OpenSource Forensik-Werkzeuge

Dipl.-Ing. Mathias Gärtner

Sachverständigenbüro Prof. Pausch & Partner
Heinheimer Strasse 38

D-64289 Darmstadt

Tel.: +49 6151 9712640

Fax.: +49 6151 9712641

Email: Mathias.Gaertner@it-svbuero.de
http://www.it-svbuero.de

Agenda

- Was ist Computer-Forensik
- Closed-Source Systeme und deren Vor- und Nachteile
- Open-Souce Systeme und deren Vor- und Nachteile

- Zusammenfassung
- Fazit

Was ist Computerforensik (I)

- Erlangen von Informationen über das Nutzerverhalten sowie gespeicherte Nutzerdaten entweder
  - Online oder
  - Offline
- Unterschied zum Hacking:
  - Legitimer Eigentümer/Besitzer ist Auftraggeber
  - Strafverfolgung

Tätigkeitsfelder der Computerforensik (II)

- Strafverfolgung: *Was hat wer wann was und wie oft getan?*
  (meistens Offline, aber…)
- Strafprävention: *Was macht wer gerade?*
  (Stichwort: Bundestrojaner)
- Industriespionage: *Wer „klaut“ Daten?*
- Kontrolle: *Wer macht was, bzw. macht jemand was unerlaubtes?*

Allgemeines Vorgehen (III)

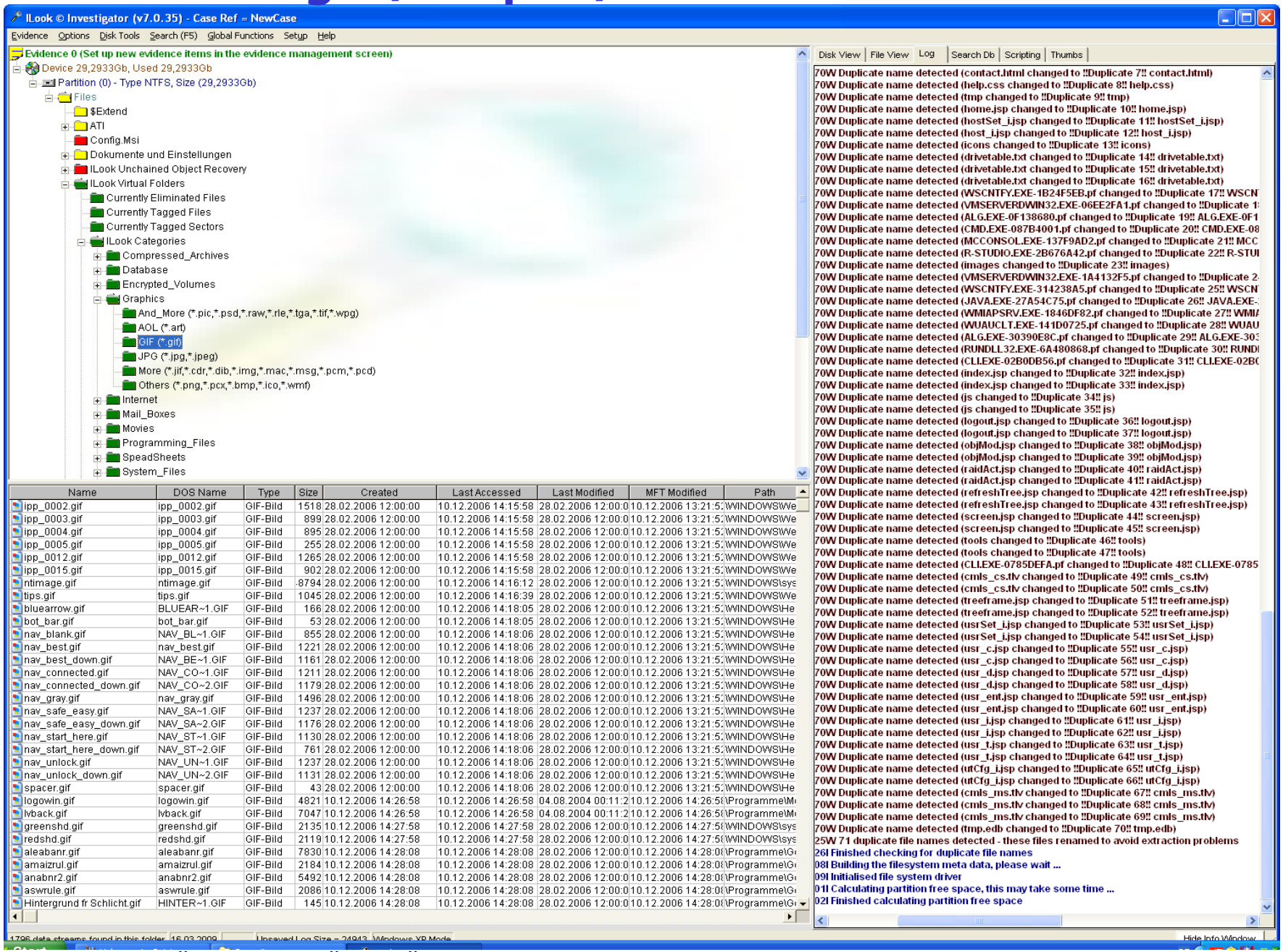
- Beweise/Spuren sichern ohne zu verändern, soweit das möglich ist
- Neutralität wahren
- Nachvollziehbar „Beweise“ zusammenstellen

- Keine illegalen Aktivitäten ausschließen
  -> Beweis sonst ggf. unverwertbar

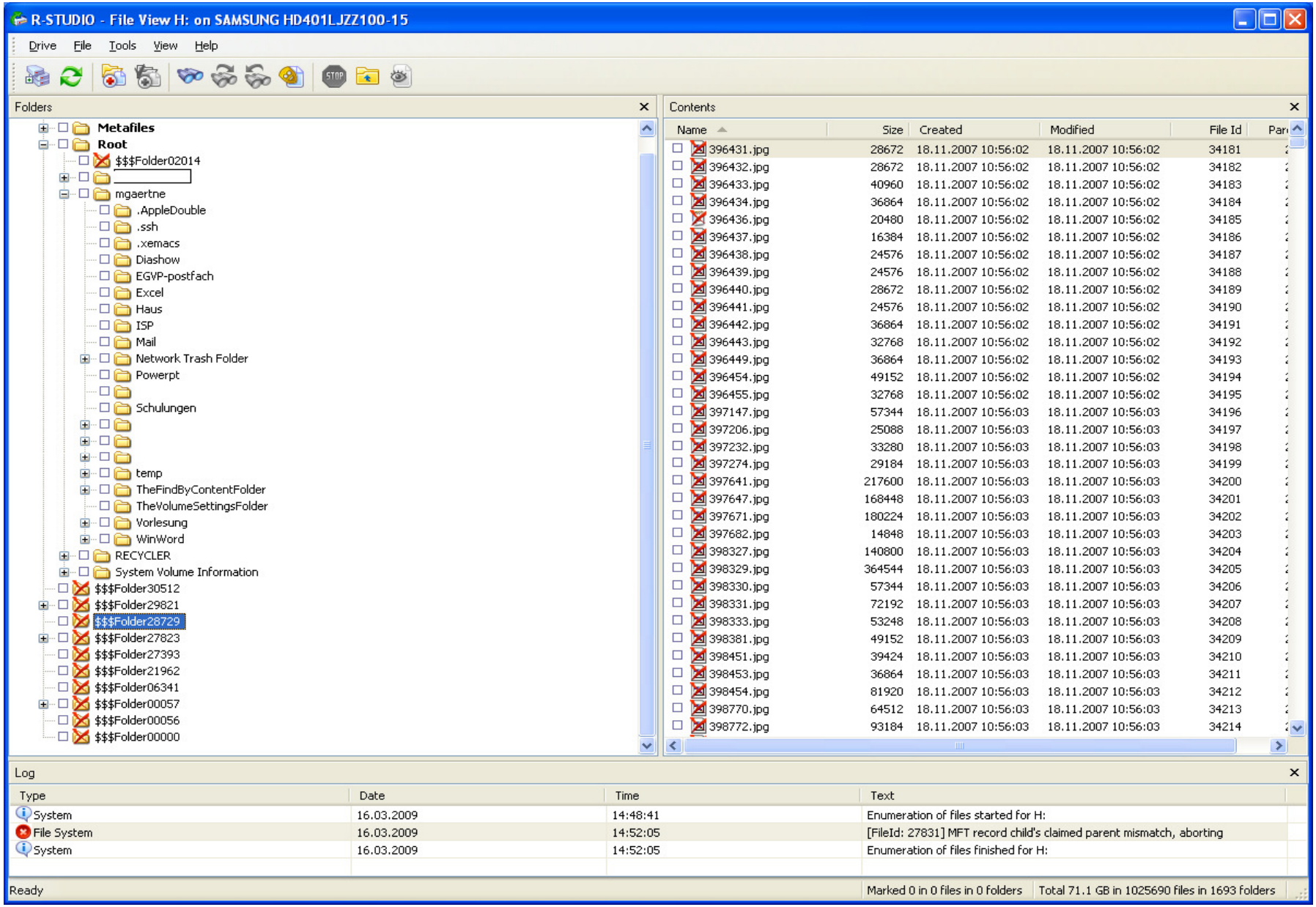
Closed-Source Programme

- Kommerziell erhältliche Programme mit einem durch den Anwender nicht, oder schwer veränderbaren Datenakquisitions-, Auswerte- und Präsentationsumfang
- In der Regel als „One-Shop“ System entwickelt
- Gebräuchlichste Systeme
  - Encase
  - iLook
  - Xways
  - Undelete-Software
  - (perkeo)

Forensic-Werkzeuge (Beispiel)



Undelete-Software



Closed-Source Software: Vor- und Nachteile

Vorteile:

- Es wird wenig technisches Know-How zur Bedienung und Herstellung von brauchbaren Ergebnissen benötigt.
- Es kann (im Rahmen der Softwaremöglichkeiten) wenig „vergessen“ werden.
- Es sind häufig sehr umfangreiche Funktionen und Auswertungen möglich.
- Sehr beweissicher, da Software darauf ausgelegt ist (Protokolle, Checksummen etc.).

Nachteile:

- Es kann nur das ausgewertet werden, was durch die Entwickler programmiert wurde.
- Reports oft sehr „amerikanisiert“ und u.U. nur bedingt für deutsche Strafverfolger sinnvoll.
- Vorgefertigte Module/Auswertungen benötigen kein umfassendes Know-How
  - „Was nicht von XXX angezeigt wird, existiert nicht“

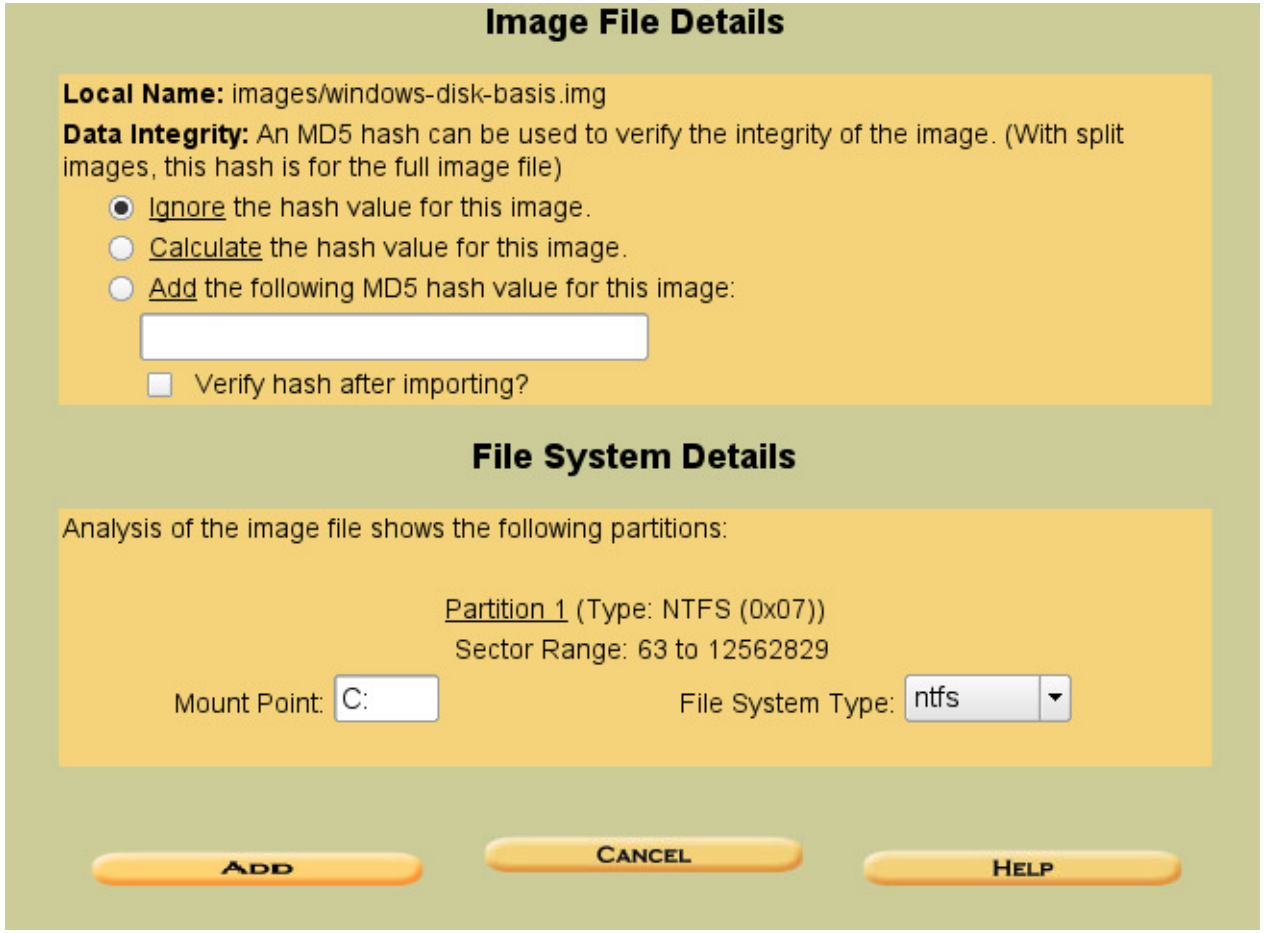
Open Source Werkzeuge (I)

- LINUX/UNIX-Tools
  - dd_rescue zum Erzeugen von Festplatteinimages
  - md5sum zum Erzeugen von Hashcodes
  - ntfsundelete zum Wiederherstellen von gelöschten Dateien
  - find zum finden von Dateien
  - file zum Feststellen von Dateiformaten
  - Screenshot zum Herstellen von Bildschirmabbildungen

Open Source Werkzeuge (II)

- **Sleuthkit** und dessen Werkzeuge
- **Foremost, recoverjpeg** zum Wiederherstellen von Bild- und anderen Dateiformaten
- z.B. **mplayer** zum Darstellen von Videos
- **gwenview/irfanview** zum Ansehen von Bilddateien und Erstellen von Zusammenfassungen (thumbnails)
- **Wireshark** zum Mitschneiden von Netzwerkaktivitäten
- ClamAV zum Überprüfen auf Viren oder Trojaner
- Quellen auf dem **Internet** (www.endungen.de, Forensik- Veröffentlichungen usw.)
- Und, und, und

Open-Source Beispiele, sleuthkit



Open-Source Beispiele, sleuthkit und dd_rescue

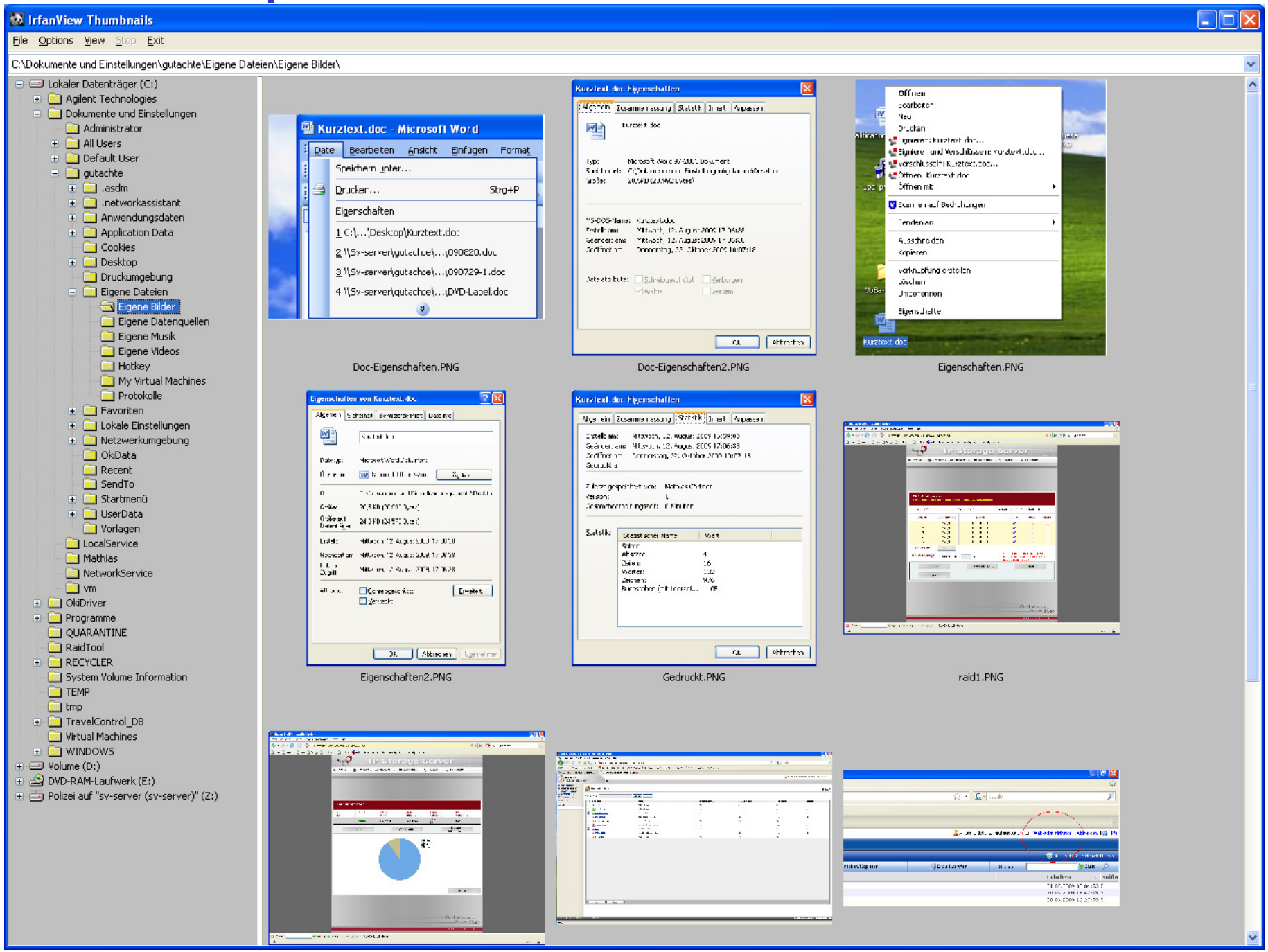
Current Directory: C:/ /Dokumente und Einstellungen/

ADD NOTE GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	d / d	../	2009-03-13 16:09:51 (MET)	2009-03-13 16:09:51 (MET)	2009-03-13 16:09:51 (MET)	2009-03-13 15:51:42 (MET)	56	48	0	5-144-6
	d / d	./	2009-03-13 15:34:09 (MET)	2009-03-13 15:34:09 (MET)	2009-03-13 15:34:09 (MET)	2009-03-13 14:57:39 (MET)	56	0	0	3416-144-6
	d / d	All Users/	2009-03-13 15:18:02 (MET)	2009-03-13 16:20:48 (MET)	2009-03-13 15:18:02 (MET)	2009-03-13 14:57:39 (MET)	56	0	0	3418-144-6
	d / d	Default User/	2009-03-13 15:33:51 (MET)	2009-03-13 15:34:09 (MET)	2009-03-13 15:33:51 (MET)	2009-03-13 14:57:39 (MET)	56	0	0	3417-144-7
	d / d	Gutachte/	2009-03-13 15:34:20 (MET)	2009-03-13 15:34:20 (MET)	2009-03-13 15:34:20 (MET)	2009-03-13 15:34:09 (MET)	56	0	0	9970-144-5
	d / d	LocalService/	2009-03-13 15:32:20 (MET)	2009-03-13 15:32:20 (MET)	2009-03-13 15:32:20 (MET)	2009-03-13 15:32:19 (MET)	56	0	0	9973-144-6
	d / d	NetworkService/	2009-03-13 15:32:02 (MET)	2009-03-13 15:32:02 (MET)	2009-03-13 15:32:02 (MET)	2009-03-13 15:32:01 (MET)	56	0	0	3395-144-6

```
auswerter:/Disk1/autopsy-2.22 # dd_rescue /dev/sda /Disk1/test
dd_rescue: (info): ipos:     64512.0k, opos:     64512.0k, xferd:     64512.0k
                   errs:       0, errxfer:        0.0k, succxfer:     64512.0k
               +curr.rate:  54479kB/s, avg.rate:  29880kB/s, avg.load:  1.4%
```

Open-Source Beispiele, irfanview



Open-Source Werkzeuge Vor- und Nachteile (I)

Nachteile:

- Sehr umfangreich, man muss schon wissen was man braucht.
- Reports sind selten automatisch erstellbar
- „Vergessen“ einer Auswertung ist leicht möglich, da die Software keinen „Fahrplan“ vorgibt.
- Beweissicherheit i.d.R. nur durch zusätzliche Maßnahmen erreichbar.
- Es sind fast immer eigene Ergänzungen notwendig, um schnell brauchbare Ergebnisse zu erhalten.
- Interpretation der Ergebnisse durch den technisch Sachverständigen ist unumgänglich.

Open-Source Werkzeuge Vor- und Nachteile (II)

Vorteile:

- Sehr umfangreich
  - fast alles ist schon mal programmiert worden und kann genutzt werden
- Der Untersucher benötigt nach wie vor technische Kenntnisse und Informationen über den internen Ablauf von Computer-Systemen.
- Sehr schneller Einsatz (pro Werkzeug) möglich , da sehr spezialisierte Werkzeuge vorliegen.

Zusammenfassung (I)

- *Closed-Source* Programme bieten umfangreiche, aber unbekannt hinreichende Auswertemöglichkeiten.
- Open-Source Programme bieten jeweils nur eine Funktion, aber durch die Vielfalt wird (fast) alles abgedeckt.
- Beim Einsatz von *Closed-Source* ist meist wenig Know-How über das zu untersuchende System an sich notwendig (ist aber hilfreich), daher recht schnell brauchbare Ergebnisse.
- *Open-Source* liefert nur das, was man mit entsprechendem Wissen auch abfragt/erstellt.

Zusammenfassung (II)

- *Closed-Source* ist i.d.R. ein System in dem bzw. mit dem alles organisiert und ausgewertet wird.
- *Open-Source* ist eine Sammlung von nicht zusammenpassenden Einzelsystemen. Ausnahme hier ist „sleuthkit“ mit „autopsy“.
- *Closed-Source* hat systematisch (nicht programmtechnisch) wenig Fehlerquellen.
- Der Einsatz von *Open-Source* bietet viele Fehlerquellen.

Fazit

- Es existiert bei *Open-Source* Systemen, anders als in *Closed-Source* Systemen, kein Forensik-Fahrplan oder Checklisten. Fehlerquelle ist hier das Übersehen bzw. Vergessen einer Auswertung.
- *Open-Source* Systeme bieten mindestens den selben Funktionsumfang wie *Closed-Source* Systeme, die einzelnen Elemente sind aber nicht aufeinander abgestimmt.
- Open-Source Systeme sind für die Wünsche des Forensikers umprogrammierbar und neue Auswertungen sind leicht einführbar.
- Der Vortragende verwendet ausschließlich *Open-Source*-Lösungen um jeweils für den Auftraggeber angepasste Ergebnisse liefern zu können. Auch sind die einzelnen Programme leichter bedienbar als eine Closed-Source-Lösung.