PES1UG20CS581
ROHITH H
J SEC

DIGITAL FORENSICS ASSIGNMENT - 01

QUESTION -01

Which are the best tools for the Data Acquisition in terms of the Digital forensics

Answer:

The best two tools for the data acquisition is the web scraping and the API calls and the advantages and disadvantages of both of them are given below

Web scraping involves using a program or script to extract data from a website

API calls involve using a program or script to send a request to a server and receive data in response.

Advantages of the web scraping tool in digital forensics are

- *Web scraping can be used to acquire data from a wide range of sources, including social media platforms, forums, and other websites.*
- *It can also be used to automate data collection from multiple sources, which can save time and resources.*
- *It can be useful in situations where data is not available through an API or is difficult to access through other means*

Disadvantages of Web scraping tools are

- *Web scraping can be difficult to set up and configure, especially for complex websites*

- *It can also be illegal to scrape private data, for example scraping information from a website without permission.*

Advantages of the API calls in the forensics are

- *API calls can be used to acquire data from specific sources, such as databases or software applications.*
- *They can be more reliable and accurate than web scraping, as the data is provided directly by the source.*
- *API calls can also be faster, as they usually return a smaller amount of data*

Disadvantages of the API calls are

- *API calls are generally specific to a particular source and may not be able to acquire data from other sources*
- *If the API keys are compromised, it could lead to unauthorized access to the data.*

QUESTION -02

Which are the best tools for the storage analysis in terms of the Digital forensics

Answer:

Sleuth Kit (TSK) and Autopsy are two popular tools for storage analysis in digital forensics. TSK is a command line tool that allows for in-depth analysis of file system metadata and file content, while Autopsy is a GUI tool that provides a user-friendly interface for searching and analyzing disk images and file systems.

PES1UG20CS581
ROHITH H
J SEC

DIGITAL FORENSICS ASSIGNMENT - 01

Advantages of the Sleuth kit TSK tool in digital forensics are

- *TSK is a collection of command-line tools, which makes it fast and efficient for analyzing large amounts of data.*
- *It is able to analyze various file systems, including NTFS, FAT, and ext2/3/4.*
- *TSK allows for in-depth analysis of file system metadata and file content, making it useful for identifying deleted or hidden files and uncovering file system-level artifacts.*
- *TSK is free and open-source, which makes it accessible to a wide range of users.*

Disadvantages of Sleuth kit (TSK) tools are

- *TSK is a command-line tool, which can make it difficult to use for those who are not familiar with command-line interface.*
- *TSK is not as user-friendly as other tools, as it requires a certain level of technical expertise to use effectively.*

Advantages of the Autopsy tool in digital forensics are

- *Autopsy is a GUI tool, which makes it user-friendly and easy to use for those who are not familiar with command-line interface.*
- *Autopsy provides a wide range of features such as keyword searches, file and metadata extraction, and report generation, which makes it easy to analyze digital evidence.*
- *Autopsy also includes a module for analyzing web artifacts, such as browser history and cookies.*
- *Autopsy is free and open-source, which makes it accessible to a wide range of users.*

PES1UG20CS581
ROHITH H
J SEC

DIGITAL FORENSICS ASSIGNMENT - 01

Disadvantages of Autopsy tools are

- *Autopsy is not as customizable as TSK, and it may not be able to analyze certain types of file systems or file system-level artifacts.*
- *Autopsy is not as powerful as TSK, as it is built on top of TSK and relies on TSK's functionality.*

QUESTION -03

Which are the best tools for the Memory analysis in terms of the Digital forensics

Answer:

Both Volatility and Rekall are free and open-source tools that are widely used in the digital forensics community. They both provide a wide range of features and plugins, making them useful for analyzing various types of data from memory dumps.

Volatility is an open-source memory forensics framework that can be used to analyze memory dumps from Windows, Linux, and Mac systems.

Rekall is another open-source memory forensics framework that can be used to analyze memory dumps from Windows and Linux systems.

Advantages of the Volatility tool in digital forensics are

- *Volatility is an open-source memory forensics framework that can be used to analyze memory dumps from Windows, Linux, and Mac systems.*
- *It provides a command-line interface and a Python API for analyzing memory dumps, which makes it versatile and adaptable to different use cases.*

- *Volatility includes a wide range of plugins for analyzing specific types of data, such as malware and browser artifacts.*
- *Volatility has an active community that develops and maintains the tool, which means that new features and plugins are often added and bugs are fixed regularly.*

Disadvantages of Volatility tools are

- *Volatility is a command-line tool, which can make it difficult to use for those who are not familiar with command-line interface.*
- *Volatility requires a certain level of technical expertise to use effectively.*

Advantages of the Rekall tool in digital forensics are

- *Rekall is another open-source memory forensics framework that can be used to analyze memory dumps from Windows and Linux systems.*
- *It provides a command-line interface and a Python API for analyzing memory dumps, which makes it versatile and adaptable to different use cases.*
- *Rekall includes a wide range of plugins for analyzing specific types of data, such as malware and browser artifacts.*
- *Rekall has a GUI option, which makes it more user-friendly for those who are not familiar with command-line interface.*

Disadvantages of Rekall tools are

- *Rekall is not as customizable as Volatility and may not be able to analyze certain types of data.*
- *Rekall requires a certain level of technical expertise to use effectively.*

PES1UG20CS581
ROHITH H
J SEC

DIGITAL FORENSICS ASSIGNMENT - 01

QUESTION -04

Which are the best tools for the Email analysis in terms of the Digital forensics

Answer:

The best two tool for analysis of the email are Forensics Email Collector (FEC) and Email Analysis Tool (EAT).

The Forensic Email Collector (FEC) is a tool that can be used to collect and analyze email data from various sources, including email servers, cloud-based email services, and local email clients. It can also be used to extract the metadata and the email content and supports variety of the email formats.

The Email Analysis Toolkit (EAT) is a tool that can be used to analyze email data from various sources, including email servers, cloud-based email services, and local email client.

Advantages of the Forensics Email Collector (FEC) tool in digital forensics are

- *FEC can be used to collect and analyze email data from various sources, including email servers, cloud-based email services, and local email clients.*
- *It can be used to extract metadata and email content, and it supports a wide range of email formats, including PST, EML, and MBOX.*
- *FEC includes features for searching, filtering, and reporting on email data, which makes it easy to analyze large amounts of email data.*

PES1UG20CS581
ROHITH H
J SEC

DIGITAL FORENSICS ASSIGNMENT - 01

Disadvantages of Forensics Email Collector (FEC) tools are

- *FEC may not be as user-friendly as other tools, as it requires a certain level of technical expertise to use effectively.*
- *It may not be as customizable as other tools, and it may not be able to analyze certain types of email data.*

Advantages of the Email Analysis Toolkit (EAT) in digital forensics are

- *EAT can be used to analyze email data from various sources, including email servers, cloud-based email services, and local email clients.*
- *It can be used to extract metadata and email content, and it supports a wide range of email formats, including PST, EML, and MBOX.*
- *EAT includes features for searching, filtering, and reporting on email data, which makes it easy to analyze large amounts of email data.*
- *EAT includes a built-in email viewer, which allows you to view email messages in their native format, making it more user-friendly.*

Disadvantages of Email Analysis Toolkit are

- *EAT may not be as customizable as other tools, and it may not be able to analyze certain types of email data.*

The contents of this are been taken/used from the different websites and referred from different websites and written as a summary