

Lab8: Challenge

CNIT42000-001

Ethan Hammond

Prof. Tahir Khan

Date Submitted: 04/06/23

Date Due: 04/06/23

Table of Contents

Table of Contents	2
Abstract	3
Report	4
Task 1:	4
Conclusion	13
Appendix A: Time Chart	14
Time Chart	14

Abstract

This lab contained finding keys within files on a folder off of a drive image. All keys were concealed within the folders with different methods and different digital forensic methods were used to uncover the keys and collect them. Uncovering methods that were used included ADS file recovery with Windows CMD tools, Autopsy investigation of hidden text, password brute forcing of encrypted files, steganography, and WinHex hex editor investigating file signatures. Software that was used was LADS via Windows CMD, Autopsy, WinHex, and OpenStego. Additional software that could have been used was Magnet Axiom, other hex editors, and other steganography tools. These tools are important for a forensic investigator to understand to do an efficient and effective job of recovering as much relevant data as possible from a drive image off of a suspect's computer. The amount of time that the lab took can be seen in the time chart in Appendix A below.

Report

Task 1:

The first tactic that was done to find the maximum amount of keys possible in a short time period was to find all ADS files. The tool 'LADS' was used via Windows CMD to find all 5 files that had ADS hidden content in them. Then, those files were investigated more thoroughly.

```
C:\Users\Ethan>"C:\temp\DataHiding\DataHiding\Useful Resources\lads\lads.exe" C:\temp\DataHiding /S
LADS - Freeware version 4.10
(C) Copyright 1998-2007 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory C:\temp\DataHiding\ with subdirectories

  size  ADS in file
-----
    26  C:\temp\DataHiding\DataHiding\2\What is hidden can be found.docx:Zone.Identifier
    26  C:\temp\DataHiding\DataHiding\3\The presence of all wavelengths of light.docx:Zone.Identifier
    26  C:\temp\DataHiding\DataHiding\4\Only the trusted one can open this.docx:Zone.Identifier
    26  C:\temp\DataHiding\DataHiding\á\10\Try Me.docx:Zone.Identifier
    26  C:\temp\DataHiding\DataHiding\á\7\GreekArchitecture.xlsx:Zone.Identifier

130 bytes in 5 ADS listed
```

Figure 4: ADS files found with LADS.

Multiple digital forensic methods were used to uncover all of the keys. The first one, located in Congrats.txt, was found after opening the \DataHiding.rar\DataHiding\ folder. The folder was unlabeled, and contained this text file shown in Figure 1 containing the key.

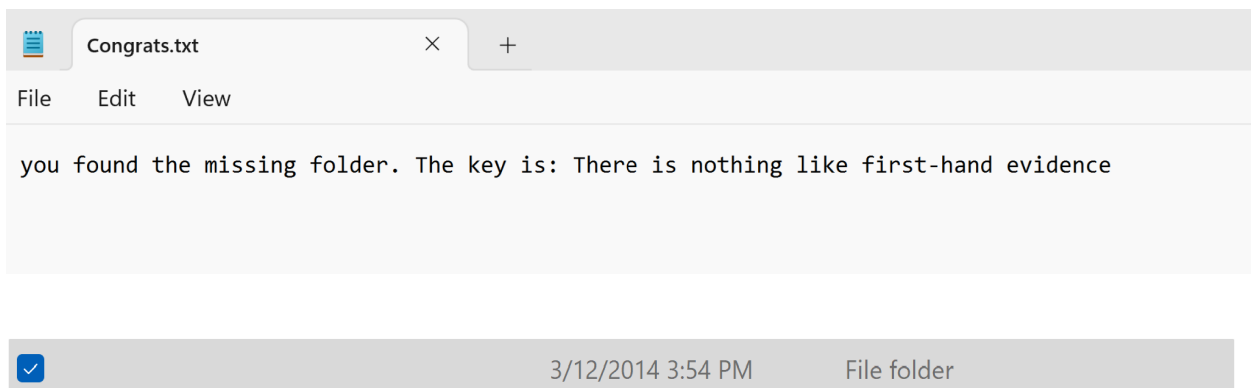
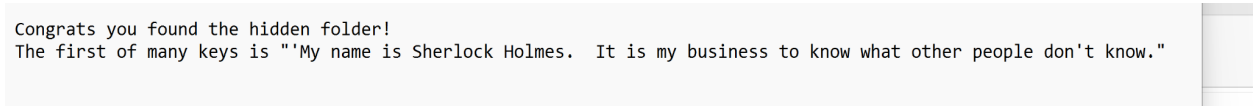


Figure 1: Congrats.txt key contents found in the rar folder.

The next key that was found was found lying in the first DataHiding folder. This was the first key, and was very simple to obtain, as there was no need for any sort of forensic software to uncover. The key can be seen below in Figure 2.



```
Congrats you found the hidden folder!  
The first of many keys is "'My name is Sherlock Holmes. It is my business to know what other people don't know."
```

Figure 2: 1_OpenMeFirst.txt found in \DataHiding\.

The next key that was found was found after running an executable file found in the '1' folder. The .exe file was changed to a .exe, and the executable was ran, revealing the next key of the lab. The executable output can be seen below in Figure 3. This was a classic file extension change, and no need for external forensic software to uncover.



Figure 3: \DataHiding\1\runMe.exe. Changed to .exe.

The next key was also found without and external forensic software as the key was in a text file inside of \DataHiding\5\system32\is.txt. The forensic countermeasure used in this situation was to place a file in a location that would blend in. System32 is not where text files are typically placed, although an experienced digital forensic investigator would find it. The key can be seen below in Figure 5.

The key is "there are no keys here"

Figure 5: Key found in system32 folder.

The next key was uncovered using forensic software as the key was hidden with ADS, and cannot be seen without software. Autopsy was used to see the full text of the file, that revealed the key in an otherwise empty word document. The key was found in \DataHiding\3\The presence of all wavelengths of light.docx and can be seen in Figure 6 below.

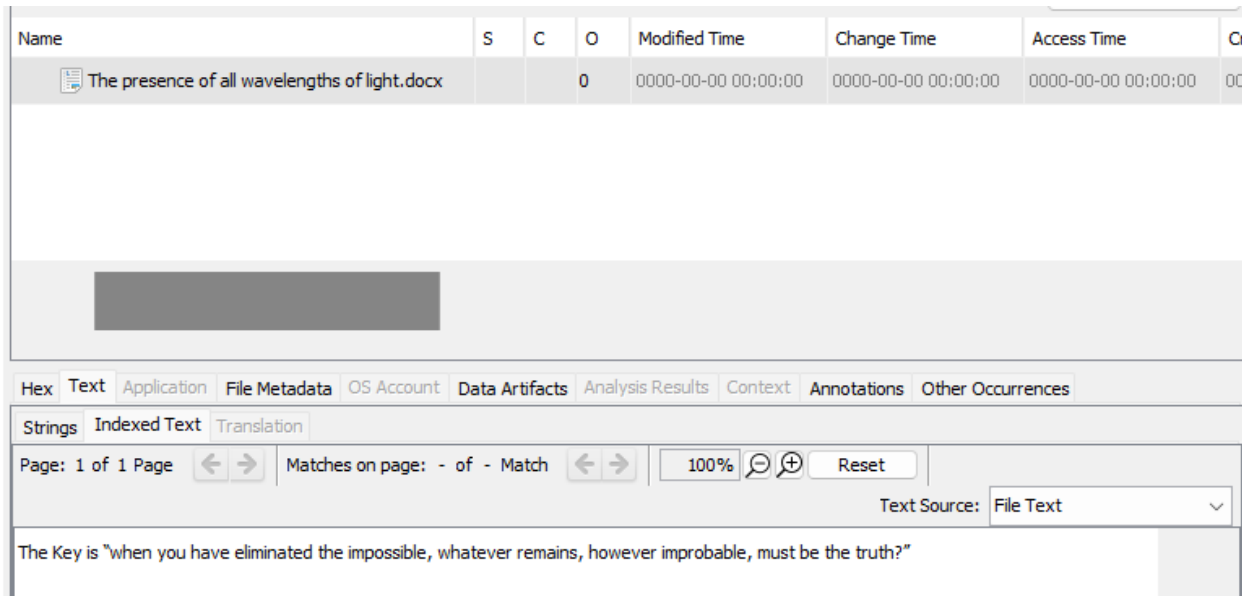


Figure 6: ADS hidden key uncovered in Autopsy.

The next key was uncovered the same way as the previous key. The message was hidden with ADS, as an MS Excel spreadsheet contained a hidden key that would not be able to be found without a file ADS finder or Autopsy to see the full text of the file. The key and file details can be seen below in Figure 7. The file was located in \DataHiding\7\GreekArchitecture.xlsx.

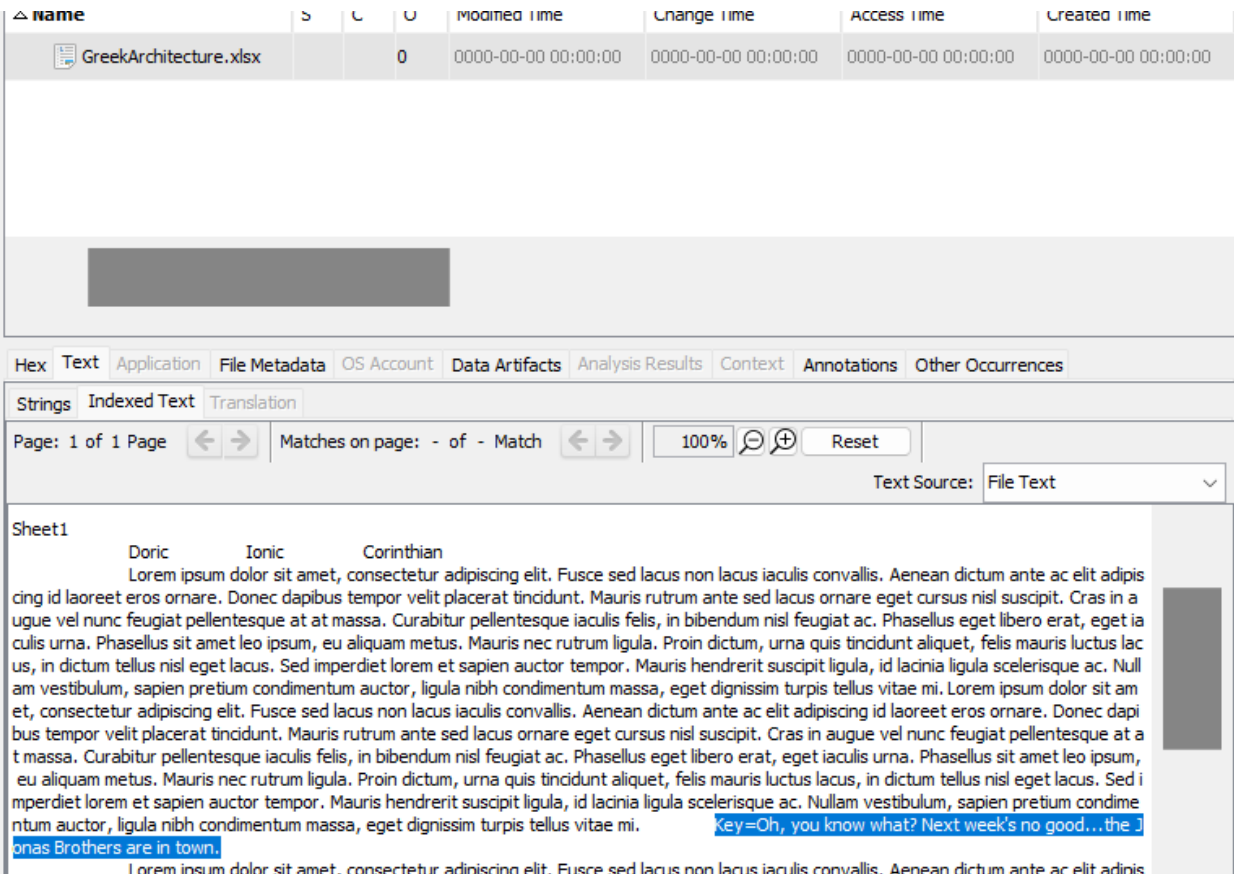


Figure 7: Greek architecture key was found with Autopsy.

The next key was found in Autopsy and was hidden by placing it in what can seem like a shortcut loop. The key was placed into a subfolder of 42 folders named 'x'. This is an attempt to hide a file when the investigator might assume that the folder was a shortcut because it was not opening, when it was really just hidden. The contents of the folder and file key.txt can be seen below in Figure 8.

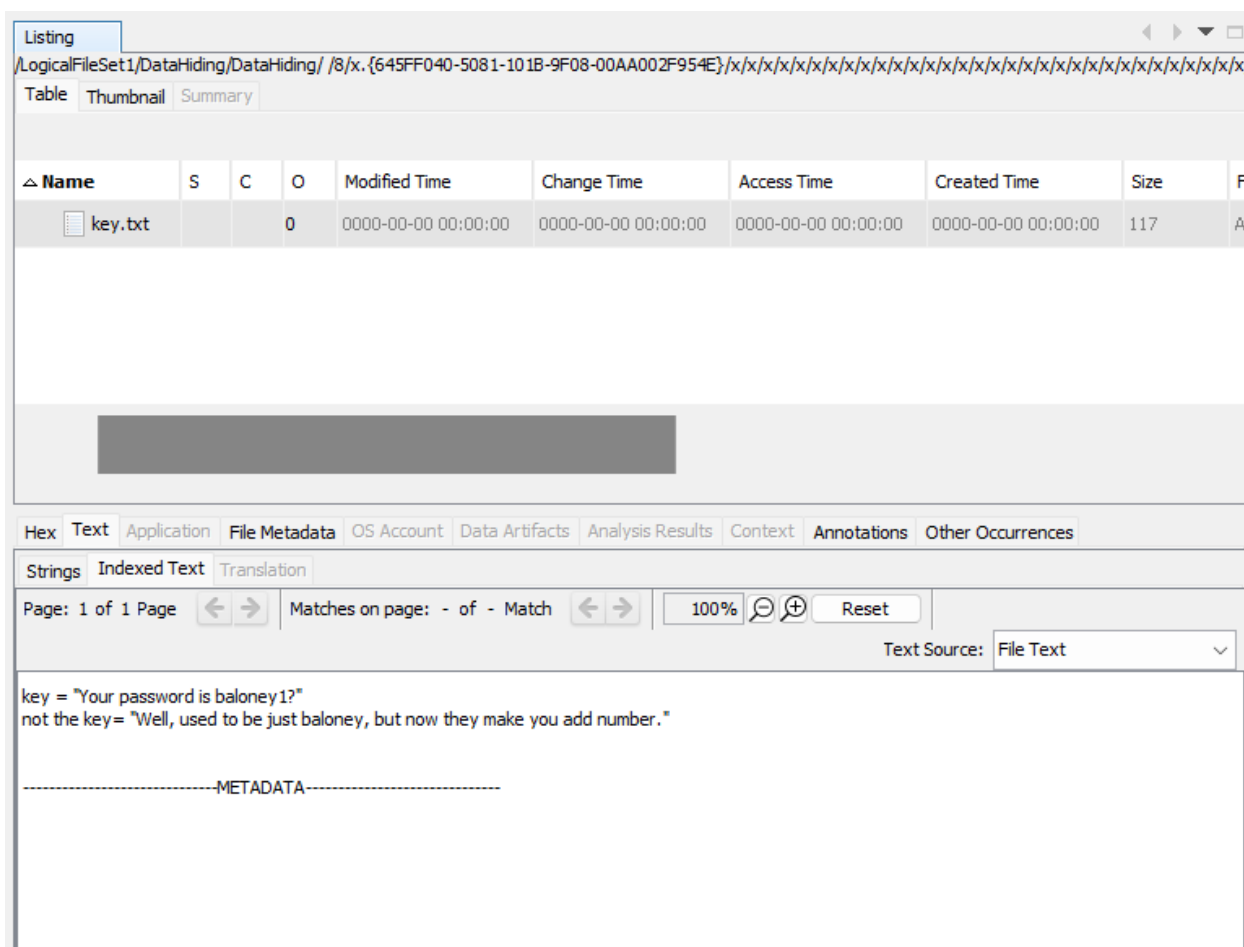


Figure 8: Opened in autopsy by expanding a ton of 'x' folders.

The next key was found by using the previous keys to brute force the password onto a file that was encrypted. The file was opened in Autopsy, and then password unlocked by attempting to use all passwords from the previous keys. After using the key 'Dr. Watson', the word document \DataHiding\4\Only the trusted can open this.docx was opened and revealed the key. The key and file contents can be seen below in Figure 9.



Awwww, Come on! It's funny!

The key is "It's where I keep all my things. Get a lot of compliments on this. Plus it's not a purse, it's called a satchel. Indiana Jones wears one."

Figure 9: Dr. Watson password to open the encrypted file.

The next key that was found was uncovered using a WinHex editor. The file `\DataHiding\9\NothingToSee.jpg` was opened in a hex editor and hex searched for a JPG file header and End of File marker. There were two offsets of 'FFD8' and 'FFD9', and after exporting the hex offset, a new JPG picture was uncovered with a key. This file and its contents can be seen below in Figure 10.



Figure 10: A second JPG file in the NothingToSee.jpg file uncovered with WinHex.

Key #	Key	Path to key	Technique
1	Figure 1	\DataHiding.rar\Data Hiding\ \Congrats.txt	Hidden Folders
2	Figure 2	\DataHiding\1_Open MeFirst.txt	None
3	Figure 3	\DataHiding\1\runMe .exe	File extension modification
4	Figure 5	\DataHiding\5\system32\is.txt.	Hiding in system32

Conclusion

Forensic investigators need to be well-versed in several different types of hidden files and tools to uncover hidden messages. Methods of hiding files include creating ADS appended files, encoding with steganography, hiding files within files, knowing operating systems and file systems, password protecting, and file extension modifications. Investigators must know the encoding methods as well as the ways to decode them. Tools have been created for encoding and decoding all of these. WinHex and hex editors, OpenStego and stego tools, Autopsy and file system viewing software, and LADS and ADS detection software have been created to combat these encoding types. If a forensic investigator knows these methods well enough, they can find all hidden files that a suspect has on a drive or drive image. With the goal of recovering all relevant information possible in mind, these tools will help digital forensic investigators do their job efficiently. As people become more effective in hiding files and evidence from investigators, forensic professionals must become more aware of encoding methods and how to combat them to recover data.

Appendix A: Time Chart

Time Chart

Task Number	Time Taken
Task 1	4 Hours
Report Writing	2 Hour
Total	6 Hours