

Defeating Anti-forensics Techniques

Module 05






Computer Hacking Forensic Investigator v9

Module 05: Defeating Anti-forensics Techniques

Exam 312-49

Module Objectives




→ 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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


Cybercriminals leave fingerprints that investigators can collect, correlate, and analyze to understand the process of crime and the motive behind it and attempt to identify the person(s) who committed it. To hinder these efforts, criminals develop and promote counter techniques and methodologies, called Anti-Forensics. These methods obstruct the process of acquiring evidence, analysis, or its credibility and sometimes leave the evidence in a manner not admissible in a court of law. Therefore, the investigators should have an understanding of these techniques, their functions, and their impact on the evidence sources. This module will discuss anti-forensic techniques and methods to overcome them.

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



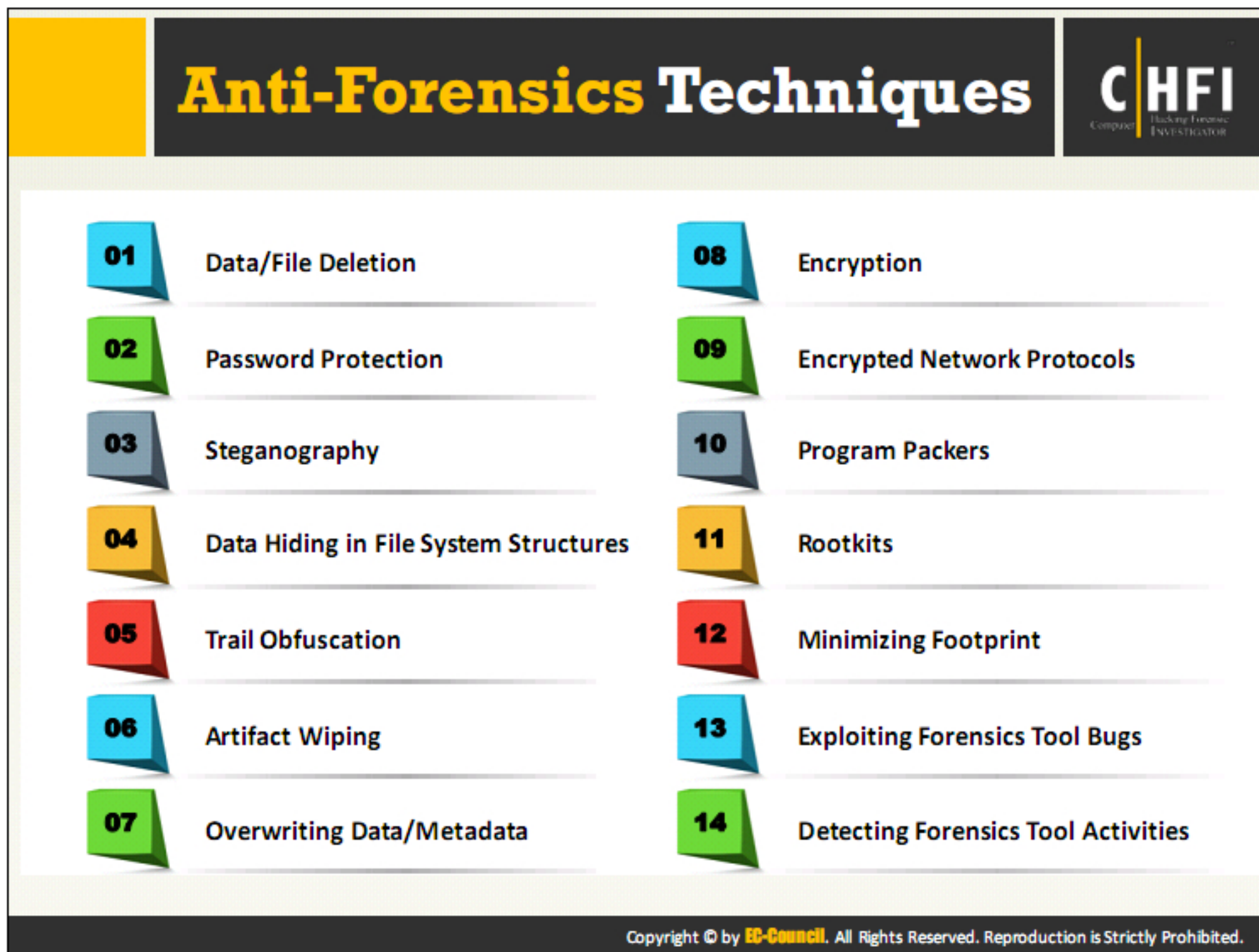
- To interrupt and prevent information collection
- To make difficult the investigator's task of finding evidence
- To hide traces of crime or illegal activity
- To compromise the accuracy of a forensics report or testimony
- Forcing the forensics tool to reveal its presence
- To use the forensics tool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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-forensics, also known as counter forensics, is a set of techniques that attackers or perpetrators use in order to avert or sidetrack the forensic investigation process or try to make it much harder. These techniques negatively impact the quantity and quality of evidence from a crime scene, thereby making the forensic investigation process difficult. Therefore, the investigator might have to conduct a few more additional steps in order to fetch the data, thereby causing delay in the investigation process.

Goals of Anti-Forensics:


- Interrupt and prevent information collection.
- Toughen the investigator's task in finding the evidence.
- Hide traces of crime or illegal activity.
- Compromise the accuracy of a forensic report or testimony.
- Force the forensic tool to reveal its presence.
- Use a forensic tool itself for attack purposes.
- Delete evidence that an anti-forensic tool has been used.




Anti-forensic techniques are the actions and methods that hinder the forensic investigation process in order to protect the attackers and perpetrators from prosecution in a court of law. These techniques act against the investigation process such as detection, collection, and analysis of evidence files and sidetrack the forensic investigators. These techniques impact the quality and quantity of the evidence of a crime scene, thereby making the analysis and investigation difficult.



Anti-forensic techniques, which include deletion and overwriting processes, also help to ensure the confidentiality of data by reducing the ability to read it. Attackers use these techniques in order to defend themselves against revelation of their actions during criminal activities. Deceitful employees may use anti-forensic tools for the destruction of data that may cause huge losses to the organization.


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




Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Intruders will be more concerned about covering the tracks of their illegal activities across a network or system and try to delete the data contained in the hard disk as part of their effort to avert detection. They also try to delete footprints of the files using specialized tools. The process includes elimination of source files, logs, and traces of data from places on the hard drive, and entries on the hard disk drive (HDD), which include attributes, orphan files, and dynamic-link library DLL files. Intruders can also securely delete data or overwrite it to mask the original data.

However, investigators can probably recover the deleted files by using various data recovery tools depending on the operating system (OS) the computer is running.

What Happens When a File is Deleted in Windows?



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.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

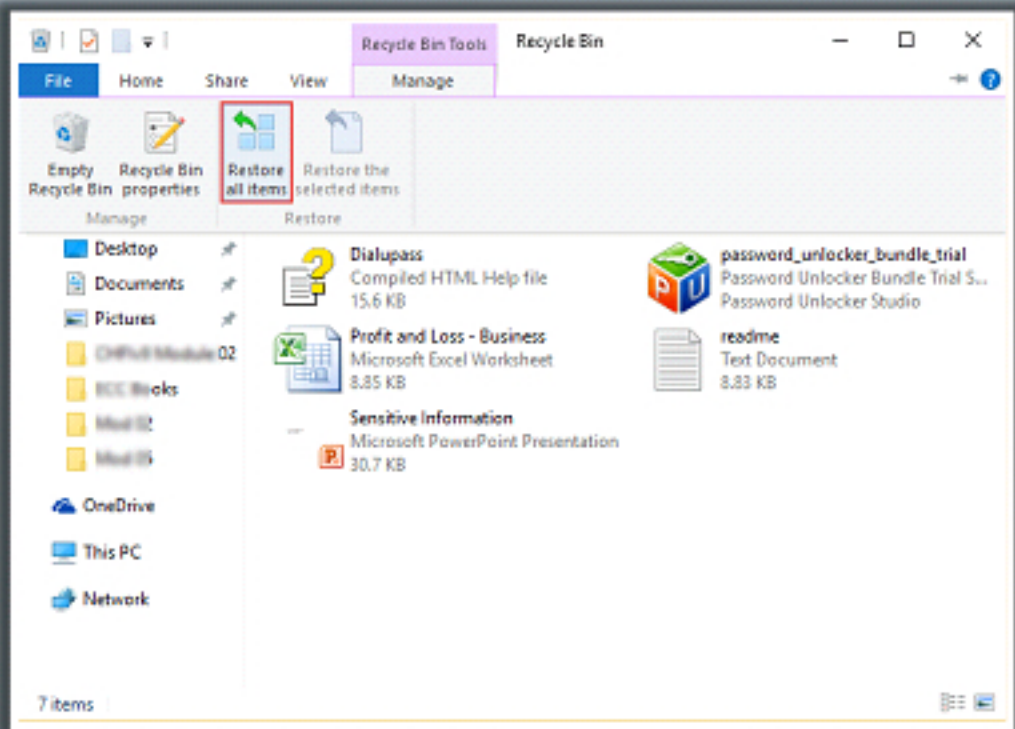
When a user deletes a file, the OS does not actually delete the file, but marks the file name in the Master File Table (MFT) with a special character. This character represents that the space once occupied by the file is ready for use.

In the 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 the deleted file. The FAT file system marks the corresponding clusters of that file as unused, though it is not empty. The Windows New Technology File (NTFS) uses different approach and marks the index field in the MFT with a special code. The computer now looks at the clusters occupied by that file as being empty. Therefore, the space is available to store a new file. Users can recover the deleted file if the system has not overwritten the space.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The Recycle Bin is a location on the Windows desktop that temporarily stores deleted files. When a user deletes an item from the hard disk, Windows sends that deleted item to the Recycle Bin, and the icon changes to full from empty. The Recycle Bin does not store items deleted from removable media, such as a floppy disk or network drive.

The items present in the Recycle Bin still consume the space in the hard disk and are easy to restore. Users can restore the deleted files to their original position with the help of the Restore option of the Recycle Bin. Even after the users delete these files from the Recycle Bin, these items still take up space in the hard disk until the OS overwrites that location.

When the Recycle Bin becomes full, Windows automatically deletes the older items. The Windows OS assigns one specific space on each hard disk partition for the Recycle Bin. The system does not store larger items in the Recycle Bin but deletes them permanently.

Following are the steps to change the storage capacity of the Recycle Bin:

1. On the desktop, right-click over the **Recycle Bin** and select **Properties**.
2. Click the location of the Recycle Bin you want to change under the Recycle Bin location (likely C drive).
3. Click **Custom size** and then enter a maximum storage size (in MB) for the Recycle Bin in the Maximum size (MB) box.
4. Click **OK**.

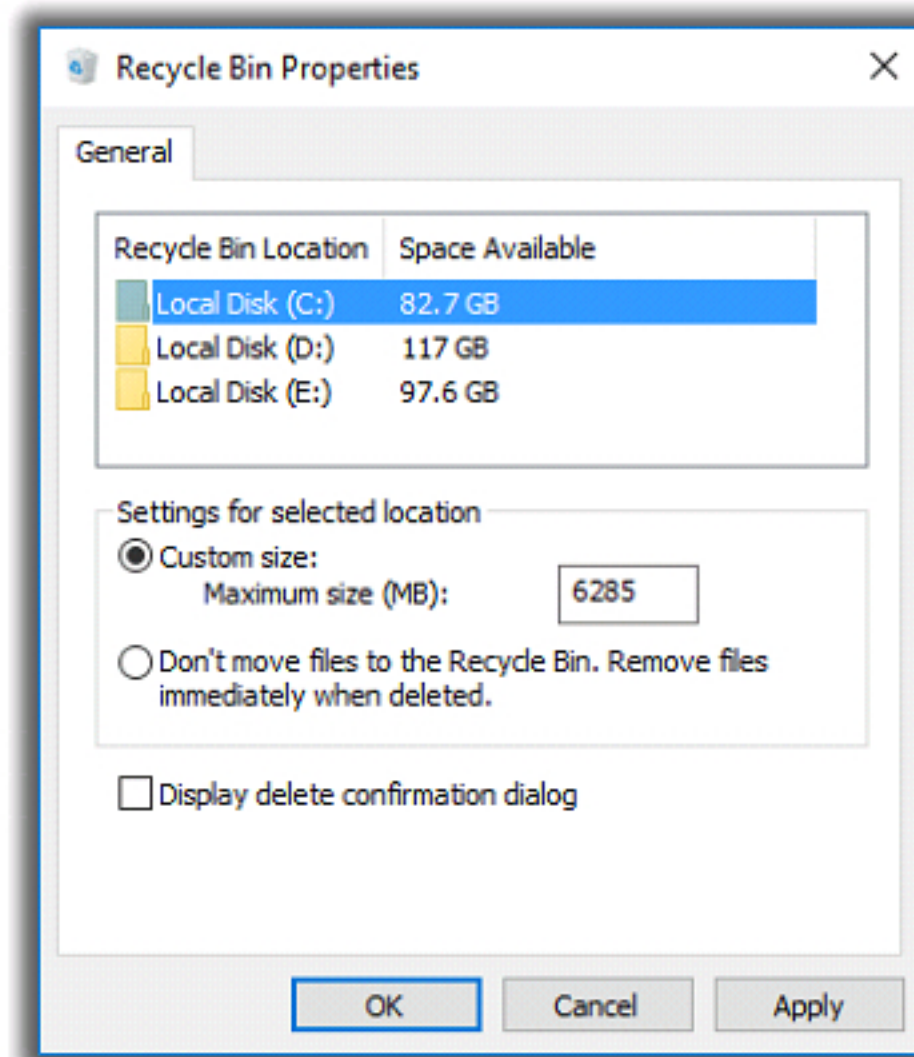



FIGURE 5.1: Configuring Recycle Bin Properties


Following are the steps to delete or restore files in the Recycle Bin:

Open Recycle Bin to perform the deletion or restoration operations.


1. To restore a file, right-click on the file icon and select **Restore**.
2. To restore all files, select All, go to **Manage** and click **Restore the selected items**.
3. To delete a file, right-click on the file icon and select **Delete**.
4. To delete all files, there are two methods:
 - Select All, right-click and select **Delete** option.
 - Go to **Manage** option in the tool bar and click **Empty** the Recycle Bin.
 - Both methods have a pop-up window to confirm whether to permanently delete the items. Click **Yes**.

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

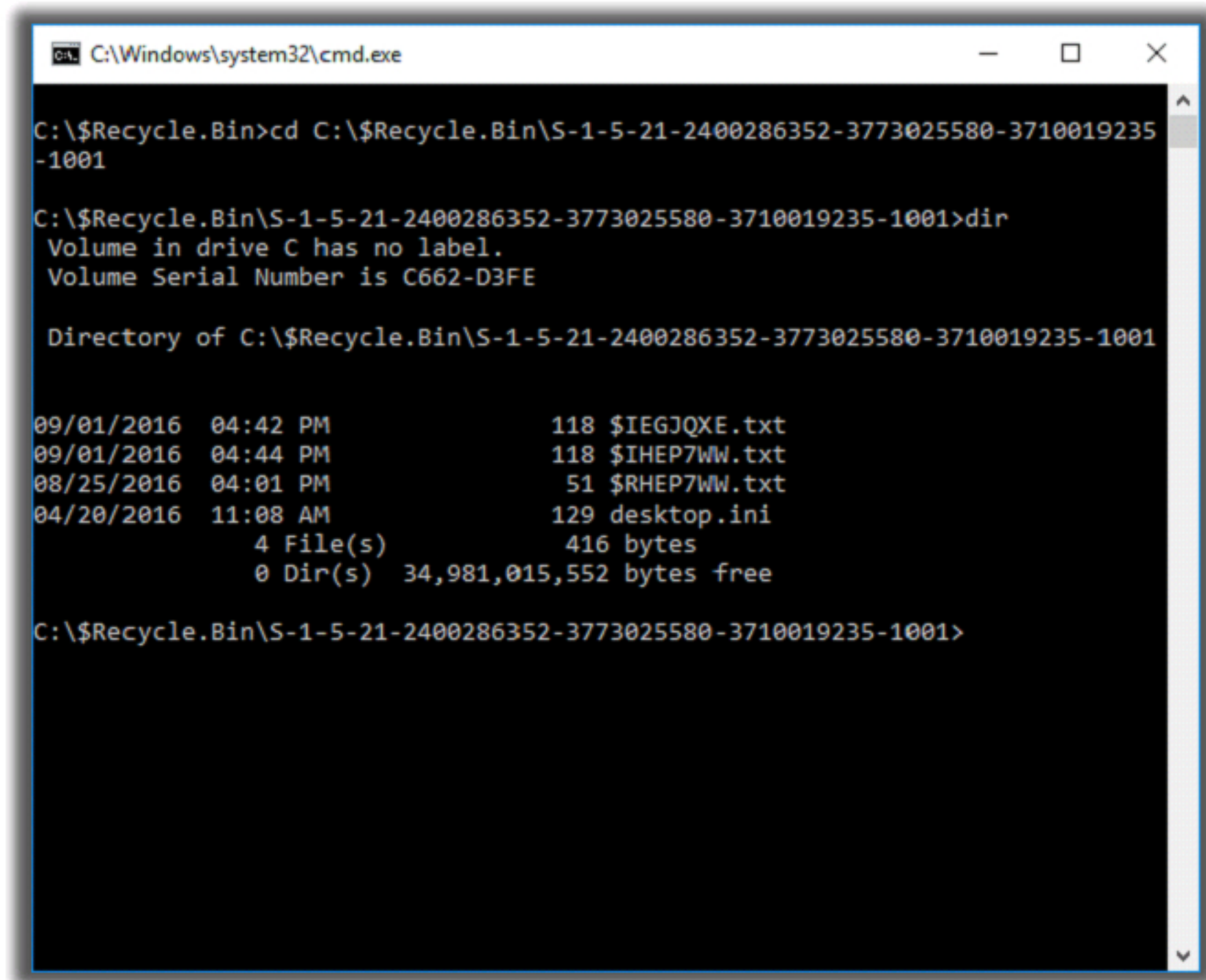
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Each drive contains a folder to store deleted files; deleted items are stored in Drive:\\$Recycle.Bin folder in Windows Vista and later versions of Windows.

The older FAT file system, used across Windows 98 and earlier versions, stored the deleted files in Drive:\RECYCLED folder, whereas the Windows 2000, XP, and NT, which deploy NTFS file system, store these files in Drive:\RECYCLER folder.

The Windows OS using a FAT file system dumps all the recycled files into a single C:\RECYCLED directory, whereas an NTFS-based file system categorizes these into directories named as C:\RECYCLER\S-.... in Windows prior to 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 the older versions had a maximum limit of 3.99 GB. Recycle Bin cannot store items larger than its storage capacity.



A screenshot of a Windows command prompt window titled "C:\Windows\system32\cmd.exe". The prompt shows the user navigating to a directory in the Recycle Bin and listing its contents. The output shows a directory listing with file names, sizes, and dates.

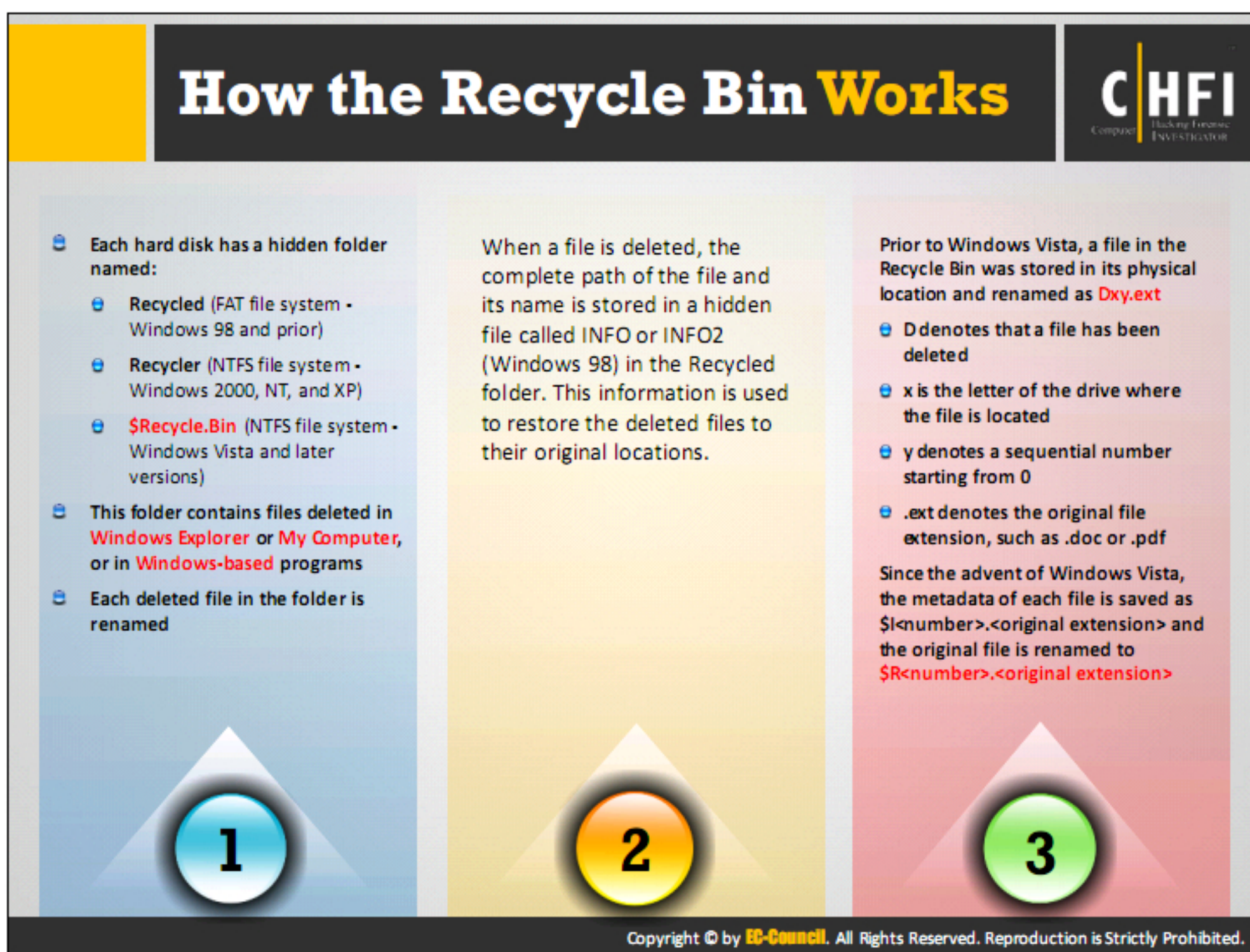
```
C:\$Recycle.Bin>cd C:\$Recycle.Bin\S-1-5-21-2400286352-3773025580-3710019235-1001
C:\$Recycle.Bin\S-1-5-21-2400286352-3773025580-3710019235-1001>dir
Volume in drive C has no label.
Volume Serial Number is C662-D3FE

Directory of C:\$Recycle.Bin\S-1-5-21-2400286352-3773025580-3710019235-1001

09/01/2016  04:42 PM                118 $IEGJQXE.txt
09/01/2016  04:44 PM                118 $IHEP7WW.txt
08/25/2016  04:01 PM                 51 $RHEP7WW.txt
04/20/2016  11:08 AM                129 desktop.ini
               4 File(s)              416 bytes
               0 Dir(s) 34,981,015,552 bytes free

C:\$Recycle.Bin\S-1-5-21-2400286352-3773025580-3710019235-1001>
```


FIGURE 5.2: Listing Directory Contents



The Windows Vista and later versions renames the files stored in the Recycle Bin as \$Ry.ext, whereas in older versions of Windows, it used be Dxy.ext. In this naming process, “x” represents the drive name, “y” a sequential number starting from 0, and “.ext” being the original file’s extension such as .doc, .docx, .pdf, etc.

When a user deletes a file or folder, the OS stores all the details of the file such as its complete path, including the original file name, in a special hidden file called “Info” or “Info2” in the Recycle Bin folder. The OS uses this information to restore the deleted file to its original location. The Recycled hidden folder contains files deleted from My Computer, Windows Explorer, and some Windows applications.

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

In the earlier versions of Windows, the system renamed the deleted file using the syntax:

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

For example, in the case of the Dxy.ext file in the Recycled folder, “x” denotes the name of drive such as “C,” “D,” and others; “y” denotes the sequential number starting from one; and .ext is the extension of the original file.

Consider the following example:

New file name:

`Dc1.txt` = (C drive, second file deleted, a .txt file)

INFO file path:

`C:\Windows\Desktop\Books.txt`

New file name:

`De7.doc` = (E drive, eighth file deleted, a .doc file)

INFO file path:

`E:\Winword\Letter to Rosemary.doc`

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

`$R<#>.<original extension>`

Example:


New file name:

`$R7.doc=(eighth file deleted, a doc file)`

INFO file path(`$I<#>.<original extension>`): `$I7.doc`

In Windows versions newer than Vista and XP, the OS stores the complete path and file or folder name in a hidden file called INFO2. This file remains inside the Recycled or Recycler folder and stores information about the deleted file. It is a master database file and very crucial for the recovery of data. INFO2 contains various details of deleted files such as: original file name, original file size, the date and time of deletion, unique identifying number, and the drive number that the file came from.

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`

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

When a user damages, corrupts, or removes the INFO2 file, the Recycle Bin loses the data. In such case, the investigators can recover or restore the lost data using data recovery software.


The damage or deletion of the file will delete it completely from the Recycle Bin, but the deleted and renamed files will still be present in the Recycled folder. As the user had renamed these files in the Recycled folder, they can search for such files and restore them manually. To restore such a file, manually search for that particular file and rename it. Click **Start → Find → Files or Folders** to find a file and then rename it.

If the Recycle Bin is not working or damaged, then delete the hidden INFO file from the Recycled folder and restart Windows to re-create the INFO file; this will enable you to access the deleted files in the Recycle Bin.

Following are the steps to delete the INFO file:

- 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 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 }

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Damaged files in the Recycle Bin folder (**C:\RECYCLER**, **C:\RECYCLER\S-** or **C:\\$Recycle.Bin\S-**) do not appear in the Recycle Bin. In such cases, follow the steps below to restore or recover the deleted files:


- Create a copy of the Desktop.ini file in the Recycle Bin folder and save it in another folder, and then delete the entire contents of the Recycle Bin folder.
- Delete all files in the Recycle Bin.
- Restore the Desktop.ini file to the Recycled folder.
- If there is no Desktop.ini file or if it is damaged, then re-create it by adding the information to blank Desktop.ini file:

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

Create the blank Desktop.ini file by following the procedure below:

- Right-click any empty space on the Windows desktop.
- Select New → Text Document.
- Name it as Desktop.ini (if you get a change of file extension warning, simply ignore it).
- Copy all the information given above into the newly created file.
- Save it and move it to the Recycled folder.

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:**
 - ➊ Open a command prompt with administrative privileges
 - ➋ Type `attrib -s -h recycler` (the Recycle Bin folder)
 - ➌ Type `del recycler`
 - ➍ Restart the computer
 - In Windows, Vista and later:**
 - ➊ Open a command prompt with administrative privileges
 - ➋ Run `rd /s /q C:\$Recycle.bin` command
 - ➌ Restart the computer

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

At times, the attacker could have tampered or damaged the Recycled Bin folder. In this case, users can delete the file and send them to the Recycled folder, even though the Recycle Bin on the desktop appears full. But, they will not be able to view the contents of the Recycle Bin or empty Recycle Bin as the damage will disable the Empty Recycle Bin command.


To overcome this, delete the Recycled folder and restart Windows; it will regenerate the folder and restore its functionality. Even if the user tries to reset or repair the Recycle Bin folder, Windows will delete the complete folder and creates a new one.

In the current Windows 10 OS, follow the steps below to repair a damaged or corrupted recycle bin folder:

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

Use this command to repair the \$Recycle.bin folder on the C drive. Perform the same operation to repair the Recycle Bin of every partition on the hard disk separately, by replacing C with the respective drive letter. Users and investigators should be very cautious while using the command, as any discrepancy can delete the wrong files or directory.

File Recovery Tools: Windows



Recover My Files

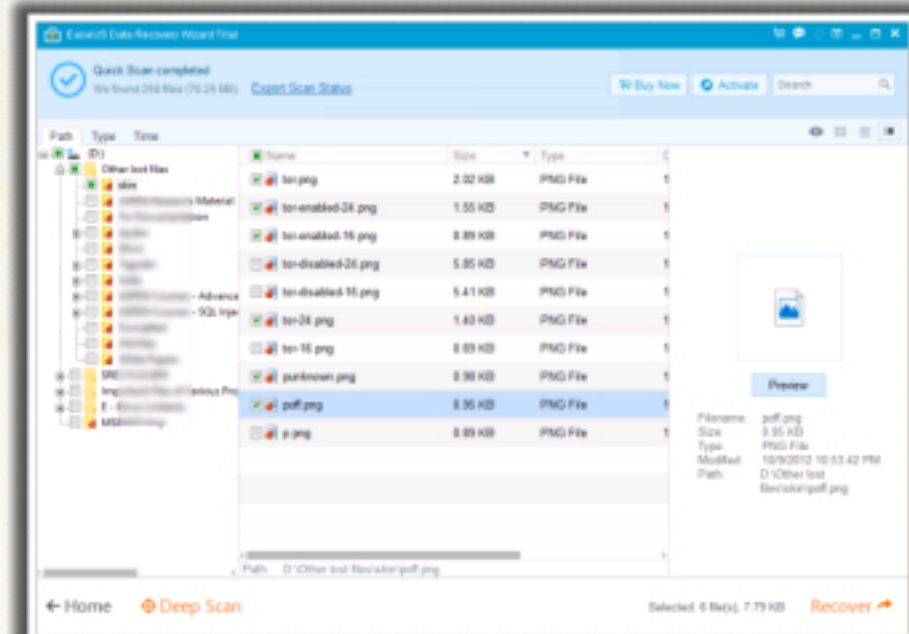
- Recover deleted files emptied from the **Windows Recycle Bin**, files lost due to the format or reinstall of a hard drive, or files removed by a virus, Trojan infection, unexpected system shutdown or software failure

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.recovermyfiles.com>



<http://www.easeus.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recover My Files

Source: <http://www.recovermyfiles.com>

Recover My Files data recovery software recovers deleted files emptied from the Windows Recycle Bin and files lost due to the format or corruption of a hard drive, virus or Trojan infection, and unexpected system shutdown or software failure.

Features:

- Recovers files even if emptied from the Recycle Bin data
- Recovers files after accidental format, even after Windows is reinstalled
- Performs disk recovery after a hard disk crash
- Recovers files after a partitioning error
- Recovers data from RAW hard drives
- Recovers documents, photos, videos, music, and email
- Recovers from a hard drive, camera card, USB, Zip, floppy disk, or other media

EaseUS Data Recovery Wizard


Source: <http://www.recovermyfiles.com>











EaseUS Data Recovery Wizard software is used to do format recovery and unformat and recover deleted files emptied from the Recycle Bin or data lost due to partition loss or damage, software crash, virus infection, unexpected shutdown, or any other unknown reasons under Windows 10, 8, 7, 2000/XP/Vista/2003/2008 R2 SP1/Windows 7 SP1. This software supports hardware RAID and hard drive, USB drive, SD card, memory card, etc. It provides the comprehensive data recovery solution for computer users to recover lost data.

Features:

- Specifies file types before file recovery to find lost files quickly
- Saves previous searching results for continuous recovery
- Scans lost files faster by skipping bad sectors automatically
- Supports English and German languages

File Recovery Tools: Windows (Cont'd)



 DiskDigger http://diskdigger.org	 Advanced Disk Recovery http://www.systweak.com
 Handy Recovery http://www.handyrecovery.com	 Windows Data Recovery Software http://www.diskdoctors.net
 Quick Recovery http://www.recoveryourdata.com	 R-Studio http://www.data-recovery-software.net
 Stellar Phoenix Windows Data Recovery http://www.stellarinfo.com	 Orion File Recovery Software http://www.nchsoftware.com
 Total Recall http://www.totalrecall.com	 Data Rescue PC http://www.prosofteng.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

DiskDigger

Source: <http://diskdigger.org>

DiskDigger is a program that undeletes and recovers lost files from hard drives, memory cards, and USB flash drives. This tool can be used to recover documents or photos accidentally deleted from the computer or from a reformatted camera memory card, or can be used to check the files that are on an old USB drive.

Features:

- It works in Windows 10, 8, 7, Vista, and XP OSs
- Shows recoverable files as a list or as thumbnail previews
- Thumbnails will show previews of image files, album art from MP3 and WMA files, and icons from executable files
- Selecting a recoverable file brings up a full preview of the file (insofar as possible). For image files, it will show the image (with pan and zoom). For document files, it will show a text-only preview of the document. For certain audio files, it will allow you to play back the sound
- Previews of JPG and TIFF files will show EXIF information (camera model, date taken, sensor settings, etc.)
- Previews of MP3 files will show ID3 information (artist, album, genre, etc.).
- Previews of ZIP files will show a list of files contained in the archive.

Handy Recovery

Source: <http://www.handyrecovery.com>

Handy Recovery is data recovery software designed to restore files accidentally deleted from hard disks and memory cards. The program can recover files damaged by virus attacks, power failures, and software faults, or files from deleted and formatted partitions. If a program does not use the Recycle Bin when deleting files, Handy Recovery can restore such files. It can also recover files moved from the Recycle Bin after it has been emptied.

It can also restore the full branch of a folder tree containing selected files and folders. Along with the main file data, the program can recover alternate data streams, which are used on the NTFS file system to store additional information about files.

Quick Recovery

Source: <http://www.recoveryourdata.com>

Quick Recovery software recovers files that have been lost, deleted, corrupted, or even deteriorated. The application searches, scans, and recovers files that are encrypted and password protected and restores them.

Features:

- Repairs and recovers Disk bad sectors
- Recovers virus-prone files, hidden, and password protected files
- Affirmative graphical user interface (GUI) feature with backup at user defined location
- Recovers and restores encrypted and system files viz. compiler

Stellar Phoenix Windows Data Recovery

Source: <http://www.stellarinfo.com>

Stellar Phoenix Windows Data Recovery recovers lost, deleted, or inaccessible data from Windows OS HDDs and other storage media.

The tool helps to recover data lost due to hard drive corruption, formatting, and virus attack.

Total Recall

Source: <http://www.totalrecall.com>

Total Recall Data Recovery Software recovers lost data from hard drives, RAID, photos, deleted files, iPods, and even removable disks connected via FireWire or USB.

Advanced Disk Recovery

Source: <http://www.systweak.com>

Advanced Disk Recovery software scans the entire system for deleted files and folders and recovers them. It scans the hard drives, partitions, external devices, and even CDs and DVDs for recoverable files. It provides two types of scans: the Quick Scan that uses MFT and the Deep

Scan that uses file signatures. Once the scan is complete, one can either preview the files/folders or recover them to a preferred location.

Windows Data Recovery Software

Source: <http://www.diskdoctors.net>

Disk Doctors Windows Data Recovery software can recover accidentally deleted files, including files emptied from the Recycle Bin and from Windows Explorer with Shift + Delete.

With Disk Doctors Windows Recovery software, it is possible to recover data from a reformatted partition (to any file system), and a corrupted, deleted, or missing partition. It locates deleted and lost partitions with the help of two scanning methods: Quick Scan and Thorough Scan. These scanning methods locate and validate lost partitions from the entire physical hard drive.

R-Studio

Source: <http://www.data-recovery-software.net>

R-Studio is data recovery software. It can recover files from FAT12/16/32/exFAT, NTFS, NTFS5 (created or updated by Windows 10, 8, 7, 2000/XP/2003/Vista). It functions on local and network disks, formatted, damaged, or deleted partitions.

Features:

- An advanced RAID reconstruction module
- A feature-rich text/hexadecimal editor
- An entire advanced disk copying/imaging module in one single piece of software, which makes R-Studio the ideal complete solution for creating a data recovery workstation

Orion File Recovery Software

Source: <http://www.nchsoftware.com>

Orion File Recovery Software searches for deleted files on the hard drive, or any external or portable drive connected to the computer. Files that are not overwritten can either be recovered or permanently deleted to prevent future recovery.

Features:

- Recovers deleted files, music, or photos
- Searches your hard drive, external drive, or flash drive
- Permanently erase files to increase security

Data Rescue PC


Source: <http://www.prosofteng.com>











Data Rescue PC recovers files from a crashed or virus-corrupted hard drive. Data Rescue PC recovers an external drive or secondary drive. It scans the drive for the files and copies them to the second drive.

Features:

- Recovers all types of files from the hard drive
- Works if the drive fails to mount or only partially operates
- Recovers deleted, lost, and damaged files
- Recovers digital pictures from the camera media even after it has been erased or reformatted
- Recovers the whole drive or just the files you need
- Recovers pictures, movies, and music from PC drives and any type of digital camera media

File Recovery Tools: Windows (Cont'd)



 Smart Undeleter http://www.recoverdeletedfilestool.com	 File Scavenger http://www.quetek.com
 DDR Professional Recovery Software http://www.recoverybull.com	 VirtualLab http://www.binarybiz.com
 Data Recovery Pro http://www.paretalogic.com	 Active@ UNDELETE http://www.active-undelete.com
 GetDataBack http://www.runtime.org	 WinUndelete http://www.winundelete.com
 UndeletePlus http://undeleteplus.com	 R-Undelete http://www.r-undelete.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Smart Undeleter

Source: <http://www.recoverdeletedfilestool.com>

Smart Undeleter recovers deleted files, even those that were deleted before the installation of the utility. It can run from a floppy disk without installation on the hard disk. This feature eliminates the risk of deleted files being overwritten and damaged beyond retrieval before you can restore them. Smart Undeleter is a multitasking intelligent utility that supports data loss recovery from FAT and NTFS file systems. It quickly retrieves lost files and also gives useful information, including a list of files, after scanning the system.

DDR Professional Recovery Software

Source: <http://www.recoverybull.com>

DDR Professional Windows Recovery Software recovers deleted files in all major data loss situations, whether lost from fixed hard drive partitions or from any USB storage media drive. The advanced data retrieval tool recovers files deleted from memory cards, digital cameras, USB drives, external HDDs, and music players, and it even recovers deleted hard drive partition files in a few mouse clicks.

Data Recovery Pro

Source: <http://www.paretologic.com>

Data Recovery Pro restores deleted emails and email attachments, so no important messages are ever lost. Data Recovery Pro will also deeply scan your hard drive, external drives, iPod Shuffle, iPod Nano, and iPod Classic to recover a wide variety of files.

GetDataBack

Source: <http://www.runtime.org>

GetDataBack recovers data if the hard drive's partition table, boot record, FAT/MFT, or root directory are lost or damaged; data was lost due to a virus attack; the drive was formatted; fdisk has been run; a power failure has caused a system crash; files were lost due to a software failure; or files were accidentally deleted. It can even recover your data when the drive is no longer recognized by Windows. This tool can likewise be used even if all directory information—not just the root directory—is missing.

UndeletePlus

Source: <http://undeleteplus.com>

UndeletePlus scans a computer or storage medium for deleted files and restores them on command. It works with computers, flash drives, cameras, and other forms of data storage. It scans the device, selects the files needed to recover, and restores the information or picture with the click of a button.

File Scavenger

Source: <http://www.quetek.com>

File Scavenger is a file “undelete” and data recovery utility for Windows 10, 8, 7, Vista, Server 2003, 2000, NT, and ME/98/95. File Scavenger recovers files that have been accidentally deleted (including files removed from the Recycle Bin, in a DOS window, from a network drive, and from Windows Explorer with the SHIFT key held down) provided that recovery is attempted before the files are permanently overwritten by new data. File Scavenger supports basic and dynamic disks, NTFS compression, alternate data streams, sparse files, Unicode filenames, etc. Except in severe cases, both the file and the folder path leading to the file can be recovered.

VirtualLab

Source: <http://www.binarybiz.com>

VirtualLab is a data recovery software that works with all Windows OSs from Windows 98 to Windows 10, 8, 7, FAT 12/16/32, and NTFS file systems. It can restore the deleted files from lost/damaged partitions, formatted disks, deleted emails, hard drives and RAID systems, and photos and flash memory cards

Active@ UNDELETE

Source: <http://www.active-undelete.com>

Active@ UNDELETE is data recovery software that helps to recover deleted files and restore deleted partitions. It restores the deleted volumes/partitions in-place, fixing volume boot sectors and ability to rollback partition changes. It supports Windows 10/8/7/Vista/XP, 2003/2008 Server OSs.

WinUndelete

Source: <http://www.winundelete.com>


WinUndelete software can be used to recover deleted files from a hard drive, flash drive, USB external drive, digital camera card, and more. WinUndelete recovers deleted files after emptying the Recycle Bin or by using other deletion actions that bypass the Recycle Bin.











R-Undelete

Source: <http://www.r-undelete.com>

R-Undelete tool recovers files from FAT and NTFS file systems. R-Undelete recover files on any local disk recognized by the software. An additional file recovery algorithm increases the file recovery quality. R-Undelete can be run from disk and folder context menus. Graphics files, videos, and audio files can be previewed in R-Undelete.

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recover4all Professional

Source: <http://www.recover4all.com>

Recover4all software recovers (undeletes) files that were accidentally deleted under Windows. It recovers the files that were accidentally deleted from the Recycle Bin, or if the drive was formatted, or if the file system was damaged. Recover4all does not require installation and can run directly from a USB disk, flash drive, etc.

Recuva

Source: <http://www.piriform.com/recuva>

Recuva recovers deleted files from one's Windows computer, recycle bin, digital camera card, or MP3 player. Its features include:

- **Superior file recovery:** Recuva can recover lost pictures, music, documents, videos, emails, or any other file type. In addition, it can recover from any rewriteable media, which includes memory cards, external hard drives, USB sticks, etc.
- **Recovery from damaged disks:** Recuva can recover files from damaged or newly formatted drives and the chances of recovery are more.
- **Deep scan for buried files:** For those hard to find files, Recuva has an advanced deep scan mode that scours one's drives to find any traces of files that have been deleted.

- **Securely delete files:** Sometimes it requires a certain file to be gone for good. Recuva's secure overwrite feature uses industry- and military-standard deletion techniques to make sure your files stay erased.

Active@ File Recovery

Source: <http://www.file-recovery.net>

Active@ File Recovery contains a CD/DVD ISO image that allows one to burn a bootable CD or DVD with a lightweight version of Windows 7 running in RAM (WinPE 3.0). It can recover data in case the system is not bootable and cannot attach the damaged hard disk drive to another machine.

Pandora Recovery

Source: <http://www.pandorarecovery.com>

Pandora Recovery allows one to find and recover recoverable deleted files from NTFS and FAT-formatted volumes, regardless of their type; it can recover pictures, songs, movies, or documents. Pandora Recovery will scan the hard drive and build an index of existing and deleted files and directories (folders) on any logical drive of the computer with supported file format. Once the scanning is complete, the user gets full control over the files to be recovered and the destination to be used for recovery.

Ontrack EasyRecovery

Source: <http://www.krollontrack.com>

Ontrack DataAdvisor file recovery software unites legacy backup catalogs from various systems and mediums into a single inventory. It provides support to multiple work stations and allows users to create catalog on their own. Once the catalogs are received, they are ingested into Ontrack DataAdvisor, and users can access them through a secured online application. It has recovery tools such as email recovery; hex viewer; self-monitoring, analysis, and reporting technology (SMART); bad block/block usage diagnostics; imaging tools; copy disk; and refresh disk. It offers hard drive monitoring with SMART scan to protect the hard drives and erase functions to free-up storage.

Seagate File Recovery Software

Source: <http://www.seagate.com>

Seagate File Recovery software recovers the files and rescue service plans for storage devices. The tool recovers files from desktops, laptops, and external hard drives as well as tablets, and on-chip memory in smartphones.

Wise Data Recovery

Source: <http://www.wisecleaner.com>

Wise Data Recovery is data recovery software used to retrieve the lost or formatted data, or data that is lost due to system crash. It can recover lost files from hard drive, external hard

drive, USB drive, memory card, digital camera, mobile phone, MP3 player, and other storage media.

Glary Undelete

Source: <http://www.glarysoft.com>

Glary Undelete software works on FAT and NTFS file systems. This tool recovers the files emptied from the Recycle Bin, in a DOS window, from Windows Explorer with the SHIFT key held down. It recovers files that have been deleted by bugs, crashes, and viruses. It can recover files that the user has compressed or fragmented or even encrypted on NTFS file system.

Disk Drill

Source: <http://www.cleverfiles.com>


Disk Drill is data recovery software for Windows PC. It can recover data from internal and external hard drives, USB flash drives, iPods, memory cards. It can recover files from partition loss, hard drive reformatting, failed bootups, accidental deletion, Recycle Bin cleanup, and memory card corruption.

PhotoRec

Source: <http://www.cleverfiles.com>

PhotoRec file data recovery software recovers lost files; video, documents, and archives from hard disks; CD-ROMs; and lost pictures from digital camera memory. It can recover media's file system if it has been severely damaged or reformatted. This tool recovers lost partitions on different file systems and makes non-bootable disks function.

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.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

In Mac OS X, data deletion can be possible due to the following reasons:

- Emptying the Mac Trash folder
- Using the Shift+Del keys
- Corruption in a hard drive
- Virus or Trojan Infection
- Unexpected system shutdown
- Software or hardware malfunction

Recovering deleted files in Mac OS X has three methods:

Method One:

When a user deletes a file from Mac-based file system, the system does not remove it completely; instead, it removes the directory of files from the folder. This de-allocates the space allocated to the file, and the freed space is available for re-allocation to store some other files. The system then sends the deleted files to the folder named "Trash." Navigate to the Trash folder, select the file, right-click (ctrl-click) on it, and select the Put Back option to recover the deleted files.

Method Two:

If user Shift-deletes the files, it bypasses the “Trash.” Investigators can still retrieve such files with data recovery techniques. Time Machine is a local Mac utility program that helps in data recovery:


- Check for the “Time Machine” application in the Utilities folder.
- Click the Time Machine option from the menu bar and select Enter Time Machine.
- The system will display arrows that will help in navigating across the system snapshots or use the timeline displayed on the right side.
- Double click the file to preview the file and its version.
- Click Restore button and the system will restore it in the original folder location.
- Even the Backup folder might contain the accidentally deleted files.











Method Three:

If the previous method fails to recover the deleted files, then use third-party software to recover files emptied from the Trash.

Note: Apple Inc., had introduced the Time Machine utility as a built-in feature in its proprietary Mac OS X systems starting with the 10.5 “Leopard” version.

File Recovery Tools: **MAC**



 AppleXsoft File Recovery for Mac http://www.applexsoft.com	 FileSalvage http://subrosasoft.com
 Disk Doctors Mac Data Recovery http://www.diskdoctors.net	 321Soft Data Recovery http://www.321soft.com
 R-Studio for Mac http://www.r-tt.com	 Disk Drill for Mac http://www.cleverfiles.com
 Data Rescue 4 http://www.prosofteng.com	 Mac Data Recovery Guru http://macosxfilerecovery.com
 Stellar Phoenix Mac Data Recovery http://www.stellarinfo.com	 Cisdem DataRecovery 3 http://www.cisdem.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Some of the software tools that help you recover deleted files in Mac include

AppleXsoft File Recovery for Mac

Source: <http://www.prosofteng.com>

AppleXsoft File Recovery for Mac is a file recovery tool for Mac. The tool scans and recovers files from the hard disk and external storage devices. It supports RAID recovery. The tool includes few advanced tools such as RAID Reconstructor, Mail Recovery, Hex Viewer, SMART, Bad Block Diagnostics, Imaging tools, and Disk Copy.

Disk Doctors Mac Data Recovery

Source: <http://www.diskdoctors.net>

Disk Doctors Mac Data Recovery tool recovers data from corrupt, deleted, and inaccessible partitions formatted by Mac. The tool recovers files from drives damaged by any virus attack, power failure, system crash, or files lost due to human error. It can recover after the volume has been reformatted, even with a different file system. It can also handle the disks with bad sectors.

R-Studio for Mac

Source: <http://www.r-tt.com>

R-Studio for Mac is Mac data recovery software from R-TT. R-Studio for Mac is designed for the Mac OS environment. It recovers files from HFS/HFS+ (Macintosh), FAT/NTFS/ReFS (Windows),

UFS1/UFS2 (FreeBSD/OpenBSD/NetBSD/Solaris), and Ext2/Ext3/Ext4 FS (Linux) partitions. In addition, raw file can be used for heavily damaged or unknown file systems. The tool can recover data on disks, even if their partitions are formatted, damaged, or deleted.

Data Rescue 4

Source: <http://www.prosofteng.com>

Data Rescue for Mac software recovers files from a crashed or virus-corrupted hard drive. It recovers photos, videos, and documents from crashed, corrupted, or non-mounting hard drives; accidentally reformatted hard drives or reinstalled OS; and previous deletion, damaged, or missing files. It can recover all file types from any HFS/HFS+ formatted drive.

Stellar Phoenix Mac Data Recovery

Source: <http://www.stellarinfo.com>

Stellar Phoenix Mac Data Recovery software recovers documents, photos, music, or videos lost due to deletion from any HFS, HFS+, FAT, ExFAT, and NTFS format-based file system. It can perform Mac file recovery on iMac, MacBook Pro, Air, Mac Mini, and Mac Pro. It recovers all deleted files with their original file names. This tool can support RAW recovery on lost volumes.

FileSalvage

Source: <http://subrosasoft.com>

FileSalvage recovery tool for Mac recovers the lost files, iTunes libraries, iPhoto collections, and lost data. This tool can recover files from a normal Mac OS hard drive, USB key, PC disk, Linux disk, FAT32 disk, FLASH card, scratched CD, Digital Camera, iPod, and file system that are recognized in Mac OS X.

321Soft Data Recovery

Source: <http://www.321soft.com>

321Soft Data Recovery for Mac recovers deleted, inaccessible, and lost files from Mac's hard drive. It can recover files lost due to deletion, formatting of the drive, partition errors, corrupted file system, hard disks, solid state drives (SSDs), memory cards, USB sticks, CD/DVD discs, and various other storage devices.

Disk Drill for Mac

Source: <http://www.cleverfiles.com>

Disk Drill for Mac recovery tool recovers data lost due to partition errors on external hard drives, files, and documents in the internal hard drive. It recovers and runs through all of its scanning functions and display a list of files that can be potentially recovered. This tool allows previewing the files and lets you choose the ones that can be successfully recovered.

Mac Data Recovery Guru

Source: <http://macosxfilerecovery.com>


Mac Data Recovery Guru, available for Mac Devices, recovers deleted files. It can recover files from a disk that has been formatted or with a corrupted file system, or files with no file system at all. The tool can make it filesystem independent. The tool can work on hard disks, USB flash sticks, USB hard disks and SSDs, SD cards, digital cameras, and android phones and tablets that are plugged into Mac.

Cisdem DataRecovery 3

Source: <http://www.stellarinfo.com>

Cisdem DataRecovery 3 software recovers photos, videos, documents, etc. on Mac hard drives and external devices. It can restore files from Mac hard drives, external hard drives, Mac notebooks, desktops, Mac server, USB drives, camcorders, memory cards, SD cards, digital cameras, mobile phones, laptops, and MP3 and MP4 players. The tool restores the lost partition and gets back the data from HFS+, FAT16, FAT32, exFAT, ext2–ext4, and NTFS file systems.

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


In Linux, the users can delete the files using “rm” command, but the file will remain on the disk. If a running process keeps a file open and then user removes or deletes the file, then its contents will occupy space on the disk, which other programs or files will not be able to reclaim. The second extended file system (ext2), the most commonly used file system in Linux, shows several places where data can hide.

It is noteworthy 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`.

The main advantage Linux has over Windows is its ability to access and recover data from otherwise problematic machines. The Linux kernel supports a large number of file systems, including VxFS, UFS, HFS, and the aforementioned NTFS and FAT file systems.


Some file systems are not readable in a Windows environment and users can easily recover such files using a bootable Linux distro, such as Knoppix.

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



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

What happens when deleting a partition?

When a user deletes a partition from a hard disk drive, two things are possible:

- All data will be lost on that deleted partition or logical drive.
- In the case of a dynamic disk, deleting a partition can delete all the dynamic volumes on the disk, leaving the disk in a corrupt state.

When a user knowingly or accidentally deletes a hard drive partition, the system does not delete everything but erases the parameters defining the partition set up, size, and location. Users can recover a deleted partition using software that is able to reestablish those parameters.

Deleting a primary partition results in empty space referred to as “unallocated disk space.” Deleting a logical drive within an extended partition results in empty space referred to as “free space” that users can allocate to create additional volumes.

Recovery of the deleted partition is the process by which the investigator evaluates and extracts the deleted partitions. This process recovers the partitions lost accidentally or due to virus, software malfunction, or even sabotage. It is possible to recover all important data lost due to accidental partition deletion by means of a partition recovery utility.

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**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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




Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

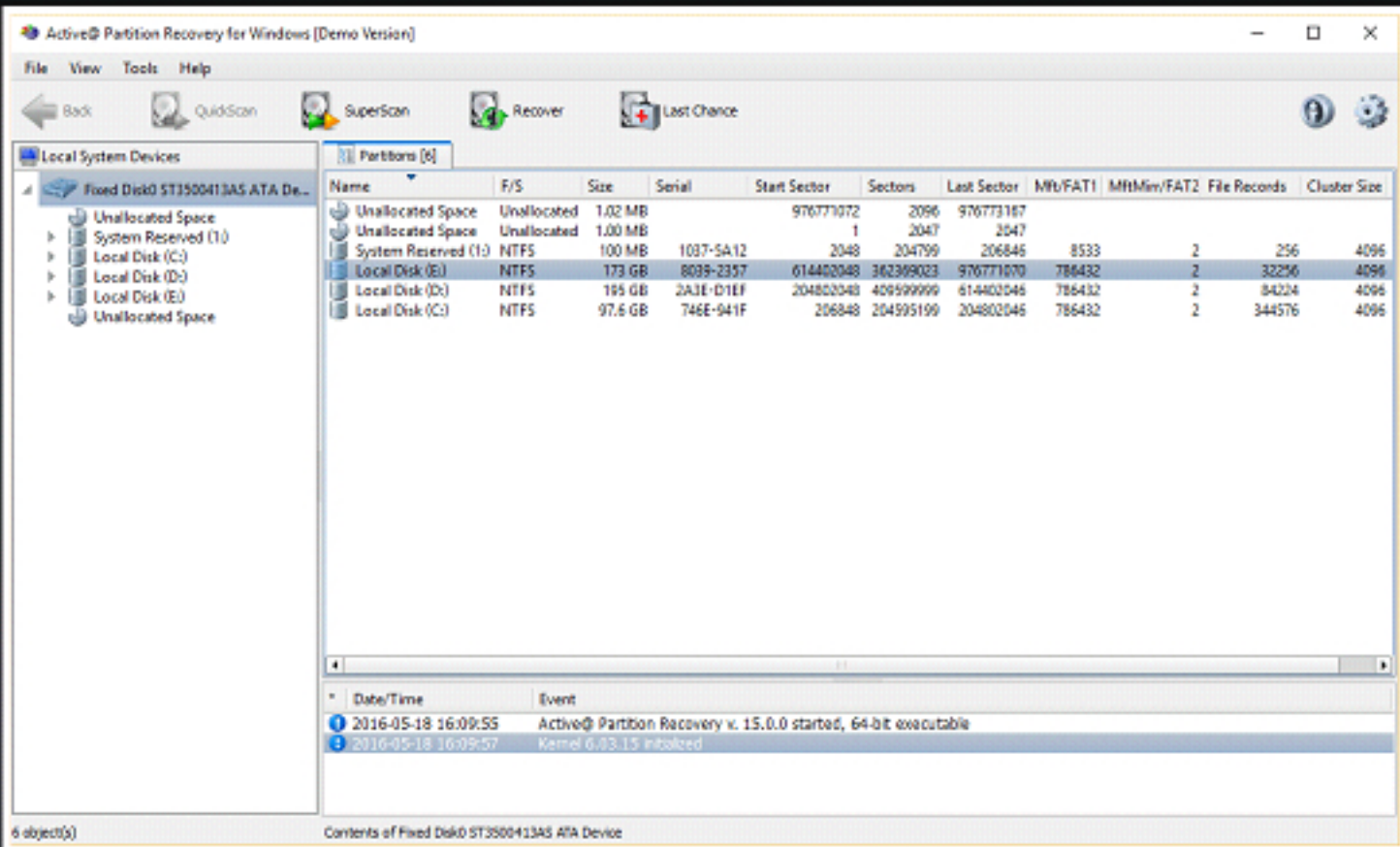
Some of the best partition recovery software includes

- Active@ Partition Recovery for Windows
- Acronis Recovery Expert
- DiskInternals Partition Recovery
- NTFS Partition Data Recovery
- GetDataBack
- EaseUS Partition Recovery
- Advanced Disk Recover
- Power Data Recovery

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>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Active Partition Recovery is a partition recovery toolkit that recovers the deleted and damaged logical drives and partitions within Windows, WinPE (recovery boot disk), and Linux (recovery LiveCD) environments.











Features:

- Restores lost partitions and disks back to working state
- Detects partitions being deleted but not reformatted
- Traces reformatted and damaged partitions
- Fixes damaged Partition Table, Master Boot Record (MBR), and GUID Partition Table GPT
- Creates a Disk Image—sector-by-sector data backup for data recovery
- Restores all data from raw, compressed, and VMWare Disk Images
- Recovers volumes lost due to accidental disk formatting, damage by virus attack, malicious program, or a power failure

Source: <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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

7-Data Partition Recovery

Source: <http://7datarecovery.com>

The partition recovery software, 7-Data Partition Recovery, recovers data from lost, deleted, or damaged partitions by accident. This software aids to recover the data when hard drive has been crashed, MBR corrupted, disk repartitioned (fdisk), partition overwritten, etc.

Features:

- Recovers from lost, deleted, corrupted, or formatted partitions
- Restores the recovered files in exactly the same original structure
- Very easy-to-use with step-by-step wizard process design

Acronis Disk Director Suite

Source: <http://www.acronis.com>

Acronis Disk Director Suite is a partition recovery tool used to recover lost or deleted data. This tool explores partition data before performing partitioning operations. It recovers volumes that were accidentally deleted or damaged due to a hardware failure.

RS Partition Recovery

Source: <http://recoverhdd.com>

RS Partition Recovery is a partition recovery tool that recovers the volumes and corrupted partitions and formatted and repartitioned hard drives to find lost data. It supports badly damaged, formatted, and repartitioned media, and rebuilds the original data structure.

Partition Find & Mount

Source: <http://findandmount.com>

Partition Find & Mount partition recovery software recovers deleted and lost partitions. It works by locating and mounting partitions into the system, thereby making the lost partitions available to any generic disk volume. It will also work when any boot record (including the MBR) is missing, damaged, or overwritten.

Advance Data Recovery Software Tools for NTFS

Source: <http://www.recoverdatatools.com>

Advance Data Recovery Software Tools for NTFS Data Recovery Software enables a user to recover deleted, corrupted, lost, or missing data from Windows NTFS partitions. It restores the lost partitions, files, and folders.

Mac Data Recovery Software

Source: <http://mac.powerdatarecovery.com>

Mac Data Recovery software, file recovery software, can recover deleted files and folders; restore lost data even if the partition is formatted or deleted; and restore data from a corrupted hard drive, virus infection, and unexpected system shutdown or software failure. It supports IDE, SATA, SCSI, USB hard disk, memory card, USB flash drive, and iPod. Mac Data Recovery includes four data recovery modules, namely, Undelete Recovery, Damaged Partition Recovery, Lost Partition Recovery, and Digital Media Recovery. Each data recovery module focuses on a different data loss case.

Quick Recovery for Linux

Source: <http://www.recoveryourdata.com>

Quick Recovery for Linux, Linux partition recovery software, recovers data from damaged, deleted, or corrupted ext2 and ext3 volumes and even from initialized disks. An exhaustive scan of the drive is performed to locate lost volumes. All found data in the lost partition is then presented in a tree structure so that the file can be copied to a working volume. Quick Recovery for Linux is a quick, simple, and easy-to-use data recovery solution that helps in file recovery.

Features:

- Linux data recovery from
 - Accidental file/folder deletion
 - Accidental formatting and creation of a different file system
 - Unexpected system shutdown or software failure

- Simulated previously existing partitions
- File recovery from missing or lost folders
- Recovers even if bad sectors hinder drive access
- Volume recovery on Linux systems with damaged Super Block, Inode list, or Group Descriptor
- Volume recovery when login password is lost

Stellar Phoenix Linux Data Recovery Software

Source: <http://www.stellarinfo.com>

Linux Data Recovery software recovers lost, deleted, formatted, or inaccessible data from ext4, ext3, ext2, FAT32, FAT16, and FAT12 file system-based volumes, irrespective of the instance of data loss.

Features:

- Recovers the lost files, directories, and hard drive volumes
- Recovers from all available hard drive types, including SCSI, SATA, EIDE, and IDE
- User-friendly interface; no technical expertise required

NTFS Data Recovery Toolkit

Source: <http://www.ntfs.com>

NTFS Data Recovery Toolkit is a set of tools for analyzing problems with NTFS partitions and files, and Data Recovery in Manual and Automated modes.

- **Partition Recovery:** Scans disks and detects deleted or severely damaged volumes by recovering deleted or damaged NTFS partitions and files.

TestDisk for Windows


Source: <http://www.cgsecurity.org>











TestDisk is data recovery software that recovers lost partitions and makes non-booting disks bootable when it is caused by faulty software, certain types of viruses, or human error (such as accidentally deleting a partition table).

Features:

- Fixes partition table and recovers deleted partition
- Recovers the FAT32 boot sector from its backup
- Rebuilds the FAT12/FAT16/FAT32 boot sector
- Fixes FAT tables
- Rebuilds the NTFS boot sector
- Recovers the NTFS boot sector from its backup

Note: TestDisk runs on DOS (either real or in a Windows 9x DOS box), Windows (NT4; 2000; XP; 2003; Vista; 2008; Windows 7, 8, and 10] x86; and x64.

Partition Recovery Tools (Cont'd)

 Stellar Phoenix Windows Data Recovery http://www.stellarinfo.com	 TestDisk for Mac http://www.cgsecurity.org
 EaseUS Partition Master http://www.easeus.com	 Starus Partition Recovery http://www.starusrecovery.com
 Hetman Partition Recovery https://hetmanrecovery.com	 Disk Drill http://www.cleverfiles.com
 MiniTool Power Data Recovery Free http://www.powerdatarecovery.com	 Stellar Phoenix Mac Data Recovery http://www.stellarinfo.com
 Remo Recover (Mac) - Pro http://www.remosoftware.com/	 ZAR Windows Data Recovery http://www.z-a-recovery.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Stellar Phoenix Windows Data Recovery

Source: <http://www.stellarinfo.com>

Stellar Phoenix Data Recovery for Windows, data recovery software, performs hard drive recovery; RAID and server recovery; database recovery; email recovery; photo, music, and video recovery; etc. It can recover data from any storage media for data loss caused by hard drive crash, physical or mechanical failure of the hard drive and other storage media, and data loss due to natural calamity, etc.

EaseUS Partition Master

Source: <http://www.easeus.com>

EaseUS Partition Master partition recovery tool is used for partition recovery and cloning. The tool recovers deleted or lost partitions from unallocated space due to any personal, hardware or software failure, or virus attack. It can recover deleted or lost partitions after repartitioning the hard drive.

Hetman Partition Recovery

Source: <https://hetmanrecovery.com>

Hetman Partition Recovery restores data from damaged FAT and NTFS disks, thereby recovering the original file and folder structure. The tool discovers all previously created volumes letting users to search and recover files from the deleted volumes.

MiniTool Power Data Recovery Free

Source: <http://www.powerdatarecovery.com>

MiniTool Power Data Recovery Free is partition recovery software for Windows and server users. The tool scans to recover the formatted, damaged, and corrupted RAW files and partitions from external and internal hard disks to recover the partitions.

Remo Recover (Mac) - Pro

Source: <http://www.remOSOFTWARE.com>

Remo Recover Mac software is a binary application that makes Mac data recovery easy on both Intel and PowerPC Mac machines. It efficiently recovers files emptied from the Trash or lost due to inaccessible Mac volumes.

The extensive volume scanning engine helps in recovering files from Mac volumes that fail to mount or have been accidentally formatted. The software has the capability to recover data even if the Disk Verify and Repair tool fails to retrieve the lost data.

Remo Recover retrieves data lost from

- Accidentally emptying the Trash
- Damaged or corrupted catalog file
- Corruption of volume header
- Corruption of Apple Partition Map
- Volume failing to mount

TestDisk for Mac

Source: <http://www.cgsecurity.org>

TestDisk data recovery software recovers lost partitions and makes non-booting disks bootable again it is caused due to faulty software, certain types of viruses, or human error (such as accidentally deleting a partition table).

Starus Partition Recovery

Source: <http://www.starusrecovery.com>

Starus Partition Recovery repairs the broken partitions and recovers the missing information. It recovers the lost and deleted files. The tool recovers files and folders from damaged, inaccessible, and repartitioned disks. It fixes corrupted disk system structures and rebuilds corrupted and overwritten file systems.

Disk Drill

Source: <http://www.cleverfiles.com>

Disk Drill, Mac data recovery software, recovers data from HFS/HFS+, FAT, NTFS, and other file systems. It undeletes Mac OS files using its two powerful Mac recovery methods: Quick and Deep scanning. Disk Drill data recovery for Mac OS X locates and recovers deleted files from any

mountable media, including the main hard drive, external hard disk, memory cards, iPods, etc. Disk Drill can recover photos, music, documents, applications, specific Mac OS X files, and other file formats.

Stellar Phoenix Mac Data Recovery

Source: <http://www.stellarinfo.com>

Stellar Phoenix Mac Data Recovery software that recovers lost, deleted, formatted, or inaccessible data from HFS, HFS+, HFS Wrapper, and FAT file system volumes irrespective of the data loss situation.

Features:

- Recovers all the deleted, lost, or formatted data such as documents, emails, pictures, music, video, etc.
- Recovers from any internal/external hard drives, USB flash drives, memory cards, and iPods
- Supports all PowerPC and Intel-based Macs

ZAR Windows Data Recovery


Source: <http://www.z-a-recovery.com>


ZAR is a Windows data recovery program. It uses thorough checks and cross-checks to derive the necessary information.

Features:

- Runs on Windows NT/2000/XP/2003/Vista/7
- Supports FAT16, FAT32, and NTFS file systems
- Provides limited ext2 (Linux file system) support
- Offers partition recovery
- Provides hardware RAID 0 and RAID 5 recovery
- Supports long and national file names
- Supports native NTFS compression


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**


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

A password refers to collection of words, letters, numbers, and/or special characters used for security processes such as user authentication or to grant access to a resource. The password ensures that unauthorized users do not access the computer, network resources, or other secured information. In addition, data files and programs may require a password.

Password protection shields information, protects networks, applications, files, documents, etc., from unauthorized users. Many organizations and individuals, who do not want others to access their data, resources and other products, employ passwords and strong cryptographic algorithms as security measures.

Attackers and intruders use these protection techniques to hide evidence data, prevent reverse engineering of applications, hinder information extraction from network devices, and prevent access of system and hard disk. This can make forensic investigators' work difficult. However, there are tools that recover the passwords. Encryption is one of the preferred techniques for deterring the forensic analysis.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Passwords are important, because they are the gateway to most computer systems. Computing devices can store and transmit passwordss as cleartext, obfuscated, and hashed passwordss, of which only hashed passwordss need cracking while the other password types can assist in the cracking phase.

- **Cleartext Passwords**

- The passwordss sent and stored in plaintext without any alteration
- Ex: Windows Registry houses automatic logon password
(HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon)
- Investigators can use tools such as Cain and Ettercap to sniff cleartext passwordss

- **Obfuscated Passwords:**


- The passwordss stored or communicated after a more or less transformation
- When transformation is reversible, password becomes unreadable when user applies an algorithm and on application of reverse algorithm, it returns a cleartext


- **Hashed Passwords:**

- Hashed passwordss seem similar to obfuscated passwordss, but the latter are reversible


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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Password crackers are the software programs that help investigators or users to recover the passwords stored or transmitted by a system. These are the tools used to identify unknown passwords and forgotten passwords of a network resource or a computer or an application. Unauthorized persons, attackers, and intruders use these tools to access protected resources. Most password-cracking techniques are successful because of weak or easily guessable passwords.

Password crackers identify correct passwords primarily in two methods, namely, dictionary searches and brute force cracking. The brute force method used by password crackers involves running the predetermined length set of characters until it finds a suitable one. The dictionary technique searches for an appropriate word in the dictionary that exactly fits as a password. Password dictionaries include a wide range of topics, such as music groups, movies, politics, etc.

Hybrid password crackers use various combinations of dictionary and brute-force cracking methods, e.g., cat01, cat02, cat03, etc. This type of cracking method is very useful if the owner had set a password with a combination of numbers.

Some password crackers even identify encrypted passwords and decrypt them. At first, these tools identify and retrieve the passwords from a computer memory and redirect to decrypt them. The tools use an algorithm much similar to that a system program had used to create an encrypted password.

To understand working of password crackers, one must be well aware of how password generators work. Password generators mostly use cryptography in their working process.

Cryptography is the study of creating and breaking codes or coded data. Crypto is a Greek word that means something hidden, veiled, obscured, mysterious, or secret. Graph is derivative of the word “graphia,” which means writing. Therefore, cryptography is the art of secret writing. Passwords use mostly encrypted form.

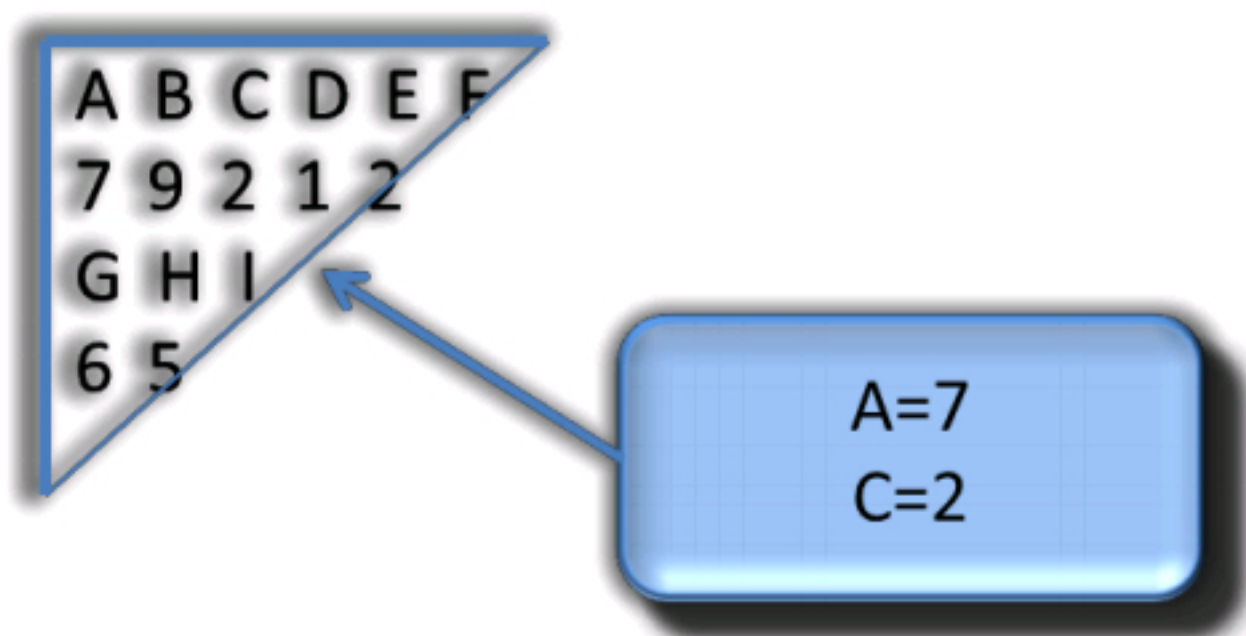


FIGURE 5.3: Cryptography Algorithms

In the above figure, there is a table, or legend, to the left. Below each letter is a corresponding number. Thus, A = 7, C = 2, and so forth. This is a code of sorts but easy to decode. ROT-13 is a method, which replaces each letter by a substitute letter. Moving 13 letters ahead derives the substitute letter.

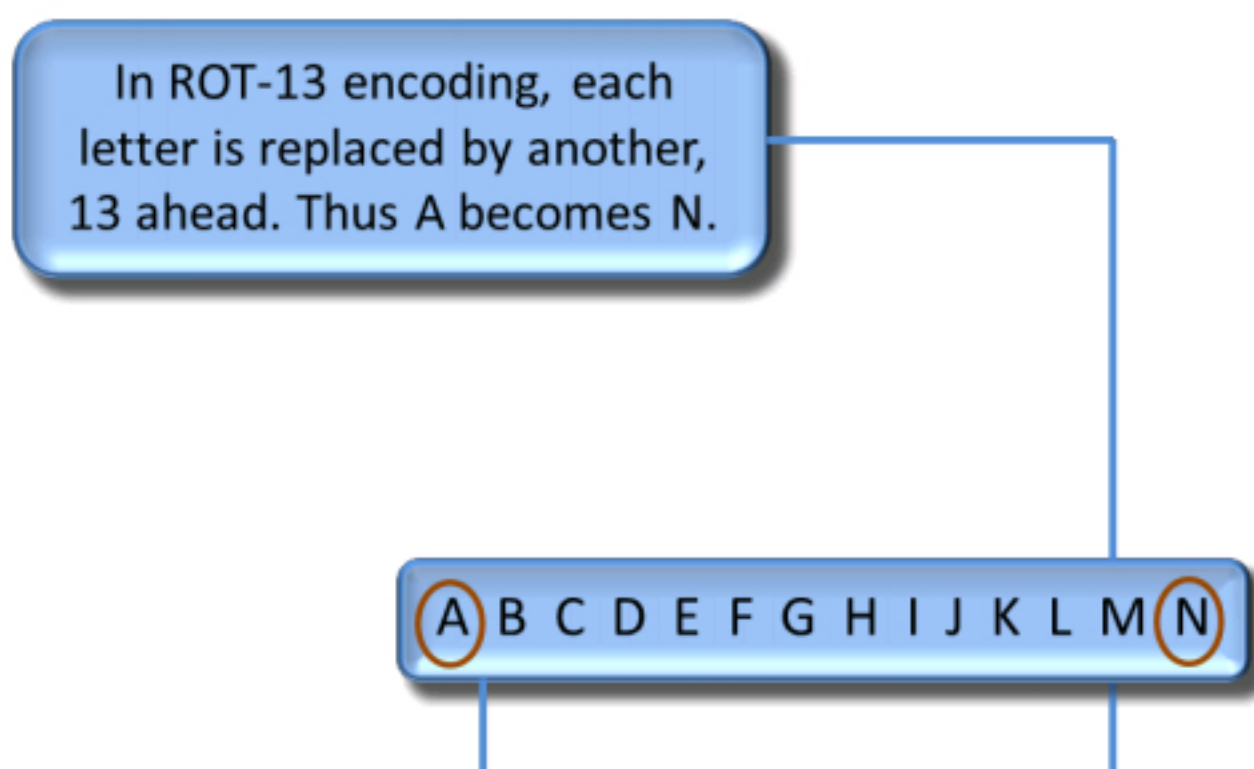


FIGURE 5.4: ROT - 13 encoding method to crack password

This is an ineffective method of encoding or encrypting a message. There are programs that quickly identify this pattern.

The following figure shows how a password-cracking process takes place:

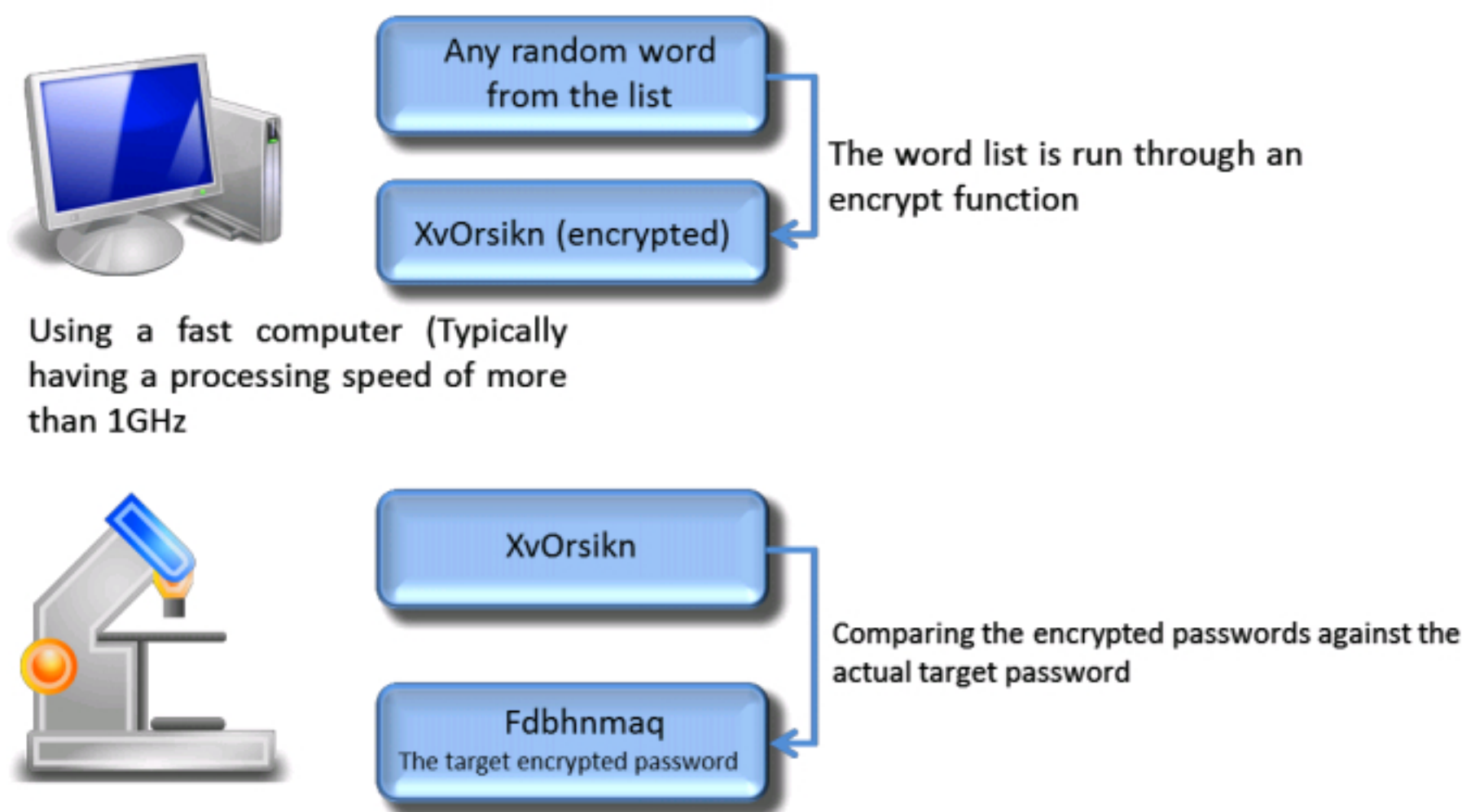


FIGURE 5.5: Process of password cracking

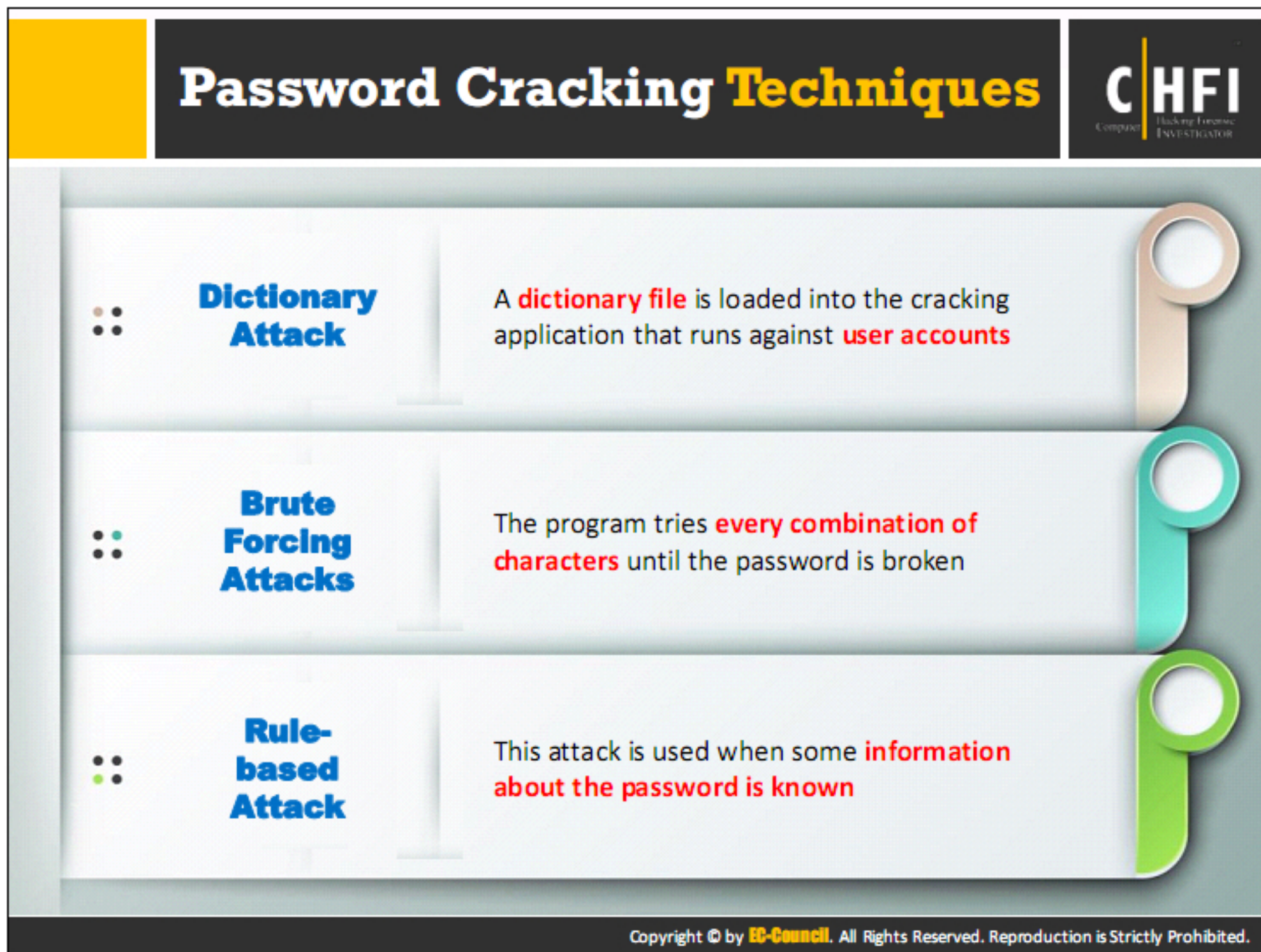
Following are the steps involved in password-cracking process:

- Create a word list with a dictionary generator program or dictionaries
- Hash or encrypt the list of dictionary words
- Compare the hashed wordlist against the target hashed password, generally one word at a time
- If it matches, the password crack is successful, and the password cracker displays the unencrypted version of the password

Some password crackers perform this task differently. They send the word list through the encryption process, generally one word at a time. Apply rules to the word and after each such application; they compare each word to the target password (encrypted). If they do not match, the cracker will send the next word through the process. The difference is not academic. The first technique is probably much faster.

It is of some significance that the various password-cracking utilities are not user-friendly. In fact, when executed, some of them forward nothing more than a cryptic message.

Note: Investigators and attackers can obtain the target's hashed password by sniffing it from a wired or wireless network or directly from the Security Accounts Manager (SAM) or shadow password files on the hard drive of a system.



There are three popular techniques for password cracking:

Method 1: Dictionary Attacks

In a dictionary attack, a dictionary file is loaded into the cracking application that runs against user accounts. A dictionary is a text file that contains a number of dictionary words or predetermined character combinations. The program uses every word present in the dictionary to find the password. Dictionary attacks are more useful than a brute-force attack. However, this attack does not work against a system that uses the passphrases or passwords not contained within the dictionary used.

This attack is applicable in two situations:

- In cryptanalysis, it helps to find out the decryption key for obtaining the plaintext from the ciphertext.
- In computer security, it helps to avoid authentication and to access a computer by guessing passwords.

Methods to improve the success of a dictionary attack:

- Use more number of dictionaries, such as technical dictionaries and foreign dictionaries that help to retrieve the correct password.
- Use the string manipulation on the dictionary, i.e., if the dictionary contains the word, "system," then try string manipulation and use "metsys" and others.

Method 2: Brute-Forcing Attacks

Cryptographic algorithms must be hard enough to prevent a brute-force attack. The definition, stated by RSA is, “Exhaustive key-search, or brute-force search, is the basic technique for trying every possible key in turns until the correct key is identified.”

Brute-force attack refers to the process of trying each and every single of the encryption keys to find the required information. Brute-force attacks need more processing power compared to other attacks.

A brute-force attack is basically a cryptanalytic attack used to decrypt any encrypted data. In other words, testing all possible keys is an attempt to recover the plaintext, which is the base for producing a particular ciphertext. The detection of key or plaintext at a faster pace compared to the brute-force attack is the process of breaking the cipher. A cipher is secure if no method exists to break that cipher other than a brute-force attack. Mostly, all ciphers lack mathematical proof of security.

Some considerations for brute-force attack are as follows:


- It is a time-consuming process.
- Can eventually trace all passwords.
- An attack against Networking Technology (NT) hash is much harder against LAN Manager (LM) hash.

Method 3: Rule-based Attack


Attackers use the rule-based attack when they know some credible information about the password, such as rules of setting the password, algorithms involved, or the strings and characters used in its creation. For example, if the attackers know that the password contains a two- or three-digit number, then they will use some specific techniques to extract the password in less time.

By obtaining useful information, such as use of numbers, the length of password, and special characters, the attacker can easily adjust the time for retrieving the password to the minimum and enhance the cracking tool to retrieve passwords. This technique involves brute-force, dictionary, and syllable attacks. The attackers may use multiple dictionaries, brute-force techniques, or simply try to guess the password.

Default Passwords

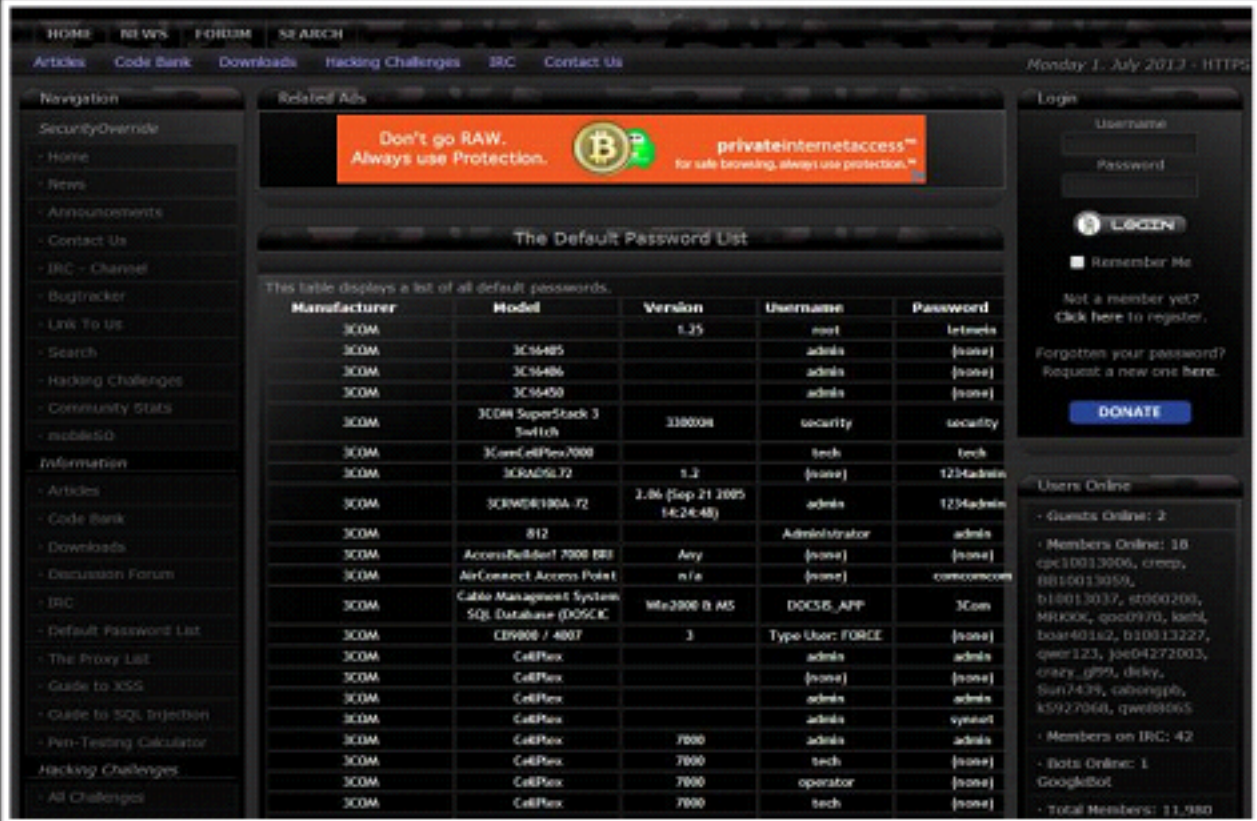


- A default password is a password supplied by the **manufacturer** with new equipment (e.g. switches, hubs, and routers) that is password protected
- You can use default passwords from the list of words or dictionary that is used to perform **password guessing attack**



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>




<http://securityoverride.org>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Default passwords refer to those supplied by the manufacturers with new equipment. Usually, default passwords provided by the manufacturers of password-protected devices allow the user to access the device during initial setup and then change the password. But often, an administrator will either forget to set the new password or ignore the password-change recommendation and continue to use the original password. Attackers can exploit this lapse and find the default password for the target device from manufacturer websites to successfully access the target device.


Source: <http://securityoverride.org>

Using Rainbow Tables to Crack Hashed Passwords




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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

A rainbow table is a lookup table specially used in recovering a plaintext password from a cipher text. It consists of a table with all possible plaintext combinations for encrypted passwords created using a specific hash algorithm. The table contains word lists such as dictionary files and brute-force lists along with their computed hash values.

The attacker uses this table to look for the password and tries to recover it from password hashes. An attacker computes the hash for a list of possible passwords and compares it to the pre-computed hash table (rainbow table). If attackers find a match, they can crack the password.

A rainbow attack is the implementation of the cryptanalytic time-memory trade-off technique. In this attack, the intruders use already calculated information stored in the rainbow tables. They store the password hash table in the memory and use it to extract plaintext password from a ciphertext.

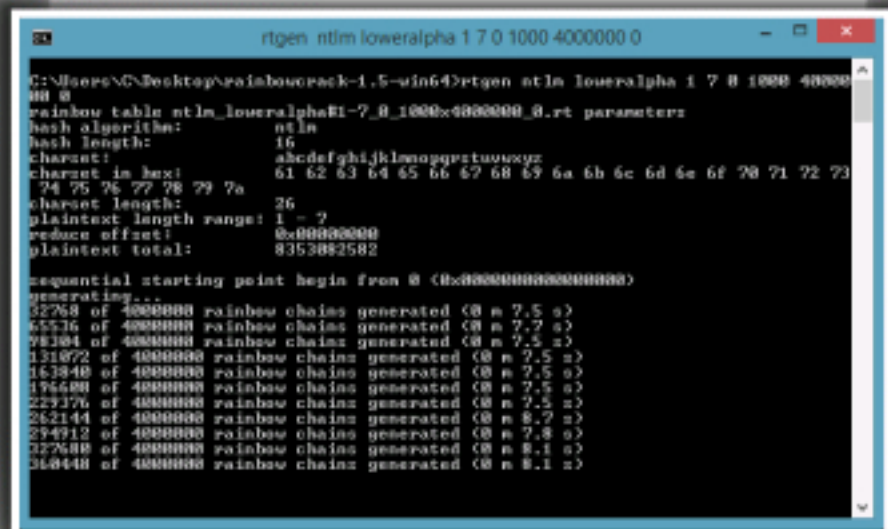
It is easy to recover passwords by comparing captured password hashes to the pre-computed tables.

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:

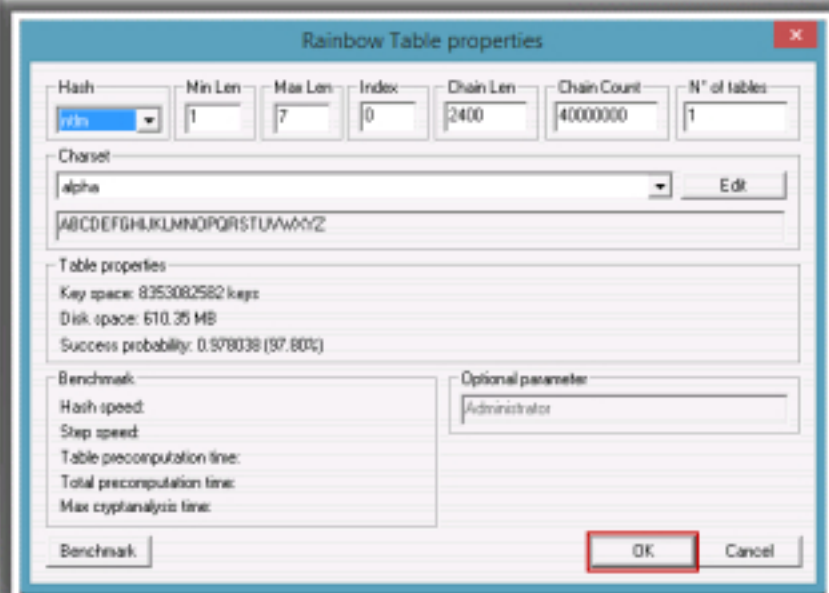
```
rtgen hash_algorithm charset  
plaintext_len_min plaintext_len_max  
table_index chain_len chain_num  
part_index
```



<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>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can create rainbow tables by using the following tools.

rtgen

Source: <http://project-rainbowcrack.com>

RainbowCrack is a general purpose implementation tool that takes advantage of the time-memory trade-off technique to crack hashes. This project allows you to crack a hashed password. The rtgen tool of this project helps to generate the rainbow tables. The rtgen program needs several parameters to generate a rainbow table.

Winrtgen


Source: <http://www.oxid.it>


Winrtgen is a graphical Rainbow Tables Generator that helps attackers to create rainbow tables from which they can crack the hashed password.

Generate Rainbow Tables Using Winrtgen:

1. Download and install **Winrtgen**.
2. Click the **Add Table** button.
3. In the Rainbow Table properties window, set up all of the properties, and click **OK**.
4. In the main program, click **OK**.


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



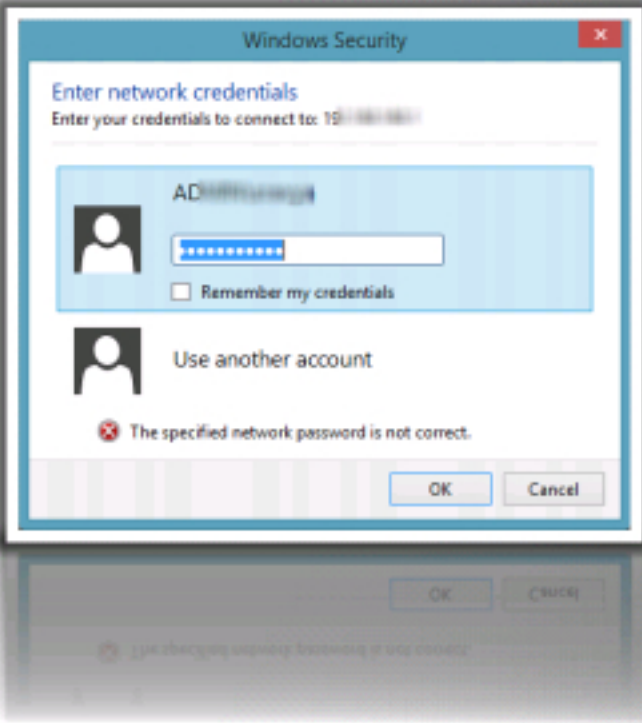
NTLM Authentication


- 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





Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

When users log in to the Windows computer, a series of steps is performed for user authentication. The Windows OS authenticates its users with the help of three mechanisms (protocols) provided by the Microsoft.

SAM Database

Windows uses the SAM database to manage user accounts and passwords in the hashed format (one-way hash). The system does not store the passwords in plaintext format but stores them in hashed format in order to protect them from attacks. The system implements SAM database as a registry file. The Windows kernel obtains and keeps an exclusive file system lock on the SAM file, as this file consists of a file system lock, which provides some security for the storage of passwords.

It is not possible to copy the SAM file to another location in case of online attacks. Because the system locks the SAM file with an exclusive file system lock, a user cannot copy or move it while Windows is running. The lock will not release until the system throws a blue screen exception or the OS has shut down. However, to make the password hashes available for offline brute-force attacks, attackers can dump the on-disk contents of the SAM file using various techniques.

The SAM file uses a SYSKEY function (in Windows NT 4.0 and later versions) to partially encrypt the password hashes.

Even if hackers use subterfuge techniques to discover the contents, the encrypted keys with a one-way hash make it difficult to hack. In addition, some versions have a secondary key, making the encryption specific to that copy of the OS.

NT LAN Manager (NTLM) Authentication


NTLM is a default authentication scheme that performs authentication using a challenge/response strategy. Because it does not rely on any official protocol specification, there is no guarantee that it works correctly in every situation. It has been on some Windows installations where it worked successfully. NTLM authentication consists of two authentication protocols: NTLM and LM. These protocols use different hash methodology to store users' passwords in the SAM database.

Kerberos Authentication

Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography. This provides mutual authentication, in that both the server and the user verify each other's identity. Messages sent through Kerberos protocol are protected against replay attacks and eavesdropping.

Kerberos makes use of the Key Distribution Center (KDC), a trusted third party. This consists of two logically distinct parts: an Authentication server (AS) and a Ticket Granting Server (TGS). Kerberos use "tickets" to prove a user's identity.

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."


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows OSs use SAM database file to store user passwords. The SAM file is stored at %SystemRoot%/system32/config/SAM in Windows systems, and Windows mounts it in the registry under the HKLM/SAM registry hive. It stores LM or NTLM hashed passwords.

NTLM supersedes the LM hash, which is susceptible to cracking. New versions of Windows still support LM hashes for backward compatibility; however, Vista and later Windows versions disable LM hash by default. The LM hash is blank in newer Windows versions. Selecting the option to remove LM hashes enables an additional check during password change operations but does not clear LM hash values from the SAM immediately. The SAM file stores a "dummy" value in its database, which bears no relationship to the user's actual password and is the same for all user accounts. It is not possible to calculate LM hashes for passwords exceeding 14 characters in length. Thus, the LM hash value is set to a "dummy" value when a user or administrator sets a password of more than 14 characters.


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**




Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


System software password cracking refers to the process of cracking the OS and all other utilities that enable a computer to function. The system creates passwords for the software to avoid access to system files and other secured information used during the booting of the system. Following are the ways by which one can access the system:

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

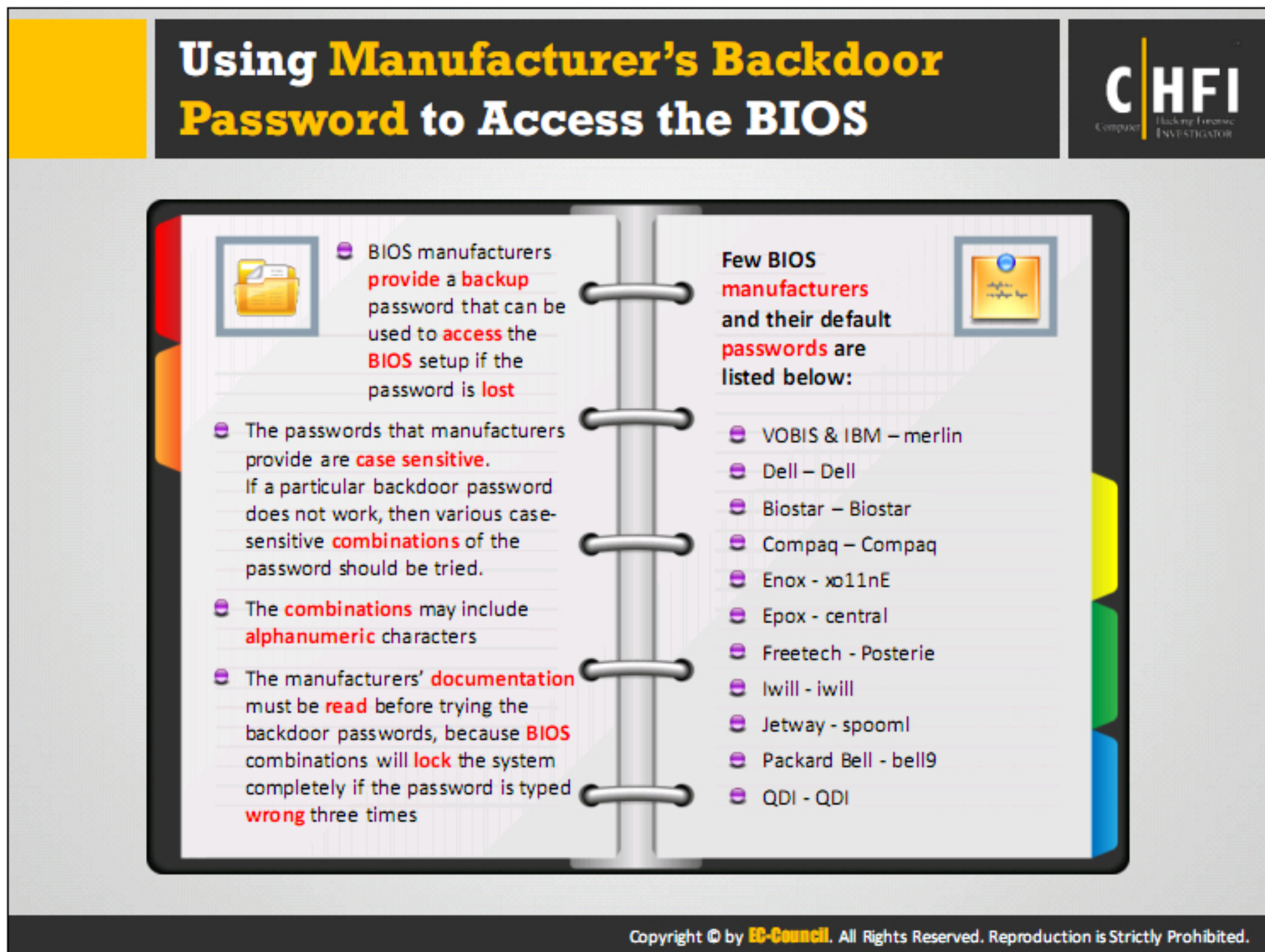
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Basic Input Output System (BIOS), a type of boot loader, is a firmware code run that runs first when the users switch on the system. The main function of BIOS is to identify and initialize system component hardware, such as the hard disk, floppy drive, and video display card.

A BIOS password protects the computer system from others and restricts access to sensitive information.

Methods to bypass/reset the BIOS password:

- Using a manufacturers' backdoor password to access the BIOS password
- Using password-cracking software
- Resetting the CMOS using the jumpers or solder beads
- Removing the CMOS battery for at least 10 minutes
- Using a professional service
- Overloading the keyboard buffer




Manufacturers provide a backdoor password to provide access to the BIOS setup if the user loses password. The passwords provided by the manufacturers are case-sensitive. If a particular backdoor password does not work, then users can try various case-sensitive combinations of the password. The combinations may include alphanumeric characters, numbers, and alphabets. Before trying the backdoor passwords, it is advised to read manufacturers' documentation because BIOS combinations will lock the system completely, if the user types wrong password three times.

Some manufacturers and the backdoor passwords they provide are as follows:

- VOBIS & IBM - merlin
- Dell - Dell
- Biostar - Biostar
- Compaq - Compaq
- Enox - xo11nE
- Epox - central
- Fretech - 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

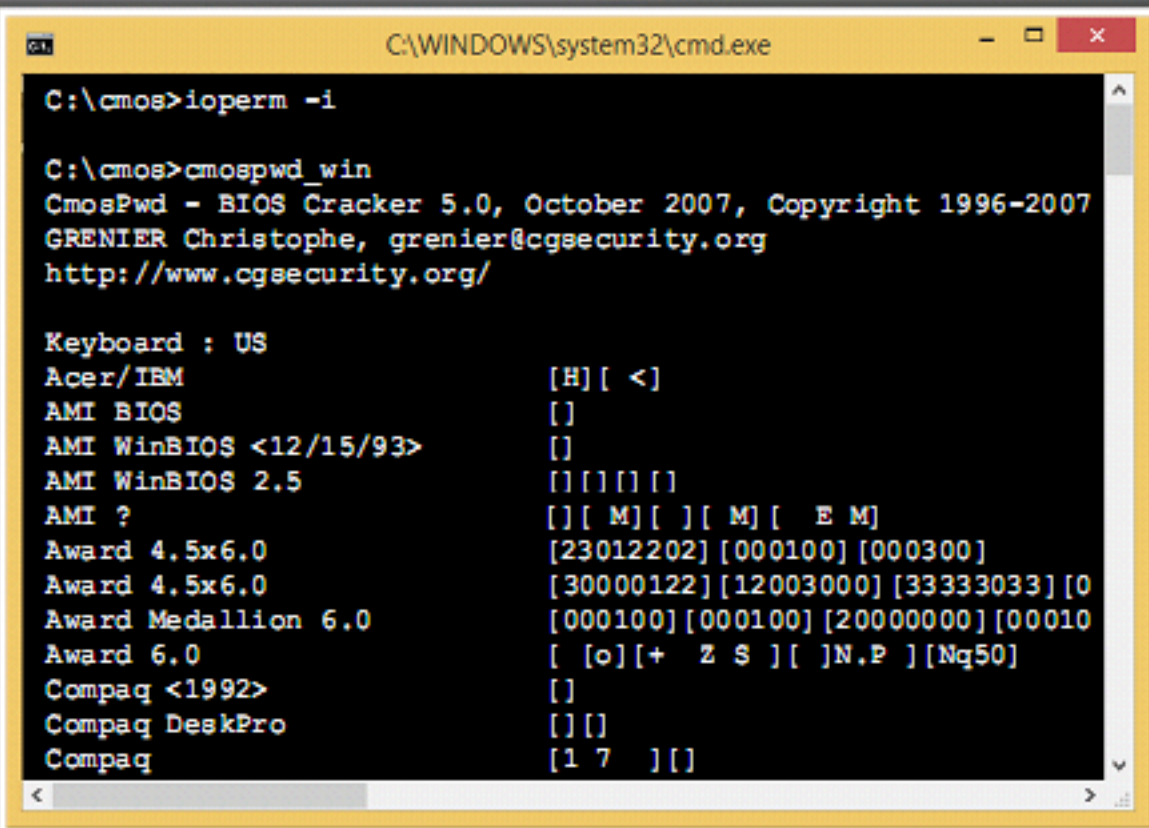
Decrypts password stored in CMOS, which is used to access BIOS SETUP

<http://www.cgsecurity.org>

DaveGrohl

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

<http://davegrohl.org>



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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The following software will help the investigators to either crack or reset the BIOS on many chipsets:

CmosPwd

Source: <http://www.cgsecurity.org>

CmosPwd is CMOS/BIOS password recovery tool. It decrypts passwords stored in CMOS used to access BIOS SETUP. CmosPwd works and compiles under Dos-Win9x, Windows NT/W2K/XP/2003, Linux, FreeBSD, and NetBSD.

CmosPwd decrypts the password stored in CMOS used to access BIOS SETUP. It works with the following BIOS:

- ACER/IBM BIOS
- AMI BIOS
- AMI WinBIOS 2.5
- Award 4.5x/4.6x/6.0
- Compaq (1992)
- Compaq (New version)
- IBM (PS/2, Activa, Thinkpad)
- Packard Bell

Module 05 Page 524

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Phoenix 1.00.09.AC0 (1994), a486 1.03, 1.04, 1.10 A03, 4.05 rev 1.02.943, 4.06 rev 1.13.1107
- Phoenix 4 release 6 (User)
- Gateway Solo—Phoenix 4.0 release 6
- Toshiba
- Zenith AMI


CmosPwd can also backup, restore, and erase cmos.

DaveGrohl

Source: <http://davegrohl.org>

DaveGrohl is a multi-threaded distributed password cracker aiming at brute-forcing OS X user passwords. Initially created in early 2011 as a password hash extractor and companion tool but has since evolved into a standalone or distributed password cracker. It supports the entire standard Mac OS X user password hashes (MD4, SHA-512, and PBKDF2) used since OS X Lion and also can extract them formatted for other popular password crackers such as John the Ripper. The latest stable release is designed specifically for Mac OS X Lion and Mountain Lion.

Resetting the CMOS using Jumpers or Solder Beads

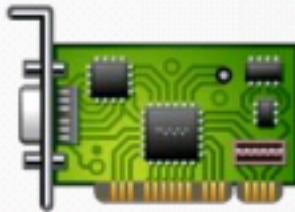


1 Resetting the CMOS using Jumpers

- 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 **jumper/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



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Resetting the CMOS using the Jumpers

The motherboard features a set of jumpers or DIP switches that clear the BIOS/CMOS settings, allowing them to reset. To reset the CMOS using the jumpers, follow the steps below:


- Check the computer or motherboard manufacturer's documentation to locate the jumpers/DIP switches.
- If the document 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.

Resetting the CMOS using the Solder Beads

To reset the CMOS using the solder beads, follow the steps below:

- By connecting or jumping specific solder beads on the chipset, it is possible to reset the CMOS.
- By going through the computer and motherboard's documentation for details, as there are too many chipsets to break down of which points to jump on individual chipsets and solder beads location can vary by manufacturer.

Removing CMOS Battery



Step 1

Shut down the **system** and disconnect the power plug

Open the **CPU cabinet** and locate the **CMOS battery** (silver circular battery) on the motherboard

Step 2

Step 3

Remove the **CMOS battery** from the socket and keep it out for 20 to 30 minutes. This **flushes** out the **CMOS memory** that stores BIOS passwords and other configurations


Replace the **battery** and **start** the **system** normally

Step 4

Note: Sometimes, manufacturers use capacitors to provide backup power to the CMOS battery. Thus, if the first attempt fails, keep the battery out for 24 hours


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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**

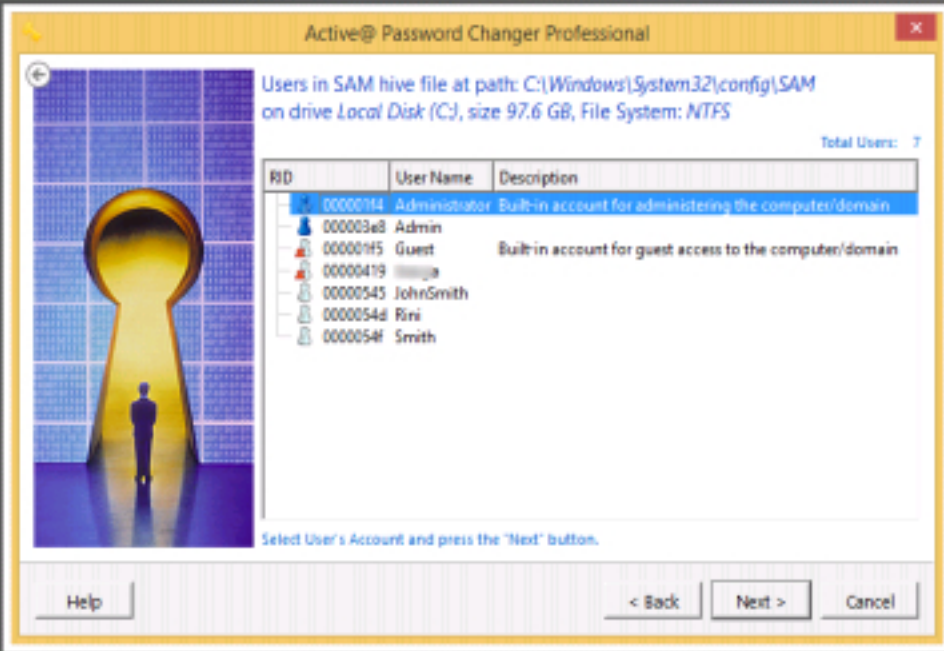


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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

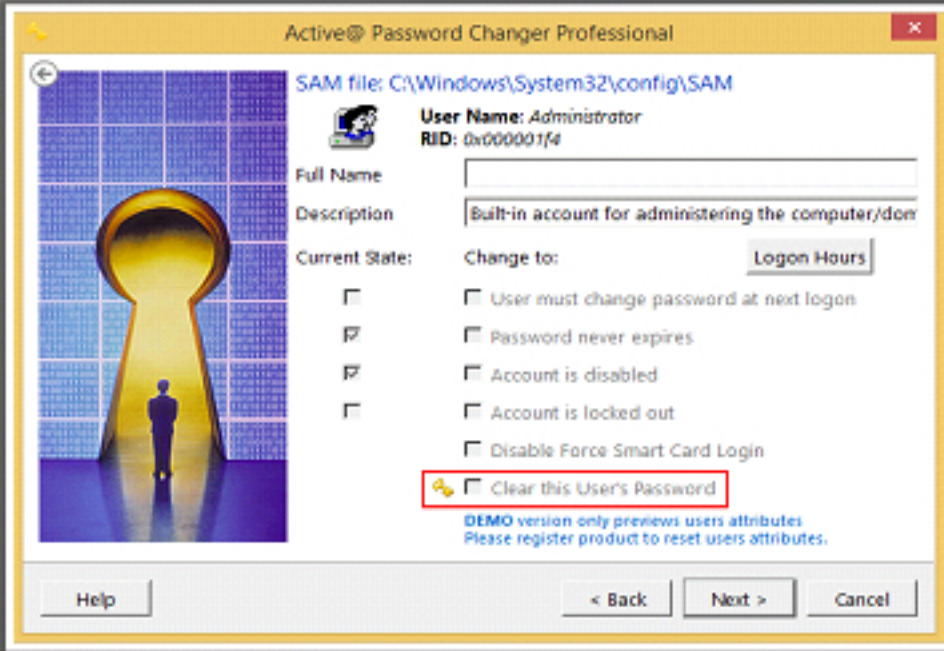


Users in SAM hive file at path: C:\Windows\System32\config\SAM on drive Local Disk (C:), size 97.6 GB, File System: NTFS

Total Users: 7

RID	User Name	Description
000001B4	Administrator	Built-in account for administering the computer/domain
000003E8	Admin	
000001F5	Guest	Built-in account for guest access to the computer/domain
00000419		
00000545	JohnSmith	
00000548	Rini	
0000054F	Smith	

Select User's Account and press the "Next" button.



SAM file: C:\Windows\System32\config\SAM

User Name: Administrator
RID: 0x000001B4

Full Name: [Empty]
Description: Built-in account for administering the computer/domain

Current State: ☐ Logon Hours

☐ User must change password at next logon
☒ Password never expires
☐ Account is disabled
☐ Account is locked out
☐ Disable Force Smart Card Login
☒ Clear this User's Password

DEMO version only previews users attributes
Please register product to reset users attributes.


<http://www.password-changer.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


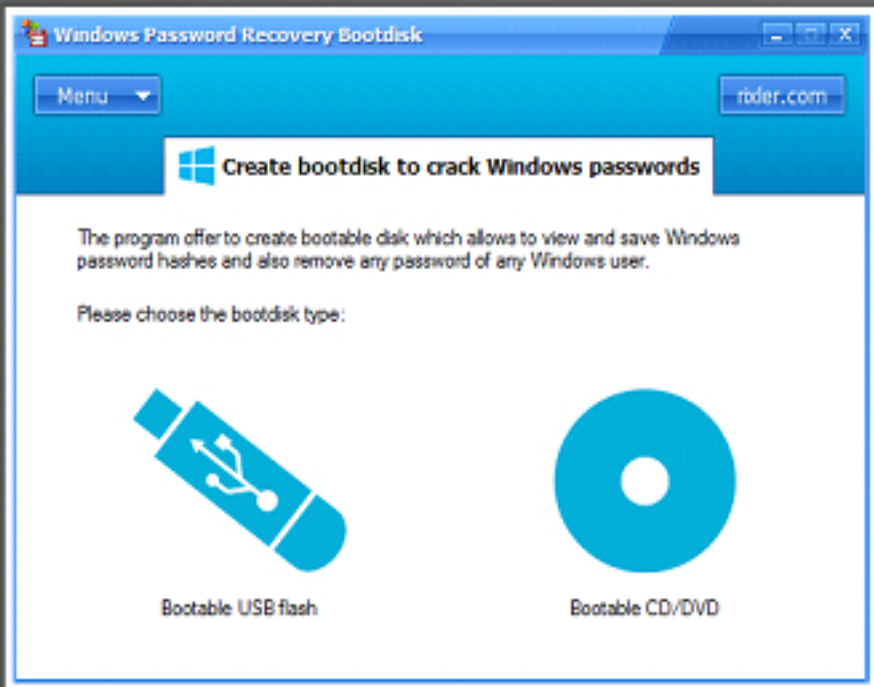
Active@ Password Changer is designed for resetting local administrator and user passwords on Windows XP/Vista/2008/2003/2000, and Windows 7 systems in case an administrator's password is forgotten or lost. Forgotten password recovery software has a simple user interface, supports multiple hard disk drives, detects several SAM databases (if multiple OS were installed on one volume), and provides the opportunity to pick the right SAM before starting the password recovery process. Active@ Password Changer displays a list of all local users. The software user simply chooses the local user from the list to reset the password. With Active@ Password Changer you can log in as a particular user with a blank password.

Source: <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.nixler.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Windows Key creates a password reset CD or USB Flash Drive that works during the boot process and instantly resets Administrator or other account passwords and Windows security settings that prevent you from logging in.

Features:

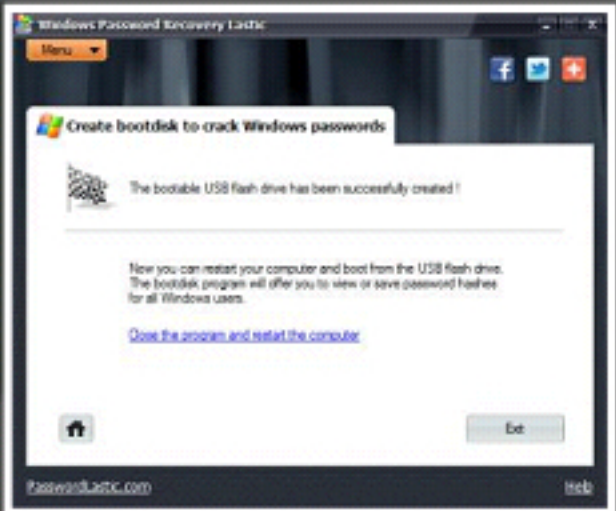
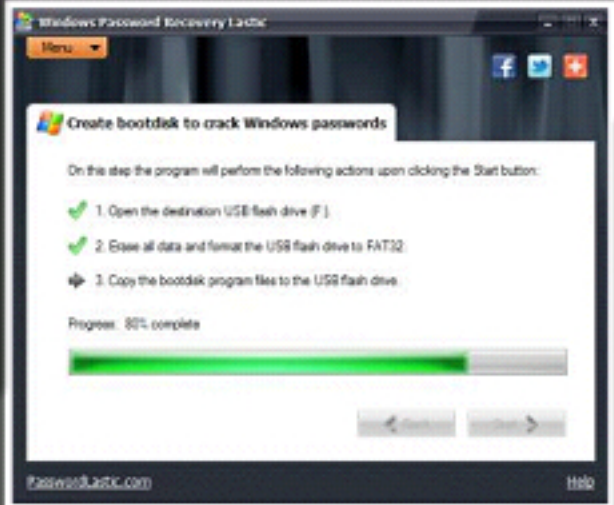
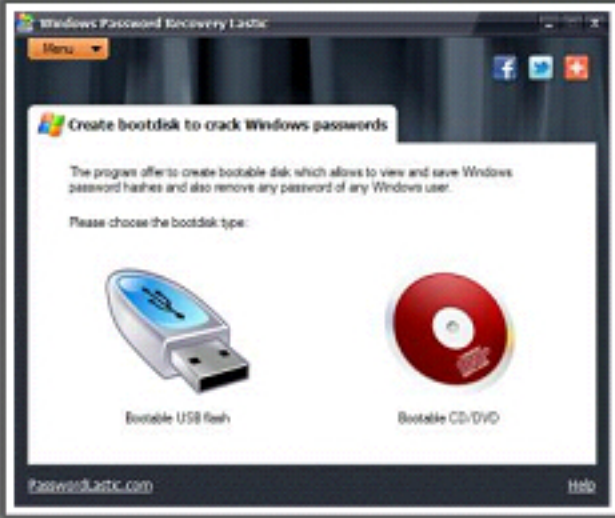
- Resets passwords with a bootable CD or USB drive
- Burns a password reset CD
- Resets Domain Administrator password
- Resets local Administrator password
- Resets local policy settings
- Resets secure boot options
- Displays account properties
- Supports RAID/SCSI/SATA drives

Source: <http://www.lostpassword.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>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Password Recovery Lastic is a password recovery tool used to recover the password in Windows OSs. This tool requires rebooting into another OS. Run the tool on another computer to create a bootable USB stick or CD/DVD disk and then Boot from it on the computer and the program lists all user accounts it finds, thereby offering an easy way to remove a password of any of them.

Once Windows Password Recovery Lastic loads its boot part from a bootable, it offers the user a choice to either remove a password of some particular Windows user account or to save its hash. Removing a password is done instantly; therefore, this is a preferable way to access the computer.

Source: <http://www.passwordlastic.com>

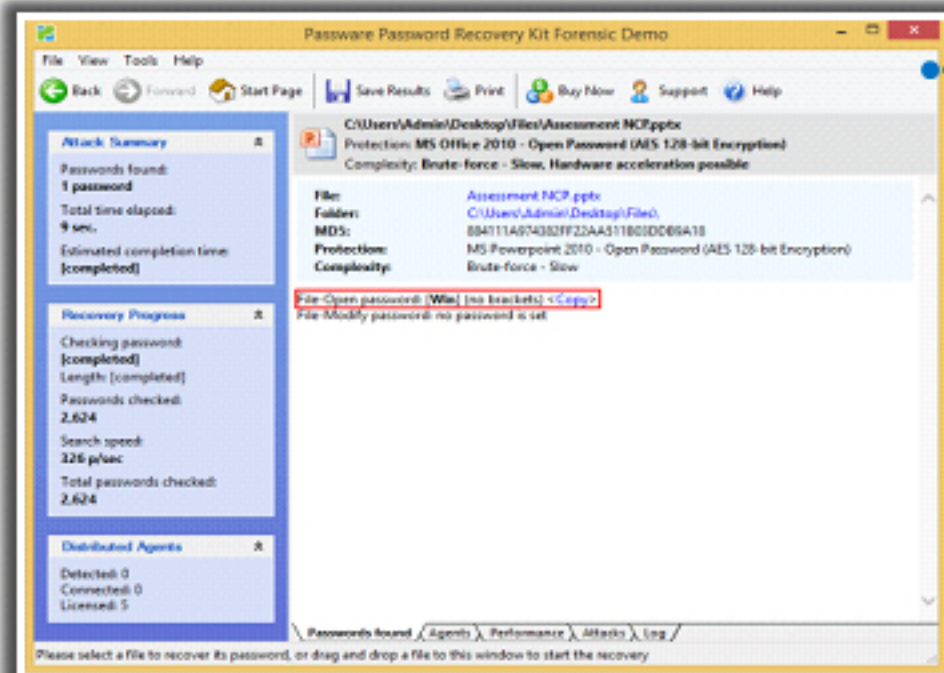
Application Password Cracking Tools



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

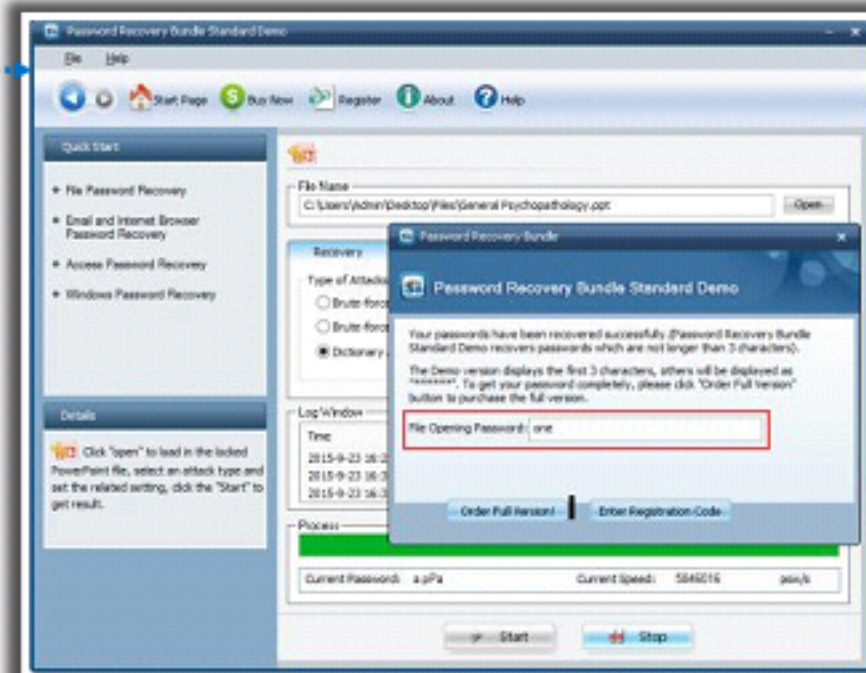
Electronic evidence discovery solution that reports all password-protected items on a computer, and decrypts them



<http://www.lostpassword.com>

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.recoverlostpassword.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Passware Kit Forensic

Source: <http://www.lostpassword.com>

This complete electronic evidence discovery solution reports all password-protected items on a computer and gains access to these items using the fastest decryption and password recovery algorithms.

Features:

- Recovers passwords for 200+ file types and decrypts hard disks providing an all-in-one user interface
- Scans computers and network for password-protected files
- Acquires memory images of the seized computers
- Retrieves electronic evidence from a Windows Desktop Search Database
- Recovers Mac User Login passwords from computer memory
- Supports Distributed and Cloud Computing password recovery
- Runs from a USB thumb drive and recovers passwords without installation on a target PC

SmartKey Password Recovery Bundle Standard

Source: <http://www.recoverlostpassword.com>

SmartKey Password recovery bundle Standard is multi-functional password recovery software. It recovers passwords for Windows Excel, Word, Access, PowerPoint, Outlook, Outlook Express, PDF, RAR/WinRAR, ZIP/WinZIP, MSN, AOL, Google Talk, Paltalk, Trillian, Miranda, Opera, Firefox, IE Browser, etc.

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

Office Password Recovery Toolbox

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

<https://www.elcomsoft.com>

<http://www.rlxer.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Advanced Office Password Recovery

Source: <http://www.elcomsoft.com>

Advanced Office Password Recovery unlocks documents created with all versions of Microsoft Office. It recovers passwords for Microsoft Word, Excel, Access, Outlook, Project, Money, PowerPoint, Visio, Publisher, and OneNote.

Features:

- Instant password recovery for multiple products
- Exploits all known backdoors and tricks in the Office family for instant recovery
- Instantly unlocks documents with previously recovered passwords
- Dictionary and brute-force attacks with user-defined masks and advanced templates

Office Password Recovery


Source: <http://www.passwordrecovery.in>

Office Password Recovery tool recovers lost or forgotten passwords for Microsoft Word, Excel, Access, PowerPoint, OneNote, Outlook email accounts, and personal folder files. It recovers all types of passwords, including instant recovery of passwords to modify, database passwords, workbook passwords, pst passwords, and email account passwords.

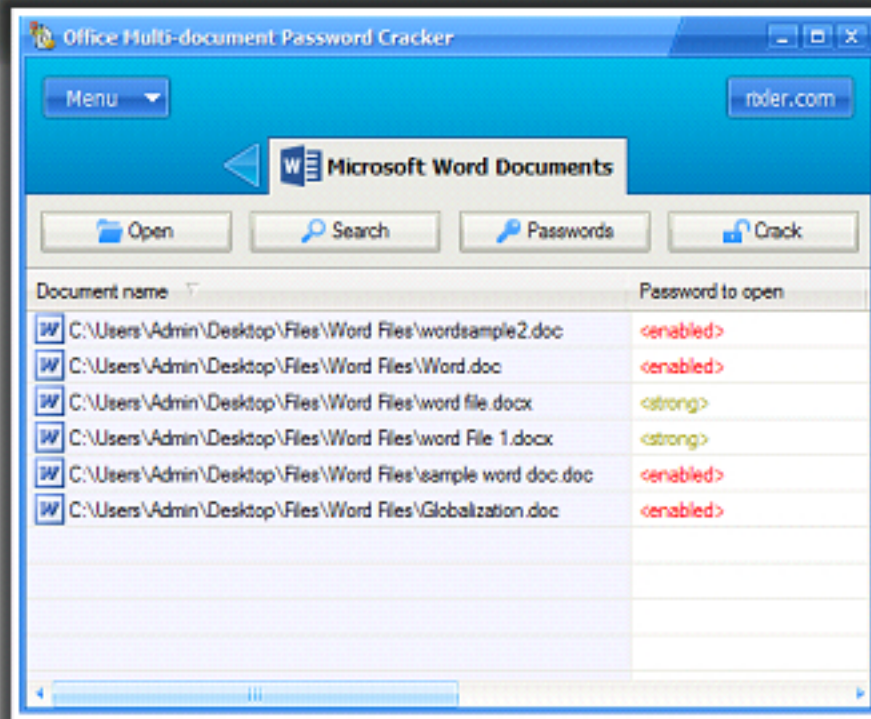
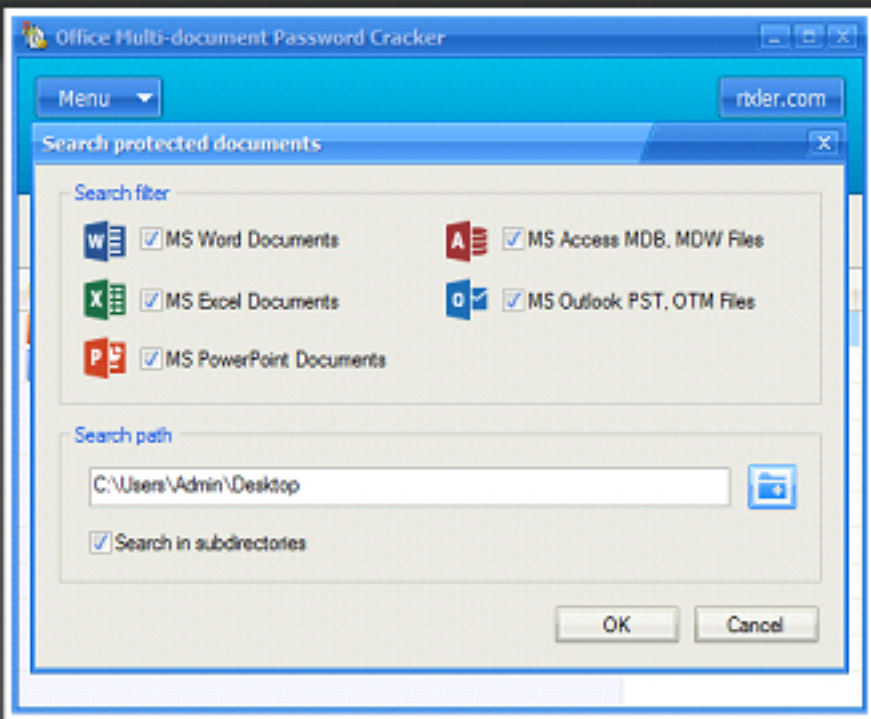
Features:

- Instant recovery of Microsoft Outlook and Microsoft Exchange passwords to open personal folders and personal storage files
- Instant recovery of MS Outlook email accounts and pst passwords, including GMail, Hotmail, Yahoo, and MSN accounts
- Recovers shared protection passwords, formatting and editing restrictions, locked cells protection, and permissions
- Instant recovery of MS PowerPoint passwords to modify presentations
- Built-in efficient attack profiles that allow the recovery of passwords with a single key press
- Recovers passwords in any language (Unicode support) and multi-language passwords

Application Password Cracking Tools (Cont'd)



- Recover 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.rlxler.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Office Multi-document Password Cracker


Office Multi-document Password Cracker cracks lost passwords to multiple MS Office documents. It scans the drives for protected documents and restores passwords from all Word, Excel, PowerPoint, Access, and Outlook documents it finds.

Features:

- Recover passwords from MS Word, MS Excel, MS Outlook, MS PowerPoint and MS Access documents, or remove them if recovery is not possible
- Find protected documents on the disk and cracks them
- Restore lost VBA project passwords
- Crack recently opened document passwords, upon startup of the program
- Online password recovery service with guaranteed privacy
- Supported types of passwords: passwords to open, passwords to modify, document protection passwords, VBA projects passwords, workbook and worksheet passwords (MS Excel only), and database and user workgroup passwords (MS Access only)


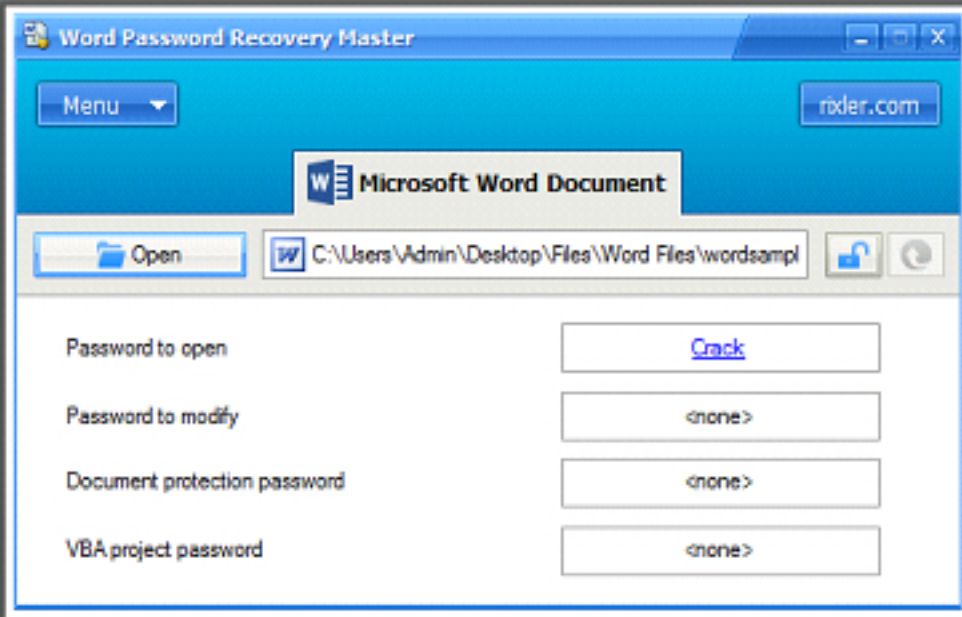
Source: <http://www.rlxler.com>

Word Password Recovery Tools



Word Password Recovery Master

Accent WORD Password Recovery



<http://www.rixler.com>

<http://passwordrecoverytools.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Word Password Recovery Master

Source: <http://www.rixler.com>

Word Password Recovery Master is used to crack password-protected documents created in MS Word 97/2000/XP/2003/2007/2010/2013. The program allows the user to crack “open,” “protection,” and “write” passwords.

Features:

- Removes the “open” MS Word password
- Removes the “protection” MS Word password
- Recovers the “write” MS Word password
- Online Word password recovery service with guaranteed privacy
- Instant recovery of passwords of any length and complexity
- Support for multilingual passwords

Accent WORD Password Recovery

Source: <http://www.passwordrecoverytools.com>

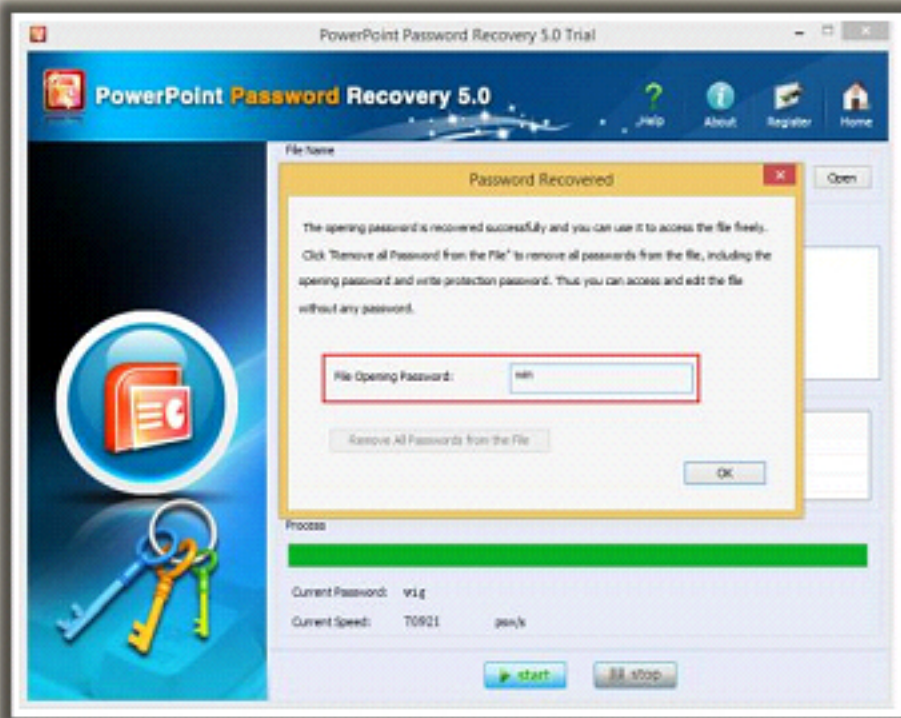
Accent WORD Password Recovery tool recovers lost Microsoft Word passwords. It provides full support for all versions of Microsoft Word with lightning-fast recovery of Microsoft Word passwords.

Features:

- Supports all versions of Microsoft Word (from Word 6/95 to Word 2010)
- Instantly deletes several types of passwords
- Automatically recovers passwords using pre-installed scenarios
- Includes Macro language for adding password mutation rules to dictionary attacks
- Reduces password recovery time on all computers with Intel and AMD processors

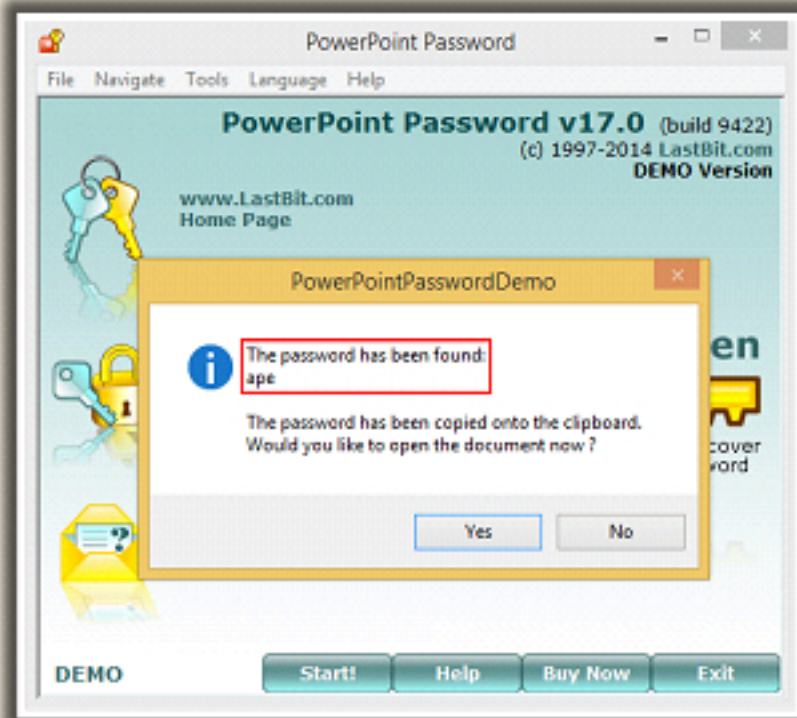
PowerPoint Password Recovery Tools

SmartKey PowerPoint Password Recovery



<http://www.recoverlostopassword.com>

PowerPoint Password Recovery



<http://passwordtools.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SmartKey PowerPoint Password Recovery

Source: <http://www.recoverlostopassword.com>

PowerPoint Password Recovery tool is designed to recover lost or forgotten MS PowerPoint presentation passwords. It uses three different searching methods: advanced dictionary attack, brute-force attack, and advanced brute-force with mask attack.

Features:

- MS PowerPoint versions 2002 to 2007 are supported
- Instantly recover all other types of PowerPoint passwords
- Include a wizard for easy setup of password recovery attacks

PowerPoint Password

Source: <http://lastbit.com>

PowerPoint Password recovers lost or forgotten passwords to PowerPoint (*.ppt) files. It supports brute-force, dictionary, hybrid dictionary, and smartforce (TM) attacks.

PowerPoint Password supports brute-force attack, dictionary attack, hybrid dictionary attack and SmartForce (TM) attack. The tool recovers simple passwords.

Excel Password Recovery Tools



PDS Excel Password Recovery



<http://www.excelpasswordcracker.com>

Accent EXCEL Password Recovery



<http://www.passwordrecoverytools.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

PDS Excel Password Recovery

Source: <http://www.excelpasswordcracker.com>

PDS Excel Password Recovery is used to crack password-protected documents created in MS Excel 97/2000/XP/2003/2007/2010 (*.xls, *.xlsx files). The application is a quick algorithm-based Excel Password Breaker. The program allows cracking “open,” “write,” “workbook,” “shared workbook,” and “worksheet” passwords.

Features:

- Group recently made best method to unlock Excel password named as Excel Password Cracker (XLS and XLSX)
- Cracks 2007 Excel password or cracks 2010 Excel password through all safe recovery process
- Recovers password using brute-force attack, and dictionary-based attacks

Accent EXCEL Password Recovery


Source: <http://www.passwordrecoverytools.com>

Accent EXCEL Password Recovery recovers lost or forgotten passwords for opening documents and modifying worksheets in Microsoft Excel 95-2010 workbooks. It uses three password recovery methods: an advanced dictionary-based attack, a brute-force attack, and a brute-force attack using an advanced mask to recover the passwords.

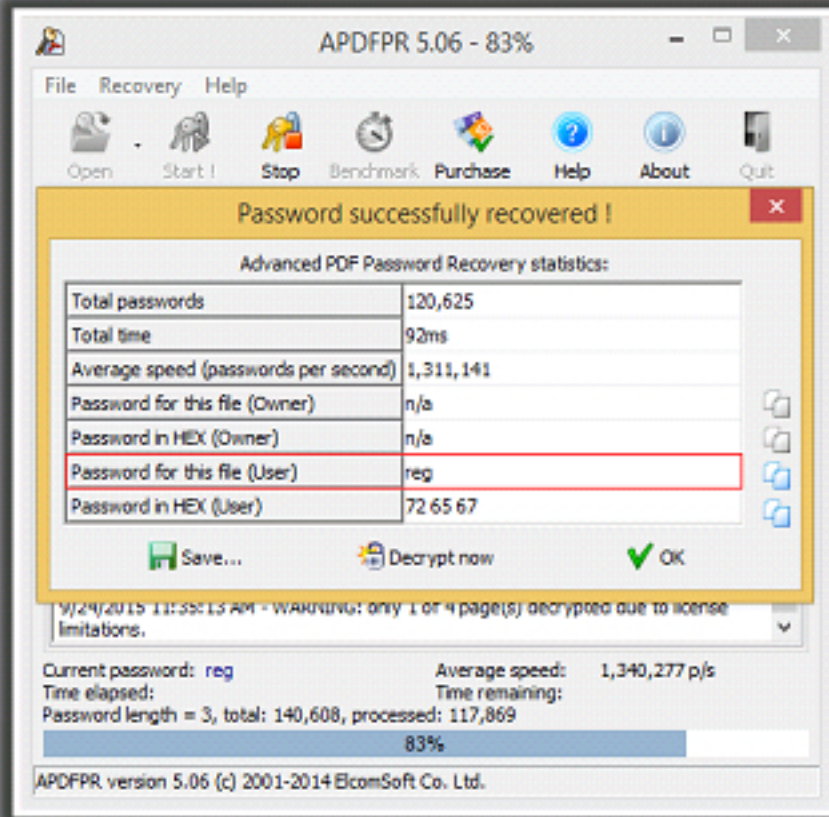
Features:

- Supports Microsoft Excel 97, Excel 2000, Excel XP, Excel 2003, Excel 2007, and Excel 2010
- Supports different password types; password to open a document, password to modify, and spreadsheet protection password
- Recovers password using brute-force attack, mask, and dictionary-based attacks

PDF Password Recovery Tools

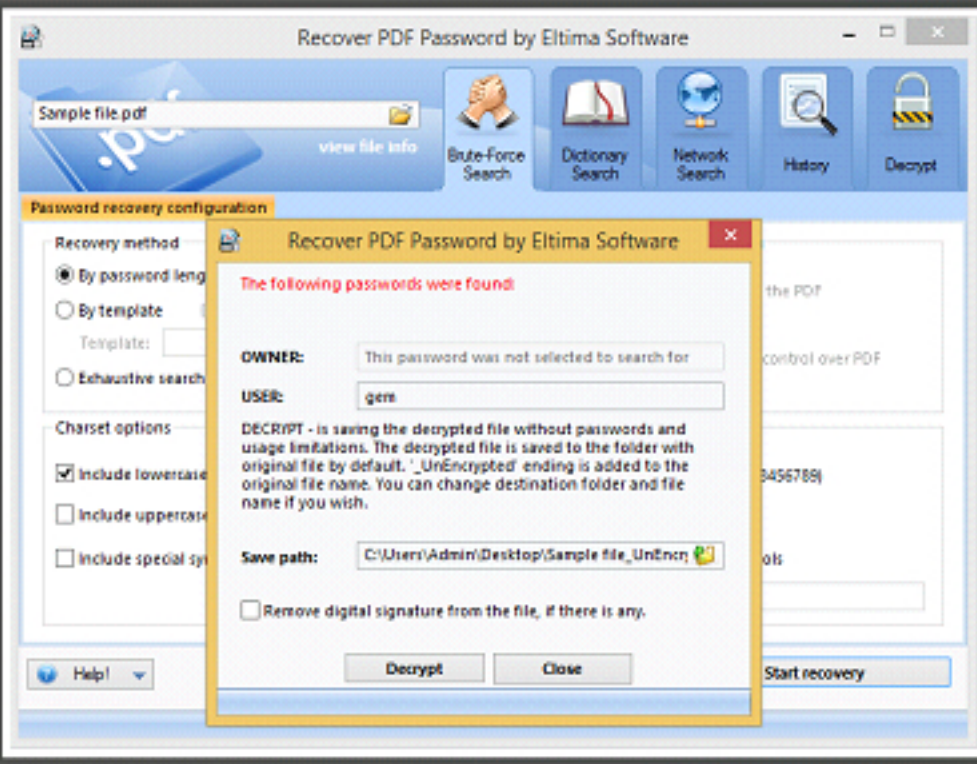


Advanced PDF Password Recovery



<https://www.elcomsoft.com>

PDF Password Cracker



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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Advanced PDF Password Recovery

Source: <https://www.elcomsoft.com>

Advanced PDF Password Recovery recovers password-protected or locked PDF documents created with all versions of Adobe Acrobat or any other PDF application.

Features:

- Instantly unlocks PDF documents with printing, copying, and editing restrictions
- Removes “owner” and “user” passwords
- Recovers passwords to open
- Supports 40-bit and 128-bit RC4 encryption as well as 128-bit and 256-bit AES encryption
- Dictionary and brute-force attacks with user-defined masks and advanced templates

PDF Password Cracker

Source: <http://www.crackpdf.com>

PDF Password Cracker is a utility to remove the security on PDF documents. Following protection methods are cracked:


- Restricted operations on file can be disabled

- It can also be used to decrypt files you know the password for

Features:

- Support AES decryption
- Decrypt PDF files protected with owner passwords
- Instantly remove restrictions on copying, printing and other actions with the file
- Support PDF1.8 (Acrobat 9.x) files, including 40-bit RC4 decryption, 128-bit RC4 decryption, and AES decryption
- Decryption, compressed files, and unencrypted metadata
- Decrypt protected Adobe Acrobat PDF files, removing restrictions on printing, editing, and copying

ZIP/RAR Password Recovery Tool: Advanced Archive Password Recovery



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

ARCHPR 4.54 - 93%

File Recovery Help

Open Start! Stop Benchmark Purchase Help About Quit

Encrypted ZIP/RAR/ACE/ARJ-file
C:\Users\Admin\Desktop\Target1-PWD Pr

Type of attack
Brute-force

Password successfully recovered !

Advanced Archive Password Recovery statistics:

Total passwords	134,677
Total time	13s 797ms
Average speed (passwords per second)	9,761
Password for this file	wow
Password in HEX	77 6f 77

Save... OK

9/24/2015 12:39:55 PM - 'wow' is a valid password for this file

Current password: wow Average speed: 9,762 p/s
Time elapsed: 13s Time remaining:
Password length = 3, total: 140,608, processed: 131,924
93%

ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

<https://www.elcomsoft.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Advanced Archive Password Recovery tool recovers protection passwords or unlocks encrypted ZIP and RAR archives created with all versions of popular archivers. The tool recovers passwords for plain and self-extracting archives created with PKZip, WinZip, RAR, and WinRAR automatically or with your assistance.


Features:

- Supports all versions of ZIP/PKZip/WinZip, RAR/WinRAR, ARJ/WinARJ, and ACE/WinACE (1.x)
- Supports strong AES encryption found in WinRAR and the new versions of WinZip
- Exploits all known vulnerabilities and implementation flaws in the various compression algorithms for faster recovery
- Supports background operation by utilizing idle CPU cycles
- Uses dictionary and brute-force attacks with user-defined masks and advanced templates


Source: <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>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Office Password-Cracking Software

Stellar Phoenix Office Password Recovery

Source: <http://www.stellarinfo.com>

Stellar Phoenix Office Password Recovery recovers files with both “Password To Open” and “Password To Modify” features applied to a single MS Office file. The Office password recovery time varies depending on the complexity of the password and the search criteria set. The software recovers MS Office password by trying out various character combinations for the specified length.

Features:

- Recovers MS Office passwords—“Password To Open” and “Password To Modify”
- Uses brute-force attack for accurate password recovery
- Facilitates masking to minimize the recovery time
- Maintains dynamic dictionary containing all recovered Office passwords

Online Password Recovery

Source: <https://www.password-find.com>

Online Password Recovery recovers passwords and unlocks 100% of the protected Microsoft Office 97/2000 documents and about 80% of the protected Microsoft Office 2007/2010

Module 05 Page 544

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

documents. This tool enables users to find Microsoft Office passwords thousand times faster than the average home computer. It instantly removes password protection from all formats of Microsoft Office documents of Office 2007/2010/2013.

Online Password Genius

Source: <http://www.isunshare.com>

Office Password Genius is Office password recovery software. It recovers office 97-2016 forgotten or lost password easily.

Features:

- Recovers Office 97-2016 password without data damage or loss
- Provides three editions for Office password recovery
- Recovers lost Office password with password attack types
- Uses brute-force attack, brute-force with mask attack, dictionary attack, and smart attack
- Three and less characters of Office password can be recovered by free trial version

Office Password Recovery Lastic

Source: <http://www.passwordlastic.com>

Office Password Recovery Lastic password recovery tool is capable of restoring, cracking, or resetting passwords to various Microsoft Office documents including MS Word, MS Excel, MS PowerPoint, MS Outlook, and MS Access. This tool uses "Password Server" technology that allows users to both crack document passwords almost instantly and keep the personal data and contents of a document safe.

SmartKey Office Password Recovery

Source: <http://www.recoverlostpassword.com>

SmartKey Office Password Recovery recovers the lost or forgotten password for Office document. It cracks passwords of MS Word, Excel, Access, PowerPoint, and Outlook etc. for Office suite.

Features:

- Instant access to password-protected documents in Microsoft Office suite (Word, Excel, PPT, Outlook, etc.)
- Boosts the speed to recover password with multi-core CPU and GPU acceleration
- Offers two recovery service: remove password and recover password
- Supports nearly all versions of Microsoft Office applications from 97 to 2016

PDF Cracking Software

PDF Password Recovery

Source: <http://www.top-password.com>

PDF Password Recovery recovers lost or forgotten password of password-protected PDF files (*.pdf). It unlocks the restricted PDF documents by removing the permissions password. It searches for the user/open password to your encrypted PDF file using the most popular password-cracking methods, that is, brute-force attack, mask attack, and dictionary attack.

Features:

- Recovers PDF owner password and user passwords
- Removes PDF restrictions on printing, editing, copying
- Supports PDF documents created with any PDF application

PDF Password Genius

Source: <http://www.isunshare.com>

PDF Password Genius is PDF file decryption software used to recover PDF document password and remove PDF open password. Supports all versions of PDF files created in Adobe Acrobat or other PDF software.

Features:

- Recovers PDF document open password effectively in few seconds
- Provides two versions to recover PDF password for people in different situations
- Enables removal of PDF restrictions on editing, coping, printing and more

SmartKeyPDF Password Recovery

Source: <http://www.recoverlostpassword.com>

SmartKey PDF Password Recovery tool recovers password-locked PDF documents created with all versions of Adobe Acrobat or any other PDF application. It decrypts PDF opening restriction by recovering user password, removes PDF copying, editing, and printing restrictions by recovering owner password.

Features:

- Recovers password to open PDF documents
- Removes restrictions on PDF copying, editing and printing
- Supports the latest Acrobat 10.0 (PDF 1.7)

Tenorshare PDF Password Recovery

Source: <http://www.tenorshare.com>

Tenorshare PDF Password Recovery tool cracks PDF passwords. The tool unlocks PDF password and disables restrictions on PDF printing, editing, and copying. It recovers the lost passwords for encrypted PDF files and recovers both PDF open password and owner password, making it free to use PDF files.

Guaranteed PDF Decrypter

Source: <http://www.quapdf.com>


Guaranteed PDF Decrypter removes restrictions of any secure PDF. Any Acrobat version up to X is supported, even with 256-bit AES or 128-bit RC4 encryption. It instantly removes PDF restrictions. The unlocked file can be opened in any PDF viewer without restrictions. Decryption of the file with password for opening is guaranteed for the documents with 40-bit key only.

Features:


- Removes restrictions in signed or certified files by digital signatures and in PDF forms
- Supports AES encryption, Unicode passwords, compressed files and unencrypted metadata

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>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

ZIP Password-Cracking Software

Accent ZIP Password Recovery

Source: <http://accentsoft.com>

Accent ZIP Password Recovery tool restores passwords to ZIP archives with support for both standard encryption and the hard-to-recover WinZip AES encryption (.zip and .zipx archives). It provides striking code optimization for Intel and AMD processors.

ZIP Password Genius

Source: <http://www.isunshare.com>

ZIP Password Genius is advanced and powerful zip password recovery software. It recovers ZIP/WinZip/7Zip archives that are lost or with forgotten password. It cracks *.zip files passwords easily.

Features:

- Supports all versions of ZIP, WINZIP, and 7ZIP archives
- Recovers zip password with ease and speed
- Stops and resumes zip password recovery process as you wish

Module 05 Page 548

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SmartKey ZIP Password Recovery

Source: <http://www.recoverlostpassword.com>

SmartKey ZIP Password Recovery tool is an easy, effective, and safe ZIP password cracker. It recovers password-protected plain and self-extracting ZIP archives created with all versions of popular archivers such as WinZip and PKZip.

Features:

- Speeds up ZIP password recovery with GPU acceleration
- Supports archives over 4 GB and self-extracting archives
- Works well with all versions of WinZIP/ZIP/PKZip archives
- Provides three efficient attack types to meet all your needs

KRyLack ZIP Password Recovery

Source: <http://www.krylack.com>

KRyLack ZIP Password Recovery tool recovers lost or forgotten passwords to ZIP (WinZIP) archives. The program can recover lost passwords on AES encrypted ZIP/ZIPX (WinZIP) archives. Self-extracting archives are supported by the application.

Features:

- Supports archives created by various software packages
- Extracts tool for ZIP, RAR, and ACE archives
- Enables custom character set for brute-force attack (non-English characters are supported)

Stellar Phoenix Zip Password Recovery

Source: <http://www.stellarinfo.com>

Stellar Phoenix Zip Password Recovery tool recovers lost or forgotten passwords of Zip files created using WinZip (Versions 8.x to 15.x).

Features:

- Recovers password set to archived files, such as ZIPX and ZIP
- Ensures 100% recovery with brute-force attack technique

RAR Cracking Software

Accent RAR Password Recovery

Source: <http://accentsoft.com>

Accent RAR Password Recovery tool restores passwords to RAR and WinRAR archives (RAR 3.x-5.x). The program uses highly optimized CPU code, ATI, and NVIDIA video cards to break RAR passwords. The search algorithm is optimized for all modern AMD and Intel processors.

Features:

- Provides standard and professional version for RAR file password recovery
- Supports all versions of WinRAR, RAR, or other archives software that can create RAR archive
- Recovers three and less characters of RAR password in trial version

cRARk 5.1

Source: <http://www.crark.net>

The password recovery tool, cRARk, works on RAR archives. It supports RAR/WinRar 2.x-5.x up to 5.0 versions. It is the tool for professionals; it uses command-line interface and has no GUI. In addition, cRARk is the freeware utility and supports Win32/64, Linux, and Mac OS OSs.

SmartKey RAR Password Recovery

Source: <http://www.recoverlostpassword.com>

SmartKey RAR Password Recovery is RAR password remover software that helps in finding passwords for encrypted WinRAR files. It holds three attack types that can easily crack RAR or WinRAR password.

Features:

- Assists in 100% RAR password cracker rate for all versions (include newest WinRAR 4.20)
- Provides three efficient attack options: brute-force, brute-force with mask, and dictionary attack
- Saves recovery process automatically and shuts down the computer automatically after recovery

KRyLack RAR Password Recovery


Source: <http://www.krylack.com>

KRyLack RAR Password Recovery tool recovers lost or forgotten passwords to RAR archives (including v3.x and v4.x, SFX, multi-volume and archives with encrypted filenames). The tool supports self-extracting archives.

Features:

- Supports RAR archives (All versions including v3.0 and v4.0) and multi-volume RAR archives
- Auto saves the password search state and resumes after a stop or a crash
- Does not limit the password length

Other Password Cracking Tools




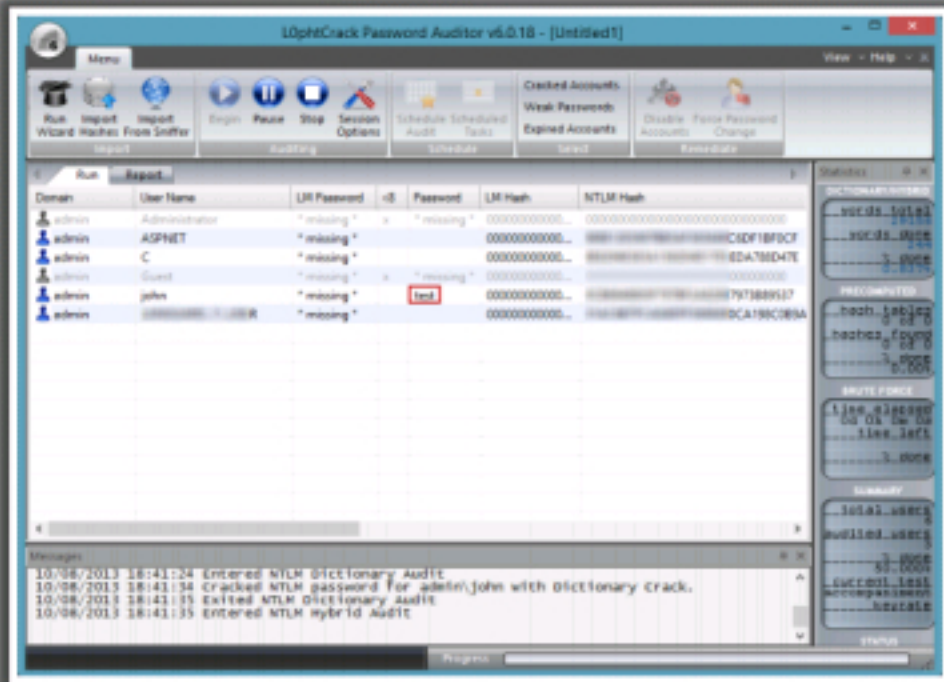
L0phtCrack

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

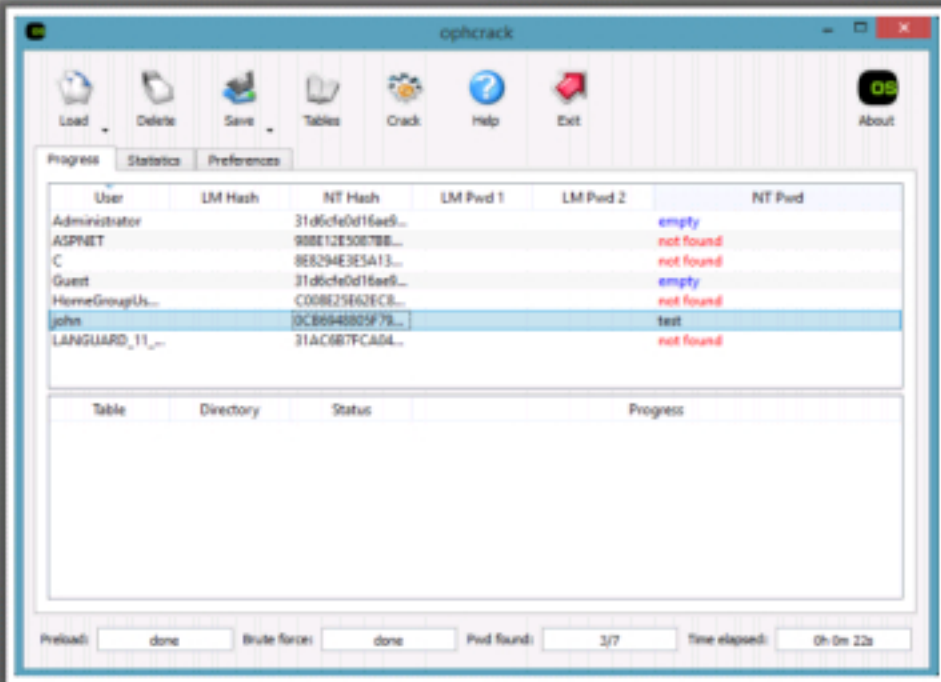
Ophcrack

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>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

L0phtCrack

Source: <http://www.l0phtcrack.com>

L0phtCrack is a password recovery or auditing application. It helps to recover lost Microsoft Windows passwords by using dictionary attacks, hybrid attacks, rainbow tables, and brute-force attacks.

Features:

- Supports pre-computed password hashes
- Imports and cracks Unix password files
- Imports passwords from remote Windows, including 64-bit versions of Vista, Windows 7, and Unix machines
- Enables users to schedule routine audits

Ophcrack

Source: <http://ophcrack.sourceforge.net>

Ophcrack is a Windows password cracker based on rainbow tables. It comes with a GUI and runs on multiple platforms.

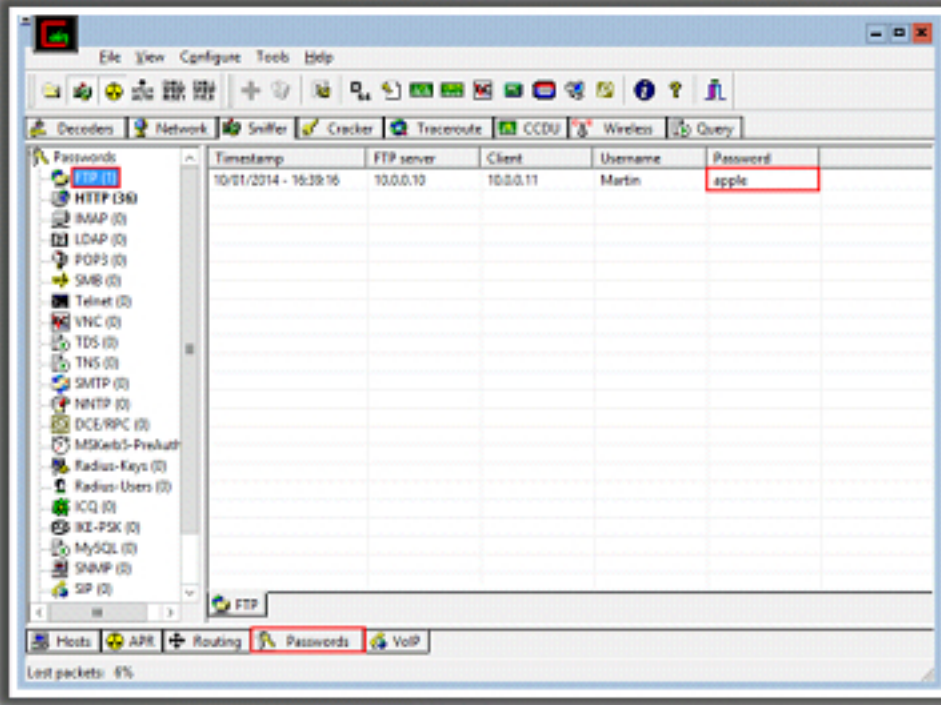
Features:

- Runs on Windows, Linux/Unix, Mac OS X, etc.
- Cracks LM and NTLM hashes
- Contains free tables for Windows XP and Vista/7
- Uses brute-force module for simple passwords
- Includes audit mode and CSV export
- Features real-time graphs to analyze the passwords
- Dumps and loads hashes from encrypted SAM recovered from a Windows partition

Other Password Cracking Tools (Cont'd)

Cain & Abel

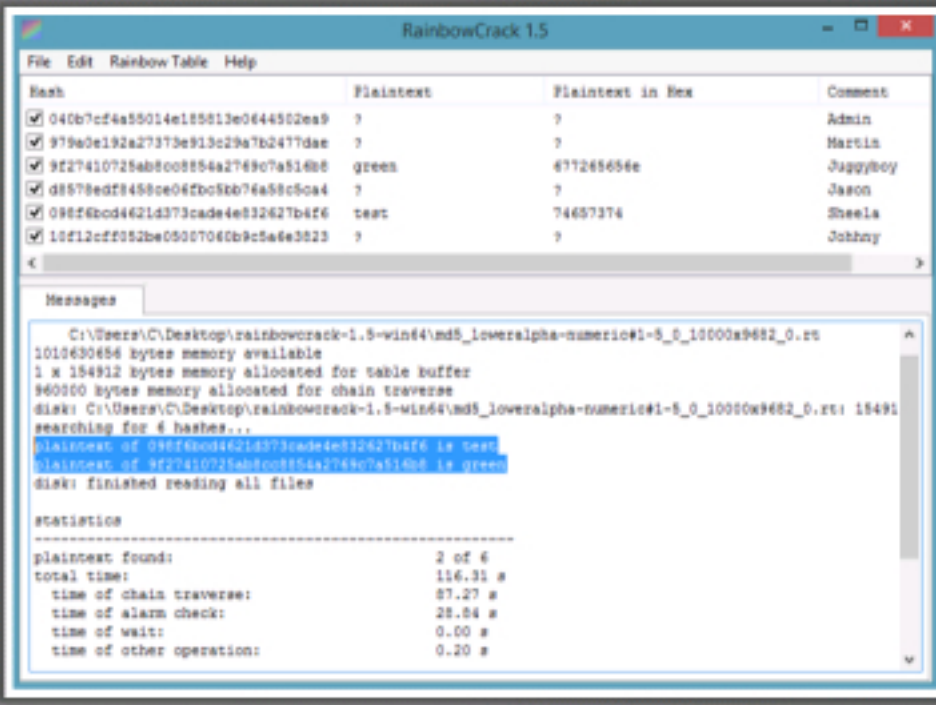
It allows recovery of various kind of passwords by **sniffing the network**, and **cracking encrypted passwords** using dictionary, brute-force, and cryptanalysis attacks



<http://www.oxid.it>

RainbowCrack

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



<http://project-rainbowcrack.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cain & Abel

Source: <http://www.oxid.it>

Cain & Abel is a password recovery tool for Microsoft OSs. It allows the recovery of passwords by sniffing the network, cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks. It covers some security aspects/weaknesses present in a protocol's standards, caching mechanisms, and authentication methods. This offers a simplified recovery of passwords and credentials from various sources.

It consists of an Arp Poison Routing (APR) that enables sniffing on switched LANs and man-in-the-middle attacks. The sniffer in this tool is also capable of analyzing encrypted protocols, such as HTTP and SSH-1, and contains filters to capture credentials from a wide range of authentication mechanisms.

Features:

- The program does not exploit any software vulnerabilities or bugs that could not be fixed with minimum effort
- It covers security aspects/weakness present in protocol's standards, authentication methods, and caching mechanisms

RainbowCrack

Source: <http://project-rainbowcrack.com>

RainbowCrack is a hash cracker. It uses a time-memory tradeoff algorithm to crack hashes. It pre-computes all possible plaintext–ciphertext pairs in advance and stores them in the “rainbow table” file. It may take a long time to pre-compute the table, but once the pre-computation is finished, hashes stored in the table can be cracked with much better performance than a brute-force cracker.

Features:

- Runs on Windows and Linux OSs
- Uses command line interface
- Supports rainbow table on any hash algorithm
- Supports rainbow table in raw file format (.rt) and compact file format (.rtc)

Other Password Cracking Tools
(Cont'd)

CHFI
Computer Hacking Forensic Investigator

pwdump7 and fgdump

pwdump7.exe

```
Administrator: Command Prompt
C:\Windows\system32>cd C:\Users\N\Desktop\pwdump7
C:\Users\N\Desktop\pwdump7>pwdump7
Pwdump v7.1 - raw password extractor
Author: Andree Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****:3136CF8D16AEF31E73C59D78C8H
90B:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:
C:\Users\N\Desktop\pwdump7>
```

<http://www.tarasco.org>

fgdump

```
Administrator: Command Prompt
C:\Users\N\Desktop\fgdump>fgdump 2.1.0 - example fgdump
fgdump 2.1.0 - fgdump and the mighty group at foofus.net
Written to make password life just a bit easier
Copyright(C) 2008 fgdump and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.

No parameters specified, doing a local dump. Specify -T if you are looking for
ftp.
-- Session ID: 2012-10-02-17-48-35 --
Starting dump on 127.0.0.1

** Beginning local dump **
OS (127.0.0.1): Microsoft Windows Unknown Professional (Build 9431) (64-bit)
Passwords dumped successfully
Cache dumped successfully

-- Summary --
Failed servers:
NONE
Successful servers:
127.0.0.1
```

<http://foofus.net>

Attacker

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

Dumps a remote machine
(192.168.0.10) using a specified
user
```

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

These tools must be run with administrator privileges

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

PWdump7

Source: <http://www.tarasco.org>


PWdump7 is an application that dumps the password hashes (OWFs) from NT's SAM database. It extracts LM and NTLM password hashes of local user accounts from the SAM database. This tool runs by extracting the binary SAM and system file from the file system and then extracts the hashes. One of the powerful features of PWdump7 is that it is also capable of dumping protected files. Use of this program requires administrative privileges on the remote system.


Fgdump


Source: <http://foofus.net>

Fgdump is basically a utility for dumping passwords on Windows NT/2000/XP/2003/Vista machines. It comes with an inbuilt functionality that has all the capabilities of PWdump and can also do a number of other crucial things, such as executing a remote executable, dumping the protected storage on a remote or local host, and grabbing cached credentials.


**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>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Offline NT Password & Registry Editor

Source: <http://pogostick.net>

Offline NT Password & Registry Editor is a utility to reset the password of any user that has a valid local account on the Windows system. It supports Windows from NT3.5 to Win8.1, 64 bit, and also the server versions (such as 2003, 2008, and 2012). It works offline, that is, the user has to shutdown his/her computer and boot off a CD or USB disk to do the password reset.

Password Unlocker Bundle

Source: www.passwordunlocker.com

Password Unlocker Bundle is a password-cracking tool that resets or recovers passwords for different file types such as Windows OS, MS SQL Servers, RAR/PDF/Word/Excel/PPT files. The tool supports brute-force and dictionary Attack. It can search for encrypted files.

Proactive System Password Recovery

Source: <http://www.elcomsoft.com>

Proactive System Password Recovery is a password recovery tool that is capable of retrieving the secure passwords using social engineering. It recovers passwords protecting office documents, ZIP, and RAR archives. Usually secure passwords require lengthy attacks to be recovered. The tool retrieves all instantly recoverable passwords and tries these passwords to unlock secure passwords.

Join the Ripper

Source: <http://www.openwall.com>

John the Ripper is a password recovery tool that cracks passwords and supports Unix, Windows, DOS, and OpenVMS. It detects weak Unix passwords, several crypt (3) password hash types most commonly found on various Unix systems, Windows LM hashes, etc.

Wfuzz

Source: <http://www.edge-security.com>

Wfuzz is a password-cracking tool designed to brute force Web applications. It can be used to find unlinked resources (directories, servlets, scripts, etc.), brute-force GET, and POST parameters for checking different kinds of injections (SQL, XSS, LDAP, etc.), brute-force parameters (user/password), fuzzing, etc.

Active@ Password Changer

Source: <http://www.password-changer.com>

Active@ Password Changer is a password recovery tool that has a simple user interface, supports multiple hard disk drives, detects several SAM databases (if multiple OS were installed on one volume), and provides the opportunity to pick the right SAM before starting the password recovery process.

Passware Kit Standard

Source: <https://www.passware.com>

Passware Kit Standard is an easy-to-use tool that recovers passwords for MS Office files, archives, PDF documents, Windows Administrators, email accounts, and other. It recovers or resets many password types instantly, uses advanced password recovery attacks such as dictionary, Xieve, brute-force, known password/part, previous passwords, and their combinations. It also includes a Wizard for easy setup of password recovery attacks.

Windows Password Unlocker

Source: <https://www.passwordunlocker.com>

Windows Password Unlocker resets Windows password on Windows 8/7/Vista/XP, and 2008/2003/2000 servers.

Features:

- Resets Windows local and domain password
- Creates new local and domain admin account
- Resets password with bootable CD/DVD/USB

LSASecretsView

Source: <http://www.nirsoft.net>

LSASecretsView is a small utility that displays a list of all LSA secrets stored in the Registry on a computer. The LSA secrets key is located under HKEY_LOCAL_MACHINE\Security\Policy\Secrets. It may contain VPN/RAS passwords, Autologon passwords, and other system keys/passwords. LSASecretsView just requires the user to copy the executable file (LSASecretsView.exe) to any of the folder and run it. The main window of LSASecretsView contains 2 panes: upper and lower panes. The upper pane displays the list of all LSA secret entries. When the user selects one or more items in the upper pane, the lower pane displays the LSA data of the selected items, in Hex and Ascii formats.











LCP

Source: <http://www.lcpsoft.com>

LCP audits user account passwords and recovers them in Windows NT/2000/XP/2003. It searches for attacks in the OS and fixes and recovers forgotten passwords. It allows .lcs files for password recovery.

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.windowpasswordsrecovery.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.recoverwindowpassword.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Password Cracker

Source: <http://www.amlpages.com>

Password Cracker is a tool used to restore forgotten passwords, including Internet Explorer.

Kon-Boot

Source: <http://www.thelead82.com>

Kon-Boot is a tool that recovers the passwords by bypassing the authentication process of Windows-based OSs. It can be used for tech repairs, data recovery, and security audits as well.

Windows Password Recovery Tool

Source: <http://www.windowpasswordsrecovery.com>

Windows Password Recovery Tool is a password recovery tool used to reset or restore the lost passwords for local and Microsoft accounts.

Hash Suite

Source: <http://hashsuite.openwall.net>

Hash Suite is a password recovery tool that recovers the lost password. The tool generates different candidate passwords (keys), hashes them, and compares the computed hashes with the stored hashes. The tool offers different ways to generate candidate passwords.

InsidePro

Source: <http://www.insidepro.com>

Insiderpro is a password recovery tool used to recover the lost passwords. It recovers passwords to hashes of all types. The tool automatically detects algorithm and finds hashes. The tool recovers passwords in Unicode.

Windows Password Recovery

Source: <http://www.passcape.com>

Windows Password Recovery is a network security analyzer and Windows password recovery tool. It implements patented password recovery technologies developed in Passcape Software, such as artificial intelligence or pass-phrase attack.

Password Recovery Bundle

Source: <http://www.top-password.com>

Password Recovery Bundle recovers lost or forgotten passwords. This tool recovers or resets passwords for Windows, PDF, ZIP, RAR, Office Word/Excel/PowerPoint documents. It also retrieves passwords for instant messengers, email clients, web browsers, FTP clients, and many other applications.

iSunshare Windows Password Genius

Source: <http://www.isunshare.com>

iSunshare Windows Password Genius is a Windows password recovery tool that helps recover forgotten Windows administrator/user password and domain administrator/user password for Windows OS, which includes Windows 10/8/7/Vista/XP/NT/2000 and Windows server 2000/2003/2008/2011/2012. The tool assists for Windows 8 Microsoft account password reset.

Features:

- Creates a new administrator account easily without logon
- Accesses to Windows system within a few minutes
- Provides four editions, Standard, Professional, Advanced, and RAID

THC-Hydra

Source: <https://www.thc.org>


THC-Hydra is a network logon cracker tool that uses dictionary or brute-force attacks to try various passwords and login combinations against a login page. This tool supports Linux, *BSD, Solaris, Mac OS X, and any Unix and Windows (Cygwin) OSs.

Windows Password Breaker Enterprise

Source: <http://www.recoverwindowpassword.com>

Windows Password Breaker is a Windows password reset tool that works for Windows 7/Vista/XP/2000 and server 2003(R2)/2008(R2). This tool allows to create a bootable password reset CD/DVD or USB flash drive to reset the lost Windows password. It resets Windows local administrator, standard user, and guest passwords on Win7/Vista/XP/2000.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Steganography, the art of hidden writing, has been in use for centuries. It involves embedding a hidden message in some transport or carrier medium and mathematicians, military personnel, and scientists have been using it. They all engage in changing the common language and transferring it through secret and hidden communication.

The history of steganography dates back to the Egyptian civilization. Today, with the emergence of the Internet and multimedia, the use of steganography is mostly digital in nature.

According to www.webopedia.com, steganography refers to “The art and science of hiding information by embedding messages within other, seemingly harmless messages. It works by replacing bits of useless or unused data in regular computer files with bits of different, invisible information.”

In general, forensic investigators should look out steganography across evidences that do not support encryption. When it is not possible to encrypt a file, the next best option for safe transfer used by the intruders is steganography. The best way to protect sensitive information is to camouflage it, instead of encrypting it. It is basically a supplement or alternative for encryption. However, an encrypted file can still hide information by using steganography. This way, there would be a double measure of protection, as the encrypted file, once deciphered, would not allow the hidden message to be seen. One has to use special steganography software to decipher the hidden message. Many websites allow people to download steganography software; they can be freeware or trial software. Usually, steganography involves messages that are out in the open for many people to view. This can go unnoticed, as

the very existence of the message is secret. Steganographic messages or images are essentially “hidden in plain sight,” unlike cryptographic messages.

In cryptography, the users cannot read the message as it is in the jumbled form. Therefore, it is correct to state that the investigators know the existence of the message. This also protects the information that is present in the cipher. When the investigator intercepts an encrypted message, it is quite damaging as it informs the enemy about its two-way communication. Steganography takes the exact opposite approach, as the uninformed user have no idea that there is communication going on.

How Steganography Works

Following are the steps representing the steganography work process:

- **Step 1:** Alice (sender) embeds the secret message into the cover message (original message).
- **Step 2:** Stego message (message containing secret message) is sent via secured channel to Bob (receiver).
- **Step 3:** Bob receives the stego message.
- **Step 4:** Bob decodes the stego message through a key.
- **Step 5:** Willie (third person) who observes the communication process between Alice and Bob thinks that the message sent is a normal message.

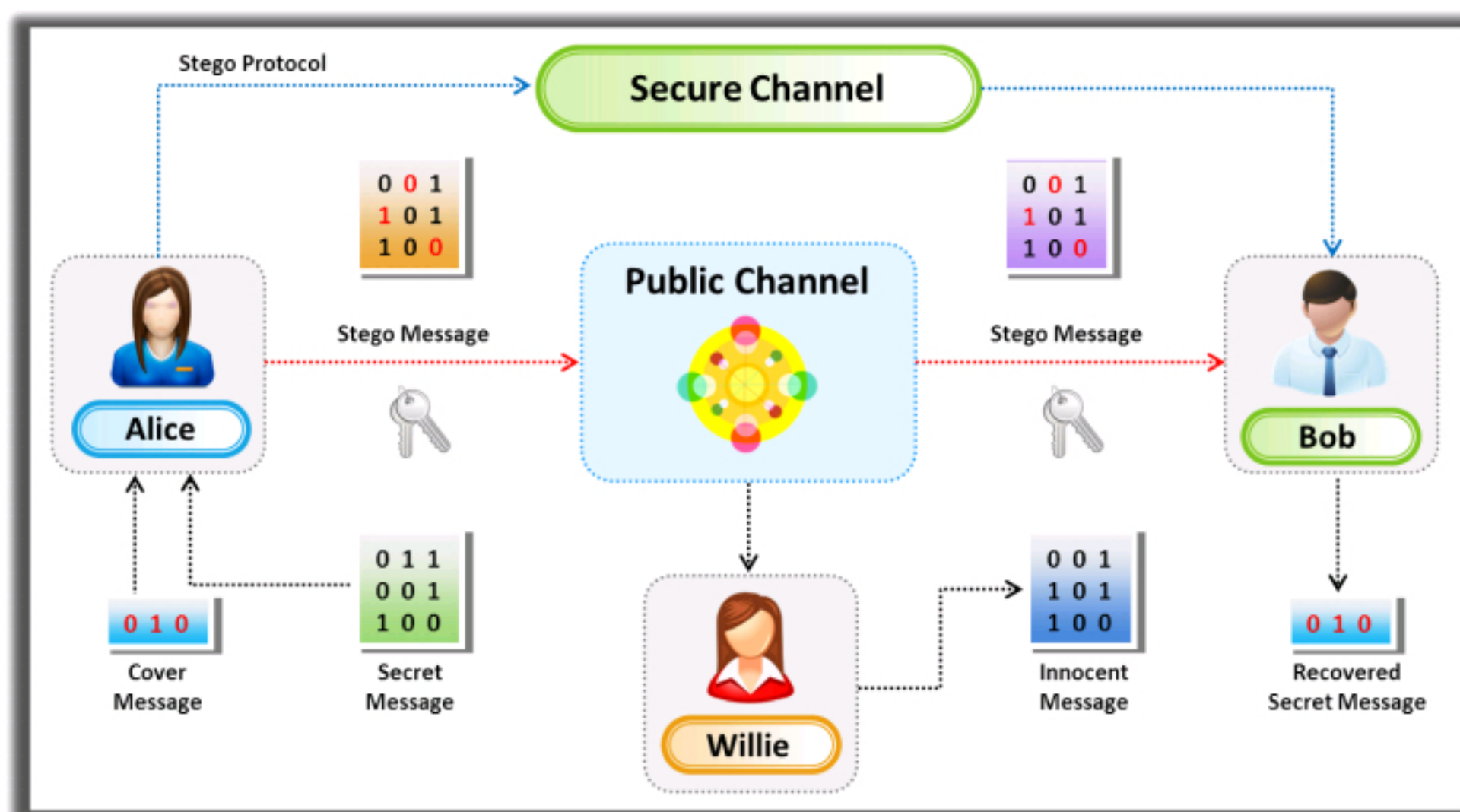
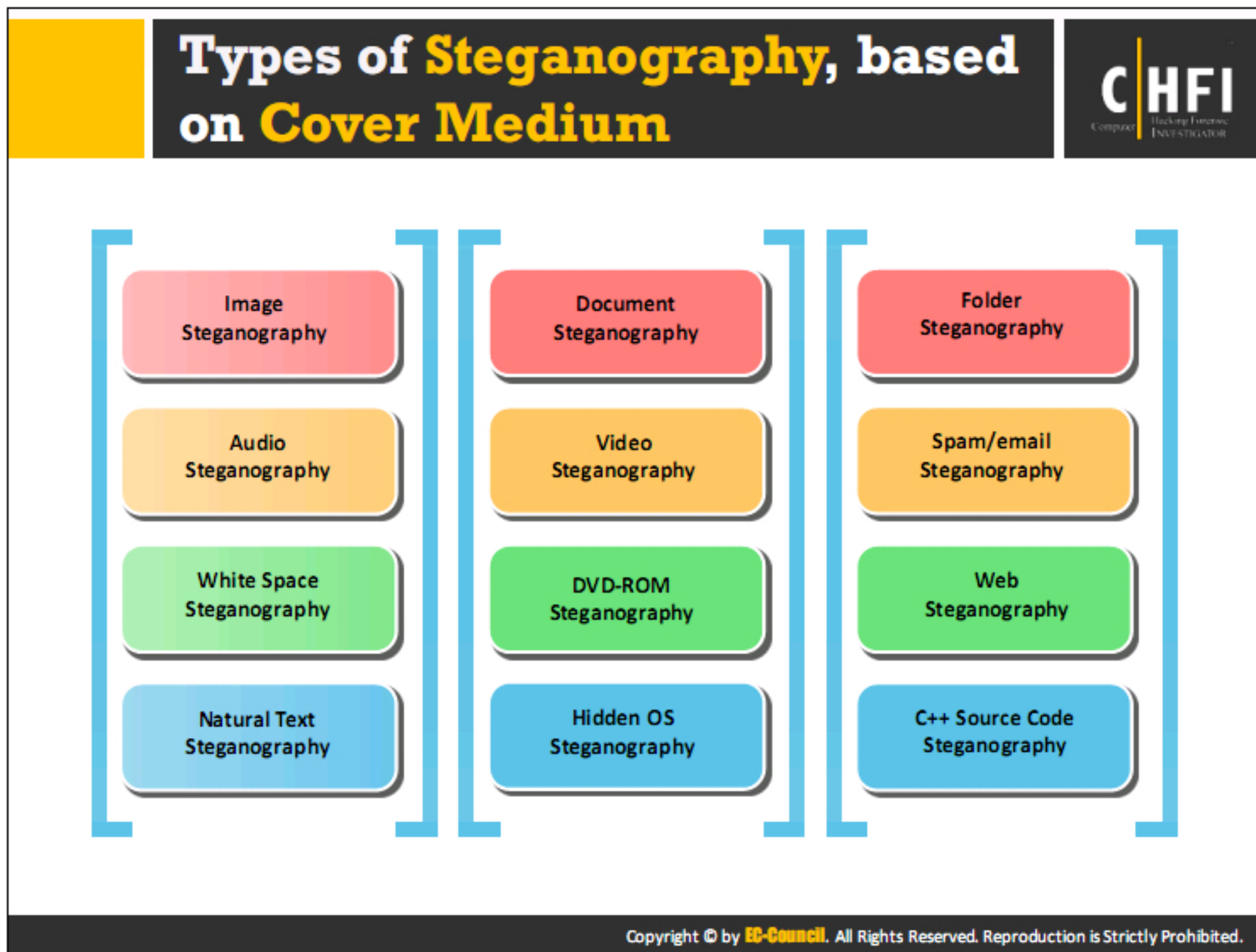


FIGURE 5.6: Steganography Process




Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the existence of the message. The increasing use of electronic file formats and new technologies has made data hiding more and more possible. Basic steganography can be broken down into two areas: data hiding and document making. Document making deals with protection against removal. It is further classified into watermarking and fingerprinting.

The different types of steganography are as follows:

- **Image Steganography:** Images are the popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats such as .png, .jpg, .bmp, etc.
- **Document steganography:** In the document steganography, user adds white spaces and tabs at the end of the lines.
- **Folder Steganography:** Folder steganography refers to hiding one or more files in a folder. In this process, user moves the file physically but still keeps the associated files in its original folder for recovery.
- **Video Steganography:** Video steganography is a technique to hide files with any extension into a carrying video file. One can apply video steganography to different formats of files such as .avi, .mpg4, .wmv, etc.
- **Audio Steganography:** In audio steganography, user embeds the hidden messages in digital sound format.





- **Whitespace Steganography:** In the white space steganography, user hides the messages in ASCII text by adding white spaces to the end of the lines.
- **Web Steganography:** In the web steganography, a user hides web objects behind other objects and uploads them to a webserver.
- **Spam/Email Steganography:** One can use spam emails for secret communication by embedding the secret messages in some way and hiding the embedded data in the spam emails. This technique refers to Spam/Email steganography.
- **DVDROM Steganography:** In the DVDROM steganography, user embeds the content in audio and graphical mode.
- **Natural Text Steganography:** Natural text steganography is converting the sensitive information into a user-definable free speech such as a play.
- **Hidden OS Steganography:** Hidden OS Steganography is the process of hiding one operation system into other.
- **C++ Source Code Steganography:** In the C++ source code steganography, user hides a set of tools in the files.

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	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Steganalysis is the process of discovering the existence of the hidden information within a cover medium. Steganalysis is the reverse process of steganography. It is one of the attacks on information security in which an attacker, called steganalyst, tries to detect the hidden messages embedded in images, text, audio, and video carrier mediums using steganography. It determines the encoded hidden message, and if possible, it recovers that message. It can detect the message by looking at variances between bit patterns and unusually large file sizes.

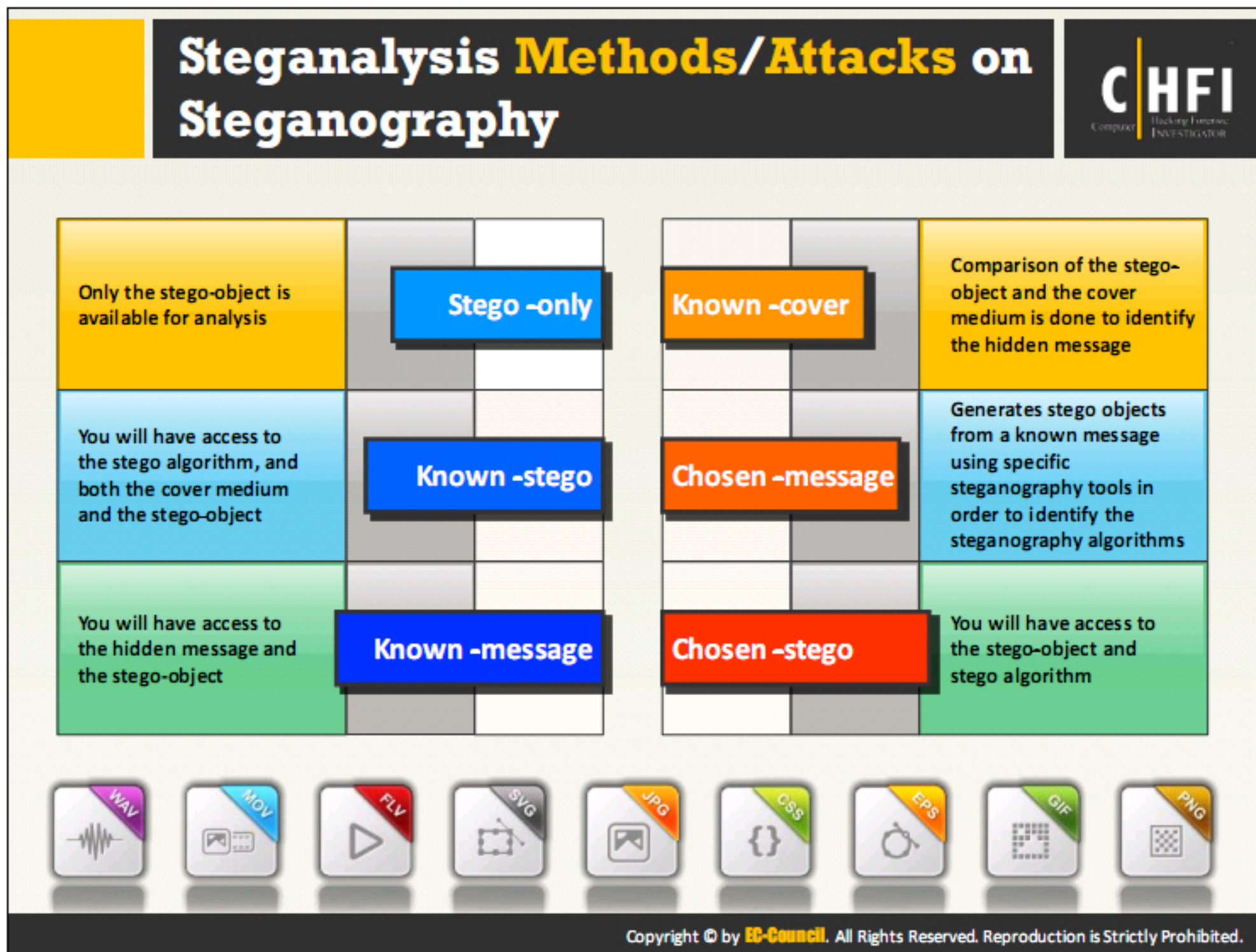
Steganalysis contains two aspects: the detection and distortion of messages. In the detection phase, the analyst observes the relationships between the steganography tools, stego-media, cover, and message. In the distortion phase, the analyst either manipulates the stego-media to extract the embedded message or removes it altogether.

The first step in steganalysis is to discover a suspicious image that may be harboring a message. This is an attack on the hidden information. There are two other types of attack against steganography: message and chosen-message attacks. In the former, the steganalyst has a known hidden message in the corresponding stego-image. The steganalyst determines patterns that arise from hiding the message and detecting this message. The steganalyst creates a message using a known stego tool and analyzes the differences in patterns. In a chosen-message attack, the attacker creates steganography media using the known message and steganography tool (or algorithm).

Cover images disclose more visual clues than stego-images. It is necessary to analyze the stego-images to identify the concealed information. The gap between cover image and stego-image

file size is the simplest signature. Many signatures are evident using some of the color schemes of the cover image.

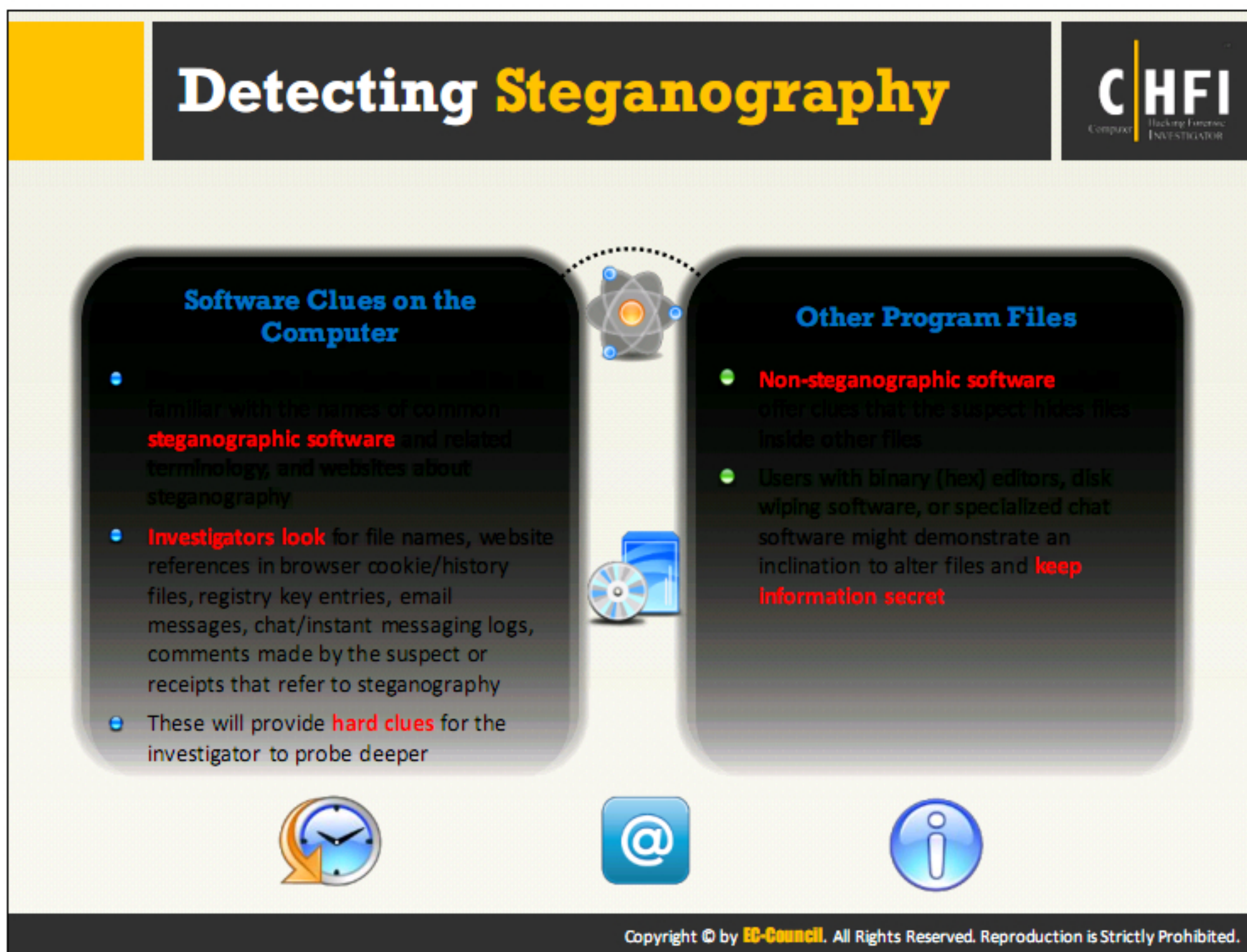
Once detected, an attacker can destroy a stego-image or modify the hidden messages. It is very important to understand the overall structure of the technology and methods to detect the hidden information for uncovering the activities.



Steganographic attacks work according to the type of information available to perform steganalysis. This information may include the hidden message, carrier (cover) medium, stego-object, steganography tools, or algorithms used to hide information. Thus, steganalysis is classified into six types: stego-only, known-stego, known-message, known-cover, chosen-message, and chosen-stego.

- **Stego-only attack:** In a stego-only attack, the steganalyst or the attacker does not have access to any information except the stego-medium or stego-object. In this attack, the steganalyst needs to try every possible steganography algorithms and related attacks to recover the hidden information.
- **Known-stego attack:** This attack allows attacker to know the steganographic algorithm as well as original and stego-object. The attacker can extract the hidden information with the information at hand.
- **Known-message attack:** The known-message attack presumes that the message and the stego-medium are available. Using this attack, one can detect the technique used to hide the message.
- **Known-cover attack:** Attackers use the known-cover attack when they have knowledge of both the stego-object and the original cover-medium. This will enable a comparison between both the mediums in order to detect the changes in the format of the medium and find the hidden message.

- **Chosen-message attack:** The steganalyst uses known message to generate a stego-object by using some steganography tool in order to find the steganography algorithm used to hide the information. The goal in this attack is to determine patterns in the stego-object that may point to the use of specific steganography tools or algorithms.
- **Chosen-stego attack:** The chosen-stego attack takes place when the steganalyst knows both the stego-object and steganographic tool or algorithm used to hide the message.



Software Clues on the Computer


During investigation, the investigators should first look at files, documents, software applications, and other suspicious files for clues hidden through steganography. Steganography investigators should also know about common steganographic techniques, software, tools, terminologies, and websites. This knowledge will help the investigators to find the process, software, and techniques used in steganography.

The investigators should find out the file names and web sites that the suspect used, by looking in the browser's cookies, history, registry key entries, mailbox, chat or instant messaging logs, and communication from or comments made. Because this data is important for investigation, it gives clues to the investigator for further procedures.

Other Program Files



It is necessary to check other program files, because the non-steganographic programs may contain clues about the covering file and hidden file. The investigators should check other softwares such as the binary (hex) editor, disk-wiping software, chat software used for changing the data from one code to another, and to keep the data secret from others.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Multimedia Files

Investigators should look for large files in the system, because large files can act as carrier files for steganography. Though a Windows computer consists of a number of graphic and audio files, they all are small in size. If the system consists of large files in abundance, the investigators can suspect these files to be carrier files with large sizes. This can be true if the computer system has many duplicate files.


Type of Crime

Already investigated crimes may also make an investigator to think about steganography. Child pornographers use steganography to hide pornographic material when they are posting it on a web site or sending it via email. Crimes related to business records also use steganography. Though a perpetrator can hide important record files by using steganographic techniques, others can obtain access to those files. Such crimes include identity theft, gambling, smuggling, and terrorism.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Text Files

For text files, the attackers alter the character position for hiding the data. One can detect these alterations by looking for text patterns or disturbances, the language used, line height, and unusual number of blank spaces.

A simple word processor can sometimes reveal the text steganography as it displays the spaces, tabs, and other characters that distort the text's presentation during text steganography. By having a closer look at following things, you can detect text steganography:

- Unusual patterns used in stego-object
- Appended extra spaces
- Invisible characters

Image Files


To detect the information hidden in the image, investigators should determine the changes in size, file format, last modified, last modified time stamp, and color palette of the file. The following points can help to detect image steganography:

- Too many display distortions in images
- Sometimes images may become grossly degraded

- Detection of anomalies through evaluating too many original images and stego-images with respect to color composition, luminance, pixel relationships, etc.
- Exaggerated “noise”


Statistical analysis methods help to scan an image for steganography. Whenever a secret message is inserted into an image, least significant bits (LSBs) will no longer be random. With encrypted data that has high entropy, the LSB of the cover will not contain the information about the original and is more or less random. By using statistical analysis on the LSB, the difference between random and real values can be identified.

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**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Audio File


Audio steganography is a process of embedding confidential information such as private documents and files in digital sound. The following are the main categories of audio steganography: LSB coding, echo coding, phase coding, and spread spectrum coding. These methods have different implementation techniques, bandwidths, and hiding standard.

Investigators can use the LSB modification technique to detect the audio steganographic files. Investigators scan for high and inaudible frequencies for information and distortions or patterns that help in detecting a secret message and try to find the differences in pitch, echo, or background noises.

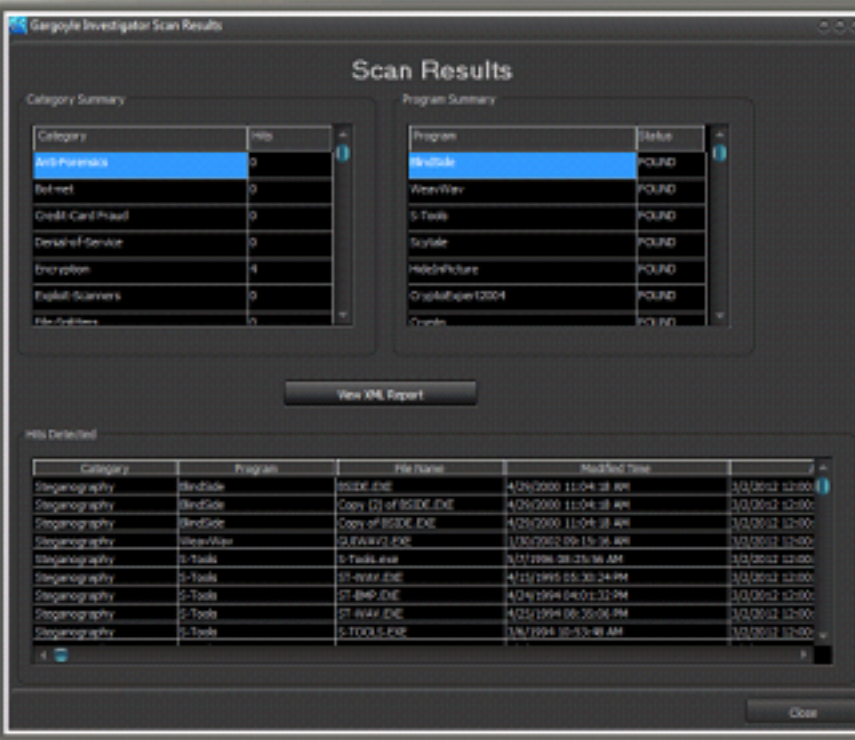
Video File

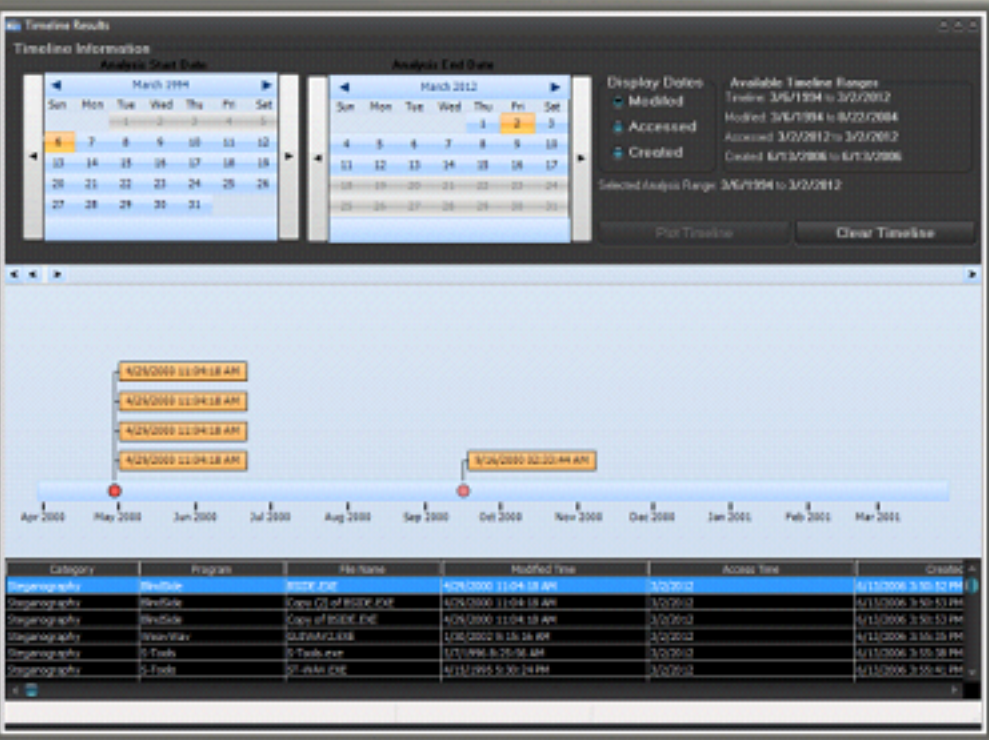
Detection of the secret data in video files includes a combination of methods used in image and audio files. Special code signs and gestures help in detecting secret data. Most methods used to detect steganography in videos require human involvement as the machines cannot effectively detect the differences.

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>

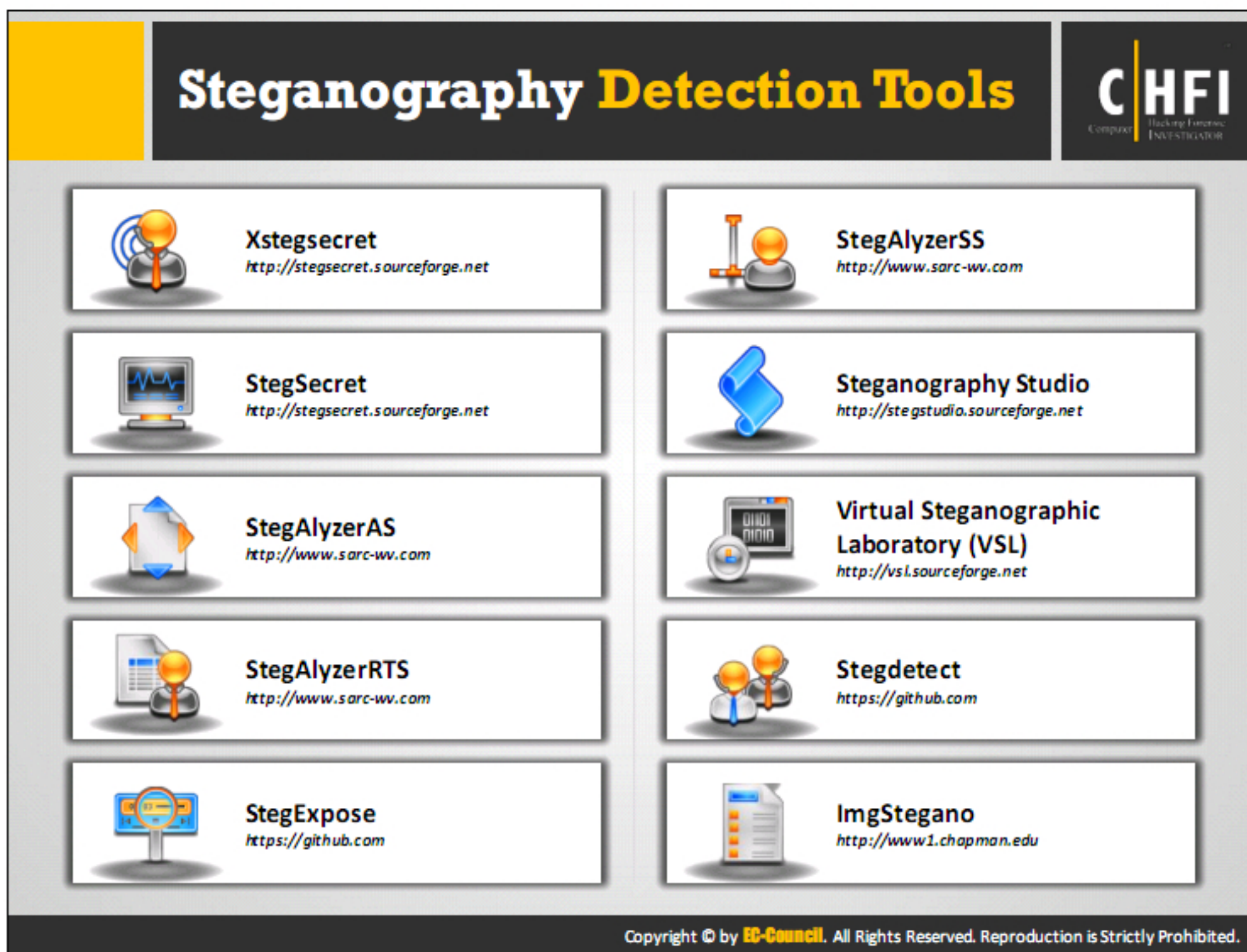
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Gargoyle Investigator Forensic Pro is a tool that conducts quick searches on a given computer or machine for known contraband and malicious programs. This tool finds remnants in a removed program as it conducts the search for the individual files associated with a particular program. Its signature contains botnets, Trojans, steganography, encryption, and keyloggers. It helps in detecting stego files created by using BlindSide, WeavWav, and S-Tools. It has the ability to perform a scan on a stand-alone computer or network resources for known malicious programs and the ability to scan within archived files.

Features:

- It scans on a stand-alone system or network resource for known contraband and hostile programs
- It comprises 20 datasets containing over 20,000 types of malicious software
- It is interoperable with popular forensic tools such as EnCase™
- It provides detailed forensic evidence reports with secure source time stamping, XML based and customizable

Source: <http://www.wetstonetech.com>



Xstegsecret

Source: <http://stegsecret.sourceforge.net>

Xstegsecret is a steganalysis software that detects hidden information from various digital media sources. It is a java-based multiplatform steganalysis tool used to detect EOF, LSB, DCTs, etc.

StegSecret

Source: <http://stegsecret.sourceforge.net>

Stegsecret is an open source (GNU/GPL) steganalysis tool that detects hidden information in different digital media. It is a java-based multiplatform steganalysis tool that detects hidden information using EOF, LSB, DCTs, etc.

StegAlyzerAS

Source: <http://www.sarc-wv.com>

StegAlyzerAS is a digital forensic tool. It identifies files and registry keys associated with steganography applications. StegAlyzerAS allows for identification of files by using CRC-32, MD5, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 hash values stored in the Steganography Application Fingerprint Database (SAFDB).

StegAlyzerRTS

Source: <http://www.sarc-wv.com>

StegAlyzerRTS is a network security application to detect digital steganographic applications and the use of those applications in real time.

StegAlyzerRTS detects insiders downloading steganographic applications by comparing the file fingerprints, or hash values, to a database of known file or artifact hash values associated with over 960 steganography applications.

StegExpose

Source: <https://github.com>

StegExpose is a steganalysis tool specialized in detecting LSB steganography in lossless images such as PNG and BMP. It has a command line interface and is designed to analyze images in bulk while providing reporting capabilities and customization, which is comprehensible for non-forensic experts.

StegAlyzerSS

Source: <http://www.sarc-wv.com>

StegAlyzerSS is a steganalysis tool designed to extend the scope of traditional computerized forensic examinations by allowing the examiner to scan suspect media or forensic images of suspect media for over 55 uniquely identifiable byte patterns, known as signatures, left inside files when particular steganographic applications are used to embed hidden information within them.

Steganography Studio

Source: <http://stegstudio.sourceforge.net>

Steganography Studio software can be used to learn, use, and analyze key steganographic algorithms. It implements several algorithms highly configurable with a variety of filters. It also implements the best image analysis algorithms for the detection of hidden information.

Virtual Steganographic Laboratory (VSL)

Source: <http://vsl.sourceforge.net>

Virtual Steganographic Laboratory (VSL) application helps in hiding data in digital images, detect its presence, and test its robustness using any number of different adjustable techniques. It provides a framework to use multiple methods at the same time. It can perform complex processing in both batch and parallel form.

Stegdetect

Source: <http://www.outguess.org>

Stegdetect is an automated tool to detect steganographic content in images. It is capable of detecting several different steganographic methods to embed hidden information in JPEG images. Given a set of normal images and a set of images that contain hidden content by a new steganographic application, Stegdetect can automatically determine a linear detection function that is applicable to yet unclassified images.

ImgStegano

Source: <http://www1.chapman.edu>

ImgStegano helps in the detection of steganography on .bmp or .png image. It uses an enhanced LSB technique to detect image steganography.

Anti-Forensics Techniques: Data Hiding in File System Structures

CHFI
Computer Hacking Forensic Investigator

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Data hiding is one of the anti-forensic techniques employed by attackers to make data inaccessible. NTFS-based hard disks contain bad clusters in a metadata file as \$BadClus and the MFT entry 8 represents these bad clusters. \$BadClus is a sparse file, which allows attackers to hide unlimited data as well as allocate more clusters to \$BadClus to hide more data.

Some hard disks have the host protected area (HPA), in which the developers can store data they want to protect (and hidden) from normal use. In addition to the above technique, the attackers use DPAs, DCOs, and slack spaces to hide the data, which will not visible to by either BIOS or OS and requires few special tools to view.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Trail Obfuscation is one of the anti-forensic technique that attackers use to mislead, divert, complicate, disorient, sidetrack, and/or distract the forensic examination process. The process involves different techniques and tools, such as

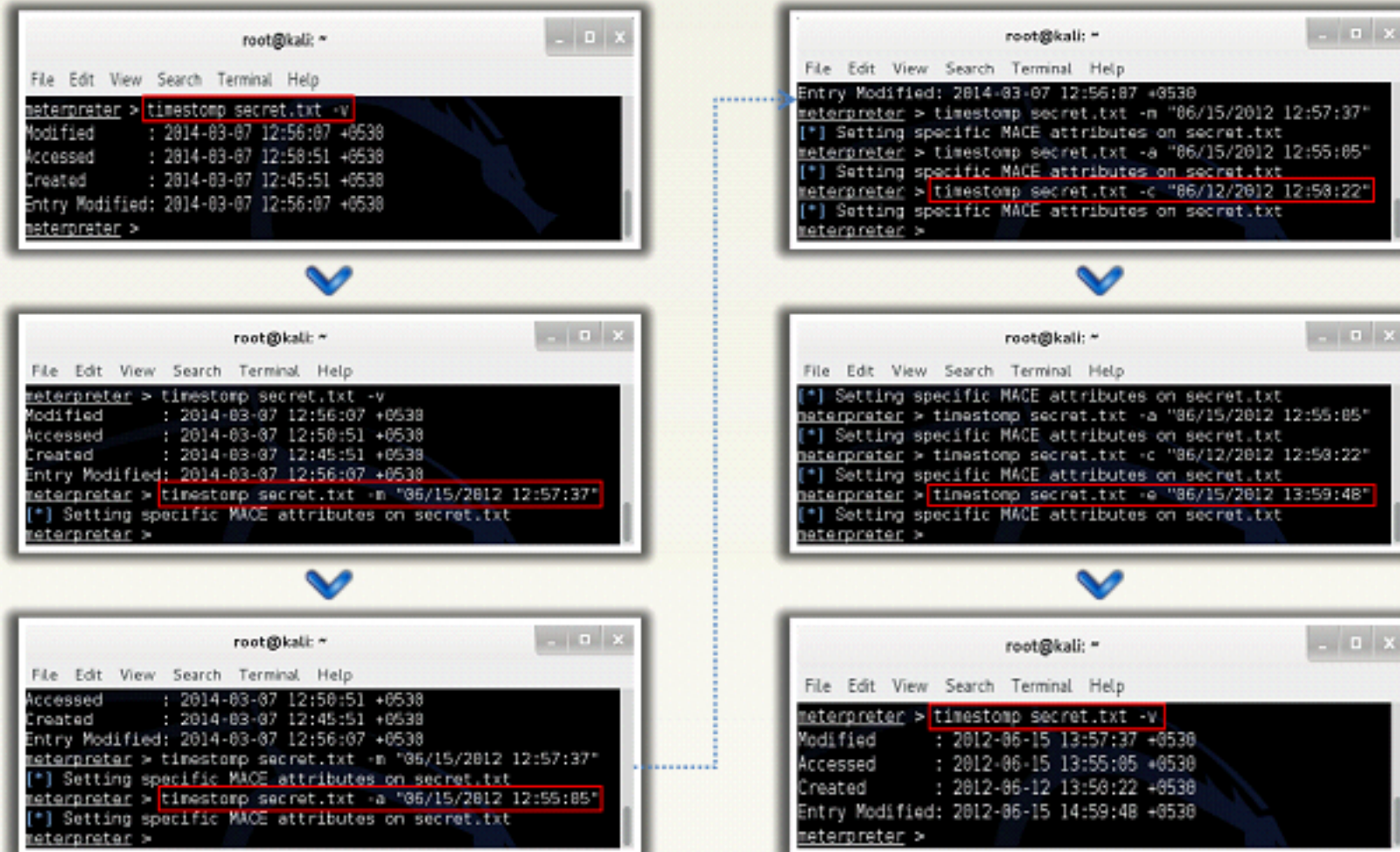
- Log cleaners
- Spoofing
- Misinformation
- Backbone hopping
- Zombie accounts
- Trojan commands

In this process, the attackers delete or modify metadata of some important files in order to confuse the investigators. They modify header information and file extensions using various tools. Timestomp, which is part of the Metasploit Framework, is one of the trail obfuscation tool that attackers use to modify, edit, and delete the date and time of a metadata and make it useless for the investigators. Transmogrify is another tool used to perform trail obfuscation.

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




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Using the Timestomp application, one can change the modified date and time stamp completely, thereby invalidating the validity of the document and misleading the investigation process.

This slide depicts step-by-step process of how the Timestomp application helps users to change the date and time of a file.

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>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Artifact Wiping refers to the process of deleting or destroying the evidence files permanently using various tools and techniques, such as disk-cleaning utilities file-wiping utilities and disk degaussing/destruction techniques. The attacker permanently eliminates particular files or the file systems.


Disk-cleaning utilities


The attackers use the tools that can overwrite the data on disks through various methods. However, these tools are not completely effective as they leave footprints. Some of the commonly used disk-cleaning utilities include Piriform, CCleaner, BCWipe Total WipeOut, Active@ KillDisk, CyberScrub's cyberCide, DriveScrubber, ShredIt, Secure Erase, etc.

File-wiping utilities

These utilities delete the individual files from an OS in a short span and leave a much smaller signature when compared with the disk-cleaning utilities. However, some experts believe that many of these tools are not effective, as they do not accurately or completely wipe out the data and also require user involvement. The commonly used file-wiping utilities are BCWipe, R-Wipe & Clean, Eraser, CyberScrubs PrivacySuite, etc.

**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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Disk degaussing and destruction techniques

Degaussing process is a technique in which attackers apply a magnetic field to a digital media device to entirely clean the previously stored data. It is an expensive technique and needs specialized equipment. Most attackers commonly depend on physical destruction of the device to destroy the evidence. Methods include disintegration, incineration, pulverizing, shredding, and melting.

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Encryption is the process of translating the data into a secret code so that only the authorized personnel can access it. It is an effective way to secure the data. To read the encrypted file, users require a secret key or a password that can decrypt the file. Therefore, most attackers use encryption technique as one of the best anti-forensic technique.

Data encryption is one of the commonly used techniques to defeat forensic investigation process and also involves encryption of codes, files, folders, and sometimes complete hard disks. Intruders use strong encryption algorithms to encrypt data of investigative value, which renders it virtually unreadable without the designated key. Some algorithms are capable of averting the investigation processes by performing additional functions including use of a key file, full-volume encryption, and plausible deniability.

Following are the 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

The encryption is easily available with various software applications and offers ease in usage, which adds to the difficulty in investigating the encryption process. VeraCrypt is one of the most widely used tools for anti-forensic 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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



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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

EFS on Microsoft Windows is a component of the NTFS file system of Windows 2000 and later versions. EFS provides file system-level encryption that enables transparent encryption and decryption of the files by using advanced, standard cryptographic algorithms, through which the manual access to any data on the computer is restricted to an outsider.

Another important feature of the EFS is the recovery certificate. This feature is very useful in cases where an organization needs to recover data of damaged or lost encryption key or when an employee is no more or dismissed from services, or moves to a different company without notice. Using the recovery certificate, forensic investigators can still recover the EFS-encrypted files.

Note: You must log in as an administrator to perform the steps given below. In addition, the given steps are not applicable to Windows 7 (Starter, Home basic, and Home Premium).

Following are the steps involved to create, install, and update a recovery certificate:

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 **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 then press **Enter**

Note: If prompted for an administrator password or confirmation, type the password or provide confirmation

Install the recovery certificate

- Insert the removable media that contains the recovery certificate
- In the **Search** box, type **secpol.msc**, and then 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 then 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**.

Update previously encrypted files with the 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 update 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>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Advanced EFS Data Recovery tool decrypts the protected files and works on all versions of Windows 2000, XP, 2003, Vista, Windows 7, 8, 8.1, and Windows Server 2008 and 2012. Recovery of the data is still possible even when the system is damaged, is not bootable, or when some encryption keys have been tampered with.


Advanced EFS Data Recovery tool recovers EFS-encrypted data that becomes inaccessible because of the system administration errors such as removing users and user profiles, misconfiguring data recovery authorities, transferring users between domains, or moving hard disks to a different PC.

This tool also helps to recover EFS-encrypted files under the following 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, corrupted file system, unbootable OS
- Reinstalled Windows or computer upgrades
- Formatted system partitions with encrypted files left on another disk

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


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Attackers use the encrypted network protocols to protect the identification of the network traffic as well as its content from forensic examination. Few cryptographic encapsulation protocols such as SSL and SSH can only protect the content of the traffic. However, to protect against the traffic analysis, attackers should also anonymize themselves whenever possible.


Attackers use virtual routers such as, the Onion routing approach, which provides multiple layers of protection. Onion routing is the technique used for secret communication over a computer network. This network encapsulates messages in layers of encryption, similar to the layers of an onion and employs a worldwide volunteer network of routers that serve to anonymize the source and destination of communications. Therefore, tracing this type of communication and attributing it to a particular source is very difficult for investigators.


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**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

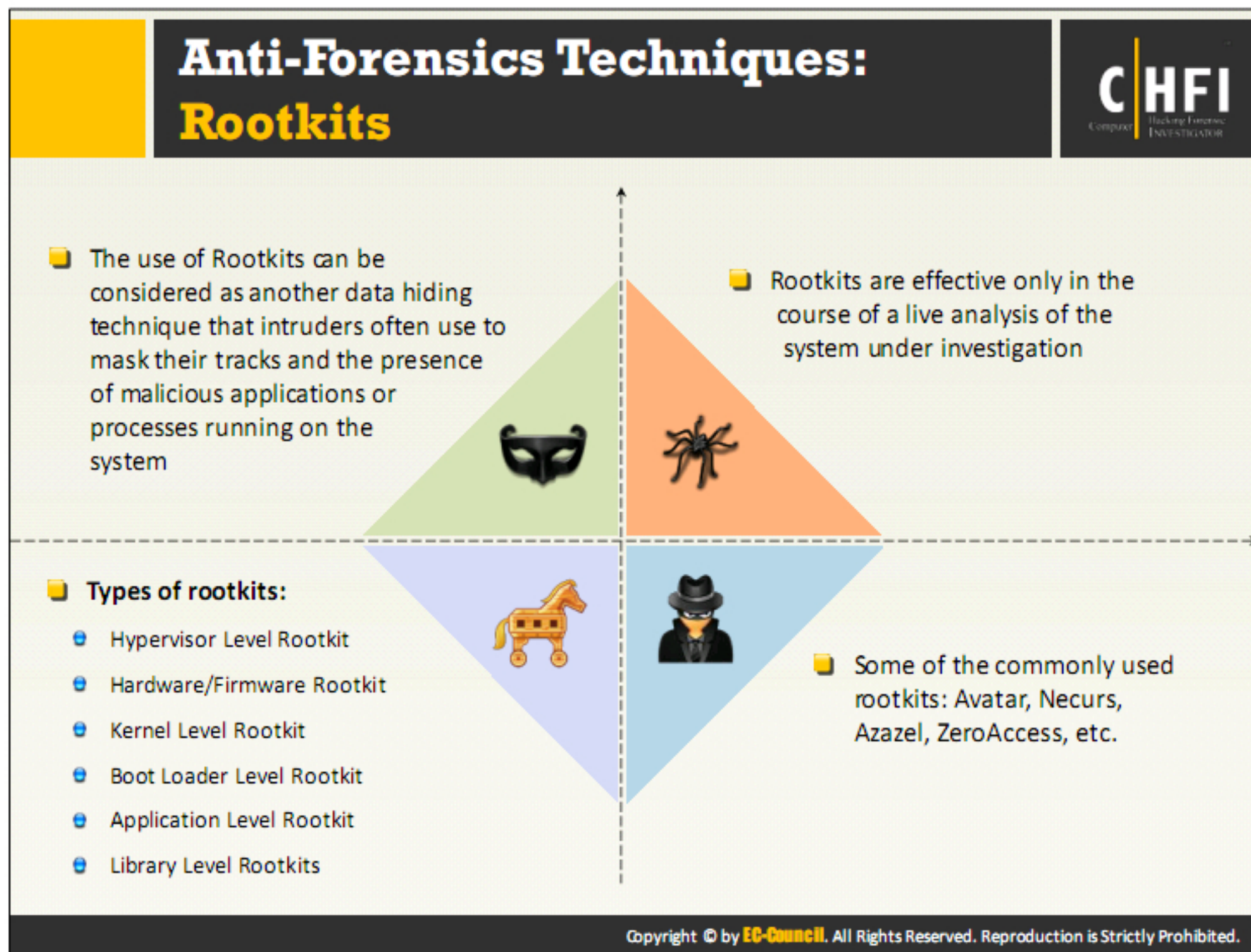
Program packers are one of the anti-forensic techniques attackers use to hide their data. The technique is similar to cryptography. The packers compress the files using various methods called algorithms. There are many different algorithms and unless the investigators know the one used to pack and have a tool to unpack it, they will not be able to access the file.

Using this technique the attacker can hide the evidence files into containers making the files hard to detect. Therefore, during forensic investigations, the investigator's first approach should be to mount compound files.

Packers can also include active protection against debugging or reverse engineering techniques. The packed programs those need a password in order to run are equally strong as encryption. Packed programs are also susceptible to static analysis if no password is required.

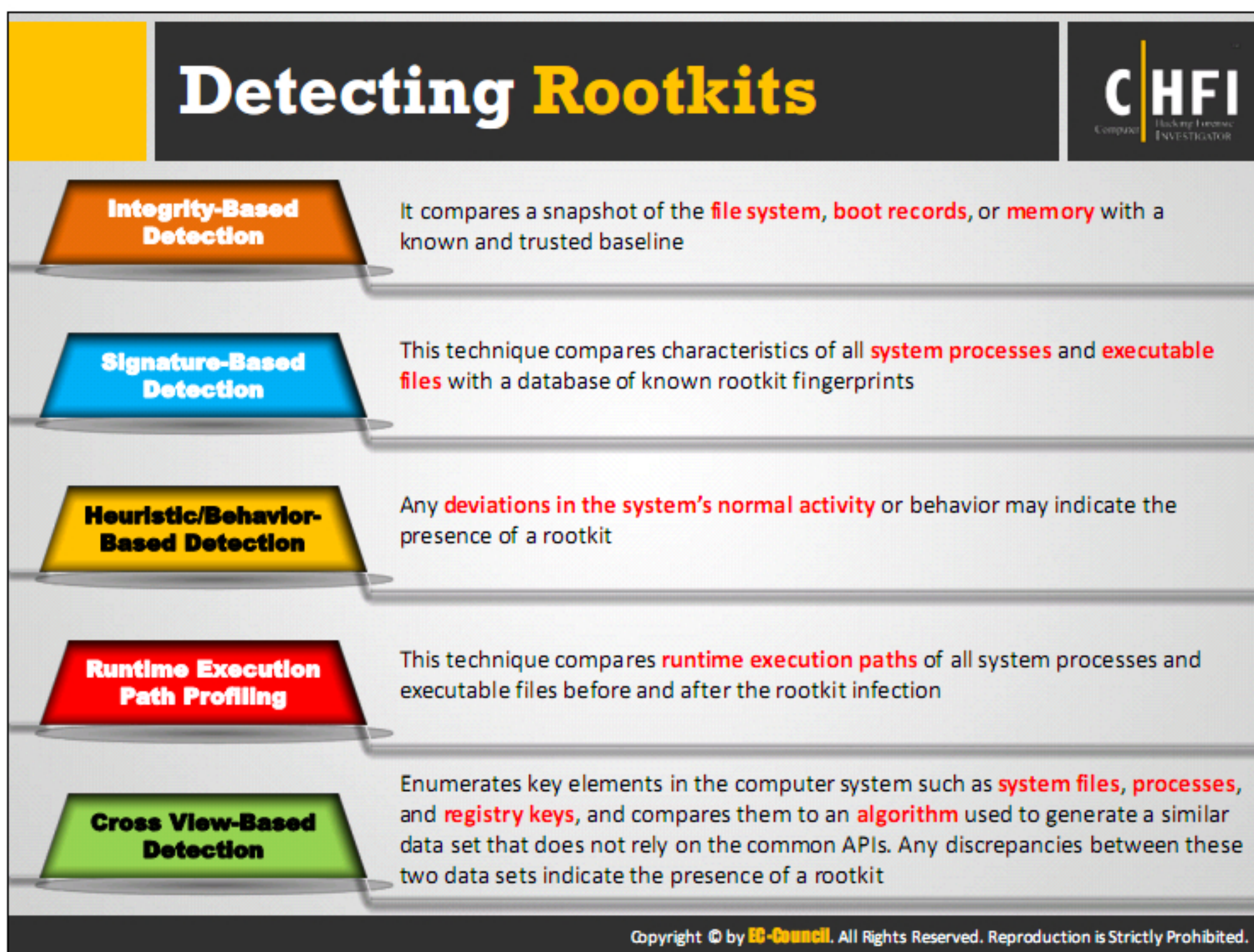
Intruders use packers to hide attack tools from detection by reverse-engineering or scanning. Packers can carry executable files, malware, and other attack elements. In case of executable files, these programs carry the unpackers built into them as well, which unpack the file when user tries to run it and installs the executable on the host system. Some of the widely used packers are UPX, PECompact, BurnEye, Exe Stealth Packer, Smart Packer Pro, etc. The investigators can dynamically analyze these types of packed executables by running them in a controlled environment and observing their behavior.

Packed programs that require a password to run are strong, whereas, the one's that do not require a password are vulnerable to static analysis.



Rootkits are one of the anti-forensic techniques that attackers use to hide data, malicious files, and processes. This software is intended to hide processes that could reveal an attack from the OS itself. Rootkits allow viruses and malware to “hide in plain sight” by concealing files in ways that antivirus software might overlook them, disguising files as legitimate system files, through unlinking processes, and even hiding from detection by the OS.

Rootkits themselves are not harmful, but they store and hide malware, bots, and worms. They are one of the challenges to forensic investigators.



Following are the rootkit detection techniques: signature, heuristic, integrity, cross view-based, and runtime execution path profiling.

Integrity-Based Detection

Integrity-based detection is a substitute to both signature- and heuristic-based detection. Initially, the attacker runs tools such as Tripware, AIDE, etc. on a clean system. These tools create a baseline of clean system files and store them in a database. Integrity-based detection functions by comparing a current file system, boot records, or memory snapshot with the trusted baseline. They notify the evidence or presence of malicious activity based on the dissimilarities between the current and baseline snapshots.

Signature-Based Detection

Signature-based detection methods work as a rootkit fingerprint. The sequence of bytes from a file can be compared with another sequence of bytes that belong to a malicious program. The method mostly scans the system files. It can easily detect invisible rootkits by scanning the kernel memory. The success of signature-based detection is less due to the rootkit's tendency to hide files by interrupting the execution path of the detection software.

Heuristic/Behavior-Based Detection

Heuristic detection works by identifying deviations in normal OS patterns or behaviors. This kind of detection is also known as behavioral detection. Heuristic detection is capable of identifying new, previously unidentified rootkits. This ability lies in being able to recognize

deviants in “normal” system patterns or behaviors. Execution path hooking is one such deviant that causes heuristic-based detectors to identify rootkits.


Runtime Execution Path Profiling

The runtime execution path profiling technique compares runtime execution path profiling of all system processes and executable files. The rootkit adds new code near to a routine’s execution path to destabilize it. The method hooks number of instructions executed before and after a certain routine, as it can be significantly different.

Cross View-Based Detection

Cross view-based detection techniques function by assuming that the attackers have disrupted the OS in some way. This enumerates the system files, processes, and registry keys by calling common APIs. These tools compare the gathered information with the data set obtained through the use of an algorithm traversing through the same data. This detection technique relies upon the fact that the API hooking or manipulation of kernel data structure taints the data returned by the OS APIs, with the low-level mechanisms used to output the same information free from DKOM or hook manipulation.

Steps for Detecting Rootkits



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.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

There are many tools available in the market to detect the presence of rootkits on the target system. But sometimes tools come up short as the malware writers always find ways to counter these automated rootkit detectors; some of their latest efforts are able to even evade it. Therefore, it is better to detect the rootkits manually. Manual detection of rootkits requires time, patience, perseverance, and expertise.

Examine the file system and registry of the system to detect the rootkits manually.

Refer the slide for steps to detect rootkits by examining file system.

Following are the steps to detect rootkits by examining the registry:

1. Run **regedit.exe** from inside the potentially infected OS.
2. Export **HKEY_LOCAL_MACHINE\SOFTWARE** and **HKEY_LOCAL_MACHINE\SYSTEM** hives in text file format.
3. Boot into a **clean CD** (such as **WinPE**).
4. Run **regedit.exe**.
5. Create a new key such as **HKEY_LOCAL_MACHINE\Temp**.
6. Load the Registry hives named Software and System from the suspect OS. The default location will be **c:\windows\system32\config\software** and **c:\windows\system32\config\system**.

7. Export these Registry hives in text file format. (The Registry hives are stored in binary format and Steps 6 and 7 convert the files to text.)
8. Launch **WinDiff** from the CD, and compare the two sets of results to detect file-hiding malware (i.e., invisible inside, but visible from outside).

Note: There can be some false positives. In addition, 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

CHFI
Computer Hacking Forensic Investigator

- **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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory injection and Syscall Proxying

In the buffer overflow exploit attack, the attackers use buffer overflows as entry to a remote system in order to inject and run code in the address space of a running program, thereby successfully altering the victim program's behavior. Then, the attacker uploads tools and saves them to the target system.

Userland Execve Technique

The "Userland Execve" technique lets programs on the victim computer to load, run without using the Unix `execve()` kernel call, thereby letting the attacker to overcome kernel-based security systems that might deny access to `execve()`.

Syscall proxying

Rather than uploading the entire exploit program, the attacker can upload a system call proxy to accept the remote procedure calls from the attacker's machine. The victim's machine executes the requested system call and sends the result back to the attacker. By doing so, the attacker need not upload the tools to the compromised machine. However, this increases the amount of network traffic between the compromised machine and the attacker, thereby creating latency. This technique helps in capitalizing the code injection vulnerabilities on a system.

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

CHFI
Computer Hacking Forensic Investigator

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


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can use a Live CD or Bootable USB Token or virtual machines installed on a different storage media to perform attack on a PC or on a series of computers, unplug the device used, and then turn off the computer. This process will leave no trace of the attack on the source computer for later investigation or analysis. Using the Virtualization software, attackers can perpetrate the attack without even rebooting the host computer. These devices allow intruders to run a variety of applications while considerably reducing the sources of evidence footprint.

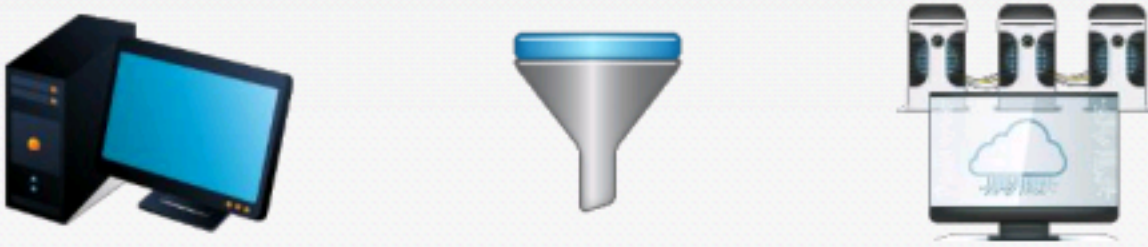
After the attack, the attacker can securely erase the files associated with the virtual machine or use the virtual machines directly on the victim's machine as a kind of super-rootkit. The forensic tool will not be able to view the virtual machines running as the super-rootkit because it is running outside the machine.


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






Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Anonymous identities and storage

Intruders/attackers create fake accounts via Gmail, Yahoo, Dropbox, etc. to safeguard their identity in case of successful forensic investigation. Using the storage space of their account, the attackers upload the attack tools and the captured information from the victim instead of storing them in their systems. Following these practices reduces the source of evidence for forensic 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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers having knowledge over the forensic tool's functionality can do a counter forensic attack against the tool and see that the tool does not capture any evidence.

The forensic investigators greatly depend on tools to evaluate the digital evidence. These tools help the investigators to acquire the required data efficiently. However, depending on the tools may be a weakness that attackers can exploit to prevent or interrupt investigations.

Anti-Forensics Techniques: Detecting Forensic Tool Activities

CHFI
Computer Hacking Forensic Investigator

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers are fully aware of the computer forensic tools that investigators use to find and analyze evidence from a victim's computer or network. Therefore, they try to incorporate forensic tools and process identification programs into the system or malware they are using. These programs act intelligently and change behavior on detecting the CFT. For example, a worm may stop propagation and even destroy the evidence when it is under surveillance.

Almost all the current hard drives have built-in self-Monitoring, Analysis and Reporting Technology (SMART). It reports the following:

- The total number of power cycles (Power_Cycle_Count)
- The total time that a hard drive has been in use (Power_On_Hours or Power_On_Minutes)
- A log of high temperatures that the drive has reached
- Other manufacturer-determined attributes
- Various malicious programs can read these attributes, which users cannot reset

The attackers use these details and modify their behavior with the anti-forensic tools to avert the process of investigation.

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



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

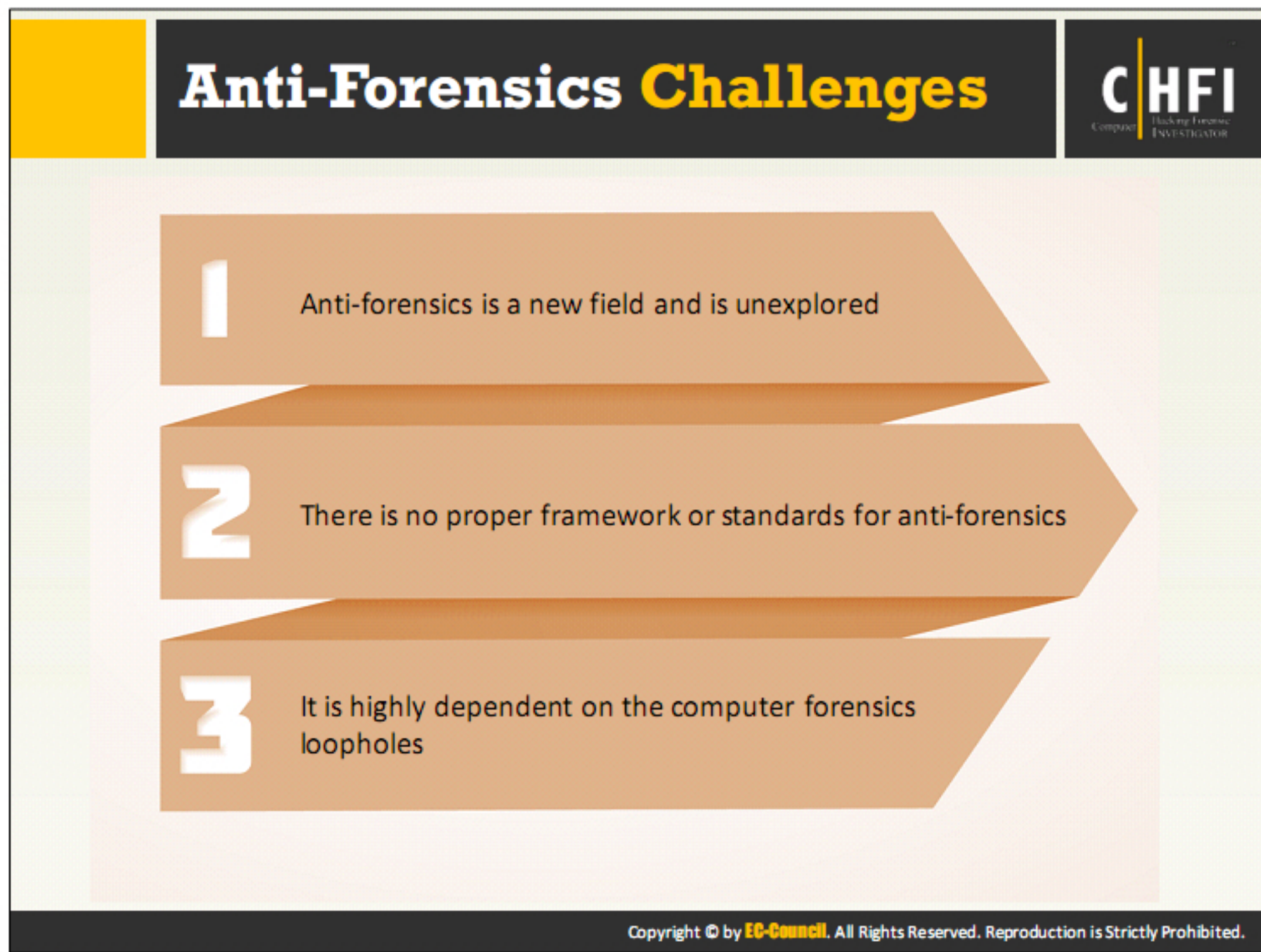
- Attacker sends packets across a network with their destination as an Ethernet and IP address that is on the subnet but currently not in use. It has a source address from a rear network
- Network monitoring tools on viewing such packets make a reverse DNS request in an attempt to resolve the hostname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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Forensics Countermeasures		CHFI Computer Hacking Forensic Investigator
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	
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.		

Investigators can overcome the anti-forensic techniques discussed in this module through improved monitoring of systems or by fixing bugs in the current generation of computer forensic tools.

- Replace weak file identification techniques with stronger ones.
- Investigators can overcome compression bombs with more intelligent decompression libraries.
- Validate the examination results with multiple tools for accuracy.
- Restrict the illegal usage of anti-forensic tools.
- Investigators should not completely depend on specific tools, as the tools themselves are not immune to attack.



Computer and Network Forensics has arisen as a new field in IT, aimed at acquiring and analyzing digital evidence to solving cases that involve the use, or more accurately, misuse of computer systems.

Various scientific techniques, procedures, and technological tools have been developed and effectively applied in this field. However, anti-forensics has newly risen as a field that aims at bypassing the efforts and objectives of the field of computer and network forensics.

- Decrypting a strong encryption
- Obtaining obscured information
- Steganography in Social Networks
- Encrypting cryptographic choices for MAC and Windows

However, anti-forensics is a relatively new field and is largely unexplored. As a result there is no proper official framework or standards, and it is highly dependent on the available loopholes in any particular situation.

Anti-Forensics Tools: Privacy Eraser

CHFI
Computer Hacking Forensic Investigator

- **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.

Name	Registry keys	Registry values	Folders	Files	Size
Internet Cache	0	0	4	54	1,129 KB
Internet History	0	0	0	42	1,431 KB
Cookies	0	0	1	3	213 KB
Sessions	0	0	0	0	213 KB
Google Chrome (4,863 Items; 484.25 MB)	0	0	3	3,856	447,722 KB
Safari (18 Items; 3.32 MB)	0	0	0	1	2,352 KB
Desktop App (2,243 Items; 104.76 MB)	0	0	0	12	656 KB
Adobe Acrobat	0	0	0	40	10,309 KB

<http://www.cybertronsoft.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Privacy Eraser is an anti-forensic solution to protect the privacy of the user by deleting the browsing history and other computer activities. This tool supports multiple web browsers such as Internet Explorer, Microsoft Edge, Firefox, Google Chrome, Safari, and Opera.

Privacy Eraser erases all digital footprints: web browser cache, cookies, browsing history, address bar history, typed URLs, autocomplete form history, saved passwords, index.dat files, Windows' run history, search history, open/save history, recent documents, temporary files, recycle bin, clipboard, DNS cache, log files, error reporting, etc.

Privacy Eraser supports plugins to extend the software's cleaning features. It supports programs such as ACDSee, Adobe Reader, Microsoft Office, WinZip, WinRAR, Windows Media Player, VLC Player, BitTorrent, and Google Toolbar. It works with Windows 10/8.x/7/Vista/2012/2008 (32/64-bit), and also supports Windows FAT16/FAT32/exFAT/NTFS file systems. The software implements and exceeds the US Department of Defense and NSA clearing and sanitizing standards, giving you the confidence that once erased, your file data is gone forever and can never be recovered.

Source: <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/libseclinux.so bash -l
```

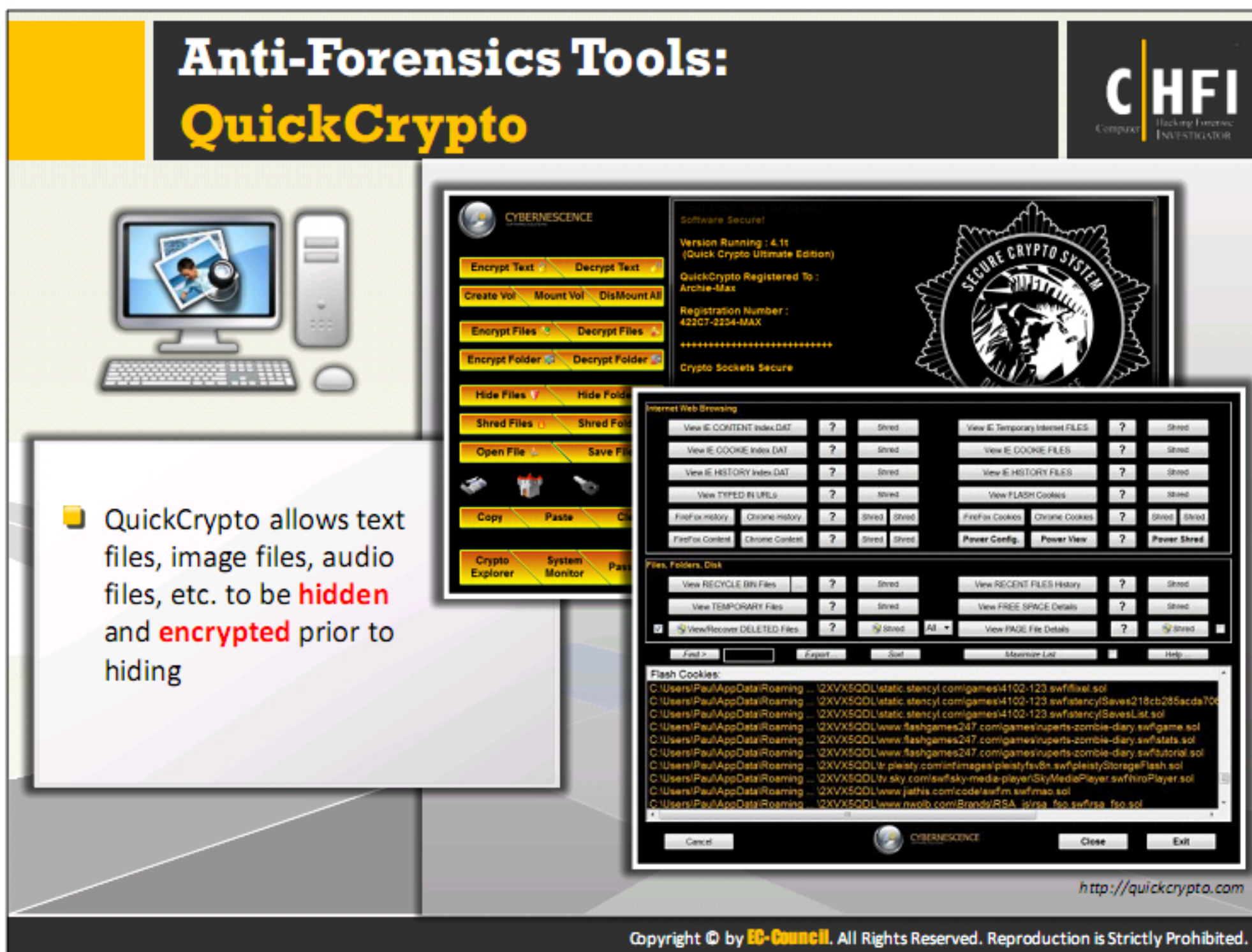
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Azazel is a userland rootkit written in C based off of the original LD_PRELOAD technique from Jynx rootkit. It is more robust and has additional features and focuses heavily around anti-debugging and anti-detection.

Features:

- Anti-debugging
- Avoids unhide, ISOFS, PS, LDD detection
- Hides files and directories
- Hides remote connections
- Hides processes
- Hides logins
- PCAP hooks avoid local sniffing
- Two accept backdoors with full PTY shells
- Crypthook encrypted accept() backdoor
- Plaintext accept() backdoor
- PAM backdoor for local and remote entry

Source: <https://github.com>



QuickCrypto is advanced Windows-based privacy and encryption software. It is a program that will hide and encrypt files, emails, and passwords. It uses the most powerful algorithms and techniques to ensure your email communication, passwords, all confidential files, and information are kept completely secure.

Features:

- File and folder encryption using super-strong encryption algorithms
- Easily encrypt emails and email attachments
- Allows you to recover accidentally deleted files
- Protects business information
- Generates and stores secure passwords
- Encrypts USB memory sticks
- Keeps files private through encryption and also hides these files (remove from the normal file system)
- Possesses steganography function
- Secure file erasure is achieved with the included file shredder to wipe and destroy files

Source: <http://quickcrypto.com>

Anti-Forensics Tools

CHFI
Computer Hacking Forensic Investigator

 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Steganography Studio

Source: <http://stegstudio.sourceforge.net>

Steganography Studio is an anti-forensic tool to analyze the key steganographic algorithms. This tool implements algorithms that are configurable with a variety of filters. It implements the image analysis algorithms for the detection of hidden information. The software is developed in Java, allowing use in multiple OSs.

CryptaPix

Source: <http://www.briggsoft.com>

CryptaPix is an anti-forensic tool, image file management, and encryption program for Windows. The tool organizes prints and secures the digital photos and downloaded image files. It secures the proprietary images from unauthorized access with 256-bit AES encryption or hides sensitive text, data, or other images into an image with the secure steganography feature.

GiliSoft File Lock Pro

Source: <http://gilisoft.com>

GiliSoft File Lock Pro is an anti-forensic tool and encrypts the files. You will never worry about data theft by malicious behavior and privacy leaks. The tool locks folders on an internal hard drive, flash drive, external USB drive, thumb drive, memory card, pen drive, and network drive. It restricts access to files, folders, and drivers; encrypts files and folders; hides files and folders

and drives to make them invisible; makes files, folders, and drives read only; or password protects files, folders, and drives.

wbStego

Source: <http://wbstego.wbailer.com>

As an anti-forensic tool, wbStego is used to hide sensitive data in a carrier file so that nobody will be aware of the existing data when sending an encrypted file.

Data Stash

Source: <http://www.skyjuicesoftware.com>

Data Stash is a steganographic security tool and used to hide the files. It allows the users to hide sensitive data files within other files using steganography.

Features:

- Hides files within files (Steganography)
- Receptacle file remains fully functional
- Supports file formats of mpg, .jpg, .mp3, .exe, .com, etc.
- Provides password protection using Blowfish encryption

OmniHide PRO

Source: <http://omnihide.com>

OmniHide PRO is a steganographic security tool used to hide files. Any file can be hidden within common image/music/video/document formats. The output file would work just as the original source file would.

Features:

- Hides files within photos, movies, documents, music, etc.
- No restrictions on input file types or size
- Enhanced security with password enabled encryption
- Free access to all future updates and patches

Masker

Source: <http://www.softpuls.com>

Masker is a steganographic security tool that encrypts files so that a password will be needed to open the files. It hides the files and folders inside carrier files, such as image files, video, program, or sound files. It allows to hide any files, even whole folders and sub-folders. The carrier file will remain fully functional. It allows transferring the carrier file through the internet, and the hidden files inside will be transferred simultaneously with the carrier file, as they are a part of the carrier file.

Features:

- Hides files, folders, and sub-folders within a carrier file and vice-versa
- Supports multiple hideouts
- Previews function (hidden files can be previewed and modified in hidden mode)
- Searches function

DeepSound

Source: <http://jpinsoft.net>

DeepSound is a steganographic security tool and audio converter that hides secret data into audio files. This application enables its users to extract secret files directly from audio files or audio CD tracks. DeepSound might be used as copyright-marking software for wave, flac, wma, ape, and audio CD. DeepSound supports encrypting secret files.

DBAN

Source: <http://www.dban.org>

DBAN, an erasure software, automatically deletes the contents of any hard disk that it can detect. This method prevents identity theft before recycling a computer. DBAN is also a commonly used solution to remove viruses and spyware from Microsoft Windows installations.

Universal Shield

Source: <http://www.everstrike.com>

Universal Shield by Everstrike Software is the ultimate protection tool for one's computer. It enables users to hide files, folders, and drives. It sets access rules using flexible security combinations for user's most precious data. Universal Shield supports Windows 7/Vista/XP/2003/2000 OSs.

Anti-Forensics Tools (Cont'd)



 Ontrack Eraser Degausser http://www.krollontrack.co.uk	 Blancco 5 http://www.blancco.com
 BatchPurifier http://www.digitalconfidence.com	 Secure IT http://www.cypherix.com
 Steganos Privacy Suite 17 https://www.steganos.com	 ParetoLogic Privacy Controls http://www.paretologic.com
 Webroot's Internet Security Complete http://www.webroot.com	 Exiv2 http://www.exiv2.org
 Blancco Flash http://www.blancco.com	 Invisible Secrets 4 http://www.invisiblesecrets.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ontrack Eraser Degausser

Source: <http://www.krollontrack.co.uk>

Ontrack DataAdvisor is a steganographic security tool. It provides security for backup systems and offers an online catalog view for the legacy tape libraries.

- Restores and migrates granularly specific items from specific tapes
- Deletes data securely with a certificate of erasure for each tape confirming the validity of the process

BatchPurifier

Source: <http://www.digitalconfidence.com>

BatchPurifier is the ideal tool to remove hidden data and metadata from multiple files.

Hidden data stored in many popular file types may contain confidential and private information that when exposed can cause you and your organization embarrassment with possible financial and legal implications.

BatchPurifier removes more than 60 types of hidden data from 25 file types, including Microsoft Office® documents (Word, Excel, PowerPoint)*, OpenOffice™ documents, PDF documents, and popular image and media file types such as JPEG, JPEG 2000, PNG, SVG, AVI, WAV, AIFF, MP3, MP4, and F4V. BatchPurifier™ can remove hidden data from files even if they are compressed within ZIP files.

Steganos Privacy Suite 17

Source: <https://www.steganos.com>

The Steganos Privacy Suite 17 is a steganographic security tool. It provides passwords for all online accounts that are automatically created, managed, and registered, regardless of whether the device is a computer, tablet, or a smartphone.

Features:

- Protects your privacy online: stops tracking anonymous browser and blocks ads
- Accesses your passwords without using a cloud possible
- Accesses your passwords via OneDrive and Google Drive
- Safer and regular reminder of password change
- Even easier mobile access with support for Touch ID on iOS
- The Internet Trace Destructor with support for Chrome, Firefox, and Internet Explorer—erases data tracks and stops the acquisitiveness of the computer

Webroot's Internet Security Complete

Source: <http://www.webroot.com>

Webroot Internet Security Complete 2017 provides real-time protection for PC's and Mac's. The tool protects against viruses, malware, phishing attacks and identity theft.

Blancco Flash

Source: <http://www.blancco.com>

Blancco Flash is a tool to permanently erase flash memory from USB drives, SD cards, micro drives, CompactFlash cards, and other flash memory storage devices. It reduces the risk of data loss and fraud by performing due diligence into best security practices.

Features:

- Permanently erase multiple flash drives, rapidly and simultaneously
- Integrate seamlessly with Blancco Mobile to maximize erasure processes and impact across mobile devices and external SD cards

Blancco 5

Source: <http://www.blancco.com>

Blancco Flash is a tool to erase data from drives, including complex SSDs in desktop/laptop computers, servers, and storage environments with the most certified and patented data erasure solution. Blancco 5 is acknowledged by DIPCOG for being suitable for erasure of SSD media. Manage your data erasure on IT assets quickly and simultaneously to streamline your data management process.

Features:

- Permanently and verifiably erases data from SSDs to improve functionality of devices
- Increases resale value of devices

Secure IT

Source: <http://www.cypherix.com>

Secure IT protects files individually through file encryption. It facilitates a customizable file shredder and the ability to generate self-decrypting email attachments, thereby allowing the user to send encrypted emails.

Features:

- High compression
- Command line processing
- Built-in file shredder
- Secure emails

ParetoLogic Privacy Controls

Source: <http://www.paretologic.com>

ParetoLogic Privacy Controls is a tool that allows the users to delete all the data related to internet activity. The tool erases all privacy files pertaining to Instant Messaging and Voice Over Internet Protocol such as AOL, ICQ, MSN, Yahoo! Instant Messenger, Google Talk, Skype, and Windows Live Messenger.

Features:

- Obliterates files from streaming video and those related to media players, including: iTunes, Windows Media Player, Winamp, VLC, RealPlayer, DivX, and QuickTime
- Finds and deletes unwanted history items from third-party applications such as Adobe Acrobat and Macromedia Flash Player
- Removes all traces of your desktop search history from applications such as: Google Desktop Search, Yahoo! Desktop Search, and AOL Desktop Search
- Cleans information from Google Toolbar, Yahoo! Toolbar, AOL Toolbar, and eBay Toolbar

Exiv2

Source: <http://www.exiv2.org>

Exiv2 is a C++ library and a command line utility to manage image metadata. It provides read and write access to the EXIF, IPTC, and XMP metadata of digital images in various formats.

Features:


- Converts EXIF and IPTC metadata to XMP and vice versa
- Supports EXIF Makernote
- Sets and deletes methods for EXIF thumbnails
- Extracts previews from RAW images and thumbnails from the EXIF metadata

- Inserts and deletes the thumbnail image embedded in the EXIF metadata
- Prints, sets, and deletes the JPEG comment of JPEG images
- Fixes the EXIF ISO settings of picture taken with Canon and Nikon cameras


Invisible Secrets 4

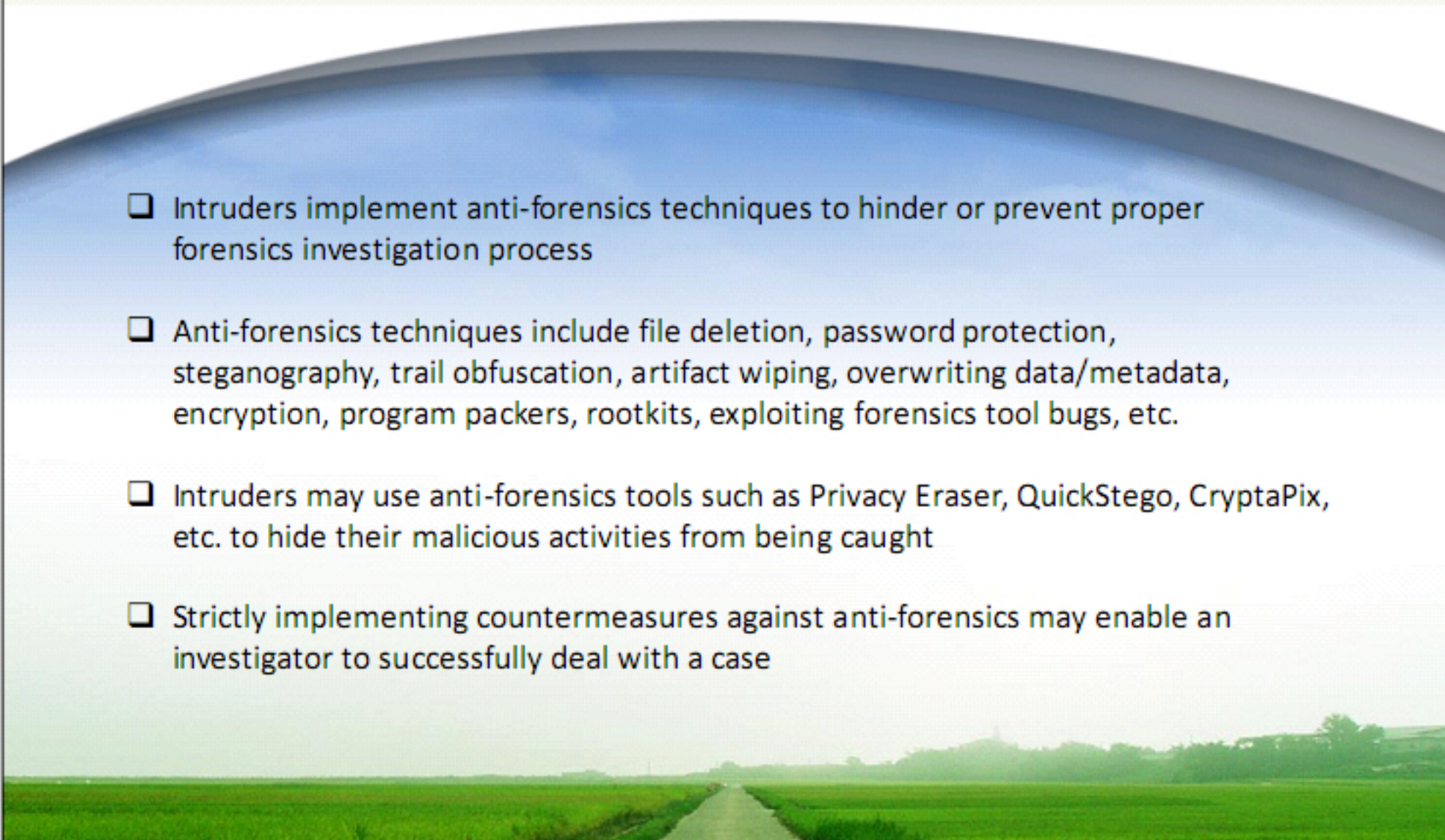
Source: <http://www.invisiblesecrets.com>

Invisible Secrets 4 is a tool to encrypt data and files for safe keeping or for secure transfer across the Internet. The tool hides files in places that on the surface appear totally innocent, such as picture or sound files or web pages. It allows file encryption to hide files from Windows Explorer and transfers them by email or via Internet.



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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

In this module, you have learned about the different anti-forensic techniques and processes intruders implement to avert the forensic investigation process. This module also discussed various methods to overcome such techniques using software and hardware tools.

In the next module, you will learn about conducting a forensic investigation on various OSs such as Windows, Mac, and Linux.