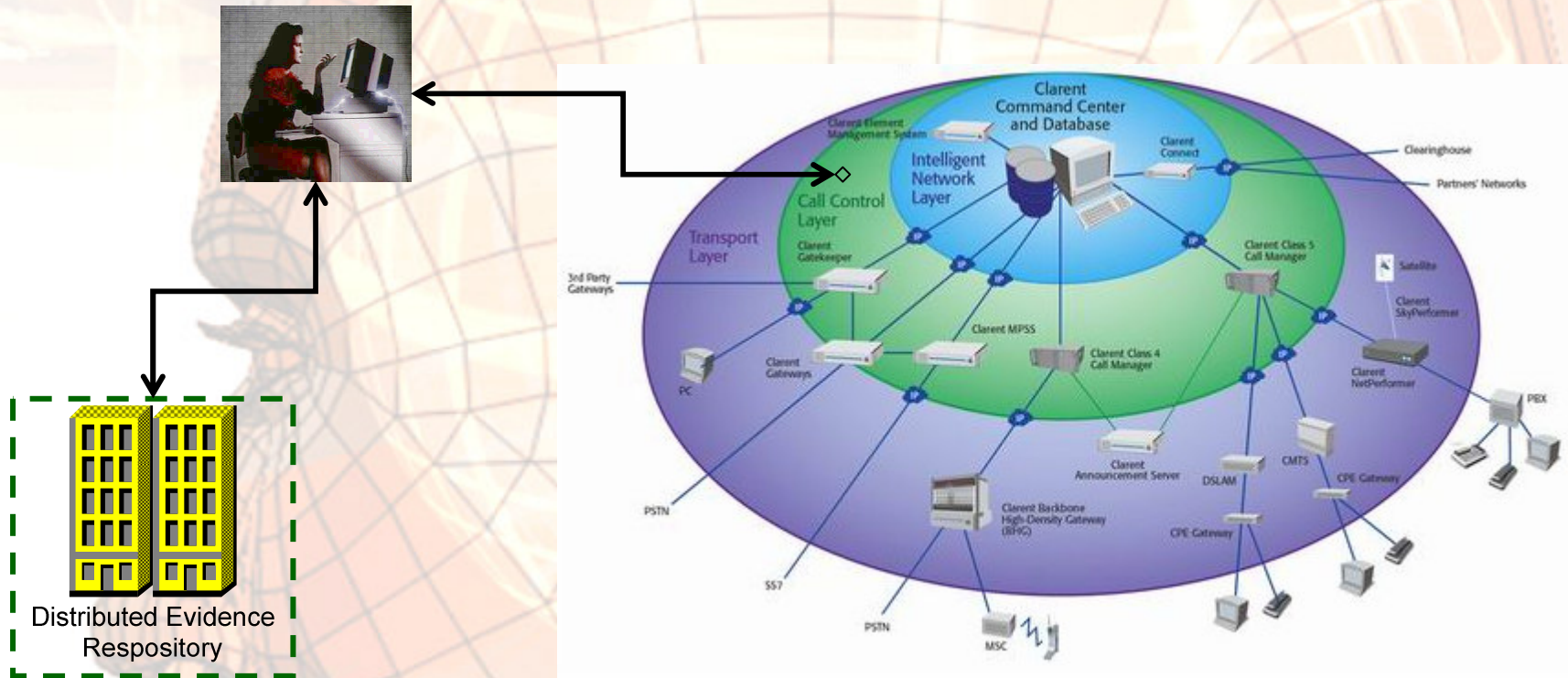


On-Demand “Live” Investigations

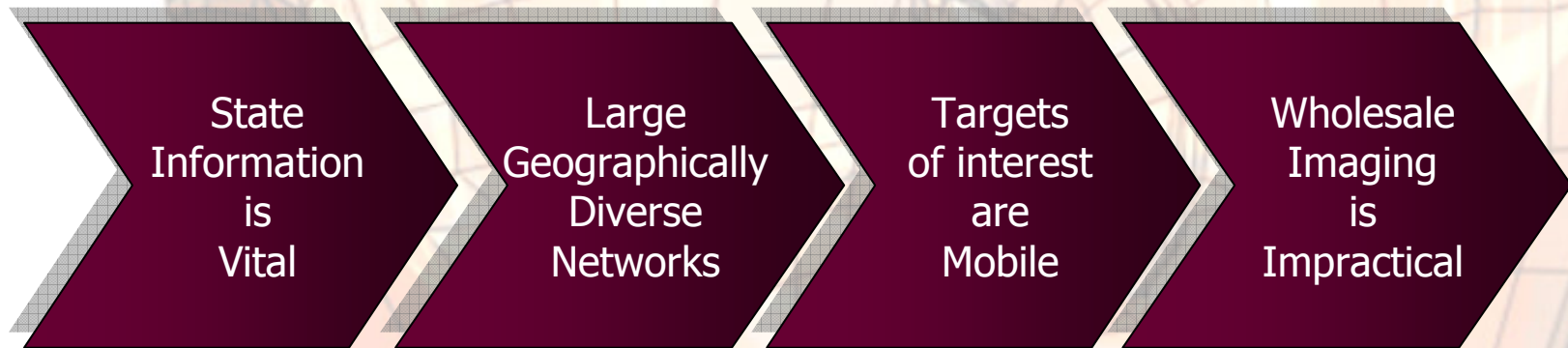
October 2007

On Demand Live Investigation



“On Demand acquisition, analysis and investigation of “live” running network devices”

Why “Live” Investigation?



Why “Live” Investigation?



The Best Evidence Rule

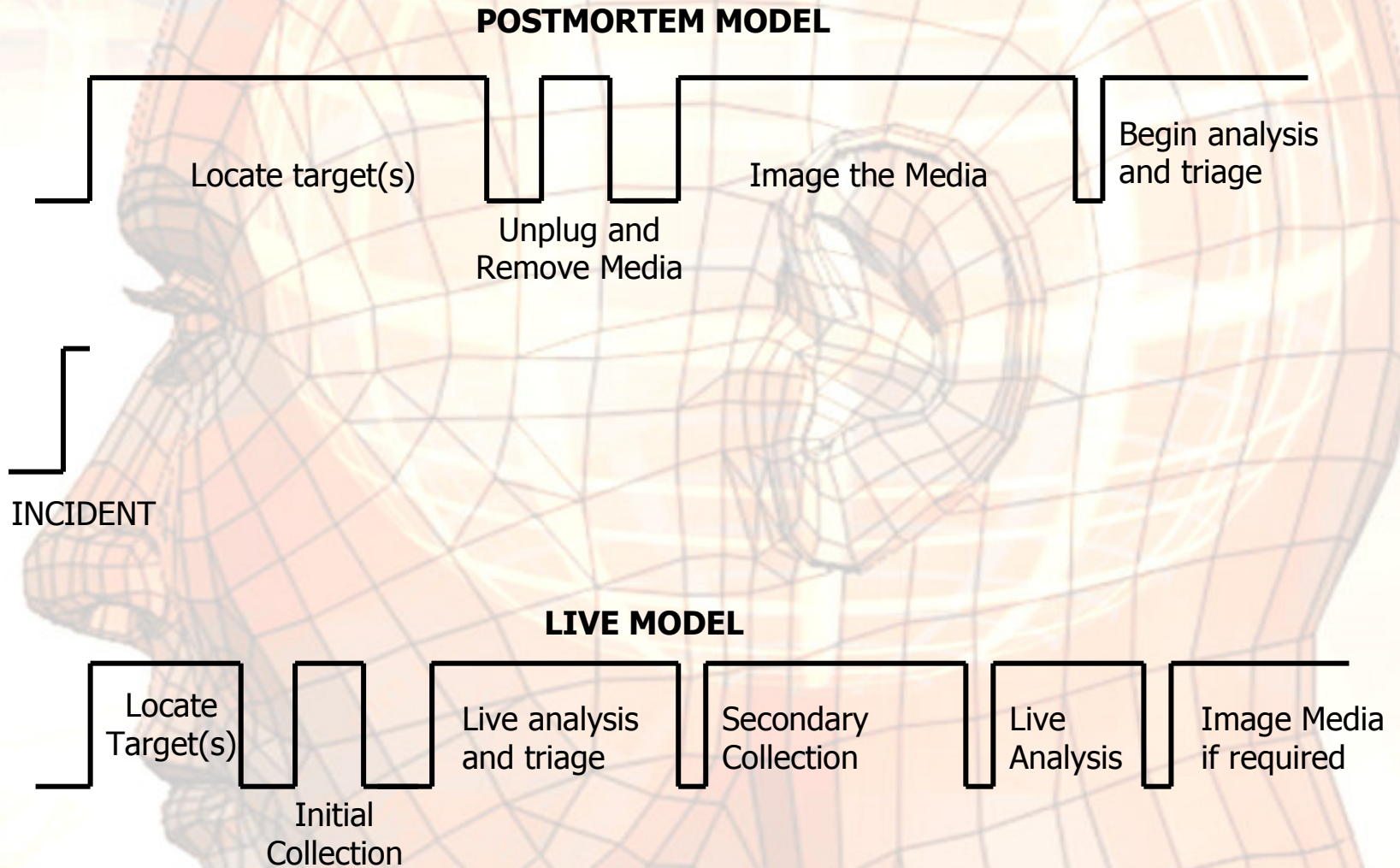
The **best evidence rule** is a common law rule of evidence which can be traced back at least as far as the 18th century. In *Omychund v Barker* (1745) 1 Atk, 21, 49; 26 ER 15, 33, Lord Harwicke stated that no evidence was admissible unless it was "the best that the nature of the case will allow". The general rule is that secondary evidence, such as a copy or facsimile, will be not admissible if an original document is available.¹

The Best Evidence Rule

- The term "writing" has been liberally interpreted to include photographs, [x-rays](#), films and digital evidence i.e. physical (bit stream) copies of hard drives.
- The question is where does Live On Demand Investigation fall?

"L I V E"

Investigation Timeline



Live Investigation Considerations

Full Real-Time Encryption

- Microsoft BitLocker
- TrueCrypt (Windows and Linux)

Solid State and Portable Media

- USB
- U3 Smart Drive

- Remote File Storage

- Xdrive® 50GB \$9.95 / month
- FlipDrive™ 100GB \$199/Year

Live Data

Memory Resident Data

- Caches
- Program Remnants
- System Remnants

Memory Resident Programs

- Applications/State
- Memory resident malware (rootkits, keyloggers, etc)

• Peripheral Interrogation

– IO Control

- IRP_MJ_READ
- IRP_MJ_DEVICE_CONTROL
- IRP_MJ_INTERNAL_DEVICE_CONTROL

Live Data

- **Memory Resident Data**
 - State information that has the potential to place a user at the keyboard of a system
 - Recent document access
 - Loaded content
 - Handle access
 - Photographs, documents, etc
 - Recently attached devices
 - Volume labels
 - Device descriptors
 - Adaptor descriptors

Live Data

- Live investigations are not just based on volatile data
- USB example:

Device Serial Number

```
##?#USBSTOR#CdRom&Ven_SanDisk&Prod_U3_Titanium&Rev_2.16#0000060412049121&1#{1186654d-47b8-48b9-beb9-7df113ae3c67}
```

- Registry holds the serial number of currently attached or previously attach USB Drive
- Early determination of environment can significantly impact investigation's course

Live Data

- Peripheral Interrogation
 - Attached peripherals can be queried directly using ioctl calls
 - USB Controllers
 - IOCTL_USB_GET_ROOT_HUB_NAME
 - IOCTL_USB_GET_NODE_INFORMATION
 - IOCTL_USB_GET_DESCRIPTOR_FROM_NODE_CONNECTION
 - Etc
 - Some devices support proprietary ioctl codes
 - i.e. IRP_MJ_DEVICE_CONTROL

Live Data

- Peripheral Interrogation
 - Peripheral information is maintained through the registry
 - Device I/O calls can augment information in the registry
 - Device I/O calls can support registry-resident data
 - Discrepancies between live data and disk data can indicate tampering and/or rootkit presence

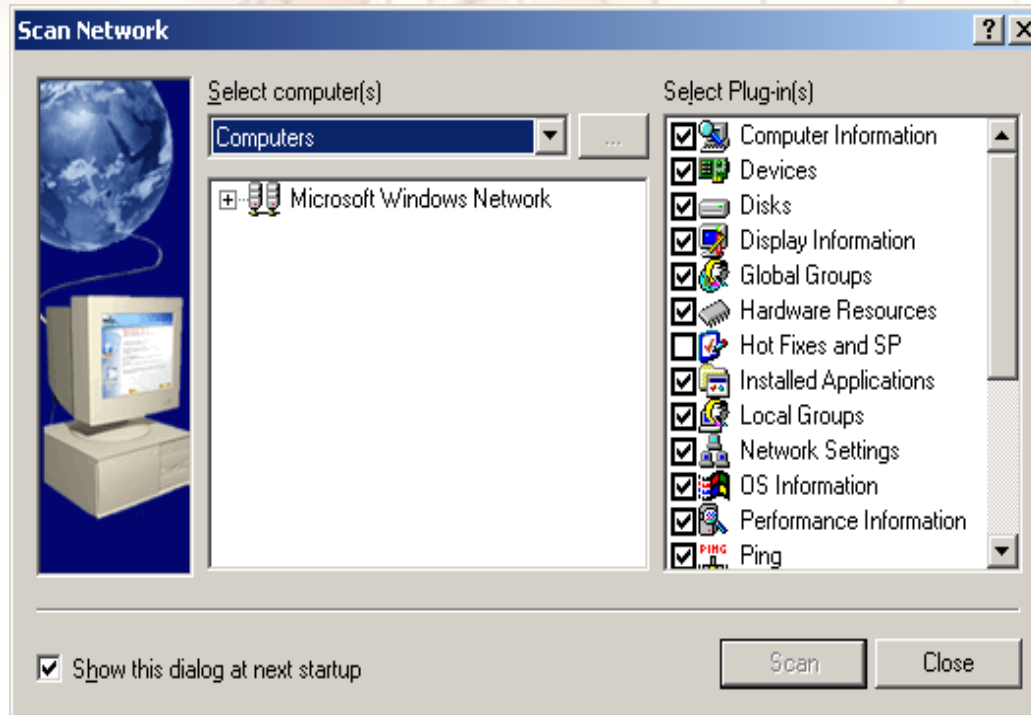
Live Data

- Rootkits
 - Rootkits can hide almost any information from a live investigation tool
 - Rootkits can be installed at different layers and can vary in sophistication
 - Combining a sophisticated rootkit with encrypted storage can present a very difficult situation for investigators
 - However, some rootkits may only have a memory signature
 - Live investigation may be the only opportunity to find some rootkits

Live Tools

- Commercial offerings
- Free Tools
 - Incident Response Collection Report (IRCS)
 - First Responders Evidence Disk (FRED)
 - Windows Forensic Toolchest (WFT)
 - Computer Online Forensic Evidence Extractor (COFEE)
 - Microsoft's SysInternals
 - WinHex
- DFRWS 2006 Paper by Ricci leong
(http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/)

Active Network Monitor



- Provides system administrators the ability to examine any computer on a network
- Requires administrative credentials
- Runs on Windows NT/2000/XP
- Gathers information on any operating system Windows 95 and newer

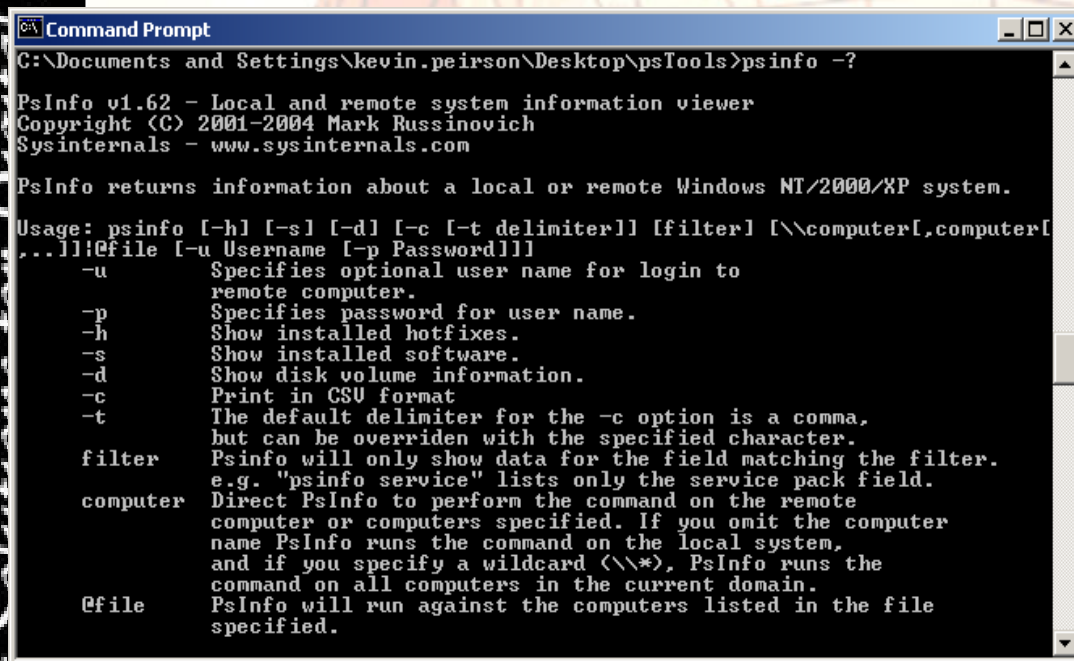
Volatools

```
C:\WINDOWS\system32\cmd.exe
C:\VolatoolsBasic-1.0.0>
C:\VolatoolsBasic-1.0.0>
C:\VolatoolsBasic-1.0.0>
C:\VolatoolsBasic-1.0.0>
C:\VolatoolsBasic-1.0.0>
C:\VolatoolsBasic-1.0.0>C:\Python25\python.exe volatools pslist -f "C:\2.dat"
Name      Pid      PPid     Thds     Hnds     Time
Idle      0        0        0        416     Thu Jan 01 00:00:00 1970
System    4        0        58       416     Thu Jan 01 00:00:00 1970
smss.exe  548      4        3        21      Tue Jul 10 19:57:40 2007
csrss.exe 612      548     12       399     Tue Jul 10 19:57:45 2007
winlogon.exe 636     548     19       504     Tue Jul 10 19:57:45 2007
services.exe 680     636     21       403     Tue Jul 10 19:57:45 2007
lsass.exe 692      636     24       356     Tue Jul 10 19:57:46 2007
svchost.exe 848     680     17       228     Tue Jul 10 19:57:46 2007
svchost.exe 912     680     11       255     Tue Jul 10 19:57:46 2007
svchost.exe 1004    680     68      1199    Tue Jul 10 19:57:46 2007
svchost.exe 1048    680     6        82      Tue Jul 10 19:57:47 2007
svchost.exe 1108    680     14       208     Tue Jul 10 19:57:47 2007
spoolsv.exe 1404    680     11       110     Tue Jul 10 19:57:49 2007
explorer.exe 1628   1568    16       571     Tue Jul 10 19:57:49 2007
mscorsvw.exe 1776   680     3        49      Tue Jul 10 19:57:52 2007
UMwareTray.exe 1836  1628    2        27      Tue Jul 10 19:57:53 2007
UMwareUser.exe 1844  1628    2        42      Tue Jul 10 19:57:53 2007
hasplms.exe 1904    680     7        79      Tue Jul 10 19:57:55 2007
UMwareService.e 2012   680     3        43      Tue Jul 10 19:57:55 2007
wscntfy.exe 608    1004    1        27      Tue Jul 10 19:57:58 2007
alg.exe   736    680     6       104     Tue Jul 10 19:58:00 2007
cmd.exe   3968   1628    1        30      Fri Jul 13 14:41:09 2007
mshta.exe 356    660     8       241     Fri Jul 13 14:42:16 2007
mmc.exe   2392   1628    5       180     Fri Jul 13 14:44:08 2007
wmipruse.exe 3304  848     8       185     Fri Jul 13 14:45:09 2007

C:\VolatoolsBasic-1.0.0>C:\Python25\python.exe volatools files -f "C:\2.dat" > f
iles.txt
C:\VolatoolsBasic-1.0.0>_
```

- ❑ Performs digital investigations against acquired memory images
- ❑ Pulls the following information out of acquired memory images: date and time, running processes, open network sockets, open network connections, open dll's, open files for each process, and OS kernel modules

PsInfo



```
Command Prompt
C:\Documents and Settings\kevin.peirson\Desktop\psTools>psinfo -?

PsInfo v1.62 - Local and remote system information viewer
Copyright (C) 2001-2004 Mark Russinovich
Sysinternals - www.sysinternals.com

PsInfo returns information about a local or remote Windows NT/2000/XP system.

Usage: psinfo [-h] [-s] [-d] [-c [-t delimiter]] [filter] [\computer[,computer[
...]]]@file [-u Username [-p Password]]
  -u      Specifies optional user name for login to
          remote computer.
  -p      Specifies password for user name.
  -h      Show installed hotfixes.
  -s      Show installed software.
  -d      Show disk volume information.
  -c      Print in CSU format
  -t      The default delimiter for the -c option is a comma,
          but can be overridden with the specified character.
  filter  Psinfo will only show data for the field matching the filter.
          e.g. "psinfo service" lists only the service pack field.
  computer Direct PsInfo to perform the command on the remote
          computer or computers specified. If you omit the computer
          name PsInfo runs the command on the local system,
          and if you specify a wildcard (\\*), PsInfo runs the
          command on all computers in the current domain.
  @file   PsInfo will run against the computers listed in the file
          specified.
```

- ❑ Provides detailed information about a target machine
- ❑ Types of information include type of installation, kernel build, registered organization and owner, number of processors and their type, memory size, the install date of the system, installed hot fixes and software applications

PsList

```
Command Prompt
C:\Documents and Settings\kevin.peirson\Desktop\psTools>pslist -?

PsList 1.26 - Process Information Lister
Copyright (C) 1999-2004 Mark Russinovich
Sysinternals - www.sysinternals.com

Usage: pslist [-d][-m][-x][-t][-s [n]] [-r n] [\computer [-u username][-p passwo
rd]]name[:pid]
  -d          Show thread detail.
  -m          Show memory detail.
  -x          Show processes, memory information and threads.
  -t          Show process tree.
  -s [n]     Run in task-manager mode, for optional seconds specified.
             Press Escape to abort.
  -r n       Task-manager mode refresh rate in seconds (default is 1).
  \computer  Specifies remote computer.
  -u         Optional user name for remote login.
  -p         Optional password for remote login. If you don't present
             on the command line pslist will prompt you for it if necessary.
  name       Show information about processes that begin with the name
             specified.
  -e         Exact match the process name.
  pid        Show information about specified process.


All memory values are displayed in KB.
Abbreviation key:
Pri          Priority
Thd          Number of Threads
Hnd          Number of Handles
UM           Virtual Memory
WS           Working Set
Priv         Private Virtual Memory
Priv Pk     Private Virtual Memory Peak
Faults      Page Faults
NonP        Non-Paged Pool
Page        Paged Pool
Cswtch      Context Switches

C:\Documents and Settings\kevin.peirson\Desktop\psTools>
```

- Gives detailed information about processes running on a target machine
- Information includes the CPU, memory, and threads

[Login](#) | [Register](#)[Current issue](#) | [▼ Subscribe](#) | [▼ Blogs](#) | [Events](#) | [eSeminars](#) | [White papers](#) | [RSS/XML](#) | [Jobs](#)[GCN Home](#) > [07/31/06 issue](#)

Special Report | 'Live' forensics is the future for law enforcement

By [Patience Wait](#), GCN Staff [Story Tools: Print this](#) | [Email this](#) | [Purchase a Reprint](#) | [Link to this page](#)[Listen to this story](#)

■ In this Special Report

- [The new DNA](#)
- [Who is accredited to analyze forensic evidence?](#)
- [Darlene Druyun's downfall: e-mail](#)
- [NIST's goal: Keep digital evidence fresh](#)

Until recently, users of computer forensics were concerned primarily with post-mortem analysis of digital media, looking for evidence of past actions.

But forensics is going "live." The term might sound like an oxymoron, but in the post-Sept. 11 world, with intelligence and counterintelligence agencies trying to spot trouble before it happens, collecting forensic evidence in real time can boost efforts to protect citizens.

"Post-mortem digital investigations—pull the plug, image-the-drives forensics—are almost obsolete in today's enterprise setting," said Chet Hosmer, chief executive officer and chief scientist of WetStone Technologies Inc. of Cortland, N.Y.

"As terabyte drives, encrypted file systems, gigabyte removable memory sticks and memory-resident root kits arrive on the scene, our only chance to collect valuable forensic evidence is through methods of live, on-the-wire forensics," he said.

Collecting possible evidence in real time, while desktop computers and servers are running, could provide the opportunity to build criminal cases while creating a window to prevent illegal acts as well, from distribution of child pornography to thwarting terrorist plots, Hosmer said. It also can make it much easier to identify geographically dispersed groups of people that are working in concert—truly connecting the dots.

Because of this, the shift toward live forensics is gaining momentum in government as well as the private sector. The Defense Cyber Crime Center is performing more and more live forensics analyses, according to Edmund Kong, director of engineering for the Defense Cyber Crime Institute, one of DC3's divisions. DCCI has developed a tool of its own for live exams, he added.

DC3 provides some support for live network investigations, usually for other military agencies such as the Naval Criminal Investigative Service or Army Criminal Investigative Division, via its Defense Criminal Forensics Laboratory.

On-Demand “Live” Investigations



Michael Duren
mike@wetstonetech.com

