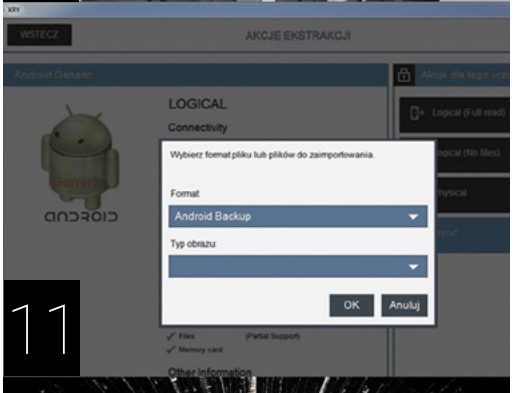
MAGAZYN

NR 30 / CZERWIEC 2016

www.magazyn.mediarecovery.pl

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Od 2009 roku piszemy dla Was
o informatyce śledczej i bezpieczeństwie IT.



Magazyn w wersji PDF

Wszystkie Magazyny możesz bezpłatnie pobrać z **www.Magazyn.mediarecovery.pl**

Informatyka śledcza w postępowaniu gospodarczym

Żyjemy w cyberświecie. Zakupy robimy w sklepach internetowych, sprawy załatwiamy w e-urzędach i korzystamy z bankowości elektronicznej. Biznes prowadzimy przy wykorzystaniu nowoczesnych technologii, bo inaczej się po prostu nie da. Możliwość komunikacji bez ograniczeń ze względu na odległość i czas spowodowała, że świat stał się nieco mniejszy. Natomiast życie społeczne i towarzyskie w dużej mierze przeniosło się do sieci, a więc do świata, który praktycznie nie ma żadnych ograniczeń.

Jarosław Góra

Skoro aktywność ludzi przeniosła się do cyberświata, tam też następują zdarzenia, które mają doniosłość prawną. Tam dochodzi do zawierania umów, załatwiania spraw administracyjnych, jak i do sporów oraz wszelkiego rodzaju nadużyć i tam też można znaleźć ślady tych zdarzeń. Wobec tego nie dziwi fakt, że informatyka śledcza z impetem wkroczyła na sale sądowe. Wobec faktu, iż rozwój nauki i postęp technologiczny w sposób bezpośredni i bardzo intensywny oddziałuje na wszystkie dziedziny życia człowieka, korzystanie z Internetu, także w obrocie prawnym stało się powszechne, a wiele czynności prawnych dokonywanych jest za pośrednictwem środków komunikacji elektronicznej, elektroniczny materiał dowodowy nabrał wręcz kluczowego znaczenia w przypadku większości postępowań sądowych. Jak wskazano wyżej, obecnie prowadzenie działalności gospodarczej bez wykorzystania nowych technologii jest praktycznie niemożliwe. Prawdą jest również to, o czym prędzej czy później przekonuje się każdy przedsiębiorca, że elementem prowadzonej działalności jest powstawanie różnego rodzaju sporów na tle prawnym, których część znajduje finał w postaci postępowania przed sądem. Być może zabrzmi to brutalnie, ale rezultat takich postępowań sądowych często nie zależy od tego, jak dana sprawa wyglądała w rzeczywistości, ale od tego, czy na potwierdzenie tej rzeczywistości przedstawi się odpowiedni materiał dowodowy. Zgodnie bowiem z podstawową zasadą prawa cywilnego ciężar udowodnienia faktu spoczywa na osobie, która z faktu tego wywodzi skutki prawne. Co więcej, strony postępowania zobowiązane są przytaczać wszystkie okoliczności faktyczne i dowody bez zwłoki , natomiast ze względu na tzw. prekluzję, sąd może pominąć spóźnione twierdzenia i dowody. Powyższe oznacza, że inicjator postępowania sądowego powinien przedstawić dowody, które potwierdzają jego racje w sprawie i powinien to zrobić już w pierwszym piśmie. Praktycznie w każdej sprawie przynajmniej część materiału dowodowego istnieje w formie cyfrowej, zatem tego rodzaju dowody również należy załączyć do pozwu. Elektroniczny materiał dowodowy, ze względu na swoją specyfikę, pociąga za sobą pewne trudności. Należy bowiem zadać o zapewnienie jego wiarygodności, poprzez odpowiednie jego zabezpieczenie oraz zaprezentowanie przed sądem. Przepisy prawa nie regulują w sposób szczególny kwestii wykorzystania w postępowaniu dowodów utrwalonych w formie cyfrowej. Z pomocą przychodzi informatyka śledcza. Takie ukształtowanie postępowania dowodowego w ramach procesu powoduje, iż współpraca prawnika z informatykiem śledczym okazuje

się niezbędna już na etapie planowania wystąpienia przez klienta na drogę sądową, jak i podczas samego procesu. Informatyka śledcza spełnia bowiem dwie zasadnicze funkcje. Z jednej strony dostarcza wskazówek i podpowiedzi, które mogą pozwolić na ustalenie istotnych dla sprawy zagadnień (funkcja informacyjna), z drugiej pozwala na udowodnienie tych okoliczności w ramach postępowania (funkcja dowodowa) poprzez wykorzystanie zabezpieczonych dowodów. Rola informatyka, co do zasady, sprowadzać się będzie zatem do identyfikacji oraz przygotowania elektronicznego materiału dowodowego na potrzeby postępowania sądowego, a więc dokonania jego odnalezienia, zabezpieczenia i przygotowania materiału do jego prezentacji. W sprawach mniej skomplikowanych, gdy do czynienia mamy z dowodami w postaci treści korespondencji elektronicznej, fotografii itp. pomoc informatyka śledczego ograniczy się do zabezpieczenia treści cyfrowych i przygotowania formy ich prezentacji. Natomiast w sprawach, gdy istotne mogą być informacje, których sama identyfikacja i odnalezienie, bądź zrozumienie wymaga wiadomości specjalnych, rola i znaczenie informatyka śledczego wzrasta diametralnie. Bez pomocy informatyka śledczego prawnik nie będzie w stanie np. wydobyć z konkretnego urządzenia informacji o przebiegu jego pracy, bądź zweryfikować, czy dana treść cyfrowa była modyfikowana, bądź w ogóle domyślić się, że dana aktywność mogła zostawić jakiś ślad. Brak udziału specjalisty z zakresu informatyki śledczej w pracach przygotowawczych do procesu może skutkować nieprawidłowym zabezpieczeniem dowodów, co wobec aktywności drugiej strony może wpływać na ich wiarygodność, jak i całkowitą kompromitację. Współpraca prawnika z informatykiem śledczym może okazać się również nieodzowna w trakcie procesu, kiedy kontestowanie twierdzeń drugiej strony poprzeć należy dowodami istniejącymi w formie cyfrowej – specjalista może wskazać na słabość stanowiska drugiej strony i potencjalne dowody, które mogą to potwierdzić, bądź na braki w elektronicznym materiale dowodowym przez tę stronę przedstawionym. W wypadkach wymagających wiadomości specjalnych sąd po wysłuchaniu wniosków stron co do liczby biegłych i ich wyboru może wezwać jednego lub kilku biegłych w celu zasięgnięcia ich opinii. Dowód z opinii biegłego jest niezbędny w przypadku, gdy zrozumienie pewnych faktów znajdujących oparcie w materiale dowodowym wymaga posiadania wiedzy specjalistycznej. Za taką należy uznać natomiast wiedzę z zakresu szeroko rozumianej informatyki. Wobec czego korzystanie z elektronicznego materiału dowodowego przed sądem bardzo często będzie się wiązać się będzie z koniecznością powołania biegłego, który pomoże sądowi orzekającemu zrozumienie i wyciągnięcie wniosków w przedstawionych dowodów, albo innymi słowy, w weryfikacji, czy twierdzenia strony powołującej się na dany materiał dowodowy są zgodne z prawdą. Strona przeciwna natomiast na pewno skorzysta w takim przypadku z okazji i spróbuje skompromitować materiał dowodowy, „uderzając" w jego wiarygodność, poprzez wykazywanie, że został on nieprawidłowo zabezpieczony lub w jakiś sposób zmodyfikowany itp. Te okoliczności również mogą zostać zweryfikowane przez biegłego. W końcu krytyczna analiza opinii przygotowanej przez biegłego w ramach postępowania również wymaga posiadania wiedzy specjalnej, zatem i tutaj pojawia się obszar, gdzie współpraca prawnika z informatykiem śledczym jest niezbędna. Żyjemy w cyberświecie, gdzie współpraca prawnika z informatykiem śledczym w ramach wystąpienia w imieniu klienta na drogę postępowania sądowego stała się niezbędna.

Autor jest adwokatem, szefem zespołu prawa własności intelektualnej i nowych technologii w kancelarii Ślązak, Zapiór i Wspólnicy. Trener w Akademii Informatyki Śledczej.

Informatyka śledcza w korporacji

Usługi z zakresu informatyki śledczej świadczone w korporacji co do zasady nie różnią się od tych, które miałem okazję realizować jeszcze przed zasileniem szeregów jednej z takich firm. Obowiązują tu takie same zasady, stosowane są te same najlepsze praktyki, zazwyczaj też wykorzystywane są te same narzędzia.

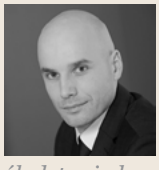
Tomasz Kemona

Co nam wolno, a czego nie?

Na zasadach, praktykach i narzędziach podobieństwa jednak się jednak kończą. Praca dla klienta biznesowego zdecydowanie różni się od działania na zlecenie tak zwanych organów uprawnionych. Jedną z takich różnic są, między innymi, istotne utrudnienia w pozyskiwaniu informacji. Na przykład firma zajmująca się hostingiem nie będzie mogła wydać na naszą prośbę żadnych danych z prywatnej skrzynki mailowej. Do tego bowiem niezbędne jest postanowienie wydane przez organy ścigania lub sąd. Innym przykładem może być operator telekomunikacyjny, który udostępniając nam biling telefoniczny, nie uwzględni w nim numerów dla połączeń przychodzących. Do ujawnienia takiej informacji nie ma przeciwwskazań technicznych, jednak operatorowi do zwolnienia go z obowiązującej tajemnicy telekomunikacyjnej również potrzebne będzie odpowiednie postanowienie. Pracując dla klientów korporacyjnych możemy jednak zazwyczaj liczyć na pełną współpracę w zakresie udostępniania nam zasobów ich danych. Naszym zleceniodawcom w głównej mierze zależy bowiem na wyjaśnieniu całego zjawiska nadużycia, z którym się borykają, przy użyciu wszelkich dostępnych informacji.

Właśnie na kompletności polega kolejna różnica w przypadku większości naszych projektów. Klient, zwracając się do nas z prośbą o pomoc, oczekuje kompletnej usługi, polegającej na kompleksowej analizie całego problematycznego zagadnienia. Z technik informatyki śledczej korzystamy tu najczęściej przy pozyskiwaniu danych dla procesu eDiscovery. Wyjaśniając w dużym skrócie – proces ten polega na wyszukiwaniu, identyfikacji dokumentów i innych danych elektronicznych istotnych dla śledztwa oraz na ich dalszym przeglądzie. Śledztwo jednak nie ogranicza się jedynie do obszaru informatyki. Swoim zakresem obejmuje również takie elementy, jak analiza danych finansowych, czy analiza powiązań kontrahentów. W każdym z tego typu projektów chodzi o jak najlepsze zrozumienie procesów zachodzących u danego klienta. Konieczna jest także identyfikacja obszarów ryzyka, w których mogą występować nadużycia lub luki do nich prowadzące. Tutaj jednak nasza praca się nie kończy. Po zbadaniu materiału formułowane są wnioski – najczęściej w postaci raportu prezentującego szczegóły dotyczące przedmiotu śledztwa. Przedstawiane są również rekomendacje działań, jakie należy podjąć, aby przeciwdziałać takim i podobnym zdarzeniom w przyszłości. Niejednokrotnie efektem naszych prac jest zgromadzenie materiału dowodowego. Może zostać on wykorzystany do złożenia zawiadomienia o popełnieniu przestępstwa lub w postępowaniu sądowym, gdzie możemy wspierać klienta prezentując ustalone fakty.

W przypadku dużych projektów zaletą korporacji jest posiadanie interdyscyplinarnych zespołów śledczych. Mogą one podjąć się przeprowadzenia dochodzenia nawet w przypadku bardzo złożonych procesów, wymagających wiedzy z różnych dziedzin, nie tylko z zakresu informatyki. Kolejną zaletą korporacji w tego typu usługach jest sieć biur zlokalizowanych na całym świecie, z którymi na co dzień wymieniamy się wiedzą i doświadczeniem, co w wielu przypadkach jest naprawdę bezcenne. Taka struktura daje możliwość szybkiej reakcji w sytuacji, gdy zachodzi konieczność zabezpieczenia i przeglądu danych nawet w odległych krajach. Łatwiej także o synchronizację zadań w wielu miejscach w tym samym czasie. Nie ma przy tym potrzeby dalekich podróży, co znacząco obniża koszty i czas realizacji usługi, przy jednoczesnym zachowaniu standardów jakościowych. To właśnie czas odgrywa kluczową rolę dla klienta. Mowa tu nie o czasie samego zabezpieczenia danych, ale przede wszystkim o czasie kompletnej analizy, aż do przedstawienia wniosków końcowych. Nie tylko w korporacjach zwykło się mawiać, że czas to pieniądz. W biznesie każda minuta, a nawet sekunda, w której przedsiębiorstwo jest narażone na zaburzenie ciągłości działania, powoduje wymierne straty – zarówno finansowe, jak i reputacyjne.



Autor jest specjalistą z dziedziny informatyki śledczej z kilkunastoletnim doświadczeniem. Menedżer w dziale śledztw i ekspertyz gospodarczych PwC odpowiedzialny za obszar eDiscovery.

Informatyka śledcza a praca prokuratora. Czy jedno jest użyteczne dla drugiego?

Bartosz Wójcik

Niniejszy artykuł ma odpowiedzieć na postawione w tytule pytanie. Moja odpowiedź w tym zakresie brzmi zdecydowanie twierdząco. A dlaczego? – o tym poniżej.

Na wstępie trzeba zaznaczyć, iż obecne czasy wymagają od prokuratorów posiadania dużej wiedzy związanej z funkcjonowaniem mechanizmów przestępczości komputerowej, internetowej czy szerzej – odnoszącej się do szerokiego spektrum nowych technologii, w tym przede wszystkim informatycznych. Statystyki prokuratorskie i policyjne nieubłaganie przekonują nas, że mijają czasy pospolitych przestępców kryminalnych, których którym w głowie rozboje, pobicia i kradzieże. Okazuje się, że łatwiej, bezpieczniej i szybciej można popełniać przestępstwa popełniać można w sieci czy za pomocą komputerów. Ryzyko wykrycia – mniejsze, szansa na wzbogacenie – dużo większa.

Co wspólnego z tym ma informatyka śledcza? Ano to, że daje prokuratorowi do ręki instrumenty, dzięki którym staje się on – lub może przy odrobinie dobrej woli się stać – pełnoprawnym przeciwnikiem dla przestępców nowej ery. Oto kilka przykładów z praktyki prokuratora.

1 telefony komórkowe – nieoceniona pomoc dla kryminalistów w popełnianiu przestępstw. Służą przede wszystkim do kontaktów i rozmów, ale także – coraz częściej – do przesyłania danych, dokonywania przelewów bankowych, zastępowania (praktycznie w każdym aspekcie) nieporęcznych komputerów czy laptopów. Przy tym – jeżeli mówimy o telefonach na kartę, a takimi najczęściej posługują się przestępcy – nie ma obowiązku rejestracji użytkownika takiego telefonu, choć ma się to zmienić w związku z przygotowywaną tzw. ustawą antyterrorystyczną. Sprawny informatyk śledczy może z zatrzymanego telefonu odzyskać masę istotnych danych – oczywiście zaczynając od książki telefonicznej i wykazu połączeń, przez treść sms-ów i mms-ów, na odwiedzanych stronach internetowych kończąc. W mojej ostatniej praktyce spotkałem się z kilkoma sprawami o charakterze tzw. pedofilskim, kiedy to sprawca właśnie w telefonach miał zapisane informacje, które pozwoliły przedstawić mu zarzuty, a później doprowadzić do skazania. Chodziło przede wszystkim o filmy i zdjęcia przedstawiające akty seksualne z udziałem małoletnich, lecz także – co już mniej oczywiste – logi do stron internetowych odwiedzanych przez pedofili oraz treść pozostawianych na tych stronach ogłoszeń (o raczej jednoznacznym charakterze).

2 Internet. Jego odmęty stanowią doskonałe pole do popisu dla sprawnych informatyków spod ciemnej gwiazdy. Jed-

nak równie sprawny informatyk śledczy potrafi zdziałać dla prokuratora w tym temacie naprawdę wiele. Rzecz opiera się na badaniu zabezpieczonych komputerów lub właśnie telefonów i wychwytywaniu odwiedzanych stron, używanych adresów, treści wysyłanych maili itp. Nierzadko w ten właśnie sposób wchodzimy na trop nowych kategorii przestępstw, jak np. phishingu. Jednocześnie dobrze ukierunkowany informatyk śledczy i bez zabezpieczonego od przestępcy komputera potrafi odnaleźć i rozpracować zagrożenie. Do tego wystarczy sama sieć internetowa. Nie bez kozery w ostatnim czasie, dostrzegłszy zagrożenie z tej strony, w komendach wojewódzkich Policji w całej Polsce powstały specjalistyczne Wydziały do walki z Cyberprzestępczością, zatrudniające najbardziej „oblatanych" w temacie funkcjonariuszy. Monitorują oni na bieżąco sieć, wykrywając co i rusz rozmaite zagrożenia i przestępstwa, od nielegalnego rozpowszechniania plików i programów objętych prawem autorskim, przez czyny o charakterze pedofilskim (wymiana plików, umawianie się z nieletnimi itd.), po naprawdę poważne naruszenia prawa, jak przestępstwa o charakterze terrorystycznym czy związane z nawoływaniem do nienawiści na tle rasowym lub narodowościowym. Utrudnieniem walki na tym polu dla informatyków śledczych bywa fakt, iż często kluczowe dla udowodnienia przestępstwa dane umieszczane są na serwerach zagranicznych – i to znajdujących się w państwach, które niekoniecznie chętnie współpracują z Polską na polu obrotu prawnego. Gwoli przykładu podam jedynie, iż w ostatnim czasie do jednej z prokuratur okręgu zamojskiego policjanci z opisanego wcześniej Wydziału dw. z Cyberprzestępczością skierowali kilka zawiadomień, z których wynikało, iż monitorując sieć natrafili oni na zdarzenia związane z dzieleniem się plikami zawierającymi treści pedofilskie. Chodziło o popularne serwisy wymiany plików, na pewno kojarzone przez większość użytkowników Internetu. Sprawcy zostali ustaleni i zatrzymani, a używane przez nich komputery i telefony podlegały zatrzymaniu dla potrzeb postępowań.

3 analizy kryminalne – podstawowa rzecz w dużych, wielowątkowych i wieloosobowych sprawach, często o charakterze gospodarczym. Analizy takie dla prokuratur przygotowują analitycy kryminalni zatrudnieni w tych jednostkach lub będący funkcjonariuszami Policji, choć zdarzają się oczywiście analitycy-informatycy „prywatni". Do opracowania analizy wystarczy tak naprawdę właściwy program komputerowy (np. Excel) oraz odrobina wysiłku, dobrej woli i cierpliwości. Dane wyjściowe, takie jak wyciągi z rachunków bankowych, dane z bilingów, wykazy osób „wrzuca" się do programu, gdzie analityk – stosując odpowiednie filtry i nakładki – modeluje je ustawiając w grupy, punktując powiązania i punkty zaczepienia. W ten sposób z morza bezładnie ułożonych danych formuje on dla prokuratora jasny i przejrzysty obraz, z którego dopiero wyłania się to, co w sprawie istotne: kto komu coś przelał i w jakiej wysokości, gdzie „poszło" to dalej, czy osoba „x" rozmawiała z osobą „y" i ile razy, co z tego wynikło, czy „y" rozmawiał potem z osobą „z", a może i „z" kontaktował się z „x"? Kombinacje można mnożyć w nieskończoność, ale i tak chodzi o to, żeby prokurator miał przed sobą jasno wyłożone mechanizmy przestępstwa. Bez komputerów, ale co ważniejsze bez dobrych informatyków śledczych w tym zakresie ani rusz.

Ramy opracowania nie pozwalają na szersze potraktowanie tematu, chociaż niewątpliwie on na to zasługuje. Powyższe przykłady w sposób oczywisty wskazują, iż bez informatyki śledczej walka z przestępczością – to walka przegrana.

Prokurator Prokuratury Rejonowej w Krasnymstawie, aktualnie delegowany do Prokuratury Okręgowej w Zamościu. Z prokuraturą związany od 2003 r. Wcześniej pełnił funkcję szefa Prokuratury Rejonowej w Zamościu.

Mediarecovery i MSAB przedstawiają

NOWE PODEJŚCIE

do zaawansowanych analiz mobile forensics.

XL XRY Logical
Wyodrębnia i odzyskuje dane poprzez komunikację z systemem operacyjnym.

XP XRY Physical
Pozyskuje i odzyskuje dane bezpośrednio z pamięci urządzenia.

XC XRY Cloud
Pozyskuje dane zapisane w „chmurze".

XPP XRY PinPoint
Pozyskuje dane z niestandardowych modeli telefonów.

XV XAMN Viewer
Przeglądarka do plików .xry z możliwością raportowania.

XS XAMN Spotlight
Narzędzie do analizy kryminalistycznej danych z różnych urządzeń.

XH XAMN Horizon
Rozbudowana przeglądarka z możliwością wyszukiwania i korelacji danych.

XE XAMN Elements
Analiza danych w formie binarnej.

XD XEC Director
Zdalne zarządzanie systemami MSAB i użytkownikami.

XX XEC Export
Eksport i konwersja plików .xry do innych formatów.

XRY
Ekstrakcja
Pozyskiwanie i odzyskiwanie danych zgodnie z najlepszymi praktykami informatyki śledczej.

XAMN
Analiza
Wizualizacja i analiza danych pozyskanych w procesie ekstrakcji.

XEC
Zarządzanie
Efektywne narzędzia do zarządzania i administrowania.

1. Miejsce zdarzenia

Szybkie zabezpieczenie danych jest konieczne w sytuacjach kiedy grozi nam utrata danych na przykład poprzez zdalne ich kasowanie, kończącą się baterią czy zablokowanie urządzenia. W takich chwilach śledczy potrzebują narzędzia takiego jak XRY Tablet używający technologii XRY Logical. Łatwe w użyciu, proste w obsłudze i szybkie w działaniu.

2. Posterunek policji

Jeśli błyskawiczne działanie nie jest konieczne, informatyk śledczy może zabrać zabezpieczone urządzenia do siebie celem analizy. Zazwyczaj śledczy wykorzystują Kiosk lub Office pracujące w technologii XRY Logical i Physical.

3. Miejsce analizy

Śledczy pracujący nad sprawą samodzielnie lub w zespole, potrzebują dostępu do dowodów. Używają XAMN Viewer i Spotlight do przeglądu poszczególnych elementów materiału dowodowego, na przykład smsów czy plików video. Pozwala to przygotować się do przesłuchania.

4. Laboratorium informatyki śledczej

Jeśli sprawa jest bardzo poważna, złożona, a analiza zabezpieczonych urządzeń stanowi wyzwanie, przekazuje się je do laboratorium informatyki śledczej (np. Mediarecovery). Doświadczeni profesjonaliści używają wersji Office technologii XRY Logical, Physical, PinPoint, Cloud i XAMN Elements do odtworzenia danych.

5. Biuro analityka

Jeśli urządzenie jest częścią większego dochodzenia, w skład którego wchodzi wiele urządzeń, dowody mogą wymagać analitycznego podejścia do wyników działań informatyków śledczych. XAMN Horizon daje przegląd każdego z badanych urządzeń, poszerza możliwości analityczne i stosuje zaawansowane sposoby wizualizacji.

6. Sala sądowa

Dowody elektroniczne są najczęściej prezentowane w sądzie w formie papierowych ekspertyz i opinii. XAMN Viewer może być użyty do prezentacji dowodów elektronicznych w sądzie. Co ważne, filmy i zdjęcia mogą zostać wyświetlone bezpośrednio z wersji elektronicznej ekspertyzy bez naruszania integralności danych.

7. Administracja

Dział IT może kontrolować zasoby techniczne i dane. Może eksportować i konwertować pliki z rozszerzeniem .xry do innych formatów używając XEC Export. Może również zdalnie zarządzać całym systemem i użytkownikami za pomocą XEC Director.

Od 2007 roku mediarecovery jest wyłącznym partnerem MSAB w Polsce.

Wywiad z Sebastianem Małychą,

prezesem Mediarecovery, największej polskiej firmy zajmującej się informatyką śledczą.

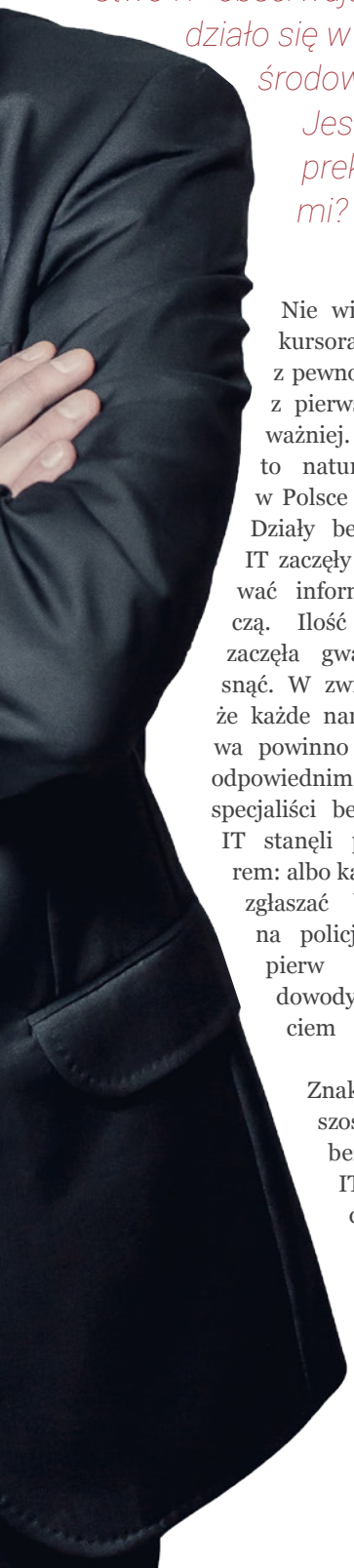
- Jakie były początki informatyki śledczej w Polsce? Wydaje się, że na samym początku była ona ściśle powiązana ze służbami, policją, prokuraturą.

Rzeczywiście tak było. Informatyka śledcza była związana wyłącznie z szeroko rozumianym wymiarem sprawiedliwości. Dziesięć, dwanaście lat temu zaczynał się proces przechodzenia naszej rzeczywistości w wymiar cyfrowy. Te zmieniające się realia wymusiły niejako na służbach zainteresowanie tematem. Zresztą nie tylko w Polsce ale na całym świecie.

To właśnie służby, jako pierwsze zaczęły szukać możliwości zebrania, czy też poszerzenia materiału dowodowego i zebrania poszlak w komputerach. Jednak w tamtym okresie nie miało to jeszcze wymiaru masowego.

Specjaliści informatyki śledczej Mediarecovery, choć nie tylko oni, włożyli sporo pracy w to żeby upowszechnić świadomość organów ścigania i wymiaru sprawiedliwości w tym zakresie. Dla przykładu w samym tylko 2007 roku przeszkoliliśmy prawie 1000 osób w obszarze możliwości analitycznych i dowodowych informatyki śledczej.

- Czy można powiedzieć, że był jakiś punkt przełomu po którym informatyka śledcza zaistniała w bezpieczeństwie IT? Czy była to raczej naturalna ewolucja? Przypomnę, że nasz Magazyn w 2010 roku dodał w nazwie „bezpieczeństwo IT" obserwując to co działo się w naszym środowisku. Jesteśmy prekursorami?



Nie wiem czy prekursorami ale z pewnością jednymi z pierwszych. A poważniej. Sądzę, że był to naturalny proces w Polsce i na Świecie. Działy bezpieczeństwa IT zaczęły się interesować informatyką śledczą. Ilość incydentów zaczęła gwałtownie rosnąć. W związku z tym, że każde naruszenie prawa powinno się zgłaszać odpowiednim organom specjaliści bezpieczeństwa IT stanęli przed wyborem: albo każdy incydent zgłaszać bezpośrednio na policję albo najpierw zabezpieczyć dowody ze wsparciem specjalistów.

Znakomita większość działów bezpieczeństwa IT wybrała drugą możliwość. Jest i było to zauważalne szczególnie w dużych firmach, korporacjach, gdzie liczba incydentów, fraudów, niezgodności w cyfrowym wymiarze zaczęła porażać ilością. Czym więcej tego typu zdarzeń, tym większa potrzeba działań po incydencie. Do tej pory wszyscy starali się zabezpieczać i tworzyć takie środowisko IT żeby incydentów nie było. Dość szybko uświadomiono sobie, że to jest po prostu niemożliwe. Incydenty stawały się coraz bardziej złożone. W związku z tym każdy dział bezpieczeństwa powinien posiadać możliwości analizy poincydentalnej.

Możliwość analizy danych, możliwość sprawdzenia co konkretnie się wydarzyło w sensie dowodowym. Często zdarza się, że po incydencie, po jego wyjaśnieniu dana firma decyduje się na drogę sądową. Mając zabezpieczone przez siebie dowody wymiernie skraca czas postępowania przygotowawczego i zwiększa szanse korzystnego dla siebie wyroku.

- Informatyka śledcza znalazła swoje miejsce w bezpieczeństwie IT już wiele lat temu. Czy można w jakiś sposób określić jej obecną rolę? Sporo się pewnie zmieniło przez ten czas.

Informatyka śledcza jest obecnie na stałe zintegrowana z bezpieczeństwem IT. Jeśli popatrzymy na incydent od jego początku, poprzez rozwój po moment, w którym dana organizacja uświadamia sobie, że ma on miejsce, kiedy firma reaguje to w ramach tej reakcji pojawia się informatyka śledcza. I to jest standard już dzisiaj. Mało tego, producenci rozwiązań bezpieczeństwa IT też zauważyli taką potrzebę i starają się jej wyjść naprzeciw. Zaczynają włączać funkcjonalności informatyki śledczej do swoich systemów.

- Omówiliśmy już przeszłość i teraźniejszość. Pytanie, które się nasuwa, brzmi co będzie w przyszłości? W którą stronę informatyka śledcza będzie się rozwijać, jakie stoją przed nią wyzwania?

Coraz większy rozwój informatyki śledczej w urządzeniach mobilnych oraz tak zwana big data czyli duże ilości danych. Te dwa obszary z pewnością będą najbardziej rozwojowe. To właśnie tam pojawiają się nowe wyzwania i nowe problemy.

W urządzeniach mobilnych jest nadal wiele różnych systemów operacyjnych, sposobów zapisów danych. To powoduje, że nie zawsze można użyć tego samego narzędzia, a co za tym idzie mobile forensics musi niezwykle szybko się rozwijać. Widzę tu jeszcze spory potencjał i będzie to kierunek rozwoju informatyki śledczej związanej z bezpieczeństwem.

Naturalną konsekwencją łatwego dostępu do danych przez użytkowników jest rozwój wszelkiego typu i rodzaju „chmur". A co za tym idzie ogromne, niespotykane do tej pory ilości danych. W związku z tym w praktyce nie jest możliwe wykonanie kopii binarnej wielu, dużych macierzy dyskowych. Dlatego dziś dość szybko rozwijają się narzędzia dające możliwość analizy live forensics. W tym przypadku nie ma potrzeby wykonywania kopii binarnej całości tylko analizuje się w czasie rzeczywistym pracujące urządzenia. Sytuacja jest w takim przypadku dynamiczna ale można przeprowadzić analizę i dopiero wyniki tej analizy zabezpieczyć jako dowód.

Jestem pewien, że z problemem badania dużych ilości danych będziemy spotykać się coraz częściej. W naszym laboratorium mamy już tego typu doświadczenia, narzędzia oraz specjalistów więc zawsze będziemy mogli pomóc służbom lub firmom.

- Dziękuję za rozmowę.

Dziękuję. A z okazji jubileuszowego, trzydziestego wydania Magazynu, życzę kolejnych trzydziestu wydań.

O tym jak Computer Forensics z Mobile Forensics w jednym domu zamieszkali.

Michał Tatar

Czy możliwe jest zatem wyjście poza jedną gałąź informatyki śledczej i znalezienie komplementarności w Computer Forensics z Mobile Forensics? Spróbujmy się o tym przekonać na podstawie praktycznego przykładu.

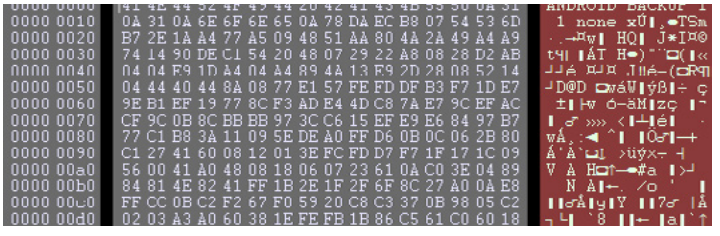
O komplementarności w informatyce śledczej na łamach Magazynu pisano kilka razy. Niepodważalnym faktem jest to, że narzędzia służące do wykonywania spraw traktujących dowody elektroniczne wzajemnie się uzupełniają. Bez poprawnego zabezpieczenia dowodu elektronicznego nie ma możliwości analizy takiego dowodu. I tak do zabezpieczenia w dziedzinie Computer Forensics może nam posłużyć odpowiednia aplikacja lub sprzęt (np. MediaImager), a do wykonania analizy i stworzenia ekspertyzy skorzystamy z zupełnie innej aplikacji (np. EnCase). Podobnie wygląda to w przypadku Mobile Forensics. Zabezpieczenie urządzenia mobilnego możemy wykonać za pomocą box'ów serwisowych, a samą analizę wykonać z użyciem specjalistycznego oprogramowania (np. XRY).

Zostałem poproszony o zabezpieczenie kilku dysków twardych pochodzących z komputerów klasy PC. Na miejscu wykonałem czynności procesowe mające na celu stworzenia kopii binarnych nośników pamięci i a zabezpieczone kopie binarne zabrałem ze sobą celem analizy. Kopie binarne zostały podłączane do oprogramowania EnCase Forensic, które oferuje szybkie poszukiwanie, odnajdywanie, analizowanie i zapisywanie dowodów elektronicznych. Wśród setek gigabajtów danych moją uwagę zwrócił fakt, iż na dysku zostały znalezione pliki oprogramowania iTunes służącego do wykonywania kopii zapasowej danych z urządzeń mobilnych firmy Apple. Zacząłem więc przeszukiwanie dysku z nadzieją odnalezienia oprogramowania innych firm, które mają możliwości podobne do iTunes. Znalazłem więc oprogramowanie Android Studio, Samsung KiES oraz Blackberry Link.

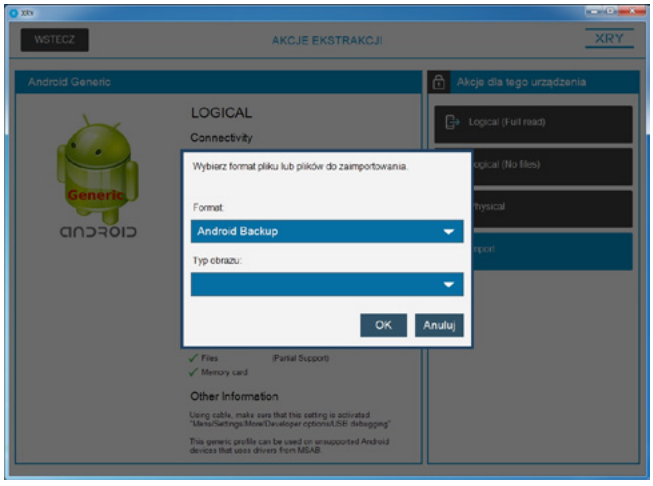
	Name	Review	Report	Follow U	Ignore	File Ext	Logical Size
57124	System.Web.9c7998a9#					9c7998a9#	304
57125	System.Management.A#					A#	304
57126	System.Management.A#					A#	560
57127	Microsoft.A2d108c15#					A2d108c15#	304
57128	Microsoft.A3ec156ec#					A3ec156ec#	304
57129	Microsoft.A46d9ce83#					A46d9ce83#	304
57130	Microsoft.A57390ac1#					A57390ac1#	304
57131	Microsoft.A7373a429#					A7373a429#	304
57132	Microsoft.A759b3824#					A759b3824#	304
57133	Microsoft.A8e385fd7#					A8e385fd7#	304
57134	Microsoft.A9d3d528f#					A9d3d528f#	304
57135	Microsoft.Aa1b230a0#					Aa1b230a0#	304
57136	[illegible]					aas	42 314
57137	backup.ab	Review				ab	33 786 298
57138	backup_mi4i.ab	Review				ab	107 294 100
57139	[illegible]					abc	25 270
57140	System.Web.Abstract#					Abstract#	304

Rysunek 1

W związku z tym faktem moje poszukiwania zostały ograniczone do odpowiednich rozszerzeń plików i folderów, które tworzą wspomniane programy. I tak moim oczom ukazał się wyniki: (Rys. 1) Pliki z rozszerzeniem .AB to nic innego jak Android Backup wykonany najprawdopodobniej za pomocą modułu ADB pochodzącego z pakietu Android Studio. Folder



Rysunek 2



Rysunek 3

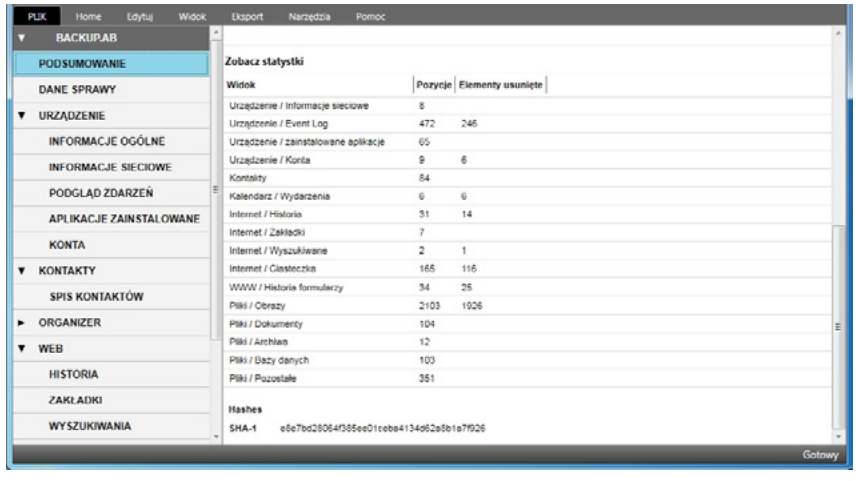
wać powyższe dane zaimportować do oprogramowania typu Mobile Forensics. Na warsztat wziąłem XRY. Natomiast nurtowało mnie pytanie, jak podpiąć pliki backupu nie mając wiedzy z jakiego urządzenia pochodzą... I tu z pomocą przyszli programiści XRY, którzy zaimplementowali w swoje narzędzie tzw. profile odczytu Generic. Profil ten charakteryzuje się specyfiką systemu operacyjnego, a nie specyfiką konkretnego urządzenia mobilnego. No to do dzieła! Importuję plik .AB (Rys. 3) Po chwili otrzymuję komplet informacji posortowanych kategoriami, z których wykonanie raportu zajmie mi chwilę. Co ciekawe, XRY odzyskał nawet skasowane informacje! (Rys. 4) W analogiczny sposób przystępuje do backupu iOS, gdzie wskazuję XRY folder danych. I znowu po chwili otrzymuję cenne informacje (Rys. 5)

Tym oto prostym sposobem z plików kopii zapasowych urządzeń mobilnych, które zostały odnalezione za pomocą oprogramowania do Computer Forensics wydobyliśmy dane pochodzące stricte z dziedziny Mobile Forensics. W dzisiejszym mobilnym świecie takie sytuacje będą na pewno pojawiać się bardzo często. Bo który świadomy użytkownik swojego urządzenia mobilnego nie przechowuje kopii zapasowych danych na swoim komputerze? Reasumując sądzę, że to wystarczający dowód na to, by odtąd obie dziedziny (CF i MF) traktować komplementarnie, a nie osobno.

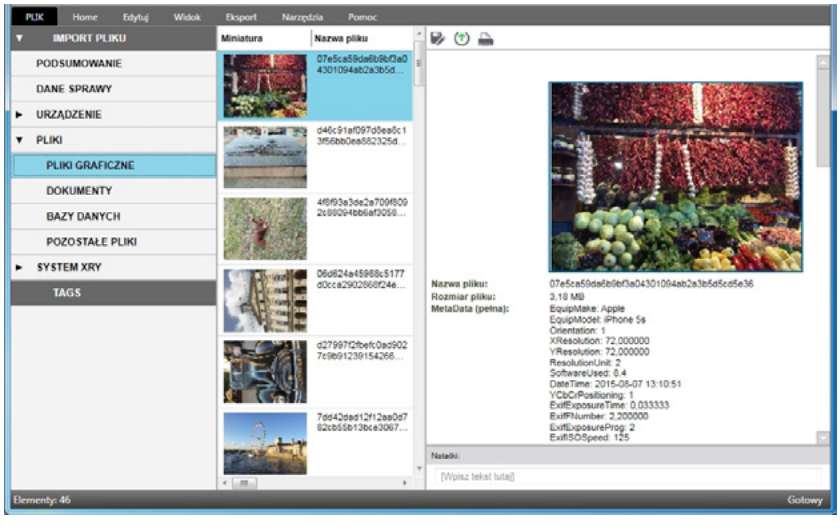
Apple Computer \ MobileSync \ Backup wskazuje ewidentnie na kopię zapasową pochodzącą z urządzenia iOS. Nie znalazłem plików z rozszerzeniem .BBB (BlackBerry Backup, który mógłby pochodzić z Blackberry Link) oraz folderów w lokalizacji Samsung \ Kies3 \ backup.

Przy próbie otwarcia pliku .AB za pomocą aplikacji dekompresującej 7-zip dostałem komunikat, że nie można otworzyć tego pliku jako archiwum. W przeglądarce heksadecymalnej widzę kod HEX, jednak obce jest mi biegłe czytanie w nim. (Rys. 2) Spójrzmy zatem na zawartość folderu kopii zapasowej urządzenia iOS. Znajdują się tu pliki bez rozszerzeń oraz nazwy nie sugerujące absolutnie nic. W przeglądarce HEX znowu nieczytelny kod...(Rys. 2)

Nie poddając się, postanowiłem spróbo-



Rysunek 4



Rysunek 5

Autor jest specjalistą w zakresie analizy urządzeń mobilnych (Mobile Forensics) w Laboratorium Informatyki Śledczej Mediarecovery. Zajmuje się również implementacją rozwiązań mobilnych zarówno w sektorze prywatnym jak i publicznym (m.in. Mobile Device Management). Trener w ramach Akademii Informatyki Śledczej.

mChallenge

Konkurs dla najlepszego śledczego Computer Forensics.

NAGRODA **5000** zł

Spróbuj sił z najlepszymi!

www.mchallenge.pl

Przy okazji 30go wydania Magazynu Informatyki Śledczej, laboratorium Mediarecovery postanowiło ogłosić konkurs skierowany do specjalistów z branży computer forensics. W ramach konkursu Media Challenge będzie można połączyć przyjemne z pożytecznym – nie tylko sprawdzić się z najlepszymi specjalistami w Polsce, ale również otrzymać nagrodę finansową.

Z tego powodu, w formie zapowiedzi, przedstawiamy wywiad z Michałem Ferdyniokiem, merytorycznym opiekunem konkursu i kierownikiem Laboratorium Informatyki Śledczej Mediarecovery.

Skąd pomysł na konkurs?

Doszliśmy do wniosku, że w Polsce nie było jeszcze **tak ciekawego i wymagającego** (dobrego zaplecza merytorycznego) **konkursu z ukierunkowaniem na informatykę śledczą.** Planujemy stworzyć taki zestaw, który faktycznie podda próbie nie tylko umiejętności analityczne ale i kreatywność a także cierpliwość uczestników. Zakładamy, że osoby chcące wziąć udział w naszym konkursie, będą posiadać te cechy i co ważne, będą mogły stanąć w szranki z najlepszymi. Polscy specjaliści IT mają wysokie notowania na świecie, więc szacujemy, że konkurencja będzie naprawdę duża.

Czego będzie dotyczyć?

Póki co nie mogę zbyt wiele zdradzić, szczegóły podamy wkrótce ale na pewno zostanie przedstawiona pewna fabuła, efektem której powstanie incydent i mnogość problemów do pokonania. Zaplanowaliśmy tę ścieżkę w taki sposób aby potencjalny uczestnik się nie nudził.

Jak będą wyglądać ramy czasowe mChallenge?

Oficjalnie do konkursu będzie można się zgłosić w połowie lipca, nabór uczestników potrwa około tygodnia. Po zamknięciu tego etapu, nastąpi kontakt z uczestnikami, przesłanie i udostępnienie pakietów konkursowych i tutaj już zaczyna się nasz „forensicowy" wyścig. Uczestnicy będą mieć około trzech tygodni na zbadanie sprawy, przedstawienie rozwiązań i ewentualne konsultacje. Liczy się czas, którego śledczy nigdy nie mają zbyt wiele.

Kto może w konkursie uczestniczyć?

Uczestnikiem konkursu może zostać praktycznie każdy, kto zgłosi chęć uczestnictwa na www.mchallenge.pl. Stąd przewidujemy, że ilość zgłoszeń może być spora. Opcjonalnie, w konkursie mogą brać również udział zespoły.

Czego uczestnik może się spodziewać?

Scenariusz całego incydentu jest przygotowany tak, aby uczestnik mógł sprawdzić się na kilku polach analitycznych. Na pewno może spodziewać się kilku ślepych uliczek, z całą pewnością ważne będzie aby wyzbyć się szablonowego myślenia, stąd brak doświadczenia w tej dziedzinie, na pewno szybko zweryfikuje kto stanie na podium.

No właśnie, podium. Skoro konkurs to i nagroda?

Dla zwycięzcy przewidziana jest nagroda finansowa w wysokości 5000 zł, uroczyste wręczenie 21 września br. podczas konferencji URDI 2016, której Mediarecovery jest partnerem oraz gwarantowane wystąpienie podczas konferencji w formie prezentacji.

Wszystkich zainteresowanych udziałem w konkursie mChallenge zachęcamy do odwiedzenia strony
www.mchallenge.pl,
na której będzie można znaleźć więcej szczegółów.

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: magazyn@mediarecovery.pl
www.magazyn.mediarecovery.pl

Redakcja
Sebastian Małycha (red. nacz.),
Przemysław Krejza
Skład, łamanie, grafika:
Mariusz Ruski

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
www.mediarecovery.pl

mediarecovery Lider informatyki śledczej