

# Tytuł szkolenia: Odzyskiwanie danych z dysków twardych

## Kod szkolenia: Odzyskiwanie danych

### Wprowadzenie

Dane cyfrowe odgrywają coraz większą rolę w działaniach biznesu, funkcjonowaniu służb publicznych i w życiu prywatnym. Bardzo często nie są one już w żaden sposób przechowywane w postaci papierowej. Nie zawsze są też dostatecznie zabezpieczone przed ich utratą. Kopia zapasowa – o ile w ogóle jest wykonywana – nierzadko okazuje się uszkodzona lub zbyt nieaktualna, by mogła z powodzeniem zastąpić utraconą informację. W pogoni za oczekiwaniami rynku, także przy produkcji nośników danych, producenci poszukują oszczędności i balansują na granicy możliwości fizycznych. Zwiększanie pojemności i wydajności przy jednoczesnym obniżaniu kosztów musi skutkować wzrostem awaryjności. Współcześnie wiele modeli dysków twardych nie mogłoby przetrwać okresu gwarancyjnego, gdyby nie zaszyte w oprogramowaniu układowym algorytmy korekcji błędów oraz zarządzania defektami powierzchni. Ale złożone oprogramowanie układowe zarządzające dyskiem samo w sobie nie jest niezawodne i jego problemy stały się osobną kategorią coraz popularniejszych usterek. Nawet jeśli sam dysk się nie zepsuje, dane mogą zostać utracone w wyniku ludzkich pomyłek, błędów systemowych, infekcji złośliwym oprogramowaniem, a także celowych działań, które z mniejszą lub większą skutecznością mogą te informacje uszkodzić. **Odzyskiwanie danych jest sztuką ratowania tego, co w danej sytuacji jest możliwe do uratowania.** Wymaga ostrożności w postępowaniu i adekwatności podejmowanych działań, tak, by nie doprowadzić do pogorszenia stanu nośnika i jego zawartości. Dlatego tak istotne znaczenie ma zrozumienie budowy i zasad funkcjonowania dysków twardych oraz umiejętność przeprowadzenia diagnostyki przed podjęciem działań, których skutki mogą być nieodwracalne.

### Adresaci szkolenia

Szkolenie adresowane jest do techników serwisów komputerowych, informatyków śledczych, techników kryminalistycznych, funkcjonariuszy służb policyjnych, administratorów systemów, osób odpowiedzialnych za reakcję na awarię infrastruktury IT, nauczycieli informatyki.

## Cel szkolenia

### Celem szkolenia jest zapoznanie uczestników z:

- dyskiem twardym, jego budową i funkcjonowaniem,
- przechowywaniem i organizacją danych w ujęciu fizycznym i logicznym,
- przyczynami awarii i utraty danych,
- narzędziami wykorzystywanymi w odzyskiwaniu danych,
- podstawami diagnostyki dysków twardych,
- podstawowymi metodami postępowania w przypadku różnych typów uszkodzeń oraz przygotowanie ich do dalszej nauki w zakresie odzyskiwania danych.

### Po szkoleniu uczestnik będzie:

- rozumiał, jak jest zbudowany i jak działa dysk twardy,
- odróżniał adresację na poziomie fizycznym, LBA i struktur logicznych,
- potrafił zminimalizować ryzyko pogorszenia stanu dysku i jego zawartości,
- potrafił zidentyfikować protokół komunikacyjny, typ magistrali i rodzaj złącza
- dobrać odpowiednią przejściówkę do podłączenia dowolnego dysku,
- umiał przeprowadzić podstawową diagnostykę, zinterpretować jej wyniki
- umiał identyfikować najpopularniejsze usterki,
- rozumiał zasady działania oprogramowania do odzyskiwania danych,
- potrafił wykonać pełną lub częściową kopię posektorową,
- potrafił poprawnie zidentyfikować model dysku
- potrafił dobrać dawcę podzespołów,
- umiał wykonać podstawowe naprawy PCB oraz przysposobić PCB dawcy,
- potrafił realnie ocenić swoje umiejętności
- potrafił powstrzymać się od działań, do których jeszcze nie jest przygotowany,
- wiedział, jak samodzielnie może rozwijać umiejętności manualne w zakresie mechaniki dysków twardych,
- znał ogólny model architektury oprogramowania układowego dysków twardych,
- umiał ograniczyć pojemność dysku twardego i usunąć takie ograniczenie,
- potrafił skomunikować się z dyskiem przez terminal szeregowy.

## Czas i forma szkolenia

- 35 godzin (5 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

## Plan szkolenia

### 1. Podstawowe zagadnienia związane z budową dysków twardych ich funkcjonowaniem i usterkami

- Zarys rozwoju technologii dysków twardych, ważniejsze zmiany technologiczne, stan badań
- Podłączenie dysku twardego do komputera. Standardy i protokoły komunikacyjne, typy magistral, rodzaje złącz
- Ogólny schemat budowy dysku twardego
- Podstawy fizyki zapisu magnetycznego. Zapis równoległy i prostopadły
- Autopsja dysku twardego z omówieniem poszczególnych elementów i ich roli w przechowywaniu danych
- Ogólny model architektury oprogramowania układowego dysków twardych
- Organizacja danych na dysku twardym. Poziomy adresacji. Podsystem translacji adresów logicznych na fizyczne
- Zarządzanie defektami. Rola list defektów w podsystemie translacji
- Podstawy serwomechanizmu. Sektory serwo, śledzenie ścieżki, sygnał błędu pozycjonowania
- Technologia SMR. Media Cache i dwupoziomowy system translacji.
- Sekwencja startowa dysku twardego.

## 2. Najczęściej pojawiające się problemy w odzyskiwaniu danych

- Problemy logiczne i fizyczne
- Struktury logiczne i ich rola w dostępie do danych. Adresacja na poziomie logicznym. Proces lokalizacji i odczytu plików
- Najczęstsze przyczyny i objawy wystąpienia problemów logicznych.
- Automatyczna naprawa uszkodzonych struktur logicznych i jej konsekwencje dla możliwości odzyskiwania danych
- Ataki złośliwego oprogramowania, szyfrowanie danych
- Logiczne zespoły złożone z wielu dysków – podstawowe informacje o macierzach RAID
- Najczęstsze błędy i problemy związane z macierzami RAID
- Degradacja i defekty powierzchni magnetycznej. Wpływ prądu zasilającego oraz czynników środowiskowych na pracę dysku twardego
- Uszkodzenia elektryczne i elektroniczne
- Skutki zalania i korozji
- Uszkodzenia mechaniczne. Najczęstsze przyczyny i mechanizm powstawania usterek
- Uszkodzenia oprogramowania układowego. Związek usterek oprogramowania układowego z architekturą i stanem technicznym dysku
- Wpływ uszkodzeń fizycznych na stan struktur logicznych
- Wpływ celowych uszkodzeń i zdarzeń losowych na stan techniczny dysku.
- Programowe i sprzętowe metody nieodwracalnego usuwania danych oraz ich skuteczność
- Wstępna wizualna analiza dysku
- Uruchomienie dysku. Znaczenie diagnostyczne odgłosów
- Znaczenie diagnostyczne paszportu dysku i błędów detekcji
- Metody wstępnego odróżniania kategorii uszkodzeń

## 3. Przegląd oprogramowania i urządzeń do odzyskiwania danych

- Podstawowe programy diagnostyczne i ich wykorzystanie
- Skanowanie powierzchni i interpretacja wyników
- Rejestr stanu i rejestr błędów oraz ich znaczenie w diagnostyce dysków twardech
- Uszkodzone sektory i ich rodzaje
- Zerowanie i remapowanie jako procedury naprawcze i ich wpływ na możliwości odzyskania danych
- Analiza SMART i jej wartość diagnostyczna
- Ogólne zasady działania programów do odzyskiwania danych
- Wybrane przykłady prostych programów do odzyskiwania danych
- Zaawansowane programy do pracy ze strukturami logicznymi
- Hex-edytory i jego wykorzystanie w odzyskiwaniu danych, możliwości bezpośredniej edycji nośnika
- Zabezpieczanie danych na drugim nośniku. Kopia posektorowa, a kopia zapasowa i obraz systemu. Blokery sprzętowe. Możliwości logicznego ukrycia dysku przed systemem operacyjnym
- Koncept mapy. Możliwości wykonania częściowej kopii posektorowej i mapowania wybranych plików
- Podstawowe narzędzia ręczne. Ochrona ESD
- Terminal szeregowy i jego przeznaczenie.
- Zaawansowane rozwiązania sprzętowe – programowe do pracy z uszkodzonymi dyskami
- Komora laminarna, jako niezbędny element czystego środowiska do ingerencji w podsystem mechaniczny dysków twardech
- Narzędzia do ingerencji w podsystem mechaniczny dysków twardech
- Przykłady rozwiązań dedykowanych i uniwersalnych
- Podstawowe informacje o urządzeniach wykorzystywanych w laboratoriach fabrycznych i naukowych

## 4. Dobór elementów do naprawy dysków

- Prawidłowa identyfikacja dysku. Marka handlowa, a model techniczny
- Schematy oznaczeń modeli stosowane przez producentów
- Rodziny modeli
- Kryteria doboru PCB
- Możliwość podstawienia PCB bez zintegrowanego mostka USB-SATA
- Podstawowe kryteria doboru dawców głowic

- Oznaczenia kodowe stosowane przez producentów
- Postępowanie w przypadku braku odpowiedniego dawcy. Dobór dawcy głowic w kategoriach prawdopodobieństwa

#### **5. Naprawa elektroniki**

- Diagnostyka uszkodzeń elektroniki
- Utlenienie i zasiarczenie kontaktów
- Elementy zabezpieczające i ich uszkodzenia
- Uszkodzenia sterownika silnika
- Mostki szyfrujące i rozwiązywanie związanych z nimi problemów
- Identyfikowanie i wymiana uszkodzonych elementów
- Przystosowanie PCB dawcy

#### **6. Wymiana głowic i talerzy w dyskach**

- Przygotowanie do pracy w komorze laminarnej, człowiek, jako źródło zanieczyszczeń
- Przygotowanie pacjenta i dawcy do rozebrania, dobór narzędzi
- Podstawy pracy w komorze laminarnej, ergonomia, zalecenia eksploatacyjne
- Kolejność demontażu podzespołów
- Magnesy stałe i mechaniczne ograniczniki wychYLENIA bloku głowic magnetycznych
- Sposoby parkowania głowic. Demontaż i montaż bloku głowic magnetycznych
- Sposób postępowania w przypadku zaparkowania głowic na powierzchni talerza
- Zablokowanie silnika
- Zanieczyszczenia powierzchni talerzy i sposoby ich usuwania
- Zarysowania talerzy, zapiły, przykłady zeszlifowanej powierzchni

#### **7. Rozwiązywanie problemów z firmware dysków**

- Klasyfikacja modułów oprogramowania układowego ze względu na znaczenie dla uruchomienia dysku i uzyskania dostępu do danych
- Moduły zamienne i unikatowe dla danego dysku oraz ich rola w dostępie do danych
- Najczęstsze problemy oprogramowania układowego i ich przyczyny
- HPA, jako metoda ograniczania pojemności nośnika i ukrywania danych
- Podsystem bezpieczeństwa, hasła ATA,
- Proces automatycznej realokacji uszkodzonych sektorów, a problem listy relo w dyskach WD
- Wprowadzenie do użycia terminala szeregowego w diagnostyce i naprawie dysków Seagate
- Wyprowadzenie ze stanu zajętości, identyfikacja ścieżek kanału odczytu
- Test głowic
- Odczyt i kasowanie SMART
- Odczyt wybranych plików systemowych strefy serwisowej
- Problem tzw. Czarnej serii (muchy CC)

#### **8. Zajęcia praktyczne / ćwiczenia**

- W przeplacie z częścią teoretyczną dotyczącą poszczególnych zagadnień
- Diagnostyka losowych usterek