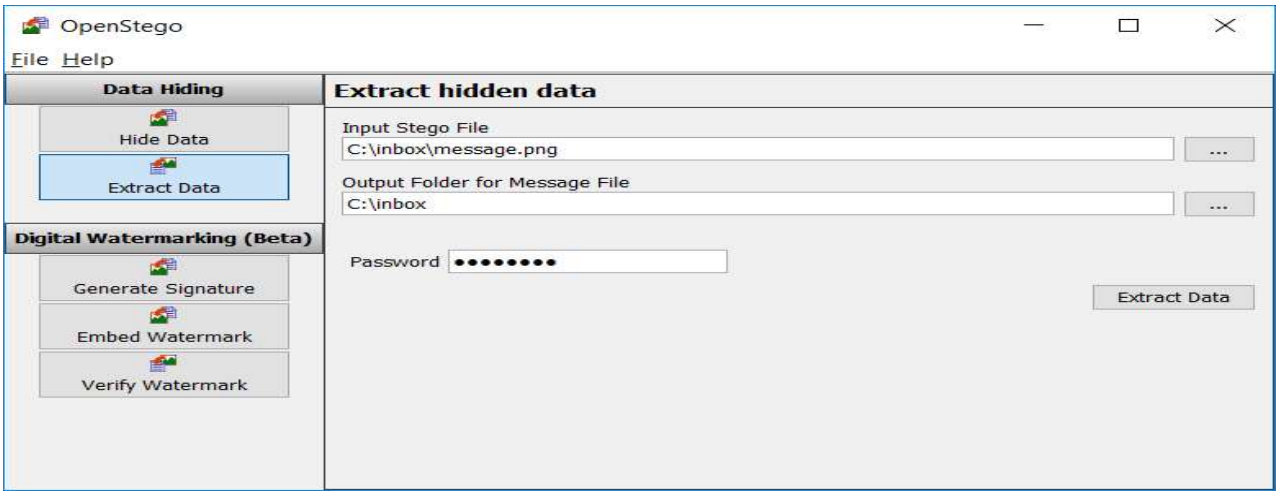
OpenStego provides two main functionalities:

- **Data Hiding:** It can hide any data within a cover file (e.g. images).
- **Watermarking (beta):** Watermarking files (e.g. images) with an invisible signature. It can be used to detect unauthorized file copying.

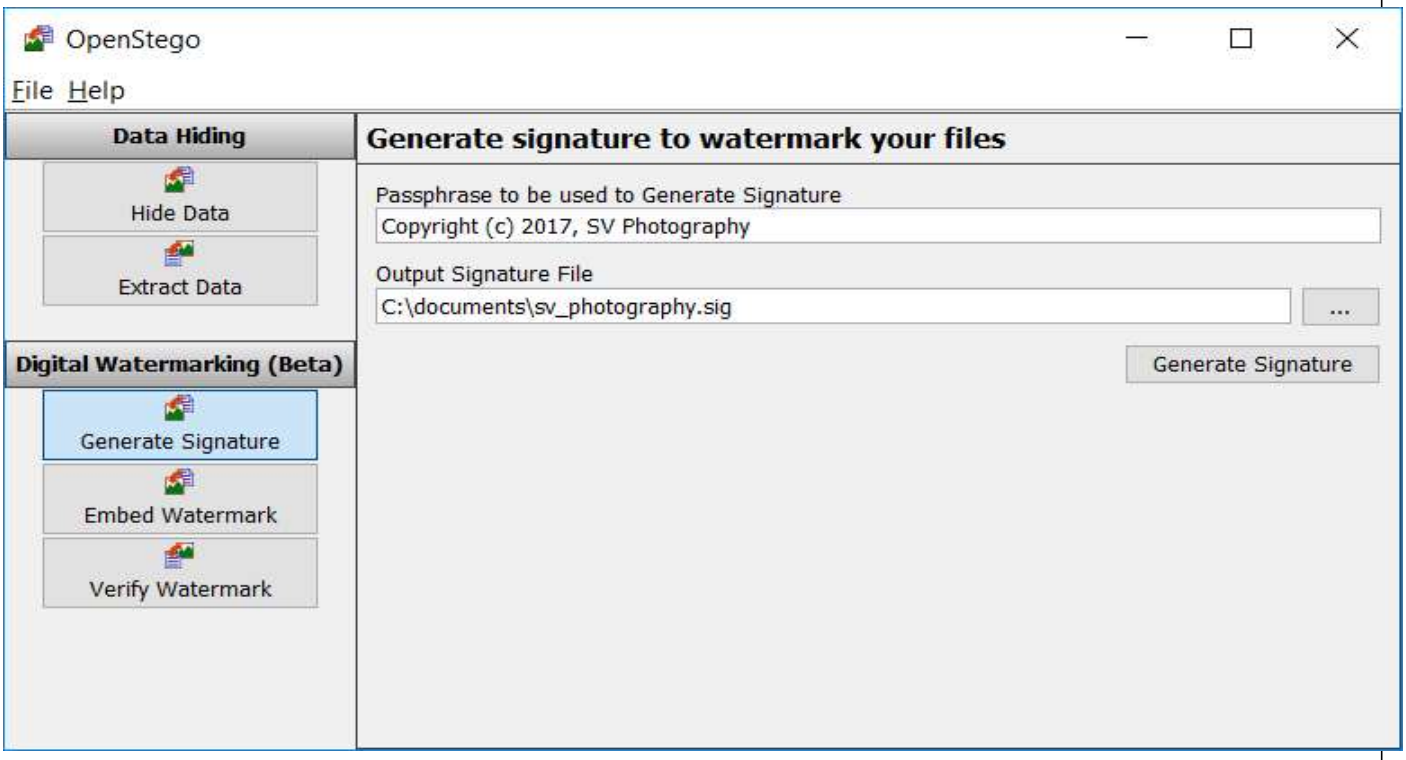
Please see Concepts page to learn more.

- **Data Hiding –**





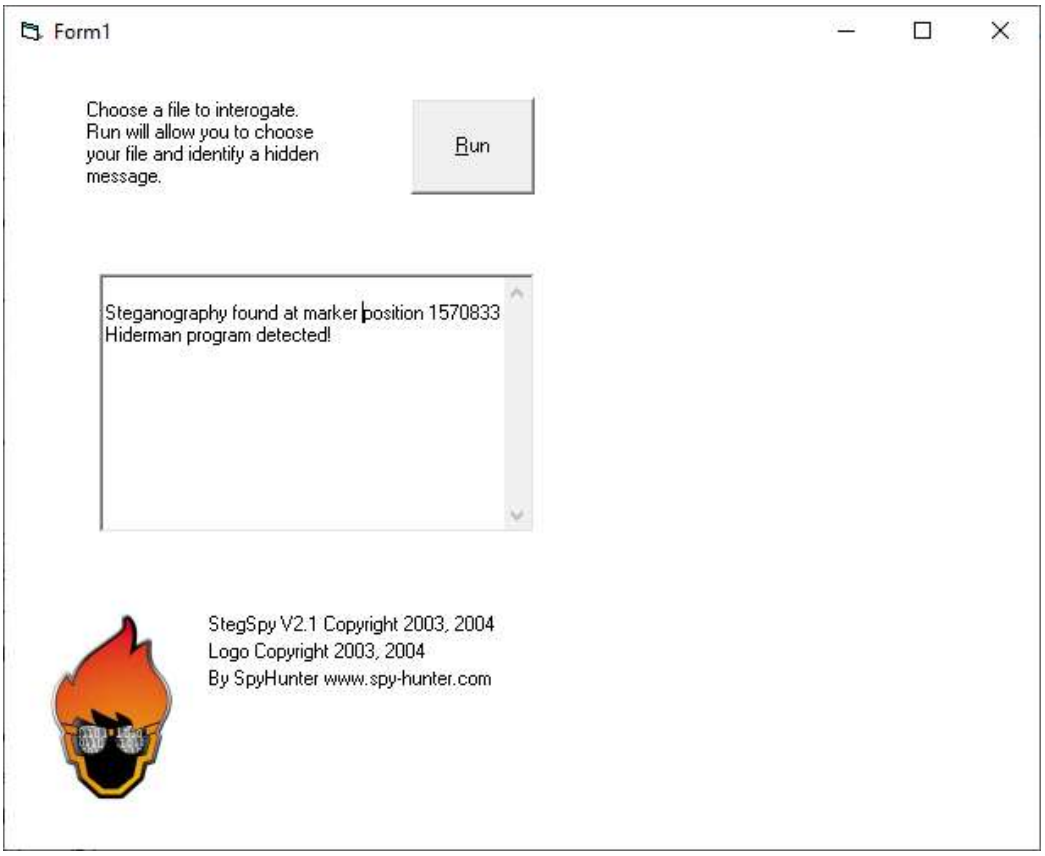
- **Watermarking (beta –**



2. StregSpy : -

StegSpy is a program always in progress. The latest version includes allows identification of a "steganized" file. StegSpywill detect steganography and the program used to hide the message. The lastest version also identifies the location of the hidden content as well. StegSpy currently identifies the following programs:

- Hiderman
- JPHideandSeek
- Masker
- JPegX
- Invisible Secrets


Form1
Choose a file to interogate.
Run will allow you to choose
your file and identify a hidden
message.
Run
Steganography found at marker position 1570833
Hiderman program detected!
StegSpy V2.1 Copyright 2003, 2004
Logo Copyright 2003, 2004
By SpyHunter www.spy-hunter.com

Experiment-7

Objective :Detect Trojans :

1. **Netstat : -** Displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. **nbtstat** allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Used without parameters, **nbtstat** displays help.

Syntax
Copy

```
nbtstat [/a <remoteName>] [/A <IPaddress>] [/c] [/n] [/r] [/R]
[/RR] [/s] [/S] [<Interval>
```

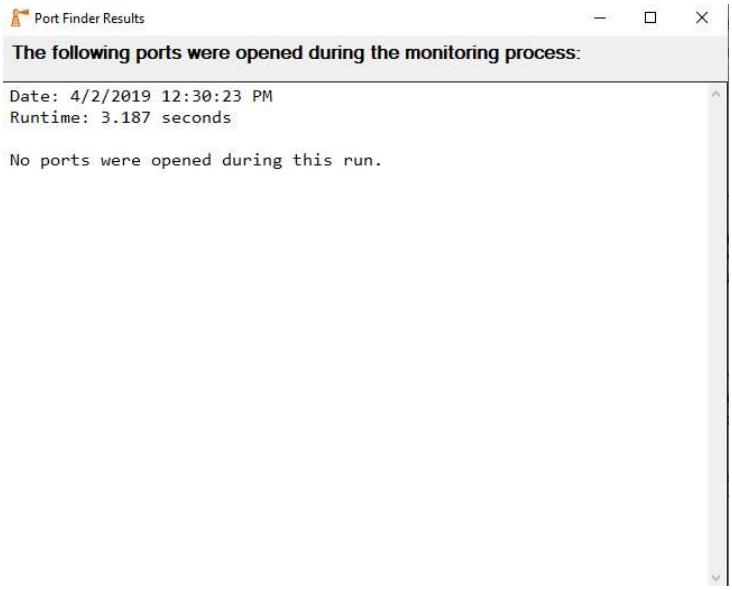
```
nbtscan
NBTscan version 1.5.1. Copyright (C) 1999-2003 Alla Bezroutchko.
This is a free software and it comes with absolutely no warranty.
You can use, distribute and modify it under terms of GNU GPL.

Usage:
nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s
separator] [-m retransmits] (-f filename)|(<scan_range>)
       -v            verbose output. Print all names received
                     from each host
       -d            dump packets. Print whole packet contents.
       -e            Format output in /etc/hosts format.
       -l            Format output in lmhosts format.
                     Cannot be used with -v, -s or -h options.
       -t timeout    wait timeout milliseconds for response.
                     Default 1000.
       -b bandwidth  Output throttling. Slow down output
                     so that it uses no more that bandwidth bps.
                     Useful on slow links, so that ougoing queries
                     don't get dropped.
       -r            use local port 137 for scans. Win95 boxes
                     respond to this only.
                     You need to be root to use this option on Unix.
       -q            Suppress banners and error messages,
       -s separator  Script-friendly output. Don't print
```

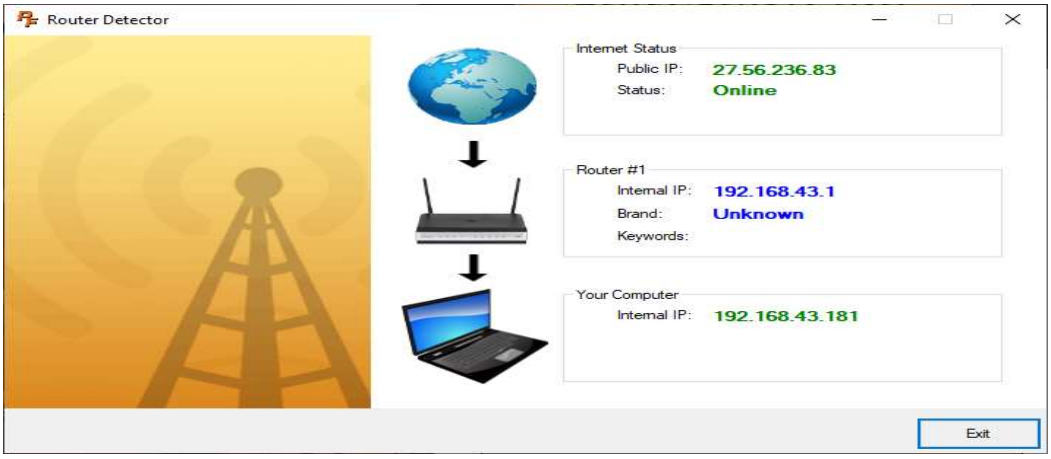
```
                    column and record headers, separate fields with
separator.
       -h           Print human-readable names for services.
                    Can only be used with -v option.
       -m retransmits       Number of retransmits. Default 0.
       -f filename  Take IP addresses to scan from file filename.
                    -f - makes nbtscan take IP addresses from stdin.
       <scan_range> what to scan. Can either be single IP
                    like 192.168.1.1 or
                    range of addresses in one of two forms:
                    xxx.xxx.xxx.xxx/xx or xxx.xxx.xxx.xxx-xxx.
Examples:
       nbtscan -r 192.168.1.0/24
              Scans the whole C-class network.
       nbtscan 192.168.1.25-137
              Scans a range from 192.168.1.25 to 192.168.1.137
       nbtscan -v -s : 192.168.1.0/24
              Scans C-class network. Prints results in script-friendly
              format using colon as field separator.
              Produces output like that:
              192.168.0.1:NT_SERVER:00U
              192.168.0.1:MY_DOMAIN:00G
              192.168.0.1:ADMINISTRATOR:03U
              192.168.0.2:OTHER_BOX:00U
              ...
       nbtscan -f iplist
              Scans IP addresses specified in file iplist.
```

2. **fPort : -**Most online port checks assume that you already have an application (such as your game or torrent) listening for the port test on your computer, and then assume that the test was OK simply because they were able to connect to your computer.

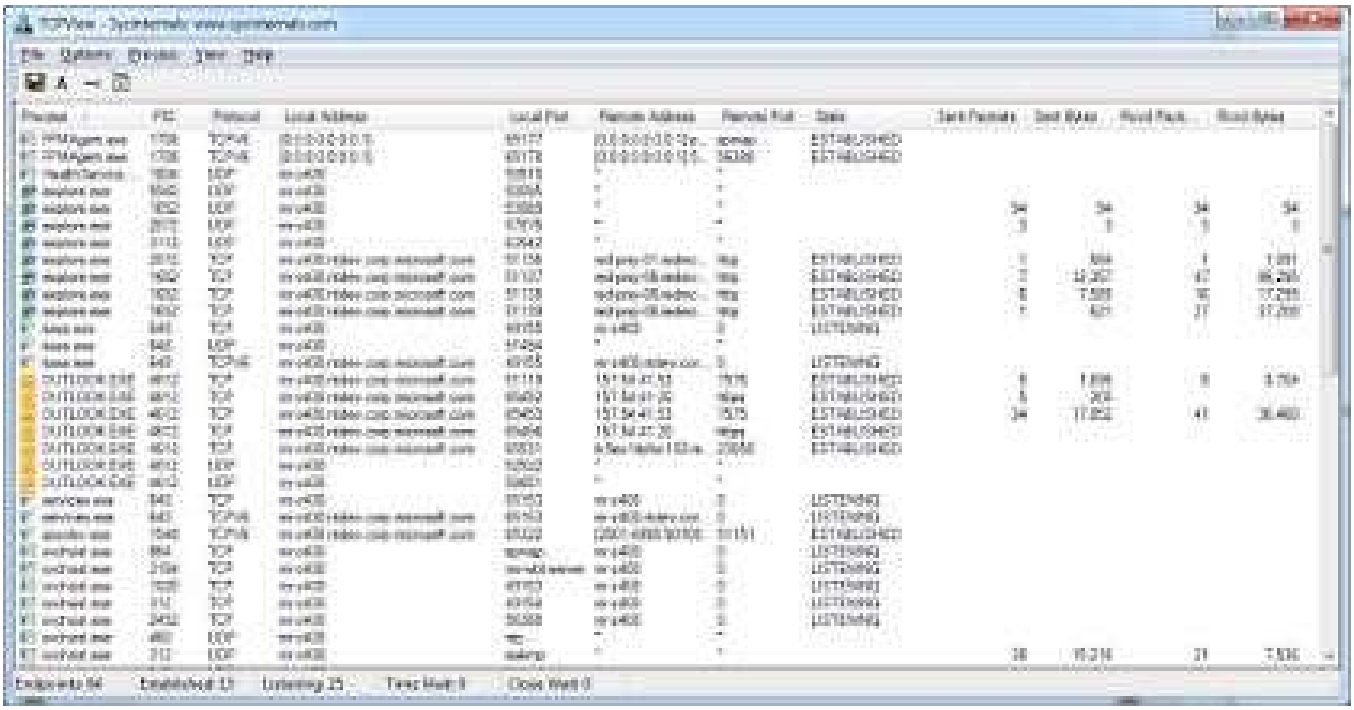
Also, web only port checkers are not able to test UDP since UDP is a connectionless protocol and there is no way to know if the packet actually made it to your computer without some sort of program on your computer waiting for that packet.

Our port test uses a local application to listen for the server trying to connect and then positively verifies that your port is forwarded.





3. **TCPView : -**TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality.

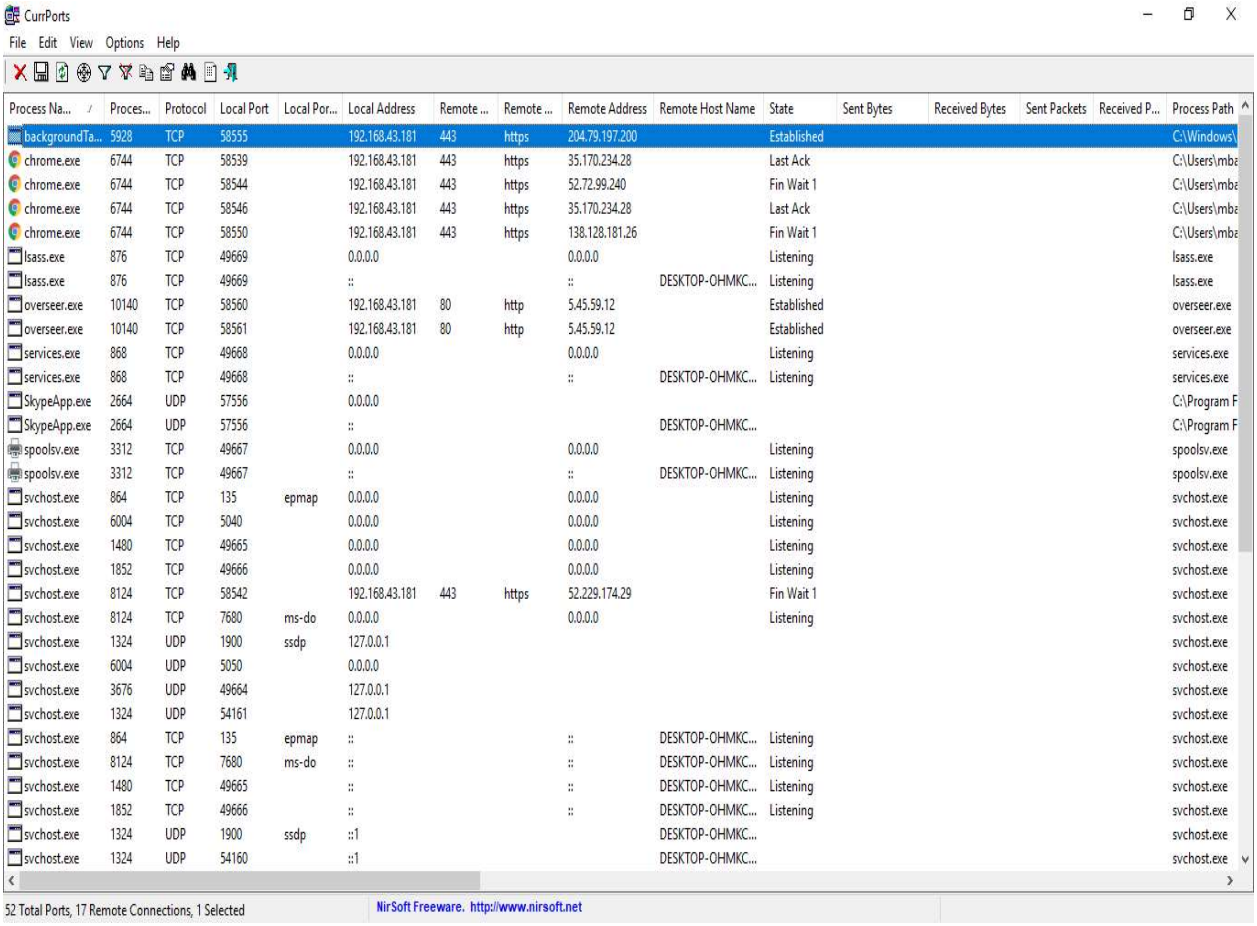


4. **CurrPorts Tool : -**CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer. For each port in the list,

information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, and so on), the time that the process was created, and the user that created it.

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP ports information to HTML file , XML file, or to tab-delimited text file.

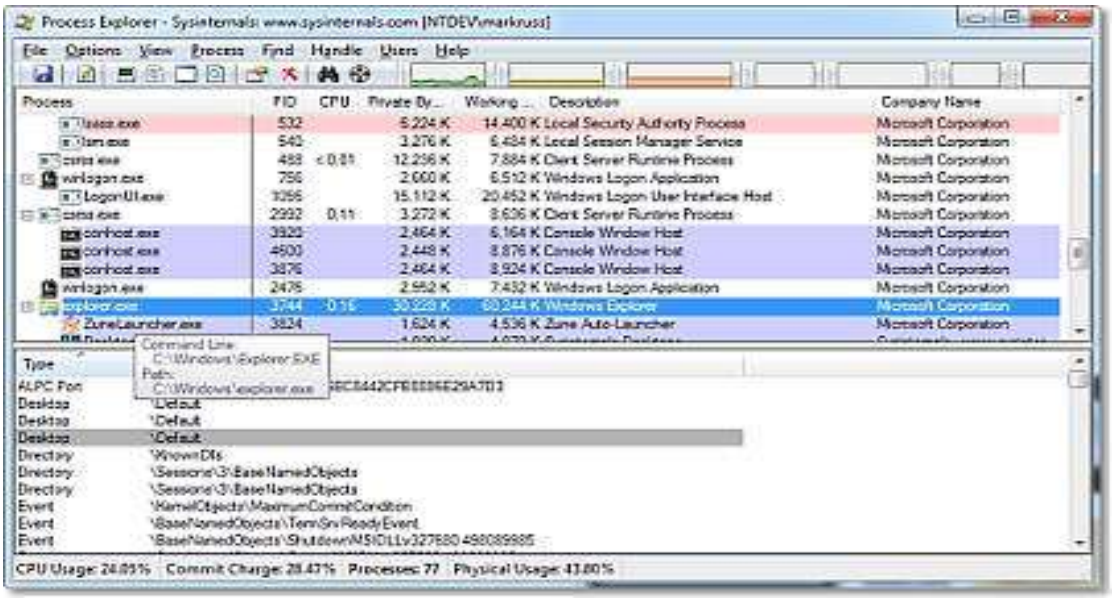
CurrPorts also automatically mark with pink color suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons)



Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	State	Sent Bytes	Received Bytes	Sent Packets	Received P...	Process Path
backgroundTa...	5928	TCP	58555		192.168.43.181	443	https	204.79.197.200		Established					C:\Windows\
chrome.exe	6744	TCP	58539		192.168.43.181	443	https	35.170.234.28		Last Ack					C:\Users\mba
chrome.exe	6744	TCP	58544		192.168.43.181	443	https	52.72.99.240		Fin Wait 1					C:\Users\mba
chrome.exe	6744	TCP	58546		192.168.43.181	443	https	35.170.234.28		Last Ack					C:\Users\mba
chrome.exe	6744	TCP	58550		192.168.43.181	443	https	138.128.181.26		Fin Wait 1					C:\Users\mba
lsass.exe	876	TCP	49669		0.0.0.0			0.0.0.0		Listening					lsass.exe
lsass.exe	876	TCP	49669		::			::	DESKTOP-OHMKC...	Listening					lsass.exe
overseer.exe	10140	TCP	58560		192.168.43.181	80	http	5.45.59.12		Established					overseer.exe
overseer.exe	10140	TCP	58561		192.168.43.181	80	http	5.45.59.12		Established					overseer.exe
services.exe	868	TCP	49668		0.0.0.0			0.0.0.0		Listening					services.exe
services.exe	868	TCP	49668		::			::	DESKTOP-OHMKC...	Listening					services.exe
SkypeApp.exe	2664	UDP	57556		0.0.0.0										C:\Program F
SkypeApp.exe	2664	UDP	57556		::				DESKTOP-OHMKC...						C:\Program F
spoolsv.exe	3312	TCP	49667		0.0.0.0			0.0.0.0		Listening					spoolsv.exe
spoolsv.exe	3312	TCP	49667		::			::	DESKTOP-OHMKC...	Listening					spoolsv.exe
svchost.exe	864	TCP	135	epmap	0.0.0.0			0.0.0.0		Listening					svchost.exe
svchost.exe	6004	TCP	5040		0.0.0.0			0.0.0.0		Listening					svchost.exe
svchost.exe	1480	TCP	49665		0.0.0.0			0.0.0.0		Listening					svchost.exe
svchost.exe	1852	TCP	49666		0.0.0.0			0.0.0.0		Listening					svchost.exe
svchost.exe	8124	TCP	58542		192.168.43.181	443	https	52.229.174.29		Fin Wait 1					svchost.exe
svchost.exe	8124	TCP	7680	ms-do	0.0.0.0			0.0.0.0		Listening					svchost.exe
svchost.exe	1324	UDP	1900	ssdp	127.0.0.1										svchost.exe
svchost.exe	6004	UDP	5050		0.0.0.0										svchost.exe
svchost.exe	3676	UDP	49664		127.0.0.1										svchost.exe
svchost.exe	1324	UDP	54161		127.0.0.1										svchost.exe
svchost.exe	864	TCP	135	epmap	::			::	DESKTOP-OHMKC...	Listening					svchost.exe
svchost.exe	8124	TCP	7680	ms-do	::			::	DESKTOP-OHMKC...	Listening					svchost.exe
svchost.exe	1480	TCP	49665		::			::	DESKTOP-OHMKC...	Listening					svchost.exe
svchost.exe	1852	TCP	49666		::			::	DESKTOP-OHMKC...	Listening					svchost.exe
svchost.exe	1324	UDP	1900	ssdp	::1				DESKTOP-OHMKC...						svchost.exe
svchost.exe	1324	UDP	54160		::1				DESKTOP-OHMKC...						svchost.exe

5. **Process Viewer : -**Ever wondered which program has a particular file or directory open? Now you can find out. *Process Explorer* shows you information about which handles and DLLs processes have opened or loaded.

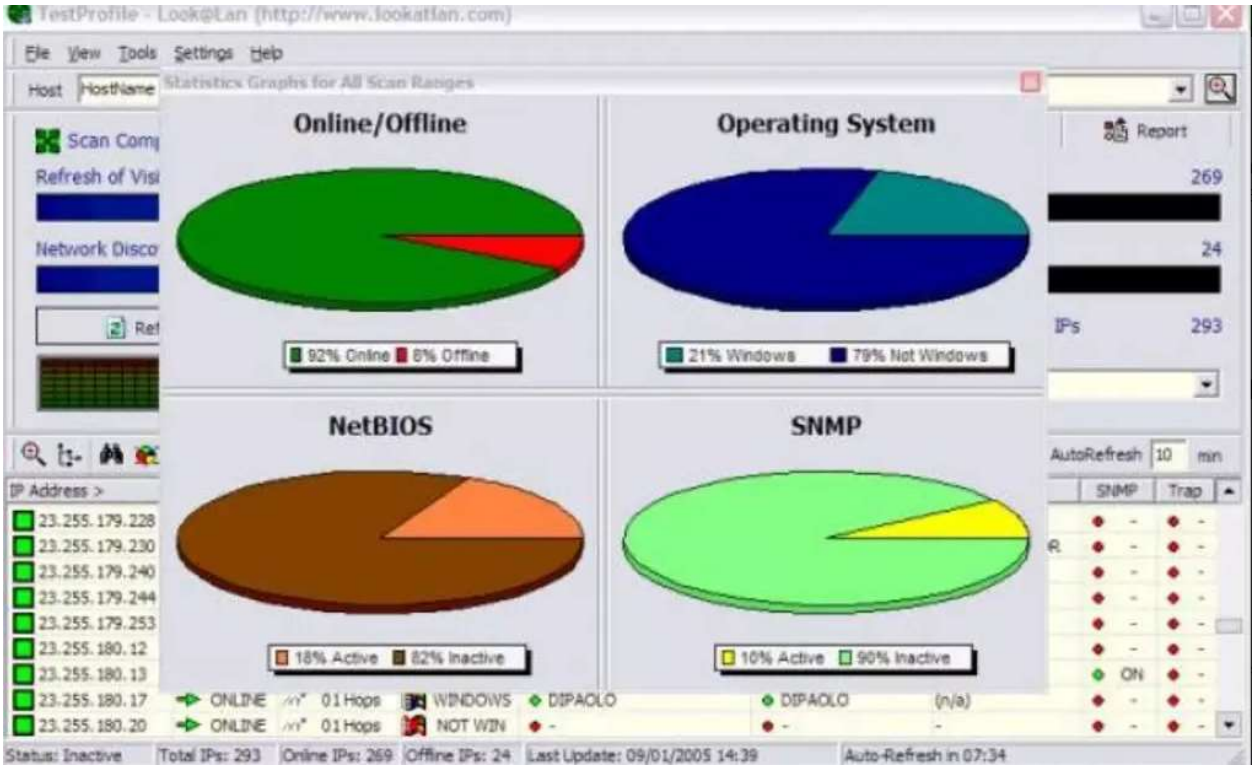
The unique capabilities of *Process Explorer* make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.



Experiment-8

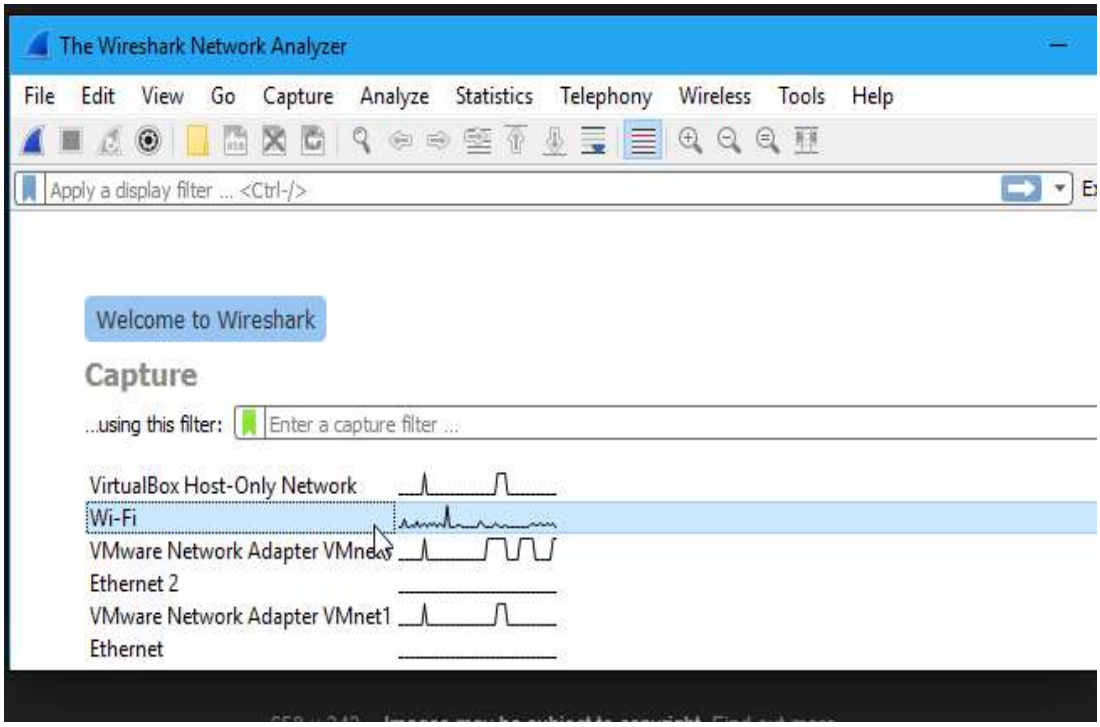
1 . Lan scanner using look@Lan : -Your network connection is probably one of the most vulnerable aspects in the digital work today. After all, if you have several computers all connected to the same network, you won't be able to keep track of what

each of them is exactly doing. They might be doing some incredibly dangerous and reckless processes, and they might damage your entire network and system. Thankfully, the days when users are unable to monitor the activity of their networks are over. Now, there are security software like **Look@LAN Network Monitoring** that users can use to **keep track of network activity**.



2 . WireShark : - It is developed and maintained by a global team of protocol experts, and it is an example of a disruptive technology.

Wireshark used to be known as Ethereal®. See the next question for details about the name change. If you're still using Ethereal, it is strongly recommended that you upgrade to Wireshark as Ethereal is unsupported and has known security vulnerabilities.



Experiment-9

Objective :Understanding DoS Attack Tools :

1. **Jolt2 : -**This program is the port of jolt2 attack to Windows XP for versions prior to SP2. Includes Delphi source code.

jolt2.exe <victim><spoof host> [options]

Options:

-P: Protocols to use. Either icmp, udp or both (default icmp)

-p: Dest port (default 7)

-n: Num of packets to send (0 is continuous (default))

-d: Delay (in ms) (default 0)

Example I: jolt2 217.155.32.170 40.41.42.43

On this attack:

- Victim: 217.155.32.170

- Source IP: 40.41.42.43

- Protocol: ICMP

- Destination Port: not used on icmp

- Count: Continuous

- Delay: 0 ms (no delay between packet

Bubonic:

It is a C program when compiled can be used against windows and Linux. Linux versions which were not updated since 2.0.3.0 kernel are vulnerable along with windows 2003 server

Land:
Land tool sends victim request by spoofing IP address of packet with IP address of victim. Since IP address of source and destination are same, system crashes as system starts flooding itself with packets.

LaTierra:
It also works as Land tool but it sends TCP packets to more than one port number.

Targa;
One of the most horrible DoS tool in list is Targa. Targa can launch DoS attack in all possible types of DoS attacks. Its efficiency increases exponentially with more number of PC's.

Blast:
Blast is TCP services stress test tool but can also be used for launching DoS attack against unprotected server.

Nemsey:
It is a program that generates random packets with random port number and IP address and floods victim with it.

Panther:
Its a packet flooding program that can overload a network connection with ICMP packets by sending fast ping requests causing a DoS attack.

Crazy Pinger:
It is also DoS tool of category flooder. It sends very large packets of ICMP to target.

FSMax:
It is a scrip-table server stress testing tool. This takes a text file as input and runs a server through a series of tests based on input. The purpose of this tool is to find buffer overflows of DoS points in a server.