‘‘Forensic Detecting Tools on Data Breaches’’

Pravin .S.Paupiah (BSC, Bsc (Hons), Msc, CEH, ECSA, CHFI)

IT Security Consultant

Lecturer

Origin of the word Forensics

- The word forensic comes from Latin word “forensic”,
- meaning "before the forum" and referring to something "of, pertaining to, or used in a court of law."
- In today's term the word forensic usually refers to a method of obtaining criminal evidence for purposes of using in a court of law.

(ref:URL: http://www.tech-faq.com/forensic-science.html)

What is computer forensics?

Computer investigation and analysis techniques that involve the identification, preservation, extraction, documentation, and interpretation of computer data to determine potential legal evidence.

Example of Data breaches

- An employee discovered that it was possible to access current and former employee W-2 forms online via a Google search. The W-2 form contained employee name, Social Security number, address, earnings, and taxes paid for 2009 and 2010. The discovery was made on December 23 of 2011. (From **Spotsylvania County Spotsylvania, Virginia)**

- A woman alerted a local news station to a stash of improperly disposed information. Credit card applications, patient names, addresses, Social Security numbers, and possibly medical records were found sitting next to a dumpster in a parking lot. The paperwork came from multiple organizations. Among the organizations were two closed branches of Pure Med Spa and Brite Smile Brite Skin. (From : **Pure Med Spa, Brite Smile Brite Skin Las Vegas, Nevada)**

- A nurse was fired after accessing patient medical records without cause. The unauthorized access exposed patient vital signs, diagnoses, and treatment notes. Patient Social Security numbers may have also been exposed. The breach was uncovered in November during an audit. (From: **Titus Regional Medical Center (TRMC) Mount Pleasant, Texas)**

Example of Data breaches

- A hacker or hackers outside of the US attempted to gain access to an OSU Internet server. Information on the server included names, medical record numbers, and dianoses of 30 patients who visited the pathology department between the late 1980s and 2004. A roster of students who had received training at the medical center in 2006 was also on the server. Officials do not believe that any personal information was taken during the attempt. A total of 30 patients and 150 students were notified. (From: **Ohio State University Medical Center Columbus, Ohio)**

- The first email dated 30 September 2011 was sent to both Respondent’s office email address and copied to her personal email address. The email contained attachment documents, namely 6 ‘chrono’ excel, containing payroll details for the month of August 2011 with employees’ names, salary, details of the calculated salary amount (NPF, PAYE), car allowances, overtimes, loans and transport. (From:**Mauritius DPO website)**

Forensics in relation with data protection

- **Type of data breaches :**

  - Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.
  - Electronic entry by an outside party, malware and spyware.
  - Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
  - Someone with legitimate access intentionally breaches information - such as an employee or contractor.
  - Lost, discarded or stolen non-electronic records, such as paper documents
  - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc
  - Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.

When we all the above had happened, then we forensic examiners come into picture to collate evidences and ultimately produce them in a court of law.

Importance of Forensics tools to Law

- Culprit must not be able evade due to technological issues

- Hence when choosing a forensic tool for analysis of an evidence, a forensic expert must:
  - Make sure that the tools is worldly recognise
  - Impossible for the defense lawyer to challenge the report done by a tool chosen by the prosecuting body

Importance of Forensics tools

- The purpose of digital forensic analysis tools is to accurately present all data at a layer of abstraction and format that can be effectively used by an investigator to identify evidence.

Some interesting statistics

- **WHO IS BEHIND DATA BREACHES?**
  - ❑ 98% stemmed from external agents
  - ❑ 4% implicated internal employees
  - ❑ <1% committed by business partners
  - ❑ 58% of all data theft tied to activist groups

(Source: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf)

- No big surprise here; outsiders are still dominating the scene of corporate data theft. Organized criminals were up to their typical misdeeds and were behind the majority of breaches in 2011.

- Activist groups created their fair share of misery and mayhem last year as well—and they stole more data than any other group. Their entrance onto the stage also served to change the landscape somewhat with regard to the motivations behind breaches.

- While good old-fashioned greed and avarice were still the prime movers, ideological dissent and pleasure felt at someone else's
  misfortune took a more prominent role across the caseload. As one might expect with such a rise in external attackers, the proportion of insider incidents declined.

(contd)

- **HOW DO BREACHES OCCUR?**

  - ❑ 81% utilized some form of hacking
  - ❑ 69% incorporated malware
  - ❑ 10% involved physical attacks
  - ❑ 7% employed social tactics
  - ❑ 5% resulted from privilege misuse

(Source: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf)

- Incidents involving hacking and malware were both up considerably last year, with hacking linked to almost all compromised records. This makes sense, as these threat actions remain the favored tools of external agents, who, as described above, were behind most breaches.

- Many attacks continue to bypass authentication by combining stolen or guessed credentials (to gain access) with backdoors (to retain access). Social tactics fell a little, but were responsible for a large amount of data loss.

Forensic Tools

- A set of tools and/or software programs used to analyze a computer for collection of evidence. It can divided into:
  - Proprietary/commercial tools
  - Open source tools

Proprietary/Commercial Tools

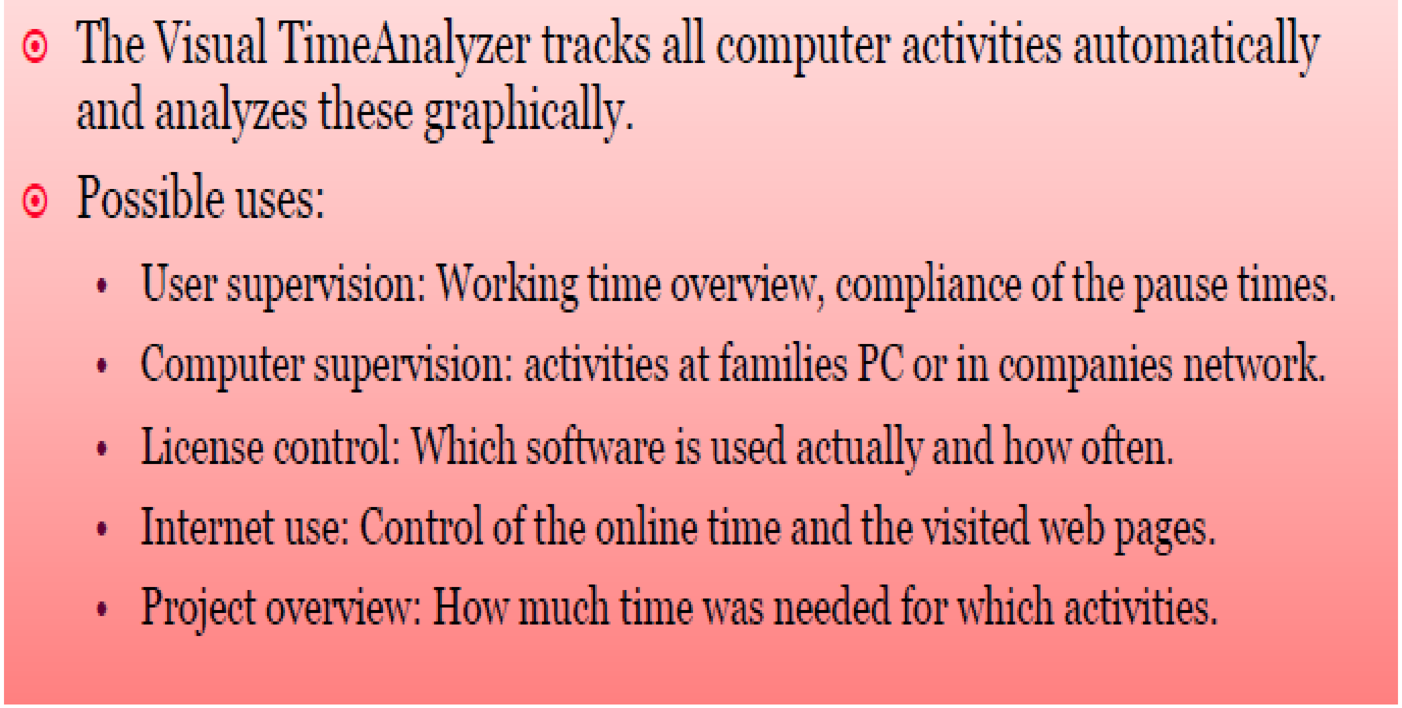
Commercial / Proprietary tools are tools that ultimately have a cost associated to it.

Commercial tools could be divided between

- Hardware
- Software

Examples of Proprietary/Commercial Tools

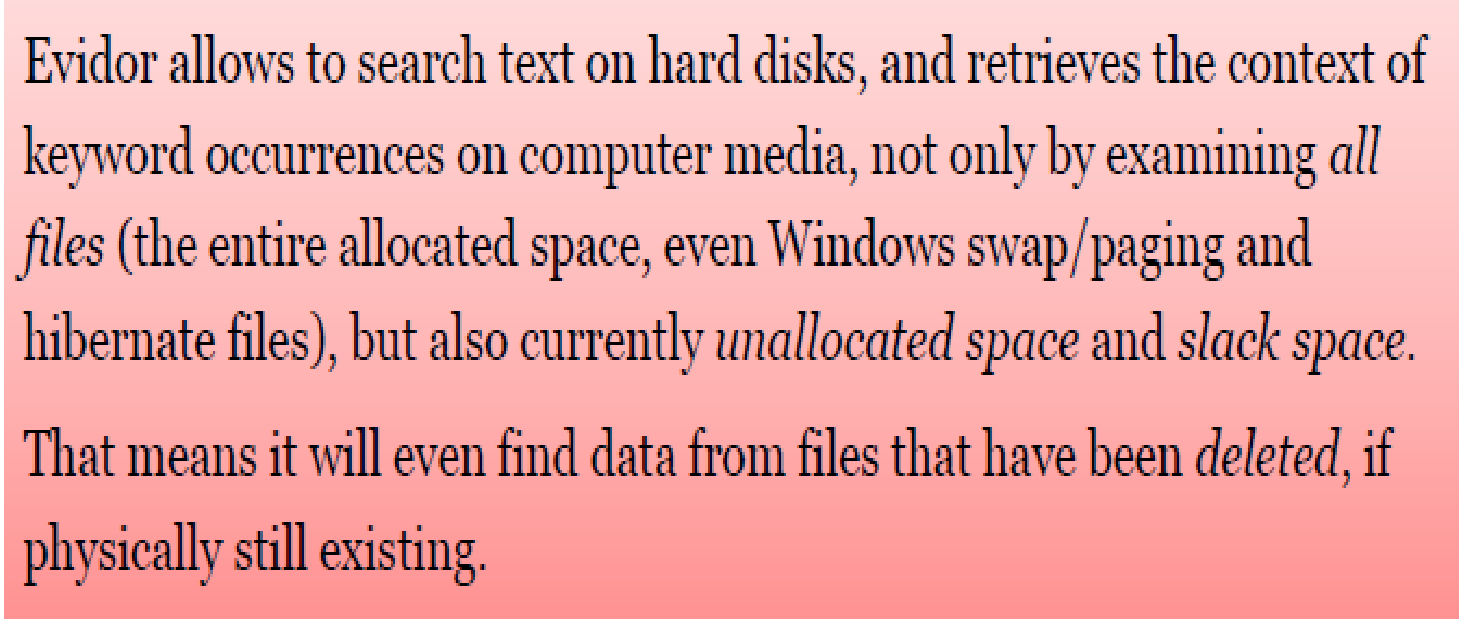
Visual TimeAnalyzer



- The Visual TimeAnalyzer tracks all computer activities automatically and analyzes these graphically.
- Possible uses:
  - User supervision: Working time overview, compliance of the pause times.
  - Computer supervision: activities at families PC or in companies network.
  - License control: Which software is used actually and how often.
  - Internet use: Control of the online time and the visited web pages.
  - Project overview: How much time was needed for which activities.

(contd)

Evidor

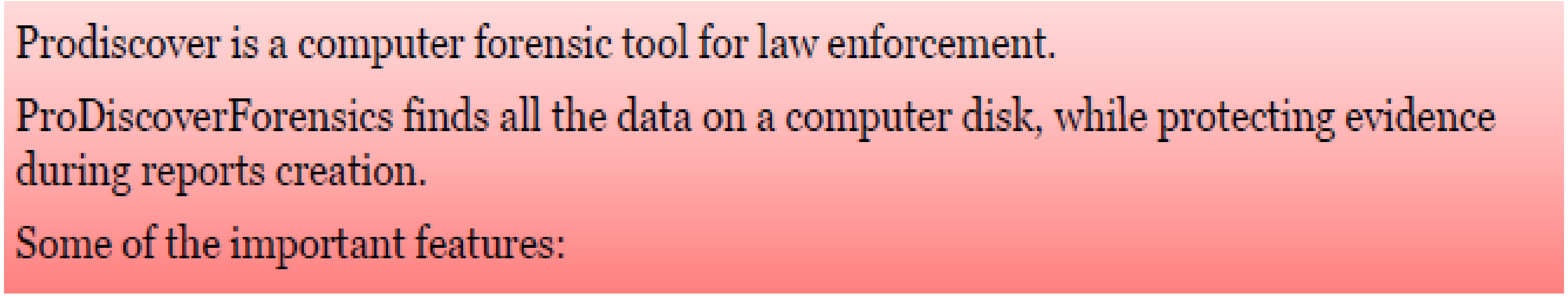


Evidor allows to search text on hard disks, and retrieves the context of keyword occurrences on computer media, not only by examining *all files* (the entire allocated space, even Windows swap/paging and hibernate files), but also currently *unallocated space* and *slack space*.

That means it will even find data from files that have been *deleted*, if physically still existing.

(contd)

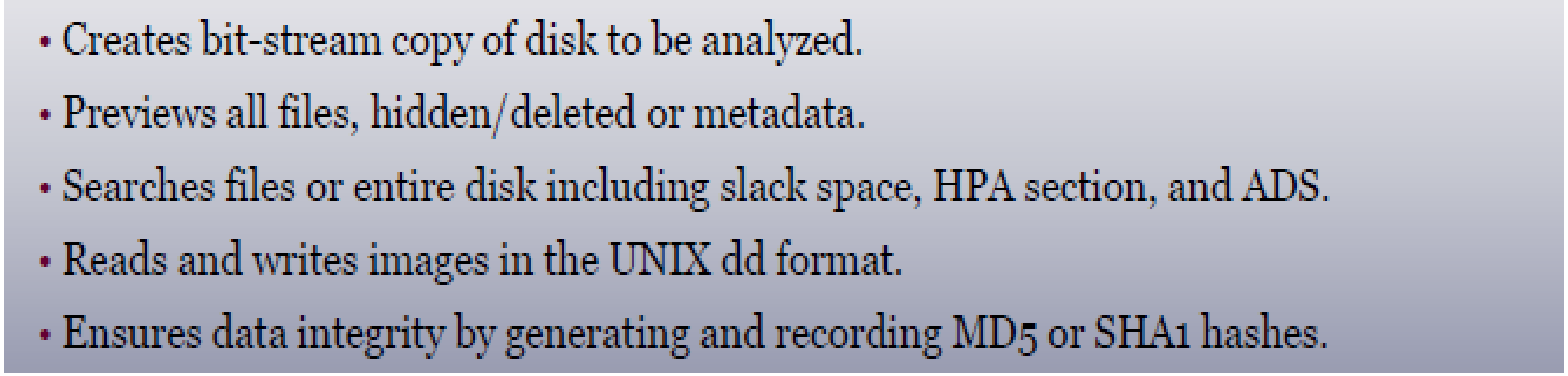
Prodiscover DFT



Prodiscover is a computer forensic tool for law enforcement.

ProDiscoverForensics finds all the data on a computer disk, while protecting evidence during reports creation.

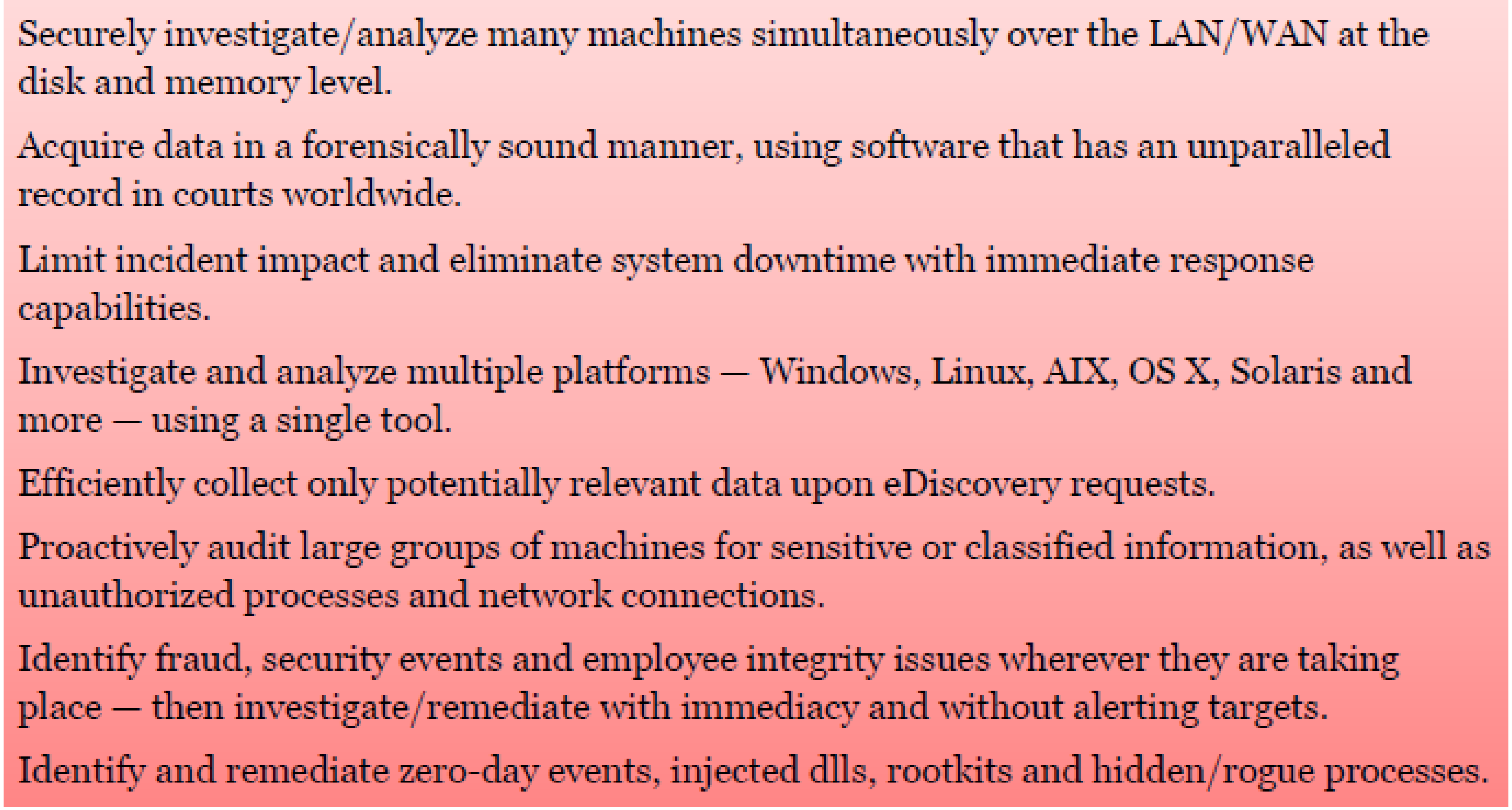
Some of the important features:



- Creates bit-stream copy of disk to be analyzed.
- Previews all files, hidden/deleted or metadata.
- Searches files or entire disk including slack space, HPA section, and ADS.
- Reads and writes images in the UNIX dd format.
- Ensures data integrity by generating and recording MD5 or SHA1 hashes.

(contd)

ENCASE



Securely investigate/analyze many machines simultaneously over the LAN/WAN at the disk and memory level.

Acquire data in a forensically sound manner, using software that has an unparalleled record in courts worldwide.

Limit incident impact and eliminate system downtime with immediate response capabilities.

Investigate and analyze multiple platforms — Windows, Linux, AIX, OS X, Solaris and more — using a single tool.

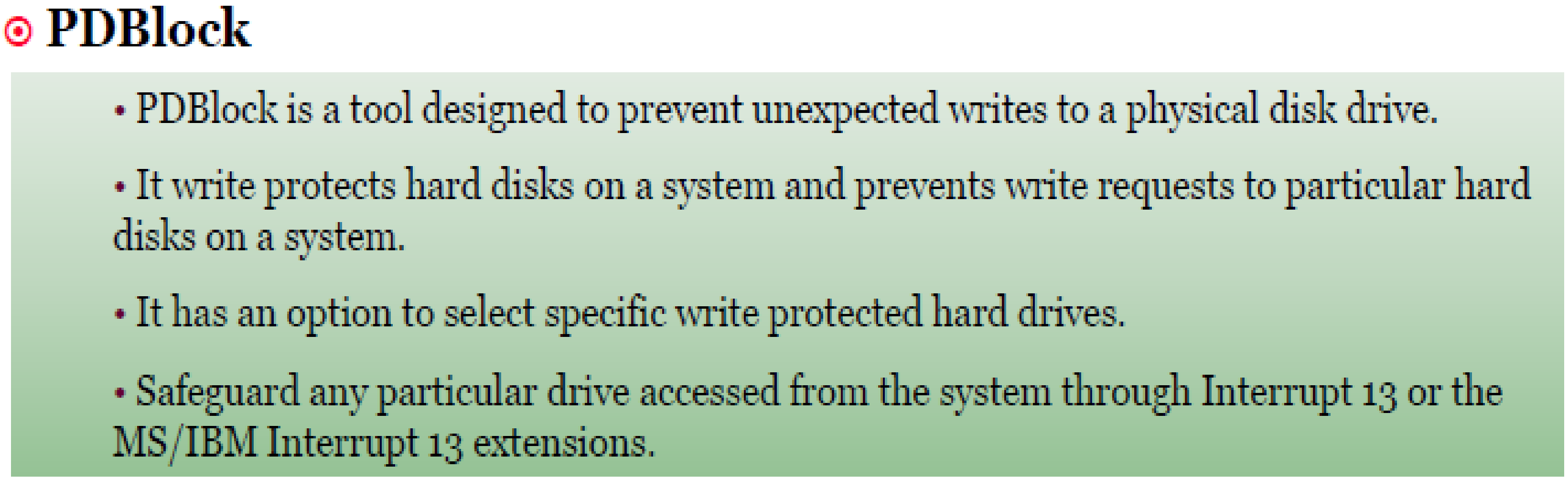
Efficiently collect only potentially relevant data upon eDiscovery requests.

Proactively audit large groups of machines for sensitive or classified information, as well as unauthorized processes and network connections.

Identify fraud, security events and employee integrity issues wherever they are taking place — then investigate/remediate with immediacy and without alerting targets.

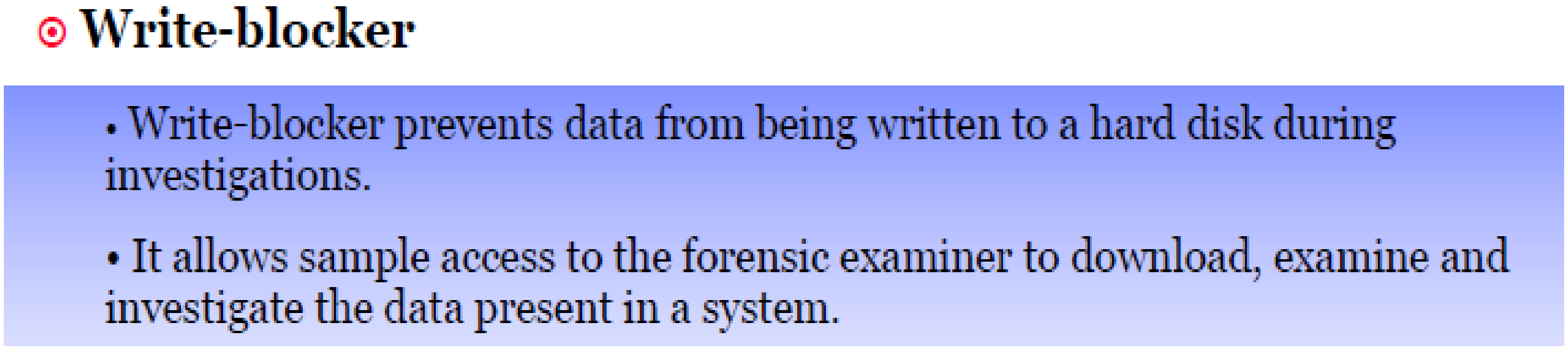
Identify and remediate zero-day events, injected dlls, rootkits and hidden/rogue processes.

Hardware based Proprietary/Commercial Tools



PDBlock

- PDBlock is a tool designed to prevent unexpected writes to a physical disk drive.
- It write protects hard disks on a system and prevents write requests to particular hard disks on a system.
- It has an option to select specific write protected hard drives.
- Safeguard any particular drive accessed from the system through Interrupt 13 or the MS/IBM Interrupt 13 extensions.



Write-blocker

- Write-blocker prevents data from being written to a hard disk during investigations.
- It allows sample access to the forensic examiner to download, examine and investigate the data present in a system.

(contd)

- The Wipe MASSter unit erases data from and sanitizes hard drives at speeds exceeding 3GB/Min for 9 drives simultaneously.
- The unit allows the user to perform high volume hard drive sanitizing operations using P-ATA S-ATA and laptop hard drives with optional adapters.
- Features:
  - High-speed wipe operation
  - Sanitize multiple drives simultaneously
  - Multiple media support
  - Partitions and formats drives
  - Sanitize different drive models and sizes
  - Password protected settings

What are Open Source Tools

Open source tools are tools that normally are available free of cost.

Examples Open Source Tools

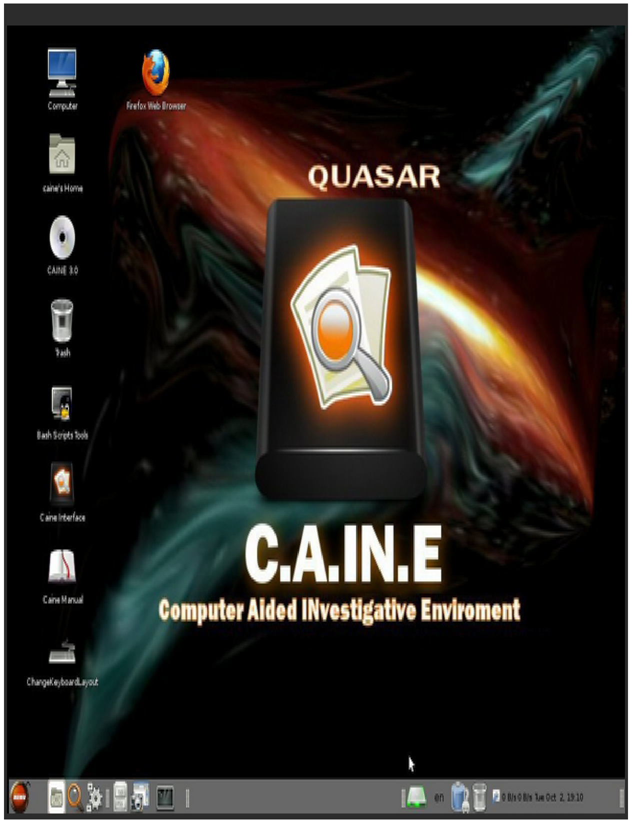
CAINE (Computer Aided Investigative Environment)

- **CAINE** (Computer Aided INvestigative Environment) is an **Italian** digital forensic project

  CAINE offers a complete forensic environment that is organized to integrate existing software tools as software modules and to provide a friendly graphical interface.

  The main design objectives that CAINE aims to guarantee are the following:

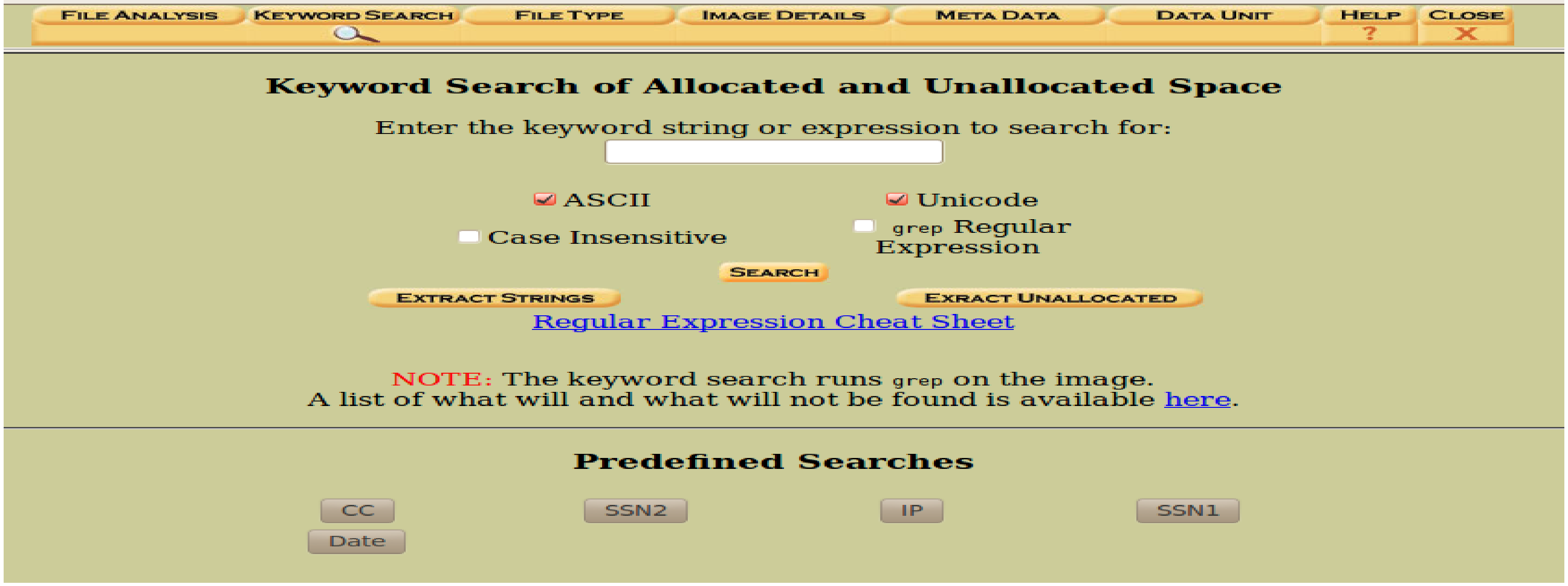
  - ❑ an interoperable environment that supports the digital investigator during the four phases of the digital investigation
  - ❑ a user friendly graphical interface
  - ❑ a semi-automated compilation of the final report



contd

Autopsy / The Sleuth Kit

- The Autopsy Forensic Browser is a graphical interface to the digital investigation tools in The Sleuth Kit. Together, they allow you to investigate the file system and volumes of a computer.



Keyword Search of Allocated and Unallocated Space

Enter the keyword string or expression to search for:

☑ ASCII ☑ Unicode

☐ Case Insensitive ☐ grep Regular Expression

Regular Expression Cheat Sheet

NOTE: The keyword search runs grep on the image.
A list of what will and what will not be found is available here.

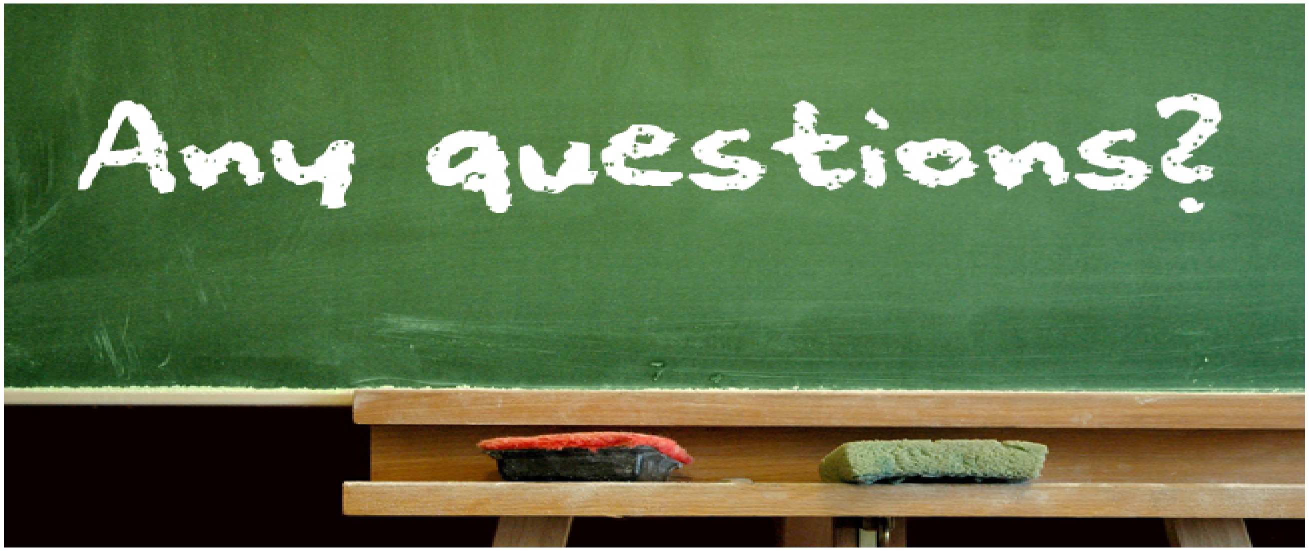
Predefined Searches

contd

Cuckoo Sandbox

- Cuckoo Sandbox is a malware analysis system.
- Its goal is to provide you a way to automatically analyze files and collect comprehensive results describing and outlining what such files do while executed inside an isolated environment.
- It's mostly used to analyze Windows executables, DLL files, PDF documents, Office documents, PHP scripts, Python scripts, Internet URLs and almost anything else you can imagine.
- But it can do much more...
  It's up to you to discover what and how.

Question Time



selukoto@gmail.com

255 3318