Student Number: 10005864 **Case Examined:** Somerset

Findings

The following evidence items were found:

No.	Description of item	Significance to case	Full Provenance to include;	Method of discovery
1	A text file that appears to explain the case. It indicates that a Gang named "Grass without the weed" have been smuggling Cannabis hidden within pieces of turf trafficked unknowingly by innocent people at an airport.	Sets the scene of the case. Gives name of gang involved and that drug smuggling is the crime being committed.	**Name:** TheCase.txt **Is Deleted:** No **File Created**: 27/10/14 16:48:36 **Last Written:** 27/10/14 16:02:52 **Last Accessed:** 27/10/14 00:00:00 **Logical Size:** 386 **Physical Sector:** 1,582,687 **Full path:** C:\TheCase.txt	Discovered when loading case into FTK and looking at the file structure.
2	A text file in a deleted zip that contains several possible passwords.	Gives password to encrypted spreadsheet, username and password to yahoo account and steganography passwords with hints towards their locations.	**Name:** 1 **Is Deleted:** Yes **File Created**: 27/10/14 15:35:00 **Last Written:** 27/10/14 15:51:12 **Last Accessed:** 26/10/14 00:00:00 **Logical Size:** 253 **Physical Sector:** 1,582,703 **Full path:** C:\ Documents and Settings/ Administrator/My Documents/_.zip/1	This item was found when looking through archived and deleted items.
3	An encrypted spreadsheet that contains the gang's drug stock.	Gives evidence towards the gang's drug stock.	**Name:** Amounts.ods **Is Deleted:** No **File Created**: - **Last Written:** 26/10/14 12:43:00 **Last Accessed:** - **Logical Size:** 11,639 **Physical Sector:** 600,103 **Full path:** C:\Documents and Settings/Administrator/ My Documents/Amounts.zip/Amount.ods	Found after discovering a password to an encrypted spreadsheet. Searched for all encrypted files using Autopsy and found there was only one containing a spreadsheet.
4	A Yahoo Messenger chat log that has been moved and the file extension changed.	Reveals that a file has been marked as corrupted using WinHex.	**Name:** important.jpeg **Is Deleted:** No **File Created**: 27/10/14 15:48:01 **Last Written:** 27/10/14 02:28:46 **Last Accessed:** 26/10/14 00:00:00 **Logical Size:** 1,692 **Physical Sector:** 665,535 **Full path:** C:\Documents and Settings/Administrator/My Documents/My Pictures/important.jpg	Found from discovering the Yahoo username and password, Looked in program files and found Yahoo messenger. Found chat logs had been deleted but contact names remained. Used this to run a keyword search which found this file.

5	A chat log between Lord Turf and several of the members of his gang.	An address, password and evidence of a falling out within the gang.	Item not found on hard drive. Instead found at this address: https://uk-mg42.mail.yahoo.com/neo/launch?.rand=26gc824uahoof&action=notepad#4932827028 username: lordturf password: Grass123	Found logging into Yahoo messenger online using the located username and password.
6	A spreadsheet containing drug trafficking information.	It gives the date, amount and type of the drug trafficked for selected dates. Also gives airports transported between, the profit made and the names of the traffickers.	**Name:** Movements.xls **Is Deleted:** No **File Created**: 27/10/14 15:47:59 **Last Written:** 27/10/14 13:36:40 **Last Accessed:** 26/10/14 00:00:00 **Logical Size:** 11,741 **Physical Sector:** 601,255 **Full path:** C:\Documents and Settings/Administrator/My Documents/Movements.xls	Found looking through Microsoft Office files.
7	A word document containing a set of instructions for members of the gang to follow.	It explains how they should approach potential traffickers, who they should target and that they get paid. If a gang member's caught they're on their own, so shouldn't use their real name.	**Name:** Memo1.odt **Is Deleted:** No **File Created**: 27/10/14 15:47:59 **Last Written:** 27/10/14 15:00:04 **Last Accessed:** 26/10/14 00:00:00 **Logical Size:** 11,741 **Physical Sector:** 600,063 **Full path:** C:\Documents and Settings/Administrator/My Documents/Memo1.odt	Found looking through Microsoft Office files.
8	An image steged with a spreadsheet containing a list of gang members with addresses and phone numbers.	A list of gang members with their address and contact number. Everyone has an associated location and supervisor. Shows LordTurf has no supervisor.	**Name:** turf5.bmp **Is Deleted:** No **File Created**: 27/10/14 15:48:01 **Last Written:** 24/10/14 20:09:02 **Last Accessed:** 26/10/14 00:00:00 **Logical Size:** 15,116,598 **Physical Sector:** **Full path:** C:\Documents and Settings/Administrator/My Documents/My Pictures/Turf/turf5.bmp	Knowing steganography had been used on an image of a garden, looking through pictures ordered by size I found this item and analysing it in S-Tools confirmed a file was hidden inside.
9	An image steged with a spreadsheet containing drug trafficking information.	This item was already discovered. It appears LordTurf hide the wrong file, as in a chat log he discloses that he wanted to hide a list of files using the exact same method.	**Name:** suitcase.bmp **Is Deleted:** No **File Created**: 27/10/14 16:48:01 **Last Written:** 24/10/14 16:19:38 **Last Accessed:** 26/10/14 00:00:00 **Logical Size:** 15,116,598 **Physical Sector:** 670,104 **Full path:** C:\Documents and Settings/Administrator/My Documents/My Pictures/Turf/turf5.bmp	Knowing steganography had been used on a corrupted file, I located a suspect file and found the modified hex after mounting the E01 file using OSFMount and reverted it back. I then used S-Tools using the password already discovered and confirmed a file was hidden.

Possible Scenario

Based upon the evidence, a possible scenario is….

A suspected drug smuggler has been arrested, known as LordTurf. He was the leader of an organised gang with the motto “Grass without the weed”, who smuggle grass onto planes and ship it around the country. They have been doing so by approaching susceptible people at airports and asking them to carry the turf in their bags, following a set of instructions sent to each member.

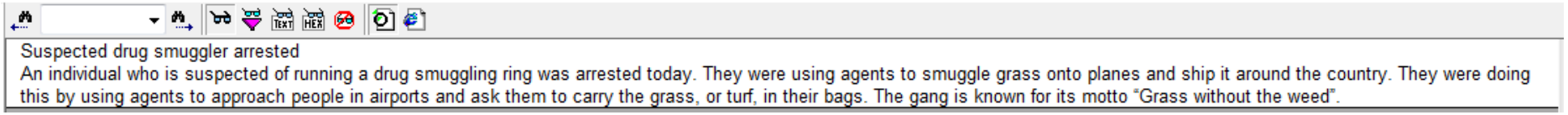
The type, stock and price that they were selling the drugs were located, along with the names of agents who have previously transported the drugs, the date, amounts, destinations and amount of profit the gang made from each. The structure of the gang was discovered, along with full names, addresses and phone numbers. A spreadsheet that contains the gangs transactions was also discovered.

The user has attempted to hide evidence using methods including:

- Steganography
- Encryption
- Bad File Extension
- Deletion
- File Corruption

Description of Evidence Items

Item 01



The file was found when first loading EnCase and sets the scene for the case. It indicates that a Gang named "Grass without the weed" have been smuggling drugs hidden within pieces of turf, likely to be Cannabis. They have approached innocent people in airports to unknowingly traffic the drugs to different locations. It appears that the leader of the gang was arrested and that this is his hard drive.

What to search for next

- Files relating to the gang or containing the words "Grass without the weed".
- Anything drug related.
- Information relating to airports.
- Files involving turf or grass.
- Key terms:
    - Grass
    - Weed
    - Cannabis
    - Drug
    - Airport
    - Turf
    - Grass
    - Smuggle

Item 02

```
excel sheet in zip folder : thisispr1vate
Yahoo username : lordturf
Yahoo password : Grass123
Locations steg password : stay0ut! type = IDEA image of a garden
Transactions steg : transactionz type = IDEA changed first FAT cluster from 36 3F to FF F7
```

This item was found when looking through archived and deleted items. It contains several useful items. It gives a password to an encrypted spreadsheet. Autopsy has one zip file listed as being encrypted and it contains an excel spreadsheet, so this password almost certainly will unlock it.

The next bit of information gives the username and password for the user's Yahoo messenger account. All the messages seem to be removed locally, but could still be found online. These details should unlock the account to see.

The remaining lines suggest two files contain steganography. I have found evidence of two Steganography tools using keyword searches, S-Tools and OpenPuff.

The first is hidden in an image of a garden and the password is stayOut! Looking through internet history I found this log:

- http://embeddedsw.net/OpenPuff_Steganography_Home.html
- C:/Documents%20and%20Settings/Administrator/Desktop/New/turf5.bmp
- C:/Documents%20and%20Settings/Administrator/My%20Documents/importantchat.txt

This suggests the file 'importantchat.txt' could be hidden in the file 'turf5.bmp' using OpenPuff. If not I will look through the images for a picture of a garden.

The second I will have to find the FAT cluster marked as FFF7 to find the file. I can then use the password transactionz to find the file.

Item 03

Type	Amount (kg)	Individual value(£ per kg)	Total value (£)
Long	100	200	20000
Cut	50	30	1500
Seeds	500	12	6000
Section	60	400	24000
Shavings	1000	300	300000

This item was found using Item 02. I searched for all encrypted files using Autopsy and found there was only one and it contained a spreadsheet. I used the password found in Item 02 and it unlocked the zip, allowing access to the hidden Amounts.ods file.

The file seems to document the gangs' total drug stock and the amount they plan to sell it for. It does not appear to link to any further items.

Item 04

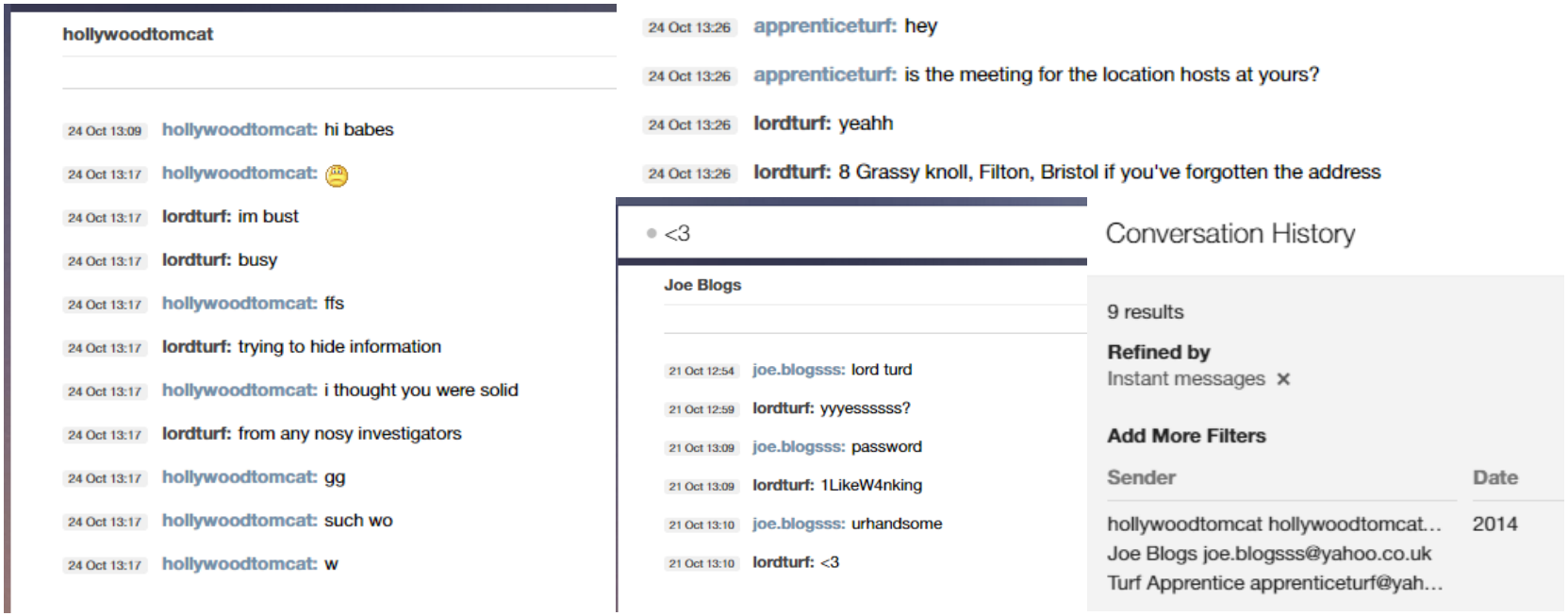
```
lordturf: how do i hide a file from view?
lordturf: like so it cant be opened at all
apprenticeturf: you could mark it either as encrypted or change the end of file
apprenticeturf: in a program called winhex
apprenticeturf: http://www.x-ways.net/winhex.zip
apprenticeturf: right here
apprenticeturf: some pretty decent instructions here too
apprenticeturf: http://www.x-ways.net/winhex/manual.pdf
lordturf: ok thats great thanks!
lordturf: got my passwords file that I don't want anyone to find :P
apprenticeturf: try putting it in a zip file as well, and then mark that as corrupt (FFF7 if
memory serves)
apprenticeturf: or just change the file extension in a zip, should do the trick
lordturd: ok cool, will do...
lordturf: im gonna save this chat too
lordturf: but ill change the file extension
apprenticeturf: good plan! (Y)
```

From seeing the Yahoo username and password, I looked in program files and found Yahoo messenger. I googled where Yahoo Messenger chat logs were held and found the file path existed. The folder structure showed that he had contacted ‘hollywoodtomcat’, ‘apprenticeturf’ and ‘Joe Blogsss’ but the chat logs had been deleted.

Running keyword searches on both these names resulted in a single jpeg. Viewing this file in Autopsy showed that it was actually a text file with a changed file extension as it displayed as above.

It reveals that a passwords file has been hidden in a zip and then marked as corrupted using WinHex. I will have to look for a corrupted zip file and see if it can be recovered.

Item 05



Using the Yahoo Messenger username and password recovered from Item 02, I was able to log in online. There are a total of 9 chat histories.

The first shows that ‘lordturf’ has been trying to hide information from investigators. The next gives his address, 8 Grassy Knoll, Filton, Bristol.

The final piece of interest gives a password, ‘1LikeW4nking’. I don’t require any passwords to files currently, but hopefully the file or account will reveal itself as I search for more items from the clues given so far.

There was also evidence that they were unhappy with one of the gang members are were planning on cutting communication with them. This could prove relevant to the case if more information is found.

Item 06

Date	Amount	Type	From	To	Profit	Agent
12/12/13	2kg	Seeds	Gatwick	Bristol	£100	Jamie Smith
14/12/13	1kg	Seeds	Heathrow	Manchester	£50	Howard Chase
15/12/13	1.5kg	Long	Gatwick	Glasgow	£200	Steve Donald
23/1/14	2.5kg	Shavings	Bristol	Glasgow	£750	Stuart Giles
25/1/14	2kg	Cut	Bristol	Gatwick	£60	Stuart Giles
30/1/14	3kg	Section	Heathrow	Manchester	£1200	Howard Chase
5/2/14	2kg	Seeds	Gatwick	Bristol	£100	Jamie Smith
6/2/14	1.5kg	Shavings	Bristol	Manchester	£450	Stuart Giles
10/2/14	1.5kg	Section	Heathrow	Manchester	£600	Howard Chase
11/2/14	2kg	Cut	Bristol	Glasgow	£60	Stuart Giles
13/2/14	1kg	Long	Gatwick	Bristol	£150	Steve Donald
14/2/14	2kg	Seeds	Bristol	Heathrow	£100	Stuart Giles
17/2/14	1.5kg	Shavings	Heathrow	Manchester	£450	Howard Chase

Looking through Microsoft Office files I discovered this item. It matches Item 03 with the items Seeds, Long, Shavings etc.

It gives the date, amount and type of the drug that has been trafficked for selected dates. It also shows the airports it has travelled between, the profit made and most importantly the name of the traffickers.

Keyword searching the names did not reveal any further information and the types of drug did not reveal any further information so does not appear to link to any further items.

Item 07

TO BE PASSED OUT TO ALL REPRESENTATIVES

Approaching potential smugglers

When approaching potential smugglers at an airport follow these simple steps to protect yourself as well as this organisation :

- Never give out your real name, although come up with a false one, telling a potential smuggler your name will endear you to them and make them less likely to back out
- Select younger individuals, late teens/early twenties are ideal, that are travelling in a pair or 3. Any more than that and they could get suspicious. Also, people with children would be perfect, however this is a no go as there is very little chance that a parent will willingly put their child at risk to make a quick bit of cash
- Try and choose someone with a larger suitcase, its easier to hide the grass in the lining, or in lots of clothes than it is in a smaller suitcase.

Once you have acquired your smuggler and they are happy to carry the grass, make sure you give them all the details i.e. where they're going, who they're meeting, how much they need to carry and how much they will be paid for this trip. Then make yourself scarce, if this thing goes sideways you must not be caught or placed at the scene of a crime.

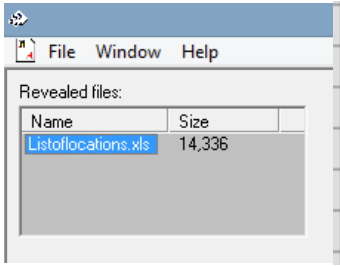
If you are caught you are on your own. For obvious reasons we cannot be seen to help you as it may incriminate higher up members of this organisation. We will do what we can behind the scenes, even though it may not seem like it. We have people we can call, but DO NOT give them any information that could lead back to us. This is imperative.

Remember, our catchphrase is Grass without the Weed.

Continuing to look through Microsoft Office files I discovered this file. It appears to be a set of instructions for members of the gang to follow. It explains how they should approach potential traffickers, who they should target and that they should not give out their real name. It details that they pay anyone who traffics the turf and that if any of the gang members are caught they are on their own.

Again, this unfortunately does not seem to link to any further evidence items.

Item 08



Location number	Location name	Host	Supervisor	Address	Contact no.
1	Main Warehouse	TurfLord	n/a	8 Grassy knoll, Filton, Bristol	07777777712
2	Docks	James Briggs	TurfLord	54 The WaterFront, Bristol	07777458744
3	Tube	Mark Feln	TurfLord	907 St James' Park, London	07854962145
4	Backup Warehouse	Chris Houser	TurfLord	43 Sackville Street, Reading	07215489664
5	Centre	Harold Draster	Chris Houser	22 Don Close, Reading	07548961236

Having exhausted any further obvious items, I decided to locate and decrypt the Steganography items.

The first is item was given a clue of it being an image of a garden with the password stayOut! Looking through internet history I found this log:

- http://embeddedsw.net/OpenPuff_Steganography_Home.html
- C:/Documents%20and%20Settings/Administrator/Desktop/New/turf5.bmp
- C:/Documents%20and%20Settings/Administrator/My%20Documents/importantchat.txt

This suggests the file ‘importantchat.txt’ was hidden in the ‘turf5.bmp’ using OpenPuff. There was further evidence of this after keyword searching ‘turf5’ and finding the original was a jpeg. This made it very suspect as the only advantage to changing the file to a bmp is to store a larger file inside it using Steganography.

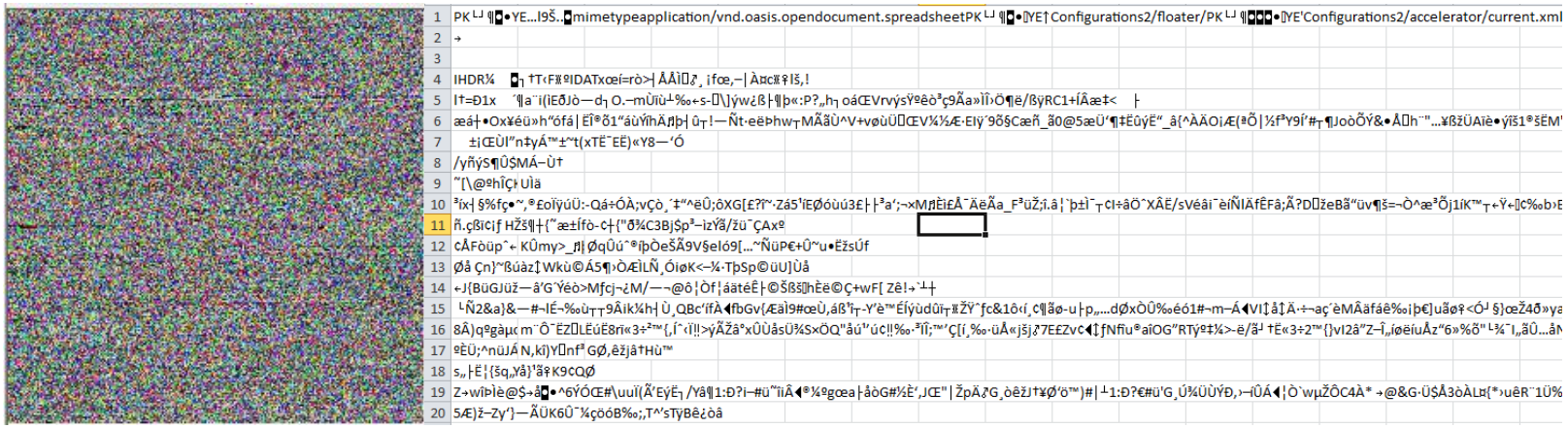
I also found evidence of S-Tools being installed, so suspected that both tools had been used between the two items.

Following the log above I attempted to unsteg the file using OpenPuff, but was only receiving error messages. I began to think more passwords were involved, as OpenPuff allows you to use up to three. However, before taking action on this assumption I decided to try S-Tools first as it was a simpler option. Thankfully it successfully unlocked the above file as shown.

The file itself appears to give a list of members of the gang along with their address and contact number. It also has an associated location name along with a supervisor. As TurfLord has no supervisor, it is safe to confirm the assumption made earlier that they are the head of the gang.

This is a key item to have collected, but unfortunately does not appear to lead to another.

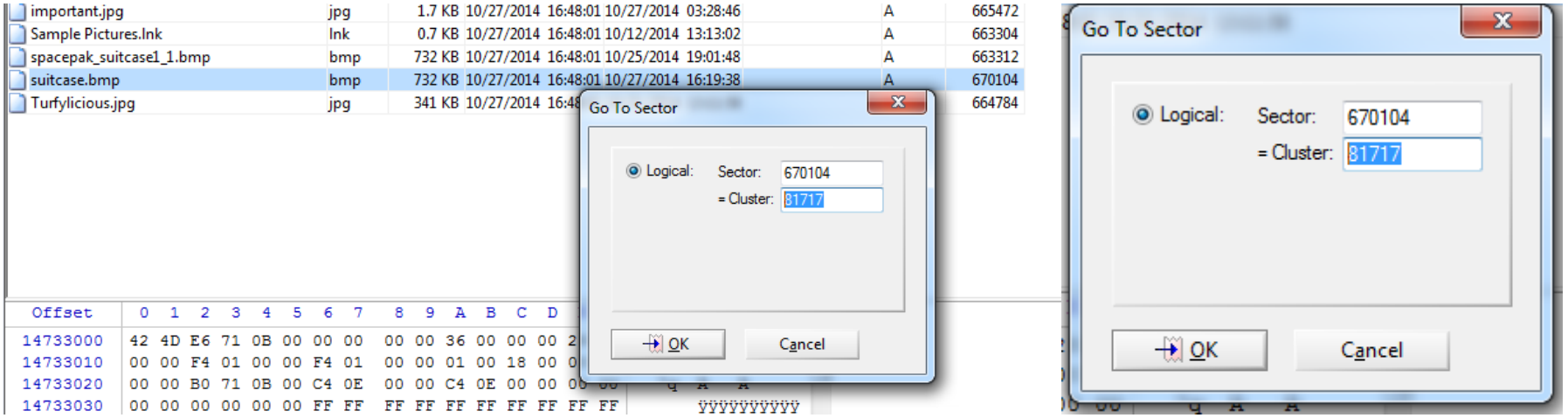
Item 09



From the evidence I had already collected I was looking for a file, likely contained within a zip that had been manually corrupted and contained steganography.

I began by looking for zip files that had been corrupted, but couldn't find anything that matched. I then looked through several large files, looking for FFF7 in the header, but found nothing.

After this I realised that the FFF7 wouldn't be in the file itself, but the hex pointing to the file. I also found the above file 'suitcase.bmp' that appears to be corrupted, especially when compared to a file named 'Copy of suitcase.bmp' of the same size that displays correctly. When trying to unsteg this file, the file above was discovered.



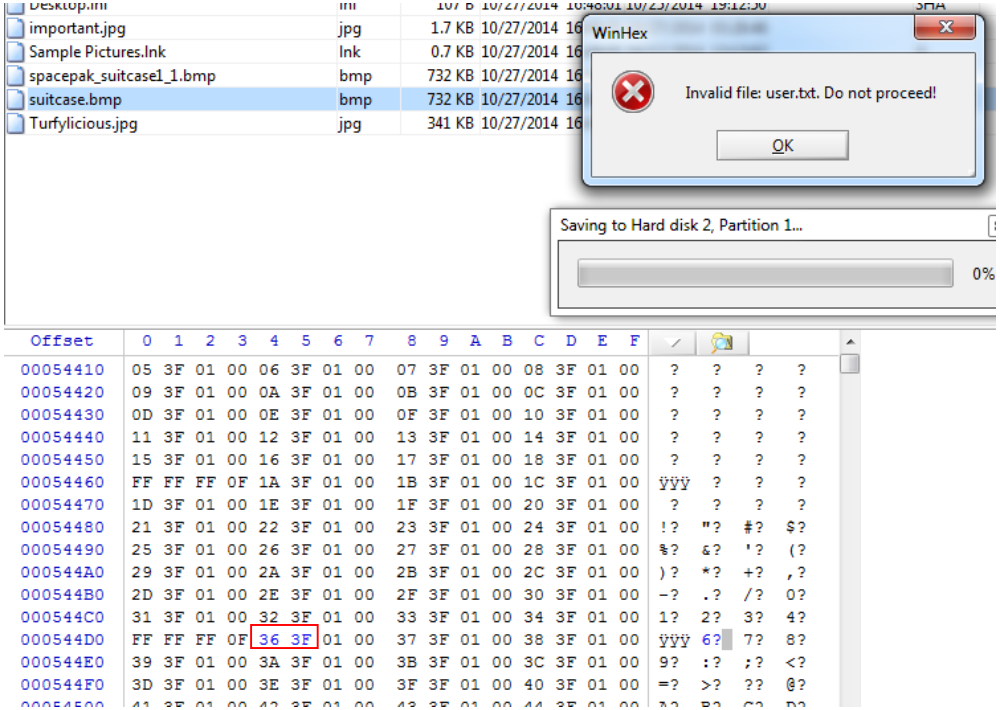
As shown above I mounted the drive using EnCase and viewed it using WinHex. I selected the file and copied the sector value. I then used this to locate the cluster value and moved to it.

The image to the left shows where the hex had been modified to FFF7 and that I have changed it back to 363F. From this point I went to save the change made, but as it was a virtual disk I was unable to do so.

I then followed the same method, but used OSFMount to mount the E01 file with read/write access. This resulted in the image above now displaying as shown to the left.

Finally I dragged the image into S-Tools and used the password 'transactionz' to unsteg the image. The file that was extracted turned out to be the same as item 6.

It appears that LordTurf made a mistake, hiding the wrong file within the image. In the chat log it stated that he wanted to hide a list of passwords and it's clear that this is the image that it was intended to be hidden within.

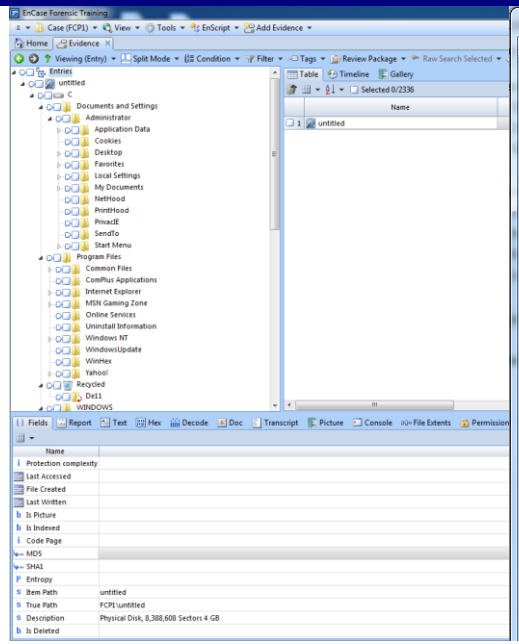
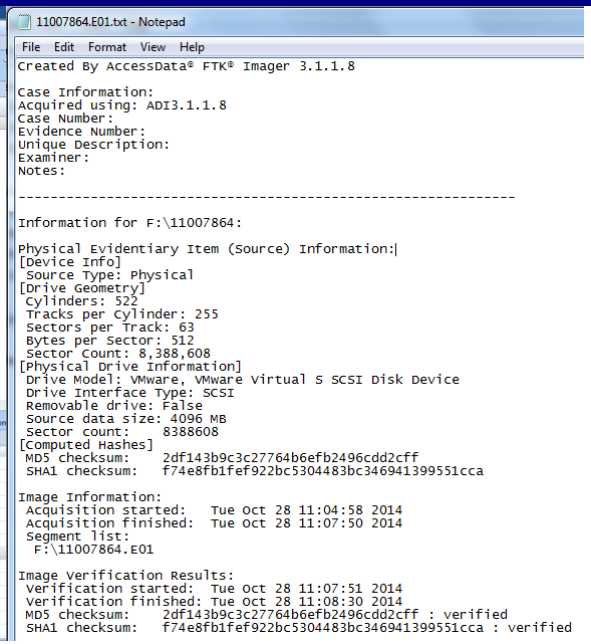


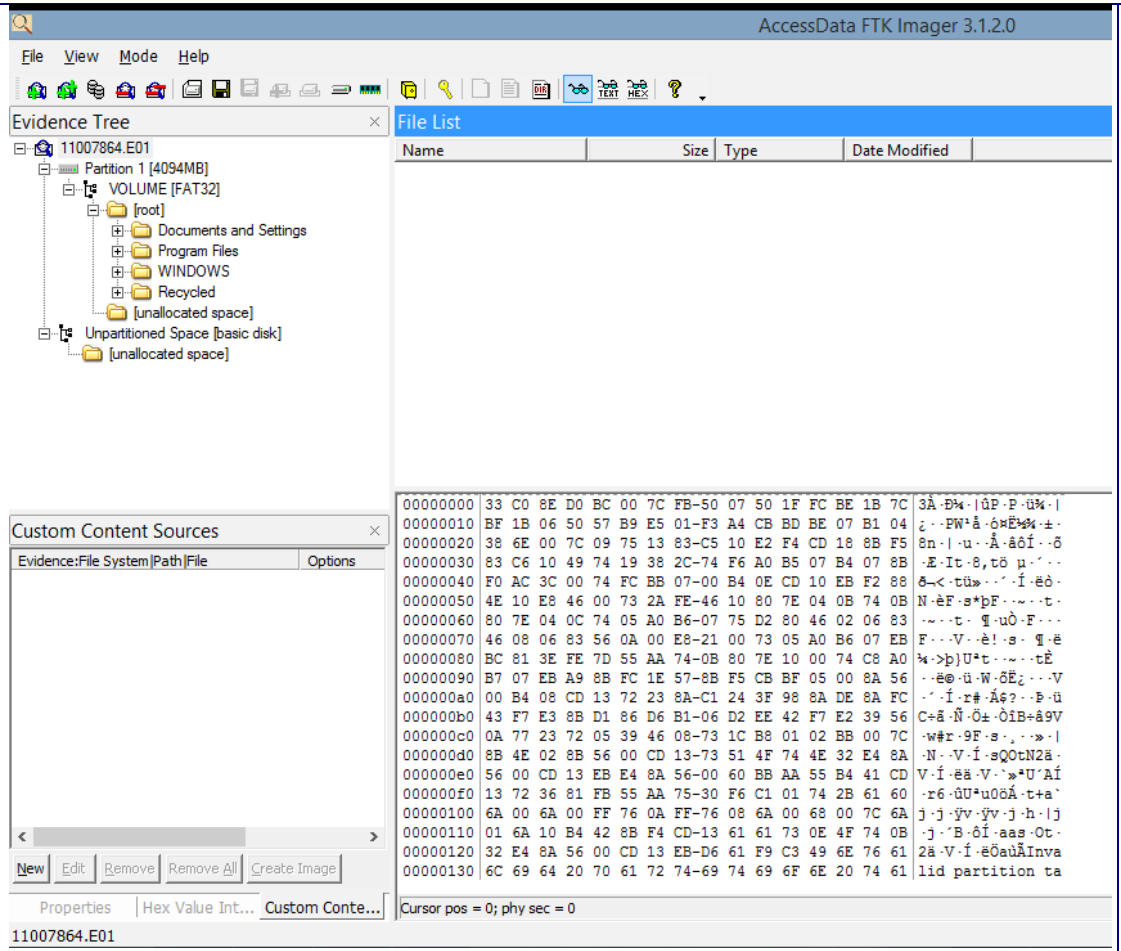
Unfortunately, this now ends the trail, as no other leads can be located using the items recovered and no other items can be located.

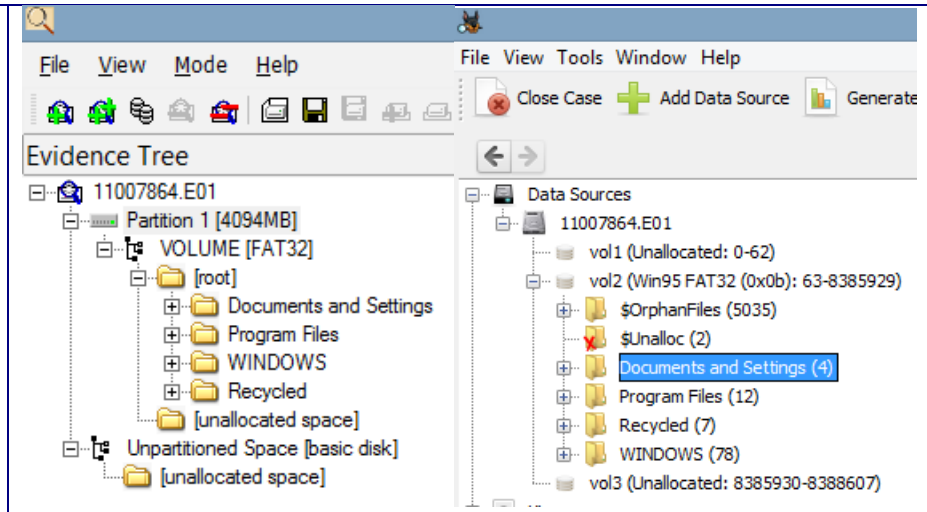
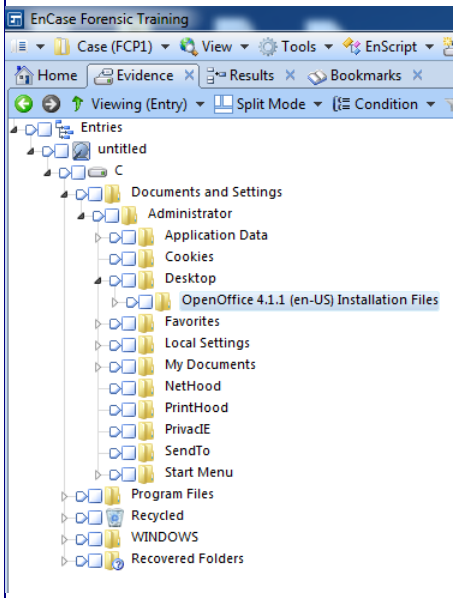
Date	Amount	Type	From	To	Profit	Agent
12/12/13	2kg	Seeds	Gatwick	Bristol	£100	Jamie Smith
14/12/13	1kg	Seeds	Heathrow	Manchester	£50	Howard Chase
15/12/13	1.5kg	Long	Gatwick	Glasgow	£200	Steve Donald
23/1/14	2.5kg	Shavings	Bristol	Glasgow	£750	Stuart Giles
25/1/14	2kg	Cut	Bristol	Gatwick	£60	Stuart Giles
30/1/14	3kg	Section	Heathrow	Manchester	£1200	Howard Chase
5/2/14	2kg	Seeds	Gatwick	Bristol	£100	Jamie Smith
6/2/14	1.5kg	Shavings	Bristol	Manchester	£450	Stuart Giles
10/2/14	1.5kg	Section	Heathrow	Manchester	£600	Howard Chase
11/2/14	2kg	Cut	Bristol	Glasgow	£60	Stuart Giles
13/2/14	1kg	Long	Gatwick	Bristol	£150	Steve Donald
14/2/14	2kg	Seeds	Bristol	Heathrow	£100	Stuart Giles
17/2/14	1.5kg	Shavings	Heathrow	Manchester	£450	Howard Chase

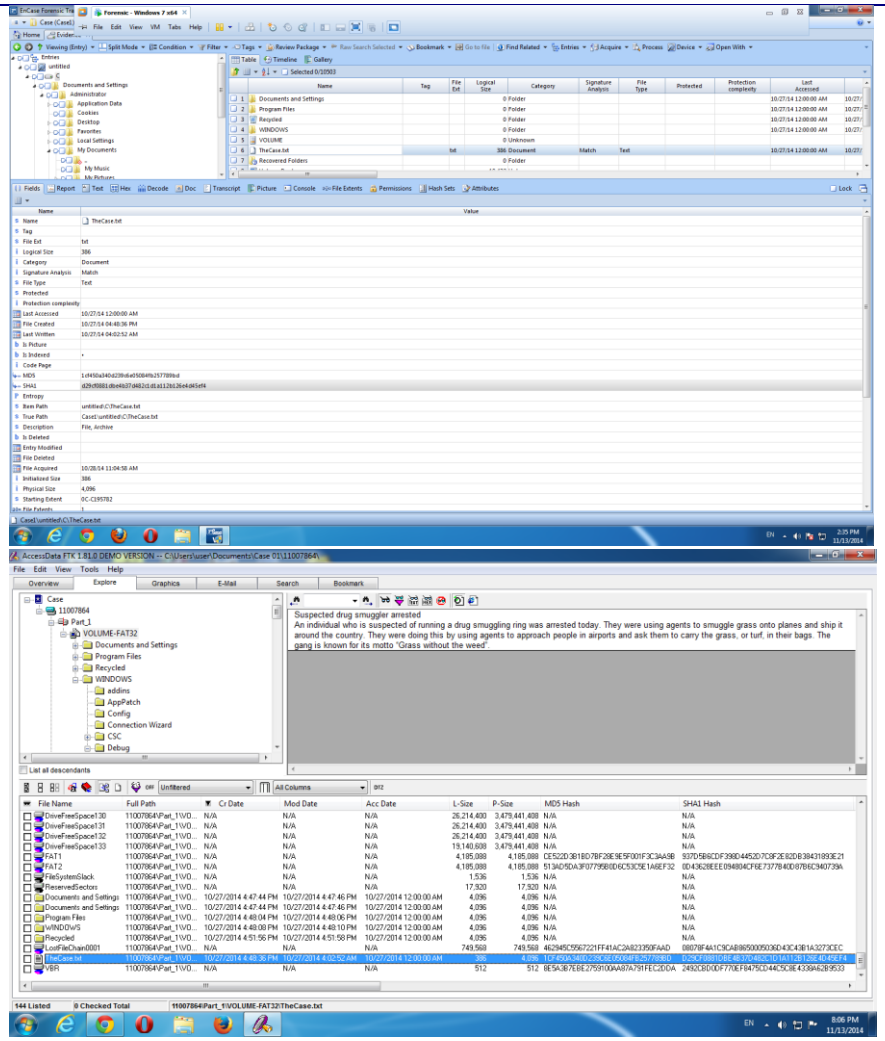
Suspect Details	Exhibit numbers, Computer details, HDD's / Partitions / OS etc.
'LordTurf' / 'TurfLord' 8 Grassy Knoll, Filton, Bristol Contact Number: 07777777712	Single hard drive recovered. Operating System: Windows XP Hard drive recovered: C: - FAT32 D:, E: F: and G: drives were also detected.

Client	University of the West of England	Reference	Somerset
OIC (plus contact details)	Dr. Lindsey Gillies - Lindsey.gillies@uwe.ac.uk	Bailed to Return Date	18 November 2014
Seize Date	28 October 2014	Case Type	Coursework
Examiner	David Norton	Exam commenced	03 November 2014
Other relevant information		Software used, versions and licensing	• FTK 1.8.1 • EnCase 7 • Autopsy 3.1.1 • WinHex • S-Tools • OpenPuff • OSFMount • SamInside • RegRipper

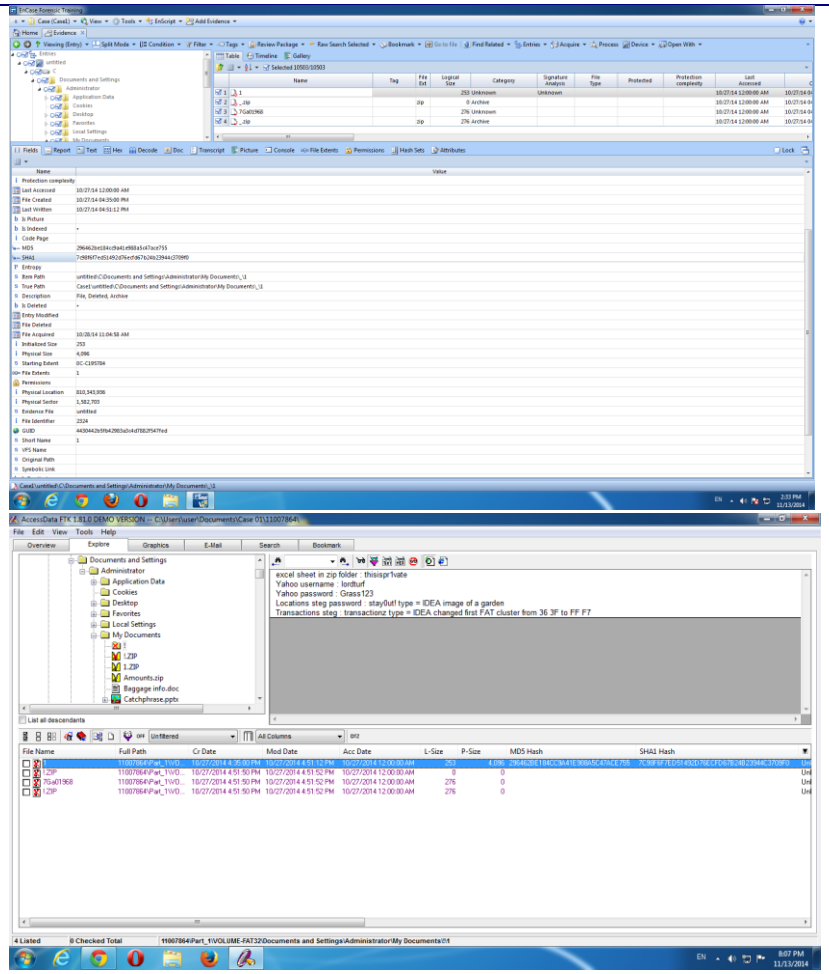
Action	Done	Date	Time	Notes	Initial
Load case & verify in EnCase	YES	03/11/2014	11:37	  Loaded into EnCase correctly. MD5 hash was not displayed, but MD5 hash is displayed in the FTK Imager report.	

Load case into FTK Imager	YES	08/11/2014	18:39	 Loaded correctly into FTK imager.	

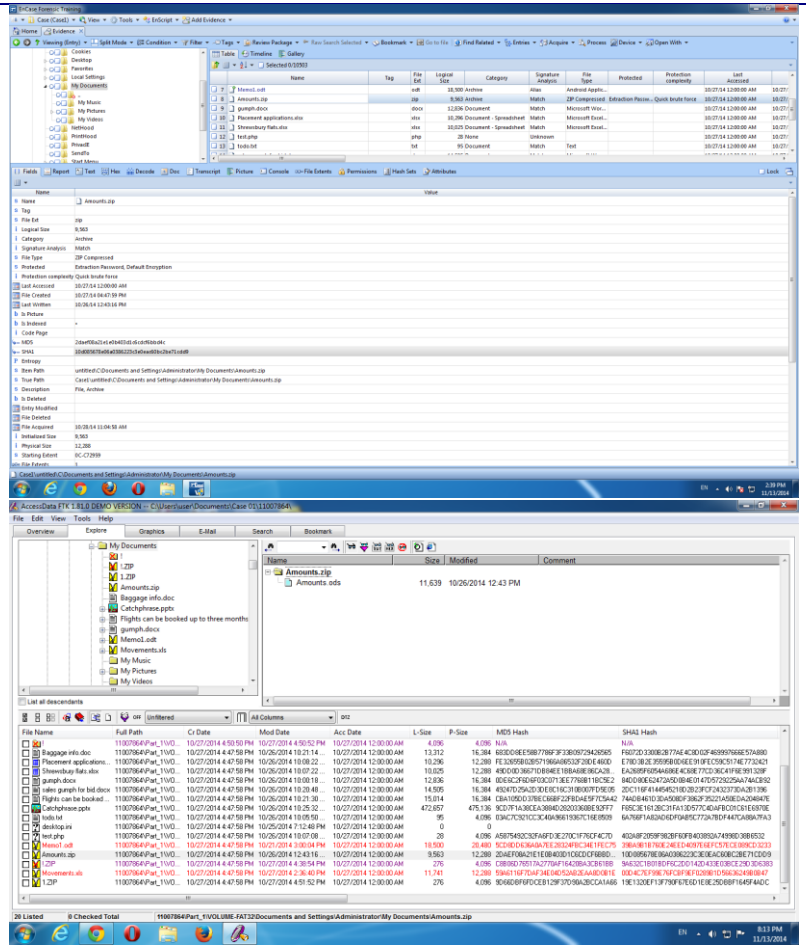
Dual verification of key evidence items.	YES	08/11/2014	18:48	 	Folder structure remains constant between FTK, EnCase and Autopsy. Only difference is the format that unallocated space is displayed. Autopsy also discovered a third volume.	



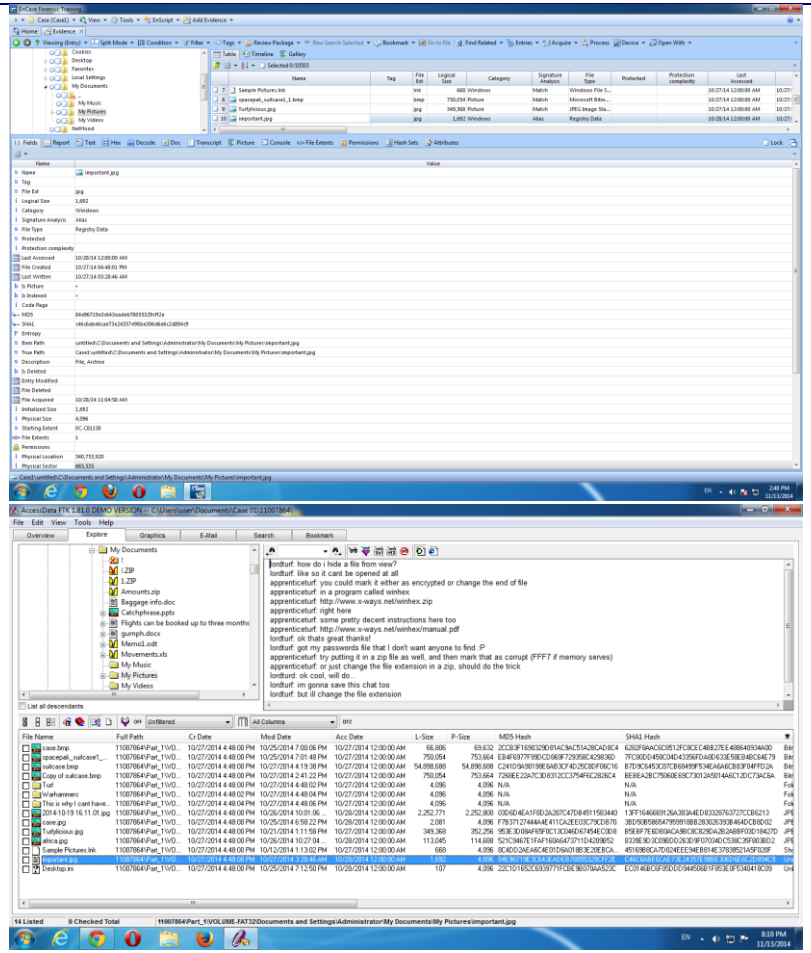
Item 1: Location, Size, MD5 & SHA1 Hash all match.



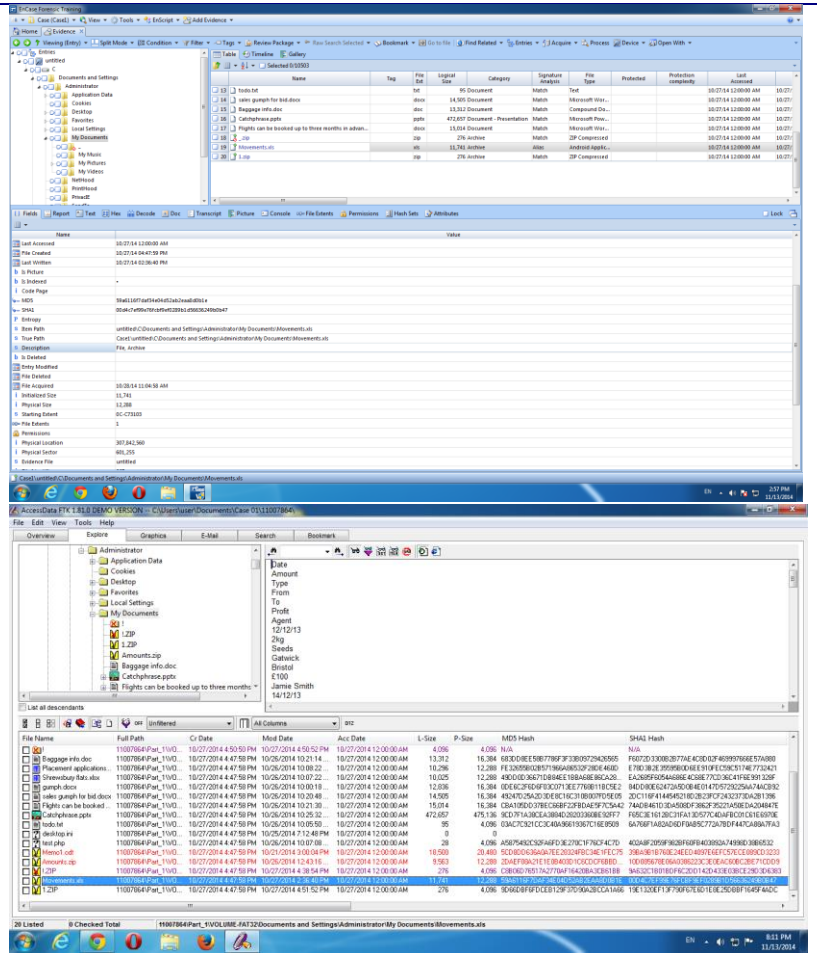
Item 2: Location, Size, MD5 & SHA1 Hash all match.



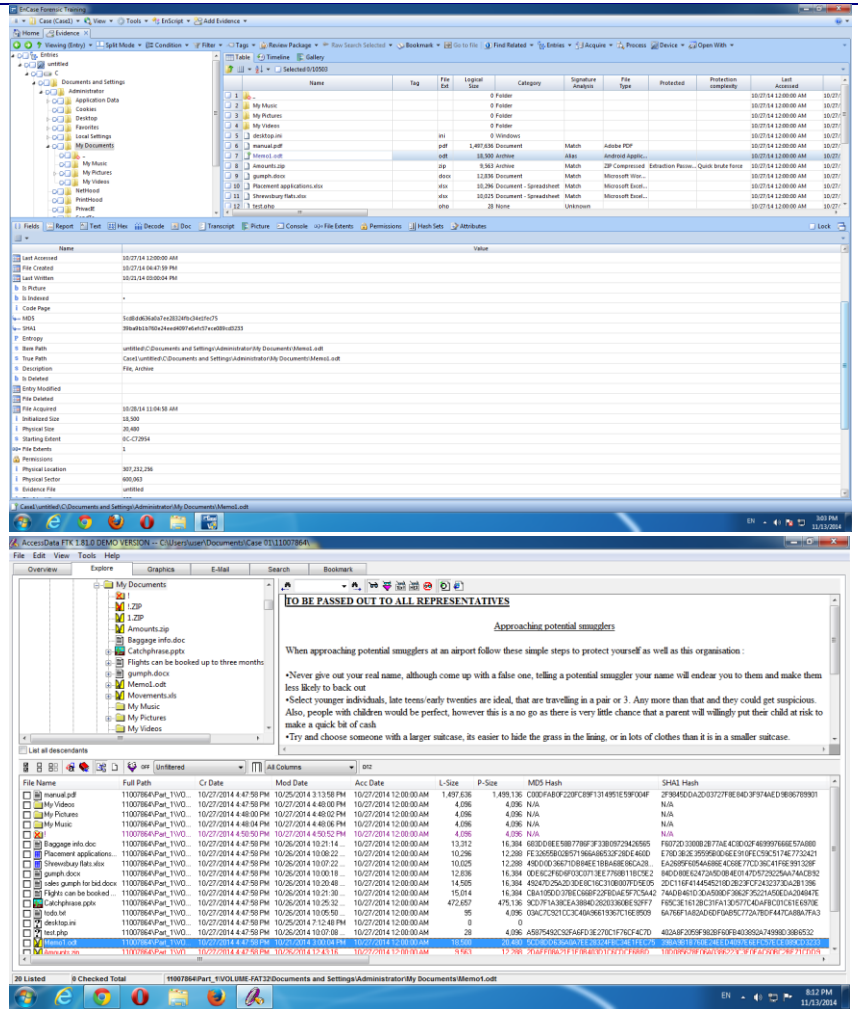
Item 3: Location, Size, MD5 & SHA1 Hash all match.



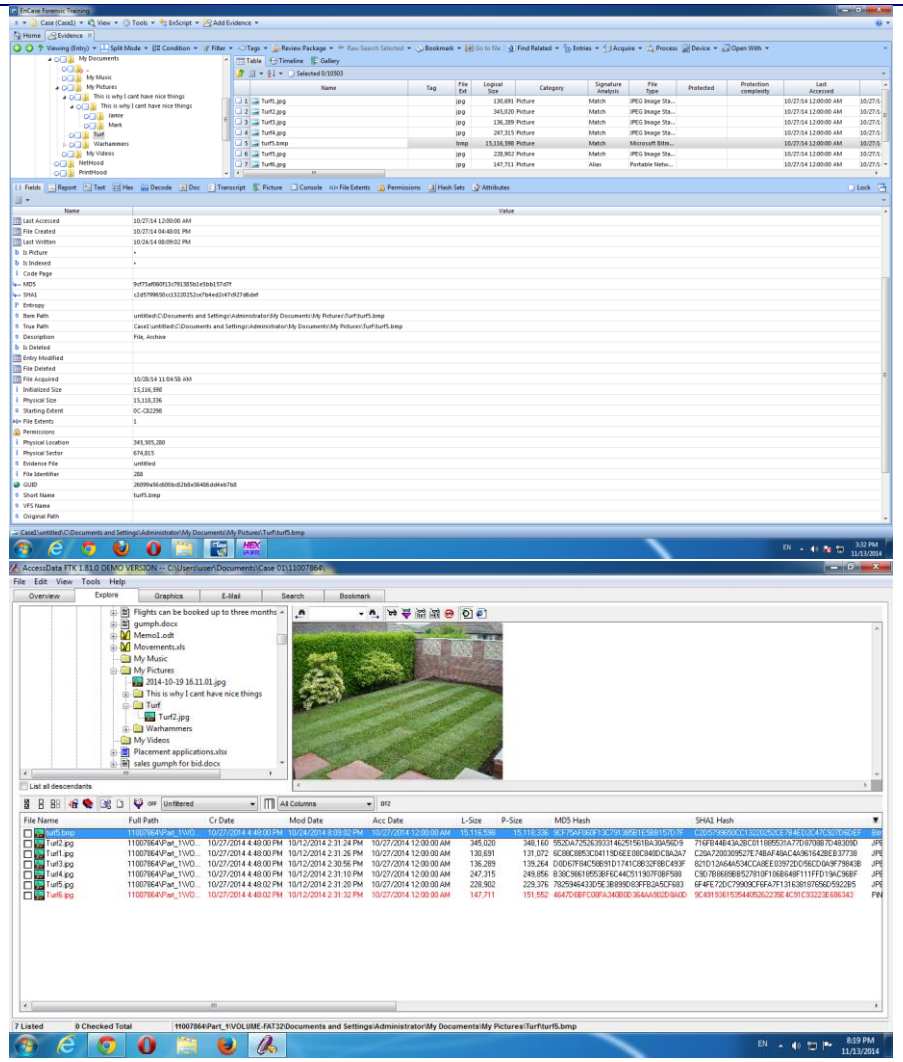
Item 4: Location, Size, MD5 & SHA1 Hash all match.



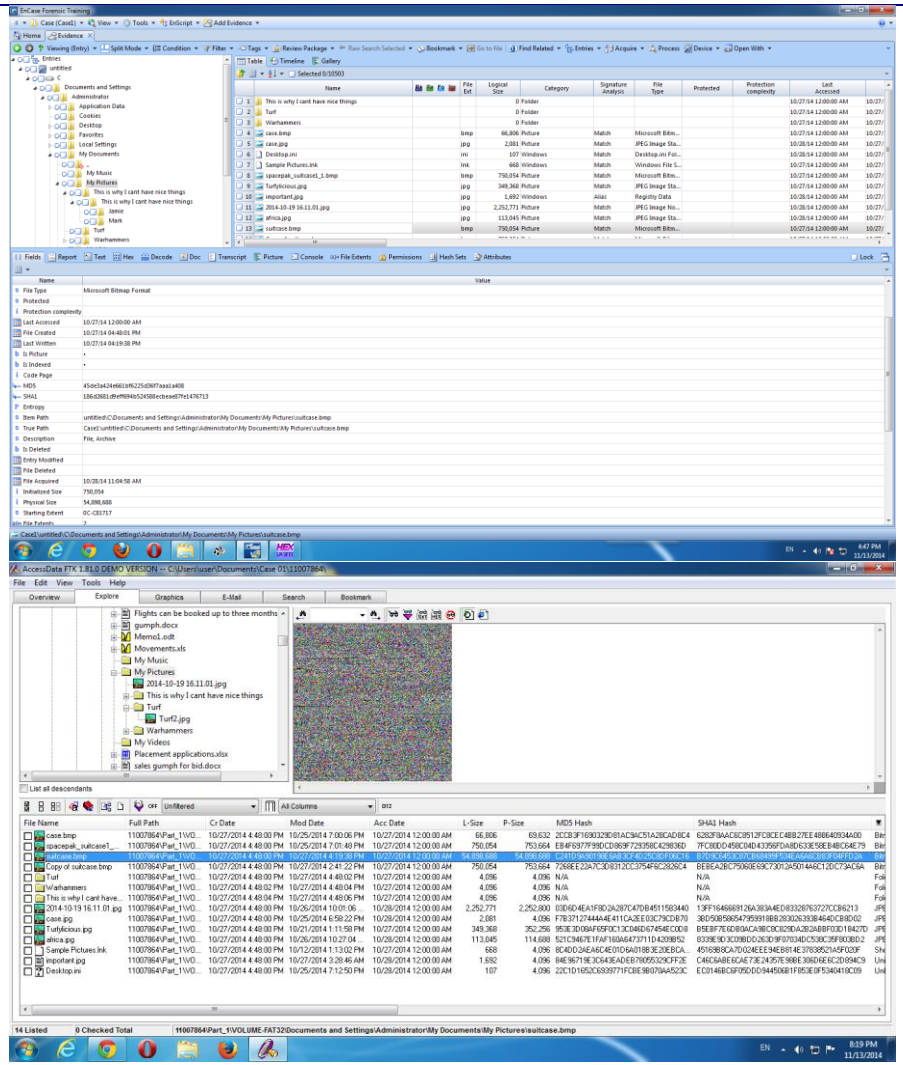
Item 6: Location, Size, MD5 & SHA1 Hash all match.



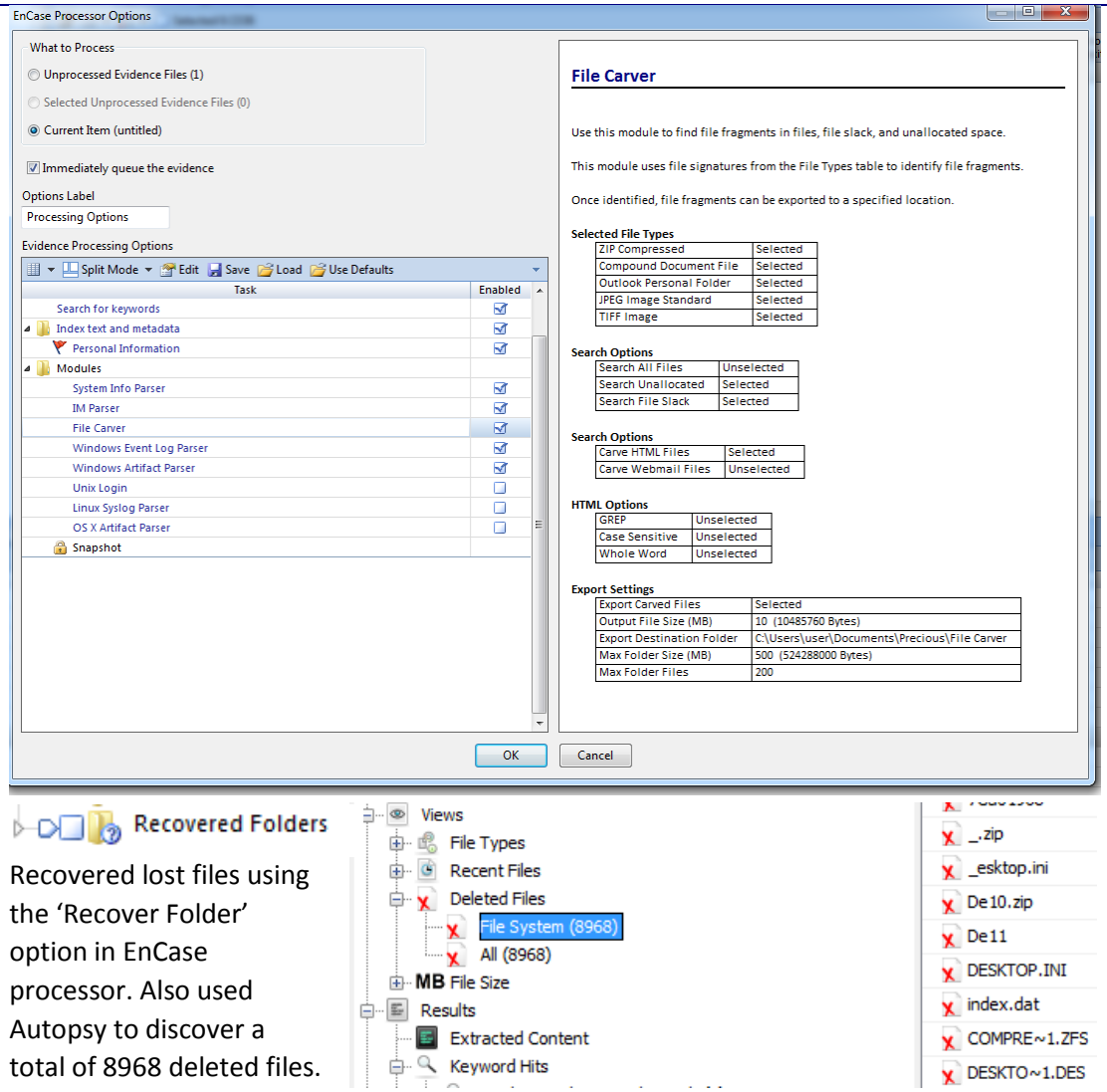
Item 7: Location, Size, MD5 & SHA1 Hash all match.

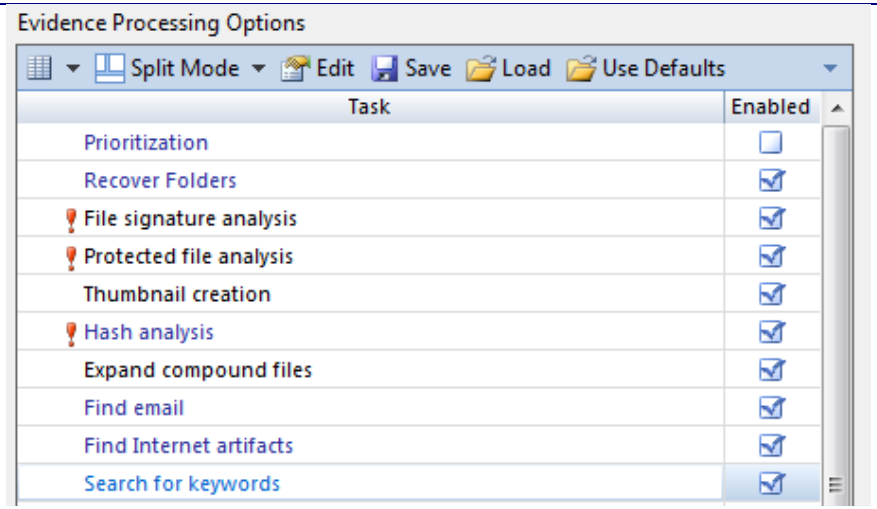


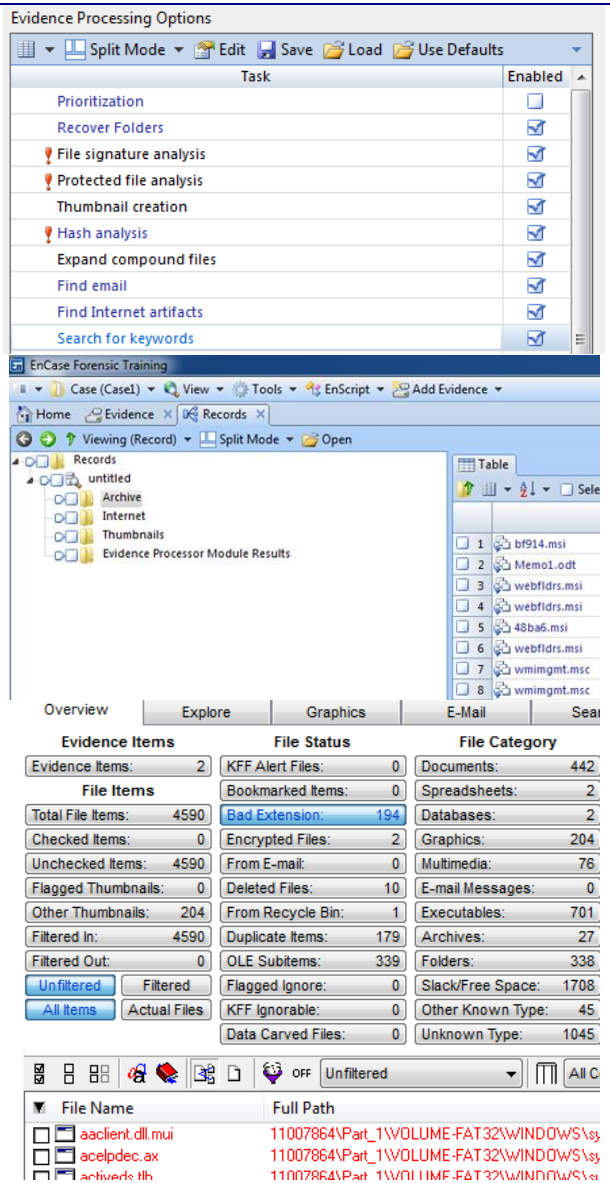
Item 8: Location, Size, MD5 & SHA1 Hash all match.

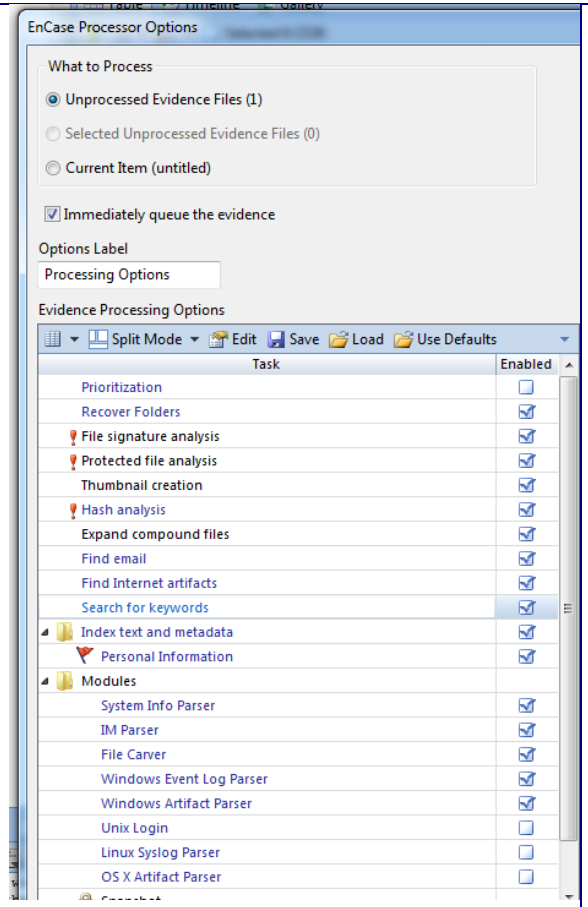


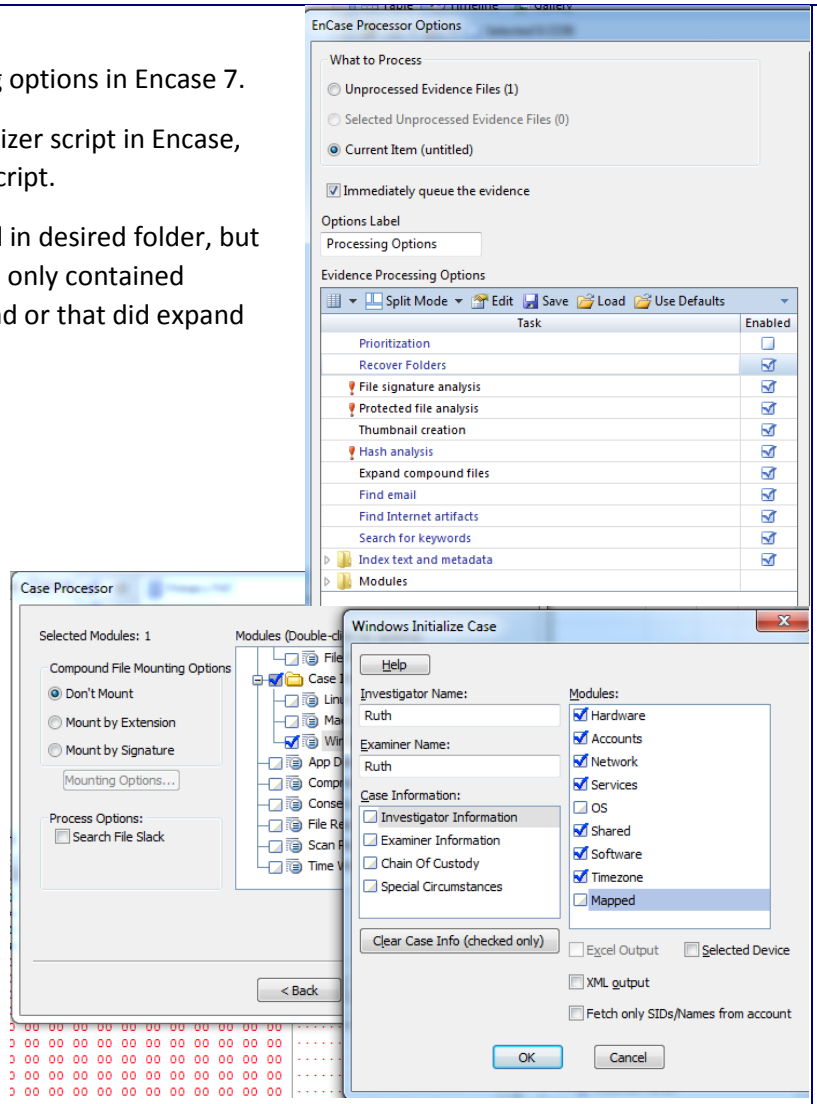
Item 9: Location, Size, MD5 & SHA1 Hash all match.

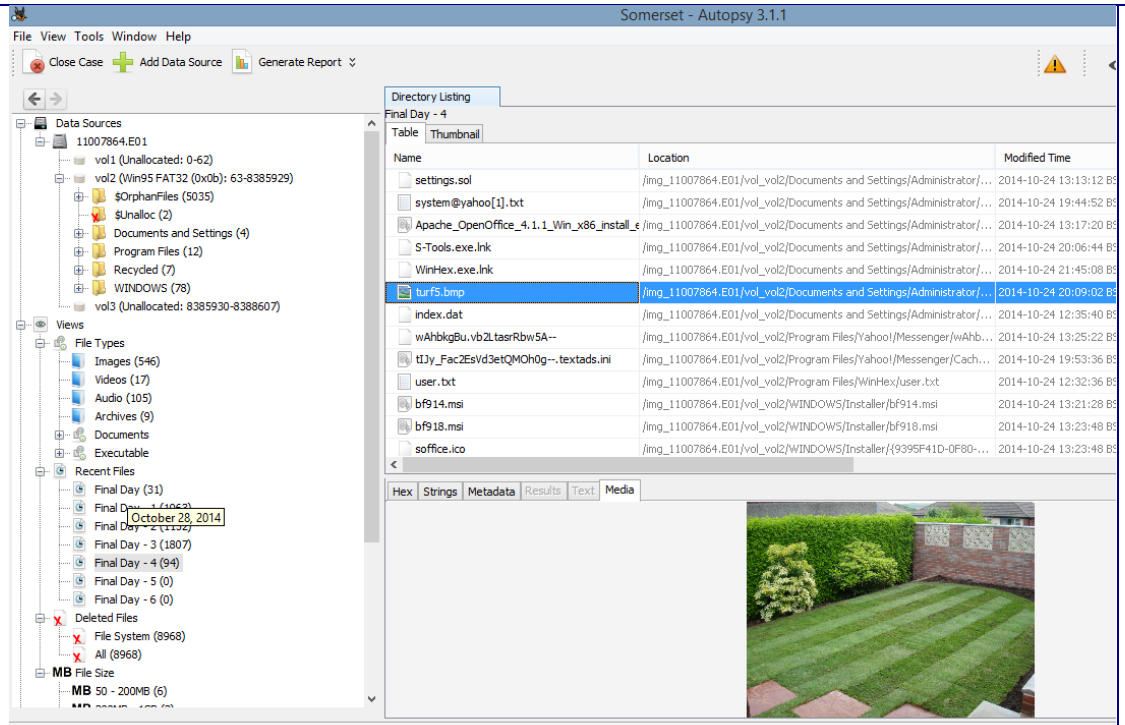
Recover lost folders (FAT16 & 32).	YES	03/11/2014	11:41	 Recovered Folders Recovered lost files using the ‘Recover Folder’ option in EnCase processor. Also used Autopsy to discover a total of 8968 deleted files. 	

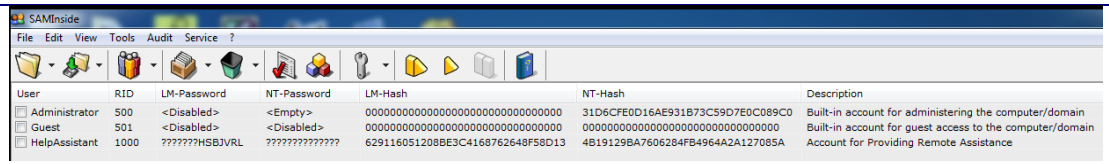
Mount archives; zip, thumbs.db, etc	YES	03/11/2014	11:41	 Mounted all archive files using the 'Expand compound files' option in EnCase processor. Found a key evidence item in a deleted zip using this method.	

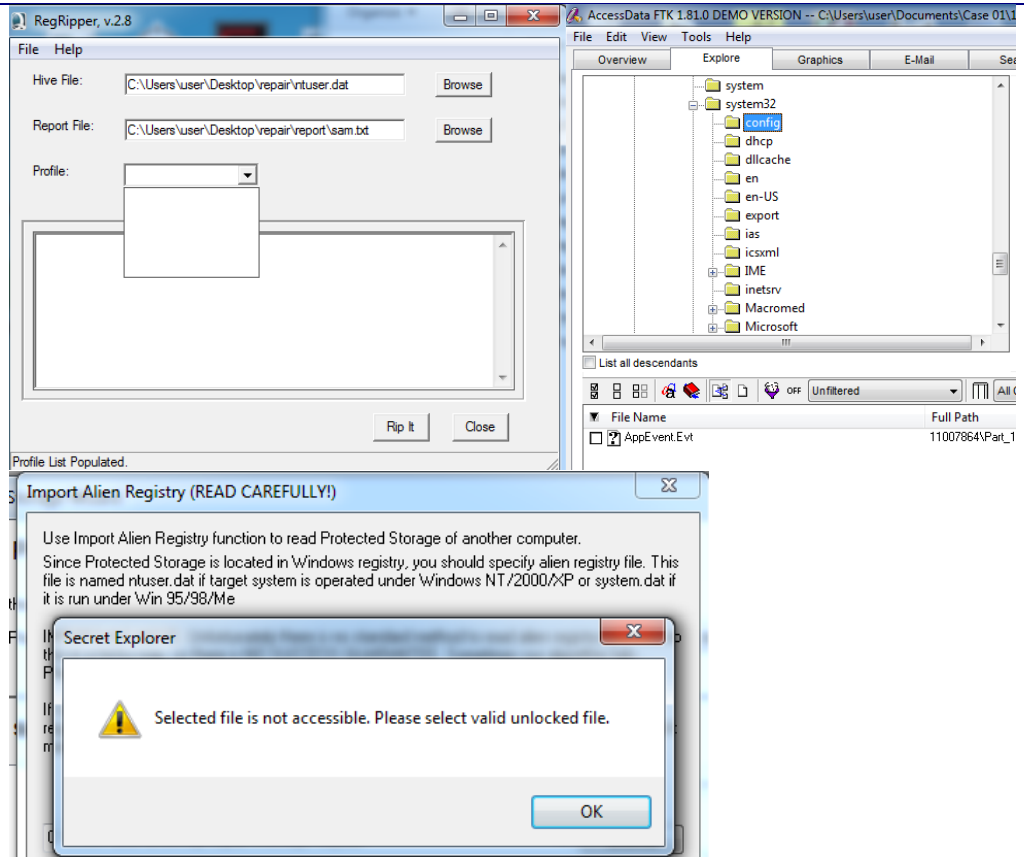
File signature analysis, compute hash values	YES	03/11/2014	11:41		Ran File Signature Analysis, Protected File Analysis and Hash Analysis in EnCase processor. Found a key evidence item in a deleted zip using this method. The results could then be analysed in the Records tab in EnCase. Files with bad file extensions could also be easily viewed in FTK.	

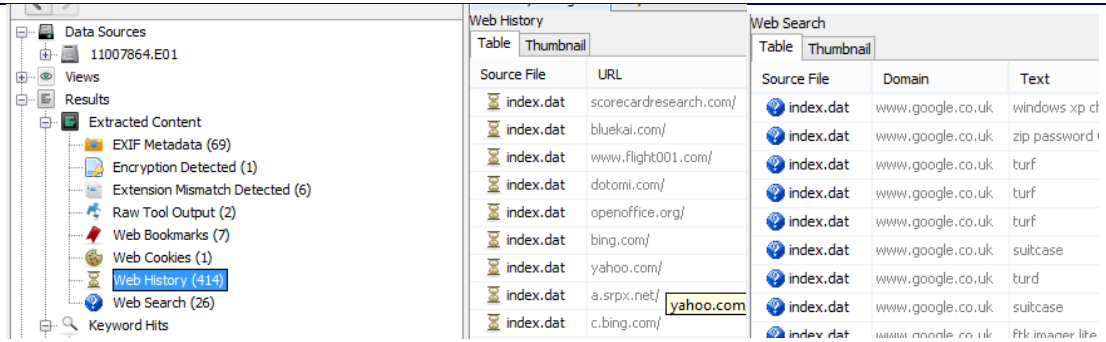
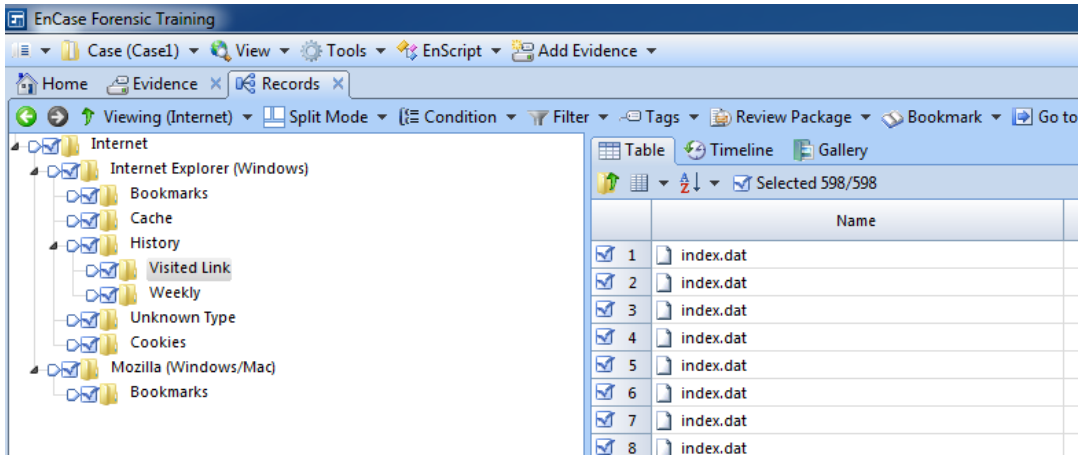
Run filefinder	YES	03/11/2014	11:41	Ran File Carver in EnCase's Processor Options. Unfortunately this did not find any additional files of obvious interest. 	

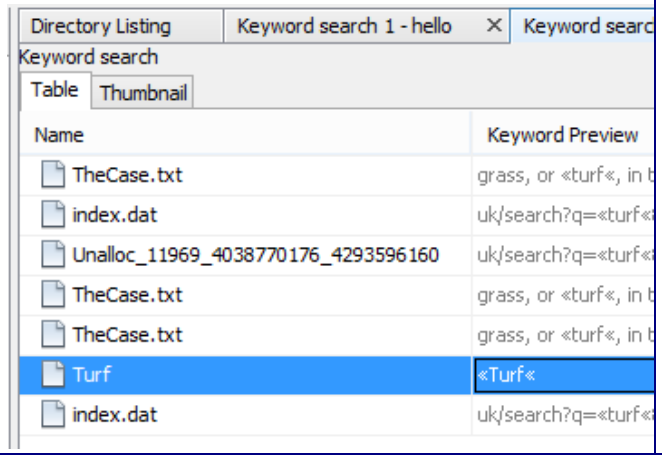
Initialise Case script	YES	03/11/2014	11:51	Completed all processing options in Encase 7. Also used the Case Initializer script in Encase, selecting the Windows Script. The script was generated in desired folder, but unfortunately the results only contained information already found or that did expand on the case. 	

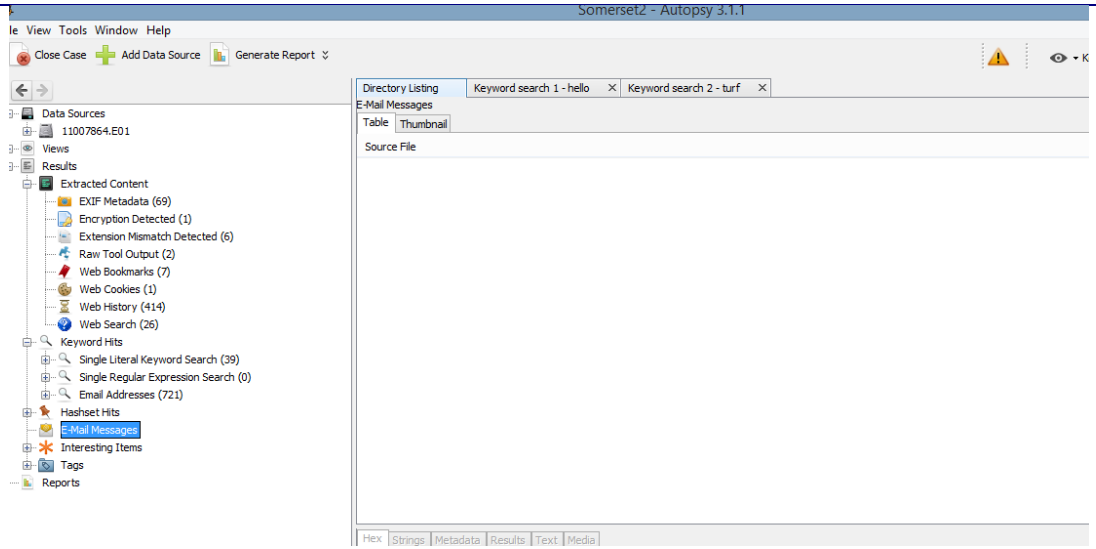
Timeline analysis, date of last activity	YES	08/11/2014	21:24	 Autopsy has a feature that gathers files into days of activity. This feature allowed the finding of the latest files edited before the image was created. This helped to find key evidence items, as such as finding an image that had been downloaded right after they had searched for Steganography.	

Log-on passwords – use SAMInside	YES	09/11/2014	00:26	 SAMInside found that there was no password set for the administrator account and was only able to find part of the HelpAssistant password. No other useful user account was detected.	

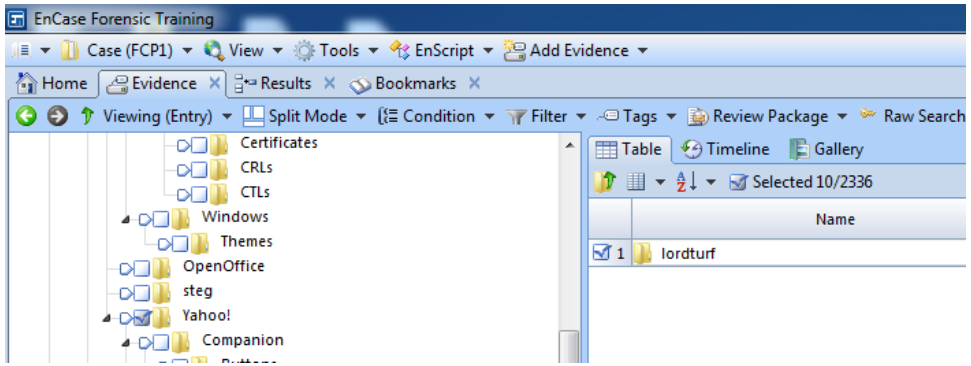
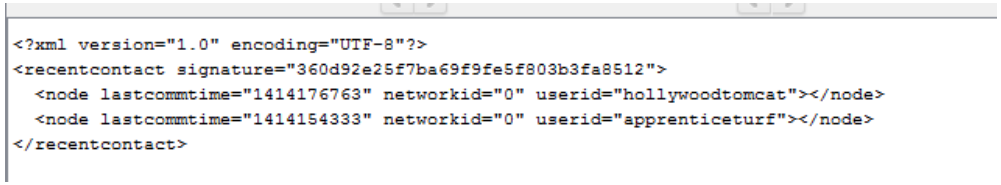
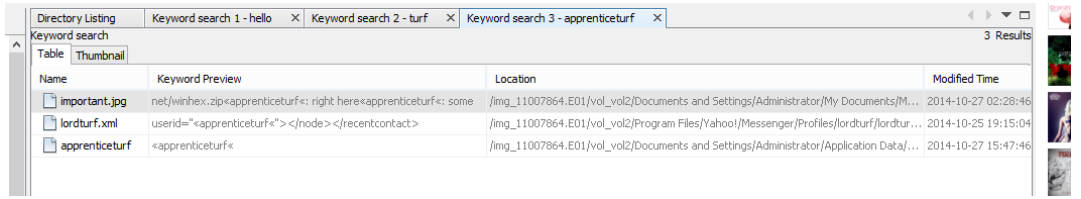
Registry protected area (Secret explorer)	YES	09/11/2014	00:57	 As the system32/config folder contained none of the usual files and there were no backup files, I attempted to use the repaired files instead. Unfortunately, these would not work in Secret Explorer or RegRipper.	

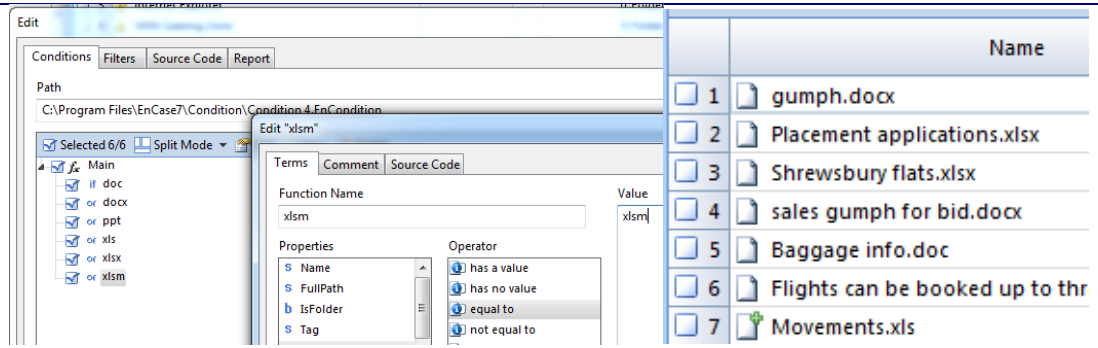
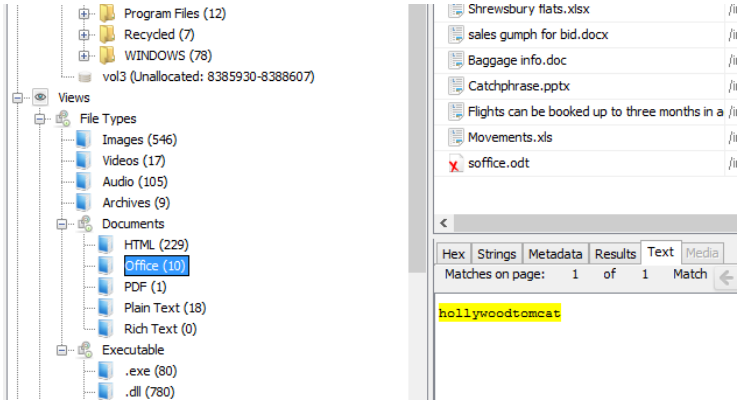
Internet History, favourites. Other browsers? Netanalysis	YES	09/11/2014	16:55	  Using EnCase I was able to find the users search history via the evidence processor tool. However, it made it difficult having to look through each file individually. Autopsy made it far easier by displaying web history and search terms as a list. This helped to find what steganography software was used.	

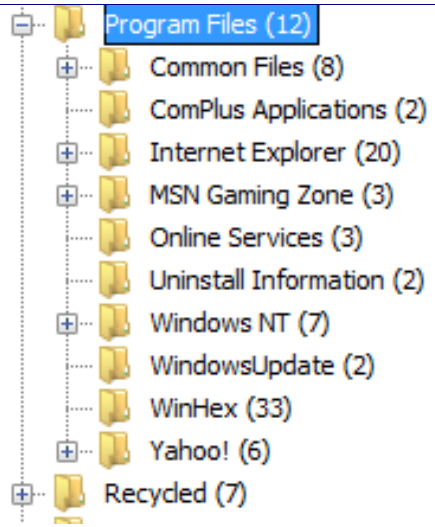
Run relevant keyword searches	YES	09/11/2014	17:08	**Search for keywords** Use this facility to search raw text for specific keywords. The keywords and their settings are specified below. **Current processing options** password pass pa55wrd pa55word pa55w0rd pa55 crime drug police agent airport Grass weed Keyword searches were run on EnCase and Autopsy numerous times throughout the project as more evidence items were discovered. This made finding new possible items easier, such as images of 'turf', which contained a hidden file. 	

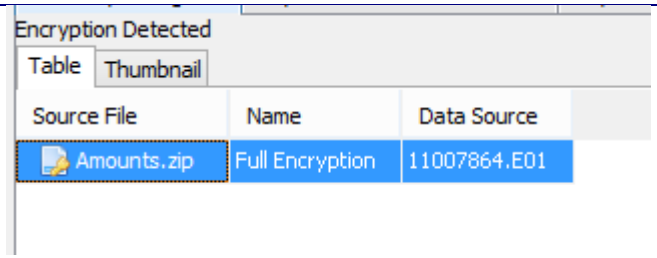
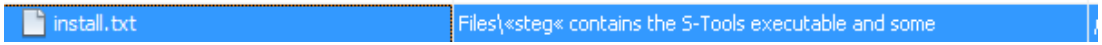
Emails, local & web-based.	YES	09/11/2014	17:43	 No email history was discovered using EnCase, FTK or Autopsy.	

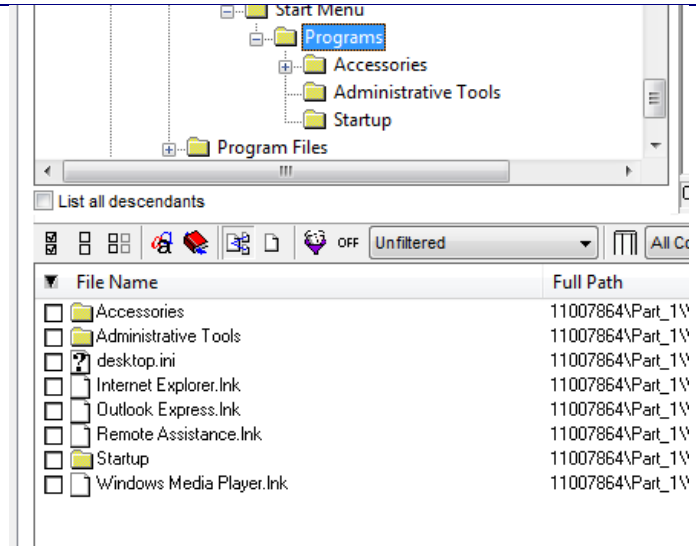
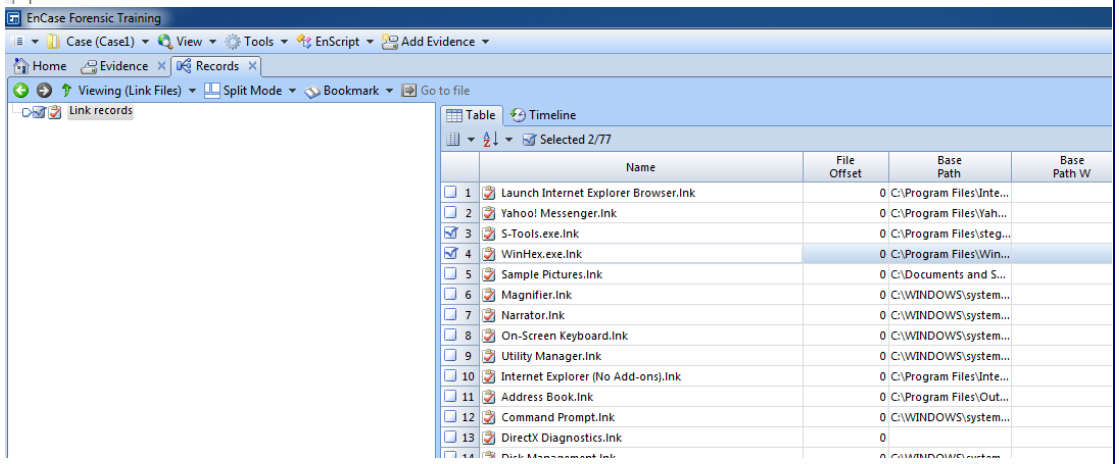
Action	Done	Date	Time	Notes	Initial

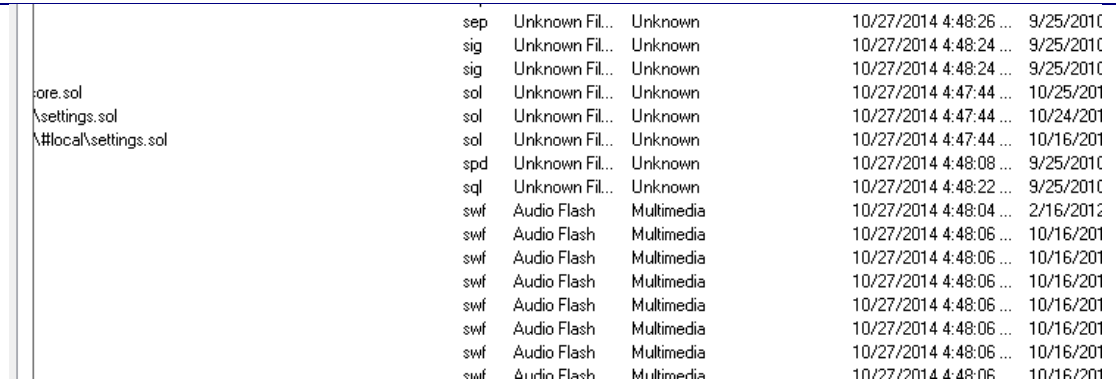
IM clients	YES	09/11/2014	17:53	
				 
				`<?xml version="1.0" encoding="UTF-8"?>`
				`<recentcontact signature="360d92e25f7ba69f9fe5f803b3fa8512">`
				`<node lastcommtime="1414176763" networkid="0" userid="hollywoodtomcat"></node>`
				`<node lastcommtime="1414154333" networkid="0" userid="apprenticeturf"></node>`
				`</recentcontact>`
				
				Yahoo Messenger was found and an account named lordturf was discovered. Also found that he has contacted 'hollywoodtomcat' and 'apprenticeturf' but the chat logs had been deleted.
				 
				
				However, running a keyword search on the names did reveal an evidence item.	

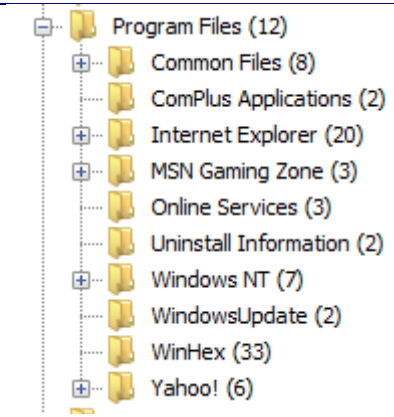
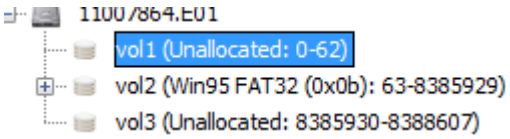
Export doc / office & exe files; look at Meta data if required	YES	09/11/2014	18:08	  I ran a conditional search on EnCase to find a list of Microsoft Office files. I also used Autopsy which catergories files by type, making it easy to view them together. This helped me to find an evidence item, as I was expecting to find at least one useful office document.	

Clean-up utilities. Check log files	YES	09/11/2014	18:11	 No clean tools were found, although it appeared that WinHex was used to hide files by changing a file header to FFF7. There were also a few files found in the recycle bin and thousands of files deleted that were recovered.	

Encryption, Steg, use FTK	YES	09/11/2014	18:21	 Using Autopsy an encrypted file Amounts was found. Further keyword searches found the password to unlock it.  Keyword searches also discovered that Steganography had been used and that S-Tools and OpenPuff had been installed, confirming steganography had been used on the hard drive.	

Link files	YES	09/11/2014	18:41	  Using EnCase a full list of Link files was found using the Process Options. I also looked for the specific files found in the Program Files folder. S-Tools, WinHex and Yahoo messenger were the programs of interest that were found.	

Print artefacts	YES	09/11/2014	19:14	 No SPL, SHD or useful TMP files.	

CD/DVD burning apps; check log files				 No CD/DVD burning apps found.  However, Autopsy and internet history did discover a D:, E: F: and G: drive, but their contents could not be found. This indicates at least one USB drive and possibly a wiped regular drive.	

Action	Done	Date	Time	Notes	Initial
Additional Notes					