A brief history of digital forensics

Although forensic science itself (including the first recorded fingerprints) has been around for over 100 years, digital forensics is a much younger field as it relates to the digital world, which mainly gained popularity after the introduction of personal computers in the 1980s.

For comparative purposes in trying to grasp the concept of digital forensics as still being relatively new, consider that the first actual forensic sciences lab was developed by the FBI in 1932.

Some of the first tools used in digital forensic investigations were developed in FBI labs circa 1984, with forensic investigations being spearheaded by the FBI's specialized **CART** (**Computer Analysis and Response Team**) which was responsible for aiding in digital investigations.

Digital forensics as its own field grew substantially in the 1990s, with the collaboration of several law enforcement agencies and heads of divisions working together and even meeting regularly to bring their expertise to the table.

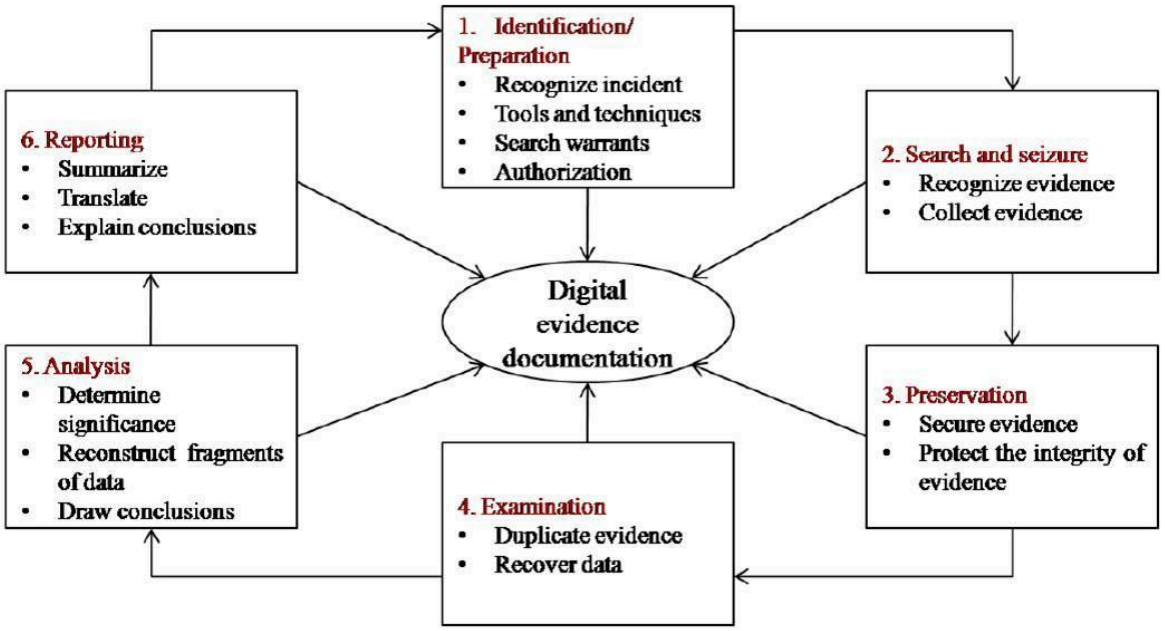
One of the earliest formal conferences was hosted by the FBI in 1993. The main focus of the event, called the **International Law Enforcement Conference on Computer Evidence**, was to address the need for formal standards and procedures with digital forensics and evidence acquisition.

Many of these conferences resulted in the formation of bodies that deal with digital forensics standards and best practices. For example, the SWGDE was formed by the **Federal Crime Laboratory Directors** in 1998. The SWGDE was responsible for producing the widely adopted best practices for computer evidence (discussed later in this chapter). The SWGDE also collaborated with other organizations, such as the very popular **American Society of Crime Laboratory Directors** (**ASCLDs**), which was formed in 1973 and has since been instrumental in the ongoing development of best practices, procedures, and training as it relates to forensic science.

It wasn't until the early 2000s, however, that a formal **Regional Computer Forensic Laboratory** (**RCFL**) was established by the FBI. In 2002, the **National Program Office** (**NPO**) was established and acts as a central body, essentially coordinating and supporting efforts between RCFL's law enforcement.

Since then, we've seen several agencies, such as the FBI, CIA, NSA, and GCHQ, each with their own full cyber crime divisions, full digital forensics labs, dedicated onsite and field agents, collaborating assiduously in an effort to take on tasks that may be nothing short of **Sisyphean**, when considering the rapid growth of technology and easier access to the internet and even the Dark Web.

With the advancement of technology, the tools for digital forensics must be regularly updated, not only in the fight against cyber crime, but in the ability to provide accountability and for the retrieval of lost data. We've come a long way since the days of floppy disks, magnetic drives, and dial-up internet access, and are now presented with SD cards, solid-state drives, and fiber-optic internet connections at Gigabit speeds.



1. Preparing for the Evidence and Identifying the Evidence

In order to be processed and analysed, evidence must first be identified. It might be possible that the evidence may be overlooked and not identified at all. A sequence of events in a computer might include interactions between:

- Different files
- Files and file systems
- Processes and files
- Log files

In case of a network, the interactions can be between devices in the organization or across the globe (Internet). If the evidence is never identified as relevant, it may never be collected and processed.

2. Collecting and Recording Digital Evidence

Digital evidence can be collected from many sources. The obvious sources can be:

- Mobile phone
- Digital cameras

- Hard drives
- CDs
- USB memory devices

Non-obvious sources can be:

- Digital thermometer settings
- Black boxes inside automobiles
- RFID tags

Proper care should be taken while handling digital evidence as it can be changed easily. Once changed, the evidence cannot be analysed further. A cryptographic hash can be calculated for the evidence file and later checked if there were any changes made to the file or not. Sometimes important evidence might reside in the volatile memory. Gathering volatile data requires special technical skills.

3. Storing and Transporting Digital Evidence

Some guidelines for handling of digital evidence:

- Image computer-media using a write-blocking tool to ensure that no data is added to the suspect device
- Establish and maintain the chain of custody
- Document everything that has been done
- Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability

Care should be taken that evidence does not go anywhere without properly being traced. Things that can go wrong in storage include:

- Decay over time (natural or unnatural)
- Environmental changes (direct or indirect)
- Fires
- Floods
- Loss of power to batteries and other media preserving mechanisms

Sometimes evidence must be transported from place to place either physically or through a network. Care should be taken that the evidence is not changed while in transit. Analysis is generally done on the copy of real evidence. If there is any dispute over the copy, the real can be produced in court.

4. Examining/Investigating Digital Evidence

Forensics specialist should ensure that he/she has proper legal authority to seize, copy and examine the data. As a general rule, one should not examine digital information unless one has the legal authority to do so. Forensic investigation performed on data at rest (hard disk) is called dead analysis.

Many current attacks leave no trace on the computer's hard drive. The attacker only exploits the information in the computer's main memory. Performing forensic investigation on main memory is called live analysis. Sometimes the decryption key might be available

only in RAM. Turning off the system will erase the decryption key. The process of creating and exact duplicate of the original evidence is called imaging. Some tools which can create entire hard drive images are:

- DCFLdd
- Iximager
- Guymager

The original drive is moved to secure storage to prevent tampering. The imaging process is verified by using the SHA-1 or any other hashing algorithms.

5. Analysis, Interpretation and Attribution

In digital forensics, only a few sequences of events might produce evidence. But the possible number of sequences is very huge. The digital evidence must be analyzed to determine the type of information stored on it. Examples of forensics tools:

- Forensics Tool Kit (FTK)
- EnCase
- Scalpel (file carving tool)
- The Sleuth Kit (TSK)
- Autopsy

Forensic analysis includes the following activities:

- Manual review of data on the media
- Windows registry inspection
- Discovering and cracking passwords
- Performing keyword searches related to crime
- Extracting emails and images

Types of digital analysis:

- Media analysis
- Media management analysis
- File system analysis
- Application analysis
- Network analysis
- Image analysis
- Video analysis

6. Reporting

After the analysis is done, a report is generated. The report may be in oral form or in written form or both. The report contains all the details about the evidence in analysis, interpretation, and attribution steps. As a result of the findings in this phase, it should be possible to confirm or discard the allegations. Some of the general elements in the report are:

- Identity of the report agency
- Case identifier or submission number

- Case investigator
- Identity of the submitter
- Date of receipt
- Date of report
- Descriptive list of items submitted for examination
- Identity and signature of the examiner
- Brief description of steps taken during examination
- Results / conclusions

7. Testifying

This phase involves presentation and cross-examination of expert witnesses. An expert witness can testify in the form of:

- Testimony is based on sufficient facts or data
- Testimony is the product of reliable principles and methods
- Witness has applied principles and methods reliably to the facts of the case

Experts with inadequate knowledge are sometimes chastised by the court. Precautions to be taken when collecting digital evidence are:

- No action taken by law enforcement agencies or their agents should change the evidence
- When a person to access the original data held on a computer, the person must be competent to do so
- An audit trial or other record of all processes applied to digital evidence should be created and preserved
- The person in-charge of the investigation has overall responsibility for ensuring that the law and these are adhered to

What is Email Forensics?

Email forensics is dedicated to investigating, extracting, and analyzing emails to collect digital evidence as findings in order to crack crimes and certain incidents, in a forensically sound manner.

The process of email forensics, it's conducted across various aspects of emails, which mainly includes

- Email messages
- Email addresses(sender and recipient)
- IP addresses
- Date and time
- User information
- Attachments
- Passwords
- logs (Cloud, server, and local computer)

To deeply and overall investigate the above crucial elements of email, potential clues are going to be obtained to help push the progress of a criminal investigation. Hence, knowing how to conduct scientific and effective email forensics has come into account. But before diving deep into practical email forensics, without a full understanding of the operation and theory of emails themselves, the forensic work is likely to be stuck.

How Email works?

Just like other digital forensics technology, it's not easy to conduct forensics without understanding the basis of the underlying technologies.

Emails are probably generated from various mediums and approaches and thus different technologies are applied accordingly.

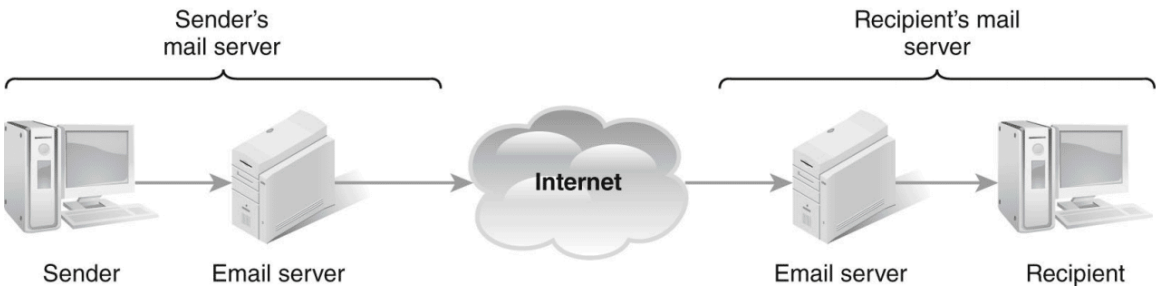
Commonly speaking, a man writes an email on his digital device, maybe a phone or computer, and then sends it to the one he wants to. Though it's seemingly the man has finished his work, the upon email processing work just starts in order to successfully and correctly be delivered to the recipient.

When an email is sent out, countless servers are actually undertaken the whole information of the email before it can really arrive in the recipient's inbox, which is said that we have to understand what's proceeding after we click the "send" button.

Email Programs and Protocols

- During the process, there are 3 protocols and 3 email programs tightly related and are vital to be known.
- Simple Mail Transfer Protocol (SMTP): it is the standard Protocol used to transmit and send emails.
- Internet Message Access Protocol (IMAP): it is one of the standard protocols used for receiving emails.
- POP3 (Post Office Protocol 3): it is one of the standard protocols used to receive mail.
- Mail Transfer Agent (MTA): sends and forwards emails through SMTP. e.g. Sendmail, postfix.
- Mail User Agent (MUA): mail client used to receive emails, which uses IMAP or POP3 protocol to communicate with the server. e.g. Outlook, Apple Mail, Gmail.
- Mail Delivery Agent (MDA): saves the mails received by MTA to local, cloud disk or designated location, meanwhile it usually scans for spam mails and viruses. e.g. Promail, Dropmail.
- Mail Receive Agent (MRA): implements IMAP and POP3 protocol, and interacts with MUA. e.g. dovecot

The theory of email running



Email Transfering

Let's take an example below for instance to better explain the theory of email running.

STEP 1: To start, someone creates an email with a Mail User Agent (MUA), typical MUAs include Gmail, Apple Mail, Mozilla Thunderbird, and Microsoft Outlook Express.

STEP 2: Regardless of the MUA used, the mail is created and sent to the user's mail transfer agent (MTA) – the delivery process uses the SMTP protocol.

STEP 3: The MTA then checks the recipient of the message (here we assume it is you), queries the DNS server for the domain name corresponding to the recipient MTA, and sends the message to the recipient MTA – again using the SMTP protocol.

At this moment, the mail has been sent from the remote user's workstation to his ISP(Internet Server Provider)'s a mail server and forwarded to your domain.

What will happen next?

Considering different network configurations, it is very likely that the mail will be transferred to another MTA during the transmission process, but eventually, an MTA will take over the mail and be responsible for delivery. Then, the MTA will deliver the mail to a mail delivery agent (MDA).

The main function of the MDA is to save the mail to the local disk. Specific MDAs can also be developed with other functions, such as mail filtering or direct mail delivery to other file locations. Thus, it should be noted that it is MDA that completes the function of storing mail on the server.

STEP 4: Now, it's time for you to check your mail.

Running MUA, you can use the IMAP protocol or POP3 protocol to query the mail server for your mail. The mail server first confirms your identity, then retrieves the mailing list from the mail store and returns the list to the MUA.

Now you can read the message.

Message location of an email

Even if we know the running theory of emails, it's recommended to be noted that different configuration on the recipient's email client varies the copies of the message to be saved.

Additionally, any server that sends a message from a party to a recipient can keep a copy of the email.

With the above root principle, it's going to equip your initial ideas before conducting your email investigation.

How to conduct Email Forensics investigation?

With the increasing popularity of the use of email based on the boom of the internet, some typical crimes are tied to email. For instance, financial crime, cyber security, and extortion software, to name a few.

To bring email criminals to justice, it's crucial to look into email investigation in cyber security.

Before we can dive into the major investigative extraction working directions of email forensics, be noted:

Local Computer-based emails: For local computer-based email data files, such as Outlook .pst or .ost files, it's recommended to follow our following techniques directly.

（Cloud）Server-based emails: For（Cloud）Server based email data files, it's not possible to conduct complete forensic work until you obtain the electronic copies in the (Cloud)server database under the consent of the service providers.

Web-based emails: For Web-based e-mail (e.g. Gmail,) investigations, it's more likely possible to just filter specific keywords to extract email address-related information instead of the overall email data and information compared to local computer-based emails.

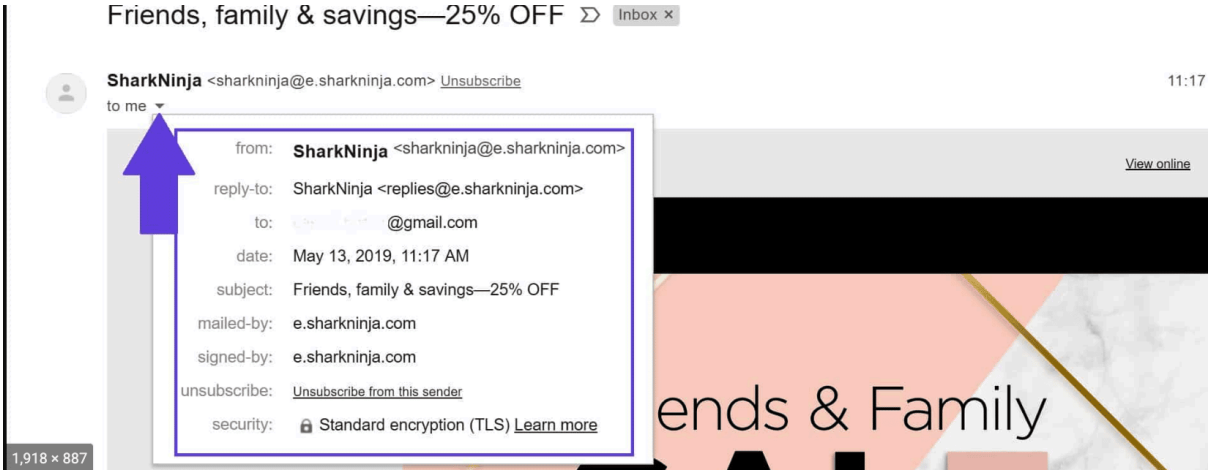
Viewing and Analyzing E-mail Headers

The primary evidence in email investigations is the email header where massive and valuable information could be found.

When carrying out the analysis, you'd be advised to get started from the bottom to the top, since the most crucial information from the sender would be on the bottom while information about the receiver would be on the topmost.

Since we already talked about MTAs where you could find out the route of the email transferred, it should be good for you to give it a detailed scan of the email header.

Here's a sample for your information:



Email Header

If you're still not familiar with the fields, check the below explanations:

From: Address of the actual sender acting on behalf of the author listed in the From field

To: The email address and, optionally, the name of the message's primary recipient(s)

Cc: Carbon copy; a copy is sent to secondary recipients

Bcc: Blind carbon copy; a copy is sent to addresses added to

Subject: A brief summary of the topic of the message

Date: A brief summary of the topic of the message

(In)Reply-To: The message-ID of the message that this is a reply to; used to link related messages together

Message-ID: An automatically generated field

Content-Type: Information about how the message is to be displayed, usually a Multipurpose Internet Mail Extensions (MIME) type

Precedence: —Commonly with values “bulk,” “junk,” or “list”; used to indicate that automated “vacation” or “out of office” responses should not be returned for this mail, for example, to prevent vacation notices from being sent to all other subscribers of a mailing list

Received: Tracking information generated by mail servers that have previously handled a message, in reverse order (last handler first)

References: Message-ID of the message to which this is a reply

The main piece of information you’re looking for is the originating e-mail’s domain address or IP address. Other than that, helpful information includes the date and time the message was sent, filenames of any attachments, and unique message number, if it’s supplied.

Give all of them a complete analysis before you move to the next step.

Email Server Investigation

To locate the source of an email, it’s required to investigate the email’s servers. Since it’s not surprising criminals tend to delete their emails in case of being caught or accused of sensitive emails.

However, there is still a chance to get them back.

In extreme cases, even though both emails have been deleted from both sides between senders and recipients, a copy might be still on the server, since there is always retention on the server after the email is successfully delivered each time due to specific government regulations for email.

Whereas, you don’t want to miss out on investigating the log before it is archived after a certain period.

For your better work implementation, take below most popular email server software under consideration:

Exchange Server (.edb)

Exchange Public Folders (pub.edb)

Exchange Private Folders (priv.edb)

Streaming Data (priv.stm)

Lotus Notes (.nsf)

GroupWise (.db)

GroupWise Post Office Database (wphost.db)

GroupWise User Databases (userxxx.db)

Linux Email Server Logs/var/log/mail.*

Network Devices

If there is no log from the email server due to various reasons, for instance, incorrect configuration on the email server, another approach is worth trying, which is the network service.

In certain cases, an internet service provider (ISP) or any other communications network stores an email. Therefore, investigators are recommended to examine the network devices such as routers and there might be chances for some clue of the source of an email.

Software embedded identifiers

When looking deep enough at the email software, a higher level analysis of the extra information on it comes into account.

Actually, information about the sender and attached files could be found sometimes in an email when you technically examine it, since in most cases, the senders tend to customize their header under Multipurpose Internet Mail Extensions (MIME) with a Transport Neutral Encapsulation Format(TNEF).

Attachment Analysis

As is known to us all, sometimes, our computer gets infected when we surf the Internet and open specific files. To cause the issue, viruses and malware are most skeptical.

When it comes to emails, it's also very common for a problematical attachment to be found and thus it's really worth investigating the attached files.

However, if the files happened to be deleted, you're suggested to consult with a digital forensic agency or use email forensics tools like DRS to recover files so that you could better examine every piece of them.

After the attachment's retrieval, you'd better analyze those suspicious files under a sandbox environment in case the file is malware and do harm to your computer.

Bulk Email Forensics

Significant mailbox collections tend to be examined, analyzed, and used as proof in legal instances. Therefore, legal experts have to work with large mailboxes in many circumstances. Most email service applications, like Perspective and Gmail, give a dashboard embedded with several valuable functions.

However, you might not get the desired results by only using keywords in the interface. Day and time are two attributes of emails considered necessary if they are produced as evidence related to an instance.

Also, email messages can be forged like physical documents, and hackers may tamper with these attributes. Moreover, since an email doesn't directly reach the receiver to the sender, recording its actual way with accurate timings is a challenging aspect.

MD5 and SHA1 Hash Values

MD5 and SHA1 would be the two most crucial hashing algorithms utilized by digital forensics professionals since it's standard practice to make use of MD5 and SHA1 hashing algorithms in email forensics brought on. These algorithms enable forensic investigators to aid digital evidence as soon as they acquire this until it finally is created in a courtroom of law.

One more reason why hash values are crucial is usually that electronic documents are shared with legal professionals and various other parties in the analysis. Therefore, making certain every person has identical replicates of the data files is vital.

Consider how many places an email may well be saved. This could be preserved on the sender's equipment, around the recipient's machine, on either the sender's or recipient's email server, or both, and in backup media with regard to either server. In the event that you consider the many places the email could stay, that should indicate to you that that is rare for an email is usually ever truly deleted.

It may always be quite difficult to get, yet it probably is out there somewhere. This is definitely one of the reasons for this why email forensics is so important.

One will need to sign into the e-mail support in order to be able to analyze emails. Google mail and similar services do not provide any kind of mechanism to access a message if that has been wiped from the trash folder.

In that circumstance, it's likely not possible to be covered.

In some cases, some sort of subpoena can be issued to the service agency, and it

may well search backups intended for the missing electronic mail

Email Tracking in Cyber Security

Js code tracking

To better locate or identify a suspect email address, it's important to attract the suspect to open a trackable email. Across cases like kidnapping and murder, it's commonly used to identify criminals.

By inserting a specific J.S code along HTTP: "img sr" tag on an image within the body of your email, it's going to be able to record at least the IP address after the suspect clicks the image, especially when the location of a suspect or cybercriminal is unknown.

Traced information identify

When acquiring tracking information, it’s no doubt to identify the information in hand to look for some clues that will benefit your forensic investigation in a way.

Below is the manual method for IP address identification where you could figure out detailed information about the IP’s owner.

http://www.whois.net

http://www.networksolutions.com/whois/index.jsp

http://www.who.is

http://www.internic.net/whois.html

http://cqcounter.com/whois/

What is the chain of custody in computer forensics?

The chain of custody in digital forensics can also be referred to as the forensic link, the paper trail, or the chronological documentation of digital evidence. It indicates the gathering, sequence of control, transfer, and analysis. It also documents everybody who handled the digital evidence, the date/time it was collected or transferred, and also the purpose for the transfer.

Why is it important to maintain the chain of custody?

It is important to maintain the chain of custody to preserve the integrity of the electronic evidence and prevent it from contamination, which might alter the state of the electronic evidence. If not preserved, the electronic evidence presented in court may be challenged and ruled impermissible.

Importance to the Examiner

Suppose that, as the examiner, you acquire metadata for a piece of electronic evidence. However, you're unable to extract meaningful information from it. The actual fact that there's no meaningful information within the metadata doesn't mean that the electronic evidence is insufficient. The chain of custody during this case helps show wherever the attainable proof may lie, wherever it came from, who created it, and the sort of equipment that was used. That way, if you want to create model, you'll be able to get that equipment, create the model, and compare it to the electronic evidence to verify the evidence properties.

Importance to the Court

It is possible to have the electronic evidence presented in court laid-off if there's a missing link within the chain of custody. it's so vital to make sure that a wholesome and meaningful chain of custody is presented along with the electronic evidence at the court.

What Is the procedure to establish the chain of custody?

In order to make sure that the chain of custody is as authentic as possible, a series of steps should be followed. it's important to notice that, the additional information a forensic professional obtains concerning the electronic evidence at hand, the additional authentic is that the created chain of custody. Due to this, it's important to get administrator information regarding the evidence: for example, the executive log, date and file information, and who accessed the files. You must make sure the following procedure is followed according to the chain of custody for electronic evidence:

Save the original materials: You must always work on copies of the electronic evidence as against to the original. This ensures that you are able to compare your work product to the original that you preserved unmodified.

Take photos of physical electronic evidence: Photos of physical (electronic) evidence establish the chain of custody and build it additional authentic.

Take screenshots of electronic evidence content: In cases wherever the evidence is intangible, taking screenshots is an effective way of establishing the chain of custody.

Document date, time, and the other information of receipt: Recording the timestamps of whoever has had the electronic evidence permits investigators to create a reliable timeline of wherever the evidence was prior to being obtained. Within the event that there's a hole within the timeline, any investigation could also be necessary.

Inject a bit-for-bit clone of digital evidence content into our forensic computers: This ensures that we obtain to complete duplicate of the digital evidence in question.

Perform a hash test analysis to further authenticate the working clone: Performing a hash test ensures that the information we tend to acquire from the previous bit-by-bit copy procedure isn't corrupt and reflects true nature of the original proof. If this is not the case, then the forensic analysis may be flawed and will lead to issues, so rendering the copy non-authentic.

The procedure of the chain of custody might be completely different: Depending on the jurisdiction within which the electronic evidence resides; but the steps are mostly identical to the ones outlined above.

What considerations are involved with the digital evidence?

A couple of considerations are concerned once handling digital evidence. We tend to shall take a glance at the foremost common and discuss globally accepted best practices.

Never work with the original evidence to develop procedures: The most important thought with digital evidence is that the forensic professionals need to build a whole copy of the evidence for forensic analysis. This can't be overlooked because, once errors are created to operating copies or comparisons are needed, it'll be necessary to match the original and copies.

Use clean collecting media: it’s important to make sure that the examiner’s storage device is forensically clean once getting the electronic evidence. This prevents the original copies from damage. Think about a scenario wherever the examiner’s data electronic evidence collecting media is infected by malware. If the malware escapes into the machine being examined, all of the electronic evidence will become compromised.

Document any extra scope: Throughout the course of an examination, information of evidentiary value could also be found that's beyond the scope of this legal authority. it's suggested that this information be documented and brought to the attention of the case agent because the information may be required to get further search authorities. A comprehensive report should contain the subsequent sections:

- Identity of the news agency
- Case identifier or submission range
- Case investigator
- Identity of the submitter
- Date of receipt
- Date of report
- Descriptive list of items submitted for examination, including serial range, make, and model
- Identity and signature of the examiner

- Brief description of steps taken throughout examination, like string searches, graphics image searches, and ill erased files
- Results/conclusions
- Consider safety of personnel at the scene. it's judicious to always make sure the scene is correctly secured before and through the search. In some cases, the examiner may only have the opportunity to do the following while onsite:
- Identify the number and type of computers.
- Determine if a network is present at a moment.
- Interview the system administrator and users.
- Identify and document the types and volume of media, including with removable media.
- Document the location from that the media was removed.
- Identify offsite storage areas and/or remote computing locations.
- Identify proprietary software system.
- Determine the operating system in question.

The considerations above need to be taken into account when dealing with electronic evidence because of the fragile nature of the task at hand.

Steganography

Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party. This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication.

Steganography hides the covert message but not the fact that two parties are communicating with each other. The steganography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme. In summary:

steganography_medium = hidden_message + carrier + steganography_key

Types

- Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods.
- Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open codes.
- Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website. A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or handwritten text.
- Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication whereas the hidden message is the covert communication. This category is subdivided into jargon codes and covered ciphers.
- Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others. Jargon codes include warchalking (symbols used to indicate the presence and type of wireless network signal [Warchalking 2003]), underground terminology, or an innocent conversation that conveys special meaning because of facts known only to the speakers. A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning.

- Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message. A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word."

Steganography Forensics

The art and science of steganalysis is intended to detect or estimate hidden information based on observing some data transfer and making no assumptions about the steganography algorithm

Steganalysis techniques can be classified in a similar way as cryptanalysis methods, largely based on how much prior information is known (Curran and Bailey 2003; Johnson and Jajodia 1998B).

- Steganography-only attack: The steganography medium is the only item available for analysis.
- Known-carrier attack: The carrier and steganography media are both available for analysis.
- Known-message attack: The hidden message is known.
- Chosen-steganography attack: The steganography medium and algorithm are both known.
- Chosen-message attack: A known message and steganography algorithm are used to create steganography media for future analysis and comparison.
- Known-steganography attack: The carrier and steganography medium, as well as the steganography algorithm, are known.

Steganography Tools

- WetStone Technologies' Gargoyle (formerly StegoDetect) software can be used to detect the presence of steganography software.
- AccessData's Forensic Toolkit and Guidance Software's EnCase can use the HashKeeper, Maresware, and National Software Reference Library (National Software Reference Library 2003) hash sets to look for a large variety of software.
- Niels Provos' stegdetect can find hidden information in JPEG images using such steganography schemes as F5, Invisible Secrets, JPHide, and JSteg.

What Is a Forensic Audit?

A forensic audit examines and evaluates a firm's or individual's financial records to derive evidence used in a court of law or legal proceeding.1 Forensic auditing is a specialization within accounting, and most large accounting firms have a forensic auditing department. Forensic audits require accounting and auditing procedures and expert knowledge about the legal framework of such an audit.

Forensic audits cover a wide range of investigative activities. A forensic audit is often conducted to prosecute a party for fraud, embezzlement, or other financial crimes. In the process of a forensic audit, the auditor may be called to serve as an expert witness during trial proceedings. Forensic audits could also involve situations that do not include financial fraud, such as disputes related to bankruptcy filings, business closures, and divorces.

KEY TAKEAWAYS

- A forensic audit is an examination and evaluation of a firm's or individual's financial records.
- During a forensic audit, an auditor seeks to derive evidence that could potentially be used in court.

- A forensic audit is used to uncover criminal behavior such as fraud or embezzlement.
- When you are a forensic auditor, you specialize in a particular brand of accounting. Smaller firms may not have a forensic auditor on the payroll, but most large, commercial accounting firms have forensic auditing departments.

Forensic audit investigations can uncover or confirm various types of illegal activities. Usually, a forensic audit is chosen instead of a regular audit if there's a chance that the evidence collected would be used in court.

How Forensic Audits Work

The process of a forensic audit is similar to a regular financial audit—planning, collecting evidence, writing a report—with the additional step of a potential court appearance. The attorneys for both sides offer evidence that either uncovers or disproves the fraud and determines the damages suffered. They present their findings to the client, and the court should the case go to trial.

If you've ever padded an expense report—or even thought about it—know that that is an example of fraud and could be uncovered easily via a forensic audit.

Planning the Investigation

During the planning stage, the forensic auditor and team will plan their investigation to achieve objectives, such as

- Identifying what fraud, if any, is being carried out
- Determining the period during which the fraud occurred
- Discovering how the fraud was concealed
- Naming the perpetrators of the fraud
- Quantifying the loss suffered as a result of the fraud
- Gathering relevant evidence that is admissible in court
- Suggesting measures to prevent such frauds from occurring in the future

Collecting Evidence

The evidence collected should be adequate to prove the fraudster's identity (s) in court, reveal the fraud scheme's details, and document the financial loss suffered and the parties affected by the fraud.

A logical flow of evidence will help the court in understanding the fraud and the evidence presented. Forensic auditors are required to take precautions to ensure that documents and other evidence collected are not damaged or altered by anyone.

Reporting

A forensic audit requires a written report about the fraud to be presented to the client to proceed to file a legal case if they so desire. At a minimum, the report should include

- The findings of the investigation
- A summary of the evidence collected
- An explanation of how the fraud was perpetrated
- Suggestions for preventing similar frauds in the future—such as improving internal controls

Court Proceedings

The forensic auditor must be present during court proceedings to explain the evidence collected and how the team identified the suspect(s). They should simplify any complex accounting issues and

explain the case in a layperson's language so that people who have no understanding of legal or accounting terms can understand the fraud clearly.

What Necessitates a Forensic Audit?

Corruption or Fraud

In a forensic audit, an auditor would be on the lookout for

- Conflicts of Interest—when a fraudster uses their influence for personal gains to the company's detriment. For example, if a manager allows and approves inaccurate expenses of an employee with whom they have a personal relationship.
- Bribery—offering money to get things done or to influence a situation in one's favor.
- Extortion—the wrongful use of actual or threatened force, violence, or intimidation to gain money or property from an individual or entity.

Asset Misappropriation

Asset misappropriation is the most prevalent form of fraud. Examples include: misappropriating cash, submitting falsified invoices, making payments to non-existent suppliers or employees, misusing assets (like company equipment), and stealing company inventory.

Financial Statement Fraud

A company can get into this type of fraud to try to show that its financial performance is better than it is. The goal of presenting fraudulent numbers may be to improve liquidity, ensure that C-level executives continue to receive bonuses, or cope with the pressure to perform.

Example of a Forensic Audit Case

Let's say that a fictional computer manufacturer, WysiKids, on the recommendation of its chief financial officer (CFO), entered into a contract with Smart Chips, Inc. to supply WysiKids with processors. However, when the contract was signed, Smart Chips was not authorized to conduct business because its license had been indefinitely revoked based on certain irregularities in a recent Internal Revenue Service (IRS) filing. WysiKids' CFO knew that Smart Chips' license was suspended, yet still suggested that their company sign on with Smart Chips, as they were secretly receiving compensation from Smart Chips for doing so.