GetData: Triage-Compatible WinPE ISO Guide

NOTE: Skip Section 1 if the ISO has been provided

Section 1: Building the Base ISO

Step 1: Install PhoenixPE

1. Download and install the latest version of PhoenixPE from https://github.com/PhoenixPE/PhoenixPE.
2. Use 7Zip to unpack the PhoenixPE files.
3. Locate and run **PEBakeryLauncher.exe** in the unpacked folder.
4. Follow the on-screen instructions to complete the installation.

Step 2: Obtain Windows ISO

1. Obtain a Windows 11 ISO file. If you don't have one, use the **Download Source ISO** button in PhoenixPE's **Source Config** script.
2. Before proceeding, ensure the ISO is compatible by checking the PhoenixPE Source Compatibility guidelines.

Step 3: Mount or Extract ISO

1. You can either mount the ISO or extract its contents using a tool like 7Zip.
2. In PhoenixPE, navigate to the **Source Config** menu.
3. Click **Extract Source ISO** and follow the on-screen instructions to extract the contents of the ISO you downloaded in Step 2.

Step 4: Configure the Source

1. In PhoenixPE, go to **Source Config -> Source Files**.
2. Select the directory containing your extracted ISO from Step 3.
3. Set the **'install.wim'** image to the Pro version. (Note: Windows S is not supported.)
4. Ensure the **'Run all programs from RAM (Boot.wim)'** option is checked.

Step 5: Enable Required Apps

1. For the purposes of a minimal build for Triage please select the following option:

Core
- Pre-Flight checks
- Core Files
- Core Registry
- Core Config
- Core WoW64

Shell
- PreShell
- Explorer Shell
- StartAllBack

Components
- Additional Files: Please see step 6 for more information
- DirectX
- Logon as Admin
- Windows PowerShell: Execution policy Bypass
- .NET: .NET Framework
- Visual C++ Runtime (all)

Tweaks
- Command Prompt
- Wallpaper: Please see additional tweaks for more information

Applications
- **Forensic tools**
  - WinFe Write Protect Tool: Additionally, tick '**Run From RAM**' option. (as of 26/05/25 script will fail, check Step 7 if failing to build at this stage)
- **System Tools**
  - PowerShell Core: Execution Policy Bypass, Run from Ram

Drivers
- Display Drivers

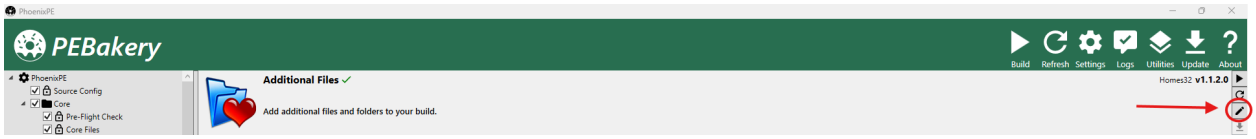
Finalize
- Bootmgr
- Post-Process
- Capture Wim

Media Creation
- Create ISO

Step 6: Add Missing DLLS

Note: This step will not work if msvfw32.dll is not present in your host machine's System32 directory. If it's missing, please download the msvfw32.dll file. You can modify the FileCopy path in version 7.6 to point to the location of msvfw32.dll on your machine.

1. Navigate to **Additional Files** in PhoenixPE.
2. In the top right hand corner, click the **Black Pencil Icon**



3. From the dropdown menu, select **Edit Script Source**.
4. Open the script in your preferred text editor.
5. Find the line that says:

```
[Process]
Echo,"Copying additional %SourceArch% files..."
```

6. Directly under this line, add the following script to move **msvfw32.dll** into the PE's **System32**:

```
If,%SourceArch%,Equal,x64,Begin
If,Not,%fb_WimFilesx64%,Equal,"",If,ExistDir,%fb_WimFilesx64%,FileCopy,
"%fb_WimFilesx64%*.",%TargetDir%
FileCopy,"C:\Windows\System32\msvfw32.dll","%TargetDir%\Windows\System3
2\msvfw32.dll"
If,Not,%fb_MediaFilesx64%,Equal,"",If,ExistDir,%fb_MediaFilesx64%,FileC
opy,"%fb_MediaFilesx64%*.",%OutputDir%
End
Else,Begin
If,Not,%fb_WimFilesx86%,Equal,"",If,ExistDir,%fb_WimFilesx86%,FileCopy,
"%fb_WimFilesx86%*.",%TargetDir%
FileCopy,"C:\Windows\System32\msvfw32.dll","%TargetDir%\Windows\System3
2\msvfw32.dll"
If,Not,%fb_MediaFilesx86%,Equal,"",If,ExistDir,%fb_MediaFilesx86%,FileC
opy,"%fb_MediaFilesx86%*.",%OutputDir%
End
```

It should look like this:

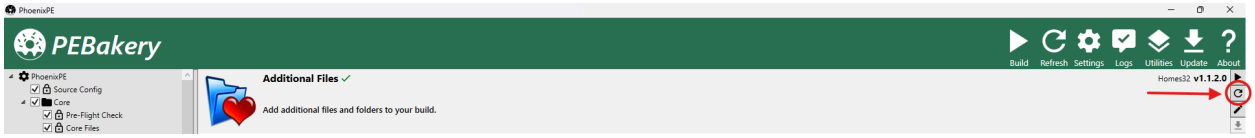
```
[Variables]

[Process]
Echo,"Copying additional %SourceArch% files..."

If,%SourceArch%,Equal,x64,Begin
  If,Not,%fb_WimFilesx64%,Equal,"",If,ExistDir,%fb_WimFilesx64%,FileCopy,"%fb_WimFilesx64%\*.*",%TargetDir%
  FileCopy,"C:\Windows\System32\msvfw32.dll","%TargetDir%\Windows\System32\msvfw32.dll"
  If,Not,%fb_MediaFilesx64%,Equal,"",If,ExistDir,%fb_MediaFilesx64%,FileCopy,"%fb_MediaFilesx64%\*.*",%OutputDir%
End
Else,Begin
  If,Not,%fb_WimFilesx86%,Equal,"",If,ExistDir,%fb_WimFilesx86%,FileCopy,"%fb_WimFilesx86%\*.*",%TargetDir%
  FileCopy,"C:\Windows\System32\msvfw32.dll","%TargetDir%\Windows\System32\msvfw32.dll"
  If,Not,%fb_MediaFilesx86%,Equal,"",If,ExistDir,%fb_MediaFilesx86%,FileCopy,"%fb_MediaFilesx86%\*.*",%OutputDir%
End

[#WimExplorex86#]
// ==========
```

7. Save and close your text editor.
8. Finally, click the **Black Refresh Arrow** (above the pencil icon from earlier) or press Ctrl + F5 to apply the changes.



Step 7: If WinFE is failing during build.

As of 26/05/25, the WinFE write protect tool is failing to build. To fix this you need to:

1. Install the protect tool manually from: https://www.winfe.net/files/IntelWinFE.7z
2. Find the provided WriteProtectTool.script.
3. Inside the script find the [UseLocalFile] section.
4. Replace:
   // Copy the manually downloaded file to the cache
   Echo,"Copying C:\Users\Getdata\Desktop\winpe\IntelWinFE.7z to %ProgramsCache%\%ProgramFolder%\%SetupFile%"
   FileCopy,"C:\Users\Getdata\Desktop\winpe\IntelWinFE.7z","%ProgramsCache%\%ProgramFolder%\%SetupFile%"
   With your download path IntelWinFE.7z path.
5. Inside PhoenixPe find the Forensic tool WinFE, navigate to the top left black pencil > Edit script source, and replace the whole thing with your new editing script.
6. Save, close, and refresh the script.

You should now be able to build WinFe.

Step 8: Customizing PE Configuration and Desktop Shortcuts

After successfully building the initial PE environment, customize the configuration to optimize for your specific use case:

Configuration Update:

1. Navigate to *PhoenixPE\Workbench\PhoenixPE\Target\Windows\System32*
2. Replace the existing *PhoenixPE.au3* file with your customized version
    - This configuration removes network components to streamline the environment
    - Adds desktop shortcuts for key forensic tools: Triage, Imager, and Memory utilities

Rebuild Process:

1. Return to the main PhoenixPE interface
2. Navigate to **Testing** → **VMware**
3. Select **Rebuild WIM + ISO** to generate the updated image

Note: Ensure you have a backup of the original *PhoenixPE.au3* file before replacement in case you need to revert changes.

Step 9: Building the PE

1. In the **Main Menu**, click the **Build** button (white arrow) to start the build process.
2. The build process will begin and may take between 2 to 10 minutes, depending on your system's performance.
3. Once the build is complete, the ISO file will be located in the **Output** directory within the PhoenixPE source folder.

Additional Tweaks

Modify Volume Name:

1. Navigate to **Media Creating** → **ISO**
2. From here you can tweak both volume name and File name of ISO directly

Adding Triage directly to the ISO

1. Navigate to the **Components** → **Additional Files** tab.

2. Within the '**Additional In Ram/Boot.wim Files**' section click on the black folder located next to the end of the **x64 Files** box.
3. Locate the FEX_Triage folder and press the 'Select Folder' button.

Change Wallpaper:

1. Navigate to **Tweaks** → **Wallpaper**
2. Under **Use Custom Desktop Wallpaper**, select your desired wallpaper

Section 2: Creating Bootable ISO and Installing Triage

Step 1: Create a Bootable USB with Rufus

1. Download and install **Rufus**.
2. Insert your USB drive into the computer.
3. Open Rufus and select your USB drive under the **Device** dropdown.
4. Under **Boot selection**, choose the Base ISO you created in Section 1.
5. Set the **Partition scheme** to **GPT**.
6. Set the **Target system** to **UEFI (non-CSM)**.
7. Rename the **Volume label** to TraigePE (if not no shortcuts will be made).
8. Keep the **File System** and **Cluster size** at their default settings.
9. Click **Start** to begin the process (this may take some time).
10. Once the process is complete, close Rufus.

Step 2: Move Triage into the Programs Folder

1. Insert the USB drive from Step 1 into your computer.
2. Locate the USB drive on your host machine (usually labeled as the volume name you set in Step 1).
3. Navigate to the **Programs** folder inside the volume.
4. Copy the **FEX_Triage, FEX_Memory, FEX_Traige** program into the **Programs** folder.
5. Safely eject the USB drive.