Computer Forensics Software Tools

Computer Forensics Software Tools

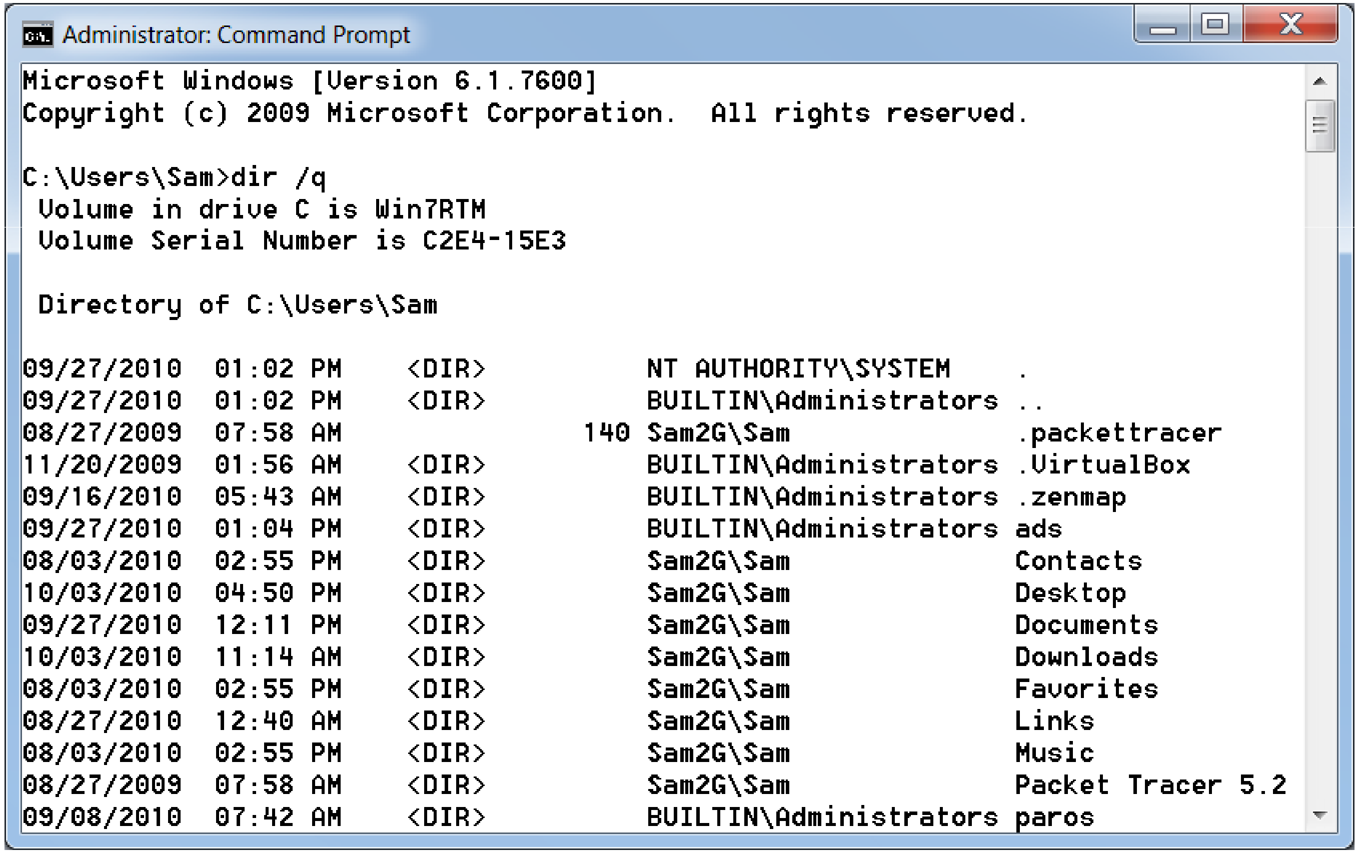
- Command-line tools
- GUI tools

Command-line Forensic Tools

- The first tools that analyzed and extracted data from floppy disks and hard disks were
  - **MS-DOS tools for IBM PC file systems**
    - Norton DiskEdit
      - First MS-DOS tools
    - Advantage
      - Require few system resources
      - Designed to run in minimal configurations
      - Fit on bootable media
      - Save time and effort

DIR /Q

- Shows file owner



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Sam>dir /q
 Volume in drive C is Win7RTM
 Volume Serial Number is C2E4-15E3

 Directory of C:\Users\Sam

09/27/2010  01:02 PM    <DIR>          NT AUTHORITY\SYSTEM    .
09/27/2010  01:02 PM    <DIR>          BUILTIN\Administrators ..
08/27/2009  07:58 AM               140 Sam2G\Sam              .packettracer
11/20/2009  01:56 AM    <DIR>          BUILTIN\Administrators .VirtualBox
09/16/2010  05:43 AM    <DIR>          BUILTIN\Administrators .zenmap
09/27/2010  01:04 PM    <DIR>          BUILTIN\Administrators ads
08/03/2010  02:55 PM    <DIR>          Sam2G\Sam              Contacts
10/03/2010  04:50 PM    <DIR>          Sam2G\Sam              Desktop
09/27/2010  12:11 PM    <DIR>          Sam2G\Sam              Documents
10/03/2010  11:14 AM    <DIR>          Sam2G\Sam              Downloads
08/03/2010  02:55 PM    <DIR>          Sam2G\Sam              Favorites
08/27/2010  12:40 AM    <DIR>          Sam2G\Sam              Links
08/03/2010  02:55 PM    <DIR>          Sam2G\Sam              Music
08/27/2009  07:58 AM    <DIR>          Sam2G\Sam              Packet Tracer 5.2
09/08/2010  07:42 AM    <DIR>          BUILTIN\Administrators paros
```

UNIX/Linux Forensic Tools

- *nix platforms
  - Have long been the primary command-line OS
  - Not used widely
  - GUIs now available
  - investigators a challenge:
    - learning the *nix command line
    - investigating the *nix environment
- *nix tools for forensics analysis
    - SMART, Helix, BackTrack , Autopsy with Sleuth Kit, Knoppix-STD

UNIX/Linux Forensic Tools

- **SMART**
  - Designed to be installed on numerous Linux versions (Gentoo, Fedora, SUSE, Debian, Knoppix, Ubuntu, Slackware)
    - Can analyze a variety of file systems
    - Many plug-in utilities are included
    - Hex viewer is available
    - Hex values are colour-coded
    - Supports Logging and Bookmarking

UNIX/Linux Forensic Tools

- **Helix**
  - Easy to use
  - You can load it on a live Windows system
    - Loads as a bootable Linux OS from a cold boot\
- **BackTrack**
  - It is a Linux Live CD
- **Autopsy and SleuthKit**
  - Sleuth Kit is a Linux forensics tool
  - Autopsy is the GUI/browser interface used to access Sleuth Kit's tools

UNIX/Linux Forensic Tools

- Knoppix-STD (Security Tools Distribution)
  - A collection of tools
  - Used for configuring security measures during computer and network forensics
  - forensically sound
    - Doesn’t allow you to alter or damage the system you’re analyzing
  - Linux bootable CD
  - Many of the tools have GUI interfaces, some are still command line only

Other GUI Forensic Tools

- Several software vendors have introduced forensics tools that work in Windows
- Simplify computer forensics investigations
- Help training beginning investigators
- Most of them come into suites of tools
- Advantages
  - Ease of use
  - Multitasking
  - No need for learning older Oss
- GUI tool vendor
  - Technology Pathways, AccessData, Guidance Software

Other GUI Forensic Tools

- Disadvantages
  - Excessive resource requirements
  - Produce inconsistent results
  - Create tool dependencies

- Some situations, GUI tools don’t work and a command-line tool is required
- Investigators must be familiar with more than one type of tool

Computer Forensics Hardware Tools

Computer Forensics Hardware Tools

- Technology changes rapidly
- hardware manufacturers have designed most computer components to last about 18 months between failures
- Hardware eventually fails
  - Schedule equipment replacements
- When planning your budget consider:
  - Failures
  - Consultant and vendor fees
  - Anticipate equipment replacement

Forensic Workstations

- Computer vendors
  - Offer a wide range of forensic workstations
  - We can tailor to meet our investigation needs
- Carefully consider what we need

- Learn to balance what we need and what our system can handle
    - PCs have limitations on how many peripherals they can handle. The more peripherals you add, the more potential problems you might have,

Forensic Workstations

- Categories
  - **Stationary**
    - tower with several bays and many peripheral devices
  - **Portable**
    - laptop computer with a built-in LCD monitor and almost as many bays and peripherals as a stationary workstation
  - **Lightweight**
    - laptop computer built into a carrying case with a small selection of peripheral options

Forensic Workstations

Stationary

Portable

Lightweight

Forensic Workstations

- Police agency labs
  - Need many options
  - use two or three configurations of PCs tohandle diverse investigations
  - keep a hardware inventory and software library
- Private corporation labs
  - Handle only system types used in the organization

Building your Own Forensic Workstation

- Build own forensic workstation or purchase from vendor
- Advantages
  - Customized to your needs
  - Save money
- Disadvantages
  - Hard to find support for problems
  - Can become expensive if careless
- Also need to identify what you intend to analyze

Purchasing a Forensic Workstation

- You can buy one from a vendor as an alternative
- Examples
  - F.R.E.D.
  - F.I.R.E. IDE
- Having vendor support can save time and frustration when problems occur
- Can mix and match components to get the capabilities needed for forensic workstation

Using a Write-Blocker

- **Write-blocker**
  - Prevents data writes to a hard disk
  - Software write-blockers
  - Hardware blockers write-blockers

Using a Write-Blocker

- Software write-blockers
  - PDBlock from Digital Intelligence
    - Run in a shell mode
    - Run only in a true DOS mode
    - Not in a Windows MS-DOS shell

Using a Write-Blocker

- Hardware write-blockers
  - Connect the evidence drive to your workstation and start the OS as usual
  - Ideal for GUI forensic tools
  - Act as a bridge between the suspect drive and the forensic workstation

Using a Write-Blocker

- Write-blocker is attached to a drive
- Still we can navigate to the blocked drive with any Windows application
  - Windows Explorer, to view files
  - Word to read files
- When you copy data to the blocked drive or write updates to a file with Word, Windows shows that the data copy is successful
- However, the write-blocker actually discards the written data—in other words**, data is written to null**
- When you restart the workstation and examine the blocked drive, you won't see the data or files you copied to it previously

Using a Write-Blocker

- Many vendors have developed write-blocking devices
  - FireWire
  - USB 2.0
  - SCSI controllers
- Most of these write-blockers enable you to remove and reconnect drives without having to shut down your workstation, which saves time

Recommendations for a Forensic Workstation

- Determine where data acquisitions will take place
- If you acquire data consider streamlining the tools
  - Choosing a computer as a stationary or lightweight forensic workstation
  - Expansion devices requirements
  - Power supply with battery backup
  - Extra power and data cables

Recommendations for a Forensic Workstation

- External FireWire and USB 2.0 ports
- Assortment of drive adapter bridges
- Ergonomic considerations
  - Keyboard and mouse
  - A good video card with at least a 17-inch monitor
- High-end video card and monitor
- With limited budget, one option for outfitting forensic lab is to use high-end game PCs

Validating and Testing Forensic Software

Validating and Testing Forensic Software

- Make sure the evidence we recover and analyze can be admitted in court
- Test and validate the software to prevent damaging the evidence

Using National Institute of Standards and Technology (NIST) Tools

- Publishes articles, provides tools, and creates procedures for testing and validating computer forensics software
- **Computer Forensics Tool Testing (CFTT)** program
  - NIST sponsors project
  - Manages research on computer forensics tools

Using NIST Tools

- NIST has created criteria for testing computer forensics tools based on:
  - Standard testing methods
  - ISO 17025 criteria for testing

Using NIST Tools

- Lab must meet the following criteria
  - Establish categories for computer forensics tools
    - Group computer forensics software according to categories
  - Identify computer forensics category requirements
    - describe the technical features or functions a forensics tool must have
  - Develop test assertions
  - Identify test cases
  - Establish a test method
  - Report test results

Using NIST Tools

- **National Software Reference Library (NSRL)** project
  - Collects all known hash values for commercial software applications and OS files
    - Uses SHA-1 to generate a known set of digital signatures called the Reference Data Set (RDS)
  - Helps filtering known information

Using NIST Tools

- The purpose of collecting known hash values is to reduce the number of known files(such as OS or program files) included in a forensics examination
- RDS help to locate and identify known bad files (illegal images and computer viruses)

Using Validation Protocols

- Always verify your results
- Use at least two tools
  - Retrieving and examination
  - Verification
- Understand how tools work
- One way to compare results and verify a new tool is by using a disk editor
  - Such as Hex Workshop or WinHex
  - But it won't work with encrypted or compressed files

Using Validation Protocols

- Disk editors
  - Do not have a flashy interface
  - Reliable tools
  - Can access raw data
- Computer Forensics Examination Protocol
  - Perform the investigation with a GUI tool
    - Usually FTK or EnCase
  - Verify your results with a disk editor
  - If a file is recovered, compare hash values obtained with both tools

Using Validation Protocols

- Computer Forensics Tool Upgrade Protocol
  - Test
    - New releases
    - OS patches and upgrades
  - If you find a problem, report it to forensics tool vendor
    - Do not use the forensics tool until the problem has been fixed
  - Use a test hard disk for validation purposes
  - Check the Web for new editions, updates, patches, and validation tests for your tools