Filesig Software Solutions
Established 2001

Case Sanitizer Validation

Note: This validation applies to Case Sanitizer v1.1 and below. Encase and Forensic Toolkit Imager are registered trademarks of Guidance Software Inc and Accessdata respectively.

Summary

Case Sanitizer has the ability to wipe selected areas of a file, which includes raw disk images. The option to be validated, referred to as 'Search and WIPE data (offset list)' allows the selective wiping of areas within a file using an offset list. The offset list contains positions within a file designated as areas to be sanitized. It is the responsibility of the examiner when selecting the positions to be sanitized.

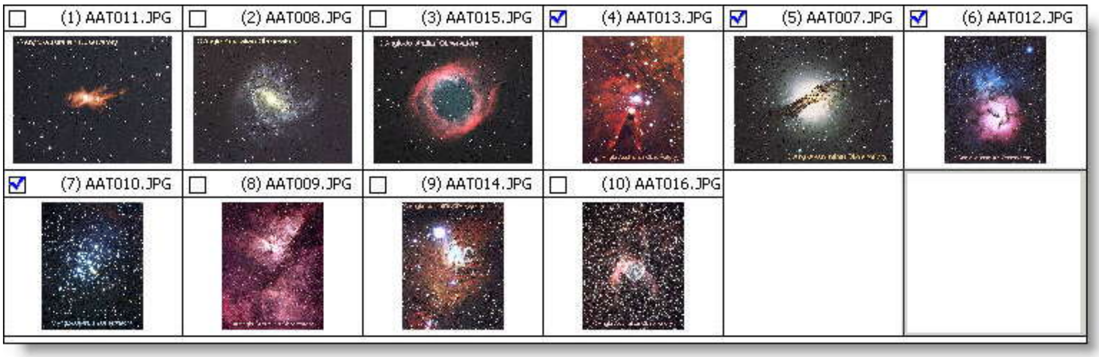
Method

The process to be tested is the ability to successfully read a selected file, sanitize selected areas and verify the results. The sanitized areas will be manually verified as part of this process.

1. Floppy Diskette, full format performed, onto which 10 sample pictures were copied. Diskette is then write-protected.

2. Using Accessdata FTKi v2.5.1, one Raw (dd) image and one E01 image was created. Image files are verified without error.

3. Using Encase v5 by Guidance Software, the E01 image was loaded and the following files were selected and then bookmarked: 'AAT013.JPG', 'AAT010.JPG', 'AAT012.JPG' and 'AAT007.JPG'.



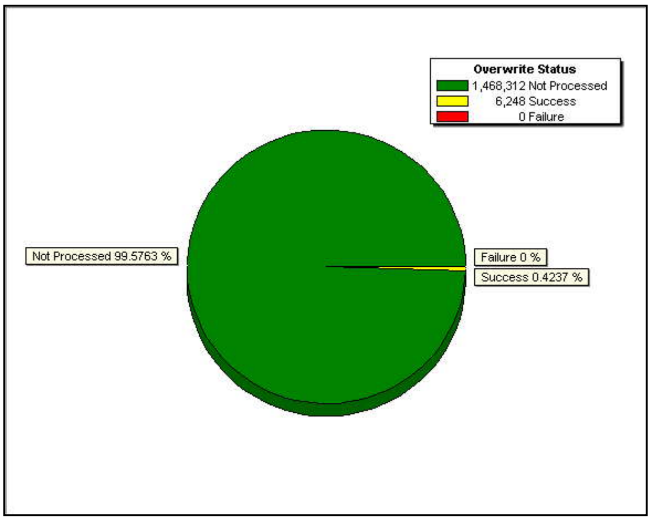
☐ (1) AAT011.JPG
☐ (2) AAT008.JPG
☐ (3) AAT015.JPG
☑ (4) AAT013.JPG
☑ (5) AAT007.JPG
☑ (6) AAT012.JPG
☑ (7) AAT010.JPG
☐ (8) AAT009.JPG
☐ (9) AAT014.JPG
☐ (10) AAT016.JPG

4. Within the bookmarks section of Encase the BOOKMARK START of the selected files was exported to a text file. *This export file was then opened in Windows Notepad and saved as an ANSI encoded text file. (By default Encase saves export lists as Unicode, at the time of writing Case Sanitizer only supports ANSI encoded text files and does not support Unicode).*

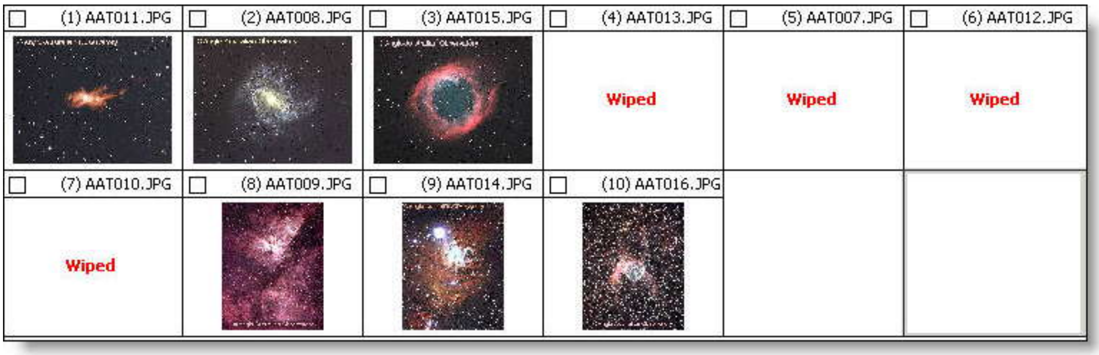
5. Using Case Sanitizer v1.1, the option 'Search and WIPE data (offset list)' is selected, CRC verification is enabled, the raw dd image is added and the exported offset list is loaded.

6. On completion, the results graph was exported (CRC verification must be enabled for this feature to function correctly).

7. Case Sanitizer creates a log detailing the areas that have been sanitized using the default file 'wipeimage.bmp'. The log file and the resulting sanitized image were verified using WinHex v13.3.



8. The sanitized image was then loaded into Encase.



Conclusion

Case Sanitizer successfully read the selected file, correctly sanitized and verified the sanitized areas.