NR 2 | CZERWIEC 2009

Magazyn informatyki śledczej

Temat numeru

W drugim numerze Magazynu informatyki śledczej poruszamy przede wszystkim tematykę analiz telefonów komórkowych pod kątem dowodowym. Okazuje się bowiem, że telefon komórkowy to niezwykle cenne źródło informacji o podejrzanych. Łatwo jednak doprowadzić do utraty informacji tam zawartych lub naruszyć ich wartość dowodową. Stąd też wspólnie ze specjalistą informatyki śledczej postaramy się wprowadzić czytelników w to złożone i pełne niespodzianek zagadnienie.

Poza tym jeden z biegłych sądowych przedstawił swój punkt widzenia dotyczący współpracy z policją. Być może wśród czytelników znajdzie się osoba, która będzie chciała opowiedzieć jak to wygląda od drugiej strony? Zapraszamy do kontaktu z redakcją i współtworzenia Magazynu. Dodatkowo zamieszczamy kolejny odcinek cyklu dotyczącego zabezpieczania danych. Tym razem autor przedstawia przykładowe dochodzenie mające na celu ustalenie tożsamości anonimowego nadawcy maila. W tym numerze również przykład z życia oraz prawne rozważania dotyczące dowodu elektronicznego.

Serdecznie dziękujemy za wszystkie przesłane maile. Piszą Państwo m.in. że nasz Magazyn ukazuje się zbyt rzadko. Do końca roku jednak nie uda nam się zmienić częstotliwości wydawania. Być może zmieni się to od stycznia 2010.

Przyjemnej lektury.

O telefonach komórkowych słów kilka

Właściwe zabezpieczenie materiału dowodowego, jakim niewątpliwie może być telefon komórkowy, jest dopiero początkiem długiej, często niełatwej drogi prowadzącej do pozyskania informacji w nim zawartych. Telefony komórkowe są coraz bardziej powszechne, a w niektórych przypadkach nawet niezbędne, zarówno w życiu zawodowym jak i prywatnym. Biorąc pod uwagę fakt, iż statystycznie co drugi mieszkaniec kuli ziemskiej jest posiadaczem „komórki", nie sposób nie zauważyć z jak wielką i wszechstronną bazą danych mamy do czynienia.

...dokończenie na stronie 3

Współpraca biegłego i policjanta

Autor porusza najważniejsze z punktu widzenia biegłego aspekty współpracy z policją.

Dariusz Walczak

Niniejszy tekst został napisany z perspektywy osoby, która nie jest prawnikiem, nie jest policjantem jest natomiast biegłym z zakresu informatyki z ponad 10 letnim doświadczeniem.

Z powyższych powodów nie zamierzam tutaj cytować żadnych artykułów i paragrafów, na podstawie których funkcjonuje w polskim prawie instytucja biegłego – inni zrobili to już wcześniej i na pewno lepiej ode mnie. Zamierzam natomiast z perspektywy biegłego podzielić się swoimi doświadczeniami i wynikającymi z nich przemyśleniami. Pierwsze pytanie, które nasuwa się przy rozpatrywaniu kwestii współpracy biegłego i policjanta to pytanie, w którym momencie postępowania należy skorzystać z wiedzy i doświadczenia biegłego? Odpowiedź jest prosta - jak najwcześniej.

...dokończenie na stronie 7.

W NASTĘPNYM NUMERZE

Skupimy się na problemie „piractwa komputerowego". To chyba najpopularniejszy w Polsce sposób na łamanie prawa. Jak donosi Business Software Alliance - organizacja skupiająca producentów oprogramowania - ponad 50% komputerów pracuje na „piratach". Następny numer ukaże się w połowie września.

UE Z MICROSOFTEM

Portal Dziennik Internautów podaje, że pomimo nawoływania przez instytucje unijne do neutralności technologicznej one same korzystają z systemu Windows i pakietu MS Office. Włoski euro poseł Marco Cappato wystosował w tej sprawie zapytanie do Rady UE, pytając dlaczego instytucje UE nadal używają programów Microsoft narażając się tym samym na duże koszta i uzależniając się od firmy amerykańskiej. Jak informuje portal otrzymał on krótką odpowiedź, że „ryzyko uzależnienia od Microsoftu (…) jest wysoce ograniczone warunkami kontraktu zawartego z firmą". W sieci pojawiło się wiele komentarzy na ten temat. Przeważały w nich opinie, iż instytucje UE powinny przedłożyć interes obywateli nad interes jednej firmy.

DROGI INTERNET

OECD (Organizacja Współpracy Gospodarczej i Rozwoju) przeprowadziła badania dotyczące wysokości opłat za Internet pośród 30 krajów członkowskich. Wynika z nich, że w tej konkurencji Polska uplasowała się na drugim miejscu tuż za Meksykiem. Średnia cena 1MB/s to u nas koszt 32,59 $.

Zabezpieczanie elektronicznych nośników informacji - część 2.

Przestępstwa z użyciem komputera

Przemysław Krejza

W poprzedniej części niniejszego cyklu zostały omówione podstawowe właściwości dowodu elektronicznego oraz zasady związane z zachowaniem jego autentyczności i wierności. Przechodząc do dalszej części związanej z zabezpieczaniem dowodów elektronicznych posłużymy się przykładem dochodzenia mającego na celu ustalenie anonimowego nadawcy wiadomości email o charakterze pornografii dziecięcej. Postępowanie zostało wszczęte na wniosek poparty wydrukiem maila nadanego z adresu email Janek@onet.pl, 11 lutego 2009 o godzinie 14:58. Wersja elektroniczna maila nie jest dostępna.

- Adres Janek@onet.pl wskazuje, że nadawca maila korzystał z usług pocztowych dostępnych w ramach serwisu Onet.pl. Dostawcy usług internetowych oraz poczty elektronicznej przechowują dane użyteczne w identyfikacji nadawcy wiadomości, takie jak informacje o abonencie, oraz rejestr połączeń zawierający adres IP i znacznik czasowy/datę używany podczas połączenia z daną usługą.
- Na podstawie postanowienia zawierającego adres poczty elektronicznej oraz dokładną datę i godzinę wysłania. Onet.pl odpowiedział, iż nie posiada informacji o abonencie jednak w danym czasie z usługi korzystał adres sieciowy IP 123.131.132.133.
- Adres IP może ujawniać dostawcę usług internetowych wysyłającego mail lub np. jego pracodawcę, gdy wysyłający korzysta z usług internetowych w pracy. Na jego podstawie możliwe jest stwierdzenie skąd został wysłany przykładowy e-mail. Wyszukiwanie poprzez Whois (np. www.whois.domaintools.com) numeru 123.131.132.133 ujawnia że jest on powiązany z dostawcą usług TP S.A. (ISP).
- Na podstawie postanowienia zawierającego adres poczty elektronicznej oraz dokładną datę i godzinę wysłana maila, TP S.A. udzieliła informacji, iż w danym czasie adres był przydzielony Janowi Kowalskiemu, ul. Zielona 11, Warszawa.
- Dane kontaktowe mogą pozwolić na podjęcie decyzji o nakazie przeszukania.

Rozpoznanie potencjalnych możliwości dowodowych

W powyższym przykładzie przeprowadzone ustalenia, wskazują, iż być może zaistniała konieczność zabezpieczenia materiału w postaci dowodów elektronicznych. Pamiętajmy jednak, że tak może się zdarzyć w ramach każdego postępowania. Działanie zgodne z zasadami informatyki śledczej wymaga od organów ścigania właściwego podejścia do dowodów pochodzących z urządzeń elektronicznych, zgodnie z obowiązującymi przepisami prawnymi, dobrymi praktykami i innymi obowiązującymi wytycznymi, o czym była mowa w poprzedniej części cyklu.

Przed rozpoczęciem działań, w przykładowej sprawie, warto zastanowić się nad odpowiedziami na poniższe pytania:

- Czy jest sens zabezpieczania/analizy urządzeń komputerowych? - np. zapisy komputerowe są przeważnie dowodem pośrednim i nie wskazują sprawcy.
- Czy może zamiast komputerów wystarczy zabezpieczyć dane?
  - Kiedy komputery?
    - Zatrzymanie komputera (lub innych urządzeń) jest niezbędne w przypadku gdy jest on przedmiotem wykonawczym.
    - Zatrzymanie drukarek lub innych urządzeń jest niezbędne jeśli służyły np. jako narzędzia drukowania lub przetwarzania np. fałszywych dokumentów.
  - Kiedy dane?
    - Kiedy wymagane będzie badanie oprogramowania (kradzież własności intelektualnej, oprogramowanie jako narzędzie przestępstwa, itd.).
    - Kiedy wymagana będzie analiza danych (zdjęcia o charakterze pornografii dziecięcej, księgowość, zapisy z rozmów, poczta elektroniczna, itd.).
- Gdzie powinno zostać przeprowadzone przeszukanie danych - w miejscu zabezpieczenia czy w laboratorium? – np. nie można zatrzymać pracy urządzeń komputerowych gdyż odpowiadają za ważne procesy lub komputer zawiera dane kilku firm, a sprawa dotyczy jednej.
- Jeśli organy ścigania skonfiskują sprzęt z miejsca przestępstwa czy muszą zwrócić sprzęt i kopie danych na nim zawartych właścicielowi przed przeprowadzeniem procesu? - Jacy eksperci powinni zostać zaangażowani? - np. sieci komputerowe wymagają znacznie większej wiedzy od eksperta.
- Jakie dodatkowe działania policji są niezbędne - na przykład: większość haseł jest uzyskiwanych w trakcie zabezpieczania przy przesłuchiwaniu świadków. W przesłuchaniu świadków należy zatem zapytać o rodzaj aplikacji lub oprogramowania, które były używane oraz jak były zabezpieczone.
- Czy przed zatrzymaniem sprzętu nie zachodzi konieczność badań przez innych biegłych (toksykologa, daktyloskopia)? - np. tylko odciski palców na klawiaturze mogą jednoznacznie wskazać która osoba ostatnio jej używała.

Znając odpowiedzi na powyższe pytania zabezpieczanie będzie zapewne lepiej przygotowane. W najkorzystniejszej sytuacji powinno być ono poprzedzone również rozpoznaniem operacyjnym.

W kolejnej części skupimy się na tych dwóch aspektach postępowania z elektronicznym materiałem dowodowym.

W kolejnych częściach omówimy rozpoznanie potencjalnych możliwości dowodowych, zabezpieczanie oraz podejście do poszczególnych typów nośników i urządzeń komputerowych.

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

O telefonach komórkowych słów kilka

Dokończenie ze strony 1...

Tomasz Kemona

Wszechstronność informacji zawartych w „komórkach" wynika z wszechstronności samych urządzeń. Dzisiejsze telefony poza swoim pierwotnym przeznaczeniem, rozwiniętym o możliwość przesyłania krótkich wiadomości tekstowych SMS, posiadają wiele innych cech, które tworzą z nich kieszonkowe centra multimedialne. Aparat

1 mld PLN
Wartość polskiego rynku telefonów komórkowych w 2009 r.

fotograficzny, kamera cyfrowa, odtwarzacz MP3, są już w zasadzie standardem. Producenci prześcigają się w dozbrajaniu urządzeń w megapiksele mające wpływ na jakość wykonywanych fotografii i kręconych filmów. Dołączają wysokiej jakości słuchawki, również bezprzewodowe, aby jakość słuchanej muzyki była lepsza, a swoboda z jaką możemy korzystać z telefonu większa. **Pojemności pamięci liczone w gigabajtach umożliwiają gromadzenie coraz większej ilości danych.** Elektroniczne terminarze ułatwiają planowanie spotkań biznesowych, wakacji, a nawet zakupów. Wbudowane odbiorniki GPS pozwalają znaleźć drogę do celu w najdalszych nawet zakątkach świata. Większość telefonów komórkowych posiada możliwość łączenia się z internetem, umożliwiając użytkownikowi surfowanie po elektronicznym świecie informacji, wysyłanie wiadomości e-mail czy korzystanie z różnego rodzaju komunikatorów. Popularne stają się również rozmowy wideo, a nawet wideokonferencje, do których wykorzystywane są wbudowane w urządzenia dodatkowe kamery i zestawy głośnomówiące.

44 mln
To ilość abonentów telefonii komórkowej w Polsce w 2008 r.

Informacje zawarte w telefonach komórkowych nie zawsze są dostępne dla użytkownika z poziomu menu aparatu telefonicznego. Często aby uzyskać do nich dostęp należy wykonać tak zwany odczyt fizyczny pamięci telefonu. **Dzięki zastosowaniu specjalistycznego sprzętu i oprogramowania możliwe jest również odzyskiwanie danych skasowanych, takich jak: spis kontaktów, spis połączeń, wiadomości SMS, wpisy kalendarza, listy zadań, notatki, zdjęcia, pliki audio oraz wideo.**

1,12 mld
Sztuk komórek sprzedano na świecie w 2007 r.

Dysponowanie samym sprzętem i oprogramowaniem nie rozwiązuje jednak problemu, niezbędna jest bowiem również znajomość procedur i wiedza na temat tego co może naruszyć integralność zawartości pamięci, a w efekcie wykluczyć komórkę jako dowód.

Przy badaniu zawartości telefonów komórkowych nie można pozwolić sobie na błędy, mogą one bowiem całkowicie zaprzepaścić możliwość wydobycia z komórki informacji, mogących mieć kluczowe znaczenie dla sprawy. Bardzo ważne jest również samo zabezpieczenie materiału dowodowego, które powinno zostać przeprowadzone w sposób właściwy dla urządzeń mobilnych, ze świadomością tego jakie konsekwencje mogą przynieść niewłaściwe działania.

Numer seryjny IMEI

Poniżej przedstawiamy mini-słownik pojęć związanych z telefonami komórkowymi. Będą pomocne osobom chcącym lepiej zaznajomić się z tą technologią.

GSM - System GSM jest jednym z systemów telefonii ruchomej. Podobnie jak w innych systemach telefonii komórkowej, połączenie można uzyskać znajdując się w obszarze zasięgu stacji bazowej.

BTS - stacja bazowa jest zestawem urządzeń dzięki któremu możliwa jest komunikacja telefonu komórkowego z siecią GSM. Najczęściej spotykane stacje bazowe posiadają wysoki maszt, na którym zainstalowane są odpowiednie zespoły anten, umożliwiających komunikację z użytkownikami. Dzięki informacjom znajdującym się na karcie SIM możliwe jest ustalenie ostatniej stacji bazowej z jaką się komunikowała, co pozwala na określenie położenie geograficznego użytkownika.

IMEI - numer seryjny telefonu. Zawiera kilka ważnych informacji: kraj, kod producenta, model aparatu oraz jego właściwy numer seryjny. Numer ten powinien znajdować się na naklejce pod baterią telefonu. Można go również odczytać wprowadzając z klawiatury specjalny kod (*#06#), powinien się wówczas wyświetlić 15 cyfrowy kod IMEI. W niektórych przypadkach możliwe jest odzyskanie oryginalnego numeru IMEI, mogącego wskazać prawowitego właściciela telefonu.

ICC - numer identyfikacyjny karty SIM. Zawiera informacje o przynależności karty do danego operatora, jak również numer seryjny karty oraz rok jej wydania. W przypadku braku kodu PIN posługując się numerem ICC można wystąpić do operatora o udostępnienie kodu PUK.

IMSI - znajdujący się w pamięci karty SIM unikalny numer identyfikujący abonenta korzystającego z usług telefonii bezprzewodowej. Pierwsze trzy cyfry tego numeru to kod MCC (dla Polski wynosi on 260), kolejne dwie to kod MNC. Na podstawie numeru IMSI możemy jednoznacznie określić przynależność karty do danej sieci GSM.

MNC - unikalny w obrębie danego kraju numer identyfikujący sieć telefonii bezprzewodowej.

PUK - ośmiocyfrowy kod umożliwiający odblokowanie karty SIM po trzykrotnym błędnym wprowadzeniu kodu PIN. Kod PUK znany jest operatorowi konkretnej sieci. Po dziesięciokrotnym błędnym wprowadzeniu kodu PUK karta zostaje trwale zablokowana.

SMSC - centrum wiadomości SMS znajdujące się w infrastrukturze technicznej operatora sieci telefonii komórkowej. Centrum to pośredniczy pomiędzy abonentami przy przesyłaniu wiadomości SMS, w celu wysłania wiadomości SMS z telefonu komórkowego, należy w jego ustawieniach wpisać właściwy numer SMSC. Na podstawie numeru SMSC możemy określić wiarygodność nadawcy wiadomości SMS.

GPRS - technologia komunikacyjna stosowana w sieciach GSM do pakietowego przesyłania danych.

„Pościg z telefonem w tle”

Z życia wzięte czyli ciekawe przypadki zabezpieczenia danych.

Jarosław Wójcik

Data: styczeń 2009r.
Podejrzenie: Podwójna księgowość, oszustwa podatkowe
Cel: Zatrzymanie osób zarządzających z równoczesnym zabezpieczeniem danych księgowych, korespondencji mailowej oraz telefonów komórkowych.

ROZPOZNANIE:
Rozpoznanie operacyjne wykonane przez funkcjonariuszy Policji, wykazało, iż firma z branży medycznej zatrudniająca 10 osób, podejrzana jest o oszustwa podatkowe na kwotę przekraczającą 2mln zł. Firmą zarządza jedna osoba – prezes.

REALIZACJA:
Data: 15 styczeń 2009r, godz. 7:00
Miejsce: Budynek parterowy, centralna Polska

Godzina 6:30. Jesteśmy w wytypowanym miejscu na 30 minut przed zaplanowanymi działaniami. Czterech policjantów z wydziału prewencji, dwóch policjantów z wydziału do walki z korupcją oraz dwóch specjalistów informatyki śledczej. Czekamy na prezesa przygotowani by rozpocząć działania w momencie jego wejścia do firmy.

7:25 pojawia się samochód prezesa – czarny Nissan patrol na niemieckich blachach. Wszyscy przygotowani, ale co to..? Czarny Nissan zamiast zatrzymać się pod firmą odjeżdża szybko przyspieszając. „Coś jest nie tak, nie ma na co czekać wchodzimy do firmy, druga ekipa podejmijcie pościg” - wydaje dyspozycje prowadzący.

Wchodzimy do środka, szybki przegląd sytuacji cztery komputery stacjonarne, dwa laptopy, serwer, 3 telefony komórkowe. Przystępujemy do zabezpieczenia.

Tymczasem równocześnie z naszymi działaniami, 2 funkcjonariuszy kontynuuje pościg za czarnym Nissanem, policjanci raportują prowadzącemu: - Zatrzymaliśmy podejrzanego po 15 minutowym pościgu, w samochodzie zabezpieczyliśmy laptopa, podczas pościgu podejrzany wykonał rozmowę telefoniczna po czym w miejscowości Wielkie Młyny wyrzucił telefon komórkowy przez okno, telefon jest w częściach.

Zabezpieczenie trwało 8 godzin, zakończyło się sukcesem, kluczowym dla sprawy okazał się laptop prezesa oraz wyrzucony telefon komórkowy, który udało się „reanimować” do celów analizy.

Podsumowanie:
W dzisiejszych realiach najważniejsze informacje można znaleźć w telefonie komórkowym. Bardziej rozbudowane modele stanowią często „centra dowodzenia” osób prowadzących działalność gospodarczą. Dlatego też ważne jest by podczas zabezpieczania oprócz sprzętu komputerowego pamiętać również o „komórkach”.

Telefon wyrzucony z pędzącego samochodu

Wywiad z Jonasem Hanssonem z Microsystemation

Nowa kampania informacyjna MicroSystemations „Catch the Bad Guys” ukazuje jak prosta może być analiza telefonów komórkowych. To rzeczywiście takie proste czy jest to zabieg marketingowy?

Produkty Microsystemation projektowane są w taki sposób, aby praca nad materiałem dowodowym przysparzała jak najmniej problemów i komplikacji. Łatwy w użyciu, wielojęzyczny interfejs, możliwość jego dopasowania do potrzeb również raportów potwierdza opinie użytkowników, że narzędzia te są przyjazne śledczemu. Zarówno .XRY jak i XACT cechuje kompleksowość – zestawy dostarczane odbiorcy zawierają całe niezbędne okablowanie, interfejsy BlueTooth oraz IrDA, całość znajduje się w poręcznej walizce. Do tego jeszcze dopracowany manual, w którym użytkownik odnajdzie wszystkie wspierane przez te produkty modele. Mało tego – każdy użytkownik ma możliwość rozwoju produktu poprzez wpisy na forum Microsystemation czy dostarczanie raportów.

Jakie były początki firmy? Skąd pomysł na produkcję sprzętu i oprogramowania do analiz śledczych telefonów komórkowych?

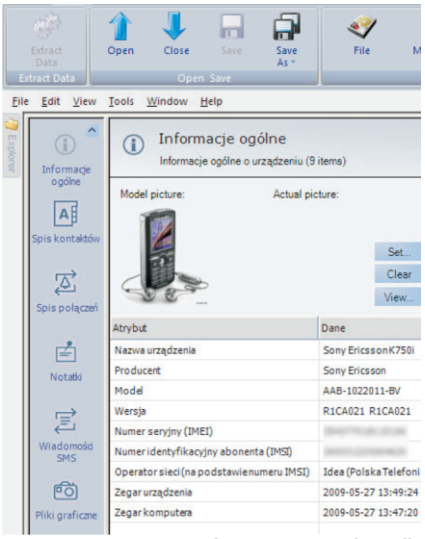
Firma Microsystemation została założona w 1984 roku i od początku zajmowała się najnowszymi technologiami w zakresie technik wymiany informacji i komunikacji. Początkowo skoncentrowano się na odpowiednim protokole transmisji używanym w przekazywaniu danych. Od 2000 roku firma zajmuje się wyłącznie technikami forensic w zakresie urządzeń mobilnych. Jeden z pierwszych produktów, jakim jest .XRY stał się de facto niedoścignionym standardem w pracy ekspertów Computer, a właściwie Mobile, Forensic.

... dokończenie na stronie 8.

Wstęp do analiz śledczych telefonów komórkowych

Tomasz Kemona

Popularne określenie „telefon komórkowy", czy też po prostu „komórka", ma w praktyce o wiele szersze znaczenie. Nie jest to jeden integralny element, lecz zestaw urządzeń mogących ze sobą współpracować, posiadających jednak odmienne cechy i służących do wykonywania różnych zadań. Przyglądając się bliżej popularnym komórkom można zauważyć, że każda z nich wyposażona jest w gniazdo karty SIM, a obecnie produkowane modele w większości posiadają również gniazdo karty pamięci.



Zrzut ekranu programu do analiz śledczych telefonów komórkowych .XRY

Karta SIM wchodząca w skład zestawu, popularnie zwanego komórką, jest jego nieodzowną częścią składową, zamontowana w specjalnym gnieździe, zazwyczaj gdzieś pod baterią, niejako z ukrycia pełni swoje kluczowe zadania. Służy między innymi do identyfikacji abonenta w sieci GSM, umożliwia poprawne logowanie oraz szyfrowanie transmisji. Bez tego małego elementu wykonywanie połączeń z telefonu komórkowego nie jest możliwe, oczywiście z wyjątkiem numerów alarmowych, takich jak 112, z którymi możemy się połączyć nawet bez zainstalowanej w aparacie telefonicznym karty SIM.

Karta SIM może również pełnić rolę pamięci przechowującej takie dane jak spis kontaktów, zawierający nazwę kontaktu oraz przypisany do niej numer. Wiadomości SMS, w ograniczonej wprawdzie ilości, jednakże również mogą znajdować się w pamięci karty SIM, w niektórych przypadkach pamięć zawiera również informacje o ostatnio wybieranych numerach telefonów, **przydatne zwłaszcza przy ustalaniu osób z którymi kontaktował się właściciel karty SIM.** W przypadku kart prepaid, popularnie zwanych telefonami „na kartę" możliwy jest odczyt z pamięci SIM'a numeru MSISDN, czyli po prostu numeru telefonu abonenta. **Karta SIM może zawierać również szereg innych informacji, które po szczegółowej analizie mogą wskazać przykładowo obszar, w którym dana karta była ostatnio zalogowana do sieci GSM.**

Aparat telefoniczny jest elementem najbardziej kojarzonym z określeniem „komórka", ze względu na najczęstsze z nim właśnie, bezpośrednie obcowanie przez użytkownika. Przy użyciu aparatu telefonicznego mamy dostęp do pozostałych elementów zestawu, czyli do karty SIM oraz karty pamięci. Aparat telefoniczny służy jako interfejs, który przy użyciu klawiatury i wyświetlacza, łączy użytkownika z zawartymi w nim danymi. Dane jakie mogą znajdować się w samym aparacie telefonicznym to oczywiście spis kontaktów, czyli nazwa kontaktu z przypisanym do niej numerem, często jednak rozszerzona o dodatkowe informacje, takie jak dodatkowe numery, adres e-mail czy nawet adres pocztowy.

Dzisiejsze aparaty telefoniczne mogą oczywiście przechowywać nawet setki wiadomości SMS, MMS oraz e-mail, ilość w konkretnym przypadku zależy jedynie od ilości pamięci w jaką producent wyposażył aparat telefoniczny. Możliwe do odczytania są również informacje o ostatnio wybieranych oraz odebranych połączeniach, wraz z datą i czasem ich wykonania, a nawet czasem trwania konkretnej rozmowy. **Istotnym jest fakt przechowywania przez aparat telefoniczny informacji o połączeniach nieodebranych, czyli faktycznie nienawiązanych, których operator może nie rejestrować, a co za tym idzie nie zostaną one zamieszczone na bilingu.**

Pamięć aparatu telefonicznego umożliwia również przechowywanie zdjęć, plików audio oraz wideo. Mogą to być zdjęcia i pliki zarejestrowane przez samo urządzenie lub mogą one pochodzić z innego źródła i być przesłane przykładowo przy pomocy wiadomości multimedialnej MMS czy też e-mail.

Nowoczesne telefony bardzo często pełnią rolę elektronicznych terminarzy zawierających listy zadań lub też inne notatki. **Terminarz aparatu telefonicznego może być synchronizowany z terminarzem komputera i być źródłem informacji o działaniach podejmowanych przez jego użytkownika, często z bardzo długiego okresu, gdyż informacje w nim zawarte nie zmuszają do noszenia ze sobą kilkusetstronicowego tradycyjnego papierowego terminarza.**

Trzecim, bardzo często pojawiającym się, elementem zestawu komórkowego jest karta pamięci, rozszerzająca pojemność pamięci aparatów telefonicznych nawet o gigabajty. Karta pamięci, w zależności od konkretnego przypadku, może przechowywać dane najróżniejszego typu, od zdjęć, plików audio począwszy, poprzez różnego rodzaju dokumenty, skończywszy na nawet pełnometrażowych filmach. Współczesne komórki mogą być oparte na mobilnej wersji systemu Windows, umożliwiającej korzystanie z pakietu Office i edycję dokumentów Word'a czy Excell'a. Pojemności kart pamięci sięgające gigabajtów również nie są niczym nadzwyczajnym, **pozwalają natomiast na przechowywanie nawet tysięcy zdjęć w jakości pozwalającej bez problemu odczytać z nich nawet takie szczegóły jak numery rejestracyjne pojazdów, nazwy ulic czy numery budynków.**

Każdy z elementów komórki może więc zawierać użyteczne informacje, aby jednak z nich skorzystać konieczne jest wykonanie pełnej analizy każdego z elementów, jak również właściwa interpretacja odczytanych danych.

Autor jest specjalistą ds. analiz śledczych telefonów komórkowych w laboratorium informatyki śledczej Mediarecovery, wykładowcą i prelegentem wielu szkoleń i konferencji.

Zestaw do analiz śledczych telefonów komórkowych

Dowód elektroniczny

Autor przedstawia kwestie związane z informacjami w formie elektronicznej z prawnego punktu widzenia.

Marek Chromik

Pomimo, iż informacje zabezpieczone z nośników cyfrowych coraz częściej odgrywają kluczową rolę w prowadzonych postępowaniach, dowód elektroniczny nie doczekał się legalnej definicji. Zarówno Kodeks Postępowania Karnego, jak i Kodeks Karny nie definiują czym jest dowód elektroniczny. Czy pojęcie odnosi się do całego komputera, telefonu, dysku twardego, czy może tylko do informacji zawartych na nośnikach? **Przyjmujemy, iż dowodem elektronicznym są informacje zapisane na nośnikach, które to informacje posiadają charakterystyczne cechy i wymagają specjalnego podejścia.** Dowód elektroniczny przeważnie będzie klasyfikowany jako poszlaka, chociaż czasami mamy do czynienia z dowodem bezpośrednim, np. nagranie wykonane telefonem komórkowym, wyraźnie wskazujące sprawcę. Charakterystyczne cechy dowodu elektronicznego są jego wadami i zaletami.

Podstawową wadą informacji w formie elektronicznej jest na pewno łatwość jej modyfikacji. Modyfikacja często wynika z nieznajomości technologii, kiedy przykładowo zabezpieczony dysk przeglądany jest bez zabezpieczenia przed ingerencją w dane. Samo załączenie zabezpieczonego komputera po sporządzeniu raportu z zabezpieczenia spowoduje zmiany dat ostatniej modyfikacji i dostępu. Obrona może podnieść, iż już po zabezpieczeniu nastąpiła ingerencja w postaci wgrania na nośnik odpowiednich treści. Daty modyfikacji i ostatniego dostępu będą wskazywały czas po zabezpieczeniu, a z punktu informatycznego, dowiedzenie, iż nie zostały wgrane jest praktycznie niemożliwe. W celu ochrony dowodu przed modyfikacją **należy stosować blokery zapisu, a dane cyfrowe w miarę możliwości autentyfikować sumami kontrolnymi.**

Kolejną cechą dowodu elektronicznego, która stanowi jego zaletę jest możliwość klonowania nośników. Ekspert z zakresu informatyki śledczej nie powinien pracować na nośniku oryginalnym, ze względu na ryzyko uszkodzenia i modyfikacji informacji. **Odpowiednio przygotowany klon nośnika (kopia binarna) umożliwia analizę w pełnym zakresie ponieważ zawiera identyczne informacje jak nośnik oryginalny.** Co więcej nie zawsze można zatrzymać sprzęt zastany w miejscu przeszukania. W takim przypadku zabezpiecza się same informacje, sporządzając raport z wykonania kopii binarnej.

Rozproszenie - cecha dowodu, która stanowi jednocześnie wadę jak i zaletę dowodu elektronicznego. Z jednej strony nie ma możliwości skompletowania wszystkich informacji o zdarzeniu, ponieważ informacje mogą znajdować się w komputerze, w logach firewalla, u dostawcy Internetu, na szeregu serwerach itp. Jednak z drugiej strony teoretycznie nie da się w pełni zatrzeć śladów przestępstwa popełnionego w sieci.

Analizując powyższe rozważania, należy uznać dowód elektroniczny za informację - cechę nośnika elektronicznego, posiadającą charakterystyczne właściwości i z tego powodu wymagającą specjalnego podejścia zarówno w trakcie zabezpieczania, jak i analizy. **Nieumiejętne obchodzenie się z takim dowodem prowadzi do jego modyfikacji, najczęściej nieumyślnej.** Dowód elektroniczny ze względu na fakt, iż jest informacją może być zwielokrotniony (z zachowaniem wierności). **Każdy błąd przy pracy z dowodem elektronicznym pozostawia ślad, który biegły informatyk wykaże w opinii, a obrona podniesie ten szczegół na sali sądowej.** Aby nie dopuścić do skompromitowania opinii, należałoby już na etapie zabezpieczania nośników współpracować z doświadczonym ekspertem informatyki śledczej, który zna specyficzne cechy dowodu i tym samym analizowane informacje pozostaną niezmienione i sterylne aż do czasu wprowadzenia dowodu z opinii do procesu.

Autor jest doktorantem kryminalistyki na Wydziale Prawa i Administracji Uniwersytetu Śląskiego, sekretarzem Stowarzyszenia Instytut Informatyki Śledczej, wykładowcą i prelegentem specjalistycznych szkoleń dla policji i prokuratury.

FBI w wirtualnej przestrzeni

Federal Bureau of Investigation prowadzi swoją działalność również w sieci

Zbigniew Engiel

FBI nie pozostaje obojętne na zmiany zachodzące w codziennym życiu obywateli. Skoro większość z nich powoli migruje w stronę wirtualnej rzeczywistości amerykańskie służby rozwijają swoją internetową działalność.

Do oczywistych w dzisiejszych czasach możliwości kontaktu poprzez pocztę elektroniczną, rozbudowaną stronę internetową www.fbi.gov dochodzą kolejne działania mające na celu być wszędzie tam gdzie potencjalne zagrożenia i ofiary. W połowie maja uruchomiono specjalny kanał na popularny serwisie YouTube.com redagowany w całości przez FBI. Stale powiększana ilość filmów przedstawia te służby „od kuchni", w akcji tak by każdy mógł poznać bliżej pracę agentów. Ciekawostką z pewnością jest film pokazujący przygotowania i pracę FBI podczas inauguracji prezydentury Baracka Obamy.

Kolejny internetowym obliczem Biura jest ich blog w największym na świecie portalu komunikacyjnym Twitter.com. Wykorzystuje się go do zamieszczania komunikatów i informacji o poszukiwanych osobach, o zagrożeniach jakie mogą dotknąć mieszkańców USA oraz do rekrutacji nowych pracowników.

FBI możemy również spotkać na amerykańskim odpowiedniku Naszej Klasy, czyli serwisie Facebook.com. Jak mówi John Miller, szef biura prasowego FBI „Chcemy być wszędzie tam gdzie są ludzie – wiemy, że dziesiątki milionów z nich spędzają czas na portalach społecznościowych dlatego i my tam jesteśmy".

Bez odpowiedzi pozostaje pytanie, kiedy polskie służby zaczną aktywizować się w cyberprzestrzeni i być w niej obecne z informacją, pomocą i wsparciem w większym stopniu niż do tej pory. Większość polskich służb posiada już obecnie strony internetowe lecz ich przejrzystość i atrakcyjność pozostawia wiele do życzenia.

Kanał FBI na Youtube.com

Współpraca biegłego i policjanta

Autor porusza najważniejsze z punktu widzenia biegłego aspekty współpracy z policją.

Dariusz Walczak

Rozumiem, w jakiej sytuacji finansowej znajdują się obecnie organa ścigania i mam świadomość, że w najbliższej dającej się przewidzieć przyszłości nic nie zapowiada aby nastąpiła w tej kwestii jakaś znacząca poprawa, ale pomoc biegłego o której myślę nie zawsze musi zaczynać się od momentu wydania formalnego postanowienia o powołaniu biegłego. **Niejednokrotnie wystarczy rozmowa w trakcie której bez jakichkolwiek szczegółów mogących stanowić naruszenie tajemnicy postępowania, policjant może ustalić lub zweryfikować przyjęty już odpowiedni tryb postępowania** z przedmiotami mogącymi stanowić potencjalny materiał dowodowy. Może zabrzmiało to trochę enigmatycznie, ale chodzi po prostu o sytuację, kiedy policjant zwraca się do biegłego np. z pytaniem: „Będziemy wykonywać czynności w mieszkaniu oraz w siedzibie firmy posiadającej wyłącznie biura i zajmującej się działalnością finansową. musimy zabezpieczyć „komputery" jak to zrobić?". Natomiast **w poważnych sprawach uważam za niezbędne już na etapie przygotowania do pierwszych czynności procesowych skorzystać przynajmniej z rady biegłego.**

Pewne służby policyjne już standardowo do czynności procesowych, w których mogą pojawić się przysłowiowe komputery powołują biegłego. Wówczas najczęściej do biegłego trafia tylko informacja: „w dniu XYZ od godziny X będziemy potrzebowali pana pomocy przy zabezpieczeniu sprzętu komputerowego, jest to mieszkanie/firma, spodziewany się X komputerów lub nie mamy żadnej wiedzy i tym. Czynności będą w miejscowości pana zamieszkania/ok. 200 km od miejsca pana zamieszkania proszę zarezerwować sobie co najmniej 6 godzin".

W takiej sytuacji to na biegłym spoczywa obowiązek właściwego zabezpieczenia i udokumentowania wszystkich czynności z tym związanych (dokumentacja fotograficzna, raporty, sumy kontrolne itp.).

Wówczas biegły analizując specyfikę sprawy oraz ujawnione i zidentyfikowane potencjalne źródła informacji proponuje prowadzącemu czynności sposób i zakres zabezpieczanego materiału, co jest bardzo istotne np. w przypadku firm, gdzie zabranie wszystkich komputerów grozi wstrzymaniem działalności firmy i wielotysięcznymi stratami. **Unikamy przy tym sytuacji, w której jako materiał dowodowy zabezpieczane są dziesiątki lub setki płyt CD z muzyką poważną, klucze sprzętowe lub urządzenia Bluetooth opisane jako „pamięci USB", albo puste obudowy po przeznaczonych do wyzłomowania komputerach.**

Kolejnym istotnym zagadnieniem są pytania do biegłego zawarte w postanowieniu, gdy już mamy zabezpieczony materiał dowodowy i nastąpił ten moment, kiedy należy poznać jego zawartość. Tutaj również, jeżeli policjant nie ma doświadczenia, lub posiada choć cień wątpliwości sugeruję konsultacje z biegłym jeszcze zanim postanowienie zostanie wydane. Unikniemy wówczas trudnych sytuacji, niepotrzebnych pretensji do biegłego, że pominął pewne istotne dla sprawy aspekty nie zauważając, że w badaniach ograniczają go właśnie pytania, na które jest zobowiązany udzielić wyczerpującej odpowiedzi.

Nie muszę w tym miejscu nikomu przypominać, że biegłemu po prostu nie wolno wykraczać poza zakres postanowienia. **Odpowiednio skonstruowane pytania znacznie ułatwiają pracę biegłemu, ale przede wszystkim prowadzącemu postępowanie policjantowi** dają gwarancję otrzymania opinii, w której znajdą się precyzyjne odpowiedzi na wszystkie ujęte w postanowieniu o powołaniu biegłego pytania. Może również zdarzyć się sytuacja, kiedy na dowodowym dysku ujawniono już w trakcie wcześniejszych badań określone treści, a obecnie powołuje się biegłego w celu przeprowadzenia ściśle określonych, dodatkowych czynności badawczych w innym kontekście. Dobrze byłoby, żeby w takiej sytuacji poinformować o tym fakcie biegłego wykonującego kolejne badanie.

Oczywiście nigdy nie jesteśmy w stanie przewidzieć do końca tego, co biegły może ujawnić w trakcie swoich badań. Czasami nie unikniemy sytuacji, gdy być może potrzebne będzie wydanie postanowienia rozszerzającego zakres pytań. **Przed podobnymi sytuacjami można częściowo zabezpieczyć się stosując pytanie „worek".** Zamiast kwestionowanego później w sądach sformułowania „Inne uwagi biegłego", które zapewne nie jest pytaniem, proponuję zadać biegłemu np. następujące pytanie: **„Czy na dostarczonym do badań materiale dowodowym w postaci * znajdują się inne treści mogące wskazywać na naruszenie przepisów obowiązującego prawa ?"**

Jest rzeczą oczywistą, że w tak krótkim artykule nie sposób zawrzeć wszystkich aspektów współpracy biegłego i policjanta. Starałem się w nim zasygnalizować jedynie najistotniejsze kwestie. **Nie ulega jednak wątpliwości, że im częściej prowadzący postępowania policjanci będą kontaktować się i konsultować z biegłymi tym mniej będzie postanowień o powołaniu biegłego, w których nie wiadomo tak naprawdę co autor miał na myśli** oraz opinii biegłego, w których nawet autor nie wie do końca o co chodzi.

Policjanci i biegli są po prostu na siebie skazani i to od nas samych zależy jak ta współpraca będzie się układać i jakiej jakości dokumenty będą wychodzić spod naszej ręki.

Autor jest biegłym III kadencji z zakresu informatyki z listy biegłych Prezesa Sądu Okręgowego w Olsztynie.

Wywiad z Jonasem Hanssonem z Microsystemation

...dokończenie ze strony 4

Firma pochodzi ze Szwecji ale Waszych produktów używają nie tylko szwedzcy policjanci?

Nasze rozwiązanie jest uznawane i stosowane przez specjalistów z całego świata (policja: szwedzka, francuska, amerykańska, angielska, holenderska, szwajcarska, belgijska, hiszpańska i wiele innych instytucji, służb i przedsiębiorstw). Produkty zostały przetestowane i znalazły uznanie w oczach takich organizacji jak NIST (National Institute of Standards and Technology) czy International Association of Computer Investigative Specialists. Rozwiązania takie charakteryzują się wysoką skutecznością, przy jednoczesnym zachowaniu standardów niezbędnych przy analizach dowodowych. Kwartalne upgrade'y pozwalają na ciągły rozwój .XRY i XACT, a dodatkowo, poprzez przesyłanie do producenta raportów ze statystykami zawierającymi badane modele telefonów, występuje możliwość wpływania na kierunki rozwoju sprzętu i oprogramowania w kolejnych wersjach.

Co jest największym problemem technicznym z waszego punktu widzenia w zakresie analiz śledczych GSM?

Najwięcej problemów przysparza mnogość producentów urządzeń mobilnych. Zdarza się, że w obrębie nawet jednej grupy produktowej (np. niskobudżetowe produkty Nokia) istnieje kilka standardów odczytu danych czy systemów zapisu plików. Często jest tak, że urządzenie nie ma dedykowanego portu komunikacyjnego – wtedy staramy się stworzyć protokół umożliwiający pobranie danych przez porty serwisowe. Już teraz nasze zestawy zawierają ok. 40 kabli, a wciąż tworzymy nowe by sprostać wymogom zaawansowanych użytkowników. Niestety producenci urządzeń mobilnych nie palą się do współpracy i strzegą swoich tajemnic dotyczących architektury i budowy telefonów.

A co z koniecznością szybkiej analizy?

Problem powstaje kiedy policjanci nie posiadają na swoim wyposażeniu odpowiedniego sprzętu i oprogramowania. Oddanie zabezpieczonego telefonu do laboratorium kryminalistycznego i oczekiwanie długie tygodnie na wyniki ekspertyzy w większości przypadków nie ma sensu. Informacje pozyskane z telefonów komórkowych szybko się dezaktualizują. Podejrzani zmieniają numery, plany, miejsca pobytu. Tego typu dane po kilku tygodniach nie będą przedstawiać już żadnej wartości dla prowadzącego dochodzenie. Dlatego tak ważna jest szybkość działania, możliwa na przykład dzięki posiadaniu własnego zestawu .XRY i XACT naszej produkcji.

Jakie są perspektywy rozwoju branży?

Chcemy rozwijać nasze produkty zgodnie z nowo pojawiającymi się trendami. Już przecież zawiązała się koalicja producentów aby stworzyć jeden standard ładowarek, za czym z pewnością pójdą inne elementy, w tym oczywiście interfejsy komunikacyjne. Z drugiej jednak strony, telefony z zegarem 600 MHz i pamięcią 128 mb ram to już nie science-fiction, i umożliwiają skuteczne szyfrowanie danych, połączeń czy steganografię. Wiąże się to z ogromem pracy przed nami. Będziemy starać się sprostać wszystkim wyzwaniom, by utrzymać pozycję niekwestionowanego lidera technologicznego w zakresie Mobile Forensic.

Magazyn informatyki śledczej
mediarecovery Instytucja Specjalistyczna

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

Redaktor prowadzący: Zbigniew Engiel.
Redakcja:
Przemysław Krejza, Marek Chromik,
Jarosław Wójcik.
Skład, łamanie, grafika: Tomasz Panek.
Reklama: Anna Czepik.

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