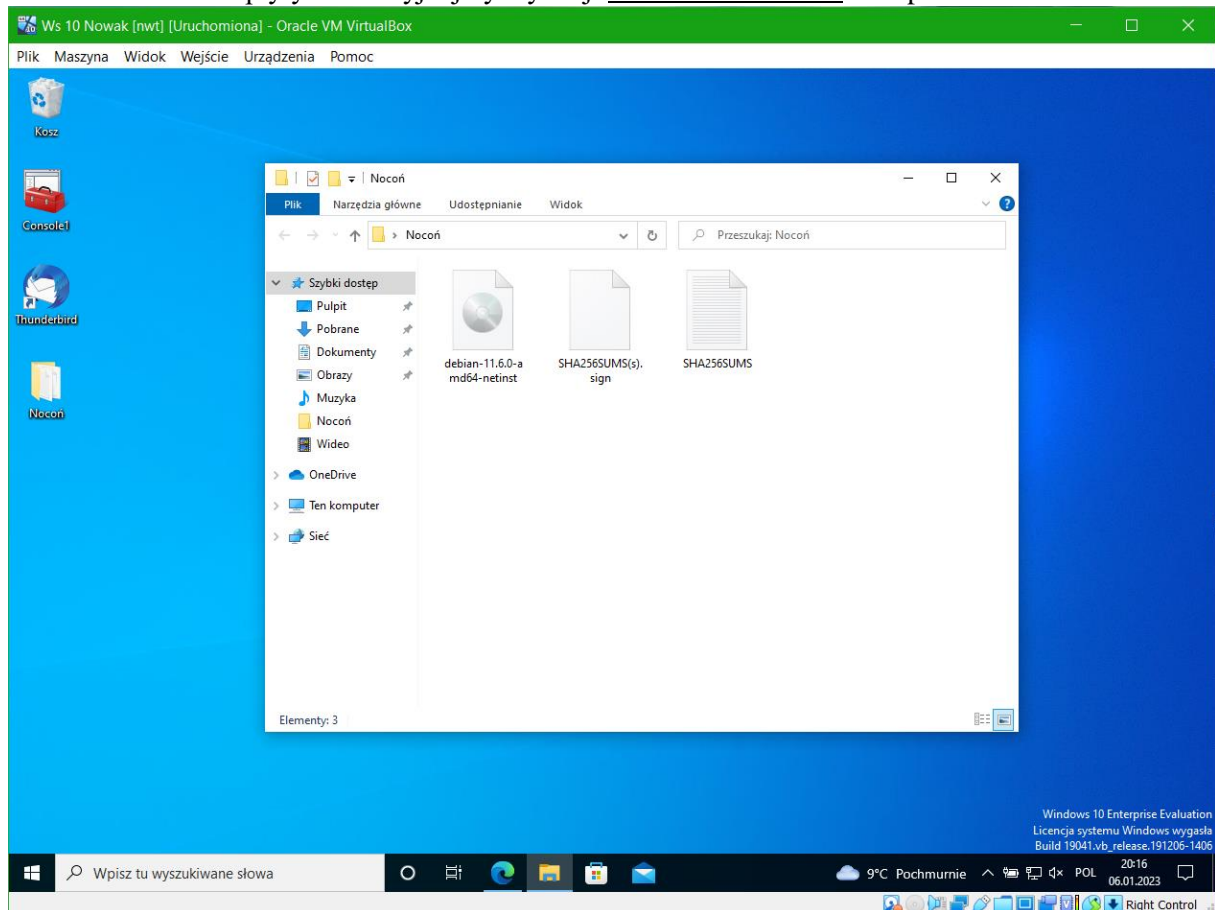


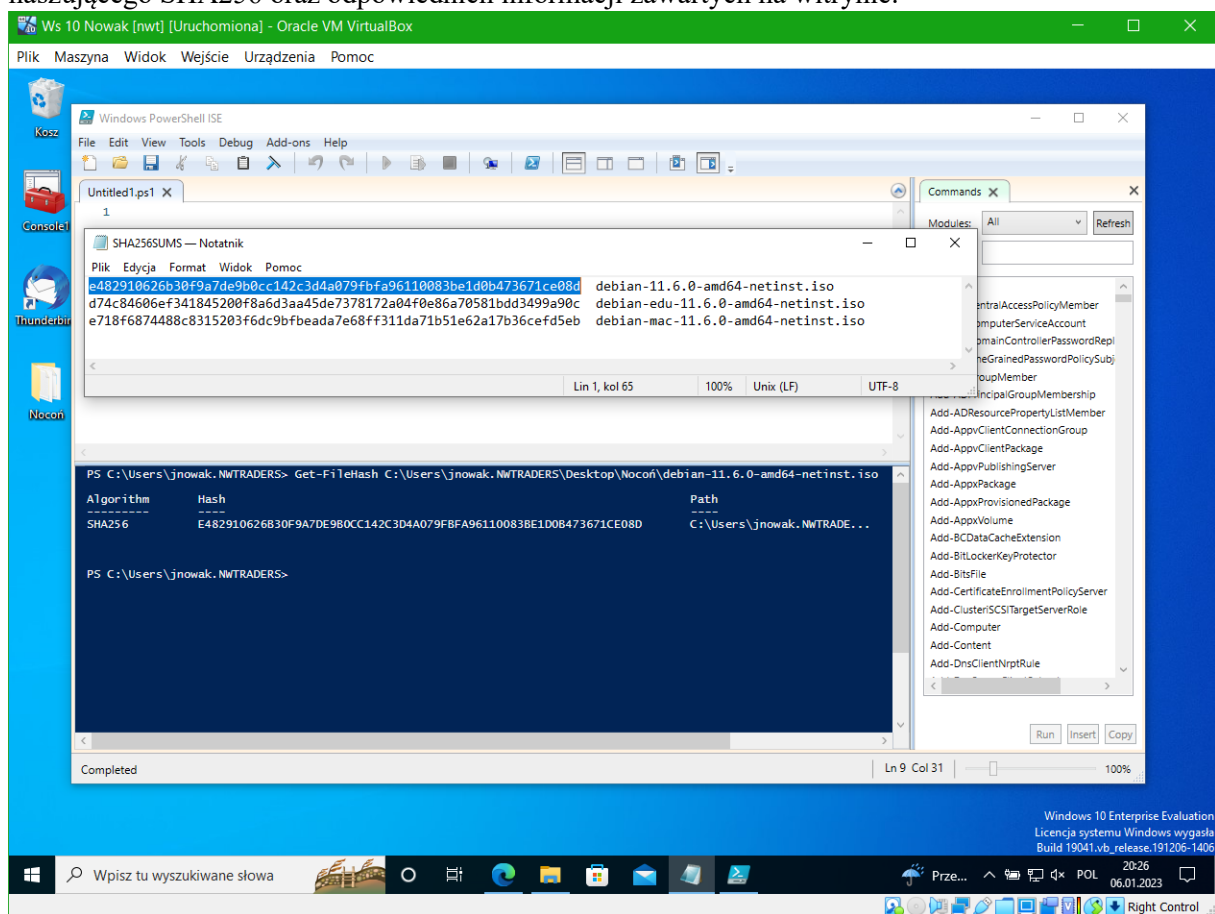
Zadania do samodzielnej realizacji w domu (Moduł 1) – Kryptograficzne metody ochrony informacji

Zadanie 1

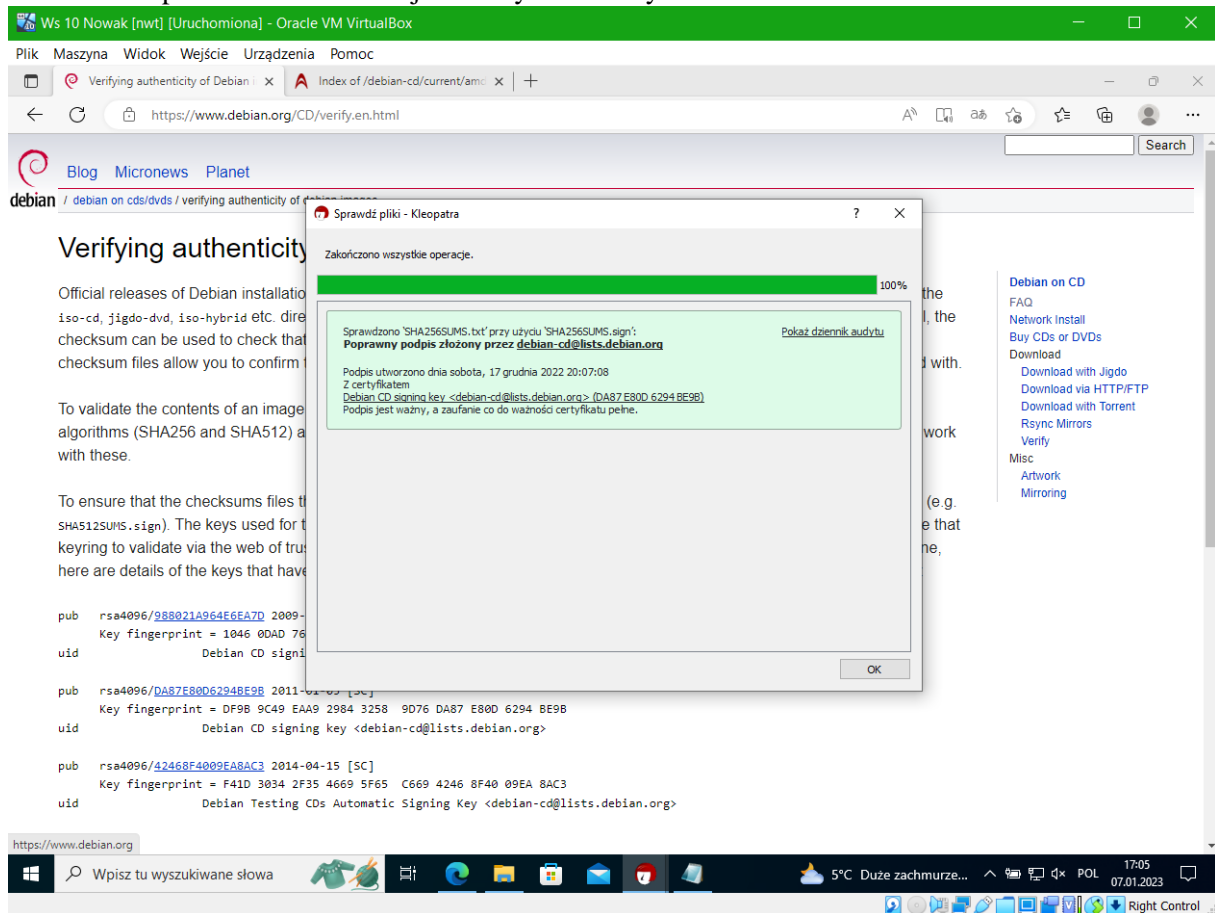
W systemie Windows "Nowak" należy pobrać (do katalogu "{Nazwisko}" utworzonego na pulpicie) obraz ISO "*netinst*" płyty instalacyjnej dystrybucji Debian GNU/Linux oraz plik "*SHA256SUMS*".



Zweryfikować prawidłowość integralności pobranego pliku ISO z wykorzystaniem algorytmu haszującego SHA256 oraz odpowiednich informacji zawartych na witrynie.

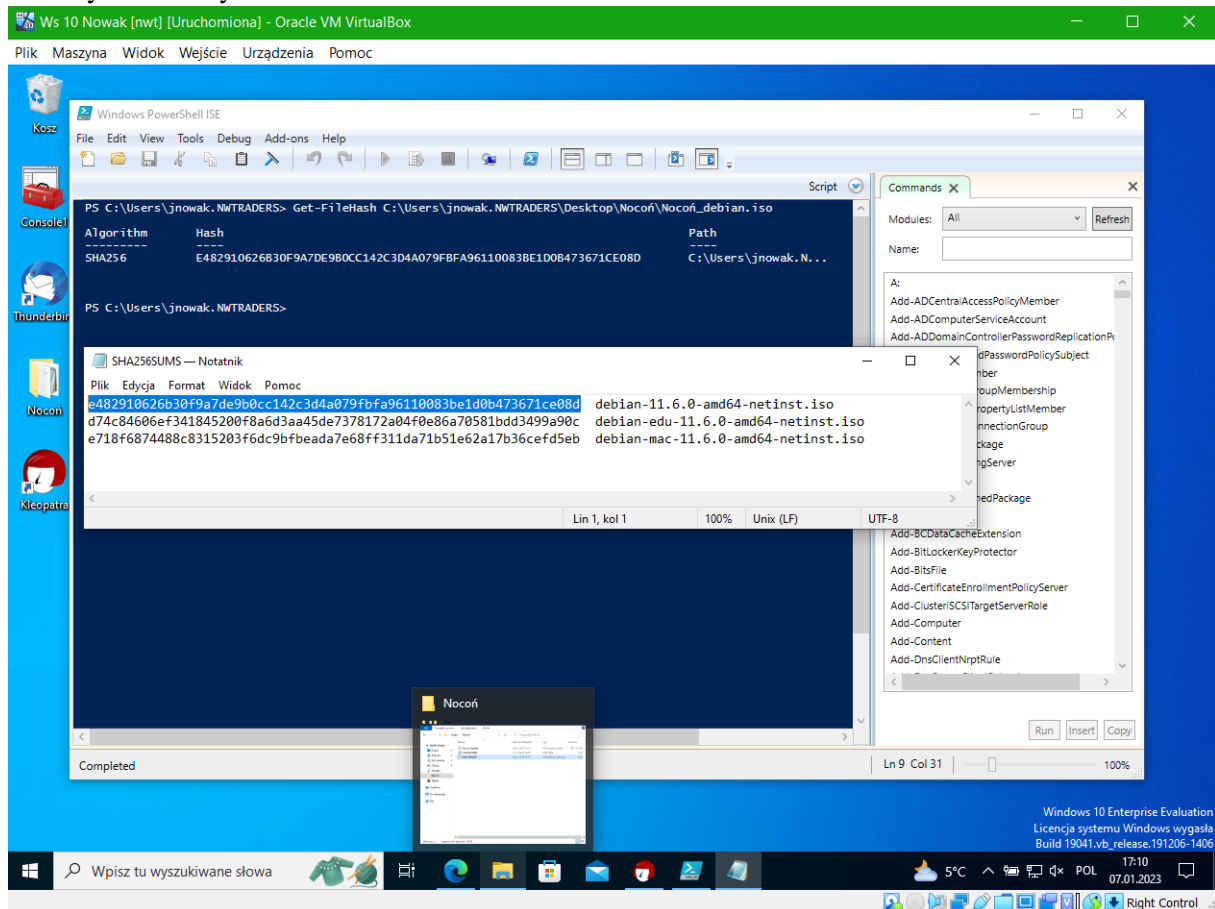


Zweryfikować podpis cyfrowy pobranego pliku "*SHA256SUMS*" z wykorzystaniem oprogramowania GPG oraz odpowiednich informacji zawartych na witrynie.



Zmienić nazwę pliku ISO na "{Nazwisko}_debian.iso" i zweryfikować prawidłowość integralności pliku ISO z wykorzystaniem algorytmu haszującego SHA256 oraz odpowiednich informacji

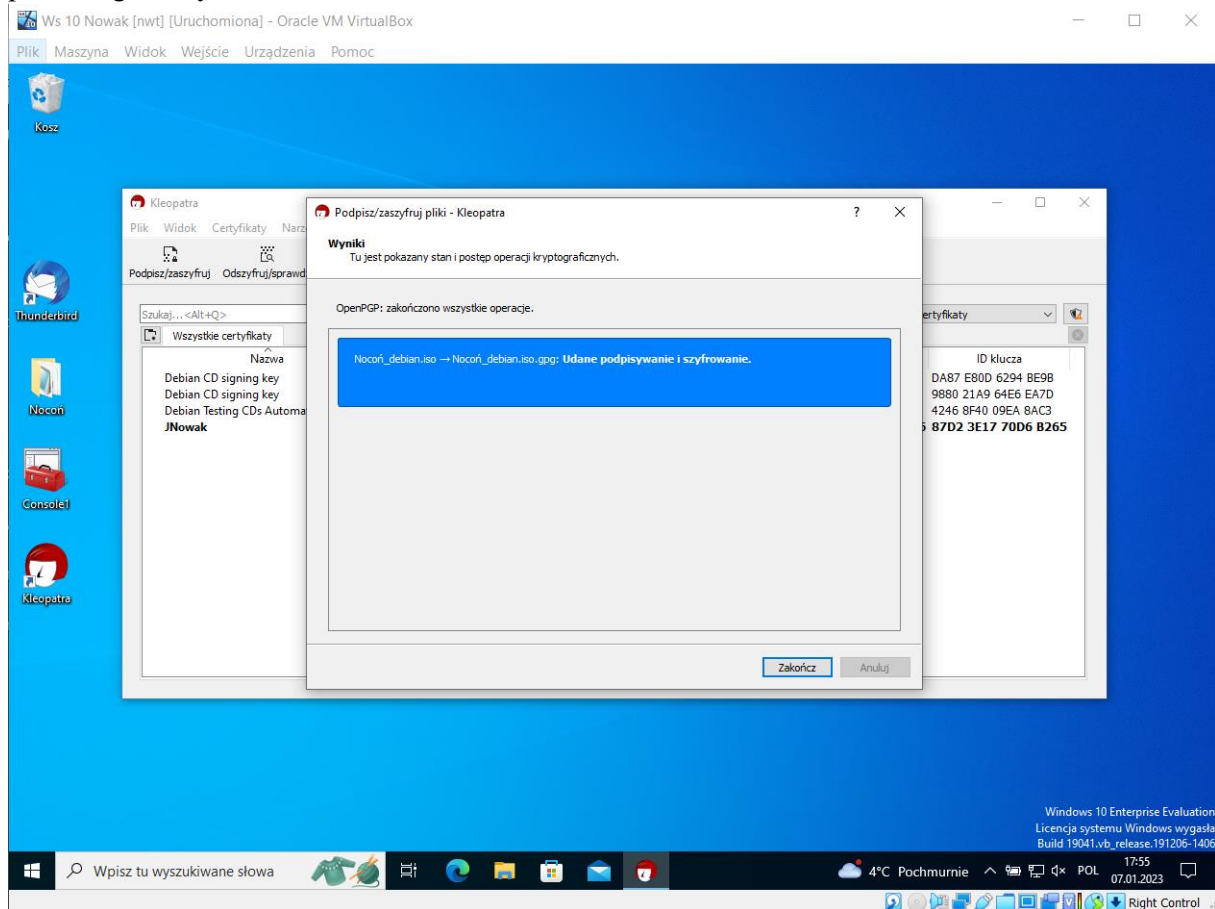
zawartych na witrynie.



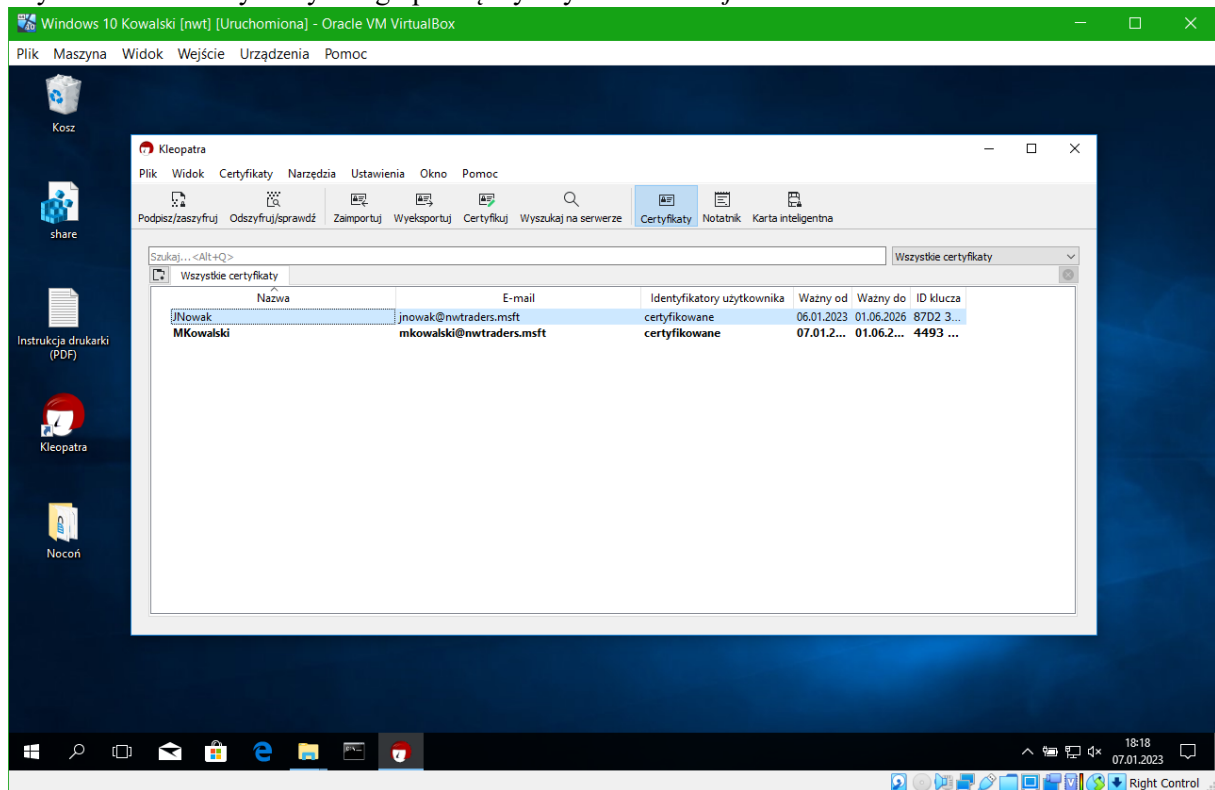
Zadanie 2

Należy w systemie Windows "Nowak" z wykorzystaniem oprogramowania Gpg4Win zaszyfrować plik "{nazwisko}_debian.iso" oraz podpisać cyfrowo zaszyfrowany plik jako użytkownik jnowak i

prześłać go do systemu Windows "Kowalski".



Wymiana klucza asymetrycznego pomiędzy użytkownikami *jnowak* oraz *mkowalski*.



Zweryfikować jako *mkowalski* podpis cyfrowy dla tegoż pliku.

