Unit 3: Evidence Management and Anti-Forensics

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you will be able to understand:

- Difference between physical and digital evidence
- Detail procedure of seizure proceedings by Investigation officer
- What are challenges to cyber forensics
- Definition of Anti-forensics and its types

1.2 DIGITAL EVIDENCE

In this chapter, we will understand the different basic concepts related to the entire technical investigation of digital evidence and its management.

Digital evidence or electronic evidence is ***"any probative information stored or transmitted in digital form that a party to a court case may use at trial".*** Section 79A of IT (Amendment) Act, 2008 defines electronic form evidence as "any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones and digital fax machines"

1.3 DIFFERENCE BETWEEN PHYSICAL AND DIGITAL EVIDENCE

Digital Evidence	Physical Evidence
It can be duplicated and the duplicated copy can be analyzed as if it was original.[62]	It cannot be duplicated as Digital Evidence
Modification or Tampering of Digital Evidence can be easily identified by using appropriate Software by comparing with the original.	If any modification or Tampering is done it would be highly difficult to identify the changes happened.
It cannot be destroyed easily. Even if the evidence is destroyed, recovery is possible(not all times)	If the Evidence is destroyed it is highly impossible to bring back to its original form.

[62] Scientific Working Group on Digital Evidence (SWGDE) of the National Center for Forensic Science (NCFS). Best Practices for Computer Forensics V2, 2006a. Retrieved From the World Wide Web on 07/07/12: URL <http://ncfs.org/swgde/documents/swgde2006/Best_Practices_for_Computer_Forensics%20V 2.0.pdf>

It facilitates working on duplicate copies of the digital media, original along with copies will still remain to help the investigators in the event of damage to the copies.	Since duplication is not possible, once the evidence is destroyed, the evidence cannot remain.
Less Tangible when compared with physical evidence	Tangible in nature

1.4 SOURCES OF DIGITAL EVIDENCE

Following are the different sources of digital evidence:-

VOLATILE EVIDENCE

Volatile data will include information about the running process, network connections, clipboard contents, and data in memory.[63]

Volatile Evidence can be found on:

- Ram Memory
- Temporary file System / Swap Space
- Cache Memory etc.

NON-VOLATILE EVIDENCE

The data can be retrieved even when the computer is switched off.

Examples of Non-Volatile Data commonly includes:

[63] Mason, D, Carlin, A, Ramos, S, Gyger, A, Kaufman, M, Treichelt, J, (2007) Is the open way a better way? Digital forensics using open source tools. The Computer Society. 1-10

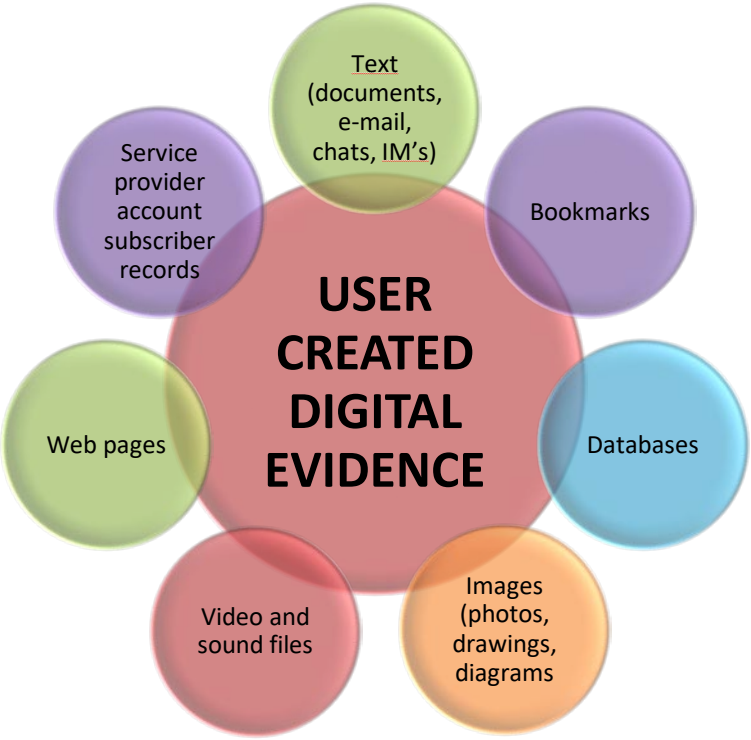
- Flash Memory
- Hard Disk, Magnetic Tape
- Optical Disc etc.

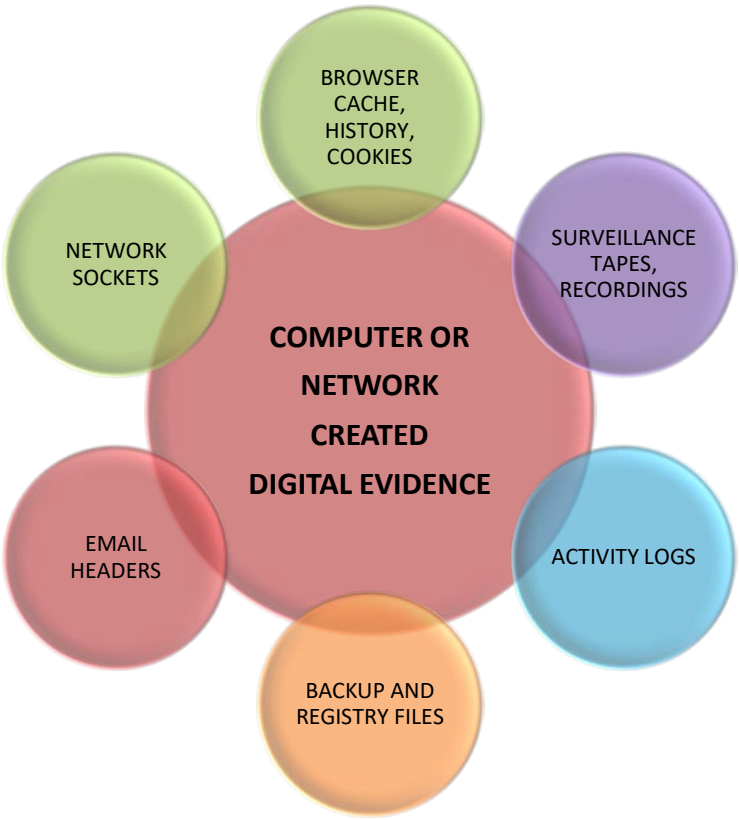
Examples of digital evidence:

- Emails
- Web Server Logs
- Digital Photographs
- ATM Transaction logs
- Word processing documents
- Instant message histories
- Files saved from accounting
- Programs
- Spreadsheet
- Internet browser histories
- Databases,
- The contents of Computer Memory,
- Computer backups,
- Computer printers
- Global Positioning System tracks,
- Logs from a hotel's electronic door locks,
- Digital video or audio files.

We can categorize digital evidence in two main subcategories:-

1. User-Created digital evidence
2. Computer Created Digital evidence


Text (documents, e-mail, chats, IM's)
Service provider account subscriber records
Bookmarks
USER CREATED DIGITAL EVIDENCE
Web pages
Databases
Video and sound files
Images (photos, drawings, diagrams


BROWSER CACHE, HISTORY, COOKIES
NETWORK SOCKETS
SURVEILLANCE TAPES, RECORDINGS
COMPUTER OR NETWORK CREATED DIGITAL EVIDENCE
EMAIL HEADERS
ACTIVITY LOGS
BACKUP AND REGISTRY FILES

1.5 SEIZURE PROCEEDINGS

Following is the probable list of equipment's which can be seized in technology-based crimes

- CPU
- Hard Disk
- Floppy Drive
- CD's & DVD's Drive
- USB Memory Sticks
- Pen Drives
- Memory Cards
- Portable Hard Disks
- Tape Drives
- Various Hi-Tech Gadgets
- & in some cases Cell phone / Mobile Handset

PANCHANAMA (SEIZURE MEMO)

The legal provisions empowering the investigation officer to conduct search and seizure are provided under section 165Cr PC and section 80 of the ITAA 2008. Panchanama and seizure procedure is as important in cybercrime investigation as in any other crime. Make sure one of the technical people from the responder side along with two independent witnesses is part of the search and seizure proceedings, to identify the equipment correctly and to guide the IO and witnesses.[64] Please refer to the notes made during the pre-investigation assessment for cross verifying and correctly documenting the technical information regarding the equipment, networks and other communication equipment at the scene of the crime. Time Zone/System Time Play a very curtail role in the entire investigation. Please make sure this information is noted carefully in the panchanama, from the system that is in "switch on" condition. Please Don't switch On any device. Please make sure serial number is allotted for each device and the same should be duly noted not only in the panchanama but also in the chain of custody and digital

[64] Kruse W Heiser J G (2001) Computer Forensics: Incident Response Essentials (1st ed), Addison Wesley Professional. USA

evidence form.[65] Make sure each device is photographed before starting of the investigation process at their original place along with a respective reference. Make sure the photograph hard disk drive or any other internal part along with the system, once removed from the system

Capture the information about the system and dada you are searching and seizing in the Panchanama . Brief the witnesses regarding the tools used to perform search and seizure of digital evidence

Hence following are the important points to be considered while drafting a seizure memo.

- Power to search, seize under Section 165 Cr PC and, Section 80 of the ITAA 2008.
- Independent Witnesses.
- Time Zone/System Time
- The serial number for each seized device
- Chain of Custody & Digital Evidence Collection forms

DIGITAL EVIDENCE COLLECTION FORM

Digital Evidence Collection form is one of the most important elements of the forensic process. It is necessary that the steps taken for collection should be accurate and repeatable with the same results every time it is done. For this to happen, proper documentation of the process used for collection needs to be maintained for every device that is collected. This documentation should contain all the information about the evidence that is visible to the naked eye. It should contain information about the kind of software and version used and the time when the collection process started and ended. This documentation called as the Digital Evidence Collection (DEC) form thus consists of the information on the evidence and the media on which the evidence is being copied to.[66]

DIGITAL EVIDENCE COLLECTION (DEC) FORM SHOULD HAVE THE FOLLOWING FIELDS

- System Information

[65] Casey, E (2004). Digital Evidence and Computer Crime, Forensic science, Computers and the Internet. Academic Press, London, UK

[66] Cuardhuain S O, (2004) An Extended Model of Cyber Crime Investigation Journal of Digital Evidence. Vol 3 Issue 1

- Type — Device type which is produced to extract evidence like desktop, laptops, etc.
- Manufacturer — The device manufacturer information to be documented.
- Model Number — The device model number information to be documented.
- Serial Number / any unique identification feature — The device serial number information to be documented.
- BIOS Date/Time — BIOS information of the device.
- Property Form Number / Evidence Number — Unique number assigned to each device for easy identification by the unit after it is brought to the police station/unit.
- It is one most important element of the forensic process.
- Proper documentation of the process used for the collection of evidence must be maintained for every device collected.
- This document should contain all information about the evidence visible to naked eye
- It should contain information about the kind of software and version used and the time collection process started and ended.
- During the process of digital evidence collection, if the IO is trained or has a technical expert to support him, He should forensically image the evidence and acquire the hash value and note the same in DEC form as well as in panchanama.
- The process, the tool and the hashing algorithm used should be reflected in DEC form the report generated by forensic tool should form as an enclosure to DEC.

CHAIN OF CUSTODY

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence. These would be people who have seized the equipment, people who are in charge of transferring the evidence from the crime scene to the forensic labs, people in charge of analysing the evidence, and so on. As electronic evidence is easy to tamper or to get damaged, it is necessary for us to know exactly who, when, what, where, and why was the evidence transferred to the Concerned person.[67]

[67] Yong-Dal S, (2008) New Digital Forensics Investigation Procedure Model. Proceedings of Fourth International Conference on Networked Computing and Advanced Information Management. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4624063>

- It refers to the documentation that shows the people who have been entrusted with the evidence.
- These would be people who have seized the device-
  - people who are in charge of transferring the evidence from the crime scene to forensic lab,
  - people in charge of analysing the evidence and so on.
- Due to the sensitive nature of digital evidence, it necessary to know who, when, what, where, and why was the evidence transferred to the concerned person.
- It is difficult to prove the integrity of the evidence if the chain of custody is not properly maintained.
- Lack of integrity in the process of custody and absence of appropriate documentation in this regard, will not be detrimental to the cybercrime investigation, during the trial but also, exposé the IO's to criminal liability under section 72 of the ITAA 2008.

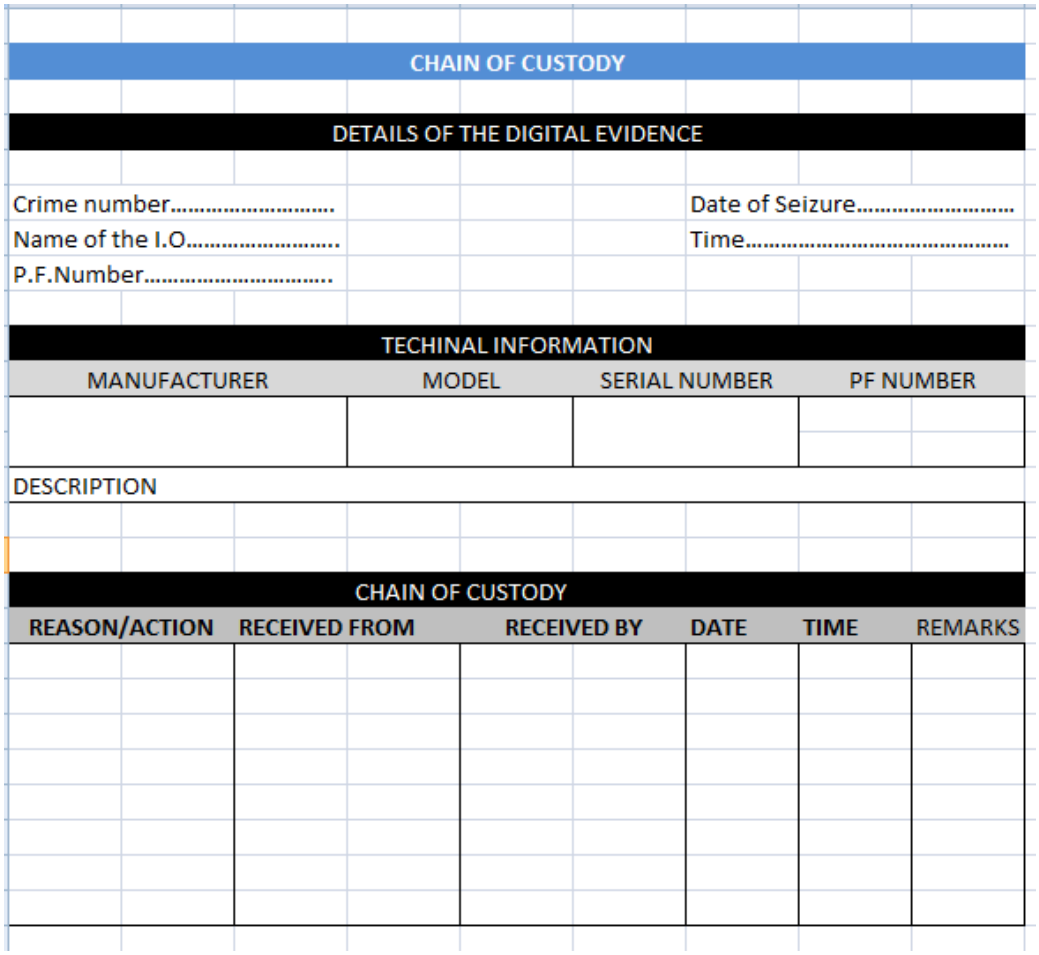
IMPORTANT POINTS TO CONSIDER FOR CHAIN OF CUSTODY

- Physically inspect the storage medium – take photographs and systematically record observations[68]
- Guard against hazards like theft and mechanical failure.
- Use good physical security and data encryption.
- Keep multiple copies in a different location.
- Protect digital magnetic media from external electric and magnetic fields.
- Ensure protection of optical media from scratches.
- Account for all people with physical or electronic access to the data.
- Keep the number of people involved in collecting and handling the devices and the data to a minimum.
- Always accompany evidence with their chain of custody forms.
- Give the evidence positive identification all the times i.e. legible and written with termagant ink.

[68] Kuchta K J, (2000) 'Computer Forensics Today Law, Investigations and Ethics Available from: <http://www.liv.ac.uk/library/ohecampus/>

- Establishing the integrity of the seized evidence through the forensically proven procedure by a technically trained IO.
- The seized original evidence can be continued to check for its integrity by comparing its hash value to identify any changes to it.

FORM



CHAIN OF CUSTODY

DETAILS OF THE DIGITAL EVIDENCE

Crime number..... Date of Seizure.....

Name of the I.O..... Time.....

P.F.Number.....

TECHINAL INFORMATION

MANUFACTURER	MODEL	SERIAL NUMBER	PF NUMBER

DESCRIPTION

CHAIN OF CUSTODY

REASON/ACTION	RECEIVED FROM	RECEIVED BY	DATE	TIME	REMARKS

1.6 CHALLENGES TO FORENSICS

The Direct Challenge to forensic is the use of anti-forensics by the attacker. In this chapter, we will see the different methods by which the forensic investigation process may become difficult for the investigating officer.

1.7 INTRODUCTION TO ANTI-FORENSICS

The objective of cyber forensics is to collect, analyse the evidence from the seized devices in such ways so that they are admissible in a court of law. There are many computer criminals are aware of this issue. They try to find a countermeasure technique and even developing tools specifically designed to conceal their activities and destroy digital evidence. Anti-forensics is a collection of tricks and techniques that are used and applied with the clear aim of forestalling the forensic investigation. Anti- forensics works in the exact opposite direction of the cyber forensics. These methods make investigation much time consuming or more expensive to carry out.

1.8 DEFINITION

Harris (2006) stated that anti-forensic is a method used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system.

Pajeket all (2012) defining the methodologies used against the computer forensics processes are collectively called Anti-Forensics.[69]

John Barbara defines anti-forensic as an approach to manipulate, erase, or obfuscate digital data or to make its examination difficult, time-consuming, or virtually impossible.

1.9 PRIMARY GOALS OF ANTI-FORENSICS

- Avoiding detection of the traces created by a certain incident.
- To make it hard or impossible to retrieve information.
- Increase the time of forensic examination.
- Casting doubt on a forensic report or testimony.
- Misguide the forensic investigator by producing false results.

[69] Liu, V, & Brown, F. (2006, April 3). Bleeding-Edge Anti-Forensics. Presentation at InfoSec World 2006. Retrieved September 11, 2007, from <stachliu.com/files/InfoSecWorld_2006-K2-Bleeding_Edge_ AntiForensics.ppt>

- Intentional destruction of possible evidence.
- Create inaccuracy in forensic findings.

1.10 TYPES OF ANTI-FORENSIC TECHNIQUES

In order to act against the forensics one has to have sound knowledge of cyber forensics. The basic stages involve in cyber forensics are identification, collection, preservation, analysis and presentation to make digital evidence admissible in a court of law. So, basically all kind of anti-forensic technique is trying to break in one of this stage.[70]

CREATING PROBLEMS AT THE EVIDENCE SOURCE

This technique is used to create more hurdles for a forensic investigator. It may result in time increased for analysis of the evidence. Sometimes this technique does not let computing device create any logs or the traces related to any event over the device. This technique also suggests permanent deletion of the information within the device. Following are some of the methods used to apply this technique

A. ***Disk Wiping*** **-** Data can be still recovered if it is a normal delete over computing device. Hence disk wiping technology is been used by an attacker to make data recovery more difficult task for the forensic investigator.

B. ***Disabling the log creating system software*** **-** Disabling tool called as Event manager which is responsible for creation of source such as modified windows registry, logon user, computer setting, application software installation etc.

C. ***Live CDs and Virtual Disks*** **-**

Live CDs are an operating system distribution that boots and runs from a read-only device. Live CDs typically have a window system, web browser and SSH client, and run with virtual memory disabled.

[70] Metasploit LLC. (2007a). Metasploit Anti-forensics home page. Retrieved September 11, 2007, from <http://www.metasploit.com/projects/antiforensics/>

D. ***Bootable USB tokens*** **-** These are similar to a Live CD except that the operating system is contained within an attachable USB device. These tokens can typically store more information than CDs and allow information to be saved, generally via encryption.

E. ***Virtual Machine*** **-** These are the "client" operating systems run inside a virtualization program such as VMWare Player, Parallels, or Microsoft Virtual PC.

F. ***Cloud Storage*** **-** In this method fraudster creates the anonymous account with different email service providers and keep the data on their cloud service which is entirely different computers. An attacker may also use some cloud services for launching an attack.

G. Live CDs are an operating system distribution that boots and runs from a read-only device. Live CDs typically have a window system, web browser and SSH client, and run with virtual memory disabled.

HIDING EVIDENCE

It mainly addresses the methods by which the data can be hidden inside the device or over transit. It makes cyber examination process more difficult. The more hurdles have been created when multiple data hiding techniques are clubbed together.[71]

A. ***Encryption*** **-** Encryption techniques transparently encrypt data when it is written to the disk and decrypt data when it is read back.
B. ***Steganography*** **-** Steganography can be used to embed encrypted data in a cover text to avoid detection. This technique mainly used to embeds text in JPEG, MBP, MP3, WAV and other multimedia files.
C. ***Slack space*** **-** Data can also be hidden in unallocated or otherwise unreachable locations that are ignored by the current generation of forensic tools.

[71] Palmer, G (2001, November 6) A Road Map for Digital Forensics Research. Digital Forensic Research Workshop (DFRWS) Technical Report (DTR) T001-01 Final. Retrieved September 11, 2007, from <http://www.dfrws.org/2001/dfrws-rm-final.pdf>

D. Data can also be hidden in unallocated or otherwise unreachable locations that are ignored by the current
E. Generation of forensic tools
F. ***HPA*** **-**Information can be stored in the Host Protected Area (HPA) and the Device Configuration Overlay (DCO) areas of modern ATA hard drives. Data in the HPA and DCO is not visible to the BIOS or operating system, although it can be extracted with special tools.
G. ***Program packers*** **-** Packers are commonly used by attackers so that attack tools will not be subject to reverse engineering or detection by scanning.
H. ***Onion Routing*** **-** It combines both approaches with multiple layers of encryption so that no intermediary knows both ends of the communication and the plaintext content.

DESTROYING EVIDENCE

This technique is used to make the evidence useless or unavailable. Evidence can be partly or completely destroyed.

A) ***Bad Sector*** **-** Attacker intentionally converts good sectors into bad sectors to make data recovery difficult in this scenario.
B) ***Disk degaussing*** **-** It is a process by which a magnetic field is applied to a digital media device. This may partially or permanently wipe the data within the disk.

COUNTERFEITING EVIDENCE

If computer criminal can found digital evidence he can create inconsistency in data retrieval, it will not credible enough to be presented in a court. Examples of this are timestamp modification and hash collision. Hence counterfeiting can be used to create fake evidence to mislead the forensic investigator.

a) OVERWRITING DATA

Overwriting programs typically operate in one of three modes:

- The program can overwrite the entire media.
- The program can attempt to overwrite individual files. This task is complicated by journaling file systems. The file itself may be overwritten, but portions may be left in the journal.

- The program can attempt to overwrite files that were previously “deleted” but left on the drive.

b) OVERWRITING METADATA

Meta Data is the extra relevant data created by files which may contain vital information. For example, it is frequently possible to determine which files the attacker accessed, by examining file “access” times for every file on the system. Metadata over wiring can confuse the investigator regarding the timeline analysis of the evidence.

c) ARTEFACT WIPING

The methods used in artefact wiping are tasked with permanently eliminating particular files or entire file systems. This can be accomplished through the use of a variety of methods that include disk cleaning utilities.

1.11 CONCLUSION

Sometimes, the process of deleting the evidence itself also create other evidence. Hence it’s up to the persistent effort of the forensic investigator. Attacker sometimes ends up creating more traces while trying to use these anti-forensics techniques. Investigation of such expert criminals is very much possible. The golden rule here is not a single crime is full proof. The mistake is the part of human behaviour and criminals are no exception to this. Hence even though there are such techniques available forensics investigation achieve its goal and reveals the facts.

1.12 LET’S SUM UP

In this chapter, we have studied the meaning of digital evidence and the difference between physical and digital evidence. We also studied the detailed procedure of seizure proceedings by Investigation officer. Finally, we ended our discussion with the primary goals of anti-forensics and the different types of anti-forensics.

1.13 FURTHER READING

- https://www.academia.edu/26177741/Computer_Anti-forensics_Methods_and_Their_Impact_on_Computer_Forensic_Investigation
- Beer, Richard & Stander, Adrie & Van Belle, Jean-Paul. (2014). Anti-Forensic Tool Use and Their Impact on Digital Forensic Investigations: A South African Perspective.

- Conlan, Kevin & Baggili, Ibrahim & Breitinger, Frank. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation. 18. 10.1016/j.diin.2016.04.006.
- R. Harris, "Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem," Digital Investigation, vol. 3, pp. 44-49, 2006.
- C. S. J. Peron and M. Legary, "Digital anti-forensics: emerging trends in data transformation techniques," in Proceedings of E-crime and Computer Evidence Conference, Technip, Monaco, 2005.

1.14 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is digital evidence?

Digital evidence or electronic evidence is "any probative information stored or transmitted in digital form that a party to a court case may use at trial".

2. What are the 2 sources of digital evidence?

- Volatile Evidence
- Non-Volatile Evidence

3. What is anti-forensics?

Anti-forensic is a method used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system.

4. What are the primary goals of anti-forensics?

- Avoiding detection of the traces created by a certain incident.
- To make it hard or impossible to retrieve information.
- Increase the time of forensic examination.
- Casting doubt on a forensic report or testimony.
- Misguide the forensic investigator by producing false results.
- Intentional destruction of possible evidence.
- Create inaccuracy in forensic findings.

1.15 ACTIVITY

Explain the different types of anti-forensic techniques along with a case study in which one of the technique is used? (1000 words)