WinFE

(home)

Build

Stage 1 (Intel)

The computer that you intend to conduct the build on should be Windows 10 Pro x64, with a build version of at least 1803. You will also need permissions to 'Run as Administrator'.

Download and install 7-Zip file archiver (https://www.7-zip.org/ (https://www.7-zip.org/)).

Obtain the Intel x86/x64 framework package from the Download (download) page

Copy the framework package to the root of a volume (e.g. F:\), then right-click the package and allow 7-Zip to 'Extract Here', this will mitigate the potential issue of having a double nested folder (e.g. F:\WinFE\WinFE) which happens when extracting from archive files.

Volume letter F:\ is going to be assumed for this guide, change accordingly to your own volume letter.

If you wish to customise the desktop background of WinFE, use this opportunity to copy your organisation's logo, which must be named 'wallpaper.jpg', to the following locations - 'F:\IntelWinFE\x86' and 'F:\IntelWinFE\x64'.

Stage 2 (Intel)

Visiit https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install (https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install) and download the installer stub file for Windows 10 ADK, version 1803. (Direct link: https://go.microsoft.com/fwlink/?linkid=873065 (https://go.microsoft.com/fwlink/?linkid=873065)).

It may work with other Windows 10 versions of the ADK, however, the testing was conducted using 1803, using any other version may produce unexpected results.

Install Windows 10 ADK, version 1803 by accepting all default options, and default installation path. (This may take some time depending on your internet speed, it also requires several Gigabytes of disk space).

Stage 3 (Intel)

Download and install FTK Imager 3.4.0.1 (This is 32-bit) from AccessData (https://accessdata.com/product-download#past-versions (https://accessdata.com/product-download#past-versions)).

Install FTK Imager to the default location, If you already have FTK Imager installed, you will need to uninstall before proceeding.

Navigate to 'C:\Program Files(x86)\AccessData\' and 'Copy' the entire 'FTK Imager' folder. You should now navigate to the location where you extracted the x86/x64 Framework.

Paste the previously copied 'FTK Imager' folder into 'F:\IntelWinFE\USB\x86-x64\tools\x86'. Remember this must be the 32-bit version of FTK Imager.

When copied, use 'Control Panel' to uninstall this 32-bit version of 'FTK Imager'.

Download and install FTK Imager 4.2.0 (This is 64-bit) from AccessData (https://accessdata.com/product-download#past-versions (https://accessdata.com/product-download#past-versions)).

Install FTK Imager to the default location, If you already have FTK Imager installed, you will need to uninstall before proceeding.

Navigate to 'C:\Program Files\AccessData\' and 'Copy' the entire 'FTK Imager' folder. You should now navigate to the location where you extracted the x86/x64 Framework.

Paste the previously copied 'FTK Imager' folder into 'F:\IntelWinFE\USB\x86-x64\tools\x64'. Remember this must be the 64-bit version of FTK Imager.

When copied, use 'Control Panel' to uninstall this 64-bit version of 'FTK Imager'.

Stage 4 (Intel)

From the 'Search Bar' next to the 'Start Menu' button, type cmd.exe, and open with administrative permissions.

From the console, type 'F:' (or whatever your volume letter is) and press enter, then use the CD command to navigate into the 'IntelWinFE' folder.

You can now build the WinFE platform by typing 'MakeWinFEx64-x86.bat' and press enter.

The build process will automatically extract the required files from the ADK installation and create the structure required to produce bootable WinFE media.

This process may take several minutes.

Leave the cmd.exe window open if you wish to produce a CD/DVD ISO file.

Stage 5 (Intel)

This step is optional, unless you wish to produce a WinFE CD/DVD bootable ISO file.

Providing that you left the cmd.exe window open from the previous stage, you can simply build a bootable WinFE ISO file by typing 'Makex64-x86-CD.bat' and press enter.

The bootable WinFE ISO file will automatically be created within the ISO folder.

Stage 6 (Intel)

This step is optional, unless you wish to produce a bootable USB Flash Drive (UFD).

The UFD should not be greater than 32 Gigabytes (This is a FAT32 size limitation imposed by Microsoft).

Firstly, open an elevated Command Line Interface shell, and type diskpart, then press enter.

You will now see a Diskpart prompt, as below:

```
DISKPART>
```

```
Type: List Disk <Enter>
```

```
Type: Select Disk X (X being your USB Flash Drive) <Enter>
```

```
Type: Clean <Enter>
```

```
Type: Create Partition Primary <Enter>
```

```
Type: Format FS=FAT32 Quick <Enter>
```

```
Type: Active <Enter>
```

```
Type: Assign <Enter>
```

```
Type: Exit <Enter>
```

Leave the Command Line Interface open as you will need this again shortly.

Navigate to 'F:\IntelWinFE\USB\x86-x64\'.

There should be a bunch of files and folders within this location (boot, efi, sources ....).

Copy all of these files and folders to the root of your newly prepared UFD.

Return to the Command Line Interface, and type the following, making sure you do not include the trailing '\' as part of the USB Flash Drive Letter:

```
bootsect.exe /nt60 <USB flash drive letter>: /force /mbr
```

Safely eject the USB Flash Drive, it is now ready to use.

Stage 7 (Intel)

This step is optional, unless you wish to produce a bootable USB Hard Disk Drive.

Firstly, open an elevated Command Line Interface shell, and type diskpart, then press enter.

You will now see a Diskpart prompt, as below:

```
DISKPART>
```

```
Type: List Disk <Enter>
```

```
Type: Select Disk X (X being your USB Hard Disk Drive) <Enter>
```

```
Type: Clean <Enter>
```

```
Type: Create Partition Primary Size = 8000 <Enter>
```

```
Type: Format FS=FAT32 Quick <Enter>
```

```
Type: Active <Enter>
```

```
Type: Assign <Enter>
```

```
Type: Create Partition Primary <Enter>
```

```
Type: Format FS=NTFS Quick <Enter>
```

```
Type: Assign <Enter>
```

```
Type: Exit <Enter>
```

```
Type: Exit <Enter>
```

Leave the Command Line Interface open as you will need this again shortly.

Navigate to 'F:\IntelWinFE\USB\x86-x64\'.

There should be a bunch of files and folders within this location (boot, efi, sources ....).

Copy all of these files and folders to the root of your newly prepared FAT32 volume.

Return to the Command Line Interface, and type the following, making sure you do not include the trailing '\' as part of the Hard Disk Drive Letter:

```
bootsect.exe /nt60 <FAT32 volume letter>: /force /mbr
```

Safely eject the Hard Disk Drive, it is now ready to use.

This method will allow you to conduct your forensic acquisition to the same device as WinFE (different partition).