9.1 Goals of Report

9.2 Layout of an Investigative Report

9.3 Guidelines for Writing a Report

9.4 Sample for Writing a Report

CHAPTER NINE

REPORT WRITING

9.1 Goals of Report

9.2 Layout of an Investigative Report

9.3 Guidelines for Writing a Report

9.4 Sample for Writing a Report

Goals of Report :

Your computer forensic reports should achieve the following goals :

1. Accurately describe the details of an incident.

2. Be understandable to decision makers.

3. Be able to withstand a barrage of legal scrutiny.

4. Be unambiguous and not open to misinterpretation.

5. Be easily referenced (using paragraph numbers for the report and Bates' numbers for attached documents).

6. Contain all information required to explain your conclusions.

7. Offer valid conclusions, opinions, or recommendations when needed.

8. Report should be ready in time.

9.1 Goals of Report

9.2 Layout of an Investigative Report

9.3 Guidelines for Writing a Report

9.4 Sample for Writing a Report

Layout of an Investigative Report :

1. Executive summary: The contextual information of the state of affairs that brought about the essential for an investigation is the "executive summary" unit.

2. Objectives: Sometimes, there could be a sudden requirement to perform hard drive forensic examination. The goals of your forensic examination can be related to virtually any subject, since any type of case/action can take place.

3. Computer evidence analyzed: The detailed information regarding the assignment of evidence tag numbers and media serial numbers, as well as descriptions of the evidence, is provided in this section.

4. Relevant findings: Summary of the findings of probative value is provided in this section. It answers the question, "What relevant items were found during the investigation?" The relevant findings should be listed in order of importance, or relevance to the case.

5. Supporting details: An in-depth look and analysis of the relative findings is provided in this section. It outlines *how* we found or arrived at the conclusions outlined in the "Relative Findings" section.

9.1 Goals of Report

9.2 Layout of an Investigative Report

9.3 Guidelines for Writing a Report

9.4 Sample for Writing a Report

Layout of an Investigative Report :

6. Investigative leads: In this section, we outline action items that could be performed to discover additional information pertinent to the investigation. If more time or additional resources were provided to the examiner or investigator, these are the outstanding tasks that could be completed.

7. Additional report subsections: In our computer forensic reports, there are several additional subsections that we often include. We have found the following subsections to be useful in specific cases, but not every case. It depends on the needs and wants of the end consumer.

9.1 Goals of Report

9.2 Layout of an Investigative Report

9.3 Guidelines for Writing a Report

9.4 Sample for Writing a Report

Guidelines for Writing a Report :

Following points are to be considered for writing a report:

1. Document investigative steps immediately and clearly:

Through our experience of writing a vast number of forensic reports, we have developed some report writing guidelines.

2. Know the goals of your analysis:

Before you begin your analysis for examination, know what the goals are. Every crime has elements of proof, for law enforcement examiners.

3. Organize your report:

Write “macro to micro.” Organize your forensic report to start at the high level and have the complexity of your report increase as your audience continues to read it.

4. Follow a template:

A standardized report template should be followed. This makes your report writing scalable, establishes a repeatable standard, and saves time.

5. Use consistent identifier:

There can be confusion created in a report by referring to an item in different ways, such as referring to the same computer as a system, PC, box, web server, victim system, and so on.

9.1 Goals of Report

9.2 Layout of an Investigative Report

9.3 Guidelines for Writing a Report

9.4 Sample for Writing a Report

Guidelines for Writing a Report :

6. Use attachments and appendices:
To maintain the flow of your report, use attachments or appendices. Right in the middle of your conclusions, you do not want to interrupt your forensic report with 15 pages of source code.

7. Have coworkers read your reports:
To read your forensic reports, employ other coworkers. This helps develop reports that are comprehensible to nontechnical personnel, who have an impact on your incident response strategy and resolution.

8. Use MD5 hashes:
Whether it is an entire hard drive or specific files, create and record the MD5 hashes of your proof. Performing MD5 hashes for all evidence provides support to the claim that you are diligent and attentive to the special requirements of forensic examination.

9. Include metadata:
Record and include the metadata for every file or file fragment cited in your report. This metadata includes the time/date stamps, full path of the file, the file size, and the file's MD5 sum.

9.1 Goals of Report

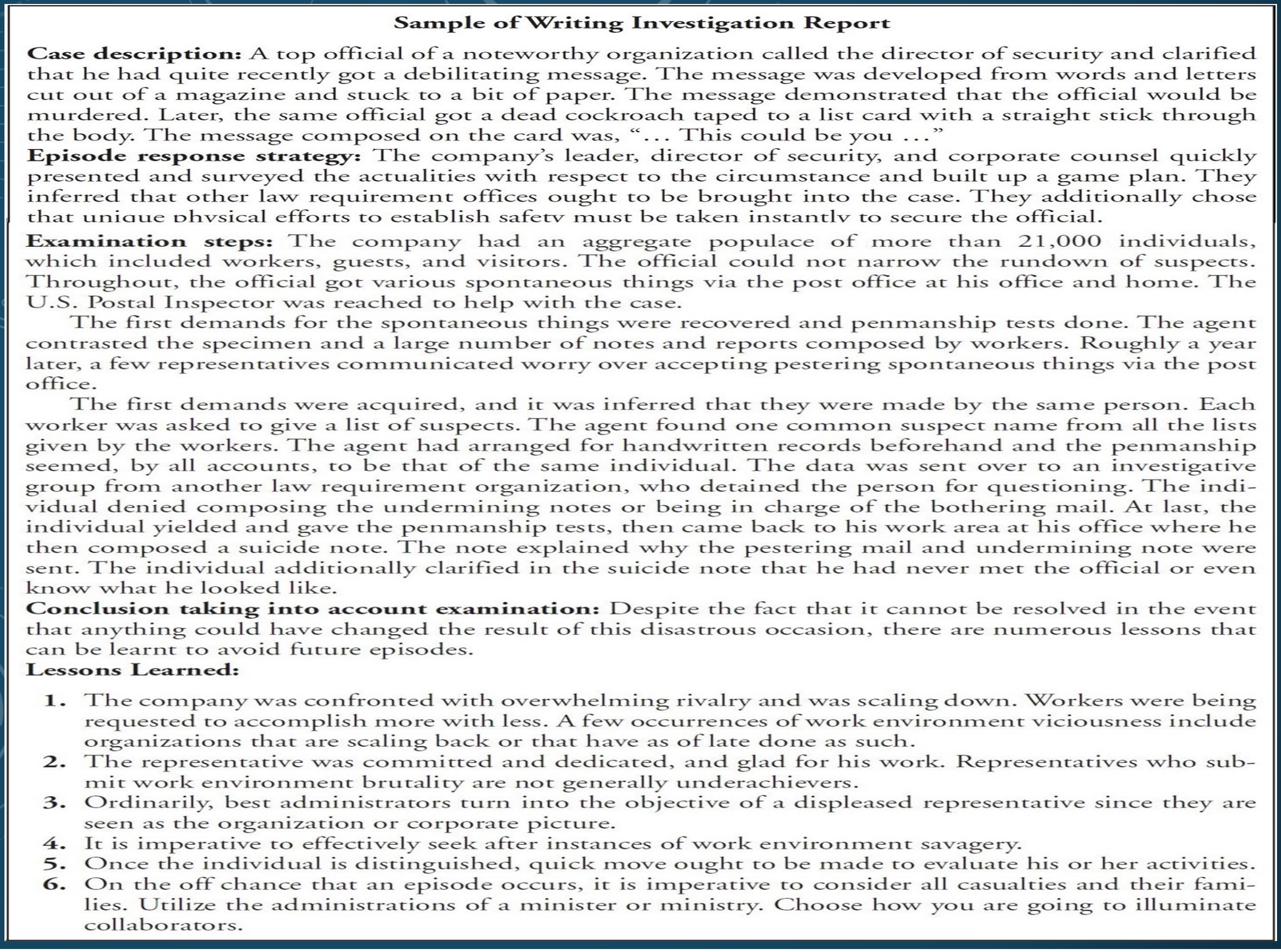
9.2 Layout of an Investigative Report

9.3 Guidelines for Writing a Report

9.4 Sample for Writing a Report

Guidelines for Writing a Report :

The following example is based on sample report writing which explains about investigation steps, experience and procedure used.



Sample of Writing Investigation Report

Case description: A top official of a noteworthy organization called the director of security and clarified that he had quite recently got a debilitating message. The message was developed from words and letters cut out of a magazine and stuck to a bit of paper. The message demonstrated that the official would be murdered. Later, the same official got a dead cockroach taped to a list card with a straight stick through the body. The message composed on the card was, "… This could be you …"

Episode response strategy: The company's leader, director of security, and corporate counsel quickly presented and surveyed the actualities with respect to the circumstance and built up a game plan. They inferred that other law requirement offices ought to be brought into the case. They additionally chose that unique physical efforts to establish safety must be taken instantly to secure the official.

Examination steps: The company had an aggregate populace of more than 21,000 individuals, which included workers, guests, and visitors. The official could not narrow the rundown of suspects. Throughout, the official got various spontaneous things via the post office at his office and home. The U.S. Postal Inspector was reached to help with the case.

The first demands for the spontaneous things were recovered and penmanship tests done. The agent contrasted the specimen and a large number of notes and reports composed by workers. Roughly a year later, a few representatives communicated worry over accepting pestering spontaneous things via the post office.

The first demands were acquired, and it was inferred that they were made by the same person. Each worker was asked to give a list of suspects. The agent found one common suspect name from all the lists given by the workers. The agent had arranged for handwritten records beforehand and the penmanship seemed, by all accounts, to be that of the same individual. The data was sent over to an investigative group from another law requirement organization, who detained the person for questioning. The individual denied composing the undermining notes or being in charge of the bothering mail. At last, the individual yielded and gave the penmanship tests, then came back to his work area at his office where he then composed a suicide note. The note explained why the pestering mail and undermining note were sent. The individual additionally clarified in the suicide note that he had never met the official or even know what he looked like.

Conclusion taking into account examination: Despite the fact that it cannot be resolved in the event that anything could have changed the result of this disastrous occasion, there are numerous lessons that can be learnt to avoid future episodes.

Lessons Learned:

1. The company was confronted with overwhelming rivalry and was scaling down. Workers were being requested to accomplish more with less. A few occurrences of work environment viciousness include organizations that are scaling back or that have as of late done as such.
2. The representative was committed and dedicated, and glad for his work. Representatives who submit work environment brutality are not generally underachievers.
3. Ordinarily, best administrators turn into the objective of a displeased representative since they are seen as the organization or corporate picture.
4. It is imperative to effectively seek after instances of work environment savagery.
5. Once the individual is distinguished, quick move ought to be made to evaluate his or her activities.
6. On the off chance that an episode occurs, it is imperative to consider all casualties and their families. Utilize the administrations of a minister or ministry. Choose how you are going to illuminate collaborators.