eForensics

VOL. 11
NO. 09

ISSN 1733-7186

THE COMPLETE GUIDE TO USING AUTOPSY

LEARN HOW TO PERFORM A **FORENSIC ANALYSIS** USING

EXPLORE HOW TO USE AUTOPSY, FROM STARTING A CASE TO **MANAGING**

HUNT HACKERS USING AUTOPSY ON A MACOS

USING **AI** AND **HIGH-TECH TOOLS**, REDEFINE

EDITOR'S WORD

Dear Readers

Today you can get a super issue devoted to the Autopsy tool. I have read every article, and they are a great source of information on this tool. You can read about other tools as supplementary material. With the help of all this knowledge, you will be armed to solve every case and rank among the industry's top experts. Why Autopsy? A lot of people have mentioned this toolkit to me. As stated in the Kate Libby article: "According to the project page (Autopsy, n.d.), Autopsy is an open-source, cross-platform digital forensics toolkit that offers a wide range of features and capabilities to aid investigators in the retrieval and analysis of digital evidence. Autopsy, also known as the Sleuth Kit, is a widely used open-source digital forensics tool that provides a comprehensive suite of features for forensic investigators. It was originally developed by Brian Carrier and has since gained widespread adoption in the digital forensics' community due to its versatility, reliability, and cost-effectiveness." With the help of our issue, you can learn more about Autopsy, understand its importance in digital forensics, and discover some of its main features. Two articles by Paulo Pereira that introduce the most recent version of Autopsy and demonstrate how to conduct digital forensics analysis using this tool will serve as the issue's introduction. You will find a fantastic article by Israel Torres about how to use Autopsy on a macOS image to hunt down hackers inside. Wilson Mendes has written an article that is sure to cause a stir. "This article delves into the exciting world of forensic investigation technology, exploring how technological innovations have revolutionized the field, from analyzing images and videos to recovering data from electronic devices. Throughout this article, you will discover how artificial intelligence, computer forensics, and other high-tech tools are redefining the limits of case solving and contributing to the relentless pursuit of justice."
In conclusion, I strongly encourage you to read all the articles included in this issue, as the technology used in forensic investigation is a powerful tool and a constantly evolving field that challenges researchers to constantly adapt and improve their skills. We invite you on "a fascinating journey into the world of forensic investigation technology".
We would like to thank our authors, reviewers, editors, and proofreaders for their valuable contributions that made this publication possible. It was a pleasure working with you and learning from your insights.
We look forward to continuing to collaborate with you and inviting others to create more exceptional content with us. Together, we can make a meaningful impact in our field.

Don't miss out on this must-read issue!

Best regards,
Ewa & the **eForensics Team**
ewa.dudzic@eforensicsmag.com

EDITOR-IN-CHIEF
JOANNA KRETOWICZ
JOANNA.KRETOWICZ@EFORENSICSMAG.COM

ASSOCIATE EDITOR
EWA DUDZIC
EWA.DUDZIC@EFORENSICSMAG.COM

Cover Image
Wiktoria Bukowska

Advisory Board
Paulo Pereira
Alessandro Lofaro, J Sc
Kharim Mchatta

Cover Design
Wiktoria Bukowska

Reviewers
David Michaud, Gabriel Carvalhaes, Ranjitha R, Davide Gabrini, Hammad Arshed, Jan-Tilo Kirchhoff, Dauda Sule, Yousuf Zubairi, Alex Giles, David von Vistauxx, Leighton Johnson III, Bartek Adach

PUBLISHER HAKIN9 MEDIA SP. Z O.O. 02-511 WARSZAWA UL. BAGATELA 10/30 EFORENSICSMAG.COM

AUTOPSY 4.21 VERSION

PAULO PEREIRA, PHD

Introduction

This article shows you how to start a case with the new version 4.21.0 of Autopsy, one of the pioneering tools responsible for the digital change in forensic investigation in recent years. The article itself does not claim to be a complete guide for a person to use Autopsy. For this, there are several sources on the web. However, an introduction is made on how to start a case in Autopsy, using an image called SUSPECT_LAPTOP, which was used in Belkasoft training and for which I received permission to use.

Version 4.21.0

Version 4.21.0 of Autopsy brings important changes over version 4.20.0. According to the repository of the tool, there are the following changes:

DIGITAL FORENSIC ANALYSIS USING AUTOPSY 4.21.0

PAULO PEREIRA, DIFIR

Introduction

This article shows a forensic analysis using Autopsy 4.21.0. The *SUSPECT.EO1* file is a disk image case study and is evidence used in Belkasoft's *X* training and CTF challenge. The article is not intended to be a complete analysis of this image because this image has a lot of detail and has an investigative complexity that would require more than one article. In this way, some parts will be analyzed with the intention of showing the use of Autopsy.

Operating System Details

Forensic analysts often ask, “Where do we start?” This question does not have one correct answer; for example, start here or start with this evidence. Often, the analyst's expertise defines where an investigation begins. Starting with the operating system (Figure 1) can be a decision that helps the analyst in identifying the name of domain accounts, structure of accounts registered in the system and the specific artifacts that were intended for the compromise of that system.

AUTOPSY: THE DIGITAL FORENSICS TOOLKIT

KATE LIBBY

Introduction

In today's entangled and bustling digital age, the need for and importance of digital forensics cannot be overstated. As technology advances, so do the methods by which individuals commit cybercrimes and hide digital evidence. In response to these challenges, digital forensic investigators rely on powerful tools and techniques to uncover hidden information, investigate cybercrimes, and support the efforts of law enforcement.

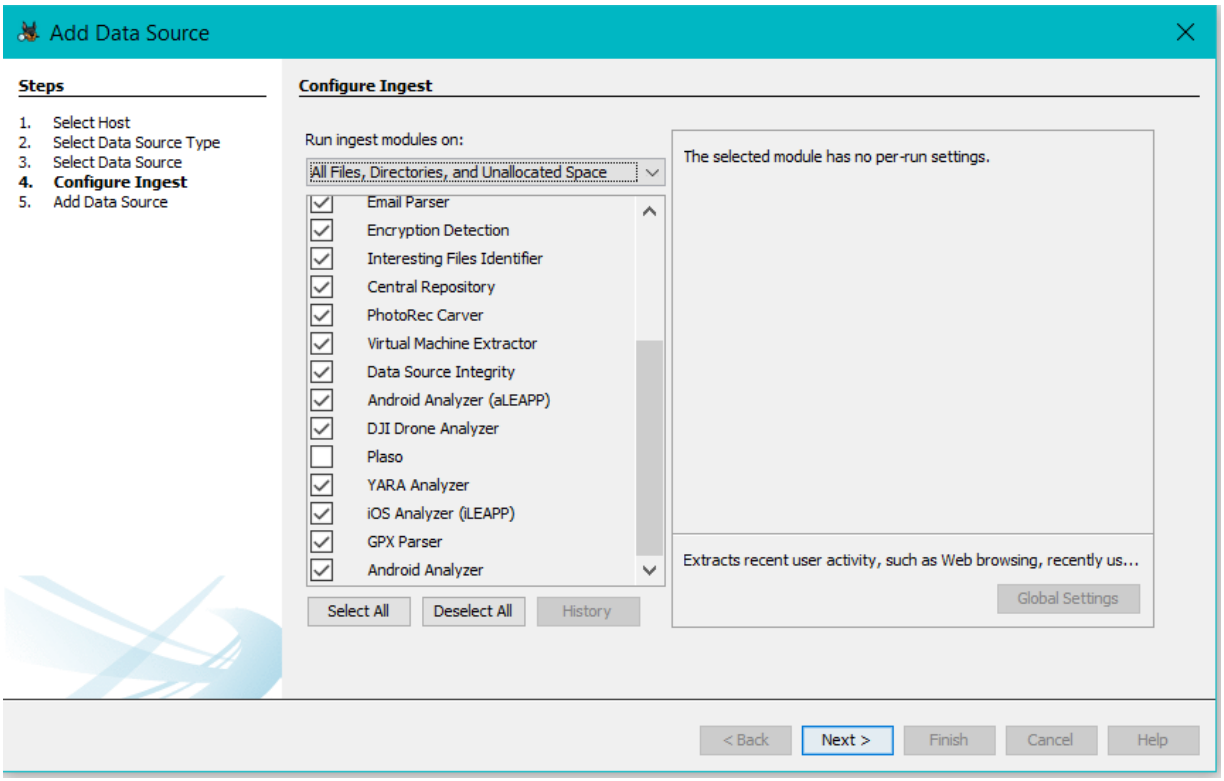
One such indispensable tool in the digital forensics' arsenal is Autopsy.

Autopsy is an open-source, cross-platform digital forensics toolkit that offers a wide range of features and capabilities to aid investigators in the retrieval and analysis of digital evidence according to the project page (Autopsy, n.d.). This essay explores Autopsy, its significance in digital forensics, and its key features, from starting a case to managing the contents of artifacts and everything in between.

Autopsy, also known as The Sleuth Kit, is a widely used open-source digital forensics tool that provides a comprehensive suite of features for forensic investigators. It was originally developed by Brian Carrier and has since gained widespread adoption in the digital forensics' community due to its versatility, reliability, and cost-effectiveness. Autopsy is available for Windows, macOS, and Linux, making it accessible to a wide range of users.

The Significance of Digital Forensics

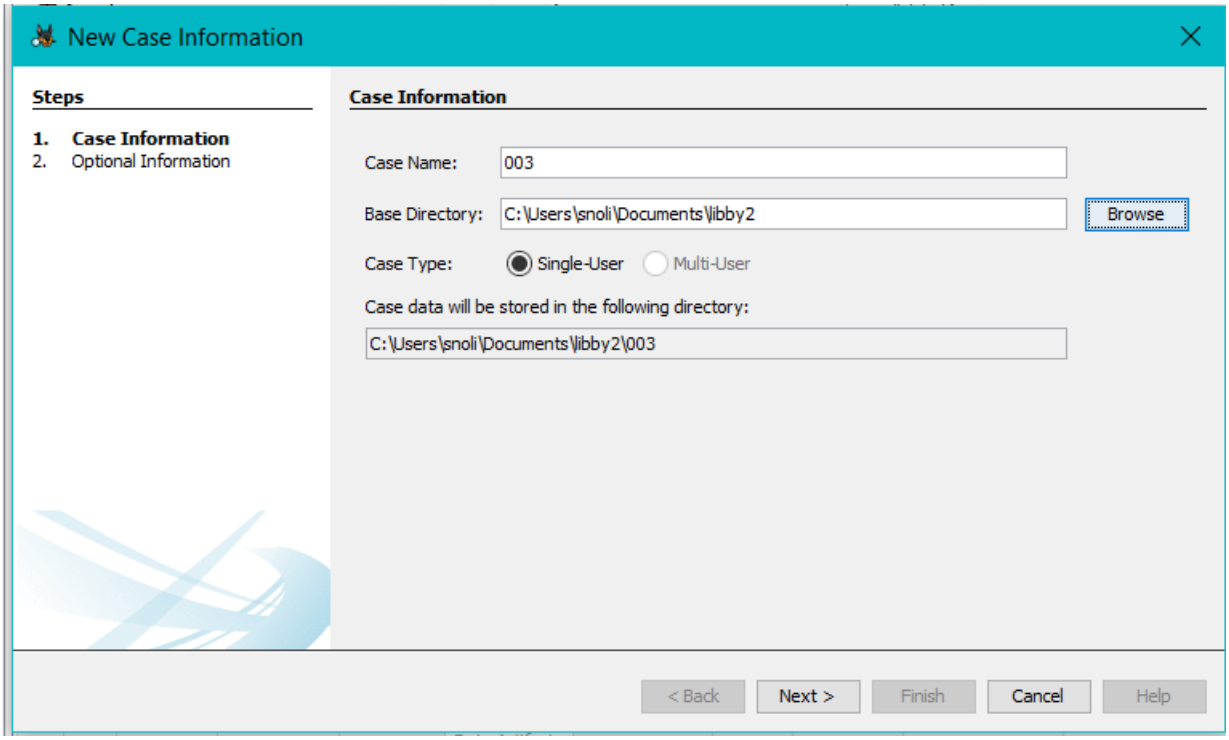
Digital forensics is the process of collecting, preserving, analyzing, and presenting electronic evidence in a legal context. It plays a vital role in criminal investigations, corporate security, incident response, and sometimes, civil litigation. With the increasing reliance on digital devices and the internet, digital evidence has become central to solving crimes and establishing culpability. Consequently, the tools and techniques used in digital forensics must continually evolve to meet the demands of modern investigative processes. Regarding Autopsy, the team at Basis Technologies are continuing to innovate the platform by adding new features, such as ingest modules, to expand the range of devices and data types.

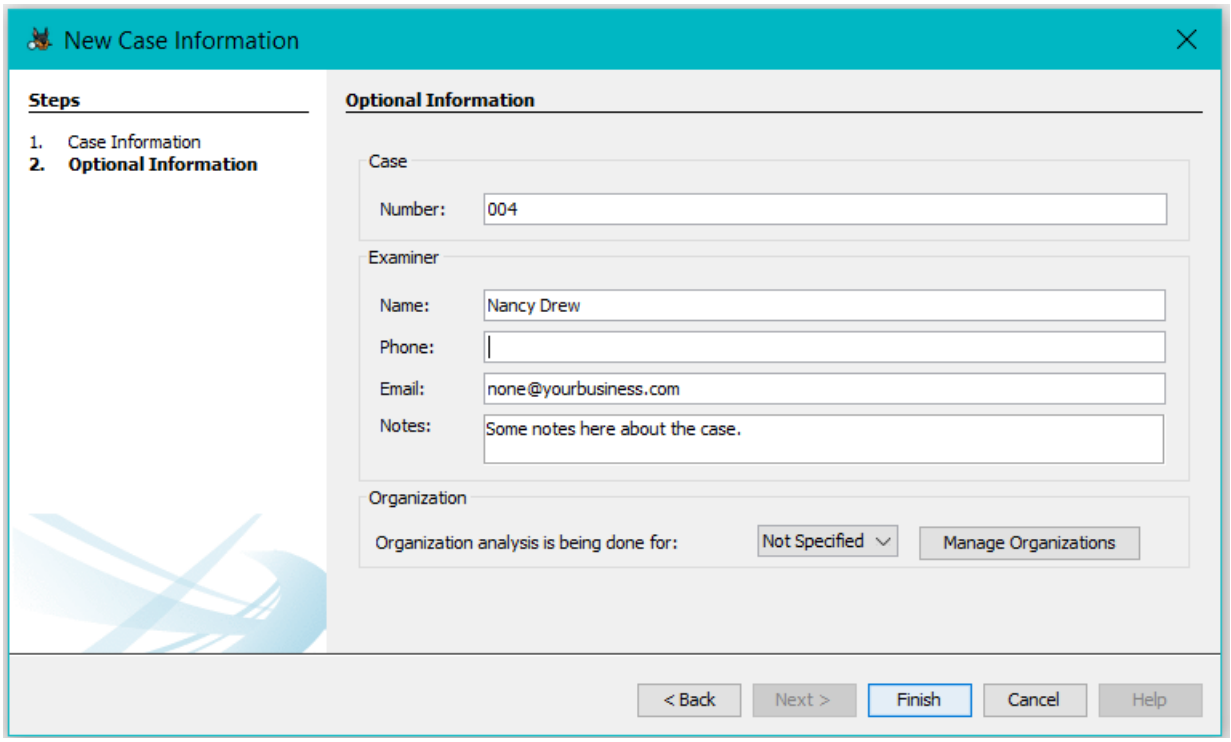


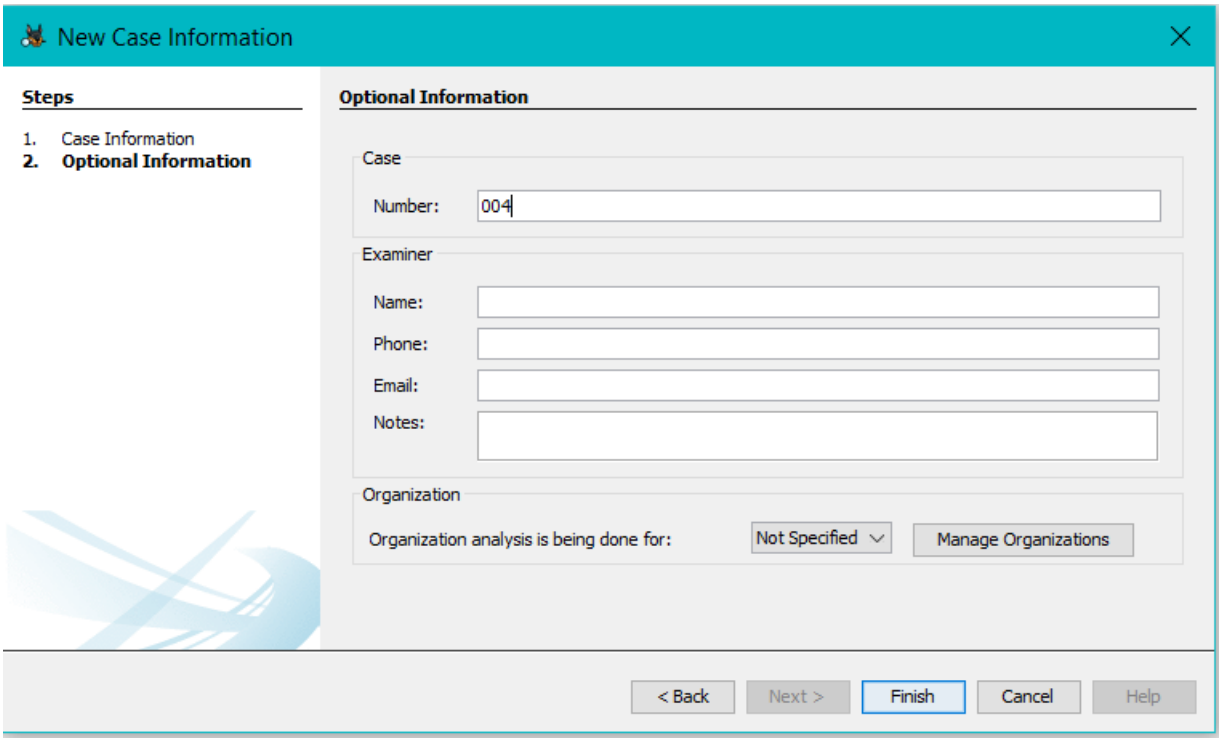
Key Features of Autopsy

Before we dive into earning our forensic wings, we must first explore some key features of Autopsy. Learning these features will enable us to navigate the framework more efficiently, thus allowing us to investigate much easier and with a bit more organization.

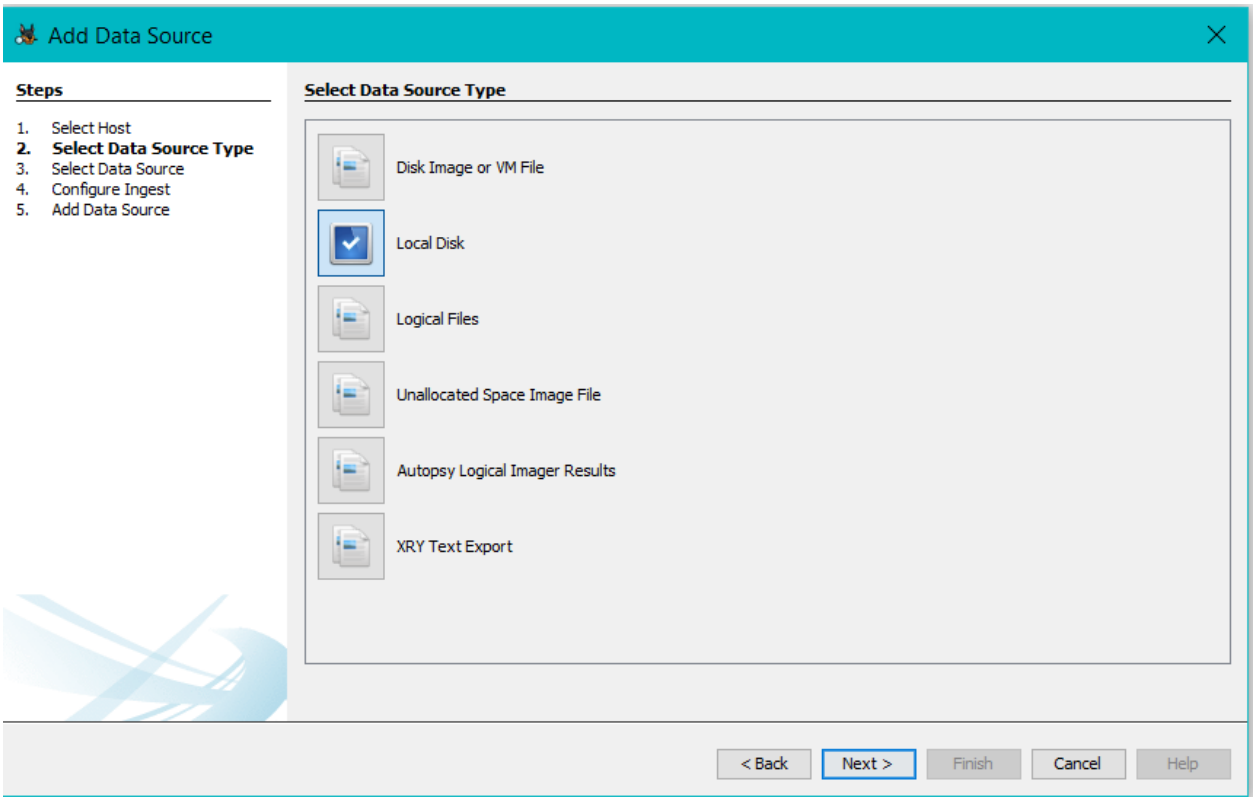
When we start Autopsy and choose to establish a new case, we are greeted with the following input fields. To move on to the next screen you must at least enter a case number. After that you can choose to populate the next step in case creation, or just move on without providing any information.



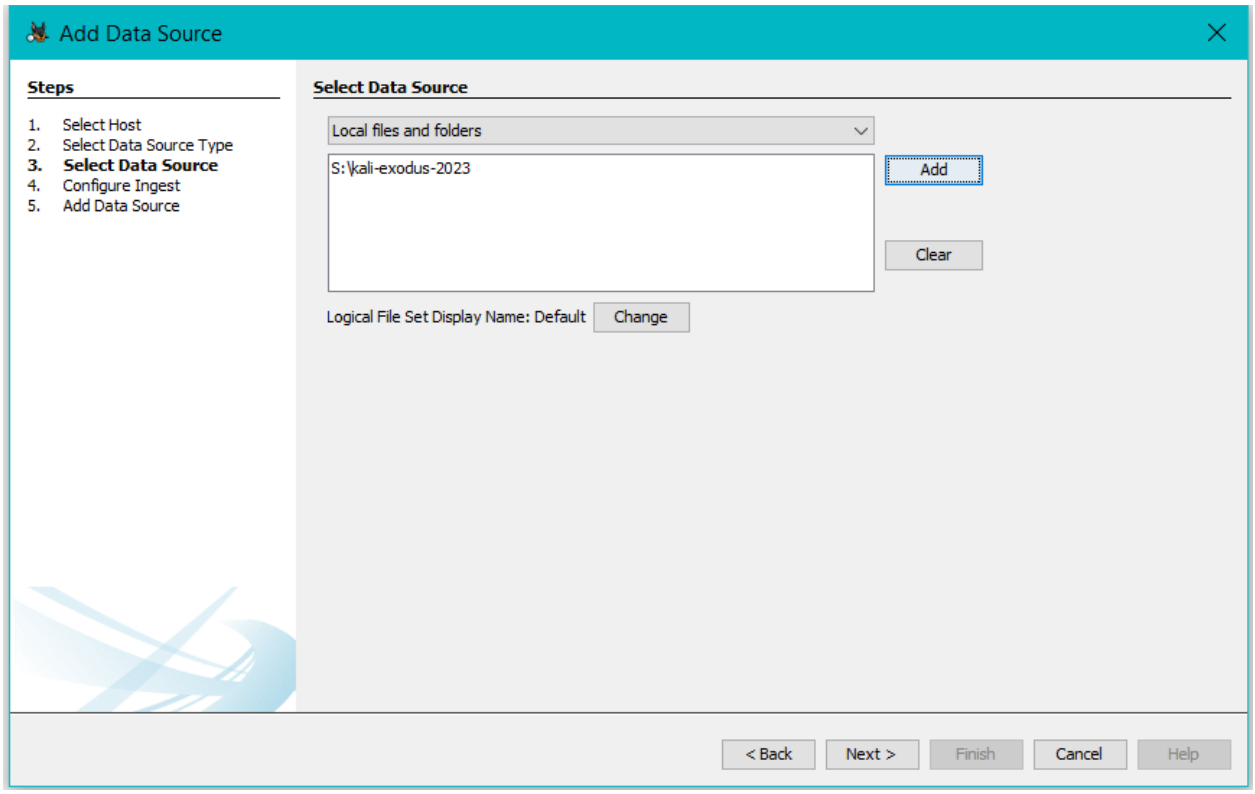




Now, we can move on to adding our data sources on which we want to perform digital forensics. As you can see from the screenshot below, we have a variety of options available to us.



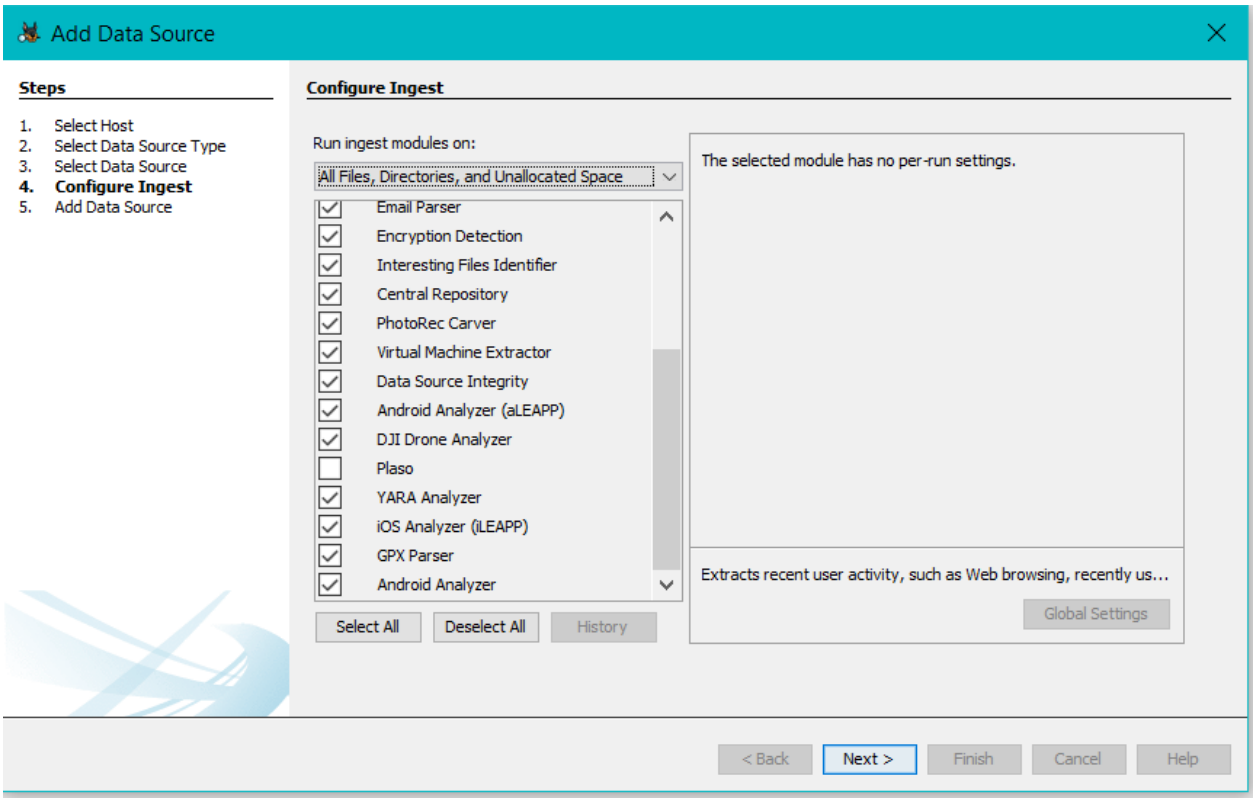
If we selected to add data from local files and folders, we must specify the location. I have selected my S:\ drive to analyze some data archives.



As far as key features are concerned, that is pretty much all it takes to establish a case and select a data source to analyze. The other features are a bit more advanced and specific depending on the type of data we are dealing with.

File System Analysis

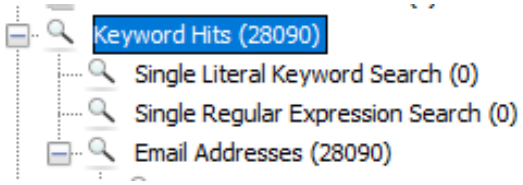
Autopsy supports the analysis of various file systems, including NTFS, FAT, exFAT, HFS+, Ext2/3/4, and UFS. This versatility ensures that investigators can examine evidence from a wide range of storage devices, such as hard drives, USB drives, drone embedded storage and memory cards. During the ingest process of the data, we can select which ingest modules we want to use, or we can select them all. I usually select them all because different types of data can be compiled on the same device.

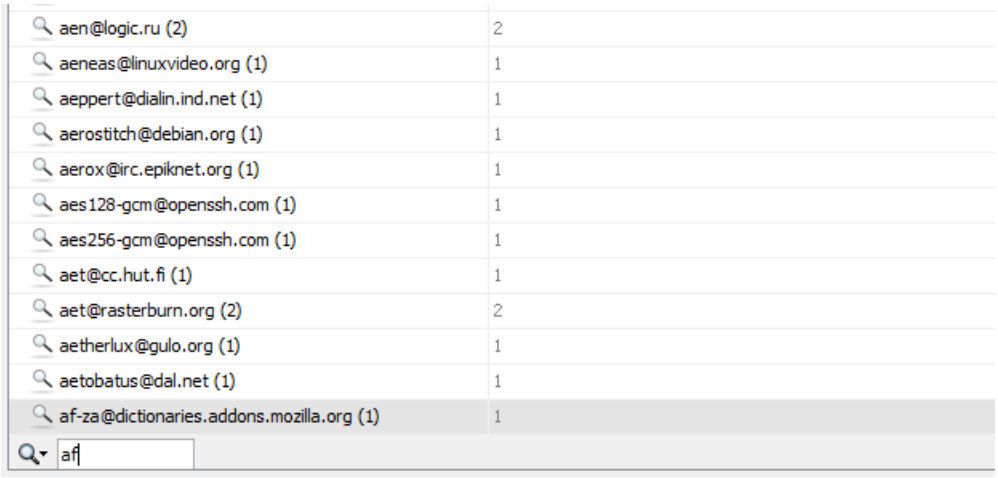


There are also plugin settings we can configure as well. Autopsy allows for developers to submit ingest modules for approval, such as Python modules (sleuthkit, n.d.).

Keyword Searching

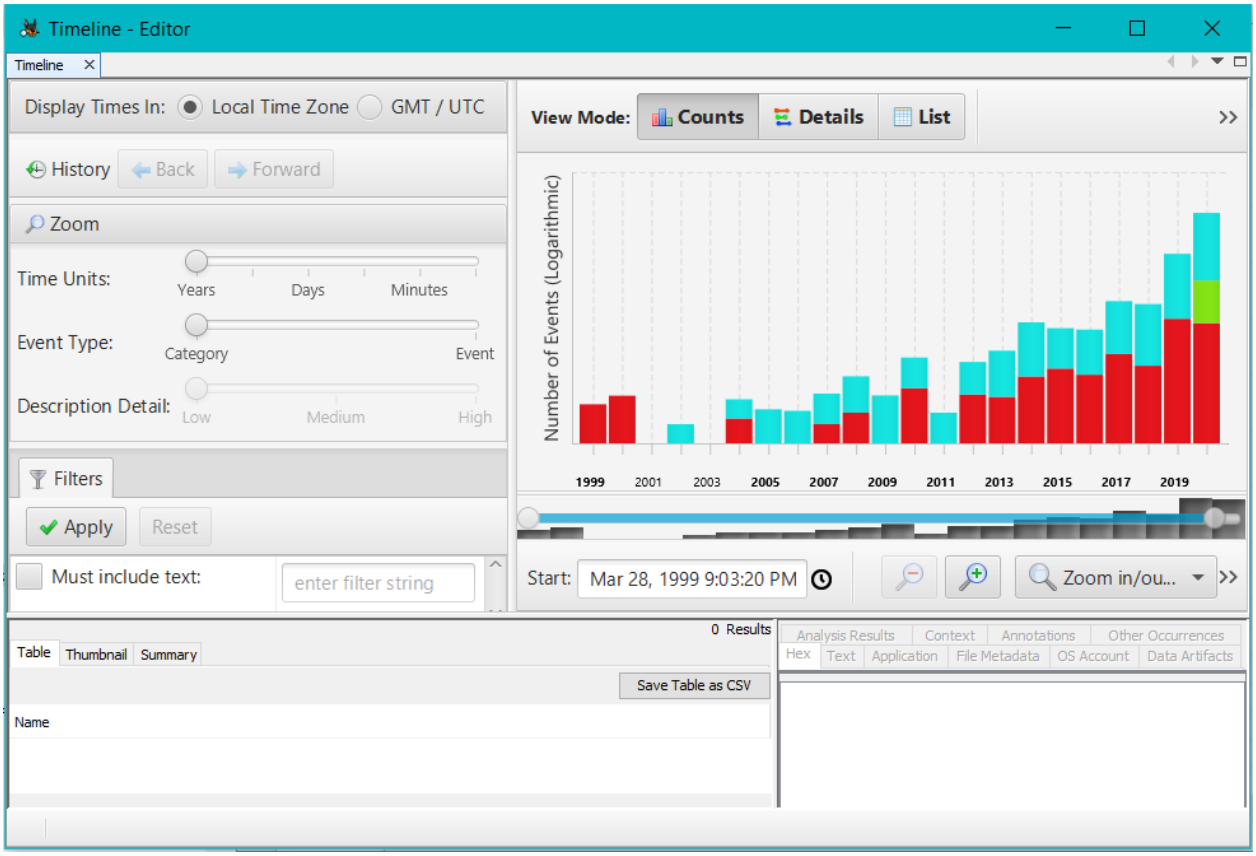
Autopsy will automatically search for keywords in accordance with the ingest modules and allows investigators to search for specific keywords or patterns within files and unallocated space. This feature is invaluable for locating crucial pieces of evidence hidden within a vast amount of data. All you have to do is select the main window and begin typing the keyword you are looking for.



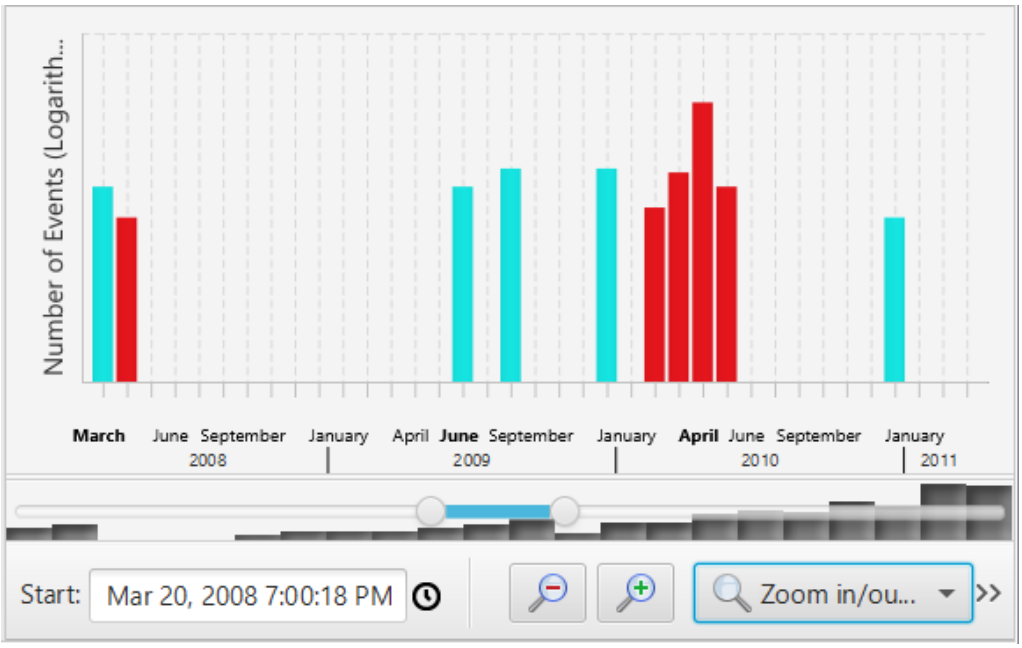


Timeline Analysis

Autopsy provides a timeline view that helps investigators reconstruct events and activities by analyzing file timestamps, including creation, modification, and access times. This is especially helpful when dealing with video artifacts; these items can be critical for establishing a sequence of events in a case.



You can provide filters as well to view the timeline differently.

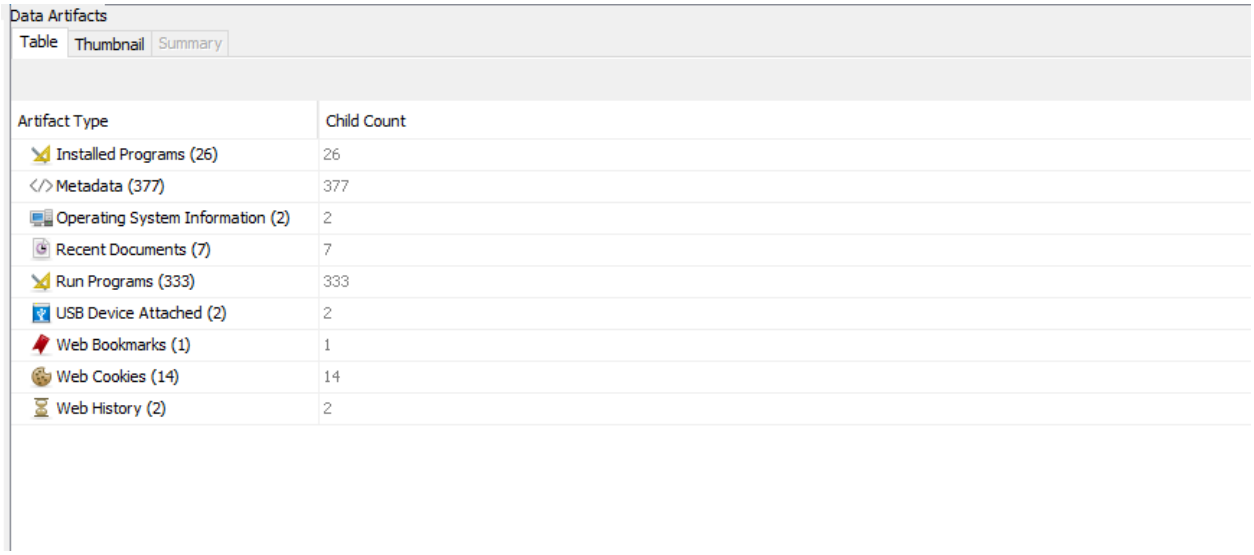


Registry Analysis

The tool supports the examination of Windows registries, enabling investigators to uncover important information about a suspect's activities, installed software, and system configurations. Being able to analyze the registry with efficiency is extremely helpful in tracking down malicious software.

Web Artifact Analysis

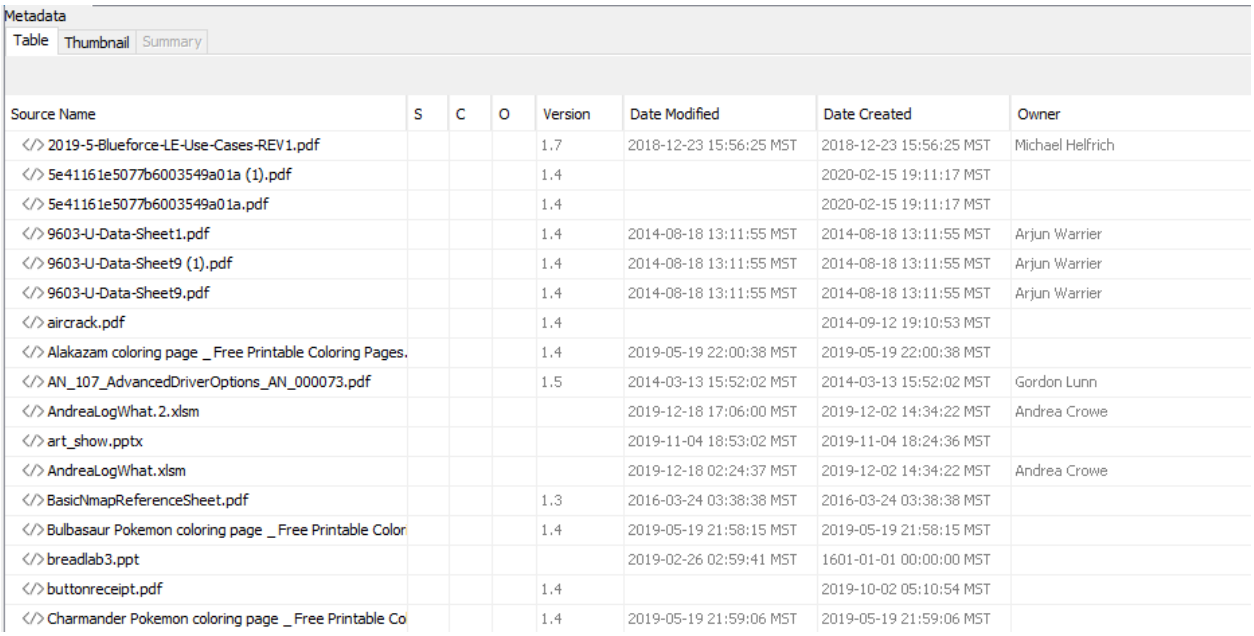
Autopsy can parse and analyze web browser artifacts, such as browser history, cookies, and downloads. This is essential for tracking online activities and identifying potential digital trails left by bad actors. Autopsy can uncover these trails with great precision and organizational intelligence. As you can see from the case below, we have a number of web artifacts to analyze, most importantly the metadata and cookies.



Data Artifacts

Table | Thumbnail | Summary

Artifact Type	Child Count
Installed Programs (26)	26
Metadata (377)	377
Operating System Information (2)	2
Recent Documents (7)	7
Run Programs (333)	333
USB Device Attached (2)	2
Web Bookmarks (1)	1
Web Cookies (14)	14
Web History (2)	2



Metadata

Table | Thumbnail | Summary

Source Name	S	C	O	Version	Date Modified	Date Created	Owner
2019-5-Blueforce-LE-Use-Cases-REV1.pdf				1.7	2018-12-23 15:56:25 MST	2018-12-23 15:56:25 MST	Michael Helfrich
5e41161e5077b6003549a01a (1).pdf				1.4		2020-02-15 19:11:17 MST	
5e41161e5077b6003549a01a.pdf				1.4		2020-02-15 19:11:17 MST	
9603-U-Data-Sheet1.pdf				1.4	2014-08-18 13:11:55 MST	2014-08-18 13:11:55 MST	Arjun Warrier
9603-U-Data-Sheet9 (1).pdf				1.4	2014-08-18 13:11:55 MST	2014-08-18 13:11:55 MST	Arjun Warrier
9603-U-Data-Sheet9.pdf				1.4	2014-08-18 13:11:55 MST	2014-08-18 13:11:55 MST	Arjun Warrier
aircrack.pdf				1.4		2014-09-12 19:10:53 MST	
Alakazam coloring page _ Free Printable Coloring Pages.				1.4	2019-05-19 22:00:38 MST	2019-05-19 22:00:38 MST	
AN_107_AdvancedDriverOptions_AN_000073.pdf				1.5	2014-03-13 15:52:02 MST	2014-03-13 15:52:02 MST	Gordon Lunn
AndreaLogWhat.2.xlsm					2019-12-18 17:06:00 MST	2019-12-02 14:34:22 MST	Andrea Crowe
art_show.pptx					2019-11-04 18:53:02 MST	2019-11-04 18:24:36 MST	
AndreaLogWhat.xlsm					2019-12-18 02:24:37 MST	2019-12-02 14:34:22 MST	Andrea Crowe
BasicNmapReferenceSheet.pdf				1.3	2016-03-24 03:38:38 MST	2016-03-24 03:38:38 MST	
Bulbasaur Pokemon coloring page _ Free Printable Color				1.4	2019-05-19 21:58:15 MST	2019-05-19 21:58:15 MST	
breadlab3.ppt					2019-02-26 02:59:41 MST	1601-01-01 00:00:00 MST	
buttonreceipt.pdf				1.4		2019-10-02 05:10:54 MST	
Charmander Pokemon coloring page _ Free Printable Co				1.4	2019-05-19 21:59:06 MST	2019-05-19 21:59:06 MST	

Email Analysis

The toolkit supports the analysis of email messages and attachments, making it possible to trace communication patterns and gather evidence from email accounts. Even if the subject

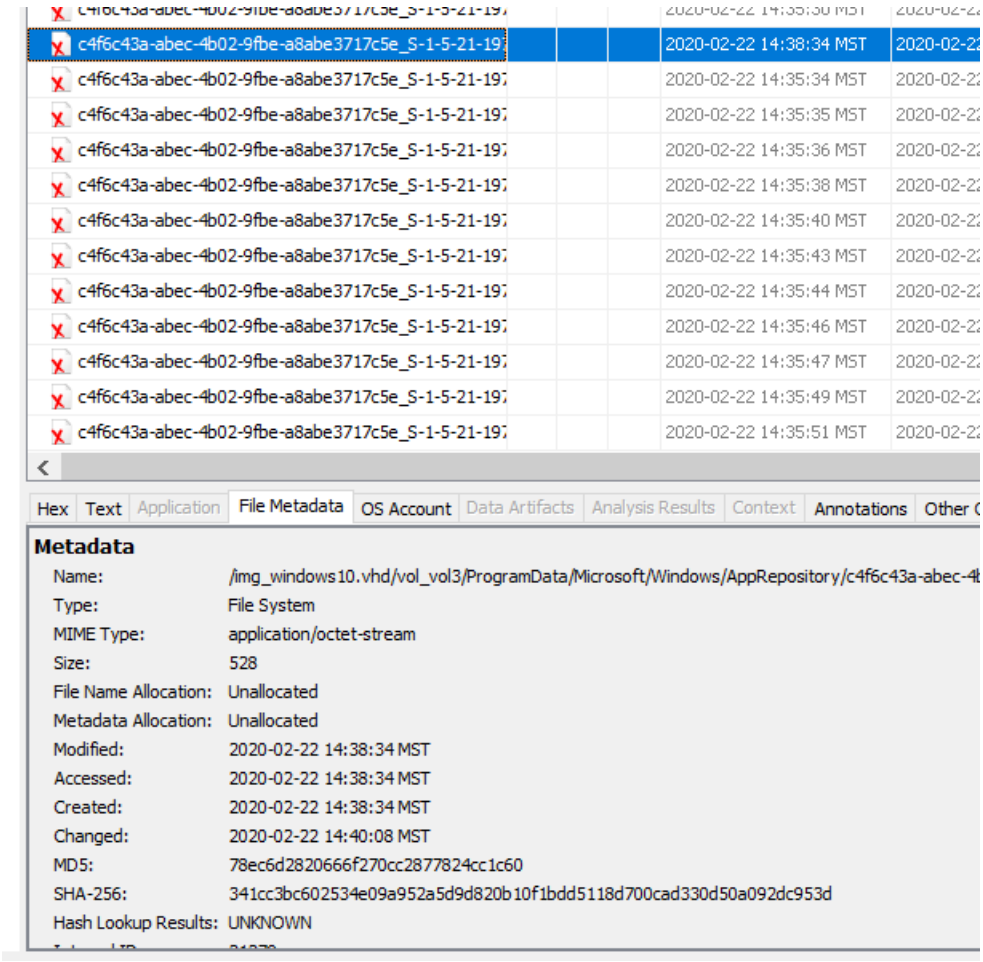
has deleted emails or the accounts associated with them, Autopsy can still detect them and the messages.

Drone Analysis

Even though Autopsy primarily focuses on digital forensics for computers and digital devices, because of its versatility, the onboard storage devices embedded within drones can be analyzed as well. Within the embedded storage, we can extract flight logs, GPS data and any captured photos and videos the drone collects during flight operations. While we don't have any drone data to display here, the extraction process is like that of an external hard drive or USB.

File Carving

Autopsy includes file carving capabilities, allowing it to recover deleted or damaged files even when file system metadata is missing or corrupted. This is quite possibly one of the neatest features, as bad actors often delete data thinking it will shroud their activities. Remember, when data is created, it cannot be uncreated, one must create new over it, in a manner of speaking.

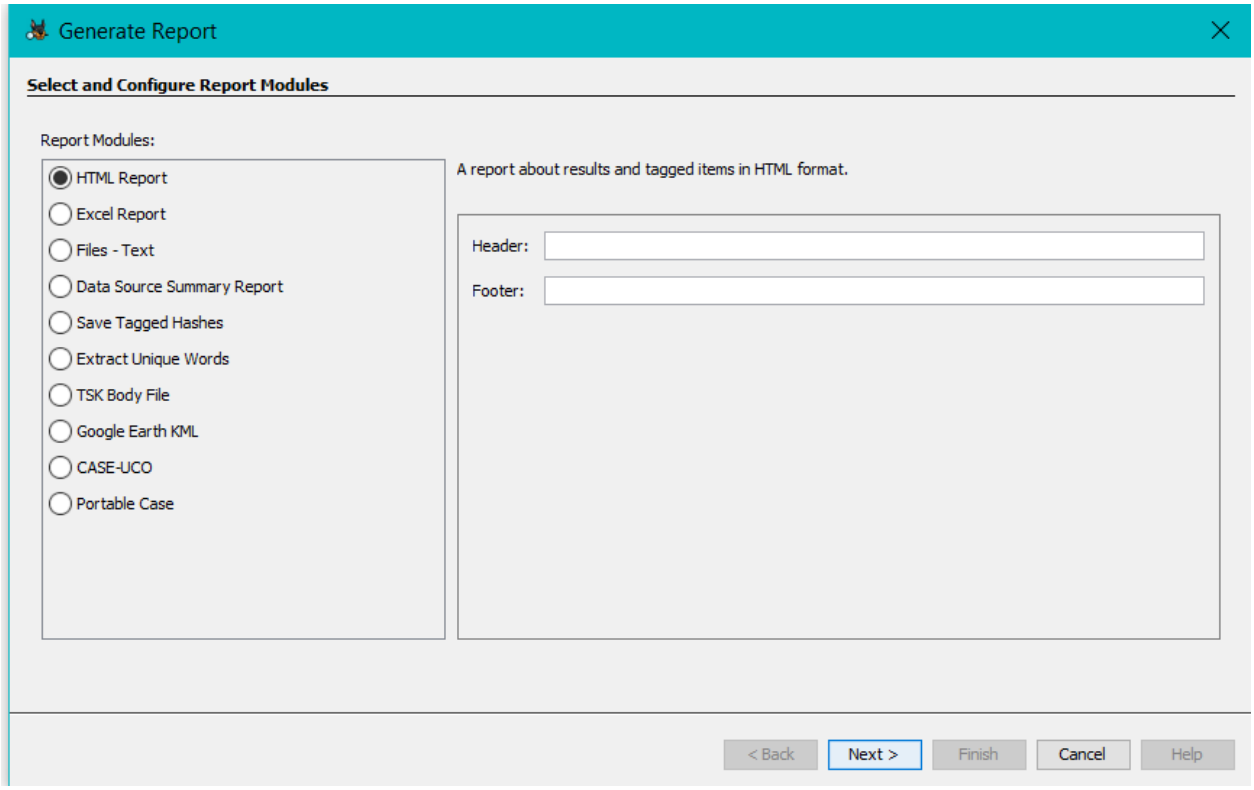


Reporting and Export

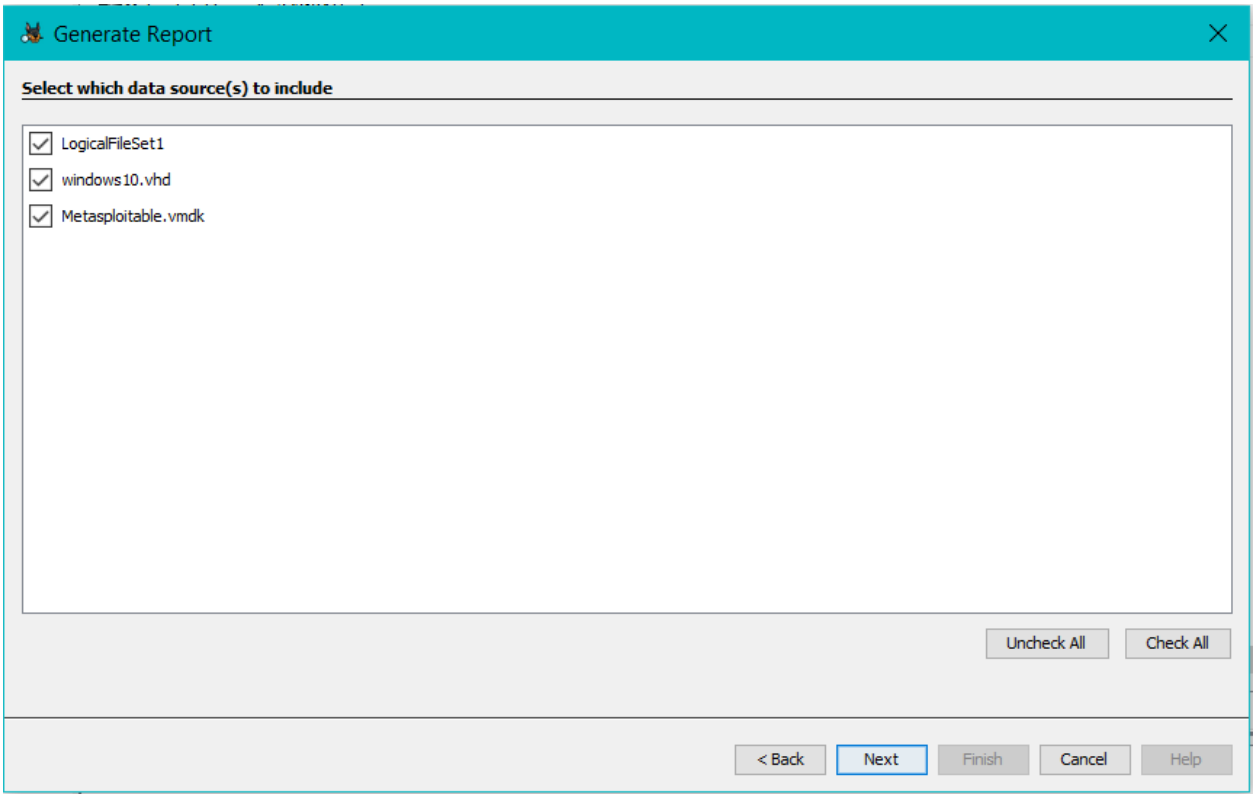
Autopsy generates detailed reports that can be used in legal proceedings. These reports provide a clear overview of the findings, making it easier for investigators to present evidence in legal proceedings, or to legal teams that will present the findings.

A feature I find that is helpful to investigators is Autopsy's ability to provide an easy-to-follow HTML report. Obviously, for the more technically inclined, there are other formats that would be more suitable. I have provided a graphical walkthrough of the report generation process, as you will see it is quite easy.

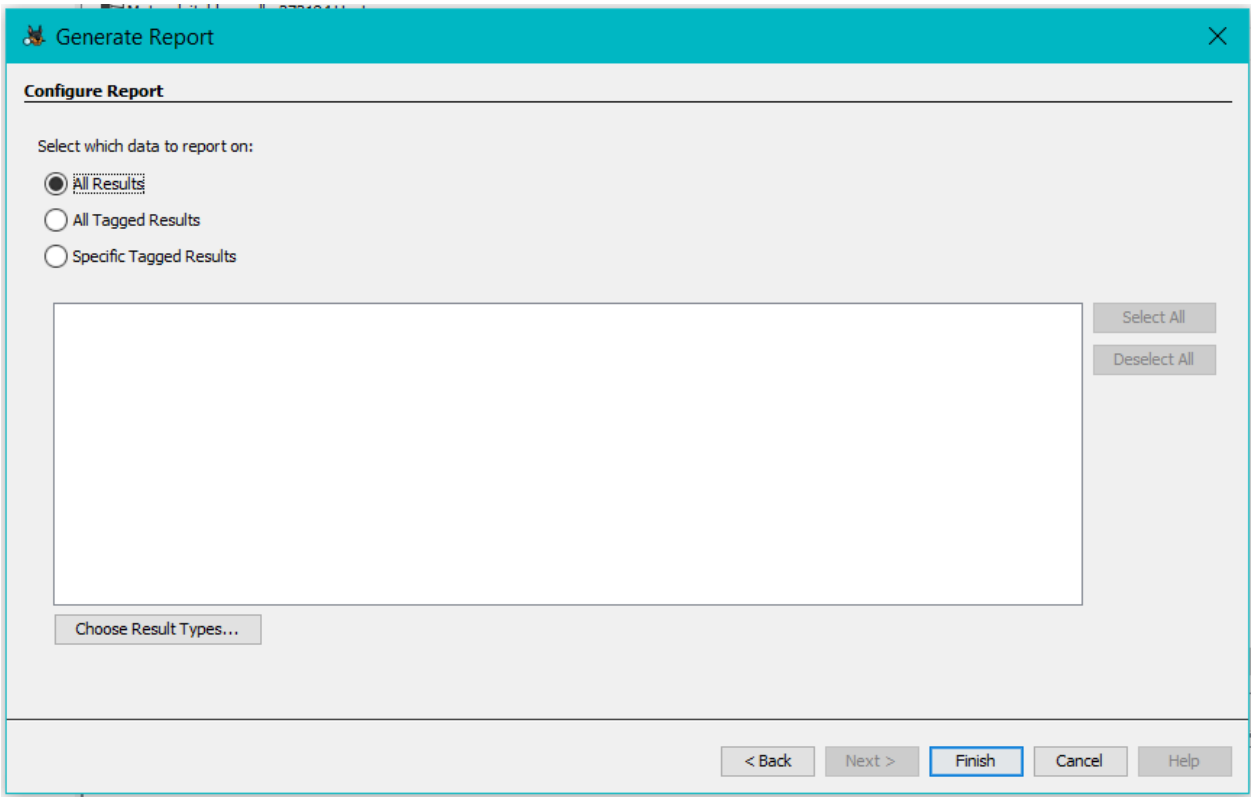
When we start the report generation process, we first decide how we would like our analysis to be presented. This, of course, will depend on your audience. Select an HTML report for less technical clients, a Google KML for geolocated artifacts or an Excel format for the more technical audience.



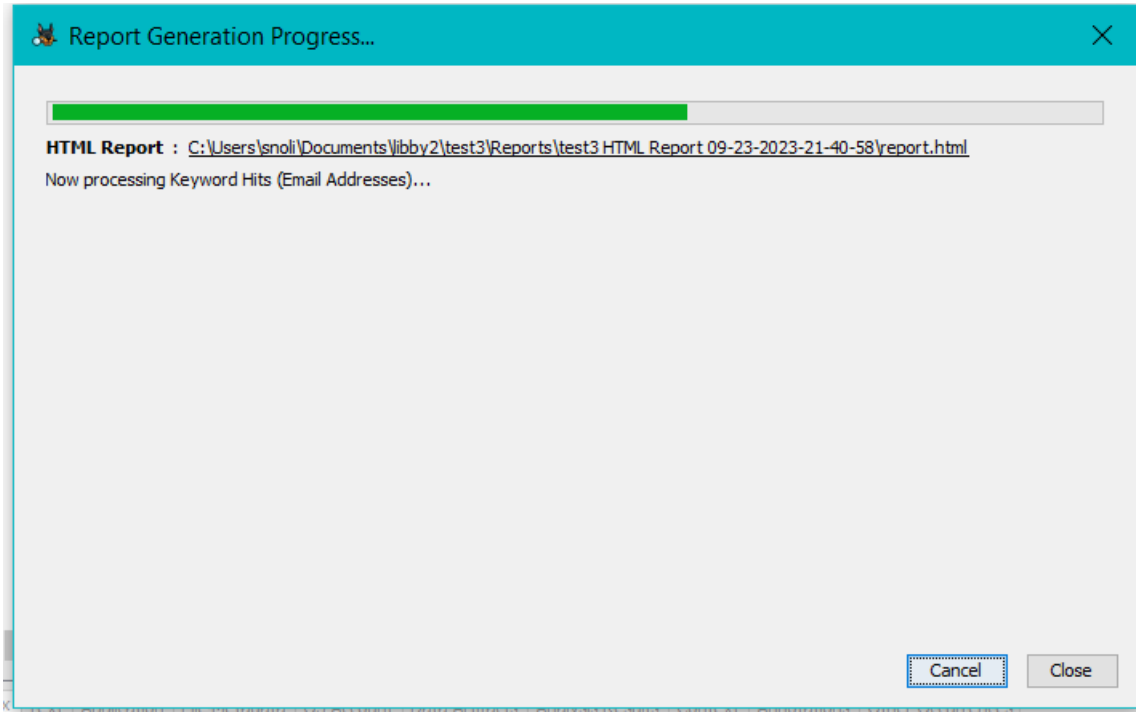
From this view, we can select which data sources to include in the report.



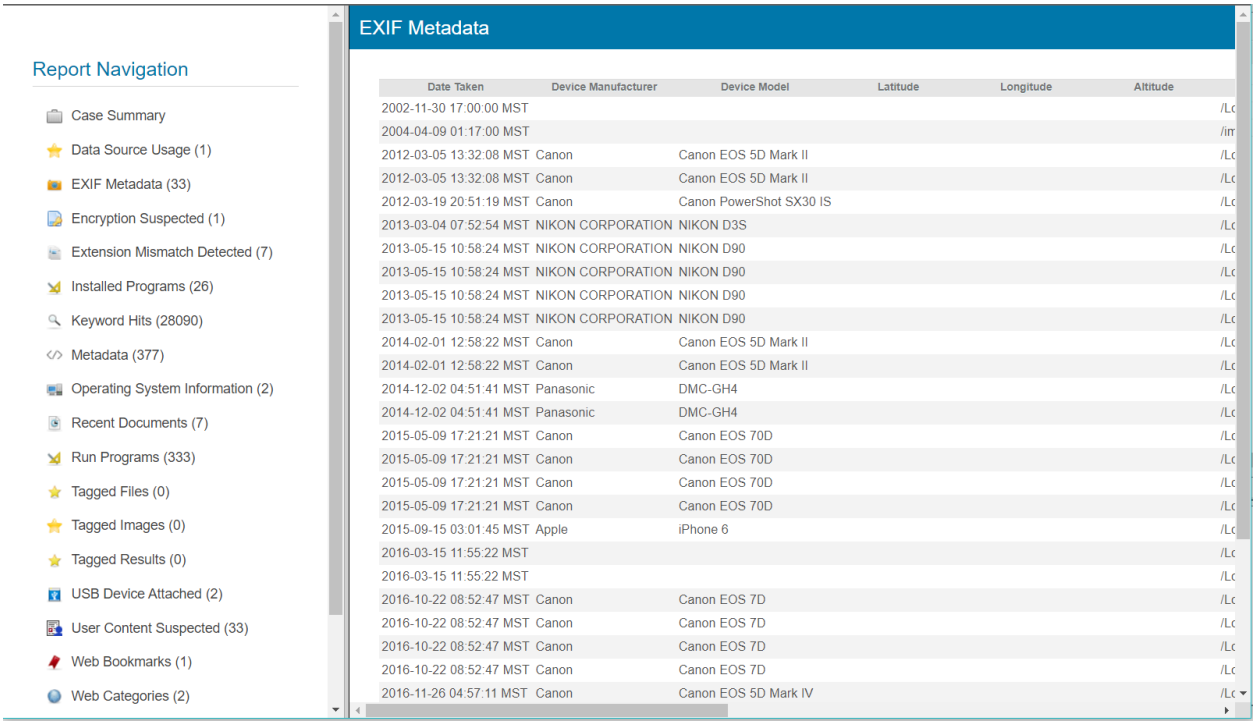
From this screen we can choose to generate a report on all results or only the specific results we wish to provide an analysis of.



The report generation process is fairly quick, though some technical variances may take a bit longer.

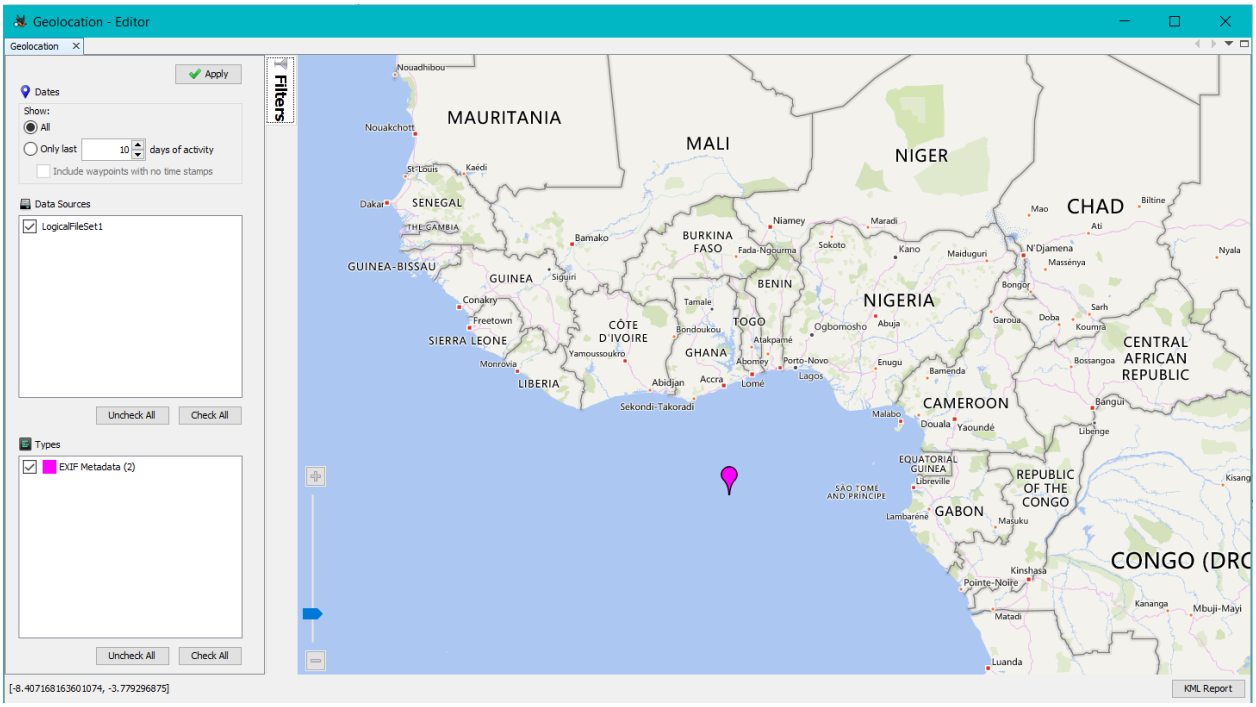


Finally, we have an HTML report that is easy to follow and can be viewed in a local browser.



Date Taken	Device Manufacturer	Device Model	Latitude	Longitude	Altitude	
2002-11-30 17:00:00 MST						/Lo
2004-04-09 01:17:00 MST						/im
2012-03-05 13:32:08 MST	Canon	Canon EOS 5D Mark II				/Lo
2012-03-05 13:32:08 MST	Canon	Canon EOS 5D Mark II				/Lo
2012-03-19 20:51:19 MST	Canon	Canon PowerShot SX30 IS				/Lo
2013-03-04 07:52:54 MST	NIKON CORPORATION	NIKON D3S				/Lo
2013-05-15 10:58:24 MST	NIKON CORPORATION	NIKON D90				/Lo
2013-05-15 10:58:24 MST	NIKON CORPORATION	NIKON D90				/Lo
2013-05-15 10:58:24 MST	NIKON CORPORATION	NIKON D90				/Lo
2013-05-15 10:58:24 MST	NIKON CORPORATION	NIKON D90				/Lo
2014-02-01 12:58:22 MST	Canon	Canon EOS 5D Mark II				/Lo
2014-02-01 12:58:22 MST	Canon	Canon EOS 5D Mark II				/Lo
2014-12-02 04:51:41 MST	Panasonic	DMC-GH4				/Lo
2014-12-02 04:51:41 MST	Panasonic	DMC-GH4				/Lo
2015-05-09 17:21:21 MST	Canon	Canon EOS 70D				/Lo
2015-05-09 17:21:21 MST	Canon	Canon EOS 70D				/Lo
2015-05-09 17:21:21 MST	Canon	Canon EOS 70D				/Lo
2015-05-09 17:21:21 MST	Canon	Canon EOS 70D				/Lo
2015-09-15 03:01:45 MST	Apple	iPhone 6				/Lo
2016-03-15 11:55:22 MST						/Lo
2016-03-15 11:55:22 MST						/Lo
2016-10-22 08:52:47 MST	Canon	Canon EOS 7D				/Lo
2016-10-22 08:52:47 MST	Canon	Canon EOS 7D				/Lo
2016-10-22 08:52:47 MST	Canon	Canon EOS 7D				/Lo
2016-10-22 08:52:47 MST	Canon	Canon EOS 7D				/Lo
2016-11-26 04:57:11 MST	Canon	Canon EOS 5D Mark IV				/Lo

The map below shows some geolocated EXIF Metadata; this would be especially useful in a report.



Autopsy in the Field

To illustrate Autopsy's practical utility, consider a hypothetical scenario where law enforcement is investigating a case of corporate espionage. The suspect is believed to have stolen sensitive company documents from their work computer. Using Autopsy, digital forensic investigators can and should be able to:

- Analyze the suspect's file system to identify deleted files related to the theft.
- Search for specific keywords or document titles within the suspect's files.
- Examine the suspect's web browsing history to determine if they accessed company resources remotely.
- Review the suspect's email correspondence for any evidence of communication with external parties involved in the espionage.
- Create a comprehensive timeline of the suspect's computer activity leading up to and after the theft.

Conclusion

In the world of digital forensics, Autopsy stands out as an invaluable toolkit that empowers investigators to extract, analyze, and interpret digital evidence efficiently and effectively. Its diverse range of features, compatibility with various platforms, and open-source nature make it a trusted and accessible resource for digital forensic professionals worldwide. As digital crimes continue to escalate and evolve, techniques and tools like Autopsy will remain essential in the ongoing battle to combat digital wrongdoing, uphold justice, and protect the integrity of digital evidence in our increasingly interconnected world.

References

https://www.autopsy.com/
https://github.com/sleuthkit/autopsy_addon_modules

About the Author

Kate Libby is a global infosec trainer and forensic data analyst. They currently work with private companies and nonprofit organizations to bridge technical gaps and capabilities.

HUNTING HACKERS USING AUTOPSY ON A MACOS IMAGE

ISRAEL TORRES

Join us as we forensically investigate this interesting scenario that often leads to rabbit holes, red herrings, canards and wild goose chases.

Introduction

In this scenario, we've received an image of a USB thumb drive (orig_128mb_image.dd) confiscated from the hacker's backpack. It was literally sewn in the lining of the backpack, which makes it even more interesting. The primary investigators did not want to plug it into any of their field laptops (they learned from the last time - another story, another time), and kicked it back here to our basement team for further analysis.

After our team imaged the 128MB USB thumb drive (do they even make those anymore?), hashed it for exhibitable evidence, and assigned it to a case, they get to play with it and see if there's anything actually on there. This is where we load it into Autopsy [1] running on macOS Sonoma via Parallels on a Windows 11 VM and see what we see.

We'll continue down below under the **Demonstration** section, so feel free to skip ahead and check it out.

Meanwhile, we'll discuss digital data in its most modern form. Nowadays, it's very common to keep data in the cloud (aka other people's computers that you or someone else rent) and that's what most people do in the most nonchalant fashion (assuming or not even caring if the data is being encrypted or scrutinized by entities, live, AI or otherwise).

Data is also kept on phones, flash drives, SD cards, DVDs, CDs, and even magnetic tape and floppy disks (using all kinds of technology from magnetic, optical, electrical, flash)… and then eventually clouded. The short of it being the cloud is what is often used as the medium transfer in the end. When was the last time you handed someone data in any other form? Let's not even bring up the transfer technologies used, such as Bluetooth, NFC, RFID, Wi-Fi, etc.

Intelligent Algorithms and Forensic Investigation: The Meeting between Sherlock Holmes and the Digital Age

Wilson Mendes

"It's not what you know, but what you can prove." Anonymous

Forensic investigation has long been a key player in the search for the truth in cases of complex crimes and incidents. However, as society evolves and criminal methods become more sophisticated, forensic science also needs to keep up with this pace of change. In this scenario, technology emerges as a powerful and indispensable ally for modern researchers.

ARTICLE'S SERIES

THE TWO-TOOL PROCESS IN DIGITAL FORENSICS: STEP 1 SELECTION

AMBER SCHROADER

When working with data that varies as much as digital data, it is crucial to follow a structured set of steps to ensure nothing gets missed. The first of these steps is the selection of the tools you are using for the processing.

With such a large variety of digital data available, the tool selection process will depend greatly on what type of data you seek and how much of a budget you must spend. Many organizations opt to minimize costs by relying on open-source technology for their investigative needs. However, choosing this method can result in a shortfall when it comes to finding all the critical data. To prevent missing critical data, every investigator should have a secondary tool to use to cross-validate their findings. No single tool can process and capture all the available data, nor does every tool parse the data the same way. That's why employing a two-tool process is a fundamental cornerstone in the field of digital forensics. The selection process outlined below lists steps to follow to maximize your tool selection.

Step 1. Isolate what you need to do.

What category of digital data will you be collecting? The answer to this question will help determine the type of tool needed. There are many digital forensics tools available with differing capabilities. Do you need an end-to-end solution to acquire and process data from a variety of digital devices? Is your work solely focused on the acquisition of data from mobile devices? Are you only focused on Mac devices and forensics? The best tool for your lab is the one that fits the type of data that your lab receives.

Digital Forensic Lab Management Made Easy with Monolith

Christopher Collins

There are multiple areas to focus on when managing a digital forensic laboratory.
Some of the important items to track are physical evidence like mobile devices or hard drives. However, how do we keep on track with other devices or evidence? In a forensics laboratory, for instance, there is hardware, software and other equipment that needs to be tracked.
Some laboratories use spreadsheets, or inventory management systems, but these methods are seldom cohesive in relation to documenting evidence and building reports.
A company called Monolith Forensics created a solution for this called Monolith. Monolith is a lab management software for digital forensics labs and teams that provide this cohesive environment.

Who is behind Monolith Forensics?

I had the opportunity to speak with Matt Danner, the Founder of Monolith Forensics.
Matt has a diverse history in digital forensics starting as a Special Investigator of the Texas Workforce Commission and the Texas State Auditor's Office. While working for the State of Texas, Matt was given the opportunity to take digital forensics training and start supporting investigations with forensic collection and examination of data. Matt eventually moved into the private sector and began managing digital forensics labs and teams. This experience with lab management made it clear to Matt that we needed better tools to manage a lab. The laboratories Matt worked with handled digital forensic cases from Civil Litigation, E-Discovery, and consulting with the Travis County Sheriff's Office on Criminal Investigations.
Just before running Monolith Forensics full-time, Matt was a senior consultant for Palo Alto Networks where he continued to work in DFIR roles and even worked on major projects involving reverse engineering of mobile applications. Matt uses this experience as a former investigator and digital forensics practitioner when creating or considering features for

FORENSICATING THREATS IN THE CLOUD

CHRIS DOMAN & MATT GEORGY

As organizations have shifted to the cloud, it's not surprising that threat actors have followed. Below we run through some of the most prominent attacks in the cloud today, and how to perform cloud forensics and incident response to resolve them.

TeamTNT, the cloud and containers

TeamTNT is a cybercriminal group that targets cloud and container environments, using various techniques to compromise and exploit them. TeamTNT has been active since at least April 2020, and has evolved its tactics and tools over time. Some of the methods used by TeamTNT include:

- Scanning for exposed Docker APIs and Kubernetes clusters, and deploying malicious containers that run cryptojacking malware or backdoors:

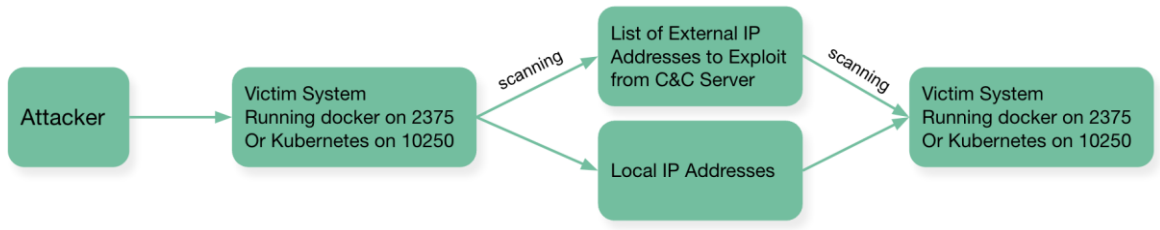


Figure 1: How TeamTNT compromises systems over exposed Docker and Kubernetes APIs

- Stealing cloud credentials from compromised instances, and using them to access other cloud resources or services:

Interview with Kate Libby

eForensics Team

Could you briefly explain when and how you first became interested in digital forensics?

I first became interested in digital forensics when I was working as a malware analyst, that would have been around the 2014-ish time frame. I was asked to assist on some data recovery, and in an instant I was hooked.

What element of this field most interests you?

Being able to discover information lost or intentionally hidden by criminals fascinated me.

Where can you obtain the most recent information about the field of digital forensics?

Industry publications, online forums, conferences, networking with fellow professionals, and of course E-Forensics magazine :)

You work with both private and for-profit companies. Would you kindly elaborate on your work?

Absolutely, being able to work with a wide range and diverse set of clients, I am able to stay current with the business trends and do some good along the way. I assist them in investigating digital incidents, recovering data, and ensuring the security of their digital assets.

Can you provide an example of a security issue you are experiencing in the workplace?

Without providing specific details due to confidentiality, security issues in the workplace can encompass various threats, such as malware infections, data breaches, or insider threats. The human element and lack of actionable education remain at the top in regard to security threat.

In addition, you are a forensic data analyst and a global infosec trainer. Would you kindly elaborate on that?

Certainly, I analyze digital evidence in legal cases and also share my knowledge and expertise with professionals worldwide through training programs, private sessions, and workshops.

WHAT DO YOU LIKE ABOUT THIS JOB?

Every case and engagement presents a new and exciting challenge and getting to aid organizations in the digital realm is extremely rewarding.

WHICH CERTIFICATES WILL YOU SUGGEST?

Certifications are a slippery slope indeed. Whatever a persons intended outcome for themselves aims to be, I suggest finding a certification that reinforces the knowledge needed. If your goal is the hardware side to things, Comptia A+ would be a good fit, moreover if you want more of a role in cyber, then CISSP, CISM may be a great fit.

WHAT LITERATURE WOULD YOU RECOMMEND AS THE BEST FOR A BEGINNER TO LEARN FROM, AND WHY?

To start I would suggest "Computer Forensics for Dummies", I know it sound silly, but it will break it down for you, this way you can gauge how quickly you grasp certain concepts. I would also suggest quality publications like E-Forensics and Journal of Digital Forensics and Law.

IF YOU HAD TO RECOMMEND A CYBER SECURITY SPECIALIST TO OTHERS. WHO, EXACTLY?

Besides myself I would recommend Nathan House of StationX. Nathan has a wealth of experience and knowledge, not to mention a team of amazing professionals.

THANK YOU

BECOME A DEEPFAKE AUDIO MASTER

THE WAY AUDIO ENRICHES OUR UNDERSTANDING OF THE WORLD AND SHAPES WHAT WE PERCEIVE TO BE THE "OBJECTIVE REALITY" OF THINGS HAS ONLY GROWN TO BE MORE PROFOUND AND IMPLICIT.