# GOVERNMENT POLYTECHNIC COLLEGE NEDUMANGAD

SEMINAR REPORT ON

## COMPUTER FORENSICS

Submitted by

ANANDHU A S

(Register no: 20131360)

**DEPARTMENT OF COMPUTER ENGINEERING**

**2022-2023**

# GOVERNMENT POLYTECHNIC COLLEGE NEDUMANGAD

## CERTIFICATE

Certified that this is a bonafied report of the seminar entitled "**COMPUTER FORENSICS**" submitted by **ANANDHU A S** (Regno:20131360) to the **GOVERNMENT POLYTECHNIC COLLEGE NEDUMANGAD** towards the partial fulfilment for the award of **DIPLOMA IN COMPUTER ENGINEERING** under the Directorate of Technical Education Government of kerala during the academic year 2022-2023

**A.PREVATHI**
HEAD OF THE DEPARTMENT
DEPT. OF COMPUTER ENGG.

GPTC, NEDUMANGAD

**REENA S**
LECTURER
DEPT. OF COMPUTER ENGG.
GPTC, NEDUMANGAD

Internal Examiner

External Examiner

## ACKNOWLEGMENT

I have immense pleasure to present this seminar on "COMPUTER FORENSICS",a topic of my personal interest.Firstly I thank 'God',the almighty for giving me such a great opportunity to present this seminar.

First and foremost I would like to express my sincere gratitude to our Principal **Mr. SHAMMNAD M S** and **Ms. A.P REVATHI** ( Head of Computer Engineering Department) for their support and encouragement through our endeavour. Equally we thank **Ms. REENA S**, our guide for her constant guidance and motivation. This would have been impossible without the assistance , co-operation and support by our beloved lectures Ms. SAJEENA , Mr. DIPU JOSE , Mr. SHAMNNAD for their immense support.

I sincerely express my gratitude to other non-teachers staff and my dear friends for their valuable co-operation and help. I will be failing in duty if I do not acknowledge with grateful thanks to the authors of the references and other literatures referred to this seminar. Last but not the least, I am very much thankful to my parents who guided me in every step which I took.

Contents Page no.

# What is Computer Forensics?

1. 1 COMPUTER FORENSICS

“computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable.”(Rodney Mckemmish 1999).

From the above definition we can clearly identify four components:-

IDENTIFYING

This is the process of identifying things such as what evidence is present, where and how it is stored , and which operating system is being used. From this information the investigator can identify the appropriate recovery methodologies, and the tools to be used.

PRESERVING

This is the process of preserving the integrity of digital evidence, ensuring the chain of custody is not broken. The data needs to preserved (copied) on stable media such as CD-ROM, using reproducible methodologies. All steps taken to capture the data must be documented. Any aw changes to the evidence should be documented, including what the change was and the reason for the change. You may need to prove the integrity of the data in the court of law.

ANALYSING

This is the process of reviewing and examining the data. The advantage of copying this data onto CD-ROMs is the fact it can be viewed without the risk of accidental changes, therefore maintaining the integrity whilst examining the changes

PRESENTING

This is the process of presenting the evidence in a legally acceptable and understandable manner. If the matter is presented in court the jury who may have little or no computer experience, must all be able to understand what is presented and how it relates to the original, otherwise all efforts could be futile.

Far more information is retained on the computer than most people realize. Its also more difficult to completely remove information than is generally thought. For these reasons (and many more), computer forensics can often find evidence or even completely recover, lost or deleted information, even if the information was intentionally deleted.

The goal of computer forensics is to retrieve the data and interpret as much information about it as possible as compared to data recovery where the goal is to retrieve the lost data.

# Characteristics

IDENTIFYING

PRESERVING

ANALYZING

PRESENTING

## NEEDS OF COMPUTER FORENSICS

- To produce evidence in the court that can lead to the punishment of the actual.
- To ensure the integrity of the computer system.
- To focus on the response to hi-tech offenses, started to intertwine.

# HISTORY OF COMPUTER FORENSICS

Began to evolve more than 30 years ago in US when law enforcement and military investigators started seeing criminals get technical. Over the next decades, and up to today, the field has exploded. Law enforcement and the military continue to have a large presence in the information security and computer forensic field at the local, state and federal level. Now a days, Software companies continue to produce newer and more robust forensic software programs. And law enforcement and the military continue to identify and train more and more of their personnel in the response to crimes involving technology.

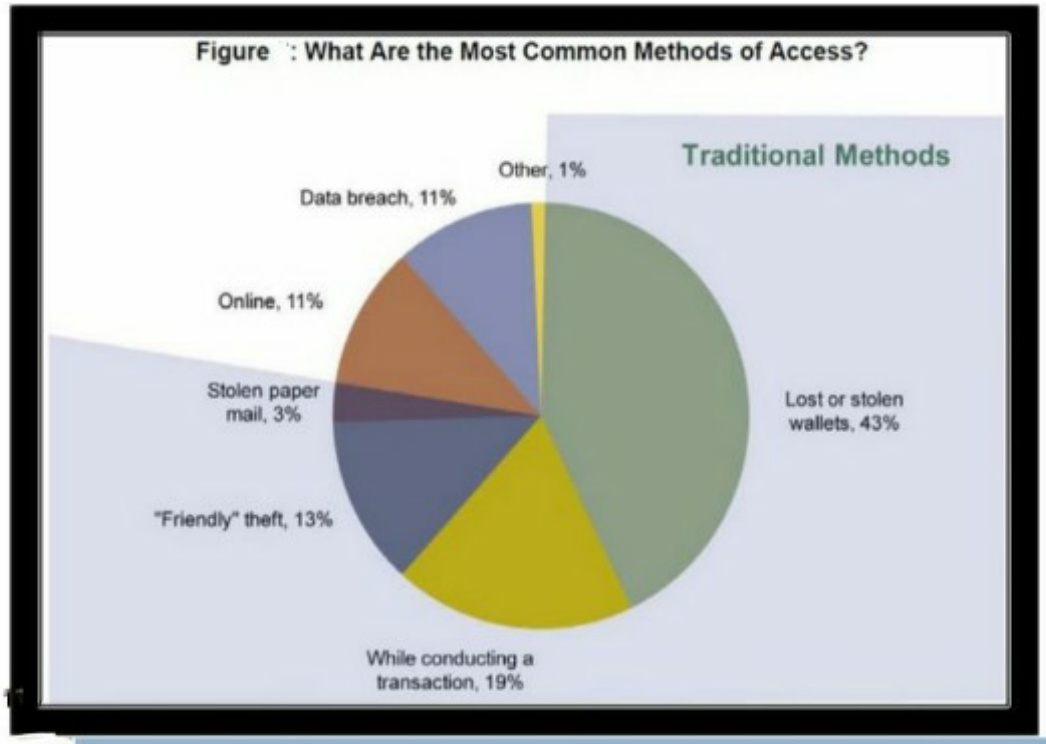
## GOAL OF COMPUTER FORENSICS

- The main goal of computer forensic experts is not only to find the criminal but also to find out the evidence and the presentation of the evidence in a manner that leads to legal action of the criminal.

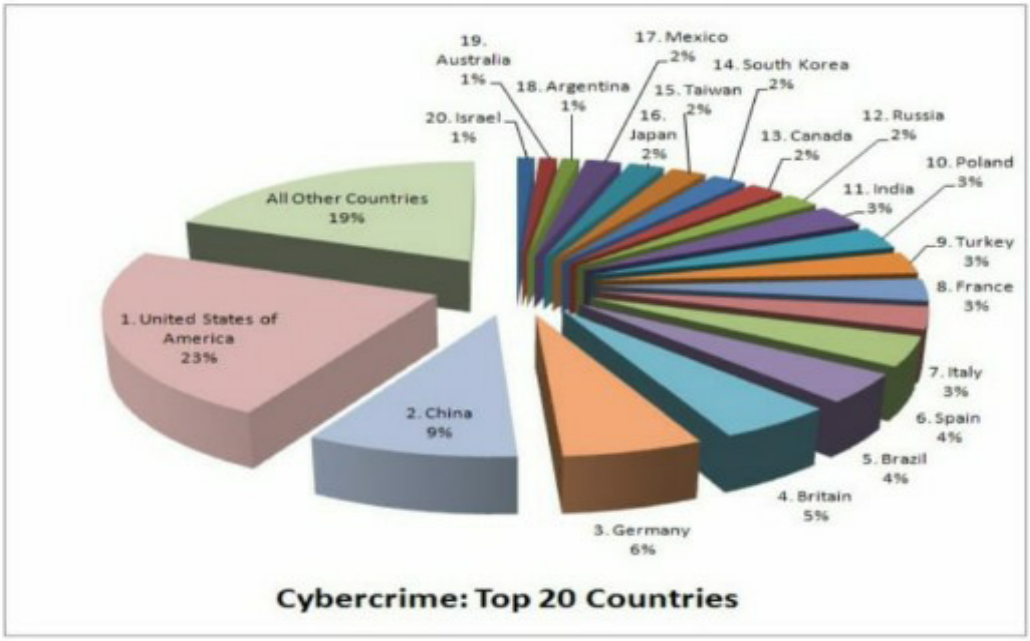
## CYBER CRIME & EVIDENCE

- CYBER CRIME

  Cyber crime occurs when information technology is used to commit or conceal an offence.




# Cybercrime: Top 20 Countries



# Evidence

- An item does not become officially a piece of evidence until a court admits it.
- Much of forensics practice concerns how to collect, preserve and analyze these items without compromising their potential to be admitted as evidence in a court of law.

## DIGITAL EVIDENCE

- "Any data that is recorded or preserved on any medium in or by a computer system or other similar device, that can be read or understand by a person or a computer system or other similar device. It includes a display, print out or other output of that data."

## TYPES OF DIGITAL EVIDENCE

1) PERSISTANT DATA

Meaning data that remains intact when the computer is turned off. E.g. hard drives, disk drives and removable storage devices (such as USB drives or flash drives).

2) VOLATILE DATA,

Meaning data that would be lost if the computer is turned off. E.g. deleted files, computer history, the computer's registry, temporary files and web browsing history.

## 5 RULES OF EVIDENCES

1) Admissible

Must be able to be used in court or elsewhere.

2) Authentic

Evidence relates to incident in relevant way.

3) Complete (no tunnel vision)

Exculpatory evidence for alternative suspects.

4) Reliable

No question about authenticity & veracity.

5) Believable

Clear, easy to understand, and believable by a jury.

# TOP 10 LOCATION FOR EVIDENCE

1) Internet History Files
2) Temporary Internet Files
3) Slack/Unallocated Space
4) Buddy lists, personal chat room records, others saved
5) News groups/club lists/posting
6) Settings, folder structure, file names
7) File Storage Dates
8) Software/Hardware added
9) File Sharing ability
10) E-mails

## Methodology

1) Shut Down the Computer
2) Document the Hardware Configuration of The System
3) Transport the Computer System to A Secure Location
4) Make Bit Stream Backups of Hard Disks and Floppy Disks
5) Mathematically Verify Data on All Storage Devices
6) Document the System Date and Time
7) Make a List of Key Search Words
8) Evaluate the Windows Swap File
9) Evaluate File Slack
10) Evaluate Unallocated Space (Erased Files)
11) Search Files, File Slack and Unallocated Space for Key Words
12) Document File Names, Dates and Times
13) Identify File, Program and Storage Anomalies
14) Evaluate Program Functionality
15) Document Your Findings

# Applications

* FINAL FRAUD DETECTION

* CRIMINAL PROSECUTION

*CIVIL LITIGATION

* CORPORATE SECURITY POLICY AND VIOLATIONS

## Who Uses Computer Forensics?

- Criminal Prosecutors
- Rely on evidence obtained from a computer to prosecute suspects and use as evidence.

- Civil Litigations
- Personal and business data discovered on a computer can be used in fraud, harassment, or discrimination cases.

- Private Corporations
- Obtained evidence from employee computers can be used as evidence in harassment, fraud, and embezzlement cases.

- Law Enforcement Officials
- Rely on computer forensics to backup search warrants and post-seizure handling.

- Individual/Private Citizens
- Obtain the services of professional computer forensic specialists to support claims of harassment, abuse, or wrongful termination from employment.

## Skills Required For Computer Forensics Application

- Programming or computer-related experience
- Broad understanding of operating systems and applications
- Strong analytical skills
- Strong computer science fundamentals
- Strong system administrative skills
- Knowledge of the latest intruder tools
- Knowledge of cryptography and steganography
- Strong understanding of the rules of evidence and evidence handling
- Ability to be an expert witness in a court of law

## Conclusion

- With computers becoming more and more involved in our everyday lives, both professionally and socially, there is a need for computer forensics.
- This field will enable crucial electronic evidence to befound, whether it was lost, deleted, damaged, or hidden, and used to prosecute individuals that believe they have successfully beaten the system.

## References


- www.google.com
- www.wikipedia.com
  - www.studymafia.org