# ICT378 Final Assignment

Christopher Cigana (33605148)

ICT378 Cyber Forensics & Information Technology

Dr Fatemeh Rezaeibagha

Submission Date: 24 MAY 2021

Word count: 4500

## Table of Contents

Contents

## 1.1 Executive Summary

A police investigation has been initiated against Jo, a m57.biz employee. Enough evidence has been collected by Police investigators so far to warrant and search and seizure of M57 computer systems to conduct digital forensic analysis to further the investigation. It is suspected that Jo has been, or is currently, involved in illicit drug activity, namely methamphetamines.

Police were approached by Aaron Greene, who purchased a computer originally owned by a patent research company, m57.biz. Mr. Greene reported that there were documents and videos related to methamphetamine use on the computer, which Police established to have been used by m57.biz employee, Jo, before being sold as-is to Mr. Greene. Police made a disk image of the suspect computer have provided it to us to conduct our digital forensic investigation.

Our task is to conduct an extensive forensic investigation on several pieces of data that have been obtained by police investigators. This data will be processed and analysed to locate further evidence of possible methamphetamine activity. A sanitized workstation will be used to conduct the investigation, to eliminate any risk of outside interference. All data files will be hashed to ensure their integrity over the course of the investigation and all analysis will be conducted with reputable digital forensic software tools and techniques.

Once our analysis and examination of the digital data has been completed, we will summarise our investigation into key findings that will guide police investigators in the next course of action. These key findings will be clear, factual, and reinforced by evidence collected from the investigation.

### 1.2 Investigation Methodology:

1. Examine the scenario and determine the requirements of the Investigation. Define and illustrate the requirements into an Executive Summary which will summarise the investigation and the steps to be taken.
2. Acquire and inventory all drive images that will be used as evidence in the investigation. This includes producing a hash value for all evidence drives, which will be used to ensure the integrity of the evidence during the investigation.
3. Document the process that was taken to acquire the evidence, allowing other parties to repeat and validate the process. Detail the tools used and how they were utilized.
    a. Examine contents of all data files in all folders.
    b. Recover file contents for all password-protected files.
    c. Identify the function of every executable file that doesn’t match hash values.

   d. Outline any instances where the different tools produced different results and discuss why this might have occurred.
   e. Ensure the integrity of all evidence and findings.
4. Screenshot certain parts of the investigation and pieces of evidence that may be of significance to the investigation.
5. Also screenshot any circumstances that are used to hypothesise or infer any opinions relating to the investigation.

## 1.3 Materials Used to Conduct Investigation & Preservation Methodology:

- Inventory of captured harddrive images:
  - Hard drive image ‘2009-11-19.E01’ (of the original sold computer) – **E01**
    - [CB76EBFB75B4736621C41BFC29770BEEF618D771EA36AA5510F60B48C0148417]
  - Second drive image purporting to be of the same computer – **AD1, AD2**
    - AD1 [F9EB80B049141F235A0281A045C5DBBAD43119FCDC692E2218E264BBAA9EF3D7]
    - AD2 [0AD3EDA65B8EF4E5DC8AC74D7002694EB6755CA782DA9B1E7C8E131525BAEA4]
  - Hard drive image ‘2009-12-01.E01’ (of the suspects replacement computer seized from M57) – **E01**
    - [4DD3C5B465431389F95105D73A0A394FF52FB4F9CD10CF9C79F9D961890DEF52]
  - Second drive image purporting to of the same computer – **AD1, AD2, AD3**
    - AD1 [2606C23DCFA624D24D79D02E175448D695B493C4ED50B3142798F1C43656D40D]
    - AD2 [9D6204B503AF814AF4AF573DB44CAF7243CFE2BB2714C37A3CC8A9C5EC09AE63]
    - AD3 [FE9B27119982B009A178D7FE65004B22CB580FEE97495D0326734BBBDD828934]

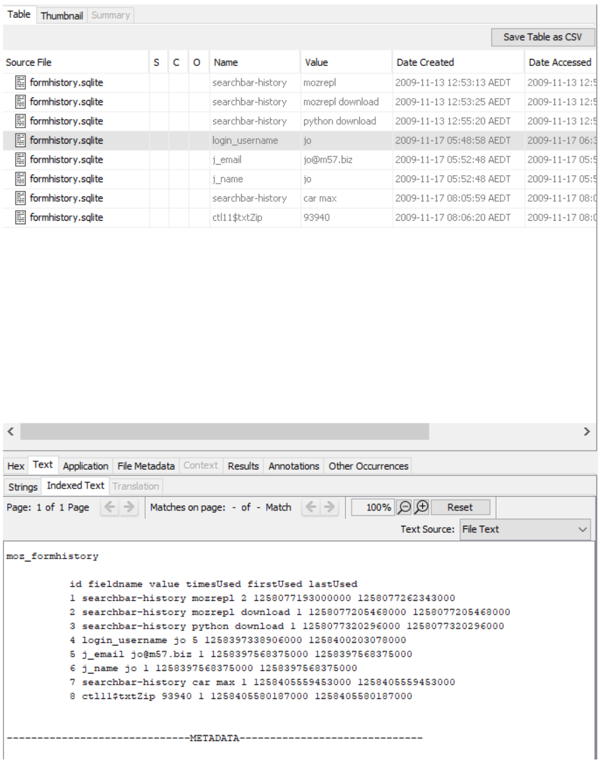
- A sanitized and correctly setup workspace that facilitates the maintaining of the integrity of the investigation.
    - This workspace will use both Windows O/S and Kali Linux O/S, contained within Virtual Machines, to conduct the investigation.
- An assortment of software that enables us to correctly and efficiently process and analyse all available data files. Full details provided in Appendix 5.5.
    - OSForensics; Autopsy; FTK Imager etc
    - 7-Zip- used to produce hash images of the data, and periodically throughout to ensure integrity.
        - Hash values use the 'SHA256' hashing algorithm for maximum integrity and are listed after each file description above.

## 2.1 Investigation Methodology

### 2.1.1 Autopsy

- For the purposes of our investigation, each piece of data we have received for anaylsis will be organised as a separate case. This ensures data integrity with hashing and allows thorough analysis on each datafile.
- The cases created in Autopsy for our investigation are as follows:
    - "jo-2009-11-19.E01"
    - "jo-2009-11-19.ad1"
    - "jo-2009-11-19.ad2"
    - "jo-2009-12-01.E01"
    - "jo-2009-12-01.ad1"
    - "jo-2009-12-01.ad2"
    - "jo-2009-12-01.ad3"
- Once processed, Autopsy highlights and compartmentalises information. This data is from a number of different areas, and if displayed in a heirarchial tree format.
- We can also see if the processed data has any significant relevance to the investigation- such as a field named "Web Form Autofill" which has several files related to the targets username and email in the m57 system. If a need arises, with proper authorisation and a warrant, to break into certain areas of the target's M57 files, we can use the below to perform some digital reconnaissance and penetration testing into m57.biz's information systems.

*2.1.1.1*

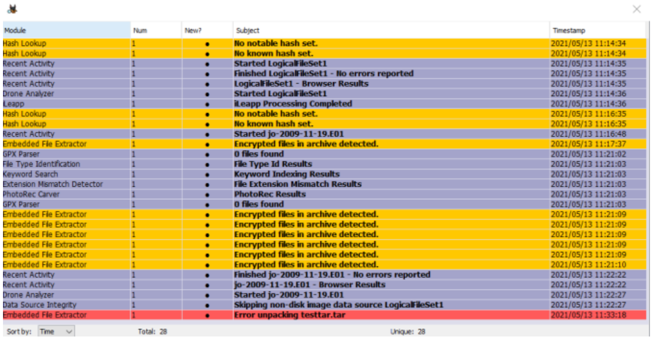


| Source File | S | C | O | Name | Value | Date Created | Date Accessed |
|---|---|---|---|---|---|---|---|
| formhistory.sqlite | | | | searchbar-history | mozrepl | 2009-11-13 12:53:13 AEDT | 2009-11-13 12:5 |
| formhistory.sqlite | | | | searchbar-history | mozrepl download | 2009-11-13 12:53:25 AEDT | 2009-11-13 12:5 |
| formhistory.sqlite | | | | searchbar-history | python download | 2009-11-13 12:55:20 AEDT | 2009-11-13 12:5 |
| formhistory.sqlite | | | | login_username | jo | 2009-11-17 05:48:58 AEDT | 2009-11-17 06:3 |
| formhistory.sqlite | | | | j_email | jo@m57.biz | 2009-11-17 05:52:48 AEDT | 2009-11-17 05:5 |
| formhistory.sqlite | | | | j_name | jo | 2009-11-17 05:52:48 AEDT | 2009-11-17 05:5 |
| formhistory.sqlite | | | | searchbar-history | car max | 2009-11-17 08:05:59 AEDT | 2009-11-17 08:0 |
| formhistory.sqlite | | | | ctl11$txtZip | 93940 | 2009-11-17 08:06:20 AEDT | 2009-11-17 08:0 |

```
moz_formhistory

          id fieldname value timesUsed firstUsed lastUsed
          1 searchbar-history mozrepl 2 1258077193000000 1258077262343000
          2 searchbar-history mozrepl download 1 1258077205468000 1258077205468000
          3 searchbar-history python download 1 1258077320296000 1258077320296000
          4 login_username jo 5 1258397338906000 1258400203078000
          5 j_email jo@m57.biz 1 1258397568375000 1258397568375000
          6 j_name jo 1 1258397568375000 1258397568375000
          7 searchbar-history car max 1 1258405559453000 1258405559453000
          8 ctl11$txtZip 93940 1 1258405580187000 1258405580187000


------------------------------METADATA------------------------------
```

- Several alerts have been raised from the processed data [2.1.1.2]. These alerts state that there is a number of encrypted files that cannot be accessed, which may indicate illicit activities and warrants further examination.

*2.1.1.2*



| Module | Num | New? | Subject | Timestamp |
|---|---|---|---|---|
| Hash Lookup | 1 | ● | No notable hash set. | 2021/05/13 11:14:34 |
| Hash Lookup | 1 | ● | No known hash set. | 2021/05/13 11:14:34 |
| Recent Activity | 1 | ● | Started LogicalFileSet1 | 2021/05/13 11:14:35 |
| Recent Activity | 1 | ● | Finished LogicalFileSet1 - No errors reported | 2021/05/13 11:14:35 |
| Recent Activity | 1 | ● | LogicalFileSet1 - Browser Results | 2021/05/13 11:14:35 |
| Drone Analyzer | 1 | ● | Started LogicalFileSet1 | 2021/05/13 11:14:36 |
| iLeapp | 1 | ● | iLeapp Processing Completed | 2021/05/13 11:14:36 |
| Hash Lookup | 1 | ● | No notable hash set. | 2021/05/13 11:16:35 |
| Hash Lookup | 1 | ● | No known hash set. | 2021/05/13 11:16:35 |
| Recent Activity | 1 | ● | Started jo-2009-11-19.E01 | 2021/05/13 11:16:48 |
| Embedded File Extractor | 1 | ● | Encrypted files in archive detected. | 2021/05/13 11:17:37 |
| GPX Parser | 1 | ● | 0 files found | 2021/05/13 11:21:02 |
| File Type Identification | 1 | ● | File Type Id Results | 2021/05/13 11:21:03 |
| Keyword Search | 1 | ● | Keyword Indexing Results | 2021/05/13 11:21:03 |
| Extension Mismatch Detector | 1 | ● | File Extension Mismatch Results | 2021/05/13 11:21:03 |
| PhotoRec Carver | 1 | ● | PhotoRec Results | 2021/05/13 11:21:03 |
| GPX Parser | 1 | ● | 0 files found | 2021/05/13 11:21:03 |
| Embedded File Extractor | 1 | ● | Encrypted files in archive detected. | 2021/05/13 11:21:09 |
| Embedded File Extractor | 1 | ● | Encrypted files in archive detected. | 2021/05/13 11:21:09 |
| Embedded File Extractor | 1 | ● | Encrypted files in archive detected. | 2021/05/13 11:21:09 |
| Embedded File Extractor | 1 | ● | Encrypted files in archive detected. | 2021/05/13 11:21:09 |
| Embedded File Extractor | 1 | ● | Encrypted files in archive detected. | 2021/05/13 11:21:09 |
| Embedded File Extractor | 1 | ● | Encrypted files in archive detected. | 2021/05/13 11:21:10 |
| Recent Activity | 1 | ● | Finished jo-2009-11-19.E01 - No errors reported | 2021/05/13 11:22:22 |
| Recent Activity | 1 | ● | jo-2009-11-19.E01 - Browser Results | 2021/05/13 11:22:22 |
| Drone Analyzer | 1 | ● | Started jo-2009-11-19.E01 | 2021/05/13 11:22:27 |
| Data Source Integrity | 1 | ● | Skipping non-disk image data source LogicalFileSet1 | 2021/05/13 11:22:27 |
| Embedded File Extractor | 1 | ● | Error unpacking testtar.tar | 2021/05/13 11:33:18 |

Total: 28　Unique: 28

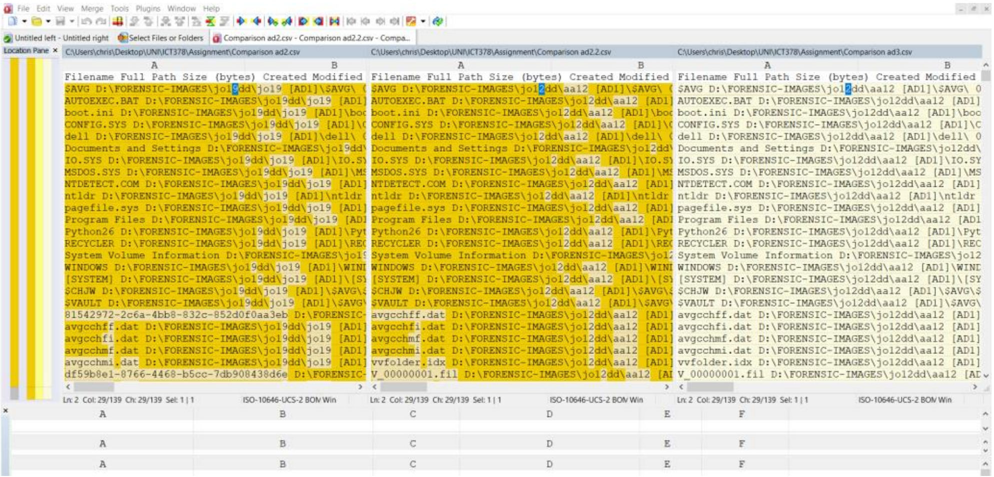
- The software has identified certain files as being suspect, namely the ‘User Content Suspected’ file tree, which has flagged images as having “EXIF metadata exists for this file”.
  - These images have been tagged (“EXIF metadata file”) for followup.
  - Based on the description provided by the software, these files may be a likely candidate to examine for use of steganography.
- Using the “Keyword Search” functionality of Autopsy allows us to define and narrow-down the recovered and processed data to determine if there is any evidence available for analysis.
- Below is the list of keywords that have been used to analyse the recovered data.

  - “Cash, drugs, methamphetamines, illicit, drug production, drug transportation, illegal, high quality, hidden.”
- Based on certain results found, we can expand our list of keywords to discover new information and expand the scope of the investigation. These new keywords include:
  - “Jordan Stanford, js9999sj@yahoo.com, test.bmp, JAR, .jar, wbk73.tmp, ‘fancybox’, ‘AnythingSlider’, (more…)”
- The new keyword searches have produced additional information that relates to illicit activity on Jo’s machine and will be expanded in the findings section. However, we will discuss the new investigation avenues here as they pertain to methodology.
- The link to Jordan Stanford from Jo’s machine has produced an email address which can be used to provide information relating to this investigation.
  - From a digital forensics persepective, we would use Jordan’s details to perform some open source intelligence (OSINT). This may link Jordan to illicit activities and this investigation. This is outside the scope of our investigation.

### 2.1.2 WinMerge

- WinMerge has been used to conduct a comparison between the different .ad files to compare them for integrity. WInMerge will confirm if the two images are the same- or if it has detected differences.
- Winmerge uses the exported files from software such as FTK Imager for its comparison.
  - “jo-2009-11-19.ad1” and “jo-2009-12-01.ad1” = files are indetical
  - “jo-2009-11-19.ad2” and “jo-2009-12-01.ad2” = difference were detected.
    - This means the program has detected a difference between the 3 12-01.ad files. This could indicate potential data tampering, a corruption has occurred during the data collection by the original investigators, or potentially the data may have been collected at different points.

### 2.1.2.1


File Edit View Merge Tools Plugins Window Help
Untitled left - Untitled right
Select Files or Folders
Comparison ad2.csv - Comparison ad2.2.csv - Compa...
Location Pane

```
C:\Users\chris\Desktop\UNI\ICT378\Assignment\Comparison ad2.csv
                    A                                   B
Filename Full Path Size (bytes) Created Modified
$AVG D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\$AVG\ (
AUTOEXEC.BAT D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]
boot.ini D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\boo
CONFIG.SYS D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\C
dell D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\dell\ (
Documents and Settings D:\FORENSIC-IMAGES\jo19dd\
IO.SYS D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\IO.SY
MSDOS.SYS D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\MS
NTDETECT.COM D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]
ntldr D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\ntldr
pagefile.sys D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]
Program Files D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1
Python26 D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\Pyt
RECYCLER D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\REC
System Volume Information D:\FORENSIC-IMAGES\jo19
WINDOWS D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\WIND
[SYSTEM] D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\[SY
$CHJW D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\$AVG\$
$VAULT D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]\$AVG\
81542972-2c6a-4bb8-832c-852d0f0aa3eb D:\FORENSIC-
avgcchff.dat D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]
avgcchfi.dat D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]
avgcchmf.dat D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]
avgcchmi.dat D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]
df59b8e1-8766-4468-b5cc-7db908438d6e D:\FORENSIC-
Ln: 2  Col: 29/139  Ch: 29/139  Sel: 1 | 1       ISO-10646-UCS-2 BOM Win
```

```
C:\Users\chris\Desktop\UNI\ICT378\Assignment\Comparison ad2.2.csv
                    A                                   B
Filename Full Path Size (bytes) Created Modified
$AVG D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\$AVG\ (
AUTOEXEC.BAT D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
boot.ini D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\boo
CONFIG.SYS D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\C
dell D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\dell\ (
Documents and Settings D:\FORENSIC-IMAGES\jo12dd\
IO.SYS D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\IO.SY
MSDOS.SYS D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\MS
NTDETECT.COM D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
ntldr D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\ntldr
pagefile.sys D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
Program Files D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1
Python26 D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\Pyt
RECYCLER D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\REC
System Volume Information D:\FORENSIC-IMAGES\jo12
WINDOWS D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\WIND
[SYSTEM] D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\[SY
$CHJW D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\$AVG\$
$VAULT D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\$AVG\
avgcchff.dat D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
avgcchfi.dat D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
avgcchmf.dat D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
avgcchmi.dat D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
vvfolder.idx D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
V_00000001.fil D:\FORENSIC-IMAGES\jo12dd\aa12 [AD
Ln: 2  Col: 29/139  Ch: 29/139  Sel: 1 | 1       ISO-10646-UCS-2 BOM Win
```

```
C:\Users\chris\Desktop\UNI\ICT378\Assignment\Comparison ad3.csv
                    A                                   B
Filename Full Path Size (bytes) Created Modified
$AVG D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\$AVG\ 0
AUTOEXEC.BAT D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
boot.ini D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\boo
CONFIG.SYS D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\C
dell D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\dell\ 0
Documents and Settings D:\FORENSIC-IMAGES\jo12dd\
IO.SYS D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\IO.SY
MSDOS.SYS D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\MS
NTDETECT.COM D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
ntldr D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\ntldr
pagefile.sys D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
Program Files D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1
Python26 D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\Pyt
RECYCLER D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\REC
System Volume Information D:\FORENSIC-IMAGES\jo12
WINDOWS D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\WIND
[SYSTEM] D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\[SY
$CHJW D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\$AVG\$
$VAULT D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]\$AVG\
avgcchff.dat D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
avgcchfi.dat D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
avgcchmf.dat D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
avgcchmi.dat D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
vvfolder.idx D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
V_00000001.fil D:\FORENSIC-IMAGES\jo12dd\aa12 [AD
Ln: 2  Col: 29/139  Ch: 29/139  Sel: 1 | 1       ISO-10646-UCS-2 BOM Win
```

- What this could mean to the investigation is that the evidence taken from these portions of the data recovered could possibly be considered suspect, as we cannot ensure their integrity. This could become more relevant if the investigation proceeds to a criminal court case.

### 2.1.3 AccessFTK Imager

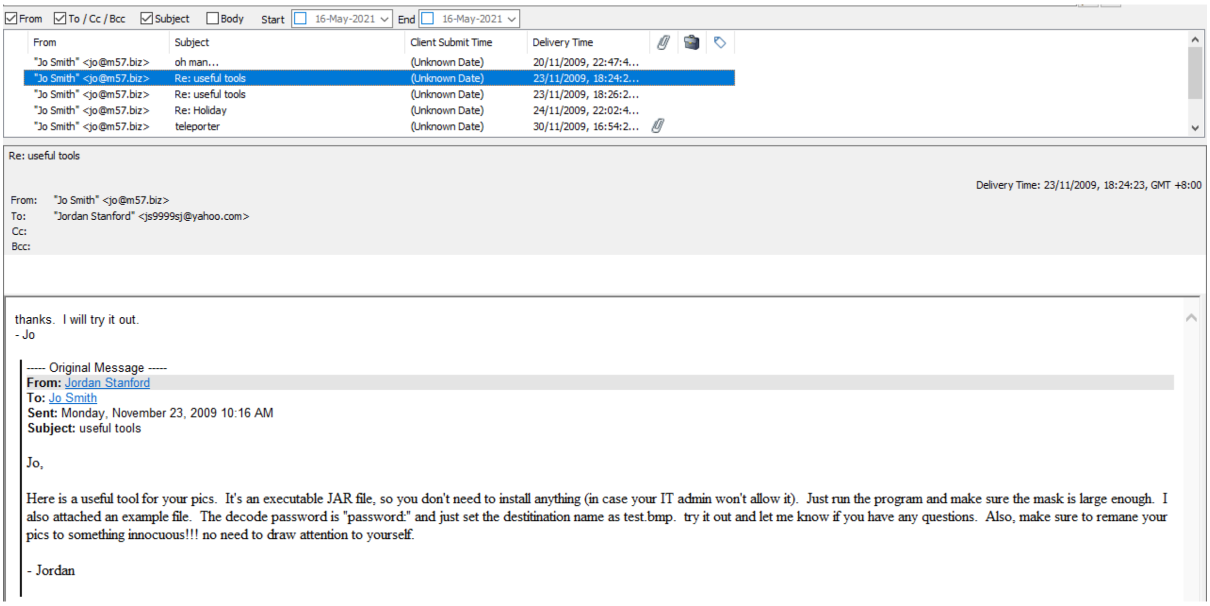
- AccessFTK Imager has been used for this investigation to add additional value and depth to the data analysis, with more software to process data we may find more avenues of information. The same aplies to OSForensics and ProDiscover used below.
- Once we have uploaded all the target images into the software, we can begin to anaylse the data and conduct our investigation. FTKImager allows us to examine the full file tree. Looking for folders with suspicious names or single letters in locations outside user data can indicate that the file does not belong to the native O/S.
- We have discovered that ‘jo-2019-11-19.ad1’ has file pathways that are not consistent with regular Windows naming conventions which contains large amounts of relevant materials to our investigation.
- Two key pieces of information from this evidence have been identified.
    - A HTML webpage containing information about methamphetamines from an organisation name EMCDDA (European Monitoring Center for Drugs and Drug Addiction), based in Lisbon, Portugal. The subdirectory contains pdf’s and files about drug rehabilitation and law enforcement.
- We then perform the same procedure on ‘jo-2009-12-01.ad1’ as above. It produces evidence in the \dell\drivers subdirectory that contains several video files with suspicious filenames that are relevant to our investigation:
    - “Benzaldehyde from Bitter Almond Oil”, “Fractional Distillation of Vimto to Obtain Touluene” and “Organic Chemistry Explained”.

- Another piece of relevant evidence that relates to the investigation can be found in \Documents and Settings\Jo\Local Settings\Temporary Internet Files. The file is called "Where can I find a good methamphetamine recipe_ -Quora_files"

### 2.1.4 OSForensics:

- OSForensics is being used to utilize a range of forensics software to ensure result integrity. The same applies to ProDiscover below.
- We create a new case in OSForensics called 'jo-2009-11-19.e01' and add the correct device to our case. The same steps were completed for 'jo-2009-12-01.e01'.
- The drives appear to be from a Windows XP computer.
- We created indexes of the suspect drives in each case. This information can be used in order to determine differences between the two suspect drive files. Both 'jo-2009-11-19.e01' and 'jo-2009-12-01.e01' indexed 2503 files.
- By opening the drive, we can see the contents in the File System Browser. A file search was conducted using the following terms:
    - "meth*, drugs, speed, cash"
- In both 'jo-2009-11-19.e01' and 'jo-2009-12-01.e01' these search terms did not return any results of note, other than a small group of system files which appear legitimate.
- Using the presets search filters we ran searches for all Image files, video files, office documents, and email files. These searches did not return any relevant results. From further examination of the 'jo-2009-11-19.e01' file structure we are not able to locate anything suspicious. The files which were present in FTKImager are also not visible in the file locations. This may be as a result of OSForensics processing E01 files, rather than the AD1 files used by FTKImager.
- As above the contents of the file structure 'jo-2009-12-01.e01' was inspected using the same filters as with 'jo-2009-11-19.e01'. We were able to determine that several image files had been moved and given inconspicuous names, which would indicate there is something to hide. This shall be discussed in the findings.
- Through the file search function, email files including Jo's inbox and sent items folders were discovered. Most of the emails appear to be work related and unrelated to this investigation. There were, however, several emails of a suspicious nature from a person named Jordan Stanford [2.1.4.1] and [2.1.4.2]. These emails provide Jo with information on how to hide information on a computer, as well as a copy of Java Invisible Ink Toolkit (which is steganography software). The email also provides information on the default password for steganographic encryption: "password". These emails are relevant to our investigation.

### 2.1.4.1



☑ From ☑ To / Cc / Bcc ☑ Subject □ Body Start □ 16-May-2021 End □ 16-May-2021

| From | Subject | Client Submit Time | Delivery Time |
|---|---|---|---|
| "Jo Smith" <jo@m57.biz> | oh man… | (Unknown Date) | 20/11/2009, 22:47:4… |
| "Jo Smith" <jo@m57.biz> | Re: useful tools | (Unknown Date) | 23/11/2009, 18:24:2… |
| "Jo Smith" <jo@m57.biz> | Re: useful tools | (Unknown Date) | 23/11/2009, 18:26:2… |
| "Jo Smith" <jo@m57.biz> | Re: Holiday | (Unknown Date) | 24/11/2009, 22:02:4… |
| "Jo Smith" <jo@m57.biz> | teleporter | (Unknown Date) | 30/11/2009, 16:54:2… |

Re: useful tools

Delivery Time: 23/11/2009, 18:24:23, GMT +8:00

From: "Jo Smith" <jo@m57.biz>
To: "Jordan Stanford" <js9999sj@yahoo.com>
Cc:
Bcc:

thanks. I will try it out.
- Jo

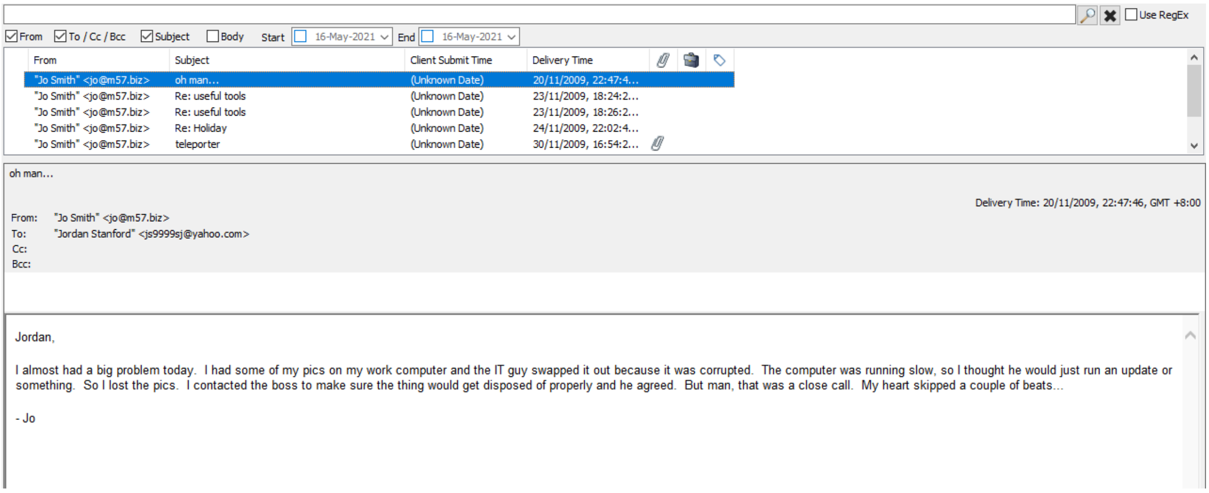
----- Original Message -----
**From:** Jordan Stanford
**To:** Jo Smith
**Sent:** Monday, November 23, 2009 10:16 AM
**Subject:** useful tools

Jo,

Here is a useful tool for your pics. It's an executable JAR file, so you don't need to install anything (in case your IT admin won't allow it). Just run the program and make sure the mask is large enough. I also attached an example file. The decode password is "password:" and just set the destitination name as test.bmp. try it out and let me know if you have any questions. Also, make sure to remane your pics to something innocuous!!! no need to draw attention to yourself.

- Jordan

### 2.1.4.2



□ Use RegEx

☑ From ☑ To / Cc / Bcc ☑ Subject □ Body Start □ 16-May-2021 End □ 16-May-2021

| From | Subject | Client Submit Time | Delivery Time |
|---|---|---|---|
| "Jo Smith" <jo@m57.biz> | oh man… | (Unknown Date) | 20/11/2009, 22:47:4… |
| "Jo Smith" <jo@m57.biz> | Re: useful tools | (Unknown Date) | 23/11/2009, 18:24:2… |
| "Jo Smith" <jo@m57.biz> | Re: useful tools | (Unknown Date) | 23/11/2009, 18:26:2… |
| "Jo Smith" <jo@m57.biz> | Re: Holiday | (Unknown Date) | 24/11/2009, 22:02:4… |
| "Jo Smith" <jo@m57.biz> | teleporter | (Unknown Date) | 30/11/2009, 16:54:2… |

oh man…

Delivery Time: 20/11/2009, 22:47:46, GMT +8:00

From: "Jo Smith" <jo@m57.biz>
To: "Jordan Stanford" <js9999sj@yahoo.com>
Cc:
Bcc:

Jordan,

I almost had a big problem today. I had some of my pics on my work computer and the IT guy swapped it out because it was corrupted. The computer was running slow, so I thought he would just run an update or something. So I lost the pics. I contacted the boss to make sure the thing would get disposed of properly and he agreed. But man, that was a close call. My heart skipped a couple of beats…

- Jo

- Within ‘jo-2009-12-01.e01’ in \Documents and Settings\Jo\Desktop\Pics there is a .jar file. This file type can be used to store data inconspicuously. By opening this file using Java, the contents of that folder became visible. The folder contains Java Invisible Ink Toolkit software, and the associated software files. This software is typically used for steganography and would indicate that there may be images on the suspect drive using steganography. This is relevant information to our investigation.

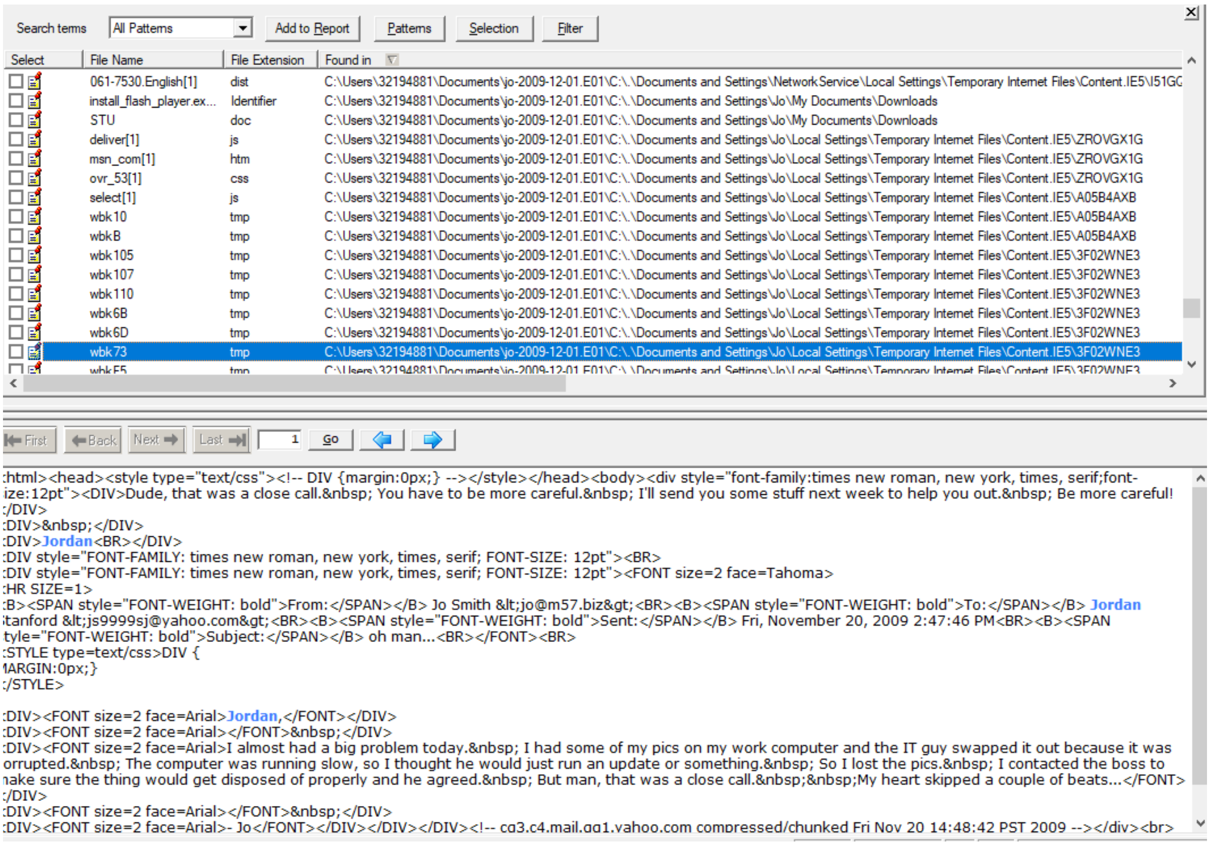
## 2.1.5 ProDiscover:

- As mentioned above, ProDiscover is being used to ensure evidence integrity. Cases are created in ProDiscover for the suspect material. These two cases are ‘jo-2009-11-19.e01’ and ‘jo-2009-12-01.e01’.
- A search is conducted in each case using a variety of terms, listed as follows:

- “meth*, speed, cash, drugs, Jordan, *.jar and illegal”

- The search did not provide any suspicious information. Some emails between Jordan and Jo were discovered. These emails are the same as previously discovered using other forensics software. They are deemed relevant to our investigation.
- Manually searching through ‘jo-2009-11-19.e01’ did not locate any suspicious or relevant data.
- The same process was conducted on ‘jo-2009-12-01.e01’. Manually navigating through the file structure located a folder able to locate \Documents and Settings\Jo\Desktop\Pics\Hidden\ which contains photos with inconspicuous names, such as ‘patent01’, however when opening the photos they appear to be images of a personal nature, as they are photos of a cat. As the images have been moved and hidden it would suggest image tampering, and therefore these images are considered relevant to our investigation.
- A keyword search using the above keywords has been conducted, which provides more results. The search for the name Jordan returned several emails and temp email files which indicated that there is something that Jo wishes to have hidden on the machine [2.1.5.1]. Searching for the terms methamphetamine, drugs, party, illegal, and *.jar did not return any results of a suspicious nature.

2.1.5.1



| Select | File Name | File Extension | Found in |
|---|---|---|---|
| □ | 061-7530.English[1] | dist | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\NetworkService\Local Settings\Temporary Internet Files\Content.IE5\I51GC |
| □ | install_flash_player.ex... | Identifier | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\My Documents\Downloads |
| □ | STU | doc | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\My Documents\Downloads |
| □ | deliver[1] | js | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\ZROVGX1G |
| □ | msn_com[1] | htm | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\ZROVGX1G |
| □ | ovr_53[1] | css | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\ZROVGX1G |
| □ | select[1] | js | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\A05B4AXB |
| □ | wbk10 | tmp | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\A05B4AXB |
| □ | wbkB | tmp | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\A05B4AXB |
| □ | wbk105 | tmp | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\3F02WNE3 |
| □ | wbk107 | tmp | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\3F02WNE3 |
| □ | wbk110 | tmp | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\3F02WNE3 |
| □ | wbk6B | tmp | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\3F02WNE3 |
| □ | wbk6D | tmp | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\3F02WNE3 |
| □ | wbk73 | tmp | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\3F02WNE3 |
| □ | wbkE5 | tmp | C:\Users\32194881\Documents\jo-2009-12-01.E01\C:\.\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\3F02WNE3 |

```
:html><head><style type="text/css"><!-- DIV {margin:0px;} --></style></head><body><div style="font-family:times new roman, new york, times, serif;font-
ize:12pt"><DIV>Dude, that was a close call.&nbsp; You have to be more careful.&nbsp; I'll send you some stuff next week to help you out.&nbsp; Be more careful!
:/DIV>
:DIV>&nbsp;</DIV>
:DIV>Jordan<BR></DIV>
:DIV style="FONT-FAMILY: times new roman, new york, times, serif; FONT-SIZE: 12pt"><BR>
:DIV style="FONT-FAMILY: times new roman, new york, times, serif; FONT-SIZE: 12pt"><FONT size=2 face=Tahoma>
:HR SIZE=1>
:B><SPAN style="FONT-WEIGHT: bold">From:</SPAN></B> Jo Smith &lt;jo@m57.biz&gt;<BR><B><SPAN style="FONT-WEIGHT: bold">To:</SPAN></B> Jordan
itanford &lt;js9999sj@yahoo.com&gt;<BR><B><SPAN style="FONT-WEIGHT: bold">Sent:</SPAN></B> Fri, November 20, 2009 2:47:46 PM<BR><B><SPAN
tyle="FONT-WEIGHT: bold">Subject:</SPAN></B> oh man...<BR></FONT><BR>
:STYLE type=text/css>DIV {
IARGIN:0px;}
:/STYLE>

:DIV><FONT size=2 face=Arial>Jordan,</FONT></DIV>
:DIV><FONT size=2 face=Arial></FONT>&nbsp;</DIV>
:DIV><FONT size=2 face=Arial>I almost had a big problem today.&nbsp; I had some of my pics on my work computer and the IT guy swapped it out because it was
orrupted.&nbsp; The computer was running slow, so I thought he would just run an update or something.&nbsp; So I lost the pics.&nbsp; I contacted the boss to
nake sure the thing would get disposed of properly and he agreed.&nbsp; But man, that was a close call.&nbsp;&nbsp;My heart skipped a couple of beats...</FONT>
:/DIV>
:DIV><FONT size=2 face=Arial></FONT>&nbsp;</DIV>
:DIV><FONT size=2 face=Arial>- Jo</FONT></DIV></DIV></DIV><!-- ca3.c4.mail.gq1.yahoo.com compressed/chunked Fri Nov 20 14:48:42 PST 2009 --></div><br>
```

### 2.1.6 Excel:

We have used Excel to side my side compare the hash values of the image files located in the suspect drives, primarily to examine the hash values of the image files. If the file name has changed but the image itself has not been tampered with, the hash value will remain the same. This analysis was done manually using the following steps.

- Using FTKImager we loaded the image drive files and exported the directory listing for each drive. This will create a copy of the directory in a CSV file in the chosen folder within the investigation computer.
- From there we opened the CSV files for both suspect images and compared the two. Any files which were deemed to be irrelevant where hidden within Excel for ease of viewing. This also ensured that the data was not altered. By manually comparing the hash files for the photos on the suspect drives the following information was gathered.
- The photos in 'jo-2009-11-19.ad1' and 'jo-2009-12-01.ad1' had had their names and location changed however the hash values remained the same, indicating that the images themselves had not been altered, or the images were altered in both images of the suspect drive.
- Whilst looking at the directory listings we noticed a group of suspicious file names. This information was used to return to FTKImager and investigate those files of suspicious names.
- From investigation using Excel we were able to determine that in 'jo-2009-11-19.ad1' the following folders contain suspicious data:
    - \dell\drivers\R54403\r\esea\r
    - \documents and settings\administrator\my documents\my pictures
    - \documents and settings\all users\documents\my videos
    - \documents and settings\jo\my documents\downloads
- Within 'jo-2009-12-01.ad1' the suspicious items are in the following locations:
    - \documents and settings\default user\desktop
    - \documents and settings\administrator\my documents\purchase
    - \documents and settings\administrator\my documents\my pictures
    - \dell\drivers\r54402\winxp\lea\rn

### 2.1.7 Image tampering

Tampering with image files, also known as steganography, is a relatively simple way of hiding data. As technology has evolved, so has the software and methods used by those hiding data.

One rudimentary method of image tampering and data concealment is achieved through Windows command prompt. By inputting a command, a person can modify the associated text file with the image (Cheddad et al, 2010, p 733). That way, if another party were to open the image file in an image file viewer, it would not display anything of note. However, if the image file were to be opened in a text viewer, the hidden data would be visible. This type of steganography is very basic, and relatively simple to discover. An example of a method which is harder to detect is double compression of a JPEG. As JPEG's are lossy, each time they are saved they are compressed, and when they are modified and tampered with, the compression pattern changes within the JPEG (Stamm et al, 2007).

Some methods for image tampering are virtually undetectable, or very difficult to detect. For example, should an image be modified, printed and rephotographed it would be near impossible to detect (Kee et al, 2011, p 7). This would only be an effective steganography method where the photo itself had been changed. Copy-move manipulation is also difficult to detect. Copy-move tampering is where part of the image is copy and pasted into the same image (Thakur and Rohilla, 2020, pp.7-8). This works by modifying the image, which then updates the prior record of the image. This does not work for hiding text.

Steganography can be used to protect against image tampering. Adding watermarks or inserting hidden text into images may be used as a means of authentication. The hidden watermark may be used to restore the tampered section of the image, as it would be hashed into the watermark (Zhu et al, 2007, pp. 516-517). This is not a widespread solution to image tampering.

#### 2.1.7.1 "Steghide & Stegoveritas"

- Utilising the suspect JPG files that we discovered in the Autopsy software, we will attempt to examine a proportion of the files for evidence of steganography. We are attempting this based on the the below information:
    - Several "out-of-place" images on a supposed workstation computer, that have no relevance to the targets role and responsibility in her job.
    - Some of the JPG files are quite large in size, which may indicate user tampering.
    - Autopsy software flagged numerous JPG file as having suspected user content.
    - The emails recovered suggested use of a "hiding" program that can be used to conceal any illicit activity.
- The methodology for achieveing this involves ensuring that the 'steghide' and 'stegoveritas' programs are installed on the forensic workstation being utilised. This is done using the linux command line:

  ```
  "# apt-get install steghide (stegoveritas)"
  ```
- Once installed, we use the command line to input the action and argument required. We outline the file that is to be examined and speciify the output file.

“#steghide extract -sf ‘stegoFile’ -xf ‘outputFile’ ”

- We can use steghide to show us what “human readable” or printable text may be embedded in the image:

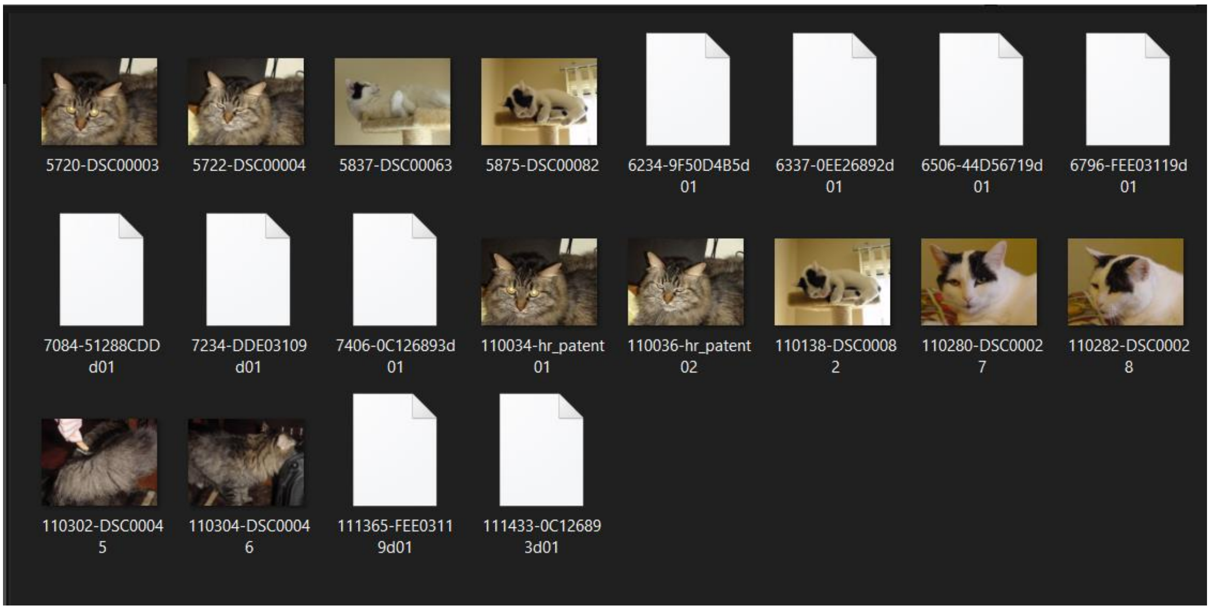
  “#strings -a ‘stegofile.jpg’ -n 6”

- We can also enable stegoveritas to inspect the image and determine what data types are making up its contents:

  “#stegoveritas ‘stegofile.jpg’ ”

- We conducted this operation on several suspect JPG files, the results of which will be discussed in the findings section.

#### 4.1.7.1.2



#### 4.1.7.2 Java Invisible Ink Toolkit:

- As Jordan had sent a copy of this software to Jo, we attempted to use the same software to decrypt the images. By downloading a copy of the suspect graphics files and running them through Java Invisible Ink Toolkit we hoped to be able to decode any hidden data in the images. This was not successful.

## 3.1 Findings:

The investigation has established that the target of the investigation, Jo, was in control of the computer for the time period that the investigation is covering. This means that the findings below are based on evidence that is directly related to, or activities conducted by, Jo on a m57.biz workstation computer.

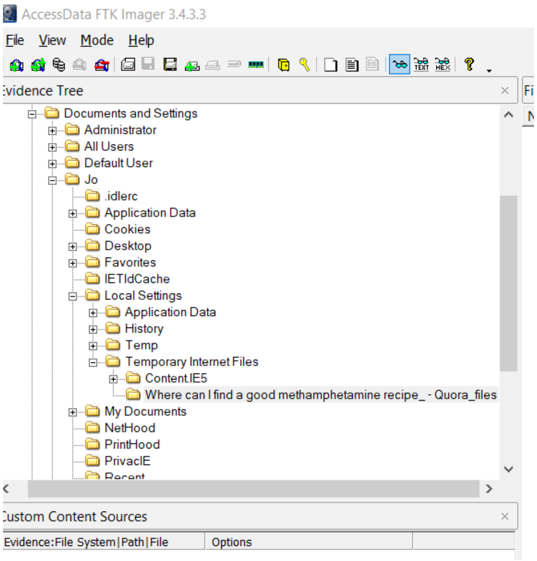
### 3.2 Finding 1- Direct reference to Methamphetamines (inculpatory)

There are several pieces of evidence that directly relate to methamphetamines. This inculpatory evidence includes Temporary Internet Files under user Jo [3.2.1], an image of crystal meth [3.2.2], an image of the chemical structure of methamphetamine [3.2.3], an image of pseudoephedrine which is another form of amphetamine [3.2.4], video files displaying different types of drug distillation [3.2.5], downloaded files that provide in-depth descriptions of methamphetamines [3.2.6], and an assortment of pdf files that contain methamphetamine information [3.2.7]. Several documents exist on the drives which are titled ‘cook.txt’ or ‘recipe.doc’ [3.2.8]. There is also evidence to suggest that Jo has been looking at or has purchased chemicals related to methamphetamine production [3.2.9].

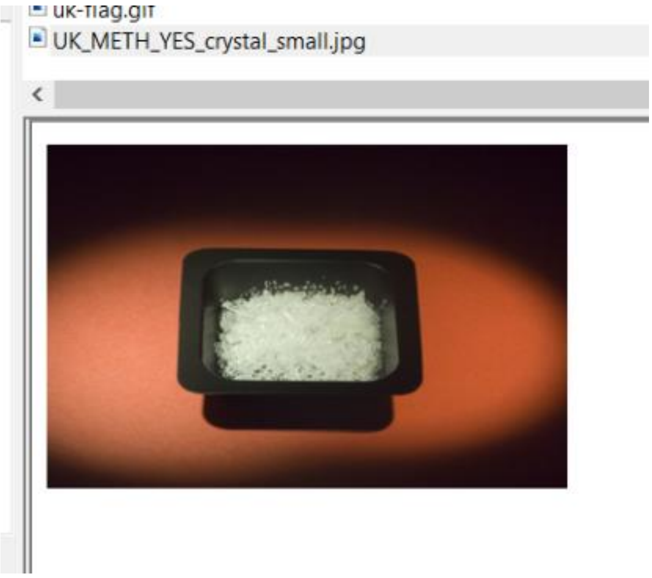
This evidence is both inculpatory and exculpatory as some of the information can be viewed in different contexts. The evidence that appears inculpatory includes the temporary internet files that are labelled ‘Where can I find a good methamphetamine recipe’. This file would indicate that Jo has actively used the internet to search how to manufacture methamphetamines. The finding is also reinforced with the evidence of the cooked crystal meth image, as well as the items in the folder names ‘purchase’. The video files that depict drug distillation is not necessarily inculpatory as these videos depict what appears to be naturopathic types of content.

Other pieces of inculpatory evidence that suggest Jo is in the early stages of methamphetamine activity is the downloaded files and pdf’s that contain a large amount of detailed information regarding methamphetamines. Both sets of evidence show the investigators that there is indeed large amounts of activity revolving around methamphetamines on Jo’s workstation- which is a primary reason for conducting the investigation in the first place.

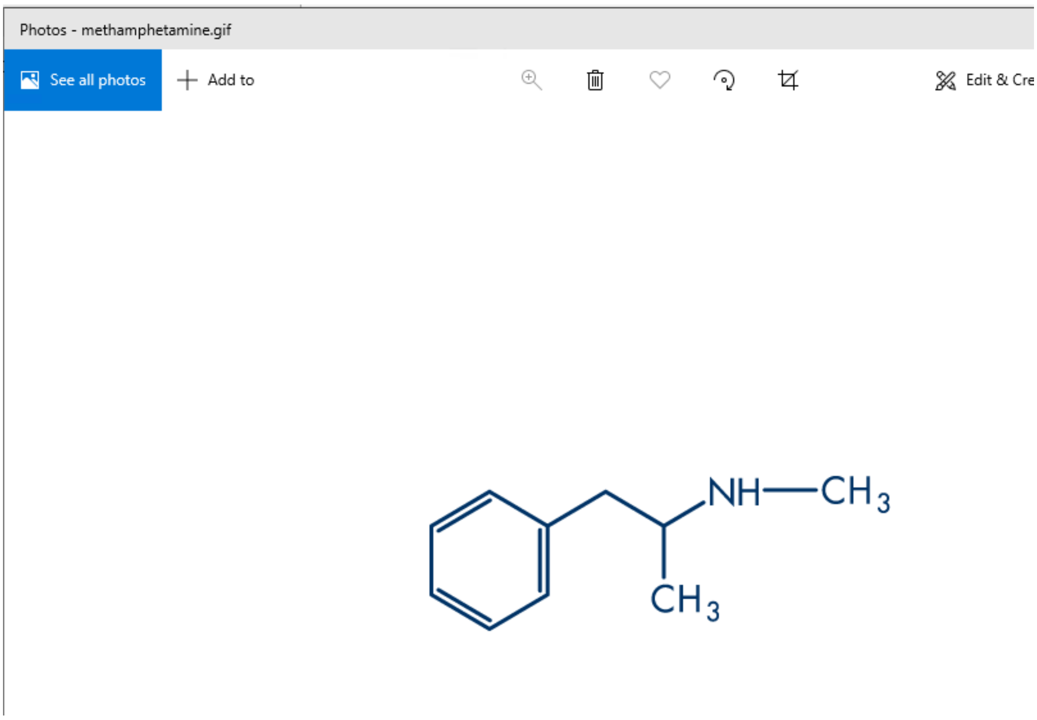
### *3.2.1*



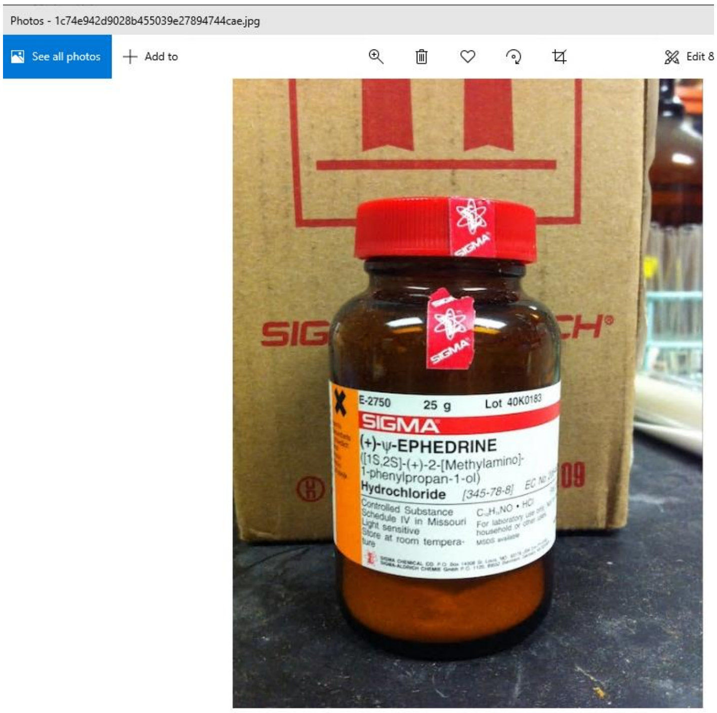
### 3.2.2


uk-flag.gif
UK_METH_YES_crystal_small.jpg

### 3.2.3

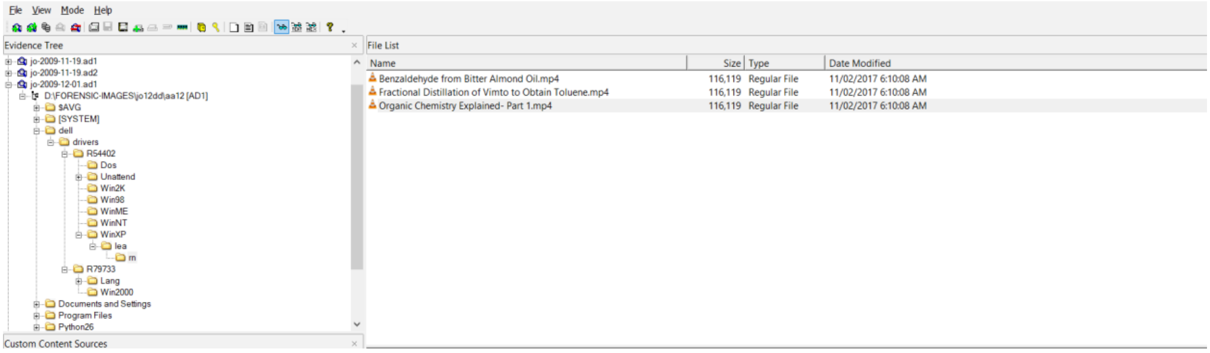

Photos - methamphetamine.gif
See all photos
Add to
Edit & Cre
NH
CH3
CH3

## 3.2.4



Photos - 1c74e942d9028b455039e27894744cae.jpg

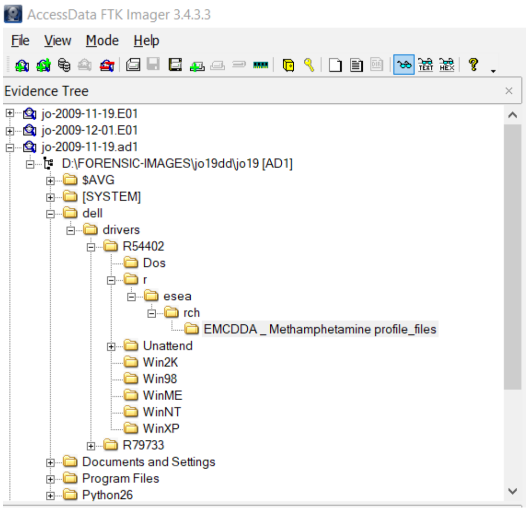
## 3.2.5



```
⊞ jo-2009-11-19.ad1
⊞ jo-2009-11-19.ad2
⊟ jo-2009-12-01.ad1
   ⊟ D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
      ⊞ $AVG
      ⊞ [SYSTEM]
      ⊟ dell
         ⊟ drivers
            ⊟ R54402
               Dos
               ⊞ Unattend
               Win2K
               Win98
               WinME
               WinNT
               ⊟ WinXP
                  ⊟ lea
                     m
            ⊟ R79733
               ⊞ Lang
               Win2000
      ⊞ Documents and Settings
      ⊞ Program Files
      ⊞ Python26
```

| Name | Size | Type | Date Modified |
|---|---|---|---|
| Benzaldehyde from Bitter Almond Oil.mp4 | 116,119 | Regular File | 11/02/2017 6:10:08 AM |
| Fractional Distillation of Vimto to Obtain Toluene.mp4 | 116,119 | Regular File | 11/02/2017 6:10:08 AM |
| Organic Chemistry Explained- Part 1.mp4 | 116,119 | Regular File | 11/02/2017 6:10:08 AM |

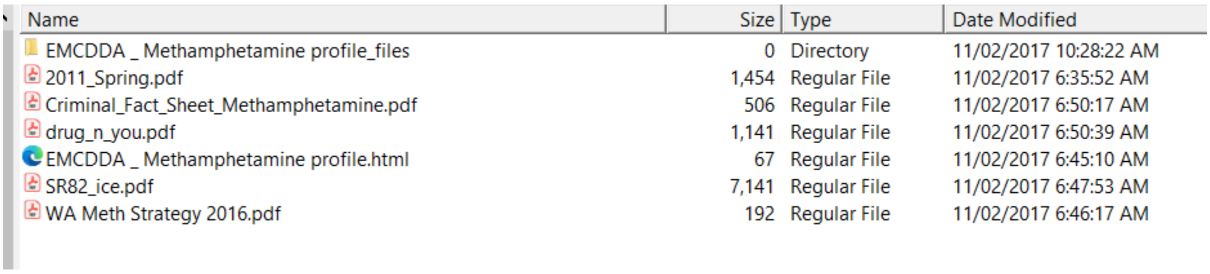
## 3.2.6



AccessData FTK Imager 3.4.3.3

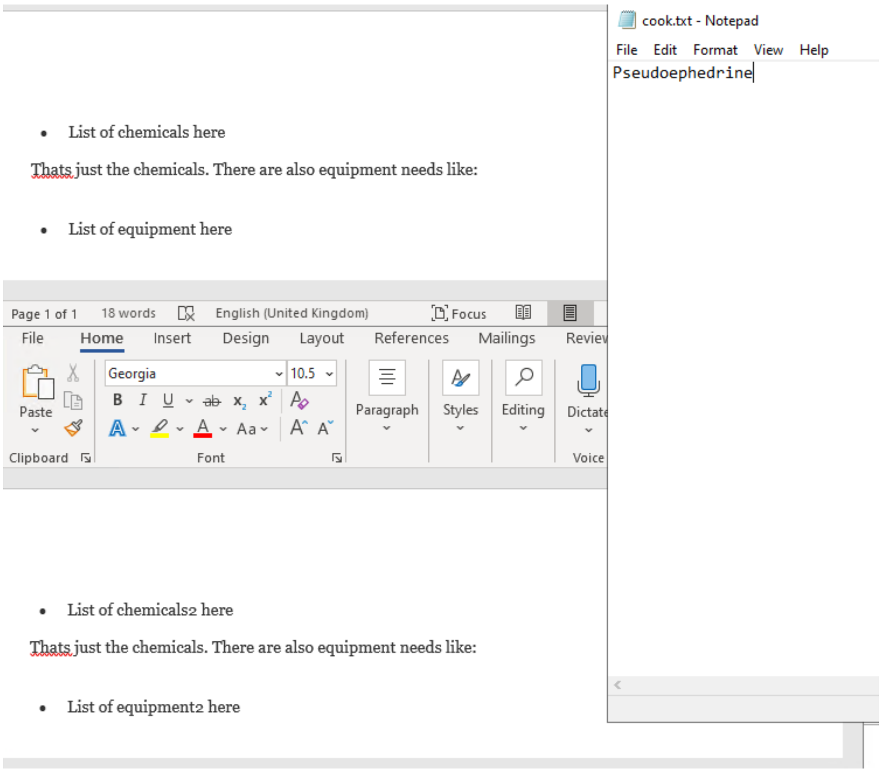
```
⊞ jo-2009-11-19.E01
⊞ jo-2009-12-01.E01
⊟ jo-2009-11-19.ad1
   ⊟ D:\FORENSIC-IMAGES\jo19dd\jo19 [AD1]
      ⊞ $AVG
      ⊞ [SYSTEM]
      ⊟ dell
         ⊟ drivers
            ⊟ R54402
               Dos
               ⊟ r
                  ⊟ esea
                     ⊟ rch
                        EMCDDA _ Methamphetamine profile_files
               ⊞ Unattend
               Win2K
               Win98
               WinME
               WinNT
               WinXP
            ⊞ R79733
      ⊞ Documents and Settings
      ⊞ Program Files
      ⊞ Python26
```

## 3.2.7



| Name | Size | Type | Date Modified |
|---|---|---|---|
| EMCDDA _ Methamphetamine profile_files | 0 | Directory | 11/02/2017 10:28:22 AM |
| 2011_Spring.pdf | 1,454 | Regular File | 11/02/2017 6:35:52 AM |
| Criminal_Fact_Sheet_Methamphetamine.pdf | 506 | Regular File | 11/02/2017 6:50:17 AM |
| drug_n_you.pdf | 1,141 | Regular File | 11/02/2017 6:50:39 AM |
| EMCDDA _ Methamphetamine profile.html | 67 | Regular File | 11/02/2017 6:45:10 AM |
| SR82_ice.pdf | 7,141 | Regular File | 11/02/2017 6:47:53 AM |
| WA Meth Strategy 2016.pdf | 192 | Regular File | 11/02/2017 6:46:17 AM |

## 3.2.8



- List of chemicals here

Thats just the chemicals. There are also equipment needs like:

- List of equipment here

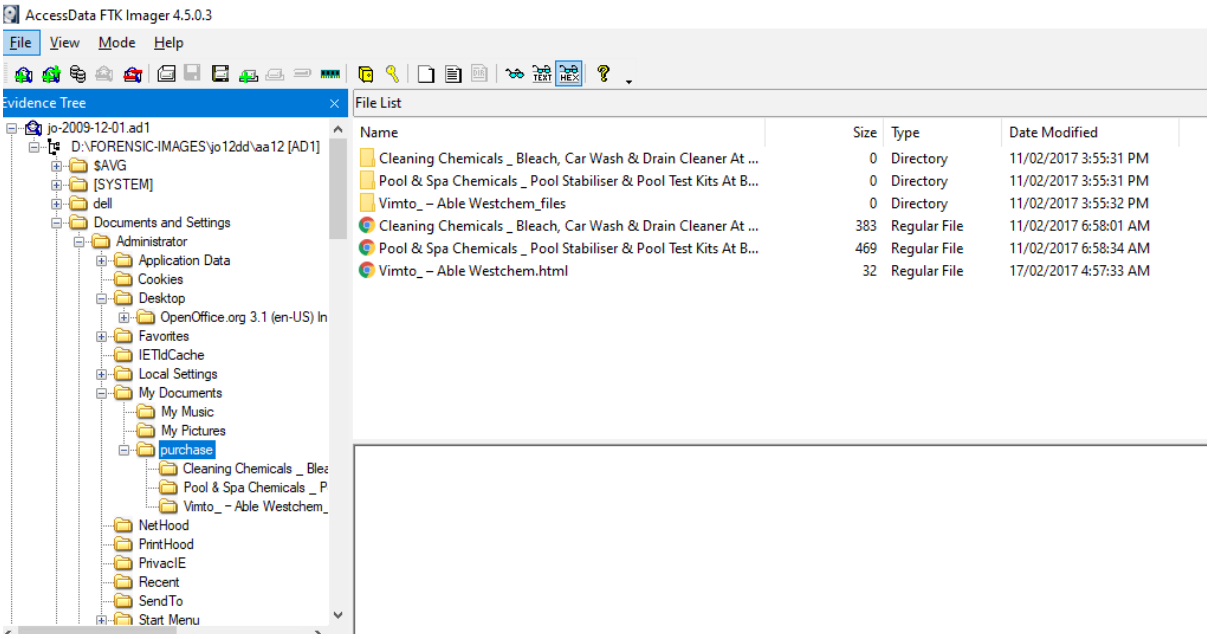
Pseudoephedrine

- List of chemicals2 here

Thats just the chemicals. There are also equipment needs like:

- List of equipment2 here

## 3.2.9



```
jo-2009-12-01.ad1
  D:\FORENSIC-IMAGES\jo12dd\aa12 [AD1]
    $AVG
    [SYSTEM]
    dell
    Documents and Settings
      Administrator
        Application Data
        Cookies
        Desktop
          OpenOffice.org 3.1 (en-US) In
        Favorites
        IETldCache
        Local Settings
        My Documents
          My Music
          My Pictures
          purchase
            Cleaning Chemicals _ Blea
            Pool & Spa Chemicals _ P
            Vimto_ – Able Westchem_
        NetHood
        PrintHood
        PrivacIE
        Recent
        SendTo
        Start Menu
```

| Name | Size | Type | Date Modified |
|---|---|---|---|
| Cleaning Chemicals _ Bleach, Car Wash & Drain Cleaner At ... | 0 | Directory | 11/02/2017 3:55:31 PM |
| Pool & Spa Chemicals _ Pool Stabiliser & Pool Test Kits At B... | 0 | Directory | 11/02/2017 3:55:31 PM |
| Vimto_ – Able Westchem_files | 0 | Directory | 11/02/2017 3:55:32 PM |
| Cleaning Chemicals _ Bleach, Car Wash & Drain Cleaner At ... | 383 | Regular File | 11/02/2017 6:58:01 AM |
| Pool & Spa Chemicals _ Pool Stabiliser & Pool Test Kits At B... | 469 | Regular File | 11/02/2017 6:58:34 AM |
| Vimto_ – Able Westchem.html | 32 | Regular File | 17/02/2017 4:57:33 AM |

## 3.3 Finding 2- Intentional illicit activities by Jo on m57.biz information systems (inculpatory)

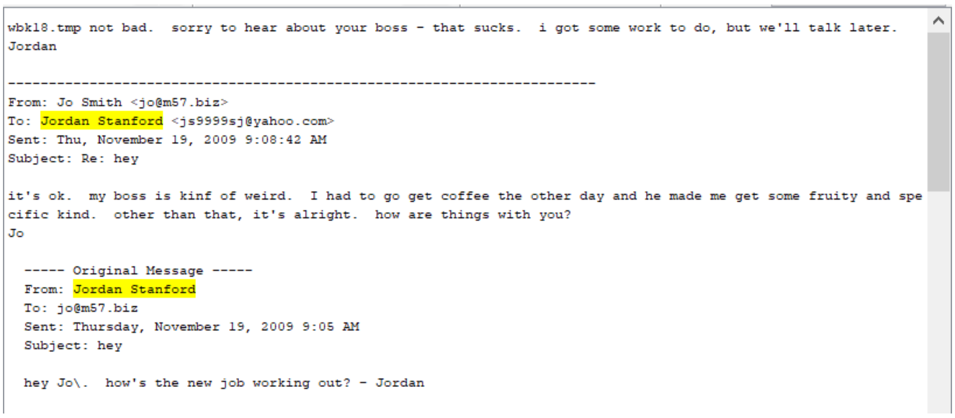
There are several pieces of inculpatory evidence that suggest that Jo has conducted illicit activities on her m57.biz workstation computer. The summation of these activities appears to be that Jo is under the guidance of an individual named Jordan Stanford, this guidance pertains to advice in attempting to hide possibly illicit images on the m57.biz information systems. This finding has been reached, as through the investigation we discovered and concluded that Jordan was a key individual in the investigation.

Jordan Stanford appears to be an acquaintance of Jo and the timeline of evidence suggests that casual emails [3.3.1], turned into suspicious interactions with Jordan Stanford providing Jo with programs to hide information on m57.biz systems, and how to use these programs [3.3.2]. This finding is inculpatory as it lends towards there having been illicit data being stored on the m57.biz systems.

This program could be using a python script and .jar file to re-route traffic flow to hide Jo's activity [3.3.3] & [3.3.4], by using proxy email addresses as targets [3.3.5].

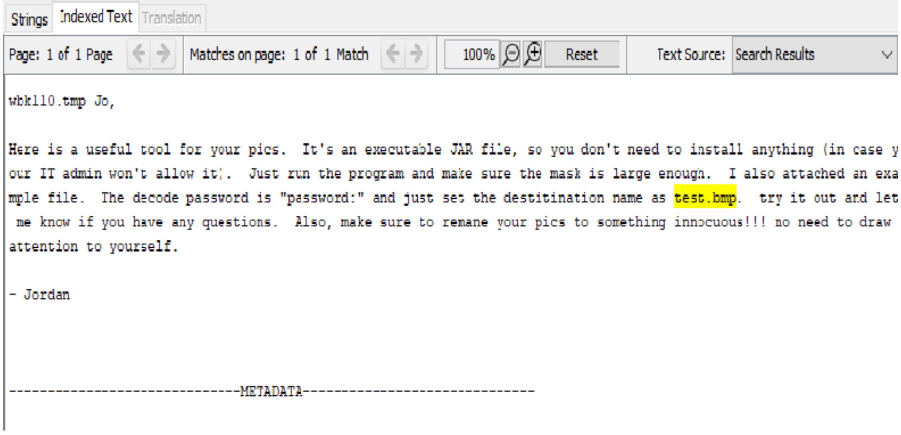
This conclusion is further enforced with another email that the investigation discovered, which outlines that Jo believed herself lucky that she was able to get her computer, which was being swapped, wiped before it was disposed of [3.3.6]. This computer that she references is the one that Aaron Greene purchased and approached police about. It appears that this event is what prompted Jordan Stanford to send the software program that hides information to Jo.

*3.3.1*



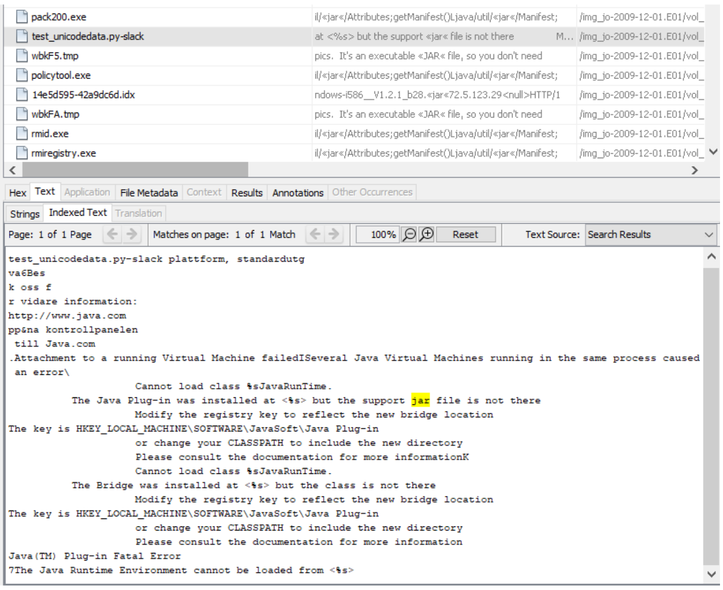
```
wbk18.tmp not bad.  sorry to hear about your boss - that sucks.  i got some work to do, but we'll talk later.
Jordan

------------------------------------------------------------------------
From: Jo Smith <jo@m57.biz>
To: Jordan Stanford <js9999sj@yahoo.com>
Sent: Thu, November 19, 2009 9:08:42 AM
Subject: Re: hey

it's ok.  my boss is kinf of weird.  I had to go get coffee the other day and he made me get some fruity and spe
cific kind.  other than that, it's alright.  how are things with you?
Jo

  ----- Original Message -----
  From: Jordan Stanford
  To: jo@m57.biz
  Sent: Thursday, November 19, 2009 9:05 AM
  Subject: hey

  hey Jo\.  how's the new job working out? - Jordan
```

### 3.3.2



```
wbk110.tmp Jo,

Here is a useful tool for your pics.  It's an executable JAR file, so you don't need to install anything (in case y
our IT admin won't allow it).  Just run the program and make sure the mask is large enough.  I also attached an exa
mple file.  The decode password is "password:" and just set the destitination name as test.bmp.  try it out and let
 me know if you have any questions.  Also, make sure to rename your pics to something innocuous!!! no need to draw
attention to yourself.

- Jordan



-----------------------------METADATA-----------------------------
```

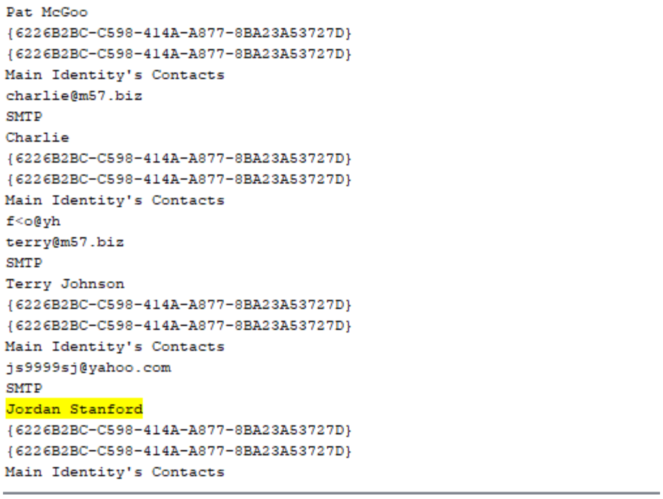
### 3.3.3



| | | |
|---|---|---|
| pack200.exe | il/«jar«/Attributes;getManifest()Ljava/util/«jar«/Manifest; | /img_jo-2009-12-01.E01/vol_ |
| test_unicodedata.py-slack | at <%s> but the support «jar« file is not there M... | /img_jo-2009-12-01.E01/vol_ |
| wbkF5.tmp | pics. It's an executable «JAR« file, so you don't need | /img_jo-2009-12-01.E01/vol_ |
| policytool.exe | il/«jar«/Attributes;getManifest()Ljava/util/«jar«/Manifest; | /img_jo-2009-12-01.E01/vol_ |
| 14e5d595-42a9dc6d.idx | ndows-i586__V1.2.1_b28.«jar«72.5.123.29<null>HTTP/1 | /img_jo-2009-12-01.E01/vol_ |
| wbkFA.tmp | pics. It's an executable «JAR« file, so you don't need | /img_jo-2009-12-01.E01/vol_ |
| rmid.exe | il/«jar«/Attributes;getManifest()Ljava/util/«jar«/Manifest; | /img_jo-2009-12-01.E01/vol_ |
| rmiregistry.exe | il/«jar«/Attributes;getManifest()Ljava/util/«jar«/Manifest; | /img_jo-2009-12-01.E01/vol_ |

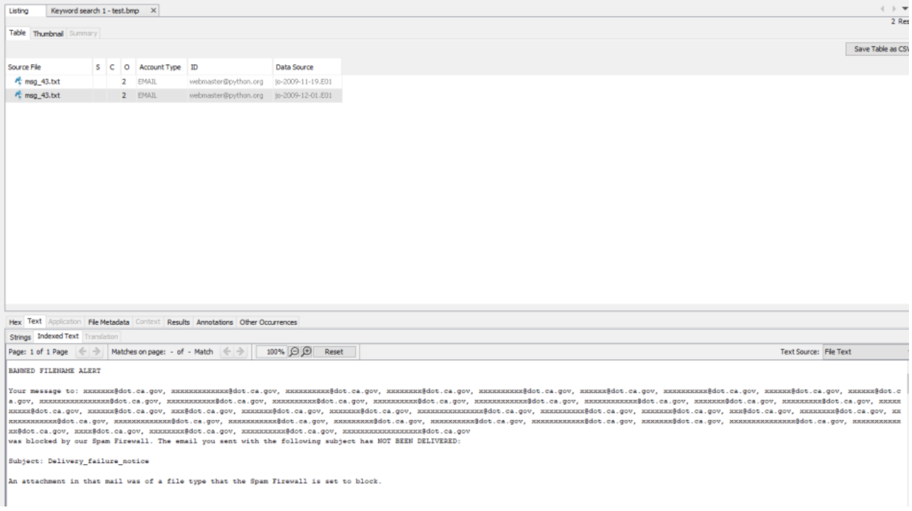
```
test_unicodedata.py-slack plattform, standardutg
va6Bes
k oss f
r vidare information:
http://www.java.com
pp&na kontrollpanelen
 till Java.com
.Attachment to a running Virtual Machine failedISeveral Java Virtual Machines running in the same process caused
 an error\
                    Cannot load class %sJavaRunTime.
          The Java Plug-in was installed at <%s> but the support jar file is not there
                    Modify the registry key to reflect the new bridge location
The key is HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Plug-in
                    or change your CLASSPATH to include the new directory
                    Please consult the documentation for more informationK
                    Cannot load class %sJavaRunTime.
          The Bridge was installed at <%s> but the class is not there
                    Modify the registry key to reflect the new bridge location
The key is HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Plug-in
                    or change your CLASSPATH to include the new directory
                    Please consult the documentation for more information
Java(TM) Plug-in Fatal Error
7The Java Runtime Environment cannot be loaded from <%s>
```

### 3.3.4



```
Pat McGoo
{6226B2BC-C598-414A-A877-8BA23A53727D}
{6226B2BC-C598-414A-A877-8BA23A53727D}
Main Identity's Contacts
charlie@m57.biz
SMTP
Charlie
{6226B2BC-C598-414A-A877-8BA23A53727D}
{6226B2BC-C598-414A-A877-8BA23A53727D}
Main Identity's Contacts
f<o@yh
terry@m57.biz
SMTP
Terry Johnson
{6226B2BC-C598-414A-A877-8BA23A53727D}
{6226B2BC-C598-414A-A877-8BA23A53727D}
Main Identity's Contacts
js9999sj@yahoo.com
SMTP
Jordan Stanford
{6226B2BC-C598-414A-A877-8BA23A53727D}
{6226B2BC-C598-414A-A877-8BA23A53727D}
Main Identity's Contacts
```

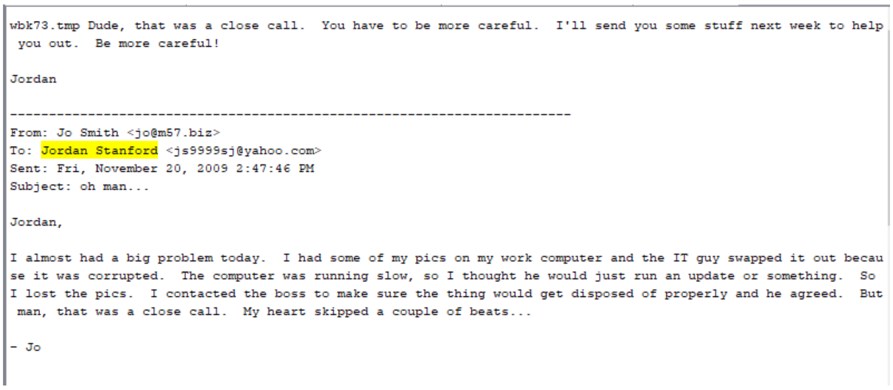
3.3.5



| Source File | S | C | O | Account Type | ID | Data Source |
|---|---|---|---|---|---|---|
| msg_43.txt |  |  | 2 | EMAIL | webmaster@python.org | jo-2009-11-19.E01 |
| msg_43.txt |  |  | 2 | EMAIL | webmaster@python.org | jo-2009-12-01.E01 |

```
BANNED FILENAME ALERT

Your message to: xxxxxxx@dot.ca.gov, xxxxxxxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxx@dot.ca.gov, xxxxxx@dot.c
a.gov, xxxxxxxxxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxxxxxxxx@dot.ca.gov, xxxxxxxxxxxx@dot.ca.gov, xxxxxxx@dot.ca.gov, xxxxxxxxx@dot.ca.gov, xxxxx
xxxxx@dot.ca.gov, xxxxxx@dot.ca.gov, xxx@dot.ca.gov, xxxxxxx@dot.ca.gov, xxxxxxx@dot.ca.gov, xxxxxxxxxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxxx@dot.ca.gov, xxx@dot.ca.gov, xxxxxxxx@dot.ca.gov, xx
xxxxxxxxxx@dot.ca.gov, xxxxxxxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxxxxxxxx@dot.ca.gov, xxxxxxx@dot.ca.gov, xxxxxxxxxxxxxxx@dot.ca.gov, xxxxxxxxxxx
xx@dot.ca.gov, xxxx@dot.ca.gov, xxxxxxxx@dot.ca.gov, xxxxxxxxxx@dot.ca.gov, xxxxxxxxxxxxxxxxx@dot.ca.gov
was blocked by our Spam Firewall. The email you sent with the following subject has NOT BEEN DELIVERED:

Subject: Delivery_failure_notice

An attachment in that mail was of a file type that the Spam Firewall is set to block.
```

3.3.6



```
wbk73.tmp Dude, that was a close call.  You have to be more careful.  I'll send you some stuff next week to help
 you out.  Be more careful!

Jordan

------------------------------------------------------------------------
From: Jo Smith <jo@m57.biz>
To: Jordan Stanford <js9999sj@yahoo.com>
Sent: Fri, November 20, 2009 2:47:46 PM
Subject: oh man...

Jordan,

I almost had a big problem today.  I had some of my pics on my work computer and the IT guy swapped it out becau
se it was corrupted.  The computer was running slow, so I thought he would just run an update or something.  So
I lost the pics.  I contacted the boss to make sure the thing would get disposed of properly and he agreed.  But
 man, that was a close call.  My heart skipped a couple of beats...

- Jo
```

## 3.4 Finding 3- Using company time and resources to setup an online presence that has methamphetamine relevance (exculpatory).

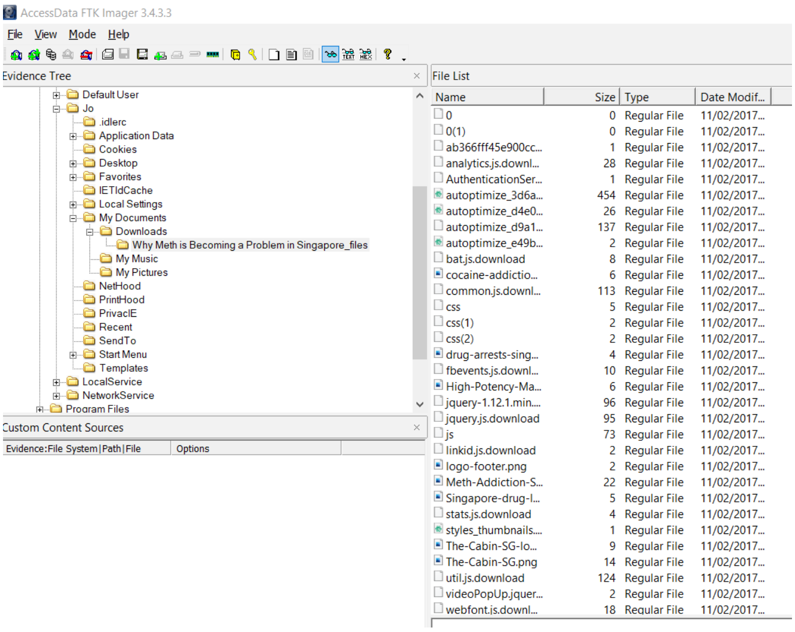
The next finding that the investigation has examined is the presence of files and directories that reference HTML and CSS files and could indicate that Jo has been trying to research and setup an online presence directly relating to methamphetamines.

Several of these folders exist on the seized data and both hold information that pertains to methamphetamines, though not in a directly illicit way. One of the folders has files and webpages from what appears to be an academic webpage that outlines why methamphetamines are becoming a problem in Singapore [3.4.1]. The other folder appears to contain web page information about the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) [3.4.2].

The fact that both files and their contents are parts of webpages could be considered either inculpatory or exculpatory. They add value to the findings relating to methamphetamine activity as they directly reference this context. However, the nature of the evidence and webpages that they depict could reference methamphetamines in a different context.

For the purposes of this investigation, this finding is inconclusive and will be considered exculpatory.

### 3.4.1

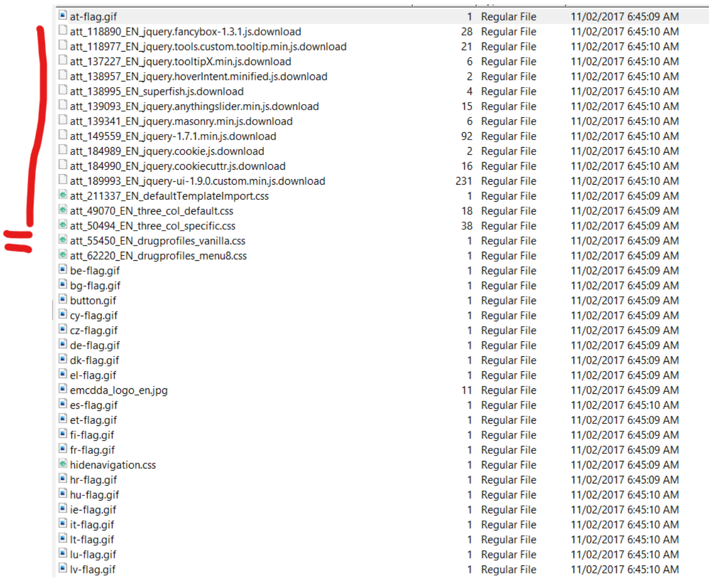


```
⊞ Default User
⊟ Jo
    .idlerc
  ⊞ Application Data
    Cookies
  ⊞ Desktop
  ⊞ Favorites
    IETldCache
  ⊞ Local Settings
  ⊟ My Documents
    ⊟ Downloads
        Why Meth is Becoming a Problem in Singapore_files
      My Music
      My Pictures
    NetHood
    PrintHood
    PrivacIE
    Recent
    SendTo
  ⊞ Start Menu
    Templates
⊞ LocalService
⊞ NetworkService
⊞ Program Files
```

| Evidence:File System\|Path\|File | Options |
|---|---|

| Name | Size | Type | Date Modif... |
|---|---|---|---|
| 0 | 0 | Regular File | 11/02/2017... |
| 0(1) | 0 | Regular File | 11/02/2017... |
| ab366fff45e900cc... | 1 | Regular File | 11/02/2017... |
| analytics.js.downl... | 28 | Regular File | 11/02/2017... |
| AuthenticationSer... | 1 | Regular File | 11/02/2017... |
| autoptimize_3d6a... | 454 | Regular File | 11/02/2017... |
| autoptimize_d4e0... | 26 | Regular File | 11/02/2017... |
| autoptimize_d9a1... | 137 | Regular File | 11/02/2017... |
| autoptimize_e49b... | 2 | Regular File | 11/02/2017... |
| bat.js.download | 8 | Regular File | 11/02/2017... |
| cocaine-addictio... | 6 | Regular File | 11/02/2017... |
| common.js.downl... | 113 | Regular File | 11/02/2017... |
| css | 5 | Regular File | 11/02/2017... |
| css(1) | 2 | Regular File | 11/02/2017... |
| css(2) | 2 | Regular File | 11/02/2017... |
| drug-arrests-sing... | 4 | Regular File | 11/02/2017... |
| fbevents.js.downl... | 10 | Regular File | 11/02/2017... |
| High-Potency-Ma... | 6 | Regular File | 11/02/2017... |
| jquery-1.12.1.min.... | 96 | Regular File | 11/02/2017... |
| jquery.js.download | 95 | Regular File | 11/02/2017... |
| js | 73 | Regular File | 11/02/2017... |
| linkid.js.download | 2 | Regular File | 11/02/2017... |
| logo-footer.png | 2 | Regular File | 11/02/2017... |
| Meth-Addiction-S... | 22 | Regular File | 11/02/2017... |
| Singapore-drug-l... | 5 | Regular File | 11/02/2017... |
| stats.js.download | 4 | Regular File | 11/02/2017... |
| styles_thumbnails.... | 1 | Regular File | 11/02/2017... |
| The-Cabin-SG-lo... | 9 | Regular File | 11/02/2017... |
| The-Cabin-SG.png | 14 | Regular File | 11/02/2017... |
| util.js.download | 124 | Regular File | 11/02/2017... |
| videoPopUp.jquer... | 2 | Regular File | 11/02/2017... |
| webfont.js.downl... | 18 | Regular File | 11/02/2017... |

### 3.4.2



| | | | |
|---|---|---|---|
| at-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| att_118890_EN_jquery.fancybox-1.3.1.js.download | 28 | Regular File | 11/02/2017 6:45:10 AM |
| att_118977_EN_jquery.tools.custom.tooltip.min.js.download | 21 | Regular File | 11/02/2017 6:45:10 AM |
| att_137227_EN_jquery.tooltipX.min.js.download | 6 | Regular File | 11/02/2017 6:45:10 AM |
| att_138957_EN_jquery.hoverIntent.minified.js.download | 2 | Regular File | 11/02/2017 6:45:10 AM |
| att_138995_EN_superfish.js.download | 4 | Regular File | 11/02/2017 6:45:10 AM |
| att_139093_EN_jquery.anythingslider.min.js.download | 15 | Regular File | 11/02/2017 6:45:10 AM |
| att_139341_EN_jquery.masonry.min.js.download | 6 | Regular File | 11/02/2017 6:45:10 AM |
| att_149559_EN_jquery-1.7.1.min.js.download | 92 | Regular File | 11/02/2017 6:45:10 AM |
| att_184989_EN_jquery.cookie.js.download | 2 | Regular File | 11/02/2017 6:45:10 AM |
| att_184990_EN_jquery.cookiecuttr.js.download | 16 | Regular File | 11/02/2017 6:45:10 AM |
| att_189993_EN_jquery-ui-1.9.0.custom.min.js.download | 231 | Regular File | 11/02/2017 6:45:10 AM |
| att_211337_EN_defaultTemplateImport.css | 1 | Regular File | 11/02/2017 6:45:09 AM |
| att_49070_EN_three_col_default.css | 18 | Regular File | 11/02/2017 6:45:09 AM |
| att_50494_EN_three_col_specific.css | 38 | Regular File | 11/02/2017 6:45:09 AM |
| att_55450_EN_drugprofiles_vanilla.css | 1 | Regular File | 11/02/2017 6:45:09 AM |
| att_62220_EN_drugprofiles_menu8.css | 1 | Regular File | 11/02/2017 6:45:09 AM |
| be-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| bg-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| button.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| cy-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| cz-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| de-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| dk-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| el-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| emcdda_logo_en.jpg | 11 | Regular File | 11/02/2017 6:45:09 AM |
| es-flag.gif | 1 | Regular File | 11/02/2017 6:45:10 AM |
| et-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| fi-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| fr-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| hidenavigation.css | 1 | Regular File | 11/02/2017 6:45:09 AM |
| hr-flag.gif | 1 | Regular File | 11/02/2017 6:45:09 AM |
| hu-flag.gif | 1 | Regular File | 11/02/2017 6:45:10 AM |
| ie-flag.gif | 1 | Regular File | 11/02/2017 6:45:10 AM |
| it-flag.gif | 1 | Regular File | 11/02/2017 6:45:10 AM |
| lt-flag.gif | 1 | Regular File | 11/02/2017 6:45:10 AM |
| lu-flag.gif | 1 | Regular File | 11/02/2017 6:45:10 AM |
| lv-flag.gif | 1 | Regular File | 11/02/2017 6:45:10 AM |

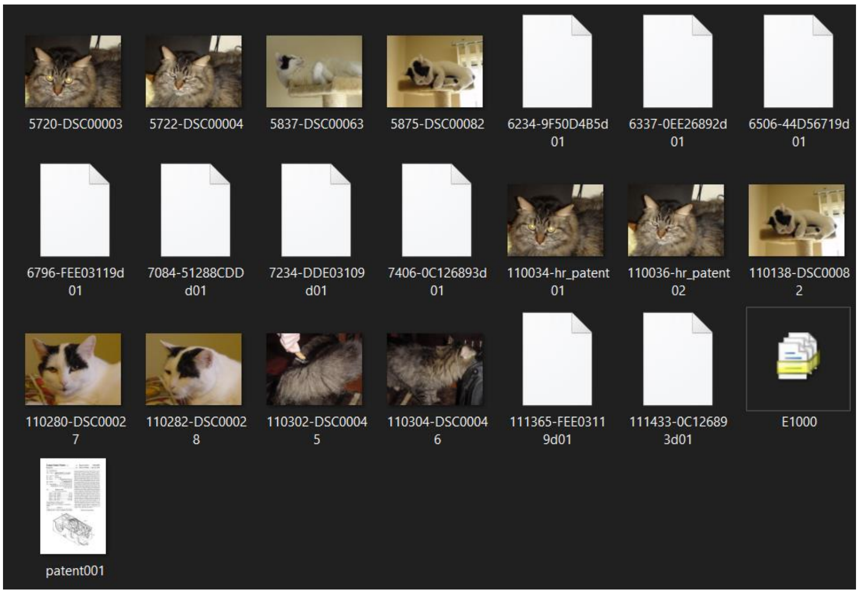
## 3.5 Finding 4- Deceptive Image files that could contain further evidence. (inculpatory)

Finding 2 relates to illicit activity on Jo's computer including what appears to be discussions on data tampering. This finding differs as it refers to image tampering only. This finding of image tampering is reinforced by the email captured that outlines that Jo was in the process of trying to achieve this. Several of the image files that have been processed by the various forensics software appear to be identical copies of each other. Further analysis has shown that the file sizes differ, and they contain different information. This could indicate the use of steganography techniques by Jo [3.5.1]. Jordan had also emailed a copy of Java Invisible Ink Toolkit to Jo, which is a software used for steganography [3.5.2] and [3.5.3].

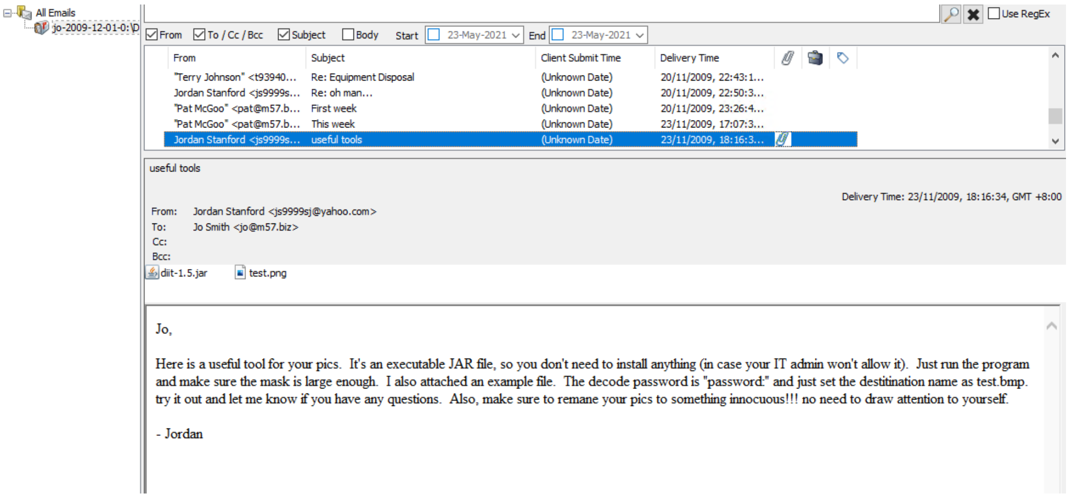
The naming conventions of some of the images suggests to us that they have been changed from their original form, which explains the double-ups of some images. The hash files of the images have not changed between the two copies of the hard drives provided by Police. This would suggest that either both copies of the images contain images which have been tampered with, or the images are unaltered. Given the other evidence discovered it suggests that the image files have been tampered with.

Certain images when extracted from forensics software were not able to be viewed by the O/S image viewers. These images were visibly blurry when viewing in forensics software. This implies that they have had certain pieces of their header information slightly altered, which makes them non-visible to standard image viewer software [3.5.4].

*3.5.1*



## 3.5.2


All Emails
jo-2009-12-01-0:\D
☑ From ☑ To / Cc / Bcc ☑ Subject □ Body Start □ 23-May-2021 End □ 23-May-2021
□ Use RegEx

| From | Subject | Client Submit Time | Delivery Time |
|---|---|---|---|
| "Terry Johnson" <t93940… | Re: Equipment Disposal | (Unknown Date) | 20/11/2009, 22:43:1… |
| Jordan Stanford <js9999s… | Re: oh man… | (Unknown Date) | 20/11/2009, 22:50:3… |
| "Pat McGoo" <pat@m57.b… | First week | (Unknown Date) | 20/11/2009, 23:26:4… |
| "Pat McGoo" <pat@m57.b… | This week | (Unknown Date) | 23/11/2009, 17:07:3… |
| Jordan Stanford <js9999s… | useful tools | (Unknown Date) | 23/11/2009, 18:16:3… |

useful tools

Delivery Time: 23/11/2009, 18:16:34, GMT +8:00

From: Jordan Stanford <js9999sj@yahoo.com>
To: Jo Smith <jo@m57.biz>
Cc:
Bcc:

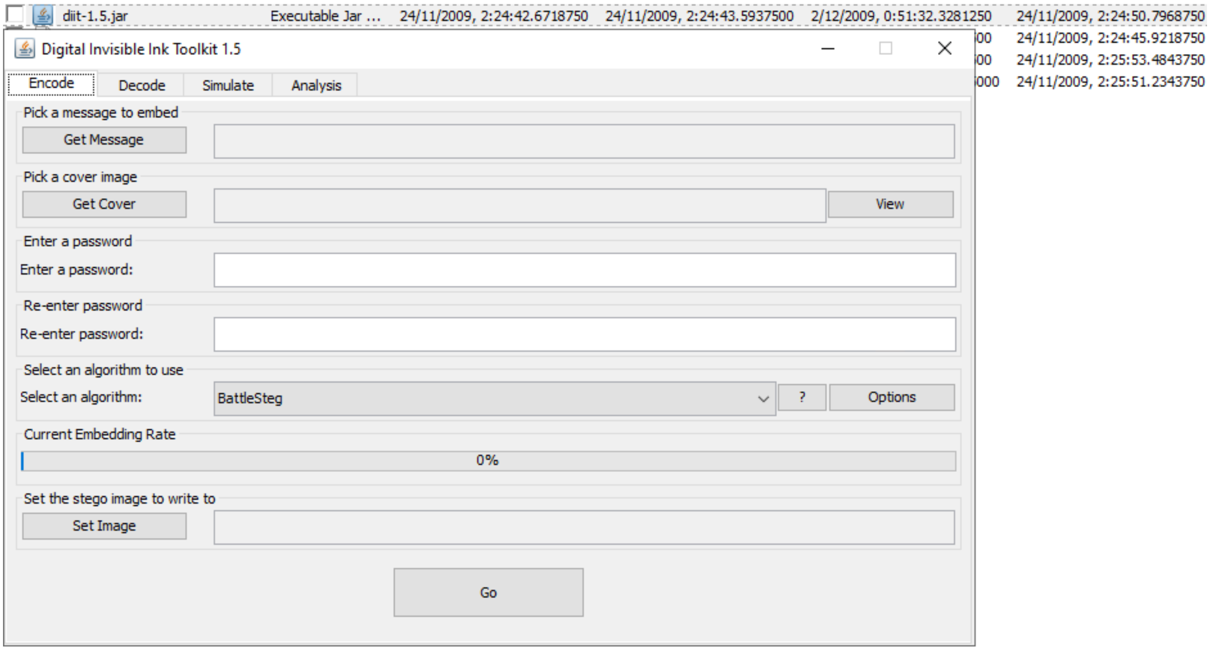
diit-1.5.jar test.png

Jo,

Here is a useful tool for your pics. It's an executable JAR file, so you don't need to install anything (in case your IT admin won't allow it). Just run the program and make sure the mask is large enough. I also attached an example file. The decode password is "password:" and just set the destitination name as test.bmp. try it out and let me know if you have any questions. Also, make sure to remane your pics to something innocuous!!! no need to draw attention to yourself.

- Jordan

## 3.5.3



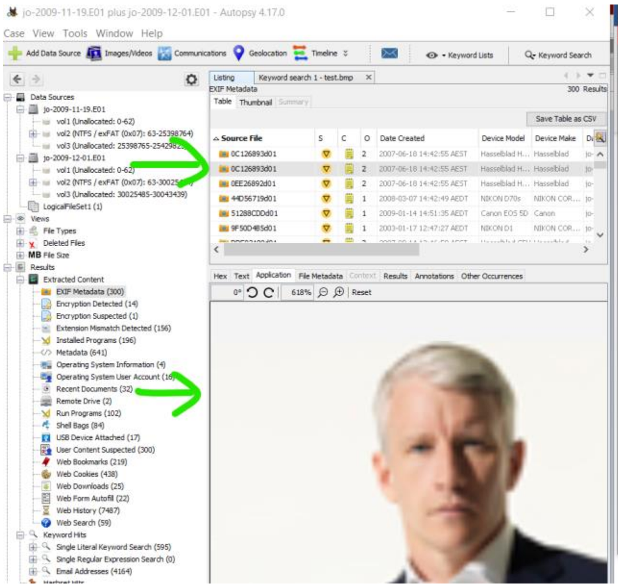
diit-1.5.jar Executable Jar … 24/11/2009, 2:24:42.6718750 24/11/2009, 2:24:43.5937500 2/12/2009, 0:51:32.3281250 24/11/2009, 2:24:50.7968750
00 24/11/2009, 2:24:45.9218750
00 24/11/2009, 2:25:53.4843750
000 24/11/2009, 2:25:51.2343750

Digital Invisible Ink Toolkit 1.5

Select an algorithm: BattleSteg

0%

### 3.5.4



jo-2009-11-19.E01 plus jo-2009-12-01.E01 - Autopsy 4.17.0

- Data Sources
  - jo-2009-11-19.E01
    - vol1 (Unallocated: 0-62)
    - vol2 (NTFS / exFAT (0x07): 63-25398764)
    - vol3 (Unallocated: 25398765-254298…
  - jo-2009-12-01.E01
    - vol1 (Unallocated: 0-62)
    - vol2 (NTFS / exFAT (0x07): 63-30025…
    - vol3 (Unallocated: 30025485-30043439)
  - LogicalFileSet1 (1)
- Views
  - File Types
  - Deleted Files
  - MB File Size
- Results
  - Extracted Content
    - EXIF Metadata (300)
    - Encryption Detected (14)
    - Encryption Suspected (1)
    - Extension Mismatch Detected (156)
    - Installed Programs (196)
    - Metadata (641)
    - Operating System Information (4)
    - Operating System User Account (16)
    - Recent Documents (32)
    - Remote Drive (2)
    - Run Programs (102)
    - Shell Bags (84)
    - USB Device Attached (17)
    - User Content Suspected (300)
    - Web Bookmarks (219)
    - Web Cookies (438)
    - Web Downloads (25)
    - Web Form Autofill (22)
    - Web History (7487)
    - Web Search (59)
  - Keyword Hits
    - Single Literal Keyword Search (595)
    - Single Regular Expression Search (0)
    - Email Addresses (4164)

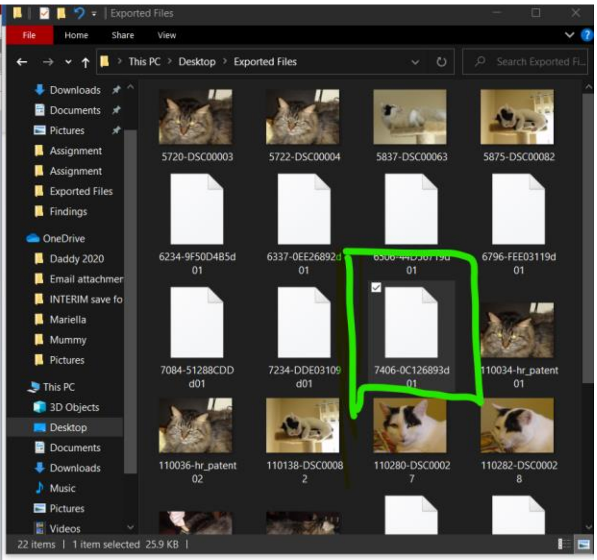
Listing | Keyword search 1 - test.bmp

EXIF Metadata — 300 Results

Table | Thumbnail | Summary — Save Table as CSV

| Source File | S | C | O | Date Created | Device Model | Device Make | D |
|---|---|---|---|---|---|---|---|
| 0C126893d01 | ▽ |  | 2 | 2007-06-18 14:42:55 AEST | Hasselblad H… | Hasselblad | jo- |
| 0C126893d01 | ▽ |  | 2 | 2007-06-18 14:42:55 AEST | Hasselblad H… | Hasselblad | jo- |
| 0EE26892d01 | ▽ |  | 2 | 2007-06-18 14:42:55 AEST | Hasselblad H… | Hasselblad | jo- |
| 44D56719d01 | ▽ |  | 1 | 2008-03-07 14:42:49 AEDT | NIKON D70s | NIKON COR… | jo- |
| 51288CDDd01 | ▽ |  | 1 | 2009-01-14 14:51:35 AEDT | Canon EOS 5D | Canon | jo- |
| 9F50D485d01 | ▽ |  | 1 | 2003-01-17 12:47:27 AEDT | NIKON D1 | NIKON COR… | jo- |

Hex Text Application File Metadata Context Results Annotations Other Occurrences
0° 618% Reset

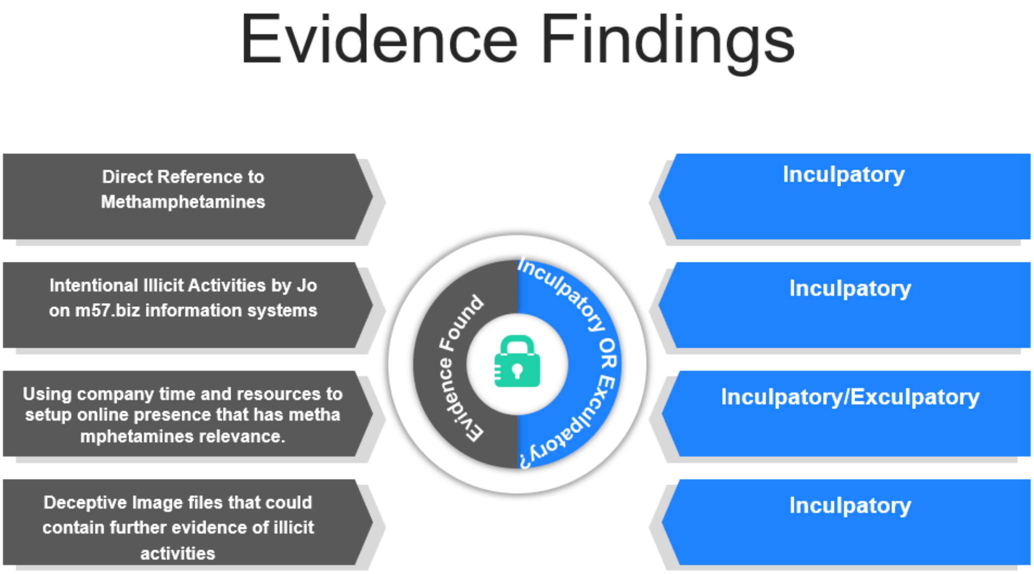


Exported Files

22 items | 1 item selected 25.9 KB |

## 3.6 Finding 5- Investigation on certain individuals.

Given the evidence it would be beneficial if an OSINT investigation is conducted into Jordan Stanford and Aaron Greene. This has not been conducted as it falls outside the scope of this investigation.



Evidence Findings

| | |
|---|---|
| Direct Reference to Methamphetamines | Inculpatory |
| Intentional Illicit Activities by Jo on m57.biz information systems | Inculpatory |
| Using company time and resources to setup online presence that has metha mphetamines relevance. | Inculpatory/Exculpatory |
| Deceptive Image files that could contain further evidence of illicit activities | Inculpatory |

## 4.1 Conclusion:

At the conclusion of this investigation we have discovered several pieces of evidence which relates to methamphetamine and other forms of amphetamines. There is not any direct evidence of drug use, however there is evidence which would suggest that Jo has been hiding data on the computer about methamphetamine production. This can be ascertained from the files discussed in Finding 1. These files indicate that Jo was researching how to start producing methamphetamine and was in the process of purchasing the required materials for methamphetamine production.

Given the rigorous evidence examination which has taken place, as well as continuous hash value checking we would suggest that the evidence collected is reliable and sound. The variety of methods used to gather and verify evidence also lends to the credibility of the evidence collected.

Evidence provided in Finding 1, particularly 3.2.6 and 3.2.7 also indicates that Jo would be aware that methamphetamine and other amphetamines are illegal to use or manufacture. Based on the evidence collected, no sufficient evidence exists of methamphetamine use or methamphetamine production. Whilst there is a large amount of evidence lending towards methamphetamine production there would not be enough to carry a conviction as it does not meet the burden of proof. Should Police have further evidence external to what is discovered in these drives, a conviction would most likely result in a guilty finding for Jo, however as it stands, the evidence found would not be sufficient on its own to lead to a successful prosecution.

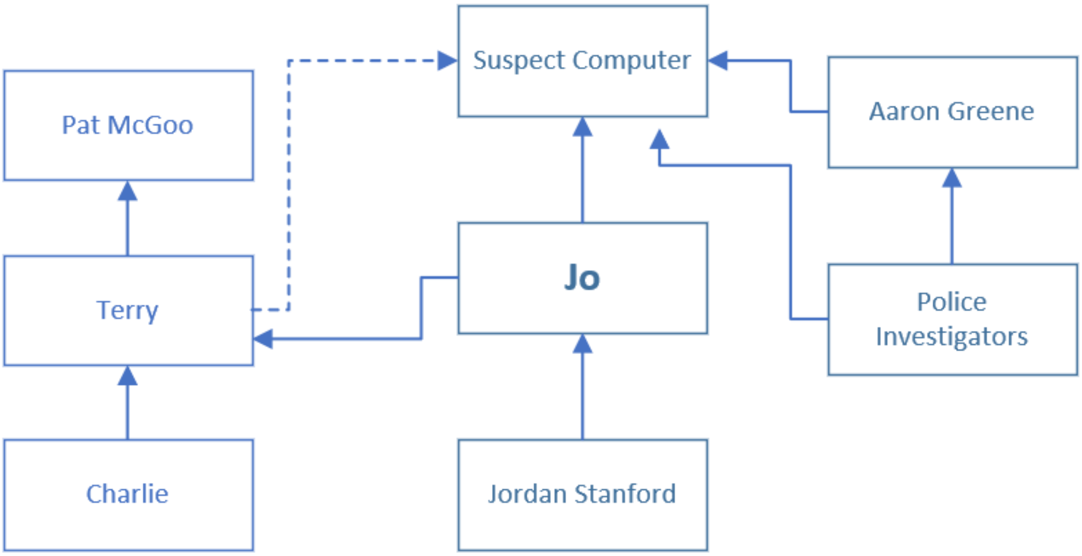
## 5.1 Appendix:

### 5.2 Persons of Interest:

| Name | Email | Link to Target | Possible Illicit Evidence Obtained? | Further Investigation required? |
|---|---|---|---|---|
| **Jo** | jo@m57.biz | (Investigation Target) | YES | YES- criminal prosecution could ensue. |
| **Pat McGoo** | pat@m57.biz | CEO of M57 Biz | NO | NO |
| **Terry** | terry@m57.biz | IT Administrator of M57 Biz | YES | YES- possible illicit software on M57 systems. Need to rule out link to current investigation. |
| **Charlie** | charlie@m57.biz | Co-worker of target. | NO | NO |
| **Aaron Greene** | aaron@greene.net | Individual who reported computer contents to Police. | NO | YES |
| **Jordan Stanford** | js9999sj@yahoo.com | Associate of target who offered advice in | YES | YES- priority investigation workstream. |

| | | | | |
|---|---|---|---|---|
| | | conducting illicit activities, provided programs and links to accomplish this end. | | |
| **Police Investigators** | police@department.org | Investigators who conducted initial data capture and preliminary investigation. | NO | NO |

## 5.3 Association Diagram:

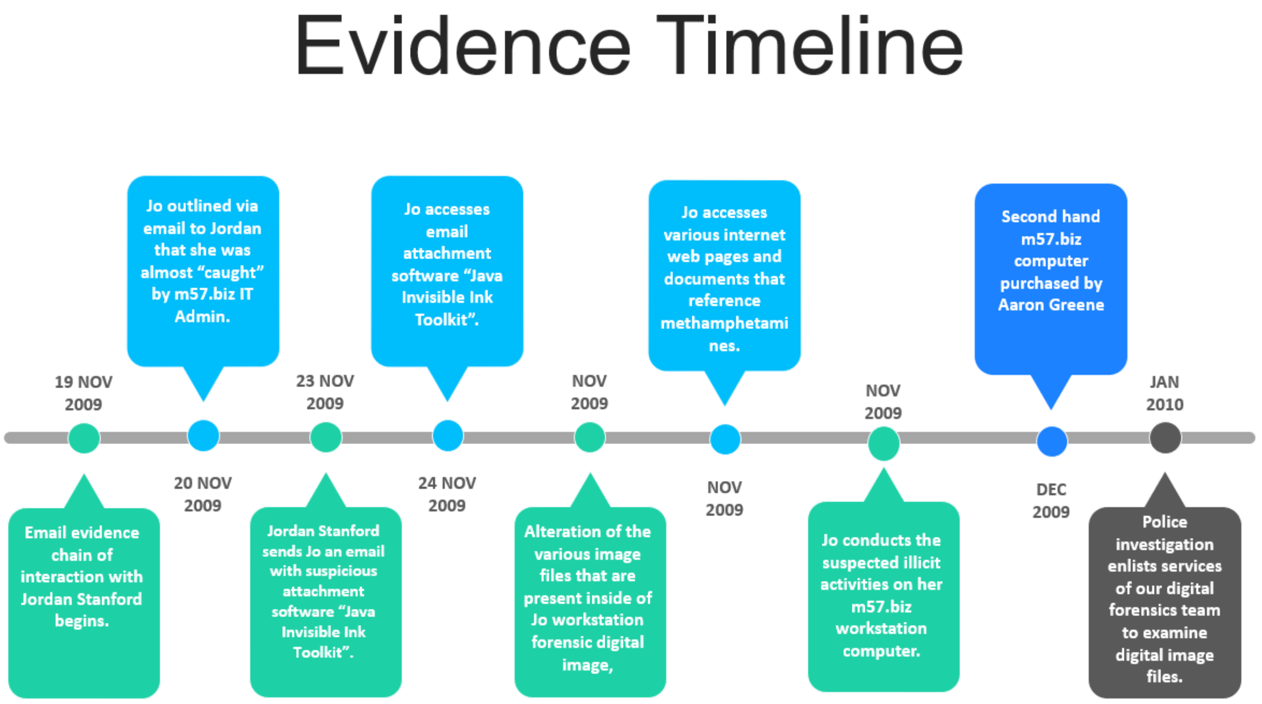


## 5.4 Evidence Listing:

- Hard drive image ‘2009-11-19.E01’ (of the original sold computer) – **E01**
    - [CB76EBFB75B4736621C41BFC29770BEEF618D771EA36AA5510F60B48C0148417]
- Second drive image purporting to be of the same computer – **AD1, AD2**
    - AD1 [F9EB80B049141F235A0281A045C5DBBAD43119FCDC692E2218E264BBAA9EF3D7]
    - AD2 [0AD3EDA65B8EF4E5DC8AC74D7002694EB6755CA782DA9B1E7C8E131525BAEA4]

- Hard drive image ‘2009-12-01.E01’ (of the suspects replacement computer seized from M57) – **E01**
    - [4DD3C5B465431389F95105D73A0A394FF52FB4F9CD10CF9C79F9D961890DEF52]
- Second drive image purporting to of the same computer – **AD1, AD2, AD3**
    - AD1 [2606C23DCFA624D24D79D02E175448D695B493C4ED50B3142798F1C43656D40D]
    - AD2 [9D6204B503AF814AF4AF573DB44CAF7243CFE2BB2714C37A3CC8A9C5EC09AE63]
    - AD3 [FE9B27119982B009A178D7FE65004B22CB580FEE97495D0326734BBBDD828934]

## 5.5 Evidence Timeline:



Evidence Timeline

19 NOV 2009 – Email evidence chain of interaction with Jordan Stanford begins.

20 NOV 2009 – Jo outlined via email to Jordan that she was almost “caught” by m57.biz IT Admin.

23 NOV 2009 – Jordan Stanford sends Jo an email with suspicious attachment software “Java Invisible Ink Toolkit”.

24 NOV 2009 – Jo accesses email attachment software “Java Invisible Ink Toolkit”.

NOV 2009 – Alteration of the various image files that are present inside of Jo workstation forensic digital image,

NOV 2009 – Jo accesses various internet web pages and documents that reference methamphetamines.

NOV 2009 – Jo conducts the suspected illicit activities on her m57.biz workstation computer.

DEC 2009 – Second hand m57.biz computer purchased by Aaron Greene

JAN 2010 – Police investigation enlists services of our digital forensics team to examine digital image files.

## 5.5 Software and tools used in Investigation:

- Autopsy
    - Version 4.17.0

  - Maintained by ‘Basic Technology Corp’
  - Utilises: Perl, Java, SQL Lite and PostgreSQL.
- FTK Imager
  - Made by ‘AccessData’
  - Includes hashing functionality and password dictionary.
- OS Forensics
  - Version 7.0
  - Made by ‘Passmark Software’
- WinHex
  - Made by ‘X-Ways Software Technology AG’
  - German company
  - Advanced hex data editor, capable of in-depth data analysis
- ProDiscover Basic
  - Made by ‘ARC Group’
  - Built in reporting tools.
- IrfanView’
  - Free-to-use for non-commercial, developer software
  - Image viewer and editor for MS Windows
- Hex Workstation
  - Made by ‘BreakPoint Software’
  - Complete set of hexadecimal development tools for MS Windows
  - Allows for manipulation of binary data
- Aid4Mail
  - Made by ‘Fookes Software’ Switzerland
  - Email migration, conversion, and forensics
- WinMerge
  - Open source differencing and merging tool for MS Windows.
  - Can compare both folder and files, presenting differences in a visual text format.
- 7-Zip
  - Version 19.00
  - Open-source software
  - File archiver, utility used to place groups of files within compressed containers.
- Kali Linux Workstation
  - Version 2021.1

  - Digital forensics and penetration testing O/S widely used in the information security profession.
  - O/S booted in VirtualBox as a Virtual Machine- this provides the most sanitized workstation possible.
- Excel
  - Microsoft Office 2016 made by Microsoft
- Java Invisible Ink Toolkit
  - Made by Java
- Steghide.
  - Version 0.5.1
  - Command line software
  - Open source
- USB-C Flash Drives
  - To hold and transport the data files given by police investigators.

## 6.1 References:

Azad, Usama. 2020. *Sleuth Kit Autopsy in-depth tutorial*. Accessed via [Sleuth Kit Autopsy in-depth tutorial – Linux Hint]

Back Slash. 2017. *How to Hide Secret Data Inside an Image or Audio File in Seconds.* 'Wonder How To. NullByte'. Accessed via [Steganography: How to Hide Secret Data Inside an Image or Audio File in Seconds « Null Byte :: WonderHowTo

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal processing*, *90*(3), 727-752.

E. Kee, M. K. Johnson and H. Farid, "Digital Image Authentication From JPEG Headers," in *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1066-1075, Sept. 2011, doi: 10.1109/TIFS.2011.2128309.

International Organisation for Standards. 2018. *ISO/IEC 27037:2012- Information technology- Security techniques- Guidelines for identification, collection, acquisition and preservation of digital evidence.* Accessed via 'iso.org' [ISO - ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence]

M. C. Stamm, S. K. Tjoa, W. S. Lin and K. J. R. Liu, "Undetectable image tampering through JPEG compression anti-forensics," *2010 IEEE International Conference on Image Processing*, 2010, pp. 2109-2112, doi: 10.1109/ICIP.2010.5652553.

Mutkawoa, Nitin J. 2018. *Linux Memory Analysis with Lime and Volatility.* Accessed via [Linux memory analysis with Lime and Volatility – Blog by Nitin J Mutkawoa (tunnelix.com)]

Nelson, Bill. Phillips, Amelia. Steuart, Chris. 2019. *Guide to Computer Forensics and Investigations: Processing Digital Evidence*. Cengage Information Security. Fifth Edition. Cengage Learning, Inc. Boston, MA. USA.

Sudyana, Didik. Prayudi, Yudi. Sugiantoro, Bambang. 2019. *Analysis and Evaluation Digital Forensic Investigation Framework using ISO 27037:2012.* DOI:10.17781/P002464. Accessed via ResearchGate [(8) (PDF) Analysis and Evaluation Digital Forensic Investigation Framework using ISO 27037:2012 (researchgate.net)]

Thakur, R., & Rohilla, R. (2020). Recent advances in digital image manipulation detection techniques: A brief review. Forensic Science International, 110311.

Wilson, Craig. 2014. *ACPO Good Practice Guide for Digital Evidence*. Association of Chief Police Officers. Accessed via 'Digital Detective Blog' [ACPO Good Practice Guide for Digital Evidence | Digital Detective (digital-detective.net)]

Zhu, X., Ho, A. T., & Marziliano, P. (2007). A new semi-fragile image watermarking with robust tampering restoration using irregular sampling. *Signal Processing: Image Communication*, *22*(5), 515-528.