Responding to the Digital Crime Scene: Gathering Volatile Data

Inno Eroraha, CISSP, CISM, CISA, CHFI, PI
Founder & Chief Strategist
NetSecurity Corporation

October 29, 2008

netSecurity Forensic Labs

netSecurity

Presentation Objectives

- To discuss the potential value of volatile data in digital investigations
- To discuss challenges in live evidence collection
- To suggest practices for collecting volatile data that can withstand legal scrutiny
- To demonstrate how-to conduct a “live investigation” on “Dicck Maxxwell,” a user suspected of a cyber crime

Live Volatile Data

- Forensics artifacts in a state of flux that can be lost when power (or network connections, in some cases) has been removed from a computing device
- Live evidence collection can mean the difference between:
  - Winning or losing a case
  - Solving or not solving a crime
  - Life or death sentence!
  - Guilt or innocence

Reasons to Collect Volatile Data

- May help determine criminal activity that can get lost if the system is powered off
- May contain passwords used for encryption
- May show indication of anti-forensic use
- May show memory resident malware which could go unnoticed by an examiner
- Can help avoid backlog of cases – performing live data collection avoids waiting for months for a full-blown investigation

Reasons to Collect Volatile Data (Cont'd.)

- Critical systems cannot be shut down and require 24x7 operation to satisfy SLA or other business requirements
- Shutting down a system may create legal liability for examiners due to damage to equipment or unintentional loss of data
- Courts request that evidence gathering be conducted using the least intrusive methods available

Forensic Soundness

- In practice, live data collection will alter evidence to some degree
  - In real-world, collection of blood splatter from a traditional crime scene alters DNA analysis
  - The goal of volatile data collection is to substantially minimize the footprint of collection tasks
- Changes to system during live data collection must be properly documented, explained, and justified, including:
  - Registry changes
  - Memory entries
  - Other changes to the system

"What is an Incident Responder to do?"

Admissibility of Volatile Data: Case Laws

- Columbia Pictures Indus. v. Bunnell (2007 U.S. Dist. LEXIS 46364 [C.D. Cal. June 19, 2007]):
  - Court held that RAM on a web server could contain relevant log data
- E-Discovery cases, where a critical server cannot be taken offline or shutdown for deep forensics analysis

Question: Are there other case laws relating to volatile data rulings? Send info to Inno@NetSecurity.com

Applicable Laws

- Know applicable local, state, and Federal laws regarding the investigation
- Some U.S. states now require that only Private Investors (PIs) are legally allowed to collect digital data and conduct forensics investigations – be sure you are abiding by these laws

Live Data Collection Challenges

- Lack of incident response capabilities or forensics readiness plan
- Untrained live data collectors
- Untested toolkits
- Untested or lack of established processes and procedures

Order of Volatility of Evidence

- Registers, cache, and peripheral memory
- Main/Physical memory
  - Microsoft Windows: \\.\PhysicalMemory
  - Unix, OS X: /dev/mem, /var/vm
  - Linux: /proc/kcore
- Virtual memory
  - Microsoft Windows: pagefile.sys, hiberfil.sys
  - Unix, Linux, OS X: swap file
- Network State
- Running processes
- Disk
- Floppies, backup media, etc.
- Archival media, including: CD-ROMs, USB drives, etc.

Sources of Volatile Data

- Random Access Memory (RAM)
- Operating System (OS)
- Network traffic captured with sniffer
- Network device logs
- “Micro” Devices (handheld, PDA, cell phones, etc.)

Volatile Data in RAM

- Data files
- Password hashes or in plain text
- Recent commands
- Residual data in slack and free space
- Running processes
- Unencrypted data
- Internet Protocol (IP) addresses
- Instant Messages (IMs)
- Malicious Software (“malware”)
- Anti-forensics tools
- Other evidentiary artifacts

Volatile Data in OS

- Windows Registry (volatile Keys/HIVEs)
- Network Configurations
  - not stored configuration since these can be altered
- Network Connections
- Running Processes
- Virtual Memory
- Open Files

Volatile Data in OS (Cont'd.)

- Login Sessions (available if a system has been configured with auditing turned on for logon attempts enabled
  - Currently logged-in users, including start and duration of each session
  - Previous successful and unsuccessful logons
  - Privileged usage
- Log files
- System time
- Password files (/etc/passwd, SAM, etc.)
- Windows Prefetch directory (may indicate recent files that have been executed on a system)

Volatile Data in Network Traffic

- Wired traffic capture
- Wireless traffic capture

Volatile Data in Network Device Logs

- Centralized storage logs
- Router logs
- Firewall logs

Volatile Data in “Micro” Devices

- PDA, Cell phone, and mobile devices contain volatile data
- “Micro” computing devices have their own live volatile data collection issues, such as constant communication – reception or transmission
- Challenges in evidence collection exist
  - Power and data cables may be difficult to obtain
  - Inadequate forensics tools to satisfy the multitude of mobile devices in (and off) the market

Shutdown System or Pull the Plug?

What about Hibernation mode?

Penalty for Shutting Down System – What You Lose

- Closing of open files
- Deletion of temporary files
- Erasure of the swap file (if a certain Windows registry key is set)
- Removal/disappearance of malicious material
  - Memory-resident rootkits
  - Trojan horses, rootkits, or malware may remove evidence of their malicious activity

Penalty for Pulling the Power Plug – What You Loose

- Removal/disappearance of malicious material
  - Memory-resident rootkits
  - Trojan horses may remove evidence of their malicious activity
- Preservation of swap files
- Preservation of temporary files
- Preservation of other information that might be altered or deleted during a graceful shutdown
- Possible corruption of OS data, such as open files
- Data loss in devices such as PDAs and cell phones when battery power is removed

Hibernation Mode

- Hibernation saves the state of an operating system (including the content of RAM) to a non-volatile storage file or partition before powering off the system
- The system is later restored to the state it was in when hibernation was invoked so that programs can continue executing as if nothing happened
- Modern OS support hibernation mode
  - Microsoft Windows 2000, XP, and 2003 (file is called “hiberfil.sys”)
  - MAC OS X v10.4 and later
  - Linux kernel 2.4, 2.6
- A forensics investigator can analyze the hibernation file to recover the image of physical memory and reveal potential evidence
- Some memory-resident rootkits could potentially intercept the instruction to begin the hibernation process and hide before allowing hibernation to begin
  - These rootkits would leave some trace (“hook”) in memory – these can be evidentiary data

Collecting Artifacts from a System in Hibernation Mode

- Carefully remove the drive from a system in hibernation mode
- Collect relevant information by:
  - Imaging the entire (or portion of) drive in a forensically sound manner
  - Copying relevant files that might contain volatile data, such as:
    - Hiberfil.sys
    - Pagefile.sys
    - Registry files
    - Password Files (SAM in Windows, /etc/passwd, /etc/shadow in Unix)
    - Temporary files
    - Internet History

Live Data Collection Challenges

- Every action or inaction performed on the system – whether initiated by a person or by the OS itself – will alter the volatile OS data in some way
- Shutting down or disconnecting the system from the network may alter evidence that may be relevant to a case
- Malicious software, rootkits, or booby traps may alter outcome of information collected
- Kernel-level rootkits and malware can alter user-level tools
- Command time-stamping – helps to answer the questions: which commands were run, at what time, and with what output

Procedural Steps for Volatile Data Collection

- "Live" forensics should be seriously considered, especially if:
  - There is volatile data of value
  - Suspect is using machine at time of seizure or attack is in progress
  - Shutting down may cause data to be unusable (i.e., drive encryption, running processes, network connections, etc.)
- Never image a system using subjects machine to avoid evidence contamination, unless imaging can't be avoided
- Record cryptographic hashes
- Create verbose notes of actions taken

Pros and Cons of Commercial Tools

- Advantages
  - Pretty GUI
  - Vendor support
- Disadvantages
  - May cost too much – all organizational assets may not be covered, and ones covered may never experience an incident!
  - Agent/software may need to be installed on a system prior to an incident
  - Some OSs may not be supported by commercial tools (Example: Linux, Windows 95, Windows NT, etc.)

Creating Forensics Toolkits

- Create toolkits with trusted binaries on CD, USB, or floppy
- Automate a script on a toolkit CD to ensure consistency in collecting volatile data – Forensic Server Project is a great toolkit in Windows
- Toolkit should have ability to transmit collected information to a remote system, with the data authenticated

Which Data to Collect When?

- Rule of Thumb – Collect as much information as possible that would leave the least amount of footprint
- Evidence might be missed if not completely collected

Order of Volatile Data Collection

- CPU Registers, cache, and peripheral memory
- Contents of physical memory
- Network connections
- Login sessions
- Running processes
- Open files
- Network configuration
- Operating system time

Live Data Collection Process

“The Process...” according to CERT

- Collect uptime, date, time, and command history for the security incident
- As you execute each forensic tool or command, generate the date and time to establish an audit trail
- Begin a command history that will document all forensic collection activities
- Collect all types of volatile system and network information
- End the forensic collection with date, time, and command history

CERT Reference: *First Responders Guide to Computer Forensics*

Suggested Steps for Volatile Evidence Collection

- Maintain a log of all actions conducted on a running machine
- Photograph the screen of the running system to document its state
- Identify the operating system running on the suspect machine
- Note date and time, if shown on screen, and record with the current actual time
- Dump the system RAM to a removable storage device or a remote system
- Check the system for the use of whole disk or file encryption
- Collect other volatile operating system data and save to a removable storage device or a remote system
- Determine evidence seizure method (of hardware and any additional artifacts on the hard drive that may be determined to be of evidentiary value)
- Complete a full report documenting all steps and actions taken

Source: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RunningComputer.pdf

Live Volatile Data Collection Scenario for “Dicck Maxxwell”

netSecurity Forensic Labs

netSecurity

The Scenario

A crime has been committed. The computer used has been identified and is still up and running. The user ("suspect"), "Dicck Maxxwell," is claiming that a malware on the system must have downloaded the illicit pornography onto his computer on his behalf. You have been recruited as the forensics czar to conduct this high-profile investigation involving Mr. Maxxwell. Dicck is still sitting at his computer when the investigators show up at the doorstep. What steps would you take to find reasonable evidence for the defense or prosecuting attorneys?

The above scenario is too common today. First responders typically report to the crime scene, faced with the "dilemma" to shutdown or not to shutdown the suspect's system Take one action or the other and it may be a "do or die" for the suspect. The remainder of this presentation walks through the practices discussed previously and the steps that a first responder can execute to produce necessary forensics artifacts associated with common operating systems.

Defendant's Scenario

- Suspect: "Dicck Maxxwell" (fictitious), Human, 42 years old, sales executive, working for a multi-billion dollar oil company
- Accused of:
  - Unproductive work habits
  - Illicit photos/activities spotted on screen and network
- Dicck's Claim: Malware must have downloaded illicit photos on his system

The Crime Scene

- A “corrupt” CD on Dicck’s desk
- A company-issued Blackberry device
- A Dell PC running Redhat Linux
- A Compaq laptop running Windows XP

Our Forensics Assignment

Collect forensics evidence from a suspect machine that is still up and running

netSecurity Forensic Labs

netSecurity

The Environment

- Suspect System: the system from which forensic evidence is sought
  - Compaq laptop, running Windows XP
  - Dell desktop, running Redhat Linux
- Forensic System: the system on which you will be performing your forensic analysis
  - Windows XP
- Volatile Data: information that is lost when the system is powered off
  - Collected from suspect systems

Network Traffic Capture

- Continue ongoing monitoring
- Capture user network traffic using Wireshark

Analyze Network Traffic

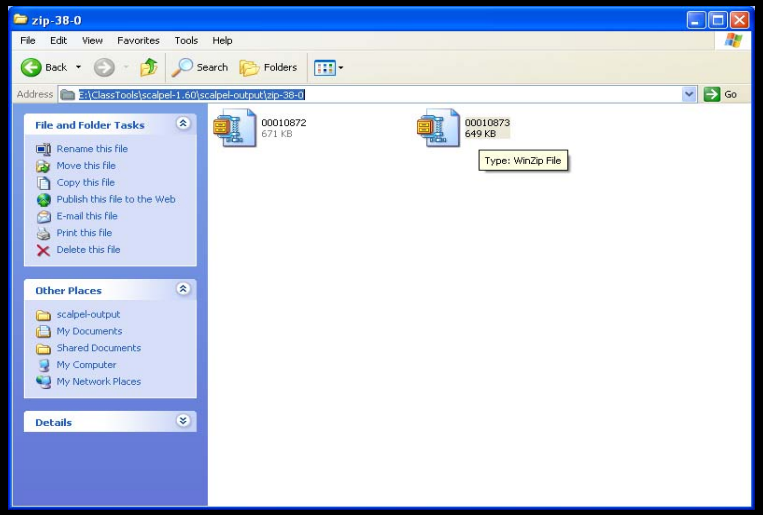
- Analysis performed after all volatile data has been collected
- Tool used is Scalpel – a data carving utility
- Command line:
  - `scalpel –i Wireshark-Traffic-Capture-DicckMaxxwell-TechnoForensics.pcap –o ScalpelOutput -t ScalpelCoverageMap -c scalpel-netsecurity.txt`

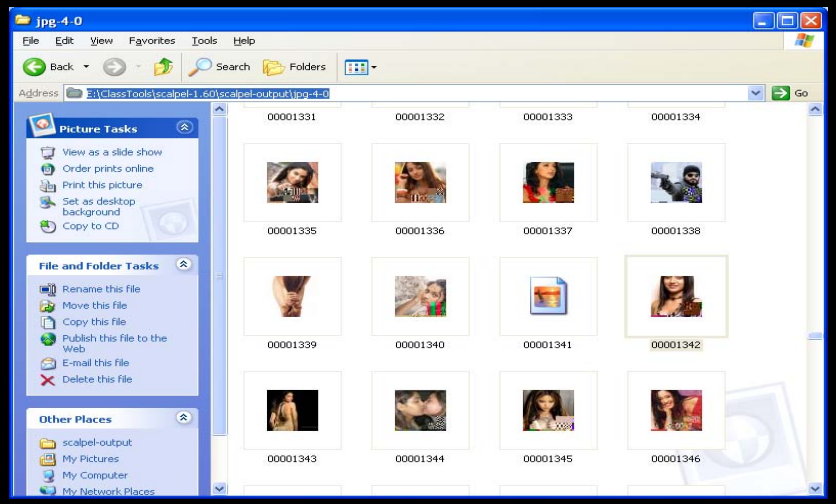
Scalpel in Action…

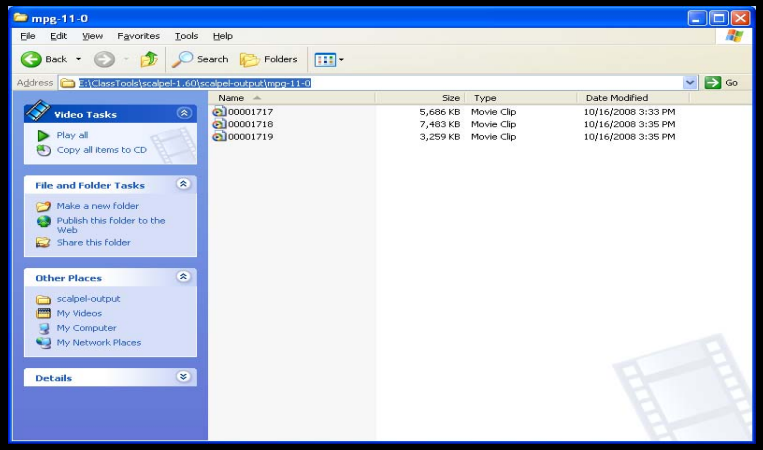
C:\WINDOWS\system32\cmd.exe - scalpel -i Wireshark-Traffic-Capture-DicckMaxxwell-Tech…

```
E:\ClassTools\scalpel-1.60>scalpel -i Wireshark-Traffic-Capture-DicckMaxxwell-Te
chnoForensics.pcap -o ScalpelOutput -t ScalpelCoverageMap -c scalpel-netsecurity
.txt
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "E:\ClassTools\scalpel-1.60\ûi"

ERROR: Couldn't open input file: ûi -- No such file or directory
Scalpel was unable to open the image file: ûi
Skipping...


Opening target "E:\ClassTools\scalpel-1.60\Wireshark-Traffic-Capture-DicckMaxxwe
ll-TechnoForensics.pcap"

Image file pass 1/2.
Wireshark-Traffic-Capture-DicckMaxxwell-TechnoForensics.pcap:  12.1%    10.0 MB
Wireshark-Traffic-Capture-DicckMaxxwell-TechnoForensics.pcap:  24.1%    20.0 MB
Wireshark-Traffic-Capture-DicckMaxxwell-TechnoForensics.pcap:  36.2%    30.0 MB
Wireshark-Traffic-Capture-DicckMaxxwell-TechnoForensics.pcap:  48.3%    40.0 MB
Wireshark-Traffic-Capture-DicckMaxxwell-TechnoForensics.pcap:  60.3%    50.0 MB
Wireshark-Traffic-Capture-DicckMaxxwell-TechnoForensics.pcap:  72.4%    60.0 MB
Wireshark-Traffic-Capture-DicckMaxxwell-TechnoForensics.pcap:  84.5%    70.0 MB
```

Scalpel's Results



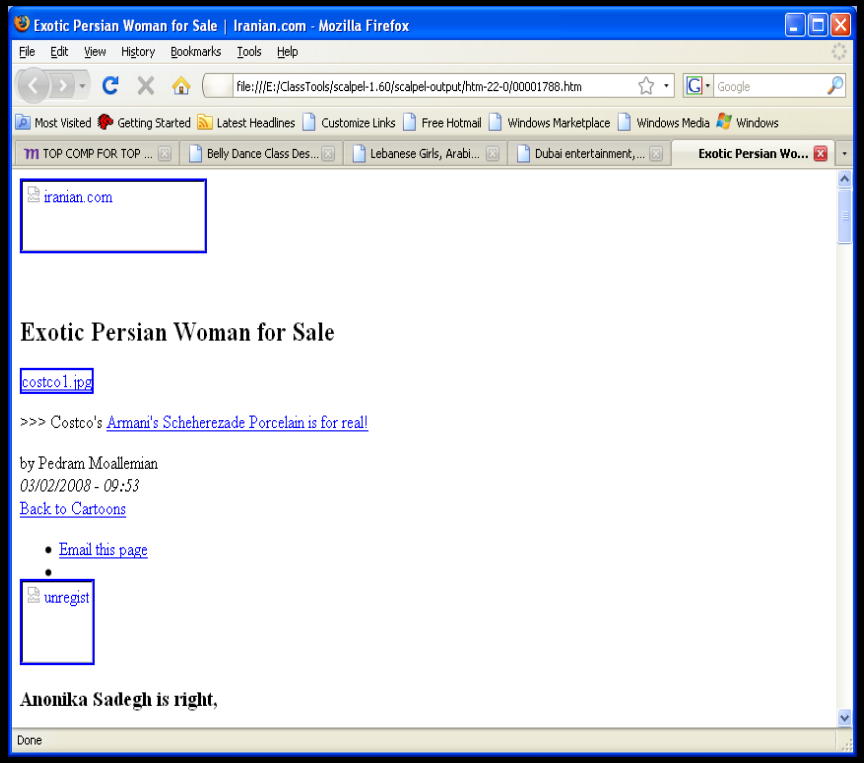


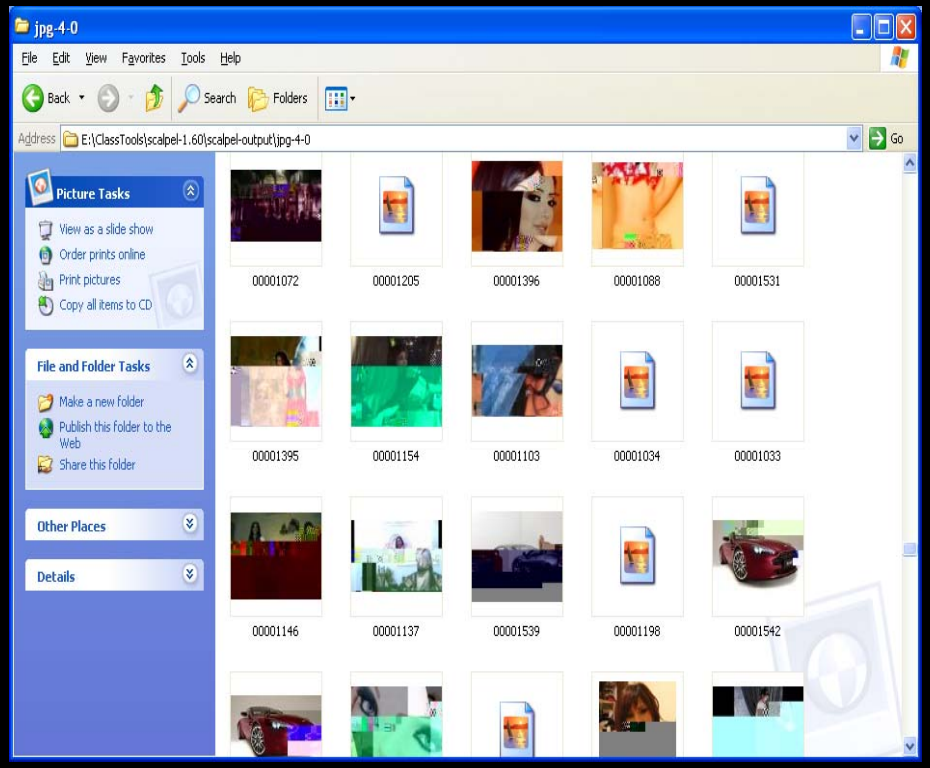


Capture Physical Memory

- Use ManTech's MDD to acquire RAM
  - `mdd_1.3.exe -o E:\Class-Workarea\MyPhysicalMemory.MDD-DiccKMaxxwell.img –v`
- Some implementation of DD may abort prematurely, probably due to user-mode access of memory

Analyze RAM with Scalpel (Notice other web sites visited in IE Tabs)





Analyze RAM with Volatility

C:\WINDOWS\system32\cmd.exe

```
C:\ForensicsClass\ClassTools\Volatility-1.1.2>\python25\python.exe volatility

        Volatile Systems Volatility Framework v1.1.1
        Copyright (C) 2007 Volatile Systems
        Copyright (C) 2007 Komoku, Inc.
        This is free software; see the source for copying conditions.
        There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A PART
ICULAR PURPOSE.

        usage: volatility cmd [cmd_opts]

        Run command cmd with options cmd_opts
        For help on a specific command, run 'volatility cmd --help'

        Supported Commands:
                connections     Print list of open connections
                connscan        Scan for connection objects
                datetime        Get date/time information for image
                dlllist         Print list of loaded dlls for each process (VERY
 verbose)
                files           Print list of open files for each process (VERY
verbose)
                ident           Identify image properties such as DTB and VM typ
e (may take a while)
                modules         Print list of loaded modules
                pslist          Print list of running processes
                psscan          Scan for EPROCESS objects
                sockets         Print list of open sockets
                sockscan        Scan for socket objects
                strings         Match physical offsets to virtual addresses (may
 take a while, VERY verbose)
                thrdscan        Scan for ETHREAD objects
                vaddump         Dump the Vad sections to files
                vadinfo         Dump the VAD info
                vadwalk         Walk the vad tree

        Example: volatility pslist -f /path/to/my/file

C:\ForensicsClass\ClassTools\Volatility-1.1.2>
```

Volatility: List of Open Files in RAM

files - Notepad

File Edit Format View Help

```
File   \AsyncConnectHlp
File   \WINDOWS\system32\stdole2.tlb
File   \WINDOWS\WinSxS\x86_Microsoft.windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
File   \Documents and Settings\dell\Local Settings\Temporary Internet Files\AntiPhishing\B3BB5BBA-E7D5-40AB-A041-A5B1C0B26C8F.dat
File   \WINDOWS\system32\Macromed\Flash\Flash9e.ocx
File   \WINDOWS\WinSxS\x86_Microsoft.windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
File   \WINDOWS\WinSxS\x86_Microsoft.windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
File   \AsyncSelectHlp
File   \Client
File   \NifsSct
File   \Documents and Settings\dell\Local Settings\Temporary Internet Files\Content.IE5\BHFXN5NI\trace[2].htm
File   \Documents and Settings\dell\Local Settings\Temporary Internet Files\Content.IE5\ENC1ICJO\iframe3[1].htm
File   \Documents and Settings\dell\Favorites
File   \NifsSct
File   \Documents and Settings\dell\Local Settings\Temporary Internet
Files\Content.IE5\LV5F32ZH\ancer;kw=Bellydancing;kw=Girls;kw=Amateur;kw=Orient;kw=Arabic;kw=Shake;kw=Sexy;kw=Children;kw=Controversial;kw=Kids;k
w=Women;kw=Saudi%20Arabia;kw=Shaking;pg=[1].htm
File   \Documents and Settings\dell\Local Settings\Temporary Internet Files\Content.IE5\BHFXN5NI\trace[1].htm
File   \WINDOWS\WinSxS\x86_Microsoft.windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
File   \Documents and Settings\dell\Local Settings\Temporary Internet Files\Content.IE5\LV5F32ZH\convert[1].htm
File   \WINDOWS\system32\msxml6.dll
File   \WINDOWS\system32\wmp.dll
File   \Documents and Settings\dell\Desktop
File   \Documents and Settings\dell\Local Settings\Temporary Internet Files\Content.IE5\LV5F32ZH\images;_ylt=A0geu5GH5fZISxIBm_RXNyoA[1].htm
File   \Endpoint
File   \Endpoint
File   \Endpoint
File   \NifsSct
File   \NifsSct
*********************************************************************
Pid: 3468
File   \ClassTools\iDefense\SysAnalyzer
File   \WINDOWS\WinSxS\x86_Microsoft.windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
File   \Documents and Settings\All Users\Application Data\Wave Systems Corp\AuthManager\biolsp.txt
File   \WINDOWS\MSWINSCK.OCX
File   \Endpoint
File   \NifsPvd
File   \NifsSct
File   \AsyncSelectHlp
*********************************************************************
Pid: 232
File   \WINDOWS
File   \WINDOWS\WinSxS\x86_Microsoft.windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
File   \WINDOWS\WinSxS\x86_Microsoft.windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
*********************************************************************
Pid: 3612
File   \Documents and Settings\dell
File   \WINDOWS\WinSxS\x86_Microsoft.windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
File   \WINDOWS\WinSxS\x86_Microsoft.windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
```

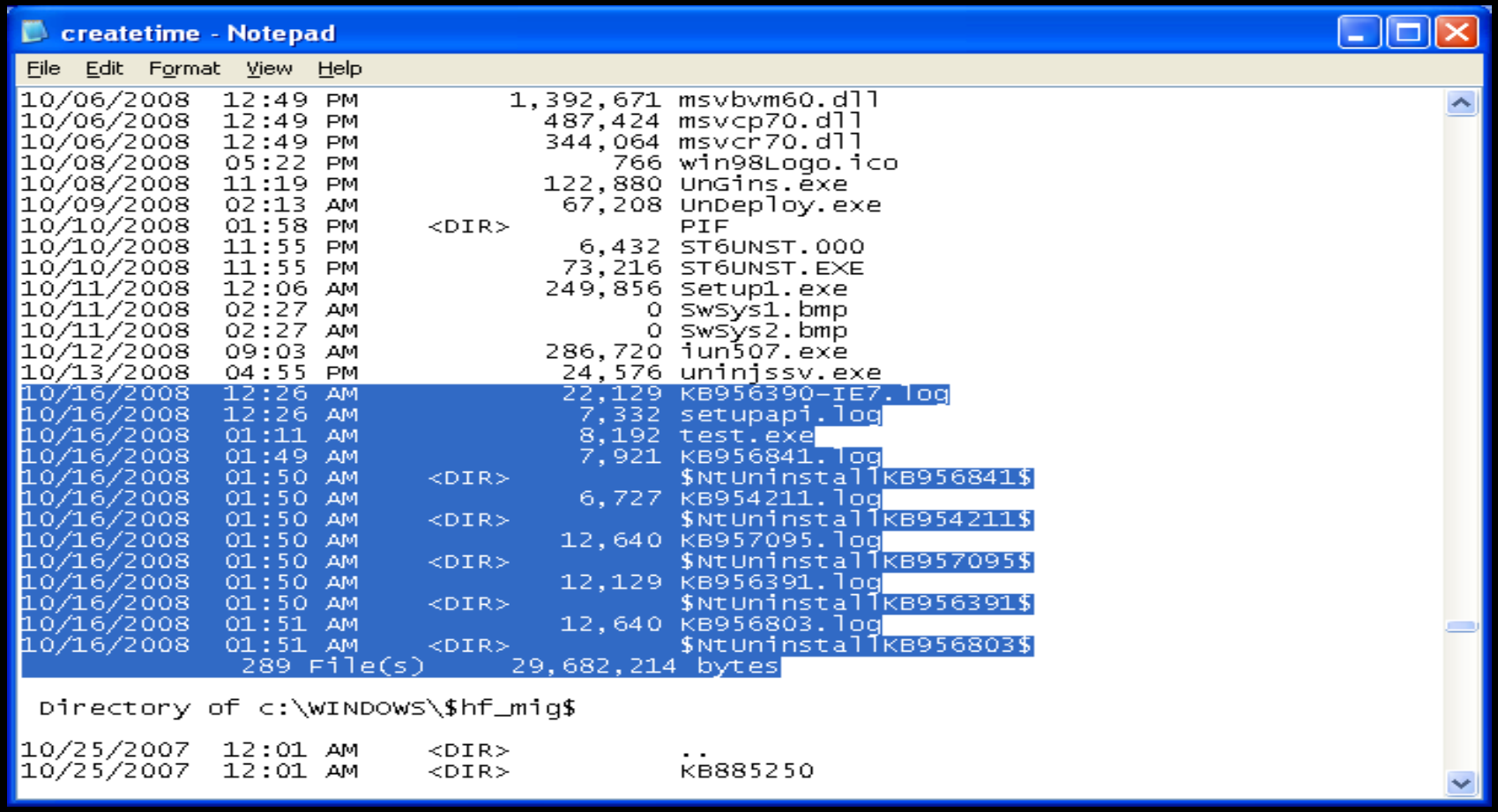
Volatility: List of Processes in RAM

plist - Notepad

File Edit Format View Help

DrgToDsc.exe	2900	268	4	161	Thu Oct 16 05:55:35 2008
issch.exe	3352	268	1	28	Thu Oct 16 05:55:39 2008
reader_sl.exe	3380	268	0	-1	Thu Oct 16 05:55:39 2008
GoogleDesktop.e	3492	268	18	540	Thu Oct 16 05:55:42 2008
vmware-tray.exe	4088	268	5	202	Thu Oct 16 05:55:43 2008
hqtray.exe	3960	268	2	68	Thu Oct 16 05:55:45 2008
GoogleDesktop.e	664	3492	3	153	Thu Oct 16 05:55:46 2008
avgnt.exe	4076	268	5	67	Thu Oct 16 05:55:46 2008
ngtray.exe	680	268	2	61	Thu Oct 16 05:55:47 2008
stsystra.exe	1116	268	5	134	Thu Oct 16 05:55:50 2008
wpctrl.exe	1168	268	1	57	Thu Oct 16 05:55:52 2008
dthtml.exe	1176	268	1	108	Thu Oct 16 05:55:52 2008
DSAgnt.exe	1296	268	15	304	Thu Oct 16 05:55:53 2008
GoogleToolbarNo	1312	268	4	182	Thu Oct 16 05:55:54 2008
Ee.exe	3668	268	1	142	Thu Oct 16 05:55:56 2008
autostart_and_p	3764	268	1	103456	Thu Oct 16 05:55:58 2008
Floater.exe	2240	1168	1	32	Thu Oct 16 05:55:59 2008
HookManager.exe	2476	1176	1	64	Thu Oct 16 05:56:00 2008
ctfmon.exe	2488	268	1	168	Thu Oct 16 05:56:00 2008
Eraser.exe	2496	268	2	94	Thu Oct 16 05:56:00 2008
GoogleDesktop.e	524	3492	6	218	Thu Oct 16 05:56:01 2008
DLG.exe	288	268	2	53	Thu Oct 16 05:56:05 2008
guardgui.exe	3680	804	0	-1	Thu Oct 16 05:56:10 2008
cmd.exe	3880	268	1	36	Thu Oct 16 05:56:24 2008
guardgui.exe	4020	804	0	-1	Thu Oct 16 05:56:36 2008
wireshark.exe	4004	268	7	207	Thu Oct 16 05:56:58 2008
dumpcap.exe	3120	4004	0	-1	Thu Oct 16 05:57:46 2008
dumpcap.exe	2904	4004	0	-1	Thu Oct 16 05:57:46 2008
dumpcap.exe	2064	4004	0	-1	Thu Oct 16 05:57:52 2008
iexplore.exe	3472	268	36	1743	Thu Oct 16 05:58:04 2008
guardgui.exe	3596	804	0	-1	Thu Oct 16 05:59:44 2008
guardgui.exe	3628	804	0	-1	Thu Oct 16 05:59:48 2008
guardgui.exe	3280	804	0	-1	Thu Oct 16 05:59:48 2008
get_pixs.exe	3468	268	6	117	Thu Oct 16 05:59:52 2008
guardgui.exe	4064	804	0	-1	Thu Oct 16 05:59:54 2008
guardgui.exe	3824	804	0	-1	Thu Oct 16 06:01:05 2008
notepad.exe	232	268	1	56	Thu Oct 16 06:02:17 2008
guardgui.exe	668	804	0	-1	Thu Oct 16 06:03:27 2008
guardgui.exe	2504	804	0	-1	Thu Oct 16 06:03:34 2008
guardgui.exe	1812	804	0	-1	Thu Oct 16 06:04:49 2008
guardgui.exe	3212	804	0	-1	Thu Oct 16 06:04:52 2008
guardgui.exe	204	804	0	-1	Thu Oct 16 06:04:57 2008
guardgui.exe	332	804	0	-1	Thu Oct 16 06:05:03 2008
taskmgr.exe	3612	1332	3	97	Thu Oct 16 06:05:50 2008
WINWORD.EXE	3792	268	9	430	Thu Oct 16 06:09:16 2008
Nessus Client.e	3852	268	1	82	Thu Oct 16 06:58:57 2008
md.exe	296	268	2	103	Thu Oct 16 06:59:09 2008
photome.exe	2060	268	1	136	Thu Oct 16 06:59:14 2008
ucheck.exe	3868	2060	0	-1	Thu Oct 16 06:59:15 2008

Some Newly Created Files



```
10/06/2008  12:49 PM         1,392,671 msvbvm60.dll
10/06/2008  12:49 PM           487,424 msvcp70.dll
10/06/2008  12:49 PM           344,064 msvcr70.dll
10/08/2008  05:22 PM               766 win98Logo.ico
10/08/2008  11:19 PM           122,880 UnGins.exe
10/09/2008  02:13 AM            67,208 UnDeploy.exe
10/10/2008  01:58 PM    <DIR>          PIF
10/10/2008  11:55 PM             6,432 ST6UNST.000
10/10/2008  11:55 PM            73,216 ST6UNST.EXE
10/11/2008  12:06 AM           249,856 Setup1.exe
10/11/2008  02:27 AM                 0 SwSys1.bmp
10/11/2008  02:27 AM                 0 SwSys2.bmp
10/12/2008  09:03 AM           286,720 iun507.exe
10/13/2008  04:55 PM            24,576 uninjssv.exe
10/16/2008  12:26 AM            22,129 KB956390-IE7.log
10/16/2008  12:26 AM             7,332 setupapi.log
10/16/2008  01:11 AM             8,192 test.exe
10/16/2008  01:49 AM             7,921 KB956841.log
10/16/2008  01:50 AM    <DIR>          $NtUninstallKB956841$
10/16/2008  01:50 AM             6,727 KB954211.log
10/16/2008  01:50 AM    <DIR>          $NtUninstallKB954211$
10/16/2008  01:50 AM            12,640 KB957095.log
10/16/2008  01:50 AM    <DIR>          $NtUninstallKB957095$
10/16/2008  01:50 AM            12,129 KB956391.log
10/16/2008  01:50 AM    <DIR>          $NtUninstallKB956391$
10/16/2008  01:51 AM            12,640 KB956803.log
10/16/2008  01:51 AM    <DIR>          $NtUninstallKB956803$
               289 File(s)     29,682,214 bytes

 Directory of c:\WINDOWS\$hf_mig$

10/25/2007  12:01 AM    <DIR>          ..
10/25/2007  12:01 AM    <DIR>          KB885250
```

Windows Prefetch Directory Listing

PrefetchDirectory-DicckMaxxWell - Notepad

File Edit Format View Help

```
 Volume in drive C has no label.
 Volume Serial Number is 14AD-59DA

 Directory of C:\WINDOWS\Prefetch

10/16/2008  01:50 AM    <DIR>          .
10/16/2008  01:50 AM    <DIR>          ..
10/16/2008  01:14 AM            44,558 010EDITOR.EXE-03B42F3D.pf
10/13/2008  10:13 PM            56,902 ACRORD32INFO.EXE-1A61B617.pf
10/16/2008  01:55 AM            28,518 AGENT.EXE-00ED4190.pf
10/15/2008  02:41 PM            12,318 APMSGFWD.EXE-09B0FDD0.pf
10/15/2008  02:41 PM            21,804 APOINT.EXE-03E36C22.pf
10/16/2008  01:55 AM            41,012 AVGNT.EXE-08C8F6E1.pf
10/13/2008  09:13 PM            65,508 AVNOTIFY.EXE-1A41E508.pf
10/16/2008  03:22 AM            32,540 AVWSC.EXE-21D2C1ED.pf
10/13/2008  10:06 PM            20,822 BASH.EXE-079C2828.pf
10/13/2008  03:44 PM            16,852 BINTEXT.EXE-164B97B0.pf
10/16/2008  01:55 AM            16,384 BRIGHTNESS.EXE-238597DB.pf
10/13/2008  09:48 PM             7,148 CHMOD.EXE-069636D3.pf
10/16/2008  01:56 AM            70,394 CMD.EXE-034B0549.pf
10/13/2008  10:00 PM            10,270 CP.EXE-38490CD5.pf
10/10/2008  02:55 PM            35,282 CSC.EXE-08AD7008.pf
10/15/2008  02:41 PM            16,210 CTFMON.EXE-05E57A5E.pf
10/10/2008  02:55 PM            16,948 CVTRES.EXE-1404C725.pf
10/13/2008  02:58 PM            23,434 DEFRAG.EXE-2858C7E2.pf
10/13/2008  09:58 PM             6,846 DF.EXE-02059414.pf
10/13/2008  02:58 PM            57,304 DFRGNTFS.EXE-38C3807C.pf
10/13/2008  09:57 PM             6,956 DIR.EXE-1631473F.pf
10/16/2008  01:56 AM            16,778 DLG.EXE-332F77D1.pf
10/15/2008  02:41 PM             3,370 DRGTODSC.EXE-3AA6A469.pf
10/16/2008  01:56 AM            18,494 DSAGNT.EXE-2C86BFCE.pf
10/16/2008  01:56 AM            21,288 DTHTML.EXE-08F9F9B5.pf
10/14/2008  04:14 PM            49,254 DUMPREP.EXE-0AF2BF67.pf
10/13/2008  09:46 PM            41,634 DW20.EXE-2834F196.pf
10/14/2008  04:48 PM            70,660 DWWIN.EXE-2C373FB7.pf
10/13/2008  09:48 PM             6,562 ECHO.EXE-0D1EC1D1.pf
10/15/2008  02:41 PM            32,194 ERASER.EXE-18F014B0.pf
10/16/2008  01:55 AM            79,712 EXPLORER.EXE-02121B1A.pf
10/13/2008  10:06 PM           108,028 FIND.EXE-0ECFEA05.pf
10/16/2008  01:27 AM            83,540 FIREFOX.EXE-06188867.pf
10/16/2008  01:56 AM            13,848 FLOATER.EXE-0DE51989.pf
10/16/2008  02:00 AM            22,886 GET_PIXS.EXE-33787175.pf
10/16/2008  03:00 AM            39,342 GOOGLEDESKTOP.EXE-16DAD850.pf
10/16/2008  01:56 AM            23,376 GOOGLETOOLBARNOTIFIER.EXE-0047A1C5.pf
10/13/2008  09:48 PM             6,838 GREP.EXE-1B585B79.pf
10/16/2008  03:11 AM            22,202 GUARDGUI.EXE-2C1384C2.pf
10/15/2008  03:00 PM            60,330 HELPSVC.EXE-1C192440.pf
10/16/2008  01:32 AM            46,596 HH.EXE-104606B2.pf
10/15/2008  02:41 PM            14,318 HKCMD.EXE-0F06AE14.pf
```

Volatile Data Capture Using Forensics Server Project (FSP)

C:\WINDOWS\system32\cmd.exe - fspc -c dicckmaxxwell -n dmaxx -i "Inno Inno" -v

```
C:\ForensicsClass\ClassTools\WindowsForensicsBook-DVD\code\FSP>fsp -c dicckmaxxw
ell -n dmaxx -i "Inno Inno" -v
'fsp' is not recognized as an internal or external command,
operable program or batch file.

C:\ForensicsClass\ClassTools\WindowsForensicsBook-DVD\code\FSP>fspc -c dicckmaxx
well -n dmaxx -i "Inno Inno" -v
Verbose mode set.
Setup complete.
Case Name: dmaxx\
Port      : 7070
Server started...
Awaiting connection...
```

C:\WINDOWS\system32\cmd.exe

```
C:\ForensicsClass\ClassTools\WindowsForensicsBook-DVD\code\FRU>fruc -s 127.0.0.1
 7070 -f fruc-dicckmaxxwell.txt -v
Verbose mode set.
"[Thu Oct 16 04:00:41 2008] \ClassTools\HELIX-v1.8\IR\sysinternals\psloggedon.ex
e" log command sent.
\ClassTools\HELIX-v1.8\IR\sysinternals\psloggedon.exe results data sent.
"[Thu Oct 16 04:00:41 2008] \ClassTools\HELIX-v1.8\IR\sysinternals\autorunsc.exe
 -a" log command sent.
\ClassTools\HELIX-v1.8\IR\sysinternals\autorunsc.exe -a results data sent.
"[Thu Oct 16 04:00:41 2008] \ClassTools\HELIX-v1.8\IR\windbg\tlist.exe -c" log c
ommand sent.
\ClassTools\HELIX-v1.8\IR\windbg\tlist.exe -c results data sent.
"[Thu Oct 16 04:00:41 2008] \ClassTools\HELIX-v1.8\IR\windbg\tlist.exe -s" log c
ommand sent.
\ClassTools\HELIX-v1.8\IR\windbg\tlist.exe -s results data sent.
"[Thu Oct 16 04:00:41 2008] \ClassTools\HELIX-v1.8\IR\windbg\tlist.exe -t" log c
ommand sent.
\ClassTools\HELIX-v1.8\IR\windbg\tlist.exe -t results data sent.
"[Thu Oct 16 04:00:41 2008] \ClassTools\HELIX-v1.8\IR\bin\openports.exe -fport"
log command sent.
\ClassTools\HELIX-v1.8\IR\bin\openports.exe -fport results data sent.
"[Thu Oct 16 04:00:41 2008] \ClassTools\HELIX-v1.8\IR\bin\openports.exe -netstar
t" log command sent.
\ClassTools\HELIX-v1.8\IR\bin\openports.exe -netstart results data sent.
"[Thu Oct 16 04:00:41 2008] \ClassTools\HELIX-v1.8\IR\microsoft\auditpol.exe" lo
g command sent.
\ClassTools\HELIX-v1.8\IR\microsoft\auditpol.exe results data sent.
"[Thu Oct 16 04:00:41 2008] \ClassTools\HELIX-v1.8\IR\bin\cmdline.exe" log comma
nd sent.
\ClassTools\HELIX-v1.8\IR\bin\cmdline.exe results data sent.
"[Thu Oct 16 04:00:41 2008] \ClassTools\HELIX-v1.8\IR\sysinternals\logonsessions
.exe" log command sent.
```

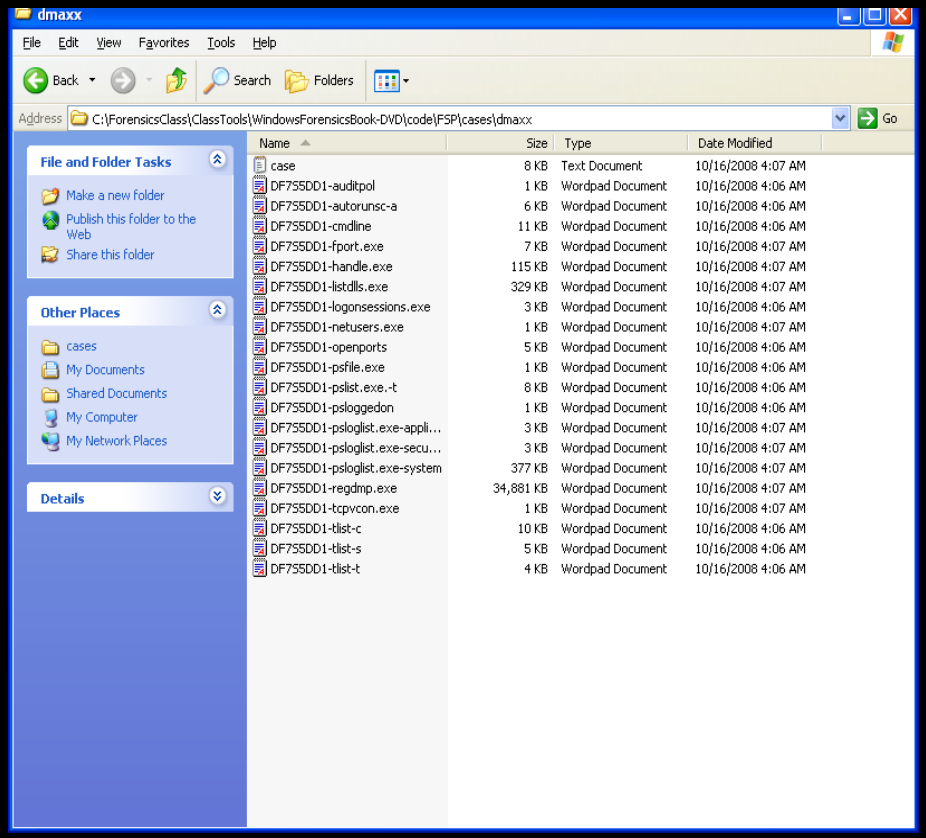
C:\WINDOWS\system32\cmd.exe - fspc -c dicckmaxxwell -n dmaxx -i "Inno Inno" -v

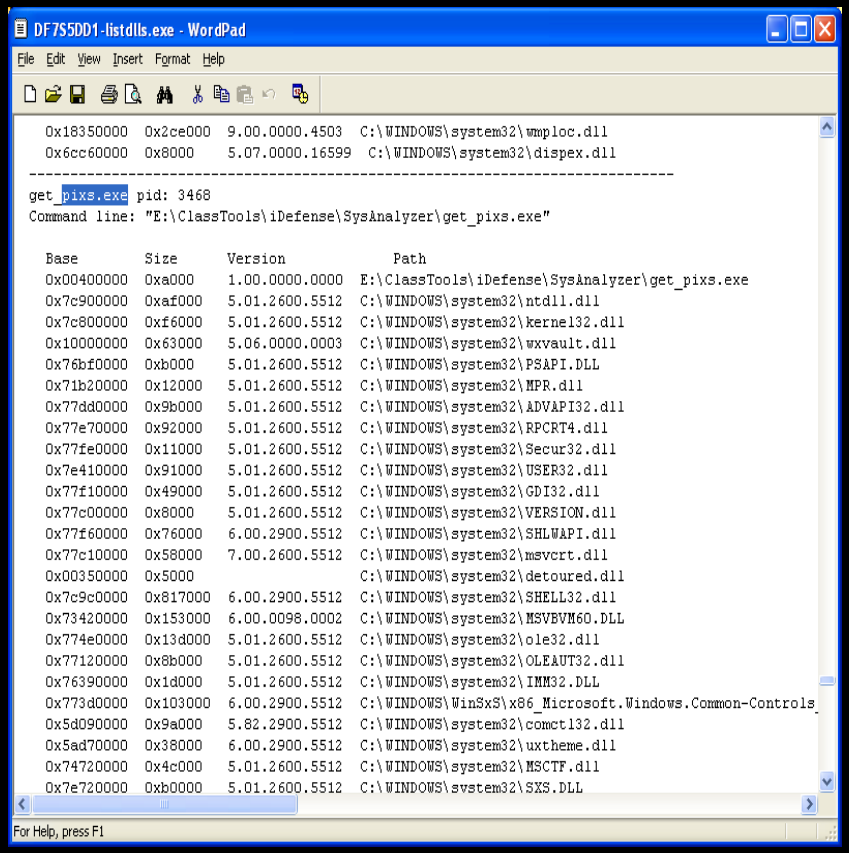
```
DATA command received: DF7S5DD1-psloglist.exe-security.dat
Terminating on signal SIGINT(2)

C:\ForensicsClass\ClassTools\WindowsForensicsBook-DVD\code\FSP>fspc -c dicckmaxx
well -n dmaxx -i "Inno Inno" -v
Verbose mode set.
Setup complete.
Case Name: dmaxx\
Port      : 7070
Server started...
Awaiting connection...
Connection from 127.0.0.1
DATA command received: DF7S5DD1-psloggedon.dat
DATA command received: DF7S5DD1-autorunsc-a.dat
DATA command received: DF7S5DD1-tlist-c.dat
DATA command received: DF7S5DD1-tlist-s.dat
DATA command received: DF7S5DD1-tlist-t.dat
DATA command received: DF7S5DD1-openports.dat
DATA command received: DF7S5DD1-openports.dat
DATA command received: DF7S5DD1-auditpol.dat
DATA command received: DF7S5DD1-cmdline.dat
DATA command received: DF7S5DD1-logonsessions.exe.dat
DATA command received: DF7S5DD1-psfile.exe.dat
DATA command received: DF7S5DD1-pslist.exe.-t.dat
```

C:\WINDOWS\system32\cmd.exe

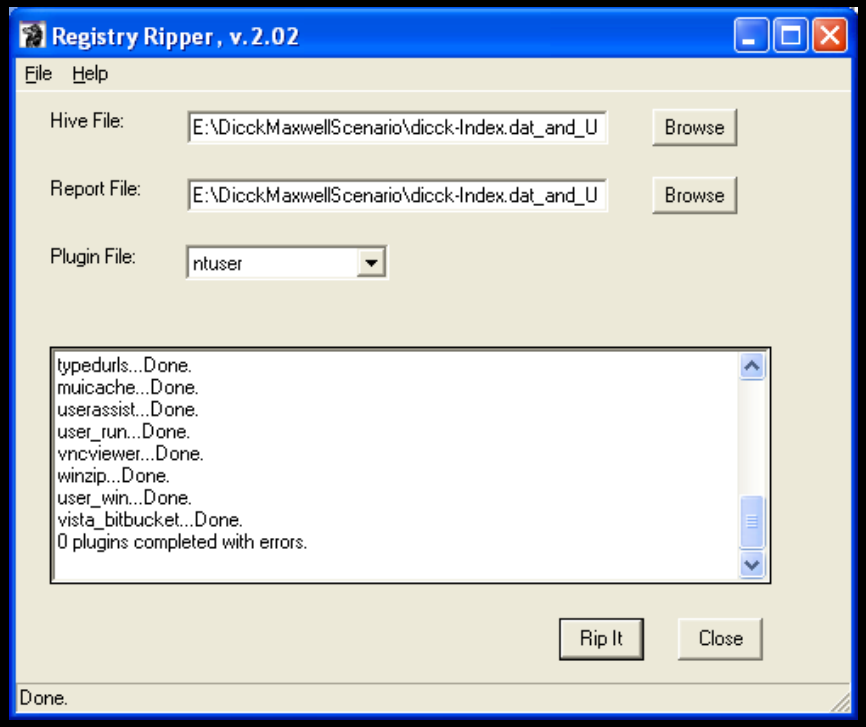
```
Connection from 127.0.0.1
DATA command received: DF7S5DD1-psloggedon.dat
DATA command received: DF7S5DD1-autorunsc-a.dat
DATA command received: DF7S5DD1-tlist-c.dat
DATA command received: DF7S5DD1-tlist-s.dat
DATA command received: DF7S5DD1-tlist-t.dat
DATA command received: DF7S5DD1-openports.dat
DATA command received: DF7S5DD1-openports.dat
DATA command received: DF7S5DD1-auditpol.dat
DATA command received: DF7S5DD1-cmdline.dat
DATA command received: DF7S5DD1-logonsessions.exe.dat
DATA command received: DF7S5DD1-psfile.exe.dat
DATA command received: DF7S5DD1-pslist.exe.-t.dat
DATA command received: DF7S5DD1-listdlls.exe.dat
DATA command received: DF7S5DD1-handle.exe.dat
DATA command received: DF7S5DD1-tcpvcon.exe.dat
DATA command received: DF7S5DD1-netusers.exe.dat
DATA command received: DF7S5DD1-fport.exe.dat
DATA command received: DF7S5DD1-regdmp.exe.dat
DATA command received: DF7S5DD1-psloglist.exe-system.dat
DATA command received: DF7S5DD1-psloglist.exe-application.dat
DATA command received: DF7S5DD1-psloglist.exe-security.dat
Terminating on signal SIGINT(2)

C:\ForensicsClass\ClassTools\WindowsForensicsBook-DVD\code\FSP>
```

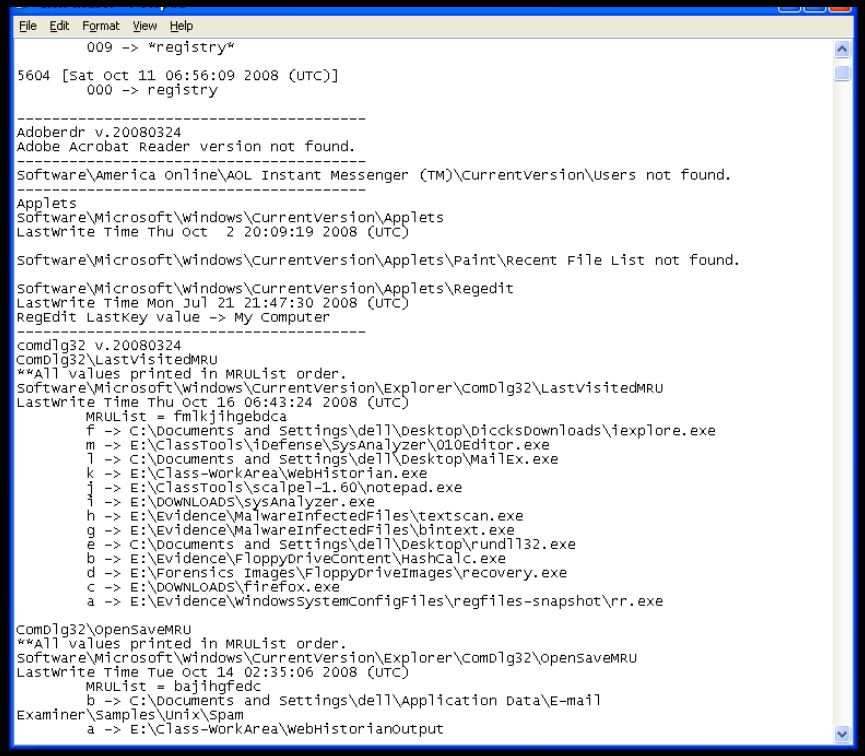
Forensic Server Project: Results of Data





Registry Analysis with RegRipper





Internet Activity Results

MyLastSearch

File Edit View Options Help

Search Text	Search Engine	Search Type	Search Time	Web Browser	Hits	URL
technology sales jobs in dubai	Google	General	10/16/2008 2:50:54 AM	Internet Explorer	3	http://www.google.com/search?hl=en&q=technology+sales+jobs+...
sales jobs in dubai	Google	General	10/16/2008 2:50:42 AM	Internet Explorer	3	http://www.google.com/search?hl=en&q=sales+jobs+in+dubai&aq...
tradeshow sales	Google	General	10/16/2008 2:47:09 AM	Internet Explorer	3	http://www.google.com/search?hl=en&q=tradeshow+sales
how to increase sales	Google	General	10/16/2008 2:46:59 AM	Internet Explorer	9	http://www.google.com/search?hl=en&q=how+to+increase+sales
how to increase slaes	Google	General	10/16/2008 2:46:34 AM	Internet Explorer	3	http://www.google.com/search?hl=en&q=how+to+increase+slaes...
najlaa	YouTube	Video	10/16/2008 2:45:48 AM	Internet Explorer	7	http://www.youtube.com/results?search_query=najlaa&search_ty...
hot araBIC models	Yahoo	General	10/16/2008 2:45:03 AM	Internet Explorer	12	http://search.yahoo.com/search;_ylt=A0geu9jH4PZIAKYAbL5XNyo...
hot araBIC BABES	Yahoo	General	10/16/2008 2:39:56 AM	Internet Explorer	9	http://search.yahoo.com/search?p=hot+araBIC+BABES&fr=ush1-f...
exotic arabic women	Google	General	10/16/2008 2:29:09 AM	Internet Explorer	6	http://www.google.com/search?hl=en&q=exotic+arabic+women
female escort dubai	Google	General	10/16/2008 2:22:42 AM	Internet Explorer	10	http://www.google.com/search?hl=en&q=female+escort+dubai
currency conversion rate UAE US	Google	General	10/16/2008 2:18:34 AM	Internet Explorer	6	http://www.google.com/search?hl=en&q=currency+conversion+ra...
hot babes	Google	General	10/16/2008 2:15:00 AM	Internet Explorer	10	http://www.google.com/search?hl=en&q=hot+babes&aq=f&oq=
ida pro download	Google	General	10/16/2008 1:22:25 AM	Internet Explorer	3	http://www.google.com/search?hl=en&rls=com.microsoft%3Aen-u...
www.hexways.com	Google	General	10/16/2008 1:22:12 AM	Internet Explorer	3	http://www.google.com/search?q=www.hexways.com&rls=com.mi...
keystroke loggers software	Google	General	10/14/2008 4:13:23 PM	Internet Explorer	10	http://www.google.com/search?hl=en&q=keystroke+loggers+soft...

334 item(s), 1 Selected — NirSoft Freeware. http://www.nirsoft.net

IEHistoryView: c:\documents and settings\dell\Local Settings\History

File Edit View Help

URL	Title	Hits	Modified Dat
file:///E:/ClassTools/scalpel-1.60/scalpel-output/jpg-4-0/00000951.jpg		1	10/16/2008 3
http://www.trywebwatcher.com/WebUI/(S(e11xag55rganqqisp2s0lfbp))/WWSetup-Install.aspx	Awareness Technologies	70	10/16/2008 3
file:///E:/ClassTools/scalpel-1.60/scalpel-output/png-5-0/00001671.png		1	10/16/2008 3
file:///E:/ClassTools/scalpel-1.60/scalpel-output/tif-8-0/00001693.tif		1	10/16/2008 3
http://www.metacafe.com/watch/422828/sexy_arabic_girl_belly_dancing	Sexy Arabic Girl Belly Dancing. - Video	84	10/16/2008 3
http://finance.yahoo.com/currency/convert?amt=2300&from=AED&to=USD&submit=Convert	UAE Dirham to U.S. Dollar Exchange Rate - Yahoo! Finance	189	10/16/2008 3
http://images.search.yahoo.com/search/images;_ylt=A0geu5GH5fZISxIBm_RXNyoA?ei=UTF-8&p=ba...	Yahoo! Image Search Results for babes for sale	19	10/16/2008 3
file:///E:/ClassTools/scalpel-1.60/scalpel-output/gif-2-0/00000004.gif		1	10/16/2008 3
file:///E:/ClassTools/scalpel-1.60/scalpel-output/gif-2-0/00000002.gif		1	10/16/2008 3

1839 item(s)

Analysis of “Suspicious” Executable with Online Malware Scanner

get_pixs.exe MD5:2a723f9b6867cfbe093a8d68534df6bf - VirSCAN.org 21% Scanner(8/38) found malware - Windows Internet Explorer

http://www.virscan.org/report/428bf2a9495cd3933f4849105c85e754.html

VirSCAN.org
submit & scan your file

Suspicious files to scan Browse... Upload
1, You can UPLOAD any files, but there is 10Mb limit per file.
2, VirSCAN supports Rar/Zip decompression, but it must be less than 10 files.
3, VirSCAN can scan compressed files with password 'infected' or 'virus'.

Language: English

Server load

File information

File Name : get_pixs.exe
File Size : 8192 byte
File Type : PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5 : 2a723f9b6867cfbe093a8d68534df6bf
SHA1 : 4ab539a45be8ca572ea22ec217068e465c2da38b

Scanner results

Scanner results : 21% Scanner(8/38) found malware!
Time : 2008/10/16 02:06:04 (EDT)

Scanner	Engine Ver	Sig Ver	Sig Date	Scan result	Time
a-squared	4.0.0.16	2008.10.15	2008-10-15	-	1.502
AhnLab V3	2008.10.16.01	2008.10.16	2008-10-16	-	0.970
AntiVir	7.9.0.4	7.0.7.45	2008-10-15	BDS/Agent.CC	2.421
Antiy	2.0.18	20081015.1487019	2008-10-15	-	0.127
Arcavir	1.0.5	200810132247	2008-10-13	-	1.233

Main Menu
- HOME
- About VirSCAN
- Report
- Help VirSCAN
- Submit Bugs
- Contact us

Other Observations

- “My Documents” directory was encrypted
- Travel arrangements were made online

Summarized Findings

- Analysis showed Dicck Maxxwell was indeed surfing the web for illicit contents
- There was a “suspicious” executable, but had nothing to do with the illicit content
  - The suspicious executable used for our analysis was simply a test tool and not a real malicious code
- Secure deletion utility was installed on system, which wipes out all temporary and cache files

Lessons Learned

- Lack of incident response team could render investigations difficult or unsuccessful
- Lack of security policy could result in misuse of corporate resources
- Shutting down the system prior to collecting evidence could have resulted in evidence lost
- Knowing local, state, and Federal laws applicable to an investigation is paramount

Some Incident Response Tools

netSecurity
Forensic Labs

netSecurity®

Non-Commercial Forensics Toolkits

- Helix CD
- Assorted Tools and Toolkits
  - SysInternals
  - SomarSoft
  - iDefense Toolkits
  - Foundstone
  - Forensics Server Project
  - Volatility Framework
  - Scalpel/Foremost

Commercial Forensics Toolkits

- Guidance Software
- ProDiscover IR
- Mandiant
- Access Data Enterprise
- Wetstone's LiveWire
- Many more

Selected References

- Guide to Integrating Forensic Techniques into Incident Response, NIST 800-86, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
- CERT Training and Education handbook, *First Responders Guide to Computer Forensics*
- Todd G. Shipley, CFE, CFCE and Henry R. Reeve, Esq., *Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community,* http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RunningComputer.pdf
- Jesse D. Kornblum, *Exploiting the Rootkit Paradox with Windows Memory Analysis*, https://www.utica.edu/academic/institutes/ecii/publications/articles/EFE2FC4D-0B11-BC08-AD2958256F5E68F1.pdf
- Selected Incident Response-related Books:
  - Carvey, Harlan, *Windows Forensic Analysis,* Syngress; Pap/DVD edition (April 24, 2007)
  - Jones, Keith J., Richard Bejtlich, and Curtis W. Rose, *Real Digital Forensics: Computer Security and Incident Response,* Addison-Wesley Professional (October 3, 2005)
  - Kevin Mandia, Chris Prosise, and Matt Pepe, *Incident Response and Computer Forensics*, McGraw-Hill/Osborne; 2 edition (July 17, 2003)
  - James M. Aquilina, Eoghan Casey, Cameron H. Malin, *Malware Forensics: Investigating and Analyzing Malicious Code*, Syngress (June 30, 2008)

Direct Comments/Questions to:

Inno@NetSecurity.com

netSecurity Forensic Labs

netSecurity®

Thank You for Coming!

netSecurity
Forensic Labs

netSecurity®