CSG256 -- Security, Privacy and Usability
Peter R. Douglass

Assignment 5
May 31, 2004

An Analysis of a Memory Image File

This memo reports the findings of an analysis of a memory image file performed by the author. The image file was obtained from a compressed file downloaded on 28 May 2004 from http://www.ccs.neu.edu/course/csg256/images/40i.img.gz .[1] This compressed file was then decompressed using the utility gunzip. The compressed file resides on a website for students of the course CSG256 at Northeastern University. The author of this memo is currently enrolled in that course.

The image file was analyzed using the forensic tools The Sleuth Kit (version 1.68), Autopsy (version 1.74), biew (version 5.6.1) and a few ad-hoc utilities written by the author. All analysis was performed on a system running Fedora Core 1 Linux. The Sleuth Kit (previously known as TASK) is a collection of open source software tools which support forensic analysis of digital media. Autopsy is a web-based user-interface for The Sleuth Kit. Biew is a "hex" file editor. The author wrote ad-hoc utilities for searching the image and for making modifications to the file allocation table within a copy of the image.

The decompressed image file consisted of 131,047,936 bytes (equivalent to 255,953 sectors of 512 bytes each). The Sleuth Kit reported 255,952 sectors; however tests showed that the final sector contained no information.

Sector 0 of the image contained a FAT16 volume boot record. The code area of this boot record contained no code or other information. The remainder of the image was organized consistently with a FAT16 file-system. The directory structure within the image appeared as:

```
+ (root directory)
  + dcim (directory)
    + 100_Fuji (directory)
  + .Trashes (directory)
    + 501 (directory)
    + _501 (file)
```

With the exception of theseitems, and space reserved for the system, the FAT16 file allocations tables showed all other sectors as unallocated.

The 501 directory contained no deleted entries. The author of this memo has not yet determined the type of the file "_501" or to make sense of its contents.

The dcim directory contained no deleted entries. The 100_Fuji directory contained 149 deleted entries. These entries were "undeleted" using the biew hex editor. The files corresponding to these entries had also been de-allocated in the file allocation tables (FATs). The author re-allocated clusters to these entries using the assumption that the files were originally allocated in contiguous memory chunks. Each of these files was then check for integrity by visual inspection of the "opened" files. (All of the files were of type .jpg or .avi).

[1] The MD5 value for the compressed file is eb80a6253f6874d325184d5860e9ab85, the MD5 value of the image file is 831b405f41f739668542c02973a8c80d.

All files appeared to have been recovered with integrity except for two. For both of the two problematic files, the assumption of contiguous memory allocation resulted in embedding a directory cluster within the file. The allocation tables were edited to “jump over” those clusters.
One of the files recovered in this way was a .jpg file, and appeared to be recovered almost completely. The second file was an .avi file, and the author’s viewing tool refused to open it.

The files recovered in the 100_Fuji directory accounted for the bulk of unallocated sectors, but not all sectors. The image was scanned for sectors containing only hexadecimal FF bytes. All sectors past the last recovered file consisted entirely of FF bytes. Additionally, after the first 48MB of the image, the sectors between recovered files consist of FF bytes. Sectors consisting only of FF bytes do not occur in the first 48MB of the image. It has not been determined whether any of the sectors between recovered files in the first 48MB have recoverable data. Searches for strings within the image failed to find significant text.

The following table summarizes the visual content of the recovered files.

Files	Description of Images	Comments
1 - 55	Scenes from a high tech fair (NEXTFEST).	The instructor for csg256 is visible in several of the images.
56 - 60	Interior of living quarters.	
61 - 64	Exteriors of some houses.	
65 - 68	Exteriors of some places of business.	The addresses of some of the business are visible. The location is widely known by street name.
69 - 92	Interior of a place of business. Includes still and moving images of performers, including musicians and at least one comedian.	A clock is visible showing the time of 9:25. The timestamp of the file indicates a time of 11:30 p.m. The name of the place of business is visible.
93	** Unrecovered .avi file **	
94 - 99	Interior of living quarters, grocery store, flowers.	
100	Motion picture of airplane on the ground.	
101	A turbine (possible a jet turbine).	
102 - 113	Interior of some exposition	Possibly the same location as in files 1-55.
114 - 123	Child's birthday party	
124	Street Corner	
128 - 144	Outdoor scenes near a waterway	Includes images of a building, a dike or break-water, some valve-stems, pwer-lines and a bridge.
145	Skeletal remains of an animal	
146 - 149	Domestic scenes	

None of the recovered .jpg and .avi files contain obscene or pornographic content.