**UNIT 1V**

**EVIDENCE COLLECTION AND FORENSIC TOOLS**

**WHAT IS FORENSIC?:**

Forensic science is the scientific method of gathering and examining information about the past which is then used in a court of law. The word forensic comes from the Latin term forēnsis, meaning **"of or before the forum."**

**WHAT IS COMPUTER FORENSIC?:**

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Forensic investigators typically follow a standard set of procedures: After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.

**INTRODUCTION**

How is it possible to identify the person who committed a crime? A single hair or clothing fiber can allow a crime to be reconstructed and lead police to the responsible person. The goal of a **crime-scene investigation** is to recognize, document, and collect evidence at the scene of a crime. Solving the crime will then depend on piecing together the evidence to form a picture

of what happened at the crime scene.

**PRINCIPLE OF EXCHANGE**

Whenever two people come into contact with each other, a physical transfer occurs. Hair, skin cells, clothing fibers, pollen, glass fragments, debris from a person’s clothing, makeup, or any number of different types of material can be transferred from one person to another. To a forensic examiner, these transferred materials constitute what is called **trace evidence**. Some

common examples of trace evidence include:

• Pet hair on your clothes or rugs

• Hair on your brush

• Fingerprints on a glass

• Soil tracked into your house on your shoes

• A drop of blood on a T-shirt

• A used facial tissue

• Paint chips

• Broken glass

• A fiber from clothing

The first person to note this condition was Dr. Edmond Locard, director of the world’s first forensic laboratory in Lyon, France. He established several important ideas that are still a part of forensic studies today. *Locard’s* *exchange principle* states that when a person comes into contact with an object or another person, a cross-transfer of physical evidence can occur. The exchanged materials indicate that the two objects were in contact. Trace evidence can be found on both persons (and/or objects) because of this cross-transfer. This evidence that is exchanged bears a silent witness to the criminal act. Locard used transfer (trace) evidence from under a female

victim’s fingernails to help identify her attacker The second part of Locard’s principle states that the intensity, duration, and nature of the materials in contact determine the extent of the transfer.

More transfer would be noted if two individuals engaged in a fistfight than if a person simply brushed past another person.

**TYPES OF EVIDENCE**

Evidence can be classified into two types: direct evidence and circumstantial evidence (Figure 2-1). **Direct evidence** includes firsthand observations such as eyewitness accounts or police dashboard video cameras. For example, a witness states that she saw a defendant pointing a gun at a victim during a robbery. In court, direct evidence involves testimony by a witness about what that witness personally saw, heard, or did. Confessions are also considered direct evidence.

**Circumstantial evidence** is indirect evidence that can be used to imply a fact but that does not directly prove it. No one, other than the suspect and victim, actually sees when circumstantial evidence is left at the crime scene. But circumstantial evidence found at a crime scene may provide a link between a crime scene and a suspect. For example, finding a suspect’s gun at the site of a shooting is circumstantial evidence of the suspect’s presence there. Circumstantial evidence can be either physical or biological in nature. Physical evidence includes impressions such as fingerprints, footprints, shoe prints, tire impressions, and tool marks. Physical evidence also includes fibers, weapons, bullets, and shell casings. Biological evidence includes body fluids, hair, plant parts, and natural fibers. Most physical evidence, with the exception of fingerprints, reduces the number of suspects to a specific, smaller group of individuals. Biological evidence may make the group of suspects very small, or reduce it to a likely individual, which is more persuasive in court.

Trace evidence is a type of circumstantial evidence, examples of which include hair found on a brush, fingerprints on a glass, blood drops on a shirt, soil tracked into a house from shoes, and others

Evidence can also be divided into class evidence and individual evidence. **Class evidence** narrows an identity to a group of persons or things. Knowing the ABO blood type of a sample of blood from a crime scene tells us that one of many persons with that blood type may have been there. It also allows us to exclude anyone with a different blood type. **Individual evidence** narrows an identity to a single person or thing. Individual evidence typically has such a unique combination of characteristics that it could only belong to one person or thing, such as a fingerprint.

*Common examples of trace evidence.*

Animal or human hair

Fingerprints

Soil or plant material (pollen)

Body fluids such as mucus, semen, saliva, or blood

Fiber or debris from clothing

Paint chips, broken glass, or chemicals such as drugs or explosives

Evidence

Direct Circumstantial

Physical Biological

It is relatively easy to recover DNA from cigarette ends found at the scene of a crime.

**THE CRIME-SCENE INVESTIGATION TEAM**

Who is involved in a crime-scene investigation? The team is made up of legal and scientific professionals who work together to solve a crime. Professionals at the scene of a crime may include police officers, detectives, crime-scene investigators, district attorneys, medical examiners, and scientific specialists. Who is at the scene?

• *Police officers* are usually the first to arrive at a crime scene. A district attorney may be present to determine whether a search warrant is necessary for the crime-scene investigators.

• *Crime-scene investigators* document the crime scene in detail and collect physical evidence. Crime-scene investigators include recorders to record the data, sketch artists to sketch the scene, photographers to take photos of the crime scene, and evidence collectors.

• *Medical examiners* (also called coroners) may be necessary to determine the cause of a death when a homicide has occurred.

• *Detectives* look for leads by interviewing witnesses and talking to the crime-scene investigators about the evidence.

• *Specialists* such as entomologists (insect biologists), forensic scientists, and forensic psychologists may be consulted if the evidence requires their expertise.

**THE SEVEN S’s OF CRIME-SCENE INVESTIGATION**

**SECURING THE SCENE**

Securing the scene is the responsibility of the first-responding police officer (**first responder**). The safety of all individuals in the area is the first priority. Preservation of evidence is the second priority. This means the officer protects the area within which the crime has occurred, restricting all unauthorized persons from entering. Transfer, loss, or contamination of evidence can occur if the area is left unsecured (Locard’s exchange principle). The first officer on the scene will begin keeping a security log of all those who visit the crime scene. The officer will collect pertinent information and request any additional needs required for the investigation. He or she may ask for more officers to secure the area. Depending on the nature of the crime, the first-responding officer may request various teams of experts to be sent to the crime scene.

**SEPARATING THE WITNESSES**

Separating the witnesses is the next priority. Witnesses must not be allowed to talk to each other. Their accounts of the events will be compared. This separation is done to avoid witnesses working together to create a story (collusion).

The following questions need to be asked of each witness:

Crime-scene investigation teams do not clean up the scene. This dirty job often falls to the victim’s family. Professional crimescene cleaners can be hired in many places to do this job.

• When did the crime occur?

• Who called in the crime?

• Who is the victim?

• Can the perpetrator be identified?

• What did you see happen?

• Where were you when you observed the crime scene?

**SCANNING THE SCENE**

The forensic examiners need to scan the scene to determine where photos should be taken. A determination may be made of a **primary crime scene** and **secondary crime scene** and priorities assigned regarding examination. A robbery in front of a store might be the primary scene, and the home of a suspect might be the secondary scene. A murder may have taken place at one location (primary scene) and the corpse found at another (secondary scene).

**SEEING THE SCENE**

The crime scene examiner needs to see the scene. Photos of the overall area and close-up photos with and without a measuring ruler should be taken. Triangulation of stationary objects should be included in the photos as reference points. A view of the crime scene should be taken from several different angles and distances. Several close-up photos of any evidence and bodies should be taken.

**SKETCHING THE SCENE**

An accurate rough sketch of the crime scene is made, noting the position of the body (if any) and any other evidence. All objects should be measured from two immovable landmarks. On the sketch, north should be labeled and a scale of distance should be provided. Any other objects in the vicinity of the crime scene should be included in the sketch. This includes doors, windows, and furniture. If the crime scene is outdoors, the position of trees, vehicles, hedges, and other structures or objects should be included in the sketch. Later ,a more accurate, final copy of the crime scene should be made for possible presentation in court. Computer programs are available to later create a neater and more accurate sketch suitable for use in a court proceeding.

**N**

Scale: 1/4” = \_\_\_\_\_\_ feet

Case number \_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Location \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SEARCHING FOR EVIDENCE**

Depending on the number of investigators, a spiral, grid, linear, of quadrant pattern should be walked and location of evidence marked, photographed, and sketched. Single investigators might use a grid, linear, or spiral pattern. A group of investigators might use a linear, zone, or quadrant pattern. These patterns are systematic, ensuring that no area is left unsearched (Figure 2-4).Additional light sources might be needed to find hair and fibers. A vacuum cleaner with a clean bag is sometimes used to collect evidence buts not the method of choice. The use of a flashlight for examination andforceps for collecting are preferable, because this method avoids picking up extraneous materials.

Linear Quadrant or Zone Spiral What happened to Natalee Holloway in Aruba in 2005? This is an unsolved case in which questions have been raised about why crime scene investigators have not been able to find her body. In fact, investigators searched the island with an array of cutting-edge tools, from a remote-controlled submersible equipped with a video camera and sonar used for probing the water under bridges and in lagoons, to telescoping rods tipped with infrared sensors and cameras used for looking beneath manhole covers and into shadowy caverns.

**SECURING AND COLLECTING EVIDENCE**

All evidence needs to be properly packaged, sealed, and labeled. Specific procedures and techniques for evidence collection and storage must be followed. Liquids and arson remains are stored in airtight, unbreakable containers. Moist biological evidence is stored in breathable containers so the evidence can dry out, reducing the chance of mold contamination. After the

evidence is allowed to air dry, it is packaged in a **paper bindle**. The bindle (or druggist’s fold) can then be placed in a plastic or paper container. This outer container is then sealed with tape and labeled with the signature of the collector written across the tape. An evidence log and a **chain of custody** document must be attached to the evidence container.

The evidence log should contain all pertinent information, including:

• Case number

• Item inventory number

• Description of the evidence

• Name of suspect

• Name of victim

• Date and time of recovery

• Signature of person recovering the evidence

• Signature of any witnesses present during collection

**Packaging Evidence**

The size of the bindle depends on the size of the evidence. If the evidence is small, the bindle can be constructed from a sheet of paper. If the evidence is large, the bindle might be constructed from a large sheet of wrapping

paper.. The steps are as follows:

1. Choose the appropriate-size sheet of clean paper for the bindle.

2. Crease the paper as shown in the figure.

3. Place evidence in the X location.

4. Fold left and right sides in.

5. Fold in top and bottom.

6. Insert the top flap into the bottom flap then tape closed

*Demonstration of packaging of dry evidence.*

*a. Placement of evidence. b. Allow evidence to dry. c. Place dried evidence on bindle paper.*

*e. Secure bindle in labeled evidence bag using stick-on label. f. Place evidence in a plastic bag with an inserted evidence label. (Note that this is a different evidence source than the bloody cloth above.) g. Seal and tape the edge of the baggie. Fold bindle. Tuck the top flap into the bottom h. Write the collector’s signature across the baggie’s taped edge.*17

7. Place bindle inside a plastic or paper evidence bag. Fold the bag closed.

8. Place a seal over the folded edge of the evidence bag.

9. Have the collector write his or her name over the folded edge. If a wet object to be packaged is large, it should be placed in a paper container and sealed to allow it to air dry. Wet evidence should never be packaged in a plastic container while wet. Any DNA present will degenerate and evidence may become moldy and useless. There are standards for collecting different types of evidence that describe how to collect and store the evidence. The Federal Bureau of Investigation and state police agencies publish descriptions of the proper procedures. Control samples must also be obtained from the victim for the purpose of exclusion. For example, blood samples found on a victim or at a crime scene are compared with the victim’s blood. If they match, the samples are excluded from further study. If the blood samples do not match, then they may have come from the perpetrator and will be further examined.

**CHAIN OF CUSTODY**

In securing the evidence, maintaining the chain of custody is essential. The individual who finds evidence marks it for identification and bags the evidence in a plastic or paper container. The final container for the evidence is a collection bag, which is labeled with the pertinent information. The container is then sealed, and the collector’s signature is written across the

sealed edge. The container is given to the next person responsible for its care. That person takes it to the lab and signs it over to a technician, who opens the package for examination at a location other than the sealed edge. On completion of the examination, the technician repackages the evidence with its original packaging, reseals the evidence in a new packaging, and signs the chain-of-custody log attached to the packaging. This process ensures that the evidence has been responsibly handled as it was passed from the crime scene to a courtroom

*Chain-of-custody procedures.*

1. *Original evidence bag b. Opened evidence bag maintaining signature on first seal c. Original evidence bag with uncut seal and signature, updated chain-of-custody log in a new sealed and signed evidence bag*

**ANALYZE THE EVIDENCE**

Following a crime-scene investigation, the forensic laboratory work begins .The FBI crime lab is one of the largest forensic labs in the world. A forensic lab processes all of the evidence the crime-scene investigation collected to determine the facts of the case. Unlike what television CSI

programs portray, forensic lab technicians are specialized and process one type of evidence. The laboratory results are sent to the lead detective. Test results eventually lead to crime-scene reconstruction; that is, forming a hypothesis of the sequence of events from before the crime was committed through its commission. The detective looks at the evidence and attempts to determine how it fits into the overall crime scenario. The evidence is examined and compared with thewitnesses statements to determine the reliability of their accounts. Evidence analysis can link a suspect with a scene or a victim, establish the identity of a victim or suspect, confirm verbal witness testimony, or even acquit the innocent. The evidence does not lie, but investigators must consider all possible interpretations of the evidence. Direct evidence is more compelling than circumstantial evidence.

**CRIME-SCENE RECONSTRUCTION**

**Crime-scene reconstruction** involves forming a hypothesis of the sequence of events from before the crime was committed through its commission. The evidence is examined and compared with the witnesses’ statements to determine the reliability of their accounts. The investigator looks at the evidence and attempts to determine how it fits into the overall crime scenario. The evidence does not lie, but it could be staged. It is important that investigators

maintain an open mind as they examine all possibilities.

CHAPTER

**STAGED CRIME SCENES**

Staged crime scenes pose a unique problem. The evidence does not match the testimony of witnesses. Here is a list of some common situations in which a crime scene is staged:

• *Arson.* The perpetrator stages a fire to cover some other crime such as murder or burglary.

• *Suicide/murder.* A victim is murdered, and the perpetrator stages the scene to look like a suicide. The death may be caused by alcohol or drug overdose. The motive could be insurance money, release from an unhappy marriage, or simply theft.

• *Burglary.* A burglary is staged to collect insurance money. In the determination of whether a crime scene is staged, the following points should be considered:

• Initially treat all death investigations as homicides.

• Do the type(s) of wounds found on the victim match the weapon employed?

• Could the wounds be easily self-inflicted?

• Establish a profile of the victim through interviews with friends and family.

• Evaluate the behavior (mood and actions) of the victim before the event.

• Evaluate the behavior (mood and actions) of any suspects before the event.

• Corroborate statements with evidential facts.

• Reconstruct the event.

• Conduct all forensic examinations to determine the facts of the case.

• Evidence must be properly handled, collected, and labeled so that the

chain of custody is maintained.

• Evidence is analyzed in a forensic laboratory, and the results are provided

to detectives, who fit the results into the crime scenario.17

The crime-scene investigator has a challenging job. His or her specialty isin securing and processing a crime scene. To be well versed in the field, extensive study, training ,and experience in crime scene investigations are needed. He or she must be knowledgeable in the areas of recognition, documentation, and preservation of evidence at a crime scene to ensure that those recovered items will arrive safely at the lab. Investigators generally turn in the evidence to forensic specialists for analysis. However, they may have to testify in court about the evidence collected, the methods used to recover it, and the number of people who came into contact with the evidence. Is the job of a crime-scene investigator the way it is portrayed on television? Let’s ask areal-life CSI. Carl Williams of Jupiter, a retired Pennsylvania state police detective, has 25years of crime-scene investigation experience. Carl says, “The television shows are for entertainment, not reality. The crime scene doesn’twrap up in an hour, never mind an entire investigation.

That can take months. Also, television doesn’t show the real horror of what one human being can do to another. Not a lot of people can stomach it. But if you take it, the job can be fascinating work. Every day was different. It was interesting. I helped stop the people who committed horrendous acts before they could do it again. I’m proud of the work I’ve done.”

What is a typical day like? Here is one scenario:

At the beginning of a shift, you might be given a list of calls that have come in from police officers overnight. You will need to prioritize them and plan to investigate the min a logical order. Once you arrive at the crime scene, you will work with the first-responding police officer and decide what the best methods are for you to obtain evidence. You will then record the scene using photography and video, and gather evidence such as shoe prints, clothing fibers, blood, and hair. You may discover fingerprint evidence by brushing surfaces with special powders and take impressions of fingerprints from anyone who has accessed the crime scene. Finally, you will secure all of your samples in protective packaging and send them to forensic laboratories for

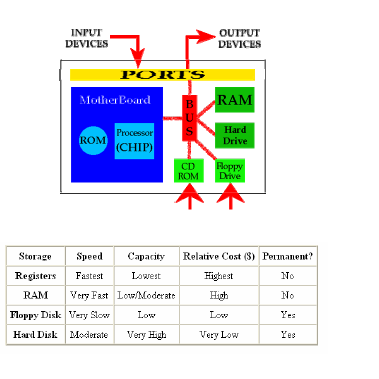
analysis. What does it take to become a crime-scene investigator? It is usually necessary to obtain a degree in crime-scene investigation through college degree programs or certification programs.

The crime-scene investigator should have an associate’s or bachelor’s degree either in an area of science, with emphasis in law enforcement and crime-scene processing, or a criminal justice degree with an emphasis in science.

**SCENES WORKING WITH WINDOWS/DOS SYSTEMS:**

How computer work?

Main components of computer



CPU / Motherboard processor

􀂾 ROM (stores system-level programs that should be available at all times, e.g. BIOS) busses / registers

􀂕􀂕 Main Memory – RAM (fast temporary memory)

Input Devices

􀂾 keyboard, mouse, …

Output Devices

􀂾 monitor, printer, …

􀂕􀂕 Secondary (Permanent) Storage

􀂾 hard disks / drive, CD-ROM,

USB, floppy,

**Operating System:**

****

**software (program + data) that runs on a computer – it manages computer hardware & provides common services for efficient execution of various application software .** OSs are found on almost all‘computing’ devices, e.g.cellular phones, video gameconsoles, web servers, routers, …

**File System** – **method of storing and organizing computer files and their data** gives an OS a road map to data on adata storage device (e.g. hard drive orCD-ROMs) file system is usually directly related toan OS



**Disk Drive** – **consists of 1 or more platters coated with magnetic material – data is stored on platters in a particular way** each platters has 2 surfaces: top & bottomkey disk drive components/elements:

􀂾 **geometry** – refers to a disk’s structure of platters, tracks, and sectors

􀂾 **head** – the device that reads and writes data to a drive – there is one head per platter

􀂾 **tracks** – concentric circles on a disk platter where data is located

􀂾 **sector** – a pie shaped section on a track, usually made up of 512 bytes (512 B)

􀂾 **a cylinder** – consists of corresponding tracks on all platters (e.g. track 12 on all d.d. platters)

**Heads** – **located on both sides of (each) platter only a few microns from the surface**

􀂕􀂕 heads are static, disk/platters rotate at speed of n\*1000 revolutions per minute! (~ 250km/h)

􀂕􀂕 heads are ‘inductive’ – they can generate a magnetic field by creating positive or negative fields, they polarize the disk (platter) surface in a very tiny area when these areas are read afterwards, the detected polarity is transformed by a ADC into a 0 or 1

**Cluster** – **a group of multiple sectors – logical unit of file storage on a hard drive** number of sectors in a cluster (2n), depends on:

􀂾 disk size: bigger disk ⇒ bigger cluster

􀂾 logical disk organization (FAT12 /16 /32 or NTFS)

􀂕􀂕 whatever the logical size of a file, it is allocated disk space in multiples of clusters!

􀂾 sectors in a cluster are physically adjacent on the disk

􀂾 clusters in a file may NOT be adjacent

􀂕􀂕 clusters are managed by computers OS



**FAT File System**

**FAT x – File Allocation Table** **– family of file systems for DOS/Windows operating systems**

􀂕􀂕 FAT (table) stores information on status of all clusters on the disk equivalent to ‘table of content’ x = 12, 16, or 32 – number of bits used for cluster identification/numbering bit-size of each FAT table entry



Example: FAT12, FAT16, FAT32





􀂕􀂕 major sections on a FAT hard disk:

**1)Boot Sector** – occupies the 1st cluster on the disk contains specific information about organization of the file system, including: type of FAT (12/16/32) system, of bytes per sector, # of sectors per track, # of sectors per cluster, # of read heads, # of FAT tables, of clusters per FAT table, etc.

2) **FAT Tables**

􀂾 list of entries corresponding to clusters on the disk each entry records current status of respective cluster

3) **Root Directory**

􀂾 stores Directory Table – table of 32-bit long entries for each file & directory created on the disk

4) **Data Area**

􀂾 contains file & directory data – occupies remaining sectors (clusters) on the disk first cluster of Data Area is numbered 2; though, this is physical sector 33!

**Slack Space** – **phenomenon caused by the way how computers store data/files:**

files are allocated cluster-sized chunks and they are written in sector-sized chunks – regardless of the actual size of data/file

􀂾 data may not be big enough to fill (all) segments, i.e. clusters

**Slack Space** 􀂕􀂕 sector slack - space between EOF and end of last sector that file was written to also known as RAM slack as OS pulls any info available in RAM at that point (memory dump)

to fill this space – e.g. logon IDs, passwords, segments of other files not an issue in post Windows 98 / NT

􀂕􀂕 cluster slack - remaining sectors in cluster also known as file slack – contains whatever was

last written by disk in those sectors (e.g. parts of a deleted file)



**Deleting FAT** – **system places deletion mark on the file**

􀂕􀂕 deletion mark ⇒ first letter of the file name is replaced with E5 (lower-case Greek letter σ)

􀂕􀂕 FAT entries of respective clusters are still unchanged! in DATA AREA cluster still preserve

the original data!

**Forensics Implications**

􀂕􀂕 On deletion of a file, the data contained in a file is NOT ‘gone’ – it is merely ‘hidden’ from he operating system and the space it occupies is made available for reuse.

􀂕􀂕 Deleted data still resides in the space previously allocated to it, unless overwritten. It is possible to ‘undelete’ (reconstruct) a file – or some of its parts – even after Recycle bin has been emptied – the only information that cannot be recovered is the first letter of the file!

􀂕􀂕 However, there may be evidential difficulties with files recovered from unallocated space. We cannot state the date and time attributes of even a complete file found in unallocated space,

as there is no respective entry in the File Directory Table.

**Disk Formatting** – **still does not erase data!**

􀂕􀂕 only pointers (FAT and FDT) get destroyed

􀂕􀂕 data that formed the file remains intact in their locations

**Disk Wiping** – secure deletion – wiped files have their directory entries and allocated space physically overwritten by random or user-defined characters

**NTFS File System:**

**NTFS** – New Technology File System **– introduced for Windows NT and Vista** provides significant improvements over FAT,including:

􀂾 **file and folder permissions** – folder and file access can be controlled individually

􀂾 **file encryption** – NTFS enables strong encryption of files and folders extremely resistant to attacks

􀂾 **file compression** – NTFS enables lossy compression on both files and folders

􀂾 **disk efficiency** – NTFS supports smaller cluster size than FAT32

􀂾 **greater reliability** – NTFS writes a log of changes being made to files and folders (NTFS journal), which helps the OS to recover from system failures …

**Windows Registry:**

**critical part of any Windows OSs - hierarchical database containing configuration information about:**

􀂾 system hardware;

􀂾 installed software (programs);

􀂾 property settings;

􀂾 profile for each user, etc.

􀂕􀂕 OS uses instructions stored in the registry to determine how installed hardware and

and software should function

􀂕􀂕 e.g. typical software comes with a Windows installer that writes to the registry during

installation

􀂾 system must be restarted for changes to take place …

**Forensics implications – information (**i.e. potential evidence**) that reside in the Registry make it a significant forensics resource**

information that can be found in theregistry include:

􀂾 general information about the OS

􀂾 startup (boot-time) applications

􀂾 logs of computers that have communicated with the host

􀂾 logs of USBs that have been connected to the host

􀂾 logs of Web site histories and typed URLs

􀂾 downloaded files/programs, e.g. wiping programs to destroy evidence

􀂾 auto complete Internet Explorer passwords

**Computer forensics tools:**

Computer forensics is a very important branch of computer science in relation to computer and Internet related crimes. Earlier, computers were only used to produce data but now it has expanded to all devices related to digital data. The goal of Computer forensics is to perform crime investigations by using evidence from digital data to find who was the responsible for that particular crime.

For better research and investigation, developers have created many computer forensics tools. Police departments and investigation agencies select the tools based on various factors including budget and available experts on the team.

These computer forensics tools can also be classified into various categories:

* Disk and data capture tools
* File viewers
* File analysis tools
* Registry analysis tools
* Internet analysis tools
* Email analysis tools
* Mobile devices analysis tools
* Mac OS analysis tools
* Network forensics tools
* Database forensics tools

In this post, we are listing a few important and popular data forensics tools. Before proceeding further, I want to make it clear that tools are added in random order. So, please do not try to consider it as a ranking of the tools.

**1. Digital Forensics Framework**

Digital Forensics Framework is another popular platform dedicated to digital forensics. The tool is open source and comes under GPL License. It can be used either by professionals or non-experts without any trouble. It can be used for digital chain of custody, to access the remote or local devices, forensics of Windows or Linux OS, recovery hidden of deleted files, quick search for files’ meta data, and various other things.

**2. Open Computer Forensics Architecture**

Open Computer Forensics Architecture (OCFA) is another popular distributed open-source computer forensics framework. This framework was built on Linux platform and uses postgreSQL database for storing data.

It was built by the Dutch National Police Agency for automating digital forensics process. It is available to download under GPL license.

**3. CAINE**

CAINE (Computer Aided Investigative Environment) is the Linux distro created for digital forensics. It offers an environment to integrate existing software tools as software modules in a user friendly manner. This tool is open source.

**4. X-Ways Forensics**

X-Ways Forensics is an advanced platform for digital forensics examiners. It runs on all available version of Windows. It claims to not be very resource hungry and to work efficiently. If we talk about the features, find the key features in the list below:

* Disk imaging and cloning
* Ability to read file system structures inside various image files
* It supports most of the file systems including FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3®, CDFS/ISO9660/Joliet, UDF
* Automatic detection of deleted or lost hard disk partition
* Various data recovery techniques and powerful file carving
* Bulk hash calculation
* Viewing and editing binary data structures using templates
* Easy detection of and access NTFS ADS
* Well maintained file header
* Automated activity logging
* Data authenticity
* Complete case management
* Memory and RAM analysis
* Gallery view for pictures
* Internal viewer for Windows registry file
* Automated registry report
* Extracts metadata from various file types
* Ability to extract emails from various available email clients.

**5. SANS Investigative Forensics Toolkit – SIFT**

SANS Investigative Forensics Toolkit or SIFT is a multi-purpose forensic operating system which comes with all the necessary tools used in the digital forensic process. It is built on Ubuntu with many tools related to digital forensics. Earlier this year, SIFT 3.0 was released. It comes for free or charge and contains free open-source forensic tools.

In a previous post at resource.infosecinstitute.com, we already covered SIFT in detail. You can read those posts about SIFT to know more about this digital forensics platform.

**6. EnCase**

EnCase is another popular multi-purpose forensic platform with many nice tools for several areas of the digital forensic process. This tool can rapidly gather data from various devices and unearth potential evidence. It also produces a report based on the evidence.

This tool does not come for free. The license costs $995.

**7. Registry Recon**

Registry Recon is a popular registry analysis tool. It extracts the registry information from the evidence and then rebuilds the registry representation. It can rebuild registries from both current and previous Windows installations.

It is not a free tool. It costs $399.

**8. The Sleuth Kit**

The Sleuth Kit is a Unix and Windows based tool which helps in forensic analysis of computers. It comes with various tools which helps in digital forensics. These tools help in analyzing disk images, performing in-depth analysis of file systems, and various other things.

**9. Llibforensics**

Libforensics is a library for developing digital forensics applications. It was developed in Python and comes with various demo tools to extract information from various types of evidence.

**10. Volatility**

Volatility is the memory forensics framework. It used for incident response and malware analysis. With this tool, you can extract information from running processes, network sockets, network connection, DLLs and registry hives. It also has support for extracting information from Windows crash dump files and hibernation files. This tool is available for free under GPL license.

**11. WindowsSCOPE**

WindowsSCOPE is another memory forensics and reverse engineering tool used for analyzing volatile memory. It is basically used for reverse engineering of malwares. It provides the capability of analyzing the Windows kernel, drivers, DLLs, virtual and physical memory.

**12. The Coroner’s Toolkit**

The Coroner’s Toolkit or TCT is also a good digital forensic analysis tool. It runs under several Unix-related operating systems. It can be used to aid analysis of computer disasters and data recovery.

**13. Oxygen Forensic Suite**

Oxygen Forensic Suite is a nice software to gather evidence from a mobile phone to support your case. This tool helps in gathering device information (including manufacturer, OS, IMEI number, serial number), contacts, messages (emails, SMS, MMS), recover deleted messages, call logs and calendar information. It also lets you access and analyze mobile device data and documents. It generates easy to understand reports for better understanding.

**14. Bulk Extractor**

Bulk Extractor is also an important and popular digital forensics tool. It scans the disk images, file or directory of files to extract useful information. In this process, it ignores the file system structure, so it is faster than other available similar kinds of tools. It is basically used by intelligence and law enforcement agencies in solving cyber crimes.

**15. Xplico**

Xplico is an open source network forensic analysis tool. It is basically used to extract useful data from applications which use Internet and network protocols. It supports most of the popular protocols including HTTP, IMAP, POP, SMTP, SIP, TCP, UDP, TCP and others. Output data of the tool is stored in SQLite database of MySQL database. It also supports IPv4 and IPv6 both.

**16. Mandiant RedLine**

Mandiant RedLine is a popular tool for memory and file analysis. It collects information about running processes on a host, drivers from memory and gathers other data like meta data, registry data, tasks, services, network information and Internet history to build a proper report.

**17. Computer Online Forensic Evidence Extractor (COFEE)**

Computer Online Forensic Evidence Extractor or COFEE is a tool kit developed for computer forensic experts. This tool was developed by Microsoft to gather evidence from Windows systems. It can be installed on a USB pen drive or external hard disk. Just plug in the USB device in the target computer and it starts a live analysis. It comes with 150 different tools with a GUI based interface to command the tools. It is fast and can perform the whole analysis in as few as 20 minutes. To law enforcement agencies, Microsoft provides free technical support for the tool.

**18. P2 eXplorer**

P2 eXplorer is a forensic image mounting tool which aims to help investigating officers with examination of a case. With this image, you can mount forensic images as a read-only local and physical disc and then explore the contents of the image with file explorer. You can easily view deleted data and unallocated space of the image.

It can mount several images at a time. It supports most of the image formats including EnCasem, safeBack, PFR, FTK DD, WinImage, Raw images from Linux DD, and VMWare images. It supports both logical and physical image types.

This tool comes for $199, but you can grab the limited feature version of the tool for free.

**19. PlainSight**

PlainSight is another useful digital forensics tool. It is a CD based Knoppix which is a Linux distribution. Some of its uses include viewing Internet histories, data carving, checking USB device usage, memory dumps extracting password hashes, information gathering, examining Windows firewall configuration, seeing recent documents, and other useful tasks. For using this too, you only need to boot from the CD and the follow the instructions.

This tool is available for free.

**20. XRY**

XRY is the mobile forensics tool developed by Micro Systemation. It is used to analyze and recover crucial information from mobile devices. This tool comes with a hardware device and software. Hardware connects mobile phones to PC and software performs the analysis of the device and extract data. It is designed to recover data for forensic analysis.

The latest version of the tool can recover data from all kind of smartphones including Android, iPhone and BlackBerry. It gathers deleted data like call records, images, SMS and text messages.

**21. HELIX3**

HELIX3 is a live CD-based digital forensic suite created to be used in incident response. It comes with many open source digital forensics tools including hex editors, data carving and password cracking tools. If you want the free version, you can go for Helix3 2009R1. After this release, this project was overtaken by a commercial vendor. So, you need to pay for most recent version of the tool.

This tool can collect data from physical memory, network connections, user accounts, executing processes and services, scheduled jobs, Windows Fegistry, chat logs, screen captures, SAM files, applications, drivers, environment variables and Internet history. Then it analyzes and reviews the data to generate the complied results based on reports.

**22. Cellebrite UFED**

Cellebrite’s UFED solutions present a unified workflow to allow examiners, investigators and first responders to collect, protect and act decisively on mobile data with the speed and accuracy a situation demands – without ever compromising one for the other. The UFED Pro Series is designed for forensic examiners and investigators who require the most comprehensive, up-to-date mobile data extraction and decoding support available to handle the influx of new data sources. Platform agnostic, the UFED Field Series is designed to unify workflows between the field and lab, making it possible to view, access and share mobile data via in-car workstations, laptops, tablets or a secure, self-service kiosk located at a station.

**Software and hardware tools:**

**Disk tools and data capture**

| **Name** | **From** | **Description** |
| --- | --- | --- |
| [Arsenal Image Mounter](https://www.arsenalrecon.com/apps/image-mounter/) | Arsenal Consulting | Mounts disk images as complete disks in Windows, giving access to Volume Shadow Copies, etc. |
| [DumpIt](http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/) | MoonSols | Generates physical memory dump of Windows machines, 32 bits 64 bit. Can run from a USB flash drive. |
| [EnCase Forensic Imager](http://www1.guidancesoftware.com/Order-Forensic-Imager.aspx) | Guidance Software | Create EnCase evidence files and EnCase logical evidence files [direct download link] |
| [Encrypted Disk Detector](http://info.magnetforensics.com/encrypted-disk-detector) | Magnet Forensics | Checks local physical drives on a system for TrueCrypt, PGP, or Bitlocker encrypted volumes |
| [EWF MetaEditor](http://www.4discovery.com/our-tools/) | 4Discovery | Edit EWF (E01) meta data, remove passwords (Encase v6 and earlier) |
| [FAT32 Format](http://www.ridgecrop.demon.co.uk/index.htm?fat32format.htm) | Ridgecrop | Enables large capacity disks to be formatted as FAT32 |
| [Forensics Acquisition of Websites](http://www.fawproject.com/en/default.aspx) | Web Content Protection Association | Browser designed to forensically capture web pages |
| [FTK Imager](http://www.accessdata.com/support/product-downloads) | AccessData | Imaging tool, disk viewer and image mounter |
| [Guymager](http://guymager.sourceforge.net/) | vogu00 | Multi-threaded GUI imager under running under Linux |
| [Live RAM Capturer](http://forensic.belkasoft.com/en/ram-capturer) | Belkasoft | Extracts RAM dump including that protected by an anti-debugging or anti-dumping system. 32 and 64 bit builds |
| [NetworkMiner](http://sourceforge.net/projects/networkminer/) | Hjelmvik | Network analysis tool. Detects OS, hostname and open ports of network hosts through packet sniffing/PCAP parsing |
| [Nmap](http://nmap.org/) | Nmap | Utility for network discovery and security auditing |
| [Magnet RAM Capture](http://www.magnetforensics.com/ram-capture/) | Magnet Forensics | Captures physical memory of a suspect’s computer. Windows XP to Windows 10, and 2003, 2008, 2012. 32 & 64 bit |
| [OSFClone](http://www.osforensics.com/tools/create-disk-images.html) | Passmark Software | Boot utility for CD/DVD or USB flash drives to create dd or AFF images/clones. |
| [OSFMount](http://www.osforensics.com/tools/mount-disk-images.html) | Passmark Software | Mounts a wide range of disk images. Also allows creation of RAM disks |
| [Wireshark](https://www.wireshark.org/) | Wireshark | Network protocol capture and analysis |
| [Disk2vhd](https://technet.microsoft.com/en-gb/sysinternals/ee656415.aspx) | Microsoft | Creates Virtual Hard Disks versions of physical disks for use in Microsoft Virtual PC or Microsoft Hyper-V VMs |

### 

| Name | From | Description |
| --- | --- | --- |
| [EDB Viewer](http://www.nucleustechnologies.com/exchange-edb-viewer.html) | Lepide Software | Open and view (not export) Outlook EDB files without an Exchange server |
| [Mail Viewer](http://www.mitec.cz/mailview.html) | MiTeC | Viewer for Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird message databases and single EML files |
| [MBOX Viewer](http://www.systoolsgroup.com/mbox-viewer.html) | SysTools | View MBOX emails and attachments |
| [OST Viewer](http://www.nucleustechnologies.com/ost-viewer.html) | Lepide Software | Open and view (not export) Outlook OST files without connecting to an Exchange server |
| [PST Viewer](http://www.nucleustechnologies.com/pst-viewer.html) | Lepide Software | Open and view (not export) Outlook PST files without needing Outlook |

[Return to top of page](https://forensiccontrol.com/resources/free-software/#top)

### 

| Name | From | Description |
| --- | --- | --- |
| [Agent Ransack](http://www.mythicsoft.com/page.aspx?type=agentransack&page=home) | Mythicsoft | Search multiple files using Boolean operators and Perl Regex |
| [Computer Forensic Reference Data Sets](http://www.cfreds.nist.gov/) | NIST | Collated forensic images for training, practice and validation |
| [EvidenceMover](http://www.nuix.com/Nuix-evidence-mover) | Nuix | Copies data between locations, with file comparison, verification, logging |
| [FastCopy](http://ipmsg.org/tools/fastcopy.html.en) | Shirouzu Hiroaki | Self labelled ‘fastest’ copy/delete Windows software. Can verify with SHA-1, etc. |
| [File Signatures](http://www.garykessler.net/library/file_sigs.html) | Gary Kessler | Table of file signatures |
| [HexBrowser](http://www.hexbrowser.com/) | Peter Fiskerstrand | Identifies over 1000 file types by examining their signatures |
| [HashMyFiles](http://www.nirsoft.net/utils/hash_my_files.html) | Nirsoft | Calculate MD5 and SHA1 hashes |
| [MobaLiveCD](http://mobalivecd-en.mobatek.net/) | Mobatek | Run Linux live CDs from their ISO image without having to boot to them |
| [Mouse Jiggler](http://mousejiggler.codeplex.com/) | Arkane Systems | Automatically moves mouse pointer stopping screen saver, hibernation etc. |
| [Notepad ++](http://notepad-plus-plus.org/) | Notepad ++ | Advanced Notepad replacement |
| [NSRL](http://www.nsrl.nist.gov/Downloads.htm) | NIST | Hash sets of ‘known’ (ignorable) files |
| [Quick Hash](http://sourceforge.net/projects/quickhash/) | Ted Technology | A Linux & Windows GUI for individual and recursive SHA1 hashing of files |
| [USB Write Blocker](http://dsicovery.com/dsicovery-software/usb-write-blocker/) | DSi | Enables software write-blocking of USB ports |
| [Volix](http://www.it-forensik.fh-aachen.de/projekte/volix/13) | FH Aachen | Application that simplifies the use of the Volatility Framework |
| [Windows Forensic Environment](http://winfe.wordpress.com/) | Troy Larson | Guide by Brett Shavers to creating and working with a Windows boot CD |

### Mac OS tools

| Name | From | Description |
| --- | --- | --- |
| [Audit](https://github.com/twocanoes/audit) | Twocanoes Software | Audit Preference Pane and Log Reader for OS X |
| [ChainBreaker](http://forensic.n0fate.com/?page_id=412) | Kyeongsik Lee | Parses keychain structure, extracting user’s confidential information such as application account/password, encrypted volume password (e.g. filevault), etc |
| [Disk Arbitrator](https://github.com/aburgh/Disk-Arbitrator) | Aaron Burghardt | Blocks the mounting of file systems, complimenting a write blocker in disabling disk arbitration |
| [Epoch Converter](https://www.blackbagtech.com/resources/freetools/epochconverter.html) | Blackbag Technologies | Converts epoch times to local time and UTC |
| [FTK Imager CLI for Mac OS](http://accessdata.com/product-download/digital-forensics/mac-os-10.5-and-10.6x-version-3.1.1) | AccessData | Command line Mac OS version of AccessData’s FTK Imager |
| [IORegInfo](https://www.blackbagtech.com/resources/freetools/ioreg-info.html) | Blackbag Technologies | Lists items connected to the computer (e.g., SATA, USB and FireWire Drives, software RAID sets). Can locate partition information, including sizes, types, and the bus to which the device is connected |
| [PMAP Info](https://www.blackbagtech.com/resources/freetools/pmap-info.html) | Blackbag Technologies | Displays the physical partitioning of the specified device. Can be used to map out all the drive information, accounting for all used sectors |
| [Volafox](http://forensic.n0fate.com/?page_id=412) | Kyeongsik Lee | Memory forensic toolkit for Mac OS X |

### Mobile devices

| Name | From | Description |
| --- | --- | --- |
| [iPBA2](http://ipbackupanalyzer.com/) | Mario Piccinelli | Explore iOS backups |
| [iPhone Analyzer](http://sourceforge.net/projects/iphoneanalyzer/) | Leo Crawford, Mat Proud | Explore the internal file structure of Pad, iPod and iPhones |
| [ivMeta](http://www.csitech.co.uk/ivmeta-iphone-metadata/) | Robin Wood | Extracts phone model and software version and created date and GPS data from iPhone videos. |
| [Last SIM Details](http://lastsimdetails.blogspot.co.uk/p/downloads.html) | Dan Roe | Parses physical flash dumps and Nokia PM records to find details of previously inserted SIM cards. |
| [Rubus](http://www.cclgroupltd.com/Buy-Software/rubus-ipd-de-constructor-utility.html) | CCL Forensics | Deconstructs Blackberry .ipd backup files |
| [SAFT](http://www.signalsec.com/saft/) | SignalSEC Corp | Obtain SMS Messages, call logs and contacts from Android devices |