FIRST Technical Colloquium

Group Discussion – Digital Forensics Tools & Techniques

February 12, 2001

Douglas W. Barbin, CISSP, CFE
Senior Consultant
Guardent, Inc.
http://www.guardent.com

GUARDENT℠

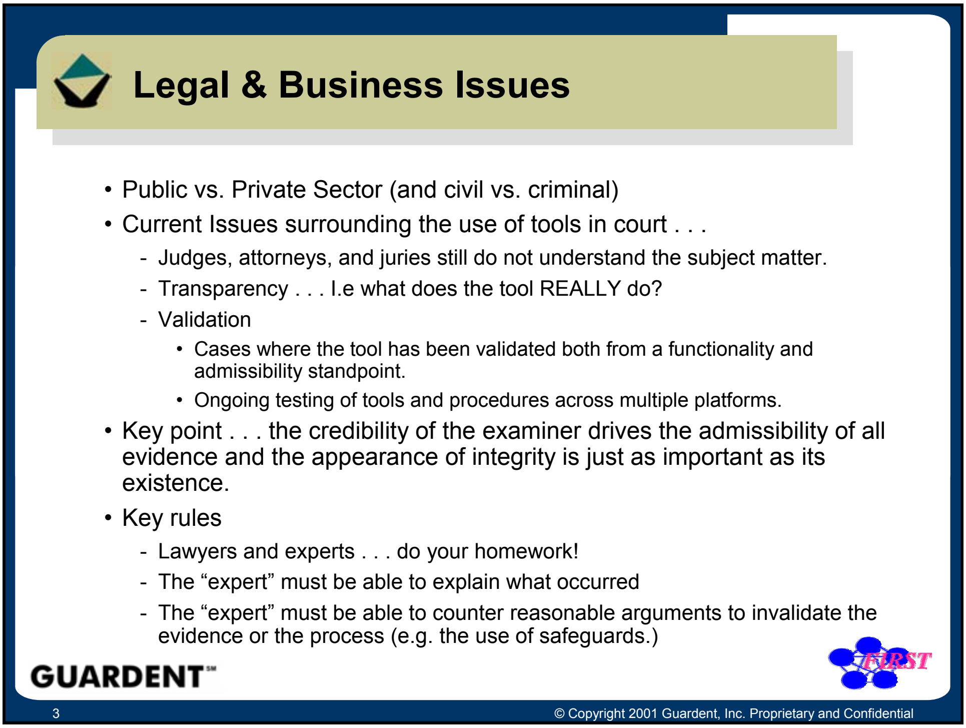
FIRST

Agenda

- **Intro - Legal & Business Issues**
- Objectives / Format
- Forensic Hardware
- Forensic Software
  - Security Magazine Rankings
  - Unix
  - Windows
- Wrap-up

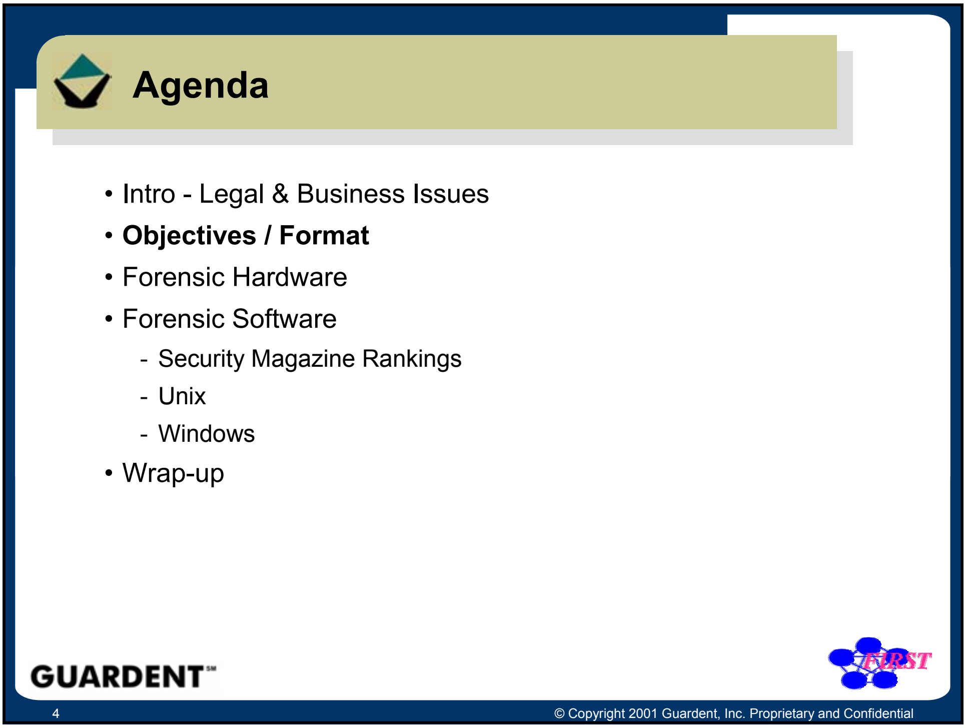
GUARDENT℠

FIRST



Legal & Business Issues

- Public vs. Private Sector (and civil vs. criminal)
- Current Issues surrounding the use of tools in court . . .
  - Judges, attorneys, and juries still do not understand the subject matter.
  - Transparency . . . I.e what does the tool REALLY do?
  - Validation
    - Cases where the tool has been validated both from a functionality and admissibility standpoint.
    - Ongoing testing of tools and procedures across multiple platforms.
- Key point . . . the credibility of the examiner drives the admissibility of all evidence and the appearance of integrity is just as important as its existence.
- Key rules
  - Lawyers and experts . . . do your homework!
  - The “expert” must be able to explain what occurred
  - The “expert” must be able to counter reasonable arguments to invalidate the evidence or the process (e.g. the use of safeguards.)



Agenda

- Intro - Legal & Business Issues
- **Objectives / Format**
- Forensic Hardware
- Forensic Software
  - Security Magazine Rankings
  - Unix
  - Windows
- Wrap-up

Objectives / Format

- Engage in structured discussion and debate on the latest forensic tools and techniques. For the purpose of this discussion, forensic tools includes tools that assist with the investigation of a computer security or related incident from a disk/file or logs perspective.
- Evaluate tools with the following criteria:
  - Key Purpose
  - Platforms
  - Benefits
  - Weaknesses
  - Estimated Cost
  - Links / URL

Agenda

- Intro – Legal & Business Issues
- Objectives
- **Forensic Hardware**
- Forensic Software
  - Security Magazine Rankings
  - Unix
  - Windows
- Wrap-up

Forensic Hardware

- “Laboratory Equipment”
  - Often large converted servers or workstations
- “Fly-away kits”
  - Often referred to as portable computers and not always easily portable
- “Laptops”
  - Difficult to interface with IDE/SCSI drives in DOS
  - Do work if running Unix dd over an isolated secure network using SSH or Netcat.
- Some companies that produce/sell forensic hardware
  - http://www.forensic-computers.com
  - http://www.digitalintel.com (Digital Intelligence)
  - http://www.computer-forensics.com (DIBS Computer Forensics)
- Bottom line . . . Forensic equipment can help out from an interface and an adaptability standpoint, but the core challenges of digital forensics are often application and operating system specific.

Agenda

- Intro – Legal & Business Issues
- Objectives
- Forensic Hardware
- **Forensic Software**
  - **Security Magazine Rankings**
  - Unix
    - Standard Unix Commands
    - Packages
  - Windows
- Wrap-up

Ernst and Young Review of Forensic Tools for Security Magazine

Tools Reviewed	Rating
• Byte Back	****
• Drive Image Pro 3.0	n/a
• EnCase 2.08	****
• Linux “dd” 6.1*	*****
• Norton Ghost	****
• Safeback 2.0*	*****
• Snapback DatArrest 4.1*	*****

Source: Security Magazine September 2000 Edition

http://www.scmagazine.com/scmagazine/2000_09/survey/survey.html

** Indicates an SC Magazine Best-Buy for 2000*

GUARDENT℠

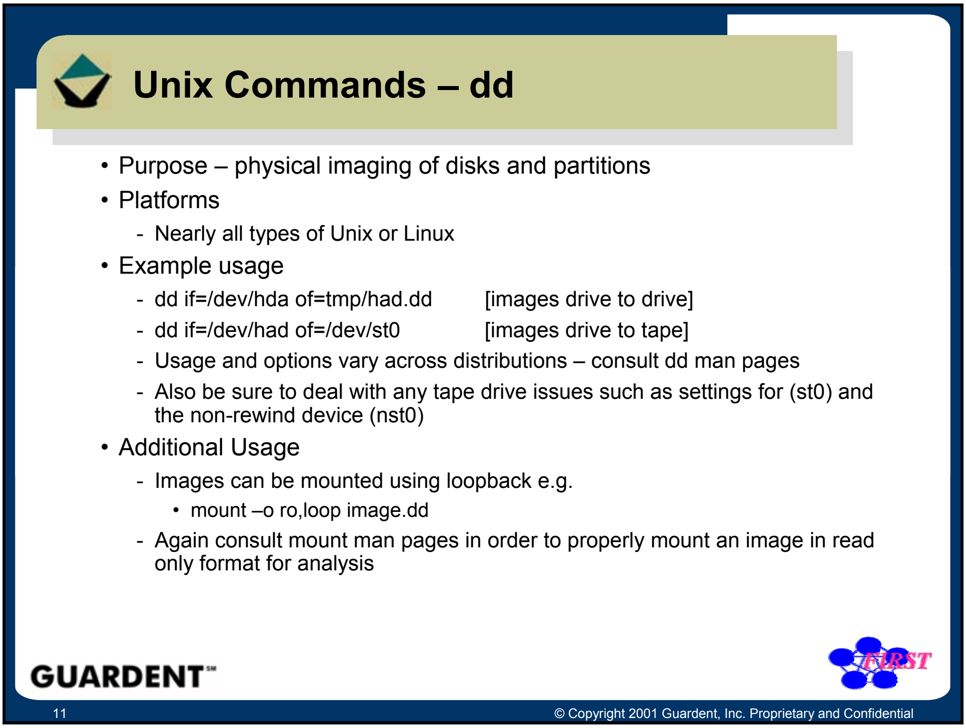
FIRST

Agenda

- Intro – Legal & Business Issues
- Objectives
- Forensic Hardware
- **Forensic Software**
  - Security Magazine Rankings
  - **Unix**
    - **Standard Unix Commands**
    - **Packages**
  - Windows
- Wrap-up

GUARDENT℠

FIRST

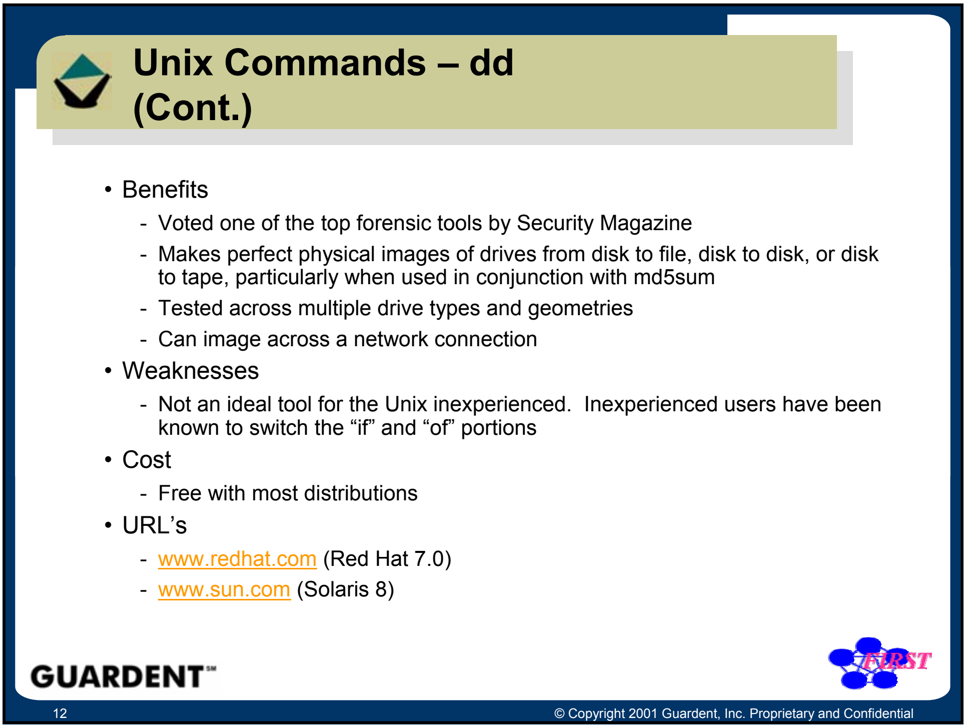


Unix Commands – dd

- Purpose – physical imaging of disks and partitions
- Platforms
  - Nearly all types of Unix or Linux
- Example usage
  - dd if=/dev/hda of=tmp/had.dd [images drive to drive]
  - dd if=/dev/had of=/dev/st0 [images drive to tape]
  - Usage and options vary across distributions – consult dd man pages
  - Also be sure to deal with any tape drive issues such as settings for (st0) and the non-rewind device (nst0)
- Additional Usage
  - Images can be mounted using loopback e.g.
    - mount –o ro,loop image.dd
  - Again consult mount man pages in order to properly mount an image in read only format for analysis

GUARDENT℠

FIRST



Unix Commands – dd (Cont.)

- Benefits
  - Voted one of the top forensic tools by Security Magazine
  - Makes perfect physical images of drives from disk to file, disk to disk, or disk to tape, particularly when used in conjunction with md5sum
  - Tested across multiple drive types and geometries
  - Can image across a network connection
- Weaknesses
  - Not an ideal tool for the Unix inexperienced. Inexperienced users have been known to switch the "if" and "of" portions
- Cost
  - Free with most distributions
- URL's
  - www.redhat.com (Red Hat 7.0)
  - www.sun.com (Solaris 8)

GUARDENT℠

FIRST

Unix Commands – grep (Global Regular Expression Parser)

- Purpose
  - Searches through an input set for matches to a specified pattern and outputs matching lines
- Platforms
  - Nearly all types of Unix or Linux
- Example usage
  - grep –n cha *.c   [looks for the string “cha” in all *.c files in the current directory and returns the string and the line number]
  - Options vary by version. Consult man pages appropriately
- Related tools
  - egrep
  - fgrep
  - find
  - finger
  - locate
  - which

Unix Commands – grep (cont.)

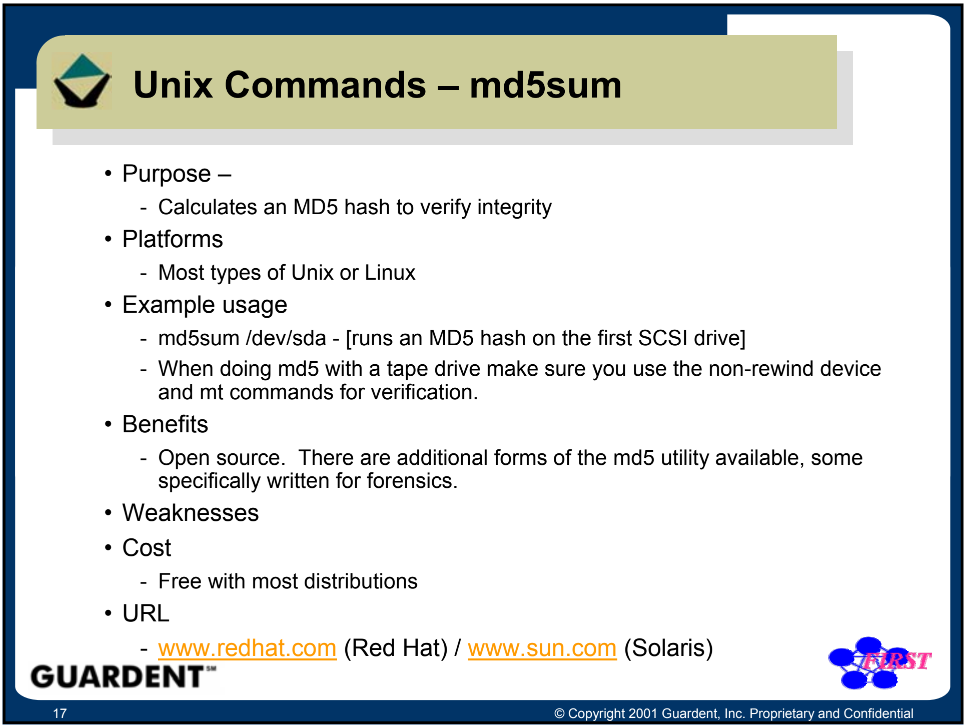
- Benefits
  - Easy to use
  - Standard Unix commands
- Weaknesses
  - May alter access times of particular files. The examiner should always try to work from a copy when possible
- Cost
  - Free
- URL
  - http://www.redhat.com
  - http://www.sun.com

Unix Commands - lsof

- Purpose
  - lists files and their associated processes. Without any arguments is similar to the ps command
- Platforms
  - Most types of Unix or Linux
- Example Usage
  - lsof –i   [shows current Internet processes]
- Benefits
  - More comprehensive than ps which just displays current processes
  - Can help identify rootkits or trojans running
- Weaknesses
  - Does not support IRIX
  - May not work if using kernal modules to hide ps in Linux

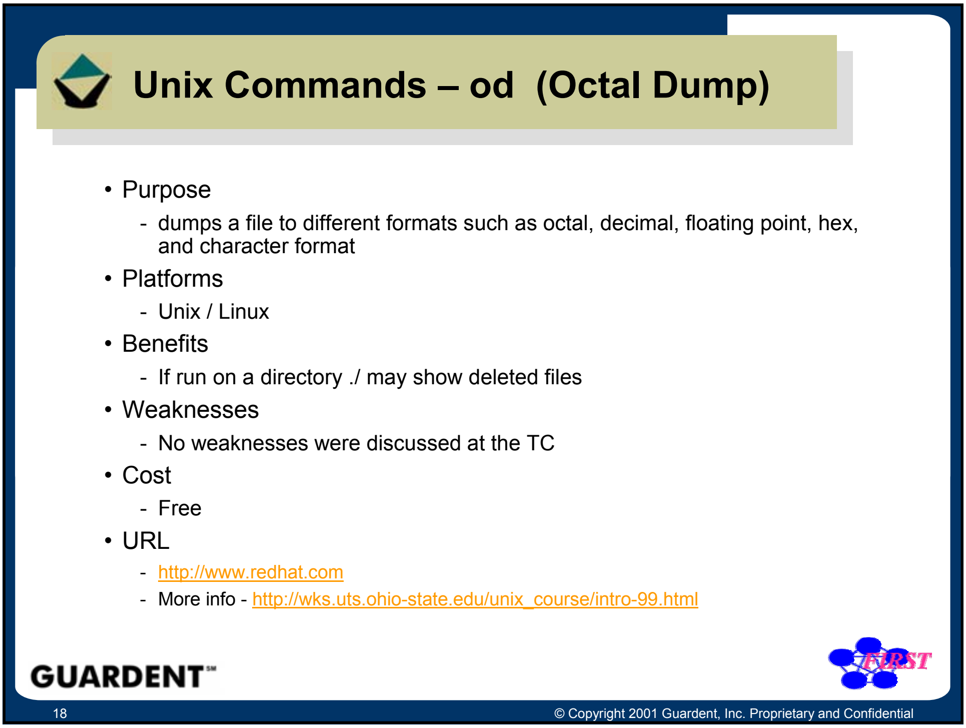
Unix Commands – lsof (Cont.)

- Cost
  - Free
- URL
  - http://www.cert.org/security-improvement/implementations/i042.05.html



Unix Commands – md5sum

- Purpose –
  - Calculates an MD5 hash to verify integrity
- Platforms
  - Most types of Unix or Linux
- Example usage
  - md5sum /dev/sda - [runs an MD5 hash on the first SCSI drive]
  - When doing md5 with a tape drive make sure you use the non-rewind device and mt commands for verification.
- Benefits
  - Open source. There are additional forms of the md5 utility available, some specifically written for forensics.
- Weaknesses
- Cost
  - Free with most distributions
- URL
  - www.redhat.com (Red Hat) / www.sun.com (Solaris)



Unix Commands – od (Octal Dump)

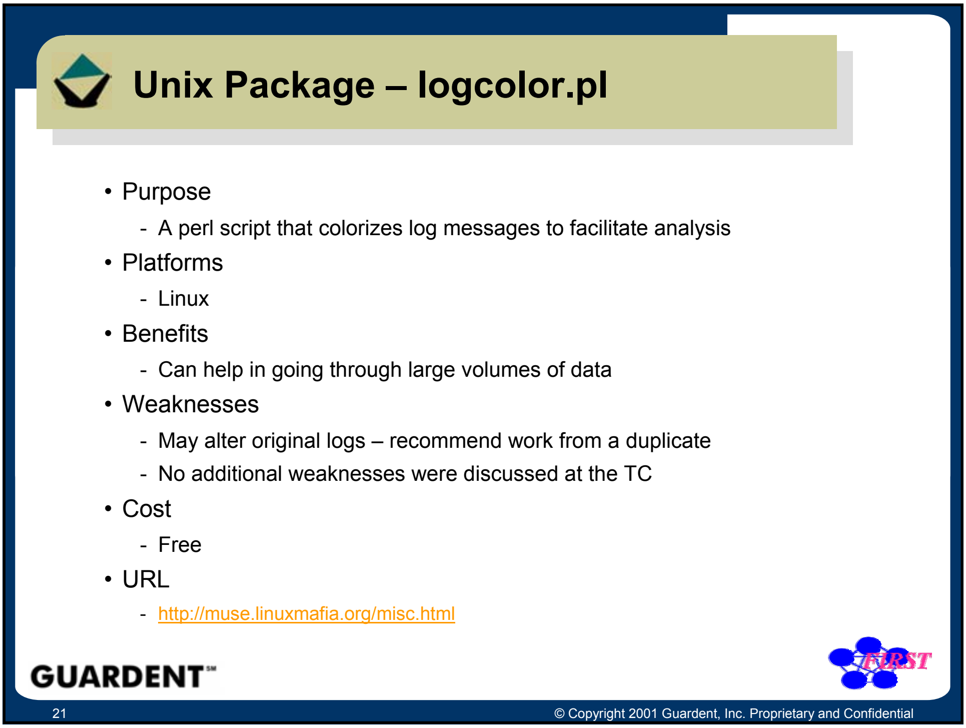
- Purpose
  - dumps a file to different formats such as octal, decimal, floating point, hex, and character format
- Platforms
  - Unix / Linux
- Benefits
  - If run on a directory ./ may show deleted files
- Weaknesses
  - No weaknesses were discussed at the TC
- Cost
  - Free
- URL
  - http://www.redhat.com
  - More info - http://wks.uts.ohio-state.edu/unix_course/intro-99.html

Unix Commands – rpm

- Purpose
  - The Red Hat Package Manager
- Platforms
  - Red Hat Linux (and related)
- Benefits
  - Easy way to display installed packages
- Weaknesses
  - May modify certain files
  - Not always complete – may not show certain trojans and hidden processes
- Cost
  - Free
- URL
  - http://www.missioncriticallinux.com/technology/crash/

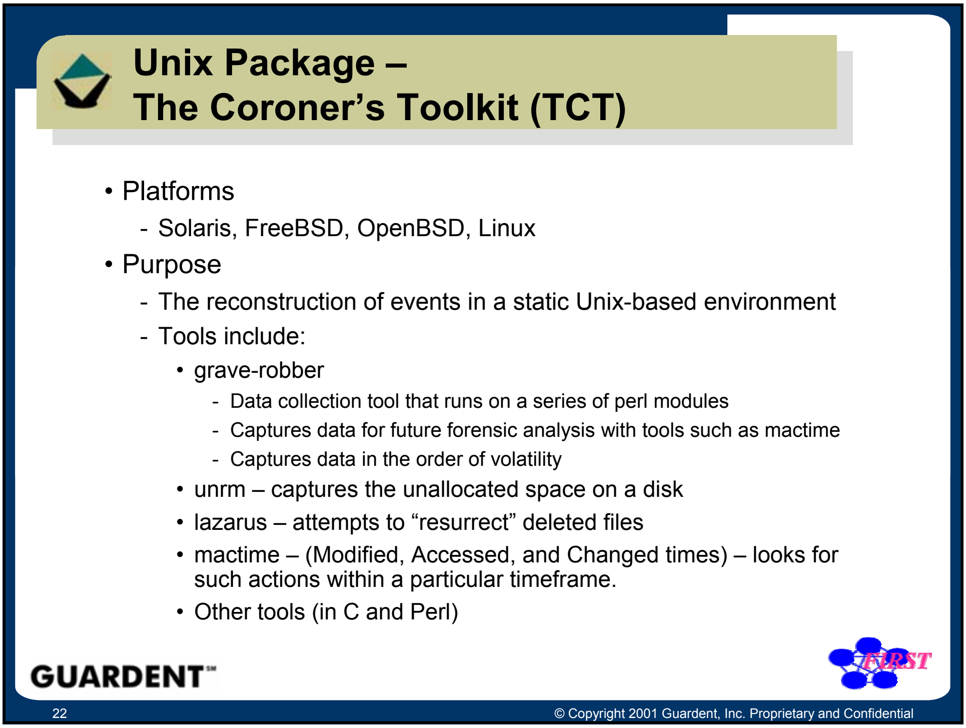
Unix Package – crash

- Purpose
  - Package tool that dumps system memory to swap by following processes through memory address space.
- Platforms
  - Linux
- Benefits
  - Can sometimes show hidden processes
- Weaknesses
  - Can alter system swap space
- Cost
  - Free
- URL
  - http://www.missioncriticallinux.com/technology/crash/



Unix Package – logcolor.pl

- Purpose
  - A perl script that colorizes log messages to facilitate analysis
- Platforms
  - Linux
- Benefits
  - Can help in going through large volumes of data
- Weaknesses
  - May alter original logs – recommend work from a duplicate
  - No additional weaknesses were discussed at the TC
- Cost
  - Free
- URL
  - http://muse.linuxmafia.org/misc.html



Unix Package – The Coroner’s Toolkit (TCT)

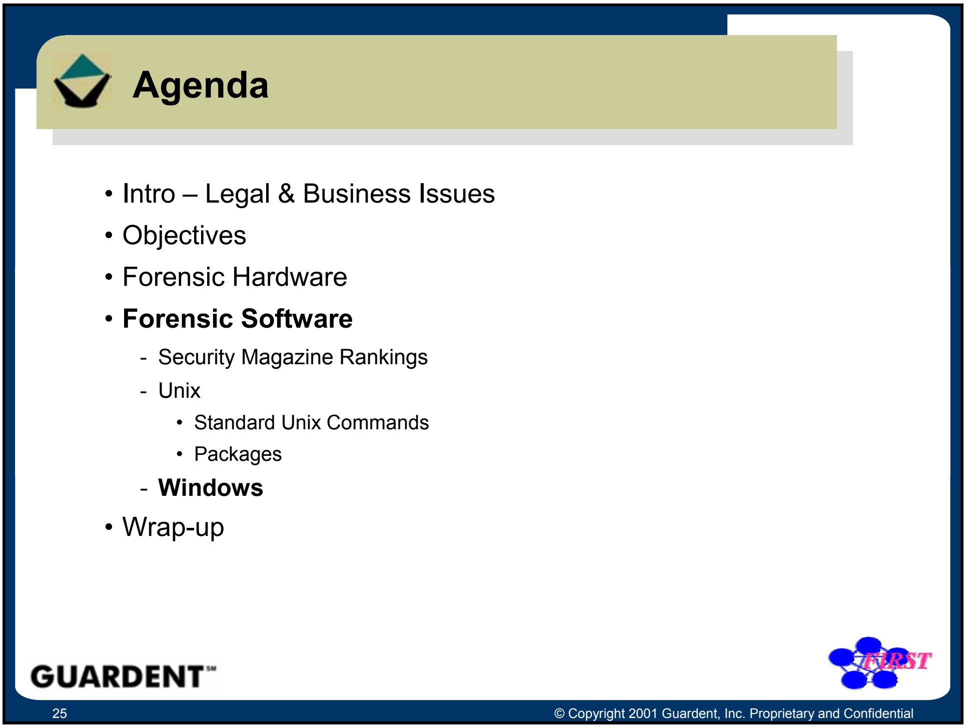
- Platforms
  - Solaris, FreeBSD, OpenBSD, Linux
- Purpose
  - The reconstruction of events in a static Unix-based environment
  - Tools include:
    - grave-robber
      - Data collection tool that runs on a series of perl modules
      - Captures data for future forensic analysis with tools such as mactime
      - Captures data in the order of volatility
    - unrm – captures the unallocated space on a disk
    - lazarus – attempts to “resurrect” deleted files
    - mactime – (Modified, Accessed, and Changed times) – looks for such actions within a particular timeframe.
    - Other tools (in C and Perl)

Unix Package – The Coroner's Toolkit (TCT) (Cont.)

- Benefits
  - Can gather live information from system memory
- Weaknesses
  - It is important to note that the installation of TCT should occur prior the incident or that the affected system should be brought into an environment where TCT exists. Installing TCT will change MAC times of some of the particular files to be examined
  - No weaknesses were discussed at the TC
- Cost
  - Free
- URL
  - http://www.porcupine.org/forensics
  - http://www.fish.com/forensics

Unix Package - Trinux

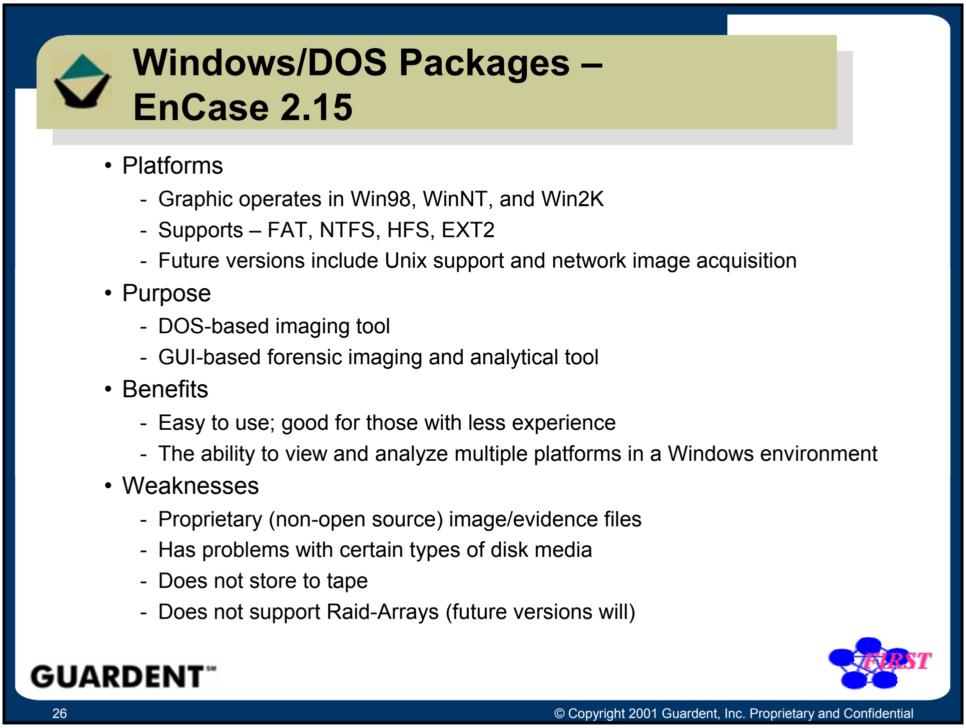
- Purpose
  - A Linux distribution with security and forensics "in-mind"
- Platforms
  - Trinux/Linux
- Benefits
  - Capable of being booted from a floppy
  - Capable of interfacing well with NTFS partitions
- Weaknesses
  - No weaknesses were discussed at the TC
- Cost
  - Free
- URL
  - http://www.trinux.org



Agenda

- Intro – Legal & Business Issues
- Objectives
- Forensic Hardware
- **Forensic Software**
  - Security Magazine Rankings
  - Unix
    - Standard Unix Commands
    - Packages
  - **Windows**
- Wrap-up

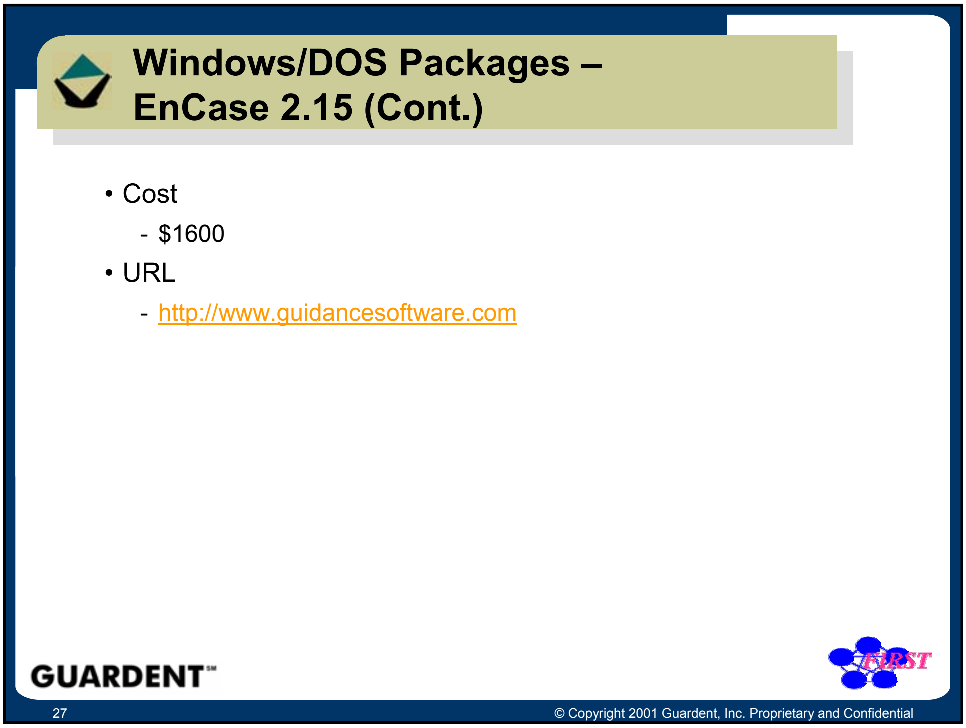
GUARDENT℠



Windows/DOS Packages – EnCase 2.15

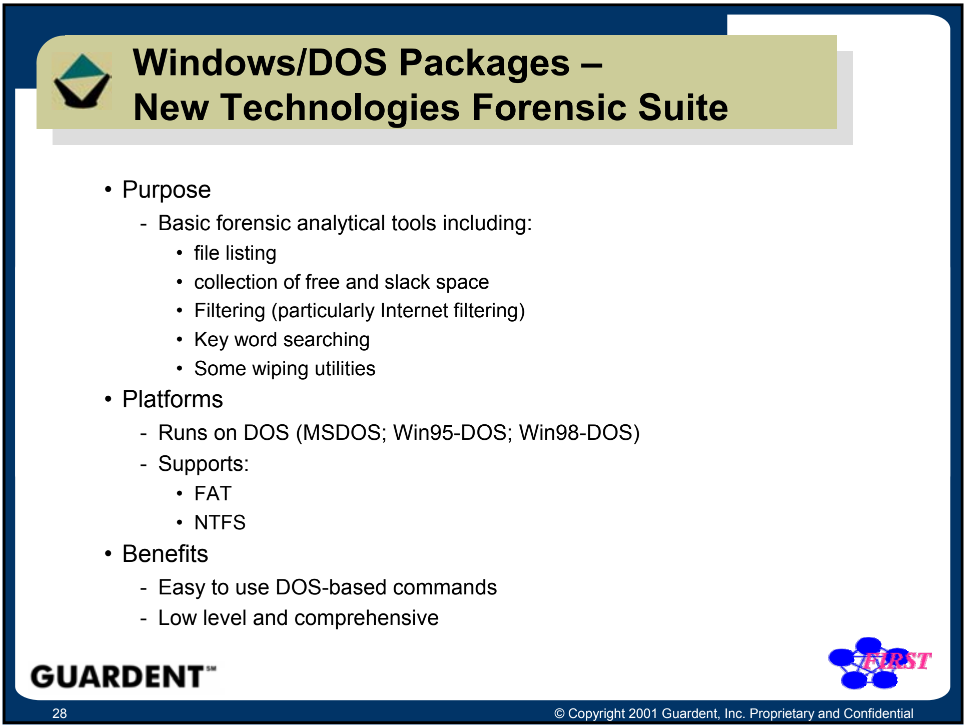
- Platforms
  - Graphic operates in Win98, WinNT, and Win2K
  - Supports – FAT, NTFS, HFS, EXT2
  - Future versions include Unix support and network image acquisition
- Purpose
  - DOS-based imaging tool
  - GUI-based forensic imaging and analytical tool
- Benefits
  - Easy to use; good for those with less experience
  - The ability to view and analyze multiple platforms in a Windows environment
- Weaknesses
  - Proprietary (non-open source) image/evidence files
  - Has problems with certain types of disk media
  - Does not store to tape
  - Does not support Raid-Arrays (future versions will)

GUARDENT℠



Windows/DOS Packages – EnCase 2.15 (Cont.)

- Cost
  - $1600
- URL
  - http://www.guidancesoftware.com



Windows/DOS Packages – New Technologies Forensic Suite

- Purpose
  - Basic forensic analytical tools including:
    - file listing
    - collection of free and slack space
    - Filtering (particularly Internet filtering)
    - Key word searching
    - Some wiping utilities
- Platforms
  - Runs on DOS (MSDOS; Win95-DOS; Win98-DOS)
  - Supports:
    - FAT
    - NTFS
- Benefits
  - Easy to use DOS-based commands
  - Low level and comprehensive

Windows/DOS Packages – New Technologies Forensic Suite

- Weaknesses
  - Only supports FAT and NTFS (no Unix/Linux)
  - Tools have not been updated in several years
  - Do nothing to analyze the active memory or current processes
- Cost
  - ~$1600 with possible discounts to law enforcement and/or government
- URL
  - http://www.forensics-intl.com/

Windows/DOS Packages – NTObjectives Forensic Toolkit

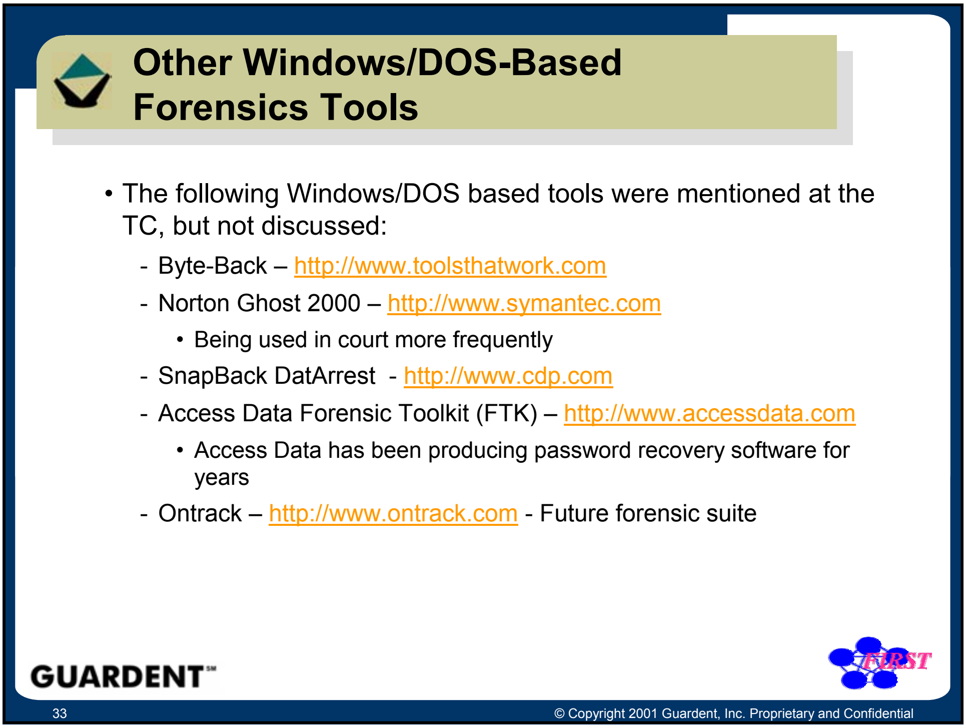
- Purpose
  - File analysis tool includes:
    - AFind - File access time finder
    - SFind - Hidden data streams finder
    - HFind - Hidden file finder
    - FileStat - Dumps file stats in a readable format
    - Hunt - List available NetBIOS info and true admin name
    - Audited - NTFS SACL Reporter lists out files being audited
    - DACLchk - Reports any Denied ACE's located after Allowed ACE's
- Platforms – WINNT/2K
- Cost – Free
- URL
  - http://www.foundstone.com

Windows/DOS Packages – Ontrack Easy Recovery Software

- Purpose
  - Data recovery program (formerly called Tiramisu)
- Platforms
  - Runs on DOS but supports:
    - FAT16
    - FAT32
    - NTFS
    - Novel
- Benefits
  - Does not allow for original data to be overwritten
  - Recovers data from multiple platforms to a DOS partition
  - Excellent support from Ontrack if needed
- Weaknesses
  - Recovering data to a FAT/DOS partition is not always ideal
- URL
  - http://www.ontrack.com

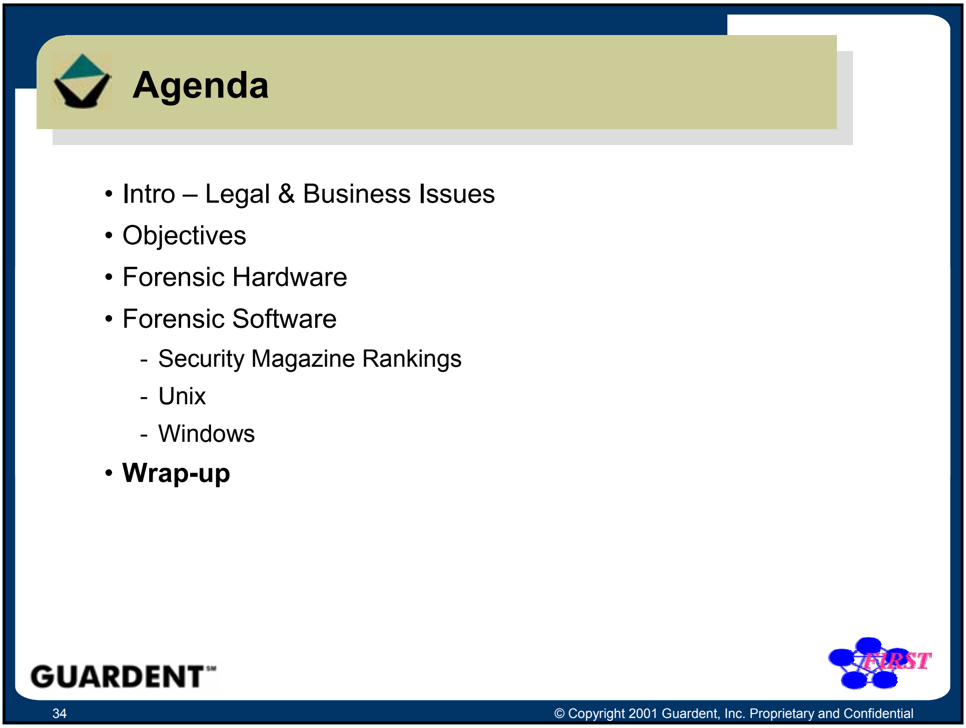
Windows/DOS Packages – Safeback 2.0

- Purpose
  - Physical (and logical if desired) imaging of hard disks
- Platforms
  - DOS (MSDOS; Win95-DOS; Win98-DOS)
- Benefits
  - Can image nearly all types of drives
  - Images drive to drive or drive to tape
  - Can support hardware Raid-Arrays; although there is some data loss
- Weaknesses
  - All images have to be restored to a separate drive. No mounting of individual images
- Cost
  - ~$1200
- URL
  - http://www.forensics-intl.com/



Other Windows/DOS-Based Forensics Tools

- The following Windows/DOS based tools were mentioned at the TC, but not discussed:
  - Byte-Back – http://www.toolsthatwork.com
  - Norton Ghost 2000 – http://www.symantec.com
    - Being used in court more frequently
  - SnapBack DatArrest - http://www.cdp.com
  - Access Data Forensic Toolkit (FTK) – http://www.accessdata.com
    - Access Data has been producing password recovery software for years
  - Ontrack – http://www.ontrack.com - Future forensic suite



Agenda

- Intro – Legal & Business Issues
- Objectives
- Forensic Hardware
- Forensic Software
  - Security Magazine Rankings
  - Unix
  - Windows
- **Wrap-up**

Wrap-up

- Encryption is an emerging issue in forensics
  - Encryption at the file level and disk level is more and more common
  - Encryption tools are designed not to be broken
  - Many times, if available, using legal authority to force someone to give a password is the most time/cost effective means of getting access to the data
- The courts are starting to be a bit more flexible from an admissibility standpoint due to the issues of availability and resources lost during a lengthy investigation
- There are new tools and techniques . . . some transparent, some not
- While a lot has changed, the credibility of the expert still drives the admissibility and credibility of the evidence. Period.

The End

Please send comments/questions to:

doug.barbin@guardent.com

+1 703.338.4003