White paper

Building a bootable OSForensics (WinPE)

Edition: 1.0

Date: 21 January 2011

OSForensics Version: Beta

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).

This document does not intend to cover product licensing issues and it is up to the reader to review this. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

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

Limitations

Windows PE 2.x 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/downloads/details.aspx?familyid=94bb6e34-d890-4932-81a5-5b50c657de08&displaylang=en
or
http://www.microsoft.com/downloads/details.aspx?FamilyID=c7d4bc6d-15f3-4284-9123-679830d629f2&displaylang=en

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 2.x 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 Vista, you will need to launch "Windows PE Tools Command Prompt" with elevated administrator privileges.

1. Create the base PE source.

The destination folder cannot already exist.

```
copype x86 c:\winpe
```

2. Mount the WinPE source

Extract the base image winpe.wim to a local directory:

```
imagex /mountrw c:\winpe\winpe.wim 1 c:\winpe\mount
```

Note: Using the peimg /list command you can see which packages are installed and available for installation. For example, `peimg /list c:\winpe\mount`

3. Install the packages that are needed.

```
xcopy "c:\program files\windows opk\tools\servicing" c:\winpe\mount\windows /s
          (or xcopy "c:\Program Files\Windows AIK\tools\servicing" c:\winpe\mount\windows /s
           for WAIK)
xcopy "c:\program files\windows opk\tools\x86" c:\winpe\mount\windows /s /Y
          (or xcopy "c:\program files\Windows AIK\tools\x86" c:\winpe\mount\windows /s /Y for
          WAIK)
peimg /install=WinPE-HTA-Package c:\winpe\mount\windows
peimg /install=WinPE-Scripting-Package c:\winpe\mount\windows
peimg /install=WinPE-XML-Package c:\winpe\mount\windows
peimg /install=WinPE-WMI-Package c:\winpe\mount\windows
```

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

Package Name	*Description*
WinPE-FONTSupport-<region>-Packages	Additional font support for ja-jp, ko-kr, zh-cn, zh-hk, and zh-tw.
WinPE-HTA-Package	HTML Application support

WinPE-MDAC-Package	Microsoft Data Access Component support
WinPE-Scripting-Package	Windows Script Host support
WinPE-SRT-Package	Windows Recovery Environment support
WinPE-WMI-Packages	Windows Management Instrumentation (WMI) support
WinPE-XML-Package	Microsoft XML (MSMXL) Parser support

4. Install the required fonts and device drivers

OSForensics requires the following fonts:

- Arial;
- Calibri;
- Courier new;
- Microsoft Sans Serif and
- Tahoma.

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

Install the NIC and Mass Storage drivers that you need. In many cases this is not required.

```
peimg /inf:c:\winpe\drivers\nic\*.inf c:\winpe\mount\windows
peimg /inf:c:\winpe\drivers\hddc\*.inf c:\winpe\mount\windows
```

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. 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\osf.exe
```

Startnet.cmd

```
wpeinit
"x:\Program Files\osforensics\osf.exe"
```

7. Prep the PE source

This command will remove any packages and language packs that are not designated for the final image.

```
peimg /prep c:\winpe\mount\windows /f
```

8. Save the changes

Create a winpe.wim image from the local directory.

```
imagex /unmount c:\winpe\mount /commit
```

9. 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.

10a. To make a bootable CD/DVD

To make an iso image for buring to CD:

```
oscdimg -n -h –b c:\winpe\etfsboot.com c:\winpe\iso c:\winpe.iso
```

Now burn the iso image (c:\winpe.iso) to the CD/DVD. You can get CD/DVD burning software from the Windows 2003 Resource Kit (cdburn and dvdburn) or use third-party software.

10b. 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> select disk 2
DISKPART> list disk
DISKPART> clean
DISKPART> create partition primary
DISKPART> select partition 1
DISKPART> active
DISKPART> format fs=fat32
DISKPART> assign
DISKPART> exit

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

Example WinPE build

A 64-bit build example:

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

```
c:
cd "C:\Program Files\Windows AIK\Tools\PETools"
copype.cmd amd64 c:\winpe_x64
imagex /mountrw c:\winpe_x64\winpe.wim 1 c:\winpe_x64\mount
xcopy "c:\Program Files\Windows AIK\tools\servicing" c:\winpe_x64\mount\windows /s
xcopy "c:\program files\Windows AIK\tools\x86" c:\winpe_x64\mount\windows /s /Y
peimg /install=WinPE-HTA-Package c:\winpe_x64\mount\windows
peimg /install=WinPE-Scripting-Package c:\winpe_x64\mount\windows
peimg /install=WinPE-XML-Package c:\winpe_x64\mount\windows
peimg /install=WinPE-WMI-Package c:\winpe_x64\mount\windows
<Copy required fonts to WinPE image >
<Install 64-bit OSForensics>
peimg /prep c:\winpe_x64\mount\windows /f
imagex /unmount c:\winpe_x64\mount /commit
<Copy winpe.wim to iso\sources\boot.wim>
oscdimg -n -h -bc:\winpe_x64\etfsboot.com c:\winpe_x64\iso c:\winpe_x64.iso
<Burn c:\winpe_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:\pctk\drivers.

4. Check if your image file (.wim) has more than 1 image in it.

```
imagex /info c:\osfpe\sources\boot.wim
```

```
…
  <IMAGE INDEX="1">
…
```

5. Mount the WinPE image from the .wim file

Extract the base image to a local directory.

```
imagex /mountrw c:\osfpe\sources\boot.wim 1 c:\osfpe\mount
```

6. Install an INF package (typically a driver) to a Windows PE image.

```
peimg /inf=c:\osfpe\drivers\*.inf /image=c:\osfpe\mount
```

```
Preinstallation Environment Image Setup Tool for Windows
Copyright (C) Microsoft Corporation. All rights reserved.

Installing INF package: c:\pctk\drivers\PMUSB2.inf

PEIMG completed the operation successfully.
```

7. Save the changes

Create a WinPE image from the local directory.

```
imagex /unmount c:\osfpe\mount /commit
```

8. Create a bootable CD/DVD or UFD.

Follow steps 9 and 10 in the "Building a Preinstall Environment" to create a bootable CD/DVD or UFD.