International Journal of Systems and Society
Volume 4 • Issue 2 • July-December 2017

A Socio-Technical Perspective on Threat Intelligence Informed Digital Forensic Readiness

Nikolaos Serketzis, Aristotle University of Thessaloniki, Thessaloniki, Greece
Vasilios Katos, Bournemouth University, Poole, UK
Christos Ilioudis, Alexander Technological Educational Institute of Thessaloniki, Thessaloniki, Greece
Dimitrios Baltatzis, International Hellenic University, Thessaloniki, Greece
George J Pangalos, Aristotle University of Thessaloniki, Thessaloniki, Greece

ABSTRACT

In this article, a DFR framework is proposed focusing on the prioritization, triaging and selection of Indicators of Compromise (IoC) to be used when investigating of security incidents. A core component of the framework is the contextualization of the IoCs to the underlying organization, which can be achieved with the use of clustering and classification algorithms and a local IoC database.

KEYWORDS

Advanced Persistent Threats, Digital Forensic Readiness, Indicators of Compromise, Intelligent Evidence Storage System, IOC, STIX, TAXII, Threat Intelligence

1. INTRODUCTION

Digital forensics dates over four decades. Unlike other forensic science disciplines, digital forensics faces the challenge to operate in a problem domain where the subject of study evolves in an intermittent, nonlinear fashion. For instance, a routine, nightly update of the software or introduction of new hardware may substantially change the behavior of the underlying system, requiring a significant revision of the digital forensics acquisition and analysis processes. Consider for example the case of evolution of traditional hard disks to solid state disk (SSD) technology. The way the latter operate invalidate many key assumptions under which forensic acquisition and investigation of disks is performed (Bednar & Katos, 2011).

Moreover, the proliferation of heterogeneous networked devices and the amount of data they are capable of producing – as captured under the terms IoT and Big Data respectively – has exacerbated the problems and challenges of digital forensics. As such, digital forensic readiness (DFR) has become a critical function of the organization's security processes and achieving efficient DFR has become a high priority. Research in digital forensics has primarily evolved through a responsive, practitioner-based attitude. The relevant literature on digital forensics is dominated by techniques and practical approaches for obtaining and analyzing data in specific contexts and system configurations. When it comes to considering DFR approaches, the level of abstraction is high causing a void and eventually a disjoint between DFR and digital forensic investigations. Most DFR research publications are limited to describing high-level and generic steps, whereas contextualization is mostly absent. This work aims

DOI: 10.4018/IJSS.2017070105

to bridge the gap by proposing a framework for a closer coupling between DFR, forensics and incident response for addressing Advanced Persistent Threats. We argue that inevitably, the prioritisation and contextualisation of the Indicators of Compromise is a sociotechnical challenge, since ultimately the forensic analyst needs to leverage automated tools to support their cyber situational awareness posture. That is, following a detection of a security breach, the threat related information needs to be quickly accessed, correlated and highlighted to allow the forensic analyst to triage, prioritise and guide their investigation in an effective manner.

The rest of the paper is structured as follows. Section 2 presents the relevant literature. In Section 3 our approach is developed. Section 4 outlines a typical APT scenario to be used as a vehicle to showcase our approach, and section 5 summarises the conclusions.

2. RELATED WORKS

In a seminal paper, Hutchins et al. (Hutchins, Cloppert, & Amin, 2011) proposed an approach for studying and improving incident response against APTs. They introduced a cyber kill chain which identifies a path comprised of 7 discrete and sequential phases an attacker follows to meet their adversarial goals. From a digital forensics perspective, the kill chain is particularly helpful in highlighting the following:

- Every successful (to the attacker) phase is a direct consequence of the respective security control failures.
- Detecting the security breach early in the chain infers low impact and potential damage.
- Late detection of the security breach implies that there are more security failures. Hence the scope of the digital forensic artifact collection is wider.

For the remainder of this section, the relevant subtopics that will enable the key chain to leverage the proposed DFR framework are presented.

2.1. Threat Intelligence

It can easily become apparent from the current literature that there is limited consensus on a definition of threat intelligence. Threat intelligence has been defined for example as a product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations (Sanders & Smith, 2014). It can be therefore considered that threat intelligence is the elaborate information about threats targeting one or more organizations.

Threat intelligence can be produced both from internal (e.g., Firewall, IDS) and external sources, such as public or commercial threat and vulnerability repositories. Externally obtained intelligence is sought as being particularly beneficial to the organization as this promotes cyber situational awareness, revealing thus the socio-technical aspects of the forensic investigation problem; an analyst will need the right technical tools to access the threat information in a timely manner, but will also need to coordinate with external to the organisation parties and peers in order to understand the subtle aspects of an APT.

Research on threat intelligence has highlighted the need for automated information exchange. To this extent, various standards and formats (openIoC, CybOX, STIX,) have been developed (MITRE, 2017a) (MITRE, 2017b) (Mandiant Corporation, 2013), with the most promising and publicly acceptable being CybOX, STIX and TAXII (Sauerwein, Sillaber, Mussmann, & Breu, 2017), (Fransen, Smulders, & Kerkdijk, 2015).

Cyber Observable eXpression (CybOX) is a standardized approach which leverages eXtensible Markup Language (XML) to encode and share information about observables in the operational cyber

domain. CybOX can be used to describe almost any type of information. Typical examples include IP addresses, domain names, filenames, file content and any sort of text pattern.

Structured Threat Information eXpression (STIX) is another structured language which is used to specify, capture, characterize and communicate standardized cyber threat information. STIX represents a holistic approach to format threat intelligence, by incorporating a broad set of information like Indicators, Incidents, Tactics, Techniques, and Procedures (TTP), Campaigns, Threat Actors, Exploit Targets, and Courses of Action (COA). As of version 3, CybOX has been integrated into the STIX schema (Barnum, 2014).

Trusted Automated Exchange of Intelligence Information (TAXII) in turn, is a mechanism that facilitates the exchange of cyber threat information. TAXII is optimized to ensure the smooth exchange of information represented in STIX (OASIS Technical Committee, 2017).

It becomes apparent that threat intelligence can assist in identifying an incident thus enhancing an organization's information security posture. On the other hand, absent or outdated information may considerably limit security personnel's awareness on a particular security incident. Should this be the case, performing a comprehensive digital forensics investigation exercise could shed light on the root-cause of the event.

2.2. Digital Forensics

Digital forensics (DF) history dates back approximately forty years, but notable maturity took place post-1997 (Garfinkel, 2010). DF encompasses a number of well-defined steps, with the aim to assist an investigator to identify the source and the root-cause of an event, thus answering six key questions; what, why, how, who, where and when (Ieong, 2006).

Despite the continuous maturity and evolution of DF, its effectiveness remains questionable, primarily due to the advances in IT industry (Garfinkel, 2010). More specifically:

- The proliferation of portable devices such as smartphones, tablets, smart TVs, etc., resulted in significant increase in the information produced and the diversity of operating systems and data.
- The volume of data that need to be examined has been increased, making the investigations lengthier in time and effort, and more expensive.
- The broad adoption of cloud services fosters the perception that new approaches to digital forensics investigations need to be evolved.
- The widespread use of encryption both in commercial and personal devices deter the extraction of forensic artifacts.
- The sophistication in malware development prevents the production of permanent forensic evidence, as many malware variations write temporary data only in RAM.
- The dissimilarity among national legal frameworks and the absence of a unified international legal framework renders cross-border investigations a challenging task.

Furthermore, Garfinkel (2010) noted the upcoming crisis in modern digital forensics by identifying some challenges in both the approaches of building the specialized tools but also the forensic analyst's practices. Perhaps the most relevant and important highlight in Garfinkel's paper is the evidence-oriented design of the digital forensic tools where the emphasis is placed on detecting possession of evidence rather than the actual crime being committed. This approach essentially invalidates the relevant tools from conducting computer focused crime investigations. Also, the silo and monolithic nature of digital forensic applications do not allow opportunities to integrate with digital forensic readiness processes.

2.3. Digital Forensic Readiness

Digital Forensic Readiness aims to maximize an organization's ability to collect credible evidence, whilst minimizing the cost of an investigation (Tan, 2001). To date, several approaches have been proposed.

Focusing on the policy dimension, Yasinsac and Manzano (Yasinsac & Manzano, 2001) stated that a set of policies like information retention, planning of response, training, investigation acceleration, prevention of anonymous activities and protection of evidence could facilitate the digital forensics process.

Rowlingson (Rowlingson, 2004) stressed out the need for the incorporation of forensic readiness to an enterprise's forensic program. Proactive evidence identification, collection, secure storage, and training are among the top priorities of their proposal.

Grobler and Louwrens (Grobler & Louwrens, 2007) underlined the overlap between information security and digital forensics and argued that digital forensic readiness must become a component of information security best practice. They also believe that the scope of DFR should be broadened to incorporate IS governance and augment the security program of the organization.

Pangalos and Katos (Pangalos & Katos, 2010) highlight that a relationship between Information Security and Digital Forensics exists. They affirm that residual risk is the main reason that drives the need for digital forensics and believe that a forensics-aware security strategy will manage to mitigate the impact of a security incident.

Valjarevic and Venter (Valjarevic & Venter, 2011) proposed a model that encompasses 10 phases including scenario definition, identification of possible sources, pre-incident collection, pre-incident analysis, incident detection, post-incident collection, post-incident analysis, definition of system architecture and assessment of implementation.

Approximately 15 years after Tan introduced the concept of forensic readiness (Tan, 2001), the emergence of ISO/IEC 27043 (International Organization for Standardization, 2015) indicates a significant level of maturity in this field. In essence, this standard developed with the aim to provide guidelines for incident investigation principles and processes, but it also acknowledges the importance of digital forensic readiness and welcomes it as a specialized class within the model.

3. THE PROPOSED DFR FRAMEWORK

As with most information security processes, DFR should be performed in a continuous and repeating fashion, rather than being a one-off process. Threat intelligence should be used to continuously inform and help prioritize the selection and collection of the necessary fields and features that would be used to support the digital forensic investigation in the event of a security incident. At this stage the distinction between a feature and an Indicator of Compromise, IoC, should be given:

Definition 1. A feature is an individual observable property capable of describing aspects of a state of a system.

Essentially a feature in this paper is meant to map to the concept of the feature as defined in the machine learning domain.

Definition 2. An Indicator of Compromise (IoC) is a specific instance or value of a particular feature.

From a machine learning perspective, an IoC can be seen as the labeling exercise, where specific tuples in a dataset are labeled. Labelling is needed in supervised or hybrid machine learning classification and clustering algorithms. For example, identified features may include IP addresses, port

numbers, file hashes, whereas an IoC would be the specific values, such as port:443, IP:61.12.13.14, hash:0x3e324ffd4e574639a0bc.

The proposed framework intends to provide a tool for prioritizing – aka triaging – and identifying the stage of an attack in the cyber kill chain (Figure 1). Reflecting upon the work by Hutchins et al. (2010) it is assumed that an APT type of attack would involve attack patterns and malicious campaigns that may manifest in one or more organizations. By continuously receiving information on IoC from external sources, the information provided by and to the DFR would support correlation activities to answer the questions of forensic interest. A high-level illustration of the framework is shown in Figure 2.

As shown in Figure 2, the digital forensics investigation is triggered at time t_d, at the first instance of detecting a security control failure and a successful compromise. On the general model, there is an amount of delay between the security incident leading to the system compromise and its detection. This delay depends on a number of factors and is outside the scope of this paper. However, what is of the primary interest and within the focus of the DFR is the efficiency by which the evidence is collected and prioritized. As such, efficient performance of forensic analysis would mean minimization of t_a-t_d, that is, a reduced depth of attack, disruption of the malicious campaign and improvement of the intrusion detection and intrusion prevention layers.

Another important aspect of the proposed approach is the continuous identification of the sources of IoCs. During an attack, not all information and IoCs will necessary be captured by the internal, in-house sensors, but some IOCs will be present in external repositories and sources. Consider for example shodan.io which captures and indexes the digital footprint of all contactable devices. During reconnaissance, an attacker may query the shodan servers to discover open ports for a specific IP

Figure 1. The cyber kill chain (adapted from Hutchins et al., 2010)

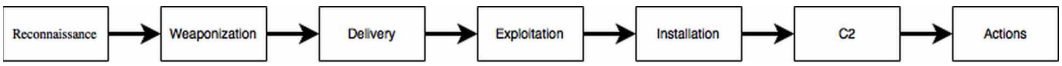
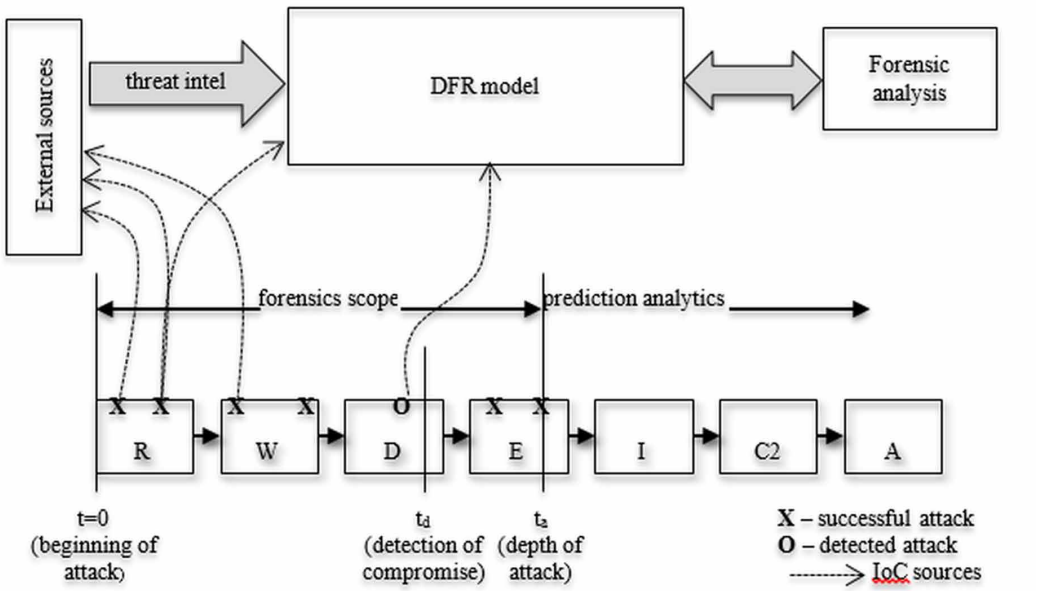


Figure 2. An integrated DFR framework



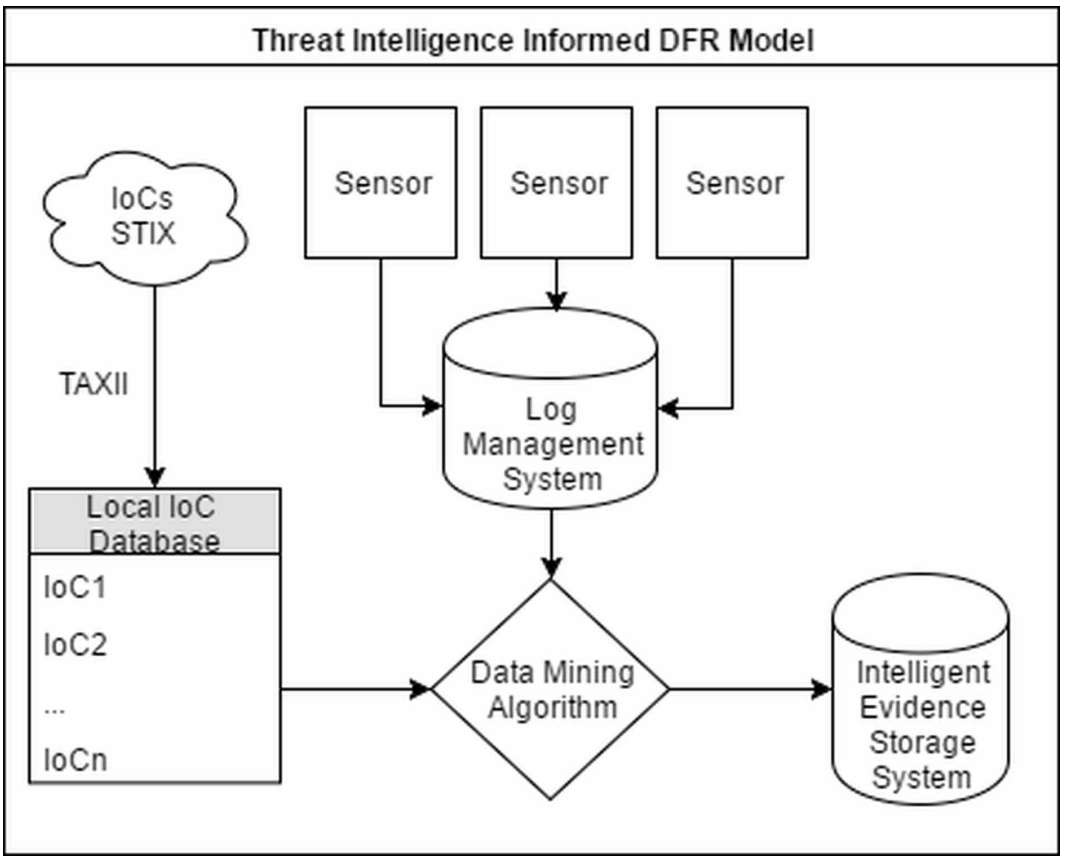
range or organizations. This would be equivalent to a port scanning attack, but without even touching the actual servers; the victim organization would be completely agnostic and oblivious of the port scanning activity since their logging servers would not log this. Therefore, for every attack (denoted as **X** or **O** in Figure 2) the corresponding IoC could be located internally, externally, or in both places. Consequently, the forensic analysis process should tap into a DFR framework capable of integrating with both external threat intelligence feeds (Open Source, OSINT) as well as with internal, Security Information and Event Management, SIEM components. These requirements essentially transform a DFR from a logging facility to a fully-blown process of clustering, classification of security incident features. This is shown in Figure 3.

More specifically, the proposed DFR methodology includes the following five steps:

3.1. Evidence Identification and Selection

Contemporary network equipment (routers, switches, etc.), security devices (Firewalls, IDSs, etc.), operating systems, and applications (web servers, mail servers, etc.) offer logging data alongside their primary operations. In a typical attack scenario, an adversary would attempt to discover the organizations' hardware and network assets, exploit their vulnerabilities, and try to install malicious applications to collect sensitive information or harm the systems themselves. In such a case, network sensors, operating systems or services themselves may collect useful data such as network connections, file changes, etc. The organizational security policies are expected to define what data should be logged. Typically, such a selection of the data is the result of a formal risk assessment procedure.

Figure 3. Threat intelligence informed DFR model



DFR, in turn, can be used as a means to ameliorate the collection process, that is to identify further possible cases that require credible evidence gathering. For instance, ISO/IEC 27043 incorporates the "scenario definition" process to describe how DFR assists in the identification of the evidence needed.

3.2. Evidence Collection

Different devices usually collect various types of data. The need to adequately store and exploit these pieces of data requires a suitable level of centrality and uniformity. The former can be achieved relatively easy, by the employment of a central Log Management System. Storing this data in a central log management system is considered a practical approach from management and security viewpoint (Elyas, Maynard, Ahmad, & Lonie, 2014). Secure logging protocols can also be engaged to enforce the integrity and accountability of the collected evidence (Accorsi, 2009).

On the other hand, the utilization of log parsers contributes to some extent, to the uniformity of the data captured. Unfortunately, it is not possible to achieve 100% homogeny in data, as they may describe various structures, like network traffic, connections, files, text, etc. Having that in mind, the authors acknowledge that the STIX language can be employed to describe the data structures of the proposed framework effectively.

Additionally, data storage mechanisms should be taken into consideration. While relational databases are considered stable and scalable solutions, the extensive employment of integrity procedures renders them inappropriate for managing log data. In contrast, NoSQL databases provide powerful query tools, but also demand hardware commitment, added programming, and administrative effort (Collins, 2014). It is thus evident that choosing the suitable log management system borrows from the "scenario definition" phase.

3.3. Creation of the Local IoC Database

As stated above, IoCs can be produced internally, as a result of an incident analysis, or externally by third-party information security firms or individuals. More accurate IoCs are commonly generated externally, as they may be the result of extensive investigatory procedures, like malware analysis.

The model that the authors propose is based on a separate, structured database containing only the appropriate IoCs. For efficiency and homogeneity reasons our proposed methodology uses the STIX language to describe the IoCs and TAXII to communicate them to the Local IoC Database.

For every IoC, their relevance to the organization's assets must also be considered before populating the Local IoC database. Thus, an initial IoC selection must be performed. This selection must take into account the results of the evidence identification phase. For example, it is worthless collecting IoCs that relate to operating systems an organization lacks. This contextualization process is a direct consequence of the threat intelligence and information sharing capabilities the DFR framework would possess.

Moreover, it is worth highlighting that all identifiable external IoCs will be subjects of the same risk assessment procedure applied for the Local IoC Database and subsequently decided whether it would be beneficial to include them.

3.4. The Data Mining Process

Information originating from the Log Management System and the Local IoC Database feed the Data Analysis System. Employing both unsupervised and supervised data mining algorithms, the Data Analysis System:

- first, identifies whether an incident has taken place and
- thereafter correlates the information pertaining to this incident.

The outputs and results of this process are then forwarded to the Intelligent Evidence Storage System.

Although the internal data mining aspects is beyond the scope of this paper an overview is presented. The records entering the Data Analysis System are classified according to their type and sensor location, thus producing clusters of similar information. Data classification algorithms are then applied to every cluster record to identify further whether it relates to a security incident.

Data classification algorithms partition data sets into predefined classes. Such categorization is based on group identifiers of these classes that are commonly known as "class labels" (Aggarwal, 2015). The proposed methodology employs indicators of compromise to define two class labels, "benign data" and "malicious data."

For example, if a record that comes into the Data Analysis System contains information relating to any IoC within the Local IoC Database, then this record is considered "malicious." Should this occur, that record is forwarded to the Intelligent Evidence Storage System, while a link analysis procedure initiates for the discovery and association with similar records.

3.5. The Intelligent Evidence Storage System

The Intelligent Evidence Storage System is the last component of the proposed methodology. It contains a central database that stores information about incidents and includes links to related records. In the event of a security incident, it is more practical and time efficient for investigators to search for evidence within the Intelligent Evidence Storage System, than checking the whole logging inventory.

4. PILOT IMPLEMENTATION: EXAMPLE APT SCENARIO

The following scenario which is used to demonstrate the advantages of the proposed DFR methodology is based on a real case attack which is part of a popular malicious campaign. An adversary group targets a company, aiming to exfiltrate confidential data. Employing the sophisticated type of watering-hole attack and social engineering techniques, the offenders exploited a zero-day web browser vulnerability and managed to install a custom-made malware on a PC which in turn initiated a tunnel connection to a command and control (C2) server listening on port 443. In this scenario, it is assumed that information security devices like firewalls, IDSs, etc. are updated to the most recent versions of signatures.

On a first decomposition of the incident, the authors note the following assumptions and observations. One of the employees visited a regular web page, but this web page has previously been tampered with a browser exploit. The network devices log the connections to the web page. The browser also holds web history. The exploitation of the web browser allowed the installation and execution of the malware on the PC, and thus, the alteration of file system's and registry's records. The antivirus database does not contain the hash signature of the malware executable, so no alarm is raised. The destination IP address where the C2 server resides does not belong to any list of blocked IP addresses while port 443 maps to https protocol, thus TCP connections to this IP address are permitted but logged as well.

A week later a private information security firm informs the company that its confidential records have been published on the internet. This firm has also identified that a new malware distribution campaign exists. So, it analyzed its characteristics and published the relevant indicators.

Following the traditional approach, should the company need to determine how the adversaries compromised its systems, a full forensic investigation is required. In particular, all log files produced by the network devices, along with terminal equipment must be examined thoroughly. It is interesting to note that, following this approach, the investigator has no a priori knowledge of the way the incident took place. Thus more time is needed to identify the indicators of compromise.

As stated above, our methodology employs IoCs. In a similar approach, the authors consider that the security firm has already created and communicated these IoCs. The proposed method checks

whether the audit logs that fit within the logging repository cross-match and further correlate with the relevant IoCs. Then, the results of this algorithm become the contents of the Intelligent Evidence Storage System. In essence, a graph database is the basis of that system which contains records of IoCs and audit logs, as well as links describing the relationship among them. Records and IoCs, are expressed as graphs, while the relationship between them as edges.

Following this approach, the correlated records within the Intelligent Evidence Storage System can assist the investigator or the analyst to identify possible reasons or sources of a compromise, narrowing the time frame she needs for performing a full forensic investigation. Recalling that time often designates cost (Reddy, Venter, & Olivier, 2012), the proposed methodology can enhance digital forensic readiness.

Initial results from the application of the proposed methodology on the above example APT scenario have produced encouraging results. More detailed experimentation is currently on the way, and it is expected that it will also confirm the correctness of our approach.

CONCLUSION

The volume, variety, and velocity of data produced by contemporary networked devices challenge the efficiency of traditional digital forensics approaches. While DFR attempts to optimize the collection of credible evidence in order to support cost-effective investigations, most of the research is limited to describing high-level and generic steps, whereas contextualization is mostly absent. In addition, the authors argue that a large volume of collected evidence may reach a point that would undermine the cost effectiveness and as such the authors recognize the need to employ Indicators of Compromise and Machine Learning techniques to produce subsets of usable data that can facilitate the investigative process should a security incident occurs. The proposed approach aims to automate only the analysis aspects that will not jeopardise the contextualisation and situational awareness capabilities of the forensic investigator, but in fact would assist them in developing an understanding of a manifestation of an APT.

REFERENCES

Accorsi, R. (2009). Safe-Keeping Digital Evidence with Secure Logging Protocols: State of the Art and Challenges. In *Proceedings of the 2009 Fifth International Conference on IT Security Incident Management and IT Forensics* (pp. 94–110). doi:10.1109/IMF.2009.18

Aggarwal, C. C. (2015). *Data Mining: The Text Book*. Springer International Publishing. doi:10.1007/978-3-319-14142-8

Barnum, S. (2014). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). MITRE Corporation.

Bednar, P., & Katos, V. (2011). SSD: New Challenges for Digital Forensics. In *Proceedings of the 8th Conference of the Italian Chapter of the Association for Information Systems* ItAIS 2011.

Collins, M. (2014). Network Security Through Data Analysis. O'Reilly Media, Inc.

Elyas, M., Maynard, S. B., Ahmad, A., & Lonie, A. (2014). Towards A Systemic Framework for Digital Forensic Readiness. *Journal of Computer Information Systems*, *54*(3), 97–105. doi:10.1080/08874417.2014.11645708

Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *Elektrotechnik & Informationstechnik*, *18*(2), 106–112. doi:10.1007/s00502-015-0289-2

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*, S64–S73. doi:10.1016/j.diin.2010.05.009

Grobler, C. P., & Louwrens, C. P. (2007). Digital forensic readiness as a component of information security best practice. *IFIP International Federation for Information Processing*, *232*, 13–24.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. In *Proceedings of the 6th Annual International Conference on Information Warfare and Security* (pp. 113–126).

Ieong, R. S. C. (2006). FORZA - Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, *3*, 29–36. doi:10.1016/j.diin.2006.06.004

International Organization for Standardization. (2015). *ISO/IEC 27043:2015. Information technology, Security techniques, Incident investigation principles and processes*.

Mandiant Corporation. (2013). OpenIOC. Retrieved from http://www.openioc.org

MITRE. (2017a). Cyber Observable eXpression (CybOX). Retrieved March 24, 2017, from https://cybox.mitre.org/about/

MITRE. (2017b). STIX: A structured language for cyber threat intelligence. Retrieved March 5, 2017, from https://oasis-open.github.io/cti-documentation/

OASIS Technical Committee. (2017). Cyber Threat Intelligence Documentation. Retrieved March 24, 2017, from https://oasis-open.github.io/cti-documentation/

Pangalos, G., & Katos, V. (2010). Information Assurance and Forensic Readiness. In Next Generation Society. Technological and Legal (pp. 181–188). doi:10.1007/978-3-642-11631-5_17

Reddy, K., Venter, H. S., & Olivier, M. S. (2012). Using time-driven activity-based costing to manage digital forensic readiness in large organisations. *Information Systems Frontiers*, *14*(5), 1061–1077. doi:10.1007/s10796-011-9333-x

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence*, *2*, 1–28.

Sanders, C., & Smith, J. (2014). *Applied Network Security Monitoring* (D. J. Bianco, Ed.). Elsevier Inc.

Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). Threat Intelligence Sharing Platforms : An Exploratory Study of Software Vendors and Research Perspectives (pp. 837–851).

Tan, J. (2001). Forensic Readiness. Cambridge, MA 02139 USA.

Valjarevic, A., & Venter, H. S. (2011). Towards a Digital Forensic Readiness Framework for Public Key Infrastructure systems. In *2011 Information Security for South Africa*.

Yasinsac, A., & Manzano, Y. (2001). Policies to Enhance Computer and Network Forensics. In *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security* (pp. 5–6). West Point, NY: United States Military Academy.

Nikolaos Serketzis has served as a cyber crime investigator at Cybercrime Division of Hellenic Police for more than ten years. Following his police studies, he obtained his BSc Degree in Computer Science from the Alexander Technological Educational Institute of Thessaloniki in 2007 and an MSc degree in forensic computing and cyber crime investigation from the University College of Dublin in 2009. Now, he is a PhD candidate at the Aristotle University of Thessaloniki, and his research interests focus in the fields of information security and digital forensics. He also holds several professional certifications in the fields mentioned above.

Vasilis Katos obtained a Diploma in Electrical Engineering from Democritus University of Thrace in Greece, an MBA from Keele University in the UK and a PhD in Computer Science (network security and cryptography) from Aston University. He is a certified Computer Hacking Forensic Investigator (CHFI). He has worked in the Industry as Information Security Consultant and served as an expert witness in Information Security for a criminal court in the UK and a misdemeanor court in Greece. His research falls in the area of digital forensics and incident response. He has participated in 2 FP7 and 3 nationally funded research projects and in a number of national and international cyberdefence exercises. He has over 80 publications in journals, book chapters and conference proceedings and serves as a referee on several reputable conferences and journals (for example, IEEE Communications Letters, Computers & Security, Information and Computer Security), and has coordinated and delivered a number of workshops, both in an academic and a security professionals context. He is member of the editorial board of Computers & Security. In terms of recognition of his research, he has received keynote speech invitations for international conferences (indicatively, the 8th European Conference on Information Warfare and Security) and his research has been addressed by reputable magazines such as the New Scientist.

Christos Ilioudis obtained his BSc degree in Computer Science from the University of Crete, Greece and his PhD on Internet security from the Aristotle University of Thessaloniki, Greece in 2002. Since 2007, he has served as Professor of Informatics Department, Alexander TEI Thessaloniki, – Greece. He has taught information systems security and Internet technology and services in the ATEI of Thessaloniki. His research interests include the areas of Internet technology and security, information systems security, and e-health. He has been working on several EU research projects on security area, e.g. e-SENS, BIOIDENTITY, HUMABIO, NETCARDS, OPUS, etc. He has been author of a variety of research articles in international journals and conferences.

Dimitrios Baltatzis received a BSc degree in mathematics from the Aristotle University of Thessaloniki, an MSc in Computer Science from the University of Gothenburg Sweden and a PhD degree in computer science from the Aristotle University of Thessaloniki (Faculty of Technology). Since 2017 he servers as teaching stuff at the International Hellenic University, Thessaloniki Greece and at the previous years, he has been teaching various courses at the Faculty of Technology of the Aristotle University of Thessaloniki, Greece and the International Hellenic University in Thessaloniki Greece. He has also taught in several universities in Greece. His research interests include the areas of Cybersecurity, Intrusion Detection, Information System security, Database systems Security and Access control. He has published several articles in international scientific journals and conference proceedings.

George J. Pangalos received a BSc degree in mathematics from the University of Athens and an MSc and a PhD degree in computer science from the University of London (University College London, UK). Since 1990, he has been with the Faculty of Technology of the Aristotle University of Thessaloniki, Greece, where he is currently a professor in the Department of Electrical and Computer Engineering (ECE) and also the director of the Informatics and Information Security laboratory of the same faculty. He has also taught in several universities in Greece and the USA. His research interests include the areas of Information Systems Design, Information System security, Health Information Systems, Database systems Security, Access control, e-Identification and e-Authentication, IT Forensics and IT security audit, Internet security and secure internet transactions, e-Health and applications, and e-Gov Applications. He has published over 200 articles in international scientific journals and conference proceedings. He has also been the author or co-author in several (more than 20) International and Greek books. He has also been involved as project leader / expert in a significant number (more than 50) major international (mostly EU funded) research and development projects in the above areas. He has also participated as an expert evaluator, after an invitation from the EU, in the selection and the assessment of several (more than 20) EU projects and studies and the formulation of EU framework research programs (FP). He has also been for several years (2004-12) the National Representative of Greece to the European Union's Security Research Program. He has been president and member of the board in several national and international scientific and professional bodies (President of the Greek Computer Society (NG), President of the Education and Research section of GCS, President and Member of the Board of the (Brussels based) European Informatics Association CECUA, Representative of Greece to the International Medical Informatics Association, Vice-President of the Greek Medical Informatics Association, etc.). He has also been director/CEO of several IT related organizations and departments (President of the Greek Centre for e-Government Applications in Social Security and Health (IDIKA), President and CEO of the Regional Health System (PESY) of Thessaly, Director of the Informatics Institute and of the under and post graduate IT schools of the Greek Productivity Centre, Member of the AUTH research management committee, Co-founder and Director of the IT Support centre of AUTH (1991-01), etc.).