applied sciences

MDPI

Article

Investigating Proactive Digital Forensics Leveraging Adversary Emulation

Valentine Machaka [1] and Titus Balan [2,*]

[1] Department of Forensic Accounting & Auditing, School of Business & Management Sciences, Harare Institute of Technology, Belvedere, Harare P.O. Box BE 277, Zimbabwe
[2] Department of Electronics and Computers, Faculty of Electrical Engineering and Computer Sciences, "Transilvania" University of Brasov, 1 Politehnicii Street, 500024 Brasov, Romania
* Correspondence: titus.balan@unitbv.ro

Abstract: Traditional digital forensics techniques are becoming obsolete due to rapid technological change. Proactive digital forensic investigations (PDFI) solve the challenges of cloud computing forensics such as evidence identification, collection, preservation, and timelining from heterogeneous cumulative data. Cumulative data heterogeneity poses significant challenges to the sound collection of electronically stored information (ESI) or digital evidence across cloud endpoints and/or networked systems. In addition, the distribution of networked systems and/or cloud environments makes it impossible for forensics investigators to be present at several premises to perform the investigation. Hence, it is important to have PDFI in place to ensure continuous operation in the event of a cyberattack, because it does not require the presence of an investigator at the target location. In this study, researchers put the idea of proactive digital forensics to the test and concluded that it is an indispensable tool for networked systems and cloud computing environments in response to modern-day digital forensics challenges. This research was based on an experimental computer science and engineering approach using a virtualised environment simulating an information communication infrastructure. To generate evidence (digital artefacts), and validate the proof-of-concept, adversary emulation was used by adapting the MITRE ATT&CK framework. Research results have shown that PDFI improves digital forensics activities in terms of speed and accuracy, thereby providing credible and timely comprehensive digital evidence. Enhanced Incident detection capabilities enable an analyst to focus much more on forensic investigation functions and thus perform their tasks effectively. However, the legality of live and/or remote forensics is still of great concern in several jurisdictions, thereby affecting the credibility of digital artefacts obtained in this manner. Nevertheless, where possible, the law component should also be kept up to date with modern-day technologies to solve any inconveniences caused by the ever-growing technology demands.

Keywords: proactive digital forensics; threat intelligence; endpoint detection & response (EDR); forensic triage; adversary emulation; electronic evidence

Citation: Machaka, V.; Balan, T. Investigating Proactive Digital Forensics Leveraging Adversary Emulation. *Appl. Sci.* **2022**, *12*, 9077. https://doi.org/10.3390/app12189077

Academic Editors: Konstantinos Rantos, Konstantinos Demertzis and George Drosatos

Received: 3 August 2022
Accepted: 5 September 2022
Published: 9 September 2022

1. Introduction

Traditional digital forensic techniques and tools are becoming obsolete as a result of technological evolution. Proactive digital forensics is the new trend, as most investigations will not require analysts to be present on the premises to obtain digital evidence. Procedurally, digital forensics has always been performed in a post-mortem analysis fashion [1]. However, in recent times, organisations must shift their focus from a reactionary to a proactive strategy. Technologically enhanced businesses need to realise the potential to detect and analyse potential evidence prior to incidents occurring, preferably when monitoring endpoints or network traffic. This allows for the extraction of evidence for criminal proceedings in a sound and timely manner whilst at the same time proving compliance. Digital forensics aims to obtain good and sound electronic evidence that is admissible in

court. Comprehensive Digital Evidence (CDE) is defined as electronic evidence containing the relevant facts necessary to establish the cause of a case, thereby connecting links to the perpetrator and leading to a successful prosecution [2].

The adversary emulation concept originates from the MITRE ATT&CK group. ATT&CK is an abbreviation for "Adversarial Tactics, Techniques, and Common Knowledge". The framework serves as a model document for tracing various methods threat actors use in the stages of a cyberattack through intrusion and exfiltration of data [3]. During adversary emulation, traces of evidence are created, enabling an investigator to identify, examine, collect, and report their findings. Adversary emulation is an offence team engagement that simulates known threats by leveraging threat intelligence to determine the attackers' actions and behaviours. The difference between adversary emulation and penetration testing stems from the fact that the former employs threat intelligence in addition to exploiting vulnerabilities or weaknesses in a system.

This research paper analyses proactive digital forensic investigations as a solution to current problems emanating from cloud computing and/or networked systems, such as evidence identification, collection, preservation, analysis and timelining from vast sets of cumulative data of a heterogeneous nature. With the increasing complexity of cloud infrastructures and distributed systems, operations must continue in the event of an incident. This study aims to analyse proactive digital forensic investigations by leveraging adversary emulation in a virtualised environment. Henceforth, the objectives for the research consist of enabling forensic-driven endpoint monitoring, simulating adversary emulation, automating the identification and collection of digital forensic artefacts, and, lastly, cross-examining evidence obtained from network and endpoint devices. The desired results were achieved by combining the efforts and functionalities of security operations and an endpoint detection and response (EDR/Digital Forensics) system. This paper is organised as follows: Section 2 details the different types of forensics approaches and related work, Section 3 describes the deployment model for proactive digital forensics, followed by the used methods and materials in Section 4. Sections 5 and 6 detail the results and their interpretation. Section 7 presents future works, and Section 8 is dedicated to conclusions.

2. Literature Review

Digital forensics is described as a part of forensic science that focuses on the investigation and examination of artefacts collected from electronic devices [4]. On the other hand, the National Institute of Standards Technology (NIST) defines it as "the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data" [5]. Proactive forensics may be described as the design and configuration of systems to make the organisation responsive to digital investigations in the future [6]. The authors' concept in [6] is centred around the ability to analyse logs, asserting that proactive forensics are long-term and involve the configuration of alerts and system properties as opposed to impulsive intrusion detection. There are three types of digital forensics: proactive, active, and reactive forensics [2]. Reactive forensics is defined as an examination of computer devices after the incident has occurred—also called dead forensics [7]. In the case that an incident did occur, proactive forensics should have already put in place processes, methods, techniques, and tools on how to conduct the investigation, thus cutting costs, reducing the impact of the incident, and improving investigative efficiency [2,8,9]. Active digital forensics, however, relies on the intrusion detection element to ensure relevant and court-ready electronic evidence when an investigation is deemed necessary [10]. Remote forensic investigations are an essential tool in the implementation of active digital forensics, and this usually requires the analyst to use some programs that pre-existed in the device being analysed within the timeframe of the incident occurring [2].

In [7], the authors performed a systematic literature review, and in their findings, they regarded the multi-component view as too broad, making it inefficient to implement within

automated solutions. Thus, proactive forensics and reactive forensics were added, with the active component removed from the resulting model. Therefore, this study adopted the definition of Proactive Digital Forensics as a method to establish processes, procedures, policies, tools, and technology ahead of time to collect an event/alert and safely preserve and examine evidence in the case of an incident [7]. The main objectives of proactive digital forensics are "system structuring and augmentation for automated data discovery, lead formation, and efficient data preservation" [2]. Proactive forensics has five phases, which are "proactive collection, event triggering, proactive preservation, proactive analysis, and lastly, preliminary reporting" [2]. Proactive digital forensics resemble digital forensic readiness and computer intrusion forensics. Computer intrusion forensics (CIF) differs from classical computer forensics in that CIF occurs when an intrusion has been detected and a need arises to assess the incident, whereas the latter is focused on gathering evidence from digital devices, which may not necessarily be a computer [11].

Intrusion detection is dependent on the analysis of logs and computer audit trails gathered from various critical infrastructures such as routers, servers, and PC workstations. Based on the same principles, forensic readiness aims at making the best use of incident data as evidence whilst minimising the cost of the forensic operation [9,12]. The resulting incident evidence has relevant potential use in internal matters, regulatory compliance, and as evidence in court. It may also be implemented in vulnerability assessments and operational troubleshooting [12]. The extent to which network security services or tools may be used in the collection of evidence from computer and network systems during an incident is unclear [8]. However, a real-time forensic examination may present to the investigators a somewhat theoretical opportunity to extract pieces of evidence about the intrusion. There have been arguments on what is better between a Host Intrusion Detection System (HIDS) and a Network Intrusion Detection System (NIDS); however, due to the sophisticated nature of modern-day attacks, a mixed solution is preferred [9]. Apart from the HIDS, Endpoint Detection and Response (EDR) systems have gained more attention recently because they constantly offer threat monitoring and rapid response, thus ensuring that an entire enterprise is protected at all times [13]. The major advantage of an EDR over the HIDS is that it combines the prevention component, enables investigation after detection, and responds within a single platform, hence providing unmatched security and operational effectiveness [13].

Traditionally, computer forensics is aimed at examining the duplicate bit-copy equivalent of a disk extracted out of memory, file and web history, network connections, jump lists, and link files, which proffer a basic understanding of the activities that would have been performed on a victim's electronic device before it was shut down [14]. Digital forensics can also be performed on live hosts using specialised software. An author in [14] proposed a collection technique in a virtualised environment involving taking snapshots of a virtual machine either through a new virtual machine instance user transfer or the use of an algorithm to determine an incident timeline to take a snapshot. However, traditional digital forensic tools are becoming outdated as technology evolves, and tools such as Forensic Tool Kit (FTK) [15] and Encase [16] might no longer handle the complicated nature of modern systems and applications [17]. Some of the drawbacks of these techniques are that they are unable to extract pre-incidental evidence and they are not very capable of being used remotely, as the communication overhead can largely impact the quality of forensic results [17,18]. The authors in [19] suggest that, for an organisation to be considered digital-forensics-ready, there should be a "communication channel, Encryption, compression, authentication of log data and proof of integrity, authenticating the client and server, and timestamping". In the cloud, there is a point where cloud security and digital forensics converge, and, hence, unifying security and digital forensics may improve the forensic capabilities as well as the security of cloud environments and/or networked systems [20].

3. Conceptual Model

The concept of proactive digital forensics resembles an architecture similar to a security operation centre (SOC), where there is continuous monitoring of the network and endpoint monitoring. Digital forensics and incidence response infrastructure (hardware and software) is installed in advance, anticipating future incidents that may require quick access to electronic evidence artefacts for investigations. Figure 1, below, illustrates the proactive digital forensics concept using a unified modelling language (UML) diagram.

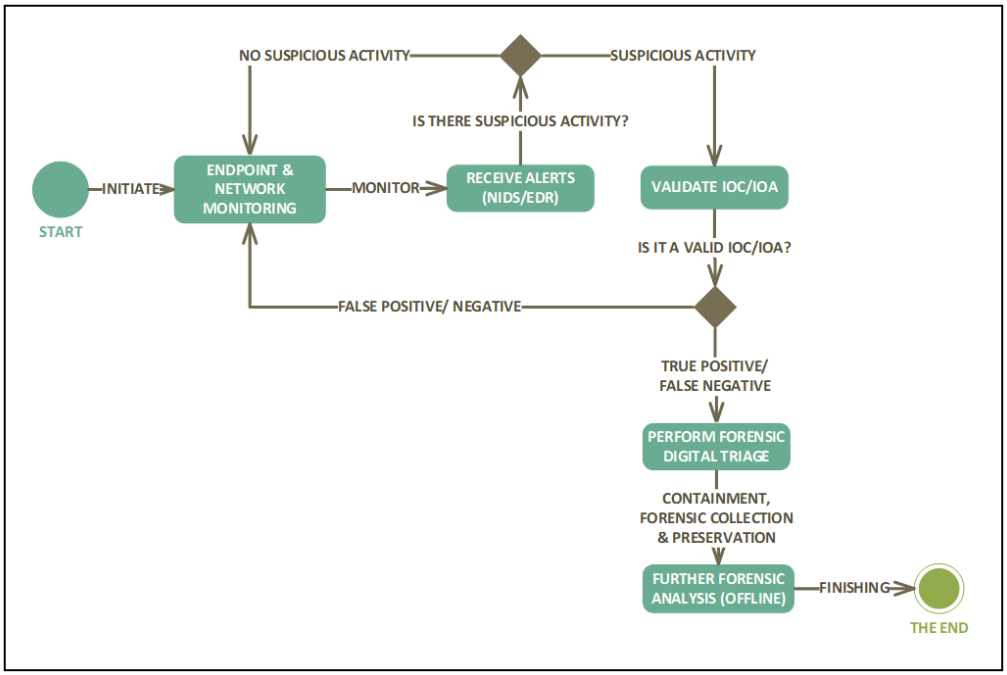

Figure 1. The deployment model for proactive digital forensics.

The proactive digital forensics investigation begins with network and endpoint monitoring, where a monitoring server assisted by an agent (in the case of an EDR) or a network tap (in the case of NIDS) constantly communicates with the network and host devices over a network in the search for suspicious behaviour. The status corresponds to an alert or notification received, and the forensic investigator verifies whether it is a positive, false positive, negative, or false negative. The investigator checks whether an Indication of Compromise (IOC) or an Indication of Attack (IOA) exists or not. Given that it exists, an investigation is initiated either on the network or the endpoint. The identification of artefacts is automatic in known attacks, which makes it easier for the forensic investigator to extract and preserve the evidence. The investigation is performed on top of security monitoring, where there is increased visibility on both the network and endpoint devices. The security events received are based on the NIDS detection capabilities either using signature-based identification or behavioural analysis. Based on the events on the NIDS, the analyst then performs a digital triage on the endpoint to obtain further details.

Unlike the solutions in [11,14,21] of taking a virtual snapshot of the computer system, which can be costly in terms of network overhead due to its size, the PDFI concept implements real-time digital forensic triage. The authors in [22] define a digital triage as a technical process that enables efficient identification, verification, and collection of ESIs to prioritise digital artefacts for easier analysis. There are several definitions of digital triage, nonetheless, the researchers have chosen to use the term "forensic digital triage" because the subsequent results are to be used for a forensic examination. In addition, the collection is done forensically, as the identified digital artefacts/ESI would be validated and verified through a hash signature calculation and transported over a secure network for further analysis, as recommended by the authors in [19]. Furthermore, unlike the traditional digital

forensics model, which does not provide pre-incidental information and analysis (normally done in a post-mortem fashion), proactive digital forensics offers a live examination, thus leading to the faster processing of evidential media. In [23], the authors took a study on the use of keystroke logging as a proactive digital forensics digital preservation technique. However, it is not mentioned that the concept is performing a live investigation or triage in near real-time.

The advantages of the proposed model are forensic readiness, an increase in organisational security posture, proof of information governance (compliance), lower downtime (continued operations), and increased precision of the identification, collection, and analysis of digital evidence. Proactive digital forensics can provide near real-time results, thereby enhancing resilience to threats and information governance needs. However, the legality of live and/or remote forensics is still of major concern in several jurisdictions, thereby affecting the credibility of digital artefacts obtained in this manner. The concept relies heavily on the principles of information security, which are confidentiality, integrity, availability (CIA), authentication, authorisation, and accountability (AAA). SOC architecture and Endpoint Detection Systems should therefore offer the principles mentioned above because security breach data or potential evidential data are categorised as sensitive data.

4. Materials and Methods

This research took an experimental computer science and engineering (ECSE) approach. It is commonly used when information is the key resultant rather than matter or energy [24]. The research design enabled the researchers to test and evaluate theories using a laboratory environment with simulated network infrastructure leveraging virtualisation technologies.

4.1. Architecture Design

A type 2 hypervisor was utilised to set up a basic infrastructural design that simulates info-communication infrastructure, as shown in Figure 2 below. It illustrates how computer hardware with an installed operating system can host several guest computers leveraging a hypervisor. The goal of the hypervisor is to create a link between the operating systems hosted on the virtual machines and the host operating system within the dynamic broadcasting mode [25]. Hence, virtual machines were installed, which are capable of working independently, communicating over a network, and accessing resources offered by the host machine.

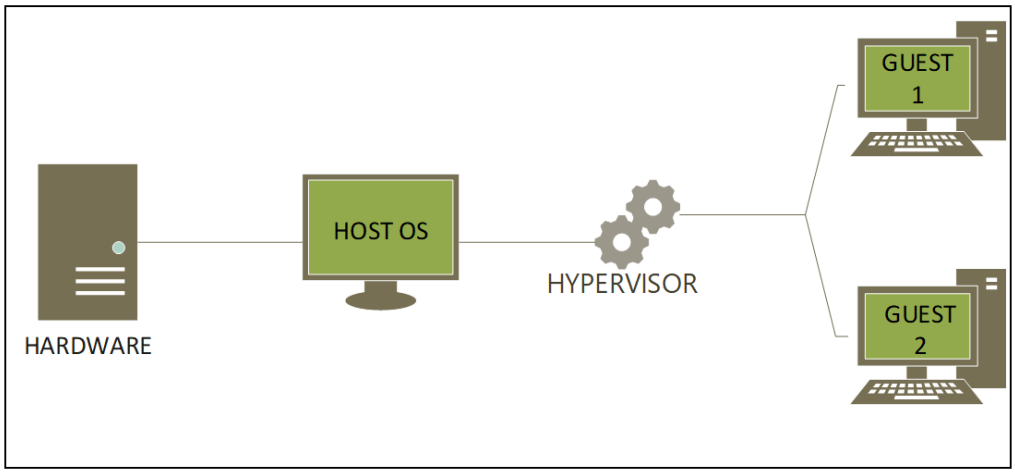

Figure 2. Type 2 hypervisor.

Figure 3 illustrates the virtualised components interaction model. It consists of three parts: the attacker (the threat actor connecting with the external router), the internet, and the internal network (connecting through the inside network). The researchers made use of

the Kali Linux virtual machine as a penetration testing tool [26]. On the edges of the attack region (External) and the internal network (Inside) are two routers. Vyos [27,28] virtualised routers are used to create a WAN network. In the internal network, there is one switch that connects the Linux web server, the Windows server, and the Analyst workstation.

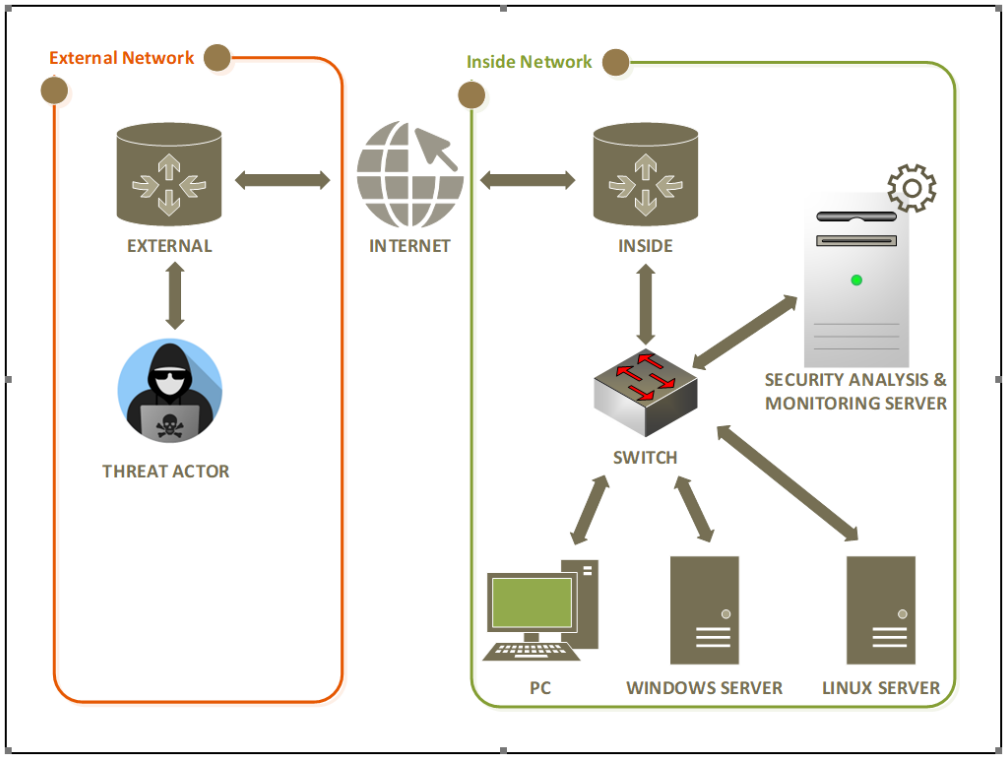

Figure 3. The virtualised components interaction model.

4.2. Research Instruments

To perform digital forensics, the researchers implemented the Integrated Digital Forensic Process model (IDPFM) [29]. The process model has five stages, which are: preparation, incident, incident response, digital forensic investigation, documentation and presentation. To simulate real-world attacks, the researchers adapted the Mitre ATT&CK atomic cycle to invoke or trigger incident detection capabilities. The researchers chose an ATT&CK technique [30], selected a test area, and executed the test to invoke systems security information in the form of events and alerts. In response to the simulated attacks, the researchers closely monitored the EDR and/or NIDS alerts for indications of compromise/attack. The researchers performed forensic investigations on the endpoint and the network, tracing the attack assuming the role of an investigator who does not know how the attack transpired. Figure 4 illustrates the testing technique employed by the researchers.

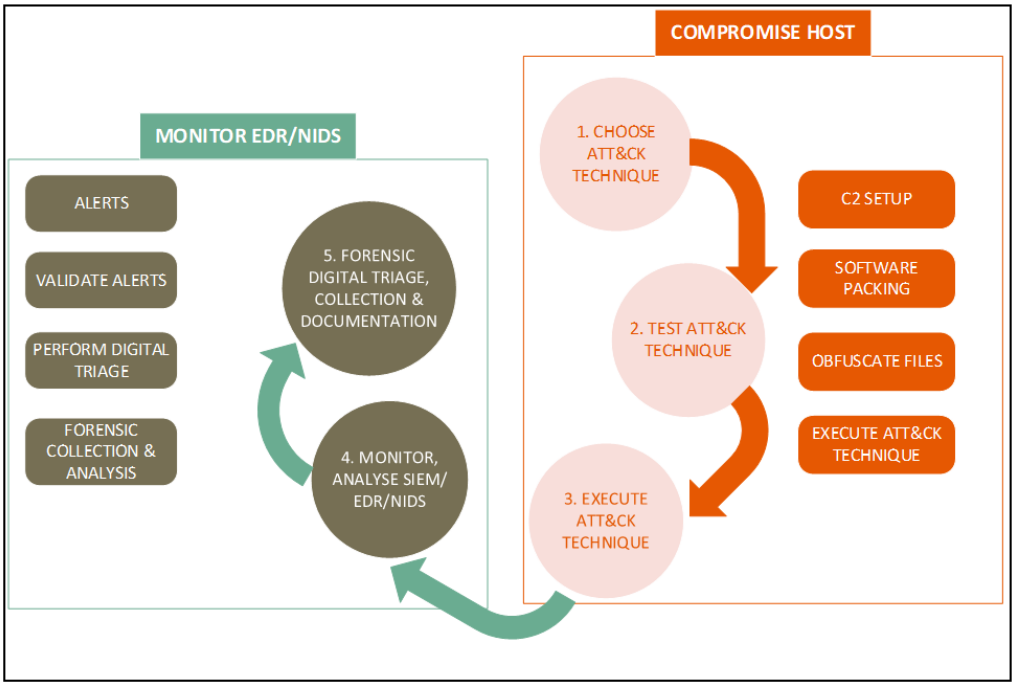

Figure 4. Structured lab testing procedure.

4.3. Tools

Adversary emulation tools such as the Metasploit framework, Covenant C2, PowerShell Empire, Nmap, Hydra, and custom scripts were utilised for the experiment. In response to the launched attacks, digital forensics and incidence response (DFIR) software such as Suricata (NIDS), Wazuh (HIDS), WireShark and CapME (backed by Stenographer), ELK stack, and the Velociraptor Digital Forensics/EDR [31] (Endpoint Detection and Response) were configured. The adversary emulation tools were installed on Kali Linux, whilst the DFIR tools were installed in the Security Onion virtual machine. During the lab experiments, a diverse range of tools mentioned above were used in different scenarios of the MITRE ATT&CK techniques. Nevertheless, the researchers, using judgemental sampling chose to demonstrate the malicious documents' social engineering technique. A malicious payload was generated through the Covenant C2 software. The payload was obfuscated for target system defence evasion, embedded in a Microsoft Excel document, and delivered to the target host. Velociraptor EDR provides security through Single Sign On (SSO) and has authorisation mechanisms through its access list (ACL) model [32], which is the role-based access control (RBAC). This ensures a secure digital forensic triage on top of the confidentiality and integrity mechanisms of the Transaction Layer Secure (TLS) certificates.

Figure 5 illustrates the malicious document execution process whereby a Microsoft document with malicious code is delivered to the target as a decoy document—for example, budget1.xlsm. The user unknowingly enables content on the file, thereby allowing the malicious shell code to connect to a C2 server, where further payloads are downloaded, executed, and extracted and infect the target device. When the target device has been infected by the malware, the threat actor gains access. One of the most important requirements a digital forensics analyst has to fulfil is to determine whether the activities evident (in the form of an audit trail) on the infected computer are due to malware or not.

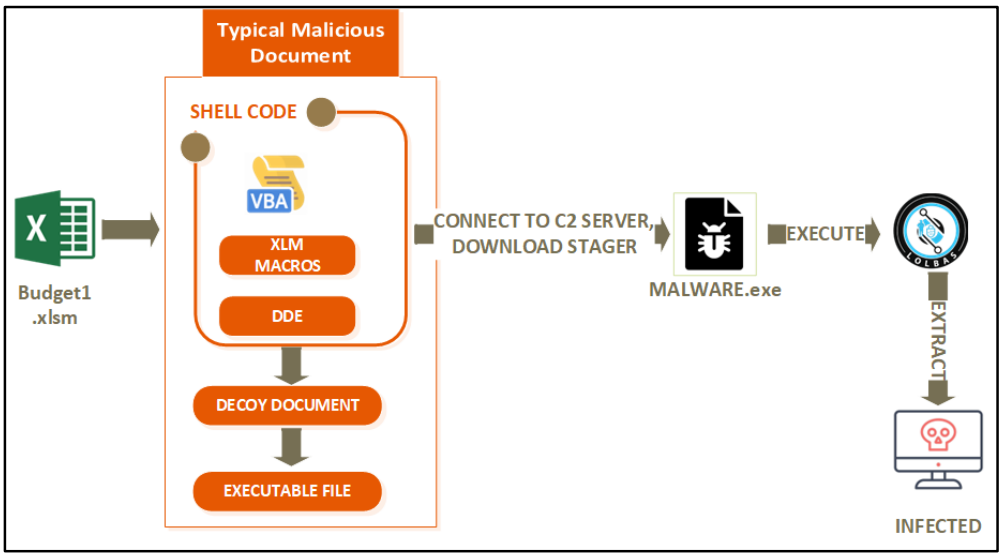

Figure 5. Malicious document execution process.

5. Results

Experimental Scenario: Malicious Documents

Malicious documents fall under social engineering [33], which can be defined as malicious activities that are facilitated through human interaction. The tactic uses psychological manipulation [34], which is the process of tricking a user to perform a certain task that will lead to the giving away of sensitive information or the opening of a backdoor that may compromise a system. The adversary first examines the target and gathers necessary information about an individual or company; then, the adversary searches for weak entry points and security protocols for a successful attack. An example is a phishing email, where a user obtains a malicious document from an email with a script that runs once macros are enabled.

In the lab experiment, the researchers launched an attack using the Covenant C2 framework to generate a payload that can be embedded in a Microsoft Excel document. Figure 6 is an illustration of the payload generation consisting of visual basic code.

The researchers delivered the infected Microsoft Excel document to the targeted machine and simulated the victim's interaction with the malicious document to gain unauthorised access to the victim's machine. Once the attack was launched, from the analyst's perspective, alerts were triggered in the Squert web interface, notifying the analyst of a possible attack.

The alerts shown in Figure 7 indicate a compromised system (hence the insignia colour), and from it, the analyst observed that there was a PowerShell file request made over an HTTP connection which was associated with a Covenant C2 framework attack. However, in real life, these connections may be encrypted with a secure transport (TLS), making the connections difficult to detect. The analyst further examined the alerts to pull a CapME transcript to obtain details of the network traffic flow (Figure 8) and observed a PowerShell script block. The transcript is a textual format of a full packet capture and can also be downloaded as a full network packet capture specifically for that event.

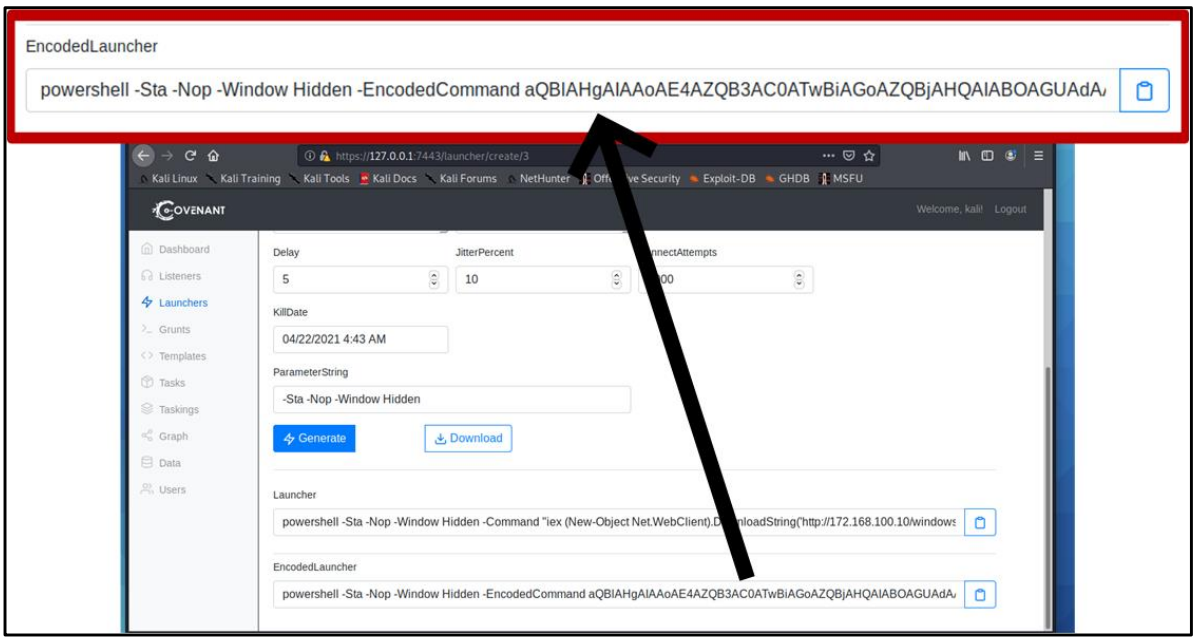

Figure 6. Covenant C2 malicious payload generation.

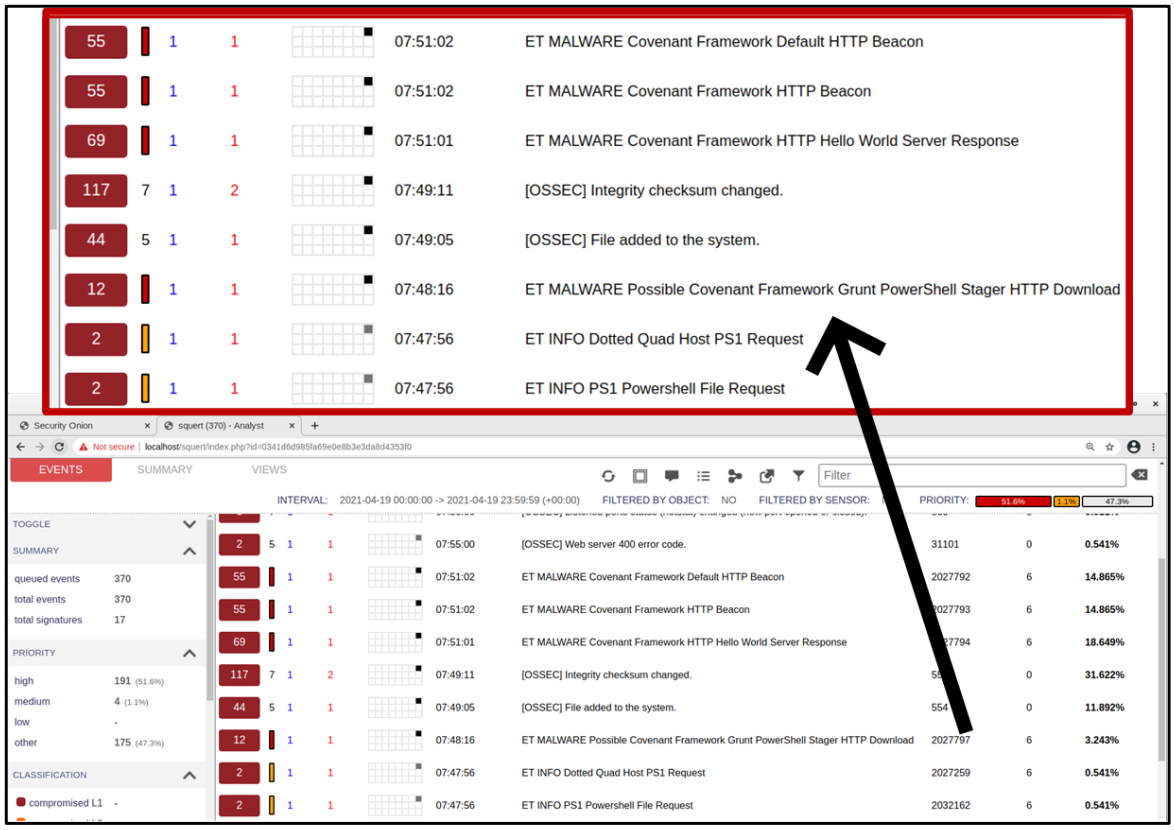

Figure 7. Squert web interface alerts.

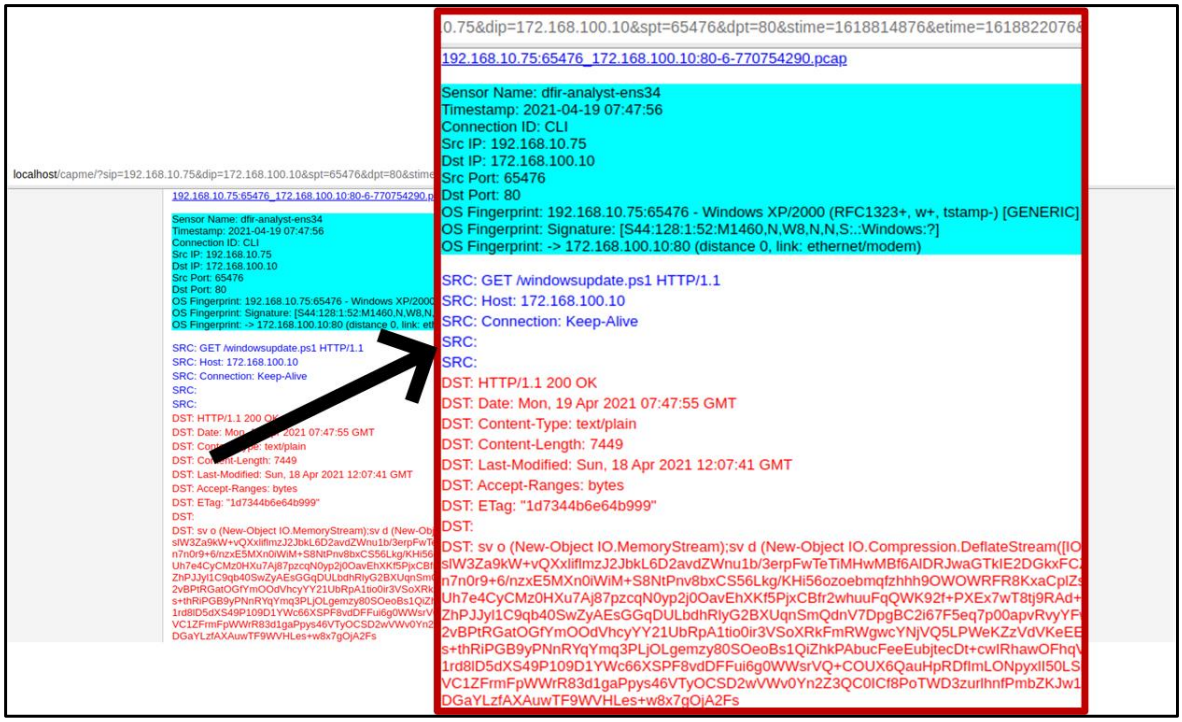

Figure 8. CapME transcript showing the PowerShell stager.

The analyst switched from the Squert web interface to the Velociraptor web interface, a digital forensics/EDR tool, to perform investigations on the endpoint device. The network investigations revealed suspicious behaviour; however, there was no knowledge of how it started, who did it, and so on. A query on events creation was performed using the velociraptor process creation artefact, and several interesting rows were returned, as shown in Figure 9.

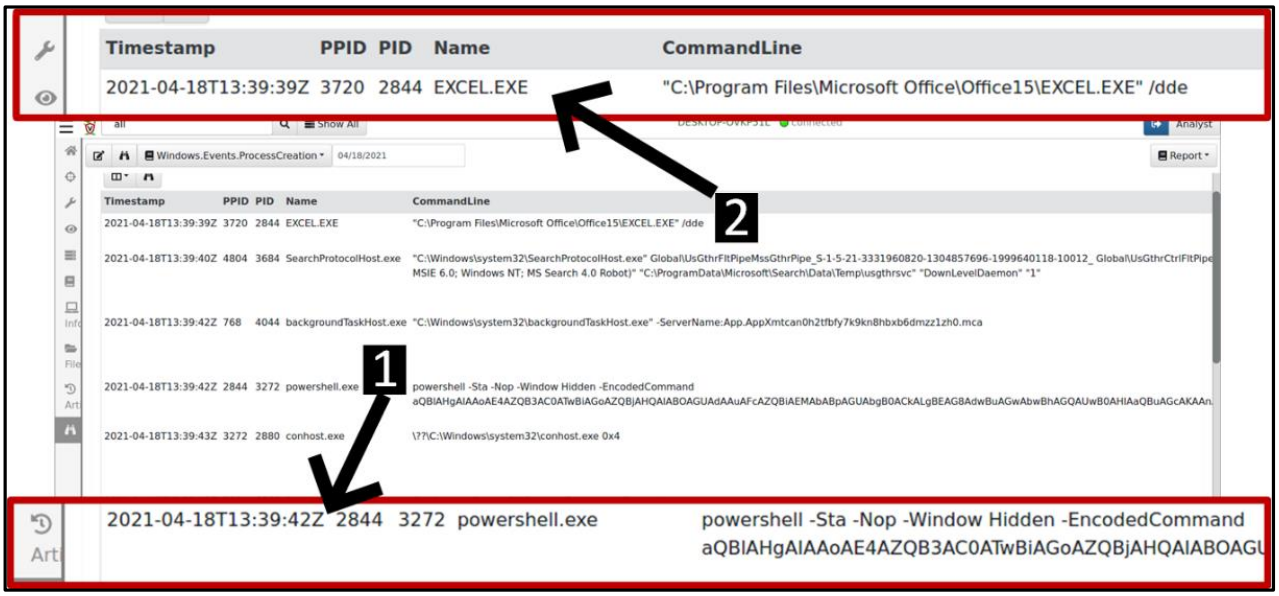

Figure 9. Velociraptor process creation events.

In Figure 9, label 1, the analyst observed evidence of a PowerShell process creation with an encoded command consisting of *-nop* (no profile) and *–Window Hidden* (window

hidden) attributes. It is evident that the excel.exe process with *PID* (process identification number) *2844* initiated the powershell.exe process with *PID 3272*, whilst the powershell.exe invoked the conhost.exe with *PID 2880*, which is used to assist third-party software in initiating and managing the command line. It is not normal for software like Microsoft Excel to launch system programs such as PowerShell, and this is suspicious behaviour.

The analyst queried for a parent-child process attack using the artefact *Windows.Attack.ParentProcess*. The Velociraptor artefact validates whether an adversary or malware is maliciously executing a legitimate process or not. The results showed that powershell.exe was the actual process name, and the actual parent's name was excel.exe. However, since the program is invoking the command line through conhost.exe, the expected parent name is explorer.exe, thus confirming the presence of malicious code executing through a legitimate process, as shown in Figure 10.

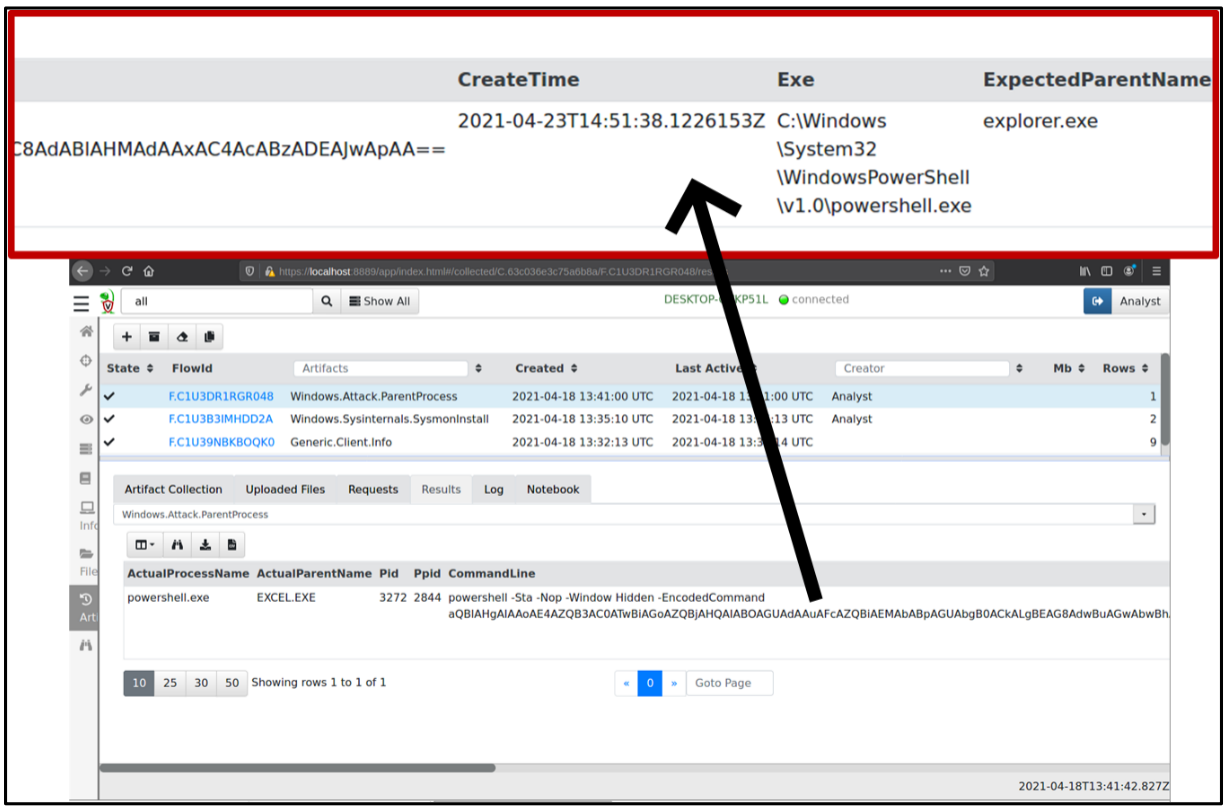

Figure 10. Malicious documents' parent process attack.

Since the PowerShell execution was associated with Excel, the analyst used the *Windows.Registry.EnabledMacro* artefact, and checked whether there was a macro-enabled registration in the registry, and determined the user it belongs to. The results (Figure 11) revealed that the user admin did enable a macro for an Excel document on the desktop.

The researchers used the velociraptor artefact *Windows.Applications.OfficeMacros* to search for documents with macros, and the results are shown below in a CSV file (Figure 12). Therefore, the analyst concludes that the attack was achieved through social engineering, employing a macro-enabled document.

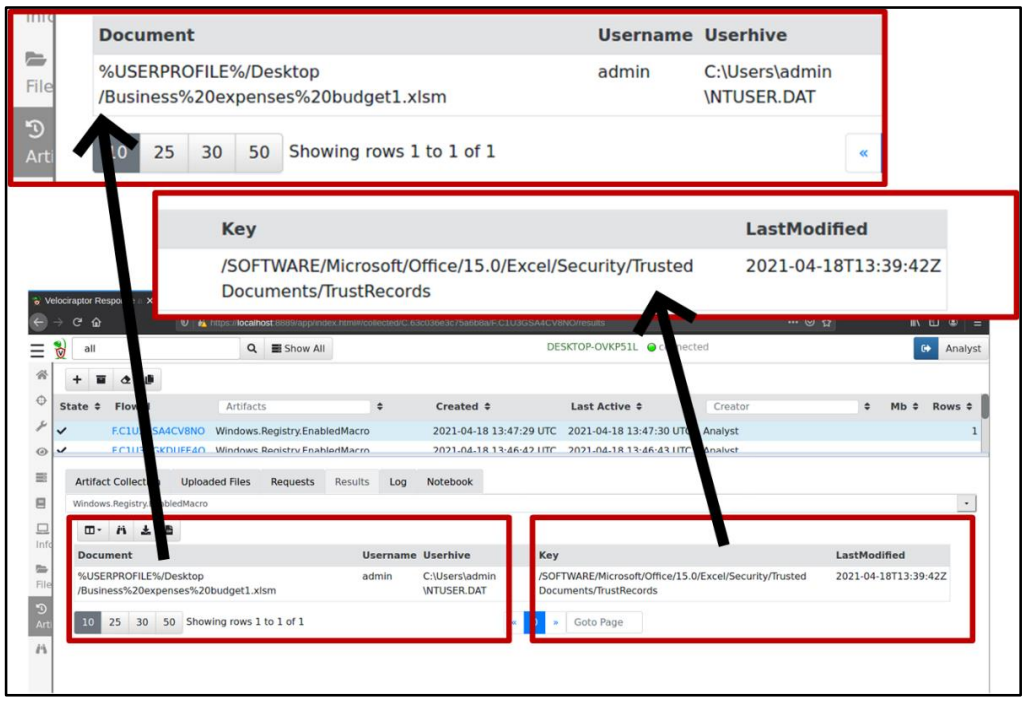

Figure 11. Validation of user action.

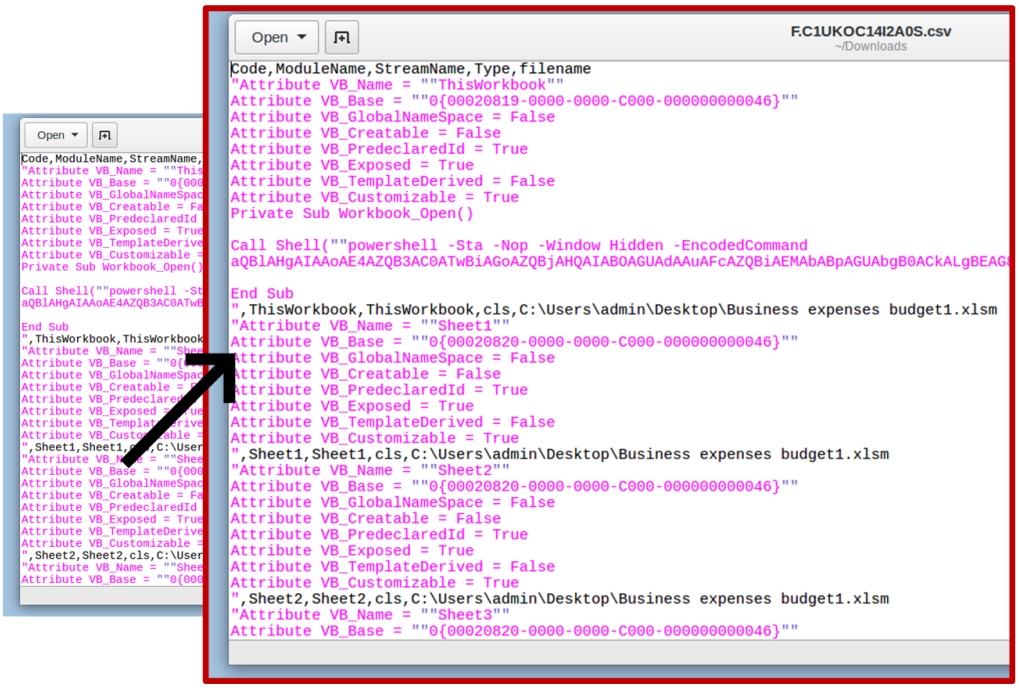

Figure 12. Macros are embedded in the document.

6. Discussion

With reference to the results section, one could observe that the digital triage was a comprehensive investigation that was conducted in near real-time. It tells a story of exactly what happened to the system from the moment of the attack to the execution of the payload and the provision of access to an attacker. Within an organisation that is incidence-response-focused, it would favour the eradication of the threat over the containment and collection of forensic evidence. However, these can occur simultaneously because an organisation will need to prove to the regulator that the attack was beyond its technical and administrative

safeguards in the case of a data breach. The research had four objectives, of which three were met and the remaining one was partially fulfilled. The first objective was to enable forensic-driven endpoint monitoring, and this was achieved by setting up a virtualised networking environment that simulated real-world networks. Of course, the virtualised environment is different from the real world; nevertheless, it provides the basis for the analysis and testing of the concept. This virtualisation setup was comprised of adversary emulation software as well as security monitoring and digital forensic tools. The velociraptor digital forensics/Endpoint Detection and Response software was installed on the monitoring server, and agents were deployed to client/server virtual machines. Through the aforementioned actions, the first step of the proactive digital forensics model was established, which is infrastructure readiness and enhanced incident-detecting capabilities.

Substantially, forensic-driven endpoint monitoring made it possible to effortlessly perform digital forensic functions such as reducing, examining, collating and reconstructing evidence from the network and endpoint devices, thus enabling the analyst to perform their duties effectively [29] whilst obtaining comprehensive digital evidence [2]. The second objective was to simulate adversary emulation that mimics the tactics, techniques, and procedures used by adversaries in compromising networks and systems. The researchers were able to reproduce seven (7) adversary emulation techniques along with the Mitre ATT&CK matrices framework [30]. For illustrative reasons, only one attack scenario has been documented and demonstrated throughout this paper. Among the implemented phases, the researchers can mention reconnaissance, initial access, execution and code persistence, privilege escalation, credential access, discovery and lateral movement, C2, and data exfiltration [35]. This technique allowed the researchers to explore various attack techniques, not only assessing how they are investigated but performing the investigation itself. Several digital forensic concepts were discussed, ranging from file systems and memory forensics to network forensics, hence providing a detailed assessment of proactive digital forensics.

The third objective was to automate the identification and collection of digital artefacts. The automation of the identification and collection of digital artefacts was carried out by the NIDS, which was assisted by Stenographer, a full packet capture software. During laboratory experiments, the researchers observed that automation in the identification component enhanced the analyst's investigative capabilities, making it more efficient to extract digital artefacts. Moreover, the Velociraptor digital forensics/EDR was very resourceful in performing forensic investigations on the endpoint, especially in acquiring live evidence over a network. However, the extraction of the artefact needed an analyst to examine and collect the digital artefacts. Hence, the researchers concluded that automated digital artefact collection can be carried out to a certain degree, that is, through enhanced detection capabilities. Therefore, automation efforts should focus on detection and preservation, while the digital forensic examination itself is performed by a forensic investigator, using their knowledge and skills along with specialised software.

The last objective was to cross-examine digital evidence found from network sources with that of endpoint devices with the intent of corroborating evidence from both perspectives. It was observed that the approach provided thorough insight and coherence between the digital artefacts found on the network and endpoint devices, hence removing any doubt that an incident indeed happened. In some experiments, it was observed that more artefacts were being found on the endpoint as opposed to the network, and vice versa. Hence, having evidence from both the network and endpoint devices will enable an analyst to observe what truly transpired.

7. Future Works

This research's main aim was to study or analyse the concept of proactive digital forensics from a hands-on perspective. The researchers were driven to give an account for proof of work/concept. Past researchers have discussed several types of digital forensics and their application in different industries from a theoretical perspective; however, only a few

had gone through an empirical investigation of the matter [2,6,10,19]. Future researchers can research in the area of automated forensic collection and preservation. Moreover, the concept can be tested with digital twins in the security of cyber-physical systems.

8. Conclusions

The researchers implemented and tested the concept of proactive digital forensics and concluded that it is an essential tool for distributed and non-distributed networked systems and cloud computing environments as a solution to the many challenges currently being faced. The lab environment resembled purple teaming, where red teams and blue teams work together to strengthen security systems; hence, applying the methodology prescribed in this study can assist organisations in testing the maturity of their digital forensics and incidence response functions. The digital forensics arena is complex; there is a need to continuously develop in response to new challenges. The level of trust required for the deployment of this concept has already been established by the SOC architecture. There should be no trust of users or policies—a subsequent measure for monitoring endpoint and network systems. Moreover, the concept deals with highly sensitive and volatile data therefore, authentication, authorisation, confidentiality, and integrity are key success factors in proactive digital forensic examinations. Therefore, modern training methods that can enable new knowledge development should be delivered in this ever-changing environment to enhance detection capabilities and effective cyber incidence responses.

Author Contributions: Conceptualisation, V.M. and T.B.; methodology, V.M.; software, V.M.; validation, V.M. and T.B.; formal analysis, V.M.; investigation, V.M.; writing—review and editing, T.B.; supervision, T.B.; project administration, V.M. and T.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: I would like to appreciate the almighty God, the University of Transilvania, Brasov, and my family for their unwavering support throughout this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Johansen, G. *Digital Forensics and Incident Response*, 1st ed.; Packt Publishing: Birmingham, UK, 2017.
2. Grobler, C.; Louwrens, C.; von Solms, S.H. A multi-component view of digital forensics. In Proceedings of the 2010 International Conference on Availability, Reliability and Security, Krakow, Poland, 15–18 February 2010; pp. 647–652.
3. Pennington, A.; Applebaum, A.; Nickels, K.; Schulz, T.; Strom, B.; Wunder, J. *Getting Started with ATT and CK*; MITRE CORP: McLean, VA, USA, 2019.
4. Tapper, C. *Cross & Tapper on Evidence*; Oxford University Press: Oxford, UK, 2010.
5. Kent, K.; Chevalier, S.; Grance, T. Guide to Integrating Forensic Techniques into Incident. 2006. Available online: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf (accessed on 19 August 2022).
6. Bradford, P.G.; Brown, M.; Perdue, J.; Self, B. Towards proactive computer-system forensics. In Proceedings of the International Conference on Information Technology: Coding and Computing, Proceedings. ITCC 2004, Las Vegas, Nevada, 5–7 April 2004; pp. 648–652.
7. Alharbi, S.; Weber-Jahnke, J.; Traore, I. The proactive and reactive digital forensics investigation process: A systematic literature review. In Proceedings of the International Conference on Information Security and Assurance, Brno, Czech Republic, 15–17 August 2011; pp. 87–100.
8. Kumar, M.; Hanumanthappa, M.; Kumar, T. Network Intrusion Forensic Analysis Using Intrusion Detection System. *Int. J. Comp. Tech. Appl.* **2011**, *2*, 612–618.
9. Solms, S.V.; Louwrens, C.; Reekie, C.; Grobler, T. A control framework for digital forensics. In Proceedings of the IFIP International Conference on Digital Forensics, Orlando, FL, USA, 29 January–1 February 2006; pp. 343–355.
10. Rafique, M.; Khan, M. Exploring static and live digital forensics: Methods, practices and tools. *Int. J. Sci. Eng. Res.* **2013**, *4*, 1048–1056.

11. Balon, N.; Stovall, R.; Scaria, T. Computer Intrusion Forensics Research Paper. In Proceedings of the CIS, Halifax, NS, Canada, 15–17 March 2002; p. 544.
12. Elyas, M.; Ahmad, A.; Maynard, S.B.; Lonie, A. Digital forensic readiness: Expert perspectives on a theoretical framework. *Comput. Secur.* **2015**, *52*, 70–89. [CrossRef]
13. Arfeen, A.; Ahmed, S.; Khan, M.A.; Jafri, S.F.A. Endpoint Detection & Response: A Malware Identification Solution. In Proceedings of the 2021 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 23–25 November 2021; pp. 1–8.
14. Reichert, Z.; Richards, K.; Yoshigoe, K. Automated forensic data acquisition in the cloud. In Proceedings of the 2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems, Philadelphia, PA, USA, 28–30 October 2014; pp. 725–730.
15. Carbone, F. *Computer Forensics with FTK*; Packt Publishing: Birmingham, UK, 2014.
16. Bunting, S.; Wei, W. *EnCase Computer Forensics: The Official EnCE: EnCase? Certified Examiner Study Guide*; John Wiley & Sons: Hoboken, NJ, USA, 2006.
17. Elhoseny, M.; Abbas, H.; Hassanien, A.E.; Muhammad, K.; Sangaiah, A.K. Secure automated forensic investigation for sustainable critical infrastructures compliant with green computing requirements. *IEEE Trans. Sustain. Comput.* **2017**, *5*, 174–191. [CrossRef]
18. Kenneally, E.E. Confluence of digital evidence and the law: On the forensic soundness of live-remote digital evidence collection. *UCLA JL Tech.* **2005**, *9*, 1.
19. Trenwith, P.M.; Venter, H.S. Digital forensic readiness in the cloud. In Proceedings of the 2013 Information Security for South Africa, Johannesburg, South Africa, 14–16 August 2013; pp. 1–5.
20. Alenezi, A.; Zulkipli, N.H.N.; Atlam, H.F.; Walters, R.J.; Wills, G.B. The impact of cloud forensic readiness on security. In Proceedings of the CLOSER, Porto, Portugal, 24 April 2017; pp. 539–545.
21. Birk, D.; Wegener, C. Technical issues of forensic investigations in cloud computing environments. In Proceedings of the 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA, 26 May 2011; pp. 1–10.
22. Jusas, V.; Birvinskas, D.; Gahramanov, E. Methods and tools of digital triage in forensic context: Survey and future directions. *Symmetry* **2017**, *9*, 49. [CrossRef]
23. Makura, S.M.; Venter, H.; Ikuesan, R.A.; Kebande, V.R.; Karie, N.M. Proactive forensics: Keystroke logging from the cloud as potential digital evidence for forensic readiness purposes. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 200–205.
24. Dodig-Crnkovic, G. Scientific methods in computer science. In Proceedings of the Promotion of Research in IT at New Universities and at University Colleges in Sweden, Skövde, Suecia, April 2002; pp. 126–130.
25. Ageyev, D.; Bondarenko, O.; Radivilova, T.; Alfroukh, W. Classification of existing virtualization methods used in telecommunication networks. In Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, 24–27 May 2018; pp. 83–86.
26. Allen, L.; Heriyanto, T.; Ali, S. *Kali Linux–Assuring Security by Penetration Testing*; Packt Publishing Ltd.: Birmingham, UK, 2014.
27. Chaitra, S.; Sharma, R. Integration of software router with Wi-Fi for enhanced security. In Proceedings of the 2017 IEEE 7th International Advance Computing Conference (IACC), Hyderabad, India, 5–7 January 2017; pp. 33–36.
28. Patil, L.; Fernandes, A.; Kahate, A.; Salunkhe, D. Virtual Private Network Implementation on PC as a Router for Privacy of Data Transfer. 2020. Available online: https://www.irjet.net/archives/V7/i3/IRJET-V7I3292.pdf (accessed on 19 August 2022).
29. Kohn, M.D.; Eloff, M.M.; Eloff, J.H. Integrated digital forensic process model. *Comput. Secur.* **2013**, *38*, 103–115. [CrossRef]
30. Strom, B.E.; Applebaum, A.; Miller, D.P.; Nickels, K.C.; Pennington, A.G.; Thomas, C.B. *Mitre ATT&CK: Design and Philosophy*; Tech. Rep.; The MITRE Corporation: McLean, VA, USA, 2018.
31. Cohen, M. Velociraptor: Digging Deeper an Introduction. Available online: https://velociraptor.velocidex.com/velociraptor-e48a47e0317d?source=user_profile (accessed on 19 August 2022).
32. Cohen, M. Velociraptor's ACL Model. Available online: https://velociraptor.velocidex.com/velociraptors-acl-model-7f497575daee (accessed on 19 August 2022).
33. AL-Otaibi, A.F.; Alsuwat, E.S. A study on social engineering attacks: Phishing attack. *Int. J. Recent Adv. Multidiscip. Res.* **2020**, *7*, 6374–6380.
34. Hijji, M.; Alam, G. A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. *IEEE Access* **2021**, *9*, 7152–7169. [CrossRef] [PubMed]
35. Quintero-Bonilla, S.; Martín del Rey, A. A new proposal on the advanced persistent threat: A survey. *Appl. Sci.* **2020**, *10*, 3874. [CrossRef]