FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

GUI für Volatility (VOLIX)

Steffen Logen
Lehrgebiet Datennetze

IT Forensik
FH Aachen

Volatility

Volatility:

Volatility ist ein freies Untersuchungstool zur Extraktion von Artefakten in einem RAM Image. Wird u.a. zur Ermittlung von Malware auf einem Rechner verwendet.

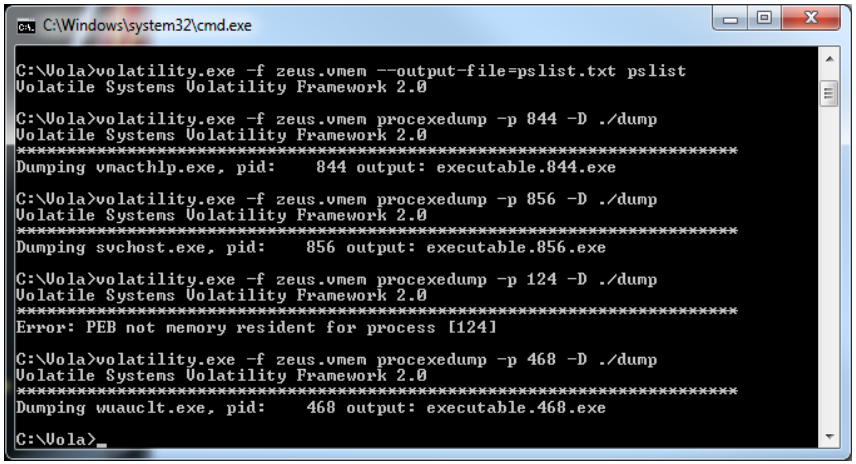
Wichtige Funktionen:

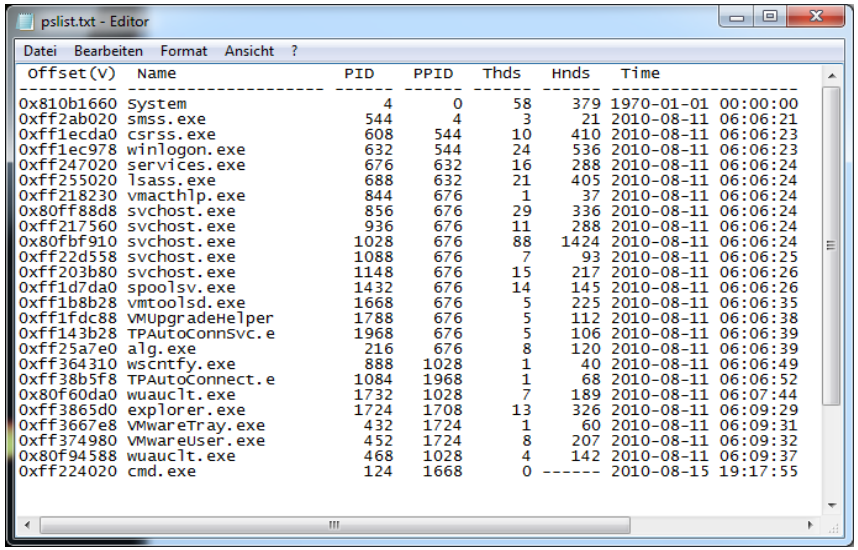
- Anzeige auf dem System laufender Prozesse
- Netzwerkverbindungen
- Geladene DLLs

- Kommandozeilen-Tool
- In Python geschrieben
- Unter GNU (General Public License) veröffentlicht

Volatility Nachteile

- Kommandozeilen-Tool
  - Umständlich
  - Relativ langsam
  - Nicht geeignet für nicht versierte Benutzer
- Speicherung von Daten
  - Ausgabe in Kommandozeile als .txt speicherbar
- Vergleichen von Daten
  - Muss manuell gemacht werden



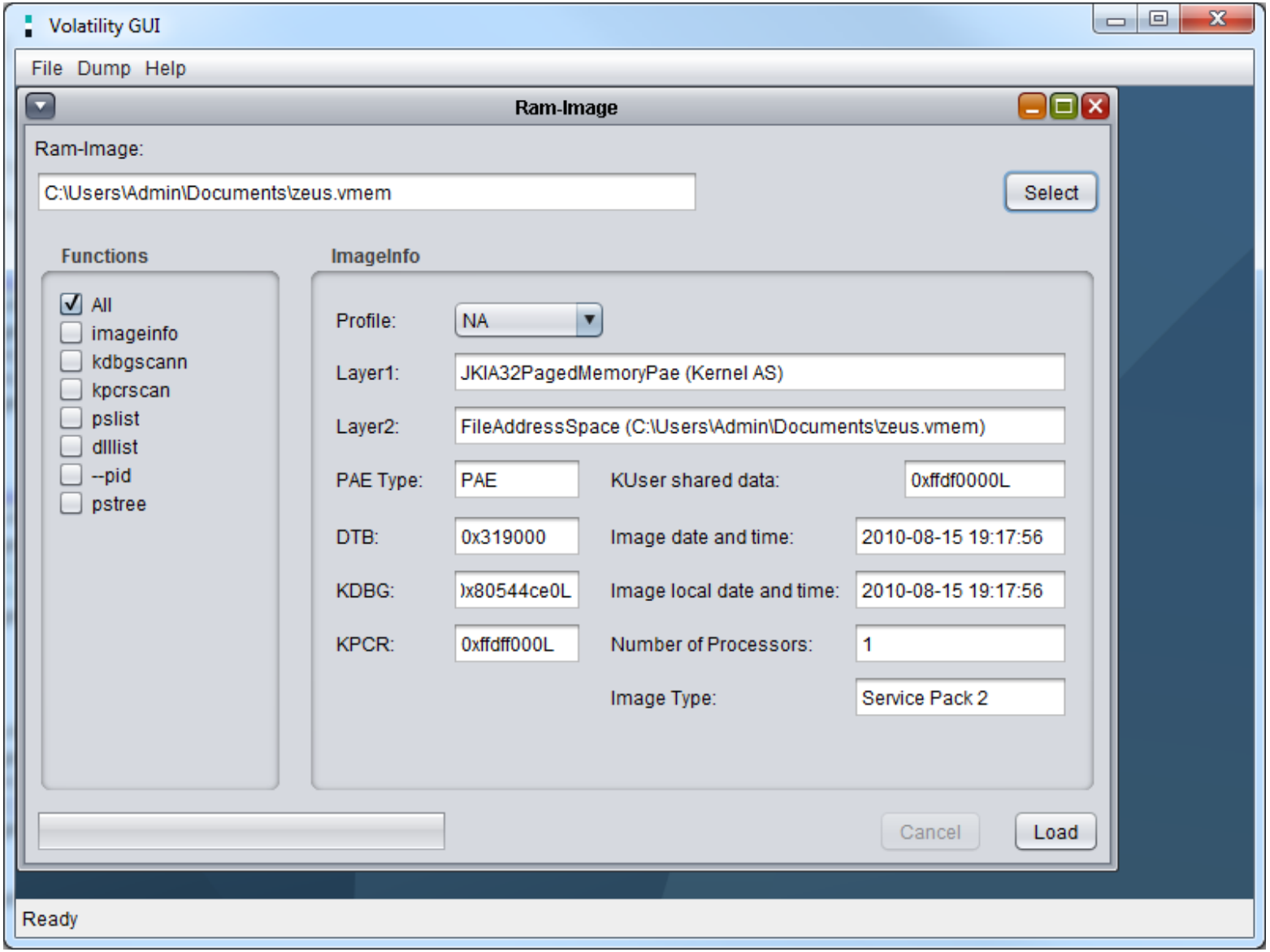


Volatility GUI (VOLIX)

Ziele der GUI

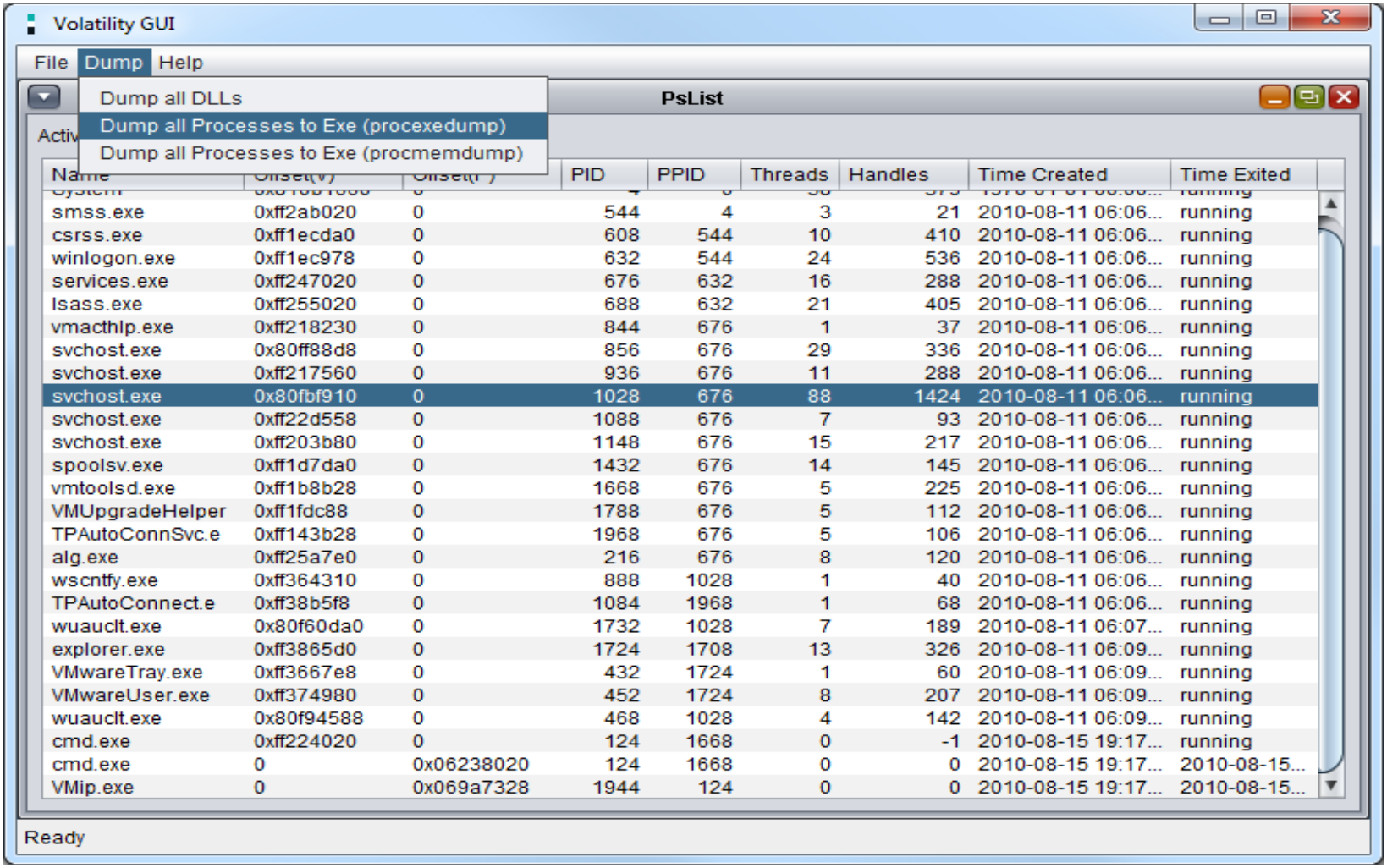
- Einfachere Bedienung von Volatility
  - GUI Bedienung ist intuitiver
  - Mehrere Befehle werden in einfache Schritte zusammengefasst
- Gesteigerte Geschwindigkeit bei Analysen
- Leichtere Vergleichbarkeit von Ergebnissen
- Speicherung der Daten
  - Speicherung in Datenbank
  - Export / Import von Ergebnissen
- Hilfestellung
- Neue Funktionen, welche mit Volatility nicht möglich sind (oder nur sehr schwer)

Volatility GUI (VOLIX)

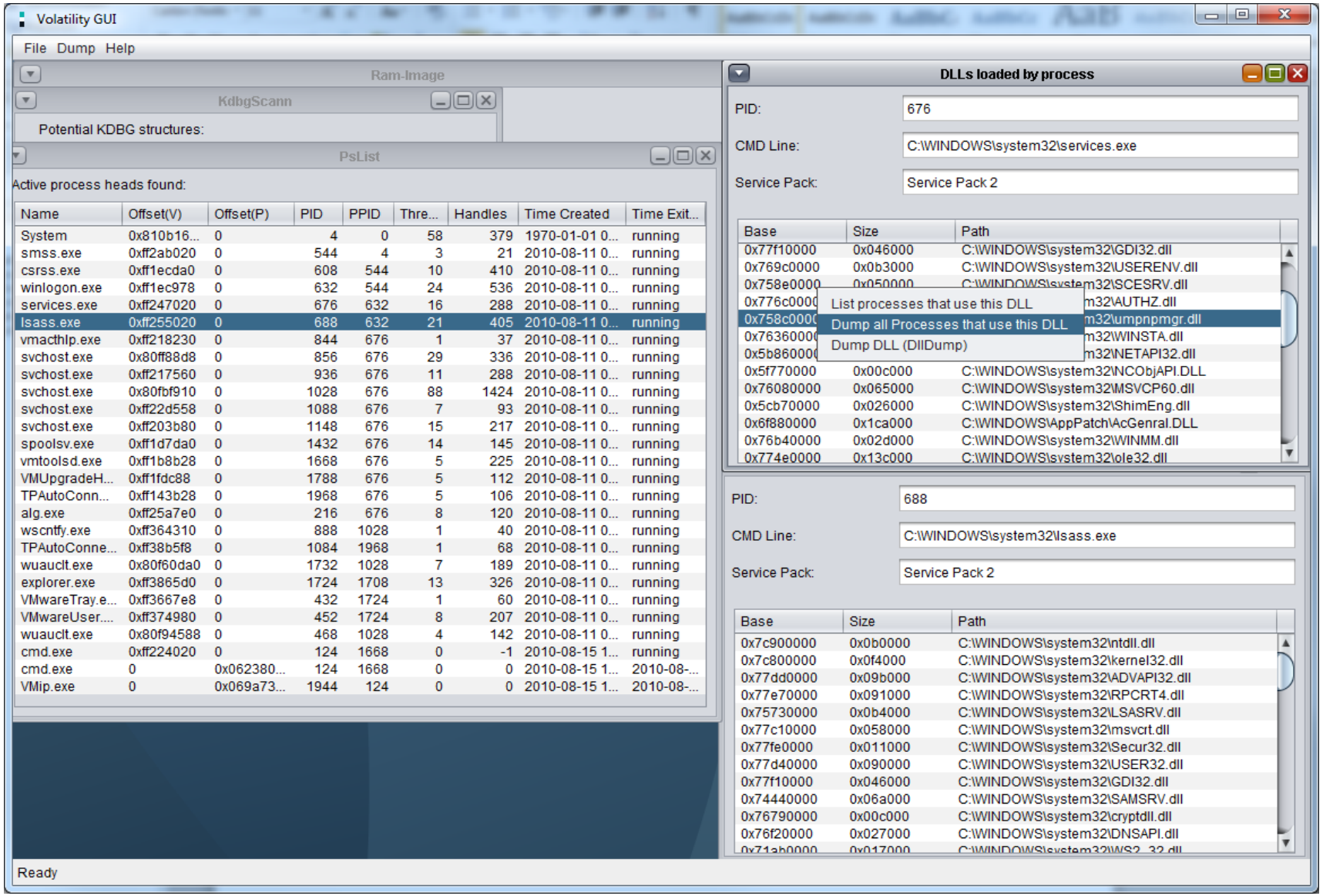


Volatility GUI (VOLIX)

- Einfaches Dumpen aller Prozesse im Image über einen Klick

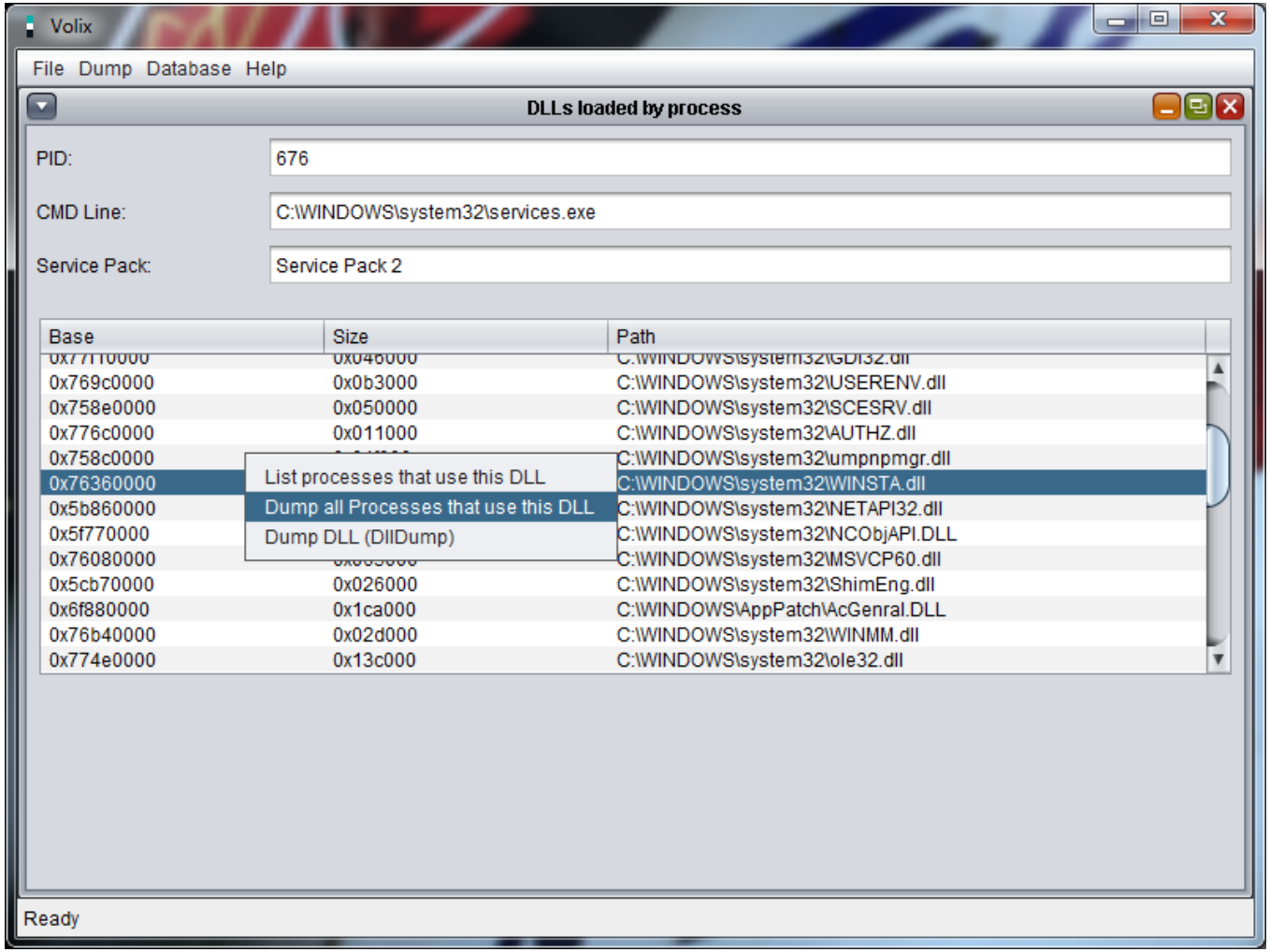


Volatility GUI (VOLIX)



Volatility GUI (VOLIX)

- Vereinfachung von Schritten,
  welche mit Volatility nur schwer möglich sind



Weitere GUI Möglichkeiten

Features welche noch nicht implementiert sind:

- Batch Analyse von Images
- Statistiken zu analysierten Images
- Grafische Auswertung durch Diagramme
  - Vergleich, welcher Prozess wie viele Netzwerkverbindungen offen hat
- Verbindungs-Diagramme
  - Welche Prozesse sind über welche DLLs miteinander verknüpft?

Projekt-Webseite

- http://www.it-forensik.fh-aachen.de/
  - im Menü „Projekte“

Danke für Ihre Aufmerksamkeit!