NR 6 | CZERWIEC 2010

Magazyn informatyki śledczej

Zmiany na rynku computer forenscic

Notowana na nowojorskiej giełdzie Guidance Software za ponad 12 milionów dolarów kupiła producenta sprzętu dla informatyki śledczej, firmę Tableau. Guidance Software jest twórcą najpopularniejszego oprogramowania do analiz śledczych – EnCase. Tableau natomiast znane jest najbardziej z produkcji blokerów, czyli podstawowych urządzeń, niezbędnych do przeprowadzania jakichkolwiek czynności związanych z cyfrowymi analizami śledczymi. Więcej o blokerach pisaliśmy w pierwszym numerze MiŚ.

Hakerzy skazani

Trwający od stycznia 2007 roku proces hakerów, którzy dokonali głośnego włamania do systemów komputerowych TJX i kradzieży danych dobiegł końca. W tamtym okresie była to największa kradzież tego typu. Łupem hakerów padło ponad 45 milionów numerów kart kredytowych, co stanowiło 80GB danych. TJX podaje, iż usuwanie skutków włamania pochłonęło 171 milionów dolarów. Skazano 11 osób, prowodyr i mózg operacji Albert Gonzales dostał wyrok 20 lat więzienia.

Napisz do nas

informatyki śledczej Magazyn

redakcja@mediarecovery.pl

Keyword czy indeks?

Przemysław Krejza

Jedną z najważniejszych technik wyszukiwania informacji w sprawach informatyki śledczej jest analiza słów kluczowych (ang. keyword search). Analiza opiera się na wyszukiwaniu i badaniu wystąpień ciągów znaków w dokumentach, mailach a nawet „pustych" miejscach na dysku. Tzw. keywordy mogą być na przykład mailami do osób, z którymi mogła być prowadzona komunikacja, nazwami firm, z którymi nieuczciwie współpracował pracownik, fragmentami wypowiedzi, itd.

Ta ważna funkcjonalność w programach śledczych realizowana jest w dwojaki sposób – „keyword serach" i „indeksowanie". Obie metody są równie skuteczne, każda ma jednak pewne ograniczenia. Tradycyjny keyword search opiera się o statyczną listę słów, które następnie są przedmiotem wyszukiwania. Kluczem do sukcesu jest tutaj zbudowanie właściwych słów – wystarczająco unikalnych, aby wystąpień (wyników) nie było zbyt dużo. Przykładowo słowo „microsoft" może mieć nawet kilkanaście tysięcy wystąpień, a słowo „przelej mi kasę" tylko kilka i to we właściwym kontekście.

Aby ułatwić nam zadanie, producenci programów śledczych wprowadzili specjalną składnię do tworzenia złożonych słów, tzw. GREP. Pozwala na przykład, zamiast wypisywania wszystkich możliwych numerów PESEL, na zakodowanie numeru do postaci: ##[0-1]#[0-3]#[0-1]#### (**parz tabela nr 1**).

Mechanizm keyword search jest niestety statyczny – wprowadzenie nowego słowa wymaga przeprowadzenia ponownego wyszukiwania.

W tym kontekście znacznie bardziej efektywne jest indeksowanie (ang. indexing). Mechanizm ten używając transkryptu „wydobywa" ze sprawy wszystkie ciągi znaków tworząc plik indeksu. Choć jest to wygodne to wadą jest czasochłonność tworzenia indeksu. W zamian, po zaindeksowaniu, możemy dowolną ilość razy wyszukiwać dowolne ciągi (również za pomocą składni GREP) bez konieczności ponownego indeksowania.

Wybierając metodę powinniśmy zatem wziąć pod uwagę na ile jesteśmy pewni swojej listy słów kluczowych i czy będzie się rozwijała. Jeśli jest statyczna stosujmy keyword seracg. W przeciwnym wypadku (wziąwszy pod uwagę ograniczenia wskazane w tabeli) wydajniejsze będzie indeksowanie (**tabela nr 2**). Chcąc skrócić czas tworzenia indeksu warto zastanowić się czy konieczne jest przetworzenie wszystkich plików czy być może wystarczające będzie wybranie samych dokumentów. Warto również zaplanować czas tak, aby proces włączyć na noc, aby rano otrzymać wyniki.

Autor jest prezesem Stowarzyszenia Instytut Informatyki Śledczej, twórcą największego w tej części Europy laboratorium informatyki śledczej.

TABELA **NR 1**

GREP	PRZYKŁAD	WYNIK WYSZUKIWANIA
.	t…….k	dowolne słowo ośmioznakowe zaczynające się na t i kończące na k (. oznacza dowolny znak) Zapis może być zastąpiony składnią: t.{6,6}k
?	magazyn ?informatyki	„magazyn informatyki";„magazyninformatyki"(? wskazuje, że znak poprzedzający może wystąpić zero lub raz). Składnię można również zapisać jako: magazyn[ ]?informatyki lub magazyn[ ]{0,1}informatyki
*	magazyn *informatyki	„magazyn informatyki";„magazyn informatyki";„magazyninformatyki" (* wskazuje, że znak poprzedzający może wystąpić zero lub więcej razy). Składnię można zapisać również jako: magazyn[ ]*informatyki
+	magazyn +informatyki	„magazyn informatyki";„magazyn informatyki"; (+ wskazuje, że znak poprzedzający może wystąpić więcej niż raz ale przynajmniej raz)
#	###	Dowolny numer trzycyfrowy (# oznacza dowolną cyfrę od 0 do 9)
()	(org)	„org" (() – grupuje znaki do bardziej złożonych konstrukcji jako AND)
{}	i{2,2}	„ii" ({x,y} – wskazuje powtórzenie znaku poprzedzającego od x do y razy)
|	.(com)|(org)|(pl)	„.com";„.org";„.pl" (| oznacza LUB)
[]	szklank[a,i]	„szklanka" i „szklanki"
[^]	szklank[^a,i]	wszystkie słowa o początku „szklank" nie kończące się na a lub i.
[-]	szklank[a-o]	Wszystkie słowa o początku „szklank" kończące się na literę w zakresie a-o. Możemy również wskazać znaki spoza zakresu a-o, gdy użyjemy składni [^a-o]
\	\.	„." (\wskazuje, że dany znak nie jest zapisany w GREP).

TABELA **NR 2**

	KEYWORD SEARCH	INDEKSOWANIE
Start	Złożona budowa słów, możliwość pomyłki	Uruchomienie opcji
Wynik	Możliwość analizy już w trakcie wyszukiwania	Długotrwałe oczekiwanie
Kolejne słowa	Powtórzenie procesu	Wynik natychmiastowy
Dane źródłowe	Zapis fizyczny lub logiczny	Transkrypt dokumentów
PDF	Ograniczone	Tak
Slaki	Tak	Nie
Złożone filtrowanie, łączenie z metadanymi	Nie	Tak
Inne korzyści	-	Możliwość tworzenia słownika z pliku indeksu

Rolą Policji jest dążenie do poprawy bezpieczeństwa teleinformatycznego.

Wywiad z nadkomisarzem Janem Kościukiem, rzecznikiem prasowym Komendanta Wojewódzkiego Policji w Gdańsku

Skala cyberprzestępczości rośnie z roku na rok, czy jest to zauważalne również w pracy funkcjonariuszy Komendy Wojewódzkiej Policji w Gdańsku? Czy wzrasta ilość zgłoszeń jakie Państwo otrzymują? Jaka jest skala tego zjawiska?

Sukcesywnie odnotowujemy coraz więcej zgłoszeń dot. łamania prawa przy wykorzystaniu sieci teleinformatycznych, teletransmisyjnych i urządzeń współpracujących z tymi sieciami. Sprawcy integrują się wirtualnie na różnego rodzaju forach internetowych, lub za pośrednictwem dostępnych form komunikacji internetowych. Podczas nawiązywanej korespondencji uzgadniają metody i zakres działania przestępczego, wykorzystując przy tym narzędzia i metody utrudniające identyfikację w sieci. Tego typu sprawcy, często wykorzystują tożsamości innych osób, podszywając się za nie na różnych serwisach internetowych, na których dochodzi do nieautoryzowanych transakcji finansowych na szkodę osób zamieszkałych na terenie Polski oraz poza jej granicami.

Czy w związku z przestępstwami z użyciem komputera stosują Państwo jakieś specjalne działania, różniące się od tych podejmowanych w przypadku przestępstw tradycyjnych?

Między innymi rolą Policji jest dążenie do poprawy bezpieczeństwa teleinformatycznego. W tym celu czynnie uczestniczymy w szkoleniach podnoszących wiedzę i kwalifikacje policjantów. Sami policjanci zajmujący się zwalczaniem przestępczości teleinformatycznej mają nierzadko wyższe wykształcenie informatyczne. Na szkoleniach opracowywane są najnowsze metody przeciwdziałania przestępczości teleinformatycznej. Te metody są automatycznie wdrażane. Ze strony Policji organizowane są konferencje z udziałem specjalistów z dziedziny informatyki i telekomunikacji oraz instytucji współodpowiedzialnych za bezpieczeństwo i funkcjonowanie sieci internetowej w Polsce, a także tego rodzaju specjaliści z innych państw. Tam przedstawiane są najlepsze metody, które umożliwiają szybkie zidentyfikowanie przestępców internetowych.

Jak często korzystają Państwo ze wsparcia instytucji specjalistycznych, biegłych sądowych z zakresu informatyki celem analiz informacji zapisanych w zabezpieczonym sprzęcie komputerowym? Jakimi przesłankami kierują się Państwo przy ich wyborze?

Każdy ujawniony i zabezpieczony dowód w sprawie jest badany przez biegłych specjalistów z danej wymaganej dziedziny. Tak więc każdy biegły, specjalista powinien spełniać określone wymagania oraz posiadać odpowiednią wiedzę z danej dziedziny, która pozwoli na wykonanie ekspertyzy zgodnie z określonymi kryteriami.

Jakiego rodzaju cyberprzestępstwa zgłaszane są najczęściej?

Oczywiście coraz częściej mamy do czynienia z przestępstwami popełnianymi przy wykorzystaniu narzędzi i metod służących do ukrywania tożsamości w Internecie. Komenda Wojewódzka Policji w Gdańsku, przy współpracy z instytucjami, których rolą jest również podnoszenie bezpieczeństwa teleinformatycznego, opracowała skuteczną metodę przeciwdziałania tego rodzaju przestępstwom.

Czy mogą Państwo podać przykład najbardziej wyróżniającego się wśród innych przypadku cyberprzestępstwa z jakim mieliście do czynienia? Czy to pod względem skomplikowania, skali, sprytu przestępców, wysokości strat poszkodowanych?

Tak jak wspomniałem na początku sprawcy podszywali się pod inne osoby na różnych serwisach, na których realizowane były transakcje finansowe. Sprawcy ci popełnili szereg przestępstw na szkodę finansową wielu ludzi zamieszkałych na terenie Polski oraz innych krajów w tym Anglii, USA, Niemiec. Straty przy tego rodzaju przestępstwach sięgały łącznie nawet do 1 mln złotych. Sprawców zatrzymaliśmy, a wobec części z nich Sąd zastosował tymczasowy areszt. Każdy z tych sprawców odpowie przed Sądem za popełnienie powyższych przestępstw, oczywiście to nie koniec. Każdy pokrzywdzony, a mam tutaj na myśli osoby fizyczne, a także instytucje mają prawo żądać od sprawcy odszkodowania, naprawy szkody lub zwrotu strat. Coraz częściej spotykamy się z wyrokiem, kiedy sprawca jest zobowiązany do zwrotu pieniędzy za wyrządzone szkody.

Czego najbardziej brakuje w codziennej służbie policjantom zwalczającym cyberprzestępczość: dostępu do wiedzy, odpowiedniej technologii, doświadczenia, czy może jeszcze czegoś innego?

Oczywiście szybszego przekazywania informacji na temat zdarzeń ze strony instytucji, jak też unormowania przepisów prawa, które regulowałyby formę współpracy Policji z instytucjami finansowymi, w tym z bankami w zakresie szybkiego reagowania.

Czy w ramach KWP w Gdańsku funkcjonuje grupa ds. walki z cyberprzestępczością? Jak to wygląda w podległych komendach miejskich i powiatowych? Czy w każdej z nich służą funkcjonariusze specjalizujący się w tego typu sprawach?

W komendach miejskich, powiatowych oraz komisariatach funkcjonują komórki zajmujące się przestępstwami gospodarczymi, w ramach których prowadzone są m.in. sprawy związane z cyberprzestepstwami. Komenda Wojewódzka Policji w Gdańsku na bieżąco nadzoruje sprawy prowadzone przez te jednostki, ale także uczestniczy i w miarę możliwości pomaga w ich realizacjach.

Podczas II Ogólnopolskiej Konferencji Informatyki Śledczej, aż 93% ankietowanych uczestników twierdziło, iż polskie prawo nie nadąża za rozwojem technologii. Jaka jest Państwa opinia na ten temat? Czy policjanci napotykają w swojej pracy przeszkody natury prawnej? Czy są przepisy, które warto byłoby udoskonalić?

Policjanci pracują zgodnie z obowiązującymi przepisami prawa. Jeżeli akty prawne związane z tą materią będą się zmieniać to również i Policja będzie się do nich dostosowywać.

Rozmawiał: Zbigniew Engiel

Hardware w informatyce śledczej

Michał Bednarski

Chciałbym podzielić się z czytelnikami kilkoma spostrzeżeniami dotyczącymi sprzętu komputerowego na potrzeby informatyki śledczej. Będę starał się zaproponować kilka rozwiązań, z których korzystam na co dzień, a które, w mojej opinii, ułatwiają lub przyspieszają pracę z materiałem dowodowym.

Konfiguracja komputera do celów informatyki śledczej polega na połączeniu szybkiego procesora, jak największej ilości pamięci RAM, świetnej karty grafiki oraz wmontowaniu tego wszystkiego w płytę główną z dobrej półki, umożliwiającą w przyszłości minimalny upgrade. Ale czy tak naprawdę to wszystko jest potrzebne jednostce centralnej, której zadaniem będzie rozwiązywanie zagadek w informatyce śledczej ?

Zacznijmy od podstaw. Od płyty głównej. Zawsze wymagałem bogactwa interfejsów, po to aby mieć nieograniczone możliwości podłączania peryferiów. Moją ulubioną jest Asus P5Q Premium, która oferuje bogactwo w postaci 14 portów USB w wersji 2.0 (10 na panelu tylnym oraz 4 do opcjonalnego montażu na panelu przednim). Taka ilość portów USB jest potrzebna, ponieważ w informatyce śledczej komputer będzie cały naszpikowany urządzeniami peryferyjnymi oraz kluczami sprzętowymi dodawanymi do każdego zakupionego oprogramowania CF. Sam w pracy operuję trzema kluczami sprzętowymi, które wolę mieć wpięte bezpiecznie w tylną część komputera (nieraz byłem świadkiem gdy osoby postronne niechcący zahaczały o klucze sprzętowe warte kilka tysięcy dolarów, bo te nieopatrznie wpięte zostały do przedniego panelu jednostki centralnej). Do kluczy dochodzi niekiedy bloker USB - jeśli chcemy wykonać kopię binarną pendrive. Podłączamy również klawiaturę, gryzonia, drukarkę, podręczny podgrzewacz do kawy i już pozostają nam w rezerwie tylko 2-3 porty USB w tylnej części obudowy.

Ta sama płyta oferuje nam 10 portów SATA z możliwością konfiguracji macierzy opartą o sprawdzony przeze mnie chipset Intel Matrix Storage Technology, którego zalety będę opisywał później.

Dwa gniazda PCI pozwolą rozszerzyć płytę główną o kontroler FireWire 800 lub 400, ze wskazaniem na ten pierwszy. Jeśli nasz bloker sprzętowy nie posiada gniazda eSATA to na pewno będzie posiadał złącza IEEE 1394 (FireWire), które są standardem w blokerach firmy Tableau oraz ICS. Chciałbym zdementować pewną opinię, która głosi, iż prędkość złącza USB 2.0 jest taka sama jak FireWire 400, a nawet większa. Otóż nie! Proszę spojrzeć do tabeli poniżej na wyniki mojego testu:

	INTERFEJS		
Badany dysk:	**USB 2.0**	**FireWire 400**	**FireWire 800**
Western Digital WD800AAJS SATA	20,5 MB/s	29,2 MB/s	42 MB/s

Jak widać FireWire 400 nieco lepiej wychodzi w porównaniu do USB 2.0 co już pozwoli nam zaoszczędzić kilka cennych minut. Dodam, że wynik dla dysku ATA był taki sam.

Omawiając przygotowanie sprzętu dla informatyki śledczej musimy przede wszystkim mieć na uwadze, aby nie zawężać gardła przepływu danych między blokerem, a jednostką centralną. Kiedy zaczynałem moją przygodę z informatyką śledczą miałem dostęp do blokera z jednym portem USB 2.0 i wykonywanie kopii binarnej dysku 160GB zajmowało sporo czasu. Potem nadszedł bloker bogatszy o FireWire 400 i 800. Jednak żeby zlikwidować całkowicie problem wąskiego gardła i naprawdę poczuć wiatr w żaglach zachęcam do uzbrojenia się w bloker z interfejsem eSATA. Na rynku jest już ich spora ilość m.in. Tableau SATA TK3u lub TK35es oraz FastBloc 3. Maksymalna prędkość brokerów (do 3Gbps) skraca czas analizy nośnika dowodowego lub wykonywania kopii binarnej. W tabeli obok pozwoliłem sobie zrobić krótkie porównanie poprzednio badanego dysku:

	INTERFEJS	
Badany dysk:	**FireWire 800**	**eSATA**
Western Digital WD800AAJS SATA	42 MB/s	70,1 MB/s

Do mojej ulubionej płyty dodawane jest jedno gniazdo eSATA do montażu na tylnich śledziach obudowy. Jeśli będziemy potrzebowali większą ilość tych gniazd to są one ogólnodostępne w sklepach. Na rynku zaczynają pojawiać się płyty główne z USB 3.0, które teoretycznie oferuje transfer do 640 Mb/s. Na potrzeby artykułu napisałem zapytanie do jednego z producentów blokerów sprzętowych odnośnie użycia w ich urządzeniach portu USB 3.0. W odpowiedzi otrzymałem listę urządzeń, które mają wypuścić w tym roku i nie wygląda na to, aby „szli" w ten interfejs. Co może znaczyć, że standardy wyznaczać będzie złącze eSATA.

Następnie trzeba zadbać o to, aby dyski twarde działały maksymalnie wydajnie. Zachęcam do konfiguracji macierzy RAID 0, tak zwanego stripe. Proponuje łączenie w pary dysków o wielkości co najmniej 500 GB. Dzięki temu zapewnimy sobie całkiem sporą przestrzeń do analizy kilku kopii binarnych nośników dowodowych oraz lepszy transfer odczytu i zapisu danych.

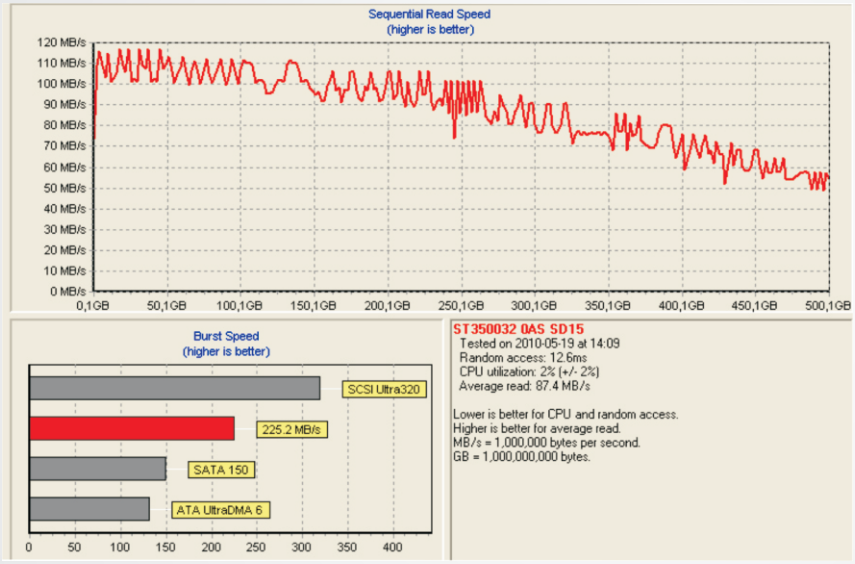
Poniżej przedstawiam test za pomocą narzędzia do benchmarku dysków twardych. W pierwszym oknie do płyty głównej podłączyłem dysk SATA Seagate ST3500320AS ze skonfigurowanym systemem operacyjnym. Jego średnia prędkość odczytu wynosi 95,6 MB/s . Natomiast w drugim oknie przedstawiam wynik testu macierzy, dwóch dysków ze skonfigurowanym systemem operacyjnym.

Jak widać praca na macierzy może znacznie przyspieszyć analizę kopii binarnej. Teraz pewnie zapytacie „No dobrze wszystko fajnie i szybko, ale co z awaryjnością?". W przypadku awarii jednego z dysków tracimy wszystkie dane - jest to wada rozwiązania opartego na macierzach. Jednak są to jednostkowe przypadki, które nie powinny odwieźć nas od użycia macierzy. Zabezpieczeniem przed ewentualnością uszkodzenia jednego z dysków jest dobrze skonfigurowany systemem backupów. Taki system pozwoli na skopiowanie ważniejszych danych oraz systemu na inny nośnik.

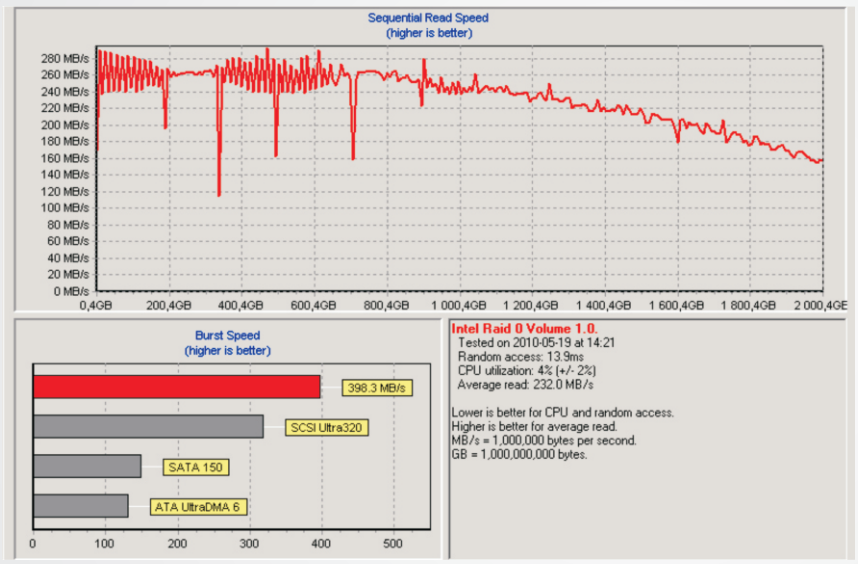
Wybór karty graficznej, ilość rdzeni procesora to drugorzędna sprawa. Na ten moment wiodące programy do informatyki śledczej tj. EnCase oraz FTK nie wykorzystują możliwości szybkich procesorów kart graficznych, jednak są prowadzone badania w tym kierunku. Przy doborze wielkości pamięci RAM pamiętajmy, że jeśli pracujemy na popularnym systemie Windows XP Pro 32 Bitto wielkość musimy ograniczyć do 4 GB. Odnośnie doboru procesora zalecenia wszy-stkich producentów oprogramowania mówią „im szybciej tym lepiej".

W porozumieniu z redakcją Magazynu Informatyki Śledczej w kolejnych numerach będę starał się umieszczać testy urządzeń „forensicowych", aby przybliżyć ich możliwości z poziomu użytkownika.

Autor jest specjalistą informatyki śledczej w laboratorium Mediarecovery, gdzie odpowiada za wdrażanie innowacji hardwareowych. Na swoim koncie ma prawie 200 ekspertyz związanych z poszukiwaniem, analizą i prezentacją elektronicznego materiału dowodowego.



*Wynik testu **SATA Seagate** ST3500320AS 500 GB*



*Wynik testu **macierzy RAID 0** opartej o chipset Intel Matrix Storage Technology w której umieszczono dwa dyski SATA Seagate ST3500320AS 500 GB*

Dowód elektroniczny w ujęciu cywilistycznym – pojęcie dowodu elektronicznego

Błażej Sarzalski

Przepisy obowiązującego Kodeksu postępowania cywilnego nie definiują pojęcia dowodu, tym bardziej próżno szukać w tych regulacjach definicji dowodu elektronicznego, nie oznacza to jednak, że ustawa nie dotyka w ogóle tej problematyki, a wszelkie próby definicyjne zakończą się fiaskiem.

Przepisem otwierającym rozważania o dowodach na gruncie Kodeksu postępowania cywilnego jest unormowanie art. 227 k.p.c., który wskazuje, iż przedmiotem dowodu są fakty mające dla rozstrzygnięcia sprawy istotne znaczenie. Przepis ten wskazuje, iż dowodem jest wszystko co niesie za sobą wiadomości istotne dla rozstrzygnięcia sprawy – innymi słowy, pod pojęciem dowodu należy rozumieć taki środek, który umożliwia przekonanie sądu orzekającego o istnieniu lub nieistnieniu faktów mających istotne znaczenie dla rozstrzygnięcia sprawy cywilnej. Gdy spojrzymy na katalog środków dowodowych w Kodeksie postępowania cywilnego zauważymy, że ustawodawca skatalogował środki dowodowe i nazwał niektóre z nich, wskazując w pierwszej kolejności na dokument, następnie zeznania świadków, opinię biegłych, oględziny, przesłuchanie stron, dowód z grupowego badania krwi, dowód z fotografii, filmu, telewizji, fotokopii, fotografii, planów, rysunków i innych przyrządów utrwalających albo przenoszących obrazy lub dźwięki, ustawodawca wymienia także, w przepisie art. 309 k.p.c. inne środki dowodowe.

Pojawia się w związku z tym pytanie, gdzie w tym obszernym katalogu należy umieścić tzw. dowód elektroniczny (lub może bardziej trafnie: „elektroniczny środek dowodowy") i czym on jest?

Człowiek dokonujący obserwacji na monitorze komputera bądź słuchający w głośnikach sprzętu audio nagrania dźwiękowego nie zdaje sobie zawsze do końca sprawy, że to, co podlega jego aktualnej percepcji jest jedynie końcowym efektem wykorzystania sprzętu elektronicznego oraz procesów programowych (częścią zewnętrzną). Dla dokonania oceny mocy dowodowej tak postrzeganych informacji osoba oceniająca (sędzia, prokurator, uczestniczący w sprawie pełnomocnik strony, sama strona postępowania) powinna rozumieć istotę pochodzenia tych informacji, nie jest ona bowiem tak prosta jak zapis dokumentu za pomocą pisma i długopisu, czy pióra, czy też rysunek bądź obraz.

W pierwszej kolejności zwrócić należy uwagę na nośnik informacji. Obecnie nośnikiem danych elektronicznych mogą być różnorodne urządzenia techniczne – urządzenia do magazynowania danych typu pendrive, płyty cd, dvd, dyski twarde, napędy zip, rzadziej już wykorzystywane dyskietki, taśmy magnetyczne, czy karty dziurkowane. Nośnikiem danych jest też jednak powietrze, w którym rozprzestrzeniają się różnorodne przekazy danych (choćby rozmowy telefoniczne w sieciach komórkowych). Aby dana informacja mogła być wykorzystana dowodowo w postępowaniu sądowym konieczne jest jednak jej utrwalenie, z tego względu, jeżeli nie dokonano utrwalenia danych elektronicznych na nośniku to niemożliwe będzie jej odczytanie. Z drugiej strony, nośnik nie jest sam w sobie dowodem w sprawie – współczesne metody powielania danych powodują, iż możliwe jest kopiowanie takich samych informacji i wprowadzanie do obrotu nawet na skalę przemysłową na wielu rodzajach nośników. To ważne z punktu widzenia osoby oceniającej moc dowodową informacji w formie elektronicznej, rozumiejąc te uwarunkowania osoba ta zdaje sobie sprawę z tego, że to czym dysponuje jest jedynie refleksem, zapisem czegoś co mogło powstać na zupełnie innym nośniku. Stąd bierze się często

poszlakowy charakter elektronicznego środka dowodowego oraz istotność precyzji w pracach nad jego zabezpieczeniem i wprowadzeniem do postępowania.

Gdy osoba oceniająca materiał dowodowy zdaje sobie sprawę z tego, czym jest nośnik informacji, to dostrzega istotę danych na nim zawartych, zwrócić jednak należy uwagę, że bez odpowiedniego sprzętu i oprogramowania żaden obserwator nie jest w stanie odkodować tych danych, elektroniczna postać zapisu, wykorzystująca zjawiska elektromagnetyczne nie jest formą zrozumiałą dla człowieka, dopiero odkodowanie w procesie programowo-sprzętowym pozwala sądowi i innym uczestnikom postępowania na percepcję wyrażonych w formie elektronicznych informacji. Stąd istotne jest, aby program i sprzęt jakim posługujemy się przy przetworzeniu danych na zrozumiałą dla człowieka formę, pozwalał zrobić to w sposób bezstratny, bez zniekształceń i błędów, w innym razie wartość środka dowodowego może być niewielka (przykład z praktyki: wygenerowanie na komputerach dwóch różnych osób pliku elektronicznego, który stanowi potwierdzenie zawarcia transakcji co do tego samego przedmiotu na serwisie aukcyjnym, co jest ewidentnym błędem programowym - wartość takiej informacji w przypadku przedstawienia jej sądowi jest nikła). Druga strona medalu to możliwość modyfikacji danych – stąd osoba oceniająca powinna zdawać sobie sprawę z tego, że zapis elektroniczny jest mimo wszystko nietrwały i tylko określone procedury zabezpieczenia danych pozwalają na przyjęcie pewności, co do okoliczności ich powstania.

...dokończenie na stronie 8

Brakujące połączenie

Deborah Leary

Globalizacja i era informacji zmieniła nasz sposób życia i pracy w społeczeństwie. Pociąga to za sobą konieczność zmiany takich dyscyplin jak śledztwo kryminalne i analiza wywiadowcza. Charakter zagrożenia, przed którym stoimy obecnie jest trudniejszy niż w kiedykolwiek w historii. Organizacje przestępcze są luźno powiązane w sieci osób, którzy ukrywają się pod pozornie normalnym życiem, w oczekiwaniu na prawie nieograniczone możliwości tworzenia chaosu i strachu w naszej społeczności. Mogą szybko zmieniać metody - a zatem nasza odpowiedź musi się do nich dopasowywać. Bezpieczeństwo publiczne i skuteczne egzekwowanie musi zaangażować się w proces innowacji, aby dotrzymać kroku problemom przestępczym.

Pojawiła się potrzeba bycia nie tylko w kontakcie z najnowszą techniką w walce z przestępczością i terroryzmem, ale także konieczność spojrzenia poza to, co jest aktualnie dostępne, by być o krok do przodu w stosunku do potencjalnych zagrożeń.

Informacja, szybko staje się najbardziej poszukiwanym i cennym surowcem na świecie. Jest powszechnie dostępna, łatwo przesyłana i wykorzystywana przez grupy przestępcze, których nie ograniczają moralne, etyczne, prawne, a nawet logistyczne bariery jakie mają organy ścigania i agencje rządowe. Oznacza to, że musimy być „krok przed" by bitwa została wygrana.

Najważniejszym obszarem, który musimy opanować jest pomysłowe i inteligentne wykorzystanie informacji, jakie posiadamy. Nauka i technika umożliwiła ludziom gromadzenie ogromnych ilości danych. Niestety, ta umiejętność nie ma swojego odpowiednika w zdolności do analizy sensu informacji.

Jedną z głównych kwestii poruszanych przez policję i agencje wywiadowcze jest efektywna i skuteczna analiza personalnych urządzeń, takich jak telefony komórkowe. Szacuje się, że w samej tylko Wielkiej Brytanii do sieci jest ich podłączonych ok. 80 milionów. Globalnie liczba ta wynosi około trzech miliardów! W konsekwencji stwarza to ogromne wyzwanie dla organów ścigania, ponieważ potężne ilości danych są trudne do zgromadzenia, przetwarzania i analizowania.

Telefony komórkowe szybko stają się nie tylko środkiem komunikacji, ale służą do przesyłania danych, zamawiania produktów, chatów. Analiza takiej ilości danych staje się czasochłonna i trudna, a w rzeczywistości niemożliwa bez pomocy zaawansowanych komputerów.

Dlatego dziś nie bez znaczenia jest fakt współpracy organów z nowoczesnymi firmami. Mając technologię do rozwiązania tego problemu Forensic Pathways umożliwia policji analizy na zasadzie "big picture". Zebrane dane połączone w sieć, pozwalają analitykowi zobaczyć powiązania tysięcy urządzeń mobilnych i komunikacji między nimi w tym samym czasie. Technologia ta wykracza poza możliwości mózgu, prezentując połączenia, które normalnie są trudne do wychwycenia.

Dochodzenie w związku z 11 września pokazało, że nie brakowało informacji aby udaremnić działalność napastnikom. Nie było jednak możliwości szybkiego łączenia krytycznych elementów. Obecnie wyszukiwanie informacji w dużych zbiorach danych nie jest już problemem. Zdolność do podjęcia szybkiego wyszukiwania i automatycznych analiz pozwala wyobrazić i uświadomić sobie sytuację.

Nowoczesna technologia umożliwia policji i służbom bezpieczeństwa pobieranie danych z różnych źródeł i łączenie ich umożliwiając skuteczne, szybkie wyszukiwanie.

Łączenie wysp informacji w "silosy danych" pomaga odnaleźć brakujące ogniwo. Zlokalizowanie igły w tysiącu stogów siana staje się możliwe. Problem nadmiaru informacji nie może być powodem do pobieżnych analiz. Obecnie Brytyjska Komenda Główna Policji stosuje naszą technologię do integracji ponad 15 milionów zestawów danych dotyczących tożsamości, zdarzeń i urządzeń, bez konieczności zakłócania codziennej pracy operacyjnej. Korzystanie z tej formy logiki, umożliwia identyfikację punktów krytycznych. Nawet bez dostępu do osobistego urządzenia przestępcy, można zidentyfikować komunikację ukazując powiązania między ludźmi.

Tylko dzięki zaangażowaniu w innowacyjność i podejmowane interdyscyplinarnych wyzwań, będziemy naprawdę skuteczne radzić sobie z wyzwaniami. Tradycyjna kryminalistyka i informatyka śledcza na arenie ery informacji, musi się rozwijać zapewniając, że jesteśmy silni wobec tych którzy łamią prawo. Ewolucja ta sprawi, że informacja i dane, które są dostępne, będą skutecznie wykorzystane w dochodzeniach.

Deborah Leary jest założycielką i dyrektorem generalnym Forensic Pathways. Firma jest międzynarodowym dostawcą usług Business Intelligence a także produktów, szkoleń i doradztwa z zakresu informatyki śledczej. W 2008 roku została uhonorowana tytułem „International Entrpreneur of the Year 2007" przez Światowe Stowarzyszenie Kobiet Przedsiębiorców. Jest przewodniczącą Midlands World Trade Forum oraz wiceprzewodniczącą United Nations UK Global Compact Network.

Magazyn informatyki śledczej
mediarecovery Instytucja Specjalistyczna

Adres redakcji:
Instytucja Specjalistyczna Mediarecovery,
40-723 Katowice, ul. Piotrowicka 61.
Tel. 032 782 95 95, fax 032 782 95 94,
e-mail: redakcja@mediarecovery.pl

Redakcja:
Zbigniew Engiel (red. nacz.),
Przemysław Krejza, Jarosław Wójcik.
Skład, łamanie, grafika: Tomasz Panek.
Reklama: Anna Czepik.

Wydawca:
Media Sp. z o.o.,
40-723 Katowice, ul. Piotrowicka 61.
Tel. 032 782 95 95, fax 032 782 95 94,
e-mail:biuro@mediarecovery.pl

Dowód elektroniczny w ujęciu cywilistycznym – pojęcie dowodu elektronicznego

...dokończenie ze strony 6

Wobec powyższego proponuję, aby przyjąć definicję elektronicznego środka dowodowego, która dotyka wszystkich z wymienionych wyżej aspektów: Dowód elektroniczny jest to każda informacja mająca utrwaloną postać elektroniczną, dająca się prawidłowo odczytać za pomocą odpowiedniego sprzętu i oprogramowania, która jednocześnie ma istotne znaczenie dla rozstrzygnięcia toczącej się sprawy cywilnej.

Tak rozumiany dowód elektroniczny powinien być przedmiotem przeprowadzenia w postępowaniu cywilnym z wykorzystaniem normy art. 309 Kodeksu postępowania cywilnego mówiącej o tzw. innych środkach dowodowych, niemniej jednak nie można wykluczyć, iż w zakresie, w jakim dane elektroniczne przybierają zewnętrzną formę obrazów lub dźwięków zastosowanie w konkretnej sprawie znajdzie też art. 308 § 1 kodeksu, który wskazuje na możliwość dopuszczenia dowodu z płyt lub taśm dźwiękowych i innych przyrządów utrwalających albo przenoszących obrazy lub dźwięki (w tym sensie dowód elektroniczny nie jest w polskim postępowaniu cywilnym absolutną nowością). Nie może jednak umknąć uwadze, że ustawodawca w przepisie art. 308 § 1 zbyt bardzo akcentuje rolę nośnika, nie zaś informacji, jaką nośnik przenosi, być może nowelizacja kodeksu w tym zakresie i wprowadzenie ogólnej regulacji elektronicznych środków dowodowych pozwoliłaby usystematyzować tą problematykę i stanowiłoby normatywną wskazówkę, co do sposobu postępowania z tego typu dowodami.

Autor jest aplikantem radcowskim w Kancelarii Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy w Katowicach.