Topic 1: Investigation Approaches

Use the Library to research how computer forensics investigators prepare for the execution of an actual investigation. What do you think are the most important investigative approaches in these cybercrime cases? What might be the result of poor investigator planning and preparation before the start of digital evidence collection, and processing? Observe the comments and replies of others in the Discussion and interact to build the content.

In my research, I was able to find a good book about digital forensics from the Kaplan Library, Computer Forensics: A Pocket Guide, by Nathan Clarke. According to Clarke (2010), there are seven stages that forensic investigators must use when collecting evidence---they are: (1) Response; (2) identification; (3) preservation; (4) collection; (5) examination (6) analysis; and (7) presentation (Clarke, 2010, p. 20). Of course, even before an investigator uses this process, there are things that a company and the forensic team can do to be proactive. Clarke (2010) suggests there are five factors that go into creating an effective forensic strategy; these factors include people, a lab, incident response, policies, and infrastructure (Clarke, 2010, p. 24).

Considering the people factor, this means that it is a company’s responsibility to hire capable forensic team members, and then to make sure those members receive continued training in the areas of forensic science. Also, there needs to be a laboratory where the forensic team can process evidence; this includes having the proper facilities to copy, secure, and analyze data. Additionally, it will be the company’s responsibility to create incident response procedures. These procedures will outline the steps each forensic team member should use in an investigation. Furthermore, there are two factors which will affect how the entire company interacts and deals with forensics; they are company policy and IT infrastructure. These factors will create an environment where all employees understand company security policies, while at the same time allowing the IT department (as well as other teams) to work with the forensic team, if and when an incidence does happen.

Personally, I think the most important approach to any cybercrime case is being prepared. Consequently, being prepared means companies need to hire the appropriate personnel, train them, create incident response procedures, create policies for all employees to follow, and have work areas that facilitate an investigation, not hinder it.

Poor processes and procedures would include: having no official procedures for incident response, companies not allocating funds to handle cybercrime, forensic investigators who do not receive consistent training, and using forensic practices that are not accepted by the forensic community and law enforcement communities.

A good practice that should be used by all forensic investigators is evidence collection. This would
Include photographing the scene, processing any live data from digital devices, documenting each step taken, learning how to move electronic devices (such as laptops) to a secure location, and finally, know when to contact law enforcement (Easttom, 2014).

Once a company has taken a proactive approach to digital forensics, processing a crime scene will be much more effective. When a cybercrime does happen, the forensic team can respond using the seven factors in the collection of evidence.

If a company does not take a proactive approach to digital forensics, the results could include losing the evidence due to poor processes, making evidence inadmissible in court, not having the knowledge or tools to collect evidence, and possibly causing an even worse security breach.

References


**Topic 2: Reviewing Candidates**

As the Lead Computer Forensics Investigator, you must hire an additional team member before the investigation of two crime scene laptops begins. Discuss some of the key questions you would ask this applicant regarding the needs for forensic imaging and evidence preservation. What should be the response given to those two questions from the applicant? Ask others on the Discussion what their opinions are on these two subject areas.

Edward Jackson

**It's all about the questions**

I would ask these questions to gauge the applicant’s knowledge about digital forensics:

(1) What is live data and how would you acquire it from a crime scene?

(2) What is meant by preservation of data, and how do you do it?
Regarding the first question, I would expect the applicant to explain to me what live data is.

**Expected answer, part 1a**

*Live data represents any information, configuration data, and the contents of memory collected while a computer is on* (Clarke, 2010).

A laptop that is found powered on at the crime scene will most likely contain cybertrails. Cybertrails are identified as any evidence that a criminal leaves behind on a digital device, which includes any logs, cookies, configuration data, files, internet history, and processes and services that may be running on the powered on laptop (Volonino, Anzaldua, and Godwin, 2010).

And, how would you collect live data?

**Expected answer, part 1b**

*Computer memory, or RAM, will be affected by the examination process, thus it is critical that as few changes be made to the operating system as possible. A good start would be to photograph the laptop screen. Then, I would document who is logged in, what the IP address is, and what processes and services are running. Some common tools I would use are ipconfig, netstat, arp, hostname, net, attrib, tasklist, and route* (Clarke, 2010).

Once all forensic evidence has been collected, you need to preserve the evidence. What is meant by the preservation of the evidence?

**Expected answer, part 2a**

*The preservation of evidence refers to maintaining the integrity of files, and really, the entire hard drive. Just by opening a file, certain changes are made, such as to the time stamp changing. Thus, preserving evidence means keeping the data on the hard drive as if it has been untouched by investigators.*

How exactly would preserve this data?

**Expected answer, part 2b**
I would use well-known, acceptable forensic tools to preserve the integrity of evidence. For example, right away I would copy the hard drive using a bit-by-bit copy utility (such as dd.exe). Then, I would only use the duplicated hard drive to perform analysis on. When it came to individual files, before opening, viewing, and analyzing files, I would use hashing techniques. Hashing, or a hash function, would permit me to first fingerprint a file, which would produce a hashed output (Clarke, 2010, p. 32). This hashed output is the fingerprint of the file in its original, untouched state. Common hashing algorithms include MD5 and SHA-1. If a file did change during the analysis, the hash output would also change. Thus, by using bit-by-bit copying software and hash functions, I could preserve the integrity of evidence.

References


Preliminary Investigation and Incident Review

You already know that a computer forensics investigators job involves discovering, analyzing, and preserving certain digital files, and data that can be used as electronic evidence. This unit describes how a computer forensics investigator performs the preliminary investigation and incident review. Additionally, the responsibilities of the investigator related to understanding legal constraints, the intent and scope of the investigation, initial reviews, and the facts of the case will also be identified.

Outcomes

After completing this unit, you should be able to:

- Explain how the investigator performs the preliminary investigation, determines the facts of the incident, and carries out incident review.
Identify the requirements for acquiring and authenticating evidence.
Identify the methods by which the investigator determines the legal restrictions, intent, and scope of the investigation.

Course outcome(s) practiced in this unit:

**IT550-2:** Perform scenario-based investigations.

What do you have to do in this unit?

- Complete assigned Reading.
- Participate in Discussion.
- Complete unit Assignment.
- Participate in Seminar or complete Alternative Assignment.
- Complete the optional Learning Activity.

Textbook Reading:

Read Chapters 3 and 4 in *System Forensics, Investigation, and Response.*
Attending live Seminars is important to your academic success, and attendance is highly recommended. The Seminar allows you to review the important concepts presented in each unit, discuss work issues in your lives that pertain to these concepts, ask your instructor questions, and allows you to come together in real time with your fellow classmates. There will be a graded Seminar in Units 1 through 5 in this course. You must either attend the live Seminar or you must complete the Seminar alternative assignment in order to earn points for this part of the class.

**Option 1: Attend Seminar:**

The Seminar will review the Unit 2 topics and Assignment, and take a look into evidence preservation via hashing techniques.

Remember, if you do not participate in the weekly Seminar, you need to complete the alternative assignment.

**Unit 2 Assignment**

**Outcomes addressed in this activity:**

**Unit Outcomes:**
• Explain how the investigator performs the preliminary investigation, determines the facts of the incident, and carries out incident review.
• Identify the requirements for acquiring and authenticating evidence.
• Identify the methods by which the investigator determines the legal restrictions, intent, and scope of the investigation.

**Course Outcome:**

**IT550-2:** Perform scenario-based investigations.

View the Rubric below for more information
Unit 2 Assignment

Outcomes addressed in this activity:

Unit Outcomes:
- Explain how the investigator performs the preliminary investigation, determines the facts of the incident, and carries out incident review.
- Identify the requirements for acquiring and authenticating evidence.
- Identify the methods by which the investigator determines the legal restrictions, intent, and scope of the investigation.

Course Outcome:

IT550-2: Perform scenario-based investigations.

Assignment Instructions:

Your forensics team has provided the initial response detailing the meaning behind the cyber-terrorism case and the different types of associated evidence. In the preliminary investigative discussion your POC for the cybercrime case would like your team to disclose, in your Forensics Plan, how you will approach the incident review, to include the identification of any collection requirements for collecting, seizing, preserving, and authenticating the evidence. You will provide the POC with the known facts of the incident and what procedures were used during the initial case reviews.

Assignment Requirements:

The expected length of the report is 8-10 pages or 2000-2500 words. Your project submission should include the following in an MS Word document:
- A title page
- A report that includes the following:
  - Effective introduction
  - The use of APA throughout the main body of the paper (e.g., Mahaney, 2009) for all technical assertions
  - How you will approach the incident review, to include the identification of any collection requirements for acquiring and authenticating the evidence.
  - How your team will approach any legal restrictions and the determination of intent and scope.
  - The known facts of the incident and what procedures were used during the initial case reviews.
  - A conclusion allowing the reader to reach a high level of understanding of all the major topics presented.
  - A reference page in APA format

Save your Word document using the following file name format: Username-IT550-Assignment-Unit#.docx (Example: TAllen-IT550 Assignment-Unit2.docx). Submit your file to the Unit 2 Assignment Dropbox by the end of Unit 2.

Written Assignment Requirements:

Written work should be free of spelling, grammar, and APA errors. Points deducted from the grade for each writing, spelling, or grammar error are at your instructor’s discretion.

Copyright Kaplan University
For more information and an example of APA formatting, see the resources in Doc Sharing or visit the KU Writing Center from the KU Homepage.

Also review the KU Policy on Plagiarism. This policy will be strictly enforced on all applicable Assignments and Discussion posts. If you have any questions, please contact your professor.

Review the grading rubric below before beginning this activity.

**Assignment Grading Rubric = 100 points**

<table>
<thead>
<tr>
<th>Assignment Requirements</th>
<th>Points Possible</th>
<th>Points Earned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment includes how you will approach the incident review, including the identification of any collection requirements for acquiring and authenticating the evidence.</td>
<td>0–25</td>
<td></td>
</tr>
<tr>
<td>Assignment includes how your team will approach any legal restrictions and the determination of intent and scope.</td>
<td>0–25</td>
<td></td>
</tr>
<tr>
<td>Assignment includes known facts of the incident and what procedures were used during the initial case reviews.</td>
<td>0–25</td>
<td></td>
</tr>
<tr>
<td>Assignment includes a conclusion allowing the reader to reach a high level of understanding of all the major topics presented.</td>
<td>0–25</td>
<td></td>
</tr>
<tr>
<td>Total (Sum of all points)</td>
<td>0–100</td>
<td></td>
</tr>
<tr>
<td>Less points deducted for spelling, grammar and APA errors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adjusted total points</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>