DOI: 10.2507/32nd.daaam.proceedings.014

ENTERPRISE TOOLS FOR DATA FORENSICS

Zlatan Moric, Jasmin Redzepagic & Frano Gatti

This Publication has to be referred as: Moric, Z[latan]; Redzepagic, J[asmin] & Gatti, F[rano] (2021). Enterprise Tools for Data Forensics, Proceedings of the 32nd DAAAM International Symposium, pp.0098-0105, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-33-4, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/32nd.daaam.proceedings.014

Abstract

Companies today face different types of cyber-crime-related attacks. There were loads of security-related problems discovered in the past couple of years - Poodle, Heartbleed, Spectre, Meltdown, Ransomware, Microsoft Exchange security problems - these are just some of the more common ones from the past couple of years. As these attacks become more prevalent, it is only a matter of time before the incident will require digital forensics investigation. Tools for data imaging, hashing, analysis, and reporting must be a part of the administrator toolkit. Many tools provide modules or toolkits. These can be applied for different functions in the forensic processes. Competencies and knowledge are often outsourced in most organizations. There will always be a demand for data forensics procedures, and it will only increase as IT develops.

Keywords: Digital Forensic; Computer Forensics Tool; RAM Forensics; Disk Forensics; Network Forensics.

1. Introduction

Digital forensics and tools that make it possible are changing quickly as the entire field is changing. [1] At the same time, it is important to have the right tool at the right time since your digital toolkit must be compatible with whatever is on the market today. This means that we must do two things at once - we need to keep track of all the things happening in the user area, both on the software and the hardware side and at the same time we need to keep track of tools that provide all the features necessary for working with said user resources. Just as an example, if we wanted to re-configure our Microsoft IIS (Internet Information Services) due to SSL-related security problems, we can use a tool like IIS Crypto that can make it much easier for us to do that. If we had issues with Ransomware, we could probably deal with that by having a correctly set up backup and disaster recovery solution. That doesn't mean that we can solve all the security problems easily, and for most of them there are precautionary steps that we can take before something happens. After a security issue happens, all that's left to do is to do forensic analysis, and that is the core subject of this paper - which tools to use to do a proper forensic analysis.

2. Use cases for digital forensic tools

Organizations face all kinds of IT challenges, from planning infrastructure to configuring stable and secure services and applications. But what is the action plan once the administrator discovers a major security issue has happened e.g., data leakage like for example a former employee downloading the source code and uploading it to the internet.

Digital Forensics is a time-consuming art of preservation, acquisition, documentation, analysis, and interpretation of evidence from different storage media types found in the organizations that reported the incident. So, in this example, an image from all disks of the suspected employee should be captured in a tamper-proof state. This information can be provided as evidence in the court or as an indicator of vulnerabilities that must be patched. If digital forensic procedures are not conducted a system can be left in a vulnerable state because of the absence of information on what caused the incidents. Also, if Digital Forensics is not performed in a criminal case, law authorities can make wrong decisions. They will make these decisions because of the misleading data or incorrect shape and form of evidence that is presented. So, ignoring the need for forensic cases in the organization can seriously damage the reputation of the business and stakeholders. Companies need to have forensic readiness. In other words, they need to have proactive procedures, people, tools, and prerequisites defined and configured. Nowadays most of the organization don't have the required skills and resources so InfoSec and supports teams are responsible for all security-related incidents. In the incident case in most organizations, the responsiveness would be reactive, not proactive. By default, Windows systems don't log the deletion or manipulation of files, this audit needs to be configured manually. Free and native features such as logging with required details need to be utilized. Administrators need to know these features exist and must configure them. Retention of logs must be defined and edited if necessary. It is a good practice to have a centralized logs system running in an environment. Types of forensic incidents can vary but data recovery is the most common use case.

Criminals always try to hide the track, so investigators try to identify all data that has been deleted, changed to different extensions, or hidden in any other way. In most cases, digital forensic include the process of discovery and/or recovery of data (evidence) using the various tools and methods available to the investigator. Also, malware investigation is a big part of digital forensic because ransomware spread by trojans and worms across a network is a major threat to individuals, companies, and military organizations. A digital forensic investigation can include tracking down identity theft of any type e.g., stolen credit card usage or a fake social media profile. Network and internet investigation are processes where investigators try to figure out sources of the network-based incident such as Denial-of-Service (regular and distributed). Also, email investigation is a big source of IT security incidents because of spam, phishing attacks, and uneducated users that open every attachment without checking the validity of the sender. Forensic investigators must identify the source IP and geo-location of the attacker. Investigator will perform investigations of malicious attachments.

Corporate espionage can also be a case for digital forensic investigations, companies nowadays need to secure their assets so that sensitive information cannot be accessed or transmitted. Lastly, forensic investigators can face global problems such as drug trafficking and child abuse that are widely exploited within the Deep Web and the internet. Highly skilled forensic analysts can bring down these dark realities by analysing internet traffic, transaction and browser history, email records, and images. To solve these kinds of incidents, investigators need to be well educated and driven, it is an intense job that requires punctuality and professionalism. Most organizations will outsource these problems to other firms that are competent in digital forensic investigation. Meaning these skills are of high value and demand for digital investigation will increase in the future.

3. Tools used in forensic processes

Any IT process needs to be well documented, so proper procedures are a key tool in any forensic investigation. Procedures ensure the integrity of the investigation. The National Institute of Standards and Technology (NIST) has implemented the Computer Forensics Tool Testing (CFTT) program that's main purpose is to test and make reports for the community. Most of the tools that will be mentioned have reports available for the public can be found on the CIFTT website (https://www.dhs.gov/science-and-technology/nist-cftt-reports#). Also, tools need to be tested in the lab environment.

This can be done using a Kali Linux (or some other tool such) virtual machine as a Forensic workstation and a client virtual PC or external media (hard drive or USB with some dummy files) to image and analyse. Kali is the best operating system for information security since it is natively equipped with all sorts of tools (and can be upgraded with additional) [2]. It comes suited with many forensic tools such as Autopsy and Guymager. Other tools can be run as a live operating system as a virtual machine (or as a USB live boot). Budget is always an issue and some solutions cost thousands of dollars but are robust, accurate, and have GUI. These tools can be open source e.g., CAINE, or commercial e.g., Paladin. Either way, forensic people need to spend a lot of time testing tools and have a skill set to adapt to case requirements. [3]

3.1. Identification and precollection

Firstly, a new case arrives and needs to be categorized accordingly [4]. A case can first be recognized as an incident alert that is acquired by email or a security operations centre system (e.g., Darktrace). In the first stage, the incident needs to be discovered, no onsite action is needed at this time. The goal is to gather as much information about the problem and the types of systems involved. Interview with the client should be done and verified by some form of the written communication (such as email) so, that the initial incident information is retained permanently. To focus efforts a digital investigation plan is created, this is a roadmap to a successful investigation. It is important to define the background of the incident (circumstances), the scope of investigation, goals, and plans of actions in terms of evidence gathering. Then the pre-collection stage needs to be done.

The stage consists of processes such as organizing the acquisition kit and documentation. The data acquisition kit contains a card reader, various adapters (various types of USB and USB to SATA), device cables (power, SATA, HDMI, VGA), networking cables (straight-through, crossover, console), and a write blocker. Write blockers are used in the investigation to protect and preserve the original evidence from being modified. If a hardware write blocker isn't available, a software tool should be used. [5] The advantage to the software write blocker is that it is installed on the investigator's workstation, one less device in the acquisition kit. Paladin is an Ubuntu-based forensic toolbox. It is a live operating system (with a small footprint) that has a range of forensic features including write blocking. Currently, there is no free version available for commercial use and the minimal price is 25 USD. CAINE (Computer Aided Investigation Environment) is a GUI-based open-source Linux distribution that integrates forensic tools as modules. It also provides features such as read-only access to drives by filtering any IO command sent to the interface. Software write blockers operate by the policy definitions that can be changed to enable writing on the disk.

On the other hand, it is easier to run daily imaging operations with the hardware write blocker, it works independently providing indicators (lights or output on the mini screen) that the computer is not tempering with the drive which contains evidence. When investing in hardware write blockers different features such as connection types, writing capability, and data transfer rate should be considered. Hard drives have increased sector size to 4096 bytes so it's a write blocker should have Advanced Format compatibilities. That format defines disk sectors that exceed the size of 512, 520, or 528 bytes. A larger sector size ensures data integrity with stronger error correction maintenance algorithms. Coolgear hardware write blocker adapter costs 65 USD and has support for Windows, Linux, and Mac operating systems. For more intense workloads Tableau Tk35u USB 3.0 Forensic Ide/SATA bridge kit but this product costs 487 USD in a brand-new state. [6]

3.2. Acquisition

Acquisition of evidence is the first most important step in any digital forensic case. It is described as collecting data for further investigation. Accountable staff retrieves a copy of disks and volatile memory from the suspected digital asset. The goal of this phase is to collect and protect the data. All data from the suspect's computers need to be collected without harming the integrity of evidence. In this procedure evidence integrity methods such as write blocker, hash generating techniques, and chain of custody must be used.

The acquisition type and requirements need to be defined. Getting approvals for the action and rehearsing the imaging process (it saves time). When a technician arrives on the scene, he will prepare to create a forensic image which is a tamper-evident container that contains files, file systems, media storage, and device data. To simplify it is a copy of a drive that is compressed into a single file. He will then photograph the evidence and start the chain of custody. The chain of custody is a form that legally ensures the integrity of the evidence as the evidence is an exchange between individuals. It also provides accountability because personal information is matched with the date and time of evidence transfer. So, in this way it is well known who had the evidence at a certain time. A document created by the Scientific Working Group on Digital Evidence (SWGDE) defines a list of aspects to consider when executing a live system acquisition procedure. The list is defined from most to least volatile and crucial. When initiating the process of imaging the device's power state needs to be checked because it is important to store data that is in RAM and paging file with as little modification as possible. Working memory often contains more evidence than hard disk data because the running process, open documents, and network connections can be identified using different tools. There is only one opportunity to collect volatile data. RAM and running processes must be captured first then system settings and storage media. 4-Magnet is a free RAM acquisition tool. It can be used to capture the current state of RAM and running processes on Windows 10 system. It allows investigators to capture the contents of physical memory into a dump file that can be analysed. 7-RAMcapture (developed by Belkasoft) is a portable tool compatible with Windows operating system. It is used for RAM capture. It exports the contents of working memory to a raw file that can be analysed by other tools.

Active network connections information such as active sockets and processes that are correlated with than can be useful for the case. Xplico is an open-source GUI based Network Forensic Analyst Tool that main goal is to extract information from network and internet captures. It can automatically decode packet capture files (.pcp) files using an IP decoder and decoder management components. It can use analyse files generated by other packet capture software such as WireShark and Fiddler. Packet captures often contain useful information such as websites browsed, emails, chats, printed files, and VOIP (Voice over Internet Protocol) or RTP (Real-time Transport Protocol) data. Xplico cant view traffic encrypted by SSL (Secure Sockers Layer).

Volatility is Python open-source forensic software that can be used to analyse RAM on most used operating systems (Windows, Linux, Mac, and Android). It can identify and export network information from the hosts such as PID, Port, Protocol, Address, the creation time of the connection. So, it is a cross-platform tool that creates a snapshot of memory also known as a memory dump. Profile of the operating system has to be chosen firstly; different systems store information in different locations. Additional plugins can be added to the existing framework. It can identify and analyse the hidden running processes that can be useful for malware analysis. Volatility can also capture command line history and a list of timestamped events, which is a must in every forensic investigation. For Microsoft profiles, there is an option for a DLL (Dynamic Link Libraries) analysis [7].

Additionally, system settings from the browser and registry can be exported and analysed. This is important because the information from users, setting, operating systems, and even hashed passwords can be found in the registry. Digital evidence and forensics toolkit Linux is an Ubuntu desktop-based tool that can be used in situations when shutting down the host is not possible. It has compatibility for on-the-fly RAM and swap file analysis. It is also equipped with tools for antimalware, data recovery, imaging, hashing, mobile forensics, and reporting. Browser history capturer by Foxton is used to extract and view internet history. It extracts all useful user data from the browser (history, sessions, searches, bookmarks, passwords, etc.) into a single file.

The next step is to collect data from storage media using a write blocker tool. Which is known as a forensic disk controller that permits read-only access to the data storage device without compromising the integrity of the data. Evidence must be preserved in a persistent state, no changes to the evidence are allowed. A user data user must be saved in a dedicated external hard drive(s) and nowhere else. A laptop is just a tool to save data on external hard disks. For this part of the process, the hard drive needs to be at least the size of the data for investigation, but it's recommended to have the double amount of storage that is required for investigation. The process of imaging can be described as extracting or copying data either as a file, partition, entire storage media or a drive [8].

- Dc3dd (Department of Defense Cyber Crime Center dd) is an upgraded version of the dd (data dump) which is a copying and conversion tool originated on 1970s Unix systems that copied all contents of a storage device in a single file. Dc3dd is maintained parallel to dd, so when the dd tool gets updated dc3dd gets an update too. Dc3dd has many enhancements over dd. It copies data from one location to another while performing data conversion. It also performs hashing on the fly (MD5, SHA-1, SHA-256, and SHA-512). It can create multiple image file copies to different devices (in different formats) and split files into multiple parts. It can verify and wipe media and has a progress indicator.
- DCFLDD (Defense Computer Forensics Labs dd) is an enhanced version of dd that is maintained and supported by the Defense Computer Forensic Lab.
- Guymager is an open-source imaging tool that's not command-line, meaning its GUI based. It has hashing and verification operations and supports files using EnCase, raw, and AFF formats. EnCase format allows investigators to conduct a detailed analysis of user files (browser data, images, documents, and registry) that are collected. Raw data is unprocessed data (common extensions are .bin, .dd, .img, .iso, .raw), sectors are copied in order. Source and target will have the same value. No additional information is stored in a raw file. Raw images are not forensic files but can be used in an investigation.
- AFF (Advanced Forensics Format) format is used to capture digital evidence for legal proceedings.
- Libewf is an open-source library that is used to create Encase evidence image files. It can be used to convert, acquire EnCase files outside of EnCase Forensic.
- Afflib can create, convert, and verify AFF image files. So, this tool can convert raw images created by guymager, dd, and other tools to AFF format.
- Forensic Toolkit (aka. FTK) is free software developed by AccessData that is used on Windows operating systems. It includes a standalone imaging program (FTK imager). It can calculate MD5 has to confirm the integrity of data that is collected. Confirmation of the validity of evidence is important for presenting data that is important for the investigation case.
- Helix 3 Pro is the enterprise commercial toolkit for digital forensics. It has compatibility for live system acquisition and disk imaging. Along with reporting features for data discovery and digital analysis.

3.3. Examination

When collecting data investigator needs to maintain the integrity of evidence. Hash values should be provided before, during, and after an acquisition. If the copy is edited, the hash values will be quite different meaning the evidence integrity is ruined. To verify that the data set has not been altered Digital Forensic analysts use tools to calculate and verify cryptographic hashing. Cryptographic hashing is a type of mathematical function that creates a unique, fixed-size mathematical value from an arbitrary set of input values. [9]

The hash value is a unique integer that is a digital fingerprint of a file or a disk. Items in a collection of digital evidence can be identified by their hash value rather than relying on the less accurate and changeable indicators such as timestamps, filename, sizes, or by direct viewing. Files can be whitelisted or blacklisted by their hash values or hash sets. Hash values are calculated by the one-way hash functions and are not reversible (this doesn't mean they are secure). Hashing is not encryption. Hashing is used to determine the integrity of content by detecting modifications to the data that consequently change the hash output. Encryption is a two-way function that encodes the data to maintain data confidentiality so only authorized entities can read it (they pose the decryption key). Hashing is irreversible while encryption is reversible. The hash algorithm will always produce the same size hash value. Typical hash sizes are 128-bits, 160-bits, and 256-bits. Larger hashes have greater reliability in representing digital information than hashes, more bits more unique items. Hash collision, mathematically impossible to prevent but the probability of two files with the same hash can be minimized by increasing the bit length of the hash. Hash length is increased by choosing the hashing algorithm that can provide larger length hashes. Hashing unambiguously identifies digital information by detecting water the digital information has changed. Hashed made from items of evidence that are physical-digital storage devices.

Hashes are part of the meta-information describing an item of evidence. Hash also identifies known information present on the storage device and is used to verify that the item of evidence has not changed. Forensic investigators store hashes in hash sets that are described in the examination report in the digital forensics' cases [10].

- Message-Digest (MD2, MD4, MD5. MD5) is used in digital forensics. It creates 128-bit message digests and is free to use.
- Secure hash algorithm (SHA-0. SHA-1, SHA-224, SHA-256, SHA-384, SHA-512). SHA-1 and SHA-256 are used in digital forensics. SHA-1 is 160-bit and SHA-256 is 256-bits. It is a US standard and free to use.
- RIPMEND is a cryptographic hash algorithm designed by Hans Dobbertin, it has a length of 160 bits.
- WHIRLPOOL is a hashing algorithm created by Vincent Rijmen and Paulo Barreto that produces the 512-bit message digest.
- TIGER algorithm is used by modern computing because of its speed and efficiency
- Sumtools (summary tools) calculate a hash value using MD5 and SHA hashing algorithms for files stream or a file system. It is also used to compare files to pre-calculated hash values.
- Hash my files is a portable free tool that is used to calculate MD5 and SHA1 hash values of files. It can generate HTML reports with information useful for the investigation such as size, timelines of data creation and modification.
- Rahash2 is a part of the radare 2 toolkit, which supports MD and SHA hashing capabilities but also and CRC, Xor, and many other algorithms that are used for unpacking and decoding all sorts of binary files. So, it can also be used for advanced work with malware files in terms of decompiling, reverse engineering, and testing malware programs in a sandbox environment. In digital forensic, it is mostly used to check the identity and verify the integrity of files.
- The Hashdeep is installed by default on the current Kali version, and it provides tools to provide forensic audit mode, block hashing (MD5, SHA1, SHA256, TIGER, WHIRLPOOL), matching using hash sets, hash disk recursively in a file tree.

After the hash, values have been checked and the integrity of the evidence integrity has been verified the next phase is to analyse the data in the search for concrete evidence.

3.4. Analysis

The goal of the analysis phase is to examine the data, identify the evidence data that is in the scope of the case and extract useful evidence information. In this phase, the recovered data (artifacts, metadata, and initial facts) is heavily researched. The investigator tries to find data that is relevant to the case and answers important questions (such as who, what, when, where why, and how) about the crime or an incident. Correlating the evidence is important to determine what happened so timestamps of events are crucial. For example, if the users deny the execution of the malware. Investigators would need to prove this by identifying the program execution artifacts and user logon events on the affected computer. Then this information would be collated with timestamps that can provide more detailed conclusions. Investigators keep in mind that an analysis is the interpretation of evidence, not absolute proof. In this case, we also need to verify that the suspected user was using his account on the computer and no one else. This can be verified by correlating the timestamps with the user's entry to the building, most companies now track the working hours with the entrance ID cards that employees need to use to enter the building. In some severe cases, video camera footage should be also considered to correlate and verify the evidence timestamps. In Digital Forensics timeline analysis is important because it arranges the events from multiple data sources in the correct order, to determine when and what happened on the system and add context to the analysis.

The Sleuth Kit (TSK) is a set of tools that can be used to analyse disk images and recover deleted files from them. Additional modules can be added to the existing framework. Autopsy runs The Sleuth Kit in the background. It identifies and lists all allocated or unallocated (deleted) files. It can identify files hidden by rootkits. It can display metadata information. It categorizes data by type and provides timeline information.

The Autopsy (installed by default on Kali) is a GUI-based tool that is used by the military, law enforcement, and corporate users to investigate cybercrime. It is free and provides features like other tools such as web artifact analysis and registry analysis. It also provides features for hash filtering, file system analysis, keyword searching and extraction geolocations, and camera information from JPEG files. It can group the files by their type. For media files, it can display images as thumbnails for a quick view and videos without the need for an external viewer. For mail fails it can parse MBOX format messages.

Encase (acquired by OpenText) is created by Guidance Software. It is used for acquisition, deep forensic analysis, and reporting. It provides functionalities for several processes in Digital Forensics including acquisition, analysis, and reporting. This tool has all the required features for conducting a digital forensic investigation such as in-depth analysis of user files and data (e.g., internet history) and data recovery. It has a scripting facility called EnScipt. All features are integrated into one tool.

3.5. Reporting

In the post-investigation reporting phase, investigators prepare the presentation of the analysis conclusions. The report needs to be prepared in a way that all stakeholders can understand. This phase requires technical and legal evaluation. Most of the law enforcement (if they do not have the technical background) doesn't have the required knowledge to determine the facts from the evidence. It is the Digital investigator's job to present the evidence and explain the techniques and methodologies used in the data analysis phase. So, the main goal is to present the evidence adequately and acceptably, defined by the court of law.

There is also a corporate type of investigation report. This report differs from law enforcement case reporting. The most important part is to present the evidence in the way in which a client who outsourced the incident can understand the cause, consequences, and responsibilities. All forensic reports should have a transparent view of the investigation process. EnCase tool is an all-purpose forensic tool. It has an integrated reporting module. It can create reports that can be easily shared. It also provides the ability to create report templates. Helix framework has a reporting component to pull concise reports on audits or ad-hoc reports based on different criteria. Processes such as collection and preservation should be explained.

Details of the analysis should be described and supported with evidence material. All crucial conclusions should be verified using at least two different techniques or tools to increase the validity and present the evidence as tested facts. The snippets from all tools used should be presented. The best approach is to avoid absolute phrases and long sentences. Also, it is a good practice to prepare a summary section for non-technical readers of the report. Presentation tools such as Sway and PowerPoint could be great tools. Short presentations that provide all important evidence, their validity, and a graphical workflow with events of the incident could be created to ensure that all participates understand the nature and cause of the incident that has occurred.

4. Conclusion

Data forensic tools must be used by an experienced forensic expert. This is important because these tools can harm the data on disks and consequently do damage to the investigation (keep in mind that dd is known as data dump but also as data destroyer). To mitigate risks, investigations must be done systematically, defined by procedures. Well-defined procedures are a crucial tool. Also, some tools like EnCase have all the required features for conducting these procedures. It is better to gather evidence with multiple tools to increase the validity of evidence. Also, some tools can perform better for different use cases. Investigators need to have experience with all tools mentioned. They need to know the best toolkits for different platforms to adapt to all scenarios that are possible. The forensic procedure can be run using only open-source tools.

First, the problem or incident needs to be defined in detail. The most important step of the investigation is acquisition. Before executing acquisition is executed a plan with evidence gathering goals should be created (to avoid time-wasting). If the acquisition is not done correctly no further investigation can be done. There is no point to analyse the data if the data was partially wiped or changed (the hash values). The experienced technician needs to execute the acquisition process, he is responsible for creating the chain of custody document, photographing the incident site and assets, and checking the power state of the affected computer (or any other IT asset). If the power is on the procedure for the live acquisition should be executed. RAM data should be exported in the memory dump file using the Volatility and other capture tools to create multiple files for verification. Volatility is a great tool because of cross-platform support and features such as active network connection and process identification and analysis with timestamps. Xplico should be used for packet capture and inspection. Browser history capturer should be used to gather information from the browser. To verify the result tools such as Fiddler, Wireshark, and command line should be used. After all the necessary that has been gathered the acquisition process should continue to the hard drives.

There are types of data alteration prevention devices. Hardware or software write blockers. Depending on the case the technician will either use PALADIN live OS as a software write blocker or connect the hard drive to the Tableau hardware write blocker and use the acquisition tool in the Kali operating system. On Kali tools such as DC3DD and Guymager will be used. The image needs to be copied to several external hard drives. One hard drive will stay as the initial state of the evidence and others will be working versions. Backup of working versions of the discs should be created. The evidence images and files will be transported to the investigation facilities. The chain of cost should be updated after every transfer or major manipulation of evidence. All the steps should be documented. When the evidence arrives for forensic analysis tools such as Hashdeep and Sum tools should be used to check the integrity of data. Afterward, the investigation of generated images, memory dumps, user settings, and data will begin. This part of the investigation will reveal the crucial evidence for the case. Tools such as The Sleuth Kit and Autopsy will be used to determine the data manipulation, deleted files, malware execution artifacts, registry manipulation, and user settings on the mounted image. Other tools such as Volatility and Xplico should be used to determine the active processes and sockets from the generated dumps. Browser data should be analysed to gather the history of internet activity and useful information such as saved passwords. In this part of an investigation, case tools are only media for evidence presentation. The investigator needs to know what to find and where to look for. The future of the case relies on the investigator's skills and knowledge. The biggest focus is on the events and data created in the incident time range. A forensic examiner can be in communication with the client's internal IT team for additional information.

The goal is to gather the evidence and answer the important questions provided by the client (such as who, what, when, where why, and how). An event timestamp collaboration will be identified. The whole process of gathering and analysing the information that led to the conclusion will be documented. The reports will be created using EnCase and Helix 3 Pro tools and consolidated into a single document along with snippets from different tools. A different version of the report document will be available. For internal use, a document with technical details will be created. A PDF summary and conclusion report of the event will be created for the client. On the investigation closer meeting or in the court of law, the fact will be presented understandably, coherently, and concisely, along with an explanation of the procedures and verifications of the evidence integrity. Graphical representation of workflow with the timestamps of the crucial events will be presented in a PowerPoint presentation. Digital forensics is a long process that's why only fast tools that provide reliability and accuracy need to be used. Criminals can make life hard and stressful for investigators. They try to cover their tracks using various anti-forensics methods (encryption, obfuscation, and cloaking techniques) to trick investigators. Cybercrime is a lucrative business and response from law enforcement agencies needs to be equally advanced. They need to continually develop intelligent solutions and educate people to use them. That is the only way to put up with a never-ending battle in the digital world. This is the resulting table from our research, with different tools suggested for different types of forensic analysis:

Tool Type	Primary	Secondary
Write Blocker	Tableau Tk35u, Tableau Tk35e	Coolgear, PALADIN
Acquisition (Hard drives)	EnCase, Guymager	EnCase, PALADIN
Acquisition (RAM)	Volatility, FTK	4-Magnet, 7-RAMcapture
Verification	Sumtools, The Hashdeep	Hash my files, Rahash2
Analysis	The Sleuth Kit, The Autopsy	Encase, Xplico
Reporting	The Sleuth Kit, EnCase, Helix 3 Pro	Powerpoint, Sway
Additional tools	PowerShell, Bash shell	Wireshark, Fiddler

Table 1. Suggested tools

To maintain the integrity of the investigation multiple tools, need to be used. This is a good practice because multiple tools can ensure the verification and backup of evidence. So, if the primary tool is not accurate, we can rely on the secondary tool which is ready. All tools (hardware and software) need to be prepared and maintained. Because of the advancements in technology tools used in digital forensic procedures must be updated regularly. Technology has come a long way and digital forensic incidents are nowadays related to solid-state drives, cloud storage, the Internet of things, fiber-optic connections with gigabit speeds, and SD cards for storage. These new challenges also promote advancements. Understanding core technological concepts such as cryptographic hashing and hard drives are important, the core foundation is still the same.

The future of forensic tools and procedures will depend on the changes in storage demands and storage systems (petabytes and later exabytes of data). The changes will also be influenced by new laws (changes to the existing laws) and practices. The malware and anti-forensic techniques will also improve so the tools used by investigators need to evolve to meet the compatibilities and sophistication of the bad guy's tools. I think that most admins do not think that these tools will ever be useful for their day-to-day tasks, so when the incident happens, they will be forced to outsource the case to some external firm and pay a lot of money for their services. A new investigator that wants to invest time in this field of information technology needs to continually learn to use cross-platform tools in an automated fashion to improve efficiency for the growing demand. Automation of forensics is a topic that needs more research because the incident and systems on which they accrue are not homogeneous, meaning incidents that happen to one client most likely will not happen the same way to others. This is a never-ending, time-consuming process and requires a lot of effort and strong nerves because a single wrong move can jeopardize the whole investigation. The logging and monitoring configurations in the company's systems are of the most value when the incident happens. This system can alert admins and help in reconstructions of incidents and evidence gathering. I think most of the IT admin crowds don't know how to improve the audit and logging settings and leave everything to the default values (why should I change it if it works). This can be problematic when they get hacked or some major incident happens. From a forensic standpoint, we shouldn't be limited to whatever evidence is available, we are responsible for the audit and logging configuration.

Machine-learning-based systems can learn and know the baseline of services and can proactively prevent incidents when the anomaly event happens. These tools will be able to send detailed reports to admins providing facts and evidence in the PDF document that can be automatically sent to the email. These tools such as Darktrace are the best for IT security assurance but very expensive on the other hand. Scientific papers suggest that many tools are impractical and do not meet the industry changes. There is also a lack of standardization of policies, ethics, development, and tools. Currently, there is no single best tool and framework that can cover every process of the investigation. Multiple tools are needed to complete the necessary actions and to verify the results. To provide accountability and retrieval of the lost data state of the art tools need to be used. But a tool is as good as a person using it. Knowledge, experience, and well-defined procedures are the keys to a successful investigation.

5. References

[1] Cisar, P.; Maravic, C.S. & Bosnjak, S. (2014). Cybercrime and digital forensics – Technologies and Approaches, DAAAM international scientific book, pp. 525–542.
[2] Parasram, S.V.N. (2020), Digital forensics with Kali Linux, Packt Publishing, ISBN 978-1838640804
[3] Murry, J. D. (2020). Digital forensic tools in Kali Linux, Pluralsight
[4] Arshad, S. (2020). Digita forensic Getting started, Pluralsight
[5] Kessler, G.C. & Carlton, G.H. (2014) A study of forensic imaging in the absence of write-blockers, Journal of Digital Forensics, Security and Law
[6] Best hardware write blockers for digital investigators. Available at: https://linuxhint.com/best_hardware_write_blockers/ Accessed: 2020-02-11
[7] Montenegro, M. (2020). Starting using Volatility, Pluralsight
[8] Dweikat, M., Eleyan, D. and Eleyan, A., Digital forensic tools used in analysing cybercrime, Journal of University of Shanghai for Science and Technology, ISSN: 1007-6735
[9] The difference between encryption, hashing and salting. Available at: https://www.thesslstore.com/blog/difference-encryption-hashing-salting/ Accessed: 2020-01-10
[10] Kumar, K. at all. (2012), Significance of hash value generation in digital forensic, International Journal of Engineering Research and Development