Unit-4

# Introduction to Computer Forensics Investigations and Electronic Evidence

**Introduction to Computer Forensics Investigations and Electronic Evidence (UNIT-4)**

**Digital Forensics**: Definition, Process, Locard's Principle of Exchange, Branches of Digital Forensics, Handling Digital Crime Scene, Important Documents and Electronic Evidence

**Introduction to Evidence Acquisition**: Identification, Acquisition, Labelling and Packaging, Transportation, Chain-of-Custody, Importance of Document and Preservation

**Acquisition Process**: Write-Blockers, Imaging Techniques, Evidence Integrity, Standard Operating Procedures for Acquisitions and Preservation of Evidence.

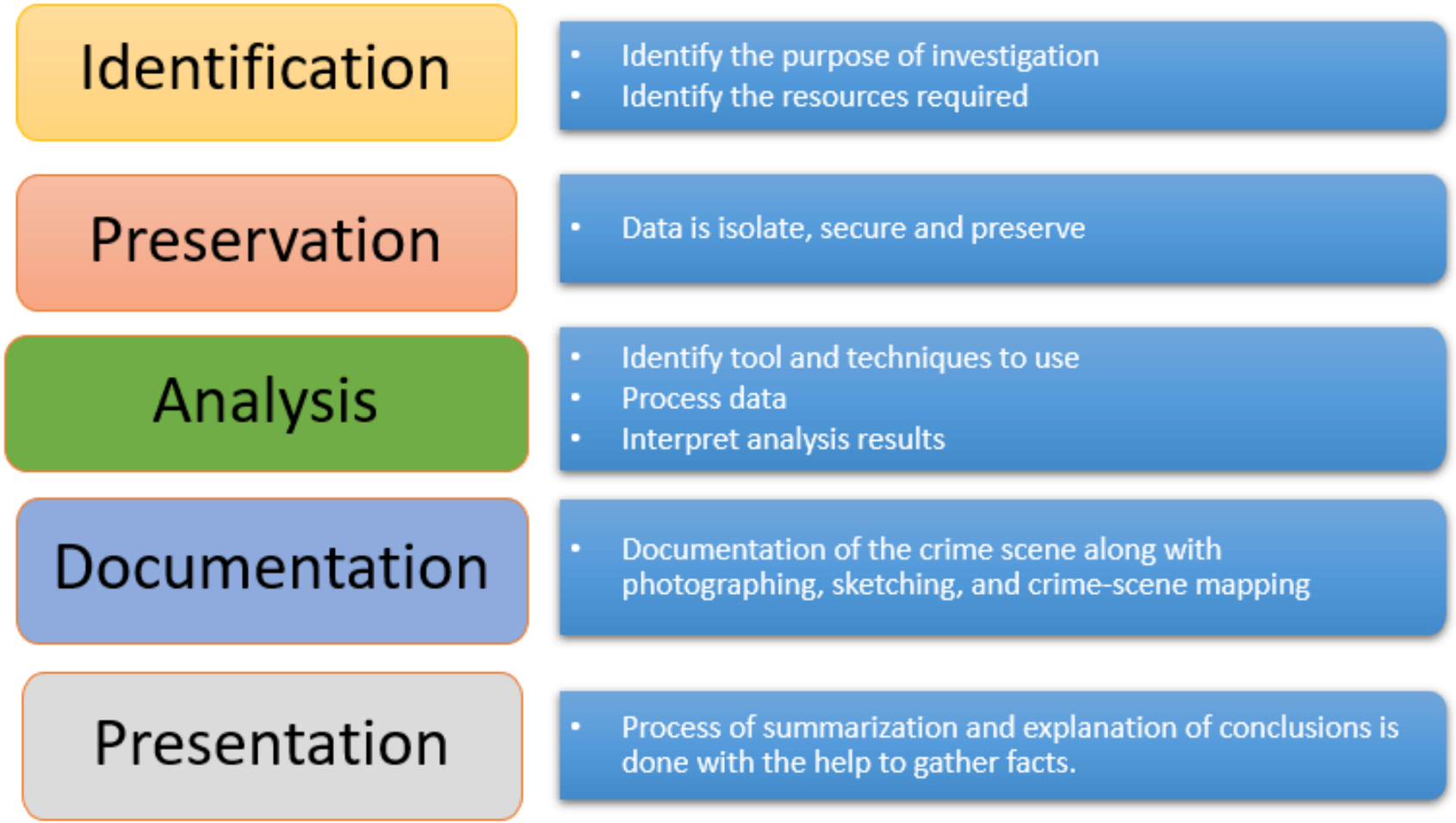
**Introduction to Data Recovery and Carving**: Importance of Data Recovery in Forensic Investigation, Carving Methods, Difference between Data Recovery and Carving.

# Digital Forensics: Definition

Computer forensics also refers to digital forensics.

It is the fusion of domains such as network forensics, server forensics, computer forensics, internet forensics, social media forensics, memory forensics, online gaming, data/disk forensics, and VR forensics.

# Digital Forensics: Process



# Nonlinear system identification based on LSSVM within the evidence framework

**Abstract:**

Support Vector machine (SVM) is a new learning machine based on the statistical learning theory. A regression algorithm based on least squares support vector machine (LS SVM) within the Bayesian evidence framework is discussed Also the Gauss kernel parameter selecting method is proposed. Under the evidence framework, the regularization and kernel parameters can be adjusted automatically, which can achieve a fine tradeoff between the minimum error and model's complexities. This method is applied to nonlinear system identification and the simulation results show the effectiveness and superiority of the proposed approach. It provides a new way for modeling and identification of complicated industrial processes.

**Published in:** 2008 Chinese Control and Decision Conference

**Date of Conference:** 02-04 July 2008 **INSPEC Accession Number:** 10142689

# Target Identification Based on Neural Network and D-S Evidence Theory

**Abstract:**

This paper presents a method of multisensor data fusion based on neuron network and reasoning (Dempster-Shafer evidence reasoning).The method can use deal with the inaccuracy and fuzzy information by D-S Evidence. And also it can give a full play to self-study of neural net, self-adapting and fault tolerant ability. In this way it has doughty robustness to uncertain information and improves the system identification rate. Then the D-S evidence is used to fuse the results derived from the neural network at different time. The result of computer simulation shows the method is effective and correct.

**Published in:** 2012 International Conference on Industrial Control and Electronics Engineering

# Preservation of digital evidence: Application in criminal investigation

**Abstract:**
Any digital device generates information that may become valuable evidence in the event of a cybercrime incident, security incident, or cyber-attack, but often the collection, management and preservation of this information is not done properly. In the legal field, once information has been obtained from the devices, it is very important to maintain it and preserve it from the initial time, through investigation, until the trial or investigation is concluded, and to preserve it for long term use, in order to avoid it to be tainted, damaged, changed or manipulated and so assuring reliability through the whole process. Preservation of digital evidence is an important aspect when deciding its admissibility in a trial in process, or in any future process, reopened by appeal, or as source of historical information. This paper contains a review of the state of the art about digital preservation in institutions dedicated to criminal investigation, analyzing concepts, related projects, tools and legal support in this area. The motivation of this paper is the idea of finding how close we are to having a framework useful to preserve digital evidence, ensuring integrity, hence increasing its admissibility, and supported by long term preservation technique.

**Published in:** 2015 Science and Information Conference (SAI)

# Acquiring and Analysing Digital Evidence - a Teaching and Learning Experience in Class

**Abstract:**
The advancement of Information and Communication Technology (ICT) offers positive and negative impacts in our daily life today. Criminals too leverage on sophisticated ICT in their modus operandi. Hence, digital evidences are abundant to be acquired and analysed as part of investigation, today. Two homegrown tools i.e. PenDua and Kloner are used for digital evidence acquisition tool while FTK and Autopsy are among tools applied for analysis of the evidences. Various artifacts are used as evidences of some made-up crime cases. The whole exercise is compiled as a learning package that can be a good exposure for beginners of Digital Evidence Forensics learners. We have tested the usage of this learning package with 120 students of a Digital Evidence Forensic class for 3 semesters. Majority of the students found that they enjoyed experiencing the hands-on to learn the proper procedure of acquiring and analyzing digital evidence, usage of several popular digital forensics tool and producing proper report. The made-up of real cases make the exercise interesting, appreciated by the students and enhance their understanding.

**Published in:** 2018 Cyber Resilience Conference (CRC)

# Application of three-dimensional optical acquisition to the documentation and the analysis of crime scenes and legal medicine inspection

**Abstract:**

This paper presents the activities aimed at testing the performance of a 3D optical system, designed for industrial and standard reverse engineering applications, to carry out the contact-less acquisition for crime scene documentation and analysis. In particular, the study focuses on two aspects. The former is the "in-field" measurement and modeling of crime scenes; the latter is the analysis of lesions, organs, bone tissues and skin wounds during legal-medicine inspection. Several study cases are presented, in order to show the high potential, the flexibility and the effectiveness of the measurement based on the optical three-dimensional approach. The paper is organized in three different sections. Section 1 briefly overviews the operative contexts and explains the purposes of the work. Section 2 describes the instrumentation and the methodology used to perform the data acquisition and elaboration. Section 3 presents the experimental cases.

**Published in:** 2007 2nd International Workshop on Advances in Sensors and Interface

# Locard’s principle of exchange

whenever two objects come into contact with one another, an exchange of materials occurs between them. This may lead to a connection between a suspect and a crime scene or a suspect and a victim, based on transferred fragments of materials.

Prove
Locard
principle

# Branches of digital forensics

- Computer Forensics
- Mobile Device Forensics
- Network Forensics
- Forensic Data Analysis
- Database Forensics
- Email Forensics
- Forensics of Malware
- Memory Forensics
- Forensics of Wireless Networks
- Forensics of Disks

# Handling digital crime scene

## What Is Digital Evidence?

Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination.

Digital evidence—

- Is latent, like fingerprints or DNA evidence.
- Crosses jurisdictional borders quickly and easily.
- Is easily altered, damaged, or destroyed.
- Can be time sensitive.

# Handling Digital Evidence at the Scene

Precautions should be taken in the collection, preservation, and transportation of digital evidence. First responders may follow the steps listed below to guide their handling of digital evidence at an electronic crime scene:

- Recognize, identify, seize, and secure all digital evidence at the scene.
- Document the entire scene and the specific location of the evidence found.
- Collect, label, and preserve the digital evidence.
- Package and transport digital evidence in a secure manner.

# Is Your Agency Prepared to Handle Digital Evidence?

Every agency should identify personnel—before they are needed—who have advanced skills, training, experience, and qualifications in handling electronic devices and digital evidence. These experts should be available for situations that exceed the technical expertise of the first responder or

# Electronic devices: Types, description and potential evidence

**Types of Computer Systems**

PC, monitor, keyboard, and mouse

Apple G3 computer, monitor, keyboard, and mouse

Apple iMac, keyboard, and mouse

Laptop computer

**Potential evidence:** A computer system and its components can be valuable evidence in an investigation. The hardware, software, documents, photos, image files, e-mail and attachments, databases, financial information, Internet browsing history, chat logs, buddy lists, event logs, data stored on external devices, and identifying information associated with the computer system and components are all potential evidence.

# Electronic devices: Types, description and potential evidence

**Types of Hard Drives**

SCSI drives SATA drive IDE drive Laptop hard drives

IDE 40-pin 2.5" IDE 44-pin

IDE power and data connections

Serial ATA (SATA)

SCSI HD 68-pin SCSI IDC 50-pin

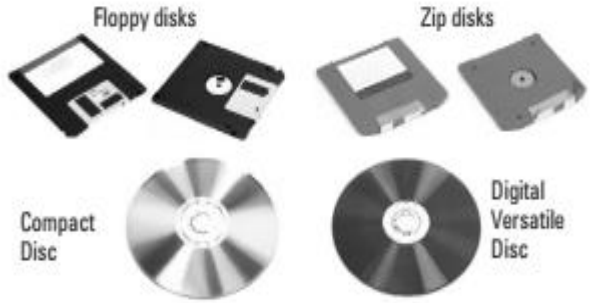
**External Hard Drive Cases**

3.5" Hard drive

2.5" Hard drive

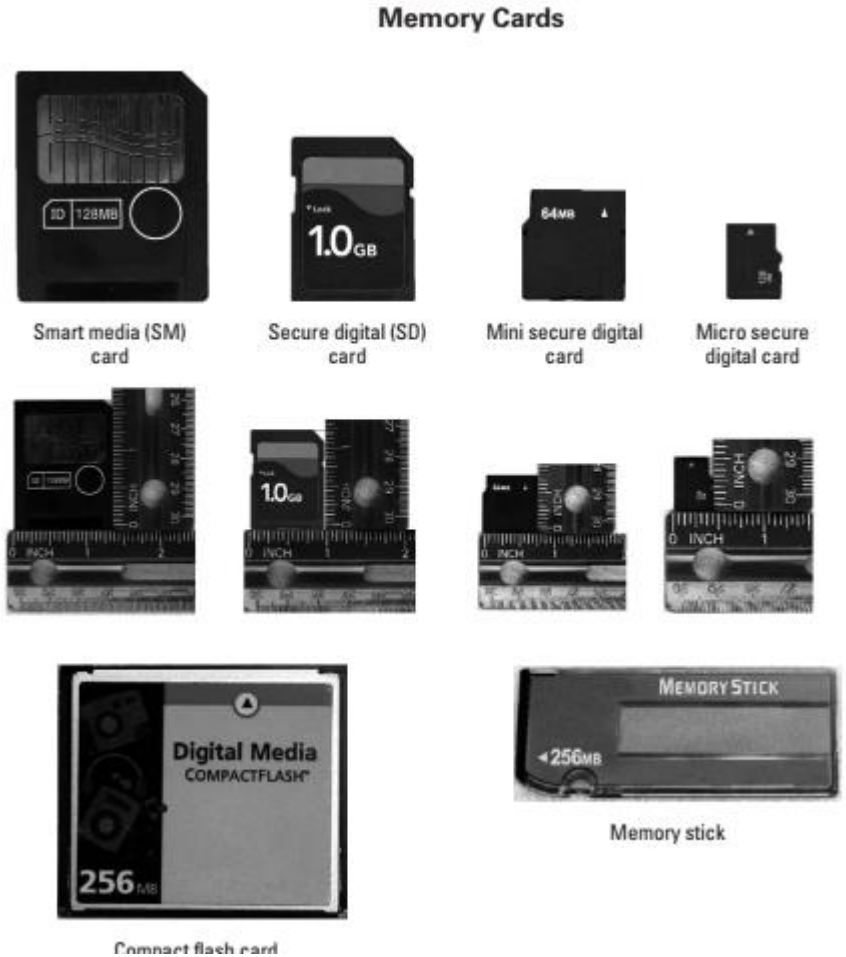
Network storage device

**Removable Media**




**Common Thumb Drives**

# Electronic devices: Types, description and potential evidence




**Potential evidence:** Storage devices such as hard drives, external hard drives, removable media, thumb drives, and memory cards may contain information such as e-mail messages, Internet browsing history, Internet chat logs and buddy lists, photographs, image files, databases, financial records, and event logs that can be valuable evidence in an investigation or prosecution.

# Electronic devices: Types, description and potential evidence

Handheld Devices

**Potential evidence:** Handheld devices such as mobile phones, smart phones, PDAs, digital multimedia (audio and video) devices, pagers, digital cameras, and global positioning system (GPS) receivers may contain software applications, data, and information such as documents, e-mail messages, Internet browsing history, Internet chat logs and buddy lists, photographs, image files, databases, and financial records that are valuable evidence in an investigation or prosecution.

# Electronic devices: Types, description and potential evidence


**Potential evidence:** The devices themselves and the functions they perform or facilitate are all potential evidence. Information stored on the device regarding its use also is evidence, such as incoming and outgoing phone and fax numbers; recently scanned, faxed, or printed documents; and information about the purpose for or use of the device. In addition, these devices can be sources of fingerprints, DNA, and other identifiers.

Create a flowchart to collect digital evidence

**Crime scene**

**Important Documents and Electronic Evidence**

# LIST A: Documents That Establish Both Identity and Employment Authorization

All documents must be unexpired.

1. U.S. passport or U.S. passport card
2. Form I-551, Permanent Resident Card or Alien Registration Receipt Card (this is commonly called a Green Card.) See Section 6.1, Lawful Permanent Residents for when a Permanent Resident Card is considered unexpired past the "Card Expires" date.
3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa (MRIV)
4. Form I-766, Employment Authorization Document (EAD) that contains a photograph. However, in certain circumstances, an EAD past its "Card Expires" date qualifies as an unexpired EAD. See Section 4.4, Automatic Extensions of Employment Authorization and/or Employment Authorization Documents (EADs) in Certain Circumstances, for more information.
5. For nonimmigrant aliens authorized to work for a specific employer incident to status, which means they are authorized to be employed based on their nonimmigrant status, a foreign passport with Form I-94 bearing the same name as the passport and an endorsement of their nonimmigrant status, as long as the period of endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form
6. Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 indicating nonimmigrant admission under the Compact of Free Association Between the United States and the FSM or RMI

**Important Documents and Electronic Evidence**

# LIST B: Documents That Establish Identity

All documents must be unexpired.

1. Driver's license or ID card issued by a state or outlying possession of the United States, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address
2. ID card issued by federal, state, or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address (This selection does not include the driver's license or ID card issued by a state or outlying possession of the United States in Item 1 of this list.)
3. School ID card with a photograph
4. Voter's registration card
5. U.S. military card or draft record
6. Military dependent's ID card
7. U.S. Coast Guard Merchant Mariner Card
8. Native American tribal document
9. Driver's license issued by a Canadian government authority

For persons under age 18 who are unable to present a document listed above:

10. School record or report card
11. Clinic, doctor, or hospital record
12. Day care or nursery school record

**Important Documents and Electronic Evidence**

# LIST C: Documents That Establish Employment Authorization

All documents must be unexpired.

1. A Social Security Account Number card, unless the card includes one of the following restrictions:
   - NOT VALID FOR EMPLOYMENT
   - VALID FOR WORK ONLY WITH INS AUTHORIZATION
   - VALID FOR WORK ONLY WITH DHS AUTHORIZATION
2. Certification of report of birth issued by the U.S. Department of State (Forms DS-1350, FS-545, FS-240)
3. Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying territory of the United States bearing an official seal
4. Native American tribal document
5. Form I-197, U.S. Citizen Identification Card
6. Form I-179, Identification Card for Use of Resident Citizen in the United States
7. Employment authorization document issued by the Department of Homeland Security. For examples, please visit uscis.gov/i-9-central. (This does not include Form I-766, Employment Authorization Document, from List A.)

https://www.ssa.gov/oag/acq/ASC_2352_204-1_Security_and_Suit_Reqrmts_ Post_10012017/ List%20 of%20 Acceptable%20Documents.pdf

# Important Documents and Electronic Evidence

**Other links to documents List**

https://www.ssa.gov/oag/acq/ASC_2352_204-1_Security_and_Suit_Reqrmts_ Post_10012017/ List%20 of%20 Acceptable%20Documents.pdf

https://www.uspto.gov/sites/default/files/documents/List_of_Acceptable_I-9_Documents.pdf

# Introduction to evidence acquisition

Evidence Based Acquisition (EBA) is a cost-effective way for academic, corporate and government libraries to evaluate and acquire content that meets the information needs of their users. With this acquisition model your library can maximise the return on investment with making informed decision based on usage.

**Steps**:

Identification->
Acquisition->
Labelling and Packaging->
Transportation->
Chain-of-Custody->
Importance of Document and Preservation

# Evidence Identification

**what can be identified as digital evidence?**

Digital evidence can be any information that is stored or transmitted in binary form that may be used as evidence in court. This includes things like emails, text messages, social media posts, digital images and videos, and more.

**How to identify ?**

1. Seizing the media.
2. Acquiring the media; that is, creating a forensic image of the media for examination.
3. Analyzing the forensic image of the original media.

**Tools that can be used to create a forensic image of media**. Some of the most popular ones include:

- FTK Imager
- Autopsy
- The Sleuth Kit

# Evidence Identification

## Types of Physical Evidence

- *Blood, semen, and saliva*
- *Documents*
- *Drugs*
- *Explosives*
- *Fibers*
- *Fingerprints*
- *Firearms and ammunition*
- *Glass*
- *Hair*
- *Impressions*
- *Organs and physiological fluids*
- *Paint*
- *Petroleum products*
- *Plastic bags*
- *Plastic, rubber, and other polymers*
- *Powder residues*
- *Soil and minerals*
- *Tool marks*
- *Vehicle lights*
- *Wood and other vegetative matter*

| Source of evidence | Search of academic databases | Online search | Stakeholder proposals (steering group, expert interviewees, call for evidence) | Total |
|---|---|---|---|---|
| **Number at each stage** | | | | |
| Evidence search | 5,315 | NA | NA | >5,000 |
| Initial screening | 492 | 100 | 136 | 706 |
| Screened evidence | 165 | 27 | 63 | 252 |
| Evidence extraction | 68 | 9 | 30 | 107 |
| Included in synthesis | | | | 72 |



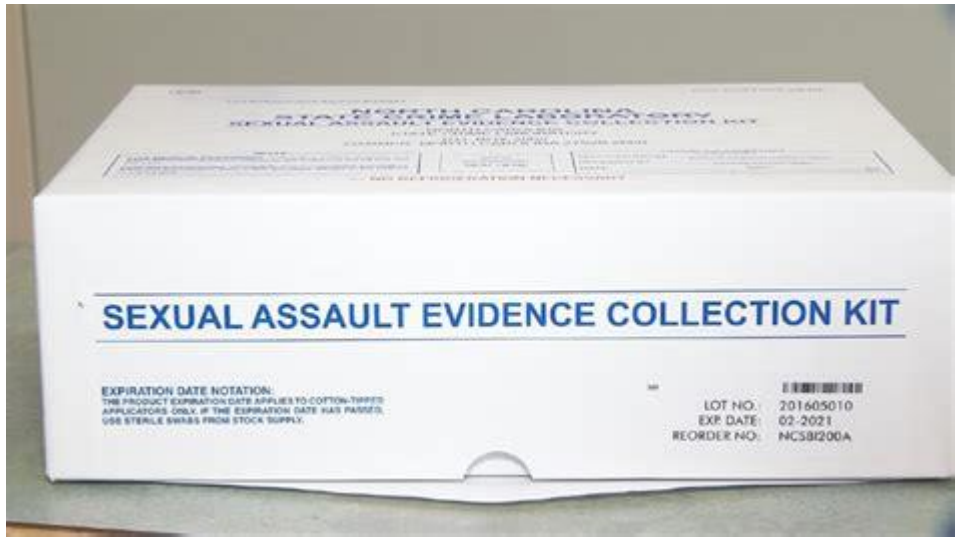
**How Evidence can be used?**

# Evidence Collection /Acquisition

Digital evidence can be collected by following these best practices:

1. Photograph the computer and scene.
2. If the computer is off, do not turn it on.
3. If the computer is on, photograph the screen.
4. Collect live data - start with RAM image (Live Response locally or remotely).
5. Collect network traffic.
6. Collect volatile data.
7. Collect non-volatile data.

# Evidence Collection (Kits)




# challenges while collecting digital evidence

Some of the challenges faced while collecting digital evidence are:

- Lack of availability of proper guidelines for collection acquisition and presentation of electronic evidence.
- Rapid change in technology.
- Big data.
- Use of anti-forensic techniques by criminals.
- Use of free online tools for investigation.
- Data is stored in electronic media and it can get damaged easily.
- Collecting data from volatile storage.
- Recovering lost data.
- Ensuring the integrity of collected data.

# Evidence preservation

Digital evidence preservation is a comprehensive endeavor that ensures the continued accessibility of valued digital information. It aims to isolate and protect digital evidence exactly as it was found, without alteration, so that it can later be analyzed.

Some of the critical steps in preserving digital evidence are:
- Do not change the current state of the device.
- Power down the device.
- Do not turn off the device.
- Do not log in to the device.
- Do not shut down the device.
- Do not install any software on the device.
- Do not connect any devices to the device.
- Do not modify or delete any files on the device.

# Evidence preservation Kits

# Evidence Examination

Digital evidence examination is the process of extracting and analyzing digital evidence. Extraction refers to the recovery of data from its media. Analysis refers to the interpretation of the recovered data and putting it in a logical and useful format. Actions and observations should be documented throughout the forensic processing of evidence.

Examination is best conducted on a copy of the original evidence. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence.

**Recent Literatures about evidence examination**

**Blockchain-based, Decentralized Evidence Archive System using IPFS**

**Abstract:** In spite of growth in technology, Indian Judiciary system somehow lacks digitalization. In the court trials cases, every argument by the lawyers, evidence presentation, witness/suspect cross examination everything will be noted down by the stenographer and everyday hearings details will be printed at the end of every court sessions. Therefore, the details about particular case will be in physical files as well as in digital format and can be accessed whenever it is needed like in the situation of case reopening. Data integrity is important in the judiciary system; when it comes to court cases, evidence integrity must be protected because even little changes in the evidence can lead to false judgments, and historical data is crucial. Where historical data archiving is necessary, Blockchain technology is suited. In the modern era, Blockchain technology is regarded as more reliable technology than any other. Blockchain technology can be used in the justice system to provide privacy and integrity, as well as efficient auditability and traceability, for storing case records and evidences. This research study has proposed a novel method using Inter Planetary File System distributed data storage to store case details and evidences on top of the Ethereum Blockchain. The case details can be stored using text and image files. The Ethereum smart contract is used for storing hash value of data in the Blockchain. The storage and access of the data in InterPlanetary File System is studied and explained using an experimental setting.

**Recent Literatures about evidence examination**

## Forensic memory evidence of windows application

**Abstract:** In modern digital investigations, forensic sensitive information can be gathered from the physical memory of computer systems. Digital forensic community feels the urge towards accurate data collection, preservation, examination, validation, data analysis and presentation. This investigative process has become an essential part of digital investigation. The extraction of forensically relevant evidence from the physical memory can reveals users' actions. This research will report the amount of evidence that can be extracted and how the evidence changes with the length of time that the system is switched on and the application is still opened. In this experiment, the quantitative assessment of user input on the most commonly used applications will be presented.

## Recent Literatures about evidence examination

### Hard evidence from computers

**Abstract:** It is becoming more and more common for criminals to use computers in the execution of a crime and there are many ways of recovering information from an assortment of storage media to find out what a computer has been used for. However, to do this, one must first know which computer has been used; without a target machine it is very difficult to link a person with a crime. In perpetrating a crime it is often only the output from a computer, in the form of a letter, set of accounts, counterfeit document or pornographic picture, which is recovered by the investigator. Document examination skills can be used to link these documents with a particular printer and thus lead to the computer that has been used. By combining the sophisticated techniques of the computer analyst with the more traditional skills of the document examiner, the Forensic Science Service has developed an investigation unit capable of assisting in a wide range of circumstances from the initial discovery of a crime to the presentation of evidence in court. The paper presents a survey of the types of evidence that may be gained from the examination of documents produced by, or associated with computers.

**Recent Literatures about evidence examination**

**iOS Digital Evidence Comparison of Instant Messaging Apps**

**Abstract:** The presence of IM (Instant Messaging) applications can have a negative impact, one of which is cybercrime. Its development is also accompanied by the development of operating systems on mobile devices used, one of which is iOS. The research conducted not only analyzed digital evidence but also compared the findings of digital evidence in WhatsApp, Telegram, and Messenger IM applications based on iOS version 13.3 on two conditions (jailed and jailbreak). The NIST 800-101 Revision 1 method is used as a guide in conducting the forensic process. Data acquisition was carried out using the Cellebrite UFED 4PC tool, data examination and data analysis were carried out using Oxygen Forensic Detective, FTK Imager and Autopsy. The results of the analysis obtained are then compared to the condition of the iPhone and the scenarios that have been executed. The results of this study indicate that the condition of the iPhone that has been jailbroken greatly affects the findings of digital evidence. WhatsApp digital evidence found on jailed iPhone devices has the same amount as the jailbroken iPhone condition with a digital evidence finding value of 71.42%. Telegram obtains more digital evidence with a digital evidence finding value of 71.42% on a jailbroken iPhone. The Messenger application shows its significance to the digital found in a jailbroken iPhone which has a percentage value of 85.71% digital discovery which is the largest value between WhatsApp and Telegram.

**Recent Literatures about evidence examination**

## Analysis of Windows 11 Link File Artifact for Evidence Gathering

**Abstract:** The objects created by the operating system are known as artifacts, and they contain crucial data about the actions taken by computer users. Thus, these artifacts are of great relevance to the forensic analyst. These artifacts can act as a evidence in a court of law to prove the digital crime. Link File or Shortcut file is one such object, presence of which confirms the usage of file in recent time. Link File are links between the executable and the applications. In this work, Link File is forensically analyzed and bring out its forensic value, knowledge it provides and perform few in-depth forensics examinations on Link File useful for analyst using open source FTK Imager tool. Lastly, we compared the Link File artifacts in various versions of Windows Operating System

**Recent Literatures about evidence examination**

## Examining Digital Forensic Evidence for Android Applications

**Abstract:** The examination of digital forensic evidence is a science highlighting the main areas of progress in forensic science. Various social media sites (SNS) providing e-mail services, messages, pictures, and videos have brought about a huge explosion in development. In recent times, Digital Forensics has expanded to be used in all institutions and companies, especially financial companies, pharmaceutical companies, and investment companies. With this electronic development, criminal activities have dramatically increased to obtain and steal data for personal or international interests or the so-called data theft. Therefore, the biggest challenge lies in protecting this information from theft and searching for digital forensic evidence so that the digital evidence is correct and sound from a forensic point of view. Against this, this paper provides a detailed review of the most important Android applications in digital forensics to attain, retrieve, and compare information altogether.

**Recent Literatures about evidence examination**

## Digital forensics: Electronic evidence collection, examination and analysis by using combine moments in spatial and transform domain

**Abstract:** A novel digital forensics tool is developed by combining wavelet invariant with spatial moments. A forensic printed circuit board image matching system is presented that is capable of probing a large database of digital images of circuit boards and compare them for similarity to provide investigation leads for electronic crimes digital forensic science investigations. The developed system has been implemented, and proved to be very efficient in detection similarities between a target image and a large image database even when the target image is noisy, scaled or mirrored.

## Recent Literatures about evidence examination

### Evaluation of Digital Evidence in Criminal Proceedings in Croatia with a Focus on Preservation Requirements and Role of Standard Operative Procedures

**Abstract:** Collection and analysis of digital evidence in criminal proceedings entails risks, such as the contamination of evidence during seizure and/or search of a computer system and the inability to establish its authenticity, which may affect its admissibility and credibility before the courts. For that purpose the requirement on digital evidence preservation is prescribed in the criminal procedure law, which should apply by default to all relevant actors. Analysis of available court decisions and rules of the Criminal Procedure Act confirms that the claims concerning mishandling and/or manipulation of digital evidence do not affect ex lege inadmissibility of such evidence. Such claims would be subject to examination on the credibility (reliability) of evidence before the courts. Any detailed technical procedures and measures to be implemented so as to ensure digital evidence preservation are best suited for regulation by standard operative procedures or perhaps even by sub-legal acts. To that effect, the standard operative procedures discussed in this paper have a proven ability to ensure the common goal of ensuring digital evidence preservation. Adherence to best practices stemming from standardized procedures has shown to be vital for ensuring that investigatory procedures and acquired digital evidence are valid and as such accepted throughout the criminal proceedings.

**Recent Literatures about evidence examination**

## Verifiable Limited Disclosure: Reporting and Handling Digital Evidence in Police Investigations

**Abstract:** Police investigations involving digital evidence tend to focus on forensic examination of storage units on personal electronic devices (laptops, smartphones, etc). However, a number of factors are making digital forensic tools increasingly ineffective: (i) storage capacities of electronic devices have increased, and so has the amount of personal information held on them, (ii) cyber crimes are increasingly committed on social media, and evidence of crimes are held on social media platforms, not necessarily on personal devices, (iii) there is a greater need for protecting digital privacy, especially when examining digital evidence from witnesses and victims of cyber crimes. These factors pose a number of practical challenges for both law enforcement agencies and citizens when disclosing and handling the digital evidence. This paper defines and illustrates the key challenges, and proposes the concept of verifiable limited disclosure, which defines a communication protocol to ensure privacy, continuity and integrity of digital evidence. More specifically, the protocol allows (i) citizens to decide what evidence to disclose to law enforcement agencies and (ii) any of the two parties to be able to prove any tampering of the disclosed evidence. The paper discusses methods for implementing the communication protocol using standard security and privacy tools and presents a pathway to evaluating their effectiveness.

# Evidence Examination tools (selection criteria)

some of the best digital forensics and cybersecurity tools. In selecting from the wide range of options, we considered the following criteria:

**Affordability**: Price may not indicate quality, but collaborative peer reviews can be. Most of the tools below are open-sourced, and all are free and maintained by a community of dedicated developers.

**Accessibility**: Unlike some proprietary brands which only sell to law-enforcement entities, all of these are available to individuals.

**Accountability**: Whether through open source projects or real-world testimonials, experts have thoroughly vetted these technologies.

**Tool used for evidence examination + Common sense**

1. Autopsy - Autopsy (sleuthkit.org)
2. Bulk Extractor: Digital Corpora: downloads/bulk_extractor/
3. CAINE - CAINE Live USB/DVD - computer forensics digital forensics (caine-live.net)
4. Digital Forensics Framework - GitHub - arxsys/dff
5. DumpZilla - dumpzilla forensic tool
6. EnCase - OpenText Encase Forensic
7. FTK Imager -Exterro - E-Discovery & Information Governance Software
8. MAGNET RAM Capture - MAGNET RAM Capture - Magnet Forensics

More Information : https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools

# Evidence Analysis

Evidence analysis is the process of examining and interpreting evidence to determine its significance. It involves the application of scientific methods and techniques to the examination of physical evidence.

The analysis process includes identifying, preserving, and analyzing the evidence. The goal is to determine what happened, how it happened, and who was involved. The analysis process should be conducted in a controlled environment to ensure that the integrity of the evidence is maintained.

+ experience required

# Evidence Presentation (in the court)

Evidence presentation is the process of presenting evidence in a clear and concise manner. The goal is to present the evidence in a way that is easy to understand and that supports the conclusions that are being drawn.

The presentation of evidence can take many forms, including written reports, photographs, videos, and charts. The presentation should be tailored to the audience and should be presented in a way that is appropriate for the situation.

# Evidence Acquisition process

**What are write blockers?**

A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data. A write blocker, when used properly, can guarantee the protection of the data chain of custody.

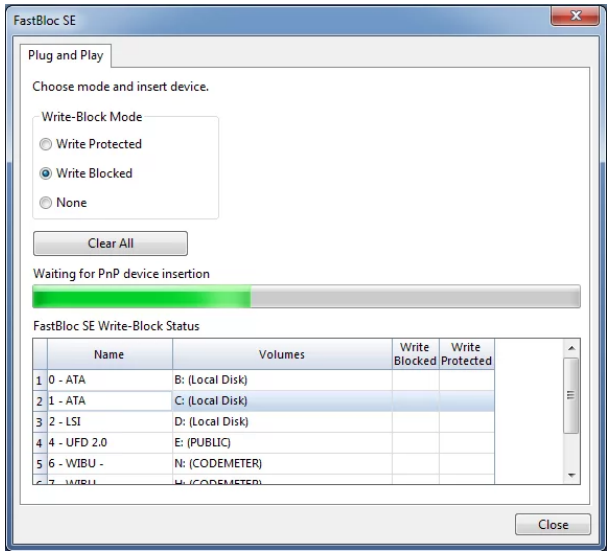

**Software versus hardware write blockers**

Software and hardware write blockers do the same job. They prevent writes to storage devices. The main difference between the two types is that software write blockers are installed on a forensic computer workstation, whereas hardware write blockers have write blocking software installed on a controller chip inside a portable physical device.

# Evidence Acquisition process

**Write-Blockers - Softwares**





**Hardware Write Blocker**

| Pros | Cons |
| --- | --- |
| ▪ Is not reliant on an underlying operating system or software-based subsystem.<br>▪ Is easier to explain and generally makes more "sense" to non-technical people.<br>▪ Clear visual indication of function through physical lights/switches.<br>▪ Generally provides built in interfaces to a number of storage devices (IDE, SATA, etc.).<br>▪ Appears to be more accepted in the general forensics community. | ▪ An additional piece of kit to carry around with you.<br>▪ An additional piece of hardware that needs to be maintained and could fail.<br>▪ Generally restricted to the available storage interfaces built into the device (additional interfaces cannot be added). |

**Software Write Blocker**

| Pros | Cons |
| --- | --- |
| ▪ The software write blocker is directly installed on your image acquisition workstation and additional hardware is not necessary (lightens the load, one less thing to fail, etc).<br>▪ Generally able to use any interface available on your imaging workstation (and any interface that could be added down the road) – prevents an additional purchase when a new storage interface is needed. | ▪ Generally still needs an external adapter of some sort to provide an interface to the drives that you are imaging (thus negating the pro of not having to carry around a physical write blocker).<br>▪ Can be more difficult to explain to a non-technical person (and thus more difficult to explain that the write blocker is actually functioning, if challenged).<br>▪ Reliant on underlying and complex hardware and/or software (i.e. operating systems). Interaction between these components creates additional complexity and introduces the possibility of failure through updates, upgrades, etc. |

# Imaging Techniques

Copy the URL and paste in browser, press enter, for more information

https://toolcatalog.nist.gov/search/index.php?all_tools=all&ff_id=1&1%5B%5D=any&2%5B%5D=any&3%5B%5D=any&4%5B%5D=any&5%5B%5D=any&6%5B%5D=any&7%5B%5D=any&8%5B%5D=any&10%5B%5D=any

https://toolcatalog.nist.gov/search/index.php?ff_id=1

# Evidence Integrity

**What is evidence integrity?**

Evidential Integrity means the state whereby there is assurance, sufficient to satisfy any judicial assessment, that Evidential Records have been correctly and lawfully generated and have not undergone unauthorised amendment or been otherwise tampered with since their creation

**How do you ensure evidence of integrity?**

Digital evidence integrity is ensured by calculating MD5 and SHA1 hashes of the extracted content and storing it in a report along with other details related to the drive. It also offers an encryption feature to ensure the confidentiality of the digital evidence.

**Why is it important for evidence integrity?**

Evidence is the key to solve any crime. Evidence integrity needs to be protected in order to make it admissible in the court of law. Digital evidence is more revealing, but it is fragile; it can easily be tampered with or modified. There are different techniques available to protect the integrity of digital evidence.

# SOP

**Standard Operating Procedures for Acquisitions and Preservation of Evidence.**

https://citizen.goapolice.gov.in/web/guest/forensic-science-lab

https://keralapolice.gov.in/storage/pages/custom/ckFiles/file/7GafuMCjLbFgjBNh8aXz8WhLv2Zqtfczvbi7Uv6m.pdf

https://www.ojp.gov/pdffiles1/nij/254661.pdf

https://www.acq.osd.mil/asda/dpc/ce/cap/docs/piee/PIEE_Records_Retention_and_Destruction_SOP_20200615.pdf

https://rm.coe.int/3692-sop-electronic-evidence/168097d7cb

**How to prepare SOP- Guidelines**

https://www.epa.gov/sites/default/files/2015-06/documents/g6-final.pdf

# Introduction to Data Recovery and Carving

**What is data recovery ?**

Data recovery is the process of retrieving lost or deleted data from a storage device. There are two types of data recovery techniques: software-based and hardware-based.

Software-based techniques use utilities that can read and copy the data from the problem storage.

Hardware-based techniques involve repairing or replacing the damaged parts of the device in a laboratory. Data recovery can be performed with different tools, such as Disk Drill or Recuva, that can scan and restore the files with their original folder structure

# Introduction to Data Recovery and Carving

**What is data carving ?**

Data carving is the forensic technique of reassembling files from raw data fragments when no filesystem metadata is available. It is commonly used when performing data recovery after a storage device failure. It may also be performed on a core memory dump as part of a debugging procedure. Data carving allows for detecting and recovering files and other objects based on filesystem contents rather than a filesystem's metadata and file structure

E.g. Data migration in the cloud

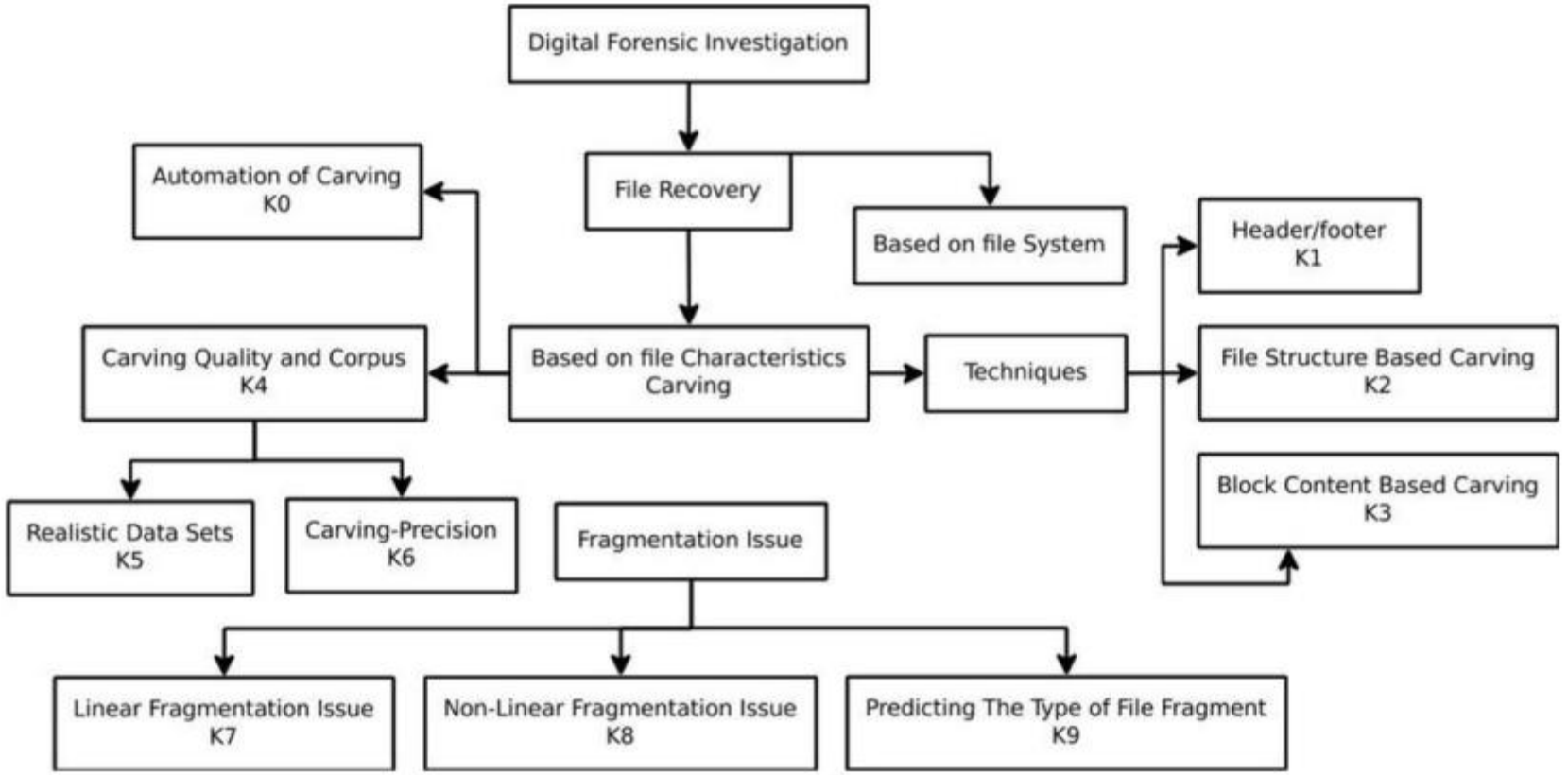
# Introduction to Data Recovery and Carving

**difference between data carving and data recovery:**

- Data carving is used when no filesystem metadata is available, while data recovery is used when the data stored in a storage device cannot be accessed in a usual way.
- Data carving detects and recovers files and other objects based on filesystem contents rather than a filesystem's metadata and file structure, while data recovery retrieves lost or deleted data from a storage device.
- Data carving is commonly used when performing data recovery after a storage device failure, while data recovery can be performed with different tools, such as Disk Drill or Recuva.
- Data carving may also be performed on a core memory dump as part of a debugging procedure, while data recovery success depends on the nature of the data loss and the timely application of the right method.
- Data carving allows for detecting and recovering files and other objects based on filesystem contents rather than a filesystem's metadata and file structure, while data recovery can be software-based or hardware-based.
- Data carving does not involve repairing or replacing the damaged parts of the device in a laboratory, while data recovery involves repairing or replacing the damaged parts of the device in a laboratory.

# Introduction to Data Recovery and Carving

**Data Carving Methods**




https://www.sciencedirect.com/science/article/pii/S2212017313003198