

Verbesserung der forensischen Untersuchung von RAM-Abbildern mit Volix II

Patrick Bock

Lehrgebiet Datennetze, IT-Sicherheit
und IT-Forensik



- Einleitung
- Probleme und Lösungen
- Fallbeispiel

- Einleitung
- Probleme und Lösungen
- Fallbeispiel

- Volatility Framework
 - Quelloffen
 - Wird ständig weiterentwickelt
 - Viele verschiedene Befehle

 - Kommandozeilenbasiert
 - Benötigt gute Kenntnis der Befehle

- Untersuchung mit dem Volatility Framework
 - Befehle einzeln eingeben
 - Parameter immer setzen
 - Parameter aus Ausgaben extrahieren
 - Keine Dokumentation der Untersuchung

```

C:\Users\Patrick\Desktop\Bachelorarbeit\VolatilityFramework>volatility-2.3.1.standalone -f C:\Users\Patrick\Desktop\Bachelorarbeit\VolatilityFramework\zeus.vmem imageinfo
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...

Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (C:\Users\Patrick\Desktop\Bachelorarbeit\VolatilityFramework\zeus.vmem)
PAE type : PAE
DTB : 0x319000L
KDBG : 0x80544ce0L
Number of Processors : 1
Image Type (Service Pack) : 2
KPCR for CPU 0 : 0xffdff000L
KUSER_SHARED_DATA : 0xffdf0000L
Image date and time : 2010-08-15 19:17:56 UTC+0000
Image local date and time : 2010-08-15 15:17:56 -0400

C:\Users\Patrick\Desktop\Bachelorarbeit\VolatilityFramework>
  
```

- Volix II (**V**olatility **I**nterface & **E**xtensions)
 - Interface für das Volatility Framework
 - Einbinden weiterer Programme

- Untersuchung mit Volix II (Version 1)
 - Befehle einfach einfügen
 - Parameter immer setzen
 - Parameter aus Ausgaben extrahieren
 - Einfache Dokumentation

The screenshot shows a software interface with a list of modules on the left and a configuration window for the 'imageinfo' module on the right.

Möglichl

- apihooks
- atoms
- atomscan
- bioskbd
- callbacks
- clipboard
- cmdscan
- connectic
- connscan
- consoles
- crashinfo**
- deskscan

Name

imageinfo

Beschreibung

Module ImageInfo

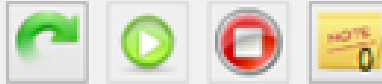
Identifiziert das Image

Befehl

imageinfo

Navigation buttons: up and down arrows.

Ergebnis



Befehl

```
imageinfo
```

```
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...
  Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
    AS Layer1 : IA32PagedMemoryPae (Kernel AS)
    AS Layer2 : FileAddressSpace (C:\Users\Patrick\Desktop\Bachelorarbeit\W
      PAE type : PAE
      DTB : 0x319000L
      KDBG : 0x80544ce0L
  Number of Processors : 1
  Image Type (Service Pack) : 2
    KPCR for CPU 0 : 0xffdff000L
    KUSER_SHARED_DATA : 0xffdf0000L
  Image date and time : 2010-08-15 19:17:56 UTC+0000
  Image local date and time : 2010-08-15 15:17:56 -0400
```

- Einleitung
- Probleme und Lösungen
- Fallbeispiel

- Problem
 - Volatility Framework 2.2 integriert
 - Aktuell Version 2.3.1 mit deutlich mehr Befehlen

- Lösung
 - Version 2.3.1 unterstützen
 - Alle Befehle implementieren

- Problem
 - Aufwendige Untersuchung
 - Jeden Befehl einzeln starten
 - Alle Ergebnisse genau untersuchen
 - Jeden Befehl neu parametrieren

- Dauert sehr lange

- Lösung
 - Untersuchung automatisieren
 - Drei Befehle werden automatisch gestartet
 - Starte bis zu drei Befehle, die keine weiteren Parameter benötigen
 - Untersuche deren Ergebnisse um bei anderen Befehlen Parameter zu setzen
 - Wiederhole bis kein Befehl mehr gestartet werden kann

- Problem
 - Befehle müssen bekannt sein
 - Abhängigkeiten unter Befehlen

- Lösung
 - Hilfestellung in Form von Wizards
 - Fragen an den Benutzer

- Problem
 - Unübersichtlicher Abschlussbericht
 - Reine Textdatei mit allen Informationen

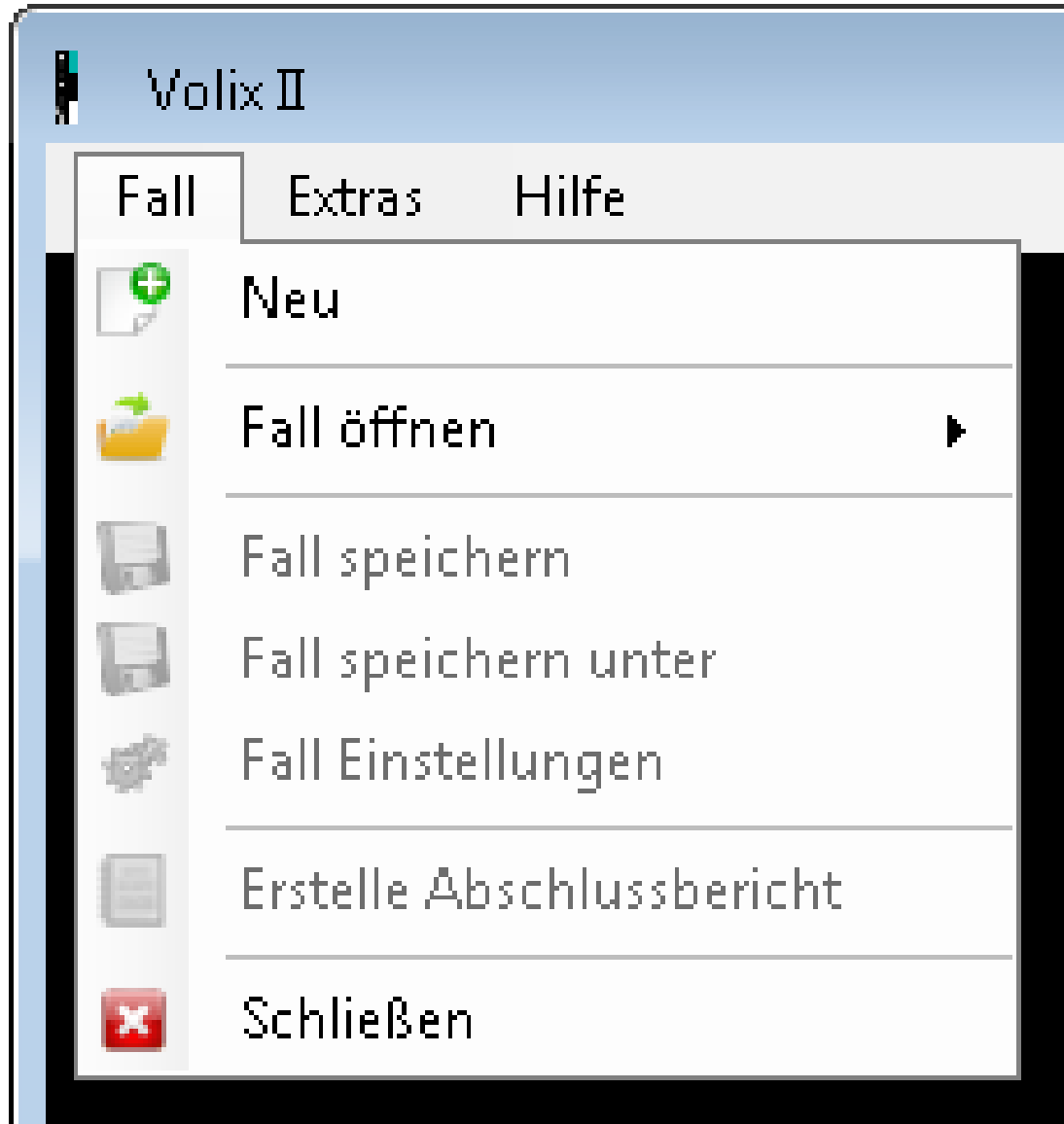
- Lösung
 - Informationen in XML-Datei
 - Darstellung durch XSL-Datei

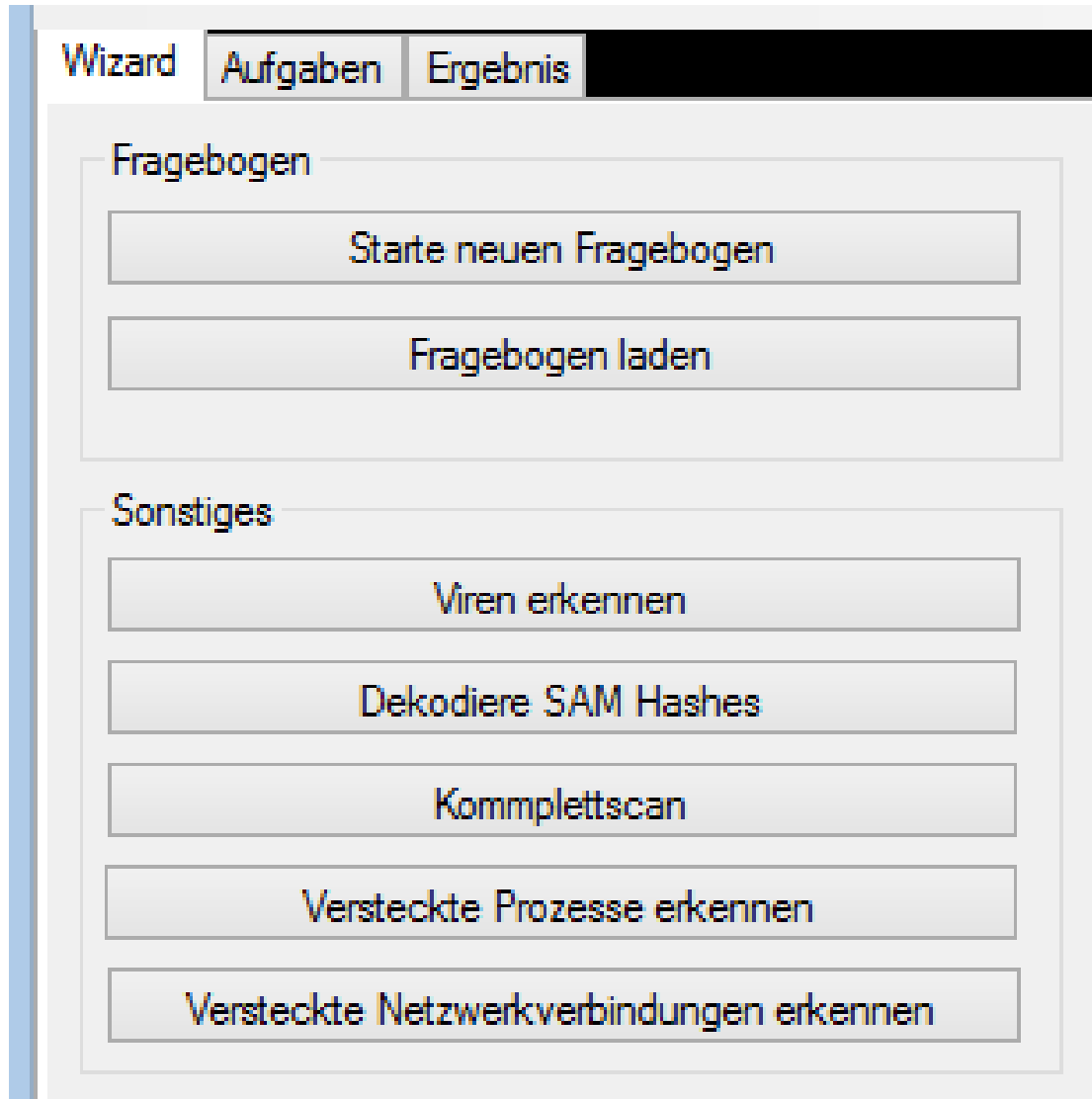
- Weitere Verbesserungen
 - Hilfe zum Programm
 - Hilfe um ein Fallbeispiel erweitert
 - Individuelle Ansicht für „hashdump“
 - Extrahiert SAM-Hashes
 - John the Ripper knackt diese

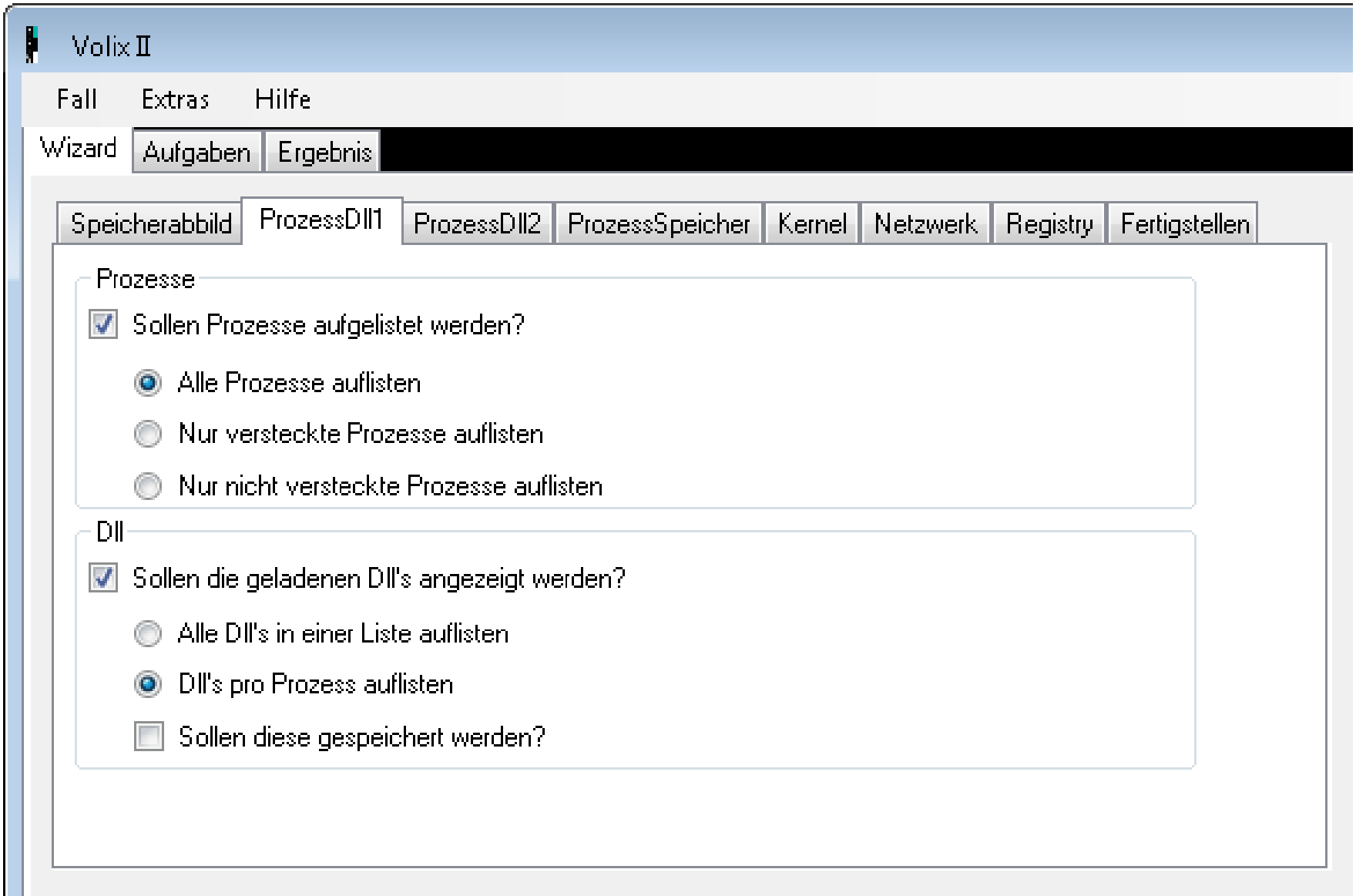
- Einleitung
- Probleme und Lösungen
- Fallbeispiel

- Vorbereitung
 - Ordnerstruktur anlegen
 - RAM-Abbild bereitstellen

- Untersuchung_BlackEnergy
 - ErgebnisDumps
 - Logdatei








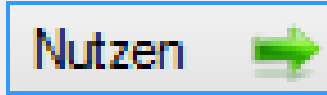

The screenshot shows the Volix II software interface. The title bar reads "Volix II". The menu bar contains "Fall", "Extras", and "Hilfe". Below the menu bar is a "Wizard" section with three tabs: "Aufgaben", "Ergebnis", and "Ergebnis" (highlighted). Underneath are several category tabs: "Speicherabbild", "ProzessDll1", "ProzessDll2", "ProzessSpeicher", "Kernel", "Netzwerk", "Registry", and "Fertigstellen". The main content area is divided into two sections: "Prozesse" and "Dll".

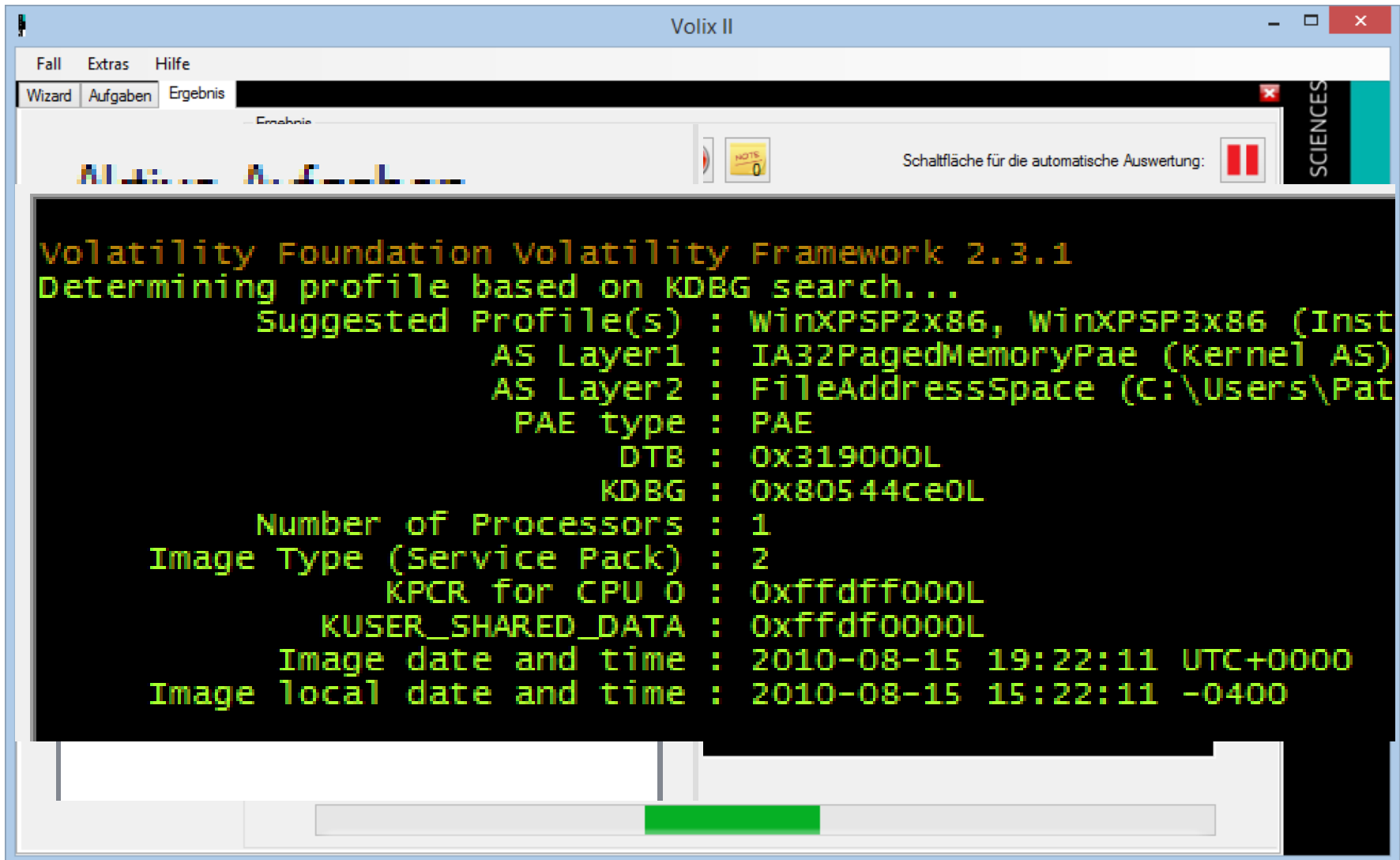
Prozesse

- Sollen Prozesse aufgelistet werden?
 - Alle Prozesse auflisten
 - Nur versteckte Prozesse auflisten
 - Nur nicht versteckte Prozesse auflisten

Dll

- Sollen die geladenen Dll's angezeigt werden?
 - Alle Dll's in einer Liste auflisten
 - Dll's pro Prozess auflisten
 - Sollen diese gespeichert werden?

Möglichkeiten		Gewählt
mac_version	  	hivelist
mac_volshell		hashdump
mac_yarascan		imageinfo
machoinfo		kdgbscan
malfind		psscan
mbrparser		handles
memdump		psxview
memmap		
messagehooks		
mftparser		
moddump		



The screenshot shows the Volix II application window. The title bar reads "Volix II". The menu bar includes "Fall", "Extras", and "Hilfe". Below the menu bar are tabs for "Wizard", "Aufgaben", and "Ergebnis". The main content area displays the output of a Volatility Framework command, showing system profile information for a Windows XP SP2/3 system.

```

Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...
  Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Inst
    AS Layer1 : IA32PagedMemoryPae (Kernel AS)
    AS Layer2 : FileAddressSpace (C:\Users\Pat
    PAE type : PAE
    DTB : 0x319000L
    KDBG : 0x80544ce0L
  Number of Processors : 1
  Image Type (Service Pack) : 2
    KPCR for CPU 0 : 0xffdff000L
    KUSER_SHARED_DATA : 0xffdf0000L
  Image date and time : 2010-08-15 19:22:11 UTC+0000
  Image local date and time : 2010-08-15 15:22:11 -0400
  
```

Aktive Aufgaben

hivelist
hashdump
imageinfo
kdgbscan
psscanner
handles
psxview
dlllist
dlllist
dlllist
dlllist
dlllist

Aktive Aufgaben

hivelist
hashdump
imageinfo
kdgbscan
psscanner
handles
psxview
dlllist
dlllist
dlllist
dlllist
dlllist

Abschlussbericht der forensischen Untersuchung eines Speicherabbildes Erstellt mit Volix II

Allgemein

Untersucher	Patrick Bock
Datum	05.05.2014 11:32:48
Dateiname	C:\Users\Patrick\Desktop\Untersuchung_BlackEnergy\be2.vmem\be2.vmem
Checksumme	50D9866ADC908508C85517D2D1F55847EC52080B7244C13960A3EF9F4AA98C2A
Kommentar	Hier gehören wichtige Informationen hin

Jobliste

Befehl	imageinfo		
Ergebnis	<pre> Volatility Foundation Volatility Framework 2.3.1 Determining profile based on KDBG search... Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86) AS Layer1 : IA32PagedMemoryPae (Kernel AS) AS Layer2 : FileAddressSpace (C:\Untersuchungen \Untersuchung_BlackEnergy\be2.vmem\be2.vmem) PAE type : PAE DTB : 0x319000L KDBG : 0x80544ce0L Number of Processors : 1 Image Type (Service Pack) : 2 KPCR for CPU 0 : 0xffdff000L KUSER_SHARED_DATA : 0xffdf0000L Image date and time : 2010-08-15 19:22:11 UTC+0000 Image local date and time : 2010-08-15 15:22:11 -0400 </pre>		
Notizen	Datum	Name	Text

Logeinträge

Datum	Text
01.05.2014 20:39:29	Neuer Fall erstellt
01.05.2014 20:41:05	imageinfo hinzugefügt
01.05.2014 20:41:05	kdbgscan hinzugefügt
01.05.2014 20:41:05	psscanscan hinzugefügt
01.05.2014	handles hinzugefügt

Vielen Dank für ihre Aufmerksamkeit