ClubHACKMag

1st Indian "HACKING" Magazine

TechGyan
Forensic Analysis of Registry

Mom's Guide
To Secure Wifi at Home

LegalGyan
What is Cyber Law ?

ToolGyan
Using Truecrypt

Issue 1 | Feb 2010

www.clubhack.com

Ladies & Gentleman, Hackers & Geeks, Nerds & Newbies

In India we were waiting to see any 'hacking' magazine to come in life and the wait was getting little longer. So finaly ClubHack decided to come out with its own 1st Indian "Hacking" Magazine called CHmag.

We at ClubHack are very much excited about the magazine and this fits into our main objective of making hacking and information security a common sense for a common man.To start with we have the sections as mentioned in the table of content below. We hope to add a lot of sections in future, all we need is input from you on what would you like to see in your magazine

Moving further we need a lot of help form the whole information security community of the country to make this a success.

Rohit Srivastwa

ClubHACK Mag

Issue 1, Feb 2010.

Team CHmag

Editor
Rohit Srivastwa

Contributing Authors
Abhijeet R Patil
getabhijeetpatil@gmail.com

Varun V Hirve
v.hirve@gmail.com

Pankit Thakkar
princepankit@gmail.com

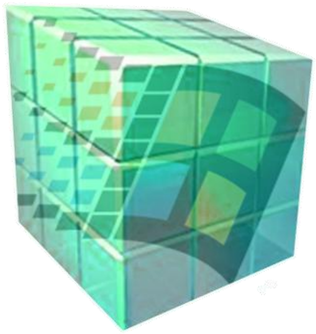
Aarja bhattacharyya
aarja16@gmail.com

Designs
Dipranjan S More
prorider_deep@yahoo.co.in

www.clubhack.com
chmag@clubhack.com

CONTENTS

Forensic Analysis Of Windows XP Registry



Windows XP Registry

Windows stores configuration data in registry. The registry is a hierarchical database, which can also be described as a configuration database. Configuration database consists of the data which is responsible for the functioning of the operating system . The registry is introduced to replace most text-based configuration files used in earlier versions of Windows

operating systems, such as .ini files, autoexec.bat and config.sys files. The registry contains most of Windows XP's settings for all the hardware,

operating system software, non-operating system software, users, etc. Whenever a user makes changes to Control Panel settings, system policies, or installed software, the changes are reflected and stored in registry.

STRUCTURE OF WINDOWS REGISTRY

The default Windows Registry Editor can be opened by typing regedit in the RUN window.

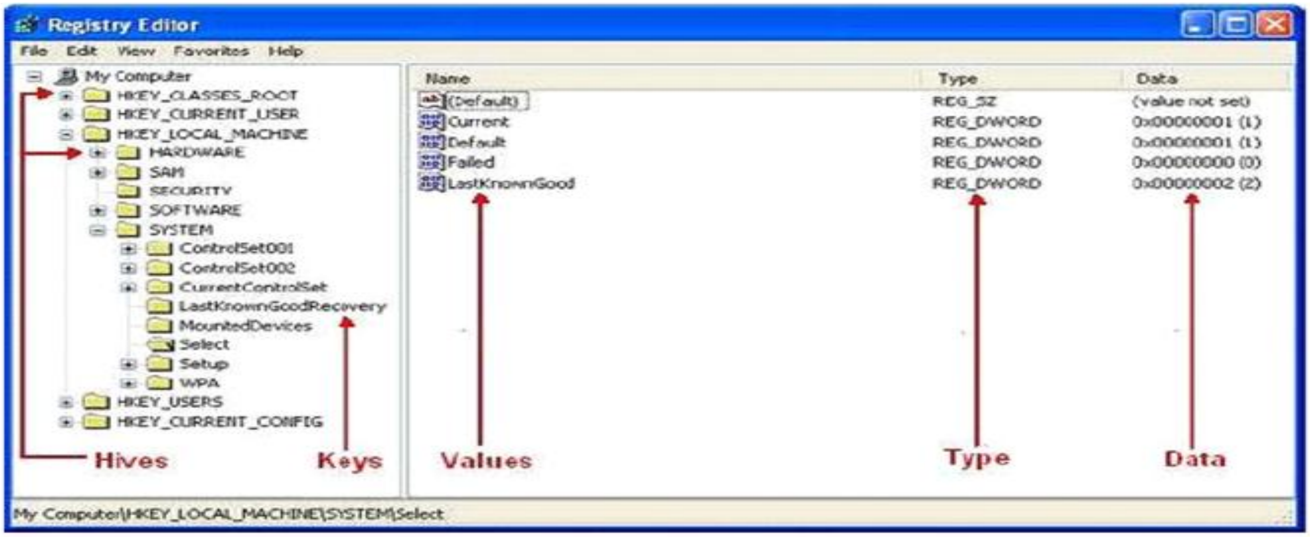
The registry can be seen as one unified "file system". The left hand pane includes (also known as the Key Pane) an organized listing of what appears to be folders. The five most hierarchical folders are called "hives" and begin with "HKEY" (an abbreviation for Handle to a key). Although five hives are visible , only two amongst them are actually "real", which are HKEY_USERS (HKU) and HKEY_LOCAL_MACHINE (HKLM). The other three are shortcuts of two branches within one of the two hives.

Each of these five hives is composed of keys, which contain values and subkeys.

Keys: Registry keys are similar to folders – in addition to values; each key can contain subkeys, which may further contain subkeys, and so on. Keys are referenced with syntax similar to Windows' path names, using backslashes to indicate levels of Hierarchy. E.g. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows.

Values: Values are the names of certain items within a key, which uniquely identify specific values pertaining to the operating system, or to applications that depend upon that value.

Type: Each value's type determines the type of data that it contains. It is like the file extension in Windows Explorer.



```
⊟ My Computer
  ⊞ HKEY_CLASSES_ROOT
  ⊞ HKEY_CURRENT_USER
  ⊟ HKEY_LOCAL_MACHINE
     ⊞ HARDWARE
     ⊞ SAM
       SECURITY
     ⊞ SOFTWARE
     ⊟ SYSTEM
        ⊞ ControlSet001
        ⊞ ControlSet002
        ⊞ CurrentControlSet
          LastKnownGoodRecovery
          MountedDevices
          Select
        ⊞ Setup
        ⊞ WPA
  ⊞ HKEY_USERS
  ⊞ HKEY_CURRENT_CONFIG
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000002 (2)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\Select

Data: Each value can be empty or null or can contain data. The data usually corresponds to the type, except that binary values can contain strings or anything else for that matter.

Below are listed the five hierarchal hives as shown in the figure above, with a brief overview for each.

1. **HKEY_CLASSES_ROOT (HKCR)**

HKCR contains two types of settings. The first is the file associations that associate different types of files with the programs that can open, print, and edit them. The second is class registrations for Component Object Model (COM – which is a Microsoft centric interface standard for software componentry) objects. This root key enables you to change a lot of the operating system's behavior.

2. **HKEY_CURRENT_USER (HKCU)**

HKCU contains the console user's per-user settings. This root key is a link to HKU\SID, where SID in the console user's security identifier. This branch includes environment variables, desktop settings, network configurations, printers, and application preferences.

3. **HKEY_LOCAL_MACHINE (HKLM)**

HKLM contains machine hardware-specific information that the operating system runs on. It includes a list of drives mounted on the system and generic configuration of installed hardware and applications.

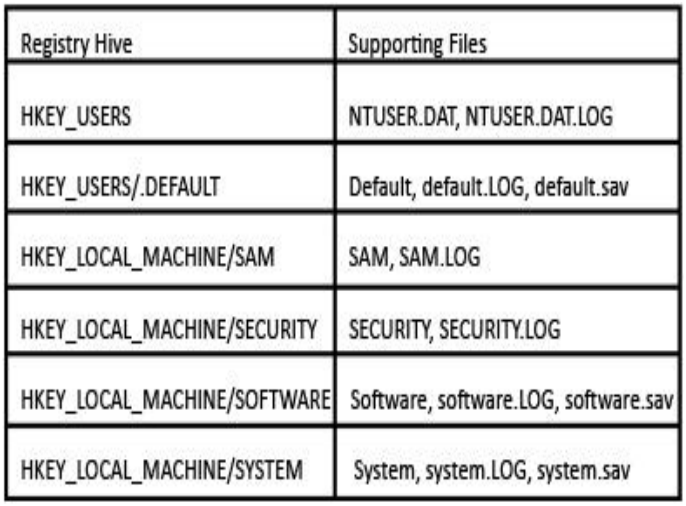
4. **HKEY_USERS (HKU)**

HKU contains configuration of all user profiles on the system, which concerns application configuration, and visual setting.

5. **HKEY_CURRENT_CONFIG (HKCC)**

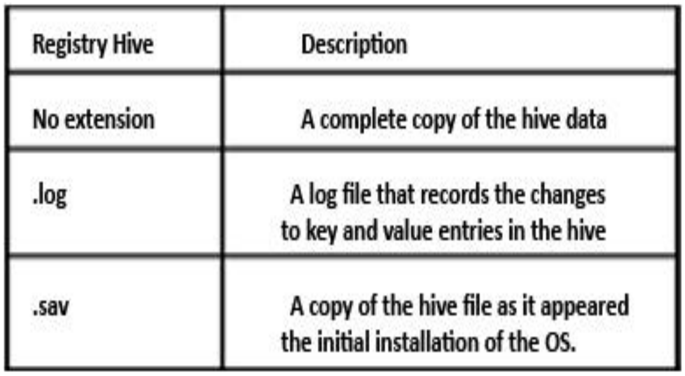
HKCC stores information about the system's current configuration. It's a link to HKLM\Config\profile.

Registry hives and their supporting files:



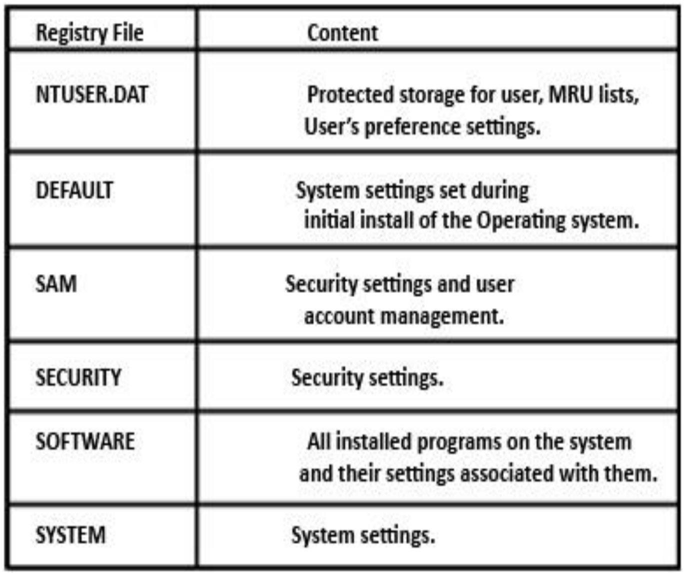
Registry Hive	Supporting Files
HKEY_USERS	NTUSER.DAT, NTUSER.DAT.LOG
HKEY_USERS/.DEFAULT	Default, default.LOG, default.sav
HKEY_LOCAL_MACHINE/SAM	SAM, SAM.LOG
HKEY_LOCAL_MACHINE/SECURITY	SECURITY, SECURITY.LOG
HKEY_LOCAL_MACHINE/SOFTWARE	Software, software.LOG, software.sav
HKEY_LOCAL_MACHINE/SYSTEM	System, system.LOG, system.sav

System file extensions associated with Registry files:



Registry Hive	Description
No extension	A complete copy of the hive data
.log	A log file that records the changes to key and value entries in the hive
.sav	A copy of the hive file as it appeared the initial installation of the OS.

Registry Files and their typical content:



Registry File	Content
NTUSER.DAT	Protected storage for user, MRU lists, User's preference settings.
DEFAULT	System settings set during initial install of the Operating system.
SAM	Security settings and user account management.
SECURITY	Security settings.
SOFTWARE	All installed programs on the system and their settings associated with them.
SYSTEM	System settings.

Importance Of Registry Analysis

The registry is the heart and soul of the Microsoft Windows XP operating system and an exponential amount of information can be derived from it. Due to vast amount of information stored in Windows registry, the registry can be a critical source for potential evidential data.

Registry Keys Of Forensic Values

HKCU\Software\Microsoft\Windows \CurrentVersion\Explorer\ComDlg32 \OpenSaveMRU

MRU is the abbreviation for Most-Recently-Used. This Key maintains a list of recently opened or saved files. Files like **.txt, .pdf, .jpg, .doc, .ppt, .avi etc.** Subkey "*" contains the full file path to the 10 most recently opened/saved files. Other subkey in OpenSaveMRU contains more entries of files which are grouped accordingly to file extension.

HKCU\Software\Microsoft\Windows \CurrentVersion\Explorer\ComDlg32 \LastVisitedMRU

This key correlates to the OpenSaveMRU key to provide extra information. Each binary

registry value under this key contains a recently used program executable filename, and the folder path of a file to which the program has been used to open or save it.

HKCU\Software\Microsoft\Windows \CurrentVersion\Explorer\RecentDo cs

This key also maintains list of files recently executed or opened through Windows Explorer. This key corresponds to %USERPROFILE%\Recent (My Recent Documents). This key contains local or network files that are recently opened and only the filename in binary is stored. It has similar grouping as the previous OpenSaveMRU key, files are organized according to file extension under respective subkeys.

HKCU\Software\Microsoft\Windows \CurrentVersion\Explorer\RunMRU

This key maintains a list of entries (e.g. full path or commands like cmd, regedit, etc) executed using the Start>Run commands. The MRUlist value maintains a list of alphabets which refer to respective values. The alphabets are arranged according to the order the entries are being added.

HKLM\SYSTEM\CurrentControlSet\Session Manager\Memory Management

This key maintains Windows virtual memory (paging file) configuration. The paging file (i.e. pagefile.sys) may contain evidential information that could be removed once the suspect computer is shutdown. This key contains a registry value called ClearPagefileAtShutdown which specifies whether Windows should clear off the paging file when computer shutdowns. By default, Windows will not clear the paging file. However, suspect may modify this registry value to 1 to signify paging file clearing during system shutdown. Forensic investigator should check this value before shutting down a suspect computer during evidence collection process.

HKCU\Software\Microsoft\Search Assistant\ACMru

This key contains recent search terms using Windows default search. Subkey 5603 contains search terms for finding folder and filenames, while subkey 5604 contains terms for finding words or phrases in a file.

HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Uninstall

Each subkey in this key represents an installed program in the software in the computer. Each subkey usually contains these two common registry values – DisplayName (program name) and UninstallString (application Uninstall component's files path, which indirectly refers to application installation path). Other possible useful registry values may exist, which includes information on install date, install source and applications version.

HKCU\Software\Microsoft\Internet Explorer\TypedURLs

This key contains a listing of 25 recent URLs (or file path) that is typed in the Internet Explorer (IE) or Windows Explorer address bar. The key will only show links that are fully typed, automatically completed while typing, or links that are selected from the list of stored URLs in IE address bar. Websites that are accessed via IE Favorites are not recorded. If suspect clears the URL history using Clear History via Internet Options menu, this key will be completely removed.

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

This key also maintains list of files recently executed or opened through Windows Explorer. This key corresponds to %USERPROFILE%\Recent (My Recent Documents). This key contains local or network files that are recently opened and

HKLM\SYSTEM\MountedDevices

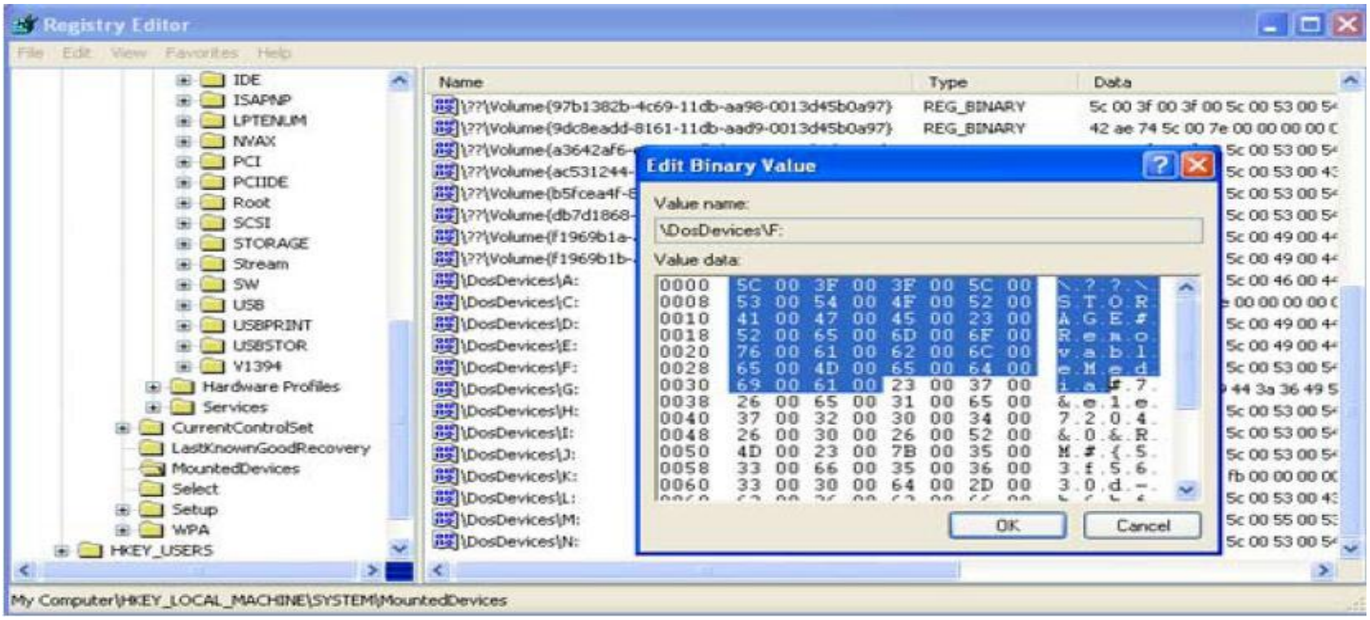
This key makes it possible to view each drive associated with the system. It stores a database of mounted volumes that is used by the NTFS file system. The binary data for each \Dos\Devices\x: value contains information for identifying each volume. This is demonstrated in the figure below, where \DosDevice\F: is a mounted volume and listed as “STORAGE Removable Media”.

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR

Anytime a device is connected to the Universal Serial Bus (USB), drivers are queried and the device’s information is stored in the registry (i.e. thumb drives, cameras etc.). Beneath each of these devices is the Device ID, which is also a serial number. The serial numbers of these devices are a unique value assigned by the manufacturer, much like the MAAC address of a network interface card.But not every thumb drive will have a serial number, particularly those that have an “&” symbol for the second character of the Device ID. For example: 6&1543608a&0.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

This key contains two or more subkeys which have long hexadecimal names that appear as Globally Unique Identifiers (GUIDs). Each subkey record values that pertain to specific objects the user accessed on the system, such as Control Panel applets, shortcuts files, programs, etc. These values however, are encoded using ROT-13 encryption algorithm. This encryption is easy to decipher using online ROT-13 decoder, such as **http://www.edoceo.com/utilis/rot13.php.**



Name	Type	Data
\??\Volume{97b1382b-4c69-11db-aa98-0013d45b0a97}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 53 00 5
\??\Volume{9dc8eadd-8161-11db-aad9-0013d45b0a97}	REG_BINARY	42 ae 74 5c 00 7e 00 00 00 00 0
\??\Volume{a3642af6-		5c 00 53 00 5
\??\Volume{ac531244-		5c 00 53 00 4
\??\Volume{b5fcea4f-8		5c 00 53 00 5
\??\Volume{db7d1868-		5c 00 53 00 5
\??\Volume{f1969b1a-		5c 00 49 00 4
\??\Volume{f1969b1b-		5c 00 49 00 4
\DosDevices\A:		5c 00 46 00 4
\DosDevices\C:		00 00 00 00 0
\DosDevices\D:		5c 00 49 00 4
\DosDevices\E:		5c 00 49 00 4
\DosDevices\F:		5c 00 53 00 5
\DosDevices\G:		44 3a 36 49 5
\DosDevices\H:		5c 00 53 00 5
\DosDevices\I:		5c 00 53 00 5
\DosDevices\J:		5c 00 53 00 5
\DosDevices\K:		fb 00 00 00 0
\DosDevices\L:		5c 00 53 00 4
\DosDevices\M:		5c 00 55 00 5
\DosDevices\N:		5c 00 53 00 5

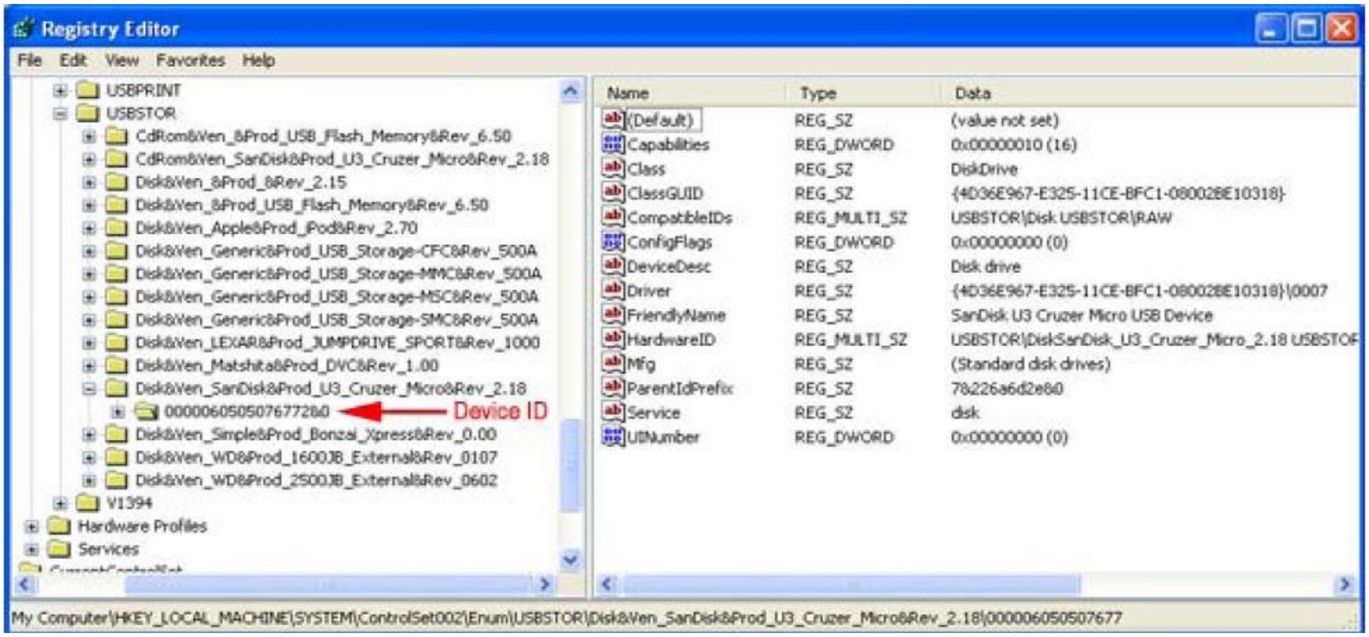
Value name:
\DosDevices\F:

Value data:

```
0000   5C 00 3F 00 3F 00 5C 00   \.?.?.\.
0008   53 00 54 00 4F 00 52 00   S.T.O.R.
0010   41 00 47 00 45 00 23 00   A.G.E.#.
0018   52 00 65 00 6D 00 6F 00   R.e.m.o.
0020   76 00 61 00 62 00 6C 00   v.a.b.l.
0028   65 00 4D 00 65 00 64 00   e.M.e.d.
0030   69 00 61 00 23 00 37 00   i.a.#.7.
0038   26 00 65 00 31 00 65 00   &.e.1.e.
0040   37 00 32 00 30 00 34 00   7.2.0.4.
0048   26 00 30 00 26 00 52 00   &.0.&.R.
0050   4D 00 23 00 7B 00 35 00   M.#.{.5.
0058   33 00 66 00 35 00 36 00   3.f.5.6.
0060   33 00 30 00 64 00 2D 00   3.0.d.-.
```

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

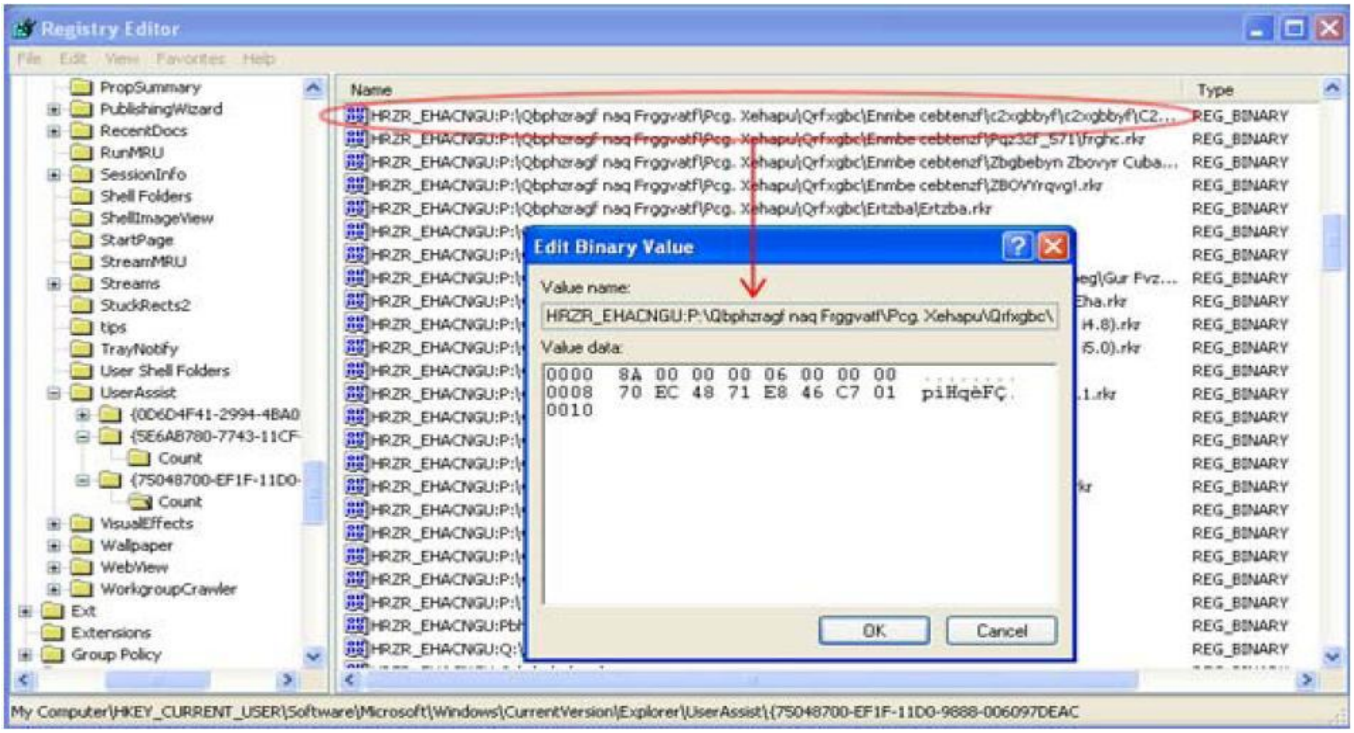
Identification of volume\DosDevice\F:


Registry Editor
File Edit View Favorites Help
USBPRINT
USBSTOR
CdRom&Ven_&Prod_USB_Flash_Memory&Rev_6.50
CdRom&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_2.18
Disk&Ven_&Prod_&Rev_2.15
Disk&Ven_&Prod_USB_Flash_Memory&Rev_6.50
Disk&Ven_Apple&Prod_iPod&Rev_2.70
Disk&Ven_Generic&Prod_USB_Storage-CFC&Rev_500A
Disk&Ven_Generic&Prod_USB_Storage-MMC&Rev_500A
Disk&Ven_Generic&Prod_USB_Storage-MSC&Rev_500A
Disk&Ven_Generic&Prod_USB_Storage-SMC&Rev_500A
Disk&Ven_LEXAR&Prod_JUMPDRIVE_SPORT&Rev_1000
Disk&Ven_Matshita&Prod_DVC&Rev_1.00
Disk&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_2.18
000006050507677280
Device ID
Disk&Ven_Simple&Prod_Bonzai_Xpress&Rev_0.00
Disk&Ven_WD&Prod_1600JB_External&Rev_0107
Disk&Ven_WD&Prod_2500JB_External&Rev_0602
V1394
Hardware Profiles
Services

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000010 (16)
Class	REG_SZ	DiskDrive
ClassGUID	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ConfigFlags	REG_DWORD	0x00000000 (0)
DeviceDesc	REG_SZ	Disk drive
Driver	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}\0007
FriendlyName	REG_SZ	SanDisk U3 Cruzer Micro USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskSanDisk_U3_Cruzer_Micro_2.18 USBSTOR
Mfg	REG_SZ	(Standard disk drives)
ParentIdPrefix	REG_SZ	7&226a6d2e&0
Service	REG_SZ	disk
UINumber	REG_DWORD	0x00000000 (0)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_2.18\000006050507677

Contents of USBSTOR key



```
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Pcg. Xehapu\Qrfxgbc\Enmbe cebtenzf\c2xgbbyf\c2xgbbyf\C2...   REG_BINARY
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Pcg. Xehapu\Qrfxgbc\Enmbe cebtenzf\Pqz32f_571\frghc.rkr      REG_BINARY
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Pcg. Xehapu\Qrfxgbc\Enmbe cebtenzf\Zbgbebyn Zbovyr Cuba...   REG_BINARY
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Pcg. Xehapu\Qrfxgbc\Enmbe cebtenzf\ZBOVYrqvg!.rkr            REG_BINARY
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Pcg. Xehapu\Qrfxgbc\Ertzba\Ertzba.rkr                         REG_BINARY
```

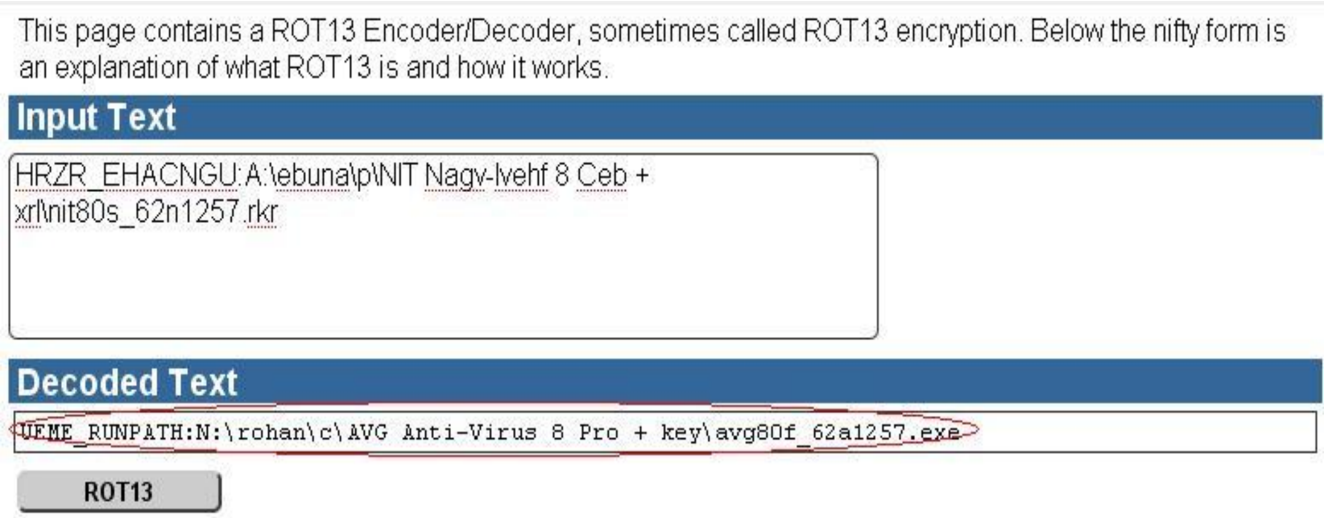
Value name:
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Pcg. Xehapu\Qrfxgbc\

Value data:

```
0000   8A 00 00 00 06 00 00 00   ........
0008   70 EC 48 71 E8 46 C7 01   piHqèFÇ.
0010
```

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEAC

UserAssist Key



This page contains a ROT13 Encoder/Decoder, sometimes called ROT13 encryption. Below the nifty form is an explanation of what ROT13 is and how it works.

Input Text

HRZR_EHACNGU:A:\ebuna\p\NIT Nagv-Ivehf 8 Ceb + xrl\nit80s_62n1257.rkr

Decoded Text

UEME_RUNPATH:N:\rohan\c\AVG Anti-Virus 8 Pro + key\avg80f_62a1257.exe

ROT-13 Cipher Decoded

With the UserAssist key, a forensic examiner can gain a better understanding of what types of files or applications have been accessed on a particular system. Even though these are definitive, for they cannot be associated with a specific date and time, it may still indicate a specific action by the user.

CONCLUSION

Given the popularity of the Windows Operating Systems, it is important for computer forensic experts to understand the complexity of the Windows Registry. The information and potential evidence that exists in the Registry make it a significant forensic resource; uncovering this data can be crucial to any computer related investigation. By understanding the fundamentals of the registry from forensics point of view, an examiner can develop a more accurate account of what occurred on the given machine. This document may not provide conclusive evidence in a registry analysis, but it does present some examples and explanations of what type of data can be found, how they can be found and why they may be relevant to an examination.

REFRENCES

Books

1. Derrick J. Farmer:- A Forensic Analysis of The Windows Registry.
2. Derrick J. Farmer: - A Windows Registry Quick Reference: For the Everyday Examiner.
3. Lih Wern Wong:- Forensic Analysis of The Windows Registry.
4. Peter Davies: - Forensics Analysis of the Windows Registry.

Online

Online ROT-13 Encoder/Decoder: - http://www.edoceo.com/utilis/rot.php

Written By
Abhijeet R Patil

The ease of using a Wireless network is spreading like an ignited fire and everyone is establishing wireless network attheir home or office . The lack of knowledge on wireless security has become a growing concern, due to which ClubHack in past has issued advisories on how to secure your home wifi networks. As a part of the first magazine we'd like to emphasize on the same and help everyone make their wifi networks secure.

Actually securing wifi at home or at a small office is very simple. Anyone can do it with existing wireless device at home and at no extra cost. We request you to follow the simple steps and make your home/office a wifi secured network. At the end of the day it's your network & your privacy which would be on stake.The ease of using a Wireless network is spreading like an ignited fire and everyone is establishing wireless network attheir home or office . The lack of knowledge on wireless security has become a growing concern, due to which **Club Hack** in past has issued advisories on how to secure your home wifi networks. As a part of the first magazine we'd like to emphasizSteps:

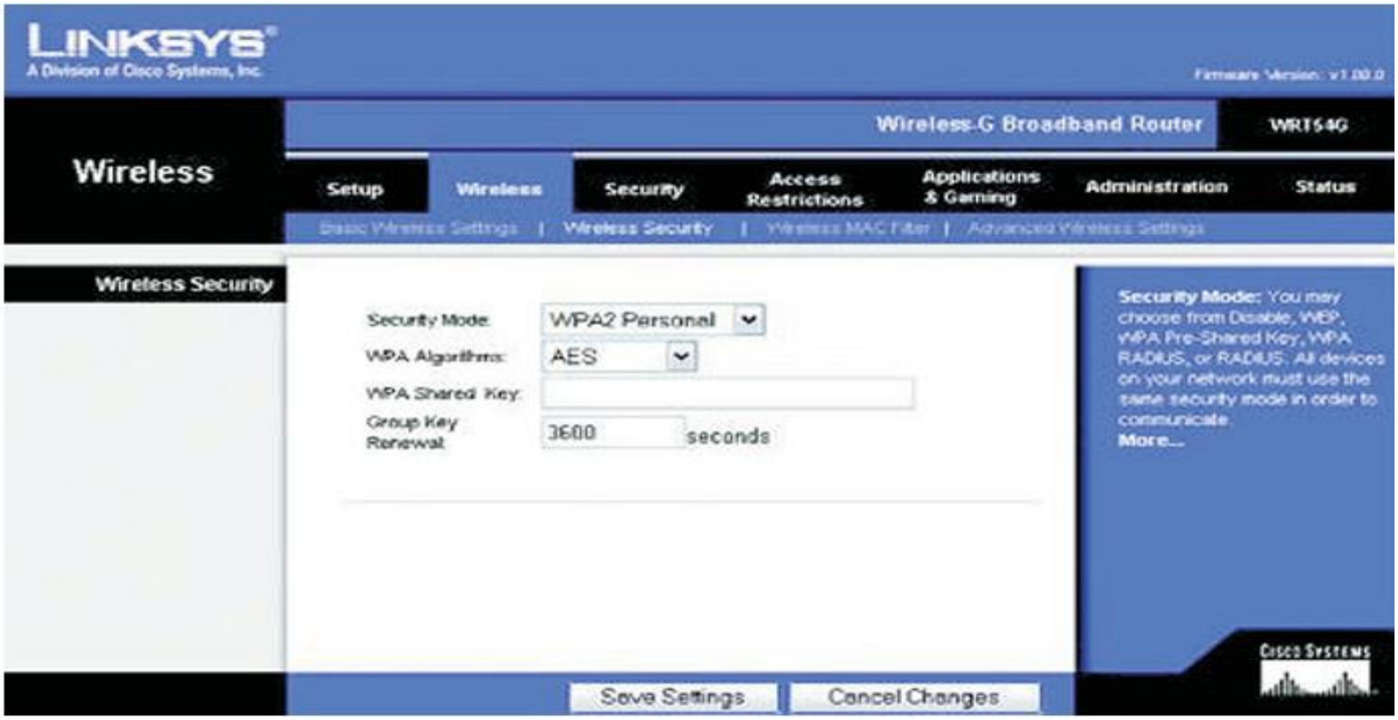
- Open the configuration of your home wifi device. Generally it is done by opening the IP address of your wireless router in the browser like Internet Explorer or Firefox.
- Login to this configuration page and go to device setting
- Change the default password of this device. (we hope you know what is called as strong password)
- Go to wireless setting or wireless security setting
- Select WPA (or WPA-PSK, WPA-Personal, depending on your device model)
- Put a strong password here too.
- Done.

Remember, one should NOT use "WEP" or "OPEN" configuration.

These screenshots of commonly used wireless devices might help you to understand it better and hence secure your network

Obviously in this 100% security is not guaranteed because nothing is 100% secure, but this will surely boost your home wifi security to more than 80% and save you from most of the common attacks on wireless networks.

To secure your wireless network beyond this level you'll have to go for something called as WIPS (Wireless Intrusion Prevention System) which would be little expensive. **Corporate users are advised to go for WIPS solutions to be safe from motivated attacks on their networks.**


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: v1.00.0
Wireless
Wireless-G Broadband Router
WRT54G
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Security
Save Settings
Cancel Changes
Cisco Systems

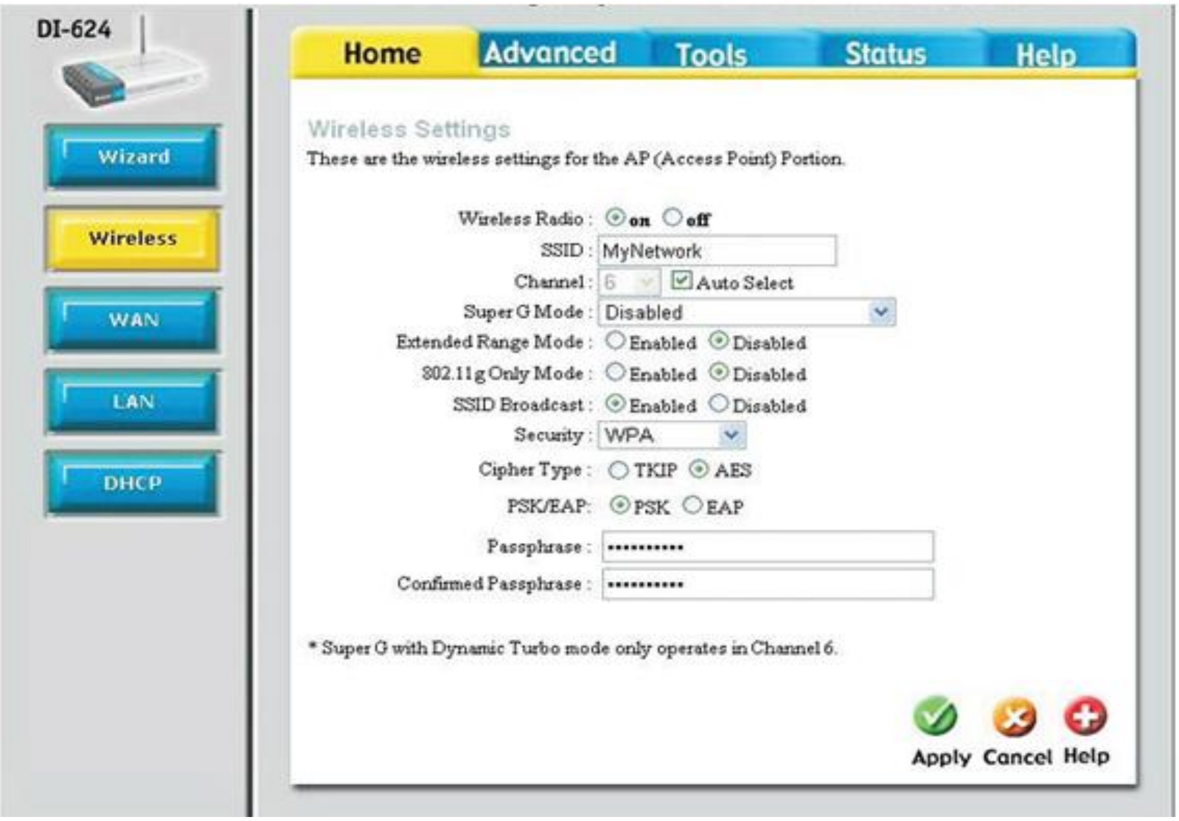
Security Mode: WPA2 Personal

WPA Algorithms: AES

WPA Shared Key:

Group Key Renewal: 3600 seconds

Security Mode: You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate.
More...

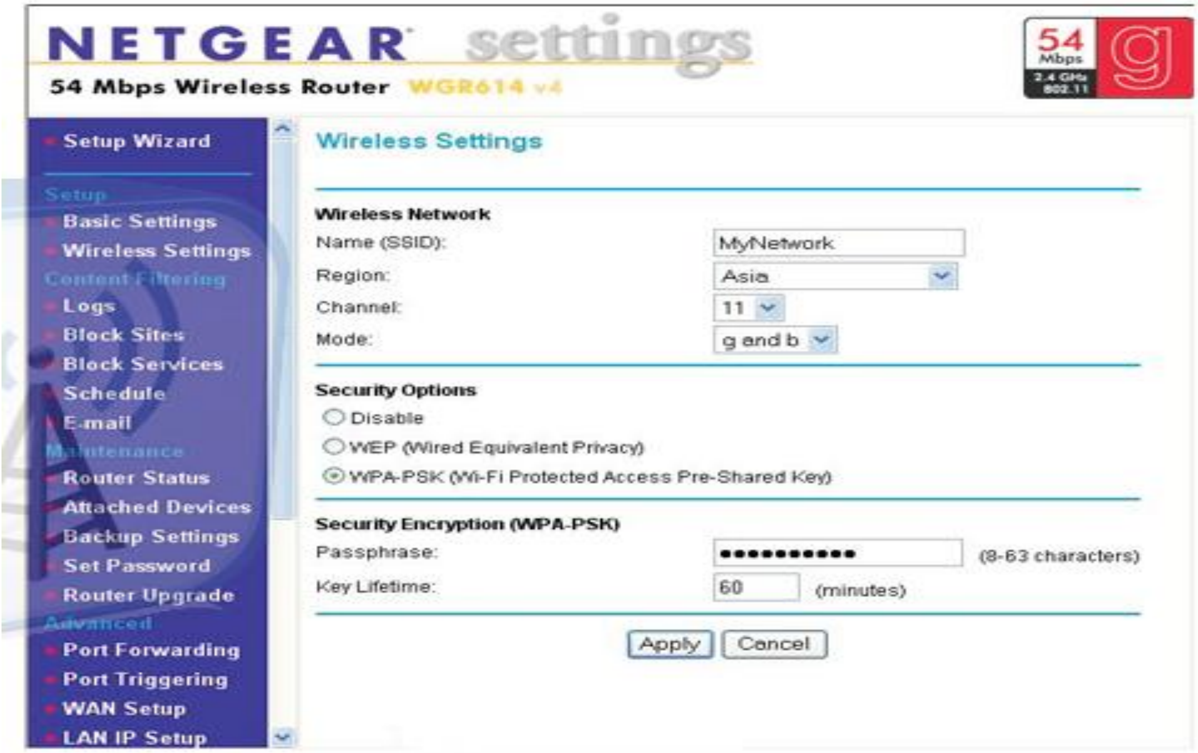


Wireless Settings

These are the wireless settings for the AP (Access Point) Portion.

Wireless Radio : ● on ○ off
SSID : MyNetwork
Channel : 6 ☑ Auto Select
Super G Mode : Disabled
Extended Range Mode : ○ Enabled ● Disabled
802.11g Only Mode : ○ Enabled ● Disabled
SSID Broadcast : ● Enabled ○ Disabled
Security : WPA
Cipher Type : ○ TKIP ● AES
PSK/EAP: ● PSK ○ EAP
Passphrase : ••••••••••
Confirmed Passphrase : ••••••••••

* Super G with Dynamic Turbo mode only operates in Channel 6.



Wireless Settings

Wireless Network
Name (SSID): MyNetwork
Region: Asia
Channel: 11
Mode: g and b

Security Options
○ Disable
○ WEP (Wired Equivalent Privacy)
● WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)

Security Encryption (WPA-PSK)
Passphrase: ••••••••••• (8-63 characters)
Key Lifetime: 60 (minutes)

Online: http://wardrive.in

Written By

Rohit Srivastwa

What is Cyber Law?

In order to arrive at an acceptable definition of the term Cyber Law, we must first understand the meaning of the term law.

Simply put, **law** encompasses the rules of conduct: (1) that have been approved by the government, and (2) which are in force over a certain territory, and (3) which must be obeyed by all persons on that territory. Violation of these rules will lead to government action such as imprisonment or fine or an order to pay compensation.

The term **cyber** or **cyberspace** has today come to signify everything related to computers, the Internet, websites, data, emails, networks, software, data storage devices (such as hard disks, USB disks etc) and even electronic devices such as cell phones, ATM machines etc. Thus a simplified **definition of cyber law** is that it is the "law governing cyber space". The issues addressed by cyber law include:

1. Cyber crime[1]
2. Electronic commerce[2]
3. Intellectual Property in as much as it applies to cyberspace[3]
4. Data protection & privacy[4]

For sake of convenience we shall briefly discuss the development of cyber law around the world under two heads – international measures and national measures

International Measures[5]

[1] An interesting definition of cyber crime was provided in the “Computer Crime: Criminal Justice Resource Manual” published in 1989. According to this manual, cyber crime covered the following:

(1) computer crime i.e. any violation of specific laws that relate to computer crime,

(2) computer related crime i.e. violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution,

(3) computer abuse i.e. intentional acts that may or may not be specifically prohibited by criminal statutes. Any intentional act involving knowledge of computer use or technology is computer abuse if one or more perpetrators made or could have made gain and / or one or more victims suffered or could have suffered loss.

This Manual can be downloaded from **http://www.eric.ed.gov/ERICWebPortal/contentdelivery/servlet/ERICServlet?accno=ED332671**

[2] The term electronic commerce or Ecommerce is used to refer to electronic data used in commercial transactions. Electronic commerce laws usually address issues of data authentication by electronic and / or digital signatures.

[3] This encompasses (1) copyright law in relation to computer software, computer source code, websites, cell phone content etc (2) software and source code licenses (3) trademark law with relation to domain names, meta tags, mirroring, framing, linking etc (4) semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts (5) patent law in relation to computer hardware and software.

[4] Data protection and privacy laws address legal issues arising in the collecting, storing and transmitting of sensitive personal data by data controllers such as banks, hospitals, email service providers etc.

[5] Sources: (1) International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime (2)

The first comprehensive international effort dealing with the criminal law problems of computer crime was initiated by the **Organisation for Economic Co-operation and Development (OECD).[6]**

From 1983 to 1985, an ad hoc committee of OECD discussed the possibilities of an international harmonization of criminal laws in order to fight computer-related economic crime. In September 1985, the committee recommended that member countries consider the extent to which knowingly committed acts in the field of computer-related abuse should be criminalized and covered by national penal legislation.

In 1986, based on a comparative analysis of substantive law, OECD suggested that the following list of acts could constitute a common denominator for the different approaches being taken by member countries:

1. The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit an illegal transfer of funds

or of another thing of value;

2. The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit a forgery;

3. The input, alteration, erasure and/or suppression of computer data and/or computer programs, or other interference with computer systems, made willfully with the intent to hinder the functioning of a computer and/or telecommunication system;

4. The infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program and put in on the market;

5. The access to or the interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions."

From 1985 to 1989, the Select Committee of Experts on Computer-Related Crime of the Council of Europe discussed the legal problems of computer crime. The Select Committee and the European Committee on Crime Problems prepared Recommendation No. R(89)9, which was adopted by the Council on 13 September 1989.

This document "recommends the Governments of Member States to take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime... and in particular the guidelines for the national legislatures".

Twenty countries originally signed the Convention on the Organisation for Economic Co-operation and Development on 14 December 1960. Since then a further ten countries have become members of the Organisation. The Member countries of the Organisation are:
Australia, Austria, Belgium, Canada, Czech republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak republic, Spain, Sweden, Switzerland, Turkey, United Kingdom and United States.

The guidelines for national legislatures include a minimum list, which reflects the general consensus of the Committee regarding certain computer-related abuses that should be dealt with by criminal law, as well as an optional list, which describes acts that have already been penalized in some States, but on which an international consensus for criminalization could not be reached.

The minimum list of offences for which uniform criminal policy on legislation concerning computer-related crime had been achieved enumerates the following offences:

1. **Computer fraud.** The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing that influences the result of data processing, thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person;

2. **Computer forgery.** The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence;

3. **Damage to computer data or computer programs.** The erasure, damaging, deterioration or suppression of computer data or computer programs without right;

4. **Computer sabotage.** The input, alteration, erasure or suppression of computer data or computer programs, or other interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunications system;

5. **Unauthorized access.** The access without right to a computer system or network by infringing security measures;

6. **Unauthorized interception.** The interception, made without right and by technical means, of communications to, from and within a computer system or network;

7. **Unauthorized reproduction of a protected computer program.** The reproduction, distribution or communication to the public without right of a computer program which is protected by law;

8. **Unauthorized reproduction of a topography.** The reproduction without right of a topography protected by law, of a semiconductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semiconductor product manufactured by using the topography.

The optional list relates to the following:

1. **Alteration of computer data or computer programs.** The alteration of computer data or computer programs without right;

2. **Computer espionage.** The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person;

3. **Unauthorized use of a computer.** The use of a computer system or network without right, that either: (i) is made with the acceptance of significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or (ii) is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or (iii) causes loss to the person entitled to use the system or harm to the system or its functioning;

4. **Unauthorized use of a protected computer program.** The use without right of a computer program which is

protected by law and which has been reproduced without right, with the intent, either to procure an unlawful economic gain for himself or for another person or to cause harm to the holder of the right.

In 1990, the legal aspects of computer crime were also discussed by the United Nations, particularly at the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, at Havana, as well as at the accompanying symposium on computer crime organized by the Foundation for Responsible Computing. The Eighth United Nations Congress adopted a resolution on computer-related crime. In its resolution 45/121, the General Assembly welcomed the instruments and resolutions adopted by the Eighth Congress and invited Governments to be guided by them in the formulation of appropriate legislation and policy directives in accordance with the economic, social, legal, cultural and political circumstances of each country. The United Nations Commission on International Trade Law (UNCITRAL) formulated the UNCITRAL Model Law on Electronic Commerce in 1996. The Model Law is intended to facilitate the use of modern means of communication and storage of information. It is based on the establishment of a functional equivalent in electronic media for paper-based concepts such as "writing", "signature" and "original".

The **Convention on Cybercrime** of the Council of Europe is currently the only binding international instrument on the issue of cyber crime. The convention serves as a guideline for countries developing a comprehensive national legislation against Cybercrime. It also serves as a framework for international cooperation between State Parties to the treaty .

The Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.

National Measures

Being at the forefront of computer technology, and being the country that developed what is today referred to as the Internet, the USA has been the global leader in developing laws relating to cyber crime.
In 1977, Senator Abraham Ribicoff introduced the first Federal Systems Protection Act Bill. This evolved into House Bill 5616 in 1986, which resulted in the Computer Fraud and Abuse Act of 1987 established. as Article 1030, Chapter 47 of Title 18 of Criminal Code. The US states of Florida, Michigan, Colorado, Rhode Island and Arizona were the first to have computer crime laws based on the first Ribicoff bill .

Some of the earlier relevant federal legislations include the Communications Fraud and Abuse Act of 1986, the Electronic Communications Privacy Act of 1986, the Credit Card Fraud Act of 1984, the Federal

[7] The signatories to the Convention are: Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

Copyright Act of 1976 and the Wire Fraud Act.

Also relevant are provisions of the Electronic Fund Transfer Act (Title XX of Financial Institutions Regulatory and Interest Rate Control Act of 1978) and the Federal Privacy Act of 1974 (codified in 5 USC Sect. 552a).

Some of the more recent US legislations relevant to cyber law are the 'No Electronic Theft' Act (1997), the Digital Millennium Copyright Act (1998), the Internet Tax Freedom Act (1998), the Child Online Protection Act (1998), the U.S. Trademark Cyberpiracy Prevention Act (1999), the Uniform Electronic Transactions Act (UETA) (1999), the Uniform Computer Information Transactions Act (UCITA) (2000), the Electronic Signatures in Global & National Commerce Act (E-Sign) (2000), the Children's Internet Protection Act (2001) and the USA Patriot Act (2001).

In **China**, the relevant laws are the Computer Information Network and Internet Security, Protection and Management Regulations (1997), the Regulations on Computer Software Protection (2002) and the Criminal Law of the People's Republic of China (1979) as revised in 1997.

In **Australia** the relevant law for cyber crime is the Cybercrime Act (2001) and the revised Criminal Code Act (1995). For electronic commerce, the relevant law is the Electronic Transactions Act 1999. Also relevant is The Commonwealth's Privacy Act (1988).

In **Canada**, the relevant law for cyber crime is the Criminal Code as amended to include computer crimes. For electronic commerce, the relevant law is the Electronic Transactions Act (2001).

In **Malaysia**, the relevant law for cyber crime is the Computer Crimes Act (1997). For electronic commerce, the relevant law is the Digital Signatures Act (1997).

In **Singapore,** the relevant law for cyber crime is the
Computer Misuse Act. For electronic commerce, the relevant law is the Electronic Transactions Act (1998).

In **United Arab Emirates (UAE),** the relevant law for cyber crime is the Federal Law No. 2 of 2006 Combating
Information Technology Crimes. For electronic commerce, the
relevant law is the Law No. 2 of 2002 of the Emirate of Dubai – Electronic Transactions and Commerce Law.

In the **United Kingdom**, the relevant laws for cyber crime are the Forgery and Counterfeiting Act (1981), Computer Misuse Act (1990), Data Protection Act (1998), Terrorism Act (2000), Regulation of Investigatory Powers Act (2000), Anti-terrorism, Crime and Security Act (2001) and Fraud Act (2006).

See "Computer Crime: Criminal Justice Resource Manual" published in 1989, downloadable from: **http://www.eric.ed.gov/ERICWebPortal/contentdelivery/servlet/ERICServlet?accno=ED332671**

For electronic commerce, the relevant laws are the Electronic Communications Act (2000) and the Electronic Signatures Regulations (2002).

In Japan the relevant laws for cyber crime are the Unauthorized Computer Access Law (Law No. 128 of 1999) and the Online Dating Site Regulating Act (June 2008).

In India, the primary legislation for cyber crimes as well as electronic commerce is the Information Technology Act (2000) as amended by the Information Technology (Amendment) Act, 2008. Also relevant for cyber crimes is the amended Indian Penal Code.

Written by

Rohas Nagpal

Command LINE

The real geek loves command line”. We have come across this saying many a times. , it’s the pickup line for geeks. So we are dedicating one section of the magazine for command line fun. Here you’ll be educated (if not already) on the simple usage of command line to fulfill your ‘shell’ dreams. Remember these shortcuts are frequently used in our scripts to make them work more efficiently and effectively. So here we are with

“Command line fun of the month”

As a bonus for the inaugural issue, we present you with two command line funs !!!!

1. Watching the File Count in a Directory

Many a times we feel the need to monitor the increasing (or sometime decreasing) number of flies in a particular directory. In this issue we’ll learn how we can watch the count of files in a particular directory continuously.

1.1.For Windows

```
C:\> for /L %i in (1,0,2) do @dir /b | find /c /v "" & ping -n 6 127.0.0.1>nul
```

This command includes some useful constructs as well:

- The for /L loop, which counts from one to two in steps of zero keeps it running infinitely.
- The /b option makes the dir command drop the garbage from its output (volume name, size, etc.)
- The find /c /v "" means to find, and count (/c) the number of lines that do not have (/v) nothing ("") because even a blank line has a CRLF, so it gets counted.

- And, we ping ourselves 6 times to introduce a 5-second delay. First ping happens instantly, the remaining happen once per second. Vista does have the "timeout /t -[N]" command, but ping is chosen because we wanted it to run on all windows box.
- Remember this will work for the present working directory

Actually dir command, when used like this, doesn't show files that are marked with the system or read-only attributes. To solve this replace the dir /b command with the dir /b /a command, this will show all files regardless of these attributes.

Thus, the resulting command:

```
C:\> for /L %i in (1,0,2) do @dir /b /a | find /c /v "" & ping -n 6 127.0.0.1>nul
```

1.2. For Linux

Everyone would agree that command line activities in Linux are very easy & fun

```
$ while :; do ls | wc -l; sleep 5; done
```

Aren't they ;)

There is another option in Linux using watch command `$ watch -n 5 'ls | wc -l'`

2. Command-Line Ping Sweeper

You can find a lot of ping sweep utilities on internet but the fun & strength lies in relying on what comes as default in any system. Remember someday you might land up on a system where you might not have your favorite set of tools.

2.1. For Windows

Here's a Windows command to do ping sweeps at the command line:

```
C:\> FOR /L %i in (1,1,255) do @ping -n 1 192.168.1.%i | find "Reply"
```

In this example FOR /L loop is a counter. The iterating variable is %i. It starts at 1, goes up by 1 upto 255 in each iteration of the loop. This example is for a /24-sized subnet. In the loop each IP is pinged only once (-n 1) with echo off (@) so that the command ping is not shown in output. The output of ping is then parsed using the find command looking for "Reply". The find command is case sensitive, so put in the cap-R in "Reply". Or, you could use /i to make the find case insensitive.

2.2. For Linux

The ping command in Linux is bit more powerful. Here you have the strength of a broadcast ping which can make the task very easy

```
# ping -b -c 3 255.255.255.255
```

This can do a broadcast ping & the responses can be utilized but unfortunately modern Windows machines don't respond to broadcast pings.

So to take the same approach as in the case of Windows, we can make it look as the following

```
$ for i in `seq 1 255`; do ping -c 1 192.168.1.$i | awk '/1 received/ {print $2}'; done
```

Here same as Windows a variable i goes in loop of 255 & sends a ping request to the IP. The result of the ping is then parsed in awk.

There is one problem in the output of ping in Linux. It generally produces multiline output and we need both beginning as well as ending part of the output to see unique IP as well as positive response of ping. To solve that we can add tr \\n ' ' to make the output a single line and make it easier for awk to understand.

The final command will now look like

```
$ for i in `seq 1 255`; do ping -c 1 192.168.1.$i | tr \\n ' ' | awk '/1 received/ {print $2}'; done
```

Written By
Rohit Srivastwa

TrueCrypt is one of the best tools known to us used for real-time on-the-fly encryption. On-the-fly encryption means encrypting every file as they are getting written on this disk and decrypting as they are being read from the disk. It is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention.

Main Features:

- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- Encrypts an **entire partition or storage device** such as USB flash drive or hard drive.
- Encrypts a **partition or drive where Windows is installed** (pre-boot authentication).

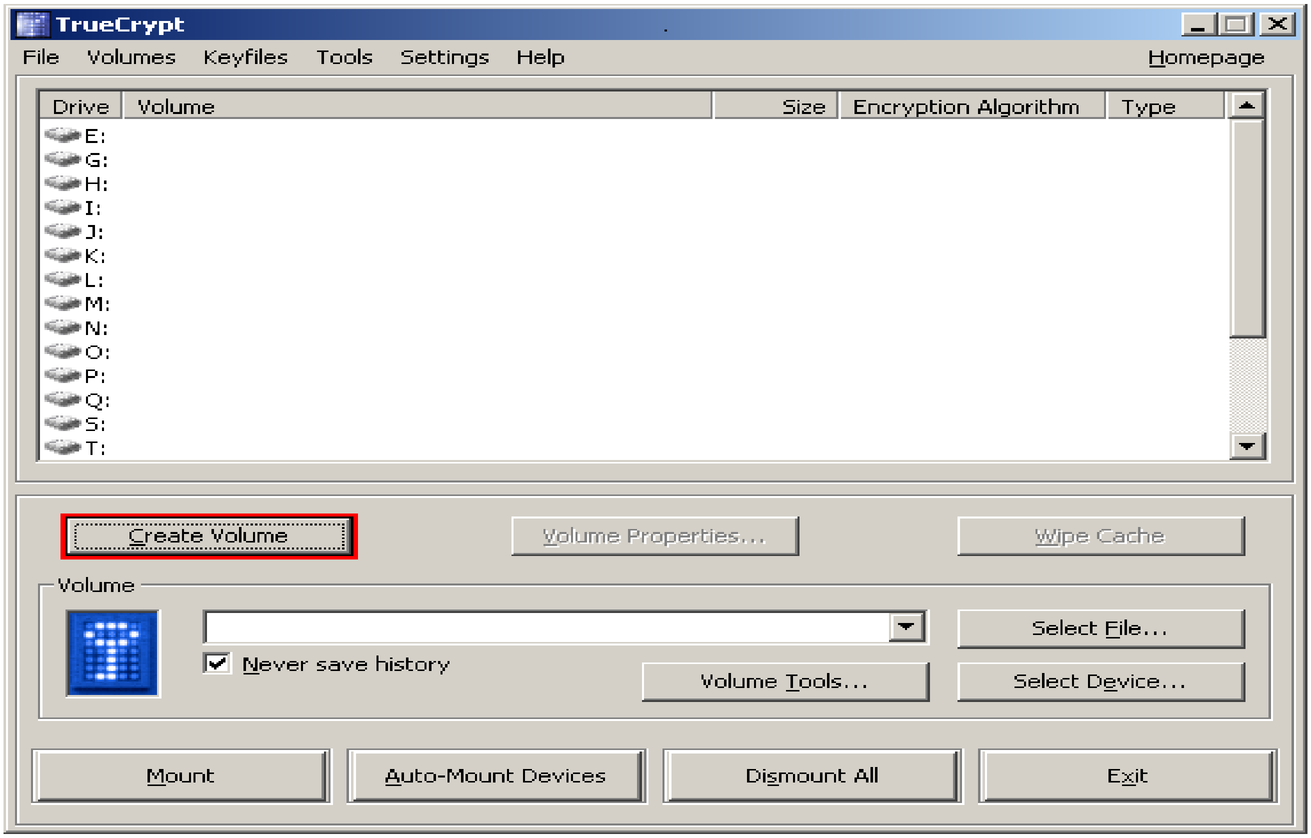
- Encryption is **automatic, real-time** (on-the-fly) and **transparent.**
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
- Provides **plausible deniability**, in case an adversary forces you to reveal the password by using
Hidden volume and **hidden operating system**.
- Encryption algorithms: AES-256, Serpent, and Twofish.

How to make and use TrueCrypt volume?

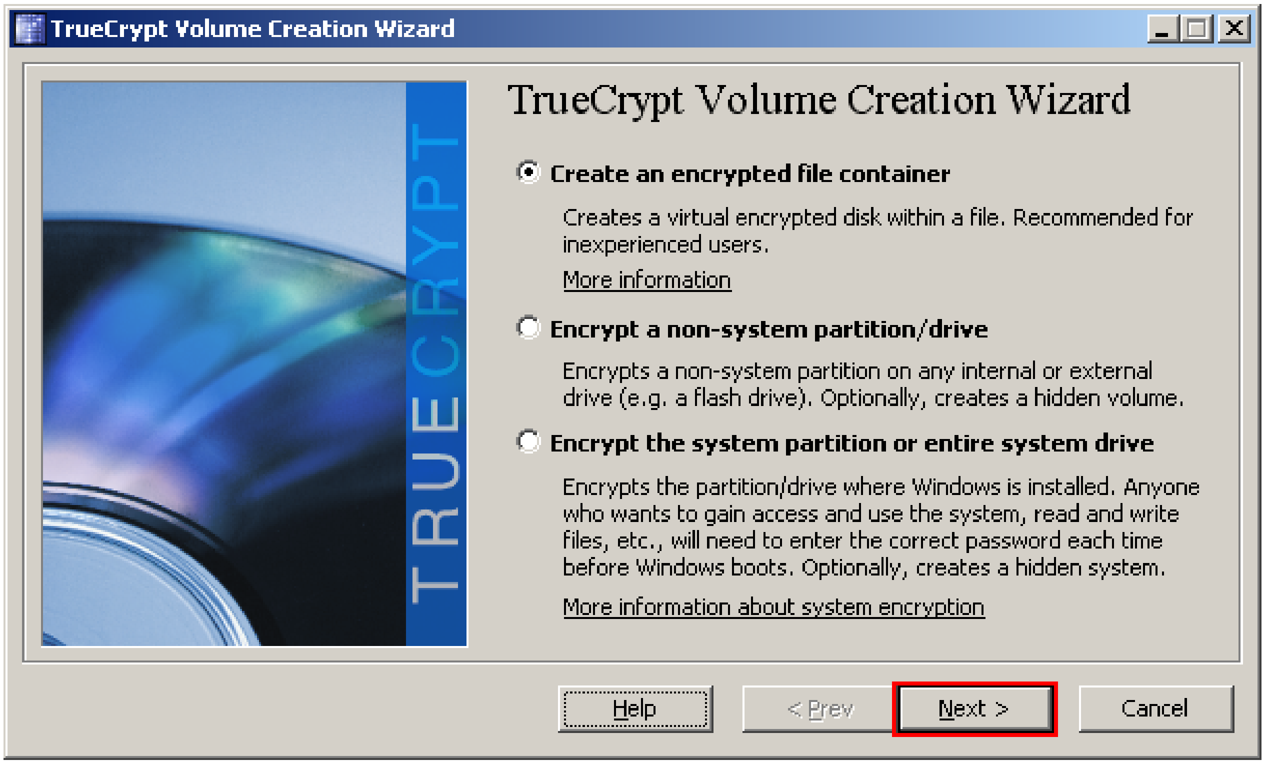
Step 1:
Download and install TrueCryptSetup.exe from http://truecrypt.org

Step 2:
Run TrueCrypt.exe from installed location

In TrueCrypt window, click Create Volume (as shown in the above figure).



Step 3:



TrueCrypt Volume Creation Wizard

● Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ Encrypt a non-system partition/drive

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption

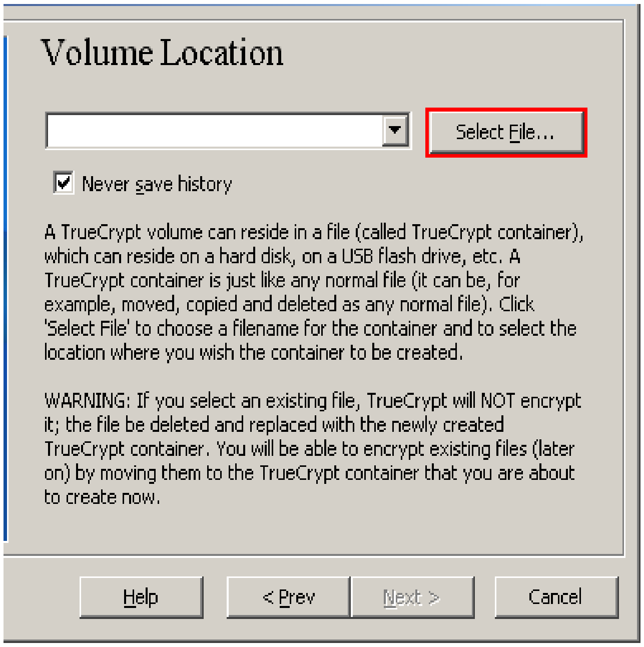
In this step, you need to choose where you wish the TrueCrypt volumeto be created. A TrueCrypt volume can reside in a file, which is also called container
, in a partition. This is where all your secret data lies
On this wizard there are three options. For the sake of this guide we will choose the first option – Create an encrypted file container and create TrueCrypt volume within a file.

Select the first option and click Next
As the option is selected by default, you can just click Next.

Note: In the following steps, the screenshots will show only the right-hand part of the Wizard window.

Step4: Now you need to choose the volume type – Standard or Hidden Volume. We will choose the first option i.e Standard True Crypt. Select it and click Next.

Step5:



Volume Location

☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

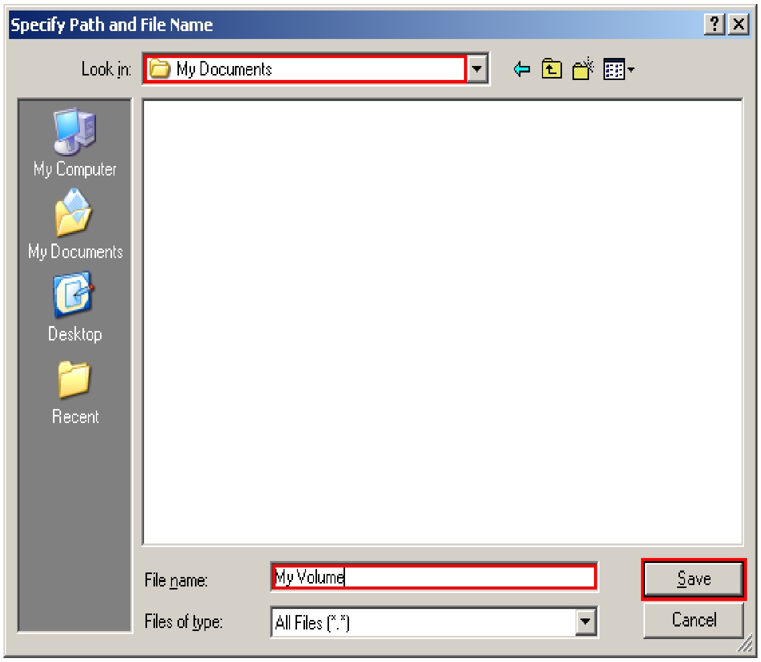
WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

Here you need to specify the location where you want to create TrueCrypt volume (file container).

A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Make sure you keep that file in safe place.

Step6:

We will create our TrueCrypt volume in the folder D:\My Documents\ and the filename of the volume (container) will be My Volume (as can be seen in the screenshot above). You may choose any other filename and location you like (for example, on a USB memory stick). Note that the file My Volume does not exist yet – TrueCrypt will create it. After clicking Save, we will be return to the TrueCrypt Creation Wizard.



Specify Path and File Name

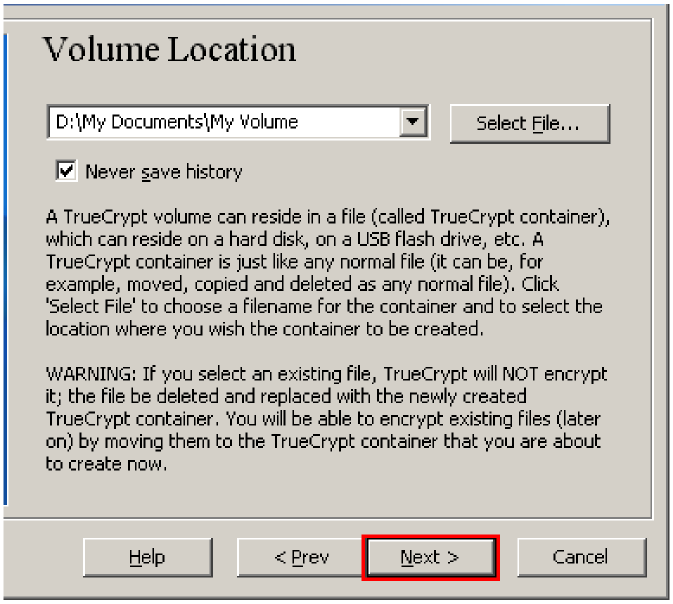
Look in: My Documents

File name: My Volume

Files of type: All Files (*.*)

Step7:

In the Volume Creation Wizard window, Click Next.



Volume Location

D:\My Documents\My Volume

☑ Never save history

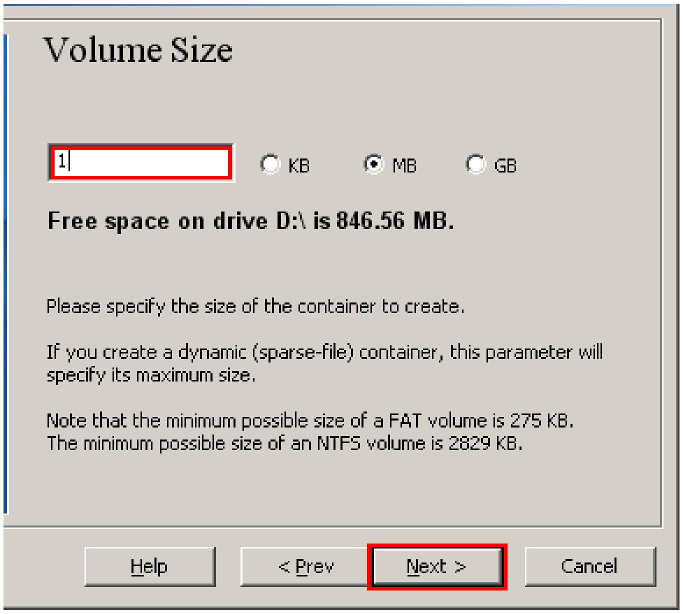
A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

Step9:

Here you need to specify the desired size in the input field.

Click Next.



Volume Size

1 ○ KB ● MB ○ GB

Free space on drive D:\ is 846.56 MB.

Please specify the size of the container to create.

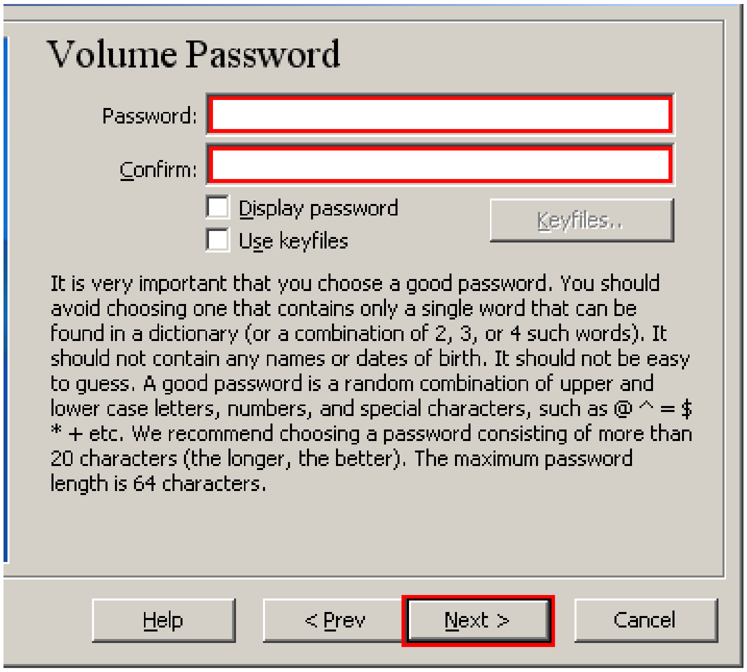
If you create a dynamic (sparse-file) container, this parameter will specify its maximum size.

Note that the minimum possible size of a FAT volume is 275 KB. The minimum possible size of an NTFS volume is 2829 KB.

Step10:

This is the most important step.

You need to choose a good volume password. Read the information given on the screen.After choosing a considerably good password click Next.



Volume Password

Password:

Confirm:

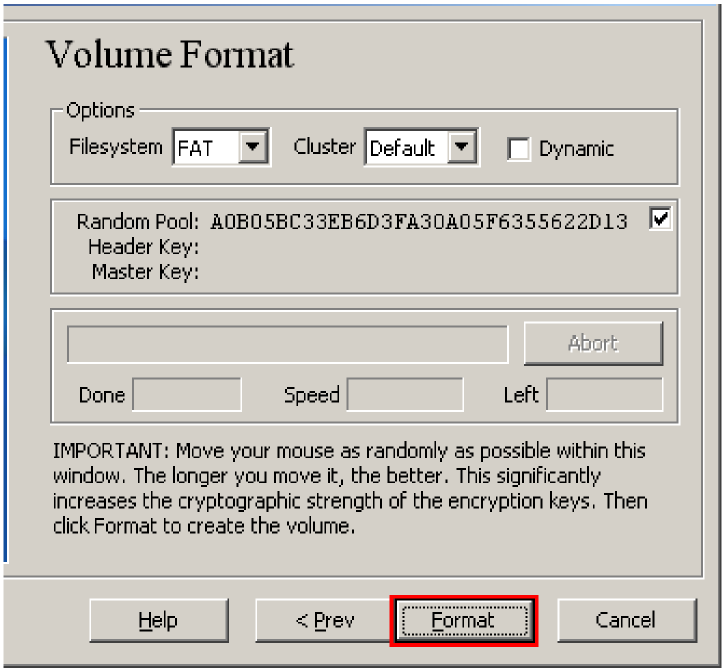
□ Display password

□ Use keyfiles

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum password length is 64 characters.

Step11:
Now you have to move your mouse as randomly as possible within the Volume Creation Wizard Window at least for 30 seconds. This significantly increases the key strength of the encryption keys which, of course, security. What works in background is random number generation based on your mouse coordinates.

Click Format.
Volume creation will begin. Depending upon the size of the volume, the volume creation time may take a long time. After it is finished, following dialog box will appear.



Volume Format

Options

Filesystem: FAT Cluster: Default □ Dynamic

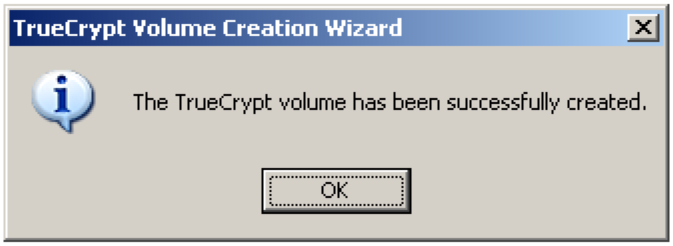
Random Pool: A0B05BC33EB6D3FA30A05F6355622D13 ☑

Header Key:

Master Key:

Done Speed Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

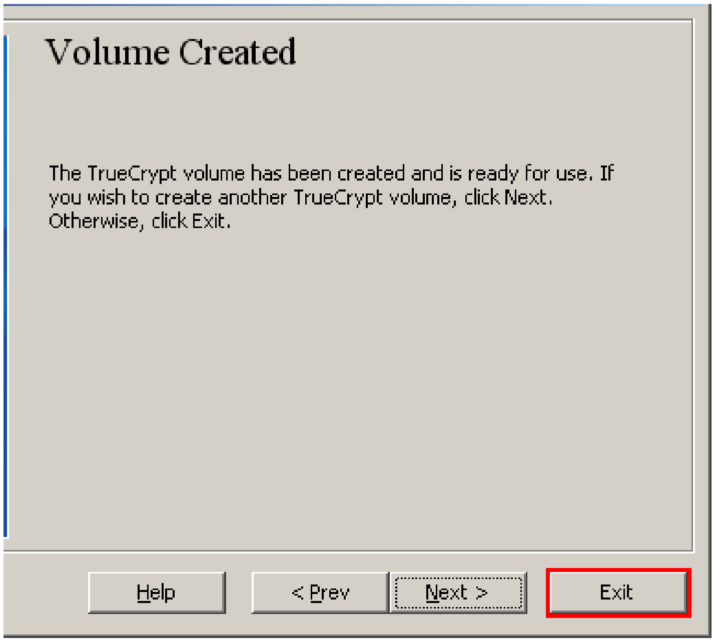


TrueCrypt Volume Creation Wizard

The TrueCrypt volume has been successfully created.

Click Ok to close the dialog box.

Step12:
We have just successfully created a TrueCrypt volume (file container).
In the TrueCrypt Volume Creation Wizard window, click Exit.
The Wizard window should disappear.



Volume Created

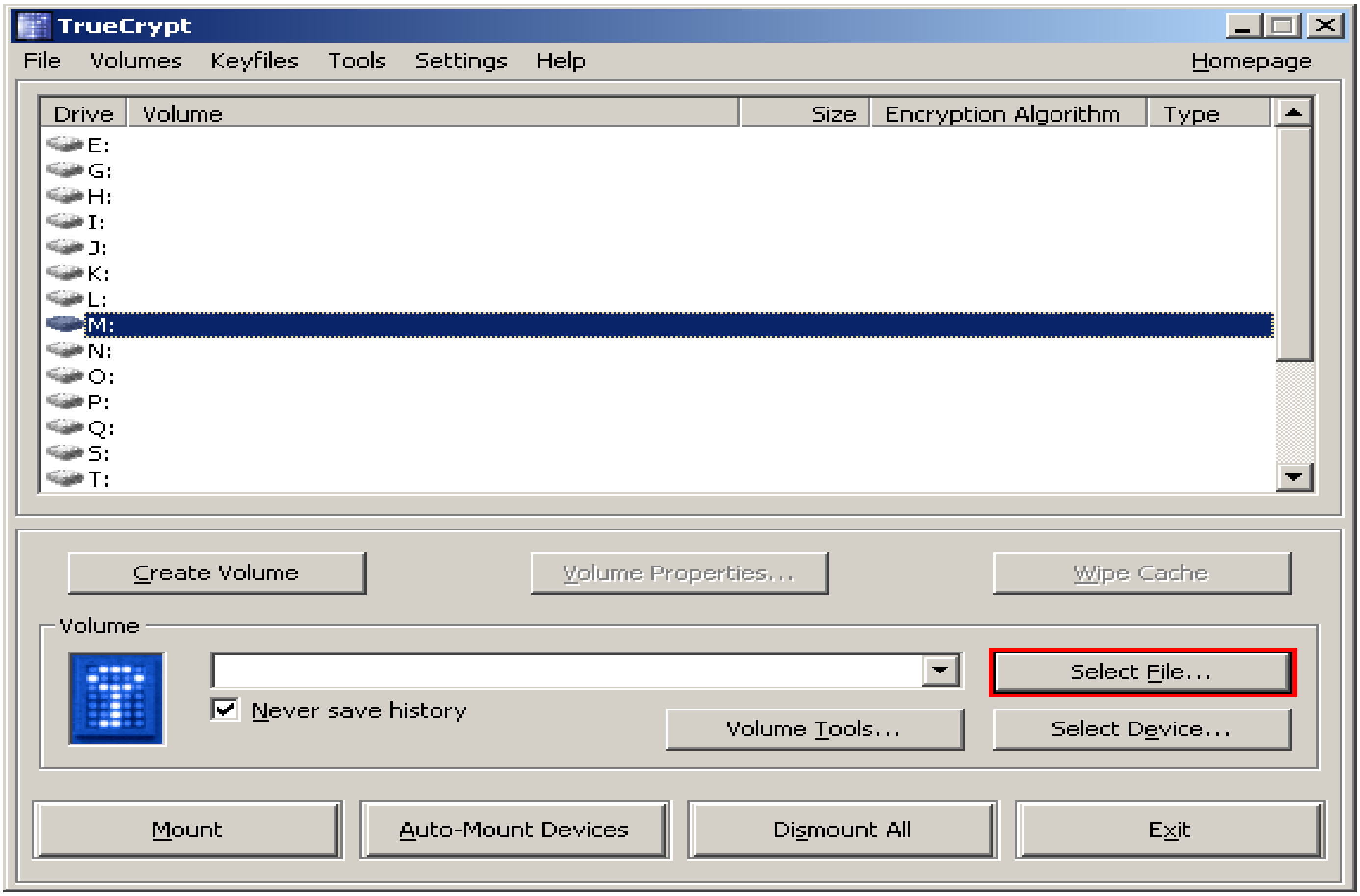
The TrueCrypt volume has been created and is ready for use. If you wish to create another TrueCrypt volume, click Next. Otherwise, click Exit.

Mounting of encrypted drive for use

Now we'll mount the volume we just created to store files. Launch TrueCrypt and continue. This time we'll use same window but for mounting the encrypted drive on a drive letter.

Step1:

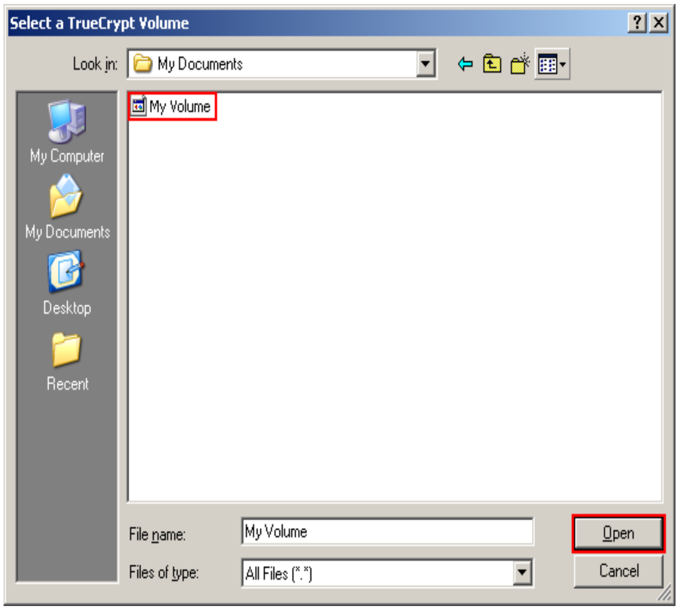
Select a drive letter from the list. This will be the drive letter to which the TrueCrypt container will be mounted.Click Select File. The standard file selector window should appear



☑ Never save history

Step 2:

Here select the container file which we created in Steps 6-11.Click Open. The file selector window should disappear.In the following steps, we will return to the main TrueCrypt window.

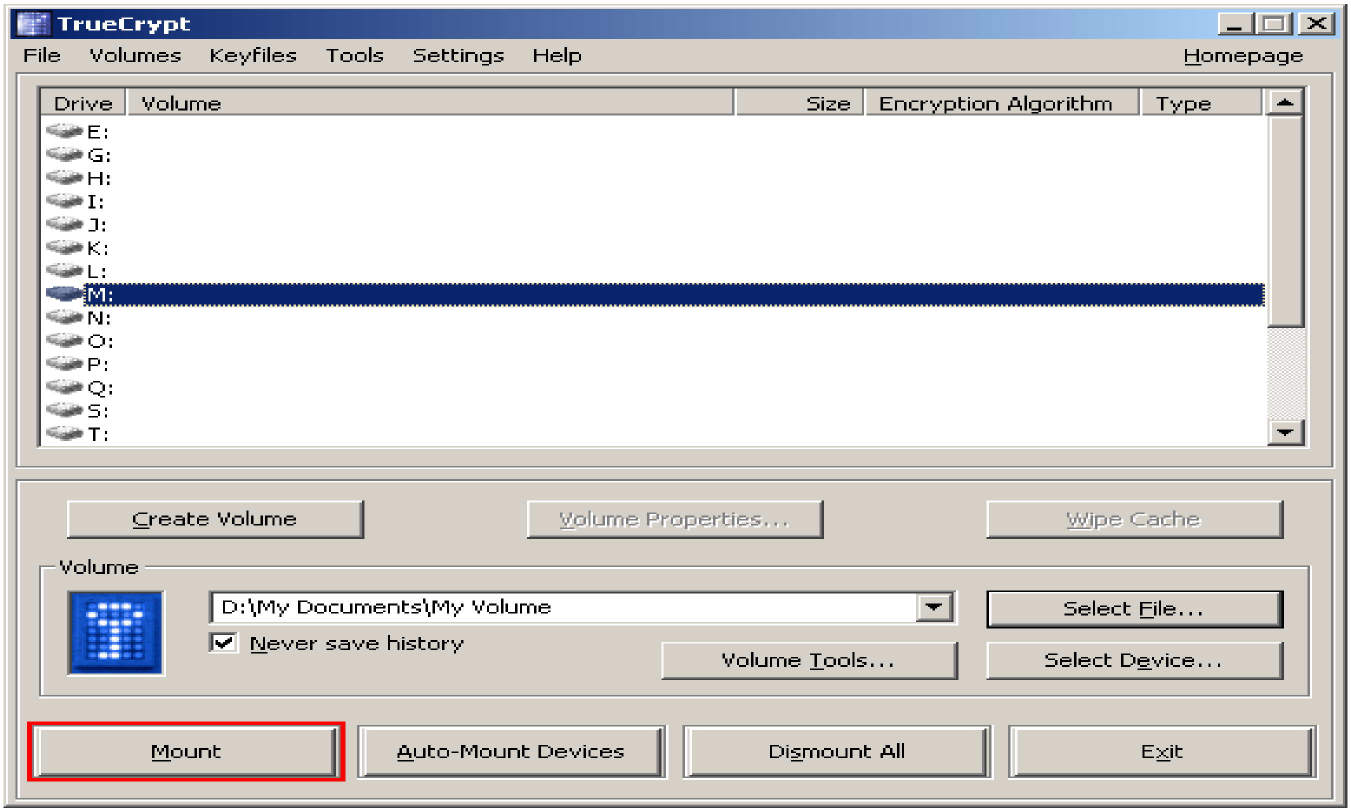


Look in: My Documents

File name: My Volume

Files of type: All Files (*.*)

Step 3:
In the main TrueCrypt window, click Mount.
Password prompt dialog window should appear.

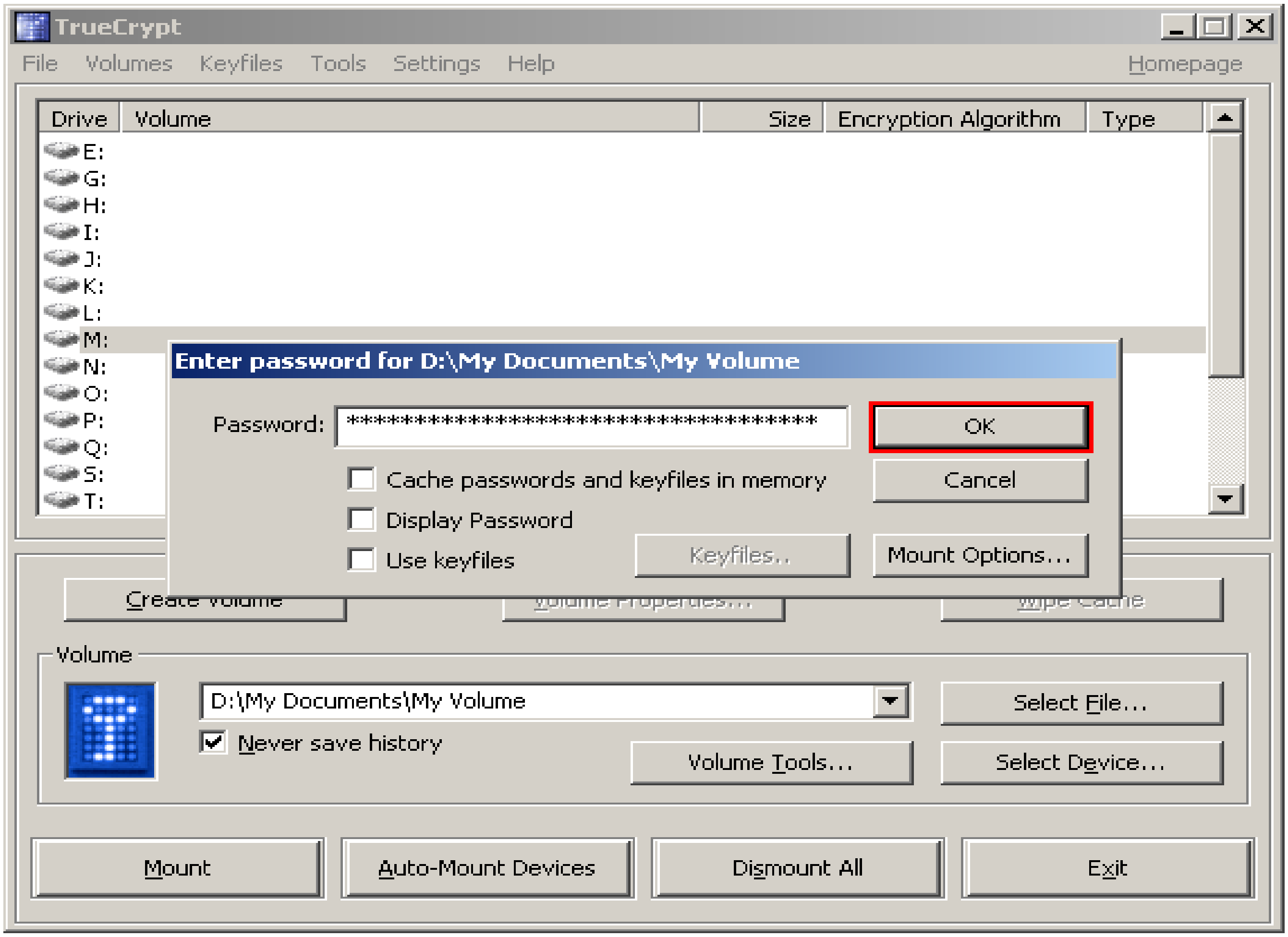


Volume: D:\My Documents\My Volume

☑ Never save history

Step4:
Type the password which you specified in Step 10 above.
Click OK in the password prompt window.

TrueCrypt will now attempt to mount the volume. If the password is incorrect (for example, if you
typed it incorrectly), TrueCrypt will notify you and you will need to repeat the previous step (type
the password again and click OK). If the password is correct, the volume will be mounted.


Enter password for D:\My Documents\My Volume

Password: ************************************

☐ Cache passwords and keyfiles in memory

☐ Display Password

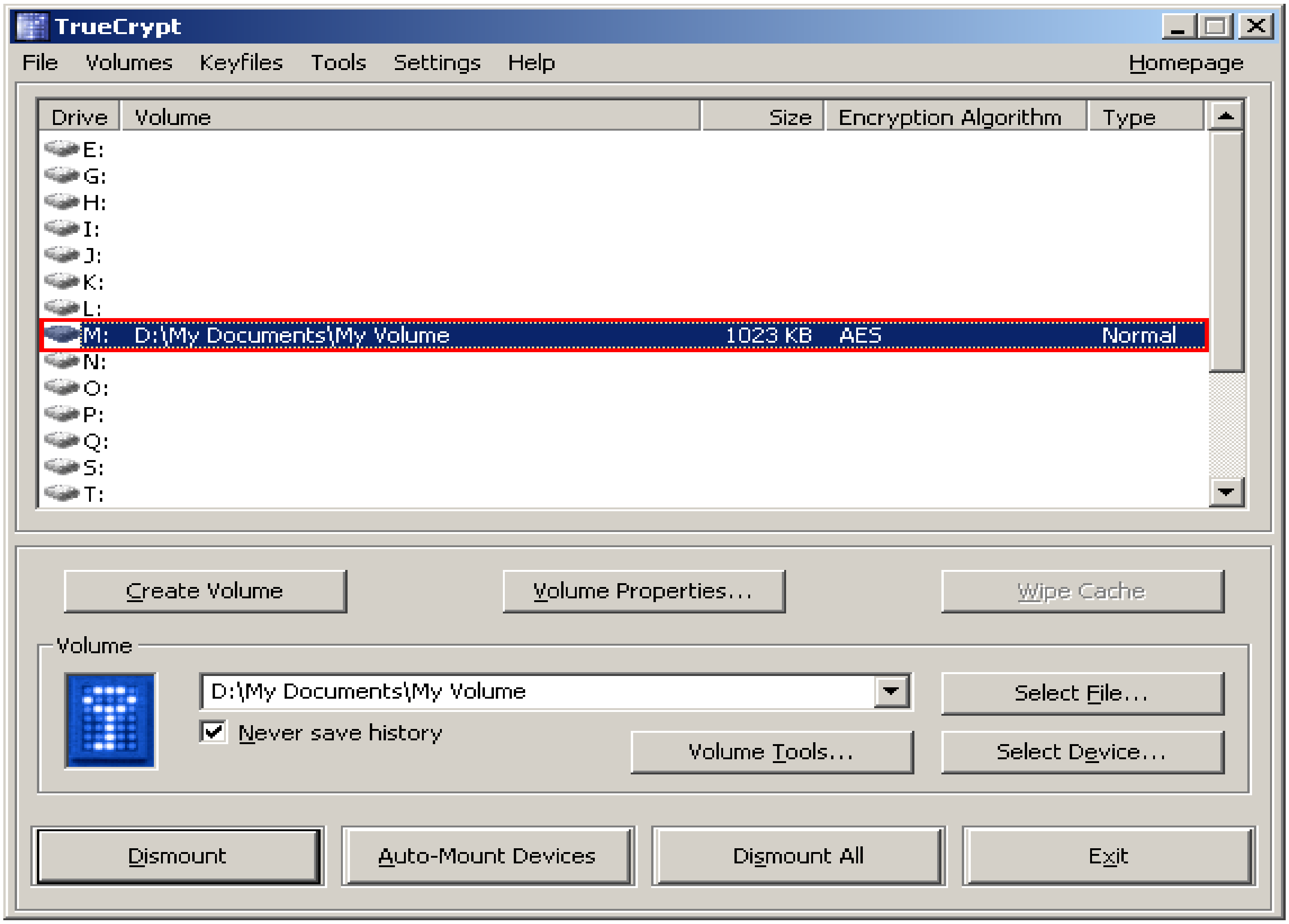
☐ Use keyfiles

Volume: D:\My Documents\My Volume

☑ Never save history

Drive	Volume	Size	Encryption Algorithm	Type
E:				
G:				
H:				
I:				
J:				
K:				
L:				
M:				
N:				
O:				
P:				
Q:				
S:				
T:				

Final Step:



Drive	Volume	Size	Encryption Algorithm	Type
E:				
G:				
H:				
I:				
J:				
K:				
L:				
M:	D:\My Documents\My Volume	1023 KB	AES	Normal
N:				
O:				
P:				
Q:				
S:				
T:				

Volume: D:\My Documents\My Volume

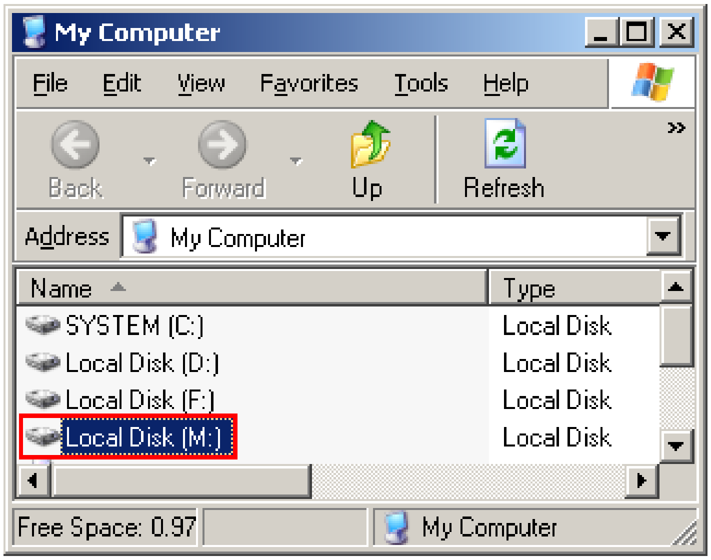
☑ Never save history

We have just successfully mounted the container as a virtual disk M:

The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves like a real disk. You can save (or copy, move, etc.) files to this virtual disk and they will be encrypted on the fly as they are being written. This can also be accessed from any application normaly If you open a file stored on a TrueCrypt volume, the file will be automatically decrypted to RAM (memory) on the fly while it is being read.

The best part is when you write/copy a file to/from the TrueCrypt volume, you will not be asked to enter the password again.

You can also browse to the mounted volume the way you normally browse to any other types of volumes. For example, by opening the 'Computer' (or 'My Computer') list and double clicking the corresponding drive letter (the letter is M in our example).



Address: My Computer

Name	Type
SYSTEM (C:)	Local Disk
Local Disk (D:)	Local Disk
Local Disk (F:)	Local Disk
Local Disk (M:)	Local Disk

Free Space: 0.97 | My Computer

You can copy files to and from the TrueCrypt volume just as you would copy them to any normal disk (for example, by simple drag-and-drop operations). Files that are being read or copied from the encrypted TrueCrypt volume are automatically decrypted on the fly (in memory/RAM).

Similarly, files that are being written or copied to the encrypted TrueCrypt volume are automatically encrypted on the fly (right before they are written to the disk) in RAM.

Note: that TrueCrypt never saves any decrypted data to a disk – it only stores them temporarily in
RAM (memory). Even when the volume is mounted, data stored in the volume is still encrypted.

When you restart Windows or turn off your computer, the volume will be
dismounted and all files
stored on it will be inaccessible (and encrypted). Even when power supply is suddenly interrupted
(without proper system shut down), all files stored on the volume will be
inaccessible (and encrypted). To make them accessible again, you have to mount the volume.

Online
http://truecrypt.org

Written By
Varun V Hirve

Poster of the Month
Dipranjan S More

www.clubhack.com