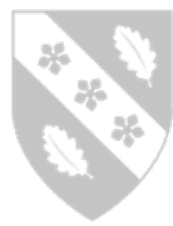


ACCD5000

Computer Forensics



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Dr. Nitheesh Murugan Kaliyamurthy

Content

1.	Research Report.....	3
1.1.	What is Digital Forensic?	3
1.2.	What is Computer Forensic?	3
1.3.	History of Computer and Digital Forensics.	3
1.4.	Applications of Computer Forensics and Digital Forensics.	4
2.	Investigation and Reporting.....	5
2.1.	Chain of Custody.....	5
2.2.	Investigation process.....	5
2.3.	Tool used.....	6
2.4.	Digital Forensics Report.....	7
3.	Annexure	9
3.1.	Process for the creation of the disk image:	9
3.2.	Screenshots of the tools used:.....	11
4.	References	13

1. Research Report

1.1. What is Digital Forensic?

Digital Forensics is a branch of forensics science specialized in digital devices [1]. It is based on recover, analyse and investigation of documents found in digital devices, often in relation to mobile devices and computer crime [2].

Digital Forensics is involved when mobile devices, social media, cloud services, and IoT devices are involved.

The term was first created as a synonym of Computer Forensics but was later described as the investigation over all digital device, capable of storing data [2].

1.2. What is Computer Forensic?

Computer Forensics is a sub-branch of Digital Forensics, centred around the evidence found in computers [3]. It aims to systematically investigate digital media, ensuring integrity, to identify, preserve, recover, analyse, and present factual findings and expert opinions concerning digital information.

Computer Forensics is not always associated with crimes. It can be used for data recovery for example.

1.3. History of Computer and Digital Forensics.

Computer Forensics appeared in the early 80s, with the increasing accessibility of computers for people. With this increase, a new type of criminality appeared: computer-related crimes.

Computer Forensics was created as a method to recover and investigate digital evidence for use in court [3]. At this time, most cybercrimes were made on computers, but with the evolution of technologies over the years, cybercrimes were extended over mobile devices, social networks, internet, etc. From this emerge the distinction between Computer Forensics and Digital Forensics, the first one being mostly centralized around computer, and the second one being centralized around other types of systems, like social networks, internet, etc.

In today's world, Digital Forensics defines all types of technology related forensics process. And depending on the media, Digital Forensics can be devised into sub-branches: Computer Forensics for computers, Mobile Device Forensics for mobile devices, etc.

1.4. Applications of Computer Forensics and Digital Forensics.

The most common application of Computer Forensics in today's world is for Law Enforcement Investigations. It is used to investigate computer-related crimes, such as hacking, identity theft, etc. It is also used to help investigations on non-computer-related crimes, such as analysing the victim's personal computer to determine clues [4].

Computer Forensics is also used in civil litigation cases, such as fraud, employment disputes, etc.

Finally, Computer Forensics can be used in data recovery.

On the other hand, one of the main uses of Digital Forensics is for cases like cyberbullying, defamation, and online fraud [4].

2. Investigation and Reporting

2.1. Chain of Custody.

The most important part of the process of evidence documentation is the chain of custody. The principle of the chain of custody is to ensure that the evidence is authentic to be relevant in the court of law. The evidence must always be in the custody of a person designated to handle it and for which it was never unaccounted.

The process of chain of custody must follow important and necessary steps, which some of them are described below:

- 1) A unique identifier for the evidence.
- 2) The name and signature of the sample collector.
- 3) The details of each evidence:
 - a. Date and time of collection.
 - b. Type of analysis required.
- 4) The name and signature of everyone involved in the process.

Each time the charge of evidence is changed, an entry of signature, date, and time is necessary for the chain of custody form.[5]

2.2. Investigation process

The investigation team is composed as follow:

- The photographer:
 - o Documents the crime scene and physical evidence using photography.
 - o Ensures that photographs accurately depict the scene and relevant evidence.
 - o Maintains chain of custody for photographic evidence to ensure its admissibility in court.
- The investigator:
 - o Conducts interviews and collects information related to the incident, retrieving digital evidence from various devices while ensuring its integrity and legal admissibility.
- The incident responder:
 - o Reacts to security incidents in real-time, working with others to secure evidence and minimize damage.
- The incident analyser:
 - o Untangles the incident or breach, pinpointing potential evidence sources and prioritizing investigation based on impact.
- The witness:
 - o Provides testimony regarding the handling and analysis of digital evidence.

- Ensures that testimony is accurate, truthful, and consistent with findings.
- Responds to questions from legal counsel and the court regarding the investigation process and evidence.
- Documenter:
 - Documents every step of the investigation.
 - Maintaining detailed logs for evidence collection, analysis, and chain of custody.
 - Prepares comprehensive reports summarizing findings and conclusions.
- The examiner:
 - Analyses digital evidence with care, preserving its integrity and documenting everything for proper review.
 - Follows forensic protocols to ensure evidence is admissible in court.
- Manager:
 - Guides the team through the investigation.

The Standard Operating Procedure (SOP) is a documented procedure outlining the steps and protocols for conducting digital investigations. It is to make sure that the investigation is carried out in respect with legal and ethical considerations. It also includes guidelines for handling different types of digital evidence, maintaining chain of custody, and protecting the integrity of data.

The order of SOP with the investigation team is as follows:

The photographer > The incident responder > The analyser > The examiner / The investigator
 During all this process the documenter must document the location of all the machines, computers, screen and evidence which are the layout of the crime scene, and the witness must watch everything to offer formal testimony in court.

2.3. Tool used.

For this coursework, I used a few tools depending on what I needed to do [[Cf. 3.1](#) and [3.2](#)].

For the creation of the image, I used FTK Imager. The reason I used it is because when creating the image, the application check if the Hash value of the image is the same as the Hash value of the disk, in order to ensure the integrity of the evidence in a court of law.

For the analysis of the image, I used two different tools: Forensic Toolkit 7.6 and Autopsy.

The reason I used two different tools is because it can give me different approaches and those tools does not give the same type of information.

With Autopsy, I was able to see the Deleted files of the disk, which wasn't the case with FTK 7.6. However, FTK 7.6 allows me to see more properties inside a document.

Some of the files inside the image were encrypted, so I used Microsoft Visual Studio and C++ to decrypt those files.

2.4. Digital Forensics Report.

This is based on lecture notes and an article of the Forensics Focus website [6].

Report of Examination

Examiner: MAFILLE Thomas – 2325532

Date: 25/04/2024

Overview – Case Summary:

For the Computer Forensics class, a fake cyberbullying scenario has been created to allow the student to perform a forensics investigation to see if the cyberbullying append or not, and who is the accused.

Physical Evidence:

E1. One (1) hard disk

E2. One (1) USB-Stick

The items listed in the “Physical Evidence” section of this report remained in a secure chain of custody of the computer forensics student throughout the analysis process.

Objectives:

I am asked to complete forensics analyse over the files inside the physical evidence, and from those evidence, deduce if there is a case of cyberbullying or not.

Forensic Analysis:

1) 11/03.

The evidence has been gathered by respecting the chain of custody and secured inside a faraday pouch.

2) 11/03.

An image of the disk is created [[Cf. 3.1](#)] using Access Data FTK Imager [7].

3) 22/04.

Using applications called Forensic Toolkit [8] and Autopsy [9], I can open the image files to analyse the content inside it [[Cf. 3.2.](#)]. Caution has been taken to ensure the time and date were set to UTC.

Inside the image files and using those applications, I can read the content inside the disk.

4) 23/04.

Using the same applications, I continue analysing the image files.

5) 24/04.

Using the same applications, I continue analysing the image files.

Relevant Findings:

During the analyse, I have found screenshots of discussion between the victim and 5 other persons on different applications: Facebook Messenger, Twitter/X and WhatsApp.

I have also found a document called “Police Report.rar”, which needed to be extract because FTK and Autopsy cannot open .rar files. Once extracted, I saw the report was encrypted, and using a password found in the “Readme.txt” file, I was able to open the .rar file, and I extracted two encrypted files. To open those encrypted files, I needed to use the “encrypt_file.cpp” file in order to decrypt the files. Using Microsoft Visual Studio and the “encrypt_file.cpp” file, I was able to decrypt the files into a .png format. Those files were the Police Report, which contain the name on the victim (Emily) and a possible suspect found by the police (Justine Elias).

Conclusion

Using the screenshots of the discussions, I can say that there is a case of Cyberbullying.

3. Annexure

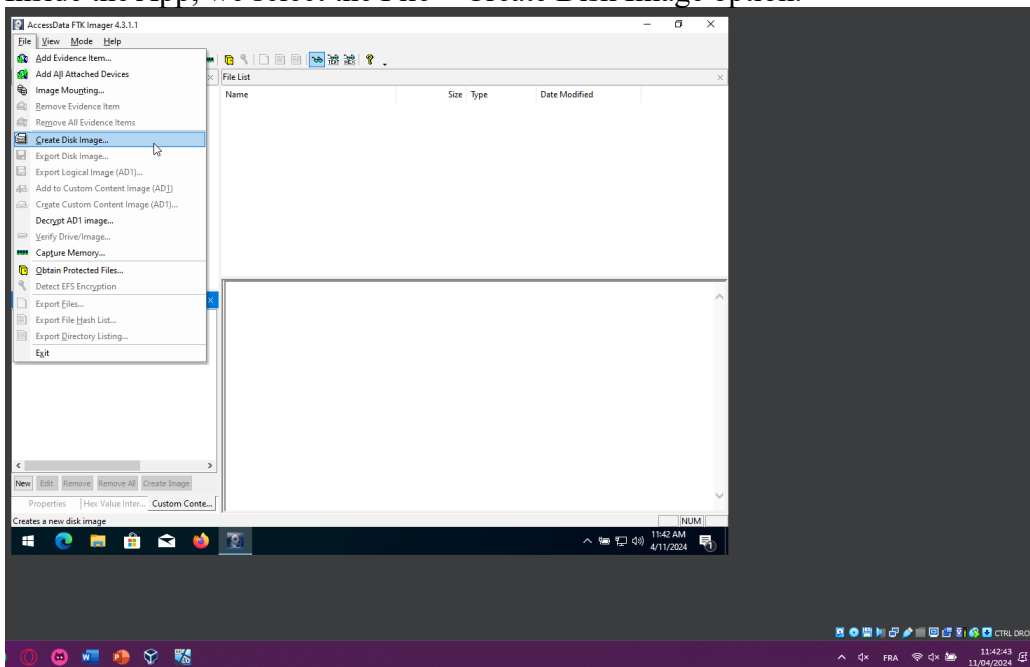
3.1. Process for the creation of the disk image:

I firstly open a Virtual Machine which represents a secured and protected environment. I make sure the VM is not connected to internet to ensure that no files can be changed by someone via the internet.

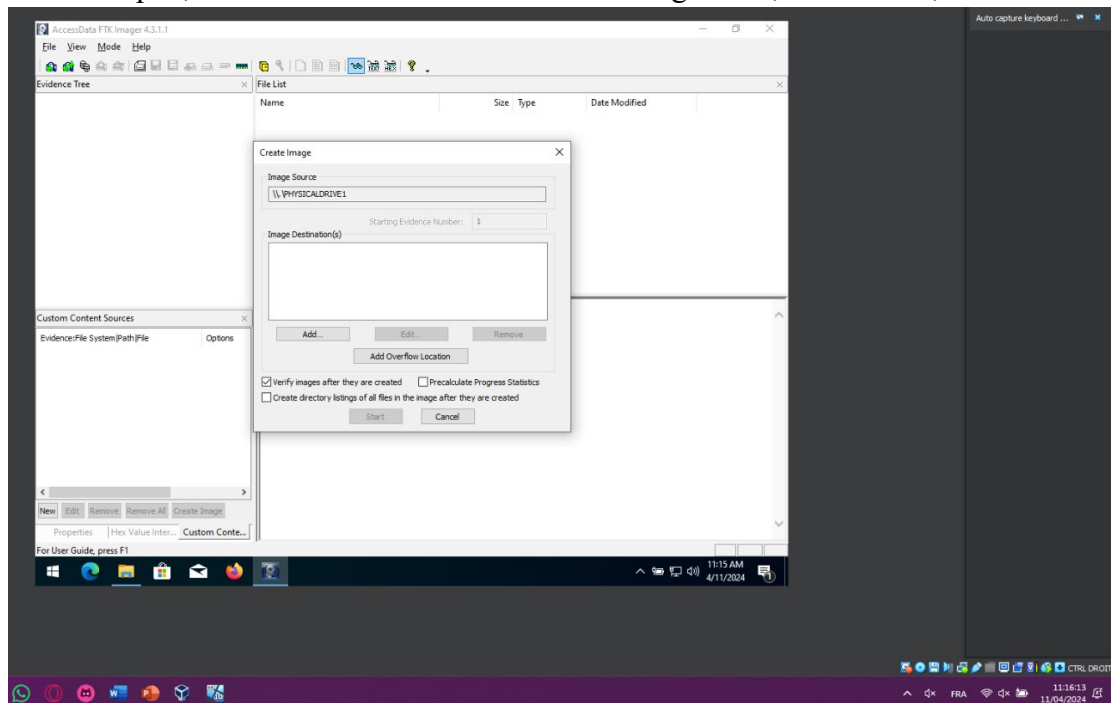
When I made the screenshots, I already created the image of the disk. It is for this reason that the VM is still connected to internet. The screenshots were made after to process, during the creation of this report to illustrate the process.

With the evidence files on a USB-stick, I used the application called AccessData FTK Imager to create the disk image.

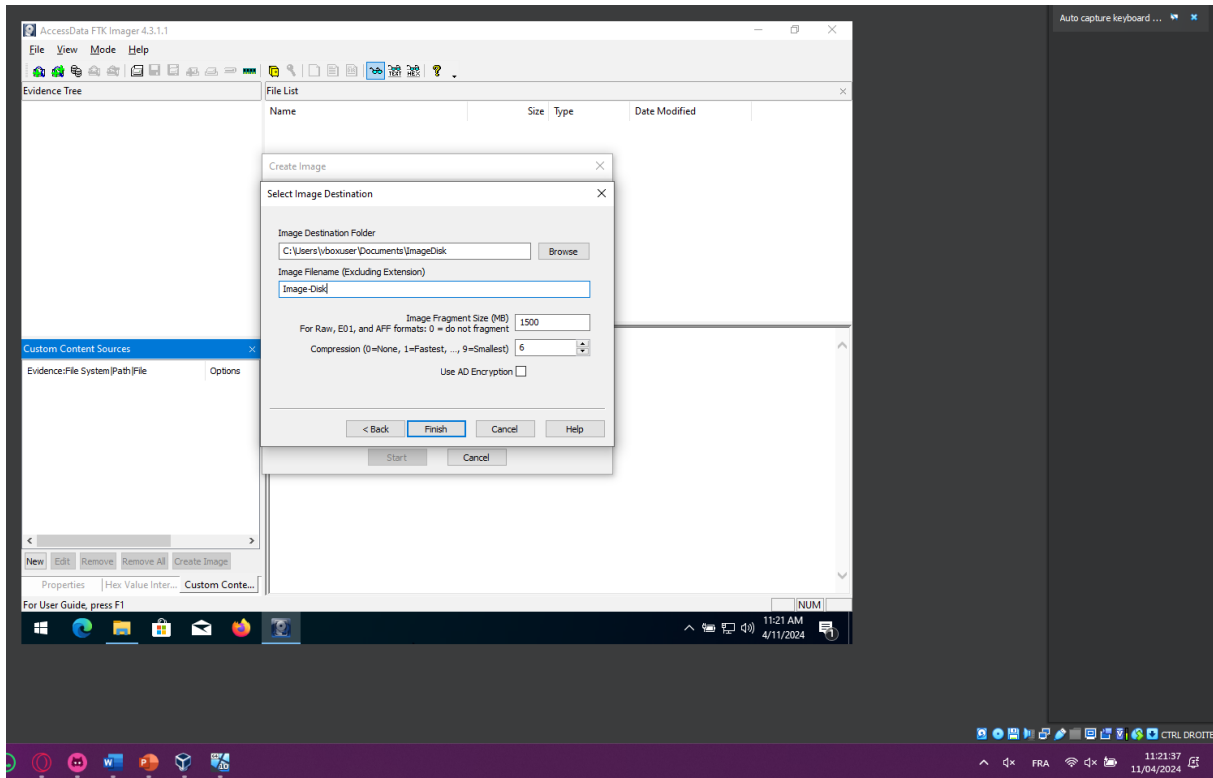
Inside the App, we select the File > Create Disk Image option.



Once the window is open, I can select the disk to create the image from, in that case, the USB-flash.

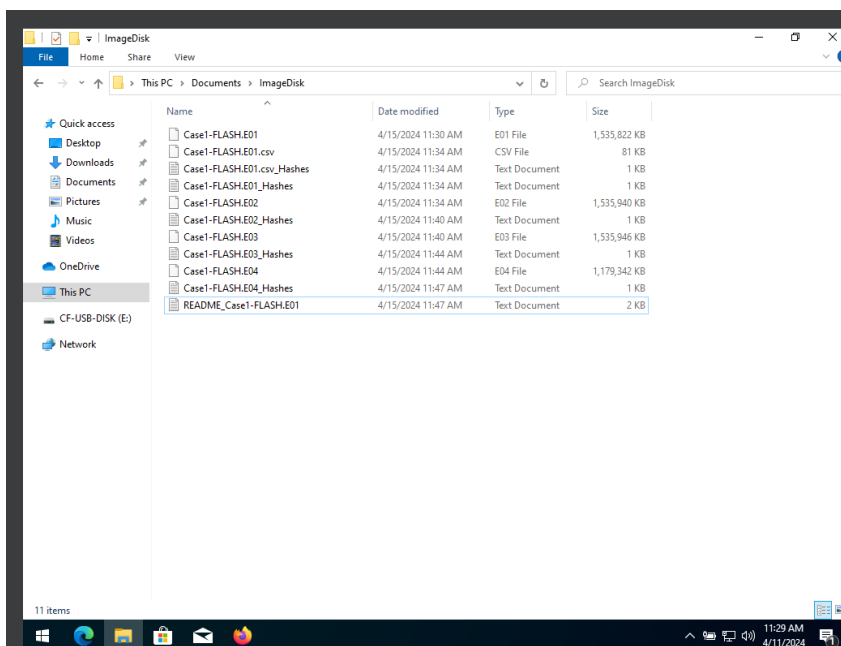


When I click on Add for the image destination, a new window open called “Select Image Destination” in which I can choose the path of the destination folder and set the name if the Image file. I can also decide to fragment the image file, if necessary, and choose the type of compression. *(In the screenshot below, I decided to fragment the image file into files of size of 1500MB)*



Once I clicked “Finish”, I can click on “Start” inside the “Create Image” window to create the image files.

Once the creation is finished, the files can be found inside the Destination folder.



3.2. Screenshots of the tools used:

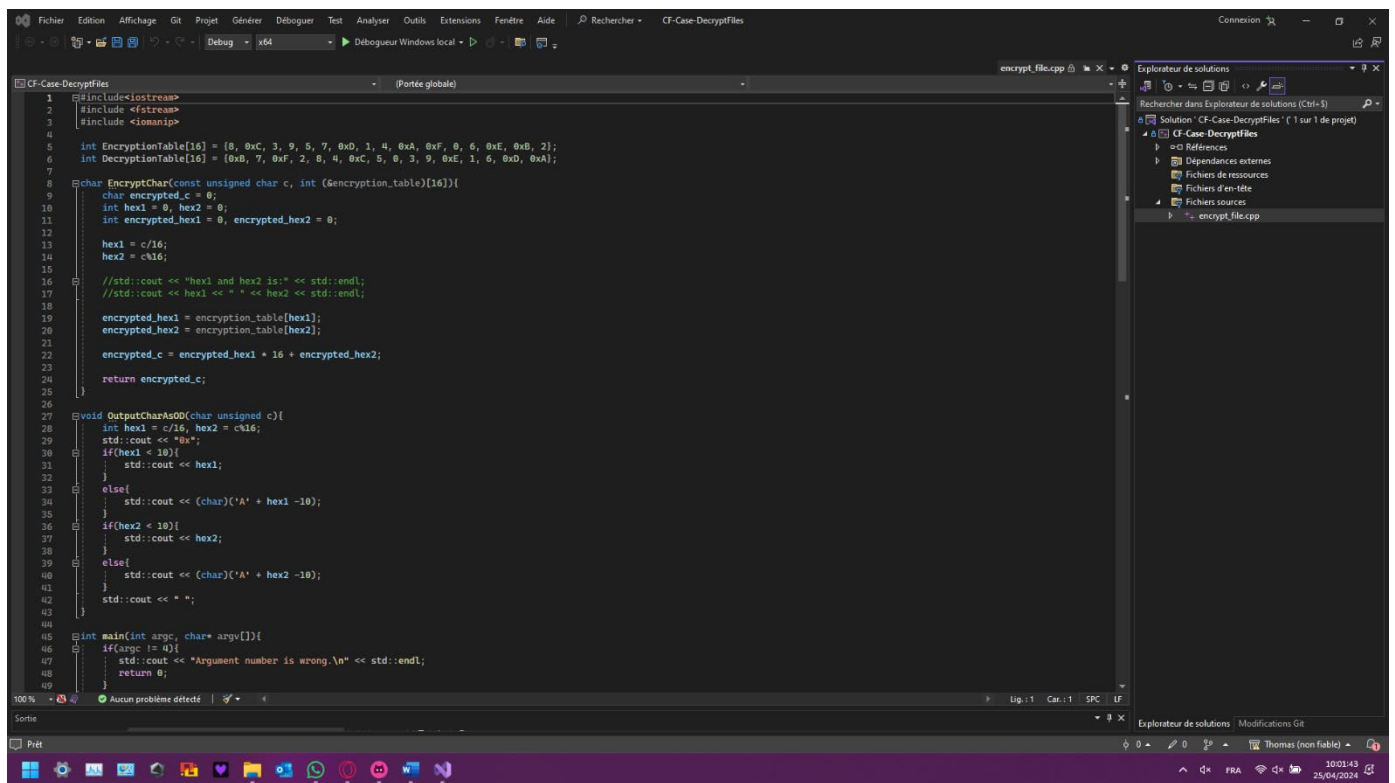
Forensic Toolkit:

The screenshot displays the Forensic Toolkit (FTK) interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, and Help. The main window is divided into several panes. On the left, the 'Evidence Items' pane shows a tree structure of the case, including 'Case1-FLASH.E01', 'Partition 1', 'STUFF [NTFS]', and various files like 'IMG_0101.jpg'. The central pane shows the 'File Content' of a selected file, displaying a WhatsApp chat message from 'Seer Musta'. The message text is: 'The world is revolving around me, and I control the metaphase. I can see you, but you can't see me! Be watchful, the legions are coming to your neighborhood...'. The bottom pane shows a 'File List' with columns for Name, Label, Item #, Ext, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, Accessed, and Modified. The list contains various image files (IMG_0101.jpg, IMG_0102.jpg, etc.) and their corresponding metadata.

Autopsy:

The screenshot displays the Autopsy 4.21.0 interface. The top menu bar includes Case, View, Tools, Window, and Help. The main window is divided into several panes. On the left, the 'Data Sources' pane shows a tree structure of the case, including 'Case1-FLASH.E01', 'Partition 1', 'STUFF [NTFS]', and various files like 'IMG_0101.jpg'. The central pane shows a 'File List' with columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and MD5. The list contains various image files (IMG_0101.jpg, IMG_0102.jpg, etc.) and their corresponding metadata. The bottom pane shows a 'Hex View' of a selected file, displaying the raw data in hexadecimal and ASCII format.

Microsoft Visual Studio 2022:



4. References

- [1] [Online]. Available: <https://www.interpol.int/How-we-work/Innovation/Digital-forensics>.
- [2] [Online]. Available: https://en.wikipedia.org/wiki/Digital_forensics.
- [3] [Online]. Available: https://en.wikipedia.org/wiki/Computer_forensics.
- [4] [Online]. Available: <https://www.ibm.com/topics/computer-forensics>.
- [5] [Online]. Available: <https://www.ncbi.nlm.nih.gov/books/NBK551677/>.
- [6] [Online]. Available: <https://www.forensicfocus.com/articles/writing-dfir-reports-a-primer/>.
- [7] [Online]. Available: <https://www.exterro.com/digital-forensics-software/ftk-imager>.
- [8] [Online]. Available: <https://www.exterro.com/digital-forensics-software/forensic-toolkit>.
- [9] [Online]. Available: <https://www.autopsy.com>.