IMF 2007 – Stuttgart, Germany

Thursday, 13. September 2007 - Workshop Day
WS 5 "Virtualisation of forensic Images", 14:00 – 15:30

Documentation

The whole presentation including extra information will be available soon on the IMF project-pages

- http://www.gi-ev.de/fachbereiche/sicherheit/fg/sidar/imf/imf2007/program.html

Almost all examples are based on the training evidence-file "Hacking Case" from the CFReDS Project

- http://www.cfreds.nist.gov/
    - http://www.cfreds.nist.gov/Hacking_Case.html

---

1. Part one: Using Live View

Ralf Moll
Landeskriminalamt Baden-Württemberg, IT-Beweissicherung
E-Mail: ralf.moll@lka.bwl.de
http://www.polizei-bw.de/lka/

1.1. Used Software

- Mount Image Pro for mounting image files
    - http://www.mountimage.com/
- FTK-Imager for converting image files
    - http://www.accessdata.com/catalog/partdetail.aspx?partno=11300
- LibEWF for converting image files
    - https://www.uitwisselplatform.nl/projects/libewf/
- Live View for creating virtual machines
    - http://liveview.sourceforge.net/
- VMware Workstation v5
    - http://www.vmware.com/products/ws/

1.2. Documentation

The presentation is based on wiki technology, so you can work with the papers

- http://en.wikipedia.org/wiki/Wiki
- http://moinmo.in/ Desktop Edition (http://moinmo.in/DesktopEdition)

2. Part two: Using VFC

Holger Morgenstern
Öffentlich bestellter und vereidigter EDV-Sachverständiger für Computerforensik
E-Mail: holger@morgenstern.net
http://www.gutachten.info/

2.1. Used Software

- Mount Image Pro for mounting image files
  - http://www.mountimage.com/
- VMware's free Disk Mount utility:
  - http://www.vmware.com/download/eula/diskmount_ws_v55.html
- VMware's free player
  - http://www.vmware.com/download/player/
- VFC
  - http://www.mountimage.com/virtual-forensic-computing-vfc.php

2.2. Documentation

You can find updated information on

- http://www.computerforensik.net/vfc.html

Notes: