MAGAZYN
INFORMATYKI ŚLEDCZEJ

mediarecovery
Wyższy poziom bezpieczeństwa

www.mediarecovery.pl

2019

W tym wydaniu

Wszystkie Magazyny możesz bezpłatnie pobrać na:

http://magazyn.mediarecovery.pl

Dlaczego nastolatek sięgnął po broń?

Dave Proulx

25 stycznia 2014 roku 19-letni Darion Aguilar opuścił przebieralnię w centrum handlowym i zaczął strzelać. Zanim zabił siebie, zastrzelił dwie młode osoby i zranił kolejnych pięć.

Po strzelaninie w centrum handlowym w Columbii, w stanie Maryland, dokonano analizy iPhone'a, jego backupu oraz komputera będącego własnością zamachowca. Do pozyskania i analizy materiału użyto oprogramowania BlackLight, które ujawniło chronologię wydarzeń prowadzących do strzelaniny i odkrycia wcześniej nieznanych szczegółów dotyczących przygotowań i stanu psychicznego nastolatka.

Mobile Forensic

Aby odtworzyć przebieg wydarzeń i znaleźć motyw działania Dave Proulx będący wtedy na stanowisku detektywa prowadzącego śledztwo analizował dane z urządzeń mobilnych, w których posiadaniu był Darion. Detektyw podkreślał, iż do tej sprawy użyto rozwiązania BlackLight, aby przyspieszyć proces wyodrębniania baz danych SQLite z urządzeń o różnych systemach operacyjnych, a następnie ich analizy. Dzięki BlackLight śledczy przeanalizowali wszelkie wiadomości (SMS/MMS, iMessage), komunikatory (m.in. Skype, TextFree), aplikacje Social Media (m.in. Facebook, Foursquare), aktywność Dariona w internecie i przechowywane przez niego materiały cyfrowe.

Motyw zbrodni

Kluczowe dla śledztwa stały się dane zarchiwizowane w chmurze. W grudniu 2013 r. czyli miesiąc przed strzelaniną, Darion zaktualizował swojego iPhone, dzięki czemu uzyskał możliwość tworzenia kopii zapasowych w iCloud. Wcześniej ta funkcja była dostępna tylko w iTunes. Detektyw Proulx podkreślił, że analiza iCloud zsynchronizowanego w nocy przed strzelaniną dostarczyła kluczowych informacji. Dzięki połączeniu w całość danych z iPhone, laptopa i kopii zapasowych z chmury, narzędzie BlackLight umożliwiło stworzenie osi czasu obrazującej aktywność online sprawcy i proces przygotowań do zamachu. Zebrane informacje udokumentowały chorobliwą fascynację zamachowca masakrą w Columbine High School z 1999 roku. Mężczyzna od dłuższego czasu tworzył własne filmy inspirowane treściami, jakie tworzyli zabójcy z Columbine. Co więcej, grał w gry online symulujące udział w tym wydarzeniu.

Zebrane informacje udokumentowały chorobliwą fascynację zamachowca masakrą w Columbine High School z 1999 roku.

Ostatnie godziny

Korzystając z przeglądarki SQLite i funkcji zapytań BlackLight ustalono, że Darion używał m.in. aplikacji na swoim iPhonie, aby wytyczyć drogę do centrum

handlowego, łącząc transport publiczny i prywatny. Odkryto również bloga zamachowca w serwisie Tumblr. Zamieścił na nim przy pomocy swojego telefonu posta tuż przed zastrzeleniem pierwszej ofiary. Podpis pod zdjęciem brzmiał:

„Musiałem to zrobić. Dzisiaj jest ten dzień. W poprzednich dniach nie podjąłem się próby, budziłem się z niepokojem, żalem i nadzieją na lepszą przyszłość. Dzisiaj było inaczej, nie czułem żadnych emocji ani empatii, ani współczucia. Będę wolny, a może nie. Nie obchodzi mnie to."

Podsumowanie

Gdy już nie da się odwrócić biegu wydarzeń pozostaje potrzeba uzyskania odpowiedzi, dlaczego do nich doszło. Z pomocą przychodzą działania i narzędzia informatyki śledczej.

W opisanej strzelaninie policja z hrabstwa Horward w stanie Maryland zaczęła używać rozwiazań od BlackBag, aby przyspieszyć swoje działania i otrzymać odpowiedzi na kluczowe pytania.

Wnioski dla polskich służb

Powyższy przykład, pomijając jego okoliczności, których na szczęście rzadko jesteście świadkami w Polsce, w dobrym stopniu obrazuje możliwości techniczne związane z pozyskaniem i analizą danych z wielu źródeł opartych o różne systemy operacyjne. Gdybyśmy chcieli przenieść na realia polskie proces pozyskania i analizy danych w opisywanym przypadku dobrym odpowiednikiem byłyby przestępstwa związane z podatkiem VAT. Występuje w nich zazwyczaj duża ilość danych, wiele źródeł, powiązanych osób. W takich dochodzeniach należałoby wybrać rozwiązania BlackBag.

Dave Proulx, Digital Forensic Instructor BlackBag

Built by Forensic Professionals for Forensic Professionals.

Digital Intelligence® FRED™ systems are used the world over to solve crimes and protect the innocent. Contact Mediarecovery sales or visit us at www.digitalintelligence.com for more information.

Digital Intelligence®

www.digitalintelligence.com

FRED™ Forensic Systems ❖ UltraBlock™ Write Blockers
UltraKit™ Forensic Acquisition Kits ❖ Forensic Hardware & Software Products
Instructor Led Training ❖ Lifetime Technical Support

Urządzenia IoT, jako źródło materiału dowodowego

Artur Piechocki, Katarzyna Gorzkowska

Gdy Richard Dabate ze szczegółami relacjonował śledczym w jaki sposób doszło do śmierci jego żony Connie, nie przypuszczał, że kluczem do poznania prawdy stanie się urządzenie Fitbit, którego pani Dabate używała podczas aktywności sportowej.

Rankiem 23 grudnia 2015 r. śledczy przybyli do położonego w USA miasta Ellington, gdzie w rodzinnym domu małżonków Dabate doszło do tragedii. Na miejscu zastali ciało zamordowanej Connie Dabate oraz jak się wówczas mogło wydawać jedynego świadka zajścia – cudem ocalałego męża. Richard Dabate opowiedział śledczym o walce stoczonej z zamaskowanym intruzem, który wtargnął do jego domu, przywiązał go do krzesła, a następnie zażądał portfela i kart kredytowych. Według relacji ten sam intruz miał zastrzelić w piwnicy Connie Dabate. Dane uzyskane z urządzenia Fitbit pozwoliły śledczym na ustalenie, że w czasie, w którym według relacji Richarda Dabate miała rozgrywać się walka z nieznanym napastnikiem, Connie Dabate przechadzała się po domu (przeszła 1217 kroków po całym domu). Urządzenie zarejestrowało także ostatni moment życia Connie. Dane uzyskane z niewielkiego krokomierza zamocowanego na ręku zmarłej przyczyniły się do postawienia Richardowi Dabate zarzutów i oskarżenia go o zabójstwo żony, składanie fałszywych zeznań i fałszowanie dowodów

Przykład opaski Fitbit (rodzaj krokomierza noszonego na ręku w trakcie np. biegania) pokazuje, że w USA dane zgromadzone dzięki urządzeniom Internetu Rzeczy coraz częściej stają się źródłem materiału dowodowego wykorzystywanego przez organy ścigania w celu ustalania przebiegu zdarzeń i weryfikowania relacji świadków. Internetem Rzeczy (ang. Internet of Things, w skrócie IoT) określana jest sieć łącząca przewodowo lub bezprzewodowo urządzenia, które pozyskują, udostępniają, przetwarzają dane, czy wchodzą ze sobą w reakcje pod wpływem danych. To, co z założenia miało stanowić narzędzie do zbierania i analizowania danych konsumenta dla lepszego zrozumienia jego potrzeb, w praktyce okazuje się być pomocne również organom ścigania i wymiarowi sprawiedliwości.

Historia zabójstwa Connie Dabate to wyłącznie jedna ze spraw kryminalnych, w której urządzenie IoT odegrało rolę cichego i niespodziewanego świadka. Jako przykłady można wskazać chociażby ustalenia w śledztwie dotyczącym śmierci Victora Collinsa. Postawienie zarzutów zabójcy Collinsa było możliwe dzięki urządzeniu Echo od firmy Amazon, znalezionym na kuchennym blacie w domu, w którym doszło do zbrodni. Wyposażone w mikrofony i czujniki urządzenie rejestrowało dźwięki, w tym słowa znajdujących się w pobliżu osób. Dane zaś były przechowywane w chmurze. Zarejestrowane nagrania dźwiękowe umożliwiły ustalenie przebiegu wydarzeń i sprawcy.

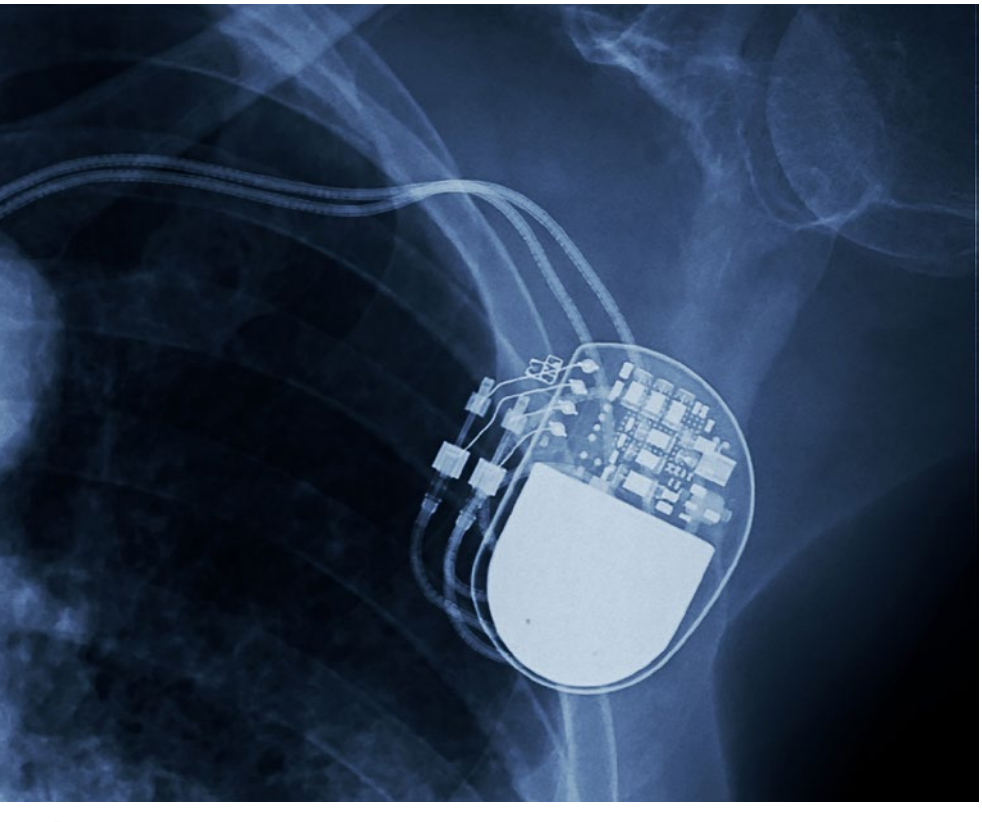
Postawienie zarzutów zabójcy Collinsa było możliwe dzięki urządzeniu Echo od firmy Amazon, znalezionym na kuchennym blacie w domu, w którym doszło do zbrodni. Wyposażone w mikrofony i czujniki urządzenie rejestrowało dźwięki, w tym słowa znajdujących się w pobliżu osób.

Należy również zwrócić uwagę, że do kategorii IoT zaliczane są nie tylko urządzenia znajdujące się w otoczeniu zewnętrznym człowieka. Jak się bowiem okazuje źródło materiału dowodowego mogą stanowić także dane uzyskane

z urządzeń znajdujących się wewnątrz ciała, jak przykładowo rozrusznik serca. W sprawie dotyczącej oszustwa ubezpieczeniowego, dane o tętnie i rytmie serca poszkodowanego przyczyniły się do wykluczenia wersji wydarzeń przedstawionej przez poszkodowanego, który twierdził, że po odkryciu pożaru zabrał swoje rzeczy i uciekł z płonącego domu przez okno sypialni. Przedstawiona przez niego wersja wydarzeń nie pokrywała się z danymi zarejestrowanymi przez rozrusznik serca. W tej sprawie kluczowe znaczenie miała opinia lekarza kardiologa, który po przeanalizowaniu odczytu danych o aktywności z rozrusznika uznał za nieprawdopodobne, aby osoba o takim stanie zdrowia w tak krótkim czasie była w stanie zgromadzić i usunąć przedmioty z płonącego domu.

> Jak się bowiem okazuje źródło materiału dowodowego mogą stanowić także dane uzyskane z urządzeń znajdujących się wewnątrz ciała, jak przykładowo rozrusznik serca.

Powyższe przykłady wskazują na ogólną tendencję do coraz częstszego sięgania po Internet Rzeczy w celach dowodowych. Dzieje się tak, ponieważ urządzenia IoT stają się popularne i powszechnie wykorzystywane. Dostrzeżone zostało także to, że dane uzyskane dzięki IoT mogą stanowić źródło cennych informacji o aktywności użytkowników, przydatnych zarówno organom ścigania, jak również stronom postępowania.



Generalnie nie widać przeszkód, aby informacje uzyskane dzięki IoT już teraz były wykorzystywane również w postępowaniach prowadzonych w Polsce. Zarówno na gruncie kodeksu postępowania cywilnego jak i kodeksu postępowania karnego przeprowadzenie takich dowodów należy ocenić jako dopuszczalne. Przykłady Fitbit, Echo i rozrusznika serca wskazują bowiem, że Internet Rzeczy może dostarczyć informacji dla ustalenia faktów mających istotne znaczenie dla rozstrzygnięcia sprawy, chociażby w myśl art. 227 Kpc.

Niemniej jednak, przeprowadzenie takich dowodów wiązałoby się z koniecznością jednoczesnego wykorzystania specjalistycznej wiedzy, m.in. z zakresu medycyny (jak w sprawie z rozrusznikiem serca). Należy przy tym wskazać chociażby na stanowisko Sądu Najwyższego, który uznał, iż dowód z taśmy magnetofonowej stanowiącej dowód rzeczowy wymaga przeprowadzenia również dowodu na identyczność zarówno utrwalonych głosów, jak i samej taśmy. Niewątpliwie urządzenia IoT ze względu na ich technicznie złożony charakter są urządzeniami o stopniu skomplikowania wyższym niż taśma magnetofonowa. Tym samym wykorzystanie informacji uzyskanych dzięki IoT nieodzownie wiązałoby się z koniecznością przeprowadzenia dowodu z opinii biegłego w myśl art. 193 § 1 Kpk, czy art. 278 Kpc.

Artur Piechocki, radca prawny, partner zarządzający w Kancelarii APLaw

Katarzyna Gorzkowska, prawnik w Kancelarii APLaw

10 więzień, 500 telefonów na miesiąc i 1 informatyk śledczy

Joel Bollö

Historia rozegrała się w amerykańskim stanie Tennessee. I choć na pierwszy rzut oka może wydawać się, że w związku z tym słabo koresponduje z polską rzeczywistością, jest to wrażenie błędne. Okazuje się, że w pewnych aspektach realia i wyzwania stojące przed służbami są bardzo podobne tak w Polsce, jak i w USA.

Służba Więzienna Stanu Tennessee (Department of Corrections Tennessee) od pewnego czasu próbowała przeciwdziałać rozwojowi gangu, który rozszerzał skalę swojej działalności pomimo tego, że duża część jego członków przebywała za kratami. Było to możliwe dzięki przemycanym za mury więzienia urządzeniom mobilnym. Dlatego też organy ścigania właśnie na nich skupiły swoją uwagę, starając się wydobyć z nich istotne dla prowadzonych działań informacje. Chciano w ten sposób zapobiegać aktom przemocy w samych więzieniach, uniemożliwić komunikację z przestępcami przebywającymi na wolności oraz zidentyfikować skorumpowany personel więziennictwa.

Niestety łatwiej było zaplanować operację niż ją wykonać. Wszystkie zarekwirowane telefony z 10 zakładów karnych przekazywano do centrali w Nashville celem analizy zawartych w nich danych. Żeby zobrazować skalę wyzwania warto powiedzieć, że w niektórych miesiącach przesyłano do analityka po 500 świeżo zarekwirowanych urządzeń. Ponad 5 pudeł zawierających po 100 telefonów w każdym. Smaczku sprawie dodaje fakt, że zajmował się tym jeden analityk śledczy. Jeden na cały stan. Można się domyślić, ile czekało się na wyniki jego pracy i jaką użyteczność miały zebrane przez niego informacje przekazywane zwrotnie po długich miesiącach od przechwycenia przemyconych urządzeń. W ten sposób pracowano do kwietnia 2017.

Problem z gangiem narastał i potęgował się. W końcu władze zdecydowały się nawiązać współpracę z firmą, która w USA cieszy się świetną renomą. Po konsultacjach ze specjalistami z MSAB władze podjęły decyzję o zainstalowaniu ośmiu terenowych stanowisk analizy urządzeń mobilnych (tzw. MSAB Kiosk) oraz pięciu aplikacji XRY na komputerach stacjonarnych. Dodatkowo po jednodniowym szkoleniu z obsługi również funkcjonariusze Służby Więziennej zyskali umiejętność ekstrakcji i analizy danych z zarekwirowanych urządzeń. Całość została połączona w sieć, zatem pojawiła się możliwość błyskawicznego podglądu informacji pozyskanych w poszczególnych zakładach karnych. Pozwoliło to na stworzenie kompleksowego obrazu siatki komunikacyjnej gangu.

Nie trzeba dużej wyobraźni, żeby zrozumieć jak przełożyło się to na efektywność działania służb. W przeciągu kilku miesięcy zidentyfikowano członków gangu, rozpoznano jego hierarchię oraz wytypowano osoby z nim współpracujące. Niektórych więźniów odizolowano, niektórych przeniesiono do innych zakładów karnych. Skorumpowanych funkcjonariuszy Służby Więziennej w części zdegradowano, innym wytoczono procesy.

Uzyskano również informacje związane z planowanymi atakami na funkcjonariuszy Służby Więziennej, dzięki czemu skutecznie je udaremniono. W efekcie władze podjęły decyzję o wyposażeniu w rozwiązania MSAB również biura kuratorów na terenie Stanu.

Podsumowując. Zaczęliśmy od liczb w tytule i na liczbach skończymy. 12 miesięcy po wdrożeniu rozwiązań MSAB, 12 osobowa grupa rozpracowująca gang przeanalizowała o 584% urządzeń mobilnych więcej, niż rok wcześniej.

Joel Bollö
CEO of MSAB

Wzmocnij swoje działania

Popraw szybkość, wydajność
i kontrolę działań mobile forensic.

Ekosystem

rozwiązań z zakresu mobile forensic

dla organów ścigania

Urządzenia mobilne są dziś jednym z najważniejszych źródeł dowodów cyfrowych w postępowaniach sądowych. W związku z tym potrzebujesz najlepszych dostępnych narzędzi, aby działać lepiej, szybciej i mądrzej. W chwili wyboru weź pod uwagę, które z oferowanych rozwiązań ułatwi Tobie oraz Twoim kolegom pracę nie tylko w laboratorium ale również w terenie. Zaufaj nam i naszemu doświadczeniu.

JEŻELI POTRZEBUJESZ WIĘCEJ INFORMACJI WEJDŹ NA STRONĘ FORENSICTOOLS.PL
LUB SKONTAKTUJ SIĘ BEZPOŚREDNIO Z NASZYM PARTNEREM -
FIRMĄ MEDIARECOVERY - BIURO@MEDIARECOVERY.PL

MSAB

www.msab.com

Konkurencja szybsza o dwa tygodnie Jak to możliwe?

Sebastian Małycha

Jak wynika z badania „*Data exfiltration study: Actors, tactics, and detection. 2017*" za 43% przypadków wycieku danych firmowych odpowiadają pracownicy. Warto podkreślić, iż większość firmowych danych przechowywana jest w formie cyfrowej, komputer i telefon staje się naturalnym narzędziem osób planujących nieetyczną działalność. Tego typu przypadki zawsze są wyzwaniem dla analityków oraz osób odpowiedzialnych za bezpieczeństwo. Szczególnie w sytuacji kiedy mamy do czynienia z milionami emaili, dokumentów i artefaktów użytkowników. W niniejszym artykule pokażemy, jak można poradzić sobie z tym problemem, wykorzystując narzędzia informatyki śledczej oraz platformę analityczną.

Wprowadzenie

Firma A z branży FMCG produkująca napoje i soki owocowe przygotowywała się do startu kampanii marketingowej związanej z wprowadzeniem na rynek nowego produktu. Dwa tygodnie przed jego premierą, bezpośrednia konkurencja, firma B, wprowadziła na rynek bardzo podobny produkt i promowała go bliźniaczo podobnymi reklamami. Jak się domyślamy cały plan marketingowo-sprzedażowy został „spalony". W konsekwencji firma A poniosła spore straty finansowe.

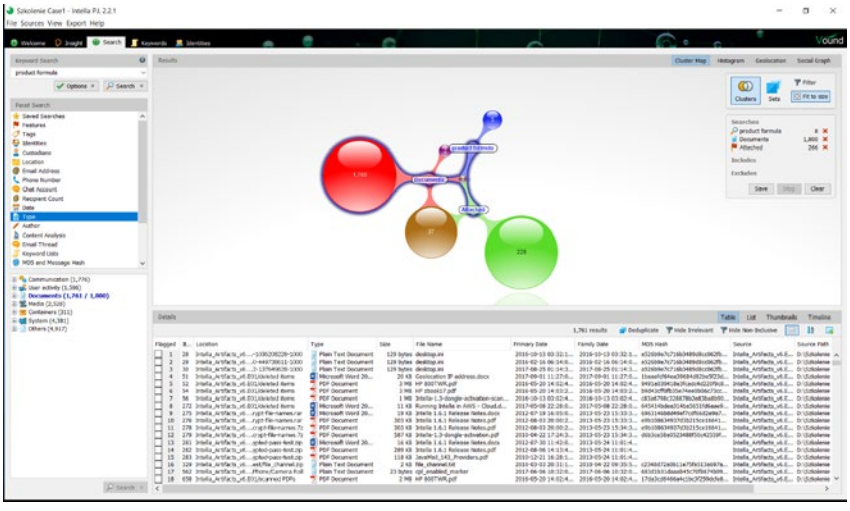
Dochodzenie wewnętrzne

W firmie A przeprowadzono dochodzenie wewnętrzne mające na celu wyjaśnienie sytuacji i znalezienie osoby lub osób odpowiedzialnych. Wytypowano pracowników, którzy wiedzieli o nowym produkcie i byli w posiadaniu kluczowych informacji na jego temat. Korzystając z usług wyspecjalizowanej firmy zewnętrznej, zabezpieczono zdalnie dane znajdujące się na ich urządzeniach służbowych. W praktyce oznaczało to jak najszybsze wykonanie kopii binarnych dysków w komputerach i laptopach osób wytypowanych oraz pełne ekstrakcje danych z ich telefonów. Użycie odpowiednich narzędzi informatyki śledczej pozwoliło firmie zewnętrznej działać zdalnie w sposób, który nie budził podejrzeń pracowników oraz nie generował dodatkowych kosztów związanych z podróżami służbowymi do poszczególnych oddziałów firmy.

W związku z koniecznością pracy z wieloma różnymi nośnikami danych (komputery i telefony) wszystkie dane wyodrębnione z tych urządzeń umieszczono w platformie analitycznej Intella, celem wykonania analizy powiązań pomiędzy urządzeniami i użytkownikami.

Przy pomocy platformy sprawdzono:

1. Którzy pracownicy i kiedy mieli dostęp (uprawniony i nieuprawniony) do informacji o składzie produktu i materiałów promocyjnych (tzw. kluczowe dane).
2. Czy którykolwiek pracownik przesyłał/rozpowszechniał poprzez jakikolwiek kanał komunikacji (skrzynka email w komputerze i telefonie służbowym, SMS, inne komunikatory, np. Skype) kluczowe dane – jeśli tak, to kto i kiedy.
3. Czy pracownicy mający dostęp do kluczowych danych, kopiowali je na nieautoryzowane (prywatne)



Rys. 1. Wyszukiwanie i filtrowanie dokumentów (rysunek poglądowy)

nośniki – jeśli tak, to kto i kiedy.
4. Czy pracownicy mający dostęp do kluczowych danych, wysyłali je do chmury lub na adresy email znajdujące się poza domeną firmy.
5. Kiedy i przez kogo kluczowe dane były drukowane.

Analiza z wykorzystaniem platformy analitycznej

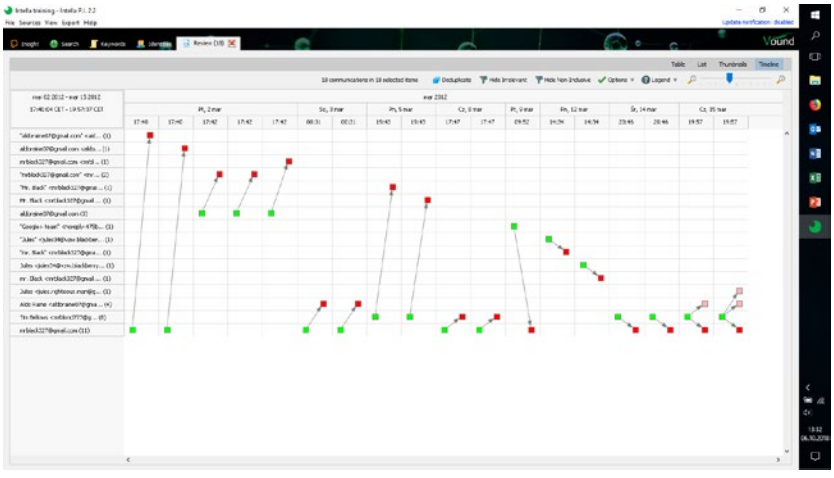
W pierwszej kolejności analiza polegała na wyszukaniu dokumentów, z uwzględnieniem załączników wiadomości email, zawierających wybrane słowa kluczowe (Rys. 1). Następnie sprawdzono załącznikami jakich wiadomości e-mail były te dokumenty, pomiędzy kim odbywała się korespondencja i przy użyciu jakich urządzeń (laptopy i telefony) (Rys. 2), a wyniki przedstawiono na osi czasu (Rys. 3). Po przeanalizowaniu dokumentów i korespondencji stało się jasne, że dwóch pracowników przechowywało kluczowe dane na swoich telefonach służbowych, które nie były odpowiednio zabezpieczone. Jeden z nich wysyłał wiadomości email sam do siebie, odbierał te wiadomości poprzez aplikację poczty w telefonie, następnie zapisywał załączniki w pamięci telefonu i przesyłał je z prywatnej skrzynki email na adres osoby z firmy B. Dalsza analiza wykazała, że jeden pracownik korzystał z prywatnej skrzynki email (Gmail) w telefonie służbowym oraz przesyłał kluczowe materiały na prywatny Google Drive (Rys. 4). W ten sposób rozstrzygnięto, kiedy kluczowe dane trafiły w ręce konkurencji.

W kolejnych krokach wykryto, że kluczowe dane były kopiowane na prywatne nośniki typu pendrive. Co więcej, ustalono jakie urządzenia i kiedy były podłączane przez poszczególnych użytkowników (Rys. 5).

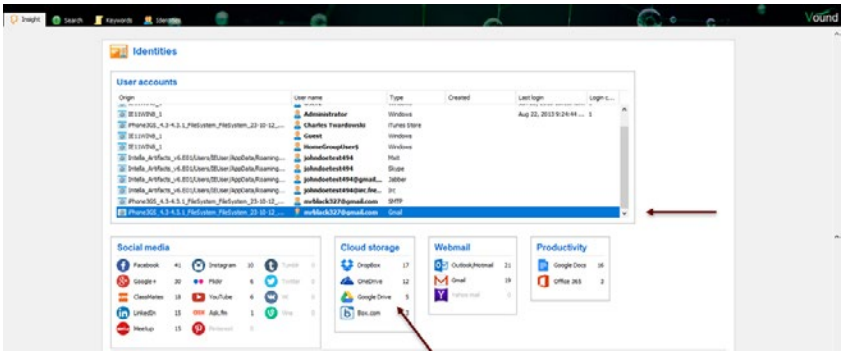
W ostatnim etapie analizy okazało się również, że materiały były drukowane przez jednego z pracowników w czasie pokrywającym się z przekazaniem tych danych konkurencji. Po połączeniu wszelkich informacji odkryto, że dane na temat nowego projektu przekazało firmie B dwóch

> Analiza wykazała, że jeden pracownik korzystał z prywatnej skrzynki email (Gmail) w telefonie służbowym oraz przesyłał kluczowe materiały na prywatny Google Drive.

Rys. 2. Analiza korespondencji e-mail (rysunek poglądowy)



Rys. 3. Korespondencja e-mail na osi czasu (rysunek poglądowy)



Rys. 4. Analiza artefaktów użytkownika i artefaktów internetowych

ściśle współpracujących ze sobą pracowników – jeden z działu handlowego, a drugi z działu marketingu. Dzięki oprogramowaniu Intella w dość krótkim czasie znaleziono sporo dowodów, które bezspornie wskazywały ich winę.

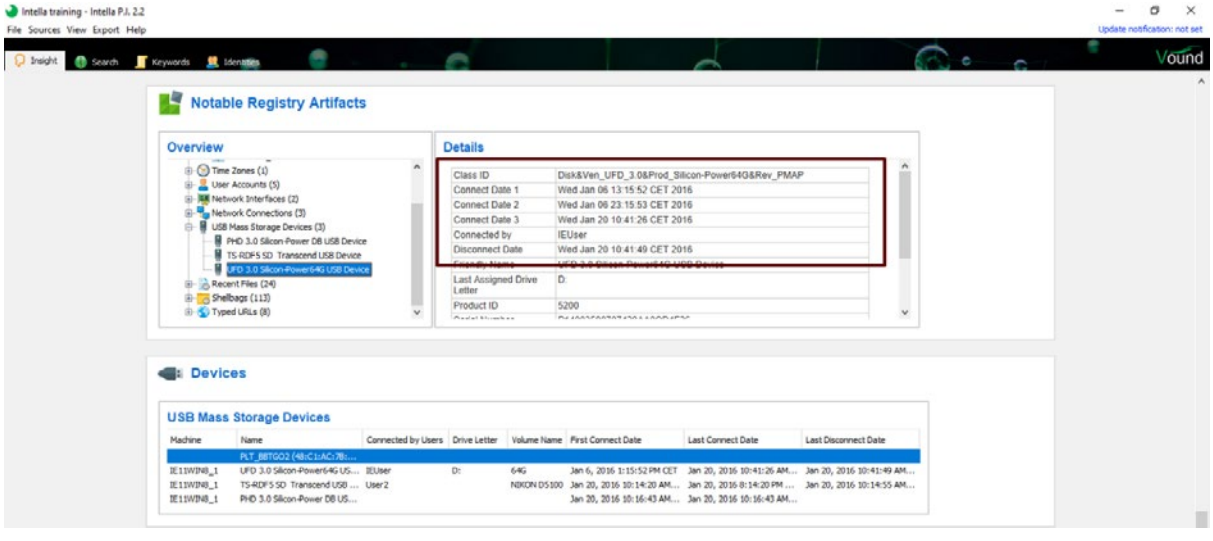
Kradzież danych z firmy A odbywała się na kilka sposobów:

» Jeden z pracowników wysyłał do osoby z firmy B wiadomości email zawierające kluczowe dane z prywatnego adresu email, lecz skonfigurowanego na służbowym telefonie,
» Dwóch pracowników kopiowało kluczowe dane na prywatne nośniki typu pendrive,
» Jeden z pracowników przesyłał kluczowe dane do chmury - na prywatny dysk Google Drive,
» Jeden z pracowników drukował dokumenty zawierające kluczowe dane, wbrew przyjętym w firmie procedurom.

Podsumowanie

Powyższy przykład miał na celu zobrazowanie skuteczności i efektywności działania platform analitycznych. Są one szczególnie użytecznym narzędziem, kiedy na analizę, jaką musimy wykonać, składa się wiele różnych urządzeń cyfrowych, komunikacja pomiędzy użytkownikami liczona w milionach wiadomości, dokumentów, załączników i jeszcze większa ilość zdarzeń sieciowych oraz wpisów w rejestrach.

Sebastian Małycha,
CEO / Prezes Zarządu
Mediarecovery



Rys. 5. Informacje o podłączanych urządzeniach typu pendrive wraz z datą i czasem zdarzenia (rysunek poglądowy)

Case study: Stabilizacja obrazu w nagraniu wideo

Zespół Amped Software

Specjaliści zajmujący się analizą video z CCTV mają bardzo często do czynienia z tanimi kamerami połączonymi z cyfrowymi rejestratorami wideo (DVR) dostarczającymi materiał bardzo niskiej jakości. Dzieje się tak, gdyż kamery te mają wysoką kompresję plików, co w rezultacie sprawia, że nagranie jest pokryte pikselowym ziarnem, a poszukiwana informacja jest niewyraźna na każdym zdjęciu poklatkowym. Taką właśnie sytuację specjaliści Amped Software mieli kilka miesięcy temu, gdy otrzymali nagranie samochodu, który brał udział w napadzie. Ich zadaniem było odczytanie tablicy rejestracyjnej.

Prześledźmy kroki postępowania specjalistów Amped Software

Otworzyliśmy wideo w Amped FIVE i zmierzyliśmy wysokość tablicy rejestracyjnej: 11 pikseli niewiele. Samochód jechał do przodu, więc próbowaliśmy zintegrować informacje z kilkunastu klatek. Niestety, prosta stabilizacja obrazu nie pomogła, gdyż tor ruchu pojazdu nie był idealnie prosty, a perspektywa tablicy rejestracyjnej zmieniała się. To co widzicie (Rys. 1) uzyskaliśmy po użyciu filtra Local Stabilization w Amped FIVE, wyśrodkowaniu kadru i regulacji ekspozycji światła.

Zauważcie, że nawet po stabilizacji, istnieje dość silne, nierównomierne rozmycie spowodowane zmianą pozycji tablicy rejestracyjnej. Sugerowało to konieczność wykonania korekty. Materiał wymagał ustabilizowania tablicy rejestracyjnej w każdej klatce trochę w inny sposób i wyrównania zmiany w perspektywie.

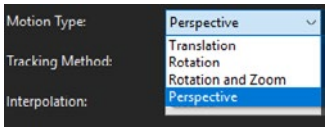
W najnowszym wydaniu Amped FIVE istnieją dwa filtry, które współpracują ze sobą, aby ustabilizować i uwydatniać w materiale wideo obiekt, który zmienia perspektywę będąc w ruchu: Perspective Stabilization (Stabilizacja perspektywy) i Perspective Super Resolution (Super rozdzielczość perspektywy).

Perspective Stabilization (Stabilizacja perspektywy)

Zaznaczamy większy obszar, wokół tablicy, aby uzyskać lepsze efekty (Rys. 2).

Po wybraniu obszaru punkty zostaną automatycznie dodane do parametrów filtra i możemy teraz wybrać Motion Type (typ ruchu), Tracking Method (metodę śledzenia) i Interpolation (interpolację).

Motion Type odnosi się do typu ruchu, który ma śledzić filtr. Wybraliśmy „Perspective".

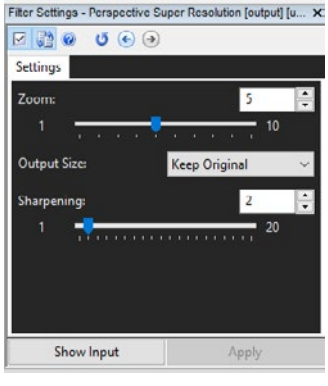


W Tracking Method (metoda śledzenia) wybraliśmy Dynamic Tracking (dynamiczne śledzenie), które porównuje każdą klatkę z poprzednią. Pozwala to ustabilizować większe odkształcenia, ale pozycja w ustabilizowanym filmie może nadal nieznacznie „dryfować".

W zakładce Output, która służy do ustalenia jakiego rodzaju rezultat chcemy uzyskać po użyciu filtra, wybraliśmy Prepare for Super Resolution, który pozostawił wideo niezmienione, ale dodał matrycę transformacji do każdej klatki.

Perspective Super Resolution

W ustawieniach zmieniliśmy powiększenie o wartość równą 5 jednostek.



W rezultacie otrzymaliśmy obraz (Rys.3).

Wyrównaliśmy nieznaczne rozmycie, które jest zwykle skutkiem integracji wybranych - kluczowych obszarów, poprzez zastosowanie delikatnego optycznego deblurowania (Rys.4).

Na koniec użyliśmy filtrów Correct Perspective i Sharpening, aby uzyskać widok tablicy na wprost i zwiększyć kontrast między znakami a tłem (Rys.5).

Przekazaliśmy obraz Policji, gdzie poproszono cztery różne osoby o niezależne dostarczenie znaków z tablicy rejestracyjnej. W rezultacie policjanci otrzymali: DI 21? ??, BT 21? MM, DT 210 AA, DT 210 MM.

W takiej sytuacji nie pozostało nic innego jak posłużyć się informacjami kontekstowymi. W przypadku włoskich tablic rejestracyjnych, takiej jak ta, można wykluczyć jakąkolwiek literę „I" i „O", ponieważ nie są one używane (za duże podobieństwo do „1" i „0"). Dodatkowo wszystkie tablice rejestracyjne zaczynające się od „B" zostały przypisane na długo przed rokiem wydania modelu samochodu, z którym mamy do czynienia. Biorąc to wszystko pod uwagę, pozostawiono tylko typy: DT 210 AA i DT 210 MM. Sprawdzając włoski rejestr pojazdów (w ramach publicznego dostępu) odkryto, że płyta DT 210 AA nigdy nie została przypisana do żadnego pojazdu. Zamiast tego tablica rejestracyjna DT 210 MM została przypisana do tego właśnie modelu samochodu o pomarańczowym kolorze.

Podsumowanie

Ten przypadek pokazuje, jak ważne jest użycie odpowiednich narzędzi we właściwej kolejności. Jak zaobserwowaliście, standardowa stabilizacja, po której następuje integracja klatek, nie była w tym przypadku najlepszym wyborem, ponieważ perspektywa tablicy rejestracyjnej zmienia się w nagraniu. Dzięki filtrom Perspective Stabilization i Perspective Super Resolution udało nam się automatycznie wybrać tablice i scalić ich informacje. Dzięki pozyskanym wskazówkom kontekstowym odczytano dane tablicy rejestracyjnej.

Zespół Amped Software

opentext™

OpenText forensics: The complete digital investigation solution

OpenText™ EnCase™ Forensic

The industry gold standard for scanning, searching, collecting and securing forensic data for internal investigations and law enforcement

Features:

- Broad OS support
- APFS decryption capabilities
- Cloud acquisition for Microsoft® Office® 365
- Mobile acquisition enhancements
- Internet artifacts collection
- Localized UI for multiple languages

OpenText™ Tableau Hardware

Winner of Forensic 4: Cast Awards for "Best Computer Forensic Hardware Tool" consecutively since 2009

Features:

Tableau Forensic Imager (TX1)

- Logical imaging and drive search
- Drive detection with whole disk encryption
- Simultaneous operations
- Intuitive UI localized in multiple languages

Tableau Forensic Hardware

- Forensic duplicators
- Forensic universal bridge
- Forensic adapters (PCIe, IDE, Micro SATA SSD, etc.)
- Regular firmware updates

opentext.com

Mobile Forensic a kwestia bezpieczeństwa danych służbowych.

Michał Tatar

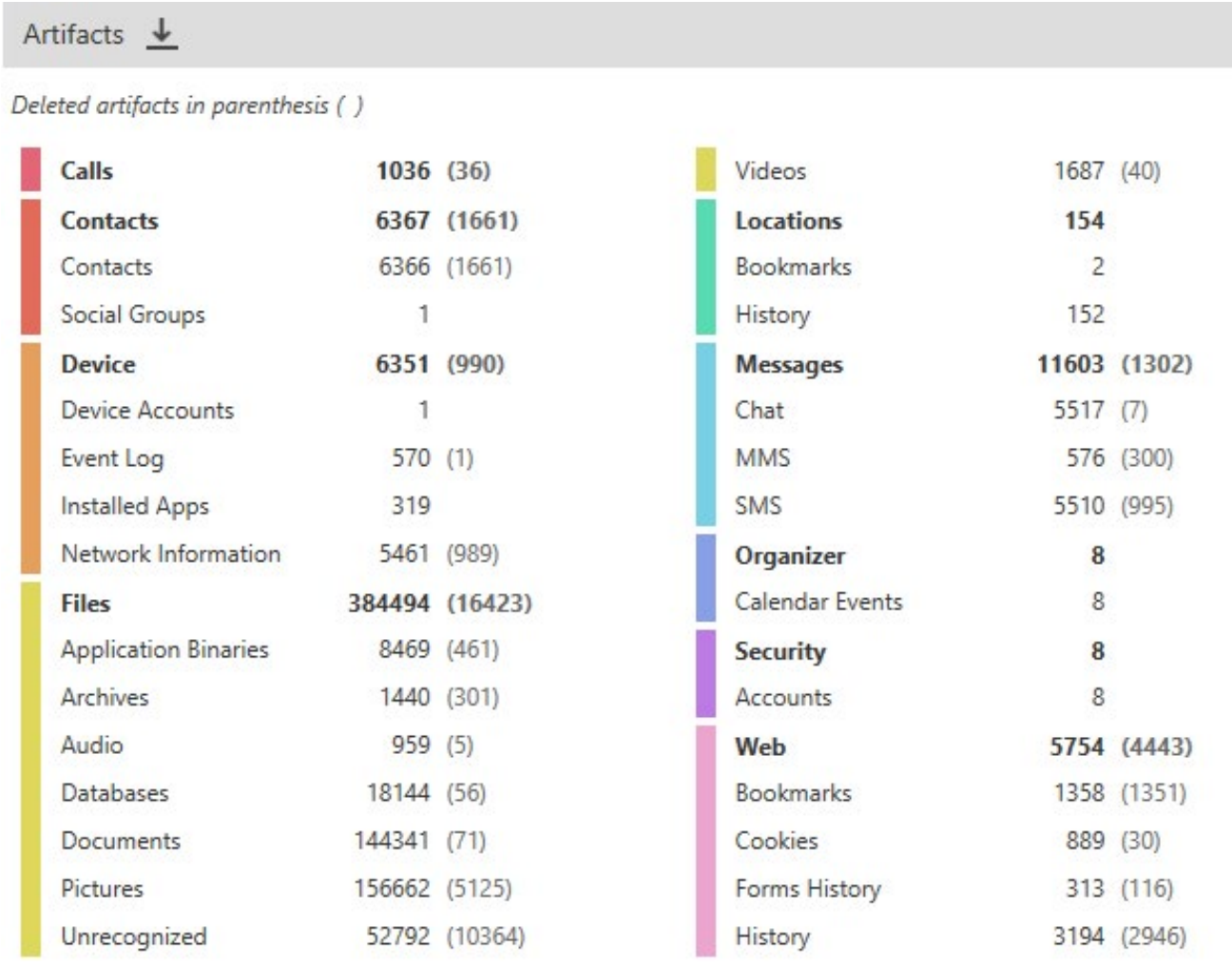
Świat pędzi nieustannie. Zdaje się, że z każdym kolejnym rokiem wręcz przyspiesza. Ludzie żyją „w biegu", mając coraz mniej czasu... A przecież jak świat światem, doba od zawsze miała 24 godziny, rok ma albo 365, albo 366 dni.
Nie o teorii czasu będę jednak pisał, ale o zjawisku, które jest wszechobecne w dzisiejszym szeroko pojętym biznesie (i nie tylko!).

Nawiązując do ostatnich raportów portalu Statista[1] szacuje się, że na całym świecie używanych jest ponad 4,5 miliarda urządzeń mobilnych. Liczba ta jest wręcz niewyobrażalna. Co więcej, zakłada się, że z roku na rok będzie stale rosnąć.
Trudno jednoznacznie oszacować, ile z tych urządzeń to te „służbowe". Warto jednak zwrócić uwagę na trend, iż wg. Google 80 procent ludzi nie opuszcza domu bez smartfona.

Trzeba się zastanowić, jak wygląda sprawa bezpieczeństwa danych w urządzeniach mobilnych, które są oznaczone jako „służbowe" (czyli takich, w których mogą być lub są przechowywane wrażliwe z punktu widzenia konkretnej firmy czy też organizacji informacje). Dodatkowo pojawia się trend BYOD (Bring Your Own Device), dzięki któremu pracownicy wpinają swoje prywatne urządzenia do zasobów organizacji i tym samym pobierają na nie służbowe wiadomości e-mail, załączniki, etc. Mając na uwadze powyższe, warto przytoczyć statystykę z ostatniego raportu Mobile Security Index 2019 wydanego przez firmę Verizon, w którym możemy przeczytać, że aż 70 milionów smartfonów ginie każdego roku, a tylko 7% z nich zostaje odzyskanych. To właśnie obrazuje pewnego rodzaju zjawisko, z którym borykają się organizacje, a które ja wziąłem pod lupę.

Spróbujmy założyć scenariusz, w którym to ja wcielam się w tego złego. Szczerze przyznam – będzie to mój pierwszy raz, kiedy stanę po ciemnej stronie mocy. W moich rękach znalazły się dwa takie same urządzenia oparte o system Android, czyli aktualnie najbardziej popularny na świecie system. Nie będę specjalnie na potrzeby tego artykułu wymieniał marki oraz modelu tych urządzeń, gdyż nie chciałbym, aby ktoś wyrobił sobie opinię (dobrą bądź złą) na temat tego producenta. Oba urządzenia po włączeniu witają mnie kodem blokady (na jednym urządzeniu założone hasło typu pattern lock, czyli popularny tzw. szla-

[1] https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/



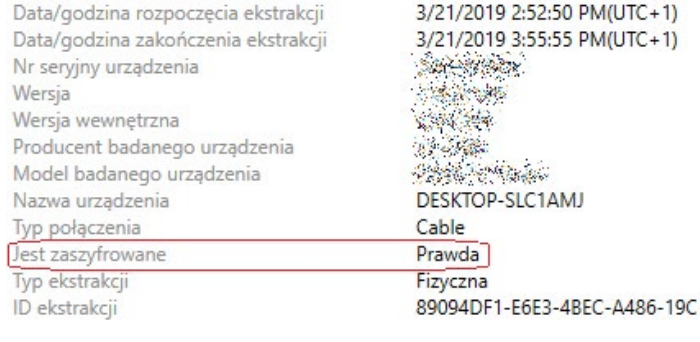
Rys. 2

czek, na drugim został użyty kod PIN). Na pierwszy rzut oka dostęp do danych w środku jest niemożliwy. Posługując się jednak specjalistycznym sprzętem i odpowiednią wiedzą, mogę dotrzeć do rozwiązań umożliwiających mi próbę uzyskania dostępu do danych zapisanych w pamięciach tych urządzeń. Urządzenie oznaczone jako nr 1 nie sprawia większych problemów. Do wyboru mam kilka możliwości – skorzystanie z podatności w obszarze Bootloader lub też odczyt pamięci metodami ISP/JTAG/Chip-Off. Wybieram opcję numer dwa, być może trudniejszą i wymagającą dodatkowych umiejętności, ale w tej sytuacji najpewniejszą.

Po poprawnym podłączeniu wykonuję pełny odczyt kości pamięci. Taki odczyt w formie pliku binarnego mogę analizować ręcznie bądź też skorzystać z gotowych parserów (automatycznych mechanizmów interpretujących kod binarny w dane rozumiane przez ludzi) zaimplementowanych w narzędziu XRY. Wynikiem tego działania jest odnalezienie hasła dostępu do urządzenia (wspomniany wcześniej pattern lock). Oprócz tego mam dostęp do wszystkich informacji zapisanych w tym urządzeniu (także do tych skasowanych, które udało się przy okazji odzyskać). (Rys. 2)

Ku mojemu zdziwieniu nie ma żadnych wiadomości e-mail. Sprawę na razie zostawiam i przechodzę do drugiego urządzenia.

Tutaj sprawa wydaje się trochę bardziej skomplikowana. Urządzenie nie oferuje możliwości odczytu pamięci metodami ISP/JTAG/Chip-Off. Dodatkowo wygląda na to, że pamięć urządzenia jest domyślnie szyfrowana. Na szczęście nie taki diabeł straszny, jak go malują. W przypadku szyfrowanych urządzeń z systemem Android istnieją możliwości technologiczne pozwalające na odczyt danych z kości pamięci oraz ich deszyfrację. W tej sytuacji skorzystam z podatności w obszarze Bootloadera (Rys. 3).



Rys. 3

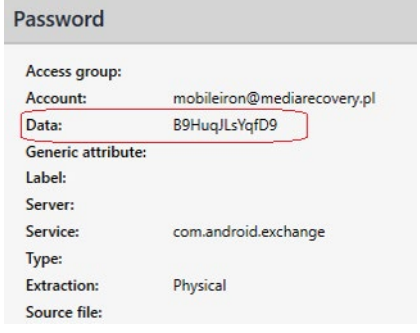
Po pierwsze, żadnego urządzenia mobilnego (nie ważne, jakiego producenta) nie możemy traktować jako natywnie bezpiecznego w 100% (bez względu na system operacyjny).

Odczyt oraz deszyfracja danych zakończyły się pełnym sukcesem. Przyjrzę się zatem wynikom. Uzyskałem komplet informacji, łącznie z wiadomościami e-mail. Mimo że telefon był zabezpieczony hasłem oraz był szyfrowany, udało mi się uzyskać dane istniejące oraz odzyskać te skasowane.

Dlaczego zatem brakuje mi wiadomości e-mail z pierwszego urządzenia? Wracam do niego, włączam i odblokowuję, znając już kod blokady (pattern lock). Moim oczom ukazuje się pełne menu telefonu. Szukam aplikacji do obsługi poczty elektronicznej. Próbuję ją uruchomić, ale przede mną kolejna zapora – o dziwo, dodatkowe uwierzytelnienie (Rys. 4).

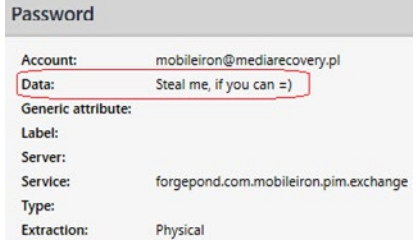
Rys. 4

Niestety nie znam tego kodu. W moim odczycie nigdzie takowego nie jestem w stanie znaleźć. Docieram do informacji, że aplikacja Secure Apps Manager to tzw. bezpieczny kontener rozwiązania firmy MobileIron. Okazuje się, że w takim bezpiecznym kontenerze użytkownik tego urządzenia przechowuje wszystkie wrażliwe informacje (poczta e-mail, służbowe notatki oraz kontakty, załączniki, etc.), do których nie jestem w stanie w żaden sposób się dostać. Analizuję informacje w urządzeniu numer 2 (w którym dane poczty elektronicznej zostały odczytane) i dochodzę do wniosku, że poczta e-mail na tym urządzeniu została skonfigurowana w natywnym kliencie poczty e-mail (poza bezpiecznym kontenerem) i mam do niej pełny dostęp (nawet do hasła konta Exchange) (Rys. 5).



Rys. 5

W urządzeniu, w którym poczta e-mail została skonfigurowana w ramach bezpiecznego kontenera, odnajduję jedynie tzw. Easter Egg (w słowniku IT, Easter Egg jest intencjonalnym, wewnętrznym żartem, ukrytą wiadomością) (Rys. 6).



Rys. 6

Zostaję zatem z prywatnymi danymi użytkownika...

Powyższy scenariusz ukazał kilka istotnych spraw z punktu widzenia bezpieczeństwa. Po pierwsze, żadnego urządzenia mobilnego (nie ważne, jakiego producenta) nie możemy traktować jako natywnie bezpiecznego w 100% (bez względu na system operacyjny). Specjalistyczne działania w obszarze Mobile Forensics pozwalają pozyskiwać dane z różnych urządzeń mobilnych (nawet mimo natywnego szyfrowania pamięci) i nawet jeśli urządzenie wydaje się bezpieczne dziś, to jutro może już takim nie być.

Problemem natomiast (bądź też ogromnym sukcesem – w zależności od której strony na to spojrzymy) jest pozyskiwanie treści z tzw. bezpiecznych kontenerów danych. Te na chwilę obecną są praktycznie nie do złamania. Jak będzie jutro? Tego nie wiem... Wiem natomiast, że cały scenariusz z mojej perspektywy był tylko zabawą, ale w rzeczywistym, pędzącym w szaleńczym tempie świecie jest jak najbardziej realny.

Michał Tatar, Mobile Security Engineer, Mediarecovery


MAGNET
FORENSICS
MAGNET AXIOM™
FIND THE EVIDENCE
THAT MATTERS.
Recover the most relevant chat, picture,
and browser history evidence possible.
magnetforensics.com

Współczesna biometryka głosu

Możliwości i zastosowanie unikalnego produktu firmy Phonexia

Dominik Gierałt

Przetwarzanie i analiza głosu to tematyka, z którą mierzy się na co dzień wiele instytucji, począwszy od rozbudowanych biur obsługi klienta (call center), banków, dyspozytorni medycznych, aż po podmioty rządowe, takie jak sądy czy organy ścigania. Związane jest to coraz częściej z wdrażanymi usługami telefonicznymi, które mają zapewnić wysoką jakość i bezpieczeństwo świadczonych usług.

Zdecydowana większość tych rozwiązań sprowadza się do nagrywania prowadzonych rozmów i kumulowania ich na rejestratorach audio. Biometryka głosu jest niezwykle pomocna do szybkiego i trafnego wyszukiwania rozmówcy w olbrzymiej ilości nagrań, a także zaawansowanego filtrowania rozmów, bez konieczności przesłuchiwania ich w czasie rzeczywistym.

Przykładów na wykorzystanie omawianej technologii jest mnóstwo. Dla instytucji, które mają przeanalizować setki godzin nagrań, niezwykle przydatnym modułem będzie transkrypcja audio. System automatycznie zapisze w formie tekstu przebieg rozmowy w trzech wariantach do wyboru: w formie jednolitego zapisu, z podziałem na dialogi, a także z zaznaczonym czasem wypowiedzi w danym nagraniu. W tym miejscu należy wskazać dodatkową funkcję w postaci słownika, za pomocą którego możliwe jest przeszukiwanie wyników transkrypcji i wskazywanie, w którym nagraniu i w jakim czasie zostały wypowiedziane wskazane słowa kluczowe. Kolejnym przykładem wykorzystania tej technologii będą centra obsługi telefonicznej, które docenią analizę rozmów pod kątem czasu reakcji rozmówcy, identyfikacji ilości rozmówców, dialogów, monologów, a także długości samego nagrania, czy też wieku i płci osoby, z którą prowadzona jest rozmowa. Dla innych przydatny będzie inte-

	Ilość godzin materiału przetwarzanego w 1 dzień pracy systemu
Identyfikacja rozmówcy	960
Transkrypcja audio	230
Wyszukiwanie słów kluczowych	1920
Identyfikacja języka wypowiedzi	960
Rozpoznawanie wieku rozmówcy	3840
Rozpoznawanie płci	38400
Diaryzacja rozmówców	9600
Określanie jakości rozmowy	384000
Detekcja aktywności głosu	28800

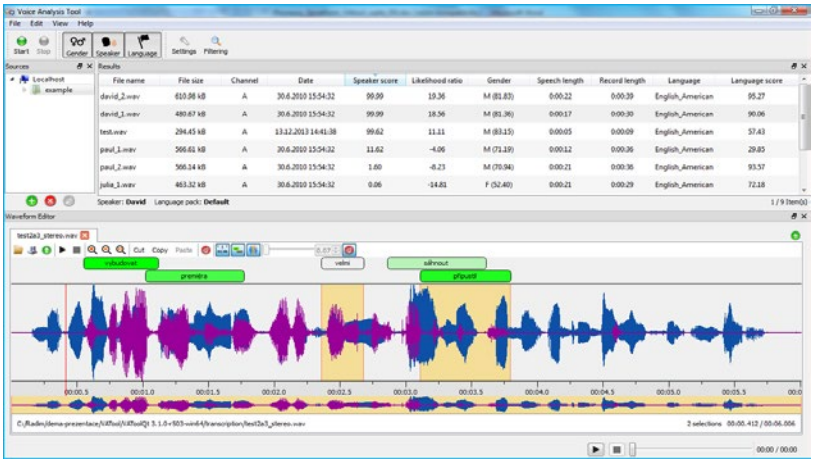
Tabela 1. Wydajność systemu dla poszczególnych modułów biometrycznych

ligentny moduł identyfikacji rozmówcy, który na podstawie wcześniejszych nagrań buduje model, umożliwiający następnie skuteczne typowanie innych rozmów tego rozmówcy, bez względu na jakość wypowiedzi, czy język jakim posługuje się w danym czasie dana osoba.

Stosując odpowiednie moduły biometryczne, jesteśmy w stanie filtrować duże zasoby nagrań i ograniczyć się do analizy materiału, który rzeczywiście zawiera treści będące w naszym zainteresowaniu. Jeśli do tego dodamy funkcję translacji offline, którą również można zintegrować z systemem to mamy produkt kompletny.

Jak to działa?

Phonexia to przede wszystkim produkt, który dzięki przejrzystości technologicznej pozwala na pełną integrację z istniejącymi systemami, rejestratorami i platformami danych, za pomocą udostępnionego REST API, jak również zestawu komend dostępnego w środowisku wiersza poleceń. Dopełnieniem rozwiązania może być tzw. Phonexia Browser - interfejs graficzny dla użytkownika końcowego, za pomocą którego możliwa jest prezentacja wykonanej analizy wraz z wynikami (Rys. 1).

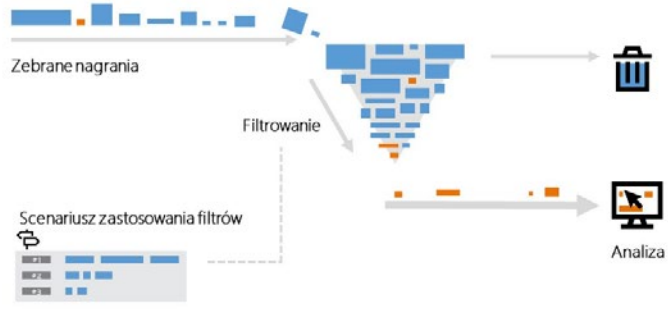


Rys. 1 Phonexia Browser – graficzny interfejs użytkownika

Phonexia pracuje na plikach audio w formacie wav. Możliwy jest także import wszelkich pozostałych rozszerzeń dzięki wspieranym kodekom, które automatycznie dobiorą parametry dla konwertowanego pliku.

Przetwarzanie dużego zasobu nagrań możemy zacząć od wyboru odpowiedniego scenariusza i schematu filtrowania danych. W zależności od potrzeb można zastosować biometrię w odpowiedniej kolejności i tym samym skrócić czas analizy (Rys. 2). W celu przeprowadzenia szybkiej i skutecznej identyfikacji rozmówcy optymalnym scenariuszem może być zastosowanie odpowiednio następujących modułów i wartości: wartość jakości rozmowy > detekcja aktywności głosu > identyfikacja języka wypowiedzi > porównanie z wcześniej utworzonym modelem rozmówcy. Tu wynikiem będzie wskazanie przez system wszystkich nagrań, w których występuje szukana osoba.

W przypadku analizy rozmowy kolejność i typ filtrów jest trochę inna. Należy wybrać kolejno: jakość rozmowy > detekcję aktywności głosu > język wypowiedzi > transkrypcję > słownik słów kluczowych. Wynikiem tego działania będą pliki transkrypcji, w których pojawiły się szukane przez nas słowa, a także ich synonimy. Oczywiście Phonexia Browser, pozwoli na podgląd danej rozmowy wraz ze wskazaniem, kto i kiedy wypowiedział szukaną sentencję.



Rys. 2 Proces filtrowania danych do analizy

Podsumowując, funkcjonalności systemu oraz łatwość integracji sprawdzi się tam gdzie na co dzień trzeba stawić czoła analizie dużej ilości nagrań. Narzędzie ułatwi pracę osobom piszącym stenogramy nagrań czy protokolantom, a w miejscach przetwarzania rozmów pozwoli na szybkie sortowanie i wyszukiwanie informacji. Narzędzie jest też niezastąpione w dziedzinie bezpieczeństwa, gdzie pozwoli np. na identyfikowanie agresywnych rozmówców i potwierdzenie czy pojawili się oni we wcześniejszych nagraniach, lub też czy nie dzwonili z fałszywymi alarmami do innych instytucji.

Dominik Gierałt
IT Security Engineer,
Mediarecovery

MAGAZYN INFORMATYKI ŚLEDCZEJ

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, Katarzyna Waniek

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