|  |  |
| --- | --- |
| C:\user-pjpf\Briefcase-SO\so\so-12-13\slides\logo-IST-Tecnico.JPG | INSTITUTO SUPERIOR TÉCNICO  Departamento de Engenharia Informática  Forensics Cyber Security  MEIC / METI 2018-2019 – 1st Semester |

Digital Forensics Report

**Daniel Chaves - 81651**

**Afonso Santos - 81861**

**Manuel Sousa - 84740**

# Objectives of the investigation

This report is the presentation of a digital forensic investigation made for “The Mole Affair” case.

The artifacts collected for this investigation were in possession of John Mole, an ex-employee of DroneX. John Mole had privileged access to the design plans of DroneX’s new revolutionary drones and is believed that he might be illicitly stealing those plans in order to sell them to DroneX’s competitors. The research present on this article is related to those artifacts, collected from a pen drive that John Dole was carrying along after returning from a trip to Germany.

The main goal of this investigation is to find evidences on collected artifacts that may help to clarify a possible involvement of John Mole in this case.

# Artifacts for analysis

We received a list of files from a pen drive that John was carrying along after returning from a trip to Germany.

The presented list constitutes all the collected artifacts in its original state.

|  |  |
| --- | --- |
| Investigation ID | A-01-CATHEDRAL-PNG |
| File name | cathedral.png |
| File Type | PNG image data, 696 x 462, 8-bit/color RGBA, non-interlaced |
| File Size | 577263 Bytes |
| sha1 sum | e87a53d1397c620979affd75cfa94e602342faec |
| md5 sum | 55fd5b1d42072955e15769b55a390400 |

|  |  |
| --- | --- |
| Investigation ID | A-02-MUNICH-TXT |
| File name | munich.txt |
| File Type | UTF-8 Unicode text, with very long lines |
| File Size | 15069 Bytes |
| sha1 sum | bef7a9c92af5c28f473c841bc3c04df732fde5ab |
| md5 sum | c6596b360ac97889c4f2d68ba6787f92 |

|  |  |
| --- | --- |
| Investigation ID | A-03-ONLINE-BANKING-ZIP |
| File name | online\_banking.zip |
| File Type | Zip archive data, at least v2.0 to extract |
| File Size | 101258 Bytes |
| sha1 sum | 4b4cf077a5c34904cd05836b800772c3aa13cca0 |
| md5 sum | b3baa737b818db4f52a681f0cf8d440c |

|  |  |
| --- | --- |
| Investigation ID | A-04-STREET-PNG |
| File name | street.png |
| File Type | PNG image data, 945 x 630, 8-bit/color RGBA, non-interlaced |
| File Size | 1264820 Bytes |
| sha1 sum | 1612d7f59e375e02e8f5232e2f8fc525260a09a9 |
| md5 sum | f1ea1beaa6a838d16b4d457c6fe68fd0 |

|  |  |
| --- | --- |
| Investigation ID | A-05-COMPRESS-PY |
| File name | compress.py |
| File Type | python 2.7 byte-compiled |
| File Size | 3101 Bytes |
| sha1 sum | a6ba03a346c07e8e2cfab00cf8fac7d1e1c220fb |
| md5 sum | 72eab63334dcd0f73418e32999b71f05 |

|  |  |
| --- | --- |
| Investigation ID | A-06-OKTOBERFEST-PNG |
| File name | oktoberfest.png |
| File Type | PNG image data, 1200 x 524, 8-bit/color RGBA, non-interlaced |
| File Size | 1234371 Bytes |
| sha1 sum | 2e58a9667b74d42520d12ce5b14ff6057811caf6 |
| md5 sum | deb345aea6cdb82ca4636c0811c292df |

|  |  |
| --- | --- |
| Investigation ID | A-07-SNOW-BMP |
| File name | snow.bmp |
| File Type | PC bitmap, Windows 3.x format, 448 x 336 x 24 |
| File Size | 451783 Bytes |
| sha1 sum | bfd05d8024239429140482813aea6760a66ea921 |
| md5 sum | a6e56c4d34d9a541b622b74c954c3fc9 |

|  |  |
| --- | --- |
| Investigation ID | A-08-WURSTEN-PNG |
| File name | wursten.png |
| File Type | PNG image data, 640 x 484, 8-bit/color RGBA, non-interlaced |
| File Size | 614191 Bytes |
| sha1 sum | 0132d58419ecf143e67763d9bb0fc931437956ea |
| md5 sum | 13c85b20b6b1e481a32700f26818333e |

# Evidence to look for

Given the goal for this investigation, we started to look for files related to DroneX, or that reveal activity that might be related to moling. We tried to find word documents, images, pdfs, text files, cad files related to drones. We also looked for emails or other textual content that could be related to moling.

# Examination details

We began our analysis by creating a read only filesystem with the artifacts for analysis. We then proceeded to look for evidences on all the files.

We begun by running “file” on all the files to obtain their extensions and running file carvers on all the files (namely binwalk and foremost). This sole analysis indicated that at the end of file snow.bmp (IID[[1]](#footnote-1) A-07-SNOW-BMP) there were extra bits not used for the image representation, that contained a text file. We extracted that to snow.txt (IID E-01-SNOW-TXT).

The file snow.txt contains a message in German which translates to “I will send you five files: Drone A plan, Drone B plan, technical specifications, passwords for DroneX data servers”

The file compress.py contained python bytecode (a programming language). We proceeded to decompress it using uncompyle6, a tool to decompile python bytecode (recover the original python source code). We recovered the file compress.dec.py.

After analyzing the code of compress.dec.py, we concluded that it is a LSB steganography tool, this is, it is a tool that hides files on the least significant bits of image files. The script used a low entropy password (13 possible passwords). We proceeded to create a tool that would tests all the possible passwords on the image files (decompress.py). We ran this tool on all the image files for all the passwords. We were able to extract the artifacts: oktoberfest.png.0.extracted.png (IID E-04-OKTOBERFESTEXT0-PNG), street.png.0.extracted.png (IID A-12-STREETEXT0-PNG), wursten.png.0.extracted.txt (IID E-05-WURSTENEXT0-TXT) . By analyzing their content, we concluded that oktoberfest.png.0.extracted.png, street.png.0.extracted.png were image files, and wursten.png.0.extracted.txt was a text file. We reran the tool on the extracted images and were able to recover street.png.0.extracted.0.extracted.txt (IID E-03-STREETEXT0EXT0-TXT), which is a text file.

The file oktoberfest.png.0.extracted.png was an image of quadcopter schematics.

The file street.png.0.extracted.png was an image of a castle, and contained inside the LSB’s the file street.png.0.extracted.0.extracted.txt

The file wursten.png.0.extracted.txt was a text file that contained access passwords for droneX server files.

The file street.png.0.extracted.0.extracted.txt was a text file that contained operating specifications for drones (named drone A, and drone B).

We also found a zip file (IID A-03-ONLINE-BANKING-ZIP) that was password protected. We decided to make a brute force attack on this file in order to retrieve the password, using a word list with 2465 elements generated by artifact A-02-MUNICH-TXT. Then we used a tool called *John The Ripper* and performed the attack using the generated dictionary. The tool printed out the word “Stadelheim”, as a possible password for this file. Finally, we opened file A-03-ONLINE-BANKING-ZIP using the password “Stadelheim” and successfully retrieved 2 files inside:

1. A Microsoft Word document labeled as online\_banking.docx (IID A-10-ONLINE-BANKING-DOCX), displaying a password inside. We could not reach any conclusive thoughts on this file.
2. A binary file without any recognizable header labeled as drone-A.bmp (IID A-11-DRONE-A-BMP). We analyzed this file with an editor called 010 Editor, where we could analyze the binary content. In this tool we saw this file had multiple PNG Section Headers. Also, those visible section headers were correct considering that each CRC presented at the final of each header were well calculated.

This made us believe that this file corresponded to a valid PNG file. In order to discover its content, we used the same editor and changed the first 4 Bytes, to the first 4 Bytes of a valid PNG file. Finally, we changed the extension of the original file to “.png” and opened the file. Now we could display the content of this image, that showed the schematics of a drone (IID E-02-DRONE-A-PNG).

On the remaining file (cathedral.png) we could not find any relevant information for this investigation.

The presented list constitutes all the new artifacts/evidences discovered during the investigation.

|  |  |
| --- | --- |
| Investigation ID | E-01-SNOW-TXT |
| File name | snow.txt |
| File Type | UTF-8 Unicode text |
| File Size | 145 Bytes |
| sha1 sum | 63515f910ad88b76950384fea470e5e3ccc3a38a |
| md5 sum | f8105917067d26e022ff6e657f6cd9d8 |

|  |  |
| --- | --- |
| Investigation ID | A-09-COMPRESS-PY |
| File name | compress.dec.py |
| File Type | Python source code file, version 2.7 |
| File Size | 2774 Bytes |
| sha1 sum | bf83e126c0166bce3d0526e0dfa0a74f5960f60f |
| md5 sum | 74ead8bf19e3f12f131666fe3752b67e |

|  |  |
| --- | --- |
| Investigation ID | A-10-ONLINE-BANKING-DOCX |
| File name | online\_banking.docx |
| File Type | PNG image data, 945 x 630, 8-bit/color RGBA, non-interlaced |
| File Size | 1264820 Bytes |
| sha1 sum | 8cf635ceba0334d0a1c018df676ad03fa06d817b |
| md5 sum | b70702822417bd39a7997a0f8c73941f |

|  |  |
| --- | --- |
| Investigation ID | A-11-DRONE-A-BMP |
| File name | drone-A.bmp |
| File Type | data |
| File Size | 92401 Bytes |
| sha1 sum | eda36e36322dd47a76bf42041dceae8be79f3652 |
| md5 sum | 05029f0ae6af62ca3350f5b094584b22 |

|  |  |
| --- | --- |
| Investigation ID | E-02-DRONE-A-PNG |
| File name | drone-A.png |
| File Type | PNG image data, 600 x 326, 8-bit/color RGB, non-interlaced |
| File Size | 92401 Bytes |
| sha1 sum | 14099f30e4b2c894cff20a3fa498808f66e31780 |
| md5 sum | d99f500968d444b5e0a1c9fd1dd69274 |

|  |  |
| --- | --- |
| Investigation ID | A-12-STREETEXT0-PNG |
| File name | street.png.0.extracted.png |
| File Type | PNG image data, 350 x 263, 8-bit/color RGBA, non-interlaced |
| File Size | 169868 Bytes |
| sha1 sum | 1b5d516a7a65da889a83c01adae7ea24d5955ac3 |
| md5 sum | d770b66b4f5833b0be194362f440e494 |

|  |  |
| --- | --- |
| Investigation ID | E-03-STREETEXT0EXT0-TXT |
| File name | street.png.0.extracted.0.extracted.txt |
| File Type | UTF-8 Unicode text |
| File Size | 1139 Bytes |
| sha1 sum | e0d5c932d2a7c13338d3cbb7ec5618066ca5a13c |
| md5 sum | 7c241b5af909484f2004359ed697e9a68abf186f |

|  |  |
| --- | --- |
| Investigation ID | E-04-OKTOBERFESTEXT0-PNG |
| File name | oktoberfest.png.0.extracted.png |
| File Type | PNG image data, 343 x 376, 8-bit/color RGBA, non-interlaced |
| File Size | 106674 Bytes |
| sha1 sum | 01ab4e16ed2b7b15c47aafc9b6a168a527a2218a |
| md5 sum | cbe4c039f3fa2b312bb95a0964ffba4d |

|  |  |
| --- | --- |
| Investigation ID | E-05-WURSTENEXT0-TXT |
| File name | wursten.png.0.extracted.txt |
| File Type | ASCII text |
| File Size | 80 Bytes |
| sha1 sum | 7c241b5af909484f2004359ed697e9a68abf186f |
| md5 sum | 3cb3f3162e4cf990168d904d3bb300b9 |

# Analysis results

We believe that someone intentionally hid information regarding drones on the files we found on this investigation by using the artifact A-05-COMPRESS-PY, which we decompiled as artifact A-09-COMPRESS-PY, with the intention of sending this files to someone else. Namely, there is a text message in German hidden at the end of the artifact A-07-SNOW-BMP, saying that files are going to be sent (evidence E-01-SNOW-TXT), and we were able to recover files related to the ones described on the text messages. This files have drone schematics for drone A and drone B (evidence E-02-DRONE-A-PNG and evidence E-04-OKTOBERFESTEXT0-PNG), specifications for drone A and B (evidence E-03-STREETEXT0EXT0-TXT), and access passwords for a droneX server (evidence E-05-WURSTENEXT0-TXT).

One of the files extracted from artifact A-03-ONLINE-BANKING-ZIP was A-10-ONLINE-BANKING-DOCX. We can’t make any conclusions regarding the content of this file as it only contains a possible password for something. Further investigation will be necessary, or it might be useful with other evidences.

# Conclusions

After this investigation we conclude that someone hid information on the files we were given related to drone A, drone B and droneX servers, and had an intention to send that information to someone else.

Instituto Superior Técnico, 26 October 2018

The Investigation Team

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Daniel Chaves | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Afonso Santos | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Manuel Sousa |

1. IID is an abbreviation of Investigation Identifier [↑](#footnote-ref-1)