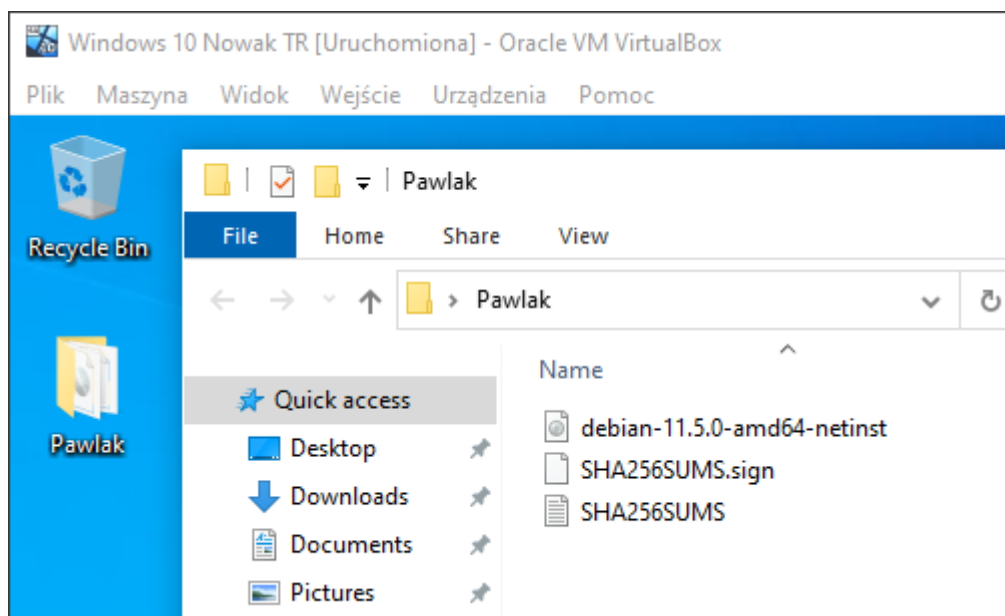


# Sprawozdanie z zadań do samodzielnej realizacji Moduł 1

## 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

```
C:\Users\jnowak\Desktop\Pawlak>certutil -hashfile debian-11.5.0-amd64-netinst.iso SHA256
SHA256 hash of debian-11.5.0-amd64-netinst.iso:
e307d0e583b4a8f7e5b436f8413d4707dd4242b70aea61eb08591dc0378522f3
CertUtil: -hashfile command completed successfully.

C:\Users\jnowak\Desktop\Pawlak>certutil -hashfile debian-11.5.0-amd64-netinst.iso SHA256 | findstr /v "hash"
e307d0e583b4a8f7e5b436f8413d4707dd4242b70aea61eb08591dc0378522f3

C:\Users\jnowak\Desktop\Pawlak>more SHA256SUMS.txt | findstr debian-11.5.0-amd64-netinst.iso
e307d0e583b4a8f7e5b436f8413d4707dd4242b70aea61eb08591dc0378522f3  debian-11.5.0-amd64-netinst.iso

C:\Users\jnowak\Desktop\Pawlak>
```

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

- import klucza publicznego

Verifying authenticity of Debian images

Official releases of Debian installation and live images come with signed checksum files, look for them in the download area. First of all, the checksum can be used to check that the images have not been tampered with, and have not been released by Debian, and have not been tampered with.

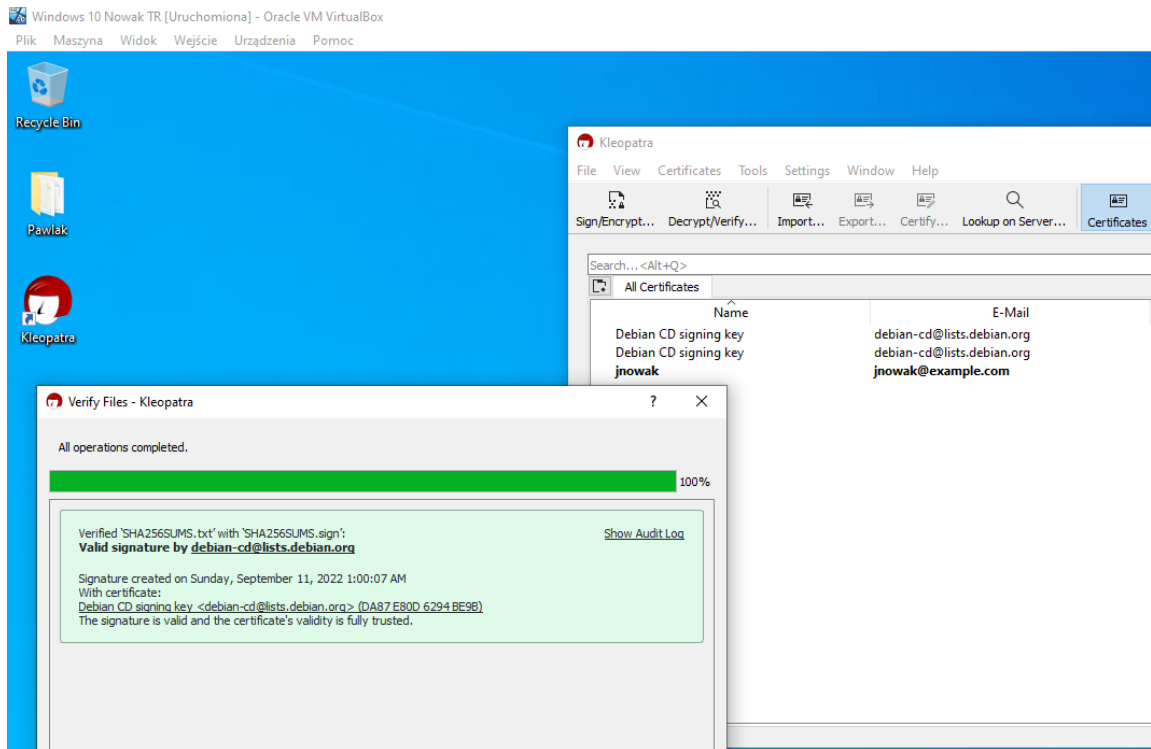
To validate the contents of an image file, be sure to use the appropriate checksum file. To ensure that the checksum files themselves are correct, use GnuPG to validate the contents of the checksum files. The best way to check them is to use that keyring to validate via the web of trust. To sign releases in recent years, and links to download the public keys directly:

```
pub rsa4096/988021A964E6EA7D 2009-10-03
Key fingerprint = 1046 0DAD 7616 5AD8 1FBC 0CE9 9880 21A9 64E6 EA7D
uid Debian CD signing key <debian-cd@lists.debian.org>

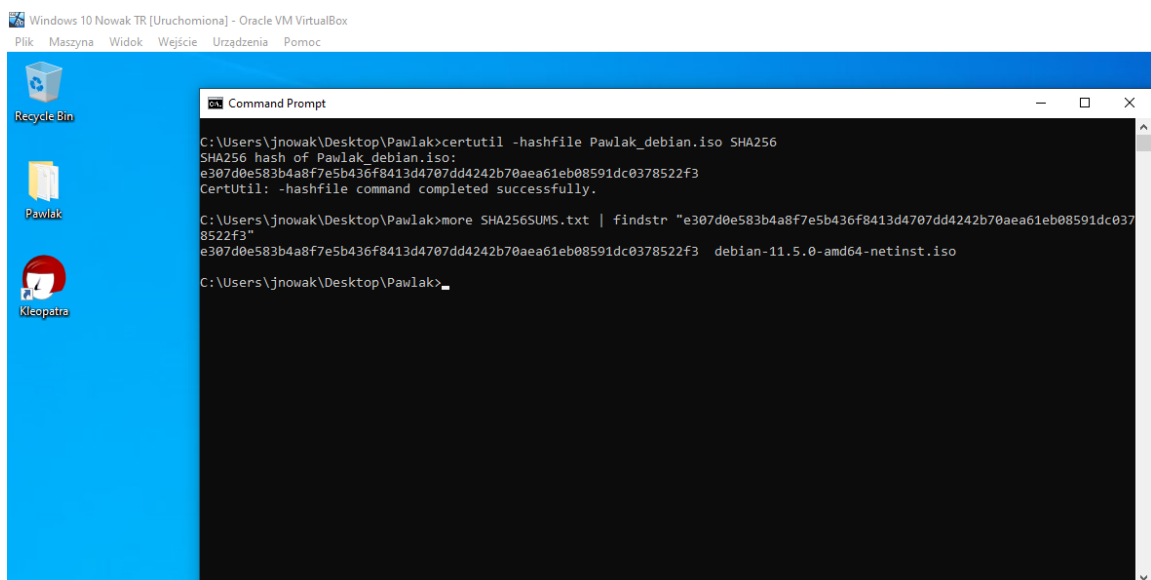
pub rsa4096/DA67E8006248E6E8 2011-01-05 [SC]
Key fingerprint = DF98 9C49 EAA0 2984 3258 9076 DAB7 E880 6294 BE98
uid Debian CD signing key <debian-cd@lists.debian.org>

pub rsa4096/42468FA009FABAC3 2014-04-15 [SC]
Key fingerprint = F41D 3034 2F35 4669 5F65 C669 4246 8F40 09EA 8AC3
uid Debian Testing CDs Automatic Signing Key <debian-cd@lists.debian.org>
```

- 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")

