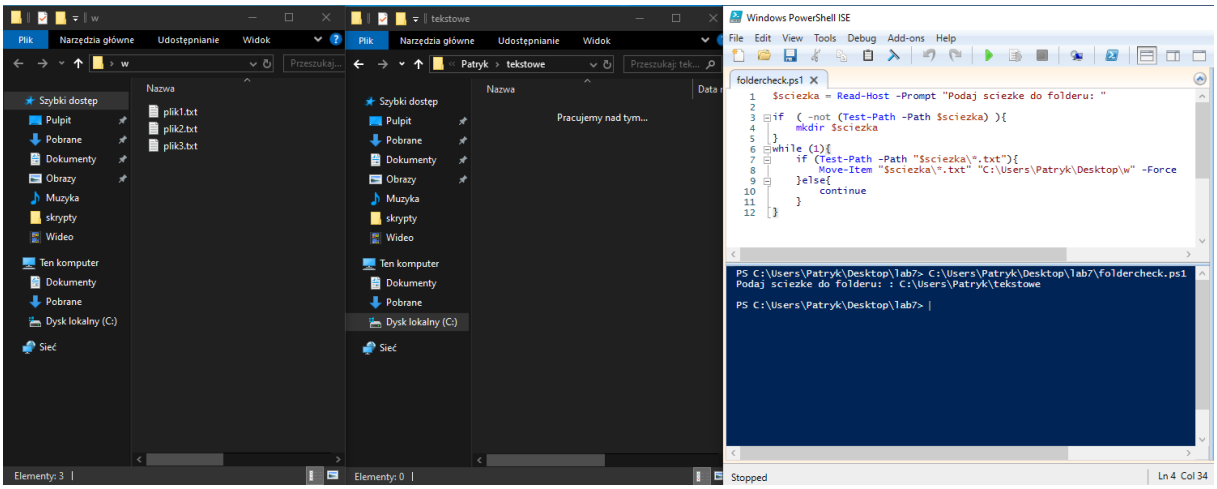
1. Napisz skrypt PowerShell, który monitoruje określony folder i automatycznie przenosi nowo dodane pliki .txt do innej lokalizacji.
   a) Jeżeli folder docelowy nie istnieje skrypt musi go utworzyć.
   b) Skrypt powinien działać ciągle aż do jego ręcznego wyłączenia.

```powershell
$sciezka = Read-Host -Prompt "Podaj sciezke do folderu: "

if  ( -not (Test-Path -Path $sciezka) ){
    mkdir $sciezka
}
while (1){
    if (Test-Path -Path "$sciezka\*.txt"){
        Move-Item "$sciezka\*.txt" "C:\Users\Patryk\Desktop\w" -Force
    }else{
        continue
    }
}
```



2. Napisz skrypt w PowerShell który:
   a) Obliczy sumę kontrolną pliku (MD5 lub SHA256).
   b) Wyśle zapytanie do API VirusTotal
   c) Zinterpretuje odpowiedź API i wyświetli informację, czy plik jest bezpieczny, czy nie.

```powershell
#Skrypt przyjmuje argument ze sciezka do pliku
param(
    $plik
)

#Obliczamy hash pliku
$hash = Get-FileHash -Algorithm SHA256 -Path $plik | Select-Object -ExpandProperty Hash

#Przypisujemy odpowiednie naglówki
$headers=@{}
$headers.Add("accept", "application/json")
$headers.Add("x-apikey", "f5269e38dd5a80f21f792c7ff31afd13fcc58aceba453f260abe388bd380850f")

#Wysyłamy zapytanie do VirusTotala
$response = Invoke-WebRequest -Uri "https://www.virustotal.com/api/v3/files/$hash"  -Method GET -Headers $headers | ConvertFrom-Json

#Po pomyślnym uzyskaniu odpowiedzi sprawdzamy czy aplikacja wykryła jakieś zgrożenia
$stat = $response.data.attributes.last_analysis_stats.malicious
if ($stat -gt 0){
    Write-Host "Plik jest szkodliwy!"
}else{
    Write-Host "Plik jest nieszkodliwy!"
}
```

Wynik dla pliku EICAR

virustotal.ps1

```powershell
#Skrypt przyjmuje argument ze sciezka do pliku
param(
    $plik
)

#Obliczamy hash pliku
$hash = Get-FileHash -Algorithm SHA256 -Path $plik | Select-Object -ExpandProperty Hash

#Przypisujemy odpowiednie naglówki
$headers=@{}
$headers.Add("accept", "application/json")
$headers.Add("x-apikey", "f5269e38dd5a80f21f792c7ff31afd13fcc58aceba453f260abe388bd380850f")

#Wysyłamy zapytanie do VirusTotala
$response = Invoke-WebRequest -Uri "https://www.virustotal.com/api/v3/files/$hash"  -Method GET -Headers $headers | ConvertFrom-Json

#Po pomyślnym uzyskaniu odpowiedzi sprawdzamy czy aplikacja wykryła jakieś zgrożenia
$stat = $response.data.attributes.last_analysis_stats.malicious
if ($stat -gt 0){
    Write-Host "Plik jest szkodliwy!"
}else{
    Write-Host "Plik jest nieszkodliwy!"
}
```

```
PS C:\Users\Patryk\Desktop\lab7>
PS C:\Users\Patryk\Desktop\lab7> .\virustotal.ps1 eicar.txt
Plik jest szkodliwy!
```

Wynik dla zwykłego pliku

virustotal.ps1

```powershell
#Skrypt przyjmuje argument ze sciezka do pliku
param(
    $plik
)

#Obliczamy hash pliku
$hash = Get-FileHash -Algorithm SHA256 -Path $plik | Select-Object -ExpandProperty Hash

#Przypisujemy odpowiednie naglówki
$headers=@{}
$headers.Add("accept", "application/json")
$headers.Add("x-apikey", "f5269e38dd5a80f21f792c7ff31afd13fcc58aceba453f260abe388bd380850f")

#Wysyłamy zapytanie do VirusTotala
$response = Invoke-WebRequest -Uri "https://www.virustotal.com/api/v3/files/$hash"  -Method GET -Headers $headers | ConvertFrom-Json

#Po pomyślnym uzyskaniu odpowiedzi sprawdzamy czy aplikacja wykryła jakieś zgrożenia
$stat = $response.data.attributes.last_analysis_stats.malicious
if ($stat -gt 0){
    Write-Host "Plik jest szkodliwy!"
}else{
    Write-Host "Plik jest nieszkodliwy!"
}
```

```
PS C:\Users\Patryk\Desktop\lab7> .\virustotal.ps1 .\plik.txt
Plik jest nieszkodliwy!

PS C:\Users\Patryk\Desktop\lab7>
```