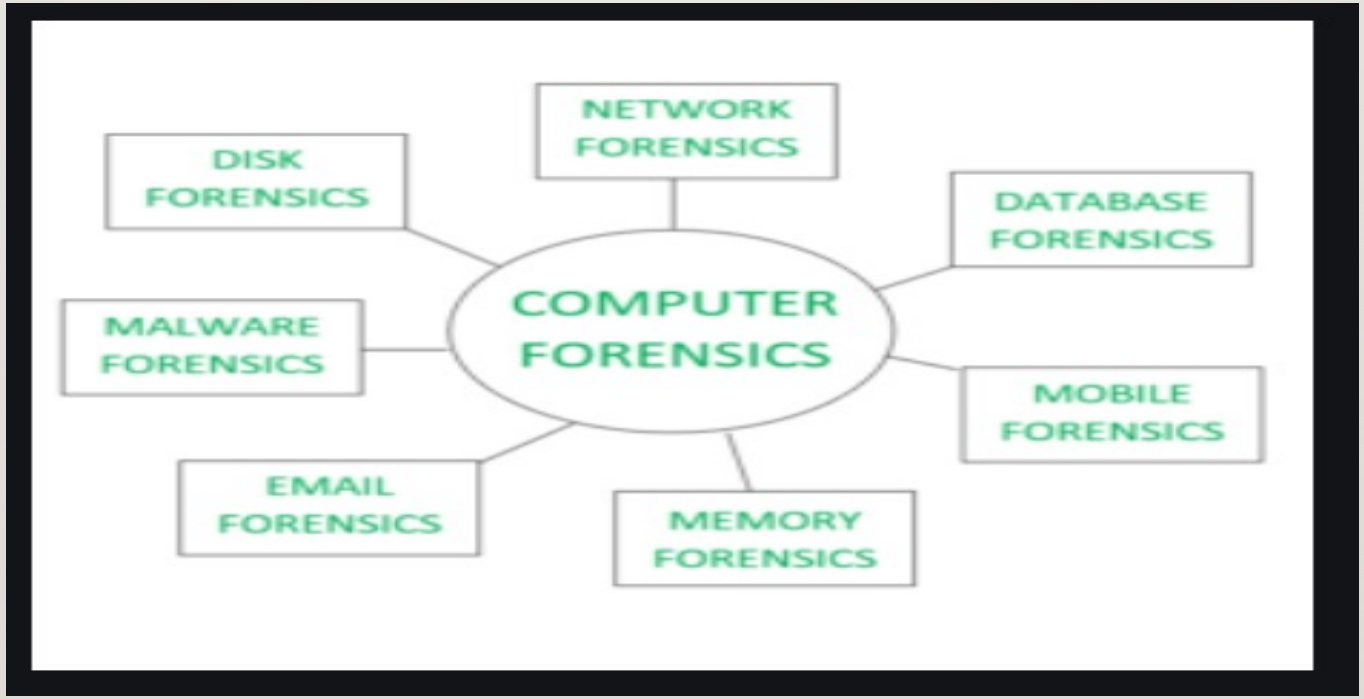
COMPUTER FORENSICS

- Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it

TYPES

- 
NETWORK FORENSICS
DISK FORENSICS
DATABASE FORENSICS
COMPUTER FORENSICS
MALWARE FORENSICS
MOBILE FORENSICS
EMAIL FORENSICS
MEMORY FORENSICS

- Disk Forensics: It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
- Network Forensics: It is a sub-branch of Computer Forensics that involves monitoring and analyzing the computer network traffic.
- Database Forensics: It deals with the study and examination of databases and their related metadata.
- Malware Forensics: It deals with the identification of suspicious code and studying viruses, worms, etc.

- Email Forensics: It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
- Memory Forensics: Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analyzing it for further investigation.
- Mobile Phone Forensics: It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it.

CHARACTERISTICS

- Identification: Identifying what evidence is present, where it is stored, and how it is stored (in which format). Electronic devices can be personal computers, Mobile phones, PDAs, etc.
- Preservation: Data is isolated, secured, and preserved. It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.
- Analysis: Forensic lab personnel reconstruct fragments of data and draw conclusions based on evidence.
- Documentation: A record of all the visible data is created. It helps in recreating and reviewing the crime scene. All the findings from the investigations are documented.
- Presentation: All the documented findings are produced in a court of law for further investigations.

PROCEDURE:

- The procedure starts with identifying the devices used and collecting the preliminary evidence on the crime scene. Then the court warrant is obtained for the seizure of the evidence which leads to the seizure of the evidence. The evidence are then transported to the forensics lab for further investigations and the procedure of transportation of the evidence from the crime scene to labs are called chain of custody. The evidence are then copied for analysis and the original evidence is kept safe because analysis are always done on the copied evidence and not the original evidence.

- The analysis is then done on the copied evidence for suspicious activities and accordingly, the findings are documented in a nontechnical tone. The documented findings are then presented in a court of law for further investigations.

TOOLS FOR LAPTOP OR PC

- COFFEE – A suite of tools for Windows developed by Microsoft.
- The Coroner's Toolkit – A suite of programs for Unix analysis.
- The Sleuth Kit – A library of tools for both Unix and Windows.

TOOLS FOR MEMORY

- Volatility
- WindowsSCOPE
- Tools for Mobile Device :
- MicroSystemation XRY/XACT

APPLICATIONS

- Intellectual Property theft
- Employment disputes
- Fraud investigations
- Misuse of the Internet and email in the workplace
- Bankruptcy investigations

ADVANTAGES OF COMPUTER FORENSICS

- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies gather important information on their computer systems or networks potentially being compromised.
- Efficiently tracks down cyber criminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

DISADVANTAGES OF COMPUTER FORENSICS

- Before the digital evidence is accepted into court it must be proved that it is not tampered with.
- Producing and keeping electronic records safe is expensive.
- Legal practitioners must have extensive computer knowledge.
- Need to produce authentic and convincing evidence.
- If the tool used for digital forensics is not according to specified standards, then in a court of law, the evidence can be disapproved by justice.
- A lack of technical knowledge by the investigating officer might not offer the desired result.

COMPUTER FORENSICS FUNDAMENTALS

1. Protect the suspected digital media during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.
2. Discover all files on the suspected digital media. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.
3. Recover all (or as much as possible of) discovered deleted files.
4. Reveal (to the greatest extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.
5. Access (if possible and legally appropriate) the contents of protected or encrypted files.
6. Analyze all possibly relevant data found in special (and typically inaccessible) areas of a disk.

BENEFITS OF FORENSICS

- **It protects and safeguards the integrity of the system.** Digital forensics teams use sophisticated and effective measures to protect and safeguard computer systems and networks from hackers, cybercriminals, and other malicious elements.
- **It collects substantial evidence.** Digital forensics teams use standardized procedures and steps to ensure the evidence gathered is sound and viable to prosecute criminals in the court of law.

- **It's useful for data recovery.** Companies and organizations can use forensics to effectively and efficiently recover sensitive and confidential data if attackers and cybercriminals have compromised their systems and networks.
- **It protects data and saves money.** Digital forensics protects important and sensitive data by employing strong cyber security measures and protects the companies from any ransomware attacks, saving precious resources like time and money.
- **It helps facilitate investigations.** The forensics department helps investigative agencies apprehend criminals or suspects by providing them with legally sound, fact-based evidence that is valid and viable in a courtroom to prosecute perpetrators.

CHALLENGES OF DIGITAL FORENSICS

- **Proving the integrity of the evidence.** The courtroom accepts electronic and digital evidence provided by the prosecuting agencies if the forensics professionals recovered and gathered it in an ethical and legal manner.
- **It's not cost-effective.** Digital forensics is an effective manner of gathering and storing evidence, but it costs a lot of money to store and gather electronic and digital evidence.
- **It requires extensive knowledge.** To successfully use digital and electronic evidence against the accused personnel, it's essential that the lawyers have extensive knowledge and expertise about digital forensics and its intricacies.
- **Provide substantial evidence.** Any digital evidence provided by the prosecution is concrete, factual and substantial because it's very simple to falsify digital evidence or tamper with it.
- **Follow and maintain standardized procedures.** If the forensics department obtains the evidence produced in the courtroom through unethical ways and not under the standard procedure, the court may disregard the evidence.

APPLICATIONS OF DIGITAL FORENSICS

- Facilitates investigations by government and law enforcement agencies
- Creates safety measures to counteract any cyber attacks and ransomware attacks
- Provides security to companies and organizations to help ensure that no sensitive data or confidential information is being leaked out of the organization
- Prevents thefts of intellectual property or breach of intellectual property rights
- Helps perform successful investigations into fraudulent accusations
- Monitors a company employees' activities on the internet to ensure that data isn't being used for malicious purposes

COMPUTER CRIMES AND COMPUTER FORENSICS

- Cybercrime refers to criminal conduct committed with the aid of a computer or other electronic equipment connected to the internet. Individuals or small groups of people with little technical knowledge and highly organized worldwide criminal groups with relatively talented developers and specialists can engage in cybercrime

- Cybercriminal is who want to generate money, commit a majority of cybercrimes. Individuals and organizations are both involved in cybercrime. Aside from that, cybercriminals might utilize computers or networks to send viruses, malware, pornographic material, and other unlawful data.

- To make money, cybercriminals engage in a range of profit-driven criminal acts, including stealing and reselling identities, gaining access to financial accounts, and fraudulently utilizing credit cards to obtain funds.

EXAMPLES OF BASIC CYBERCRIMES

- Stolen credit card information: The most common cybercrime is when a person's credit card information is stolen and used unlawfully to acquire or purchase goods or services over the internet.
- Hacking into a government website: Another type of cybercrime is tampering with sensitive government data.
- Theft of user accounts: Yahoo experienced a serious data breach from 2013 to 2016 that resulted in the theft of three billion user accounts. The attackers gained access to private information and passwords that were used to access user accounts in other online services. Most of this data is available even today on the dark web.
- Compromised IoT devices: In 2016, over one million connected devices in the IoT were compromised by attackers who took advantage of existing software vulnerabilities. It is the largest DDoS attack to date
- Loss of control and access to content: The WannaCry attack, which was allegedly launched by North Korea, in 2017, unleashed ransomware that locked down content on user devices.

- Phishing campaigns: The phishing campaigns infiltrate corporate networks by sending authentic-looking fraudulent emails to users in an organization and tricking them into performing actions such as downloading attachments or clicking on links. The viruses or malware then spreads to the systems, and, eventually, ends up in the organizations' networks.
- Some other common examples of cybercrimes include the sale of illegal items, such as drugs, arms, or counterfeit goods, illegal gambling, solicitation, production, distribution, or possession of child pornography, etc.

CLASSIFICATION OF CYBERCRIMES

1. **Individual:** It is a cybercrime that entails a single individual disseminating malicious or unlawful material via the internet. For example, distributing pornography, human trafficking, and online stalking.
2. **Property:** This cybercrime involves obtaining access to individuals' bank or credit card information, accessing their funds, making online transactions, or executing phishing schemes to persuade individuals to give away personal information.
3. **Government:** While these cybercrimes are uncommon, they are nevertheless considered significant offenses. It entails breaking into government databases and hacking official websites.

WHAT ARE THE DIFFERENT TYPES OF CYBER CRIME?

- There are several types of cybercrimes; the most common ones are email frauds, social media frauds, banking frauds, ransomware attacks,, identity theft, etc.

- Malware
- Malware is a broad phrase that encompasses a wide range of cyberattacks such as Trojans, viruses, and worms. Malware can simply be described as code written to steal data or destroy things on a computer.

- **Viruses:** Viruses, like their biological namesakes, attach themselves to clean files other clean files. Viruses can spread uncontrollably, causing damage to the core as well as deleting and corrupting files. Viruses usually appear as executable files from the internet.
- **Trojan:** This type of malware masquerades as legitimate software that can be prefers to function invisibly and creates security backdoors that allow other the system.
- **Worms:** Worms use the network's interface to infect a whole network of devices, either locally or via the internet. Worms infect more machines with each successive infected machine.

PHISHING

- Phishing frequently poses as a request for information from a reputable third party. Phishing emails invite users to click on a link and enter their personal information.
- In recent years, phishing emails have become much more complex, making it impossible for some users to distinguish between a real request for information and a fraudulent one. Phishing emails are sometimes lumped in with spam, but they are far more dangerous than a simple advertisement

THERE ARE FIVE STEPS TO PHISHING

- **Preparation:** The phisher must pick a business to target and figure out how to obtain the email addresses of that business' customers.
- **Setup:** Once the phisher has decided which entity to mimic and who the victims will be, the setup process can begin. The phisher constructs and distributes communications and collects data.
- **Carry out the attack:** This is a process that most people are familiar with. The phisher sends a fake message that appears to come from a well-known source.

- **Recording data:** The phisher keeps track of the information that victims submit to websites or pop-up windows.
- **Identity theft and fraud:** The phisher uses the collected information to make unlawful transactions or perform other forms of fraud; up to a quarter of the victims never fully recover

DDOS ATTACK

- As the name suggests, a denial-of-service (DoS) attack focuses on disrupting network service. Attackers transmit a large amount of data traffic via the network until it becomes overloaded and stops working. A DoS attack can be carried out in a variety of ways, but the most common is a distributed denial-of-service (DDoS) attack. It involves the attacker sending traffic or data, by utilizing several machines, that will overload the system.
- An individual may not recognize that their computer has been hijacked and is helping to the DoS attack in many cases. many large-scale DoS attacks have occurred in the past. Many instances of large-scale DoS attacks have been implemented as a single sign of protests toward governments.

MAN-IN-THE-MIDDLE ATTACK

- A man-in-the-middle attack can obtain information from the end-user and the entity with which they are communicating by impersonating the endpoints in the online information exchange.
- **Let us take a look at an example to learn more about this attack.**
- If the user is banking online, the man in the middle would communicate with the user by impersonating the bank. The man in the middle would receive all information transferred between the user and the bank including sensitive data related to bank accounts.

EFFECTS OF CYBERCRIME

- According to a 2018 report published by McAfee, the economic impact of cybercrimes is estimated to cost the global economy nearly $600 billion annually.
- Financial loss is one of the obvious effects of cybercrimes, and it can be quite significant. But cyber crimes also have several other disastrous consequences for businesses such as:
- Investor perception can become a huge problem after a security breach causing a drop in the value of businesses.
- Businesses may also face increased costs for borrowing, and raising more capital can be challenging as well after a security breach.
- Loss of sensitive customer data can result in penalties and fines for failing to protect customer data. Businesses may be sued over data breaches.

- Due to loss of reputation and damaged brand identity after a cyberattack, customers' trust in a business will decline. Businesses not only end up losing current customers but also find it difficult to gain new customers.
- Direct costs may also be incurred such as the cost of hiring cybersecurity companies for remediation, increased insurance premium costs, public relations (PR), and other services related to the attack.

HOW TO PREVENT CYBER CRIMES?

- **Backup all data, system, and considerations:** This enables data stored earlier to assist businesses in recovering from an unplanned event.
- **Enforce concrete security and keep it up to date:** Choose a firewall with features that protect against malicious hackers, malware, and viruses. This enables businesses to identify and respond to threats more quickly.
- **Never give out personal information to a stranger:** They can use the information to commit fraud.
- **Check security settings to prevent cybercrime:** A cyber firewall checks your network settings to see if anyone has logged into your computer.
- **Using antivirus software:** Using antivirus software helps to recognize any threat or malware before it infects the computer system. Never use cracked software as it may impose the serious risk of data loss or malware attack.

- **When visiting unauthorized websites, keep your information secure:** Using phishing websites, information can easily bypass the data.
- **Use virtual private networks (VPNs):** VPNs enable us to hide our IP addresses.
- **Restriction on access to your most valuable data:** Make a folder, if possible, so that no one can see confidential documents.

DIGITAL EVIDENCE

- Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, among other places.
- Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device[1]. This evidence can be acquired when electronic devices are seized and secured for examination.

- Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime.
- For example, suspects' e-mail or mobile phone files might contain critical evidence regarding their intent, their whereabouts at the time of a crime and their with other suspects.

When it comes to digital evidence, in essence, it can be anything from logs and all the way to video footage, images, archives, temporary files, replicant data, and even data that's stored inside a device's RAM (otherwise known as volatile data), as long as they are regarded as part of clue for a digital investigation.

TYPES OF DIGITAL EVIDENCE

- 1. Logs
- 2. Video footage and images
- 3. Archives
- 4. Active data
- 5. Metadata
- 6. Residual data
- 7. Volatile data
- 8. Replicant data

- **OS logs**

Examples include events pertaining to system access, security alerts, the duration of a user's login session, when the device was shut down, etc.

- Typically, OS logs are stored in a particular system directory (the exact location depends on the operating system in use).

- **Database logs**
- Since they mostly reveal what changes were made to a particular database, these can be a vital source of crime evidence as well as a useful approach for debugging and troubleshooting in the unfortunate event of any technical issues with the database in question.

- Email logs
- Often presented in a CSV format, email logs can reveal certain details about the sender and content, which includes their email address, time and date of delivery, delivery status, cc, bcc, subject, content type, and error codes (if applicable), while mostly stored in the email's header.
- As we've elaborated in our latest email forensics guide, many cyber criminals use email as their go-to communication channel for the purposes of extortion, financial crime, and distributing illegal materials.
- Alongside email logs, any file attachments also count as one of the evidence types, so they should be closely examined, right along with the server logs through which the email was sent.

- Software logs
- Just like the OS logs, so too do certain software logs count as one of the most important sources of digital evidence.
- Among other things, they contain details regarding what action was performed while the program was running as well as indicate any errors or crashes that can be used for debugging purposes.
- Every software can store these in its own pre-defined location, which may or may not be the installation directory.

- Network logs

These can be viewed as different types of evidence because they also contain clues about what an individual was doing on the internet, including what websites that person has visited, what messages were exchanged with another party, and what the content of the messages was.

A digital forensics examiner should let evidence reveal the truth, so be on the lookout for timestamps and IP addresses – two crucial evidence types that will serve as proof in a court of law.

- Phone logs

A phone's infrastructure encompasses various kinds of evidence, including photos taken, videos recorded, system logs, app logs, and call logs, the latter of which contain crucial details such as the duration of a call, inbound and outbound numbers, etc.

Mobile forensics experts also analyze and examine other types of digital evidence that can be found on a mobile device, including geo indicators (where the device has traveled) and EXIF data the photos may store.

- IP logs

Since everyone who browses the internet gets assigned a unique IP address, knowing this crucial detail allows a digital forensics investigator to trace their real identity and physical location by cooperating with ISPs.

- Device fingerprints

There are many forensic categories of devices where evidence can be found, and each device can generate a unique fingerprint that consists of its hardware specs, the OS it's running (down to the exact version), and even other odd bits and pieces such as the graphics drivers it's running or what fonts are installed.

Therefore, even if a cybercriminal attempts to mask their IP when connecting to a server, the device fingerprint can be collected regardless.

To effectively conduct log forensics, the key thing a log forensics investigator should know about logs of any kind is that they are automatically placed on the device, either by some kind of software that is installed or by the operating system itself.

VIDEO FOOTAGE AND IMAGES

- Out of all the types of digital evidence, video footage and images can be classified as the visible data type, just like the logs we discussed earlier.
- There are many types of digital evidence that fall into this category, including CCTV footage, videos recorded on a mobile device, digital camera footage, voice recordings, etc.
- However, unlike your typical logs, multimedia files may require specialized tools to investigate that go beyond typical multimedia players.

RETRIEVING VIDEO EVIDENCE – A PRACTICAL EXAMPLE

- To give you a practical example, let's suppose your law enforcement department is tasked with having to retrieve CCTV footage from a no-name brand surveillance system. Even if you manage to dismantle the device and retrieve the files in a forensically sound manner, you're still going to need to find a way to open them somehow to examine their contents.

THE SOLUTION TO INACCESSIBLE FILE FORMAT TYPES

- Therefore, the only solution that is viable in practice is employing a professional video forensics tool like VIP 2.0 by SalvationDATA.
- Since it supports all the formats used by almost any DVR and NVR device in existence, you will be able to crack the case in record time by accessing a wide array of file formats without issues, all while preserving the integrity of the files, built-in reporting, and 24/7 access to customer support.
- Also, VIP 2.0 comes with integrated recognition features such as motion detection, thus allowing you to automatically find the exact section of the video footage that contains valuable digital evidence for your case.

ARCHIVES

- Various types of evidence can come in the form of an archive, whether it be:

1. Zip/Rar/similar files
2. Databases
3. Backups
4. Software-specific archives

- Technically, since they can contain all sorts of extractable file formats, archives can be regarded as a wildcard source of evidence, which contains anything from:

1. Images
2. Text files
3. Documents
4. Source codes
5. Videos
6. or even other archives.

ACTIVE DATA

- Have you ever noticed how popular content editors and word processors like Microsoft Word often create temporary files on your hard drive while you're in the midst of typing and working on a document?

This is what's referred to as active data and it's a visible data type.

In fact, many operating systems and applications can create this type of file, including:

1. Email clients
2. Image viewers
3. Word processors
4. Scanners

METADATA

- Unlike the previous types of digital evidence we've discussed, metadata falls into the invisible data type category because it typically requires special software to be able to view it.
- For instance, a photo file on a hard drive or storage media can contain additional data regarding the file's creation such as where the photo was taken, otherwise known as EXIF data.
- This **data is attached to the file and reveals details such as:**

1. Where the photo was taken
2. The time and date the photo was taken
3. What lens was used during the process
4. The camera's model and brand

RESIDUAL DATA

- Residual data is deleted or overwritten data that may contain digital evidence if successfully recovered. Since it's not typically visible through a file browser, it's classified as an invisible data type.
- To understand the concept, you have to keep in mind that when someone deletes a file from a device, the data is still there – it's just unlinked from the file structure itself so it doesn't show up in a search or when viewing the contents of a hard drive or storage device through a file browser.
- Note that every deleted file has the risk of being overwritten by other data, which is particularly true if the hard drive space is running out. That's why it's of paramount importance to act swiftly if you want to recover data that was deleted.

VOLATILE DATA

- Volatile data is the kind of data that is not being written to the disk itself, hence belonging to the invisible data type category. Some viruses, for example, don't write themselves to the hard drive to leave minimal traces behind and avoid detection by antivirus software.
- Therefore, in order to detect them, the RAM needs to be checked and its contents analyzed by a qualified digital forensics analyst.
- For obvious reasons, volatile data needs to be checked before the device is powered off, otherwise, it can be lost forever. To add additional complexity to the challenge, even the very act of launching a digital forensics tool and loading it into the device's RAM can change the RAM's contents, the very same thing we're trying to analyze.

REPLICANT DATA

- For the final entry on our digital evidence list, we have replicant data, another invisible data type.
- On some occasions, various types of software or system processes will leave temporary backup files or directories behind to prevent the unfortunate scenario of losing data (for example, if the user forgets to save whatever they were working on and closes the program).
- An example of this would be Photoshop files and even temporary web cache files.

- Other examples of replicant data include:

1. Web cache and cookies
2. Temporary directories
3. Data blocks

NON VOLATILE DATA

- Non-volatile data is any data that can be retrieved even after the computer loses power or is turned off. This includes data stored on your hard drive, USB thumb drives, CDs and DVDs, or even paper printouts that are sitting around the computer and the workstation area

FILE ANALYSIS TOOL

- Digital forensic is a process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. There are many tools that help you to make this process simple and easy. These applications provide complete reports that can be used for legal procedures

Best Computer Forensics Tools

Name	Platform	Link
ProDiscover Forensic	Windows, Mac, and Linux	Learn More
Sleuth Kit (+Autopsy)	Windows	Learn More
CAINE	Windows, Mac, and Linux	Learn More
PDF to Excel Convertor	Windows, Mac, Mobile	Learn More
Google Takeout Convertor	Windows	Learn More

PRODISCOVER FORENSIC

- ProDiscover Forensic is a computer security app that allows you to locate all the data on a computer disk. It can protect evidence and create quality reports for the use of legal procedures. This tool allows you to extract EXIF(Exchangeable Image File Format) information from JPEG files.
- **Features**:

1. This product supports Windows, Mac, and Linux file systems.
2. You can preview and search for suspicious files quickly.
3. This Digital forensics software creates a copy of the entire suspected disk to keep the original evidence safe.
4. This tool helps you to see internet history.
5. You can import or export .dd format images.
6. It enables you to add comments to evidence of your interest.
7. ProDiscover Forensic supports VMware to run a captured image.
8. **Link**: https://www.prodiscover.com

SLEUTH KIT (+AUTOPSY)

- Sleuth Kit (+Autopsy) is a Windows based utility tool that makes forensic analysis of computer systems easier. This tool allows you to examine your hard drive and smartphone.
- **Features**:

1. You can identify activity using a graphical interface effectively.
2. This application provides analysis for emails.
3. You can group files by their type to find all documents or images.
4. It displays a thumbnail of images to quick view pictures.
5. You can tag files with the arbitrary tag names.
6. The Sleuth Kit enables you to extract data from call logs, SMS, contacts, etc.
7. It helps you to flag files and folders based on path and name.
8. **Link**: https://www.sleuthkit.org

CAINE

- CAINE is a Ubuntu-based app that offers a complete forensic environment that provides a graphical interface. This tool can be integrated into existing software tools as a module. It automatically extracts a timeline from RAM.
- **Features**:

1. It supports the digital investigator during the four phases of the digital investigation.
2. It offers a user-friendly interface.
3. You can customize features of CAINE.
4. This software offers numerous user-friendly tools.
5. **Link**: https://www.caine-live.net

PDF TO EXCEL CONVERTOR

- Acrobat PDF to Excel Convertor transfers PDF data and content right into an Excel spreadsheet. This converted file proves helpful for tracking down cybercriminals from anywhere in the world. This computer forensic tool supports both partial and batch conversion.
- **Features:**

1. Allows you to work from anywhere
2. Super-fast with high-quality output
3. Allows you to work from anywhere
4. It retains the original layout and formatting

PALADIN

- PALADIN is Ubuntu based tool that enables you to simplify a range of forensic tasks. This Digital forensics software provides more than 100 useful tools for investigating any malicious material. This tool helps you to simplify your forensic task quickly and effectively.
- **Features**:

1. It provides both 64-bit and 32-bit versions.
2. This tool is available on a USB thumb drive.
3. This toolbox has open-source tools that help you to search for the required information effortlessly.
4. This tool has more than 33 categories that assist you in accomplishing a cyber forensic task.
5. **Link**: https://sumuri.com/software/paladin/

ENCASE

- Encase is an application that helps you to recover evidence from hard drives. It allows you to conduct an in-depth analysis of files to collect proof like documents, pictures, etc.
- **Features**:

1. You can acquire data from numerous devices, including mobile phones, tablets, etc.
2. It is one of the best mobile forensic tools that enables you to produce complete reports for maintaining evidence integrity.
3. You can quickly search, identify, as well as prioritize evidence.
4. Encase-forensic helps you to unlock encrypted evidence.
5. It is one of the best digital forensics tools that automates the preparation of evidence.
6. You can perform deep and triage (severity and priority of defects) analysis.
7. **Link**: https://www.guidancesoftware.com/encase-forensic

SIFT WORKSTATION

- SIFT Workstation is a computer forensics distribution based on Ubuntu. It is one of the best computer forensic tools that provides a digital forensic and incident response examination facility.
- **Features**:

1. It can work on a 64-bit operating system.
2. This tool helps users to utilize memory in a better way.
3. It automatically updates the DFIR (Digital Forensics and Incident Response) package.
4. You can install it via SIFT-CLI (Command-Line Interface) installer.
5. This tool contains numerous latest forensic tools and techniques.
6. **Link**: https://www.sans.org/tools/sift-workstation/

FTK IMAGER

- FTK Imager is a forensic toolkit is developed by AccessData that can be used to get evidence. It can create copies of data without making changes to the original evidence. This tool allows you to specify criteria, like file size, pixel size, and data type, to reduce the amount of irrelevant data.
- **Features**:

1. It provides a wizard-driven approach to detect cybercrime.
2. This program offers better visualization of data using a chart.
3. You can recover passwords from more than 100 applications.
4. It has an advanced and automated data analysis facility.
5. FTK Imager helps you to manage reusable profiles for different investigation requirements.
6. It supports pre and post-processing refinement.
7. **Link**: https://accessdata.com/products-services/forensic-toolkit-ftk

MAGNET RAM CAPTURE

- Magnet RAM capture records the memory of a suspected computer. It allows investigators to recover and analyze valuable items which are found in memory.
- **Features**:

1. You can run this app while minimizing overwritten data in memory.
2. It enables you to export captured memory data and upload it into analysis tools like magnet AXIOM and magnet IEF.
3. This app supports a vast range of Windows operating systems.
4. Magnet RAM capture supports RAM acquisition.
5. **Link**: https://www.magnetforensics.com/resources/magnet-ram-capture/

X-WAYS FORENSICS

- X-Ways is software that provides a work environment for computer forensic examiners. This program is supports disk cloning and imaging. It enables you to collaborate with other people who have this tool.
- **Features**:

1. It has ability to read partitioning and file system structures inside .dd image files.
2. You can access disks, RAIDs (Redundant array of independent disk), and more.
3. It automatically identifies lost or deleted partitions.
4. This tool can easily detect NTFS (New Technology File System) and ADS (Alternate Data Streams).
5. X-Ways Forensics supports bookmarks or annotations.
6. It has the ability to analyze remote computers.
7. You can view and edit binary data by using templates.
8. It provides write protection for maintaining data authenticity.
9. **Link**: http://www.x-ways.net/forensics/

WIRESHARK

- Wireshark is a tool that analyzes a network packet. It can be used to for network testing and troubleshooting. This tool helps you to check different traffic going through your computer system.
- **Features**:

1. It provides rich VoIP (Voice over Internet Protocol) analysis.
2. Capture files compressed with gzip can be decompressed easily.
3. Output can be exported to XML (Extensible Markup Language), CSV (Comma Separated Values) file, or plain text.
4. Live data can be read from the network, blue-tooth, ATM, USB, etc.
5. Decryption support for numerous protocols that include IPsec (Internet Protocol Security), SSL (Secure Sockets Layer), and WEP (Wired Equivalent Privacy).
6. You can apply intuitive analysis, coloring rules to the packet.
7. Allows you to read or write file in any format.
8. **Link**: https://www.wireshark.org

VOLATILITY FRAMEWORK

- Volatility Framework is software for memory analysis and forensics. It is one of the best Forensic imaging tools that helps you to test the runtime state of a system using the data found in RAM. This app allows you to collaborate with your teammates.
- **Features**:

1. It has API that allows you to lookups of PTE (Page Table Entry) flags quickly.
2. Volatility Framework supports KASLR (Kernel Address Space Layout Randomization).
3. This tool provides numerous plugins for checking Mac file operation.
4. It automatically runs Failure command when a service fails to start multiple times.
5. **Link**: https://www.volatilityfoundation.org

E-FENSE

- E-fense is a tool that helps you to meet your computer forensics and cybersecurity needs. It allows you to discover files from any device in one simple to use interface.
- **Features**:

1. It gives protection from malicious behavior, hacking, and policy violations.
2. You can acquire internet history, memory, and screen capture from a system onto a USB thumb drive.
3. This tool has a simple to use interface that enables you to achieve your investigation goal.
4. E-fense supports multithreading, that means you can execute more than one thread simultaneously.
5. **Link**: http://www.e-fense.com/products.php

WHICH FACTORS SHOULD YOU CONSIDER WHILE SELECTING A DIGITAL FORENSIC TOOL?

- The following factors should be considered while selecting a digital forensic tool:

1. Security
2. Support for multiple platforms
3. User-friendly interface
4. Features and functionalities offered
5. Support for multiple devices
6. Support for multiple file formats
7. Analytics features
8. Integrations and Plugins support

NETWORK FORENSICS TOOLS

- **tcpdump**

Tcpdump is a popular command line tool available for capturing and analyzing network traffic primarily on Unix based systems. Using tcpdump, we can capture the traffic and store the results in a file that is compatible with tools like Wireshark for further analysis. Tcpdump can either be used to do a quick packet capture for troubleshooting or for capturing traffic continuously in large volumes for future analysis. It is worth noting that tcpdump can be used to capture both layer 2 and layer 3 data. The latter may cause disk space problems as the size of the resulting capture file can grow depending on the volume of the network traffic. In addition to the ability to capture large amounts of traffic, tcpdump also supports the use of filters to avoid capturing unnecessary traffic or to capture only the traffic we are interested in. One should be extra cautious with this feature, as applying filters can lead to missing potential evidence.

WIRESHARK

- It would be a surprise if someone worked in the Cyber Security field and not heard of the tool Wireshark. Wireshark is an open-source tool available for capturing and analyzing traffic with support for applying filters using the graphical user interface. On the system, where Wireshark is running one can choose the interface on which traffic needs to be captured.

NETWORK MINER

- According to the official website netresec.com, “NetworkMiner is an open source Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.
- NetworkMiner makes it easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface. The way data is presented not only makes the analysis simpler, it also saves valuable time for the analyst or forensic investigator.

SPLUNK

- Splunk is a proprietary, portable, highly extensible log aggregation and analysis tool. Splunk performs capturing, indexing, and correlating the real time data in a searchable container and produces graphs, alerts, dashboards and visualizations. When it comes to network forensics, splunk plays a crucial role in providing evidence from various sources. While Splunk is a popular commercial tool, a free version is offered with limited features. It comes with an easy to use Graphical User Interface.

SNORT

- Snort is one of the most popular network Intrusion Detection Systems available for free. There is a commercial version of Snort available, which is currently offered by Cisco. Snort is highly configurable, which allows the users to add custom plugins called preprocessors. In addition to it, it comes with a great set of output options. At its core, Snort provides alerts based on rulesets provided to it. The Snort administrator needs to feed the rules as the default installation doesn’t come with any rules by default. However, Snort website provides rulesets that can be fed into Snort. In addition to these rules, one can write custom alert rules.

DATABASE ANALYZERS

- Database forensics is a sub-field of the digital forensics discipline that deals with the preservation, extraction, analysis and presentation of digital evidence and findings.
- With scientific forensics in mind, it is often used in litigation, criminal investigation and organisational inquiry purposes. However, it can also be used as a ***specialized database extraction skill to query the database*** and find out what happened.

DB BROWSER FOR SQLITE

- Popular among users and developers who want to create, search and edit databases compatible with SQLite, DB Browser for SQLite is a free, lightweight open-source tool with a clean interface.
- The database software supports Windows, macOS and Linux operating systems. One prominent feature of this tool is the ability to export multiple tables to CSV, all in a single group, to analyse together.

FEATURES

1. Create and compact database files
2. Create, define, modify and delete tables
3. Import and export tables from/to CSV files
4. Import and export databases from/to SQL dump files
5. Examine a log of all SQL commands issued by the application
6. Plot simple graphs based on table or query data

DATABASE FORENSIC ANALYSIS SYSTEM

- Database Forensic Analysis System is a commercial software that supports multiple relational and non-relational databases such as Oracle, SQLite, MySQL, mongoDB, redis and Cassandra.
- The database forensic software assist in ***resolving the problems about the deleted /corrupted/fragmented database files***, false file system, restriction of application system accessibility, etc.

SOME OF THE MAIN FEATURES INCLUDE

1. Unrestricted Accessibility to the database files – no need for password or account info from the application system
2. Extraction and Recovery for the normal/deleted/damaged database files – e.g. tables, views, triggers
3. Multiple Analysis Functions – e.g. .keyword searching, SQL statement query, visual connection analysis

LOG ANALYZER FOR SQL

- This commercial forensic tool was designed specifically for database administrators to *analyze log files transactions of MySQL Server databases and recover deleted transaction logs*.
- Log Analyzer for SQL scans the forensic details of Redo, General, and Binary logs to identify abnormalities in the MySQL database.
- The forensic tool helps you preview the type of transaction (insert, delete, and update), the time of the transaction, the name of the transaction, and the table name involved in the query.

FEATURES

1. Saving of logs in multiple formats, such as MySQL, CSV, HTML, and XLS format.
2. Date filters on log transactions and log transaction data to analyze the data for a particular time period
3. Option to save log report of the MySQL log file analysis process

SQLITE VIEWER

- Foxton forensics has a free tool called SQLite Viewer that is used for inspecting the contents of SQLite databases.
- The forensic software has a database searcher that automatically load all SQLite databases from folder and subfolders. ***Images are stored in the database are also automatically extracted*** and viewable by examiners in the built-in gallery interface.
- SQLite Viewer has a hex viewer to examine BLOBs and export them to a file for further analysis.

EMAIL SCANNERS

- **Email forensic tools** (also known as *email analysis software*) are **digital tools that process, clean, parse, visualise and extract information from emails** to provide analysts with the information they need to conduct and solve investigations.

LIST OF EMAIL FORENSIC TOOLS

1. Sintelix
2. Xtraxtor
3. Aid4Mail Forensic
4. MailXaminer Forensic Email Analysis Software
5. MailPro+
6. Autopsy
7. Advik Email Forensic Wizard

8. Stellar data recovery
9. Advik MBOX to PDF Converter
10. FreeViewer
11. eMailTrackerPro
12. EmailTracer

FEATURES OF EMAIL FORENSIC SOFTWARE

1. Automatic network and link diagram generation
2. Fast email inspection from multiple views
3. Advanced keyword search filters
4. Report generation
5. Deleted email recovery