Responding to the Digital Crime Scene: Gathering Volatile Data

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

October 29, 2008
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

  - 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 Investigators (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 Lose

• 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”
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
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 in Action…

E:\ClassTools\scalpel-1.60>scalpel -i Wireshark-Traffic-Capture-DicckMaxxwell-TechnoForensics.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\ui"
ERROR: Couldn't open input file: ui -- No such file or directory
Scalpel was unable to open the image file: ui
Skipping...

Opening target "E:\ClassTools\scalpel-1.60\Wireshark-Traffic-Capture-DicckMaxxwell-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

Responding to the Digital Crime Scene: Gathering Volatile Data
Copyright © 2008 NetSecurity Corporation. All Rights Reserved.
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:\ForensicsClass\ClassTools\Volatility-1.1.2>\python26\python.exe volatility
Volatile Systems Volatility Framework v1.1
Copyright © 2007 Volatile Systems
Copyright © 2007 Konoko, Inc.
This is free software; see the source for copying conditions.
There is NO warranty; see the source for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

usage: volatility [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
  connectscan    Scan for connection objects
  dillist        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
  plist          List of running processes
  mmmap          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)
  threadscan     Scan for ETWREAD objects
  vaddump        Dump the Vad sections to files
  vadinfo        Dump the VAD info
  vadwalk        Walk the vad tree

Example: volatility plist -f /path/to/my/file
```

Responding to the Digital Crime Scene: Gathering Volatile Data
Copyright © 2008 NetSecurity Corporation. All Rights Reserved.
Volatility: List of Open Files in RAM

Responding to the Digital Crime Scene: Gathering Volatile Data

Copyright © 2008 NetSecurity Corporation. All Rights Reserved.
Volatility: List of Processes in RAM

Responding to the Digital Crime Scene: Gathering Volatile Data
Copyright © 2008 NetSecurity Corporation. All Rights Reserved.
Some Newly Created Files

```
File          Edit Format View  Help
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 msvcp70.dll
10/06/2008  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 STGUNST.000
10/10/2008  11:55 PM  73,216 STGUNST.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 Unig327.exe
10/13/2008  04:55 PM  24,576 Uninstallsv.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 KB9566841.log
10/16/2008  01:50 AM  <DIR> $NTUninstallKB9566841$%
10/16/2008  01:50 AM  <DIR> 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 KB956291.log
10/16/2008  01:50 AM  <DIR> $NTUninstallKB956291$
10/16/2008  01:51 AM  12,640 KB956805.log
10/16/2008  01:51 AM  <DIR> $NTUninstallKB956805$
289 File(s)  29,082,214 bytes
```
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>File Name</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/16/2008</td>
<td>01:50 AM</td>
<td>&lt;DIR&gt;</td>
<td>C:\WINDOWS\Prefetch</td>
</tr>
<tr>
<td>10/16/2008</td>
<td>01:50 AM</td>
<td>&lt;DIR&gt;</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>01:14 AM</td>
<td>44,558 OICEDITOR.EXE-03B42F3F.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>01:13 AM</td>
<td>56,902 ATCRODS42INFO.EXE-1A4D3B1C.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>01:55 AM</td>
<td>28,533 AGENT.EXE-0CD41509.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>02:41 AM</td>
<td>12,528 ARMS.PDFM.EXE-09805B9D.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>02:41 PM</td>
<td>21,804 APPOINT.EXE-03E35B92.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>03:55 AM</td>
<td>41,612 AVD.EXE-026B8525.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>09:13 AM</td>
<td>65,198 AWNCFM.EXE-0A3A12D3.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>03:22 AM</td>
<td>32,148 AWSC.EXE-20D21B2E.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>03:06 AM</td>
<td>20,882 BASH.EXE-070C2B88.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>06:44 PM</td>
<td>36,123 BENTEXT.EXE-16A4975E.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>03:55 AM</td>
<td>16,988 BRIGHTNESS.EXE-239597D6.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>09:45 AM</td>
<td>7,448 DRIVER.EXE-069635D5.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>01:56 AM</td>
<td>70,304 CMD.EXE-05466949.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>10:00 AM</td>
<td>10,270 CP.EXE-38450C93.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>02:55 PM</td>
<td>35,282 CSS.EXE-00AD7008.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>02:41 AM</td>
<td>16,230 CRF.EXE-0E377A63.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>02:55 AM</td>
<td>16,230 CTVS.EXE-1404C725.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>02:55 AM</td>
<td>23,394 DCBFILE.EXE-2898C762.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>09:58 PM</td>
<td>6,846 DF.EXE-05054103.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>09:58 PM</td>
<td>57,204 DPREF.EXE-38E8870C.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>10:57 PM</td>
<td>6,956 DR.EXE-1531473F.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>10:56 AM</td>
<td>16,778 DUG.EXE-332F7761.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>07:41 PM</td>
<td>3,370 DICT.POC.EXE-3A4A6469.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>01:56 AM</td>
<td>18,494 DMGR.EXE-2C869FCE.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>01:56 AM</td>
<td>22,238 DMVIEW.EXE-08F8F895.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>04:14 PM</td>
<td>49,254 DUMP.EXE-0AF2B5E7.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>09:46 PM</td>
<td>41,634 DW2.EXE-28341996.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>04:48 PM</td>
<td>70,660 DWGIN.EXE-2C1755B7.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>09:48 AM</td>
<td>6,562 ECHO.EXE-0DD6CD11.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>02:41 AM</td>
<td>32,194 ERASER.EXE-188F519D.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>01:56 AM</td>
<td>76,732 EXPLORER.EXE-05131614.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>10:06 PM</td>
<td>108,028 EXIT.EXE-0E0E7D3D.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>04:27 AM</td>
<td>83,140 FIREFOX.EXE-0618895F.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>01:56 AM</td>
<td>13,848 FLOAT.EXE-0F519380.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>03:00 AM</td>
<td>48,196 GOOGLE.EXE-1A4D4B53.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>01:56 AM</td>
<td>23,376 GOOGLETOOL.EXE-0647EAC5.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>09:48 AM</td>
<td>6,938 GUI.EXE-1B987B93.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>03:11 AM</td>
<td>22,202 GUARD.EXE-2C130842.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>03:00 PM</td>
<td>60,030 HELP.EXE-1C192A40.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>01:52 AM</td>
<td>46,196 IE.EXE-104C60B2.pf</td>
<td></td>
</tr>
<tr>
<td>10/16/2008</td>
<td>02:41 AM</td>
<td>14,318 HKCMD.EXE-0F06AE14.pf</td>
<td></td>
</tr>
</tbody>
</table>
Volatile Data Capture Using Forensics Server Project (FSP)
Registry Analysis with RegRipper
Internet Activity Results

<table>
<thead>
<tr>
<th>URL</th>
<th>Title</th>
<th>Hits</th>
<th>Modified Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>file://:ClassTools/scapel-1.6/scapel-output/img-2-0/0000951.jpg</td>
<td>Awareness Technologies</td>
<td>1</td>
<td>10/16/2008</td>
</tr>
<tr>
<td><a href="http://www.strywebwatcher.com/WebUI/55e1f50c504f9483e2508_bj%D0%BF%D1%8B">http://www.strywebwatcher.com/WebUI/55e1f50c504f9483e2508_bjпы</a> ё)/WWW/Setup-Install.aspx</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>file://:ClassTools/scapel-1.6/scapel-output/img-5-0/00001571.png</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>file://:ClassTools/scapel-1.6/scapel-output/lr-5-0/00001693.1l</td>
<td>Sexy Arabic Girl Belly Dancing - Video</td>
<td>84</td>
<td>10/16/2008</td>
</tr>
<tr>
<td><a href="http://images.search.yahoo.com/search/images.jsp?fr=00open&amp;intt=3&amp;16896=16896&amp;bypic=">http://images.search.yahoo.com/search/images.jsp?fr=00open&amp;intt=3&amp;16896=16896&amp;bypic=</a>...</td>
<td>Yahoo Image Search Results for babies for sale</td>
<td>19</td>
<td>10/16/2008</td>
</tr>
</tbody>
</table>
Analysis of “Suspicious” Executable with Online Malware Scanner
Other Observations

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

- Analysis showed Dick 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
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


- **CERT Training and Education handbook, First Responders Guide to Computer Forensics**


- 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](https://www.utica.edu/academic/institutes/ecii/publications/articles/EFE2FC4D-0B11-BC08-AD2958256F5E68F1.pdf)

- **Selected Incident Response-related Books:**
Direct Comments/Questions to:

Inno@NetSecurity.com
Thank You for Coming!