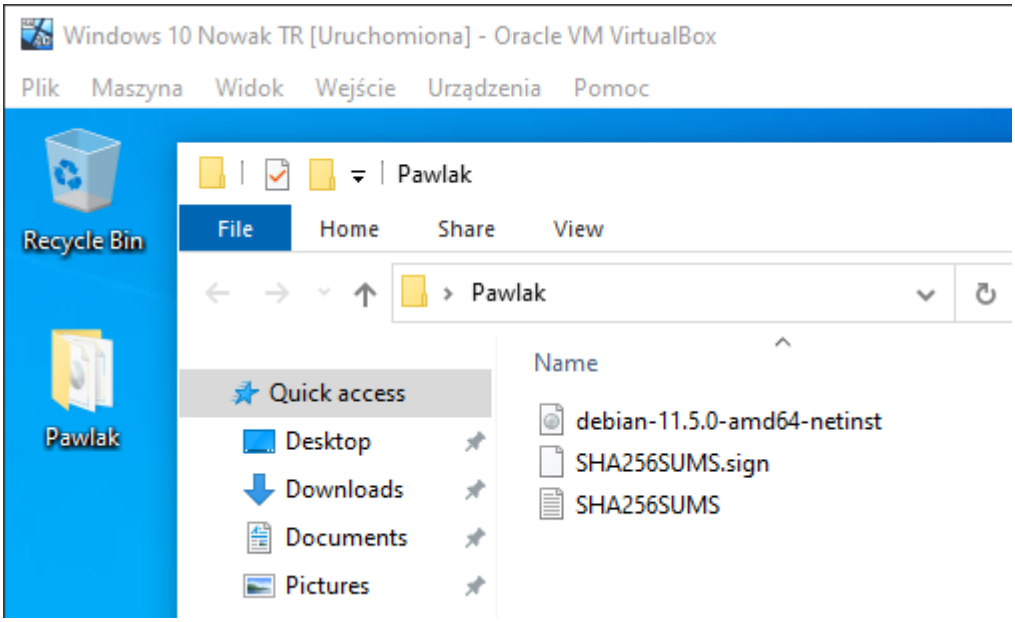
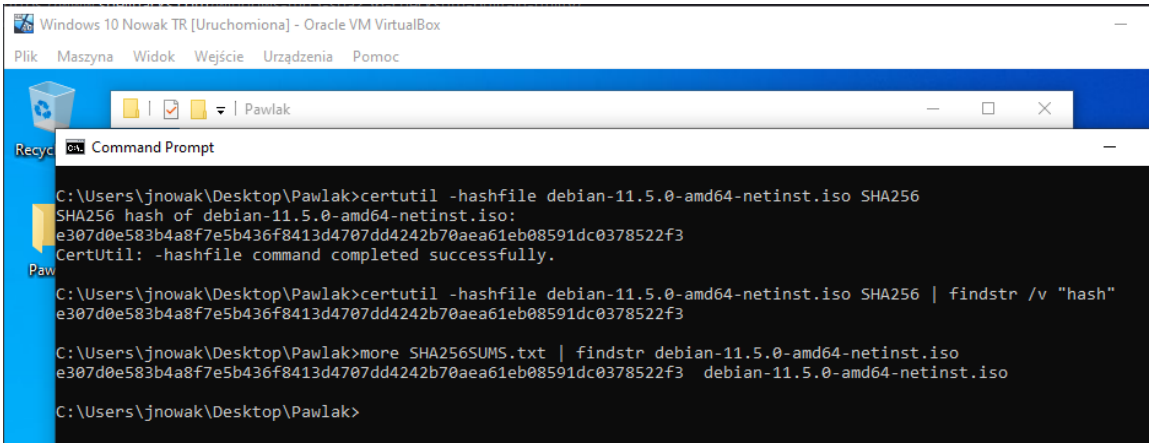
Sprawozdanie z zadań do samodzielnej realizacji Moduł 1

Zadanie 1

1. W systemie Windows "Nowak" należy pobrać (do katalogu "{Nazwisko} utworzonego na pulpicie") z witryny https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/ obraz ISO "netinst" płyty instalacyjnej dystrybucji Debian GNU/Linux, jak również plik "SHA256SUMS".

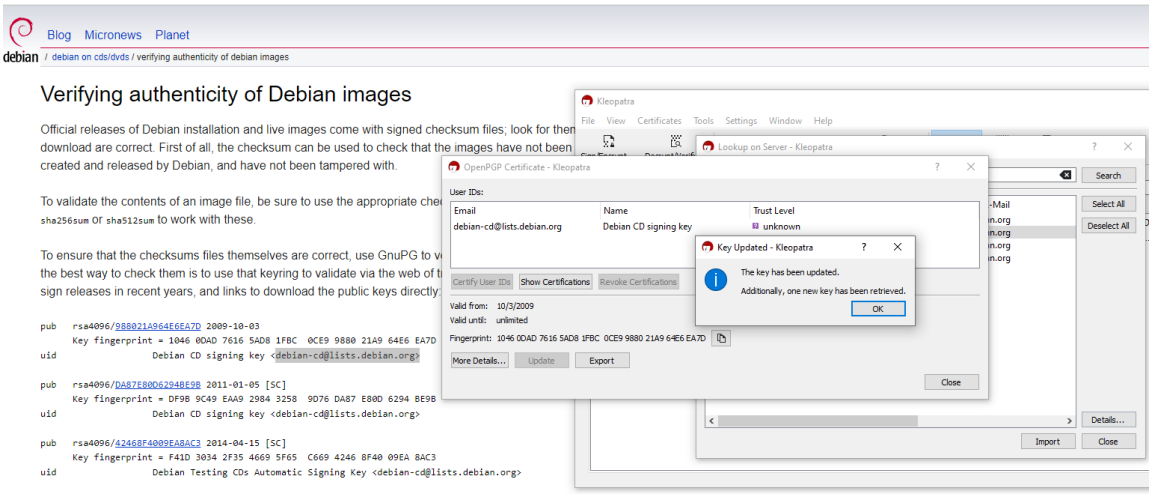


2. Zweryfikować prawidłowość integralności pobranego pliku ISO z wykorzystaniem algorytmu haszującego SHA256 oraz odpowiednich informacji zawartych na w/w witrynie

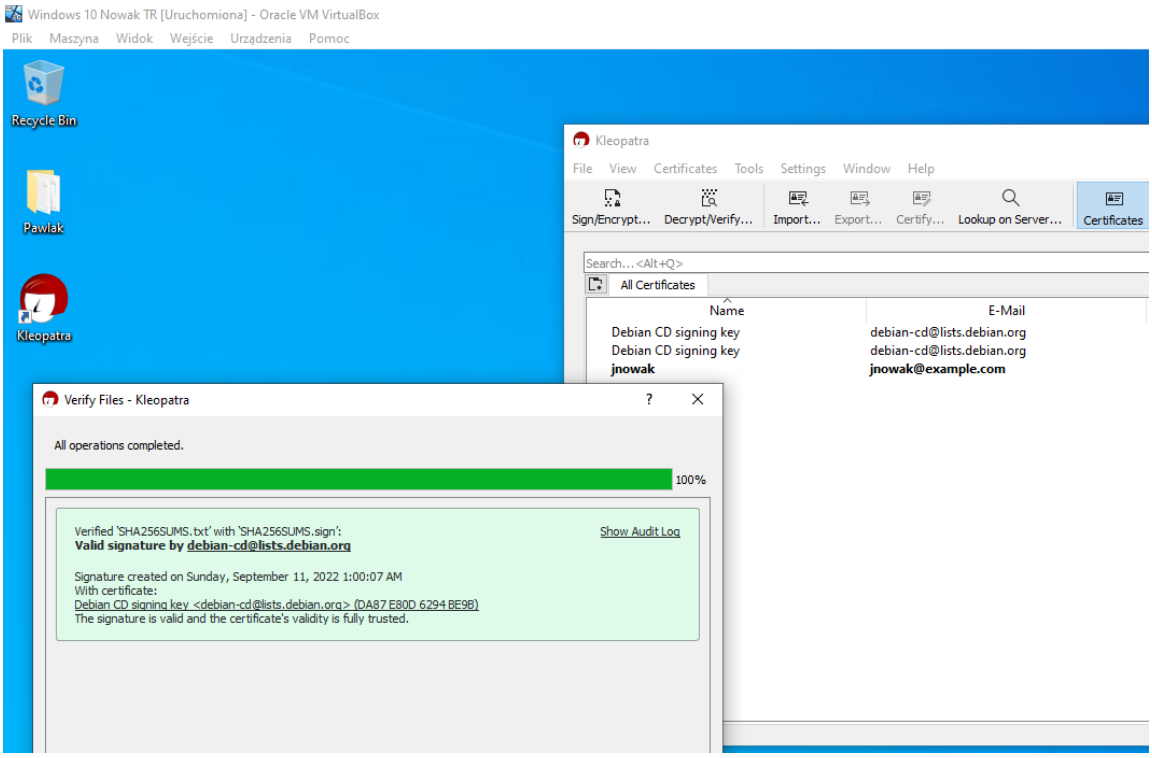


3. Zweryfikować podpis cyfrowy pobranego pliku "SHA256SUMS" z wykorzystaniem oprogramowania GPG oraz odpowiednich informacji zawartych na w/w witrynie

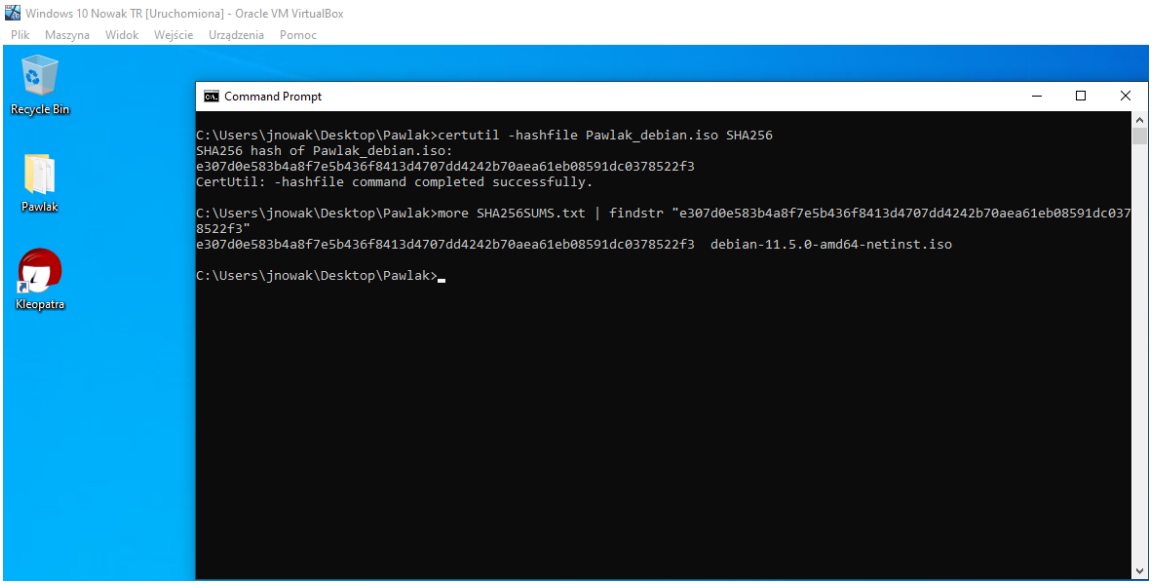
   - import klucza publicznego



   - weryfikacja pliku



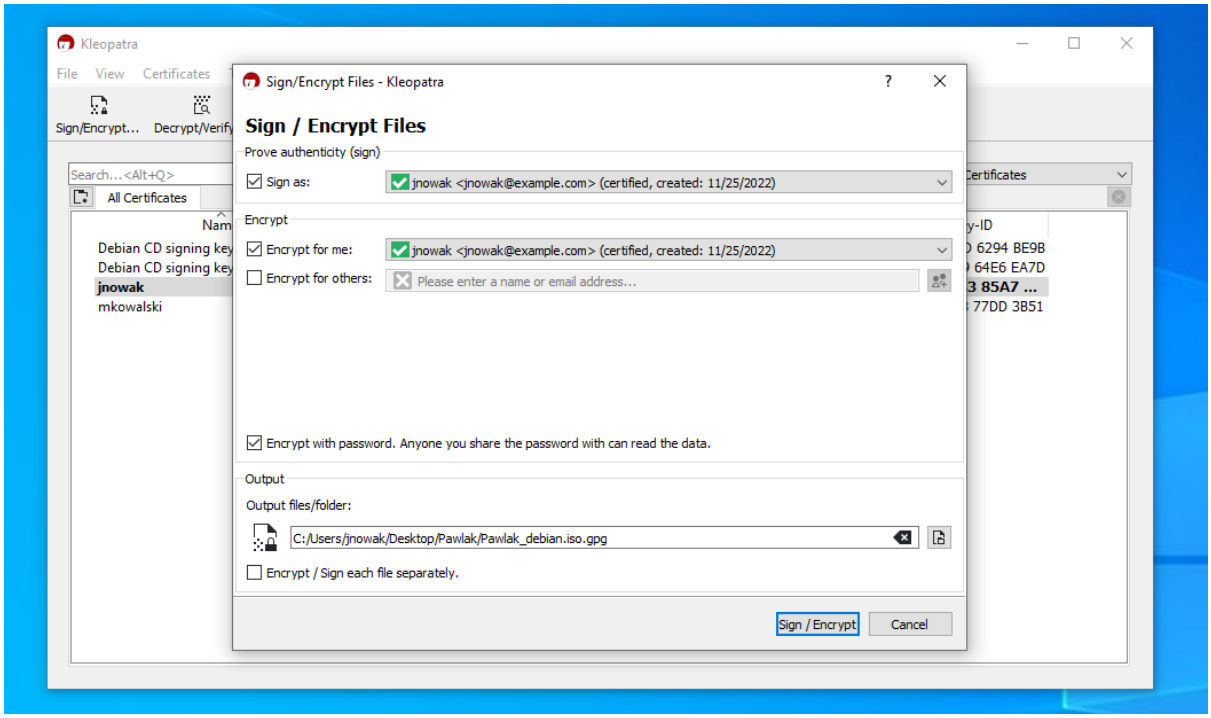
4. Zmienić nazwę pliku ISO na "{Nazwisko}_debian.iso" (pod {Nazwisko} należy podstawić własne nazwisko - jest to warunkiem zaliczenia sprawozdania) i następnie zweryfikować prawidłowość integralności pliku ISO z wykorzystaniem algorytmu haszującego SHA256 oraz odpowiednich informacji zawartych na w/w witrynie

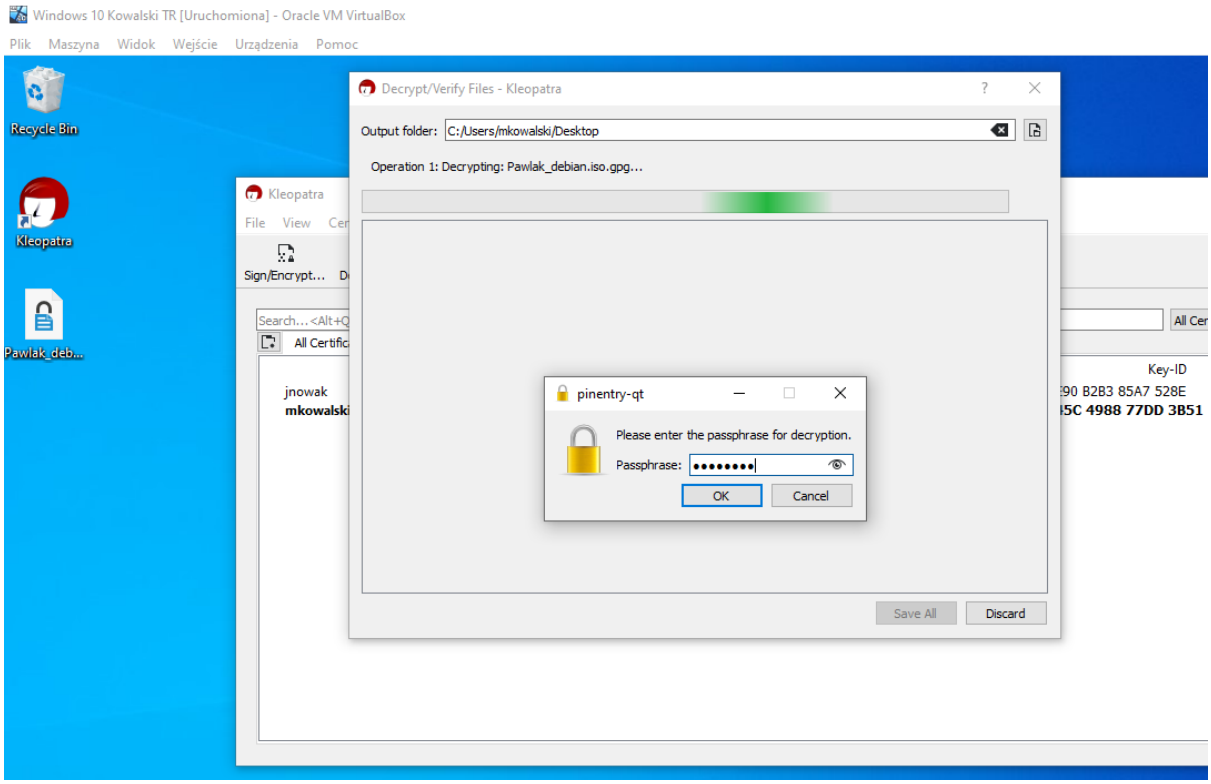


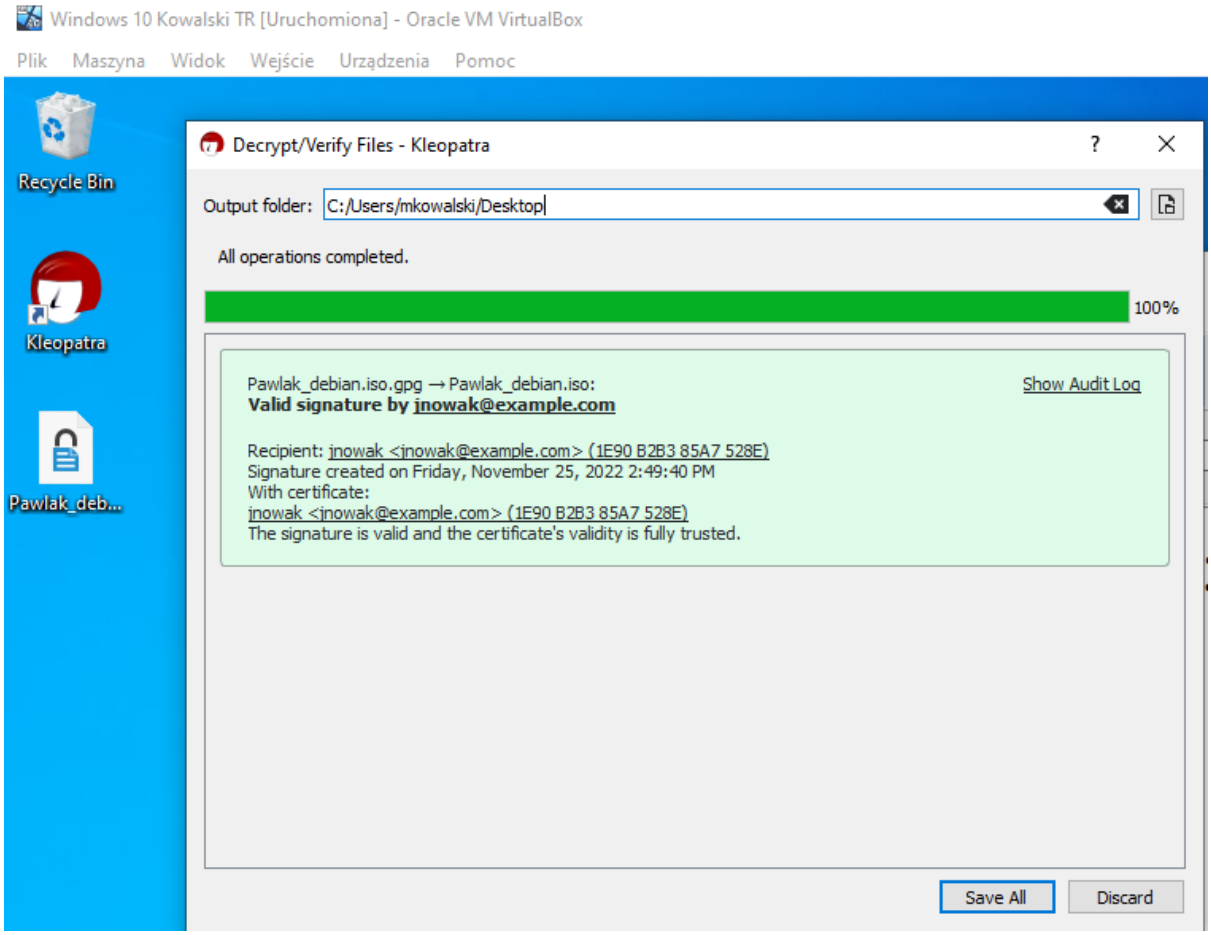
integralność pliku jest zachowana po zmianie nazwy

Zadanie 2

Należy w systemie Windows "Nowak" z wykorzystaniem oprogramowania Gpg4Win zaszyfrować plik "{nazwisko}_debian.iso" (wykorzystując klucz symetryczny AES256) oraz podpisać cyfrowo zaszyfrowany plik jako użytkownik jnowak (wykorzystując algorytm haszujący SHA256), a następnie przesłać go do systemu Windows "Kowalski" i tam zweryfikować jako mkowalski podpis cyfrowy dla tegoż pliku.
(Oczywiście najpierw konieczna jest odpowiednia wymiana klucza asymetrycznego pomiędzy użytkownikami "jnowak" oraz "mkowalski")




Windows 10 Kowalski TR [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Recycle Bin
Kleopatra
Pawlak_deb...
Decrypt/Verify Files - Kleopatra
Output folder: C:/Users/mkowalski/Desktop
Operation 1: Decrypting: Pawlak_debian.iso.gpg...
pinentry-qt
Please enter the passphrase for decryption.
Passphrase:
OK
Cancel
Save All
Discard


Windows 10 Kowalski TR [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Recycle Bin
Kleopatra
Pawlak_deb...
Decrypt/Verify Files - Kleopatra
Output folder: C:/Users/mkowalski/Desktop
All operations completed.
100%
Pawlak_debian.iso.gpg → Pawlak_debian.iso:
Valid signature by jnowak@example.com
Show Audit Log
Recipient: jnowak <jnowak@example.com> (1E90 B2B3 85A7 528E)
Signature created on Friday, November 25, 2022 2:49:40 PM
With certificate:
jnowak <jnowak@example.com> (1E90 B2B3 85A7 528E)
The signature is valid and the certificate's validity is fully trusted.
Save All
Discard