# Reporting for Digital Forensics

**Jason Wilkins,**
Clayton County Police Dept.

Live Online

**FREE SUMMIT: JULY 22–23**
**TRAINING: JULY 26–31**

SANS
DFIR SUMMIT
& TRAINING 2021

# AGENDA

Introduction

The Importance of Reports

Guidelines for Writing

Generating Reports

# INTRODUCTION

Jason Dywane Wilkins

- 8 Years US Navy (Seabees) “CAN DO!”
- 15 Yrs Firefighter / EMT / HAZMAT Tech / Rescue Tech
- AAS Criminal Justice – Iowa Central Community College
- AAS Computer Networking – Iowa Central Community College
- 4 Yrs Network Analyst for The Carlstar Group
- 2 Yrs Crime & Intelligence Analyst / Digital Forensics Analyst – Clayton County Police Department – Metro Atlanta, GA
- Magnet Certified Forensic Examiner
- Instructor in Digital Forensics - Iowa Central Community College
- Inventor of Rictameter


# THE IMPORTANCE OF REPORTS

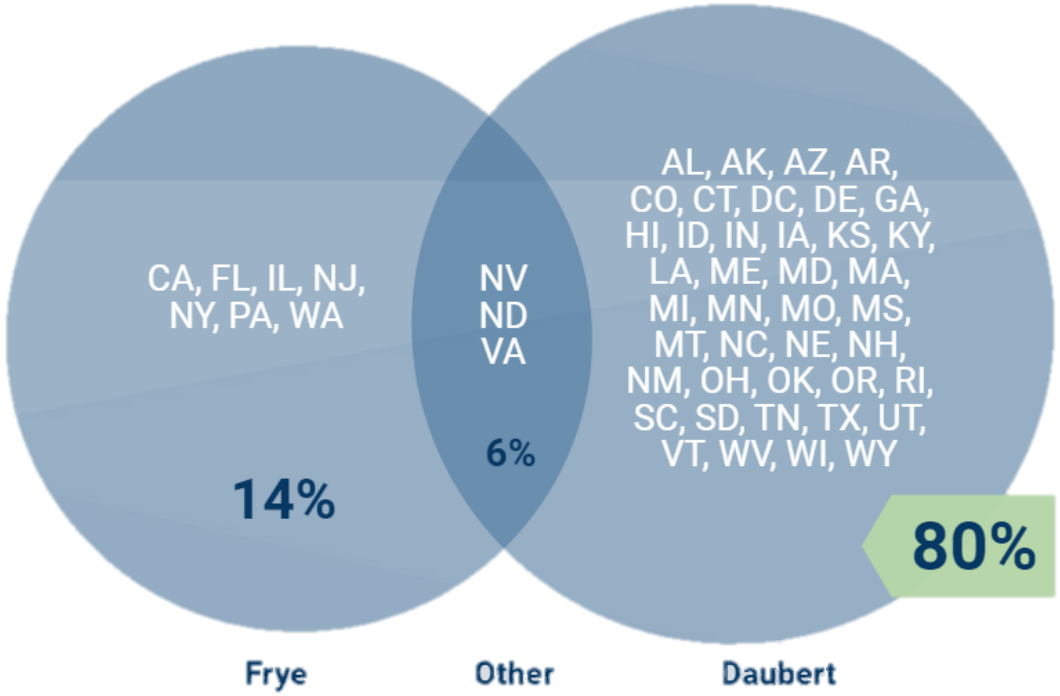
LET'S DIVE IN

# EXPECT TO BE CROSS-EXAMINED

# EXPERT WITNESSES MUST PROVIDE A WRITTEN REPORT


- Federal Rules of Civil Procedure Rule 26 - FRCP 26 (a) (2)
- Federal Rules of Evidence – FRE 702, 703, 705
- Daubert vs. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579
- Frye vs. United States, 293 F. 1013 (D.C. Cir. 1923)

# GENERALLY ACCEPTED OR SCIENTIFICALLY VALID?



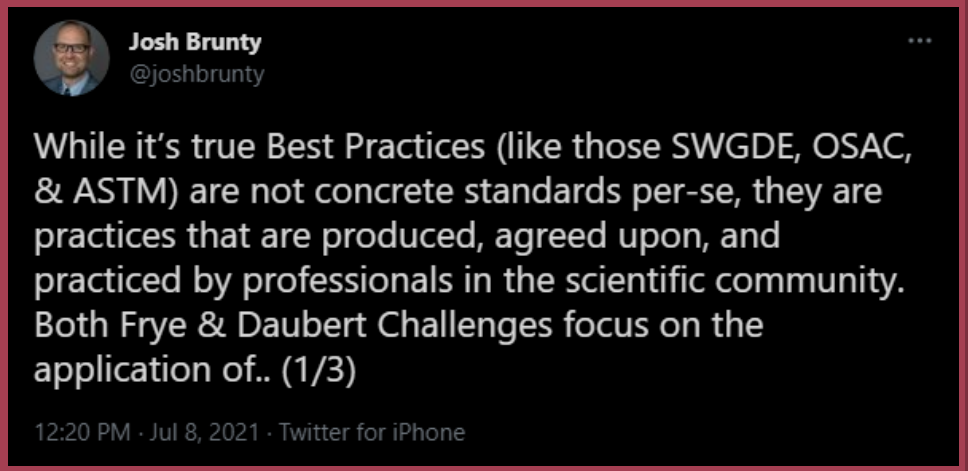

## Frye v Daubert

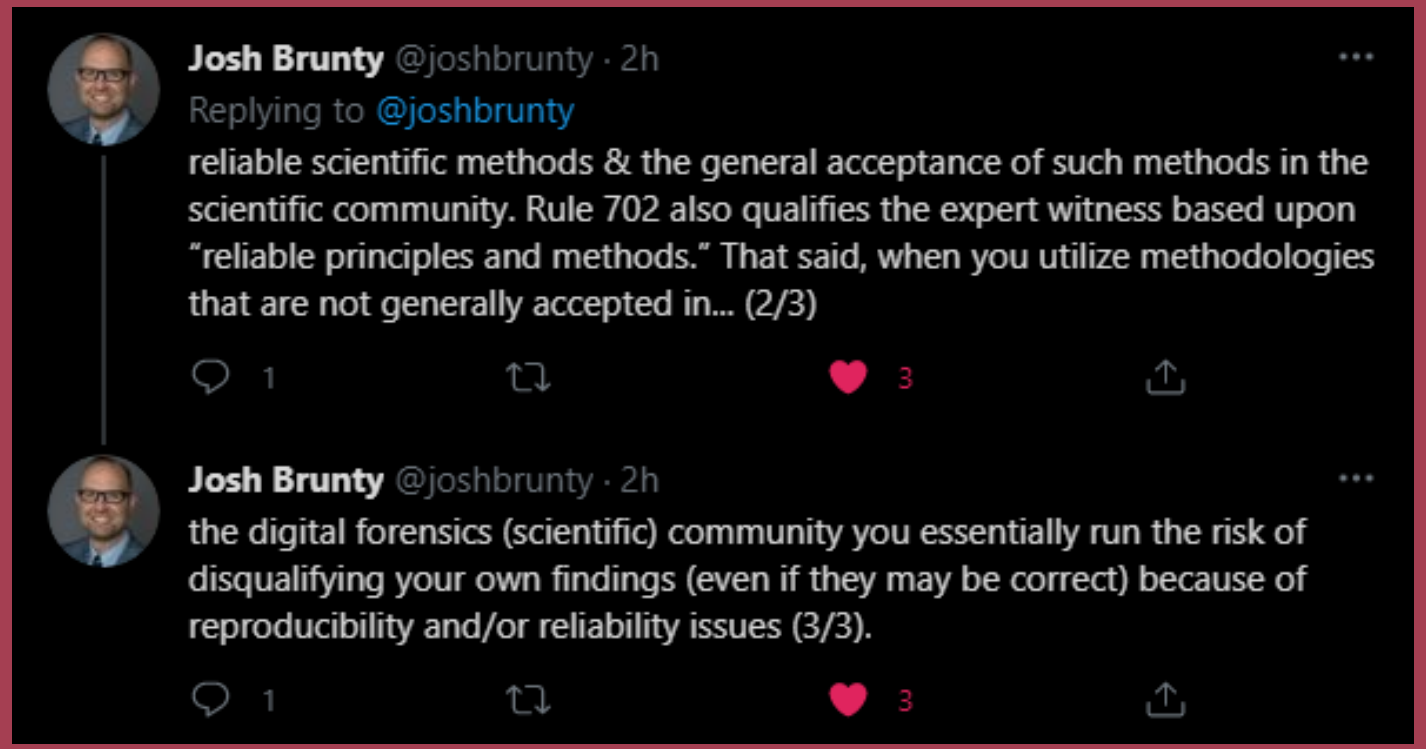
**Frye**

- The basic Fry rule:
  - Testimony must be based on a principle that is "sufficiently established to have gained general acceptance"
- What does the test involve?
  - 1. A pre-trial ruling
  - 2. whether the basic **principle** is ultimately based has been
  - 3. **generally accepted**

**Daubert**

- Basic Daubert rule:
  - Reasoning or methodology underlying the testimony must be scientifically valid
- What does the test involve?
  - 1. a preliminary ruling
  - 2. on whether the **theory or technique**
  - 3. is **scientifically valid**

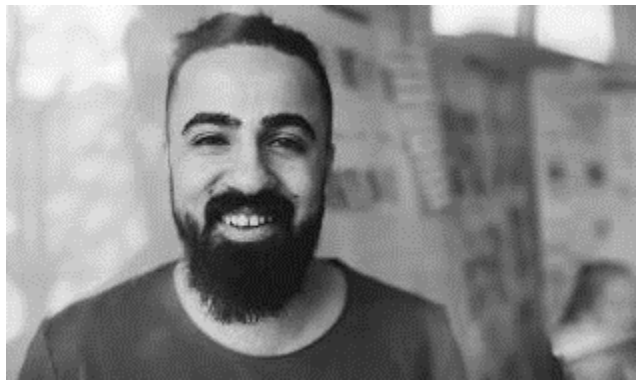

Josh Brunty
@joshbrunty
While it's true Best Practices (like those SWGDE, OSAC, & ASTM) are not concrete standards per-se, they are practices that are produced, agreed upon, and practiced by professionals in the scientific community. Both Frye & Daubert Challenges focus on the application of.. (1/3)
12:20 PM · Jul 8, 2021 · Twitter for iPhone


Josh Brunty @joshbrunty · 2h
Replying to @joshbrunty
reliable scientific methods & the general acceptance of such methods in the scientific community. Rule 702 also qualifies the expert witness based upon "reliable principles and methods." That said, when you utilize methodologies that are not generally accepted in... (2/3)
1
3
Josh Brunty @joshbrunty · 2h
the digital forensics (scientific) community you essentially run the risk of disqualifying your own findings (even if they may be correct) because of reproducibility and/or reliability issues (3/3).
1
3

In addition to opinions and exhibits, the written report must specify fees paid for expert witness service over preceding 4 years.

PRO TIP: KEEP TRANSCRIPTS OF PRIOR TESTIMONY



# LIMIT REPORT TO SPECIFICS

Before you begin writing, identify your audience and the purpose of the report to help you focus on specifics.

If the audience has little technical knowledge you may have to educate them on technical issues.

Make an examination plan to serve as a guideline for expected questions.

# GUIDELINES FOR WRITING

JUST THE FACTS

# PROFESSIONAL OPINION


The law requires that an expert who doesn't have personal knowledge about a system or occurrence must state opinions by response to hypothetical questions.

Unlike an ordinary witness, you are giving evidence as an opinion based on professional knowledge and experience.

State ONLY the facts necessary to answer the question.

ANYTHING that you write down as part of your examination is subject to discovery from the opposition.

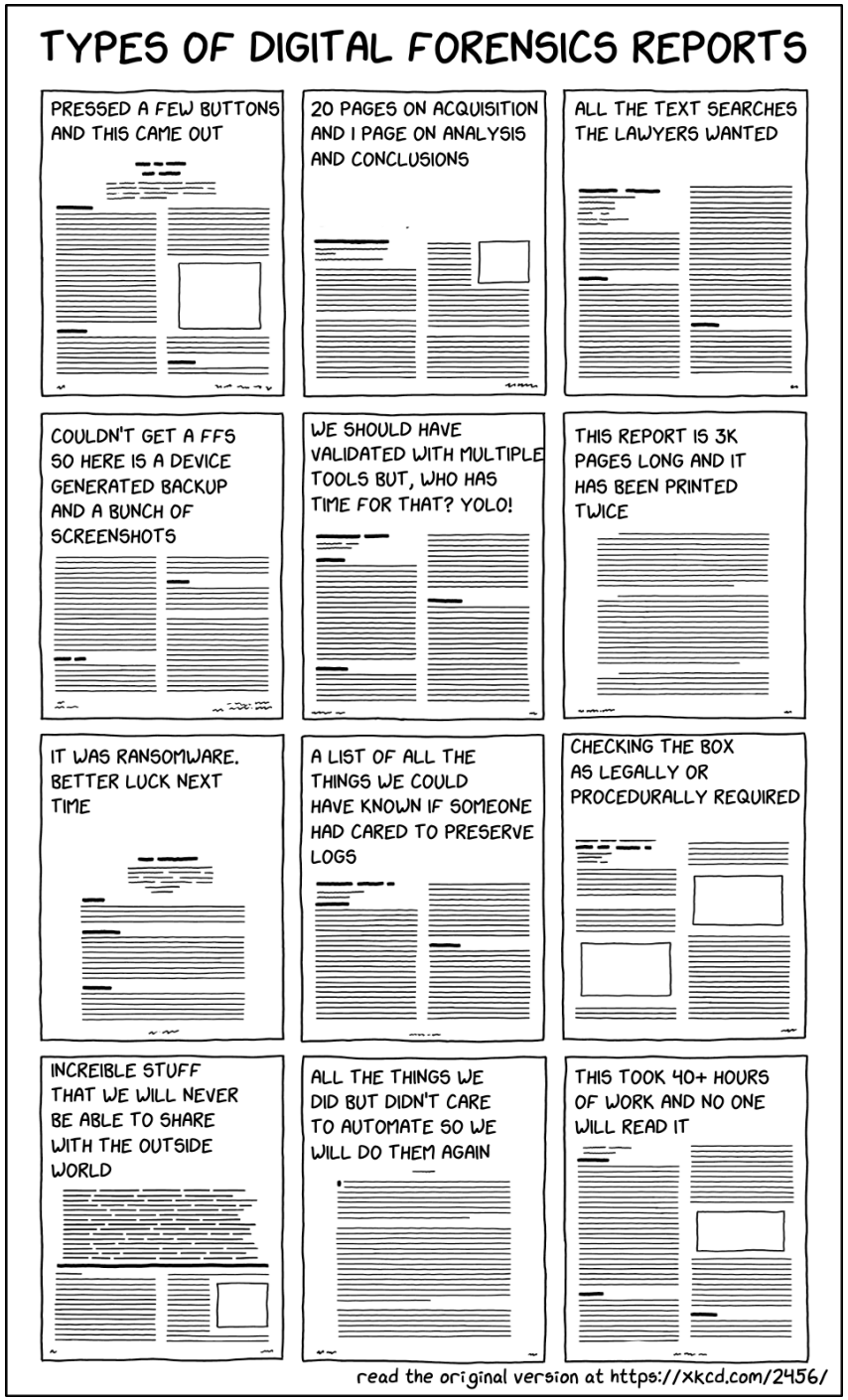



Image courtesy of Alexis Brignoni

# REPORT STRUCTURE

## ORDER MAY VARY

- Abstract (or summary)
- Table of Contents
- Body of Report
- Conclusion
- References
- Glossary
- Acknowledgements
- Appendixes

- Each section should be titled
- The abstract is a summary, so write it last.

# THINGS TO CONSIDER

## WRITE CLEARLY

- Is it easy to read? Think of your audience.
- Is it organized and relevant?
- Is the language simple and direct?
- Is it accurate and consistent?
- Check grammar, spelling, and punctuation.

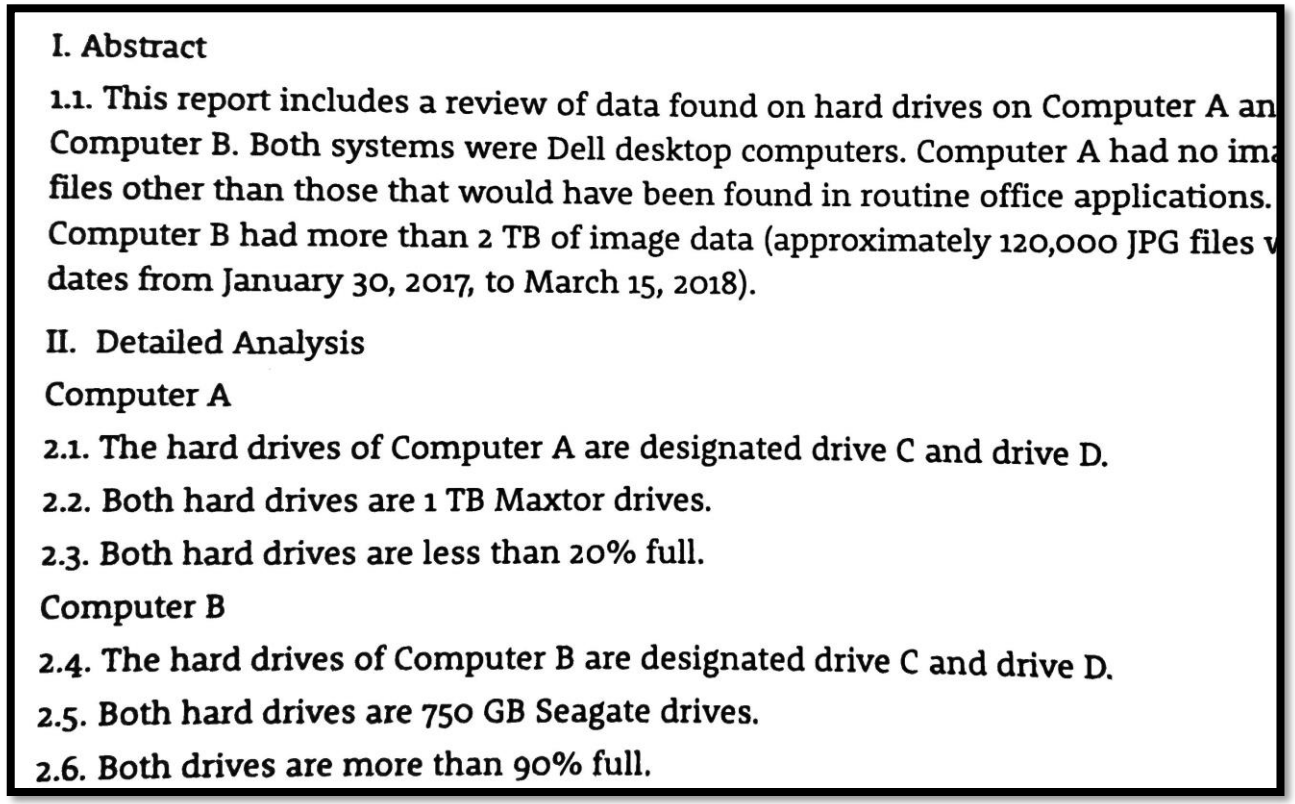
## CONSIDER STYLE

- Use a natural language style. Talk of yourself in the first person.
- Avoid vague language and generalizations.
- Avoid repetition and being overly detailed.
- Project objectivity.

## USE SIGNPOSTS

- Use sequence language. (i.e. The first step was…)
- Highlight main points so readers can scan quickly.
- When evaluating, “The problem with this is…” “This means that…”

# USE A NUMBERING SYSTEM



I. Abstract

1.1. This report includes a review of data found on hard drives on Computer A an Computer B. Both systems were Dell desktop computers. Computer A had no ima files other than those that would have been found in routine office applications. Computer B had more than 2 TB of image data (approximately 120,000 JPG files v dates from January 30, 2017, to March 15, 2018).

II. Detailed Analysis

Computer A

2.1. The hard drives of Computer A are designated drive C and drive D.

2.2. Both hard drives are 1 TB Maxtor drives.

2.3. Both hard drives are less than 20% full.

Computer B

2.4. The hard drives of Computer B are designated drive C and drive D.

2.5. Both hard drives are 750 GB Seagate drives.

2.6. Both drives are more than 90% full.

- A report using a numbering system divides material into sections and restarts numbering with each main section.

- With this system, readers can scan the headings and understand how one part of the report relates to the other.

# USE SUPPORTING MATERIAL

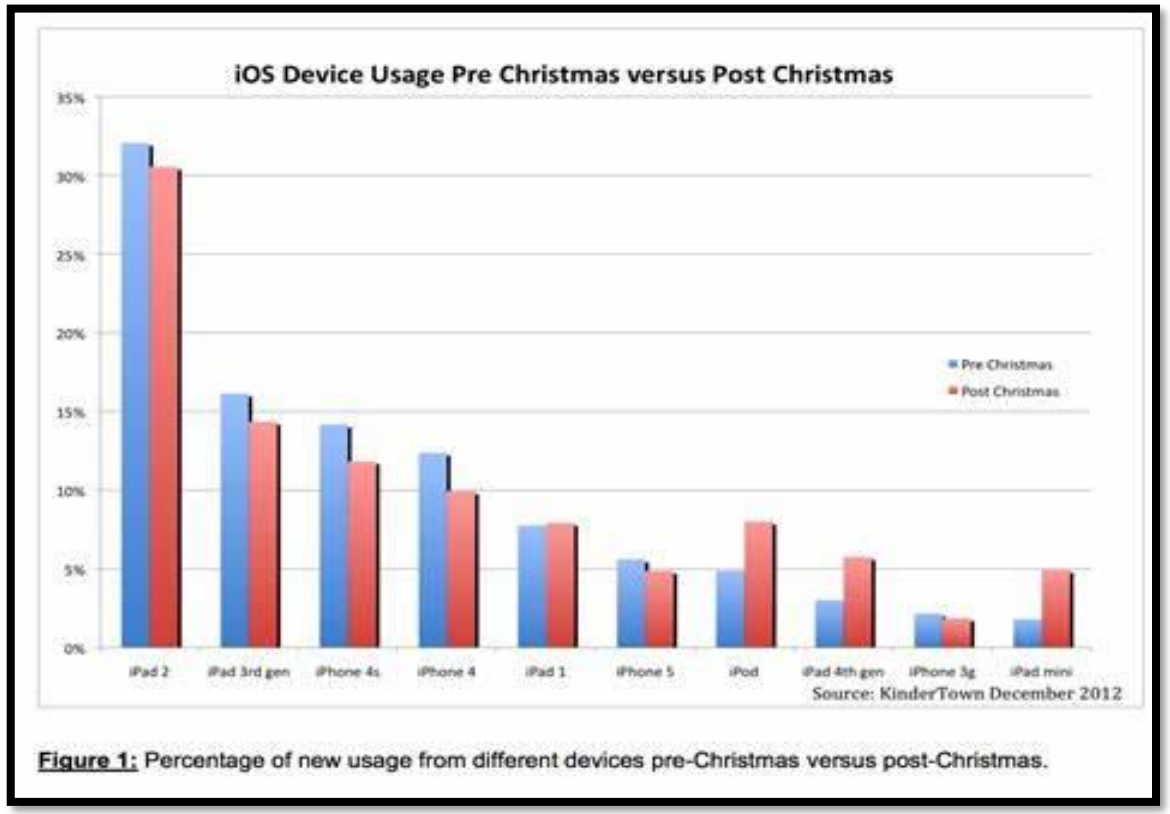
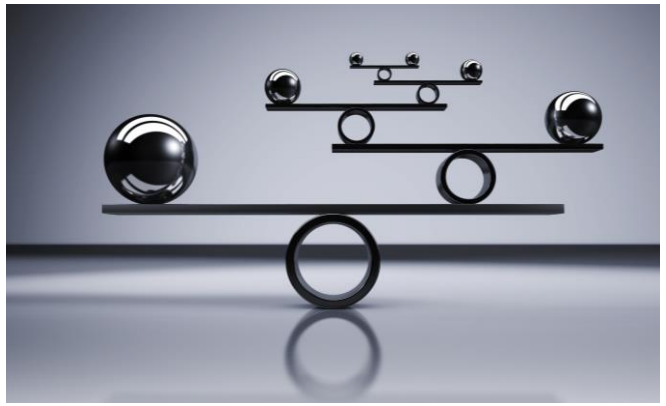



**Figure 1:** Percentage of new usage from different devices pre-Christmas versus post-Christmas.

- Number figures and tables sequentially as they are introduced. (i.e. Figure 1, Table 1, etc)

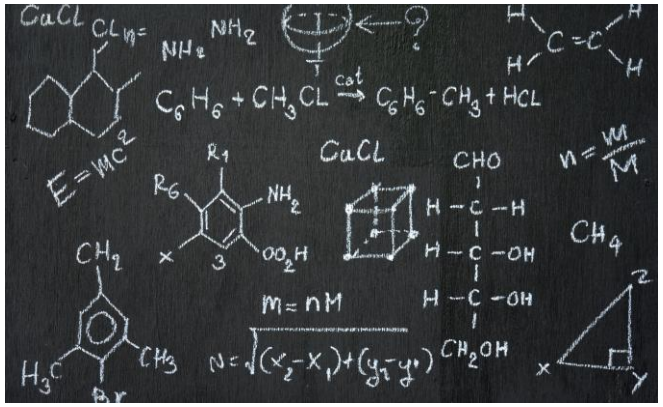
- Figure captions should supply descriptive information and be inserted after the paragraph in which it is introduced.

# MORE THINGS TO CONSIDER



## FORMAT CONSISTENTLY

- How you format is less important than being consistent.
- Use the same font throughout.
- Use % OR “Percent”, but not both.




## INCLUDE CALCULATIONS

- Give the common name for hashing algorithms used. (i.e. MD5)
- Explain why you chose the hash and cite National Software Reference Library (NSRL) as an authority.

## PROVIDE ERROR ANALYSIS

- A statement of limitations of knowledge and uncertainty is necessary to protect your credibility.
- Be sure to state that there is no absolute assurance that a file’s timestamp is a reflection of its actual creation time.

# EXPLAIN YOUR RESULTS AND CONCLUSIONS

- Describe what you ACTUALLY found, not what you HOPED to find.

- Include these explanations as you present results in a logical manner using headings and subheadings to provide clarity.


"I like the creative way you manipulate reality. You may be just the man we need to write our corporate annual reports."

# PROVIDE REFERENCES

References

Owner/Author/Creator. (Publication Date or n.d.). *Title of image in italics* [media type such a Painting, Outdoor mural, Photograph, Infographic]. Retrieved from URL

Emery, A. (2016, August 8). *Flamingo* [Photograph]. Retrieved from https://unsplash.com/@alanemery?photo=SYzUF6XcWBY

Featherstone, D. (n.d.). *Pink Flamingo Lawn Ornament* [Photograph]. Retrieved from http://americanhistory.si.edu/collections/search/object/nmah_1425282

BioExpedition Publishing. (2014). *American Flamingo* [Infographic]. Retrieved from http://www.flamingos-world.com/american-flamingo-infographic/

- You MUST cite ALL material you have used as sources for the content of your work.
- Give enough detail so that someone else could track down the information.
- Follow a standard format like APA or MLA.


19


# SOME EXAMPLE REPORTS

- Forensic Examination of Digital Evidence: A Guide for Law Enforcement (US DoJ)
- https://tinyurl.com/4x42mwz6

- Example of An Expert Witness Digital forensics Report
- https://tinyurl.com/sbmh6mde

# GENERATING TOOL REPORTS

USE THE TOOLS!

Cellebrite

MAGNET FORENSICS

Autopsy®
OPEN | EXTENSIBLE | FAST


# SO MANY TOOLS!

- **Although forensics software reports what was found and where, (aka a "Tool Report") it is YOUR responsibility to explain the significance of the evidence and define limitations.**

Example Tool Report Provided by Heather Mahalik

https://tinyurl.com/npbrb3fy

# THANK YOU


Jason Wilkins

+1 (404) 764-0480

jasonwilkins@outlook.com


https://twitter.com/TheJasonWilkins

https://www.linkedin.com/in/jasondywanewilkins/