(You’re Name Here)

Final Paper: Forensic Plan

* Executive Summary
  + Purpose
  + Scope
  + Authority
* Terminology
  + Collection
  + Examination
  + Analysis
  + Reporting
  + Legal Hold
  + Record Retention
  + Incident
  + Event
  + Breach
  + Media
  + Data
  + Information
  + Evidence
  + File
  + Baseline
* Data Collection
  + System/Technology
    - Identify potential sources of Data
      * Email, Windows Computers, and Cloud Storage
    - Copy media, including volatile digital evidence
    - Use sanitized, clean media only to copy onto
    - SANS Investigative Forensic Toolkit (SIFT)
  + Process/Procedure
    - Maintain logs of actions taken
    - Label all evidence with an evidence tag (if possible) and record it on the evidence log
    - When collecting for law enforcement, only collect media/files covered by the search warrant (consult legal counsel)
    - Follow all applicable laws (Computer Fraud & Abuse Act, Federal Wiretap Act, Electronic Communication and Privacy Act etc)
  + Interviews/Investigations
    - How to schedule meets with necessary contacts
    - Who to have in the meetings
  + Chain of custody
    - Define ownership of evidence
    - Log every person who has physical custody of evidence
    - Log actions performed on evidence and when the action was taken
    - Store the evidence in a secure location
    - Perform analysis only on copied media
    - Preserve original and copied media
* Examination
  + Examined copied media only
  + Identify the information of interest from acquired media
  + Filter extraneous information
* Analysis
  + Study the data to draw a conclusion
  + Correlate data
  + Compare data to known baselines
  + Review for potential leads, repeat Collection>Examination>Analysis process as necessary
* Reporting
  + Clearly communicate results
  + Create a detailed report with all relevant information along with a high level executive summary
  + Identify actionable information
  + Identify problems that need to be remediated
  + Provide report to CISO, CFO and responsible management
* Recommendation
  + Identify problems identified that need to be remediated, but not included in official report
  + Report these findings to the CISO as well as responsible/relevant management

Sources:

<https://www.giac.org/paper/gcfa/283/forensic-investigation-plan-cookbook/108356>

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>