ARTUR SKROUBA

Sygnaturowe odzyskiwanie danych (RAW)

Stopień trudności

Zdarzają się sytuacje, w których po usunięciu, formacie czy też częściowym nadpisaniu danych nie można ich odzyskać w pierwotnej formie za pomocą meta danych zawartych w systemie plików. Niniejszy artykuł przybliży nam tematykę odzyskiwania danych (plików) po sygnaturach (RAW) – czyli ostatnią deskę ratunku w takich sytuacjach…

Z ARTYKUŁU DOWIESZ SIĘ

ogólny zarys – czym są meta dane systemów plików,

czym są sygnatury plików,

kiedy stosuje się odzyskiwanie danych w trybie sygnaturowym (RAW),

odzyskiwanie danych po sygnaturach w praktyce.

CO POWINIENEŚ WIEDZIEĆ

znać podstawy obsługi systemu operacyjnego, w którym pracujesz,

mieć ogólne pojęcie o systemie plików, na którym pracuje twój system operacyjny,

mieć ogólne pojęcie o strukturze i budowie plików.

Na wstępie kilka słów o tym, czym są i jaką rolę spełniają meta dane dyskowych systemów plików.

Każdy system operacyjny komputerów osobistych w celu przechowywania danych zmuszony jest do korzystania z systemów plików (ang. *file system*), który obrazuje sposób i metody przechowywania, adresowania, zapisu i usuwania danych binarnych w postaci plików lub katalogów na nośniku. Mówiąc w skrócie – jest on spisem treści danych, które zawarte są na nośniku pamięci masowej (dysku) oraz bazą jego atrybutów (data utworzenia, modyfikacji, typ, rozmiar, prawa dostępu i modyfikacji, właściciel, lokalizacja itp.) Szczególnym miejscem jest obszar tzw. meta danych (np. plik mft dla systemu NTFS), w którym zdefiniowane są ww. atrybuty.

Dla poszczególnych systemów plików obszary meta danych zdefiniowane są następująco:

- NTFS – jest to mft (ang. *Master File Table*),
- FAT 16/32 – tablica alokacji FAT oraz katalog główny (ang. *Root Directory*),
- Ext2/3 – węzły (ang. *I-node*),
- HFS/+ - MDB (ang. *Master Directory Block),*
- Novell – DET (ang. *Directory Entry Table*).

Uszkodzenie lub zniszczenie takiego obszaru skutkuje brakiem możliwości dotarcia do szukanych plików wraz z ich wszystkimi atrybutami (lokalizacja, struktura, daty, nazwa długość). Ponadto, istnieją przypadki, w których samo usunięcie części danych – katalogów lub plików – częściowo lub całkowicie uniemożliwia odzyskanie tych danych wraz ze strukturą (lokalizacją) oraz kompletem innych atrybutów. Takie utrudnienia występują np. w systemie plików ext3 (nadpisywanie danych adresujących do *inodów* usuniętych struktur), bądź w systemach HFS/+ używanych w platformach firmy Apple.

Czym są sygnatury plików

Każda aplikacja systemu operacyjnego może czytać, przetwarzać i zapisywać dane w postaci plików o ustalonym standardzie – potocznie zwanym typem pliku. W celu oznaczenia typu pliku wprowadzono rozszerzenia, występujące po nazwie i sugerujące z jakim typem mamy do czynienia. Każdy z typów plików posiada swoją własną, indywidualną strukturę, która determinuje sposób kodowania i przechowywania danych w danym pliku. Poza zewnętrznym rozszerzeniem istnieje sygnatura pliku. Jest to ciąg kilku bajtów umieszczony wewnątrz pliku określający jego typ. Na ogół rodzaj sygnatury jest indywidualny dla każdego typu plików.

Budowa sygnatury

Sygnaturę pliku przyjęto określać za pomocą znaków z szesnastkowego systemu liczbowego (heksadecymalnego). Na ogół długość sygnatury wynosi kilka do kilkunastu bajtów. I tak np. plik typu *.jpg* posiada ogólną sygnaturę w postaci 3 bajtów:

`FF D8 FF`

Za pomocą powyżej zdefiniowanej sygnatury będzie można zlokalizować wszystkie rodzaje plików w standardzie *.jpg*. Często użycie dłuższej sygnatury (4 lub więcej bajtów) będzie definiowało już konkretny podtyp pliku *.jpg*, stosowny dla danego producenta jego formatu, np.:

- `FF D8 FF E1` – standard DCF *.jpg* (ang. *Design rule for Camera File system*),
- `FF D8 FF E0` – standard JFIF *.jpg* (ang. *File Interchange Format*).

Warto też wspomnieć, że niektóre podtypy tych samych rozszerzeń plików mogą mieć całkiem inną sygnaturę. I tak np. dla plików typu *.wmf* istnieją dwie sygnatury o całkiem innej budowie:

- `D7 CD C6 9A 00 00` – sygnatura plików *.wmf* używanych przez systemy Windows od 95 wzwyż,
- `01 00 09 00 00 03` – sygnatura plików *.wmf* używanych przez systemy Windows 3.x.

Należy pamiętać, że konkretne sygnatury lub rozszerzenia nie muszą być przypisane do jednego, określonego typu plików. Spotykane są sytuacje, gdzie takie same rozszerzenia mogą oznaczać zupełnie różne typy plików i posiadać różne sygnatury. Także odwrotnie – te same sygnatury mogą być używane przez pliki o różnych rozszerzeniach. Jednak takie sytuacje należą do rzadkości.

Lokalizacja sygnatury – offset

Offset sygnatury jest to wartość liczbowa – zawierająca się w przedziale od 0 do 512 (są wyjątki, gdzie offset może być większy niż 512) i wyraża przesunięcie adresowania pierwszego bajtu sygnatury od pierwszego bajtu w pierwszym sektorze pliku.

Prawie zawsze sygnatura pliku znajduje się w jego pierwszym sektorze. Także w przeważającej większości przypadków zlokalizowana jest ona na samym początku sektora – początek sygnatury znajduje się w pierwszym bajcie pierwszego sektora. W takim przypadku definiowana wartość offsetu przyjmuje wartość 0. Składnia sygnatury w takim przypadku będzie wyglądała następująco:

`0xFFD8FF`

gdzie: 0 oznacza wartość offsetu (sygnatura zaczyna się od 1 bajtu pierwszego sektora), `FFD8FF` – sygnatura dla plików *.jpg*

Rzadziej występują typy plików, których początek sygnatury jest przesunięty o określoną liczbę bajtów. Wtedy składnia takiej sygnatury wygląda następująco:

`4x6D6F6F76`

gdzie: 4 oznacza wartość offsetu, (sygnatura zaczyna się od 4 bajtu pierwszego sektora), `6D6F6F76` – oznacza sygnaturę pliku *.mov* (używanego przez *Quick Time Movie File*).

Offset sygnatury jest cechą indywidualną każdej z sygnatur – jej wartość jest determinowana przez producenta specyfikacji dla danego rodzaju pliku.

Trzeba pamiętać, że niektóre pliki mogą zawierać okresowo występujące wewnętrzne meta dane struktury zawartości, w których można zaobserwować i wyodrębnić powtarzające się cyklicznie tzw. podsygnatury strumieniowe. Taką specyfiką charakteryzują się np. niektóre strumienie AV. Jako przykład można podać format MPEG-2, gdzie na ogół można ustalić występującą periodycznie podsygnaturę (np. w większości standardowych plików typu *.vob* taka podsygnatura występuje co 2048 bajtów).

Dla większości typów plików (tych najbardziej rozpowszechnionych) znalezienie sygnatury nie powinno stanowić większego problemu. Poza tym, prawie wszystkie programy typu Data Recovery (pracujące w trybie RAW) posiadają już wbudowane własne listy sygnatur, po których mogą przeszukiwać nośniki.

Zgoła innym problemem jest określenie sygnatury lub offsetu w nietypowych plikach. Najczęściej są one generowane przez specyficzne urządzenia lub programy autorskie. W takich sytuacjach najprostszym rozwiązaniem jest analiza nagłówków kilku innych plików tego samego typu. Możemy to zrobić za pomocą zwykłego TotalCommandera (F3 i 3 – podgląd heksadecymalny). W ten sposób będziemy mogli porównać zawartość nagłówka pliku i określić sygnaturę. Podobnie ma się sprawa z wartością offsetu – jeżeli znamy już sygnaturę należy zaobserwować jej położenie względem pierwszego bajtu w sektorze.

Stopka pliku

Niektóre typy plików, oprócz charakterystycznego początku (czyli nagłówka, w którym najczęściej zawarta jest sygnatura), posiadają także specyficzne zakończenie pliku, czyli stopkę. Przykładowo do takich rodzajów plików należy plik z rozszerzeniem *.mp4*, który jest standardowym kontenerem AV dla MPEG-4.

Stopkę można zidentyfikować jako charakterystyczny ciąg bajtów znajdujący się na końcu określonego typu plików.

Identyfikacja i lokalizacja stopki może być niezbędna do edycji i naprawy pliku.

Dokładne informacje na temat typów większości spotykanych plików i ich sygnatur można uzyskać pod adresem *www.filext.com*.

Odzyskiwanie danych w trybie sygnaturowym

Ogólnie rzecz ujmując aplikacje, odzyskujące dane, działają według dwóch schematów:

- odtwarzają dane w oparciu o meta dane systemu plików,
- skanują cały obszar dysku i odzyskują *surowe* (RAW) pliki bez użycia meta danych – jest to właśnie odzyskiwanie danych w trybie sygnaturowym.

Oczywiście najlepszą i najwygodniejszą formą jest możliwość odtworzenia danych w oparciu o pierwszą możliwość (np. poprzez odtworzenie zawartości pliku *.mft* dla systemu plików NTFS). Wtedy otrzymujemy kompletny obraz poprzedniej zawartości dysku, wraz ze strukturą, nazwami oraz wszystkim innymi atrybutami (daty, prawa, itp.) Niestety czasami jest to niemożliwe. W momencie, gdy meta dane (systemu plików) są częściowo lub całkowicie uszkodzone dotarcie do danych we wspomnianej formie jest na ogół niemożliwe. Pozostaje tylko tryb sygnaturowy.

Tryb sygnaturowy (RAW)

Odzyskiwanie danych w trybie sygnaturowym to nic innego jak skanowanie całego obszaru nośnika w celu znalezienia i identyfikacji określonych ciągów bajtów (sygnatur). Procedura ta wykonywana jest automatycznie, na zasadzie przeskanowania wszystkich sektorów i odnalezienia jednolitego ciągu bajtów, zaczynających się charakterystyczną sygnaturą. W wyniku skanowania otrzymujemy listę, zawierającą wszystkie pliki posiadające zadaną sygnaturę we wskazanym przez offset miejscu. Charakteryzuje się ona następującymi cechami:

- pliki nie posiadają oryginalnych nazw (przy automatycznym skanowaniu, tzn. przy wykorzystaniu aplikacji typu Data Recovery w trybie RAW pliki są kolejno numerowane, np. 001.doc, 002.doc, itd.),
- pliki nie posiadają praw,
- pliki nie posiadają oryginalnych dat,
- lista zawiera wszystkie pliki, które kiedykolwiek istniały na dysku (czyli razem z plikami istniejącymi, odzyskujemy też pliki, które zostały wcześniej wykasowane oraz częściowo nadpisane).

W zależności od potrzeb, odzyskiwanie danych w trybie RAW powinno być stosowane tam gdzie nie ma innej możliwości dotarcia do danych (np. plik nie jest adresowany przez uszkodzony *.mft*) oraz nie występują inne czynniki mogące stać na przeszkodzie skorzystania z plików odzyskanych w ten sposób. Może mieć to miejsce np. w przypadku potrzeby odtworzenia całych katalogów z plikami powiązanymi ze sobą (np. bazy danych). W takich przypadkach, nie będziemy w stanie odtworzyć poprawnej struktury katalogów, nazw plików i ich lokalizacji.

Sygnaturowe odzyskiwanie danych pofragmentowanych

Kolejną przeszkodą w dotarciu do danych metodą sygnaturową jest fakt istnienia plików, które są pofragmentowane. Generalną zasadą jest to, że danych (czyli plików), które są częściowo lub całkowicie pofragmentowane nie da się odzyskać tą metodą. Dzieje się tak dlatego, że dane dotyczące powiązań i adresowania bloków logicznych (klastrów), które są pofragmentowane znajdują się w meta danych woluminu (np. *.mft*). Dlatego też, samo zeskanowanie obszaru danych, z pominięciem analizy systemu plików nie da nam poprawnych wyników. Odzyskamy pliki, które nie będą się otwierać lub będą otwierały się z błędami.

Poza tym należy pamiętać, że istnieją systemy plików, w których nawet niewinne usunięcie pofragmentowanych danych może sprawiać wiele kłopotów przy próbie ich odzyskania. I to nie tylko w przypadku próby ich odzyskania metodą RAW, lecz także w przypadku analizy meta danych systemu plików. Ma to miejsce np. w przypadku dość jeszcze popularnego FAT16/32, gdzie przy usuwaniu danych zerowane są całe łańcuchy FAT (jest zwalniane miejsce) i odzyskać można poprawnie tylko pierwszy klaster. W takich przypadkach jedyną szansą na odzyskanie sprawnych danych jest posłużenie się metodą kombinowaną (opis w dalszej części).

Odzyskiwanie danych po sygnaturach w praktyce

Przed przystąpieniem do pracy należy zrobić kopię binarną (posektorową) naszego nośnika. Istnieje wiele narzędzi, za pomocą których możemy przeprowadzić taką operację. Jednym z nich jest program ByteBack – oferuje on blokadę zapisu oraz niskopoziomowy dostęp do dysku przez INT 13.

Jako środowisko pracy najlepiej przygotować oddzielny komputer klasy PC z zainstalowanym systemem operacyjnym (min. Win XP SP1 – automatyczna obsługa LBA 48). Oczywiście możemy wykorzystać naszą macierzystą jednostkę (na której doszło do utraty danych) – ale w tym przypadku należy wyjąć z niej nasz dysk i zamienić go innym, na którym zainstalujemy od nowa system operacyjny. Komputer powinien mieć wystarczająco dużo wolnego miejsca na dysku systemowym lub powinniśmy się zaopatrzyć w dodatkowy dysk – na dane które będziemy odzyskiwać. Użycie systemu Windows gwarantuje nam dostęp do dużej ilości aplikacji typu Data Recovery. Z tego też tytułu nasz komputer powinien być podpięty do Internetu.

Po zgromadzeniu wszystkich potrzebnych nam narzędzi możemy rozpocząć pracę. W tym celu podpinamy (wykonaną wcześniej) kopię naszego dysku źródłowego jako dodatkowy (nie systemowy!) dysk w naszej stacji roboczej i uruchamiamy system.

UWAGA! Podczas uruchamiania systemu należy zwrócić uwagę, aby nie doszło do uruchomienia programu Scandisk! Jeżeli zobaczymy taki komunikat – to bezwzględnie należy anulować taką operację (mamy na to 10 sekund).

Po uruchomieniu systemu sprawdzamy, czy dysk z którego będziemy odzyskiwać dane jest widoczny w systemie jako urządzenie fizyczne (ustawienia -> panel sterowania -> menadżer urządzeń -> stacje dysków). Jeżeli tak – to możemy przejść do dalszego etapu jakim jest wybór metody skanowania nośnika.

UWAGA! Jeżeli dysk zawierający kopię naszych danych jest widziany logicznie (jako wolumin) to absolutnie nie wolno wykonywać na nim żadnych operacji zapisu!

Skanowanie automatyczne

Na rynku funkcjonuje wiele narzędzi, które potrafią odzyskiwać automatycznie dane w trybie sygnaturowym. Jednym z najbardziej znanych narzędzi jest program *Recovery My Files*. Program tego typu pozwala na zeskanowanie całego nośnika pod kątem poszukiwań plików zawierających wybrane wcześniej sygnatury. Program może także próbować sam określać długość pliku – jeżeli dla niego takie informacje są osiągalne.

Korzystanie z automatycznych aplikacji zalecane jest w następujących przypadkach:

- szukamy większej ilości plików tego samego typu np. .jpg,
- poszukujemy typy plików powszechnie znanych i rozpowszechnionych,
- nie przewidujemy dalszej obróbki znalezionych plików (pod kątem ich naprawy).

Większość automatycznych aplikacji posiada własne bazy sygnatur najpopularniejszych typów plików. Ponadto niektóre z programów skanujących dają możliwość wprowadzenia własnej, unikalnej sygnatury wraz z wielkością offsetu. Z

takiej możliwości będziemy zmuszeni skorzystać, gdy będziemy poszukiwać nietypowych typów plików.

Case study – klient utracił dostęp do danych poprzez sformatowanie całego 200 GB dysku (system plików ntfs) i postawienie na nowo systemu operacyjnego. Poprzednio miał zajęte ok. 80% dysku. Interesowało go odzyskanie tylko ok. 1000 zdjęć dziecka w formacie *.nef* – objętościowo ok. 10 GB danych. Po przeskanowaniu całego dysku odzyskano 1361 plików – z czego po weryfikacji – sprawnych 952.

Skanowanie manualne

Wybór tej metody jest zalecany w przypadku, gdy szukamy pojedynczych i mało znanych typów plików. Poza tym stosuje się go w przypadku dłuższych plików, zawierających więcej niż jedną sygnaturę, plików tekstowych oraz plików bazodanowych. Do tej metody możemy użyć edytor heksadecymalny np. WinHex. Oferuje on możliwość przeszukiwania nośnika po sygnaturach z możliwością określenia długości znajdowanych sektorów. Posiada możliwość edycji istniejących oraz definiowania nowych, wpisywanych sygnatur wraz z jego offsetem. Poza tym – edytorskie możliwości programu pozwalają na późniejszą obróbkę i naprawę znalezionych plików.

Należą do nich: skanowanie dysku z pominięciem obszarów adresowanych przez system plików, lokalizacja sygnatur, stopek, skład pliku wielosygnaturowego, itp.

Niestety – przy korzystaniu z manualnej aplikacji do odzyskiwania danych w trybie RAW wymagana jest minimalna wiedza na temat budowy plików oraz umiejętność w pracy z danym programem.

Case study – firma dostarczyła dysk z nagraniem uroczystości rodzinnej jednego z klientów. Pojemność dysku 60 GB, system plików FAT. Format szukanych plików – *.mp4* (full HD). Ilość – ok. 60 filmów. Przez błąd użytkownika, dane zostały wykasowane. Dysk był już w innej firmie i odzyskiwanie danych zakończyło się niepowodzeniem. Firma ta odzyskała pliki *.mp4*, które się nie otwierały. Okazało się, że szukane pliki są pofragmentowane, a pliki które wspomniana firma zdołała odzyskać zawierają poprawnie adresowane tylko pierwsze bloki. Analiza struktury plików *.mp4* (plik typu kontener) pozwoliła ustalić występowanie wielu sygnatur. Po zeskanowaniu i wyizolowaniu bloków zawierających poszczególne sygnatury zostały one poskładane do jednego pliku. Na tym etapie film był odzyskany – otwierał się poprawnie – ale jeszcze nie było dźwięku. Pozostało wyodrębnienie (z danych nadmiarowych pliku) ścieżki audio. Odzyskano 56 sprawnych plików z filmami.

Skanowanie RAW – tryb kombinowany

Tryb kombinowany powinien być stosowany tam, gdzie istnieje szansa chociaż częściowego poprawnego odczytu meta danych systemu plików oraz tam, gdzie ze względu na występowanie sporej ilości pofragmentowanych danych jesteśmy zmuszeni oprzeć się chociaż o szczątkowe informacje zawarte w np. *.mft*. Do takich aplikacji należy np. program R-Studio. Aplikacja tego typu skanuje całą powierzchnię dysku oraz jednocześnie analizuje meta dane systemu plików. Wadą takich rozwiązań jest na ogół brak analizy korelacyjnej między wynikami tych trybów

pracy. Dlatego często należy wykonać taką *kombinację* ręcznie. Jako przykład możemy posłużyć następującym case study: pewna firma dostarczyła dysk, z którego został usunięty jeden plik zawierający bazę danych. Na 20 GB dysku – był on zapełniony prawie w całości – znajdowały się dane księgowe i zainstalowany był system Win98 (FAT32). Próby odzyskania pliku zarówno przez aplikację bazującą na analizie FAT, jak i w oparciu o skanowanie sygnaturowe nie przyniosły oczekiwanego rezultatu (silnik bazy danych nie otwierał odzyskiwanego pliku). Oczywistym było, że szukany plik musi być pofragmentowany. Rozwiązanie przyniosło wyizolowanie pierwszego klastra pliku (z sygnaturą) i dopasowanie występujących w następnej kolejności obszarów, które były oznaczone jako wolne (nie adresowane) w tablicy alokacji. Ponieważ posiadaliśmy informację o wielkości szukanego pliku (z *Root Directory*) dopasowanie pozostałych bloków było już tylko kwestią kilku prób.

Podsumowanie

Przy podejmowaniu prób samodzielnego odzyskiwania danych należy pamiętać o kilku podstawowych zasadach:

- przed jakąkolwiek próbą należy wykonać kopię binarną (posektorową) nośnika,
- nie wolno zapisywać jakichkolwiek danych na dysku, z którego dane są odzyskiwane,
- jeżeli musimy odzyskać ważne dane i nie dysponujemy podstawową wiedzą, aby to wykonać – powinniśmy zgłosić się do wyspecjalizowanej firmy.

Profesjonalne usługi odzyskiwania danych wymagają ogromnej wiedzy i specjalistycznego laboratorium. W ostatnim okresie na polskim rynku pojawia się bardzo wiele firm oferujących taką usługę, jednak jej jakość pozostawia wiele do życzenia. W całej tej masie firm jest tylko kilka, które dysponują stosowną wiedzą i warsztatem pozwalającym odzyskać dane we wszystkich możliwych przypadkach (tzn. tam gdzie fizycznie jest to możliwe). Dlatego każdy, kto zechce skorzystać z takiej usługi, powinien bardzo starannie dokonywać wyboru firmy, bądź osoby, której chcemy powierzyć swoje nośniki w celu odzyskania danych. Kuriozalne jest to, że na rynku można spotkać coraz więcej firm lub osób reklamujących się jako jednostki wyspecjalizowane w odzyskiwaniu danych, jednocześnie nie mających gruntownej wiedzy oraz warsztatu pozwalającego na skuteczne wykonanie takiej usługi. I tak, np. światowy średni poziom skuteczności odzyskiwania danych wynosi ok. 76% na 100 zgłoszonych przypadków (źródło: Wikipedia). Jest to spowodowane tym, iż sytuacje takie jak nadpisanie utraconych danych, bądź fizyczne uszkodzenie powierzchni roboczej nośników nie należą do wyjątków. Niestety, coraz częściej można spotkać reklamy, które delikatnie mówiąc … naciągają rzeczywistość. Coraz więcej firm ogłasza się jako ta *najlepsza*, przelicytowując się w skuteczności: 95% czy nawet 99%! Mało tego: na rynku pojawiają się reklamy sugerujące 100% skuteczności (!) w odzyskiwaniu danych czy też mówiące o *gwarancji* na odzyskanie danych. Jest to omamianie zdesperowanego klienta i świadome wprowadzanie go w błąd (powinien się temu przyjrzeć UOKIK). Nie ma bowiem na świecie firmy potrafiącej odzyskiwać dane z każdego przypadku ich utraty. Często działania te mają na celu tylko *złapanie* klienta w celu wyciągnięcia od niego pieniędzy za usługę sprawdzenia, bądź analizy czy się da dane odzyskać, a na końcu stwierdzenia *Niestety nie udało się, ale się napracowałem, więc kliencie zapłać!*.

Jeszcze większą patologią jest funkcjonowanie tzw. *bezpłatnej analizy*, która jest warunkowa. Z grubsza rzecz biorąc, polega to na tym, że coraz więcej firm oferuje bezpłatną analizę nośnika pod warunkiem, że po jej przeprowadzeniu klient skorzysta w danej firmie z usługi odzyskania danych. W przypadku rezygnacji, klient musi pokryć koszty przeprowadzonej analizy oraz inne ukryte opłaty – w przypadku dysków twardych mogą to być kwoty do kilkuset złotych. I nie byłoby w tym nic złego, gdyby nie fakt, że taka praktyka przyczyniła się do rozpowszechnienia się pewnego procederu, a mianowicie: coraz częściej nieuczciwe firmy po wykonaniu analizy decydują się na stosowanie cen zaporowych, np. 30 tysięcy złotych za odzyskanie danych. Jak łatwo przewidzieć – w efekcie klient rezygnuje i z tego tytułu niestety musi zapłacić za wykonaną analizę. Mało tego – niektóre firmy dodatkowo żądają także opłaty za wydanie dysku (nośnika) – ponieważ *wykonały* dodatkową pracę wykraczającą poza standardową analizę wstępną… W tej sytuacji właściciel sprzętu ma związane ręce, ponieważ wcześniej, w momencie przyjęcia dysku do analizy podpisał stosowne zobowiązanie bez dokładnego zapoznania się z nim. Faktycznie – przy takich praktykach teoretyczna skuteczność może osiągać prawie 100% i jeszcze gwarantuje przypływ gotówki w każdym możliwym przypadku. Prowadząc taką firmę, równie dobrze można by nic nie robić – oprócz wystawiania faktur. Wystarczy mieć dobry PR, profesjonalnie wyglądającą stronę WWW czy reprezentacyjną siedzibę.

Dlatego pamiętajmy – przed wyborem firmy odzyskującej dane powinniśmy gruntownie przeanalizować jej rzetelność. Ufajmy tylko sprawdzonym firmom, mogącym się pochwalić wieloletnią praktyką poświadczoną certyfikatami i nagrodami (takimi jak medale, nagrody konsumenckie, poświadczenia dla rzetelnych firm). Także przed oddaniem (lub wysłaniem) nośnika należy zapoznać się z warunkami, które będziemy musieli pisemnie zaakceptować (dokładnie czytajmy druki zamówień i regulaminy). W trakcie rozmowy wstępnej sprawdźmy, czy bezpłatna analiza jest faktycznie bezwarunkowa oraz domagajmy się podania widełek cenowych (chodzi o cenę maksymalną!) za konkretny rodzaj potencjalnego możliwego uszkodzenia, tak aby uniknąć przykrych niespodzianek.

Uwaga

Zarówno autor, jak i redakcja, nie ponoszą żadnej odpowiedzialności za jakiekolwiek szkody i straty powstałe w wyniku stosowanie się do wskazówek w niniejszym artykule. Nie zaleca się stosowania niniejszych metod w warunkach amatorskich, kiedy w grę wchodzi ryzyko utraty danych, mogące stanowić zagrożenie dla życia, zdrowia lub powodujące znaczne straty. W takiej sytuacji należy zwrócić się do wyspecjalizowanych firm typu Data Recovery.

Artur Skrouba
Autor studiował na wydziale Fizyki i Astronomii Uniwersytetu Warszawskiego; jest także absolwentem Szkoły Głównej Handlowej w Warszawie na kierunku Finanse i Bankowość. Na co dzień zajmuje się profesjonalnym odzyskiwaniem danych w firmie DataMax Recovery, w której pełni funkcję jednego z inżynierów technicznych.
Kontakt z autorem: *artur.skrouba@data-max.pl.*