Digital Forensics in Cyber Security Exercises

Livia ROȘU and Georgiana SUBAȘU

***Abstract*—The increased exposure to cyber threats is determined by the use of digital systems and their highly available connectivity. In order to mitigate cyber risks, optimum solutions are sought regarding the development of various methods for training in cyber security. Cyber training exercises have been created from the need to improve knowledge and skills, currently providing an enhancement to the detection and response capability to security incidents.**

One area in which cyber training exercises bring a major benefit is digital forensics. This paper aims to review the required criteria for building cyber exercises for training in the digital forensics field. It also emphasizes the importance of these training exercises in acquiring and improving the necessary skills for a promptly and efficiently response to security incidents. Our paper focuses on the benefits of using digital forensics methods and techniques to extract the information needed for monitoring and scoring participants' activities.

***Index Terms*—Cyber Exercises, Cyber Security, Digital Forensics, Monitoring, Training.**

I. Introduction

Cyber security is a very much discussed field today due to the new types of threats and attacks and the complex methods of preventing and combating them. New security incidents bring with them the need of having a higher level of education in this area. Increasingly complex attacks require organizations to pay special attention to employees preparedness to handle these situations. Besides existing commercial solutions available, organizations want their experts to be able to prevent and respond in case of a security incident in a short time.

The pillar in response to cyber security incidents is the digital forensics domain. The initiation in this field of the unspecialized employees, but also the continuous training of those that are already specialized are the main concerns of the organizations regarding this field.

The most common method of training in digital forensics is cyber security exercises. These enables both theoretical and practical levels of training, providing a safe, isolated environment to participants in which they can acquire new abilities, apply their knowledge, or test their skills in collection and analyzing digital data and even responding to simulated security incidents.

A challenge, in terms of cyber security exercises, is their design and construction. The training through customized exercises according to the needs of each entity and situation is more and more desirable to the detriment of commercial solutions. Besides the special technical requirements imposed by every training participants in the exercise, the monitoring of the activities is the most important element for a rigorous validation of the participants knowledge and actions.

Therefore, the digital forensics domain has two major roles in cyber security exercises: digital forensics as a training exercise and the monitoring responsibility in order to score the activities of participants.

In recent years, industry research has focused on creating cyber training exercises in digital forensics area. This can be a way of initiating and training those who want to develop and implement their own cyber exercises.

In the paper [1], the authors describe the development of a smaller scale competition where the participants can learn ethical hacking using an isolated environment in which they can train and test both attacker or defender abilities. The competition provides the possibility to measure performance automatically.

When designing this type of exercise, it is important to establish its construction stages [2], as well as the objectives, depending on the abilities and capabilities that participants have to acquire [3].

Starting from simple training exercises, complex cost-effective approaches have been achieved using virtual environments. Recent research [4] suggests a life cycle of the cyber training exercises as a methodology to account for their deployment and development.

Evaluating the performance of the participants is the main purpose of cyber training exercises. It is desired to differentiate a beginner from an advanced one. This involves collecting data about the human-machine transactions or evaluations based on questionnaires [5]. In the evaluation phase, the time for score the actions is the most important, so the possibility of doing this automatically takes the lead [6].

Cyber security exercises not only increase the capabilities of a future specialist in a certain field, such as digital forensics, but also develop cyber hygiene, a pool of skills that any user needs to have in order to be able to prevent possible security incidents. Fulfilling the goals of training exercises involves the existence of well-trained mentors [7]. They are responsible for the monitoring of the participants actions in an effective way. Therefore, a trained user can easily become a mentor or can be part of the monitoring team after they have gained enough experience.

Cyber exercises based on virtual infrastructure have gained a high reputation from the need to carry out training at lower costs [8].

Due to integration of virtualization technologies in cyber training exercises, monitoring becomes an accessible task. This can be done with the help of virtual machine analysis techniques [9], but also through customized methods such as log analysis [10].

L. Roșu is with the Doctoral School for Defense and Security Systems Engineering, Military Technical Academy, 39-49 George Coșbuc Ave., Sector 5, 050141, Bucharest, Romania (e-mail: livia.rosu@mta.ro).

G. Subașu is with the Doctoral School for Defense and Security Systems Engineering, Military Technical Academy, 39-49 George Coșbuc Ave., Sector 5, 050141, Bucharest, Romania (e-mail: georgiana.subasu@mta.ro).

Digital Object Identifier 10.32754/JMT.2018.1.02

II. Digital Forensics in Cyber Security Context

Digital forensics is the branch of forensics science dealing with the investigation and analysis of artifacts that are extracted from electronic evidences, collected from the computer's memory, storage devices, mobile devices, packets transmitted over a network, etc.

Depending on the source of the electronic evidence, the domain can be divided into:

- Computer forensics - deals with the investigation of volatile or non-volatile data collected from a computer, so analysis methods are shared in the following two:
  - Static/post-mortem forensics - investigating evidence collected after the incident, when the computer is turned off;
  - Live/dynamic forensics - investigating the evidence collected during the runtime computer, aiming volatile memory;
- Network forensics - involves collecting and investigating data from the network;
- Cloud forensics - represents the application of forensics science in cloud computing. It can be said that cloud forensics combine cloud computing with network forensics because it is necessary to analyze data from network, storage media and virtualization systems [11];
- Mobile forensics - deals with investigating evidence collected from mobile phones;
- Database forensics - investigates evidence collected from databases and their related metadata.

Due to the sensitivity of the taken actions in the field of digital forensics, specialists have expressed the need for well-established stages to be followed in an investigative process.

In the paper [12], a study was conducted on the common phases of the procedures adopted in the field. The authors proposed a five-stage model. Regardless of the number of stages and their division, it is important to keep the integrity of the evidence.

An important aspect of the methodology used in the investigation of electronic evidence is that at any time or stage it must be possible to consult laws, procedures, principles, requirements or standards related to the field.

A preliminary step to the investigation is the preparation of the analysis environment or laboratory environment specially designed for the investigative process, the tools used for the acquisition and analysis and the necessary documents.

The first stage of the technical investigation process is to identify the incident. Also, at this stage, an incident response is attempted if there is a human resource trained for these situations.

Following the response to the incident, the investigation continues with the acquisition of volatile and non-volatile data for a future detailed analysis in the specialized environment. Before the actual analysis, the evidence can be duplicated and then examined to extract the information of interest for the analysis phase. This phase is the most complex of the investigation process.

After the attempt to respond to the incident and analysis of collected data, the information obtained can be correlated and the chain of events can be reconstructed in order to establish the conclusion of the case and the measures to be taken to prevent the same type of incident.

In terms of technical investigation, it is necessary to have an analysis environment that respects the uniqueness of each evidence, the legal regulations in the field, analysis procedures and their chronology and with high flexibility. Flexibility can be given by many tools, free or commercial, depending on the needs and financial resources available. Due to reduced costs and the possibility of customization, virtual environments are often used. This requires a good understanding of the implications of using virtualization in such situations.

Virtualization makes possible the analysis by multiple users in the same time, in an isolated environment, using a single virtual machine by each specialist or a virtual private network.

A disadvantage of using virtualization can be the need for large storage space. This problem has been eliminated by creating automated analysis systems that allow the examination of different types of evidence in a very short time with minimal resources without requiring from user advanced and specialized knowledge in the field. However, with the evolution of cyber attacks, there has also been a need for an advanced analysis that can complement or be correlated with the results of automated analysis. This requires a high level of knowledge in the field.

In support of those that are newly initiated in the field, cyber security exercises have been created and developed as a form of training in an appropriate environment. Cyber training exercises can be organized in the form of a competition, cyber training exercises to improve security and defense or proactive security exercises.

III. Training in Digital Forensics by Cyber Security Exercises

Due to the increasing use of electronic systems that can have vulnerabilities potentially exploited by attackers, users need cyber security training from entry level to advanced, both theoretical and practical knowledge required by the current cybernetic context. This can be done with the help of cyber security exercises.

It is possible to train theoretically through table-top exercises that involve discussions aimed to establishing the level of security and mitigating the risk of becoming a victim of a cyber attack.

Improving the defense plan, becoming aware of the impact of a cyber attack or knowing different ways to detect and respond to security incidents are skills that can be gained through practical hands-on exercises that can address multiple scenarios, mapped on the activity of participants, based on realistic simulation of cyber security incidents.

A cyber security exercise involves defining and assigning responsibilities for teams, with different roles, that are participating at training: the control team (green team); defenders (blue team); attackers (red team); and the monitoring team (white team) [13].

- *Green Team* - coordinate and lead the implementation of the exercise and is responsible for its overall effectiveness. It initiates scenario events in a way that allows testing the students, monitoring the results, and extracting information about what works and what does not;

- *Red team* - simulates similar events to cyber attacks and delivers them to the blue team;
- *Blue Team* - is the team that will participate at all challenges included in the exercise scenario being trained and evaluated depending their actions;
- *White Team* - helps the green team and is responsible for monitoring the actions taken by the red and blue teams, documenting the results and providing feedback on these activities to the green team. The most important responsibility is to monitor the success or failure of the blue team in managing incidents and reacting against cyber attack scenarios.

Several approaches to cyber security exercises are available, but the jeopardy-style is the most complex type because it can train both the blue team and the red team through specific defensive or offensive challenges, with increasing difficulty tasks, both theoretical and practical.

The areas included in jeopardy-style exercises are diverse:

- digital forensics;
- networking;
- cryptography;
- web applications;
- mobile security;
- steganography;
- reverse engineering.

Designing a Cyber Security Exercise is based on certain aspects such as the goals of the exercise, the levels of difficulty, the domains and subdomains from which the tasks originate, what skills they want to be developed, the infrastructure and the available tools.

Therefore, the digital forensics field can be included in cyber training exercises through the defensive actions performed by the *blue team*, but also in the monitoring or evaluation process and activities dissemination - *white team*.

In paper [2], the authors have proposed a series of seven phases of construction of a cyber security exercise. We will further detail them in a direct relationship with the construction of a digital forensics exercise.

Establishing the objectives of the exercise. This phase defines the direction in which the exercise will go. The purpose of a digital forensics exercise is, in most cases, to apply and understand a particular or a set of more techniques used in the field, in order to be properly combined in complex process of responding to cyber security incidents. Establishment of objectives is done taking into account the desired level of difficulty.

Exercise approach. In the digital forensics domain, the approach will always be mixed, both defensive and offensive. For training in this field, the jeopardy-style exercise is used, in which the participant can learn how to collect data, recover files, discover, extract and analyze artifacts. These exercises can also be approached from the perspective of the attacker, being a way to understand his thinking by participating in various specific challenges: obtaining victim data, discovering security breaches, gaps and vulnerabilities, infecting the target, maintaining access to the system, etc. A method of practicing techniques and tools in digital forensics is the participation in cyber security competitions, the most current and encountered approach of training exercises.

Topology of the exercise. At this stage, the available infrastructure is very important. If the dificulty level of the exercise is low, a participant can use a single system, but for greater complexity, it can use a network, especially if the exercise also includes network forensics tasks. To all this is added the necessary systems for the green and white teams. The red team can be simulated using scripts.

Creating the scenario. At this stage, it determines how the evidence for the investigation will be obtained, the types of data analyzed, how they will be analyzed, the techniques and tools that the participants will use and how the whole scenario is gradually divided.

Establishing the set of rules. Rules are set regarding the general course of the exercise, how the participants will get or lose points, what are the accepted approaches, what limitations they have, and the legal regulations that they will be considering.

Choosing metrics. All the actions taken will be appreciated as good or worse depending on the execution time, the number of strings observed, the number of string searches, the number of attempts of some commands. The staff responsible for the quantification of the results will evaluate if the command parameters were entered correctly from first try, if they used the well-known help function, if they have been able to correlate information for an advanced search, but also how many and what tools they used to do all of the above.

Lessons Learned. At the end of the exercise it is recommended to draw up a document with all the observations during and after the exercise, what problems have been encountered, what is the feedback of the participants, the scores, the most used instruments, and the correlation of those.

Cyber training exercises in the digital forensics field can include tasks from several branches of it, separated or interconnected. The scenario can include exercises that involve obtaining and analyzing data from the hard drive, removable storage devices or RAM memory of a system. They can also be combined with network forensics tasks, because often these two subdomains complement each other.

The new types of malware use methods of hiding or securing the code by obfuscation or cryptographic algorithms; therefore, exercises that require discovery of packings and unpacking of data, as well as password cracking, are also very useful.

Another approach to these exercises can be the one in which a participant trains to handle the anti-forensics techniques such as steganography. This is the science of hiding data in other types of data. Also, obfuscation of the code is an anti-forensics technique. The scenario may include discovering hidden text in an image. Combining steganography with cryptography can be a real challenge for participants with a higher level of knowledge, this technique being included in advanced exercises, for professionals [14].

Because of the growing use of mobile phones, attacks on them are more common, and training in mobile forensics is required even for a simple user.

An advanced approach to cyber attacks is through malware, and these are increasingly complex, requiring training in reverse engineering and advanced debugging and disassembly techniques.

Among digital forensics techniques that can be learned and practiced in training exercises are included:

- *Using antivirus software* - a file is given and scanned to determine if it is infected. This is the first and most simple technique used by specialists.

- *Hash values*. Calculate the values of cryptographic hash functions to look for them in well-known data sharing databases about malicious files. The most used cryptographic hash function is md5.
- *Packers*. Attackers often use packers to hide data, so it is useful to check if the file extension has been modified [15].
- *Portable Executable files*. Sometimes analyzing different file formats can provide important information. For example, the Portable Executable file format is used by Windows executables, DDLs, etc. Analyzing these files can reveal which features have been imported, exported, dependences on other functions for correct and complete run. Also, in the header of this file type there are important data, such as the necessary resources for execution [16].
- *Strings*. One of the simplest and most useful techniques is to search for strings such as function names, registry keys, unique names, IPs, URLs, software names, etc.

Also, cookies analysis is useful, recovering deleted files, analysis of temporary files, print spool files, and reviewing unallocated space. If the exercises include network forensics, the packets are also analyzed [17].

If it is possible to run the sample, important data can be found from volatile memory areas available only when the system is running [15]:

- Process monitoring can provide information such as running time, running security, the modules that the process has loaded, the process memory content, the path to the executable file;
- Windows Registry Analysis - for example, you can see the changes made to some registry values;
- Analysis of the called functions and their parameters to determine the behavior of a program;
- Analysis of DDLs as they can contain code and resources that can be shared between multiple processes;
- Monitor system calls;
- Search for rootkits with specialized tools.

Cyber exercises for training in digital forensics should be designed so that participants would have the posibility to train gradually, with simple exercises with a single technique to apply and few tools to use, to very complex exercises with combined tasks from different subdomains of digital forensics, with multiple approaches and numerous ways of solving, also taking into account the decisions taken during the solving of the given situation.

The goal of all exercises should be to acquire the ability to apply and combine the learned techniques in a realistic situation such as the response to incidents, according to the findings made during the investigation, without having the hints as it is possible to receive during the exercises.

In paper [3], the authors conducted a study that outlined the main features needed for an entry-level course in digital forensics by questioning more people. The conclusion was that the preferred approach is practical exercise, replacing presentations with live demonstrations and extending hands-on exercises. Also, this paper refers to Bloom's Taxonomy [18], a defined model of learning objectives which includes the cognitive categories of knowledge, comprehension, application, analysis, synthesis, and evaluation. Each word corresponds to a verb that describes exactly the action needed to accomplish each goal:

- *Recognize* a specific string among lots of characters (Knowledge).
- *Describe* what is the functionality of a tool (Comprehension).
- *Mount* an image of a hard disk with an appropriate tool (Application).
- *Determine* the types of artifacts found (Analysis).
- *Explain* the code of a malware (Synthesis).
- *Assess* which tool should be used for the specific artifacts (Evaluation).

Starting from the previously exemplified learning objectives, we can build cyber exercises with diverse scenarios, combining the branches of digital forensics in a more constructive way for participants, giving them the opportunity to learn, test and practice numerous techniques.

A cyber exercise for training in digital forensics provides the most appropriate solution for testing skills and capabilities, responsiveness in limited situations as well as the level of team cohesion. To quantify the effectiveness and the benefits of a training exercise requires the measurement of the outcomes.

The organizers' challenge, more than the design and implementation of an incident scenario list, is the way to evaluate and generate an automatically score for those participants who follow the activities proposed to achieve the objectives of the exercise.

IV. Monitoring Participants Activities through Digital Forensics Technicques

Digital forensics techniques can be used for enhancing the evaluation methods and procedures in order to extract and achieve Lessons Learned.

For any type of training exercises, it is imperative to have an effective, preferably automatic monitoring of the participants actions in order to quantify them for the scoring stage. The specialists involved in the scoring process, the white team, are responsible for monitoring the participants' activities, in an efficient and rigorous way, by setting the criteria for obtaining or losing points. These are selected in the phase of choosing the metrics that will be used in the exercise. Certain specific criteria that can be considered as a metric in a training exercise:

- the time to discover a flag and use it to respond to the next challenge;
- the parameters of using a tool in relation to the time required to meet the goals;
- the unlocking of some services with a flag. The time used to unlock a service also includes the time used to find the flag. A service can be tested at any time during an exercise, the action being scored if the service is working correctly at the time of the evaluation;
- the commands introduced or the number of commands entered to block / unblock a service;
- the number of flags discovered can be a measurement criterion because the exercises can have several challanges and the successful completion of one of these leads to the acquisition of a flag. Some exercises are on the principle "all-or-nothing", meaning that only by discovering the final flag, all the available points can be accumulated;
- the use of some tools can lead to a decrease in score. A specific list of tools can be prohibited and the

automated ones may be in that list because the participants' effort would be minimal;
- the use of the Internet is possible but with a certain limit. This could make the difference between a participant with a level of knowledge already acquired and a beginner, because the beginner can search for basic information such as the functionality of certain tools or file types;
- the moment of logging on a server;
- the owning of some files. An important rule in the digital forensics domain is to maintain the integrity of the data. It can be required to make a copy of the data and the assessment criterion can be the existence of the copy, in the indicated place and the time of creation.
- building of reports that highlight the activity of the participants, applying the same evaluation metrics as in the case of owning files;
- the number of recovered files;
- checking the installed tools and choosing the correct ones, according to the desired category, in order to create the analysis environment.

All of this information can be obtained by digital forensics specialists, from the white team, addressing different methods. Monitoring procedure generally depends on the infrastructure that is used to build the cyber training exercise.

The most common approaches for building the infrastructure of a cyber security exercise are those in which some components are virtualized. In small-scale exercises, all components can be physical systems to enhance scenario realism, or another option can be a hybrid infrastructure that combines virtual machines with real physical systems.

With the existing tools and techniques, regardless the type of architecture, specialists can perform an effective assessment of the activities undertaken during the exercises.

The current trend in building cyber exercises for training is the virtualization technology because they require minimal resources, facilitate simultaneous simulations, quick reconfiguration and efficient management. Virtualization fulfills all the optimal conditions required for a digital data analysis environment, being a recommended solution for cyber training exercises.

An ideal training environment can determine the level of participants' skills before an exercise through the placement tests or by monitoring the activities performed during the exercise.

Virtualization technology comes to support the monitoring and evaluation of participants by offering the possibility of taking snapshots, preserving copies of virtual machines from several phases during the exercise. Manual analysis of a virtual machine is time consuming even if there are many specialized tools to do that. A quick approach needed to monitor an exercise is possible, thanks to a technique introduced in the work [9], Virtual Machine Introspection (VMI), which is widely used by digital data analysis specialists. The VMI allows extraction of information both inside and outside the virtual machine, without manual examination.

Due to the customizable character of the exercises, digital forensics specialists felt the need to create their own monitoring methods such as automated log centralization and analysis. In some solutions specialized tools have been used to collect data about human-machine transactions. The paper [10] propose a way to automatically analyze logs collected by using the Tracer FIRE platform. This platform was developed to measure the performance of the participants according to their interaction with the available machine.

Automatically extraction of information of interest, using scripts, from reports sent by participants, can be another way of tracking their activity.

The virtualization technology is widely used and present common aspects with cloud computing because the commercial solutions that provide cloud services can also be used as a training environment for cyber security exercises [19].

Therefore, monitoring solutions can be found in cloud forensics techniques. They can be divided into client forensics, cloud (server) forensics and network forensics. The most appropriate techniques for monitoring participants' activities are the specific client forensics techniques [11].

The newer infrastructure-building technologies, such as containers, represent a real challenge for the digital data analysis specialists in terms of organizing and setting up an exercise or collecting the data needed for the monitoring actions process.

Compared to the virtual machines that simulate an entire operating system, containers simulate services or applications that use the same operating system kernel. In terms of performance, containers are a faster and more efficient version toward the virtual machines [20]. Cloud service providers are already using this option. In terms of container analysis, things are not as simple as their use. By sharing the same operating system, it is difficult to collect all the data from the container but also those related to it, from the operating system kernel. In paper [21], the authors have created a framework for collecting data from containers, running on multiple hosts, in a useful format for digital data investigators.

The problem of data collection being solved, the possibility of container monitoring remains questionable. In support of these, several tools have been developed to monitor the performance of container-simulated services. In a digital forensics training exercise a superficial monitoring is not sufficient, so there have been created systems that allow the extraction of metrics in order to measure user performance [22].

The chosen metrics for the scoring phase are the main pillar for the methods of extracting information about the activities performed by participants during an exercise and their achieved performance.

Monitoring, testing and evaluating the skills and activities of trained personnel using digital forensics techniques and methods is the main element through which training exercises can be improved and developed.

V. CONCLUSION

The digital forensics domain is a complex one requiring a continuous development to respond to the new challenges. The latest security threats require an in-depth knowledge of the techniques applicable to an incident and advanced abilities for detecting and effective response to cyber security incidents.

The most modern training methods that facilitate the acquisition of new knowledge, testing and assessing skills are cyber security exercises. Effective awareness training can improve the management of cyber risk and incident

response, fulfilling the requirements and responsibilities that make the changing of action course of a real security incident possible.

Our paper aims to highlight the importance of considering the digital forensics field in cyber training exercises. Digital forensics challenges integrated into cyber security exercises have a well-established role, bringing major benefits in the development of cyber education.

The role of digital forensics in training cyber security specialists is highly visible and requires accountability in terms of testing and determining the methods used for identification, collection and preservation of digital evidence.

By approaching different digital forensics methods and techniques one can improve the monitoring of participants' performance if they are using an appropriate environment in order to obtain realism, isolation, flexibility and scalability.

This study provides a new vision of training with cyber security exercises and contributes to the ongoing improvement of the digital forensics knowledge and skills.

REFERENCES

[1] A. Sagala and D. P. Lumbantoruan, "Developing a Small Scale Cyber Defense Competition," *ARPN Journal of Engineering and Applied Sciences*, vol. 10, no. 2, pp. 467-472, Feb. 2015. http://www.arpnjournals.com/jeas/research_papers/rp_2015/jeas_0215_1478.pdf

[2] V. V. Patriciu and A. C. Furtuna, "Guide for designing cyber security exercises," in Proc. 8th WSEAS International Conference on E-Activities and Information Security and Privacy, Puerto De La Cruz, Spain, pp. 172-177, Dec. 14-16, 2009.

[3] J. R. Kiper, "Forensication Education: Towards a Digital Forensics Instructional Framework," *The SANS Institute*, US, 2017.

[4] M. Frank, M. Leitner, and T. Pahi, "Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education," in Proc. 15th IEEE Intl. Conf. DASC/PiCom/DataCom/CyberSciTech, Orlando, FL, Nov. 6-10, 2017, pp. 38-46. doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.23

[5] J. McClain, et al., "Human performance factors in cyber security forensic analysis," *Procedia Manufacturing*, vol. 3, pp. 5301-5307, 2015. doi: 10.1016/j.promfg.2015.07.621

[6] R. G. Abbott, J. McClain, B. Anderson, K. Nauer, A. Silva, and C. Forsythe, "Automated Performance Assessment in Cyber Training Exercises," presented at the I/ITSEC No. SAND2015-5156C, Orlando, FL, 2015.

[7] R. Thomson, "Mentoring in Cyber Education: Capture-the-Flag Exercises to Promote Good Cyber Hygiene in Disadvantaged Populations," *West Point Military Academy*, 2017.

[8] M. Black, D. Chapman, and A. Clark, "The Enhanced Virtual Laboratory: Extending Cyber Security Awareness through a Web-based Laboratory," *Information Systems Education Journal*, vol. 16, no. 6, pp. 4-12, 2018. http://isedj.org/2018-16

[9] T. Garfinkel and M. Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection," in Proc. *NDSS Symp*, vol. 3, no. 2003, pp. 191-206, Feb. 2003.

[10] R. G. Abbott, et al., "Log analysis of cyber security training exercises," *Procedia Manufacturing*, vol. 3, pp. 5088-5094, 2015. doi: 10.1016/j.promfg.2015.07.523

[11] A. Pichan, M. Lazarescu, and S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," *Digital Investigation*, vol. 13, pp. 38-57, 2015. doi: 10.1016/j.diin.2015.03.002

[12] Y. Yusoff, R. Ismail, and Z. Hassan, "Common phases of computer forensics investigation models," *International Journal of Computer Science & Information Technology*, vol. 3, no. 3, pp. 17-31, Jun. 2011. doi: 10.5121/ijcsit.2011.3302

[13] P. Čeleda, J. Čegan, J. Vykopal, and D. Tovarňák, "KYPO–A Platform for Cyber Defence Exercises," in Proc. STO-MP-MSG-133: M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence, NATO Science and Technology Organization, Munich, Germany, 2015. doi: 10.14339/STO-MP-MSG-133-08-doc

[14] G. Abboud, J. Marean, and R. V. Yampolskiy, "Steganography and visual cryptography in computer forensics," in Proc. 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), 2010, pp. 25-32. doi: 10.1109/SADFE.2010.14

[15] *Artifact analysis fundamentals*, ENISA, Heraklion, Greece, 2014.

[16] K. Hahn, "Robust static analysis of portable executable malware," M.S. dissertation, Faculty of Computer Science, Mathematics and Natural Sciences, University of Applied Sciences, Economics and Culture - *HTWK Leipzig*, Germany, 2014.

[17] Y. Prayudi and I. Riadi, "Implementation of malware analysis using static and dynamic analysis method," *International Journal of Computer Applications*, vol. 117, no. 6, pp. 11-15, May 2015. doi: 10.5120/20557-2943

[18] B. S. Bloom, M. D. Engelhart, E. J. Furst, W. H. Hill, and D. R. Krathwohl, "Taxonomy of educational goals. Handbook I: Cognitive Domain," 2nd edition, New York, LONGMAN, 1956.

[19] R. S. Weiss, et al., "Teaching cybersecurity analysis skills in the cloud," in Proc. 46th ACM *Technical Symposium on Computer Science Education*, Kansas City, MO, 2015, pp. 332-337. doi: 10.1145/2676723.2677290

[20] Z. Li, M. Kihl, Q. Lu, and J. A. Andersson, "Performance Overhead Comparison between Hypervisor and Container based Virtualization," in Proc. 2017 IEEE 31st International Conference *Advanced Information Networking and Applications (AINA)*, Taipei, Taiwan, 2017, pp. 955-962. doi: 10.1109/AINA.2017.79

[21] S. Wu and J. Du. "DCFF: a container forensics framework based on Docker", in Proc. *2*016 3rd International Conference on Materials Engineering, Manufacturing Technology and Control, Atlantis Press, Taiyuan, China, 2016, pp. 1644-1650. doi: 10.2991/icmemtc-16.2016.313

[22] C. Stelly and V. Roussev, "SCARF: A container-based approach to cloud-scale digital forensic processing," in Proc. 7th DFRWS, Digital Investigation, vol. 22, Aug. 2017, pp. S39-S47. doi: 10.1016/j.diin.2017.06.008