Journal of Global Information Management
Volume 30 • Issue 2

Designing and Evaluating an Automatic Forensic Model for Fast Response of Cross-Border E-Commerce Security Incidents

Chia-Mei Chen, Department of Information Management, National Sun Yat-sen University, Taiwan
Zheng-Xun Cai, Department of Information Management, National Sun Yat-sen University, Taiwan
Dan-Wei (Marian) Wen, Guilin University of Electronic Technology, China

ABSTRACT

The rapid development of cross-border e-commerce over the past decade has accelerated the integration of the global economy. At the same time, cross-border e-commerce has increased the prevalence of cybercrime, and the future success of e-commerce depends on enhanced online privacy and security. However, investigating security incidents is time- and cost-intensive as identifying telltale anomalies and the source of attacks requires the use of multiple forensic tools and technologies and security domain knowledge. Prompt responses to cyber-attacks are important to reduce damage and loss and to improve the security of cross-border e-commerce. This article proposes a digital forensic model for first incident responders to identify suspicious system behaviors. A prototype system is developed and evaluated by incident response handlers. The model and system are proven to help reduce time and effort in investigating cyberattacks. The proposed model is expected to enhance security incident handling efficiency for cross-border e-commerce.

KEYWORDS

Digital Forensics, E-Commerce Forensic System, E-Commerce Forensics, E-Commerce Forensics Framework, E-Commerce Security, Forensic Process, Forensics Framework, Incident Response

INTRODUCTION

The explosive expansion of information technologies offers unprecedented opportunities for businesses to expand their markets through cross-border e-commerce, which accounted for roughly 20% of total global online transactions in 2015 (MEDICI Team, 2015) and continues to increase rapidly. The use of ICT is a critical factor in improving service productivity in e-commerce (Rabeh, Islam, Samer, Adnan, & Mustafa, 2019), and the growth of cross-border multi-national e-commerce has set trends for a major overhaul of the online industry (Sanjeev et al., 2019). Many governments consider now cross-border e-commerce as a new dimension of trade (Lianos, Mantzari, Durán, Darr, & Raslan, 2019). However, this increase in cross-border e-commerce activity has been accompanied by a commensurate increase in cyber-crime (Lau, 2018; Shrivastava, 2016). Not only have financial firms suffered serious losses due to cyberattacks (Ismail, 2018), governments, academic institutions, and high-tech firms have also experienced severe information breaches, with significant impacts on policy, research results, and competitive advantage. It is suggested that a serious cyberattack occurs

DOI: 10.4018/JGIM.20220301.oa5

every 39 seconds and that cybercrime could cost businesses up to $5.2 trillion over the next five years (Bera, 2019).

Privacy and security have emerged as two key requirements for successful cross border e-commerce (Karwatzki, Dytynko, Trenz, & Veit, 2017; Sung, 2006; Sutton, Khazanchi, Hampton, & Arnold, 2008). To prevent cyberattacks, businesses promote security awareness through information security education, training and awareness programs which have shown to improve employee security behavior (Winfred, Daniel Okyere, & Peace, 2019). In addition to national regulatory frameworks to promote user privacy protection, trans-national measures have been implemented to ensure cross-border e-commerce security. For instance, in 2016 the Organization for Economic Cooperation and Development (OECD) published its "Consumer Protection in E-commerce" (OECD, 2016) to stress the importance of consumer data security, especially for cross-border e-commerce. In addition, beginning in 2018, EU member states have implemented the General Data Protection Regulation (Tikkinen-Piri, Rohunen, & Markkula, 2018) and the European Data Protection Regulations to harmonize data privacy laws.

In addition to these overarching guidelines for securing e-commerce safety, new attention has focused on measures related to responding to security incidents. As defined in the RFC 2350 ("Expectations for Computer Security Incident Response") (Brownlee & Guttman, 1998), a security incident is any adverse event which compromises some aspect of computer or network security. Generally, it is related to the compromise of confidentiality (e.g., user privacy), integrity (e.g., alteration of confidential information) or availability of information (e.g., Denial of Service attacks). The security incident response process includes evidence collection to facilitate rigorous investigations to protect cybersecurity (Baryamureeba & Tushabe, 2004), entailing evidence acquisition, collection and preservation, analysis, examination, and result reporting (Ademu, Imafidon, & Preston, 2011) using multiple forensic tools and technologies and comprehensive security domain knowledge. This makes identifying and tracking cyberattacks a time- and cost-intensive task for businesses. Moreover, prompt incident response is essential to reducing damage and loss from cyber-attacks.

Digital forensics is a prominent component of incident response and handling that involves collecting and analyzing digital evidence, detecting suspicious patterns of attacks, and presenting an analysis report after a cyberattack incident (Lianos et al., 2019; Shrivastava, Kumar, Gupta, Bala, & Dey, 2018). The goal of digital forensics is forensically examine computerized media to distinguish, protect, recuperate, investigate and express realities and suppositions about advanced data (Shrivastava, Sharma, Khari, & Zohora, 2018). In doing so, evidence reconstruction is achieved after a crime committed by a standalone computer and evidence interpretation from any digital sources (Shrivastava, Sharma, & Dwivedi, 2012).

To fight cyber-crime, digital forensics should acquire as much relevant evidence as possible. Digital evidence (Novak, Grier, & Gonzales, 2018) is stored or transmitted in binary form in various storage media including hard drives, flash memory, random access memory, system logs, application logs, process information, network traffic, etc. The amount of data generated and stored due to our daily activities is increasing rapidly. An IDC study estimated that, in 2020, the world produced more than 5,200 gigabytes of data for each person alive (Gantz & Reinsel, 2012). With the rapid increase of digital evidence, digital forensic investigators have to search through massive amounts of evidence to identify suspicious behavior, raising the need for sophisticated automatic digital forensic tools and procedures (Pollitt, Caloyannides, Novotny, & Shenoi, 2004).

For most e-commerce cyber-attacks, incident handlers require a forensic model to assess a reported incident and prioritize it before initiating a potentially costly and lengthy formal or legal procedure. A digital forensic investigation is often initiated to ascertain certain facts in response to an incident. Prioritizing incidents is critical in the incident response process as well as for damage control. The legal foundation focuses on the use of forensic tools and techniques for the recovery, handling, analysis, and preservation of digital evidence, as opposed to firewalls, antivirus, routing, or intrusion detection. However, the incident response process takes much time and effort (Ryan &

Shpantzer, 2002). Furthermore, most businesses lack the ability to collect, preserve, and analyze digital evidence and to respond and handle security incidents, which raises a critical need for an automatic digital forensic model.

To address the abovementioned issues and to make digital forensics more accessible for understaffed organizations, this research proposes an automatic forensic model that intelligently integrates the multiple incident response stages (evidence acquisition, evidence analysis and correlation, attack detection, and incident report). The proposed model features a knowledge base in place of human security expertise required for evidence analysis and attack detection, thus addressing the shortage of qualified forensic experts. A prototype system is developed for practical evaluation, with the aim to reduce investigation time and thus incident damage.

While prior studies in digital forensics have proposed many methods for evidence analysis or attack detection (Montasari, 2016b; Shrivastava, 2016; Shrivastava, Sharma, & Dwivedi, 2012), none have attempted to design an automatic digital forensic model with a knowledge base that integrates the stages of incident response. The novelty of the proposed model is two-fold: integrating multiple incident response phases and including a knowledge base to perform evidence collection and analysis in an automatic and intelligent way.

This research makes the following contributions: (1) an automatic digital forensic model to integrate multiple incident response and handling stages; (2) a knowledge database to analyze evidence in an intelligent way; (3) a preliminary incident analysis report to assess the severity of an incident and to assist in incident response prioritization; and (4) a prototype system to demonstrate the practicality of the proposed model.

The remainder of this paper is organized as follows. Section 2 provides the relevant forensic background and reviews the forensic process. The proposed model is presented in Section 3. Experimental results applying empirical data to the forensic model are explained in Section 4. Section 5 draws conclusions and proposes recommendations for future work.

RELATED WORK

This section briefly reviews the increasing need for digital forensics in e-commerce, followed by a review of forensic process models.

Increasing Need for Digital Forensics

Increased attention has focused on data privacy (Anderson, Baskerville, & Kaul, 2017; Karwatzki et al., 2017), especially in the context of cross-border e-commerce (Barkatullah & Djumadi, 2018; Frik & Mittone, 2019). Many national governments have launched legislative initiatives to implement improved security requirements. For instance, federal law in the United States imposes obligations on businesses to protect user privacy (Thoren-Peden & Meyer, 2018). In addition, the EU's General Data Protection Regulations require organizations to implement appropriate technical and organizational measures for data protection, and failure to properly handle incidents of data exfiltration can result in exorbitant fines.

Meeting privacy protection regulatory requirements requires effective digital forensics – the search for traces used to track the actions of cyber-criminals (Baryamureeba & Tushabe, 2004; Shrivastava, 2017; Shrivastava, Sharma, et al., 2018). Digital forensics has been useful in monitoring and detecting suspicious transactions in financial transaction systems through database analysis (Khanuja & Adane, 2019). Activities in digital forensics include the acquisition, collection, and preservation of digital evidence, the analysis and examination, and the generation of reports (Abschnitt, 2019; Ademu et al., 2011; Tan, 2001). For example, EU organizations are required to report cyber incidents within 72 hours, with details on the leaked data, ensuing damage, and how the breach occurred. Digital forensics best practices can help organizations meet these requirements.

To this end, organizations need to develop an appropriate capability to preserve, collect, protect, and analyze digital evidence (Reggiani, 2016) so that they can respond quickly to cyber incidents and retrieve digital evidence while it is still available (Park et al., 2018; Reggiani, 2016). Besides, a comprehensive report will be generated based on evidence analysis so that cybersecurity officers can react promptly to secure the organization and to enhance privacy protection.

As web browser sessions have become a common vehicle for cyber-attacks (Umar, Yudhana, & Faiz, 2018), advancing digital forensics to collect and store cybercrime evidence (Arewa, 2018) is of critical importance to privacy protection as e-commerce becomes increasingly borderless.

Digital Forensic Models

According to guidelines for electronic crime scene investigation developed by the U.S. Department of Justice (Ballou, 2010) and others (Shrivastava, Sharma, & Dwivedi, 2012), digital forensics follow four steps: (1) Acquisition – finding relevant evidence at the crime scene which usually starts with acquiring data from the victim's equipment; (2) testing – verifying whether the collected evidence is original and confirming that it has not modified for the following analysis; (3) analysis – searching for traces relevant to the cyber-crime, such as identifying suspicious processes and dubious IP addresses from network traffic, the results of which need to be documented; and (4) reporting – concluding the analysis results and the cause of the incident for further action. These guidelines serve as a foundation for digital forensic models including the Enhanced Digital Investigation Process Model (Baryamureeba & Tushabe, 2004) and its subsequent improvements (Agarwal, Gupta, Gupta, & Gupta, 2011).

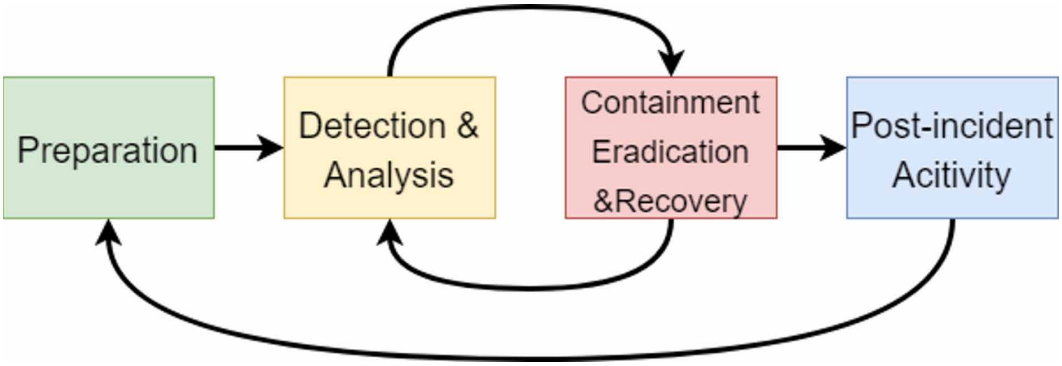
Based on their practical and professional experiences, SANS (Chisholm, 2010) made the following recommendations for digital forensics: (1) use existing tools rather than developing new programs, (2) use live data, (3) conduct bit stream imaging, (4) never add, delete, modify or filter the collected data, (5) hash all the evidence, (6) record all behaviors, and (7) back-up the evidence. These recommendations accentuate the need to integrate existing tools and emphasize maintaining the integrity of the evidence throughout the forensic process. Based on the above recommendations, Van Barr et al. (Van Baar, Van Beek, & van Eijk, 2014) examined whether digital forensic services can ease the burden of forensic experts in the Netherlands. They emphasized the importance of the authenticity and integrity of digital evidence. In response to the need for an integrated forensic model, Yen et al., (Yen, Yang, & Ahn, 2009) implemented a digital forensic system to ease the burden of evidence acquisition on security and forensic staff. Incident investigators still require security and forensic expertise to effectively analyze the evidence.

Forensic process models provide a procedure for investigating security incidents. Yusoff et al. (Yusoff, Ismail, & Hassan, 2011) reviewed several digital forensic models and identified commonly shared processes including pre-processing, acquisition and preservation, analysis, presentation, and post-processing. The Computer Forensics Investigative Process, proposed by Pollitt (Pollitt, 1995) consists of four sequential stages: acquisition, identification, evaluation, and admission. Evidence is collected in the acquisition stage and is analyzed in the identification stage. The evaluation stage concludes the incident analysis result which is presented to the legal authorities in the admission stage.

Palmer (DFRWS, 2001) proposed a digital forensic investigation process based on the model proposed by Yusoff et al., consisting of six stages: identification, preservation, collection, examination, analysis, and presentation. The identification stage performs system monitoring and audit analysis; preservation ensures chain of custody integrity; collection acquires the relevant evidence using approved tools; examination ensures the integrity and validity of the collected evidence; analysis examines the evidence and identifies activities related to the incident; and finally, in the presentation stage, the investigator provides a report describing the incident in detail. Compared with the previous model, Palmer's approach provides more detailed steps for investigators, but both include actions to ensure the investigation's legitimacy.

Reith et al. (Reith, Carr, & Gunsch, 2002) proposed a model based on Palmer's, with nine components: identification, preparation, approach strategy, preservation, collection, examination,

Figure 1. NIST incident response life cycle



analysis, presentation and return evidence. The model provides a general framework that can be applied to a range of incidents but suffers from certain shortcomings, some of which are identified by the authors themselves. The approach is too high-level to be practical, there is no easy method by which to evaluate model performance, and each sub-category is cumbersome to use. Kohn et al. (Kohn, Eloff, & Eloff, 2013) argued that the examination phase should involve extracting potential digital evidence.

Carrier and Spafford (Carrier & Spafford, 2003) developed a model consisting of seventeen phases. The model adapts physical crime scene processes in a digital crime scene, defined as a virtual, software-generated environment that contains digital evidence. Baryamureeba and Tushabe (Baryamureeba & Tushabe, 2004) criticized the model's practicality, suggesting that malicious activity might is not included in the physical or digital investigation, thus negatively impacting the accuracy of event sequence reconstruction.

Kent et al. (Kent, Chevalier, Grance, & Dang, 2006) created a guideline for organizations to develop their digital forensic capability, using IT professionals for information security incident response. This high-level guideline consists of four steps: collection, examination, analysis, and reporting. Beebe and Clark (Beebe & Clark, 2005) proposed a model focusing on lower-level digital forensic activities for practical use. Their model consists of six phases: preparation, incident response, data collection, data analysis, findings presentation, and incident closure. However, its lower-level details are limited to the data analysis phase. Montasari (Montasari, 2016a, 2016b) surveyed the existing digital forensic investigation models, noted the lack of a comprehensive model encompassing the entire digital investigative process, and highlighted the importance of methodical analysis of digital evidence.

The USA National Institute of Standards and Technology (NIST) published its Computer Security Incident Handling Guide (Cichonski, Millar, Grance, & Scarfone, 2012) to establish a successful incident response. As shown in Fig. 1, the guidelines recommend an incident response model consisting of four phases: preparation, detection and analysis, containment eradication and recovery, and post-incident activity. During the preparation stage, an organization implements preventive controls. The next two phases often cycle back and forth as an incident might involve additional hosts. The detection and analysis stage defines incident severity and alerts the organization. Once the incident is adequately handled, the organization reports the cause of the incident along with steps to be taken to prevent future incidents.

Source: Cichonski, Millar, Grance, and Scarfone (2012)

The above-mentioned models mostly provide general forensic processes that involve whole organizations along with some external parties or artifacts such as security controls, written documents,

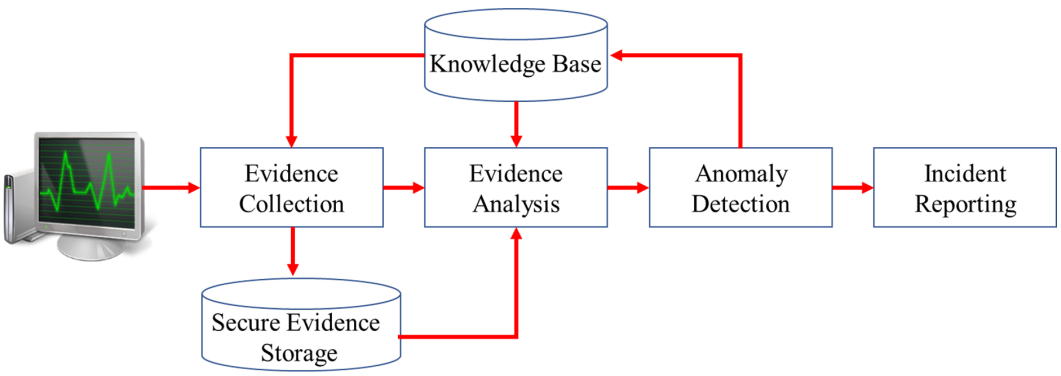
personnel, etc. This study builds on the prior work, developing a model for first incident responders to efficiently handle information cyberattacks and prioritize incidents for further actions.

Evidence collection, analysis, and detection are key issues in the design and implementation of a forensic model, and determine incidence response efficiency and timeliness, along with the extent to which damage can be controlled. To our best knowledge, the present study is the first to attempt the automation of incident handling from evidence collection through analysis and detection, using the integration of various forensic techniques to establish an automatic forensic model.

METHODOLOGY

Despite being developed as a proactive measure, Digital Forensic Readiness is mostly implemented only at the policy level (Park et al., 2018). Thus, a real practical forensic model is needed. This study proposes a digital forensic model to help organizations comply with readiness policy. The proposed automatic forensic model collects and analyzes digital evidence for incident handlers to identify attacks and anomalies. The proposed model follows the incident response life cycle recommended by the NIST (Cichonski et al., 2012) and provides a preliminary incident investigation to assist first responders in promptly and efficiently assessing incident severity. Furthermore, a knowledge database is designed to replace human expertise for evidence analysis and attack detection. The third phase of the guideline, Containment Eradication & Recovery, requires that forensic professionals manually inspect suspicious behaviors to prevent the accidental removal of important files. Therefore, the proposed model eliminates this phase and produces an incident report for incident handlers. The model consists of the following phases: evidence collection, evidence analysis, attack detection, and incident reporting. Figure 2 below provides a detailed illustration of the proposed model.

Figure 2. Proposed automatic forensic model



NIST (Mukasey, Sedgwick, & Hagy, 2008) suggests that evidence acquisition and evidence analysis should be performed on two separate machines to ensure evidence integrity. Thus, the proposed model exports the collected evidence in a coherent format to a remote machine for future analysis and data integrity can be ensured through various cryptographic methods, such as hashes or blockchain.

The knowledge base consists of two parts. The first part is used for evidence collection and stores information about where the digital evidence is located, as it may be located at different resources and different system versions keep event log files in different folders. In the initial evidence collection phase, incident handlers could customize the evidence acquisition rules based on the characteristics of the target incident by modifying the configuration files.

Evidence analysis and attack detection is very time-consuming and requires security professionals to manually search massive amounts of evidence data to find traces of suspicious activities. To increase the efficiency of this labor-intensive task, the second part of the knowledge base contains patterns of misbehaviors such as signatures of malware, indicators of compromise, malicious payload patterns, or malicious domains, and is used for evidence analysis. Security experts or machine learning models can be used to develop this function using security advisories and vulnerability reports. The knowledge base should be updated whenever a new attack is identified or a new vulnerability is reported. It can be updated automatically through cyber threat intelligence provided by venders or an open source threat sharing platform such as (TBA) MISP[1]. Using the knowledge base, the proposed model automatically analyzes the evidence by searching for activity patterns that describe the signatures of anomalies.

MODEL IMPLEMENTATION

To evaluate the practicality of the proposed model, an automatic forensic system (AFS) based on the proposed model is implemented for Window-based systems. The SANS white paper (Chisholm, 2010) suggests that adopting existing software in evidence collection is preferable than implementing a new solution. Hence, our implementation attempts to integrate existing tools as follows.

Phase One: Evidence Collection

In the implementation, the developed AFS collects the following evidence sources from the victim machine: network, processes, registry, and event log. Malware may exhibit various anomalous behaviors such as executing as system process or commonly-used browsers, modifying registry values, connecting to control and command server, etc.

The evidence collection module locates and collects evidence according to the knowledge base configuration. The collected evidence is stored securely with integrity protection by a hash standard, such as SHA256. To automatically acquire verifiable evidence, the evidence collection tools are chosen based on the following criteria: provided by system vendors or open source; facilitated with script or command interface; and can export evidence found.

After careful selection, five tools are adopted for collecting evidence from various sources including network, process, system setting, and system logs (see Fig. 3). For network evidence, CurrPorts is a network acquisition tool collecting network connection information on a target machine. Process evidence is collected using two Windows built-in tools: WMIC and Procmon. WMIC provides basic information about the running processes on a target machine, and Procmon captures detailed process behaviors including file and system activities. With respect to system setting and logs, Windows built-in Wevtutil is applied to retrieve Windows Event Logs and Autoruns to extract registry information where Windows stores system configuration and the processes running during system boot.

Like commercial evidence collection tools, the implemented evidence collection module integrating the above tools is provided in a portable device, such as a USB flash memory, and can be executed directly without extra installation, fulfilling NIST requirements. The algorithm of this module is presented in Fig. 4. It loads the evidence collection rules from the knowledge base and executes the digital evidence acquisition tools to collect raw evidence. The raw evidence in various formats is transformed into the unified format, CSV, and stored to the database for analysis.

Phase Two: Evidence Analysis and Attack Detection

In this implementation, the evidence analysis and attack detection phases are combined into a single module. A replicate of the collected evidence is produced for analysis to preserve evidence integrity. The evidence is analyzed based on misbehavior patterns described by the knowledge base and all suspicious behaviors identified from various evidence sources are correlated to improve detection performance.

Figure 3. Selected evidence collection tools and collected evidence

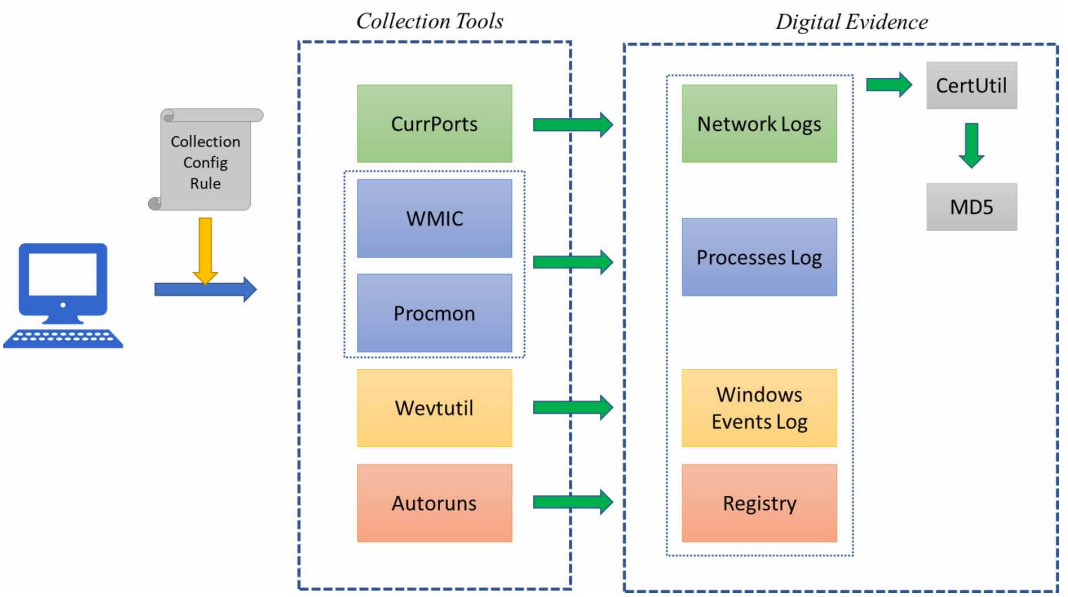


Figure 4. Evidence collection algorithm

```
Function EvidenceCollection()
{
    from knowledge_base import rules.collection
    import AFS.collector # Purposed system.
    # Read collection rules from knowledge base.
    collector.readRules(rules.collection)
    # Execute and get results from those digital acquisition tools.
    Foreach tool in acquisition_tools:
        evidence.append(collector.execute(tool).getResults())
    # Preprocessing the evidence and store to database, without changing original evidence.
    Foreach evid in evidence:
        save_to_db(collector.preprocessor(evid))
}
```

The process of evidence analysis and detection is illustrated in Fig. 5 and its pseudo code is presented in Fig. 6. The process contains analyzing different kinds of evidence and comparing patterns with known attack patterns in the knowledge base, thus to detect suspicious processes. The evidence analysis module individually analyzes the different types of evidence and then correlates them together. The knowledge base information can provide misbehavior patterns in the abovementioned evidence

Figure 5. Process of evidence analysis and attack detection

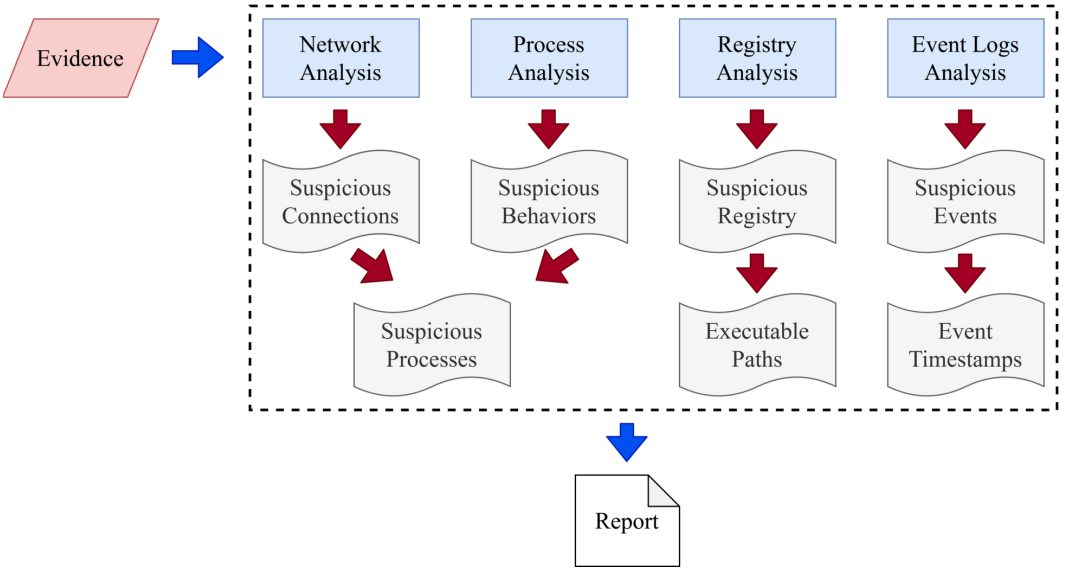


Figure 6. Algorithm for evidence analysis and attack detection

```
Function EvidenceAnalysisAttackDetection()
{
    from knowledge_base import rules.analysis
    import AFS.analyzer # Purposed system.
    # Fetch analysis rules from knowledge base.
    analyzer.readRules(rules.analysis)
    # Read preprocessed evidence from database.
    evidence = read_from_db().orderedByCategory()
    Foreach cat in evidence.category:
        Foreach item in cat:
            info.append(analyzer.analyze(data = item, category = cat))
    correlated_evidence = analyzer.correlate(info, keys = rules.analysis.correlation)
    Foreach process_info in correlated_evidence:
        Foreach rule in rule.analysis.misbehavior:
            if (match(process_info, rule)):
                suspicious.append(process_info)
}
```

types, for example, searching for suspicious network connections to malicious domains listed in the knowledge base. The process evidence analysis identifies abnormal parent-child process relationships or suspicious process behaviors, such as file access or network connections. The registry evidence analysis checks for suspicious software running in system boot; the system event log analysis checks for suspicious process activities. Suspicious behavior may appear in different types of evidence; for example, suspicious network connections can be captured by network evidence and event logs. Therefore, the results from the above evidence analyses are correlated and integrated by process ID in the final step, so that network and process analyses jointly offer general information of the suspicious process, registry analysis provides the location of the process, and event logs analysis gives the specific timestamp of the suspicious activities.

Phase Three: Incident Reporting

Incident reports are generated based on the detection results from the previous module. Evidence for identified suspicious behaviors is displayed for human inspection during the third phase of the incident response life cycle. An incident report is exported in Jason format, including the detection results of suspicious processes, files, network connections, and events.

EVALUATION

Based on incident response time metrics (Hoffman, 2018), the average time detection time is 84 days. An automatic forensic system could provide a quick review of security incidents and shorten the incident response time. To evaluate the performance of the proposed forensic model, two experiments were conducted. Experiment 1 evaluates whether the proposed system can identify misbehaviors by tested malware, with detection results validated by human experts. Experiment 2 compares the time efficiency of the proposed system against professional forensic investigators.

The system implementation and experiments are written in Python 3 on a personal computer with Intel Core i5 7500 processor (2 cores) and 4GB RAM. The implemented system was tested on various operating systems including Windows 7, 8, 10, and Ubuntu 16.04.

Various types of malware listed in Table 1 were tested on a fully patched Windows 8 machine, including backdoor, Trojan, and ransomware. In real cases, evidence is mixed up with a large amount of normal user behavior data. Therefore, to mimic real-world attacks, the victim machines were installed with commonly used applications and operated by normal users over time so that the collected evidence included mostly normal behaviors like document editing, web browsing, program development and

Table 1. Evaluated malware.

Malware
Backdoor.W32.Buterat!c
TrojWare.Win32.CoinMiner.B
TrojWare.Win32.Ransom.Locky.AI
Trojan-Banker.Win32.Emotet.ayjo
HEUR:Backdoor.Win32.Agent.gen
Trojan.Win32.Siscos.wgv
Trojan-Ransom.Win32.GandCrypt.cja
HEUR:Trojan.Win32.Generic
Trojan.Ransom.BlackRuby

testing, gaming, video conferencing, etc. The average time for AFS to collect necessary evidence is half an hour after an attack takes place.

Experiment 1: Detection Verification

Experiment 1 verifies whether the incident reports generated by AFS could identify suspicious behaviors due to attacks. The incident reports of the above mentioned malware were reviewed by an incident handler and all were verified as correct. The verification results demonstrate that the proposed model and the developed system can identify attacks with 100% accuracy.

To demonstrate the identified suspicious behaviors of the incident report, Fig. 7 presents a summarized incident report for malware TrojWare.Win32.CoinMiner.B is organized into three parts: suspicious registry, suspicious processes, and log records of suspicious events. This malware sample disguises itself as a screen saver file, photo.scr, and updates the registry to run whenever the victim machine boots up, launching a brute force attack on port 21, spawning processes and threads to mine cryptocurrency, and erasing and turning off the audit log in order to cover its traces. The summary report successfully identifies the above suspicious behaviors and provides their key information.

The suspicious registry part identifies which registry entries were modified and which suspicious executable files were added to run automatically at startup, as shown in Box 1. The suspicious process part identifies process ID 2064 as having created many connections to port 21 performing brute force attacks and forking many processes and threads, as shown in Box 2. The log records of suspicious events as outlined in Box 3 indicate that the audit log was cleared out (event ID 1100) and the event logging service was shut down (event ID 1102). Some malware might perform the same function multiple times to ensure the expected action has been completed, and the malware tested performed audit log deactivation multiple times.

The system verifies the malware using VirusTotal. The report provides the detection result and indicates the location of the suspicious process for incident handlers to perform malware removal, as shown in Boxes 1 and 2. Incident handlers can retrieve the corresponding evidence through the location provided by the report. The proposed system provides detailed information for each part in case incident handlers intend to examine specific misbehavior. For illustration, a snapshot of network misbehavior report shown in Fig. 8 demonstrates that process ID 2064 has made many connections to port 21 of many remote hosts and attempted brute force attacks. The names and locations of the suspicious processes are provided as well.

Experiment 2: Time Efficiency Comparison

The volume of evidence might affect analysis and detection time. This experiment evaluates time performance with different volumes of evidence by AFS and human investigation. The evidence used in this experiment was obtained from executing various types of malware, and the volume of evidence had huge differences on time because of the characteristics of different malware behaviors. For example, few ransomware behaviors were performed once all files were encrypted, but the cryptocurrency miner kept running and produced many activities such as connecting to the mining pool and exhausting computer resources. To demonstrate the detection time efficiency, the proposed system is compared with a professional human investigator recruited from TACERT (Taiwan Academic Network Computer Emergency Response Team) with more than five years of experience in incident handling and digital forensics. The participating investigator manually reviewed the evidence and provided incident investigation reports. The proposed system and incident investigator analyzed 10 various incident cases and the time needed for analysis and detection was recorded. Table 2 compares the time performance between the proposed system (column: Time by AFS) and the human investigator (column: Time by investigator).

The results demonstrate that AFS is on average nine times faster than human investigation. In addition, the time required by human investigation varied more significantly than the proposed system, especially when dealing with evidence of different levels of volume and complexity. The standard

Figure 7. Sample incident report of "TrojWare.Win32.CoinMiner.B"

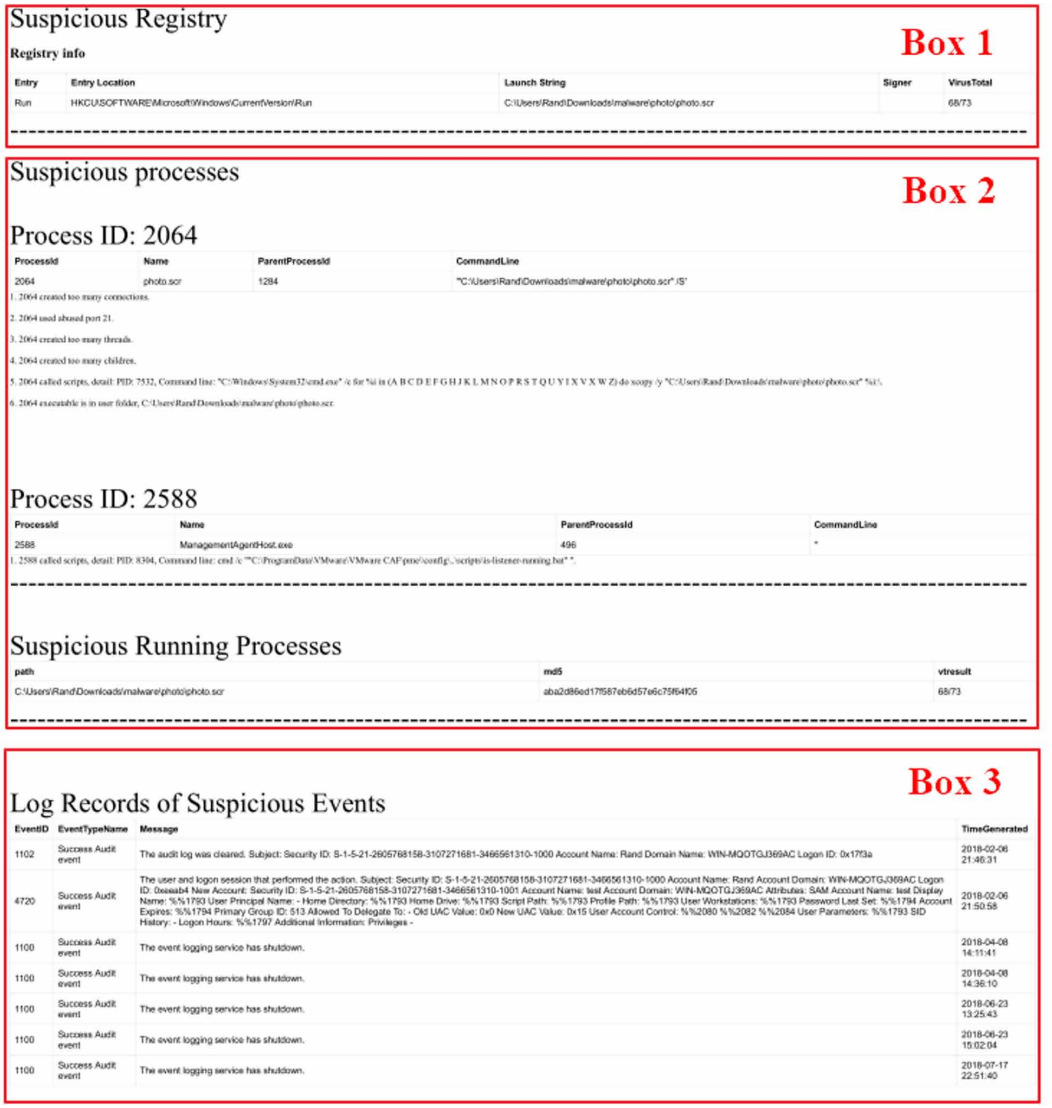


Figure 8. Snapshot of a detailed incident report on network misbehaviors

processes that made too many connections

processID	processName	localAddress	localPort	remoteAddress	remotePort	state	protocol	pathType	processPath
2064	photo.scr	192.168.91.159	15990	219.240.167.36	21	Syn-Sent	TCP	User folder	C:\Users \Rand\Downloads \malware\photo \photo.scr
2064	photo.scr	192.168.91.159	15989	144.88.46.36	21	Syn-Sent	TCP	User folder	C:\Users \Rand\Downloads \malware\photo \photo.scr
2064	photo.scr	192.168.91.159	15988	163.104.46.36	21	Syn-Sent	TCP	User folder	C:\Users \Rand\Downloads \malware\photo \photo.scr
2064	photo.scr	192.168.91.159	15986	32.74.156.36	21	Syn-Sent	TCP	User folder	C:\Users \Rand\Downloads \malware\photo \photo.scr
2064	photo.scr	192.168.91.159	15991	170.187.159.36	21	Syn-Sent	TCP	User folder	C:\Users \Rand\Downloads \malware\photo \photo.scr
2064	photo.scr	192.168.91.159	15662	10.76.32.36	21	Syn-Sent	TCP	User folder	C:\Users \Rand\Downloads \malware\photo \photo.scr
2064	photo.scr	192.168.91.159	15985	60.30.192.36	21	Syn-Sent	TCP	User folder	C:\Users \Rand\Downloads \malware\photo \photo.scr
2064	photo.scr	192.168.91.159	15984	62.237.105.36	21	Syn-Sent	TCP	User folder	C:\Users \Rand\Downloads \malware\photo \photo.scr

Table 2. Time performance comparison

Size of evidence	Time by AFS (secs)	Time by investigator (secs)	Speedup Ratio (Investigator/AFS)
216MB	19	198	10.42
244MB	18.67	194	10.39
245MB	15.67	165	10.53
262MB	19.33	244	12.62
326MB	21	313	14.90
478MB	23.67	177	7.48
593MB	24.67	342	13.86
695MB	26.33	350	13.29
1.15GB	34.33	152	4.43
1.51GB	44.67	166	3.72
Avg size: 578.2MB	Avg: 23.38 MB/s	Avg: 2.51 MB/s	Avg: 9.30

deviation of the analysis and detection time by AFS is 8.75 seconds, while that by the investigator is 77.15 seconds. Shortening analysis and detection time facilitates timely response to cyberattacks and damage reduction, thus the time efficiency demonstrated in this experiment illustrates the value of the proposed model for improved cyber security.

DISCUSSION

This research aimed to propose a model for automatic digital forensic that integrates incident response stages and propose a system with an expert knowledge base for general system administrators. The model consists three phases (i.e.: evidence collection and preservation, evidence analysis and attack detection, and automatic report generation), and the system was implemented and evaluated using two experiments. The results of the first experiment demonstrate that the proposed model successfully identified potential threats, while the second experiment demonstrated that the proposed automatic forensic model can provide significant time savings for investigators. The system's average processing time is 23.38 MB/s compared to 2.51 MB/s for manual investigation. Our experiments confirmed that adopting a knowledge base can facilitate identifying cyber threats automatically. In particular, we improved digital forensic by consolidating multiple stages in one system to shorten time needed to generate a preliminary forensic report. To confirm the reliability of the results, the participants in the model and system evaluation were required to have related forensic experience and professional knowledge, thereby making them competent to provide insights.

There are several theoretical and practical implications of this research. First, we highlighted developing a database of expert knowledge and revealed that a knowledge database has a vital role in reducing the time required for digital forensic processes. The experiment results demonstrated that an expert knowledge database can reduce human effort in the forensic process. Second, document transformation methods and rule comparison tools can be used to develop an automatic and integrated forensic system to produce informative forensic reports. The evaluations strongly supported the implementation of this system to connect existing applications for different stages in digital forensic, and significantly demonstrated the usefulness of the system in improving the efficiency for digital forensic.

Third, this research has an important implication for e-commerce, which has been seriously challenged by increasing amount and complexity of cyber threats. The results of this research showed that an automatic and integrated digital forensic tool is capable of enhancing defend against cyber threats. Last, while digital forensic used to consume much time and energy of experts to provide reports for companies to take corresponding actions when facing cyber threats, this research provides a substitute for expert involvement so that e-commerce firms can respond to cyber threats with less human efforts. The findings suggest merit in further exploring the possibilities of automation in defending cyber threats.

In spite of the aforementioned implications, this research has some limitations. First, we evaluated the model and system with nine more common viruses used in cyber attacks. The validity of future experiments could be improved if a wider range of viruses is tested with the model and system. In addition, although this research integrated the most accepted and suitable application that was originally tailored for one specific digital forensic stage, further development of a model and system that can incorporate more applications would contribute to more comprehensive employment of automatic digital forensic.

CONCLUSIONS AND FUTURE RESEARCH

Increasingly sophisticated cyberattacks threaten customer privacy and transaction safety, raising the need for automatic and integrated digital forensics (Umar et al., 2018). This research provides an automatic digital forensic model comprising evidence acquisition, evidence analysis, attack detection,

and incident reporting, and integrating a knowledge base built with the relevant knowledge of security professionals. The model follows the NIST incident handling guide and streams incident handling phases in a pipeline. The proposed model meets the criteria of minimizing the impact of cyberattacks (Khanuja & Adane, 2019) and gathering evidence from multiple sources (Arewa, 2018). As most e-commerce firms lack digital forensic capabilities to respond to security incidents in a timely manner (Hutchings, 2012), this research provides two major contributions to enhancing cybersecurity in this era of rapid expansion and increasing complexity of cross-border e-commerce: (1) automatic detection of suspicious behaviors and events and (2) generation of timely forensic reports to facilitate efficient handling of cyber incidents. To sum up, the proposed digital forensic model, together with the implemented system, facilitates improved cybersecurity for cross-border e-commerce.

Nevertheless, this research leaves room for improvement, including the development of fully automated data collection. In the current research, evidence acquisition is triggered by an indication of attack. Cyber criminals are increasingly capable of removing the traces of their attacks, necessitating the automatic collection of potential evidence before attacks are confirmed. This is different from simply collecting log files for transactions. Storing log files is a means of passive protection allowing investigators to excavate traces as needed. Modern machine learning techniques can help construct proactive protections by building models to detect suspicious connections or transactions at a very early stage, and initiate evidence collection prior to any trace removal. Another improvement towards automatic forensics would be building a feedback mechanism into the system. As massive attacks of the same type tend to take place in a concentrated period of time, when one type of attack is confirmed by the proposed system, related information can be used for proactive protection against similar attacks over the coming days or weeks. Feedback from incident investigators could enhance cyber security as well as reduce incident response times.

Lastly, advanced digital forensics models should consider new trends in web technologies, such as mobile ad hoc networks and mobile phone applications (Shrivastava, 2018). One major development has been the adoption of semantic web practices (Shrivastava, Sharma, & Bawankan, 2012) for back-end communication (Praveen Kumar & Suguna, 2020) and front-end content generation (Shrivastava, Sharma, & Bawankan, 2012) as the range of e-commerce products and consumers becomes increasingly diverse. With the proliferation of semantic web practices in e-commerce, scholars have raised the need to enhance cyber security with semantic web services (Singh & Nayak, 2019). As digital forensics plays a key part in securing e-commerce, digital forensic models and tools must track such emerging technologies.

REFERENCES

Abschnitt, S. z. (2019). *DER.2.2 Vorsorge für die IT-Forensik*. Retrieved from https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_2_2_Vorsorge_f%C3%BCr_die_IT-Forensik.html

Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A new approach of digital forensic model for digital forensic investigation. *International Journal of Advanced Computer Science and Applications*, *2*(12), 175–178.

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security*, *5*(1), 118–131.

Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. *Journal of Management Information Systems*, *34*(4), 1082–1112. doi:10.1080/07421222.2017.1394063

Arewa, A. (2018). Borderless crimes and digital forensic: Nigerian perspectives. *Journal of Financial Crime*, *25*(2), 619–631. doi:10.1108/JFC-12-2016-0079

Ballou, S. (2010). *Electronic crime scene investigation: A guide for first responders*. Diane Publishing.

Barkatullah, A. H., & Djumadi, . (2018). Does self-regulation provide legal protection and security to e-commerce consumers? *Electronic Commerce Research and Applications*, *30*, 94–101. doi:10.1016/j.elerap.2018.05.008

Baryamureeba, V., & Tushabe, F. (2004). *The enhanced digital investigation process model.* Paper presented at the The Digital Forensic Research Conference DFRWS 2004, Baltimore, MD.

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, *2*(2), 147–167. doi:10.1016/j.diin.2005.04.002

Bera, A. (2019). *Cyber Attack Statistics*. Retrieved from https://safeatlast.co/blog/cyber-attack-statistics/

Brownlee, N., & Guttman, E. (1998). *Expectations for computer security incident response (2070-1721)*. Academic Press.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*(2), 1–20.

Chisholm, C. (2010). Integrating Forensic Investigation Methodology into Ediscovery. The SANS Institute.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1–147. doi:10.6028/NIST.SP.800-61r2

DFRWS. (2001). *A Road Map for Digital Forensic Research.* Paper presented at the Digital Forensic Research Conference, Utica, NY.

Frik, A., & Mittone, L. (2019). Factors Influencing the Perception of Website Privacy Trustworthiness and Users' Purchasing Intentions: The Behavioral Economics Perspective. *Journal of Theoretical and Applied Electronic Commerce Research*, *14*(3), 89–125. doi:10.4067/S0718-18762019000300107

Gantz, J., & Reinsel, D. (2012). The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east. *IDC iView: IDC Analyze the future, 2007*(2012), 1-16.

Hoffman, C. A. (2018). *Deeper Dive: Using Response Time Metrics to Drive Incident Response Preparedness & Response Improvement*. Retrieved from https://www.dataprivacymonitor.com/data-security-incident-response/using-response-time-metrics-to-drive-incident-response-preparedness-response-improvement/

Hutchings, A. (2012). Computer security threats faced by small businesses in Australia. *Trends and Issues in Crime and Criminal Justice*, (433), 1–8.

Ismail, N. (2018). *Cybercrime costs financial services sector more than any other industry, with breach rate tripling over past 5 years*. Retrieved from https://www.information-age.com/cybercrime-costs-financial-services-sector-123470776/

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. *Journal of Management Information Systems*, *34*(2), 369–400. doi:10.1080/07421222.2017.1334467

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, *10*(14), 800–886. doi:10.6028/NIST.SP.800-86

Khanuja, H. K., & Adane, D. (2019). To Monitor and Detect Suspicious Transactions in a Financial Transaction System Through Database Forensic Audit and Rule-Based Outlier Detection Model. In M. Rui Pedro, S. Carlos, & I. Helena (Eds.), *Organizational Auditing and Assurance in the Digital Age* (pp. 224–255). IGI Global. doi:10.4018/978-1-5225-7356-2.ch012

Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers & Security*, *38*, 103–115. doi:10.1016/j.cose.2013.05.001

Lau, L. (2018). *Cybercrime 'pandemic' may have cost the world $600 billion last year*. Retrieved from https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html

Lianos, I., Mantzari, D., Durán, G. M., Darr, A., & Raslan, A. (2019). *The Global Governance of Online Consumer Protection and E-commerce: Building Trust*. Academic Press.

MEDICI Team. (2015). *Everything you need to know about cross-border e-commerce*. Retrieved from https://gomedici.com/everything-you-need-to-know-about-cross-border-e-commerce/

Montasari, R. (2016a). An ad hoc detailed review of digital forensic investigation process models. *International Journal of Electronic Security and Digital Forensics*, *8*(3), 205–223. doi:10.1504/IJESDF.2016.077444

Montasari, R. (2016b). A comprehensive digital forensic investigation process model. *International Journal of Electronic Security and Digital Forensics*, *8*(4), 285–302. doi:10.1504/IJESDF.2016.079430

Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008). *Electronic Crime Scene Investigation: A Guide for First Responders* (2nd ed.). National Institute of Justice.

Novak, M., Grier, J., & Gonzales, D. (2018). New Approaches to Digital Evidence Acquisition and Analysis. *National Institute of Justice Journal*, *280*, 1–8.

OECD. (2016). *OECD Recommendation on Consumer Protection in E-commerce*. Retrieved from https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf

Park, S., Akatyev, N., Jang, Y., Hwang, J., Kim, D., Yu, W., Shin, H., Han, C., & Kim, J. (2018). A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. *Digital Investigation*, *24*, S93–S100. doi:10.1016/j.diin.2018.01.012

Pollitt, M. (1995, 1995). *Computer forensics: An approach to evidence in cyberspace.* Paper presented at the the National Information Systems Security Conference, Baltimore, MD.

Pollitt, M., Caloyannides, M., Novotny, J., & Shenoi, S. (2004). Digital forensics: Operational, legal and research issues. In *Data and Applications Security XVII* (pp. 393–403). Springer. doi:10.1007/1-4020-8070-0_28

Praveen Kumar, Y., & Suguna. (2020). *Review of Semantic Web Mining in Retail Management System Using Artificial Neural Network.* Paper presented at the Advances in Decision Sciences, Image Processing, Security and Computer Vision, Cham, Switzerland.

Rabeh, M., Islam, A., Samer, J., Adnan, K., & Mustafa, Z. Y. (2019). The Role of Information and Communications Technology (ICT) in Enhancing Service Sector Productivity in Palestine: An International Perspective. *Journal of Global Information Management*, *27*(1), 47–65. doi:10.4018/JGIM.2019010103

Reggiani, M. (2016). *A brief introduction to Forensic Readiness*. Retrieved from https://resources.infosecinstitute.com/a-brief-introduction-to-forensic-readiness/#gref

Reith, M., Carr, C., & Gunsch, G. H. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*(3), 1–12.

Ryan, D. J., & Shpantzer, G. (2002). *Legal aspects of digital forensics*. Academic Press.

Sanjeev, P., Sai Vijay, T., Chandan, P., Abhishek, B., Nikhil, S., & Subham, C. (2019). Clustering E-Shoppers on the Basis of Shopping Values and Web Characteristics. *Journal of Global Information Management*, *27*(2), 24–38. doi:10.4018/JGIM.2019040102

Shrivastava, G. (2016). *Network forensics: Methodical literature review.* Paper presented at the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom).

Shrivastava, G. (2017). Approaches of network forensic model for investigation. *International Journal of Forensic Engineering*, *3*(3), 195–215. doi:10.1504/IJFE.2017.082977

Shrivastava, G. (2018). Editorial: Investigating New Evolutions and Research in Digital Forensic & Optimization. *Recent Patents on Engineering*, *12*(1), 3–4. doi:10.2174/1872212112011803081131 30

Shrivastava, G., Kumar, P., Gupta, B. B., Bala, S., & Dey, N. (2018). *Handbook of Research on Network Forensics and Analysis Techniques*. IGI Global. doi:10.4018/978-1-5225-4100-4

Shrivastava, G., Sharma, K., & Bawankan, A. (2012). *A new framework semantic web technology based e-learning.* Paper presented at the 2012 11th International Conference on Environment and Electrical Engineering.

Shrivastava, G., Sharma, K., & Dwivedi, A. (2012). Forensic computing models: Technical overview. *CCSEA, SEA, CLOUD, DKMP*, *CS & IT*, *5*, 207–216.

Shrivastava, G., Sharma, K., Khari, M., & Zohora, S. E. (2018). Role of cyber security and cyber forensics in India. In *Handbook of Research on Network Forensics and Analysis Techniques* (pp. 143–161). IGI Global. doi:10.4018/978-1-5225-4100-4.ch009

Singh, N. K., & Nayak, S. K. (2019). The Threat Detection Framework for Securing Semantic Web Services. *Journal of Computational and Theoretical Nanoscience*, *16*(12), 5099–5104. doi:10.1166/jctn.2019.8569

Sung, T. K. (2006). E-commerce critical success factors: East vs. West. *Technological Forecasting and Social Change*, *73*(9), 1161–1177. doi:10.1016/j.techfore.2004.09.002

Sutton, S. G., Khazanchi, D., Hampton, C., & Arnold, V. (2008). Risk analysis in extended enterprise environments: Identification of critical risk factors in B2B E-Commerce relationships. *Journal of the Association for Information Systems*, *9*(3-4), 151–174. doi:10.17705/1jais.00155

Tan, J. (2001). *Forensic readiness*. Cambridge, MA: @stake, Inc.

Thoren-Peden, D., & Meyer, C. (2018). *Data Protection 2018*. Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. doi:10.1016/j.clsr.2017.05.015

Umar, R., Yudhana, A., & Faiz, M. N. (2018). Experimental Analysis of Web Browser Sessions using Live Forensics Method. *Iranian Journal of Electrical and Computer Engineering*, *8*(5), 2951–2958. doi:10.11591/ijece.v8i5.pp2951-2958

Van Baar, R. B., Van Beek, H. M. A., & van Eijk, E. J. (2014). Digital Forensics as a Service: A game changer. *Digital Investigation*, *11*, S54–S62. doi:10.1016/j.diin.2014.03.007

Winfred, Y., Daniel Okyere, W., & Peace, K. (2019). SETA and Security Behavior: Mediating Role of Employee Relations, Monitoring, and Accountability. *Journal of Global Information Management*, *27*(2), 102–121. doi:10.4018/JGIM.2019040106

Yen, P.-H., Yang, C.-H., & Ahn, T.-N. (2009). Design and implementation of a live-analysis digital forensic system. *Proceedings of the 2009 international Conference on Hybrid information Technology*. doi:10.1145/1644993.1645038

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. *International Journal of Computer Science and Information Technologies*, *3*(3), 17–31. doi:10.5121/ijcsit.2011.3302

ENDNOTE

[1] https://www.misp-project.org/index.html

Chia-Mei Chen has joined in the Department of Information Management, National Sun Yat-Sen University since 1996. She was Section Chef of Network Division and Deputy Director, Office of Library and Information Services in 2009-2011. She had served as a coordinator of TWCERT/CC (Taiwan Computer Emergency Response Team/ Coordination Center) during 1998 to 2013 and established TACERT (Taiwan Academic Network Computer Emergency Response Team) in 2009. She is a Deputy Chair of TWISC@NCKU, a branch of Taiwan Information Security Center. She continues working for the network security society. Her current research interests include anomaly detection, malware analysis, network security, and cloud computing.

Zheng-Xun Cai is a PhD student in Department of Information Management, National Sun Yat-Sen University. His research focuses on digital forensics, including network, process, registry and Windows event log.

Dan-Wei (Marian) Wen is an Associate Professor at Business College, Guinlin University of Electronic Technology. She received her Ph.D. in Business Administration from the Department of Business Administration, National Cheng-Kung University in Taiwan. Her research interests include industry dynamics, catching-up strategy, and data mining.