A Serious Game-Based Peer-Instruction Digital Forensics Workshop

Ludwig Englbrecht, Günther Pernul

A serious game-based peer-instruction digital forensics workshop

Ludwig Englbrecht[0000−0002−8546−3017] and Guenther Pernul

Department of Information Systems, University of Regensburg, Regensburg, Germany
{ludwig.englbrecht,guenther.pernul}@wiwi.uni-regensburg.de

Abstract. Increasing threats in the area of information security raise the necessity for companies to be prepared for a digital forensic investigation. However, even the best investments in technology and infrastructure will fail if employees are not adequately trained. In this paper we propose a workshop concept combining the peer instruction method and elements from the field of serious games. The goal of the combined methods is to enable the participants to investigate a use case in an interactive and playful way. Our concept guides the participants step by step into an increasingly independent way of performing a digital forensic investigation.

Keywords: Digital Forensics · Workshop · Peer Instruction · Serious Games · Capture the Flag

1 Introduction

Over the past few years, threats exposed by cybercrime has increased significantly around the world. Due to the increasing threat of cybercrime, many companies are implementing ambitious technical measures to ensure information security. In doing so, they often rely mainly on defensive IT security measures instead of benefiting from methods from the field of Digital Forensics (DF). Digital traces collected during forensic investigations allow a comprehensive clarification of an IT security incident and can also be used as conclusive evidence in court [1].

However, the best security system is useless if cybercriminals can obtain confidential information by manipulating targets. People are often underestimated and seen as one of the biggest risk factors for information security. Inadvertent actions, a lack of security culture and insufficiently trained personnel are a popular target for attackers in most companies.

Consequently, raising employee awareness for computer crime and the use of DF techniques in companies contribute to a holistic information security. In this context the human has been recognized as an important information security factor. Von Solms and Warren [2] proposes a risk framework that can be used to understand human security issues originating from a lack of security awareness. A human can make a valuable contribution to the detection of an IT security incident if he or she detects and reports suspicious activities [3].

An enterprise can be prepared for a possible investigation of an IT security incident. Besides the technical and organizational measures, employees play a central part in DF. A well-planned training course for employees can make a massive contribution to being prepared for a DF investigation. The awareness for DF can significantly increase the maturity level of a company for Digital Forensic Readiness (DFR). However, this aspect is one of the most difficult challenges to reach a company-wide maturity level in DFR [4].

The aim of our workshop concept is to provide the participants with the skills of a DF investigation. The participants are put into the role of a DF expert, collect data and analyze traces in order to be able to understand procedures of a DF investigation. Furthermore, their awareness of cybercrime should be increased.

The paper is structured as follows. In the following section we present basics in DF, peer instruction, and serious game concepts. The development approach for a workshop concept is presented in section 3. In Section 4 a possible implementation of the workshop is described. Section 5 provides a summary and an outlook on future work.

2 Background and related work

2.1 Digital forensics

The forensic science deals with the application of scientific methods for investigations in legal cases [5]. Forensic scientists have to adapt questions of a legal case into scientific questions and answer these by using appropriate and scientifically validated methods [6]. This means, that DF has to provide profound methods to preserve and process digital evidence to guarantee the highest possible objectivity in DF investigations [7].

The collection and analysis of digital evidence must be based on a defined procedure. The model of Kent et al. [8] is a common procedure for forensic investigations. The investigation process is divided into four phases: *Collection, Examination, Analysis and Reporting*. This model has been used as a baseline for our workshop.

2.2 Peer Instruction Learning

Peer instruction (PI) was developed by the physicist Eric Mazur as part of his lectures at Harvard University [9]. Studies have shown the improvement of learning success through the use of the method [10],[9]. This led to an increased application of PI in the teaching of scientific subjects.

DF combines concepts from three different disciplines: computer science, criminology and law. The use of PI is intended to facilitate the understanding of DF and the interaction of the three subject areas [9].

Objectives pursued through PI. One goal is the activation of the participants by toggling between professional input and PI comprehension questions.

With this the participants are actively involved in the lecture and are encouraged to cooperate. They are also encouraged to not only passively learn the material, but to independently reflect and interpret the learning content and to link it to their previous knowledge. [9]

Deepening the understanding of the concept. PI focuses on promoting a basic understanding of concepts. Questions concerning the understanding help to internalize and adapt what has been learned. The greatest learning effect is achieved through the discussion phase. The participants are asked to convince others of their own solution to the question by using technical arguments. In this way, cognitive learning processes are initiated and the participants benefit from the form of learning through teaching. In addition, ambiguities, misunderstandings and misconceptions are identified and can be solved in a targeted manner. [9]

Instant feedback to the teacher. This teaching method enables the teacher to verify knowledge already during the lecture and receives direct feedback about how much the participants have understood. The teacher can then adapt the design of the course to the needs of the learners. This can be done, for example, to specifically address uncovered ambiguities or knowledge gaps. [9]

However, the above-mentioned objectives can only be achieved if the method is implemented correctly. The procedure of a PI sequence and the formation of effective comprehension questions are explained in detail in the following section.

2.3 Serious game concepts

Games can provide an interacting and motivational environment for learning [11]. Entertainment can be seen as the main motivation for traditional games. However, in the last decade, serious games that combine both computer and video games for non-entertaining purposes have become popular [12]. For this work we use Marsh's definition [12].

We also focus on digital game-based learning in an experiential environment. This is one aspect of the serious games continuum. In experiential environments, an *inductive learning* approach is used. In comparison to that, traditional instructional design usually includes methods to encourage *deductive learning*.

Inductive learning empowers students to deepen their understanding of content and develop their inference and evidence-gathering skills. This concept has been successfully applied in privacy-related areas to increase the awareness of shared information via social networks [13]. Inductive learning also provides a powerful setting to let students discover and verify hypotheses during a DF investigation. Adapted to our workshop digital evidence are meant to be found and verified to reconstruct a malicious action.

3 A serious game-based peer-instruction digital forensics workshop

By combining PI with a competitive serious game, we pursue three main goals in our workshop concept. After a motivational lecture under the guidance of the

lecturer, the students are supposed to switch to an independent processing mode. The lecturer guides the students and checks their understanding of the task at regular intervals. The second goal is to gradually reduce the workload of the lecturer. This is achieved by systematically reducing the amount of assistance. And the third goal is that the students solve the challenges of a Capture the Flag (CTF) as independently as possible and thereby experience a game-based and competitive-like character of the workshop. In Fig. 1 our workshop concept

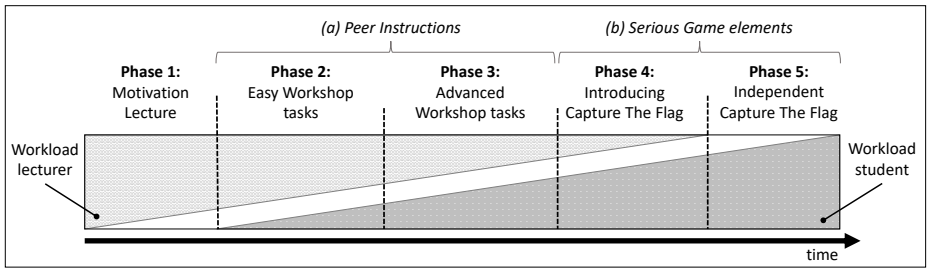

Fig. 1. Illustration of our workshop concept

is illustrated and grouped into five phases. In the following the different phases and the relation to the workload of the lecturer *(light grey)* and the workload of the students *(dark grey)* over the time will be described:

Phase 1: Motivation Lecture. In this phase a motivating lecture on the topic of DF will be held. This will show the basics and general procedures of DF. In addition, the special features of digital evidence and the investigation process will be explained. The teaching content has its origin in a Europe-wide decentralized cybersecurity curriculum [14]. This source enables the usage and exchange of clear content, module and delivery structure, and the appropriate tool support to facilitate collaboration and content reuse. In this phase the students only have to listen attentively and do not have to perform any activities.

Phase 2: Easy Workshop tasks. At the beginning of the actual workshop unit the case of the examination is briefly presented. A story frame will be created which will continue through the next phases.

In this phase the students are introduced to the techniques for the clarification of an IT security incident. The lecturer must still provide considerable support in the use of the forensics tools and the explanation of case-specific characteristics. By using peer-instruction, students can be given small tasks to find traces and to deduce the cause of the incident. In phase 2 and 3 PI is used several times as a short sequence during the lecture.

In a PI sequence, the participants are asked a multiple-choice format question about the content of the course. They are given two to three minutes to answer the question by hand signals, voting slips, clickers or mobile devices [10]. The aim of this first vote is to obtain a spontaneous and individual answer to the question asked by the instructor [9].

Depending on the results, the continuation of the lecture will be adjusted accordingly. If the participants answer the question correctly between 30% and 80%, a peer discussion and a second vote is held [15], [10]. In the discussion, the participants are given three to five minutes to convince their neighbors of their own solution with arguments. By explaining the problem to each other, conceptual thinking processes are set in motion and the understanding is deepened. Consequently, the rate of correct answers is usually higher in the second vote. [10]

If the rate of correct answers is less than 30%, the teacher needs to provide further explanations and then repeat the vote. However, if more than 80% of the answers are correct after the first vote, the question can be resolved by one participant and the discussion phase can be skipped. [15]

The success of the PI method is therefore primarily dependent on the questions of understanding. The intention is not to ask for knowledge, but to facilitate the processing and internalization of the contents.

The formulation of questions of understanding is crucial for the learning success of the participants when using PI. The aim of the multiple-choice questions is to promote the transfer of knowledge, to motivate discussion among the participants and to check the understanding of the presented content. Answering the questions should require the application of concepts and the transfer of previously learned knowledge. In this way the greatest learning effect is achieved [10]. In this paper the process of developing comprehension-oriented questions is applied and illustrated in Fig. 2.

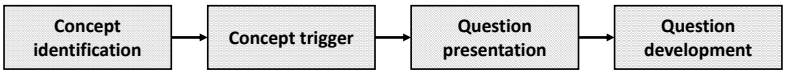

Fig. 2. Process for developing peer instruction conceptual questions (based on [10])

Concept Identification. The concept is determined, which needs to be conveyed to the participants through the PI question [10],[16].

Concept Trigger. Suitable "concept triggers" are selected to be included in the question. These are hidden elements that cause conceptual thought processes in the participants and should stimulate discussion [16]. An example is "Compare and contrast", in which the participants have to compare different situations with each other and conclude on the correct solution. [10]

With the concept trigger *Use "none of the above"* the participants are given the opportunity to reject the remaining answer options and to think about alternatives. [10]

Question Presentation. The next step is to determine how the question should be formulated and presented. There are various possibilities: In the scenario question, a scenario is described to which the question of understanding refers. The participants have to check the described situation for its clearly formulated and implied characteristics and decide on the correct answer. Example-

Questions, however, are limited to giving an example (e.g. an excerpt of a code). This variant leaves less room for interpretation than the scenario question. In a Definition Question, a definition is given, so that in order to answer the question, it is necessary to differentiate from other concepts. In the Diagram Question, a corresponding graph must be interpreted correctly in order to solve the question of understanding. In feature-questions, certain features of a concept must be correctly identified and assigned. [10]

Question development. The multiple-choice comprehension question is then formulated and completed on the basis of the previous process steps [10].

Phase 3: Advanced workshop tasks. In this phase, the degree of difficulty with regard to finding and interpreting digital traces is systematically increased. Tools such as *file carvers* and elements from the field of *open source intelligence* will be used. Since the lecturer has already introduced the analysis environment and tools in the previous phase, a low level of support from the lecturer is expected in this phase. The students will also learn to answer the questions of the lecturer more independently. By means of peer-instruction, the lecturer can monitor the learning progress and repeat teaching content if necessary.

Phase 4: Development of a subsequent Capture the Flag. In the previous phase the students have already learned to use and work with the forensics tools. Now the participants move into a competition. This means that the participants can now form teams and a CTF to the presented case is carried out. In this phase the instructor must explain the procedure and the rules of the CTF. A CTF is a good concept to introduce students to a variety of technical concepts within the computer science curriculum [17].

Through the previous phases the students have a common level of knowledge in DF and are already familiar with the case that needs to be analyzed. With this, the story has already been imparted for a serious game. Especially the use of a CTF ensures at that point of time an active and playful participation in the investigation of the incident. The main goal of this serious game situation is to encourage a competitive atmosphere between the groups.

The individual stages of the CTF can now be solved by the student with the methods learned before. By submitting the solution the students can find out if the solution was correct. In this phase, the lecturer steps more and more into the background in order not to disturb the competitive spirit. However, he offers assistance in case of unexpected complications.

Phase 5: Independent Capture the Flag. The last phase of the workshop is mainly focused on the independent solution of given challenges within the CTF. The procedure is similar to the previous phase. However, it is important that the lecturer is only marginally available for questions. The goal for the participants is to work out a dynamic and independent solution for practical questions in the field of DF. This can even go so far that the lecturer is no longer physically present and can only be reached by email. This phase can be extended to a period of several days as the students can solve the questions independently of their location.

4 Instantiating of the workshop concept

The basic course architecture is designed to be a more generalized concept within the cybersecurity discipline. This enables a broad adaption in DF and related areas (e.g. incident response or malware analysis). We focus within our instantiating of the workshop concept on business-related crime to attract the attention of managers and decision-makers of an organization.

4.1 Conception of the workshop

Based on the theoretical foundations of digital forensics described in section 2 and the proven teaching method of PI, the workshop on the investigation of white-collar crime using Mobile Forensics Analysis was designed in four successive steps. The development process is based on a top-down approach. The methodology describes a procedure in which the planning stages are concretized step by step from top to bottom and finally a connection is established.

The first step was to define the objectives and target group of the workshop. The next step was to determine the practical and theoretical knowledge, taking into account the characteristics of the participants, which is necessary to achieve the previously defined goals. The contents are to be worked out by the workshop participants themselves in a use case and internalized by PI and a CTF. In the third step, a fictitious white-collar crime case was developed with the decisive roles and scenes that are used for forensic clarification. At the same time, the PI comprehension questions and CTF challenges were formulated to deepen the presented contents. Based on this, the schedule of the workshop was determined.

4.2 The goal of the workshop

For a successful workshop concept it is essential to define the objectives and the target group. Both points have a significant influence on the subsequent elaboration. The definition of the objectives and target group of the workshop is described below.

Companies are increasingly becoming victims of cybercrime and the digital attacks are also costing companies a significant amount of money. Given this increasing threat, organizations are making a high technical effort to protect themselves from attacks. However, people are regularly underestimated and seen as one of the biggest risk factors for information security. Besides technology, the consideration of the human factor as a security measure is also decisive. The aim of our workshop is to sensitize the participants to the topic of cybercrime and thus to minimize the dangers caused by employees in this area in companies and organizations.

The use of DF enables companies not only to detect cyber attacks but also to prosecute the perpetrators. However, many organizations have not yet been aware of the benefits of DF in this context. For this reason, the workshop aims to use Mobile Forensics Analysis to clarify a fictitious white-collar crime case in order to strengthen the understanding of the importance of information security

in companies and to illustrate the role of DF in securing evidence that can be used in court and in solving the crime.

Target group. The technical measures and the associated IT experts are only one part of a security system. The workshop focuses on managers since they are responsible for personnel management tasks and thus have a significant influence on the behavior of other employees in the company. In addition, young professionals and graduates, i.e. young employees who are about to start their careers are among the target groups of the workshop. They are highly motivated to put their knowledge into practice. This can contribute to the rapid spread of a security-aware culture within a company.

Based on the defined objectives and the characteristics of the defined target group, the content of the workshop is determined in the next section.

4.3 Definition of the content of the workshop

The aim of the workshop is to sensitize the participants to the tactics of cybercriminals and to create an awareness for responsible security actions in everyday life. When determining the content of the workshop, it must be taken into account that the participants do not necessarily have in-depth IT knowledge. The presented contents and all connections must be coherent, understandable and interesting. In this way, the attention of the participants can be maintained throughout the entire presentation and thus the best learning effect can be achieved.

In our workshop the participants should first be informed about current threats of cybercrime in general to get motivated. They will also learn current cases, causes of threats, (resulting) damages and factors that promote cyber attacks in companies. They will also learn the characteristics of the most common manifestations: phishing (identity theft), malware, ransomware (digital blackmail), social engineering, botnets, DDoS attacks and CaaS.

After an introduction to a fictitious white-collar crime case to be dealt with, the workshop participants are thereafter introduced to the forensic process according to Kent et al. [8] as an essential component of DF. The interaction between employees and IT experts is crucial in forensic investigations and will be highlighted in the lecture.

Using a fictitious case study, the tasks of the four phases of the investigation process Collection, Examination, Analysis and Reporting are demonstrated. The focus is particularly on understanding the volatility of digital evidence. Knowledge about this shows that evidence can be inadvertently destroyed in the event of an IT security incident. In this context, the participants will be familiarized with the characteristics of persistent, semi-persistent and volatile traces. They will learn that traces must be captured according to a specific sequence of preservation, depending on their volatility, and that they must be collected and processed by means of post-mortem or live analysis.

Through the live analysis of digital traces using examples, the participants are given the opportunity to put themselves in the role of an IT forensic scientist and apply the basic principles of forensic science. For this purpose, hypotheses are

established during the clarification of the fictitious white-collar crime case and verified or falsified during the forensic investigation process. The digital traces found are identified, classified and individualized according to Inman and Rudin [18]. Subsequently, the associations are established and based on this the course of events is reconstructed. Finally, the participants receive recommendations for behavior with regard to cyber attacks and preventive measures for companies are explained.

The practical and theoretical contents and interrelationships are better demonstrated within the workshop by working through the use case. This will be explained in detail in the next section.

4.4 Development of a use case

By processing a use case, the participants of the workshop are expected to understand cybercrime and DF techniques. The workshop will use realistic case descriptions to demonstrate cybercrime and the procedure of a DF investigation.

The reasons for espionage have remained unchanged to this day. However, the methods and possibilities have evolved over time. Nowadays, for example, services for committing or supporting computer-based crimes (e.g. CaaS) can be easily purchased over the internet [19]. The illegal services offered include the sale of commercial malware such as spyware, which enables to spy on the infected system and thus obtain confidential information.

The use case is a core component of the workshop and, in view of this new threat potential, addresses the use of the popular manifestations of computer crime. Especially CaaS and social engineering in the context of espionage will be addressed.

The participants will be introduced to the case study with the presentation of two fictitious companies in the lighting industry. Hyperlight AG is the current market leader with a turnover of approximately 4 billion EUR and would like to secure its competitive position in the future. Luxia AG (approx. 2 million EUR turnover), on the other hand, has only a small market share so far. By installing a commercial spyware on the smartphone of a sales representative of the competitor company, Luxia AG can gain considerable competitive advantages through espionage. As a result, Hyperlight AG suffers high material and immaterial damages.

The task of the participants is to put themselves in the role of an IT forensic scientist and to clarify and reconstruct this course of events through forensic investigation. The four phases of the investigation - collection, examination, analysis and reporting - are explained step by step and illustrated using examples. In the collection phase they learn about the characteristics of persistent, semi-persistent and volatile data and the differences between post-mortem and live analysis are explained. On the basis of the knowledge acquired, the participants decide to perform a live analysis on the infected smartphone. The examination of the application memory, network traffic and browser cache will be illustrated as realistically as possible by providing a modified smartphone. The digital traces

found are identified, classified and individualized according to Inman and Rudin [18]. Based on the derived associations and verified hypotheses the course of events can be reconstructed step by step:

Luxia AG has made use of the illegal business model CaaS. CaaS generally offers a comprehensive range of tools and technologies as services to support or carry out cyber attacks. The participants can be made aware of the fact that nowadays no extensive IT knowledge is necessary to carry out cyber attacks. In this way, commercial spyware is installed on the smartphone of the Hyperlight AG sales employee by the competitor company. This is initially noticeable through conspicuous features such as slow reaction times, program crashes and disturbances during telephone calls. In this way, the workshop participants learn about the signs of an infected mobile phone. They also discover that the spyware collects a variety of confidential information such as GPS data, messages and images unnoticed and without the system user's consent, and forward it to the attacker's server. To install commercial spyware, usually physical access to the smartphone is required.

This is intended to sensitize workshop participants to the fact that social engineering can be used to obtain safety-relevant data comparatively easily by exploiting human components. After the clarification and reconstruction of the course of events, the material and immaterial damages following a cyber attack will be discussed using Hyperlight AG as an example. During the processing of the use case, the knowledge transfer is checked and deepened several times by PI comprehension questions. The next section deals with the development of the corresponding questions.

4.5 Formulation of peer instruction comprehension questions

Peer instruction comprehension questions are not intended to test knowledge, but rather to facilitate the participants' understanding and internalization of the contents presented. In addition, the discussion potential of the question is particularly important in order to initiate thought processes and thus achieve the greatest learning success. Five PI sequences will be used in the workshop. In the following, the development of the comprehension-oriented questions used in the lecture will be explained.

The first PI comprehension question is based on the development of cybercrime as presented earlier in this paper. For this purpose, current cases are presented on the one hand and diagrams are shown on the other hand on the increase in the number of cyber attacks and the costs of companies in connection with computer crime (Example/Diagram-Question). In order to answer the question, it is necessary to interpret and reason the diagrams (Concept Triggers: Interpret representations, Analysis and reasoning). In this way, the participants learn about the factors that promote cyber attacks (Concept Triggers: Extend the context). In the use case, features of a smartphone infected with spyware are listed (Feature-Question).

In order to answer the second question of understanding, these signs must be compared with the characteristics of the various manifestations of cybercrime

that have been identified previously (Concept Trigger: Compare and contrast). It is necessary to select those types of cyber attacks that can cause the described abnormalities. By answering the question, the participants are also given the option of rejecting the remaining answers (Concept Trigger: Use "none of the above"). This should motivate them to think about alternative solutions.

The workshop covers the properties and effects of spywares and fileless malware (scenario question). Participants have previously learned how to use post-mortem and live analysis. In the context of the third PI comprehension question, they have to decide on the appropriate approach for obtaining and processing digital traces in the respective situation (Concept Trigger: Qualitative question). In order to answer the question, it is necessary to compare the two approaches (Concept Trigger: Compare and contrast). Based on this, the correct solution can be concluded after the analysis of the described scenario (Concept Trigger: Analysis and reasoning).

After the incident has been reconstructed (Scenario-Question), the workshop participants should identify the damage caused by the cyber attack in the context of the fourth comprehension-oriented question (Concept Trigger: Qualitative questions). To answer the question, assumptions must be made (Concept Trigger: Require unstated assumptions). This is intended to sensitize the participants to potential material and immaterial damage.

Based on the content presented within the workshop, especially the characteristics of DF investigations, the final question of understanding will address possible problems of criminal prosecution of cyber attacks (feature-question) (Concept Trigger: Extend the context). For this purpose, the respective answer options of the multiple-choice question must be evaluated and justified by the participants (Concept Trigger: Qualitative question, Analysis and reasoning).

Through these five PI comprehension questions, the teacher can verify the participants' knowledge and receive feedback on how much the participants have understood. The distribution of questions during the workshop is illustrated in the next section.

4.6 Time schedule of the workshop

After determining the theoretical foundations of DF to be taught, developing the use case and formulating the PI comprehension questions, the workshop was developed. As a final result of the conception, the corresponding time schedule and procedure will be described in detail in this section.

A total of three and a half hours are scheduled for the workshop (break/s are not included). This allows the workshop to be held as a half-day teaching module. The lecture will be divided into the following sections:

Phase 1: Introduction and motivation. First, the participants are introduced to the topic. Current cases of cybercrime will be highlighted and the increasing threats of cyber attacks for companies will be illustrated with adequate diagrams. Then the potential material and immaterial damages are discussed. The participants will also learn about the manifestations of phishing, malware, ransomware (digital blackmail), social engineering, botnets, DDoS attacks and

CaaS. This section will take about 30 minutes to motivate the students and to frame the context.

Phase 2: Presentation of the Use Case. Next, the use case is presented. Subsequently, the participants are asked to relate the described signs of an infected smartphone to the corresponding manifestations of cybercrime they have previously learned. This is performed by means of a PI comprehension question. Furthermore, a first hypothesis is put forward and spyware as a specific form of malware is explained. This section will take about 30 minutes to bring up ideas and discuss the input of the participants followed by performing easy workshop tasks.

Phase 3: Forensic Investigation 1/2. The third section begins with a short presentation of the forensic investigation process. The tasks of the first process step *collection* are explained. In particular, the volatility of digital traces and the backup sequence based on them are illustrated. In addition, the participants will learn the characteristics and use of the basic approaches of post-mortem and live analysis. The understanding will be tested with a PI comprehension question. Next, the *examination phase* of an investigation will be introduced. It is necessary to analyze application memory, network traffic and browser cache of the smartphone for digital traces. For this section about 30 minutes are planned to find a good balance between the explanation of the tools and the interpretation of the results.

Phase 4: Forensic investigation 2/2. This section introduces the core of the workshop, the *analysis phase*. Participants will learn how to apply the basic principles of forensic science to the Inman and Rudin forensic process [18]. The digital traces found by the participants are identified, classified and individualized. Subsequently, associations are made and previously established hypotheses are verified. In phase 4 the CTF is introduced first and the participants solve different challenges under guidance. Finally, the case will be reconstructed and the extent of damage caused by the cyber attack will be discussed.

The last step of the forensic investigation process, the reporting, is described. A cyber kill chain will then be drawn and the course of events will be summarized once again using the seven points Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives [20].

The presentation of preventive measures is important to bridge the gap between the fictitious case and possible future situations. The workshop concludes with the presentation of measures to prevent cyber attacks. The participants will receive recommendations for behavior and preventive measures for companies and organizations will be explained. Approximately 15 minutes are scheduled for the presentation of preventive measures.

The lecture contains a total of five PI comprehension questions to review and deepen the presented contents. For each question 5 - 9 minutes are planned (these are already included in the duration of the respective section). For the whole phase 4, about 90 minutes are scheduled.

Phase 5: Capture the flag. The last phase of the workshop is mainly focused on the independent solution of given CTF questions. The concept of

a CTF is applied. For this phase the remaining time as well as time after the workshop can be used. This means that the participants can solve the challenges after the workshop.

The workshop should also be prepared and followed up. The preparation includes the planning of a sufficiently large room. Furthermore, the technology required for the presentation should be checked beforehand. The schedule and agenda of the workshop can be sent electronically to the participants a few days before. In the follow-up, a protocol of the results should be provided together with feedback forms. The time planned for the CTF is very individual and can range from a minimum of 30 minutes to a period of days. This allows the students to pursue and deepen the content outside of the workshop.

5 Conclusion and future work

Companies are increasingly becoming victims of cybercrime and the digital attacks are also costing companies more and more money. For this reason, a workshop was designed to clarify white-collar crime using Mobile Forensics Analysis. The aim is to sensitize employees of companies and to create an awareness for responsible security actions in everyday life. In addition, the advantages of methods from DF to be able to react quickly and purposefully to cyber attacks need to be illustrated. The workshop was conceived in four successive steps. First, the objectives and target group were defined in detail. Based on this, the theoretical and practical knowledge about cybercrime and DF has been defined. This has been incorporated in a use case and enriched with PI comprehension questions. The use of the teaching method PI supports the processing and internalization of the presented contents during the entire workshop. For this purpose five comprehension-oriented multiple-choice questions and a CTF were formulated. As a final result of the design, a time and sequence plan was then drawn up, linking the previous planning stages.

However, the question of the success of this security awareness measure remains open. To improve and strengthen the security culture is also an important component of a holistic information security. Therefore, the measurement of employee awareness and the effectiveness of an interactive workshop based on the concept of this paper will be addressed in future work.

Acknowledgment. This work is partly performed under the BMBF TRIO project which is supported by the German Federal Ministry of Education and Research. (https://www.innovative-hochschule.de/de/innovative-hochschulen/trio)

References

1. Meier, S.: Digitale Forensik in Unternehmen. Ph.D. thesis, University of Regensburg (2017)
2. von Solms, R., Warren, M.: Towards the human information security firewall. International Journal of Cyber Warfare and Terrorism (IJCWT) **1**(2), 10–17 (2011)

3. Vielberth, M., Menges, F., Pernul, G.: Human-as-a-security-sensor for harvesting threat intelligence. Cybersecurity **2**(1), 23 (2019)
4. Englbrecht, L., Meier, S., Pernul, G.: Towards a capability maturity model for digital forensic readiness. Wireless Networks (2019)
5. Cohen, F.: Toward a science of digital forensic evidence examination. In: Chow, K., Shenoi, S. (eds.) Advances in Digital Forensics VI - Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China, 2010. IFIP Advances in Information and Communication Technology, vol. 337, pp. 17–35. Springer (2010)
6. Elyas, M., Ahmad, A., Maynard, S.B., Lonie, A.: Digital forensic readiness: Expert perspectives on a theoretical framework. Computers & Security **52**, 70 – 89 (2015)
7. Grobler, T., Louwrens, C.P., von Solms, S.H.: A framework to guide the implementation of proactive digital forensics in organisations. In: ARES 2010, Fifth International Conference on Availability, Reliability and Security, 15-18 February 2010, Krakow, Poland. pp. 677–682. IEEE Computer Society (2010)
8. Kent, K., Chevalier, S., Grance, T., Dang, H.: Guide to integrating forensic techniques into incident response. NIST Special Publication **10**(14), 800–86 (2006)
9. Crouch, C.H., Mazur, E.: Peer instruction: Ten years of experience and results. American journal of physics **69**(9), 970–977 (2001)
10. Johnson, W.E., Luzader, A., Ahmed, I., Roussev, V., III, G.G.R., Lee, C.B.: Development of peer instruction questions for cybersecurity education. In: 2016 USENIX Workshop on Advances in Security Education (ASE 16). USENIX Association, Austin, TX (2016)
11. Kiili, K.: Digital game-based learning: Towards an experiential gaming model. The Internet and higher education **8**(1), 13–24 (2005)
12. Marsh, T.: Serious games continuum: Between games for purpose and experiential environments for purpose. Entertainment Computing **2**(2), 61–68 (2011)
13. Cetto, A., Netter, M., Pernul, G., Richthammer, C., Riesner, M., Roth, C., Sänger, J.: Friend inspector: A serious game to enhance privacy awareness in social networks. CoRR **abs/1402.5878** (2014)
14. Tokola, T.J., Schaberreiter, T., Quirchmayr, G., Englbrecht, L., Pernul, G., Katsikas, S.K., Preneel, B., Tang, Q.: A collaborative cybersecurity education program. In: Cybersecurity Education for Awareness and Compliance, pp. 181–200. IGI Global (2019)
15. Lasry, N., Mazur, E., Watkins, J.: Peer instruction: From harvard to the two-year college. American journal of Physics **76**(11), 1066–1069 (2008)
16. Ahmed, I., Roussev, V.: Peer instruction teaching methodology for cybersecurity education. IEEE Security & Privacy **16**(4), 88–91 (2018)
17. McDaniel, L., Talvi, E., Hay, B.: Capture the flag as cyber security introduction. In: 2016 49th Hawaii International Conference on System Sciences (HICSS). pp. 5479–5486 (Jan 2016)
18. Inman, K., Rudin, N.: The origin of evidence. Forensic science international **126**(1), 11–16 (2002)
19. Manky, D.: Cybercrime as a service: a very modern business. Computer Fraud & Security **2013**(6), 9–13 (2013)
20. Yadav, T., Rao, A.M.: Technical aspects of cyber kill chain. In: International Symposium on Security in Computing and Communication. pp. 438–452. Springer (2015)