HyperionDev

Digital Forensics

Task

Visit our website

Introduction

In this task, you will learn about digital forensics and how it relates to other cyber security topics. Digital forensics is the practice of collecting, analysing, and presenting digital evidence in a manner that is legally admissible in a court of law. It is an essential aspect of cyber security, as it involves identifying, preserving, and analysing digital evidence to support criminal investigations or other legal proceedings. Later on in this task, we'll apply what we've learnt by examining the forensic data of a file.

Digital forensics can investigate a wide range of cyber-related crimes, including cyber stalking, cyber bullying, identity theft, online fraud, and cyber espionage. It can also support civil cases, such as intellectual property disputes or employment law cases.

The process of digital forensics typically involves several steps:

1. **Identification**: This involves identifying the devices and systems containing relevant digital evidence.
2. **Preservation**: This involves preserving digital evidence to ensure integrity and authenticity.
3. **Collection**: This involves collecting digital evidence in a legally admissible manner.
4. **Analysis**: This involves analysing the collected evidence to identify relevant information and draw conclusions.
5. **Presentation**: This involves presenting the results of the analysis in a legally admissible manner, such as through written reports or testimony in court.

Data recovery, analysis, and investigation

Data recovery, analysis, and investigation are critical components of digital forensics and are used to identify and analyse digital evidence in support of criminal investigations or other legal proceedings.

Data **recovery** involves extracting data from damaged, corrupted, or inaccessible storage media. This can include recovering data from damaged hard drives, flash drives, or other types of storage media. Data recovery is essential to digital forensics, as it allows investigators to access potentially valuable evidence that may otherwise be lost or inaccessible.

Data **analysis** involves examining collected data to identify relevant information and draw conclusions. This can include analysing log files, email messages, social media posts, and other types of digital data. Data analysis is an essential step in the digital forensics process, as it helps investigators identify patterns of activity, relationships between individuals, and other relevant information.

Data **investigation** involves data analysis to support criminal investigations or other legal proceedings. This can include conducting interviews, gathering additional evidence, and preparing reports or testimony for use in court. Data investigation is an essential aspect of digital forensics, as it helps to identify suspects, establish motives, and build a case against individuals or organisations involved in cyber-related crimes.

Cyber ethics and best practices

Cyber ethics refers to the principles and values that govern the responsible use of technology and the internet. It encompasses a broad spectrum of topics, including privacy, security, online behaviour, and social responsibility.

Best practices in cyber ethics involve adopting responsible behaviours and techniques when using technology and the Internet to protect against potential risks. Some examples of cyber ethics activities include:

1. **Protecting personal and sensitive data**: This involves taking steps to protect personal and sensitive data from unauthorised access or misuse, such as using strong passwords, enabling two-factor authentication, and avoiding sharing personal information online.

2. **Respecting intellectual property**: This involves respecting the intellectual property rights of others, such as properly citing sources and obtaining permission before using copyrighted material.

3. **Protecting online privacy**: This involves taking steps to protect online privacy by using secure websites and networks and being cautious about sharing personal information online.

4. **Being aware of cyber security risks**: this involves being aware of the potential risks associated with using technology and the Internet and taking steps to protect against these risks, such as by using antivirus software and keeping software and devices up to date.

5. **Promoting online safety and security**: this involves promoting online safety and security for oneself and others, such as by educating others about cyber security risks and best practices, and reporting any suspicious activity or potential threats.

Digital forensics tools

Many different types of digital forensics tools can be used to collect, analyse, and present digital evidence in a manner that is legally admissible in a court of law. Some examples of digital forensics tools include:

Data carving tools

Data carving tools search for and extract specific data types from a disk or storage device, even if the data is not organised in a traditional file structure. Some examples include:

1. **PhotoRec**: A free, open-source data carving tool that can recover a wide range of file types from various storage devices. It can handle both deleted files and files that have been overwritten or damaged.

2. **Scalpel**: Another open-source data carving tool that can recover deleted files from a variety of storage devices. It can scan for specific file types using regular expressions, and can also recover files that have been fragmented or partially overwritten.

3. **Foremost**: A data carving tool that is included with The Sleuth Kit, a suite of forensic tools. It can recover deleted files from a variety of storage devices, and can also scan for specific file types using header and footer definitions.

Network forensics tools

Network forensics tools capture and analyse network traffic to identify patterns of activity or anomalies that may indicate a security threat. Some examples include:

1. **Wireshark**: A free, open-source network protocol analyser that can be used to capture and analyse network traffic in real time. It can decode and display a wide range of protocols and includes features such as filtering, colour coding, and protocol decoding.

2. **NetWitness Investigator**: A commercial network forensic tool that can analyse network traffic and logs to identify security threats and incidents. It includes features such as packet capture, traffic analysis, and log analysis.

3. **NetworkMiner**: A free, open-source network forensic tool that can be used to analyse network traffic and extract information such as file transfers, email conversations, and web page visits. It can also decode and display various network protocols and includes features such as packet capture and protocol decoding.

File analysis tools

File analysis tools analyse specific types of files, such as email messages or log files, to identify relevant information and extract metadata. Some example tools include:

1. **Interactive Disassembler (IDA) Pro**: IDA Pro is a commercial disassembler and debugger that is widely used for reverse engineering and software analysis. It can analyse a wide range of file formats, including executables, libraries, and firmware images, and can generate detailed disassembly listings and call graphs. IDA Pro also includes debugger and scripting capabilities, which allow you to analyse the behaviour of a program as it runs.

2. **Ghidra**: A free, open-source reverse-engineering tool developed by the National Security Agency (NSA). It includes features such as disassembly, decompilation, and analysis of executable files, as well as a debugger and scripting capabilities. Ghidra is designed to be easy to use and can handle a wide range of file formats.

3. **Rekall**: An open-source memory analysis tool that can be used to analyse the contents of a computer's memory. It includes features such as memory acquisition, memory forensics, and memory analysis, and can be used to identify malware, extract evidence, and understand the behaviour of a system. Rekall can be used on both live systems and memory dumps and supports a wide range of file formats.

Mobile device forensics tools

Mobile device forensics tools are specialised tools for analysing data from mobile devices like smartphones or tablets. Some example tools include:

1. **Oxygen Forensic Detective**: A commercial mobile device forensics tool that can be used to extract and analyse data from a wide range of mobile devices, including smartphones, tablets, and GPS units. It includes features such as data extraction, data analysis, and report generation.

2. **Mobile Phone Examiner Plus (MPE+)**: MPE+ is a commercial mobile device forensics tool developed by AccessData.

Forensic imaging tools

Forensic imaging tools create an exact copy of a disk or storage device, including hidden or deleted data, to preserve the original data and make it available for analysis. Some example tools include:

1. **FTK Imager**: A commercial forensic imaging tool developed by AccessData. It can be used to create forensic images of a wide range of storage media,

including hard drives, memory cards, and removable drives. It includes features such as data verification, hashing, and compression.

2. **dd**: dd is a command-line tool that is included with most Unix-like operating systems. It can be used to create forensic images of a wide range of storage media, including hard drives, memory cards, and removable drives. It is a powerful tool, but it requires a high level of expertise to use effectively.

The importance of digital forensics

Digital forensics is vital in the context of cyber crime, cyber law, hacking, data breaches, identity theft, data extraction for legal cases, and regulatory compliance, for several reasons:

1. **Cyber crime**: Provides a systematic and legally admissible way to collect, analyse, and present digital evidence supporting criminal investigations related to cybercrime.

2. **Cyber law**: A vital tool for supporting cyber law, the body of law governing the use of technology and the Internet. Digital forensics can be used to gather and analyse evidence in support of cyber law cases, such as civil cases involving intellectual property disputes or employment law cases.

3. **Hacking**: Can be used to identify and track the activities of hackers and to gather evidence supporting criminal investigations related to hacking.

4. **Data breaches**: Can be used to identify the cause of a data breach, track the activities of individuals involved in the violation, and gather evidence supporting criminal investigations or other legal proceedings related to data breaches.

5. **Identity theft**: Can be used to identify the cause of identity theft, track the activities of individuals involved in the robbery, and gather evidence supporting criminal investigations or other legal proceedings related to identity theft.

6. **Data extraction for legal cases**: Extracts relevant data from digital devices or storage media to support legal cases, such as civil or criminal cases.

7. **Regulatory compliance**: Can be used to demonstrate compliance with regulatory requirements related to the collection, use, and protection of digital data, such as data protection laws and regulations.

Take note

Please note: there is an additional reading in this task's folder entitled **Guide to Integrating Forensic Techniques into Incident Response**. Read this if you would like a deeper understanding of the importance of forensic techniques used for incident response. Please keep in mind that this reading is for enrichment and is **optional**.

Programming and digital forensics

Digital forensics often involves using programming concepts and tools to collect, analyse, and present digital evidence for legal proceedings. Some programming concepts commonly used in digital forensics include:

1. **Data structures**: Used to organise and store data to make it easier to access and analyse. In digital forensics, data structures are often used to store and organise log data, email messages, and other digital evidence.

2. **Algorithms**: These are instructions to solve specific problems or perform specific tasks. In digital forensics, algorithms are often used to automate the process of analysing digital evidence, such as identifying activity patterns or extracting relevant metadata.

3. **Scripting languages**: These are programming languages that are used to automate tasks or processes. In digital forensics, scripting languages are often used to automate the collecting and analysing of digital evidence, such as by creating scripts to extract data from log files or email messages.

Some programming tools and languages commonly used in digital forensics include:

1. **Python**: A popular programming language often used in digital forensics due to its flexibility and powerful data-processing capabilities.

2. **Structured query language (SQL)**: A programming language used to manage and query databases. In digital forensics, SQL is often used to access and analyse log data, email data, and other digital evidence stored in databases.

3. **EnCase**: A popular digital forensics tool used to collect and analyse digital evidence. It includes various features and tools for analysing data from multiple sources, including hard drives, mobile devices, and cloud storage.

Potential career options

Many potential jobs combine programming and digital forensics skills, including:

1. **Digital forensics analyst**: Responsible for collecting, analysing, and presenting digital evidence supporting criminal investigations or other legal proceedings. This may involve using programming skills to automate collecting and analysing digital evidence or developing custom tools and scripts for specific tasks.

2. **Cyber security analyst**: Responsible for protecting an organisation's networks and systems from cyber risks and threats. This may involve using programming skills to develop custom tools and scripts for analysing data from various sources, such as log files, network traffic, and mobile devices.

3. **Data analyst**: Responsible for collecting, analysing, and presenting data to support decision-making and problem-solving. This may involve using programming skills to develop custom tools and scripts for collecting and analysing data from various sources.

4. **Cyber crime investigator**: Responsible for conducting investigations into cyber crimes, such as cyberstalking, cyberbullying, identity theft, online fraud, and cyber espionage. This may involve using programming skills to develop custom tools and scripts for analysing data from various sources to identify activity patterns and build a case against suspects.

Now that you are familiar with the fundamentals of digital forensics, it's time to try putting some of these into practice.

Take note

In this practical task, you will use digital forensics techniques and Python to extract the metadata from a chosen file.

There are many reasons why you may want to extract the metadata from a file, including:

1. **To identify the source of a file**: Metadata can often include information about the creator or source of a file, such as the author's name, the date and time the file was created, and the application or device used to create it. This can be useful in identifying the origin of a file and determining its authenticity.

2. **To understand the history of a file**: Metadata can also include information about the history of a file, such as the dates and times it was modified, the applications or devices used to modify it, and the users who accessed it. This can

be useful in understanding the evolution of a file and determining its relevance to an investigation.

3. **To contextualise a file**: metadata can also include information about the context in which a file was used or created, such as the location, the device or application used, and the network or Internet connection. This can be useful in understanding the context in which a file was used and determining its significance to an investigation.

Practical task

In this practical task, you will create a tool to extract metadata from a given file using Python and display it in a user-friendly format. This will help you gain practical experience with digital forensics techniques, as well as with programming in Python.

You'll need to start off by choosing a Python library or package that can be used to extract metadata from a file, such as the `os` or `pathlib` module. In Python 3.4, `pathlib` is now part of the standard library. For Python 3.3 and earlier, to install `pathlib` you will need to enter the following into your command line or terminal:

```
pip install pathlib
```

Research how to use the chosen library or package to extract metadata from a file. This may involve reading the documentation, looking at code examples, or experimenting with the library or package in VS Code or your chosen Python editor or IDE. Some specific websites to use as an online resource for this task can be found below:

1. Here are some websites that you can use as online resources for researching how to use the `os` and `pathlib` modules to extract metadata using Python:
    - The library or package's official documentation:
        - The official documentation for the os module can be found at **os — Miscellaneous operating system interfaces — Python 3.12.3 documentation**.
        - The official documentation for the pathlib library can be found at **pathlib — Object-oriented filesystem paths — Python 3.12.3 documentation**.
2. Online tutorials and guides: Many websites offer tutorials and guides on using specific Python libraries and packages. Here are a couple of examples of tutorials that cover the `os` and `pathlib` modules:

    - A handy tutorial on using the `os` module to work with files and directories in Python can be found **here**.

3. A tutorial on using the `pathlib` module to work with files and directories in Python can be found in **Python's pathlib Module: Taming the File System**.
4. YouTube tutorials: Here are a couple of examples of YouTube tutorials that might be useful:
    - A tutorial on using the **os module to work with files and directories** in Python.
    - **Here's another helpful tutorial**.

Follow these steps:

- Create a Python file called **forensics.py** in your task folder.
- We will use the `os` module for this task, but `pathlib` is another useful Python module for extracting metadata.

Okay, let's begin:

- Write a Python program that can take a file as input and extract the metadata from it. Start by importing the chosen module, and then define a function that takes a file path as input and returns the metadata for that file.
- Use the chosen module to extract the metadata from the file, such as the file type, size, creation date, and other relevant information. Store the metadata in appropriate data structures, such as dictionaries, lists, or tuples.
- Use **pprint** to display the extracted metadata in a clear and organised way.
- Test your program with the test file provided in your Dropbox folder to ensure that it extracts metadata accurately.

Important: Be sure to upload all files required for the task submission inside your task folder and then click "Request review" on your dashboard.

Optional task

Follow these steps:

- Extend your program by adding additional features, such as the ability to extract metadata from multiple files at once, or to display the metadata in a graphical format. This may involve modifying your existing code or writing new functions or classes to implement the additional features.
- Use **tkinter** to create a graphical user interface.

Share your thoughts

Please take some time to complete this short feedback **form** to help us ensure we provide you with the best possible learning experience.