Digital Forensics Handbook

by Harjinder Singh Lallie (HL@warwick.ac.uk)

Contents

Part I
Basic Investigation

1 Introduction

This handbook aims to guide you through the tutorial/lab sessions within the digital forensics/cyber security incident management modules. Although teaching staff are available and present to help you throughout the tutorial sessions, the guide is intended to enable you to self-lead yourself through the work. The writing style has been presented in a way to enable you to work independently throughout this.

This manual is undergoing continual development. I would like your feedback on how helpful/not helpful it/bits of it have been.

The guide is based around several software, the dominant being Autopsy. Autopsy is a digital forensic tool used to analyse hard disk images, and file systems such as NTFS, FAT, HFS+, Ext3, and UFS.

The source code is available to enable the development of unique and specialist utilities. Commercial versions do not normally allow this and where they do provide a facility for the development of modules, it often involves writing code in specialist scripting languages. An example of this is the EnScript language in EnCase. The Autopsy/Sleuthkit software comes in two 'flavours':

- *'The Sleuth Kit (TSK)'* is a collection of command line tools that allow you to investigate disk images. This is a very flexible set of tools which allow you to incorporate your own modules.
- *'Autopsy'* is a Windows GUI version of the digital investigation tools. The GUI version also allows developers to integrate their own tools. This is the version we are using in these tutorials.

This manual is based on Autopsy 4.19.3 running in a Windows environment there may be some small variations to the notes presented herein compared to the version and the operating system environment that your lab is running.

Another tool we will be using is called: FTK Imager (v4.7.1.2). FTK Imager is used to create digital forensic images (DFI) and is also useful for viewing the DFI in hex format.

The full list of tools that may be used, with URLs of where you can download them, is provided in Section 1.4.

1.1 Tools and Materials

This manual will specify tools and materials needed in each element of the tutorial as follows:

Materials

A pre-created ingested case directory called `Stanley` which contains the DFI: `Stanley.E01`.

1.2 Convention

Please note the following conventions in this tutorial. File/case/image names will be presented in a violet courier font. Areas of the visual interface space will be in a teal font like this. DFIs will be presented in a red font like this

I sometimes abbreviate long paths or link names where the path or link name is obvious to the reader. For example, vol2 (NTFS / exFAT (0x07): 3504-778239) becomes vol2...

1.3 Forensic Workstation, case files and images (DFIs)

You will be provided with a Forensic Workstation in the form of a virtual machine configured specifically to support this handbook. The Forensic Workstation should contain all the software needed for the work and the coursework, and pre-configured case files. You are welcome of course to create your own forensic workstation, however, whilst we will do our best to support you if there are problems with the workstation, we cannot guarantee of course it will operate in the same way and exactitude as the one provided.

Case directories have been pre-created to (a) save time (b) reduce the likelihood that student generated case files might not be configured with the correct ingest settings required for the tutorial work. These can be found in a directory external to the VM. One of your first tasks will be to create a permanent mount to the volume/directory that contains the case files.

DFIs –Digital Forensic Images are provided within each case directory in a directory called _DFI. So if you are working on the Stanley case, the Stanley.E01 DFI is found within the _DFI directory for that case file.

Be aware that if you delete the case directory, you will also be deleting the DFI. If you wish to recreate a case, make sure you copy the DFI from the original directory.

1.4 List of tools used

Some or all of the following tools will be used within the tutorials. The list is not conclusive, and version numbers may differ.

- Autopsy 4.19.3 (http://www.sleuthkit.org/)
- FTK Imager 4.7.1.2 (https://accessdata.com/product-download/ftk-imager-version-4-1-1)
- GPXSee (https://www.gpxsee.org/)
- Registry Explorer 2.0.0.0 (https://ericzimmerman.github.io/#!index.md)
- MFT Explorer 2.0.0.0 (https://ericzimmerman.github.io/#!index.md)
- Hashcalc 2.02 (https://hashcalc.en.softonic.com/)
- Exiftool 12.72 (https://exiftool.org/)
- Hex Editor Neo (https://www.hhdsoftware.com/free-hex-editor)

- DB Browser for SQLite (https://sqlitebrowser.org/dl/)

1.5 Errors in the Handbook

These notes have been written so that they can be used as self-study notes (non-instructor led). Every care has been taken to ensure there are no errors or ambiguities in this set of tutorial notes (of course). Please report any errors, ambiguities or suggestions for improvement so that the tutorial notes can be corrected.

1.6 Errors in the Tool

Autopsy is an open source tool undergoing continual development. As with many forensic tools, there are several shortcomings/errors in the tool. Some of these shortcomings may be highlighted over the course of this tutorial.

Digital forensic tools are not error free. Many of them contain idiosyncrasies and errors, which investigators quickly become aware of. Investigators can cater for these errors as long as they are aware of them. As you progress through the tutorial, you will notice a few errors with Autopsy. Some of these are just feature errors, for example, in version 4.3.1, when a user searched for the same keyword more than once, Autopsy enumerated the result count. Unfortunately, many versions later, this error still seems to exist.

1.7 Figures and misnomers

Please note, this manual is updated each year, some of the figures may not exactly match what you see in your environment. Please also be aware that, from time to time, the numbers specified in the manual may not exactly match what you see. For example, the manual might say you should be seeing 'x' files in a particular search, however, you only see 'y'. Please do not worry. This may be because of a mismatch between the ingest settings applied when that portion of the manual was written compared to when the case directory was created for you.

1.8 What the manual does not (yet) include

As I said earlier, this manual is under continual development. I have not yet included the following elements within this manual. Although some of the tutorials exist, and although depending on which module you are studying you may already have studied that material, it has not yet been included in the manual. Currently, if you want to explore these further you will need to do your own independent research:

- Malware analysis on a DFI.
- Shell Bags analysis.
- MFT/File system analysis.
- Intrusive file signature analysis.

- Drone analysis.
- Dashcam analysis.
- Android file system analysis.
- IoS analysis.
- MAC OS analysis.

2 Managing Cases

Materials

A pre-created ingested case directory called `Animal` which requires the DFI: `Animal.E01` (also provided in the directory).

A pre-created ingested case directory called `TrashedDisk` which requires the DFI: `TrashedDisk.E01` (also provided in the directory)

In this section of the tutorial, you will learn how to create/open a case. You will learn about ingest modules and about the data sources that one might investigate. You will add some evidence files to the case.

Before we proceed though, let's try to understand that the term *case* means different things to different people. To a *case manager* - the person that has overall responsibility for a case, the case includes fingerprint evidence, DNA evidence, witness testimonies, and a whole collection of different forms of evidence. To a digital investigator however, a *case* is a containing environment which holds and indexes digital evidence sources pertaining to the case under investigation. All investigative work is done in this case, important items of evidence are tagged and subsequently included with a report of the investigation.

In this tutorial, we will create a 'dummy' case called `DeleteMe`. You will save this cases into a cases directory. You will add two data (evidence) sources to it, and then close it. We will not use this case again.

1. Create a local directory to store your cases.
2. Launch Autopsy

You are presented with a welcome screen presenting the following options (Figure 1 left):

- `New Case`
- `Open Recent Case`
- `Open Case`

Previously created cases can be opened by either selecting `Open Case` or `Open Recent Case`. The open recent case option presents a list of the most recent opened cases. This can often be an easier and quicker way of opening a case. Next, we need to give the case a name, and provide a directory name in which all the case files will be located. The report relating to the investigation is stored within the case directory - as are XML files pertaining to the tags and links created during the course of the investigation.

Autopsy creates a case file with the extension: `.AUT` within this directory. We will explore this directory in a few moments.

3. As this is our first case, select `Create New Case`
4. Enter `DeleteMe` as the case name.

5. Save the case in the cases directory that you created earlier and then select `Next`. When (and if) promoted to create the directory, select `Yes`.

6. Next, we need to give the case a number. If this was a case being investigated by an organisation or a law enforcement agency, a number would automatically be assigned to the case by the case manager. In our case however, enter 001 for the case number and your name as the examiner, and then selecy `Finish`

7. The next screen presents you with an option to generate or specify a host. Leave this as default (*Generate new host...*).

After digital storage systems have been seized and recorded as per the chain of custody procedures, the next step of the process is to create a digital forensic image (DFI) of the evidence. The DFI is a bit for bit - exact copy of the original evidence. Investigators conduct an investigation on the DFI rather than the original evidence, this ensures that the original data is not corrupted as a result of the investigation. When the DFI is viewed in a forensic investigation system

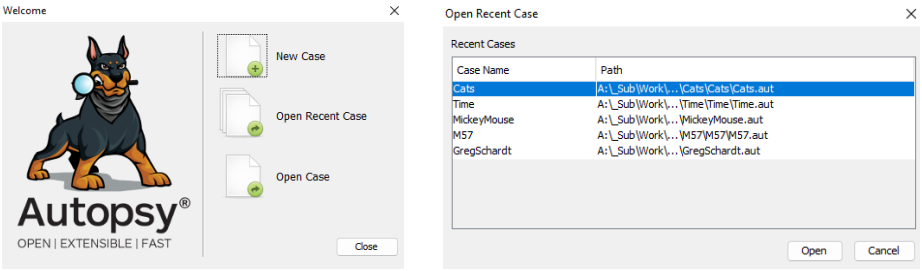


Figure 1: The welcome screen (left) and opening a recent case (right)

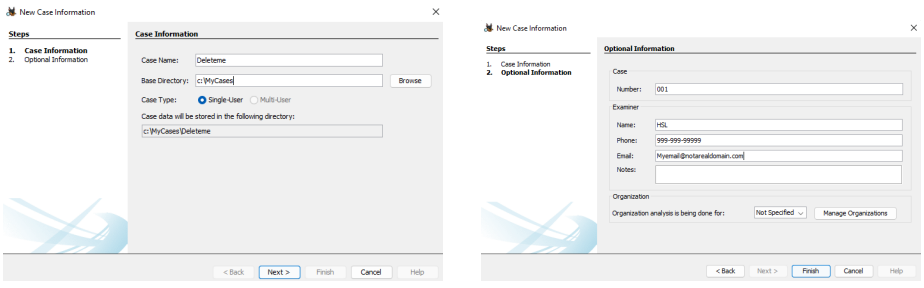


Figure 2: The new case screen

the investigator is presented with a precise unaltered view of the original digital storage system (DSS).

The DFI of the digital storage system is different to a mirror copy which is where an exact copy of the viewable portion of a volume is made onto another disk. In theory you should be able to use the mirror copy and boot from it as you can with the original disk, this is not possible with the image.

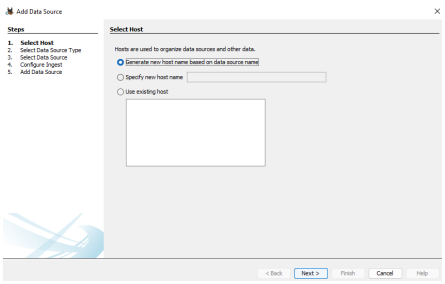


Figure 3: The host screen

Next we need to add a data source for the investigation (Figure 4.) We shall proceed to describe a few data sources. This is not a complete list of the data source types that Autopsy accepts but highlights the more popular data sources.

Disk Images. A disk image is a DFI. DFIs can be created using a number of applications such as EnCase and FTK. At the time of writing, Autopsy cannot create forensic copies, having said that, there are plenty of open source options which will allow the investigator to achieve the same. Forensic copies can take a number of formats, Autopsy supports the following formats: Raw Single (*.img, *.dd, *.raw, *.bin); Raw Split (*.001, *.aa); EnCase (*.e01); Virtual Machine Disk (*.vmdk); Virtual Hard Disk (*.vhd). The ability to add VM files is useful. This allows the investigator to create experimental environments in virtual machines and then investigate the outcomes/results of those experiments using Autopsy.

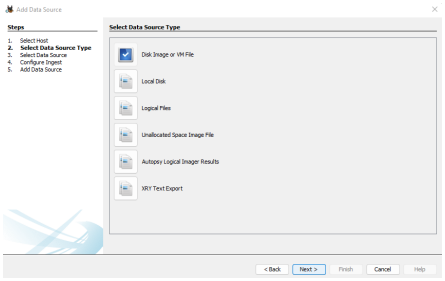


Figure 4: Adding a data source

Local Disk. The *local disk* option allows an investigator to add a data source such as a USB (connected to a write blocker of course) without needing to create a forensic image first.

Logical File. This enables an investigator to add a folder or individual files, again without needing to create a forensic image.

8. Select `Disk Image or VM File`

9. Leave the `Ignore orphan files in FAT file systems` option unchecked.

Orphan files are those files which at some point were deleted and for which,

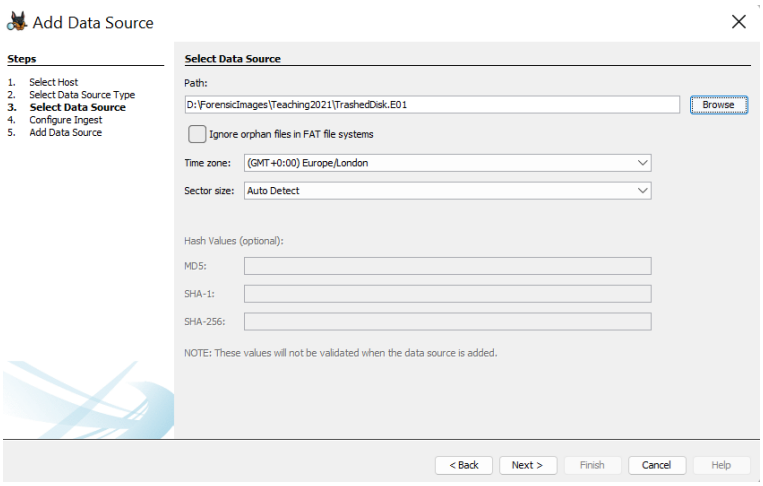


Figure 5: Data source selection

unlike other deleted files, it is not possible to determine the location of the file or folder within the directory structure prior to when the file was deleted.

The timezone is an important consideration as this is useful in benchmarking time within a case.

10. Select the timezone in which the media was seized – which in our case is (GMT +0:00) Europe/London.

11. Click on `Browse` and then browse to the directory which contains the `TrashedDisk.E01` image file, select it and then click open (Figure 5)

12. Now select `Next`

Autopsy's ingest modules are a set of pre-processing functions which search through a DFI and extract and index data that matches given categories such as EXIF data, emails, embedded files, Text messages / SMS / MMS; Call Logs; Contacts; Tango Messages; Words with Friends Messages; GPS from the browser and Google Maps; and GPS from cache.wifi and cache.cell files from Android images. One of the benefits of Autopsy's open source concept is that ingest modules can be created and added to the software to provide additional functionality.

The ingest modules are executed when an evidence item is created. This form of pre-processing, whilst taking a lot of time when setting up the case, speeds up the investigation. Ingest processing can take a long time. Consequently, when large disk storage systems are involved, it is normal to leave the ingest running overnight.

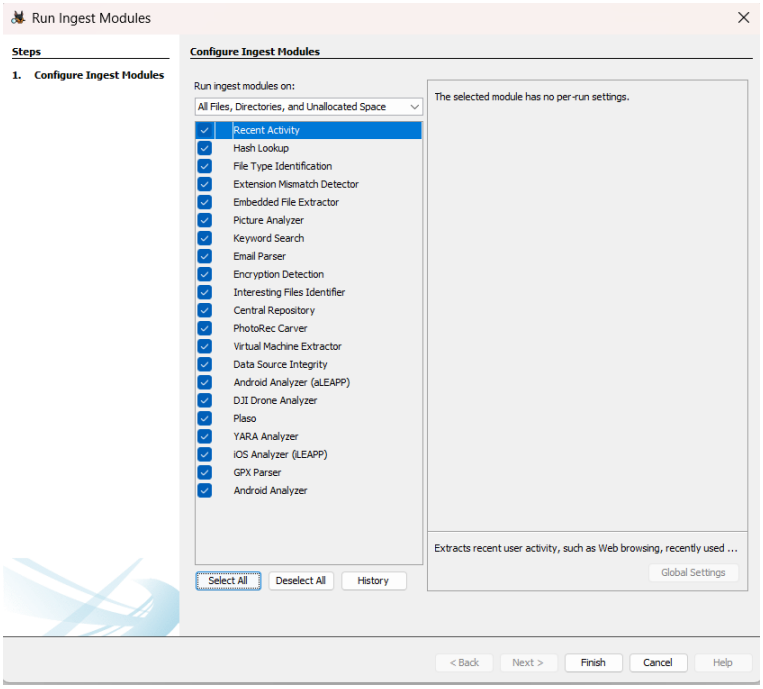


Figure 6: Configuring the Ingest Modules

13. Ensure that all the ingest modules are selected. Please note however, that we are dealing with 'small' DFIs, in reality you might disable some, such as Android Analyzer (aLEAPP), DJI Drone Analyzer, Plaso, YARA Analyzer, iOS Analyzer, GPX Analyzer, Android Analyzer.

14. Note that two of these ingest modules have sub-options which also need to be selected. These are as follows: `Keyword search` : (select all options i.e. phone numbers; IP addresses; email addresses; URLs; credit card numbers) (Figure 6).

15. `Extension mismatch detector` select: check only multimedia and executable files and ensure that skip files without extensions and skip known files are also selected.

16. Click `next`

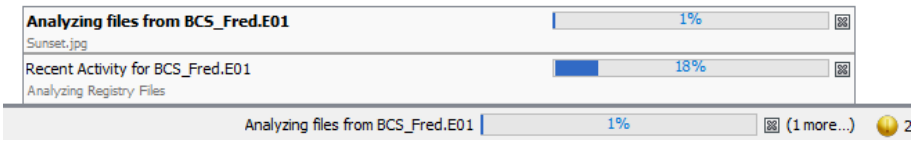


Figure 7: Fine Ingest Analysis

NOTE

It is not necessary to enable all the ingest options. The ingest can be run at any time after a case has been created/evidence added by going through the `tools--Run Ingest Modules--IMAGENAME` options.

For a fuller description of the ingest modules presented at this screen, please see the Autopsy documentation online.

17. At the final screen select `Finish`.

When you reach this screen, note that in the bottom right of the Autopsy window there is a message advising that Autopsy is analysing the image (Figure 7). At times, it might seem like the case analyser is stuck. Click on the `more` link (bottom right), to see that it is actually processing files. During the process, Autopsy is analysing keywords and extracting web search hits. Although you can now begin exploring the DFI, you should not run any searches or add tags until the ingest analysis has completed.

NOTE

Later, if you ever have problems performing a search, you may want to run an ingest on the data source in question. However, be aware of a flaw in some versions of the Autopsy tool which enumerate search hits each time you run an ingest. In other words, a second ingest will double the number of mismatched extensions.

2.1 Adding more evidence to a case

At any point, you can add more evidence by selecting the `Add Data Source` option in the main Autopsy screen. You might want to do this because you want to investigate and view ALL the evidence files relating to a single case at the same time.

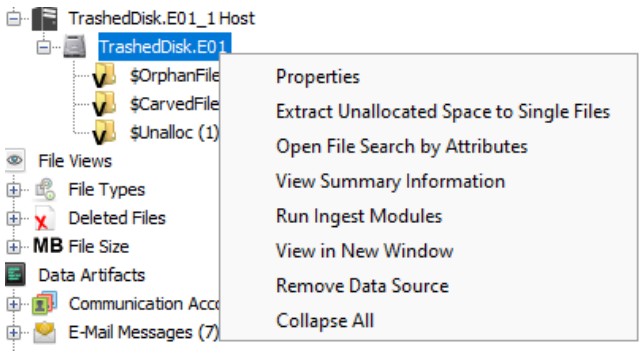


Figure 8: Removing a Data Source

18. Select the `Add Data Source` option from the main Autopsy screen. This brings the Add data dialogue box up for you to follow through as in the previous steps.

19. Follow the steps outlined earlier and add the `animal.e01` image.

20. You can now check that both items have been added by selecting the `Data Sources` icon on the top left of the browser window. This will reveal the names of the evidence files added to the case.

21. A data source can be removed by right clicking on the data source (not the host label) and selecting `Remove Data Source` as shown in Figure 8). This is for information only - do not remove a data source.

2.2 Viewing case information

Case details can be viewed at any time during the investigation as follows:

22. With the case still open, select `Case--Case Details`.

This presents the `Case Details` dialogue box (Figure 9) and allows the user to rename the case and/or delete the case.

Sometimes it is useful to get an overview of the type of data a data source contains. Autopsy has a simple triage facility which reveals the number of images, audio files, documents, executables etc., a data source has.

23. To access this, select the `Case---Data Sources Summary` menu

24. Select the `TrashedDisk.E01` data source. Note that this data source contains 10 documents and 62 images (Figure 10 left). If one were to explore this data source (which we will not do right now), one would find that the 62 images are not user-accessible and are all deleted.

25. Select the `Animal.E01` data source. This data source is more diverse (Figure 10 right), and contains 197 images, a single audio file, 276 documents, 103 executables, and a number of unknown/other files.

2.3 The Data Source Hash

An investigator **must** work on a forensic copy (*digital forensic image - DFI*) of the original evidence source. The investigator must also make clear that he/she worked on a DFI, that the DFI was the same as the evidence seized (unaltered), and prove this through declaring the hashes of the original compared with the DFI. In addition to declaring the hashes, the investigator also declares the name of the DFI investigated, e.g. `Animal.E01`.

The DFI must be unaltered and be an exact provable copy of the original. To achieve this, a hash is made of the original DFI. The hash is stored in the container (for instance in the .E01 or .DD file). The hash is also supplied separately to the investigator. The investigator (or rather the tools) calculate a hash of the DFI provided, the two hashes are compared. If the hashes are identical, then the investigation proceeds as normal (and an explicit statement

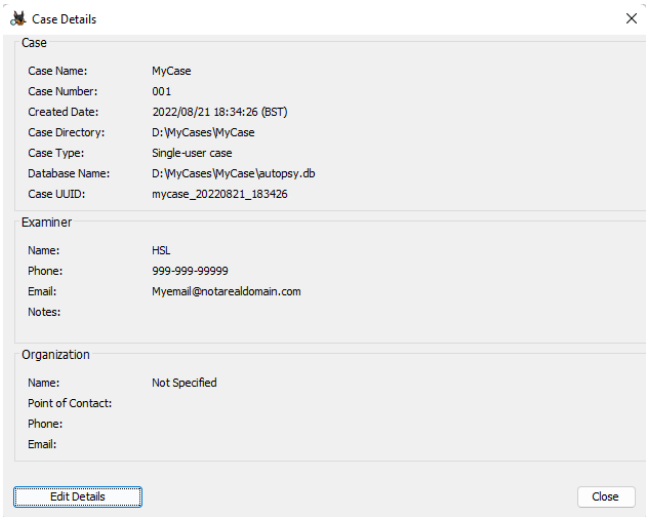


Figure 9: Case details

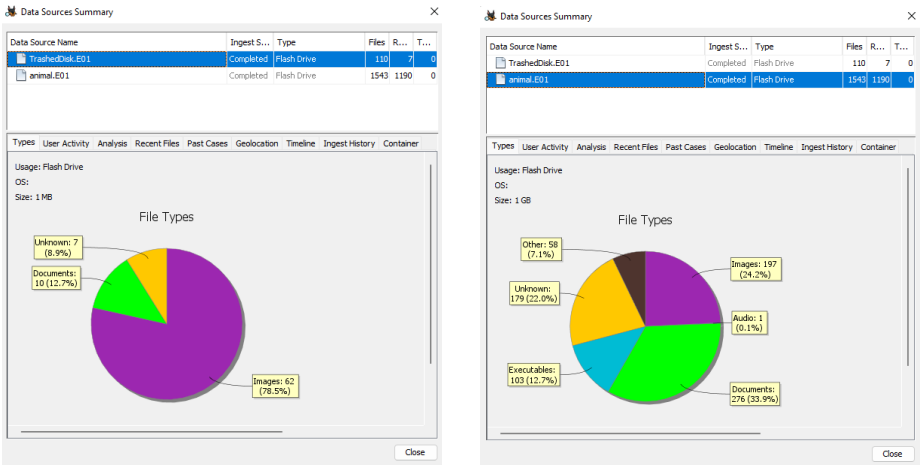


Figure 10: Case details

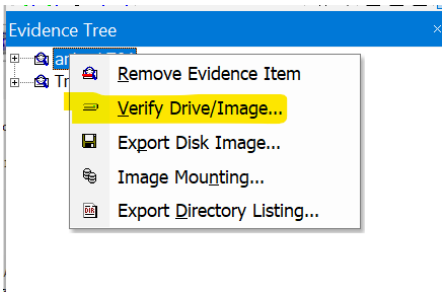


Figure 11: Verifying a DFI

made in the case report to confirm this). If the hashes are not identical, the DFI is referred back to the case manager for further advice.

In this Section, we will verify whether the hashes of the two DFIs we are using can be verified. You can do a hash verification internally within Autopsy by following the guidelines presented here: https://sleuthkit.org/autopsy/docs/user-docs/4.20.0/data_source_integrity_page.html, however, we are going to use this opportunity to introduce FTK Imager. Note, I personally prefer the information provided by the FTK Imager hash verification module.

26. Start up FTK Imager.
27. Access the `File--Add Evidence Item` menu.
28. Select `Image File`
29. Select `browse`

30. Right click on the `animal.E01` DFI and select `Verify Drive / Image` (Figure 11).

31. Once the verification is completed, the results are displayed as shown in Figure 12. This Figure returns the MD5 hash and the SHA1 hash.

32. Repeat this for the `TrashedDisk.E01` DFI.

Note the hashes:
`animal.E01` MD5 Hash: `c00fd4ce8d3b7145243fab14fe608ef1`,
SHA1: `1205eb6f1ca7db056e9b2456d6e50241b31b4ed8`
`TrashedDisk.E01` MD5 Hash: `5fac16f52ca3ccac4cfdb512aeac2b3c`
SHA1: `92906d4f34fdd27a584903d3b4c5c3314f21706e`.

Hashes

When a DFI is created, the tool that creates the DFI calculates a CRC (cyclic redundancy check) of each block of data, and an MD5 and/or SHA1 hash of the entire storage space of the source from byte 0 to the last byte as shown in Figure 13 top. The CRC is stored at the end of each block in the resulting DFI, and the hash is stored in the footer. The hash is referred to as a *Stored verification hash*.

Some of the earlier tools did not have the facility to calculate SHA1 hashes, hence they stored the MD5, but did not store a SHA1. This is probably what has happened in Figure 12 right.

Note also, that although some tools had the provision to calculate both MD5 and SHA1, they asked a user whether they wanted this stored. If a user opted not to store a SHA1, the tool stored zeroes in the DFI where the SHA1 hash should have been. This is what has happened in Figure 12 left.

When *FTK Imager* verifies the hash in the last few steps outlined above, FTK take the data blocks from the DFI and recalculates the hash, this is referred

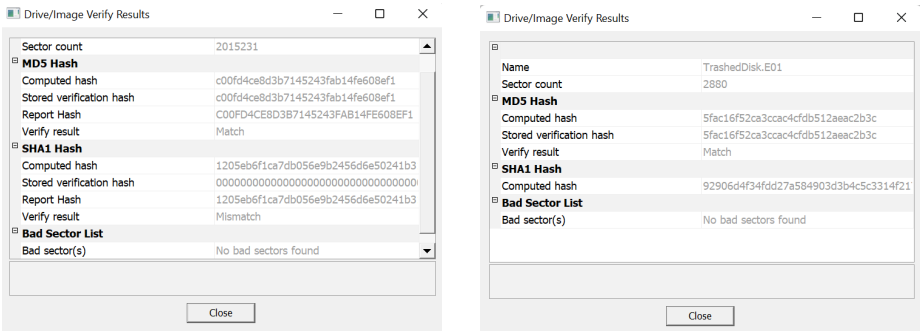


Figure 12: Case details

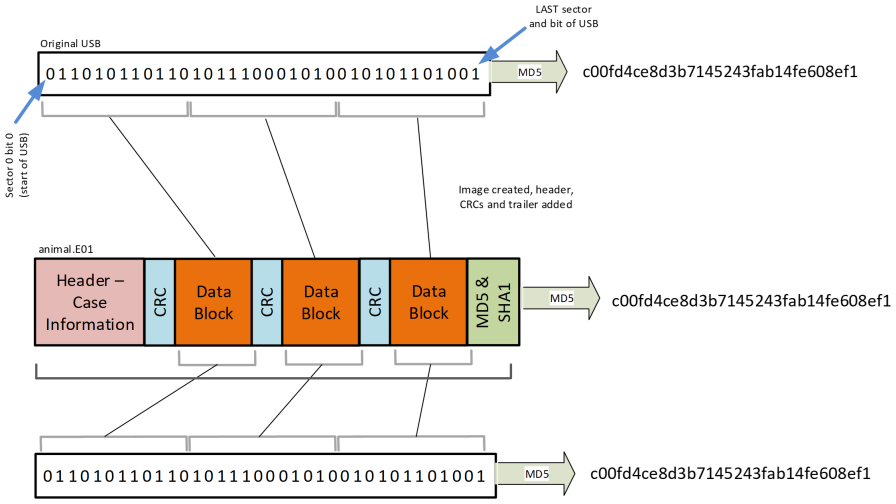


Figure 13: Understanding DFI hashes

to as a *Computed hash*. The *Computed Hash* is compared with the *Stored Verification Hash* and returns a *match* or *mismatch*.

Some DFI creation tools, FTK Imager being an example, also create a text report of the DFI creation process. You can view this in the file `animal.E01.txt`. The contents of this file are as follows:

```
Status:  Completed
Start:  10/30/12 10:46:43AM
Stop:  10/30/12 10:48:03AM
Time:  0:01:20
Name:  animal
Path:  J:\Forensic cases\Animal\animal.E01
GUID: 3EF87E38CF45F049B33E2DCD7819AF49
Acquisition MD5:  C00FD4CE8D3B7145243FAB14FE608EF1
```

We can see from the contents of this file that the MD5 hash is given in upper case and matches the hash in the verification dialogue box presented by FTK (Figure 12 left). This is referred to as a *Report Hash*.

In both cases, The MD5 hashes match. However, the `TrashedDisk.E01` returns a SHA1 hash, but does not confirm whether it is a match or mismatch. Let's try to understand what has happened here.

Not all DFI creation tools create both the MD5 and the SHA1 hash. Figure 12 returns a SHA1 hash for both DFIs, reports a *mismatch* for `Animal.E01` and neither a *match* or *mismatch* for `TrashedDisk.E01`. When the `Animal.E01` was created, DFI creation tool did not create or insert a SHA1 hash. There is no SHA1 hash to compare with, hence Autopsy cannot confirm whether it is a

match or mismatch.

Viewing DFI information within Autopsy

Information relating to the DFI can also be found within Autopsy as follows:

33. In the `tree view`, select the host that contains the DFI for which you wish to check DFI information.
34. The `result view` alters to show the DFIs attached to this host. Select any DFI.
35. In the `content view`, select `File Metadata`. This displays the MD5 and other data relating to the DFI. This view contains more information than the associated text file might contain.

2.4 Closing the case

For the sake of completeness, we are going to close the case file and then reopen the case. There's one student in the room that will not know how to do this :-)

36. Cases can be closed by either: a. Selecting the `Close case` icon on the top left of the screen, or selecting `Case--Close Case`

    This takes you back to the welcome screen.
37. From this screen select `open case`
38. Navigate to the directory that contains the `DeleteMe` case file. It is named `DeleteMe.aut`.
39. Select this file and select `open`

The case directory is very important in an investigation. Recall, that you have created a case and defined the case directory.

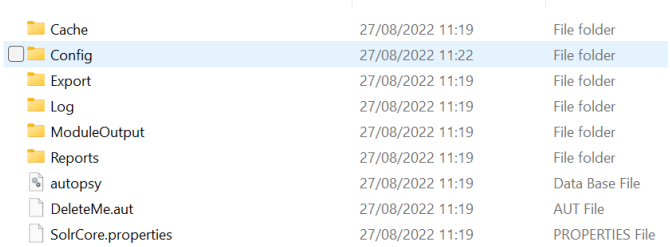


Figure 14: The Case directory

40. Navigate to that directory (Figure 14).

This directory contains six folders (`Cache, Export, Log, ModuleOutput, Reports` and `Temp`), a database (`autopsy.db`) file and the case file (`Deleteme.aut`). The structure and purpose of the directories can be described as follows:

- #`Cache`. Contains working cache to help Autopsy
- #`Export`. The default directory for exporting files (right click file, select extract)
- #`Log`. Keeps a running log of the case
- #`ModuleOutput`. Stores files extracted as a result of the ingest process
- #`Report`. The default report storage directory
- #`Temp`. Contains temporary files used when Autopsy is running.
- `autopsy.db` is a database file which stores all the case configuration data to include bookmarks, searches and any other data pertinent to that particular case. This can be accessed using an SQL browser (DB Browser for SQLite for instance)
- `Deleteme.aut` is an XML file that stores high level settings relating to the case.

41. Open this file with a text editor.

You will notice that this file stores the 'high level' details entered when you created the case such as the case name, number, examiner name etc. This file does not record the name of the image, however, it does record the name and location of the case database file (`autopsy.db`).

For a case to operate correctly, you need the case directory (intact) and the image file. If you move the image file to another location, Autopsy will prompt you for the file when you open the case and then remember it. In other words, you can move the image file reasonably easily.

However, if you move the case (i.e. the case directory) to another location, Autopsy will present errors when you try to open the case. If you move the case, you must alter the name of the directory that contains the database file in the `Database` field in the XML file.

You are now going to create a case on your own. The ingest process is likely to take around twenty minutes. You may want to complete the next step just before a break, or at the end of a lesson (or indeed in your own time).

3 Understanding the Autopsy Environment

Materials

A pre-created ingested case directory called `Stanley` which requires the DFI: `Stanley.E01` (also provided in the directory)

In this tutorial you will familiarise yourself with the Autopsy environment, and in particular understand the different views and methods of presenting the data pertaining to the case.

The Autopsy environment can be split into four basic components, these are shown in Figure 15 and discussed in further detail below.

1. Open the `Stanley` case.

   We are now going to explore the environment.

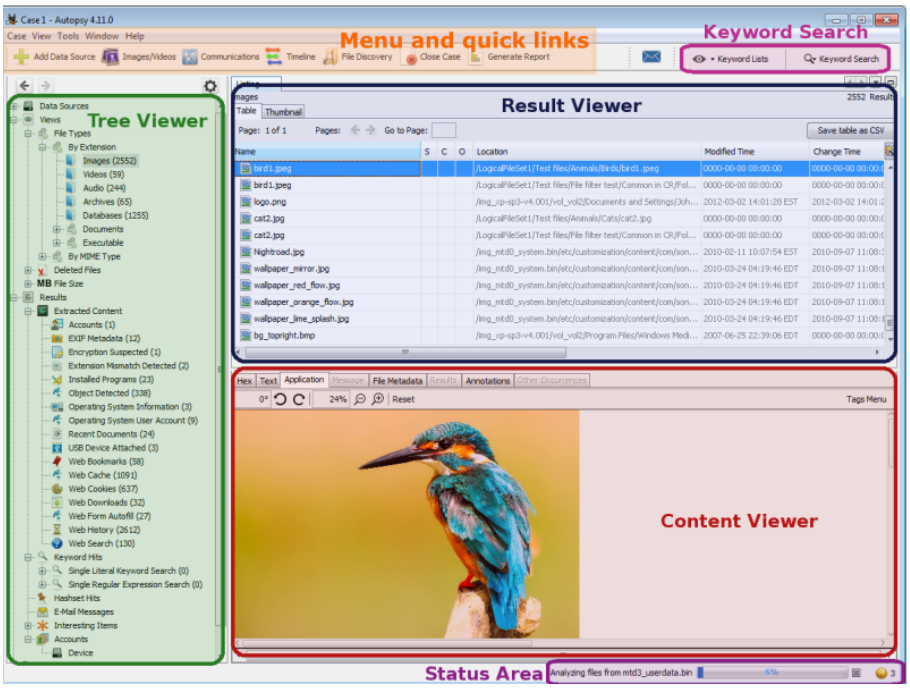


Figure 15: The Autopsy Environment[1]

[1] Adapted from: https://sleuthkit.org/autopsy/docs/user-docs/4.18.0/uilayout_page.html NB: This screenshot is from v4.11.0 and may not be identical to the version you are using, the fundamental elements remain the same.

The Menu. Like most menu systems, the Autopsy menu enables the investigator to utilise features in the software quickly and conveniently. Below the menu we see a set of *quick links* which are the set of icons at the top of the UI. These link to several useful features. One of the most useful features is the `Keyword List` which we shall explore later in this module.

3.1 Tree viewer

The `Tree Viewer`, situated on the left of the interface, is divided into `Data Sources`, `File Views`, `Data Artifacts`, and `Analysis Results`.

3.1.1 Data Sources

The `Data Sources` view presents the DFIs that have been attached to this case and the directory structures of each of these DFIs. Each DSS is presented with its image file name, the tree structure below it presents the partition structure of the original digital storage system.

Exploring a data source The `data sources` view presents technical data pertaining to the volumes contained within the DFI. This data is derived from the partition table on the original DSS.

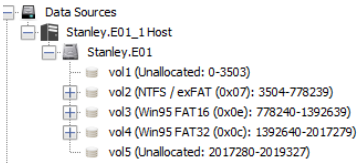


Figure 16: Data sources

Notice that this DFI has 5 volumes as shown in Figure 16. `Vol1` and `Vol5` are unallocated. This means that these volumes are not recorded as having been formatted and containing usable data according to the partition table. We are always wary of this, and will want to check that this is actually the case by examining the unallocated volumes. It is possible they contain important data.

It is common to report the structure as the investigator sees it, albeit at a high level. The reason for this is for all parties concerned to establish a common footing on what the structure of the DFI is. There is no need to report sector start/end, but the court finds it useful to know the number of volumes their file system, usable/unallocated spaces, and especially if artefacts exist in unallocated space.

`Vol2, Vol3` and `Vol4` are formatted and were usable volumes. They contained NTFS, FAT16, and FAT32 file systems respectively. Their start and end sector lengths are provided.

2. Select and expand the `Stanley.E01` DFI
3. In the `Result Viewer` select the `Table` view (Figure 17)

Exporting the table view

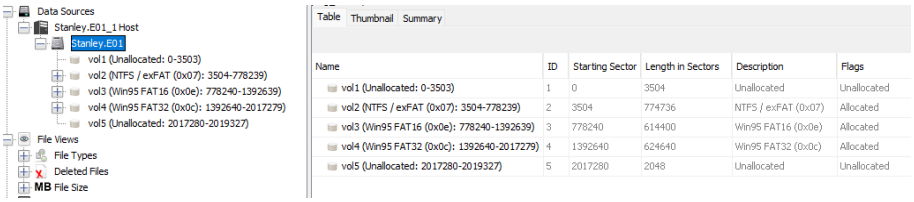


Figure 17: Data sources presented in table view

The `Table View` presents the same detail. However, this has an added feature in enabling an investigator to export the table view into a CSV file - which can then be incorporated within a report. This can be especially useful when dealing with reasonably complex directories which contain deleted files, deleted directories, and files of interest.

There are two ways of exporting the table view.

4. Select `vol2...`
5. Select the `Save Table as CSV`
6. Save the table with filename `SampleExport1`
7. Open this file and examine its contents (just to check it worked)

   Now let's try the second method in which you only export selected files.
8. Select five files using the CTRL+Click
9. Right click on any one of these files and select `Export Selected Rows as CSV` Figure 18, bottom
10. Save the table with filename `SampleExport2`

Viewing a data source summary

Selecting a data source in the `Data Sources` view will present the contents of that volume in the `Results View` (Figure 19). The `Summary` tab in the `Results`

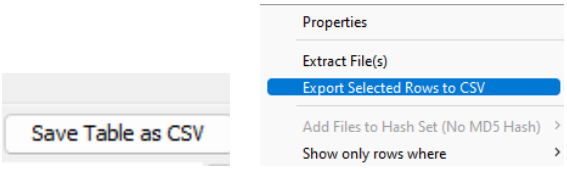


Figure 18: Exporting the `Table View` or selected rows as CSV

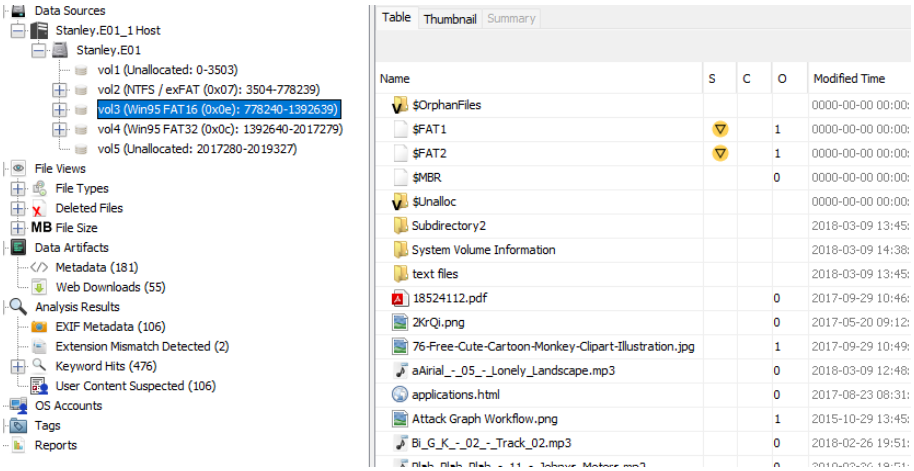


Figure 19: Viewing file in the `Results Viewer`

`View` presents a graphic summary of the types of files present on the data source (Figure 20). Note that the `Summary` tab only becomes activated when you have selected a DFI.

Understanding the data source `Table View`

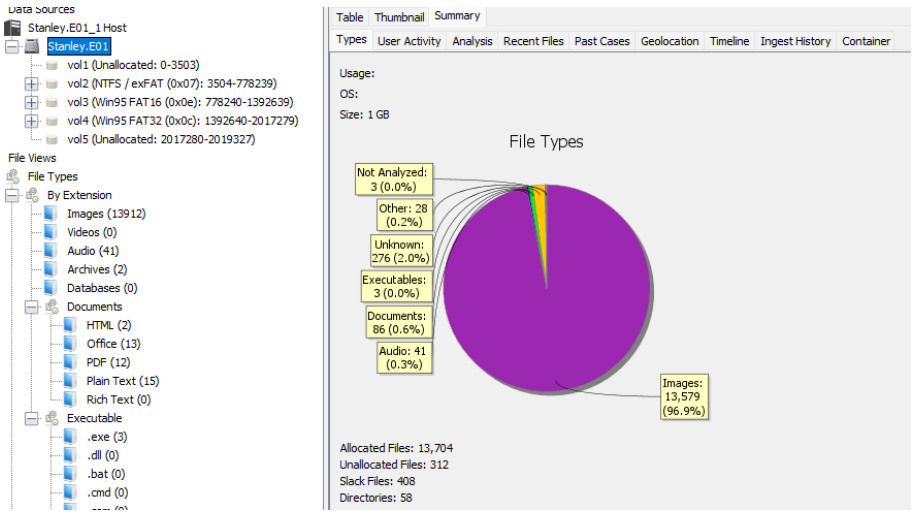


Figure 20: Viewing the volume file summary in the `Results Viewer`

The Table View alters depending on what you have selected and can present up to 20 columns of information.

11. Select Vol2....

The Table View alters to represent the : Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(DIR), Flags (Meta), Known, MD5 Hash, SHA-256 Hash, MIME Type, Extension, and Location

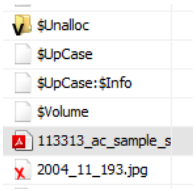


Figure 21: Files represented with three types of icon

Note that in the list presented in Table View, the Names column presents four types of files, those without an icon, those with a red cross, those that begin with a $, and those represented with a 'V' (Figure 21. Files represented with a red cross are deleted files which may or may not be recoverable. Files Represented with a 'V' are virtual files. These are files that did not exist in the original DFI, but have been 'created' by Autopsy. Examples of this include attempts to represent Unallocated space ($Unalloc) and Orphan files ($OrphanFiles).

Filenames that begin with a $ (e.g. $AttrDef, $BadClus, $MFT) are not ordinarily viewable in Windows File Explorer. They are hidden system files which are essential for a system operate effectively. Autopsy reveals these for the investigator.

Let's explore the Table view, or at least elements of it that are not immediately obvious.

12. Select Vol2....

    The S column highlights items that have been auto-scored by an ingest module, or manually identified as a notable file. These are files that are not bookmarked (i.e. 'should be included in the report') but are files the investigator wants to come back to and investigate further before deciding whether or not to include them.

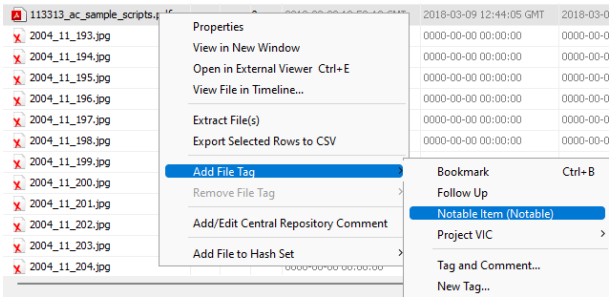


Figure 22: Scoring items

13. Right click on 113313_ac_sample_scripts.pdf from the Table View (Figure 22)
14. Select Add File Tag--Notable Item (Notable). Note that the S column for this file now has an exclamation mark.
15. Remove the notable file tag by following the same procedure

The C column indicates whether a comment has been added to a file. You will do this later on.

The O column indicates the number of duplicate occurrences of a file in the volume.

16. Select vol2.../sample images/EXIF

    Note that 5 of the files in this directory have 1 duplicate occurrence.
17. To discover where the duplicate occurrence is, select 2000px-Census-2000-Data-Top-US-Ancestries-by-County.svg.png
18. in the Result View, select the Other Occurrences tab.

    This reveals that this file also exists in /sample images/photosdfi/image 06.png

At this stage, we assume that you already understand the MACc times (modified, accessed, changed, created), but we will remind ourselves of the difference between the modification and changed time. The modified time is the time when the contents of the file were last modified, and change time is the time when the file's inode was changed, for example, the file permissions were changed. The change time is file specific.

The remaining columns are reasonably straightforward to understand.

3.1.2 Content Views

The Content View is activated when a file is selected in the Result Viewer. The Content View is context-aware. The tabs alter depending on the content selected in Result Viewer and on the ingest modules that have been executed on the case.

The Content View presents a file in multiple views. The content view is divided into several tabs as follows: Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurences.

Hex

Often an investigator needs to analyse an artefact in hex format. Autopsy includes a basic hex-viewer. For more advanced functionality, I recommend *HxD* or *Hex Workshop*. I use both. Hex Workshop has an excellent colour mapping

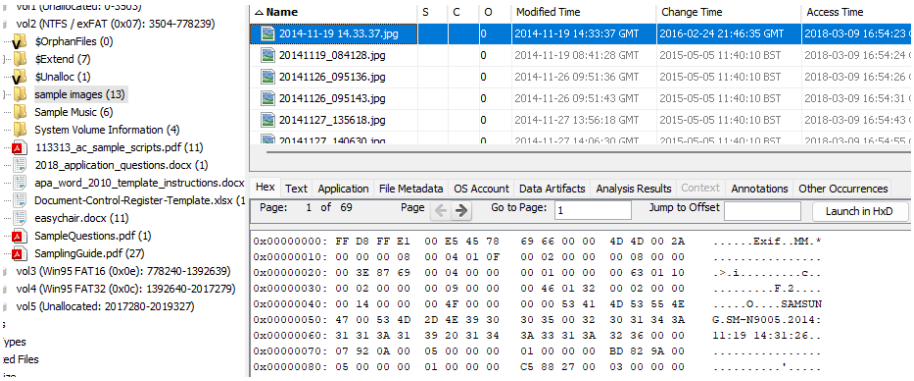


Figure 23: The Hex Viewer

and bookmarking facility which HxD does not. However, HxD is faster (and a bit easier to navigate).

19. Select `Stanley.E01/vol2.../sample images`
20. Select `2014-11-19 14.33.37.jpg`
21. Select `Hex` in the `Content view`

The format of the hex representation (Figure 23) is reasonably consistent with most hex viewers in that the offsets are listed (top/left), each byte of data is represented as two hex digits, and the right hand side of the screen represents the ASCII character for each HEX.

Hex viewers count file locations using the 0th byte as an offset. Hence, jumping to byte 1000, is calculated from the 0th byte. You can navigate the file a 'page' at a time by selecting the left/right arrows, or go to a specific byte offset. The `hex` tab also provides an option to `Launch in HxD` if you have installed HxD.

Text

The Text tab has three sub tabs for displaying the text contained in the selected item.

Strings

The `Strings` view presents the file as raw unformatted text. This can be useful for many file types - but quite unhelpful for others. For instance, viewing a `.docx` file in this format is quite unhelpful, where as viewing an image which has metadata is somewhat helpful. This view is especially helpful for code based files such as `.html`. This view is useful for textual/document files, but not very helpful for photos, videos, audio etc.

22. Select the file `Q0.2TutorialPart0.1.html` from: `File Views--File Types--By MIME type|text|html`
23. Select the `Strings` view in the `data view` selection tab

Note that this presents the `.html` file in its raw html format.

Application

The `application` view attempts to present the file using Autopsy's file convertor function.

24. Select `2014-11-19 14.33.37.jpg` in `Stanley.E01/vol2.../sample images`
25. Select `Application` in the `data view` selection. The `application` tab in the `content viewer` displays the contents of this file.

The `Application` view can also play mp3 and some video files

26. Select `vol2.../Sample Music/09_-_Imagine.mp3`
27. Select `Application` in the `data view` selection
28. The 'play' button at the bottom of the screen will enable you to play this file

File Metadata

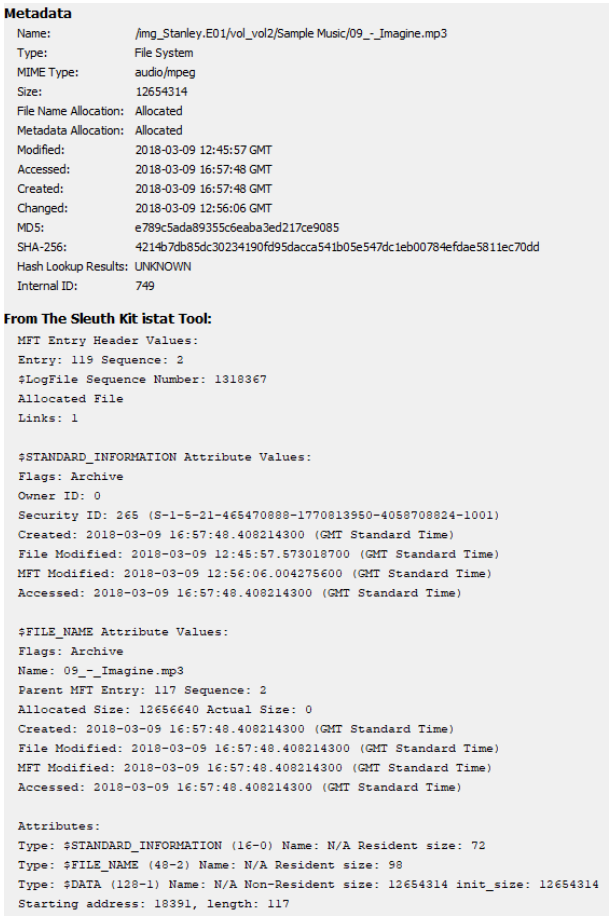
The `File Metadata` view presents the metadata associated with the file from a file system viewpoint. The data in this view is extracted from the Master File Table, which we will cover later in this module.

29. Select `vol2.../Sample Music/09_-_Imagine.mp3`
30. Select `File Metadata` in the `Content View` tab

The `Content View` changes to reflect a range of file metadata (Figure 24). This view repeats some of the data presented in the `Table View` when a directory is selected such as modified, accessed, created, and changed times. The MD5 and SHA256 associated with a file, are also presented. Further down, more information is extracted from the MFT to include the *Standard Information (SI)* and *File Name (FN)* attributes. Finally, further down the list, (Figure 24 bottom), we see the cluster addresses associated with the file.

OS Accounts

If the information is present/exists, the `OS Accounts` tab displays the operating system account information associated with a file.



Metadata

Name:	/img_Stanley.E01/vol_vol2/Sample Music/09_-_Imagine.mp3
Type:	File System
MIME Type:	audio/mpeg
Size:	12654314
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-03-09 12:45:57 GMT
Accessed:	2018-03-09 16:57:48 GMT
Created:	2018-03-09 16:57:48 GMT
Changed:	2018-03-09 12:56:06 GMT
MD5:	e789c5ada89355c6eaba3ed217ce9085
SHA-256:	4214b7db85dc30234190fd95dacca541b05e547dc1eb00784efdae5811ec70dd
Hash Lookup Results:	UNKNOWN
Internal ID:	749

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
Entry: 119 Sequence: 2
$LogFile Sequence Number: 1318367
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 265 (S-1-5-21-465470888-1770813950-4058708824-1001)
Created: 2018-03-09 16:57:48.408214300 (GMT Standard Time)
File Modified: 2018-03-09 12:45:57.573018700 (GMT Standard Time)
MFT Modified: 2018-03-09 12:56:06.004275600 (GMT Standard Time)
Accessed: 2018-03-09 16:57:48.408214300 (GMT Standard Time)

$FILE_NAME Attribute Values:
Flags: Archive
Name: 09_-_Imagine.mp3
Parent MFT Entry: 117 Sequence: 2
Allocated Size: 12656640 Actual Size: 0
Created: 2018-03-09 16:57:48.408214300 (GMT Standard Time)
File Modified: 2018-03-09 16:57:48.408214300 (GMT Standard Time)
MFT Modified: 2018-03-09 16:57:48.408214300 (GMT Standard Time)
Accessed: 2018-03-09 16:57:48.408214300 (GMT Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 98
Type: $DATA (128-1) Name: N/A Non-Resident size: 12654314 init_size: 12654314
Starting address: 18391, length: 117
```

Figure 24: File Metadata

Data Artifacts

The `Data Artifacts` tab is only activated when one of `Metadata` or `Web Downloads` is selected in `Data Artifacts` in the `Tree Viewer`. We will come back to this later.

Analysis Results

The `Analysis Results` tab shows all analysis results associated with the item selected in the result viewer. The `Analysis Results` tab is only activated when one of corresponding links is selected in `Analysis Results` in the `Tree Viewer`. We will come back to this later.

Context

The `Context tab` shows information on where a file came from and allows you to navigate to the original result. For example, it can show the the URL for downloaded files and the email message a file was attached to.

Annotations

The annotation feature can be helpful in enabling an investigator to record thoughts/comments about an artefact.

The `Annotations tab` shows information added by an analyst about a file or result. It displays any tags and comments associated with the file or result, and if the Central Repository is enabled it will also display any comments saved to the Central Repository.

31. Right click on `vol2.../Sample Music/09_-_Imagine.mp3`, and select `Add/edit Central Repository Comment`
32. In the dialogue box, enter the words: *This is a comment made by an investigator when analysing this file* (Figure 25 second figure down)
33. Select `Annotations` in the `Content View` tab

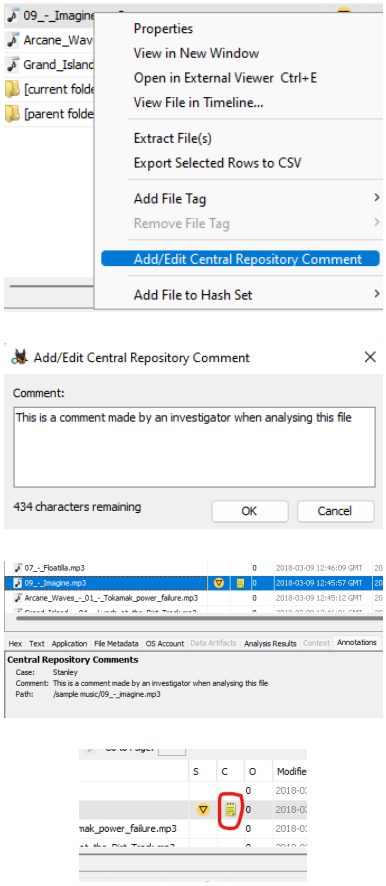


Figure 25: Adding a file comment

The comments just added are presented. Note that a 'notepad' is now presented in the 'comment' column in the `Table View` (Figure 25 bottom).

Other Occurrences

The `Other Occurrences` tab reveals, as the name says, other occurrences of the same file. This is useful to know as the same file may exist in another directory, and then be copied into a collection in another. We can trace which file existed first and build a picture around file movements.

Autopsy determines other occurrences by comparing file hashes.

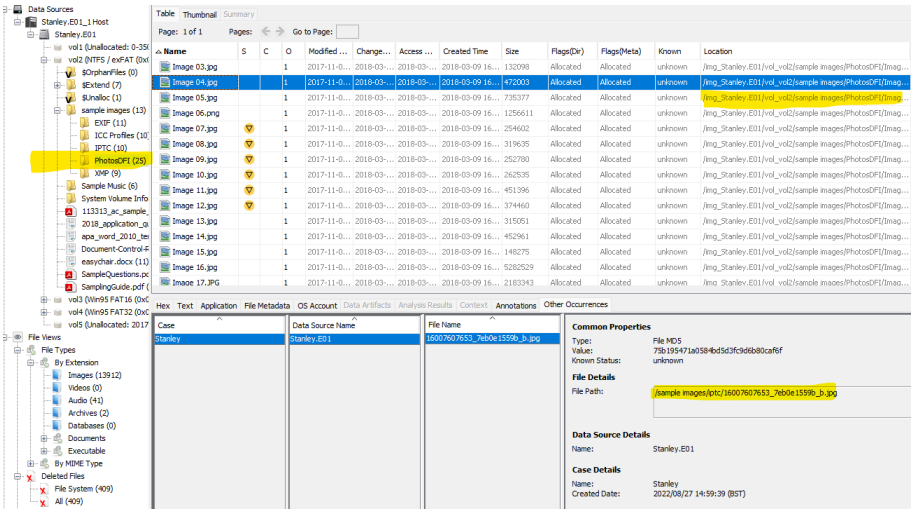


Figure 26: Viewing files in the `Other Ocurrences` tab

34. Select `Data Sources--Stanley.E01_1 Host--Stanley.E01--vol2...--sample images--PhotosDFI`

35. Select `Image 04.jpg`

36. Right click on this file and select `Properties`

    The MD5 for this file is `75b195471a0584bd5d3fc9d6b80caf6f` and the SHA1 is `afcd5066b38c713a7115d37cf059d358cd14b92f11f632c9e7c21913040c6de8`

37. Select `Other Occurrences`

    This reveals that the same file exists in the `vol2...--sample images--iptc` directory, but has a file name `16007607653_-7eb0e1559b_b.jpg`

38. Find that file and compare the hashes. Are they the same file?

3.1.3 File Views

File Types

The `File View` (Figure 27) provides a summary of the presence of specific file types. The file types can be viewed *By Extension, By MIME type, by deleted files* and *by file size*. We are not going to explore each and every one of these. For now, we are going to explore how the `result view` responds to a selection in the `file view`.

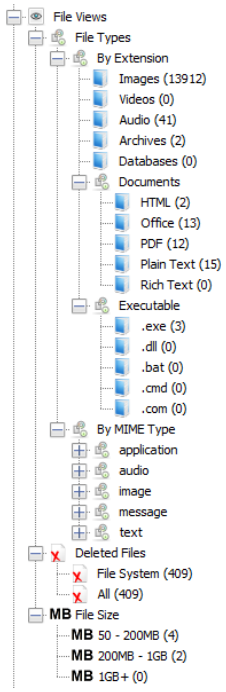


Figure 27: The File View

39. Select the following `File views--File Types--By Extension--Images` A list of files are presented in the `result view`. These are files that have a common photo extension, for example .jpg, .bmp, .PNG

40. Select the `Tumbnail` tab in the `result view`

41. The first thumbnail screen might not present any files as they fall in the category described above. You will have to scroll forward to the third thumbnail screen to see the first thumbnail.

    Where it can, Autopsy will present a thumbnail of files on this volume. We say where possible because forensic tools are often not able to view files, where they are deleted files where portions of the file are no longer available.

Note that the `File views--File Types--By Extension--Images` view suggests that there are 13,912 images on this volume. Compare this with the `File views--File Types--By MIME Type--Image` view. This is proposing that there are 1+623+12449+504+1+2=13,580 image files, a discrepancy of 332 files. Why is this?

The `File views--File Types--By Extension--Images` view reads file extensions and presents any file that has a photo extension. The `File views--`

File Types--By MIME Type--Image view however, is more intrusive, this view examines the *file signature*. Although file extensions can be easily changed, the file signature is a 2 to 8 (there may be more) byte file header which defines the file type. This is discussed in more detail later in this module.

Deleted Files

The Deleted Files view reveals deleted files on the File System and in the whole image (All).

42. Select File views--Deleted Files--File System

    This reveals 409 files which have been deleted on this DFI.

43. Observe the file sizes of these in the Result Viewer and notice that many have a file size of 0.

44. Select 2004_11_193.jpg and now observe the Content Viewer (Figure 28 top). Note that the Hex, Text and Application tabs are greyed out. They are not available. This is because there is nothing to show. These files are well and truly deleted, they are not recoverable.

45. Scroll down to a file with the name 2005_07 (India)_250.jpg. It might take a fair bit of scrolling to find this file.

    Notice that this file can be viewed by selecting the Application tab in the Content Viewer (Figure 28 middle).

    This file has a non-zero byte size. But that is not the only reason it is viewable.

46. Now find the file: 2005_07 (India)_251.jpg. This file also has a non-zero file size, but is NOT viewable.

47. Finally, find file: 2005_07 (India)_266.jpg. Notice that the Content Viewer displays part of this file, but not the rest 28 bottom)

Recall:

- 2002_11_193.jpg is a zero byte deleted file and is not viewable.
- 2005_07 (India)_250.jpg is a deleted non-zero byte file, and is viewable.
- 2005_07 (India)_251.jpg is a deleted non-zero byte file, but is not viewable.
- 2005_07 (India)_266.jpg is a deleted non-zero byte file and is partially viewable.

We will refer to these as 193, 250, 251, and 266 (last 3 digits in the filename).

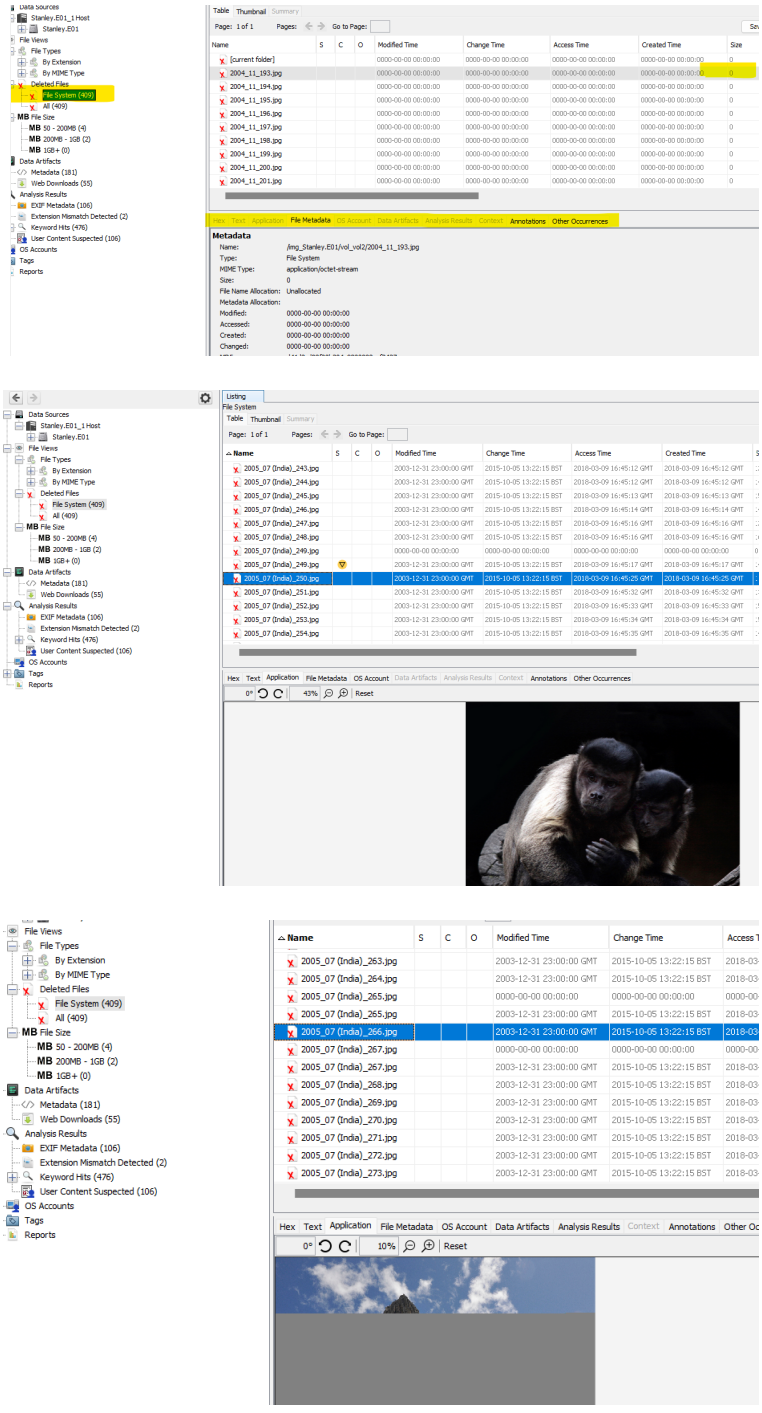


Figure 28: Viewing deleted files in the `Content Viewer`

193, is not viewable because it has a zero file size. The file name still exists in the *master file table*, there is an entry for it therein. The entry specified the name of the file with associated dates. The entry might even point to clusters (we will cover this later in the module). The file is recorded in the master file table as having zero bytes, because the file does not actually exist on the volume.

250 exists in the master file table (MFT). The MFT record allocates some clusters to this file (and therefore a file size). The file header for this file is intact. The file is viewable.

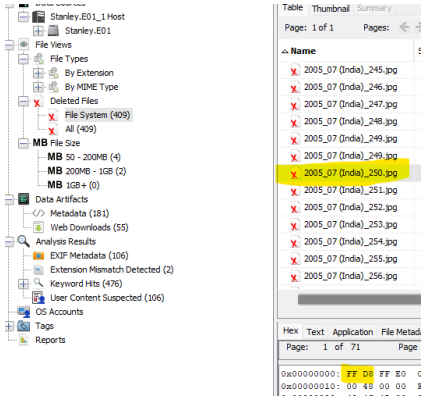


Figure 29: The headers of 2005_07 (India)_250.jpg

48. Select 2005_07 (India)_250.jpg

49. In the Content Viewer select the Hex tab. Note that the first two bytes for this file are FF D8. This is the JPEG file signature indicating that this is a JPEG file. (Figure 29).

50. Select 2005_07 (India)_251.jpg.

51. In the Content Viewer select the Hex tab. Note that the first two bytes for this file are 5B EF. This is not a JPEG file header, in fact I'm not sure whether this is a valid file header for any type of photo. It is not viewable. We could experiment with changing the file signature (judging by the contents, it is a lot more than the signature that will need changing), maybe we may be able to recover it.

52. Select 2005_07 (India)_266.jpg

53. In the Content Viewer select the Hex tab. Note that the first two bytes for this file are FF D8. This is a JPEG file signature indicating that this is a JPEG file.

So why can we only view part of this file? In this case, although some of the clusters allocated to this file are still accessible, others are not, they have been overwritten. Autopsy has done the best that it can to present this file.

You will have noticed that whenever you select a file in Table View, the Content View tab keeps defaulting to Application. This can be annoying, especially when say we just want to analyse a set of Analysis Results. We can 'fix' this so that it stays on the last selection as follows:

54. Select Tools--Options--View

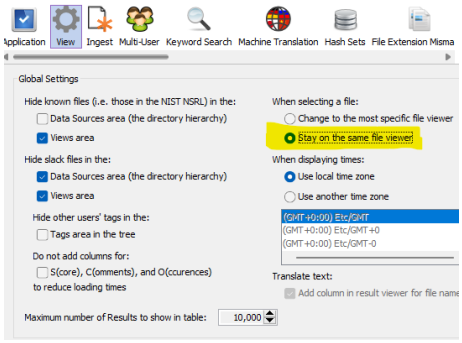


Figure 30: Staying on the same file view

55. Select `Stay on the same file viewer` (Figure 30)

File Size

The `File Size` view presents files according to the file size divided into three categories, files sizes between: 50 - 200MB, 200MB - 1GB, and 1GB+

3.1.4 Data Artifacts

Metadata

The `metadata` view link attempts to extract file metadata and present this to the investigator in the `Content Viewer`. This feature can presently be described as *in development* as the metadata presented is often quite lacking.

56. Select `vol4.../Templates/garden-rose-red-pink-56866.jpeg`
57. Select `Data Artifacts` in the `Content Viewer` (Figure 31)

    Note the limited metadata presented in this view. This is not a comprehensive list, possibly not even very useful. More metadata is accessible using other tools, for example, a simple Windows view.
58. Right click on `garden-rose-red-pink-56866.jpeg` and select `Extract File(s)`
59. Save the file
60. Right click on the saved file and select `properties`
61. Select the `Details` tab, scroll down and note that the *Camera Maker* is NIKON CORPORATION. Further metadata is presented herein.

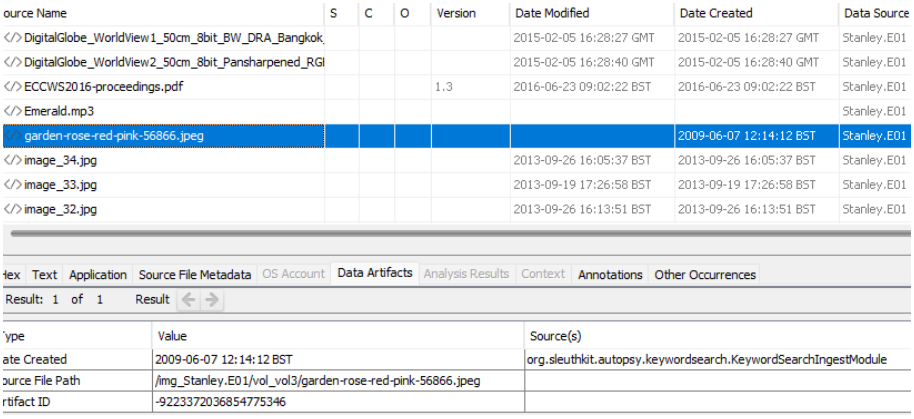


Figure 31: Viewing Metadata

Web Downloads

The `Web Downloads` link presents likely download sources for some of the files within the DFI. This data is derived from the Zone.Identifier file created in some volumes.

62. In the `File views--File Types--By Extension--Images` select the file: `G704031893.jpg`.

    Assume that this (deleted) file is a file of interest, and we want to know where it came from.

    We can see that this file is not accessible, it cannot be viewed. Let's see if we can identify where this file may have come from

63. In the `tree view` (not the `content view`), select the `Data Artifacts--Web Downloads` link

64. In the Result Viewer window, select `G704031893.jpg:Zone.Identifier`

    The `Data Artifacts` tab in the `Content Viewer` outlines that this file was downloaded from `http://www.graphicobsession.com/telechimg.php?FTS=1&R=7b571162932ebd9eeedec615ddf5a1b040618ee50&F=G704031893` It's a long shot, but let's see if this file is still there.

65. Access the url `http://www.graphicobsession.com/telechimg.php?FTS=1&R=7b571162932ebd9eeedec615ddf5a1b040618ee50&F=G704031893` using your browser

    This returns a blank. However, a Google search for the photo `G704031893` (Figure 32) reveals the photo at:

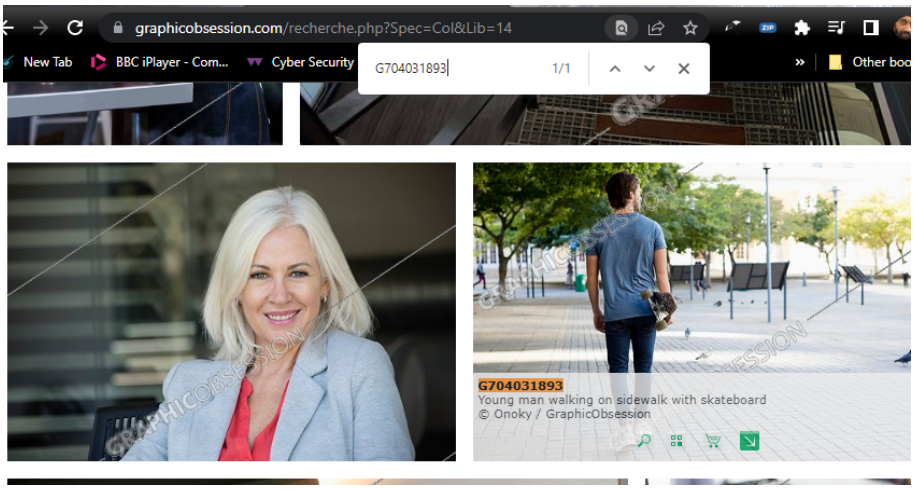


Figure 32: Finding a potentially downloaded file

https://www.graphicobsession.com/fiche.php?PR=%2Frecherche.php%3FIdRech%3D6777240%26Page%3D1%2317&I=17696521&C=nu&TL=REC&IG=6777240&II=17&Ord=

You could now compare the hashes of both files to see if it is the same file.

3.1.5 Analysis Results

.

This section is divided into `EXIF Metadata`, `Extension Mismatch Detected` and `Keyword Hits`

EXIF Metadata

While the `Metadata` section earlier did not convey much useful metadata, this section is a bit more useful - but could nevertheless be improved significantly.

66. Select `EXIF Metadata`
67. The first file in the list in `Table View` should be `2014-11-19 14.33.37.jpg`, select this file.
68. In the `Content Viewer` select the `Analysis Results` tab.
69. The metadata reveals that this photo was taken with a SAMSUNG SM-N9005 (Figure 33 left).

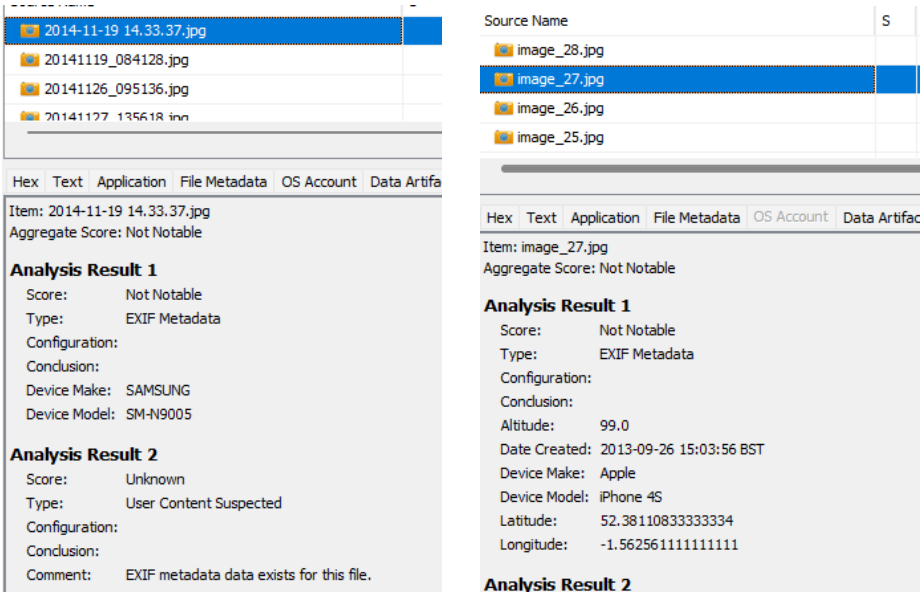


Figure 33: Viewing metadata in Autopsy

70. Now select file `image_27.jpg`. The file metadata in this case reveals the make/model (Apple iPhone 4S) as well as the latitude and logitude (52.38110833333334 and -1.562561111111 111) (Figure 33 right)

Extension Mismatch Detected

Operating systems generally recognise files from the extension of a file, the operating systems uses this to determine how to open the file. It searches for the application program that is associated with that particular file type and then uses it to open the file. So for instance, if we assume a file named: `picture.jpg`, the operating system looks at the extension `.jpg` and opens the file using the program associated with it – which might typically be *Windows Paint*. If the extension of this program is changed to `.doc`, the Windows operating system will try to open the file with the *Microsoft Word* application – which in this case will cause an error.

This means that a user may be able to 'hide' particular files simply by changing the extension. Forensic investigation tools allow investigators to interrogate file structures and check for such inconsistencies. Whilst the file extension is a useful mechanism for determining the file type, a much more useful measure is the header of the file. The header comprises of a number of bytes which lead up to the actual data in the file, the format of the header is defined in accordance with agreed standards. At this point we are going to proceed to view the

header of two types of files – JPG and GIF files. Before we do that, note that https://en.wikipedia.org/wiki/List_of_file_signatureswikipedia outlines some of the more popular file signatures.

These hexadecimal codes are the essential sections of the file headers which tell us what type of file we are viewing. This means that although a file extension may have been changed (to try to hide the file), the headers will tell us what type of file it actually is.

An investigator cannot be expected to browse through all the files in a DFI to identify mismatched extensions. Autopsy includes a feature to identify mismatched extensions.

71. Select `Extension Mismatch Detected`
72. Note that two files have been identified as having mismatched extensions.
73. Select the file named `Payroll.xls`
74. The `Table View` alters to reveal some information about the type of file this actually is. The `Table View` proposes that the *'File has MIME type of application/pdf'* (Figure 34).
75. The `Content View` presents what appears to be a PDF.
76. Select the `Hex` tab in the `Content View`. This reveals that the first four bytes of this file are `25 50 44 46` - the file signature for a PDF

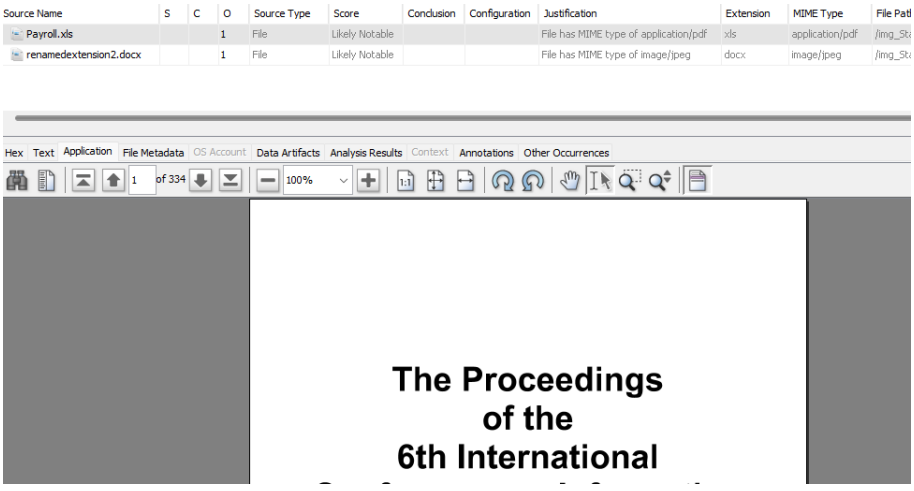


Figure 34: Viewing mismatched extensions

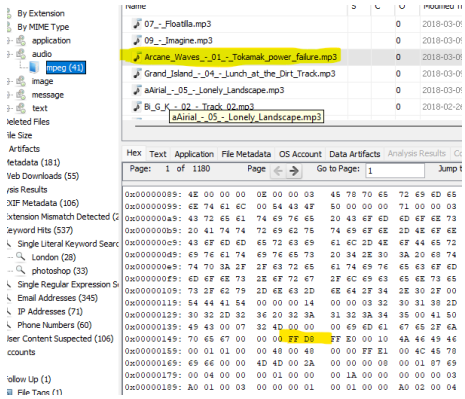


Figure 35: Embedded files and metadata

77. The second file in the `Extension Mismatch Detected` is `renamedextension2.docx`. Select this file to reveal that the file is actually a JPEG.

78. Select the `Hex` tab in the `Content View`. This reveals that the first four bytes of this file are `FF D8` - the file signature for a JPEG

Embedded files

Some files contain embedded files. i.e. files within files. A good example of this are MP3 files which may contain album art, often in JPEG format

79. Select `File Views--File Types--By MIME Type--audio-MPEG`

80. Locate the file `Arcane_Waves_-_Tokamak_power_failure.mp3`

81. Go to offset 137 and notice the presence of the JPEG code `FF D8` (Figre 35). This exists here because this MP3 has embedded artwork. You can check this if you want by extracting the file and viewing in an MP3 app

Keyword Hits

The `Keyword Hits` link presents the result of some of the ingest functions and also your searches.

82. Pull down the `Keyword Search` menu at the top right of Autopsy.

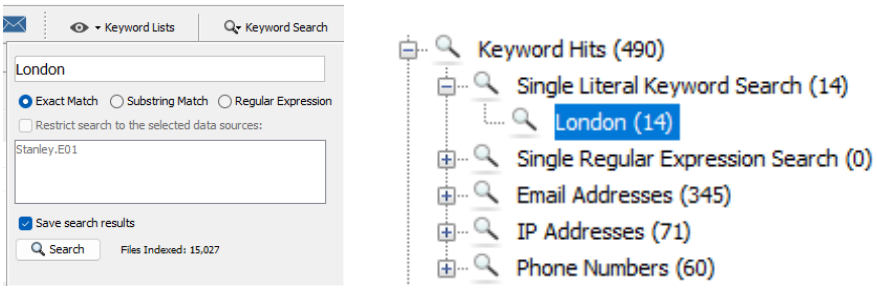


Figure 36: Keyword Hits

83. Type in `London` and press return (Figure 36 left).
84. Autopsy performs a quick search for this term, and then adds it to the results in the `Keyword Hits`
85. Select the + next to `Single Literal Keyword Search` (Figure 36 right)
86. Select `London`. The `Table View` alters to return the list of keyword hits for the word 'London'. We will explore keyword searching later in the module.

NOTE

If you want to save the result of a search, you must select `Save search results`. If you do not, the result of the search will be presented to you , but not saved.
If you then turn on `Save search results`, the result of that search will be saved, and cannot be 'unsaved'/deleted. So, if you turn this option on, run a search, and receive the results, but later decide it is not what you wanted, it will stay in the case file and cannot be removed (other than through a very intrusive edit of the `.db` file.
Next, be aware that if you have the `Save search results` option turned on, and run the same search twice, the result in the `Keyword Hits` section are enumerated, in this case, doubled.
What I am trying to warn you of is - don't 'commit' a search (i.e. select `Save search results`) until you are happy with the results that have appeared. If you are happy, and want to save the results of that search, run it again, this time turn on `Save search results`, but do not run it again!

3.1.6 OS Accounts

As part of standard reporting procedure, the investigator reports details of all the user accounts active on the DFI being investigated. The kind of data that they might report include: user account names, date of last login, last shutdown, whether the password has been changed. This information can be vital for helping to determine (a) whether there are other third parties of interest, (b) whether the 'it was someone else' defence might be valid.

This information is available in the registry. In more recent versions of Autopsy, present version included, Autopsy has made some of this information available to an investigator through the `OS Accounts` section. Although some information is presented herein, this does not include all the information that an investigator might want to see. For that, the investigator may need to resort to a registry analysis. As a hint of what an investigator might want to report, see the notes in my 'items of interest from a registry forensics viewpoint' lecture.

The feature is available through the `Results--OS Accounts` menu option. The `Stanley` case does not contain any data because this is not a Windows install, it is a DFI extracted from a USB. However, as an example. see Figure 37

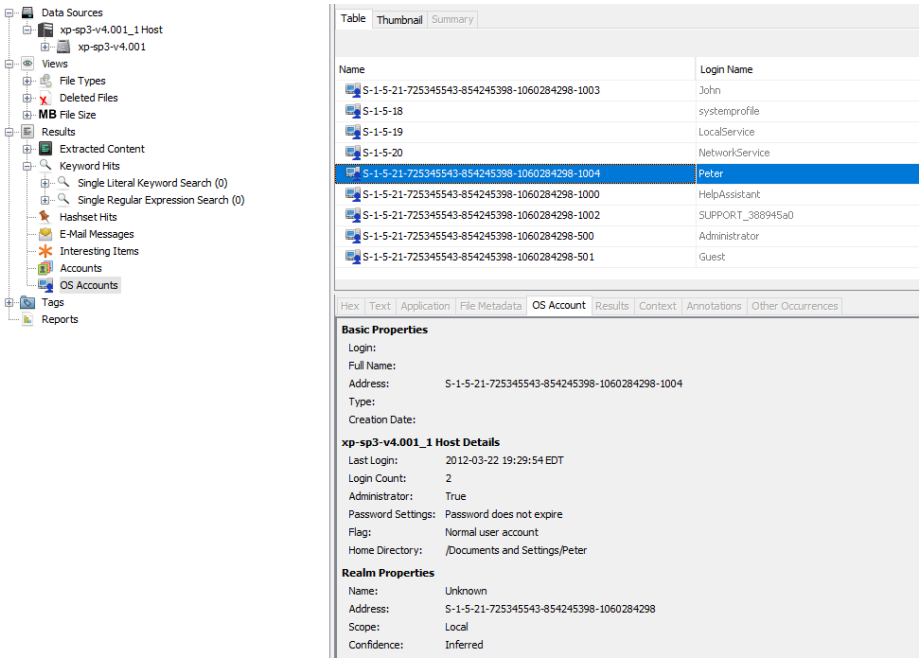


Figure 37: OS Accounts

4 Tagging and Bookmarking

Materials

A pre-created ingested case directory called `Stanley` which requires the DFI: `Stanley.E01` (also provided in the directory)

Bookmarking enables investigators to highlight items of importance. The investigator can return to these items and analyse them in further detail before determining whether or not to include them in their investigation report.

Depending on the size of the investigation team, the digital investigation role is often split into an *examiner* and an *analyst*. The *examiner* performs the initial examination, reveals items of interest, and tags them to be followed up (investigated further). The *analyst* then focuses on the items that have been tagged, analyses them in more detail, and determines whether they need to be included in the report.

There can often be confusion about the use of *follow up* tags and *bookmarks/tags*. The Autopsy documentation is not helpful or clear. So, I (with my experience of FTK, and Encase) interpret their use as follows. A *follow up tag* can be roughly translated to the job an examiner will perform which is *'I believe this file is important, I need to come back to it (follow up) and decide whether it is, if it is, I will bookmark it for inclusion in the report. Bookmarking/tagging* roughly translates to *'I have analysed this file and it needs to be included in my report'*. It is not as easy as that, because Autopsy will include BOTH in its report. You need to determine how you use these two features, and I would suggest you follow my advice :-)

4.1 Adding a Follow-Up Tag

The `Tags` link in the `Tree view` contains all the tags created by the investigator.

1. Click on the `Keyword Hits` link, and then select `London`. If `London` does not appear, perhaps because you missed out the steps in 3.1.5, go back to 3.1.5 and repeat that process first.

2. Right-click on the file `G704031861.jpg`, and select `Add File Tag` and then `Follow Up` (Figure 38)

   The options presented in this screen are reasonably self-explanatory, in any case, we will be covering bookmarks in more details later in the module.

3. Select `Tags--Follow up--File Tags (1)`

Note that the `Tree View` has altered to reveal a single file. Later, the investigator will return to this file and investigate it further if required.

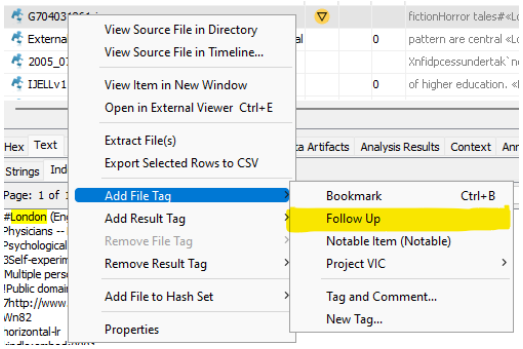


Figure 38: Adding a Tag

Let's add another follow up tag.

4. Navigate to `vol3...--text files`
5. Right click on `3.19532.MW4DOOKAGWPHNUN2LLOAW3MDTLW3KOPQA.txt` and select `Add File Tag--Follow Up`
6. Having analysed the file, and determined that it is of importance to our investigation, we can bookmark it by following the steps outlined below.

   Note that (a) the file appears in the `Bookmark--File Tags` link, and (b) it stays in the `Bookmark--Follow Up` link too. This is where some discipline needs to kick in. If the examiner has determined that the file is of relevance and must be included in the report,

Adding a Bookmark

Remember that bookmarks are included in the final report, follow up tags are not.

1. Navigate to `vol3...-->text files`
2. Right click on the file entitled `3.19532.MW4DOOKAGWPHNUN2LLOAW3MDTLW3KOPQA.txt`
3. Right click on this file and select `Add file tag-->bookmark`

   Note that you can bookmark any file by selecting and pressing `CTRL B`
4. Bookmark the file entitled `3.19533.DC1PMT3UBYSQWPSGKNI4YLHOZRLIR2QDB (1).txt` - this time by selecting it and pressing `CTRL B`

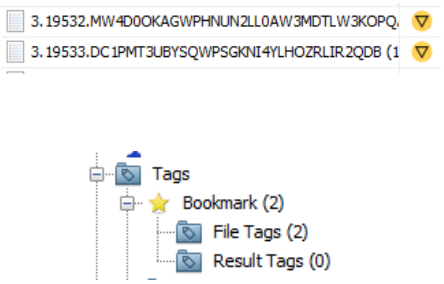


Figure 39: Bookmarking

Note that the status field for the two files that you bookmarked has changed (a yellow circle with a downward pointing black triangle), and that a `Bookmark` link has appeared in the `Tree view` (Figure 39).

5. Expand the `Tags` view and select `File Tags`. The `Result Viewer` changes to show the two files that have been bookmarked.

Removing a Bookmark

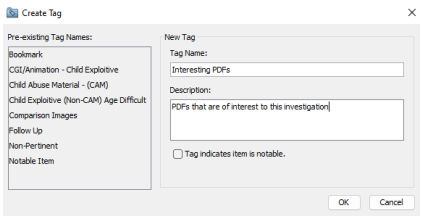
6. Navigate to the `Tags--Bookmark--File Tags` view.
7. Select the file `3.19532.MW4D0OKAGWPHNUN2LL0AW3MDTLW3KOPQA.txt` in the `Results View`
8. Right click on this file and select `Remove File Tag-->Bookmark`

Creating bookmark categories

Hitherto, we have been marking files with a generic bookmark – or bookmarks that come as standard with Autopsy. Often it is useful and necessary to add our own bookmark categories. In the following steps we will create a category called `Interesting PDFs` and add a few PDFs to this category.

9. Navigate to `vol3...`
10. Right click on the file `18524112.pdf` select `Add File Tag-->New Tag`
11. In the `Tag Name` box type in `Interesting PDFs`.
12. In the `Description` add a description for this Tag, for example, 'PDFs that are of interest to this investigation' (Figure 40 top)

Note that this new tag appears in the Tags list (Figure 40 bottom). Also note that this tag will now appear everytime you right click on a file and add a file tag.



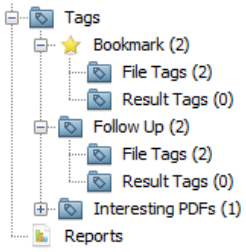


Figure 40: Creating Tags

13. Find and add all the PDFs to this new category. If you have done it right, there should be 12 files added to this category.

Adding Comments to Tags

Although we added a comment to the *Interesting PDFs* category. Quite often there is a specific comment that in investigator wants to make about a particular file. This can be done through `Add File Tag--Tag and Comment`

14. Navigate to `Vol3...`
15. Select the file `ECCWS2016-proceedings.pdf`
16. Right click this file and select `Add File Tag--Tag and Comment`
17. In the `Comment` box, type in *'Proceedings of a conference that took place in 2016'*

4.2 Adding tags through searches

Hitherto, we have been manually selecting files and bookmarking them. Often we want to do this as a result of a search process (because we found something notable).

18. In the `Keyword Search` type in *Rodosek*
19. The search hits will appear in the `Analysis Results--keyword hits--Single iteral keyword search` link in the `Tree viewer`
20. Select the file `ECCWS2016-proceedings.pdf`

The results are presented in the `Analysis Results` tab in the `Content View`. At this stage, the examiner would analyse this result, and make a decision as ot whether this needs to be tagged. If it is to be tagged, what type of tag should it be. For example, is this a *notable file*?

21. Right click on the file and consider whether we should be adding a *file tag* or a *result tag*.

    In this case, it is not the presence of the file we are interested in, but the presence of the name within 'any' file.

22. Select `Add Result Tag`

    Now decide whether create a bookmark, add this item to be followed up later, or record it as a notable item.

23. In our case, we are going to record it simply as a `Notable Item`

4.3 Auto tagging files

Investigators are often presented with very large DFIs, sometimes containing 100,000s of files of interest. Investigating and tagging these can be extremely time consuming. Hash databases help the investigator by auto-tagging files of interest. You will complete two case studies to demonstrate this. In the first case study, you will manually create a hash set, this will demonstrate how to generate your own hash database in an investigation. In the second case study, you will use a pre-created case study and part simulate an investigation into illegal images.

4.3.1 Case study 1: AAN Sounds[1]

Materials

A pre-created ingested case directory called `Stanley` which requires the DFI: `Stanley.E01` (also provided in the directory)

You work for AAN Sound - a record label which produces music for some of the UK's top names. Music files are stored on a central server protected with RBAC controls. The company does not allow employees to copy files to their computer, all editing and processing must be done on a server. These and other controls are in place to prevent music leakage.

In recent months, AAN noticed that music tracks have been leaked. You have been commissioned to investigate this. Your first step was to request a hash

[1] Credit for the hash dataset task goes to Niju Binu, MSc Cyber Security Management (class of 2023) who created this tutorial

database of every file of interest on the central server. An internal investigation resulted in a USB stick being seized from a suspect employee. The USB stick was imaged as `Stanley.E01`.

You will now create a hash database (`.idx` file), import it in Autopsy and determine whether any files on the DFI match the hashes in the hash database.

The MD5 hashes of interest are given as follows:

```
d0ed6c3715909b126409355e601c6435
e789c5ada89355c6eaba3ed217ce9085
e4d6839a3644426ec0b3dda8bdd1d70c
565ab9f21d080b5b59515f3f306b700b
e41f43e9433f46d9df5c84a207db90e9
20b4304a2be3c22454d529e56a892679
52455365549d04b55a29512175210dc6
46d9e92ea008ec6c5616e23aced60a84
6f8abac4c1c618dcc6787da7350b3d3f
2bd15b17f2255712e0f077afbf6085d7
40825b4efcf5765f7efe029949c0ffaf
03c5849f7431157d4e45308c18764635
ed1b2e31fabf3709e627e791eff09abc
03c5849f7431157d4e45308c18764635
c1ac8c6c9db4b05201d0233c5e8bffb5
642e1984241d3e8b51970251c510c39d
73a7aa8084f3c29b3bc8d2b4928893c2
6f8abac4c1c618dcc6787da7350b3d3f
4011bf42eae11fac5ecc39eaeaa17032
```

4.4 Solution

1. Create a text file
2. Copy and paste the MD5 hashes in (I have not tested with the SHA256 hashes) into this text file
3. Save the file as `MusicPirates.idx`
4. Open the `Stanley` case.

   We are going to part-ingest this file again, but we are only going to mark notable files against the newly created hash database.
5. Right click the `Stanley.e01` file in `Data Sources`.
6. Turn ALL the ingest options OFF - i.e. deselect them. This is very important.
7. Select `run ingest -- Hash lookup -- Global Settings -- Import Hash Set -- Open`

8. Point to `MusicPirates.idx`
9. Note that the `Index Status` is red. Select `Index`. This will create an index for this file.
10. Select `OK -- Finish`
11. Now let Autopsy add this DFI. It will begin the ingest process, let it complete.
12. In the `tree viewer`, note that there is a new entry under `Analysis Results` which reads: `Hashset Hits--MusicPirates`. This should have 19 hits next to it. Select this and note that it highlights the files which match the 19 hashes you added to the database.

Please note, there is an exercise which runs through the process of using the NSRL database in Appendix A.

4.4.1 Case study 2: Illegal Images

Materials

`IMDK.E01`, `IMDK.E01.txt`, `CatA.idx`, `CatB.idx` and `CatC.idx`

Please note this is a directory containing these 5 files, it is not a pre-created case.

The investigation of illegal images is time consuming, psychologically difficult, and can result is subjective decision making. Pre-created hashes in the form of the CAID (Child Abuse Image Database) helps speed things up by providing a pre-created dataset which can be used to auto-tag files of interest.

In this case study you are going to simulate this process.

Section 1 of the Protection of Cute Pets Act 1978 (PCA 1978) makes it illegal to possess, distribute, or create images and/or pseudo-images of spiders, lizards, and cats. (Images of dogs are OK :-)). The CPS guidelines categorise these images into three categories:

1. Category A (Spiders, the worst)
2. Category B (Lizards, pretty bad)
3. Category C (Cats, not good).

After years of investigating these images, it has become clear that the investigation can be psychologically difficult, can result in mistakes, and can be time consuming.

Police authorities have collaborated to create CAID (Creepy Animal Image Database). The database is divided into three files which can be added to Autopsy and ingested to auto tag files.

For the CPS to entertain a prosecution, an investigation must cross the threshold of 250 category A, 250 Category B, and 250 Category C images.

1. Create a new case, add the data source `IMDK.E01`
2. When you are asked to ingest modules, select `Deselect All`
3. Turn on `Picture Analyser` and `Hash Lookup`
4. Select `Hash Lookup`
5. Select `Global Settings`
6. Select `import hash set`
7. Find the three hash databases you downloaded, select the first of these (`CatA.idx`)
8. Ensure that `notable` is selected.
9. Select `OK`
10. Repeat this for the next two (`CatB.idx` and `CatC.idx`)
11. Select each hashset and select `index`.
12. Once these are indexed, select `OK`

After ingest, note that `hashset hits` is now visible in the `Tree View`. There should be 212 CatA, 241 CatB, 227 CatC entries. This does not meet the CPS guidelines, we need 250 in each category. We will add more later on.

The hashset hits now need to be tagged. There is a presumption that you have randomly viewed these and trust the result of the hashset hits. For each CatA, CatB, CatC hashset list in turn:

13. Select the `Hashset Hits--CatA`
14. The results appear in the `Content view`. Select all the files in the `content view` (press CTRL+A to select all the files.)
15. Right click on these files and select `Add results tag--New Tag`
16. Name the tag `Category A`, `Category B`, or `Category C`, respectively
17. Select `Tag indicates item is notable`
18. Select `OK`

As we outlined earlier, we do not yet have enough items in each category to take this to the CPS and secure a prosecution. We need 38 more CatA, 9 CatB, and 23 CatC. Find them and tag them into the appropriate categories as follows:

19. Select the folder `MySpecialPictures` in the `tree view` (`data sources...IMDK.E01`).
20. Select `Thumbnail` in the `content view`
21. Investigate and then select multiple items in each category. Multiple files can be selected using the CTRL+select buttons
22. Right click on the items and select `Add File tags--CategoryA, CategoryB, CategoryC` as appropriate (Figure 41)

Stop when you have 250 in each category.

When you are ready to generate the report (Chapter 7), follow the steps outlined in the report section, but select `Specific Tagged Results` and then deselect `Notable Item (Notable)` and select each of the categories.

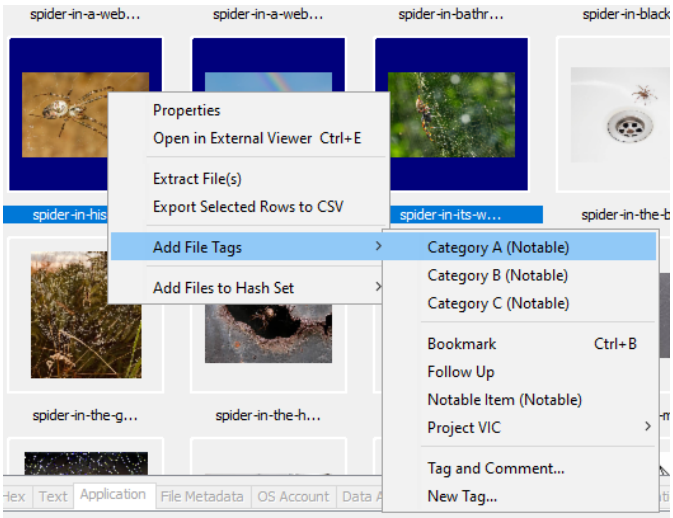


Figure 41: Tagging multiple files

5 Performing Keyword Searches

Materials

A pre-created ingested case directory called `Stanley` which requires the DFI: `Stanley.E01` (also provided in the directory)

Autopsy enables investigators to perform two types of searches: *Keyword Searches* which search the content of files, and *attribute searches* which search file attributes. Keyword searches can be divided into three sub-types: *exact string matches, subset string matches* and *regular expressions*.

The bulk of a digital investigation tends to be built around searching for artefacts on the digital storage system. This involves developing a list of search terms (influenced by the case manager), each of which is applied in turn. The results are then analysed individually and can comprise of file names (you will recall that we have a separate search facility available for this), entries inside documents and the presence of the search term in cache, search, history files. This is only a small subset of the locations in which the search result might be found.

The investigator analyses the results and determines which of these are relevant. The relevant results are then bookmarked for further investigation.

Search results often form the crux of the investigation and therefore the results have to be repeatable. In other words, when the search is performed again by another person, they should arrive at exactly the same results. This can only happen if the SAME search is performed on the DFI. Therefore, it is very useful to keep a log/record of the search terms that were applied. This again requires a degree of organisation and professionalism.

NOTE:
(1) Keyword searches might fail if the appropriate ingest modules have not been enabled.
(2) Your results might be slightly different to mine because I enabled a slightly different set of ingest modules to you.

5.1 Keyword Searches

The keyword search enables investigators to perform exact string, subset string matches, and regular expression searches. Search terms have to be 'designed' carefully – not only because they can take a long, but because poorly designed search terms will result in hundreds, perhaps thousands of often useless results. As an example, presume we are interested in any reference to `htm` (web) files in emails, or other places within the DFI. We could perform the following process.

23. Select the `Keyword Search` (top right of the screen)

24. type in `htm`
25. Ensure that the `exact match` option is selected
26. **The next bit is important.** Ensure that the `Save search results` option is turned off, i.e. it is not ticked. **Often, investigators run searches which result in irrelevant results and have to run searches a few times before finding exactly what they want. If this option is not turned off, those irrelevant results are saved each time.**
27. Select `search`

The results of searches are displayed in `Analysis Results--Keyword Hits--Single Literal Keyword Search`

NOTE: This is very important otherwise the result of the search is saved. The search might result in irrelevant hits, you may have to run a few searches to get exactly what you want, then and only then do you save the results of the search.

28. Select `htm`. Note that there are 77 hits.

    The results of the search are displayed in two places: in a tab in the `Table view`, and in the `table view`.

    Note that none of the search hits are `htm` files – we did not set out to search for `htm` files.

29. Select `Picturesque_073.jpg`
30. Select the `Analysis Results` tab in the `Result view`

    This reveals the following text: `@[h:} 4_ L xGrnO c!]I 8U@≪HTm≪ rlz a,ey6 OQ-ED nZ+( zyi"`

    Note that the search term htm exists within this pattern of text.

This example demonstrates the point about 'designing' a search term.

5.2 Keyword List Searches

Quite often, investigators need to repeat searches across cases and/or perform complex searches involving multiple keywords. The `keyword lists` function enables investigators to save keyword searches and repeat them in other cases. Furthermore, Autopsy includes several pre-configured keywords.

Keyword lists are pre-configured search terms and patterns that can be saved by the investigator for future use. Autopsy includes five keywords as standard: Phone numbers, IP Addresses, Email Addresses, URLs, and Credit Cards. As

an investigator, you can create more and add them to this list of basic searches. When an investigator creates more keyword lists, these can be executed automatically when a case is created. In fact, you have already done that. A number of keyword searches were performed when we added the evidence and enabled the *keyword search* ingest module. The result of this automated keyword search is displayed in `Analysis Results--Keyword Hits`.

At that point we added an email address search. This resulted in 344 URL hits.

NOTE: Ordinarily, you would not repeat the URL search that we are about to do as Autopsy has already identified URLs for you. If there is a particular website address you are searching for, and 2106 URLs are too much to visually trawl through (which they are of course), you would build a specific search term to match what you are looking for.

31. If you have no IP address search hits in the `Analysis Results--Keyword Hits` row, then this was not executed when the original case was created. We can do this now as follows: `Keyword Lists--IP Addresses`. Ensure `Save search results` is turned ON this time (we want to save the results).
32. If you DO have IP address search hits (i.e. it was run when the case was created) OR you have just run it above, you will notice that there are 50 results. However, not all of these are IP addresses, some are false positives.
33. Select `1.0.15.0` and then select `Analysis Results` in the `Content View`.

    Note that the search hit is:

    ```
    ersion %s/win%d (%s)≪1.0.15.0≪mar 28 2013the
                        syste
    ```

    This is not an IP address. This stresses the importance of analysing results before they are tagged for inclusion in the report.

34. Pull down `Keyword Lists`
35. Select `Manage Lists`
36. Select `New List`
37. Name this list *Names*
38. Select `New Keywords` and then select `Exact Match`

39. Enter the following names one on each line without a comma:

    ```
    Harold, harold, Susan, susan, John, john, Tom,
    tom
    ```

40. Pull down `Keyword Lists`
41. Select `Names`
42. Select `Search`

    This generates 180 results (Figure 42, please note this figure is from an older version of Autopsy and might not match what you have found).

5.3 File Searches by Attributes

The `File Search by Attributes` function allows the investigator to search for file names and other file attributes such as the size of the file, the MACc times etc.

43. Select the `Tools` menu
44. Select `File Search by Attributes`
45. In the `Name` box, type in `pdf`
46. Select `search`

This search generates 24 results which are displayed in a new tab in the `Table view`. Unlike the keyword searches, these results are not created in a node in the `Tree View`.

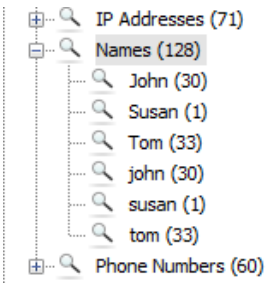


Figure 42: Result of a Keyword List Search

5.3.1 File Size Searches

47. Select the `Tools` menu
48. Select `File Search by Attributes`
49. Select the `size` box
50. Select `greater than`
51. Enter 50 and then pull down the `size metric` box and select MB
52. Select `search`

You should receive 5 results.

Note that we have already seen the file size view in the `data explorer`. Note also, that this view gives us 4 results and not 5. Clearly it is important to understand the differences in these types of results (and be prepared to explain them if required). In this example, the keyword search also includes a file called `$BadClus`. The existence of this file suggests that there may have been a bad cluster on the original digital storage system (again very useful to know!).

5.3.2 Date Searches

53. Select the `Tools` menu
54. Select `File Search by Attributes`
55. Select the `date` box and then enter the start date to be: `01/01/2018` and the end date to be `09/30/2018`. Leave all other boxes as they are.
56. Select `Search`

    This returns 20 results.

Note that the dates are in 'US' format. There appears not to be any way of changing this, so the second date is actually the 1st of March 2018.

6 The Timeline

Materials

A pre-created ingested case directory called `Stanley` which requires the DFI: `Stanley.E01` (also provided in the directory)

In this tutorial we will learn how to use the timelining feature and in particular learn how to generate customised timelines, applying filters to timelines and viewing timelined items as thumbnails.

Timelining is a particularly important aspect of any investigation. Quite often, the timeline of an investigation can reveal exculpatory or inculpatory evidence, occasionally, the timeline provides new leads and directions for an investigation. Timelining in a digital investigation utilises the time stamps attached to files and communications and contained within metadata. Autopsy incorporates a timeline facility that automates the process of timelining. The timeline is accessed as follows:

57. Access the `tools` menu
58. Select `Timeline` option
59. Alternatively, select `Timeline` from the quick launch area.

This launches the timeline generation function. It will probably take a few moments for the timeline to be generated (Figure 43).

The resulting timeline presents a visual representation of the MACc times on the image. This is opened in a separate window.

When the timeline generator has finished, the resulting timeline is presented in a timeline window editor.

The timeline window editor can be divided into a number of zones as outlined in the Figure 44.

6.1 Period Configuration

In the `Chart area`, we can notice some activity from 1997 intermittently all the way up to the present day.

Let's assume that the time period of interest is 1st December 2012 to 1st March 2018. The timeline can be modified to highlight a given range as follows:

60. Select the `clock` icon on the date in the bottom left of the `Chart Area`.
61. Alter the day, month and year to 1st December, 2012 from the dialogue box presented.
62. Alter the time to 00:00

The time can be entered manually, alternatively you can use the slider to adjust the time.

63. Select the `tick` to accept the date (Figure 45)

64. Alter the end date from the dialogue box on the bottom right of the timeline screen to 1st March, 2018 set the time to 00:00. Please note that if your window is not wide enough, you may have to select the >>to pull the timeline configuration panel down.

    Note that you can also alter the time period by simply typing it in the format: `DD-MMM-YYY HH:MM:SS`

The chart area alters to reflect this time period.

65. The scale of the graph can be set to a `logarithmic` or `Linear` scale by selecting the appropriate option at the top of the page

The `View Mode` in the `Chart Area` enables an investigator to see the information in three different views, as a `count` which displays counts of individual events; `Details` which provides details and counts of events; and `List` which presents a list of all activities within the time period.

The chart area is navigated by using the sliding bar and the magnifying glass at the bottom of the chart area.

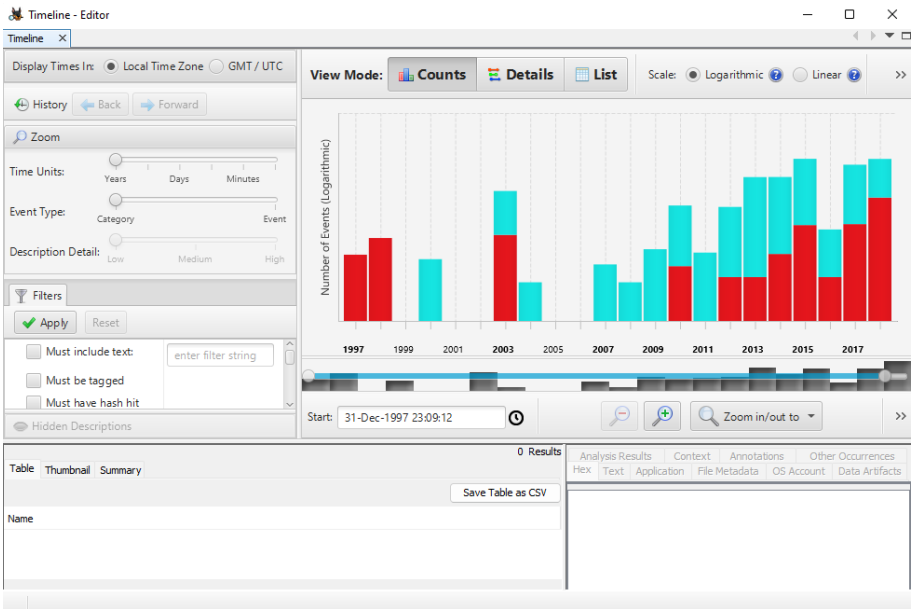


Figure 43: The Timeline

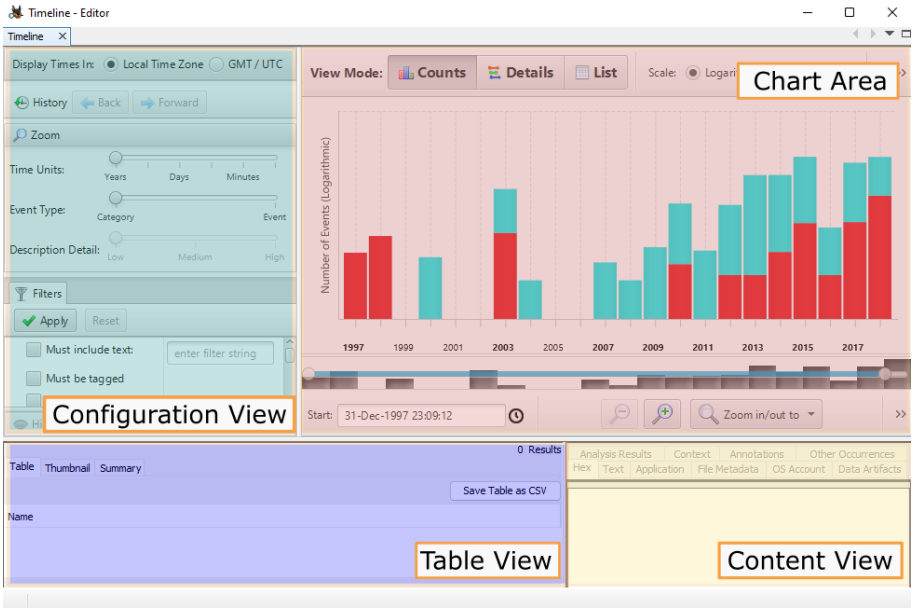


Figure 44: The Timeline View

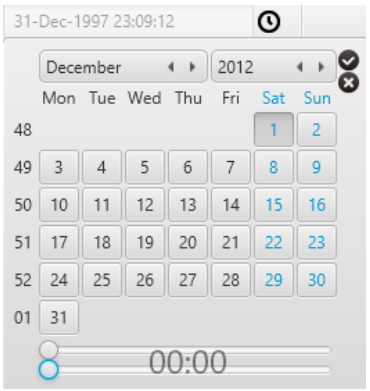


Figure 45: Altering the Timeline

6.2 View Mode

6.2.1 The Details View

66. Select the `details` view

    This presents the file names with a colour/icon coding to highlight the file-type.

67. Select the file: `/Picturesque_038.jpg` (Figure 46)

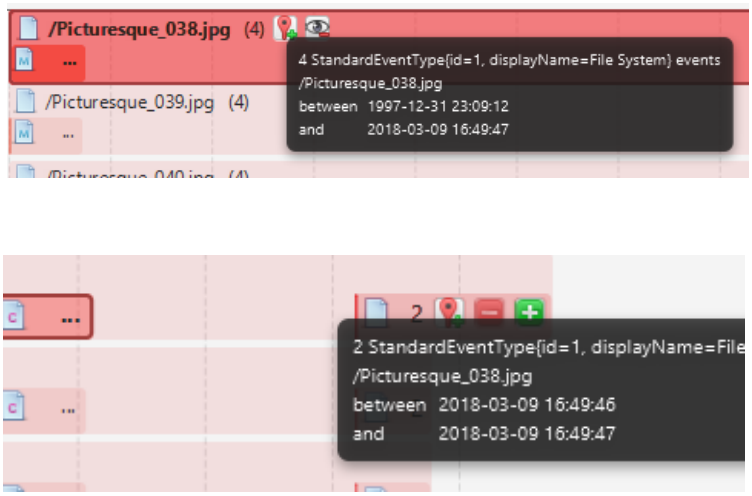


Figure 46: The details view in the timeline

Note that the `Table View` has altered and it now presents the MACc times of this file. The `Thumbnail` tab has become activated. In this case, it will not present anything as it is a deleted file with all clusters inaccessible. If this were an active file, the `Thumbnail` tab would display the file.

68. The *plot* icon is used to highlight files of interest in this view. Hover over the file to reveal the *plot* icon (Figure 46 top). Select this. This positions the file in the upper half of the viewer.

69. Select it again to restore the file.

70. at the bottom right of this file selection is a white box. Hover over this to reveal another *plot* icon (Figure 46 bottom)

71. Select this and note that the `Table View` has altered again to reveal all occurrences of this file.

6.2.2 The List View

The `List` view (Figure 47) presents all the files within the defined period along with events associated with these files. The data for this view is obtained from the MFT and the $USNJournal.

This view identifies dates/times when files were created and modified, when EXIF data was created.

72. Select the `List` view in `View Mode`

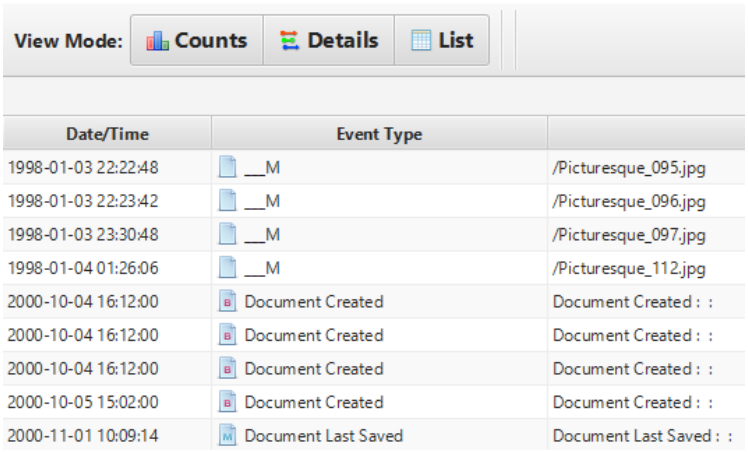


Figure 47: The list view in the timeline

73. Alter the time period to: `07-Nov-2003 00:00:00` to `08-Nov-2003 00:00:00`

    This reveals three entries (Figure 48).

74. Select the `Exif` entry. Note that the `Content View`, hitherto inactive, is activated.

75. Select the `File Metadata` view in the `Content View` and note the file MACc times. These are all dated 2017 or 2018.

76. Now select the `Hex` tab. Note the date: `2003:11:07 05:08:51`. This is the date that the metadata in this photo was recorded and is most likely the date the photo was taken.

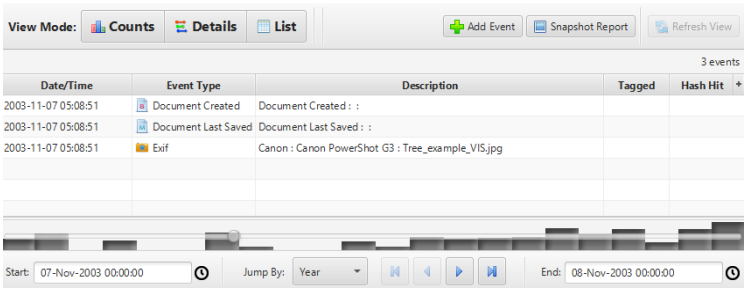


Figure 48: The list view in the timeline (2)

6.3 Applying Filters

The timeline can easily become inundated with too much detail. The `filters` function in the `Configuration view` helps to reduce the amount of detail that appears in the timeline.

Presume we are interested in Files created on this DFI. Maybe this was a USB given to the suspect on a known date and we are interested in the files he/she added to it.

77. Set the time span to `01-Dec-1998 23:09:12` to `09-Mar-2018 16:58:36`
78. Select `Limit event types to` in the `Configuration View`
79. Select `File Created`
80. Select Apply

    The result (Figure 49) reveals activity seemingly on a single day in 2018
81. We can now observe this activity by selecting `Details` or `List`

    Repeat this again and identify any files that have EXIF data attached.

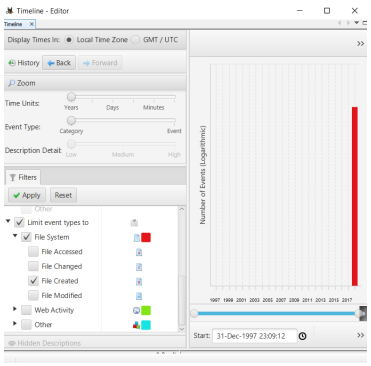


Figure 49: The Configuration View

7 Reporting

Materials

A pre-created ingested case directory called `Stanley` which requires the DFI: `Stanley.E01` (also provided in the directory)

The report generated by Autopsy presents all the bookmarked/tagged items. This is not the final report, the Autopsy report should be integrated into the investigator's final report in any way they feel necessary. For instance, the investigator may choose to organise tagged photos into a named appendix, the timeline in another appendix.

The investigator's report will contain a main body explaining the evidence. That element of the report has to be written by the investigator and is not auto-generated by Autopsy.

The Autopsy report is presented in the `Reports` node in the `Tree View`.

1. The Autopsy report can be initialised by selecting the `Tools` menu and then selecting `generate report` Or selecting the `Generate Report`icon from the quick links at the top of the screen.

At the next screen (Figure 50), the investigator can select between ten formats. A brief description of each report type is given below.

- `HTML report` - this can be viewed in a browser. This is by far the most valuable report format and can be a very useful mechanism for demonstrating the results to a jury.
- `Excel report` - produces summary data of the investigation. The investigator is able to determine which tagged results are exported.
- `Files-Text` - generates MAC data for every file in the report for relevant files. Figure 51 shows the options for this report.

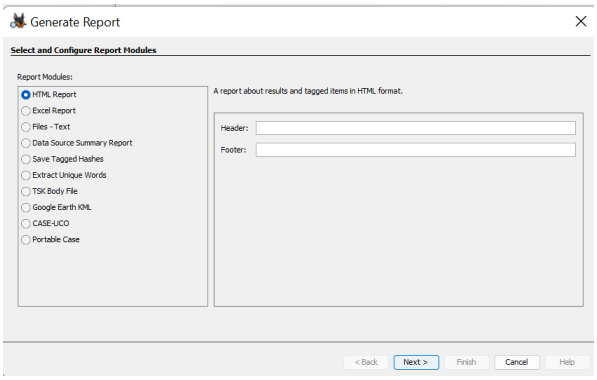


Figure 50: Creating a Report

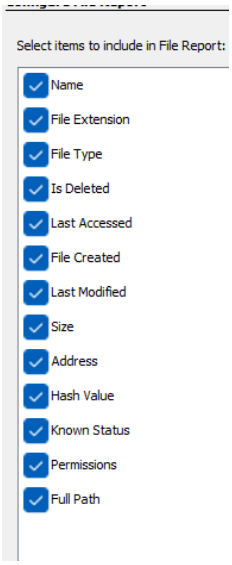


Figure 51: Report options

- The `Data Source Summary Report` provides a summary of the evidence attached to the case.
- The `Save Tagged Hashes` extracts the hashes of each tagged file.
  This option does not actually generate a report. Instead, this option enables the investigator to add the hashes of some/all tagged files to an Autopsy hash set which can subsequently be used by the Hash Lookup Module. If you select this option, you can either 'Configure Hash Sets' to create a new hash set, or you can add to an existing hash set.
  If a hash set is created, then the hashset look up is enabled at ingest (and the appropriate hash set selected), everything that was tagged with one of the selected tags in this case will show up as Hashset Hits.
  Hash sets can be used to compare files previously seen.
- The `Extract Unique Words` report is reasonably self-explanatory.
- `TSK body file` – A report in 'body file format' which reports MACc times for every file. These MACc times can be used in various timeline analysis tools.
- `Google Earth/KML` – generates a report of coordinates found within the data sources. These can be mapped using Google Maps and other tools.
- The `CASE-UCO` is a JSON formatted Cyber-investigation Analysis Standard Expression (CASE) Ontology report.
- The `Portable Case` format can be imported into new cases.

We will proceed to creating a HTML report of our 'investigation'. The HTML report is very useful in that it can be easily viewed on computer systems, can be shared easily, and enables an easy navigation between the various tags.

2. Select `HTML report`
3. In the `header` type in `My First Investigation`
4. The next screen enables the investigator to select the data sources they wish to include within the report output. In our case, there is only one source.

Note that the HTML report still names the data sources included within the case, but excludes the items tagged within those data sources. This can cause some confusion to investigators who 'expected' certain items to appear within the final report.

5. At the next screen, you are presented with an option to either include `All Results`, `All Tagged Results`, or `Specific Tagged Results`. Select `All Tagged Results`.
6. The report can be opened directly from the directory identified in the previous step, or by selecting the `Report` link in the `Tree View`.

Figure 52 shows the various report sections.

Reports

7. Select the `Generate Report` icon in the `Quick Links` area at the top of the Autopsy screen.

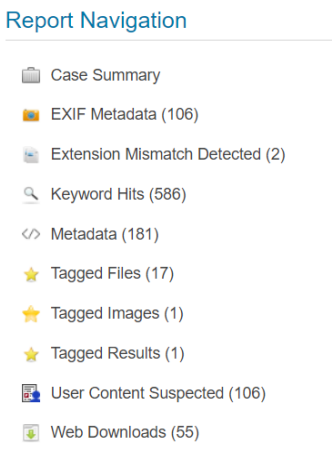


Figure 52: The Autopsy HTML Report

8. In the first screen (Figure 50 Left), leave the header and footer blank (when you create your own report, you can consider how you populate this)
9. Leave the default option: `HTML Report` as it is
10. Select `Next`
11. In the second screen leave the default and only option (`Stanley.E01`) selected, (Figure 50 Right)
12. Select `Next`
13. In the final screen, again leave all options selected as they are. Note that this presents you with the opportunity to decide what is included in the report.
14. select `Finish`
15. Now select the `Reports` link in the `Tags` link. The `Table View` alters to reveal the report that you have just created.
16. Double click on this report. It will open in a HTML viewer. We will not explore the layout of this report, other than to say that the selecting the `Tagged Files` section of this report (Figure 53) reveals the tagged file in the right hand window. Selecting the file in the right hand window will reveal the contents of this file.

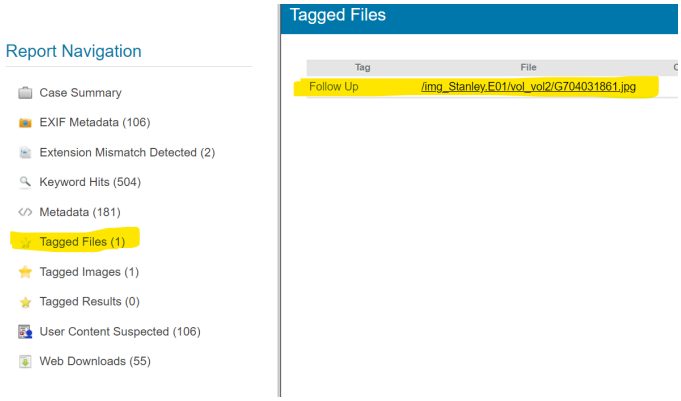


Figure 53: An Autopsy report

Part II
Intrusive Analysis

8 The Registry

Materials

A pre-created ingested case directory called `GregSchardt` which requires the DFI: `GregSchardt.E01` (also provided in the directory)

The Windows registry is *"A central hierarchical database used in Microsoft Windows... to store information that is necessary to configure the system for one or more users, applications and hardware device"*[2]. The registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system, and the ports that are being used.

Through the course of this tutorial, you will answer some of 12 questions, typically important to a forensic investigation:

Operating System

1. What is the operating system (inc build)?
2. When was the operating system installed?
3. Who (which user) installed it?

Names and Accounts

4. What is the name of the computer
5. Who (appears to have) has an account on this system?
6. When did they last log in?
7. When did each of them last shutdown the computer?
8. What was the timezone the computer was set to?
9. What USB devices have been accessed on this system?
10. What WiFi networks have been accessed on this system?
11. What programmes have been installed on this system? Is there evidence of programmes having been uninstalled (see my paper)?

Recent activity

12. What were the most recently accessed files, programmes, and sites?

[2] Microsoft Computer Dictionary 5th Ed (2002)

8.1 Registry organisation

The registry structure has not changed much since it was conceived. The registry is organised into 7 hives. A hive is a collection of files which store the actual data. Each hive is organised into *keys* and *sub keys*. Each *key* has a several *values*, each of which contains associated *data* (Figure 54). There are five main hives:

- HKEY_CLASSES_ROOT abbreviated as HKCR
- HKEY_USERS abbreviated as HKU
- HKEY_CURRENT_USER abbreviated as HKCU
- HKEY_LOCAL_MACHINE abbreviated as HKLM
- HKEY_CURRENT_CONFIG abbreviated as HKCC

8.2 HKEY_CLASSES_ROOT (HKCR)

HKCR contains data related to object linking to ensure that the 'correct' application opens the file when selected. For example, for an mp3 file, a pointer will be registered to the file as a windows sound object which can be handled by windows media player.

Questions that this key might answer include:

A What app was the suspect using to create the jpeg, pdf,other files?

B What evidence is there of apps that might have been used, but now appear deleted?

8.3 HKEY_USERS (HKU)

HKU stores the entire configuration setting for ALL system users (unlike HKEY_CURRENT_USER which stores information about a specific user).

This key helps the investigator differentiate between settings that apply to all users, and those that apply to a specific user.

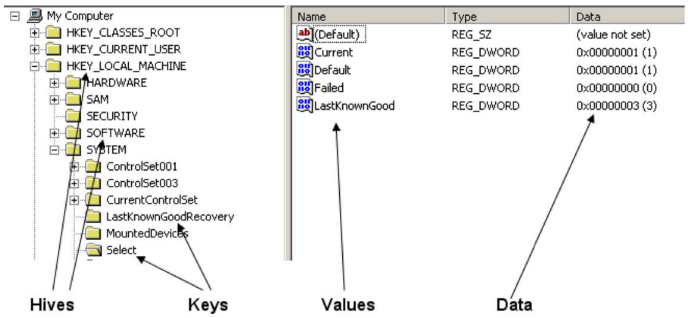


Figure 54: The Registry Structure

8.4 HKEY_CURRENT_USER HKCU)

HKCU and HKLM are the two most important keys in any windows investigation. HKCU contains configuration information for a specific user. This includes information such as:

- user folders
- screen colours
- Screen saver
- control panel settings are stored here
- Application usage information
- Internet activity details

When a user logs onto windows, configuration information is applied from here Data is stored in NTUSER.DAT

The value of this key can be demonstrated in the following case study.

22 individuals were arrested in a $100,000 credit card fraud case in Houston. Examination of NTUSER.DAT on the first suspect's laptop led to external files containing multiple other names, addresses, and credit card numbers that where being used online to purchase items. This led to the identification of further suspects, and 21 further warrants of arrest (totalling 22).[3]

8.5 HKEY_LOCAL_MACHINE (HKLM) and HKEY_CURRENT_CONFIG (HKCC)

Along with HKCU, HKLM is the the most important registry key (for forensic purposes). HKLM contains configuration information particular to the computer. Information from this hive is used by applications, device drivers, and the operating system HKLM contains five subkeys:

- Hardware: Database describing the physical hardware in the computer, the way device drivers use that hardware, and mappings and related data that link kernel-mode drivers with various user-mode code
- SAM: The Security Accounts Manager. Security information for user and group accounts
- Security: A database that contains the local security policy, such as specific user rights
- Software: Information about software (and associated configuration information) installed on the local computer.
- System: Database that controls system start-up, device driver loading, NT 4 services and OS behaviour.

HKCC contains Information about the hardware data that the system uses to boot up.

8.6 Registry files

The registry is stored in several files. When Windows boots up, the registry brings together data from these files. Forensic investigators investigate the indi-

[3] Sammons, J., 2012. *The basics of digital forensics: the primer for getting started in digital forensics.* Elsevier.

vidual constituent registry files. The files (and their locations) associated with the hives outlined above are:

- HKCU comprising the files Ntuser.dat, Ntuser.dat.log available at Users/Username and at Documents and Settings/{username} on a Windows XP machine
- HKCC comprising the files System, System.alt, System.log, System.sav available at windows/ system32/ config
- HKLM/ SAM comprising the files Sam, Sam.log, Sam.sav available at windows/ system32/ config
- HKLM/ Security comprising the files Security, Security.log, Security.sav available at windows/ system32/ config
- HKLM/ Software comprising the files Software, Software.log, Software.sav available at windows/ system32/ config
- HKLM/ System comprising the files System, System.alt, System.log, System.sav available at windows/ system32/ config
- HKU/ DEFAULT comprising the files Default, Default.log, Default.sav available at windows/ system32/ config

These are the files that we must extract to be able to analyse the registry. However, for the purpose of the present tutorial, we are only interested in the following files: Ntuser.dat, System, Sam, Security, Default, and Software

8.7 TASK: Extracting and viewing Registry Files

NOTE

I want to begin this section of the tutorial with a warning. In my experience, registry tools are quite flaky. None of the tools that I am aware of seem to work perfectly, and there is more work to be done to produce a registry analyser.
This tutorial works, however, you will find the navigation of the tool quite awkward and occasionally frustrating.

The Windows registry files are stored in the Windows/System32/Config directory, and the user registry in Documents and Settings on a Windows 98 machine. We are now going to extract the registry files, and then view them using Registry Explorer.

1. Create a directory called GregSchardtRegistries
2. Open **FTK Imager**
3. Select File--Add Evidence Item

4. Select `Image File`
5. Navigate to `_MyImages` and locate `4Dell Latitude CPi.E01`
6. Select `Open--Finish`
7. Navigate to `Partition1--NONAME[NTFS]--[root]`
8. Navigate to `vol2/WINDOWS/system32/config`, CTRL+select `default, SAM, Security, Software` and `system` and extract these to the `GregSchardtRegistries` you created earlier.
9. Navigate to `Documents and Settings/Mr. Evil`
10. Extract `NTUSER.DAT` to a directory within `GregSchardtRegistries` called `MrEvilRegistry`

    Note that ordinarily, you would do this for each user registry.

Now the registry files have been extracted, we are going to view them using Registry Explorer (v2.0).

1. Start *Registry Explorer*
2. Select `File--Load Hive`
3. Select the `GregSchardtRegistries` directory
4. Select the registry files which are (reminder) `default, SAM, SECURITY, Software` and `system`.
5. Add the Mr.Evil registry file too (reminder: `NTUSER.DAT`)

   We now have a hive of registry files (Figure 55). Having to open so many keys every time we need to work on this hive can be awkward and time consuming. *Registry Explorer* enables us to save this as a project file.
6. Save this hive by selecting `File--Project--Save`

Going forward, you can open this hive and work on the registry without needing to repeat the above steps each time.

Note that some of the hives indicate `Unassociated deleted values, Associated deleted values` and `Associated deleted records`. Over time, registry values get deleted as a natural consequence and because of deliberate manipualtion. *Registry Explorer* is able to reveal these values.

8.7.1 The Operating System

We are now going to learn the registry location of important evidence by answering a series of questions. We begin with the operating system:

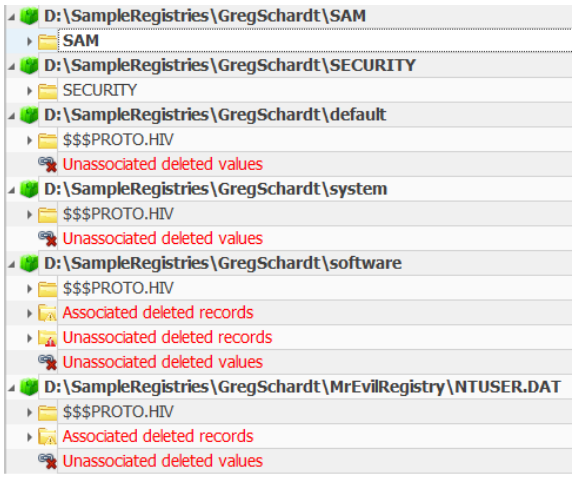


Figure 55: The registry view in registry explorer

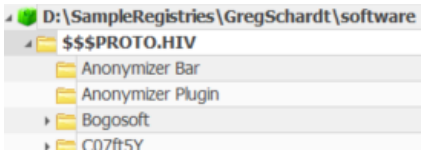


Figure 56: Manually navigating hives

8.7.2 What is the operating system?

This information can be found in:

`SOFTWARE/Microsoft/Windows NT/CurrentVersion`

There are two ways to of accessing registry keys, navigating through the hives directly, or searching for them. Searching is obviously faster. Although the search method is faster, you might be using a tool that does not support searching.

7. We will begin by navigating a hive to find a particular key - the *currentversion* key in this case. Expand the `software` key
8. Expand `$$$PROTO.HIV` (Figure 56).
9. Now continue navigating through `Microsoft--Windows NT--CurrentVersion`

This gets you to the screen shown in Figure 57 (Top).

This is one way of finding keys. It is long winded and can get confusing. Another method is to search directly for the key.

10. Press CTRL+F, this opens a new dialogues box.
11. Type in *currentversion* into the dialogue box and press `Search` in the left hand of the dialogue box (there are two `Search` buttons.)
12. There are multiple hits in multiple keys. Remember that the key we are specifically interested in is `SOFTWARE/Microsoft/Windows NT/Curr entVersion`. This appears further down the list.
13. The correct entry is shown in Figure 57 (Top).

    Double click on the entry. This takes you back to the original window, and highlights the search result (Figure 57, bottom).

    The key that we are interested in is the `ProductID` key which reveals that the operating system is *Windows XP*.

This has demonstrated that searching the registry for forensic information is awkward and long winded. This area of forensics requires a lot more research,

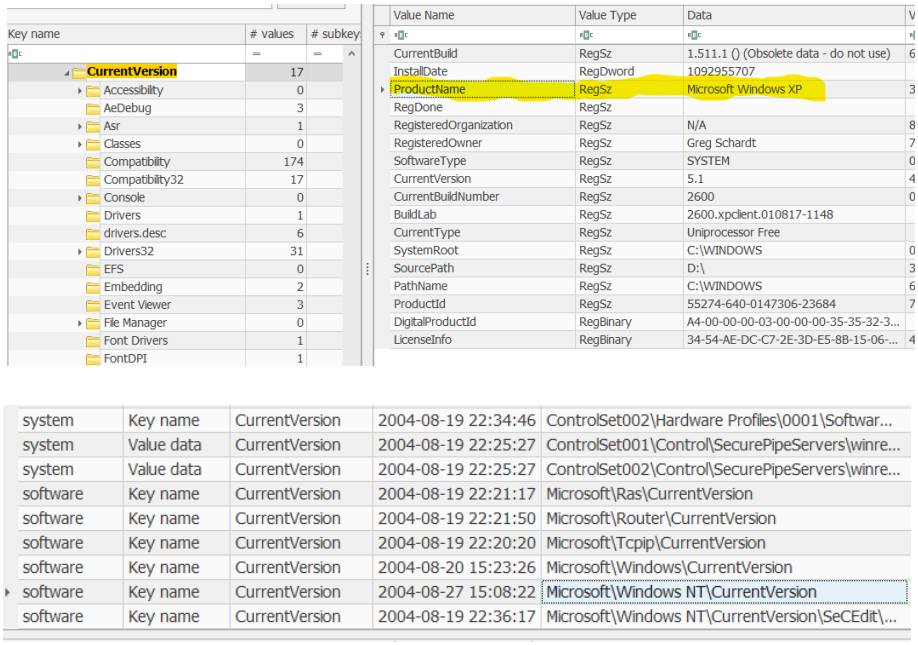


Figure 57: Searching the registry

development, and work. Frankly, we need better tools which can make the extraction of evidence fundamental to a forensic investigation easier.

8.7.3 Who is the Registered Owner?

This information can be found in:

`SOFTWARE/Microsoft/Windows NT/CurrentVersion`

This reveals that the registered owner is *Greg Schardt*.

8.7.4 Install date

The following case study exemplifies the importance of knowing the install date of an operating system:

An employee returns a corporate laptop after quitting role. The laptop was 'wiped clean' and the employee argued that he had "lost all the recent corporate designs". The laptop was investigated to reveal that the employee had installed a (nearly) fresh install of Windows 10, and had most likely removed sensitive files before handing in his notice. The registry evidence led investigators to perform a more detailed forensic investigation which revealed the missing recent research designs.[4]

The install date can be found in the key `InstallDate`. This key reveals the install date to be 1092955707. This is a Unix timestamp which tracks time as a running total of seconds from the Unix Epoch on January 1st, 1970 at UTC.

14. Go to `https://www.epochconverter.com`
15. Enter the Unix timestamp (1092955707) This reveals the install date/time to be be: Thursday, 19 August 2004 22:48:27

8.7.5 Computer Name

The *computer name identifies the computer on a network.* The *computer name* can be found on a Windows XP machine at:

`SYSTEM/ControlSet001/Control/ComputerName/ComputerName`

and on a Windows 7+ machine at:

`SYSTEM/CurrentControlSet/Control/ComputerName/ActiveComputerName`

[4] Windows update did it, https://www.tetradefense.com/digital-forensics-services/forensic-case-files-windows-update-did-it/

The computer we are investigating has already been shown to be a Windows XP machine, hence we will be looking for: `SYSTEM/ControlSet001/Control/ComputerName/ComputerName`

16. Either navigate directly to the key, or (preferably) search for *computername*.

    This reveals the *computer name* to be `N-1A9ODN6ZXK4LQ`

Now you know how to navigate and search the registry, you just need to know the full key path to find a particular item in the registry.

8.7.6 When did a user last log in?

It is useful to know when a user last logged into a system. This information can be found at:

`SAM/Domains/Account/Users/`

.

17. You can either search for `Users` using CTRL+F or navigate (manually) to `SAM/Domains/Account/Users/Names/Mr. Evil`

The resulting key is presented in Figure 58. This overview presents the investigator with a lot of useful information. We can see the names of all accounts (`User Name`) and the order in which accounts were created. This is not too important in this case as we have four default accounts (`500, 501, 1000, 1002`) and one user account (`Mr. Evil`). This view shows us when the password was last changed, and the `Last Login Time` which in this case is `2004-08-27 15:08:23`.

8.7.7 When was this system last shutdown?

The system shutdown time is a good indicator of when the system was last used. We say 'good' indicator because the shutdown time is recorded in 'graceful

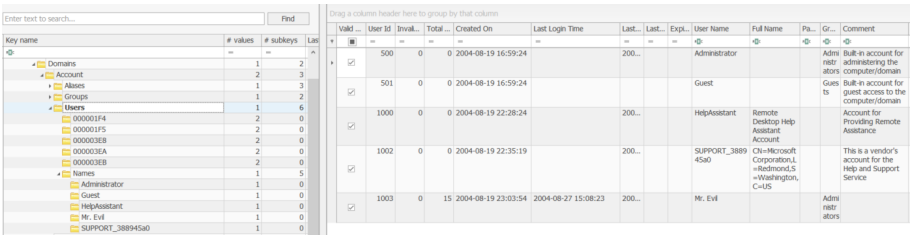


Figure 58: Data sources

shutdowns', i.e. when the user chooses to shutdown the computer. If power is lost, or a user holds the power button down (normally for five seconds) to force an instant system shutdown.

The shutdown date/time is available at:

`SYSTEM/ControlSet001/Control/Windows`

18. Search for the shutdown key

    This returns a shutdown date/time of `C4-FC-00-07-4D-8C-C4-01`. You can convert this by following `https://www.save-editor.com/tools/wse_hex.html` to give `127380951931092160`.

    The number is represented in Little Endian format This can now be converted here: `https://www.epochconverter.com/ldap`, this returns: *Friday, 27 August 2004 16:46:33 GMT+01:00*

19. Alternatively, you can right click on the key and selected `Data Interpreter`.

    The `Data Interpreter` (Figure 59) converts the selected byte stream into a series of formats. The interpreter, does not understand the data that has been selected, and especially does not understand that format it should be converted to. So the data interpreter converts the selected byte stream to several formats in anticipation that one of them is the required format. In this case it is, and we can see from Figure 59 that the same data as revealed through the 'manual' steps has been returned.

8.8 Programs

While the presence of particular files is important in an investigation, sometimes of equal importance concerns the programs that have been run. An investigator will have lots of questions to ask, for example:

- What programs have been installed on this system?

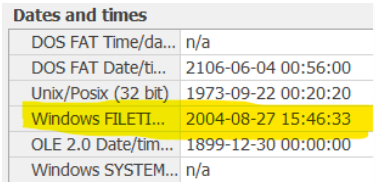


Figure 59: The Data Interpreter

- What programs were recently run?
- When were they run?
- Is there evidence of programs having been uninstalled?

8.8.1 What programs have been installed on this system?

A reasonably comprehensive list of programs that have been installed on a system can be found at:

`SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall`

We say 'reasonably comprehensive' because most Windows programs are designed to install the 'uninstall' details at the same time as the program is installed (so it can be uninstalled). However, not all programs do this. Furthermore, some programs are run directly from the `.exe`. *Registry Explorer* is a case in point. This means that we cannot completely rely on the data found. It is possible that a program was uninstalled, and there is no record left of it. As an example of this, consider that further program install details can also be found here:

`SOFTWARE/ Microsoft/Windows/CurrentVersion/Installer/UserData/S-1-5-18/Products/{GUID}`

20. Navigate to `SOFTWARE/Microsoft/Windows/ CurrentVersion/Uninstall` or search for `Uninstall`

    This presents a list of programs along with the *last write timestamp* which is the last time a value was written to the corresponding registry key (Figure 60).

21. Now navigate to `SOFTWARE/ Microsoft/Windows/CurrentVersion/Installer/UserData/S-1-5-18/Products/{GUID}`

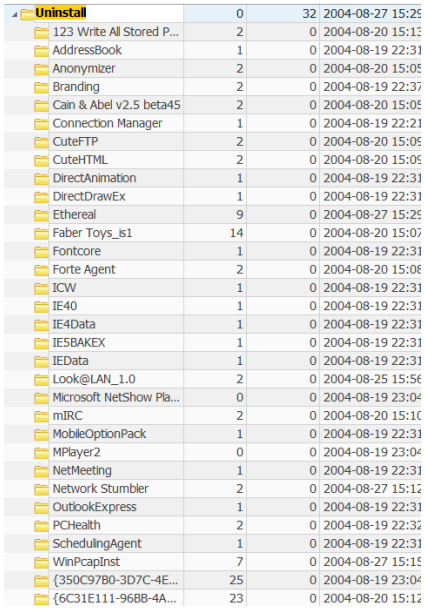
    This presents further evidence of two more programs: *WebFldrs XP* and *Powertoys For Windows XP*

22. Check whether these entries exist in `SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall` and that if they do, the install dates are consistent.

8.8.2 When were they installed?

The following case study exemplifies the importance of needing to know when programs were last executed. These are often some of the 'more important' programs,

A trucker was caught smuggling 3,300 pounds of marijuana. He was questioned and arrested after the weight of the truck was found to be inconsistent



Uninstall	0	32	2004-08-27 15:25
123 Write All Stored P...	2	0	2004-08-20 15:13
AddressBook	1	0	2004-08-19 22:31
Anonymizer	2	0	2004-08-20 15:05
Branding	2	0	2004-08-19 22:37
Cain & Abel v2.5 beta45	2	0	2004-08-20 15:05
Connection Manager	1	0	2004-08-19 22:21
CuteFTP	2	0	2004-08-20 15:09
CuteHTML	2	0	2004-08-20 15:09
DirectAnimation	1	0	2004-08-19 22:31
DirectDrawEx	1	0	2004-08-19 22:31
Ethereal	9	0	2004-08-27 15:25
Faber Toys_is1	14	0	2004-08-20 15:07
Fontcore	1	0	2004-08-19 22:31
Forte Agent	2	0	2004-08-20 15:08
ICW	1	0	2004-08-19 22:31
IE40	1	0	2004-08-19 22:31
IE4Data	1	0	2004-08-19 22:31
IE5BAKEX	1	0	2004-08-19 22:31
IEData	1	0	2004-08-19 22:31
Look@LAN_1.0	2	0	2004-08-25 15:56
Microsoft NetShow Pla...	0	0	2004-08-19 23:04
mIRC	2	0	2004-08-20 15:10
MobileOptionPack	1	0	2004-08-19 22:31
MPlayer2	0	0	2004-08-19 23:04
NetMeeting	1	0	2004-08-19 22:31
Network Stumbler	2	0	2004-08-27 15:12
OutlookExpress	1	0	2004-08-19 22:31
PCHealth	2	0	2004-08-19 22:32
SchedulingAgent	1	0	2004-08-19 22:31
WinPcapInst	7	0	2004-08-27 15:15
{350C97B0-3D7C-4E...	25	0	2004-08-19 23:04
{6C31E111-96BB-4A...	23	0	2004-08-20 15:12

Figure 60: The uninstall list

with the bill of lading. A forensic investigation of his laptop found references to recent files which turned out to be forged bill of lading documents. The software used to create these documents had recently been deleted.[5]

Program install dates can be found here::

`SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall`

23. Not all programs here have an install date. In fact, only three of the programmes have an install date. For the rest, the best we may have is the *Timestamp* which may be the only evidence we can cite in our report.

    Note that for the *PowerToys* app, the install date is given as `20040820`. This is presented in the format `YYYYMMDD` and is in a different format to dates we have been getting used to. This timestamp translates directly into 20-08-2004.

One of the problems with the registry (and Windows in general) is that there are multiple date formats in existence, some of which still exist to provide backwards compatibility. As a further example of this:

24. Expand the `Uninstall` key

[5] US v Diaz https://infosecusa.com/us-v-diaz-marijuana-possession-new-mexico

25. Select WinPcapInst

Note that the date is provided in the format MM/DD/YYYY. So thus far we have already dealt with 4 different file formats in the registry. There are many more...

8.8.3 What programs were recently run?

This information is not easily available. An investigator has to piece together data from several places. The main indicator is still:

SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall

On systems newer than and including Windows 7, we can also find evidence in these locations:

- SOFTWARE/Classes/Local Settings/Software/Microsoft/Windows/Shell/MuiCache
- SOFTWARE/Microsoft/Windows/ShellNoRoam/MUICache
- SOFTWARE/Microsoft/Windows NT/CurrentVersion/AppCompatFlags/Compatibility Assistant/Persisted
- SOFTWARE/Microsoft/Windows NT/CurrentVersion/AppCompatFlags/Compatibility Assistant/Store

Perhaps the most conclusive evidence of when a program was last executed is found in a user's individual profile here:

NTUSER.DAT/Software

26. Navigate to NTUSER.DAT/Software

27. Analyse the last run time (given as 1093015489) for the program MIRC (Figure 61). The procedure for doing this was given on Page 78 (step 14). When you convert this, you will get: 2004-08-20 16:24:49

28. How far after this program was installed, was it last used?

Executed through Start--Run

Windows programs are typically executed in two ways, either through the file explorer – for example by clicking on an icon, selecting the program from the task bar, through the Start--Run command, or through the command line. Programs executed through Start--Run can be found in:

HKEY_CURRENT_-
USER/software/microsoft/Windows/currentVersion/explorer/RunMRU

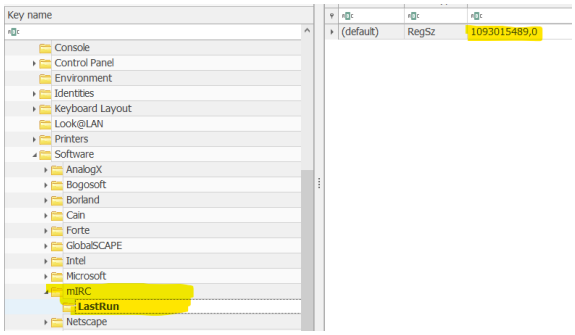


Figure 61: The uninstall list

29. Navigate to `HKEY_CURRENT_USER/software/microsoft/windows/currentVersion/explorer/RunMRU`

This reveals that the app most recently executed through the `Start--Run` feature was *telnet*, and that this was executed on 2004-08-26 15:05:15. This is not the most recently executed app though, there is evidence (for you to find) of UEME_UISCUT having been executed on 2004-08-27 15:46:00 and *Internet Explorer* having been last executed on 2004-08-27 15:42:40.

Programs executed through the *File Explorer*

Programs executed through the *File Explorer* can be found at:

`Software/Microsoft/Windows/CurrentVersion/Explorer/UserAssist`

30. Navigate to `Software/Microsoft/Windows/CurrentVersion/Explorer/UserAssist`

This presents two global identifiers which are pretty standard in any Windows install. GUID for Windows XP (`5E6AB780-7743-11CF-A12B-00AA004AE837` and `75048700-EF1F-11D0-9888-006097DEACF9`). Each version of Windows has similar GUIDs, for instance with Windows 7, the two standard UserAssist GUIDs are `CEBFF5CD-ACE2-4F4F-9178-9926F41749EA` and `F4E57C4B-2036-45F0-A9AB-443BCFE33D9F`.

31. Select `UserAssist`

    The `Value` screen (shown in Figure 62 top) reveals the data associated with each program. Figure 62 (bottom) reveals the same data in AccessData Registry Viewer.

The original registry data is stored in ROT13 format. *Registry Explorer* has taken this data and converted it into a readable format. Let's take one example entry and work through it.

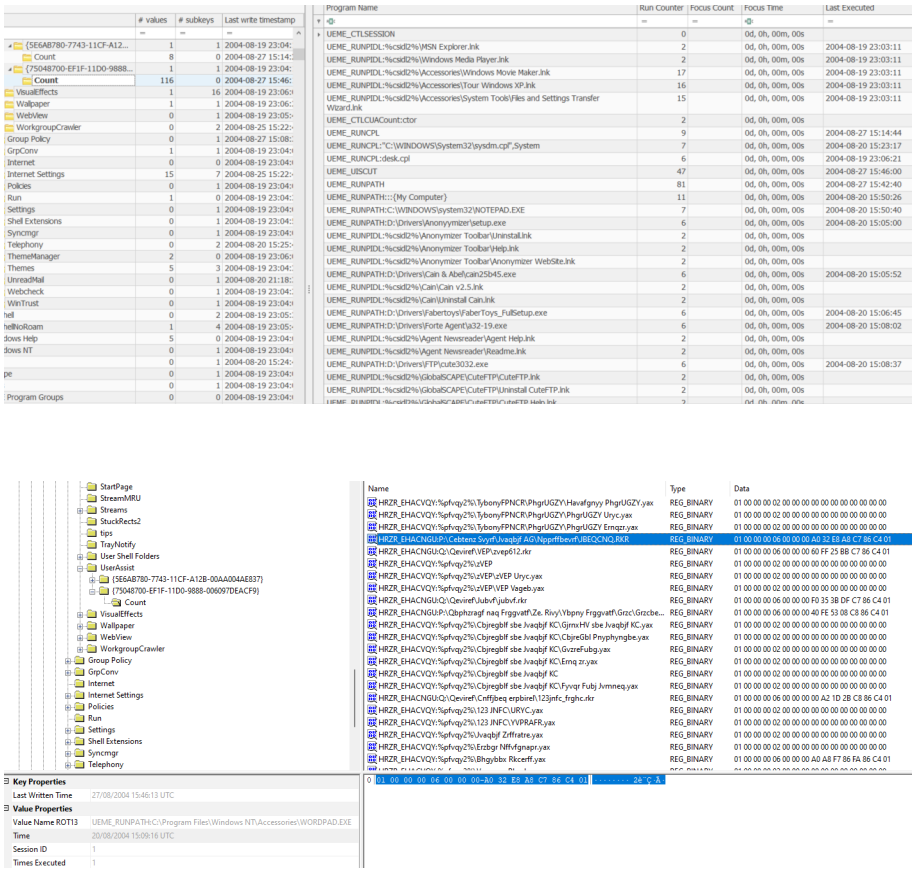


Figure 62: User Assist in Registry Explorer (top) and Accessdata Registry Viewer (bottom)

32. Find the entry for *WORDPAD*.

Note that the *run counter* is 6, and the last executed date is 2004-08-20 15:09:16. The original data, which we can extract using another tool such as *AccessData Registry Viewer*, reads as follows:

`01 00 00 00 06 00 00 00 A0 32 E8 A8 C7 86 C4 01`[6].

The format of this key has changed between Windows XP and Windows 7 onwards. We are going to explore the Windows XP format. The format of this key is as follows: 4 bytes: Session ID (`01 00 00 00`), 4 bytes: times executed

[6]For a better understanding of UserAssist and how it has changed between Windows XP and Windows 7 upwards, see: Singh, B. and Singh, U., 2017. Program Execution Analysis using UserAssist Key in Modern Windows. In SECRYPT (pp. 420-429).

(06 00 00 00), and 8 bytes: last executed in FILETIME format (A0 32 E8 A8 C7 86 C4 01). If you want to (almost) manually convert the filetimes, then https://www.save-editor.com/tools/wse_hex.html and https://www.epochconverter.com/ldap are your friends.

The times executed starts counting at 5, so a value of 06 00 00 00 in this case means 1. You will notice that every entry with a value of 6 (1) has a corresponding last executed time. The value 6 is only ascribed once the program is executed, until then, when it is installed, it has a value of 2. A value of 0 means the program has been hidden.

Let's examine the Value screen in *Registry Explorer* a bit further. Notice that every program entry is preceded with UEME. This stands for user execution method and aims to shed some light on how a program was executed. The methods of execution can be defined as follows:

- UEME_UIQCUT: Quick Launch menu shortcut
- UEME_UISCUT: Desktop shortcut
- UEME_RUNCPL: Control applets (.cpl)
- UEME_RUNPATH: This entry keeps data about executed programs
- UEME_RUNPIDL: Executed PIDLs (pointer to an item identifier list)

This is not an exhaustive list.

33. The registry reveals how many times a program has been executed. Sort the list by clicking on the Run Counter twice. This organises the list with the highest value at the top.

We can see that There were 81 (actually 76) program executions (through *UEME_RUNPATH*), that 47 (actually 42) of these were through desktop shortcuts (UEME_UISCUT), and none were through the quick Launch menu (UEME_UIQCUT). We can see that the program executed the most was *Internet Explorer* executed 19 (actually 14) times and was last executed on 2004-08-27 15:42:40. Finally, we can see that the program that was most recently executed according to this list was UEME_UISCUT executed on 2004-08-27 15:46:00 and that *Internet Explorer* was last executed on 2004-08-27 15:42:40.

Before we end this section on the *UserAssist*, it is worth spending a moment on the *focus count* and the *focus time*. This was introduced from Windows 7 onwards, hence why all the values are blank or zero.

From Windows 7 onwards, Windows tracks how long an application is in focus. The *focus counter* tracks how many times an application was focused, and the *focus time* - the length the application received focus. So a user might have used WordPad for five minutes, then brought Google Chrome to the forefront, and then went back to WordPad and spent another five minutes on it. The *focus count* will be 2 and the *focus time* will be 10 minutes.

8.8.4 What programs have been set to autorun?

The autorun feature is enabled automatically by programs, e.g. Dropbox is set to run automatically by default, or manually by a user, e.g., user selects to have

Google Chrome open and land on a home page automatically. Autorun evidence can be found at the following places:

- NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Run
- NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/RunOnce
- SOFTWARE/Microsoft/Windows/CurrentVersion/RunOnce
- SOFTWARE/Microsoft/Windows/CurrentVersion/policies/Explorer/Run
- SOFTWARE/Microsoft/Windows/CurrentVersion/Run

34. What programs have been set to autorun?

8.8.5 What documents were most recently opened?

Recently opened documents can be found at NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Explorer/RecentDocs

35. Navigate to NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Explorer/RecentDocs

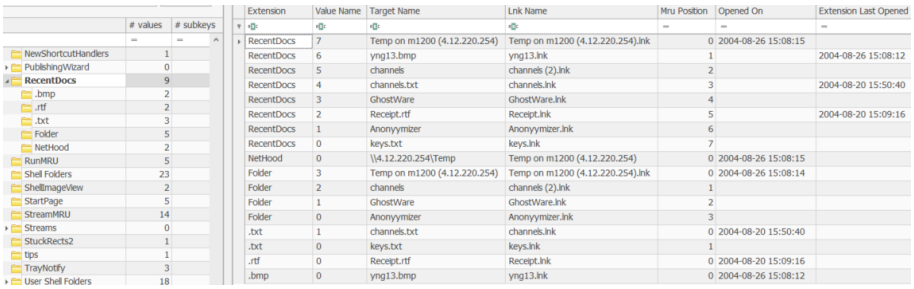
The Values screen (Figure 63) provides the names of files, the links used to open those files, the position of a file in the most recent documents list (with 0 being the newest), the time it was opened, and the time the extension (e.g. .bmp, .txt was last opened.

36. Navigate to the individual file type lists on the left to reveal the time that .bmp, .rtf, .txt folders, and *Nethood* (network shortcuts) were opened.

We can see for example, that Receipt.rtf was opened directly by clicking on a link to this file at 2004-08-20 15:09:16, that four folders were recently opened, and that one of these was opened over a network (Temp on m1200 (4.12.220.254))

8.8.6 What USB devices have been accessed from this machine?

The following case study exemplifies the importance of investigating last inserted USB drives in a forensics investigation.



	# values	# subkeys
NewShortcutHandlers	1	
PublishingWizard	0	
RecentDocs	9	
.bmp	2	
.rtf	2	
.txt	3	
Folder	5	
NetHood	2	
RunMRU	5	
Shell Folders	23	
ShellImageView	2	
StartPage	5	
StreamMRU	14	
Streams	0	
StuckRects2	1	
tips	1	
TrayNotify	3	
User Shell Folders	18	

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	7	Temp on m1200 (4.12.220.254)	Temp on m1200 (4.12.220.254).lnk	0	2004-08-26 15:08:15	
RecentDocs	6	yng13.bmp	yng13.lnk	1		2004-08-26 15:08:12
RecentDocs	5	channels	channels (2).lnk	2		
RecentDocs	4	channels.txt	channels.lnk	3		2004-08-20 15:50:40
RecentDocs	3	GhostWare	GhostWare.lnk	4		
RecentDocs	2	Receipt.rtf	Receipt.lnk	5		2004-08-20 15:09:16
RecentDocs	1	Anonyymizer	Anonyymizer.lnk	6		
RecentDocs	0	keys.txt	keys.lnk	7		
NetHood	0	\\4.12.220.254\Temp	Temp on m1200 (4.12.220.254)	0	2004-08-26 15:08:15	
Folder	3	Temp on m1200 (4.12.220.254)	Temp on m1200 (4.12.220.254).lnk	0	2004-08-26 15:08:14	
Folder	2	channels	channels (2).lnk	1		
Folder	1	GhostWare	GhostWare.lnk	2		
Folder	0	Anonyymizer	Anonyymizer.lnk	3		
.txt	1	channels.txt	channels.lnk	0	2004-08-20 15:50:40	
.txt	0	keys.txt	keys.lnk	1		
.rtf	0	Receipt.rtf	Receipt.lnk	0	2004-08-20 15:09:16	
.bmp	0	yng13.bmp	yng13.lnk	0	2004-08-26 15:08:12	

Figure 63: Most Recently Opened Documents

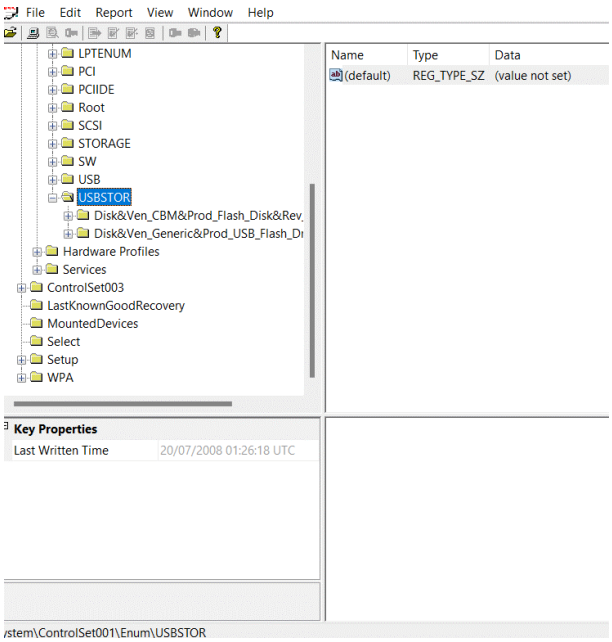


Figure 64: Sample USBSTOR entries

A laptop and two hard disks were recovered following a raid on a hotel. Two suspects were arrested. During interview, suspect A claimed that although the laptop was his, the offending hard disks containing illegal images were not his and had never been connected to laptop. Registry analysis of the `USBSTOR` *key showed that both hard disks had been connected to the laptop.*[7]

Each time a USB device is inserted in a USB port, Windows creates a record of the device in the registry. This is helpful to an investigator who may be interested in locating other devices of interest to the investigation. USB details can be found at:

`SOFTWARE/Microsoft/Windows Portable Devices/Devices`

and

`SYSTEM/CURRENTCONTROLSET/ENUM/USBSTOR`

The *GregSchardt* DFI does not contain any USB information. An example is presented in Figure 64 from another DFI (view presented using RegEdit).

[7]Sammons, J., 2012. The basics of digital forensics: the primer for getting started in digital forensics. Elsevier.

8.8.7 Which WiFi networks has this device connected with?

Each time a Windows machine connects with a WiFi network, the registry creates a record for that device. These records can be found at:

`System/CurrentControlSet/Services/TCPIP/Parameters/Interfaces`

37. Navigate to `System/CurrentControlSet/Services/TCPIP/Parameters/Interfaces`, this reveals four entries.
38. Navigate through each one to reveal the DHCP server, lease times, and other details
39. Convert this time to understand what time the user last connected to this WiFi
40. Was this the last WiFi that the user connected to? If not, which was, and at what time?

This view does not reveal the name of the DHCP server. This can be very useful – and often more user friendly.

The *GregSchardt* DFI does not contain any DHCP information. An example is presented in Figure 65 from another DFI. This shows a sample registry in which the DHCP domain name is revealed. This is taken from a Windows 7 machine, note that more fields were introduced at this point.

You are ready to complete the Registry task at Section F on Page 98.

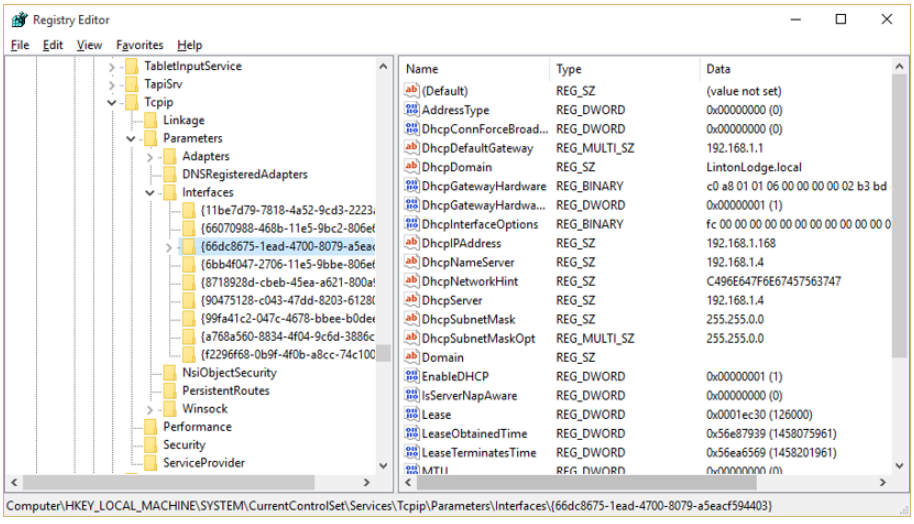


Figure 65: Sample WiFi registry entry

A Adding a *known files* database

Materials

A pre-created ingested case directory called `GregSchardt` which requires the DFI: `4Dell Latitude CPi.E01` (also provided in the directory). The directory also contains `4Dell Latitude CPi.E02` which is opened automatically by Autopsy.
The National Software Reference Library (NSRL) available from: `https://sourceforge.net/projects/autopsy/files/NSRL/`. This is downloadable in IoS, Android, and Computer format. We are only interested in the computer format.
Please note: You should not complete this exercise in class time as the installation of the database takes considerable time. Whilst having tremendous benefits, cthe installation onsiderably slows down the initial creation of a case. As an example, creating the GregSchardt case without the database ingestion enabled takes around 20 minutes, with this enabled, it can take 2 hours.

The National Software Reference Library (NSRL) is a database of known files. The library has collected software from various sources and incorporates file profiles from popular software.

This library can be added to Autopsy to enable Autopsy to 'ignore' these files in its' analysis. This saves time in an investigation.

1. Download the latest Windows library from: `https://sourceforge.net/projects/autopsy/files/NSRL/` (Figure 66)
2. Unzip the library. Remember where you have stored this.
3. Create a new case called `GregSchardt2`
4. Add the DFI `4Dell Latitude CPi.E01`. Please note that there are two files with this name, the second has an extention `.E02`, the second file is added automatically, you do not need to add this file.

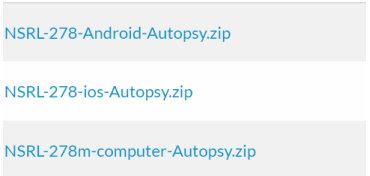


Figure 66: National Software Reference Library (NSRL)

5. When you get to the ingest screen, select Hash lookup -- Global Settings -- Import Hash Set -- Open
6. Point to the unzipped hash set
7. Select OK -- OK
8. Now let Autopsy add this DFI. It will begin the ingest process, let it complete.

Note that although these have been auto-tagged, they will only be added to the final report if you choose to add them. In the next case study, you will manually add auto-tagged files to the report.

To add the database to an already created file, do this.

1. Download a pre-made index from http://sourceforge.net/projects/autopsy/files/NSRL and unzip the file.
2. In tree view, right click on the DFI (.E01), select run ingest module -- choose Hash look up -- deselect all and chose only the Hash look up to ingest
3. scroll down a bit --- global setting --import hash set (.idx) -- open -- tick notable -- ok
4. Note on the right that the Index Status is red. Select Index. This will create an index for this file. Select finish you will see the blue bar that ingesting in progress
5. To make sure that you did it correctly, go to the tree view -- Analysis Results. You will see the Hash Hits grouped by the name of the hash set. If the hash set hits had associated comments, you will see them in the "Comment" column in the result viewer along with the file hash.

B Task 1, Discovering the Autopsy Environment

Materials

A pre-created ingested case directory called `Stanley` which requires the DFI: `Stanley.E01` (also provided in the directory)

1. What is the sector length of `vol3` in the `Stanley.E01` image?
2. How many files are in the root directory of `vol4` in the `Stanley.E01` image?
3. How many photo/image files are there in the root directory of `vol3`?
4. What is the name, date and time of the oldest non-system file in the root directory of `vol4`?
5. There are 15 mp3 files in the root directory of `vol3`. Do you have any reason to believe that any of them are not genuine mp3 files?
6. Without extracting/opening the file, what do you believe is the source of and the contents of `curly_1709_librivox.zip` in `vol4`? How did you arrive at these views?
7. What is the 'short filename' of Attack Graph Workflow.png in the root of `vol3`? How did you determine this?
8. The email address: `ulf.haeussler@ndu.edu` appears in two files in the root of `vol3`: `Hutchins et al (2011), Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.pdf` and `Payroll.xls`. Do you believe there is a reason for this?
9. What did Brian Hoskins require of Ina Rangel on the 4th October 2000?
10. Are there any files 50MB in the image? If so, what are their names?
11. How many PDF file types are on the system? Is there any reason to believe that any of these are not actually PDF Files?

C Task 2, the Norman Case

Materials

A pre-created ingested case directory called `Norman` which requires the DFI: `Norman.E01` (also provided in the directory)

This tutorial is designed to enhance your understanding of Autopsy. Examine the `Normal.E01` DFI and answer the following questions.

1. What is the MD5 hash of the digital forensic image?
2. What is the timezone that the DFI is set to?
3. How many partitions does the DFI have?
4. How many of the above partitions have a valid file system and what format are these file systems?
5. At which sector does the first valid partition (`vol2`) end?
6. Is there any evidence that files or part of the file system may have been copied over from a cloud storage folder? If so, what is the evidence?
7. Is it possible to ascertain the make and model of camera used to take the picture of the rose? If so, what is the make and model?
8. What is the size of the master boot record on vol2
9. Does the size of the master boot record on `vol2` differ from the size of the master file table on `vol4`?
10. Is it possible to ascertain whether the active file: `TPS Report.docx` on `vol3` and the inactive (deleted) file `TPS Report.docx` on `vol1` are the same size? If so what is their size?
11. How many mismatched extensions are there in the DFI?
12. Of the files identified above, only one can actually be viewed in the `media` tab in the `content viewer`. This file has an incorrect extension. What should the correct extension of this file be?
13. How is it possible to verify what the correct extension of this file should be?

14. How many files have a `.png` or an extension similar to the term `.png`?
15. How many of the files found above are active files?
16. How many files were created, modified, accessed or changed between 01-May-2017 00:00:00 and 02-Jun-2017 00:00:00?
17. In which two years has the bulk of activity taken place in the DFI? utf-8

D Task 2, the Animal Case

Materials

A pre-created ingested case directory called `Animal` which requires the DFI: `Animal.E01` (also provided in the directory)

Summary of the proceedings and applications

The Wildlife National Parks Department is currently investigating a large number of animal welfare cases, and prosecuting according to the Animal Welfare Act 2006. The Department conducted raids on a number of properties believed to be offering wildlife for sale from around the world.

The department also conducted checks on a number of pet shops and possible web sites originating in the UK with the help of the Metropolitan Police.

Issues before the Court

1. *Whether or not the digital evidence has any connection to a web site concerned with the sale of animals.*
2. *Whether the device contains animal stock considered to be unlawful according to The Animal Welfare 2006 subsections 3,4,9*

Your instructions

Please address the following issues in your report:

1. Are any animals at risk in terms of cruelty and welfare?*
2. Is there any evidence of James Jones communicating with third parties?
3. Is there evidence of hidden data?

*For the purpose of this task, interpret the term *cruelty* very loosely.

E Task 3, the IP Theft Case

Materials

A pre-created ingested case directory called `IPTheft` which requires the DFI: `IPTheft.E01` (also provided in the directory)

Ms. Dotty is the secretary of Mr. John Muller, the head of dashboard research at WMB Cars. She was arrested from her office address (WMB Cars, Coventry, CV4 7ML) on 12th February 2015. She has been accused of stealing corporate data including highly confidential research designs. She is also accused of planning to sell the corporate data to a rival firm named 'SMB cars'.
A 4GB USB stick was seized by the West Lands police force from her office desk.
The suspect argues that she lost this USB stick six months before and claims that someone is trying to set her up, as a part of workplace politics.
Two witnesses have alleged that they saw Ms. Dotty taking photos in research head's cabin after office hours on multiple occasions but they were not able to provide indicative times. They believe that the photos were taken from the computer screen. The research head Mr. John Muller stated that Ms. Dotty was given an official warning on 3rd December 2012 for downloading corporate files onto an external drive. On that occasion, Ms. Dotty claimed that it was done to enable her to work from home. John Muller adds that there had been no further suspicious activities after that incident and that Ms. Dotty had earned a high privileged status in the last year due to her exceptional performance.
You are supplied with:

1. An 4 GB Genesys Logic Inc. Generic USB Storage (USB 2.0) with the serial number 000000000250. MD5 hash of the device is '883c067026eccb4085ea2511a3424a61'

You are to investigate:

1. Does the MD5 hash match?
2. What is the device ID and Timezone of the image?
3. Whether or not the Digital evidence shows any connection with the suspect.
4. Whether or not the Device contains any confidential corporate data which are owned by WMB Cars.
5. Whether or not the Device contains any evidence of IP theft and any communication regarding its sale.
6. Is there any evidence of Ms. Dotty's involvement in IP theft?

7. Are there any files containing confidential corporate data in the digital evidence?
8. Is there any evidence of Ms. Dotty communicating with a third party for the purpose of selling intellectual property?
9. Is there any evidence to show that a sale took place?
10. Is there any evidence of other employees involved in in the sale of corporate data?
11. Is there any form of obfuscation methods used in the evidence?
12. What is the timeline of activities that happened?

F Task 4: The M57 Registry

The `M57` registry and several others have been provided to you in a directory called `SampleRegistries`

Having completed the registry tutorial, you should examine the M57 registry and answer the following questions:

Operating System

1. What is the operating system (inc build)?
2. When was the operating system installed?
3. Who (which user) installed it?

Names and Accounts

4. What is the name of the computer
5. Who (appears to have) has an account on this system?
6. When did they last log in?
7. When did each of them last shutdown the computer?
8. What was the timezone the computer was set to?
9. What USB devices have been accessed on this system?
10. What WiFi networks have been accessed on this system?
11. What programs have been installed on this system? Is there evidence of programs having been uninstalled (see my paper)?

Note.
1. Expect to have to do more research. We have not covered every registry value that you will need. For instance, we did not cover timezones.
2. The M57 computer is running a newer operating system than the GregSchardt

G Task 5, the Hacking Case

Materials

A pre-created ingested case directory called `GregSchardt`.

A Dell CPi notebook was seized on 20th September 2004 with the serial number: VLQLW. An external 'home made' antenna (802.11b) was also seized.
It is alleged that the notebook was used for hacking purposes. It is also alleged that the Greg Schardt (the alleged owner of the notebook) has been parking his vehicle within range of Wireless Access Points (such as Starbucks and T-Mobile Hotspots) where he would then intercept internet traffic in an attempt to get credit card numbers, usernames & passwords.
It is acknowledged that you may not be able to answer every single question given herein. However you should attempt to answer most of these. Note that you may need an independent registry viewer to see some of the artefacts.

1. What is the image hash?
2. Is there any software that could be used for hacking on the notebook?
3. Is there evidence of any data that may have been generated as a result of the use of the software?
4. how many software did you find that may have been used for hacking?
5. Operating System
6. What was the operating system used on the notebook?
7. Was there another operating system installed on this machine prior to that?
8. When was the installation date of the operating system and any other programs (hacking software)?
9. Who was the registered owner?
10. What is the computer account name?
11. How many accounts are recorded (total number)?
12. What is the account name of the user who mostly uses the computer?
13. Who was the last user to logon to the computer?

14. Who is the administrator of this computer?
15. Does anybody else have administrative access to the computer?
16. How is administrator access to this computer secured?
17. Could this security be bypassed? If so how?
18. Based on the above what are the probabilities that Greg Schardt is Mr. Evil?
19. What is web based email address of the main user of this machine?
20. Ethereal, a popular "sniffing" program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?
21. What is the time-zone setting?
22. When was the last recorded computer shutdown date/time?
23. What are the IP address and MAC addresses of the computer?
24. What is the SMTP email address for Mr. Evil?
25. What are the NNTP (Mail server) settings for Mr. Evil?
26. What two installed programs show this information?
27. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?
28. This IRC program has the capability to log chat sessions. List 3 IRC channels that the user of this computer accessed.
29. What is the primary domain name?
30. List the network cards used by this computer
31. An internet search for vendor name/model of NIC cards by MAC address can be used to find out which network interface was used. In the above answer, the first 3 hex characters of the MAC address report the vendor of the card. Which NIC card was used during the installation and set-up for LOOK@LAN?

32. List 5 newsgroups that Mr. Evil has subscribed to
33. What type of wireless computer was the victim (person who had his internet surfing recorded) using?
34. What websites was Mr. Evil accessing?
35. How many executable files are in the recycle bin?
36. Are these files really deleted?
37. How many files are actually reported to be deleted by the file system?
38. Perform an Anti-Virus check. Are there any viruses on the computer?