

Odtwarzanie i badanie dowodów przestępstw komputerowych

Autorzy:

Michael G. Noblett

Starszy Partner
Booz-Allen & Hamilton
Falls Church, Virginia

Mark M. Pollitt

Szef Zespołu
Computer Analysis and Response Team
Federal Bureau of Investigation
Washington, DC

Lawrence A. Presley

Instruktor Szkoleniowy
Forensic Science Training Unit
Quantico, Virginia

Wprowadzenie

Świat staje się ciasnym miejscem do życia i do pracy. W biznesie, w przemyśle i w naszych domach zachodzi technologiczna rewolucja w komunikacji i wymianie informacji. Na codzień przesyłamy pieniądze drogą elektroniczną i bardziej prawdopodobne jest otrzymanie wiadomości e-mail, niż listu. Obecnie zakłada się, że populacja użytkowników Internetu wynosi ok. 400 milionów.

W erze informacji zmieniają się też regulacje prawne. W przypadku niektórych, tradycyjnych przestępstw, zwłaszcza w sektorze finansowym i handlowym, coraz częściej wykorzystuje się nowinki technologiczne. Ślady w dokumentach papierowych stają się śladami elektronicznymi. Przestępstwa takie, jak kradzież i manipulacja danymi wykrywa się każdego dnia. Akty przemocy także poddają się efektom wieku informacji. Poważny atak terrorystyczny może nadejść nie tylko w postaci ciężarówki wyładowanej materiałem wybuchowym, lecz także za pośrednictwem Internetu. Pamiętnik seryjnego mordercy może powstać na dyskietce lub na twardym dysku komputera, zamiast na kartkach zeszytu.



Fot: 1 Pracownicy FBI badający zawartość twardego dysku komputera

Podobnie jak nasza codzienna praca, która stopniowo przechodzi przemianę - od wytwarzania wyrobów do przetwarzania informacji, tak i działalność przestępcza, w znacznej mierze przenosi się do cyberprzestrzeni, w której dowody istnieją wyłącznie w formie elektronicznej, a dochodzenia są przeprowadzane w trybie on-line.

Dziedzina Computer Forensic

Dziedzina computer forensic powstała w celu zaadresowania specyficznych potrzeb wymiaru sprawiedliwości, polegających na maksymalnym wykorzystaniu nowych dowodów elektronicznych. Computer forensic polega na zdobywaniu, zabezpieczaniu, odtwarzaniu i prezentowaniu danych, które zostały przetworzone w sposób elektroniczny i zapisane na nośnikach komputerowych. W dziedzinie sądownictwa, nic od czasów powstania technologii DNA nie miało tak wielkiego wpływu na poszczególne rodzaje śledztw i wyroków, jak badania typu computer forensic.

Computer forensic różni się od większości dyscyplin sądowych. Materiał dowodowy poddawany badaniom i techniki dostępne organom ścigania są produktami sektora prywatnego. Co więcej, w odróżnieniu od tradycyjnych analiz sądowych, zwykle wymaga się, by badanie danych elektronicznych można było przeprowadzić w dowolnej fizycznej lokalizacji, nie tylko w kontrolowanym środowisku laboratoryjnym.

Computer forensic, w odróżnieniu od innych analiz, których wyniki stanowią wnioski podatne na różne interpretacje, dostarcza bezpośrednich informacji i danych, stanowiących dowody o wielkim znaczeniu w każdym postępowaniu. Ten bezpośredni sposób zbierania danych ma szerokie implikacje zarówno dla służb dochodzeniowych i specjalistów sądowych, jak i dla wyników samego badania.

Nowe zasady współpracy

Analizy sądowe miały decydujący wpływ na wyniki niezliczonej ilości dochodzeń. W celu uzyskania jak najwyższego stopnia obiektywizmu i minimalizacji ryzyka stronniczości, analizy te tradycyjnie prowadzone są odrębnie od prac dochodzeniowych. Wykorzystuje się do nich tylko te szczegóły uzyskane w śledztwie, które są konieczne do przeprowadzenia badania. Szczegóły te mogą zawierać możliwe źródła zanieczyszczeń znajdujące się na miejscu zdarzenia lub odciski palców osób niezwiązanych ze śledztwem, które dotykały dowodu. Analizy sądowe opierają się na założeniu, iż raport oparty będzie na obiektywnych wynikach naukowego badania. Cała sprawa, która stanowi przedmiot dochodzenia, może odgrywać niewielką rolę w procesie badawczym. Dla przykładu:

badanie DNA w sprawie dotyczącej gwałtu, może być przeprowadzone bez znajomości nazwiska ofiary, podejrzanego, czy specyficznych okoliczności przestępstwa.

W przeciwieństwie do powyższych przykładów, badania dowodów elektronicznych, by były skuteczne, muszą opierać się na informacjach uzyskanych w trakcie dochodzenia. Przy przeciętnej pojemności komputera PC wynoszącej ok 30GB i systemach, których pojemność często przekracza 60 GB, prawdopodobne jest, że z praktycznego punktu widzenia niemożliwe będzie dogłębne zbadanie każdego pliku przechowywanego na zatrzymanym komputerze. Ponadto, ponieważ komputery są wykorzystywane przez tak szerokie spektrum użytkowników w ramach organizacji, może to rodzić prawne ograniczenia w zakresie przeszukiwania wszystkich plików. Komputery adwokatów lub lekarzy oprócz dowodów przestępstwa mogą zawierać także informacje dotyczące ich klientów lub pacjentów, które są prawnie chronione. Dane przechowywane na głównym serwerze mogą zawierać obciążający e-mail przygotowany przez podejrzanego, lecz także e-mail niewinnej osoby postronnej, która ma prawo do prywatności korespondencji.

Tak, jak trudno byłoby przeskanować każdy plik w systemie komputerowym, tak samo trudno byłoby ekipie śledczej zapoznać się ze wszystkimi informacjami w nich zawartymi. Na przykład, 12 GB wydrukowanego tekstu utworzyłoby plik papieru o wysokości 24 pięter. Z powodów pragmatycznych, analiza computer forensic jest najbardziej skuteczna, gdy ekipie badawczej dostarczy się jak najwięcej informacji dowodowych i szczegółów śledztwa. Na ich podstawie, analityk może stworzyć listę słów kluczowych, służącą wyselekcjonowaniu specyficznych, dowodowych i związanych ze sprawą informacji spośród bardzo dużej grupy plików. Mimo, iż analityk może być osobą uprawnioną do przeszukiwania każdego pliku, ograniczenia czasowe i inne prawne przeszkody mogą na to nie pozwolić. Analiza tego typu powinna ograniczać się w większości przypadków wyłącznie do dobrze zidentyfikowanej informacji dowodowej.

Wyniki analizy

Analizy dowodowe na przestrzeni lat dostarczały ważnych i wiarygodnych rezultatów. Dla przykładu warto przytoczyć analizy DNA, które dostarczały szczegółowych informacji identyfikujących konkretne osoby. Aby wesprzeć ich wyniki, analitycy DNA zebrali

szeroki zakres danych statystycznych na temat profili DNA, na których opierali swe wnioski. Dla porównania, badanie typu computer forensic wybiera lub wytwarza informację. Celem analizy danych elektronicznych jest odszukanie informacji związanych ze sprawą. Aby wesprzeć wyniki badań computer forensic, potrzebne są procedury, które zapewnią, że na nośnikach znajdują się wyłącznie oryginalne informacje, niezmodyfikowane przez proces analityczny. W odróżnieniu od badań DNA czy innych analiz, badania computer forensic nie dają w efekcie stwierdzeń poddających się interpretacji, co do dokładności, wiarygodności, czy znaczenia określonych danych lub informacji.

Poza charakterem materii dowodowej i dostępem do informacji dotyczących sprawy, niezbędnych do efektywnej analizy, istnieje jeszcze jedna istotna różnica między tradycyjnymi badaniami sądowymi, a analizą dowodów elektronicznych. Tradycyjne badania przeprowadzane są w środowisku laboratoryjnym i postępują w sposób logiczny, stopniowo, zgodnie z powszechnie akceptowanymi praktykami. W porównaniu z nimi badania typu computer forensic są niemal całkowicie uzależnione od technologii, przeprowadzane na ogół poza laboratorium, a przebieg analizy w niemal każdym przypadku jest odmienny.

Wspólne cele

Mimo wspomnianych powyżej rozbieżności, zarówno wnioski badawcze płynące z tradycyjnych technik, jak i informacje uzyskane w efekcie analizy computer forensic stanowią istotny element postępowania dowodowego. We wszystkich tych dziedzinach stosuje się te same przepisy i najlepsze praktyki laboratoryjne wykorzystywane w dochodzeniach. Oba rodzaje badań są prezentowane w sądach, oba muszą dawać ważne i wiarygodne rezultaty. W tym celu niezbędne są jak najlepsze procedury i reguły postępowania opracowane zgodnie z zasadami sztuki badawczej.

Dziedzina computer forensic, w odróżnieniu od innych tradycyjnych technik, nie może polegać wyłącznie na uzyskiwaniu podobnych dowodów w każdym przypadku. Na przykład, DNA pochodzące z dowolnego źródła, po oczyszczeniu i zredukowaniu go do podstawowej formy, ma charakter rodzajowy. Od tej pory, reguły postępowania wykorzystywane w analizach DNA mogą być zastosowane we wszystkich sprawach.

Wymiar sprawiedliwości uzyskuje w oparciu o reguły postępowania stosowane w analizach DNA ważne i wiarygodne rezultaty. Z powodów wymienionych poniżej, analizy dowodów elektronicznych rzadko zawierają te same elementy standardowych i powtarzalnych testów:

- Systemy operacyjne, które definiują, czym jest dany komputer i w jaki sposób działa, różnią się w zależności od producenta. Na przykład, techniki wypracowane dla komputerów osobistych wykorzystujących środowisko Windows mogą nie odpowiadać systemom UNIX'owym, które stanowią środowisko wieloużytkownikowe.
- Aplikacje są unikalne.
- Metody składowania danych różnią się zarówno pod względem sprzętowym, jak i rodzajem wykorzystywanych nośników.

Typowe analizy komputerowe muszą uwzględniać dynamicznie zmieniający się i zróżnicowany świat, w którym pracuje każdy analityk computer forensic.

Badanie dowodów elektronicznych

Dowody elektroniczne w postaci przedmiotów materialnych takich, jak układy mikroprocesorowe, płyty, procesory, nośniki danych, monitory i drukarki można opisać łatwo i bezbłędnie jako unikalne formy dowodów materialnych. Rejestracja danych, ich opis, przechowywanie i stan dowodów materialnych są dobrze rozumianymi pojęciami. Laboratoria policyjne posiadają szczegółowe plany opisujące akceptowalne metody postępowania z dowodami materialnymi. Jeśli dowody elektroniczne zawierają element materialny, nie stanowią one wielkiego wyzwania dla analityków. Jednakże, dowód, mimo iż składowany na nośniku fizycznym, jest niewidoczny i istnieje tylko w metafizycznej formie elektronicznej. Wynikiem badania jest odtworzenie tej niewidocznej informacji. Mimo, iż laboratoria computer forensic bardzo dobrze radzą sobie z utrzymaniem integralności przedmiotów materialnych, analizy tego typu wymagają także utrzymania integralności zawartej w nich informacji. Wyzwaniem dla badań computer

forensic jest wypracowanie metod i technik, które dostarczą ważnych i wiarygodnych wyników a jednocześnie ochronią prawdziwe dowody — informację — przed uszkodzeniem.

Aby jeszcze bardziej skomplikować to zagadnienie, dowody elektroniczne prawie nigdy nie istnieją w formie odizolowanej. Informacja stanowiąca dowód jest produktem powstałym z przechowywanych danych, przy udziale aplikacji wykorzystanej do ich stworzenia i systemu komputerowego, który kierował całym procesem. W mniejszym stopniu informacje te stanowią także produkt narzędzi software'owych wykorzystanych w laboratorium do ich wydobycia.

W computer forensic niebagatelne znaczenie ma także gwałtownie zmieniające się środowisko informatyczne. Jednakże, nawet w obliczu tych zmian, agencje wymiaru sprawiedliwości rozumieją potrzebę uniwersalnych rozwiązań i nawołują do stworzenia standardów dla analiz tego typu.

Dla zilustrowania standardów niezbędnych do przeprowadzenia analizy dowodów elektronicznych, posłużymy się przykładem laboratorium, które wymaga, by badania danych dokonywane były (jeśli to tylko możliwe i uzasadnione z praktycznego punktu widzenia) na kopiach oryginalnych dowodów. Wymóg ten stanowi **zasadę** badania. Zasada stanowi logiczną konsekwencję podejścia stosowanego w środowisku badaczy, polegającego na ochronie oryginalnych dowodów przed przypadkowym, czy też nieumyślnym zniszczeniem lub modyfikacją. Zasada ta opiera się na założeniu, iż dowody elektroniczne mogą być z łatwością duplikowane, w celu uzyskania całkowicie zgodnej z oryginałem kopii.

Stworzenie kopii i upewnienie się, że jest ona całkowicie zgodna z oryginałem wymaga zastosowania kolejnego elementu standardu, czyli **obowiązującej polityki i przyjętej praktyki**. Każda agencja wymiaru sprawiedliwości i każdy z badaczy musi każdorazowo podjąć decyzję, w jaki sposób wprowadzić powyższą zasadę w życie. Czynniki, które mają wpływ na tę decyzję to rozmiar zestawu danych, metoda wykorzystana do ich stworzenia i nośnik, na którym są one zapisane. W niektórych przypadkach wystarczy jedynie porównać rozmiar i daty utworzenia plików oryginalnych oraz ich kopii. W innych sytuacjach, konieczne może okazać się zastosowanie bardziej zaawansowanych technicznie

i rygorystycznych pod względem matematycznym technik takich, jak cykliczna kontrola nadmiarowa (cyclical redundancy check - CRC) lub zastosowanie jednokierunkowej funkcji haszującej (message digest - MD).

CRC i MD są algorytmami komputerowymi, które generują unikalne matematyczne reprezentacje danych. Są one kalkulowane dla oryginału i dla kopii a następnie porównywane pod kątem zgodności. Wybór narzędzi wykorzystywanych do tworzenia kopii informacji zależy w znacznej mierze od rodzaju dowodu, z jakim badacz ma do czynienia, niż od polityki obowiązującej w danym laboratorium. Prawdopodobnie specjaliści będą potrzebowali kilku różnych opcji, by móc każdorazowo wykonać to zadanie.

Analitik odpowiedzialny za wykonanie kopii dowodu musi najpierw podjąć decyzję odnośnie wymaganego poziomu weryfikacji, zwłaszcza w przypadku dużych plików i przy napiętych terminach. Matematyczna precyzja i siła tych algorytmów jest zwykle wprost proporcjonalna do czasu wymaganego do przeprowadzenia obliczeń. Jeśli analitik ma milion plików do zduplikowania, o wielkości 1 KB, czas i moc obliczeniowa systemów będą stanowić decydujący czynnik. Okoliczności te spowodują prawdopodobnie wybór szybszego, lecz mniej dokładnego algorytmu.

Po podjęciu decyzji o wyborze najlepszej metody duplikacji, następnym krokiem będzie wykonanie kopii. Zadanie to opisują kolejne elementy standardu, a więc **procedury i techniki**. Procedury muszą być kompletne i zawierać szczegółowe opisy czynności niezbędnych do skopiowania danych, weryfikacji prawidłowego przebiegu operacji i zapewnienia, że uzyskano kopię całkowicie zgodną z oryginałem.

Tradycyjne analizy sądowe takie, jak badania DNA próbek krwi pobranych z miejsca zdarzenia, wypracowały rutynowe i standardowe kroki, które mogą być powtarzane w każdej sprawie. W przypadku analiz computer forensic nie istnieje coś takiego, jak ogólna procedura. Dowód elektroniczny prawdopodobnie będzie zupełnie inny w każdym przypadku i będzie wymagał specjalnie opracowanego planu.

Wnioski

Ważne i wiarygodne metody odtwarzania danych z komputerów, jako dowodów w postępowaniach sądowych, nabierają coraz większego znaczenia w praktyce wymiarów sprawiedliwości na całym świecie. Metody te muszą być na tyle pewne, by umożliwić odtworzenie wszystkich informacji. Muszą one także zapewniać, że oryginalne dowody nie uległy zmianie oraz, że żadne dane nie zostały do nich dodane lub z nich usunięte.