Lab #5 - Assessment Worksheet

Analyzing Images to Identify Suspicious or Modified Files

Course Name and Number: CYBS 7359 - 010

Student Name: Natnael Kebede

Instructor Name: Dr. Renita Murimi

Lab Due Date: 03/01/2020

Lab Assessment Questions

1. Why might it be important to confiscate and identify the websites and kinds of images found on a suspect's computer?

   it might be important to confiscate and identify the websites and kinds of images found on a suspect's computer because they are also evidence of the motives and illegal activities undertaken , which is particularly important with investigating child pornography or sex offender cases.

2. Explain what the P2 Commander Image Analyzer does and what it looks for.

   The Image Analyzer scans all images to determine if any are suspected to contain sensitive material that may be relevant to a criminal investigation. It also lets one adjust the sensitivity of the engine for the scan process.

3. How do you decrease the amount of false positives in the Highly Suspect or Suspect categories?

   You can do decrease the amount of false positives in the Highly Suspect or Suspect categories by decreasing the Engine Sensitivity setting and sliding the ticker of the slide ruler related to the option, to the left.

4. Into how many different categories does P2 Commander’s Sorted Files feature categorize all of the identified files? What are these categories?

   17 Categories: 1.Documents 2.Email 3.Chats 4.Spreadsheets 5.Graphics 6.Databases 7.Executable 8.Compressed 9.Multimedia 10.Text 11.XML 12.Encrypted 13.Financial files 14.Game Console Files 15.Others 16.Image Analyzer Results 17.Recovered from Unallocated Space

5. How many files did the Sorted Files feature identify on the evidence drive?

   3,152 Files

6. Where would you look to identify a rogue application, malicious spyware application, or keyboard logger application on the target evidence drive?

   Within the Executables category in the left pane of the Sorted Files content on the case

7. Where would you look to identify ZIP files and compressed files that may actually contain embedded malicious software?

   Within the Compressed category in the left pane of the Sorted Files content on the case

8. Where must you also look to examine possible image files on the evidence drive under investigation?

   Within the Image Analyzer Results category in the left pane of the Sorted Files content on the case

9. Why is it also important to look under the Graphics folder directly under the Sorted tree as well as the Image Analyzer Results category?

   The Graphics category can be just as important as the Image Analyzer Results category because files that are not suspected of suspicious content or were filtered out of the search for some other reason are included in the Graphics category within the Sorted Files list, and can still be evident for investigation purposes.