Preparation and Planning of the Development of a Proficiency Test in the Field of Digital Forensics

Damir Delija, Goran Sirovatka,Igor Spoljaric Sanja Krajinovic
TVZ, Zagreb, Croatia
MUP, Zagreb, Croatia
ddelija@tvz.hr, gsirovatka@tvz.hr ,ispoljaric@mup.hr, skrajinovic@mup.hr

Abstract **- This paper presents the planning and preparation of a proficiency test for the field of digital forensics. The paper provides an elaboration of the idea and procedure of creating a forensic experiment, the result of which will be a test of expertise applicable for various organizations engaged in digital forensics. The whole process of planning, selecting forensic tools, defining forensic procedures, and producing test forensic images is shown, explaining and elaborating the criteria used in the selection, and the expected results. The proficiency test is planned for a smart electric bicycle.**

Keywords - Proficiency testing, digital forensic

I. INTRODUCTION

The forensic laboratory and forensic experts have to undertake accreditation and certification as it is required in various laws and regulations. This is especially hard in the area of digital forensic where forensic tools are always steps behind the technology development, causing problems in practice, and requiring great personal skills, and expertise from the practitioners. As it is noted in the PCAST report of 2016 [3], there is a huge urgent need for reliable skills and methods: "…. there is an ongoing effort in digital forensics to develop methods and processes to deal with each new technology as a source of digital evidence. Studies are needed to establish the reliability and validity of these digital forensic methods and processes. DFRWS contributes to these ongoing efforts by attempting to address the needs of coming years, concentrating on new technology and refining existing digital forensic methods and processes."

Proficiency testing is a crucial part of the forensic accreditation process [1]. NIST defines proficiency testing as „Proficiency testing is the evaluation of practitioner performance against pre-established criteria. External proficiency testing may be used for inter-laboratory comparisons, while internal proficiency testing may be used for intra-laboratory comparisons." [2].

It is important to have a test that covers new technologies and devices. At the moment in digital forensics each year, a huge amount of new smart devices is introduced each of them being a new challenge for tools, procedures, and expertise. To address this issue, among other measures, it is essential to timely develop proficiency tests and distributed them among the forensic community. One of the main organizations for this role is "ENFSI – European Network of Forensic Science", whose mission is to improve knowledge and methods in the forensics, as it is stated in [4], "The purpose of ENFSI as a network of experts is to share knowledge, exchange experiences and come to mutual agreements in the field of forensic science." One of its key goals is to "encourage all ENFSI laboratories to comply with best practice and international standards for quality and competence assurance"

In the development of the new proficiency test various partners should be involved, TVZ, Greyp, and Forensic Laboratory Ivan Vucetic, where the forensic laboratory has the role of the integrator and the key forensic case validator.

II. PLAN

According to the International Organization for Accreditation bodies" Competence is the demonstrated ability to apply knowledge and skills and, where" [7] and we believe that multi-technology tests can help acquire competencies for rapidly growing technologies in the field of digital forensics. To create a new proficiency test it is essential to be familiar with the subject of the test, tools, and procedures to be used.

We will suggest a test for new device: "electric bicycle". As a new device is used as a base for the proficiency test some additional consideration should be taken. The initial process of device analyses should be done strictly in order with current existing forensic standard operating procedures (SOP), with support from the device vendor. In this case, the electric bicycle is not yet used for proficiency testing. A detailed understanding of how such devices work and how data is generated on them is required to produce reliable data for the proficiency test. Also, detailed insider knowledge of the device will provide expertise on how to customize future proficiency test images while keeping authenticity and reliability. There is no sense to have one proficiency test data set for all, it should be a set of tests, like in the academic exams. To generate required data, an approach similar to creating personalized forensic exam images can be used.

Data should be collected in a forensically sound way in post-test and pre-test environments, while the whole test should be done in a strictly controlled environment with calibrated and tested forensic tools.

In the current situation, data are stored on the electric bicycle, mobile devices connected with bicycles, and cloud storage of the bicycle producing company.

Forensic analyses of the vendor-specific cloud storage is a problem for the available digital forensic tools, exactly what happens in this work. Non-standardiesd vendor clouds, in the context of proficiency testing and defining standard operation procedures (SOP), are a serious challenge for digital forensics.

Data that will be used as the base for proficiency testing is based on a cycling trip. Such cycling trip should be also recorded with an independent tool and planned on the map to identify possible artifact which can be found in collected data, like geo-coordinates along the route, WIFI identificators, terrain features, which can influence the operating mode of the bicycle, and similar.

Data extraction should be done by existing standard operating procedures (SOP) while modifications of the SOP should be introduced after preliminary analyses of the devices if necessary. It is not expected to have a modification of the SOP since the bicycle is equipped with standard modules that can be forensically acquired with standard tools and procedures.

To create a useful proficiency test it is essential to see this effort as a project and as a process with well-defined goals and steps. The creation of the test requires compliance with regulations, but also test should be able to follow the development of the technology. If a new version of the device is released this process should be able to recreate a new version of the test by following already established steps

A. Planned Project phases

In the plan we defined 6 project phases:

- Creating and implementing scenarios
  - This phase is a critical one since it contains data creation and acquisition for the proficiency test, it covers data creating
- Making a forensic copy and distribution
  - In this step all data from involved devices and cloud storage are acquired, by SOP, preliminary data analyses should be done to validate if the scenario was successful. In this phase cooperation among all team members is crucial, especially during the first run. All steps need to be documented and verified to stay forensically correct.
- Collection of Results
  - Results of the data acquisition are collected, compared, documented, and analyzed. The analysis is done on the triage level to identify if there are some problems or corrupted data.
- Processing and evaluation of results
  - Forensic artifacts are identified and analyzed for their value in the proficiency testing, additional analyses are done by secondary tools, with double checks and controls with other team members to be sure that interpretations of the artifacts are corrected. Appropriate artifacts are identified as digital evidence which will be part of the proficiency test, with a detailed description of how this evidence was created and how it depends on the devices from which it was collected, its volatility attributes, and life span. Methods how to modify basic artifacts are also devised, to create unique variations of proficiency tests.
- Proficiency test creation and distribution
  - A proficiency test is created based on the results of the previous steps. All necessary documentation is created and verified. Proficiency tests are done with different tools to see feasibility and correctness. In this step students from TVZ will be used as beta testers. Quality control is done based on the forensic lab standards. The final version of proficiency tests is delivered to ENFSI for further actions and usage.

All activities should be done according to existing SOP and quality controls from the involved forensic

Figure 1. Greyp bicycle forensic image – WIFI connection artifacts

laboratory, all participants should be familiar with SOP and quality requirements to keep results sound. Everything should be done and documented as an ordinary digital forensic process, based on the currently accepted practices in the main forensic laboratory.

III. EXAMPLE: GREYP ELECTRIC BICYCLE

Greyp G6 is an innovative high-class electric mountain bicycle equipped with electronics and sensors and a Linux operating system. The Bicycle was provided by the kindness of the Greyp company, both with necessary technical expertise and knowledge. Details of the bicycle can be found on the vendors' web page www.greyp.com.

Important technical characteristics of the Greyp G6:

1. Front and rear camera 1080p@30fps
2. 4G modules eSIM, Bluetooth, WIFI, USB
3. GPS, 3-axles gyroscope, accelerometer
4. Embedded Linux File System (Ext4)
5. 2 GB RAM

Due to the connection between different technologies (mobile phone forensics, Cloud forensics, Linux forensics, live data forensics) Greyp G6 is a challenging choice for forensic analyses and designing related competency tests.

IV. PRELIMINARY RESULTS

In the current first phase of the project, in “Creating and implementing scenarios" some data is already collected, and the feasibility of the available forensic tools are tested on the data collected from Greyp bicycle.

Various data extracting methods were used to see which one can extract data best, the acquired data was triaged and previewed in FTK imager and EnCase v8, while data from the cloud and mobile devices were extracted later. Also detected artifacts were later confirmed in crosscheck with other forensic tools. The artifacts found were also discussed with technical personnel from Greyp, hardware and software developers, to see understand in detail how these artifacts are created and what changes are expected in their lifetime.

In figures 1 and 2, the Greyp bicycle file system image in raw forensic format (dd extraction) is seen through FTK imager. It presents Linux file systems with various possible artifacts for further analyses. More data is

Figure 2. Greyp bicycle forensic image – WIFI connection artifacts in unallocated space on the file system

available after full analyses in Encase v8. WIFI connection artifacts are identified in the normal place on the file system in figure 1 and the unallocated space figure 2. WIFI artifacts are valuable digital evidence and a very useful combination for the proficiency test questions. Unfortunately, Covid 19 pandemic restrictions reduced the number of free WIFI available on the cycling route.

Artifacts identified with FTK and Encase were confirmed with other forensic tools (X-Ways,UFED) in further analyses. This artifact was created when the device was connected to the WIFI through actions of network manager tool on Linux, later after disconnection from WIFI, connection data was erased and that action creates artifacts in the unallocated space (figure 2), found during forensic analyses, in the pattern searching step.

Such a scenario is a very convenient part of the proficiency test, for example, various questions about WIFI artifacts can be asked: which WIFI networks were

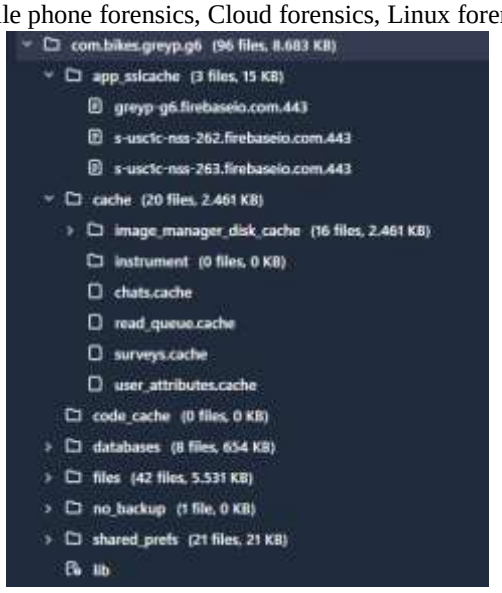

Figure 3. Greyp application SQLite database structure in Cellebrite's UFED Physical Analyzer

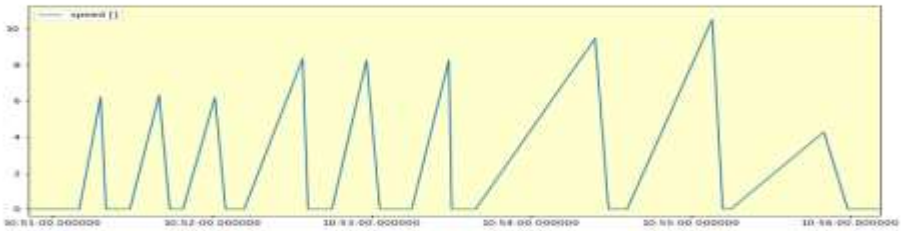

Figure 4. Greyp bicycle speed over time in milliseconds, data extracted and plotted from Greyp forensic image

counted, when, can this be confirmed with known WIFI position from the maps. Also, timeline issues and deeper analyses into erased data can be done to find out when WIFI data were erased since artifacts are found in the ext4 file system where it is highly possible to find inode related to erased data as it is presented in the various scenarios in" The Law Enforcement and Forensic Examiner's Introduction to Linux" [9].

RAM image acquisition was done by the Linux dd command. Comparing recordings (data) from the file system (/recordings) and RAM log files, identical data can be found, so it is possible to recover data and /or to confirm data from the file system. Later forensic images were triaged and preliminarily analyzed through Encase [5] and FTK imager [6], while other tools like Celebrite UFED [10] and Blacklight were used as back-office control.

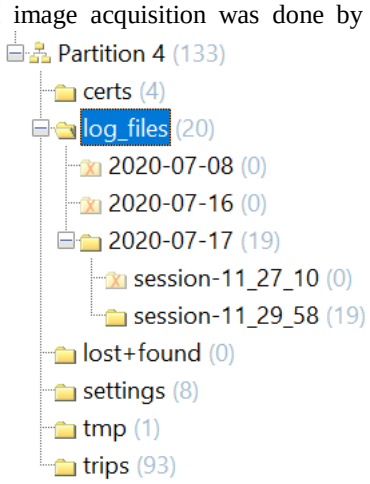

Figure 5. Structure of filesystem, view of log files in X-Ways forensics tool, from Greyp forensic image

The bicycle operating system stores data in the file system also sends some of the user data to a paired mobile phone (Android or iOS) and some of the data to the Cloud service. Data sent to a mobile device is stored in the Greyp application (com.Bicycles.greyp.G6), which contains records of submitted and received files over the mobile network. To get access to this artifact UFED tool from Celebrite was used, it SQL analyzer was used to verify Greyp SQLite database structure as can be seen in figure 3.

Important forensic artifacts are sent from the bicycle to the Cloud service. These data include GPS coordinate data, accelerometer data, bicycle speed, brake status, and gyroscope. To extract, analyze and plot this data tools in python 3.7 was used. The results of this extraction and graphing are presented in figure 4. This data can be used with additional processing to verify the cycling timeline.

V. CONCLUSION

At the moment the process is going slowly because of problems related to the covid19 pandemic. This cause some infrastructure issues, which prevented full analyses with a different tool, so the project is behind the expected schedule. Also, the lockdown of services like restaurants and cafés limited access to publicly accessible WIFI what the limited number of forensic artifacts in the collected images.

From preliminary results of analyses of first cycle trips, it is obvious there are enough digital artifacts that can be used for the planned proficiency test. These artifacts are compatible with various digital forensic tools like Cellebrite Physical Analyzer version 7.40, XWays Forensics 19.8, FTK, FTK imager EnCase v8.0, which were used for preliminary analysis and crosscheck of results. The ideas about Linux forensics presented in [9] in various Sleuth Kit Exercises are the perfect match for artifacts found in Greyp image, we strongly believe that

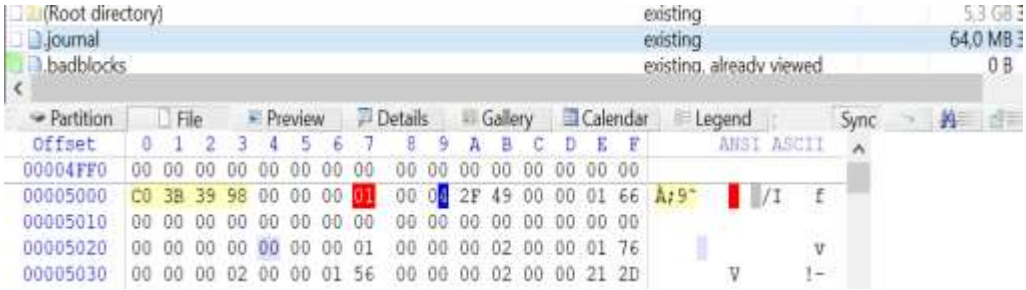

Figure 6. Hexadecimal view of a journal file for manual parsing ib X-ways tool, from Greyp forensic image

such tasks and procedures should be included in the future proficiency test. Stress on the command line Linux forensic skills as it is presented in [9] will be very useful to forensic practitioners in nearby future during complex forensic analyses of devices like Greyp bicycle, but not only for it but for all complex devices and IoT systems. On the conceptual level, forensic practitioners should be able to efficient forensic analyses of a system of devices, like Greyp, mobile devices and cloud is in this case, without a dedicated tool that hides all complexity from them.

The most important conclusion is a proficiency test is possible, fully based on data acquired, by available tools and procedures. In the preliminary examination, the test scenario was successfully reconstructed. Reconstructed data included various digital artifacts:

- user and bicycle communication,
- streaming video recordings of the bicycle camera via a mobile device,
- lap and speed of movement of the bicycle and
- brake status.

This artifact promises a very challenging test, all of the artifacts can be included in the future test data. Since these artifacts are from different areas of digital forensics, it provides multidisciplinary proficiency test covering :

- mobile forensics,
- SQLite database forensics,
- Android/iOS forensics,
- metadata forensics,
- 3rd party app forensics,
- Linux forensics (ext4 file system),
- Live data forensics (RAM images), and a
- Cloud forensics.

Procedures and procedures performed show that it is possible to develop a staged proficiency test. The implemented steps and procedures should be formalized as SOPs and the necessary critical evaluation should be carried out. The problems observed, especially always cloud, are potential limitations in protocol development and the following stages must develop the necessary tools and additional tests as needed [12], [13].

This model of proficiency test development creates the basis and model for proficiency test development for upcoming technology devices, which contributes to increasing the quality of digital forensics.

To fulfill the goal of a useful proficiency test ideas from “Digital Triage Forensics” [8] are crucial, since its present experience from modern real-life wartime scenarios. The proficiency testing is at the moment oriented to the laboratories but we believe that with the increase of live forensic because of intelligent systems proliferation proficiency testing should at least include some scenarios and skills related to such situations.

REFERENCES

[1] David Lilburn Watson, Andrew Jones: Digital Forensics Processing and Procedures, Syngress, August 2013, ISBN: 9781597497459

[2] Scientific Working Group Proficiency Testing, https://www.nist.gov/system/files/documents/2018/03/13/swganth_proficiency_testing.pdf, visited 16.1.2021

[3] PCAST Releases Report on Forensic Science in Criminal Courts, https://obamawhitehouse.archives.gov/blog/2016/09/20/pcast-releases-report-forensic-science-criminal-courts, visited 16.1.2021

[4] ENSFI, https://enfsi.eu/about-enfsi/, visited 16.1.2021

[5] EnCase® Forensic, The Gold Standard in Forensic Investigations – including Mobile Acquisition, https://security.opentext.com/encase-forensic, visited 16.1.2021

[6] FORENSIC TOOLKIT (FTK)® Dead-Box Forensics https://accessdata.com/products-services/forensic-toolkit-ftk, visited 16.1.2021

[7] ILAC G19:08/2014 Modules in a Forensic Science Process This document is intended to provide guidance for forensic science units involved in examination and testing in the forensic science process by providing application of ISO/IEC 17025 and ISO/IEC 17020.https://ilac.org/latest_ilac_news/ilac-g19082014-published/ visited 06.02.2021.

[8] S.Pearson, R.Watson: “Digital Triage Forensics”, Syngress, 2010, ISBN: 9781597495974, https://learning.oreilly.com/library/view/digital-triage-forensics/9781597495967/ visited 06.02.2021

[9] B.J.Grundy: “The Law Enforcement and Forensic Examiner’s Introduction to Linux”, 2020, https://www.linuxleo.com/Docs/LinuxLeo_4.94.pdf, visited 06.02.2021

[10] UFED The industry standard. Cellebrite's complete collection solution examines more types of devices and data to produce meaningful insights quickly, https://www.cellebrite.com/en/ufed-ultimate/, visited 06.02.2021

[11] X-ways Computer forensics software made in Germany, https://www.x-ways.net/,visited 06.02.2021

[12] Wilhelm Bauera, Sven Schulera, Tim Hornungb, Jacob Deckerc: Development of a Procedure Model for Human-Centered Industry 4.0 Projects – ScienceDirect, https://www.sciencedirect.com/science/article/pii/S235197892030473X, visited 06.02.2021

[13] David Lilburn Watson, Andrew Jones: Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements 1st Edition, ISBN-10: 9781597497428, Singress,2013