Problems of Forensic Sciences 2014, vol. 100, 282–294

ISSN 1230-7483

COMPUTER SCIENCE IN FORENSIC RESEARCH

Bartosz KOWALSKI, Jacek MORAWIEC, Robert RADZISZEWSKI

Institute of Forensic Research, Kraków, Poland

Abstract

In recent years, the emergence of many new technologies in the field of telecommunications has become a major challenge for forensic computer science. The transformation of the mobile phone into a multifunctional smartphone, the full integration of telecommunications services with computer networks and the ubiquity of the Internet, which is not only a source of information, but also a place where data are stored outside local resources in order to hide them – these phenomena mean that methods used up till now are becoming inadequate. Whereas for older models of mobile telephones, it was only possible to establish the telecommunications operator that made the connection in question and the country where it was made, for new models of smartphones, experts are expected to provide the exact route travelled by the given device, projected onto the plan of a city or an area. Much information of a new quality has appeared on data carriers, requiring the development of appropriate methods of access, analysis and presentation. This article attempts to summarise how modern forensic computer science is responding to these challenges.

Key words

Mobile devices; Cloud data storage; Data carriers; Monitoring.

Received 15 September 2014; accepted 24 October 2014

1. Introduction

From the perspective of 2014, the initial years of the twenty-first century may be considered as the best period for forensic computer science – a relatively young field experiencing rapid development during these initial years. In addition to increasing the possibility of recovering statistical data, methods were also developed that allowed us to reconstruct the history of events. Methods for the analysis of Internet events were developed and attention was paid to the importance of the swap file – which is an upgrade of physical memory whose content, despite turning off the computer on which it is located, is not lost. The first decade of this century was characterised by a relatively stable set of hardware and software. The hard drive or drives of a single computer, usually using Microsoft Windows XP, were the main subjects of analysis. The main object of interest was a relatively small set of file formats, usually Microsoft Office documents, image files in JPEG format and videos in AVI and WMV. From the technical side, the type and number of different interfaces were almost unchanged with the predominance of the IDE/ATA interface for drives. Many tools for analysing various data formats were created. The development of forensic computer science methods and tools was faster than changes in hardware and system software. The analysis of mobile phones with a very narrow – from today's perspective – functionality was limited to making copies of existing text messages, address book and call list or recovering deleted call data.

This situation has changed significantly over the last few years (Garfinkel, 2010). The main sources of these changes include:

– The dominance of the USB 2.0 and 3.0 interface as the main method of connecting external devices, and the increasing diversity of these devices. A shift from IDE/ATA to SATA interface for hard drives.
– The rapid growth of hard drive capacity resulting in longer duration of imaging and data analysis. The emergence of a new type of solid-state drives based solely on semiconductor memory has meant the need for a new approach to this type of data carriers.
– A qualitative change in mobile communications associated with the emergence of smartphones – telephones with an extended operating system and functionality comparable to that of personal computers. There has been a rapid development of operating systems such as Apple iOS, Windows Phone, Blackberry and Symbian with an increasingly noticeable lead on the part of Android. Devices have been equipped with many new features such as GPS location, car navigation, camera, video camera, wireless communications and NFC contactless payment.
– The tendency to replace laptops with tablets equipped with GPS communication systems and wireless communications, using their own flash memory or resources available over the Internet instead of the traditional hard disk drive.
– The emergence of a new technology, i.e. cloud computing, which has allowed us both to store our own data on the Internet and use applications running remotely.
– Cloud computing – which is the use of the same network resources from multiple devices – necessitates not only analysing individual devices, but also determining the correlation between them.
– The prevalence of strong encryption systems means data recovery in encrypted form is not in itself sufficient to use these data as evidence.
– The new interfaces and communication systems, especially wireless ones, are exposed to new attacks. Physical access to cables connecting systems is no longer essential. You can remotely capture information transmitted by radio. Especially in the early period, each new interface and new specification includes many loopholes that make it easy to attack. The tendency to regard cybercrimes as the equivalent of physical aggression on their territory by the legal systems of an ever-increasing number of countries shows how dangerous the consequences of these loopholes can be. Disruption of the work of systems of, for example, air traffic control or electrical power can produce effects comparable to a conventional weapons attack.

Of the mentioned advances, the development of smartphones and cloud computing necessitates that new methods be constantly developed for both data access and analysis. There is no standard way to analyse the content of smartphones. Many methods of securing data involve modification of this material evidence. When access through a standard interface does not help, it is necessary to use service links or to de-solder memory chips and read them outside of the phone. Given the number of mobile phone models and their memory chips, this implies a continuing race between new solutions by manufacturers of smartphones and the development of new technology for extracting data from them.

Cloud computing causes the dispersal of data. On a device constituting evidence, you may only find fragments of data that indicate criminal activity, while the most important files may be stored in the cloud. Modern specialised software that supports computer experts is more orientated towards finding a specific file or a record than searching for connections between found data. Existing tools are helpful when searching for files according to pre-set criteria – some are useful for determining if a programme allowing spreading (dissemination) of files around the Internet is installed on the disc, whereas other tools enable you to check whether and when these files were sent. Nevertheless, we lack tools orientated towards detecting specific activity of the user.

The proliferation of data encryption systems and the constant danger of unwanted software installing itself has increased interest in the structure of information in computers' RAM. In particular, the acquisition of an image of such memory when securing a computer before turning it off may significantly speed up data recovery, or even be a pre-requisite for the possibility of recovery from an encrypted disc. In the absence of the memory image, a method called "brute-force attack" can be resorted to, which involves checking all possible combinations. Such an attack only has a chance of succeeding for a limited time (of the order of weeks or months), and if there are relatively short passwords, consisting of a limited set of characters (for example, only lowercase letters of the Latin alphabet).

Later in this article, we present in more detail how modern forensic computer science deals with new problems posed by the developing technology of digital devices.

2. Mobile devices and cloud data storage

In the modern world, a growing demand for all kinds of mobile devices – which are changing everyday life – can be seen. Such devices include mobile phones, especially smartphones, tablets, satellite navigation, video recorders, smart watches and smartbands. As mobile devices become ever more widespread, their importance as evidence increases. This is closely related to the amount of data recorded and stored in the memories of these devices or via them on external data carriers (memory cards, servers, cloud). These data may be qualitatively significant as evidence – for instance, the most recent calls made by a mobile phone, geolocation points recorded by navigation systems, WiFi settings, etc. In the past, mobile phones only recorded information related to their functioning in the GSM network, but now they also record information from navigation and WiFi systems. These data significantly broaden our ability to reconstruct both the way in which a telephone was used and its history (where it was at a given moment, etc.). Mobile devices, especially mobile phones, are characterised by a large variety of solutions. In recent years, this has resulted in the development of new methods of analysis for particular devices and in given types of devices. These methods can be divided into two types on the basis of technical capabilities: logical and physical.

Logical methods involve the analysis of content that is accessible from the device interface, for instance existing contacts, text messages, call history, the history of GPS navigation routes, photos, voice recordings, videos, etc. Advantages of such analysis are the speed and ease of access to the data. Disadvantages are the lack of access to system data and a partial modification of the device memory, for instance, when connecting the phone to the test device *via* Bluetooth.

Physical methods encompass two activities: obtaining an image of the device's memory and analysis of this image. Obtaining a memory image involves additional complications and difficulties, since access to the technical documentation of the equipment is limited or – most frequently – impossible. Hence, the development of an appropriate method is time-consuming, requires specialist knowledge and access to test devices of the same type. In extreme cases, these methods may require permanent modification of the device, for instance, removal of the memory chip from the motherboard of the device. The second range of activities – the analysis of an image of the device's memory – depends on how you get this image. Applying the same method of obtaining the image regardless of the device model can in some cases lead to erroneous results or even make analysis of the memory image impossible. Image analysis at the binary level enables us to reach deleted data. Disadvantages of this analysis are the need for specialist knowledge and equipment, and the time-consuming nature of the activities. The advantage of this method is the ability to analyse memories that have secure access to the device *via* a password, for example, a PIN number or pattern lock, etc.

Currently, for the analysis of mobile devices, forensic computer experts most frequently use systems containing professional hardware and software that support analysis by both logical and physical methods. These solutions include UFED systems by Cellebrite, XRY by Micro Systemation, Oxygen Forensics by Oxygen Forensics Inc. and MOBILEdit by COMPELSON Labs, etc.

UFED and XRY systems are the most comprehensive, as they enable the analysis of various types of mobile devices made by different manufacturers – for instance, mobile phones, GPS, tablets, etc. (Glisson, Strorer, Buchanan-Wollaston, 2013). An additional advantage of these systems is access to a wide range of adapters and cables for connecting to the analysed devices and the possibility of updating the base of supporting devices, which is important in view of the rapidly growing market. Currently, UFED and XRY systems support the analysis of more than 5,000 mobile devices. With the use of these systems, it is also possible to analyse selected devices to which access is blocked by a password. Other systems enable the analysis of a smaller number of devices and are primarily intended for the analysis of mobile phones, including smartphones.

A problem that forensic computer experts currently encounter relates to the overlapping of functionality between groups of devices and the increase in functionality of devices. Smartphones are a good example of this. Smartphones include a range of mobile phone functionality and are most frequently associated with this group. However, thanks to additional features such as satellite navigation, camera, voice recorder, wireless (WiFi, Bluetooth and NFC), smartphones may be linked with other groups of devices. This multifunctional nature affects the diversity and amount of data collected. Considering the fact that the internal memory of these devices is of the order of several gigabytes and most smartphones support external memory cards, up to a size of 128 GB (e.g. Samsung Galaxy S5), we can conclude that they are useful sources of information for courts. Unfortunately, access to these data can very frequently only be obtained after the appropriate decoding of them.

Another concept that has been developed in recent years and has gained in popularity – thanks partly to mobile devices – is the cloud. The concept of the cloud is associated with virtualisation and is usually described as remote access to resources and IT services *via* the Internet. In principle, we can propose a simplified division into public, private and hybrid clouds. While the use of private clouds is limited to a narrow group of users, public clouds are available for many users. Public clouds have a global reach and are available around the clock. Private clouds can have both a local (for instance, own network) and global reach (commercial services), and access to them is limited to selected users. Hybrid clouds are a combination of these two models, i.e., public and private clouds. Each of these clouds can be used for processing data, i.e., cloud computing, or data storage (cloud storage).

Access to the resources of the cloud depends on how it is used. In some cases, it may be access to the infrastructure of servers and data centres (for instance, Microsoft Azure, Amazon EC2, or Oracle Cloud), access to an application (for instance, Google Docs, Microsoft Office Online, etc.), and in other cases – access to disc storage (for instance, DropBox, Google Drive, OneDrive, iCloud, etc.). The most common way of using clouds among private users is to store data. This is most frequently accomplished by synchronizing performed by the user or automatically performed in the background by an application or by saving data directly to disc storage in the cloud by the user or an application. Advantages of clouds are the availability of data, the possibility of synchronisation of data on various devices and the ability to share data with other users.

From the point of view of forensic computer science, clouds are connected with a lot of challenges and problems in the field of data analysis. The data recorded and stored in the memories of devices may not – after some time has passed – be available even for experts using advanced techniques due to the effect of overwriting of the memory. However, thanks to the properties of the cloud it is possible to reach copies of the data. Access to data in clouds is possible from a service provider, if the content is not encrypted by internal mechanisms of the clouds or by third-party programmes. The default settings of programmes that allow you to connect to cloud resources will automatically save the data in the cloud. The devices that use cloud resources, typically by means of dedicated client programmes, retain the information, so you can determine what was transferred and when and where. In some cases, some of the data (for instance, file headers) are saved in the device memory, and access to the whole is achieved only after connection with cloud resources. Mobile devices not only synchronise the data saved by the user, but also the configuration data (for instance WiFi settings), location data (for instance geolocation points), data on the operation of the device (for instance start-up time of the device), etc.

Another problem for judicial bodies is obtaining access to the user's data or files in cloud resources, the existence of which is indicated by traces revealed in the course of analysis. Most popular clouds, such as DropBox, Google Drive, Drive One or iCloud have servers located outside the borders of Poland and thus other regulations apply there (the laws of the country where they are located).

The above mentioned description shows that an expert in the field of forensic computer science, when analysing a device, may only have access to partial information, but this information may still be crucial for explaining the operation of the device and the method of data transfer, and hence how the device was used.

3. Modern data carriers

All the above mentioned devices have built-in memories where the user's operating system and the user's data are stored. In these memories, we can find office documents, movies, music, photographs, correspondence, and much more information.

In recent years, the rapid development of the electronics industry has enabled the miniaturisation of electronic devices that are essential for everyday life. A natural consequence of this has been the development of ever newer and smaller models of data carriers to meet the need to store ever more data. Today, SATA hard drives have gained the greatest popularity in personal computers and servers, and they have replaced the older solutions – ATA/IDE and SCSI. At the same time, solid-state drives and flash drives that use semiconductors to collect information are becoming ever more popular.

In the last few years, the physical size of the disc has decreased, while its capacity has significantly increased. The way in which electronic devices are used has influenced the production of suitable carriers for specific applications. We can distinguish hard drives used for desktops, servers and registrars, and flash memory for digital cameras, mobile phones and USB portable memory. The multitude of solutions applied has created a variety of service systems. Practically each of the standards – SATA, IDE, and USB – requires separate hardware to read the content of their memories. This concerns both the structure of data

carriers and the way of connecting them, and the logical layout of data stored on them. The most versatile data carriers such as hard drives are now produced in versions for a given class of device. One of the producers of this type of equipment marks given series with an individual colour, depending on their application. For example, devices marked green and blue are for home use, mainly for data storage, ones marked red are for file servers, and black are for computing stations. Different hard drives are used in servers and others in video surveillance recorders, despite the fact that they look identical from the outside. The situation with flash memories in the form of memory cards or with USB flash drive is similar. Digital cameras and video cameras need high speed-transmission systems, but not necessarily with a large capacity. In contrast, to transfer data or as an extension of mobile phones' memory, we tend to use models with a higher capacity because the transmission speed is of secondary importance. Increasingly frequently, device manufacturers publish lists of recommended and tested data carriers. Data carriers other than those recommended by the manufacturer sometimes do not work properly with the server, which frequently makes it difficult to analyse the operation of a device which is using a substitute carrier.

It turns out that it is more economical to produce discs of greater capacity. This has led to the widespread use of discs with a storage capacity of several terabytes, wherever there is not a high turnover of data. As a result, once information has been recorded on a given carrier it is still largely recoverable for a long time despite deletion by the user. The high capacity of the carrier allows you to place new data in a previously unused part, which means that data deleted by a user will not be overwritten. In addition, both the devices themselves and modern data carriers have built-in data security systems. So more often than not, the actual space on the data carrier available to the user is smaller than the total capacity of the carrier. When the built-in control system detects read errors in a given area it replaces it with another area. From this moment on information written in an area acknowledged as defective will not be available to the user. Therefore, the user will not be able to modify this data area. The expert, however, may read and analyse these data. However, this requires knowledge of the structure and the software of the data carrier. Specialised equipment designed for this type of carrier is also needed, such as PC-3000 or DeepSpar Disk Imager (Byers, Shahmehri, 2008). Selection of relevant information from among less important information will be the next issue. This in turn requires the use of appropriate software that supports data mining and reporting – for example, X-Ways Forensics or EnCase Forensic.

There are now new possibilities for the recovery of deleted files. An example is the ability to recover a large number of individual fragments of files and to arrange them into a readable whole, based on analysis of the structure of the individual fragments. Experts also have at their disposal software that allows them to search automatically for video or multimedia content that is similar to a given pattern.

Manufacturers of everyday electronic devices, including data carriers, often do not make the technical documentation for produced devices available. In such cases, the expert must frequently interpret the analysed data from the devices based on comparative studies.

Some users protect their data from unauthorised access by encrypting. The available encryption systems, such as TrueCrypt or BitLocker (Kornblum, 2009), are common and effective. Thus, the breaking of such security is sometimes very time-consuming or even impossible to achieve within a reasonable time.

Some data carriers crash or are intentionally damaged by owners who do not want the information stored in them to be revealed. Therefore, systems to recover data from parts of corrupted carriers have been developed (for instance, the PC-3000 system). Recovery mostly involves using de-soldered parts of a carrier that does not function as a whole. For example, the expert de-solders memory modules out of defective USB memories and reads the contents using a special reader, then combines the data of the multiple systems according to an algorithm defined for the device, and only then interprets all data.

At present, monitoring systems are one of many applications of hard drives. The use of fully digital recording may increase the amount of data recorded on carriers in comparison with the previously used systems based on VHS tapes. The application of digital image processing has enabled significant expansion of the capabilities of this system: for instance, now it is possible to play recorded material with continuous recording. Modern monitoring devices may be considered as special computers designed to perform continuous recording of an image sent from connected cameras onto a hard drive (Poole, Zhou, Abatis, 2009). They have a built-in operating system that enables operation of cameras and data carriers that is similar to the systems currently used in desktop computers; however, special versions of carriers are used ever more frequently. These are carriers for the continuous and rapid transfer of large amounts of data. This increases the productivity of the carriers by enabling easy transfer of recordings from the recorder to the

computer, where the material can be freely converted. The image captured by the camera is by its nature an analogue signal, while the recording is in digital form. This recording is performed by the software, which appropriately encodes the information, converting the analogue recording to digital form. At this point, the problem of using different types of recording systems arises. Some manufacturers use recording formats such as MPEG, DIVX and WMV, while others have decided to modify these standards due to licensing restrictions or patent (van Dongen, 2008).

Despite the existence of a series of standards of image recording, manufacturers are using ever newer systems to encode information that are mutually incompatible. These newer coding systems enable storage of more information with minimum use of space on the data carrier. The use of very different and undocumented changes in the way of recording information has become a major problem faced by experts when analysing and recovering data from such devices.

The widespread and frequent use of monitoring systems as an effective preventive tool has resulted in the emergence of a large number of low-cost devices. These devices have practically no technical documentation. Besides, the newer versions of such products are completely incompatible with previous devices in terms of software, structure and connectors, so there is frequently a need to replace the entire system of cameras and accessories. Additionally, some of them crash due to poor quality. This situation makes it very difficult to recover deleted data or data lost from the recording device due to a failure. The lack of documentation makes it necessary to analyse the structure of the recording from scratch. It is frequently necessary to determine whether a loss or momentary loss of a recording has occurred because of equipment failure or because of deliberate action on the part of the user. To solve these sorts of problems, it is necessary to evaluate the operation of such equipment by operating a test recorder, preferably of the same type as the evidential recorder. To retrieve lost recordings, it is frequently necessary to write – based on conclusions from the testing – your own programmes, which will allow you to rebuild the data structure. In a significant number of analyses, this leads to recovery of the lost recordings. It sometimes happens that recordings recovered in this way have the incorrect date and time. This makes it necessary to verify whether you have the right recordings but with the wrong date and time, or whether they are completely different recordings.

The use of a digital recording system has enabled the transmission of video over the Internet in real time. Damage to the recording system itself is not necessarily tantamount to loss of recorded data, because copies of the data may be archived in a remote centre or in a cloud. The high resolution of digital recordings allows you to recover more details from images. This increases the chance of identifying persons and objects. Specialised programmes that support the work of the expert make it possible to measure the size of persons and objects, taking into consideration the distortion resulting from the angle of the camera.

4. Conclusions

In recent years, forensic computer science has been forced to face new challenges in the form of new devices and new types of encoding and recording of information. There has been distinct progress – which allows us to meet these challenges – in areas such as: searching for and recovering deleted image and video files, access to data in the memory of smartphones, recognition of new formats of data stored there and ways of presenting them. Techniques for recovering data from memory chips that have been de-soldered from a device – which are used when other methods have failed – have been developed. In the era of full integration of local area networks with the Internet and mobile telephony, methods of determining where to look for relevant data require further research. Apart from technical problems, legal regulations regarding access to data, for instance in the cloud, are becoming ever more important. Strong encryption systems, which are increasingly being used, are a major obstacle to interpreting recovered data.

A new development regarding programmes supporting the work of the computer expert is first attempts at not only finding pieces of information, but also ascertaining their association with each other (for instance, software presenting a diagram of the connections between people based on call lists and address data recovered from multiple phones). In view of the ever-increasing amount of data to be analysed, it has become necessary to develop tools that not only allow you to search for a single piece of information, but are also able to group information logically.

References

1. Byers, D., Shahmehri, N. (2008). Contagious errors: Understanding and avoiding issues with imaging drives containing faulty sectors. *Digital Investigation*, *5*(1), 29–33.
2. Garfinkel, S. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*, S64–S73.

3. Glisson, W. B., Strorer, T., Buchanan-Wollaston J. (2013). An empirical comparison of data recovered from mobile forensic toolkits. *Digital Investigation*, *10*(1), 44–45.
4. Kornblum, J. D. (2009). Implementing BitLocker Drive Encryption for forensic analysis. *Digital Investigation*, *5*(2–3), 75–84.
5. Poole, N. R., Zhou, Q., Abatis, P. (2009). Analysis of CCTV digital video recorder hard disk storage system. *Digital Investigation*, *5*(2–3), 85–92.
6. van Dongen, W. S. (2008). Case study: Forensic analysis of Samsung digital video recorder. *Digital Investigation*, *5*(1), 19–28.

Corresponding author
Bartosz Kowalski
Instytut Ekspertyz Sądowych
ul. Westerplatte 9
PL 31-033 Kraków
e-mail: bkowalski@ies.gov.pl

Problems of Forensic Sciences 2014, vol. 100, 282–294

INFORMATYKA W EKSPERTYZIE KRYMINALISTYCZNEJ

1. Wstęp

Z perspektywy roku 2014 początkowe lata XXI wieku można uznać za najlepsze lata informatyki sądowej, dziedziny stosunkowo młodej i przeżywającej gwałtowny rozwój w tym okresie. Oprócz coraz większych możliwości odzyskiwania danych statycznych pojawiły się również metody, które pozwalały także odtworzyć historię zdarzeń. Opracowywano metody jej analizy w sieci, jak również zwrócono uwagę na znaczenie tzw. pliku wymiany będącego rozszerzeniem fizycznej pamięci, którego zawartość, mimo wyłączenia komputera, nie ulega utracie. Pierwsza dekada bieżącego wieku charakteryzowała się stosunkowo stabilnym zestawem urządzeń i programów. Obiektem analiz był głównie dysk lub dyski pojedynczego komputera, najczęściej pracującego w systemie Microsoft Windows XP. Głównym przedmiotem zainteresowania był stosunkowo niewielki zestaw formatów plików, zazwyczaj dokumenty Microsoft Office, pliki graficzne w formacie JPEG i filmowe w formacie AVI i WMV. Od strony technicznej rodzaj i liczba różnych interfejsów była prawie niezmienna z dominacją interfejsu IDE/ATA dla dysków. Powstało wiele narzędzi przeznaczonych do analizy poszczególnych formatów danych. Rozwój metod i narzędzi informatyki sądowej był szybszy niż zmiany sprzętu i oprogramowania systemowego. Analiza telefonów komórkowych o bardzo wąskiej – z dzisiejszej perspektywy – funkcjonalności ograniczała się do wykonania kopii istniejących SMS-ów, książki adresowej i wykazu połączeń lub ich odzyskania, gdy zostały usunięte.

Ten obraz uległ istotnej zmianie w ciągu ostatnich kilku lat (Garfinkel, 2010). Główne źródła tych zmian to:

- Dominacja interfejsu USB 2.0 i 3.0 jako głównego sposobu podłączania urządzeń zewnętrznych oraz coraz większa różnorodność tych urządzeń. Odejście od interfejsu IDE/ATA na rzecz interfejsu SATA w przypadku dysków twardych.
- Szybki wzrost pojemności dysków twardych powodujący wydłużenie czasu tworzenia obrazów i analizy danych. Pojawienie się nowego typu dysków SSD, opartych wyłącznie o pamięci półprzewodnikowe, oznaczał konieczność nowego podejścia do tego typu nośników danych.
- Jakościowa zmiana w telefonii komórkowej związana z pojawieniem się smartfonów – telefonów z rozbudowanym systemem operacyjnym i funkcjonalnością porównywalną z funkcjonalnością komputerów osobistych. Nastąpił szybki rozwój systemów operacyjnych, takich jak Apple iOS, Windows Phone, Blackberry czy Symbian z coraz wyraźniej zauważalną przewagą systemu Android. Urządzenia wyposażone zostały w wiele nowych funkcji, takich jak lokalizacja GPS, nawigacja samochodowa, aparat fotograficzny, kamera, łączność bezprzewodowa i płatność zbliżeniowa NFC.
- Tendencja do zamiany laptopów na tablety wyposażone w systemy łączności GPS i łączności bezprzewodowej, wykorzystujące zamiast tradycyjnego dysku twardego własną pamięć *flash* lub zasoby dostępne przez sieć.
- Pojawienie się nowej technologii, tzw. przetwarzanie w chmurze (ang. cloud computing), która umożliwiła zarówno przechowywanie własnych danych w sieci, jak i korzystanie z aplikacji uruchamianych zdalnie.
- Przetwarzanie w chmurze, korzystanie z tych samych zasobów sieciowych z wielu urządzeń oznacza konieczność analizy nie tylko pojedynczych urządzeń, ale także ustalenia korelacji między nimi.
- Rozpowszechnienie się silnych systemów szyfrowania powoduje, że samo odzyskanie danych w postaci zaszyfrowanej nie wystarcza, by można z nich skorzystać dowodowo.
- Nowe interfejsy oraz systemy łączności, w szczególności łączności bezprzewodowej, stwarzają nowe zagrożenia atakiem. Nie jest już konieczny fizyczny dostęp do przewodów łączących systemy informatyczne. Można zdalnie przechwycić informację przekazywaną drogą radiową. Każdy nowy interfejs, nowa specyfikacja zawiera, szczególnie w początkowych okresie, szereg luk, które ułatwiają atak. Jak groźne mogą być ich następstwa, świadczy tendencja do uznawania cyberprzestępczości w prawodawstwie wciąż rosnącej liczby państw za równoważne z fizyczną agresją na jego terytorium. Zakłócenie pracy systemów np. kontroli lotów lub systemu energetycznego może wywołać skutki porównywalne z atakiem bronią konwencjonalną.

Z wymienionych zmian rozwój smartfonów i przetwarzanie w chmurze wymuszają ciągłe opracowywanie nowych metod zarówno dostępu do danych, jak i ich analizy. Nie ma standardowego sposobu na analizę zawartości smartfonu. Aby zabezpieczyć dane, wiele metod musi zakładać konieczność modyfikacji tego dowodu rzeczowego. Gdy dostęp przez standardowy interfejs nie daje rezultatu, konieczne jest użycie łączy serwisowych lub wylutowanie układów pamięci i odczytanie ich poza telefonem. Biorąc pod uwagę liczbę modeli telefonów i układów pamięci w nich zawartych, implikuje to ciągły wyścig między nowymi rozwiązaniami producentów

smartfonów i rozwojem nowych technologii odzyskiwania z nich danych.

Przetwarzanie w chmurze powoduje rozproszenie danych. Na dowodowym urządzeniu można stwierdzić tylko fragmenty danych świadczących o przestępczej działalności, a najistotniejsze pliki mogą być zapisane w chmurze. Obecne oprogramowanie specjalistyczne wspomagające biegłego informatyka jest bardziej ukierunkowane na znalezienie konkretnego pliku lub zapisu niż na wspomaganie procesu analizy polegającej na powiązaniu znalezionych danych. Istniejące narzędzia są pomocne przy szukaniu plików według zadanych kryteriów – jedne w ustaleniu, czy na dysku jest zainstalowany program, który pozwala je rozpowszechniać w sieci, jeszcze inne umożliwiają stwierdzenie, czy i kiedy pliki te zostały wysłane do internetu. Brakuje natomiast narzędzi ukierunkowanych na wykrycie konkretnej aktywności użytkownika.

Rozpowszechnienie się systemów szyfrowania danych oraz stałe zagrożenie zainstalowaniem się niechcianego oprogramowania zwiększyło zainteresowanie strukturą informacji w pamięci RAM komputera. W szczególności pozyskanie obrazu takiej pamięci w trakcie zabezpieczania komputera, przed jego wyłączeniem, może istotnie przyśpieszyć odzyskanie danych lub wręcz przesądzić o możliwości ich odzyskania z zaszyfrowanego dysku. Przy braku obrazu pamięci pozostaje metoda tzw. „ataku brutalnego" polegającego na sprawdzaniu wszystkich możliwych kombinacji. Taki atak, w ograniczonym czasie (rzędu tygodni czy miesięcy), ma szanse powodzenia tylko przy stosunkowo krótkich hasłach i składających się z ograniczonego zbioru znaków (np. wyłącznie małe litery alfabetu łacińskiego).

W dalszej części artykułu przedstawiono bardziej szczegółowo, jak współczesna informatyka sądowa radzi sobie z nowymi problemami stwarzanymi przez rozwój technologii urządzeń cyfrowych.

2. Urządzenia mobilne i chmury danych

We współczesnym świecie można zauważyć rosnące zapotrzebowanie na różnego rodzaju urządzenia mobilne, które zmieniają codzienne życie. Do takich urządzeń należą telefony komórkowe, a zwłaszcza smartfony, tablety, nawigacje satelitarne, rejestratory wideo, inteligentne zegarki typu smartwatch czy opaski typu smartband. Wraz z popularyzacją urządzeń mobilnych rośnie ich znaczenie w postępowaniu dowodowym. Ma to ścisły związek z liczbą danych zapisywanych i przechowywanych w pamięciach tych urządzeń lub za ich pomocą na zewnętrznych nośnikach danych (karty pamięci, serwery, chmury). Dane te pod względem jakościowym mogą mieć znaczącą wartość dowodową, np. ostatnio wykonane połączenia telefonem komórkowym, zapisane punkty geolokalizacji z systemów nawigacji, ustawienia sieci WiFi itp. W przeszłości w telefonie komórkowym zapisywane były tylko informacje związane z jego funkcjonowaniem w sieci GSM, natomiast obecnie zapisywane są dodatkowo informacje pochodzące z systemów nawigacji i łączności WiFi. Dane te znacząco poszerzają możliwość zarówno odtworzenia sposobu użytkowania telefonu, jak i jego historii (gdzie znajdował się w danym czasie itp.). Urządzenia mobilne charakteryzuje duża różnorodność rozwiązań w każdym z wymienionych typów urządzeń, co najbardziej widać na przykładzie telefonów komórkowych. W ostatnich latach przyczyniło się to do opracowania nowych metod analizy dla poszczególnych urządzeń, także w danym typie urządzeń. Metody te ze względu na możliwości techniczne można podzielić na dwa rodzaje – logiczne i fizyczne.

Metody logiczne sprowadzają się do analizy zawartości, która jest dostępna z poziomu interfejsu urządzenia, np. istniejące kontakty, wiadomości tekstowe, historia połączeń, przebyte trasy z nawigacji GPS, dostępne zdjęcia, nagrania głosowe, nagrania wideo itp. Zaletą tego typu analizy jest szybkość i łatwość dostępu do danych. Wadą jest brak dostępności do danych systemowych oraz częściowa modyfikacja pamięci urządzenia, np. ustawienie połączenia telefonu z urządzeniem badawczym *via* protokół Bluetooth.

W metodach fizycznych można wskazać dwa zakresy działań, tj. uzyskanie obrazu pamięci urządzenia oraz analiza tego obrazu. Uzyskanie obrazu pamięci niesie dodatkowe komplikacje i trudności, ponieważ dostęp do dokumentacji technicznej urządzeń jest ograniczony, a najczęściej niemożliwy. Stąd też opracowanie odpowiedniej metody jest czasochłonne, wymaga wiedzy specjalistycznej oraz dostępu do urządzeń testowych tego samego typu. Metody te w skrajnych przypadkach mogą wymagać trwałej modyfikacji urządzenia, np. wymontowania układu pamięci z płyty głównej urządzenia. Drugi zakres działań, czyli analiza obrazu pamięci urządzenia, jest uzależniona od sposobu uzyskania tego obrazu. Zastosowanie tego samego sposobu wykonania obrazu niezależnie od modelu urządzenia może w niektórych sytuacjach prowadzić do błędnych wyników lub nawet braku możliwości przeanalizowania obrazu pamięci. Analiza obrazu na poziomie binarnym umożliwia dotarcie do usuniętych danych. Wadą takiej analizy jest konieczność posiadania wiedzy i sprzętu specjalistycznego oraz czasochłonność działań. Zaletą metody fizycznej jest możliwość analizy pamięci, które mają zabezpieczony dostęp do urządzenia poprzez ustawione hasła, np. kod PIN lub wzorzec (ang. pattern lock) itp.

Aktualnie biegli z zakresu informatyki sądowej do analizy urządzeń mobilnych najczęściej wykorzystują systemy zawierające profesjonalne urządzenia i oprogramowanie, które wspierają analizę zarówno metodami logicznymi, jak i fizycznymi. Do powyższych rozwiązań

należy zaliczyć systemy UFED firmy Cellebrite, XRY firmy Micro Systemation, Oxygen Forensics firmy Oxygen Forensics Inc. oraz MOBILEdit firmy COMPELSON Labs itp.

Systemy UFED i XRY są najbardziej rozbudowane, gdyż umożliwiają analizę urządzeń mobilnych różnych producentów i różnego przeznaczenia, np. telefonów komórkowych, nawigacji GPS, tabletów itp. (Glisson, Strorer, Buchanan-Wollaston, 2013). Dodatkowymi zaletami tych systemów jest dostęp do szerokiej gamy adapterów i przewodów umożliwiających podłączenie analizowanych urządzeń oraz możliwość uaktualnienia bazy wspierających urządzeń, co przy tak dynamicznie rozwijającym się rynku ma duże znaczenie. Aktualnie systemy UFED i XRY wspierają analizę ponad 5000 urządzeń mobilnych. Z wykorzystaniem tych systemów istnieje również możliwość analizy wybranych urządzeń, do których dostęp jest zablokowany poprzez ustawione hasło. Pozostałe systemy umożliwiają badanie mniejszej liczby urządzeń i przeznaczone są głównie do analizy telefonów komórkowych, w tym smartfonów.

Problem, z jakim obecnie spotykają się biegli z zakresu informatyki sądowej, dotyczy przenikania funkcjonalności pomiędzy grupami urządzeń oraz zwiększania funkcjonalności urządzeń. Dobrym przykładem takiego stanu rzeczy są urządzenia typu smartfon. Smartfon obejmuje zakres funkcjonalności telefonu komórkowego i z tą grupą najczęściej jest kojarzony. Jednakże jego dodatkowe funkcje, takie jak nawigacja satelitarna, aparat fotograficzny, dyktafon, łączność bezprzewodowa (WiFi, Bluetooth i NFC) powoduje, że można go powiązać również z innymi grupami urządzeń. Ta wielofunkcyjność ma wpływ na różnorodność i liczbę gromadzonych danych. Biorąc pod uwagę fakt, że pamięć wewnętrzna tych urządzeń średnio oscyluje na poziomie kilku gigabajtów i większość smartfonów umożliwia obsługę zewnętrznych kart pamięci, nawet do wielkości 128 GB (np. Samsung Galaxy S5), można stwierdzić, że jest to źródło informacji użytecznej procesowo. Niestety bardzo często zdarza się, że dostęp do tych danych można uzyskać dopiero po odpowiednim ich zdekodowaniu.

Kolejnym pojęciem, które powstało w ostatnich latach i zyskało na popularności, również dzięki urządzeniom mobilnym, są tzw. chmury. Pojęcie chmury związane jest z wirtualizacją i opisuje się je zazwyczaj jako zdalny dostęp do zasobów i usług informatycznych poprzez internet. Zasadniczo można pokusić się o uproszony podział na chmury publiczne, prywatne i hybrydowe. O ile zastosowanie chmur prywatnych jest ograniczone do wąskiego grona odbiorców, o tyle chmury publiczne są dostępne dla wielu użytkowników. Chmury publiczne mają zasięg globalny i są dostępne w cyklu całodobowym. Chmury prywatne mogą mieć zarówno zasięg lokalny (np. sieć własna), jak i globalny (usługi komercyjne), a dostęp do nich jest ograniczony do wybranych użytkowników. Chmury hybrydowe są połączeniem dwóch modeli, tj. chmury publicznej i prywatnej. Każda z tych chmur może być wykorzystana do przetwarzania danych (ang. cloud computing) lub tylko do przechowywania danych (ang. cloud storage).

Dostęp do zasobów chmur zależy od sposobu jej wykorzystania. W niektórych przypadkach może to być dostęp do infrastruktury z serwerami i centrami danych (np. Microsoft Azure, Amazon EC2, Oracle Cloud), dostęp do aplikacji (np. Google Docs, Microsoft Office Online, itp.), a w innych dostęp do pamięci dyskowej (np. DropBox, Google Drive, OneDrive, iCloud itp.). Najbardziej rozpowszechniony sposób wykorzystywania chmur wśród użytkowników prywatnych to przechowywanie danych. Najczęściej realizowane jest to poprzez synchronizację wykonaną przez użytkownika albo przeprowadzaną w tle automatycznie przez aplikację lub zapisywanie danych bezpośrednio na pamięć dyskową w chmurze przez użytkownika lub aplikację. Zaletą stosowania chmur jest dostępność danych, możliwość synchronizacji danych na różnych urządzeniach oraz możliwość współdzielenia danych z innymi użytkownikami.

Z punktu widzenia informatyki sądowej chmury niosą ze sobą dużo wyzwań i problemów w zakresie analizy danych. Dane zapisywane i przechowywane w pamięci urządzeń z czasem mogą nie być dostępne nawet dla biegłych wykorzystujących zaawansowane techniki ze względu na efekt nadpisywania tejże pamięci. Jednakże dzięki właściwościom chmury można dotrzeć do ich kopii. Dostęp do danych w chmurach jest możliwy z poziomu dostarczyciela usługi, o ile te treści nie są szyfrowane, z wykorzystaniem wewnętrznych mechanizmów chmury lub programów firm trzecich. Ustawienia standardowe programów, które umożliwiają połączenie z zasobami chmury, powodują automatyczne zapisanie danych w chmurze. Urządzenia, które korzystają z zasobów chmury, zazwyczaj z wykorzystaniem dedykowanych programów klienckich, zachowują w pamięci informacje, dzięki którym można ustalić kiedy, co i gdzie zostało transferowane. W niektórych przypadkach zdarza się, że część danych (np. nagłówki plików) są zapisywane w pamięci urządzenia, a dostęp do całości uzyskuje się dopiero po połączeniu z zasobami chmury. Urządzenia mobilne nie tylko synchronizują dane zapisane przez samego użytkownika, ale również dane konfiguracyjne (np. ustawienia sieci WiFi), dane lokacyjne (np. punkty geolokacji), dane dotyczące funkcjonowania urządzenia (np. czas uruchomienia urządzenia) itp.

Osobnym problemem jest uzyskanie przez organ procesowy dostępu do danych lub plików użytkownika w zasobach chmury, na których istnienie wskazują ślady ujawnione w trakcie ekspertyzy. Większość popularnych chmur, takich jak DropBox, Google Drive, One Drive czy iCloud ma serwery umieszczone poza granicami na-

szego kraju, a co za tym idzie, zastosowanie mają inne regulacje prawne (państwa, w jakim są ulokowane).

Z powyższego opisu wynika, że biegły z zakresu informatyki sądowej, analizując urządzenie, może mieć dostęp tylko do cząstkowych informacji, jednakże te informacje i tak mogą być kluczowe do wyjaśnienia sposobu działania urządzenia i sposobu transferu danych, a zatem do informacji, w jaki sposób urządzenie było wykorzystywane.

3. Współczesne nośniki danych

Wszystkie urządzenia, o których była mowa powyżej, posiadają wbudowaną pamięć, w której przechowywany jest system operacyjny oraz dane użytkownika. Znajdziemy w nich dokumenty biurowe, filmy, muzykę, fotografie, korespondencję i wiele innych informacji.

Szybki rozwój przemysłu elektronicznego na przestrzeni ostatnich lat pozwolił na miniaturyzację urządzeń elektronicznych niezbędnych w życiu codziennym. Naturalną konsekwencją było opracowanie coraz nowszych i mniejszych modeli nośników, by sprostać potrzebie przechowywania coraz to większej liczby danych. Obecnie w komputerach osobistych i serwerach największą popularność osiągnęły dyski twarde typu SATA, które zastąpiły starsze rozwiązania typu ATA/IDE oraz SCSI. Jednocześnie coraz większą popularność zdobywają dyski SSD oraz pamięci typu *flash* wykorzystujące półprzewodniki do gromadzenia informacji.

W przeciągu kilku ostatnich lat zmniejszyła się fizyczna wielkość dysku, a jednocześnie znacznie zwiększyła jego pojemność. Sposób wykorzystania urządzeń elektronicznych ukierunkował produkcję odpowiednich nośników do poszczególnych zastosowań. Można wyróżnić dyski twarde stosowane do komputerów biurowych, serwerów, rejestratorów oraz pamięci *flash* do aparatów i kamer cyfrowych, telefonów komórkowych czy do pamięci przenośnych USB. Mnogość stosowanych rozwiązań spowodowała powstanie różnych systemów ich obsługi. Praktycznie każdy ze standardów SATA, IDE, USB wymaga osobnego sprzętu do odczytania zawartości ich pamięci. Mówimy tutaj zarówno o konstrukcji i sposobie podłączania nośnika, jak i logicznej organizacji zapisanych na nich danych. Najbardziej uniwersalne nośniki, jak dyski twarde, są już produkowane w wersjach przeznaczonych dla urządzeń danej klasy. Jeden z producentów tego typu urządzeń poszczególne serie oznacza kolorami w zależności od zastosowania. Dla przykładu oznaczone kolorem zielonym i niebieskim to urządzenia przeznaczone do użytku domowego, głównie do przechowywania danych, oznaczone kolorem czerwonym do serwerów plików, a czarnym do stacji obliczeniowych. Inne dyski stosuje się w serwerach, a inne w rejestratorach monitoringu wizyjnego, mimo że z zewnątrz wyglądają identycznie. Podobnie jest z pamięciami typu *flash* w postaci kart pamięci czy pamięci USB. Do aparatów i kamer cyfrowych potrzebne są układy o dużej szybkości transmisji, a niekoniecznie o dużej pojemności. Natomiast do przenoszenia danych czy jako rozszerzenie pamięci telefonów komórkowych raczej stosuje się modele o większej pojemności, gdyż szybkość transmisji ma drugorzędne znaczenie. Coraz częściej producenci urządzeń publikują listę zalecanych i przetestowanych nośników. Zdarza się, iż inne niż zalecane przez producenta nośniki nie współpracują poprawnie z serwerem, co niejednokrotnie utrudnia analizę działania urządzenia z wykorzystaniem nośnika zamiennego.

Okazuje się, że bardziej ekonomicznie jest produkować dyski o większej pojemności. Spowodowało to powszechne stosowanie dysków o pojemności rzędu kilku terabajtów, wszędzie tam, gdzie nie ma dużej rotacji danych. W efekcie tego informacje raz zapisane na danym nośniku, pomimo ich skasowania przez użytkownika, przez dłuższy czas są jeszcze w znacznym stopniu do odzyskania. Duża pojemność nośnika pozwala na umieszczenie nowych danych w obszarze uprzednio niewykorzystanym, co powoduje, że dane usunięte przez użytkownika nie są nadpisywane. Ponadto same urządzenia, jak i nowoczesne nośniki, mają wbudowane systemy bezpieczeństwa danych. Najczęściej polega to na tym, że rzeczywista dostępna dla użytkownika ilość miejsca na nośniku jest mniejsza od fizycznej pojemności nośnika. Wbudowany system zarządzania w przypadku wykrycia błędów odczytów w danym obszarze zastępuje go innym. Od tego momentu informacja zapisana w obszarze uznanym za uszkodzony nie będzie dostępna dla użytkownika. Użytkownik zatem nie będzie miał możliwości modyfikacji tego obszaru danych. Biegły może jednak te dane odczytać i poddać analizie. Wymaga to jednak znajomości budowy nośnika i działania jego mikroprogramowania. Konieczny jest też specjalistyczny sprzęt przeznaczony do danego rodzaju nośnika, taki jak PC-3000 czy DeepSpar Disk Imager (Byers, Shahmehri, 2008). Następnym problemem będzie wyselekcjonowanie istotnej informacji spomiędzy tych mniej ważnych. To z kolei wymaga zastosowania odpowiedniego oprogramowania wspomagającego wyszukiwanie danych i raportowanie, np. X-Ways Forensics czy EnCase Forensic.

Powstały nowe możliwości odzyskiwania usuniętych plików graficznych. Przykładem jest możliwość odzyskania dużej liczby pojedynczych fragmentów plików i ułożenie ich w czytelną całość, bazując na analizie struktury poszczególnych fragmentów. Biegły ma również do dyspozycji oprogramowanie pozwalające na automatyczne wyszukiwanie treści graficznej czy multimedialnej podobnej do zadanego wzorca.

Producenci urządzeń elektronicznych codziennego użytku, w tym nośników danych, często nie udostępniają dokumentacji technicznej wytwarzanych urządzeń.

W takim przypadku biegły niejednokrotnie musi dokonać interpretacji danych z analizowanych urządzeń na podstawie przeprowadzonych badań porównawczych.

Część użytkowników zabezpiecza swoje dane przed nieuprawnionym dostępem poprzez szyfrowanie. Dostępne systemy szyfrowania, jak TrueCrypt czy BitLocker (Kornblum, 2009), są powszechne i skuteczne. Przełamanie takich zabezpieczeń bywa więc bardzo czasochłonne lub wręcz niemożliwe do wykonania w racjonalnym czasie.

Pewna część nośników ulega awarii bądź jest celowo uszkadzana, gdy właściciel nie chce, aby informacje w nich zapisane zostały ujawnione. Opracowano zatem systemy do odzyskiwania danych z pojedynczych elementów uszkodzonych nośników (np. system PC-3000). Odbywa się to najczęściej z wykorzystaniem wylutowanych części nośnika, który jako całość nie funkcjonuje. Na przykład z uszkodzonych pamięci USB wylutowuje się moduły pamięci i odczytuje ich zawartość za pomocą specjalnych czytników, a następnie łączy dane według ustalonego dla danego urządzenia algorytmu z kilku układów w całość i dopiero wtedy interpretuje.

Jednym z zastosowań dysków twardych są obecnie systemy monitoringu. Zastosowanie w pełni cyfrowego zapisu pozwala zwiększyć ilość rejestrowanego materiału na nośniku w stosunku do stosowanego wcześniej systemu opartego o kasety VHS. Zastosowanie cyfrowego przetwarzania obrazu pozwoliło znacznie zwiększyć możliwości tego systemu, np. realne stało się odtwarzanie zarejestrowanego materiału z zachowaniem ciągłości rejestrowania. Nowoczesne urządzenia monitorujące można traktować jako specjalne komputery przystosowane do wykonywania ciągłego zapisu na dysku twardym obrazu rejestrowanego przez podłączone kamery (Poole, Zhou, Abatis, 2009). Mają one wbudowany system operacyjny pozwalający na obsługę kamer oraz nośników danych podobny jak stosowane obecnie w komputerach biurowych, jednakże coraz częściej używa się specjalnych wersji nośników. Są to nośniki przeznaczone do pracy ciągłej oraz szybkiego transferu dużej liczby danych. Pozwala to na zwiększenie wydajności nośników poprzez umożliwienie łatwego przenoszenia zapisów z rejestratora do komputera, na którym można taki materiał dowolnie przetwarzać. Obraz rejestrowany przez kamery jest z natury rzeczy sygnałem analogowym, zapis natomiast jest realizowany w formie cyfrowej. Zadanie to dokonywane jest przez oprogramowanie, które odpowiednio koduje informacje, przetwarzając zapis analogowy na cyfrowy. Tutaj pojawia się problem stosowania różnego rodzaju systemów zapisu. Jedni producenci korzystają ze standardów zapisu takich jak MPEG, DIVX czy WMV. Inni decydują się na modyfikacje powyższych standardów ze względu na ograniczenia licencyjne czy patentowe (van Dongen, 2008).

Producenci pomimo istnienia szeregu standardów zapisu obrazu stosują coraz to nowsze systemy kodowania informacji, wzajemnie niezgodne. Te nowsze systemy kodowania pozwalają na zapisanie większej liczby informacji przy minimalnym wykorzystaniu przestrzeni nośnika danych. Użycie bardzo różnych i nieudokumentowanych zmian w sposobie zapisu informacji stało się obecnie głównym problemem, z jakim spotykają się biegli przy analizie i odzyskiwaniu danych z takich urządzeń.

Powszechne i częste stosowanie systemów monitoringu jako skutecznego środka prewencyjnego spowodowało pojawienie dużej liczby tanich urządzeń. Urządzenia te praktycznie pozbawione są jakiejkolwiek dokumentacji technicznej. Poza tym nowsze wersje takich produktów są całkowicie niekompatybilne z poprzednimi pod względem oprogramowania, konstrukcji i złącz, co niejednokrotnie wymaga wymiany całego systemu kamer i akcesoriów. Dodatkowo część z nich ulega awariom spowodowanym niską jakością wykonania. Taki stan rzeczy bardzo utrudnia odzyskanie skasowanych bądź utraconych wskutek awarii danych z urządzenia rejestrującego. Brak dokumentacji powoduje konieczność analizowania od podstaw struktury zapisu. Często również zachodzi potrzeba ustalenia, czy utrata lub chwilowy zanik rejestracji wystąpił wskutek awarii urządzenia, czy celowego działania użytkownika. Niezbędna do rozwiązania tego typu problemów jest ocena działania takiego urządzenia poprzez uruchomienie testowe rejestratora, najlepiej tego samego typu, co dowodowy. Niejednokrotnie, aby uzyskać utracone zapisy, konieczne jest napisanie, na podstawie wniosków wyciągniętych z przeprowadzanych testów, własnych programów, które pozwolą odbudować strukturę danych. W znacznej liczbie ekspertyz prowadzi to do odzyskania utraconych nagrań. Zdarza się, że tak odzyskane nagrania mają niewłaściwą datę i czas. Powoduje to konieczność weryfikacji, czy są to właściwe nagrania, a tylko dane dotyczące daty i czasu są niewłaściwe, czy są to zupełnie inne nagrania.

Zastosowanie cyfrowego systemu rejestracji dało możliwość transmisji obrazu przez sieć internetową w czasie rzeczywistym. Zniszczenie samego systemu rejestracji nie musi być równoważne z utratą zarejestrowanych nagrań, ponieważ ich kopia może być archiwizowana w zdalnym ośrodku lub w chmurze. Duża rozdzielczość cyfrowego zapisu pozwala na odzyskanie z obrazu większej liczby szczegółów. Zwiększa to szansę identyfikacji osób i przedmiotów. Specjalistyczne programy wspomagające pracę biegłego dają możliwość zmierzenia wymiarów osób i przedmiotów, uwzględniając zniekształcenia wynikające z kąta ustawienia kamery.

4. Podsumowanie

W ostatnich latach informatyka sądowa musiała zmierzyć się z nowymi wyzwaniami w postaci nowych urządzeń, rodzajów kodowania i zapisu informacji. W takich dziedzinach jak wyszukiwanie i odzyskiwanie usuniętych plików graficznych i filmowych, dostęp do danych w pamięci smartfonów, rozpoznanie nowych formatów danych tam zapisywanych i sposobów ich prezentacji nastąpił wyraźny postęp, który pozwala sprostać tym wyzwaniom. Dopracowane zostały techniki odzyskania danych z wylutowanych z urządzenia układów pamięci, stosowane wtedy, gdy inne metody dostępu zawiodą. W dobie pełnej integracji lokalnych sieci komputerowych z internetem i telefonią komórkową dopracowania wymagają metody pozwalające ustalić, gdzie szukać istotnych danych. Oprócz problemów technicznych, o wiele większego znaczenia nabierają regulacje prawne dotyczące dostępu do danych np. w chmurze. Coraz częściej stosowane systemy tzw. silnego szyfrowania stanowią istotny problem związany z interpretacją odzyskanych danych.

Nową jakością w zakresie programów wspomagających pracę biegłego informatyka są pierwsze próby nie tylko odnajdywania pojedynczych informacji, ale także ich skojarzenia ze sobą (np. programy prezentujące diagram powiązań między osobami na podstawie list połączeń i danych adresowych odzyskanych z wielu telefonów). Wobec ciągle zwiększającej się liczby danych do analizy, konieczne staje się rozwijanie narzędzi nie tylko umożliwiających szukanie pojedynczej informacji, ale również grupujących je logicznie.