

WinFE



IMF 2009

5th International Conference on IT Security Incident Management & IT Forensics

September 15th to 17th, 2009
Stuttgart, Germany

<http://www.imf-conference.org/>
<mailto:2009@imf-conference.org>

Conference of SIG SIDAR
of the German Informatics Society (GI).



In Cooperation with



SIDAR



Technically Co-Sponsored by



Organisation Support



WinFE

- forensic environment based on Windows
 - + availability of system drivers
- starting from Windows 2008 / Vista SP1
- AIK is sufficient to build a WinFE CD
- Make sure you have a valid license from Microsoft to use your Boot-CD!!!
 - <http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08>
 - paper „Troja“ / Troy Larson „How to Build Windows FE (Forensic Environment) with the Windows Preinstallation Environment 2.1“
 - <http://www.twine.com/item/113421dk0-g99/windows-fe>

Automated Installation Kit (AIK) für
Windows Vista SP1 und Windows
Server 2008

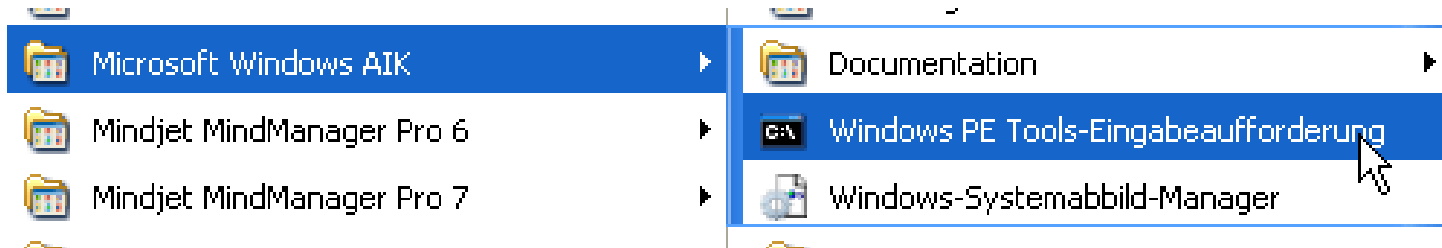


Kurzbeschreibung

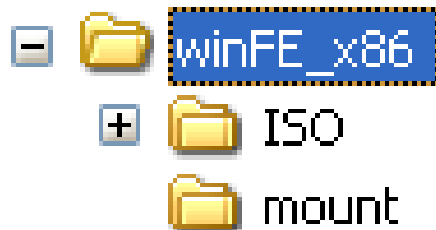
Das Windows Automated Installation Kit (Windows AIK) wurde entwickelt, um IT-Spezialisten in Unternehmen bei der Anpassung und Bereitstellung der Betriebssystemfamilien Windows Vista und Windows Server 2008 zu unterstützen.

WinFE

- install AIK
- open AIK command line



- `copyype.cmd <architecture> <target>`
 - `copyype.cmd x86 G:\winFE_x86 [amd64|ia64]`



WinFE

- AIK uses a .wim File to boot
- for configuration this has to be mounted:
 - `imagex /mountrw G:\winFE_x86\winpe.wim 1 G:\winFE_x86\mount`

```
G:\winFE_x86>c:imagex /mountrw G:\winFE_x86\winpe.wim 1 G:\winFE_x86\mount
ImageX Tool for Windows
Copyright (C) Microsoft Corp. All rights reserved.

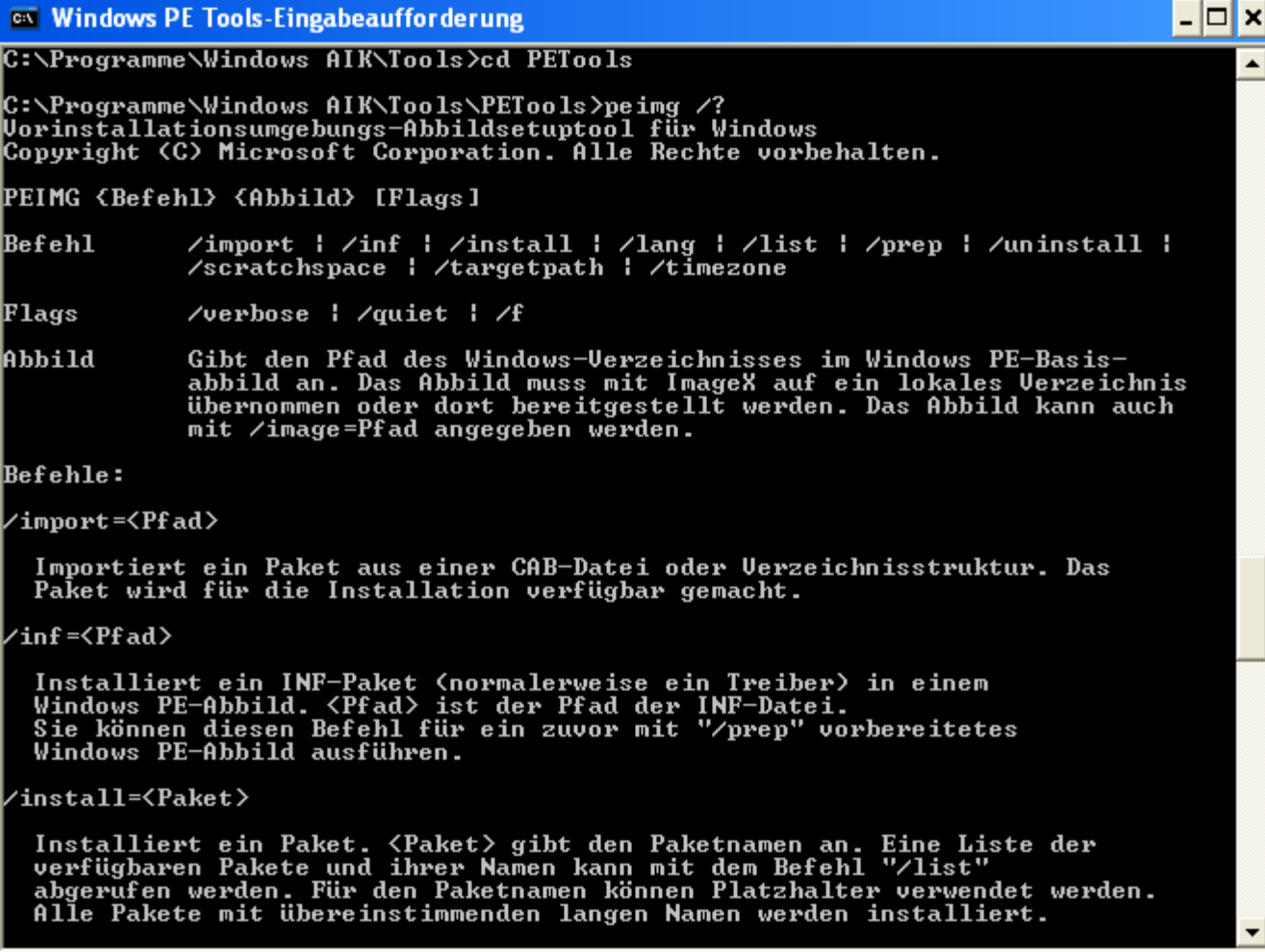
Mounting (RW): [G:\winFE_x86\winpe.wim, 1] ->
                [G:\winFE_x86\mount]

Successfully mounted image (RW).
```

- (check the path if you can't access the tools - ..\x86 should be included)

WinFE

- install drivers



```
C:\Programme\Windows AIK\Tools>cd PETools

C:\Programme\Windows AIK\Tools\PETools>peimg /?
Vorinstallationsumgebungs-Abbildsetuptool für Windows
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

PEIMG <Befehl> <Abbild> [Flags]

Befehl      /import ! /inf ! /install ! /lang ! /list ! /prep ! /uninstall !
            /scratchspace ! /targetpath ! /timezone

Flags       /verbose ! /quiet ! /f

Abbild      Gibt den Pfad des Windows-Verzeichnisses im Windows PE-Basis-
            abbild an. Das Abbild muss mit ImageX auf ein lokales Verzeichnis
            übernommen oder dort bereitgestellt werden. Das Abbild kann auch
            mit /image=Pfad angegeben werden.

Befehle:

/import=<Pfad>

    Importiert ein Paket aus einer CAB-Datei oder Verzeichnisstruktur. Das
    Paket wird für die Installation verfügbar gemacht.

/inf=<Pfad>

    Installiert ein INF-Paket (normalerweise ein Treiber) in einem
    Windows PE-Abbild. <Pfad> ist der Pfad der INF-Datei.
    Sie können diesen Befehl für ein zuvor mit "/prep" vorbereitetes
    Windows PE-Abbild ausführen.

/install=<Paket>

    Installiert ein Paket. <Paket> gibt den Paketnamen an. Eine Liste der
    verfügbaren Pakete und ihrer Namen kann mit dem Befehl "/list"
    abgerufen werden. Für den Paketnamen können Platzhalter verwendet werden.
    Alle Pakete mit übereinstimmenden langen Namen werden installiert.
```

- peimg.exe /inf=<path to .inf> G:\winFE_x86\mount\Windows

WinFE

- Where to get drivers? -> vendor, or:



MorgensternHolger Einstellungen Abmelden

DriverPacks

ForensicBlog » ForensicIndex » SeiteFinden » WinPE/Anleitung » DriverPacks

AktuelleÄnderungen SeiteFinden HilfeInhalt ForensicIndex HandyIndex **DriverPacks**

Editieren (Text) Editieren (GUI) Info Abonnieren Verweis hinzufügen Dateianhänge Weitere Aktionen: ▾

Treiber für Windows-Systeme

- <http://driverpacks.net/DriverPacks/>

What DriverPacks are currently available?

Currently there are **10 DriverPacks** available, all for the wnt5_x86-32 OS platform:

- DriverPack Chipset
- DriverPack CPU
- DriverPack Graphics A
- DriverPack Graphics B
- DriverPack Graphics C
- DriverPack LAN
- DriverPack MassStorage
- DriverPack Sound A
- DriverPack Sound B
- DriverPack WLAN

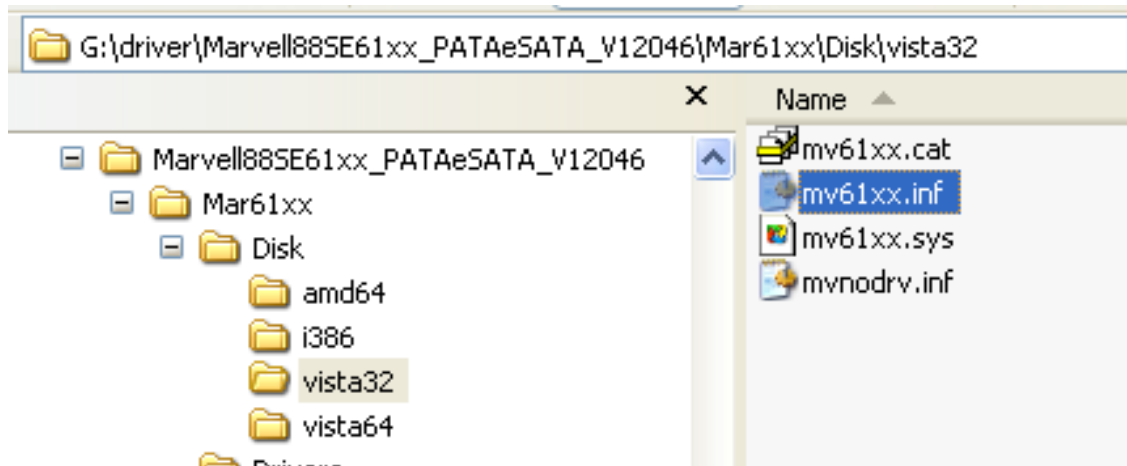
Or go to the **overview** page, if you prefer that. And of course there's an **UpdateTracker** for the DriverPacks as well!

and to slipstream them, you will also need:

- **DriverPacks BASE**

WinFE

- just unpack and include .inf



- Peimg.exe
/inf=G:\driver\Marvell88SE61xx_PATAeSATA_V12046\Mar61xx\Disk\vista32\mv61xx.inf
G:\winFE_x86\mount\Windows

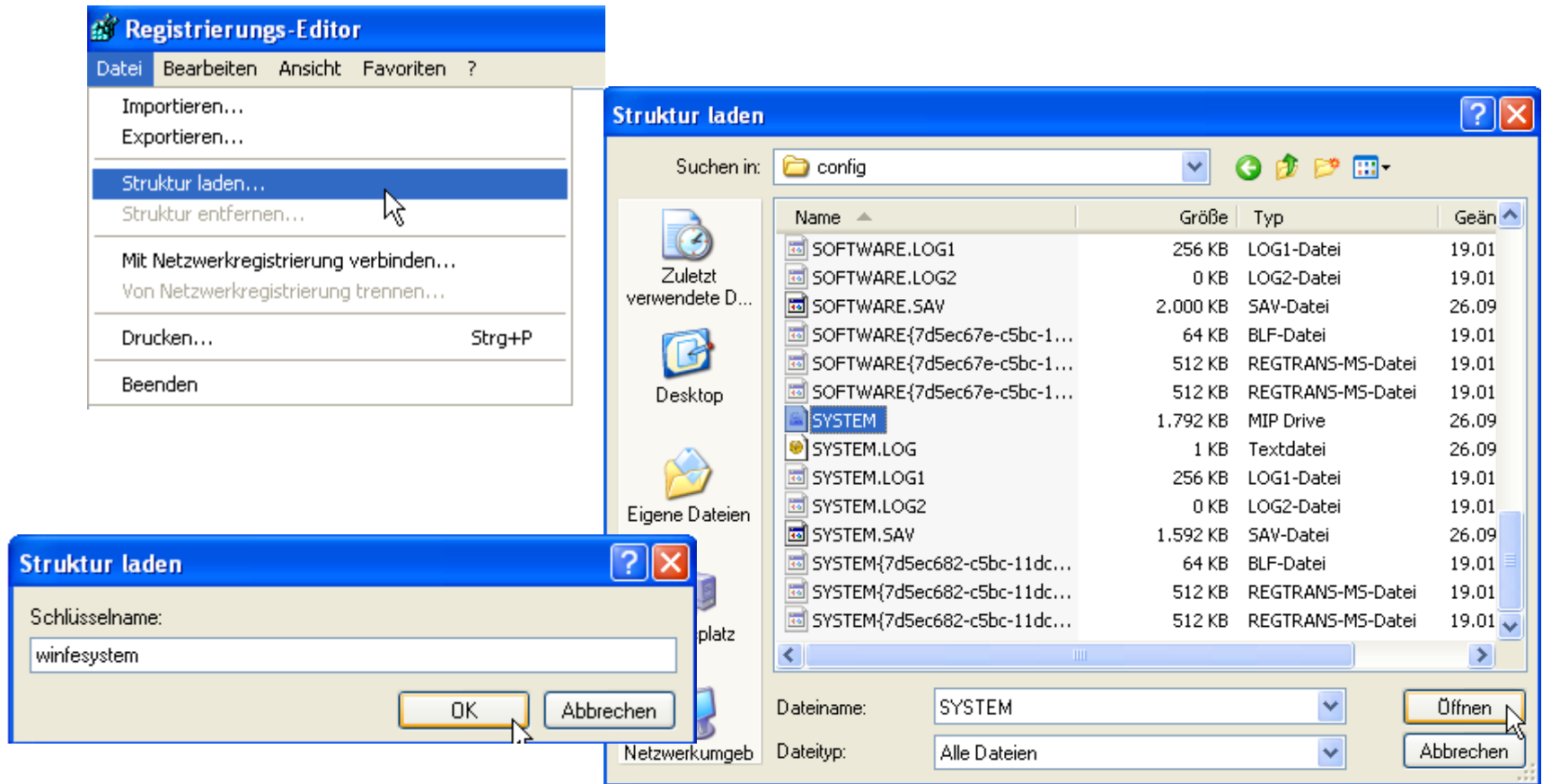
```
G:\winFE_x86>c:Peimg.exe /inf=G:\driver\Marvell88SE61xx_PATAeSATA_U12046\Mar61xx
\Disk\vista32\mv61xx.inf G:\winFE_x86\mount\Windows
Vorinstallationsumgebungs-Abbildsetuptool für Windows
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

INF-Paket wird installiert: G:\driver\Marvell88SE61xx_PATAeSATA_U12046\Mar61xx\D
isk\vista32\mv61xx.inf

PEIMG hat den Vorgang erfolgreich abgeschlossen.
```

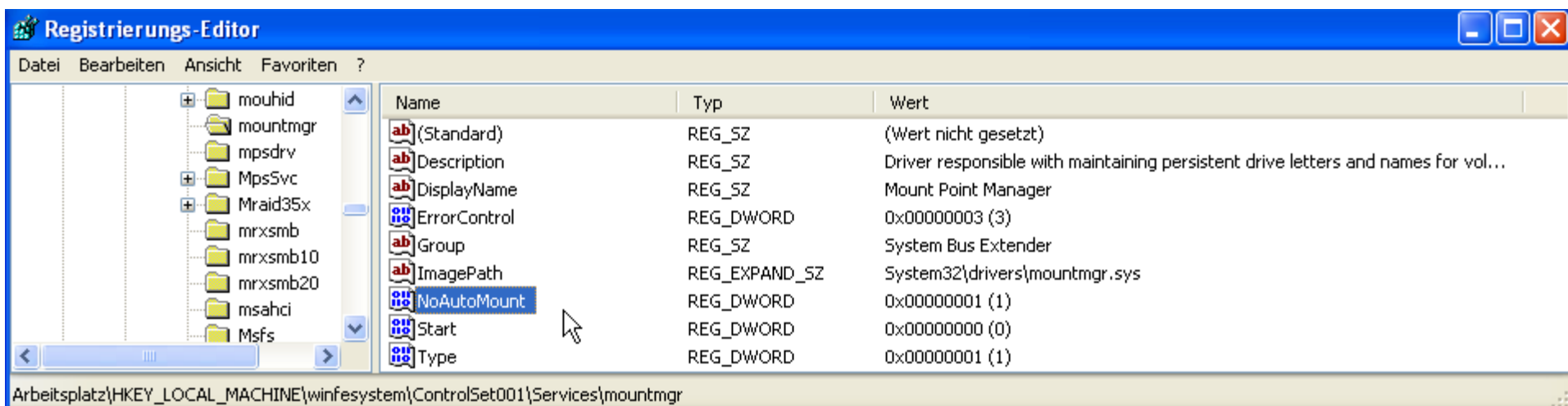
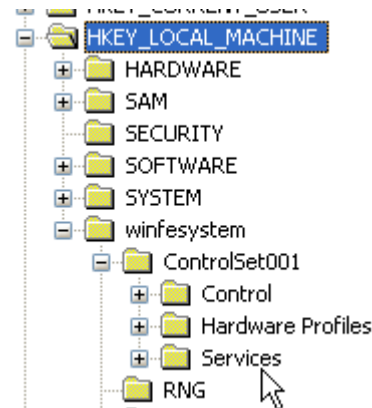
WinFE

- Two registry keys to make PE into FE:



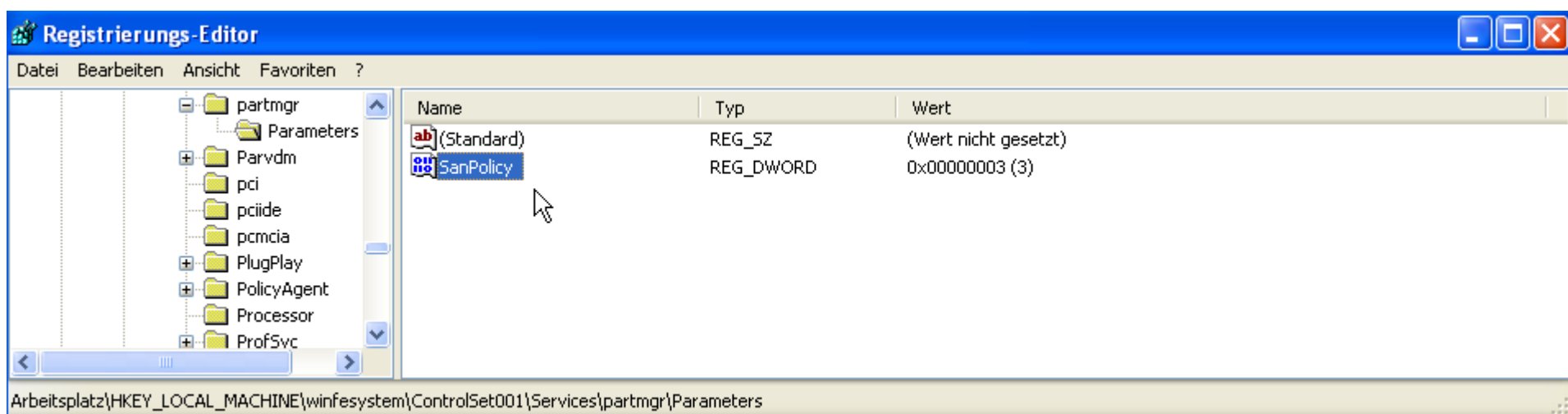
WinFE

- **HKEY_LOCAL_MACHINE\winfesystem\ControlSet001\Services\MountMgr\NoAutoMount = 1**



WinFE

- **HKEY_LOCAL_MACHINE\winfesystem\ControlSet001\Services\partmgr\Parameters**
- **SanPolicy = 3**



WinFE

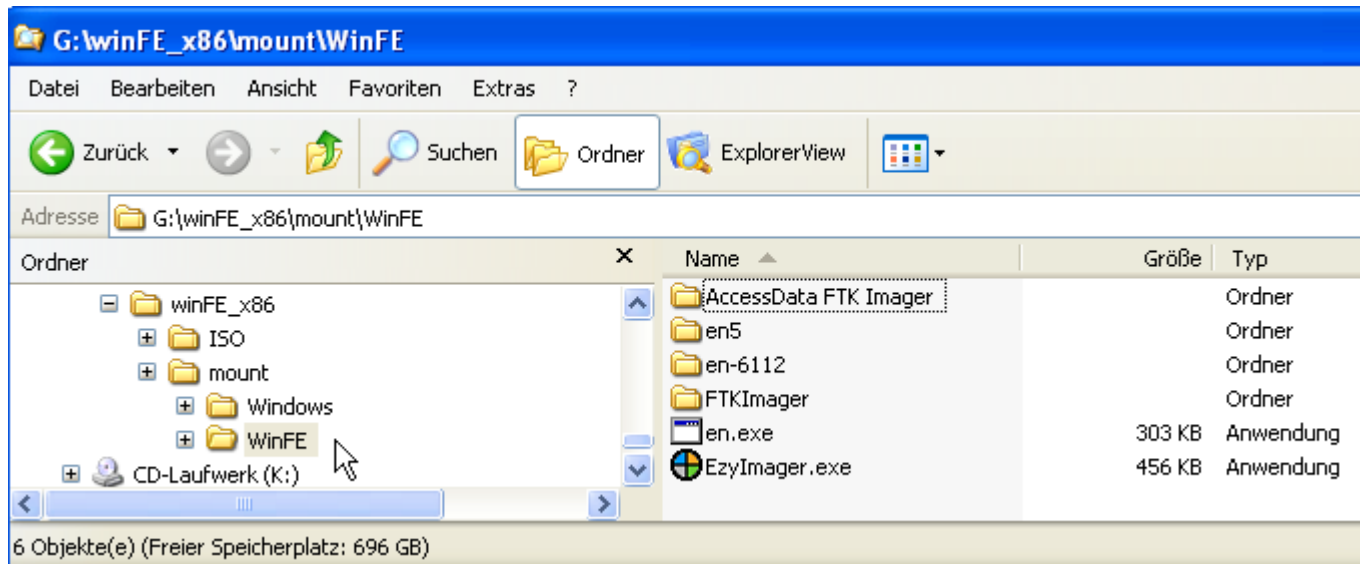
- **remove registry structure winfesystem:**



- **updates are written to the mounted .wim file**

WinFE

- Add your own forensic tools directory to the .wim...

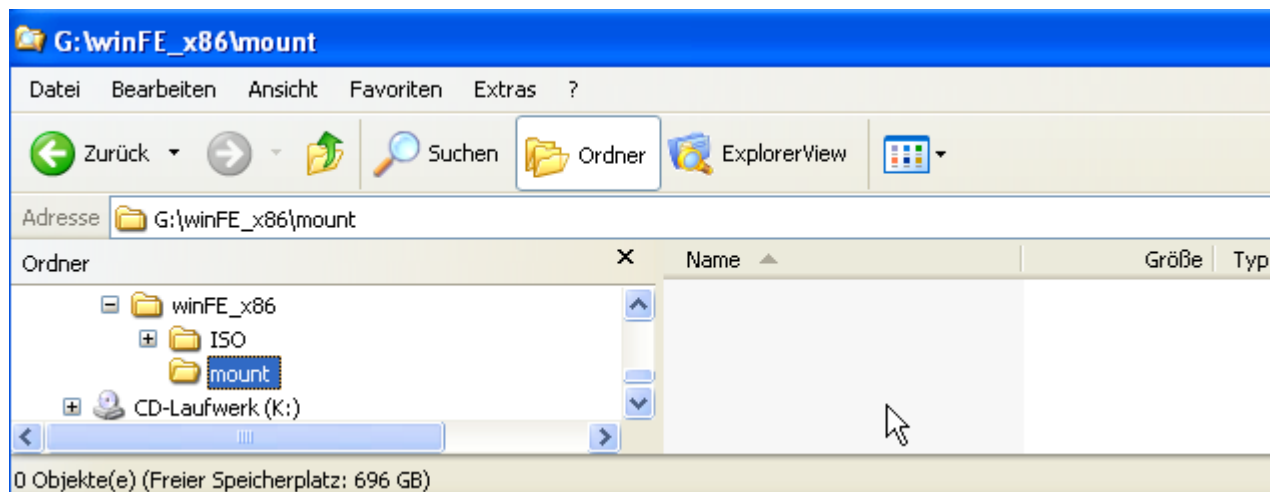


WinFE

- **Commit all updates!!**
- **imagex.exe /unmount /commit G:\winFE_x86\mount**

```
G:\winFE_x86>c:..\x86\imagex.exe /unmount /commit G:\winFE_x86\mount  
  
ImageX Tool for Windows  
Copyright (C) Microsoft Corp. All rights reserved.  
  
Unmounting: [G:\winFE_x86\mount]...  
Successfully unmounted image.
```

- **The mount directory should be empty after that ;-)**



WinFE

- delete boot.wim in
G:\winFE_x86\ISO\sources
- copy winpe.wim to
G:\winFE_x86\ISO\sources and rename
it to **boot.wim**

The top screenshot shows a Windows Explorer window with the address bar set to 'G:\winFE_x86\ISO\sources'. The left pane shows the folder structure: winFE_x86 > ISO > sources. The right pane shows a single file named 'boot.wim' with a size of 281.322 KB, type 'WIM-Datei', and a date of 26.09.2008 19:07.

The bottom screenshot shows a Windows Explorer window with the address bar set to 'G:\winFE_x86\ISO\sources'. The left pane shows the folder structure: Recycled > System Volume Information > winFE_x86 > ISO > sources. The right pane shows three files: 'WinFE_x86.iso' (308.742 KB, ISO Image, 26.09.2008 19:11), 'winpe.wim' (282.645 KB, WIM-Datei, 18.02.2009 19:32), and 'winpe_Microsoft Windows Vist...' (101 KB, CLG-Datei, 26.09.2008 17:24). A mouse cursor is hovering over the 'winpe.wim' file.

WinFE

- build an ISO image out of that
- `oscdimg -n -m -o -bG:\winFE_x86\etfsboot.com G:\winFE_x86\ISO G:\winFE_x86\WinFE_x86.iso`

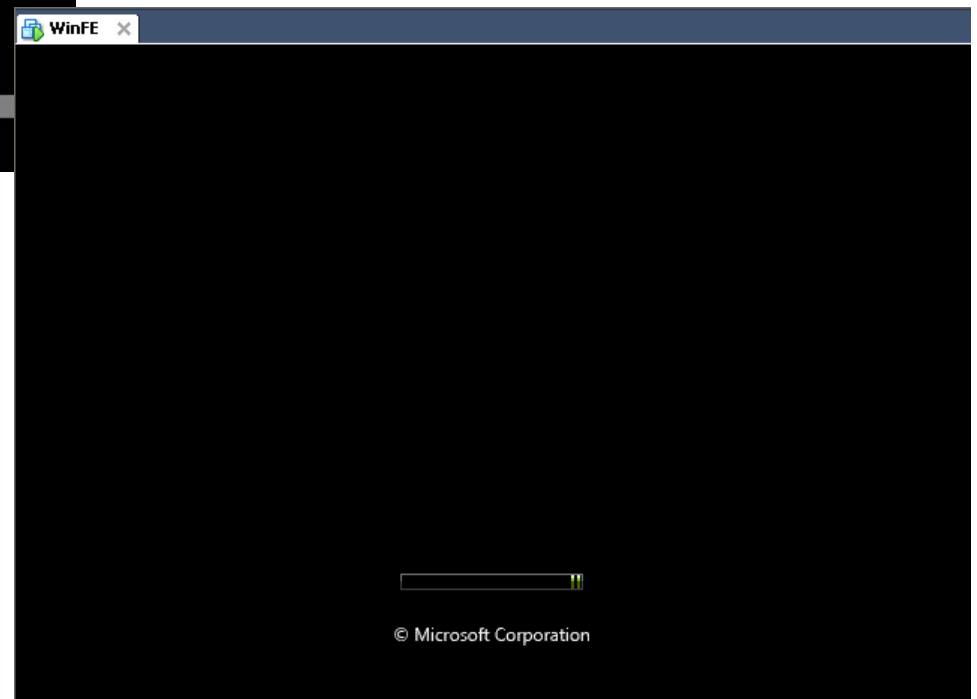
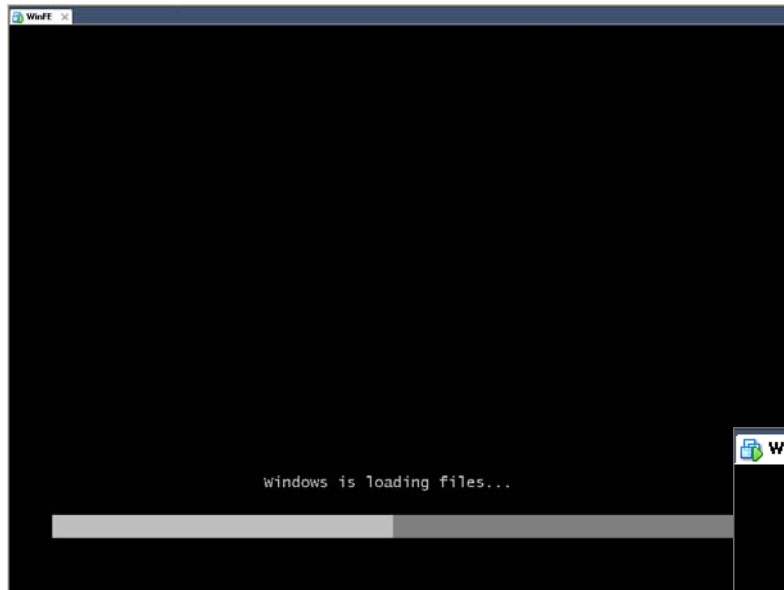
```
G:\winFE_x86>c:..\x86\oscdimg /?
OSCDIMG 2.54 CD-ROM and DVD-ROM Premastering Utility
Copyright (C) Microsoft, 1993-2007. All rights reserved.
Licensed only for producing Microsoft authorized content.

Usage: OSCDIMG [options] sourceroot targetfile

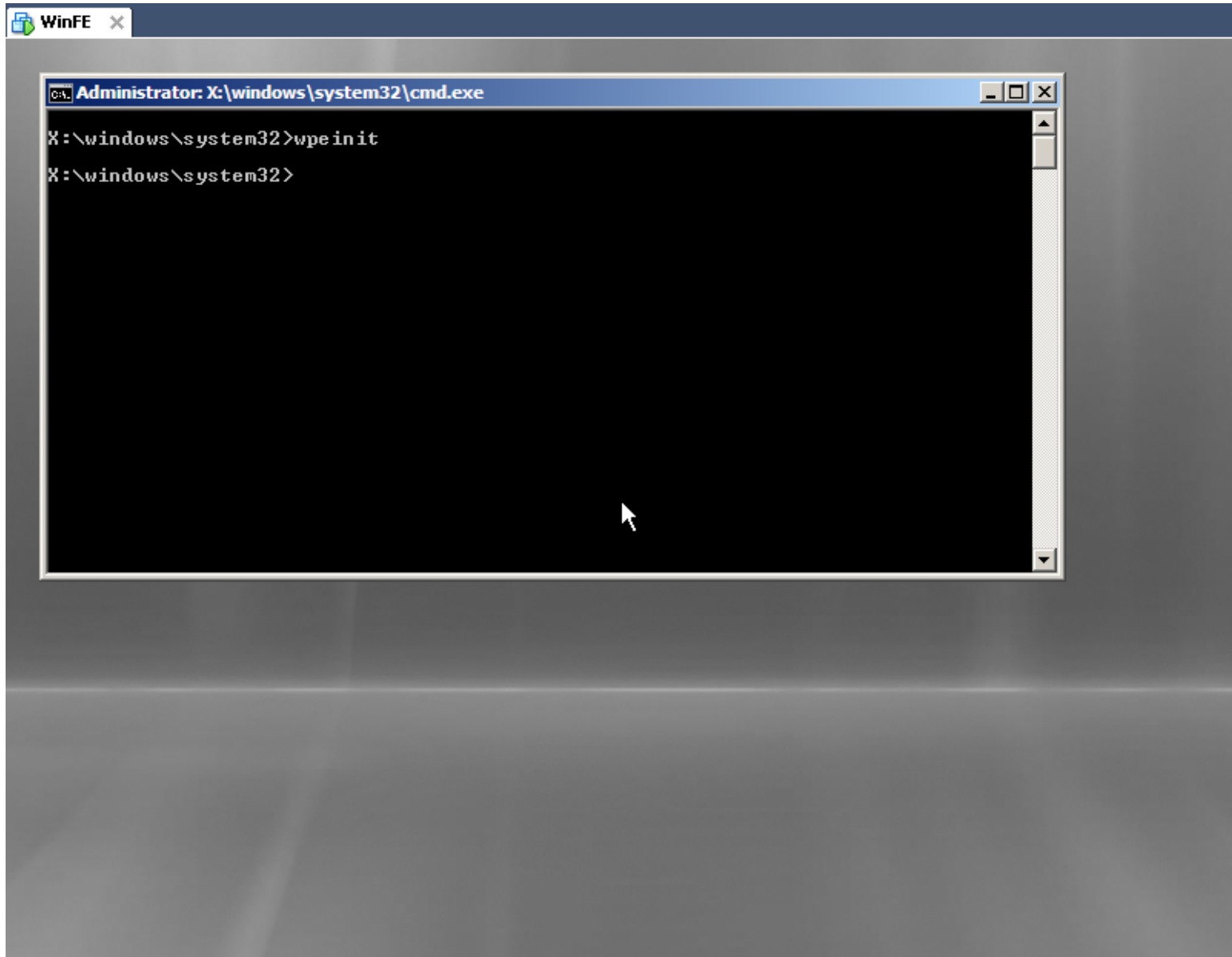
For option information, use -help with one of the following categories
  ISO          Options for the ISO 9660 file system
  Joliet       Options for the Joliet file system
  UDF          Options for the UDF file system
  Boot        Options for bootable CDs
  Optimize    Options for optimization
  Order       Options for ordering the files
  DVD         Options for DVD video and audio
  Mesg        Options for displaying warnings and messages
  Other       Options that do not fit in any other category
```

- finally burn your WinFE CD...

WinFE



WinFE



WinFE

The screenshot displays the WinFE application window, which is part of the EnCase Acquisition suite. The main window is titled "Choose Devices" and features a tree view on the left under "Local Drives" and a table of available devices on the right.

	Name	Label	Access	Sectors	Size	Write Blocked	Read File System
<input type="checkbox"/>	1 A	NO NAME	Windows	2.880	1,4MB		•
<input type="checkbox"/>	2 D	NECVMWarV	ASPI	154.371	301,5MB		•
<input type="checkbox"/>	3 X	NTFS	Windows	6.173	3MB		•
<input type="checkbox"/>	4 0	VMware, VM	ASPI	33.554.432	16GB		•

Below the main window, a command prompt window is open, showing the execution of the 'dir' command in the WinFE directory. The output lists files and folders with their timestamps, sizes, and types.

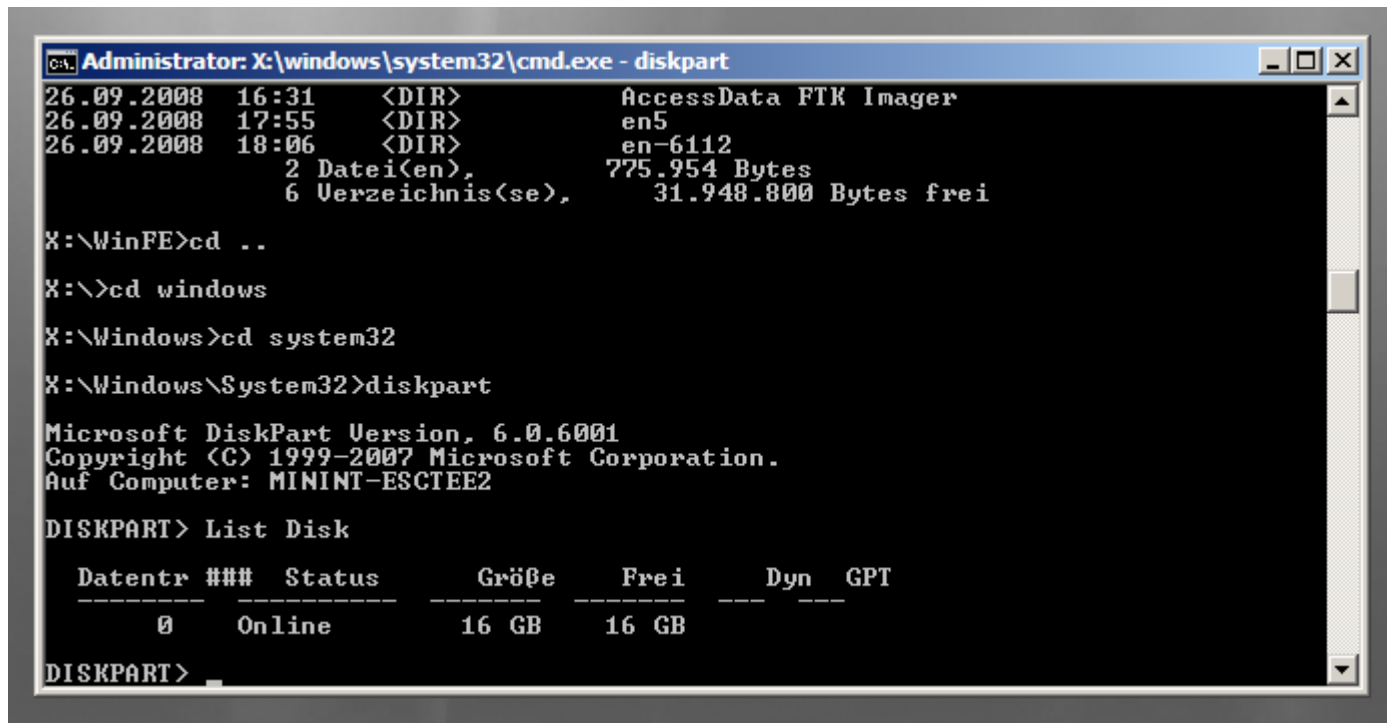
```
Administrator: X:\windows\system32\cmd.exe
X:\WinFE>dir
Datenträger in Laufwerk X: ist Boot
Volumeseriennummer: D60A-0DC2

Verzeichnis von X:\WinFE

26.09.2008  13:30    <DIR>          .
26.09.2008  13:30    <DIR>          ..
14.03.2007  16:10           309.914 en.exe
26.09.2008  16:17           466.040 EzyImager.exe
26.09.2008  13:33    <DIR>          FTKImager
26.09.2008  16:31    <DIR>          AccessData FTK Imager
26.09.2008  17:55    <DIR>          en5
26.09.2008  18:06    <DIR>          en-6112
                2 Datei(en),       775.954 Bytes
                6 Verzeichnis(se),  31.948.800 Bytes frei

X:\WinFE>
```

WinFE



```
Administrator: X:\windows\system32\cmd.exe - diskpart
26.09.2008 16:31 <DIR> AccessData FTK Imager
26.09.2008 17:55 <DIR> en5
26.09.2008 18:06 <DIR> en-6112
                2 Datei(en), 775.954 Bytes
                6 Verzeichnis(se), 31.948.800 Bytes frei

X:\WinFE>cd ..
X:\>cd windows
X:\Windows>cd system32
X:\Windows\System32>diskpart

Microsoft DiskPart Version 6.0.6001
Copyright (C) 1999-2007 Microsoft Corporation.
Auf Computer: MININT-ESCTEE2

DISKPART> List Disk

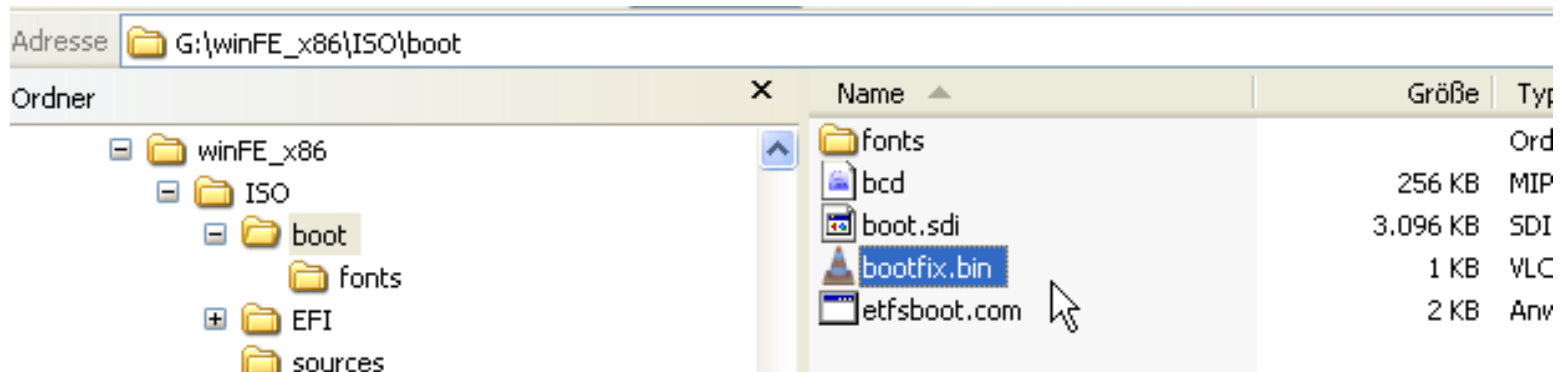
  Datentr   ###  Status      Größe   Frei     Dyn  GPT
  -----
           0   Online     16 GB   16 GB
DISKPART>
```

WinFE

- **use diskpart to manage your drives**
- **some useful commands:**
 - **LIST DISK | VOLUME**
 - **Rescan**
 - **Select Disk | VOLUME #**
 - **Attributes disk | volume clear readonly**
 - **Assign letter=?**

WinFE

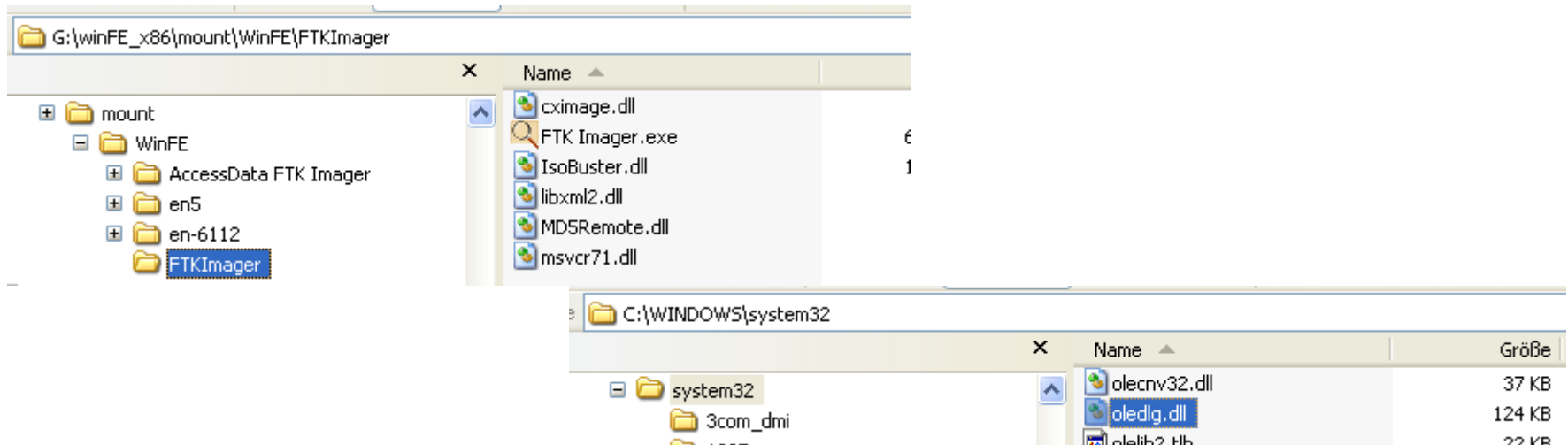
- „Press any key to boot from CD / DVD “
 - Be really fast ;-)) or better, also in case of power failures:
 - remove „bootfix.bin“ in the \ISO\boot directory before creating the ISO image



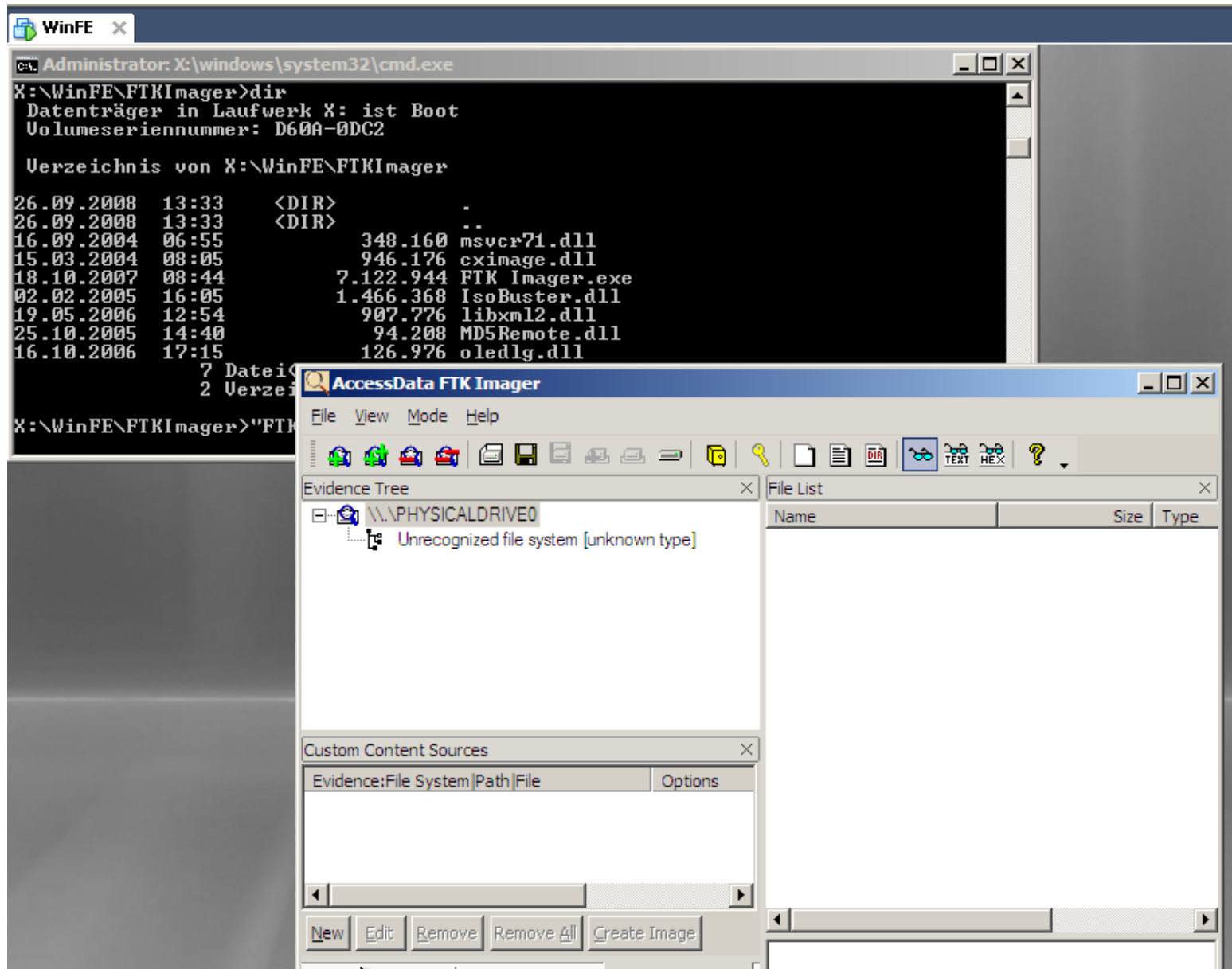
WinFE

- **FTK Imager**

- **Should be running without any installation, but the missed to mention that**
- **you have to copy „oledlg.dll“ from your C:\Windows\system32 to the FTK directory :-)**



WinFE



WinFE

- **Encase**
 - **Should work, but internal path settings are a problem**
 - **Workaround:**
 - **Create a drive X on your local machine and install a new Encase onto it**
 - **Copy the Encase directory then from drive X: to your mounted .wim – since WinFe mounts your tool folder to a ram drive X, Encase should be happy with it...**

WinFE

Let me stress again, this should be “Plan B”, just in case... the real project is clearly grml forensics, which is following now in the second part!



Von der Industrie- u. Handelskammer Bodensee-Oberschwaben
öffentlich bestellter und vereidigter Sachverständiger für Technik,
Systeme und Anwendungen der Informationsverarbeitung sowie
Computerforensik

Holger Morgenstern
Diplom-Informatiker

Breslauer Straße 24
72501 Gammertingen
morgenstern@gutachten.info

Tel. 07574/914-01
Fax 07574/914-03
www.gutachten.info