Laboratorium 7

Narzędzia dyskowe i plikowe

W pakiecie Sysinternals Windows dostępnych jest kilka narzędzi monitorujących działania przeprowadzane na dyskach oraz plikach (do pracy przy laboratorium pobierz plik nd.zip).

Pierwszym narzędziem jakie zostanie opisane jest **AccessChk**. Aplikacja przeznaczona jest dla administratorów systemu Windows. Narzędzie pokazuje dostęp poszczególnych użytkowników lub grup użytkowników do plików, folderów, rejestru oraz usług systemowych. Jednym słowem aplikacja rozszerza informacje dotyczące zabezpieczeń sytemu. Program działa w trybie tekstowym, a poszczególne polecenia należy wywoływać w następujący sposób:

```
accesschk [-s][-e][-u][-r][-w][-n][-v][[-k][-p [-f]][-o [-t <object
type>]][-c]|[-d]] [username] <file, directory, registry key, process,
service, object>
```

Przykład zastosowania:

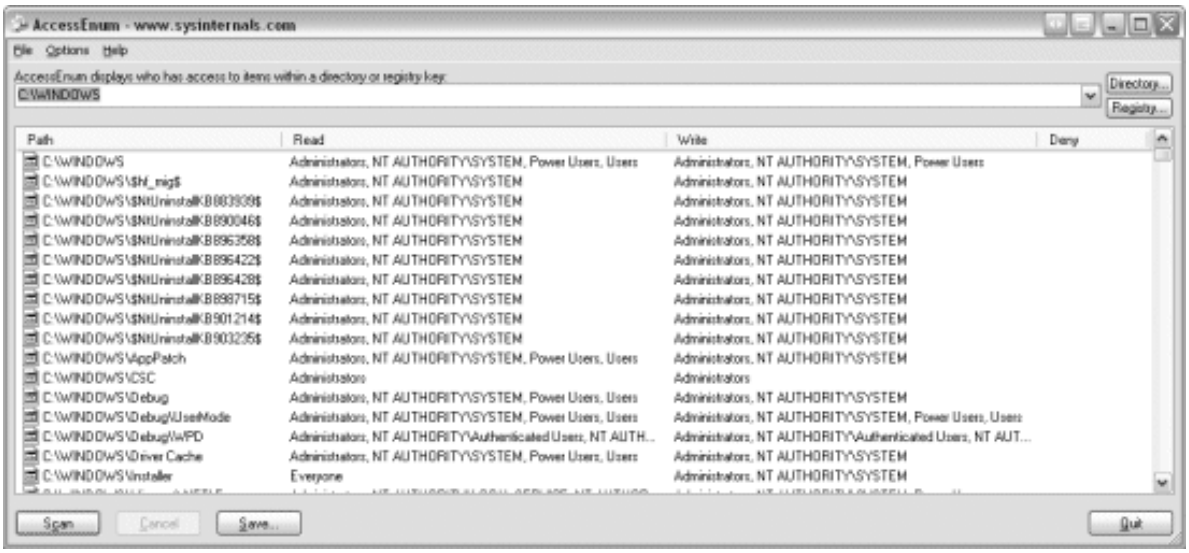
```
accesschk -wuo everyone \basednamedobjects
```

Powyższą komendę należy wpisać, aby zobaczyć wszystkie obiekty, które mogą modyfikować wszyscy użytkownicy systemu komputerowego.

```
accesschk "power users" c:\windows\system32
```

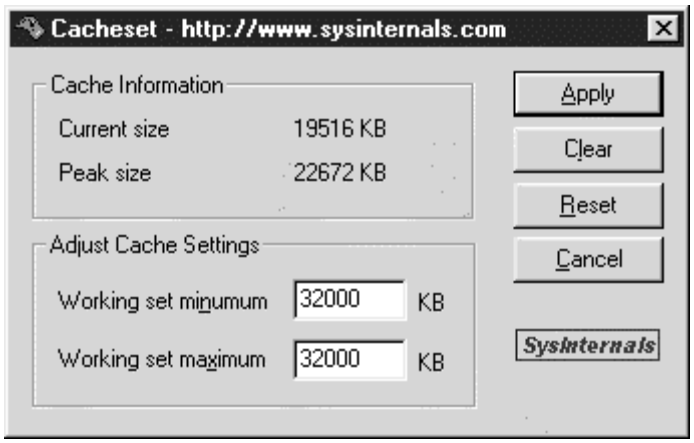
Komenda ta wyświetla raport o dostępności administratora systemu do plików i ustawień w folderze \Windows\System32.

Kolejnym narzędziem plikowym i dyskowym jest **AccessEnum**, dzięki któremu możliwe jest błyskawiczne sprawdzenie uprawnień dotyczących poszczególnych plików czy kluczy rejestru. Jeżeli na przykład zdarzy się, że do pewnych katalogów mają dostęp wszyscy użytkownicy bez względu na uprawnienia, będzie to podstawa do wszczęcia dochodzenia. **AccessEnum** pozwala nie tylko na sprawdzenie uprawnień, lecz również porównanie aktualnego stanu systemu z zapisanym tuz po instalacji systemu. Za pomocą tej aplikacji możliwe jest również dokładnie sprawdzenie, jakie modyfikacje w systemie wprowadza każda nowa zainstalowana aplikacja, w tym na przykład te, które zawierają spyware. Rys. 1 przedstawia działanie narzędzia AccessEnum



Rys. 1. Narzędzie AccessEnum

Narzędziem pozwalającym manipulować pamięcią podręczną (cache) dla operacji dyskowych jest **CacheSet.** Aplikacja ta pokazuje obecny rozmiar pamięci cache i największy do tej pory osiągnięty rozmiar tejże pamięci. Program umożliwia również ustawienie minimum i maksimum dla tego rodzaju pamięci. Wprowadzone zmiany odnoszą natychmiastowy skutek. Narzędzie możne posłużyć do dostrojenia serwera Windows NT w celu uzyskania lepszej wydajności pracy. Na rysunku 2 przedstawiono narzędzie CacheSet.

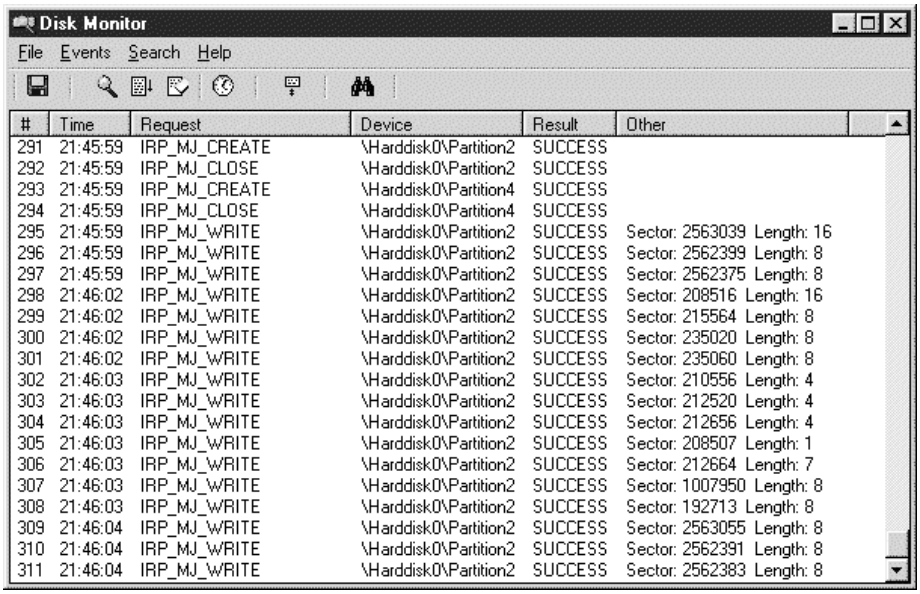


Rys. 2. Aplikacja CacheSet

Za narzędzie dyskowe i plikowe znajdujące się w paczce Sysinternals należy uznać aplikację **Contig.** Contig to bardzo wydajny defragmentator dysków. Program można wyróżnić wysokim stopniem defragmentacji, pomimo tego, iż sam proces bywa dłuższy niż w programach konkurencyjnych – po wykonaniu takiego zabiegu można mieć pewność, że nasz dysk został sprawdzony bardzo dokładnie, a dane poukładane w najlepszym porządku, co zwiększy wydajność systemu operacyjnego jak również aplikacji działających pod jego kontrolą. Aplikacja jest uruchamiana z linii komend,

co dla niektórych użytkowników może sprawić małe problemy, z pomocą przyjdzie wtedy dodatek do Contig o nazwie Power Defragmenter GUI przygotowany przez innego programistę. Jest to graficzna nakładka na Contig pozwalająca na obsługę narzędzia poprzez interfejs okienkowy w formie kreatora. Contig to najprawdopodobniej najprecyzyjniejszy z dostępnych za darmo defragmentatorów na rynku. Razem z dostępną nakładką tworzą świetny zestaw utrzymujący dyski twarde w bardzo dobrej kondycji.

Kolejnymi narzędziami typowo dyskowymi są **DiskMon**, **DiskView**, **Du (Disk Usage).** Aplikacja DiskMon służy do wyświetlenia całej aktywności dysku twardego w systemie Windows. Pozwala on dokładnie określić, który sektor dysku jest w tej chwili używany i jaka jest wykonywana operacja (zapis/odczyt). Dzięki temu można bardzo szczegółowo ustalić ewentualne błędy. Po wyborze opcji „Minimize to Tray Disk Light" program lokuje się automatycznie w obszarze powiadomień i zmienia kolor ikony w zależności od operacji: zapis-czerwony, odczyt-zielony, brak-szary. DiskMon może mieć wiele zastosowań, jednym z nich jest monitorowanie, czy podejrzany program nie próbuje zapisywać danych w systemowych obszarach dysku w boot rekordzie lub w MBR. Log działania programu można w każdej chwili zapisać do pliku. Dostępne są też funkcje wyszukiwania wśród zapisanych zdarzeń. Aplikację DiskMon przedstawiono na rysunku 3.



Rys. 3. Aplikacja DiskMon

DiskView jest to aplikacja przedstawiająca kompleksowe dane na temat zajętości miejsca na dyskach twardych komputera. Narzędzie ukazuje, które klastry zajęte są przez dane pliki, co z pewnością posłuży użytkownikom zmuszonym do usuwania błędnych sektorów na dysku

twardym. Program pozwala również na odczyt danych Master File Table oraz na usuwanie plików, tak aby ich późniejszy odczyt nie był możliwy.

Aplikacja Du (Disk Usage) to proste narzędzie konsolowe, służące do rekursywnego obliczania ilości zajmowanego miejsca na dysku przez dany plik bądź katalog. Aplikacja wywołana bez użycia parametrów dla niej dostępnych zacznie przeszukiwać wskazany katalog i wypisywać rozmiary wszystkich plików i katalogów znajdujących się w nim i w podkatalogach. Domyślne wywołanie Du jest nie szczególnie poręczne więc przedstawiam inne, bardziej praktyczne.

Sposoby wywoływania Du:

- **zwykłe liczenie rozmiaru katalogu** – najczęstszą operacją wykonywaną przy pomocy aplikacji Du, jest liczenie rozmiaru pojedynczego katalogu. Należy to wykonać przy użyciu poniższego polecenia:

  ```
  $ du –sh files/
  7.5G     files/
  ```

  Można zauważyć, iż za sprawa opcji „h” rozmiar został wyświetlony w „ludzkim” formacie. natomiast opcja „s” posłużyła do tego, by wyświetlone zostało tylko podsumowanie, a nie wszystkie kroki liczenia.

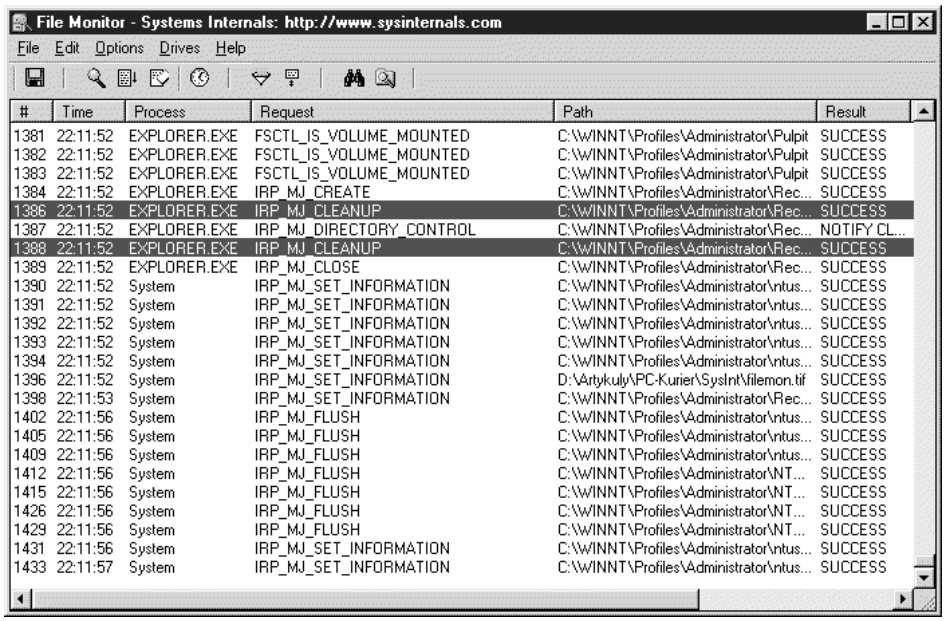
- **poszukiwanie katalogu zajmującego najwięcej miejsca** – w wielu przypadkach brakuje miejsca na dysku twardym i potrzebna jest wiadomość co zajmuje najwięcej miejsca. W takich przypadkach może okazać się przydatne takie wywołanie narzędzia Du:

  ```
  $ du –s * | sort –nr
  702352      lib
  652540      share
  155500      bin
  38152       include
  19856       sbin
  6420        local
  608         src
  520         lib64
  40          games
  28          X11R6
  ```

  Jak widać na powyższym przykładzie, tak wywołana aplikacja Du wyświetla pliki i katalogi w kolejności od najwięcej do najmniej zajmowanego miejsca na dysku twardym.

Disk Usage w połączeniu z innymi programami to potężne narzędzie, używane z pod konsoli. Aplikacja jest przydatna kiedy trzeba znać rozmiar katalogu łącznie z jego zawartością.

Następnym narzędziem z grupy dyskowe i plikowe jest **FileMon,** aplikacja wyświetla i monitoruje aktywność sytemu plików w czasie rzeczywistym. Opcje zaawansowane programu pozwalają śledzić, w jaki sposób aplikacje używają plików i bibliotek. Dzięki temu programowi możliwe jest śledzenie problemów występujących w konfiguracji systemowej. narzędzie precyzyjnie wyświetla kiedy otwarto, odczytano, zapisano bądź usunięto pliki. Aplikacja jest banalnie prosta w obsłudze, zaczyna monitorowanie w momencie uruchomienia, a wyniki mogą zostać zapisane, a następnie poddane analizie. Zastosowanie File Monitora jest bardzo szerokie: za jego pomocą możemy sprawdzać, czy programy, którym nie ufamy, nie próbują np. odczytywać zawartości naszego twardego dysku (pliki z hasłami użytkowników) i nie wysyłają potem tych informacji gdzieś w świat. Program może także monitorować sloty mailowe i łącza nazwane kanały do komunikacji pomiędzy procesami. Aplikacje FileMon przedstawiono na rysunku 4.



Rys. 4. Uruchomiona aplikacja FileMon

Kolejnych kilka narzędzi to **EFSDump**, **Junction**, **MoveFile**, **NTFSinfo**, **PageDefrag**, **PendMoves.**

EFSDump to narzędzie, które wyświetla informacje na temat osoby, która zaszyfrowała plik oraz listę osób, które mogą go odszyfrować.

Junction to aplikacja pozwalająca zarządzać w ramach systemu NTFS tzw. dowiązaniami symbolicznymi, czyli katalogami będącymi w istocie wskaźnikami do innych fizycznych katalogów.

MoveFile (char*LokalizacjaObecna, char*NowaLokalizacja) – funkcja przenosi plik bądź katalog wraz z jego podkatalogami do nowej wskazanej lokalizacji. Przy użyciu tej funkcji można, również zmieniać nazwę pliku lub katalogu.

NTFSinfo jest to aplikacja uruchamiana z poziomu wiersza poleceń. Dzięki niej można wyświetlić informacje dotyczące określonego woluminu, specyficzne dla systemu plików NTFS, takie jak liczba sektorów, całkowita liczba klastrów, liczba klastrów wolnych oraz początek i zakończenie strefy MFT (główna tablica plików – składająca się z plików systemowych).

PageDefrag narzędzie służące do defragmentacji aktualnie używanych plików. Program nie defragmentuje całego dysku/partycji ale jedynie pliki używane aktualnie.

PendMoves aplikacja służąca do zarządzania i podglądu procesu aktualizacji plików podczas restartu systemu (przykład – zainstalowano nakładkę (łatkę), która wymaga restartu systemu ponieważ pliki wymagane w procesie aktualizacji są aktualnie używane i jedyna możliwością ich podmiany to wykonanie tejże operacji poza normalna praca systemu). Narzędzie umożliwia sprawdzenie jakie pliki zostaną przy najbliższym restarcie wymienione, oraz umożliwia ręczną modyfikację tej listy.

Następna grupą narzędzi dyskowych i plikowych proponowanych przez firmę Sysinternals są **PsFile**, **PsTools**, **SDelete**, **ShareEnum**, **Streams**, **Sync** oraz **VolumeId.**

PsFile narzędzie służące do uzyskiwania szybkiej informacji na temat, jakie pliki są udostępnione, z jakimi uprawnieniami i kto w systemie z nich korzysta. Aplikacja została stworzona jako rozwinięcie polecenia netfile, Jest ona także poleceniem konsolowym, o następującej składni wywołania:

```
psfile [\\ZdalnyKomputer[-uUżytkownik[-pHasło]]][[Id|ścieżka][-c]]
```

gdzie:

- u – określa nazwę użytkownika komputera zdalnego,
- p – hasło tego użytkownika,
- Id – identyfikator pliku, który chcemy zamknąć lub o którym chcemy wyświetlić informacje,
- c – zamyka określone przez Id pliki.

PsTools to zestaw narzędzi linii poleceń, które służą pomocą przy administrowaniu systemami Windows 2000/NT, a mianowicie dostarczają dokładnych informacji na temat

komputera, systemu operacyjnego, zainstalowanych programów jak również pomagają zabić (zamknąć) wybrany proces, zmienić hasło na komputerze lokalnym bądź zdalnym. Plik archiwum zawiera skompresowane pliki .exe odpowiedzialne za poszczególne zadania. Każdy z dostępnych działa w trybie tekstowym, dzięki czemu można je uruchamiać w konsoli odzyskiwania systemu.

SDelete aplikacja służąca do kasowania plików do czynności tej jednak wykorzystuje specjalne API (ang. *Application Programming Interface*, interfejs programowania aplikacji) do defragmentacji, które umożliwia zlokalizowanie ostatnich kopii danych. Program SDelete wykorzystuje metodę pośrednia kasowania kopii starych – tworzy w systemie ogromny plik, który stopniowo zapełnia wolne miejsce na dysku. Jest to jednak operacja bardzo czasochłonna i zależna od wielkości dysku.

Program ShareEnum pozwala rozwiązać problemy związane z zabezpieczeniem plików współdzielonych. Dzięki niemu można dowiedzieć się jakie pliki są współdzielone i z jakimi uprawnieniami. Takie informacje możemy uzyskać podając zakres adresów IP komputerów, ich grupę roboczą lub nazwę domeny.

Aplikacja Streams (Alternate Data Streams ADS) w tłumaczeniu wielokrotne/alternatywne strumienie danych, czyli dodatkowe dane na partycjach NTFS umożliwiające utworzenie ukrytych plików „pod" innym już istniejącym plikiem/folderem. Plik frontowy jest jedynym widocznym spod Explorer, linii komend i menedżera plików, natomiast pliki ukryte czyli strumienie nie są widoczne. Dane zapisane w strumieniach są „bezśladowe" – wielkość pliku głównego nie zmienia się wcale za to magicznie ucieka miejsce na dysku. Na przykład można mieć dysk 60 GB, a na min tylko jeden widoczny plik o wielkości 20 KB i ukryć w nim strumienie o wielkości prawie całego dysku.

Narzędzie Sync to prosta aplikacja pracująca w linii poleceń pozwalająca na jednokierunkową synchronizację folderów. Dzięki czemu tylko katalog docelowy jest zmieniany, natomiast źródłowy pozostaje nienaruszony. Program jest napisany w języku Java.

Bardzo prostym narzędziem jest również VolumeId które określa numer woluminu przechowującego plik.