PassMark® White Paper

Building a bootable OSForensics image (WinPE 3.0)

Edition: 2.1

Date: 10 August 2012

Overview

OSForensics can be configured to run from a bootable CD/DVD or USB Flash Drive (UFD). This can be useful so as to not run on the target operating system or if the target operating system is inoperable. This document aims to assist people in setting up an environment that allows PassMark OSForensics to be used in these situations.

To run OSForensics on a system without an operating system you need to set up a "Pre-install environment" that allows Microsoft Windows to be booted from a CD/DVD or USB Flash Drive. This document describes setting up a Microsoft Window Pre-install environment (WinPE) environment that includes both Windows and OSForensics on a bootable CD/DVD or bootable USB Flash Drive (UFD). The document also describes how to inject new device drivers into the Windows image for system specific hardware (if required).

Audience

This paper is targeted at companies and individuals that need to build a Bootable version of OSForensics. It is aimed at people with technical PC knowledge.

Standard Environment

The standard environment described in this document is:

- WinPE 3.0
- OSForensics Beta (or higher).
- Hardware including at least 512MB of RAM.

Limitations

Windows PE 3.0 can be obtained with the Microsoft Windows Automated Installation Kit (WAIK) or from the Microsoft OEM Preinstall Kit (OPK) Tools. There are differences with the capabilities of the PE in each of these versions, but these differences have no impact on this guide.

This guide is written using the OPK Tools and WAIK. It will also make x86 and x64 versions, and you need to use drivers suitable to your build. It is recommended that you track which drivers (if required) you end up putting into your PE.

Note that in our testing the 32-bit version of OSForensics will not run in a 64-bit WinPE environment – use the 64-bit version of OSForensics in this scenario.

You will need to run the tools with (elevated) Administrator privileges.

Downloads

Microsoft Windows Automated Installation Kit (WAIK) can be downloaded here:
http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5753

Microsoft OEM Preinstall Kit (OPK) can be downloaded here (you will need to be a registered Microsoft OEM and have an account with Microsoft):
http://www.microsoft.com/oem/sblicense/OPK/default.mspx
or
http://oem.microsoft.com/script/contentpage.aspx?PageID=501924

The latest version of the OSForensics can be downloaded here:
http://www.osforensics.com/

Building a Preinstall Environment

This section describes how to build a WinPE 3.0 boot CD or DVD with OSForensics.

This is a final walkthrough to create a functional PE image that will automatically load OSForensics upon opening. You need to install the WAIK/OPK Tools first (as well as OSForensics) before you should start. Also make sure to have your drivers ready. All commands are done by using the WAIK or OPK *Windows PE Tools Command Prompt*, which is a special paths CMD that will appear in the Start menu after you install that tool.

If you are running Windows 7, you will need to launch "Windows PE Tools Command Prompt" with elevated administrator privileges.
i.e. Start … All Programs … Microsoft Windows AIK … Deployment Tools Command Prompt
(Right mouse click and select 'Run as administrator').

1. Create the base PE source.
The destination folder cannot already exist.
copype x86 c:\osfpe

2. Mount the WinPE source
Extract the base image winpe.wim to a local directory:
DISM /Mount-wim /WimFile:c:\osfpe\winpe.wim /index:1 /MountDir:c:\osfpe\mount

Note: After mounting the base image, you can use the "DISM /Get-Packages" command to see which packages are installed and available for installation.
For example, DISM /image:c:\osfpe\mount\ /Get-Packages

3. Install the packages that are needed.
DISM /image:c:\osfpe\mount /Add-Package /PackagePath:"C:\Program Files\Windows AIK\Tools\PETools\x86\WinPE_FPs\winpe-wmi.cab"
DISM /image:c:\osfpe\mount /Add-Package /PackagePath:"C:\Program Files\Windows AIK\Tools\PETools\x86\WinPE_FPs\winpe-hta.cab"
DISM /image:c:\osfpe\mount /Add-Package /PackagePath:"C:\Program Files\Windows AIK\Tools\PETools\x86\WinPE_FPs\winpe-scripting.cab"

The packages available are as listed in the Microsoft WinPE documentation. An extract follows:

Package Name	Description
WinPE-FONTSupport-*<region>*	Additional font support for the following languages: ja-JP, ko-KR, zh-CN, zh-HK, and zh-TW.
WinPE-HTA	HTML Application support. Enables the creation of GUI applications using the Windows Internet Explorer® script engine and HTML services.
Winpe-LegacySetup	The Media Setup feature package. All Setup files from the \Sources folder on the Windows media. Add this package when servicing Setup or the \Sources folder on the Windows media. Must be added with the Setup feature package. To add a new Boot.wim to the media, add either child package in addition to the Setup and Media packages. This package is required to support Windows Server® 2008 R2 installation.
WinPE-MDAC	Microsoft® Data Access Component support. Enables queries to SQL servers with Active Directory Objects (ADO). Example usage: building a dynamic Unattend from unique system information.
WinPE-PPPoE	Enables Point-to-Point Protocol over Ethernet (PPPoE) support. Create, connect, disconnect and delete PPPoE connections from Windows PE.
WinPE-Scripting	Windows Script Host (WSH) support. Enables batch file processing using WSH script objects.
WinPE-Setup	The Setup feature package (parent). All Setup files from the \Sources folder common to Client and Server.
WinPE-Setup-Client	The Client Setup feature package (child). The Client branding files for Setup. Must be added after the Setup feature package.
WinPE-Setup-Server	The Server Setup feature package (child). The Server branding files for Setup. Must be added after the Setup feature package.
WinPE-SRT	The Windows Recovery Environment feature package. Provides a recovery platform for automatic system diagnosis and repair and the creation of custom recovery solutions.
WinPE-WMI	Windows Management Instrumentation (WMI) support. A subset of the WMI providers that enables minimal system diagnostics.
WinPE-WDS-Tools	The Windows Deployment Services tools feature package. Includes APIs to enable a multicast scenario with a custom Windows Deployment Services client and Image Capture utility.

Package Name	*Description*
WinPE-FONTSupport-<region>	Additional font support for ja-jp, ko-kr, zh-cn, zh-hk, and zh-tw.
WinPE-HTA	HTML Application support
WinPE-MDAC	Microsoft Data Access Component support
WinPE-Scripting	Windows Script Host support

WinPE-SRT	Windows Recovery Environment support
WinPE-WMI	Windows Management Instrumentation (WMI) support
WinPE-WDS-Tools	The Windows Deployment Services tools feature package

4. Install the required fonts and device drivers
OSForensics requires the following fonts:

- Arial
- Calibri
- Courier New
- Microsoft Sans Serif

These can be copied from your Windows installation disk (or an existing Windows installation C:\Windows\Fonts) to C:\osfpe\mount\Windows\Fonts.

Install the NIC and Mass Storage drivers that you need. In many cases this is not required.
DISM /image:c:\osfpe\mount\ /Add-Driver /driver:c:\osfpe\drivers\nic /recurse / ForceUnsigned
DISM /image:c:\osfpe\mount\ /Add-Driver /driver:c:\osfpe\drivers\hddc /recurse / ForceUnsigned

Note: By including the /recurse switch you tell to the command to recurse the drivers' subfolders for valid .inf drivers and by including the /ForceUnsigned you tell the command to ignore driver signing requirements.

Note: After installing the drivers, you can use the "DISM /Get-Drivers" command to see which drivers are installed.
For example, DISM /image:c:\osfpe\mount\ /Get-Drivers -- View 3rd party drivers
DISM /image:c:\osfpe\mount\ /Get-Drivers /all -- View all drivers

5. Install the OSForensics software
After step 2, you can find the directory structure of the PE with Windows Explorer.

In OSForensics, choose the option to Install to USB. Specify the Installation location Directory as mount\Program Files\OSForensics.

Note: If you want your own image for the WinPE background, replace the default image mount\Windows\System32\winpe.bmp with you own image.

6. Automate the launching of OSForensics.
There are two methods that you can use to launch OSForensics. You can either edit \mount\windows\system32\startnet.cmd or create a winpeshl.ini file and place it in the \mount\windows\system32 directory. For testing purposes, it is recommended you use the startnet.cmd method, because you will have access to the command prompt. If you use winpeshl.ini, you will not be able to use a command prompt, but will stop regular users from having direct access into the PE itself once booted. You should not use both options, if winpeshl.ini is present, it will ignore the startnet.cmd file.

Winpeshl.ini
[LaunchApps]

%SYSTEMDRIVE%\Windows\System32\wpeinit.exe
"%SYSTEMDRIVE%\Program Files\OSForensics\Program Files\osf32.exe"
(or "%SYSTEMDRIVE%\Program Files\OSForensics\Program Files\osf64.exe" – 64bit image)

Startnet.cmd
wpeinit
"X:\Program Files\OSForensics\Program Files\osf32.exe"
(or "X:\Program Files\OSForensics\Program Files\osf64.exe" – 64bit image)

7. Commit the changes and save the image
Create a winpe.wim image from the local directory.
DISM /unmount-Wim /MountDir:c:\osfpe\mount /Commit

8. Make the boot disk
Now at this point you can *rename the c:\osfpe\winpe.wim to boot.wim and place it in the ISO\Sources folder* to burn a CD, USB Flash Drive or you can add it to the Boot Images in Windows Deployment Services.

9a. To make a bootable CD/DVD
To make an iso image for buring to CD:
OSCDIMG -n -h -bc:\osfpe\etfsboot.com c:\osfpe\iso c:\osfpe.iso

Now burn the iso image (c:\osfpe.iso) to the CD/DVD. You can use the CD/DVD burning software that comes with Windows 7 or use third-party software.

9b. To make a bootable USB Flash Drive (UFD)
From the command prompt, partition and format the UFD. Make sure you select the correct disk number, as this will delete everything on the disk (the below example shows a UFD with physical disk number 2 and volume letter G.

C:\Users\Administrator>diskpart
DISKPART> list disk
DISKPART> select disk 2
DISKPART> clean
DISKPART> create partition primary
DISKPART> select partition 1
DISKPART> active
DISKPART> format fs=fat32 (or ntfs)
DISKPART> assign
DISKPART> exit

C:\Users\Administrator>xcopy c:\osfpe\iso*.* G:\ /s /e /f

Example WinPE build

A 64-bit build example:

<Open the *Windows PE Tools Command Prompt* with administrator privileges>

copype amd64 c:\osfpe_x64
DISM /Mount-wim /WimFile:c:\osfpe_x64\winpe.wim /index:1 /MountDir:c:\osfpe_x64\mount
DISM /image:c:\osfpe_x64\mount /Add-Package /PackagePath:"C:\Program Files\Windows AIK\Tools\PETools\amd64\WinPE_FPs\winpe-wmi.cab"
DISM /image:c:\osfpe_x64\mount /Add-Package /PackagePath:"C:\Program Files\Windows AIK\Tools\PETools\amd64\WinPE_FPs\winpe-hta.cab"
DISM /image:c:\osfpe_x64\mount /Add-Package /PackagePath:"C:\Program Files\Windows AIK\Tools\PETools\amd64\WinPE_FPs\winpe-scripting.cab"
<Install required device drivers and fonts for your target Operating System – refer Step 4>
<Install 64-bit OSForensics – refer step 5>
<Create startnet.cmd or winpeshl.ini – refer step 6>

DISM /unmount-Wim /MountDir:c:\osfpe_x64\mount /Commit
<Copy winpe.wim to iso\sources\boot.wim – refer step 8>
OSCDIMG -n -h -bc:\osfpe_x64\etfsboot.com c:\osfpe_x64\iso c:\osfpe_x64.iso

<Burn c:\osfpe_x64.iso to a CD>

Please consult the documentation that comes with the WAIK/OPK Tools for further information or configurations.

Adding drivers to the WinPE image

This section describes how to install device drivers into an existing WinPE image for updated hardware.

1. Make a copy of the WinPE image to work with.
For example, if your WinPE image is on a UFD, copy the contents of the UFD to c:\osfpe

2. Create a directory to mount the image into.
e.g. c:\osfpe\mount (this must be an empty directory).

3. Copy your driver files
Copy your driver files (*.inf, *.sys, *.cat etc) to a temporary directory, e.g. copy the 32-bit Passmark USB 2.0 Loopback drivers to c:\osfpe\drivers.

4. Check if your image file (.wim) has more than 1 image in it.
DISM /Get-Wiminfo /wimfile:c:\osfpe\sources\boot.wim

```
…
Index : 1
…
```

5. Mount the WinPE image from the .wim file
Extract the base image to a local directory.
DISM /Mount-wim /WimFile:c:\osfpe\sources\boot.wim /index:1 /MountDir:c:\osfpe\mount

6. Install an INF package (typically a driver) to a Windows PE image.
DISM /image:c:\osfpe\mount\ /Add-Driver /driver:c:\osfpe\drivers /recurse /ForceUnsigned

```
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385

Image Version: 6.1.7600.16385

Searching for driver packages to install...
Found 1 driver package(s) to install.
Installing 1 of 1 - c:\osfpe\drivers\PMUSBosfpe2.inf: The driver package was successfully installed.
The operation completed successfully.
```

7. Save the changes
Create a WinPE image from the local directory.
DISM /unmount-Wim /MountDir:c:\osfpe\mount /Commit

8. Create a bootable CD/DVD or UFD.

Follow steps 8 and 9 in the "Building a Preinstall Environment" to create a bootable CD/DVD or UFD.

Troubleshooting

DISM Error 50

Ensure you are using the correct version of WAIK for your current version of Windows.

DISM Error 0xC1420127

If the image was not uncounted cleanly after the last mount you may encounter this error. Ensure the image has been un-mounted and then use the command “dism /cleanup-wim”

Blank screen when booting from USB

After copying the files to the USB and booting from it you may see a blank screen and no windows loading screen is displayed. This may indicate a hardware error with the USB drive that is preventing it from booting and it is recommended to try another USB drive.