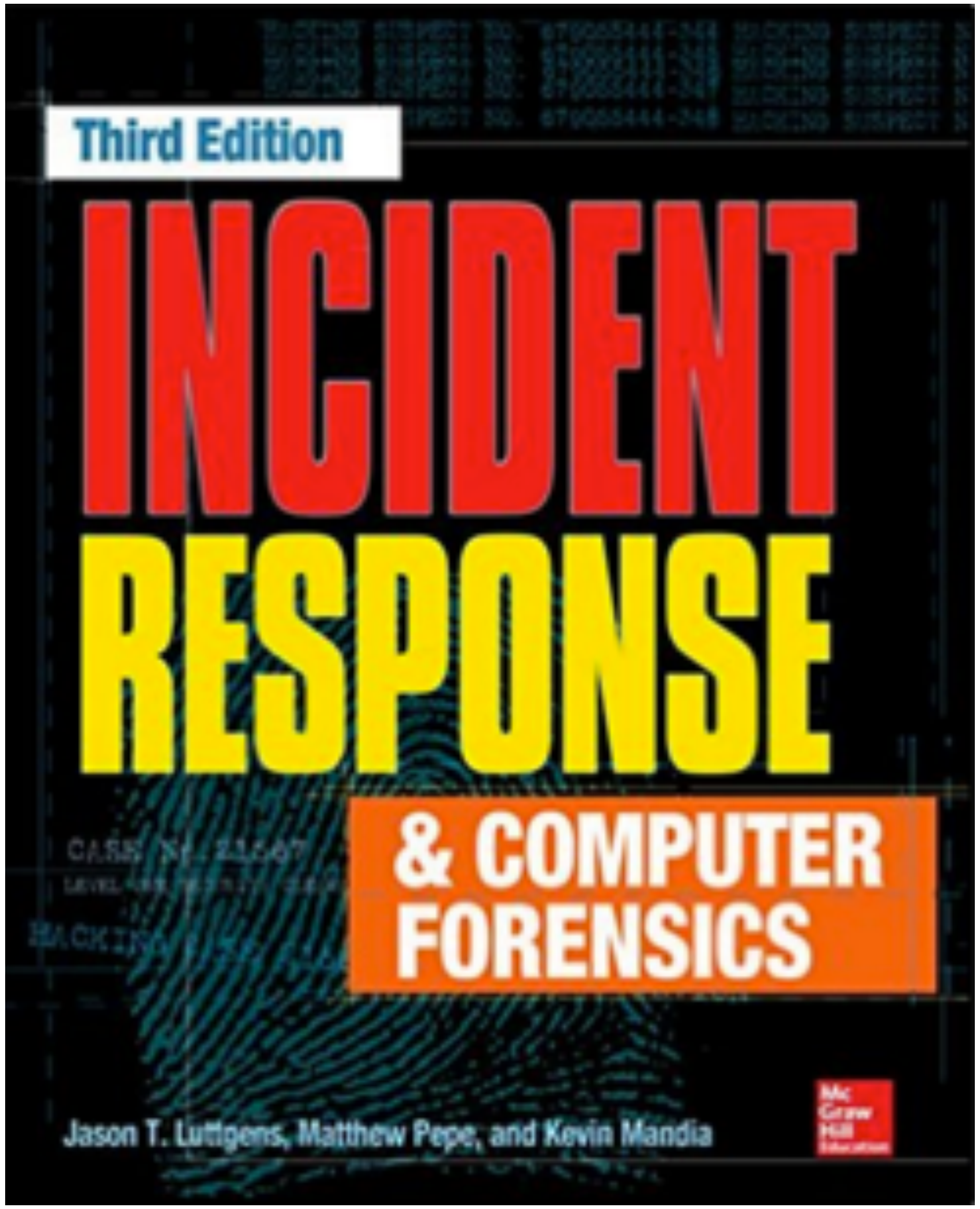
# CNIT 121: Computer Forensics



## Ch 16: Report Writing

# Why Write Reports?

- **Legal or policy requirements**
- **Recommended anyway whenever you analyze evidence or respond to an incident**
- **Writing a report also organizes your thoughts and improves accuracy**
- **Also preserves lessons learned**

# When Not to Write

- **Legal concerns about discovery**
- **The deliverable is a verbal report**
- **Make sure legal staff know your standard documentation procedures**
- **Label interim reports "DRAFT"**
  - **So later changes don't look like incompetence or deceit**

# Reporting Standards

- **Focused -- answer relevant questions**
  - **Main Q&A should be easily found; reader should not have to put together information from different parts of the report**
- **Understandable -- consider your audience**
  - **Executive summary is for CEO or CSO; not technical hands-on staff**

# Reporting Standards

- Stick to the facts
  - Avoid terms or phrases that can easily be misinterpreted or are subjective
  - Double-check facts
  - Do not mingle facts and opinion
- Timely
  - Begin documenting before you finish investigating

# Reporting Standards

- **Reproducible**
  - **Explain what you did thoroughly enough that another forensic examiner can reproduce your findings**

# Report Style and Formatting

- **Focused, accurate, and concise**
  - **Clearly answer the questions that were asked**
  - **In as few words a possible**
- **Write in active voice**
  - **"The attacker stole the data", not "The data was stolen by the attacker"**

# Report Style and Formatting

- **Past tense**
- **Use concise sentences**
  - **Fewer than 30 word**
- **Be specific**
  - **Avoid vague terms like "numerous", "several", or ",many"**
  - **State the exact number**

# Report Style and Formatting

- **State what you did, not what you couldn't do**
  - **You'll sound incompetent if you say you tried and failed to do something**
  - **Explain why, like "the operating system reused the deleted file's space, making the deleted file unrecoverable"**
- **Use transitions**
  - **Say what you are about to say, say it, and then summarize what you said**

# Report Style and Formatting

- **Use acronyms correctly**
  - **Spell them out the first time you use them**
  - **Check to make sure you have the names exactly correct**
- **Avoid jargon and ambiguous words**
  - **"Exfiltrate" is jargon; use "data theft" instead**
  - **"Compromised" is vague: say exactly what happened**

# Report Style and Formatting

- **Use names consistently**
  - **Choose "system" or "host" or "node" and stick with it**
- **Avoid informal language**
  - **"Examined", not "checked out"**
- **Clearly identify opinion**
  - **Support opinions with facts**
  - **Unsupported opinions don't belong in forensic reports**

# Expert Witness

- **Only expert witnesses can state opinions that will be treated as evidence in court**
- **You must meet qualifications established in court**
  - **An impressive resume is important**
- **Examiners who are not expert witnesses should state only facts, not opinions**
- **You may need to hire a consultant to act as an expert**

# Formatting Standards

- **Use consistent font and spacing**
- **Dates and times -- be consistent**
  - **Never use 05/05/05 because it's ambiguous**
  - **"January 28, 2012" is better**
  - **24-hour UTC time is best, not local time**

# Formatting Standards

- Standardize metadata reporting
  - Filename, timestamps, path, MD5, etc.
  - Should be in the same format every time
- Use captions and references
  - In Microsoft Word

# Formatting Standards

- **Use tables and figures appropriately**
  - **Often the most effective way to present information**
  - **Be consistent with font, borders, and shading**
  - **Include captions, and reference the captions in the narrative**
- **Use bulleted and numbered lists when appropriate**

# Report Content and Organization

- **Develop templates for each type of report**
    - **Overall incident**
    - **General analysis**
    - **Malware analysis**

# Incident Report

- **Title page and table of contents**
  - **Organization investigated, incident number or name, date, investigating organization**
  - **May be marked "Privileged and confidential"**
- **Background**
  - **How the incident was discovered, what response was, goals of investigation**
  - **Two paragraphs long**

# Incident Report

- **Findings**
  - **Goals of investigation in a very clear and brief manner**
  - **Part of the executive summary**
  - **No more than a page long**
- **Recommendations**
  - **Short-term and long-term**

# Incident Report

- **Mid-level sections**
  - **Findings from individual analysis reports are aggregated, interpreted, and summarized**
- **Individual analysis reports**
  - **Full reports, such as forensics, live response, and malware**
  - **Foundation for all findings in the incident report**

# Incident Report

- **Appendices**
  - **Long listings, log files, file listings**
  - **Tables or figures that take more than one page**

# Analysis Report

- **Title page and table of contents**
- **Background**
- **Findings**
- **Evidence examined**
- **Timelines**
- **Analysis details**
- **Appendices**

# Quality Assurance

- **QA review or "peer review"**
  - **Report is examined for compliance with style, formatting, content, and technical accuracy**
  - **Reviewer cannot be someone who wrote the report**
- **Check file metadata to make sure information from one report doesn't leak into another**
  - **Link Ch 14j**