ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2014
Seria: ORGANIZACJA I ZARZĄDZANIE z. 74 Nr kol. 1921

Jacek GRUBER, Ireneusz J. JÓŹWIAK, Dawid KOWALCZYK
Wydział Informatyki i Zarządzania
Politechnika Wrocławska

METODY ODZYSKIWANIA I KASOWANIA DANYCH Z NOŚNIKÓW MAGNETYCZNYCH I NOŚNIKÓW PAMIĘCI FLASH

Streszczenie. Gdy nastąpi uszkodzenie nośnika danych, większość danych można odzyskać za pomocą jednego z wielu programów narzędziowych do odzyskiwania danych. Z drugiej strony, gdy na nośnikach danych przechowywane są dane poufne, to po uszkodzeniu danych lub po awarii nośników danych dane należy z tych nośników skutecznie skasować za pomocą specjalnych programów narzędziowych, a nośniki trzeba zwykle również zniszczyć fizycznie, uniemożliwiając ewentualne próby odzyskania z nich poufnych danych. W artykule porównano programy narzędziowe odzyskiwania i kasowania danych, a także sposoby niszczenia nośników danych.

Słowa kluczowe: utrata danych, program odzyskiwania danych, kasowanie danych, niszczenie nośników danych.

DELETING AND RECOVERING DATA STORED ON MAGNETIC OR FLASH MEDIA

Summary. When media data is damaged, most of the data can be recovered using one of the many utilities for data recovery. On the other hand, when the media data is stored sensitive or secret data, after data corruption or data storage media failure should the media to effectively erase using special utilities and carriers must usually also destroy physically impossible any attempt to recover from their confidential data. In this article we performed a comparison of utilities and recovery, and deleting data, as well as methods of physical destruction of storage media.

Keywords: data loss, data recovery programs, data deleting and erasure, destruction of media data.

1. Wprowadzenie

Większość artykułów mających w tytule „odzyskiwanie danych" dotyczy archiwizowania danych i odzyskiwania danych z utworzonych kopii zapasowych. Kilka artykułów dotyczy firm, które specjalizują się w odzyskiwaniu danych ze zniszczonych napędów [3-9].

Zwiększające się ilości danych na dyskach twardych to problem dotyczący każdego użytkownika komputera, zwłaszcza jeśli jest on podłączony do Internetu. Dane komputerowe są bowiem narażone na różne niebezpieczeństwa. Utrata danych jest chyba najbardziej nieprzyjemną sytuacją dla posiadacza komputera. Przyczyną może być awaria komputera, atak wirusa, przypadkowe skasowanie i wiele innych nieprzewidzianych sytuacji, ale ich rezultaty nieraz bywają katastroficzne. Odzyskiwanie danych jest niekiedy droższe od skutków jakiejkolwiek innej awarii sprzętu komputerowego. Najprostszym sposobem ochrony danych przed ich utratą jest zapobieganie utracie. Awaria może się jednak zdarzyć zawsze. W takich sytuacjach najlepszym rozwiązaniem mogą się okazać programy do odzyskiwania danych. Internet oferuje wiele często darmowych wersji takiego oprogramowania.

Zabezpieczenia danych zgromadzonych w formie elektronicznej są coraz doskonalsze, ale i tak zawsze może dojść do ich utraty [7]. Szanse odzyskania utraconych zapisów elektronicznych są jednak coraz większe. W Katowicach znajduje się jedno z najlepszych na świecie laboratoriów odzyskujących dane ze zniszczonych nośników magnetycznych – Ontrack Odzyskiwanie Danych – polski oddział firmy Kroll Ontrack. Firma nie tylko odzyskuje cenne dane, lecz może także dostarczać elektronicznych środków dowodowych wymiarowi sprawiedliwości.

2. Niszczenie nośników

Nagłówek „Duża liczba darmowych programów do odzyskiwania danych z nośników" sprawia, iż instytucje, które na nośnikach danych przechowują poufne dane, są zmuszone do kasowania ich za pomocą specjalnych programów, a nawet do niszczenia całych nośników [3-5, 7, 8, 10].

Tarnowska firma InfoMark we współpracy z naukowcami z Wrocławia opracowała nową technologię niszczenia nośników danych przez ich degradację w specjalnie dobranej mieszaninie kwasów. Współcześnie stosowane techniki niszczenia zapisu informacji niejawnej są oparte albo na kasowaniu jej z nośnika za pomocą silnych impulsów elektromagnetycznych (degaussery), albo na niszczeniu mechanicznym (zginacze Garner) lub na mechanicznej degradacji przez rozdrabnianie mechaniczne nośnika (niszczarki stosowane

przez ABW). Wszystkie te metody pozostawiają odpady, które mogą być w różnym stopniu podatne na próby odzyskiwania danych dzisiaj lub w przyszłości, zwłaszcza wraz z szybkim postępem technologicznym. Technologia opracowana w Polsce polega na umieszczeniu talerza dysku w mieszance kwasów, a jedyną pozostałością po tym zabiegu jest płyn zawierający roztwór soli glinu z konstrukcji talerza oraz ferromagnetyków tworzących warstwę nośnika. Zatem nie ma mowy o możliwości odzyskania zawartości informacyjnej z tego produktu.

Bardzo często instytucje państwowe nie do końca wiedzą, co robić z nośnikami przeznaczonymi do kasacji. Zapisane na nich informacje w żadnym wypadku nie powinny dostać się w ręce osób nieuprawnionych, jednak w instytucji nie ma warunków do przechowywania nośników wycofanych z użytku. Amatorskich sposobów na uniemożliwienie dotarcia do danych jest wiele. Najpopularniejsze z nich to metoda „na gwoździa", polegająca na przebiciu długim gwoździem całego dysku. Inna, wymagająca nieco więcej wysiłku, to rozłożenie dysku na części i zniszczenie talerzy przez uderzenia młotka.

Dane na cyfrowych nośnikach danych są zapisane w postaci ładunków elektromagnetycznych, dlatego najskuteczniejszą metodą jest po prostu rozmagnesowanie tych urządzeń. Używa się do tego celu urządzenia o nazwie „degausser". Gromadzi on energię elektryczną, zamienia ją na impuls elektromagnetyczny i uwalnia go wokół kasowanego nośnika. Po takiej akcji wszystkie dane zostają bezpowrotnie usunięte. Wystarczy włożyć nośnik w kieszeń i nacisnąć przycisk.

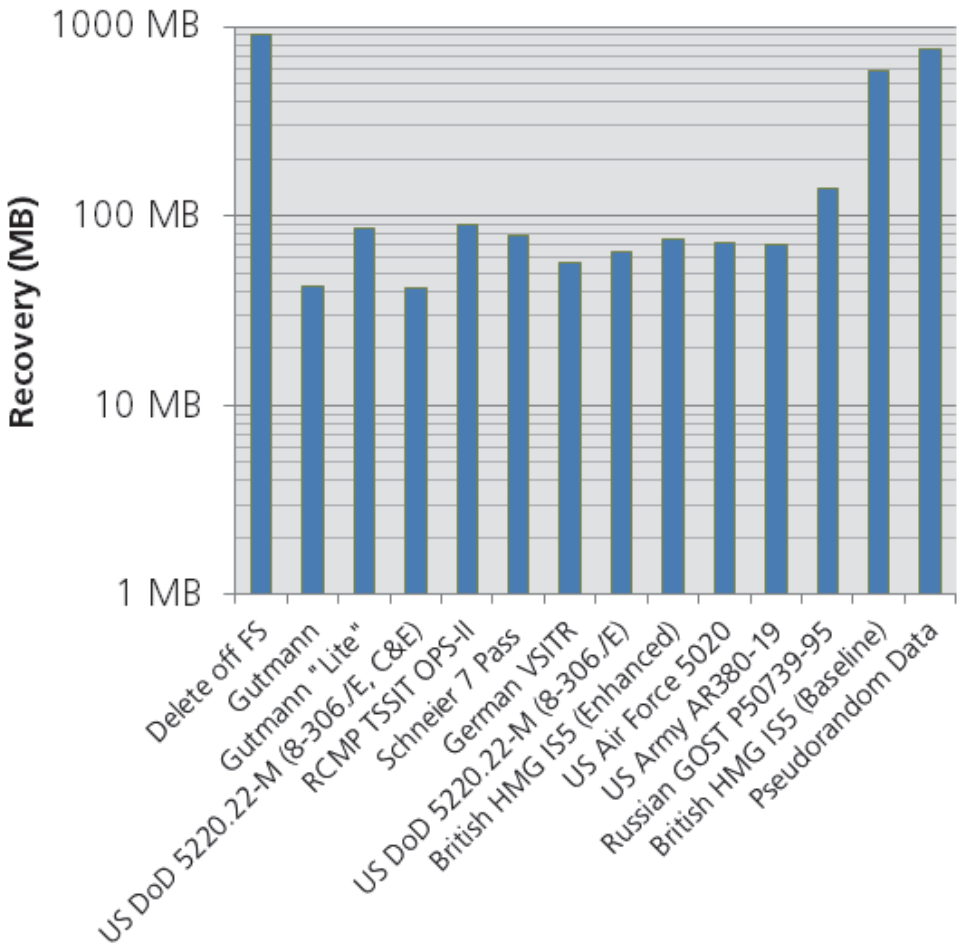
Bardziej popularną metodą stosowaną do niszczenia nośników danych jest stosowanie specjalnych niszczarek, które w sposób fizyczny niszczą dysk. Takie urządzenie niszczy twardy dysk przez zginanie, łamanie elementów napędu. W wyniku zgniatania talerze są wygięte i oddzielone od piasty, obudowa dysku twardego jest pęknięta i płytki drukowane są podzielone. Niszczarka nie korzysta z oprogramowania i jest w stanie zniszczyć wszystkie rodzaje dysków twardych niezależnie od wielkości, systemu operacyjnego lub interfejsu.

Inną równie skuteczną metodą na pozbycie się niepotrzebnych, ale wciąż tajnych danych jest spalenie nośnika. W specjalnie przygotowanym piecu, rozgrzanym do bardzo wysokiej temperatury, umieszcza się dyski twarde. W ten sposób całkowicie pozbywamy się dysku, nie pozostaje po nim żaden element, który może zostać poddany analizie w celu odzyskania danych.

3. Usuwanie danych z dysków SSD

Dyski SSD powoli zdobywają popularność i odbierają rynek HDD [2]. Wciąż są od nich sporo droższe, jednak szybszy transfer danych i większa niezawodność przekonują do tych urządzeń coraz więcej osób. Okazuje się jednak, że SSD mają poważną wadę, która jest

szczególnie ważna dla przedsiębiorstw czy agend rządowych. Bezpieczne usunięcie danych nie jest tak łatwym zadaniem, jak w przypadku dysków twardych starszej generacji. Problemy, na jakie można trafić, chcąc skutecznie usunąć dane z dysków SSD, tak aby nie można było ich odzyskać, są na tyle duże, że nie można stosować metod, które działały w przypadku zwykłych dysków magnetycznych. Bezpieczne usunięcie jednego pliku jest na dyskach SSD prawie niemożliwe [2]. Nawet najbardziej zaawansowane algorytmy nadpisywania mogą pozostawić na dysku do 4% oryginalnych danych.



Rys. 1. Skuteczność różnych algorytmów usuwania danych z dysków SSD
Fig. 1. Complex systems of multi-bottom bore holes drilled from one cluster to many coal seams
Źródło: [1].

Podczas jednego z eksperymentów naukowców z Uniwersytetu Kalifornijskiego wobec plików zastosowano 14 różnych metod usuwania danych (rys. 1). Wykorzystano m.in. algorytmy amerykańskich sił zbrojnych (US DoD 5220.22-M, US Air Force 5020, US Army AR380-19), rosyjski GOST P50739-19, brytyjski HMG ISS, Schneier 7 Pass i inne. Żaden z nich nie usunął pliku całkowicie, pozostawiając na SSD od 10 do 1000 megabajtów informacji.

Użycie degaussera wbrew pozorom nie zniszczy danych na dyskach SSD. Same dyski SSD nie przechowują danych na nośnikach magnetycznych, ale na pamięci typu Flash, lecz

badacze mieli nadzieję, że degausser zniszczy inne elementy elektroniczne dysku, np. chipy. Niestety, dane na żadnym z dysków nie zostały uszkodzone przez degaussera.

Obecny w dyskach SSD firmware, a dokładnie Firmware Translation Layer (FTL), pozwala co prawda na wielokrotne nadpisanie całego dysku danymi, ale jest to procedura zdecydowanie zbyt czasochłonna, ponadto FTL duplikuje pliki na dysku, np. podczas procesu *garbage-collector* (jeden z testowanych plików został odnaleziony w 16 kopiach). Komendy znane z ATA i SCSI, pozwalające na bezpieczne usuwanie danych „ERASE UNIT", były dostępne tylko na 8 z 12 testowanych dysków SSD, a tylko na 4 zakończyły się sukcesem. Jeszcze gorzej sprawa wyglądała z komendą „ERASE UNIT ENH".

Naukowcy z laboratorium systemów nieulotnych pracują teraz nad technikami, które umożliwią dokładne kasowanie danych z SSD. Ostrzegają, że dopóki technologie takie nie zostaną opracowane, właściciele SSD powinni zachowywać szczególną ostrożność podczas pozbywania się dysków wykorzystywanych do przechowywania istotnych danych.

4. Możliwości wykorzystania programu Easy Recovery do odzyskiwania danych

Programy do odzyskiwania danych są to narzędzia specjalistyczne służące do wyszukiwania na nośniku plików, które nie są widoczne przez system. Oprogramowanie tego typu w większości przypadków jest płatne, ale istnieje możliwość skorzystania z darmowych, 30-dniowych wersji demonstracyjnych. Wersje demonstracyjne mają pewne ograniczenia, zazwyczaj jest to brak możliwości kopiowania danych wyszukanych na nośniku. Jednak umożliwiają one w niemal każdym przypadku bezpłatne skanowanie nośnika w celu poszukiwania utraconych danych. Ze względu na dużą liczbę programów użytkowych specjalizujących się w obszarze odzyskiwania danych Autorzy tej pracy zdecydowali się na dokładniejsze sprawdzenie jednego z nich – programu Easy Recovery. Wybór tego programu został podyktowany jego dużą popularnością. W ocenie użytkowników narzędzie to daje duże możliwości w korzystaniu z różnych metod odzyskiwania danych. Ponadto program zawiera inne przydatne funkcje, takie jak diagnostyka dysku, naprawianie niektórych plików z pakietu Microsoft Office, możliwość aktualizacji.

Pliki wykasowane z nośnika w rzeczywistości pozostają na nim, tylko informacja o nich zostaje wykasowana z tablicy alokacji, tak że nie są one widoczne przez system. Podczas formatowania dysku dochodzi do usunięcia tablicy alokacji i zapisania jej na nowo w tym samym lub w innym systemie plików, co powoduje, że pliki nie są widziane przez system. Miejsce, w którym się znajdowały pliki, jest uznawane za puste i jeśli dojdzie do ponownego zapisu, to nowe pliki są umieszczane w pierwszych wolnych sektorach. Jeśli nośnik nie zostanie ponownie zapisany, wówczas można je odzyskać, korzystając z programów do

odzyskiwania danych. Program Easy Recovery to, jak już wspomniano, jedna z najpopularniejszych aplikacji do odzyskiwania danych utraconych w wyniku błędów logicznych na nośniku lub w wyniku błędu użytkownika. W dalszej części artykułu przedstawiono wyniki przeprowadzonych badań skuteczności odzyskiwania danych tym programem w kilku najczęściej przytrafiających się przypadkach utraty danych.

4.1. Wykorzystanie programu Easy Recovery do odzyskiwania danych z dysku twardego

W dysk twardy jest wyposażony każdy komputer. Na nim zazwyczaj instaluje się system operacyjny umożliwiający korzystanie z komputera, jak również przechowuje się dane, z których się najczęściej korzysta. W przypadku odzyskiwania danych z dysku twardego pojawia się problem, który nie dotyczył pamięci Flash (ponieważ jest ona nośnikiem wymiennym), mianowicie nie powinno się odzyskiwać danych na dysku, z którego te dane zostały usunięte, ponieważ może to spowodować nadpisanie utraconych plików. Dotyczy to również instalowania programów na tym dysku, zamykania systemu i wielu innych czynności, których nie powinno się wykonywać w razie utraty.

Do badań użyto dysku zapasowego o pojemności rzeczywistej 1,51 GB, który był podłączony do komputera w tzw. kieszeni. Dysk został sformatowany w systemie plików FAT 32 pod systemem Windows, a w późniejszej części badań korzystano z systemu NTFS. Dysk był wykorzystywany tylko do przenoszenia danych. Program podczas badań będzie próbował odzyskiwać w każdym przypadku te same dane, czyli:

156 zdjęć, kilka zdjęć ma nazwy przyporządkowane przez aparat,
4 filmów nagranych w formacie .AVI z nazwą porządkową z aparatu,
1 film .RMVB,
1 film w formacie .WMA,
1 plik instalacyjny,
1 plik .PDF,
3 pliki .MP3,
41 plików dokumentowych umieszczonych w jednym folderze i w dwóch podfolderach, wśród nich znajduje się 8 plików ukrytych .TMP.

Również dla dysku twardego próby odzyskania danych wykonano po trzy razy. Podczas prób zamodelowano następujące przypadki utraty danych:

pliki usunięte szybkim formatowaniem z partycji FAT 32,
pliki usunięte normalnym formatowaniem z partycji FAT 32,
przypadkowe skasowanie plików z partycji FAT 32,
przypadkowe skasowanie plików z partycji NTFS,
sformatowanie partycji NTFS,
pliki wykasowane z partycji FAT 32 i nadpisane przez nowe dane,

formatowanie programem Partition Magic 8.0 i zmiana systemu na NTFS,
opracowanie partycji, zniszczenie partycji i zmiana systemu plików na FAT 32.

Podczas formatowania dysku z danymi niezależnie od tego, czy skorzystano z szybkiej metody, czy dogłębnego formatowania, wynik odzyskiwania danych metodą Format Recovery był ten sam: odzyskano 70,5% zdjęć, 33,3% filmów i 100% dokumentów. Pozostałych plików nie odzyskano. Zauważono również, że wśród zdjęć i filmów, które zostały odzyskane, brakowało plików zajmujących kolejne miejsca na dysku (końcowe zdjęcia i filmy w folderze). Dodatkowo wszystkie pliki, które były umieszczone poza folderem, zostały utracone. W wyniku odzyskiwania danych metodą Raw Recovery również uzyskano takie same dane zarówno w przypadku formatowania szybkiego, jak i dogłębnego. Dodatkowo odzyskano 1,51 GB danych, co jest równe pojemności całego dysku twardego. Do próby wykorzystano 156 zdjęć, które to zostały odzyskane, jednak 9 z tych zdjęć nie wyświetla kompletnego obrazu. Również zostały odzyskane fragmenty filmów, które były przechowywane na dysku, jednak podobnie jak w przypadku karty Flash również tutaj filmy te zostały podzielone, a części filmów zostały zapisane jako pliki .JPG o bardzo dużej pojemności w porównaniu z innymi zdjęciami (mimo że ich jakość jest słaba). Plik filmowy z rozszerzeniem .RMVB zamienił swój format na .RM i nie był możliwy do odtworzenia w całości. Plik .PDF został odzyskany w całości, jednak nie może być odtworzony. Odzyskano 2 pliki muzyczne .MP3, które poprawnie działały. Wśród dokumentów odzyskano tylko 48,8% poprawnie działających plików. Pliku instalacyjnego nie odzyskano. Odzyskanych danych metodą Raw Recovery było dużo więcej. Znaleziono wśród nich: pliki muzyczne (31 plików .MP3, w tym 30 działających, 4 pliki .MID, w tym 4 działające, 40 .WAV, żaden nie działa), pliki graficzne (190 .JPG, w tym 190 działających, 145 .GIF, w tym 145 działających), pliki instalacyjne (48 plików, w tym 12 działających), pliki dokumentowe (22 działające).

Wśród plików zdjęciowych .JPG znaleziono 29 zdjęć przed ich formatowaniem, które poprawnie działały. Prawie wszystkie pliki .MID i .MP3 dały się odtworzyć w całości, natomiast pliki .WAV nie były możliwe do odtworzenia. Nie było także problemów z uruchomieniem plików graficznych .GIF. Wśród odzyskanych plików instalacyjnych, z czego 12 plików działała poprawnie, nie było możliwości znalezienia pliku, który wykorzystano w badaniu, ponieważ większość plików została podzielona i odzyskana pod inną nazwą.

4.2. Porównanie działania programu Easy Recovery z innymi programami podczas odzyskiwania danych z karty pamięci

Karta pamięci Flash jest najczęściej używana w urządzeniach przenośnych. W badaniach wykorzystano kartę pamięci Secure Digital o pojemności 512 MB (rzeczywista wielkość 488 MB) sformatowaną w systemie FAT 16.

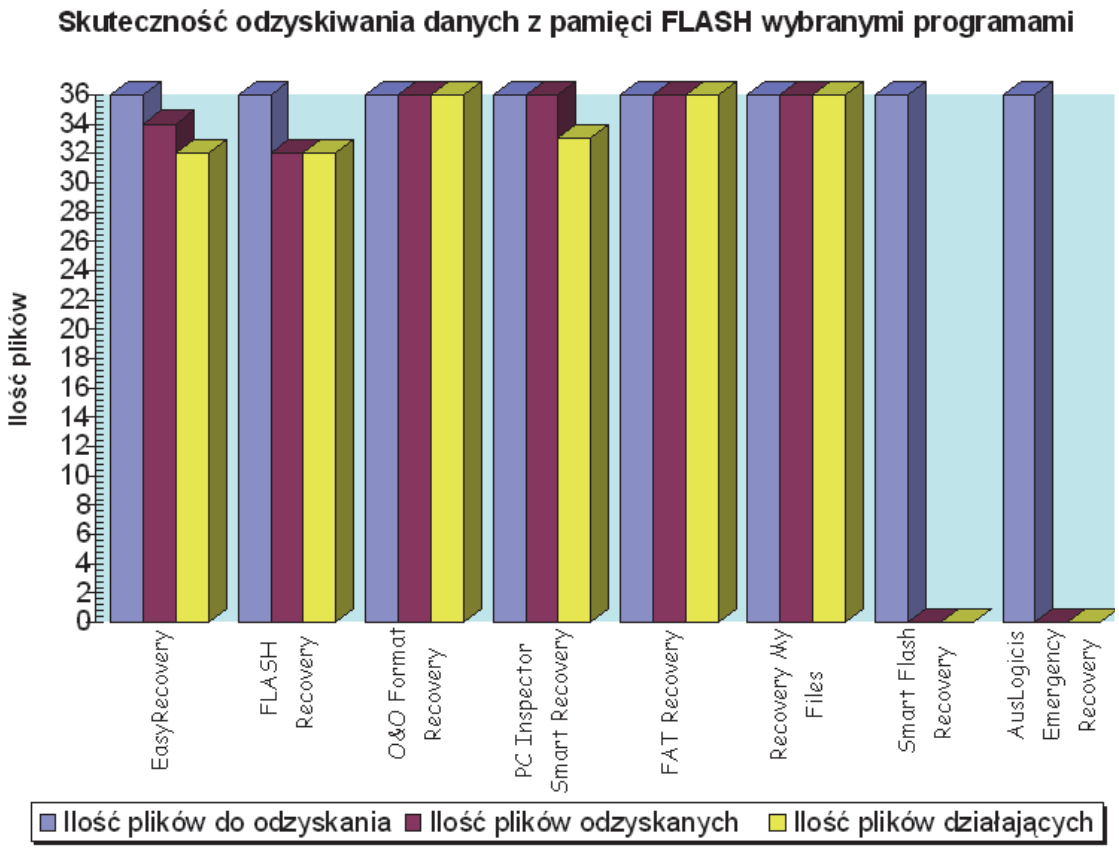
Karta ta jest wykorzystywana do robienia zdjęć oraz nagrywania krótkich filmów aparatem firmy Samsung oraz pełni funkcję pendrive'a do przenoszenia danych i tworzenia kopii zapasowych.

Tabela 1

Podsumowanie wyników odzyskiwania danych z karty

Programy	Liczba utraconych plików	Liczba odzyskanych plików	Liczba działających plików
Easy Recovery	36	34	32
Flash Recovery	36	32	32
O&O Format Recovery	36	36	36
PC Inspector Smart Recovery	36	36	33
FAT Recovery	36	36	36
Recovery My Files	36	36	36
Smart Flash Recovery	36	0	0
AusLogicis Recovery	36	0	0

Źródło: Opracowanie własne.



Rys. 2. Skuteczność odzyskiwania danych z pamięci Flash wybranymi programami
Fig. 2. Complex systems of multi-bottom bore holes drilled from one cluster to many coal seams
Źródło: [1].

Materiał badawczy, który odzyskiwał program, był w każdym przypadku ten sam i obejmował dane w postaci:

- 33 zdjęć zrobionych przez aparat z nazwą przyporządkowaną przez aparat,
- 3 filmów nagranych przez aparat w formacie .AVI z nazwą przyporządkowaną przez aparat.

Podsumowanie wyników odzyskiwania danych za pomocą programu, który podczas badań będzie próbował odzyskiwać w każdym przypadku te same dane, przedstawiono w tabeli 1. Skuteczność odzyskiwania danych z pamięci Flash wybranymi programami przedstawiono na rysunku 2.

5. Wnioski

Celem artykułu było pokazanie, iż utracone lub skasowane dane z nośników można w łatwy sposób odzyskać za pomocą darmowych ogólnodostępnych narzędzi [10]. Artykuł dowodzi zatem, że w celu bezpiecznego usunięcia danych nie wystarczy zwykłe usunięcie danych za pomocą systemu operacyjnego. Dane te należy usunąć przy wykorzystaniu specjalistycznych narzędzi, które wielokrotnie nadpiszą dany sektor nośnika. Nawet wielokrotnie nadpisane dane mogą zostać odzyskane przez analizę ścieżek na talerzu dysku twardego. Głowica dysku nie zawsze idealnie trafia w to samo miejsce, dlatego jest możliwość odczytania poprzednio namagnesowanego obszaru. Te badania pokazują, iż kasowanie naprawdę poufnych informacji wymaga zniszczenia całego nośnika.

Bibliografia

1. Aminian K.: Evaluation of Coalbed Methane Reservoirs. Petroleum & Natural Gas Eng. Dept. West Virginia University, USA 2009.
2. Błoński M.: Z SSD nie można bezpiecznie usunąć danych (20.05.2014), http://kopalniawiedzy.pl/SSD-HDD-bezpieczenstwo-dysk-dane,12552.
3. Czarny P.: Odzyskiwanie danych w praktyce. Wydawnictwo Helion, Gliwice 2002.
4. Krawczyk P.: Nowa polska technologia niszczenia dysków, [w:] IPsec.PL (20.05.2014), http://ipsec.pl/informacja-niejawna/2007/nowa-polska-technologia-niszczenia-dyskow.html.
5. Kuniszewski S.: Przegląd programów do odzyskiwania plików – Dane z odzysku. Czasopismo „Chip” 2002, nr 10, s. 40.

6. Norton Ghost – Podręcznik użytkownika. Opracowanie zbiorowe. Wydawnictwo Symantec, Warszawa 2002.
7. Odzyskiwanie danych, [w:] mydata.pl (20.05.2014), http://mydata.pl/odzyskiwanie-danych.
8. Pawlak M.: Ostatnia deska ratunku. Czasopismo „Chip" 2002, nr 10, s. 22.
9. Preston W.C.: Backup & Recovery. O'Reilly, 2006, p. 42-43.
10. 10 darmowych programów do odzyskiwania danych, [w:] benchmark.pl (20.05.2014), http://www.benchmark.pl/testy_i_recenzje/darmowe-programy-do-odzyskiwania-danych.html.

Abstract

The increasing amount of data on the hard drives of computers poses a serious threat to each user, owner or administrator of the computer, especially if the computer is connected to the Internet. Computer data are in fact exposed to various risks. Data loss is probably the most stressful situation for the user or owner of the computer. The reason for failure can be a virus attack, accidental deletion, and many other unforeseen situation, but the effects of their often tend to be catastrophic. Data recovery is often more expensive than the effects of any other hardware failure.

The easiest way to protect data loss prevention. Failure can always happen, however. In such situations, the best solution may be programs for data recovery.

A comparison of utilities and recovery, and deleting data, as well as methods of physical destruction of storage media is performed in this article.