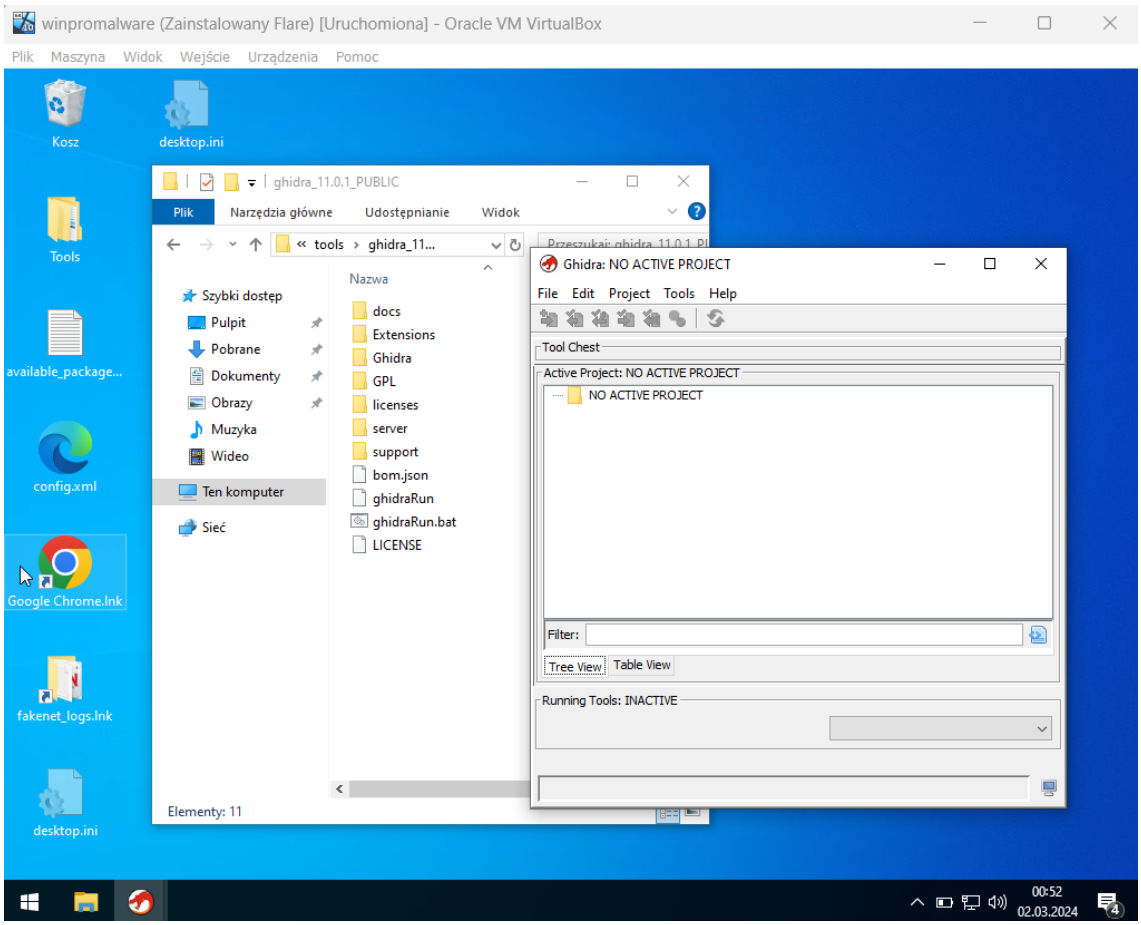
Analiza Malware Laboratorium nr 1

Raport – Nikodem Jakubowski

Tworzenie środowiska testowego (sandbox) do celów analizy malware.

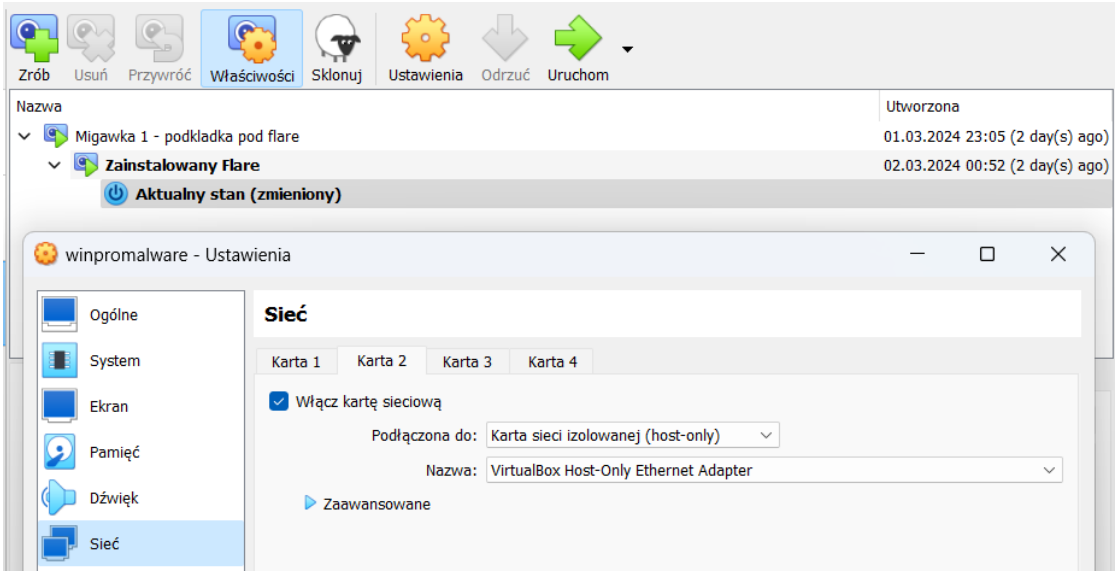
Utworzyłem maszynę wirtualną z Windows 10 Pro (wersja Pro, żeby łatwiej było znaleźć „gpedit.msc” bez potrzeby instalacji dodatkowych skryptów). Przygotowałem maszynę do spełnienia minimalnych wymagań „Flare-VM”. Microsoft Update wyłączyłem zgodnie z instrukcją. Microsoft Defender również, ale przy pomocy „gpedit.msc” (dodatkowo należało w cmd wykonać komendę „gpupdate”, żeby zmiana się zapisała). Stworzyłem migawkę przed instalacją „Flare-VM” jak i po, co wiele razy mnie uratowało, bo nie raz maszyna się zacinała na jakimś procesie. Wszystkie testy/wymagania „Flare-VM” zostały spełnione przed instalacją.

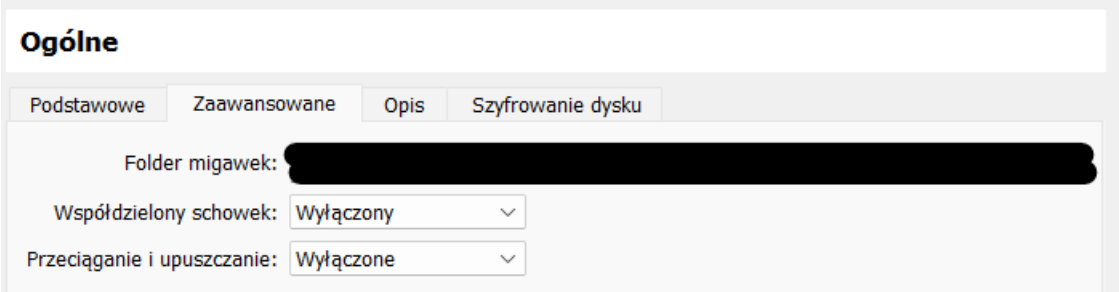
Aktualna wersja „Flare-VM” zawiera również program „Ghidra”, który jest gotowy do działania – zdjęcie poniżej.



Z jakiegoś powodu tło pulpitu się nie zmieniło co charakterystyczne dla „Flare-VM”. To widocznie częsty błąd, bo spytałem innych studentów i u nich wygląda to tak samo. Długo myślałem, że to wyznacznik poprawnej instalacji. Po porównaniu efektów z innymi zorientowałem się, że kluczowa jest zawartość.

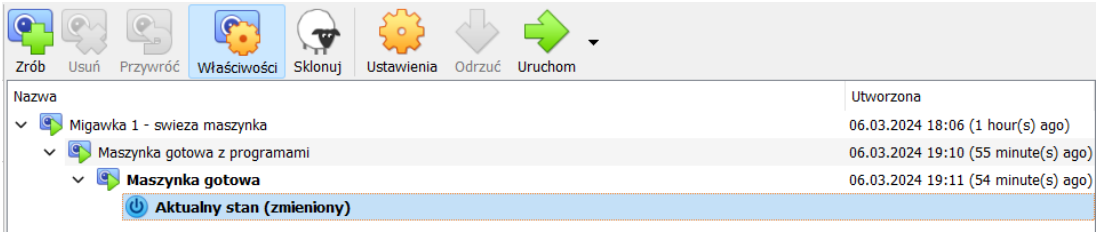
Skonfigurowałem sandboxa zgodnie z instrukcją: stworzyłem migawki, karta sieciowa w trybie host-only, wyłączyłem współdzielone foldery i schowek.



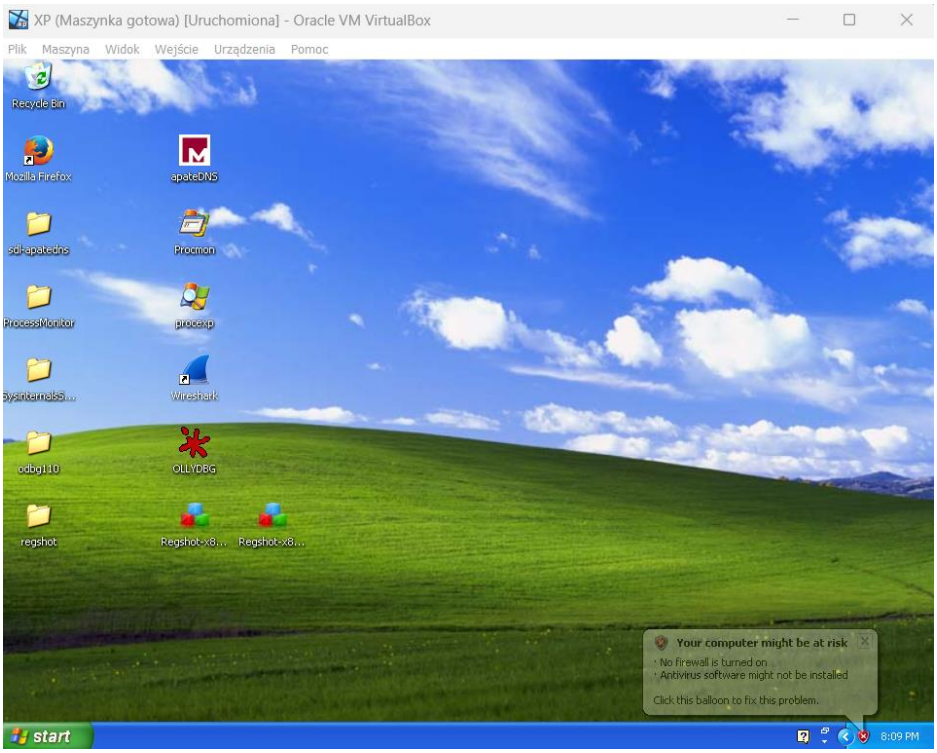


Konfiguracja Windows XP SP3 32bit wraz z programami.

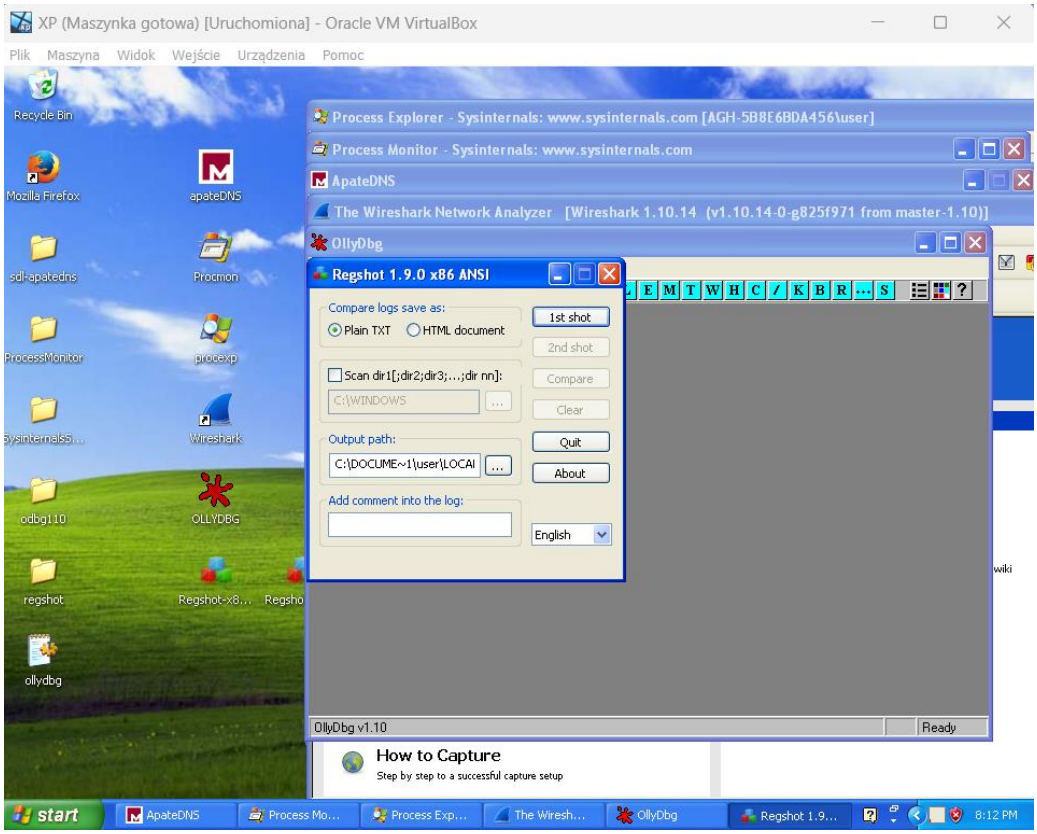
Po aktualizacji „VirtualBox” do najnowszej wersji w końcu udało się zainstalować „Windows XP” z SP3. Poniżej zdjęcia migawek.



Poniżej zdjęcie pulpitu z pobranymi programami.



Na poniższym zdjęciu przedstawiam wszystkie programy włączone jednocześnie.



Dodatkowo wyłączyłem aktualizacje i wszystkie zabezpieczenia. Oczywiście wyłączyłem wszystkie dodatki gościa po konfiguracji, a gdy na maszynie już dodam zainfekowane próbki to przełączę kartę sieciową na host- only.