

Odzyskiwanie danych, czyli jak zaoszczędzić na specjalistycznych usługach.

Tomasz Xięski

2010 r.

1 Wykład część pierwsza

- 1 Kopie zapasowe
- 2 S.M.A.R.T
- 3 Naprawa dysków

2 Wykład część druga

- 1 Fakty i mity odnośnie odzyskiwania danych

3 Wykład część trzecia

- 1 Programy do odzyskiwania danych
- 2 Parę praktycznych porad
- 3 Profesjonalne odzyskiwanie danych

Backup czyli profilaktyka i jeszcze raz profilaktyka

Aby zapobiec utracie danych... **wykonuj regularnie kopie zapasowe!!!**

Metody tworzenia kopii zapasowych:

- **Niestrukturalna** - brak jest określonego sposobu tworzenia kopii i zapisywane jest minimum informacji na temat tego co zostało "skopiowane" a co nie. Przykład: stos płyt z plikami.
- **Pełna** - tworzony jest pełen dokładny obraz dysku/partycji/danych. Gwarantuje najwyższy poziom bezpieczeństwa, ale potrzebuje również dużo miejsca.
- **Przyrostowa** (ang. *incremental*) - zapisywane są jedynie różnice między inną (pełną bądź przyrostową) kopią zapasową. Wymaga najmniej miejsca, ale musimy po kolei odtwarzać wszystkie kopie przyrostowe.
- **Różnicowa** (ang. *differential*) - różnica między ostatnią pełną kopią zapasową.
- **Ciągła ochrona danych** - system ciągle monitoruje wszystkie zmiany dokonane na obszarze objętym ochroną. Nie mylić z RAIDem! Umożliwia ona przywrócenie starych wersji plików.

Czym robić kopie zapasowe?

Rozwiązania darmowe

- Cobian Backup
- FBackup
- DrivelImage XML
- EASEUS Todo Backup
- Paragon Backup & Recovery 10 Free Edition
- Clonezilla

Rozwiązania płatne

- Acronis True Image
- Nero BackItUp & Burn
- Norton Ghost
- Macrium Reflect
- Windows Backup and Restore Center

MS Office też robi kopie zapasowe

Zapisywanie dokumentów

Zapisz pliki w tym formacie:

Dokument programu Word (*.docx)

Zapisz informacje Autoodzyskiwania co 5 min

Lokalizacja pliku Autoodzyskiwania:

C:\Users\Rex\AppData\Roaming\Microsoft\Word\

Domyślna lokalizacja pliku:

C:\Users\Rex\Documents\

Zapisywanie

- Monituj przed zapisaniem szablonu Normal ⓘ
- Zawsze twórz kopię zapasową**
- Kopiuj pliki przechowywane zdalnie na komputer i aktualizuj je podczas zapisywania
- Zezwalaj na zapisywanie w tle

S.M.A.R.T (*Self-Monitoring, Analysis and Reporting Technology*)

- jest to system monitorowania i powiadamiania o błędach działania dysku twardego na podstawie odpowiednich parametrów.

Wszystkie nowoczesne dyski są wyposażone w tą technologię.

Niestety nie jest ona do końca ustandaryzowana, dlatego sposób podawania informacji zależy wyłącznie od producenta dysku. Dlatego też nie należy porównywać parametrów dla dysków różnych producentów bo może prowadzić to do nieporozumień.

Aby odczytać informacje S.M.A.R.T. należy mieć odpowiednie oprogramowanie do tego celu, np. *Active SMART*, *Hard Disk Sentinel*, *smartmontools*, *SpeedFan*, *HdTune*.

Pojedynczy atrybut S.M.A.R.T zawiera:

- **identyfikator (ID)**: numer danego atrybutu
- **nazwa (attribute name)**: nazwa danego atrybutu
- **bieżący (value)**: obecna wartość atrybutu [znormalizowana 0 (źle) - 253 (dobrze)]
- **najgorszy (worst)**: najgorsza zmierzona i zapamiętana wartość danego atrybutu (znormalizowana)
- **próg (threshold)**: najniższa wartość atrybutu ustawiona przez producenta danego dysku
- **wartość RAW (RAW value)**: surowa (odczytana bezpośrednio) wartość danego atrybutu ukazuje obecny stan dysku.

Atrybut jest prawidłowy, gdy jego wartość jest wyższa lub równa z progiem. Jeśli próg jest równy 0 dla jakiegoś atrybutu, to atrybut nie powinien być brany pod uwagę.

Najważniejsze atrybuty S.M.A.R.T.

- **Read Error Rate** - wskaźnik odczytu błędów występujących podczas odczytywania danych z powierzchni dysku. Wartość, która nie równa się zero może oznaczać problemy z powierzchnią dysku, głowicami odczytu/zapisu lub z niezbyt dokładnie umieszczonymi głowicami na ścieżce zapisu. Napędy Seagate często wskazują nieprawidłową (wysoką) wartość.
- **Reallocated Sectors Count** - Liczba ponownie realokowanych (na nowo przydzielonych) sektorów. Im więcej "bad sektorów" tym wydajność dysku mniejsza. Duża wartość nie wróży nic dobrego.
- **Spin Retry Count** - Liczba prób rozpędzenia talerzy dysku (do osiągnięcia normalnej prędkości pracy). Wzrost wartości atrybutu oznacza problemy z podsystemem mechanicznym dysku.
- **End-to-End error** - Atrybut ten oznacza, że po przesłaniu przez bufor danych, ich parzystość nie jest zgodna (pomiędzy kontrolerem a twardym dyskiem).

Najważniejsze atrybuty S.M.A.R.T. c.d.

- **Command Timeout** - Liczba przerwanych operacji z powodu przerw w komunikacji z dyskiem twardym. Wartości większe od zera świadczą o problemach z dostarczaniem zasilania do dysku lub z połączeniami (taśma sygnałowa).
- **Reallocation Event Count** - Wartość atrybutu wskazuje na całkowitą liczbę prób przeniesienia danych z "bad sektorów" do zapasowego obszaru. Liczone są udane jak i nieudane próby.
- **Current Pending Sector Count** - Liczba "niestabilnych" sektorów (oczekujących na ponowne przydzielenie z powodu błędu odczytu).
- **Uncorrectable Sector Count** - Całkowita liczba nekorygowalnych błędów przy zapisywaniu lub odczytywaniu sektora. Wysoka wartość świadczy o problemach z powierzchnią dysku lub innymi związanymi z odczytem.
- **Soft Read Error Rate** - Liczba błędów wynikająca z próby zapisu danych poza ścieżką zapisu.

Jak skuteczny jest S.M.A.R.T?

Należy pamiętać, że S.M.A.R.T. **nie uchroni nas przed wszelkimi** niemożliwymi do przewidzenia **awariami** (nagły dopływ prądu, błędne podłączenie dysku, przegrzanie, uszkodzenia mechaniczne, awaria elektroniki).

Nie należy w pełni ufać programom monitorującym. Podawane wartości mogą być niedokładne (np. temperatura może być podawana z dokładnością do ± 10 stopni), lub na tyle niskie, że nie wywołują alarmu (ostrzeżenia), a jednak powinny być wzięte pod uwagę. Dlatego **należy samemu od czasu do czasu analizować** wszystkie parametry w celu wykrycia potencjalnych problemów.

Niektóre kontrolery/sterowniki twardego dysku nie dostarczają wartości progowych S.M.A.R.T lub wartości te równe są zeru/nieprawidłowe.

Przykład niesprawnego dysku - brak ostrzeżenia?

Info S.M.A.R.T.

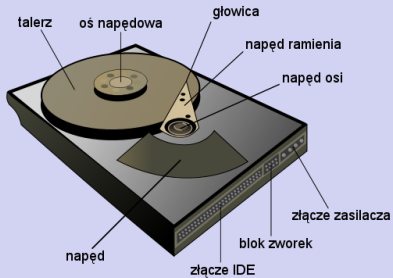
ID	Atrybut	Wartość	Najgorszy	Wartość progowa...	Stan	Nie przetworz...
1	Raw_Read_Error_Rate	100	100	051	OK	3
3	Spin_Up_Time	069	069	011	OK	10030
4	Start_Stop_Count	100	100	000	OK	232
5	Reallocated_Sector_Ct	100	100	010	OK	0
7	Seek_Error_Rate	253	253	051	OK	0
8	Seek_Time_Performance	100	100	015	OK	10641
9	Power_On_Hours	100	100	000	OK	1042
10	Spin_Retry_Count	100	100	051	OK	0
11	Calibration_Retry_Count	100	100	000	OK	0
12	Power_Cycle_Count	100	100	000	OK	10
13	Read_Soft_Error_Rate	100	100	000	OK	2
187	Reported_Uncorrect	100	100	000	OK	2
190	Airflow_Temperature_Cel	080	067	000	OK	3368550
194	Temperature_Celsius	080	065	000	OK	3536322
195	Hardware_ECC_Recovered	100	100	000	OK	496383
196	Reallocated_Event_Count	100	100	000	OK	0
197	Current_Pending_Sector	100	100	000	OK	0
198	Offline_Uncorrectable	100	100	000	OK	1
199	UDMA_CRC_Error_Count	100	100	000	OK	0
200	Multi_Zone_Error_Rate	100	100	000	OK	0
201	Soft_Read_Error_Rate	253	253	000	OK	0

A jeśli musimy jednak dane odzyskać to co?

Istnieją cztery główne **fazy odzyskiwania danych**:

- 1 Napraw dysk doprowadzając go do stanu używalności. Etap ten najczęściej wymaga odpowiednich narzędzi, warunków i umiejętności.
- 2 Zrób kopię sektorów bit po bicie - dostępne są odpowiednie narzędzia programowe jak i sprzętowe. Często stosowana jest tutaj kopia odwrotna (*backwards imaging*).
- 3 Przeprowadź logiczne odzyskiwanie plików i struktur partycji - ten etap jest często wykonywany jako jedyny przez użycie wyspecjalizowanych programów.
- 4 Napraw uszkodzone pliki (które mogły się znajdować w uszkodzonych sektorach) - wyciągnij tyle informacji ile się da.

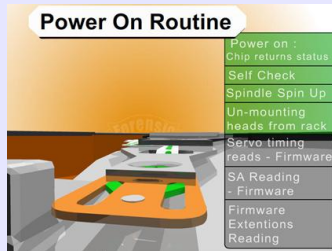
Co w trawie piszczy, czyli dysk od środka



Podłączam go do prądu i...

Sekwencja startu dysku twardego przebiega następująco:

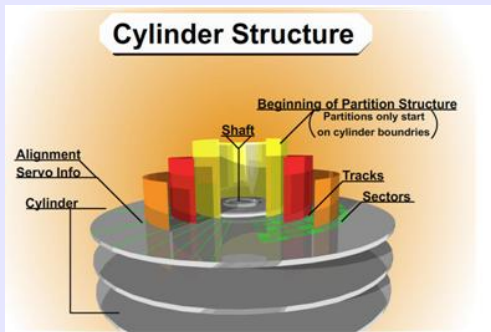
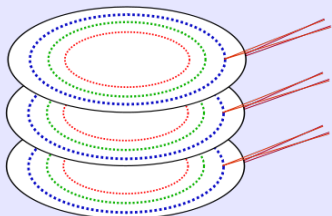
- 1 Wszystkie układy dysku zgłaszają swój status (gotowość).
- 2 Układy przeprowadzają self-check (czy jestem uszkodzony czy sprawny?).
- 3 Talerze zostają wprowadzone w ruch.
- 4 Głowice opuszczają rampę parkującą (o ile jest wystarczający przepływ powietrza).
- 5 Odczytywany jest Servo timing info (informacja o aktualnym położeniu geograficznym głowicy)
- 6 Odczytywany jest obszar SA (System Area) wraz ze wszelkimi potrzebnymi modułami. W przypadku błędu odczytywany jest SA z pozostałych kopii (jeżeli takie są dostępne na dysku).
- 7 Dysk jest gotowy do pracy i przyjmowania komend.



Gdzie są moje dane? Co to CHS?

CHS (ang. Cylinder-Head-Sector, czyli cylinder-głowica-sektor) jest metodą adresowania danych na dysku twardym.

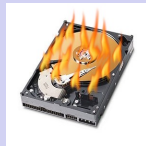
Głowice zazwyczaj znajdują się po obydwu stronach talerza. Każdy talerz podzielony jest na **ścieżki**. Pojedynczy **cylinder** jest natomiast zbiorem ścieżek będących jedna nad drugą (jest ich tyle samo co głowic). Każda ścieżka jest podzielona na **sektory**(bloki). Każdy **sektor** zawiera 512 bajtów.



Wykład część druga - czyli czas na rozluźnienie

A to tylko pierwszy etap odzyskiwania...

Przekazana wiedza stanowi tak naprawdę **wprowadzenie** do **pierwszego** etapu odzyskiwania danych - czyli doprowadzenie dysku do stanu umożliwiającego operacje na nim. Teraz jeszcze musimy przejść przez **trzy** etapy, czyli: wykonanie obrazu dysku, odzyskanie informacji, oraz naprawa uszkodzonych plików. Jest to naprawdę **CIĘŻKA** praca.



Czas trochę odetchnąć...

Pora teraz przedstawić kilka najczęściej spotykanych **faktów** i **mitów** związanych z odzyskiwaniem danych...

Sposób powszechnie znany, który niejednokrotnie jest używany nie tylko w stosunku do dysków twardych. Jeżeli urządzenie źle działa trzeba je przecież “zmotywować” do lepszego działania. Czy więc desperackie “uderz parę razy dysk śrubokrętem” faktycznie działa?

Odpowiedź: Prawie “*działa*”.

Uzasadnienie: Były przypadki, gdy **delikatne pchnięcie** dysku pozwalało rozruszać ramię głowicy, które utknęło przez jakies drobne uszkodzenie.

Czy zatem należy stosować? **NIE**. W nowoczesnych konstrukcjach coraz to bardziej maleje odległość głowicy do talerza dysku (rzędu mikrometrów). Nawet delikatna wibracja może spowodować porysowanie powierzchni talerza, a co za tym idzie często uszkodzenie samej głowicy i nieodwracalne zniszczenie części danych.

Mit 2 - Upuść na podłogę

Bez względu na idiotyczne brzmienie, część forów internetowych do dziś zarzeka się, że upuszczenie dysku na podłogę potrafiło przywrócić go do stanu używalności. Geneza tego mitu jest podobna jak poprzednia. Czy więc ma w sobie ziarno prawdy? Odpowiedź: Absolutnie **NIE**.

Uzasadnienie: Kiedyś uważano, że jeżeli coś się w dysku zatnie (np. motor, głowica, uszkodzone łożysko) to wstrząs spowodowany upadkiem pozwoli te elementy odblokować.

Czy zatem należy stosować? **NIE**. Jest to najprostszy sposób na bardzo poważne uszkodzenie dysku, a tym samym utratę danych. Mit można stosować tylko jeżeli chcemy mieć motywację do kupna nowego dysku :).

Mit 3 - Podgrzej go albo ochłodź

Ten mit jest chyba najpopularniejszy wśród plotek i serwisów społecznościowych. Skoro ma tyle zwolenników czy ma choć ziarno prawdy w sobie?

Odpowiedź: W pewnych przypadkach **może na krótką chwilę przywrócić dysk do życia.**

Uzasadnienie: Na dysku zapisane są dane umożliwiające głowicy ustalenie jej aktualnego położenia i wyszukanie konkretnego sektora danych. W wyniku nadmiernych temperatur metalowe części mogą ulegać rozszerzeniu przez co sektory nieznacznie się przemieszczają. Pod wpływem niskiej temperatury metal się kurczy.

Czy zatem należy stosować? **NIE.** Woda jakie dostaje się do wnętrza dysku po schłodzeniu oraz rozciąganie czy kurczenie sprawia, że elementy i struktura magnetyczna na talerzach często ulega nieodwracalnemu zniszczeniu.

Mit 4 - Otwieranie dysku

Niektórzy twierdzą, że jeżeli zrobimy to dostatecznie ostrożnie, otwarcie dysku nie spowoduje żadnych uszkodzeń. Przecież mamy czyste ręce i wszystko robimy delikatnie. Czy to prawda?

Odpowiedź: Byłoby miło, ale **nie**.

Uzasadnienie: Niesprzyjające warunki atmosferyczne takie jak podniesiona wilgotność czy obecność drobinek kurzu i pyłu w powietrzu są zabójcze dla dysku. Dlatego też są one szczelnie opakowane, tak by nie przedostawały się do ich wnętrza wspomniane drobiny.

Czy zatem należy stosować? **NIE**. Dysk można jedynie otwierać przy użyciu wyspecjalizowanych narzędzi i w pomieszczeniu klasy 100 (tzw. Clean Room Class 100)-pomieszczenie, gdzie jest maksymalnie 100 cząsteczek kurzu (nie większych niż 0.5 mikrona) na $30,48\text{cm}^3$ powietrza..

Mit 5 - Wymiana płytki drukowanej (PCB)

Jeżeli podejrzewamy problem z elektroniką dysku to wymiana płytki drukowanej na inną ze sprawnego dysku z tej samej serii może przywrócić dysk do sprawności.

Odpowiedź: **W pewnych przypadkach tak.**

Uzasadnienie: Jeżeli odpowiednio dobierzmy elektronikę (tak by była jak najbardziej zbliżona do naszego uszkodzonego dysku) to jest szansa, że problem zostanie wyeliminowany.

Czy zatem należy stosować? **Tylko i wyłącznie jeżeli ma się doświadczenie i wymaganą wiedzę.** Nie wystarczy zamienić płytki na tą z tego samego modelu dysku. Może to prowadzić nawet do jego uszkodzenia. Jest wiele czynników, które muszą się zgadzać, by taka wymiana mogła zostać przeprowadzona (jak zgodność odpowiednich cyfr numeru seryjnego, wersji mikro kodu itp).

Mit 6 - Oprogramowanie do odzysku danych

Niektórzy twierdzą, iż stosowanie programów do odzyskiwania danych nie rodzi żadnej szkody dla danych i kondycji dysku. Czy jest to zawsze prawda?

Odpowiedź: **Nie zawsze.**

Uzasadnienie: Jeżeli mamy do czynienia z uszkodzeniem wyłącznie logicznym (błąd systemu plików, przypadkowe skasowanie partycji) to jak najbardziej możemy sami spróbować odzyskać dane. Jeżeli mamy do czynienia z uszkodzeniem fizycznym, takie programy mogą je pogorszyć.

Czy zatem należy stosować? **Tylko i wyłącznie jeżeli ma się doświadczenie i wymaganą wiedzę.** Programy bardzo często skanują cały dysk w poszukiwaniu pozostałości po danych. Jeżeli mamy uszkodzoną głowicę lub jeśli najedzie ona na uszkodzony obszar dysku istnieje duże prawdopodobieństwo, że pogorszymy tylko stan techniczny dysku.

Darmowe

- Recuva
- PC INSPECTOR File Recovery
- Glary Undelete
- EASEUS Deleted File Recovery
- BulletProof File Copy
- TestDisk & PhotoRec

Płatne

- Active@ Partition Recovery
- GetDataBack
- Ontrack EasyRecovery
- Recover My Files
- Stellar Phoenix Windows/Linux/Mac Data Recovery

Kilka porad, które mogą zmniejszyć skutki awarii dysku i utraty danych:

- 1 Pamiętaj o regularnym robieniu **kopii zapasowych** - profilaktyka najlepszą obroną!
- 2 Jeżeli bezpieczeństwo danych jest priorytetem zainwestuj w macierz dyskową **RAID 1** (*Mirroring*).
- 3 Monitoruj regularnie parametry **S.M.A.R.T.**
- 4 Zadbaj o dobrą wentylację komputera - elektronika nie lubi nadmiernego ciepła.
- 5 Jeżeli już musisz odzyskiwać dane - rób to z głową! Pamiętaj, że każde podłączenie dysku do zasilania (i próby odczytu/zapisu) zmniejszają szanse na odzyskiwanie większej liczby danych. Bądź przygotowany.
- 6 Jeżeli uszkodzenie przekracza Twoją wiedzę, doświadczenie, czy umiejętności zaufaj specjalistom. Korzystaj z usług renomowanych firm zajmujących się DR(odzyskiwaniem danych).

Lista firm:

- Stream Data - <http://www.odzyskiwaniedanych.info.pl/>
- Kroll Ontrack - <http://www.krollontrack.pl/>
- MiP Data Recovery - <http://www.odzyskiwaniedanych.net/>
- DataLab - <http://www.datalab.pl>
- DABI Sp. z o.o. - <http://www.dabi.pl>

Jak wybrać dobrą firmę?

- Liczba oddziałów
- Referencje
- Jasno podane sposoby kontaktu i wysyłki
- Wykonanie i treść zawarta na stronie internetowej

Dziękuję za uwagę!

Czy są jakieś pytania?

Tomasz Xięski

e-mail: tomasz.xieski@us.edu.pl