Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Becoming a Forensic Investigator

One of the forensic analyst's primary functions is the dissemination of the forensic process to the intended audience. To do their jobs successfully, they must write forensic reports that are both technically accurate and easy to read. A great investigation can be rendered largely ineffective if the resulting report is poor. In fact, a report that is disorganized and poorly written may actually hinder their case. Many find forensic technical writing a difficult job, particularly in making reports readable for the inten...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Forensics for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Writing a Computer Forensic Technical Report

Introduction

One of the forensic analyst's primary functions is the dissemination of the forensic process to the intended audience. To do their jobs successfully, they must write forensic reports that are both technically accurate and easy to read. A great investigation can be rendered largely ineffective if the resulting report is poor. In fact, a report that is disorganized and poorly written may actually hinder their case. Many find forensic technical writing a difficult job, particularly in making reports readable for the intended audience. This paper will offer a methodology to ensure a repeatable standard and hopefully make the job of forensic technical writing easier.

Report Preparation

Forensic information has limited value if it is not collected and reported in a usable form and presented to those who need to apply the information. Therefore, a big goal of the process is a standard way to document *why* the computer system was reviewed, *how* the computer data was reviewed, and *what* conclusions were arrived at. Computer forensic technical report writing requires a documented process to ensure a repeatable standard is met by the forensic analyst or the organization he is representing. The computer forensic report should achieve the following goals (taken from Incident Response, 2nd Edition – see References):

- Accurately describe the details of an incident
- Be understandable to decision-makers
- Be able to withstand a barrage of legal scrutiny
- Be unambiguous and not open to misinterpretation
- Be easily referenced
- Contain all information required to explain your conclusions
- Offer valid conclusions, opinions, or recommendations when needed
- Be created in a timely manner

We will propose a general methodology based on the five major stages of technical report preparation. Within these general stages, we will add the specific details or guidelines as they relate to the field of computer forensics.

The five major stages of technical report preparation are (From NASA's Guide to Research and Technical Writing – see References):

1. Gathering the data
2. Analyzing the results

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

3. Outlining and Organizing the report
4. Writing the rough draft
5. Revising the rough draft

Gathering the data

Technical report preparation begins with proper planning. An orderly investigation is a prerequisite for an orderly technical report. A common thread in successful technical report writing is the ability to foresee the general content of the report before the forensic process begins. On way to do this is to keep the future report in mind during the course of the forensic process.

Maintain orderly records as the data are gathered. Document investigative steps immediately. Maintaining orderly records and documentation requires discipline and organization, but it is essential to successful forensic technical writing. Write everything down in an orderly fashion that is understandable to you and others (your intended audience). Do not use shortcuts or shorthand, since such vague notations can result in a failure to comprehend the notes by yourself or others. Writing clearly and concisely at the moment of evidence discovery promotes accuracy and saves time later. Discipline yourself to follow this philosophy: Document as you go!

Don't forget – during this phase consider how the forensic data should be presented in the technical report and record the results in this manner. Thus, any need for additional forensic data will be revealed before the forensic program is completed.

Analyzing the results

This phase is probably the most difficult because it requires considerable thought and effort to decide what you want to tell your audience. The beginning of this stage overlaps the gathering data stage, since you want to know what goals of your examination are before you begin your analysis (data analysis should begin as the data are collected). This will foster a focused report, what is what your audience wants.

During the analysis and data review, conclusions should be drawn. This is the most important step in the technical report preparation because the conclusions are the reason for the report and the basis for the technical report preparation. However, a caveat must be mentioned at this point: be very careful listing the conclusions as the data are being gathered. Limited information gathered during the "Gathering the Data" phase may lead the forensic analyst to incorrect assumptions. As data are gathered, the conclusions may (and probably will) change. The risk of incorrect conclusions is that it creates the potential for

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

“reasonable” doubt in the courtroom. Therefore, it is best to document the conclusions in this phase (Analyzing the Results), since most of the data has already been gathered. Once the conclusions are drawn, it is best to list them in descending order of importance.

Let us digress a moment and discuss an important concept of forensic reporting. As discussed above, conclusions drawn is the most important step in the report. A report that offers a conclusion (an opinion) is referred to as an *expert report*. The expert opinion is governed by the Federal Rules of Evidence (FRE) under rule FRE 705. A report that offers no opinion does not meet the legal definition of an expert report. For example, law enforcement examiners are generally trained to create forensic reports that offer no opinions; they merely state the facts. Thus, if a case goes to trial, a forensic analyst can either be called a technical witness or an expert witness. As a technical witness, the forensic analyst is only providing the facts as found in the forensic investigation. The forensic analyst presents the evidence and explains what it is and how it was obtained. The forensic analyst does not offer conclusions, only the facts.

However, as an expert witness, the forensic analyst has opinions and conclusions about what was observed. The opinions and conclusions are based on experience and the facts found during the forensic investigation and examination of the data obtained. Corporate and private sector forensic analyst are usually requested to offer an opinion in court. In most cases, the forensic analyst’s professional opinion about a case is the most useful item to the client.

Selection of the data to be used in the forensic report is another important part of this step. Developing a consistent way of referencing each item throughout the report is critical. A good suggestion is to create a unique identifier or reference tag for each person, place, and thing referred to in the forensic report. The label will identify the item for the remainder of the forensic report. For example, using descriptive labels such as MARK LAPTOP or IIS WEB SERVER, instead of tag1 (for MARK LAPTOP) or tag2 (IIS WEB SERVER), helps to eliminate confusion.

Forensic analysis usually results in illustrations for the forensic report. Figures and tables organization should be carefully considered since illustrations are one of the best ways of emphasizing and supporting conclusions. After the illustrations are prepared, it’s important to write the significant points about each. It is helpful to consider the following questions: what is the figure supposed to show? How were the data obtained? Are there any qualifications to the figure? These questions are important and useful when the forensic report writing begins.

Using attachments and appendices are important to maintaining the flow of the forensic report. It is important not to interrupt the forensic report with pages and pages of source code right in the middle of a conclusion. A good rule of thumb is that any information, files, and code that are over a page should be included as

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

appendices or attachments. Every file that contributes to the conclusion should be included as an appendix to the forensic report. This allows the report to stand alone so it can be referenced for any questions that may arise in a judicial or administrative process.

Finally, create and record the MD5 hashes of the evidence as well as record and include the metadata for every file cited in the forensic report. By recording the MD5 values, the audience can feel confident that the forensic analyst is handling the data in the appropriate manner. The same applies to the metadata. Those reading the report appreciate the details included, and the forensic analyst will likely need the details to remove any ambiguity about the files during testimony.

Outlining and Organizing the report

Outlining is a necessary preliminary step to forensic technical writing. Without the outline, most inexperienced forensic analyst write reports that are confusing and difficult to follow. This stage is a natural progression from the forensic analysis performed in the previous stage. In the analysis stage, concentration was on *what* results should be presented in the forensic report. In the outlining stage, concentration is directed on *how* the results should be presented.

Organizing the report is also critically important. A good suggestion for the forensic report is to start at the high level, and have the complexity of the forensic report increase. This way, the high-level executives need to read only the first page to get a summary of the conclusions. They usually are not interested in the low-level details that support the conclusion.

It is recommended that the forensic report writer follow a standardized report template. This makes the forensic technical report writing scalable, establishes a repeatable standard, and saves time. A template format will be presented and a brief discussion of each section will follow (from Incident Response, 2nd Edition – see References). This is only a template, and can be modified as desired by the forensic report writer.

Each forensic report produced by the forensic analyst could include any of the following sections:

- Executive Summary
- Objectives
- Computer Evidence Analyzed
- Relevant Findings
- Supporting Details
- Investigative Leads
- Additional Subsections and Recommendations

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Executive Summary

This section is the background information that resulted in the investigation. This is the area usually read by senior management. It is recommended that this section do the following:

- Include who authorized the forensic investigation
- Describe why a forensic examination of computer media was necessary
- List what significant findings were found
- Include a signature block for the examiner(s) who performed the investigation

All people involved in the investigation are included, along with important dates of pertinent communications.

Objectives

This section outlines all tasks accomplished in the investigation.

Computer Evidence Analyzed

The evidence is introduced in this section. All evidence collected and interpreted are included. A good suggestion for communicating this information is using a table to illustrate the evidence collected. It is also a good suggestion to not create a formal checklist of the procedures or include a checklist into the final forensic report. Checklists are easily challenged in court by the opposing counsel.

Relevant Findings

A summary of the findings of value are included in this section. This is the conclusions and opinions of the forensic analyst. It answers the question, "What relevant items were found during the investigation?" They should be listed in order of importance, or relevance to the case. Organization, in a logical way, is a key component.

Supporting Details

This section supports the "Relevant Findings" section by providing an in-depth look and analysis of the relevant findings. It outlines *how* the forensic analyst arrived at their conclusions in the "Relevant Findings" section. This is a good

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

section for the illustrations, such as tables and figures produced by the investigation.

Investigative Leads

This is the outstanding tasks section. Investigations have to end somewhere usually because the forensic analyst is under time-constraints. However, there are tasks the forensic analyst could have completed had the investigator had more time. If more tasks could have been completed, more compelling evidence could have been collected. This must be documented, and this section is often important for law enforcement that may continue with the investigation.

Additional Subsections and Recommendations

This depends on the needs of the intended audience. For example, the audience may want to know the exact attack that was performed, which may require analyzing a binary. So, a section “Binary Analysis” may be appropriate to the investigation. Also common is a breakdown subsection of Internet activity and Web browsing history. The recommendation section is to help the intended audience or client to be better prepared and trained for the next incident. This usually includes countermeasures that can be immediately implemented to strengthen the client’s security posture.

Writing the Rough Draft

With a logically organized outline such as the template for computer forensic reports, writing the rough draft will be much easier. However, due to the nature of the technical materials included in forensic reports, several versions are performed; do not expect to write the final version in the first attempt. Each version will be an improvement over the other. This final version is considered a “rough” draft because it still must go through a series of technical reviews.

A necessary suggestion is to have your co-workers read the forensic report. Remember, the forensic report must be readable by technical and non-technical personnel, and may also be used in court. Have non-technical personnel read the forensic report to determine if it is comprehensible to them. The non-technical personnel will include legal counsel, Human Resources personnel and business managers. It is important to take into consideration the technical capability and knowledge of the intended audience. Writing style becomes important. Therefore, a glossary of terms may be added to help the non-technical personnel.

Revising the Rough Draft

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Finally, we've made it to the last stage! However, this is an important step, and the one most often overlooked by inexperienced technical forensic writers. In this step, the "appearance" (readability) is improved without doing major modifications to the structure of the report.

Successful forensic technical writers may use a variety of methods to review and revise the report. One of the best methods involves three separate reviews of the forensic report (From NASA's Guide – See References):

1. The first review is of the material in the forensic report. Ask these questions: Are the conclusions valid? Is sufficient information given to support the conclusions? Is enough information given to explain the results? Have all irrelevant ideas been deleted? Are the illustrations pertinent and necessary?

2. The second review is of the mechanics and organization of the report. Ask these questions: Are the subject and purpose clearly stated? Does the report flow smoothly from beginning to end (or topic to topic)? Are the relations between topics clear? Is each illustration clear and properly labeled? Are all required parts of the report included?

3. The third review is of spelling and grammar, particularly punctuation and sentence structure. Ask these questions: Is each sentence written effectively? Are the sentence varied in length and complexity to avoid monotony? Are the words specific and not vague? Have unnecessary words been deleted from the report?

Make sure you can answers yes to all of these questions. If not, the draft is not finished.

Conclusion

The forensic technical report is written to communicate the results of the forensic analyst's forensic examination. A formal report presents evidence as testimony in court, at an administrative hearing, or as an affidavit. Besides presenting facts, forensic reports can communicate expert opinion. Writing the forensic technical report can be a daunting task. The purpose of this paper was to lay out a methodology for producing forensic analysis in a written format. Remember, a great investigation can be rendered largely ineffective if the resulting documentation/report is poor. In fact, a forensic report that is disorganized and

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

poorly written may actually hinder the advancement of the forensic analyst's case.

References

Mandia, K., Prosise, C., and Pepe, M. Incident Response, 2nd Edition. McGraw-Hill/Osborne, 2003

Nelson, B., Phillips, A., Enfinger, F., and Steuart, C. Guide to Computer Forensics and Investigations. Thomson Course Technology, 2004

NASA's Guide to Research and Technical Writing:
URL: http://grcpublishing.grc.nasa.gov/Editing/vidoli.CFM

Federal Rules of Evidence (FRE) 705:
URL: http://www.law.cornell.edu/rules/fre/705.html

Submitted by
Mark Maher, CPA, CISSP, GCFA, GCIA, GCIH
August 9, 2004

© SANS Institute 2004, Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced