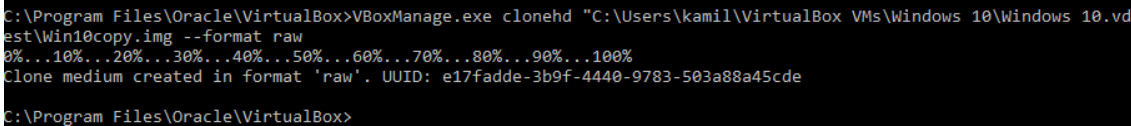


# Informatyka śledcza - Projekt

Projekt ma na celu wykorzystanie w praktyce poznanych narzędzi znajdujących się w „otwartym kodzie” do potencjalnej analizy śledczej. W ramach zajęć wymagane jest przeprowadzenie symulacji działania użytkownika, którego nośnik danych został zabezpieczony w wyniku procesu karnego. Schemat działania:

1. Stworzenie wirtualnego środowiska (VirtualBox/VMware + Windows/Linux/macOS).  
VirtualBox - <https://www.virtualbox.org/wiki/Downloads>
2. Na zainstalowanym wirtualnym systemie, student opisując swoje działania w dokumencie projektowym zasymuluje normalne użytkowanie systemu polegające na:
  - zmianach ustawień systemowych (rejestr, cmd, zapora systemowa, itp.),
  - pobraniu i instalacji dodatkowego oprogramowania (np. Notepad++ itp.),
  - pobraniu kilku darmowych plików graficznych oraz dodaniu kilku zdjęć wykonanych telefonem komórkowym (otoczenia poza domem – włączony tryb lokalizacji),
  - wykorzystaniu przeglądarki www do wyszukania i wyświetlenia przykładowych witryn internetowych, które mogłyby świadczyć o zainteresowaniach użytkownika,
  - utworzeniu kilku plików tekstowych (notatnik/ word/pliki .pdf),
  - usunięciu kilku plików i utworzonych wcześniej folderów w ramach działań użytkowych systemu.
3. Kolejnym krokiem jest konwersacja pliku wirtualnego dysku (vdi lub vmdk) do formatu raw (przykład dla formatu vdi):
4. Instalacja aplikacji Autopsy (<https://www.autopsy.com/download/>).
5. Utworzenie nowej sprawy.
6. Zaimportowanie obrazu systemu (.img) do programu.
7. Przeprowadzenie analizy.
8. Sporządzenie szczegółowej dokumentacji projektowej z przeprowadzonych czynności (.pdf), uwzględniając w to zrzuty ekranu.

Dodatkowo proszę o wybranie kilku narzędzi do przeprowadzenia analiz polegających na:

1. Zrzucie pamięci RAM oraz jej analizy (działania w ramach systemu Linux).
2. Wyciągnięciu danych ze smartfona (IOS lub Android) lub pobranie gotowego obrazu systemu mobilnego do analizy (obraz udostępniony na platformie MS Teams). Analiza plików (PLIST i SQLite).
3. Wykorzystaniu narzędzia ExifTool do wyciągnięcia metadanych z plików graficznych oraz przedstawienia metod odzyskiwania straconych danych (Foremost, Scalpel, RecoverJPEG).
4. Utworzeniu kopii binarnej nośnika (np. DD, DCFLDD, DC3DD, itp.) zawierającego dane nadające się do analizy oraz pozyskanie informacji o samym obrazie (mmls, fls, img\_stat, ewftools, itp.).

5. Własny pomysł (np. analiza ruchu „NetFlow”, konfiguracji urządzenia sieciowego lub inną formę analizy omówioną na wykładzie).