TPCT's
College of Engineering, Osmanabad

Laboratory Manual

Computer system security & Laws

For

Fanal Year Students

Manual Prepared by

Mr.A.A.Nikam

Author COE, Osmanabad

TPCT's

College of Engineering
Solapur Road, Osmanabad
Department of Computer Science & Enggineering

Vision of the Department:

To achieve and evolve as a center of academic excellence and research center in the field of Computer Science and Engineering. To develop computer engineers with necessary analytical ability and human values who can creatively design, implement a wide spectrum of computer systems for welfare of the society.

Mission of the Department

The department strives to continuously engage in providing the students with in-depth understanding of fundamentals and practical training related to professional skills and their applications through effective Teaching- Learning Process and state of the art laboratories pertaining to CSE and inter disciplinary areas.Preparing students in developing research, design, entrepreneurial skills and employability capabilities.

College of Engineering

Technical Document

This technical document is a series of Laboratory manuals of Department of Computer Science & Engineering and is a certified document of College of Engineering, Osmanabad. The care has been taken to make the document error-free. But still if any error is found. Kindly bring it to the notice of subject teacher and HOD.

Recommended by,

HOD

Approved by,

Principal

Copies:

1. Departmental Library
2. Laboratory
3. HOD
4. Principal

FOREWORD

It is my great pleasure to present this laboratory manual for third year engineering

students for the subject of CSSL keeping in view the implementing advanced java concepts.

As a student, many of you may be wondering with some of the questions in your mind regarding the subject and exactly what has been tried is to answer through this manual.

Faculty members are also advised that covering these aspects in initial stage itself, will greatly relived them in future as much of the load will be taken care by the enthusiasm energies of the students once they are conceptually clear.

H.O.D.

LABORATORY MANUAL CONTENTS

This manual is intended for the final year students of engineering branches in the subject of CSSL. This manual typically contains practical/Lab Sessions related Signals and Systems covering various aspects related to the subject to enhance understanding.

Students are advised to thoroughly go through this manual rather than only topics mentioned in the syllabus as practical aspects are the key to understanding and conceptual visualization of theoretical aspects covered in the books.

Mr. A.A.Nikam

SUBJECT INDEX

1. DOs and DON' Ts in Laboratory:

1. Make entry in the Log Book as soon as you enter the Laboratory.

2. All the students should sit according to their roll numbers starting from their left to right.

3. All the students are supposed to enter the terminal number in the log book.

4. Do not change the terminal on which you are working.

5. All the students are expected to get at least the algorithm of the program/concept to be implemented.

6. Strictly observe the instructions given by the teacher/Lab Instructor.

Instruction for Laboratory Teachers::

- Submission related to whatever lab work has been completed should be done during the next lab session. The immediate arrangements for printouts related to submission on the day of practical assignments.
- Students should be taught for taking the printouts under the observation of lab teacher.
- The promptness of submission should be encouraged by way of marking and evaluation patterns that will benefit the sincere students.

.

2.Pre-Lab

Introduction to Computer system security & Laws

Questions:

1] What do you mean by Computer security?
2]What is Principle of Security?What is network security model?
3]Describe authentication & authorization?

1.Installation & Demonstration of N-Map tool

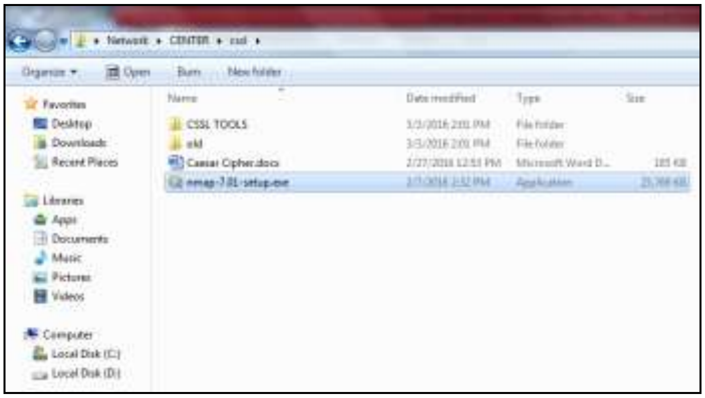
Aim-To install & demonstrate nmap tool.

Objective:Student will be able to install namap tool.

Tools required :N-Map software tool.

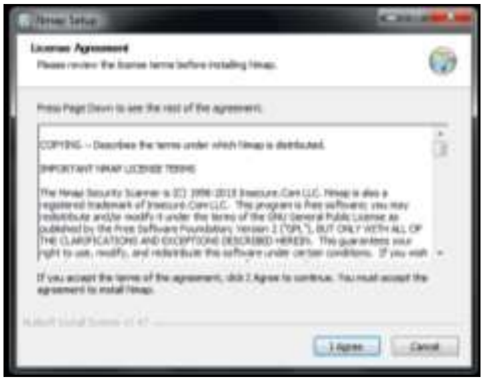
Theory: Zenmap is the official graphical user interface (GUI) for the Nmap Security Scanner. It is a multi-platform, free and open-source application designed to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users.

Steps to install:-
1.Select installation file and run it



Name	Date modified	Type	Size
CSSL TOOLS	3/1/2016 2:01 PM	File folder	
old	3/1/2016 2:01 PM	File folder	
Caesar Cipher.docx	2/27/2016 12:53 PM	Microsoft Word D...	185 KB
nmap-7.01-setup.exe	2/7/2016 2:32 PM	Application	25,768 KB

2.lisence agreement & Click on I agree



License Agreement

Please review the license terms before installing Nmap.

Press Page Down to see the rest of the agreement.

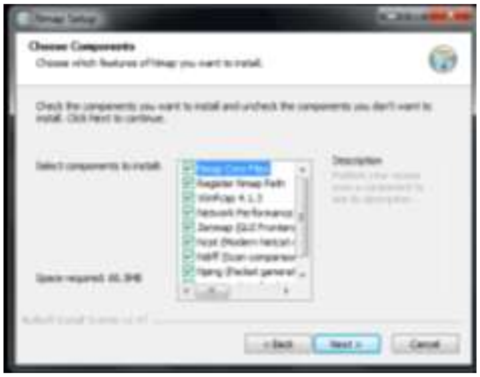
COPYING -- Describes the terms under which Nmap is distributed.

IMPORTANT NMAP LICENSE TERMS

The Nmap Security Scanner is (C) 1996-2015 Insecure.Com LLC. Nmap is also a registered trademark of Insecure.Com LLC. This program is free software; you may redistribute and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; Version 2 ("GPL"), BUT ONLY WITH ALL OF THE CLARIFICATIONS AND EXCEPTIONS DESCRIBED HEREIN. This guarantees your right to use, modify, and redistribute this software under certain conditions. If you wish

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.

3. Choose Component & Click Next Button



Choose Components

Choose which features of Nmap you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ Nmap Core Files
- ☑ Register Nmap Path
- ☑ WinPcap 4.1.3
- ☑ Network Performance
- ☑ Zenmap (GUI Frontend)
- ☑ Ncat (Modern Netcat
- ☑ Ndiff (Scan comparison
- ☑ Nping (Packet generation

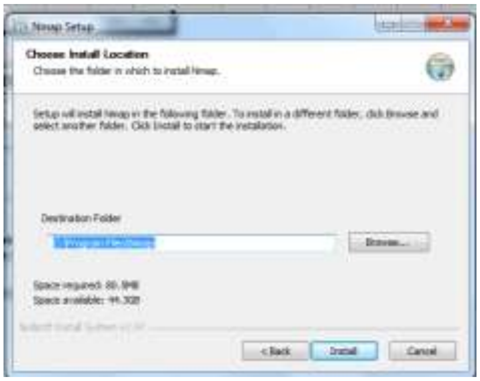
Description

Position your mouse over a component to see its description.

Space required: 80.3MB

Nullsoft Install System v2.47

4.Choose Install Location Click on Install Button



Choose Install Location

Choose the folder in which to install Nmap.

Setup will install Nmap in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

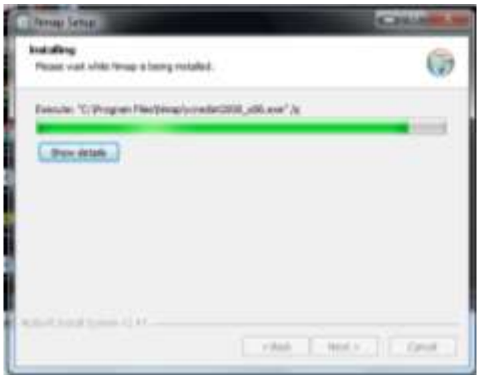
Destination Folder: C:\Program Files\Nmap

Space required: 80.3MB

Space available: 44.3GB

Nullsoft Install System v2.47

5.Installing



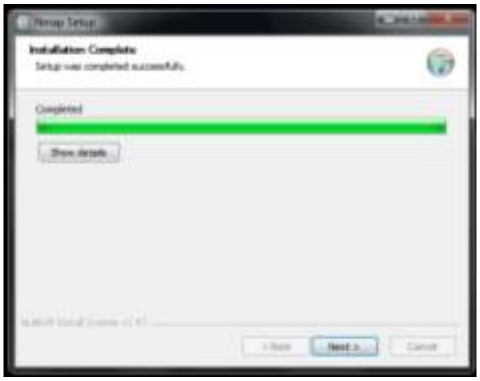
Installing

Please wait while Nmap is being installed.

Execute: "C:\Program Files\Nmap\vcredist2008_x86.exe" /q

Nullsoft Install System v2.47

6. Installation complete & Click on Next button



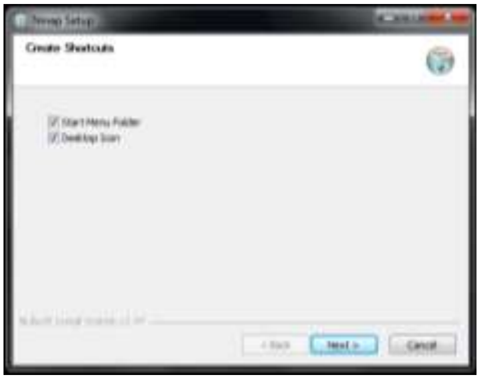
Installation Complete

Setup was completed successfully.

Completed

Nullsoft Install System v2.47

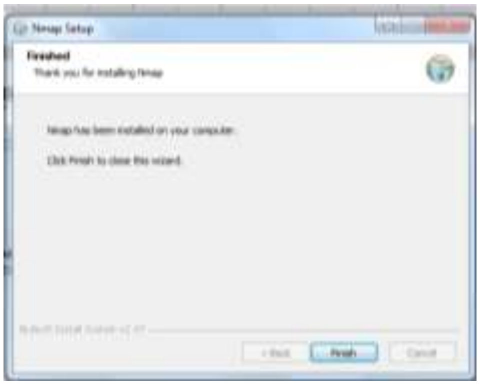
7.Create Shortcut & Click on Next Button



Create Shortcuts

☑ Start Menu Folder
☑ Desktop Icon

8.Finished& Click on Finish Button



Finished

Thank you for installing Nmap

Nmap has been installed on your computer.

Click Finish to close this wizard.

Conclusion:Hence we installed & demonstrate n-map tool.

2. **Perform an experiment to demonstrate use of nmap tool for Port Scanning.**

Aim-To perform n-map tool for port scanning.

Objective:-students will be able to perform port scanning using n-map tool.

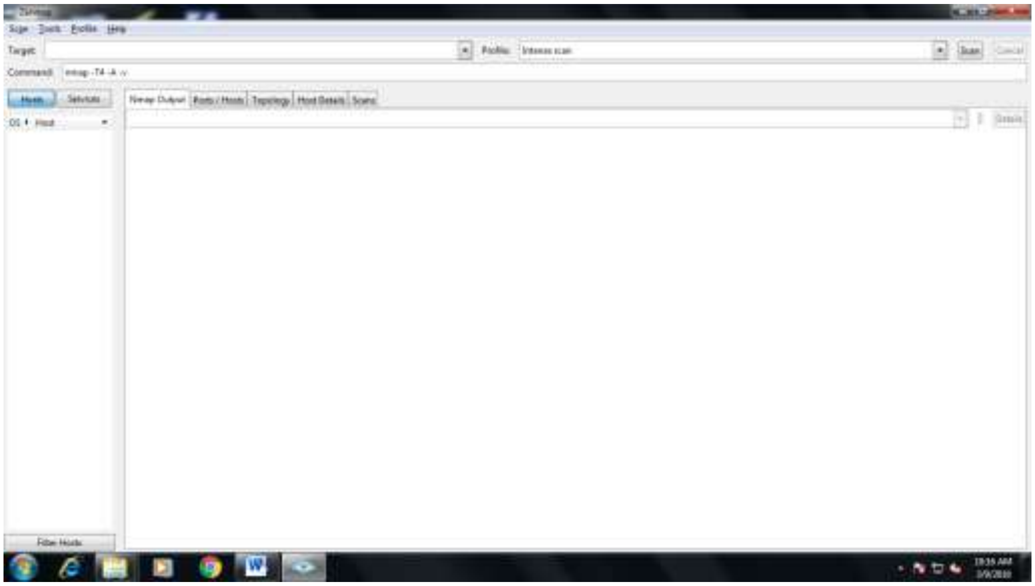
Tools required:-N-map software tool.

Theory:-

Zenmap is the official graphical user interface (GUI) for the Nmap Security Scanner. It is a multi-platform, free and open-source application designed to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scans can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

Scanning

Begin Zenmap by typing **zenmap** in a terminal or by clicking the Zenmap icon in the desktop environment



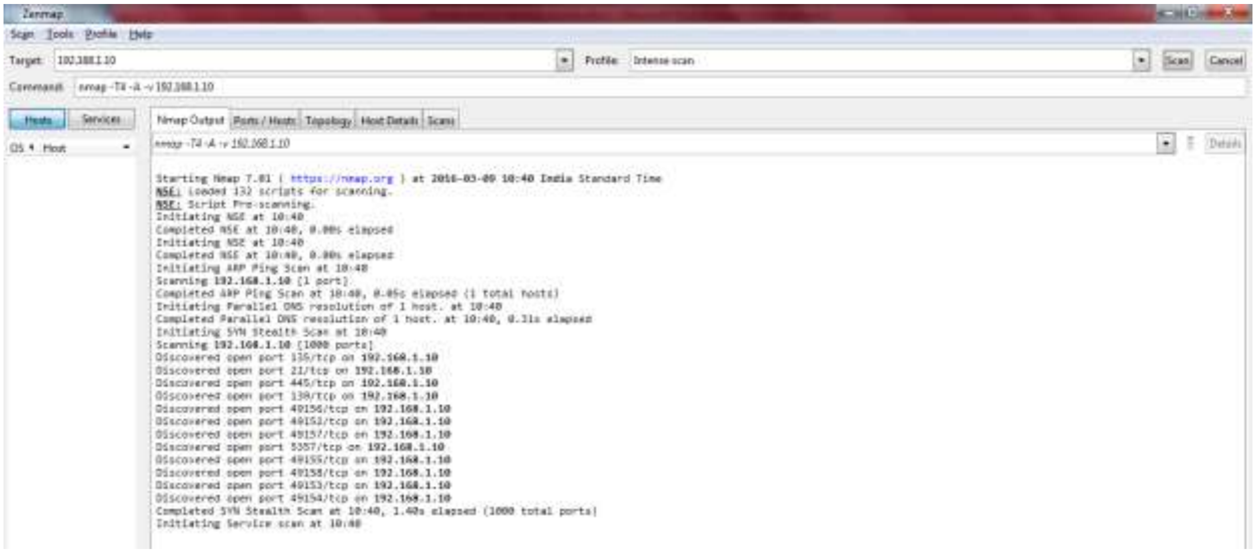
Target:

Profile: Intense scan

Command: nmap -T4 -A -v

In Target area write IP address or Web address & from Profile list choose proper scan type & Click on Scan

One of Zenmap's goals is to make security scanning easy for beginners and for experts. Running a scan is as simple as typing the target in the “Target” field, selecting the “Intense scan” profile, and clicking the “Scan” button.



Target: 192.168.1.10
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.10

```
nmap -T4 -A -v 192.168.1.10

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-09 10:40 India Standard Time
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:40
Completed NSE at 10:40, 0.00s elapsed
Initiating NSE at 10:40
Completed NSE at 10:40, 0.00s elapsed
Initiating ARP Ping Scan at 10:40
Scanning 192.168.1.10 [1 port]
Completed ARP Ping Scan at 10:40, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:40
Completed Parallel DNS resolution of 1 host. at 10:40, 0.31s elapsed
Initiating SYN Stealth Scan at 10:40
Scanning 192.168.1.10 [1000 ports]
Discovered open port 135/tcp on 192.168.1.10
Discovered open port 21/tcp on 192.168.1.10
Discovered open port 445/tcp on 192.168.1.10
Discovered open port 139/tcp on 192.168.1.10
Discovered open port 49156/tcp on 192.168.1.10
Discovered open port 49152/tcp on 192.168.1.10
Discovered open port 49157/tcp on 192.168.1.10
Discovered open port 5357/tcp on 192.168.1.10
Discovered open port 49155/tcp on 192.168.1.10
Discovered open port 49158/tcp on 192.168.1.10
Discovered open port 49153/tcp on 192.168.1.10
Discovered open port 49154/tcp on 192.168.1.10
Completed SYN Stealth Scan at 10:40, 1.40s elapsed (1000 total ports)
Initiating Service scan at 10:40
```

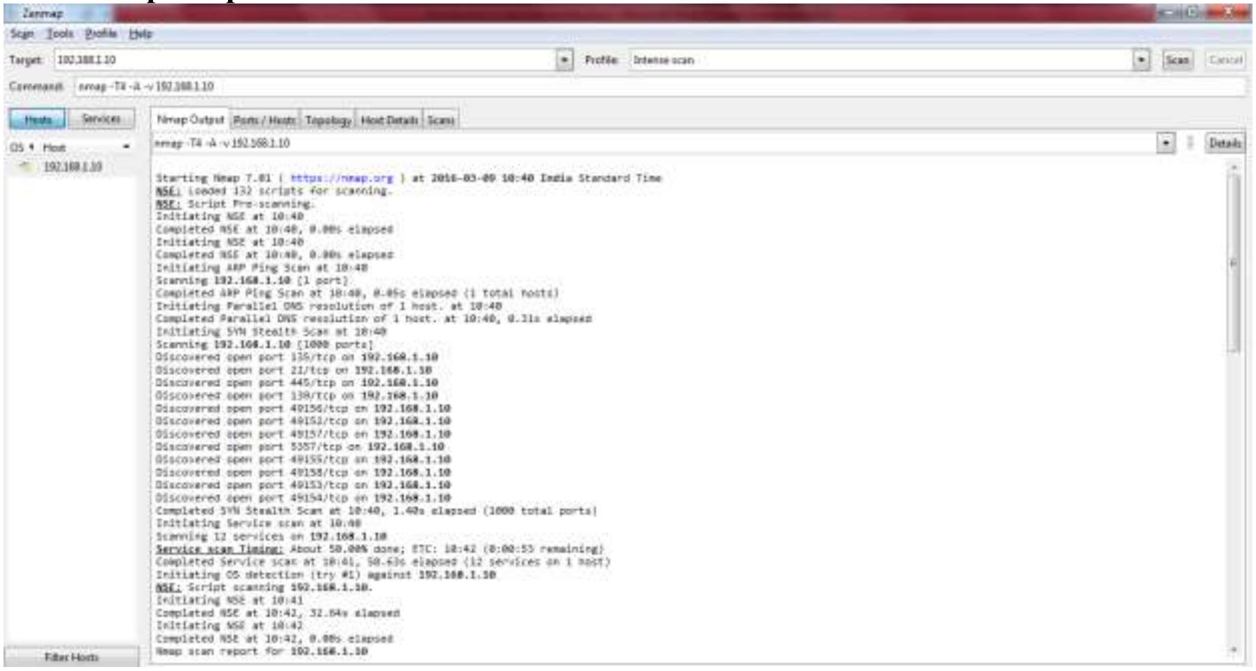
Interpreting Scan Results

Nmap's output is displayed during and after a scan. This output will be familiar to Nmap users. Except for Zenmap's color highlighting, this doesn't offer any visualization advantages over running Nmap in a terminal. However, other parts of Zenmap's interface interpret and aggregate the terminal output in a way that makes scan results easier to understand and use.

Scan Results Tabs

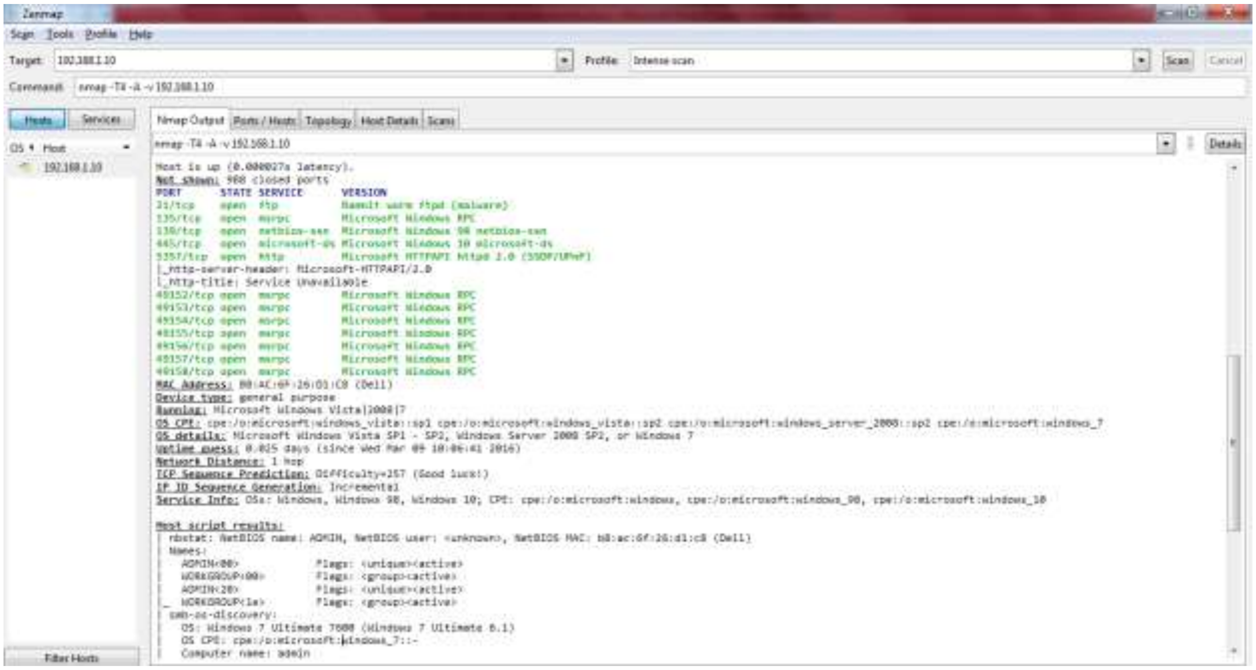
Each scan window contains five tabs which each display different aspects of the scan results. They are: “Nmap Output”, “Ports / Hosts”, “Topology”, “Host Details”, and “Scans”. Each of these are discussed in this section.

The “Nmap Output” tab



Target: 192.168.1.10
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.10

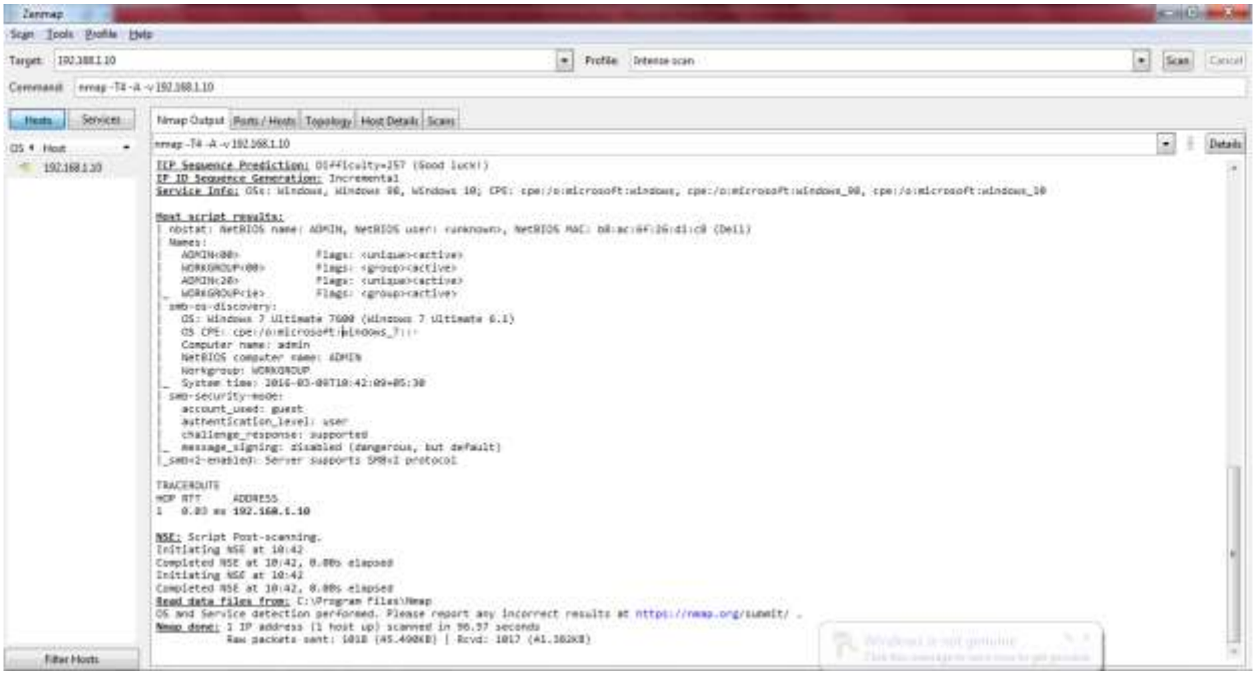
```
nmap -T4 -A -v 192.168.1.10

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-09 10:40 India Standard Time
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:40
Completed NSE at 10:40, 0.00s elapsed
Initiating NSE at 10:40
Completed NSE at 10:40, 0.00s elapsed
Initiating ARP Ping Scan at 10:40
Scanning 192.168.1.10 [1 port]
Completed ARP Ping Scan at 10:40, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:40
Completed Parallel DNS resolution of 1 host. at 10:40, 0.31s elapsed
Initiating SYN Stealth Scan at 10:40
Scanning 192.168.1.10 [1000 ports]
Discovered open port 135/tcp on 192.168.1.10
Discovered open port 21/tcp on 192.168.1.10
Discovered open port 445/tcp on 192.168.1.10
Discovered open port 139/tcp on 192.168.1.10
Discovered open port 49156/tcp on 192.168.1.10
Discovered open port 49152/tcp on 192.168.1.10
Discovered open port 49157/tcp on 192.168.1.10
Discovered open port 5357/tcp on 192.168.1.10
Discovered open port 49155/tcp on 192.168.1.10
Discovered open port 49158/tcp on 192.168.1.10
Discovered open port 49153/tcp on 192.168.1.10
Discovered open port 49154/tcp on 192.168.1.10
Completed SYN Stealth Scan at 10:40, 1.40s elapsed (1000 total ports)
Initiating Service scan at 10:40
Scanning 12 services on 192.168.1.10
Service scan Timing: About 50.00% done; ETC: 10:42 (0:00:53 remaining)
Completed Service scan at 10:41, 58.63s elapsed (12 services on 1 host)
Initiating OS detection (try #1) against 192.168.1.10
NSE: Script scanning 192.168.1.10.
Initiating NSE at 10:41
Completed NSE at 10:42, 32.84s elapsed
Initiating NSE at 10:42
Completed NSE at 10:42, 0.00s elapsed
Nmap scan report for 192.168.1.10
```



Target: 192.168.1.10
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.10
192.168.1.10

```
nmap -T4 -A -v 192.168.1.10
Host is up (0.000027s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Bamcit warm ftpd (malware)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows 98 netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 10 microsoft-ds
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: B8:AC:6F:26:D1:C8 (Dell)
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP1 - SP2, Windows Server 2008 SP2, or Windows 7
Uptime guess: 0.025 days (since Wed Mar 09 10:06:41 2016)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows 98, Windows 10; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_10

Host script results:
| nbstat: NetBIOS name: ADMIN, NetBIOS user: <unknown>, NetBIOS MAC: b8:ac:6f:26:d1:c8 (Dell)
| Names:
|   ADMIN<00>            Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   ADMIN<20>            Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7600 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
|   Computer name: admin
```

The “Nmap Output” tab is displayed by default when a scan is run. It shows the familiar Nmap terminal output. The display highlights parts of the output according to their meaning; for example, open and closed ports are displayed in different colors. Custom highlights can be configured in zenmap.conf (see the section called “Description of zenmap.conf”).



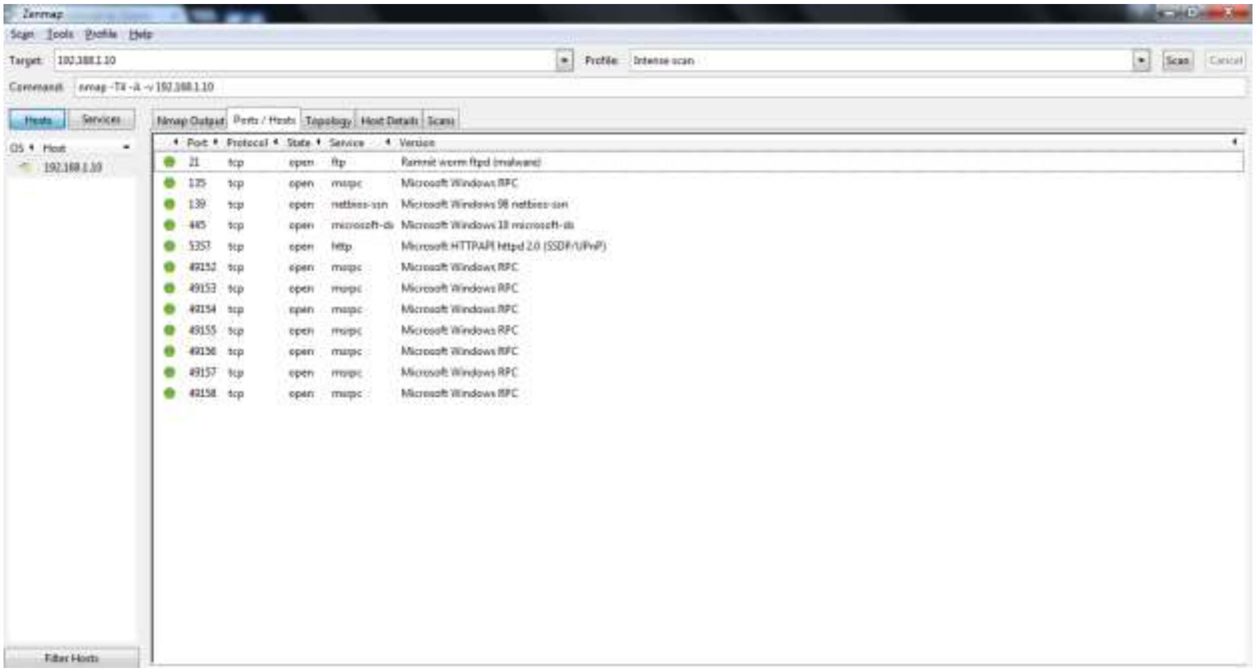
Target: 192.168.1.10
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.10
192.168.1.10

```
nmap -T4 -A -v 192.168.1.10
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows 98, Windows 10; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_10

Host script results:
| nbstat: NetBIOS name: ADMIN, NetBIOS user: <unknown>, NetBIOS MAC: b8:ac:6f:26:d1:c8 (Dell)
| Names:
|   ADMIN<00>            Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   ADMIN<20>            Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7600 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
|   Computer name: admin
|   NetBIOS computer name: ADMIN
|   Workgroup: WORKGROUP
|_  System time: 2016-03-09T10:42:09+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   0.03 ms 192.168.1.10

NSE: Script Post-scanning.
Initiating NSE at 10:42
Completed NSE at 10:42, 0.00s elapsed
Initiating NSE at 10:42
Completed NSE at 10:42, 0.00s elapsed
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 96.57 seconds
           Raw packets sent: 1018 (45.490KB) | Rcvd: 1017 (41.382KB)
```

Recall that the results of more than one scan may be shown in a window (see the section called “Scan Aggregation”). The drop-down combo box at the top of the tab allows you to select the scan to display. The “Details” button brings up a window showing miscellaneous information about the scan, such as timestamps, command-line options, and the Nmap version number used.

The “Ports / Hosts” tab

he “Ports / Hosts” tab's display differs depending on whether a host or a service is currently selected. When a host is selected, it shows all the interesting ports on that host, along with version information when available. Host selection is further described in the section called “Sorting by Host”.



Target: 192.168.1.10

Profile: Intense scan

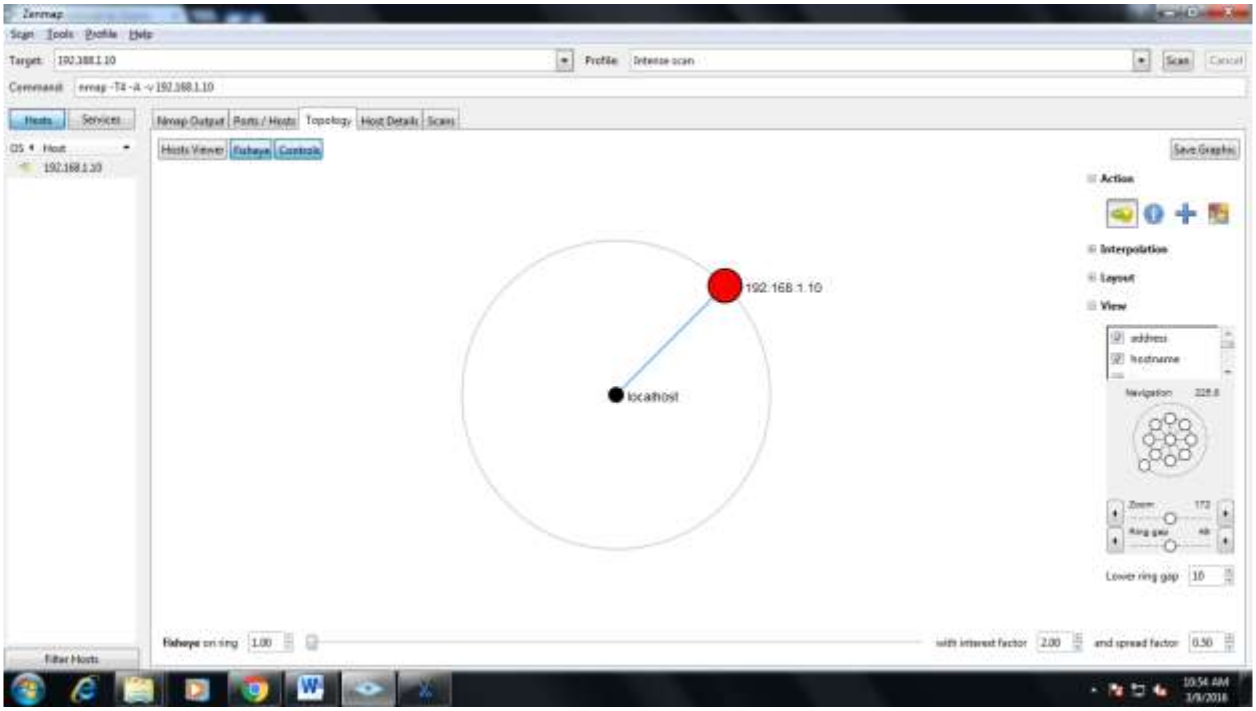
Command: nmap -T4 -A -v 192.168.1.10

	Port	Protocol	State	Service	Version
●	21	tcp	open	ftp	Ramnit worm ftpd (malware)
●	135	tcp	open	msrpc	Microsoft Windows RPC
●	139	tcp	open	netbios-ssn	Microsoft Windows 98 netbios-ssn
●	445	tcp	open	microsoft-ds	Microsoft Windows 10 microsoft-ds
●	5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
●	49152	tcp	open	msrpc	Microsoft Windows RPC
●	49153	tcp	open	msrpc	Microsoft Windows RPC
●	49154	tcp	open	msrpc	Microsoft Windows RPC
●	49155	tcp	open	msrpc	Microsoft Windows RPC
●	49156	tcp	open	msrpc	Microsoft Windows RPC
●	49157	tcp	open	msrpc	Microsoft Windows RPC
●	49158	tcp	open	msrpc	Microsoft Windows RPC

When a service is selected, the “Ports / Hosts” tab shows all the hosts which have that port open or filtered. This is a good way to quickly answer the question “What computers are running HTTP?” Service selection is further described in the section called “Sorting by Service”.

The “Topology” tab

The “Topology” tab is an interactive view of the connections between hosts in a network. Hosts are arranged in concentric rings. Each ring represents an additional network hop from the center node. Clicking on a node brings it to the center. Because it shows a representation of the network paths between hosts, the “Topology” tab benefits from the use of the --traceroute option. Topology view is discussed in more detail in the section called “Surfing the Network Topology”.



Target: 192.168.1.10

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.10

Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50

The "Host Details" tab

The "Host Details" tab breaks all the information about a single host into a hierarchical display. Shown are the host's names and addresses, its state (up or down), and the number and status of scanned ports. The host's uptime, operating system, OS icon (see Figure , "OS icons"), and other associated details are shown when available. When no exact OS match is found, the closest matches are displayed. There is also a collapsible text field for storing a comment about the host which will be saved when the scan is saved to a file (see the section called "Saving and Loading Scan Results").

Each host has an icon that provides a very rough "vulnerability" estimate, which is based solely on the number of open ports. The icons and the numbers of open ports they correspond to are

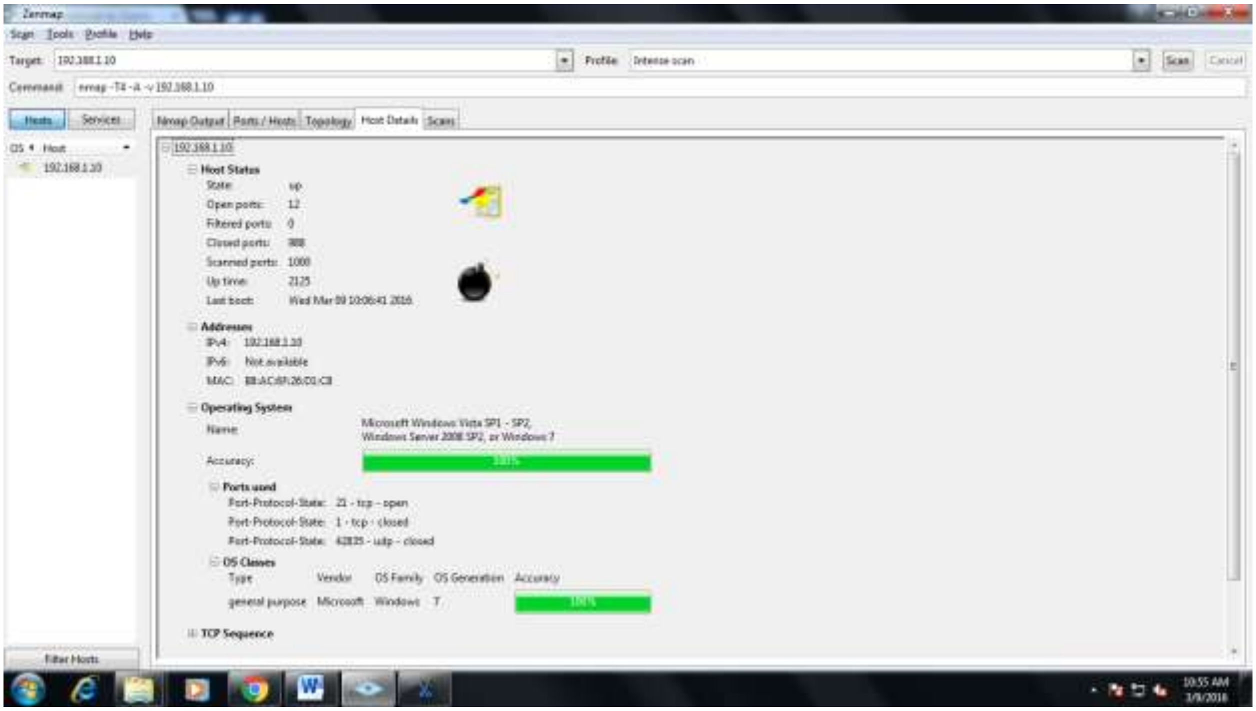
0–2 open ports,

3–4 open ports,

5–6 open ports,

7–8 open ports, and

9 or more open ports.



Target: 192.168.1.10
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.10

192.168.1.10

Host Status
State: up
Open ports: 12
Filtered ports: 0
Closed ports: 988
Scanned ports: 1000
Up time: 2125
Last boot: Wed Mar 09 10:06:41 2016

Addresses
IPv4: 192.168.1.10
IPv6: Not available
MAC: B8:AC:6F:26:D1:C8

Operating System
Name: Microsoft Windows Vista SP1 - SP2, Windows Server 2008 SP2, or Windows 7
Accuracy: 100%

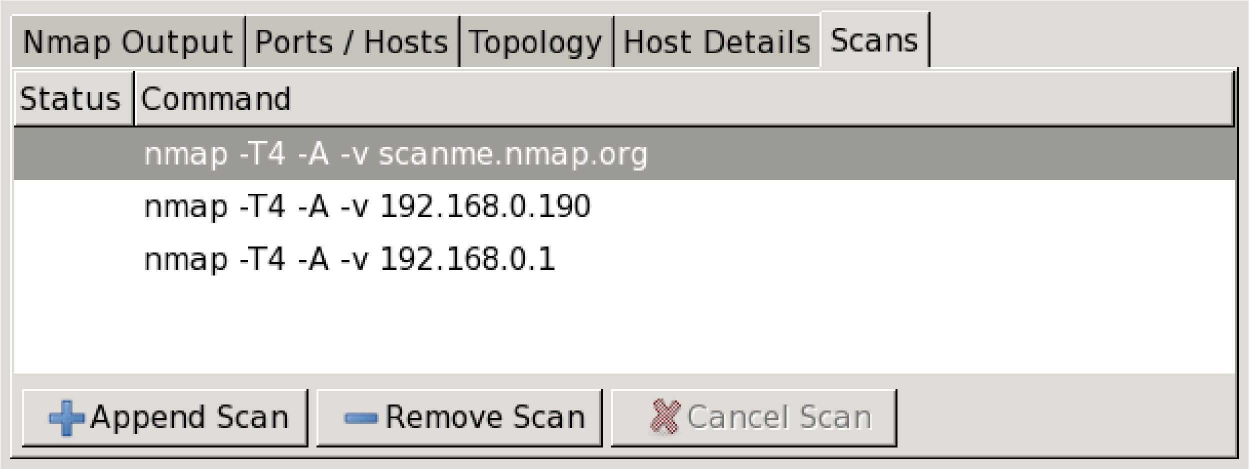
Ports used
Port-Protocol-State: 21 - tcp - open
Port-Protocol-State: 1 - tcp - closed
Port-Protocol-State: 42835 - udp - closed

OS Classes

Type	Vendor	OS Family	OS Generation	Accuracy
general purpose	Microsoft	Windows	7	100%

TCP Sequence

The “Scans” tab



Status	Command
	nmap -T4 -A -v scanme.nmap.org
	nmap -T4 -A -v 192.168.0.190
	nmap -T4 -A -v 192.168.0.1

The “Scans” tab shows all the scans that are aggregated to make up the network inventory. From this tab you can add scans (from a file or directory) and remove scans.

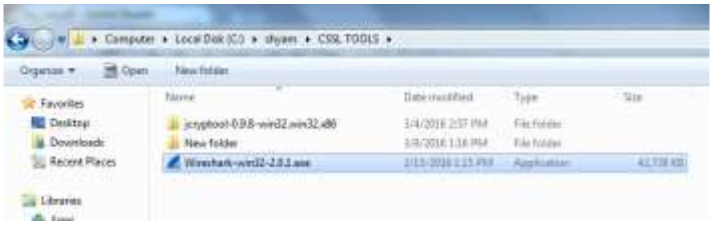
While a scan is executing and not yet complete, its status is “Running”. You may cancel a running scan by clicking the “Cancel Scan” button.

Conclusion :-Hence we perform port scanning using n-map tool.

3. Installation and demonstration of Wireshark Network Analyzer tool.

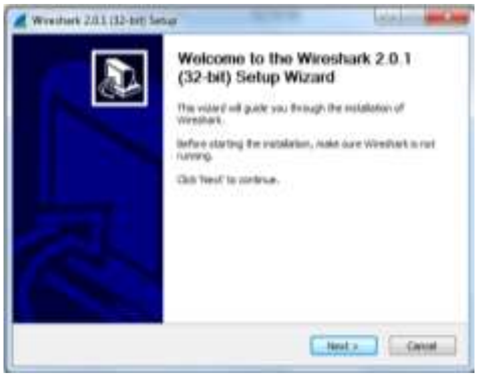
Aim:-To install & demonstrate wireshark network analyzer.
Objective:-Students will be able to install & demonstrate wireshark network analyzer
too.l.
Tools Required: Wireshark netwok analyzer software.
Theory:

1. Select & open Wireshark setup file.



Name	Date modified	Type	Size
jcryptool-0.9.8-win32.win32.x86	3/4/2016 2:57 PM	File folder	
New folder	3/9/2016 1:16 PM	File folder	
Wireshark-win32-2.0.1.exe	1/15/2016 1:15 PM	Application	42,728 KB

2. Wireshark Setup wizard Click on next button



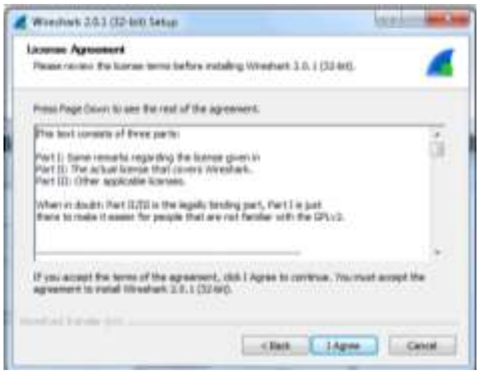
Welcome to the Wireshark 2.0.1 (32-bit) Setup Wizard

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

3. Liscence agrreement click on I Agree



License Agreement

Please review the license terms before installing Wireshark 2.0.1 (32-bit).

Press Page Down to see the rest of the agreement.

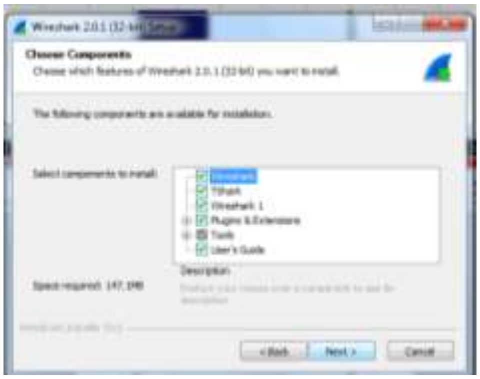
This text consists of three parts:

Part I: Some remarks regarding the license given in
Part II: The actual license that covers Wireshark.
Part III: Other applicable licenses.

When in doubt: Part II/III is the legally binding part, Part I is just there to make it easier for people that are not familiar with the GPLv2.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 2.0.1 (32-bit).

4. Choose Components & Click on Next button



Choose Components

Choose which features of Wireshark 2.0.1 (32-bit) you want to install.

The following components are available for installation.

Select components to install:

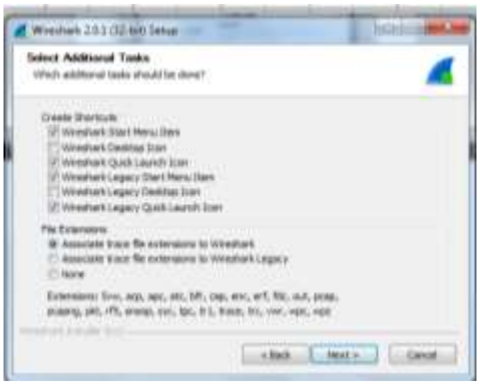
- ☑ Wireshark
- ☑ TShark
- ☑ Wireshark 1
- ☑ Plugins & Extensions
- ▣ Tools
- ☑ User's Guide

Description

Position your mouse over a component to see its description.

Space required: 147.1MB

5. Select Additional Task & Click on Next Button



Select Additional Tasks

Which additional tasks should be done?

Create Shortcuts

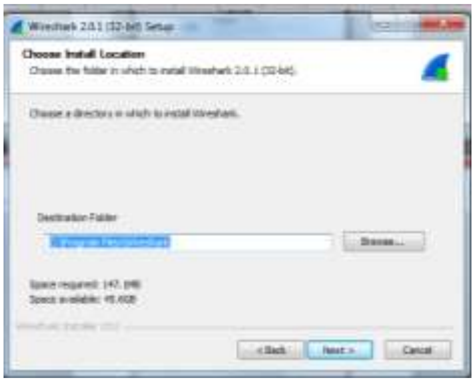
- ☑ Wireshark Start Menu Item
- ☐ Wireshark Desktop Icon
- ☑ Wireshark Quick Launch Icon
- ☑ Wireshark Legacy Start Menu Item
- ☐ Wireshark Legacy Desktop Icon
- ☑ Wireshark Legacy Quick Launch Icon

File Extensions

- ● Associate trace file extensions to Wireshark
- ○ Associate trace file extensions to Wireshark Legacy
- ○ None

Extensions: 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, out, pcap, pcapng, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz

6. Choose Install location



Choose Install Location

Choose the folder in which to install Wireshark 2.0.1 (32-bit).

Choose a directory in which to install Wireshark.

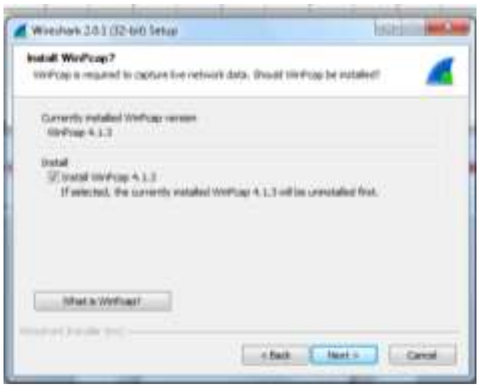
Destination Folder

C:\Program Files\Wireshark

Space required: 147.1MB

Space available: 45.6GB

7. Install Wincap& Click Next Button



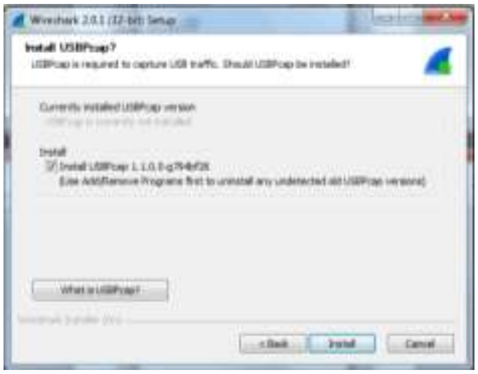
Install WinPcap?

WinPcap is required to capture live network data. Should WinPcap be installed?

Currently installed WinPcap version
WinPcap 4.1.3

Install
☑ Install WinPcap 4.1.3
If selected, the currently installed WinPcap 4.1.3 will be uninstalled first.

8. Install USB Pcap& Click Next Button



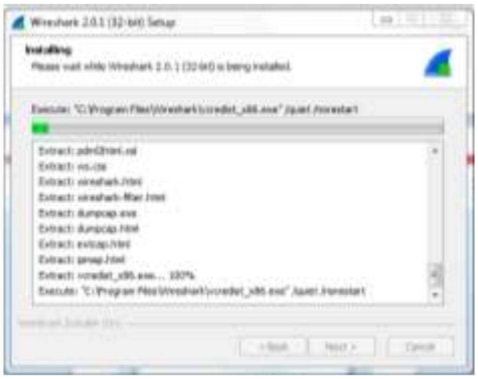
Install USBPcap?

USBPcap is required to capture USB traffic. Should USBPcap be installed?

Currently installed USBPcap version
USBPcap is currently not installed

Install
☑ Install USBPcap 1.1.0.0-g794bf26
(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)

9. Installing Wireshark



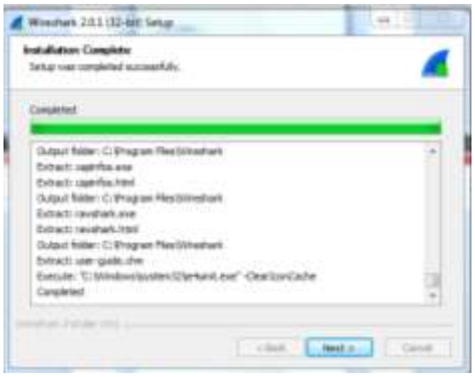
Installing

Please wait while Wireshark 2.0.1 (32-bit) is being installed.

```
Execute: "C:\Program Files\Wireshark\vcredist_x86.exe" /quiet /norestart
```

```
Extract: pdml2html.xsl
Extract: ws.css
Extract: wireshark.html
Extract: wireshark-filter.html
Extract: dumpcap.exe
Extract: dumpcap.html
Extract: extcap.html
Extract: ipmap.html
Extract: vcredist_x86.exe... 100%
Execute: "C:\Program Files\Wireshark\vcredist_x86.exe" /quiet /norestart
```

10.Insatallation Complete & Click on Next button



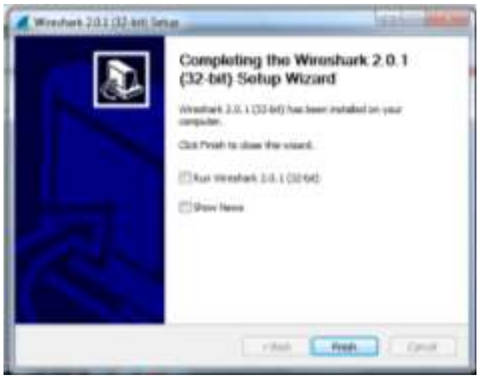
Installation Complete

Setup was completed successfully.

Completed

```
Output folder: C:\Program Files\Wireshark
Extract: capinfos.exe
Extract: capinfos.html
Output folder: C:\Program Files\Wireshark
Extract: rawshark.exe
Extract: rawshark.html
Output folder: C:\Program Files\Wireshark
Extract: user-guide.chm
Execute: "C:\Windows\system32\ie4uinit.exe" -ClearIconCache
Completed
```

11. Completing the Wireshark Setup wizard & Click on Finish



Completing the Wireshark 2.0.1 (32-bit) Setup Wizard

Wireshark 2.0.1 (32-bit) has been installed on your computer.

Click Finish to close the wizard.

□ Run Wireshark 2.0.1 (32-bit)

□ Show News

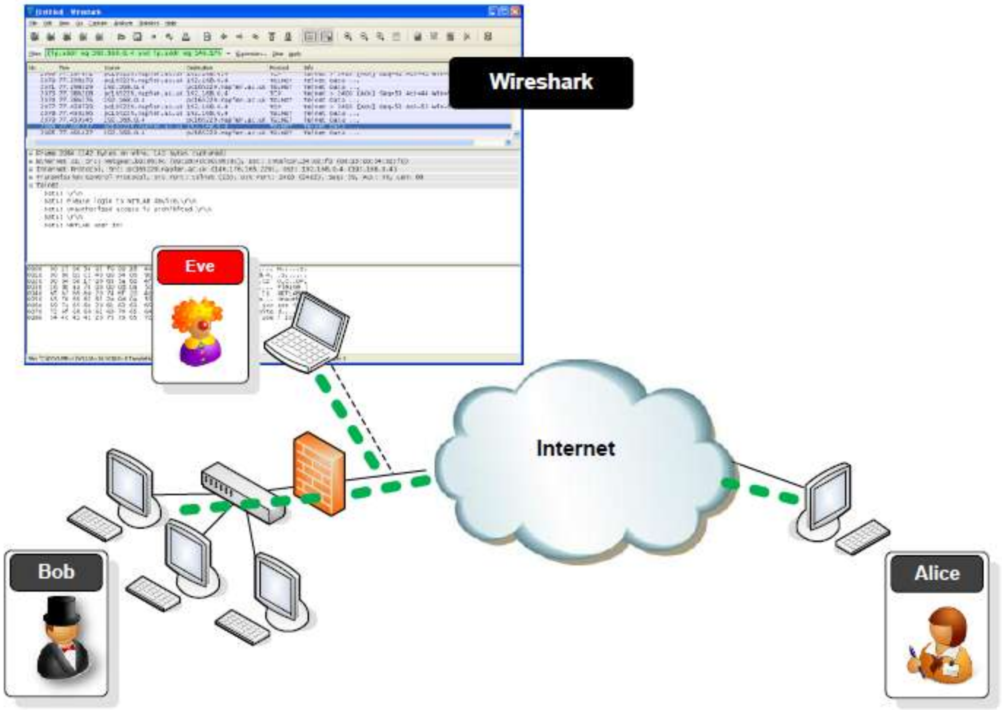
Conclusion: Hence we installed wireshark network analyzer.

4.Perform an experiment to demonstrate the use of Wireshark network analyzer to sniff for router traffic.

Aim:To perform sniff operation for router traffic using wireshark network analyzer.
Objective:students wiil able perform sniff operation for router traffic using wireshark network analyzer.
Tools Required: wireshark network analyzer software.
Theory:

Packet Capture (Packet Sniffing)

A **packet sniffer** is an application which can capture and analyse network traffic which is passing through a system’s Network Interface Card (NIC). The sniffer sets the card to **promiscuous mode** which means all traffic is read, whether it is addressed to that machine or not. The figure below shows an attacker sniffing packets from the network, and the **Wireshark**packet sniffer/analyser (formerly known as ethereal).

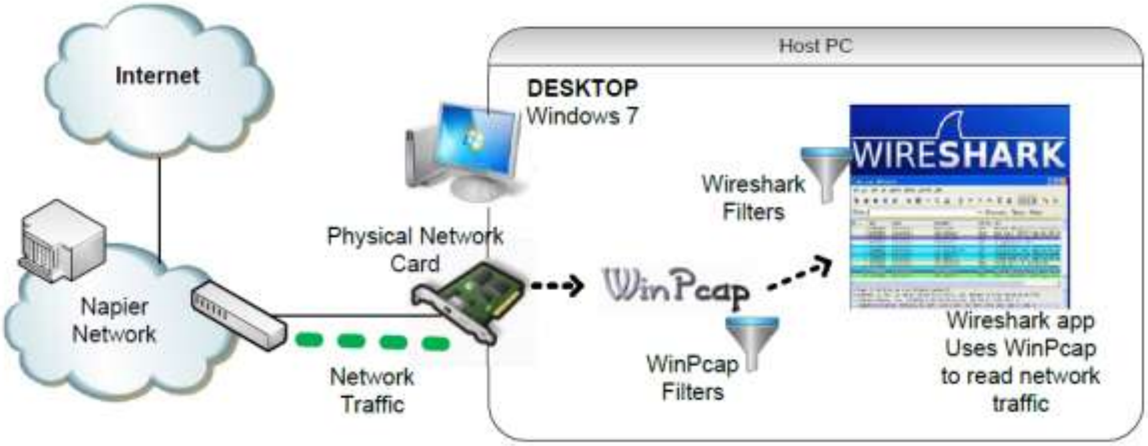


Packet Analysis

Wireshark is an open source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorising packet details based on protocol, as well as having functionality to filter and search the traffic, and pick out TCP streams. Wireshark can also save packet data to files for offline analysis and export/import packet captures to/from other tools. Statistics can also be generated for packet capture files.
Wireshark can be used for **network troubleshooting**, to **investigate security issues**, and to **analyse and understand network protocols**. The packet sniffer can exploit information passed in plaintext, i.e. not encrypted. Examples of **protocols** which pass information in plaintext are **Telnet, FTP, SNMP, POP, and HTTP**.

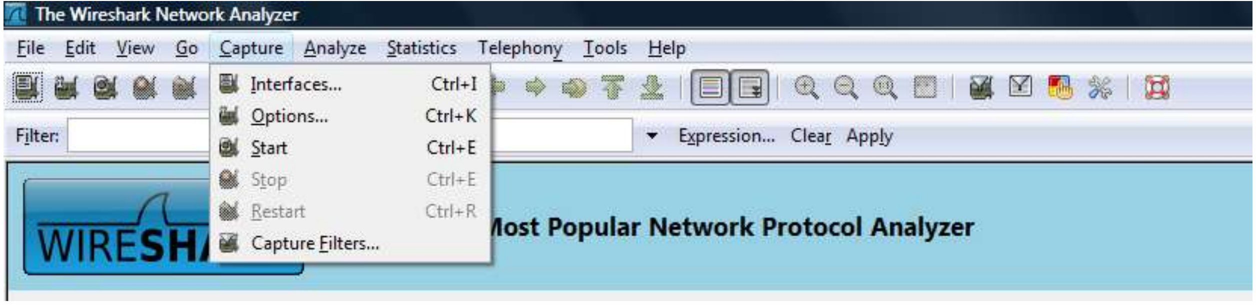
Wireshark is a GUI based network capture tool. There is a command line based version of the packet capture utility, called **TShark**. TShark provides many of the same features as it's big brother, but is console-based. It can be a good alternative if only command line access is available, and also uses less resources as it has no GUI to generate.

Using Wireshark to Capture Traffic

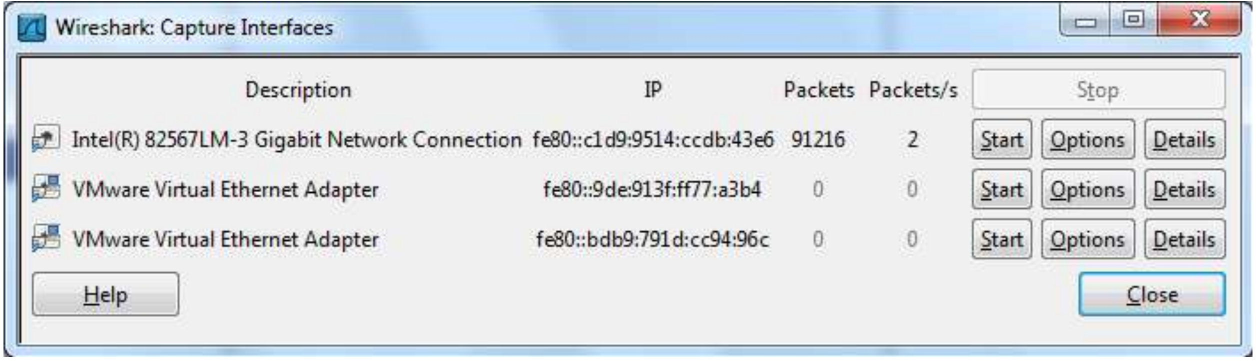


Select a Network Interface to Capture Packets through.

Start the Wireshark application. When Wireshark is first run, a default, or blank window is shown. To list the available network interfaces, select the **Capture->Interfaces** menu option.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Interfaces... Ctrl+I
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Filter:
Expression... Clear Apply
WIRESHA
Most Popular Network Protocol Analyzer

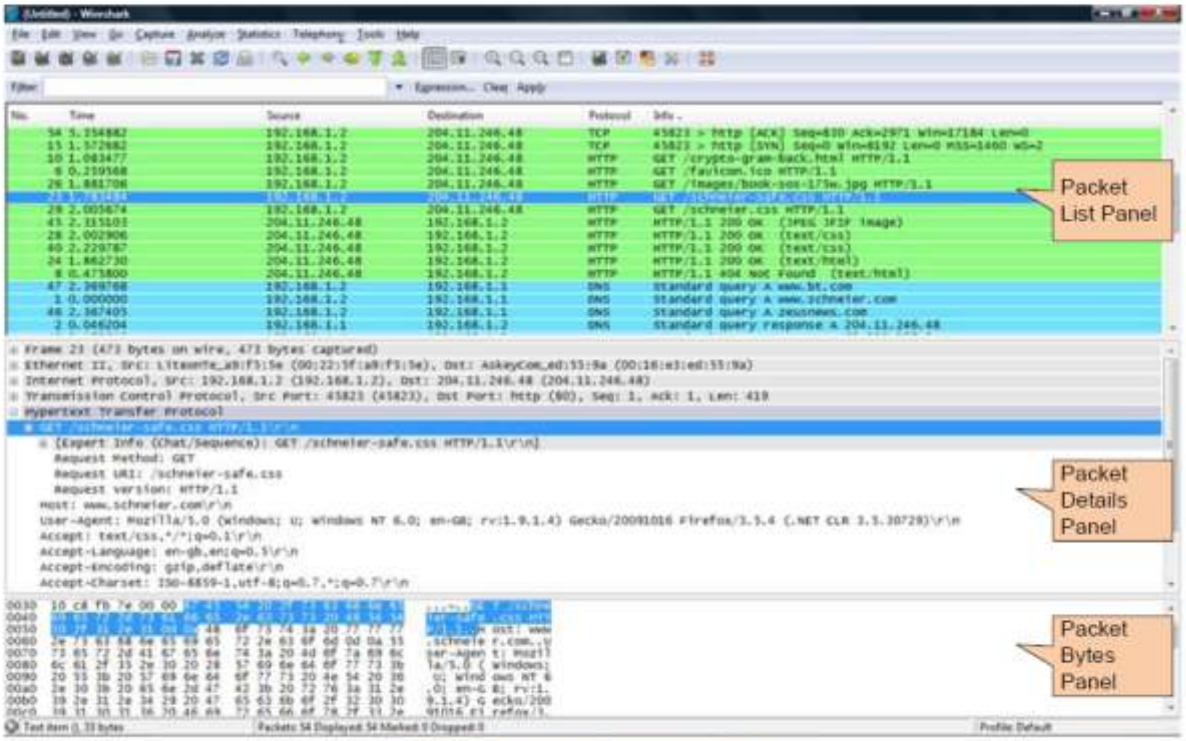
Wireshark should display a popup window such as the one shown in Figure 2. To capture network traffic click the **Start** button for the network interface you want to capture traffic on. Windows can have a long list of virtual interfaces, before the Ethernet Network Interface Card (NIC).


Wireshark: Capture Interfaces

Description	IP	Packets	Packets/s	Stop		
Intel(R) 82567LM-3 Gigabit Network Connection	fe80::c1d9:9514:ccdb:43e6	91216	2	Start	Options	Details
VMware Virtual Ethernet Adapter	fe80::9de:913f:ff77:a3b4	0	0	Start	Options	Details
VMware Virtual Ethernet Adapter	fe80::bdb9:791d:cc94:96c	0	0	Start	Options	Details

Figure 2 - Wireshark Interfaces Window

Generate some network traffic with a Web Browser, such as Internet Explorer or Chrome. Your Wireshark window should show the packets, and now look something like.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
Packet List Panel
Packet Details Panel
Packet Bytes Panel

```
No.  Time      Source         Destination    Protocol Info
  54 5.354882  192.168.1.2    204.11.246.48  TCP      45823 > http [ACK] Seq=830 Ack=2971 Win=17184 Len=0
  15 1.572682  192.168.1.2    204.11.246.48  TCP      45823 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
  10 1.083477  192.168.1.2    204.11.246.48  HTTP     GET /crypto-gram-back.html HTTP/1.1
   6 0.219568  192.168.1.2    204.11.246.48  HTTP     GET /favicon.ico HTTP/1.1
  26 1.881706  192.168.1.2    204.11.246.48  HTTP     GET /images/book-sos-175w.jpg HTTP/1.1
  23 [illegible] 192.168.1.2  204.11.246.48  HTTP     GET /schneier-safe.css HTTP/1.1
  29 2.005674  192.168.1.2    204.11.246.48  HTTP     GET /schneier.css HTTP/1.1
  45 2.315103  204.11.246.48  192.168.1.2    HTTP     HTTP/1.1 200 OK  (JPEG JFIF image)
  28 2.002906  204.11.246.48  192.168.1.2    HTTP     HTTP/1.1 200 OK  (text/css)
  40 2.229787  204.11.246.48  192.168.1.2    HTTP     HTTP/1.1 200 OK  (text/css)
  24 1.862730  204.11.246.48  192.168.1.2    HTTP     HTTP/1.1 200 OK  (text/html)
   8 0.473800  204.11.246.48  192.168.1.2    HTTP     HTTP/1.1 404 Not Found  (text/html)
  47 2.369768  192.168.1.2    192.168.1.1    DNS      Standard query A www.bt.com
   1 0.000000  192.168.1.2    192.168.1.1    DNS      Standard query A www.schneier.com
  48 2.367405  192.168.1.2    192.168.1.1    DNS      Standard query A zeusnews.com
   2 0.046204  192.168.1.1    192.168.1.2    DNS      Standard query response A 204.11.246.48
```

```
⊞ Frame 23 (473 bytes on wire, 473 bytes captured)
⊞ Ethernet II, Src: LiteonTe_a8:f5:5e (00:22:5f:a8:f5:5e), Dst: AskeyCom_ed:55:9a (00:16:e3:ed:55:9a)
⊞ Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 204.11.246.48 (204.11.246.48)
⊞ Transmission Control Protocol, Src Port: 45823 (45823), Dst Port: http (80), Seq: 1, Ack: 1, Len: 419
⊟ Hypertext Transfer Protocol
  ⊟ GET /schneier-safe.css HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET /schneier-safe.css HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /schneier-safe.css
      Request Version: HTTP/1.1
    Host: www.schneier.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-GB; rv:1.9.1.4) Gecko/20091016 Firefox/3.5.4 (.NET CLR 3.5.30729)\r\n
    Accept: text/css,*/*;q=0.1\r\n
    Accept-Language: en-gb,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
```

```
0030  10 c8 fb 7e 00 00 [illegible]
0040  [illegible]                                          ter-safe .css HTT
0050  [illegible]          48 6f 73 74 3a 20 77 77 77      P/1.1..H ost: www
0060  2e 73 63 68 6e 65 69 65  72 2e 63 6f 6d 0d 0a 55   .schneie r.com..U
0070  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Agen t: Mozil
0080  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 3b   la/5.0 ( Windows;
0090  20 55 3b 20 57 69 6e 64  6f 77 73 20 4e 54 20 36    U; Wind ows NT 6
00a0  2e 30 3b 20 65 6e 2d 47  42 3b 20 72 76 3a 31 2e   .0; en-G B; rv:1.
00b0  39 2e 31 2e 34 29 20 47  65 63 6b 6f 2f 32 30 30   9.1.4) G ecko/200
00c0  39 31 30 31 36 20 46 69  72 65 66 6f 78 2f 33 2e   91016 Fi refox/3.
```

Text item (), 33 bytes   Packets: 54 Displayed: 54 Marked: 0 Dropped: 0   Profile: Default

Figure 3 - Wireshark capuring traffic

To stop the capture, select the **Capture->Stop** menu option, Ctrl+E, or the Stop toolbar button. What you have created is a Packet Capture or ***'pcap'***, which you can now view and analyse using the Wireshark interface, or save to disk to analyse later.

The capture is split into 3 parts:

1. **Packet List Panel –** this is a list of packets in the current capture. It colours the packets based on the protocol type. When a packet is selected, the details are shown in the two panels below.
2. **Packet Details Panel –** this shows the details of the selected packet. It shows the different protocols making up the layers of data for this packet. Layers include Frame, Ethernet, IP, TCP/UDP/ICMP, and application protocols such as HTTP.
3. **Packet Bytes Panel –** shows the packet bytes in Hex and ASCII encodings.

To select more detailed options when starting a capture, select the **Capture->Options** menu option, or **Ctrl+K**, or the Capture Options button on the toolbar (the wrench). This should show a window such as shown in Figure 4.

Some of the more interesting options are:

 Capture Options > Interface - Again the important thing is to select the correct Network Interface to capture traffic through.

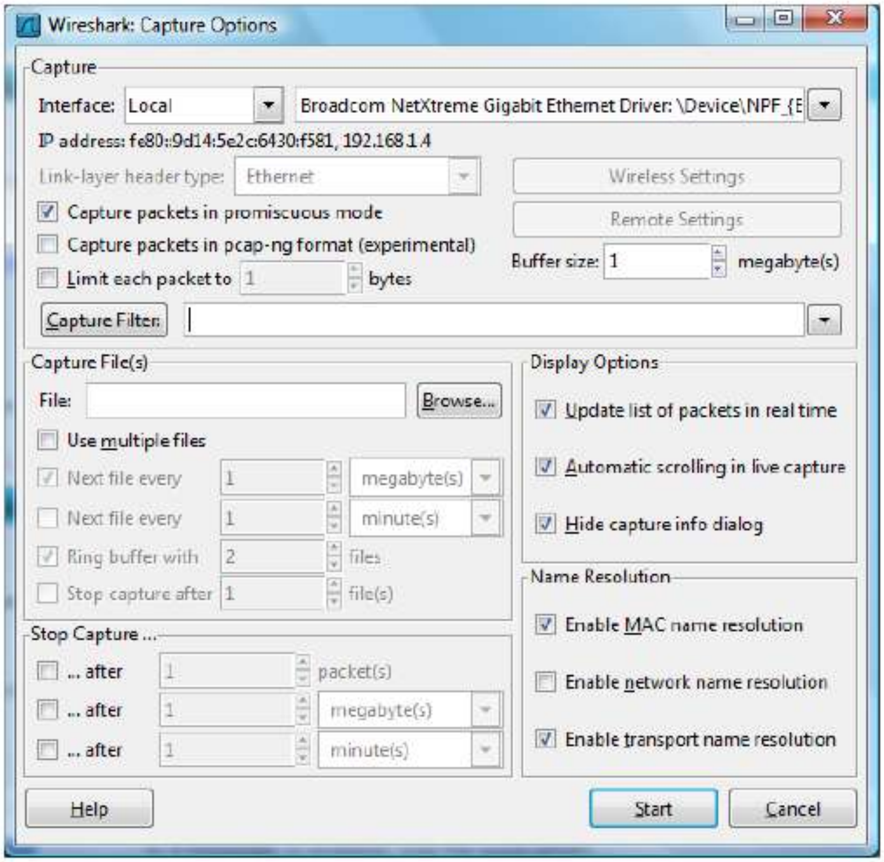
 Capture Options > Capture File – useful to save a file of the packet capture in real time, in case of a system crash.

 Display Options > Update list of packets in real time – A display option, which should be checked if you want to view the capture as it happens (typically switched off to capture straight to a file, for later analysis).

□ ***Name Resolution > MAC name resolution*** – resolves the first 3 bytes of the MAC Address, the Organisation Unique Identifier (OUI), which represents the Manufacturer of the Card.

□ ***Name Resolution > Network name resolution*** – does a DNS lookup for the IP Addresses captured, to display the network name. Set to off by default, so covert scans do not generate this DNS traffic, and tip off who's packets you are sniffing.

Make sure the **MAC name resolution** is selected. Start the capture, and generate some Web traffic again, then stop the capture.



Wireshark: Capture Options

Capture

Interface: Local ▾ Broadcom NetXtreme Gigabit Ethernet Driver: \Device\NPF_{E ▾

IP address: fe80::9d14:5e2c:6430:f581, 192.168.1.4

Link-layer header type: Ethernet ▾

☑ Capture packets in promiscuous mode

☐ Capture packets in pcap-ng format (experimental)

☐ Limit each packet to 1 bytes

Buffer size: 1 megabyte(s)

Capture Filter:

Capture File(s)

File:

☐ Use multiple files

☑ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☑ Ring buffer with 2 files

☐ Stop capture after 1 file(s)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

☐ Enable network name resolution

☑ Enable transport name resolution

Figure 4 - Wireshark Capture Options

Conclusion:-Hence we performed sniff operation for router traffic using wireshark network analyzer

5. Installation and demonstration of Jcrypt tool.

Aim:-To install & demonstrate Jcrypt Tool .

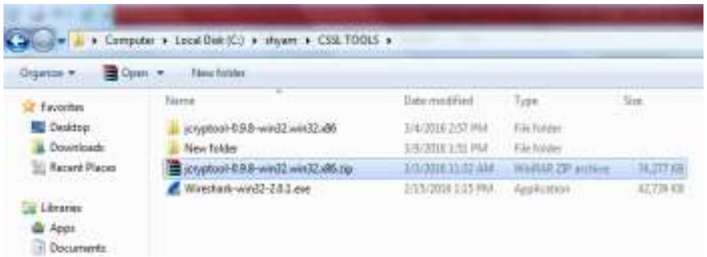
Objective:-Students wiil able to install & demonstrate Jcrypt tool.

Tools Required:Jcrypt tool software.

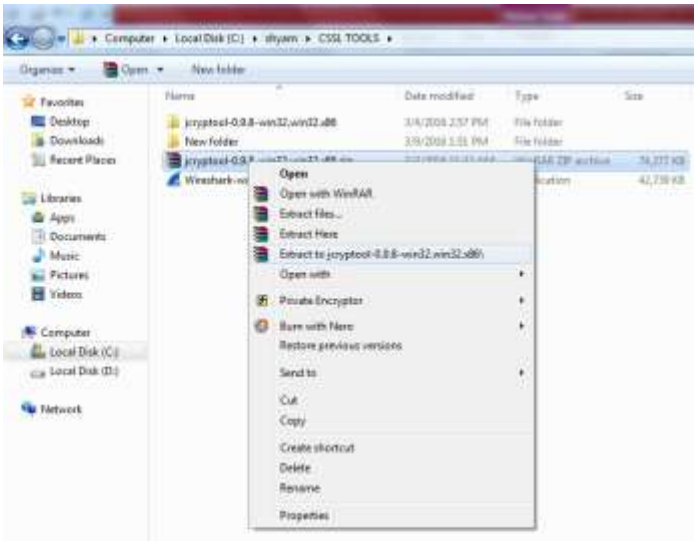
Theory:

Steps to install:

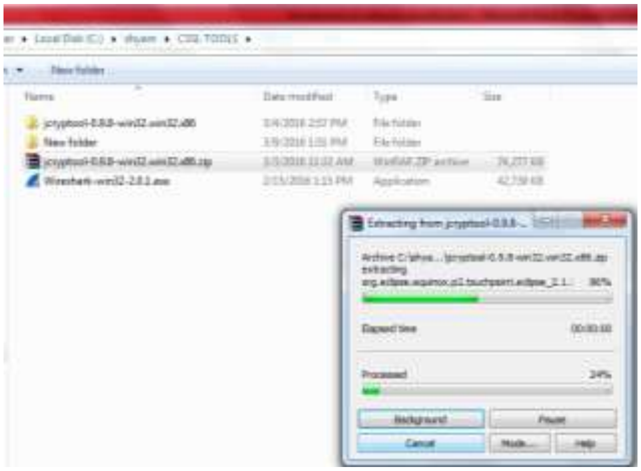
1. Select Jcrypt zip file to extract



2. Right Click & select Extract to Jcryptool



3. Extracting from Jcryptool zip file



Name	Date modified	Type	Size
jcryptool-0.9.8-win32.win32.x86	3/4/2016 2:57 PM	File folder	
New folder	3/9/2016 1:55 PM	File folder	
jcryptool-0.9.8-win32.win32.x86.zip	3/3/2016 11:32 AM	WinRAR ZIP archive	74,277 KB
Wireshark-win32-2.0.1.exe	2/15/2016 1:15 PM	Application	42,739 KB

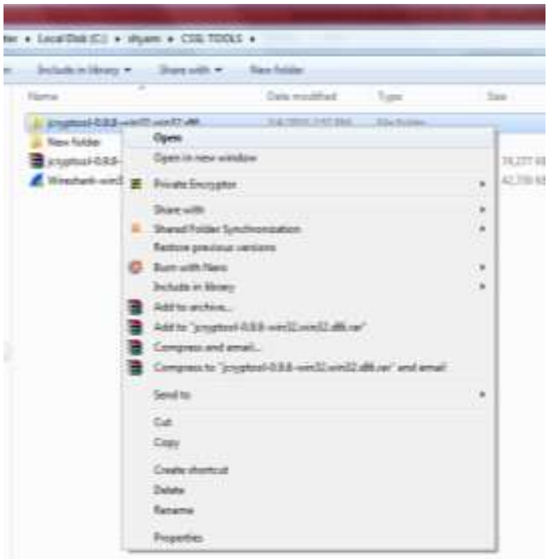
Extracting from jcryptool-0.9.8-...

Archive C:\phos...\jcryptool-0.9.8-win32.win32.x86.zip
extracting
org.eclipse.equinox.p2.touchpoint.eclipse_2.1... 86%

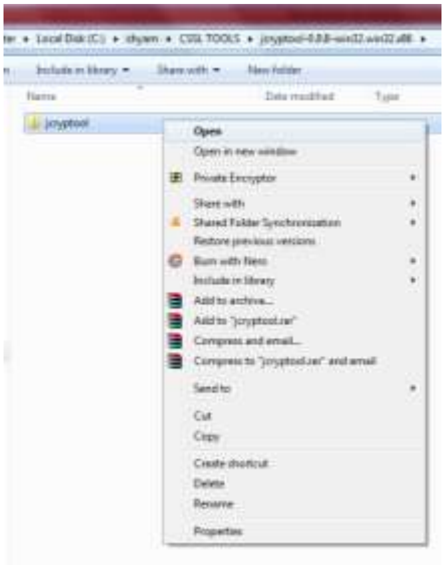
Elapsed time 00:00:10

Processed 24%

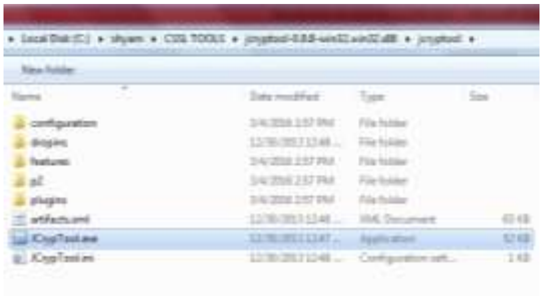
4. Now open Extracted jcryptool folder by click right button of mouse



5. open jcryptool folder by click right button of mouse

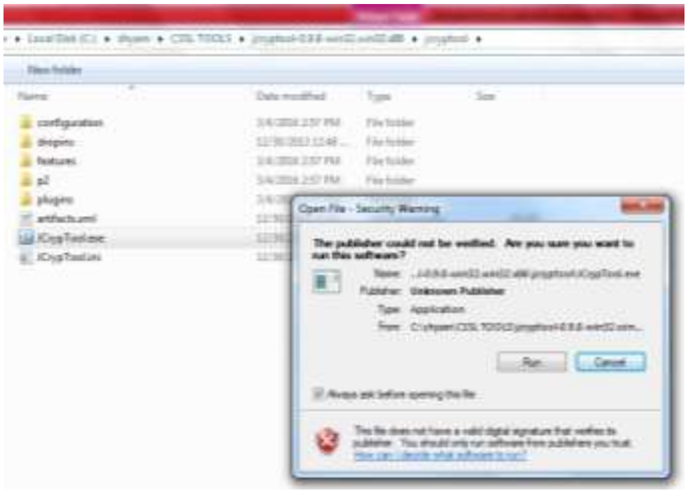


6. Double Click on JCrypt Tool.exe


Local Disk (C:) ▸ shyam ▸ CSSL TOOLS ▸ jcryptool-0.9.8-win32.win32.x86 ▸ jcryptool ▸
New folder

Name	Date modified	Type	Size
configuration	3/4/2016 2:57 PM	File folder	
dropins	12/30/2013 12:48 ...	File folder	
features	3/4/2016 2:57 PM	File folder	
p2	3/4/2016 2:57 PM	File folder	
plugins	3/4/2016 2:57 PM	File folder	
artifacts.xml	12/30/2013 12:48 ...	XML Document	63 KB
JCrypTool.exe	12/30/2013 12:47 ...	Application	52 KB
JCrypTool.ini	12/30/2013 12:48 ...	Configuration sett...	1 KB

7. Click on Run Button



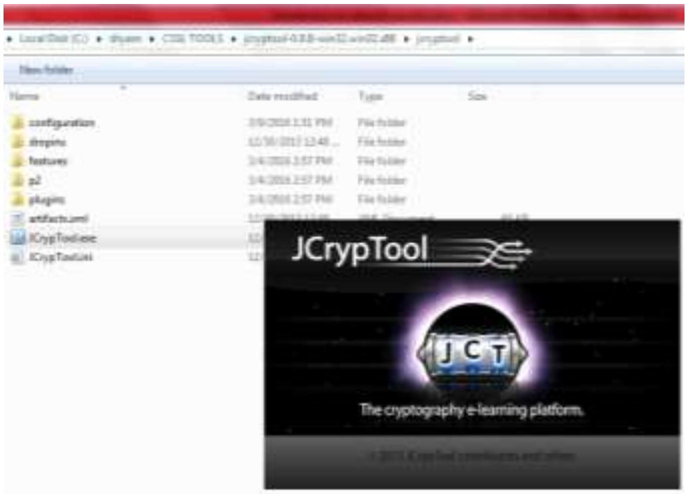
The publisher could not be verified. Are you sure you want to run this software?

Name: ...-0.9.8-win32.win32.x86\jcryptool\JCrypTool.exe
Publisher: Unknown Publisher
Type: Application
From: C:\shyam\CSSL TOOLS\jcryptool-0.9.8-win32.win...

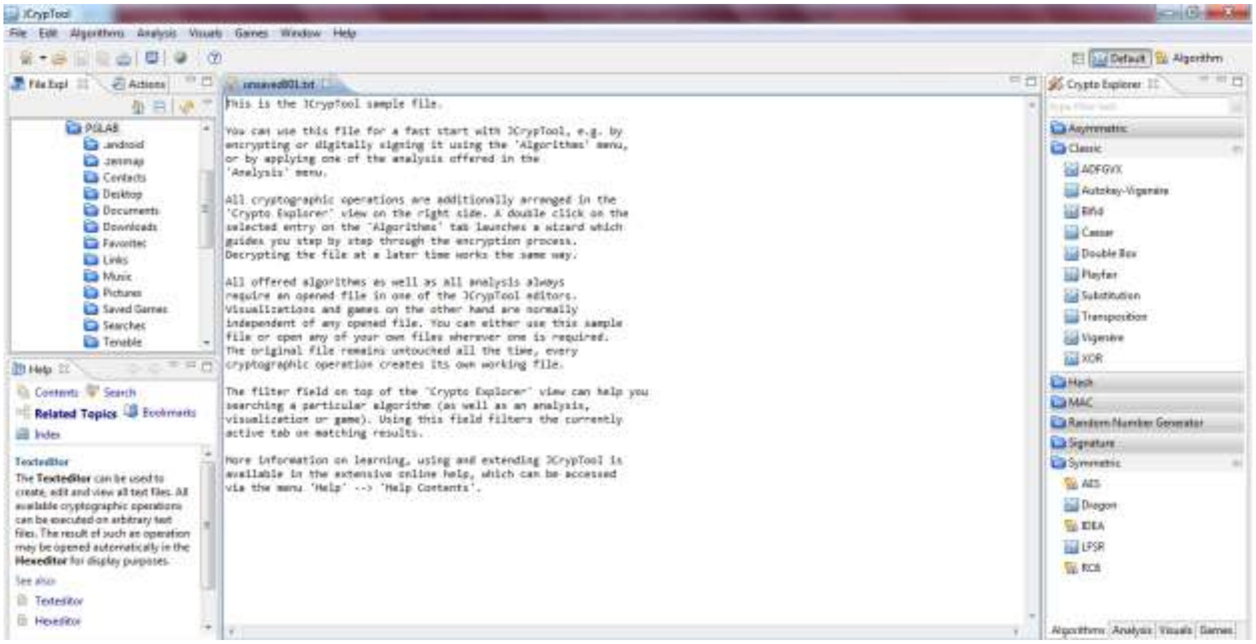
☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

8. JCrypt Tool is now Loading


Local Disk (C:) ▸ shyam ▸ CSS TOOLS ▸ jcryptool-0.9.8-win32.win32.x86 ▸ jcryptool ▸
New folder
Name
Date modified
Type
Size
configuration
dropins
features
p2
plugins
artifacts.xml
JCrypTool.exe
JCrypTool.ini
JCrypTool
The cryptography e-learning platform.

9. This is workspace of JCrypt Tool



Texteditor

The **Texteditor** can be used to create, edit and view all text files. All available cryptographic operations can be executed on arbitrary text files. The result of such an operation may be opened automatically in the **Hexeditor** for display purposes.

See also

Texteditor

Hexeditor

```
This is the JCrypTool sample file.

You can use this file for a fast start with JCrypTool, e.g. by
encrypting or digitally signing it using the 'Algorithms' menu,
or by applying one of the analysis offered in the
'Analysis' menu.

All cryptographic operations are additionally arranged in the
'Crypto Explorer' view on the right side. A double click on the
selected entry on the 'Algorithms' tab launches a wizard which
guides you step by step through the encryption process.
Decrypting the file at a later time works the same way.

All offered algorithms as well as all analysis always
require an opened file in one of the JCrypTool editors.
Visualizations and games on the other hand are normally
independent of any opened file. You can either use this sample
file or open any of your own files wherever one is required.
The original file remains untouched all the time, every
cryptographic operation creates its own working file.

The filter field on top of the 'Crypto Explorer' view can help you
searching a particular algorithm (as well as an analysis,
visualization or game). Using this field filters the currently
active tab on matching results.

More information on learning, using and extending JCrypTool is
available in the extensive online help, which can be accessed
via the menu 'Help' --> 'Help Contents'.
```

Conclusion:-Hence we installed & demonstrated Jcrypt tool software.

6. Using Jcrypt tool (or any other equivalent) to demonstrate asymmetric, symmetric crypto algorithm

Aim:- To demonstrate asymmetric, symmetric crypto algorithm using Jcrypt tool.

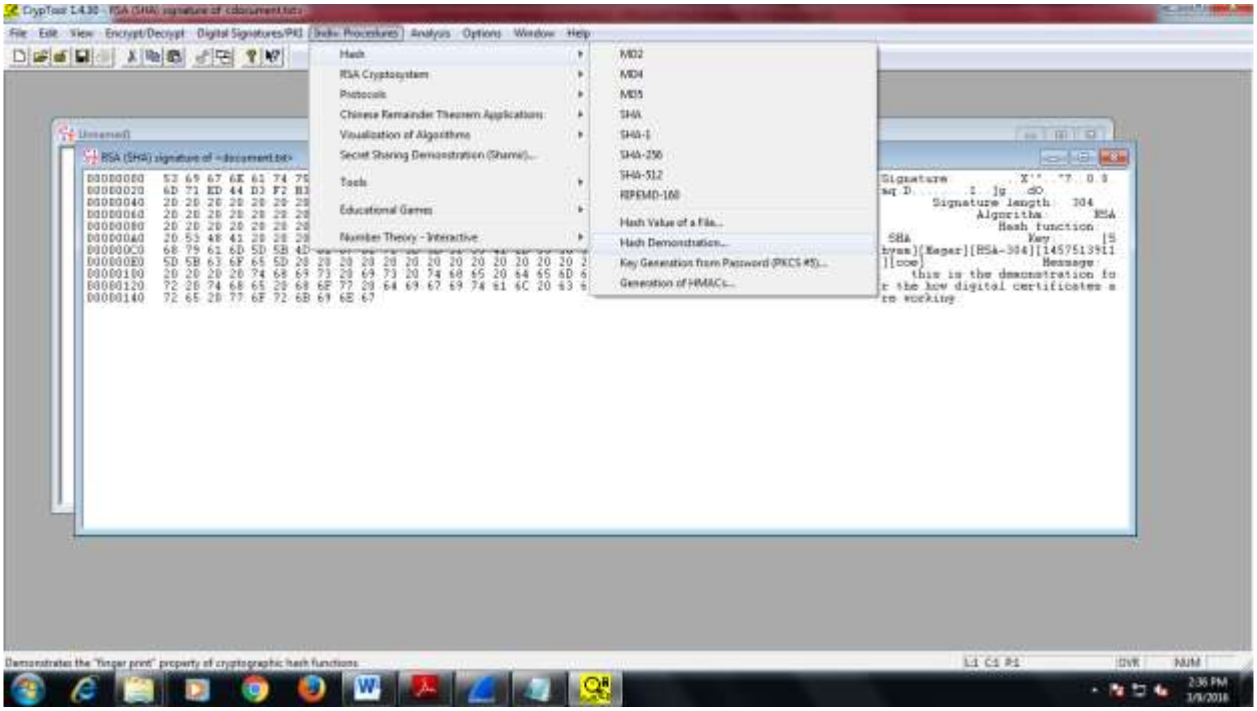
Objective:Student will able to demonstrate asymmetric, symmetric crypto algorithm using Jcrypt tool.

Tools Required:Jcrypt tool.

Theory:

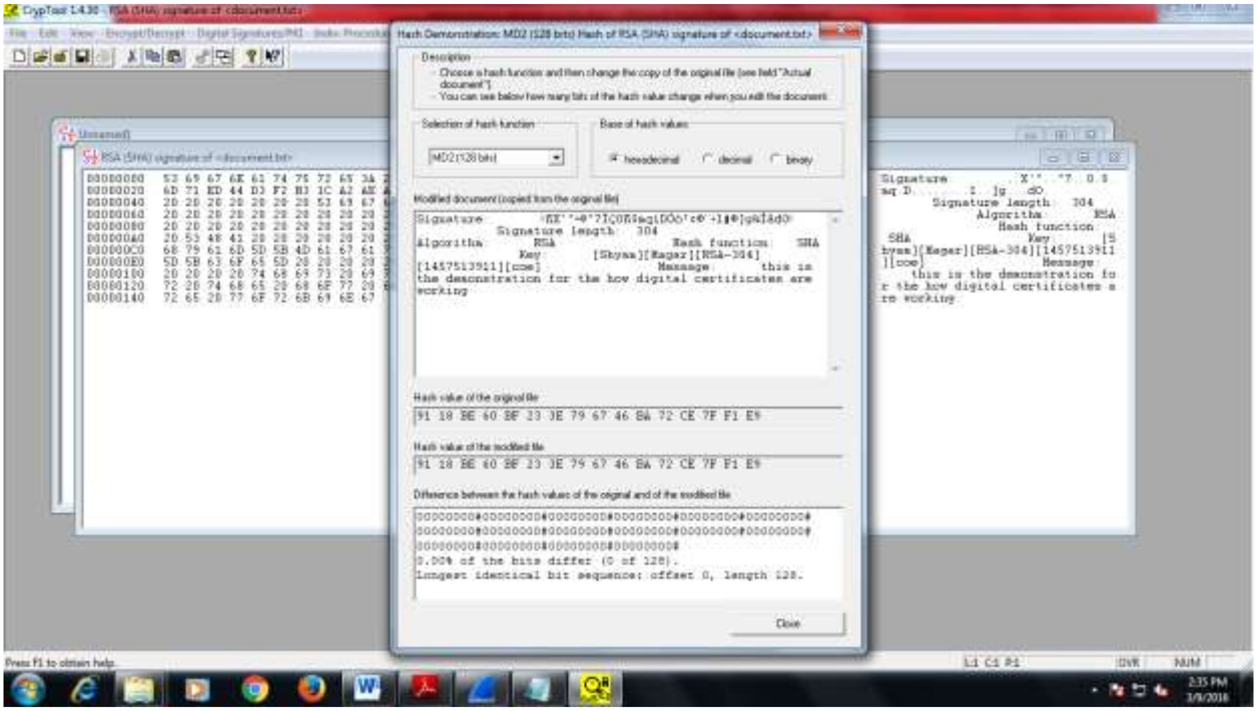
Hash Function

1. Select Indiv. Procedure →Hash →Hash Demonstration →


CrypTool 1.4.30 - RSA (SHA) signature of <document.txt>
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
Help
Hash
RSA Cryptosystem
Protocols
Chinese Remainder Theorem Applications
Visualization of Algorithms
Secret Sharing Demonstration (Shamir)...
Tools
Educational Games
Number Theory - Interactive
MD2
MD4
MD5
SHA
SHA-1
SHA-256
SHA-512
RIPEMD-160
Hash Value of a File...
Hash Demonstration...
Key Generation from Password (PKCS #5)...
Generation of HMACs...
Unnamed1
RSA (SHA) signature of <document.txt>
Demonstrates the "finger print" property of cryptographic hash functions
L1 C1 P1
OVR
NUM
2:36 PM
3/9/2016

```
00000000   53 69 67 6E 61 74 75                                   Signature        X'' '7  0 S
00000020   6D 71 ED 44 D3 F2 B3                                   mq D.        I  ]g   dO
00000040   20 20 20 20 20 20 20                                          Signature length   304
00000060   20 20 20 20 20 20 20                                               Algorithm        RSA
00000080   20 20 20 20 20 20 20                                                  Hash function
000000A0   20 53 48 41 20 20 20                                    SHA                Key        [S
000000C0   68 79 61 6D 5D 5B 4D                                   hyam][Nager][RSA-304][1457513911
000000E0   5D 5B 63 6F 65 5D 20 20 20 20 20 20 20 20 20 20 20 20 2   ][coe]                   Message
00000100   20 20 20 20 74 68 69 73 20 69 73 20 74 68 65 20 64 65 6D 6      this is the demonstration fo
00000120   72 20 74 68 65 20 68 6F 77 20 64 69 67 69 74 61 6C 20 63 6   r the how digital certificates a
00000140   72 65 20 77 6F 72 6B 69 6E 67                          re working
```

2. Selection of hash Function



Hash Demonstration: MD2 (128 bits) Hash of RSA (SHA) signature of <document.txt>

Description
- Choose a hash function and then change the copy of the original file (see field "Actual document")
- You can see below how many bits of the hash value change when you edit the document

Selection of hash function: MD2 (128 bits)

Base of hash values: ● hexadecimal ○ decimal ○ binary

Modified document (copied from the original file)

```
Signature         ·ßE''-Φ"7ÏÇ0ß§aq{DÖõ'c®'+1‡®]gÅÍÅdO
            Signature length:   304
Algorithm:        RSA                 Hash function:    SHA
                Key:       [Shyam][Magar][RSA-304]
[1457513911][coe]                   Message:      this is
the demonstration for the how digital certificates are
working
```

Hash value of the original file

```
91 18 BE 60 BF 23 3E 79 67 46 BA 72 CE 7F F1 E9
```

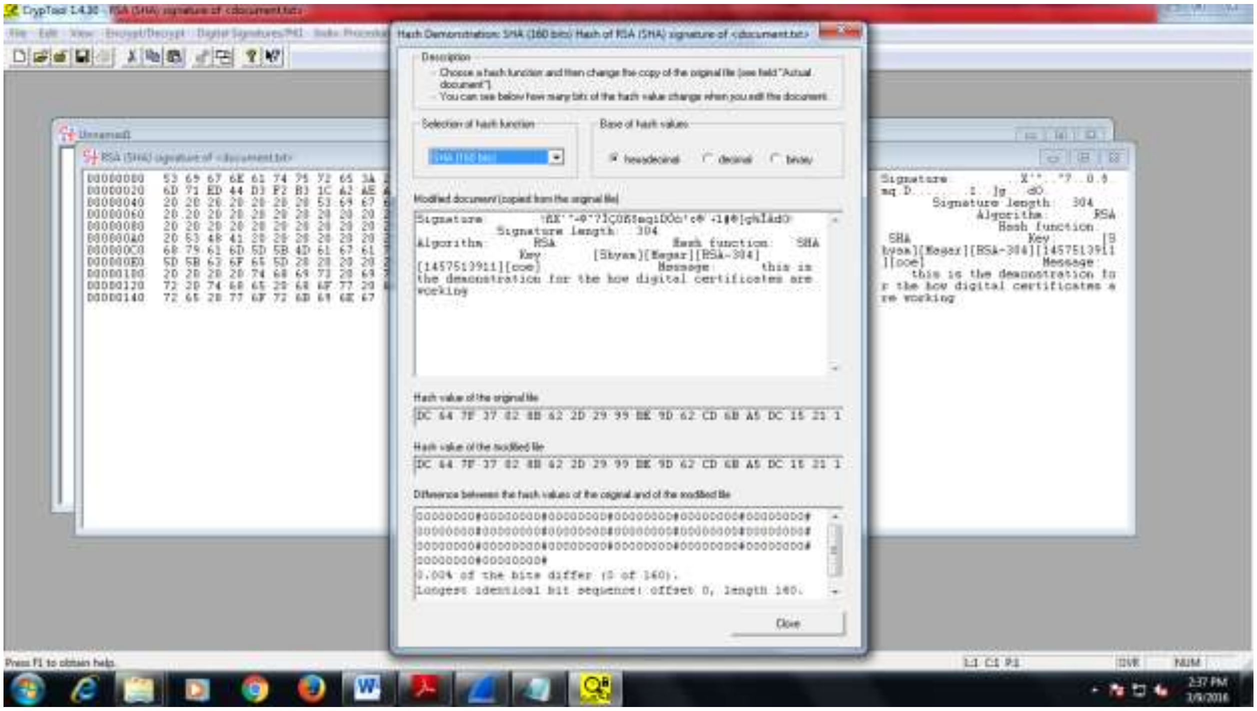
Hash value of the modified file

```
91 18 BE 60 BF 23 3E 79 67 46 BA 72 CE 7F F1 E9
```

Difference between the hash values of the original and of the modified file

```
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#00000000#00000000#
0.00% of the bits differ (0 of 128).
Longest identical bit sequence: offset 0, length 128.
```

3. Select hash function SHA you get hash code value



Hash Demonstration: SHA (160 bits) Hash of RSA (SHA) signature of <document.txt>

Description
- Choose a hash function and then change the copy of the original file (see field "Actual document")
- You can see below how many bits of the hash value change when you edit the document

Selection of hash function: SHA (160 bits)

Base of hash values: ● hexadecimal ○ decimal ○ binary

Modified document (copied from the original file)

```
Signature         ·ßE''-Φ"7ÏÇ0ß§aq{DÖõ'c®'+1‡®]gÅÍÅdO
            Signature length:   304
Algorithm:        RSA                 Hash function:    SHA
                Key:       [Shyam][Magar][RSA-304]
[1457513911][coe]                   Message:      this is
the demonstration for the how digital certificates are
working
```

Hash value of the original file

```
DC 64 7F 37 02 8B 62 2D 29 99 BE 9D 62 CD 6B A5 DC 15 21 1
```

Hash value of the modified file

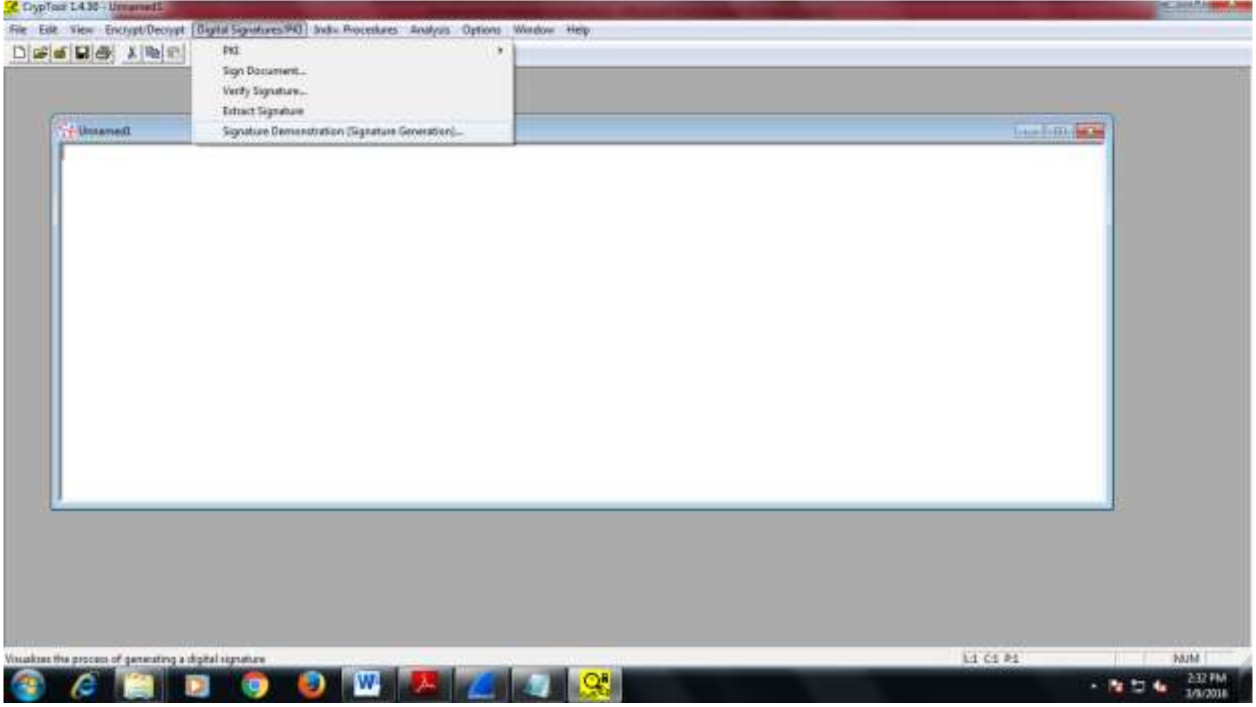
```
DC 64 7F 37 02 8B 62 2D 29 99 BE 9D 62 CD 6B A5 DC 15 21 1
```

Difference between the hash values of the original and of the modified file

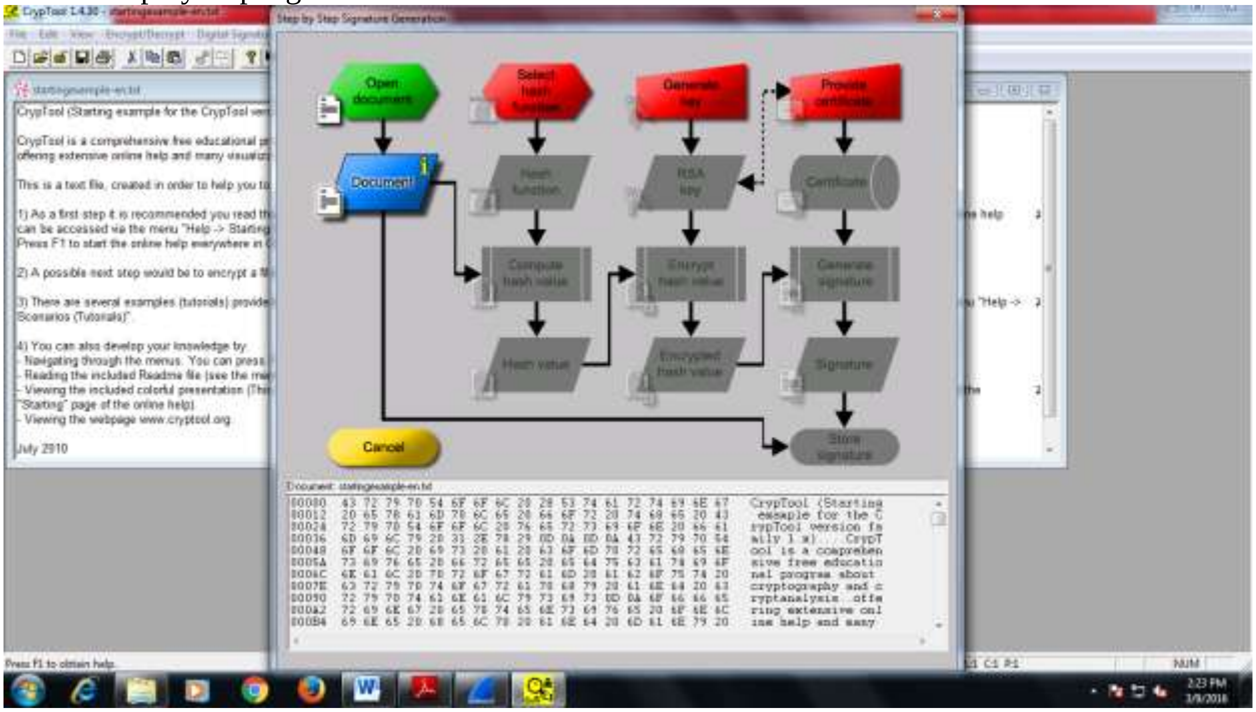
```
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#
0.00% of the bits differ (0 of 160).
Longest identical bit sequence: offset 0, length 160.
```

Digital Signatures

1. Select Digital Signature menu →signature demonstration


CrypTool 1.4.30 - Unnamed1
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
PKI
Sign Document...
Verify Signature...
Extract Signature
Signature Demonstration (Signature Generation)...
Unnamed1
Visualizes the process of generating a digital signature
L1 C1 P1
NUM
2:32 PM
3/9/2018

2. Step by step signature



CrypTool (Starting example for the CrypTool ver

CrypTool is a comprehensive free educational p
offering extensive online help and many visualiz

This is a text file, created in order to help you to

1) As a first step it is recommended you read th
can be accessed via the menu "Help -> Starting
Press F1 to start the online help everywhere in C

2) A possible next step would be to encrypt a fil

3) There are several examples (tutorials) provide
Scenarios (Tutorials)".

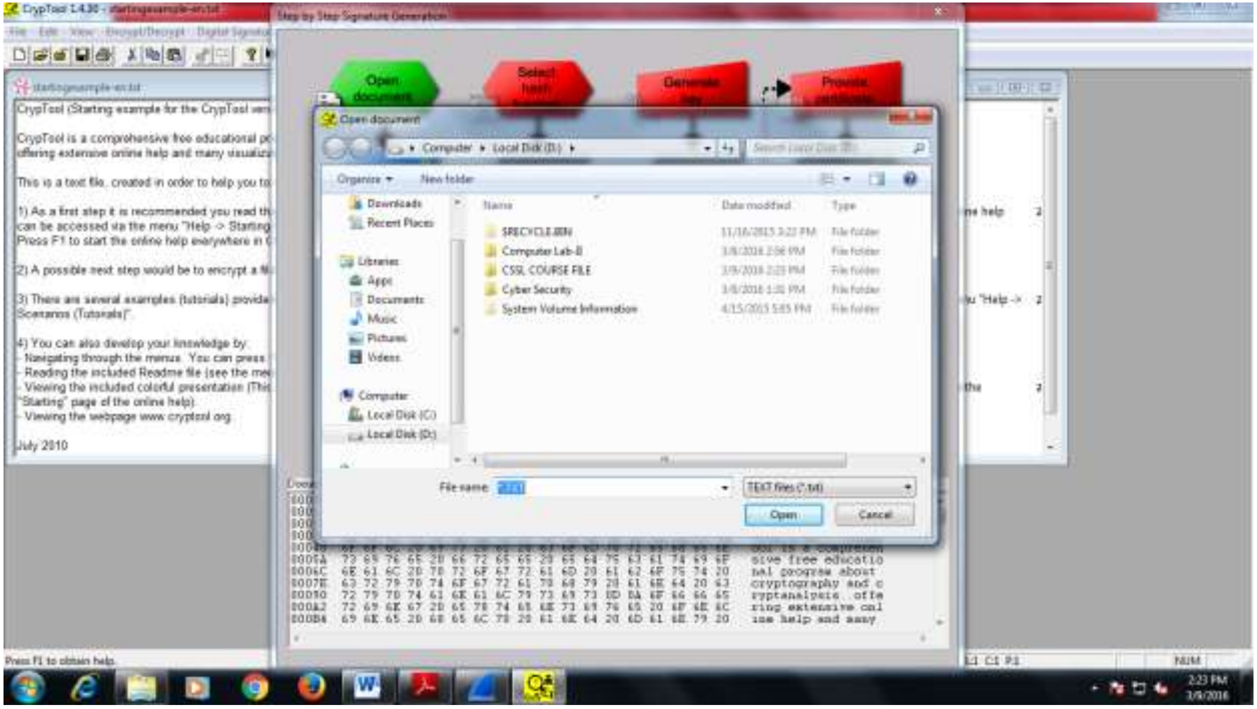
4) You can also develop your knowledge by:
- Navigating through the menus. You can press
- Reading the included Readme file (see the me
- Viewing the included colorful presentation (Thi
"Starting" page of the online help).
- Viewing the webpage www.cryptool.org.

July 2010

Document: startingexample-en.txt

```
00000  43 72 79 70 54 6F 6F 6C 20 28 53 74 61 72 74 69 6E 67   CrypTool (Starting
00012  20 65 78 61 6D 70 6C 65 20 66 6F 72 20 74 68 65 20 43    example for the C
00024  72 79 70 54 6F 6F 6C 20 76 65 72 73 69 6F 6E 20 66 61   rypTool version fa
00036  6D 69 6C 79 20 31 2E 78 29 0D 0A 0D 0A 43 72 79 70 54   mily 1.x)....CrypT
00048  6F 6F 6C 20 69 73 20 61 20 63 6F 6D 70 72 65 68 65 6E   ool is a comprehen
0005A  73 69 76 65 20 66 72 65 65 20 65 64 75 63 61 74 69 6F   sive free educatio
0006C  6E 61 6C 20 70 72 6F 67 72 61 6D 20 61 62 6F 75 74 20   nal program about
0007E  63 72 79 70 74 6F 67 72 61 70 68 79 20 61 6E 64 20 63   cryptography and c
00090  72 79 70 74 61 6E 61 6C 79 73 69 73 0D 0A 6F 66 66 65   ryptanalysis..offe
000A2  72 69 6E 67 20 65 78 74 65 6E 73 69 76 65 20 6F 6E 6C   ring extensive onl
000B4  69 6E 65 20 68 65 6C 70 20 61 6E 64 20 6D 61 6E 79 20   ine help and many
```

3. Click on open document & select txt file



CrypTool (Starting example for the CrypTool ver

CrypTool is a comprehensive free educational pr
offering extensive online help and many visualiz

This is a text file, created in order to help you to

1) As a first step it is recommended you read th
can be accessed via the menu "Help -> Starting
Press F1 to start the online help everywhere in C

2) A possible next step would be to encrypt a fil

3) There are several examples (tutorials) provide
Scenarios (Tutorials)".

4) You can also develop your knowledge by:
- Navigating through the menus. You can press
- Reading the included Readme file (see the me
- Viewing the included colorful presentation (Thi
"Starting" page of the online help).
- Viewing the webpage www.cryptool.org.

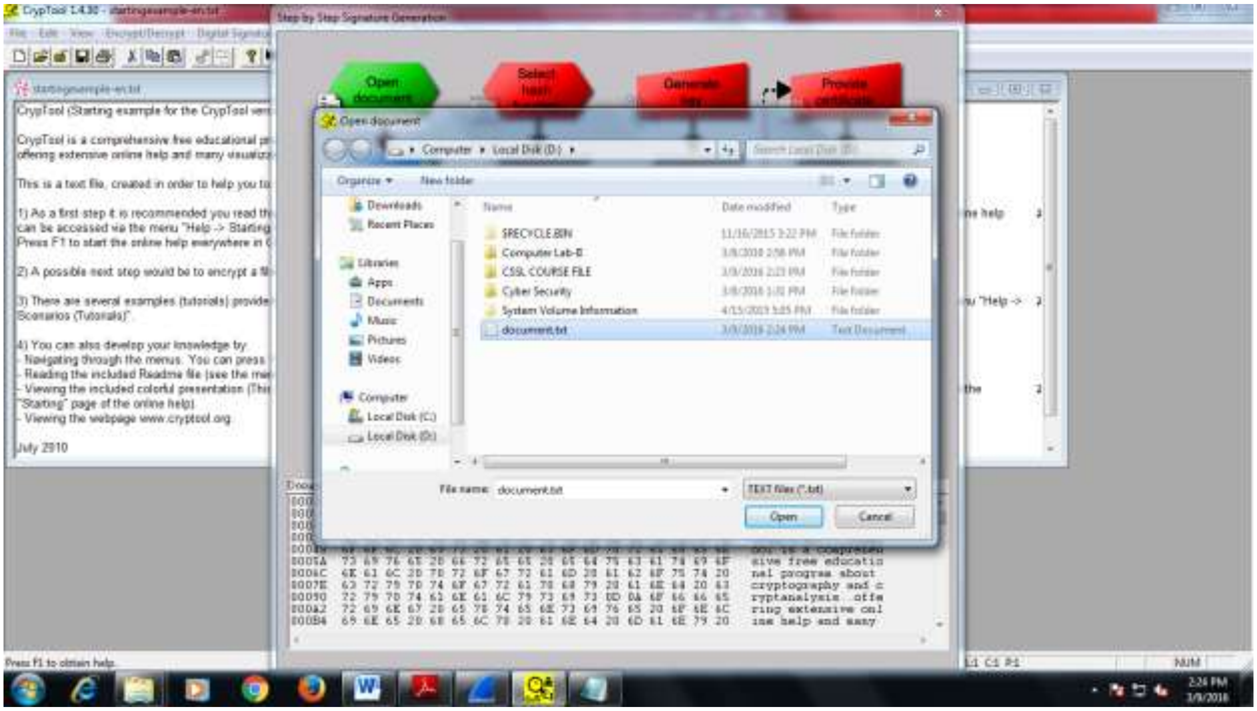
July 2010

Name	Date modified	Type
$RECYCLE.BIN	11/16/2015 3:22 PM	File folder
Computer Lab-II	3/8/2016 2:56 PM	File folder
CSSL COURSE FILE	3/9/2016 2:23 PM	File folder
Cyber Security	3/8/2016 1:31 PM	File folder
System Volume Information	4/15/2015 5:05 PM	File folder

File name: 2121

TEXT files (*.txt)

```
0005A  73 69 76 65 20 66 72 65 65 20 65 64 75 63 61 74 69 6F   sive free educatio
0006C  6E 61 6C 20 70 72 6F 67 72 61 6D 20 61 62 6F 75 74 20   nal program about
0007E  63 72 79 70 74 6F 67 72 61 70 68 79 20 61 6E 64 20 63   cryptography and c
00090  72 79 70 74 61 6E 61 6C 79 73 69 73 0D 0A 6F 66 66 65   ryptanalysis  offe
000A2  72 69 6E 67 20 65 78 74 65 6E 73 69 76 65 20 6F 6E 6C   ring extensive onl
000B4  69 6E 65 20 68 65 6C 70 20 61 6E 64 20 6D 61 6E 79 20   ine help and many
```



CrypTool (Starting example for the CrypTool vers

CrypTool is a comprehensive free educational pr
offering extensive online help and many visualiza

This is a text file, created in order to help you to

1) As a first step it is recommended you read th
can be accessed via the menu "Help -> Starting
Press F1 to start the online help everywhere in C

2) A possible next step would be to encrypt a fil

3) There are several examples (tutorials) provide
Scenarios (Tutorials)".

4) You can also develop your knowledge by:
- Navigating through the menus. You can press
- Reading the included Readme file (see the me
- Viewing the included colorful presentation (This
"Starting" page of the online help)
- Viewing the webpage www.cryptool.org

July 2010

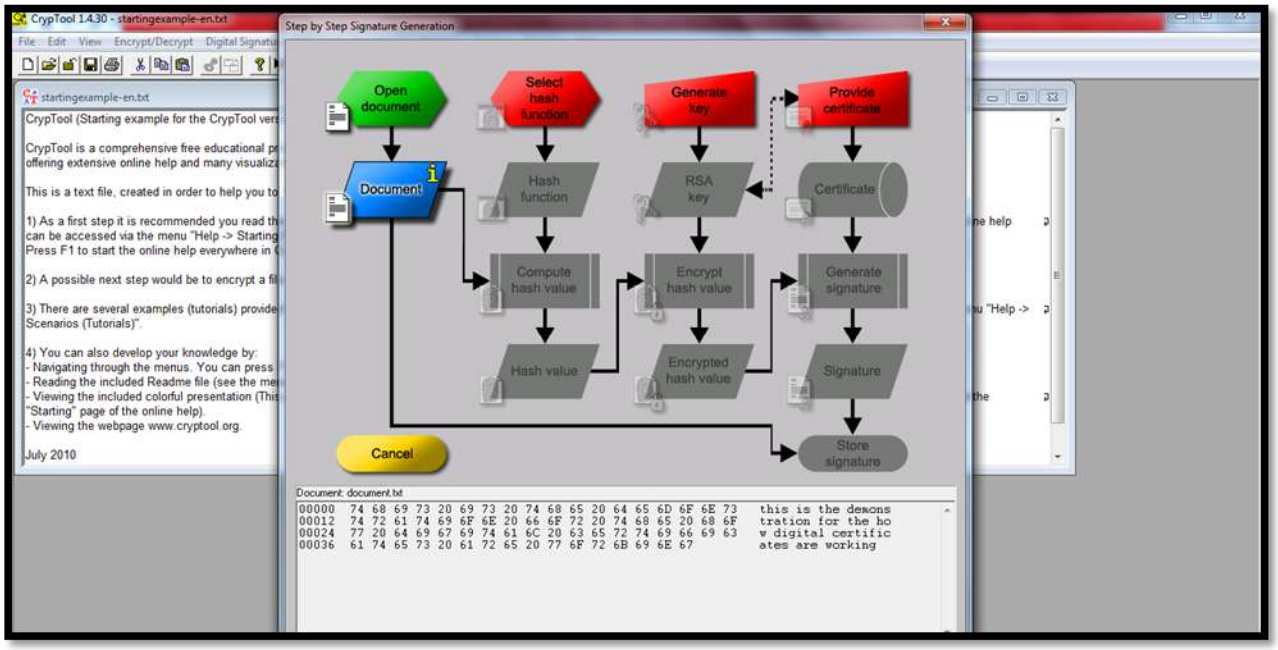
Name	Date modified	Type
$RECYCLE.BIN	11/16/2015 3:22 PM	File folder
Computer Lab-B	3/8/2016 2:58 PM	File folder
CSSL COURSE FILE	3/9/2016 2:23 PM	File folder
Cyber Security	3/8/2016 1:02 PM	File folder
System Volume Information	4/15/2015 5:05 PM	File folder
document.txt	3/9/2016 2:24 PM	Text Document

File name: document.txt

TEXT files (*.txt)

```
00005A  73 69 76 65 20 66 72 65 65 20 65 64 75 63 61 74 69 6F   sive free educatio
00006C  6E 61 6C 20 70 72 6F 67 72 61 6D 20 61 62 6F 75 74 20   nal program about
00007E  63 72 79 70 74 6F 67 72 61 70 68 79 20 61 6E 64 20 63   cryptography and c
000090  72 79 70 74 61 6E 61 6C 79 73 69 73 0D 0A 6F 66 66 65   ryptanalysis  offe
0000A2  72 69 6E 67 20 65 78 74 65 6E 73 69 76 65 20 6F 6E 6C   ring extensive onl
0000B4  69 6E 65 20 68 65 6C 70 20 61 6E 64 20 6D 61 6E 79 20   ine help and many
```

4. Document is converted in to hexadecimal value & ready to compute hash value



CrypTool (Starting example for the CrypTool vers

CrypTool is a comprehensive free educational pr
offering extensive online help and many visualiz

This is a text file, created in order to help you to

1) As a first step it is recommended you read th
can be accessed via the menu "Help -> Starting
Press F1 to start the online help everywhere in C

2) A possible next step would be to encrypt a fil

3) There are several examples (tutorials) provide
Scenarios (Tutorials)".

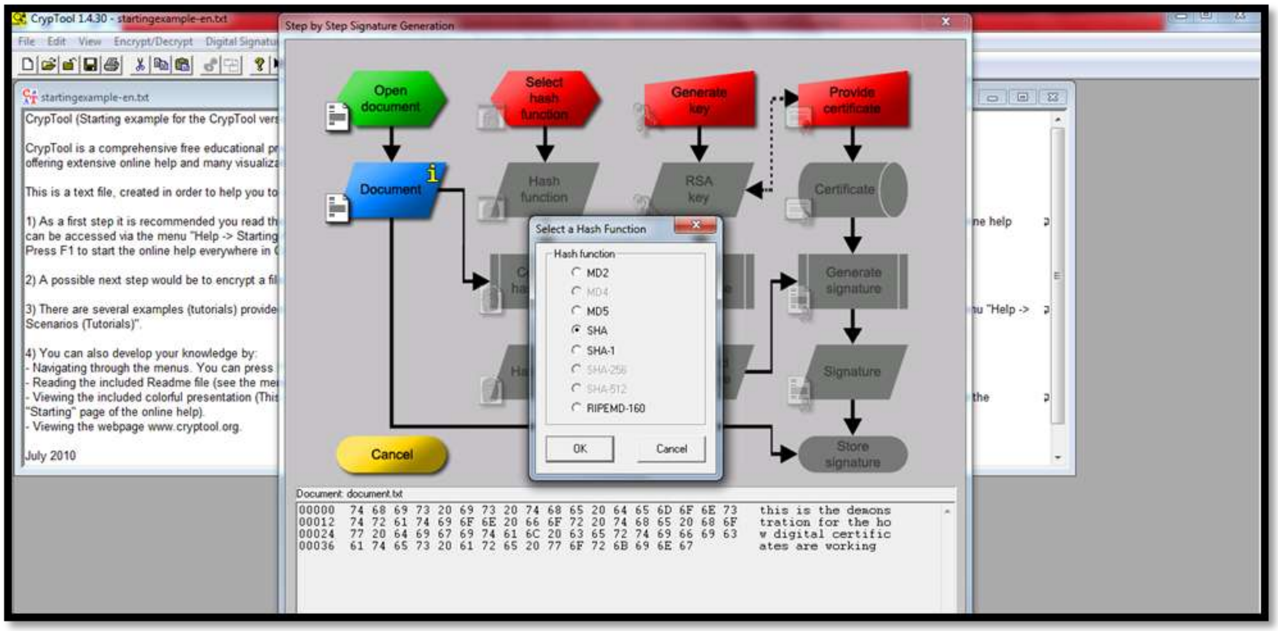
4) You can also develop your knowledge by:
- Navigating through the menus. You can press
- Reading the included Readme file (see the me
- Viewing the included colorful presentation (This
"Starting" page of the online help).
- Viewing the webpage www.cryptool.org.

July 2010

Document: document.txt

```
00000  74 68 69 73 20 69 73 20 74 68 65 20 64 65 6D 6F 6E 73   this is the demons
00012  74 72 61 74 69 6F 6E 20 66 6F 72 20 74 68 65 20 68 6F   tration for the ho
00024  77 20 64 69 67 69 74 61 6C 20 63 65 72 74 69 66 69 63   w digital certific
00036  61 74 65 73 20 61 72 65 20 77 6F 72 6B 69 6E 67         ates are working
```

5. Select Hash function from given list as SHA



Hash function
○ MD2
○ MD4
○ MD5
● SHA
○ SHA-1
○ SHA-256
○ SHA-512
○ RIPEMD-160

CrypTool (Starting example for the CrypTool vers

CrypTool is a comprehensive free educational pr
offering extensive online help and many visualiz

This is a text file, created in order to help you to

1) As a first step it is recommended you read th
can be accessed via the menu "Help -> Starting
Press F1 to start the online help everywhere in C

2) A possible next step would be to encrypt a fil

3) There are several examples (tutorials) provide
Scenarios (Tutorials)".

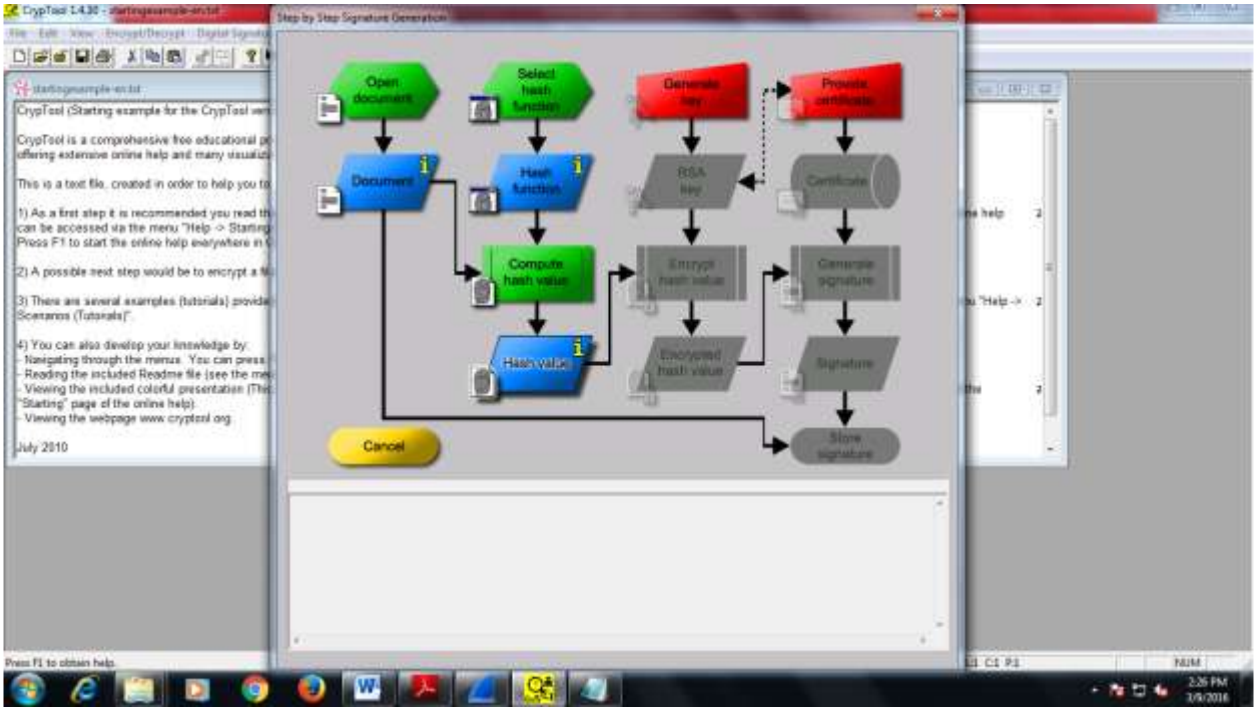
4) You can also develop your knowledge by:
- Navigating through the menus. You can press
- Reading the included Readme file (see the me
- Viewing the included colorful presentation (This
"Starting" page of the online help).
- Viewing the webpage www.cryptool.org.

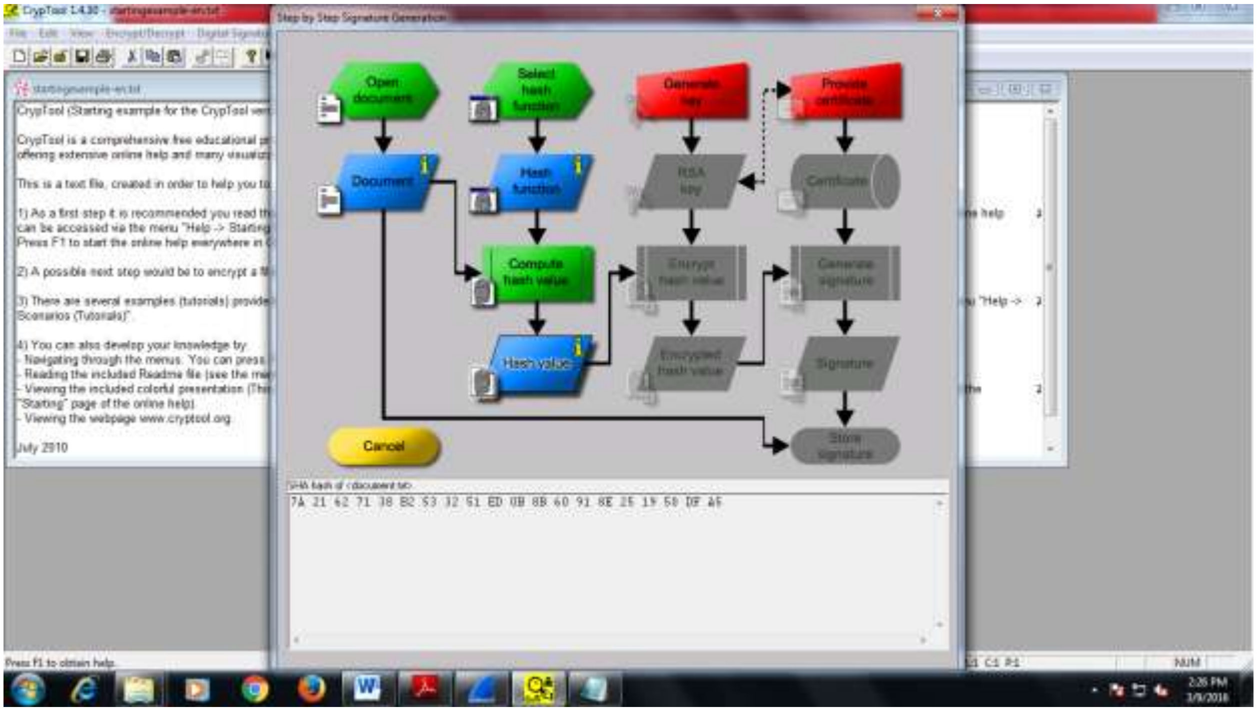
July 2010

Document: document.txt

```
00000  74 68 69 73 20 69 73 20 74 68 65 20 64 65 6D 6F 6E 73   this is the demons
00012  74 72 61 74 69 6F 6E 20 66 6F 72 20 74 68 65 20 68 6F   tration for the ho
00024  77 20 64 69 67 69 74 61 6C 20 63 65 72 74 69 66 69 63   w digital certific
00036  61 74 65 73 20 61 72 65 20 77 6F 72 6B 69 6E 67         ates are working
```

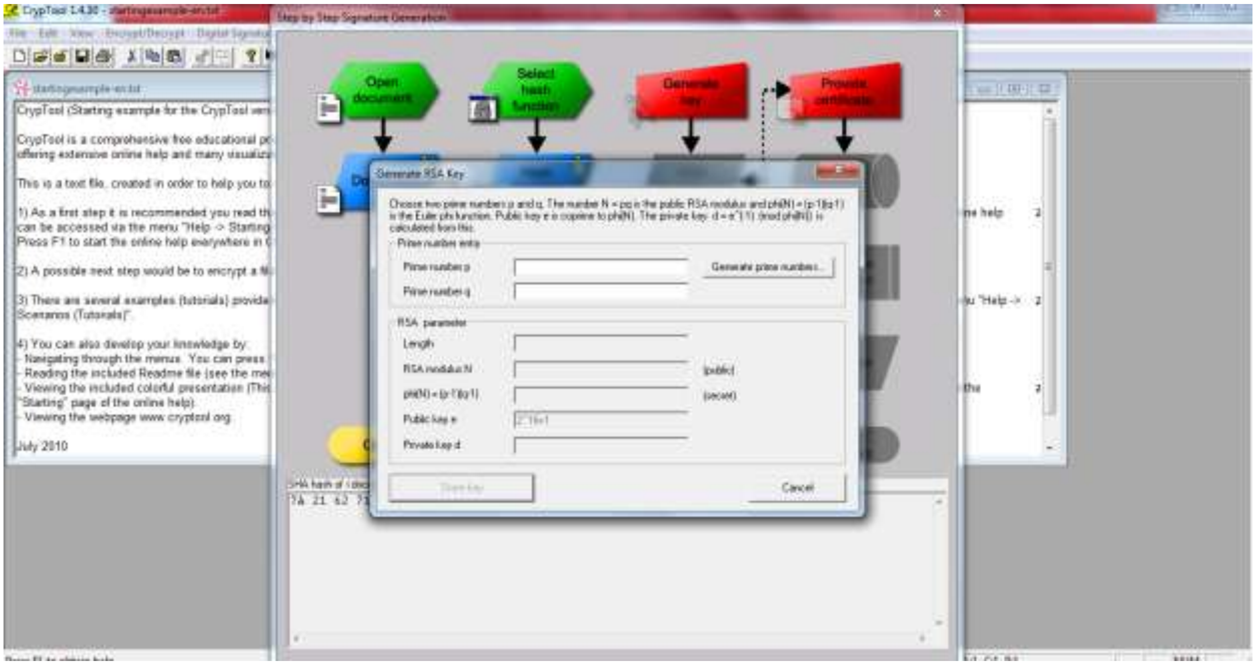
6.Click on compute hash value & hash value you will get the hash value





```
SHA hash of <document.txt>
7A 21 62 71 38 B2 53 32 51 ED 0B 8B 60 91 8E 2F 19 50 DF A6
```

7.Click on generate key & provide P & Q value for generating prime no



CrypTool 1.4.30 - startingexample-en.txt
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate
Generate RSA Key

Choose two prime numbers p and q. The number N = pq is the public RSA modulus and phi(N) = (p-1)(q-1) is the Euler phi function. Public key e is coprime to phi(N). The private key: d = e^(-1) (mod phi(N)) is calculated from this.

Prime number entry

Prime number p:

Prime number q:

RSA parameter

Length:

RSA modulus N: (public)

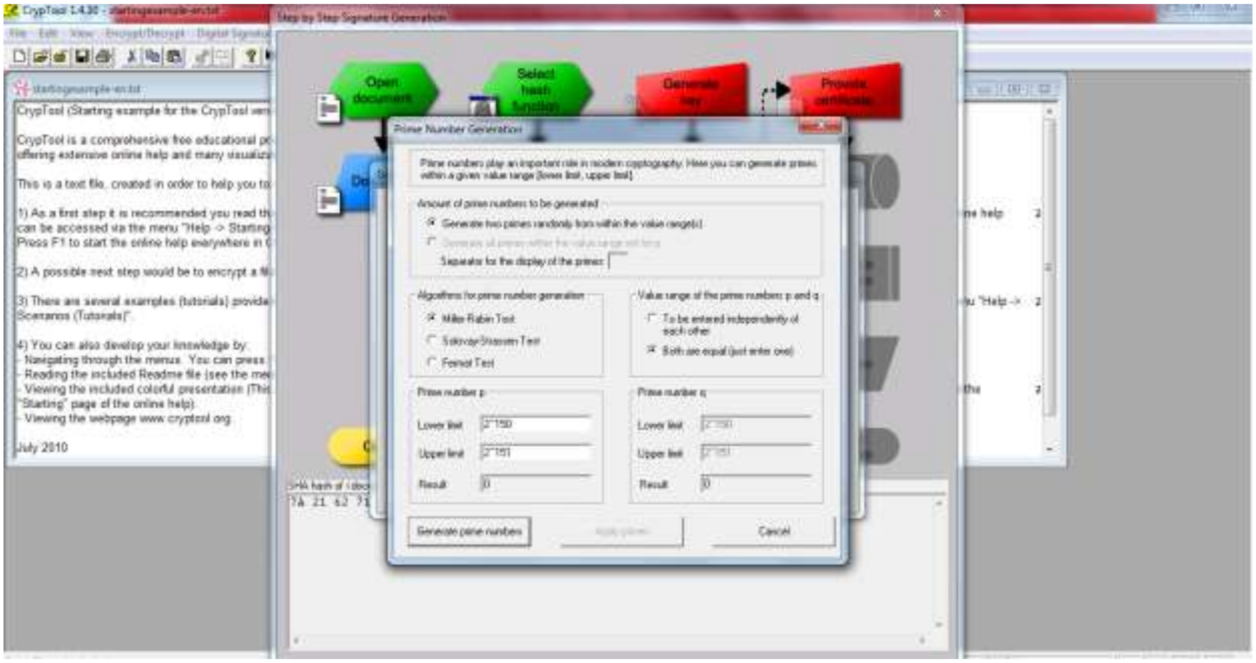
phi(N) = (p-1)(q-1): (secret)

Public key e: 2^16+1

Private key d:

Generate prime numbers...
Store key
Cancel

8. Generate prime no according to algorithm



CrypTool 1.4.30 - startingexample-en.txt
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate

Prime Number Generation

Prime numbers play an important role in modern cryptography. Here you can generate primes within a given value range [lower limit, upper limit].

Amount of prime numbers to be generated

- ● Generate two primes randomly from within the value range(s)
- ○ Generate all primes within the value range (ad hoc)

Separator for the display of the primes:

Algorithms for prime number generation

- ● Miller-Rabin Test
- ○ Solovay-Strassen Test
- ○ Fermat Test

Value range of the prime numbers p and q

- □ To be entered independently of each other
- ● Both are equal (just enter one)

Prime number p

Lower limit: 2^150

Upper limit: 2^151

Result: 0

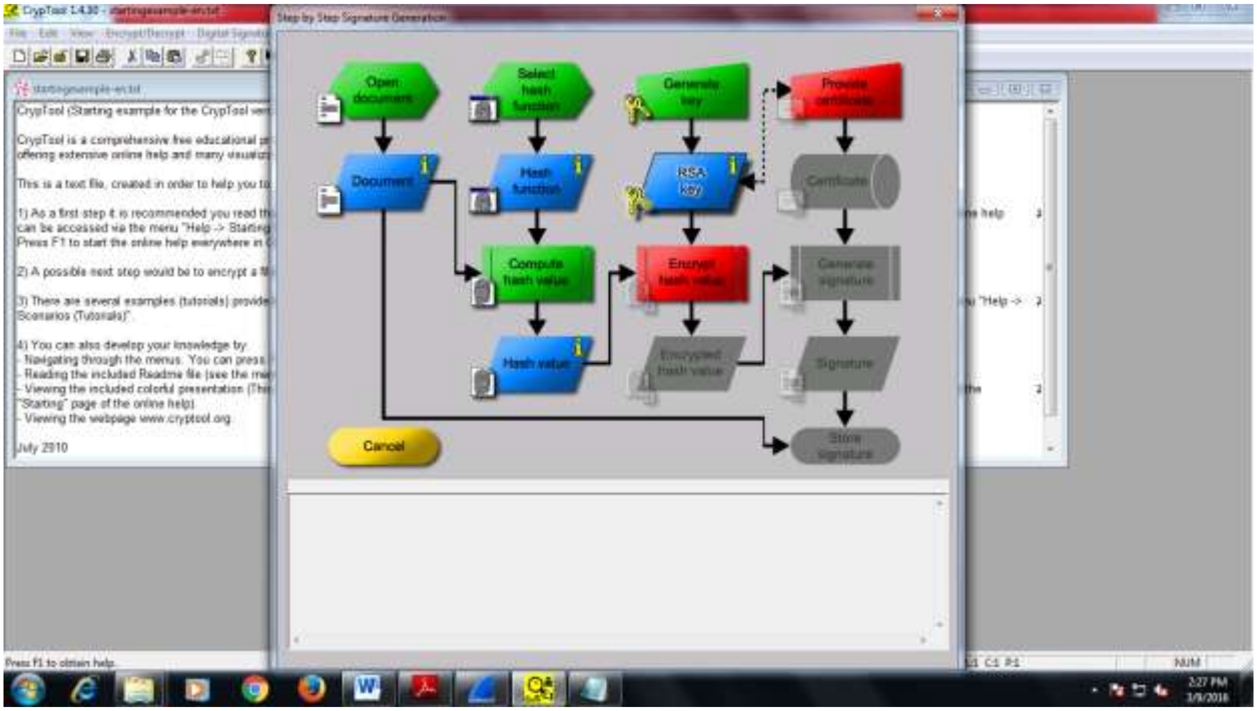
Prime number q

Lower limit: 2^150

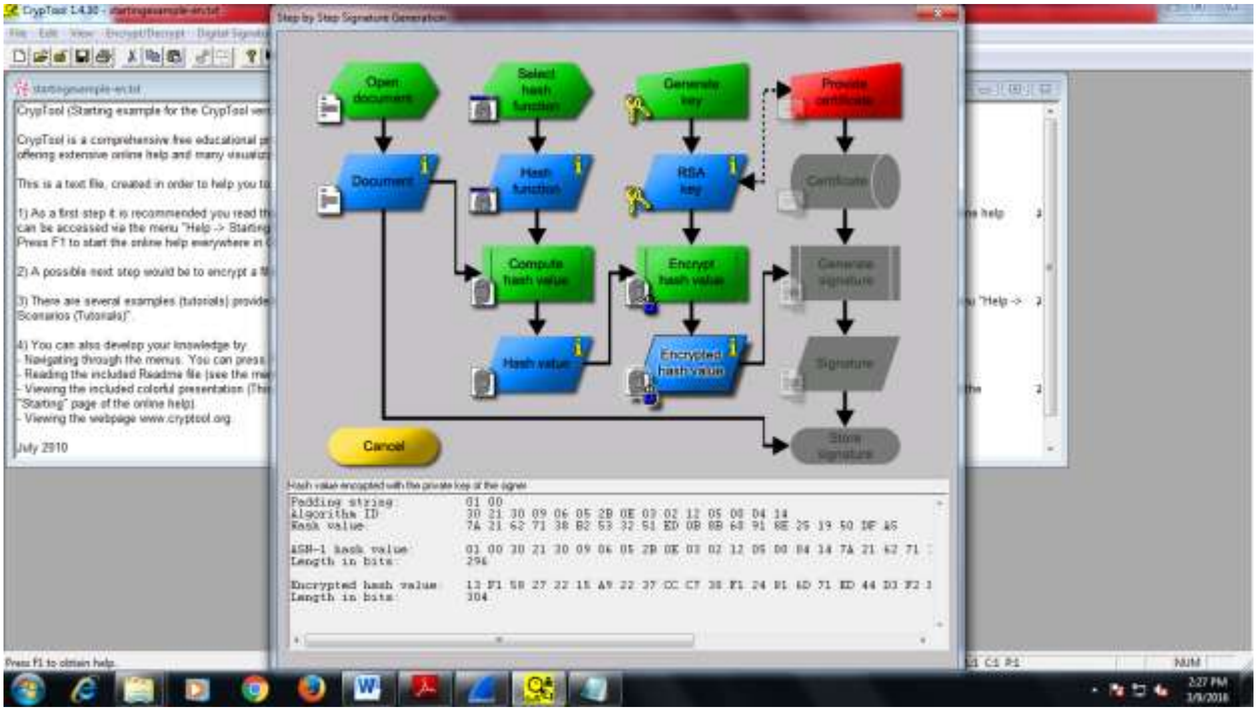
Upper limit: 2^151

Result: 0

10. Generate the RSA key & click on encrypt hash value



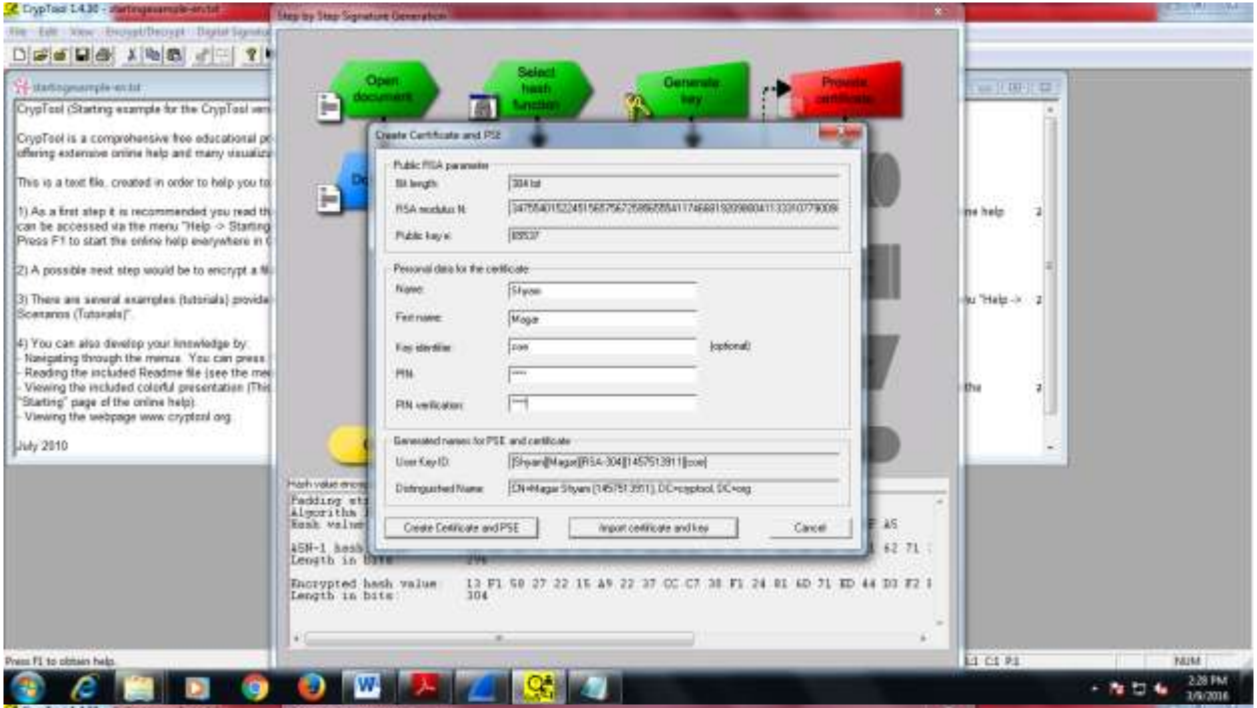
11.Check Encrypted HashValue



Hash value encrypted with the private key of the signer

```
Padding string:          01 00
Algorithm ID:            30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14
Hash value:              7A 21 62 71 38 B2 53 32 51 ED 0B 8B 68 91 8E 25 19 50 DF A5

ASN-1 hash value:        01 00 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 7A 21 62 71
Length in bits:          296

Encrypted hash value:    13 F1 58 27 22 15 A9 22 37 CC C7 38 F1 24 B1 6D 71 ED 44 D3 F2
Length in bits:          304
```

12. Provide Digital Certificate



Public RSA parameter

Bit length: 304 bit

RSA modulus N: 34755401522451565756725986555411746681920988041133310779008

Public key e: 65537

Personal data for the certificate

Name: Shyam

First name: Magar

Key identifier: coe (optional)

PIN: ****

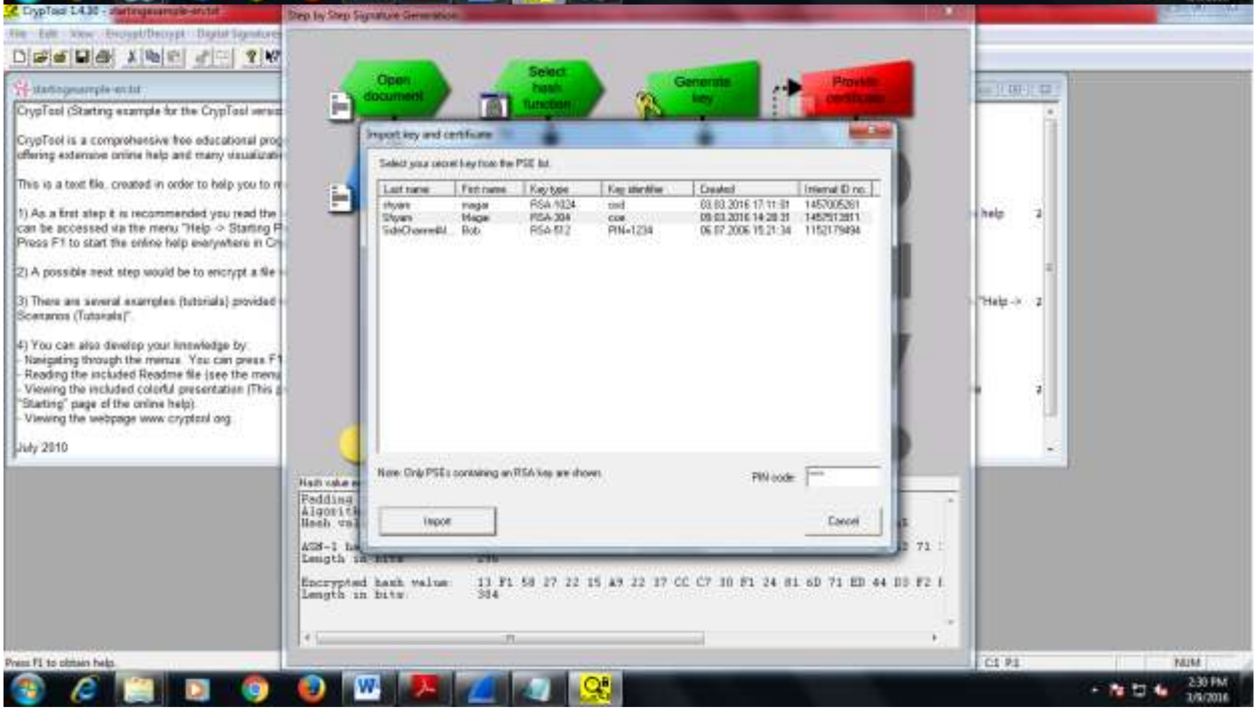
PIN verification: ****

Generated names for PSE and certificate

User Key ID: [Shyam][Magar][RSA-304][1457513911][coe]

Distinguished Name: CN=Magar Shyam [1457513911], DC=cryptool, DC=org

```
Encrypted hash value:   13 F1 58 27 22 15 A9 22 37 CC C7 38 F1 24 81 6D 71 ED 44 D3 F2
Length in bits:         304
```



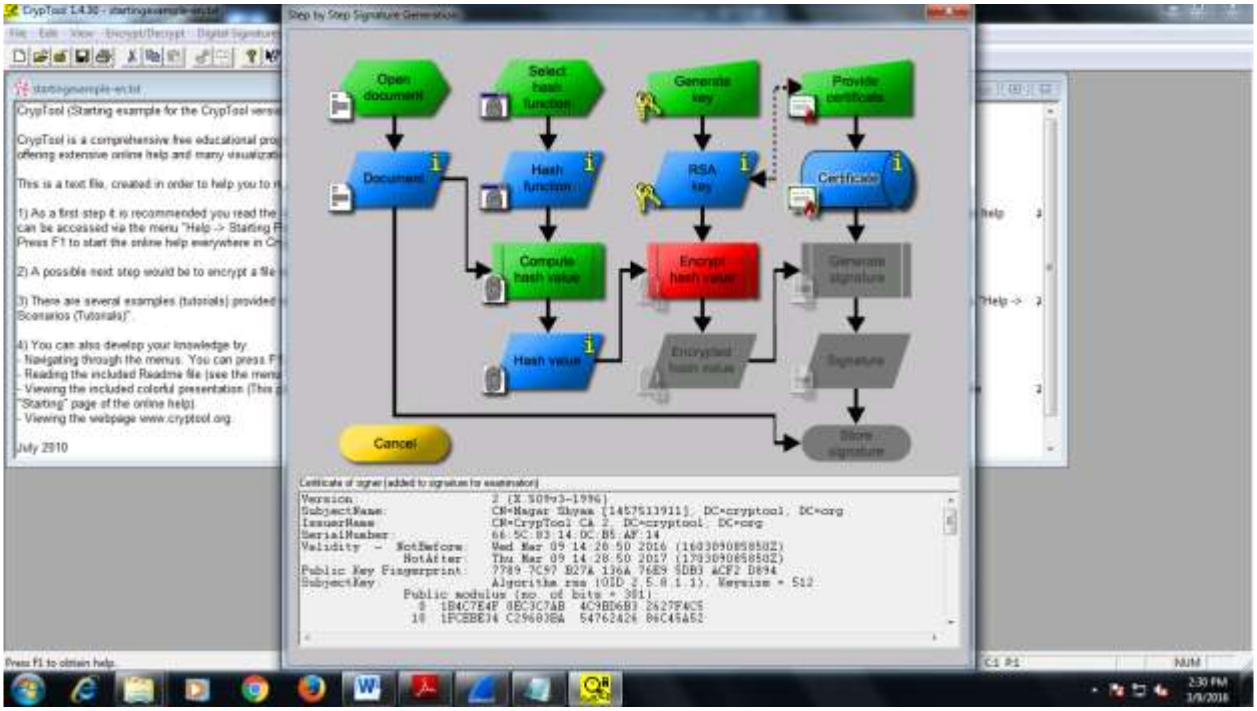
Select your secret key from the PSE list

Last name	First name	Key type	Key identifier	Created	Internal ID no.
shyam	magar	RSA-1024	cod	03.03.2016 17:11:01	1457005261
Shyam	Magar	RSA-304	coe	09.03.2016 14:28:31	1457513911
SideChannelAt...	Rob	RSA-512	PIN=1234	06.07.2006 15:21:34	1152179494

Note: Only PSEs containing an RSA key are shown.

PIN code: ****

```
Encrypted hash value:   13 F1 58 27 22 15 A9 22 37 CC C7 30 F1 24 81 6D 71 ED 44 D3 F2
Length in bits:         304
```



CrypTool (Starting example for the CrypTool versi

CrypTool is a comprehensive free educational pro
offering extensive online help and many visualizati

This is a text file, created in order to help you to n

1) As a first step it is recommended you read the
can be accessed via the menu "Help -> Starting P
Press F1 to start the online help everywhere in Cr

2) A possible next step would be to encrypt a file

3) There are several examples (tutorials) provided
Scenarios (Tutorials)".

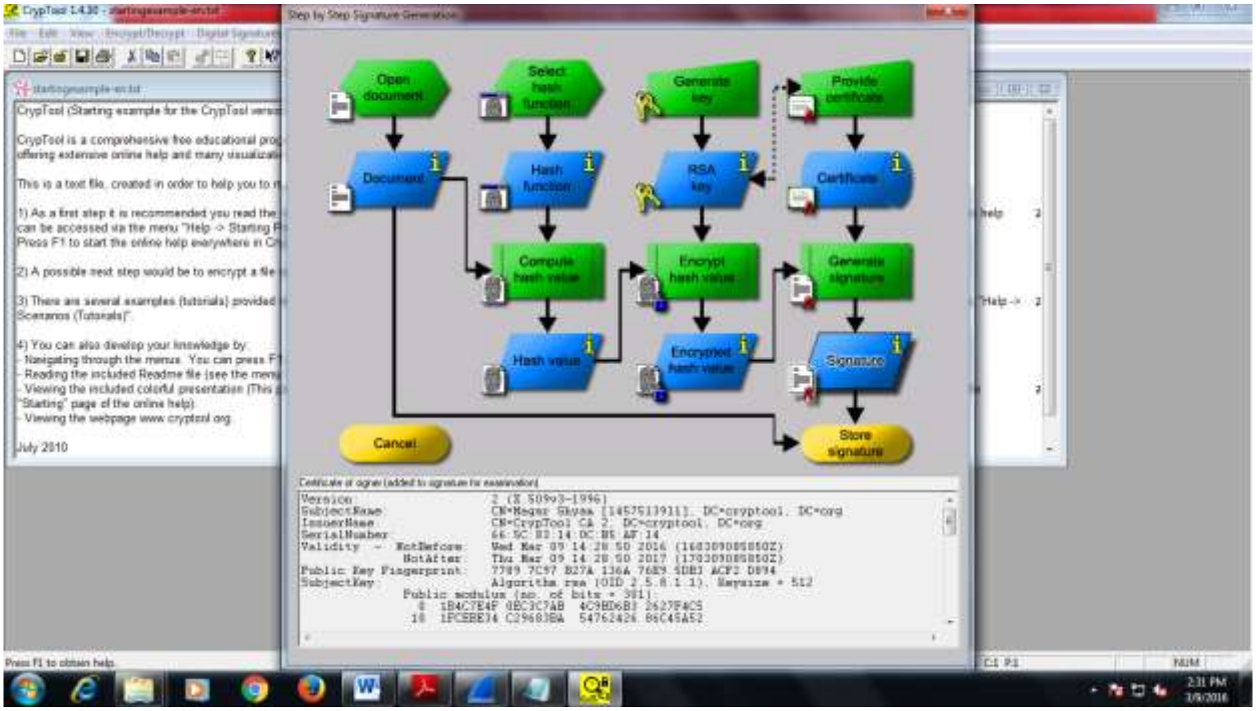
4) You can also develop your knowledge by:
- Navigating through the menus. You can press F
- Reading the included Readme file (see the menu
- Viewing the included colorful presentation (This p
"Starting" page of the online help).
- Viewing the webpage www.cryptool.org.

July 2010

Certificate of signer (added to signature for examination)

```
Version:                       2 (X.509v3-1996)
SubjectName:                   CN=Nagar Shyam [1457513911], DC=cryptool, DC=org
IssuerName:                    CN=CrypTool CA 2, DC=cryptool, DC=org
SerialNumber:                  66:5C:03:14:DC:B5:AF:14
Validity  -  NotBefore:        Wed Mar 09 14:28:50 2016 (160309085850Z)
             NotAfter:         Thu Mar 09 14:28:50 2017 (170309085850Z)
Public Key Fingerprint:        7789 7C97 B27A 136A 76E9 5DB3 ACF2 D894
SubjectKey:                    Algorithm rsa (OID 2.5.8.1.1), Keysize = 512
             Public modulus (no. of bits = 381):
               0  1B4C7E4F 0EC3C7AB  4C9BD6B3 2627F4C5
              10  1FCEBE34 C29603BA  54762426 86C45A52
```

13. Generate Certificate & Signature



CrypTool (Starting example for the CrypTool versi

CrypTool is a comprehensive free educational pro
offering extensive online help and many visualizati

This is a text file, created in order to help you to n

1) As a first step it is recommended you read the
can be accessed via the menu "Help -> Starting P
Press F1 to start the online help everywhere in Cr

2) A possible next step would be to encrypt a file

3) There are several examples (tutorials) provided
Scenarios (Tutorials)".

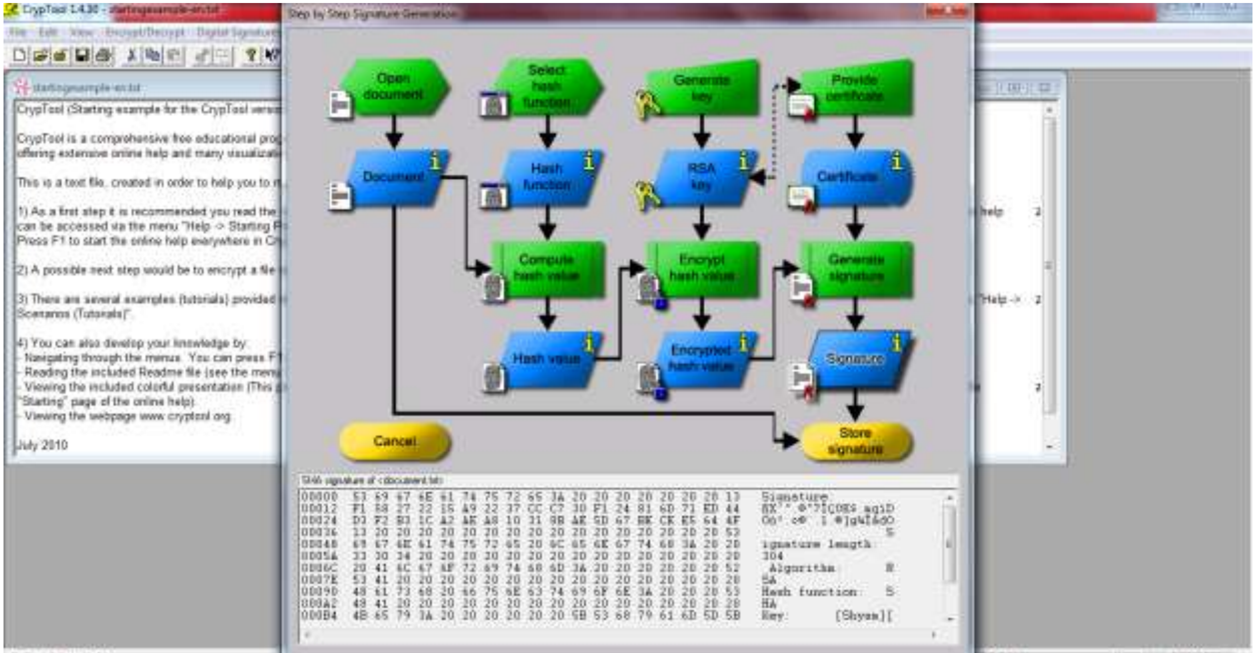
4) You can also develop your knowledge by:
- Navigating through the menus. You can press F
- Reading the included Readme file (see the menu
- Viewing the included colorful presentation (This p
"Starting" page of the online help).
- Viewing the webpage www.cryptool.org.

July 2010

Certificate of signer (added to signature for examination)

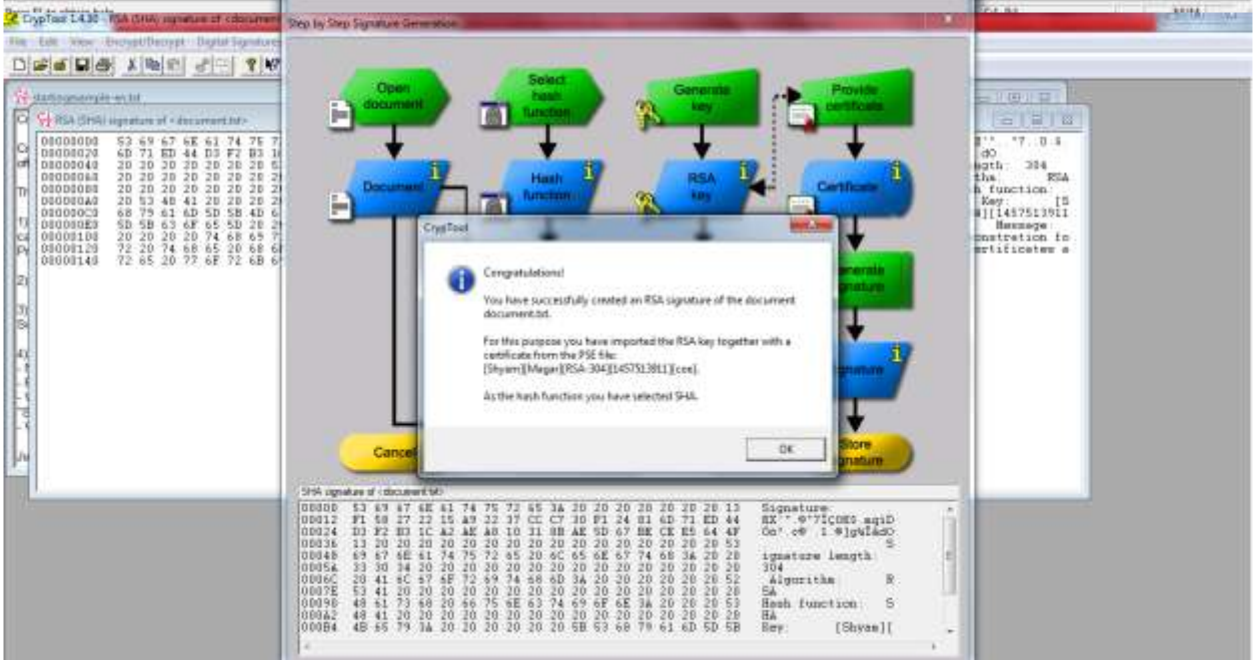
```
Version:                       2 (X.509v3-1996)
SubjectName:                   CN=Nagar Shyam [1457513911], DC=cryptool, DC=org
IssuerName:                    CN=CrypTool CA 2, DC=cryptool, DC=org
SerialNumber:                  66:5C:03:14:DC:B5:AF:14
Validity  -  NotBefore:        Wed Mar 09 14:28:50 2016 (160309085850Z)
             NotAfter:         Thu Mar 09 14:28:50 2017 (170309085850Z)
Public Key Fingerprint:        7789 7C97 B27A 136A 76E9 5DB3 ACF2 D894
SubjectKey:                    Algorithm rsa (OID 2.5.8.1.1), Keysize = 512
             Public modulus (no. of bits = 381):
               0  1B4C7E4F 0EC3C7AB  4C9BD6B3 2627F4C5
              10  1FCEBE34 C29603BA  54762426 86C45A52
```

14. Check the Digital Signature & Store the Signature



SHA signature of <document.txt>

```
00000  53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 13   Signature:
00012  F1 58 27 22 15 A9 22 37 CC C7 30 F1 24 81 6D 71 ED 44   ñX'".©"7ÌÇ0ñ$ mqíD
00024  D3 F2 B3 1C A2 AE A8 10 31 8B AE 5D 67 BE CE E5 64 4F   Óò³ ¢®¨ 1 ®]g¾ÎådO
00036  13 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53                    S
00048  69 67 6E 61 74 75 72 65 20 6C 65 6E 67 74 68 3A 20 20   ignature length:
0005A  33 30 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   304
0006C  20 41 6C 67 6F 72 69 74 68 6D 3A 20 20 20 20 20 20 52    Algorithm:      R
0007E  53 41 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   SA
00090  48 61 73 68 20 66 75 6E 63 74 69 6F 6E 3A 20 20 20 53   Hash function:   S
000A2  48 41 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   HA
000B4  4B 65 79 3A 20 20 20 20 20 20 5B 53 68 79 61 6D 5D 5B   Key:      [Shyam][
```


CrypTool 1.4.30 - RSA (SHA) signature of <document.txt>
Step by Step Signature Generation
RSA (SHA) signature of <document.txt>

CrypTool

Congratulations!

You have successfully created an RSA signature of the document document.txt.

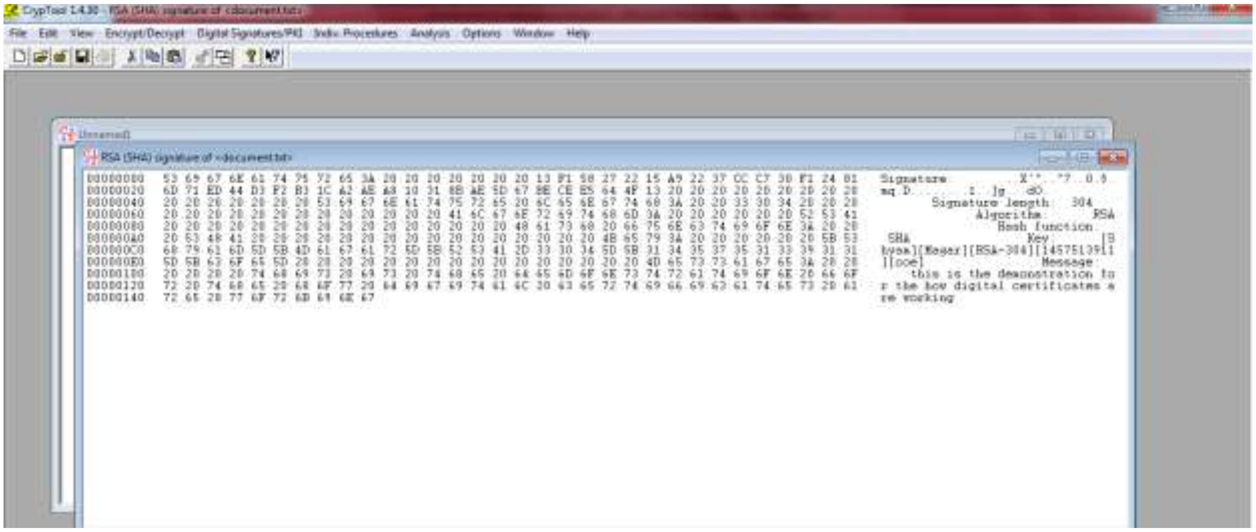
For this purpose you have imported the RSA key together with a certificate from the PSE file: [Shyam][Megan][RSA-304][1457513811][cee].

As the hash function you have selected SHA.

OK

SHA signature of <document.txt>

```
00000  53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 13   Signature:
00012  F1 58 27 22 15 A9 22 37 CC C7 30 F1 24 81 6D 71 ED 44   ñX'".©"7ÌÇ0ñ$ mqíD
00024  D3 F2 B3 1C A2 AE A8 10 31 8B AE 5D 67 BE CE E5 64 4F   Óò³ ¢®¨ 1 ®]g¾ÎådO
00036  13 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53                    S
00048  69 67 6E 61 74 75 72 65 20 6C 65 6E 67 74 68 3A 20 20   ignature length:
0005A  33 30 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   304
0006C  20 41 6C 67 6F 72 69 74 68 6D 3A 20 20 20 20 20 20 52    Algorithm:      R
0007E  53 41 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   SA
00090  48 61 73 68 20 66 75 6E 63 74 69 6F 6E 3A 20 20 20 53   Hash function:   S
000A2  48 41 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   HA
000B4  4B 65 79 3A 20 20 20 20 20 20 5B 53 68 79 61 6D 5D 5B   Key:      [Shyam][
```



```
00000000   53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 20 20 20 13 F1 58 27 22 15 A9 22 37 CC C7 30 F1 24 81   Signature          X''..''7..0.$
00000020   6D 71 ED 44 D3 F2 B3 1C A2 AE A8 10 31 8B AE 5D 67 BE CE E5 64 4F 13 20 20 20 20 20 20 20 20 20   mq.D........1..]g..dO.
00000040   20 20 20 20 20 20 20 53 69 67 6E 61 74 75 72 65 20 6C 65 6E 67 74 68 3A 20 20 33 30 34 20 20 20          Signature length:  304
00000060   20 20 20 20 20 20 20 20 20 20 20 20 20 41 6C 67 6E 72 69 74 68 6D 3A 20 20 20 20 20 20 52 53 41                Algorithm:      RSA
00000080   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 48 61 73 68 20 66 75 6E 63 74 69 6F 6E 3A 20 20                   Hash function:
000000A0   20 53 48 41 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 4B 65 79 3A 20 20 20 20 20 20 5B 53    SHA                Key:      [S
000000C0   68 79 61 6D 5D 5B 4D 61 67 61 72 5D 5B 52 53 41 2D 33 30 34 5D 5B 31 34 35 37 35 31 33 39 31 31   hyam][Magar][RSA-304][1457513911
000000E0   5D 5B 63 6F 65 5D 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 4D 65 73 73 61 67 65 3A 20 20   ][coe]                Message:
00000100   20 20 20 20 74 68 69 73 20 69 73 20 74 68 65 20 64 65 6D 6F 6E 73 74 72 61 74 69 6F 6E 20 66 6F       this is the demonstration fo
00000120   72 20 74 68 65 20 68 6F 77 20 64 69 67 69 74 61 6C 20 63 65 72 74 69 66 69 63 61 74 65 73 20 61   r the how digital certificates a
00000140   72 65 20 77 6F 72 6B 69 6E 67                                                                       re working
```

Conclusion:Hence we demonstrated asymmetric, symmetric crypto algorithm using Jcrypt tool.

6. Kerberos

Aim:To study Kerberos network authentication protocol.

Objective:Students will able to understand Kerberos network authentication protocol.

Theory:-

What is Kerberos?

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.

The Internet is an insecure place. Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by malicious hackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, other client/server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server.

Some sites attempt to use firewalls to solve their network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a very bad assumption. Most of the really damaging incidents of computer crime are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict how your users can use the Internet. (After all, firewalls are simply a less extreme example of the dictum that there is nothing more secure then a computer which is not connected to the network --- and powered off!) In many places, these restrictions are simply unrealistic and unacceptable.

Kerberos was created by MIT as a **solution to these network security problems**. The Kerberos protocol uses **strong cryptography** so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

Kerberos is freely available from MIT, under copyright permissions very similar those used for the BSD operating system and the X Window System. MIT provides Kerberos in source form so that anyone who wishes to use it may look over the code for themselves and assure themselves that the code is trustworthy. In addition, for those who prefer to rely on a professionally supported product, Kerberos is available as a product from many different vendors.

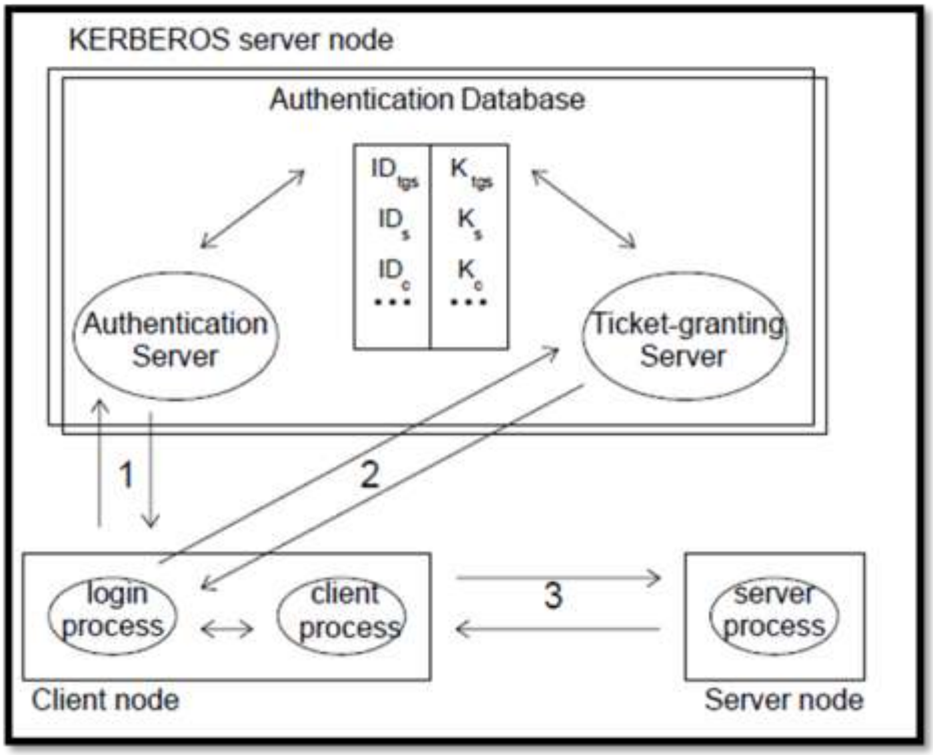
In summary, Kerberos is a solution to your network security problems. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. We hope you find Kerberos as useful as it has been to us. At MIT, Kerberos has been invaluable to our Information/Technology architecture.

Kerberos' architecture

● Kerberos server
● client processes
● application servers

Kerberos' server
● executes in a dedicated, physically secure computer
● encompasses:
○ Authentication database
->stores secret keys of all system's subjects
○ Authentication server (*AS*)
-> certifies the users' identities
○ Ticket-granting server TGS (servidor de bilhetes/emissor de chaves)
->supplies clients with tickets to be used with servers
● it is a KDC, *Key Distribution Center*
Client processes
● execute on “normal” computers
● the user owning client processes is authenticated only once, on log on
● access to services (from application servers) is only possible by means of ticket supplied from Ticket-granting server
Application servers
● execute on networked computers
● each shares a specific key with Ticket-granting server
● only serve clients with tickets proved genuine
Authentication (and key distribution) protocol
● based on Needham-Schroeder's authentication protocol
● so, uses the concept of “tickets”

Ticket
● piece of data delivered to an entity (*A*) to be forwarded, later on, to another (*B*)
● the data is ciphered, to be only understood by the final recipient (*B*)
● typically, contains a session key to be used in conversations between *A* and *B*
○ the whole point is to allow *A* and *B* to authenticate each other, if they both have already authenticated themselves with the Ticket-granting server
...Kerberos' authentication protocol (cont.)
Protocol's structure:
1. user's authentication (*login*) and getting of ticket and key to be used with Ticket-granting server
2. getting of the ticket and key for interaction with an Application server
3. interaction with Application server



...Protocol's structure: interaction details (cont.)

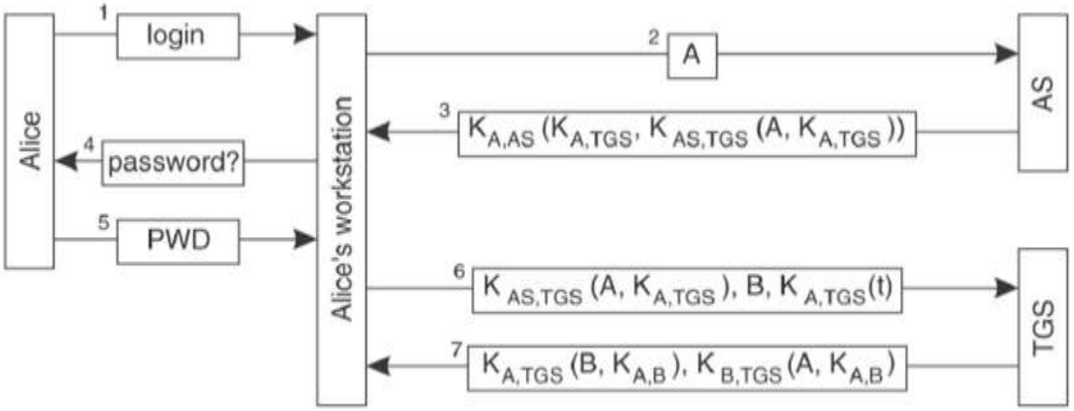

Alice
Alice's workstation
AS
TGS
1 login
2 A
3 $K_{A,AS}(K_{A,TGS}, K_{AS,TGS}(A, K_{A,TGS}))$
4 password?
5 PWD
6 $K_{AS,TGS}(A, K_{A,TGS}), B, K_{A,TGS}(t)$
7 $K_{A,TGS}(B, K_{A,B}), K_{B,TGS}(A, K_{A,B})$

Fig. Kerberos: initial authentication sequence (from *A*), 1-5, and getting of ticket and session key for application server (B), 6-7.

...Protocol's structure: interaction details (cont.)

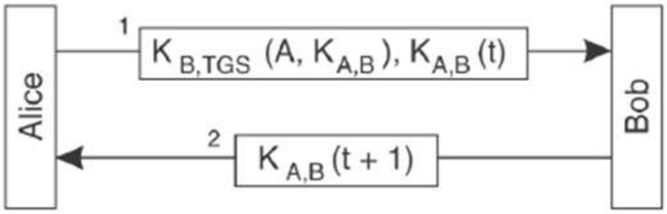


Fig. Kerberos: mutual authentication sequence between Client *A* and server *B*.

Conclusion :-Hence we studied Kerberos network authentication protocol.

8. IT ACT 2000

Aim:To study IT act 2000.

Objective:Student will understand Information technology act 2000

Theory:
As discussed in the first chapter, the Government of India enacted the Information Technology (I.T.) Act with some major objectives to deliver and facilitate lawful electronic, digital, and online transactions, and mitigate cyber-crimes.

Salient Featuresof I.T.Act

The salient features of the I.T. Act are as follows:

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It defines in a new section that *cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public*.
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- It is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that *nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957*.

Scheme of I.T.Act

The following points define the scheme of the I.T. Act:

- The I.T. Act contains **13 chapters** and **90 sections**.
- The last four sections namely sections 91 to 94 in the I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.
- It commences with Preliminary aspect in Chapter 1, which deals with the short, title, extent, commencement and application of the Act in Section 1. Section 2 provides Definition.
- Chapter 2 deals with the authentication of electronic records, digital signatures, electronic signatures, etc.
- Chapter 11 deals with offences and penalties. A series of offences have been provided along with punishment in this part of The Act.
- Thereafter the provisions about due diligence, role of intermediaries and some miscellaneous provisions are been stated.
- The Act is embedded with two schedules. The First Schedule deals with Documents or Transactions to which the Act shall not apply. The Second

Schedule deals with electronic signature or electronic authentication technique and procedure. The Third and Fourth Schedule are omitted.

Application of the I.T.Act

As per the sub clause (4) of Section 1, *nothing in this Act shall apply to documents or transactions specified in First Schedule*. Following are the documents or transactions to which the Act shall not apply:

- **Negotiable Instrument** (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
- A **power-of-attorney** as defined in section 1A of the Powers-of-Attorney Act, 1882;
- A **trust** as defined in section 3 of the Indian Trusts Act, 1882;
- A **will** as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
- Any **contract** for the sale or conveyance of immovable property or any interest in such property;
- Any such class of documents or transactions as may be notified by the Central Government.

Amendments Brought in the I.T.Act

The I.T. Act has brought amendment in four statutes vide section 91-94. These changes have been provided in schedule 1-4.

- The first schedule contains the amendments in the Penal Code. *It has widened the scope of the term "document" to bring within its ambit electronic documents.*
- The second schedule deals with amendments to the India Evidence Act. *It pertains to the inclusion of electronic document in the definition of evidence.*
- The third schedule amends the Banker's Books Evidence Act. *This amendment brings about change in the definition of "Banker's-book". It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device. Similar change has been brought about in the expression "Certified-copy" to include such printouts within its purview.*
- The fourth schedule amends the Reserve Bank of India Act. *It pertains to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institution.*

Intermediary Liability

Intermediary, dealing with any specific electronic records, is a person who on behalf of another person accepts, stores or transmits that record or provides any service with respect to that record.

According to the above mentioned definition, it includes the following:

- Telecom service providers
- Network service providers
- Internet service providers
- Web-hosting service providers
- Search engines
- Online payment sites
- Online auction sites
- Online market places and cyber cafes

Highlights of the AmendedAct

The newly amended act came with following highlights:

- It stresses on privacy issues and highlights information security.
- It elaborates Digital Signature.
- It clarifies rational security practices for corporate.
- It focuses on the role of Intermediaries.
- New faces of Cyber Crime were added.

The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law. The law defines the offenses in a detailed manner along with the penalties for each category of offence.

Offences

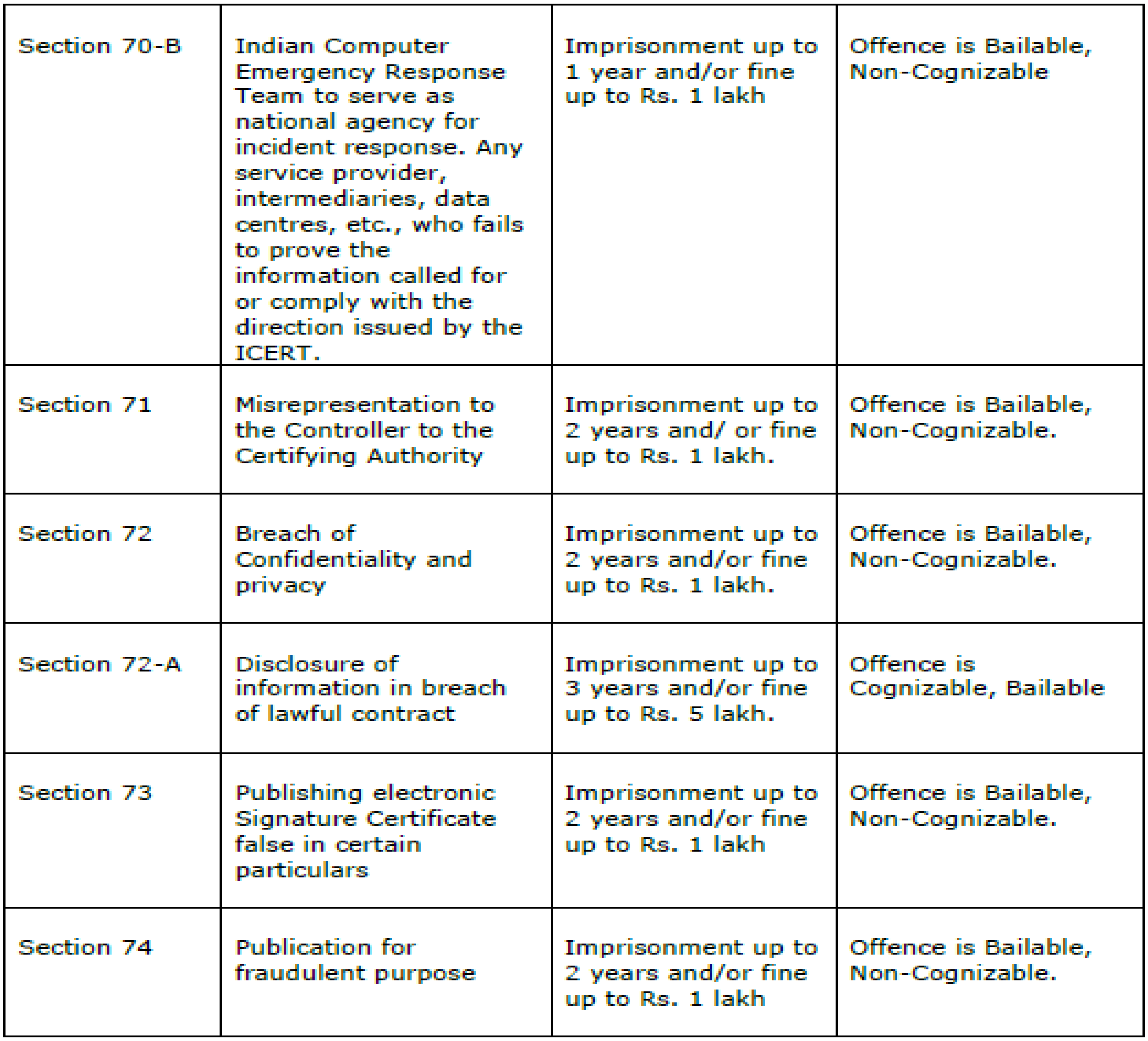
Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.
Cyber-crime usually includes the following:

- Unauthorized access of the computers
- Data diddling
- Virus/worms attack
- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking
- Email bombing
- Salami attacks
- Physically damaging computer system.

The offences included in the I.T. Act 2000 are as follows:

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Section 67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
Section 68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
Section 69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
Section 69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
Section 69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
Section 70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.



Section 70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable
Section 71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
Section 72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
Section 72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
Section 73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
Section 74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

Conclusion: Hence we studied IT act 2000.

10. Implementation of RSA algorithm using any appropriate programming language.

Aim:To implement RSA algorithm using C.

Objective :Students will able to implement RSA algotihm.

Tools required:Turbo C.

Theory:

Program:

```
#include<stdio.h>
#include<conio.h>
#include<stdlib.h>
#include<math.h>
#include<string.h>
long int p,q,n,t,flag,e[100],d[100],temp[100],j,m[100],en[100],i;
char msg[100];
int prime(long int);
void ce();
long int cd(long int);
void encrypt();
void decrypt();
void main() {
        clrscr();
        printf("\nENTER FIRST PRIME NUMBER\n");
        scanf("%d",&p);
        flag=prime(p);
        if(flag==0) {
                printf("\nWRONG INPUT\n");
                getch();
        exit(1);
    }
    printf("\nENTER ANOTHER PRIME NUMBER\n");
    scanf("%d",&q);
    flag=prime(q);
    if(flag==0||p==q) {
        printf("\nWRONG INPUT\n");
        getch();
        exit(1);
    }
    printf("\nENTER MESSAGE\n");
    fflush(stdin);
    scanf("%s",msg);
    for (i=0;msg[i]!=NULL;i++)
    m[i]=msg[i];
    n=p*q;
    t=(p-1)*(q-1);
    ce();
    printf("\nPOSSIBLE VALUES OF e AND d ARE\n");
    for (i=0;i<j-1;i++)
    printf("\n%ld\t%ld",e[i],d[i]);
    encrypt();
    decrypt();
    getch();
}
```

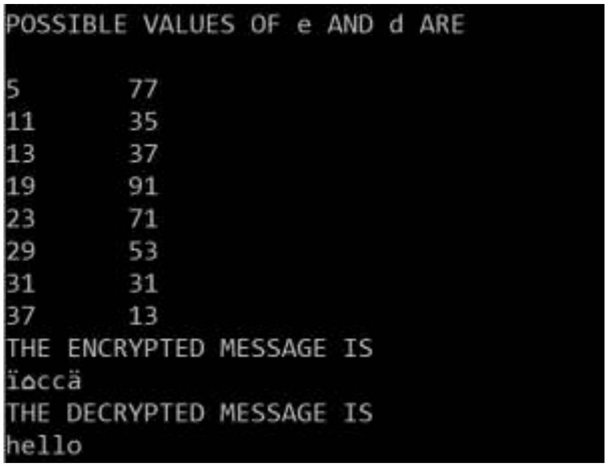
```
int prime(long int pr) {
        int i;
        j=sqrt(pr);
        for (i=2;i<=j;i++) {
                if(pr%i==0)
                   return 0;
        }
        return 1;
}
void ce() {
        int k;
        k=0;
        for (i=2;i<t;i++) {
                if(t%i==0)
                   continue;
                flag=prime(i);
                if(flag==1&&i!=p&&i!=q) {
                        e[k]=i;
                        flag=cd(e[k]);
                        if(flag>0) {
                                d[k]=flag;
                                k++;
                        }
                        if(k==99)
                             break;
                }
```

```
    }
}
long int cd(long int x) {
    long int k=1;
    while(1) {
        k=k+t;
        if(k%x==0)
          return(k/x);
    }
}
void encrypt() {
    long int pt,ct,key=e[0],k,len;
    i=0;
    len=strlen(msg);
    while(i!=len) {
        pt=m[i];
        pt=pt-96;
        k=1;
        for (j=0;j<key;j++) {
            k=k*pt;
            k=k%n;
        }
        temp[i]=k;
        ct=k+96;
        en[i]=ct;
```

```
                i++;
        }
        en[i]=-1;
        printf("\nTHE ENCRYPTED MESSAGE IS\n");
        for (i=0;en[i]!=-1;i++)
        printf("%c",en[i]);
}
void decrypt() {
        long int pt,ct,key=d[0],k;
        i=0;
        while(en[i]!=-1) {
                ct=temp[i];
                k=1;
                for (j=0;j<key;j++) {
                        k=k*ct;
                        k=k%n;
                }
                pt=k+96;
                m[i]=pt;
                i++;
        }
        m[i]=-1;
        printf("\nTHE DECRYPTED MESSAGE IS\n");
        for (i=0;m[i]!=-1;i++)
        printf("%c",m[i]);
}
```

Output:

```
ENTER FIRST PRIME NUMBER

7


ENTER ANOTHER PRIME NUMBER

17


ENTER MESSAGE

hello
```



```
POSSIBLE VALUES OF e AND d ARE

5       77
11      35
13      37
19      91
23      71
29      53
31      31
37      13
THE ENCRYPTED MESSAGE IS
ï⌂ccä
THE DECRYPTED MESSAGE IS
hello
```

Conclusion:Hence we implemented RSA algorithm using C.