FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Digital Forensics of RAM Images Using VOLIX II

Patrick Bock

FH Aachen, University of Applied Sciences

IT Forensik
FH Aachen

Contents

Contents

Introduction

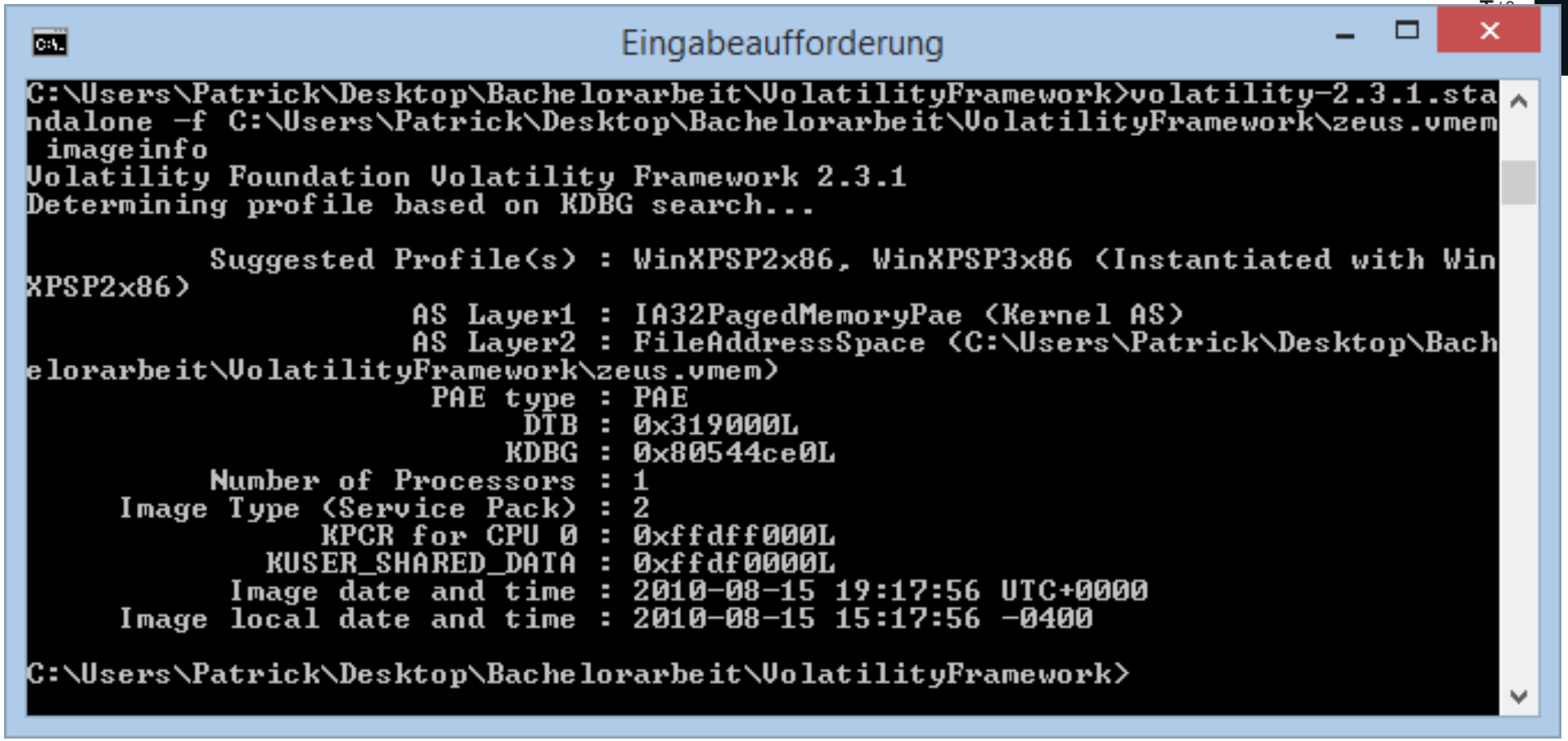
- Volatility Framework
  - Open source
  - Is under constant development
  - Many different commands

  - Command line program
  - Requires good knowledge of the commands

Introduction

- Investigation with the Volatility Framework
  - Type in every command
  - Set all parameters manually
  - Extract information for parameters from results
  - No documentation of the procedure

Introduction

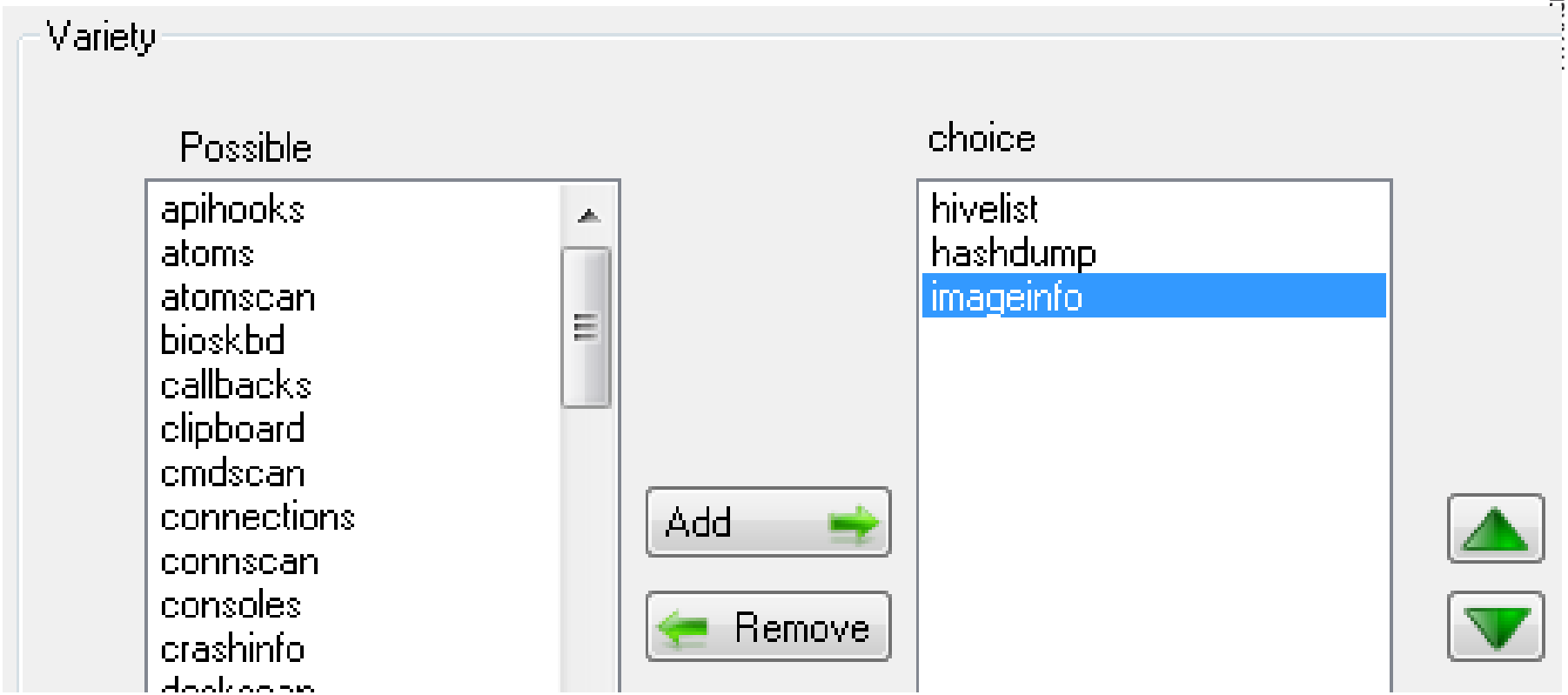


Introduction

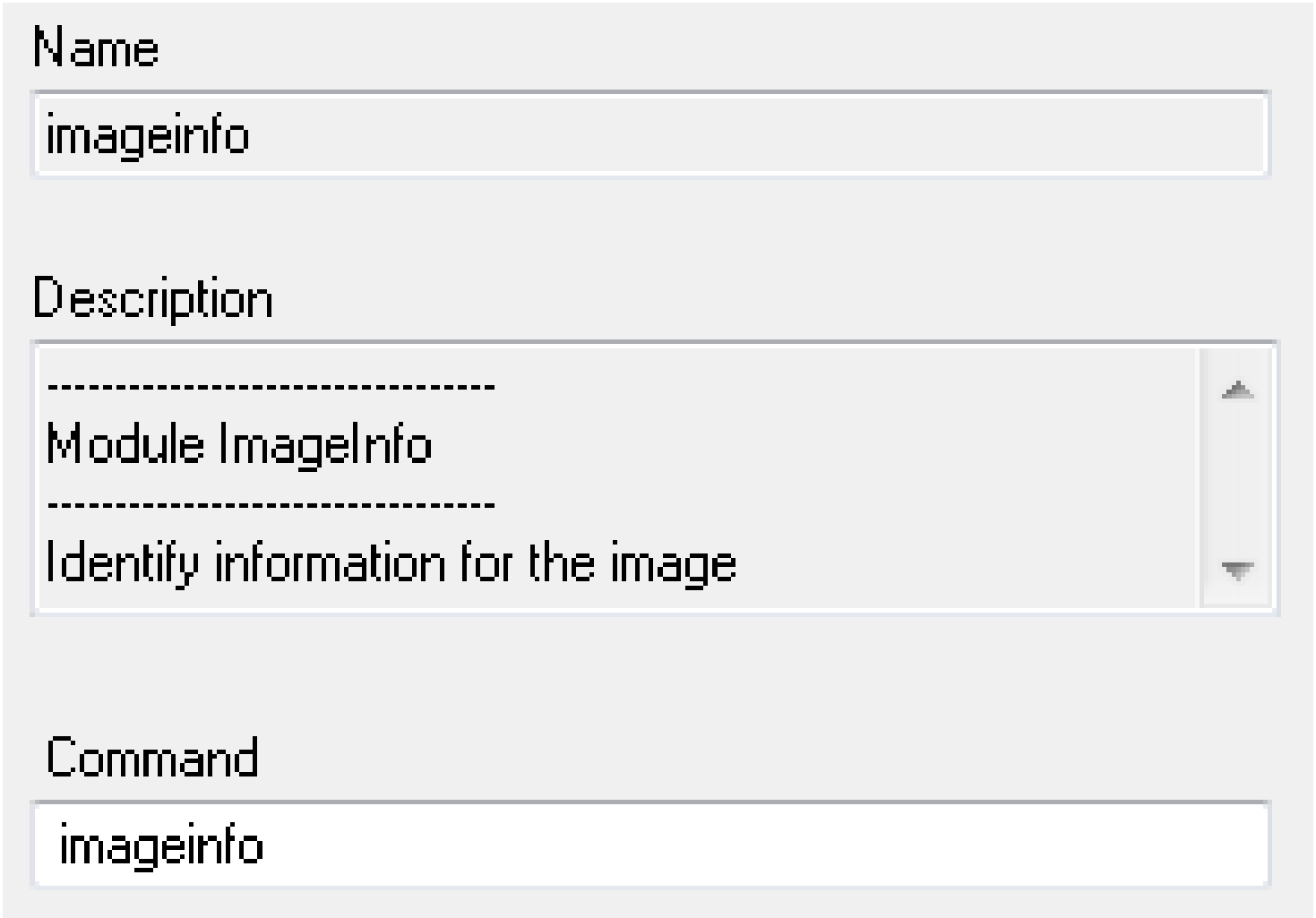
- Volix II (**Vol**atility **I**nterface & E**x**tensions)
  - Interface for the Volatility Framework
  - Embed other programs

- Investigation with Volix II (Version 1)
  - Add commands easily
  - Set all parameters manually
  - Extract information for parameters from results
  - Simple documentation

Introduction



Introduction



Introduction

Result

Buttons for the selected job:

Button for automatic run:

Command

```
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:\Untersuchungen\Untersuchung_BlackEnergy
                      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
```

Contents

Problems and Solutions

- Problem
  - Volatility Framework 2.2 integrated
  - Current version 2.3.1 has much more commands
- Solution
  - Support version 2.3.1
  - Implement all commands

Problems and Solutions

- Problem
  - Extensive investigation
  - Start each command
  - Inspect all results precisely
  - Parameterize each command

  - Takes a long time

Problems and Solutions

- Solution
  - Automate investigation
  - Let commands run parallel

  - Start up to three ready commands
  - When a command is finished examine its result
  - Set parameters for commands
  - Repeat until no command can be started

Problems and Solutions

- Problem
  - User has to know the commands
  - Dependencies among commands
- Solution
  - Assistance in the form of Wizards
  - Questionnaire for the user

Problems and Solutions

- Problem
  - Simple final report
  - Plain text file with all the information

- Solution
  - Information in XML-File
  - Representation by XSL file

Problems and Solutions

- Further improvements
  - Better helpfile for the program
  - Case example in the helpfile

  - Individual dialog view for „hashdump“
  - Extract SAM hashes
  - Crack hashes with John the Ripper

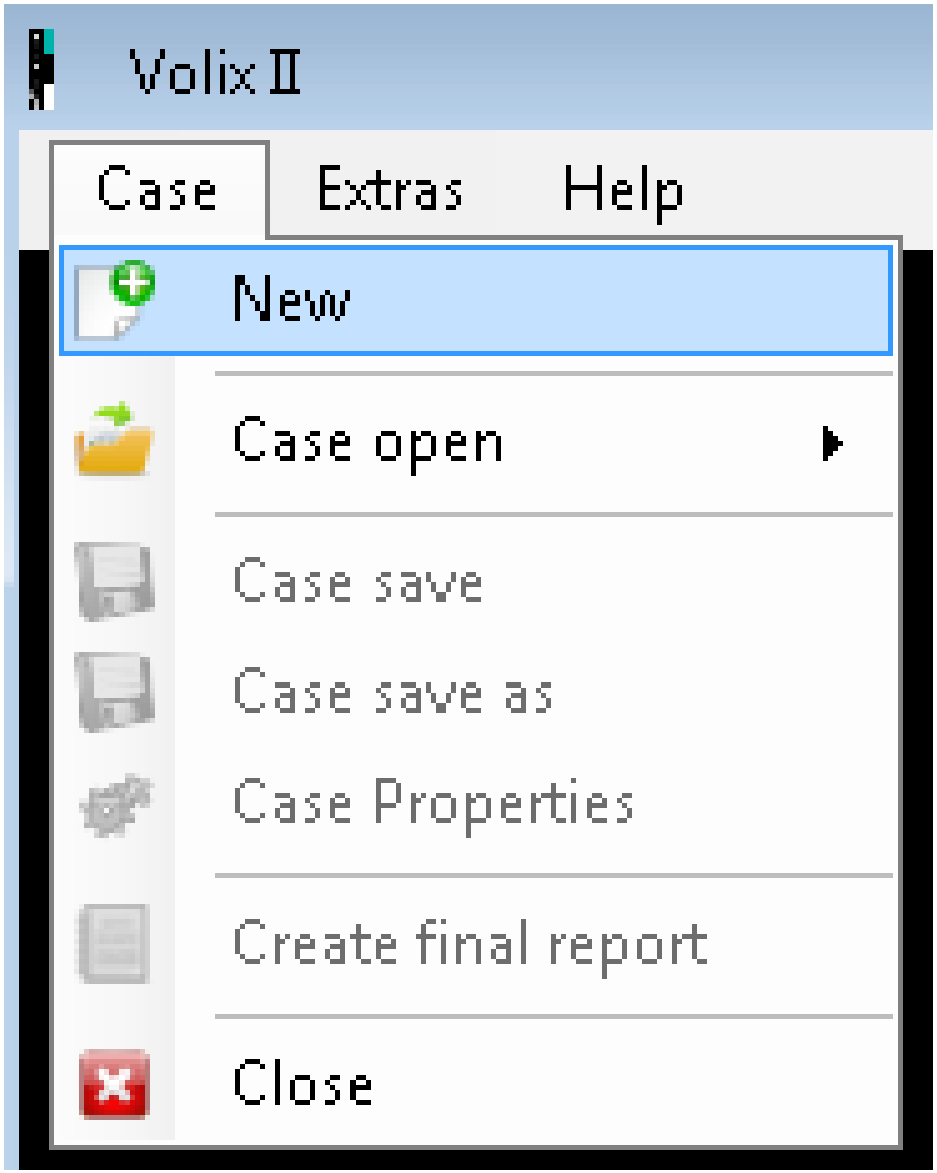
Contents

Case example

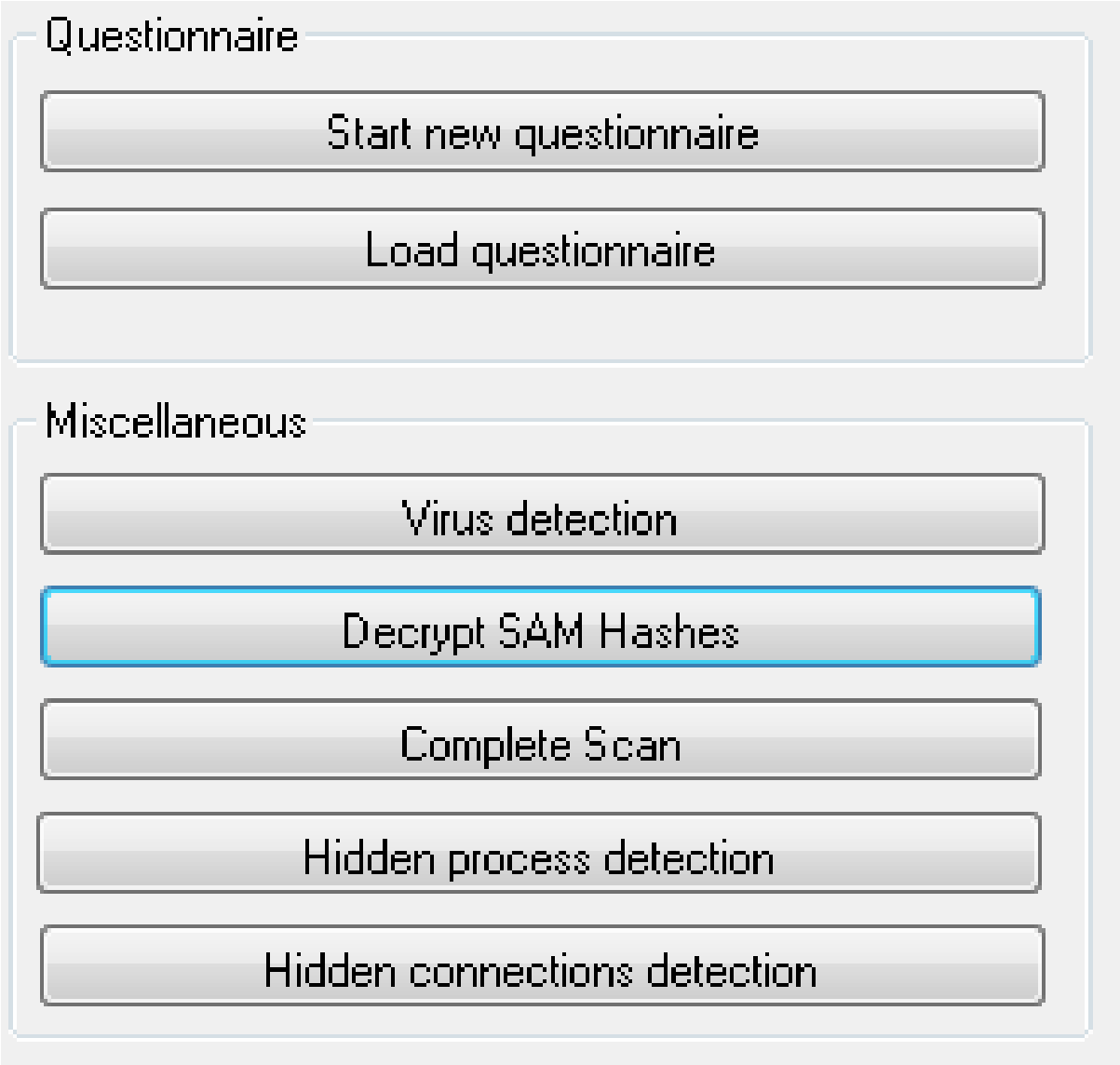
- Preparation
  - Create folder structure
  - Provide RAM image

  - Investigation_BlackEnergy
    - ResultDumps
    - Miscellanous

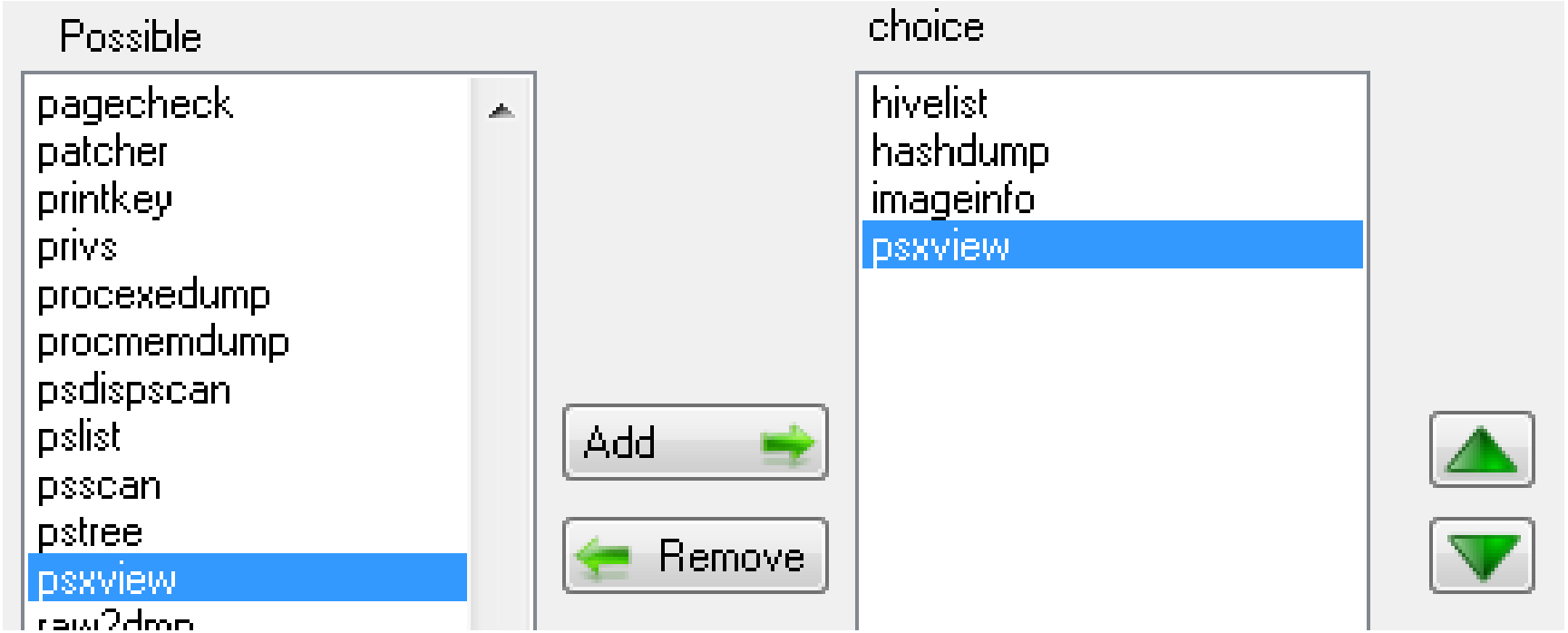
Case example



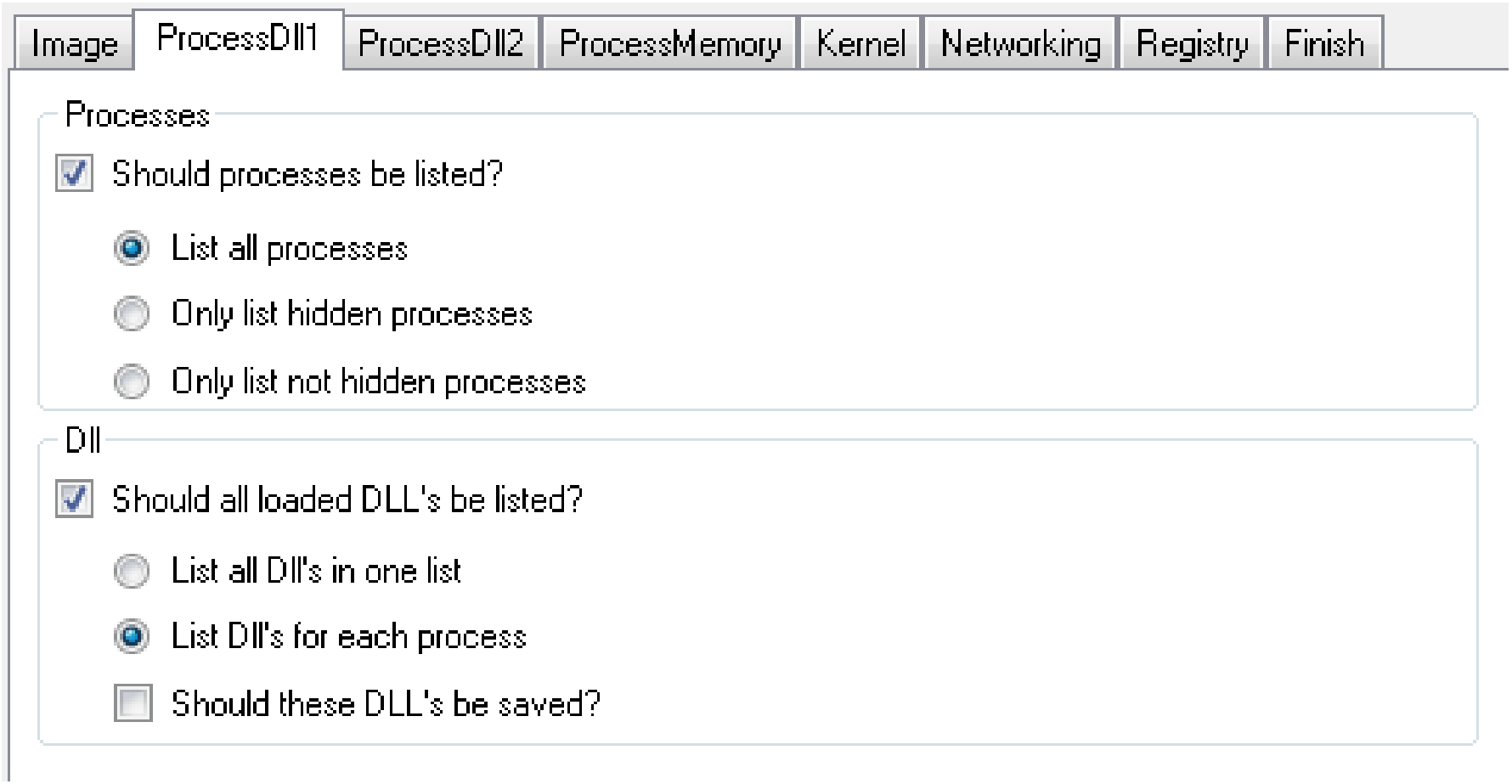
Case example



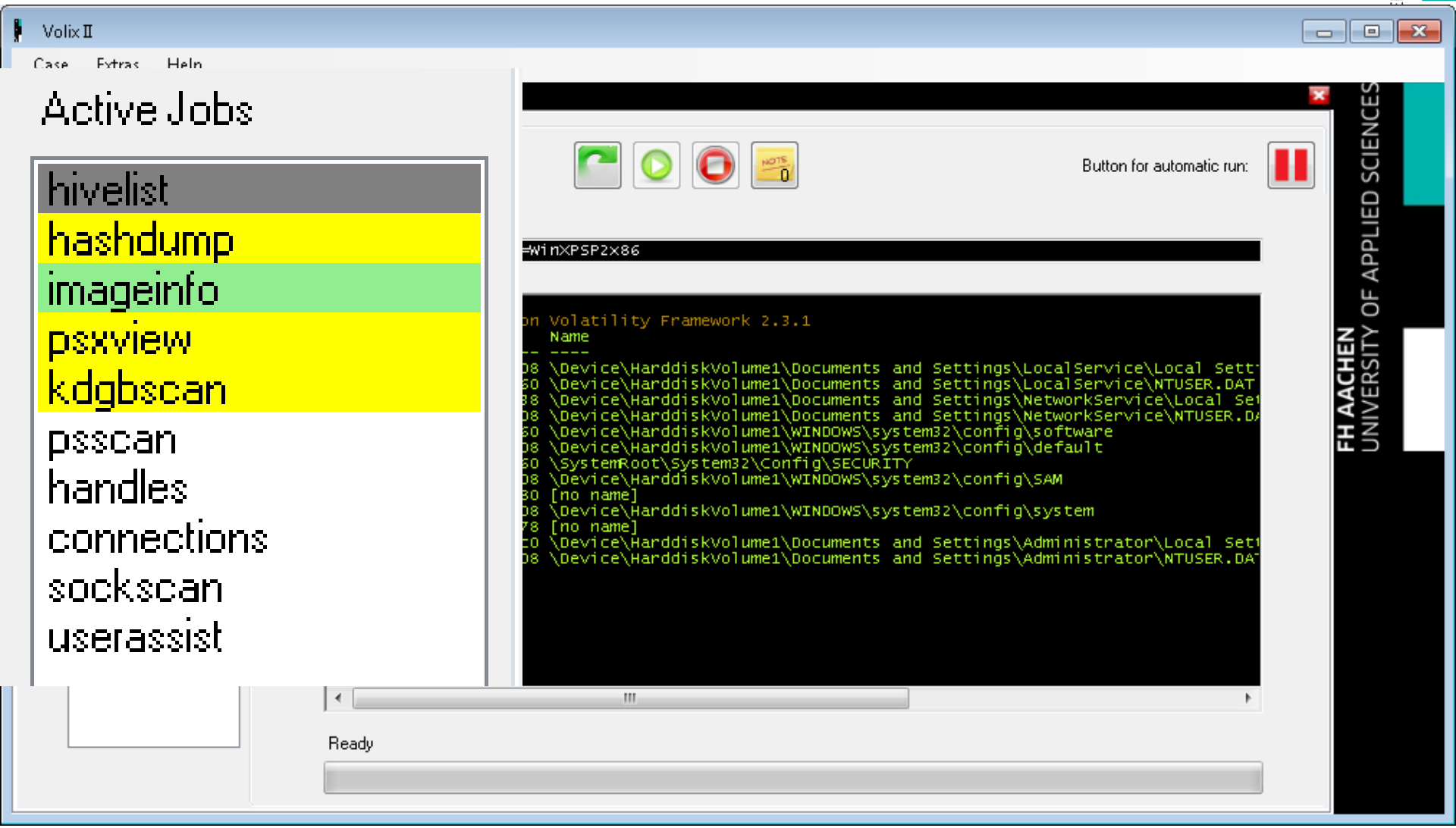
Case example



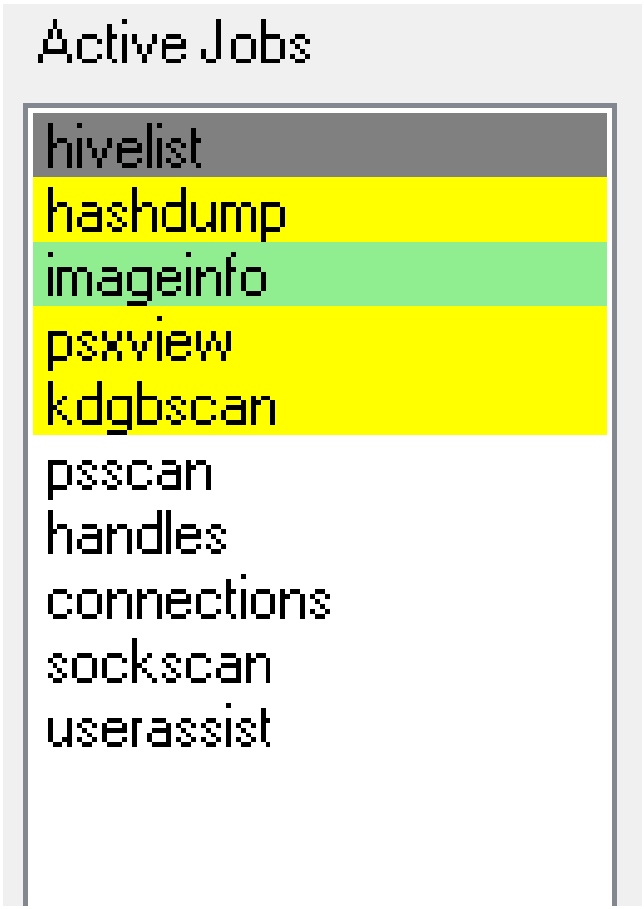
Case example



Case example



Case examp


Active Jobs
hivelist
hashdump
imageinfo
psxview
kdgbscan
psscan
handles
connections
sockscan
userassist


Active Jobs
hivelist
hashdump
imageinfo
psxview
kdgbscan
psscan
handles
connections
sockscan
userassist
dlllist


Active Jobs
hivelist
hashdump
imageinfo
psxview
kdgbscan
psscan
handles
connections
sockscan
userassist
dlllist

Case example

Final report of the forensic investigation of a memory image Created with Volix II

Generally

Investigator	Patrick Bock
Date	11.05.2014 21:04:27
Filename	C:\Untersuchungen\Untersuchung_BlackEnergy\be2.vmem\be2.vmem
Checksum	50D9866ADC908508C85517D2D1F55847EC52080B7244C13960A3EF9F4AA98C2A
Comment	This is vey useful information!

Case example

Joblist

Command	imageinfo

Result

```
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
```

Note	Date	Name	Text

Case example

Log entrys

Date	Text
11.05.2014 20:03:27	New case created
11.05.2014 20:03:37	hivelist added
11.05.2014 20:03:37	hashdump added
11.05.2014 20:03:37	imageinfo added
11.05.2014 20:11:10	---------- UTC: 11.05.2014 18:11:10 Plugin imageinfo
11.05.2014 20:28:21	Case closed
11.05.2014 20:29:54	Case loaded

Conclusion

Thank you for your attention

VOLIX II is available under

http://www.it-forensik.fh-aachen.de/projekte/volixe

Workshop

RAM-Image:

http://code.google.com/p/volatility/wiki/SampleMemoryImages

VirusTotal:

https://www.virustotal.com/de/