POLITECHNIKA
OPOLSKA

PRZEGLĄD NAUK STOSOWANYCH

pod redakcją
Mariusza Rząsy

nr 19

Wydział Ekonomii i Zarządzania
Opole, 2018

Przegląd Nauk Stosowanych

Nr 19

ISSN 2353-8899

Przegląd Nauk Stosowanych Nr 19 (2)

Redakcja: Mariusz R. Rząsa

Wszystkie artykuły zostały ocenione przez dwóch niezależnych recenzentów

All contributions have been reviewed by two independent reviewers

Projekt okładki: Krzysztof Kasza

Opracowanie graficzne: Oficyna Wydawnicza Politechniki Opolskiej

Wydanie I, 2018 r.

ISSN 2353-8899

Spis treści

SŁOWO WSTĘPNE

Ten numer Przeglądu Nauk Stosowanych poświęcony jest w całości ogólnopolskiej konferencji naukowej zatytułowanej „Praktyczne aspekty i możliwości wykorzystania potencjału naukowo- badawczego oraz transfer wiedzy pomiędzy sektorem nauki, a jednostkami Krajowej Administracji Skarbowej", która odbyła się w Opolu w dniach 13-14 marca 2018 r. z inicjatywy Izby Administracji Skarbowej w Opolu i Politechniki Opolskiej. W niniejszym numerze Przeglądu Nauk Stosowanych zamieszczono informacje o konferencji oraz opublikowano wybrane artykuły autorów wystąpień konferencyjnych. Wśród autorów artykułów są zarówno pracownicy naukowi uczelni, jak również pracownicy i funkcjonariusze jednostek Krajowej Administracji Skarbowej. Wiele artykułów posiada dwóch autorów reprezentujących obydwa środowiska, co dowodzi współpracy pomędzy tymi sektorami.

Głównym celem tego naukowego wydarzenia była dyskusja i wymiana doświadczeń pomiędzy środowiskiem naukowym uczelni a przedstawicielami izb administracji skarbowej z całego kraju dotycząca możliwych form i obszarów zacieśnienia współpracy obu środowisk. W trakcie dwóch dni konferencji teoretycy i praktycy mogli spotkać się i podyskutować o możliwościach oraz korzyściach, jakie daje partnerstwo nauki z administracją skarbową. Ku satysfakcji Organizatorów konferencja charakteryzowała się wysokim poziomem merytorycznym dyskusji, a jej tematyka spotkała się z dużym zainteresowaniem przedstawicieli obu środowisk. Mamy nadzieję, że publikacja będzie nie tylko źródłem wiedzy, dobrych praktyk,ale także inspiracją dla innych jednostek administracji publicznej.

Paweł Cybulski
Podsekretarz Stanu
Zastępca Szefa Krajowej Administracji Skarbowej
Ministerstwo Finansów
ul. Świętokrzyska 12
00-916 Warszawa
pawel.cybulski@mf.gov.pl

Wojciech ZIMOCH

NARZĘDZIA INFORMATYKI ŚLEDCZEJ W SŁUŻBIE ZWALCZANIA PRZESTĘPCZOŚCI EKONOMICZNEJ

Streszczenie: Wyzwaniem dla współczesnych inżynierów staje się dostarczanie obecnemu społeczeństwu narzędzi pozwalających na coraz sprawniejszy przepływ informacji w formie cyfrowej. Z jednej strony narzędzia te pozwalają na błyskawiczną wymianę komunikatów, z drugiej pozwalają na tworzenie dokumentów, baz danych itp. Cyfryzacja wkrada się w każdy zakamarek dzisiejszego życia, również do świata przestępczego. Dlatego służby odpowiedzialne za zwalczanie przestępczości również powinny mieć możliwość wykorzystania technologii cyfrowej do podjęcia skutecznych działań w obszarach, które nadzorują. Z uwagi na olbrzymie zaawansowanie współczesnej technologii nie są one jednak w stanie same wytworzyć potrzebnych narzędzi. Otwiera się tutaj olbrzymi obszar do działania dla środowiska naukowego, a w szczególności uczelni technicznych, które przy współdziałaniu ze służbami ,dysponując odpowiednim zapleczem kadrowym i organizacyjnym, są w stanie wytworzyć narzędzia m.in. w obszarze informatyki śledczej, której zadaniem jest dostarczanie dowodów cyfrowych prowadzącym dochodzenia. Narzędzia te oczywiście powinny posiadać określone funkcjonalności i spełniać elementarne wymogi.

Słowa kluczowe: informatyka śledcza, dowód cyfrowy, przestępczość.

FORENSIC TOOLS FOR THE PROVISION OF ECONOMIC CRIME

Abstract: The challenge for modern engineers is to provide the public with tools that enable an increasingly efficient flow of information in digital form. On the one hand, these tools enable an exchange of instant message. On the other hand, it allows us to make documents, databases, etc. Digitization is present in almost every aspect of today's life, including the criminal world. Therefore, services responsible for combating crime should also be able to use digital technology to take effective action in the areas they oversee. However, due to the enormous advancement of modern technology, they are not able to create the tools they need. This problem may introduce us to some possibilities for the scientific community, in particular for technical universities. These institutions are able to create the tools needed in the area of computer forensics, that aims to provide digital evidence to investigators. To do so they have to cooperate with the services, staff and organizational resources. Of course, these tools should provide certain level of functionality and should also meet elementary requirements.

Keywords: forensic, digital evidence, criminality.

1. WSTĘP

Cyfryzacja dotyka nas z każdej strony. Zagląda do życia prywatnego i służbowego. Stanowi podstawowy element rzeczywistości, a technologie informatyczne stają się istotnym narzędziem wspomagającym wykonywanie pracy, służącym do przekazywania informacji, czy po prostu do rozrywki. Nie inaczej dzieje się w obszarze przestępczości. Na tym polu technologię wykorzystuje zarówno jedna i druga strona barykady. Technika komputerowa bardzo pomaga w popełnianiu przestępstw czy wykroczeń, ale również coraz lepiej służy organom ścigania do ich wykrywania. Aby ujawniania te były możliwe należy poznać i stale ulepszać dostępne narzędzia informatyczne wykorzystywane m.in. do walki z przestępczością ekonomiczną. Narzędzia te zdają egzamin w takich obszarach jak analiza ryzyka, informatyka śledcza czy analiza kryminalna i chociaż te dyscypliny się przenikają, to każda z nich stanowi autonomiczny instrument. Aby efekty w zakresie zwalczania przestępczości były najlepsze całkowita autonomia nie jest jednak wskazana, a konieczne jest współdziałanie.. Gdy informatyk śledczy dostarcza olbrzymią ilość danych, analityk kryminalny może poddać je poszerzonej dedukcji, a osoba prowadząca dochodzenie pozyskać niezbite i celne dowody przestępczej działalności na podstawie których można określić nowe ryzyka np. w obszarze przestępczości ekonomicznej. Zdiagnozowane obszary z kolei przyczyniają się do lepszej prewencji i skuteczniejszego typowania do kontroli. Pozwala to na angażowanie sił i środków dokładnie tam, gdzie występują zagrożenia naruszenia prawa.

W nowoczesne narzędzia cyfrowe: oprogramowanie i sprzęt obowiązkowo powinna być dziś wyposażona każda służba powołana do egzekwowania prawa. Technologia cyfrowa to obecnie nie tylko alternatywa dla dotychczas wykorzystywanych narzędzi kontrolnych i procesowych, ale konieczność i przyszłość sprawnej walki z przestępczością, w tym z przestępczością ekonomiczną. Należy jednak pamiętać, że służby, chociaż są beneficjentami technologii cyfrowych, to same nie są autorami narzędzi, z których korzystają. Stają się one tylko i wyłącznie użytkownikami tych produktów, które dostarczają producenci. Warto podkreślić, że rynek narzędzi tego rodzaju jest rynkiem niszowym i hermetycznym. Istnieją oczywiście bezpłatne, powszechnie dostępne narzędzia do odzyskiwania danych, ale tylko te płatne i profesjonalne zapewniają odpowiedni poziom uzyskiwanych wyników. W obszarze konstruowania profesjonalnych narzędzi informatycznych wykorzystywanych w analizie kryminalnej, informatyce śledczej czy analizie ryzyka istnieje właśnie olbrzymie pole dla pracy naukowej, która dostarczałaby praktyczne, a nie teoretyczne rozwiązania, możliwe do wykorzystania w pracy służb. Niewątpliwie przy opracowaniu tych narzędzi pomocne byłyby same służby, kierunkując i testując zaproponowane narzędzia.

2. DOWÓD CYFROWY

Aby właściwie przedstawić problem wykorzystania narzędzi informatycznych w zwalczaniu przestępczości należy poprawnie zdefiniować pojęcie dowodu elektronicznego. Tutaj w pierwszej kolejności nasuwa się skojarzenie z urządzeniem,

które służy nam do komunikacji, pracy, które wykorzystujemy do pisania, obliczeń, zestawień, projektowania, odtwarzania multimediów, a przechodząc na język informatyków - do przetwarzania danych. To właśnie komputer, czy telefon komórkowy stanowi zainteresowanie śledczych, kiedy jest mowa o zabezpieczeniu dowodów. Gdy się jednak dłużej zastanowimy, to okazuje się, że nie sprzęt, który wykorzystujemy jest ważny, a wytworzone i przechowywane na nim dane. To one stanowią dowód w sprawie i to właśnie te dane nazywamy dowodem cyfrowy. Zabezpieczony materiał cyfrowy określa jego twórcę, wskazuje na czas, a nawet miejsce jego wytworzenia, określa nadawców i odbiorców wiadomości, zawiera określone treści, wskazuje użytkowników urządzeń, czy opisuje daną sytuację.

Biorąc pod uwagę sposób wytworzenia danych można je podzielić na:

- dane wytworzone przez użytkownika – np. pisma napisane przy pomocy edytorów tekstu, wiadomości poczty elektronicznej i komunikatorów, notatki i zapisy elektronicznych kalendarzy, prezentacje,
- dane wygenerowane samodzielnie przez urządzenia do przetwarzania danych – np. zapisy transakcji bankowych, wykazy połączeń, tzw. metadane, czyli dane o danych (np. gdzie i kiedy, przy pomocy jakiego urządzenia zostało wykonane zdjęcie cyfrowe), symulacje komputerowe, efekty obróbki materiału zdjęciowego czy filmowego,
- dane mieszane, czyli generowane przez człowieka i komputer – np. pliki arkuszy kalkulacyjnych, rejestry handlowe, skany dokumentów.

3. INFORMATYKA ŚLEDCZA – NARZĘDZIE POZYSKANIA DOWODÓW CYFROWYCH

Jednym z podstawowych narządzi wspomagania dzisiejszej kontroli jest informatyka śledcza. Można powiedzieć, że informatyka wyodrębniła się z nauk matematycznych. Z biegiem lat i rozwojem technologii stała się samoistną gałęzią nauki, swoistym połączeniem nauk ścisłych oraz techniki. Naturalną konsekwencją takiego stanu rzeczy było pojawienie się kolejnych specjalizacji w obrębie tej nowej dziedziny wiedzy. Podobnie jak w przypadku takich dyscyplin jak np. medycyna czy technika, w informatyce również zaczęto wykorzystywać specjalistyczną wiedzę do działań wspomagających stosowanie i egzekwowanie prawa. Medycyna sądowa czy technika kryminalistyczna są dzisiaj dyscyplinami bez których nie można wyobrazić sobie pracy służb. Obecnie do grona dziedzin nauki wspomagających zwalczanie przestępczości dołączyła informatyka poprzez jej gałąź, jaką jest informatyka śledcza.

Chcąc krótko zdefiniować tę dziedzinę nauki możemy powiedzieć, że jest to wykorzystywanie wiedzy informatycznej w praktyce. Nasuwa się wówczas kolejne pytanie, na czym ono jednak polega. Trzeba w tym miejscu zauważyć, że informatyka śledcza jest częścią kryminalistyki, która zgodnie z definicją Tadeusza Hanauska, jest nauką *o taktycznych zasadach i sposobach oraz o technicznych metodach i środkach rozpoznawania, a także wykrywania prawnie określonych, ujemnych zjawisk społecznych, a w szczególności przestępstw i ich sprawców oraz udowad-*

niania istnienia lub braku związku między osobami a zdarzeniami.[13] Można z tego wywieść, że również informatyka śledcza ma za zadanie dostarczyć dowody w prowadzonym dochodzeniu czy śledztwie. Aby je pozyskać i wykorzystać później w procesie karnym, podobnie jak każdy inny dowód, muszą one być odnalezione, zabezpieczone, przeanalizowane i odpowiednio zaprezentowane. Można zatem informatykę śledczą zdefiniować jako praktyczne wykorzystanie wiedzy o lokalizowaniu, pozyskiwaniu, analizowaniu, zabezpieczaniu i prezentacji dowodów elektronicznych. Aby jeszcze lepiej zdefiniować to określenie przychodzi na myśl bardziej obrazowe porównanie. Porównując pracę informatyka do czynności przesłuchania można powiedzieć, że informatycy śledczy „przesłuchują" nośniki danych, a jeszcze dobitniej, biorąc pod uwagę jedno z najpowszechniej wykorzystywanych obecnie urządzeń - „spowiadają telefony". Gdyby się głębiej nad tym zastanowić to ta alegoria ma mocne zakorzenienie w rzeczywistości. W dawnych czasach informacja była przekazywana ustnie, później pisemnie. Dzisiaj jest przekazywana przy pomocy technologii cyfrowych. Dawniej, aby otrzymać rzeczywisty obraz sprawy należało „wydobyć" prawdę z osoby przesłuchiwanej lub zdobyć odpowiedne dokumenty zawierające zapisy odnoszące się do niej. Obecnie wiele potrzebnych informacji można odcyfrować z danych zawartych w urządzeniach, z których każdy z nas korzysta na co dzień. Współczesna technologia pozwala nie tylko na prosty odczyt danych, które są jawne, ale również np. na odczyt danych skasowanych. Pozwala także na prześledzenie naszej aktywności w sieci, na wskazanie miejsc, w których przebywaliśmy czy odczytanie naszej korespondencji. W czasach gdy do prowadzenia korespondencji wykorzystywano wyłącznie papier jego zniszczenie, o ile nikt nie wykonał odpisu z oryginału, było równoznaczne z unicestwieniem dowodu. Dzisiaj list elektroniczny (e-mail) istnieje w wielu kopiach. Można go odnaleźć na komputerze lub smartfonie nadawcy, na serwerach poczty wychodzącej i przychodzącej, a nawet- dzięki programom zwanym „klientami poczty"- np. na komputerze odbiorcy korespondencji. Głośnym przykładem wykorzystania dowodów elektronicznych w postaci korespondencji e-mailowej w procesie karnym była sprawa katastrofy budowlanej na terenie Międzynarodowych Targów Katowickich w roku 2006. W sprawie tej prokurator posiadał m.in. dowody w postaci e-maili na to, że członkowie zarządu byli świadomi zagrożenia, ale mimo tego nie podjęli stosownych działań. Innym spektakularnym przykładem wykorzystania informatyki śledczej była głośna sprawa Katarzyny Waśniewskiej, dzieciobójczyni z Sosnowca, w której udało się odtworzyć historię jej wizyt na stronach internetowych i przez to wskazać na poszlaki świadczące o przygotowywaniu zabójstwa. Śledczy m.in. wykazali, że oskarżona poszukiwała w sieci odpowiedzi na takie pytania jak: „jak zabić bez śladów", „czy można zabić bez pozostawienia śladów", „dochodzenie policyjne przy zaczadzeniu tlenkiem węgla", „zasiłek pogrzebowy niemowlaka", „pochówek dzieci martwo urodzonych", „kremacja niemowlaka cena", „nieumyślne spowodo-

[13] Hanausek T.: *Kryminalistyka – zarys wykładu*, wyd. Zakamycze 2005 r., s. 23.

wanie śmierci" oraz „cennik trumien dla dzieci w miejskim zakładzie pogrzebowym”[14].

Chcąc uszczegółowić definicję informatyki śledczej uwzględniając jej poszczególne elementy należy przyjąć, że to wiedza o:

1. lokalizowaniu dowodów cyfrowych, czyli ich odnajdywaniu na różnego rodzaju nośnikach (dyski twarde komputerów, dyskietki, płyty CD, pamięci przenośne, serwery, telefony komórkowe itp.), a także internetowych nośnikach danych (portale społecznościowe, dyski w chmurze czy wyszukiwarki internetowe)[15],
2. pozyskiwaniu, czyli ich odczytaniu z urządzeń lub sieci (w tym również pozyskaniu danych skasowanych lub zaszyfrowanych),
3. analizowaniu, czyli przeszukiwaniu baz danych pod określonym kątem (np. wyszukiwaniu określonych adresatów korespondencji elektronicznej), wyszukiwaniu powiązań pomiędzy danymi,
4. zabezpieczeniu, czyli procesowym zabezpieczeniu dowodów cyfrowych np. w postaci kopii binarnych całych nośników czy kopii plików (kopie uwierzytelnione tzw. sumą kontrolną, którą to operację można porównać do potwierdzenia dokumentu „za zgodność z oryginałem”,
5. prezentacji, czyli takim przedstawieniu dowodów cyfrowych (zapisaniu w określonym formacie), który pozwala na ich odtworzenie przy pomocy standardowych, ogólnie dostępnych programów (np. programu MS Office czy odtwarzacza plików multimedialnych - WMP). Odpowiednia prezentacja pozwala na poddanie zgromadzonych danych dalszej analizie, np. przez analityków kryminalnych lub na prostą prezentację dowodów na sali sadowej.

Wskazany wyżej podział wyznacza funkcjonalność narzędzi, którymi posługują się informatycy śledczy, a które mogłoby dostarczyć środowisko naukowe. Można je podzielić na narzędzia do:

1. procesowego pobierania i zabezpieczania (akwizycji) danych zgromadzonych na nośnikach fizycznych, w tym wykonywania kopii całych nośników,
2. procesowego pobierania i zabezpieczania danych z pamięci ulotnych (RAM) i pracujących systemów komputerowych, w tym kopii wyodrębnionych plików (live forensic),
3. pozyskiwania i analizy danych pochodzących z urządzeń mobilnych (Mobile Forensic),
4. pozyskiwania i analizy zapisu dźwięku i obrazu,
5. odzyskiwania danych,
6. analizy pobranych danych,
7. pozyskanie danych z pojazdów samochodowych,

[14] Artykuł na portalu WP wiadomości z dnia 03-09-2013, *Katarzyna W. skazana na 25 lat więzienia za zabójstwo córki Magdy* (http://wiadomosci.wp.pl/katarzyna-w-skazana-na-25-lat-wiezienia-za-zabojstwo-corki-magdy-6031331089179265a)

[15] Jakub Dzikowski, *Uniwersytet Ekonomiczny w Poznaniu: Wyszukiwanie danych osobowych w Internecie dla celów Informatyki Śledczej*, STUDIA OECONOMICA POSNANIENSIA 2013,vol.1,no.2(251)

8. pozyskiwania danych pochodzących z sieci (chmury obliczeniowej).

Pierwsza grupa narzędzi to najczęściej sprzęt pozwalający na realizację naczelnego motta, którym kierują się informatycy śledczy, czyli „widzę wszystko, nie zmieniam nic". Do grupy tej zaliczają się tzw. blokery zapisu, duplikatory czy kopiarki dysków, posiadające funkcję blokady zapisu. Można w uproszczeniu stwierdzić, że pozwalają one na wykonanie procesowej kopii binarnej dysku, która jest identyczna z oryginałem, przy czym oryginał danych pozostaje „nietknięty".

Drugą grupę stanowią programy pozwalające na wykonanie czynności z zakresu informatyki śledczej na pracującym systemie. Muszą one dać możliwość szybkiego zabezpieczenia danych, do których po wyłączeniu komputera dostęp będzie niemożliwy, np. z uwagi na szyfrowanie lub wyłączenie opcji archiwizowania zapisu rozmów z komunikatorów. Z drugiej strony winny one umożliwiać pobranie danych w sytuacji, gdy niemożliwe jest wyłączenie np. pracujących serwerów. W tym przypadku oczekiwane narządzie powinno umożliwić celowane (technika *Triage*) pobranie, na miejscu realizacji, tylko istotnego dla sprawy materiału dowodowego i pominięcie kopiowania nieistotnych danych.

Trzecia grupa to zwykle narzędzia sprzętowo-programowe, które pozwalają na dostęp do danych zgromadzonych na urządzeniach mobilnych (telefony komórkowe, tablety, nawigacje GPS, itp.)[16]. Sprzęt taki wykorzystywany jest głównie przez organy ścigania lub inne służby powołane do ochrony państwa. Funkcjonariusze tych służb oczekują, aby narzędzia te gwarantowały nie tylko wysoką skuteczność, ale również w wielu przypadkach - pełną mobilność. Sprzęt taki powinien umożliwiać wyodrębnianie, dekodowanie i analizę danych z wszelkich urządzeń mobilnych. Powinien zapewniać dostęp nie tylko do urządzeń niezabezpieczonych, ale również do sprzętu zabezpieczonego np. hasłem czy poprzez znak graficzny (pattern lock). Precyzując- narzędzie to musi posiadać funkcjonalność pozwalającą na logiczną i fizyczną ekstrakcję danych, czyli dać dostęp do systemu plików, haseł i każdego rodzaju danych zgromadzonych na urządzeniu mobilnym, także tych usuniętych i chronionych.

Czwartą grupę stanowią oprogramowanie lub zestawy składające się z urządzeń i programów, których zadaniem jest pozyskanie, zdekodowanie, obróbka i ponowne zgranie danych, stanowiących zapis dźwięku, obrazu lub nagrań video. Wymagania stawiane dedykowanemu oprogramowaniu to przede wszystkim: możliwość dekodowania materiału video z różnych typów rejestratorów (różne typy plików), automatycznego wyodrębnienia wskazanych obiektów (np. identyfikacja twarzy, sekwencje ruchu, sekwencje w danym obszarze), wyboru/indeksowania określonego czasu i terminu nagrania. Oczywiście oczekiwane narzędzie musi również posiadać

[16] Wiodącymi produktami komercyjnymi (zestawy oprogramowanie + osprzęt) wykorzystywanymi obecnie przez organy ścigania oraz firmy z branży informatyki śledczej i odzyskiwania danych są m.in. UFED firmy Cellebrite oraz XRY firmy MSAB

pełną zdolność do odzyskiwanie danych, które z różnych przyczyn zostały uszkodzone lub skasowane[17].

Narzędzia reprezentujące piątą i szóstą grupę najczęściej występują na rynku jako koherentne oprogramowanie posiadające taką funkcjonalność, jak[18]:

- możliwość przeglądania przestrzeni wolnej i nieprzydzielonej,
- odzyskanie danych, w tym odzyskiwanie w trybie RAW,
- ustalanie cech charakterystycznych podłączanych nośników,
- przeszukiwanie przestrzeni „slack",
- możliwość przeglądania atrybutów oraz uprawnień dotyczących plików,
- umożliwienie dostępu do alternatywnego strumienia danych (ADS),
- indeksowanie plików oraz metadanych,
- obsługa bazy danych NIST (NSRL),
- możliwość analizowania sygnatur plików,
- możliwość analizowania pamięci RAM,
- możliwość analizy backup-ów urządzeń mobilnych,
- umożliwienie analizy metadanych plików (EXIF),
- możliwość analizy entropii,
- umożliwienie analizowania rejestrów systemowych.

Nowym wyzwaniem dla informatyki śledczej jest zabezpieczanie danych generowanych przez pojazdy samochodowe. Postęp w zakresie cyfryzacji nie ominął również takiej dziedziny jak motoryzacja, a można wręcz powiedzieć, że zaczyna w niej dominować. Współczesny samochód nie może się już poruszać bez zintegrowanej z układami mechanicznymi elektroniki. Większa część układów samochodu jest sterowana komputerowo, co wiąże się z przetwarzaniem danych, ale również ich archiwizacją. Dane dotyczące np. parametrów pracy czy błędów silnika nie będą istotne w prowadzonych dochodzeniach przeciwko przestępczości ekonomicznej. Jednak dzisiejsze samochody „pamiętają" dużo więcej. W zależności od wyposażenia możemy spodziewać się danych geolokalizacyjnych, w tym informacji o przebytych trasach wraz ze znacznikami czasowymi, jak również danych o inicjowanych lub odbieranych połączeniach. Te ostatnie informacje mogą pochodzić z urządzeń pokładowych, bądź z urządzeń przyłączanych do systemów samochodu, jak np. telefon komórkowy, tablet czy laptop podłączony poprzez Bluetooth.

Ostatnią grupę stanowią narzędzia do analizy i zabezpieczania danych w rozległych sieciach komputerowych (cloud computing[19]). Jeszcze do niedawna, aby

[17] Narzędzia wykorzystywane dopozyskiwania tego typu danych to to m.in. DVR Examiner firmy DME Forensics lub HX-Recovery for DVR

[18] Przykładem takiego profesjonalnego narzędzia, którego funkcjonalność odpowiada wyszczególnionej, jest program EnCase® Forensic firmy OpenText Corp wcześniej Guidance Software

[19] *Chmura obliczeniowa* (również przetwarzanie w chmurze, ang. cloud computing) – model przetwarzania danych oparty na użytkowaniu usług dostarczonych przez usługodawcę (wewnętrzny dział lub zewnętrzna organizacja).

pozyskać dowody cyfrowe np. korespondencję elektroniczną czy dane księgowe, wystarczało zatrzymać urządzenia, na których dane te były przechowywane, a które znajdowały się w posiadaniu kontrolowanych czy firm (komputery osobiste, firmowe serwery, telefony komórkowe, itp.). Obecnie, szczególnie z uwagi na olbrzymią ilość danych, nie są już one przechowywane w pamięci posiadanych urządzeń, ale na specjalnych zewnętrznych, odpowiednio zabezpieczonych serwerach u dostawców świadczących takie usługi. Osoby prywatne w systemach chmurowych przechowują swoje np. zdjęcia, muzykę, filmy. Firmy zamiast rozrywki przesyłają do wirtualnego magazynu ważne dane w postaci np. dokumentacji księgowej czy wytarzanych w firmie dokumentów. Wyzwaniem staje się więc prawidłowe procesowe zabezpieczenie tych danych i dotarcie przez informatyka śledczego do wirtualnych sejfów. Nie zagłębiając się w problemy natury prawnej dotyczące globalnego charakteru sieci Internet (serwery - magazyny danych nie znajdują się w państwie, w którym prowadzone jest kontrola lub postępowanie) do rozwiązania jest coraz więcej problemów technicznych, związanych przede wszystkim brakiem fizycznego dostępu do komputera, jak również zabezpieczeniem dostępu poprzez różne sposoby uwierzytelnienia, szyfrowanie czy olbrzymią ilość danych. Problemem jest nie tylko zdobycie samych danych, ale również ustalenie ich położenia (lokalizacji serwerów) oraz zabezpieczenie przed ich zdalnym skasowaniem. W sytuacji posiadania danych problemem jest ustalenie- kto i gdzie je wytworzył. Wszystko to i wiele nie innych problemów powinno znaleźć rozwiązanie w opracowywanych narzędziach dla informatyków śledczych, mających za zadanie zabezpieczanie danych w chmurze.

Dodatkowym nowym wyzwaniem jest skonstruowanie narzędzia umożliwiającego identyfikację i zabezpieczenie kryptowalut, które będzie działać niezależnie od rodzaju badanego urządzenia, przeznaczonego do wykonywania transakcji w obszarze kryptowalut np. przy użyciu tzw. portfeli, czyli miejsca służącego do przechowywania elektronicznego pieniądza (kluczy prywatnych). Oczekiwana funkcjonalność w tym zakresie mogłaby się sprowadzać do automatyzacji rozpoznawania odpowiedniego kodu oraz umożliwienia dokonania zabezpieczenia odnalezionej kryptowaluty.

4. TWORZENIE NARZĘDZI INFORMATYKI ŚLEDCZEJ

Dowód elektroniczny, a przez to informatyka śledcza, zaczynają pełnić kluczową rolę w procesie karnym spełniając dwie podstawowe funkcje:

- informacyjną – czyli ukierunkowaną na odnalezienie wskazówek pomocnych w prowadzeniu dochodzenia,
- dowodową – czyli ukierunkowaną na dostarczanie dowodów popełnienia określonych czynów.

Podkreślenia wymaga fakt, że obie funkcje są ze sobą nierozerwalnie związane i nawzajem się przenikają. Pozyskane dane mogą stanowić wszak nie tylko wskazówkę, ale zarazem dowód w sprawie.

Aby w pełni korzystać z dobrodziejstwa jakim jest dowód cyfrowy potrzebna jest nie tylko specjalistyczna wiedza informatyka śledczego, ale dostarczenie mu narzędzia, które cały proces akwizycji, analizy i zabezpieczenie danych ułatwi i zautomatyzuje. W innym przypadku praca wykonywana przez specjalistę wymagałaby każdorazowego poświęcenia ogromnej ilości czasu na „ręczne" pozyskanie elektronicznego materiału dowodowego. Tutaj otwiera się olbrzymie pole dla działań świata naukowego, aby we współpracy z organami ścigania dostarczać im nowe i coraz lesze narzędzia sprzętowe i programowe do informatyki śledczej. Taką możliwość daje odpowiednie zaplecze kadrowe i sprzętowe uczelni oraz czas, który może być poświęcony na badania i wdrożenie. Pracownicy naukowi dają także gwarancję tego, że narzędzia informatyki śledczej będą spełniały elementarne warunki, jakimi są:

- połączenie zasad prawa z techniką komputerową - sprzęt i oprogramowanie musi pozwolić na otrzymywanie wyników, które w procesie karnym mogą zostać zweryfikowane,
- zapewnienie powtarzalności wyników,
- automatyzacja czynności,
- czytelność i prostota interfejsu,
- maksymalna uniwersalność narzędzia w określonym obszarze (np. w obszarze urządzeń mobilnych) - dostęp do różnych formatów danych,
- dostęp do wszystkich metadanych,
- zapewnienie dostępu do danych „ulotnych",
- czytelność generowanych raportów – raport powinien być zrozumiały dla osób bez wykształcenia informatycznego,
- możliwość zrzutu zabezpieczonego materiału do popularnych formatów (np. pdf, doc, docx, xls,xlsx, avi, mp4 itp.),
- umożliwienie indeksowania badanego materiału (np. z uwagi na znaczniki czasowe),
- ingerencja w badany system komputerowy lub urządzenie w minimalnym, niezbędnym zakresie (bez otwierania niepotrzebnych okien i programów; bez niepotrzebnego zamykania już uruchomionych, itd.),

Niektórzy mogą powiedzieć, że takie narzędzia już na rynku istnieją, a służby i firmy działające w tym obszarze są w ich posiadaniu. Jednak z całą stanowczością trzeba stwierdzić, że ciągły, błyskawiczny rozwój technologii cyfrowej tworzy olbrzymi obszar do zagospodarowania, a istniejące narzędzia wymagają ciągłej aktualizacji i dostosowania do nowości. Nie one są również doskonałe i nie potrafią poradzić sobie ze wszystkimi urządzeniami, zabezpieczeniami czy rodzajami danych. Tak więc wejście w obszar tworzenia narzędzi dla informatyki śledczej, a przy tym współdziałanie uczelni ze służbami, jest ze wszech miar przydane i zapewnia korzyści dla obu stron tym bardziej, że działanie to nie kończy się wraz z wytworzeniem produktu, ale jest to proces ciągły, który nie ma ram czasowych. W dobie błyskawicznego rozwoju technologii cyfrowej i urządzeń na niej bazujących brak stałej aktualizacji wytworzonych narzędzi oraz wsparcia dla produktu postawiłby pod

znakiem zapytania sens jego tworzenia. Funkcjonalność takiego produktu w krótkim czasie stałaby się niewystarczająca, a z czasem narzędzie to byłoby bezużyteczne. Konstruowanie narzędzi dla informatyki śledczej zapewni uczelni technicznej możliwość tworzenia nie tylko teoretycznych rozwiązań, ale konkretnych produktów wykorzystywanych w praktyce, wymuszając na kadrze uczelni ciągły rozwój. Drugiej stronie zapewni to dostęp do innowacyjnych rozwiązań, które mogą zastąpić używane technologie lub okazać się ich uzupełnieniem.

Literatura:

[1] Hanausek T.: *Kryminalistyka – zarys wykładu*, Zakamycze 2005 r., s. 23.
[2] Jakub Dzikowski, *Wyszukiwanie danych osobowych w Internecie dla celów Informatyki Śledczej,* Uniwersytet Ekonomiczny w Poznaniu: STUDIA OECONOMICA POSNANIENSIA 2013,vol.1,no.2(251)
[3] Arkadiusz Lach,: *Dowody elektroniczne w procesie karnym,* Dom Organizatora Toruń 2004
[4] Cory Altheide, Harlan Carvey: *Informatyka śledcza. Przewodnik po narzędziach open source*, Helion, 2014
[5] Artur M. Kalinowski,: *Metody inwigilacji i elementy informatyki śledczej,* CSH, Kwidzyń 2011
[6] Przemysław Gwizd, *Analiza danych w informatyce śledczej; Bezpieczeństwo: teoria i praktyka*: czasopismo Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego 7/4, 43-58 (2013)
[7] Czasopismo*: Magazyn informatyki śledczej i bezpieczeństwa IT,* Wydawca Media Sp. z o.o. [https://magazyn.mediarecovery.pl/]

Źródła internetowe

[8] portal WP, wiadomości z dnia 03-09-2013, Katarzyna W. skazana na 25 lat więzienia za zabójstwo córki Magdy [dostęp: http://wiadomosci.wp.pl/katarzyna-w-skazana-na-25-lat-wiezienia-za-zabojstwo-corki-magdy-6031331089179265a]
[9] EnCase® Forensic [dostęp: https://www.guidancesoftware.com/encase-forensic]
[10] Cellebrite [dostęp: https://www.cellebrite.com/en/home/]
[11] MSAB [dostęp: https://www.msab.com/]
[12] Berla CorporationB [dostęp: https://berla.co/]
[13] DME Forensics [dostep: https://dmeforensics.com/dvr-examiner/]
[14] HX Recovery for DVR [dostęp: http://www.hxdvr.com/]

podinsp. mgr inż. Wojciech Zimoch
Izba Administracji Skarbowej w Opolu / Opolski Urząd Celno-Skarbowy w Opolu
Centrum Techniczne Informatyki Śledczej KAS
e-mail: wojciech.zimoch@mf.gov.pl

POLITECHNIKA OPOLSKA

ISSN 2353-8899