Human Interaction and Emerging Technologies (IHIET 2023), Vol. 111, 2023, 830–839
https://doi.org/10.54941/ahfe1004091

Training for Digital Forensics and Incident Response

Marko Schuba, Tim Höner, and Sacha Hack

FH Aachen University of Applied Sciences, Aachen, Germany

ABSTRACT

The work of a digital forensics expert is far more extensive and varied today than it was just a few years ago. Especially after hacking attacks on organizations, experts in DFIR (Digital Forensics and Incident Response) come into play. In this paper, we present a learning platform that enables people to learn DFIR from scratch. To achieve this goal, the content of the learning platform was defined, evaluated and prepared with the help of experts from industry and government. The experts were interviewed and the results incorporated into initial scenarios that were implemented in individual modules on the learning platform Ilias, with a distinction being made between the basics and the main DFIR part.

Keywords: IT, Forensics, Incident response, Digital forensics, DFIR, Training

INTRODUCTION

The digitization of our society is progressing relentlessly. This has been accompanied for years by an increase in the number of cases in which digital systems or data are the target or catalyst of a crime. The Federal Criminal Police Office's situation report on cybercrime in Germany paints a grim picture (GFOCI, 2021). In 2021 alone, the number of recorded cybercrimes increased by twelve percent compared to the previous year. Solving these crimes is the task of digital forensics experts. Yet the clearance rate is only just below 30 percent. One of the reasons for this is the lack of well-trained personnel.

Unfortunately, the training of digital forensic experts is not trivial, because the work of a forensic expert today involves much more than the classic search for clues on a computer. Countless subject areas and specializations fall under the umbrella term "digital forensics". This multitude of topics makes it impossible to cover them completely in a single training. Feedback from the industry has made it clear that starting a career as a digital forensics specialist is accompanied by a steep learning curve and that additional training opportunities often need to be taken advantage of. Therefore, the desire arose for prospective digital forensic experts to be given an opportunity for training and further education that is oriented towards the requirements of companies and authorities and focuses on the forensic processing of hacker attacks: DFIR (Digital Forensics and Incident Response).

In order to define the contents of such a DFIR training, a qualitative research method was chosen, which is based on expert interviews. The selection of interviewees is intended to reflect the range of potential employers. For the learning method theoretical sections alternate with practical sections in order to be able to directly apply what has been learned theoretically in practice. This approach was coined by John Dewey (Dewey, 1997) and is already used in many IT security trainings. In addition, the resulting DFIR training should be as modular as possible so that it can be quickly expanded or adapted.

EXISTING LEARNING OPPORTUNITIES IN DIGITAL FORENSICS

There are already a number of training courses in the area of digital forensics, which are offered by commercial service providers in particular.

SANS Institute

The SANS Institute (SANS 2023) offers high-quality education and training in various disciplines of IT security. The different contents are divided into so-called "skill paths". For example, there is the learning path "Cyber Defense & Blue Team Operations" or "ICS/SCADA Security" (Industrial Control Systems, Supervisory Control and Data Acquisition), but also "Digital Forensics and Incident Response". Each learning path consists of different courses. The SANS Institute itself divides the courses into different difficulties, i.e., knowledge levels of the participants. For beginners, for example, the course "FOR308: Digital Forensics Essentials" is offered, which teaches participants basic concepts of digital forensics and creates a foundation on which further courses can build. In addition, there are courses for special areas of digital forensics, such as cloud or ICS forensics.

EC-Council

EC-Council (International Council of Electronic Commerce Consultants) (EC Council 2023) provides education and training in IT security. In the field of forensics it offers the so-called "Computer Hacking Forensic Investigator (CHFI)". The course is constantly updated and is now available in version 10. The course does not require any special prior knowledge in the field of digital forensics but covers a wide range of content. A total of 16 modules is covered with different areas of focus, ranging from Computer Forensics Investigation Process to IoT Forensics. Therefore, the entire course offers a comprehensive overview many important topics in digital forensics. The CHFI course works with a mixture of theory and practice. In small sections, participants can independently try out the tools and techniques discussed and thus consolidate their knowledge.

Infosec Institute

The Infosec Institute (Infosec 2023) also offers education and training in the field of IT security. In addition to classic penetration testing courses, there is also the learning path "Computer Forensics" which is divided into 13 smaller course sections. In this learning path the participants receive information and knowledge about different areas of computer forensics. The learning path is limited to forensic investigations of single systems. Only network forensics is addressed as an additional topic. The Infosec Institute also mixes practical sections with theoretical ones. The theory is largely taught via prepared videos. The practical part is done via cloud-hosted labs, which do not require any special software or hardware on the part of the students. At Infosec Institute, you cannot buy individual courses, but must purchase an annual license. This gives access to the complete training catalog.

Various Online Providers

In addition to the larger providers mentioned, there are a number of general training platforms that also offer digital forensics content, e.g., Udemy (Udemy, 2023) which is an online learning platform where instructors can make their course content publicly available and where 59 courses in digital forensics are currently offered. Another example is OpenLearn (Open, 2023), which follows a similar principle to Udemy, but currently offers only one course in digital forensics. edX (EDX, 2023) describes itself as an online university offering courses and content from a total of 160 partner universities. Due to the proximity to the university environment, the course content is well prepared and meets a certain quality standard. In the area of digital forensics, for example, the basic course “Computer Forensics” is offered.

Summary on Training Options

Several training options are available for interested beginners. However, these can be problematic in several respects. In the case of service providers, the costs that can arise for participants should not be neglected. In addition, learning opportunities that require fixed attendance times are also difficult, as these are not always compatible with normal daily routines. ≪In terms of content, the courses cover a wide range of topics. However, the important area of DFIR is only sparsely represented, which makes it necessary to expand the training options.

EXPERT INTERVIEWS METHODOLOGY

In order to find and evaluate possible course content, experts from business and government were consulted. The personal experiences and assessments of the respective interviewees are of crucial importance to good course content. For this reason, a qualitative research method (Brannan et al., 2017) was chosen. Here, the goal is not to be able to compile representative statistics, but to gain honest and deep insights into the everyday work of digital forensic experts. The answers and results are not necessarily quantifiable, but they make it possible to derive concrete situations or circumstances that experts face in this environment. Content can then be extracted from these results in the follow-up, which significantly increases the relevance of the resulting course.

Interview Type, Expert Selection, and Interview Evaluation

To obtain the desired information, semi-structured interviews were used (Meyer et al., 2009). In this approach, an openly conducted interview is structured with the help of a guideline. Partially structured means that questions are also formulated in an open manner, giving the interview participants the opportunity to speak freely about their experiences. The guideline serves mainly as an orientation aid to repeatedly provide key words that continue the conversation and gently guide it in the desired direction. A great advantage of the semi-structured interview is that information can also be obtained that the interviewer was completely unaware of. The guide therefore also offers sufficient freedom to address previously unknown information without losing focus on the central questions.

The selection of the interview partners was based on selection criteria. These limit the choice of possible candidates but ensure that the answers are qualitatively more suitable for this elaboration. All interviewees should be working in the field of digital forensics. This is self-explanatory and was the basic requirement for all participants. The current work environment of the participants should be able to cover a broad spectrum. Thus, it was important that interview partners from the private sector, but also from law enforcement agencies were involved.

For the semi-structured expert interviews thematic units with a contextual connection were formed, irrespective of the point mentioned in the interview. For the purpose of this content analysis, categories are developed based on the central questions and the statements of the interview partners. After the interviews were analyzed, subcategories were formed to further compress the content and improve clarity. The subcategories formed were then assigned to specific text passages.

Interview Guideline

A guideline was drawn up for conducting the interviews. This was intended to structure the interviews and was divided into four sections for this purpose.

1. Presentation of the topic: Before the actual interview, the interviewees are informed about the intention of this work. For this purpose, a short summary of the topic is given. This leads to the fact that the participants have the intention in the back of their minds when answering the individual questions and can better estimate which purpose the respective question serves.
2. Questions about the person and introduction to the topic: In this part of the interview, the focus is on the background of the interview partners, e.g. their current position but also their educational background and career.
3. Key questions: This section focused on the requirements for DFIR experts. The questions form the core of the interviews and dive deeply into the experts' experiences in DFIR processes, tools, and needs.
4. Conclusion and summary: Here, the interviewer is given a summary of the interview process so far and his or her answers are briefly reflected upon. The whole procedure is intended to enable the interview partner

to make any additions or corrections. This ensures that the interviewer has documented everything correctly.

Interview Partners

Four experts were interviewed. Emphasis was placed on a personal environment so that the interviewees could speak freely and openly. At the start, participants were asked whether the conversation could be recorded, which made it possible to transcribe the answers verbatim. The experts were:

- Consultant for an IT security company in NRW (North-Rhine Westphalia). The company is a classic consulting firm in the field of IT security, covering many disciplines from penetration testing and forensics to data protection topics. The interviewee is frequently involved in forensics of all kinds.
- IT security consultant for a medium-sized company in NRW. The company focusses on cloud technologies and advises its customers in many areas including security-related topics. The consultant has already worked as an IT security consultant in previous jobs and thus has a broad range of knowledge.
- Consultant for a large accounting firm whose services range from insurance services and tax consulting to other consulting services for private or public sectors. The company also provides IT security and forensics services for their clients. The consultant works in the field of digital forensics.
- Digital forensics expert of a German police authority. By contributing to the investigation of criminal offenses the expert has gained broad and deep insights into the activities of a digital forensics expert at law enforcement agencies. He currently works mainly in the field of mobile forensics.

EXPERT INTERVIEW RESULTS

It was interesting to learn that none of the interviewees had a standardized DFIR approach being used in their respective organization. Rather, there were overriding goals that shaped the respective phases of the forensic investigations. These could best be formulated as follows: Understand, Control, Cleanup and Restart. However, the approach taken in each of these phases was very much shaped by the incident in question and the customers associated with it. It was therefore difficult for the respondents to make general statements. The respondents were most explicit on the subject of time pressure. This was the most difficult aspect when starting a career, even more so than technical issues. While training is often about finding very correct and technical solutions, the reality is much more time critical. The constant inquiries and waiting for results from the customer would put enormous pressure on the forensic investigators. Here, the wish was expressed several times to include this circumstance in the training.

Important Information in DFIR Cases

In the context of an incident response forensic investigation the aim is to identify information that can clarify the course of events. This key information is also called "Indicator of Compromise" (IoC) and are indicative of possible malicious behavior of components or systems. IoCs are therefore the focus of a forensic investigation and it is extremely relevant to learn what kind of IoCs are being looked for and in which data sources they can be found. In a training, such information sources should be presented in particular. Once an initial IoC has been found, it can provide clues as to the type of active threat. It was therefore also interesting to see how to proceed after finding such a clue. Log files were cited by all stakeholders as the most important source of data to find out what happened, which systems were affected, and how to restore systems to a secure state. Traditional computers, network and security systems were mentioned as important log file sources to contain information on the spread of the incident.

DFIR Tools and Techniques

One training goal should be to allow participants to get to know and try out tools and techniques that are used in the real world. In addition to programs that have been developed specifically for forensic investigations, more general tools should also be mentioned here. Depending on the previous education, participants may already know different operating systems, programming languages or tools. To be able to prepare all participants of the course optimally for their later working life, it was therefore important to find out which basics forensic experts have to bring along nowadays. The evaluation of the interviews showed that there is no uniform tool chain even within an organization. This was confirmed by various statements of the participants. Nevertheless, different commonly used tools were mentioned repeatedly. These included Grafana Loki (GrafanaLabs 2023), Thor APT Scanner (NextronSystems 2023), Loki IOC and YARA Scanner (Neo23x0 2023), and Autopsy (Autopsy 2023). Knowledge of Yara (VirusTotal 2023) was also mentioned as important.

DFIR TRAINING PROGRAM DEVELOPMENT

Based on the interviews, a DFIR training program was designed. Implementation has taken place for some initial scenarios but is far from complete. However, the work forms a basis for the implementation of a complete training program. All lessons were tested for their function and feasibility and are suitable for the course program in the way described.

Learning Management Platform - Ilias

The open-source Learning Management Platform Ilias was chosen as the basis (Ilias, 2023). Ilias provides a platform for the presentation for theoretical content. Tests and quizzes can be used to assess learning levels in various question types, on the one hand as a self-monitoring tool for the participants, and on the other hand as a way for the supervisors to check the learning success of the individual participants.

Gamification - CTFd

CTFd is a free, open source capture the flag platform (CTFd, 2023). Capture the Flags are established competitions in the IT world. The basic principle of CTFs is the acquisition of so-called flags, which can then be handed in on a platform. Depending on the speed or correctness of the answer, points are awarded which can be viewed on a scoreboard. CTFd takes over the role of gamification in the DFIR course. CTFs are mainly intended to accompany the practical labs. On the CTF page, participants will then find the tasks to be completed, rankings, progress bars and their achieved points. By comparing them with other participants, the aim is to increase motivation.

Practical Part - Lab Design

Labs are hands-on assignments that can be completed asynchronously by the participants. This means that students can access the content of the practical sections at any time and from anywhere. Currently, virtual machines are used for this purpose, but it is planned to host the VMs on a centralized server infrastructure in the long term. A VM based on Kali Linux (OffSec, 2023) serves as basis. Kali is a freely available Linux distribution and is the operating system of choice in the environment of IT security and forensics. Consequently, the handling of Linux is a crucial skill for any DFIR expert, which was also reflected in the interviews. Kali is adapted to work in a DFIR environment and provides many required tools. All other required tools, images, data or scripts are integrated into the basic Kali VM, so that in the end a “single source of truth” is created. When changes are made to the course, only the master image of this VM needs to be edited. Using such a VM it is also quite easy to generate “snapshots”, i.e., images of the virtual machine in a certain state, so participants can switch back to an error-free state at any time once problems should occur.

General Structure of the Course

During the course, a complete forensic case, should be presented in the most possible realistic way. “Realistic” means: based on the examples, tools and techniques provided by the interview experts. If this is not possible due to licensing issues or from a technical perspective, adequate substitutes should be used. To optimize the learning success, the course is structured in two parts.

The first part consists of many small lessons, each including a theory part and a practical exercise. Here, the complete process of a forensic investigation will be presented and explained and the participants get to know each tool and technique, including background information. In addition, the central VM is required to be able to complete practical tasks. CTFd is not yet used. After the first part, participants should be able to assess and solve small forensic cases. They should have learned how to use different tools and be able to put this knowledge into practice. Topic areas of the first part are:

- Introduction to Forensics
- Dealing with Linux

- Creating a RAM image
- Creating a hard disk image
- Dealing with different image formats
- Extracting information from images
- Information on special devices and systems
- Structuring information
- Search IoCs
- Cleaning and restarting systems
- Completion of a forensics and dealing with time pressure.

In the second part, gamification will play a greater role. Here, it should be possible to play through a complete case without any further theoretical components. This part takes place entirely in a lab and is prepared as capture the flag exercise.

Participants receive a problem in the form of questions and must come up with a possible solution themselves. For each correct solution, i.e., each flag found, the participants receive points and experience. The points are used for direct comparison with others and are intended to increase motivation. The experience symbolizes the personal progress of each participant. For this part of the course, CTFd is used as a platform. Participants thus have a clear separation between theory sections and pure practice.

The implementation of the second part is again based on the Kali VM, which is also used in the first part. In addition, further images are required to represent the network of a compromised victim. The individual tasks guide the participants through the case and always give hints for the next steps. The simulated network of the victim is shown in Fig. 1.

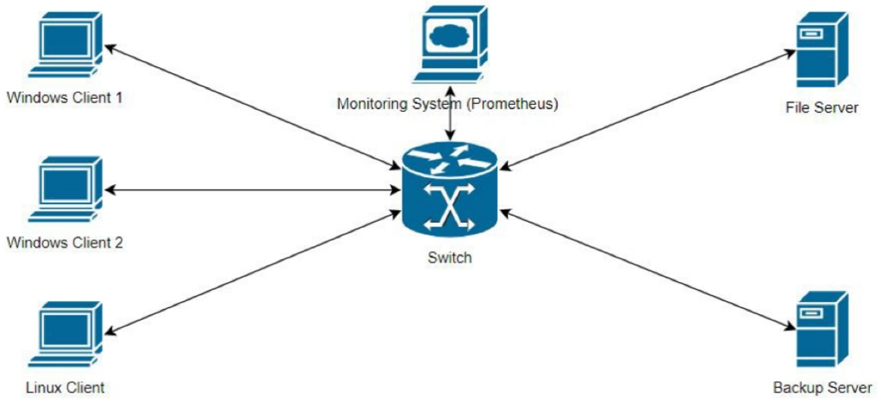

Figure 1: Structure of the scenario network.

Within the scenario, the attack with a ransomware is simulated. The ransomware used is Emotet (SophosLabs, 2023). Emotet primarily spreads via email attachments and then uses a variety of other techniques to reload further malware, cover its tracks and spread further.

The scenario begins in the middle of this attack. Participants receive image files from the three client machines and the file server. In addition, they receive the complete extract of log files taken from the monitoring system. As further information they receive statements of the "customer". The customer has stopped further network communication. This means that the images correspond to the current image of the computers and further infection during processing is excluded. Based on this information, the participants can find out what threat they are dealing with, how the malware spread and which systems are affected. The most important points are listed here:

- From the image of "Windows Client 1" it is possible to determine how the initial infection took place. Thor APT Scanner provides evidence of Emotet.
- Connections to Command & Control servers can be found in the log files, which are also indicative of Emotet. Emotet itself can reload various malware. The execution of the subsequent malware can also be found in the logs. The downstream malware in this case is a cryptominer, which uses the systems' computing time to mine cryptocurrencies.
- Emotet behaves like a worm and can spread independently in a network. The spread can also be traced using the images or the logs.
- Overall, all systems except "Windows Client 2" are affected.
- When restarting, make sure that no backups can be used because the backup server itself is also affected. Since there is no image for this, this information must be extracted from the log files.

Procedure from the point of view of the participants:

1. Getting to know CTFd: In this section, participants will first learn about the CTFd platform. The "Scoreboard" and "Challenges" sections will be highlighted. The Scoreboard gives participants an overview of their current score at any time. Under Challenges all tasks of the participants can be found.
2. Introduction of the case: The introduction to the case can also be found under Challenges. This is formulated from the customer's point of view and contains all the information needed for further investigations.
3. The individual tasks: Participants can then look at the individual tasks. These are formulated in such a way that they correspond to requests from the customer. This is to simulate cooperation with the customer. The faster and better the participants answer these questions the more points they receive. This corresponds to the satisfaction of the customer.
4. Prepare a final report: Once the case is solved and all questions are answered, a final report must be prepared. This report should contain a technical report and a summary for non-technicians. This report will be checked manually and will result in bonus points for the participants at the end.

CONCLUSION

This paper described how a possible training course for prospective digital forensic experts with focus on DFIR could look like. Since the course content is based on the results of expert interviews, a good introduction to DFIR is facilitated including technology but also other framework conditions such as time pressure or communication with the customer. In addition to learning theoretical knowledge of digital forensic topics with the help of Ilias, practical parts and gamification in the form of CTFs improve the participant's training motivation.

REFERENCES

Autopsy. (April 14, 2023) Autopsy Digital Forensics. url: https://www.autopsy.com/.

Brannan, G. D. Tenny, S. Brannan, J. M. Qualitative Study. (2017) Stat-Pearls Publishing LLC.

CTFd LLC. (April 14, 2023) CTFd. url: https://ctfd.io/.

Dewey, John. (1997). Experience And Education. Free Press. ISBN: 978-0-6848-3828-1.

EC Council. (April 14, 2023) Computer Hacking Forensic Investigator. URL: https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/.

EDX.org. (April 14, 2023) Edx.org. URL: https://www.edx.org/.

GFOCI - German Federal Office of Criminal Investigation. (2021). Cybercrime Bundeslagebild 2021 (transl. Cybercrime Situation Report 2021).

GrafanaLabs. (April 14, 2023) Grafana Loki. URL: https://grafana.com/oss/loki/.

Ilias.de. (April 14, 2023) Ilias - The open source learning management system. URL: https://www.ilias.de/.

Infosec Institute. (April 14, 2023) Infosec Institute - Learning Path Computer Forensics. URL: https://www.infosecinstitute.com/skills/learning-paths/computer-forensics.

Meyer, M. Aghamanoukjan, A. Buber, R. (2009) Qualitative Interviews. GWV Fachverlage GmbH. ISBN: 978-3-8349-0976-3.

Neo23x0. (April 14, 2023) Loki IOC and YARA Scanner. URL: https://github.com/Neo23x0/Loki.

NextronSystems. (April 14, 2023) Thor APT Scanner. URL: https://www.nextron-systems.com/thor/.

OffSec Services Limited. (April 14, 2023) Kali Linux. URL: https://www.kali.org/.

Open.edu. (April 14, 2023) open.edu. URL: https://www.open.edu/openlearn/.

SANS Institute. (April 14, 2023) Cybersecurity Courses Certifications. URL: https://www.sans.org/cyber-security-courses/?focus-area=digital-forensics&msc=main-nav.

SophosLabs Research Team. (2021) Emotet exposed: looking inside highly destructive malware. Network Security.

Udemy. (April 14, 2023) Udemy.com. URL: https://www.udemy.co/.

VirusTotal, (April 14, 2023) YARA. URL: https://github.com/VirusTotal/yara.