Forensic Investigation and Analysis:

Introduction to Forensic Analysis

Forensic analysis is the process of analysing and interpreting digital evidence in order to investigate and solve crimes.

- It is an important part of the field of digital forensics, which is focused on the recovery and analysis of digital evidence from electronic devices.
- Digital devices such as computers, smartphones, tablets, and other electronic devices are often involved in criminal activity and can contain a wealth of information that can be used to help solve crimes.
- This includes data such as user activity, system configurations, network traffic, and communication logs.
- The process of forensic analysis involves the collection, preservation, and analysis of digital evidence in a forensically sound manner.
- This means that investigators must use methods and tools that preserve the integrity of the evidence and do not alter or damage the data in any way.
- It also involves the use of specialized software and techniques to extract and analyze the data in order to identify relevant information and link it to the crime being investigated.
- Forensic analysis can be used to investigate a wide range of crimes, including cybercrime, fraud, theft, and even murder.
- It can be used to uncover digital evidence such as emails, text messages, images, videos, and documents. It can also be used to recover deleted or damaged data and to identify patterns and trends in the data that may be relevant to the investigation.

Live forensic analysis

Live forensic analysis is the process of analyzing a running system in real-time without altering or stopping its operations. This type of analysis is often used in situations where it is not possible to shut down the system in question, such as in critical infrastructure, network servers, and mission-critical systems.

Live forensic analysis involves the use of specialized tools and techniques to analyze the system's memory, network traffic, and running processes. It can provide investigators with valuable information about the system's current state and activity, as well as any ongoing threats or security breaches.

One of the main challenges of live forensic analysis is to ensure that the analysis process itself does not interfere with the system's operations or compromise its integrity. This requires the use of forensically sound techniques and tools that do not alter or damage the system in any way.

Some of the common tools and techniques used in live forensic analysis include:

1. Memory analysis: This involves the analysis of the system's RAM to identify running processes, open files, and network connections.

2. Network analysis: This involves the capture and analysis of network traffic to identify any suspicious activity, such as unauthorized access or data exfiltration.

3. System profiling: This involves the collection of system information, such as hardware configurations, running services, and installed software, to identify potential vulnerabilities or misconfigurations.

4. Process monitoring: This involves the monitoring of running processes to identify any suspicious behavior or activity.

Live forensic analysis can be a powerful tool for investigators, but it requires specialized training and expertise to ensure that the analysis is conducted in a forensically sound manner and does not compromise the integrity of the system being analyzed.

Describe the investigative triad (see lecture slides 1) and the purpose of each of the elements in it.

The investigative triad in forensic science consist of three groups that are responsible for ensuring and maintaining a very a soundly secure computing environment in any organizational setup.

The three groups represent each side of a triangle and they usually work independent of each other though they draw and share expertise in various areas of interest.

1. Vulnerability assessment: This group involves checking the integrity of the server and the system on which the work is done. It involves the checking the security of the operating system and the applications involved. People who work in this group test for known vulnerabilities of OSs and applications used in the network.
2. Incident Response: This group detects intruder attacks by using automated tools and monitoring network firewall logs manually. When an external attack is detected, the response team tracks, locates, and identifies the intrusion method and denies further access to the network.
3. Computer investigations: manages investigations and conducts forensic analysis of systems suspected of containing evidence related to an incident or a crime. For complex casework, the computer investigations group draws on resources from those involved in vulnerability assessment, risk management, and network intrusion detection and incident response.

Data carving

Data carving, also known as file carving, is the forensic technique of reassembling files from raw data fragments when no filesystem metadata is available. It is a common procedure when performing data recovery, after a storage device failure, for instance.

- It may also be performed on a core memory dump as part of a debugging procedure.
- File carving is a recovery technique that merely considers the contents and structures of files instead of file system structures or other meta-data which is used to organize data on storage media.
- Bulk Extractor is a popular open-source data carving tool used by forensic investigators to recover digital evidence from various types of media.

Bulk Extractor

Bulk Extractor is designed to extract data from unstructured sources, such as disk images, memory dumps, and network traffic, by searching for specific patterns or signatures associated with various file types, including documents, images, and multimedia files.

Bulk Extractor can also identify and extract metadata associated with the recovered files, such as timestamps, geolocation data, and email headers.

The process of using Bulk Extractor typically involves the following steps:

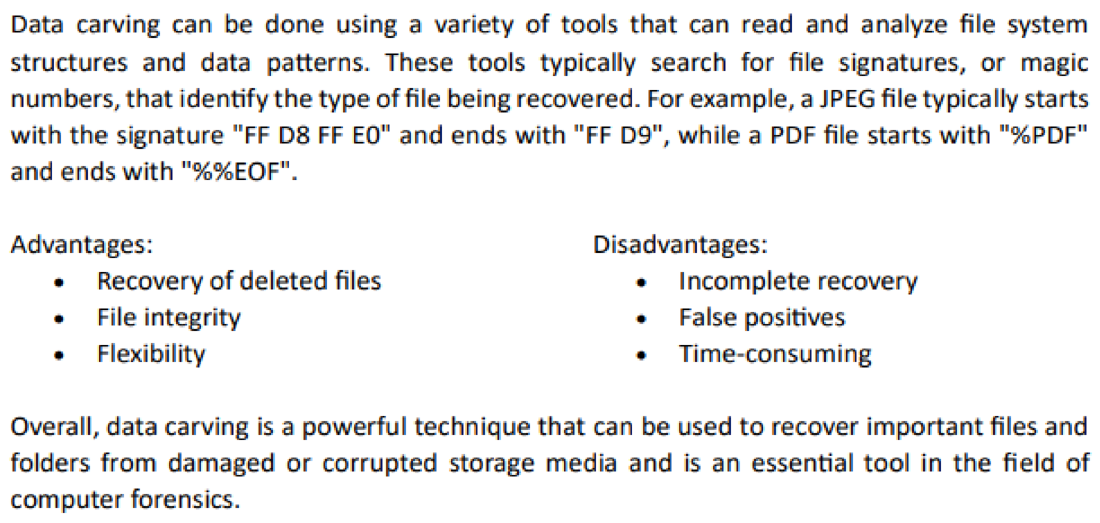
1. Acquisition: The first step is to acquire a forensic image of the media containing the data to be carved, such as a hard drive or memory card. The forensic image should be created using a forensically sound method to ensure the integrity of the data.

2. Analysis: The next step is to analyze the forensic image using Bulk Extractor. The tool can be run in a command-line interface or with a graphical user interface (GUI) to search for specific file types or metadata.

3. Carving: Once the search criteria have been defined, Bulk Extractor will begin carving the data and extracting any recoverable files. The extracted files can be saved to a separate location for further analysis.

4. Verification: It is important to verify the integrity of the recovered files by comparing them to known good copies of the same files or by calculating the hash value of the files and comparing them to the hash value of the original files.

5. Reporting: Finally, a report can be generated to document the findings of the data carving process, including the number and types of files recovered, the location of the recovered files, and any relevant metadata.



Data carving can be done using a variety of tools that can read and analyze file system structures and data patterns. These tools typically search for file signatures, or magic numbers, that identify the type of file being recovered. For example, a JPEG file typically starts with the signature "FF D8 FF E0" and ends with "FF D9", while a PDF file starts with "%PDF" and ends with "%%EOF".

Advantages:

- Recovery of deleted files
- File integrity
- Flexibility

Disadvantages:

- Incomplete recovery
- False positives
- Time-consuming

Overall, data carving is a powerful technique that can be used to recover important files and folders from damaged or corrupted storage media and is an essential tool in the field of computer forensics.

Forensic analysis of acquired data in Windows involves the collection, preservation, and analysis of digital evidence from a Windows-based system. This includes the recovery of deleted files, the analysis of system logs, and the identification of suspicious activity or malicious software.

The first step in the forensic analysis of Windows-based systems is to acquire a copy of the system's hard drive or storage device in a forensically sound manner. This involves creating a bit-by-bit copy of the original data using specialized imaging tools that ensure the integrity of the data is preserved.

Once the data has been acquired, the forensic analysis process begins. This typically involves a number of steps, including:

1. File system analysis: This involves the examination of the file system on the acquired drive to identify files, directories, and other data structures.

2. Recovery of deleted files: This involves the use of specialized tools to recover deleted files that may be relevant to the investigation.

3. Registry analysis: This involves the examination of the Windows Registry to identify any suspicious entries or modifications.

4. Event log analysis: This involves the examination of Windows event logs to identify any suspicious activity or errors.

5. Network analysis: This involves the analysis of network traffic and network connections to identify any unauthorized access or data exfiltration.

6. Malware analysis: This involves the use of specialized tools to identify and analyze any malicious software that may be present on the acquired system.

In addition to these steps, forensic analysts may also use other techniques and tools to identify and analyze digital evidence on the acquired system. These may include password cracking tools, steganography detection tools, and other specialized software designed to help identify and analyze digital evidence.

Overall, the forensic analysis of acquired data in Windows requires specialized training, expertise, and tools to ensure that the analysis is conducted in a forensically sound manner and that the integrity of the digital evidence is preserved.

Forensic investigation and analysis often involve analyzing various types of digital evidence, including registry files and log files.

Registry Files:

- Registry files are databases used by the Windows operating system to store information about system configurations, installed software, user profiles, and other system settings. Registry files can contain important information related to a digital investigation, such as user login history, network configurations, and program execution data.
- Investigating registry files typically involves extracting the data and analyzing it using forensic tools to identify any relevant information. Common registry keys that are often analyzed during forensic investigations include the 'UserAssist' key, which contains information about user activity, and the 'RecentDocs' key, which contains information about recently accessed documents.

Log Files:

- Log files are records of system activity that are generated by operating systems, applications, and network devices. Log files can contain important information related to a digital investigation, such as user activity, network connections, and system errors.
- Investigating log files typically involves analyzing the data using forensic tools to identify any relevant information. Common log files that are often analyzed during forensic investigations include event logs, web server logs, and firewall logs.

To analyze registry files and log files during a forensic investigation, forensic investigators typically use specialized software tools that allow them to extract and analyze the data in a forensically sound manner. These tools typically include hash verification features to ensure the integrity of the data, keyword searching features to identify relevant information, and reporting features to document the findings. It is important for forensic investigators to follow standard procedures and best practices to ensure the reliability and admissibility of the evidence in a court of law.