Paweł Odor

Odzyskane dane
rozbitej Columbii, sprawy FBI, zdjęcia Krzysztofa Wielickiego

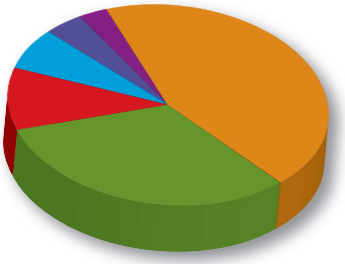
Czarna skrzynka rozbitego wahadłowca Columbia, tysiące spraw dochodzeniowych FBI, wielka powódź w Czechach, ścigani gangsterzy – to przykłady spraw rozwiązanych przez specjalistów odzyskiwania danych tylko w XX wieku, a historia branży *data recovery* sięga 1985 roku. Nie oznacza to, że danych nie próbowano odzyskiwać wcześniej.

Pierwszy przypadek odzyskiwania danych

Najstarszy przypadek utraty danych komputerowych jest związany z odkryciami Charlesa Babbage i Ady Lovelace. W 1833 roku, Babbage rozpoczął prace nad stworzeniem pierwszego komputera. Ten wynalazek, znany jako maszyna analityczna, stał się podstawą konstrukcji współczesnych komputerów.
Jesienią 1841 roku zaprezentował programowalną maszynę liczącą na seminarium we Włoszech. Prezentacją zainteresowała się Ada Lovelace, jeden z najznakomitszych matematyków tamtych czasów. Lovelace i Babbage opracowali system programowania urządzenia przy użyciu kart perforowanych Jacqaurda. Przed jedną z prezentacji maszyny, Babbage nieprawidłowo włożył kartę i uległa ona uszkodzeniu. Odtworzenie zapisanego programu ze zniszczonego nośnika na inną kartę, pomimo wielu prób, okazało się niemożliwe.
Ten pierwszy przypadek utraty danych spowodował, że rozpoczęto udoskonalanie procesu zapisu informacji i poszukiwanie bardziej skutecznych metod, które między innymi umożliwiałyby łatwe odzyskanie danych w przypadku ich utraty.
Wraz z rozwojem technologii zapisu danych powstała cała dziedzina wiedzy zajmująca się odzyskiwaniem utraconych danych.
W przeciwieństwie do pierwszej, nieudanej próby odzyskania danych, dziś w większości przypadków informacje elektroniczne udaje się odzyskać.

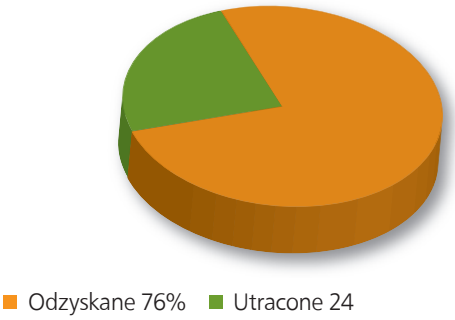
Człowiek – największe zagrożenie danych

21 lat temu trzej amerykanie jako pierwsi na świecie rozpoczęli świadczenie usług odzyskiwania danych zakładając firmę o nazwie Ontrack. Nikt wtedy nie zdawał sobie sprawy, że człowiek stanowi jedno z największych zagrożeń dla danych (rys.1.).



Uszkodzenie fizyczne 44% Błąd człowieka 32% Inne 10% Wirus 7%
Błąd programu 4% Klęska żywiołowa 3%

Pomimo rosnącej liczby zabezpieczeń, udoskonalanych systemów *back-up* z roku na rok tracimy coraz więcej informacji. Do największego w Europie Środkowej i Wschodniej laboratorium odzyskiwania danych zlokalizowanego w Katowicach trafia z roku na rok o 30 procent więcej przypadków. Podczas gdy urządzenia stają się coraz bardziej doskonałe, zawodzi człowiek.
Jednocześnie większość utraconych danych wraca do ich właścicieli. Średnia światowa skuteczność odzyskiwania danych wynosi obecnie 76 procent (rys. 2.).



Data recovery krok po kroku

Jak wynika z doświadczeń specjalistów *data recovery* na całym świecie, 50 procent firm, które utraciły swe strategiczne dane i nie odzyskały ich w ciągu pierwszych dziesięciu dni bankrutuje. Druga połowa ponosi gigantyczne straty. Dlatego firmy odzyskiwania danych muszą działać szybko i sprawnie. W tym celu na przestrzeni lat wypracowały cały proces odzyskiwania danych.

Pierwszy krok

Pierwszy kontakt, zazwyczaj telefoniczny, z firmą świadczącą usługi odzyskiwania danych jest z punktu widzenia kryterium czasu najważniejszy. Prawidłowo przeprowadzona rozmowa wstępna pozwala zdobyć podstawowe informacje.
Do podstawowych pytań zadawanych podczas pierwszej rozmowy należą te o rodzaj nośnika i jego konkretny typ, rodzaj utraconych danych (typy plików), system operacyjny i system plików oraz maksymalny czas, w którym dane powinny zostać odzyskane.
W przypadku uszkodzeń fizycznych nośnika znajomość jego marki i typu pozwala na zdobycie często niestandardowych części, jeszcze przed tym jak trafi on w ręce specjalistów.
Gdy nośnik jest wyjątkowo nietypowy (np. AS 400) dochodzi do tzw. *on-time engineering*, czyli skonstruowania narzędzi do odczytu i napisania oprogramowania specjalnie dla dedykowanego problemu.
Podczas pierwszej rozmowy dowiemy się również jak zabezpieczyć nośnik i przygotować go do transportu lub jak sprawdzić, czy przypadek jest na tyle trudny, że wymaga ingerencji specjalistów. Czasem okazuje się, że wystarczy użyć programu do samodzielnego odzyskiwania danych.

Ekspertyza

Nośnik, który trafia do profesjonalnego laboratorium odzyskiwania danych niezwłocznie poddawany jest ekspertyzie.
Jest ona pierwszym etapem rzeczywistego odzyskiwania danych. Określony zostaje rodzaj uszkodzenia (fizyczne i/lub logiczne), czas potrzebny do przywrócenia utraconych informacji oraz technologia jakiej należy użyć. Specjaliści, w razie potrzeby, usuwają uszkodzenie mechaniczne nośnika, które uniemożliwia zastosowanie narzędzi *software'owych* (Ontrack posiada ich ponad 400), a następnie sporządzają listę plików, które są możliwe do odzyskania. Raport zawierający listę plików jest skomplikowanym dokumentem. Dlatego klienci Ontracka mogą skorzystać z aplikacji Ontrack Verifile (http://www.ontrack.pl/verifile). Umożliwia ona przejrzenie listy plików możliwych do odzyskania.

Odzyskujemy dane w laboratorium

Nośniki produkowane są w sterylnych, niemalże „kosmicznych" warunkach. Każdy przypadek utraty danych spowodowany mechanicznym uszkodzeniem nośnika wymaga ingerencji w jego wewnętrzną strukturę.
W celu zapewnienia maksymalnego bezpieczeństwa danych konieczne jest zachowanie warunków bezwzględnej czystości powietrza. Normą dla dysków twardych jest klasa 100. Urządzeniem pozwalającym zachować tak sterylne warunki w pracy nad otwartym dyskiem jest stanowisko z komorą laminarną (*clean bench*) – (patrz zdjęcie na str. 22).
Dzięki jej zastosowaniu zwiększa się nie tylko prawdopodobieństwo odzyskania danych, ale również żywotność twardego dysku. Praca na otwartym dysku w nieodpowiednich warunkach skraca jego żywotność od 100 do 10 000 razy w zależności od modelu i marki nośnika.
Po wyeliminowaniu uszkodzenia fizycznego nośnika następuje proces zwany obróbką *software'ową*.

Fot. Ontrack

Z użyciem standardowego lub opracowanego specjalnie na potrzeby konkretnego przypadku oprogramowania, dane zostają przywrócone do postaci umożliwiającej ich odczytanie.
W laboratorium Ontracka jako jedynym w tej części Europy właściciele dysków twardych objętych gwarancją nie tracą jej w przypadku utraty danych. Otrzymując certyfikat Ontrack, otrzymują od producentów dysków twardych nowy nośnik. Odzyskane dane z uszkodzonego dysku kopiowane są na wybrany przez klienta nośnik (najczęściej CDR/DVD, a w przypadku gdy ilość danych jest duża, inny dysk twardy lub macierz) i przesyłane do siedzimy firmy będącej właścicielem danych.

I co dalej?

Dla klienta zlecającego usługę odzyskania danych działania związane z *data recovery* kończą się w momencie otrzymania odzyskanych informacji.
Dla profesjonalnej firmy *data recovery* trwają zazwyczaj jeszcze przez 30 dni, kiedy to kopie odzyskanych danych przechowywane są, za zgodą klientów, w laboratoryjnych archiwach zapasowych. Zwiększa to bezpieczeństwo danych i minimalizuje zagrożenie wynikające z konieczności powtórnego odzyskania tych samych informacji, w przypadku uszkodzenia nośników, które dostał klient. Po upływie tego czasu dane są bezpowrotnie usuwane z archiwów.
Wszystkie dane przetwarzane w Ontracku są objęte klauzulą najwyższej poufności i podlegają procedurom stosowanym dla informacji ściśle tajnych.

Przypadki nie zawsze poważne

Choć rzeczywistość specjalistów odzyskiwania danych obfituje w sprawy poważne, często najwyższej rangi, z tysięcy trafiających co roku do Ontrack przypadków, specjaliści wybrali kilka, które zasługują na szczególną uwagę. Od listopada 2004 roku co 12 miesięcy powstaje ranking najbardziej nietypowych przypadków utraty danych. Oto 3 z nich, pozostałe można znaleźć na www.ontrack.pl

AKWARIUM

Podczas wielkiej powodzi w Czechach, we wrześniu 2002 roku, polskie laboratorium Ontracka ratowało dane z zalanych komputerów w Pradze. Zgodnie z upublicznionymi wcześniej poradami odnośnie zabezpieczenia nośnika zalanego wodą nie należy dopuścić do jego wyschnięcia. Bardzo dosłownie potraktował poradę pewien Czech, który wsadził swój dysk do akwarium wypełnionego wodą i w takiej formie dostarczył osobiście nośnik do katowickiego laboratorium odzyskiwania danych Ontrack.

UTRACONE ZDJĘCIA KRZYSZTOFA WIELICKIEGO

Krzysztof Wielicki, wybitny polski himalaista, zdobywca korony Himalajów, podczas swojej ostatniej wyprawy w Himalaje w 2004 roku archiwizował wszystkie zdjęcia cyfrowe oraz nagrania audio na urządzeniu photobank, służącym do archiwizacji danych o dużej pojemności. Photobank przenoszony był przez tragarza w jednym z pakunków. Tragarz, podczas przerwy w marszu, najpierw rozbił urządzenie rzucając na ziemię plecak, a następnie usiadł na tej części plecaka, w której znajdował się photobank. Odzyskane zdjęcia sławnego himalaisty znajdziemy pod adresem www.ontrack.pl/wielicki

LATAJĄCY LAPTOP KSIĘGOWEGO GANGU

W 2003 roku w jednym z dużych polskich miast uciekający przed ścigającymi go policjantami przestępca wbiegł ze swoim komputerem na dach trzypiętrowego budynku. Żeby pozbyć się dowodów przestępstwa zapisanych w komputerze przenośnym zrzucił laptop z dachu budynku na ulicę. Przestępca, prawdopodobnie księgowy gangu, został ujęty, a rozbity komputer trafił do laboratorium Ontracka w Katowicach. Odzyskane dane posłużyły jako dowód w sprawie.

Autor jest głównym specjalistą odzyskiwania danych i computer forensics w firmie Ontrack.