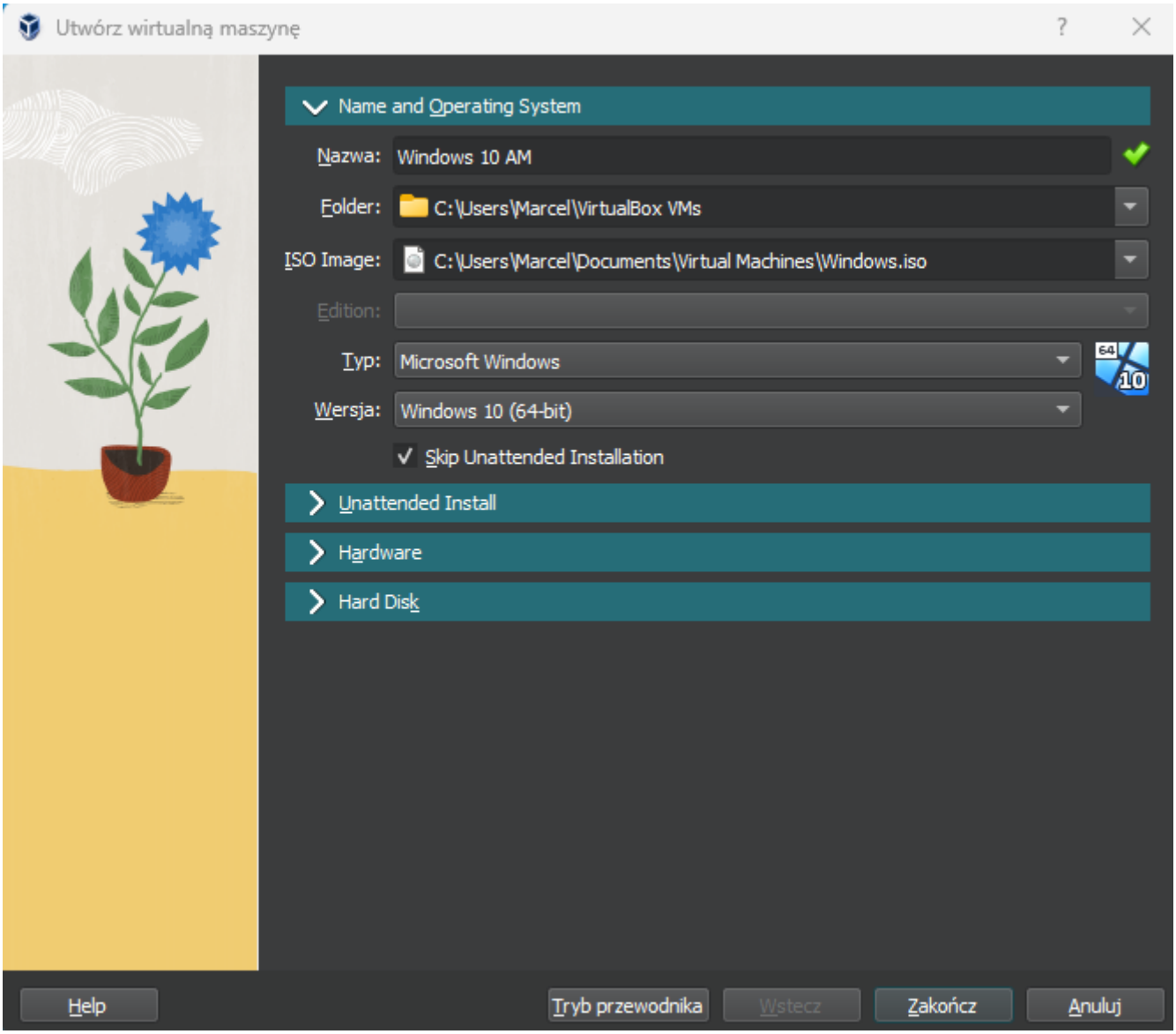
Przygotowanie środowiska do Analizy Malware

Instalacja Systemu Windows 10

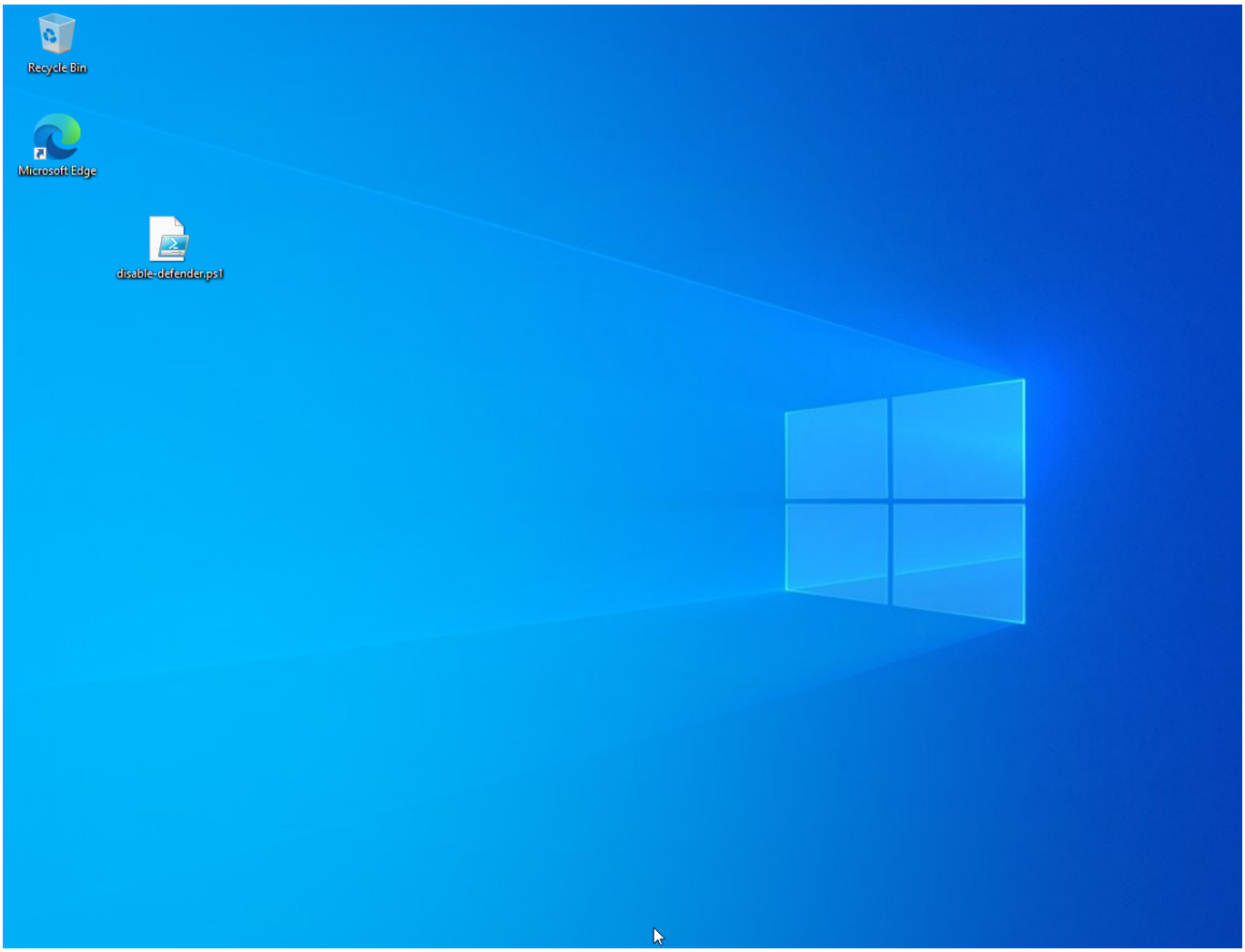


Dla systemu windows należy przeznaczyć conajmniej 60 GB miejsca na dysku
Ja przeznaczyłem:

- 80 GB miejsca na dysku
- 8 GB pamięci RAM
- 6 wątków procesora

Następnie należy przejść przez proces instalacji

Po udanej instalacji mamy gotowy system Windows 10



Instalacja Flare VM

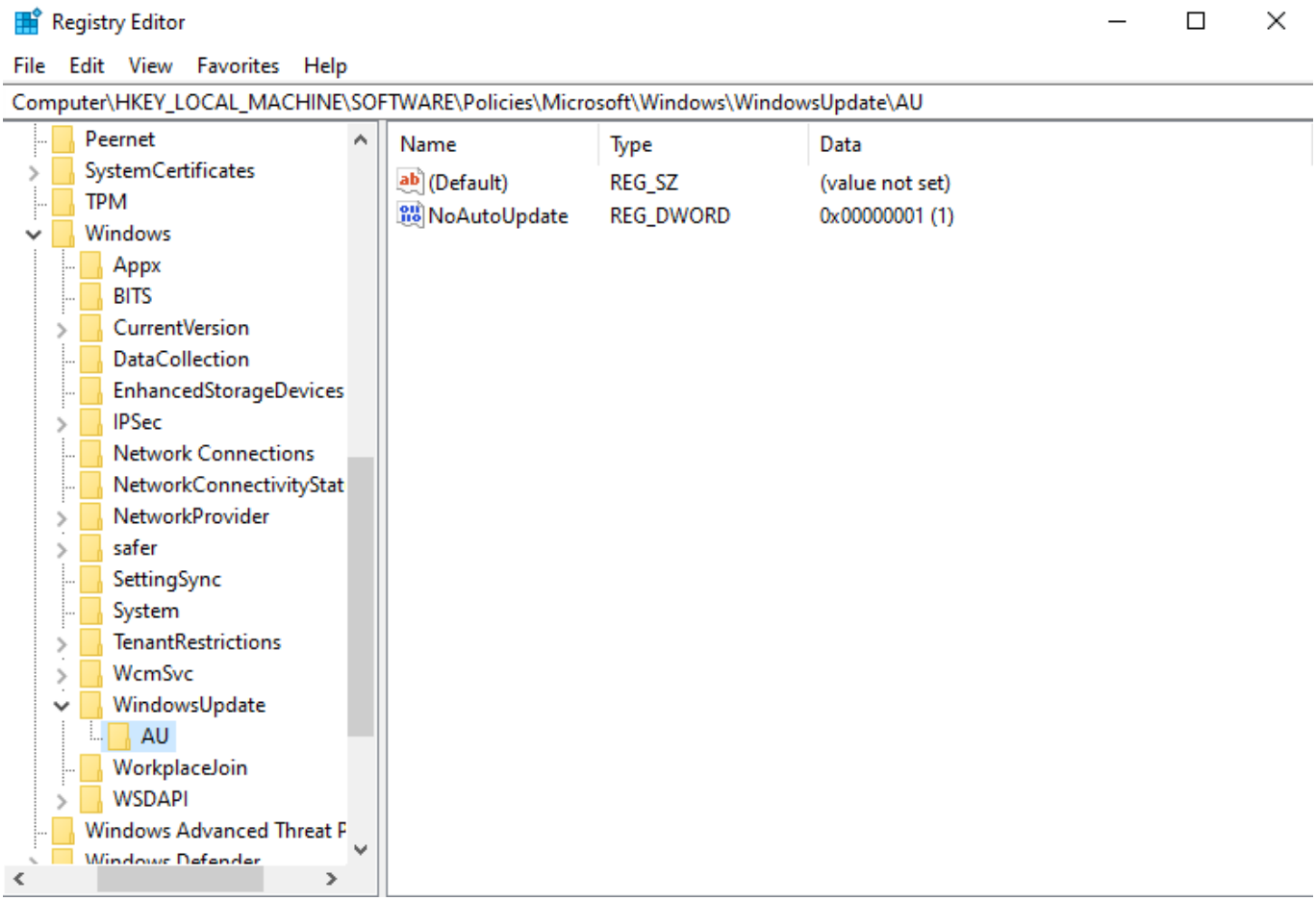
Zanim zainstaluje się środowisko Flare VM, należy przejść przez kilka kroków

Wyłączenie Windows Update

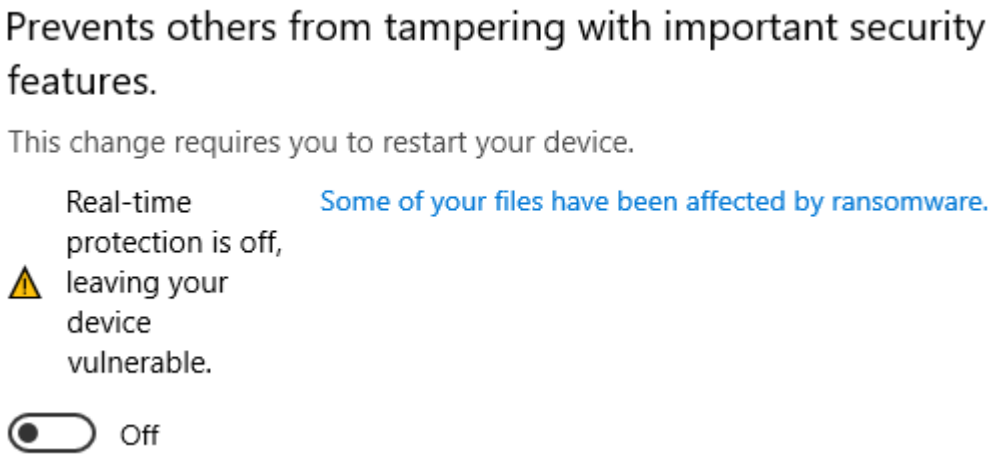
Windows Update można wyłączyć na 2 sposoby

- Group Policy Edit (Wymagany Windows Pro)
- Windows Registry

Ja miałem problem z użyciem GPE, dlatego dodałem klucz do rejestru za pomocą poradnika



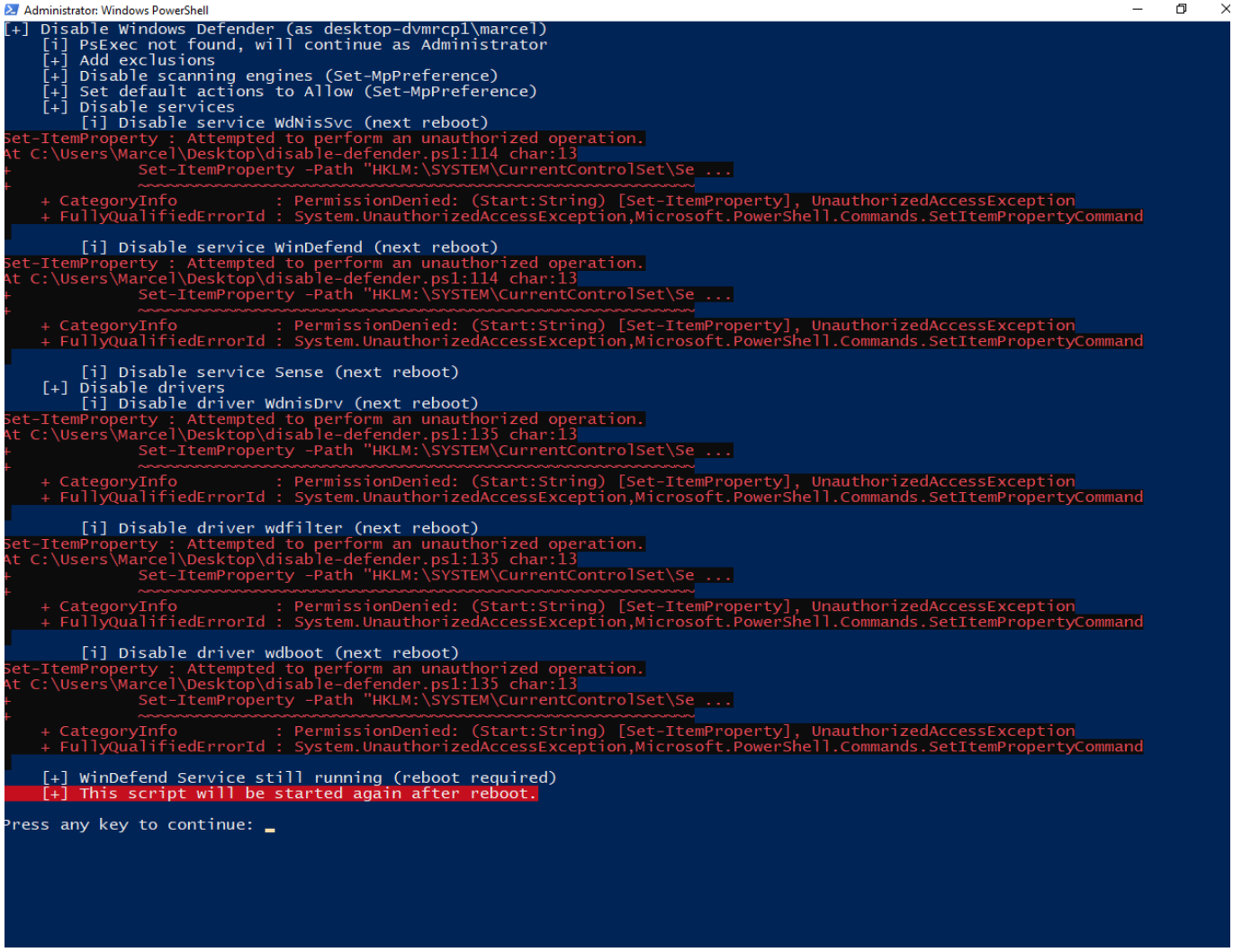
Wyłączenie Tamper Protection



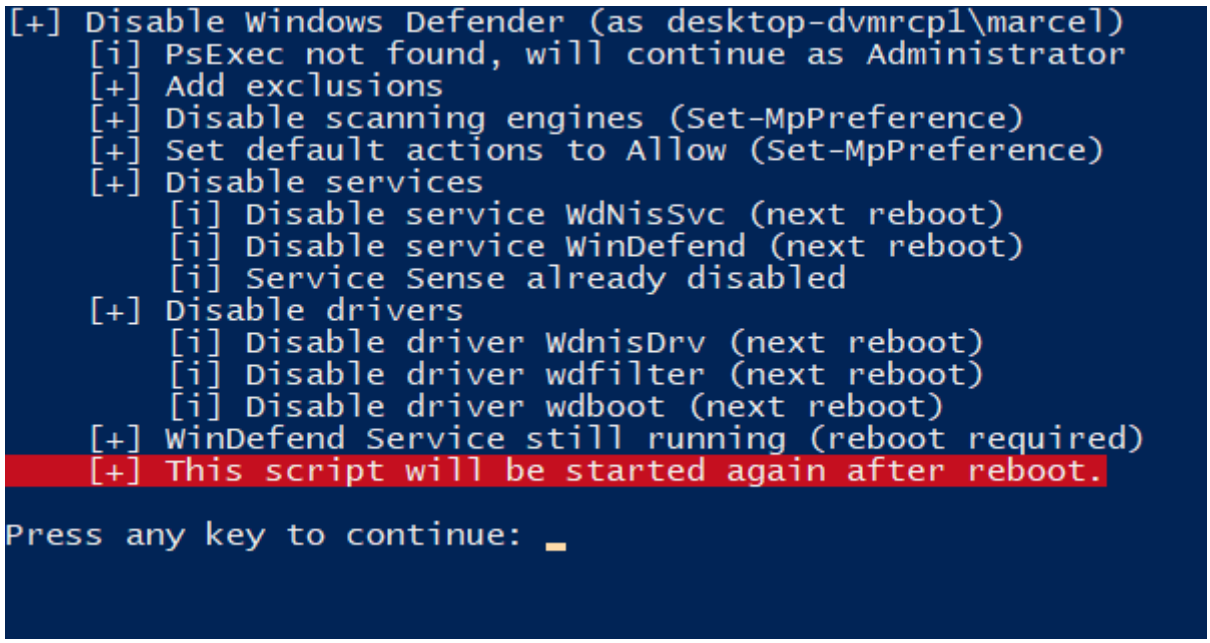
Wyłaczenie Windows Defender

Ostatnim krokiem przed instalacją Flare VM jest wyłączenie Windows Defendera

Posłużyłem się do tego skryptem, który automatycznie go wyłącza



Skrypt potrzebuje 5 cykli restartowania, aby wyłączyć winodows defender całkowicie



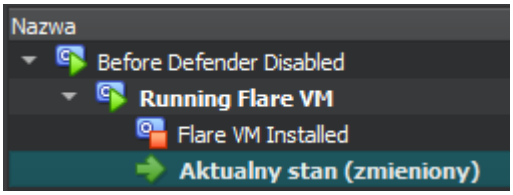
Skrypt powinien bez problemów wyłączyć Windows Defender

Flare VM

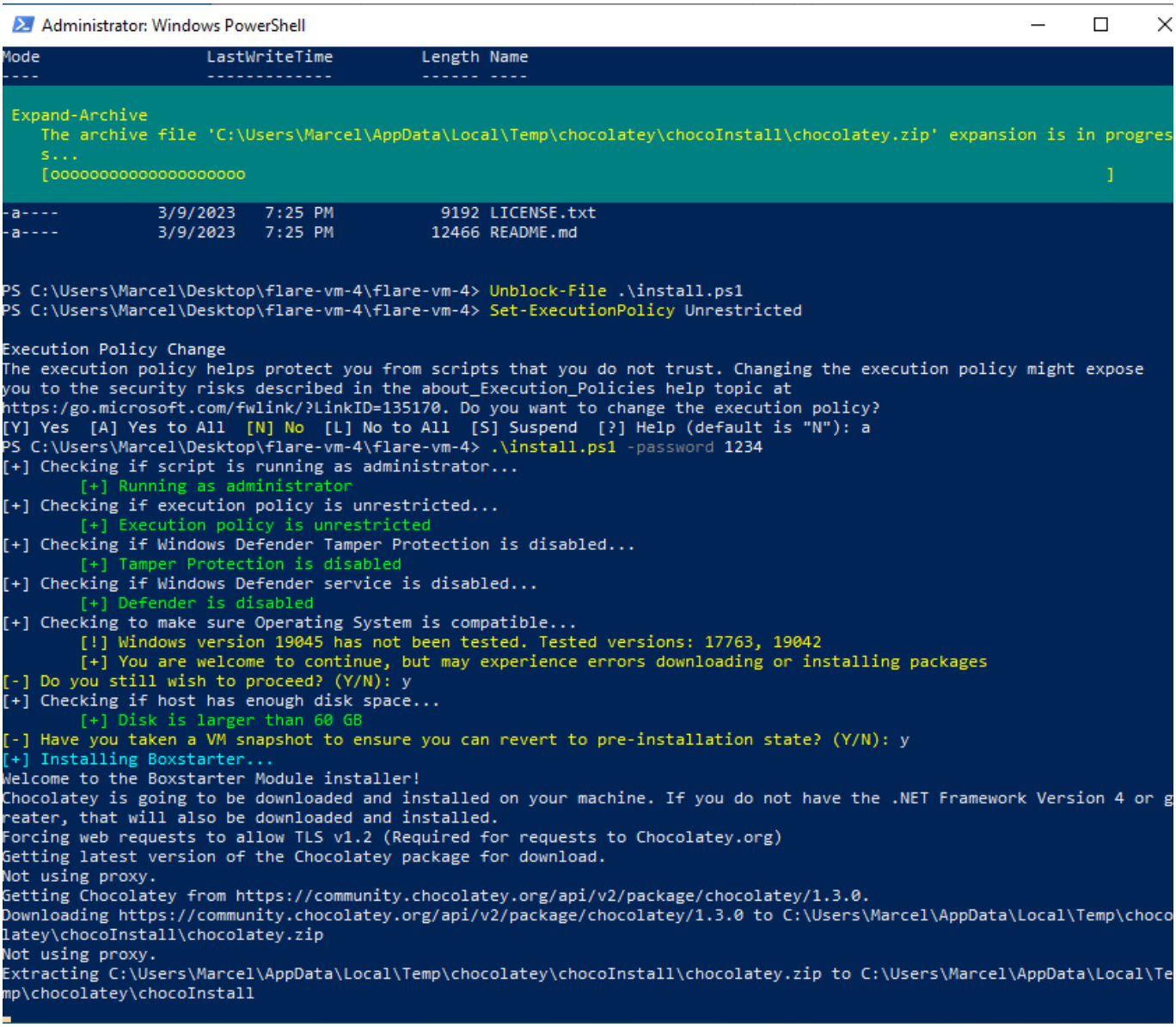
Aby zainstalować Flare VM, sklonowalem repo, wykonałem polecenia z instrukcji instalacji, a następnie włączyłem skrypt

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          3/9/2023   7:25 PM                flare-vm-4


PS C:\Users\Marcel\Desktop\flare-vm-4> cd .\flare-vm-4\
PS C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4> ls


    Directory: C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          3/9/2023   7:25 PM            550 .gitattributes
-a----          3/9/2023   7:25 PM            469 .gitignore
-a----          3/9/2023   7:25 PM           1851 config.xml
-a----          3/9/2023   7:25 PM          13129 flarevm.png
-a----          3/9/2023   7:25 PM          45869 install.ps1
-a----          3/9/2023   7:25 PM         162897 installer_gui.png
-a----          3/9/2023   7:25 PM           9192 LICENSE.txt
-a----          3/9/2023   7:25 PM          12466 README.md


PS C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4> Unblock-File .\install.ps1
PS C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): a
PS C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4> .\install.ps1 -password 1234
[+] Checking if script is running as administrator...
        [+] Running as administrator
[+] Checking if execution policy is unrestricted...
        [+] Execution policy is unrestricted
[+] Checking if Windows Defender Tamper Protection is disabled...
        [+] Tamper Protection is disabled
[+] Checking if Windows Defender service is disabled...
        [+] Defender is disabled
[+] Checking to make sure Operating System is compatible...
        [!] Windows version 19045 has not been tested. Tested versions: 17763, 19042
        [+] You are welcome to continue, but may experience errors downloading or installing packages
[-] Do you still wish to proceed? (Y/N): y
[+] Checking if host has enough disk space...
        [+] Disk is larger than 60 GB
[-] Have you taken a VM snapshot to ensure you can revert to pre-installation state? (Y/N):
```

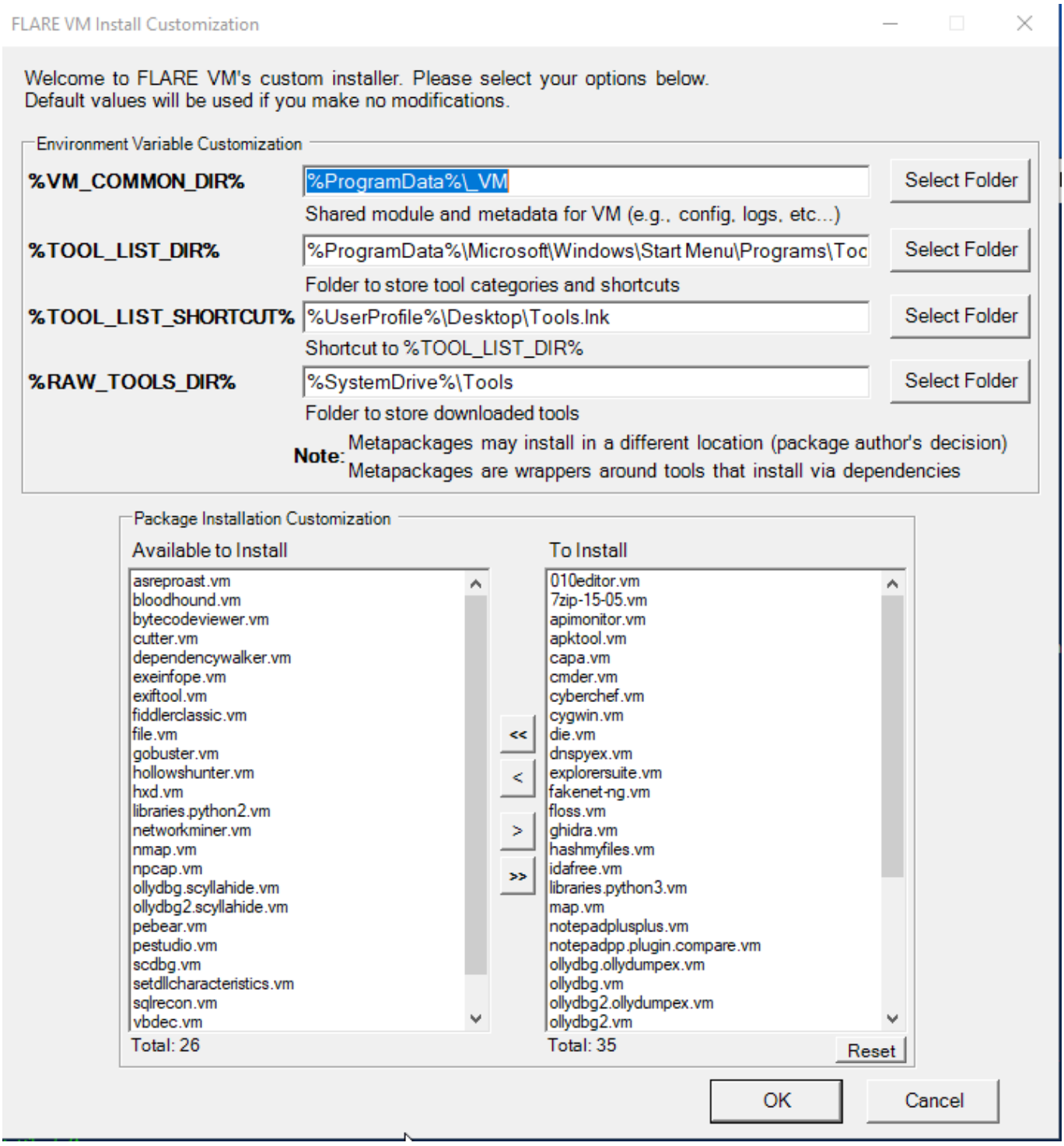
Skrypt upewnia się, że zrobiliśmy migawkę (snapshota) przed instalacją



Skrypt instaluje teraz Boxstartera oraz Chocolatey



Okienko z wyborem narzędzi do zainstalowania



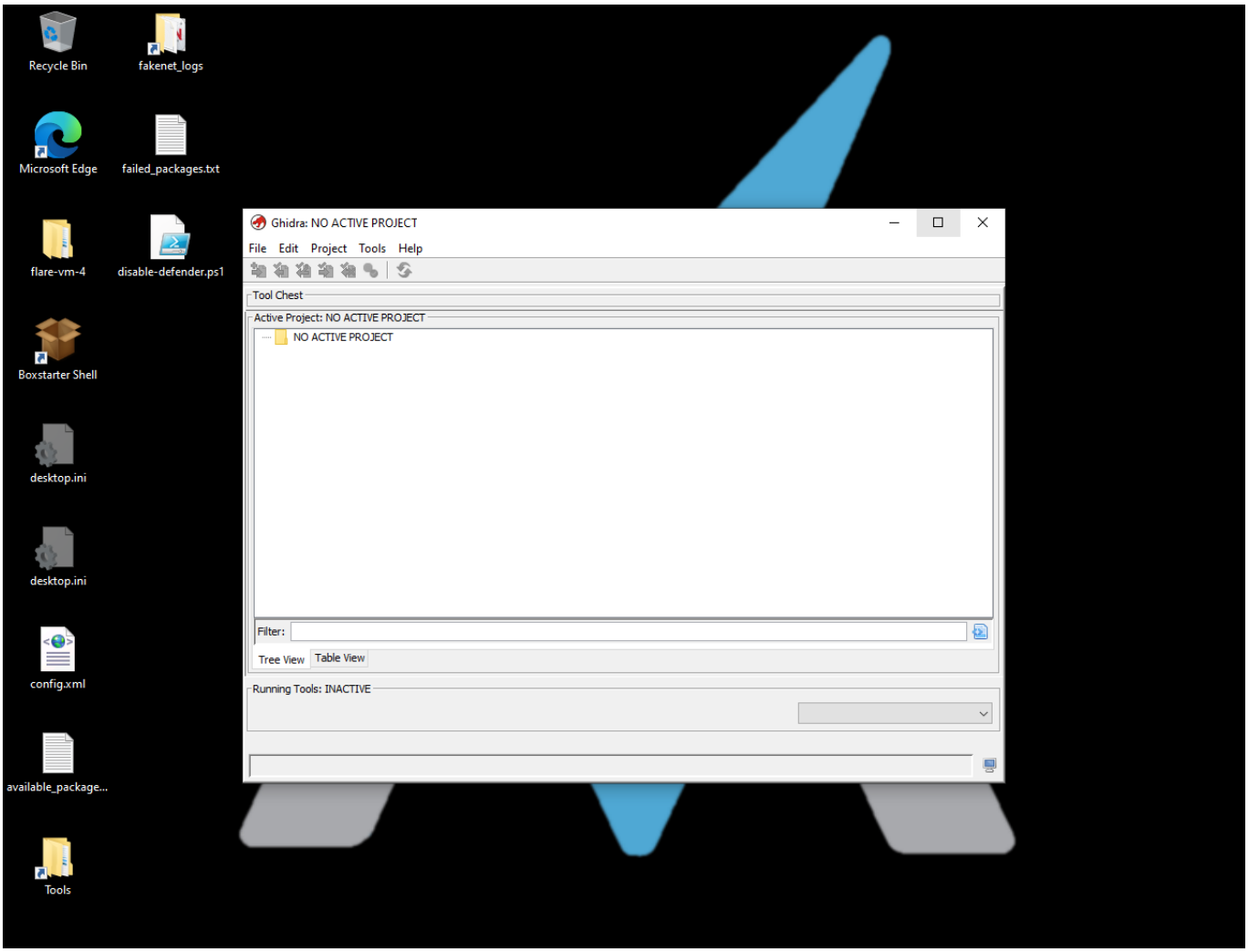
Po wyborze narzędzi została przeprowadzona instalacja narzędzi, która potrwała kilkadziesiąt minut

Po instalacji tak powinno wyglądać gotowe środowisko

Pozostałe kroki

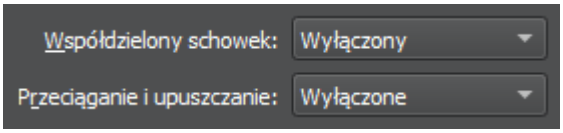
Ghidra

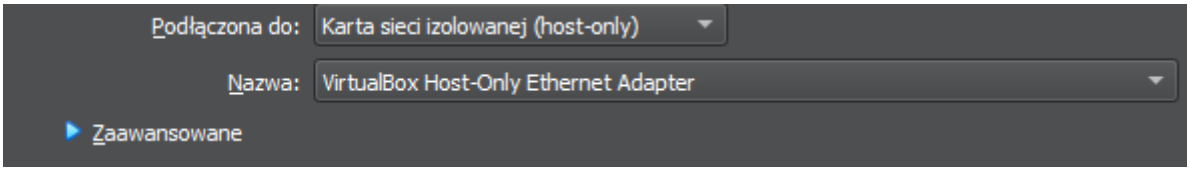
Programu Ghidra nie trzeba pobierać, ponieważ został już zainstalowany wraz z Flare VM



Izolacja Maszyny

Aby malware nie miał dostępu do Hosta należy go od niego jak najbardziej odseparować

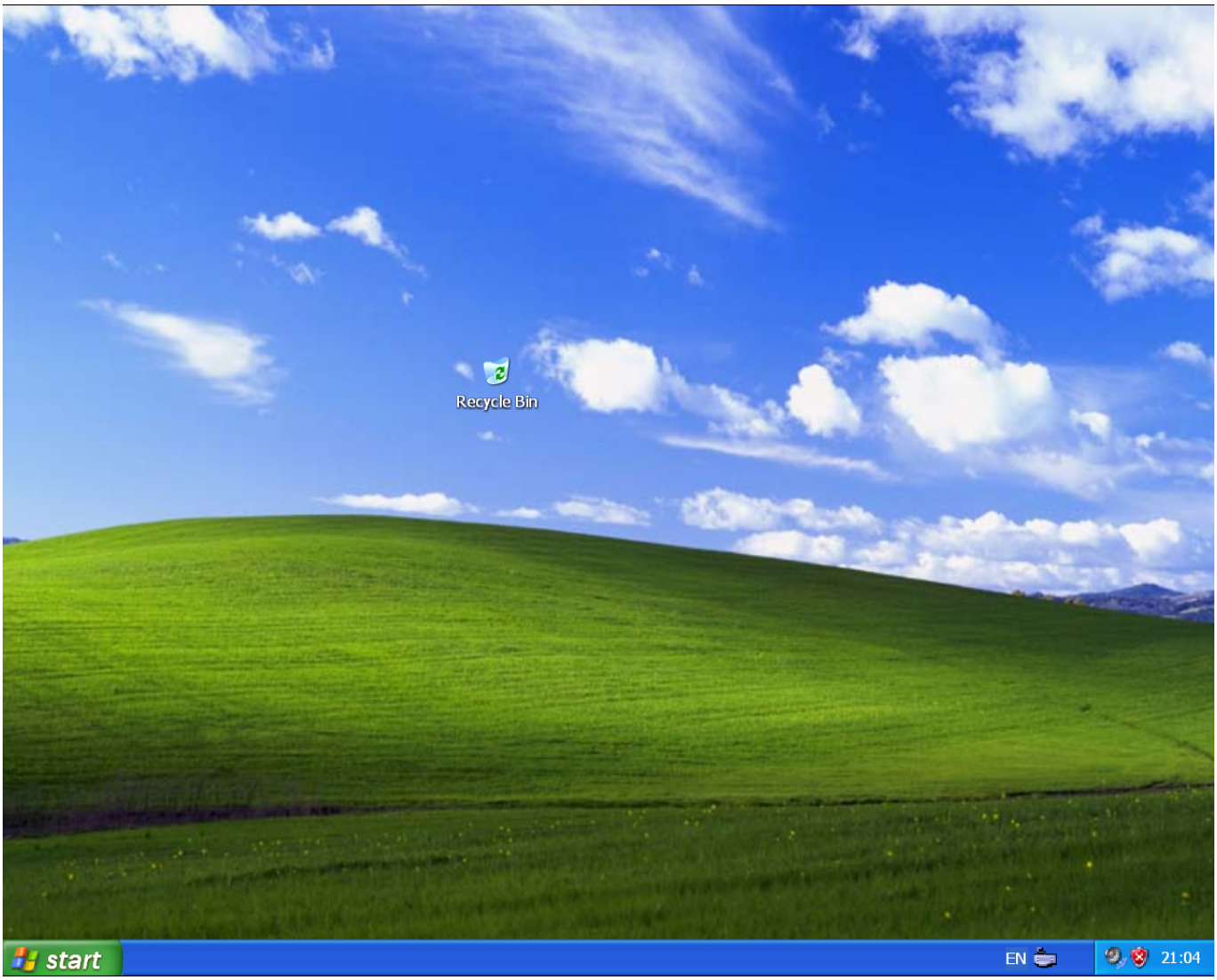




Windows XP

Na potrzeby labów 3+ zainstalowałem również Windows XP

Do aktywacji użyłem klucza
B2RBK-7KPT9-4JP6X-QQFWM-PJD6G
Klucz działa dla każdej instalacji Windowsa XP



Podsumowanie

- Windows Defender wyłączony
- Maszyna FlareVM do analizy malware została zainstalowana bez problemów
- Maszyna jest odizolowana od sieci oraz systemu Hosta
- Potrzebne narzędzia zostały zainstalowane
- Windows XP zainstalowany