UNIT I - DIGITAL FORENSICS

What is Digital Forensics?

While it is easy to say you have a general idea of digital forensics, given the existence of crime shows like *CSI: Cyber* or *Criminal Minds*, where a dramatized equivalent is shown, the reality is a little less advanced. While it is true that digital forensics is a revolutionary tool fit for the modern age of information technology, it is never as rapid as those television programs lead you to believe.

Digital forensics is a branch of the same forensic science used by crime scene investigators that focuses on crimes using information technology like computers, mobile phones, tablets, etc. The rise of digital forensics began when Florida ratified the Florida Computer Crimes Act in 1978. In 1980, federal laws followed suit to recognize the crimes using earlier computer models.

To apply digital forensics, law enforcement professionals require an assortment of tools, programs, and skills that will enable them to access protected data. While most television shows portray this as a single “tech whiz” forensic technician breaking into a criminal’s network, the reality is less exciting.

Digital forensics requires warrants, like all forensic assessments, and is generally used to acquire logs from legally confiscated devices, confirm alibis, verify search history, and so on. Aggressive hacking attempts by law enforcement are generally reserved for members of international defense agencies.

It is also important to note that most digital forensic tools have limitations that make them fallible in certain situations. The media portrayal of digital forensics has tainted the public’s understanding of what digital forensics is capable of and the process the forensic technicians must follow. In most cases, digital forensics has a 9-phase program law enforcement professionals follow to apprehend the cybercriminal. These 9 phases cover different parts of the forensic process and ultimately connect to help the law enforcement agency make a righteous arrest.

Phases of Digital Forensics

Phase 1: First Response

Perhaps the most important part of digital forensics is the initial response made by the forensic team. In most crimes, the first few hours are among the most important since it gives the criminals less time to cover their tracks. This is no different with digital forensics since hardware can be destroyed and evidence lost forever. While technicians can almost always recover cloud data, it is still important that the forensic team be prepared to launch a prompt response. The first response phase of digital forensics begins when a security incident occurs and a report is made to the proper channels.

Once the report comes in, the forensic team must immediately begin their investigation by proceeding to the site of the incident. Whether it was a network breach or a device was associated with a crime, the team must immediately deploy to begin the forensic process in earnest.

Phase 2: Search and Seizure

The next phase of digital forensics is the acquisition of evidence sources. When a forensic team is tasked with searching for evidence, they often need to access the device where that information is stored. With the proper warrants, a forensic technician is permitted to seize your computer, mobile device, and any other technology that can store data.

This is accomplished by having investigators seize the devices so long as the warrant is valid. For example, a warrant permitting an investigator to seize your phone does not necessarily mean they can seize your laptop. When cybercrimes are suspected, most warrants allow the seizure of all devices capable of the crime. Search and seizure is important to every type of case, but cybercrimes authorize the seizure of specific items.

Phase 3: Evidence Collection

Once the investigators have seized the devices associated with the cybercrime, the forensic technicians can begin their work. Collecting evidence is not as simple as opening the device and uncovering the suspect’s secrets. Cybercriminals tend to hide the evidence of their deeds with just as much digital protection as what they breached to access information. They might even try to purge the information from the device to hide their guilt.

For this reason, digital forensic technicians must employ various forensic programs and tools to decrypt and recover data. Even data that has been deleted can be forensically recovered from the device's hard drive. Through these techniques, forensic technicians can collect data proving or disproving the suspect's involvement in cybercrime.

Phase 4: Securing of the Evidence

When collecting evidence to prove criminal activity, there is a sacred trust called chain of custody that preserves the integrity of the evidence. This chain of custody determines how the evidence is stored, who can access it, who authenticates it, etc. While the technicians collect the evidence, they do not necessarily examine it or retain control over it.

Any evidence found on the devices must be secured and stored per the chain of custody used for that specific case. This means the evidence cannot be tampered with or altered to implicate or exonerate the suspect. If it comes to light that the forensic team did not store the data following the chain of custody, the case could lead to a mistrial, and a potential criminal could go free.

Phase 5: Data Acquisition

The data acquisition stage is similar to evidence collection, though data acquisition specifically pertains to electronically stored information (ESI). While the evidence collection stage can include hardware, data acquisition is strictly about the data stored on the hardware.

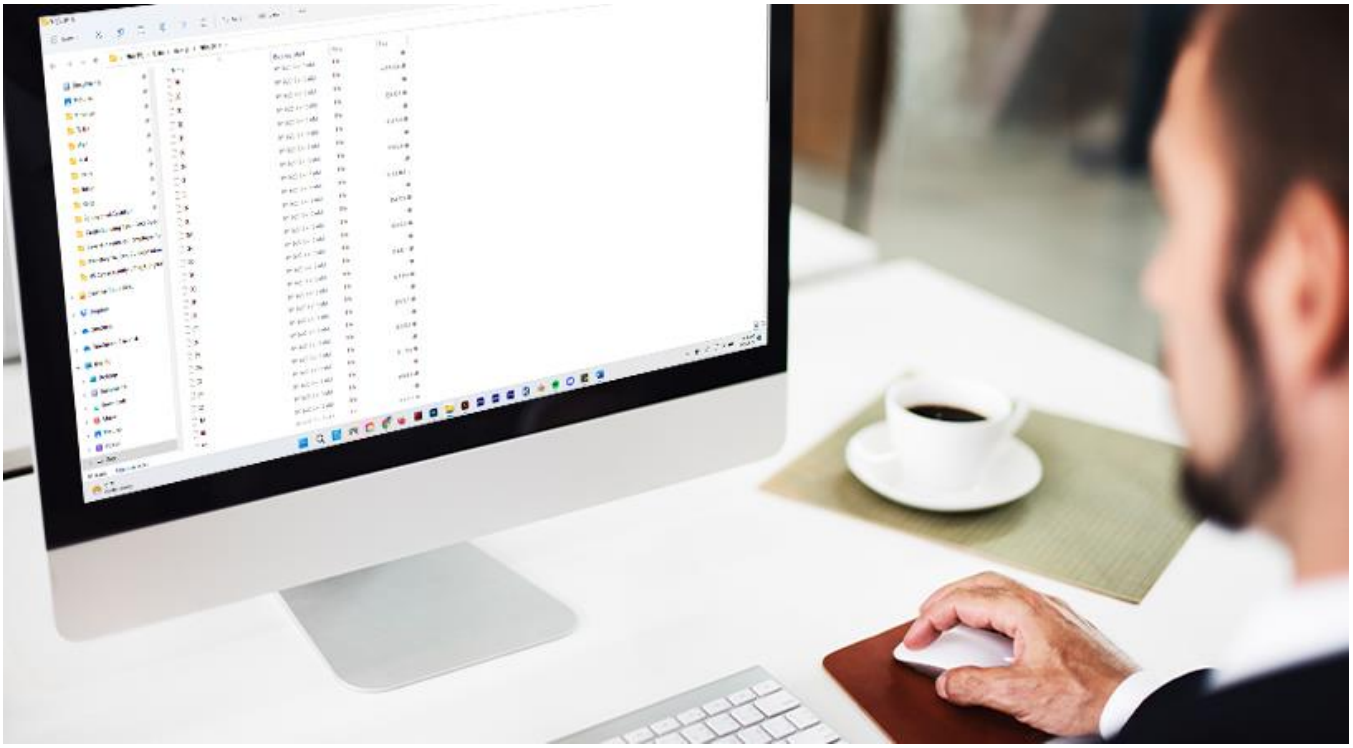
Electronically stored information refers to any user-created documents or files stored on the device's hard drive, including:

- Microsoft Office or similar documents.
- Video files.
- Blueprints and maps.
- Digital photographs.
- Scanned images.
- E-mails.
- Digital audio files.

Other documents qualify, but these are some of the most commonly sought files on devices. These documents could pertain to the case and must be collected for examination. However, the technician recovering these documents must not compromise the integrity of the files while extracting them. Even an accidental keyboard tap that adds an extra letter to a Microsoft Word document is considered an alteration that invalidates the file as evidence.

Phase 6: Data Analysis

While acquiring evidence from seized devices is fundamental to any digital forensic investigation, it is not enough to only access the data. Once the evidence has been located, it must be analyzed to determine whether it is pertinent to the case. Once the chain of custody has been established, a technician can analyze the data for anything that might prove useful in a court setting or confirm that the suspect was involved in cybercriminal activity.



This analysis helps prepare the law enforcement team for courtroom settings and justifying the prosecution's case. It is also used to filter impertinent information from the evidence files, such as vacation photos or a list of pet names.

Phase 7: Evidence Assessment

Arguably the most important part of the process, the investigators must assess the information recovered and link it to the crime for which the suspect is accused. If none of the recovered data confirms the suspect's involvement, the wrong person might have been accused. For this reason, investigators must compare the analyzed data to other details about the case that might not pertain to digital forensics.

For example, if the suspect is accused of hacking a private network and recently researched the programs used by the victim, it might make them seem guilty. But if the suspect had no motive and their device showed no signs of recent hack attempts, they might have been a victim of coincidence. Conversely, if the victim has a history of hostility with the victim and there are signs of hacking software on the device, the case becomes stronger. Evidence assessment is the part of digital forensics that most closely connects with standard police work.

Phase 8: Documentation and Reporting

The next digital forensics phase occurs after the initial investigation is complete and preparations for a court case are underway. Once the evidence is collected, authenticated, analyzed, and assessed, it must be documented and reported under state and federal law. Any legal case, civil or criminal, requires evidence to be submitted as part of a discovery process.

The evidence must be approved by the judge overseeing the case, and the prosecution must send copies to the defense's legal counsel to maintain fair knowledge of the case on both sides. It is illegal to surprise the defense with newly discovered documents from the devices halfway through the trial.

Every piece of evidence collected from the defendant's devices must be submitted to discovery after phases 1 through 7 are complete. Otherwise, the evidence will be rendered inadmissible and useless in a court of law. It also jeopardizes the case since it makes the prosecution seem devious.

Phase 9: Expert Witness Testimony

Virtually every criminal case, cybercrime included, has an expert witness who can provide insight into the significance of the evidence. Criminal trials are presented to a jury of the defendant's peers, and the jurors might not have the knowledge necessary to understand the importance of forensically recovered ESI.

When dealing with cybercrimes, they will almost certainly not know the significance of certain malware tools and how they relate to the case. For that reason, digital forensics teams serve as expert witnesses who can testify in court to confirm the importance of the evidence. They affirm the usefulness of the data using terminology that the jurors can understand. Doing so helps them connect the dots between what was recovered from the devices and the defendant's guilt.

While serving as an expert witness is not strictly technical, digital forensic technicians' knowledge makes them as valuable as the information they collect.

seizure of digital information

The seizure of digital information is a critical step in the field of digital forensics. It involves the physical or logical acquisition of digital data from various devices and storage media for the purpose of investigation and analysis. Here are more detailed aspects of the seizure phase:

Identification of Target Devices: Before seizing any digital information, investigators must identify the specific devices or storage media relevant to the investigation. This may include computers, mobile phones, external hard drives, servers, cloud accounts, or other digital storage devices.

Legal Authorization: It is crucial to obtain legal authorization to seize digital information. This authorization typically comes in the form of search warrants or subpoenas, which are issued by a court. Without proper legal authority, the seizure of digital evidence may not be admissible in court.

Chain of Custody: Establishing a chain of custody is essential during the seizure phase. This involves documenting who handled the evidence, when it was collected, where it was found, and any other relevant details. The chain of custody helps maintain the integrity and admissibility of the evidence.

Physical and Logical Seizure: Digital information can be seized physically or logically:

a. Physical seizure involves physically confiscating the devices or storage media, which may be done by law enforcement or forensic experts. It may require temporarily disconnecting devices from networks, unplugging cables, and removing hardware components.

b. Logical seizure involves making a copy (forensic image) of the digital data without altering the original. This is typically the preferred method, as it minimizes the risk of altering or damaging the evidence. Forensic tools are used to create a bit-for-bit copy of the data, preserving its integrity.

Documentation: Detailed documentation is maintained throughout the seizure process. This includes noting the make and model of devices, serial numbers, the condition of the equipment, and any visible damage. Photographs and written descriptions are often used to capture the state of the devices at the time of seizure.

Data Encryption and Passwords: If digital evidence is encrypted or protected by passwords, investigators may need to employ specialized techniques and tools to gain access to the data. This may involve cracking encryption keys or recovering passwords in accordance with the law.

Safeguarding Evidence: Once seized, the digital evidence must be securely stored and protected to prevent any unauthorized access or tampering. Physical evidence is typically stored in a secure evidence locker, while digital copies are often stored on write-protected media to prevent changes.

Preservation of Original Evidence: The original evidence must be carefully preserved in its unaltered state to maintain its integrity and admissibility in court. This is essential in case the defense requests access to the original evidence for independent analysis.

Handling Electronic Evidence: Proper handling of electronic evidence is crucial to prevent data corruption or contamination. Investigators should avoid running any software or altering data on the seized devices unless it is necessary for immediate operational purposes.

Chain of Custody Continuation: The chain of custody documentation continues throughout the investigation, noting the movement, handling, and access to the seized evidence by various individuals.

Handheld forensics

Handheld forensics, also known as mobile device forensics, is a specialized subfield of digital forensics that focuses on the acquisition, analysis, and investigation of data stored on mobile devices, such as smartphones, tablets, and portable media players. Here's a more detailed overview of the key aspects of handheld forensics:

Types of Mobile Devices: Handheld forensics covers a wide range of mobile devices, including smartphones (e.g., iPhone, Android devices), tablets (e.g., iPad), feature phones, portable media players, and GPS devices.

Data Acquisition: Mobile devices contain a vast amount of data, including call logs, text messages, emails, photos, videos, contacts, app data, and more. Forensic investigators use specialized tools and techniques to acquire a forensic image or logical copy of the data on these devices. This process ensures that the original data remains intact.

Physical vs. Logical Acquisition: Depending on the device and its security features, investigators may perform physical or logical acquisitions. Physical acquisition involves making a bit-by-bit copy of the device's memory, including deleted data. Logical acquisition focuses on extracting active data from the device without necessarily capturing deleted data.

Unlocking and Password Bypass: In some cases, investigators may need to unlock or bypass device security measures, such as PINs, passcodes, and biometrics, to access the data. This process may require specialized tools and expertise to avoid data loss or device lockout.

App Data Analysis: Mobile devices host a wide range of applications, and their data can be crucial to an investigation. Investigators analyze app-specific data, including chat messages, social media activity, geolocation, and more. Third-party tools may be necessary to interpret the data from proprietary apps.

Location Data: Many mobile devices have built-in GPS functionality. Handheld forensics can uncover location history data, which can be vital in criminal investigations. Location data can be obtained from various sources, including GPS coordinates, cell tower data, and Wi-Fi networks.

Cloud Forensics: In addition to data stored on the device itself, investigators may need to access data stored in the cloud. This includes data stored on platforms like iCloud, Google Drive, or Dropbox. Obtaining access to cloud data often requires legal cooperation and specialized cloud forensic techniques.

Data Recovery: Mobile devices may contain deleted data that could be relevant to an investigation. Forensic tools and techniques are used to recover deleted files, messages, and other digital artifacts.

Report Generation: Detailed reports are created to document the findings of the mobile device forensic analysis. These reports include information about the acquired data, analysis results, and any relevant artifacts discovered during the investigation.

Legal Considerations: As with any form of digital forensics, legal considerations are paramount. Investigators must ensure that all actions are conducted in compliance with the law, and proper chain of custody is maintained. Evidence collected should be admissible in court.

Expert Testimony: Mobile device forensic experts may be called upon to testify in court as expert witnesses to explain the methods used, the significance of the findings, and the validity of the evidence.

Forensic Software and Hardware /Analysis and Advanced Tools

Analysis and advanced tools are crucial components of digital forensics that help investigators extract, interpret, and make sense of the digital evidence gathered during an investigation. These tools and techniques are used to uncover hidden information, identify patterns, and draw conclusions from the data. Here's an overview of analysis techniques and some of the advanced tools used in digital forensics:

Analysis Techniques:

File System Analysis: This involves examining the structure and content of file systems on storage devices. File system analysis helps investigators identify files, directories, and metadata, as well as recover deleted or hidden data.

Keyword and String Searching: Investigators use keyword and string searching to locate specific terms, phrases, or patterns within digital evidence. This technique is valuable for finding relevant information in documents, emails, and other files.

Timeline Analysis: Creating timelines of events based on timestamp data is crucial in digital forensics. It helps reconstruct the sequence of actions and interactions on a system, which can be essential for understanding the progression of a case.

Link Analysis: Link analysis is used to visualize connections and relationships between various pieces of digital evidence. It can help identify communication patterns, networks, and associations among individuals or entities.

Data Carving: Data carving is the process of recovering files and fragments of data from unallocated space or from damaged or partially overwritten storage media. It can help retrieve deleted files or files with damaged file system records.

Registry Analysis: Analyzing the Windows registry can provide insights into system configuration, user activities, and application usage. It can reveal a wealth of information, including user accounts, installed software, and recent activity.

Network Traffic Analysis: In cases involving network-related incidents, such as cyberattacks, network traffic analysis helps trace the origin of attacks, identify malware, and understand the flow of data within a network.

Memory Forensics: Memory forensics involves analyzing the volatile memory (RAM) of a computer to identify running processes, open network connections, and malware. It is crucial for investigating live, active systems.

Malware Analysis: In cases involving malware, analysts reverse-engineer malicious code to understand its functionality, origin, and potential impact. This is essential for cybercrime investigations.

Advanced Tools:and software

Paraben Corporation

Paraben Corporation entered the cybersecurity marketplace in 1999, focused on digital forensics, risk assessment, and security solutions. Today, in a world with billions of devices, Paraben covers forensic investigations involving email, computers, smartphones, and Internet of Things (IoT) devices.

Key Differentiators

- The Paraben E3 Forensic Platform streamlines data from multiple sources.
- E3:Universal covers all devices, E3:DS is for mobile forensics, E3:P2C is for computer forensics, and E3:EMAIL for email.
- There are hash databases for filtering; viewers for files, hex, text, RTF, and emails; and automated embedded data detection (OLE).
- Paraben provides remote access with collection from machines and cloud storage.
- Paraben offers IoT support for brands like Xbox and Amazon Echo and cloud support for Google, Dropbox, and Slack.
- Users have the ability to work with multiple data sources together for analysis; can collect from a wide range of sources including computers, smartphones, IoT, and cloud to sort the data to logical categories; recover information; and search in multiple languages.
- Capabilities provided at a single price point with components such as cloud for computers and mobile are included.

Pricing: Monthly pricing is available for access to training courses, with a software license included. A free version is also available.

The Sleuth Kit And Autopsy

The Sleuth Kit (TSK) and Autopsy are popular open-source digital investigation tools. Sleuth Kit enables administrators to analyze file system data via a library of command-line tools for investigating disk images. Autopsy is its graphical user interface (GUI) and a digital forensics platform used in public and private computer system investigations to boost TSK's abilities.

Key Differentiators

- TSK offers well-regarded and reviewed disk and data capture tools.
- Capabilities include timeline analysis, hash filtering, file and folder flagging, and multimedia extraction.
- Autopsy allows users to efficiently analyze hard drives and smartphones.
- Its plug-in architecture allows users to find add-on modules or develop custom modules in Java or Python.
- Sleuth Kit is a collection of command-line tools and a C library to analyze disk images and recover files.
- Commercial training, support, and custom development is available from Basis Technology.
- The core functionality of TSK is to analyze volume and file system data.
- The library can be incorporated into larger digital forensics tools, and the command-line tools can be directly used to find evidence.
- TSK is used by law enforcement, military, and corporate examiners to investigate what happened on a computer.
- TSK can be used to recover photos from a camera's memory card.

Pricing: TSK and Autopsy are open source and free, but commercial support is available.

OpenText

Founded in 1991 in Waterloo, Ontario, OpenText offers enterprise content management, networking, automation, discovery, security, and analytics services. OpenText EnCase solutions include Endpoint Security (endpoint detection and response, or EDR), Endpoint Investigator (DFIR), Forensic, Mobile Investigator, and Advanced Detection. These solutions help with recovering of evidence from multiple device types and hard drives, automating the preparation of evidence, deep and triage analysis, and evidence collection and preservation.

Key Differentiators

- EnCase Forensic is court-proven in finding, decrypting, collecting, and preserving forensic data from a variety of devices, while ensuring evidence integrity and integrating with investigation workflows.
- EnCase can acquire evidence from a variety of sources and dig deep into each source to uncover potentially relevant information.
- Predefined or customized conditions and filters can quickly locate evidence.
- Evidence processing, integrated workflows, and flexible reporting are all features offered by EnCase.
- EnCase works across computers, laptops, and mobile devices to determine whether further investigation is warranted.
- The platform ranks evidence by importance.
- Real-time evaluation of evidence is provided.

Pricing: OpenText EnCase pricing is available upon request.

Magnet Forensics

Noticing that digital forensic tools used by law enforcement were insufficient, Canadian police officer Jad Saliba founded Magnet Forensics in 2011. The company offers digital forensic investigative tools to public and private organizations. Products include Magnet Axiom Cyber for incident response, Magnet Automate Enterprise, and Magnet Ignite for triage.

Key Differentiators

- Magnet Forensics now has more than 4,000 customers in over 100 countries.
- Magnet supports every digital evidence source, not just Linux and Windows OS.
- Magnet Axiom Cyber incident response is used to perform remote acquisitions and recover and analyze evidence from computers, the cloud, and mobile devices.
- Magnet Automate Enterprise is an automation solution used to simultaneously collect and process evidence from multiple endpoints in the wake of a security incident.
- Magnet Ignite performs fast, remote scans and initial analysis of endpoints as a triage action.
- Magnet Forensics performs remote acquisitions of Mac, Windows, and Linux endpoints, even when they aren't connected to company networks.
- Data can be recovered from apps such as Microsoft Office 365 and Slack as well as storage services like Amazon Web Services and Microsoft Azure.
- All evidence is brought into one location where security teams can analyze it.
- Evidence can simultaneously be recovered and processed from multiple endpoints.
- SIEM (security information and event management) and EDR tools are integrated into workflows and a digital investigation can automatically be triggered when a threat is detected.

Pricing: Magnet doesn't provide pricing, but free trials are available.

CAINE

The Computer-Aided Investigative Environment (CAINE) is an Italian open-source Ubuntu- and Linux-based distribution for digital forensic purposes. CAINE integrates with existing Windows, Linux, and Unix systems security tools.

Key Differentiators

- CAINE provides automatic extraction of timelines from RAM (random access memory).
- It is an interoperable environment that supports the digital investigator during the four phases of the digital investigation.
- All block devices are blocked in read-only mode.
- CAINE can be used with a GUI named Unblock, which is present on CAINE's desktop.
- CAINE assures that all disks are protected against accidental writing operations.
- If the user needs to write a disk, it can be unlocked.

Pricing: CAINE is open source and thus free.

Kroll Computer Forensics

Kroll’s computer forensics services and experts ensure that no digital evidence is overlooked and assist at any stage of an investigation or litigation, regardless of the number or location of data sources.

Key Differentiators

- Physical and digital evidence is examined to uncover what did or did not happen, using a combination of computer forensic expertise and traditional investigative techniques.
- Defensible methodologies and solutions are available to identify and preserve electronic data.
- Regardless of the volume and complexity of collection needs, Kroll gathers data for electronic investigation and forensic analysis or forensic discovery.
- Whether data was deleted or manipulated on purpose or by accident, Kroll analyzes the digital clues left behind to uncover critical information.
- Experts are available on call to serve as an expert witness or special master.

Pricing: Available upon request.

SANS SIFT

SIFT Workstation is a collection of free and open-source incident response and forensic tools to perform digital forensic examinations. Offering an array of free and open-source DFIR solutions, the SIFT Workstation provides various options for deployment including virtual machine (VM), native installation on Ubuntu, or installation on Windows via a Linux subsystem.

Key Differentiators

- Developed by the SANS Institute in 2007, SIFT works on 64-bit OS, automatically updates the software with the latest forensic tools and techniques, and is a memory optimizer.
- SIFT Workstation is continually updated and has over 125,000 downloads.
- SIFT Workstation is used as part of SANS Institute training on incident response, network forensics, and cyber threat intelligence.
- It can analyze file systems, network evidence, memory images, and more.
- Support is available for NTFS, ISO9660 CD, HFS, and FAT.
- SIFT Workstation has been upgraded to improve memory utilization.
- There is cross compatibility between Linux and Windows systems.

Pricing: Available for free from SANS.

Exterro

Hailing from Portland, Oregon, Exterro launched in 2004 and specialized in workflow-driven software and governance, risk, and compliance (GRC) solutions. While all of our picks inherently support organizations' needs to maintain compliance, Exterro is especially valuable to assist in-house legal teams, streamline compliance processes, and control risks.

Exterro offers products across e-discovery, privacy, risk management, and digital forensics. Known for its forensics-focused products dubbed FTK, its capabilities include Mac and mobile data investigations, remote agent endpoint collection, scalable DPE (data processing environment), and automated workflows.

Key Differentiators

- Exterro's operations are SOC 2 Type 2 certified and FedRAMP authorized.
- Products are split into FTK Imager, FTK Lab, FTK Central, FTK Enterprise, and FTK Connect (previously known as API-specific solutions).
- The overall Exterro FTK Forensic Toolkit has been used in digital forensics for over 30 years for repeatable, reliable investigations.
- All FTK solutions feature fast data processing, including for mobile data extractions.
- Exterro provides remote endpoint investigation, triage, collection, and remediation.
- Unlimited DPE scalability is available to meet heavy demand.
- Exterro requires minimal training.
- Exterro is a web-based, collaborative platform to centralize forensic evidence.
- Automation is available for workflow tasks and orchestration with SIEM and SOAR (security orchestration, automation, and response) platforms.
- Examiners can perform a rapid risk assessment of a suspected compromised endpoint — even if it is disconnected from the VPN network — by previewing the live contents of an off-network endpoint before performing a time-consuming collection.
- Integration with cybersecurity platforms, such as Palo Alto Cortex XSOAR, allows users to capture and preserve endpoint data immediately upon detection of a possible threat.
- No API (application programming interface) or Python scripting is required.

Pricing: FTK Imager is free; quote available upon request for other Exterro FTK solutions.

Volatility

Volatility is a command-line memory analysis and forensics tool for extracting artifacts from memory dumps. Volatility Workbench is free, open-source, and runs in Windows. This forensics framework for incident response and malware analysis is written in Python and supports Microsoft Windows, Mac OS X, and Linux.

Key Differentiators

- There is no need to install a Python script interpreter.
- Memory forensics technology enables investigators to analyze runtime states using RAM data.
- Knowledge of operating system (OS) internals, malicious code, and anomalies is used to enhance its tools.
- Embedded API can be used for lookups of PTE (page table entry) flags.
- Volatility has support for kernel address space layout randomization (KASLR).
- There is an automated execution of a failure command after multiple failed starts.
- In 2020, the Volatility Foundation released a complete rewrite of the framework known as Volatility 3 to address technical and performance challenges associated with the original code base released in 2007.

Pricing: The Volatility framework is free and open source.

X-Ways

X-Ways Forensics is a work environment for computer forensic examiners. Known for not being resource-hungry, yet speedy, it is based on the WinHex hex and disk editor and offers additional disk and data capture software, cloning, imaging, and other tools.

Key Differentiators

- X-Ways is portable and runs off of a USB stick on any given Windows system without installation if desired.
- X-Ways downloads and installs within seconds.
- Computer forensic examiners are enabled to share data and collaborate with investigators that use X-Ways Investigator.
- X-Ways runs under Windows XP/2003/Vista/2008/7/8/8.1/2012/10/2016/2019/11, 32-bit/64-bit, and standard/PE/FE.
- Automatic detection of lost or deleted partitions is made.
- Read partitioning is available for file system structures inside .dd image files.
- X-Ways provides analysis of remote computers.
- X-Ways can access disk and RAID configurations and detect NTFS (new technology file systems) and ADS (alternate data streams).
- There are templates to view and edit binary data.
- X-Ways offers built-in interpretation of JBOD, RAID 0, RAID 5, RAID 5EE, and RAID 6 systems, Linux software RAIDs, Windows dynamic disks, and LVM2.
- Native support is available for FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3, CDFS/ISO9660/Joliet, and UDF.

Pricing: X-Ways publishes its prices and claims a pricing advantage over competitors.

Cellebrite

Started in 1999 in Israel, Cellebrite specializes in mobile device forensics for law enforcement and enterprises that need to collect, review, analyze, or manage device data. The Digital Intelligence Investigative Platform helps unify the investigative life cycle and preserve digital evidence.

Key Differentiators

- Cellebrite Universal Forensic Extraction Device (UFED) can extract physical and logical data.
- Recovery methods include exclusive bootloaders, automatic EDL (emergency download) capability, and smart ADB (Android Debug Bridge).
- Cellebrite can provide analysis on Windows and Mac.
- Users can find internet history, downloads, recent searches, top sites, locations, media, messages, recycle bin, USB connections, and more.
- AI-assisted picture and video categorization, filtering, and support for whole disk encryption are available features.
- Cellebrite shows the timeline of an event and reveals the real story behind each case.

- Cellebrite is designed to scale and sift through large datasets.
- Cellebrite creates customized, court-ready reports.
- The platform exports findings easily.

Pricing: Available upon request.

ProDiscover

prodiscover®

COMPUTER FORENSICS

ProDiscover launched in 2001 to help public and private organizations solve digital crimes. As of 2021, the India-based provider works in over 70 countries with more than 400 clients, including the NIST, NASA, and Wells Fargo. ProDiscover Forensics captures evidence from computer systems for use in forensic investigation to collect, preserve, filter, and analyze evidence.

Key Differentiators

- ProDiscover offers three products that prioritize computer forensics, incident response, electronic discovery, and corporate policy compliance investigations.
- ProDiscover locates data on a computer disk as well as protecting evidence and creating reports.
- EXIF data can be extracted from JPEG files.
- Copies of suspicious disks can be made.
- Support is available for VMware to run captured images.
- ProDiscover supports Windows, Mac, and Linux file systems.
- Evidentiary reports can be prepared and presented in court.
- ProDiscover previews and images disks.
- Memory forensics is available.
- ProDiscover offers text search with multilingual capabilities.
- ProDiscover includes cloud, social media, Web, and email investigation.

Pricing: Available upon request.

Wireshark

First developed in 1998, Wireshark does forensic investigation and analysis of network packets and conducts testing and troubleshooting of networks. This includes inspection of hundreds of protocols in a three-pane packet browser that encapsulates data structures.

Key Differentiators

- Wireshark is multi-platform compatible, running on Windows, Linus, macOS, Solaris, FreeBSD, and NetBSD.
- Network analysis is available with VoIP (voice over Internet Protocol) analysis.
- Wireshark can capture files compressed with gzip and export outputs to XML, CSV, or plain text.
- Users can see what's happening on a network.
- Live capture and offline analysis are available.
- Captured network data can be browsed via a GUI, or via the teletypewriter (TTY)-mode TShark utility.
- Wireshark can read and write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer (compressed and uncompressed), Sniffer Pro, and NetXray, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, and WildPackets EtherPeek/TokenPeek/AiroPeek.
- Decryption support is available, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2.

Pricing: Wireshark is free and open source and boasts an active user community, but commercial training is also available.

Xplico

Created in 2007, Xplico is a network forensics analysis tool that restructures data via a packet sniffer. It specializes in port independent protocol identification (PIPI) to reconstruct application data to identify its protocols. Available as a free and open-source tool, Xplico's primary objective is to extract application data from an internet traffic capture.

Key Differentiators

- Xplico supports HTTP, IMAP, POP, SMTP, IPv6, and more.
- Xplico creates XML files that identify the flows and pcap (inputs file) contained in each data structure reassembled.
- Multithreading is possible.
- There are no data entry limits.
- Xplico can execute reserve DNS (Domain Name System) lookup from DNS pack.
- Xplico provides output data and information in SQLite database or Mysql database and/or files.
- All data reassembled by Xplico has an associated XML file that uniquely identifies it.
- Realtime elaboration.
- TCP (Transmission Control Protocol) reassembly with ACK (acknowledgement) verification is available for any packet or soft ACK verification.
- Reverse DNS lookup from DNS packages is contained in the input files, not from an external DNS server.

Pricing: Xplico is free and open source.

LogRhythm

LogRhythm is best known for SIEM, threat intelligence, and UEBA (user and entity behavior analytics). Started in 2003 out of Boulder, Colorado, the company includes network forensics via a feature known as NetMon, but the company has been refocusing its forensics efforts as part of its network detection and response (NDR) and endpoint monitoring solutions.

Key Differentiators

- LogRhythm aggregates packet capture and derived metadata, preserves the log data, and uses network forensic sensors to fill in the gaps.
- LogRhythm measures mean time to respond (MTTR).
- Dashboards are able to identify threats.
- LogRhythm offers application recognition of over 3,000 applications and metadata for visibility into network sessions.
- Script-based deep packet analytics (DPA) is available for real-time detection.
- LogRhythm provides session-based full packet capture.
- LogRhythm offers Layer 4–7 analysis with application ID.
- SmartCapture selective packet capture is available.
- Automation actions can obtain sessions through packet capture and future case analysis.

Pricing: Available upon request, but you may still be able to obtain NetMon Freemium.

Global Digital Forensic

Global Digital Forensics has been involved in computer forensic analysis and litigation support for over two decades. It offers a range of forensic services covering all digital devices. Founded in 1992, GDF also provides e-discovery services, penetration testing, and breach response services.

Key Differentiators

- Global Digital Forensics has its own labs as well as a global network of responders, allowing it to perform forensic analysis for virtually anything in any environment.
- GDF provides expert computer witness testimony in cases.
- Features include investigative tools for computers, email, mobile devices, social networks, and disk drives.
- Data retrieval and recovery services are available.
- GDF provides forensic readiness assessments.
- GPS and smartphone tracking, internet history analysis, image recovery and authentication, and chip-off analysis are available.
- GDF offers recovery of data from all devices, from mainframes to smartphones.
- Users can find evidence in log files and video.

Pricing: Available upon request.

Forensic Hardware:

Write Blockers: Write blockers are hardware devices that prevent any write operations to the storage media being investigated. They ensure the integrity of the evidence during the acquisition phase.

Digital Forensic Workstations: These specialized computers are configured with hardware components optimized for forensic analysis, such as multiple drive bays, large storage capacity, and powerful processors.

Hardware Imagers: Hardware imagers, like Tableau, provide efficient and reliable solutions for creating forensic copies of storage media. They often support various interfaces (e.g., SATA, IDE, USB) and provide hash verification.

Mobile Device Forensic Tools: Mobile device acquisition and analysis hardware, such as Cellebrite's Physical Analyzer and XRY, are used to connect, extract, and analyze data from mobile devices.

Network Packet Capture Tools: Tools like Network TAPs and capture cards are used for capturing network traffic in a forensically sound manner.

Write-Once Media: These are specialized optical or solid-state storage media that can be written to once and then become read-only, ensuring the preservation of digital evidence without alteration.

Portable Forensic Kits: Compact, all-in-one forensic kits, such as the Digital Intelligence UltraBlock UFED Field Kits, are designed for field deployments and offer both hardware and software components.

Hardware Cryptocurrency Wallets: In cases involving digital currency investigations, specialized hardware wallets like Ledger and Trezor may be used to secure and access cryptocurrency holdings for analysis.

SIM Card Readers: These devices are used to extract data from SIM cards, which can contain valuable information in mobile device investigations.

Forensic Accessories: Various accessories like evidence bags, tamper-evident seals, Faraday bags, and anti-static tools are essential for proper handling and storage of digital evidence.

Forensic Technology and Practices

Forensic technology and practices encompass a wide range of tools, techniques, and methodologies used by forensic professionals to investigate and analyze evidence in various fields, including law enforcement, cybersecurity, civil litigation, and more. These technologies and practices are crucial for uncovering the truth, solving crimes, and ensuring justice. Here's an overview of key forensic technology and practices:

1. Digital Forensics:

Computer Forensics: The examination of computer systems and digital devices to recover, analyze, and preserve electronic evidence.

Mobile Device Forensics: The specialization focused on extracting and analyzing data from smartphones, tablets, and other portable devices.

Network Forensics: The analysis of network traffic, logs, and packets to investigate cybercrimes and security incidents.

2. DNA Analysis:

DNA Sequencing: The process of determining the order of nucleotides in a DNA molecule, which is used for identifying individuals and solving crimes.

DNA Databases: Databases containing DNA profiles from individuals, aiding in the identification of suspects and victims.

3. Fingerprint Analysis:

Automated Fingerprint Identification Systems (AFIS): Computerized systems for comparing and matching fingerprints in criminal investigations.

Latent Print Analysis: The examination of latent (hidden) fingerprints at crime scenes to identify suspects.

4. Ballistics and Firearms Analysis:

Firearm and Toolmark Examination: The study of fired bullets, cartridge cases, and firearms to link them to specific firearms or connect them to crime scenes.

Gunshot Residue (GSR) Analysis: The examination of particles and residues produced by the discharge of firearms.

5. Forensic Anthropology:

Identification of Human Remains: The analysis of human skeletal remains to determine the identity of individuals, including age, sex, ancestry, and cause of death.

6. Document Examination:

Handwriting Analysis: The study of handwriting and signature characteristics to determine authenticity.

Document Authenticity: The examination of documents, including ink, paper, and printing methods, to establish their authenticity in legal cases.

7. Trace Evidence Analysis:

Fiber Analysis: The examination of clothing fibers, textiles, and materials found at crime scenes.

Hair Analysis: The examination of human and animal hair for identification and forensic significance.

8. Toxicology:

Chemical Analysis: The examination of biological samples to detect the presence of drugs, alcohol, and other toxic substances.

Postmortem Toxicology: Analyzing body fluids and tissues in deceased individuals to determine the cause of death.

9. Crime Scene Investigation:

Evidence Collection: The proper and systematic collection, documentation, and preservation of physical evidence from crime scenes.

Crime Scene Reconstruction: The process of piecing together evidence and events to reconstruct the sequence of events leading to a crime.

10. Ballistic Imaging:

Firearm and Toolmark Databases: Storing digital images of bullets, cartridge cases, and toolmarks to compare them with evidence from crime scenes.

11. Video and Audio Analysis:

Video Forensics: The examination of digital video evidence, including enhancing video quality and authenticating footage.

Audio Forensics: The analysis of audio recordings to determine their authenticity and content.

12. Facial Recognition:

Facial Recognition Software: Advanced software for identifying individuals based on facial features, used in surveillance and criminal investigations.

13. Cryptocurrency Forensics:

Blockchain Analysis: The examination of cryptocurrency transactions and addresses to trace illicit financial activities, such as money laundering and cybercrime.

Forensic technology and practices continue to evolve with advancements in science, computing, and data analysis. These tools and methodologies are vital for solving complex cases, ensuring the integrity of evidence, and supporting the legal system in the pursuit

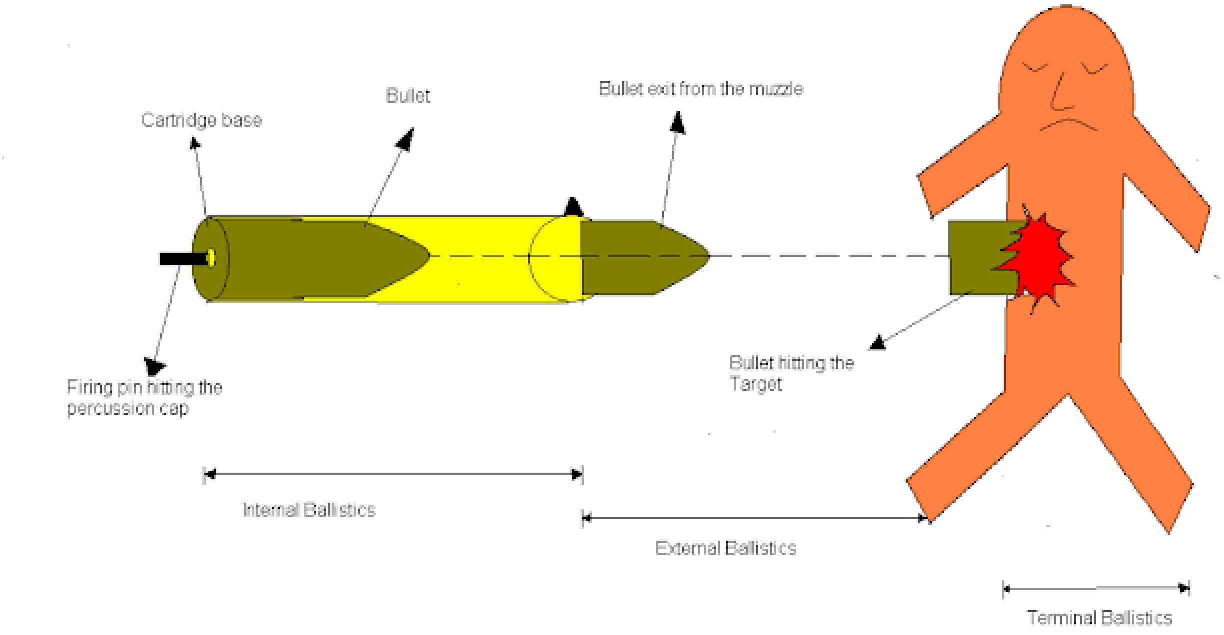
of justice. Proper training and adherence to ethical and legal standards are essential for the successful application of forensic practices.

Forensic Ballistics and Photography

Ballistics:

The term ballistics refers to the science of study of the action, motion and behaviour of a projectile during its flight in any given medium. The flight path of a bullet includes:

•Travel down the barrel **(Internal Ballistics),**
•Path through the air **(External Ballistics),** and
•Path through a target **(Terminal Ballistics)**


Cartridge base
Bullet
Bullet exit from the muzzle
Firing pin hitting the percussion cap
Bullet hitting the Target
Internal Ballistics
External Ballistics
Terminal Ballistics

Forensic Ballistics:

Is that branch of forensic science which deals with the examination of the firearm and related evidences encountered at the scene of crime in a shooting incident, and their linkage to the firearm, and Identification of the shooter.

A ballistic expert need to answer the following questions:

1.Type of The Firearms used
2.Identification of the Firearm
3.Individual Characteristics of Firearm
4.Range of Firing
5.Direction of Firing
6.Identification of the Shooter
7.Medico legal aspects: - Suicide/Homicide/Accident

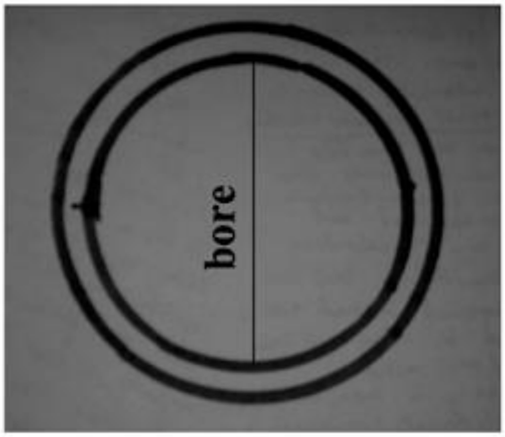
FIREARM

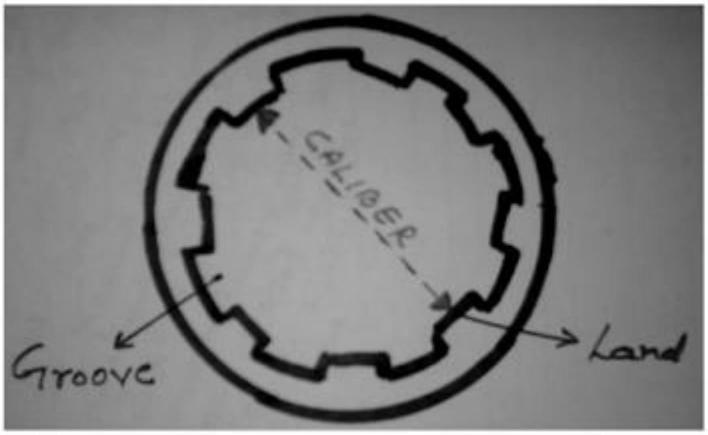
Any instrument which is designed or adapted to discharge a projectile or hurl a projectile with the help of force applied by the expanded gases of main charge (propellant). Firearms can be smooth bore, rifled bore, manual/semi-automatic/automatic, handguns, shoulder guns etc.

SMOOTH BORE: -

A gun with a smoothbore (uniform smooth) that shoots cartridges that contain "shot" or small metal pellets (of lead or steel) as the projectiles. The internal diameter of the smooth bore gun is smooth and have no grooving inside the barrel.

For Example: - Shot guns and country made firearms

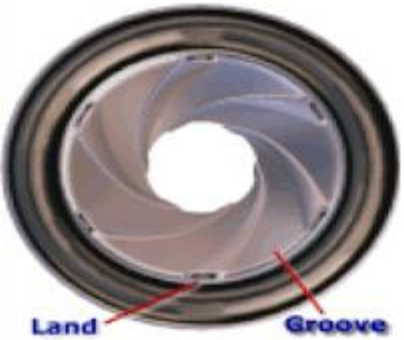




RIFLED BORE: -

These contain rifling (grooving) in their barrel. The spiral grooves cut inside a gun barrel that give the bullet a spinning motion. The metal between the grooves is called a "land".

For Example : - Rifles, Revolver, Pistols, Machine Guns etc.



Rifling provides a steady uniform and gyratory (spinning) motion to the projectile during flight. The gyratory motion has two important effects on the bullet :

- It stabilizes the bullet flight with nose on position
- Increases the effective range of firing
- It decreases the air resistance.

Ammunition (Cartridges)

Cartridge= Primer + Main Charge + Projectile + Cartridge Case

An Ammunition is the assembly of primary charge (also known as primer/initiator or detonator, usually high explosives), the main charge (also known as the gun powder or propellant), the projectile (may be in the form of shots/pellets or single bullet), and the case or shell.

IDENTIFICATION & INDIVIDUALIZATION OF FIREARM

Basic Principle: -

No two firearms, even those of the same make and model, will produce the same unique marks on fired bullets and cartridge cases. Manufacturing processes, use, and abuse leave surface characteristics within the firearm that cannot be exactly reproduced in other firearms.

All cases that involve firearms identification start with preliminary examinations of the evidence for similar ***class characteristics*** and different ***Individual Characteristics.***

Class characteristics can be defined as:

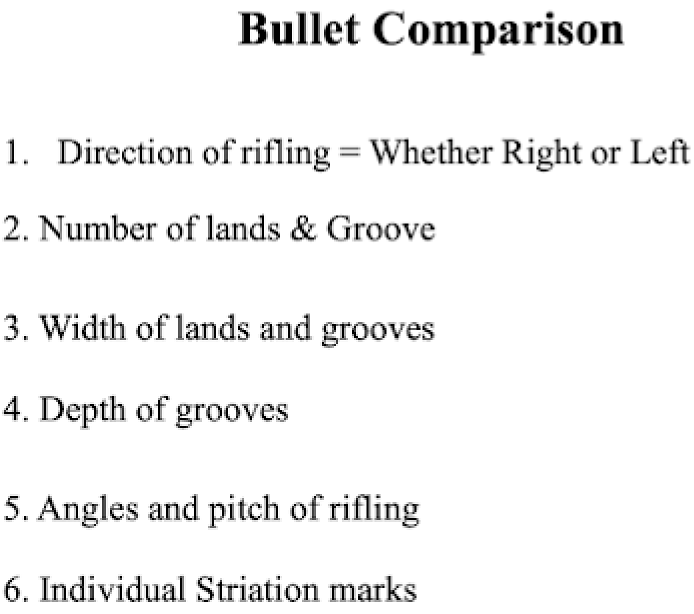
Intentional or design characteristics that would be common to a particular group or family of items.

The class characteristics of firearms that relate to the bullets fired from them includes the ***caliber*** of the firearm and the ***rifling*** pattern contained in the barrel of the firearm.

Cartridges and Cartridge cases on the other hand are examined for class similarities in what are called ***breech marks***, ***firing pin impressions***, ***extractor marks***, ***ejector marks*** and others.

Individual characteristics can be defined as:

marks produced by the random imperfections or irregularities of tool surfaces. These random imperfections or irregularities are produced incidental to manufacture and/or caused by use, corrosion, or damage. They are unique to that tool and distinguish it from all other tools.



Bullet Comparison

1. Direction of rifling = Whether Right or Left
2. Number of lands & Groove
3. Width of lands and grooves
4. Depth of grooves
5. Angles and pitch of rifling
6. Individual Striation marks

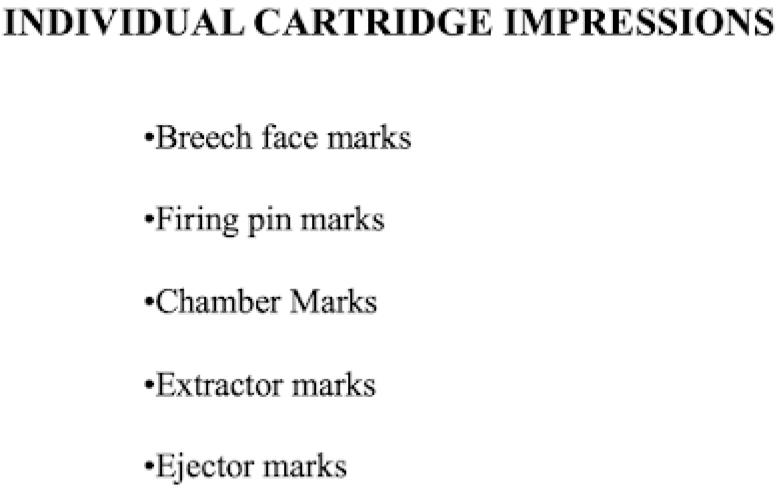
Cartridge Case Examination & Comparison

Class Characteristics: -

Identification number
Manufacturer Marks
Weight
Diameter
Base design
Length of bearing surface
Color
Shape

Cartridge base

Cartridge Surface



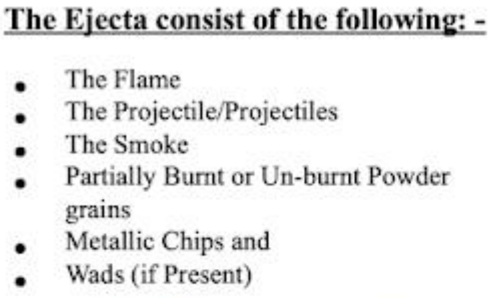
INDIVIDUAL CARTRIDGE IMPRESSIONS

- Breech face marks
- Firing pin marks
- Chamber Marks
- Extractor marks
- Ejector marks

RANGE OF FIRING (Distance of Firing)

Estimation of Range of firing totally depends upon the deposition of the Gun Shot Residue (GSR) over the wound.

The projectile comes out from the muzzle along with the EJECTA



<u>The Ejecta consist of the following: -</u>

- The Flame
- The Projectile/Projectiles
- The Smoke
- Partially Burnt or Un-burnt Powder grains
- Metallic Chips and
- Wads (if Present)

Each Ejecta particle (flame, smoke etc) is a having a certain distance of traveling from the muzzle which depends upon the following: -

- **Nature of Firearm (Smooth bored/ Rifled bore)**
- **Nature of Ammunition (Black Powder/Semi smokeless Powder/Smokeless Powder)**
- **Nature of the Target**
- **Caliber of the Firearm**

- **Length of the Barrel**

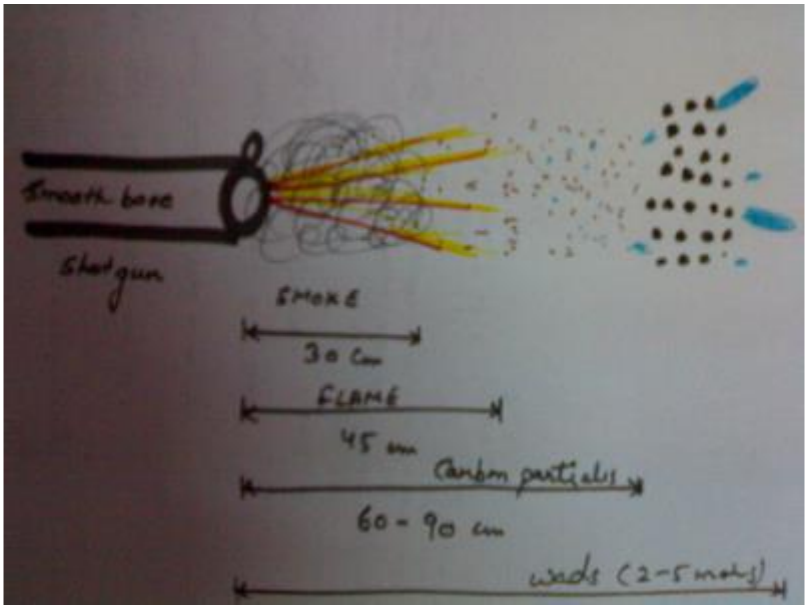
But as an average for the Standard Firearm the approximate distance for different ejecta particle is as follows: -

In case of Shotguns: -

- Smoke travels up to a distance of 30 cm
- Flame up to 45 cm
- Partially burnt & un-burnt particles up to a distance of 60-90 cm
- Wads up to 2-5 meters
- Shots are dispersed according to distance

In case of rifled weapons:-

- Smoke up to 30 cm
- Flame up to 8 cm
- Powder grains & metallic chips up to 60-90 cm



Each and every ejecta particle is responsible for different phenomena over the gun shot wound (firearm injury) as follows: -

- Smoke produces Blackening or Smudging over the wound

- Flame is responsible for Burning of Skin, Scorching and Singeing of hairs

- Partially burnt or un burnt powder grains are responsible for Tattooing

- The projectile is responsible for the collaring (contusion collar/Grease collar/abrasion collar)

Forensic photography

Forensic photography may refer to the visual documentation of different aspects that can be found at a crime scene. It may include the documentation of the crime scene, or physical evidence that is either found at a crime scene or already processed in a laboratory. Forensic photography differs from other variations of photography because crime scene photographers usually have a very specific purpose for capturing each image.[1] As a result, the quality of forensic documentation may determine the result of an investigation, in that with the absence of good documentation, investigators may find it impossible to conclude what did or did not happen

Crime scenes can be major sources of physical evidence that is used to associate or link suspects to scenes, victims to scenes, and suspects to victims. Locard's exchange principle is a major concept that helps determine these relationships of evidence. It is the basic tenet of why crime scenes should be investigated. Anything found at a crime scene can be used as physical evidence as long as it is relevant to the case, which is why the documentation of a crime scene and physical evidence in its true form is key for the interpretation of the investigation.

Knowing that crucial information for an investigation can be found at a crime scene, forensic photography is a form of documentationthat is essential for retaining the quality of discovered physical evidence. Such physical evidence to be documented includes those found at the crime scene, in the laboratory, or for the identification of suspects.

All forensic photography must consider three elements at a crime scene: the subject, the scale, and a reference object. Also, the overall forensic photographs must be shown as a neutral and accurate representation.[1]

Features of forensic photography

Common types of photography such as creative and artistic photography give a different purpose than forensic photography.

Crime scene photography allows us to capture essential aspects of the presented from the crime scene, including its scope, the focal points of the scene, and any physical or material evidence found at or from a result of it.[1] With the use of crime scene photography, the context of the crime scene can be represented through a series of photographs; aiming to tell the whole story. Such photographs are used to capture the physical environment of the scene and its surroundings, in addition to physical evidence *in situ* and key areas of the crime scene (e.g., entrances and exits). Moreover, these photographs may be taken at various ranges depending on the content that is being captured. For example, physical evidence (e.g., footprints, wound details, trace evidence, etc.) may require close-up images, whereas the conditions of a room may only require overall and/or midrange photography. Photographs may also be supported with video recordings.

Evidence photography

This form of photography is to provide images of the varying types of physical evidence and used as evidence in court, part of the case record, or by other investigators; typically of forensic findings during the analysis of various forensic disciplines. Forensic laboratories generally use infrared, ultraviolet (UV), x-ray, or laser radiation in addition to cameras and microscopes, to represent details that would otherwise be invisible to the naked eye. However, it is crucial that such details do not interfere with the appearance and condition of the evidence being documented.

To ensure quality photographs, general evidence is documented under the following conditions:

1. The evidence is placed on a clean and distraction-free background (i.e., background paper, butcher paper, neutral countertop, etc.).
2. Even illumination. This can be achieved with two light sources of equal power and distance, placed approximately 45 degrees toward the evidence.
3. The camera should be placed directly overhead of the evidence. A ladder or scaffolding may be required for larger items.
4. Case number and scale present in all photographs.
5. All sides of the evidence photographed
6. Close-up photographs of relevant details found on the evidence.

Impression photography

Photographs of impressions such as fingerprints, footwear impressions, and tool marks require certain standards as they may be analyzed, compared, and searched through a large digital databases. For example, fingerprints are often entered into the Automated Fingerprint Identification System (AFIS). To meet the standards for such material evidence, they must:

1. Fill the frame with the impression to take advantage of the camera's resolution;
2. Include a scale for accurate calibration;
3. Have parallel planes of the subject, scale, and image;
4. Be in sharp focus and exposed correctly; and
5. Have even illumination of the area of interest.

In addition, it is suggested that these impression images be recorded in camera RAW, although the photographer may decide to edit via Photoshop or another editing software. That will create a TIFF image, but increase the quality of the image.[1]

Mug shots

Mug shots are taken for individuals who have been charged with a crime, and once one is created, it is automatically entered into a master database with any existing information on that individual. To maintain consistent quality, standardized lighting, background, and distance is required.[1] In addition to associating file information, physical features (e.g., hair and eye colour, facial hair, tattoos, etc.) are also associated and an appropriate photo line-up is required.

Methods

Photograph of a paper fragment with a ruler for scale

All forensic photographs must contain three elements: the subject, a scale, and a reference object. Crime scene photographs should always be in focus, with the subject of the photograph as the main object of the scene. There should always be a scale or ruler present. This will allow investigators the ability to resize the image to accurately reconstruct the scene. The overall photographs must be a fair and accurate representation of what is seen. Any change in color may misidentify an object for investigators and possibly jurors.

Preliminary overall photographs should attempt to capture the locations of evidence and identifying features of the scene, such as addresses, vehicle identification numbers and serial numbers, footwear/tire mark impressions, and the conditions of the scene. While the purpose of the overall photograph is to document the conditions of the scene and the relationship of objects, the medium range photograph serves to document the appearance of an object.

In all photographs, a scale must be included, as well as a marker to indicate the identity of the object in question. Again, objects in medium-range photographs must be a fair and accurate representation of what is seen. Adjusting the photographic principles or lighting may allow the photographer to achieve this goal.

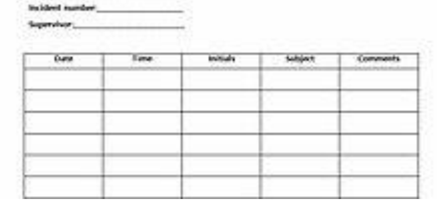
Accuracy

If any evidentiary photographs are to be taken for use in a critical comparison examination at a later time, guidelines must be followed in accordance with the best practices of digital evidence.

1. The digital image must be captured in a lossless compression format. The two widely accepted lossless compression formats are tagged image file format (TIFF) and RAW. TIFF is a universal file type, whereas RAW files are proprietary based upon the manufacturer of the camera. Specialized software may be required to open and enhance a RAW image.
2. The camera must be on a grounded platform, such as a copy stand or tripod' In general, the human body cannot stop natural vibrations with a camera shutter speed slower than 1/60 of a second. Using a grounded platform will allow the subject matter to be in complete focus.
3. The camera shutter must be controlled by a remote cord or by using the timer mode. The simple action of depressing the shutter control will cause the camera to vibrate, losing focus on the subject matter.

Photographers must also understand the principles of photography. When the photographers take the photographs itself, they must consider three components. These three components are ISO, shutter speed and aperture.

Documentation


Photograph Log

Date:____________________

Location:__________________

Incident number:______________

Supervisor:_________________

Date	Time	Initials	Subject	Comments

Example of a photo log

The responding officer must also maintain a photo log if any photographic documentation is taken. The log should contain the date and time of the photograph, the subject matter, and any additional notes. These logs must be maintained within a case file or incident report, as they are a part of the examination record and discoverable material at trial.

Use of flash**[edit]**

External flash units are helpful tools when responding to a crime scene and for the proper documentation of evidence. The white balance of a photo flash unit is set to mimic daylight to ensure the proper color balance of the subject matter. The photographer must be mindful of the reflections that can occur due to the directionality of the flash and the position of the subject matter. To avoid flash reflections, the flash must either be removed from the camera body, creating an angle, or bounced off the ceiling.

Equipment

The tools required to properly document the crime scene include:

- Notepad
- Clipboard and/or digital tablet device
- Graph paper
- Writing instruments (pens, pencils, markers)
- Still camera with external flash and extra batteries
- Video camera
- Tripod
- Measurement instruments (tape measures, rulers, electronic measuring devices, perspective grids, etc.)
- Evidence identification and position markers or placards
- Photographic log
- colored cones

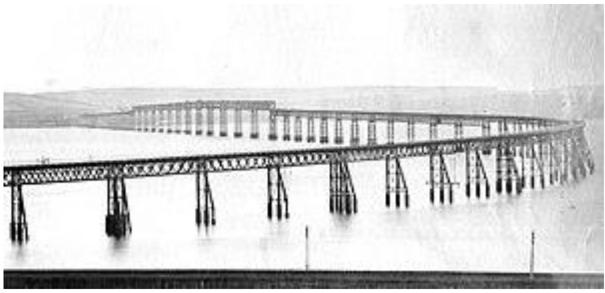
Fit for court

The images must be clear and usually have scales. They serve to not only remind investigators of the scene, but also to provide a tangible image for the court to better enable them to understand what happened. The use of several views taken from different angles helps to minimize the problem of parallax. Overall images do not have scales and serve to show the general layout, such as the house where the murder is thought to have occurred. Context images show evidence in context, like how the knife was next to the sofa. Close up images show fine detail of an artifact, such as a bloody fingerprint on the knife.

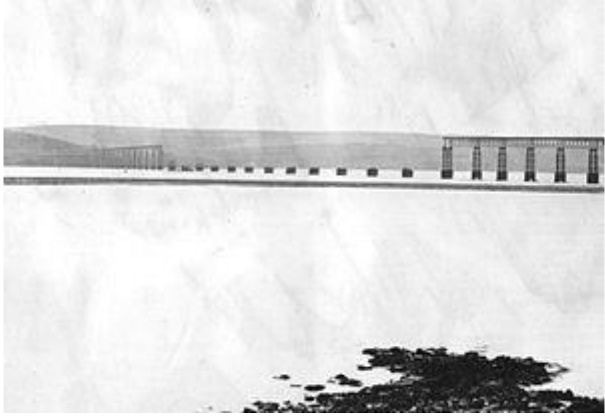
Road traffic incident (RTI) photographs show the overall layout at the scene taken from many different angles, with close-ups of significant damage, or trace evidence such as tire marks at a traffic collision. As with crime scene photography, it is essential that the site is pristine and untouched as far as is possible. Some essential intervention, such as rescuing a trapped victim, must be recorded in the notes made at the time by the photographer, so that the authenticity of the photographs can be verified.

As with all evidence a chain of custody must be maintained for crime scene photographs. Sometimes a CSI (forensic photographer) will process his/her own film or there is a specific lab for it. Regardless of how it is done any person who handles the evidence must be recorded. Secure Digital Forensic Imaging methods may be applied to help ensure against tampering and improper disclosure. Accident scene pictures should also be identified and sourced, police photographs taken at the scene often being used in civil cases.

Analysis of historic photographs



Original Tay Bridge from the north



Photograph of 1880 showing fallen Tay Bridge

Crime or accident scene photographs can often be re-analyzed in cold cases or when the images need to be enlarged to show critical details. Photographs made by film exposure usually contain much information which may be crucial long after the photograph was taken. They can readily be digitized by scanning, and then enlarged to show the detail needed for new analysis. For example, controversy has raged for a number of years over the cause of the Tay Bridge disaster of 1879 when a half-mile section of the new bridge collapsed in a storm, taking an express train down into the estuary of the river Tay. At least 75 passengers and crew were killed in the disaster.

The set of photographs taken a few days after the accident have been re-analyzed in 1999–2000 by digitalizing them and enlarging the files to show critical details. The originals were of very high resolution since a large plate camera was used with a small aperture, plus a fine-grain film. The re-analyzed pictures shed new light on why the bridge fell, suggesting that design flaws and defects in the cast iron columns which supported the centre section led directly to the catastrophic failure. Alternative explanations that the bridge was blown down by the wind during the storm that night, or that the train derailed and hit the girders are unlikely. The re-analysis supports the original court of inquiry conclusions, which stated that the bridge was "badly designed, badly built and badly maintained".

Face, Iris and Fingerprint Recognition and Audio Video Analysis.

Face, iris, and fingerprint recognition, along with audio and video analysis, are critical technologies in the field of biometrics and forensics. They are used for identifying individuals and analyzing digital media, contributing to various applications, from law enforcement and security to access control and surveillance. Here's an overview of each of these technologies:

1. Face Recognition:

Definition: Face recognition, or facial recognition, is a biometric technology that identifies individuals by analyzing the unique patterns, features, and characteristics of their faces.

Applications: Face recognition is used in security systems, access control, law enforcement, and border control. It can also be employed for identity verification in smartphones, social media tagging, and facial authentication.

2. Iris Recognition:

Definition: Iris recognition is a biometric technique that identifies individuals by analyzing the patterns in the colored part of the eye (the iris).

Applications: Iris recognition is used in access control systems, national ID programs, and airport security. It is known for its accuracy and resistance to fraud.

3. Fingerprint Recognition:

Definition: Fingerprint recognition is the oldest and most widely used biometric method. It identifies individuals based on the unique patterns of ridges, loops, and whorls on their fingertips.

Applications: Fingerprint recognition is used in law enforcement, border control, smartphone and laptop security, and access control systems. It is a widely accepted method for identification.

4. Audio Analysis:

Definition: Audio analysis involves the examination of sound recordings, voiceprints, and other acoustic features to determine the identity of a speaker, the content of the audio, or to analyze background noises and environmental factors.

Applications: Audio analysis is used in forensic investigations, voice recognition for access control, and content analysis for various purposes, including sentiment analysis and transcription.

5. Video Analysis:

Definition: Video analysis encompasses the examination of video footage, which includes video enhancement, object tracking, facial recognition within video streams, and the interpretation of events captured on video.

Applications: Video analysis is critical in surveillance and security systems, as well as in forensic investigations, traffic management, and social media content analysis.

6. Video Forensics:

Definition: Video forensics is a specialized area of video analysis that focuses on the authentication, enhancement, and analysis of video evidence for legal purposes.

Applications: Video forensics is used to analyze and present video evidence in criminal investigations, court proceedings, and incident reconstructions.

These technologies are often integrated into broader biometric systems or digital forensic toolkits. They offer valuable means of identifying individuals, enhancing security, and analyzing digital media for various purposes, from preventing unauthorized access to solving crimes and improving surveillance systems. Additionally, advancements in artificial intelligence and machine learning have further improved the accuracy and capabilities of these technologies.