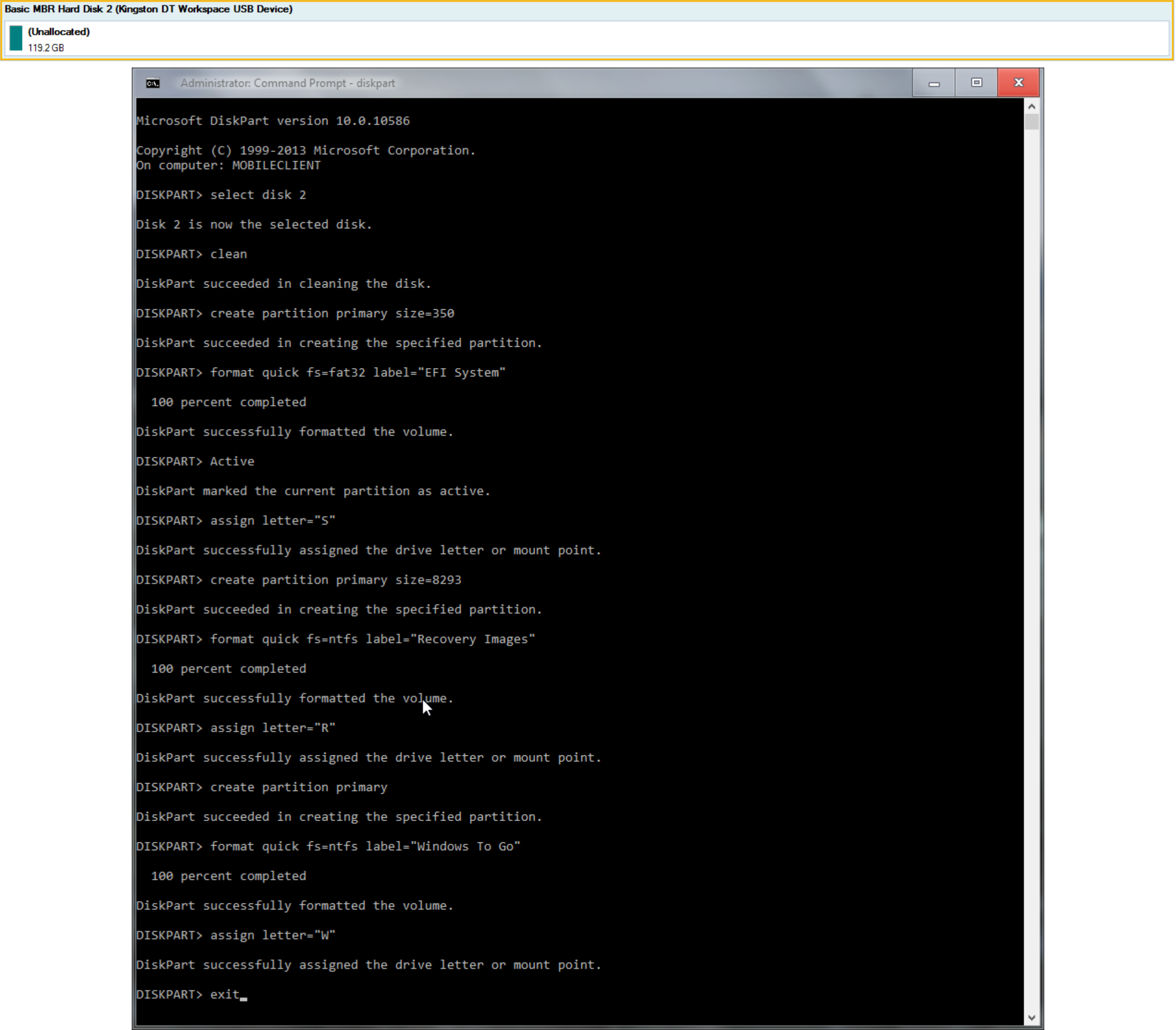


# CREATING A MULTI-BOOT WINDOWS TO GO DRIVE

This requires a USB device that shows up as a fixed disk, Normal USB keys will not work as multiple partitions are needed  
Any external HDD will work though.

First initialize the disk as MBR and clean the disk.



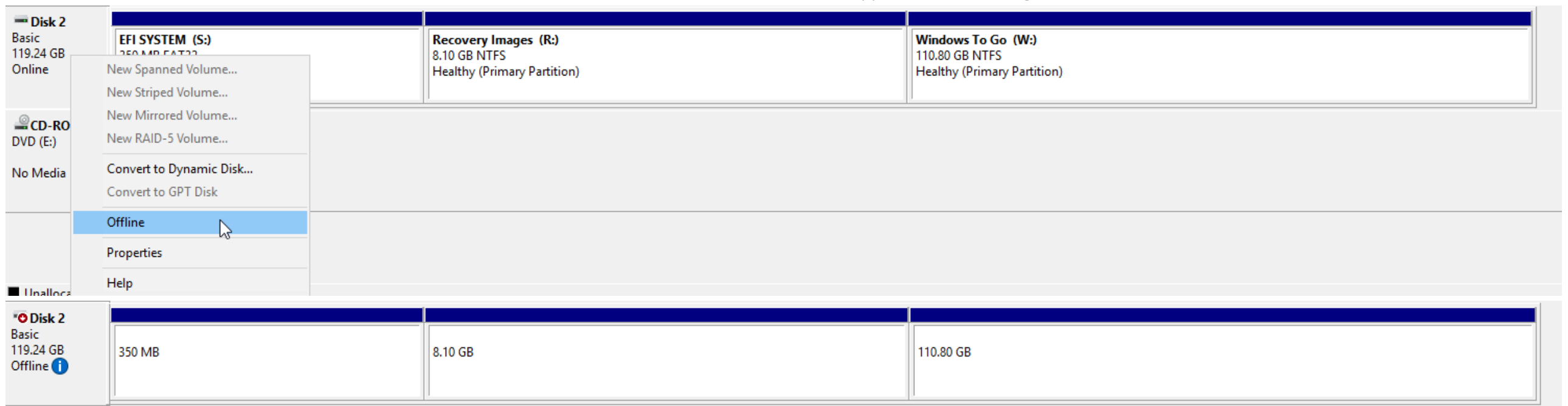
Now create the partitions, the code I used was

```
diskpart
select disk 2
clean
create partition primary size=350
format quick fs=fat32 label="EFI System"
Active
assign letter="S"
create partition primary size=8293
format quick fs=ntfs label="Recovery Images"
assign letter="R"
create partition primary
format quick fs=ntfs label="Windows To Go"
assign letter="W"
exit
```

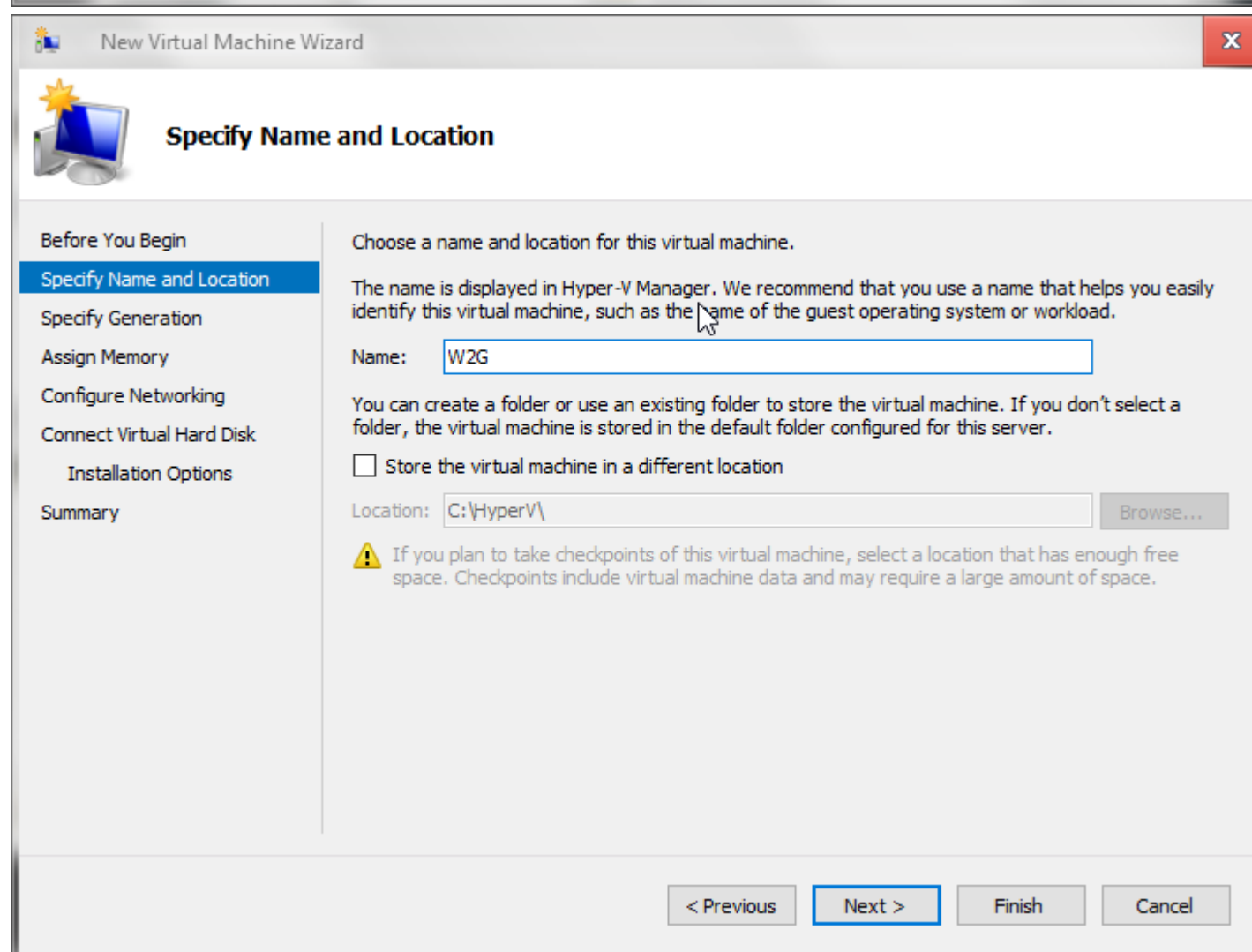
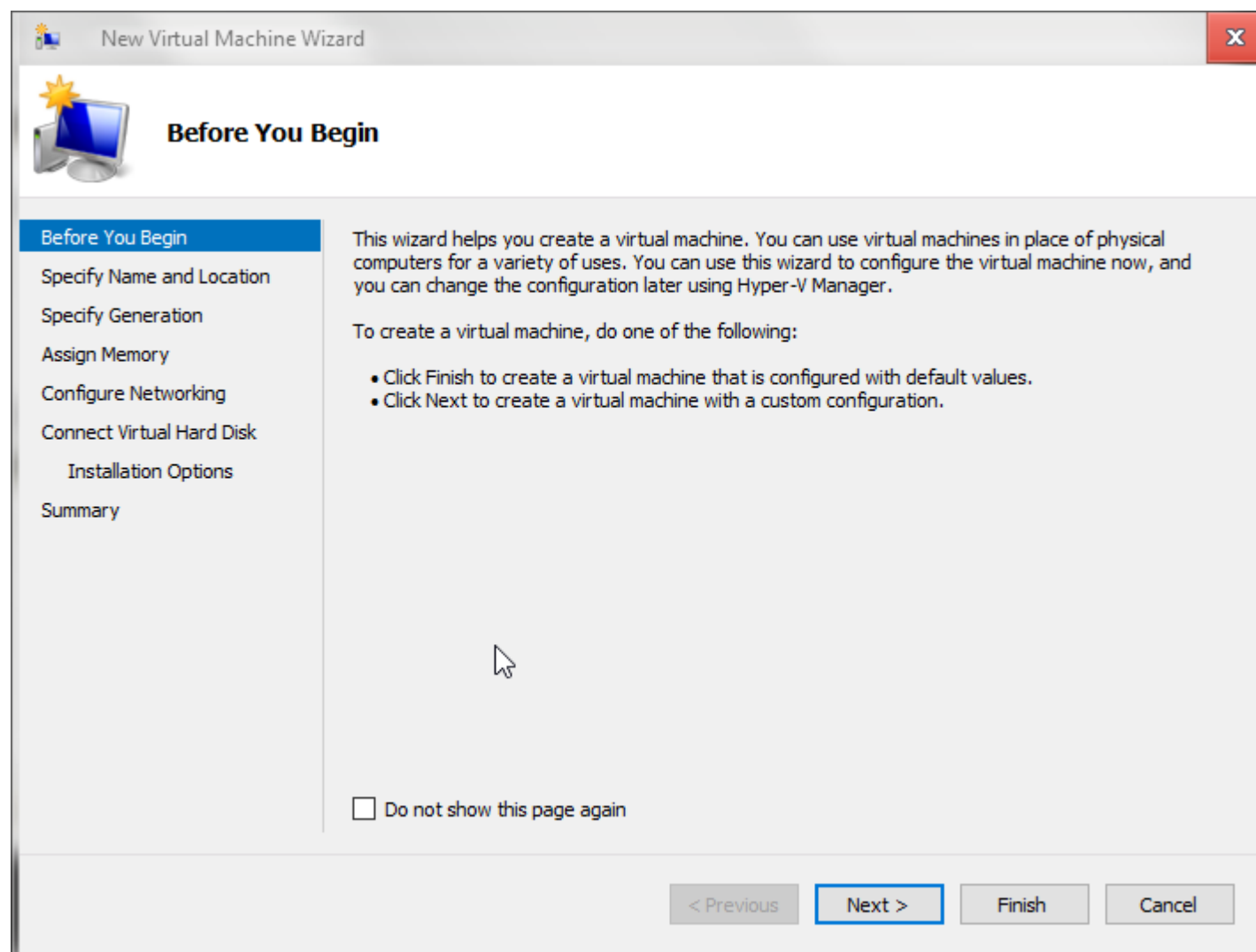
This gives 3 partitions

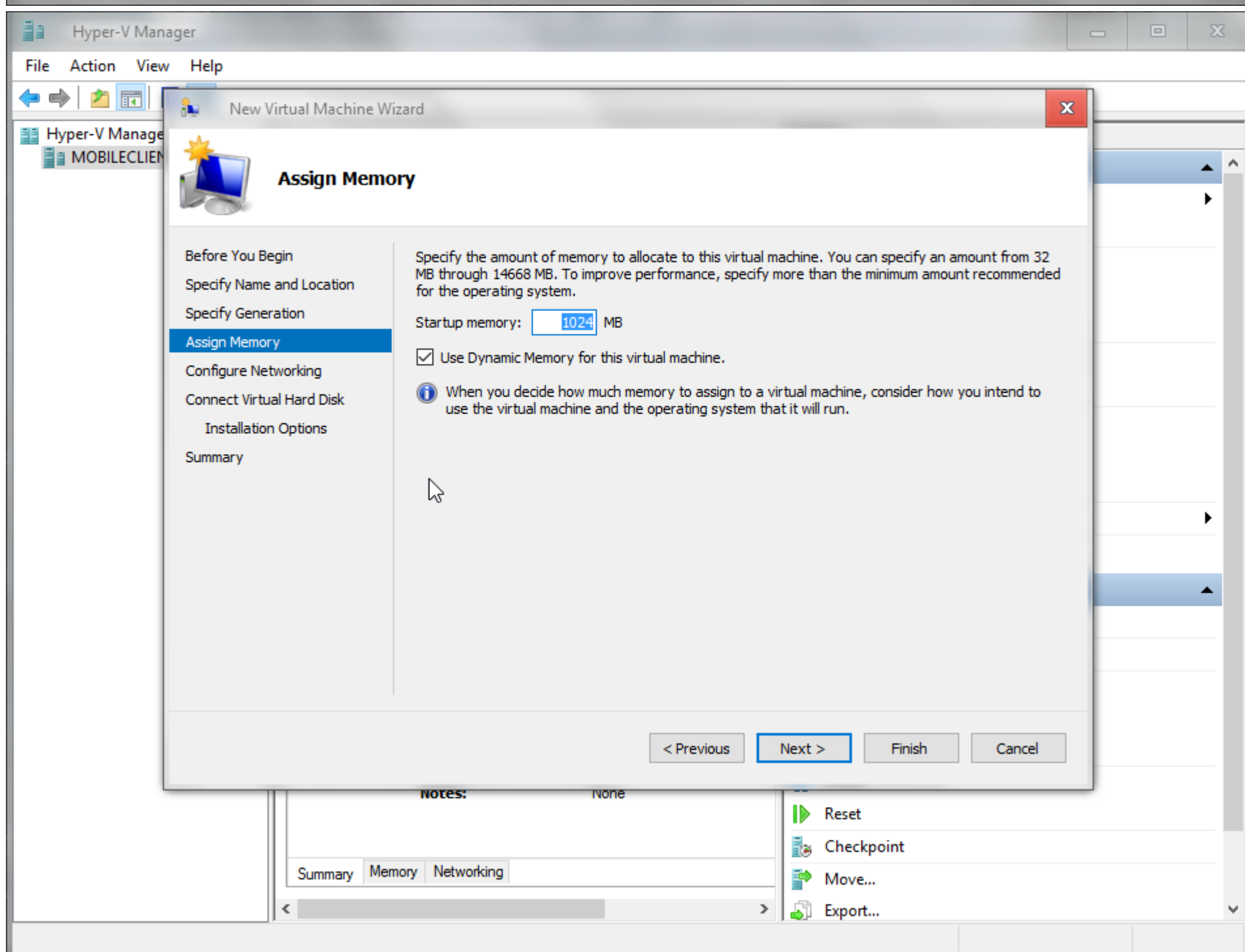
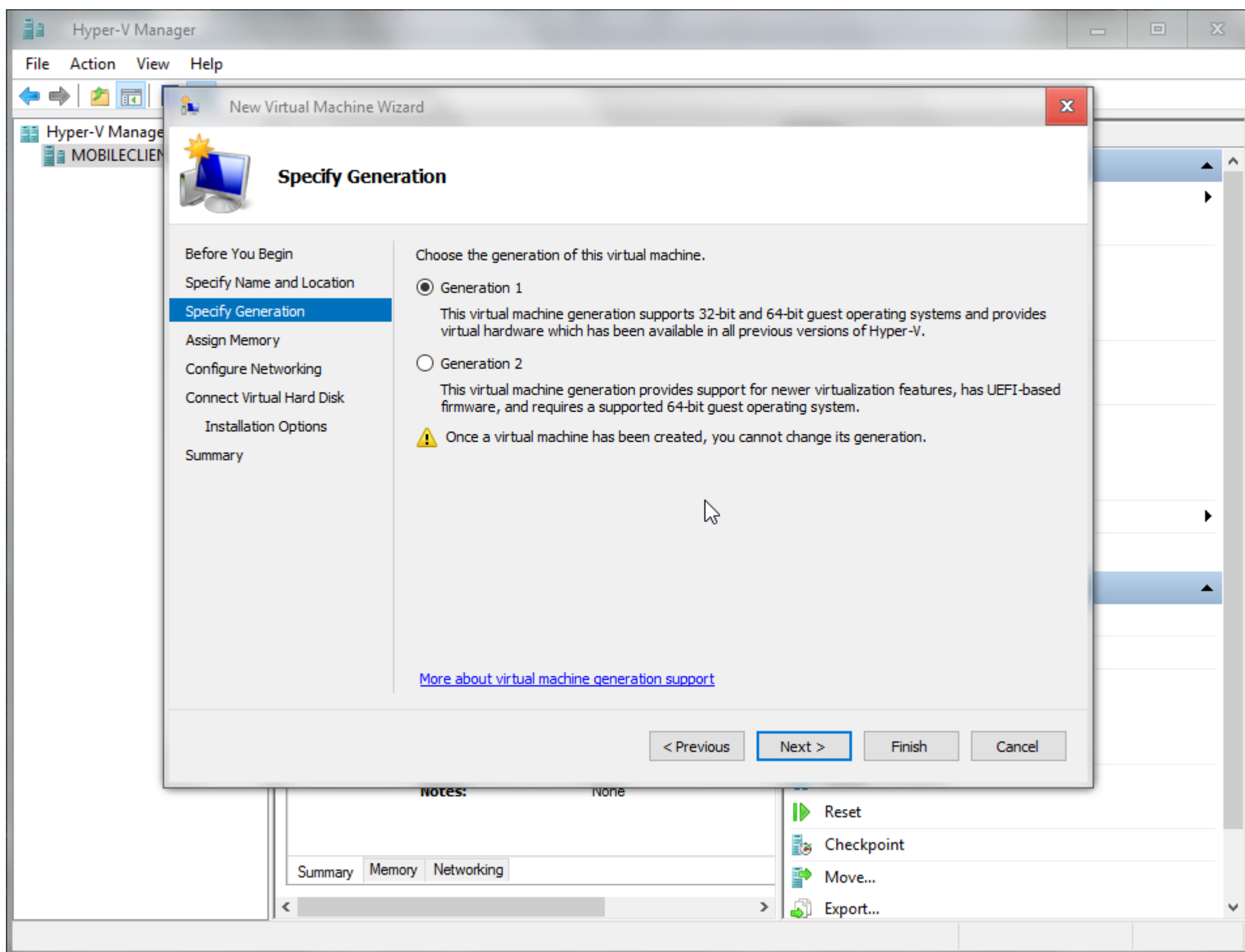


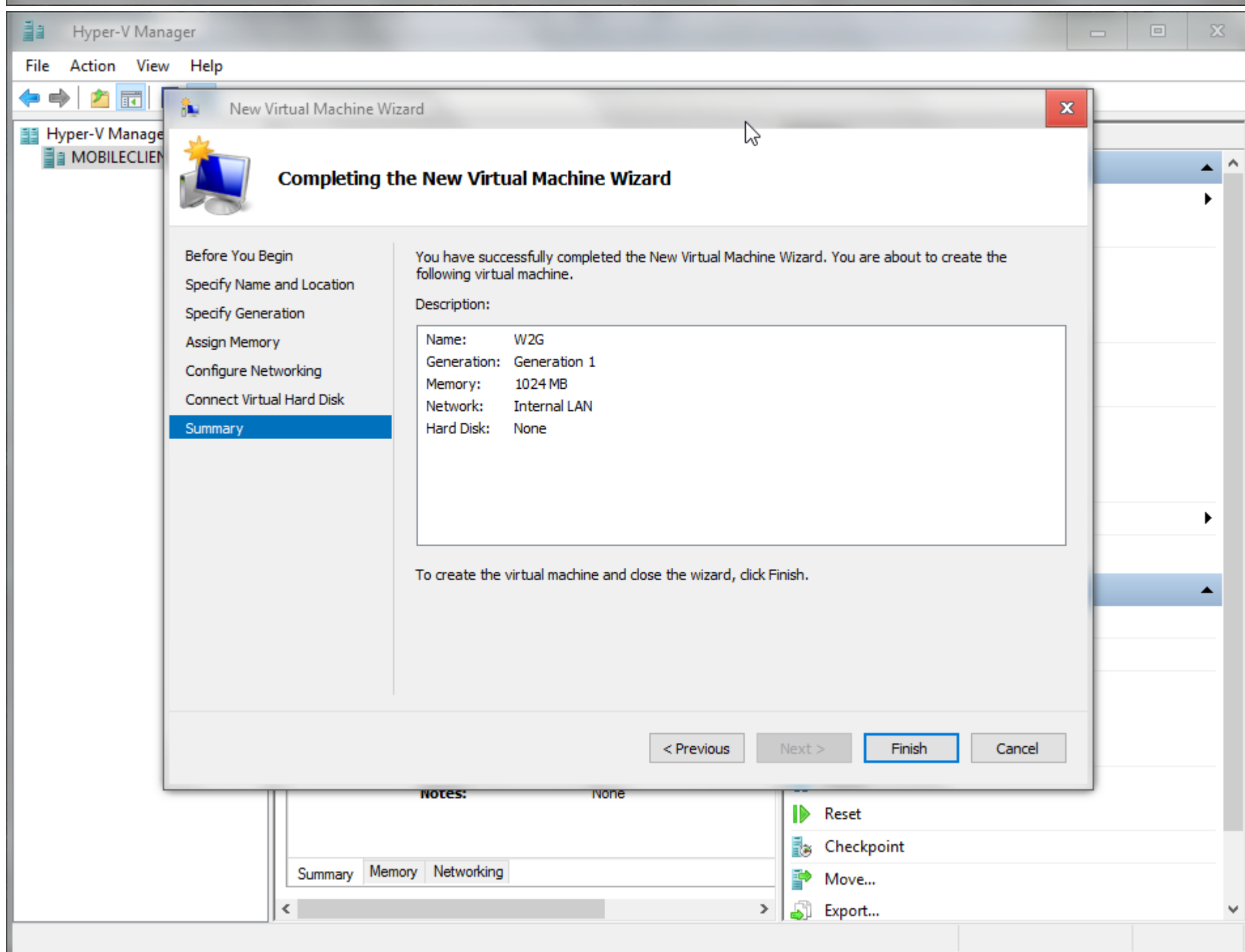
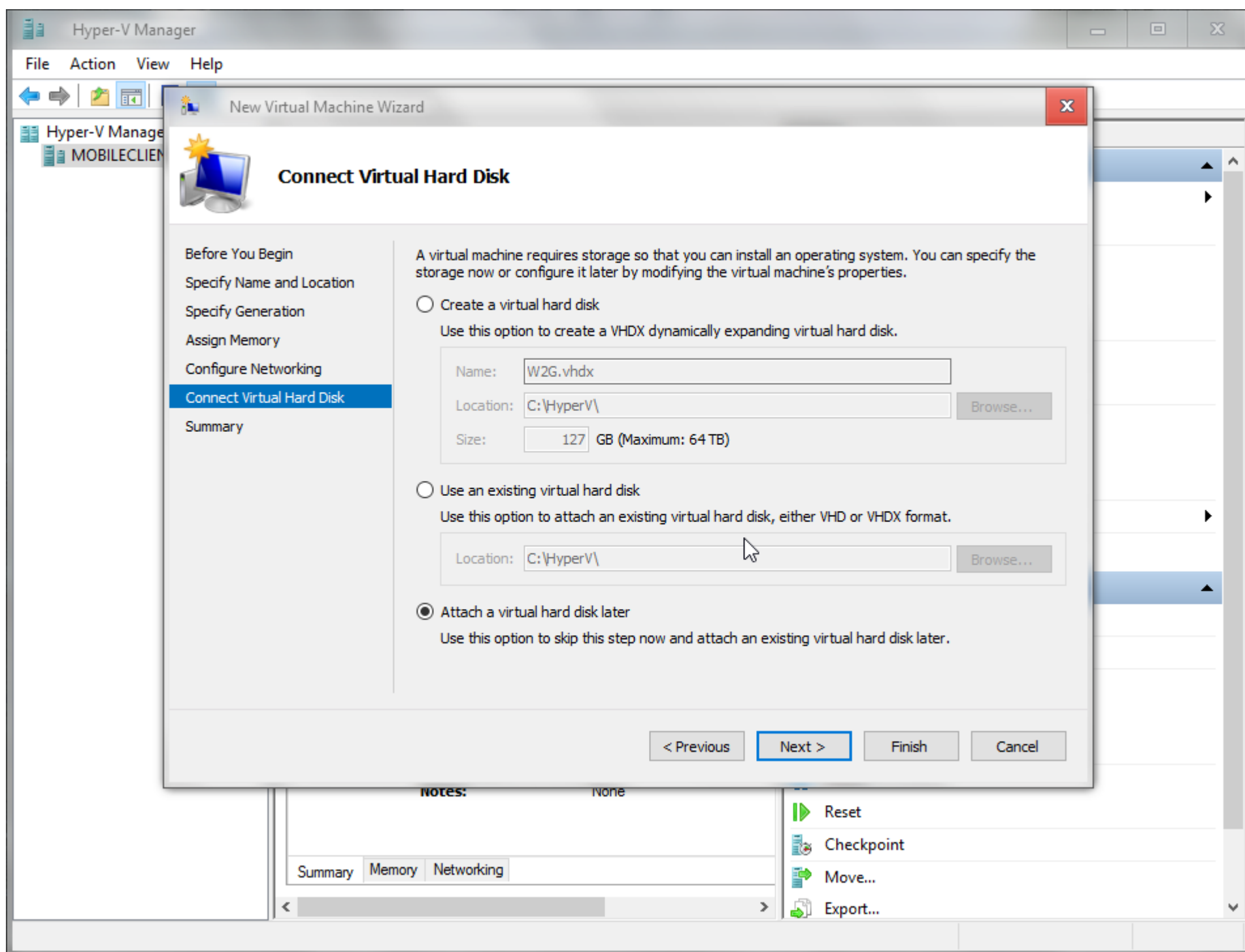
Now take the drive offline so it can be used in HyperV for testing and installation.



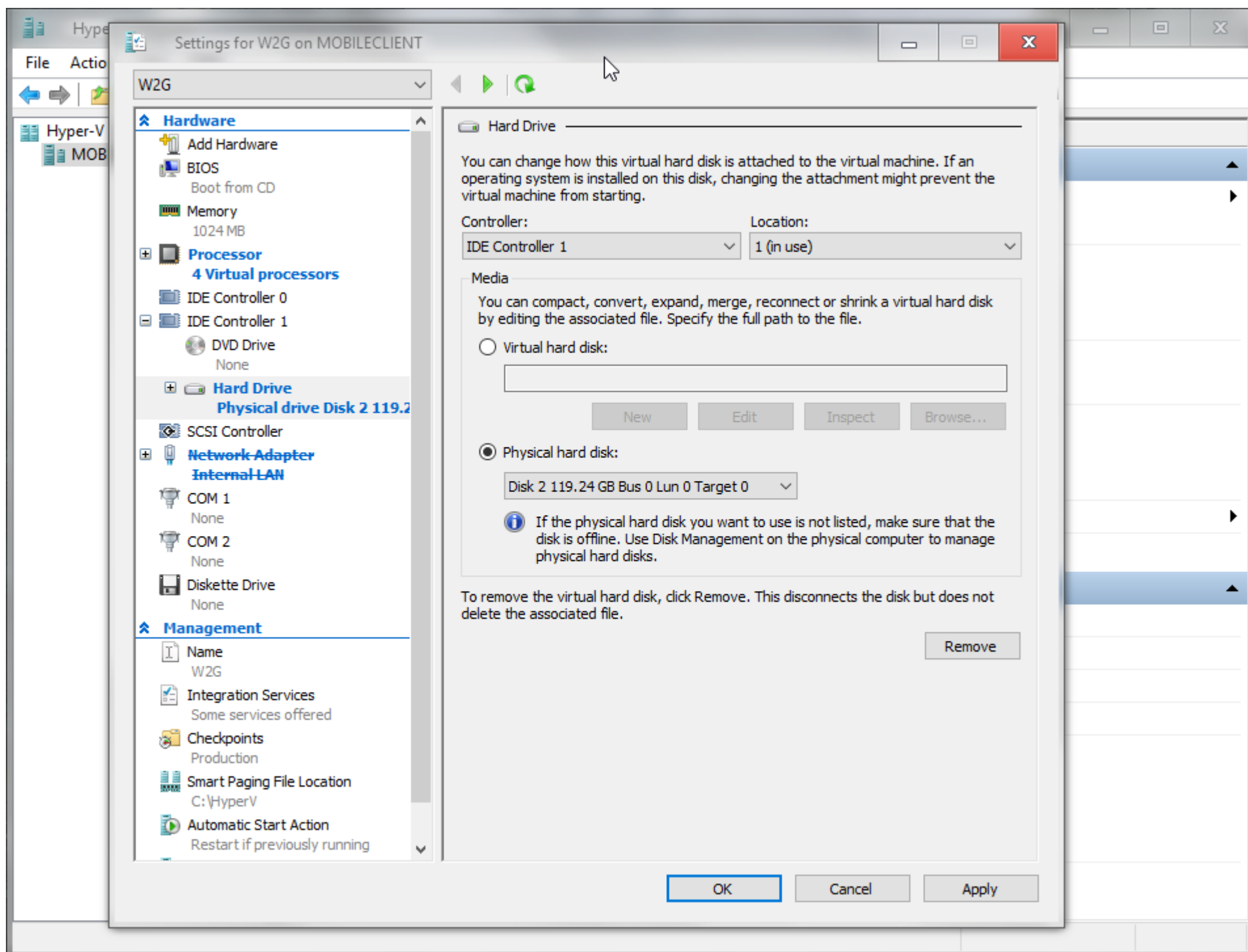
### Create a Gen 1 VM







Add the W2G drive as a passthrough drive.



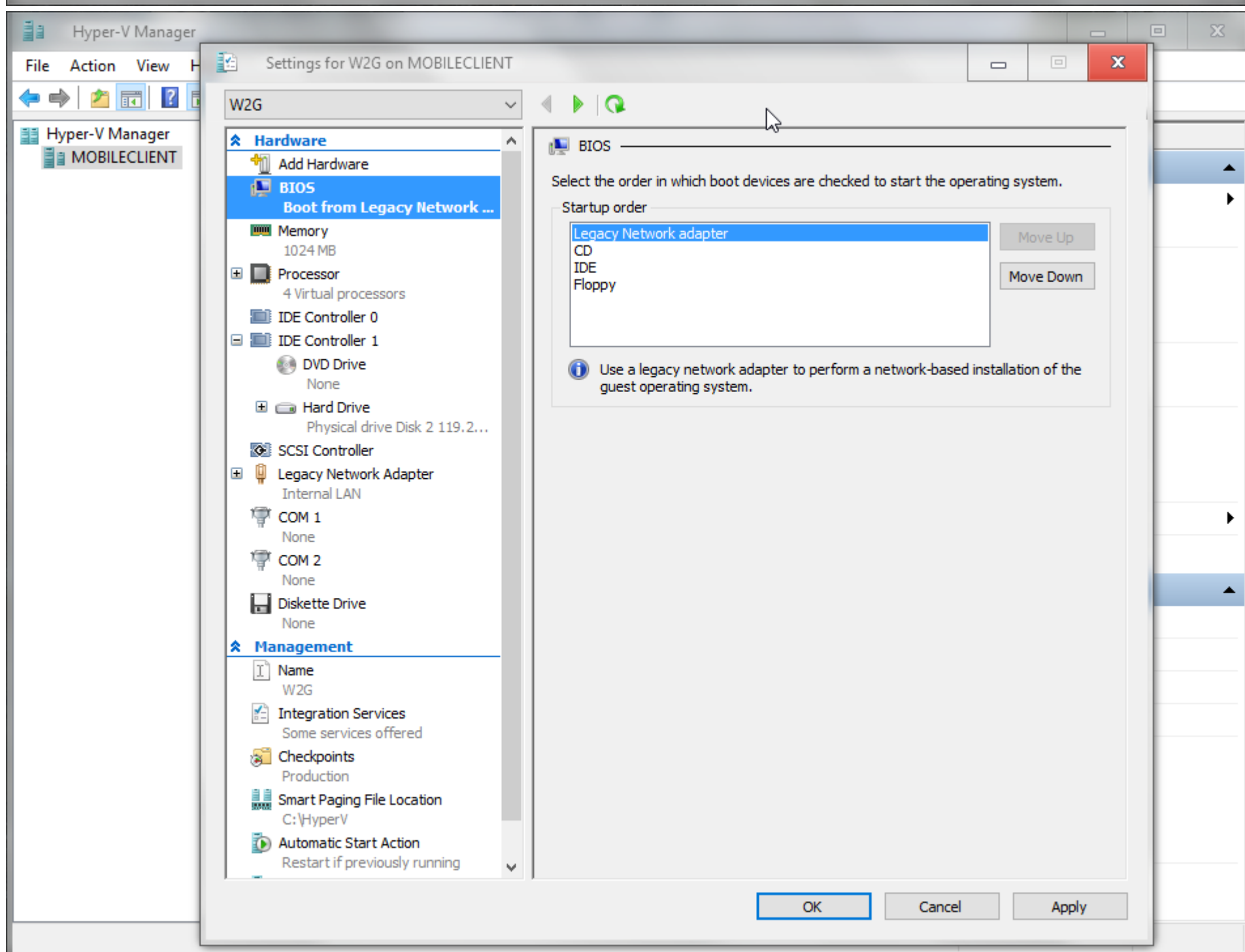
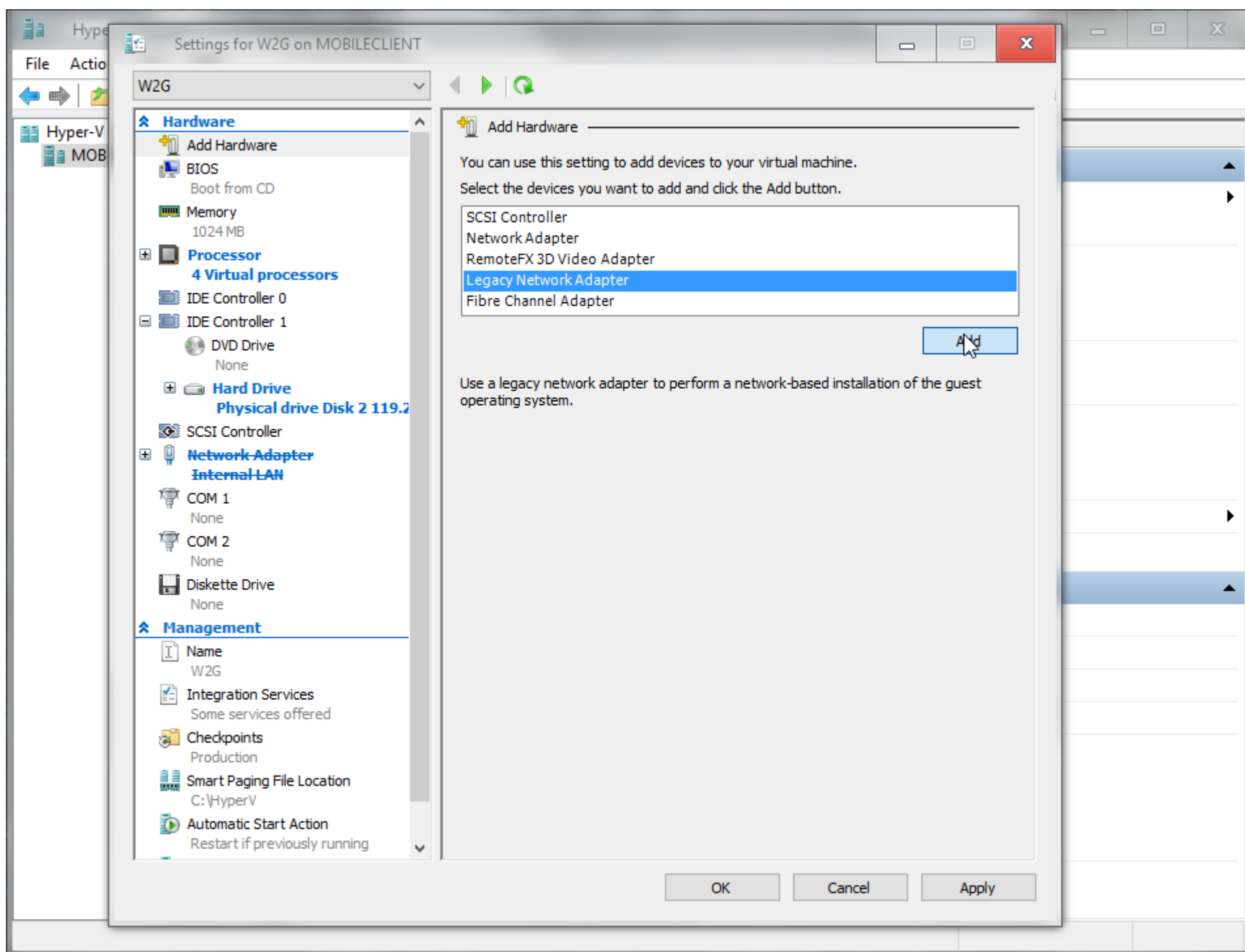
From here you have 2 choices

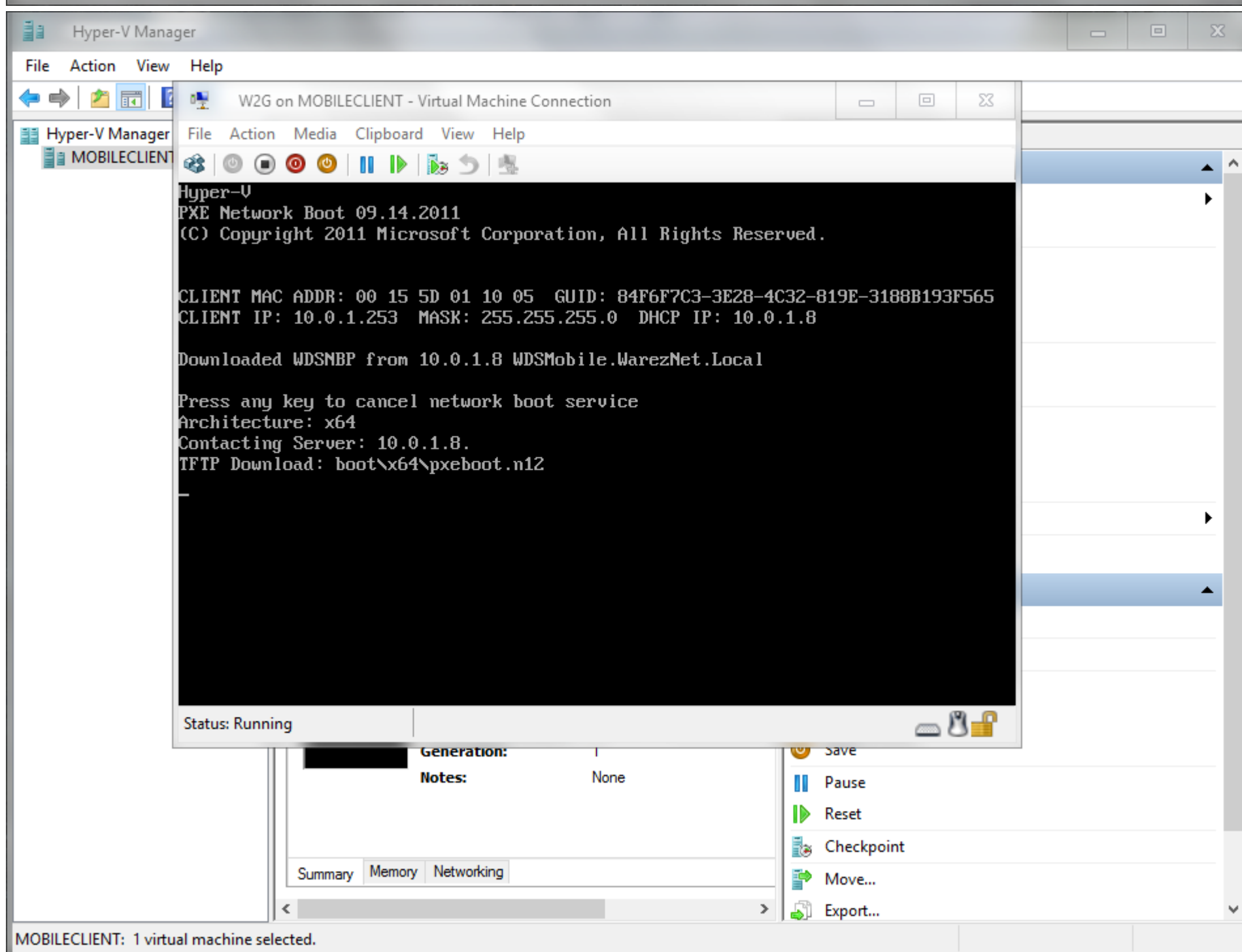
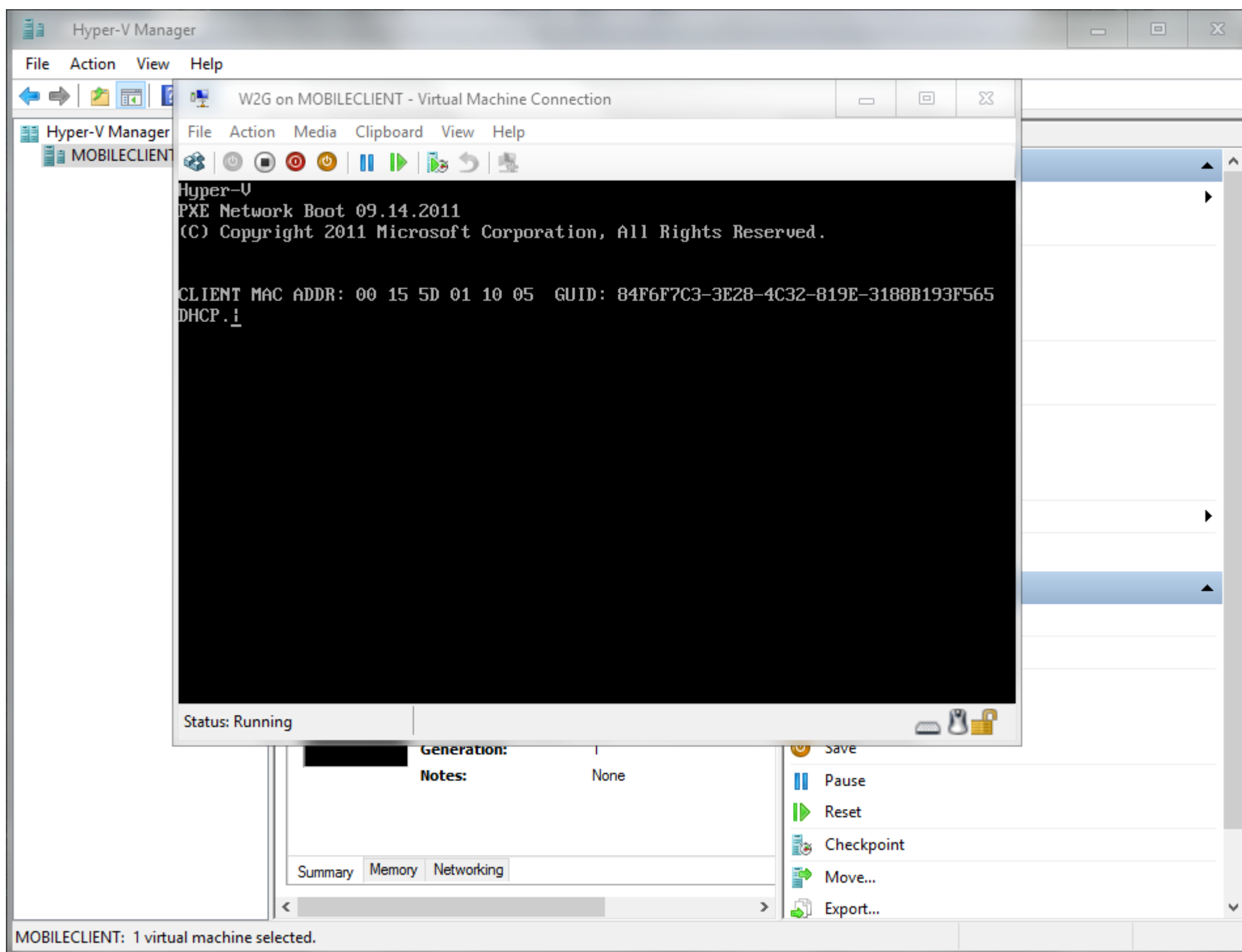
If you are deploying more than one of these devices you can use WDS to install the Windows image of your choice

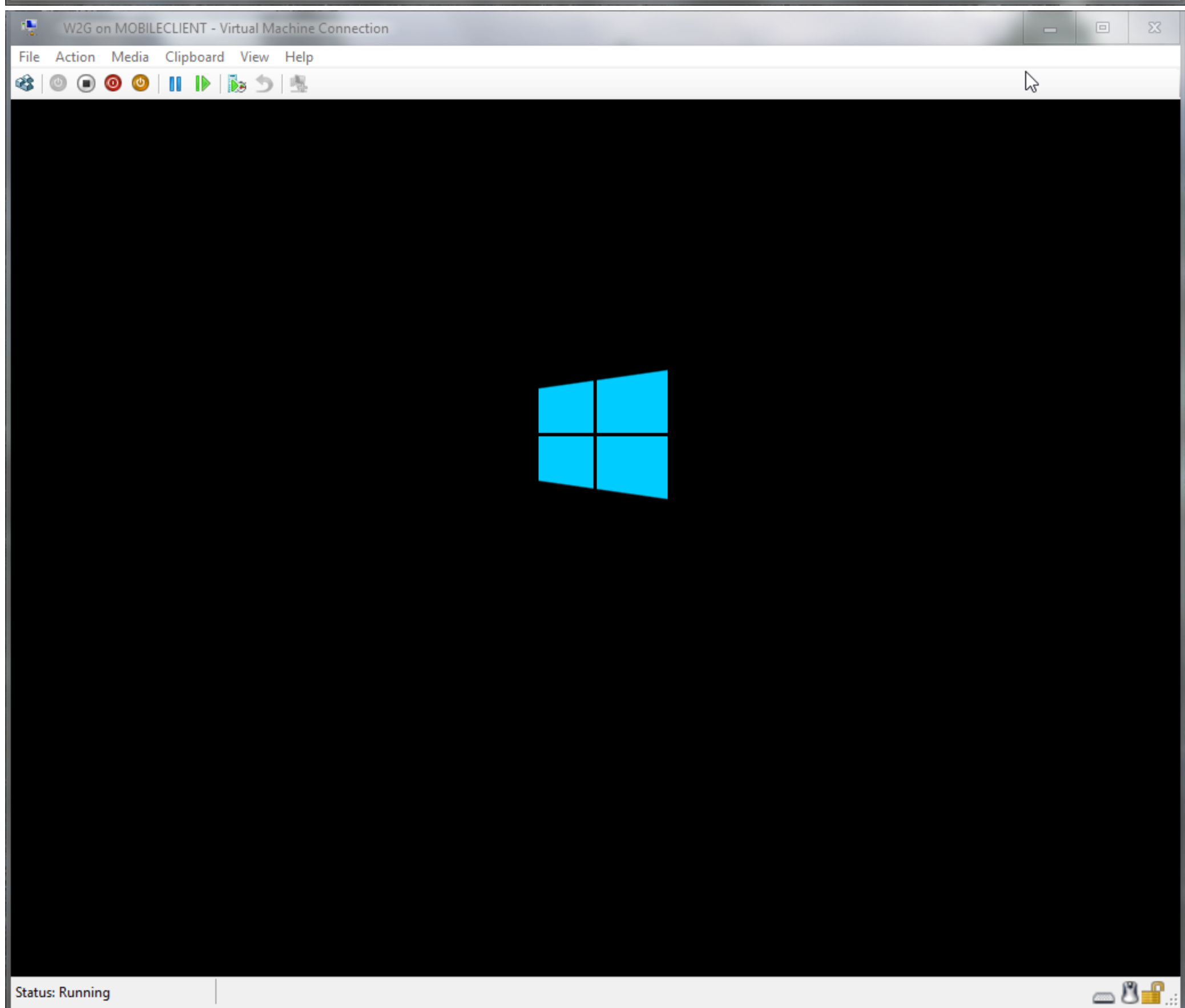
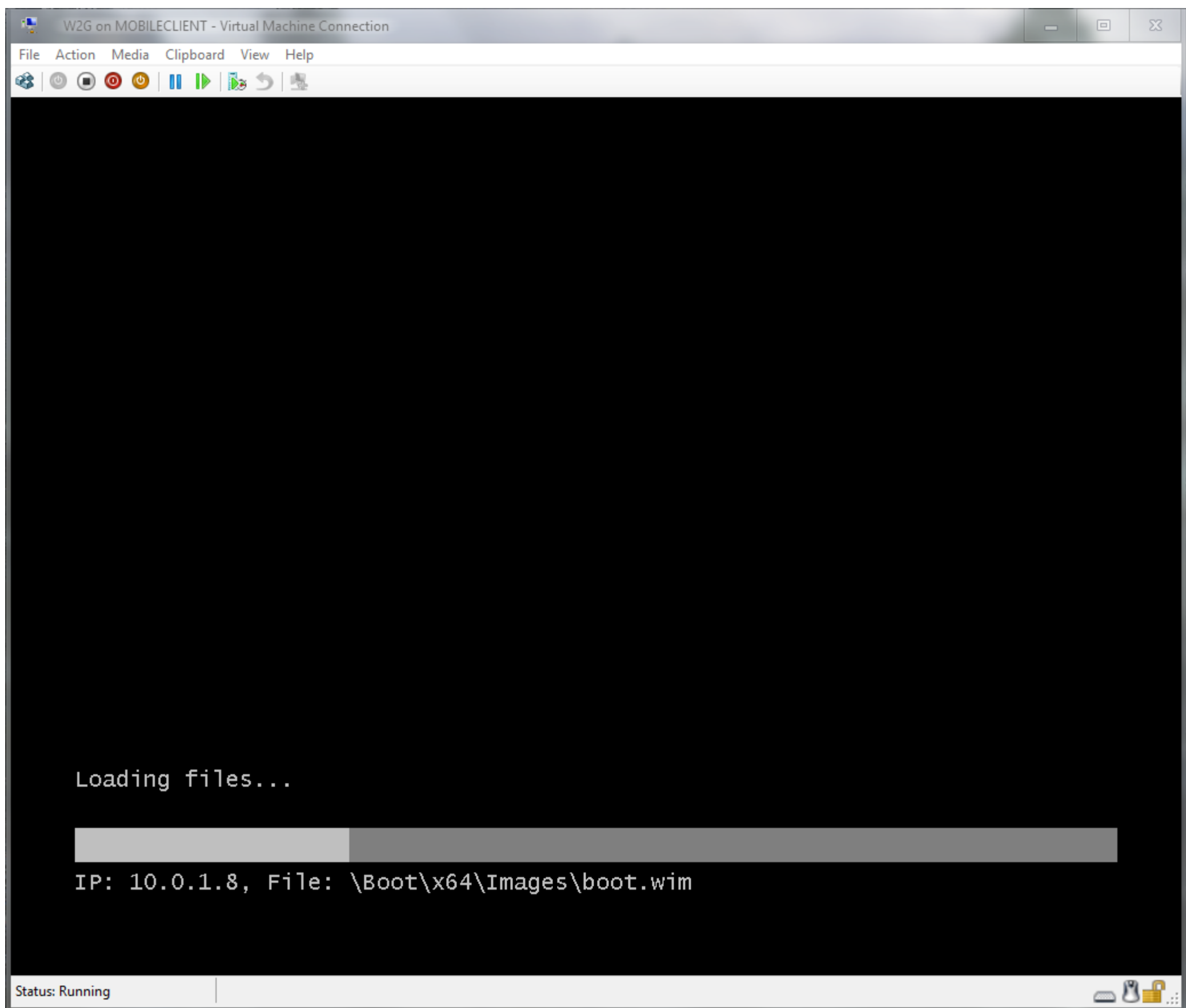
otherwise, you can bring the drive online now and use the following code to create the windows partition

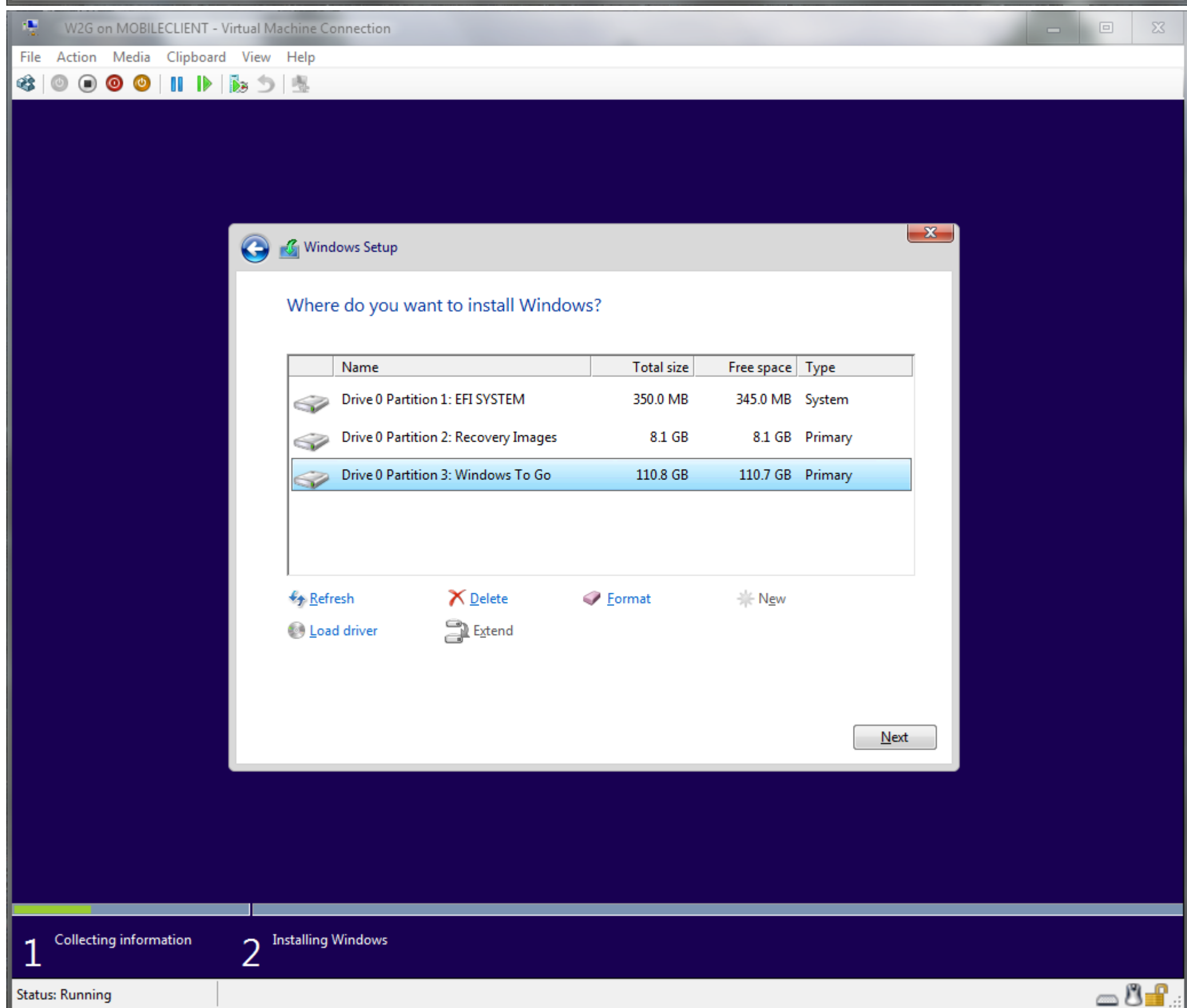
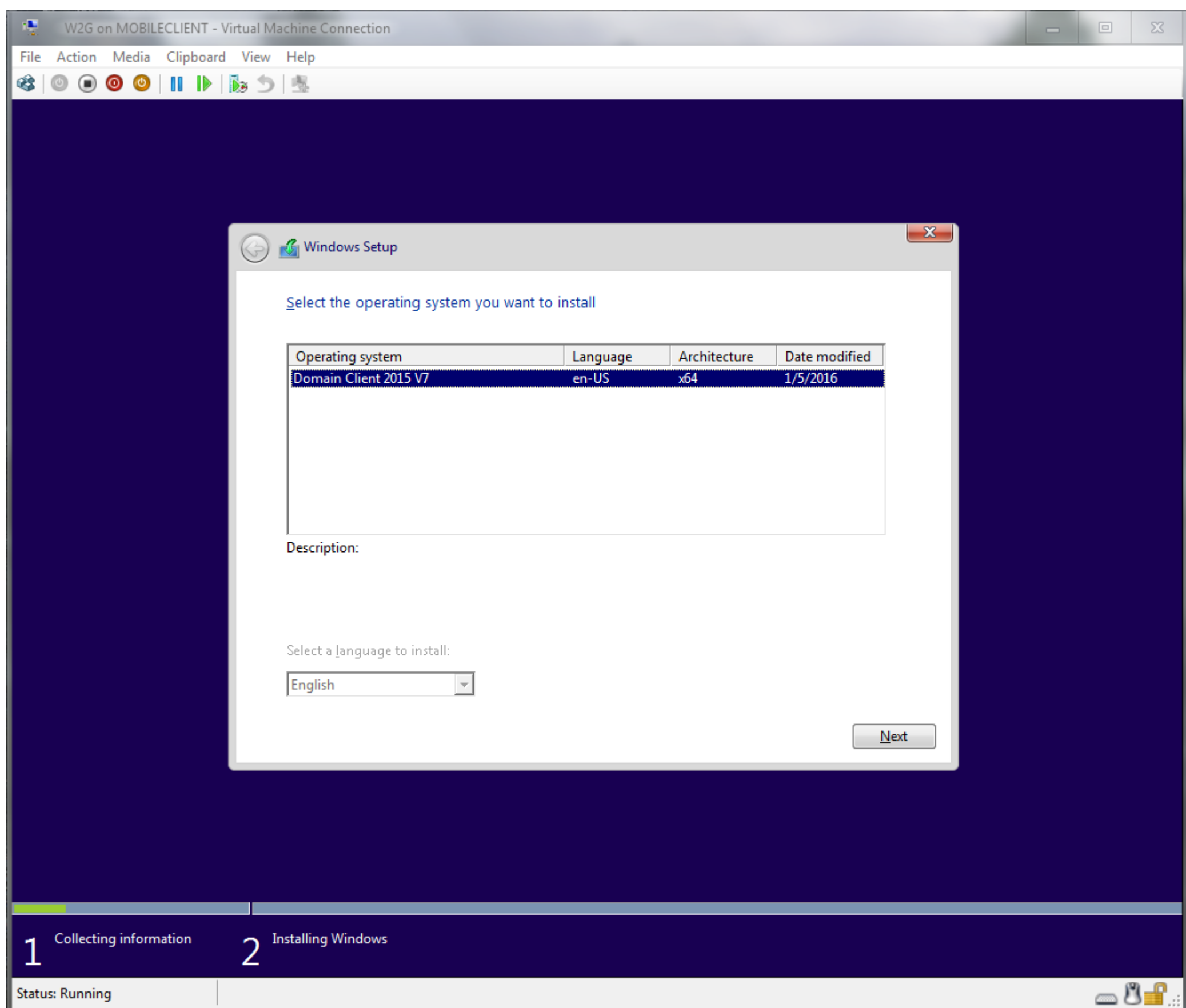
```
Dism /apply-image /imagefile:E:\sources\install.wim /index:1 /ApplyDir:W:\
bcdboot w:\Windows /s S: /f ALL
```

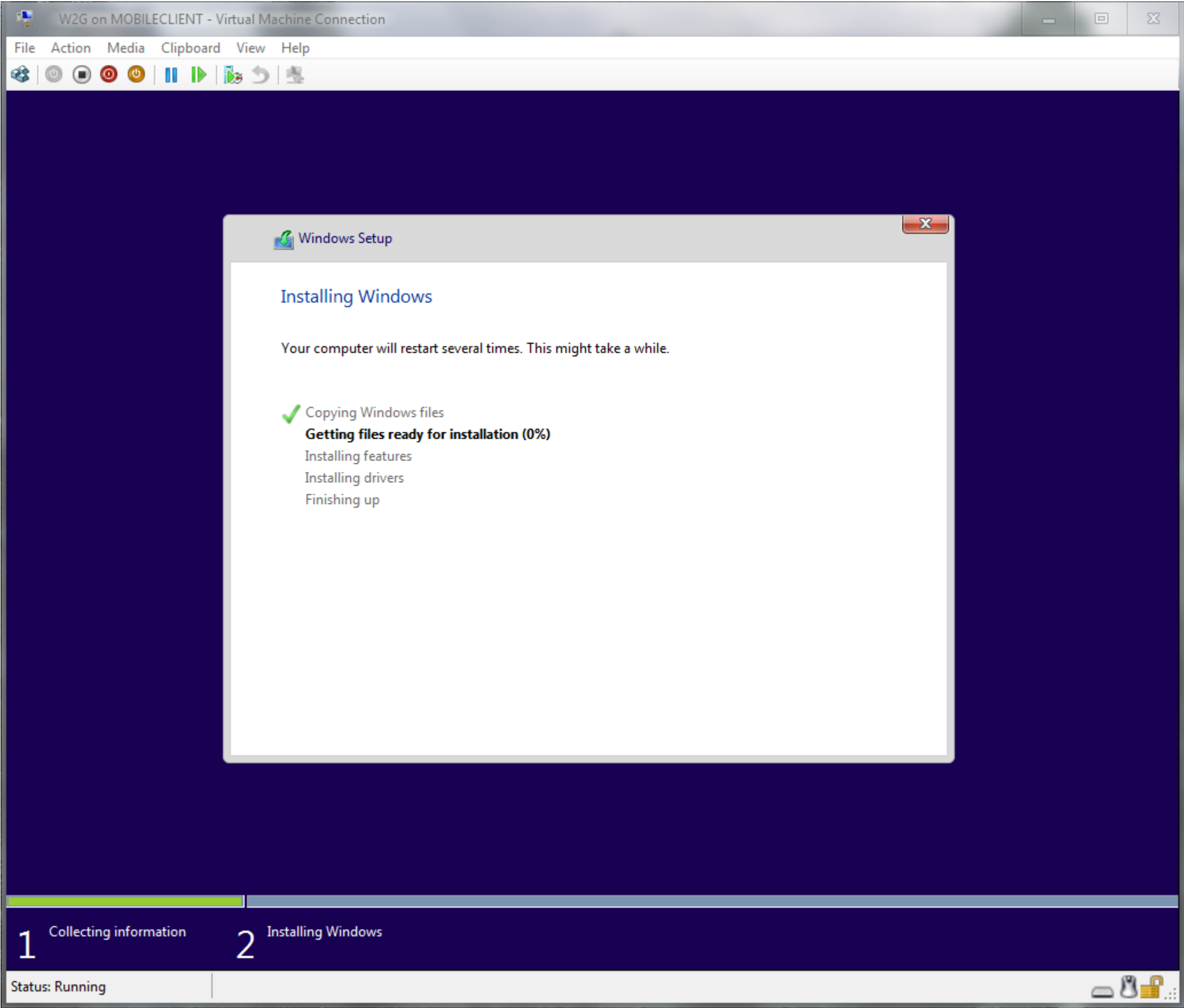
And you can skip the following steps until instructed



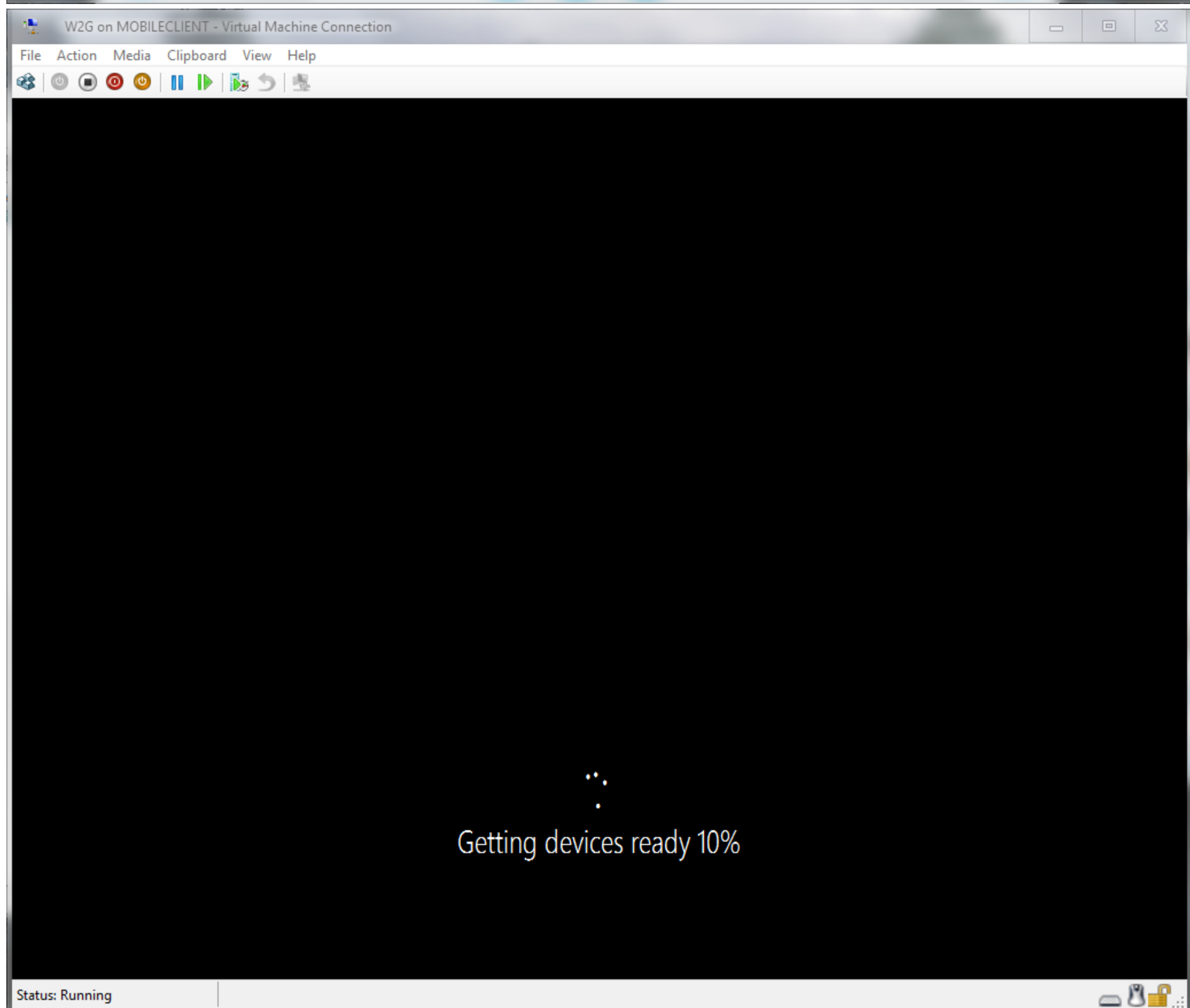
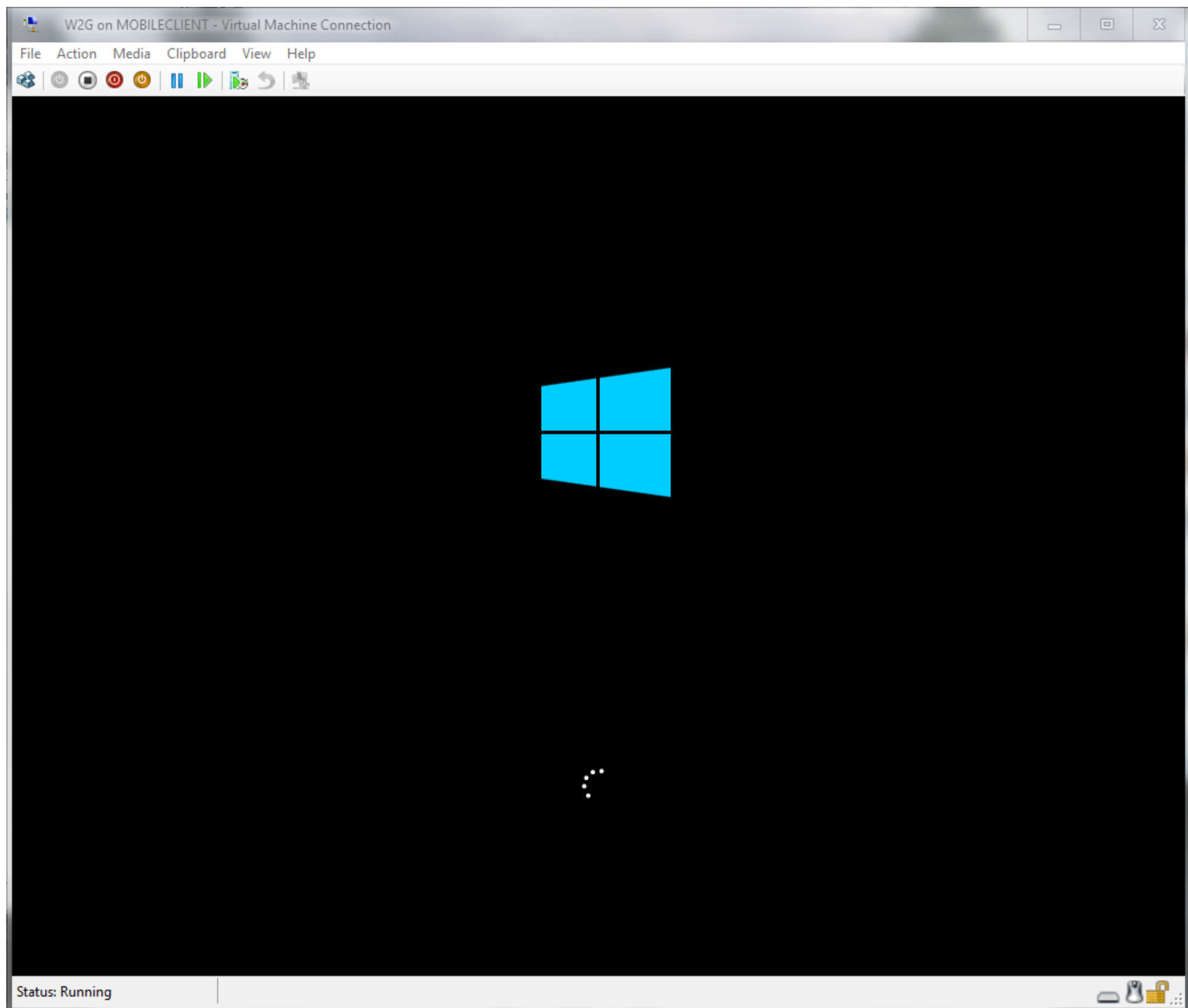


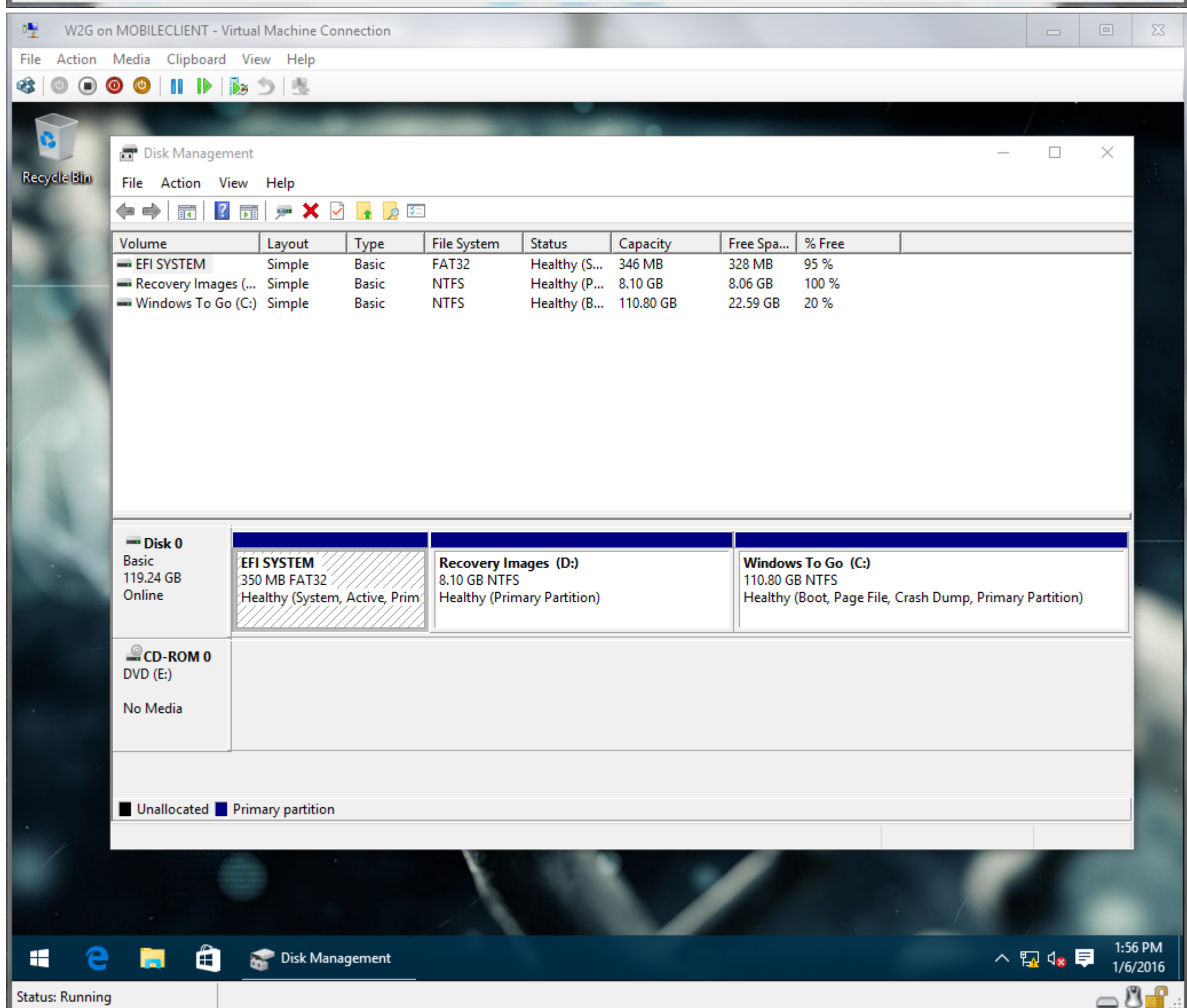
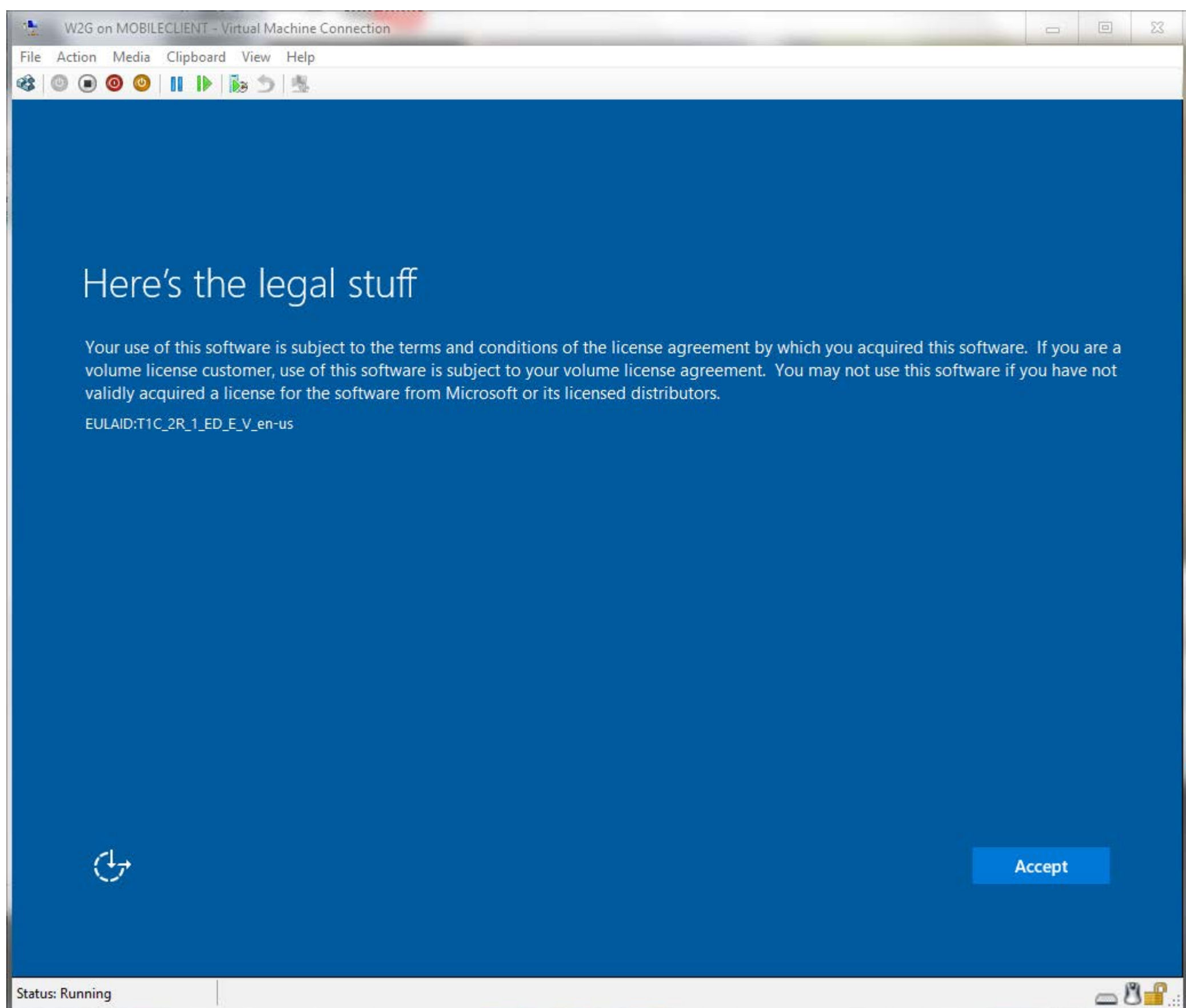


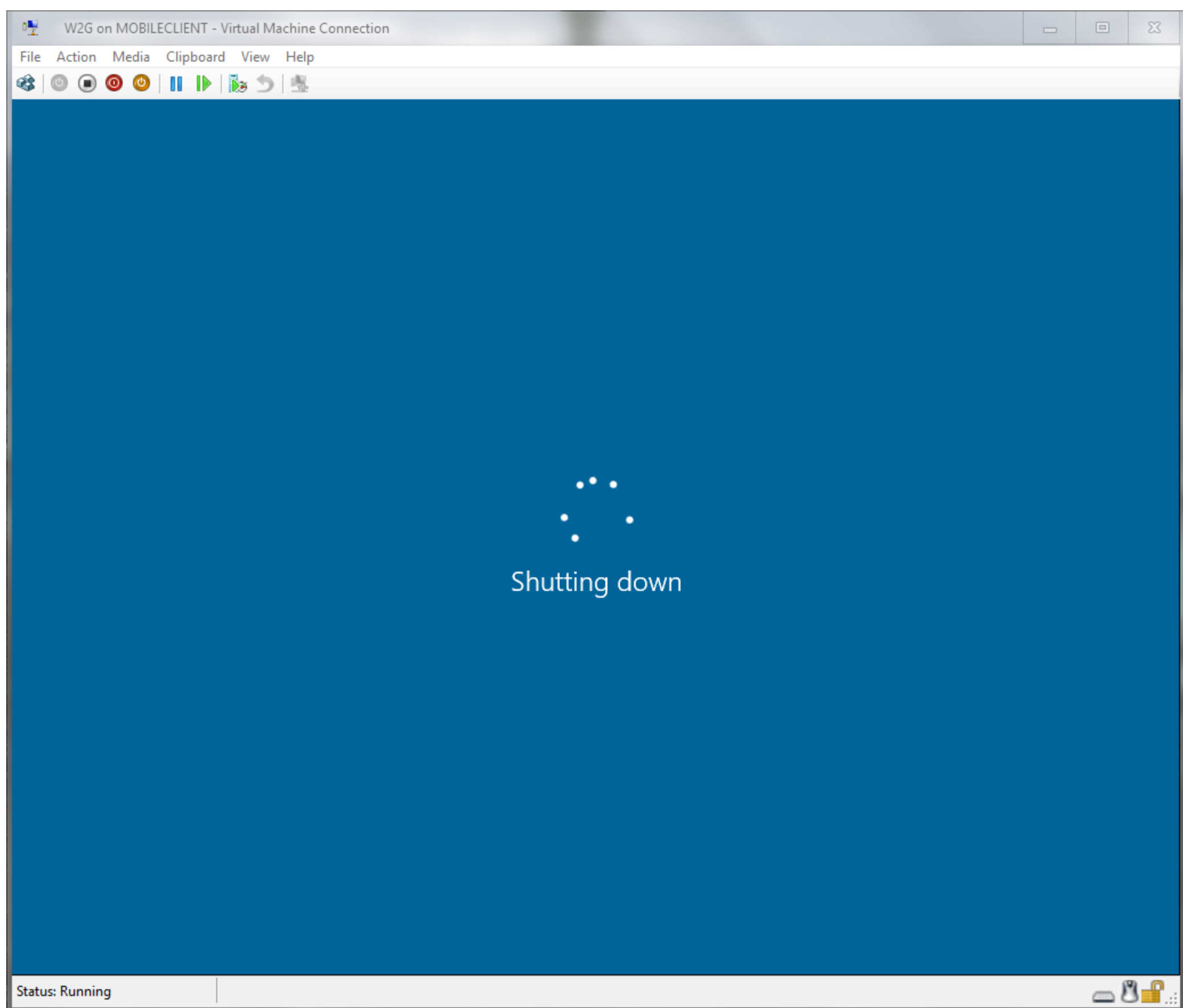




If you deployed the image manually you can power up your VM and continue from here





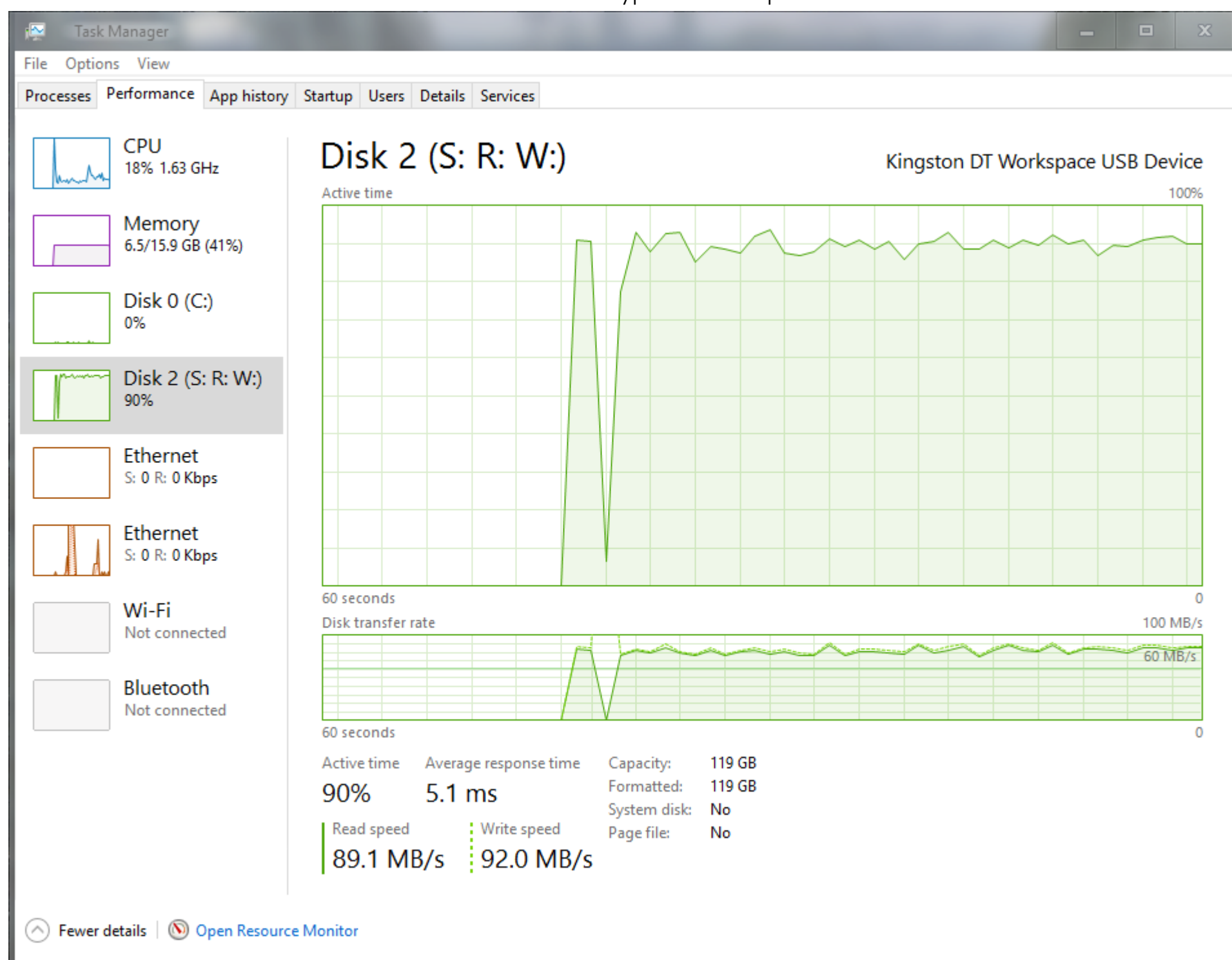


Now we can bitlocker the drive

Bring it online again and run the following commands

```
$password = ConvertTo-SecureString -String SOMEPASSWORD -AsPlainText -Force
Enable-BitLocker W: -PasswordProtector $password
```

Wait until the encryption is completed



```
Administrator: Windows PowerShell

-----
Point           Percentage      Enabled      Status
-----
Data           W:           110.80 EncryptionInProgress 1 {RecoveryPassword, Pas... False Off

PS C:\Windows\system32> manage-bde -status W:
BitLocker Drive Encryption: Configuration Tool version 10.0.10011
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume W: [Windows To Go]
[Data Volume]
Size: 110.80 GB
BitLocker Version: 2.0
Conversion Status: Encryption in Progress
Percentage Encrypted: 32.3%
Encryption Method: XTS-AES 128
Protection Status: Protection Off
Lock Status: Unlocked
Identification Field: Unknown
Automatic Unlock: Disabled
Key Protectors:
    Numerical Password
    Password

PS C:\Windows\system32>
```

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

CPU 12%

Memory 6.1%

Disk 0%

Disk 0%

Ethernet S: 0%

Ethernet S: 0%

Windows Firewall No

Bluetooth No

Administrator: Windows PowerShell

Protection Status: Protection On  
Lock Status: Unlocked  
Identification Field: Unknown  
Automatic Unlock: Disabled  
Key Protectors:  
 Numerical Password  
 Password

PS C:\Windows\system32> manage-bde -status W:  
BitLocker Drive Encryption: Configuration Tool version 10.0.10011  
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume W: [Windows To Go]  
[Data Volume]  
Size: 110.80 GB  
BitLocker Version: 2.0  
Conversion Status: Fully Encrypted  
Percentage Encrypted: 100.0%  
Encryption Method: XTS-AES 128  
Protection Status: Protection On  
Lock Status: Unlocked  
Identification Field: Unknown  
Automatic Unlock: Disabled  
Key Protectors:  
 Numerical Password  
 Password

PS C:\Windows\system32>

PS C:\Windows\system32> manage-bde -status W:  
BitLocker Drive Encryption: Configuration Tool version 10.0.10011  
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

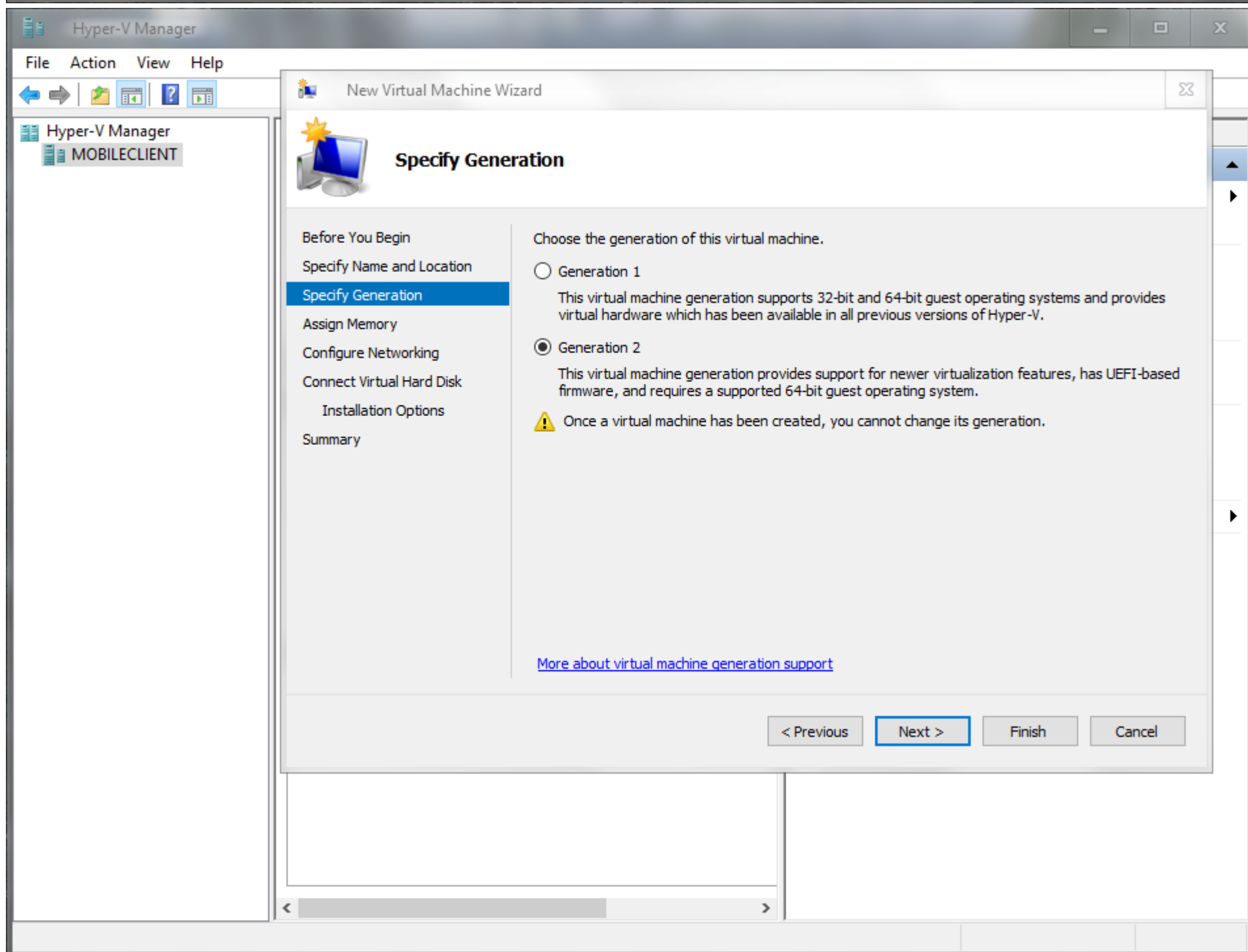
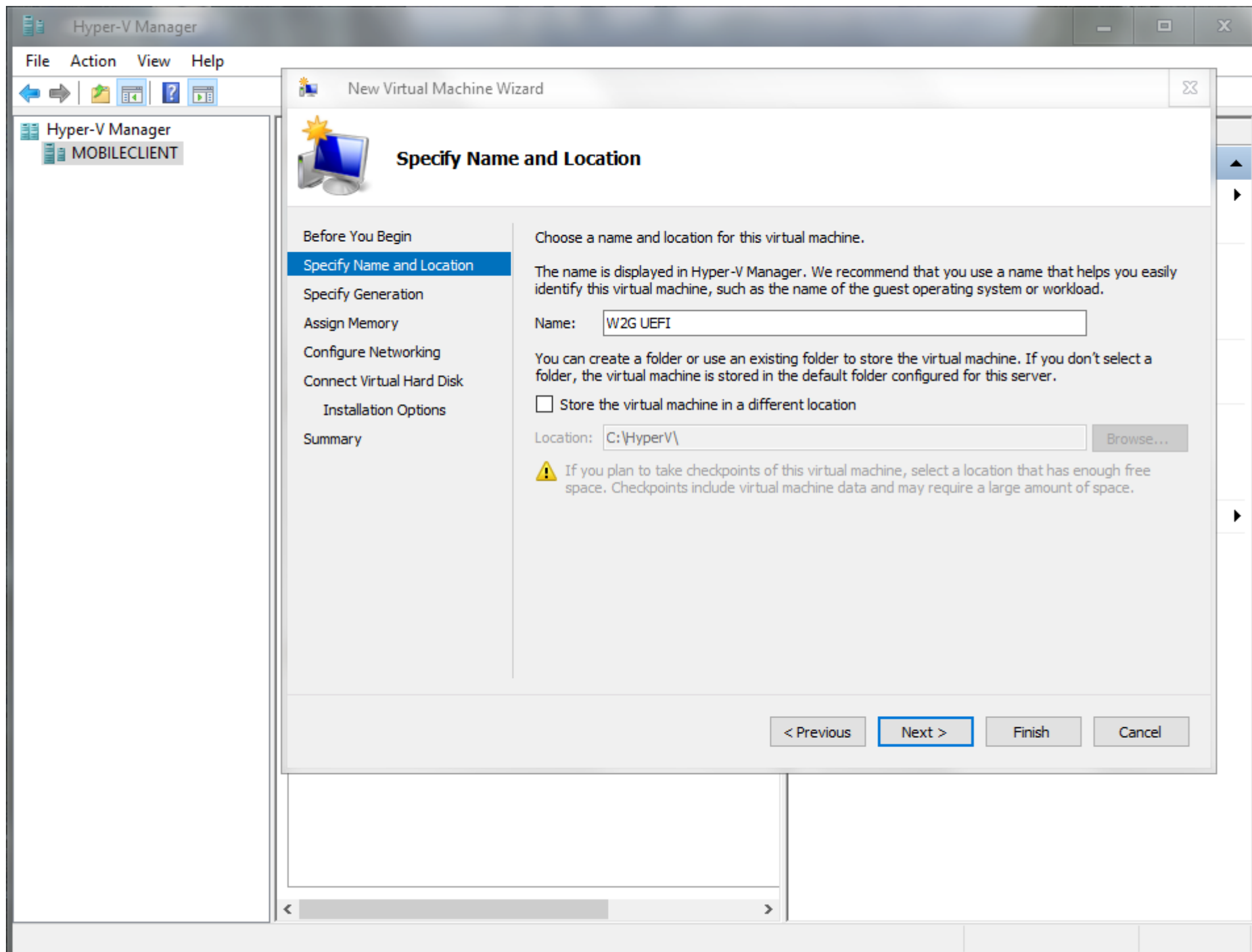
Volume W: [Windows To Go]  
[Data Volume]  
Size: 110.80 GB  
BitLocker Version: 2.0  
Conversion Status: Fully Encrypted  
Percentage Encrypted: 100.0%  
Encryption Method: XTS-AES 128  
Protection Status: Protection On  
Lock Status: Unlocked  
Identification Field: Unknown  
Automatic Unlock: Disabled  
Key Protectors:  
 Numerical Password  
 Password

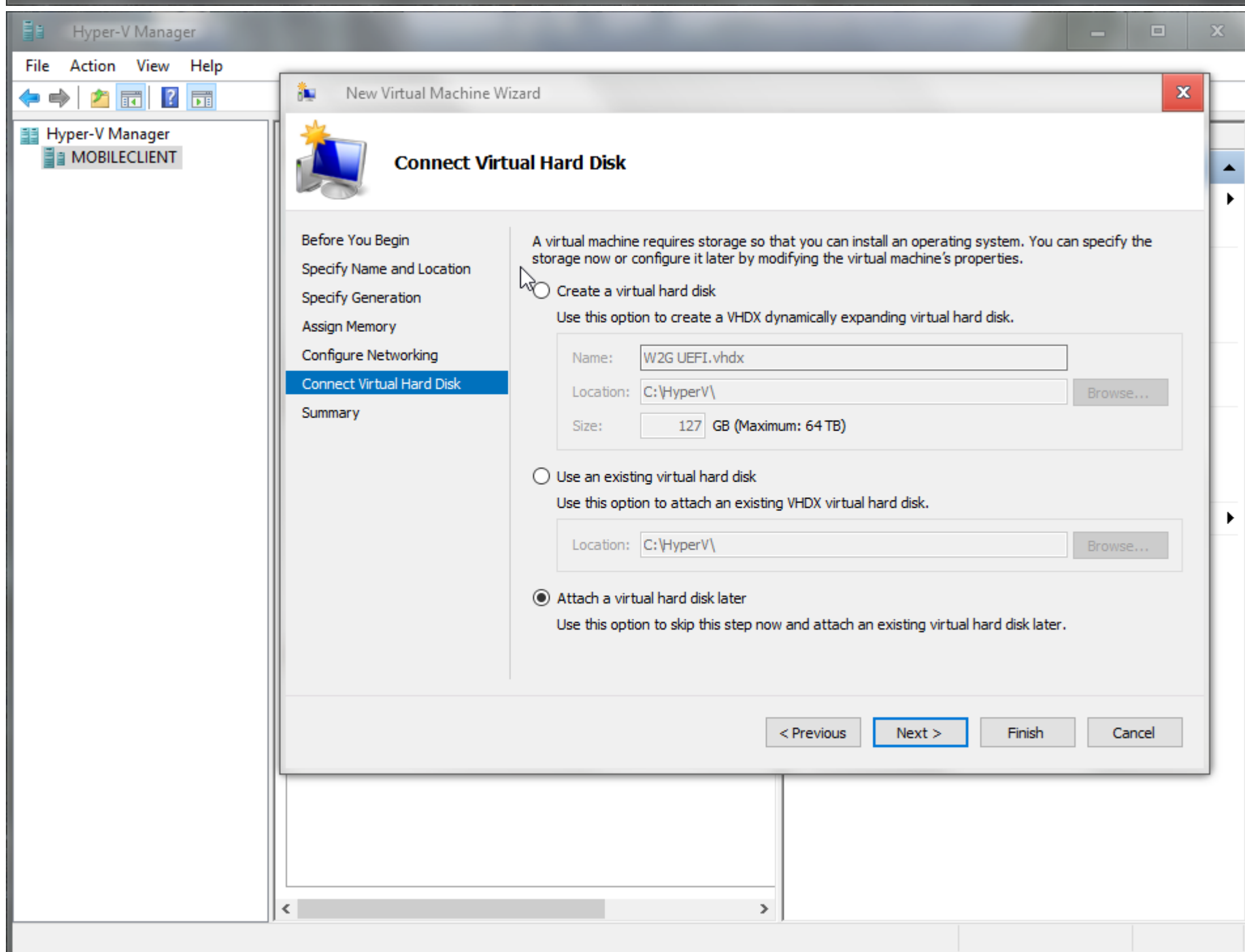
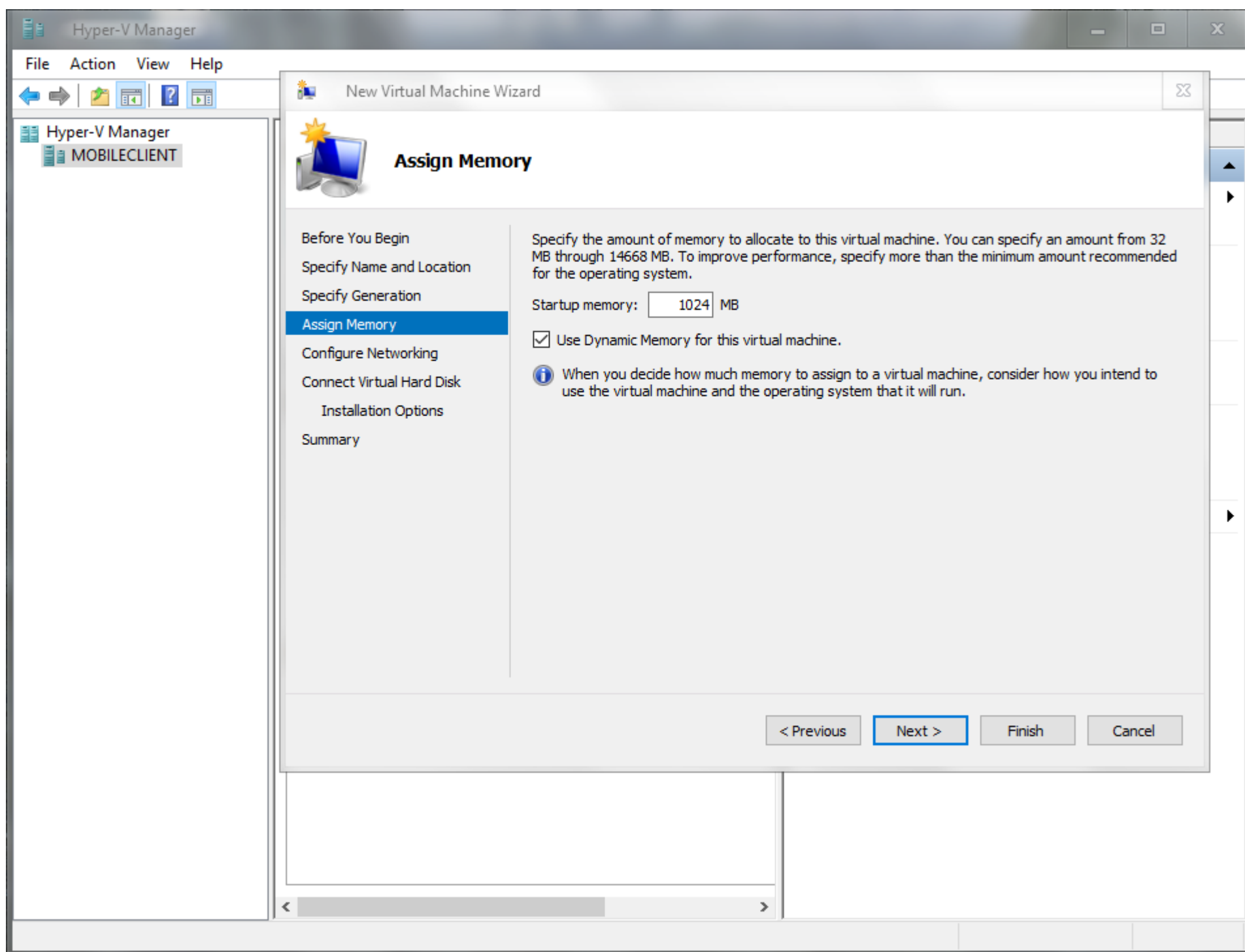
PS C:\Windows\system32>

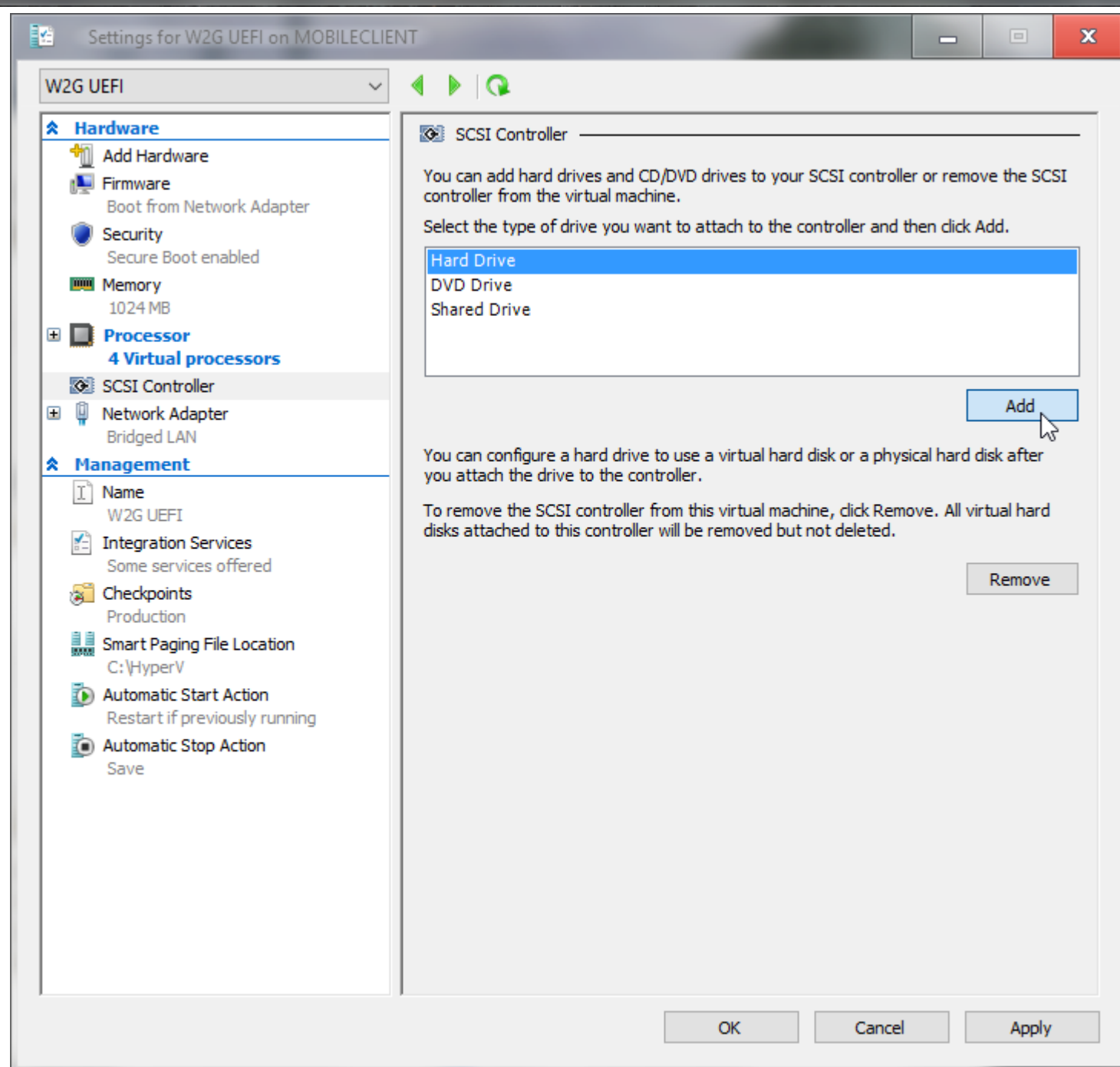
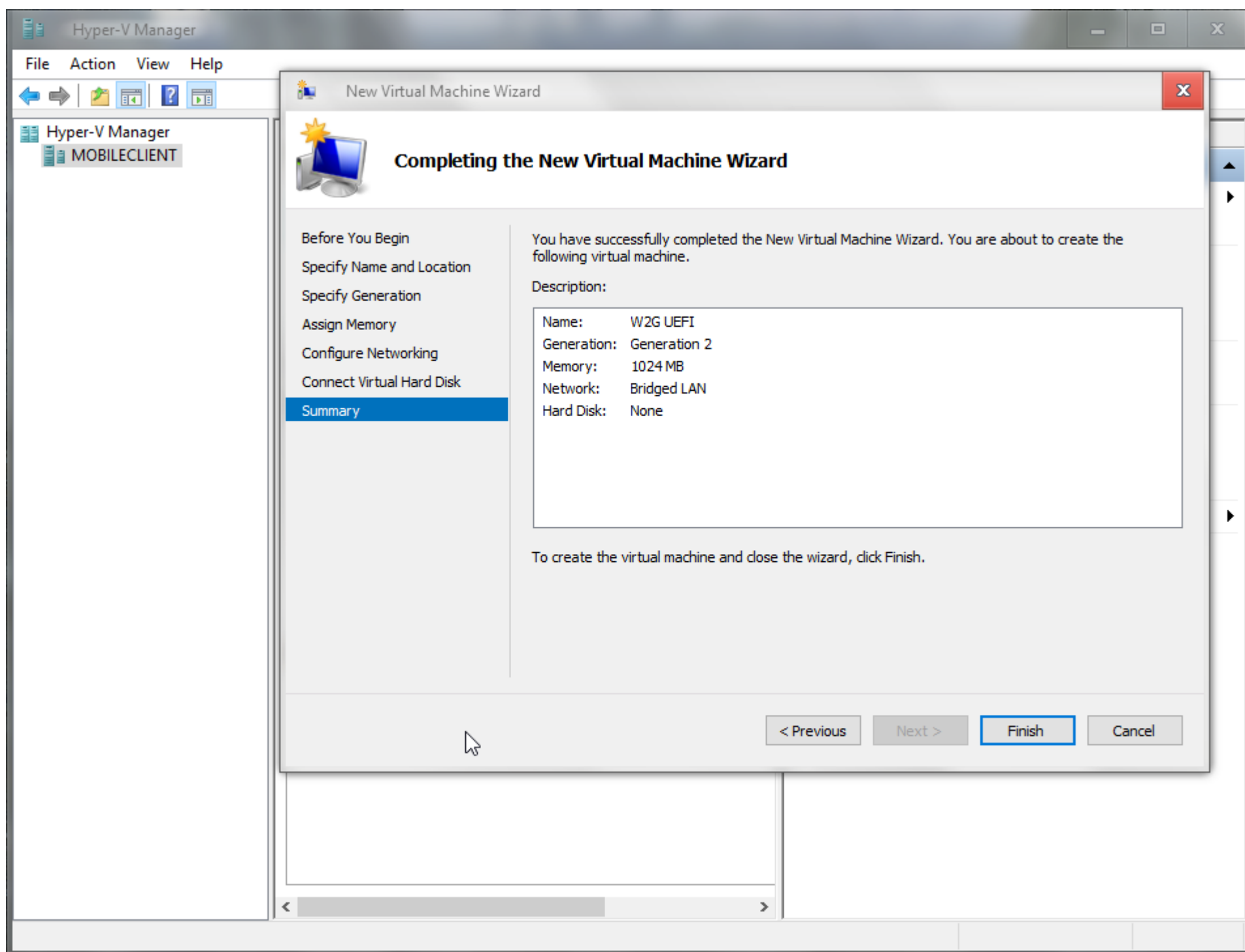
Fewer details

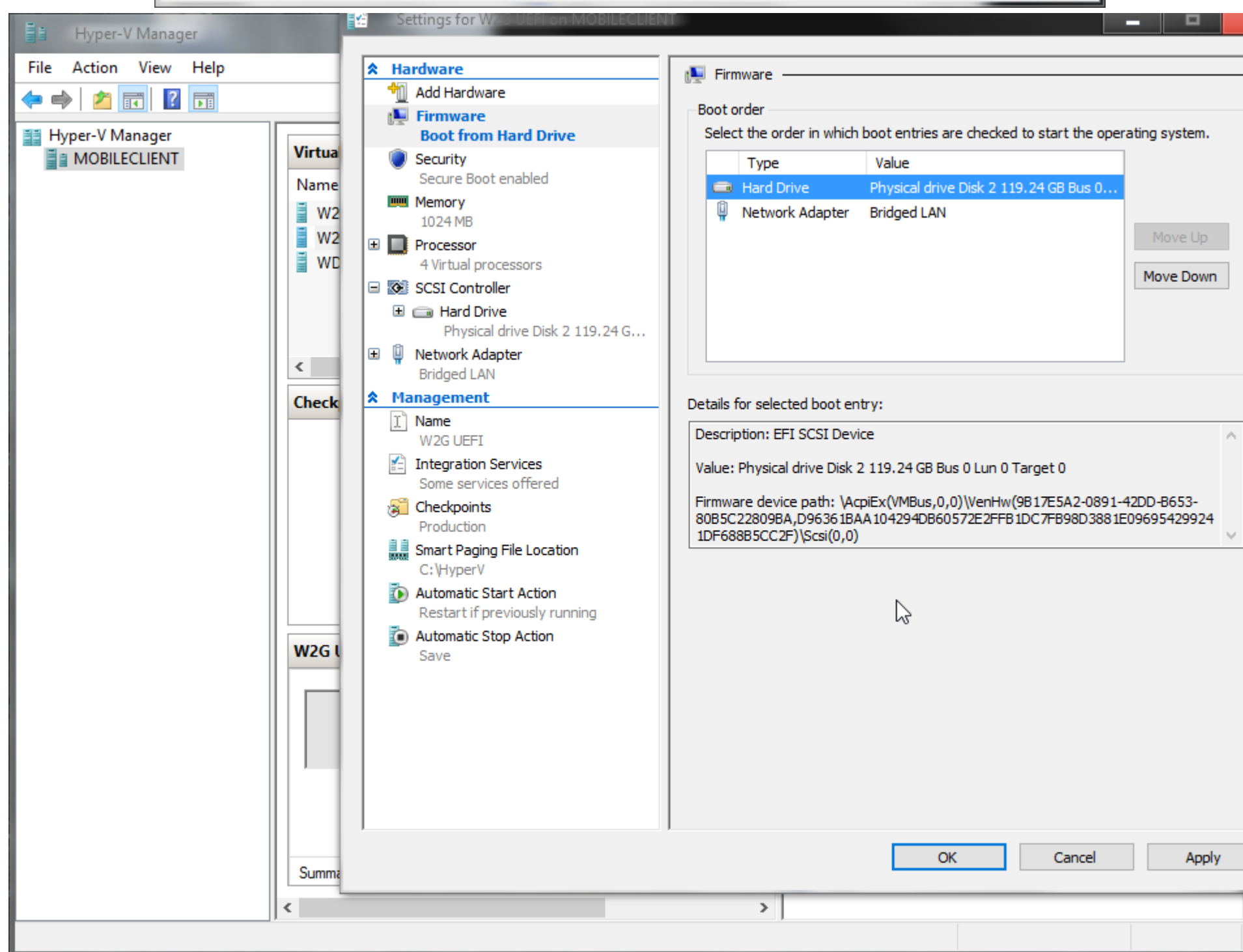
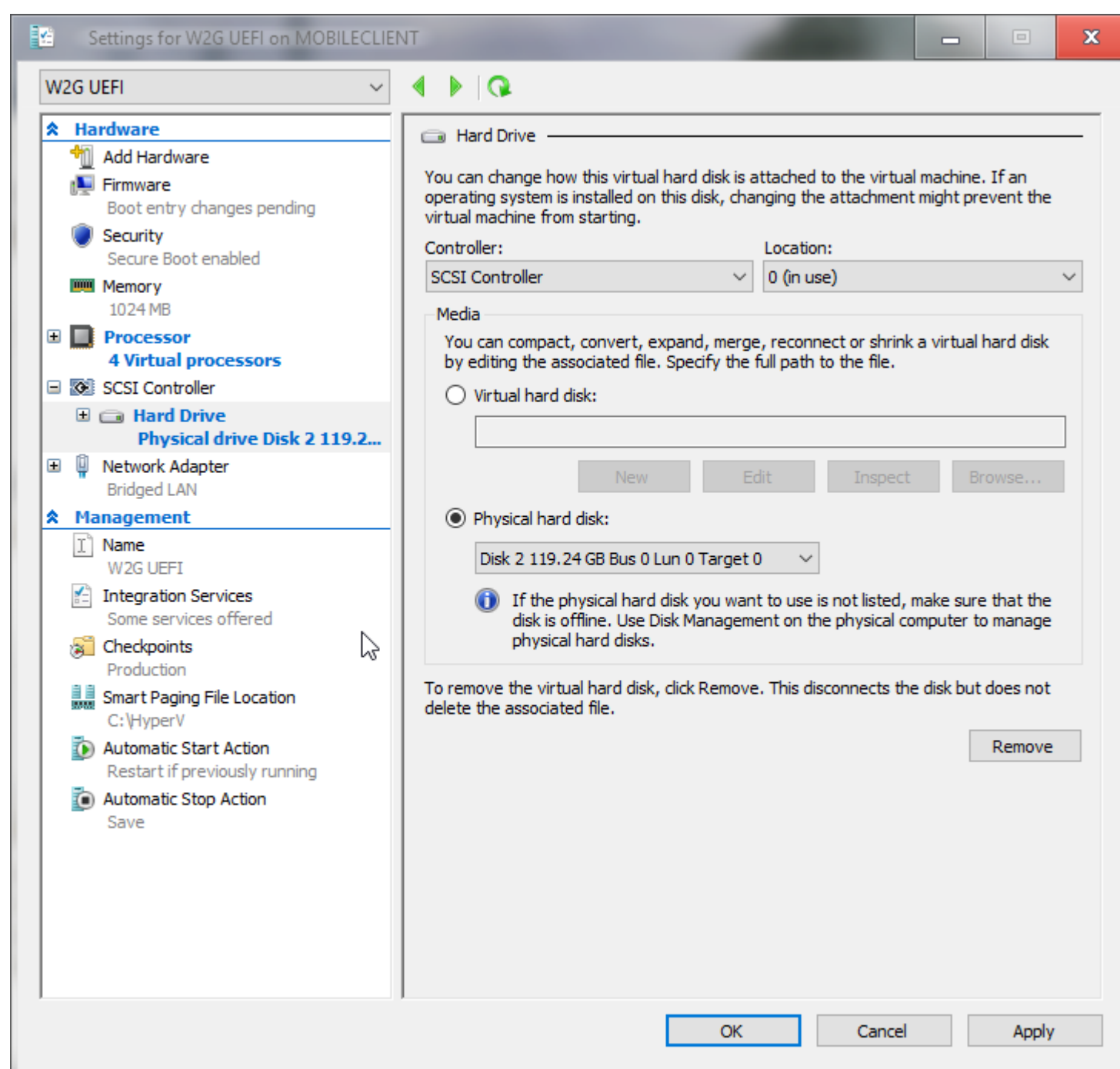
Open Resource Monitor

Now make the drive offline and make a new VM Gen 2 this time

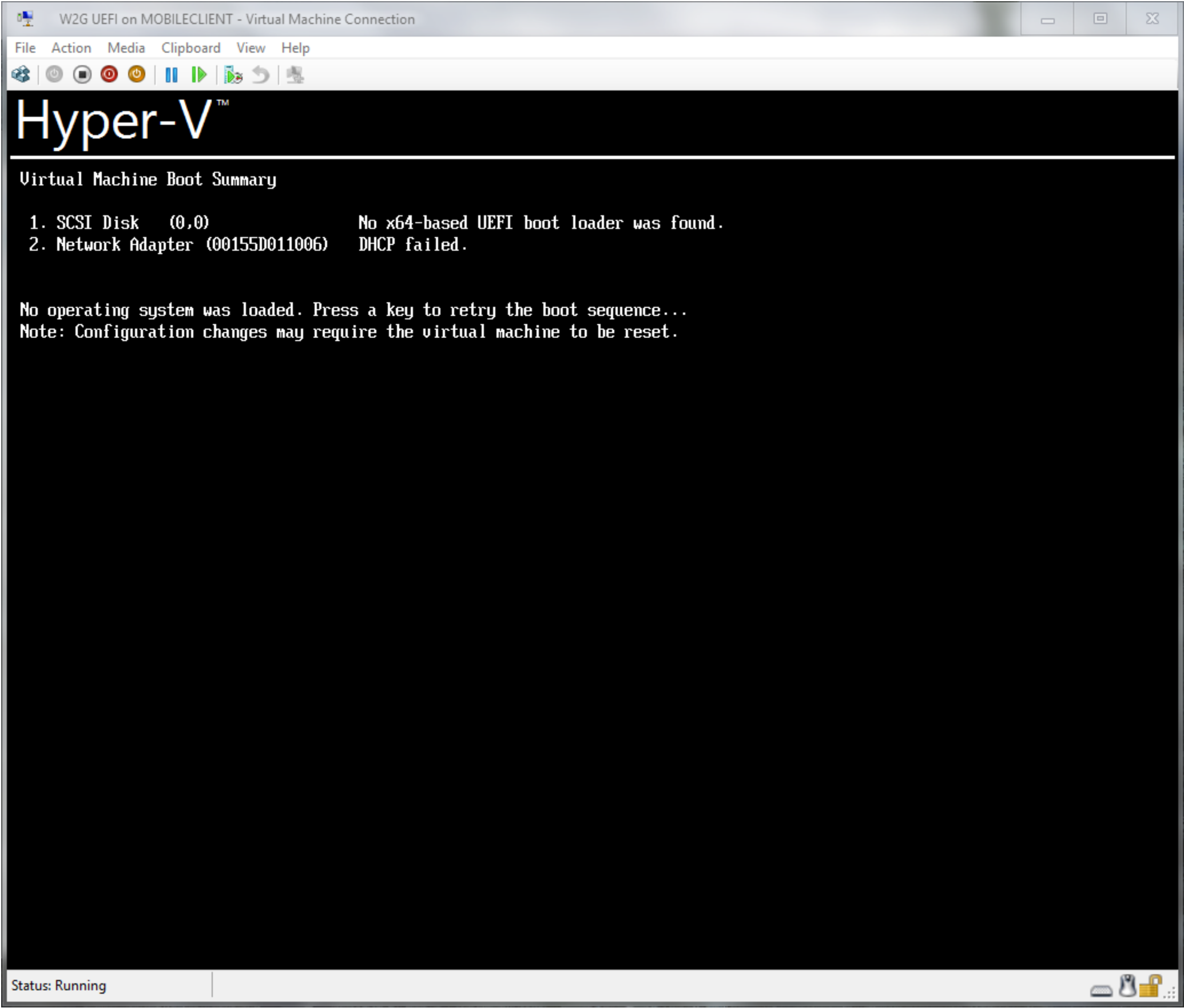


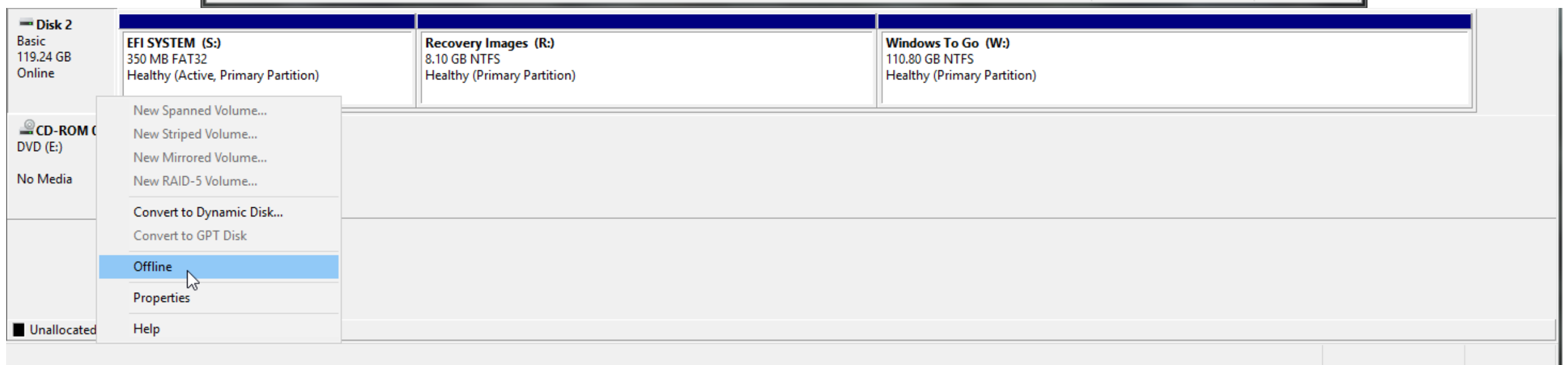
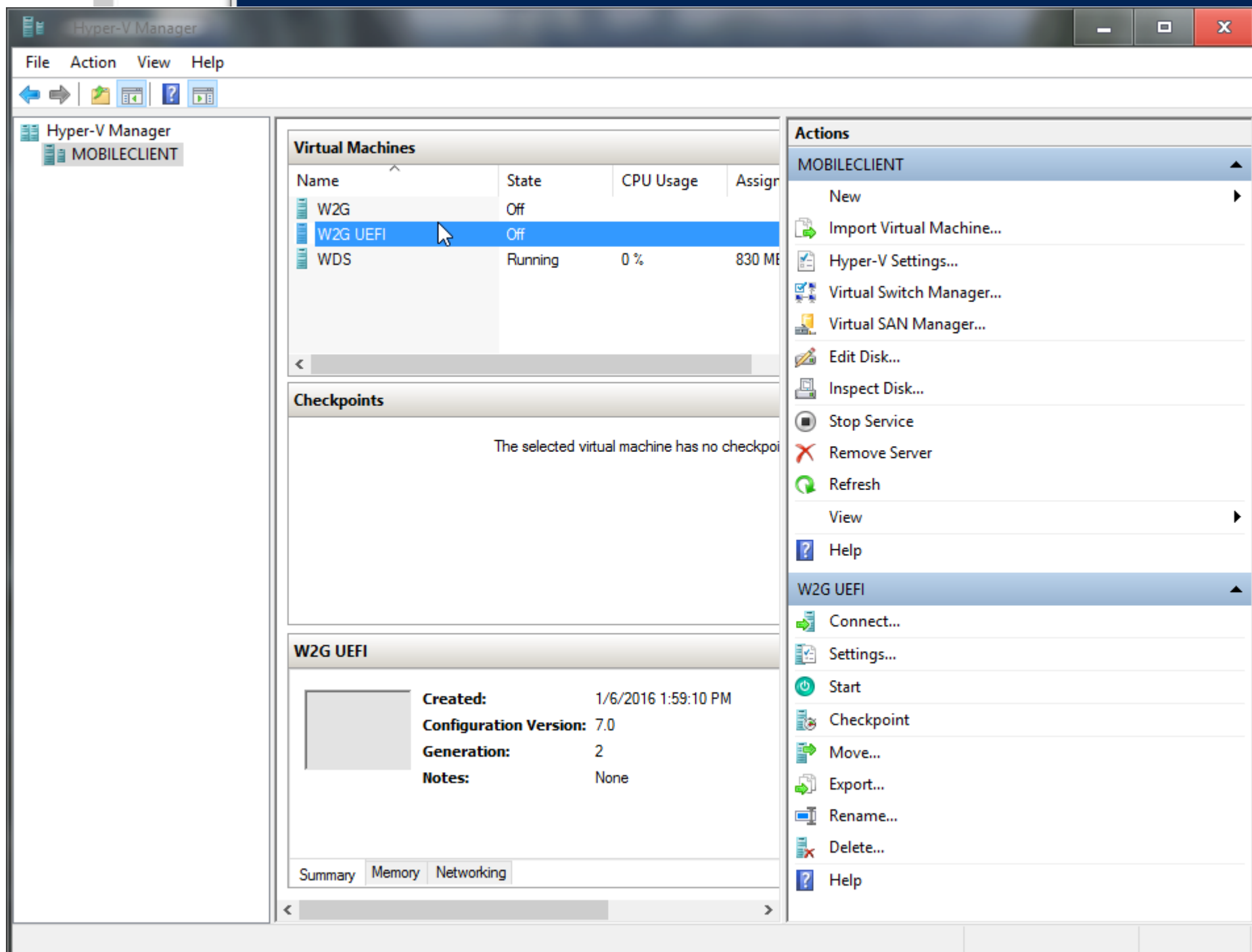
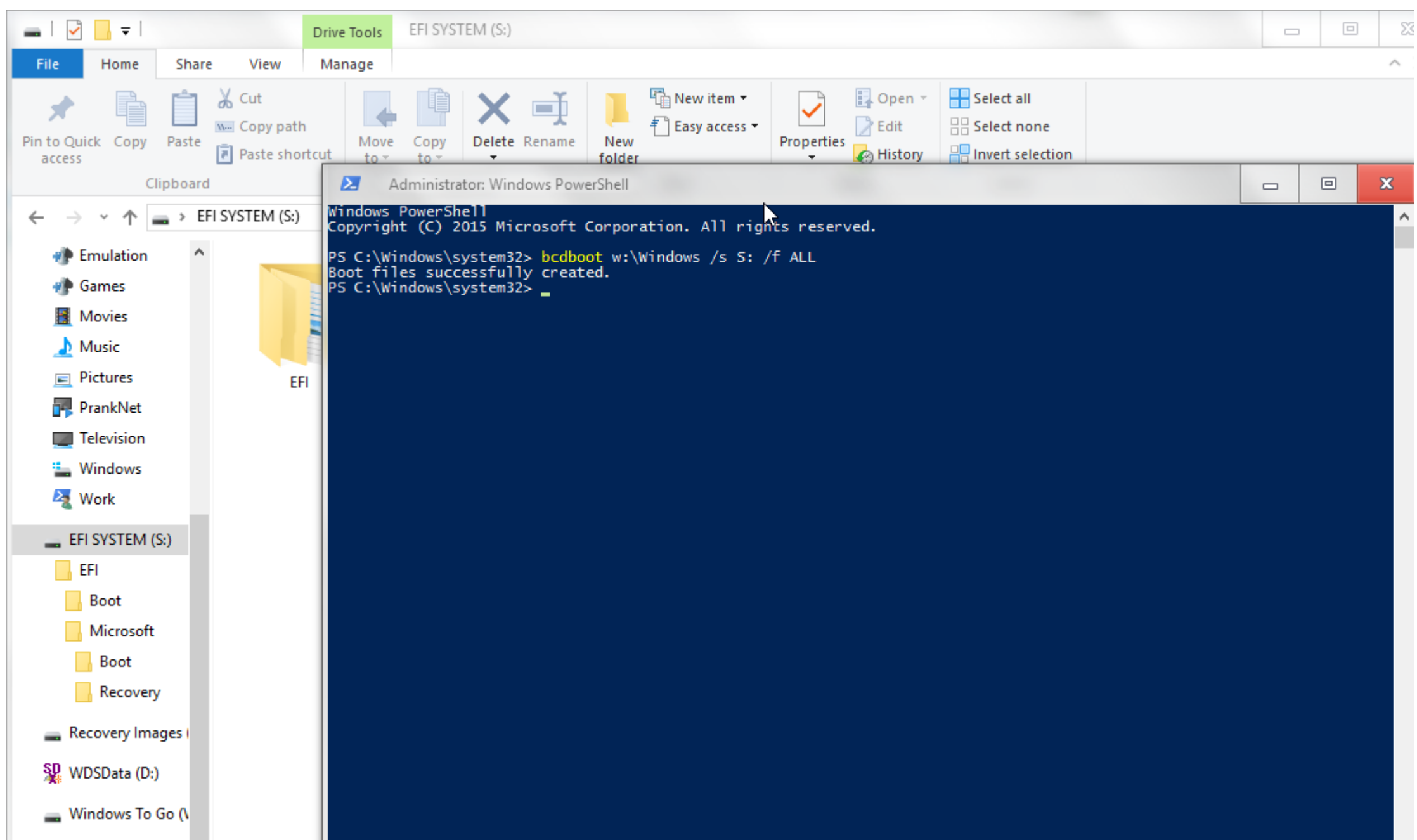




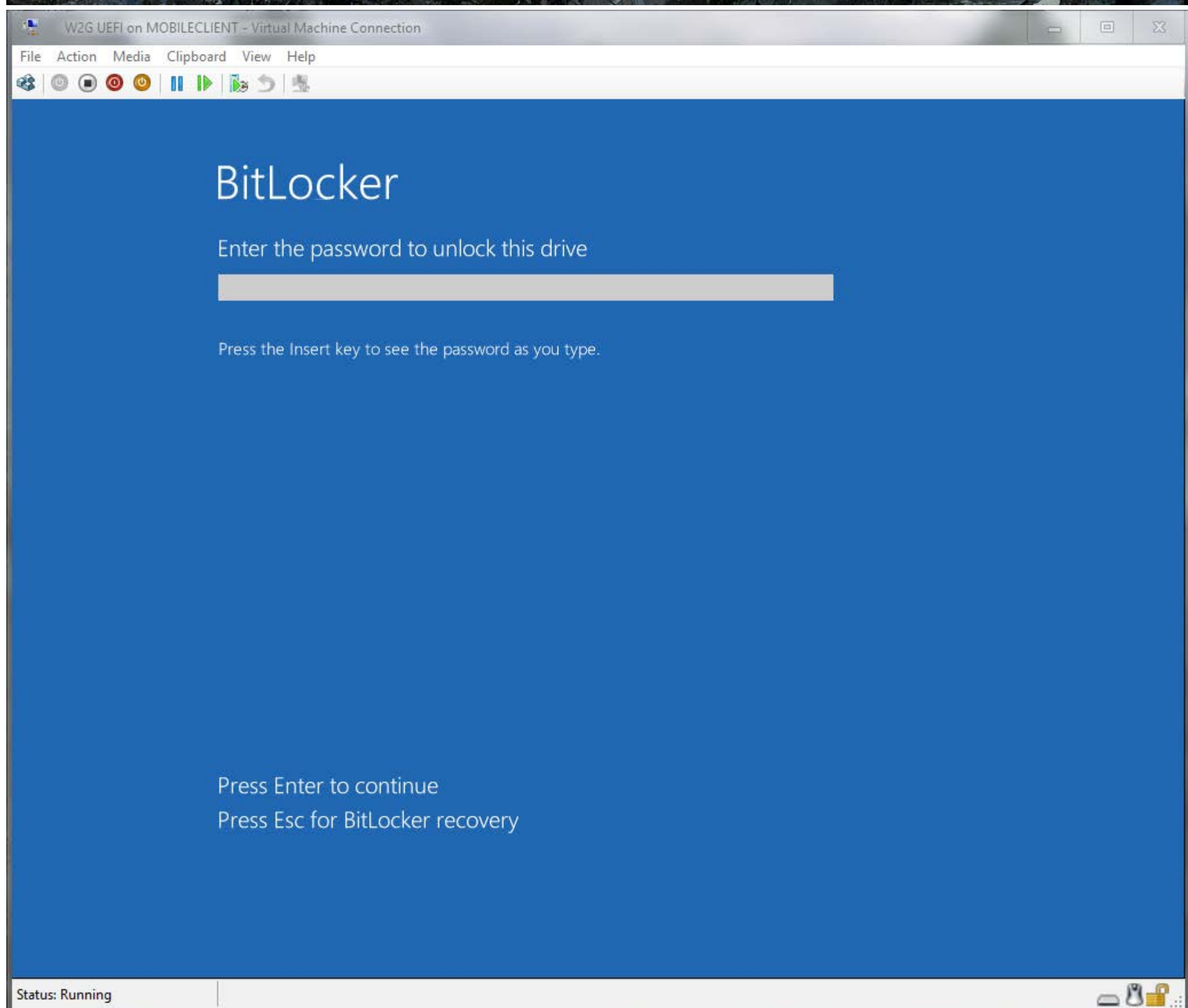
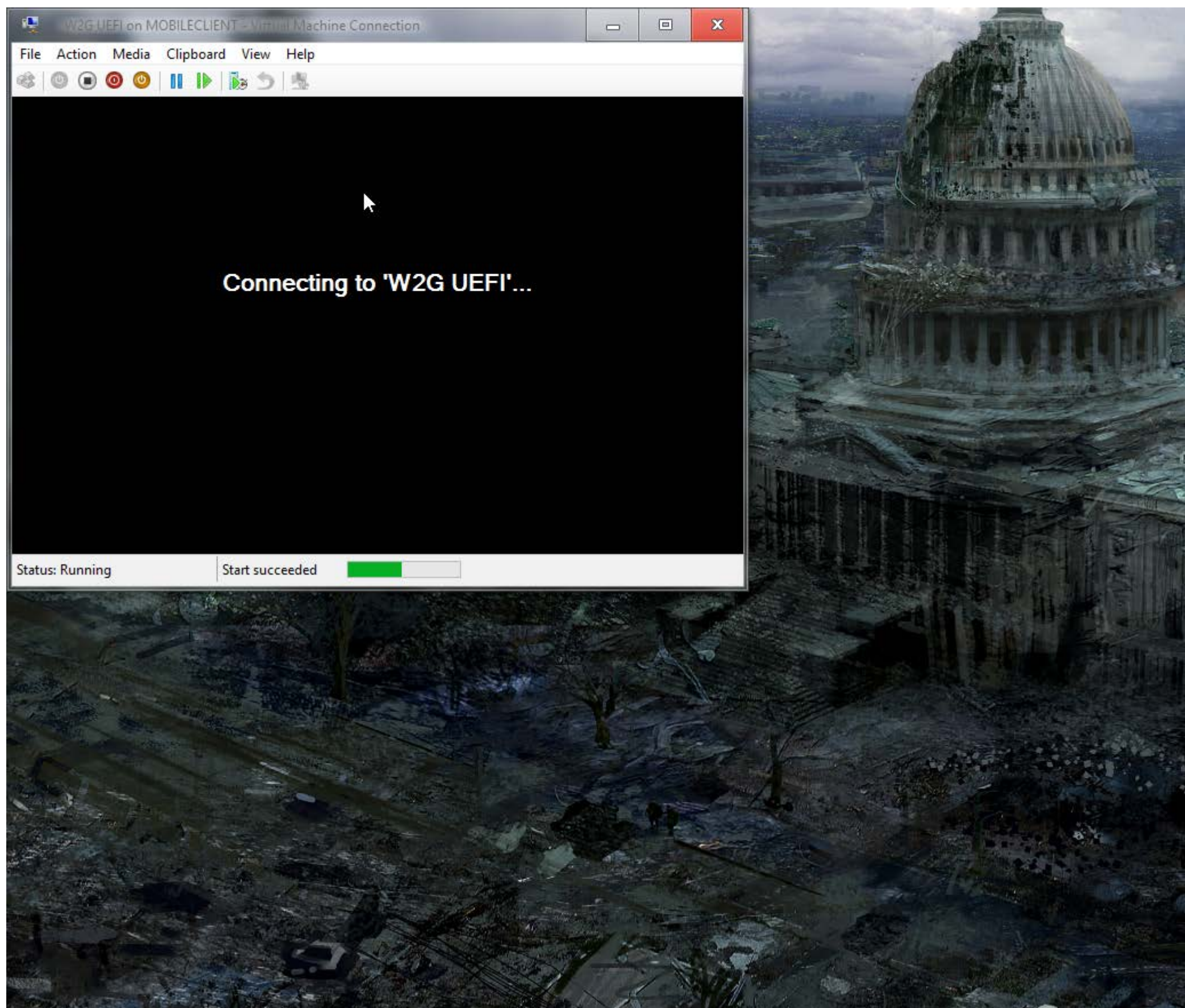


If you used WDS the drive will now fail to boot as the installer only copied the bios boot files so use the following commands

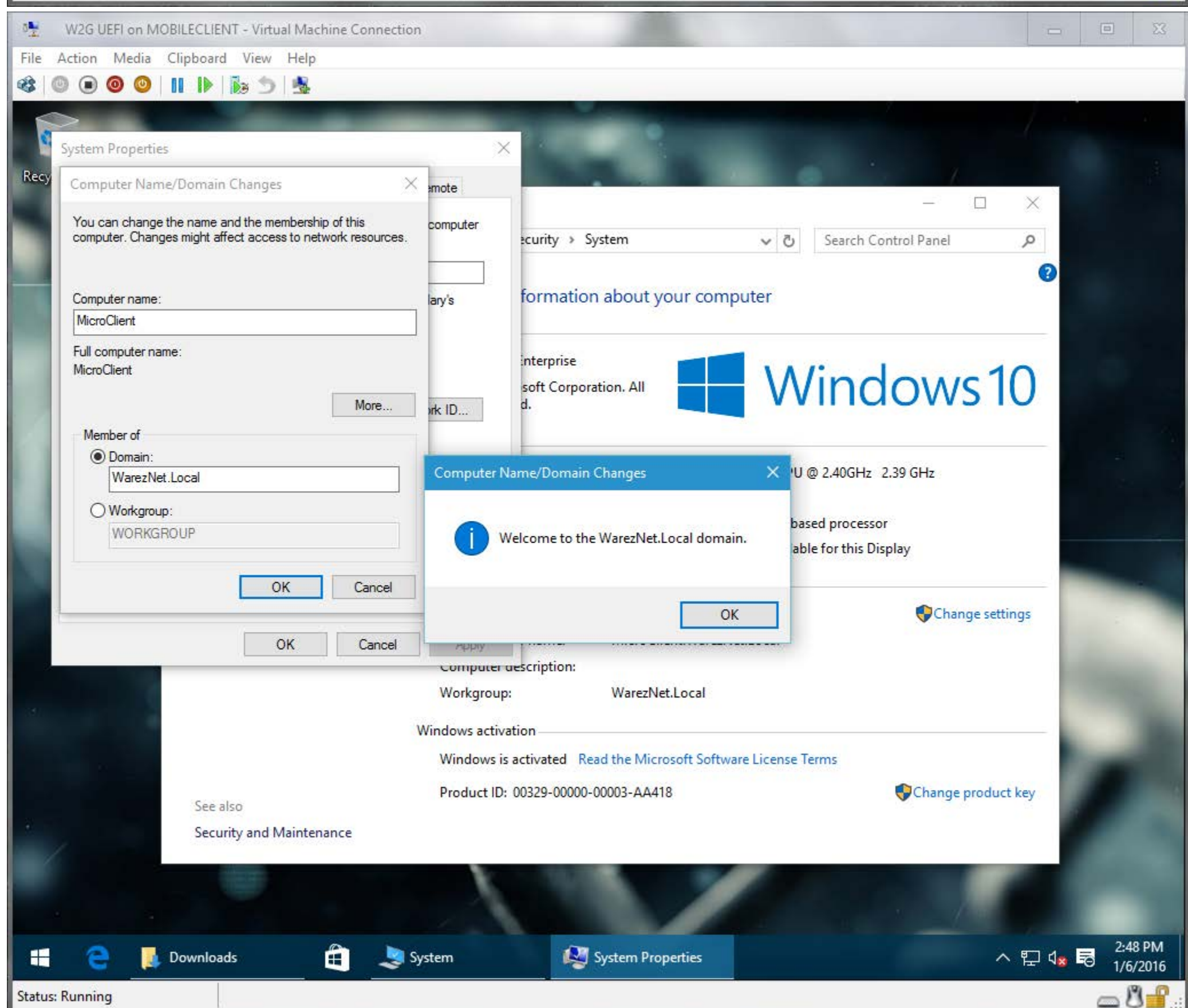
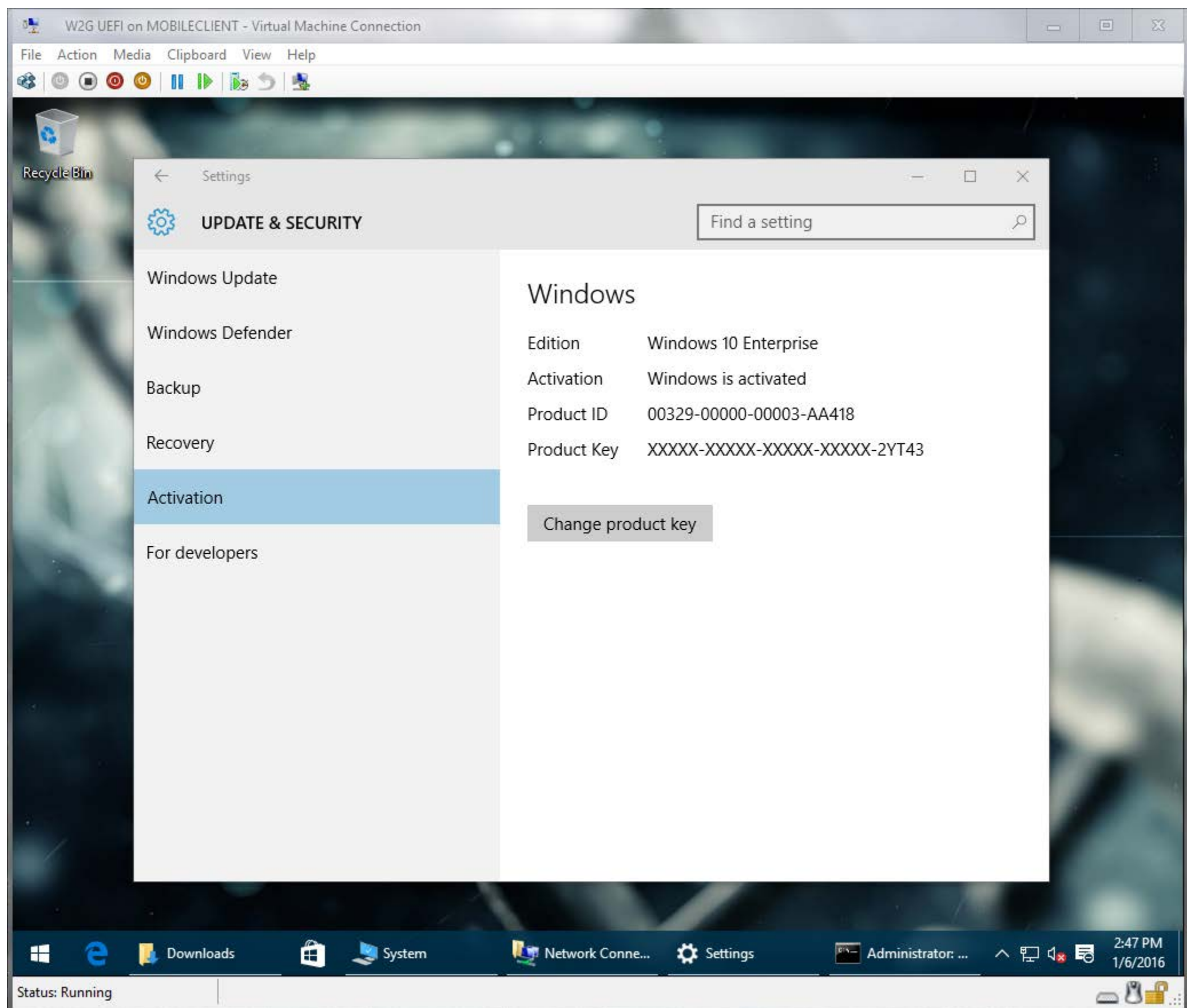




The UEFI machine should now boot

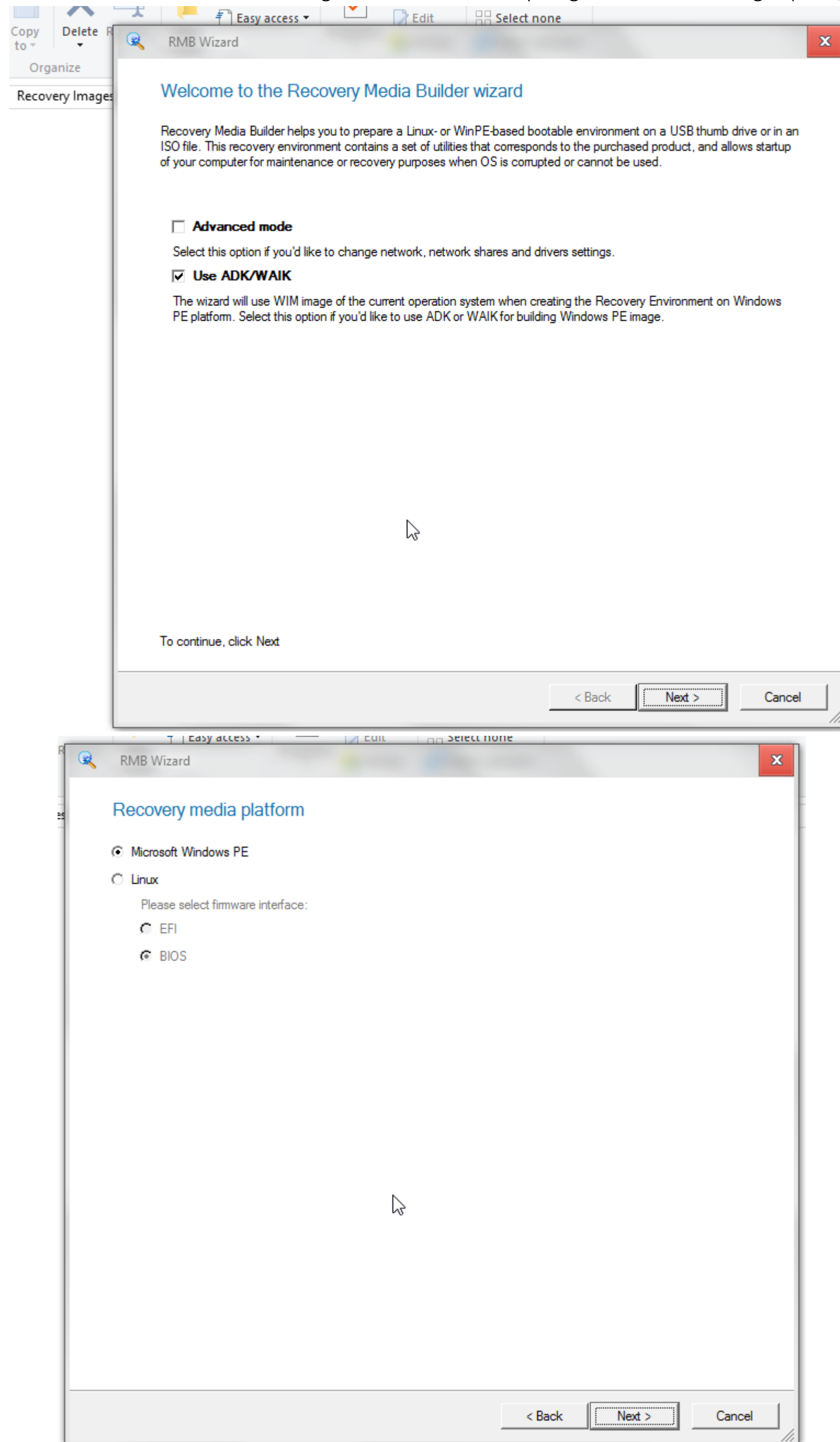



Now you can activate/domain join/install whatever you need



So that's the Windows To Go part completed now for the recovery and installation images.

To start this off build a Windows PE boot disk like im doing here with the latest paragon hard disk manager (UEFI/Secure Boot Compatible)



 RMB Wizard ✕

### Recovery media format


☒ ISO image


Please specify image file location:

Browse...


☐ Removable flash media

Please select USB-flash drive:

 USB Drive 1, Realtek PCIE Card Reader (119 GB)

 USB Drive 2, Kingston DT Workspace (119.2 GB)

< Back Next > Cancel

 RMB Wizard ✕

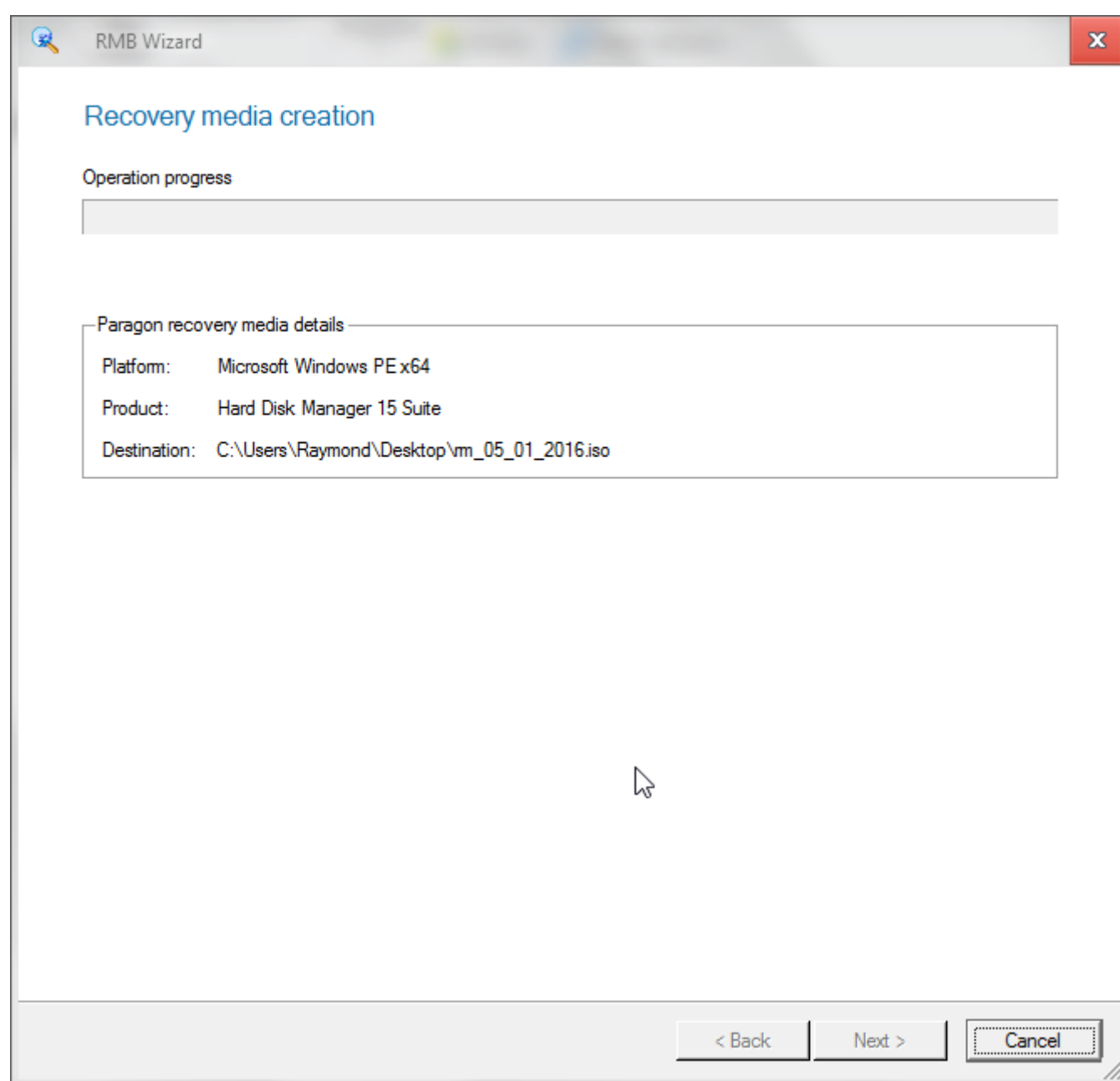
### Please specify where to find WAIK/ADK

Path to installed WAIK/ADK:

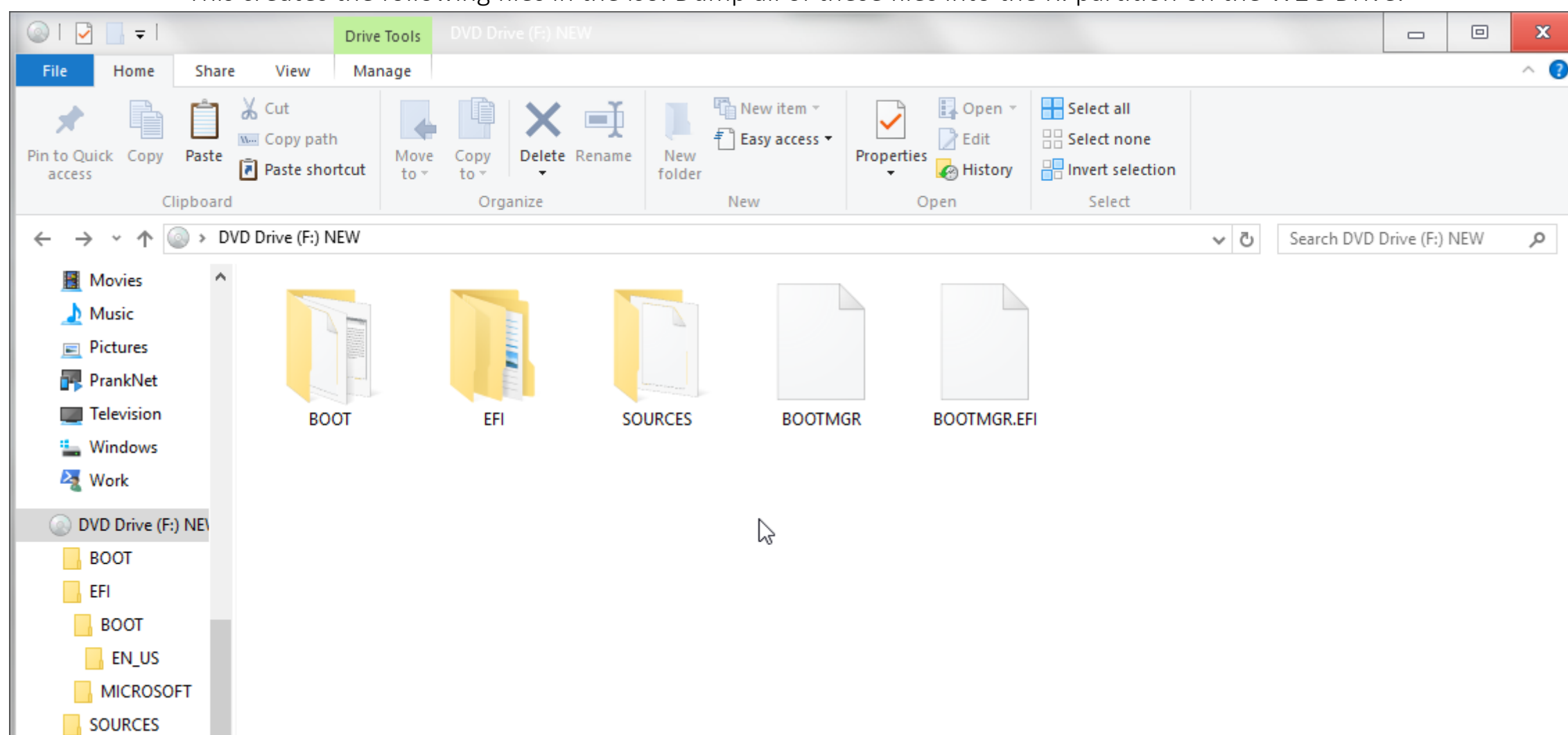
Browse...

[Download WAIK/ADK](#)

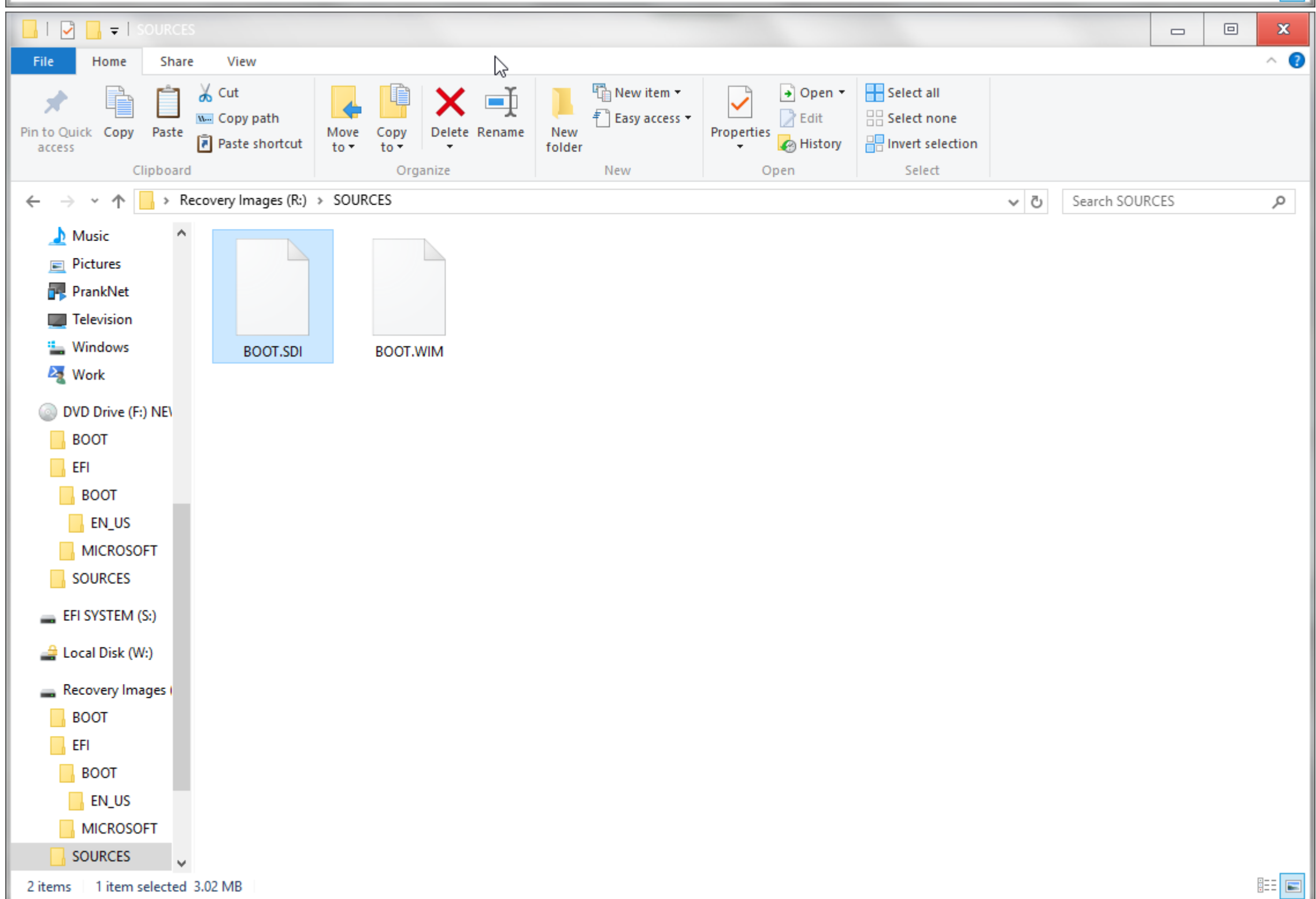
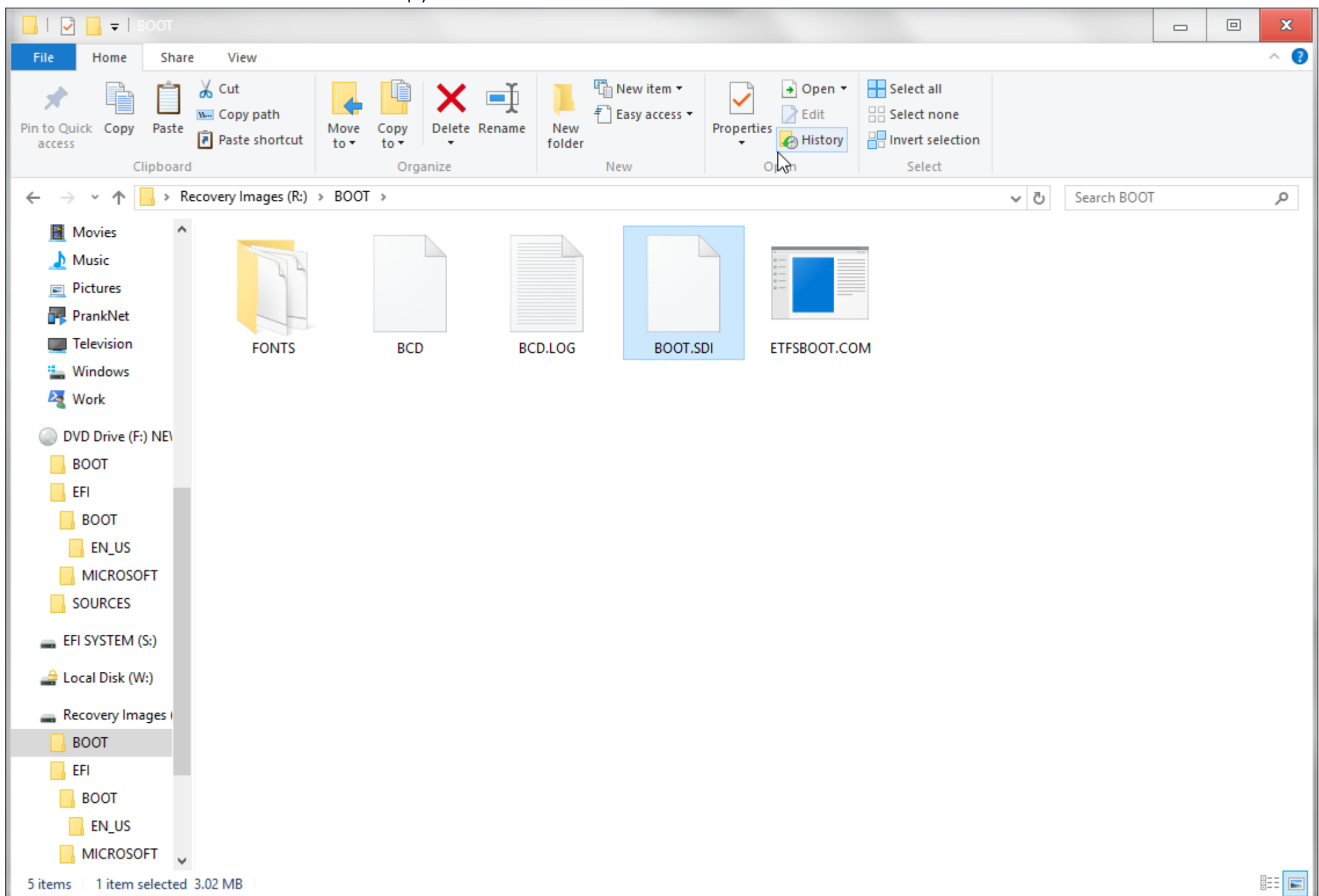
< Back Next > Cancel



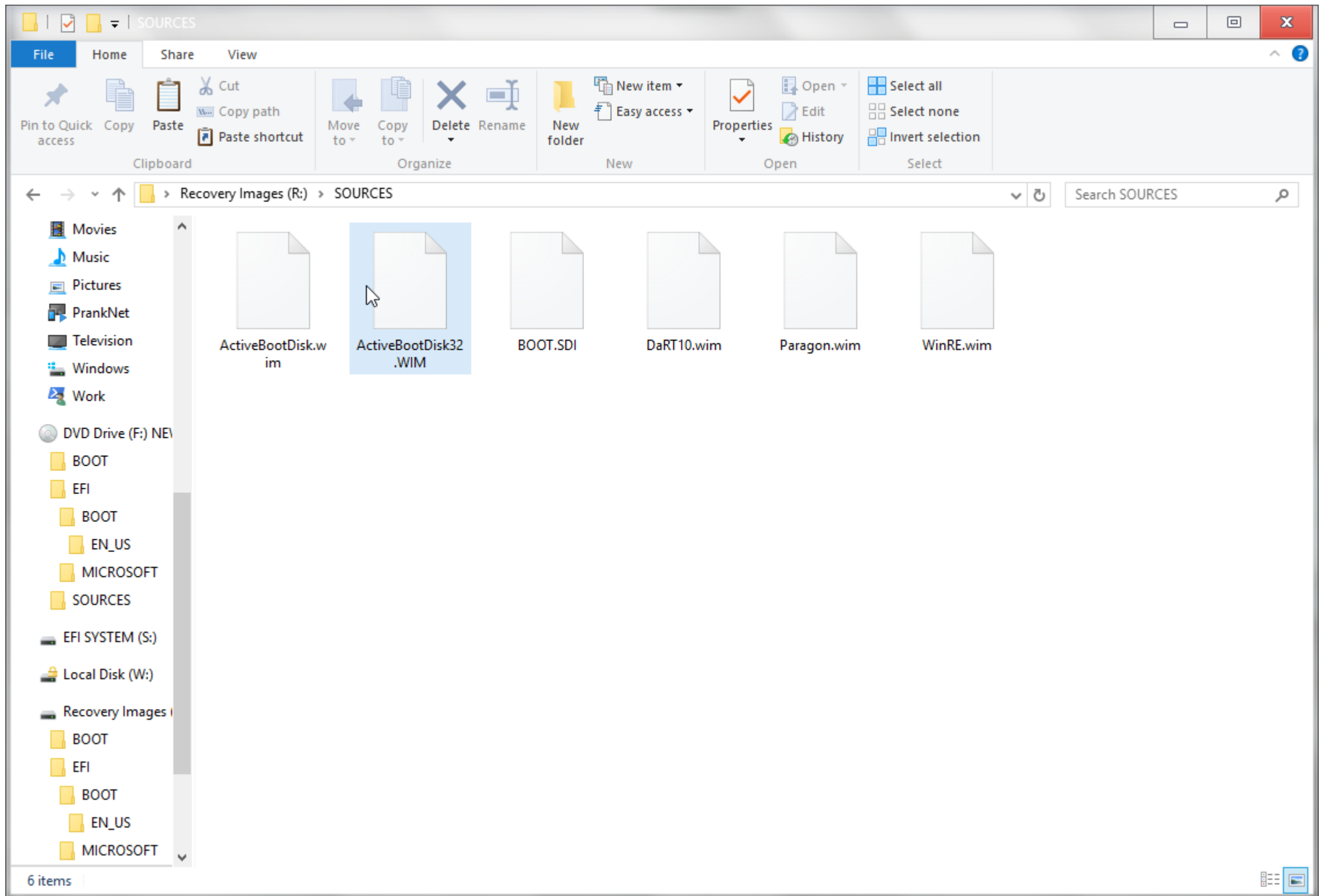
This creates the following files in the iso. Dump all of these files into the R: partition on the W2G Drive.



Now copy the BOOT.SDI from the boot folder to the sources folder



Now you can place any Windows PE boot images into the sources folder and rename them so they don't overwrite.



Now comes the difficult part. We need to add these boot images to the boot menu. This is the code I used

```
bcdedit /export C:\ProgramData\WarezNet\WarezNet_Source.bcd
bcdedit /set {default} bootmenupolicy standard
bcdedit /create {ramdiskoptions}
bcdedit -set {ramdiskoptions} ramdisksdidevice partition=R:
bcdedit -set {ramdiskoptions} ramdisksdipath \sources\boot.sdi
bcdedit -set {bootmgr} timeout 5

for /f "tokens=1-5" %a in ('Bcdedit /create /d "Windows Recovery Environint" /application osloader') do set guid1=%c
bcdedit -set %guid1% device ramdisk=[R:]\sources\WinRE.wim,{ramdiskoptions}
bcdedit -set %guid1% path \windows\system32\winload.efi
bcdedit -set %guid1% osdevice ramdisk=[R:]\sources\WinRE.wim,{ramdiskoptions}
bcdedit -set %guid1% winpe yes
bcdedit -set %guid1% nx optin
bcdedit -set %guid1% detecthal yes
bcdedit -set %guid1% systemroot \Windows
bcdedit -displayorder %guid1% -addlast

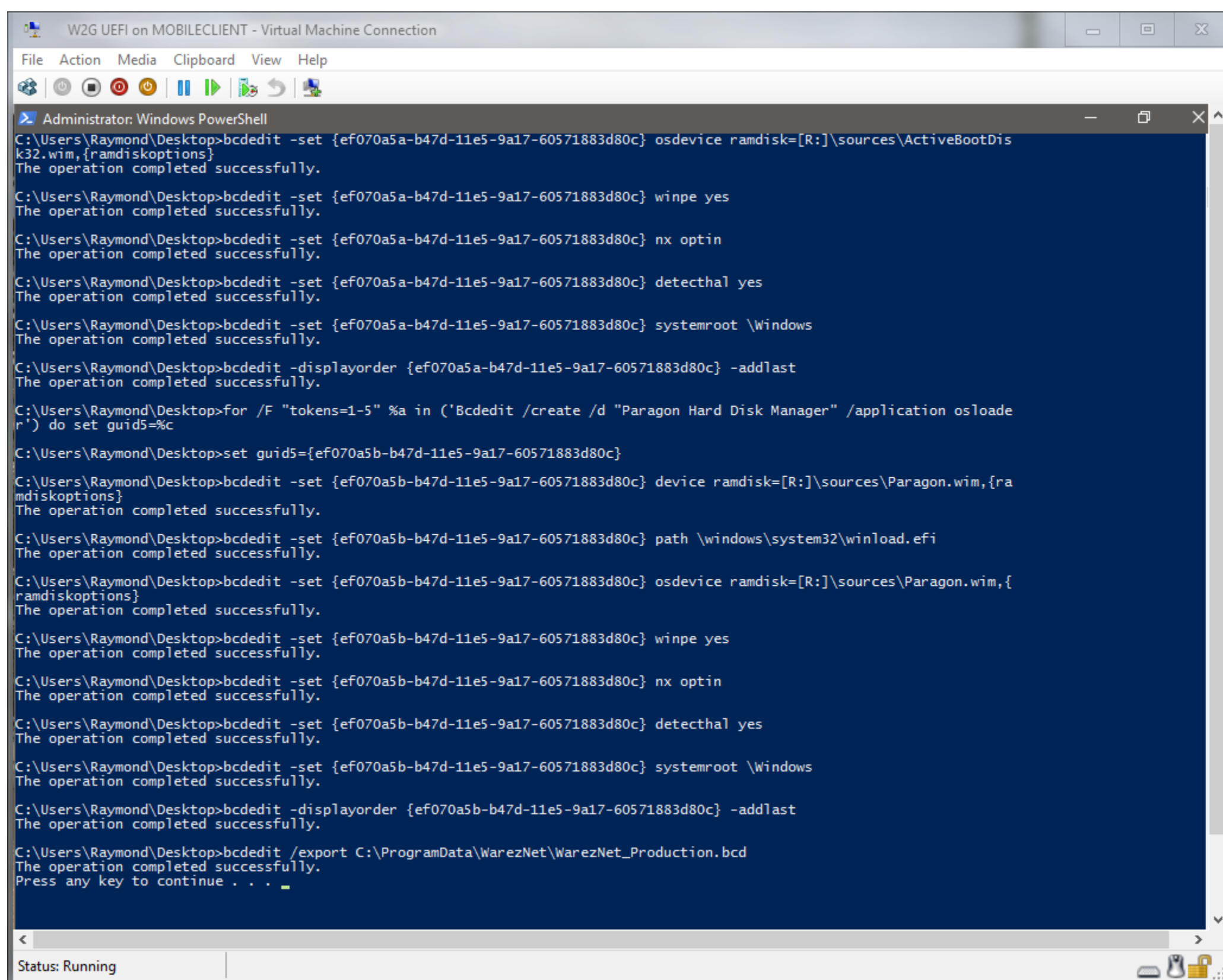
for /f "tokens=1-5" %a in ('Bcdedit /create /d "Microsoft DaRT" /application osloader') do set guid2=%c
bcdedit -set %guid2% device ramdisk=[R:]\sources\DaRT10.wim,{ramdiskoptions}
bcdedit -set %guid2% path \windows\system32\winload.efi
bcdedit -set %guid2% osdevice ramdisk=[R:]\sources\DaRT10.wim,{ramdiskoptions}
bcdedit -set %guid2% winpe yes
bcdedit -set %guid2% nx optin
bcdedit -set %guid2% detecthal yes
bcdedit -set %guid2% systemroot \Windows
bcdedit -displayorder %guid2% -addlast

for /f "tokens=1-5" %a in ('Bcdedit /create /d "Active Boot Disk" /application osloader') do set guid3=%c
bcdedit -set %guid3% device ramdisk=[R:]\sources\ActiveBootDisk.wim,{ramdiskoptions}
bcdedit -set %guid3% path \windows\system32\winload.efi
bcdedit -set %guid3% osdevice ramdisk=[R:]\sources\ActiveBootDisk.wim,{ramdiskoptions}
bcdedit -set %guid3% winpe yes
bcdedit -set %guid3% nx optin
bcdedit -set %guid3% detecthal yes
bcdedit -set %guid3% systemroot \Windows
bcdedit -displayorder %guid3% -addlast

for /f "tokens=1-5" %a in ('Bcdedit /create /d "Active Boot Disk 32" /application osloader') do set guid4=%c
bcdedit -set %guid4% device ramdisk=[R:]\sources\ActiveBootDisk32.wim,{ramdiskoptions}
bcdedit -set %guid4% path \windows\system32\winload.efi
bcdedit -set %guid4% osdevice ramdisk=[R:]\sources\ActiveBootDisk32.wim,{ramdiskoptions}
bcdedit -set %guid4% winpe yes
bcdedit -set %guid4% nx optin
bcdedit -set %guid4% detecthal yes
bcdedit -set %guid4% systemroot \Windows
bcdedit -displayorder %guid4% -addlast

for /f "tokens=1-5" %a in ('Bcdedit /create /d "Paragon Hard Disk Manager" /application osloader') do set guid5=%c
bcdedit -set %guid5% device ramdisk=[R:]\sources\Paragon.wim,{ramdiskoptions}
bcdedit -set %guid5% path \windows\system32\winload.efi
bcdedit -set %guid5% osdevice ramdisk=[R:]\sources\Paragon.wim,{ramdiskoptions}
bcdedit -set %guid5% winpe yes
bcdedit -set %guid5% nx optin
bcdedit -set %guid5% detecthal yes
bcdedit -set %guid5% systemroot \Windows
bcdedit -displayorder %guid5% -addlast

bcdedit /export C:\ProgramData\WarezNet\WarezNet_Production.bcd
```



```
Administrator: Windows PowerShell
C:\Users\Raymond\Desktop>bcdedit -set {ef070a5a-b47d-11e5-9a17-60571883d80c} osdevice ramdisk=[R:]\sources\ActiveBootDis
k32.wim,{ramdiskoptions}
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -set {ef070a5a-b47d-11e5-9a17-60571883d80c} winpe yes
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -set {ef070a5a-b47d-11e5-9a17-60571883d80c} nx optin
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -set {ef070a5a-b47d-11e5-9a17-60571883d80c} detecthal yes
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -set {ef070a5a-b47d-11e5-9a17-60571883d80c} systemroot \Windows
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -displayorder {ef070a5a-b47d-11e5-9a17-60571883d80c} -addlast
The operation completed successfully.

C:\Users\Raymond\Desktop>for /F "tokens=1-5" %a in ('bcdedit /create /d "Paragon Hard Disk Manager" /application osload
e r') do set guid5=%c

C:\Users\Raymond\Desktop>set guid5={ef070a5b-b47d-11e5-9a17-60571883d80c}

C:\Users\Raymond\Desktop>bcdedit -set {ef070a5b-b47d-11e5-9a17-60571883d80c} device ramdisk=[R:]\sources\Paragon.wim,{ra
mdiskoptions}
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -set {ef070a5b-b47d-11e5-9a17-60571883d80c} path \windows\system32\winload.efi
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -set {ef070a5b-b47d-11e5-9a17-60571883d80c} osdevice ramdisk=[R:]\sources\Paragon.wim,{
ramdiskoptions}
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -set {ef070a5b-b47d-11e5-9a17-60571883d80c} winpe yes
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -set {ef070a5b-b47d-11e5-9a17-60571883d80c} nx optin
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -set {ef070a5b-b47d-11e5-9a17-60571883d80c} detecthal yes
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -set {ef070a5b-b47d-11e5-9a17-60571883d80c} systemroot \Windows
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit -displayorder {ef070a5b-b47d-11e5-9a17-60571883d80c} -addlast
The operation completed successfully.

C:\Users\Raymond\Desktop>bcdedit /export C:\ProgramData\WarezNet\WarezNet_Production.bcd
The operation completed successfully.
Press any key to continue . . .
```

When these commands are run the boot images will now appear in the boot menu.

In the case that you don't want to unlock bitlocker and load the full Windows To Go image you can press f11 to pick one of these images.

