Alexander Cannell

Professor Barker

10/04/2012

CSIS 3700

1. What is the primary goal of a static acquisition?
   Static acquisition is a data acquisition method used when a suspect drive is write-protected and can't be altered. If disk evidence is preserved correctly, static acquisitions are respectable.

2. Name the three formats for computer forensics data acquisitions.
   -Raw Format
   -Proprietary Format
   -Advanced Forensic Format

3. What are two advantages and disadvantages of the raw format?

   Advantage:

   Raw format are fast data transfers and the capability to ignore minor data read errors on the source drive.

   Disadvantage:

   Some raw format tool especially freeware versions, might not collect marginal sectors on the source drive, meaning they have a low threshold of retry read on weak media spots on a drive. Many commercial tools have a much higher threshold of retry reads to ensure that all data is collected.

4. List two features common with proprietary format acquisition files.
   -the option to compress or not compress image files
   -the capability to split an image into smaller segmented files for archiving purposes
   - the capability to integrate metadata into the image file

5. Of all the proprietary formats, which one is the unofficial standard?
   Expert witness format

6. Name two commercial tools that can make a forensics sector by sector copy of a drive to a larger drive.
   -Encase
   -SafeBack

7. What does a logical acquisition collect for an investigation?
   The logical acquisition collect's is only specific files of interest to the case.

8. What does a sparse acquisition collect for an investigation?
   The sparse acquisition collect's specific files of interest to the case as well as fragments of unallocated data.

12. Why is it good practice to make two image s of a suspect drive in a critical investigation?
    To make sure you have a backup copy, or at least one good copy of the evidence in case it fails at life.

13. When you perform an acquisition at a remote location what should you consider to prepare for this task?

    To determine whether there is sufficient electrical power, lighting, check if the temperature, and humidity at the location.