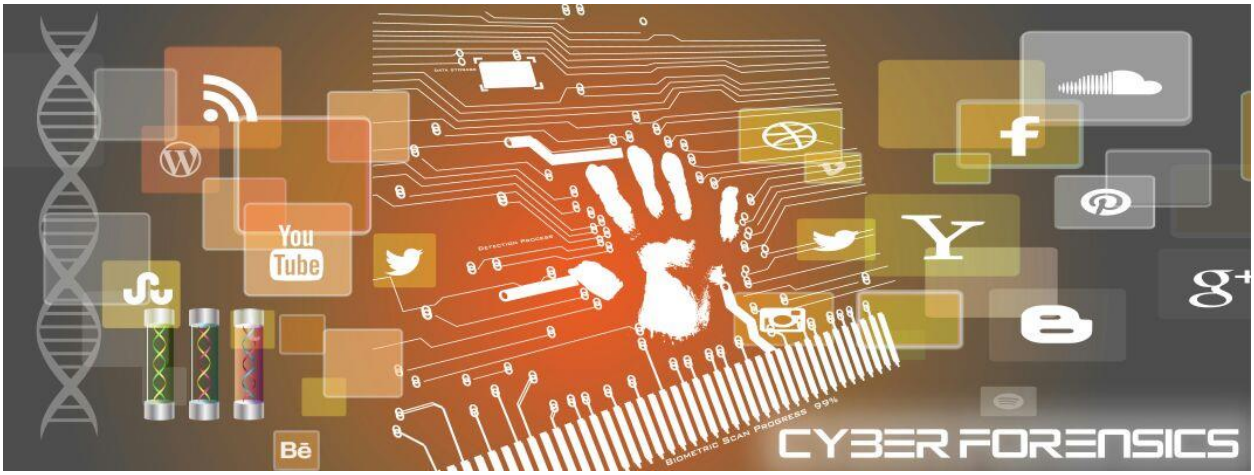



# Training Workshop Outline

| | |
|---|---|
| **Title** | Cyber Forensics |
| **Duration** | 40 hours |
| **Tuition Fees** | USD 2,500 |

# Cyber Forensics

## Course Overview:

The term cyber-crime no longer refers only to hackers and other external attackers. Almost all every case of financial fraud or employee misuse involves a very strong element of computer-based evidence. The entire workshop is driven by hands-on exercises and case studies to ensure that all aspects have a real-life scenario-based approach.

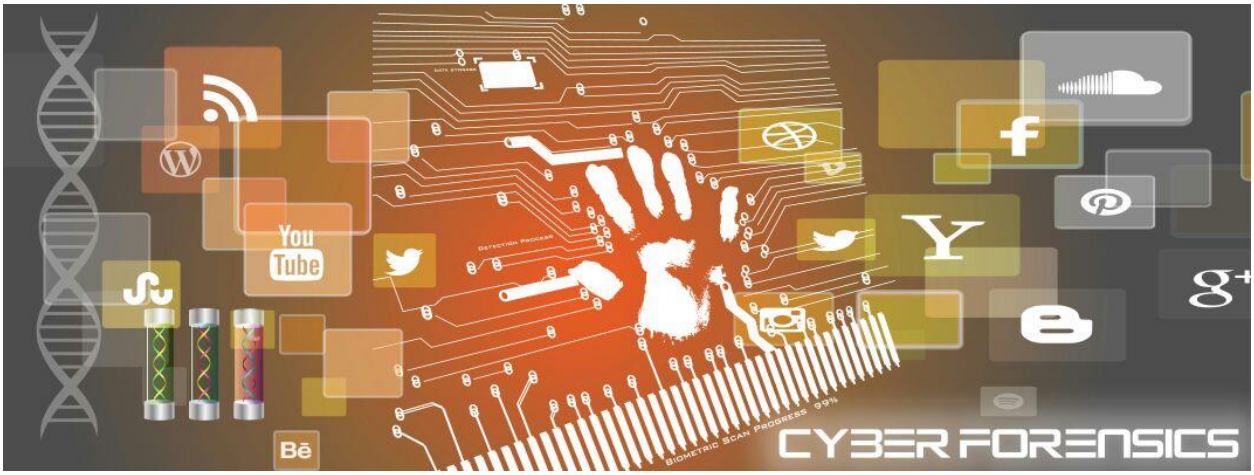
## Benefits:

This program addresses the key questions of:

· What should one do when there is a suspicion of a computer-based crime?

· What tools and techniques are most likely to yield the right set of clues?

· Demonstration with the worlds' leading forensics tool – Encase




## Target Audience:

- College Students

- Auditors and financial fraud examiners

- Chief Security Officers and Chief Technology Officers

- Professionals seeking a career in computer forensics and Cyber Crime Investigations

- Security and Network Administrators

## Prerequisites:

- Basic Knowledge of Computer and Internet

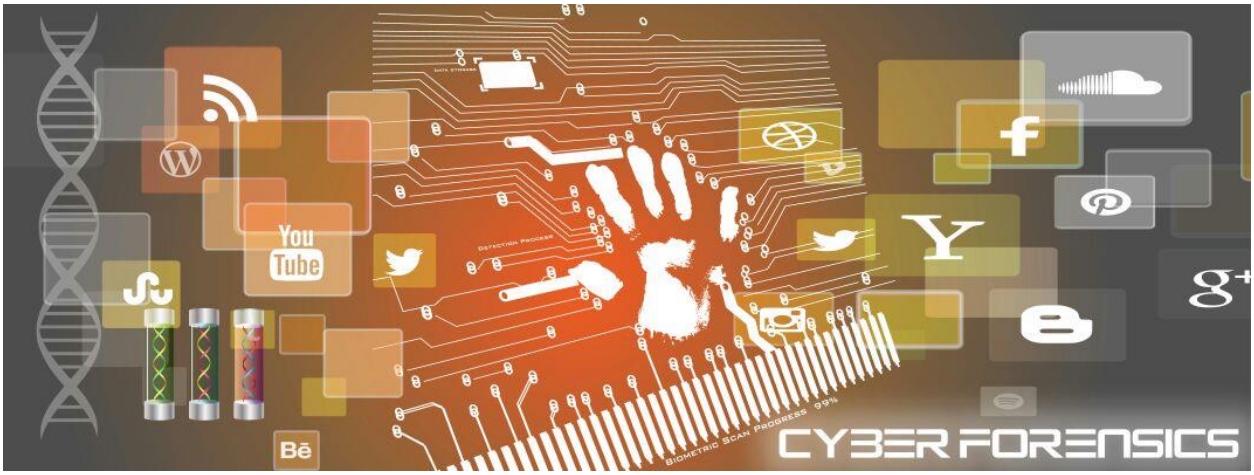
## Course Length:

- 40 Hours

## What will you learn?

Using practical scenarios based artifacts with the latest disk technologies, you will learn the following:

- The principles and guidelines for computer and mobile forensic investigations
- The process of evidence seizure and continuity
- The forensic acquisition of an electronic device
- How data is stored on electronic media
- The core functionality of forensic examination software
- How to identify platform specific forensic artifacts.

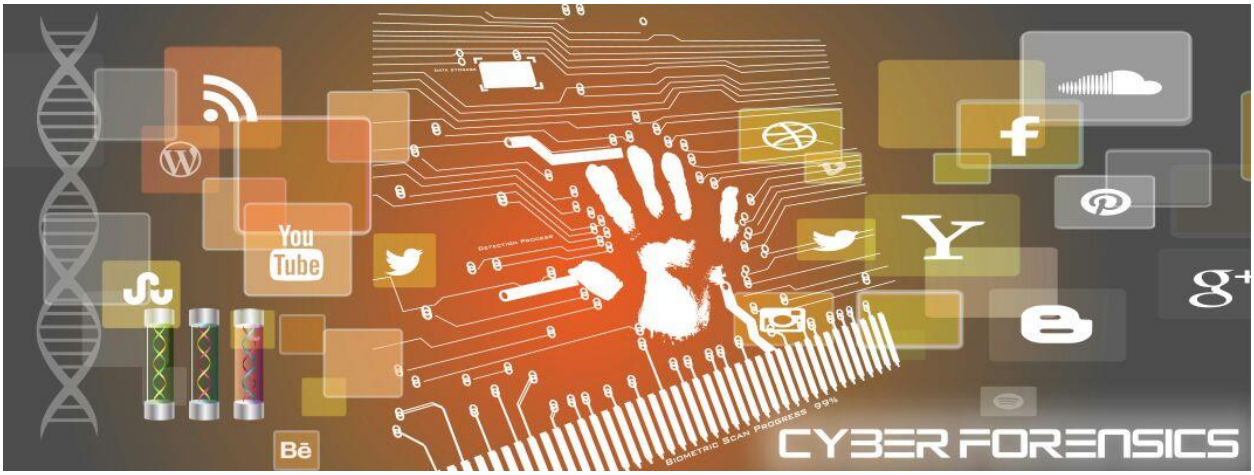



## The course will also provide answers to many questions including:

- What is Cyber Forensics?
- How and where is data actually stored on a device?
- What is the difference between forensic imaging and cloning?
- Is keyword searching an effective way to identify data on a device?
- How is hashing used in forensics?
- What happens when a user deletes a file?
- How can 'Private' web-browsing work?
- Can data be recovered after a 7 pass overwrite?
- Is there a backdoor to passwords and encryption?
- Who was using a computer on a particular occasion?
- How can I identify if and when a user edited or accessed a file?
- How to perform cyber forensic examination in a legal manner?
- Do we have any shortcuts to catch the attacker?
- How to perform mobile, computer, network and cloud forensics?

## Tools of trade:

1. Encase
2. FTK
3. Blackdog
4. UFED
5. Taruntala
6. Mobiledit
7. Oxygen Forensic
8. sleuth kit




9. x-ways
10. Passware kit forensics
11. AD-Triage
12. Easeus Data Recovery
13. x1 social discovery toolkit
14. Falcon Imager
15. Foca
16. Irecovery
17. Wipe Master
18. Drivespy

Note: These are a partial set of tools to be used and many lightweight tools will be used in the lab sessions for different purposes.

## Module 1: Computer Forensics in Today's World

1.1 Define computer forensics

1.2 Discuss the evolution of computer forensics

1.3 Explain the objectives and benefits of computer forensics

1.4 Discuss forensic readiness planning in detail

1.5 Explain cyber crimes

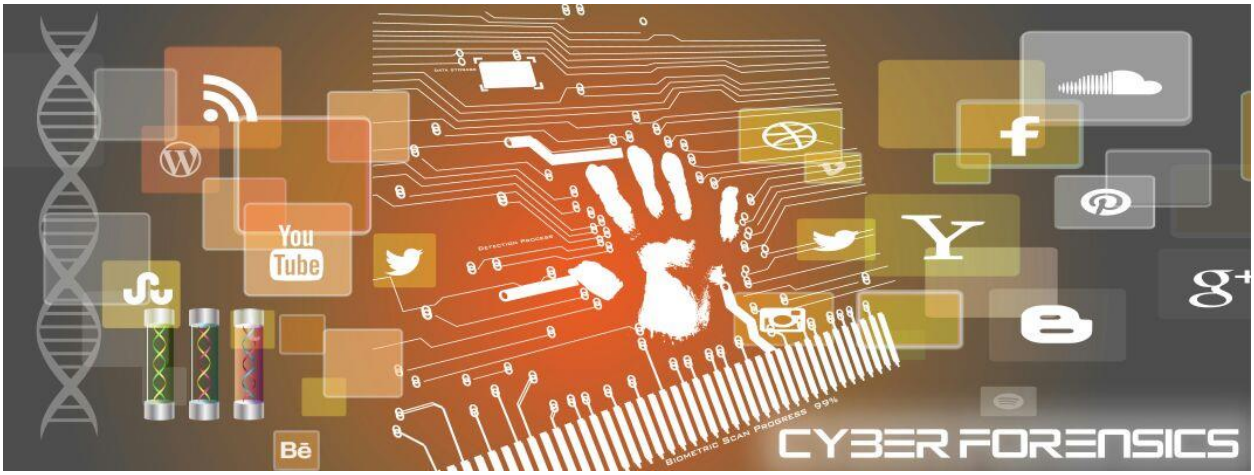
1.6 Examine various computer crimes

1.7 What is cybercrime investigation?

1.8 Explain the key steps and rules in forensic investigation

1.9 What is the role of a forensics investigator?

1.10 How to access computer forensics resources




1.11 Describe the role of digital evidence in forensic investigation

1.12 Understanding Corporate Investigations

1.13 Explain the key concepts of Enterprise Theory of Investigation (ETI)

1.14 Discuss various legal issues and reports related to computer forensic investigations

## Module 2: Computer Forensics Investigation Process

2.1 Provide an overview of computer crime investigation process

2.2 Describe computer forensic investigation methodology

2.3 Summarize the steps to prepare for a computer forensic investigation

2.4 How to obtain a search warrant

2.5 How to evaluate and secure a scene

2.6 How to collect and secure the evidence in a forensically sound manner

2.7 Explain the different techniques to acquire and analyze the data

2.8 Summarize the importance of evidence and case assessment

2.9 How to prepare the final investigation report

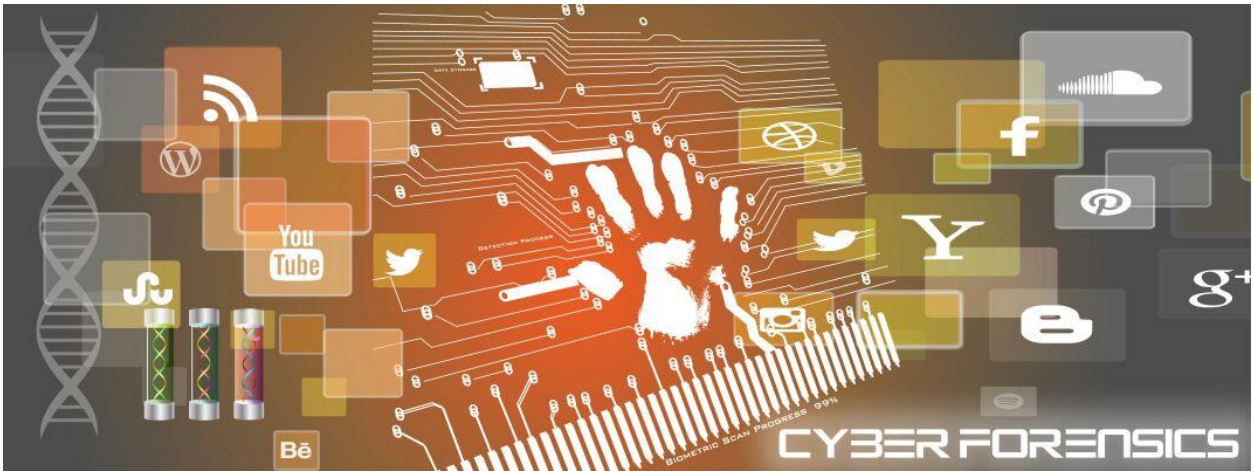
2.10 Testify in the Court as an Expert Witness

## Module 3: Searching and Seizing Computers

3.1 How to searching and seize computers without a warrant

3.2 Discuss the Fourth Amendment's "Reasonable Expectation of Privacy"

3.3 What is consent and discuss the scope of consent






3.4 Summarize the steps involved in searching and seizing computers with a warrant

3.5 Examine the basic strategies for executing computer searches

3.6 Discuss the Privacy Protection Act

3.7 Describe drafting the warrant and affidavit

3.8 Explain the post–seizure issues

3.9 Describe the Electronic Communications Privacy Act

3.10 What is voluntary disclosure?

3.11 Electronic Surveillance in Communications Networks

3.12 Discuss how content is different from addressing information

3.13 Provide an overview of evidence and authentication

## Module 4: Digital Evidence

4.1 Define digital evidence and explain its role in case of a computer security incident

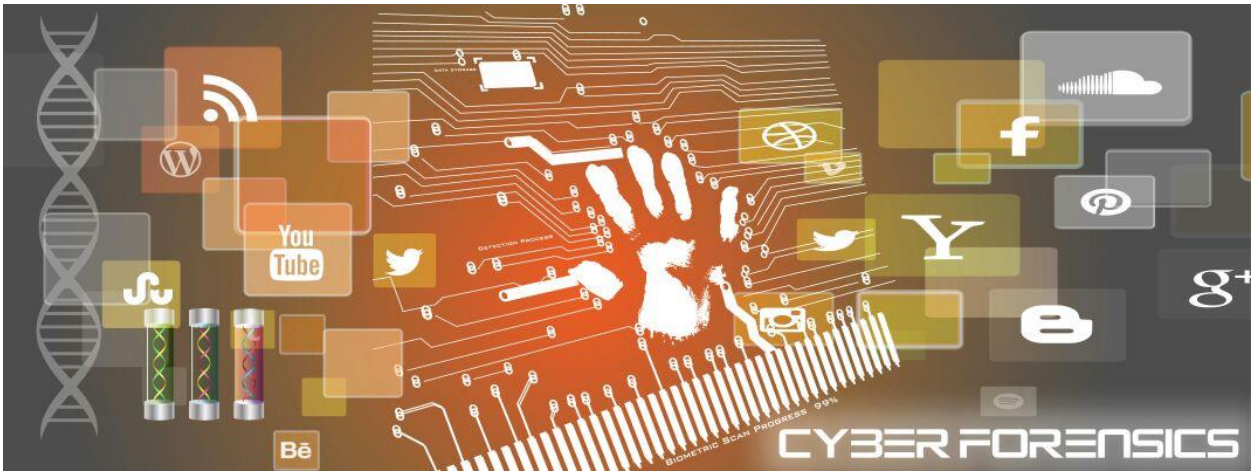
4.2 Discuss the characteristics of digital evidence

4.3 What are the various types of digital data?

4.4 What is best evidence rule?

4.5 Discuss federal rules of evidence

4.6 Summarize the international principles for computer evidence




4.7 Discuss about the Scientific Working Group on Digital Evidence (SWGDE)

4.8 What are the considerations for collecting digital evidence from electronic crime scenes?

4.9 Provide an overview of digital evidence examination process and steps involved

4.10 Explain electronic crime and digital evidence consideration by crime category

## Module 5: First Responder Procedures

5.1 Define electronic evidence

5.2 Who is first responder?

5.3 Provide an overview on how to collect and store the electronic evidence

5.4 Describe first responder tool kit and how to create it

5.5 How to get first response from laboratory forensic staff

5.6 Provide an overview on how to collect and secure the electronic evidence at crime scene

5.7 Explain how to conduct preliminary interviews

5.8 How to document electronic crime scene

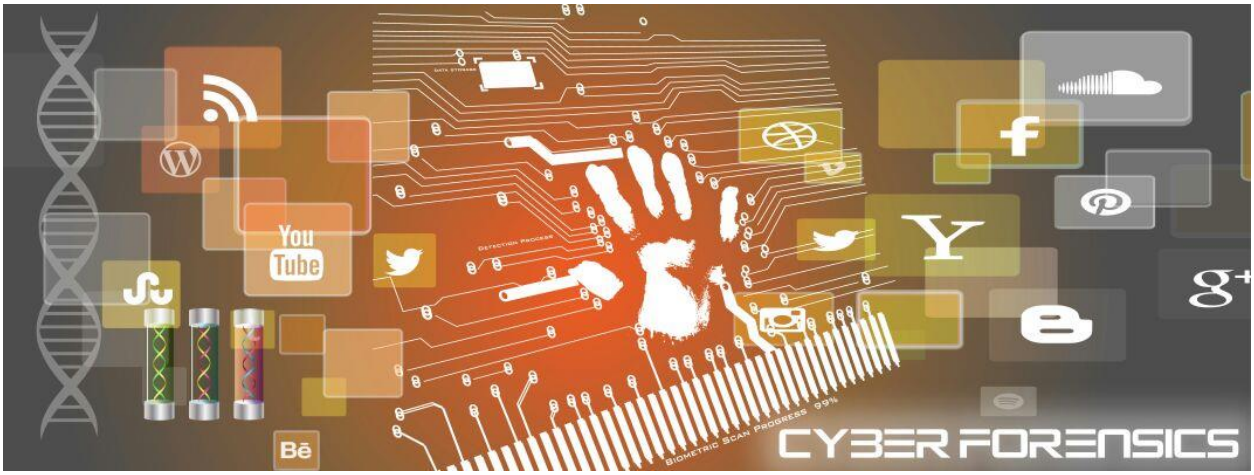
5.9 Explain how to collect and Preserve electronic evidence

5.10 Explain how to package and transport electronic evidence in a forensically sound manner

5.11 How to prepare report on crime scene

5.12 Provide a checklist for the first responders

5.13 Discuss the first responder's common mistakes




## Module 6: Computer Forensics Lab

6.1 How to set up a computer forensics lab

6.2 Discuss the investigative services in computer forensics

S M E X 63

– C O N F I D E N T I A L –

6.3 What are the basic hardware requirements in a forensics lab?

6.4 List and summarize various hardware forensic

6.5 Discuss the basic software requirements in a forensics lab

6.6 Summarize various software forensic tools

## Module 7: Understanding Hard Disks and File Systems

7.1 What is a hard disk drive?

7.2 Explain solid-state drive (SSD)

7.3 Provide an overview of physical and logical structure of a hard disk

7.4 Describe the various types of hard disk interfaces

7.5 Examine the components of a hard disk

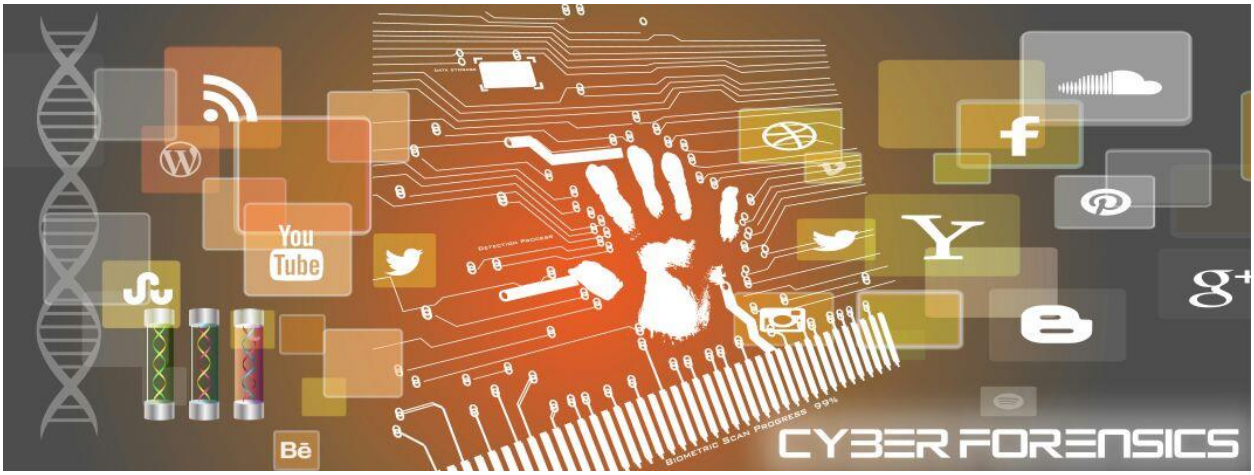
7.6 What are disk partitions?

7.7 Explain Windows and Macintosh boot process

7.8 What are file systems?

7.9 Explain various types of file systems

7.10 Provide an overview of Windows, Linux, Mac OS X, and Sun Solaris 10 file systems




7.11 Discuss about CD-ROM/DVD File System

7.12 Explain about RAID storage system and RAID levels

7.13 Explain file system analysis using the sleuth Kit

## Module 8: Windows Forensics

8.1 What is a volatile information?

8.2 Explain what network and process information is

8.3 Define non-volatile information

8.4 Describe memory dump

8.5 Parsing Process Memory

8.6 Describe different techniques for collecting nonvolatile information such as registry settings and event logs

8.7 Explain various processes involved in forensic investigation of a Windows system such as memory analysis, registry analysis, IE cache analysis, cookie analysis, MD5 calculation, Windows file analysis, and metadata investigation

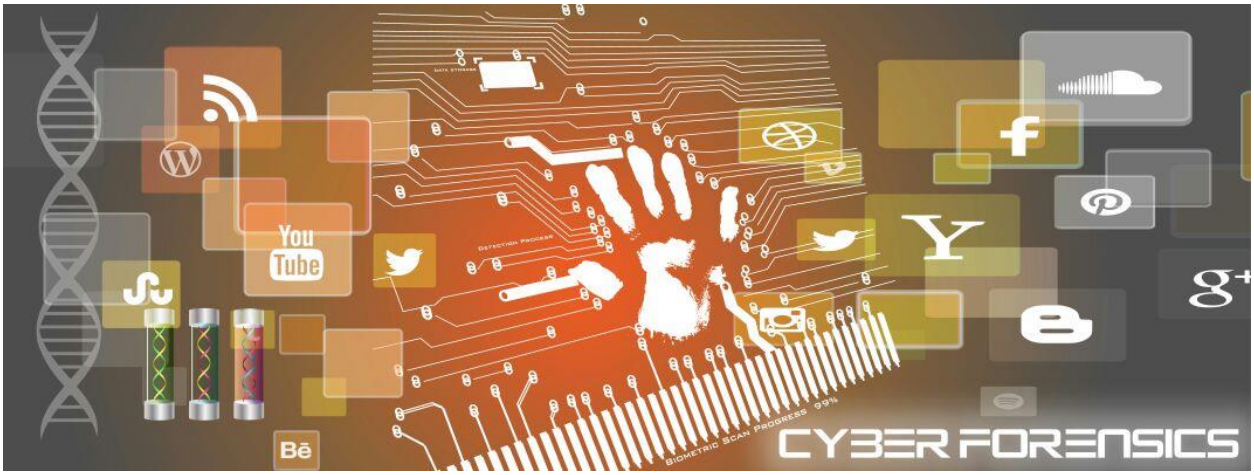
8.8 Provide an overview of IIS, FTP, and system firewall logs

8.9 Discuss the importance of audit events and event logs in Windows forensics

8.10 Explain the static and dynamic event log analysis techniques

8.11 Discuss different Windows password security issues such as password cracking

8.12 How to analyze restore point registry settings




8.13 Provide an overview of cache, cookie, and history analysis

8.14 How to evaluate account management events

8.15 How to search with event viewer

8.16 Discuss various forensics tools

## Module 9: Data Acquisition and Duplication

9.1 Define data acquisition and explain various types of data acquisition systems

9.2 Explain various data acquisition formats and methods

9.3 How to determine a best acquisition method

9.4 What is contingency planning for image acquisitions?

9.5 Describe static and live data acquisition

9.6 Provide an overview of volatile data collection methodology

9.7 Explain various types of volatile information

9.8 What are the requirements of disk imaging tool

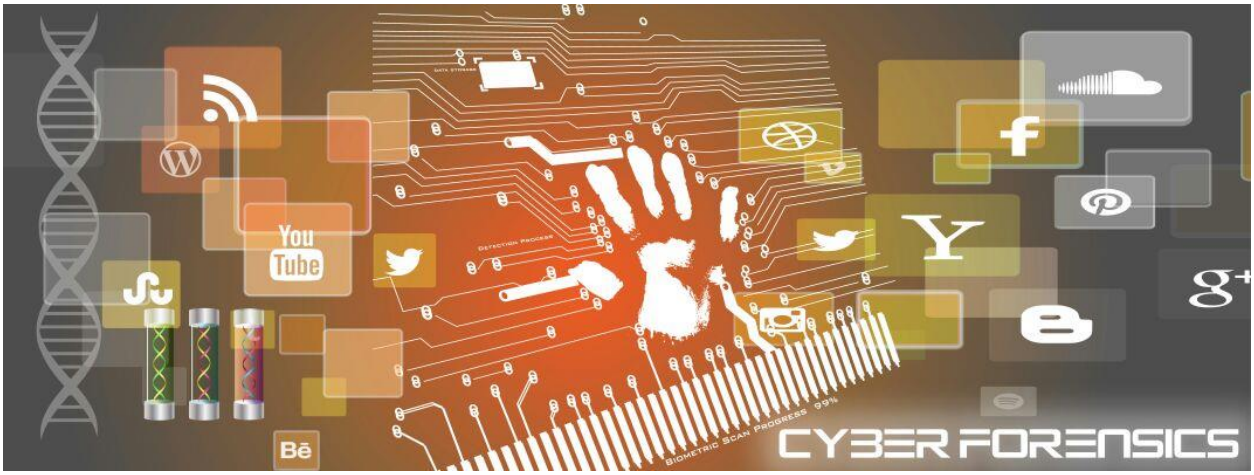
9.9 How to validate data acquisitions

9.10 Discuss Linux and Windows validation methods

9.11 How to acquire RAID Disks

9.12 Examine the best practices of acquisition

9.13 List various data acquisition software and hardware tools




## Module 10: Recovering Deleted Files and Deleted Partitions

10.1 Explain how to recover files in Windows, MAC, and Linux

10.2 Discuss file recovery tools for Windows, MAC and Linux

10.3 How to identify creation date, last accessed date of a file, and deleted sub-directories

10.4 How to recovering the deleted partitions and list partition recovery tools

## Module 11: Forensics Investigations Using Access Data FTK

11.1 What is Forensic Toolkit (FTK®) and discuss its various features

11.2 Explain FTK installation steps

11.3 Discuss about FTK Case Manager

11.4 How to restore an image to a disk

11.5 Explain FTK examiner user interface

11.6 How to verify drive image integrity

11.7 Discuss how to mount an image to a drive

11.8 Summarize the steps involved in creating a case

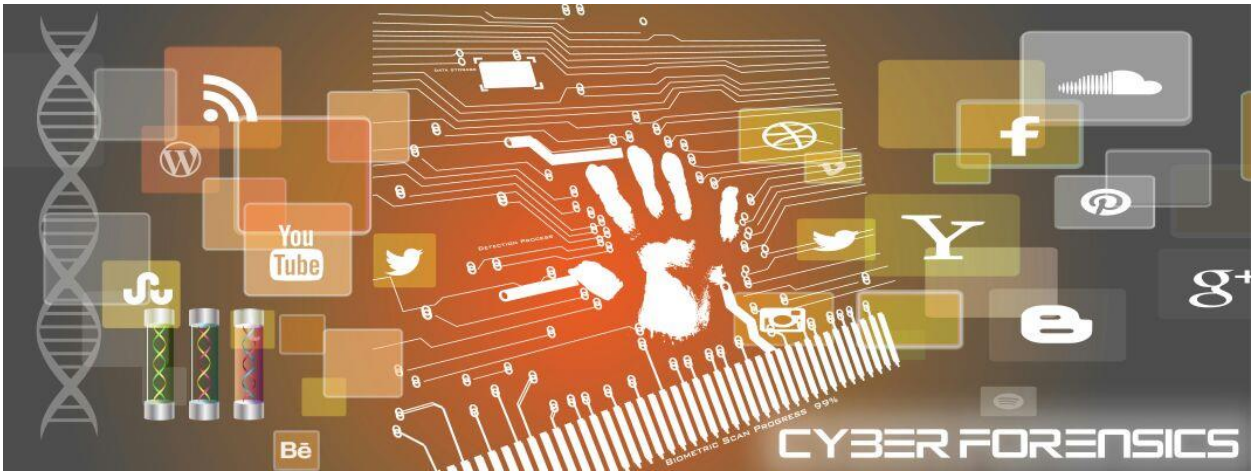
11.9 Discuss the functions of FTK interface tabs

11.10 Explain the steps involved in adding evidence to a case

11.11 1How to acquire local live evidence

11.12 Explain the steps involved in acquiring data remotely using remote device management system (RDMS)

S M E X 65






11.13 Discuss the steps involved in imaging drives

11.14 How to mount and unmount a Device

11.15 11Explain the steps involved in conducting an index search and live search

11.16 How to decrypt EFS Files and Folders

## Module 12: Forensics Investigations Using EnCase

12.1 Provide an overview of EnCase forensics

12.2 Discuss EnCase, its uses, and functionality

12.3 Discuss about EnCase forensics modules

12.4 How to install EnCase forensic

12.5 Explain how to configure EnCase

12.6 Provide an overview of case structure

12.7 What is case management?

12.8 How to add a Device to a Case and how to acquire a Device

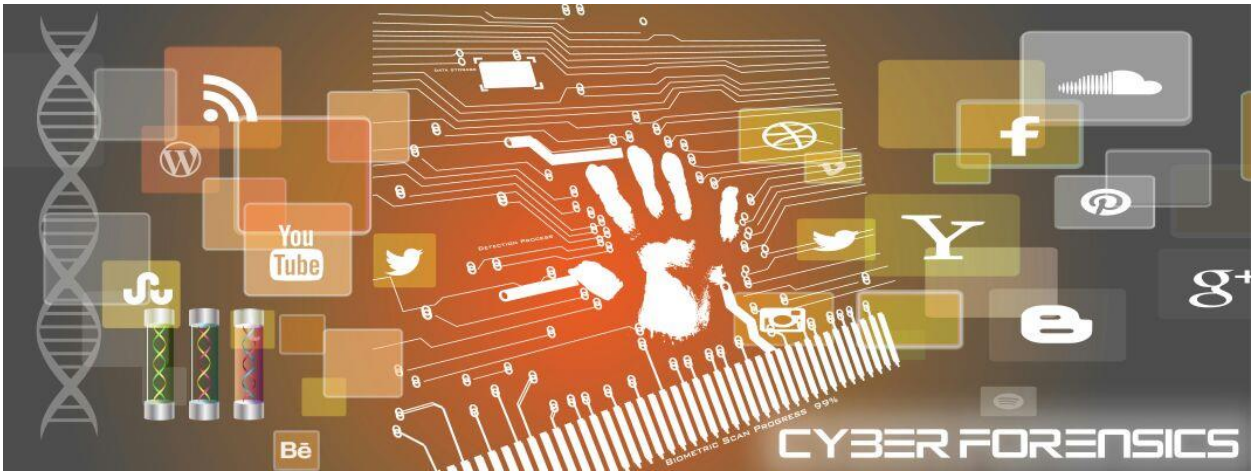
12.9 Explain the verification process of evidence files

12.10 What is a source processor?

12.11 How to set up case options

12.12 Discuss how to analyze and search files

12.13 Describe how to view file content




12.14 Provide an overview on bookmarks

12.15 How to create various types of bookmark

12.16 Explain how to create a report using the report tab

12.17 How to export a Report

## Module 13: Steganography and Image File Forensics

13.1 Summarize steganography and its types

13.2 List the application of steganography

13.3 Discuss various digital steganography techniques

13.4 What is Steganalysis?

13.5 How to Detect Steganography

13.6 List various steganography detection tools

13.7 Discuss about image file formats

13.8 How to compress data

13.9 How to process forensic image using MATLAB

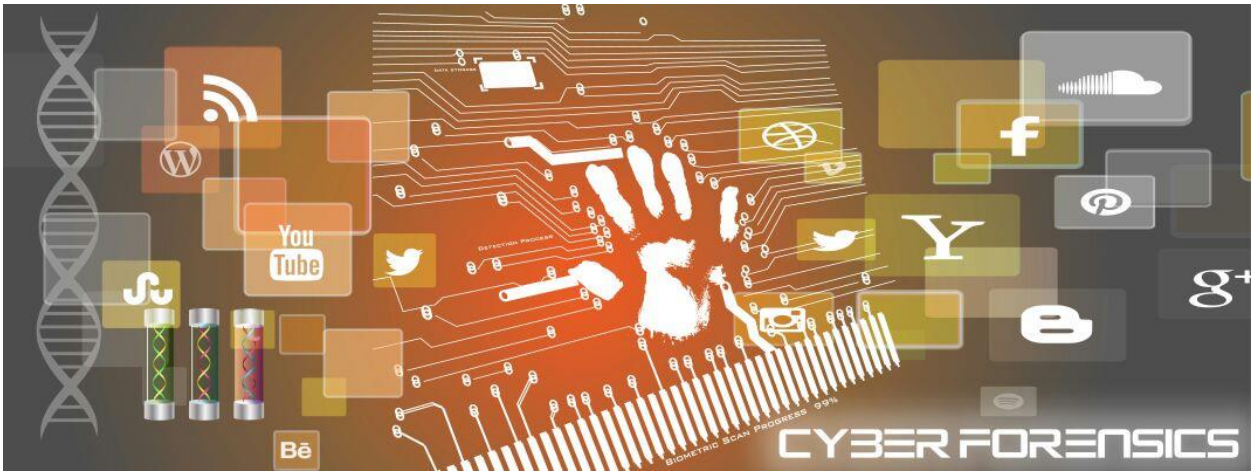
13.10 Explain how to locate and recover image files

13.11 How to identify unknown file formats

13.12 List picture viewer tools and image file forensic tools

## Module 14: Application Password Crackers

14.1 What are the terminologies used




14.2 Explain the functionality of password crackers

S M E X 66

– C O N F I D E N T I A L –

14.3 Summarize various types of passwords

14.4 What is a password cracker?

14.5 How Does a Password Cracker Work?

14.6 Discuss various password cracking techniques

14.7 List various types of password attacks

14.8 List various system and application software password cracking

14.9 What are default passwords?

14.10 Discuss various password cracking tools

## Module 15: Log Capturing and Event Correlation

15.1 What are computer security logs?

15.2 Discuss about logon event in Window

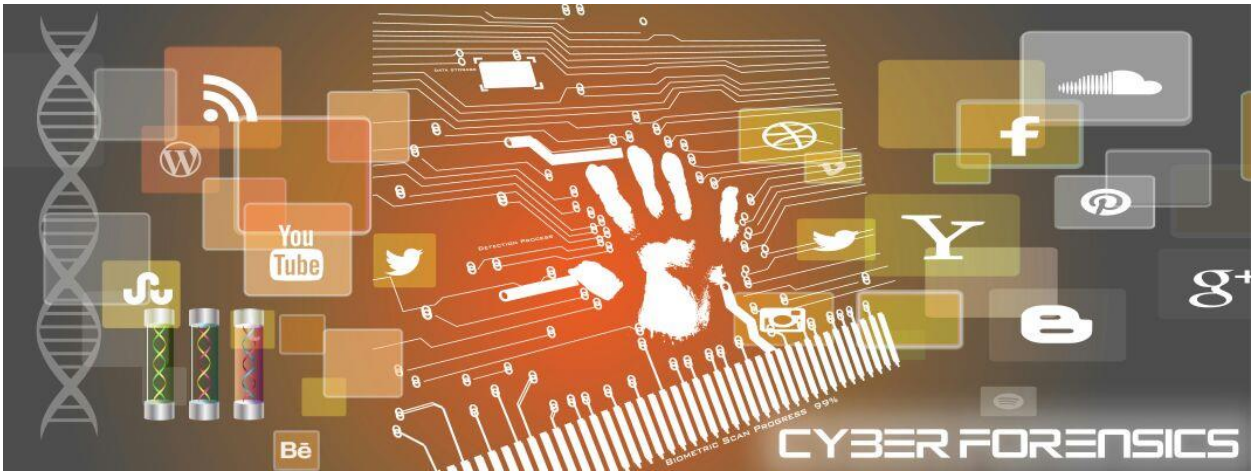
15.3 What are IIS LOGS?

15.4 How to view the DHCP logs

15.5 What is ODBC LOGGING?

15.6 Explain legality of using logs

15.7 Explain log management




15.8 Discuss various challenges in log management

15.9 What is centralized logging

15.10 Discuss about syslog

15.11 Why Synchronize Computer Times?

15.12 What is NTP?

15.13 List various NIST time servers

15.14 Discuss various event correlation approaches

15.15 List various log capturing and analysis tools

## Module 16: Network Forensics, Investigating Logs and Investigating Network Traffic

16.1 Summarize network forensics concepts

16.2 Explain the network forensics analysis mechanism

16.3 What are intrusion detection systems (IDS?)

16.4 Define the terms firewall and honeypot

16.5 Discuss various network vulnerabilities

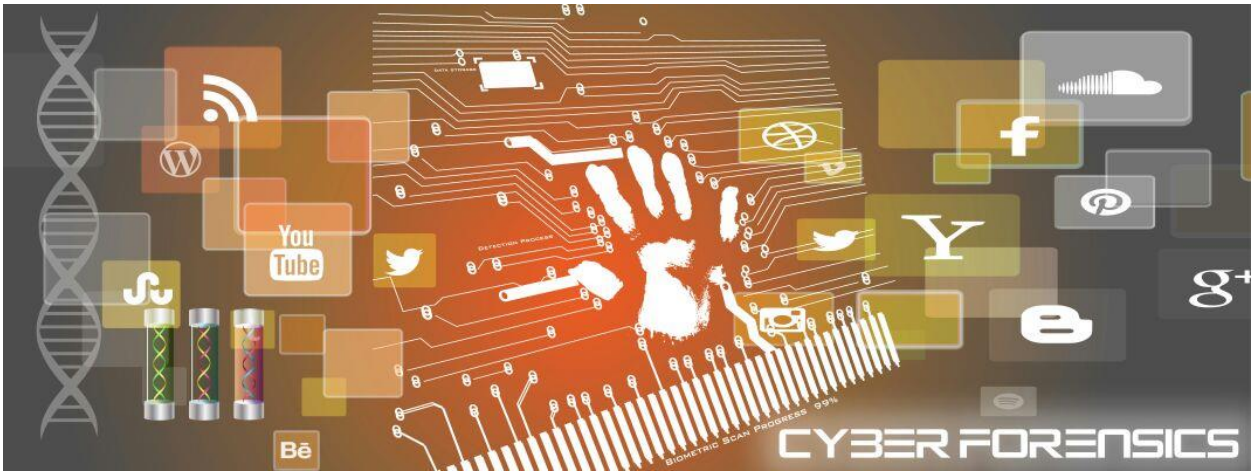
16.6 Explain various types of network attacks

16.7 Explain new line injection attack and timestamp injection attack

16.8 Where to Look for Evidence?

16.9 How to handle logs as evidence

16.10 Explain how to condense a log file




16.11 Why to Investigate Network Traffic?

16.12 How to acquire traffic using DNS poisoning techniques

16.13 Explain how to gather from ARP table

16.14 List various traffic capturing and analysis tools

## Module 17: Investigating Wireless Attacks

17.1 Discuss various advantages and disadvantages of wireless networks

17.2 list different components of wireless networks

17.3 What are the various types of wireless networks?

17.4 List various types of wireless standards

17.5 What is MAC FILTERING?

17.6 What is a Service Set Identifier (SSID?)

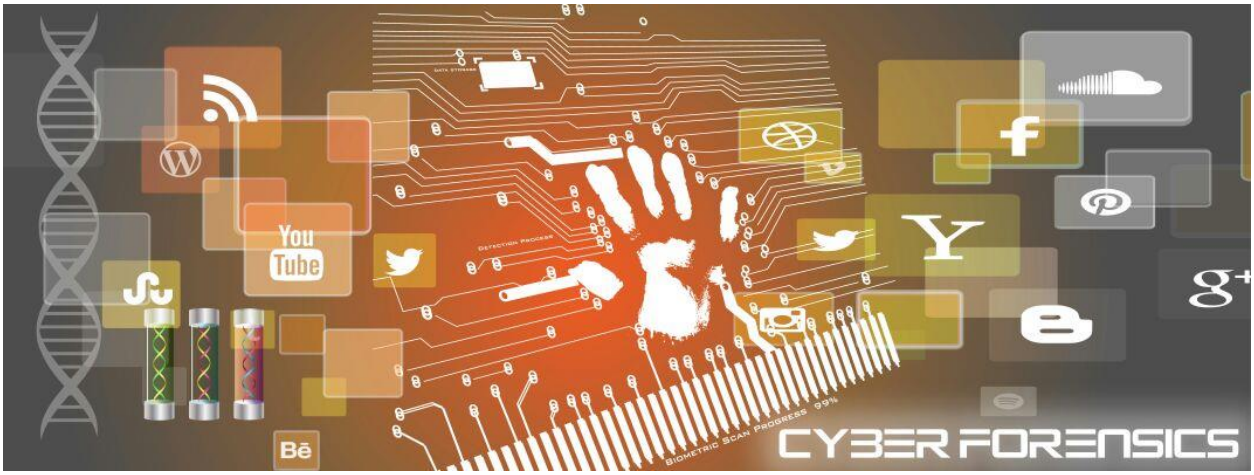
17.7 Discuss various types of wireless encryption

17.8 List various types of wireless attacks

17.9 How to investigate wireless attacks

17.10 What are the requirements of a tool design and summarize the best practices for wireless forensics

17.11 List various wireless forensics tools




## Module 18: Investigating Web Attacks

18.1 What are Web Applications?

18.2 Explain Web application architecture

18.3 Why Web servers are compromised

18.4 Provide an overview of Web logs

18.5 What are Internet Information Services (IIS) and apache Web server Logs

18.6 Discuss various types of Web attacks

18.7 How to investigate Web attacks

18.8 Explain the investigation process of Web attacks in Windows-based servers

18.9 Describe how to investigate IIS and Apache logs

18.10 When does Web page defacement occur?

18.11 Discuss various security strategies to Web applications

18.12 List various Web attack detection tools

18.13 Discuss about various tools for locating IP address

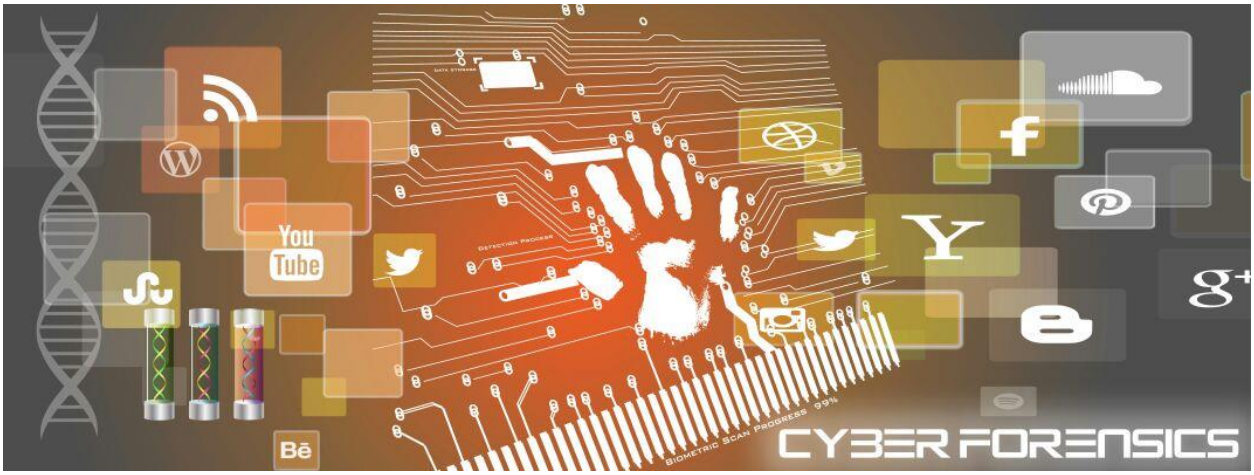
## Module 19: Tracking Emails and Investigating Email Crimes

19.1 Explain the terms Email system, Email Clients, Email Servers, and Email Message

19.2 Discuss the importance of electronic records management

19.3 Discuss various types of Email crimes

19.4 Provide examples of Email header




19.5 List Common Headers

19.6 Why to Investigate Emails

19.7 Discuss the steps involved in investigation of Email crimes

19.8 List various Email forensics tools

19.9 What are the different laws and acts against Email Crimes?

## Module 20: Mobile Forensics

20.1 List different mobile devices

20.2 What are the hardware and software characteristics of mobile devices?

20.3 What is a cellular network?

20.4 Provide an overview of mobile operating system

20.5 Discuss various types of mobile operating systems

20.6 What a Criminal can do with Mobiles Phones?

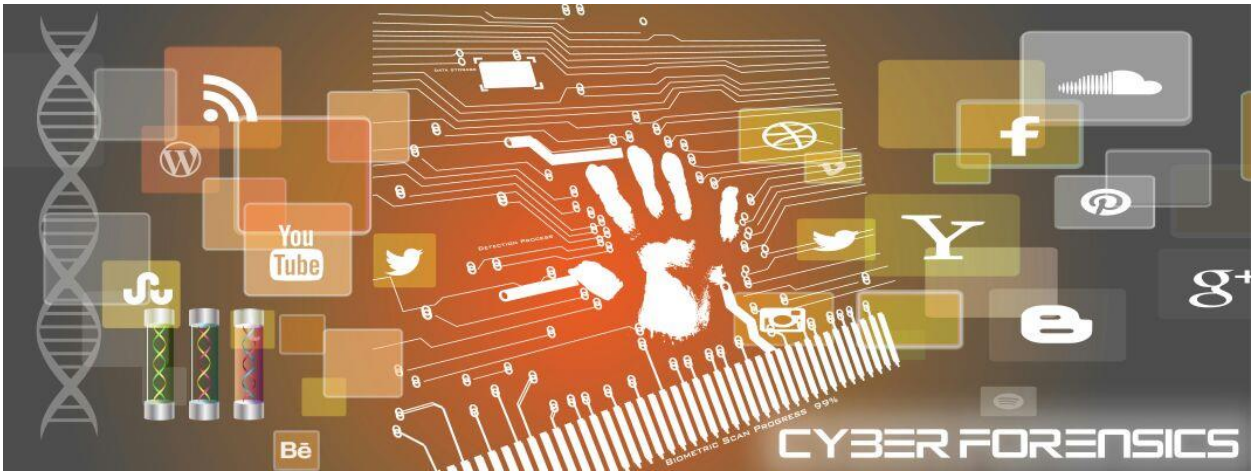
20.7 Describe various mobile forensics challenges

20.8 Discuss various memory considerations in mobiles

20.9 What are the different precautions to be taken before investigation?

20.10 Explain the process involved in mobile forensics

20.11 List various mobile forensic hardware and software Tools




## Module 21: Investigative Reports

21.1 Explain importance of reports and need of an investigative report

21.2 Discuss the salient features of a good report

21.3 Provide computer forensics report template

21.4 How is a report classified?

21.5 Provide layout of an investigative report

21.6 What are the guidelines for writing a report?

21.7 Provide an overview of investigative report format

21.8 How to document a case report

21.9 What are the best practices for investigators?

21.10 How to write a report using FTK and ProDiscover

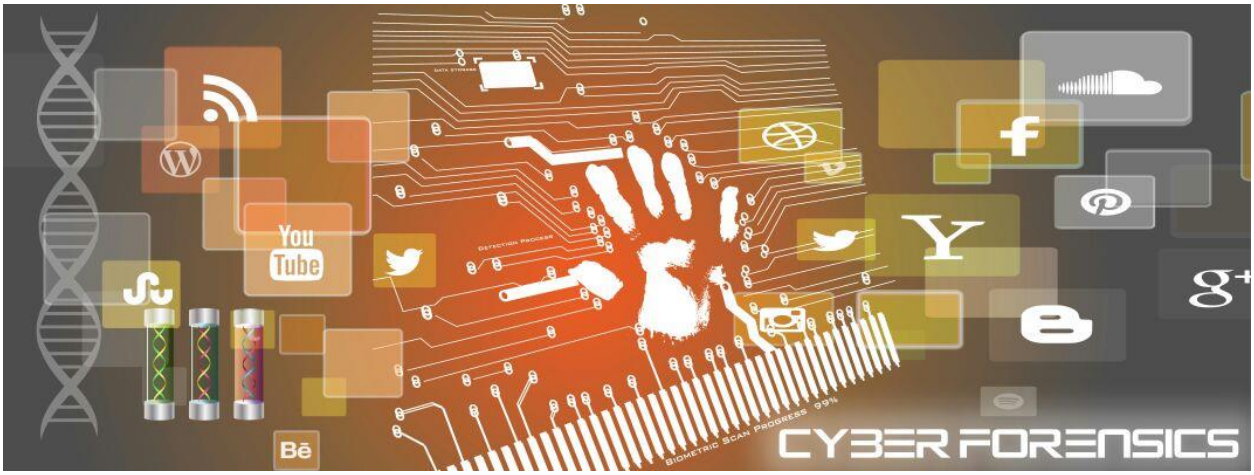
## Module 22: Becoming an Expert Witness

22.1 What is an Expert Witness?

22.2 Explain the role of an expert witness

22.3 Describe various types of expert witnesses

22.4 What is the scope of expert witness testimony?




22.5 Explain the differences between Technical Witness and Expert Witness

22.6 What are the various steps involved in evidence processing

22.7 How to prepare a report

22.8 List the rules pertaining to an expert witness' qualification

22.9 How to testify in the court

22.10 What are the general ethics while testifying?

22.11 How to testify during direct and cross-examination

22.12 How to find a computer forensic expert