

Working and Verified process to obtain forensic image:

Microsoft Surface Pro Tablet

SDFE Jeffrey A. Cunningham

Background: The Microsoft Surface Pro contains a 64bit UEFI motherboard, which requires a 64bit UEFI version of the WINPE built. Also, there is only one USB port (if you have access to the dock it may have more and you can boot from a USB thumbdrive and image to another external, but in our examination we only had access to the tablet itself, henceforth the use of a 1TB external HDD) and can use a USB hub to attach the hard disk drive (HDD), keyboard and mouse. This boot method does however allow touch screen access.

There are many methods out there that will create a WINPE or WINFE. This by far is the easiest method I have found to create an external USB storage boot device. Once you make it once it gets easier. There are many custom applications you can add later and even change the wallpaper so you can identify it was your device that booted. I considered creating an ISO, but many devices no longer come with a CD/DVD drive and most definitely a tablet does not usually come with one.

Highly emphasized to test and validate your build before using on a piece of evidence. You will be the one testifying to the process.

Ten steps for success provided. Green highlighted areas indicate information of importance and yellow highlighted areas are commands entered.

1. Forensic Wipe of your 1TB external HDD
2. Follow Microsoft instructions:

5/14/2014 WinPE: Install on a Hard Drive (Flat Boot or Non-RAM)
<http://technet.microsoft.com/en-us/library/hh825045.aspx>

WinPE: Install on a Hard Drive (Flat Boot or Non-RAM)

Applies To: Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2
Windows Preinstallation Environment (Windows PE) is a minimal operating system where you can prepare a PC for installation, deployment, and servicing of Windows.

Here's how to download and install it to an internal or external hard drive.
These instructions show how to set up a basic Windows PE installation that runs from the drive. This can sometimes give you better performance than booting from memory, and can help you run Windows PE on PCs or virtual environments with low memory.

This procedure is also known as a *non-RAMDISK boot*, or a *flat boot*.

Note:

When Windows PE is running from the drive, you must turn off the PC before disconnecting the drive to avoid losing your work.

Install the Windows ADK

Create a Set of Either 32-bit or 64-bit Windows PE Files

1. Click Start, and type deployment. Right-click Deployment and Imaging Tools Environment and then select Run as administrator.
2. In the Deployment and Imaging Tools Environment, copy the Windows PE files for the PCs you want to boot.

The 64-bit version of Windows PE can boot 64-bit UEFI and 64-bit BIOS PCs:

```
copy /b amd64 C:\WinPE_amd64
```

The 32-bit version of Windows PE can boot 32-bit UEFI, 32-bit BIOS, and 64-bit BIOS PCs:

```
copy /b x86 C:\WinPE_x86
```

Create a Working Directory for Windows PE Files

1. Click Start, and type deployment. Right-click Deployment and Imaging Tools Environment and then select Run as administrator.
2. From the Deployment and Imaging Tools Environment, create a working directory for the Windows PE files.

Install Windows PE to the Media

```
copy /b amd64 C:\WinPE_amd64
```

1. Use DiskPart to prepare the partitions.

Note: The following commands prepare a USB hard drive that can boot on either a BIOS-based or UEFI-based PC.

On UEFI-based PCs, Windows PE requires a boot partition formatted using the FAT32 file format, which only supports file sizes up to 4 GB.

We recommend creating a separate partition on the drive, formatted using NTFS, so

that you can store Windows images and other large files.

where *<disk number>* is the listed number of the external USB hard drive.

```
diskpart
list disk
select <disk number>
clean
rem === Create the Windows PE partition. ===
create partition primary size=2000
format quick fs=fat32 label="Windows PE"
assign letter=P
active
rem === Create a data partition. ===
create partition primary
format fs=ntfs quick label="Other files"
assign letter=O
list vol
exit
```

2. Apply the Windows PE image to the hard drive.

```
dism /Apply-Image /ImageFile:"C:\WinPE_amd64\media\sources\boot.wim" /Index:1
/ApplyDir:P:\
```

3. Set up the boot files.

```
BCDboot P:\Windows /s P: /f ALL
```

Note: Ignore any warning messages that say "Warning: Resume application not found."

3. Place "EnCase Imager 64bit" exe to root of P:

(Note: The 32bit system files are not in this so FTK Imager is not an option at this time.

```
*****Convert to a WINFE so it does not mount the internal drives*****
```

4. Edit SYSTEM registry keys: Instructions at <http://gverswijvel.wordpress.com/tag/san-policy-4/> by opening the cmd shell.

```
REG LOAD HKLM\WINFE32 P:\Windows\System32\config\SYSTEM
```

```
REG ADD HKLM\WINFE32\ControlSet001\Services\MountMgr /v NoAutoMount /t REG_DWORD /d 1 /f
```

```
REG ADD HKLM\WINFE32\ControlSet001\Services\partmgr\Parameters /v SanPolicy /t REG_DWORD /d 4 /f
```

```
REG ADD HKLM\WINFE32\ControlSet001\Control\FileSystem /v DisableDeleteNotification /t REG_DWORD /d 1 /f
```

```
REG UNLOAD HKLM\WINFE32
```

5. This method allows the use of a USB hub. Attach keyboard, mouse and HDD to powered USB hub. The HDD needs to be on its own power side of the hub. Example: If you use a four port hub, plug the keyboard and mouse side by side and the HDD on its own side (for some reason this has to be done).

6. Disable TPM and Secure boot. Microsoft instructions

<http://www.microsoft.com/surface/en-us/support/warranty-service-and-recovery/how-to-use-the-bios-uefi>

You can access the following firmware features on Surface Pro and Surface Pro 2:

- **Secure Boot Control.** Secure Boot technology blocks the loading of uncertified bootloaders and drives.
- **Trusted Platform Module (TPM).** TPM technology provides major advancement over BIOS in the area of hardware-based security features.

How do I get to the UEFI settings?

The UEFI settings can only be adjusted during system startup. To load the UEFI firmware settings menu:

Step

1: Shut down (power off) Surface.

Step

2: Press and hold the volume-up (+) rocker on the side of Surface.

Step Press and release the power button on the top of Surface, then release the

3: volume-up rocker. The UEFI menu will display within a few seconds.

UEFI menu options

The UEFI settings that you can modify are:

- **Trusted Platform Module (TPM)**
The currently configured state of TPM (**Enabled** or **Disabled**) is highlighted. To change the state, tap the other one, then confirm on exit.

Secure Boot Control

The currently configured state of Secure Boot (**Enabled** or **Disabled**) is highlighted. To change the state, tap the other one, then confirm on exit.

7. Boot from external HDD: Microsoft instructions

<http://www.microsoft.com/surface/en-us/support/storage-files-and-folders/boot-surface-pro-from-usb-recovery-device>

Start from a bootable USB device when Surface is off

Step

1: Attach a bootable USB device to the USB port.

Step

2: Press and hold the volume-down (–) rocker.

Step

3: Press and release the power button.

Step 4: When the Surface logo appears, release the volume rocker. Surface will start the software on your USB device.

8. You will be presented with a CMD window. DIR to the root directory. Execute the EnCase Imager 7 64bit exe.

You will be prompted that Multilanguage support (MLANG) is not installed, but it can be ignored.

Image the HDD to be the NTFS partition you created.

9. **SHUTDOWN** the tablet. Use the command "wpeutil shutdown"

10. Now add your EnCase image files to your case and verify.