Digital forensic: Analyzing disks

Jan Gašperlin

University of Ljubljana Faculty of Computer and Information Science
E-Mail: jg1724@student.uni-lj.si

1 Introduction

At course digital forensic we were assigned task to analyze given vmdk for specific string denoted by folder name in which they reside. We obtained four disks in which we had to find all files containing one of string sequence AAAA, BBBB, CCCC, DDDD. We had to approach those disk as if they were real and made appropriate disk images. Which we analyzed further using forensic tools such as Autopsy.

2 Plan

Before we started with work we made detailed plan which was separated in 3 parts as followed:

- Create backup images
  - Make sure no data on disk could be changed
  - Use tool *dd* to copy complete data from disk into .img file
  - Make sure copies are identical using sha256sum to calculate hash
- Analyze images using forensic tools
  - Search for string sequence on disk (allocated and unallocated space)
  - Restore deleted files
  - Carve out potential files in unallocated space
  - Search for string sequence in all files
  - Examine images if sequence is visual
  - Examine document if sequence is drawn using ascii characters
- Present analyze results
  - Present files in which string sequence was found
  - Present image files in which string sequence was observed
  - Present additional abnormalities during analysis

3 Creating images

Since we are doing digital forensic we decided to use Kali Linux distribution that comes with installed forensic tools which we plan to use for analysis. At the same time we will use this distribution to make disks backup image files. We used Virtual Box to setup our environment in which we mounted provided vmdk-s. This was done one disk at the time on which we used the following commands:

```
# Make sure no changes happen to disk
# sdb is our mounted disk
blockdev --setro /dev/sdb
blockdev --setro /dev/sdb1
blockdev --setro /dev/sdb2

# Make copy, bs=256k speeds up the process
dd bs=256k if=/dev/sdb conv=noerror,sync
 of=disk_{XXXX}_backup.img

# Check if hash matches
dd bs=256k if=/dev/sdb conv=noerror,sync
| sha256sum


dd bs=256k if=disk_{XXXX}_backup.img
conv=noerror,sync | sha256sum
```

We obtained following hash codes:

- Disk AAAA: 4f99b5e35edc1ca4434dbce45af421 40e081bad39c5667c0cc92f03e4a74d8ba
- Disk BBBB: 363b94da7c9a5cf7726198127722c7 9dc6d34f83569b09ae12729c1f1815c9fc
- Disk CCCC: 97e2844aabf09470364b0c248f90a2 e80275810acebe7906fe3fa93e9b837bfb
- Disk DDDD: 5c58472573f865540f1d93ae6ea16a 3cf3a172a4ce7f59c2a5144bc096b10479

4 Analysis

We found bug in Autopsy provided with Kali Linux and were unable to search strings. This is why we decided to use Windows distribution to do our analysis. We created shared folder in VM and copy disk images to host Windows system. We used Autopsy 4.11.0 to analyze disk, which was ingested by default modules. Keyword-Search module was configure to search for string *XXXX*. Digest was ran on complete disk including unallocated space. Upon digesting image we used keyword search result to further analyze disk. We tried to narrowed it down more with regular expression but were unsuccessful since it was not case-sensitive. We noticed abundant amount of

files in which sequences were found, but only rarely as string. To search for string we extracted only previously found files and run our script using command

```
./search_strings.sh searched/
        files_contains_XXXX.txt
```

The first argument represents folder that contains extracted files, second arguments is string sequence we are searching for and third argument is output folder. Scripts consist of following commands:

```
DIR=$1
OUTPUT=$2
echo "" > $OUTPUT
SEARCH_STRING="XXXX"
if [ -z $3 ]
then
 echo "Searching for default
  string $SEARCH_STRING"

else
 SEARCH_STRING=$3
 echo "Searching for
  string $SEARCH_STRING"

fi
for filename in $DIR/*; do
 strings < "$filename" |
  grep "$SEARCH_STRING" > /dev/null

 if [ $? -eq 0 ]
 then
  echo "Found in    $filename"
  echo "$filename" >> $OUTPUT
 fi
done
echo "Files found"
cat "$OUTPUT" | wc -l
```

This reduced number of files, but there were still many.

Further we restored all deleted and carved files found by Autopsy this includes unallocated space. This was done similarly by extracting files and then running our script.

We also manually checked pictures that were recently modified or accessed, if they contain XXXX sequence in picture.

Since we also need to report what happened on computer we looked at most recently deleted files, browser history, browser cookies and document files.

4.1 Disk AAAA

We found following items

- Files found in file system containing sequence XXXX
  - Count: 1066
  - Using script to find XXXX: 417
  - Important boot file *vol2/Boot/da-DK/bootmgr.exe.mui* also contains string XXXX, but it was part of background-color attribute value and was deemed safe.
- Extracted deleted and carved files
  - Count: 3006
  - Using script to find XXXX: 1
- Browser cookies
  - Total number of cookies: 8
  - Interesting cookie: From url `http://246059135.log.optimizely.com/` although site does not contain anything.
- We found some files that have wrong extension possible hiding, some of them even had XXXX pattern found on path *Windows/winsxs/x86_prnca00x.inf_31bf3856ad364e35_6.1.7600.16385_none_8ce7dc434dabb706/I386/CNBP1.DAT*
- Browser history - We noticed that IE was used to download Firefox.
- Documents
  - Documents - We found no pdf document and only single word document, that described types printing.
- We noticed that tmp.edb file (Microsoft Exchange Server) also contained lowercase *xxxx*

No serious abnormalities were detected during disk analysis. We mostly searched files that were filtered with search for string *XXXX* and took into consideration last access time and last modified time. If perpetrator was capable of changing files metadata in this case time a more detailed analysis would be needed.

4.2 Disk BBBB

We found following items

- Files found in file system containing sequence XXXX
  - Count: 1071
  - Using script to find XXXX: 417
- Deleted and carved files restored
  - Count: 3006
  - Using script to find XXXX: 1
- Browser cookies - No changes from previous drive
- We found same files with wrong extension
- Files most likely we are searching for
  - Users/user/Documents/eko_cert.odt - contained string XXXX and was recently modified
  - Users/user/test.mp4 - a video file displaying XXXX
  - Confidential pictures of auto design
    - Users/user/Pictures/confidential-04.jpg Contains black XXXX, we also carved this file two times
    - Users/user/Pictures/confidential-01.jpg Contains white XXXX
    - Users/user/Pictures/weeee_43.gif Contains Brown XXXX

  - Users/user/Documents/document.odt - Dokument doc, ki vsebuje XXXX
  - User/user/ Harry Potter folder we found files script.js and css.css that were recently modified. We included them into html that had empty body tag in hopes script will render XXXX. As result we got some buttons that did not do anything. We figured we needed cookie file which we stop searching for since time was of essence.

4.3 Disk CCCC

We found following items

- Files found in file system containing sequence XXXX
  - Count: 1071
  - Using script to find XXXX: 417
- Deleted and carved files restored
  - Count: 3006
  - Using script to find XXXX: 1
- Browser cookies - No changes from previous drive
- We found same files with wrong extension
- Files most likely we are searching for
  - Users/user/Documents/eko_cert.odt - contained string XXXX and was recently modified
  - Users/user/test.mp4 - a video file displaying XXXX
  - Pictures
    * Users/user/Pictures/confidential-02.jpg - Contains black XXXX
    * Users/user/Pictures/confidential-01.jpg - Contains white XXXX
    * Users/user/Pictures/weeee_43.gif - Contains Brown XXXX
    * Users/user/Pictures/xxxx.jpg - Name and it contains black XXXX
    * Users/user/Pictures/SabOnline10.GIF - Contains XXXX
    * Users/user/Pictures/chat_system_2x.png - Contains XXXX
  - Users/user/Pictures/lorem.doc - It contains XXXX
  - Users/user/Documents/document.odt - Dokument doc, ki vsebuje XXXX
  - User/user/ Harry Potter folder we found files script.js and css.css that were recently modified. We included them into html that had empty body tag in hopes script will render XXXX. As result we got some buttons that did not do anything. We figured we needed cookie file which we stop searching for since time was of essence.
  - Users/user/Documents/narocilo.odt - Vsebuje dopise podatke o kriminalnem pocetju
  - Users/user/Documents/jaz_nisem_nic_posebnega.odt - Vsebuje dopise podatke o kriminalnem pocetju
  - ProgramData/Misrosoft/.../Report.wer - Vsebuje dopise podatke o kriminalnem pocetju

4.4 Disk DDDD

We found following items

- Files found in file system containing sequence XXXX
  - Count: 1066
  - Using script to find XXXX: 417
- Deleted and carved files restored
  - Count: 3006
  - Using script to find XXXX: 1
- Browser cookies - No changes from previous drive
- We found same files with wrong extension

5 Conclusion

It appears perpetrators tried to steel some documents regarding auto design and production. Most helpful during our analysis was definitely modified and access timestamp, while deleted and carved files were also easy to spot, with addition that most of them were located in user home folder. Additional reports for each disk are available at `https://github.com/JGasp/df-sem1-report`, which were made using Autopsy.