A STRUCTURED APPROACH TO INCIDENT POST MORTEMS
By Peter Stephenson, CPE, CISSP, CISM, CIFI, FICAF

Abstract: Investigators of digital incidents generally think in terms of using digital forensics and the digital investigative process for the purpose of identifying the perpetrator of the incident. However, today many organizations are more concerned with finding out what weaknesses allowed the attack to be successful and identifying effective countermeasures for the future.

This is a specialized branch of digital forensic science that does not necessarily deal with the legal aspects of a digital investigation. In some regards post mortem analysis must be more rigorous than a typical investigation because the future security of the organization may turn on the outcome. As well, in some cases insurance settlements may depend upon an accurate appraisal of the root cause of the incident and its damage.

In this paper we discuss the digital investigative process in light of post mortem analysis, offer a structured approach based upon a consensus investigative framework and suggest cautions that the investigator should keep in mind during the post mortem process.

A Structured Process for Digital Investigation

We begin with a structured framework for conducting a digital investigation. This framework, developed by the Digital Forensics Research Workshop, gives us a starting point for virtually all digital investigations. It is especially useful in an incident post mortem because it adds the structure that gives the findings credibility.

Generally speaking, if we consider the concept of forensic science in general, we find that it is a body of practice focused at determining why something failed. It could be a dead body, a collapsed building or a penetrated computer system. While the general, simple definition of forensic science is the application of natural science to matters of law (and the specific simple definition of digital forensic science is the application of computer science and mathematics to matters of law), there are other, equally important, aspects of forensic science. Those aspects relate to underlying root causes of events and the techniques used to understand them.

The Digital Forensics Research Workshop (DFRWS) has given us a good starting point with a consensus framework for a digital investigation. That framework is shown in Figure 1.

---

Each of the classes (identification, preservation, collection, examination, analysis and presentation) has several elements related to it. Those elements in **bold** type are required for a complete, structured investigation. The rest may be addressed as applicable.

It may be noted that at least two of the required elements (chain of custody and legal authority) appear to focus more upon the applicability to matters of law than to a post mortem. The reason for this is that, at the start of a post mortem, it is indeterminate as to whether the investigation will result, ultimately, in legal action.

While most of the required elements are clear as to meaning, there are two that are pervasive and need clear definition: preservation and traceability. Traceability is the continuity of a chain of evidence throughout an investigation that leads to the credibility and correctness of the conclusions. According to the DFRWS “Traceability (cross referencing and linking) is key as evidence unfolds.”

Preservation deals with those elements that relate to the management of items of evidence. The DFRWS describes this class as “...a guarded principle across ‘forensic’ categories.” [DFRW01]. The requirement for proper evidence handing is basic to the digital investigative process as it relates to legal actions.

There is a common ground between theoretical and forensic science. That common ground is a collection of reliable methods. Those methods are characterized by:

---

**Table: DFRWS Framework for Digital Investigation**

<table>
<thead>
<tr>
<th>IDENTIFICATION</th>
<th>PRESERVATION</th>
<th>COLLECTION</th>
<th>EXAMINATION</th>
<th>ANALYSIS</th>
<th>PRESENTATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event/Crime Detection</td>
<td>Case Management</td>
<td>Preservation</td>
<td>Preservation</td>
<td>Preservation</td>
<td>Documentation</td>
</tr>
<tr>
<td>Resolve Signature Imaging Technologies</td>
<td>Approved Methods</td>
<td>Traceability</td>
<td>Traceability</td>
<td>Expert Testimony</td>
<td></td>
</tr>
<tr>
<td>Profile Detection Chain of Custody</td>
<td>Approved Software Validation Techniques</td>
<td>Statistical</td>
<td>Clarification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complaints Legal Authority</td>
<td>Pattern Matching Data Mining</td>
<td>Recommended Countermeasure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Monitoring Lossless Compression Hidden Data Discovery Timeline Statistical Interpretation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Analysis Sampling Hidden Data Extraction Link</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Reduction</td>
<td>Spatial</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Techniques</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Integrity
Competence
Defensible technique
Relevant experience

A scientific approach to an incident post mortem demands that we develop theories and then attempt to prove or disprove them. During an incident post mortem we may develop many theories of the events that produced the end result of the incident. We then must apply facts as we discover them in an attempt to discredit or support those theories. If we cannot support them, or if we find facts that counter our hypothesis, we must discard the theory and move on to a new one. The End-to-End Digital Investigation (EEDI) process lends itself well to this type of investigation.

PERFORMING AN INCIDENT POST MORTEM

It is very important to note that an incident post mortem is not incident response. Post mortems often are called for in large measure because a traditional incident response failed. Successful attacks by certain classes of worms or viruses are examples of incidents that may happen too fast for adequate response if the target network is vulnerable. When such an incident occurs, organizations must analyze the underlying root causes of the success and implement countermeasures to prevent future successes. In such cases, referring to the DFRWS Framework, we should include such things as mission impact in the presentation class.

There are two important cautions that investigators should keep in mind when performing an incident post mortem. First, the obvious answer is not always the complete answer. Complex problems often have complex solutions. Second, and conversely, don’t over-complicate the process. Typically the over-all solution is a collection of simpler ones. That is not inconsistent with the first caution, however. Simply because a complex problem has a complex solution does not mean that the solution necessarily is complicated. Most attacks succeed because of underlying flaws in the victim’s security architecture. Often those flaws can be remediated with a number of fairly simple countermeasures.

The general process for conducting an incident post mortem is:

- “Get the lay of the land. Examine network maps, interview key witnesses, learn what appeared to have happened from those who were there and watched it happen.
- Collect evidence. Get every log you can find whether you think it will be useful or not. At this stage you are casting a very wide net. You don’t yet know what happened so you don’t yet know what to look for. If the incident suggests that

imaging some computers is necessary, get them imaged as fast as you can before precious evidence is lost. Contact Internet service providers that may have been in the path and get logs preserved pending subpoenas. In short, as you would in an investigation that you expect to lead to the identification of a suspect, freeze time.

- Collect a set of incident hypotheses. At this point quantity is more important than quality. Don’t get silly – the hypothesis that space aliens caused the incident may be a bit far out to take up valuable time proving or disproving.

- Conduct detailed interviews. Gather as much detail about what happened as you can. A good tool for conducting interviews is to prepare, with the help of a knowledgeable person, a timeline of observed events. This timeline can include events as seen by various groups such as network operations, security, users, etc. It should also include any meetings that were held by response teams or other involved persons and the purpose and conclusions of those meetings. Include when various involved individuals were notified of the incident and all other information that helps you create a picture of events as they occurred. This will be very difficult because during an incident a certain amount of chaos rules. Do the best you can. Take the timeline and use it as the basis for interviews of all involved parties. Note carefully the discrepancies and, through repeated interviews attempt to resolve them. Remember, in a serious incident cover-ups are common.

- Process your physical (digital) evidence. Use the correlation techniques discussed in earlier columns plus some analysis techniques we will discuss in coming months to reduce your data (there will be huge amounts of it) to information and, ultimately, to knowledge.

- Refine your hypotheses, rejecting those not supported by facts as they emerge. You also will find that as facts emerge they suggest new theories. Don’t be shy about considering them.

- When you get down to a couple of likely theories (they may be combinations of several earlier ideas) test them rigorously against the facts. Look for counterexamples and alternative explanations that might discredit your explanation. Make sure you haven’t missed anything or any interview that could shed additional light on the problem. Use whatever data analysis tools you can to validate the impact of your data upon your final theories.”

**USING THE FRAMEWORK**

Applying the DFRWS Framework gives us the key elements of process that we need to follow. By following the Framework carefully we ensure that our conclusions have credibility and, if we are unable to follow the Framework due to lack of data, political stonewalling or other mitigating circumstance, gaps will show clearly what is missing and why the post mortem cannot draw reliable conclusions. In short, following the Framework gives our investigation credibility and explains clearly when conclusions cannot be drawn reliably.
**Identification Class**

The identification class describes how we identify the incident and determine what, in general, happened. The Event/Crime Detection element is required for this class and, in a post mortem, it is very simple. The victim has succumbed to an attack of some sort, the attack is over, the clean-up done and it is time to figure out why it was successful. However, other elements of this class can help the investigator focus upon the real nature of the event. For example, the existence of logs from an intrusion detection system may offer us the ability to resolve a signature or detect anomalies. Other logs may provide us with data for an audit analysis. Interviews with operators may surface complaints of unavailable data or systems at the time of the attack or, under the best of circumstances, just prior to the failure of such systems.

Unlike other types of investigations an incident post mortem deals with an incident that, in all probability, actually occurred. However, even though the average (about 50%) of incidents that are not security related in traditional investigations does not apply here, there may be some smaller number of post mortems that reveal network anomalies instead of malicious acts. Part of the post mortem is the assurance that the incident is what it appeared to be. Thus, the conclusion that no malicious act was the root cause of the event may be credible and the investigator should always consider it.

**Preservation Class**

This class sets guidelines for us to follow relating to how we manage our evidence. On my post mortem (PM) team I have a single person responsible for this class and it pervasive inclusion in most other classes of the Framework. The creation of a chain of custody is usually reserved for legal applications of the forensic process. However, at this stage of the PM we have no idea where our evidence will take us. We could, indeed, uncover the source of the attack and the victim may wish to take legal action. We may find negligence on the part of the victim’s employees that could result in disciplinary action. In that case management will want to be secure in the knowledge that evidence was handled properly and was not subject to contamination.

**Collection Class**

It is critical that investigators use only tools that have been validated for the use to which the investigators are going to put them. While there are many tools that appear to perform similar tasks, it is best to stick to those that are intended for investigative purposes. These tools are known to not alter data and to present that information which the investigator intends them to produce.

Most important, however, is the notion that the investigator is trained and experienced in conducting this type of investigation. It is not uncommon to see IT personnel conduct post mortems. These individuals, though, are not trained in forensic techniques or in the handing of evidence. While they have valuable technical input into the investigation, they should be used only as resources unless they have appropriate forensic and
investigative training. This supports James and Nordby’s principles of defensible
technique and relevant experience.

**Examination Class**

Evidence is identified and preserved procedurally in the preservation class. It is collected
in the collection class. An example of this process is the identification of a computer as
the victim of an attack. In the preservation class the investigator would impound the
computer or its disks and place it/them into a chain of custody. In the collection class the
investigator would take a bit-stream image of the disks and place those images in chain of
custody. The investigator would also take a work copy of the images. At this point the
investigator only has obtained a gross data set (all of the data on the disks) that he or she
believes to contain evidence. He or she has isolated that gross data set into protected
custody and has prepared for examination, the task of this (examination) class.

In this class the investigator begins to examine the gross data set for clues as to the root
causes of the attack’s success. In this class preservation of evidence integrity continues
and traceability of the evidence chain begins. The investigator must pay close attention
to the other elements of this class to ensure that the evidence that is extracted maintains
both integrity and reliability.

**Analysis Class**

This is where the real work begins and hypotheses begin to form. Adherence to the
elements of this class help ensure that the analysis is credible and that conclusions are
supported by facts. Preservation and traceability persist in this class. Techniques such as
link analysis, protocol analysis, data mining and statistical analysis apply in this class.

**Presentation Class**

In this class the investigator documents findings, evidence, procedure and conclusions.
Since this is an incident post mortem a mission impact statement is appropriate. This
may include an estimation of loss as a result of the incident. Also, the presentation class
should always include recommended countermeasures. The underlying reason for
conducting an incident post mortem is the identification of the root weaknesses and
appropriate countermeasures to repair them.

**THE POST MORTEM TEAM**

The team conducting the post mortem is not small. Except in rare circumstances where
multiple skills exist in a single person, the team needs to cover several skill sets:

- **Quality manager** – responsible for managing all evidence, investigator notes,
  chain of custody and interview scheduling
- **System specialist** – responsible for all network and platform aspects of the
  investigation. This person (or persons) should cover all of the network
protocols in the affected network including applicable internetworking devices, firewalls, etc.

- **Code specialist** – this person works with the system specialist(s) to reverse engineer malicious code and understand how it worked, what it did, if possible who wrote it, etc.
- **Business process specialist** – usually skilled in such mechanisms as BS7799, COBIT and other auditing standards, as well as applicable regulatory rules and standards, this person assesses the business process failures that contributed to the success of the incident. He or she may also be involved in assessing impact on the victim.
- **Team leader** – responsible for the investigative process, managing the team, correlating team findings and aspects of data reduction and fusion. This person also is responsible for the final report and presentation to management.

**CONCLUSION**

There are some key issues that accompany the EEDI/Post Mortem process. First, it is critically important that evidence be gathered in support of the basic EEDI evidence rules:

**Primary and Secondary Evidence**

“Primary evidence is evidence that is corroborated by other pieces of primary evidence and, in turn, corroborates additional primary evidence in a chain of evidence. Primary evidence makes up the evidence chain in a digital investigation. Primary evidence may, in turn, be corroborated additionally by secondary evidence. In special circumstances, such as the first piece of evidence in a chain, sufficiently clear and obvious evidence (such as evidence that a computer has been the victim of an attack) may be considered primary evidence if it is corroborated by a significant body of secondary evidence and, in turn, corroborates other primary evidence.

Secondary evidence is evidence that is not, itself, corroborated but may serve to corroborate primary evidence. Secondary evidence rarely stands alone credibly since it does not have anything to support it directly. Secondary evidence may be circumstantial, for example. The presence of secondary evidence in sufficient quantity and of sufficient quality may, however, serve to tell a compelling story of how a series of digital events occurred.”

This raises the issue of corroboration. In any investigation, especially an incident post mortem, corroboration is critically important. The EEDI process allows investigators to mix traditional evidence and digital evidence to obtain a complete chain of evidence with appropriate corroboration.

---

Other Issues

A second issue is the assumption of an event. As we stated earlier, about 50% of all events in progress are not security-related even though they may appear so at first glance. That number is smaller for fully realized incidents such as those subject to a post mortem some extended period after the fact. However, there is some number of such incidents that have no malicious origins. The investigator should keep that in mind as he or she conducts the PM.

Third is the issue availability of evidence. In a typical investigation where the attack is in progress or recently completed, the first task is to preserve evidence. That can pose challenges due to small storage space for logs, log retention policies, logging structure of important devices including networking devices as well as the more obvious platforms, intrusion detection systems and firewalls. In a post mortem there is a better than even chance that much evidence has disappeared over time. The first effort of the PM team must be to retrieve as much evidence as possible. Since the team has no idea, at the outset, where the investigation will take them, they must cast a very wide net and collect all evidence possible, whether its applicability to the investigation is obvious or not. It is not uncommon for lay individuals to question this policy and it should be explained at the outset to set proper expectations and avoid political repercussions.

The fourth issue is that of internal politics. It is not uncommon for post mortems of especially catastrophic incidents to result in disciplinary action. The anticipation of such actions can cause a difficult political atmosphere for the investigating team. Before undertaking an incident post mortem it is a good idea to get full support at the highest levels of the organization. That means at the president or board of director level. Anything lower can result in political positioning that can invalidate completely the efforts of the investigating team.

Incident post mortems can be a very effective way to understand and remediate security weaknesses that result in a successful attack against the organization. They are difficult and expensive to conduct, but if conducted using a rigorous structured approach they can provide clear and credible understanding of the event and its impact on the organization as well as a roadmap for preventing such occurrences in the future.

Because they are difficult and expensive to conduct, formal incident post mortems should be reserved for only those events, usually complex, that pose serious threat to the IT infrastructure and coincident data, those events that indicate ongoing threats against the organization and those events that may result in liability on the part of the organization.