CHAPTER-1

INTRODUCTION

1.1. Overview

It is usually been accepted these days that there is an enduring evolution in
technologies (including computers, networks, smart homes, e-commerce and the
Internet etc.) that are progressively involved in every aspects of our life. Illegitimate
activities and crimes have also been increased with this progression. Various
organizations suffer from various computer crimes and the criminals that commit them
have a range of stimuli. e.g., Criminal may have goals to steal money from someone’s
bank account, Steal private data of individuals, to destroy reputation of rival and many
more. As shown in Figure 1.1, various computer crimes and the percentages of
organizations affected in the Middle East for the period of 2007-09.

Figure 1.1 Computer crimes in the Middle East Source of statistics: (Dwyer, 2010)
1.2. Concept of Cyber Forensics

Since the computers are now being used as a weapon to commit criminal activities. This introduced the field in the forensic investigation is the "PC Forensics (Personal Computer Forensics)", more generally known as "Digital Forensics". There are different definitions exist as referenced beneath: “Digital Forensics” is the gathering, protection, examination, and introduction of computer related proofs. Digital forensic and investigation includes the distinguishing proof, conservation, extraction, documentation, and investigation of advanced records to decide forthcoming lawful proof.

From above definitions, unmistakably the objective of computer related crime scene investigation is the disclosure of digital evidence that is acceptable in the court. It is commonly acknowledged that the requirement of storage capacity is increasing exponentially. Henceforth, the bit by bit duplication of digital evidences from storage media is tedious and complex errand. One approach to make the procedure simpler and more brilliant is to begin hunting down evidence in the most significant parts of the computer systems. Those areas are destined to have data that is lucrative to the forensics investigator. Such territories incorporate Windows Registry, Process data and Event logs and so forth.

Forensics is the utilization of scientific knowledge to accumulate, examination, and presentation of evidence to the courts. The word forensics signifies "to convey to the court". Computer forensics can be characterized as the accumulation and examination of information from the computer systems including all computer networks (wireless or wired), communication channels in a way that is acceptable in a courtroom [1][32].

Digital forensics is a branch of forensic science focused on recovery and investigation of artefacts found on digital devices [2][3][4]. These days, time plays vital role to conclude any given assignment. By applying various tools and techniques, we can finish an undertaking as fast as could reasonably be expected, it is increasingly advantageous
things since it saves a lot of activities, labour, money and different assets. So utilizing less assets and time to get expected result is most desired thing nowadays. In digital forensic investigation, investigator needs to analyse every computers of a network to locate a suspicious computer. On the off chance that examiner wants to get the entire picture of the crime scene then the bit by bit disk duplication of each storage media needed. Hence, it requires a lot of backup storage media, time and money. It may waste the valuable time of investigators. This task may engage investigators along with non-productive task of disk duplication instead of analysing the evidences. Therefore, Investigators need most plausible evidence/computer system that could give direction to committed crimes.

Digital forensics Investigators are more concentrated on persistent and volatile data of computer system to find suspicious artefacts. Persistent data is permanently stored inside hard disk or other medium and reside there even the computer is shutdown. Whereas, Volatile data is lost from the memory, if there is no power supply to the computer system. Moreover, volatile data should be gathered first as it may lost without power supply. Volatile data mostly reside in registries, cache memory, and Random Access Memory (RAM) etc. Since, the effervescent nature of volatile data, it should be acquired in real time or near to real time [1].

Digital forensic evidence consists of exhibits, each consisting of a sequence of bits, presented by witnesses in a legal manner, to help jurors establish the facts of the case and support or disprove legal theories of the court case. Demonstrations are presented as the evidence that must be conveyed using proper chain of custody.

1.2.1 Digital Forensics on a Wide Perspective

Computer Forensics: A combination of various tools and techniques to locate the appropriate forensic evidences from the computer system. It tends to be done through live just as dead investigation. It is broadly utilized in civil proceedings as well.
Digital Forensics: It is the part of forensic science encompassing the recuperation and investigation of relevant information found in digital devices, much of the time in respect to computer crimes. "Digital forensics" is typically related to analysing digital devices for forensic purpose. In this way, it includes computer systems as well as incorporates different digital devices like iPods, mp3 players, Gaming Consoles and so forth.

Mobile Forensics: It is the examination of cell phones, for example, GPS navigation systems, Smart mobile phones.

Database Forensics: It deals with the legal investigation of databases and their metadata. An adequate knowledge of various standards to encode information on computer disk is needed to study relational databases. A documentation of various standards used to encode data in prominent database sellers like Microsoft SQL Server and Oracle has been added to the open area and is fundamental to comprehend and resolve the problems of data authenticity and data integrity.

Network Forensics: It is a sub-part of digital forensics relates with the observation and examination of computer network traffic to gather data, legal evidence, or intrusion detection. Attention on: "get it as you can" and in a more intelligent way "stop look listen".

Multimedia Forensic - It is the part of digital forensics that includes the investigation of sound, video and picture (Digital media).

Evidence - Evidence in its broad sense incorporates everything that is utilized to characterize or exhibit reality of the case.

Investigation - It endeavours to reproduce past events, computer based malicious activities.
The Locards Principle - The Principle of Exchange. Locard's rule holds that the culprit of a crime will carry something into the crime scene and leave with something from it, and that both can be utilized as criminological evidence. "Wherever he steps, whatever he contacts, whatever he leaves, even unwittingly, will fill in as a quiet observer against him. Physical evidence can’t be wrong, it can't lie itself, and it can't be entirely missing. Just human inability to discover it, think about and comprehend it can reduce its value."

1.2.2 Job of Cyber Forensics

- Prevents Cyber Crime
- Detects Cyber Crime
- Truth Assessment[6]

1.3. Overview of the digital forensics analysis methodology

The detailed definition of computer forensics is as per the following: "The utilization of scientifically derived and proven method towards the protection, gathering, approval, recognizable proof, investigation, translation, documentation and introduction of digital evidence got from digital sources to encourage or advancing the recreation of occasions observed to be criminal" [7].

The key components of PC forensics are recorded beneath:

- The utilization of scientific techniques
- Collection and conservation
- Validation
- Identification
- Analysis and elucidation
- Documentation and demonstration
The vital steps Preparation or Extraction, Identification, and Analysis are engaged in any pre-examination investigation process. Practically speaking, organizations may isolate these tasks into different groups. As this is worthy and for the most part fundamental, it might prompt miscommunication. For different law requirements, organizations to work viably together, they should impart without distortion. The investigation group must archive the whole case and be unequivocal when alluding to explicit areas.

The arraigning lawyer and digital measurable inspector must impart to one another about the procedure finished at each phase of an investigation or indictment. The procedure is hypothetically iterative, so they likewise need to choose the occasions the procedure ought to be rehashed. It is basically significant that everybody comprehend whether a case just needs arrangement, extraction, and distinguishing proof, or whether it likewise requires investigation.

The fundamental strides in the forensics procedure mentioned here come after investigators get scientific information and a solicitation, however before the revealing and examination is initiated. Analysts must be unambiguous about each phase that happens in the approach. In specific circumstances, be that as it may, analysts may gather the means or decrease the condensed parts of the investigation procedure. At the point when analysts request the rundown, for example, "Pertinent Forensic Data List" they don't intend to suggest that the rundown are physical archives. The rundown might be composed or things submitted in digital structure. At last, the analysts regularly repeat this whole procedure, since a finding or determination may demonstrate another lead to be contemplated. [8]

1.3.1 Preparation/Extraction

Analysts begin the procedure by asking whether there is sufficient digital data to continue. They must be certain about clear request is on hand and there is adequate information accessible to endeavour its appropriate response. On the off chance that
anything isn't available, they speak with the requester. Else, they may proceed with the procedure.

The initial step of digital legal investigation process is the approval of all accessible software and hardware tools, to guarantee that they work legitimately. There is as yet a debate in the digital forensics community about the recurrence of utilization of the forensic products and hardware ought to be tried. Various digital criminological communities concurred that, by any chance, investigators should approve each accessible software and hardware equipment after chose to place it being used for investigation reason. They ought to likewise recheck after any updates and fixes available, or any reconfiguration happened.

After digital scientific investigator gets ready apparatuses, the person creates the copy duplicate of the criminological information according to the request and confirms the honesty. This procedure must follow the law requirement and has just obtained the digital information through reasonable lawful procedure and made the digital criminological picture.

The criminological picture is a bit-by-bit duplication of the information that exists in the first digital media without any modifications. It likewise accepts that the digital legal investigator has acquired ephemeral duplicate of the resided data. On the off chance that investigators get the first evidence, they have to make a brief duplicate and save the chain of custody of unique information. The inspectors ensure the duplicate in their authority must be indispensable and impeccable. They check it by applying different hashing calculations like md5, RSA of the evidences. Investigators may counsel if any issue discovered with identified with digital evidences.

After check of the trustworthiness of digital evidences to be investigated, a guide is created to separate basic information. They build up and improve the forensic request into survey about the gathered digital evidences. The forensic software tools that help them to get cures of issues are chosen. Investigators have essential thoughts of
disclosure according to the request or case. They add these to an "Inquiry Lead List," that is the list of requested things. For instance, the request may give the lead "scan for child pornography". As they grow new pieces of information, they add them to the pending list, and as they exhaust the inquiry list, they mark them "prepared" or "wrapped up".

For each pursuit piece of information, inspectors extricate significant evidence and imprint that search lead as prepared. They add anything separated to a second list called an "Extracted Data List." Examiners seek after all the search leads, adding results to this second list. At that point they move to the following period of the procedure, distinguishing proof.

1.3.2 Identification

Analysts repeat the procedure of recognizable proof for every component on the Extracted Data list. At first, they decide the sort of thing it is. On the off chance that it is immaterial to the forensic request, they basically comment on it as "prepared" and go further. Same as in a physical searching, if an investigator gets through a thing that is cause to look liable, yet outside the extent of the first court order, it would be prudent that the analyst immediately stop that movement, inform the appropriate people, including the requester, and wait for the further directions. For instance, law implementation may catch a computer system for evidence for tax fraud evidence, yet the analyst may discover the child pornography data. The most reasonable strategy, in the process of discovering evidence outside the extent of a warrant, is to stop the inquiry and seek after the warrant's authority or to get another warrant.

On the off chance that the thing is suitable to the forensic request, investigators report it on a third list, the "Important Data List". This list is an accumulation of information identified with answer the first original forensic request. For instance, in identity theft case, important information may incorporate social security number, pictures identified with false recognizable proof, or messages or
emails about data fraud. It might likewise conceivable that a thing lead to another pursuit lead. An email or talk may uncover that the objective was utilizing another nickname. That would prompt another look for the discovered epithet. The analysts would backtrack and add that hint to the "Hunt Lead List", henceforth they would review to research it in future.

A thing can likewise understand new potential source of information. For instance, investigators may found another email account that the target using. Further, law requirement might need to arrange the substance of the new email or social record. Investigators may likewise discover new evidence pointing to the targeted files on a removable Universal Serial Bus (USB) drive—the law implementation may not discover in the first search. Under these conditions, law implementation may consider to get another court order to search for the USB drive. A criminological examination may prompt a wide range of kinds of new evidences. Hardly any more models incorporate Event logs, Windows logs, and video security footages and some more. Analysts may record these on one more rundown that is known as the "New Source of Data list".

Presently, analysts backtrack to any new leads created. For any new information seek drives, analysts may consider backtrack to the Extraction venture to process every one of those. Moreover, for any new wellspring of information that may find new evidence, analysts consider to back to every past advance and acquire and get picture of measurable information.

At this phase simultaneously, it is advantageous for investigators to illuminate the requester regarding their unique decisions. It is additionally significant time for analysts and the requester to examine about their convictions, the arrival on venture will be for seeking after new leads. Contingent upon the movement of a case, removed and recognized applicable information may offer instinct to the requester enough data to push the case ahead, and analysts should not have to do additionally work. For instance, in a financial balance data burglary case, if an analyst recuperates a mind-boggling number of introduced programming to separate delicate data sorted out
in client made indexes, an examiner might most likely secure a liable request with no further legal examination. On the off chance that straightforward extricated and recognized information isn't adequate, at that point analysts move to the following stage, examination.

1.3.3 Analysis

In the examination stage, inspectors associate every one of the focuses and plan a total review for the requester. For each thing on the Relevant Data List, inspectors clears up inquiries like what, where, who, when, and how. They endeavour to clarify which client or application made, got, altered or sent everything, and how it initially existed into the case. Inspectors likewise give insight concerning where they discovered it. Most basically, they clarify the reason of this data is important and what it intends to the case.

Frequently analysts may deliver the most profitable examination by concentrating on when the reality occurred and creating a timetable that passes on a level headed certainty. For each suitable thing, inspectors attempt to clarify when it was gotten to, made, changed, sent, got, saw, propelled and erased. They see and clarify a sequential request of occasions and note the synchronous occasions occurred.

Analysts make the archive of all their examination, and other data proper to the legal solicitation, and upgrade everything to a last rundown, the "Investigation Results List." It is the rundown of all the expressive information that answers who, when, what, how, where, and different inquiries. The data on this rundown satisfies the measurable solicitation. Without a doubt, even at this late period of the method, somewhat may create new data look for leads or a wellspring of data leads. In case it happens, examiners add them to the correct records and consider coming back to dissect them totally.
To finish with, inspectors go through these means iteratively; they can react to the scientific solicitation. They move to the Forensic Reporting stage. This is where inspectors archive results so the requester can fathom them and use them for the situation.

Legal detailing is outside the extent of this exploration, however its significance can't be misrepresented. The last report is the most ideal route for inspectors to talk the actualities to the requester. Criminological detailing is the basic in light of the fact that the whole legal procedure is just worth as much as the data analysts convey to the requester. After the announcing, the requester cases level investigation where the person in question (conceivably with analysts) deciphers the discoveries with regards to the entire case.[9]

1.4. Statement of Problem

Essential focal point of this research is to extricate persistent and volatile data of computer system which can be utilized for digital forensic investigation purpose. Digital forensic investigators utilize forensics devices to separate evidences from a computer system. Be that as it may, have certain impediments as far as profundity examination of evidences, time required for extracting group of information for investigation, Storage limit of storage media and so forth. This research will discover another approach of extraction of digital forensics evidences that would modify the existing process of evidence extraction.

Extraction of persistent and volatile data would minimize time of gathering forensic information from computer system. Along these, Cyber forensics investigators don't need to save additional time in extracting just information. This research focus around diminishing time of extricating evidences from a computer system by applying new approach. Therefore, Time expected to prove committed crime would be reduced.
We focus on the digital data that must be forensically sound by nature. This forensically sound information may not be available as expected by investigators. It may be stored in raw format. There must be some techniques should be applied to deduce the fact from raw format data. Hence, Extraction of data from computer system and applying proposed methodology would produce much more relevant facts for investigators.

Consequently, this research has a place with Applied Research Category which finds some answer for some squeezing functional issue.

1.5. Objectives

Principle Research Objectives are:

- To discover various areas of computer system that incorporates forensically sound evidences.
- To collect forensic evidences in such a manner that it can be further analyzed.
- To derive forensic evidences from existing data that could be demonstrated about perpetrated offense.
- To minimize the required efforts and resources for the forensic investigation process.

1.6. Definition of Terms

**Digital Forensics** - Digital forensics (once in a while known as digital forensic science) is a category of forensic science consolidating the recovery and examination of data found in digital devices, routinely in association with digital crime.
**Digital Forensic Investigation** - A digital forensic investigation commonly comprises of 3 stages: acquisition or imaging of exhibits, analysis, and reporting.

**Computer Forensic** – It is also known as “PC forensics”. It is the utilization of examination and investigation methodology to gather and preserve evidence from a particular digital device in a way that is suitable for presentation in an official court. The goal of PC forensics is to perform legally acceptable investigation while keeping up a recorded chain of evidence to find exactly which malicious activities performed on a digital device and the responsible person for it.

**Acquisition**: The phase in a PC forensic examination wherein the digital data involved is gathered. Regularly the method utilized is a bit-by-bit duplication or a forensic working image of the hard drive or other media being referred to.

**Active Files, Active Data**: Data on a PC that isn't erased and is commonly open to access and visible to the user for the normal usage.

**Allocated space / sector / block**: The logical storage area on the hard disk or any other digital media allotted to a file by the Operating System.

**Allocation Block**: An adjoining group of sectors that is the smallest amount of storage space allocated to a file by the operating system, for example, Microsoft Windows.

**Ambient Data**: The opposite of active data. Ambient data is the data that lies in regions not accessible for the user. This data reside in file slack space, virtual memory files, unallocated cluster and different regions not allotted to active files.

**Application**: Commonly known as a Program, or (once in a while) Software. The product used to get to and make files or documents. Microsoft Word is an application
that works with word processing documents. Microsoft Excel is an application that works with spreadsheets.

**Archival Data:** Often related to backups, archival data is commonly kept on another storage media, for example, CD or Magnetic tape, and is mostly compressed. Such data isn't typically quickly accessible to the user and should be restored from the backup device to access it.

**ASCII:** Stands for "American Standard Code for Information Exchange." It is pronounced as "Ass-key" and often alluded to as "ASCII text." ASCII assigns a numerical code for each character on a keyboard; consequently ASCII text is frequently conceivable to human without need of much interpretation.

**Audit Trail:** An ordered record of system activities on a PC or network security system that may monitor user activities, for example, user logins, files access, and other different activities.

**Backup:** A copy of data that is kept for the emergency purpose against data loss in a system, maintaining integrity, media failure or potentially to keep archival data. Backups might be encrypted or compressed, and are generally isolated from the system containing the original version of the data that is being backed up.

**Backup Server:** A PC on a network that is intended to be utilized to back up data from different PCs on the network. A Backup Server may likewise be utilized as a File Server, as an Application Server or as a Mail Server.

**Backup media:** It is the storage media where backup data is stored. It may any type of media, for example, CD-ROM, magnetic tapes, Digital Versatile Disk (DVD), floppy diskettes, external hard disks, magneto-optical drives, Zip drives, WORM drives and numerous others.
**Bit**: The smallest unit of information, comprising of a zero or a one, means "binary digit."

**Bit stream or bit-by-bit copy**: A duplication of every contiguous sector on a hard disk or other media, without respect to allotment of data. Sometimes, it is misidentified with mirroring.

**Block**: An allocation block, as alluded to in the Macintosh Operating System.

**Buffer**: A memory area that is used temporary for storage purpose. This stored data may be written to a buffer file.

**Buffer file**: It is a file written from temporary data stored in a buffer.

**Burn**: The way toward making a CD-ROM or DVD.

**Byte**: Consecutive eight bits.

**Cache**: A storage area where frequently useful data for the process might be kept for quick access. There are three principle kinds of cache: program cache, memory cache and disk cache.

**Chain of Custody**: As in different fields, a record of the ordered history of (electronic) evidence.

**Cluster**: It is also known as allocation blocks, a cluster are an adjacent group of sectors that is the smallest amount of space assigned to a file by an operating system, for example, Microsoft Windows. These clusters mostly range in size from 4 sectors to 64 sectors.
**Compressed file, zipped file:** It is a file that is encoded by utilizing less space than the original copy of file in its uncompressed state. A zipped file may not compressed using compression algorithm like compressed files. A zipped file is basically created for sending and sharing purpose as it is turned into one file.

**Cookie:** While using internet or browser program, a small file containing piece of information is accessed by a web browser and usually written to a user’s computer system. An abbreviated type of the expression, "magic cookie," cookies are utilized for tracking, verifying, and keeping up data about users, mostly to provide facility to interconnect user and website. Cookies are stored on a client’s storage area and contain the timestamp about particular website accessed.

**Corrupt Data, Corrupt File:** A file that is harmed. Harm may have happened coincidentally amid transmission, duplicating, through operating system exceptions, physical harm to the media on which the information was stored, or however different methods.

**Deep Web:** A piece of the Internet (about 95% of it) that isn't indexed by various search engines like Bing, Yahoo and Google or something like that and is commonly not available by internet browsers, for example, Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome. It incorporates various internal networks, databases, communities and resources.

**Data:** Digital Information stored on a PC that isn’t a part of a process.

**Default:** It is a value automatically assigned to different parameters without user intervention.

**Deduplication:** A procedure performed on a collected data from various sources, regardless of whether from a files, locations, or computer systems, or from inside an
email file. The procedure is intended to yield one copy of given file, email or record of computer system.

**Delete:** To make a file or email move from a live or active state to an ambient state, mostly done by transferring a file to the recycle bin or trash on a computer, or by using Del key on the selected file. Deleted files, mostly not permanently removed from computer until it is overwritten.

**Desktop:** In a Graphical User Interface (GUI, for example, Windows or the Macintosh OS, files or directories (folders) visible before a user opens any window. The desktop is a graphical view for the users’ ease of choosing or selecting a particular file or process stored in main memory or secondary memory.

**Desktop computer:** An independent PC that is commonly intended to be associated with a monitor and keyboard (although some personal computers, for example, the Macintosh iMac, have the monitor integrated), as particular from a laptop, and from a Server.

**Directory:** A hierarchically arranged (Tree structure or any other) listing of files stored on a storage media. The topmost directory is called as root directory. The other directories nested within a root directory are called subdirectories. In a GUI based operating systems, a directory is appears as a folder and shown as particular graphical image called icon.

**Disk:** Generally a hard disk. Floppy diskettes are regularly alluded to as disks.

**Disk Cache:** RAM used to accelerate access to stored data. It may be a piece of a PC's RAM, or might be RAM incorporated into the disk drive itself.
**Disk Mirroring**: Data duplicated to another hard disk or to another area on the equivalent hard drive so as to have a total, indistinguishable duplicate of the original.

**Download**: The exchange of information between two PCs, by and large over a computer network or internet. One may download a file from the Internet, for example. “copy” a file from a computer system. For example, a typical oversight is to state that one downloaded a file from a disk, when a file is replicated (not downloaded) from a disk.

**Email**: Electronic mail. Messages transmitted over a network of computers, coordinated to a given client, either in group or individually. Email might be stored in a text format, or in an encrypted form. The Microsoft Outlook stores email messages in an encrypted file; most other email programs store messages as a text.

**Encryption**: A procedure to render a file unreadable to unauthorized users or computer process.

**Exabyte**: 1024 Petabytes

**File Extension, Extension**: It is a part of a file name, as a rule pursues a "dot" or period in a file name. Some operating systems, such a Microsoft Windows, rely upon the extension to recognize what program is utilized to open the given file. Microsoft word documents, for example have ".doc” or “.docx” as their extension.

**Filename**: The name of a file. Also, referred as the file name that exclude the extension like .doc, .txt, .docx etc.

**File Attribute**: Properties related with a file that are kept with the listing of file directory. Such attributes incorporate the date and time the file was last created, modified or accessed by a user.
**File Server:** A PC on a computer network that is utilized to store files from and for numerous clients on the network. A file server may likewise be utilized as an Application Server, a Backup Server, or as a Mail Server. It may be utilized as a backup for the PCs on the network.

**File signature:** Information contained inside a file that distinguishes its type, despite the fact that the file's extension may have been changed.

**File slack:** Information at the end of a cluster that has not been totally filled or overwritten by a file. The file may finish before the end of the cluster; consequently the group may contain information from a previous file.

**Floppy diskette, floppy:** A square-shape box holds the rotating flexible plastic magnetically coated disk used for data storage. At this process, the 8” and 5.25” variety of floppy diskette is out of date, and the 3.5” variety is moving toward obsolescence. The most well-known floppy diskettes hold 1.44 MB of information.

**Folder:** in a GUI, a folder is the portrayal of a directory and may contain files and other, nested folders.

**Forensic Image:** A forensically stable and complete duplicate of a hard drive or other digital media, for the most part proposed for use as evidence. Such duplicates incorporate slack space, unallocated space, and boot record. A forensic image is mostly having a calculated hash value that authenticates the image to prove that it is exact duplicate of the original copy.

**Gigabyte (GB):** 1024 megabytes (MB), or 1,048,576 KB, or 1,073,741,824 bytes. Frequently considered to be one billion bytes.
GUI: Graphical User Interface. A picture and symbol based interface intended to make control of computer information simple. Normal GUIs are Microsoft Windows and the Macintosh OS.

Hard Disk: Currently the primary storage media for data on most computer systems, Consists of a fixed chassis containing a quickly rotating metal-covered platter, or pile of platters that are magnetically encoded as data is kept in by enclosed magnetic read or write heads.

Hash or Hash Value: A hash is a number produced from a string of text. A hash value might be created for an individual file, or for the entire hard disk. A matched hash basically ensures that a duplicate is indistinguishable to the original copy. It doesn't totally ensure this due to hash collision issue.

IP Address (IPv4): An electronic identifier for a particular device or computer system on the World Wide Web or other electronic network utilizing the TCP/IP protocol. An IP address is a series of four numbers isolated by periods ("dots"), each number is range from 0 to 255. An example would be 192.168.34.157 "IP" means "Internet Protocol."

IP Address (IPv6): An electronic identifier for a particular device or computer system on the World Wide Web or other electronic network utilizing the TCP/IP protocol. An IP address is a series of four numbers isolated by periods ("dots"). An IPv6 address is a series of eight gatherings of four hexadecimal digits with every gathering being isolated by colons, for instance 4021:0ca3:123e:ae42:0300:7d2e:0371:7224, however is in some cases abbreviated.

Keylogger: A program or device intended to track the keys types on a computer system. It may be utilized for espionage, or monitoring, for example, to gather passwords. Some keyloggers might be accessed remotely.
**Keyword Search**: A typical procedure utilized in PC forensic and electronic discovery, a keyword search is normally performed to discover and distinguish each event on a PC or other media of a given phrase or word, regardless of whether said word or phrase occurs in deleted files or unallocated space.

**Kilobyte (KB)**: 1024 bytes.

**Log files**: It is a file that contains different activities performed by different applications and operating systems.

**Megabyte (MB)**: 1024 Kilobytes (KB), or 1,048,576 bytes. Mostly considered to be one million bytes.

**Memory Cache**: Also known as RAM cache, it is rapid access memory designed to store recently accessed data or frequently accessed data for quicker use. On the Macintosh, RAM cache may likewise be disk cache.

**Network**: It is a group of computer systems electronically connected to have the capacity to share files or different resources, or for electronic communication. The World Wide Web is an especially large network.

**Partition**: It is a logical outlining on a disk drive such that an individual drive may act as two smaller disk drives.

**PDA**: Personal Digital Assistant. A handheld device that may have various functions, one of which is normally a type of electronic data. PDAs may contain programs, data files and storage space, a digital camera and related storage, a phone and related telephone directory and other information.
PDF: It is an Adobe Acrobat document. PDF means Portable Digital Format. It is a common format for text as well graphical data that could not be easily modified or altered.

Petabyte: 1024 Terabytes, or 1,125,899,906,900,000 bytes – more than a quadrillion bytes.

Program: Also known as a Software or an Application. The application used to create or access files or documents. Corel WordPerfect and Microsoft Word are applications that work with word processing documents. Microsoft Excel is an application that work with or spreadsheets.

Protocol: An agreed or settled upon standard format for connecting, communicating, or exchanging information between two devices or computer systems. There are numerous communication protocols exists, for example, TCP (Transmission Control Protocol), UDP (User Datagram Protocol) etc.

RAM: Random Access Memory. It is a computer chip that store digital information in electronic form.

Registry Hives: The Windows registry is comprised of sub files called "hives". Individual Windows User settings and some history of utilization are kept in the different hives and might be refreshed as the computer is utilized.

SAM Hive: "Security Account Manager" that stores Users' passwords

System Hive: Contains data about the Windows system setup, mounted devices, alternative configurations for services and drivers.

1.7. Importance of Study
Digital forensics is a wide field contains different strides to perform investigation process. The resources required to perform investigation process is reliant on storage media to be backup. In the present period, storage capacities of digital devices are growing as exponential rate. To keep pace with such developing innovation, expected resources to perform investigation process is likewise discovered.

Henceforth, this research focuses around extraction of forensically sound evidences and to minimize the needed resources for the investigation process. Hence, Forensic investigators can concentrate on examination process as opposed to gathering evidences from different non-significant digital data.

1.8. Thesis Organization

This thesis sorted out in six unique chapters. Chapter 1 and 2 presents various terminologies used and past work done by researchers. The core of this thesis is chapter 3 and 4, which presents proposed methodology and usage which incorporates identification of few digital forensic objects and derived intuition from available digital evidence. To approve the plausibility of methodology, chapter 5 depicts investigation and approval of proposed methodology that make the exploration worth. At long last chapter 6 manages the end which recapitulates the exploration and finishes up with the future thoughts in this promising field.