



Cyber  
law

Cyber  
forensics



*What does  
cyber law  
means?*

Information technology law (also called "cyber law") concerns the law of information technology, including computing and the internet. It is related to legal informatics, and governs the digital dissemination of both (digitalized) information and software, information security and electronic commerce. aspects and it has been described as "paper laws" for a "paperless environment". It raises specific issues of intellectual property in computing and online, contract law, privacy, freedom of expression, and jurisdiction.



# Importance of cyber law

- it touches almost all aspects of transactions and activities on and concerning the Internet
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet, websites, email, computers, cell phones, software and hardware, such as data storage devices.



# Cyber acts in India

- INDIAN PENAL CODE, 1860.
- INDIAN EVIDENCE ACT, 1872.
- BANKERS BOOK EVIDENCE ACT, 1891.
- GENERAL CLAUSES ACT, 1897
- IT ACT 2000





## Role of cyber law

➤ Basically cyber law is a list of sections and acts which is basically used in cases of cyber crimes and cyber threats.

To make our digital life safe by defending us from cyber threats



# Resource

- <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4284&context=californialawreview>

Title- Robotics and the Lessons of Cyberlaw

Publication year- 2015

Author-Ryan calo

Writer-Ryan calo

Journal- California Law Review

[https://www.ijntr.org/download\\_data/IJNTR03050003.pdf](https://www.ijntr.org/download_data/IJNTR03050003.pdf)

Title-Cyber Crime Problem Areas, Legal Areas and the Cyber Crime Law

Publication year-2017

Author-Dr mir mohammad azad

Writer-syeda shajia sharmin, Advocate Kazi Nafiul Mazid

Journal-International Journal of New Technology and Research



# Cyber forensics

Computer forensics (also known as computer forensic science) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European court systems.



# Computer Forensics Investigation Procedure

FR

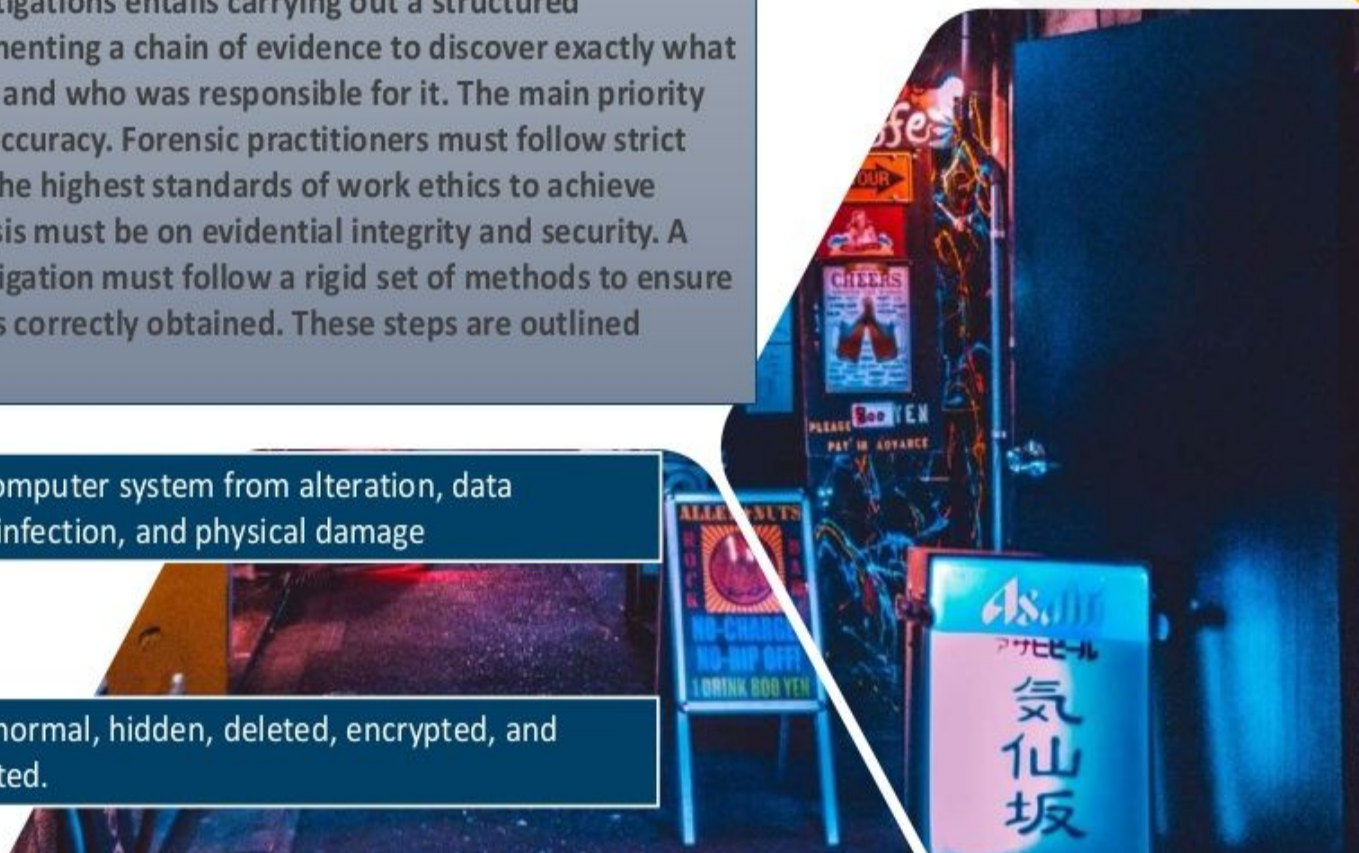
Computer forensics investigations entails carrying out a structured investigation while documenting a chain of evidence to discover exactly what happened on a computer and who was responsible for it. The main priority of computer forensics is accuracy. Forensic practitioners must follow strict guidelines and maintain the highest standards of work ethics to achieve accuracy because emphasis must be on evidential integrity and security. A Computer Forensic investigation must follow a rigid set of methods to ensure that computer evidence is correctly obtained. These steps are outlined below:

Protect

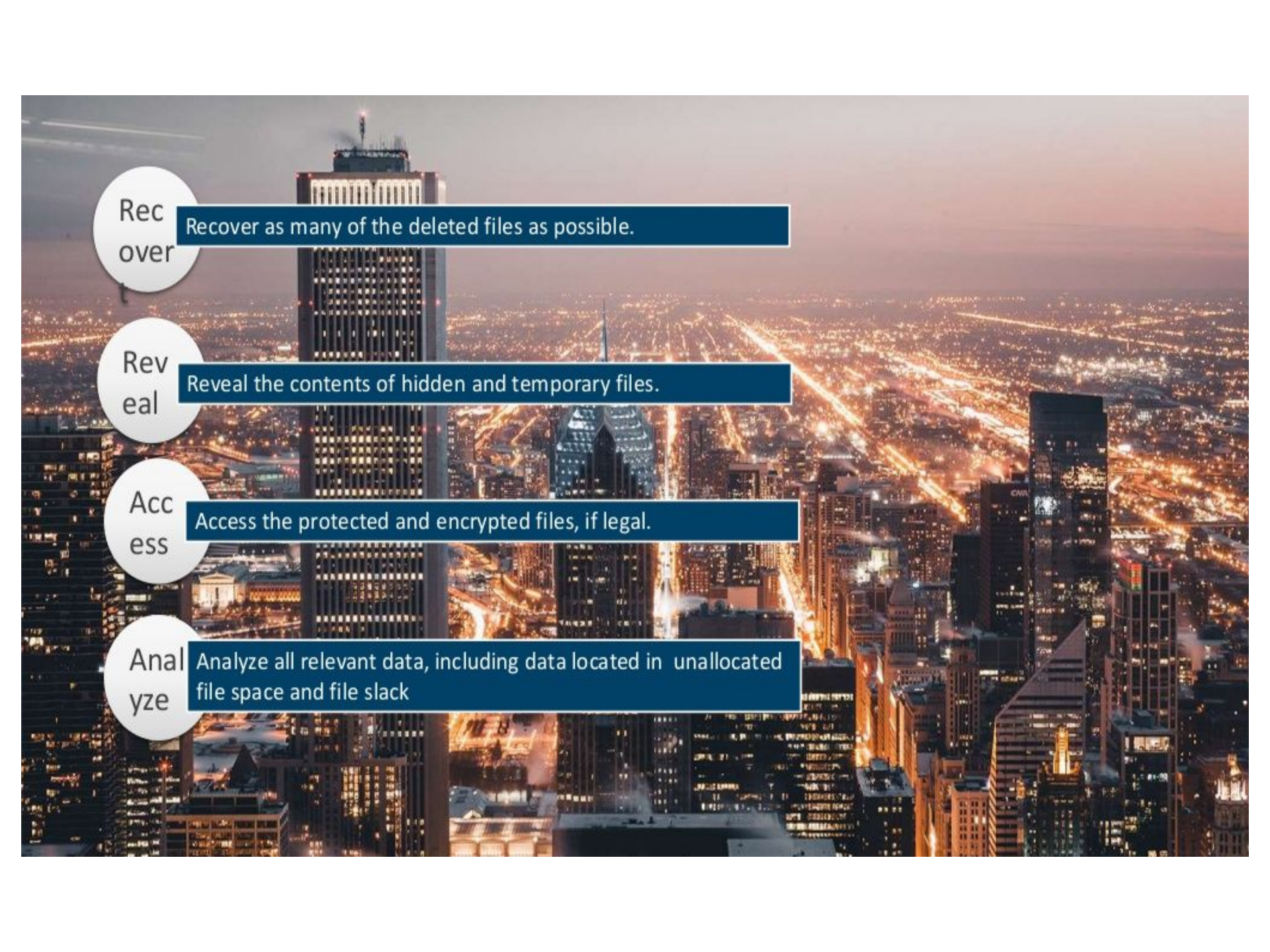
Protect subject computer system from alteration, data corruption, virus infection, and physical damage

Discover

Uncover all files: normal, hidden, deleted, encrypted, and password-protected.







Recover

Recover as many of the deleted files as possible.

Reveal

Reveal the contents of hidden and temporary files.

Access

Access the protected and encrypted files, if legal.

Analyze

Analyze all relevant data, including data located in unallocated file space and file slack





Report

Print out a listing of all relevant files, and provide an overall opinion on the system examination.

technology

Provide expert testimony or consultation, if required.



## Techniques in Computer Forensics Investigation

A number of techniques are used during computer forensics investigations, these include;

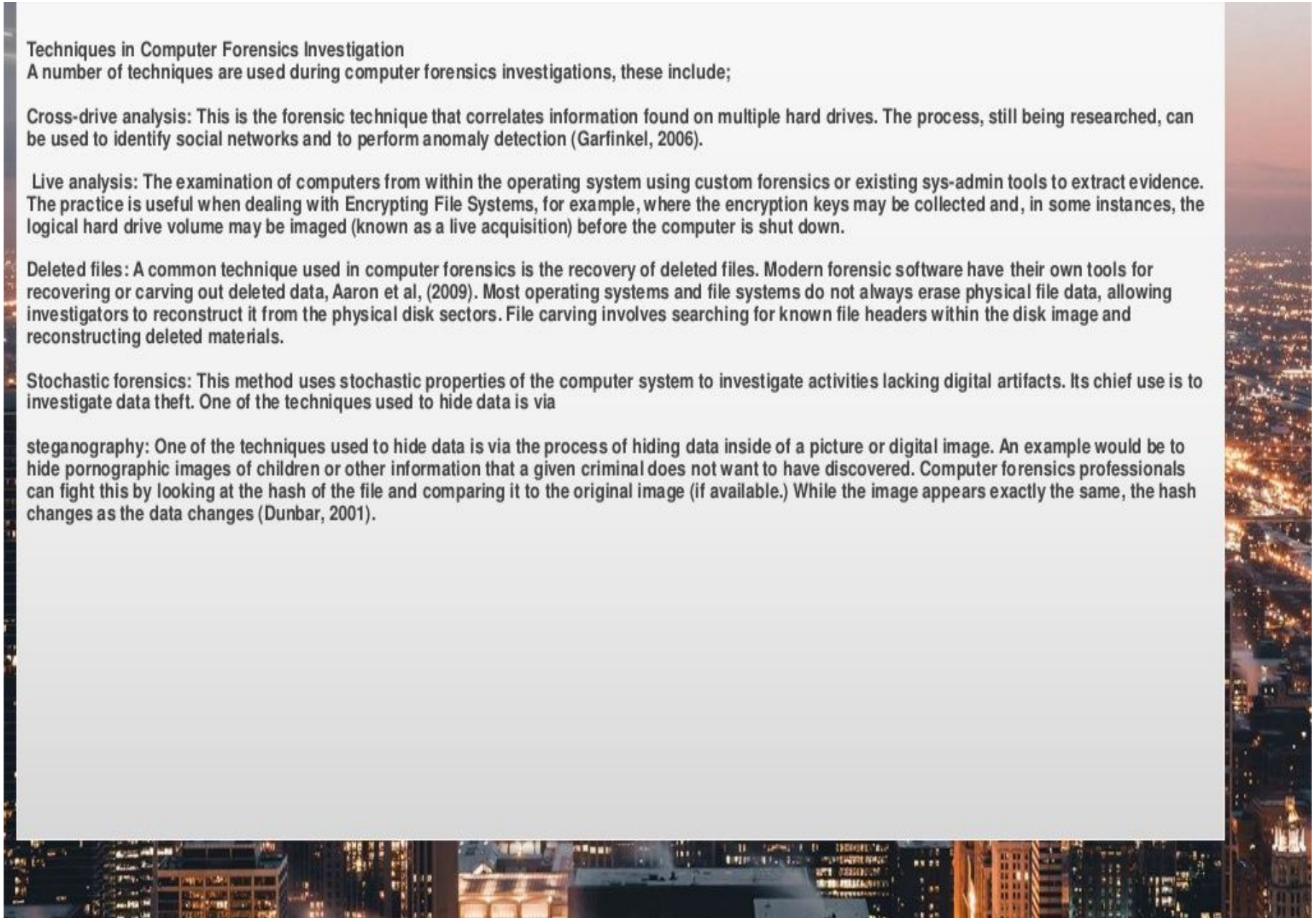
**Cross-drive analysis:** This is the forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection (Garfinkel, 2006).

**Live analysis:** The examination of computers from within the operating system using custom forensics or existing sys-admin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.

**Deleted files:** A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data, Aaron et al, (2009). Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

**Stochastic forensics:** This method uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft. One of the techniques used to hide data is via

**steganography:** One of the techniques used to hide data is via the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the image appears exactly the same, the hash changes as the data changes (Dunbar, 2001).



# Major challenges in CF

1. The lack of real data sources
2. The young and ever changing nature of the field
3. The dependency on tools
4. The lack of published error rates for the various widely used digital forensics tools
5. The lack of basic research in this domain (cite our paper)
6. The lack of agreed upon standards and processes
7. The limitation of the hardware standards being used during the acquisition of data
8. The volatility of the evidence – such as RAM
9. The continuous change in technology
10. The use of anti forensics techniques and tools
11. The lack of a common body of knowledge





<https://www.ajol.info/index.php/stech/article/viewFile/154713/144296>

Title-Computer Forensics Investigation; Implications for Improved Cyber Security in Nigeria

Publication year- 2017

Author-Chigozie-Okwum, Chioma C, Michael, Daniel O.

Writer-Ugboaja, Samuel G.

Journal-african journals online

<https://www.aaai.org/ocs/index.php/SSS/SSS15/paper/viewFile/10227/10092>

Title-Data Sources for Advancing Cyber Forensics: What the Social World Has to Offer

Publication year- 2015

Author-Ibrahim Baggili


Writer- Frank Breitingner

Journal-UNH Cyber Forensics Research & Education Group / Lab



## **Role of cyber forensics**

**Computer forensics is the process of using the latest knowledge of science and technology with computer sciences to collect, analyze and present proofs to the criminal or civil courts. .Forensics is the process which deals in finding evidence and recovering the data.**





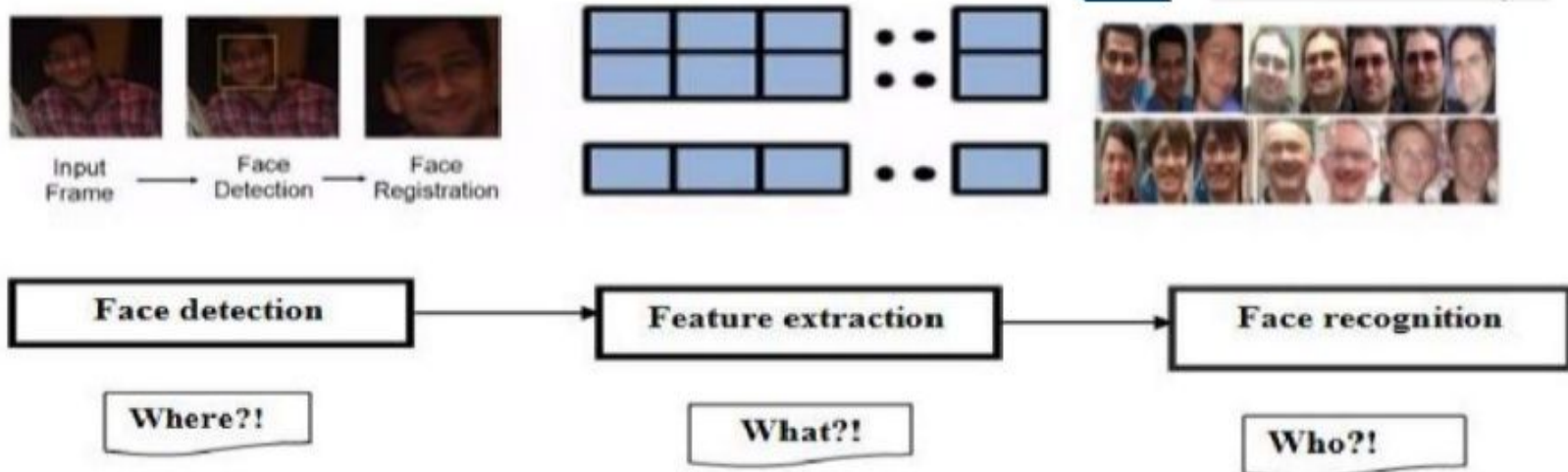
➤ Face recognition technology is a combination of various other technologies and their features and characteristics makes face recognition a better performer depending upon the application.

➤ Iris recognition is a high reliable biometric security system that acquires increased attention. The human iris is an annular region between the black pupil and the white sclera. The texture of iris is unique to each subject. The iris is first localized with two circles in the image. Then the iris part is unwrapped to a rectangular region where the iris texture is analyzed. In general the whole procedure of feature Extraction of iris recognition system includes two steps. Initial, an arrangement of one-dimensional (1-D) force signs is built keeping in mind the end goal to adequately portray the most imperative data in the first two-dimensional (2-D) picture. Second, utilizing a specific class of dyadic wavelets, a position arrangement of neighborhood sharp variety focuses in such flags is recorded

➤ A fingerprint scanner typically works by first recording fingerprint scans of all authorized individuals for a particular system or facility. These scans are saved within a database. The user requiring access puts their finger on a hardware scanner, which scans and copies the input from the individual and looks for any similarity within the already-stored scans. If there is a positive match, the individual is granted access. Fingerprint scanners most commonly use an individual's thumbprint as identification.



# How face recognition works



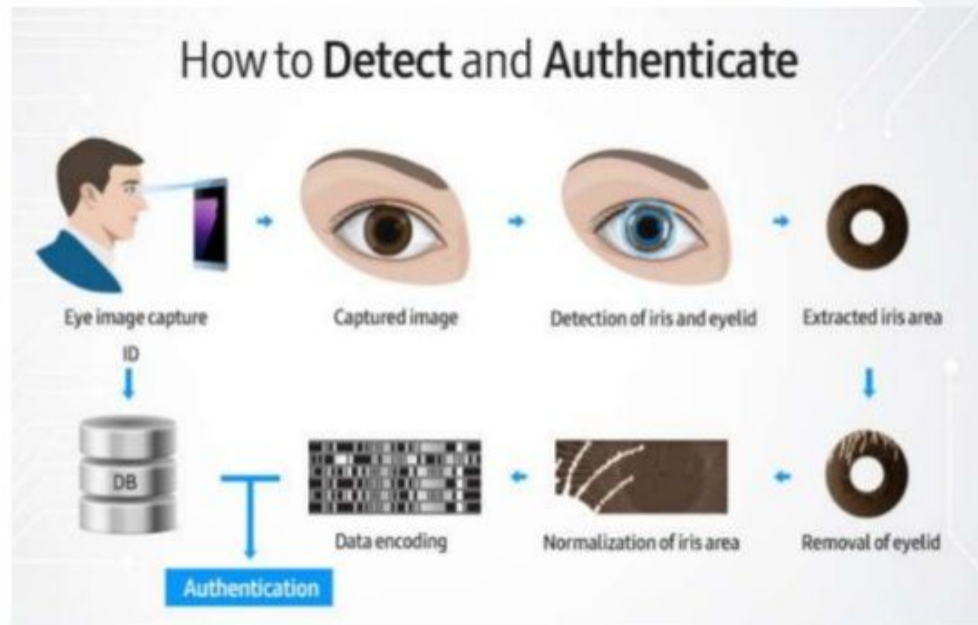
FR

Genetic algorithm is used in detecting and extracting the facial features from the video stream by eigen technique. The feature based Genetic algorithm is chosen as it deals with geometrical elements of the human face also in order to perform math calculus in change detection mechanism.



# The process of iris recognition consisting of the following

FR

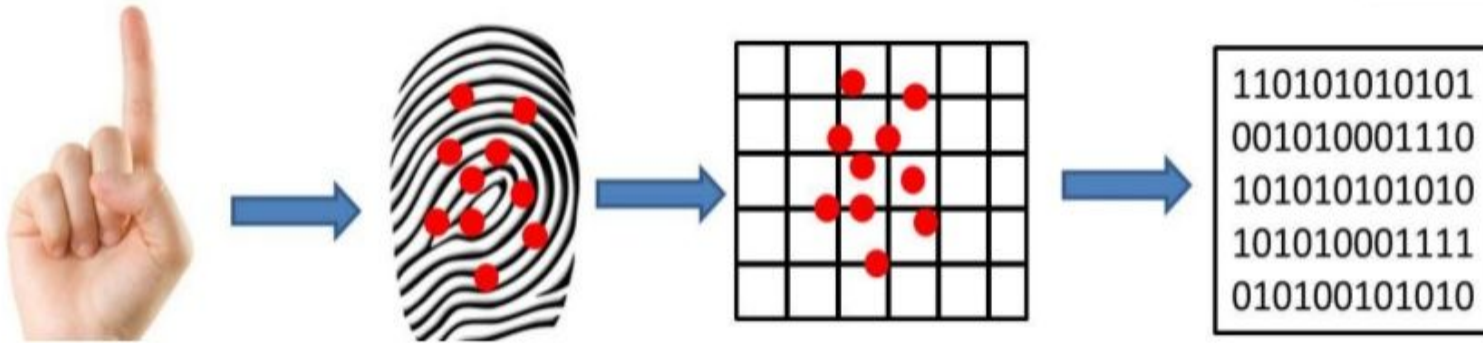


Finding an Iris in an Image

Iris Feature Encoding by 2D Wavelet Demodulation

Recognising iris

# How fingerprint recognition work



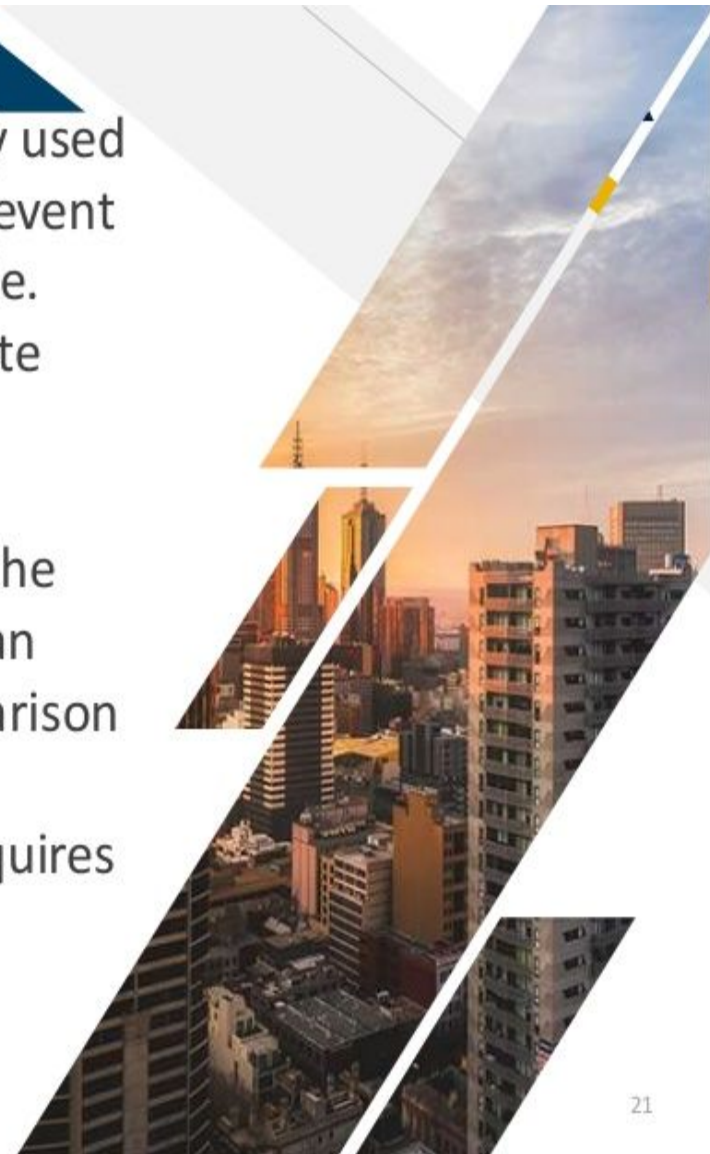
method of identifying the identity of an individual based on the comparison of two fingerprints .It consists of three parts: a) fingerprint enrollment b) fingerprint verification c) Fingerprint identification. Fingerprint Enrollment: The fingerprint is captured by putting it on the fingerprint device's sensor. It is very important phase because the captured image quality depends on way it is put on the sensor.



**Fingerprint Verification:** Verification is typically used for fingerprint positive recognition, used to prevent the use of the same identity by multiple people. There is one-to-one mapping between template and individual's fingerprint.

**Fingerprint Identification:** A match is found between each individual and templates of all the users in the database. The system recognizes an individual by conducting a one to many comparison with an individual's identity.

The analysis of fingerprints to find a match requires the comparison of several fingerprint feature pattern which includes patterns like minutiae points, ridge orientation



<http://14.139.205.163:8080/jspui/bitstream/123456789/144/1/2016PGCAIS06.pdf>

**Title-**ENHANCED RSA KEY GENERATION MODELING USING FINGERPRINT BIOMETRIC

**Publication year-** 2016

Author-neha bansal

Writer-neha bansal

Journal- DEPARTMENT OF COMPUTER APPLICATIONS  
NATIONAL INSTITUTE OF TECHNOLOGY

[https://www.bedicon.org/wp-](https://www.bedicon.org/wp-content/uploads/2018/01/laws_topic4_source1.pdf)

[content/uploads/2018/01/laws\\_topic4\\_source1.pdf](https://www.bedicon.org/wp-content/uploads/2018/01/laws_topic4_source1.pdf)

**Title-**comparing FINGERPRINT BIOMETRIC authentication

**Publication year-** 2017

Author-obi ogbanufe

Writer-dan j kim

Journal-Decision Support Systems  
and Electronic Commerce

<https://pdfs.semanticscholar.org/dc97/ceb1faf945e780a92be651b022a82e3bff5a.pdf>

**Title-**50 years of biometric research: Accomplishments, challenges, and opportunities

**Publication year-** 2016

Author-AnilK.Jain , Karthik Nandakumar

Writer-Arun Ross

Journal-pattern recognition letters





# References

- [https://www.slideshare.net/MayankDiwakar/ppt1-132598823?qid=7a9d8e61-d895-47f9-ae1d-6d81d5016663&v=&b=&from\\_search=1](https://www.slideshare.net/MayankDiwakar/ppt1-132598823?qid=7a9d8e61-d895-47f9-ae1d-6d81d5016663&v=&b=&from_search=1)