VOLUME 26 | SEPTEMBER, 2021 ISSN 2456-9704

# CRITICAL ANALYSIS OF DIGITAL FORENSIC IN CRIMINAL JUSTICE

*By Ananta Aggarwal*
*From Amity Law School, Noida*

## ABSTRACT
Although cybercrime is on the rise, it is uncertain if law enforcement authorities will be able to investigate and effectively punish those responsible. As a result of the many publicised assessment process, it has become clear that law enforcement authorities are unable to properly undertake inquiries of the number and complexity that are present in many of these instances, even if they have been doing them for many years. Forensic digital forensics was addressed in this research along with cyber-crime and the global economic growth. Other topics included the reasons for conducting a case, the many branches of digital forensics, potential sources for evidence and data, and standard operating procedures.

***Keywords***: Digital Forensic, Criminal Justice, Investigation, Legal aspects.

## INTRODUCTION
Computers are used to perpetrate crimes, and law enforcement increasingly utilises computer to combat crime due to the expanding field of digital data forensics.

A digital piece of evidence may be used in court if it's saved or transferred as binary data and can thus be relied upon. Amongst many other locations, it may be located on a computer hard disc or a mobile phone. Child pornography and credit card fraud are both examples of e-crime for which digital evidence is frequently used. The use of digital evidence is no longer limited to e-crime prosecutions; it is being utilised in all kinds of criminal prosecutions. E-mails and mobile phone files, for example, may include crucial information about the motives of the suspects, their locations at the time of the crime, and their connections with other criminals. At least 10 people had their lives cut short since 1974 when the BTK serial murderer went on the run, thanks to the use of an old floppy disc.

Computer forensics, or the collecting and analysis of digital evidence, is being integrated into the architecture of law enforcement agencies as a means of combating e-crime and gathering relevant forensic evidence for all offences. The requirement to educate police to gather digital evidence and keep up with quickly changing technology like computer operating systems puts criminal justice organisations under pressure.

As the amount of digital crime rises, so does the need for law enforcement personnel with computer forensics skills. A large number of law enforcement organisations, such as your local police officer and the CBI, depend on computer forensic evidence to help them capture bad guys.

A technique is currently in use for computer forensics, which is rapidly expanding in usage in a wide range of criminal investigative applications. Computers have always been associated with criminal activity, but now the roles are reversed, and forensics may utilise computer forensics to apprehend perpetrators who think their

crimes go unpunished because they don't leave a digital trail.[1]

When it comes to computer and mobile crimes, the field of digital forensics (also known as digital forensic science) is particularly important since it deals with the recovery, investigation, inspection and analysis of evidence discovered on digital media.

Original definition of the word "digital forensics" included examination of digital data stored on any device. However, this definition now encompasses all devices that can store digital data. Its origins lie in the personal computer revolution, which erupted about 1977 or 1978. The subject took shape in bits and pieces throughout the 1990s, and policy measures didn't develop until the dawn of the new century.

There are many uses for digital forensics investigation. The most typical use is in criminal or civil court to prove or disprove a theory. Murder, theft, and assault on the person are just a few examples of crimes that are pursued by the government when someone is accused of committing them. To put it another way: Civil lawsuits concern themselves with preserving the individual's right to privacy (typically in relation to family conflicts), whereas business lawsuits frequently include some kind of electronic discovery (eDiscovery) as part of the digital forensics' investigation.

Additionally, in the business sector, forensics may play a role, for example, in internal company investigations or in penetration investigations, which are investigations by specialists into the nature and scope of an illegal network intrusion.
Investigations are split into many sub-areas according to the kind of digital devices involved; computer and network forensics, forensic data analysis, and mobile device forensics are examples of these branches. Seizure, forensic imaging (capture), and examination of digital media are all common forensic procedures.[2] A report on the evidence gathered is also common.

Forensic digital forensics may be used to find direct proof of a crime, establish alibis, assess intent, identify sources (e.g., in copyright disputes), or authenticate documents in addition to identifying evidence. Forensic investigations may include considerably more complicated time-lines or hypotheses than other fields of forensic research (where the typical goal is to give answers to a series of simpler inquiries).

If you're in the legal profession, you know how fast digital forensics can move from a plot device in one of your favourite TV shows to a critical piece of evidence in your case. In the field of forensic science, Digital Forensics refers to the process of recovering and analysing data from digital devices. Digital Forensics Specialists can help you retrieve important data to support your case.
Cybercrimes, or crimes involving a security breach in a system or network, are often investigated by Digital Forensics Specialists. Digital forensics experts can help in a variety of ways when a cybercrime happens. From protecting data that has been obtained by criminals to re-constructing data from computers on the network suspected of being engaged in criminal activity and/or contract

[1] CRL.A. 527 of 2014

[2] 1984 AIR 1022, 1984 SCR (3) 292

or fiduciary responsibility breaches, they provide a wide variety of services.[3]

Forensics is a straightforward subject on paper, but it's much more complicated in reality. It's a digital archaeology with a deadline on its side. Finding data to utilise in a study makes this process more challenging. In order for information to be useful in court, it has to be preserved using forensic methods. First Legal creates a duplicate of the drive using our proprietary software, preserving the original's format. The next step is to build a working copy that will be used to conduct research.

Both businesses and legal firms may benefit from digital forensics. It's very uncommon for companies to hire a forensic investigator to assist them construct a case against an employee they suspect is disseminating trade secrets or keeping unlawful material on their premises. While the employee may be able to delete their own personal data, it is very improbable that they will have access to the company's network or servers. As a result, knowing where to search is all that is required to win the case. Information pieces will be used to piece together what occurred by creating a digital picture of the server at the workplace.

The easiest way to get evidence from a digital device that may be relevant to your case is to hire a certified investigator who is well-versed in digital forensics. When you employ a certified investigator, you can be certain that the data they gather is accurate and free of bias. The majority of our licenced investigators at First Legal have come from the law enforcement community, with a focus on digital forensics. All of these sleuths are well qualified and have a lot of trial experience. There will be an opportunity for your investigator to speak about their actions as well as their justifications and techniques. In addition to delivering the facts, a skilled forensic investigator also understands how to modulate their voice intonation. When they look at the jurors, they know to look at the judge. You need to work with investigators that know how to testify since even the smallest facts may have a significant effect on your case.

**HISTORY**

Before the 1970s, existing laws were used to prosecute computer crimes. The Florida Computer Crimes Act of 1978 recognised the first computer crimes by outlawing the illegal addition, deletion, or alteration of data on a computer system without permission. Laws were enacted to address copyright, privacy/harassment (such as online harassment, happy smacking and cyberbullying) and child pornography as the types of computer offenses perpetrated grew in the following years. In the 1980s, federal laws started to include computer crimes for the first time. In 1983, regulation was first passed in Canada. The Federal Computer Fraud and Abuse Act of 1986 was followed by changes to the Australian Crimes Act in 1989 and the British Computer Misuse Act in 1990 in the United States and the United Kingdom, respectively.[4]

**1980s–1990s: Growth of the field**

In the 1980s and 1990s, as computer crime grew in popularity, law enforcement agencies began to form specialist units to handle technological elements of inquiries. These

[3] Ibid

[4] "Florida Computer Crimes Act". Archived from the original on 12 June 2010. Retrieved 31 August 2010

units were often formed on a nationwide basis. To provide two examples, in 1984 the FBI established a "Computer Analysis and Response Team, and in 1985 the British Metropolitan Police fraud squad" established a computer crime unit inside its fraud squad. There were also computer enthusiasts among the early members of these organisations who were in charge of the field's initial research and direction.

As early as 1986, Cliff Stoll's investigation of hacker Markus Hess used computer forensics in a real-world setting. Stoll, who used computer and network forensic methods in his inquiry, was not a trained investigator. Early forensic exams often followed the same pattern.

These new and fundamental investigative resources were in great demand throughout the 1990s. As a result of the increased demand on central units, regional and even local level organisations were formed to assist manage the workload. As an instance, "the British National Hi-Tech Crime Unit (now known as the Serious Organised Crime Agency (SOCA)) was established in 2001 to offer a national infrastructure for computer crime, with people stationed both centrally in London and with different regional police forces."[5]

Throughout that time, the discipline of digital forensics evolved from the ad hoc tools and methods created by these hobbyist practitioners. The other forensic disciplines evolved from scientific research, not the other way around. A publication by Collier and Spaul in 1992 sought to convince the forensic science community of the value of this new field of study, which had previously only been utilised informally. Because of this rapid growth, there was a dearth of standards and training. He stated in 1995 in his book "High-Technology Crime: Investigating Cases Involving Computers" that the biggest forensic problem for law enforcement in the 1990s was to seize, preserve, and analyse evidence held on computers. Police and detectives frequently gather and analyse electronic data even though forensic procedures like fingerprinting and DNA testing are typically conducted by highly trained specialists.

**2000s: Developing standards**

The necessity for uniformity has prompted the publication of digital forensics standards since 2000 by a variety of organisations and authorities. "Best practises for Computer Forensics," published in 2002 by the Scientific Working Group on Digital Evidence (SWGDE), was supplemented in 2005 by the release of an ISO standard. The Convention on Cybercrime, a European-led international convention, went into effect in 2004 with the goal of harmonising national computer crime legislation, investigative methods, and international cooperation. Too far, 43 countries have ratified the pact and 16 have signed it (including the United States, Canada, Japan, South Africa, the United Kingdom, and several European states).

The topic of education was also addressed. Commercial organisations (typically forensic software makers) started to provide certification programmes, and Centrex, the UK's specialised investigator training

[5] Simson L. Garfinkel (August 2010). "Digital forensics research: The next 10 years". Digital Investigation. 7: S64–S73.

facility, includes digital forensic analysis as a subject on its curriculum.

Even for crimes not usually connected with digital forensics, mobile devices, which advanced beyond basic communications systems in the late 1990s and have been proven to be valuable sources of information, have grown more readily accessible. It's still difficult to do a thorough digital examination of phones because of the unique nature of the devices.

With the rise of cybercrime comes the threat of cyber warfare and terrorism. The Joint Forces Command of the United States determined in a study released in February 2010 that adversaries would use cyberspace to attack business, academia, administration, and military forces in the air, land, sea, and space domains. Cyberspace has shattered the physical boundaries that protect a nation's trade and communication in the same manner that airpower did during World War II.

Digital forensics is still dealing with problems that have yet to be addressed. According to Peterson and Shenoy's "Digital Forensic Research: The Good, the Bad, and the Unaddressed" article from 2009, digital forensics research has a preference for Windows operating systems. In 2010, Simson Garfinkel outlined the challenges that digital investigations will face in the future, such as the growing size of digital media, the widespread availability of encrypted data to customers, the rising amount of computer systems and file formats, and the legal restrictions placed on investigators. The study also found problems with on-the-job training and exorbitant entry costs for newcomers to the profession.

**Development of forensic tools**

When digital forensic tools were few in the 1980s, investigators had to rely on live media analysis, looking at systems from inside the operating system and extracting evidence with available sysadmin tools. Accidentally or not, this technique posed the danger of altering disc data, giving rise to allegations of evidence tampering. In the early 1990s, a variety of tools were developed to deal with the issue.

The Government Security Training Centre initially identified the need for such software in 1989, leading to the development of IMDUMP (by Michael White) and Safe Back in 1990. (Developed by Sydex). DIBS (a hardware and software solution) was commercially launched in 1991 in the UK, while Rob McKemmish made Fixed Disk Image available to Australian law enforcement for free in 1992. Examiners might make an identical duplicate of a piece of digital material to work on while keeping the original disc intact for verification thanks to these toolsets as the need for digital evidence increased in the late 1990s, commercial systems like EnCase and FTK[6] were created that allowed analysts to analyse copies of media without having to use live forensics to study the originals. With the rise of "live memory forensics" in recent years, technologies like Windows SCOPE have become available.

Similar tool development has recently happened for mobile devices; originally, investigators were able to obtain data directly

[6] • ISO/IEC 17025:2005, General Requirements for the Competence of Testing and Calibration Laboratories, 1st Revision, 2005, International Standard Organization.

from the device, but specialised tools like XRY or Radio Tactics Aceso quickly emerged.[7]

**Why digital evidence forensics matters**

However, the private and confidential nature of this data makes it impossible to achieve its full value for police departments and law enforcement organisations. Digital evidence forensics is a way of gathering, preserving, and analysing forensic information that is becoming more essential in crime solving and other legal problems, even though pcs and other data gathering equipment are used everywhere. It helps civil and criminal judicial systems by guaranteeing the integrity of digital evidence in court.

The gathering, processing, and distribution of digital evidence may be expedited via digitalization rather than manual procedures for agencies that span the whole spectrum of police departments and criminal justice. There are a number of key investigative technology solutions available in the EvidenCentral Marketplace that have been pre-integrated, vetted and pre-certified to operate with EvidenCentral's "end-to-end digitalization system, includes Nice Investigate and Nice Inform solutions. To make virtual hearings and testimony in court more efficient, the legal profession is increasingly relying on technology solutions. As businesses strive to enhance their agility, speed, and data-driven decision-making, digitalization is not a new requirement for business executives. However, COVID-19 has made it much more important.

The pandemic is a watershed moment for change, and the underlying reason driving digital transformation at this time is the increasing and growing need for digital intelligence. Legal professionals were only beginning to explore the full potential of technology prior to the outbreak. Investing in digital transformation may lead to a variety of problems, including architecture, security, and dependability, among others. Government agencies must help communities comprehend about using techniques for the advantage and protection of residents as well as how to concentrate, inside the legislative structure, on some kinds of information due to crime actions. Privacy issues and a lack of confidence among municipal governments and police departments are critical topics in most nations.

**Forensic process**

An inquiry into digital forensics is usually divided into three stages: the collection of evidence, analysis, and presentation. In an ideal world, acquisition would entail taking a picture of the device's volatile memory (RAM) and making an identical copy of the medium at the industry level (or "forensic duplicate"), sometimes with a write obstructing measure to prevent the source from being modified. As storage media have grown in size and innovations like cloud computing have emerged, more people are turning to "live" acquisition, where a "logical" duplicate of the data is obtained rather than a full picture of the actual storage medium. An image (or logical copy) is created by hashing the original media/data (using a method like SHA-1 or MD5) and then comparing the results to the hashed values.

'Hybrid Forensics' (also known as "distributed Forensics") is an alternate (and

[7] Ibid

patent-pending) method that integrates digital forensics with eDiscovery. This strategy was implemented in a commercial product called ISEEK, which was presented at a symposium in 2017 along with test results.

It's important to note that evidentiary material is recovered throughout the analysis step utilising various methods and technologies. This stage was described as "an in-depth systematic search of evidence linked to the alleged crime" in an article published in the International Journal of Digital Evidence in 2002. Professor of criminal justice Brian Carrier proposed an "intuitive process" in 2006, where the obvious information is first discovered and then "extensive searches are undertaken to help fill in the gaps."[8]

A variety of methods are used to perform search terms throughout digital media (including files and unclaimed and slack area), recover lost data, and extract registry information, although these are the most popular (for example to list user accounts, or attached USB devices).

Often, less-skilled employees may conduct analyses of the data to recreate past events or acts and draw general judgments. Following the completion of an inquiry, the findings are typically documented in a written report that is accessible to the general public.

**Collecting Criminal Evidence**

Computer forensics has progressed to the point that it may be used as evidence in a court of law. Evidence management and collection has become a very precise procedure in law enforcement because of this. Computer forensics experts are in great demand.

Hacking, espionage, and bank fraud are all types of crimes for which the FBI employs IT experts to gather important evidence. Computer forensics have now become a common investigative technique for the FBI. In certain instances, proof of premeditation may be collected via technologies like as cell phones, tablets, and hard drives.

Criminal investigators' use of computer forensics is expanding all the time. Crimes committed by criminals utilising technology are increasing in number as it improves.[9]

Computer forensics has a solid reputation for detecting fraudsters of all stripes. While this is still the case, the police are now utilising computer forensics to find serial killers, and they have daily access to encrypted material that may be used in court.

**Computer Forensics Tools and Tasking**

Researchers are those who choose to work in this field. Encrypted files and the "living box" approach, as well as many other fantastic new software types utilised in the most recent methods accessible, will be investigated by them. Those in the area of information technology who make this choice are regarded as unique.

In this phase of the criminal probe, many of the duties include retrieving lost files, looking for security vulnerabilities in

[8] The Role and Impact of Forensic Evidence in the Criminal Justice Process by Joseph Peterson, Ira Sommers, Deborah Baskin, and Donald Johnson,2010

[9] Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies by Teri A. Cummins Flory ( Purdue University),2016

cybercriminals, and deleting passwords. For attorneys, judges and juries to evaluate, information must be controlled and translated after it has been gathered.

While it's tempting to believe that computer forensics' primary job is to retrieve fraud data, that's absolutely not the case. As most of the early cases solved were of this kind, computer forensics got its start this manner. The BTK Killer, on the other hand, was apprehended and computer forensics found during a search of his house were utilised as evidence in his court case.[10]

Is there a history of computer forensics dating back to the days of the floppy disc? Certainly, and police are using computers with everything from search to warrants. As technology progresses, so will criminals' methods of concealment. Technology and the methods by which it is studied seem to have no upper limit.

**Cold Case Files Solved Using Computer Forensics**

Cold case files are being reopened and solved with the use of digital forensics by law enforcement authorities. When new technology emerges, it opens up new opportunities for accessing data from old hard drives in order to solve crimes that have been unresolved for a long time.

As databases are used to store case files for law enforcement, computer forensics will play an increasingly important part in criminal investigations. The mere act of collecting and organising old forensic evidence from unsolved cases has revealed information that investigators may have overlooked during the early stages of the case. These advancements have the potential to transform criminal investigations forever.

**The Role of Computer Forensics in Crime**

Due to the increasing difficulty for law enforcement in obtaining information that may be used as evidence, computer forensics will be more in demand. This expanding area of research need the services of IT specialists skilled in retrieval of information for law enforcement more than ever before.

According to Forbes Magazine's list of top professions for 2015, the top spot goes to information technology (IT) specialists. Having an IT specialist on the force may help solve issues faster and have a bigger impact than just being an important member of the team.

Norwich University, the country's oldest private military school, has long been a pioneer in interdisciplinary learning. As a result of its online programmes, Norwich offers students the opportunity to make a difference in their professions and communities.

Continuing the legacy of values-based education, Norwich University offers a difficult and gratifying educational experience via organised, disciplined, and demanding coursework. More learners than ever before have access to our comprehensive curriculum thanks to online programmes like the Master of Science in Cybersecurity.

The National Security Agency and the Department of Homeland Security have recognised Norwich University as a "National Centre of Academic Excellence in

[10] SUPRA 1

Cyber Défense. With the online Master of Science in Cybersecurity degree, students have the option to specialise in five different areas such as policies, processes, and the entire framework of a cyber security programme in-depth study.[11]

## APPLICATIONS

The field of digital forensics is widely utilised in criminal cases as well as in private detective work. It has long been linked with criminal law, when evidence is gathered to prove or disprove a theory in front of the courts. There are times when the work here is done as part of an overall study that encompasses many other disciplines. The evidence gathered may be utilised for reasons other than judicial procedures, such as intelligence collection (for example to locate, identify or halt other crimes). As a consequence, forensic standards for intelligence collection are occasionally relaxed.

Digital forensics is a component of electronic discovery (also known as eDiscovery) in civil litigation and business issues. Criminal investigations utilise forensic techniques, although the criteria and limits are frequently different. Digital forensics may also be used in business investigations that don't involve the courts.

Unauthorized network infiltration is a classic case. As a damage-limitation exercise, a forensic expert examines the type and scope of the attack to determine the degree of any infiltration and to try to identify the attacker. Phone line assaults were widespread in the 1980s, but now they are almost exclusively carried out through the Internet.[12]

Digital forensics investigations are primarily concerned with locating and recovering unbiased proof of illegal conduct (termed actus reus in legal parlance). However, the wide variety of information stored on digital devices may be useful in other investigations.

### Attribution

Individual activities may be traced back to meta data and other logs. Personal papers saved on a computer's hard disc, for instance, may be used to locate the drive's owner.

### Alibis and statements

Digital evidence may be used to cross-check the information supplied by individuals involved. For instance, during the Soham murder case, the offender's alibi was invalidated by the mobile call logs of the individual he purported to be with at the moment.

### Intent

Investigations may be used to establish the intent of a criminal as well as discover concrete proof of a crime being perpetrated (known by the legal term men’s rea). For instance, convicted killer Neil Entwistle's Internet history contained allusions to a website detailing how to kill people.

### Evaluation of source

In earlier versions of MSWord, a Global Unique Identifier (GUID) was included in files to identify the machine upon which file was produced. This information may be used to track out the origin of a specific piece of

[11] Ibid

[12] M Reith; C Carr; G Gunsch (2002). "An examination of digital forensic models". International Journal of Digital Evidence.

data. It's critical to know if a file was created on the digital device under examination or whether it came from somewhere else (like the Internet).

**Document authentication**

Meta data linked with digital documents may be readily changed in relation to "Evaluation of source". When it comes to document authenticity, the goal is to identify and discover any falsifications that have occurred.

**Limitations**

In a forensic inquiry, the usage of encryption may be a significant hindrance since it prevents the first inspection from finding relevant evidence utilising keywords. Laws requiring the disclosure of encryption keys are still new and controversial. Although brute-force passwords and cryptography can be bypassed, there are methods available, such as in smartphones and Computers, where bootloader approaches are used to first obtain device material before forcing it to discover the password or encryption key.

**Branches**

Due to laws being broken by criminals and the widespread usage of tiny digital devices (such as tablets, phones, and memory sticks), the scope of a digital forensics' investigation is no longer limited to retrieving data from computers alone. Volatile memory is found in some of these gadgets, whereas non-volatile memory is found in others. For obtaining information from volatile memory, adequate methods exist. For obtaining information from non-volatile recollection resources, there is no comprehensive methodology or a framework in place yet.[13]Digital forensics inquiry may be divided into many categories based on the equipment, media, or artefacts under examination.

**Computer forensics**

To understand the present status of a digital artefact, such as a computer network, storage media, or digital records, digital forensics is used. Computers, programmable (digital devices with basic processing capability and onboard memory), and static memory are often covered under the field (such as USB pen drives).

Depending on the scope of the investigation, everything from internet history records to the actual contents on the hard drive may be examined using computer forensics. An excel spreadsheet found on Joseph Edward Duncan's computer in 2007 helped authorities prove malice aforethought and get him the death sentence. When emails describing torture and death desires were discovered on Sharon Lopatka's computer in 2006, her assassin was found.

**Mobile device forensics**

Retrieval of digital data or evidence from smart phones falls within the purview of digital forensics, which includes mobile devices. A mobile device varies from a computer in that it has an internal communication system (like GSM) and unique storage methods (like an SD card). Data such as phone numbers and communications (SMS/Email) are typically the focus of an investigation rather than recovering lost data in detail. Patrick Lumumba was cleared of the murder of Meredith Kercher thanks to SMS data gleaned from his mobile cell phone.

[13] STANDARD OPERATING PROCEDURE OF DIGITAL EVIDENCE COLLECTION (Digital Forensics Department, Cybersecurity Malaysia)

Cell site logs, which monitor the gadgets within its range, or the inbuilt gps/location tracking of mobile devices are both helpful for giving location information. In 2006, the kidnappers of Thomas Onofri were tracked down thanks to information gleaned from such a database.[14]

**Network forensics**

To obtain intelligence, gather evidence, or identify intrusions, network forensics monitors and analyses computer network traffic, both locally and across wide area networks (WANs). In most cases, traffic is snooped at the packet level and either saved for further analysis or immediately censored. Network data, in contrast to other types of digital forensics, is often dynamic and seldom recorded, making the field very reactive."

"Computer hackers Aleksey Ivanov and Gorshkov were enticed to the United States by the FBI in 2000 for a fictitious interview for a job". The FBI was able to gather information from Russian-based devices by monitoring network traffic from the duo's laptops.

**Forensic data analysis**

In digital forensics, Forensic Data Analysis is a subfield. It looks at data structure to see if there are any trends of potential fraud that may be traced back to financial crime.

**Database forensics**

In digital forensics, database forensics refers to the study of databases and associated information for forensic purposes. In order to construct a chronology or retrieve important information, investigators make use of database content, log files, and in-RAM data.

**Cybercrime and Global Economic Growth**

A cybercrime is one that takes place when someone is connected to the Internet, whether that person is physically present or not. Child pornography, kidnapping minors via chat rooms, and other forms of online abduction are all examples of computer crime. Other types of computer crime include scams, cyber-terrorism, and the development and/or spread of viruses such as Spam and phishing. All of these offences are made easier by computers.

The definition of a cyber-attack is "deliberate acts to modify, disrupt, mislead, degrade, or destroy information systems and network or the information and/or programmes residing in or traversing these systems or networks," according to the FBI. Using cyber-attack weapons is straightforward[15]. The results vary from simple defacing of a webpage to data theft and theft of intellectual property, spying on target network, and even major service interruption caused by cyber-attack weapons.[16]

Cyber criminals have a variety of goals, but they all have access to the resources necessary to develop attack vectors that lead to their objectives being met. They may defraud, steal identities, steal money, and loot companies, banks, countries, regions, and even people. They may also conduct these crimes.

[14] Forensic Examination of Digital Evidence: A Guide for Law Enforcement

[15] Legal Aspects of Digital Forensics by Daniel J. Ryan and Gal Pantzer

[16] ISO/IEC 27037:2013, Guidelines for Identification Collection, Acquisition and Preservation of digital evidence, International Standard Organization.

As a global issue, cybercrime poses the greatest danger to businesses of all sizes. Numbers represent the societal effect. More sophisticated and scalable cybercrime technologies are being used by cybercriminals to violate the privacy of their victims, and it is working. In 2017, over two billion data records were hacked, while in the first half of 2018, over 4.5 billion records were broken.

**Reasons for Conducting a Digital Forensic Investigation**

In the last decade, technology has advanced in previously unimaginable ways, and although these advancements have benefitted both people and companies, they have also become instruments for frauds and cyber criminals to steal money and data while avoiding discovery. To conceal their illegal operations and transfer money between countries and across the world, hackers rely on cutting-edge technology. It's a complicated business, and they've got a lot of resources to assist them hide from the law enforcement authorities. As a result, investigators charged with catching cyber criminals have had to keep up with the times. These crooks and their actions are being tracked by a new breed of detectives known as digital forensic practitioners. The tools and methods they utilise in combination with digital forensics offer invaluable insight into attack patterns, how criminal organisations operate, their motives, and the latest tactics and tools they use. Threat intelligence and knowledge resources benefit greatly from the evidence provided by this study.

When a business discovers a breach, the evidence obtained from a digital forensic investigation aid in incident handling and clean-up operations, as well as providing information on new attack pathways and sophisticated malware kinds that were previously unknown. Additionally, it may be used to track an advanced persistent threat (APT) that employs a wide range of tactics and technologies to accomplish its goals. Invasive, persistent threats (APTs) are aimed at specific targets and may remain unnoticed on the victim's network for weeks or even months.

A digital forensic investigation may assist find out who or what is behind these assaults. Such technologies are regularly used by security experts to investigate network intrusions—not to bring the perpetrators to justice, but to figure out how they got in and close the loophole. When files are accidentally formatted or destroyed, data recovery companies depend on comparable techniques to restore them.[17]

Digital forensics is the process for identifying, trying to collect, assessing, and trying to report on material gathered on computer systems, portable devices, and systems in such a manner that all of the proof is appealable in a legal context, regardless of the motivation for the investigation, explanation, or rebuilding of digital forensic testing. Violence, murders, people smuggling, fraud, and drug selling are just a few of the crimes where evidence is increasingly discovered on electronic devices that were either used by the offender or the victim.

The use of digital forensics is essential for law enforcement and investigations, but it may also be used in commercial, private, or public organisations. A person's computer

[17] Ibid

systems and a business network's activities both leave digital footprints, which may vary from web browser history caches and cookie to documents metadata, deleted file fragments, email headers, process logs and backup files (among other things).

**How does digital forensic help gather evidence for investigation**

When we speak about digital forensics, we're typically talking about computer crimes, but it's also used to describe the study of objects or materials discovered in mobile technology and the retrieval of these offences. It is essentially the procedure of searching, saving, extracting and recording digital data to create evidence that may be utilised in a court of law later on that is referred to as a digital forensic investigation (DFI).

Using digital forensics for business investigations, such as computer hacking or internal investigations, is possible. This is where digital forensics experts look for signs of a network incursion or a system breach. To keep up with the ever-expanding area of cybercrime investigation, forensic experts are increasingly turning to digital sources like databases and firewalls.[18]

**What is the role of forensic in evidence verification?**

Since "Forensic" comes from the Latin word for “before the forum," it is known as "forensic." Criminal charges trace all the way back to Roman times, when they referred to making a case before a crowd of people in a forum.

Both the accused and the acquitted will present their arguments based on their versions of events. Whoever has the greatest arguments and delivery will win the case. Both "legal proof" and "a type of public exposition" derive from this one root.

Professionals in evidence validation employ forensics to check the veracity of their findings. Examining the evidence may potentially provide new information about the case or assist in the resolution of issues that were previously unresolved, at the very least if forensics were unavailable.

The field of forensic science is self-contained, although contemporary forensics makes heavy use of technology to aid in its investigation. Because new and improving technology is being utilised to carry out these fundamental tasks to enhance outcomes and minimise any margin of error, they are still employed to determine results.[19]

**The help of information and technology in the forensic field**

As technology continues to permeate every area of our lives, it's no surprise that crime-solving methods have evolved into something out of science fiction. Real forensic methods, such as retinal scan and trace proof biochemistry, seem like something out of a science fiction movie.

Developments in forensic technology have made it possible to do things like fingerprint, DNA mapping, ocular scanning, and generating full pictures of objects discovered in parts, such as reconstructing a face from a skull. Within 24 hours after death, experts are

[18] SUPRA 2

[19] Adams, Richard (2013). '"The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice"

also able to determine which drugs were infused into the victim's system.
Experts and detectives' lives have been made much simpler by integrating forensics and technology to tackle issues that would otherwise be impossible to solve.

Forensics has benefited from the development of many innovative methodologies and procedures. Examples of such people include:

- It is possible to observe the damage before it manifests on the skin using alternative light imaging.
- Forensic carbon-14 dating is used to determine the age of found human remains.
- Broken glass may be analysed using Laser Ablation Reluctantly Coupled Plasma Mass Spectrometry (LA-ICP-MS), which analyses even tiny fragments to discover crucial indications like bullet direction, impact force, or impact type. It's possible that the weapon used in the crime is significant as well. This method aids in the re-creation of it.
- Using 3D Forensic Facial Reconstruction, a potential physical appearance may be extrapolated from the bones of a deceased person.
- Even in the 21st century, current forensic technology has been shown correctly on television.

**Analysis of the growing role of technology in criminal justice**

Professionals in the criminal justice system have begun using new technology in their offices, labs, and courts as a result of their creation. Researchers, judges and attorneys now have the tools they need to keep ahead of criminals because to advances in computer technology. As a result, both prospective and existing legal professionals should stay abreast of technology advancements in their industry by attending continuing education courses.[20]

- System for Geographic Information and Positioning (GIS/GPS).
- Detection of gunshots (GDS).
- Drones, Robots, and Robotic Cameras.
- Autonomous License Plate Recognizers.
- Databases and the exchange of data.
- The use of digital video recording equipment.
- Rapid Identification Systems (RIS)
- Computers for automobiles.
- Dispatching via computer.
- 3D crime scene photography.

## ADVANTAGES AND DISADVANTAGES

### ADVANTAGES

1. Cybercrime may be curbed to some degree using current and specialised computing software and apps. Sniffing packets and other network monitoring techniques are available to do this. Examples include IP address tracing and email address tracking. Computer forensics is the term for this field of study.
2. To examine accidents and identify their causes, forensic analysis studies the vehicle's state, eyewitness reports, tyre and other markings, and calculates the driving behaviour, for instance.
3. It incorporates anthropology and may be used to determining a person's gender.
4. Using forensics and biometrics, it is possible to identify the fingerprint of the suspect on evidence collected from a crime scene.

[20] Forensic Examination of Digital Evidence: A Guide for Law Enforcement, National Institute of Justice, Apr. 2004, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf, viewed on

5. By looking at the deceased's wounds and bruises, and the places where they died, a post-mortem report may assist establish how they died. When someone dies suddenly from natural causes, a medical examiner looks into the matter.
6. It may also be used to find out how much alcohol is in your system by testing your saliva or urine.
7. In cases of sexual assault or rape, clinical forensic drugs are used to identify the perpetrators and victims, as well as defensive wounds on the victim and gunshot wounds, as well as pattern of wounds in domestic abuse and self-inflicted injuries.
8. Phone conversation or mobile record monitoring is part of forensic which is used to identify speakers and improve speech as well as authenticate tapes and other key phonological tools.
9. Photographic evidence, credit card forgery and fraud, footprint and digital image evidence are all important elements of forensics.

**DISADVANTAGES**

Forensic science and technology, while its numerous benefits, has certain drawbacks. They're as follows:

1. Because it exposes private information about the person, DNA mapping is considered unethical.
2. The judgement is postponed because technical and forensic investigation takes a long time.
3. No one will have access to the forensic evidence at all times.
4. Interpretation of the forensic examination varies from one forensics expert to the other.
5. The results of a forensic investigation cannot be independently verified since there is no established standard. This requires a diverse set of skills and expertise.
6. The experimental investigation may be skewed by misunderstandings or misinformation.
7. Forensics equipment may be quite costly.
8. This necessitates in-depth investigation. It's possible that a minor mistake may lead to an erroneous number.
9. Evidence may be manipulated, resulting in an incorrect verdict.
10. Forensic analysis may be hindered by powerful variables such as political or financial pressures.
11. It's difficult to innovate when everything is done in the same way.[21]
12. It is very difficult to preserve the privacy and confidentiality of the information collected.[22]

**ISSUES AND CHALLENGES**

The use of technologies in police forensic inquiry faces three major difficulties. They're as follows:

- Obstacles on the technical side
- Problems with the law
- Problems with resources

As new technologies emerge, so do forms of crime and the people who commit them. A method used by criminals to conceal, modify, or erase their crime trail is known as an anti-forensic method in digital forensics. Professionals in digital forensics employ forensic technologies to collect evidence against offenders. Digital forensics is

[21] https://www.swgde.org/documents/Current%20Documents/2006-07.

[22] Supplemental Requirements for the Accreditation of Forensic Science Testing Laboratories, 2011 edition, ASCLD/LAB-International, 2010.

regarded as one of the world's most difficult problems. Forensic methods may be broken down into the following categories:

"Archive data; encryption; covert channels; data hiding in storage space; steganography; operating in the cloud; skill gaps; and legal difficulties."
It's more difficult to provide digital evidence since the legal framework often takes a softer approach and doesn't recognise all aspects of cyber forensics as relevant.

Most of the time, this happens so because cyber police are unable to identify a possible evidence source. The integrity of electronically stored evidence is often questioned in court. The gathering of electronic evidence is rejected since there are no standards or explanations for how it was done. The following categories apply to legal issues:

- "Absence of guidelines and standards
- Privacy issues
- Preservation of electronic evidence
- Limitation of the Indian Evidence Act, 1872
- Admissibility in courts
- Power for gathering digital evidence
- Resource challenges"

Because digital evidence is much more delicate than physical proof, when crime rates grow, so does the volume of data that has to be analysed. This places an increased responsibility on digital forensics experts to analyse such enormous amounts of data.
Forensic specialists utilise a variety of technologies to verify the accuracy of the data in order to expedite the investigation. However, working with these tools is not without its own set of difficulties. There are three types of resource challenges:

- Technological advancements
- Increase in volume and duplication of data

## CRITICAL ANALYSIS

Furthermore, the introduction of novel technologies and procedures that provide value (innovation) for users may lead to a shift in the criminal justice system.

New scientific and technological application Forensic science services have seen a significant rise in demand in fields including microbiology, chemistry, and information systems during the past several decades. There will be an instant desire for new technology that can help solve crimes if it is accessible.

## RECOMMENDATIONS

When it comes to the forensics of the arts and sciences such as photography, archaeology, and the like, the goal isn't only to figure out how old something is. Thus, forensics has developed significantly and become more trustworthy it is utilising modern technology to assist.

## LANDMARK JUDGEMENTS

**Jagdeo Singh V. The State and Ors**

"Dealing with the recording of an overheard telephone conversation on CD and CDR without a certificate," the Hon'ble High Court of Delhi said in this case. In accordance with Section 65B of the Indian Evidence Act of 1872, the court determined that secondary electronic evidence lacked a certificate. A court cannot consider evidence under Section 65B of the Indian Evidence Act of 1872 for any reason.

**Union of India and Anr V. G.M. Koki and Ors.**

A non-maternity language is a legislative tool often used to give effect to provisions that are contradictory to other provisions in the same act or legislation, i.e., to prevent the operation and effect of all such provisions from taking effect.

## CONCLUSION

It's no surprise that forensics is one of the fastest-growing industries, given the state of the art in this area. It is essential to understand that in the framework of the scientific disciplines mentioned above, new kinds of trace evidence came into play. These clauses have not been considered before, either because of a lack of evidence or a lack of techniques for examining the evidence.

Digital forensic science has developed a whole new universe of trace classes as a result of this. Physical and digital impulses coexist together in today's hybrid society. There aren't many criminal investigations in the Netherlands in the twenty-first century that don't include digital scars. This means that forensic service providers need to collect and examine digital evidence from a wide range of sources.

Inevitably, the variety and sophistication of equipment used by digital forensic investigators will grow as time goes on, and that's a fact.

In the coming, we will witness the digital forensic profession growing more entrenched and acquiring legitimacy as we also see its usage growing in all kinds of investigations. Electronic content should be accepted more readily in courts and tribunals as the profession develops and becomes more sophisticated.

One reason for this is because judges and juries will be more familiar with digital forensic evidence, but it will also be a consequence of advancements like a contract for these investigators, as well as new and better ways of presenting evidence. The challenges confronting the digital forensic scientists will continuing to plague businesses, though. Greater workloads are a consequence of a rise of relevant devices and their additional storage capacity, which are causing these issues.

Additionally, the right to privacy will remain a source of contention for digital forensic investigators. In light of this, investigators will continue to confront difficulties in interpreting and contextualising the ever-increasing amounts of data they encounter while using a conventional computer. Sadly (or fortunately, depending on your point of view), computer users seldom erase data.

In order to enhance communication between digital forensic investigators and criminal justice authorities, this connection will continue to grow. It's a win-win situation since the criminal justice system will be more informed on evidentiary standards, which will allow digital forensic investigators to focus on more important aspects of the investigation.

*****