Lab 7 - Assessment Worksheet

Automating E-mail Evidence Discovery

Course Name and Number: CYBS 7359-010

Student Name: Natnael Kebede

Instructor Name: Dr. Renita Murimi

Lab Due Date: 3/23/2020

Lab Assessment Questions

1. What was the content of the chat message between badguy11111 and badguy22222?

   The content of the chat message was a conversation about getting some money transferred, and it is going to a blue account. Additionally, the message indicates that there are two accounts that exist: a blue account and red account, with the red one being used for credit cards.

   Following the money transfer conversation, the message shows badguy11111 wishing badguy22222 a good trip to Germany, with thanks on both sides for shopping and completing their business transaction.

2. What program was identified by E3 as the chat software used by badguy11111?

   The program that was identifies by E3 as the chat software used by badguy11111 is Skype.

3. Explain how MD5 and SHA1 hash codes generated by E3 helps maintain the chain of evidence in a digital forensic investigation.

   During an investigation, a forensic investigator must be able to prove that the evidence was not altered during the course of the investigation. By comparing the hash code before the data is reviewed with the hash code after the investigation, the investigator can be assured that the data is preserved as long as the hash code did not change.

4. What was the e-mail application used by badguy11111 on the evidence hard drive under investigation?

   The e-mail application used by badguy11111 on the evidence hard drive under investigation was Eudora e-mail client using Microsoft Exchange E-mail.

5. What is the importance of the e-mail header to a forensic investigation?

   The e-mail header contains useful information such as the sender's account and the date. It also includes a message ID and an indication of whether or not the particular message is a reply to a related message. Additionally, the header keeps a record of the message's journey as it travels through communication network, providing an audit trail of every machine through which the email has passed.

   All of these make the header important to a forensic investigation since many computer crimes involve email and that even the investigation of non-computer crimes can require extracting evidence from e-mail sources.

6. How many attachments were included in the e-mails from badguy11111's evidence drive? What were the names of the files?

   There were three attachments included in the e-mails from badguy11111's evidence drive. The names if these files are:

   C:\Documents and Settings\Administrator\Desktop\badnotes1.txt
   C:\Documents and Settings\Administrator\Desktop\badnotes1.txt
   C:\Documents and Settings\Administrator\Desktop\badnotes2.txt