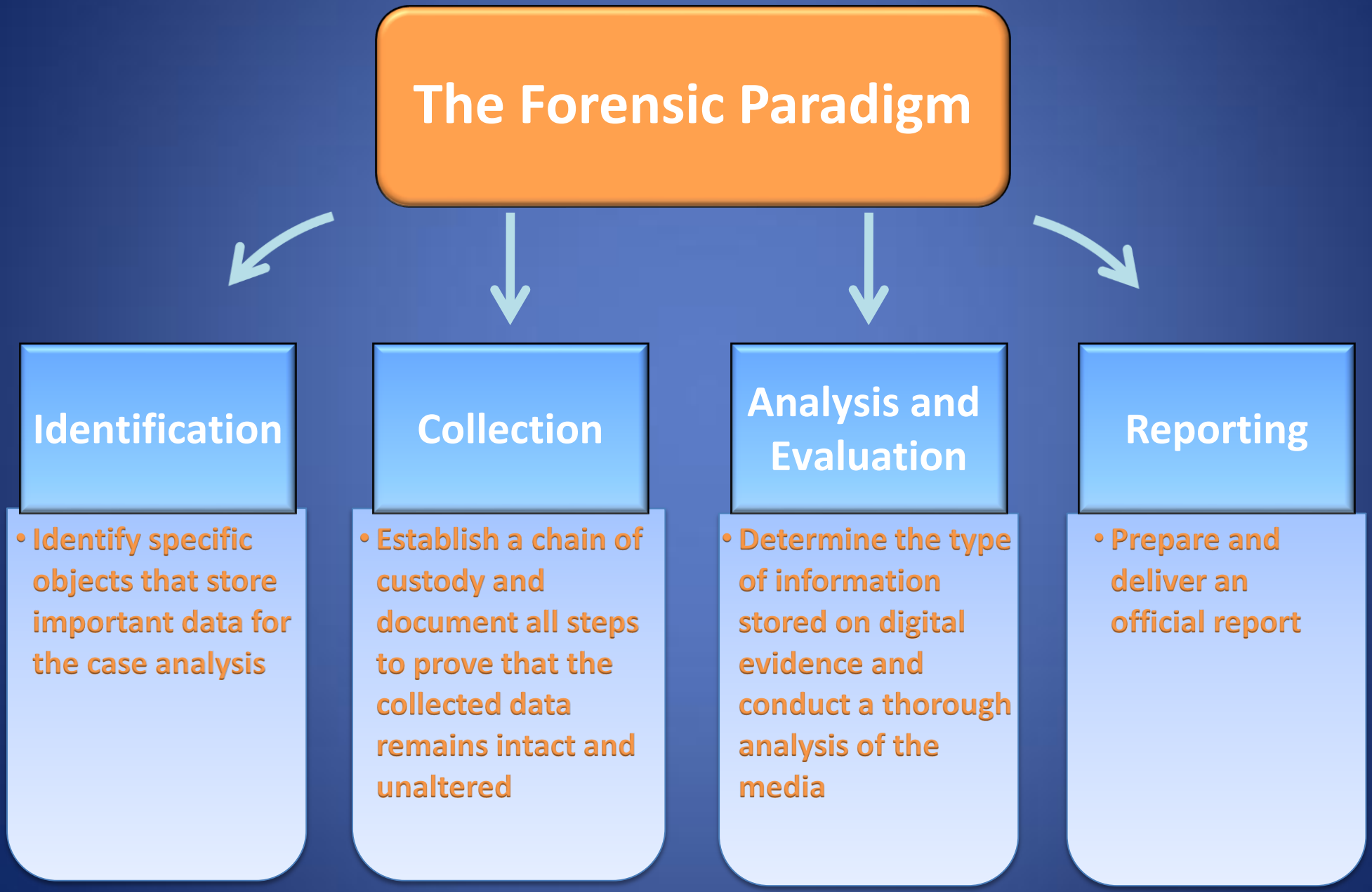
Computer Forensics

What is Computer Forensics?

- Scientific process of preserving, identifying, extracting, documenting, and interpreting data on a computer
- Used to obtain potential legal evidence

Computer Forensics Procedures



Identification: Common Mistakes …

- You are the investigator, which objects do you think will be useful for investigations?
  1. Computer (case and power supply)
  2. Just the hard drive (without computer)
  3. Monitor
  4. Keyboard and mouse
  5. Media (CD, DVD, USB drives, etc.)
  6. Printer

Digital forensics does not replace traditional forensic analysis

Any action that modifies the crime scene could invalidate evidence in court

Collection

- To collect computer evidence, care must be taken not to change the evidence
  - Imaging media using a write-blocking tool to ensure the suspect device is not be modified
  - Establishing and maintaining the chain of custody
  - Documenting everything that has been done
  - Using only tools and methods that have been tested and evaluated to validate their accuracy and reliability

Forensic Constraints

- Chain of custody
  - Maintain possession of all objects
  - Must be able to trace evidence back to source
  - “Prove” source integrity
- Priority by volatility
  - Some data is more volatile
  - RAM > swap > disk > CDs/DVDs
  - Idea: capture more volatile evidence first

Image Evidence: Laptop

Why Use Images

- Information on digital media is easily changed.
- Once changed it is usually impossible to detect that a change has taken place (or to revert the data back to its original state) unless other measures have been taken
- A common practice is calculate a cryptographic hash to establish a check point
- Examining a live file system changes state of the evidence
- The computer/media is the “crime scene”
- Protecting the crime scene is paramount as once evidence is contaminated, it cannot be decontaminated
- Really only one chance to do it right!

Collection: Common Mistakes …

- What is the first step to collect evidence, when you find:
  - A computer turned on
  - A computer turned off

A computer on a crime scene should be considered fully adversarial

HotPlug!


HOTPLUG LT™
MOUSE JIGGLER
Prevents a computer from falling asleep while you work!
wiebeTECH PCD
our best ideas store yours™

Analysis and Evaluation

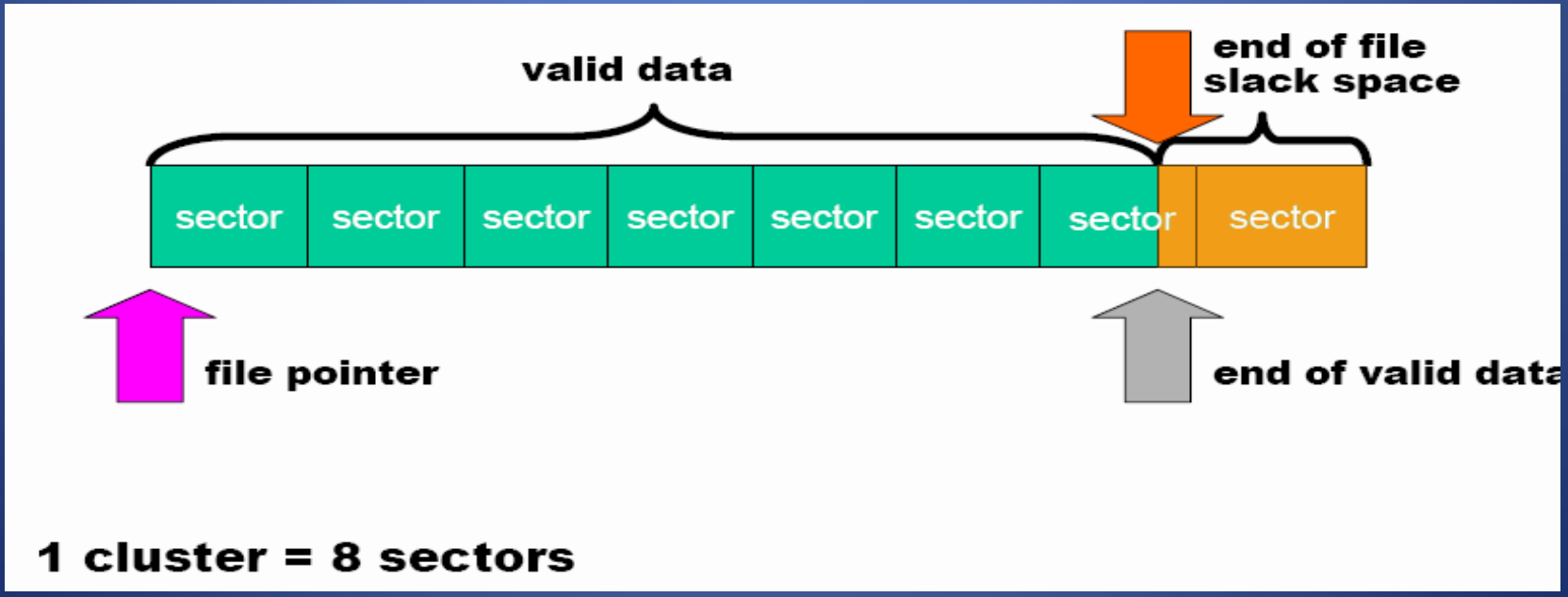
- Know where evidence can be found
- Understand techniques used to hide or “destroy” digital data
- Toolbox of techniques to discover hidden data and recover “destroyed” data
- Cope with HUGE quantities of digital data…
- Ignore the **irrelevant**, target the **relevant**
- Thoroughly understand circumstances which may make “evidence” unreliable
  - If you have a hard drive with a broken sector that gives different result, what happens when you hash the entire drive?

Where is the Evidence?

- Undeleted files, expect some names to be incorrect
- Deleted files
- Windows registry
- Print spool files
- Hibernation files
- Temp files (all those .TMP files in Windows!)
- Slack space
- Swap files
- Internet browsing histories
- Alternate or “hidden” partitions
- On a variety of removable media (USB drives, backup tapes, …)

Hidden Data in the Hard Drive Slack Space

- Slack space is the space between
  - The logical end of the file (i.e., the end of the data actually in the file) and
  - The physical end of the file (i.e., the end of the last sector devoted to the file).



Digital Forensics Tools

- Forensics tools are typically command line tools that are guaranteed not to alter the disk:
  - HELIX a live cd with a plenty of forensic tools ready to be used
  - ENCASE a series of proprietary forensic software products produced by Guidance Software
  - AUTOPSY …

How to Hide Data?

- Cryptography
- Steganography
  - The process of hiding data inside other data (e.g. image files).
- Change file names and extensions
  - E.g. rename a .doc file to a .tmp file
- Hidden tracks
  - most hard disks have # of tracks hidden (i.e. track 0)
  - They can be used to hide/read data by using a hex editor
- Deleted Files
  - not truly deleted, merely marked for deletion.

During Forensic is important to do not use any tools that write to the disk

Why Create a Duplicate Image?

- A file copy does not recover all data areas of the device for examination
- Working from a duplicate image
  - Preserves the original evidence
  - Prevents inadvertent alteration of original evidence during examination
  - Allows recreation of the duplicate image if necessary

Bitstream vs. Backups

- Forensic copies (Bitstream)
  - Bit for bit copying captures all the data on the copied media
  - Including hidden and residual data (e.g., slack space, swap, residue, unused space, deleted files etc.)
- Often the “smoking gun” is found in the residual data.
- Logical vs. physical image

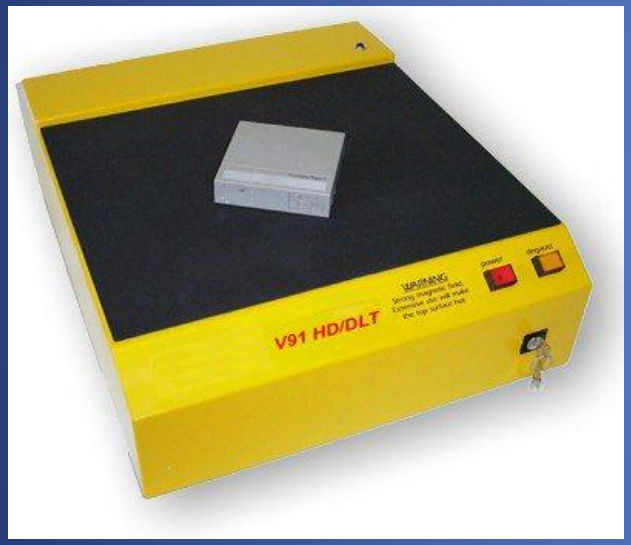
Reporting

- Accurately describe the details of an incident
- Be understandable to decision makers
- Be able to withstand legal scrutiny
- Be unambiguous and not open to misinterpretation
- Be easily referenced
- Contain all information required to explain the conclusions
- Offer valid conclusions, opinions, or recommendations when needed
- Create report in a timely manner

Anti-Forensic and Data Security

- Anti-forensic techniques try to frustrate forensic investigators and their techniques
- Securely deleting data, so that it cannot be restored with forensic methods
- Prevent the creation of certain data in the first place
- Data which was never there, obviously cannot be restored with forensic methods.

Privacy Through Media Destruction



Degausser
Magnetic Field

or

shredder

or thermite…

Disk Wiping

- Simple erase
  - The data is still on the drive but the segment has been marked as available
  - Next time data is written to the drive it MAY overwrite the segment
- Destructive erase
  - First overwrites all data in the file with random data
  - Next marks the segment as available
  - It may be possible to find ghost images of what was previously on the disk surface

Overwriting Hard Drive Data: The Great Wiping Controversy, ICISS 2008

Solid-state drives (SSD)

- Different deletion/allocation mechanism
  - E.g. Erase in 256KB blocks, write in 4KB blocks
- Wear-leveling and extra space
- Specific commands to mark data (TRIM)