

# GUI für Volatility (VOLIX)

Steffen Logen  
Lehrgebiet Datennetze



## 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

- 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

```

C:\Windows\system32\cmd.exe

C:\Vola>volatility.exe -f zeus.vmem --output-file=pslist.txt pslist
Volatile Systems Volatility Framework 2.0

C:\Vola>volatility.exe -f zeus.vmem procexedump -p 844 -D ./dump
Volatile Systems Volatility Framework 2.0
*****
Dumping unacthlp.exe, pid: 844 output: executable.844.exe

C:\Vola>volatility.exe -f zeus.vmem procexedump -p 856 -D ./dump
Volatile Systems Volatility Framework 2.0
*****
Dumping svchost.exe, pid: 856 output: executable.856.exe

C:\Vola>volatility.exe -f zeus.vmem procexedump -p 124 -D ./dump
Volatile Systems Volatility Framework 2.0
*****
Error: PEB not memory resident for process [124]

C:\Vola>volatility.exe -f zeus.vmem procexedump -p 468 -D ./dump
Volatile Systems Volatility Framework 2.0
*****
Dumping wuauclt.exe, pid: 468 output: executable.468.exe

C:\Vola>
    
```

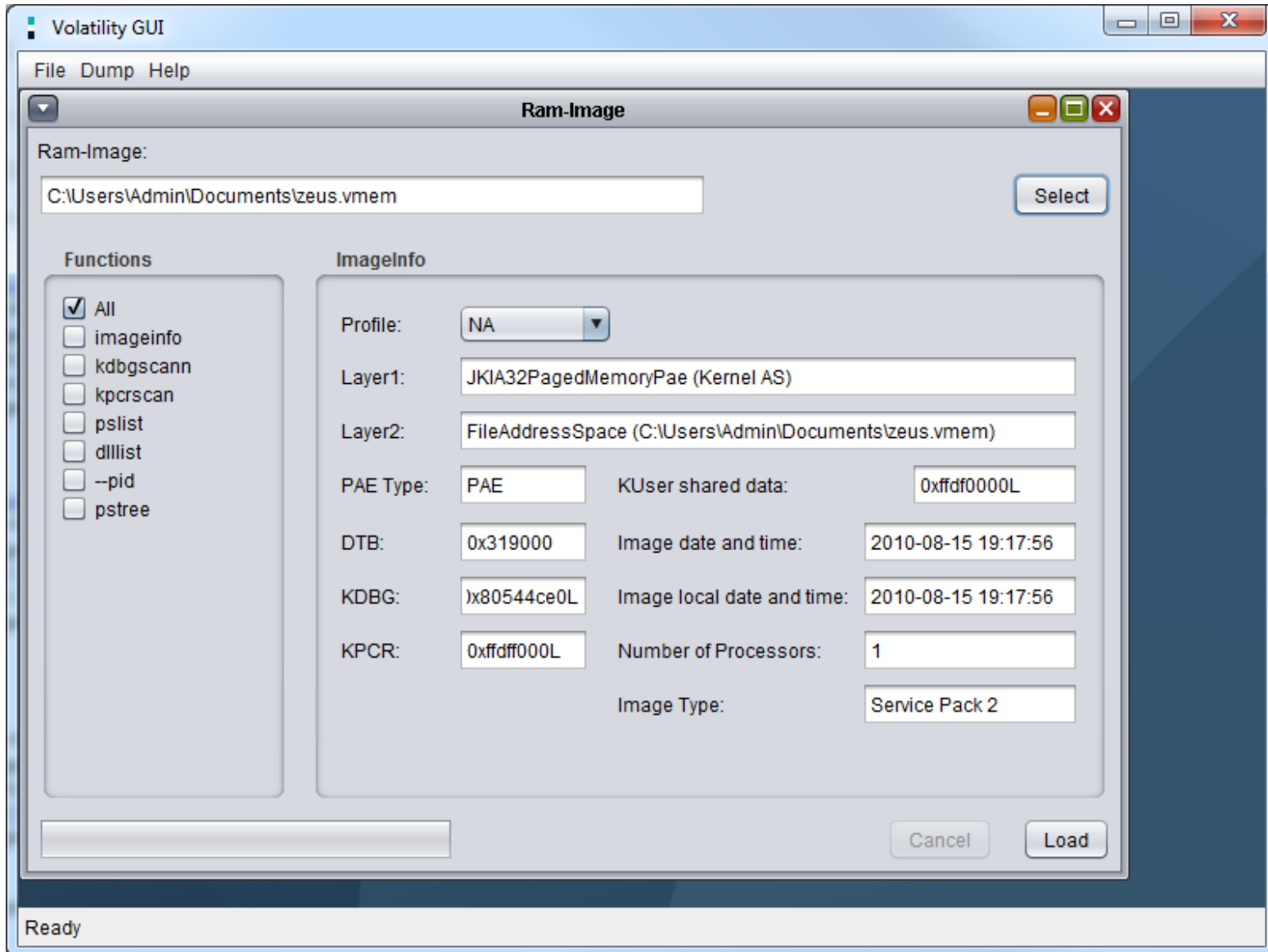
pslist.txt - Editor

Offset(V)	Name	PID	PPID	Thds	Hnds	Time
0x810b1660	System	4	0	58	379	1970-01-01 00:00:00
0xff2ab020	smss.exe	544	4	3	21	2010-08-11 06:06:21
0xff1ecd00	csrss.exe	608	544	10	410	2010-08-11 06:06:23
0xff1ec978	winlogon.exe	632	544	24	536	2010-08-11 06:06:23
0xff247020	services.exe	676	632	16	288	2010-08-11 06:06:24
0xff255020	lsass.exe	688	632	21	405	2010-08-11 06:06:24
0xff218230	vmaacthlp.exe	844	676	1	37	2010-08-11 06:06:24
0x80ff88d8	svchost.exe	856	676	29	336	2010-08-11 06:06:24
0xff217560	svchost.exe	936	676	11	288	2010-08-11 06:06:24
0x80fbf910	svchost.exe	1028	676	88	1424	2010-08-11 06:06:24
0xff22d558	svchost.exe	1088	676	7	93	2010-08-11 06:06:25
0xff203b80	svchost.exe	1148	676	15	217	2010-08-11 06:06:26
0xff1d7da0	spoolsv.exe	1432	676	14	145	2010-08-11 06:06:26
0xff1b8b28	vmtoolsd.exe	1668	676	5	225	2010-08-11 06:06:35
0xff1fd0c8	VMUpgradeHelper	1788	676	5	112	2010-08-11 06:06:38
0xff143b28	TPAutoConnSvc.exe	1968	676	5	106	2010-08-11 06:06:39
0xff25a7e0	alg.exe	216	676	8	120	2010-08-11 06:06:39
0xff364310	wsentfy.exe	888	1028	1	40	2010-08-11 06:06:49
0xff38b5f8	TPAutoConnect.exe	1084	1968	1	68	2010-08-11 06:06:52
0x80f60da0	wuauclt.exe	1732	1028	7	189	2010-08-11 06:07:44
0xff3865d0	explorer.exe	1724	1708	13	326	2010-08-11 06:09:29
0xff3667e8	VMwareTray.exe	432	1724	1	60	2010-08-11 06:09:31
0xff374980	VMwareUser.exe	452	1724	8	207	2010-08-11 06:09:32
0x80f94588	wuauclt.exe	468	1028	4	142	2010-08-11 06:09:37
0xff224020	cmd.exe	124	1668	0	-----	2010-08-15 19:17:55

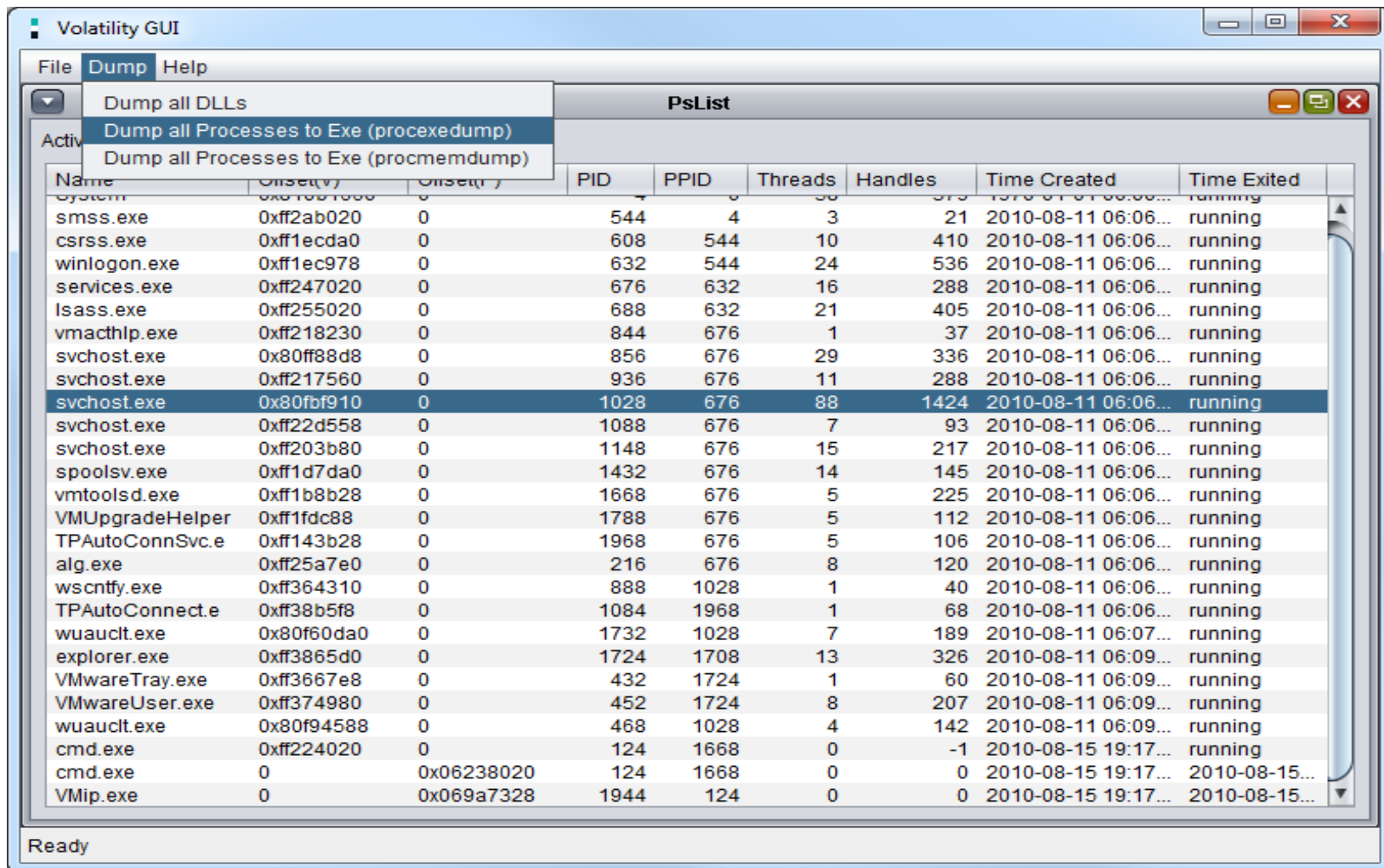
## Ziele der GUI

- 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)

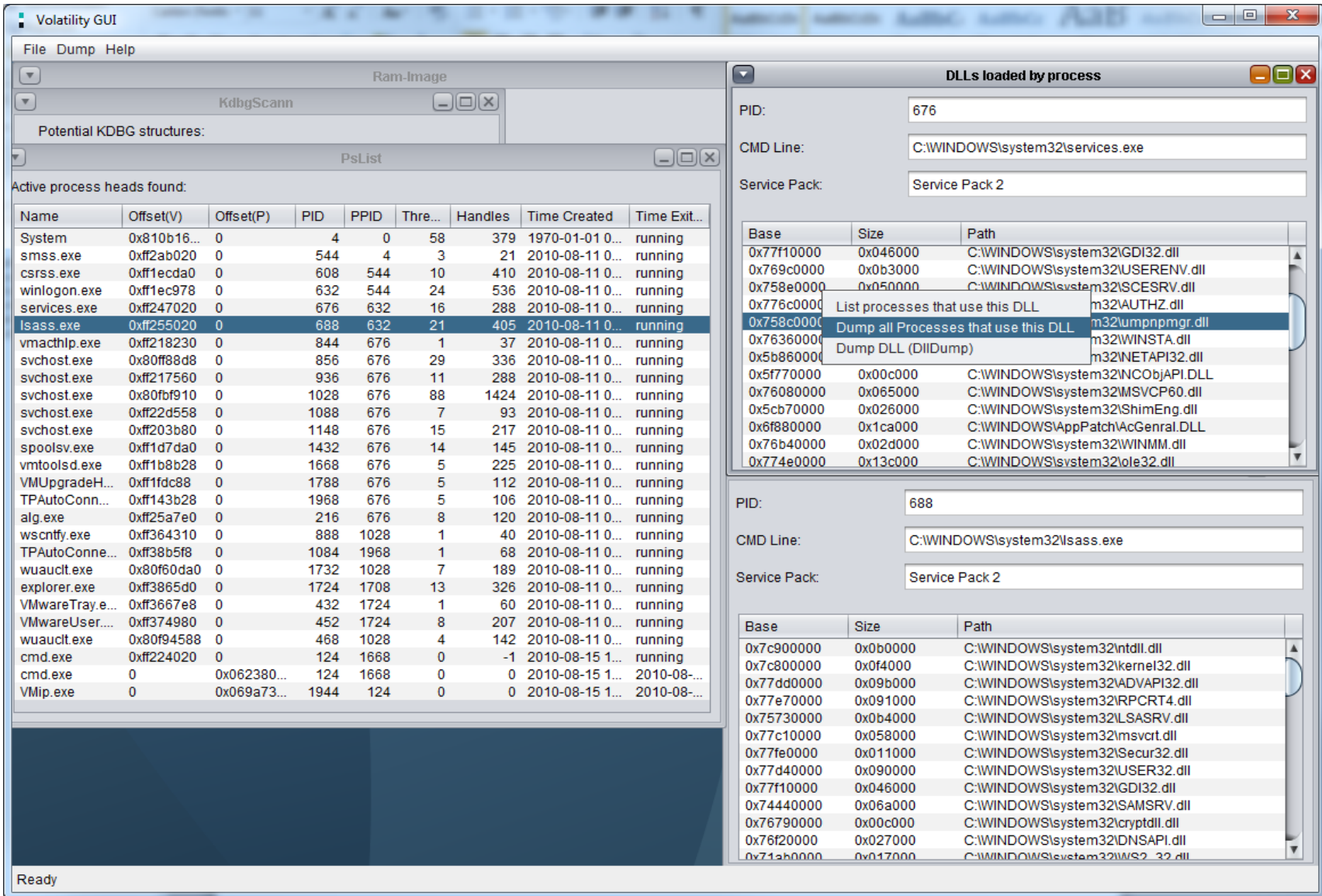
# Volatility GUI (VOLIX)



- Einfaches Dumpen aller Prozesse im Image über einen Klick



# Volatility GUI (VOLIX)



The screenshot displays the Volatility GUI interface. The main window is titled "Volatility GUI" and contains several panes:

- File Dump Help**: A menu bar at the top left.
- Ram-Image**: A pane for loading memory images, currently showing "KdbgScann".
- Potential KDBG structures:**: A pane for selecting kernel debugging structures.
- PsList**: A pane showing a list of active processes. The "Active process heads found:" section contains a table with columns: Name, Offset(V), Offset(P), PID, PPID, Thre..., Handles, Time Created, and Time Exit... The process "lsass.exe" is highlighted.
- DLLs loaded by process**: A pane showing details for a selected process. It includes fields for PID, CMD Line, and Service Pack. Below these is a table of loaded DLLs with columns: Base, Size, and Path. A context menu is open over the entry "m32lumpnpmgr.dll", with options: "List processes that use this DLL", "Dump all Processes that use this DLL", and "Dump DLL (DllDump)".

The "Active process heads found:" table is as follows:

Name	Offset(V)	Offset(P)	PID	PPID	Thre...	Handles	Time Created	Time Exit...
System	0x810b16...	0	4	0	58	379	1970-01-01 0...	running
smss.exe	0xff2ab020	0	544	4	3	21	2010-08-11 0...	running
csrss.exe	0xff1ecdad	0	608	544	10	410	2010-08-11 0...	running
winlogon.exe	0xff1ec978	0	632	544	24	536	2010-08-11 0...	running
services.exe	0xff247020	0	676	632	16	288	2010-08-11 0...	running
lsass.exe	0xff255020	0	688	632	21	405	2010-08-11 0...	running
vmacthlp.exe	0xff218230	0	844	676	1	37	2010-08-11 0...	running
svchost.exe	0x80ff88d8	0	856	676	29	336	2010-08-11 0...	running
svchost.exe	0xff217560	0	936	676	11	288	2010-08-11 0...	running
svchost.exe	0x80fb910	0	1028	676	88	1424	2010-08-11 0...	running
svchost.exe	0xff22d558	0	1088	676	7	93	2010-08-11 0...	running
svchost.exe	0xff203b80	0	1148	676	15	217	2010-08-11 0...	running
spoolsv.exe	0xff1d7da0	0	1432	676	14	145	2010-08-11 0...	running
vmtoolsd.exe	0xff1b8b28	0	1668	676	5	225	2010-08-11 0...	running
VMUpgradeH...	0xff1fdc88	0	1788	676	5	112	2010-08-11 0...	running
TPAutoConn...	0xff143b28	0	1968	676	5	106	2010-08-11 0...	running
alg.exe	0xff25a7e0	0	216	676	8	120	2010-08-11 0...	running
wscntfy.exe	0xff364310	0	888	1028	1	40	2010-08-11 0...	running
TPAutoConne...	0xff38b5f8	0	1084	1968	1	68	2010-08-11 0...	running
wuauclt.exe	0x80f60da0	0	1732	1028	7	189	2010-08-11 0...	running
explorer.exe	0xff3865d0	0	1724	1708	13	326	2010-08-11 0...	running
VMwareTray.e...	0xff3667e8	0	432	1724	1	60	2010-08-11 0...	running
VMwareUser....	0xff374980	0	452	1724	8	207	2010-08-11 0...	running
wuauclt.exe	0x80f94588	0	468	1028	4	142	2010-08-11 0...	running
cmd.exe	0xff224020	0	124	1668	0	-1	2010-08-15 1...	running
cmd.exe	0	0x062380...	124	1668	0	0	2010-08-15 1...	2010-08-...
VMip.exe	0	0x069a73...	1944	124	0	0	2010-08-15 1...	2010-08-...

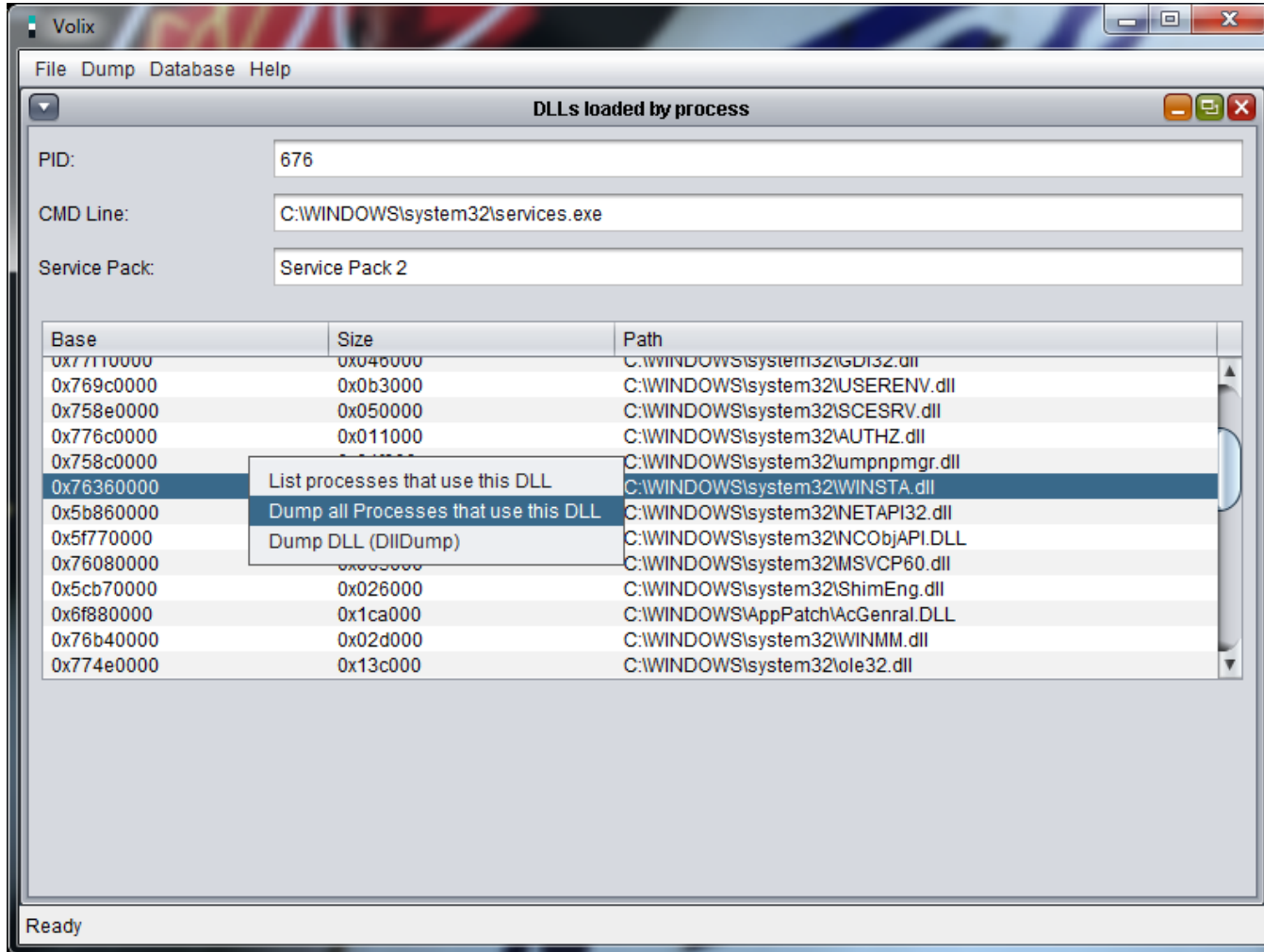
The "Dumps loaded by process" pane shows details for PID 676 (services.exe) and PID 688 (lsass.exe). The DLLs loaded by process 676 include:

Base	Size	Path
0x77f10000	0x046000	C:\WINDOWS\system32\GDI32.dll
0x769c0000	0x0b3000	C:\WINDOWS\system32\USERENV.dll
0x758e0000	0x050000	C:\WINDOWS\system32\SCESRV.dll
0x776c0000		m32\AUTHZ.dll
0x758c0000		m32\lumpnpmgr.dll
0x76360000		m32\WINSTA.dll
0x5b860000		m32\NETAPI32.dll
0x5f770000	0x00c000	C:\WINDOWS\system32\NCOBJAPI.DLL
0x76080000	0x065000	C:\WINDOWS\system32\MSVCP60.dll
0x5cb70000	0x026000	C:\WINDOWS\system32\ShimEng.dll
0x6f880000	0x1ca000	C:\WINDOWS\AppPatch\AcGenral.DLL
0x76b40000	0x02d000	C:\WINDOWS\system32\WINMM.dll
0x774e0000	0x13c000	C:\WINDOWS\system32\ole32.dll

The DLLs loaded by process 688 include:

Base	Size	Path
0x7c900000	0x0b0000	C:\WINDOWS\system32\ntdll.dll
0x7c800000	0x0f4000	C:\WINDOWS\system32\kernel32.dll
0x77dd0000	0x09b000	C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000	0x091000	C:\WINDOWS\system32\RPCRT4.dll
0x75730000	0x0b4000	C:\WINDOWS\system32\SASRV.dll
0x77c10000	0x058000	C:\WINDOWS\system32\msvcr7.dll
0x77fe0000	0x011000	C:\WINDOWS\system32\Secur32.dll
0x77d40000	0x090000	C:\WINDOWS\system32\USER32.dll
0x77f10000	0x046000	C:\WINDOWS\system32\GDI32.dll
0x74440000	0x06a000	C:\WINDOWS\system32\SAMSRV.dll
0x76790000	0x00c000	C:\WINDOWS\system32\cryptdll.dll
0x76f20000	0x027000	C:\WINDOWS\system32\DNSAPI.dll
0x712b0000	0x017000	C:\WINDOWS\system32\WS2_32.dll

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





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?

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



The screenshot shows the website's main menu on the left and a project banner on the right. The menu is titled 'HAUPTMENÜ' and lists the following items: Startseite, Veranstaltungen, **Projekte** (with sub-items DIRECT and VOLIX), Archiv, Pressemeldungen, Kontakt, and Impressum. The banner features a background image of a server rack with glowing blue lines. In the foreground of the banner is a green circuit board with four black chips, labeled 'VOLIX'. Below the board, the text 'Volatility Interface & Extension' is displayed in orange and black.

# Danke für Ihre Aufmerksamkeit!