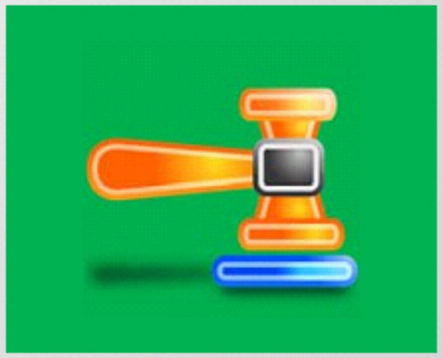
Defeating Anti-forensics Techniques

Module 05

Designed by Cyber Crime Investigators. Presented by Professionals.



Module Objectives

C|HFI Computer Hacking Forensic Investigator

After successfully completing this module, you will be able to:

1. Define anti-forensics and list the goals of anti-forensics
2. Review anti-forensics techniques
3. Extract evidence from deleted files/partitions, password protected files, and stego material
4. Identify trial obfuscation, artifact wiping, data/metadata overwriting, and encryption
5. Identify encrypted network protocols, program packers, rootkits and detection methods
6. Examine different techniques attackers use to avoid detection during investigation
7. Interpret anti-forensics countermeasures
8. Understand challenges faced by Investigators to defeat anti-forensics

What is Anti-Forensics?

- Anti-forensics (also known as counter forensics) is a common term for a set of techniques aimed at **hindering or preventing a proper forensics investigation process**
- They may reduce the quantity and quality of **digital evidence** available

Goals of Anti-Forensics

- To interrupt and prevent information collection
- To make difficult the investigator's task of finding evidence
- To hide traces of crime or illegal activity
- To compromise the accuracy of a forensics report or testimony
- Forcing the forensics tool to reveal its presence
- To use the forensics tool itself for attack purpose
- To delete evidence that an anti-forensics tool has been run

Anti-Forensics Techniques

CHFI Computer Hacking Forensic Investigator

01 Data/File Deletion

02 Password Protection

03 Steganography

04 Data Hiding in File System Structures

05 Trail Obfuscation

06 Artifact Wiping

07 Overwriting Data/Metadata

08 Encryption

09 Encrypted Network Protocols

10 Program Packers

11 Rootkits

12 Minimizing Footprint

13 Exploiting Forensics Tool Bugs

14 Detecting Forensics Tool Activities

Anti-Forensics Techniques: Data/File Deletion

- Covering tracks of their illegal activity is often a concern for intruders. As a part of it, intruders will **delete files** which they believe maybe incriminating

- Investigators can, however, probably get those files back by using various **data recovery tools**, depending on the operating system the computer is running

What Happens When a File is Deleted in Windows?

C|HFI Computer Hacking Forensic Investigator

FAT File System

- The OS replaces the first letter of a deleted file name with a hex byte code: E5h
- E5h is a special tag that indicates that the file has been deleted
- The corresponding cluster of that file in FAT is marked as unused, although it will continue to contain the information until it is overwritten

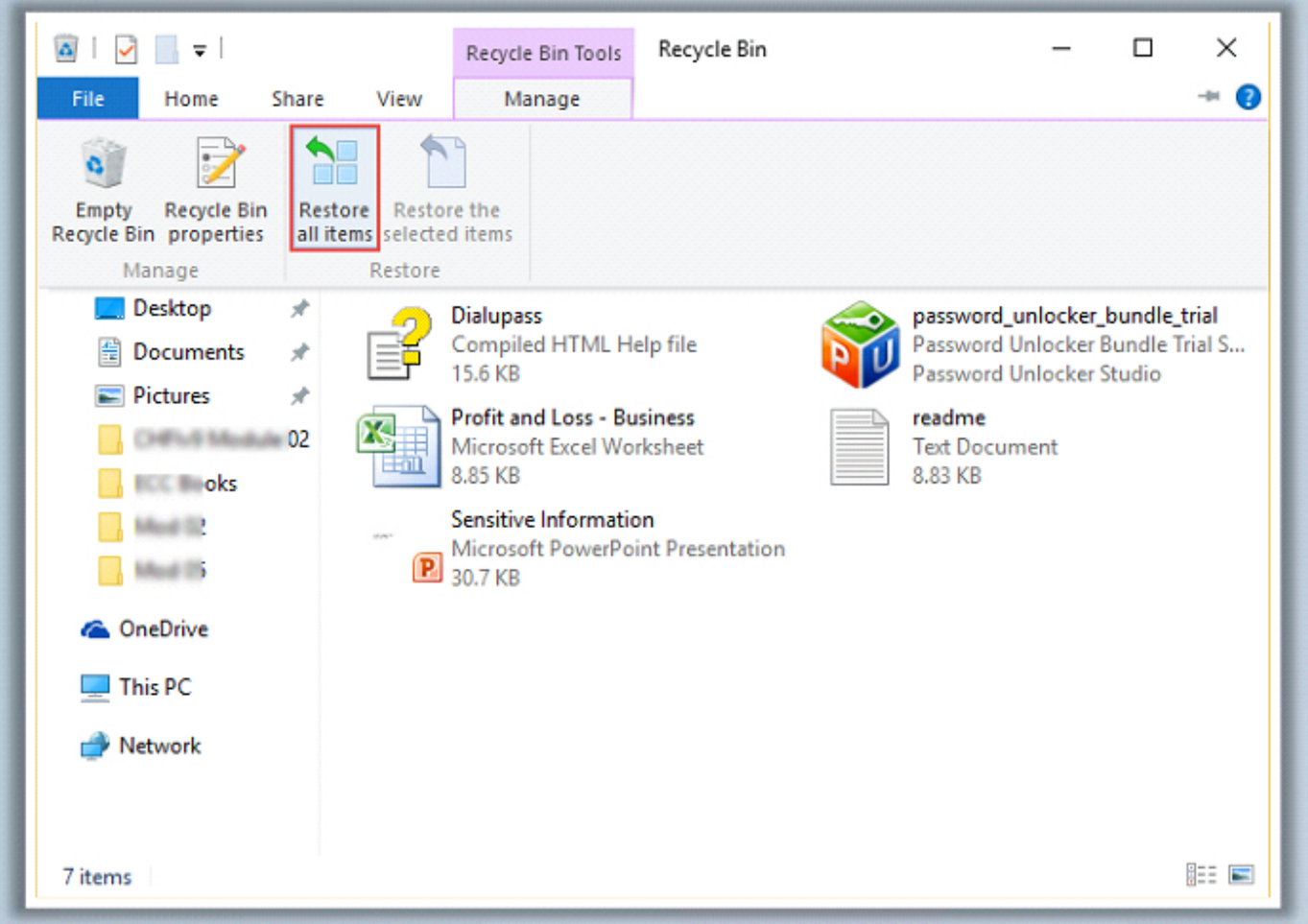
NTFS File System

- When a user deletes a file, the OS marks the file as deleted in the master file table (MFT)
- The clusters allocated to the deleted file are marked as free in the $BitMap ($BitMap file is a record of all used and unused clusters)
- The computer now notices those empty clusters and avails that space for storing a new file
- The deleted file can be recovered if the space is not allocated to any other file

Note: On a Windows system, performing normal **Delete** operation sends the files to the Recycle Bin. Whereas performing the **Shift+Delete** operation bypasses the Recycle Bin.

Recycle Bin in Windows

- The Recycle Bin is a temporary storage place for deleted files, which is located on the Windows desktop
- The file remains in the Recycle Bin until you empty the Recycle Bin or restore the file
- Items can be restored to their original positions with the help of the **Restore all items** option of the Recycle Bin



Note: Deleting a file or folder from a network drive or from a USB drive may delete them permanently instead of being stored in the Recycle Bin

Storage Locations of Recycle Bin in FAT and NTFS Systems

The actual location of the **Recycle Bin** depends on the type of OS and file system. On older FAT file systems (Windows 98 and prior), it is located in **Drive:\RECYCLED**

On NTFS file systems:

On Windows 2000, NT, and XP it is located in **Drive:\RECYCLER**

On Windows Vista and later versions, it is located in **Drive:\$Recycle.Bin**

All recycled files on the FAT system are dumped into a single **C:\RECYCLED** directory, while recycled files on the NTFS system are categorized into directories named as **C:\RECYCLER\S-....** (prior to Windows Vista) and **C:\$Recycle.Bin\S-....** based on the user's Windows Security Identifier (SID)

There is no size limit for Recycle Bin in Vista and later versions of the Windows, whereas in older versions it was limited to a maximum of **3.99 GB**; items larger than the storage capacity of the Recycle Bin cannot be stored in the Recycle Bin

Note: On attaining maximum storage limit of Recycle Bin, the system permanently deletes the oldest files to make space

How the Recycle Bin Works

- Each hard disk has a hidden folder named:
  - **Recycled** (FAT file system - Windows 98 and prior)
  - **Recycler** (NTFS file system - Windows 2000, NT, and XP)
  - **$Recycle.Bin** (NTFS file system - Windows Vista and later versions)
- This folder contains files deleted in Windows Explorer or My Computer, or in Windows-based programs
- Each deleted file in the folder is renamed

1

When a file is deleted, the complete path of the file and its name is stored in a hidden file called INFO or INFO2 (Windows 98) in the Recycled folder. This information is used to restore the deleted files to their original locations.

2

Prior to Windows Vista, a file in the Recycle Bin was stored in its physical location and renamed as Dxy.ext

- D denotes that a file has been deleted
- x is the letter of the drive where the file is located
- y denotes a sequential number starting from 0
- .ext denotes the original file extension, such as .doc or .pdf

Since the advent of Windows Vista, the metadata of each file is saved as $I<number>.<original extension> and the original file is renamed to $R<number>.<original extension>

3

How the Recycle Bin Works (Cont'd)

- Prior to Windows Vista, the deleted file was renamed using the syntax:

  `D<original drive letter of file><#>.<original extension>`

- Example:

  De7.doc = (File is deleted from E drive, it is the eighth file received by recycle bin, and is a doc file)

- The information about the deleted file is stored in a master database file named INFO2 located at `C:\Recycler\<USER SID>\`
- INFO2 contains:
  - Original file name
  - Original file size
  - The date and time the file was deleted
  - The files unique identifying number in the recycle bin
  - The drive number that the file came from

- In Windows Vista and later versions, the deleted file is renamed using the syntax:

  `$R<#>.<original extension>`, where <#> represents a set of random letters and numbers

- At the same time, a corresponding metadata file is created which is named as:

  `$I<#>.<original extension>`, where <#> represents a set of random letters and numbers the same as used for $R

- The $R and $I files are located at `C:\$Recycle.Bin\<USER SID>\`
- $I file contains:
  - Original file name
  - Original file size
  - The date and time the file was deleted

Damaged or Deleted INFO2 File

1. If the INFO2 file is damaged or deleted, no file appears in the Recycle Bin
2. The files in the Recycled folder have been renamed
3. If the INFO2 file is deleted, it is re-created when you restart Windows
4. The INFO2 file is a hidden file. To delete the INFO2 file, follow these steps:
   - Open a command prompt window
   - Type `cd C:\RECYCLER\S-..User SID` (Change directory to Recycle Bin folder)
   - Type `attrib -h info*`
   - Type `del info2`

Damaged Files in Recycle Bin Folder

- Damaged files in the Recycle Bin folder (**C:\RECYCLER, C:\RECYCLER\S-...** or **C:\$Recycle.Bin\S-....**) do not appear in the Recycle Bin
- To restore the deleted files, follow this process:

1. **Create a copy of the Desktop.ini file in the Recycle Bin folder and save it in an another folder**
2. **Delete all files in the Recycle Bin**
3. **Restore the Desktop.ini file to the Recycle Bin folder**
4. **If the Desktop.ini file is not present or is damaged, you can re-create it by adding the following information to a blank Desktop.ini file:**

```
[.ShellClassInfo]CLSID={645FF040-5081-101B-9F08-00AA002F954E}
```

Damaged Recycle Bin Folder

- The Recycle Bin folder itself can **be damaged**
- Files are **moved** to the folder, and the Recycle Bin appears full, but you cannot view the contents and the "**Empty The Recycle Bin**" command is unavailable
- **Deleting** this folder and **restarting** Windows will re-create this folder and **restore functionality**:

  In Windows, prior to Vista:

  - Open a command prompt with administrative privileges
  - Type attrib -s -h recycler (the Recycle Bin folder)
  - Type del recycler
  - Restart the computer

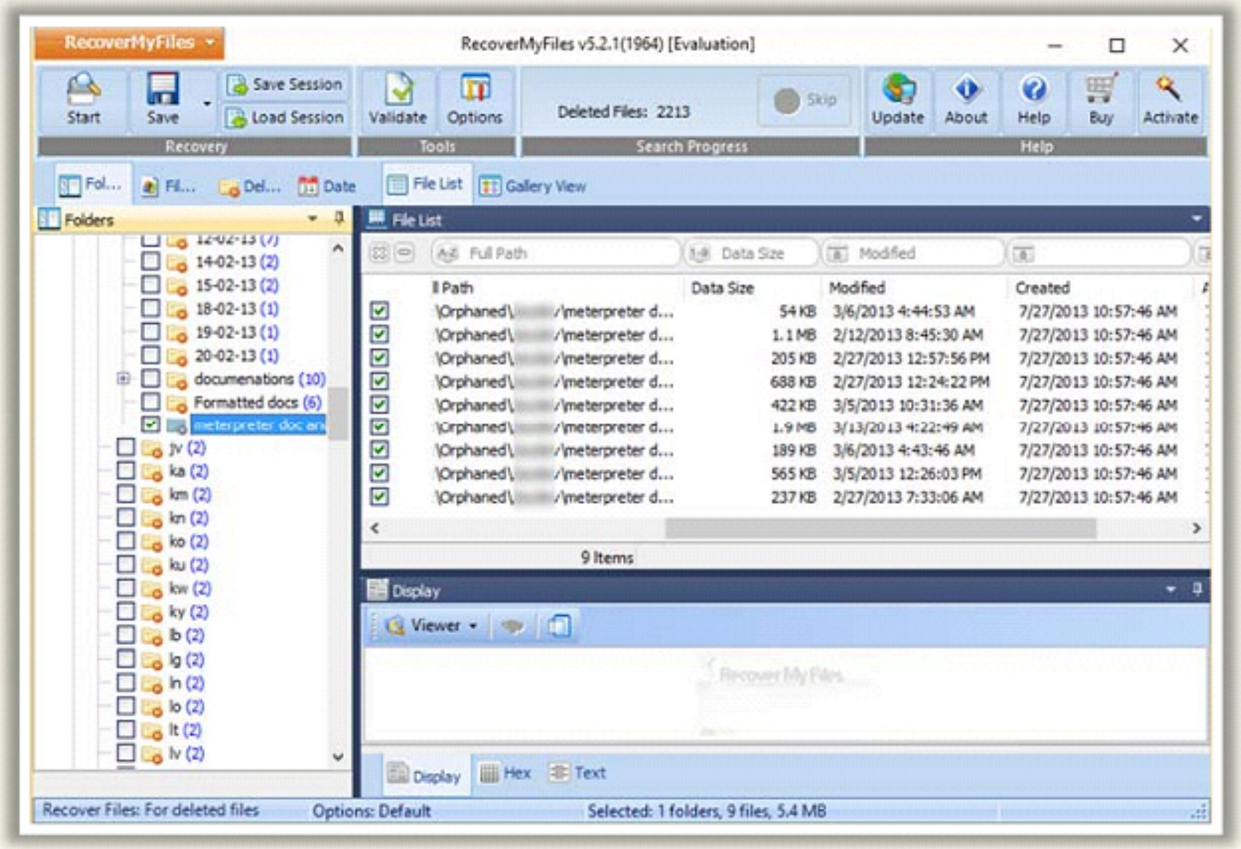
  In Windows, Vista and later:

  - Open a command prompt with administrative privileges
  - Run rd /s /q C:\$Recycle.bin command
  - Restart the computer

File Recovery Tools: Windows

Recover My Files

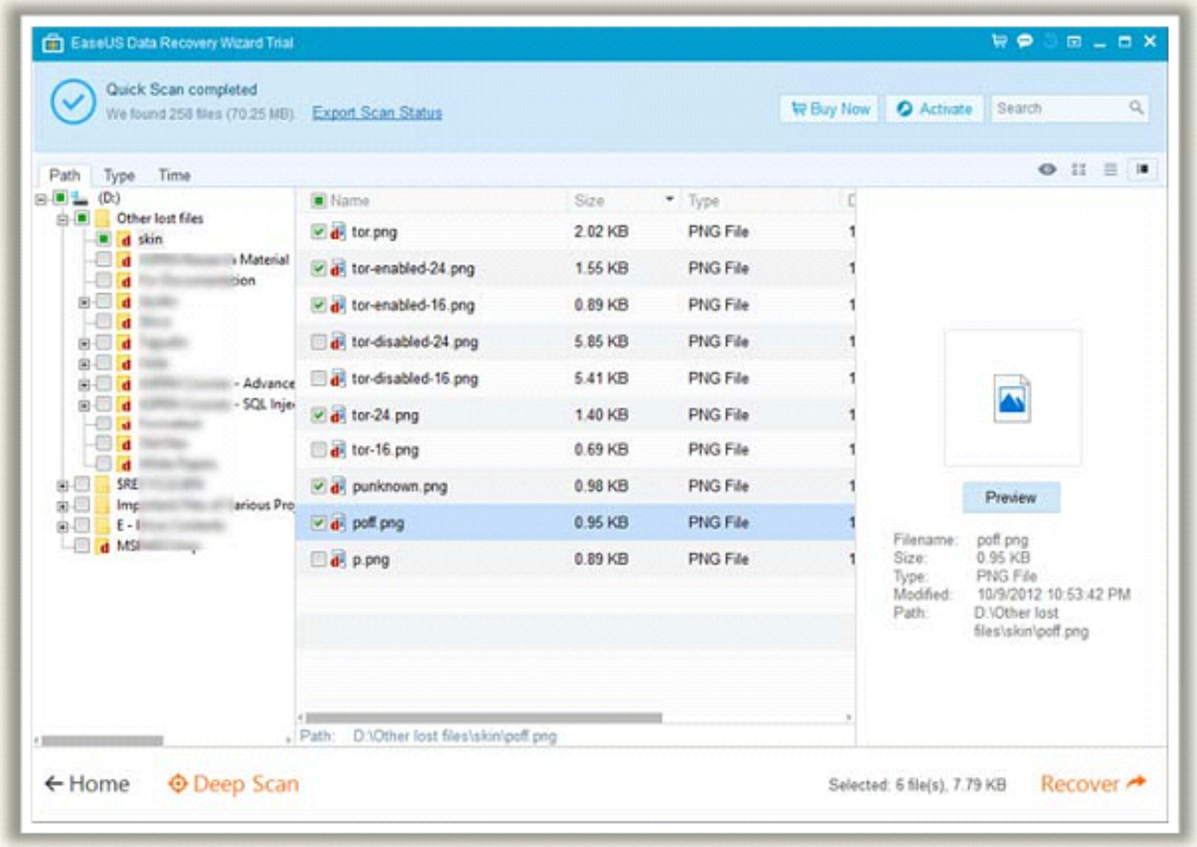
- Recovers deleted files emptied from the **Windows Recycle Bin**, files lost due to the format or reinstall of a hard drive, or files removed by a virus, Trojan infection, unexpected system shutdown or software failure



http://www.recovermyfiles.com

EaseUS Data Recovery Wizard

- Hard drive data recovery software to **recover lost data from PC**, laptop or other storage media due to deleting, formatting, partition loss, OS crash, virus attacks, etc.



http://www.easeus.com

File Recovery Tools: Windows (Cont'd)

DiskDigger
http://diskdigger.org

Handy Recovery
http://www.handyrecovery.com

Quick Recovery
http://www.recoveryourdata.com

Stellar Phoenix Windows Data Recovery
http://www.stellarinfo.com

Total Recall
http://www.totalrecall.com

Advanced Disk Recovery
http://www.systweak.com

Windows Data Recovery Software
http://www.diskdoctors.net

R-Studio
http://www.data-recovery-software.net

Orion File Recovery Software
http://www.nchsoftware.com

Data Rescue PC
http://www.prosofteng.com

File Recovery Tools: Windows (Cont'd)

Smart Undeleter
http://www.recoverdeletedfilestool.com

DDR Professional Recovery Software
http://www.recoverybull.com

Data Recovery Pro
http://www.paretologic.com

GetDataBack
http://www.runtime.org

UndeletePlus
http://undeleteplus.com

File Scavenger
http://www.quetek.com

VirtualLab
http://www.binarybiz.com

Active@ UNDELETE
http://www.active-undelete.com

WinUndelete
http://www.winundelete.com

R-Undelete
http://www.r-undelete.com

File Recovery Tools: Windows (Cont'd)

Recover4all Professional
http://www.recover4all.com

Seagate File Recovery Software
http://www.seagate.com

Recuva
http://www.piriform.com/recuva

Wise Data Recovery
http://www.wisecleaner.com

Active@ File Recovery
http://www.file-recovery.net

Glary Undelete
http://www.glarysoft.com

Pandora Recovery
http://www.pandorarecovery.com

Disk Drill
http://www.cleverfiles.com

Ontrack® EasyRecovery
http://www.krollontrack.com

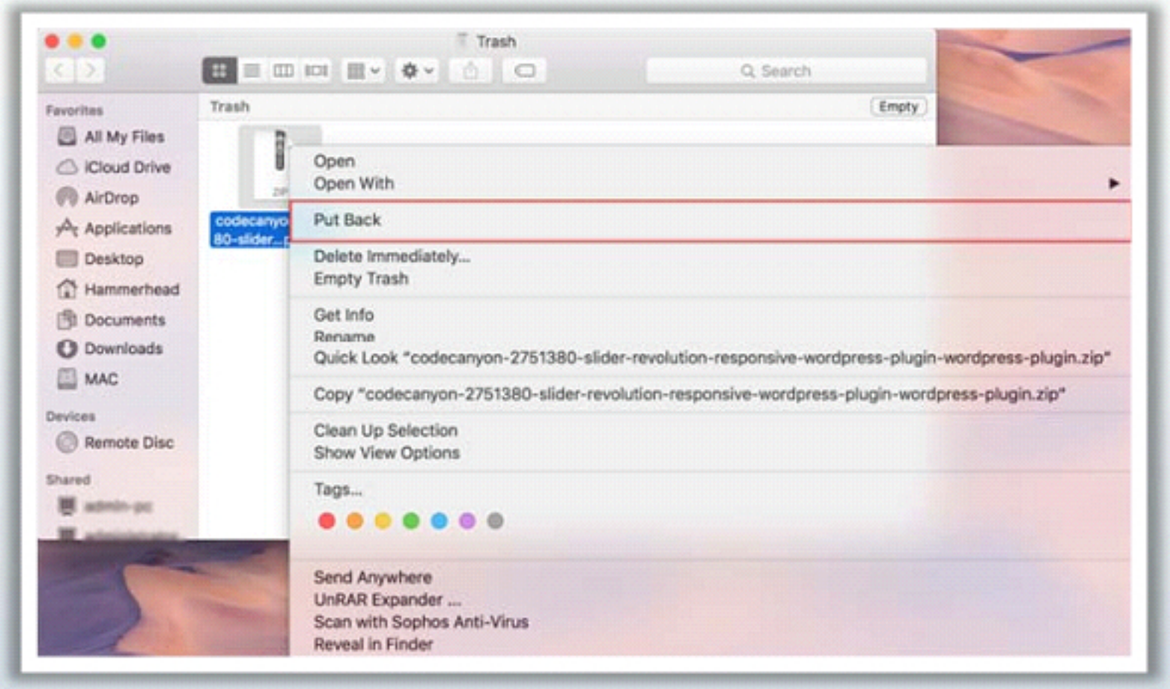
PhotoRec
http://www.cgsecurity.org

File Recovery in Mac OS X

- Deleting a file in Mac just removes it from the directory of files in the folder
- This **de-allocates the space allocated** to the file deleted, creating free space to store a new file

Methods to recover deleted files in MAC OS X:

- The deleted files are moved to the "**Trash**" folder in MAC. To restore, right-click the file and click on the **Put Back** option



- Time Machine is the built-in backup feature of MAC OS X 10.5 or newer versions. Investigator has to check if he/she can restore files from the Time Machine backup
- Other way to restore deleted files is using third-party software (recovers files emptied from the trash bin) such as FILERECOVERY® 2016 (http://filerecovery.com), Mac Data Recovery (http://www.kerneldatarecovery.com), MacKeeper Files Recovery (http://www.data-retrieval.net), Boomerang Data Recovery (https://www.boomdrs.com), Data Recovery for Mac (https://www.binarybiz.com), etc.

File Recovery Tools: MAC

AppleXsoft File Recovery for Mac
http://www.applexsoft.com

Disk Doctors Mac Data Recovery
http://www.diskdoctors.net

R-Studio for Mac
http://www.r-tt.com

Data Rescue 4
http://www.prosofteng.com

Stellar Phoenix Mac Data Recovery
http://www.stellarinfo.com

FileSalvage
http://subrosasoft.com

321Soft Data Recovery
http://www.321soft.com

Disk Drill for Mac
http://www.cleverfiles.com

Mac Data Recovery Guru
http://macosxfilerecovery.com

Cisdem DataRecovery 3
http://www.cisdem.com

File Recovery in Linux

1. In Linux, files that are deleted using the command `/bin/rm` remain on the disk
2. If a running process keeps a file open and then removes the file, the file contents are still on the disk, and other programs will not reclaim the space
3. The second extended file system (ext2) is designed in such a way that it shows several places where data can be hidden
4. It is worthwhile to note that if an executable erases itself, its contents can be retrieved from a `/proc` memory image. The command `cp /proc/$PID/exe/tmp/file` creates a copy of a file in `/tmp`
5. Third-party tools such as Stellar Phoenix Linux Data Recovery, R-Studio for Linux, TestDisk, PhotoRec, Kernel for Linux Data Recovery, etc. can be used to recover deleted files from Linux

Recovering Deleted Partitions

- What Happens When a **Partition Is Deleted**?
  - When an intruder deletes a partition on a logical drive, **all the data on the drive is lost**
  - When an intruder deletes a partition on a dynamic disk, **all dynamic volumes on the disk are deleted**, thus corrupting the disk

- Deleting a hard drive partition does not mean deleting everything, but just the **parameters** that mark how the partition is setup

- The deleted partition can be **recovered**, as it is not originally deleted, by using a software that reestablishes those parameters

Recovering Deleted Partitions (Cont'd)

Method 1	Method 2	Method 3

- **Restart** the system with a Windows install DVD in the system
- Hit the keys listed on the screen to **go to the BIOS**
- In the BIOS, check the menu for "**boot priority**" or "**boot order**" to set the DVD as the first boot device
- **Restart** the system and let Windows start the installation process
- Accept all the choices to let Windows install, but opt "**Repair**" rather than "**Install**"
- Now when a DOS-like screen appears, type "**fixboot**" and press "**Enter**"
- **Restart** the system and **check** if the deleted partition is **restored**

Recovering Deleted Partitions (Cont'd)

Method 1 | **Method 2** | Method 3

- Shut down the system and take the **hard drive out**
- Install the hard drive as a **slave** to another drive on a working system
- Now attempt to **recover** the deleted partition on the original system

Note: This method is not the safest way to avoid losing data

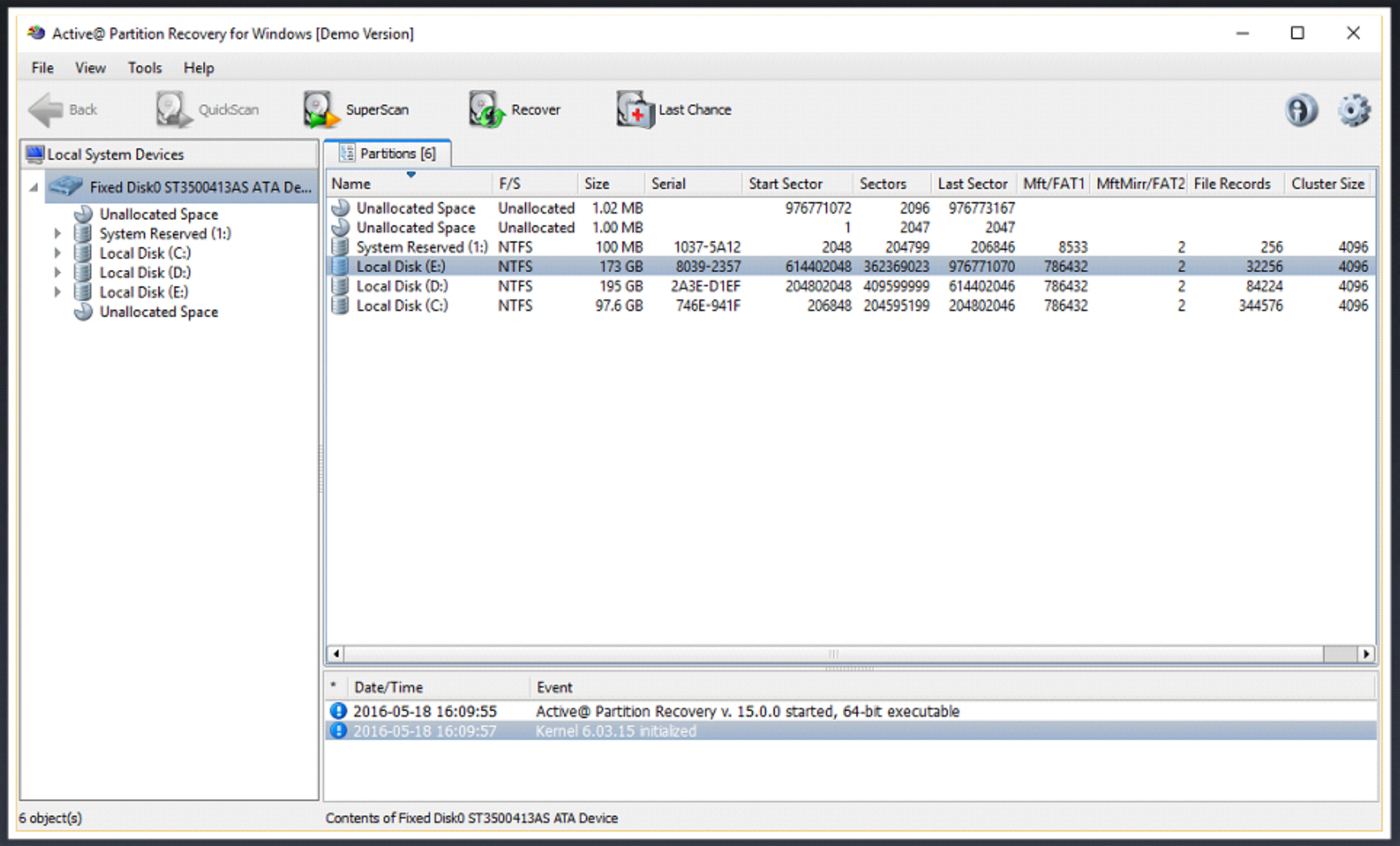
Recovering Deleted Partitions (Cont'd)

Method 1 | Method 2 | **Method 3**

- Use a **third-party partition recovery** software to recover the drive
- Run the program and follow the instructions to **recover the partition**
- Once restored, copy the files of the drive that had the partition recovered onto another drive. This prevents corruption of files

Partition Recovery Tools:
Active@ Partition Recovery

- The Active@ Partition Recovery tool allows you to **recover deleted and damaged logical drives and partitions** within DOS, Windows, WinPE (recovery boot disk) and Linux (recovery LiveCD) environments



http://www.partition-recovery.com

Partition Recovery Tools

7-Data Partition Recovery
http://7datarecovery.com

Mac Data Recovery
http://mac.powerdatarecovery.com

Acronis Disk Director Suite
http://www.acronis.com

Quick Recovery for Linux
http://www.recoveryourdata.com

RS Partition Recovery
http://recoverhdd.com

Stellar Phoenix Linux Data Recovery Software
http://www.stellarinfo.com

Partition Find & Mount
http://findandmount.com

NTFS Data Recovery Toolkit
http://www.ntfs.com

Advance Data Recovery Software Tools for NTFS
http://www.recoverdatatools.com

TestDisk for Windows
http://www.cgsecurity.org

Partition Recovery Tools (Cont'd)

Stellar Phoenix Windows Data Recovery
http://www.stellarinfo.com

EaseUS Partition Master
http://www.easeus.com

Hetman Partition Recovery
https://hetmanrecovery.com

MiniTool Power Data Recovery Free
http://www.powerdatarecovery.com

Remo Recover (Mac) - Pro
http://www.remosoftware.com/

TestDisk for Mac
http://www.cgsecurity.org

Starus Partition Recovery
http://www.starusrecovery.com

Disk Drill
http://www.cleverfiles.com

Stellar Phoenix Mac Data Recovery
http://www.stellarinfo.com

ZAR Windows Data Recovery
http://www.z-a-recovery.com

Anti-Forensics Techniques: Password Protection

- Investigators often come across the **password protected systems** or files during the investigation process
- In such cases, they use specialized **password cracking software** in order to circumvent the protection
- Time taken to crack passwords depends on their **strength**
- Weak passwords could be broken in less than a second, while strong passwords would take **years to crack**

Password Types

Cleartext Passwords

- A cleartext password is sent over the wire (and also over wireless) or stored on some media as it is typed without any alteration

  Ex: Windows Registry houses automatic logon password (`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`)
- **Cain** and **Ettercap** can be used to sniff cleartext passwords

Obfuscated Passwords

- Obfuscated passwords are those that are **stored or communicated after being more or less transformed**
- **Transformation is reversible**. After applying an algorithm the password becomes unreadable and after applying a reverse algorithm it returns to cleartext. This process is called as obfuscation

Hashed Passwords

- Hashed passwords are **similar to obfuscated passwords**, but the latter are reversible
- Passwords are hashed using **hash algorithms** (MD5, SHA, etc.) that are not reversible

Note: Only hashed passwords need cracking, while the other password types can assist in cracking phase

Password Cracker and its Working

- Password cracker is a software program that is used to **recover passwords** of a **system**, **network resource**, or an app, when lost or forgotten

How it Works?

- A **word list** is created with the help of a **dictionary generator** program or dictionaries
- The list of **dictionary words** is **hashed** or **encrypted**
- The **hashed wordlist** is **compared** against the **target** hashed password, generally one word at a time
- If it matches, that **password** has been **cracked** and the password cracker displays the **unencrypted version** of the password

Note: The target hashed password can be obtained by sniffing it from a wired network, wireless network, directly from the Security Accounts Manager (SAM) database, or shadow password files on the hard drive of a system

Password Cracking Techniques

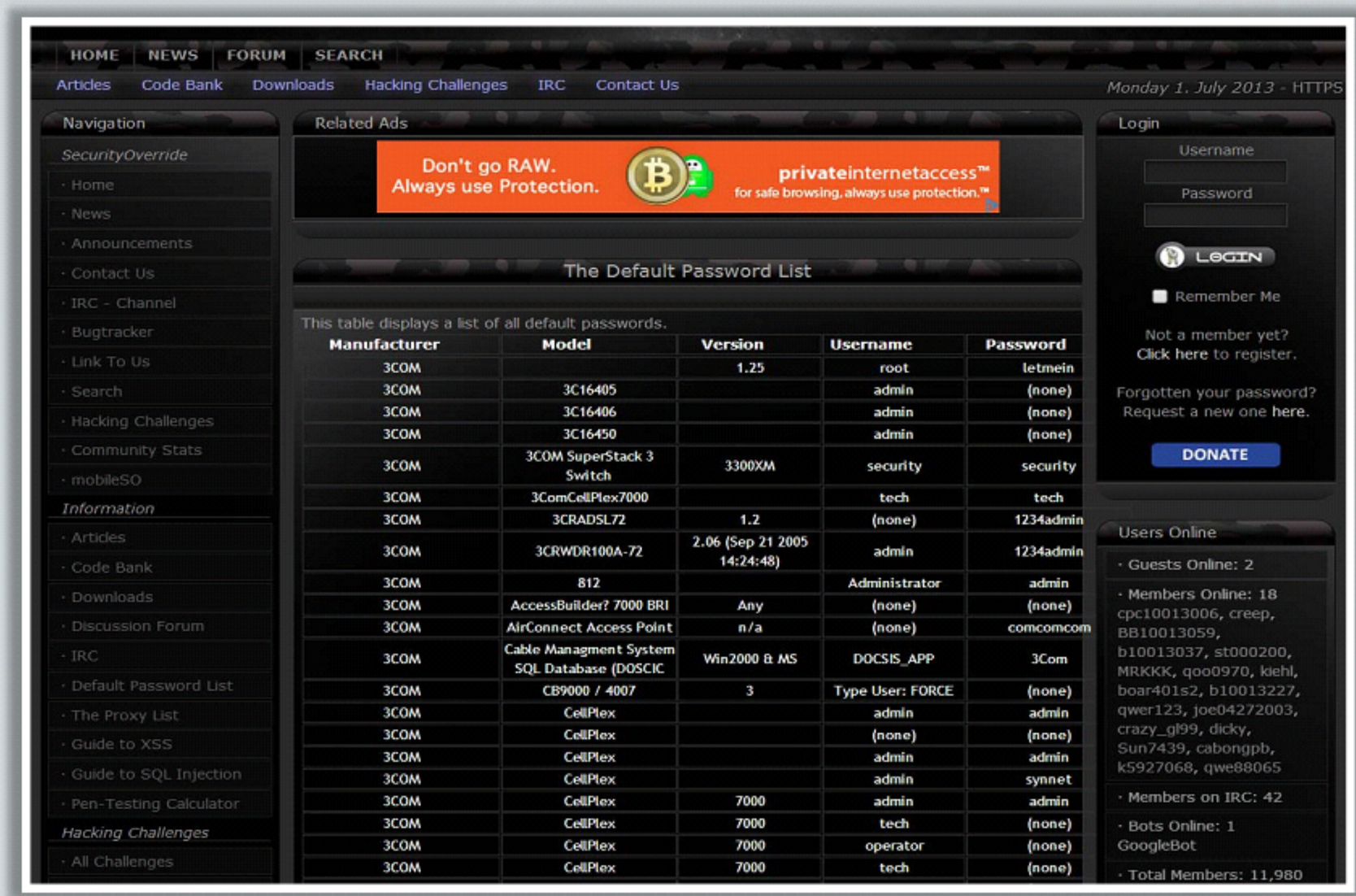
Dictionary Attack	A **dictionary file** is loaded into the cracking application that runs against **user accounts**
Brute Forcing Attacks	The program tries **every combination of characters** until the password is broken
Rule-based Attack	This attack is used when some **information about the password is known**

Default Passwords

- A default password is a password supplied by the **manufacturer** with new equipment (e.g. switches, hubs, and routers) that is password protected
- You can use default passwords from the list of words or dictionary that is used to perform **password guessing attack**

Online tools to search default passwords:

- http://cirt.net
- http://default-password.info
- http://www.defaultpassword.us
- http://www.passwordsdatabase.com
- https://w3dt.net
- http://www.virus.org
- http://open-sez.me
- http://securityoverride.org
- http://www.routerpasswords.com
- http://www.fortypoundhead.com



HOME | NEWS | FORUM | SEARCH

Articles | Code Bank | Downloads | Hacking Challenges | IRC | Contact Us

Monday 1. July 2013 - HTTPS

Navigation

SecurityOverride
- Home
- News
- Announcements
- Contact Us
- IRC - Channel
- Bugtracker
- Link To Us
- Search
- Hacking Challenges
- Community Stats
- mobileSO

Information
- Articles
- Code Bank
- Downloads
- Discussion Forum
- IRC
- Default Password List
- The Proxy List
- Guide to XSS
- Guide to SQL Injection
- Pen-Testing Calculator

Hacking Challenges
- All Challenges

Related Ads

Don't go RAW. Always use Protection. privateinternetaccess™ for safe browsing, always use protection.™

The Default Password List

This table displays a list of all default passwords.

Manufacturer	Model	Version	Username	Password
3COM		1.25	root	letmein
3COM	3C16405		admin	(none)
3COM	3C16406		admin	(none)
3COM	3C16450		admin	(none)
3COM	3COM SuperStack 3 Switch	3300XM	security	security
3COM	3ComCellPlex7000		tech	tech
3COM	3CRADSL72	1.2	(none)	1234admin
3COM	3CRWDR100A-72	2.06 (Sep 21 2005 14:24:48)	admin	1234admin
3COM	812		Administrator	admin
3COM	AccessBuilder? 7000 BRI	Any	(none)	(none)
3COM	AirConnect Access Point	n/a	(none)	comcomcom
3COM	Cable Managment System SQL Database (DOSCIC	Win2000 & MS	DOCSIS_APP	3Com
3COM	CB9000 / 4007	3	Type User: FORCE	(none)
3COM	CellPlex		admin	admin
3COM	CellPlex		(none)	(none)
3COM	CellPlex		admin	admin
3COM	CellPlex		admin	synnet
3COM	CellPlex	7000	admin	admin
3COM	CellPlex	7000	tech	(none)
3COM	CellPlex	7000	operator	(none)
3COM	CellPlex	7000	tech	(none)

Login

Username

Password

LOGIN

Remember Me

Not a member yet? Click here to register.

Forgotten your password? Request a new one here.

DONATE

Users Online

- Guests Online: 2
- Members Online: 18 cpc10013006, creep, BB10013059, b10013037, st000200, MRKKK, qoo0970, kiehl, boar401s2, b10013227, qwer123, joe04272003, crazy_gl99, dicky, Sun7439, cabongpb, k5927068, qwe88065
- Members on IRC: 42
- Bots Online: 1 GoogleBot
- Total Members: 11,980

http://securityoverride.org

Using Rainbow Tables to Crack Hashed Passwords

C|HFI Computer Hacking Forensic Investigator

Rainbow Table

A rainbow table is a precomputed table which contains word lists like **dictionary files** and **brute force lists** and their **hash values**

Compare the Hashes

Capture the hash of a **password** and compare it with the precomputed hash table. If a match is found, then the password is cracked

Easy to Recover

It is easy to recover passwords by comparing captured password hashes to **precomputed tables**

Precomputed Hashes

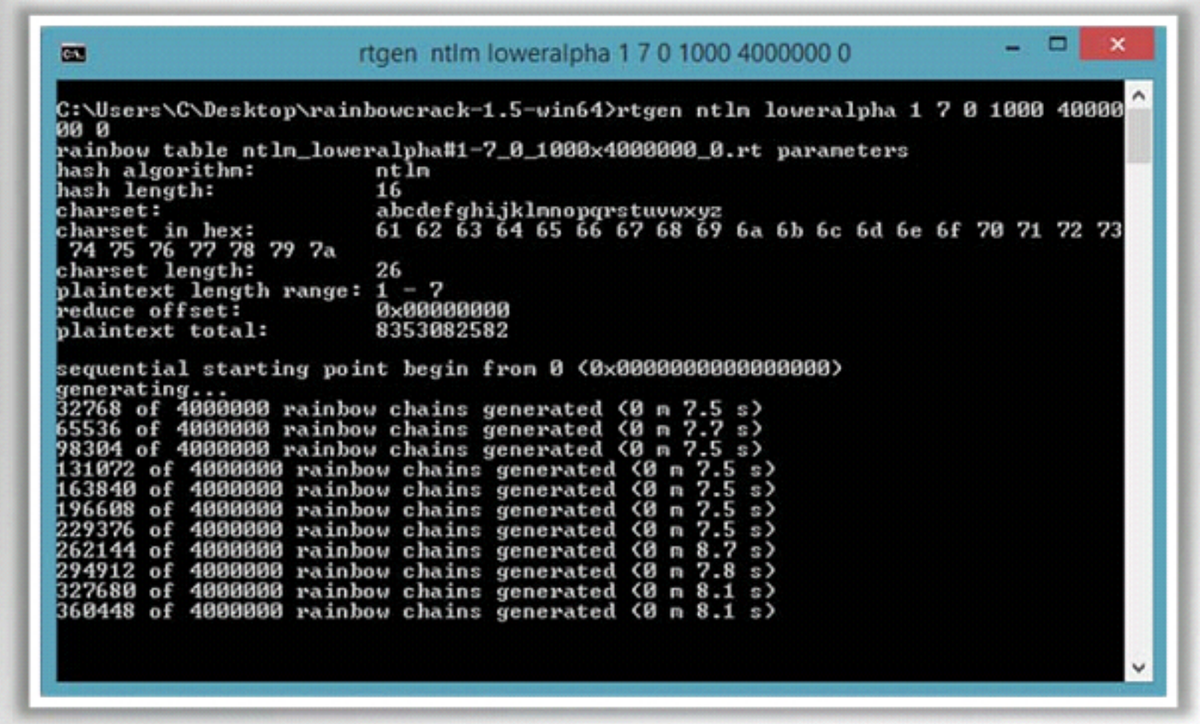
1qazwed	4259cc34599c530b28a6a8f225d668590
hh021da	c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf	3cd696a8571a843cda453a229d741843
sodifo8sf	c744b1716cbf8d4dd0ff4ce31a177151

Tools to Create Rainbow Tables: rtgen and Winrtgen

rtgen

- The rtgen program needs **several parameters** to generate a rainbow table. The syntax of the command line is:

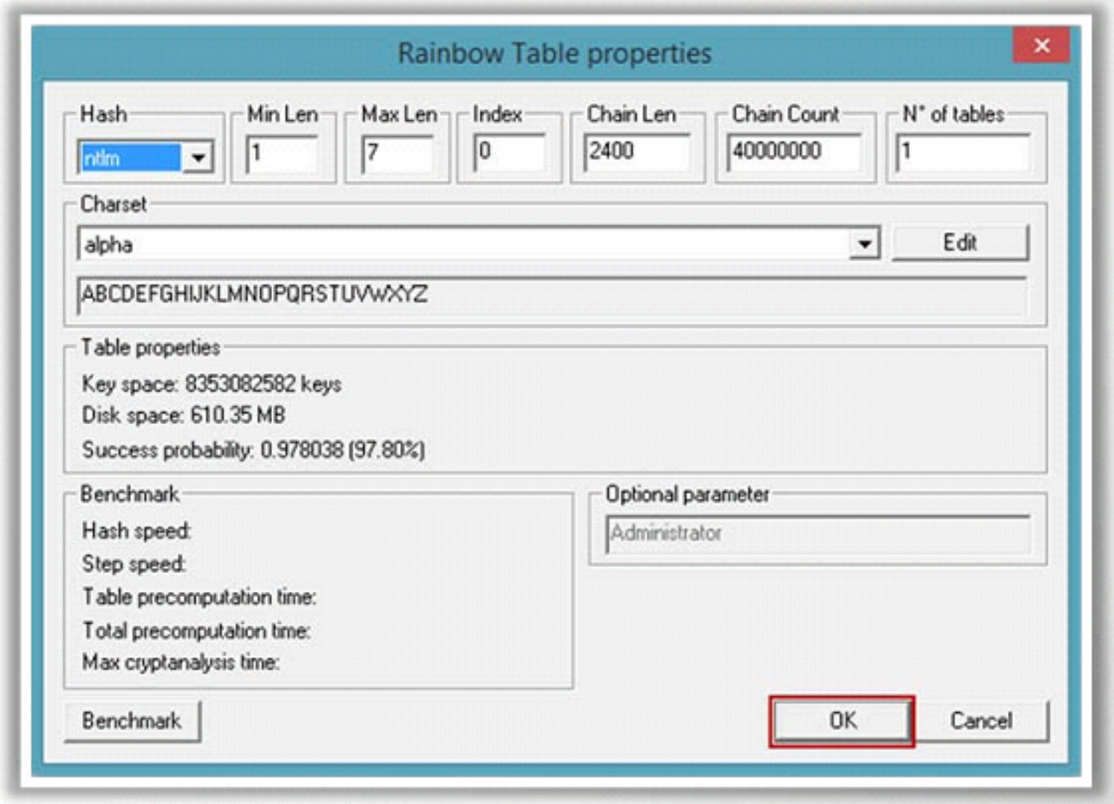
```
rtgen hash_algorithm charset
plaintext_len_min plaintext_len_max
table_index chain_len chain_num
part_index
```



http://project-rainbowcrack.com

Winrtgen

- Winrtgen is a graphical **Rainbow Tables Generator** that supports LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2 (256), SHA-2 (384), and SHA-2 (512) hashes



http://www.oxid.it

Microsoft Authentication

Security Accounts Manager (SAM) database

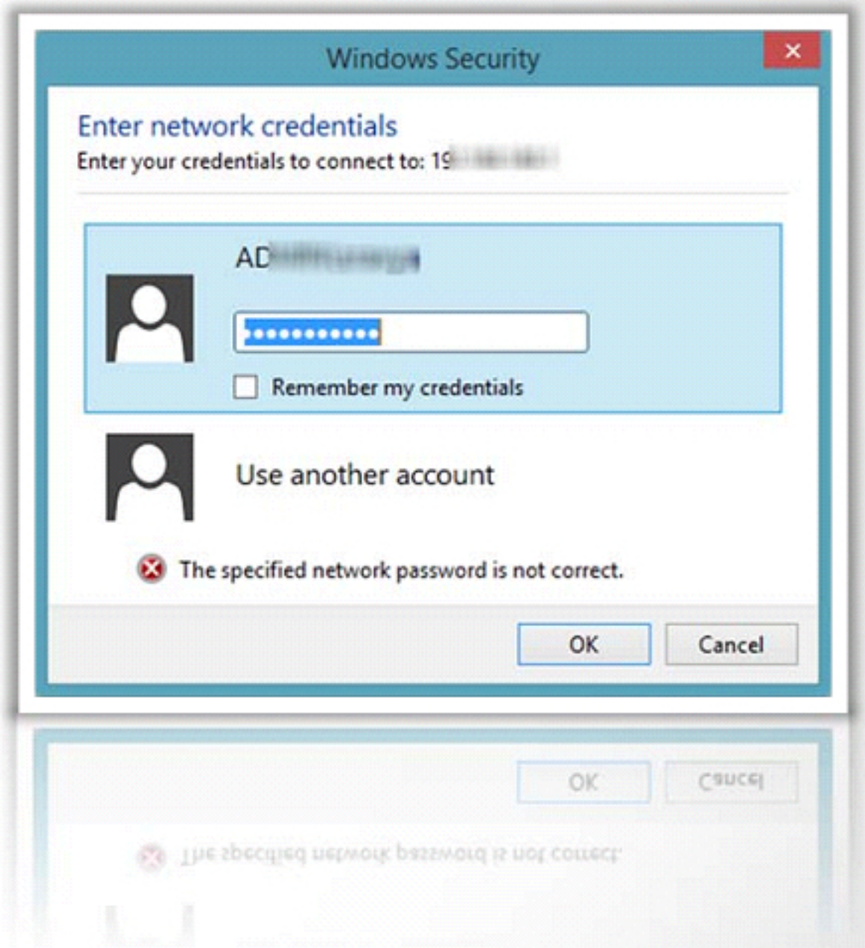
Windows stores user passwords in SAM, or in the **Active Directory database** in domains. Passwords are never stored in clear text; passwords are hashed and the results are stored in SAM

NTLM Authentication

- The typology of NTLM authentication protocols:
  1. **NTLM authentication protocol**
  2. **LM authentication protocol**
- These protocols store user passwords in the SAM database using different hashing methods

Kerberos Authentication

Microsoft has upgraded its **default authentication protocol** to Kerberos, which provides a stronger authentication for client/server applications than NTLM



Windows 8

How Hash Passwords Are Stored in Windows SAM?

Shiela/test

Password hash using LM/NTLM

```
Shiela:1005:NO PASSWORD****
*****************:0CB694880
5F797BF2A82807973B89537:::
```

SAM File is located at `c:\windows\system32\config\SAM`

```
Administrator:500:NO PASSWORD*******************:61880B9EE373475C8148A7108ACB3031:::
Guest:501:NO PASSWORD*******************:NO PASSWORD*******************:::
Admin:1001:NO PASSWORD*******************:BE40C450AB99713DF1EDC5B40C25AD47:::
Martin:1002:NO PASSWORD*******************:BF4A502DA294ACBC175B394A080DEE79:::
Juggyboy:1003:NO PASSWORD*******************:488CDCDD2225312793ED6967B28C1025:::
Jason:1004:NO PASSWORD*******************:2D20D252A479F485CDF5E171D93985BF:::
Shiela:1005:NO PASSWORD*******************:0CB6948805F797BF2A82807973B89537:::
```

User name | User ID | LM Hash | NTLM Hash

"LM hashes have been disabled in Windows Vista and later Windows operating systems; LM will be blank in those systems."

System Software Password Cracking

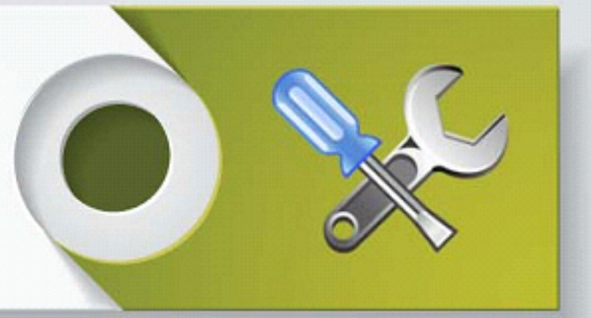
System software includes **low-level programs** (such as OSs, compilers, utilities that manage system resources, etc.) that interact with the PC at a basic level

System software password cracking is defined as cracking the **operating system** and all other **utilities** that enable a computer to **function**

Passwords for system software are created to **prevent access** to system files and other secured **information** that is used during a system's boot process

Ways to access a system by cracking passwords:

- **Bypassing the BIOS password**
- **Using tools to reset admin password**



Bypassing BIOS Passwords

- BIOS (Basic Input Output System) is a **firmware code** run by a system when **powered on**. It is a type of **boot loader**
- The main function of BIOS is to **identify** and **initialize** system component hardware (such as hard disk, floppy drive, and video display card)

Methods to Bypass/Reset BIOS Password

1. Using a manufacturer's **backdoor password** to access the BIOS
2. Using **password cracking software**
3. **Resetting the CMOS** using jumpers or solder beads
4. **Removing the CMOS battery** for at least 10 minutes
5. **Overloading** the keyboard **buffer**
6. Using a **professional service**

Using Manufacturer's Backdoor Password to Access the BIOS

- BIOS manufacturers **provide** a **backup** password that can be used to **access** the **BIOS** setup if the password is **lost**
- The passwords that manufacturers provide are **case sensitive**. If a particular backdoor password does not work, then various case-sensitive **combinations** of the password should be tried.
- The **combinations** may include **alphanumeric** characters
- The manufacturers' **documentation** must be **read** before trying the backdoor passwords, because **BIOS** combinations will **lock** the system completely if the password is typed **wrong** three times

Few BIOS manufacturers and their default passwords are listed below:

- VOBIS & IBM – merlin
- Dell – Dell
- Biostar – Biostar
- Compaq – Compaq
- Enox - xo11nE
- Epox - central
- Freetech - Posterie
- Iwill - iwill
- Jetway - spooml
- Packard Bell - bell9
- QDI - QDI

Using Password Cracking Software

The following software can be used to either crack or reset the BIOS on many chipsets

CmosPwd

Decrypts password stored in CMOS, which is used to access BIOS SETUP

http://www.cgsecurity.org

DaveGrohl

It is a multithreaded, distributed password cracker. It aims at brute-forcing OS X user passwords.

http://davegrohl.org

C:\WINDOWS\system32\cmd.exe

```
C:\cmos>ioperm -i

C:\cmos>cmospwd_win
CmosPwd - BIOS Cracker 5.0, October 2007, Copyright 1996-2007
GRENIER Christophe, grenier@cgsecurity.org
http://www.cgsecurity.org/

Keyboard : US
Acer/IBM                        [H][ <]
AMI BIOS                        []
AMI WinBIOS <12/15/93>          []
AMI WinBIOS 2.5                 [] [] [] []
AMI ?                           [] [ M] [ ] [ M] [   E M]
Award 4.5x6.0                   [23012202] [000100] [000300]
Award 4.5x6.0                   [30000122] [12003000] [33333033] [0
Award Medallion 6.0             [000100] [000100] [20000000] [00010
Award 6.0                       [ [o] [+   Z S ] [ ]N.P ] [Nq50]
Compaq <1992>                   []
Compaq DeskPro                  [] []
Compaq                          [1 7   ] []
```

Note: If your PC is locked with a BIOS administrator password that does not allow access to the floppy drive, these utilities may not work

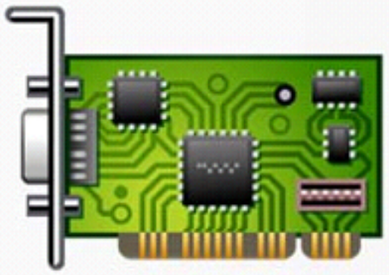
Resetting the CMOS using Jumpers or Solder Beads

1 Resetting the CMOS using Jumpers

- By adjusting the jumpers or dipswitches on a motherboard, all custom settings, including BIOS passwords, will be cleared
- Check the computer or motherboard manufacturer's documentation to locate the **jumpers/dip switches**
- If the documentation is not available, by default the **jumper position** is across pins 1 and 2
- Shut down the system and unplug the power cord
- Move the jumper from its default position so that it is across **pins 2** and **3**; this clears the BIOS/CMOS settings
- Now, turn on the machine to verify that the password has been reset
- Once cleared, turn off the computer and return the jumper to its original position

2 Resetting the CMOS using Solder Beads

- Connecting or jumping specific **solder beads** on the chipset is likely to reset the CMOS
- There are **too many chipsets** to do a breakdown of which points to jump on individual chipsets, and the location of these solder beads can **vary according to the manufacturer**, so please check the computer and motherboard documentation for details



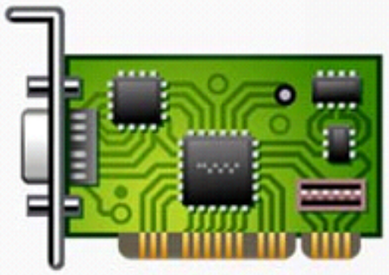
Resetting the CMOS using Jumpers or Solder Beads

1 Resetting the CMOS using Jumpers

- By adjusting the jumpers or dipswitches on a motherboard, all custom settings, including BIOS passwords, will be cleared
- Check the computer or motherboard manufacturer's documentation to locate the **jumpers/dip switches**
- If the documentation is not available, by default the **jumper position** is across pins 1 and 2
- Shut down the system and unplug the power cord
- Move the jumper from its default position so that it is across **pins 2** and **3**; this clears the BIOS/CMOS settings
- Now, turn on the machine to verify that the password has been reset
- Once cleared, turn off the computer and return the jumper to its original position

2 Resetting the CMOS using Solder Beads

- Connecting or jumping specific **solder beads** on the chipset is likely to reset the CMOS
- There are **too many chipsets** to do a breakdown of which points to jump on individual chipsets, and the location of these solder beads can **vary according to the manufacturer**, so please check the computer and motherboard documentation for details



Overloading the Keyboard Buffer and Using a Professional Service

Overloading the keyboard buffer

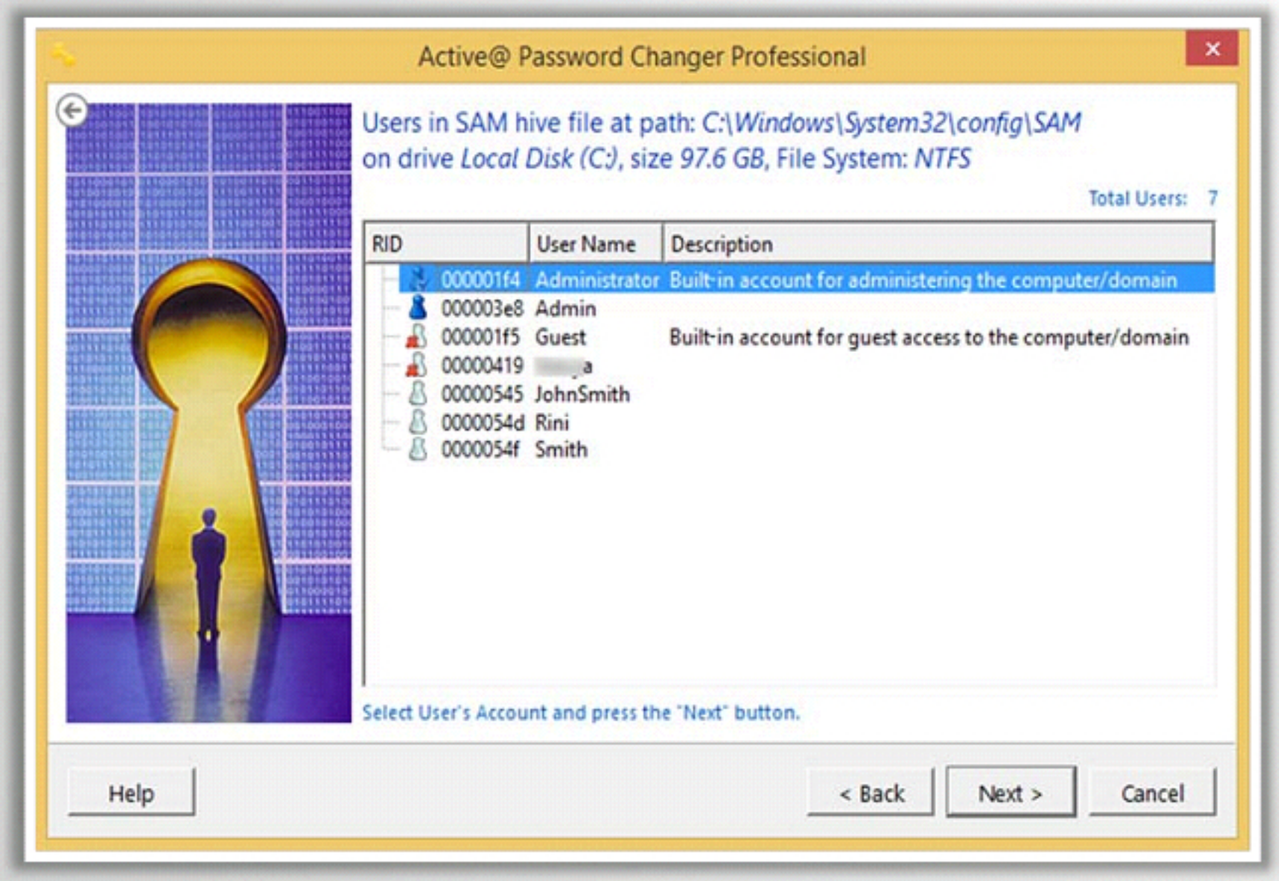
- On some older systems, you can force the CMOS to enter its **setup screen on boot** by overloading the keyboard buffer
- This is achieved by hitting the **ESC** key over 100 times in rapid succession, or by booting with the keyboard or mouse unattached to the systems

Using a professional service

- Professional services can be used if the manufacturer of the laptop or desktop PC would not **reset the BIOS password**
- Password Crackers, Inc., offers a variety of services for desktop and laptop computers; all you need to provide is **legitimate proof of ownership**

Tool to Reset Admin Password: Active@ Password Changer

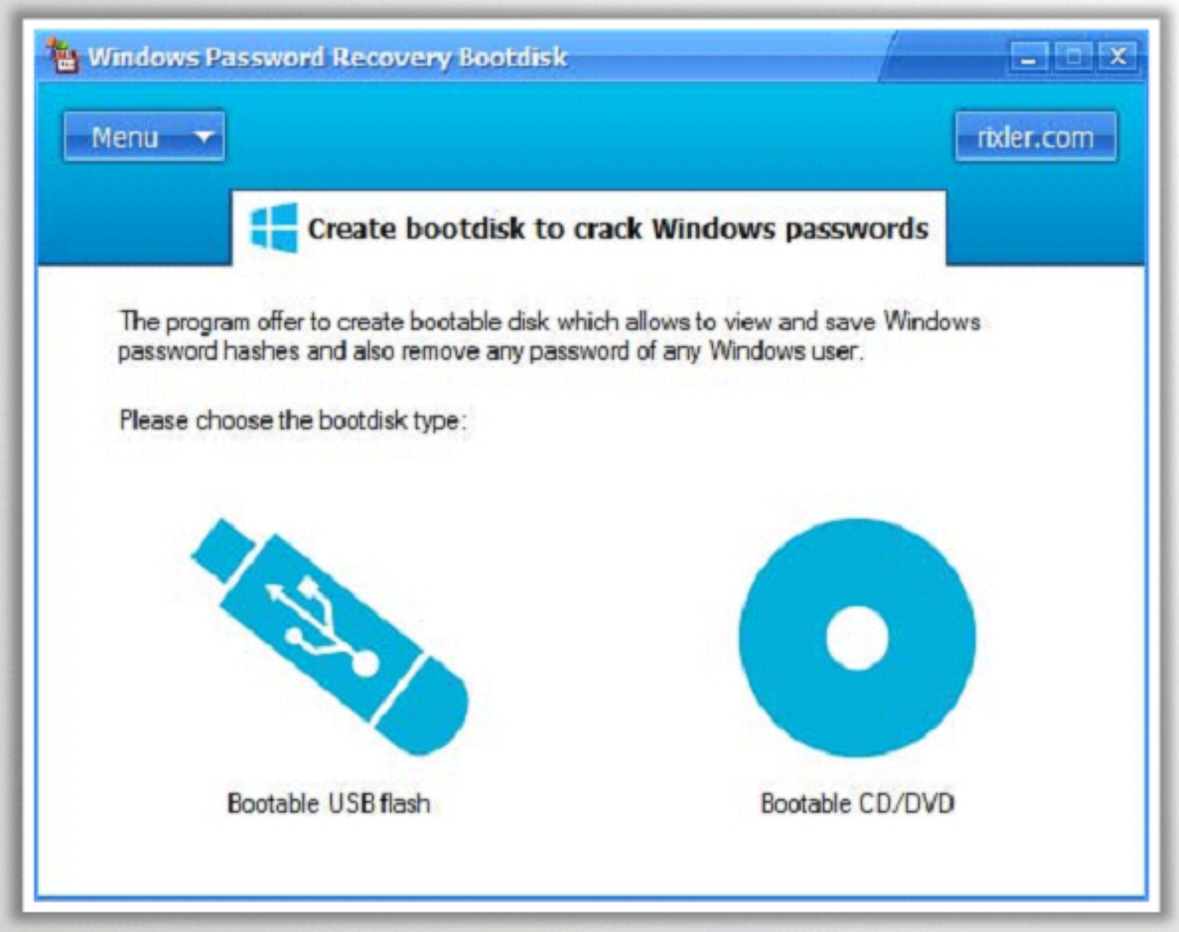
- Active@ Password Changer is designed for **resetting** local administrators and user passwords on Windows operating system in case an Administrator's password is **forgotten or lost**
- With Active@ Password Changer, you can log in as an Administrator or a particular user with a blank password

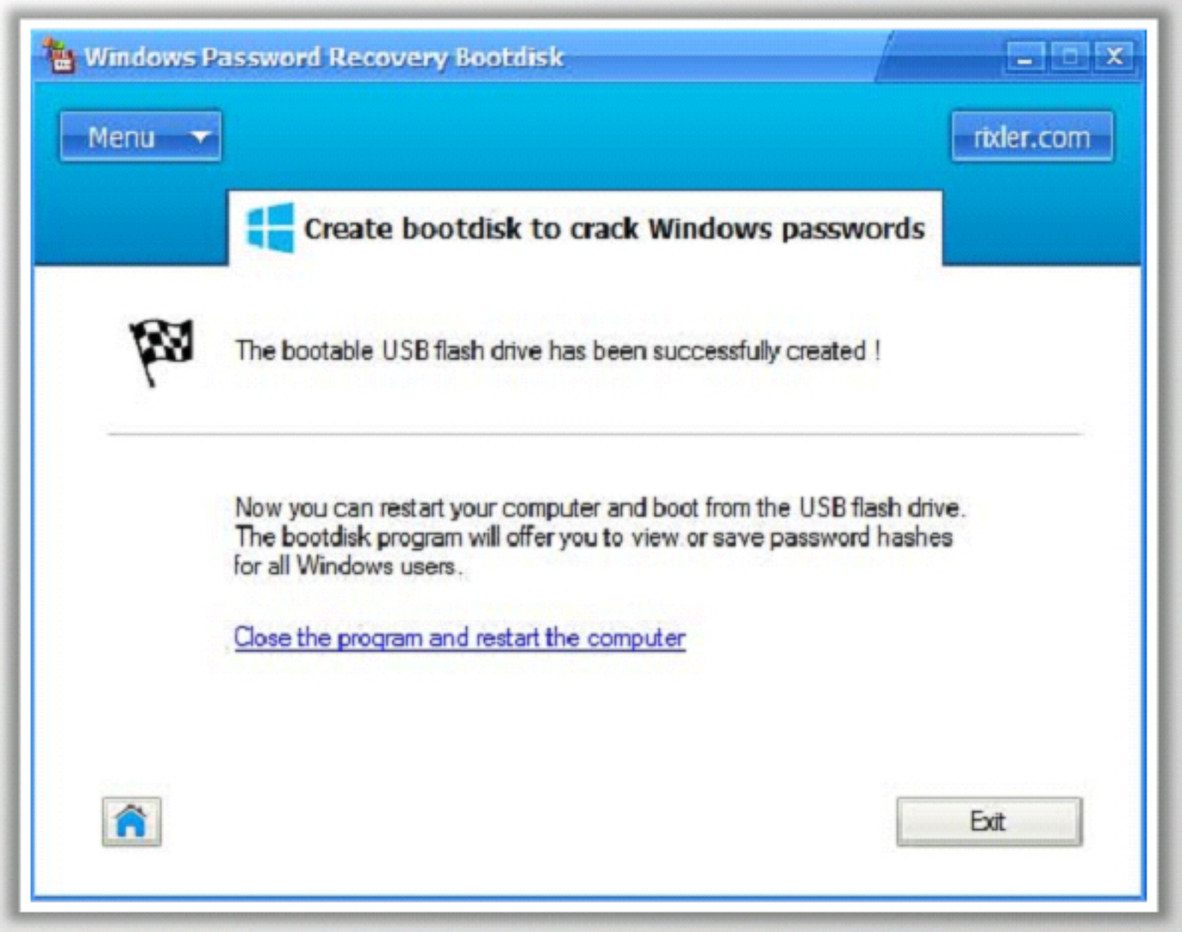


http://www.password-changer.com

Tool to Reset Admin Password: Windows Password Recovery Bootdisk

- Windows Password Recovery Bootdisk **removes the password** and, thus, allows login to the account
- The program **creates a bootdisk** or a bootable USB stick, and writes a special Linux-like OS there
- Booting from such a **disk allows to remove a Windows account password**, or recover its hash for further retrieval of lost passwords

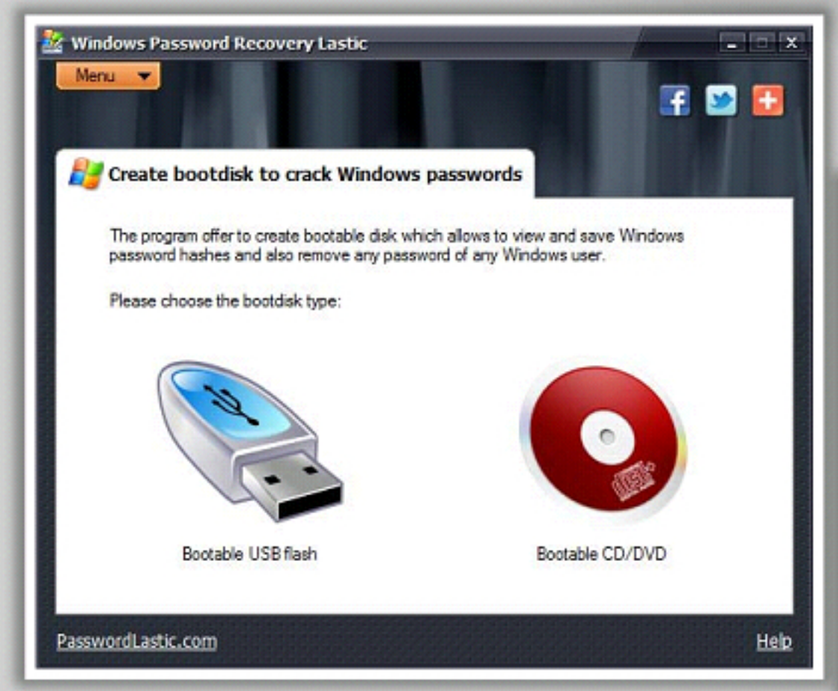


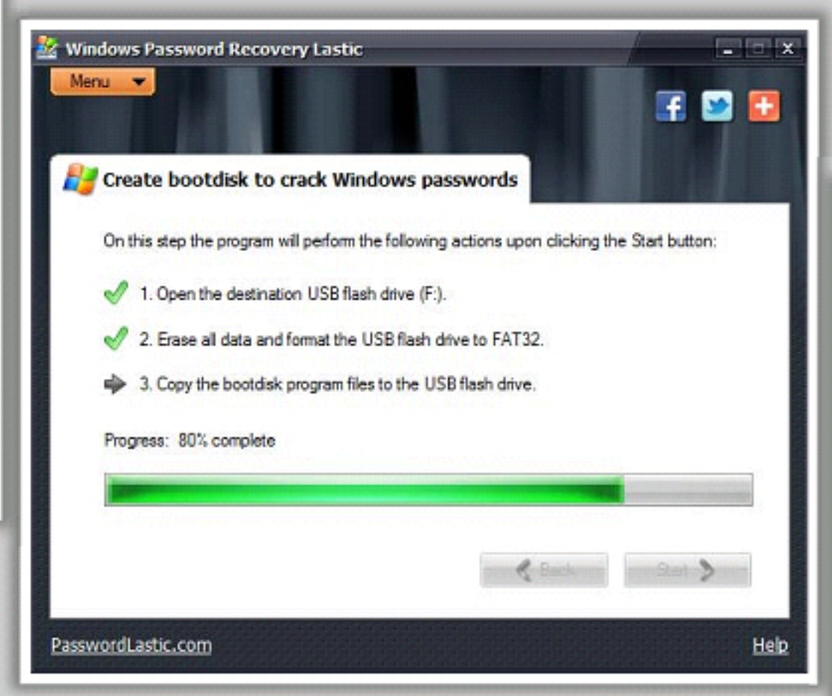


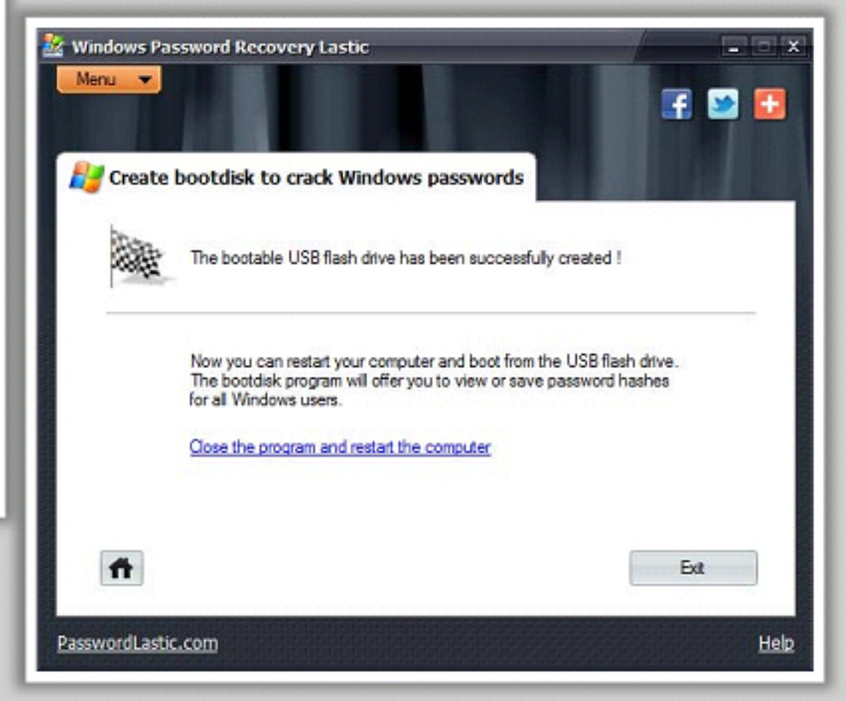
http://www.rixler.com

Tool to Reset Admin Password: Windows Password Recovery Lastic

- Windows Password Recovery Lastic **allows the removing of a password for a specific Windows user**, or recovering the hash of a password, thus providing one with the possibility of restoring the original password







http://www.passwordlastic.com

Application Password Cracking Tools

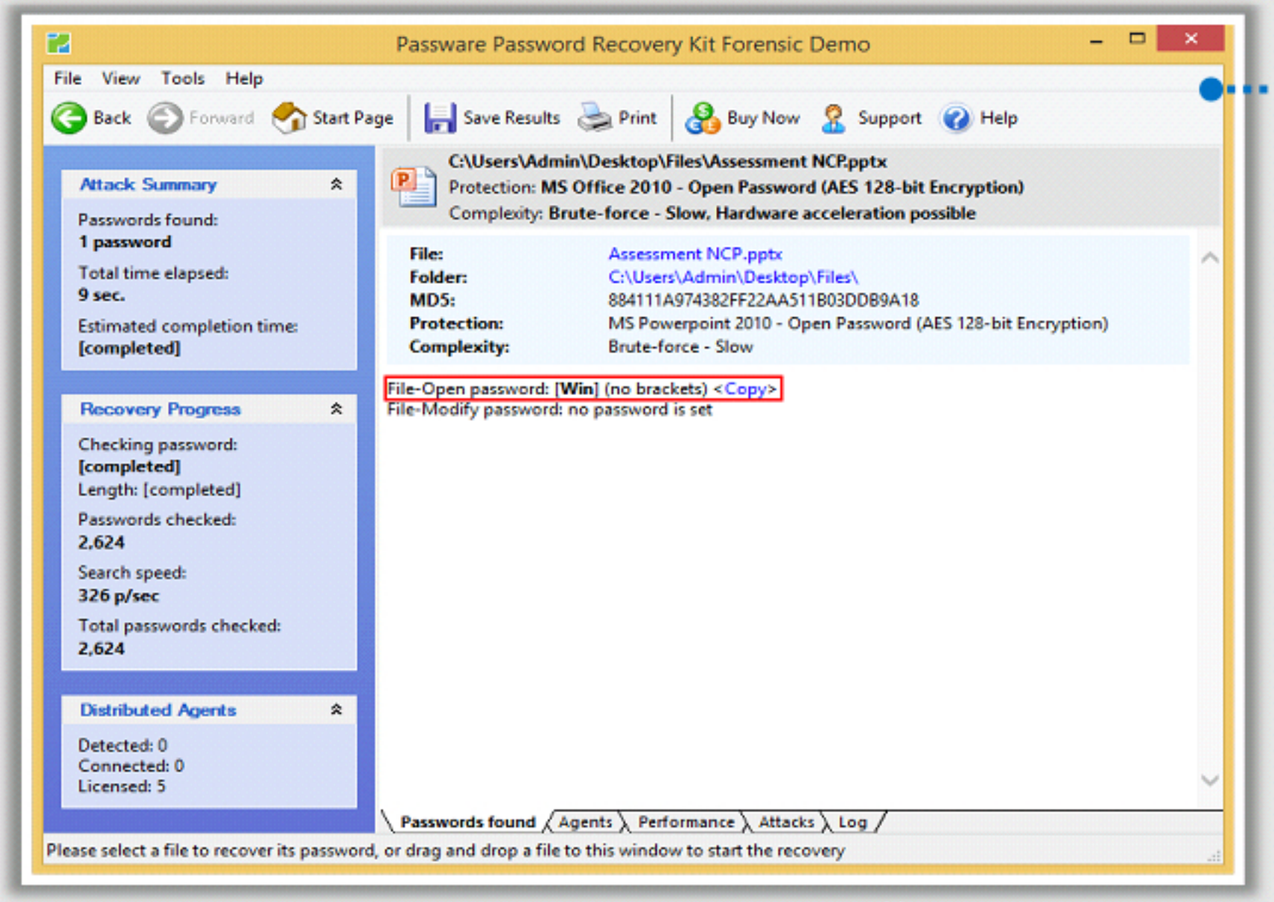
Applications software, also known as end-user programs (such as Web design software, word processors, graphics software, etc.), allow an user to perform their everyday tasks on the PC like sending email, editing an image, creating a webpage, etc.

Passware Kit Forensic

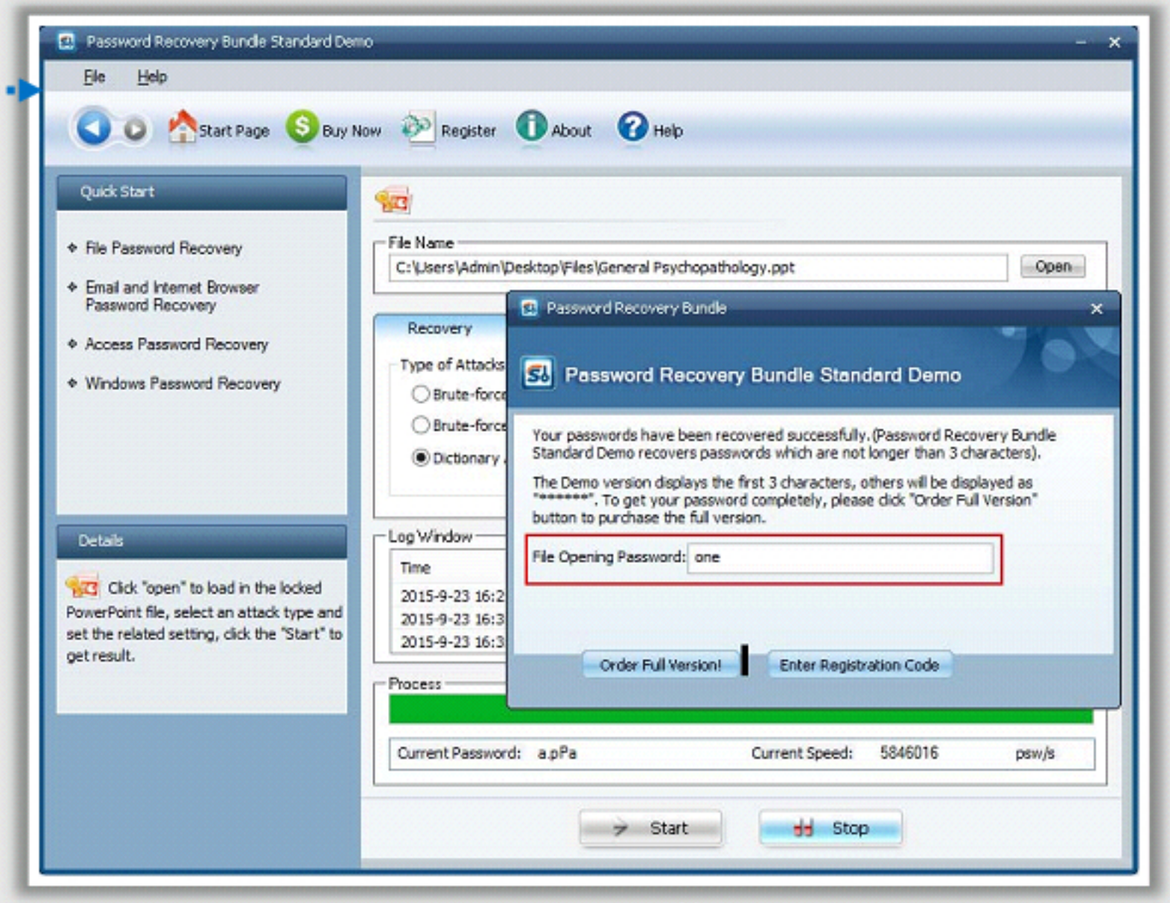
Electronic evidence discovery solution that reports all password-protected items on a computer, and decrypts them

SmartKey Password Recovery Bundle Standard

Recovers passwords for Windows, Excel, Word, Access, PowerPoint, PST, Outlook, Outlook Express, RAR/WinRAR, ZIP/WinZIP, PDF, IE Browser, SQL, e-mail, online websites, etc.



http://www.lostpassword.com

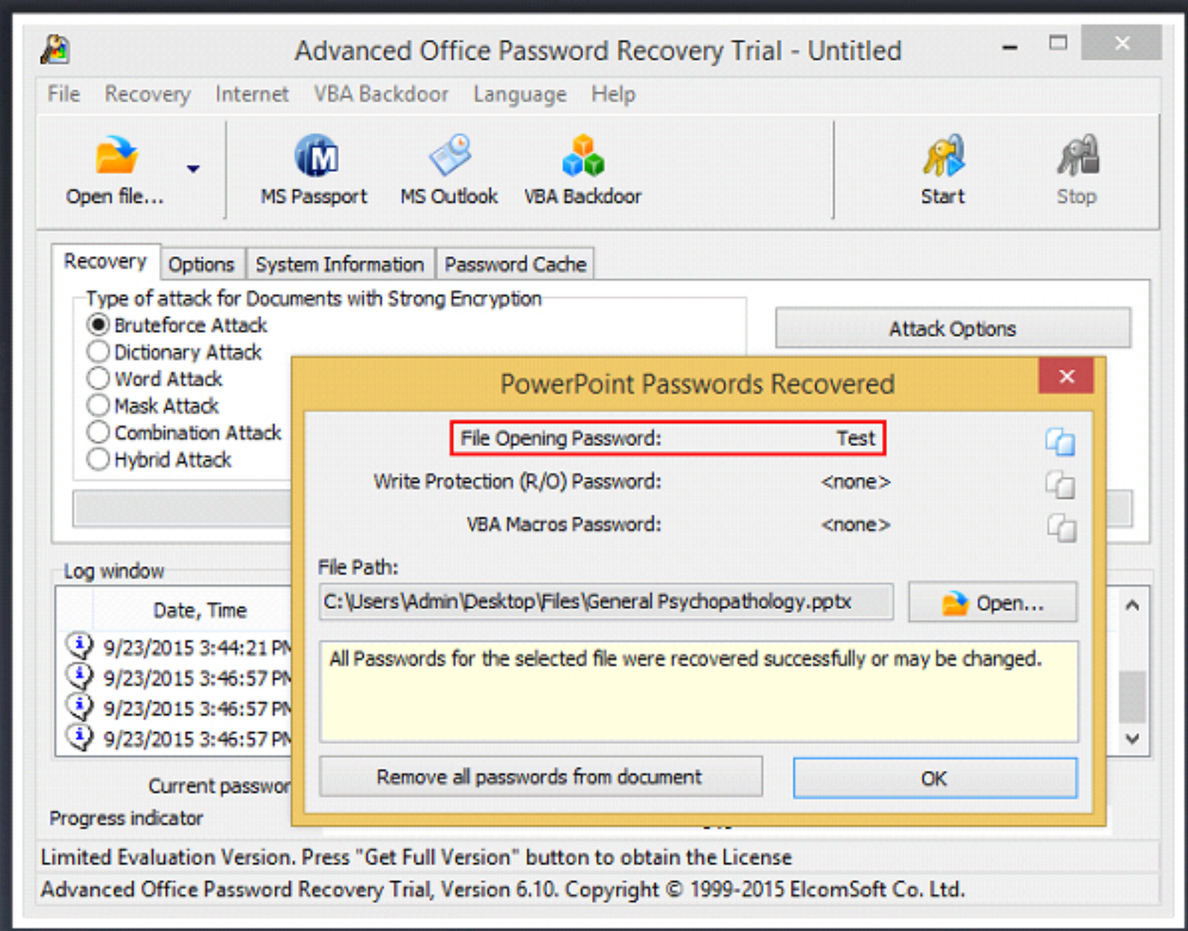


http://www.recoverlostpassword.com

Application Password Cracking Tools (Cont'd)

Advanced Office Password Recovery

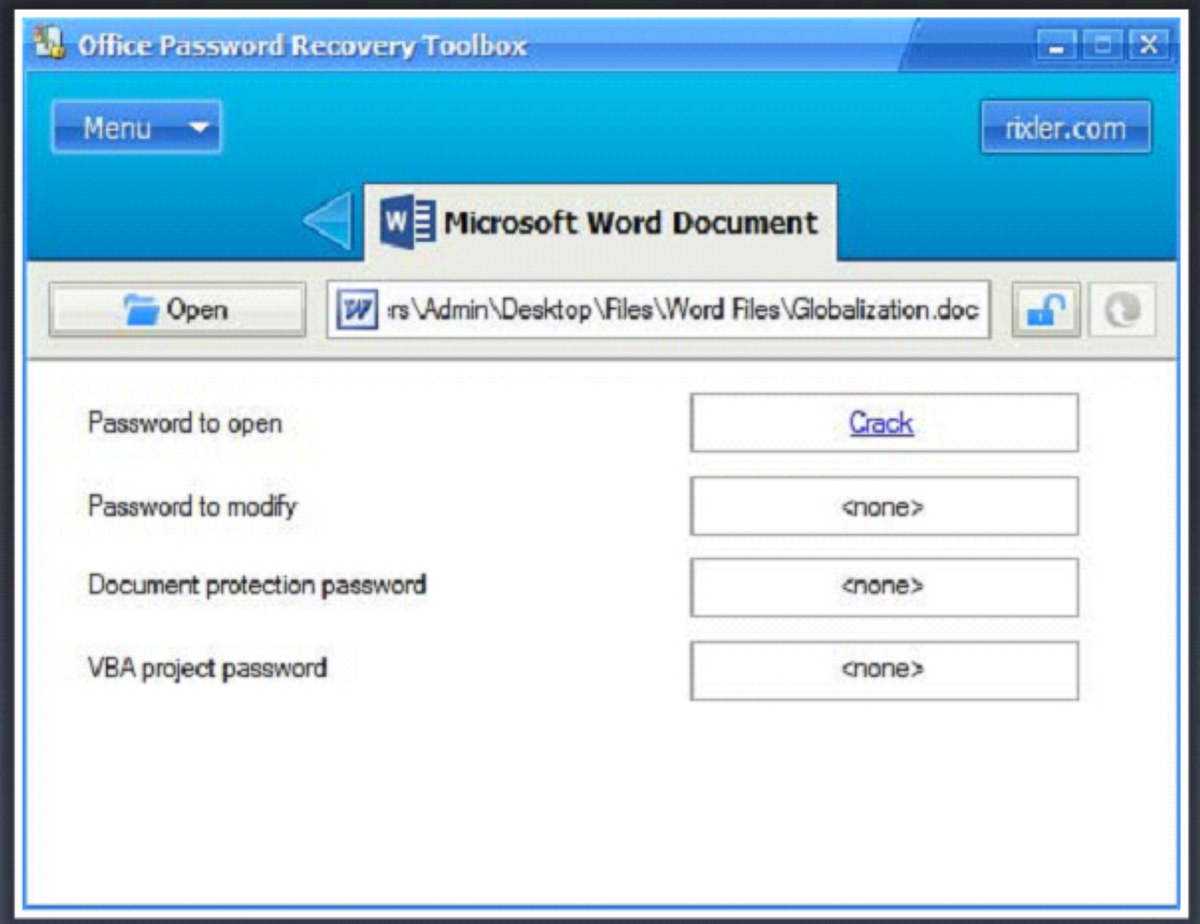
Recovers, replaces, removes or circumvents passwords instantly, protecting or locking documents created with Microsoft Office applications



https://www.elcomsoft.com

Office Password Recovery Toolbox

A comprehensive solution for **recovering** MS Word, Excel, Outlook, Access, PowerPoint, and VBA passwords

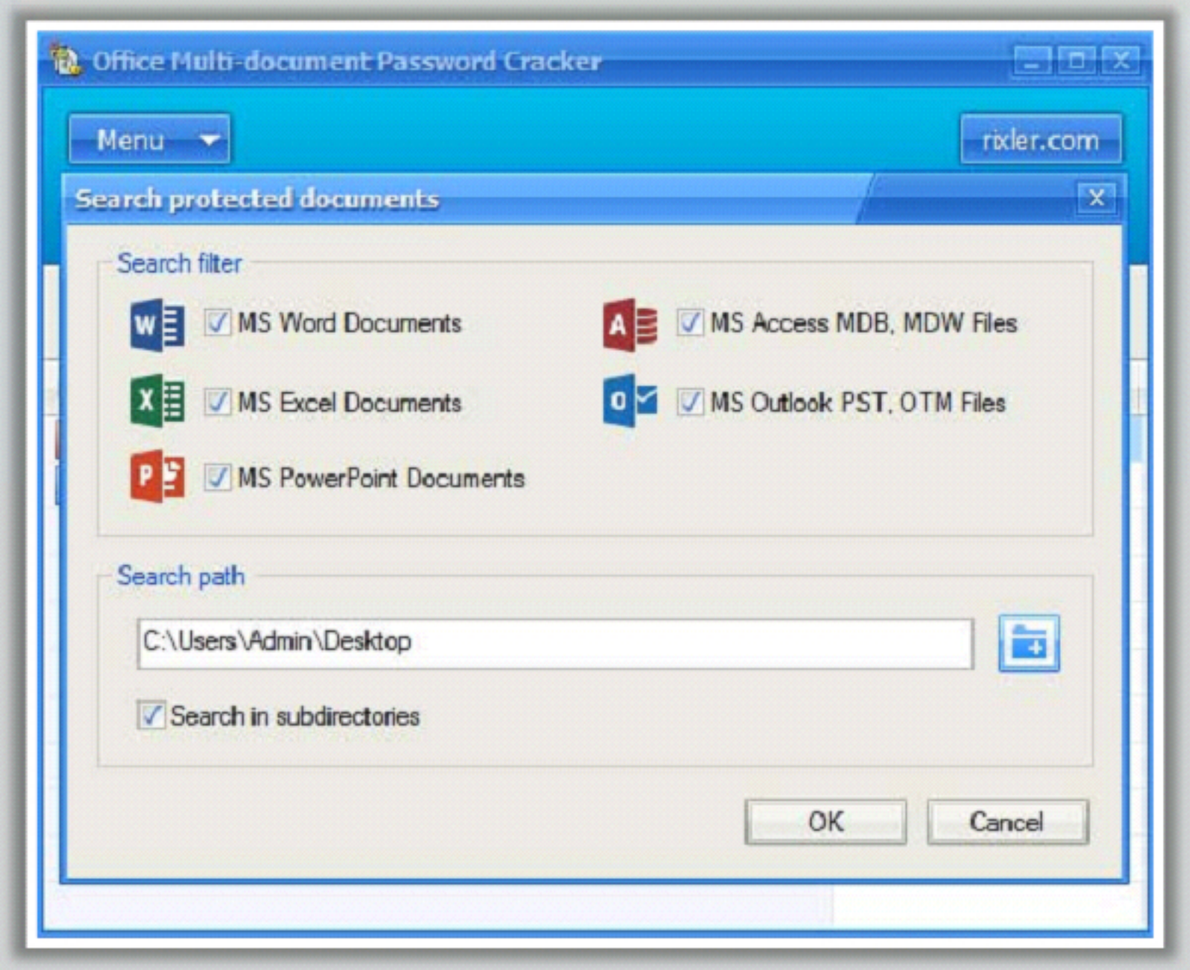


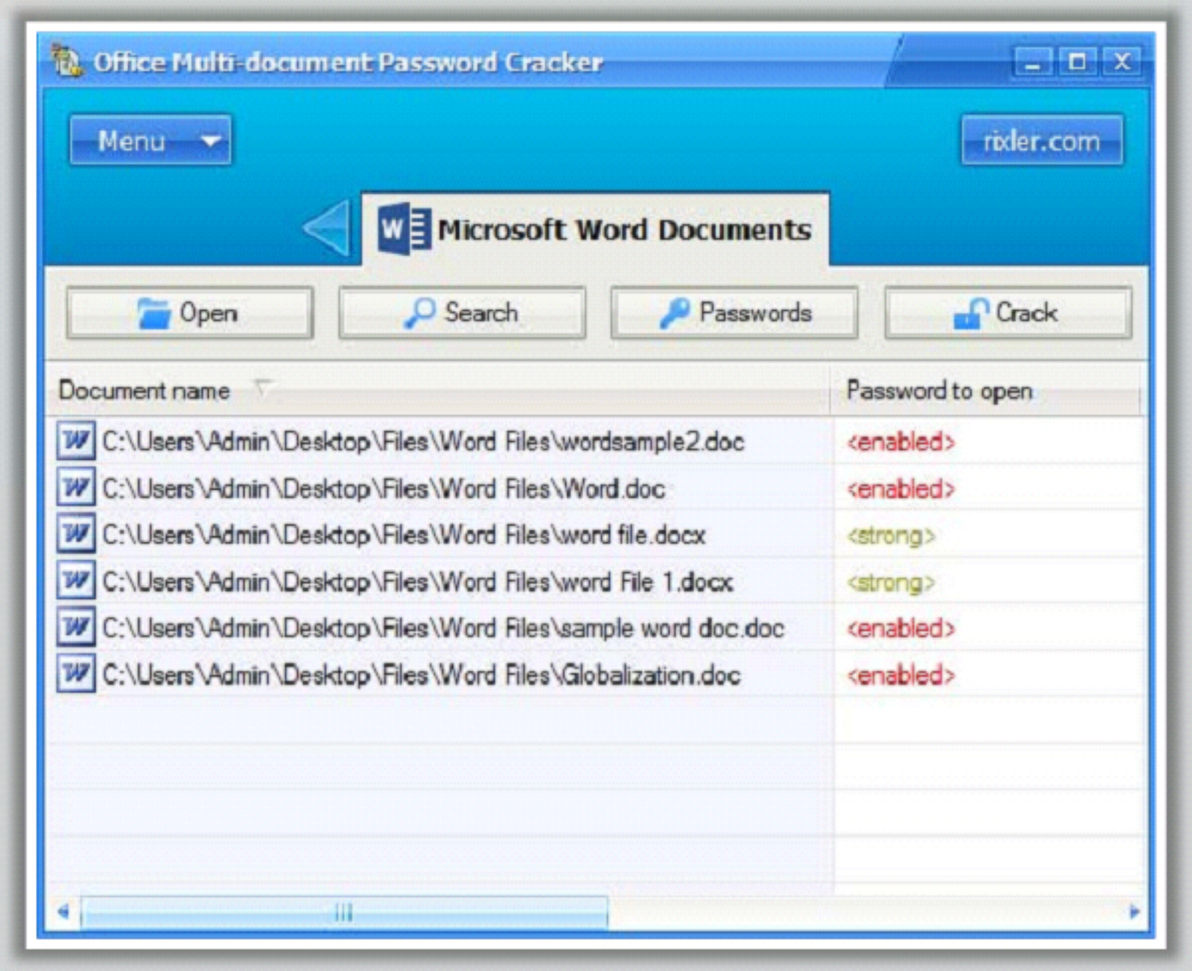
http://www.rixler.com

Application Password Cracking Tools (Cont'd)

Office Multi-document Password Cracker

- Recovers lost or forgotten passwords to multiple MS Office documents
- It scans the drive for protected documents, and restores or deletes passwords from all Word, Excel, PowerPoint, Access, and Outlook files it finds

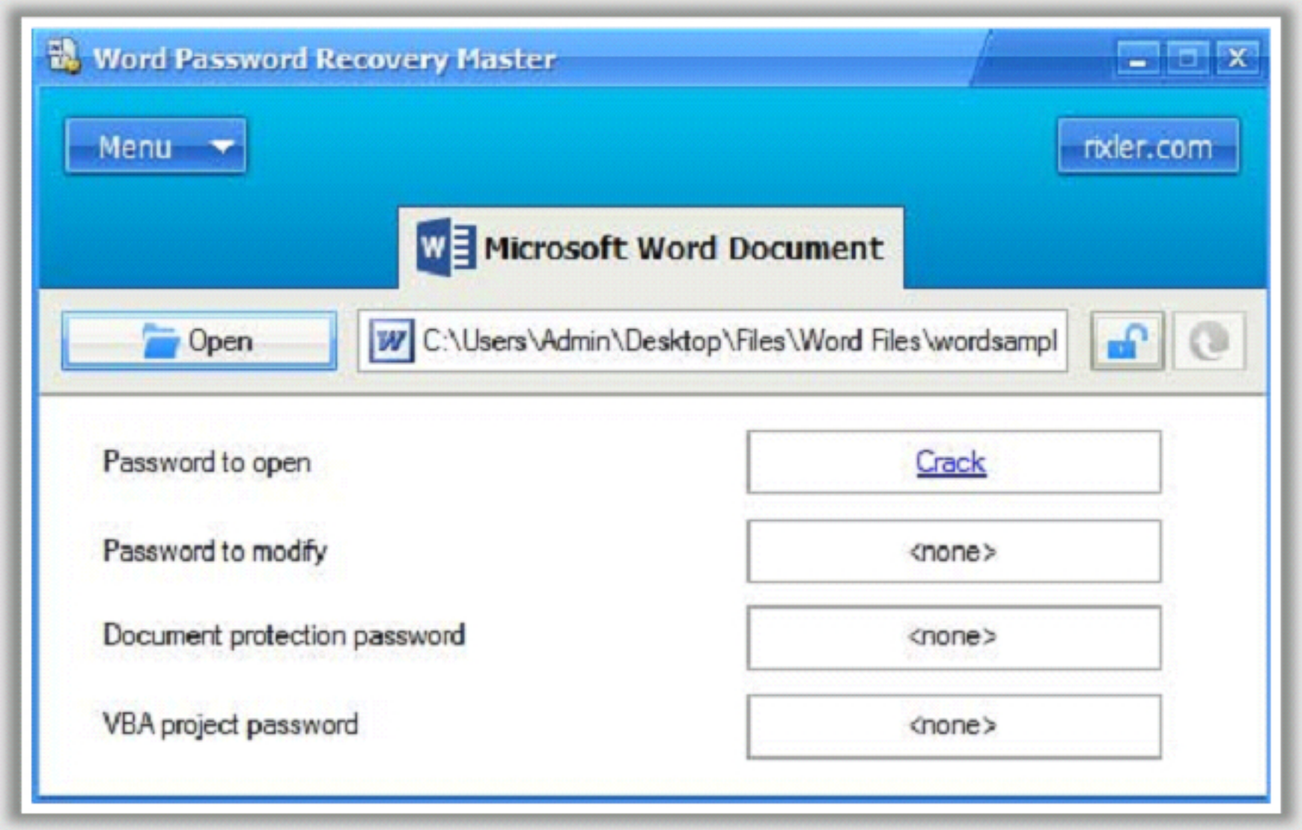




http://www.rixler.com

Word Password Recovery Tools

Word Password Recovery Master



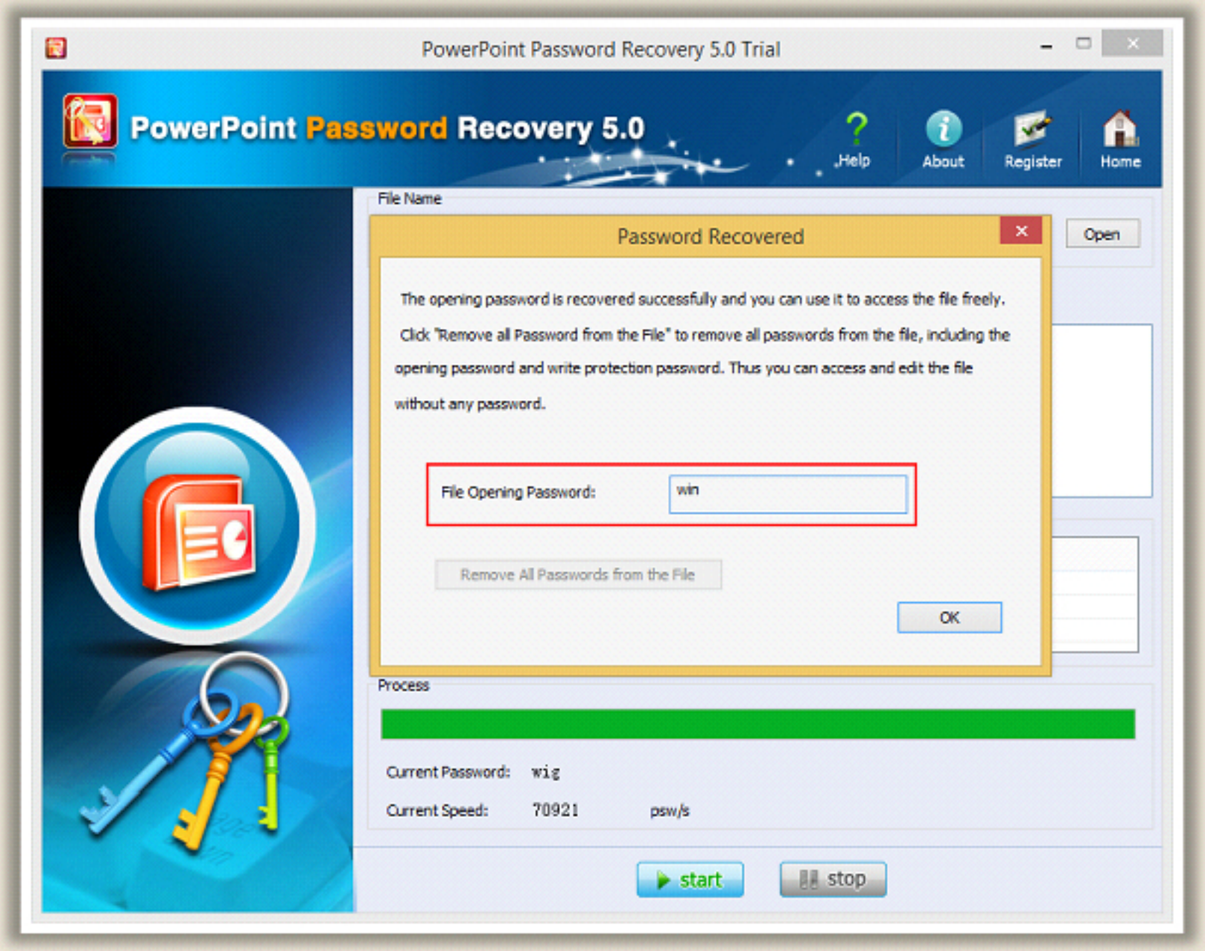
http://www.rixler.com

Accent WORD Password Recovery

http://passwordrecoverytools.com

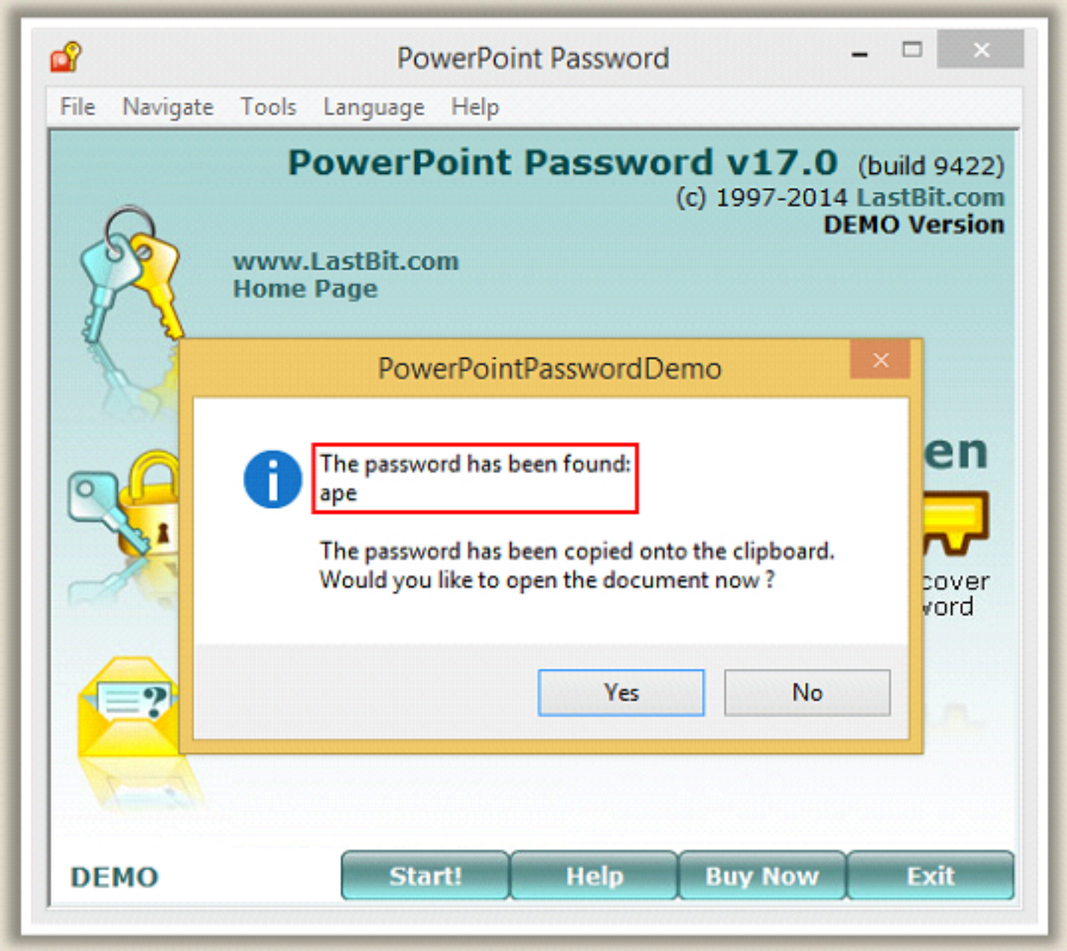
PowerPoint Password Recovery Tools

SmartKey PowerPoint Password Recovery



http://www.recoverlostpassword.com

PowerPoint Password Recovery



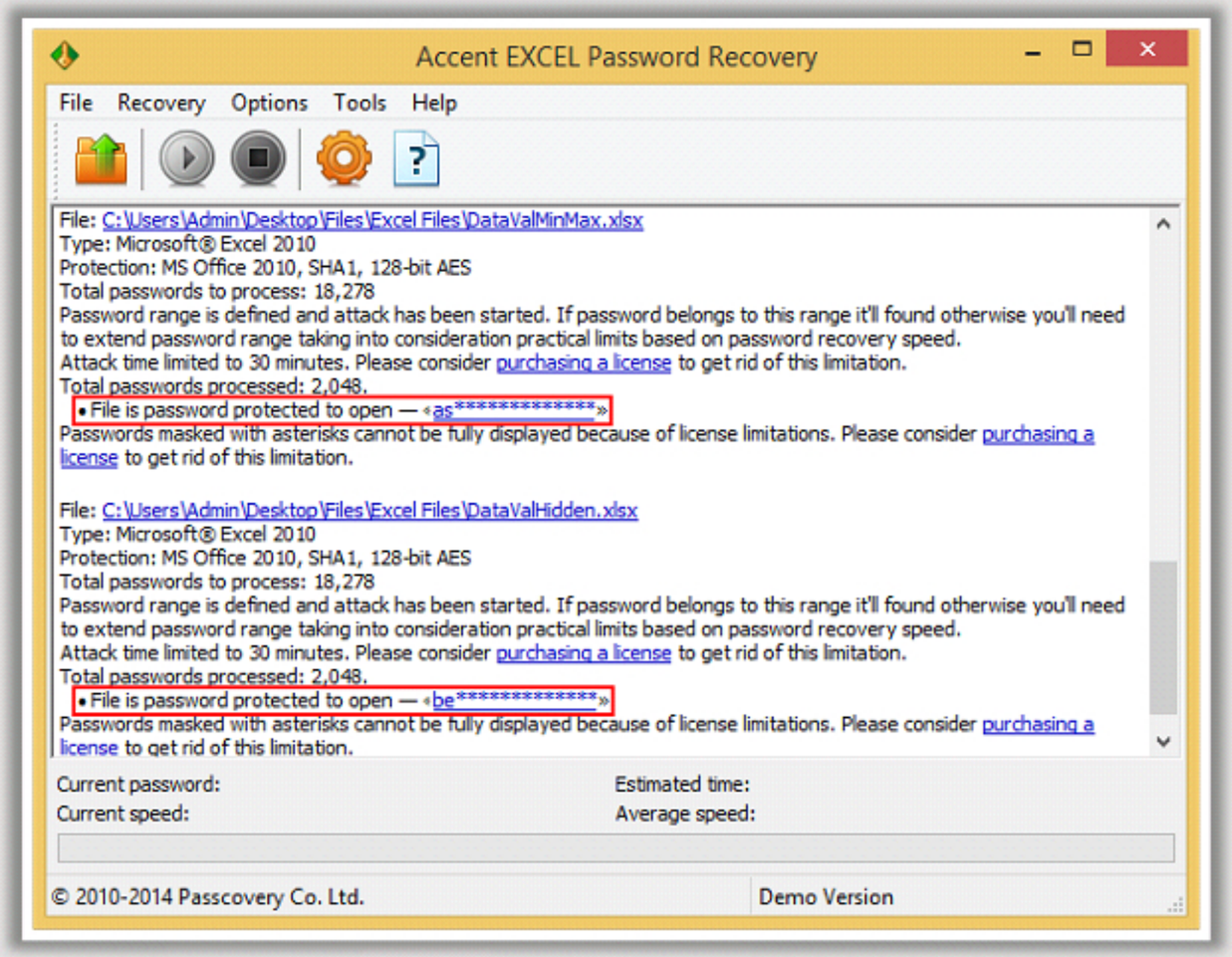
http://passwordtools.com

Excel Password Recovery Tools

PDS Excel Password Recovery

http://www.excelpasswordcracker.com

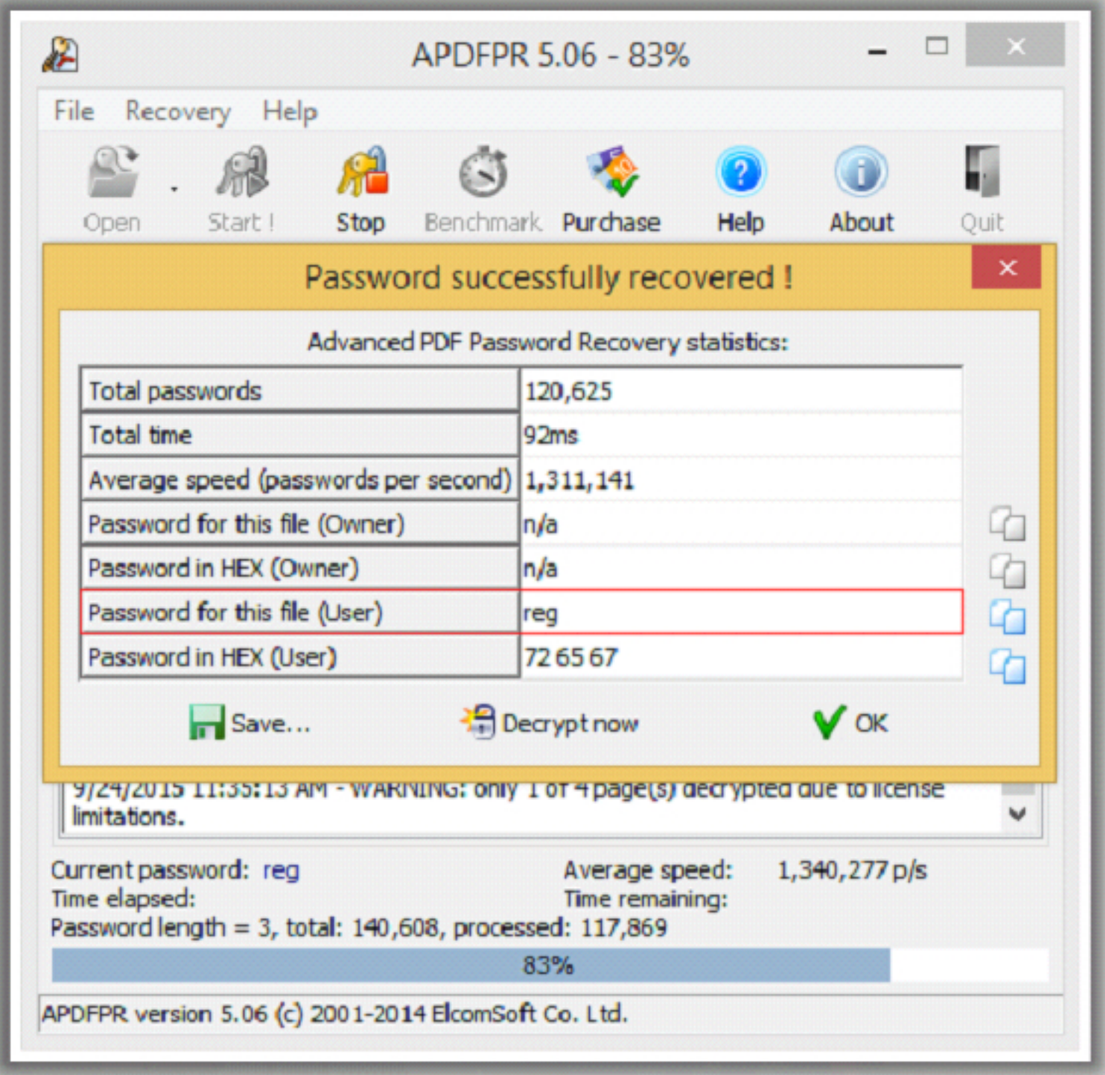
Accent EXCEL Password Recovery



http://www.passwordrecoverytools.com

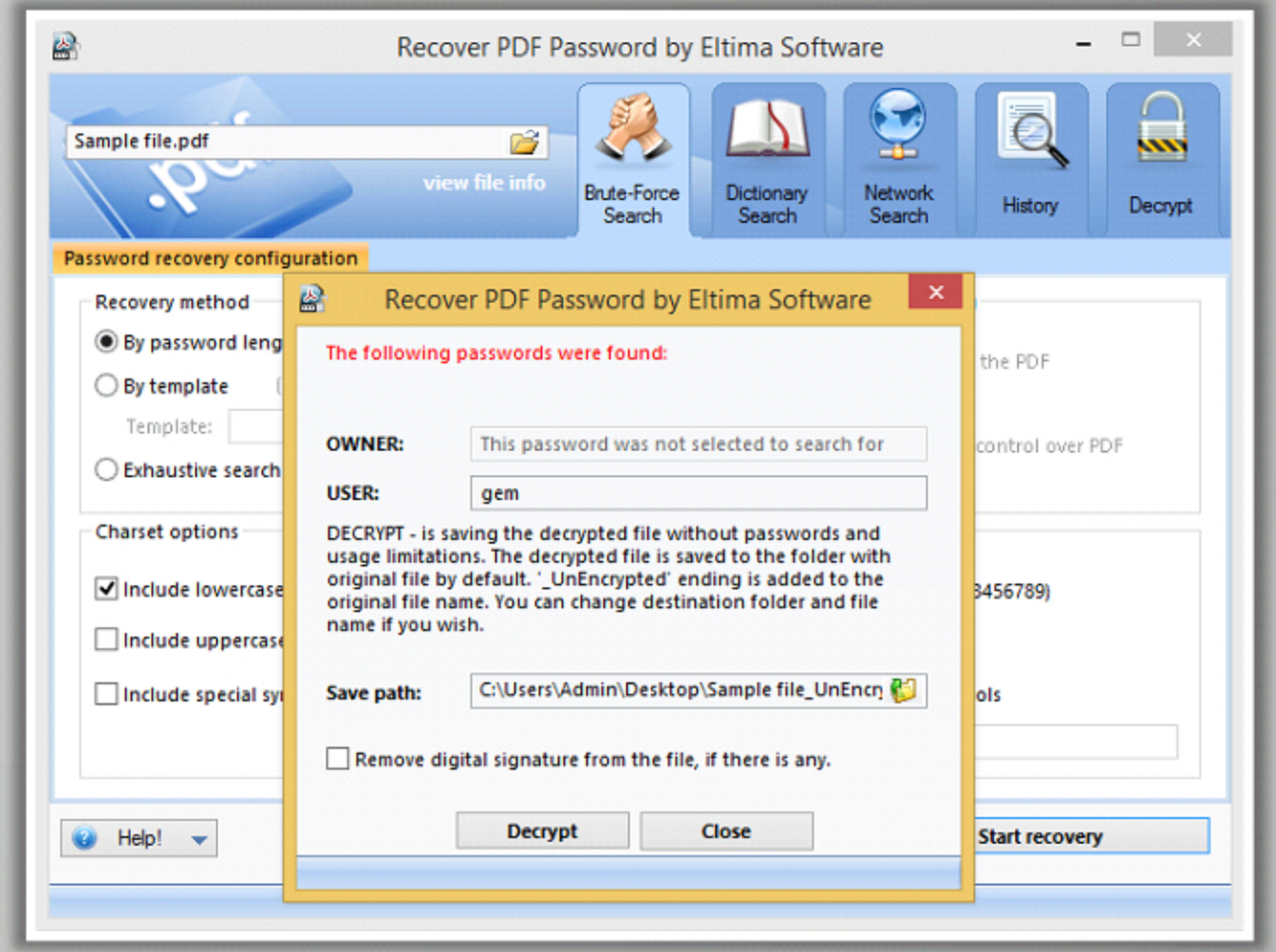
PDF Password Recovery Tools

Advanced PDF Password Recovery



https://www.elcomsoft.com

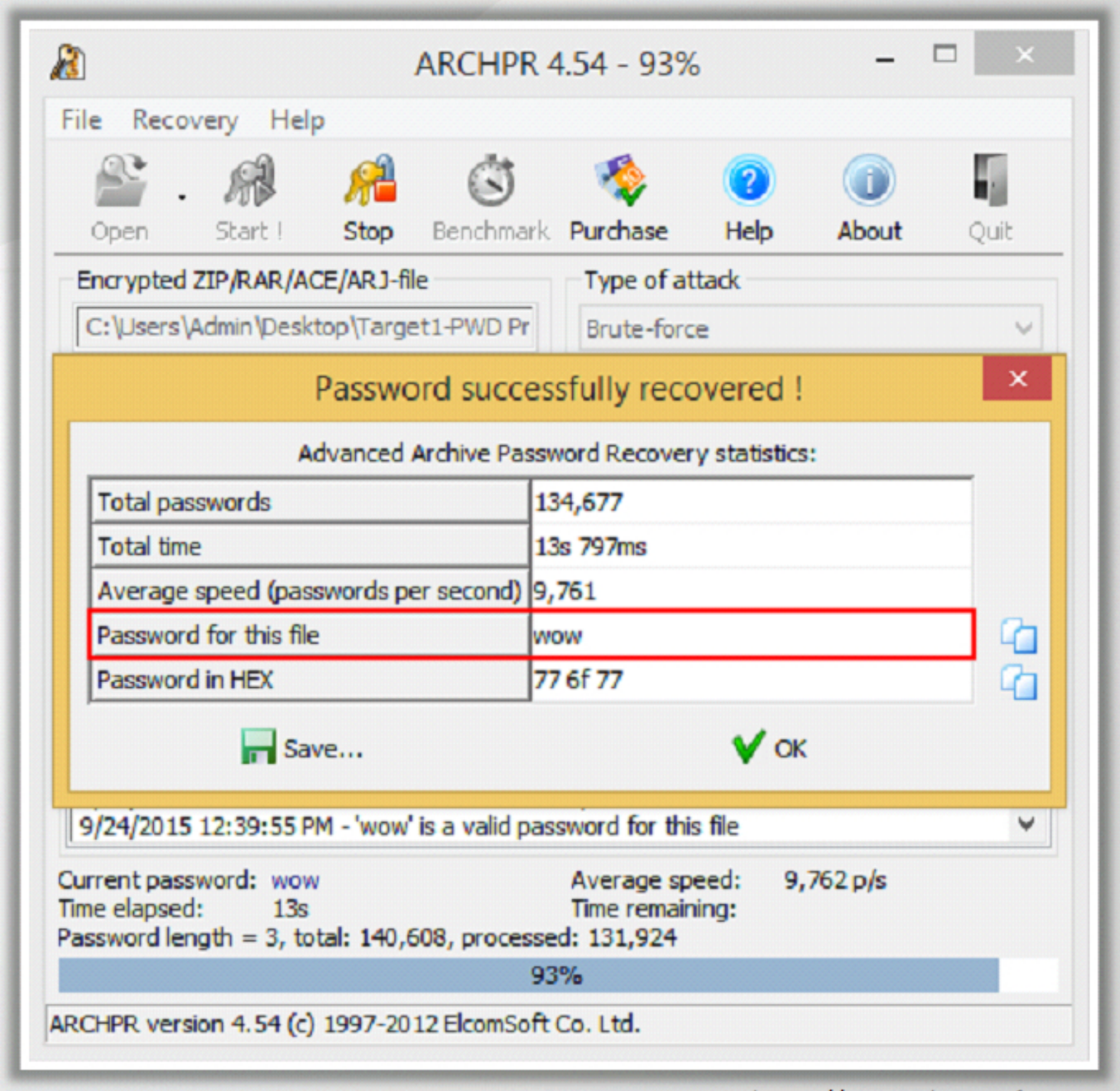
PDF Password Cracker



http://www.crack-pdf-password.com

ZIP/RAR Password Recovery Tool: Advanced Archive Password Recovery

Advanced Archive Password Recovery **recovers protection passwords**, and unlocks encrypted ZIP and RAR archives



https://www.elcomsoft.com

Other Application Software Password Cracking Tools

Office Password Cracking Software

Stellar Phoenix Office Password Recovery
http://www.stellarinfo.com

Online Password Recovery
http://www.password-find.com

Office Password Genius
http://www.isunshare.com

Office Password Recovery Lastic
http://www.passwordlastic.com

SmartKey Office Password Recovery
http://www.recoverlostpassword.com

PDF Cracking Software

PDF Password Recovery
http://www.top-password.com

PDF Password Genius
http://www.isunshare.com

SmartKey PDF Password Recovery
http://www.recoverlostpassword.com

Tenorshare PDF Password Recovery
http://www.tenorshare.com

Guaranteed PDF Decrypter
http://www.guapdf.com

Other Application Software Password Cracking Tools (Cont'd)

ZIP Password Cracking Software

Accent ZIP Password Recovery
http://passwordrecoverytools.com

ZIP Password Genius
http://www.isunshare.com

SmartKey ZIP Password Recovery
http://www.recoverlostpassword.com

KRyLack ZIP Password Recovery
http://www.krylack.com

Stellar Phoenix Zip Password Recovery
http://www.stellarinfo.com

RAR Cracking Software

Accent RAR Password Recovery
http://passwordrecoverytools.com

RAR Password Genius
http://www.isunshare.com

cRARk 5.1
http://www.crark.net

SmartKey RAR Password Recovery
http://www.recoverlostpassword.com

KRyLack RAR Password Recovery
http://www.krylack.com

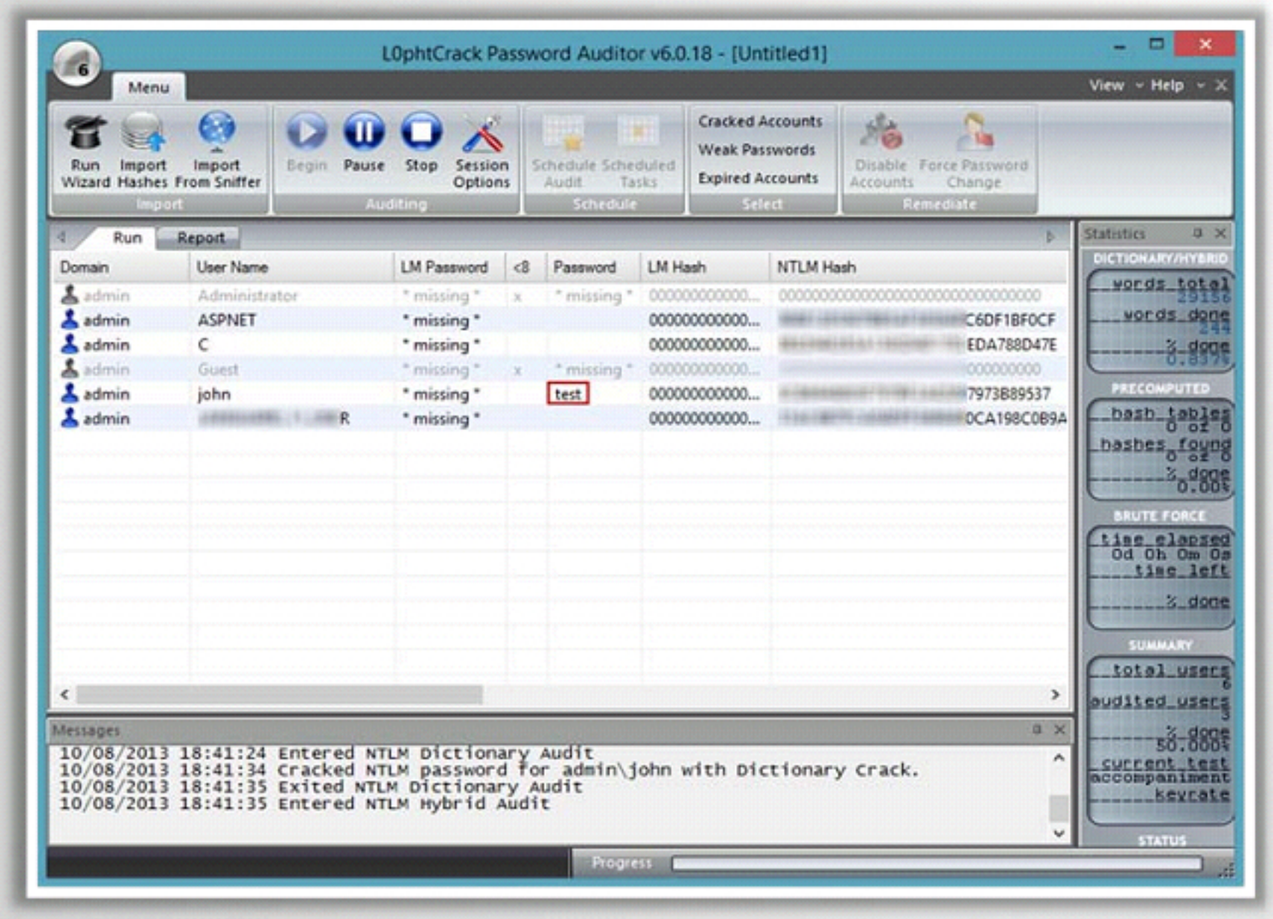
Other Password Cracking Tools

L0phtCrack

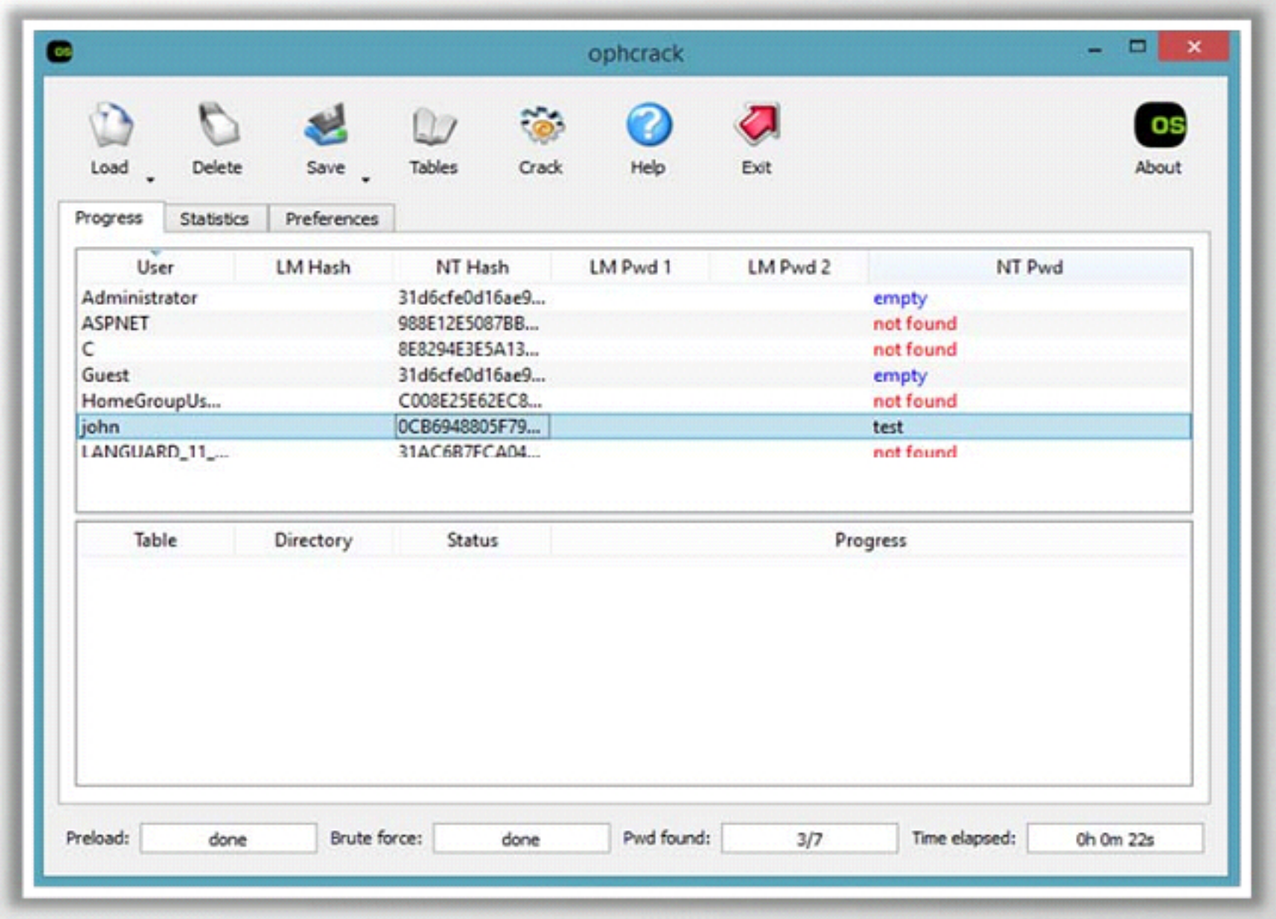
L0phtCrack is a password **auditing** and **recovery** application packed with features such as scheduling, hash extraction from 64-bit Windows versions, and networks monitoring and decoding

Ophcrack

Ophcrack is a Windows password cracker based on **rainbow tables**. It comes with a Graphical User Interface and runs on multiple platforms



http://www.l0phtcrack.com

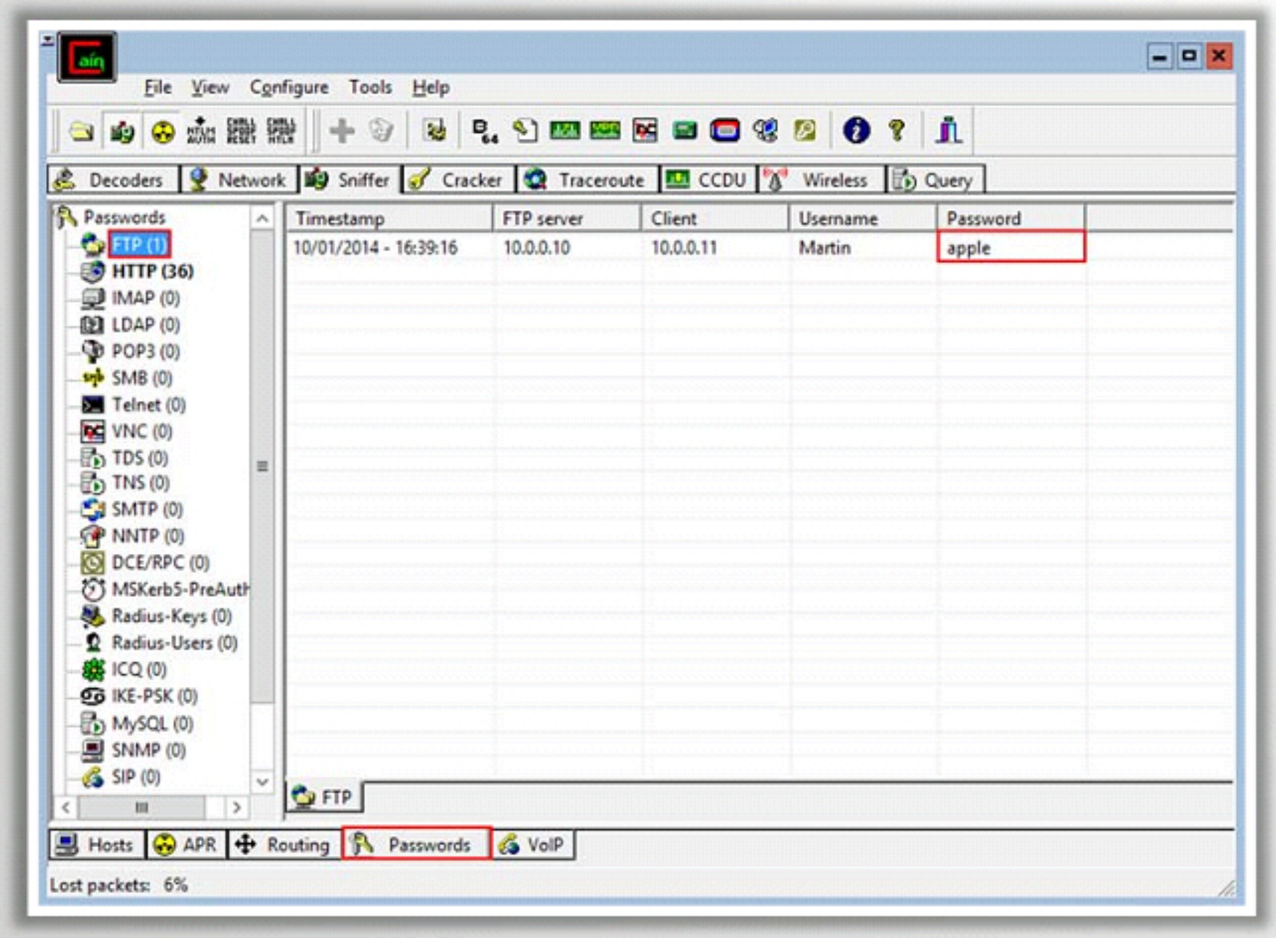


http://ophcrack.sourceforge.net

Other Password Cracking Tools (Cont'd)

Cain & Abel

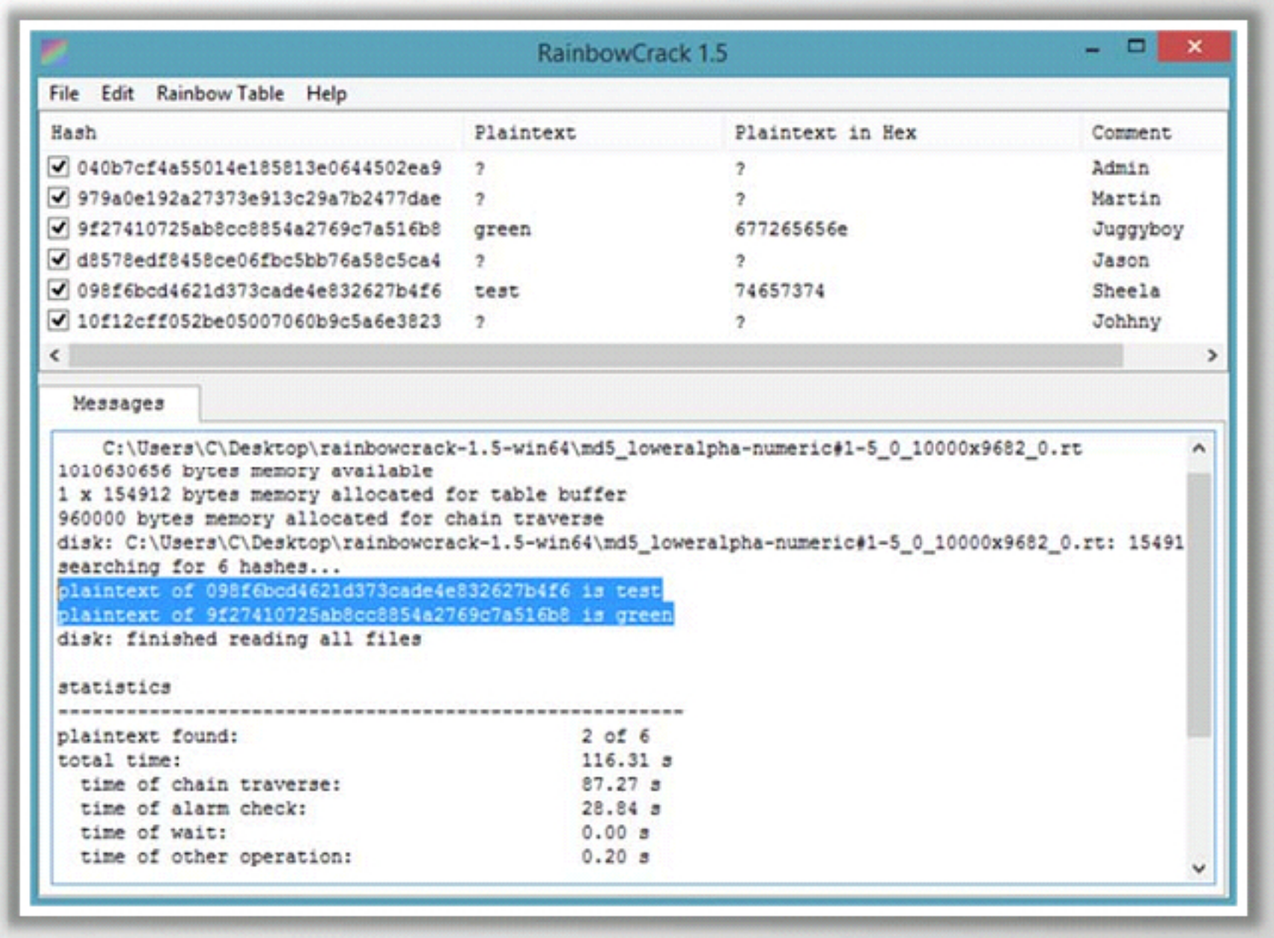
- It allows recovery of various kind of passwords by **sniffing the network**, and **cracking encrypted passwords** using dictionary, brute-force, and cryptanalysis attacks



http://www.oxid.it

RainbowCrack

- RainbowCrack cracks hashes with **rainbow tables**. It uses **time-memory tradeoff** algorithm to crack hashes

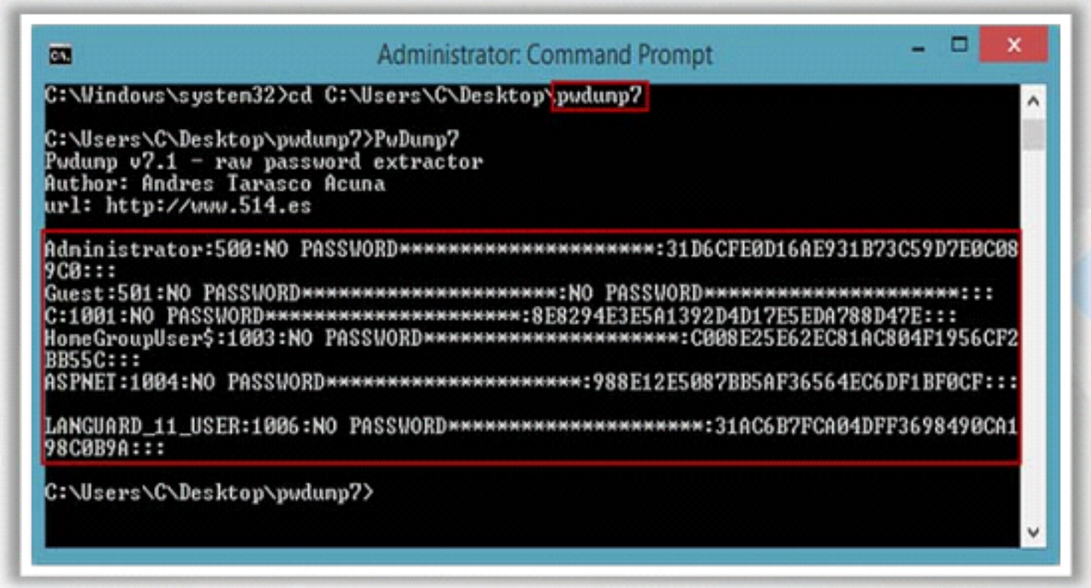


http://project-rainbowcrack.com

Other Password Cracking Tools (Cont'd)

pwdump7 and fgdump

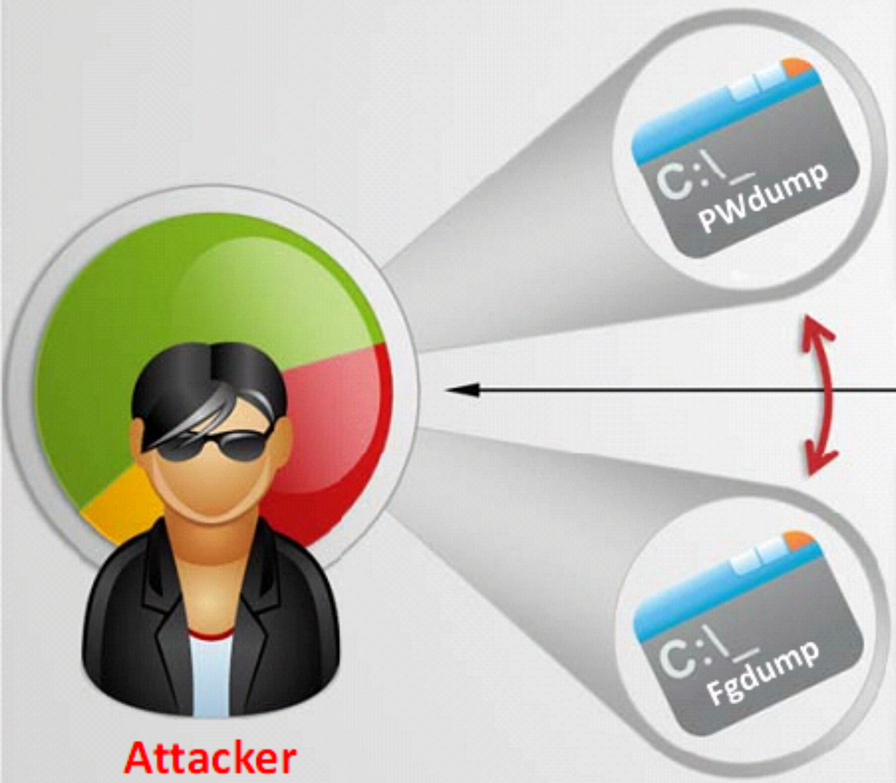
pwdump7.exe

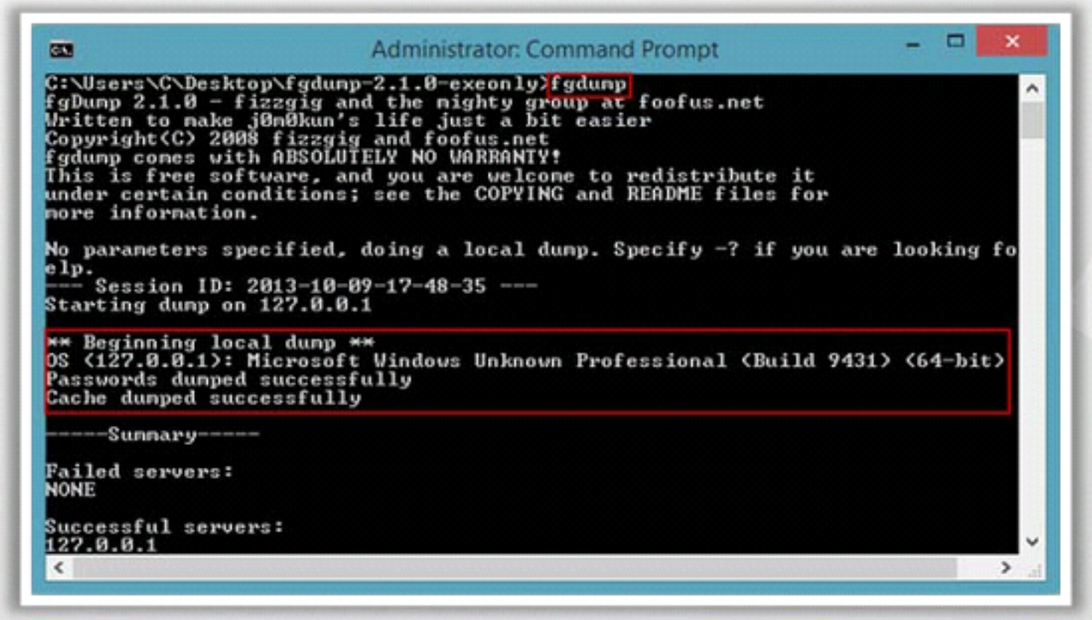


http://www.tarasco.org

PWDUMP extracts LM and NTLM password hashes of local user accounts from the database

fgdump works like pwdump but also extracts cached credentials and allows remote network execution





http://foofus.net

```
fgdump.exe -h 192.168.0.10
-u AnAdministrativeUser -p
14mep4ssw0rd
```

Dumps a remote machine (192.168.0.10) using a specified user

These tools must be run with administrator privileges

Other Password Cracking Tools (Cont'd)

Offline NT Password & Registry Editor
http://pogostick.net

Active@ Password Changer
http://www.password-changer.com

Password Unlocker Bundle
http://www.passwordunlocker.com

Passware Kit Standard
https://www.passware.com

Proactive System Password Recovery
https://www.elcomsoft.com

Windows Password Unlocker
https://www.passwordunlocker.com

John the Ripper
http://www.openwall.com

LSASecretsView
http://www.nirsoft.net

Wfuzz
http://www.edge-security.com

LCP
http://www.lcpsoft.com

Other Password Cracking Tools (Cont'd)

Password Cracker
http://www.amlpages.com

Windows Password Recovery
http://www.passcape.com

Kon-Boot
http://www.thelead82.com

Password Recovery Bundle
http://www.top-password.com

Windows Password Recovery Tool
http://www.windowspasswordsrecovery.com

iSunshare Windows Password Genius
http://www.isunshare.com

Hash Suite
http://hashsuite.openwall.net

THC-Hydra
https://www.thc.org

InsidePro
http://www.insidepro.com

Windows Password Breaker Enterprise
http://www.recoverwindowspassword.com

Anti-Forensics Techniques: Steganography

Steganography is a technique of **hiding a secret message** within an ordinary message, and **extracting it at the destination** to maintain confidentiality of data

Often, intruders use the steganography technique to hide information about their illegal activity (**list of the compromised servers**, source code for the hacking tool, plans for future attacks, etc.)

Utilizing a graphic image as a cover is the most popular method to conceal the data in files

Steganography disrupts the process of forensics investigation, which can, however, be overcome by using **steganalysis tools** and techniques

Types of Steganography, based on Cover Medium

Image Steganography

Audio Steganography

White Space Steganography

Natural Text Steganography

Document Steganography

Video Steganography

DVD-ROM Steganography

Hidden OS Steganography

Folder Steganography

Spam/email Steganography

Web Steganography

C++ Source Code Steganography

Steganalysis

- Steganalysis is the art of discovering and rendering covert messages using steganography

Challenge of Steganalysis

- Suspect information stream may or may not have encoded hidden data
- Efficient and accurate detection of hidden content within digital images is difficult
- The message might have been encrypted before insertion into a file or signal
- Some of the suspect signals or files may have irrelevant data or noise encoded into them

Steganalysis Methods/Attacks on Steganography

Only the stego-object is available for analysis	**Stego -only**	**Known -cover**	Comparison of the stego-object and the cover medium is done to identify the hidden message
You will have access to the stego algorithm, and both the cover medium and the stego-object	**Known -stego**	**Chosen -message**	Generates stego objects from a known message using specific steganography tools in order to identify the steganography algorithms
You will have access to the hidden message and the stego-object	**Known -message**	**Chosen -stego**	You will have access to the stego-object and stego algorithm

Detecting Steganography

Software Clues on the Computer

- Steganographic investigators need to be familiar with the names of common **steganographic software** and related terminology, and websites about steganography
- **Investigators look** for file names, website references in browser cookie/history files, registry key entries, email messages, chat/instant messaging logs, comments made by the suspect or receipts that refer to steganography
- These will provide **hard clues** for the investigator to probe deeper

Other Program Files

- **Non-steganographic software** might offer clues that the suspect hides files inside other files
- Users with binary (hex) editors, disk wiping software, or specialized chat software might demonstrate an inclination to alter files and **keep information secret**

Detecting Steganography (Cont'd)

Multimedia Files

- Look for the **presence** of a large volume of suitable **carrier files**
- A computer system with an especially large number of files could be **steganographic carriers**, and are potential suspects
- This is particularly true if there are a significant number of seemingly **duplicate "carrier" files**

Type of Crime

- The type of crime being investigated may also make an investigator think more about **steganography** than other types of crime
- Child pornographers, for example, might use steganography to **hide their wares** when posting pictures on a website or sending them through email
- Crimes that involve **business type records** are also examples where steganography might be used because the **perpetrator** can hide the files but still get access to them; consider accounting fraud, identity theft (lists of stolen credit cards), drugs, gambling, hacking, smuggling, terrorism, and more

Detecting Steganography (Cont'd)

Text File

- For text files, alterations are made to the **character positions** for hiding the data
- The alterations are detected by looking for **text patterns** or disturbances, language used, and an unusual amount of blank spaces

Image File

- The hidden data in an image can be detected by **determining changes** in size, file format, the last modified timestamp, and the color palette pointing to the existence of the hidden data
- **Statistical analysis** method is used for image scanning

Detecting Steganography (Cont'd)

Audio File

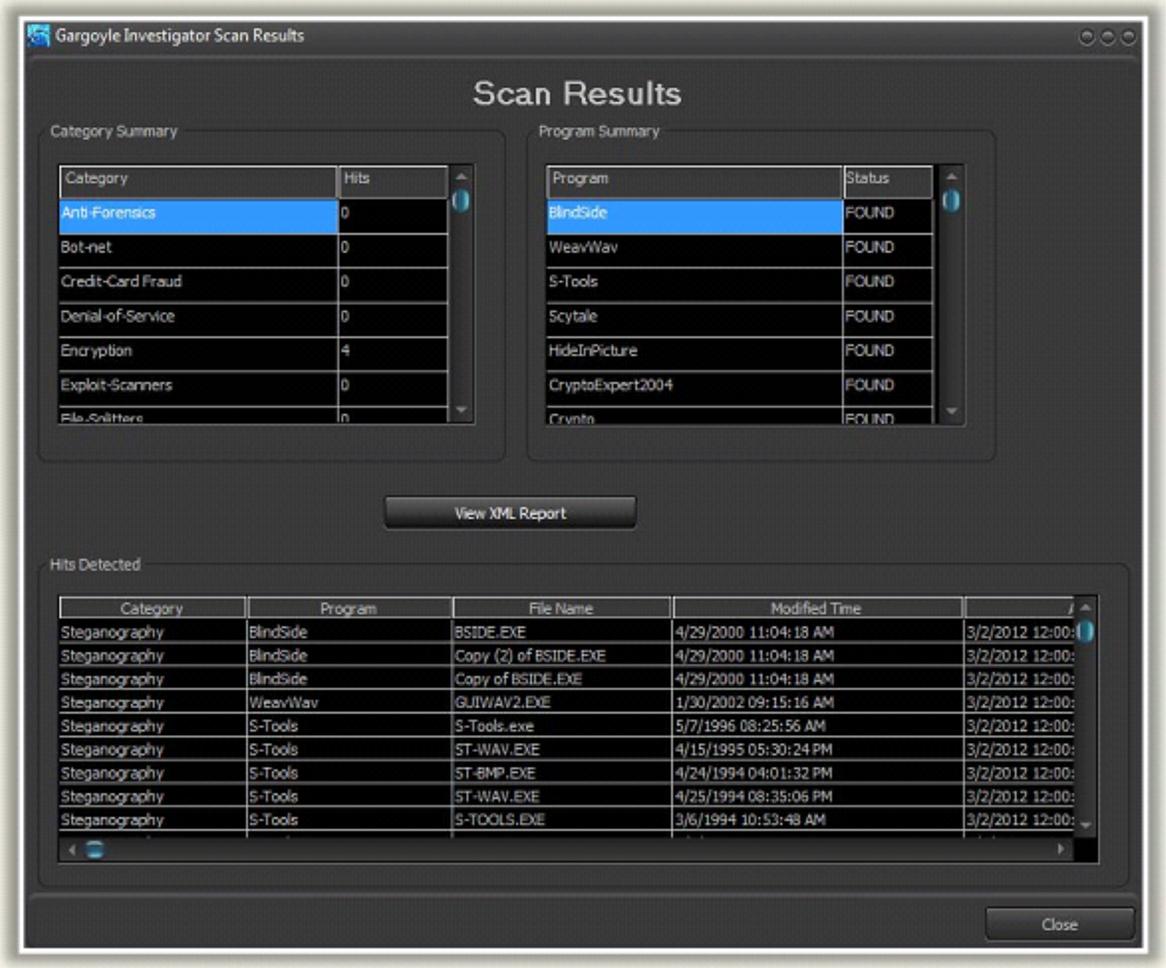
- Statistical analysis method can be used for detecting audio steganography as it involves **Least Significant Bit** (LSB) **modifications**
- **Inaudible frequencies** can be scanned for hidden information
- **Odd distortions and patterns** show the existence of the secret data

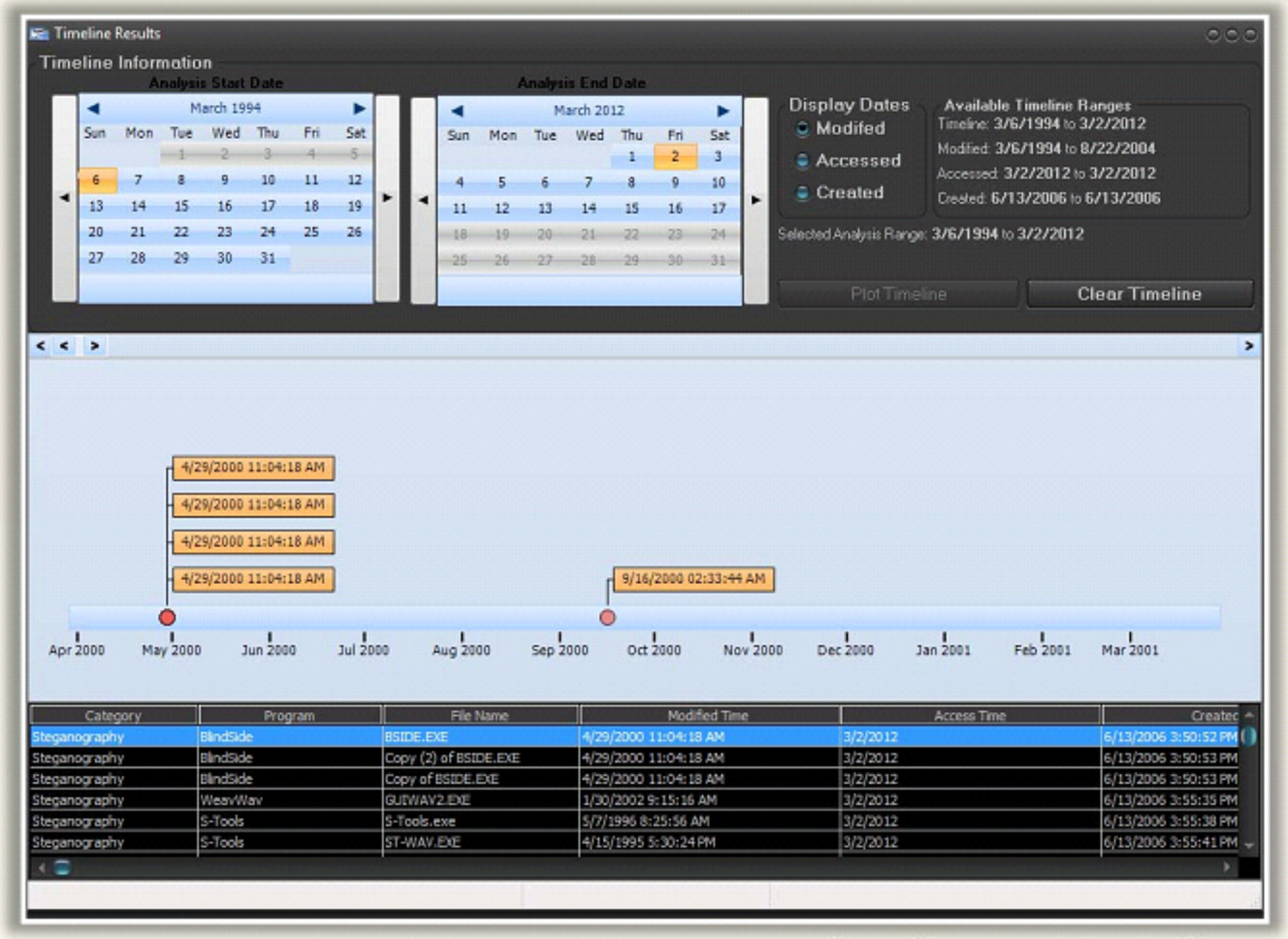
Video File

- Detection of the secret data in video files includes a **combination of methods** used in image and audio files
- Special code **signs** and **gestures** can also be used for detecting **secret data**

Steganography Detection Tool: Gargoyle Investigator™ Forensic Pro

- Gargoyle Investigator™ Forensic Pro provides inspectors with the ability to conduct a quick search on a given computer or machine for known **contraband** and **hostile programs**
- Its **signature set** contains over 20 categories, including Botnets, Trojans, Steganography, Encryption, Keyloggers, etc. It helps in detecting stego files by using BlindSide, WeavWav, S-Tools, and other steganography tools





http://www.wetstonetech.com

Steganography Detection Tools

Xstegsecret
http://stegsecret.sourceforge.net

StegSecret
http://stegsecret.sourceforge.net

StegAlyzerAS
http://www.sarc-wv.com

StegAlyzerRTS
http://www.sarc-wv.com

StegExpose
https://github.com

StegAlyzerSS
http://www.sarc-wv.com

Steganography Studio
http://stegstudio.sourceforge.net

Virtual Steganographic Laboratory (VSL)
http://vsl.sourceforge.net

Stegdetect
https://github.com

ImgStegano
http://www1.chapman.edu

Anti-Forensics Techniques: Data Hiding in File System Structures

Intruders use tools and techniques that **hide data in various locations of a computer system** (slack space, memory, hidden directories, hidden partitions, bad blocks, ADSs, etc.), which are often overlooked by modern forensic tools

- **Slacker** — Part of the Metasploit framework that hides data in the slack space of NTFS file system
- **FragFS** — Hides data within the NTFS Master File Table (MFT)
- **RuneFS** — Hides data in "bad blocks" inode
- **KY FS** — Hides data in null directory entries
- **Waffen FS** – Hides data in ext3 journal file
- **Data Mule FS** — Hides data in inode reserved space

Other areas where data can be hidden include:

- Host Protected Areas (HPA) and Device Configuration Overlay (DCO) areas of modern ATA hard drives
- Data hidden in these areas is not visible to the BIOS or OS, but it can be extracted with special tools

Anti-Forensics Techniques: Trail Obfuscation

- The purpose of trail obfuscation is to **confuse**, **disorient**, and **distract the forensics investigation process**
- Attackers **mislead investigators** via log tampering, false e-mail header generation, timestamp modification, and various file headers' modification

Some of the techniques attackers use for data/trail obfuscation:

- Log cleaners
- Spoofing
- Misinformation
- Zombie accounts
- Trojan commands

Traffic content obfuscation can be attained by means of VPNs and SSH tunneling

Anti-Forensics Techniques: Trail Obfuscation (Cont'd)

Timestomp is one of the most widely used trail obfuscation tools that allow **deletion** or **modification** of **timestamp-related** information on files

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
meterpreter > timestomp secret.txt -v
Modified      : 2014-03-07 12:56:07 +0530
Accessed      : 2014-03-07 12:50:51 +0530
Created       : 2014-03-07 12:45:51 +0530
Entry Modified: 2014-03-07 12:56:07 +0530
meterpreter >
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
meterpreter > timestomp secret.txt -v
Modified      : 2014-03-07 12:56:07 +0530
Accessed      : 2014-03-07 12:50:51 +0530
Created       : 2014-03-07 12:45:51 +0530
Entry Modified: 2014-03-07 12:56:07 +0530
meterpreter > timestomp secret.txt -m "06/15/2012 12:57:37"
[*] Setting specific MACE attributes on secret.txt
meterpreter >
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Accessed      : 2014-03-07 12:50:51 +0530
Created       : 2014-03-07 12:45:51 +0530
Entry Modified: 2014-03-07 12:56:07 +0530
meterpreter > timestomp secret.txt -m "06/15/2012 12:57:37"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -a "06/15/2012 12:55:05"
[*] Setting specific MACE attributes on secret.txt
meterpreter >
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Entry Modified: 2014-03-07 12:56:07 +0530
meterpreter > timestomp secret.txt -m "06/15/2012 12:57:37"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -a "06/15/2012 12:55:05"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -c "06/12/2012 12:50:22"
[*] Setting specific MACE attributes on secret.txt
meterpreter >
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -a "06/15/2012 12:55:05"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -c "06/12/2012 12:50:22"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -e "06/15/2012 13:59:48"
[*] Setting specific MACE attributes on secret.txt
meterpreter >
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
meterpreter > timestomp secret.txt -v
Modified      : 2012-06-15 13:57:37 +0530
Accessed      : 2012-06-15 13:55:05 +0530
Created       : 2012-06-12 13:50:22 +0530
Entry Modified: 2012-06-15 14:59:48 +0530
meterpreter >
```

Anti-Forensics Techniques: Artifact Wiping

- Artifact wiping involves various methods aimed at **permanent deletion** of particular files or entire file systems

Artifact wiping methods:

Disk Cleaning Utilities

- Uses various methods to overwrite the existing data on disks
- Some of the commonly used disk cleaning utilities include BCWipe Total WipeOut, Active@ KillDisk, CyberScrub's cyberCide, DriveScrubber, ShredIt, Secure Erase, etc.

File Wiping Utilities

- Deletes individual files from an operating system
- Some of the commonly used file wiping utilities include BCWipe, R-Wipe & Clean, Eraser, CyberScrubs PrivacySuite, etc.

http://www.recovermyemail.com

Anti-Forensics Techniques: Artifact Wiping (Cont'd)

Disk degaussing/destruction techniques

- Disk degaussing is a process by which a **magnetic field** is applied to a digital media device, resulting in a entirely clean device of any previously stored data
- **Physical destruction** of the device is one of the most widely used techniques to ensure data wiping
- NIST recommends a variety of methods to accomplish **physical destruction of the digital media**, which includes disintegration, incineration, pulverizing, shredding and melting
- Intruders use disk degaussing/destruction techniques to **make the evidentiary data unavailable** to forensics investigators

Anti-Forensics Techniques: Overwriting Data/Metadata

- Intruders use various programs to overwrite data on a storage device, making it difficult or impossible to recover. These programs can overwrite data, metadata, or both
- Overwriting programs (disk sanitizers) work in three modes:
  - Overwrite entire media
  - Overwrite individual files
  - Overwrite deleted files on the media

Overwriting Metadata:

- Investigators use metadata to create a timeline of attacker actions by organizing all of the computer's timestamps in sequential order
- Though, attackers can use tools to wipe the contents of media, that action itself might draw the attention of investigators, therefore, attackers cover their tracks by overwriting the metadata (i.e. access times), rendering the construction of timeline difficult
- Ex: Timestomp (part of the Metasploit Framework) is used to change MACE (Modified-Accessed-Created-Entry) attributes of the file
- Another way to overwrite metadata is to access the computer in such a way that metadata is not created

  Examples: Mounting a partition as read-only, or accessing through the raw device, prevents the file access times from being updated

  Setting Windows registry key "**HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate**" to **1** disables updating of the last-accessed timestamp

Anti-Forensics Techniques: Encryption

- Data encryption is one of the commonly used techniques to **defeat forensics investigation process**
- Intruders use strong encryption algorithms to encrypt data of investigative value, which renders it virtually unreadable without the **designated key**
- Also, most encryption programs are capable to perform additional functions which include use of a key file, **full-volume encryption**, and plausible deniability that makes the investigator's job more difficult
- Built-in encryption utilities provided by Microsoft for Windows 7 and later:
  - **BitLocker** encrypts an entire volume
  - **Encrypting File System (EFS)** - encrypts individual files and directories
- **VeraCrypt** is one of the most widely used tools for anti-forensics encryption

Encrypting File System (EFS): Recovery Certificate

You can recover EFS-encrypted files in case of a damaged or lost encryption key by means of a recovery certificate

Note: You must be logged on as an **administrator** to perform the steps given below. Also, the given steps are not applicable to Windows 7 (Starter, Home basic, and Home Premium)

Step 1: Create the recovery certificate

- Open a Command Prompt window
- Insert a removable media such as a disc or USB drive to store the certificate
- Navigate to the directory on the removable media drive where you want to store the recovery certificate by typing in the removable media drive letter, and then press Enter
- Type cipher /r:<file name> (file name is the name to be given for the recovery certificate), and press Enter
- Note: If prompted for an administrator password or confirmation, type the password or provide confirmation

Encrypting File System (EFS): Recovery Certificate (Cont'd)

C|HFI Computer Hacking Forensic Investigator

Step 2: Install the recovery certificate

- Insert the removable media that contains the recovery certificate
- In the Run utility, type **secpol.msc**, and press Enter
- Note: If prompted for an administrator password or confirmation, type the password or provide confirmation
- In the left pane, double-click **Public Key Policies**, right-click **Encrypting File System**, and then click **Add Data Recovery Agent**...
- In the **Add Recovery Agent Wizard**, click **Next**, and then navigate to the recovery certificate
- Click the certificate and click **Open.** When asked if you want to install the certificate, click **Yes**, click **Next**, and then click **Finish**
- Now open a **Command Prompt window**, type **gpupdate**, and then press **Enter**

Step 3: Update the encrypted files with new recovery certificate

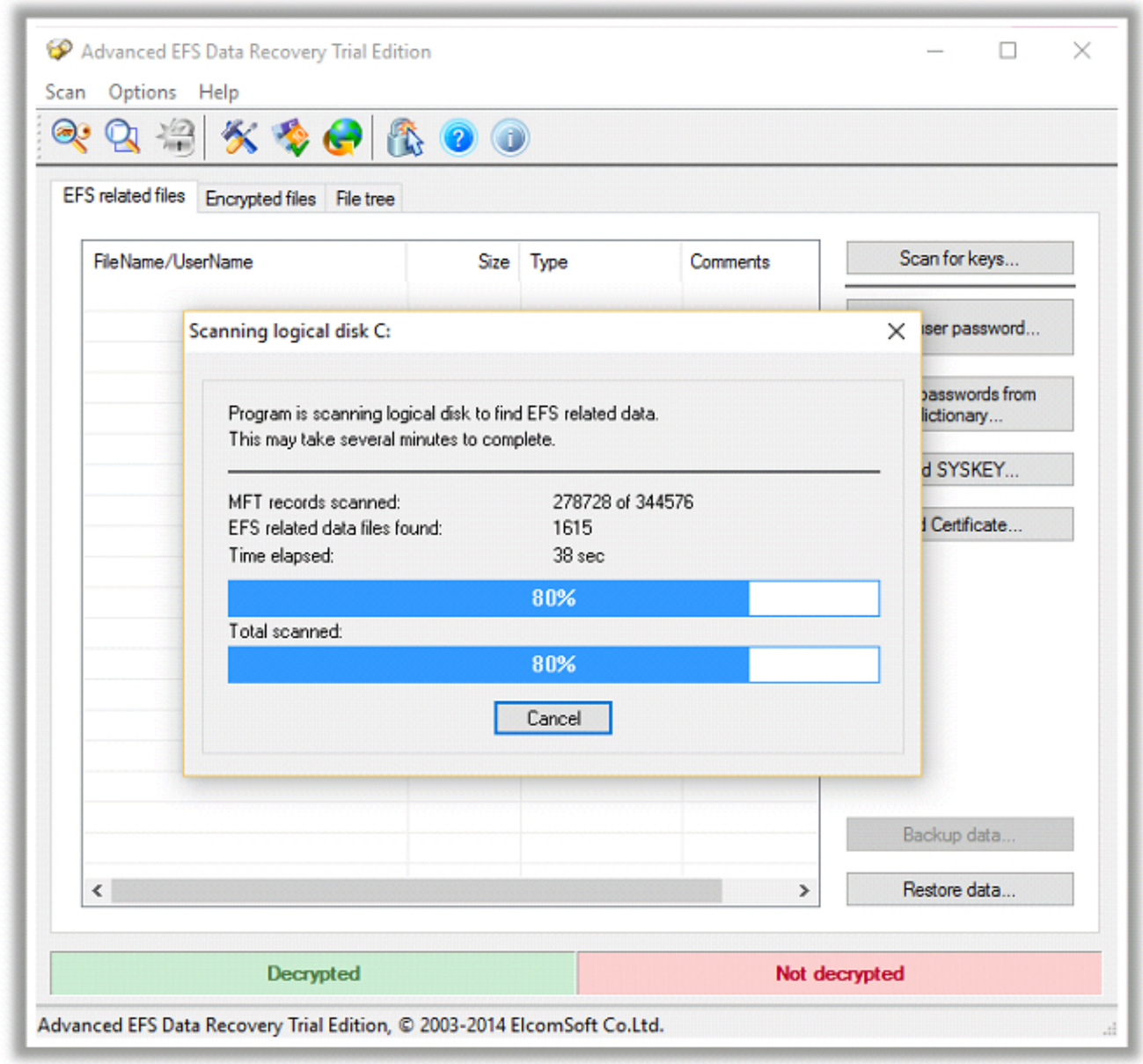
- Log on to the account used when the files were first encrypted
- Open a **Command Prompt** window, type **cipher /u**, and then press **Enter**

Note: If you do not choose to update encrypted files with the new recovery certificate right at that time, the files will automatically be updated the next time you open them

Advanced EFS Data Recovery Tool

Advanced EFS Data Recovery helps to **recover EFS-encrypted files** under various circumstances:

- EFS-protected disk inserted into a different PC
- Deleted users or user profiles
- User transferred into a different domain without EFS consideration
- Account password reset performed by system administrator without EFS consideration
- Damaged disk, corrupt file system, or unbootable operating system
- Reinstalled Windows or computer upgrades
- Formatted system partitions with encrypted files left on another disk



https://www.elcomsoft.com

Anti-Forensics Techniques: Encrypted Network Protocols

- Intruders deploy **cryptographic encapsulation protocols** such as SSL/TLS and SSH for anti-forensics purpose
- SSL/TLS and SSH protocols **encrypts the network traffic**, protecting only its content. However, protection against traffic analysis requires the use of intermediaries
- **Onion routing** combines both approaches with multiple layers of encryption, such that no intermediary knows both ends of the communication and the plaintext content

Anti-Forensics Techniques: Program Packers

1. Packer is a program used to **compress or encrypt the executable programs**
2. Intruders use packers to **hide attack tools** from being detected by reverse-engineering, or scanning
3. Some of the widely used packers: PECompact, BurnEye, **Exe Stealth Packer**, **Smart Packer Pro**, etc.
4. Packed programs that require a password to be run are considered to be strong. Whereas, the one's which do not require a password are **vulnerable to static analysis**

Anti-Forensics Techniques: Rootkits

- The use of Rootkits can be considered as another data hiding technique that intruders often use to mask their tracks and the presence of malicious applications or processes running on the system

- Rootkits are effective only in the course of a live analysis of the system under investigation

- **Types of rootkits:**
  - Hypervisor Level Rootkit
  - Hardware/Firmware Rootkit
  - Kernel Level Rootkit
  - Boot Loader Level Rootkit
  - Application Level Rootkit
  - Library Level Rootkits

- Some of the commonly used rootkits: Avatar, Necurs, Azazel, ZeroAccess, etc.

Detecting Rootkits

CHFI Computer Hacking Forensic Investigator

Integrity-Based Detection

It compares a snapshot of the **file system**, **boot records**, or **memory** with a known and trusted baseline

Signature-Based Detection

This technique compares characteristics of all **system processes** and **executable files** with a database of known rootkit fingerprints

Heuristic/Behavior-Based Detection

Any **deviations in the system's normal activity** or behavior may indicate the presence of a rootkit

Runtime Execution Path Profiling

This technique compares **runtime execution paths** of all system processes and executable files before and after the rootkit infection

Cross View-Based Detection

Enumerates key elements in the computer system such as **system files**, **processes**, and **registry keys**, and compares them to an **algorithm** used to generate a similar data set that does not rely on the common APIs. Any discrepancies between these two data sets indicate the presence of a rootkit

Steps for Detecting Rootkits

C|HFI Computer Hacking Forensic Investigator

1 Run "*dir /s /b /ah*" and "*dir /s /b /a-h*" inside the potentially infected OS and save the results

2 Boot into a clean CD, run "*dir /s /b /ah*" and "*dir /s /b /a-h*" on the same drive and save the results

3 Run a clean version of WinDiff on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from outside)

Note: There will be some false positives. Also, this does not detect stealth software that hides in BIOS, video card EEPROM, bad disk sectors, Alternate Data Streams, etc.

Anti-Forensics Techniques that Minimize Footprint

- **Memory Injection and Syscall Proxying**
  - In the buffer overflow exploit, an intruder injects and executes the code in the address space of a running program, thereby **altering the victim program's behavior**
  - Usually, buffer overflows are intended to access the remote system, after which attack tools are uploaded, which get saved in the **target machine's hard disk**
  - **Userland Execve Technique**:
    - Loads and runs programs on the victim's machine without using Unix execve() kernel call, thus defeating kernel-based security systems
    - Syscall proxying is a technique whereby the attacker uploads system call proxy, which receives remote procedure calls from the attacker's machine, executes them on the victim's machine, and sends back the results to the attacker
- **Advantage** – no need to upload attack tools on to the victim's machine
- **Disadvantage** – Increases network traffic between the attacker and victim machine leads to possible problematic latency

Anti-Forensics Techniques that Minimize Footprint (Cont'd)

Live CDs

- Portable OS distribution that boots and runs from a read-only device
- Live CDs may include GUI and tools for pen testing, forensics, anonymous browsing, etc.

Bootable USB Tokens

- Similar to a Live CD except that the OS distribution is contained within an USB device. These devices store more information than CDs, and allow data encryption
- Attacker can boot a copy of OS from a Live CD or bootable USB token on to a PC provided by the institution, use it to attack a series of computers, and then turn off the PC. This leaves no trace of an attack on the computer for later investigative analysis.

Virtual Machines

- Usually store all of the states associated with the client OS to files on the storage media of the host computer
- Attackers have to just securely delete the files associated with the virtual machine to erase all the evidence
- Also, most of the forensics investigation tools fail to detect rootkits running in a virtual environment

Anti-Forensics Techniques that Minimize Footprint (Cont'd)

- **Anonymous identities and storage**:

  Intruders create fake accounts via Gmail, Yahoo, Dropbox, etc. to protect their identity. Also, the storage capacity of accounts is now increased, which attackers utilize to **store attack tools** and **captured information**

- In doing so, there is a **reduction in the evidence** required for forensics investigation process

Anti-Forensics Techniques: Exploiting Forensics Tools Bugs

Having access to a CFT or knowledge on how it works, helps attackers to craft data that show bugs within the CFT. When properly triggered, these bugs can fulfill many anti-forensics goals

- **Failure to validate data**
  - CFTs that fail to validate their input data can possibly be subverted
  - An attacker can craft data to exploit buffer-overflow bugs in network monitoring tools such as tcpdump, Snort, and Ethereal
  - In specific, it is easy to exploit this vulnerability in a network forensics analysis tool as it is exposed to much of the traffic from an attacker
- **Denial of service attacks**
  - Any CFT resource (memory, CPU, etc.) whose use is determined by input data is subject to a possible DoS attack
  - Ex: Carefully crafted regular expressions can cause Windows log file analysis tools to hang
  - Others offensives include compression bombs that cause DoS attacks on CFTs and tools analyzing the content of container files
- **Fragile heuristics**
  - An attacker having knowledge about the heuristics that a CFT uses to identify files can exploit them
  - Ex: EnCase identifies a Windows file as executable if it has an .exe extension and the letters "MZ" as the first two characters
  - Tools such as Transmogrify converts a text file into an executable by changing the .txt extension to .exe and placing the letters "MZ" at the start of the file, which tricks EnCase into identifying it as binary, and not scanning it

Anti-Forensics Techniques: Detecting Forensic Tool Activities

Anti-forensics tools (AFTs) have the capability to change their behavior on **detecting the use of CFT**

Ex: A Worm may not propagate if it discovered that the network is under surveillance

Using Self-Monitoring, Analysis and Reporting Technology (SMART):

- **SMART built into hard drives report:**
  - Power cycle count
  - Power On time
  - Log of high temperatures the drive has reached
  - Other manufacturer-determined attributes
- These counters can be consistently read by user programs and cannot be reset
- AFTs read these SMART counters to identify forensics analysis attempts, and modify their behavior accordingly

  Ex: High Power On time might indicate that the hard drive has been imaged

Anti-Forensics Techniques: Detecting Forensic Tool Activities (Cont'd)

C|HFI Computer Hacking Forensic Investigator

Two primary techniques to detect network forensics:

- **Detecting hosts in "Promiscuous" mode**
  - Many network forensics tools use an Ethernet interface in promiscuous mode to capture all packets on the LAN
  - Often, these tools are not configured in such a way that they do not transmit on the network that is being examined
  - Thus, they can be detected by the way they respond to pings, ARPs, and malformed IP packets

- **DNS monitoring**
  - Attacker sends packets across a network with their destination as an Ethernet and IP address that is on the subnet but currently not in use. It has a source address from a rear network
  - Network monitoring tools on viewing such packets make a reverse DNS request in an attempt to resolve the hostname
  - By noticing that the DNS server is handling such requests, an attacker may conclude that packets are being monitored

Anti-Forensics Countermeasures

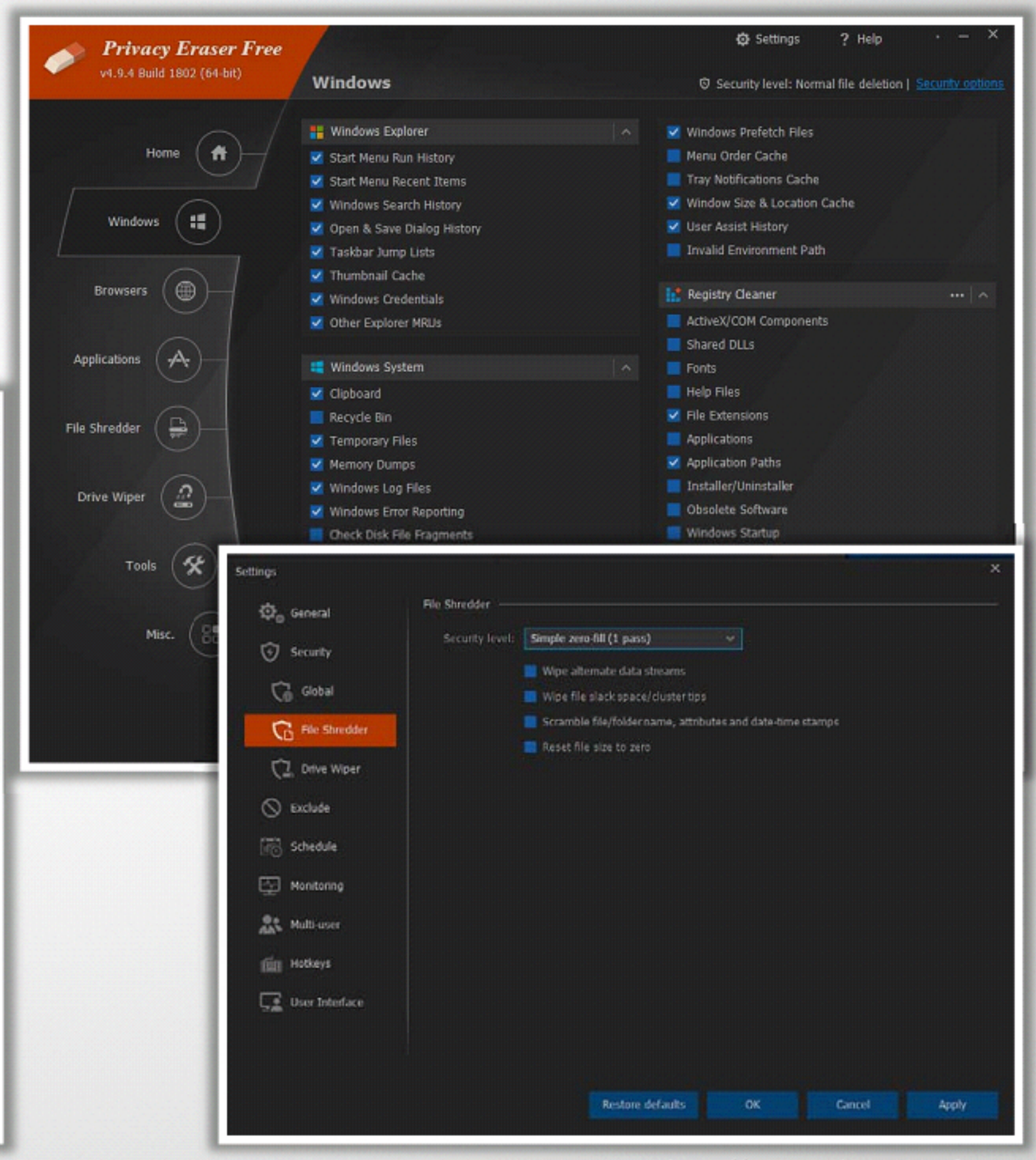
1. Train and educate the forensic investigators about anti-forensics
2. Validate the results of examination using multiple tools
3. Impose strict laws against illegal use of anti-forensics tools
4. Understand the anti-forensic techniques and their weaknesses
5. Use latest and updated CFTs, and testing them for vulnerabilities
6. Save data where the attacker can't get at it, such as log hosts, CD-ROMs, etc.
7. Use intelligent decompression libraries to defend against compression bombs
8. Replace weak file heuristics with stronger ones

Anti-Forensics Challenges

1. Anti-forensics is a new field and is unexplored
2. There is no proper framework or standards for anti-forensics
3. It is highly dependent on the computer forensics loopholes

Anti-Forensics Tools: Privacy Eraser

- **Privacy Eraser** protects your privacy by deleting browsing history and other computer activities
- It will erase all digital footprints - browser cache, cookies, browsing history, address bar history, typed URLs, saved passwords, Windows' run history, search history, recent documents, temporary files, recycle bin, clipboard, DNS cache, log files, etc.



http://www.cybertronsoft.com

Anti-Forensics Tools: Azazel Rootkit

Azazel is a userland **rootkit written in C** based off of the original LD_PRELOAD technique from Jynx rootkit

FEATURES

- Anti-debugging
- Avoids unhide, lsof, ps, and ldd detection
- Hides files, directories, and remote connections
- Hides processes and logins
- PCAP hooks avoid local sniffing
- PAM backdoor for local and remote entry
- Log cleanup for utmp/wtmp entries
- Uses xor to obfuscate static strings

Terminal

```
localhost:~ $ git clone https://github.com/chokepoint/azazel.git
```

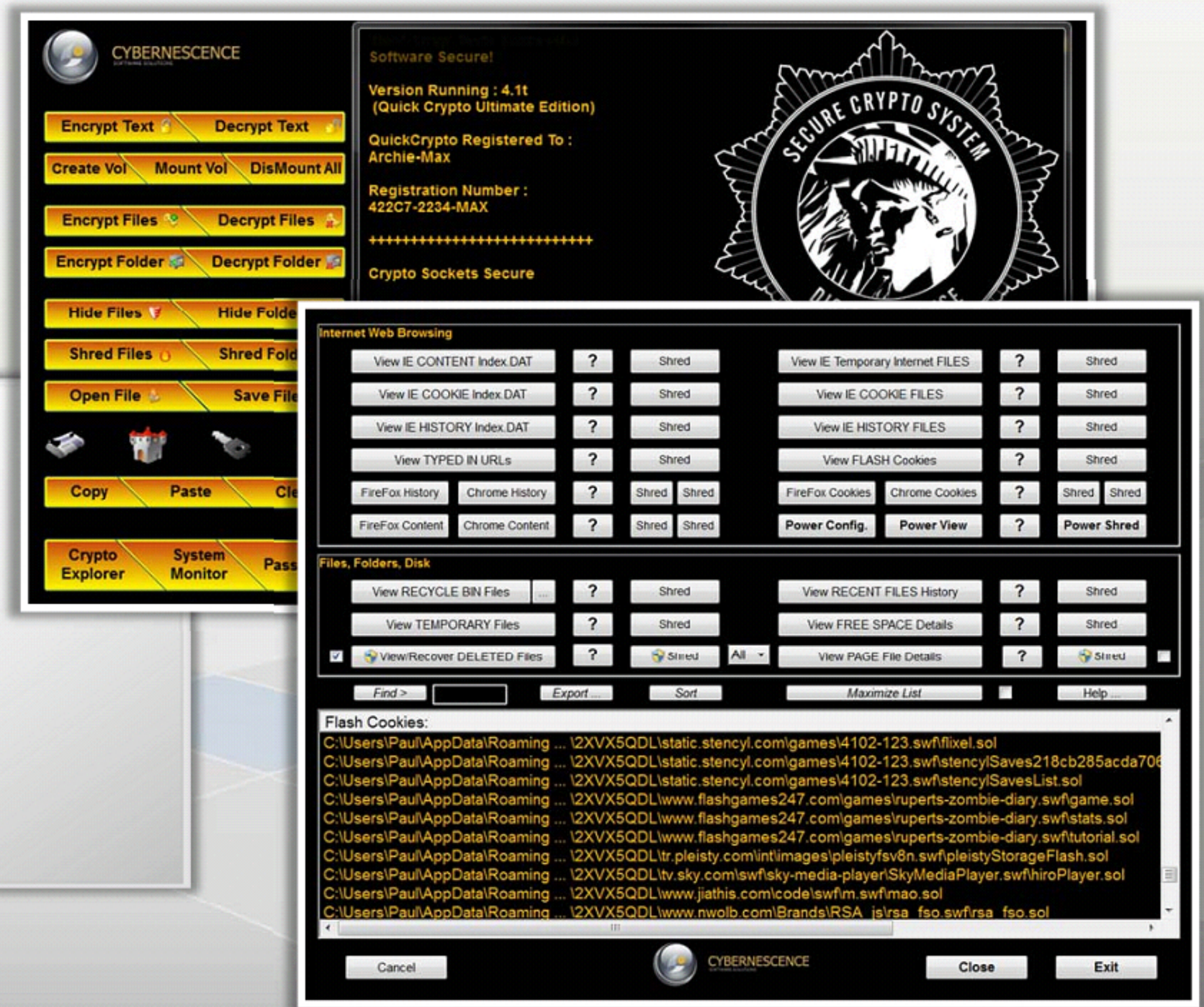
Terminal

```
localhost:~ $ make
```

Terminal

```
localhost:~ $ LD_PRELOAD=/lib/libselinux.so bash -l
```

Anti-Forensics Tools: QuickCrypto



- QuickCrypto allows text files, image files, audio files, etc. to be **hidden** and **encrypted** prior to hiding

http://quickcrypto.com

Anti-Forensics Tools

Steganography Studio
http://stegstudio.sourceforge.net

OmniHide PRO
http://omnihide.com

CryptaPix
http://www.briggsoft.com

Masker
http://www.softpuls.com

GiliSoft File Lock Pro
http://gilisoft.com

DeepSound
http://jpinsoft.net

wbStego
http://wbstego.wbailer.com

DBAN
http://www.dban.org

Data Stash
http://www.skyjuicesoftware.com

Universal Shield
http://www.everstrike.com

Anti-Forensics Tools (Cont'd)

Ontrack Eraser Degausser
http://www.krollontrack.co.uk

BatchPurifier
http://www.digitalconfidence.com

Steganos Privacy Suite 17
https://www.steganos.com

Webroot's Internet Security Complete
http://www.webroot.com

Blancco Flash
http://www.blancco.com

Blancco 5
http://www.blancco.com

Secure IT
http://www.cypherix.com

ParetoLogic Privacy Controls
http://www.paretologic.com

Exiv2
http://www.exiv2.org

Invisible Secrets 4
http://www.invisiblesecrets.com

Module Summary

- Intruders implement anti-forensics techniques to hinder or prevent proper forensics investigation process
- Anti-forensics techniques include file deletion, password protection, steganography, trail obfuscation, artifact wiping, overwriting data/metadata, encryption, program packers, rootkits, exploiting forensics tool bugs, etc.
- Intruders may use anti-forensics tools such as Privacy Eraser, QuickStego, CryptaPix, etc. to hide their malicious activities from being caught
- Strictly implementing countermeasures against anti-forensics may enable an investigator to successfully deal with a case