

BN 309 Computer forensics

Assignment 1



Name: Bibek Lamichhane

MIT ID: MIT213769

SCHOOL: Melbourne instiyute of technology

unit coordinator: Muhammad Ijaz

Contents

[**Introduction** 1](#_Toc173667680)

[**Similarities between Autopsy and Pro Discover Basic** 1](#_Toc173667681)

[**Difference between Autopsy and Pro Discover Basic** 3](#_Toc173667682)

[**Computer Forensic Tools Analysis** 4](#_Toc173667683)

[**Data Preparation** 4](#_Toc173667684)

[**Data Acquisition** 6](#_Toc173667685)

[Autopsy 6](#_Toc173667686)

[Pro Discover Basic 12](#_Toc173667687)

[**Conclusion** 17](#_Toc173667688)

[**References** 17](#_Toc173667689)

# **Introduction**

This project is set to recover key evidence from a 16GB USB device, which was recovered from a scene of crime. This device contains files in different formats and might constitute important evidence in a murder case. It consists of installing two of the best forensic tools (Autopsy and Pro Discover Basic), which are then compared, recording a procedure for how data is collected, and finally ensuring that what has been documented can be used in a court proceeding. The aims of this exercise are mostly to enhance knowledge of digital forensics, give awareness of tools to students, and make them ready for forensic investigation in real life.

# **Similarities between Autopsy and Pro Discover Basic**

Pro Discover Basic and Autopsy are some of the key digital forensic tools with functions that range from the basic ones in metadata analysis, file recovery, and forensic photography. These devices create incremental copies of storage mediums to preserve all data, even files that have been deleted. Sophisticated search functions, including keyword, file type, and pattern search, make finding relevant evidence easier, with user-friendly interfaces that allow this process to be done more easily [1]. These programs support several file systems and operating systems, including Windows, Mac, and Linux. They also put at one's disposal the functionality of network forensics, extensive possibilities for reporting, and timeline analysis to understand the chronology of events. Extensive documentation and community support make them very useful during forensic investigations [2].

A screenshot of a computer

Description automatically generated

Fig 1: Search Function in Pro Discover Basic

A screenshot of a computer

Description automatically generated

Fig 2: keyword search function in autopsy

A screenshot of a computer

Description automatically generated

Fig 3: File recovery in autopsy

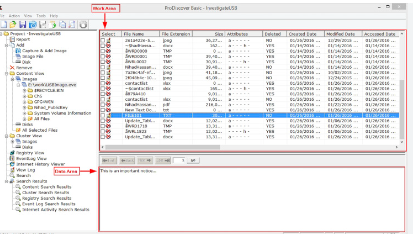


Fig 4: Recover deleted files in Pro Discover Basic

# **Difference between Autopsy and Pro Discover Basic**

Although these are the most essential digital forensic tools, Autopsy and Pro Discover Basic have a good number of differences. Autopsy is an open-source tool, very widely applied both in professional and academic fields, and publicly available; it was developed by Basis Technology. It has an easy-to-use graphical user interface and supports other applications, including The Sleuth Kit, which runs on Windows, Linux, and Mac OS [3]. Its big community offers wide support and frequent updates. Pro Discover Basic by Technology Pathways is commercial software with licensing that has seen the same tool in wide use in the commercial world. It offers many advanced features in live memory capturing, detailed analysis of network traffic, and thorough Windows registry and internet artifact checking. Primarily targeted for windows environments, While Pro Discover Basic has extensive industry standard reporting features and high-end, committed customer support, it is both comparatively limited and higher priced than Autopsy. With these differences, Autopsy looks most appealing to flexible, affordable investigations with community-driven upgrades, while Pro Discover Basic is mostly meant for in-depth, professional forensic work needing advanced capabilities [4].

**A screenshot of a computer

Description automatically generated**

Fig 5: Autopsy image

**A screenshot of a computer

Description automatically generated**

Fig 6: Pro Discover Basic image

# **Computer Forensic Tools Analysis**

The major requirement in conducting a comprehensive forensic investigation concerning the homicide case, particularly on the 16GB USB drive, will be Pro Discover Basic. First, create a bit-by-bit forensic image of the USB device to ensure that all data, including deleted files, is appropriately preserved. Pro Discover Basic is a very nice tool for recovering files; it allows the recovery of deleted files, including pictures, audio, video, and documents. Metadata is also deeply analyzed to present vital information, like dates of creation and modification, and access histories [5].

It can take advantage of advanced live memory acquisition and network analysis via Pro Discover Basic for the identification of any erratic data and relative network activities. It has strong search functions that allow for keyword and pattern searches, which will make it easy to identify evidence concerning the murder. Internet artifacts and registry entries must also be examined to deduce some information about user behavior.

Lastly, use Pro Discover Basic's reporting feature to create a very detailed, professional-grade report that will properly document your findings and be suitable for submission to the court. Employ Pro Discover Basic's dedicated customer support for technical assistance or any advanced questions that you might have during your investigation [6].

# **Data Preparation**

Ten files of different extensions such as PDF, doc, PNG, mp3, and mp4 have been created to prepare the data as evidence for this homicide case.

A screenshot of a computer

Description automatically generated

Fig 7: Ten files created to support as evidence for a homicide case

Modifying the attributes of all files such as:

* Author: Bibek Lamichhane
* Organization: MIT
* Comments: Created for assignment of BN309
* Date and Time created: 22/JUL/2024 & 10:09 PM

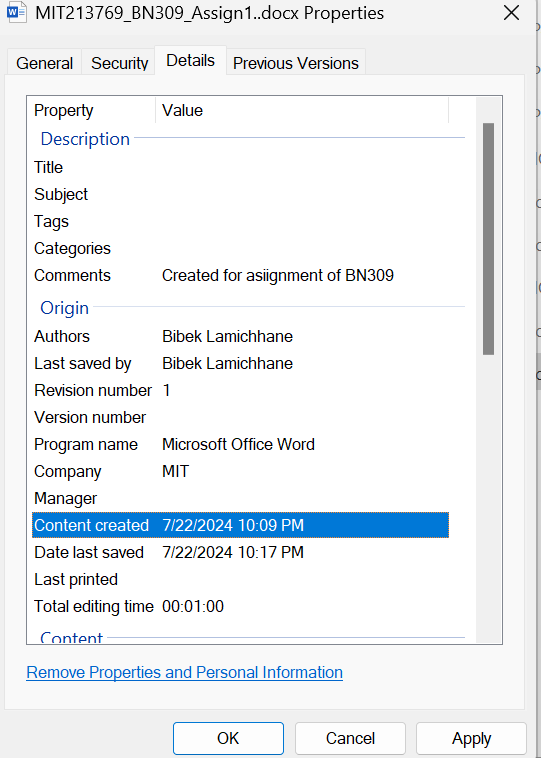


Fig 8: Changed attribute of the file

Again, changing the file extension from .docx into .jpeg and .pdf to .jpeg format as:

A screenshot of a computer

Description automatically generated

Fig 9: Changed extension files snapshot

Deleting five files including the file whose extension has been modified along with each type of file:

A screenshot of a computer

Description automatically generated

Fig 10: Updated snapshot after the deletion of the five (5) different types of files

# **Data Acquisition**

## Autopsy

Initial GUI interface of the software

A screenshot of a computer

Description automatically generated

Fig 11: Initial interface of autopsy

Click on the new case and select the appropriate base directory to store the homicide case information.

A screenshot of a computer

Description automatically generated

Fig 12: Filling case information

After that fill in the optional information and set the organization information and click on finish button:

A screenshot of a computer

Description automatically generated

Fig 13: Filling optional information

Then the source interface to add data will pop up, and select generate new host name and click next;

A screenshot of a computer

Description automatically generated

Fig 14: Generating and selecting host

Click on Local disk to discover the USB that you have inserted and the data that need to be retrieved which are already deleted.

A screenshot of a computer

Description automatically generated

Fig 15: Selecting the data source type

Select the appropriate data source by clicking the select disk option.

A screenshot of a computer

Description automatically generated

Fig 16: Selecting the appropriate source for data analysis

And then the interface will pop up saying the data source is being added and analyzed.

A screenshot of a computer

Description automatically generated

Fig 17: Data processing phase

We can see that all the files deleted from the USB drive have been recovered along with metadata.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Fig 18: Deleted files found

Now, recovering the png and mp3 files file including metadata. After that select the USB as a destination to be recovered and the files are being successfully extracted.

A screenshot of a computer

Description automatically generated

Fig 19: Successful extraction and recovery of the deleted files

Result after successfully files is extracted. The reason that I have used MP3, and PNG image formats to recover is that PNG image files contain the picture of the criminal during the murder time whereas the mp3 files contain the voice of the criminal and victim as well as their conversation.

A screenshot of a computer

Description automatically generated

Fig 20: Final proof of data acquisition

Autopsy is a rather user-friendly, open-source digital forensics tool suitable for investigating the 16GB USB device in a murder case. It efficiently deals with issues concerning legal admissibility, time constraints, data integrity, and device identification. Autopsy works on the recovery and analysis of deleted files and detailed metadata by providing a very comprehensive search with keyword, file type, and metadata search features. It uses hash functions to ensure the integrity of the data. Also, it makes forensic images in a bid to project every single data accurately. Autopsy, with its legal compliance and extensive reporting tools, enables forensic investigations to find essential evidence more efficiently and cost-effectively [7].

## Pro Discover Basic

Initial GUI of Pro Discover Basic

A screenshot of a computer program

Description automatically generated

Fig 21: Initial interface of the software

After filling the case information save the files into the appropriate location to change its extension, so that can be analyzed by the software.

A screenshot of a computer

Description automatically generated

Fig 22: Saving the files to change its extension to. Eve

Select action>add>image file to capture the image to analyze.

A screenshot of a computer

Description automatically generated

Fig 23: Adding the files that need to be changed into image files.

After that, the interface will pop up which asks to fill in the information to be filled. Select source drive> destination>split the image to 400mb>image format to pro discovers>technician name>image number>description as per requirements. Set the compression of the files to No and set the password so that an authorized person can only get access after a successful image capture.

A screenshot of a computer

Description automatically generated

Fig 24: Selection of data source and filling up the credentials required

The interface will pop up and start to capture the image of whatever evidence that has been stored/creared and deleted in the USB drive. It might take a while to capture the image so be patience.



Fig 25: Data processing phase

A screenshot of a computer error

Description automatically generated

Fig 26: Completion of the image being captured

Now, that the image has been captured go to action>capture image>select the appropriate image file that has been captured and open it. It will ask for the password to log in to see the data and evidence.

A screenshot of a computer login box

Description automatically generated

Fig 27: Geeting access to the image with the password that has been assigned on the initial phase

After a successful login attempt, we can see and analyze the deleted data as shown in the fig 28. These are the files that we need to retrieve.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Fig 28: Initial interface of the image files that have been deleted and not been deleted.

After that select the data (click on the box) that you want to retrieve. In my case, I have selected the pdf files and added a comment as evidence discovered. Right-click on the same file>copy file and select the appropriate destination to be saved for successful acquisition.

A screenshot of a computer error

Description automatically generated

Fig 29: Selecting one of the deleted files and adding comments to be retrieved

I have selected the USB drive to retrieve the PDF files to analyze them as evidence for the investigation of homicide case. The reason why I chose a PDF file is that it contains a text message from the criminal and his intention to begin this crime.

A screenshot of a computer

Description automatically generated

Fig 30: Proof of successful acquisition of data (pdf file)

Forensic research in the homicide case by exploitation of the 16GB USB drive recovered from the flat of the suspect is possible with Pro Discover Basic. It takes care of issues such as hardware compatibility, time constraints, device identification, integrity of data, and legal admissibility. Advanced searching in this tool—by keyword, file type, metadata, and pattern searching—is necessary to find relevant evidence. It has comprehensive seizure protocols, including the exact creation of forensic pictures, data integrity verification using hash functions, and custody chain maintenance. Pro Discover Basic is a very good tool for performing a full and legally sound forensic investigation since it contains all kinds of features, which are very important to find significant evidence in a case like this [8].

# **Conclusion**

In the final analysis, Autopsy and Pro Discover Basic are excellent resources for forensic analysis concerning the 16GB USB drive in this homicide case. With its sophisticated live memory capture, network analysis, and thorough metadata evaluation, Pro Discover Basic is ideal for any deep investigation and provides the highest level of data integrity and assurance of report quality. Autopsy is a free, open-source, easy-to-use tool that allows access to very powerful forensic features at a very low cost. It excels in metadata analysis, recovery of files, and the generation of reports. Since both technologies have competency in handling issues of data capture, search and seizure protocols, and compliance with the law, they are very well-suited to find crucial evidence that will enable in-depth forensic investigations in difficult instances [9].

# **References**

[1] Fakiha, B.S., 2022. Cybersecurity: Analysis and Application of ProDiscover Forensic Toolkit. *Social Medicine*, *15*(3), pp.146-152.

[2] Basso, C. and Stone, J.R., 2022. Autopsy in the era of advanced cardiovascular imaging. *European Heart Journal*, *43*(26), pp.2461-2468.

[3] Kävrestad, J., Birath, M. and Clarke, N., 2024. Autopsy Forensics. In *Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications* (pp. 179-193). Cham: Springer International Publishing.

[4] Bhatt, S. and Garg, G., 2021, July. Comparative analysis of acquisition methods in digital forensics. In *2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 129-134). IEEE.

[5] Bhatt, S. and Garg, G., 2021, July. Comparative analysis of acquisition methods in digital forensics. In *2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 129-134). IEEE.

[6] Dubey, H., Bhatt, S. and Negi, L., 2023. Digital forensics techniques and trends: a review. *Int. Arab J. Inf. Technol.*, *20*(4), pp.644-654.

[7] Pooryousef, V., Cordeil, M., Besançon, L., Hurter, C., Dwyer, T. and Bassed, R., 2023, April. Working with forensic practitioners to understand the opportunities and challenges for mixed-reality digital autopsy. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (pp. 1-15).

[8] Javed, A.R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K. and Gadekallu, T.R., 2022. A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access*, *10*, pp.11065-11089.

[9] Al Jouhi, M. and Al Hosani, S., 2022. Windows Forensics Analysis. *Emirati Journal of Policing & Security Studies*, *1*(1), pp.4-11.