MAGAZYN

NR 19/WRZESIEŃ 2013

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Triage i Live Forensic.
Analizy w środowisku „big data"
V Konferencja Informatyki Śledczej

METODYKA TRIAGE
Karol Szczyrbowski

DOWÓD ELEKTRONICZNY
CZY JESTEŚMY GOTOWI?
CZYLI NOTARIUSZ W ROLI PRINTSCREENA
Janusz Tomczak

LIVE FORENSIC - Zasady zbierania dowodów elektronicznych
Przemysław Krejza

LIVE FORENSIC-Kontrowersje prawne związane z materiałem dowodowym.
Jarosław Góra

V Ogólnopolska Konferencja Informatyki Śledczej. Warszawa - 4 październik, Biblioteka Uniwersytecka w Warszawie. **Organizator:**

Od redakcji

19 numer Magazynu Informatyki Śledczej i Bezpieczeństwa IT, który właśnie trzymasz w ręku poświęciliśmy w całości tematyce Triage i Live Forensic – nowym metodom akwizycji danych, które w przełomowy sposób ułatwiają pracę informatyków śledczych.

Obserwując gigantyczną ilość danych przetwarzanych każdego dnia w chmurze oraz galopujący wzrost pojemności dysków nietrudno zdać sobie sprawę, że analizy śledcze wykonywane tradycyjnymi metodami wymagającymi czasochłonnego zabezpieczenia wszystkich nośników wkrótce stracą rację bytu. Potrzebna jest wstępna selekcja i segregacja danych przeznaczonych do analizy.

Rewolucja jaką okazały się metody Triage i Live forensic porównywana jest czasami z przełomem, który dokonał się w badaniu trzeźwości kierowców podczas zastąpienia badań w laboratorium przenośnym alkomatem. Niewątpliwie pozwala zaoszczędzić czas i środki, niejednokrotnie marnotrawione na ekspertyzy niepotrzebnych nośników. Obrazki na których komputery przeznaczone do zabezpieczenia wywozi się z firmy wózkami powoli odchodzą w przeszłość.

Live Forensic umożliwia analizę danych obecnych na włączonych systemach a więc także dostępnych w chmurze i pamięci RAM, podgląd uruchomionych aplikacji, podłączonych urządzeń bez ryzyka utraty dostępu do danych spowodowaną np. szyfrowaniem . Triage pozwala na zawężenie obszaru poszukiwań wyłącznie do istotnych danych co owocuje szybszym postępem prac związanych z ekspertyzą. Czasem można ją wydać już tego samego dnia – co w przypadku kanonicznej metody prowadzenia analiz byłoby niewykonalne.

W numerze między innymi: wprowadzenie do Live Forensic, Triage okiem praktyka oraz dlaczego notariusz nie jest potrzebny w procesie zabezpieczania materiału dowodowego.

Oczywiście ograniczenia wydawnicze nie pozwalają nam na pełne wyczerpanie tematu. Dla zainteresowanych nieocenionym źródłem wiedzy będzie z pewnością V Ogólnopolska Konferencja Informatyki Śledczej, która odbędzie się 4 października w Warszawie.

Magazyn Informatyki Śledczej i Bezpieczeństwa IT jest patronem medialnym tego wydarzenia. Wszystkich chętnych odsyłamy do zapoznania się ze szczegółami na stronie www.siis.org.pl/konferencja.

W skrócie:

Ujawniony budżet National Security Agency

10,8 miliarda dolarów – tyle według informacji ujawnionych przez Washington Post wynosi budżet operacyjny NSA, który w 2013 roku zostanie przeznaczony m.in. na inwigilację Internautów. Warto zaznaczyć że na przestrzeni ostatnich 9 lat kwota ta uległa podwojeniu. Zatrudniając ponad 23 tys. osób jest drugą (po CIA) największą agencją wywiadowczą USA. Dodajmy że łączny budżet wszystkich 12 agencji wywiadowczych w USA wynosi 52,8 miliarda dolarów czyli dokładnie trzykrotność rocznych wydatków NASA.

XRY 6.6 na testach w Polsce

Microsystemation, producent rozwiązań do analiz urządzeń mobilnych ogłosił premierę najnowszej wersji swojego flagowego produktu. XRY v. 6.6 pozwala na dostęp i ekstrakcję danych z ponad 9500 modeli urządzeń mobilnych. Urządzenie umożliwia m.in. odczyt wiadomości SMS, MMS, email, zawartości skrzynki telefonicznej, lokalizacji GPS, kalendarzy czy historii www. Polski dystrybutor udostępnia Polskim służbom sprzęt do darmowych testów.

EnCase Portable

Jest rozwiązaniem umożliwiającym przeprowadzenie procesu Triage zgodnie z zasadami informatyki śledczej. Dzięki skróceniu czasu dotychczas przeznaczonego na zebranie danych można poświęcić go więcej na właściwą analizę materiału dowodowego. Dzięki prostocie obsługi proces zbierania danych może być przeprowadzany również przez osoby nietechniczne, a kompaktowe rozmiary zapewniają wysoką mobilność.

Live Forensic - zasady zbierania dowodów elektronicznych

Przemysław Krejza

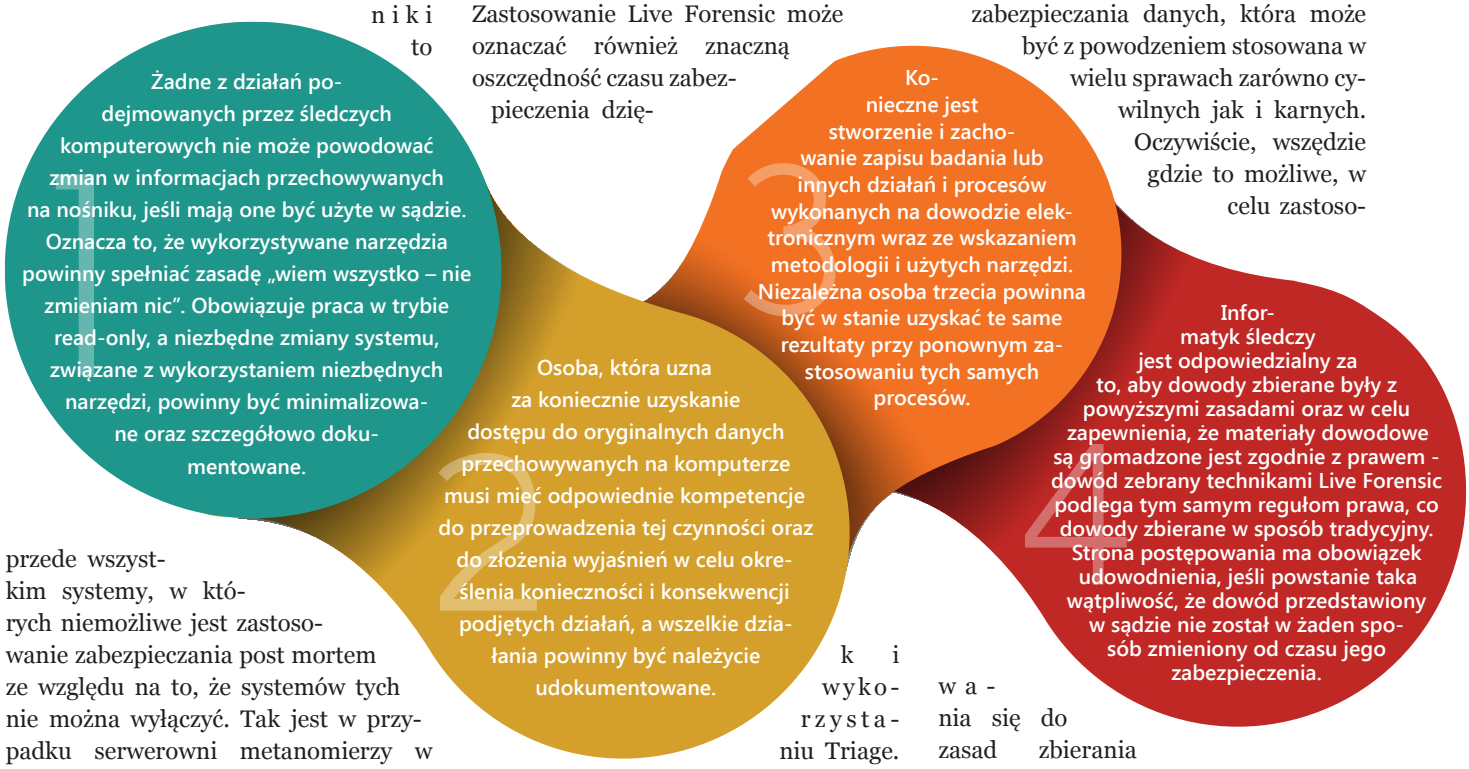
Live Forensic to technika zbierania dowodów elektronicznych z systemów komputerowych bez ich wyłączania. Przykłady zastosowań tej techniki to przede wszystkim systemy, w których niemożliwe jest zastosowanie zabezpieczania post mortem ze względu na to, że systemów tych nie można wyłączyć. Tak jest w przypadku serwerowni metanomierzy w kopalniach lub serwerów hostujących ważne aplikacje biznesowe. W tych sprawach konieczne jest zabezpieczenie dowodów bez wyłączania komputerów. Live Forensic pozwala również na skopiowanie informacji z komputera, którego nośnik trwały może być zaszyfrowany, a komputer ten jest włączony. W takim wypadku, przed wyłączeniem, istnieje możliwość skopiowania danych, których rozszyfrowanie nie będzie możliwe.

Techniki Live Forensic są również niezbędne w przypadku zabezpieczania pamięci RAM, która jest cennym źródłem dowodów we wszystkich sprawach – począwszy od analiz powłamaniowych oraz malware, na nieuczciwości pracowników kończąc, gdzie maile lub rozmowy komunikatorów będą znajdowały się w pamięci, mimo wyłączonych archiwów komunikatorów.

Zastosowanie Live Forensic może oznaczać również znaczną oszczędność czasu zabezpieczenia dzięki wykorzystaniu Triage. Dzięki tej technice możliwe jest przeanalizowanie materiału dowodowego na miejscu zabezpieczania i pominięcie kopiowania nieistotnych nośników. Targeted Triage z kolei, pozwala na zabezpieczenie tylko wybranych danych (bez kopiowania całych nośników), co jest szczególnie istotne np. w sprawach gdzie na serwerze z danymi znajdują się informacje wielu podmiotów, a nie tylko „podejrzanego".

Zasady gromadzenia dowodów w technice Live Forensic są dokładnie takie same jak w technikach „tradycyjnych". Jak zwykle ważna jest dbałość o integralność dowodu. Konieczne jest także przedstawienie sposobu, w jaki zebrano dowód przedstawiając kolejne etapy tego procesu. Obowiązują cztery podstawowe zasady.

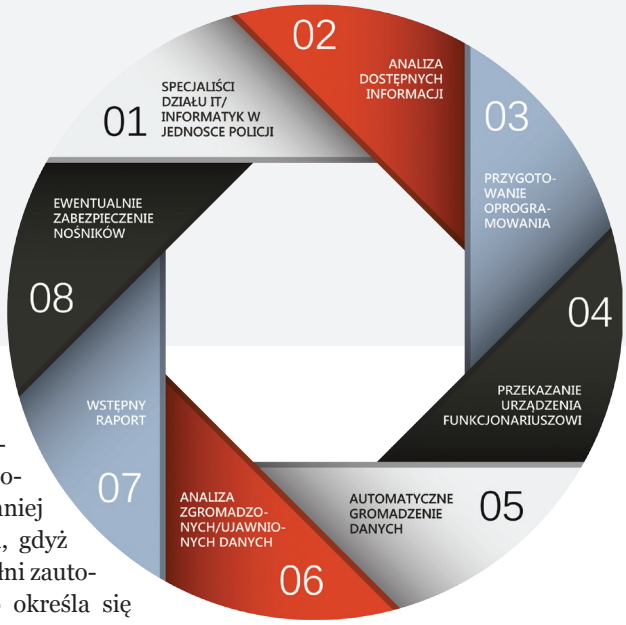
Live Forensic jest nowoczesną techniką zabezpieczania danych, która może być z powodzeniem stosowana w wielu sprawach zarówno cywilnych jak i karnych. Oczywiście, wszędzie gdzie to możliwe, w celu zastosowania się do zasad zbierania dowodów elektronicznych, powinno wykonywać się kopię binarną całego nośnika danych. Częściowe lub selektywne kopiowanie plików może być uznane za alternatywę jedynie w określonych okolicznościach, np., gdy ilość danych przeznaczonych do skopiowania czyni wykonanie kopii całościowej niemożliwym lub zaistniały określone ryzyka – np. nośnik jest zaszyfrowany. Jednakże śledczy powinny być pewni, że w takim wypadku zabezpieczyli wszystkie istotne dowody oraz użyli odpowiednich narzędzi. ■



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

Metodyka Triage w informatyce śledczej

Karol Szczyrbowski



Metodologia Triage jest nowym podejściem do procesu zabezpieczania i analizy danych cyfrowych na potrzeby informatyki śledczej. W ostatnim czasie zyskuje coraz większą popularność kosztem tradycyjnego modelu wykonywania analiz. Pojęcie „Triage" pochodzi od terminu medycznego, określającego sposób selekcji rannych na polu walki. W przypadku informatyki śledczej jest procesem identyfikacji, sortowania oraz filtrowania mającym na celu ustalenie priorytetów oraz kategorii, zabezpieczanych lub gromadzonych informacji/danych.

Sam proces, w odróżnieniu od tradycyjnego modelu, różni się znacznie ilością danych zebranych podczas zabezpieczenia materiału dowodowego. Ilość „zbędnych" informacji zostaje tutaj w sposób drastyczny ograniczona, dzięki czemu sama analiza dotyczy jedynie danych mających związek ze sprawą. Wykorzystanie podejścia typu Triage może wynikać z różnych potrzeb oraz sytuacji przed którymi staje osoba mająca zabezpieczyć dane. Są nimi np. włączony komputer z zaszyfrowanym dyskiem twardym, brak możliwości lub czasu wymaganego na zabezpieczenia całego nośnika danych, potrzeba wyodrębnienia określonych danych.

Samo powstanie i coraz większa popularność metodologii Triage wynika z narastających problemów, z którymi borykają się informatycy śledczy. Coraz pojemniejsze nośniki danych (w tym roku do sprzedaży detalicznej zostały wprowadzone dyski twarde o pojemności 4 TB a na rok 2014 zostały zapowiedziane dyski 5 i 6 TB) oraz ogromna ilość danych zalegających na nich wpływają na czas i koszty pracy co także przekłada się na dłuższe wykorzystanie sprzętu na którym prowadzone są czynności związane z informatyką śledczą.
Dodatkowo, wykorzystanie narzędzi typu Triage pozwala na współpracę z mniej wyszkolonym personelem, gdyż sam proces może być w pełni zautomatyzowany. Początkowo określa się cele działania oraz programuje narzędzia Triage – najczęściej występujące w postaci „kluczy USB". Czynności te wykonuje specjalista, aby móc później przekazać go dalej osobom, które będą mogły podłączyć narzędzie do badanego komputera a tym samym pozwolić na jego automatyczne uruchomienie i wykonanie wcześniej zaprogramowanych działań na badanym komputerze.

Ta funkcjonalność pozwala na zwiększenie wielkości zespołu biorącego udział w zabezpieczeniu bez potrzeby przeprowadzania specjalistycznych szkoleń. Coraz większą bolączką informatyków śledczych staje się szyfrowanie partycji systemowych lub całych dysków twardych, które mniej lub bardziej skutecznie utrudniają ich pracę. Podejście typu Live Forensics (zabezpieczanie materiału z włączonego komputera) wraz z procesem Triage może być skutecznym rozwiązaniem tego problemu.

Przydatność metodologii Triage najlepiej ukazuje sytuacja w której w firmie, w której znajdowało się 200 komputerów podejrzewano, że któryś z pracowników ściąga pliki graficzne zawierające pedofilię dziecięcą na komputer.
Zaprojektowano narzędzie tak, by zostały wyodrębnione wszystkie pliki graficzne, które zostały w późniejszym etapie sprawdzone przez informatyka śledczego. Założono, że każdy komputer, na którym znaleziono jakiekolwiek pliki graficzne zawierające materiały pornograficzne, zostanie zakwalifikowany do późniejszej, pełnej analizy.

Odpowiednie wykorzystanie narzędzi Triage pozwoliło ograniczyć liczbę zabezpieczanego sprzętu z 200 do 20 komputerów, czyli aż o 90% ! Ostatecznie, wpłynęło to znacząco na czas i koszty przeprowadzenia zabezpieczenia i analizy danych a firma mogła dalej funkcjonować bez większych zakłóceń. Nietrudno sobie wyobrazić jaki wpływ na działanie przedsiębiorstwa miałoby zabezpieczenie wszystkich 200 komputerów.

Kolejnym przykładem jest sytuacja kiedy podejrzewano pracownika o przechowywanie na komputerze dokumentów, do których nie powinien mieć dostępu. Ze względu na delikatny charakter i brak możliwości wykonania pełnej kopii binarnej, postanowiono o wykorzystaniu narzędzia Triage. Zostało ono zaprogramowane tak by przeszukiwało komputer pod kątem występowania dokumentów oraz słów kluczowych co pozwoliło na wstępne odnalezienie dokumentów i późniejsze dalsze działania w celu udowodnienia winy pracownika.

By przybliżyć ideę oraz praktyczne wykorzystanie Triage w procesie informatyki śledczej, zapraszam do wzięcia udziału w V Ogólnopolskiej Konferencji Informatyki Śledczej noszącej tytuł „Analizy w środowisku big data. Triage i Live Forensic", która odbędzie się 4 października 2013 w Warszawie.

Autor jest młodszym specjalistą informatyki śledczej w laboratorium Mediarecovery.

Live Forensic - kontrowersje prawne związane z materiałem dowodowym

Jarosław Góra

Informatyka śledcza ma na celu odszukanie, zabezpieczenie i dostarczenie elektronicznego materiału dowodowego, świadczącego o popełnionym przestępstwie, nadużyciu, czy zaistniałym incydencie. Tradycyjnie, informatycy śledczy zabezpieczają nośnik, którego kopia binarna poddawana jest następnie szczegółowej analizie (tzw. model post mortem). Jednak dziś, kiedy odchodzi się od tradycyjnych nośników danych zainstalowanych w urządzeniach na rzecz chmury obliczeniowej, a także kiedy wiele informacji dostarczają dane ulotne, coraz większe znaczenie odgrywa informatyka śledcza w modelu live forensic.

Na pierwszy rzut oka model ten „gryzie się" z podstawową zasadą informatyki śledczej - „widzę wszystko, nie zmieniam nic" i pracy na kopii - zapewniających pełną integralność materiału dowodowego oraz rozliczalność działań podjętych przez informatyka śledczego.

Zatem, czy materiał dowodowy zgromadzony metoda live forensic może zostać wykorzystany przed sądem?

Jednym z najczęściej podnoszonych w praktyce zarzutów wobec elektronicznego materiału dowodowego polega na wskazaniu, że osoba zabezpieczająca ten materiał dokonała jego modyfikacji, przez co przestaje on być wiarygodny. Z tego właśnie względu informatycy śledczy nie ingerowali w oryginalny nośnik, który zabezpieczali w sposób uniemożliwiający dokonywanie jakichkolwiek modyfikacji, natomiast analizy dokonywali na kopii binarnej. Z reguły wyłączali urządzenie i zabierali je celem sporządzenia kopii i przeprowadzenia analizy.
Dziś dane, które mogą mieć znaczenie dla rozstrzygnięcia sprawy, a więc które mogą stanowić dowód w postępowaniu przed sądem, nie znajdują się często na urządzeniu, ale na wirtualnym dysku (w chmurze), z którym urządzenie łączy się poprzez mobilny internet. Z drugiej strony, nawet jeśli mamy do czynienia z „tradycyjnym" urządzeniem wyposażonym we własny dysk to po pierwsze, mając na uwadze często gigantyczną pojemności takich dysków nie warto zabezpieczać ich w całości, ale dokonać pewnej selekcji, a po drugie nie można ignorować informacji gromadzonych na nośnikach ulotnych np. w pamięci RAM, która obecnie może mieć 8 GB (i więcej) pojemności. I w końcu warto pamiętać, że wyłączenie urządzenia może być nieodwracalne i w przypadku skutecznego szyfrowania utraci się dostęp do danych.

Rozwiązaniem wskazanych wyżej problemów zdaje się być przeprowadzanie „operacji na żywym organizmie", a więc na uruchomionym urządzeniu i jego oryginalnych nośnikach (trwałych i ulotnych), przy otwartym dostępie do danych znajdujących się w chmurze. Poprzez odpowiednie narzędzia informatyk śledczy podłącza się do działającego systemu i dokonuje zabezpieczenia danych (po ich wcześniejszej ocenie i selekcji), które następnie analizuje.

Jednak z modelem live forensic wiąże się klika poważnych problemów.
Pierwszy dotyczy nieuniknionego pozostawiania śladów działalności informatyka śledczego w analizowanym systemie i na badanych nośnikach, a więc może naruszać integralność. Z technicznego

MAGAZYN
INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: redakcja@mediarecovery.pl

Redakcja
Sebastian Małycha (red. nacz.),
Przemysław Krejza
Skład, łamanie, grafika: Marcin Wojtera
Reklama: Sebastian Małycha

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: biuro@mediarecovery.pl

mediarecovery
Lider informatyki śledczej

punktu widzenia nie da się bowiem ingerować w system (używać go) bez pozostawiania śladów tej ingerencji. To zaś naraża na zarzut, o którym wspominałem wyżej, który może skłonić sąd do uznania dowodów za niewiarygodne (skoro zabezpieczający i analizujący dowód mógł wpłynąć na jego treść).

Drugi dotyczy wątpliwości, czy dokonujący zabezpieczenia informatyk śledczy, działający nawet na zlecenie organów ścigania w ramach postępowania przygotowawczego, jest uprawniony do zabezpieczenia i analizy danych znajdujących się na wirtualnym dysku (w chmurze), dostępnych za pośrednictwem badanego sprzętu (systemu). Czy organy ścigania nie powinny jednak zwrócić się o udostępnienie tych danych do podmiotu świadczącego usługę w chmurze na rzecz osoby, której sprzęt jest analizowany?
Analiza sprzętu komputerowego (zasobów systemu informatycznego) w ramach postępowania karnego to nic innego jak instytucja przeszukania, dokonywana w celu znalezienia rzeczy (informacji) mogących stanowić dowód w sprawie. Należy pamiętać, że podstawą przeszukania jest uzasadnione podejrzenie, że poszukiwane rzeczy, a w naszym przypadku dane informatyczne, znajdują się tam, gdzie są poszukiwane, a więc na danym urządzeniu. W przypadku danych w chmurze, informacje znajdują się gdzieś na serwerze podmiotu świadczącego usługi cloudcomputingu. Jeśli poprzez badany sprzęt brak jest dostępu do danych w chmurze np. ze względu na konieczność podania loginu i hasła, nie pozostaje nic innego jak zwrócić się do usługodawcy o udostępnienie znajdujących się w chmurze danych. Co jednak w przypadku, kiedy dostęp przy pomocy badanego sprzętu jest możliwy?

W mojej ocenie, jeśli zachodzi uzasadnione podejrzenie, że na wirtualnym dysku, do którego dostęp jest możliwy bez przełamywania zabezpieczeń (dostęp nie jest zabezpieczony, albo użytkownik nie wylogował się), znajdują się informacje mogące stanowić dowód w sprawie, należy dokonać ich oględzin, przeszukania i ewentualnie zabezpieczenia.

Jeśli natomiast chodzi o zabezpieczenie się przed ewentualnym zarzutem naruszenia integralności zabezpieczanego materiału dowodowego, zabezpieczenie powinno odbywać się z poszanowaniem dobrych praktyk, tj.:

- precyzyjne dokumentowanie każdej czynności – protokół – pomocnym rozwiązaniem może być protokołowanie również za pomocą urządzenia rejestrującego obraz i dźwięk,
- udział w czynnościach kliku osób, sporządzających własne notatki ze wszystkich dokonywanych czynności i ich rezultatów,
- używanie uruchomionego systemu w minimalnym, niezbędnym zakresie (bez otwierania niepotrzebnych okien i programów; bez niepotrzebnego zamykania już uruchomionych, itd.)
- używanie odpowiednich narzędzi informatyki śledczej, dedykowanych dla metody live forensic, podłączanych przez zewnętrzne porty (bez instalacji na badanym systemie),
- znajomość narzędzi, których się używa – wiedza o tym, jakie ślady narzędzia te pozostawią w badanym systemie.

Celem stosowania się do wyżej wskazanych, przykładowych dobrych praktyk (przepisów nigdzie nie znajdziemy, orzecznictwa również brak) jest zapewnienie pełnej rozliczalności z czynności dokonanych przy zabezpieczeniu oraz możliwość odparcia zarzutu o naruszenie integralności poprzez dokładne wskazanie w jakim zakresie nastąpiła ingerencja w system, na którym dokonano zabezpieczenia danych.

Podsumowując, w mojej ocenie materiał dowodowy zgromadzony i zabezpieczony w modelu live forensic, na skutek pracy informatyka śledczego „na żywym organizmie", może zostać wykorzystany przed sądem w każdym rodzaju postępowania. Poprzez zastosowanie się do dobrych praktyk unikniemy zarzutów w zakresie naruszenia cudzych praw, czy „zanieczyszczenia" materiału dowodowego.

Autor jest szefem Zespołu Prawa IP i Nowych Technologii w kancelarii Ślązak, Zapiór i Wspólnicy, Kancelaria Adwokatów i Radców Prawnych. Specjalizuje się w zakresie prawa własności intelektualnej i nowych technologii. Prelegent na wielu konferencjach, a także prowadzący szeregu szkoleń związanych z IP, IT oraz bezpieczeństwem informacji. Trener w ramach Akademii Informatyki Śledczej.

Dowód elektroniczny - czy jesteśmy gotowi?

Czyli notariusz w roli printscreena.

Janusz Tomczak

Problem do rozwiązania? - uwagi na tle praktyki wykorzystania informatyki śledczej w postępowaniach dowodowych toczących się na podstawie ustawy

Informatyka śledcza jest dziedziną, która rozwija się tak szybko jak szybko rozwijają się technologie informatyczne i cyfrowe. Niemniej stwierdzenie, że prawo nie nadąża za rozwojem technologii w przypadku informatyki śledczej nie jest nawet nieadekwatne, - ono w żaden sposób nie odzwierciedla złożoności zagadnień, które powstają w związku z możliwościami wykorzystania zaawansowanych narzędzi, którymi posługują się informatycy śledczy.

Problem nie tkwi jednak tylko i wyłącznie w niedoskonałości obowiązującego prawa. Aby uzyskać pełny obraz funkcjonowania informatyki śledczej w praktyce wymiaru sprawiedliwości należy zwrócić uwagę z jednej strony na rosnącą liczbę czynności procesowych z udziałem biegłych z zakresu informatyki, podnoszący się poziom wyposażenia jednostek prokuratury i sądownictwa w środki umożliwiające przechowywanie oraz prezentację materiałów cyfrowych, z drugiej strony ogólny, niski poziom wiedzy prawników na temat zastosowania technologii informatycznych w ich pracy, przeważającą niechęć prawników - osób o formacji humanistycznej do nauk ścisłych, które wykorzystują już dawno „wyparte" przez nich pojęcia m.in. „algorytmu", itp. Prawnicy przyzwyczajeni są zazwyczaj do tradycyjnych metod analizy dostępnych informacji o prowadzonej sprawie i z nieufnością podchodzą do nowinek w tym zakresie.

Kiedy przygotowując się do napisania niniejszego tekstu zwróciłem się do kilkudziesięciu moich kolegów (adwokatów i radców prawnych) z pytaniem: z jakim sposobem zabezpieczenia treści znajdujących się w internecie zetknęli się w swojej praktyce – w odpowiedzi uzyskałem informację, że był to protokół sporządzony przez notariusza, który opisał w nim fakt wyświetlenia na jego kancelaryjnym komputerze strony internetowej o określonej treści w określonym czasie. Większość z nich to osoby mające do czynienia głównie z procesami cywilnymi niemniej dominowała opinia, że jest to najpewniejszy sposób „uchwycenia" w czasie i miejscu określonej treści, co pokazuje po części stan wiedzy o informatyce śledczej. Metoda poświadczania przez notariusza określonych zdarzeń, co do zasady, nie zmieniła się od stuleci.

W większości tekstów prawniczych poświęconych informatyce śledczej kontekst, w którym umieszcza się to pojęcie dotyczy zabezpieczania dowodów. Chodzi zatem o sytuacje, w których istotne jest utrwalenie w formie elektronicznej informacji - bez ingerowania w nie – mających znaczenie dowodowe w sprawie.

Kodeks postępowania karnego w tym zakresie odsyła zainteresowanych poprzez „odpowiednie stosowanie" do przepisów o zatrzymaniu rzeczy i przeszukaniu (Rozdział 25, art. 236a Kodeksu postępowania karnego), a więc regulacji, która od początku tworzona była na potrzeby zbierania dowodów rzeczowych. Takie podejście ogranicza rolę informatyka do roli technika dbającego o wiarygodność i autentyczność zabezpieczanych danych.

Kodeks pomija jednak funkcje „wykrywcze" informatyki śledczej jako narzędzi ściśle śledczych, służących zbieraniu i analizowaniu informacji. Być może zagadnienia te nie powinny być przedmiotem regulacji prawnokarnych a administracyjnych, uwzględniających potrzeby ochrony danych osobowych, w tym powtarzaną od kilku lat potrzebę uregulowania zagadnienia monitoringu w miejscach publicznych. 30 marca 2009r., w odpowiedzi na interpelację poselską nr 7857 ówczesny sekretarz stanu w Ministerstwie Sprawiedliwości „w sprawie postępowania z dowodami elektronicznymi" wyjaśnił, że: „Odnosząc się do postulowanej w interpelacji weryfikacji przepisów dotyczących omawianej problematyki, należałoby rozstrzygnąć w pierwszej kolejności, na ile specyfika dowodów elektronicznych wymaga wydania aktu prawnego normującego kwestie związane z zabezpieczaniem i przetwarzaniem dowodów elektronicznych. Wskazać należy bowiem, że w odniesieniu do innych specyficznych dowodów kwestie te w znacznej części pozostawiono do rozstrzygnięcia kryminalistyce i innym gałęziom nauki, których osiągnięcia są wykorzystywane w procesie karnym. Z uwagi na dynamiczny rozwój informatyki i telekomunikacji problematyczne zagadnienie stanowiłaby również kwestia odpowiedniego stopnia szczegółowości takich unormowań, aby wskutek bardzo szybkiego rozwoju tych dziedzin nauki nie stanowiły one wkrótce praktycznej bariery w postępowaniu z dowodami elektronicznymi, falsyfikując aktualność wprowadzonych tymi unormowaniami rozwiązań."

W zakresie poruszonego w interpelacji problemu kwalifikacji biegłych wydających opinie w przedmiocie dowodów elektronicznych należy stwierdzić, że z uwagi na okoliczność, że ocena dowodów elektronicznych zazwyczaj wymaga posiadania wiadomości specjalnych, zwykle organ procesowy na podstawie art. 193 K.p.k. zasięga opinii biegłego lub stosownej instytucji naukowej lub specjalistycznej. Każdy biegły zobowiązany jest do wykonania powierzonych mu obowiązków z całą sumiennością i starannością, zgodnie ze złożonym przyrzeczeniem. Kryteria,

jakie spełniać ma biegły każdej specjalności, oraz tryb ustanawiania biegłych sądowych, pełnienia przez nich czynności oraz zwalniania ich z funkcji określa rozporządzenie ministra sprawiedliwości z dnia 24 maja 2005 r. w sprawie biegłych sądowych (Dz. U. Nr 15, poz. 133).

Przedstawiony w interpelacji postulat dotyczący wprowadzenia wyższych wymagań wobec biegłych opiniujących dowody elektroniczne powinien zostać zrealizowany zarówno w stosunku do biegłych tej specjalności, jak również wszystkich innych biegłych sądowych, po uchwaleniu przez Sejm opracowanej w Ministerstwie Sprawiedliwości, w formie projektu, ustawy o biegłych sądowych.

W projekcie tym, znajdującym się obecnie na końcowym etapie uzgodnień wewnętrznych, przyjęto rozwiązania gwarantujące obiektywną weryfikację wiedzy i umiejętności biegłych, i to zarówno przed ich wpisaniem na listę biegłych sądowych, jak i po dokonaniu takiego wpisu, w trakcie pełnienia funkcji biegłego sądowego." W ostatnich tygodniach, a więc po ponad 5 latach od przygotowania owej odpowiedzi na stronach Ministerstwa Sprawiedliwości opublikowane zostały założenia do projektu ustawy o biegłych sądowych.

Dokument, jak wynika z jego tytułu jest „projektem założeń projektu ustawy" a więc stopień jego ogólności jest delikatnie mówiąc znaczny, niemniej tym co uderza, mając na uwadze powyższą odpowiedź Ministra jest fakt, że wśród organizacji i instytucji, którym projekt został przesłany do konsultacji nie ma żadnej zajmującej się wyłącznie informatyką, w tym informatyką śledczą.

„Wyróżnieni" zostali m.in. biegli geodeci, doradcy podatkowi i biegli rewidenci. Jeśli projektowana ustawa wejdzie w życie będzie bez wątpienia jednym z ważniejszych aktów prawnych wpływających na kształt postępowań dowodowych karnych i cywilnych. Głos informatyków, w tym tych zajmujących się informatyką w toku prac nad nią nie może być pominięty w sytuacji, w której spodziewamy się rosnącego znaczenia tej dziedziny dla postępowań dowodowych prowadzonych na podstawie ustawy. ■

Janusz Tomczak, adwokat partner w kancelarii Wardyński i Wspólnicy Spółka komandytowa