xmount – on-the-fly image conversion and a bit more

Eine Einführung in die Benutzung von xmount / OpenGates zu forensischen Zwecken.

Police Judiciaire Luxembourg - Section NT
Gillen Daniel <Daniel.GILLEN@police.etat.lu>

Übersicht

- Probleme bei der forensischen Analyse von Festplatenabbildern und der forensischen Post-Mortem-Analyse von PCs
- xmount / OpenGates
- Live Demos
- Abschließende Zusammenfassung

Probleme bei der forensischen Analyse von Festplattenabbildern

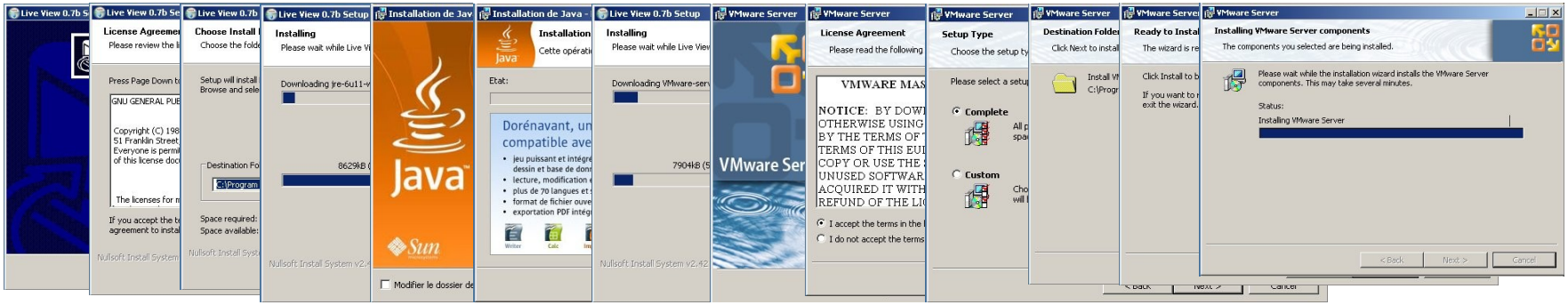
- Viele verschiedene zueinander inkompatible Formate (DD, EWF (Encase), AFF (Sleuthkit))
- Viele verschiedene Analysetools die nicht alle Formate unterstützen (z.B. mount → kein EWF, photorec → kein AFF, ...)

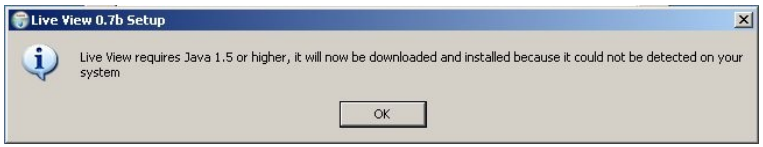
Probleme bei der forensischen Post-Mortem-Analyse von PCs

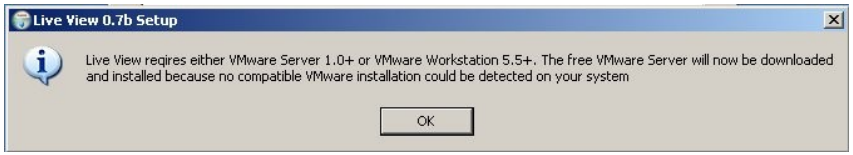
- Starten des PCs oft nützlich (z.B. zum Virusscan mittels Knoppicillin etc...)
- Starten des PCs oft notwendig (z.B. Bei der Analyse von proprietärer Software wie Buchhaltungsprogrammen oder dem Verhalten von Malware)
- Festplatteninhalt darf aber nicht verändert werden
- Originale Hardware evtl nicht vorhanden oder defekt

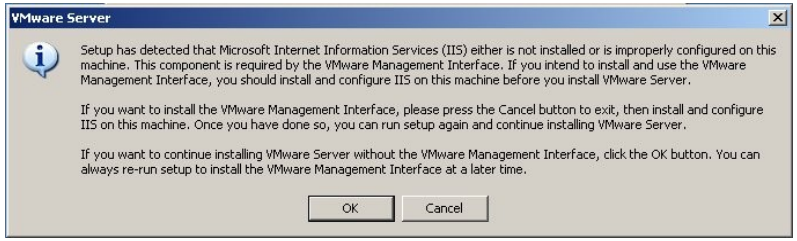
LiveView

- Unübersichtliche Installation (Download und Installation von zusätzlicher proprietärer Software während der Installation)





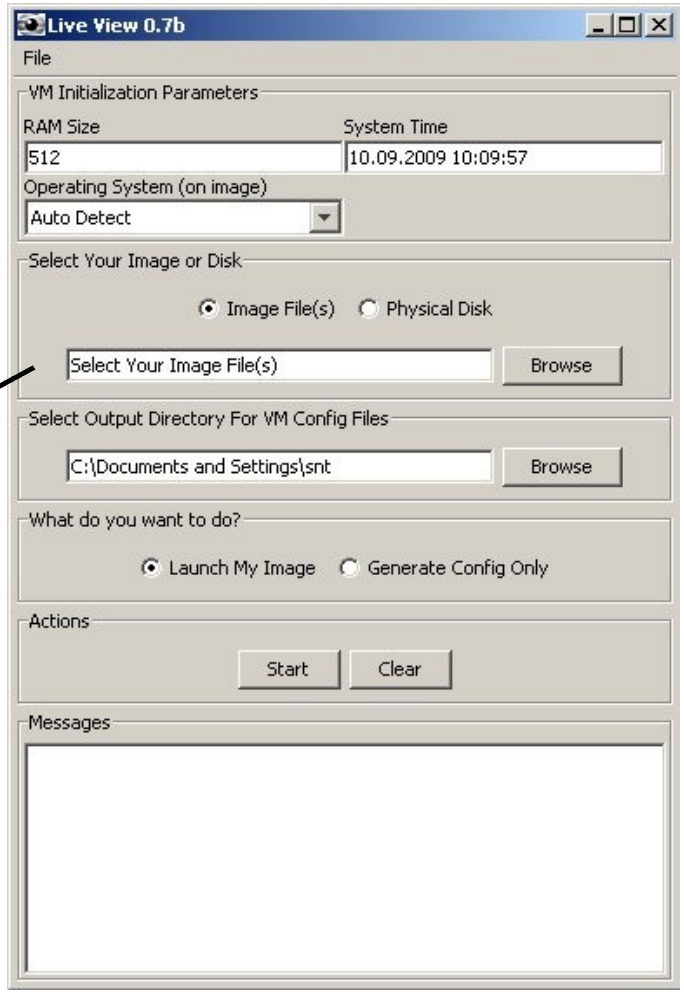




LiveView (Fortsetzung)

- Voller Funktionsumfang nur unter Windows
- Unterstützt nur VMWare
- “Vertraut” dem Schreibschutz von VMWare

- Als Quellformat werden ohne zusätzliche (kostenpflichtige) Tools nur DD Festplattenabbilder unterstützt.



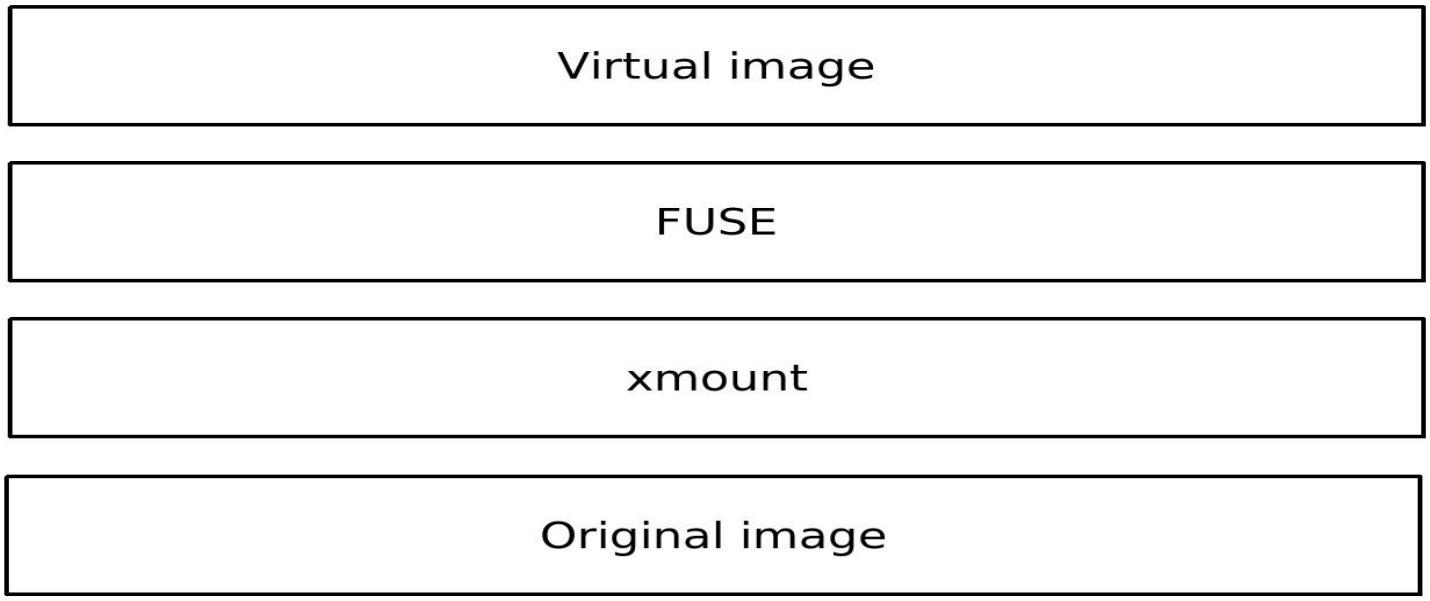
Was kann xmount

- On-the-fly Konvertierung zwischen verschiedenen Formaten.
    - Quellformat: DD, EWF und AFF
    - Zielformat: DD, VDI (VirtualBox) und VMDK (VMWare)
- Virtueller Schreibzugriff auf die geschützten Festplattenabbilder (Alle Änderungen werden in eine Cache-Datei geschrieben)

- xmount --in ewf --out dd ./ddisk.EE?? ./mnt
- xmount --in ewf --out vdi --cache ./disk.cache ./disk.E?? ./mnt

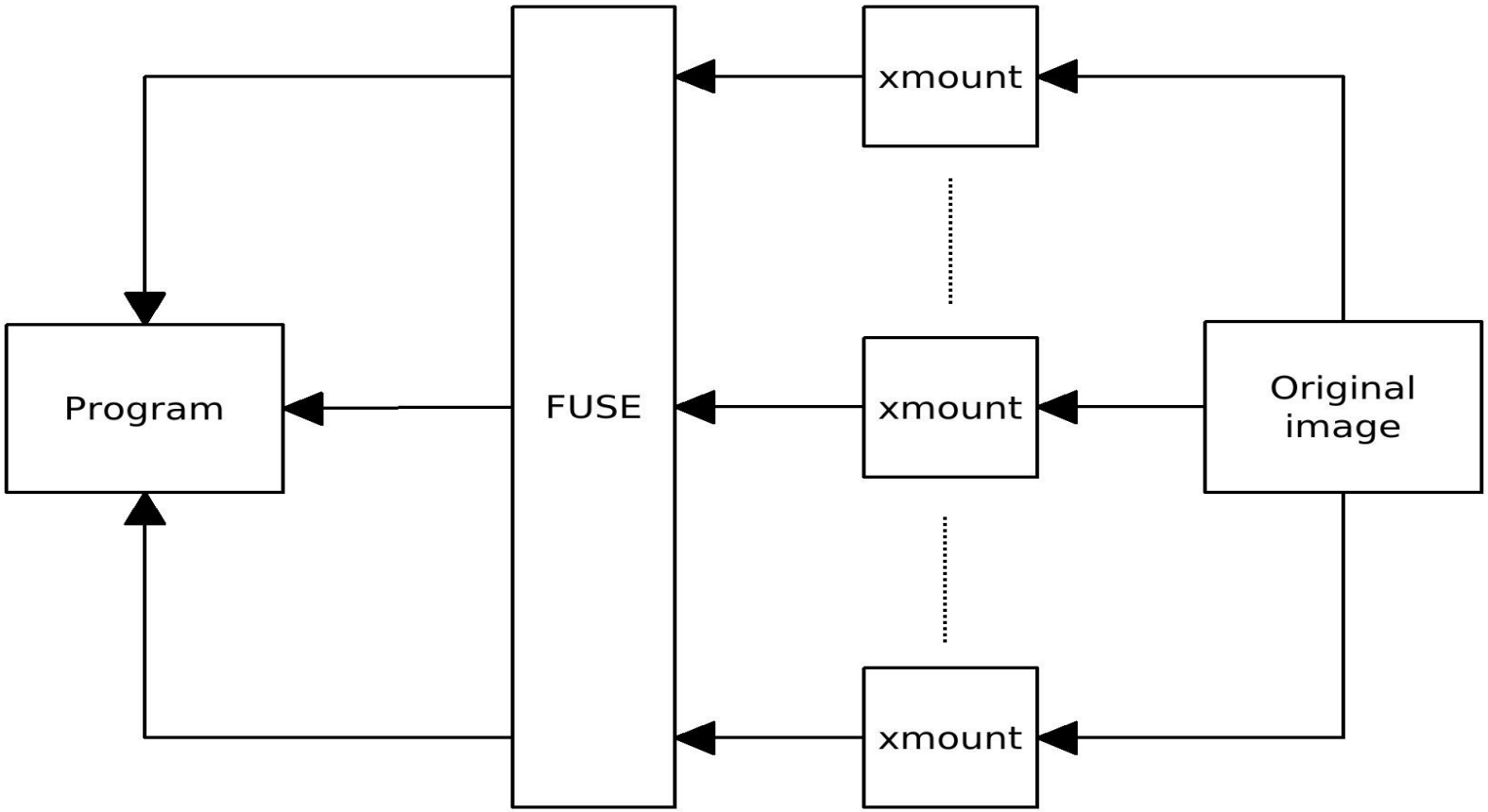
Wie funktioniert xmount

- Erstellen eines virtuellen Dateisystems mittels FUSE (Filesystem in USErspace: ermöglicht das Erstellen virtueller Dateisysteme)



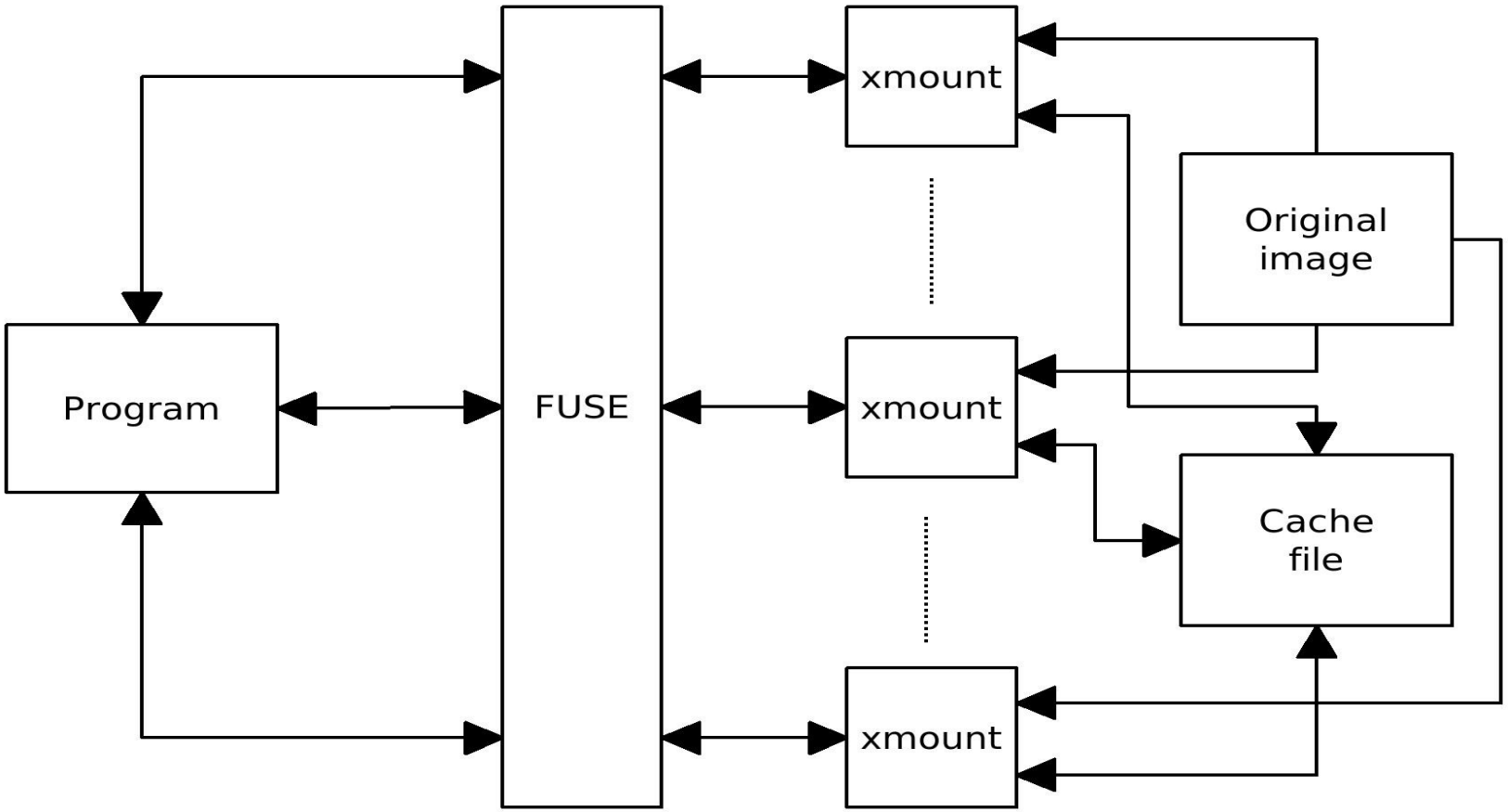
Wie funktioniert xmount (Fortsetzung)

- Lesezugriff auf die virtuelle Image Datei



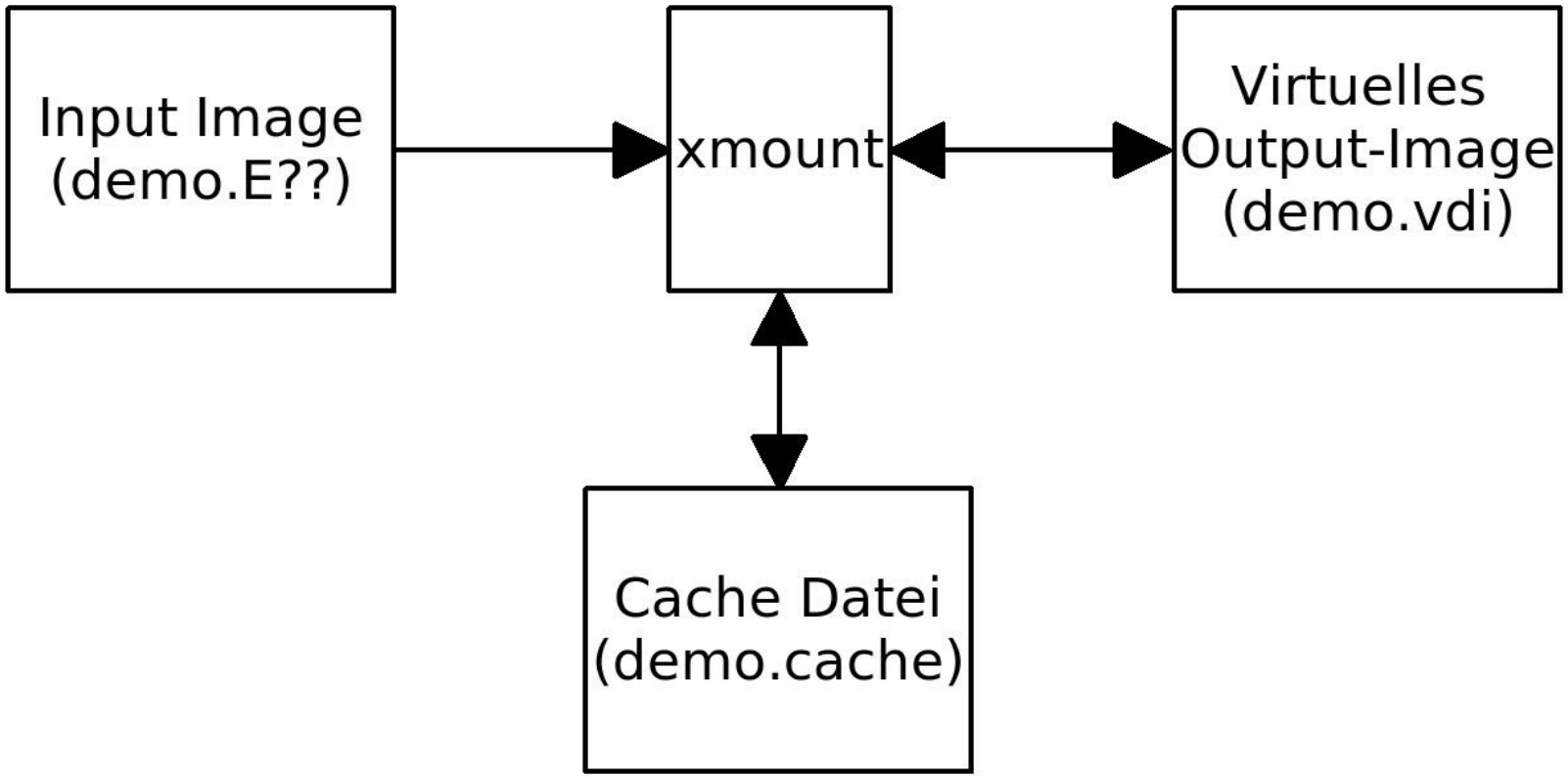
Wie funktioniert xmount (Fortsetzung)

- Lese- / Schreibzugriff auf die virtuelle Image Datei



Wie funktioniert xmount (Fortsetzung)

- Vereinfachte Funktionsweise:
  xmount --in ewf --out vdi --cache demo.cache demo.E?? ./mnt



Voraussetzungen für die Virtualisierung von Festplatten

- Linux mit Kernel >= 2.6 und FUSE-Unterstützung
- xmount
- QEMU, KVM, VirtualBox, VMWare, o.ä.
- Um Windows zu virtualisieren evtl OpenGates

OpenGates

- Aktivieren der Legacy IDE Treiber
- Rücksetzen der Account Passwörter
- Löschen von problematischen Treibern
- Ermittlung der verwendeten HAL-Version (HAL ist der von Windows benutzte Hardware Abstraction Layer. Dieser wird einmalig bei der Installation der Hardware individuell angepasst und kann somit zu Problemen beim späteren Virtualisieren führen)
- Kopieren von AntiWPA (Nach massiven Änderungen der Hardware möchte Windows oft neu Aktiviert werden. AntiWPA umgeht diesen unnötigen Schritt)

Live Demo (EWF nach DD)

Live Demo (EWF nach VDI mit Schreibzugriff und Virtualisierung)

Abschließende Zusammenfassung

- Vorteile:
  - Reine OpenSource / GPL Lösung
  - Unterstützung der wichtigsten Quellformate DD, EWF und AFF
  - Unterstützung der wichtigsten Zielformate DD, VDI und VMDK
  - Auswertestationen können Dank 64bit Linux volle Hardwareleistung nutzen
  - Integrierter Schreibschutz sowie virtueller Schreibzugriff
- Nachteile:
  - Kein Booten von Abbildern einzelner Partitionen möglich
  - Kein Erstellen virtueller Maschinen für VMWare Player (Es wird nur die virtuelle Festplatte erstellt)

Weiterführende Informationen und Downloads

- Projekt Homepage: https://www.pinguin.lu
- Debian Paketserver: http://deb.pinguin.lu

Noch Fragen?