Lecture 7- Anti-Forensics Techniques

Dr. Zunera Jalil

Email: zunera.jalil@au.edu.pk

8th April 2025

Anti Forensics

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.

Anti Forensics

- Attackers try to **reduce** the **quality** and **quantity** of **digital evidence**.
- Attackers try to cover their tracks by deleting browser history, cache memory, and even cookies.
- Use **programmed software and tools** to alter their digital footprints.

Anti Forensics

- **Makes a computer investigator's life difficult.**
- Cybercriminals can perform a wide range of nefarious activities (committing fraud, stealing crucial data, etc.)

- Anti forensic tools are **designed to hide, remove, and eventually hinder cyber forensic analysis**.
- Exhausting to retrieve evidence during

  a computer investigation.

Some Examples

- Attacker can alter the header of a file to deceive people.
  - **Changing the header from .jpg to .mp3** will give the impression of an audio file, but the system will still treat as an image file.
  - An investigator focused on a particular file format can skip over important evidence.

Some Examples

- Attacker can use slack space, i.e., unused space of a file, to hide sensitive sections of a file.

- Dividing a file into smaller sections and hiding the information in the slack space, makes the data retrieval and data assembly challenging.

Anti-Forensic Techniques

01 Data/File Deletion

02 Password Protection

03 Steganography

04 Data Hiding in File System Structures

05 Trail Obfuscation

06 Artifact Wiping

07 Overwriting Data/Metadata

08 Encryption

09 Encrypted Network Protocols

10 Program Packers

11 Rootkits

12 Minimizing Footprint

13 Exploiting Forensics Tool Bugs

14 Detecting Forensics Tool Activities

Data/File Deletion

- To hide their criminal and illegal activities, attackers sometimes delete important data and files.
- Recovering deleted data and files can help investigator in their cases
- **Data Recovery tools** are used to recover deleted data.

In FAT file system, when a file is deleted:

- OS replaces the first letter of a deleted filename with hex byte code **"E5h"**
- The cluster of this file is marked as unused even if it still contains the information until it is overwritten

Data Deletion

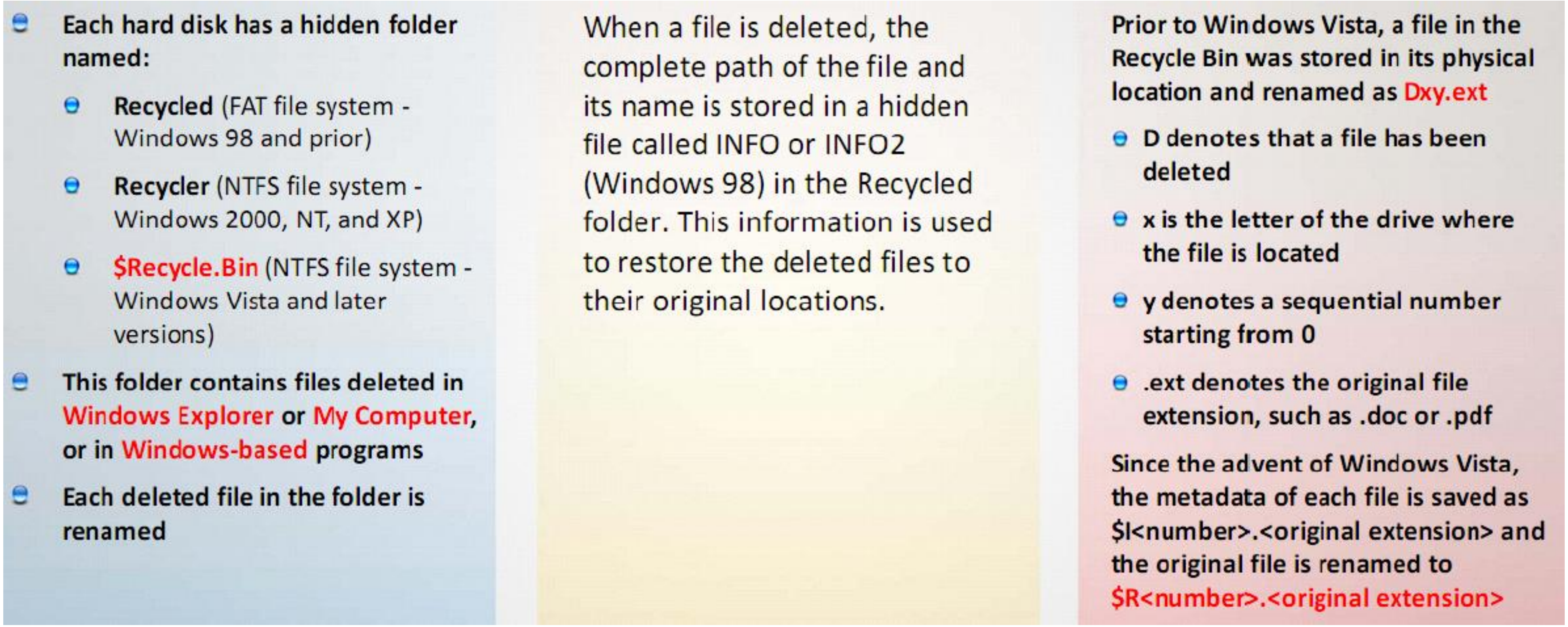
- **In NTFS file system, when a file is deleted:**
  - OS marks the file as deleted in master file table (MFT)
  - Cluster allocated to file is marked as free in $Bitmap
  - Empty clusters are available for new files
- **$BitMap** file keeps track of all of the used and unused clusters on an NTFS volume.
- When a file takes up space on the NTFS volume the location it uses is marked out in the $BitMap.

https://whereismydata.wordpress.com/2009/06/01/forensics-what-is-the-bitmap/

Where is Recycle Bin located?

- A temporary storage space for deleted files in Windows OS. Files can be restored.
- Recycle Bin location:
  - **C:\RECYCLED –(FAT-Windows 98 and prior)**
  - **C:\RECYCLER – (NTFS-Windows 2K, NT and XP)**
  - **C:\$Recycle.Bin (NTFS- Current)**
- All deleted files in FAT goes to C:\RECYCLED directory
- All deleted files in NTFS categorized into directors in C:\RECYCLER\$..
- **No size limit on recycle bin in Vista and later versions.** Previously it was max 3.99GB

Where Deleted Data goes?



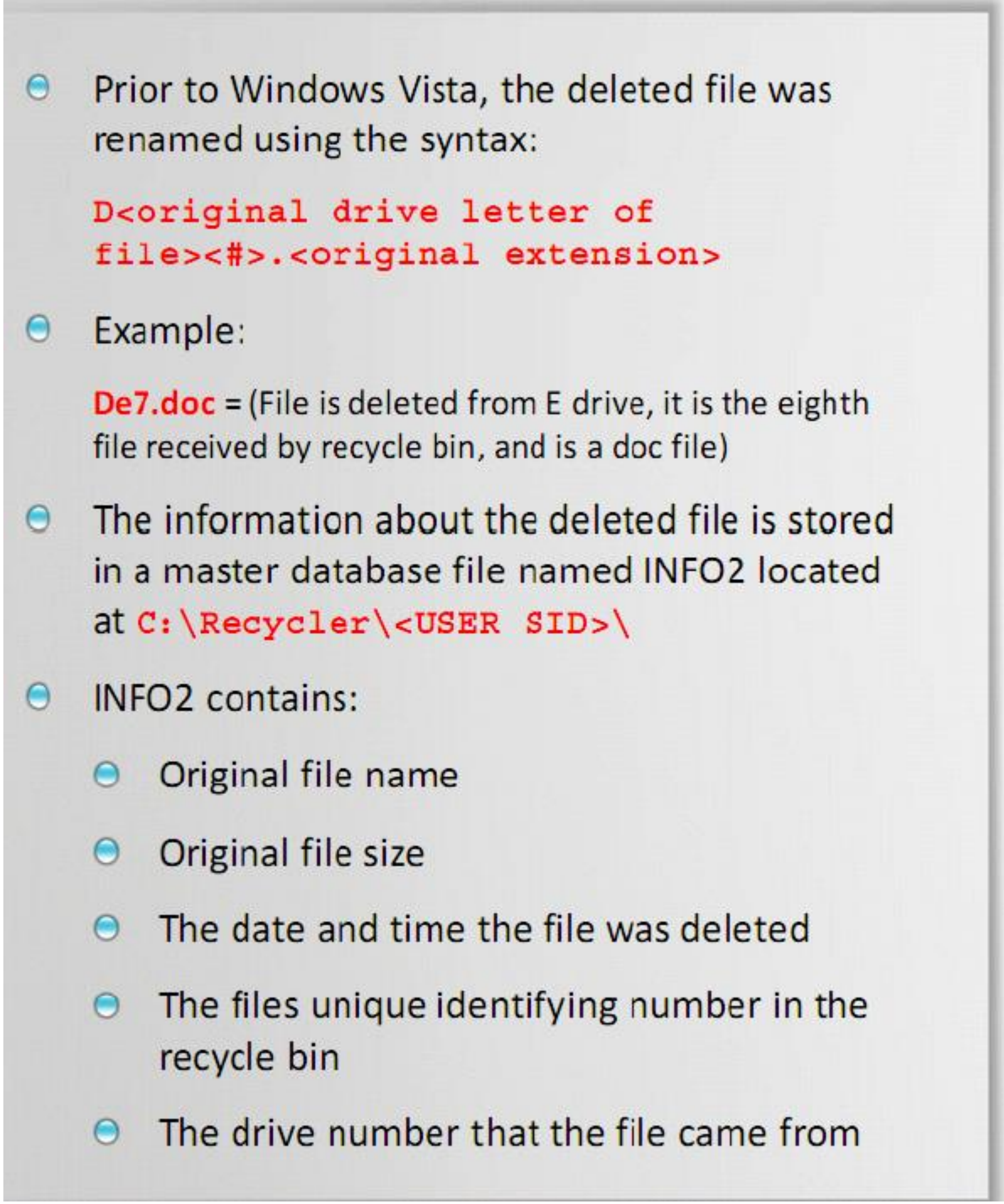
- Each hard disk has a hidden folder named:
  - **Recycled** (FAT file system - Windows 98 and prior)
  - **Recycler** (NTFS file system - Windows 2000, NT, and XP)
  - $Recycle.Bin (NTFS file system - Windows Vista and later versions)
- This folder contains files deleted in Windows Explorer or My Computer,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

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

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

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

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



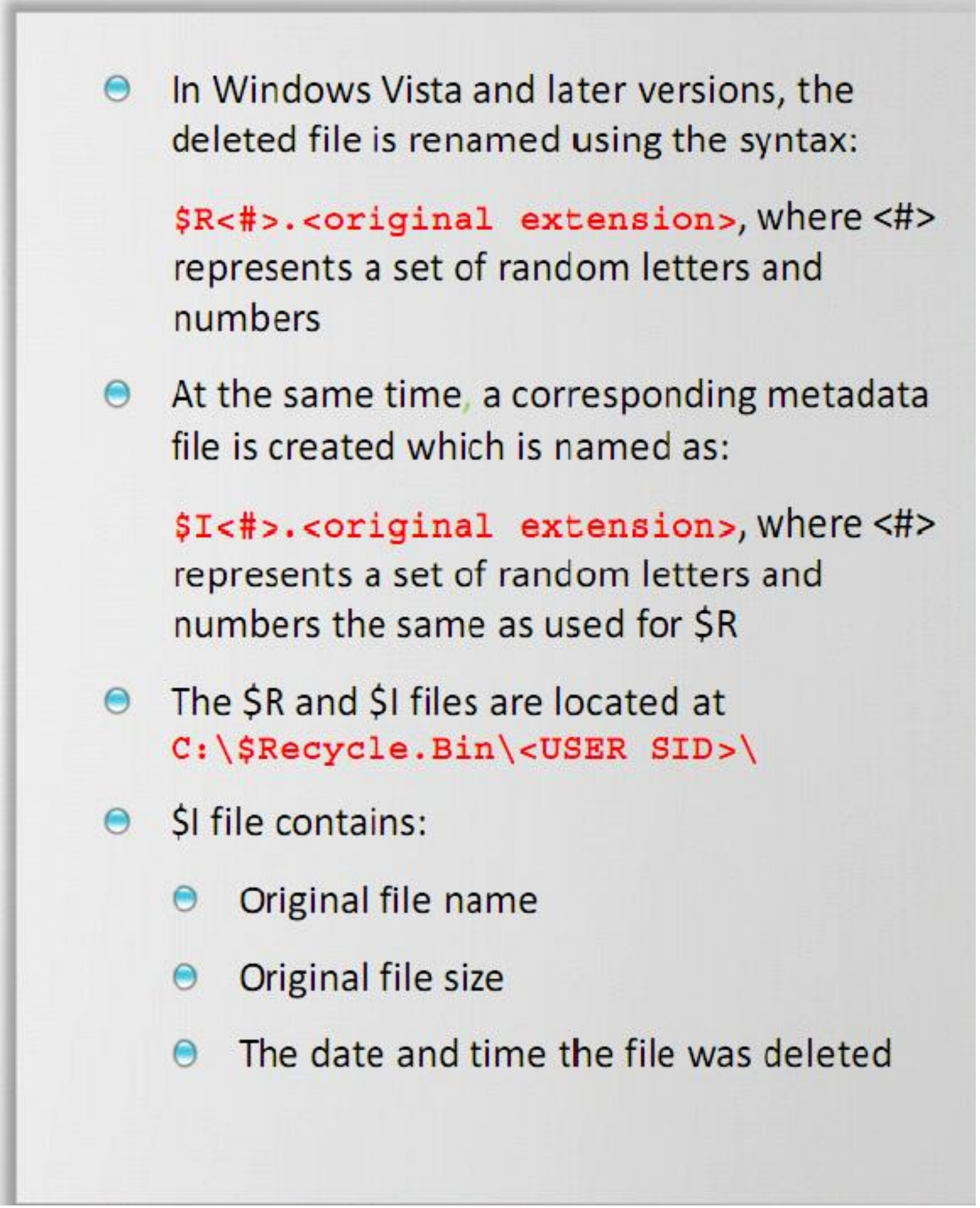
- Prior to Windows Vista, the deleted file was renamed using the syntax:

  `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

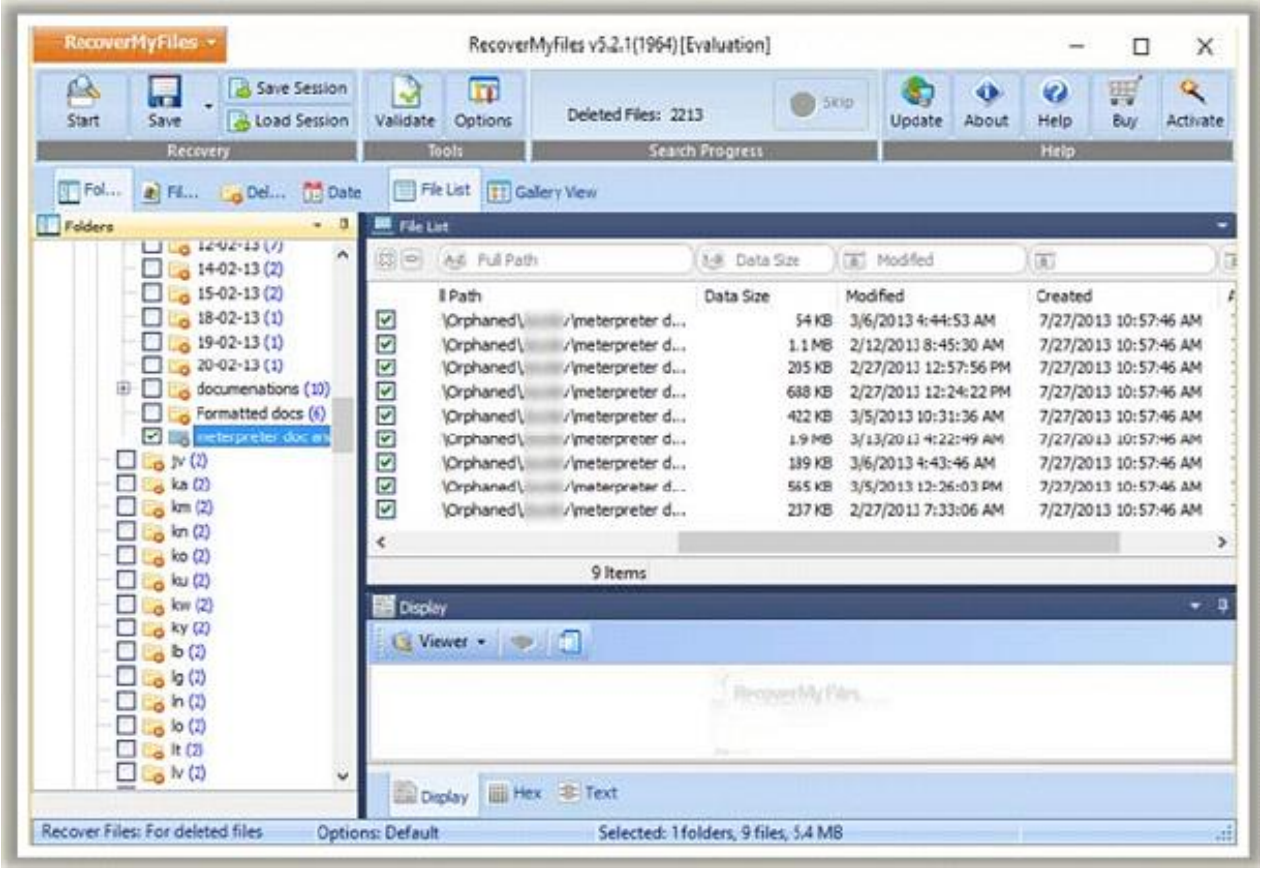
- At the same time, a corresponding metadata file is created which is named as:

  `$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

Recovering Files in Windows

- Sometimes recovering files that are deleted from Recycle bin is required.
- A file can be lost due to reinstallation or may get removed by a virus or a system failure.
- Recovery tools are used to recover lost data from storage media.
  - Disk Drill
  - Recuva
  - R-Studio
  - **EaseUS Data Recovery**
  - Stellar Recovery



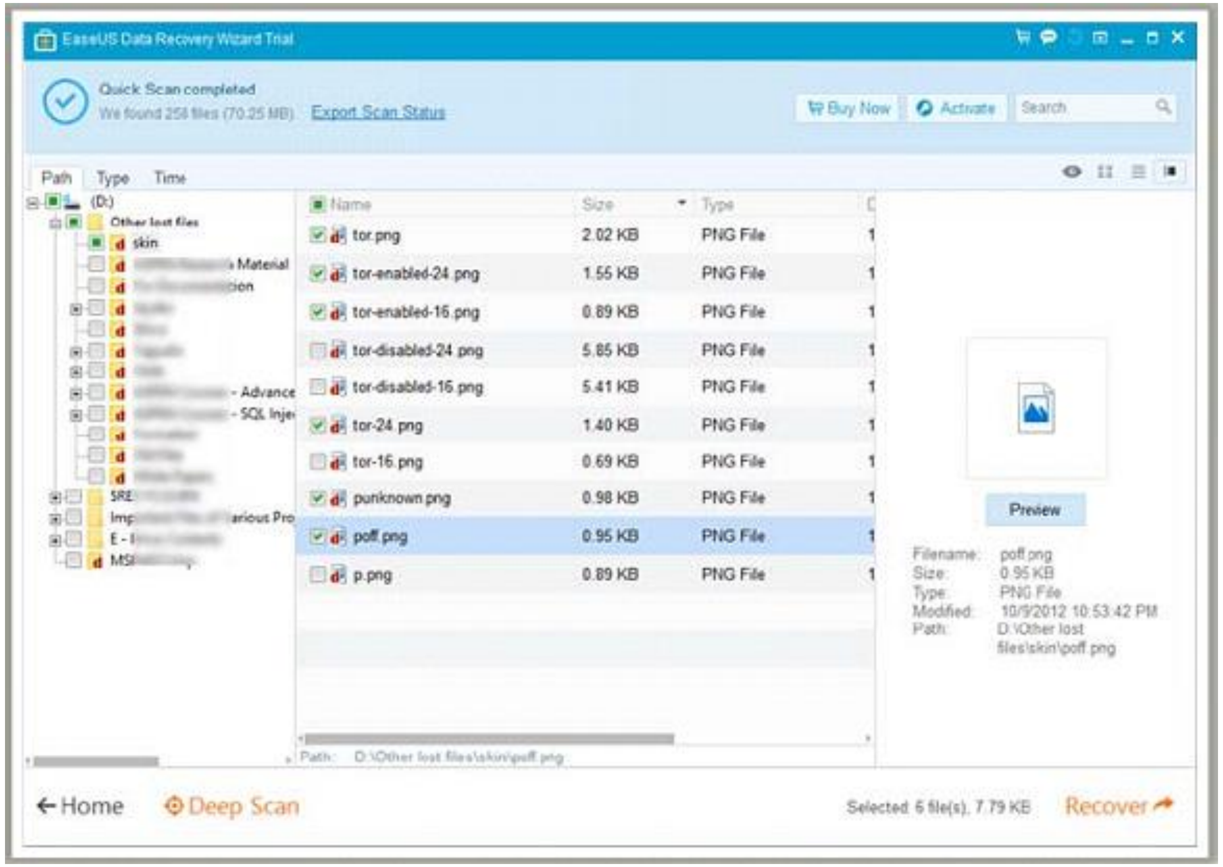
RecoverMyFiles v5.2.1(1964) [Evaluation]

Deleted Files: 2213

☑	Path	Data Size	Modified	Created
☑	\Orphaned\[redacted]/\meterpreter d...	54 KB	3/6/2013 4:44:53 AM	7/27/2013 10:57:46 AM
☑	\Orphaned\[redacted]/\meterpreter d...	1.1 MB	2/12/2013 8:45:30 AM	7/27/2013 10:57:46 AM
☑	\Orphaned\[redacted]/\meterpreter d...	205 KB	2/27/2013 12:57:56 PM	7/27/2013 10:57:46 AM
☑	\Orphaned\[redacted]/\meterpreter d...	688 KB	2/27/2013 12:24:22 PM	7/27/2013 10:57:46 AM
☑	\Orphaned\[redacted]/\meterpreter d...	422 KB	3/5/2013 10:31:36 AM	7/27/2013 10:57:46 AM
☑	\Orphaned\[redacted]/\meterpreter d...	1.9 MB	3/13/2013 4:22:49 AM	7/27/2013 10:57:46 AM
☑	\Orphaned\[redacted]/\meterpreter d...	189 KB	3/6/2013 4:43:46 AM	7/27/2013 10:57:46 AM
☑	\Orphaned\[redacted]/\meterpreter d...	565 KB	3/5/2013 12:26:03 PM	7/27/2013 10:57:46 AM
☑	\Orphaned\[redacted]/\meterpreter d...	237 KB	2/27/2013 7:33:06 AM	7/27/2013 10:57:46 AM

9 Items

Recover Files: For deleted files   Options: Default   Selected: 1 folders, 9 files, 5.4 MB



EaseUS Data Recovery Wizard Trial

Quick Scan completed

We found 258 files (70.25 MB)

	Name	Size	Type
☑	tor.png	2.02 KB	PNG File
☑	tor-enabled-24.png	1.55 KB	PNG File
☑	tor-enabled-16.png	0.89 KB	PNG File
□	tor-disabled-24.png	5.85 KB	PNG File
□	tor-disabled-16.png	5.41 KB	PNG File
☑	tor-24.png	1.40 KB	PNG File
□	tor-16.png	0.69 KB	PNG File
☑	punknown.png	0.98 KB	PNG File
☑	poff.png	0.95 KB	PNG File
□	p.png	0.89 KB	PNG File

Filename: poff.png
Size: 0.95 KB
Type: PNG File
Modified: 10/9/2012 10:53:42 PM
Path: D:\Other lost files\skin\poff.png

Path: D:\Other lost files\skin\poff.png

Selected: 6 file(s), 7.79 KB

Recovering Deleted Partition

- An attacker can delete a partition on a logical drive and all data on the drive is lost apparently.
- Just the parameters about how the partition is organized are deleted, not the whole data itself.
- Data can be recovered.
- **Active@Partition Recovery tool** used to recover deleted and damaged logical drives and partitions.

- **To repair a damaged or corrupted recycle bin**
  - 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

- **In Windows 10, you can repair a damaged or corrupted recycle bin folder:**

i. Open a command prompt with administrative privileges

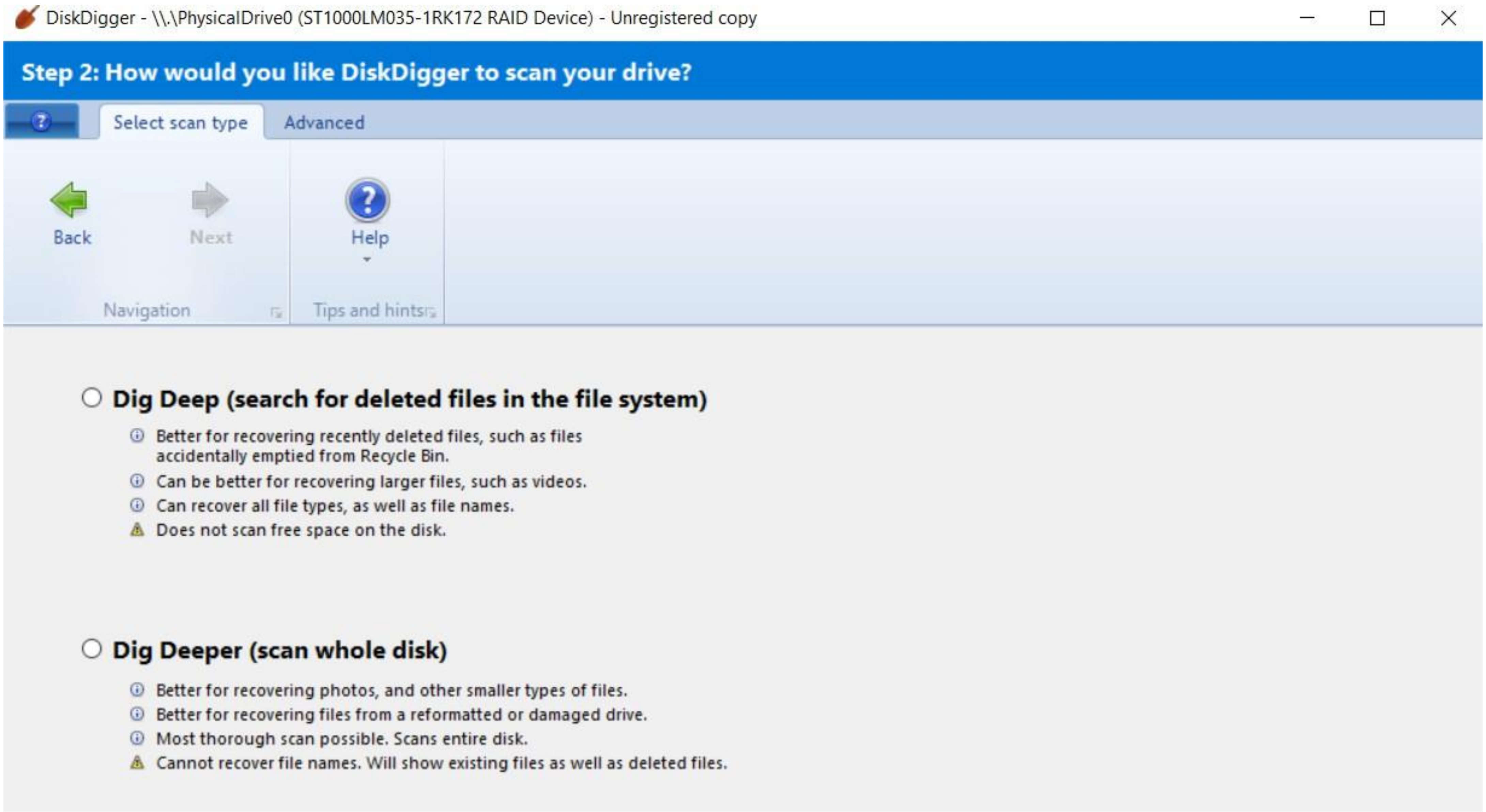
ii. Run rd /s /q C:\$Recycle.bin command

iii. Restart the computer

iv. 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

https://diskdigger.org/download

https://diskdigger.org/download



DiskDigger - \\.\PhysicalDrive0 (ST1000LM035-1RK172 RAID Device) - Unregistered copy

Step 2: How would you like DiskDigger to scan your drive?

○ Dig Deep (search for deleted files in the file system)

- ⓘ Better for recovering recently deleted files, such as files accidentally emptied from Recycle Bin.
- ⓘ Can be better for recovering larger files, such as videos.
- ⓘ Can recover all file types, as well as file names.
- ⚠ Does not scan free space on the disk.

○ Dig Deeper (scan whole disk)

- ⓘ Better for recovering photos, and other smaller types of files.
- ⓘ Better for recovering files from a reformatted or damaged drive.
- ⓘ Most thorough scan possible. Scans entire disk.
- ⚠ Cannot recover file names. Will show existing files as well as deleted files.

https://download.cnet.com/Total-Recall-Data-Recovery/3000-2094_4-77416790.html

Timestomping

- Timestomping changes the time and date of when a file or an application was *created, accessed, modified and/or executed*, disguising a user's actions.
- Changing the attributes in the MFT (master file table). MFT keeps track of everything:
  - Where files reside
  - What they're named
  - When they were made
  - Who can access the files

Timestomping

- MFT acts as the ‘brain’ of your storage drive.
- If a threat actor executed malware at a certain time and date, but then used timestomping, they could make it appear that the malware was executed earlier or later than it really was.
- Makes it harder to identify the timeline or sequence of events during a cyber incident.

Password Protection

- Sometimes data sources are password protected and investigators need to break passwords.

- Time to crack a password is related to bit strength (*see* password strength), which is a measure of the password's entropy, and the details of how the password is stored.

- Most methods of password cracking require the computer to produce many candidate passwords, each of which is checked.

Types of Passwords

- **Three types of passwords:**
  - **Cleartext:** Stored and transmitted as it is typed
  - **Obfuscated:** Stored and transmitted after transformation (reversible)
  - **Hashed:** using hash algorithms(MD5/SHA) but not reversible.

Password Breaking

- **Password Crackers -** used to recover passwords of a system, network resources, a file or an application.
- Breaking Methods are:

1. **Dictionary Attack:**
   - Intruder attempts to **crack** a **password**-protected security system with a “**dictionary** list” of common words and phrases used by businesses and individuals.
2. **Brute Force Attack:**
   - A program tries every combination of ASCII characters until the password is broken
3. **Rule Based Attack:**
   - A **password cracking** technique when an attacker knows which **rules passwords** in a particular system are **based** on, such as “alphanumeric and eight characters long.

Rainbow Tables

Rainbow table cracking

i. A word list is created and then hashed to present a "pre-compiled" listing for use in the software

ii. The hashed word list is used to compare against "target" passwords that we want to decrypt

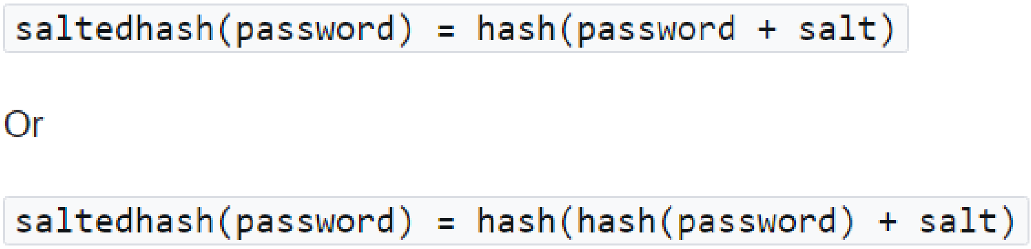
iii. If we get a match, we know the hash value and the corresponding clear-text equivalent, i.e., the password !!

iv. Possible tools to do this

Rainbow table creation tools

i. Rtgen

ii. Winrtgen



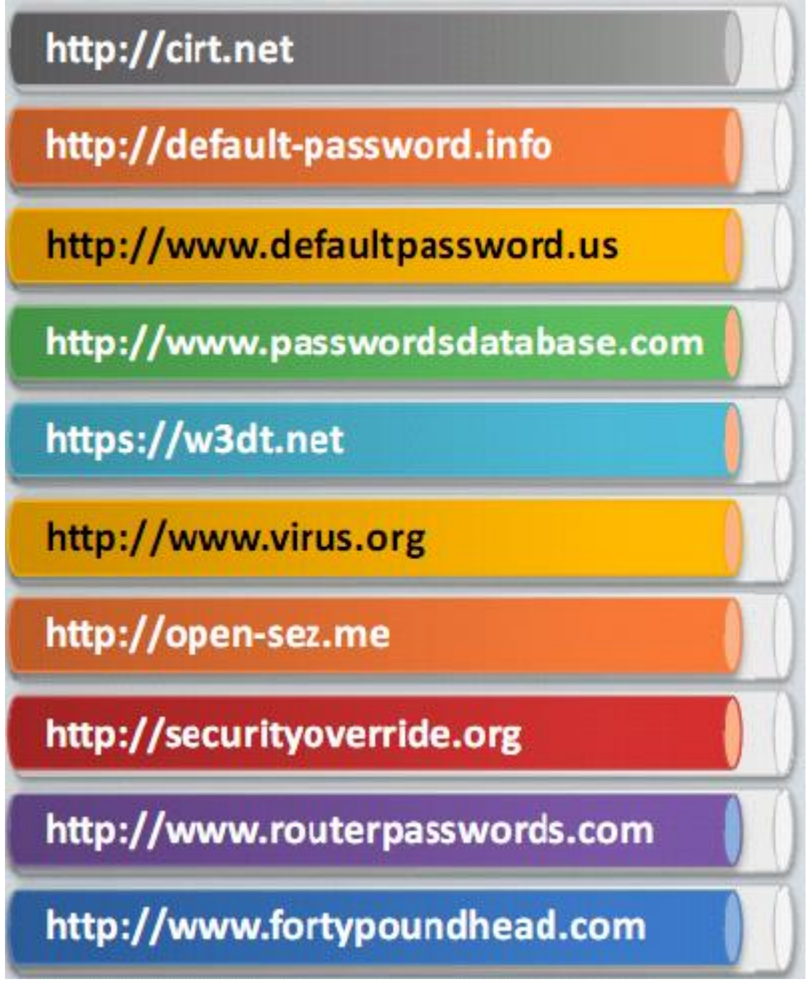
```
saltedhash(password) = hash(password + salt)
```

Or

```
saltedhash(password) = hash(hash(password) + salt)
```

Password Protection

- Sometimes users do not change the password supplied by manufacturer of devices.
- Default password can be used to break.
- You can search for default passwords in databases:



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

Password Cracking

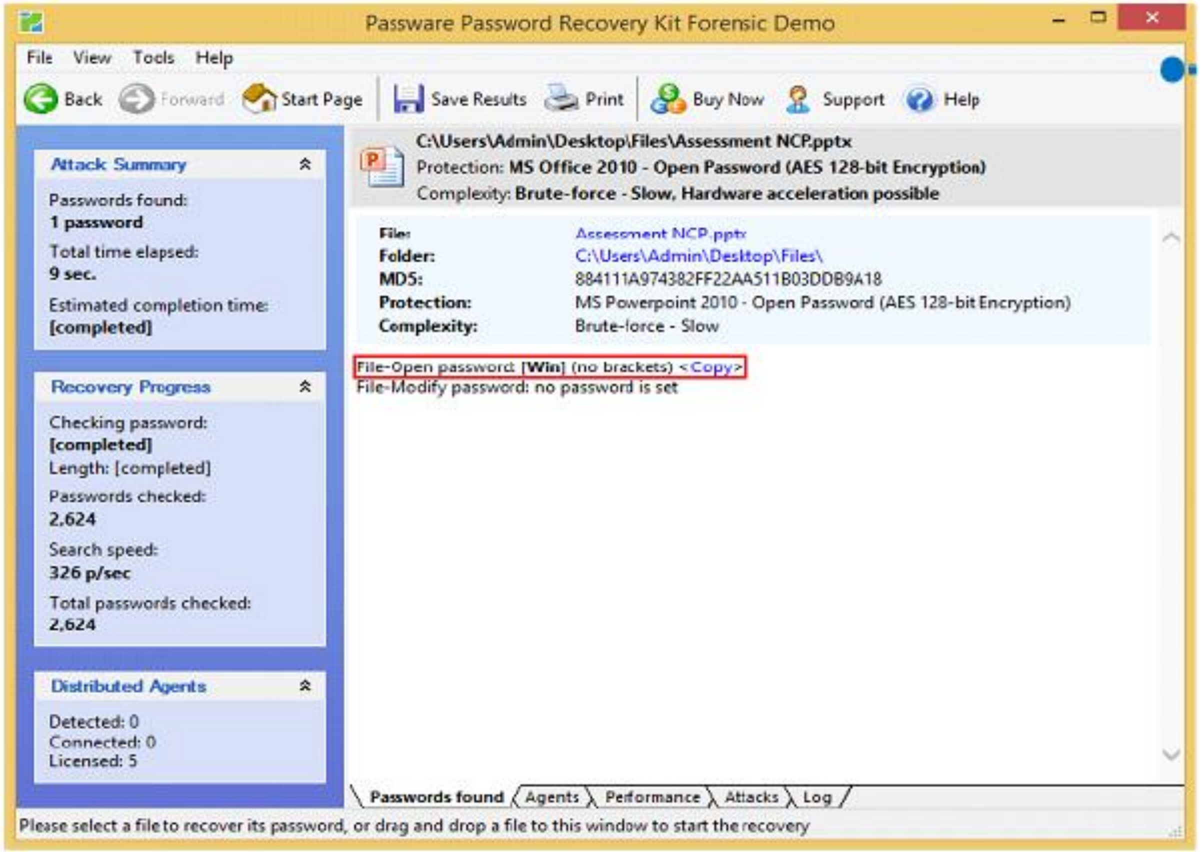
- John the Ripper Password Cracker

https://www.openwall.com/john/

- Wfuzz

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

- Passware



C:\Users\Admin\Desktop\Files\Assessment NCP.pptx
Protection: **MS Office 2010 - Open Password (AES 128-bit Encryption)**
Complexity: **Brute-force - Slow, Hardware acceleration possible**

Passwords found:
1 password
Total time elapsed:
9 sec.
Estimated completion time:
[completed]

Checking password:
[completed]
Length: [completed]
Passwords checked:
2,624
Search speed:
326 p/sec
Total passwords checked:
2,624

Detected: 0
Connected: 0
Licensed: 5

File:	Assessment NCP.pptx
Folder:	C:\Users\Admin\Desktop\Files\
MD5:	884111A974382FF22AA511B03DDB9A18
Protection:	MS Powerpoint 2010 - Open Password (AES 128-bit Encryption)
Complexity:	Brute-force - Slow

File-Open password: **[Win]** (no brackets) <Copy>
File-Modify password: no password is set

Please select a file to recover its password, or drag and drop a file to this window to start the recovery

Password Attack Categories

Passive on-line

1. Wire sniffing
2. Man-in-the-Middle (MitM)
3. Replay
    - Using the victim’s session ID

Active on-line

1. Guessing
2. Malware
3. Hash Injection

Offline

1. Pre-computed/Rainbow Tables - http://projectrainbowcrack.com/table.htm
2. Distributed Network (grids !!)

Steganography

- Steganography is the **act of concealing data in plain sight**.
- Most often, data is exchanged via an image.
- A portion of the image is altered so that it is not identifiable easily.
- The processed file looks ordinary and can go unnoticed.
- In the modern-day, the message is concealed using microdots and invisible ink.

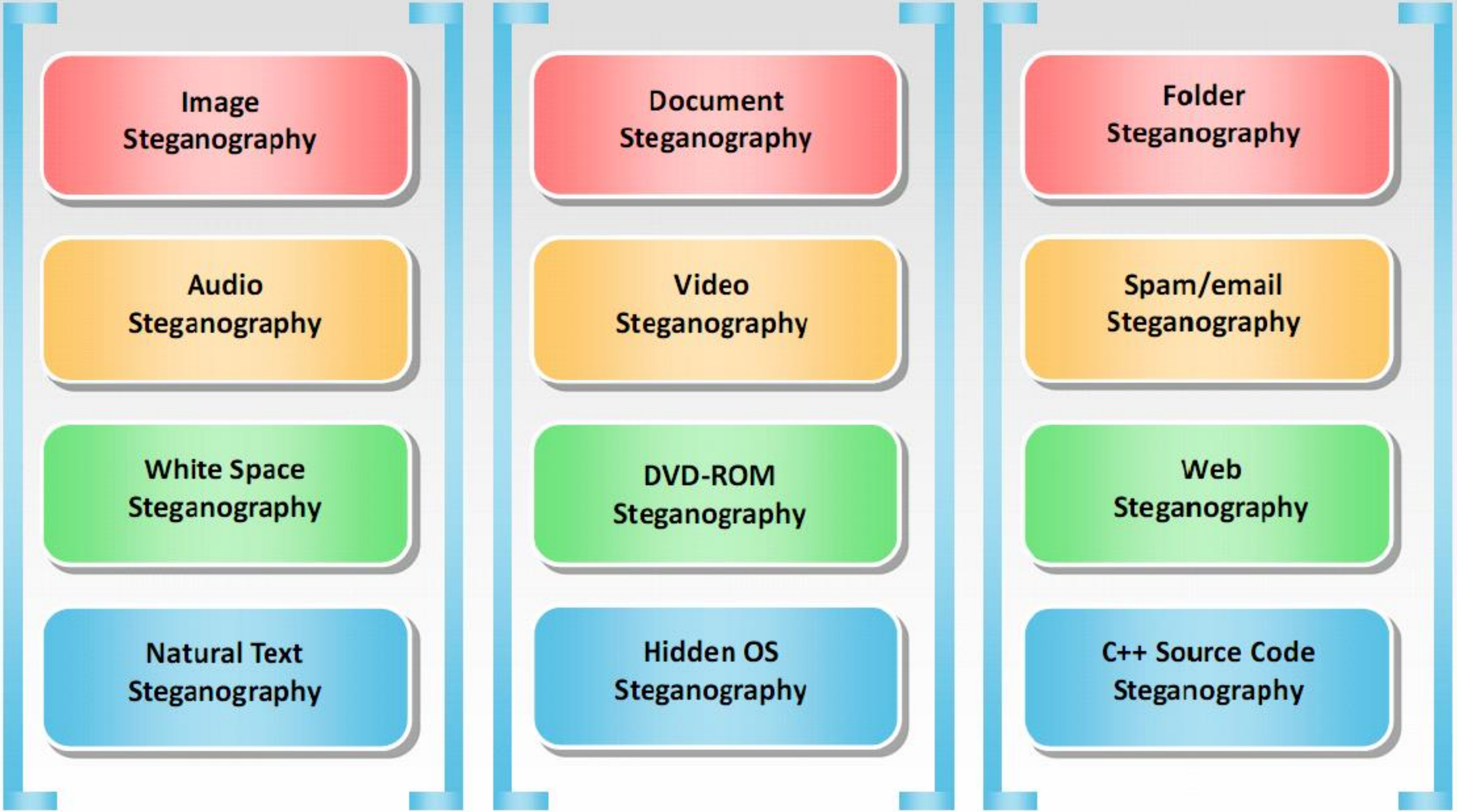


Image Steganography

Audio Steganography

White Space Steganography

Natural Text Steganography

Document Steganography

Video Steganography

DVD-ROM Steganography

Hidden OS Steganography

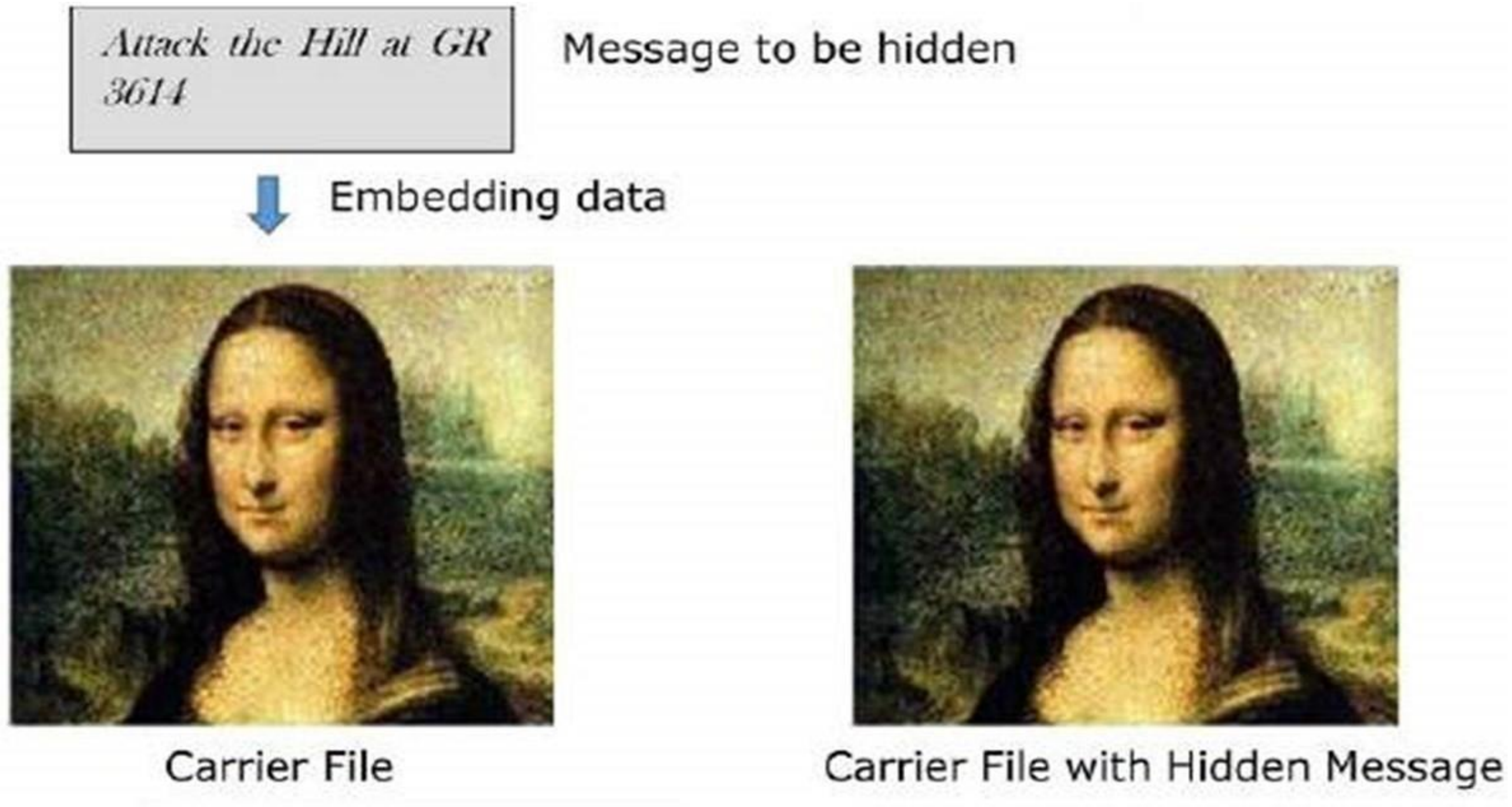
Folder Steganography

Spam/email Steganography

Web Steganography

C++ Source Code Steganography

Example



Attack the Hill at GR 3614

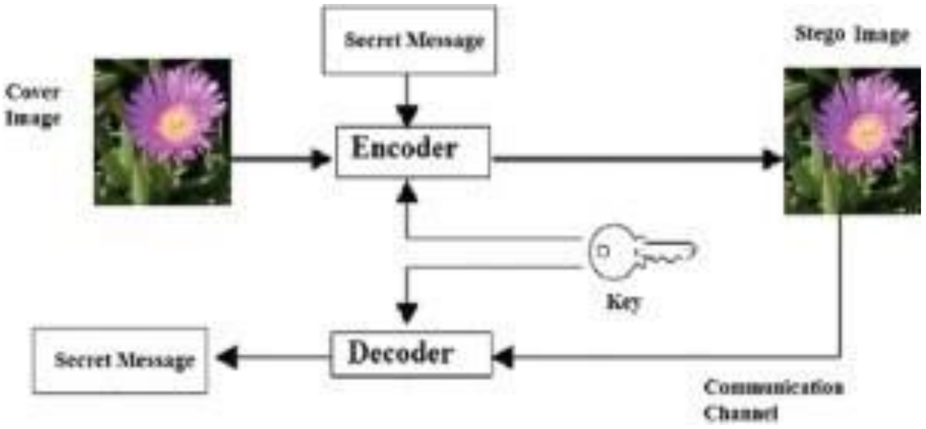
Message to be hidden

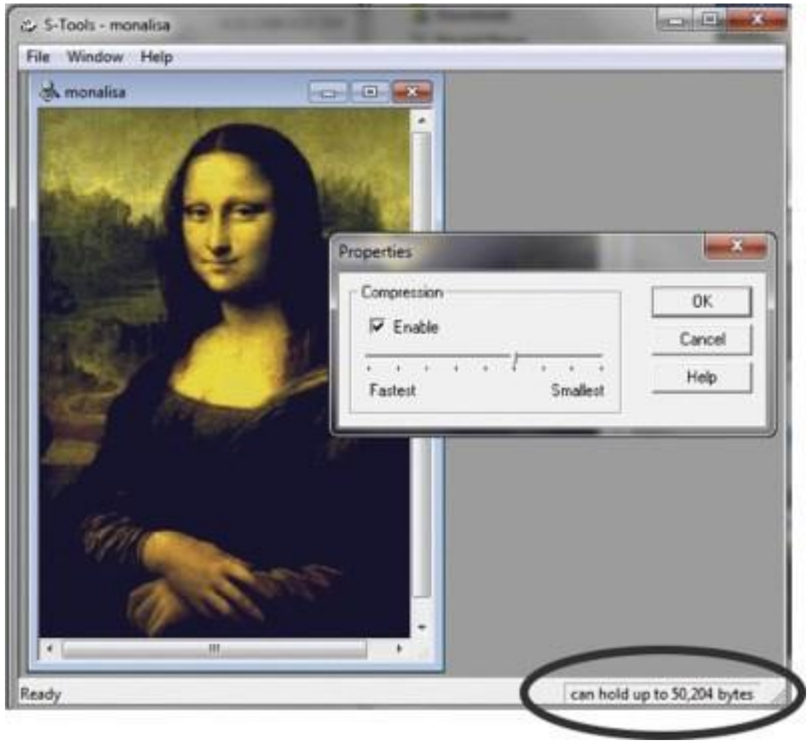
Embedding data

Carrier File

Carrier File with Hidden Message

Steganography in images





Compression

☑ Enable

Fastest Smallest

Ready

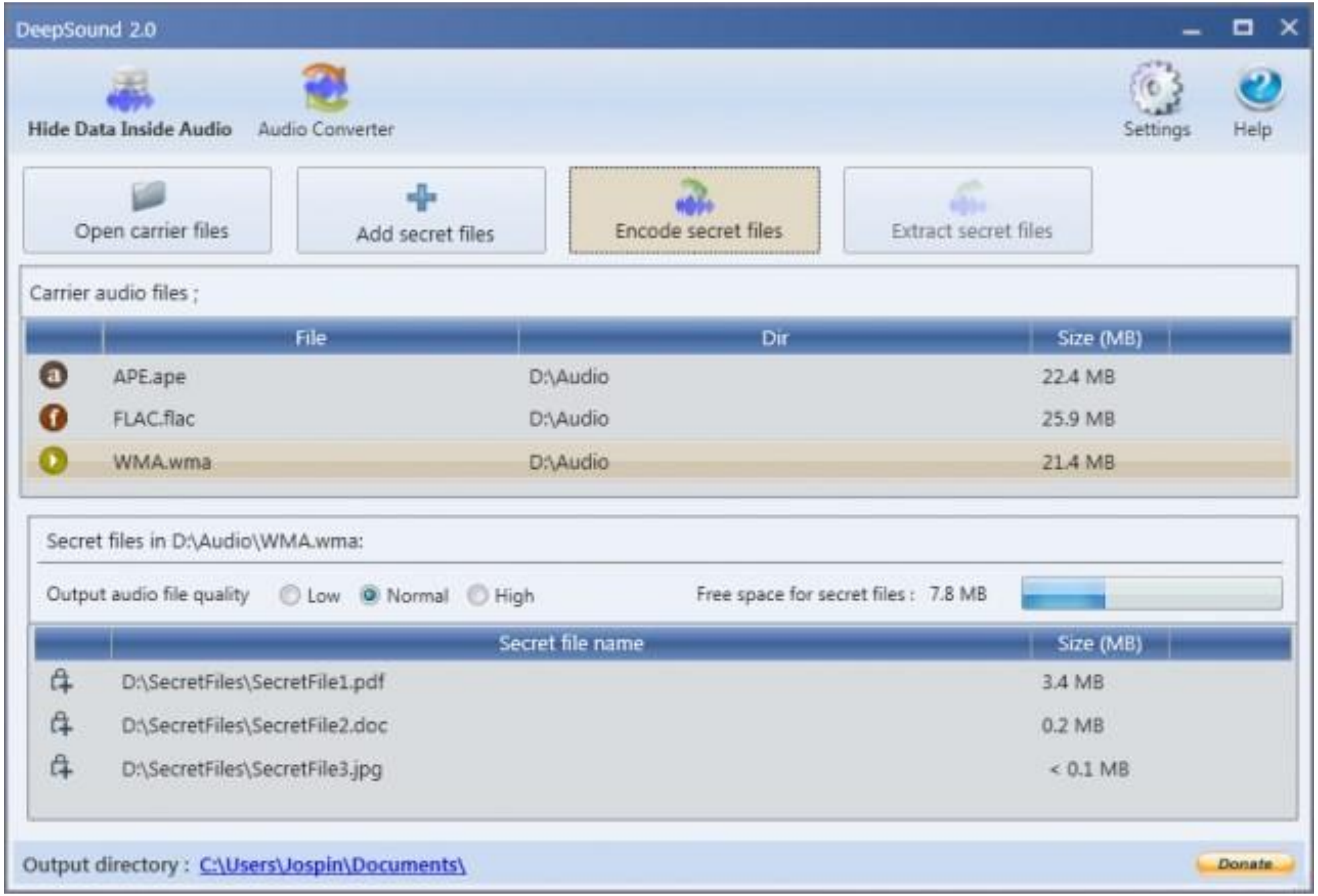
can hold up to 50,204 bytes

https://stylesuxx.github.io/steganography/

Steganography

- There is another form, **linguistic steganography**, where the message is hidden in a natural context.
- Steganography allows messages and even huge files to be hidden in pictures, text, audio, and video files.
- It is challenging to identify a steganography-attack, but repetitive patterns can reveal the secret message to the investigator.
- Professionals use advanced tools to spot hidden data.

Steganography in Audio



Carrier audio files ;

	File	Dir	Size (MB)
a	APE.ape	D:\Audio	22.4 MB
f	FLAC.flac	D:\Audio	25.9 MB
	WMA.wma	D:\Audio	21.4 MB

Secret files in D:\Audio\WMA.wma:

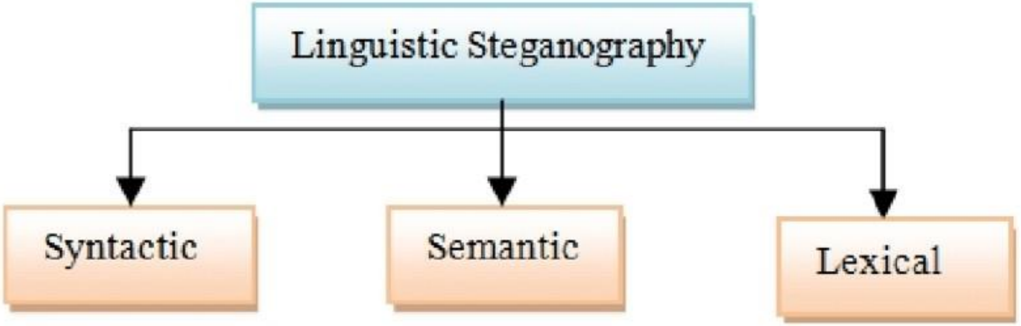
Output audio file quality ○ Low ● Normal ○ High

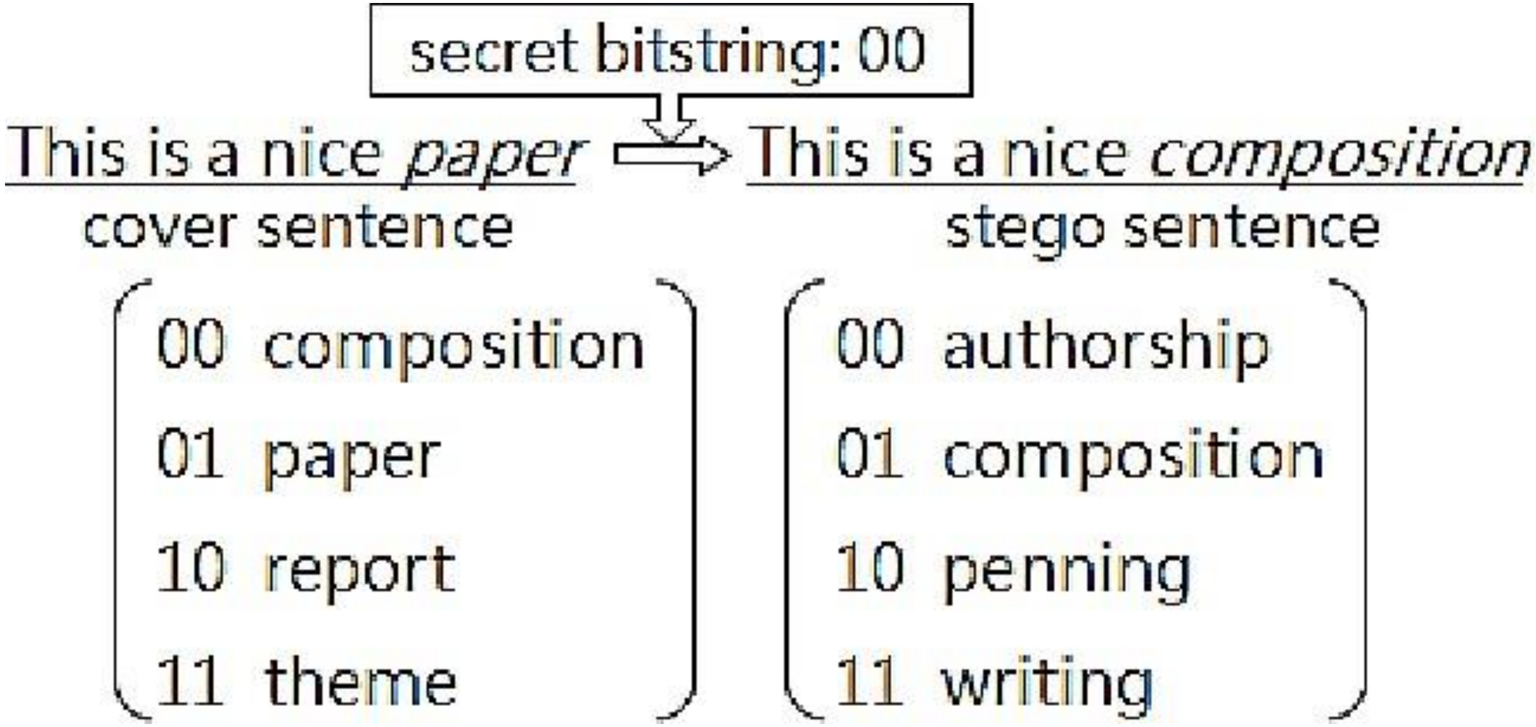
Free space for secret files : 7.8 MB

	Secret file name	Size (MB)
	D:\SecretFiles\SecretFile1.pdf	3.4 MB
	D:\SecretFiles\SecretFile2.doc	0.2 MB
	D:\SecretFiles\SecretFile3.jpg	< 0.1 MB

Output directory : C:\Users\Jospin\Documents\

Steganography





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:

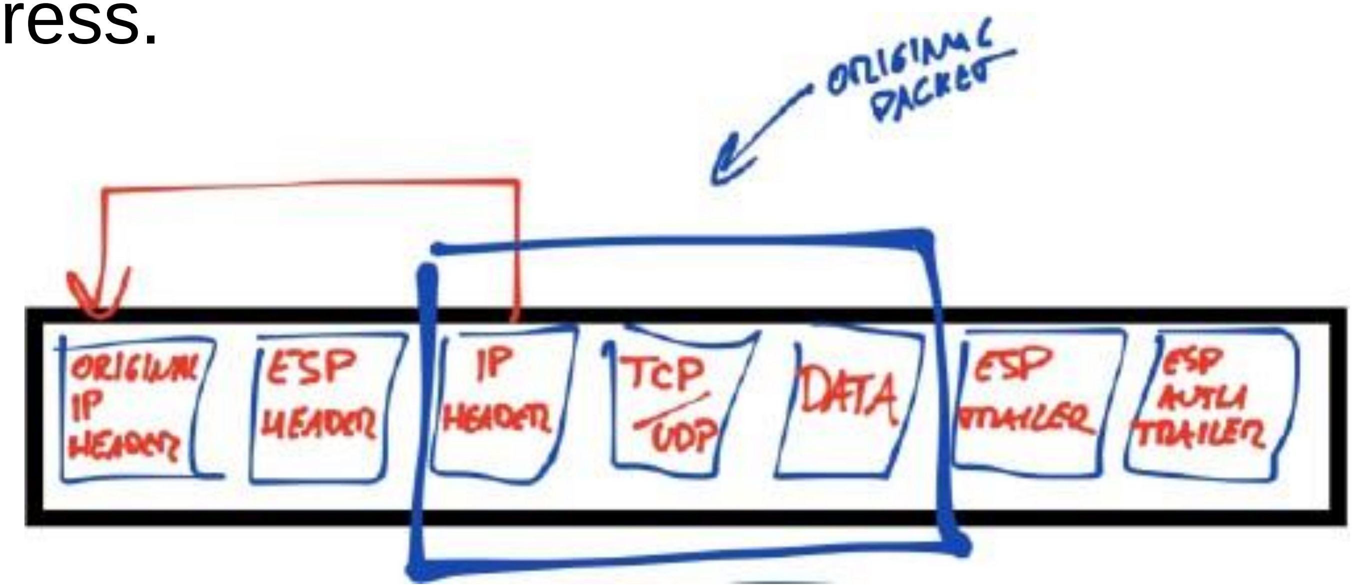
- Host Protected Areas (HPA) and Device Configuration Overlay (DCO) areas of modern ATA hard drives
- Data hidden in these areas is not visible to the BIOS or OS, but it can be extracted with special tools

Tunneling

- This method uses encapsulation to allow private communications to be exchanged over a public network.
- The data packets will flow from public networks, thus generating no suspicion.
- **Example:**
  - Using a Virtual Private Network (VPN), which encrypts the data for security reasons.
- To eliminate such **attacks**, **organizations must continuously monitor their encrypted network connections**.

Tunneling

- Encapsulating (Packaging/ Placing) entire packet in another packet of same or higher layer.
- Placing IP Packet with Private Address inside the IP Packet with Global Address.



VPN-Virtual Private Network

- **A means of carrying private traffic over a public network**.
- Connects two private networks, over a public network, to form a virtual network
- Virtual means two private networks seem to be seamlessly connected to each other.
- Seemingly part of a single virtual private network (although physically they are two separate networks).
- **Benefits: connectivity, security, privacy**
- The VPN should provide the same connectivity and privacy you would find on a typical local private network.

VPN

- Placing packet of one layer into packet of another layer.
- Usually Packets of Higher Layers are encapsulated by Packets of lower Layer.

Onion Routing

- The process of sending messages which are encrypted in layers, denoting layers of an onion, is referred to as onion routing.
- Data packet goes through several networking nodes where every layer of encryption gets peeled off.
- With the stripping of the final layer, the message gets closer to reaching its destination.
- The message remains anonymous to the entire message delivery chain except the nodes placed after the source and before the destination.

https://www.sciencedirect.com/science/article/abs/pii/S0379073819301082

Onion Routing

- One of the best practices to fight against onion routing is to use reverse routing.
- This elimination process is time-consuming but can be used to defeat onion routing.

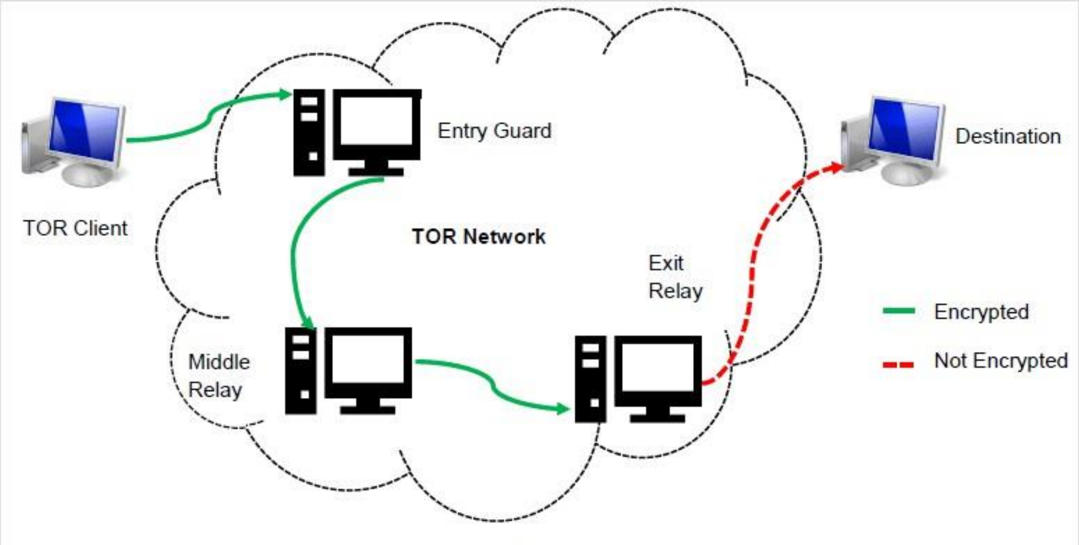
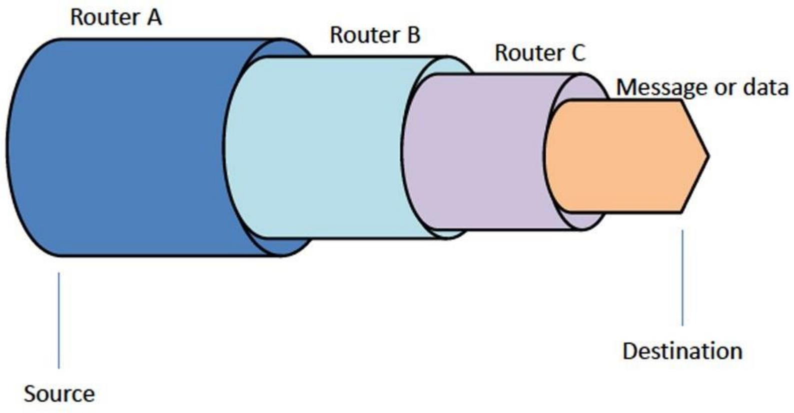


Fig 1. TOR Circuit



Obfuscation

- A technique that makes a message difficult to understand because of its ambiguous language is known as obfuscation.
- This method uses jargon and ingroup phrases to communicate.
- Could be intentional and unintentional.
- Objective of obfuscation is to reduce the risk of exposure.
- Can be done by altering the signature or fingerprint of malicious code.

https://www.digitalforensics.com/blog/obfuscation-and-detection-techniques/

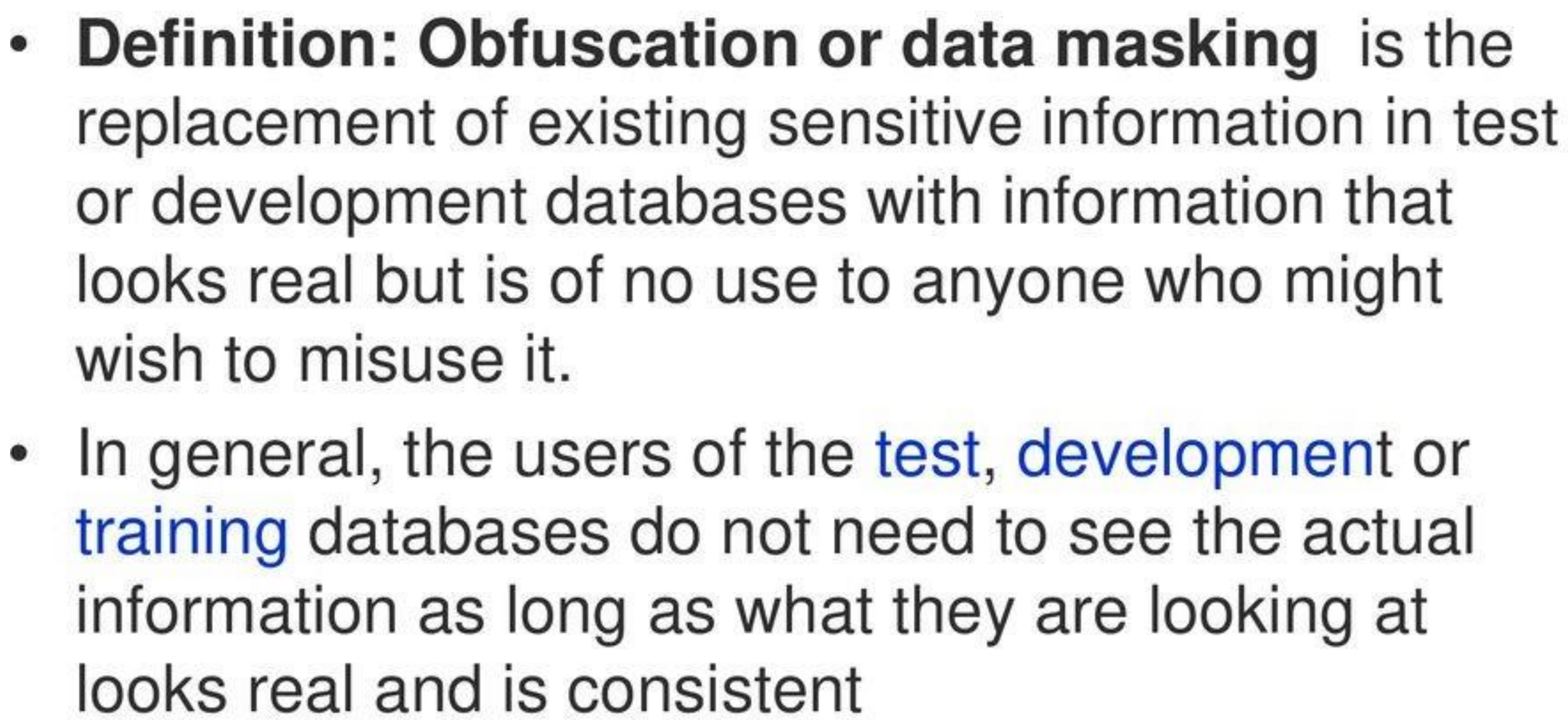
http://cet4862.pbworks.com/w/file/fetch/69342454/Craiger,%20Swauger,%20and%20Marberry.pdf

Obfuscation

- Attackers try to make forensics investigations more difficult and resource-consuming.
- To deter attack obfuscation is preventing a host from being compromised in the first place.
- De-obfuscation is the same as countering onion routing. Removing layers exposes clean and readable code.

https://info-savvy.com/anti-forensics-techniques-trail-obfuscation-artifact-wiping-encryption-encrypted-network-protocols-and-program-packers/

Obfuscation



- **Definition: Obfuscation or data masking** is the replacement of existing sensitive information in test or development databases with information that looks real but is of no use to anyone who might wish to misuse it.
- In general, the users of the test, development or training databases do not need to see the actual information as long as what they are looking at looks real and is consistent

Spoofing

- The act of disguising communication to gain access to unauthorized systems or data.

- Spoofing can be performed through emails, phone calls, and websites.
- Two most common ways of spoofing are:
  - IP Spoofing
  - MAC Spoofing

Spoofing

- IP Spoofing –
  - Perpetrators use a different IP address to hide their system’s IP address for initiating malicious activities.
  - Generally, this type of spoofing intends to carry out a distributed denial of service (DDoS).
  - It can be performed either manually or by the use of tools.
- MAC Spoofing –
  - MAC addresses usually cannot be changed, but with technical skills, it is not impossible.
  - With MAC spoofing, cyber attackers use fake MAC addresses.
  - This is one of the difficult spoofing methods to counter.

Spoofing

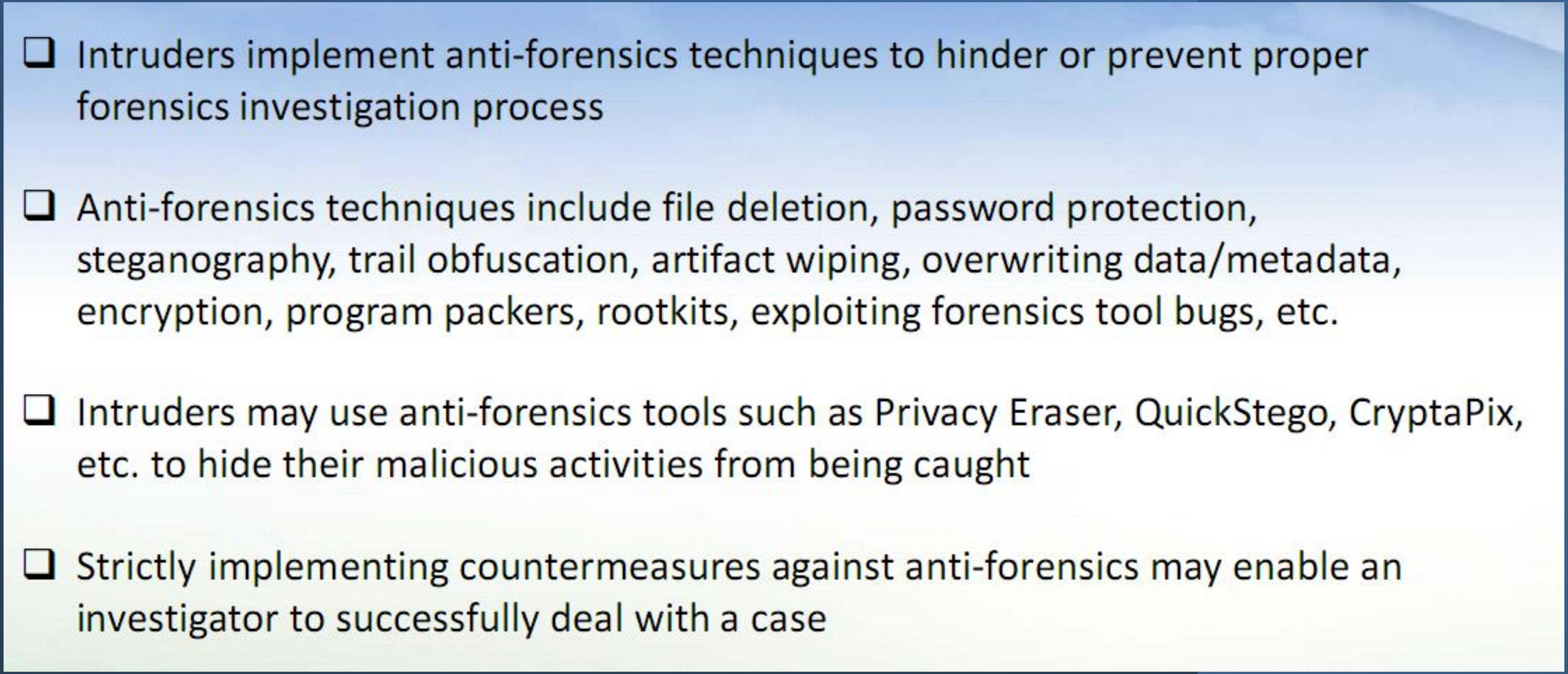
- Other types of spoofing include ARP spoofing, DNS spoofing, email spoofing, and many more.

- Forensic investigators have many tools and techniques to identify spoofing, e.g.
  - examining email headers in the case of email spoofing
  - investigating wireless access point activities in case of MAC spoofing, and likewise.

How to Defend against Anti-Forensics?

- **Preventive**
  - Firewalls, Access control, Regular patching, Secure configuration, Anti-malware software, training and awareness
- **Detective**
  - Detective systems can prove invaluable.
  - SIEM, EDR, SOC.
- **Responsive**
  - Forensic investigators must be suitably qualified and up to date with the latest anti-forensics techniques and digital forensic software.
  - Have a clear cyber incident response plan that, among other things, states when to escalate a security event.

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

Class Activity

Open the Google drive link shared on WhatsApp

Explore tools, manual and slides

References

- ✓ https://info-savvy.com/anti-forensics-techniques-that-minimize-footprint/
- ✓ https://www.anti-forensics.com/
- ✓ https://digital-forensics.enterprisesecuritymag.com/cxoinsight/evaluating
  challenges-and-impacts-of-antiforensics--nid-1054-cid-59.html
- ✓ https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1145&context=msi
  a_etds
- ✓ https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9116399
- ✓ CHFI v9

ANY QUESTIONS