

Digital Forensics of RAM Images Using VOLIX II

Patrick Bock

FH Aachen, University of Applied Sciences



- Introduction
- Problems and Solutions
- Case example

- Introduction
- Problems and Solutions
- Case example

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

- Command line program
- Requires good knowledge of the commands

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

```

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 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

Variety

Possible

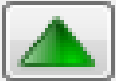
- apihooks
- atoms
- atomscan
- bioskbd
- callbacks
- clipboard
- cmdscan
- connections
- connscan
- consoles
- crashinfo
- desktop

Add 

 Remove

choice

- hivelist
- hashdump
- imageinfo**



Name

imageinfo

Description

.....

Module ImageInfo

.....

Identify information for the image

Command

imageinfo

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|
```

- Introduction
- Problems and Solutions
- Case example

- Problem
 - Volatility Framework 2.2 integrated
 - Current version 2.3.1 has much more commands

- Solution
 - Support version 2.3.1
 - Implement all commands

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

- Takes a long time

- 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

- Problem
 - User has to know the commands
 - Dependencies among commands

- Solution
 - Assistance in the form of Wizards
 - Questionnaire for the user

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

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

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

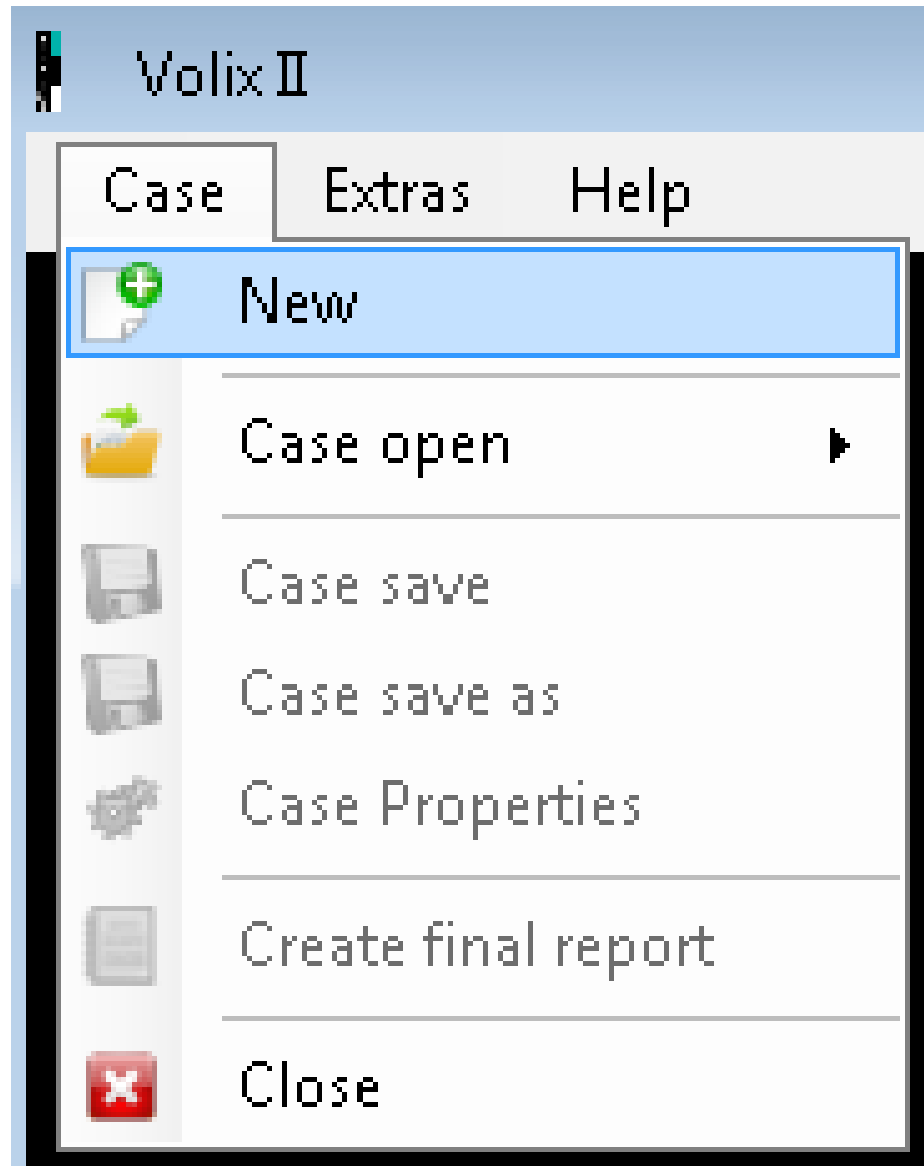
 - Individual dialog view for „hashdump“
 - Extract SAM hashes
 - Crack hashes with John the Ripper

- Introduction
- Problems and Solutions
- Case example

- Preparation
 - Create folder structure
 - Provide RAM image

- Investigation_BlackEnergy
 - ResultDumps
 - Miscellaneous

Case example



Case example

Questionnaire

Start new questionnaire

Load questionnaire

Miscellaneous

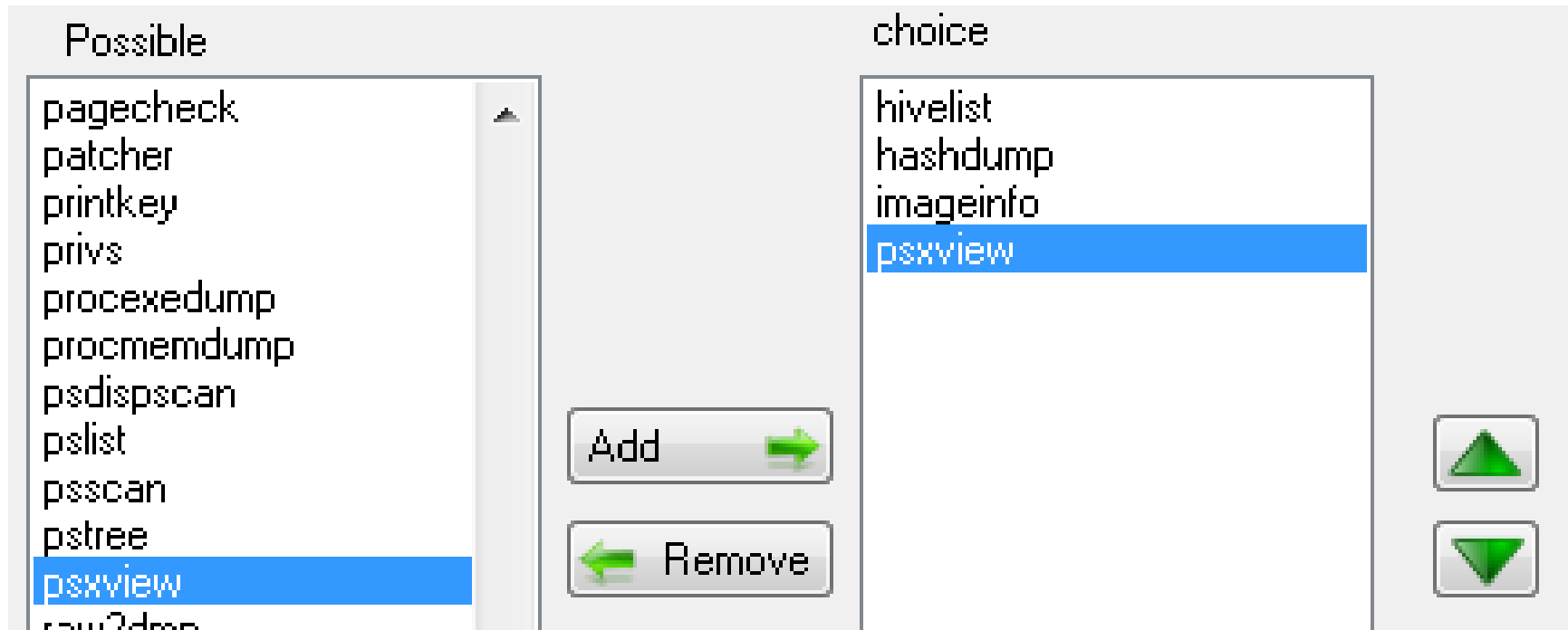
Virus detection

Decrypt SAM Hashes

Complete Scan

Hidden process detection

Hidden connections detection



The screenshot displays a software interface with two main panels: "Possible" and "choice".

- Possible:** A list of tools including pagecheck, patcher, printkey, privs, procexedump, procmemdump, p3disp3scan, p3list, p3scan, p3tree, psxview (highlighted in blue), and raw2dmp.
- choice:** A list of tools including hivelist, hashdump, imageinfo, and psxview (highlighted in blue).

Between the panels are two buttons: "Add" with a right-pointing green arrow and "Remove" with a left-pointing green arrow. To the right of the "choice" panel are two green arrow buttons, one pointing up and one pointing down.

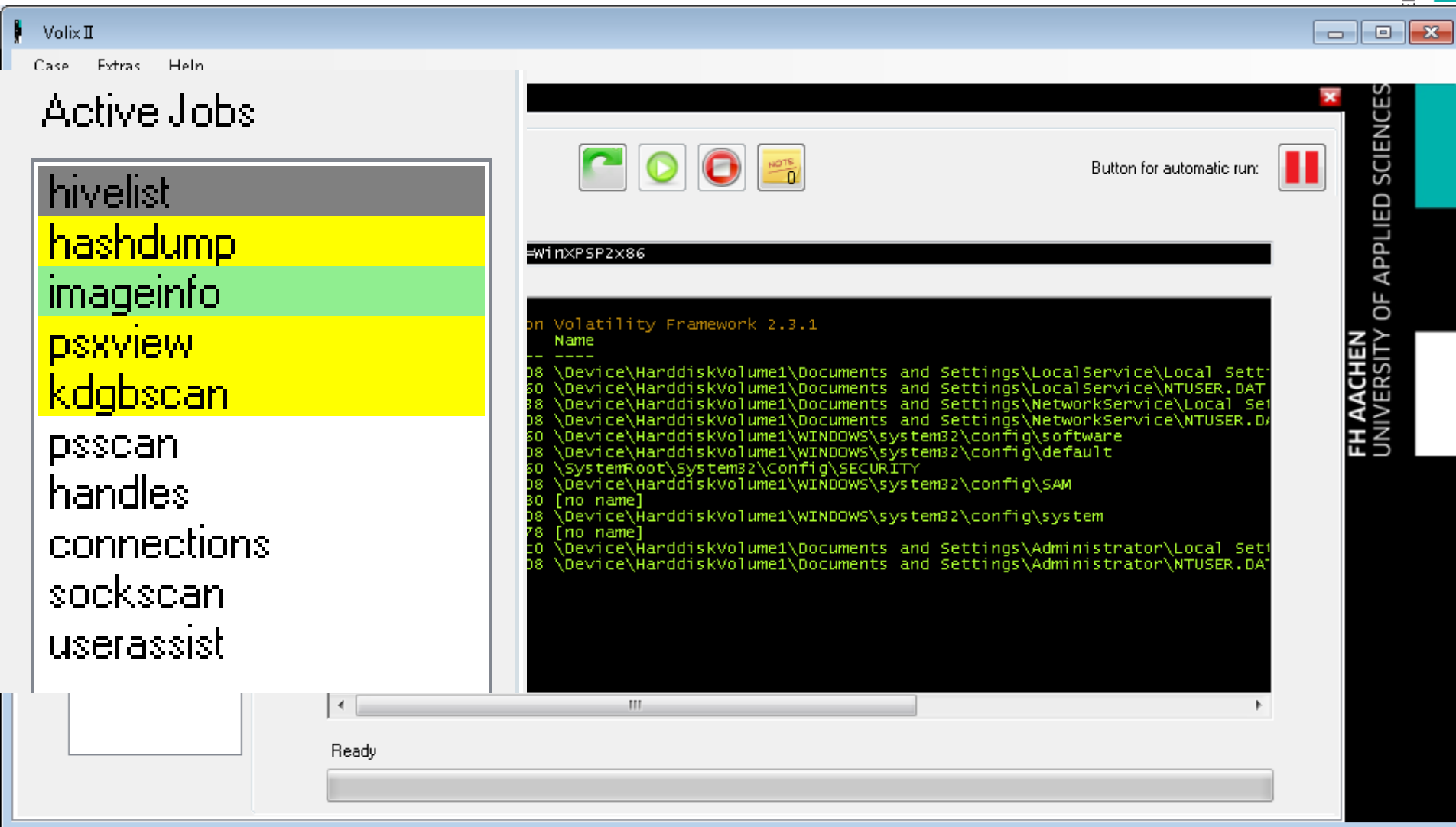
Image ProcessDll1 ProcessDll2 ProcessMemory Kernel Networking Registry Finish

Processes

- Should processes be listed?
 - List all processes
 - Only list hidden processes
 - Only list not hidden processes

Dll

- Should all loaded DLL's be listed?
 - List all Dll's in one list
 - List Dll's for each process
 - Should these DLL's be saved?



The screenshot shows the Volix II application window. On the left, the 'Active Jobs' panel lists several tools: hivelist, hashdump, imageinfo, psxview, kdgbscan, psscan, handles, connections, sockscan, and userassist. The main area displays a terminal window with the following output:

```

on Volatility Framework 2.3.1
Name
--
08 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Sett
60 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
88 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local sei
08 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.Da
60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
08 \Device\HarddiskVolume1\WINDOWS\system32\config\default
60 \SystemRoot\System32\Config\SECURITY
08 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
80 [no name]
08 \Device\HarddiskVolume1\WINDOWS\system32\config\system
78 [no name]
c0 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Sett
08 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
  
```

At the bottom of the terminal window, the status 'Ready' is visible.

Active Jobs

```

hivelist
hashdump
imageinfo
psxview
kdgbscan
psscan
handles
connections
sockscan
userassist
    
```

Active Jobs

```

hivelist
hashdump
imageinfo
psxview
kdgbscan
psscan
handles
connections
sockscan
userassist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
    
```

Active Jobs

```

hivelist
hashdump
imageinfo
psxview
kdgbscan
psscan
handles
connections
sockscan
userassist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
dllist
    
```

pages

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!

Joblist

Command	imageinfo		
Result	<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>		
Note	Date	Name	Text

Log entries

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

Thank you for your attention

VOLIX II is available under

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

RAM-Image:

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

VirusTotal:

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