NR 1 | KWIECIEŃ 2009

Magazyn informatyki śledczej

Tytułem wstępu

Naszym celem jest przygotowanie magazynu, który będzie obiektywnym źródłem praktycznej i teoretycznej wiedzy dotyczącej pracy z elektronicznym materiałem dowodowym.

XXI wiek jest bez wątpienia wiekiem informacji. Postępująca komputeryzacja spowodowała, że przyjmują one najczęściej formę elektroniczną. Już ponad 93 % wszystkich poruszających się w świecie informacji to dane w formie cyfrowej. Nawet te słowa, czytane w papierowym wydawnictwie powstały przecież w komputerze.

Rewolucja cyfrowa bezpośrednio dotyka również funkcjonariuszy policji, prokuratorów, sędziów. Codziennością jest przecież zabezpieczanie podczas czynności - bez względu na rodzaj kwalifikacji kodeksowej - komputerów osobistych, przenośnych pamięci, telefonów komórkowych, aparatów fotograficznych, zapisów monitoringu itp.

Stąd też pomysł na niniejszy magazyn, poruszający najważniejsze problemy związane z przejawami cyfrowej rewolucji w codziennej pracy funkcjonariuszy i wymiaru sprawiedliwości. Będziemy starali się radzić w oparciu o nasze wieloletnie doświadczenia jako instytucji specjalistycznej posiadającej największe w tej części Europy laboratorium informatyki śledczej. Będziemy również zapraszać do współpracy innych ekspertów, najlepszych w swych dziedzinach by podzielili się swą wiedzą z czytelnikami.

„Magazyn informatyki śledczej" będzie pojawiał się raz na kwartał. Mamy również nadzieję, że z numeru na numer będzie powiększał swoją objętość. Zapraszamy do lektury!

Informatyka śledcza to codzienność w pracy organów ścigania

W następnym numerze:

Tematem wiodącym będzie tak zwany mobile forensics czyli analizy telefonów komórkowych. To dość nowa i szybko rozwijająca się dziedzina przysparzająca specjalistom sporo kłopotów. Ciągłe zmiany technologiczne, tysiące modeli i systemów oznaczają problemy. Z drugiej strony „komórki" to nieocenione źródło dowodów i poszlak.

Wspólnie ze specjalistami postaramy się odpowiedzieć na najczęstsze pytania z tym związane. Zamieścimy również drugą część cyklu o zabezpieczaniu sprzętu komputerowego oraz kolejny przykład z życia.

Następny numer Magazynu pojawi się w połowie czerwca 2009 roku.

Bloker - podstawowe narzędzie informatyki śledczej

Bez tego urządzenia nie powinno się nawet przymierzać do wydania opinii lub ekspertyzy z zakresu informatyki

Blokery to urządzenia uniemożliwiające ingerencję w badany nośnik. Pozwalają na odczyt informacji czy też wykonanie kopii ale nie pozwalają niczego dodać, zmienić czy poprawić. Ich zastosowanie w ramach czynności nie pozwoli podnieść obronie zarzutu manipulacji. Użycie blokera nie wymaga wysokiej wiedzy technicznej czy instalacji dodatkowego oprogramowania. Badany nośnik widoczny jest w menu jak każde inne urządzenie.Dlatego też blokery nazywane są podstawowym narzędziem informatyki śledczej.

Popularna jest historia jednego z biegłych, który badał komputer pod kątem nielegalności nie używając blokera. Dodatkowo nie miał swojego komputera więc opinię sporządził w komputerze podejrzanego. To oczywiście przypadek skrajny. Można jednak założyć, że biegły nie posiadający blokera nie powinien wykonywać analiz sprzętu komputerowego. [ZE]

Przykładowy bloker

NAPISZ DO NAS

Jesteśmy otwarci na współpracę. Masz coś ciekawego do powiedzenia w zakresie informatyki śledczej? Chciałbyś przeczytać o czymś na naszych łamach? Chcesz skomentować artykuł?

Napisz:
redakcja@mediarecovery.pl

PIERWSI PIRACI ARESZTOWANI

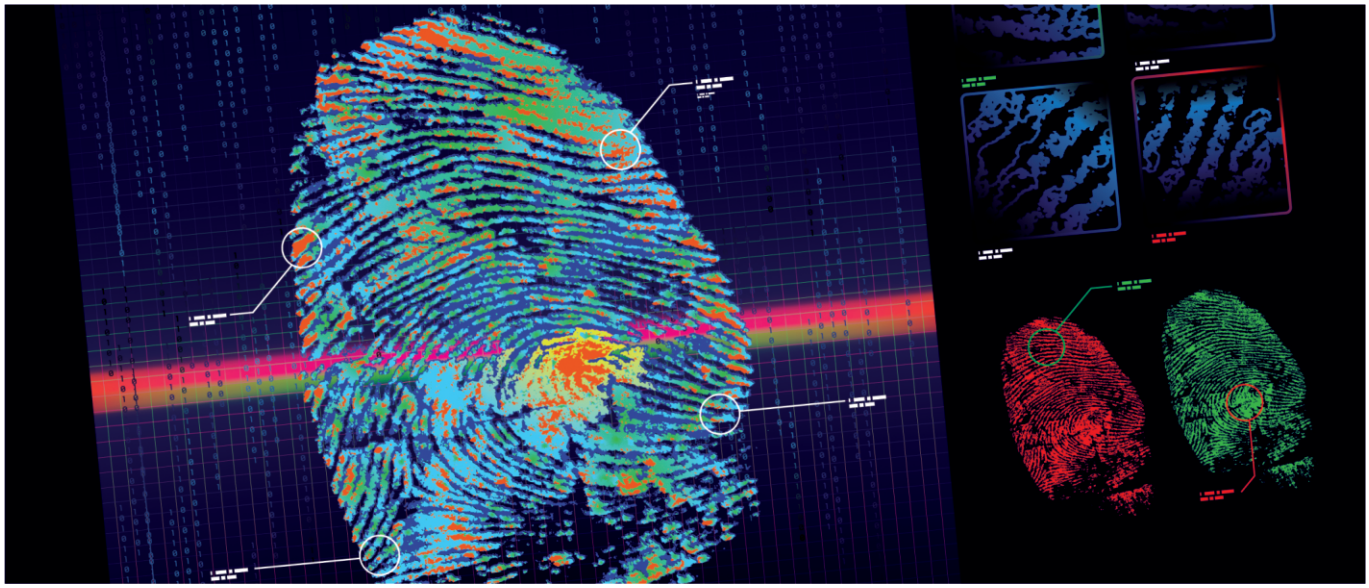
Portal Interia.pl poinformował, iż we Szwecji aresztowano pierwsze dwie osoby za piractwo. Wprowadzone nowe prawo zmniejszyło ruch w sieci o 1/3. Specjaliści twierdzą, że to etap przejściowy, a piraci znajdą nowe sposoby na obejście przepisów. Dwaj zatrzymani mężczyźni podejrzani są o udostępnianie plików chronionych prawami autorskimi. Wydaje się – jak informuje portal – że następnym krajem zmieniającym przepisy będzie Francja.

CYBER OBAMA

The Wall Street Journal informuje, iż nowa administracja w Białym Domu poważnie podchodzi do tematu cyberzagrożeń. Utworzone zostanie stanowisko Krajowego Doradcy ds. Cyberbezpieczeństwa, koordynujące działania w tym zakresie wszystkich rządowych agencji.

Dobre praktyki w poszukiwaniu i zabezpieczaniu dowodów elektronicznych. cz.1

W ramach tego cyklu skupimy się przede wszystkim na dowodach elektronicznych oddzielając je od tradycyjnie pojmowanego sprzętu komputerowego.



Przemysław Krejza

Komputery i cyfrowe nośniki informacji są coraz częściej wykorzystywane w nielegalnej działalności różnego typu. Komputer może służyć w dowolnym rodzaju przestępstwa bądź to jako narzędzie popełnienia czynu o charakterze przestępczym, być przedmiotem wykonawczym samego przestępstwa lub przechowywać zapisy mogące być dowodami innych przestępstw.

W ocenie możliwości dowodowych pochodzących z elektronicznych nośników informacji mogą pomóc następujące przykłady:

1. Komputer lub informacja na nim zapisana jako przedmiot wykonawczy – np. komputer lub jego elementy pochodzą z kradzieży lub oprogramowanie zainstalowane na komputerze nie posiada odpowiednich licencji.
2. Komputer jako narzędzie czynu o charakterze przestępczym – np. oprogramowanie zainstalowane na komputerze służyło do przełamywania zabezpieczeń w obcych systemach lub do podrabiania dokumentów.
3. Komputer lub zapisana na nim informacja zawiera dowody innych przestępstw – np. dealer narkotyków przechowuje informacje o dostawcach lub na komputerze zainstalowany jest komunikator za pomocą którego morderca porozumiewał się z ofiarą.
4. Komputer służył zarówno jako narzędzie przestępstwa jak i przechowuje informacje, które mogą być dowodami – np. haker używał komputera do atakowania innych systemów i przechowuje na nim informacje o skradzionych kartach kredytowych.

Jak widać z powyższych przykładów współczesne dochodzenie, a potwierdzają to statystyki, może w każdym momencie prowadzić do konieczności zabezpieczenia i analizy sprzętu komputerowego lub znacznie częściej, dowodów zapisanych na elektronicznych nośnikach informacji – tzw. dowodów elektronicznych. We wszystkich bowiem przypadkach, poza pierwszym, wartość dowodową będzie posiadał zapis w komputerze a nie sam sprzęt.

Dowód elektroniczny posiada cechy szczególne, które odróżniają go od „tradycyjnych" dowodów rzeczowych. Obrazy, dźwięk, tekst i inne dane przechowywane na np. dyskach twardych mogą być łatwo niszczone i uszkodzone. Informacyjna właściwość nośnika może zostać zmieniona poprzez modyfikację lub usunięcie danych, w tym również poprzez celową manipulację. Ponadto zapis z jakim mamy do czynienia w systemach komputerowych, umożliwia manipulację w taki sposób, że nie będzie możliwe stwierdzenie czy i kiedy zmiany te nastąpiły. Z drugiej strony, zrozumienie cech dowodu elektronicznego, pozwala na wprowadzenie nowych technik jak na przykład zabezpieczenie tylko zawartości nośników bez zatrzymywania sprzętu komputerowego.

Dowód elektroniczny wymaga również specyficznego podejścia w całym postępowaniu od zabezpieczenia, poprzez analizę, aż po prezentację w sądzie. Takie podejście, poprzez „najlepsze praktyki", wprowadza informatyka śledcza. Sprowadzają się one przede wszystkim do dbania o jego dwie podstawowe cechy - autentyczność i wierność. Autentyczność odpowiada za bezsporność pochodzenia materiału, a wierność za możliwość stwierdzenia czy materiał nie został w jakikolwiek sposób zmieniony w trakcie zabezpieczania lub analiz. Zachowanie autentyczności i wierności opiera się o następujące zasady:

1. Zabezpieczany sprzęt i nośniki powinny być prawidłowo (jednoznacznie, z wyróżnieniem cech indywidualnych) oznakowane, opisane w protokole zabezpieczania i oplombowane.
2. Dowód powinien być zachowany w stanie z chwili zabezpieczenia z dokładnym odnotowaniem daty i czasu w protokole zabezpieczania.
3. Zatrzymanie danych z pominięciem sprzętu komputerowego powinno opierać się o tworzenie kopii utworzonej na zasadzie równości z oryginałem (o tego typu kopii w kolejnych numerach Magazynu).
4. Jedyną możliwością autentyfikacji materiału jest wyliczenie w momencie zabezpieczania sumy kontrolnej nośnika (poświęcimy jej odrębny artykuł).
5. Badania powinny być prowadzone wyłącznie na kopii, tak aby nie naruszyć wartości dowodowej oryginału i umożliwić inne (innym biegłym) badania na tym samym materiale.
6. Konieczne badania prowadzone na oryginale, powinny być prowadzone z użyciem technik uniemożliwiających zmiany zapisów zawartych na badanym nośniku.

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

Po nitce do kłębka

Z życia wzięte czyli ciekawe przypadki zabezpieczenia danych.
W tym cyklu będziemy starali się pokazać najciekawsze przykłady związane z zabezpieczeniem dowodów elektronicznych.

Jarosław Wójcik

Data: jesień 2008r.
Miejscowość: w południowej Polsce
Cel: sprawdzenie adresów IP komputerów obecnie połączonych z serwerem rozdzielającym sygnał płatnej telewizji cyfrowej czyli praca na „żywym organizmie".

ROZPOZNANIE:
Rozpoznanie operacyjne wykonane przez funkcjonariuszy Komendy Miejskiej Policji wykazało, iż w mieszkaniu nr 8, przy ul. Żeromskiego 53*, osoba zarządzająca osiedlową siecią komputerową udostępnia bez zezwolenia sygnał płatnej telewizji cyfrowej. Zabezpieczenie serwera podczas pracy pozwoli na zebranie informacji dotyczących adresów IP komputerów pobierających nielegalny sygnał.

REALIZACJA:
Data: 12 wrzesień 2008 r., godz. 7:00
Miejsce: mieszkanie prywatne, piętro 4

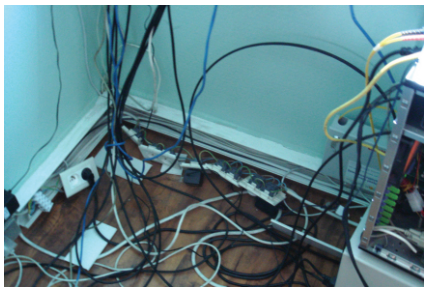
Jesteśmy we czterech. Trzech policjantów i ja, specjalista informatyki śledczej. Pukamy do drzwi wytypowanego mieszkania. Otwiera je młody mężczyzna w wieku około 30 lat. Po wylegitymowaniu okazuje się bratem podejrzanego. W domu jest sam. Niestety widok funkcjonariuszy nie ucieszył go zbytnio. Nie jest zbyt rozmowny, na większość pytań odpowiada wzruszeniem ramion i oschłym stwierdzeniem „nie wiem" albo „brata nie ma, nie wiem kiedy będzie". Lecz nie załamujemy rąk. Bez podejrzanego też powinniśmy sobie poradzić. Chwila namysłu, krótki przegląd sytuacji, przystępujemy do przeszukania. Telewizor to dobry punkt wyjściowy, jest zapewne podłączony do poszukiwanego przez nas serwera. I rzeczywiście to dobry trop. Po kablu jak po przysłowiowej „nitce" dotarliśmy do „kłębka" czyli piwnicy, gdzie wśród zakurzonych regałów, połamanych mebli i mnóstwa kartonowych pudeł stał poszukiwany serwer. Bez monitora, klawiatury i myszki.

Cwaniaki - pomyślałem sobie ale to akurat nie był problem. Byliśmy przygotowani i na taką ewentualność. Szybkie podłączenie moni-tora, klawiatury, myszki, i… pojawia się obraz. Ale, ale co to? Wskaźnik sam porusza się po ekranie! Mała konsternacja z mojej strony, chwila zastanowienia. *Panie komisarzu* - mówię - *ktoś jest zalogowany zdalnie do tego serwera i zaczyna formatować dyski*. Komisarz pyta co możemy zrobić w tej sytuacji. *Szybko wyłączajmy z prądu* – radzę. Krótka wymiana zdań, szybka, jedyna słuszna decyzja specjalisty informatyki śledczej i działanie. Bezpardonowe, brutalne wyłączenie serwera pozwoliło zachować zapisy na dyskach. Niestety prawdopodobnie informacje kto w danym momencie i z jakiego adresu IP był podłączony zostały utracone. Prawdopodobnie, bo jak powiedziałem policjantom - *wszystko zależy od konfiguracji serwera*. To ustalimy na spokojnie już u nas w laboratorium informatyki śledczej. W toku przeprowadzonych działań zabezpieczono 1 serwer, 2 komputery stacjonarne, 1 laptop, 4 pamięci USB, 141 płyt CD/DVD.

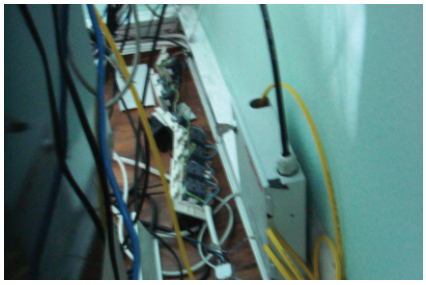
PODSUMOWANIE:
Ta historia ma pokazać, jak ważną rolę odgrywa rozpoznanie operacyjne. Równie ważne, jeśli nie ważniejsze jest uniemożliwienie osobom będącym na terenie realizacji czynności jakiejkolwiek komunikacji z osobami z zewnątrz. To prawdopodobnie brat podejrzanego dał mu znać smsem, że w mieszkaniu jest policja. Na szczęście w tym przypadku dzięki szybkiej reakcji informatyka, dane nie zostały usunięte, a cała akcja zakończyła się sukcesem.

* Wszystkie dane umożliwiające identyfikację osób i miejsc zostały zmienione.

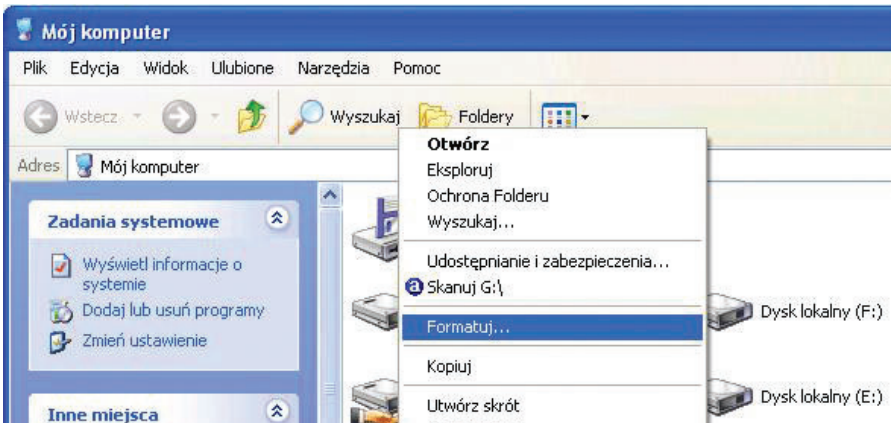
Zdjęcia operacyjne – miejsce zatrzymania, serwer.



Zdjęcia operacyjne – miejsce zatrzymania, infrastruktura sieciowa.



Zdjęcia operacyjne – miejsce zatrzymania, infrastruktura sieciowa.



Zdjęcia operacyjne – zrzut ekranu serwera

Zakres opinii

Zdaniem autora żaden biegły, wydający opinię nie powinien wykraczać poza zakres ekspertyzy, wyznaczony przez organ procesowy w postanowieniu.

Marek Chromik

Problem pojawiający się przy wielu opiniach dotyczy sytuacji, w której biegły wykracza poza jej zakres. Jeżeli celem postanowienia jest na przykład stwierdzenie występowania treści o charakterze pornografii dziecięcej, to biegły nie powinien w tej ekspertyzie, bez konsultacji z organem procesowym określać nielegalności oprogramowania, a już na pewno nie może określać wysokości szkody, z tym związanej.

Jeżeli jednak biegły w toku badań pozyskuje inne informacje, może, a czasami nawet powinien poinformować organ, który wydał postanowienie. Powinność ta pojawia się w przypadku, gdy biegły znajduje informacje świadczące o możliwości popełnienia przestępstwa. To organ procesowy zadecyduje, czy rozszerzyć zakres opinii, a jeżeli tak, to w jakiej formie. Co więcej powołany biegły może nie mieć kompetencji do badania i opiniowania w pewnym zakresie.

Możliwe, że informacje znalezione przez biegłego będą wymagały powołania innego eksperta. Wielu biegłych, w tym informatyków wykracza poza rygorystyczny zakres opinii. Naraża to opinię na kompromitację. Obrona zawsze może podnieść kwestię niekompetencji biegłego w stosunku do części opinii.

Przykładem jest wyliczanie szkody związanej z nielegalnym oprogramowaniem. Rzadko bowiem zdarza się, aby biegły informatyk był jednocześnie „biegłym rewidentem". Kluczową więc rolę odgrywa tutaj postanowienie wydawane przez organ procesowy. Postanowienie wyznaczające zakres opinii musi zawierać takie pytania, aby biegły mógł w ramach swoich kompetencji wydać rzetelną opinię. Kompetencje biegłego wyznaczające zakres w jakim może on opiniować, znaleźć można w sądach, przy których biegli są wpisani na listę biegłych. Składając wniosek o ustanowienie biegłego, wnioskodawca musi wskazać „dziedzinę biegłości" z podaniem dokładnego jej zakresu. Jeżeli powołuje się biegłego informatyka w celu zbadania telefonów komórkowych, a zakres biegłego obejmuje tylko i wyłącznie badanie komputerów, to wnioski z wydanej opinii bardzo łatwo podważyć w sądzie. Poruszając aspekt kompetencji badania telefonów komórkowych należy mieć szczególnie na uwadze nie tylko kompetencje biegłego, ale również sprzęt i oprogramowanie niezbędne do analizy GSM. Jeżeli biegły nie wpisał w zakresie swoich kompetencji analizy telefonów, najprawdopodobniejszą przyczyną będzie fakt, iż taki biegły nie dysponuje odpowiednimi narzędziami.

Podsumowując powyższe rozważania należy zauważyć, iż profesjonalna opinia, która nie zostanie w łatwy sposób podważona przez obronę, w dużej mierze zależy od działania samego organu procesowego. Pytania zawarte w postanowieniu, zadane w sposób konkretny i niewykraczający poza kompetencje biegłego są kluczem do wydania rzetelnej opinii. Wcześniejsza konsultacja z ekspertem pozwoli w sposób wyczerpujący sformułować postanowienie, a współpraca organu z biegłym w trakcie wydawania ekspertyzy wykluczy ewentualne błędy formalne oraz niedomówienia.

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