U.S. Department of Energy
Office of Inspector General
Technology Crimes Section

Live Incident Response

The Law Enforcement Perspective

Assistant Special Agent-in-Charge
Daniel Persson

OVERVIEW

- Background
- Law Enforcement (LE) Mindset
- Collection of Evidence
- Triage
- Final Thoughts

Background

- Current Duties
  - Assistant Special Agent-in-Charge OIG Technology Crimes Section (TCS)
    - Handle all LE related Tech Crimes for DOE
    - Digital media analysis
    - LE-centric intrusion cases
    - CP cases in DOE complex
    - LE POC for DOE in all joint investigations
      - FBI, AFOSI, ICE, etc

- What I Don't Do
  - I am not a Lawyer
  - I am not an Auditor
  - I don't create DOE policy
    - How can IG create and audit policy?
    - How can I define what DOE policy is?
  - I don't investigate APT – other people do

- Current Problem: “How can we take the traditional LE mindset and apply it to today’s Incident Response environment?”

Law Enforcement (LE) Mindset

- Catch the Bad Guys

- Traditional Law Enforcement Mindset
  - Seize physical evidence (drugs, body)
  - Don’t alter the item
  - Remove it from the scene
  - Analyze it later
  - Reference the original at all times

- Computer Evidence is Different
  - Physical computer vs. resident data
  - Corrupting data part of collection
  - Data lost during shut down
  - Seizure re-victimizes Department
    - Hardware loses value
    - Reacquire hardware
    - Restore data from good backup
  - Easy to collect too much

Evidence Collection

- Forensic Computer Imaging

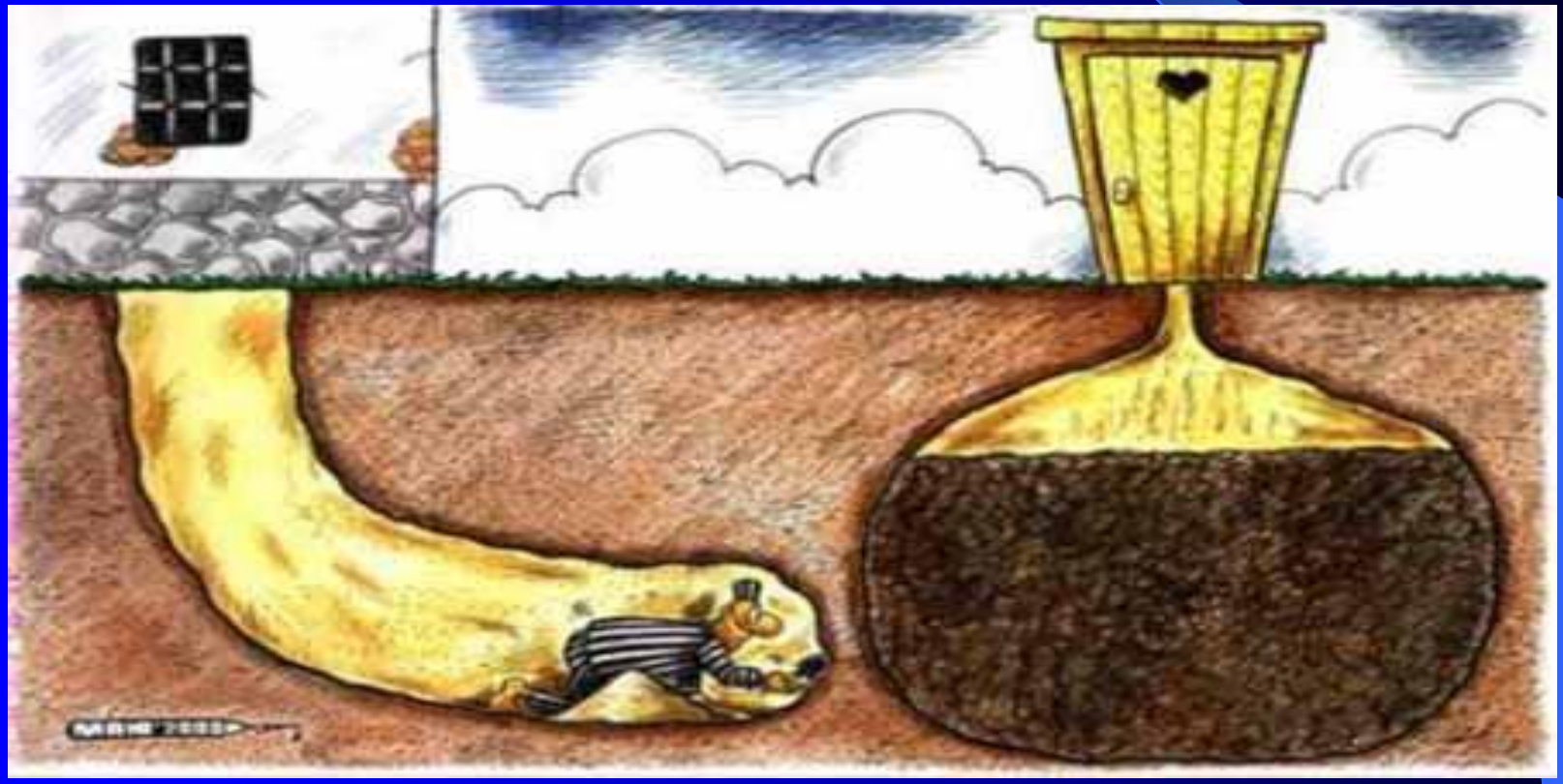
- Digital Evidence Importance
  - Holds evidence of a crime
    - Copies of fraudulent contracts
    - Emails showing Intellectual Property theft
    - Contacts in an online counterfeit ring
  - Holds evidence about a crime
    - Timestamps on files used by attacker
    - TCP network connection to IP address
    - USB serial number entry in registry (USBSTOR)

- What Can We Capture?
  - RAM
    - RAM resident malware
    - Keys/passwords
    - Data fragments
    - Unpacked executables
  - Processes
    - Source
    - Links
    - Scheduled

- Networking
  - Active/listening/recent connections
  - Routing tables
  - Services listening on specific ports
- Logons
  - Users remotely logged on
  - Systems connected to shares
  - Recent activity

  - Services
    - What's listening
    - What's running
  - DLL shared libraries
  - File handles
- Whatever we don't collect we lose
  - Far more challenging to recreate on dead box
  - Some data can't be recreated (e.g. RAM)

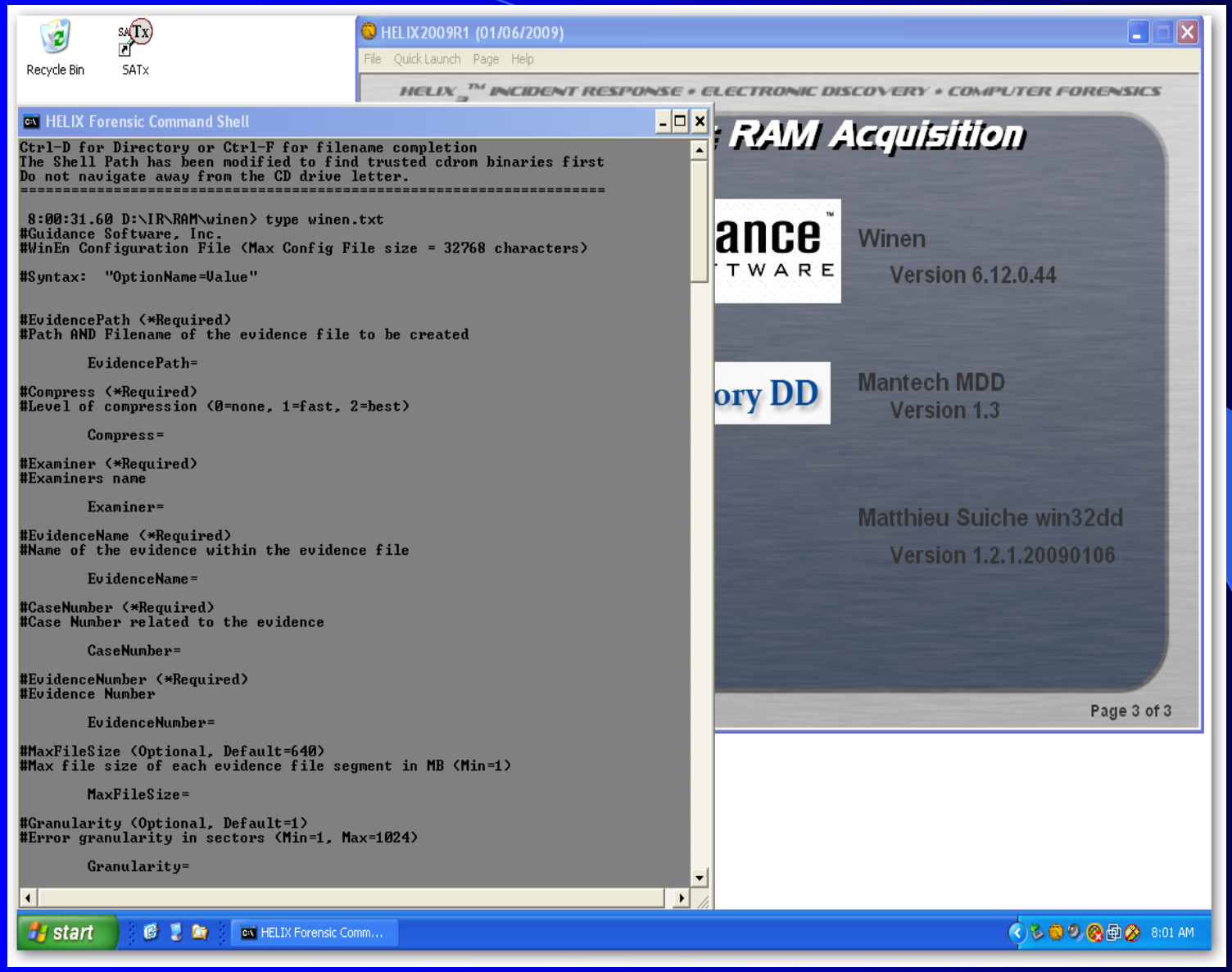
- Methodology
  - Have a plan!



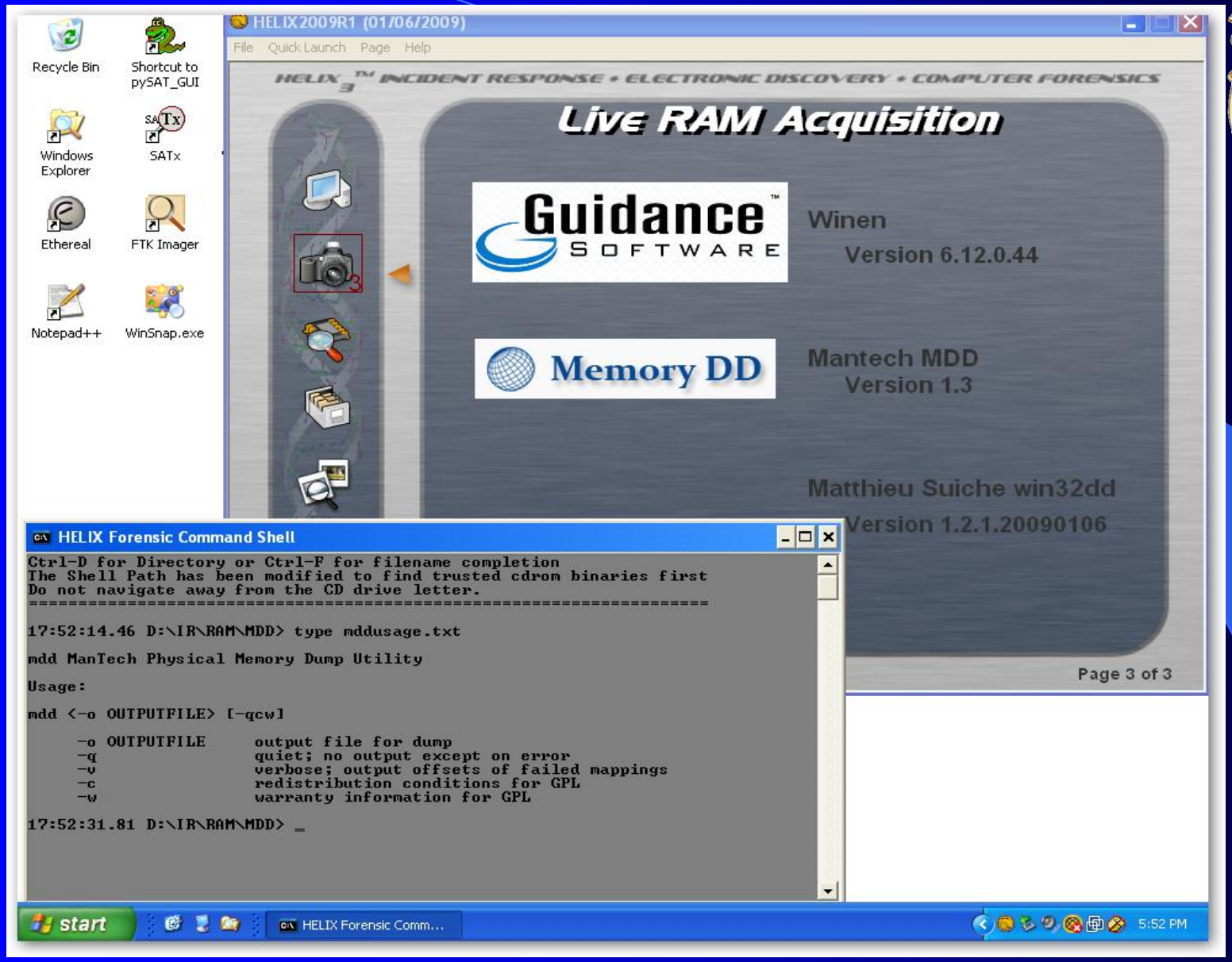
- Learn tools
  - Limitations
  - Affect on system
- Test on non-production systems
  - Various OS versions
  - Different user levels
- Static binaries
  - Helix CD/website
  - Tested production binaries

- Set up proper collection process
  - RAM should be 1st
  - Use RFC 3227 Order of Volatility as guideline
- Repeatable (scripted) process
  - Recreate steps at a later date
  - Avoids missing steps
  - Train new members quickly
  - Rapid remote deployment

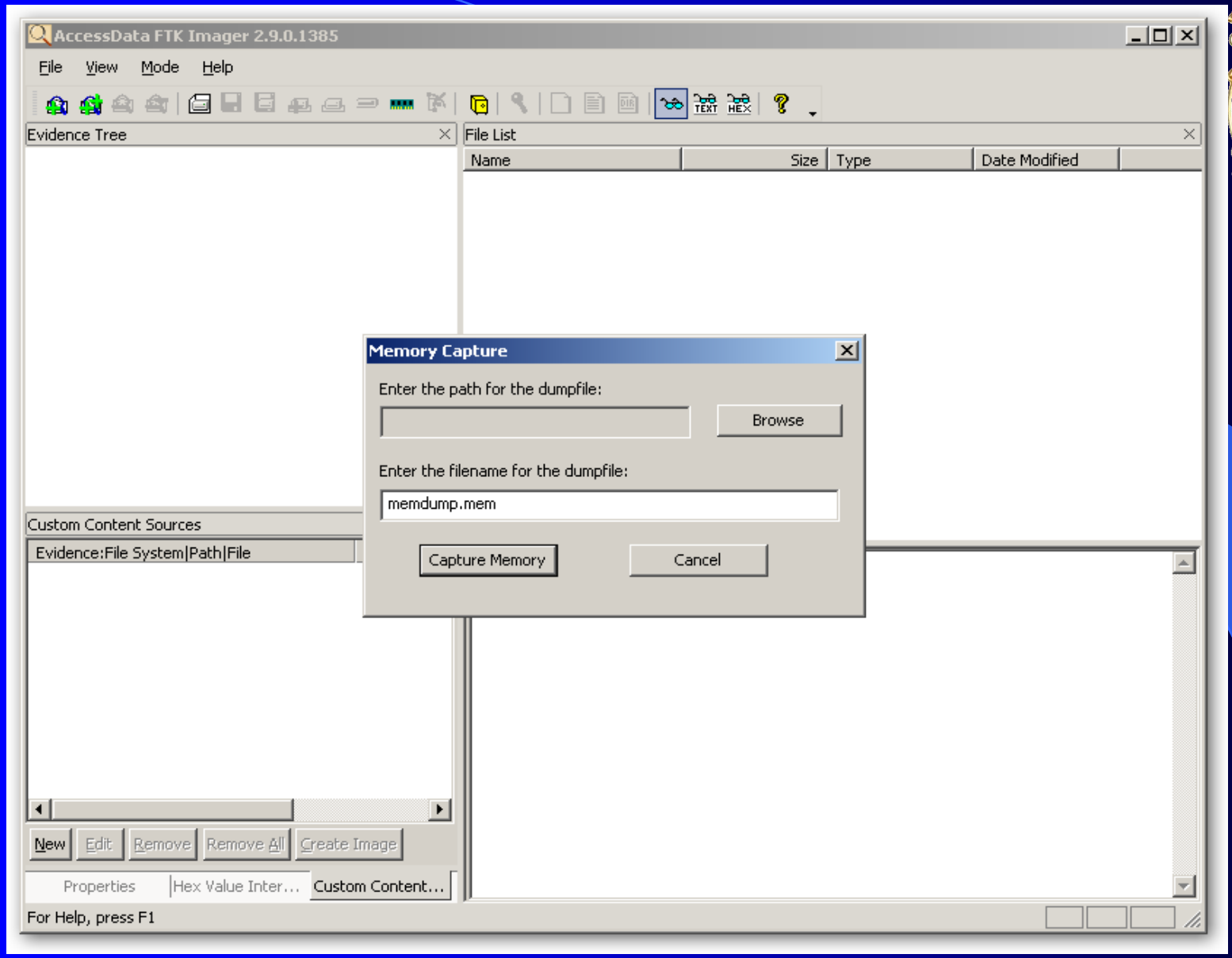
- RAM Collection – Winen
  - Created by Guidance Software
    - Large forensic firm
    - Numerous in-house developers
  - Included on Helix CD
  - Allows for case metadata


Recycle Bin
SATx
HELIX2009R1 (01/06/2009)
File Quick Launch Page Help
HELIX ™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
RAM Acquisition
HELIX Forensic Command Shell
Ctrl-D for Directory or Ctrl-F for filename completion
The Shell Path has been modified to find trusted cdrom binaries first
Do not navigate away from the CD drive letter.
8:00:31.60 D:\IR\RAM\winen> type winen.txt
#Guidance Software, Inc.
#WinEn Configuration File (Max Config File size = 32768 characters)
#Syntax: "OptionName=Value"
#EvidencePath (*Required)
#Path AND Filename of the evidence file to be created
EvidencePath=
#Compress (*Required)
#Level of compression (0=none, 1=fast, 2=best)
Compress=
#Examiner (*Required)
#Examiners name
Examiner=
#EvidenceName (*Required)
#Name of the evidence within the evidence file
EvidenceName=
#CaseNumber (*Required)
#Case Number related to the evidence
CaseNumber=
#EvidenceNumber (*Required)
#Evidence Number
EvidenceNumber=
#MaxFileSize (Optional, Default=640)
#Max file size of each evidence file segment in MB (Min=1)
MaxFileSize=
#Granularity (Optional, Default=1)
#Error granularity in sectors (Min=1, Max=1024)
Granularity=
ance
TWARE
Winen
Version 6.12.0.44
ory DD
Mantech MDD
Version 1.3
Matthieu Suiche win32dd
Version 1.2.1.20090106
Page 3 of 3
start
HELIX Forensic Comm...
8:01 AM

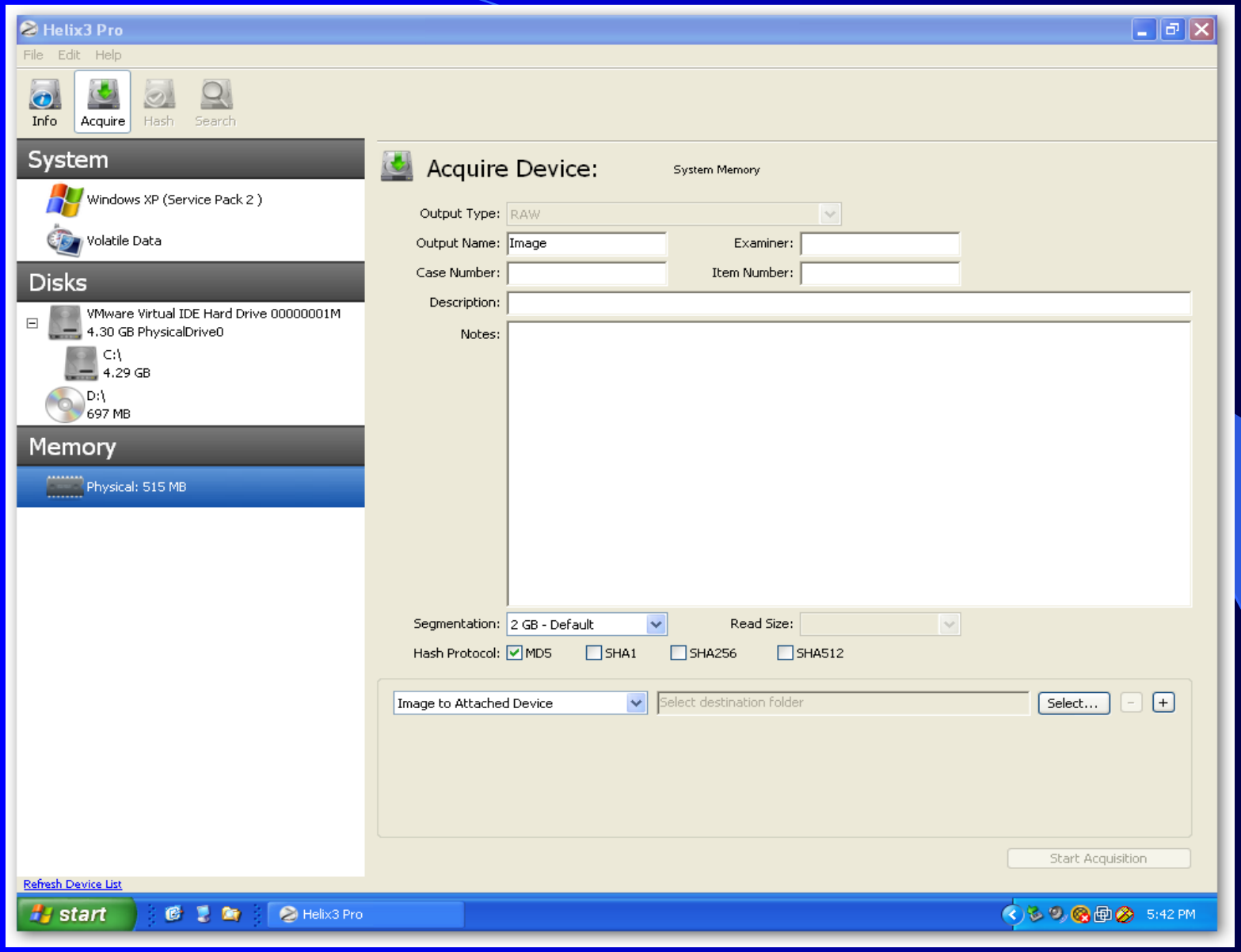
- RAM Collection – MDD
  - Created by ManTech International
  - Included on Helix CD
  - Some known issues
    - 2008 Server
    - Windows Vista/7


Recycle Bin
Shortcut to pySAT_GUI
Windows Explorer
SATx
Ethereal
FTK Imager
Notepad++
WinSnap.exe
HELIX2009R1 (01/06/2009)
File Quick Launch Page Help
HELIX 3 INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Live RAM Acquisition
Guidance SOFTWARE
Winen
Version 6.12.0.44
Memory DD
Mantech MDD
Version 1.3
Matthieu Suiche win32dd
Version 1.2.1.20090106
Page 3 of 3
HELIX Forensic Command Shell
Ctrl-D for Directory or Ctrl-F for filename completion
The Shell Path has been modified to find trusted cdrom binaries first
Do not navigate away from the CD drive letter.
17:52:14.46 D:\IR\RAM\MDD> type mddusage.txt
mdd ManTech Physical Memory Dump Utility
Usage:
mdd <-o OUTPUTFILE> [-qcw]
-o OUTPUTFILE output file for dump
-q quiet; no output except on error
-v verbose; output offsets of failed mappings
-c redistribution conditions for GPL
-w warranty information for GPL
17:52:31.81 D:\IR\RAM\MDD> _
start
HELIX Forensic Comm...
5:52 PM

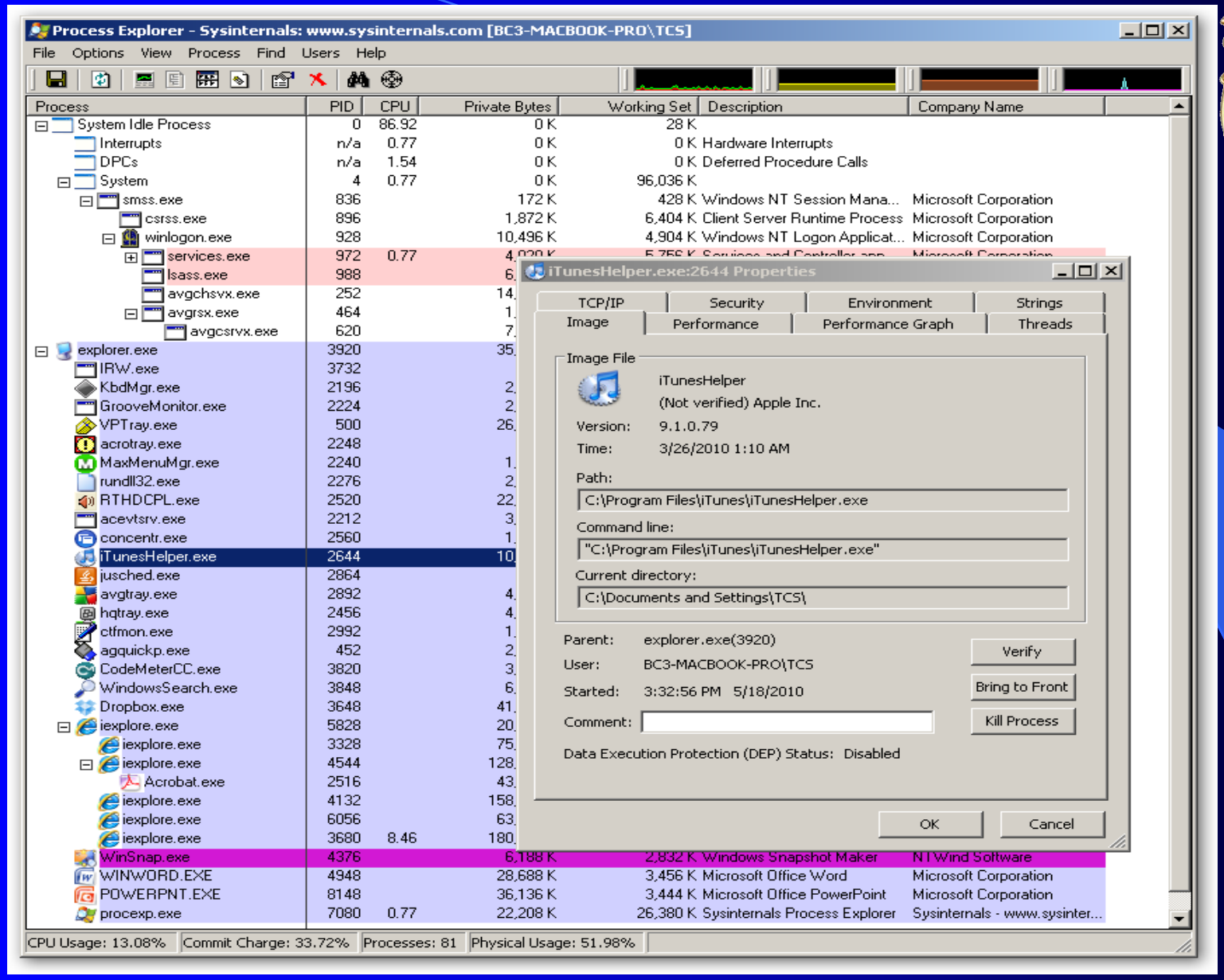
- RAM Collection – FTK Imager 2.9
  - Created by AccessData
    - Large forensic firm
    - Numerous in-house developers
  - *Not included on Helix CD (2.5.3)*
    - Current version on Helix doesn't support RAM


AccessData FTK Imager 2.9.0.1385
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Memory Capture
Enter the path for the dumpfile:
Browse
Enter the filename for the dumpfile:
memdump.mem
Capture Memory
Cancel
Custom Content Sources
Evidence:File System|Path|File
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Content...
For Help, press F1

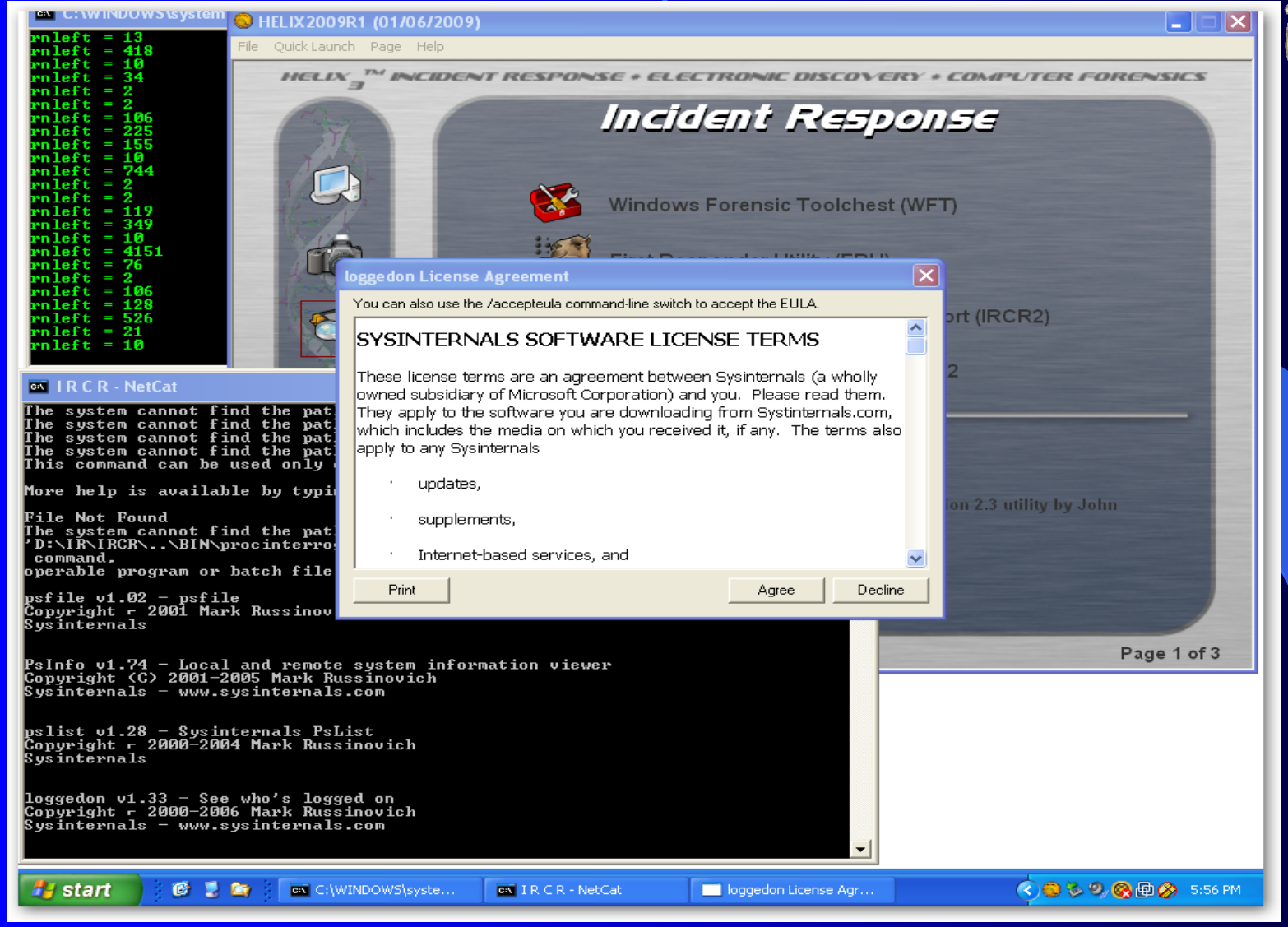
- RAM Collection – Helix Pro
  - Created by e-fense
    - Makers of Helix forensic CDs
    - Well known in IR community
  - Flexible output
    - Attached drive
    - Networked to system running Helix Pro receiver
  - Paid subscription required


Helix3 Pro
File Edit Help
Info
Acquire
Hash
Search
System
Windows XP (Service Pack 2)
Volatile Data
Disks
VMware Virtual IDE Hard Drive 00000001M
4.30 GB PhysicalDrive0
C:\
4.29 GB
D:\
697 MB
Memory
Physical: 515 MB
Acquire Device:
System Memory
Output Type: RAW
Output Name: Image
Examiner:
Case Number:
Item Number:
Description:
Notes:
Segmentation: 2 GB - Default
Read Size:
Hash Protocol: MD5 SHA1 SHA256 SHA512
Image to Attached Device
Select destination folder
Select...
Start Acquisition
Refresh Device List
start
Helix3 Pro
5:42 PM

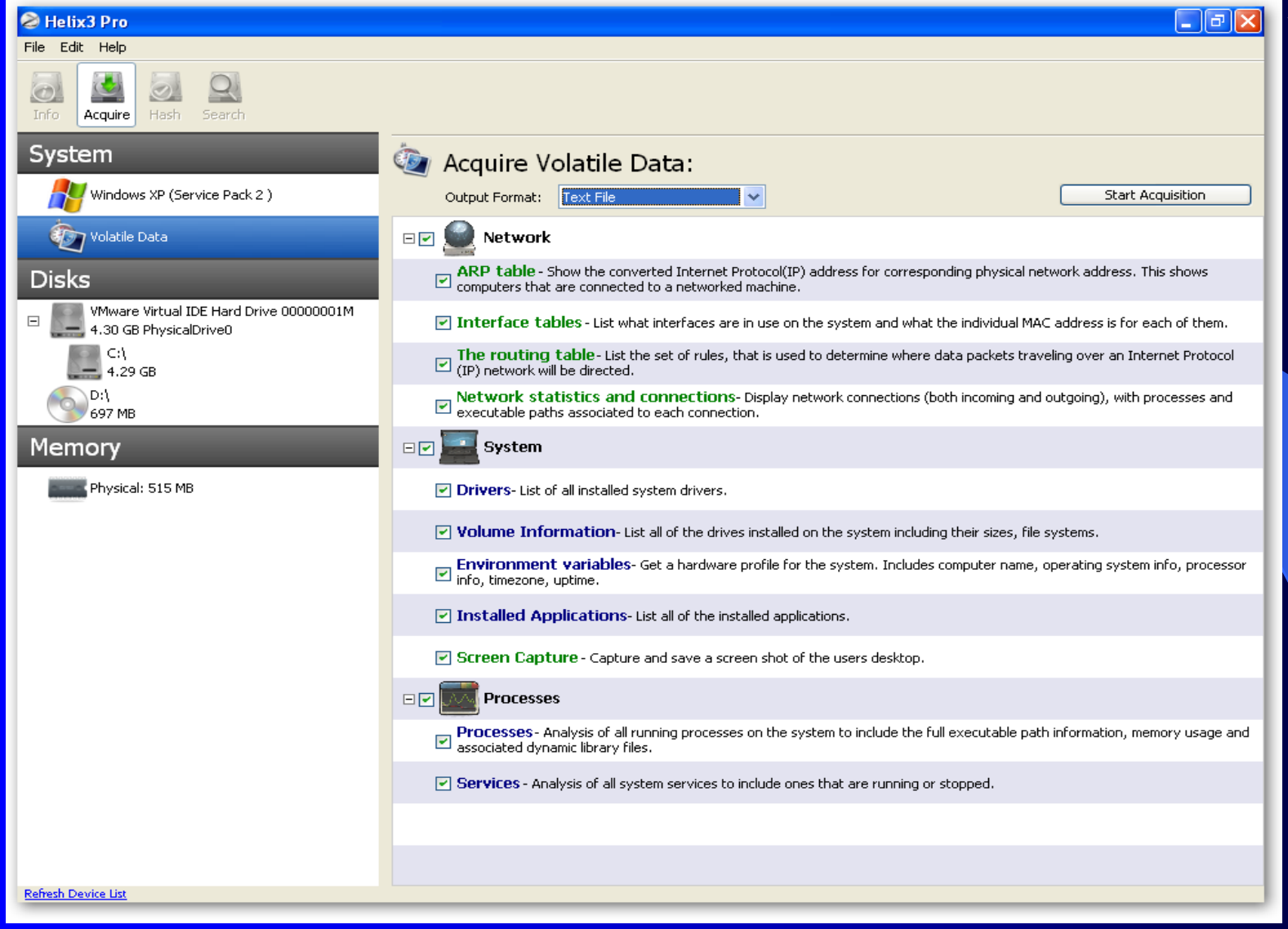
- Volatile Data Collection – Sysinternals
  - Purchase by Microsoft
    - Created by Mark Russinovich
    - Long use in IR community
  - Numerous capabilities
    - Command line tools
    - GUI tools


Process Explorer - Sysinternals: www.sysinternals.com [BC3-MACBOOK-PRO\TCS]
File Options View Process Find Users Help
Process PID CPU Private Bytes Working Set Description Company Name
System Idle Process 0 86.92 0 K 28 K
Interrupts n/a 0.77 0 K 0 K Hardware Interrupts
DPCs n/a 1.54 0 K 0 K Deferred Procedure Calls
System 4 0.77 0 K 96,036 K
smss.exe 836 172 K 428 K Windows NT Session Mana... Microsoft Corporation
csrss.exe 896 1,872 K 6,404 K Client Server Runtime Process Microsoft Corporation
winlogon.exe 928 10,496 K 4,904 K Windows NT Logon Applicat... Microsoft Corporation
services.exe 972 0.77
lsass.exe 988
avgchsvx.exe 252
avgrsx.exe 464
avgcsrvx.exe 620
explorer.exe 3920
IRW.exe 3732
KbdMgr.exe 2196
GrooveMonitor.exe 2224
VPTray.exe 500
acrotray.exe 2248
MaxMenuMgr.exe 2240
rundll32.exe 2276
RTHDCPL.exe 2520
acevtsrv.exe 2212
concentr.exe 2560
iTunesHelper.exe 2644
jusched.exe 2864
avgtray.exe 2892
hqtray.exe 2456
ctfmon.exe 2992
agquickp.exe 452
CodeMeterCC.exe 3820
WindowsSearch.exe 3848
Dropbox.exe 3648
iexplore.exe 5828
iexplore.exe 3328
iexplore.exe 4544
Acrobat.exe 2516
iexplore.exe 4132
iexplore.exe 6056
iexplore.exe 3680 8.46
WinSnap.exe 4376 6,188 K 2,832 K Windows Snapshot Maker NTWind Software
WINWORD.EXE 4948 28,688 K 3,456 K Microsoft Office Word Microsoft Corporation
POWERPNT.EXE 8148 36,136 K 3,444 K Microsoft Office PowerPoint Microsoft Corporation
procexp.exe 7080 0.77 22,208 K 26,380 K Sysinternals Process Explorer Sysinternals - www.sysinter...
CPU Usage: 13.08% Commit Charge: 33.72% Processes: 81 Physical Usage: 51.98%
iTunesHelper.exe:2644 Properties
TCP/IP Security Environment Strings
Image Performance Performance Graph Threads
Image File
iTunesHelper
(Not verified) Apple Inc.
Version: 9.1.0.79
Time: 3/26/2010 1:10 AM
Path:
C:\Program Files\iTunes\iTunesHelper.exe
Command line:
"C:\Program Files\iTunes\iTunesHelper.exe"
Current directory:
C:\Documents and Settings\TCS\
Parent: explorer.exe(3920)
User: BC3-MACBOOK-PRO\TCS
Started: 3:32:56 PM 5/18/2010
Comment:
Data Execution Protection (DEP) Status: Disabled
Verify
Bring to Front
Kill Process
OK
Cancel

- Volatile Data Collection – IRCR
  - Included on Helix CD
  - Scripted data collection
    - Output to a netcat listener
    - Large text file
  - Numerous interactive messages
    - Need to monitor while running
    - Sysinternals EULAs on screen


rnleft = 13
rnleft = 418
rnleft = 10
rnleft = 34
rnleft = 2
rnleft = 2
rnleft = 106
rnleft = 225
rnleft = 155
rnleft = 10
rnleft = 744
rnleft = 2
rnleft = 2
rnleft = 119
rnleft = 349
rnleft = 10
rnleft = 4151
rnleft = 76
rnleft = 2
rnleft = 106
rnleft = 128
rnleft = 526
rnleft = 21
rnleft = 10
HELIX2009R1 (01/06/2009)
File Quick Launch Page Help
HELIX3™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Incident Response
Windows Forensic Toolchest (WFT)
loggedon License Agreement
You can also use the /accepteula command-line switch to accept the EULA.
SYSINTERNALS SOFTWARE LICENSE TERMS
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals
updates,
supplements,
Internet-based services, and
Print
Agree
Decline
Page 1 of 3
I R C R - NetCat
The system cannot find the pat
The system cannot find the pat
The system cannot find the pat
The system cannot find the pat
This command can be used only
More help is available by typi
File Not Found
The system cannot find the pat
'D:\IR\IRCR\..\BIN\procinterro
command,
operable program or batch file
psfile v1.02 - psfile
Copyright r 2001 Mark Russinov
Sysinternals
PsInfo v1.74 - Local and remote system information viewer
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com
pslist v1.28 - Sysinternals PsList
Copyright r 2000-2004 Mark Russinovich
Sysinternals
loggedon v1.33 - See who's logged on
Copyright r 2000-2006 Mark Russinovich
Sysinternals - www.sysinternals.com
start
C:\WINDOWS\syste...
I R C R - NetCat
loggedon License Agr...
5:56 PM

- Volatile Data Collection – Helix Pro
  - Simple GUI interface
  - Flexible output
    - Attached drive
    - Networked to system running Helix Pro receiver
  - Paid subscription required


Helix3 Pro
File Edit Help
Info
Acquire
Hash
Search
System
Windows XP (Service Pack 2)
Volatile Data
Disks
VMware Virtual IDE Hard Drive 00000001M
4.30 GB PhysicalDrive0
C:\
4.29 GB
D:\
697 MB
Memory
Physical: 515 MB
Refresh Device List
Acquire Volatile Data:
Output Format:
Text File
Start Acquisition
Network
ARP table - Show the converted Internet Protocol(IP) address for corresponding physical network address. This shows computers that are connected to a networked machine.
Interface tables - List what interfaces are in use on the system and what the individual MAC address is for each of them.
The routing table - List the set of rules, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed.
Network statistics and connections - Display network connections (both incoming and outgoing), with processes and executable paths associated to each connection.
System
Drivers - List of all installed system drivers.
Volume Information - List all of the drives installed on the system including their sizes, file systems.
Environment variables - Get a hardware profile for the system. Includes computer name, operating system info, processor info, timezone, uptime.
Installed Applications - List all of the installed applications.
Screen Capture - Capture and save a screen shot of the users desktop.
Processes
Processes - Analysis of all running processes on the system to include the full executable path information, memory usage and associated dynamic library files.
Services - Analysis of all system services to include ones that are running or stopped.

- Volatile Data Collection – e-fense
  - Live Response/Aperio
    - USB drive based
    - Automated collection and storage

- Live Response/Aperio
  - Automated collection =“Agent Proof”

  - Centralized analysis console

Triage

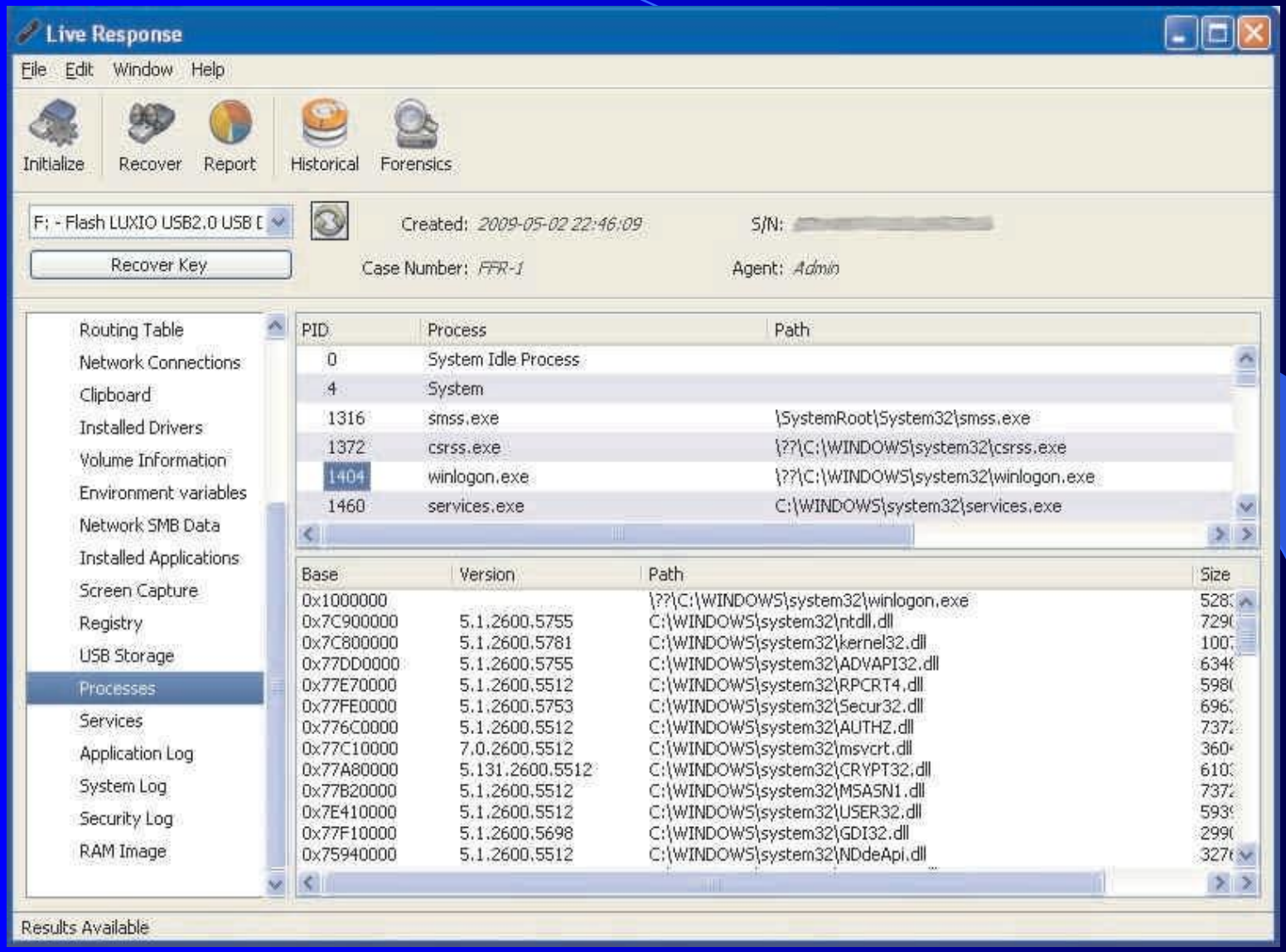
- Collection was Initial Challenge

- New Challenge – Rapid Analysis
  - Quickly aggregate and compare data
  - Still labor intensive
  - Aspects of interest
    - What ports connected
    - IP addresses utilized
    - Processes (names, sources, utilization)
    - Find a commonality

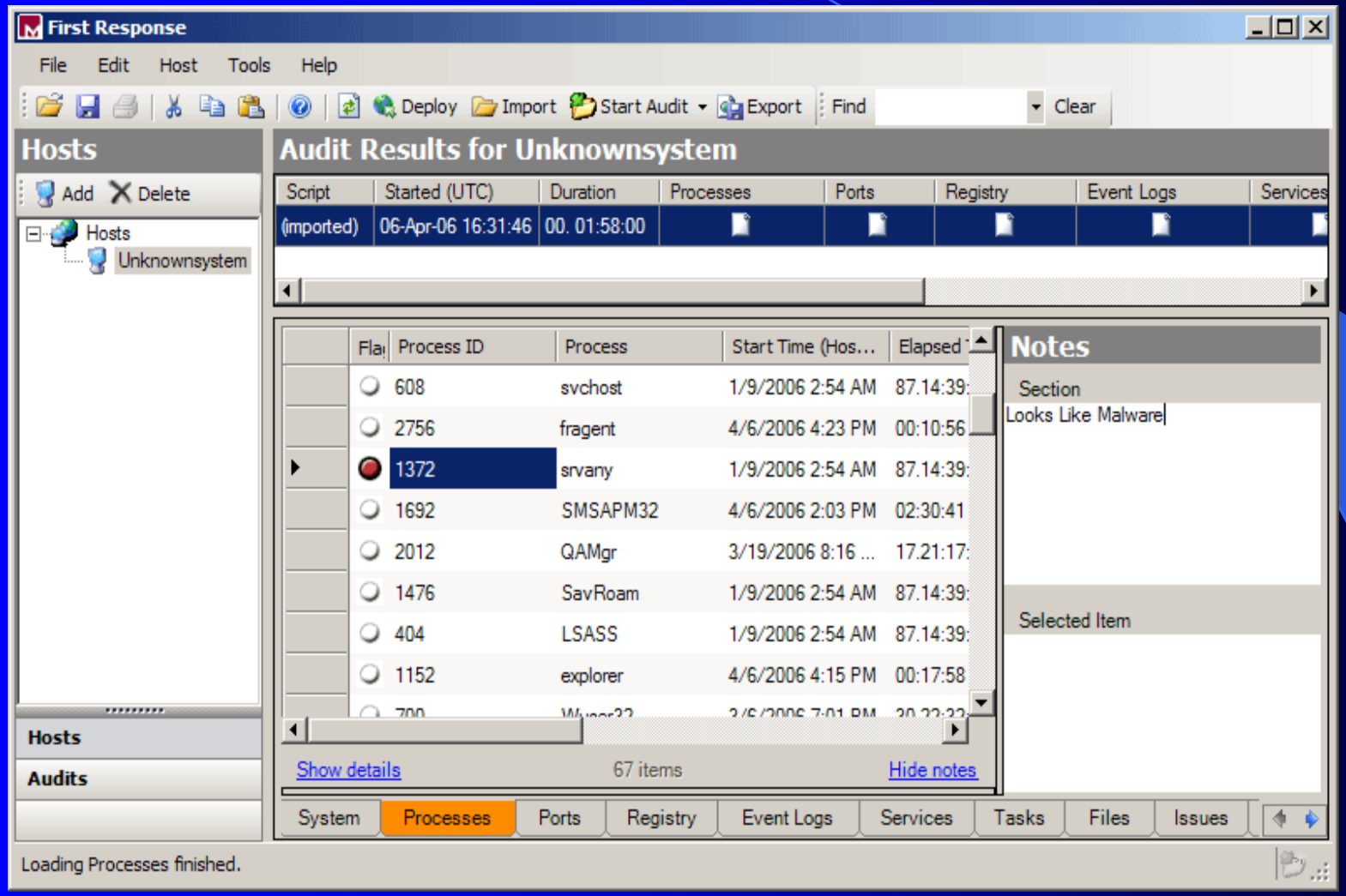
- Enterprise Level Platforms
  - Have hook into systems
  - Common output/reporting
  - No need for physical access to computer
  - Pre-deployed agent
  - Require network access to system
  - Ensure agent is working and communicating

- Non-Enterprise Level
  - Much more challenging
  - Need collection/analysis tools
  - Requires physical access to systems

- Triage Tools- Live Response/Aperio
  - Centralized collection
  - Easy to run multiple cases concurrently
  - Comparison between systems cumbersome
  - Extensive reports


Live Response
File Edit Window Help
Initialize
Recover
Report
Historical
Forensics
F: - Flash LUXIO USB2.0 USB D
Created: 2009-05-02 22:46:09
S/N:
Recover Key
Case Number: FFR-1
Agent: Admin
Routing Table
Network Connections
Clipboard
Installed Drivers
Volume Information
Environment variables
Network SMB Data
Installed Applications
Screen Capture
Registry
USB Storage
Processes
Services
Application Log
System Log
Security Log
RAM Image
PID Process Path
0 System Idle Process
4 System
1316 smss.exe \SystemRoot\System32\smss.exe
1372 csrss.exe \??\C:\WINDOWS\system32\csrss.exe
1404 winlogon.exe \??\C:\WINDOWS\system32\winlogon.exe
1460 services.exe C:\WINDOWS\system32\services.exe
Base Version Path Size
0x1000000 \??\C:\WINDOWS\system32\winlogon.exe
0x7C900000 5.1.2600.5755 C:\WINDOWS\system32\ntdll.dll
0x7C800000 5.1.2600.5781 C:\WINDOWS\system32\kernel32.dll
0x77DD0000 5.1.2600.5755 C:\WINDOWS\system32\ADVAPI32.dll
0x77E70000 5.1.2600.5512 C:\WINDOWS\system32\RPCRT4.dll
0x77FE0000 5.1.2600.5753 C:\WINDOWS\system32\Secur32.dll
0x776C0000 5.1.2600.5512 C:\WINDOWS\system32\AUTHZ.dll
0x77C10000 7.0.2600.5512 C:\WINDOWS\system32\msvcrt.dll
0x77A80000 5.131.2600.5512 C:\WINDOWS\system32\CRYPT32.dll
0x77B20000 5.1.2600.5512 C:\WINDOWS\system32\MSASN1.dll
0x7E410000 5.1.2600.5512 C:\WINDOWS\system32\USER32.dll
0x77F10000 5.1.2600.5698 C:\WINDOWS\system32\GDI32.dll
0x75940000 5.1.2600.5512 C:\WINDOWS\system32\NDdeApi.dll
Results Available

- Triage Tools - Mandiant First Response
  - Centralized collection
    - Pre-deployed agents
    - Individual system collection
  - Easy comparison between systems
    - Compare specific aspects
      - Processes
      - Ports
    - Ability to add analysis notes to file


First Response
File Edit Host Tools Help
Deploy Import Start Audit Export Find Clear
Hosts
Add Delete
Hosts
Unknownsystem
Audit Results for Unknownsystem
Script Started (UTC) Duration Processes Ports Registry Event Logs Services
(imported) 06-Apr-06 16:31:46 00. 01:58:00
Fla Process ID Process Start Time (Hos... Elapsed
608 svchost 1/9/2006 2:54 AM 87.14:39:
2756 fragent 4/6/2006 4:23 PM 00:10:56
1372 srvany 1/9/2006 2:54 AM 87.14:39:
1692 SMSAPM32 4/6/2006 2:03 PM 02:30:41
2012 QAMgr 3/19/2006 8:16 ... 17.21:17:
1476 SavRoam 1/9/2006 2:54 AM 87.14:39:
404 LSASS 1/9/2006 2:54 AM 87.14:39:
1152 explorer 4/6/2006 4:15 PM 00:17:58
Notes
Section
Looks Like Malware
Selected Item
Show details
67 items
Hide notes
System Processes Ports Registry Event Logs Services Tasks Files Issues
Hosts
Audits
Loading Processes finished.

Final Thoughts

- Identify Commonalities between Attacks
  - Tie attacks together
  - Determine Modus Operandi
  - Create profile
- Trace Attacks to Common Sources
  - IPs
  - Servers
  - Controllers

- Gather Info at Service Provider Level
  - 2703(f) Preservation Letters
    - Provides time to get Court Order
    - Notifies service provider of intent
  - 2703(d) Disclosure
    - Provides customer communications
    - Provides customer records

- Use Info Gathered
  - Profile of attack and user data
    - Determine attribution
    - Attempt to serve warrant on individual(s)
    - Present case for prosecution - Federal Court System
  - Share information with LE partners
    - Gather history on person or group
    - Provide common threat picture

- Work with Cyber Security
  - CS knows systems, networks, processes best
  - Don't want to be stumbling block in process
  - Augment process by running parallel with copy of evidence
    - Provide attribution when possible
    - Provide deterrent
    - De-conflict with
      - FBI, USSS, DOD, ICE
      - CI and Intel elements

Questions?