# DIGITAL FORENSICS 101

>whoami

- Aaron J. Scantlin
- Adjunct Professor - College of Engineering
- Security Analyst - MU Division of IT
- Conduct Committee/DJ/Speaker - SecKC
- GSEC, GCFA certified
- ***Huge nerd***

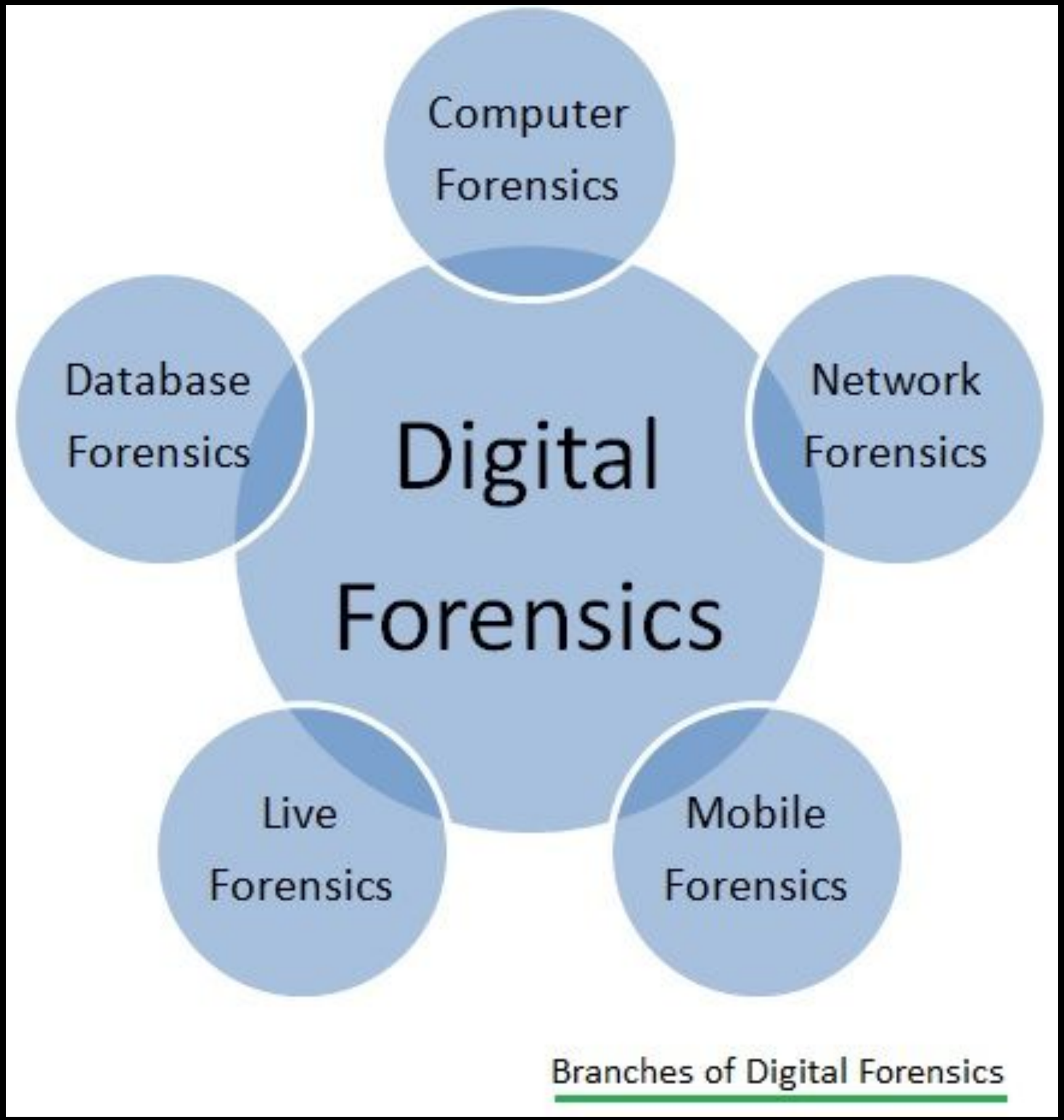

# What Is Digital Forensics?

The Digital Forensics Research Workshop in 2001 defined Digital Forensic Science as [6]:

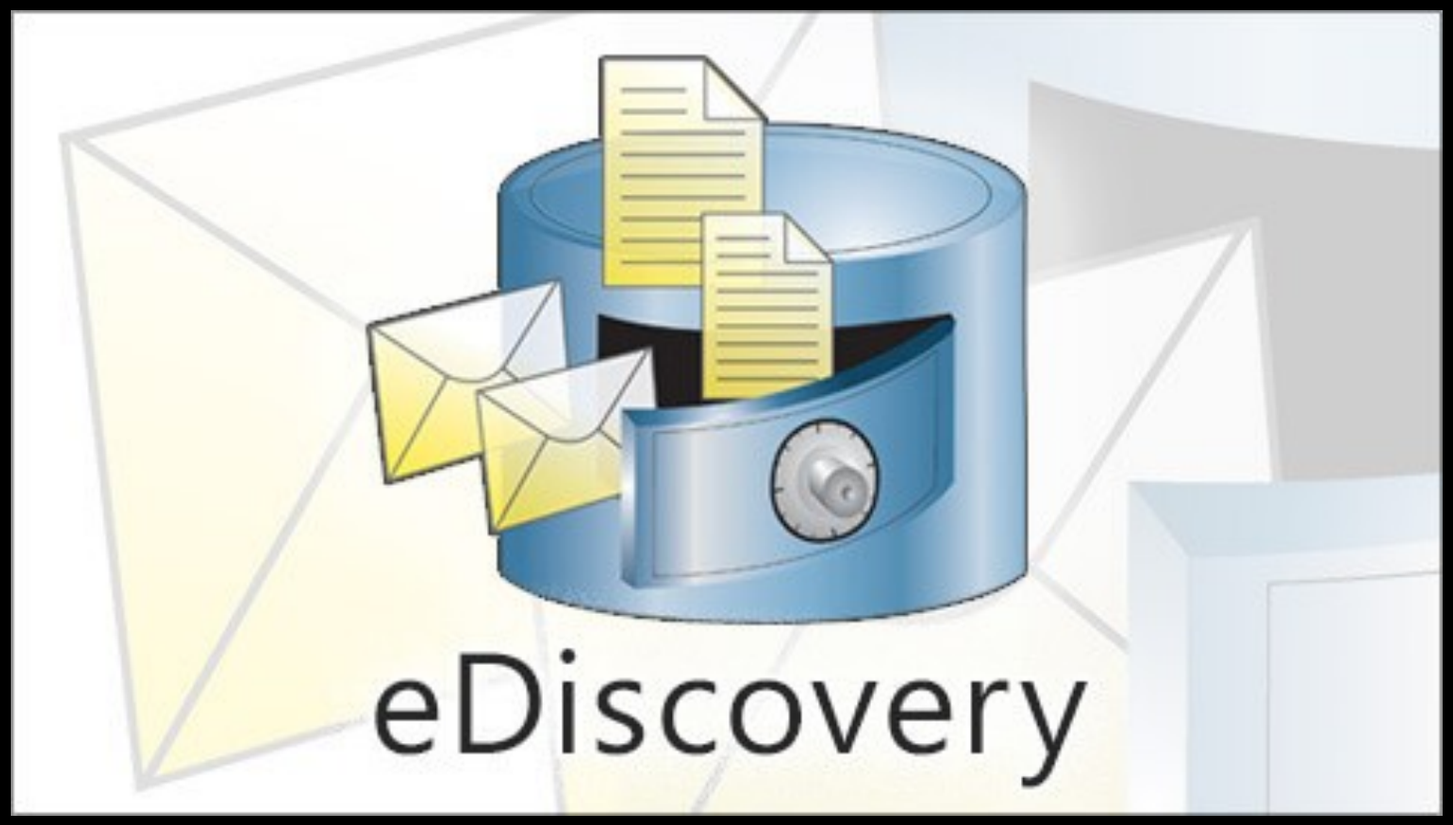
> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

"The process of acquiring and examining digital artifacts that correspond to activity in the physical realm."

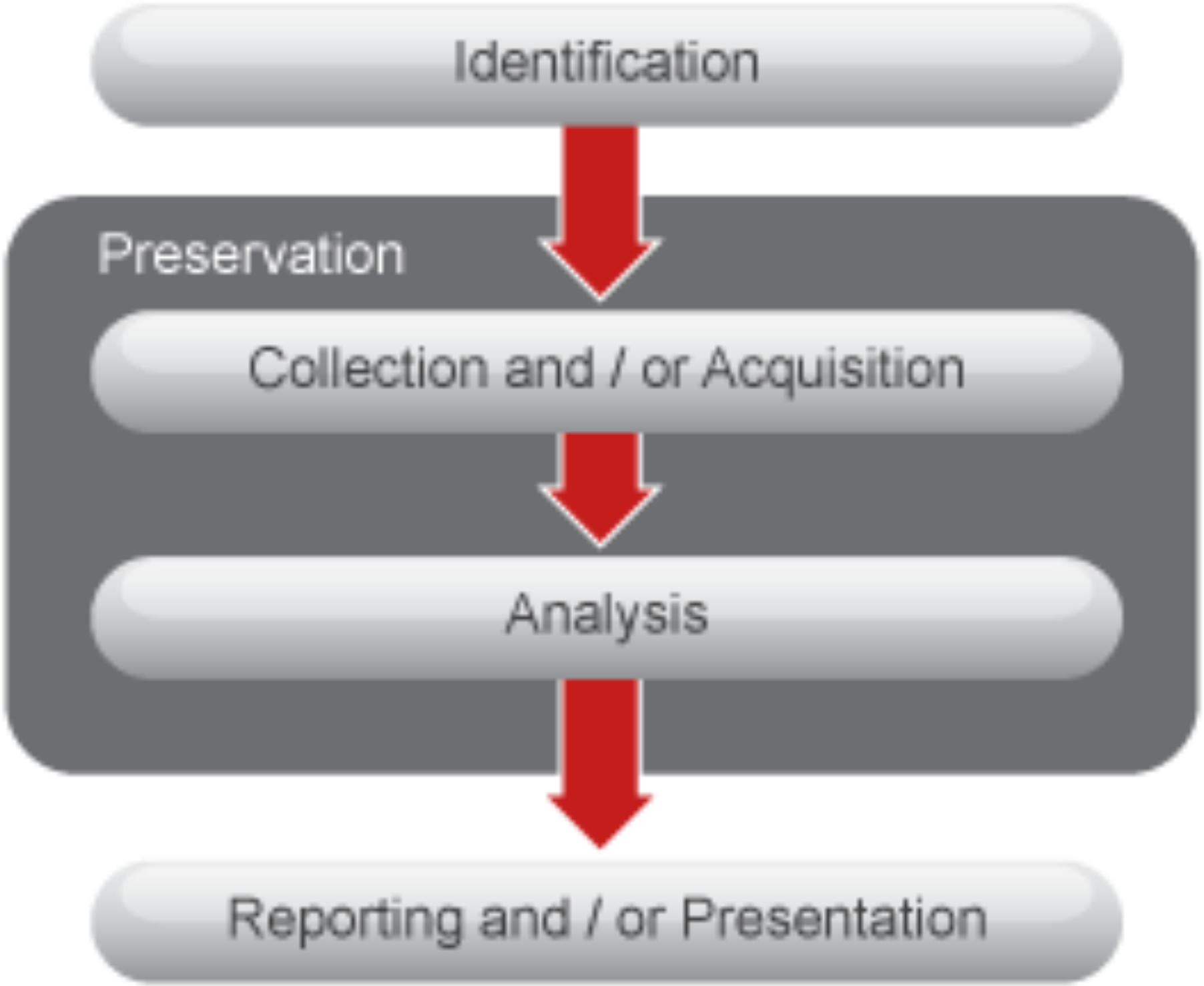
-Me, like a week ago I think?




Branches of Digital Forensics


eDiscovery

# DIGITAL FORENSIC METHODOLOGY



AUGUST 3, 2013
#481920
LOG: 0

JULY 9, 2013
#453201
LOG: 1

# IDENTIFICATION

# ACQUISITION

# MEMORY ACQUISITION TOOLS

- Windows: FTK Imager, Redline
- macOS: Rekall (only works up to 10.12)
- Linux: Rekall
- Virtual Machines: Take a snapshot of the running system
  - QEMU/Xen: If you have access to the hypervisor manager, these platforms allow you to dump memory of a running guest


TABLEAU
FireWire800+USB2.0 SATA Bridge
A On
B On
DC IN B
DC IN A
USB 2.0
800
800
800
400
SATA
Power
SATA Detect
Host Detect
Write Block
Activity
DC OUT
Maxtor
DiamondMax Plus 9
80GB SATA/150 HDD
Made under U.S. and foreign patents issued and pending.
For full warranty, patent or installation information, contact: www.maxtor.com
Maxtor is not responsible for consequential damages, including loss or recovery of data.
3.5 SERIES
FRAGILE
OLD MAIL SERVER
Made in Singapore

# DISK ACQUISITION TOOLS

- Can you physically remove the hard drive from the target?
  - If so, FTK Imager
- If not:
  - macOS: Paladin
  - Everything else
    - Boot the system using your preferred Live Linux distro (suggestion: SIFT Workstation)
    - Mount the target disk and use dd to copy

# ANALYSIS

# MEMORY IMAGE ANALYSIS TOOLS

Volatility

(Memory analysis of macOS 10.13+ requires a paid tool at this time.)

```
remnux@remnux:/media/C8D5-495F/TorrentLocker$ volatility -f xpsp3-after-infection.dmp --profile=WinXPSP3x86 pstree
Volatility Foundation Volatility Framework 2.3.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c8830:System                                      4      0     56    263 1970-01-01 00:00:00 UTC+0000
. 0x81f877c0:smss.exe                                 536      4      3     19 2014-12-19 20:24:47 UTC+0000
.. 0x822a1020:csrss.exe                               600    536     11    338 2014-12-19 20:24:48 UTC+0000
.. 0x81f16da0:winlogon.exe                            624    536     17    502 2014-12-19 20:24:49 UTC+0000
... 0x822f64f0:wpabaln.exe                           1940    624      1     58 2014-12-19 20:26:51 UTC+0000
... 0x81df5020:lsass.exe                              680    624     20    344 2014-12-19 20:24:49 UTC+0000
... 0x81f0c850:services.exe                           668    624     16    255 2014-12-19 20:24:49 UTC+0000
.... 0x81de5da0:svchost.exe                          1024    668     59   1159 2014-12-19 20:24:49 UTC+0000
..... 0x81d98020:wscntfy.exe                          260   1024      1     28 2014-12-19 20:24:51 UTC+0000
.... 0x822a3708:spoolsv.exe                          1444    668     10    130 2014-12-19 20:24:51 UTC+0000
.... 0x81efb750:svchost.exe                          1072    668      6     83 2014-12-19 20:24:49 UTC+0000
.... 0x81f08380:vmacthlp.exe                          836    668      1     25 2014-12-19 20:24:49 UTC+0000
.... 0x822ef020:alg.exe                               328    668      6    107 2014-12-19 20:26:04 UTC+0000
.... 0x82279780:svchost.exe                           852    668     15    189 2014-12-19 20:24:49 UTC+0000
..... 0x81e8eb28:wmiprvse.exe                         868    852      5    136 2015-02-28 17:07:59 UTC+0000
.... 0x82192d08:svchost.exe                           932    668      9    257 2014-12-19 20:24:49 UTC+0000
.... 0x82185360:svchost.exe                          1140    668     14    199 2014-12-19 20:24:50 UTC+0000
.... 0x82190020:vmtoolsd.exe                         1020    668      6    259 2014-12-19 20:26:00 UTC+0000
0x8225e020:explorer.exe                              1872   1380      8    328 2015-02-28 17:06:16 UTC+0000
 0x822f2020:vssadmin.exe                             1168   1872      0 ------ 2015-02-28 17:06:16 UTC+0000
 0x8214a8e0:IEXPLORE.EXE                             1224   1872      5    194 2015-02-28 17:14:54 UTC+0000
0x821711a0:explorer.exe                              1564   1548     15    569 2014-12-19 20:24:51 UTC+0000
. 0x8216b590:vmtoolsd.exe                            1668   1564      5    213 2014-12-19 20:24:52 UTC+0000
. 0x81f544f8:VMwareTray.exe                          1660   1564      1     52 2014-12-19 20:24:52 UTC+0000
```

The parent process of explorer.exe does not exist. This is rather suspicious!

Explorer.exe launched Volume Shadow Copies util?

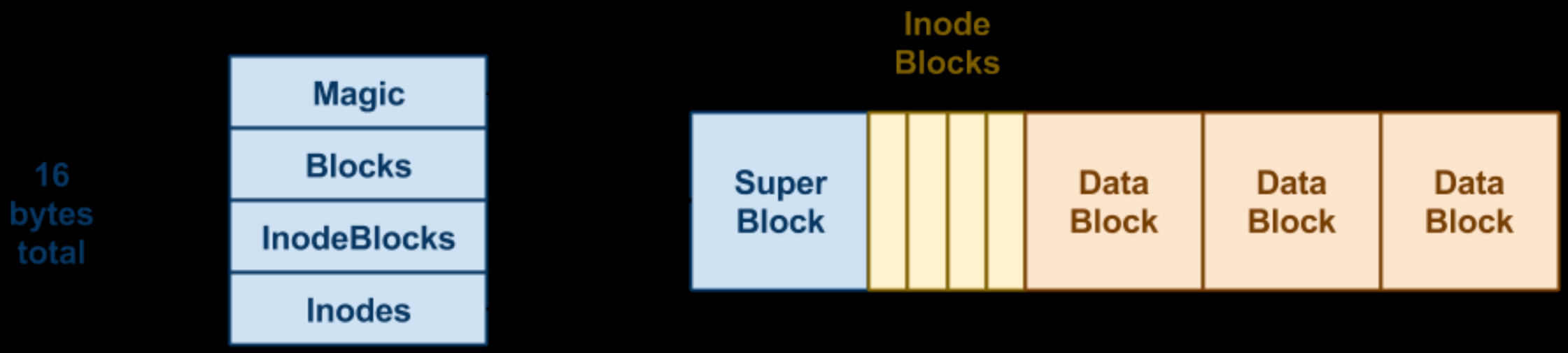
# DISK IMAGE ANALYSIS TOOLS

SIFT

# WHAT ARE WE LOOKING AT?

Under the hood, all files are just a collection of hex bytes.

A file system describes how those files are stored.

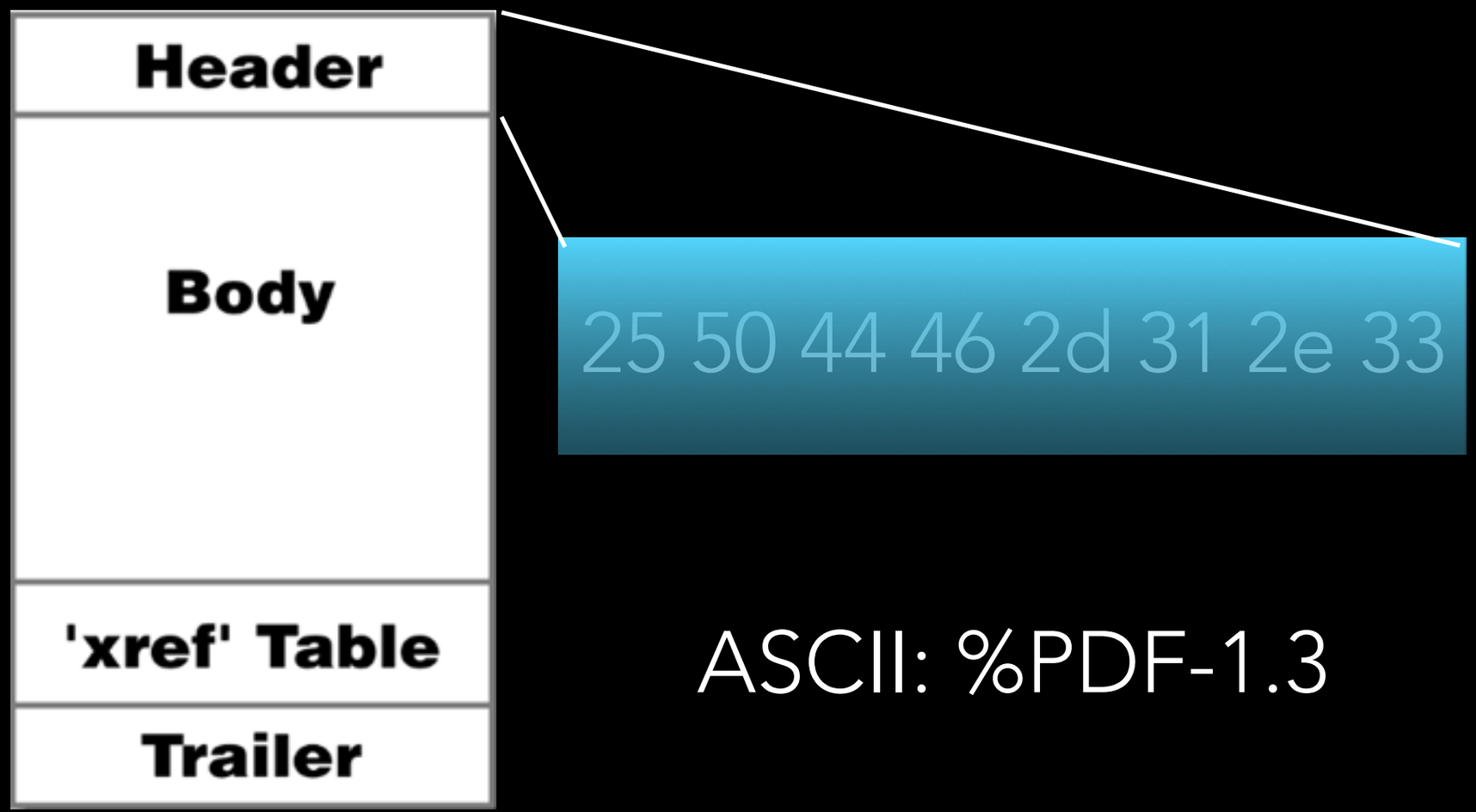



SFS (Simple File System)

# WHAT ARE WE LOOKING AT?

Similarly, files themselves contain a file header prepending the actual data contained in it.

PDF File Format



*a totally real image of me doing file carving*

00 00 01 Bx MPEG

[512 (0x200) byte offset]

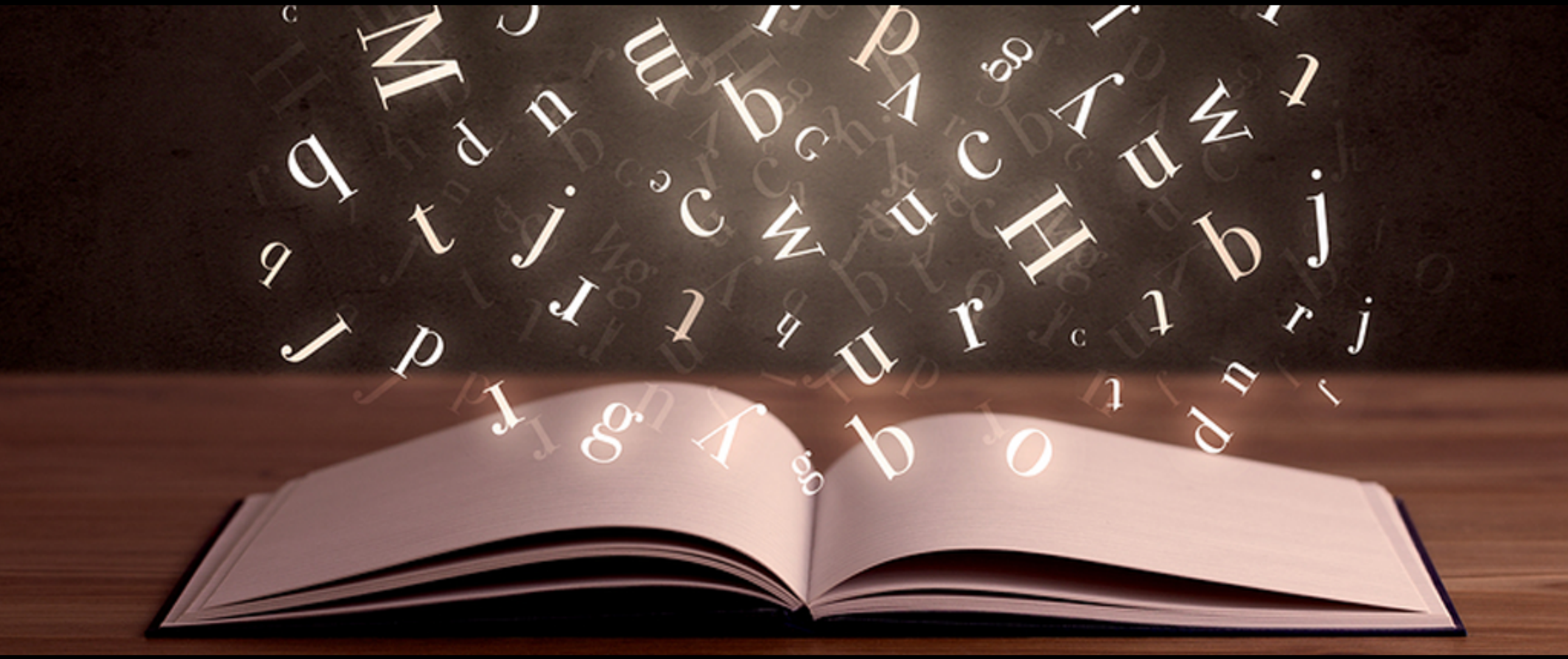
00 6E 1E F0 PPT

FF D8 JPG

89 50 4E 47 0D 0A 1A 0A PNG

SOME COMMON "MAGIC NUMBERS"

HTTPS://WWW.GARYKESSLER.NET/LIBRARY/FILE_SIGS.HTML



# REPORTING

**Formal Forensic Report Template** (use as a template to create your formal report)

- Recopy verbatim everything not in italics and fill in appropriate information where asked.
- Use specific technical terms, but provide CLEAR explanations about them.
- Use the questions at the end of each scene as a guide for your analysis.
- Report should be typed font size 12, Arial or times new roman, 1.5 spacing, <1" margins
- Report is due January 26, 2011.

**To:** Dr. Sheila Gonzalez

**From:** (*Place your team members' names here)*

**Re:** Theodore Gardner: examination of the skeletal remains. Case # *(fill in a number).*

**Introduction:**

On the 19th day of January 2011, at approximately *(give time class begins )*the remains of Theodore Gardner were exhumed. Dr. Sheila Gonzalez presented the skeletal remains to her lab assistants. Dr. Gonzalez and her team began the investigation ordered by the Grand Jury into the death of the 15 year old male. An autopsy of the skeletal remains was performed. The complete skeleton was comprised of *(list the 2 divisions of the skeletal system & the groups of bones contained in each)*. The lab assistants were given the instructions to analyze and research facts collected via physical observations and radiographs and to explain and analyze causes and processes that occurred regarding the evidence gathered.

**Skeletal Assessment:**

(*Discuss the evidence gathered concerning the skeletal remains of Theo Gardner… use appropriate vocabulary from chapter)*

**Analysis**:

(*Explain and analyze causes and processes that occurred that would result in the evidence you collected from the Theo Gardner's bones)*

**Expert Opinion:**

(*Draw a conclusion with your expert team concerning whether Theo was abused by his aunt and uncle or his death was simply an untimely event)*

Things to consider as you investigate the death of Theo Gardner and write your Forensic report:

- What is the most compelling piece of evidence in the case for your conclusion?
    - What is not so compelling?
    - Is there anything in the case that your group found irrelevant?
    - What is not so compelling?
    - Is there anything in the case that your group found irrelevant?