Coursework Digital Forensics Essentials & Incident response
Module code M2G421123
Session: 2015/2016, 1st Diet

Matthias Seifert
Student ID: S1540546
mseife200@caledonian.ac.uk

December 10, 2015

Contents

Chapter 1

Contemporaneous Notes

The contamporaneous notes for this coursework are included in the zip file (see `coursework.Notes`).

Chapter 2

Self-reflection

Doing the coursework has shown me that it is very important to really know the tools one is working with. Not only is it very time consuming if you have to find out how a tool works when applying it to a system under investigation but it also has a influence on the outcome of the investigation. The more steps have to be repeated during the investigation the more errors may happen especially if a lot of trial-and-error is involved.
In order to achieve better results faster some (maybe self developed) tools come in handy. Especially when hash values have to be created a bash shell script like `createhashes <file>` that creates both md5 ans SHA1 and saves both of them to a predefined directory in the names `<filename>.sha1` and `<filename>.md5` or a script comparing the file extensions and the internal file information the would be a big help. Comparing file extensions and internal file information manually may work for about 70 files but is not possible for a larger amount of files.
The next point is that the accuracy of the case notes created is unbalanced in my opinion. While some steps like the creation of hash values for the downloaded zip file and the files contained may not be necessary in the scope of this coursework but are descibed very precisely a more precise description of the use of Autopsy would be necessary.
Finally the contents of both allocated and deleted data on the given virtual disk have not been examinated at all. While I am not entirely sure if this was part of the coursework this would definitely be part of a real investigation.

Appendices

Appendix A

List of files included in the .zip archive

Table A.1: **Files included in the coursework**

Filename	Description
`acquisition.script`	`acquisition.script` as mentioned in the case notes
`acquisition.script.clean`	`acquisition.script` without escape sequences.
`coursework.Notes`	The case notes written with Forensic casenotes
`deletedFiles_files/`	Additional files to display `deletedFiles.html`
`deletedFiles.html`	Website containing information about deleted files from Autopsy
`fileHash.list`	md5 hash values of all allocated files on the given virtual disk.
`fileHash.list.md5`	md5 hash of `fileHash.list`
`fileInformation.list`	The information for each allocated file on the given virtual disk.
`fileInformation.list.md5`	s md5 hash of `fileInformation.list`
`files.list`	The list of all files allocated files on the given virtual disk.
`files.list.md5`	md5 hash of `files.list`
`la.1.script`	`la.1.script` as mentioned in the case notes
`la.1.script.md5`	md5 hash of `la.1.script`

To be continued on the next page

Files included in the coursework – continuation

Filename	Description
`la.2.script`	`la.2.script` as mentioned in the case notes
`la.2.script.md5`	md5 hash of `la.2.script`
`la.3.script`	`la.3.script` as mentioned in the case notes
`la.3.script.md5`	md5 hash of `la.3.script`
`mounting.script`	`mounting.script` as mentioned in the case notes
`mounting.script.clean`	`mounting.script` without escape sequences
`mounting.script.md5`	md5 hash of `mounting.script`
`restoredHashes.list`	List of the md5 hash values of the restored file
`restoredHashes.list.md5`	The md5 hash of `restoredHashes.list`
`sdb1.md5`	md5 hash of `/dev/sdb1`
`sdb1.sha1`	SHA1 hash of `/dev/sdb1`
`timeline.txt`	The time line of fiole acticity as retrieved from Autopsy.
`timeline.txt.md5`	md5 hash of `timeline.txt`