

Bezpieczne usuwanie danych i utylizacja

Czas: 2 × 45 min

praca indywidualna

Cel: Sprawdzenie w praktyce, które metody usuwania danych pozwalają je odzyskać, a które je niszczą, oraz przygotowanie protokołu zniszczenia danych przed przekazaniem sprzętu do utylizacji.

Po zajęciach potrafisz:

- odzyskuje usunięte pliki programem PhotoRec i ocenia skuteczność odzysku
- nadpisuje wolne miejsce (`cipher /w`) i cały dysk (`diskpart clean all` , `nwipe`)
- wyjaśnia, dlaczego na dyskach SSD stosuje się Secure Erase lub Sanitize zamiast nadpisywania
- sporządza protokół zniszczenia danych zgodny z zasadami RODO
- wskazuje prawidłową drogę utylizacji zużytego sprzętu (WEEE)

Sprzęt i materiały

- komputer stacjonarny z VirtualBox i maszyną wirtualną Windows 11
- pendrive z Ventoy (tylko jako źródło obrazu ShredOS — nie jest wymazywany)

Oprogramowanie

- **TestDisk & PhotoRec** — wersja dla Windows; `qphotorec_win.exe` ma interfejs graficzny
cgsecurity.org/wiki/TestDisk_Download
- **ShredOS (nwipe)** — obraz .iso — do VM lub na pendrive z Ventoy
github.com/PartialVolume/shredos.x86_64/releases
- **Narzędzia wbudowane Windows** — `cipher` , `diskpart` , Zarządzanie dyskami
- **NIST SP 800-88 rev. 2 (wytyczne usuwania danych)** — metody Clear, Purge, Destroy
csrc.nist.gov/pubs/sp/800/88/r2/final

Przygotowanie przed zajęciami

- Dodaj do VM Windows 11 dwa nowe dyski VDI po 1 GB. W Zarządzaniu dyskami utwórz na nich woluminy NTFS z etykietami `TEST1` i `TEST2`.
- Przygotuj zestaw plików testowych: po 3 pliki jpg, docx (lub pdf) i txt — bez danych osobowych.
- Pobierz PhotoRec (Windows) i obraz ShredOS (.iso).

Bezpieczeństwo

- `diskpart clean all` i `nwipe` nieodwracalnie niszczą cały wybrany dysk. Przed wykonaniem sprawdź `detail disk` (rozmiar 1 GB, etykieta TEST) i pokaż ekran nauczycielowi.
- W ShredOS wybieraj wyłącznie dysk testowy — nigdy dysk systemowy, pendrive z Ventoy ani pierwszy dysk komputera.
- Wymazywanie drugiego dysku fizycznego w ShredOS tylko za zgodą nauczyciela i po odłączeniu pierwszego dysku (kabel SATA przy wyłączonym zasilaniu).
- Pliki odzyskane zapisuj na dysk `C:` maszyny wirtualnej, nigdy na dysk, z którego odzyskujesz.
- Nie odzyskuj danych z cudzych nośników — dotyczy to także pendrive'ów znalezionych w pracowni.

Przebieg zadania

1 Scenariusz 1 — zwykłe usunięcie

Na woluminie TEST1.

1. Skopiuj pliki testowe na TEST1. Zapisz ich liczbę i rozmiar.
2. Usuń je klawiszami Shift+Delete, a następnie wykonaj szybkie formatowanie woluminu TEST1.
3. Uruchom `qphotorec_win.exe` jako administrator, wybierz dysk 1 GB (TEST1), system plików Other/NTFS, przeszukiwanie całego woluminu, folder docelowy `C:\odzysk1`.
4. Policz odzyskane pliki każdego typu i otwórz po jednym — oceń, czy są kompletne. Zwróć uwagę, że nazwy plików nie zostały odzyskane.

2 Scenariusz 2 — nadpisanie wolnego miejsca

Na woluminie TEST2.

1. Skopiuj pliki testowe na TEST2 i usuń je (Shift+Delete).
2. Nadpisz wolne miejsce: `cipher /w:<litera TEST2>:\` w Terminalu (administrator). Zanotuj czas działania i co wypisuje program.
3. Uruchom PhotoRec na TEST2 (folder `C:\odzysk2`) i porównaj wynik ze scenariuszem 1.

3 Scenariusz 3 — wymazanie całego dysku

Ponownie na dysku TEST1.

1. Skopiuj pliki testowe na TEST1 jeszcze raz. Uruchom `diskpart`, wykonaj `list disk`, `select disk <nr dysku 1 GB>`, `detail disk` — pokaż ekran nauczycielowi.
2. Wykonaj `clean all` i zanotuj czas. Sprawdź dysk w Zarządzaniu dyskami.
3. Uruchom PhotoRec na tym dysku (folder `C:\odzysk3`) i zapisz wynik.
4. Opcjonalnie: wyłącz VM, w VirtualBox zamontuj obraz ShredOS jako napęd optyczny i uruchom z niego VM. W `nwipe` zaznacz tylko dysk TEST2 (1 GB), wybierz metodę i weryfikację, uruchom wymazywanie i zrób zdjęcie podsumowania.

4 Dyski SSD, protokół i utylizacja

Część teoretyczna na podstawie wytycznych NIST SP 800-88 i dokumentacji producenta dysku SSD z Twojego stanowiska.

1. Sprawdź na stronie producenta dysku SSD (lub dysku z laptopa), jakim narzędziem wykonuje się Secure Erase/Sanitize. Zapisz nazwę narzędzia i warunki (np. odblokowanie dysku, zasilanie).
2. Przyporządkuj metody z zajęć do kategorii Clear, Purge, Destroy.
3. Wypełnij protokół zniszczenia danych dla fikcyjnego komputera księgowości przekazywanego do utylizacji.
4. Sprawdź, gdzie w Twojej gminie można oddać zużyty sprzęt elektroniczny (punkt selektywnej zbiórki, sklep przy zakupie nowego) i zapisz źródło.

W sprawozdaniu umieść

- ☐ tabela wyników trzech scenariuszy (pliki usunięte, odzyskane, kompletne)
- ☐ zrzuty: wynik PhotoRec, praca `cipher /w`, ekran `detail disk` przed `clean all`
- ☐ przyporządkowanie metod do kategorii NIST oraz opis metody dla SSD
- ☐ wypełniony protokół zniszczenia danych
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego po usunięciu pliku i szybkim formatowaniu dane nadal da się odzyskać?
2. Dlaczego wielokrotne nadpisywanie nie jest pewną metodą dla dysków SSD i pendrive'ów, a co robi polecenie Sanitize?
3. Czym różni się `cipher /w` od `diskpart clean all` — kiedy użyć każdego z nich?
4. Jakie obowiązki wynikają z RODO, gdy szkoła lub firma pozbywa się komputera z danymi osobowymi?

Kryteria oceny

Kryterium	Punkty
Trzy scenariusze wykonane bezpiecznie (właściwy dysk, sprawdzone przez nauczyciela)	6
Rzetelna tabela wyników i porównanie skuteczności	4
Kategorie NIST i metoda dla SSD	3
Protokół zniszczenia danych i utylizacja	4
Odpowiedzi na pytania kontrolne	3
Razem	20

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