

Process Monitor — co robi program?

Czas: 2 × 45 min

praca indywidualna

Cel: Nauczenie się śledzenia operacji plikowych i rejestru programów w Process Monitor oraz wykorzystania go do znalezienia ustawień programu i przyczyny błędu.

Po zajęciach potrafisz:

- rejestruje zdarzenia Process Monitor i zawęża je filtrami
- ustala, jakie pliki i klucze rejestru tworzy instalator programu
- znajduje miejsce, w którym program zapisuje swoje ustawienia
- diagnozuje błąd wynikający z brakującego pliku (wynik NAME NOT FOUND)
- zapisuje wyniki do plików PML i CSV

Sprzęt i materiały

- komputer stacjonarny z VM Windows 11 (zadanie 26 roku 1) z migawką lub Windows 11 na drugim dysku

Oprogramowanie

- **Process Monitor (Sysinternals)** — wymaga uprawnień administratora learn.microsoft.com/sysinternals/downloads/procmon
- **Instalator 7-Zip (64-bit)** 7-zip.org
- **Notepad++ — wersja przenośna (zip)** — pakiet .zip, bez instalacji notepad-plus-plus.org/downloads

Przygotowanie przed zajęciami

- Wykonaj migawkę VM. Pobierz do VM Process Monitor, instalator 7-Zip i paczkę zip Notepad++.

Bezpieczeństwo

- Process Monitor rejestruje bardzo dużo zdarzeń — zatrzymaj przechwytywanie (Ctrl+E), gdy nie jest potrzebne, inaczej VM zwolni i zabraknie pamięci.
- Zapisane pliki PML/CSV mogą zawierać nazwy Twoich plików, ścieżki i dane z rejestru. Nie przesyłaj ich poza sprawozdanie, a z komputera szkolnego usuń po zajęciach.
- Nie zmieniaj i nie usuwaj kluczy rejestru znalezionych w Process Monitor poza przygotowanym ćwiczeniem.

Przebieg zadania

1 Pierwsze kroki i filtr

1. Uruchom `Procmon64.exe` jako administrator. Zatrzymaj przechwytywanie (Ctrl+E) i wyczyść listę (Ctrl+X).
2. Otwórz Filter → Filter... i dodaj warunek: Process Name — is — `notepad.exe` — Include. Zatwierdź.
3. Włącz przechwytywanie, uruchom Notatnik, wpisz tekst, zapisz plik `test.txt` na pulpicie i zamknij. Zatrzymaj przechwytywanie.
4. Znajdź operacje zapisu pliku `test.txt` (Operation: CreateFile, WriteFile). Sprawdź w Tools → Process Tree, jaki proces uruchomił Notatnik.

2 Co robi instalator?

1. Zmień filtr: Process Name — begins with — `7z` (nazwa instalatora). Wyczyść listę i włącz przechwytywanie.
2. Uruchom instalator 7-Zip, zainstaluj program z ustawieniami domyślnymi i zatrzymaj przechwytywanie.
3. Dodaj filtr Operation — is — `WriteFile`, a potem zamień go na `RegSetValue`. Zapisz, w jakich katalogach powstały pliki i jakie klucze rejestru zostały utworzone (Tools → File Summary i Registry Summary pomogą).
4. Zapisz zdarzenia: File → Save → Events displayed using current filter — jako PML oraz jako CSV.

3 Gdzie program trzyma ustawienia?

1. Rozpakuj Notepad++ do `C:\Narzedzia\npp`. Ustaw filtr Process Name — is — `notepad++.exe`.
2. Włącz przechwytywanie, uruchom Notepad++, zmień jedno ustawienie (np. Ustawienia → Preferencje → motyw lub język) i zamknij program.
3. Znajdź plik, do którego zapisano ustawienia (Path contains `config.xml`). Porównaj z instalowaną wersją: gdzie zapisywałyby ustawienia (wskazówka: zmienna `%APPDATA%`)?

4 Diagnoza błędu — brakujący plik

Symulujesz program, który nie działa, bo brakuje mu pliku konfiguracyjnego.

1. Utwórz `C:\Test\ustawienia.ini` z dowolną treścią i skrypt `C:\Test\aplikacja.cmd` z treścią: `type C:\Test\ustawienia.ini || echo BLAD: program nie moze sie uruchomic` i w kolejnej linii `pause`.
2. Uruchom skrypt — działa. Zmień nazwę `ustawienia.ini` na `ustawienia.old` i uruchom ponownie — pojawia się błąd.
3. W Process Monitor ustaw filtr Process Name — is — `cmd.exe` oraz Result — is — `NAME NOT FOUND`. Uruchom skrypt i znajdź zdarzenie wskazujące brakujący plik.
4. Zamknij Notepad++, zmień nazwę jego `config.xml` i uruchom go z przechwytywaniem. Opisz, jak program poradził sobie z brakiem pliku (zdarzenia NAME NOT FOUND, a potem zapis nowego pliku). Przywróć migawkę VM.

W sprawozdaniu umieść

- ☐ zrzut filtrów i drzewa procesów
- ☐ tabela plików i kluczy rejestru utworzonych przez instalator 7-Zip
- ☐ lokalizacja ustawień Notepad++ w wersji przenośnej i instalowanej
- ☐ zrzut zdarzenia NAME NOT FOUND z diagnozą błędu
- ☐ fragment pliku CSV (kilka wierszy)
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego bez filtra praca z Process Monitor jest prawie niemożliwa?
2. Co oznaczają wyniki SUCCESS, NAME NOT FOUND i ACCESS DENIED? Który z nich zwykle wskazuje problem z uprawnieniami?
3. Dlaczego wersja przenośna programu zapisuje ustawienia w swoim katalogu, a instalowana w profilu użytkownika?
4. Jak technik może wykorzystać Process Monitor, gdy program po aktualizacji przestał się uruchamiać i nie wyświetla komunikatu?

Kryteria oceny

Kryterium	Punkty
Poprawne filtry i przechwytywanie	3
Analiza instalatora — pliki i rejestr	5
Lokalizacja ustawień programu	3
Diagnoza brakującego pliku	5
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).