INTERNATIONAL SCIENTIFIC CONFERENCE “ARCHIBALD REISS DAYS”
THEMATIC CONFERENCE PROCEEDINGS OF INTERNATIONAL SIGNIFICANCE

INTERNATIONAL SCIENTIFIC CONFERENCE

"ARCHIBALD REISS DAYS"

Belgrade, 2-3 October 2018

THEMATIC CONFERENCE PROCEEDINGS OF INTERNATIONAL SIGNIFICANCE

VOLUME II

Academy of Criminalistic and Police Studies
Belgrade, 2018

Publisher
ACADEMY OF CRIMINALISTIC AND POLICE STUDIES
Belgrade, 196 Cara Dušana Street (Zemun)

Computer Design
JOVAN PAVLOVIĆ
DRAGOLJUB MILUTINOVIĆ

Impression
200 copies

Print
Službeni glasnik, Belgrade

THE CONFERENCE AND THE PUBLISHING OF PROCEEDINGS WERE SUPPORTED BY THE MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGICAL DEVELOPMENT OF THE REPUBLIC OF SERBIA

ISBN 978-86-7020-405-8
ISBN 978-86-7020-190-3

HONORARY COMMITTEE

Goran Bošković, PhD, Academy of Criminalistic and Police Studies, Belgrade, **President**
Sima Avramović, LLD, Dean of the Faculty of Law, Belgrade
Ivica Radović, PhD, Dean of the Faculty of Security, Belgrade
Major-General Mladen Vuruna, PhD, Rector of the University of Defence, Belgrade
Branislav Đorđević, PhD, Director of the Institute of International Politics and Economics, Belgrade

International members

Olivier Ribaux, PhD, Director of the School of Criminal Justice, University of Laussane, Switzerland
Norbert Leitner, PhD, President of the Association of European Police Colleges,
Director of SIAK, Vienna, Austria
General Cao Shiquan, PhD, President of the Chinese National Police University,
Beijing, People's Republic of China
Hao Hongkui, PhD, President of the Criminal Investigation Police University of China,
Shenyang, People's Republic of China
Major-General Andrey Kochin, PhD, Acting Head of the St. Petersburg University
of the Ministry of Internal Affairs of the Russian Federation
Major-General Vladimir Tretyakov, PhD, Chief of the Volgograd Academy
of the Ministry of Internal Affairs of the Russian Federation
Police Colonel Roman Blaguta, PhD, Rector of the Lviv State University of Internal Affairs, Ukraine
Major-general Vladimir Bachila, PhD, Head of the Academy of the Interior Ministry of the Republic of Belarus
José García Molina, PhD, Director of Spanish Police Academy, Ávila
Police Colonel Marek Fałdowski, PhD, Commandant-Rector of Police Academy, Szczytno, Poland
Lucia Kurilovská, PhD, Rector of the Academy of the Police Force, Bratislava, Slovakia
Major-General Panagiotis Kordolaimis, Commander of the Hellenic Police Academy, Athens, Greece
Yilmaz Çolak, PhD, President of the Turkish National Police Academy, Ankara
Adrian Iacob, PhD, Rector of the Police Academy "Alexandru Ioan Cuza", Bucharest, Romania
Simion Carp, PhD, Rector of the Academy "Ştefan cel Mare",
Ministry of the Interior of the Republic of Moldova, Kishinev
Zoltán Rajnai, PhD, Dean of the Donát Bánki Faculty of Mechanical and Safety Engineering,
Óbuda University, Hungary
Andrej Sotlar, PhD, Dean of the Faculty of Criminal Justice and Security, Ljubljana, Slovenia
Nikola Dujovski, PhD, Dean of Faculty of Security, Skopje, Macedonia
Predrag Ćeranić, PhD, Dean of the Faculty of Security Science, University of Banja Luka, BiH
Nedžad Korajlić, PhD, Dean of the Faculty for Criminal Justice, Criminology and Security Studies,
University of Sarajevo, BiH
Velimir Rakočević, PhD, Dean of the Faculty of Law, Podgorica, Montenegro
Boban Saranović, Director of Police Academy, Danilovgrad, Montenegro

PROGRAMME COMMITTEE

Biljana Simeunović-Patić, PhD, UCIPS, Belgrade, **President**
Aleksey Bashan, PhD, Academy of MoI of Belarus
Andy Bécue, PhD, University of Lausanne, Switzerland
Jay Dawes, PhD, University of Colorado, Colorado Springs, USA
Gorazd Meško, PhD, Faculty of Criminal Justice and Security, Ljubljana,
University of Maribor, Slovenia
Jozef Meteňko, PhD, Academy of Police Force, Bratislava, Slovakia
Imre Rudas, PhD, Obuda University, Budapest, Hungary
Slobodan Simonović, PhD, Western University, London, Canada
David D. Stephens, M.S., Forensic Science Consultants, Inc., USA
John Winterdyk, PhD, Mount Royal University, Calgary, Canada
Đorđe Đorđević, PhD, UCIPS, Belgrade
Zoran Đurđević, PhD, UCIPS, Belgrade
Stevo Jaćimovski, PhD, UCIPS, Belgrade
Saša Mijalković, PhD, UCIPS, Belgrade
Dragan Mlađan, PhD, UCIPS, Belgrade
Obrad Stevanović, PhD, UCIPS, Belgrade
Dane Subošić, PhD, UCIPS, Belgrade
Slaviša Vuković, PhD, UCIPS, Belgrade
Petar Čisar, PhD, UCIPS, Belgrade
Smilja Teodorović, PhD, UCIPS, Belgrade
Jelena Radović-Stojanović, PhD, UCIPS, Belgrade
Dragoslava Mićović, PhD, UCIPS, Belgrade

ORGANIZING COMMITTEE

Darko Simović, PhD, UCIPS, Belgrade, **President**
Saša Milojević, PhD, UCIPS, Belgrade
Aleksandar Bošković, PhD, UCIPS, Belgrade
Valentina Baić, PhD, UCIPS, Belgrade
Nenad Koropanovski, PhD, UCIPS, Belgrade
Aleksandra Ljuština, PhD, UCIPS, Belgrade
Nikola Milašinović, PhD, UCIPS, Belgrade
Brankica Popović, PhD, UCIPS, Belgrade

TABLE OF CONTENTS

TOPIC III
Police organization – structure,
Functioning and human resources

TOPIC IV
Contemporary security challenges

TOPIC V
Cyber crimes and it security

TOPIC VI
Innovative methods in forensic science

COMPREHENSIVE FORENSIC EXAMINATION WITH BELKASOFT EVIDENCE CENTER

Brankica Popović, PhD[1]
Kristijan Kuk, PhD
University of Criminal Investigation and Police Studies, Belgrade

Ana Kovačević
Faculty of Security Studies, University of Belgrade, Serbia

Abstract: The enhancement and proliferation of information and communication technology (ICT) has tackled every aspect of human activity: work, leisure, sport, communication, medicine, etc. All around us we can see mobile phones and other connected devices that are now ubiquitous, changing trends in consumer behaviour. Therefore, there is no surprise in fact that such technologies can play a significant role in committing or assisting a crime, since data held on digital devices can give a detailed insight into people's lives, communications, contacts, friends, family and acquaintances. In order to help law enforcement investigation of such crimes, digital forensic is performed with the aim of collecting crime-related evidence from various digital media and analyse it. Investigators use various forensic techniques to search hidden folders, retrieve deleted data, decrypt the data or restore damaged files, etc. Obtaining evidence such as location data, photos, messages or internet searches can be beneficial, if not crucial, in assisting the police with criminal investigations. Since advances in technologies have led to an increase in the volume, variety, velocity, and veracity of data available for digital forensic analysis, without efficient techniques and tools such investigation would require a tremendous amount of effort and time. That is the reason for expansion in the market of digital forensic tools, both proprietary and free for use, that are available today. In this paper an insight of digital forensic process is given, emphasizing the role of digital forensic tools in providing digital evidence. The possibility of one particular tool, Belkasoft Evidence Center – BEC, in acquisition and analysis of digital evidence was briefly described.

Keywords: cybercrime**,** digital evidence, digital forensic tools, memory forensic tools

INTRODUCTION

Modern societies are increasingly dependent on electronic networks and information systems. The evolution and proliferation of information-communication technology (ICT) and rapid integration of the Internet in almost all aspects of human activity, although having large beneficial effect, have also increased vulnerability of modern society through introduction of

1 Corresponding author mail: brankica.popovic@kpa.edu.rs

novel types of criminal activity – cybercrime. Many Internet dependent services are frequent targets of cyber-attacks making a cybercrime often a part of our real life experience.

Since majority of information is created, modified and consumed entirely in digital form,[2] it is of most importance for any investigation to be able to get access to them in order to perform analysis and provide digital evidence to the court. Considering the amount of data that have to be processed, it is clear that some automatic tools have to be used in order to provide information (digital evidence) in efficient and timely manner.

Today we have a variety of available tools that can be used in process of gathering (acquisition and analysis) of digital evidence, both proprietary and free for use. There is not a single tool that can serve for all purposes, but there are some solutions and integrated tools that can make the difference in digital investigation process, and which are recognized by the expert (both forensic and legal) as efficient and trustworthy. Among them there is the solution provided by Belkasoft, named Belkasoft Evidence Center (BEC).

The aim of this is paper is to describe the possibilities of automatic forensic tools that can be used to facilitate cybercrime investigation, with focus on Belkasoft tool – BEC. The paper is organized as follows: in the first section there is a brief introduction to the concept of cybercrime, digital evidence and digital forensic; in the second section a role of digital forensic in fighting cybercrime is briefly explained, followed by the section stating the most popular digital forensic tools. The fourth section is dedicated to the explanation of possibilities that BEC can provide in digital forensic process. Finally, after the brief conclusion the list of used references is provided at the end of the paper.

BASIC FACTS ABOUT CYBERCRIME, DIGITAL EVIDENCE AND DIGITAL FORENSIC PROCESS

What is cybercrime?

Cybercrime, alternatively referred to as computer crime, e-crime, electronic crime, or high-tech crime was firstly considered as a crime that involves a computer and networks, where computer may be the target or the tool for committing a crime. In the preamble of the Convention on Cybercrime[3] of the Council of Europe, cybercrime is defined as "activities that are directed against the integrity, confidentiality and availability of computer systems and data networks, as well as any misuse of these system, networks and computer data" (CETS 185, 2001).

Later in 2007, the EU Commission's communication defined cybercrime as: "criminal acts committed using electronic communications networks and information systems or against such networks and systems" (COM/2007/0267 final, 2007). In this definition two broad categories of crime are covered:

1. Crimes specific to the Internet, such as attacks against information systems, denial of service and hacking;[4] and

2. 'Internet facilitated' crimes (or computer assisted crimes) – crimes where computers are used in an online environment as tools to commit more traditional crimes (e.g. online fraud and forgery,[5] the dissemination of illegal content such as child sexual abuse

2 Some activities such as chats and social networking are even unimaginable outside the virtual space
3 Also known as the "Budapest Convention"
4 Can also be directed against the crucial critical infrastructures
5 Through instruments such as identity theft, phishing, spam and malicious code

material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia).[6]

What is digital evidence and digital forensics?

With the digital revolution and expansion of electronic devices daily usage in almost all aspects of life it became clear that digital data found within them (especially within ones with electronic storage capacity) can supply vital evidence to investigators. That is the reason why in the Version 5 of the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence (ACPO, 2012) term 'computer based evidence' was replaced with 'digital evidence', reflecting the development of investigating information security incidents in a wider context. Today terms 'digital evidence' and 'electronic evidence' are used as synonyms referring to 'various types of data in electronic form that are relevant in investigating and prosecuting criminal offences - including 'content data' such as e-mails, text messages, photographs and videos - often stored on the servers of online service providers, as well as other categories of data, such as subscriber data or traffic information regarding an online account. These types of data are often essential in criminal investigations to identify a person or to obtain information about their activities' (MEMO/18/3345, 2015). We can say that digital evidence is now present or potentially present in almost every crime.

Digital evidence, like any other evidence, must be: admissible, authentic, accurate, complete and convincing to juries. Yet, digital evidence differs from other evidence in a way that it might be invisible to the untrained eye[7] and can easily be altered during evidence collection. Therefore, in order to be admissible in a court of law, it must be handled with a proper care meaning that seizure, custody, control, transfer, analysis and disposition of the evidence must be chronologically documented in a proper way constituting a 'Chain of custody' (CoC).

Digital evidence is highly volatile so an imperative is to preserve it as soon as possible. Since it may be altered or destroyed through normal use, an appropriate technique must be used from the very moment of identification the evidence as relevant for an investigation. Therefore it requires special tools and equipment, as well as specialized training and expert testimony.

Digital evidence is provided by recovering and analysing data and material obtained from electronic devices and cloud-based services, in the process also known as digital forensics. Digital Forensics is the branch of forensic science that focuses on identifying, acquiring, preserving, processing, analysing and reporting of digital evidence. It relies on scientific methods that are demonstrably reliable, accurate, and repeatable so that they may be used in judicial proceedings. In other words, Digital Forensics can be seen as the application of digital investigation and analysis techniques in order to perform a structured examination of a digital storage medium, while maintaining a documented chain of evidence, for the purpose of gathering information admissible in evidence in a court of law or in a disciplinary procedure. The objective of digital forensics is to follow the standardised investigation process while documenting any evidence that is stored digitally which may indicate to the person responsible for the crime. Therefore, forensic methodology can be described through the three A's: *Acquire* (do not alter or damage the original); *Authenticate* (proof that your recovered evidence is the same as the original); *Analyse* (inspect evidence without altering it).

A major challenge to digital forensic analysis is the ongoing growth in the volume of data seized and presented for analysis. This is a result of the continuing development of storage technology, including increased storage capacity in consumer devices and cloud storage services, and an increase in the number of devices seized per case. Consequently, this has led to

6 More on https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

7 Often retrieved from places known or accessible only to experts

increasing backlogs of evidence awaiting analysis, often many months to years, affecting even the largest digital forensic laboratories (Quick & Choo, 2014).

ROLE OF DIGITAL FORENSICS IN FIGHTING CYBERCRIME

When we talk about Cybersecurity we are considering it as "a very wide-ranging term that covers all aspects of the protection of citizens, businesses and critical infrastructures from threats that arise from their use of computers and the Internet" (Sommerwille, 2016). Cybersecurity incidents are diversifying both in terms of who is responsible and what they seek to achieve. Today, the border between cybercrime and 'traditional' crime is blurring as criminals use the internet both as a way to scale up their activities, and also as a source to find new methods and tools to commit crime. Yet, as stated in Joint Communication to the European Parliament and the Council from 2017, "in the vast majority of cases, the chances of tracing the criminal are minimal, and the chances of prosecution smaller still" (JOIN/2017/0450 final, 2017). Although effective investigation and prosecution of cybercrime is considered as a key deterrent to cyber-attacks, finding useful information for cybercrime investigations, mostly in the form of digital traces, is still a major challenge for law enforcement authorities.

In order to strengthen the law enforcement response to cybercrime in the EU, in 2013 the European Cybercrime Centre (EC3) was established by Europol, with the aim of helping protect European citizens, businesses and governments from online crime. Each year, EC3 publishes the Internet Organised Crime Threat Assessment (IOCTA), as the strategic report on key findings and emerging threats and developments in cybercrime. It also provides key recommendations for fighting cybercrime in an effective and concerted manner (to law enforcement, policy makers and regulators).

Together with strategy and operations, forensics is considered as one of the three pillar in EC3 approach to the fight against cybercrime, as shown in Figure 1.

Figure 1. EC3 three-pronged approach to the fight against cybercrime[8]

8 Source: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Trained and skilled individuals (Digital/**Computer Forensic Experts)** work not only for public law enforcement but also in the private sector in order to carry out tasks related to the collection and analysis of digital evidence. They are responsible for the identification, acquisition, authentication, preservation, analysis, and presentation of evidence for prosecution purposes (INFOSEC Institute, 2018). They are also faced, among other problems, with rapidly changing computer technology, encrypted files and volumes and a large number of anti-forensics tools, which all requires more time and money for the investigating organisation (Irons & Lallie, 2014).

Digital forensics can be performed as:

- Traditional Forensics - when target system is turned off (static analysis);
- Live Forensics - when target system is in working mode (Often Incident Response).

Traditional approach includes generating forensic image (bit-by-bit copy) of targeted device hard disk after device is switched off. Then, a detailed investigation (collection and analysis of digital evidence) is performed. Although widely adopted mainly because it guaranties no (or there is a slim chance for) modification of disk data, the main drawback of this approach is evidential loss of so-called 'live' data - information whose existence in volatile memory depends on power.

Therefore today it is obligation for every digital forensic analyst to use methodology which advocates extracting 'live' system data before system is shut down in order to preserve memory, process, and network information that would be lost with traditional forensic approach. Examination of the volatile memory, i.e. performing Memory Forensics is a must and therefore making a RAM dump becomes a standard operating procedure when acquiring digital evidence before switching the system off and taking the hard drive out. It is essential to realize that acquiring volatile memory will inevitably leave acquisition footprint. This process may be acceptable to the law enforcement officer performing the acquisition, but in order to make evidence acceptable to the court the entire acquisition process must be carefully documented. Currently, most court systems are ready to recognize the fact that certain footprint is introduced by law enforcement during the acquisition process (Afonin & Gubanov, 2013).

The official ACPO Guidelines (ACPO, 2012) recommend the following standard procedure for capturing a memory dump:

- Perform a risk assessment of the situation: is it evidentially required and safe to perform volatile data capture?
- If so, install volatile data capture device to a removable data carrier (such as a USB stick) – preferably, this has already been done prior to starting the operation;
- Plug the data carrier into the machine and start the volatile data collection script;
- Once complete, stop the device (particularly important for USB devices which if removed before proper shutdown can lose information);
- Remove the device;
- Verify the data output on a separate forensic investigation machine (not the suspect system);
- Immediately follow with standard power-off procedure.

The European agency ENISA has also provided a guide for first responders in the area of gathering the evidence related to a cybercrime, with the aim of providing guidance for Computer Emergency Response Teams (CERTs) on how to deal with evidence and evidence gathering process. It emphasized that CERT first responders have different priorities than law enforcement, as the primary function of a CERT is normally to ensure that the provision of

the service is returned or maintained. Evidence collection is usually only secondary to them, unlike for law enforcement where the sound evidence collection is typically of highest priority (ENISA & Anderson, 2015).

There is another distinction in analyses process, whether examination should be carried on:

- Physical media that holds binary data or
- Logical representation.

Depending on the case, the examination and analysis can be performed on raw data (physical analysis), or on data as they are arranged and saved by the operating system (logical) (Casey, 2004).

In order to help experts in performing digital forensics, a number of proprietary and free tools are available today, performing single action or in the form of integrated complete solution performing all steps in digital investigation from acquisition and analysis of digital evidence to the creation of report that will be submitted to the court.

DIGITAL FORENSIC TOOLS

Rapid evolution of digital evidence sources requires constant improvement in forensic techniques and procedures. The amount of collected data requires appropriate tools in order to make investigation of cybercrime efficient and useful. Use of proper procedures, techniques and tools is essential for digital forensic process.

Each forensic investigation must be traceable and repeatable by other forensic specialists with the same final conclusion. Compared to physical evidence, digital evidence requires different training and tools which both must follow technological advances. In some cases tools and examination techniques from few years ago are insufficient and incompatible with current technology and their use consequently increases the risk of missing critical information or otherwise jeopardizing an investigation. Using the most up to date tools can help mitigate challenges to the acceptability of results of digital evidence analysis in court.

As digital devices (e.g., computers, mobile phones, and GPS devices) become ubiquitous, the analysis of digital evidence is becoming increasingly important to the investigation and prosecution of crimes as it can reveal information about movement of suspects and criminal associates. But, without the right tools (designed to facilitate, among others, temporal, spatial and network analysis of volume of digital evidence) those complex data sets could remain useless for investigators. Examining millions of pieces of low level data in order to extract high-level information is a time consuming and exhausting work, requiring some automatic methods. Also, triage tools are seen as effective means of getting useful information early without waiting for in depth analysis of the entire target system (Soltani & Seno, 2017).

Digital forensic tools and techniques allow collection of evidence from various digital devices, even one that is difficult to get such as destroyed, locked, or obfuscated data. On the other side, criminals are adopting new rules by making attempts to counter forensic efforts. Some of the actions they perform include: wiping data, deleting files, faking or clearing logs, histories and other traces of performed activities, encrypting the entire volume, etc. These measures, performed in order to hide traces of activity, are called anti forensics (Gubanov, 2012).

A variety of digital forensic tools exist today. Some of them are made for acquisition of volatile data before a suspect system is shut down (capture the live memory - memory dump

tools) like: FTK (Forensic Tool Kit) Imager,[9] Madiant Memoryze,[10] DumpIt,[11] OSForensics,[12] CaptureGUARD,[13] Belkasoft Live RAM Caputer,[14] etc.

There are some outstanding tools that can be used for the acquisition and analysis process (for compute) such as: Volatility,[15] EnCase,[16] Autopsy,[17] Forensic Toolkit (FTK®),[18] CAINE,[19] SANS Investigative Forensics Toolkit–SIFT,[20] **Cellebrite UFED**[21] **and** Belkasoft Evidence Center.

In order to find tools that meet one's specific technical needs, forensic practitioners can use easily searchable catalogue of forensic tools provided by NIST - Computer Forensics Tool Catalog.[22]

In the next section we will briefly describe the possibilities of Belkasoft products in digital forensic process.

DIGITAL FORENSICS WITH BELKASOFT EVIDENCE CENTER

Belkasoft Evidence Center (BEC)[23]is an all-in-one forensic solution for acquiring, locating, extracting, searching, analysing, storing and sharing digital evidence stored inside mobile and computers devices, RAM and cloud. It can extract digital evidence from multiple sources where the most forensically important artefacts are selected for investigator to review, examine more closely and add to report. The tool looks out at hidden locations and for encrypted information for detailed investigation, and carves out damaged or deleted files.

It is well known and wide used in law enforcement agencies, outperforming in real life investigation some of the most known tools such as EnCase (Antyasov & Ufimtcev, 2016; Filipić & Protrka, 2016; Umar et. al., 2017).

BEC can perform the following tasks:

9 Free Access Data tool that can acquire live memory and paging file on 32bit and 64bit systems. More on https://accessdata.com/product-download
10 Free memory forensic software that helps investigators find digital traces in live memory. Memoryze can acquire and/or analyze memory images and on live systems can include the paging file in its analysis. More on https://www.fireeye.com/services/freeware/memoryze.html
11 Generate a physical memory dump of Windows machines. Can be deployed as executable on USB keys, for quick incident responses needs. More on: https://zeltser.com/memory-acquisition-with-dumpit-for-dfir-2/
12 More on: https://www.osforensics.com/osforensics.html
13 Physical Memory Acquisition Hardware which can be used with WindowsSCOPE Cyber Forensics. More on: http://www.windowsscope.com/products/
14 More on: https://belkasoft.com/ram-capturer
15 The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License (GPL v2), for the extraction of digital artifacts from volatile memory (RAM) samples. More on: https://www.volatilityfoundation.org/
16 Multi-purpose forensic platform. More on: https://www.guidancesoftware.com/encase-forensic
17 Open Source Digital Forensic Software. More on: https://www.autopsy.com/
18 More on: https://accessdata.com/products-services/forensic-toolkit-ftk
19 CAINE (Computer Aided Investigative Environment) is a Linux Live CD that contains a wealth of digital forensic tools. More on: https://www.caine-live.net/
20 SIFT Workstation is a group of free open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. More on: https://digital-forensics.sans.org/community/downloads
21 More on: https://www.cellebrite.com/en/products/ufed-ultimate/
22 More on: https://toolcatalog.nist.gov/index.php
23 More on: https://belkasoft.com/ec

- forensically acquiring a device, RAM or a cloud;
- reviewing device file system, deleted data and special places;
- searching communications, documents and media;
- finding deliberately deleted artefacts;
- if artefacts are robustly deleted, finding implicit traces;
- searching encrypted files and decryption;
- in-depth SQLite database analysis;
- link analysis based on communication in multi-device cases.

Comprehensive Digital Forensic Investigation with BEC can be performed in three steps:

1. **Data acquisition**
   a. capturing a Live RAM dump and
   b. creating a forensic image of the suspect's hard drive
2. **Discovering and Analysing Evidence**
   a. applying techniques to identify and extract data – Examination
   b. using data and resources to prove a case – Analysis
3. **Creating Reports, Sharing Evidence and Getting Ready for a New Case**

Acquisition

When starting new case in BEC, we can choose whether we want to add the existing data source or we want to acquire and analyse a new one (Figure 2). With *Belkasoft Acquisition Tool*, obtaining data from following types of data sources are currently supported:

- Hard or removable drives - physical acquisition (as DD or E01 image) of hard drives, SSD drives and removable drives connected to computer, laptop or tablet.
- Mobile devices - data from Android and iOS devices (iPhones, iPads), including iOS 10. For rooted Android devices physical image is acquired, otherwise logical image is acquired.
- Cloud data - data can be downloaded from most important clouds such as Google, WhatsApp, Instagram and all popular email clouds.

Figure 2. Adding data source for examination in BEC

Additionally, with *Belkasoft Live RAM Capturer*

• Computer RAM memory - of a running Windows computer, laptop or tablet can be dumped in a raw format.

Creating a forensic image of the suspect's hard drive is considered as an essential step, a must-do in any investigation and must not be omitted. BEC also accepts memory images and disk images in all popular forensic formats (EnCase E01 and Ex01 images, FTK images, UFED physical dumps for mobile phones, DD images, SMART images, JTAG and chip-off dumps, VMWare, VirtualBox and Virtual PC files, Hibernation and page files, etc.), allowing processing of images previously acquired with non-Belkasoft imaging tools. It is important to understand that one process is performed for traditional (magnetic, spinning discs) hard drives and common flash memory such as USB sticks and memory cards, while solid-state drives (SSD) present an entirely different issue. SSD drives represent a new storage technology, operating much faster compared to traditional hard drives. They utilize a completely different way of storing information internally, which makes it much easier to destroy information and much more difficult to recover it. Traditional forensic methods fail[24] (there are some exceptions in some circumstances) when attempting recovering information deleted from SSD drives, or trying to recover anything from an SSD drive formatted with either Quick or Full format. Anyway, this issue is beyond the scope of this paper.

As stated earlier **memory dumps** can be a valuable source of ephemeral evidence and volatile information. Analysing a memory capture is a bit different from a hard drive analysis. With memory analysis one can try to actually recreate what the suspect was doing at the time of the system capture. Memory forensics can provide information about applications and running processes, passwords, login credentials, terminated and cache processes, traces left by malware and all other volatile data that are lost when device is turned off. Therefore, memory dumps may contain passwords to encrypted volumes (TrueCrypt, BitLocker, or PGP), account login credentials for many webmail and social network services such as Gmail, Yahoo Mail, Hotmail; Facebook, Twitter, Google Plus; file sharing services such as Dropbox, Flickr, SkyDrive, etc. Acquiring memory dump for memory analysis can be performed with *Belkasoft Live RAM Capturer* (Figure 3.).

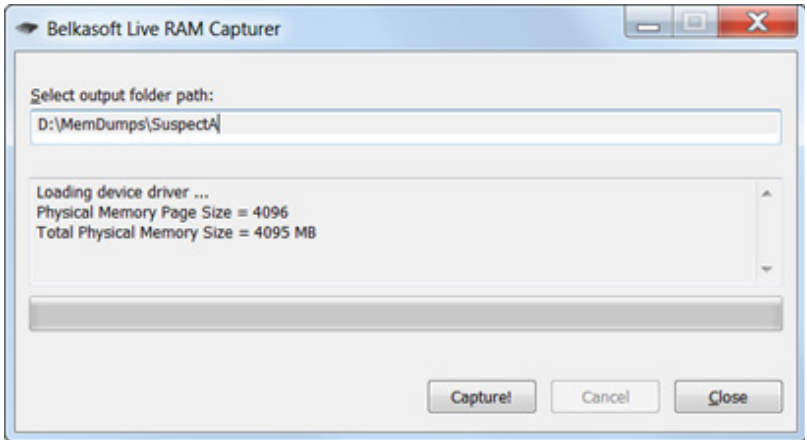

Figure 3. Acquiring memory image using Belkasoft Live RAM Capturer

24 Due to the use of TRIM command, releasing the space (making it free for writing) is done by effectively zeroing information as soon as it's marked as deleted by the operating system.

Belkasoft Live RAM Capturer is a free forensic tool that allows reliable extraction of the entire contents of computer's volatile memory – even if protected by an active anti-debugging or anti-dumping system.[25] The tool runs in the system's most privileged kernel mode, and allows acquisition of the complete contents of the computer's RAM along with protected memory areas.

Memory dump is stored with .mem extension and can be later added as a data source and analysed with BEC (or some similar analysis software). Besides RAM image file, a path to hibernation or page files (hiberfil.sys and pagefile.sys) can also be specified. These two kinds of files may contain Live RAM data written on a hard drive as a part of Windows functioning, thus they are important source of RAM artefacts, because the RAM contents may survive switching a computer off. Also, some other tools can be used to extract decryption keys out of the RAM dump and use them to decrypt and mount protected volumes (e.g., Elcomsoft Forensic Disk Decryptor[26] or Passware Kit Forensic[27]).

BEC allows searching for various forensic artefacts inside the memory, like browser histories, including deleted data and private browsing history, SQLite databases, pictures, documents, messenger chat histories, registry files, and more.

In order to carry on Live RAM analysis, data carving is used. Carving technique is a bit-precise sequential scan of the media for various artefacts. Carving can locate evidence, ignoring file names and file system, by reading low-level data directly from the media and looking for particular sequences of bytes or characteristic signatures specific to certain types of evidence. It may give a clue that some interesting data can be stored in a particular spot on the disk. Data carving is an indispensable technique which allows locating evidence that was deleted, destroyed, or never stored on the hard drive at all (page file, hibernation file, RAM contents).

Loading the data sources on which carving will be performed is shown in Figure 4. The result of the carving process is shown in Figure 5, where the extracted Gmail remnants indicate corruption of the messages (not all fields are available).

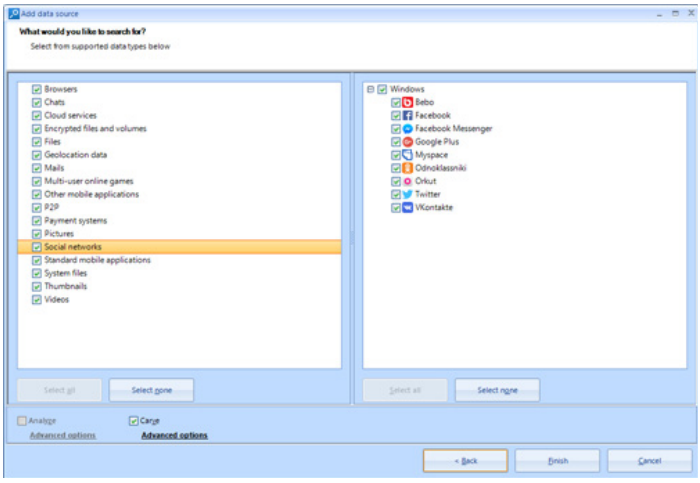

Figure 4. Data sources that can be carved and searched for evidence

25 Due to recent changes made by Microsoft in certification of kernel-mode drivers, Microsoft's policy has toughened, and Live RAM Capturer has stopped working on certain versions of Windows 7.
26 More on: https://www.elcomsoft.com/efdd.html
27 More on: https://www.passware.com/kit-forensic/

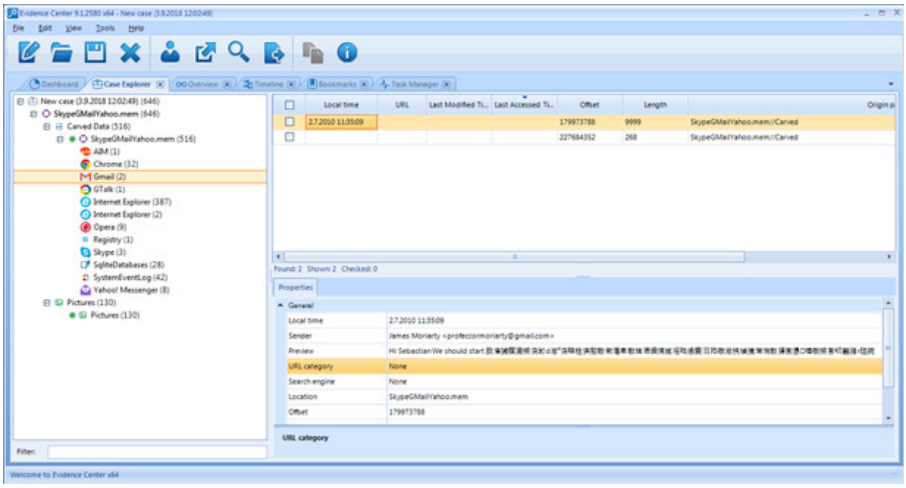

Figure 5. *The result of carving process performed on memory dump*

Discovering and Analysing Evidence

After acquiring forensic images of RAM and disk, BEC is used to retrieve the existing and deleted evidence in full auto mode from all major operating systems, both computer and mobile (Windows, Linux, MacOS X, iOS, Android, Windows Phone, Blackberry). The following types of data can be located or recovered if deleted:[28]

- Pictures and Videos;
- Emails;
- Web browser histories, cookies, passwords, cache, etc.;
- Mobile application data;
- Chats and instant messenger histories;
- Office documents;
- Peer-to-peer Software;
- Social network communications, Cloud Services and Online Games;
- Registry files;
- System files and configurations;
- Encrypted files and Volumes;
- SQLite databases;
- PCAP files;

The following types of analysis are available:

- Search and analysis of the existing and deleted files;
- Data carving and destroyed evidence recovery;
- Live RAM analysis;
- Hibernation and page file analysis;

28 More on: https://belkasoft.com/ec

- Native SQLite analysis with free list support (discovers deleted SQLite records, e.g. Skype conversations, WhatsApp messages, iPhone deleted SMS/text messages, Chrome downloads, etc.);
- Picture/photo analysis including EXIF and GPS analysis, face/pornography/text/forgery detection;
- Video key frame extraction;
- Encryption detection;
- Network traffic analysis, and many others.

In Live RAM analysis carving can help extracting recent messenger conversations, text messages sent and received, and any other temporary information used by applications, such as Facebook, Gmail and World of Warcraft (Gubanov, 2012). Although the obtained information may be damaged or partially overwritten, they still can provide enough evidence for the investigation as it can be seen in Figure 6.

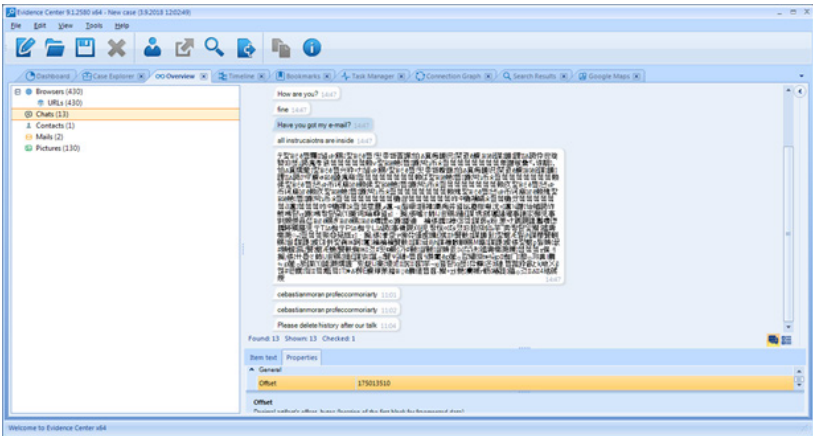

Figure 6. Evidence provided by memory dump analysis

In BEC an automatic multimedia content analysis is provided, helping investigators in quick detection of pornography content, human faces, specific text or forgery as shown in Figure 7.

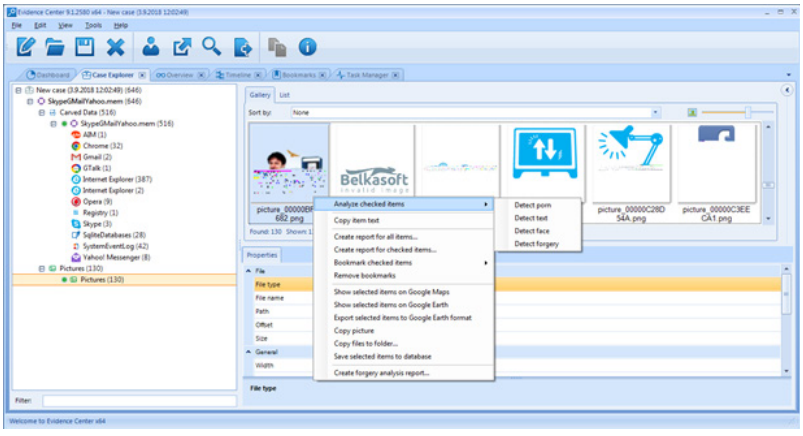

Figure 7. Different types of multimedia analysis with BEC

In order not to lose credibility as acceptable evidence, images presented as court evidence must not be manipulated in any way. An investigator using BEC can perform forgery detection techniques (from Forgery Detection plugin) on discovered images and provide the probability of the image being manipulated (forged). By doing so they can validate whether digital pictures submitted as evidence are in fact acceptable.

Creating Reports

Finally, a report can be automatically obtained in order to help presenting in the court the significance of the obtained digital evidence. BEC allows creating reports in all most popular formats (text, HTML, XML, PDF, CSV, etc.). The report options are highly customizable and the resulting report can be presented in court or shared with a colleague. An example of the report in HTML format is shown in Figure 8.

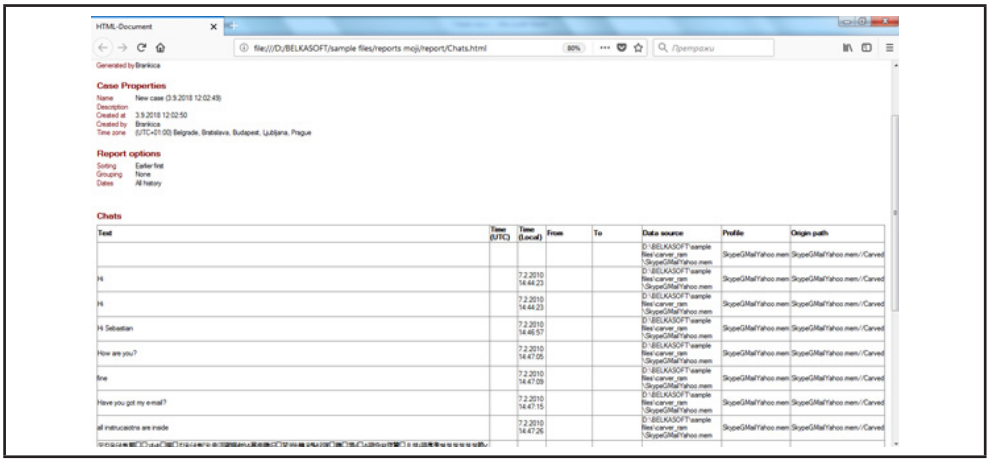

Figure 8. Part of Report (in html format) for Chats previously shown in Figure 6

CONCLUSION

Digital forensics (especially memory and cloud forensics) is an emerging field, rapidly growing in the last decade. With the aim of providing digital evidence which will help law enforcement investigation of cybercrimes, it relies on utilization of adequate techniques and tools. There is a variety of available tools on the market designed to perform a single task (e.g., acquisition) or multiple tasks (analysis, reporting, etc.) in digital forensic process. Since advances in technologies (e.g., ubiquitous computing) have led to an increase in the volume and variety of data available for digital forensic analysis, the need for efficient techniques and tools is rapidly growing. Although efficiency and effectiveness of even most popular tools is not yet sufficient to handle the tremendous increase in cybercrime, without them the investigation of cybercrime would be almost impossible.

There are a number of digital forensic tools that become a standard in forensic investigation providing digital evidence that are acceptable to the court of law. This paper has discussed one of them, Belkasoft Evidence Center, whose capabilities were briefly presented.

ACKNOWLEDGMENT

This paper is the result of the research on the project 'Forensic methods in criminalistics', which is financed by the Academy of Criminalistic and Police Studies. The work was partly supported by a grant from the Ministry of Education and Science, Republic of Serbia [Project number TR 34019].

REFERENCE

1. ACPO (Association of Chief Police Officers). (2012). *Good Practice Guide for Digital Evidence*. Retrieved on May, 15th, 2018., from https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
2. Afonin, O. & Gubanov, Y. (2013). Catching the ghost: how to discover ephemeral evidence with Live RAM analysis, *DFI Magazine*, May 2013, Retrieved on June, 15th, 2018., from https://belkasoft.com/live-ram-forensics
3. Antyasov, IS & Ufimtcev, MS. (2016). Software and methods of recovery of information in the process of computer forensics (in Russian), *Вестник УрФО БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ*, № 3(21), 16-23. Retrieved on May, 8th, 2018., from http://www.info-secur.ru/is_21/is_21.pdf
4. Casey E. (2004). *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, Elsevier Academic Press, London, UK
5. Council of Europe, CETS 185. (2001). *Convention on Cybercrime,* Budapest, 23 November 2001. Retrieved on May,21st, 2018., from https://www.coe.int/en/web/cybercrime/the-budapest-convention
6. ENISA & Anderson, P. (2015). *Electronic Evidence - A Basic Guide for First Responders. Project Report*. European Network and Information Security Agency (ENISA). http://doi.org/10.2824/068545
7. European Commission, COM/2007/0267 final. (2007). *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cyber crime*, {SEC(2007) 641} {SEC(2007) 642}, Retrieved on May, 22nd, 2018., from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex-%3A52007DC0267
8. European Commission - Fact Sheet, MEMO/18/3345. (2015). *Frequently Asked Questions: New EU rules to obtain electronic evidence*, Brussels, 17 April 2018. Retrieved on May, 21st, 2018., from http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm
9. Filipić, K. & Protrka, N. (2016). Uloga forenzičkog softvera EnCase pri radu s elektroničkim tragovima. *Kriminalistička teorija i praksa*, 3(2/2016), 121-134. Retrieved on June, 5th, 2018., from https://hrcak.srce.hr/182423
10. Gubanov, Y. (2012). Retrieving Digital Evidence: Methods, Techniques and Issues, *Forensic Focus*, July 2012, Retrieved on May, 18th, 2018., from https://www.forensicmag.com/article/2012/05/retrieving-digital-evidence-methods-techniques-and-issues
11. INFOSEC Institute. (2018). *Computer Crime Investigation Using Forensic Tools and Technology*, Posted in Forensics, General Security on January 26, 2018. Retrieved on April 23rd, 2018., from https://resources.infosecinstitute.com/computer-crime-investigation-using-forensic-tools-and-technology/#gref

12. Irons, A. & Lallie, HS. (2014). Digital forensics to intelligent forensics, *Future Internet*, 6, 584-596, doi:10.3390/fi6030584
13. Joint communication to the European parliament and the Council, JOIN/2017/0450 final. (2017). *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, Retrieved on April 28th, 2018., from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450
14. Quick, D.& Choo, KKR. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges, *Digital Investigation*, 11(4), 273-294, https://doi.org/10.1016/j.diin.2014.09.002
15. Soltani, S. & and Seno, SAH. (2017). A survey on digital evidence collection and analysis, *In 7th International Conference on Computer and Knowledge Engineering (ICCKE)*, pp. 247-253, Mashhad, 2017. https://doi.org/10.1109/ICCKE.2017.8167885
16. Sommerville, I. (2016). *Software Engineering, 10th edition*, Pearson Education Limited, Harlow, England
17. Umar, R., Riadi, I. & Zamroni, GM. (2017). A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements. *International Journal of Advanced Computer Science and Applications(IJACSA)*, 8(12), 69-75. http://dx.doi.org/10.14569/IJACSA.2017.081210