FACTA UNIVERSITATIS
Ser: **Elec. Energ.** Vol. 25, N^{o} 2, August 2012, pp. 121 - 136
DOI: 10.2298/FUEE1202121S

THE IMPORTANCE AND THE ROLE OF FORENSICS OF MOBILE

Žaklina Spalević, Željko Bjelajac, Marko Carić

Law Faculty of Economics and Justice, University Business Academy, Novi Sad, Serbia

Abstract. *Scientific-technological development, along with initiating integrative forces that offer improvement of the quality of human life, concurrently created prerequisites for individuals to exploit certain innovations for performing criminal activities. Modern criminals wander through electronic networks, and assisted by high technology, perform a variety of criminal acts and "launder" large sums of money. Computer forensics is a technological, systemic control of the computer system and its content for the purpose of gathering evidence of a criminal act or other abuse that it has been used for. Digital forensics requires particular expertise that goes beyond traditional data collection, as well as employment of techniques available to the final user or system support personnel. In this context, this article examines principles, methods and procedures in mobile device investigation, which nowadays represent a multifunctional, powerful computer weapon, and considers the necessity to update concrete procedures in accordance with the development and growth of IT.*

Key words: *digital forensics, forensics of mobile devices, cyber crime, cyber crime investigation, security and protection of communication networks*

1. INTRODUCTION

According to the state law, computer crime represents criminal offense where the use of computer technology is manifested as a method of performing a criminal act or it represents means or the target of the criminal act, thus realizing relevant consequences in criminal or legal terms [1]. Computer crime is an unlawful violation of property that implies purposefully altered computer data (computer manipulation), destruction (computer sabotage) or common utilization with hardware (time theft) [2].

The basic elements of computer crime offense include event, circumstances and psychological state of the perpetrator that allows classification and profiling of the criminal. During the execution of computer crime, the computer may be:

- Aim of the attack (computer intrusion, theft, or data destruction),
- Means of the attack (credit card fraud, sending spam or images),
- Link to regular crime (drug or human trafficking, child pornography),
- Repository of digital evidence of computer crime.

Received June 9, 2011
Corresponding author: Žaklina Spalević
Law Faculty of Economics and Justice, University Business Academy, Novi Sad, Serbia

Forms of computer crime include: unlawful use of services and unauthorized acquisition of information, computer theft, computer fraud, sabotage, terrorism and crime related to criminal networks. Common forms of computer crime are: theft of computer service, unauthorized access, software piracy, exposure, theft and alteration of computer data, extortion through computer, unauthorized database access, stolen password abuse, transmission of destructive viruses, and industrial and political espionage.

2. COMPUTER AND CYBER CRIME

Nowadays, information flow represents a basis of system functioning in any developed state while computer networks are the main platform for the effective functioning of the financial system. Crime related to computer networks is the form of criminal behavior in which the role of cyber space appears threefold:

- **Computer networks as tools or means** – Contemporary criminals increasingly use computer networks as means for the realization of intentions. This is particularly common in child pornography [3], abuse of intellectual property, or online sales of illegal goods (drugs, human organs, brides).
- **Computer networks as the goal of the attack –** Targets of the attacks include services, functions and contents on the network. Services and data are stolen, segments of the network or the entire network or computer system are damaged or destroyed, or operative functions are hindered. In any case, the goal of the perpetrators is the network which is invaded by malware, DOS attacks, etc [4].
- **Computer network as the environment of the realization of attack –** This environment often serves to conceal criminal actions, primarily related to pedophiles as well as other criminals. Certainly, there are other roles as well, such as employment of network as a symbol of intimidation, mainly perceived in computer crime rather than cyber crime. The concept of *Cyber* in this way represents the environment which is equipped with high technology, exceedingly developed computer networks, where the systems' ownership is not defined, that is, where the real and virtual face. It is important to note that cyber crime certainly has 'attributes' of crime as “illegal or temporarily criminalized form of behavior” [5].

Depending on the committed act, cyber crime may be political or financial. Political cyber crime implies [6]:

- Cyber espionage and cyber sabotage in computer environment,
- Hacking,
- Cyber terrorism (the Internet as a weapon and communication system of terrorist organizations),
- Cyber war.

Financial cyber crime implies [6]:

- Cyber fraud (false electronic trade of the securities, false financial offers for the purpose of obtaining information on bank accounts of the subjects who are target of the attack),
- Hacking,
- Theft of Internet time, theft of Internet services,
- Piracy of software, microchips and BP,

- Cyber industrial espionage,
- Spam,
- Production and distribution of unauthorized malware such as child pornography, pedophilia, religious sects, spreading of racial, Nazi, or similar ideas and attitudes,
- Abuse of women and children,
- Manipulation of contraband products, substances or goods – drugs, human organs, weapons,
- Violation of cyber privacy – email monitoring, wiretapping, chat rooms recording, e-conference surveillance, inclusion and analysis of spy software and 'cookies' (spyware protection software).

Depending on the forms, damages associated to computer crime may be:

- Financial – which may appear when perpetrators commit an act for the purpose of acquiring financial profit for themselves; unlawful material profit can be acquired or not, but perpetrators objectively cause certain damage by performing the act, or when perpetrators do not act aiming to obtain profit for themselves or others, but objectively cause financial damage.
- Non-financial – represent unauthorized disclosure of others' secrets or other "indiscrete harmful action".
- Combined – when disclosure of certain secret, or violation of author rights, by abusing computer or computer networks, may damage someone's reputation, breach moral right and concurrently cause concrete financial damage as well.

3. Security and Integrity of Public Communication Networks

The rapid growth of information-communication technology was not followed by an adequate legal regulation in most of the states. The undefined cyber space, different concepts of electronic communication, lack of competent individuals or bodies following the development of IT, legal norms and indivisibility of space of acting of the offenders in the field of cyber and computer crime, further complicate this issue. For preparation and commitment of criminal offenses in the field of cyber and computer crime, electronic communication is used as a channel for the main attack regardless whether it comes to individual or corporate users. The main goals of the perpetrators include: abuse of communication service, theft of personal data (in particular identity and financial data), and breach of privacy [7]. There is a variety of known scenarios of abuse of services that cause financial damage to the users in networks for transmission of speech, such as an array of abuses of service mechanisms with increased tariff (*premium rate*), unknown missed calls (*call-back scam*), *phishing*, *whishing* [8]... Therefore, telephone and Internet network converge in the field of technology into deception techniques of the users. Increased use of the Internet results in augmented forms of online theft supported by social engineering (*phishing*). The main purpose of electronic communication networks, services and communication equipment is transmission of messages and information. Nevertheless, electronic communication networks serve to some users to conceal their activities (presence, identity, movement, contacts, content of communication), harass or blackmail other users, steal, abuse and trade personal data, systematically monitor or record other users' activity or merely use services and network infrastructure as technical logis-

tics of criminal acts, offenses or other forms of dishonest acts unrelated to electronic communication. In this way, they do not cause direct financial damage, but these forms of malicious use belong to a wider context of fraud or a certain category of violating information security, breach of privacy and abuse of personal data, which further illustrates essential interrelatedness of these concepts.

The right to inviolability of the secrecy of letters and other means of communication and the right to protection of personal data are guaranteed by the Constitution of the Republic of Serbia as basic human rights and freedoms [9]. Deviation from the principle of inviolability of the secrecy of electronic communications is allowed only temporarily and based on a valid court order, in case they are necessary for the purpose of criminal proceeding or protection of security of the Republic of Serbia, in accordance with the law (Article 41) [9]. It is prohibited and punishable to use personal data that are not obtained in accordance with law, except for the purpose of criminal proceeding or protection of security of the Republic of Serbia, in accordance with the law (Article 42) [9]. In regards to electronic communications, International Court for Human Rights in Strasburg (ECHR), in the case of *Copland vs. United Kingdom* in 2007 decided that information related to the time and duration of phone conversation and in particular selected numbers of users represent "an integral part of phone communication" [10]. Considering that the verdicts of the ECHR are obligatory for the Republic of Serbia, it is clear that the principle of inviolability of the secrecy of electronic communications should be equally applied on the content and data of the electronic communications in Serbia.

4. THE CONCEPT OF INVESTIGATING CYBER CRIME

The main purpose of the investigation of cyber crime is to form and provide the judicial system with strong and irrefutable evidence of guilt, and/or evidence for the release of the suspect and/or right sanctioning for the committed offenses. Methodology of investigating and proving cyber crime is based on the methods of investigation in classic crime, considering the specificity of investigating sensitive and rapidly changeable digital evidence. In the field of cyber crime it is almost impossible to secure direct evidence, but it is possible to form strong and irrefutable digital evidence from a series of indirect digital evidence stored and generated in corresponding computer systems and networks. IOCE defines digital evidence as any information in digital form with an appropriate attestation or liberating value or value of reasonable doubt and it is stored or transmitted in digital form [11]. For judicial practice to accept computer generated and memorized digital evidence, it is necessary to prescribe procedures through legislation and by-laws at national level including:

- Handling and storing digital evidence
- Forensic acquisition of evidence
- Analysis of evidence
- Expert opinions and testimonies on digital evidence

Digital forensics is a science focused on gathering, storage, identification, analysis and documenting of digital evidence or data that has been stored, processed or transferred in digital form. The complexity of digital forensics and rapid growth of IT resulted in departmentalization and strict specialization of experts in various fields. Therefore, specific

areas of digital forensics are discriminated, such as computer forensics, forensics of mobile devices, network forensics and database forensics. Among a variety of digital forensic models, the most frequent are: The DFRWS Framework Meta-Model, The Reith, Carr and Gunsch Model, The Ciardhuain Model, The Beebe and Clark Model, Kruse and Heiser Model, DOJ Model, Lee's CSI Model and Casey Framework Model.

5. DIGITAL FORENSIC INVESTIGATIONS

Digital forensic investigation is commonly observed through official (public) and corporate (private) investigation as two basic categories.

Official digital forensic investigation involves police investigative bodies and special prosecution for cyber crime that conduct investigation on the basis of Law on criminal procedure, Law on combating cyber crime, Law on electronic communication, Law on protection of information and information systems, Law on digital evidence, Law on electronic signature and Law on electronic commerce.

General process of official digital forensic investigation, on the basis of "step-by-step" model entails 4 phases [12]: Initial investigation, Tracking the perpetrator, Discovering identity of the perpetrator and Arrest.

In true cases of cyber crime, at the stage of preliminary investigation and search, investigative bodies collect evidence of reasonable doubt and put in a claim against the suspect who can also be unknown individual. On the basis of police findings, the prosecutor provides a warrant for investigation from investigative judge and initiates official investigation [13]. Based on a valid court order, suspicious computer or communication system can be temporary confiscated; that is, physical image of the hard disk or memory content of IT system and devices for the purpose of forensic acquisition and data analysis can be taken.

Corporate digital forensic investigation is comprised of the initial three phases of public investigation applicable to investigation within corporation. This form of investigation is conducted by corporate digital forensics, administrator of computer networks assisted by experts on physical transfer and data protection in the corporation [14]. Quality corporate investigation implies performance of each stage for the purpose of:

- Eliminating the obvious,
- Forming hypotheses of the attack,
- Reconstructing criminal act,
- Tracing suspicious computer used for the attack,
- Analyzing source, target and intermediate computers,
- Preparing evidence, which implies the presentation of the computer itself before court if applicable,
- Submission of findings and evidence material (investigation report) to corporate investigative bodies or official investigative bodies for further procedure.

Standard procedure of corporate forensic investigation contains several phases that involve team work of corporate investigative bodies and official IT experts of the corporation [15]:

1. Testing suspect and witnesses.
2. Preparing bodies for investigation (locating compromised computer).
3. Inquiring resources of the suspect.
4. Checking the log file records and other information on the suspect.

5. Complete marking and sorting of indirect evidence with detailed notes on the content and space for the signature of the person who takes over the evidence material.
6. Protecting memorized data with evidence from any alterations.
7. Ensuring time interval of evidence as solid proof.
8. Utilizing forensic tools to verify events as criminal act.
9. Control check-up of the flow of each phase of the investigation.
10. Collecting, analyzing and preparing evidence for the trial.
11. Developing a detailed report on the investigation, documentation and provision of suggestions for further proceedings.
12. Deciding on the organizational level to: cancel, continue in the organization or submit the case to competent authorities.

The main problems in the corporate forensic investigation include:

- Bodies of corporate forensic investigation cannot lead investigation outside of the organization or its computer system.
- Corporate investigation has no legal permission for search or seizure of the compromised computer or communication device outside of its IKS.
- Bodies of corporate investigation must consider the publicity of the information of the attack in IKS due to business reputation and clients' trust.

Based on reasonable doubt of the corporate investigative bodies, official investigative bodies with a valid search warrant in the process of preparing and realizing search and seizure of the suspicious computer for the purpose of providing digital evidence must apply *Standard procedure of computer seizure as evidence* [16], which should contain the following elements:

- Legal working framework (court order) and limitations in dealing with confidential data.
- Confirmation of credibility and competency of the investigative body.
- Identification of all seized media except HD (tapes, printer cartridges, zip, floppy, CD ROM, DVD, memory card, combined receiver-transmitter devices) and documents related to storage of digital evidence (content, data on certification/testing/ examination and the analysts' name.
- Storage of digital evidence in adequate environment (temperature, humidity, dust, magnetic fields, etc.) and in appropriate manner.
- Detailed report on processing and the structure of HD of the suspicious computer and memory content of communication devices.

6. FORENSICS OF MOBILE DEVICES

The majority of population is not aware of the potential of "*Smart phones", i*Pod, BlackBerry, PDA devices (*Personal digital assistant*) and risks related to their destructive use. The fact that modern mobile phones or PDA devices today have performances of a computer desktop five years ago significantly indicates their power. It is difficult to precisely define mobile devices considering that many devices such as video cameras become increasingly smaller. Forensic of mobile device is primarily performed on mobile phones and PDA devices, although it is posited that it also involves forensics on mobile

video cameras. Technological development of mobile communications is pretty fast, resulting in a constant battle between individuals and organized groups, who wish to conceal development and utilization of data that have been illegally used, and forensic investigators. Forensic investigation of mobile devices must consider three facts that discriminate it from computer forensic investigation:

- Great changeability of operative systems, standards of production of the devices, technology of data storage, procedures of data protection and interface devices.
- The diversity of platforms of mobile devices in contrast to standardization in the computer world.
- Utilization of wireless technology for communication (infrared communication with a few meters range, B*luetooth* communication with 20 meters range and wireless communication by standard 802.11 range until 100 meters).

In contrast to computer forensics, mobile devices forensics can hardly be standardized and it does not imply the same rules as standardized forensics. The example that illustrates this is the prohibition of writing on the medium that is a subject of classic forensic investigation which is not valid in some cases of mobile devices forensics.

According to the type of mobile device and services it provides to the user, several categories of evidence are distinguished in forensics of mobile devices:

User ID is utilized in provider networks of mobile phones as a proof of authenticity of the users and verification of the types of services available to users. Mobile device is identified by an international number for identification of mobile devices (IMEI). SIM (*Subscriber Identity Modules*) card contains a number labeled as international number for identification of users (IMSI) used for registering to a system, secret code for verification and other information. IMEI and IMSI numbers are independent, which provides users' mobility. SIM card can be protected from unauthorized access by personal identification number or a password.

Diary of mobile devices often contains timely arranged lists of incoming, missed, replied and selected numbers, as well as GPS information, connection moments on appropriate network cells and moment of connection termination with network cells. This information can lead to a very precisely controlled location of the user in specific moment of time.

Contacts within the mobile device can be considered a list of potential witnesses, victims or accomplices, which may contain photos, email address, physical address, alternative phone numbers and much other useful information on individuals in Contacts.

Text messages contain segments of evidence and time determinants which are very valuable in investigation. Modern computer procedures allow for reconstruction and tracing of damaged or deleted messages.

Calendar can indicate the suspects' movement, obligations, or individuals they had contacted.

Electronic mail provides information on internet communication of the suspect.

Instant messages are messages exchanged in real time and may contain complete conversations and time determinants.

Images.

Audio records.

Multimedia messages.

Application documents represent documents that can be generated in some modern mobile devices in the form of calculation, presentation and other document formats.

SD cards often serve for data transfer from a computer to a mobile device and vice versa and therefore represent important evidence in investigation.

The purpose of forensic software is to provide protection of the existing data on the original device which ensures the integrity of the collected data. In case of mobile devices, it is at times necessary to write on their memory in order to obtain certain information. This should certainly be reduced to a minimum. Basically, data is copied from the original device, but time features are altered in this case which complicates proving that the integrity of data has not been compromised. In case investigation is performed on a new mobile device, for which there are no standardized forensic tools, it is recommended to provide additional copies of the data and precise description of the employed procedures and methods.

6.1. Mobile phones and SIM cards

Forensic acquisition of data and data retrieval from mobile devices represent non-standardized processes due to quick changes in technology of services that provide this non-standardization. Nowadays, memory contents of mobile phones are kept on three basic memory components:

- ROM (*Read Only Memory*) memory of mobile phones protects operative system and software for diagnosing mistakes and device damages.
- RAM (*Random Access Memory*) memory of mobile phones serves for temporary utilization of used data while the device operates.
- Memory cards, MiniSD cards, SD cards or MMC mobile cards represent additional memory resources for storage of applicative data saved by the users of mobile phones.

When initiating the investigation, it is necessary to assume type of network within which mobile phone functioned and on this basis select joint forensic tools and procedures of investigation. Today, 3 types of mobile networks are defined [17]:

- CDMA (*Code Division Multiple Access*) network does not have the *Subscriber Identity Module* (SIM) module, which means that all the data are saved on the mobile phone. These networks are prevalent in the US.
- GSM (*Global System for Mobile Communication*) networks use SIM module as separate components designed as transferable element from one to the other device. GSM networks are dominant in Europe.
- IDEN (*Integrated Digital Enhanced Network*) networks use system of advanced SIM cards (USIMs) developed in Motorola.

After determining the type of mobile network within which mobile phone functioned, the exact type of mobile phone is determined and on these bases characteristics and applicative potential of the device are evaluated. Determination of the exact type of mobile phone is performed by searching the producer, serial number of the device that is commonly placed under the battery, synchronization software and codes of the producer.

Based on the producers' code, placed in the same area as the serial number, it is possible to obtain information such as phone producer, model, and code of the state where it was produced. Operative system of mobile phones contains the following codes that de-

fine the identity of a mobile phone as unique device: *Electronic Serial Number (ESN)*, *Integrated Circuit Card Identification (ICCID)*, and International Mobile Equipment Identifier (IMEI) [18].

Based on the type of mobile phone and its performance it is possible to define potential places where evidence material could be found. Based on the producer's specifications, which may be diverse than the real state in the mobile phone, due to adjustments of the user, it is possible to have insight into the following technical performances of the device: Wireless connection networks (*Bluetooth*, WI-Fi or infrared technology), Internet access, Technical camera features, PIM (*Personal information manager*) contains calendar, contacts, and software for production and overview of different types of documents, Types of messages that mobile phone can generate, send and receive (SMS, multimedia, email), Types of applications included in the phone delivered to the user and Interface for connecting with other IT devices.

SIM card within GSM and IDEN network allows users to transfer data i.e. contacts, messages, as well as users' authenticity among mobile phones. Despite changing the phone, the user can always be traced based on the passive or active use of the SIM card. In forensic investigation, it is not recommended to access mobile phone through another SIM card as it might damage evidence. Cloning SIM cards by using forensic tools is the safest way to access mobile phone that provides validity and immutability of the evidence on the mobile phone. SIM card is protected by PIN code (*Personal identification number*) length ranging from 4 to 8 numbers, responsible for data protection both on the SIM and the mobile phone. In case mobile phone is blocked due to multiple inappropriate PIN code entry, it can be unlocked by using PUK code (*PIN Unblocking Key*). In case PUK is entered inappropriately three times, mobile phone cannot be unblocked anymore.

Analysis, processing and data collection on PDA devices as independent devices is performed in a similar way as in case of mobile phones. If we compare their features, the only difference between PDA and mobile phone is that PDA cannot make calls. Nevertheless, today's s*mart phones* have all the possibilities as independent PDA devices.

Digital cameras represent mobile devices for forming and storage of photos and video records that use a standard or USB port for communication with computer and standard memory MiniSD or Compact Flash cards to increase memory capacity [19]. In digital forensic investigation of these devices, they are treated as medium for data storage and thus, the application of standard methods and procedures and tools of digital forensics is provided. Taking into account that analysis and search are conducted via USB port, it is not allowed to write on the medium in order to prevent content modification. The same principle applies for reading and searching memory cards. Mobile digital audio devices i.e. MP3 players and iPods are also treated as medium for data storage.

6.2. Tools, devices and procedures in forensic processing of mobile devices

In mobile device forensics, logical forensic acquisition of data is dominant in regards to physical acquisition in practice, taking into account that mobile forensic techniques follow the same format and that forensic software uses operative system of mobile phones to extract data. Physical acquisition is used to extract data that operative system does not see or cannot access. Mobile forensics primarily deals with acquisition of data from mobile phones and PDA devices. Tools for mobile forensics can be grouped in two categories:

- CDMA forensic tools for acquisition of mobile phone data
- GSM forensic tools for acquisition of mobile phone data and SIM card data (Paraben, CellDEK kit, Oxygen software, Crownhill, InsideOut Forensics).

The main devices utilized in digital forensics of mobile phones include:

- Faraday bags, which prevent any type of communication of mobile device under investigation with external mobile devices and isolate the device. Faraday bags act as large external antenna and intercept radio waves, thus redirecting radio signal from the mobile device. That is, it prevents reception or sending of data and isolates the device. In mobile forensics environment, device isolation is the first step on arrival at investigation scene;
- SIM card reader;
- Connection cables for mobiles with computer and battery chargers for mobiles.

Following the seizure of mobile device, validity of data must be ensured, which is achieved by total isolation of mobile device with any type of wireless communication (other mobiles, Bluetooth, WI-Fi or infrared communication with any external device) [20]. This must be achieved, since it cannot be allowed to delete data or potential evidence in investigation. Furthermore, it should be considered that there are devices that can use wireless connection from a safe distance to destroy the mobile phone that is subject to investigation. The isolation process must be performed in order to present data from mobile device before court as valid and with unquestionable integrity. Isolation process of mobile device can be performed in three basic ways:

- Isolating wireless communication by using Faraday bags or jamming devices.
- Switching off the device.
- Placing the device in the air space without any wireless form of communication even though it entails a risk of alteration of data on the mobile device.

Following mobile phone isolation, it is necessary that the battery remains charged to prevent loosing data in the working memory. In the process of tracing necessary data in case of a GSM device, primarily the SIM card is cloned; image is made of the data by using card reader, taking care to prevent writing on original medium.
Following data extraction for the analysis, forensic tools perform find-and-catch sophisticated software functions. When data are extracted from the device itself, the applied procedures do not differ from those used in SIM acquisition.

7. LAW ON ELECTRONIC COMMUNICATION OF THE REPUBLIC OF SERBIA

Parliament of the Republic of Serbia on June 29 2010 adopted Law on electronic communication. It stipulates management, utilization and control over radio-frequency spectrum, protection of users and customers rights, security and integrity of the electronic communication networks and services [1]. This law also provides secrecy of electronic communication, legal interception and data retention, supervision of compliance of this law and measures for violations of this law.

This law caused numerous reactions in the political arena in Serbia due to the Article 128., which defines that the operator is obliged to keep data on electronic communication for the purposes of investigation, detection of criminal acts and criminal proceedings, in accordance with the law on criminal proceedings, as well as for the protection of national

and public safety of the Republic of Serbia. Public ombudsman, Council for the suppression of corruption and certain legal expert organizations challenge this law indicating that the controversial article 128 violates citizen's rights and their right on privacy of communication. Supporters of this notion highlight the analogy between written and electronic communication i.e. article 41 of the Constitution that guarantees the inviolability of letters. They support that similar law has been rejected by the parliament of the Federal Republic of Germany whereas some states have special regulation regarding surveillance of communication. In order to access the kept data of the providers, in some states the authorization is given by the minister of the secret services or police (Hungary), special parliamentary board, other independent bodies selected by the parliament, while elsewhere internal regulation allows the approval by the chief of service or police, even the local one (UK).

Nevertheless, IT experts consider that communication between two or more state institutions can be timely and protected. The association of informatics of Serbia supports that a center with a judge on call should be established that could instantly receive electronic requests of services for surveillance of communication among citizens and straight reply to their requests. Authenticity of these requests should be guaranteed by encryption. Newly formed state and judicial bodies would be equipped with modern technology that would ensure instant electronic documentation of the entire communication between services and the court, ensuring future supervision of this system.

It is necessary to consider the fact that the price of communication equipment that allows interception and surveillance of electronic communication is currently pretty low and available even to individuals. This equipment can be directly ordered through the internet. Considering the indications that our communication space is being monitored by unauthorized individuals, certain security agencies that promote themselves through internet and foreign secret services, it should be pointed out that the controversial article 128 provides quicker effective work of the secret services in our country. In addition, the primary role of the operators of mobile and stable telephony would be the provision of modern equipment that can prevent unauthorized interception of communication. To date, operators did not have a legal obligation to provide this equipment, which has been violating the privacy of the users of telecommunication services. On the other hand, utilization of kept data on attempted or actual communication provides forensics of mobile devices greater possibility to establish with certainty the authenticity of evidence that will be presented before court.

8. Application of IP Cameras in Digital Forensics

IP (Internet Protocol) camera represents a combination of camera and computer. Camera transmits images through the IP network, allowing authorized users to locally or remotely view, store and manage video signal (packet stream), through a standardized infrastructure of the IP based network [21]. IP camera contains its own IP address, network connection, web server, FTP server, client email, alarm management, programs and other features. IP camera does not require PC connection, since it functions independently and can be placed at any place with an IP connection. Besides video, the network also has other functions and information transmitted by the same network connection. IP camera connected to a network achieves bi-direct link and it is integrated with the rest of the

system to a high level of scalable environment. IP camera communicates with several applications to perform a variety of tasks, such as motion or different video signal streams. Signal transferred by the IP camera is a compressed digital video (stream). The signal is transmitted to the IP based network through the switches.

IP cameras offer several advantages (see Fig. 1): High resolution camera (megapixels) with progressive image scanning, Pan/tilt, zoom, digital input and output through internet protocol together with video and Complete flexibility and scalability.

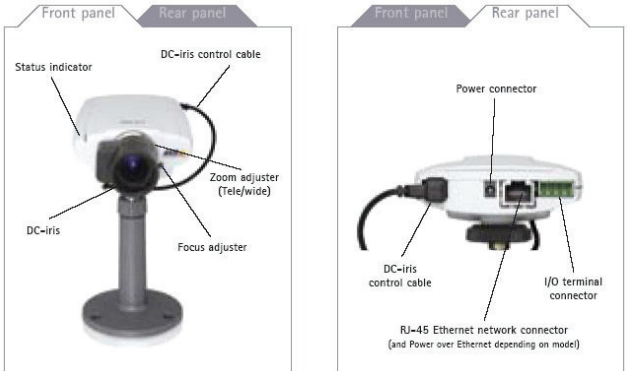

Fig. 1. The appearance of IP cameras that are used in digital forensics.

Fig. 2. Comparison between progressive, interlaced and 2 CIF-based scanning techniques.

Image quality is a key feature of any camera, and it is particularly important in video surveillance and applications of remote monitoring where property and people security are a major factor (see Fig. 2). Network camera performs signal processing, compression and allows network transport. Image quality depends on several factors: Optical selection, Type of image sensor, Power of signal processing and sophistication level of implemented algorithm in the chip. Nowadays, there are two techniques for creating video signal: progressive scanning and semi-image scanning [22]. The selection of the technique depends

on the application and purpose of the video system, in particular when it is expected to capture moving objects and provide visibility of details in motion images.

The image indicates that progressive scanning is the optimal option in video surveillance when it comes to moving objects. When camera detects a moving object, image sharpness depends on the utilized technology. The image shows 4 JPEG images recorded by different cameras using progressive scanning; 4CIF scans of semi-image and 2CIF respectively. The analysis of image indicates: all techniques create clear background image, dented edges due to motion in scanning semi-image, motion blur caused by a lack of resolution in 2CIF example, while only in progressive scanning the driver can be identified. Each digital system of video surveillance uses compression to manage the size of files for storage and viewing that are transmitted through the network. Requested *bandwidth* (wide bandwidth) and data storage demonstrate that non-compressed video is unpractical and expensive which is why compressed technologies are put forward as an effective method to reduce the amount of data sent through the network. Various types of compression are available nowadays. Compressed technology can be owned by a single company that produced and supports it or it may be standardized and supported by multiple companies (see Fig. 3).

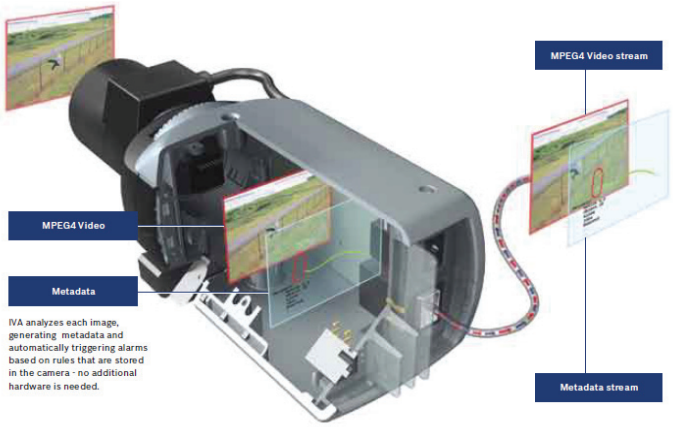

Fig 3. Adequate compression in the process of video surveillance.

The selection of adequate compression is of vital importance for successful installation of video surveillance. Compression of image and video can be performed with loses and without. In case of compression without losses, each pixel is unmodified, so this method offers identical image following decompression. However, in this case, the ration of decompression is very limited. The most common form of compression without loses is GIF. As the ration of compression is limited, these forms are unpractical for the use in network video solutions, where large amount of images is stored and transmitted. Therefore, several methods and standards of compression with loses have been developed. The basic concept is the reduction of objects commonly invisible to human eye and significant extension of the degree of compression. Compression methods also have two approaches: compression of peaceful image and video compression. The standard utilized in the IP cameras is MPEG 4, version 10, H.264.

Groups behind the H.263 and MPEG-4 standards have been united to form new generation of video compression standards. AVC has been developed, known also as H.264 or MPEG-4 version 10 [23]. The intention is to achieve a high degree of data compression. This standard should provide good quality of video at bit rates significantly lower than those required for previous standards, without resulting in unpractical design or expensive installation. This standard represents the future of video surveillance, due to its main features as very quality video at speeds lower than previous standards. In order to achieve the requested performance, a specific hardware is necessary, which is the reason why it is still not prevalent to a larger extent. Primary, it implies very quick and demanding processors that are pretty expensive.

As mentioned, video signal (stream, data) from IP cameras are transmitted through networks. The method of transmission is IP address. IP address (*Internet Protocol Address) represents* a unique number utilized for devices to identify and communicate with each other in a network that uses internet protocol standards.

IPv4, version 4 IP address, addresses are represented with 4 octets (8 bits) separated points, „ .“, with each ranging from 0-255. For example, the address could be „192.36.253.80“. In this version, IP address contains 32 bits, i.e. 4 bytes, which theoretically makes 4 294 967 296 (over 4 billion) unique addresses of home interfaces. In practice, there are insufficient IP addresses available, so there is a pressure to expand the range of addresses through version 6 IP address. IP address is divided into a part of the network and a part of the host. The boundaries of these two parts are determined by the length of prefix or net mask. Net mask 255.255.255.0 means that the first three bytes will be network address while the last byte will be the host address. The length of prefix is a different method of determining these boundaries. For instance, for the same address from the previous example, the length of prefix is 24 bytes (192.36.253.80/24).

Certain address blocks are reserved for domestic use:

- 10.0.0.0/8 (net mask 255.0.0.0),
- 172.16.0.0/12 (net mask 255.240.0.0),
- 192.168.0.0/16 (net mask 255.255.0.0),

These addresses are provided for the private internet. They cannot be routed by the public internet. IPv6, or version 6 of Internet protocol, is developed as advancement in evolution of internet protocol and it will coexist for a while with the old version IPv4. IPv6 is developed to provide constant spreading of the internet by number of connected users (hosts) and by the amount of data that are transmitted. The most noticeable improvement of IPv6 regarding IPv4 is that the IP address is prolonged from 32 bytes to 128 bytes. This extension represents the adjustment to the expected internet growth, providing unlimited (for all purposes and intentions) number of networks and systems. For instance, IPv6 is developed so that there would be a unique address for each phone and mobile electronic device. Due to the aforementioned, it is perceived that the purchase of these IP cameras demands large amount of resources, which is not so expensive in the long term regarding security or digital forensics. Literally, for every location recorded by camera with the events occurring, statistic of events and motion is made and achieved as meta-data (data on data). In order to facilitate the work of individuals monitoring 4 or more cameras concurrently, algorithm for scanning images is implemented in each camera and camera is set to a motion-detection function. In the main server where the cameras are connected, there is a database (meta-data) that camera compares with a moving image

provided on CCD or CMOS chip. Since it is a bi-directional transmission, this communication is quick and easy. The most common method is VCA (Video Content Analysis). Regardless of the number of monitored cameras, this is a serious challenge for the operator. The supervision of the one only monitor for a long time results in fatigue of the brain system and limitation of perception; statistically, after 20 minutes of observing a single monitor, the operator misses around 90% of details on the monitor; this is when the VCA algorithm acts, which is of great importance in digital forensics regarding analysis of certain events (see Fig. 4).

a) b)

Fig. 4. a) Analysis of details on the monitor, b) Tracking speed and direction of target trajectory.

Functioning independently from the central analytic server, each camera can be set differently. It is possible to select advanced image detection from insignificant event to crucial trajectories for surveillance. Live image is constantly observed and it is stored as data steam on a server with hard disks connected in RAID. Events are instantly demonstrated while data is stored for further analysis in case of the alarm. Intelligent video constant analysis (VCA) follows the track of trajectories in image when camera is set to a function motion-detection [24].

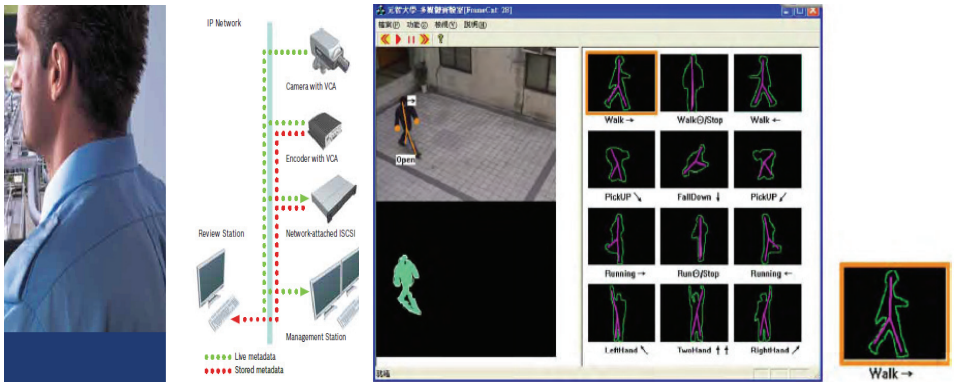

Fig. 5. Software for analysis and comparison of trajectories of any suspicious events.

The VCA algorithm follows the speed and direction of trajectory as well as its form. For example, someone invaded the land for oil processing and activated the alarm; the VCA algorithm in the IP camera constantly follows image motion which is instantly converted into meta-data and sent to a central server. In central server, all meta-data are activated. When it comes to an event that requires employment of digital forensics, as in the given example, forensics will re-configure software for trajectory comparison and analyze any suspicious event provided by software, searching for the desired event that fits the given meta-data trajectory. During comparison, system continues to record on the basis of previously set software, independently from the work of forensics.

REFERENCES

[1] *Law on electronic communication*, Official Gazette of Republic Serbia, No. 44/10, 2010.
[2] P. Stephenson, *Investigating Computer-Related Crime*, CRC Press, Boca Raton, 2000.
[3] Z. Bjelajac, *Cyber crime and internet pedophilia*, University Bussines Academy, Novi Sad, 2011.
[4] S. Ó. Ciardhuáin, *An Extended Model of Cybercrime Investigations*, International Journal of Digital Evidence, Vol. 3, No.1, 2004.
[5] V.N. Pawar, S. N. Talbar, *An Investigation of Significant Object Recognition Techniques*, International Journal of Computer Science and Network Security, Vol. 9, No. 5, pp. 17-29, 2009.
[6] Z. Bjelajac, *Contemporary tendencies in money laundering methods: review of the methods and measures for its suppression*, The Research Institute for European and American Studies RIEAS, No. 151, pp. 13-15, 2011.
[7] J. Robinson, *Internet as the Scene of Crime*, International Computer Crime Conference, Oslo, 2000, www.ccips.org.
[8] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, London, 2000.
[9] Constitution of the Republic of Serbia, *Official Gazette*, No. 98/06.
[10] http://www.echr.coe.int/ECHR/EN/Header/Case-Law/Published+case+law/Citation.
[11] International Organization on Computer Evidence (IOCE), http://www.ioce.org.
[12] B. Carrier, *A Crash Course in Digital Forensics,* Google Docs. Basis Technology Corporation, June 14, 2006, http://www.basistech.com/knowledge-center/forensics/crash-course-in-digital-forensics.pdf.
[13] R. Saferstein, Criminalistics: *An Introduction to Forensic Science*, Pearson / Prentice Hall, Upper Saddle River, NJ. 588, 2004.
[14] J. Cosic, Computer forensics – wide aspects of application, Infotech-Jahorina, Vol. 9, Ref. E-VI-9, p. 857-860, 2010.