

How to do a forensic analysis of Android 11 artifacts

D.Delija, D.Sudec, G.Sirovatka and M.Žagar

Zagreb University of Applied Sciences (CROATIA)

dina.sudec@tvz.hr, ddelija@tvz.hr, gsirovatka@tvz.hr, mzagar@tvz.hr

Abstract - This paper compares the results obtained using several forensic tools on various Android 11 operating system devices. New and old functionalities of Android 11 store a vast volume of raw data and important forensic artifacts on mobile devices. The amount and type of data found on mobile devices demand further development of mobile forensics procedures. This development should be based on the streamlined procedures for the existing forensic to obtain more useful forensic artifacts. This means not using only one forensic tool, but combining results from multiple forensic tools in the analysis phase, after the data acquisition from Android 11 devices. The used forensic tools are Belkasoft Evidence Center X, Autopsy, and ALEAPP, with results presented and compared. The collected digital evidence shows the combined results are more substantial than the sum of particular ones

Keywords: mobile forensics, Android 11, forensic tools

I. INTRODUCTION

Looking from a digital forensic perspective introduction of mobile devices have completely changed the way of life because it provides opportunities to users equal that were exclusively related to personal computers [7], which makes mobile devices a new reach set of forensic artifacts instead of computers, with new caveats for same basic forensic artifacts [1],[2].

Given the various possibilities of using mobile devices, there are also cases when they are used for some illegal actions, which is why they initiate an investigation and seek digital evidence. There are various tools for forensic analysis of mobile devices which follow the digital forensic guidelines defined by ACPO [5]. The most well-known full-cycle tools that can be used to perform full forensic analysis are Cellebrite UFED, MSAB XRY, Paraben Mobile Field Kit [1],[3],[9]. Included in these tools are all the necessary auxiliary parts for various physical and logical extraction methods. There are also other well-known standalone tools are Oxygen, Magnet forensic, MOBILedit, Belkasoft, Lantern, Elcomsoft, GrayKey, and others [6],[2].

The current price is very high and ranges up to over \$ 10,000 with the annual license fee being about 30% of the price of the tool, making them difficult to access for the vast majority of forensic laboratories and academia. which is why most can only afford two or three.

Their capabilities vary depending on the complexity of use, the analysis capabilities they can perform, the format of the data they can process to the results they ultimately present. Due to all the above, the decision to choose a tool is not at all easy and simple. In addition to the fact that the appropriate data is needed to collect data for analysis, it is

even more important to choose the right tool that will be able to meet the requirements of each case. The market situation with a large number of different types and models of mobile devices and operating systems is a great challenge for forensic tool manufacturers who could perform a quality analysis of a mobile device and provide the necessary evidence. Manufacturers specializing in tool development for only one type of mobile device operating system is a necessary direction because, given the fundamental differences in file systems, it is difficult to produce tools that will be able to meet the analysis requirements of all existing operating systems [8],[9].

This paper aimed to analyze the Android 11 operating system using various commercial and open-source tools since the Android 11 was the most stable new version of the Android OS at the time of writing [10],[11],[12] with a detailed description of used encryption [13], [15]. The intention was to compare the quality of the results obtained. Choosing a tool is not an easy process. There are commercial tools on the market approved by courts and other government institutions whose results are accepted as credible. Such tools are expensive and only some offer trial versions lasting up to 30 days with some limitations, such as the limit of 50% of the data in the final report. There are also free open-source tools with fewer features. In part, this is understandable because it is unprofitable to develop a free tool that will do everything and requires significant resources.

Given the different capabilities of the tested tools and the results obtained are different. For some information and evidence, it was necessary to further research and look for details in both open source tools and commercial tools after the analysis. There is a significant difference in the tool that only performs triage, so in part, the results obtained cannot be compared with others that perform the entire analysis. For the same reason, it is not possible to compare the duration of the analysis.

Based on the results obtained, it can be concluded that it does not matter which tool will be used in forensic investigations. The obtained results are difficult to compare in most of the analyzed categories.

To further successfully develop mobile forensics, it is necessary to further develop tools that are so automated that they do not require additional analysis and research but provide results that will unquestionably answer fundamental questions about the user, contacts, messages, or communication. It is equally important that the tool be as complete as possible in the sense that it allows the collection and analysis of data, but also that the kit contains everything you need to process a case from start to finish.

Accessing mobile forensics in such a way that the tool is a box with all the necessary parts, such as various cables to connect the mobile device to the workstation, will speed up forensic analysis procedures and enable better results.

There are data collection tools on the market nowadays, analysis tools, and very few quality tools that support both functionalities. A unique tool that can collect and analyze is important for mobile forensics because with different tools we get different results, which is shown in this paper.

Obtaining different results is a reason to check using other tools so that the most important conclusions and facts can be further verified and confirmed. It is often the case that tools do not support some versions of applications or devices, so it is necessary to do the analysis manually by converting the extracted data into a readable format. Tools often have errors due to the complexity of their development, given a large number of manufacturers and models of mobile devices as well as operating systems tools have to support in analyses. The occurrence of errors in tools is another reason to check their functionality by checking the results obtained with another tool. The level of complexity of mobile forensics is increased by the occurrence of cases of organized crime investigation involving a large number of mobile devices that need to be legally, qualitatively, and accurately analyzed, which is impossible to do in the desired and necessary short time.

There are specialized tools on the market that, in addition to data collection and analysis options, have the option of accessing encrypted and inaccessible data, legally. The world's leading recognized tool for such extraction on devices running the iOS operating system is Greykey, manufactured in the United States and recognized and used in over 1000 agencies in 30 countries. In February this year, Greykey unveiled the ability to extract data from encrypted and locked leading mobile devices, the Samsung S20 and S9 powered by the Android operating system. In addition to Greykey, the world-renowned Cellebrite Premium, which supports legally based full file system data extraction on any iOS device and also physical and full file system extraction of encrypted files on a large number of advanced devices running Android, is appreciated.

Given the above, it is reasonable to expect the development of tools in the future that will be able to fully meet the challenges of mobile forensics in terms of the legal basis, speed, reliability, and comprehensiveness of extracted data and the quality of forensic analysis results.

II. FORENSIC TOOLS USED

Belkasoft Evidence Center X

Belkasoft Evidence Center X is a commercial forensic tool from Belkasoft [16]. The trial version of the tool lasts 28 days, is available on the official website, and is available via a link that comes via email after check-in.

The tool interface is easy to use. It is possible to start working immediately after installation. There are options for collecting, analyzing, and presenting digital evidence from computers, mobile devices, and cloud services. In the case of buying a tool, a portable version of the Belkasoft Evidence Reader tool is available for free. It is related to „reader“ variants of forensic tools, which have only search, bookmark, and report options.

The main actions are automated and after giving the basic parameters for processing evidence, the Belkasoft Evidence Center X can work unattended. The useful feature is for each basic task, the tasks tab records the time and duration of the task execution.

The tool supports all the most operating systems for desktops and mobile devices. It can acquire the forensic images of physical drives and logical volumes, virtual machines, data backups from mobile devices images obtained by the main forensic tools for mobile forensics, JTAG, and chip-off acquired data. Is fully automated and searches the entire device itself and can successfully identify thousands of types of digital artifacts. There are filters and predefined search capabilities, which can speed up forensic analysis. It is possible to restore corrupted and incomplete SQLite databases, deleted records, and deleted history files.

By using the File System Hex Viewer, and Type Converter tools Belkasoft Evidence Center X allows the analyst to drill down on the contents of files and folders. With the help of customizable functions, it is possible to recover deleted and hidden artifacts and analyze memory processes.

The report can be created in several formats such as text, HTML, XML, CSV, PDF, RTF, Excel, Word, EML, KML.[16].

A. Autopsy

The Autopsy is a free open source forensic tool, a complete platform for forensic analysis of digital media and mobile devices [17]. The Autopsy tool was originally developed as a graphical interface for Linux Sleuth Kit. Since version 3 is a tool that can be installed and used independently on Windows operating systems too. The tool is fast and easy to use and can expand and upgrade using existing modules developed by other users.

The main features of the Autopsy are comparable with commercial tools. There are simple installation on the Windows operating system, automated workflow from data loading to analysis, analysis of hard drives and smartphones, indexed search, extracting data from web browsers and images, finding deleted artifacts. The advanced feature supports the multi-user work, which allows multiple forensics analysts to collaborate on one case. This method of cooperative working can speed up analysis and the generation of the final report, but such work requires processing power and storage space [25].

B. ALEAPP

ALEAPP is a free open-source tool, a part of the project by Alexis Brignoni [18]. The author emphasizes that the project is the property of the forensic community, which makes it available for development, testing, and use. The project consists of tools for triage of Android, iOS, and macOS (Macintosh Operating System) operating systems.

A distinctive feature of the tool is speed. In a very short time, it can perform triage of the Android operating system. ALEAPP is based on python programming language, it supports triage of forensic image format *.zip, *.tar and logical extraction formats.

The purpose of ALEAPP is a triage tool in forensic laboratories. Used as an auxiliary tool for forensic investigators when commercial tools are unavailable or when it is a surging situation during a mass investigation. Its additional purpose is to be a framework for independent testing and evaluation of tools.

The ALEAPP tool is available on the project's Github page [26]. The project consists of several versions or special tools:

- ALEAPP - Event records and Protobuf parsing for Android devices;
- ILEAPP - Event records and runway parsing for iOS devices;
- UIDAS - Compare the contents of two text files Android-UsageStats-XML-Protobuf - Usage Status and Protobuf Parse;
- iOS-Mobile-Installation-Logs-Parser - parsing iOS installation on a mobile device;
- DFIR-SQL-Query-Repo - A collection of SQL queries as templates for digital forensics.

It is possible to do triage for one option at a time. Generally, there is the possibility of selecting information about user profile, application usage, call logs, chat communication, internet browser usage, device information, media file metadata, text messages, and Wi-fi profiles. After the options are selected, triage is started, its progress can be traced. After the triage process is completed, the tool itself opens the report in HTML format and stops.

III. OVERVIEW OF ANALYSIS RESULTS AND TOOL COMPARISON

Generally, each tool has certain pros and cons for itself. Comparing different tools is not easy for many reasons. It is necessary to observe their possibilities but also the final results to get some more detailed insight. Since Belkasoft Belkasoft Evidence Center X, Autopsy, and Aleapp are different tools used for a common task, a set of attributes is used for comparison. These attributes are based on main forensic tasks and the feature sets of used tools. Choice of the attributes are based on the experience and most common tasks in the forensic analyses of mobile devices, this attribute are:

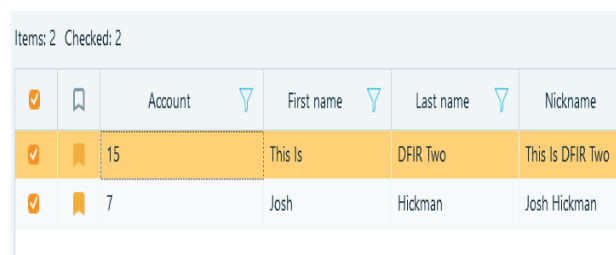
1. Tool complexity – present how complex this tool is for the user;
2. Multiuser work- if the tool can be used in multiuser mode;
3. Main functions – main forensic tasks it tool can do;
4. Area of Analysis – which forensic device areas it can analyze;
5. Duration of analysis- how long it takes;
6. Results- what kind of artifacts is found;
7. Contacts – number and quality of contacts discovered;

8. Call logs - number and quality of call logs;
9. Applications - number and quality of application;
10. SMS - number and quality of messages;
11. Photos were taken with the device's camera - number of photos;
12. Artifacts found – total number of found artifacts;
13. Making a bookmark – if a tool can create bookmarks for discovered artifacts;
14. Final reports – if reports are predefined or can be tailored.

Important artifacts in forensic analyses of the mobile device are user profiles, applications, SIM cards info, messages, photos, multimedia, call logs, application metadata, etc. The importance of artifacts is based on the Crime type/digital evidence comparison presented in the „Electronic Crime Scene Investigation: A Guide for First Responders 2nd edition“ [19]. Relevance of artifacts is based on how these artifacts present usage of mobile devices, especially in communication among users, the timeline of activities, geographical locations, and the most important ownership information.

The findings and specific findings for each forensic tool are presented. Differences are big and only proper cooperation and verifying results can provide correct results from findings.

Figure 1 shows two profiles found with the Belkasoft Evidence Center Xtool. Profiles are easy to find because the tool classifies them as profiles that exist on the device. The Autopsy tool has found a total of 16 profiles from various applications, but without reviewing the system files it is not possible to determine what the device profile is related to. The ALEAPP tool found only one profile, one that is related to a SIM card.



Account	First name	Last name	Nickname
15	This Is	DFIR Two	This Is DFIR Two
7	Josh	Hickman	Josh Hickman

Figure 1. Profiles found with Belkasoft, source: screen image from author's analyses

7

Figure 2 shows the basic profile data and serial numbers found by viewing system files obtained by Belkasoft Evidence Center X . Same can also be found by the Autopsy. The ALEAPP tool has just found one profile, this is DFIR two with the associated email address.

	profil 7	profil 15
Ime	Josh	This Is
Prezime	Hickman	DFIR Two
MSSISDN	+19195794674	
IMSI	310260976111372	
ICC-ID	89011203004067132462	

Figure 2. User profiles and serial numbers found, the language used was Croatian so screenshot has Ime for first name and prezime for the last name, source: authors work

1) Check by SIM serial numbers found

All tools provide the same SIM data, which is correct. By verifying the ICC-ID number 89011203004067132462, it was found that the SIM card is used on the territory of Canada and the United States.

By checking the IMSI number 310260976111372 found that the number is used in the United States, the network operator is T-Mobile USA, Inc. The mobile network is T-Mobile USA and the status on the network is "active". The same can be verified by checking the numbers 310 and 260 for which the result is T-Mobile, USA since IMSI is composed of MCC (Mobile Country Code) and MNC (Mobile Network Code) numbers. The rest of the numbers 976111372 indicate the unique number of MSIN (Mobile Subscriber Identity Number) subscribers.

By checking the MSISDN number +19195794674, it was found that this number of the mobile device used in the United States, in the city of Sanford, NC, and the provider is Suncom DbA T-mobile USA.

2) Applications on mobile devices:

On the device, the Belkasoft Evidence Center X tool found a total of 200 installed applications, Autopsy 230 and ALEAPP 165.

Belkasoft Evidence Center X can easily determine that 174 apps have been installed on the „This Is DFIR Two“ profile, of which 25 are for chat and secure communication and 10 are for tracking health data from a smartwatch, while 26 chat apps are installed on the „Josh Hickman“ profile. This cannot be easily determined in the other two tools without reviewing and analyzing the system files.

3) Messages

View messages and easily filter in Belkasoft Evidence Center X. tool found the user achieved communication using several different secure communication applications such as Telegram, Signal, Skout, Text now, Silent phone, Viber Messenger, Wire, Signal private messenger, Imo, Kik, and Line.

With the Autopsy tool, it is possible to determine the message total number by simply viewing all installed applications, but it is not possible to determine communication details without viewing deeper into system files.

The ALEAPP tool displays data on the applications used by classifying them as device applications and manufacturer applications, which means that these are not standard applications on the device but were subsequently installed. ALEAPP found 27 SMS messages, but their content is not visible which is a drawback. In the other two tools, it is possible to immediately see the content of messages, and more important more messages were found, Belkasoft Evidence Center X found 58 and Autopsy 54.

4) Images found on the mobile device

Belkasoft Evidence Center X found 7244 images that were mostly exchanged in chat and SMS communication. The Autopsy found 7592 images and ALEAPP does not search for images.

5) Photos were taken by mobile device

Belkasoft Evidence Center X found three photos taken with the mobile device camera with geolocation data. Also, it is possible to find the place where they were photographed. The Autopsy tool found 2 photos with geolocation data and ALEAPP has no that option.

6) Comparison of the forensic tools

The Belkasoft Evidence Center X tool is a complete forensic software solution because it can extract data and analyze data from computers, mobile devices, RAM, and cloud services. The format of the data analyzed is not as important as it would be limiting as it is with some other commercial tools that analyze only the data collected with those tools. As restrictive as that may be, it is understandable if we look at it from the position of a tool manufacturer that guarantees quality if it has control over all the processes and actions that precede it. The tool is designed for use for one user and does not allow you to work in a team. About the other two tools, the results of the analysis are presented by the tool in a visually interesting and practical way. Some results do not require additional analysis of system files, but it is enough to make simple filtering. As for system files, when the desired photo is found in the result, for example, it is easy to position yourself on the folder of the original directory and copy the file directly from the tool to some desired location, which is very convenient. The tool allows you to create your tags, as well as mark one artifact with multiple different tags, which is convenient if we want to see for example how many applications there are and which of these applications are installed on a particular profile in this case. Image file analysis with all selected search options took 2 hours and 27 minutes.

Figure 3 shows the result of the search by the results of the calls logs, which shows that the tool for some reason displayed the same call as a result 42 times, which indicates the need for additional research, ie after analysis, it is not possible to conclude from the results that so many calls. This is not the case with the other two tools.

Items: 584 Checked: 42

	Dir...	Caller	Callee	Time (UTC)	Duration
<input checked="" type="checkbox"/>	Incoming	1364243771	858233690	22.9.2020, 23:14:44	90
<input checked="" type="checkbox"/>	Incoming	1364243771	858233690	22.9.2020, 23:14:44	90
<input checked="" type="checkbox"/>	Incoming	1364243771	858233690	22.9.2020, 23:14:44	90
<input checked="" type="checkbox"/>	Incoming	1364243771	858233690	22.9.2020, 23:14:44	90
<input checked="" type="checkbox"/>	Incoming	1364243771	858233690	22.9.2020, 23:14:44	90
<input checked="" type="checkbox"/>	Incoming	1364243771	858233690	22.9.2020, 23:14:44	90
<input checked="" type="checkbox"/>	Incoming	1364243771	858233690	22.9.2020, 23:14:44	90

Figure 3 View duplicate results for a single call I Balkasoft tool, source: screen image from author's computer screen

The Autopsy tool is free and supports the possibility of a team of forensic scientists working on one case. It can analyze data from computers, mobile devices, and RAM. Visually, the tool is not complicated, it is easy to use but the results obtained by analysis regardless of what is presented by certain default categories require additional searches and additional work. Image analysis with all selected search options took 3 hours and 43 minutes.

The ALEAPP tool is free and searches for very little data compared to the other two tools but is characterized by the simplicity of the interface, and the speed of the analysis. This is done on purpose since the tool is not used for classical forensic analysis but triage in cases where some important data needs to be quickly obtained or if other commercial tools are not available. It is easy to use and fast get reports after the analysis is performed. In this paper, ALEAPP was used only for the analysis of Android operating systems. The analysis with all possible options took just under 4 minutes.

Table 1: Side-by-side view of results comparative results of analyses using the tools described; source: author's work

	Belkasoft Evidence Center X	Autopsy 4.13.0	ALEAP version L3
Tool complexity	complex, easy to use	complex, easy to use	extremely simple, easy to use
Multiusers work	single-user	multi-user	single-user
Main functions	collection, analysis, presentation	collection, analysis, presentation	triage, presentation
Area of Analysis	computers, mobile devices, ram, cloud services	computers, mobile devices, ram,	andriod mobile devices
Duration of analysis:	2:00:27	3:20:25	0:03:59
Results	phonebook, calls, messages, communication	phonebook, calls, messages, communication	calls, messages, communication
Contacts	751	108	15 (just calls)

	(all contacts from all applications)	(all contacts from all applications)	
Call logs	584 (a large number of duplicate calls)	30	15
Applications	200	330	265
SMS	58	54	27
Photos were taken with the device's camera	3	2	0
Artifacts found	22,409	9370	17.434
Making a bookmark	yes	yes	yes
Final reports	possibility of choice	predefined depends on the chosen type of analyses	predefined depends on the chosen type of analyses

IV. CONCLUSION

The conclusion of this paper is the importance of using more forensic tools in preplanned and organized order during the investigation. It was shown that results from different tools can be combined and manually verified to get the quality and reliability of forensic extracted data.

The comparison of collected digital evidence shows the combined results are more substantial than the sum of particular ones.

The results obtained using several forensic tools Android 11 operating system devices depend on the tool used, as is shown in Table 1. New and old functionalities of Andriod 11 store a vast volume of raw data and important forensic artifacts on mobile devices which can be easily lost or duplicated because of tools features. The amount and type of data found on mobile devices demand further development of mobile forensics procedures [8].

This development should be based on the streamlined Stanard operating procedures [14] for the existing forensic to obtain more useful artifacts but based on parallel use of more than one tool. This means not relying only on one forensic tool, but combining results from multiple forensic tools in the analysis phase, after the data acquisition from Android 11 devices.

The used forensic tools can vary but it is important to have an understanding of each tool's advantages and cons both with understanding the purpose of the tool and its position in the forensic process that was shown in this paper.

The choice of the tool and order of usage depends on the goal of the investigation and the expected artifacts which are relevant for the investigation.

REFERENCES

- [1] Sammons, J. „The basics of digital forensics: the primer for getting started in digital forensics“. Syngress, Elsevier Inc. ISBN 978-0-12-801892-7 Available on the network at: <https://learning.oreilly.com/library/view/the-basics-of/9780128016350/>, accessed 13.06.2021.
- [2] Wikipedia, „Mobile device forensics“, Available on the network at: https://en.wikipedia.org/wiki/Mobile_device_forensics, accessed 13.06.2021.
- [3] Ayers, R., Brothers, S., Jansen, W., „Guidelines on Mobile Forensic“, NIST Special Publication 800-101 Revision 1 pdf, Available on the network at: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-101r1.pdf>, accessed 13.06.2021.
- [4] Skulkin, O., Tindall, D., Tamma, R., „Learning Android Forensics, Second Edition, Analyze Android devices with the latest forensic tools and techniques“, Packt Publishing Ltd., ISBN 978-1-78913-101-7, Available on the network at: <https://learning.oreilly.com/library/view/learning-android-forensics/9781789131017/5aca5a5c-e415-4f20-96ee-16d92a884f8a.xhtml>, accessed 15.06.2021.
- [5] Digital Detective, „ACPO Good Practice Guide for Digital Evidence“ pdf, Available on the network at: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf, accessed 17.06.2021.
- [6] Eforensics Magazine, „Introduction to mobile forensic“, <https://eforensicsmag.com/introduction-to-mobile-forensics/>, accessed 15.06.2021.
- [7] Statista, „Digital 2020. Global Digital Overview“, <https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/>, accessed 17.06.2021.
- [8] Reiber, L. 2016) „Mobile Forensics Investigations A Guide to Evidence Collection, Analysis and Presentation“. McGraw-Hill Education. ISBN: 978-0-07-184364-5. Available on the network ., <https://learning.oreilly.com/library/view/mobile-forensic-investigations/9780071843645/>, accessed 17.06.2021.
- [9] Bomisetty, S., Tamma, R., Mahalik, H. 2014. „Practical mobile forensic“, Packt Publishing Ltd. ISBN 978-1-78328-831-1 pdf, Available on the network. <https://pre-uneplive.unep.org/redesign/media/assets/images/Practical%20Mobile%20Forensics.pdf>, accessed 17.06.2021.
- [10] End of life, „Android OS Version History“, Available on the network at: <https://endoflife.date/android>, accessed 19.06.2021.
- [11] Social compare, „Android platform“, Available on the network at: <https://socialcompare.com/en/comparison/android-versions-comparison>, accessed 19.06.2021.
- [12] Statista, „Android operating system share worldwide by OS version from 2013 to 2020“, Available on the network at: <https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/>, accessed 19.06.2021.
- [13] Guiding tech, „What is encryption on Android and how to enable it“, Available on the network at: <https://www.guidingtech.com/34481/android-encryption/>, accessed 22.06.2021.
- [14] Lilburn Watson, D., Jones, A. 2013. „Digital Forensics Processing and Procedures“, Syngress. ISBN: 978-1-59749-745-9, Available on the network Dostupno na: <https://learning.oreilly.com/library/view/digital-forensics-processing/9781597497428/>, accessed 22.06.2021.
- [15] Android central, „Android 11 review: Conversation starter“, Available on the network at: <https://www.androidcentral.com/android-11-review>, accessed 16.06.2021.
- [16] Belkasoft made easier, „Belkasoft Evidence Center X“, Available on the network at: <https://belkasoft.com/x>, accessed 13.06.2021.
- [17] Autopsy Digital Forensic, „Download datasheet“, Available on the network at: <https://s3.amazonaws.com/resources.Autopsy.com/datasheets/Autopsy-EN.pdf>, accessed 18.06.2021.
- [18] Github, "Brigs Abrignoni", Online, Available at: <https://github.com/abrignoni>, accessed 24.06.2021.
- [19] Technical Working Group for Electronic Crime Scene Investigation „Electronic Crime Scene Investigation: A Guide for First Responders 2nd edition“, US Dep. Of Justice, 2008, Available at <https://www.ojp.gov/pdffiles1/nij/219941.pdf>