

## 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.	<b>Name:</b> TheCase.txt <b>Is Deleted:</b> No <b>File Created:</b> 27/10/14 16:48:36 <b>Last Written:</b> 27/10/14 16:02:52 <b>Last Accessed:</b> 27/10/14 00:00:00 <b>Logical Size:</b> 386 <b>Physical Sector:</b> 1,582,687 <b>Full path:</b> 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.	<b>Name:</b> 1 <b>Is Deleted:</b> Yes <b>File Created:</b> 27/10/14 15:35:00 <b>Last Written:</b> 27/10/14 15:51:12 <b>Last Accessed:</b> 26/10/14 00:00:00 <b>Logical Size:</b> 253 <b>Physical Sector:</b> 1,582,703 <b>Full path:</b> 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.	<b>Name:</b> Amounts.ods <b>Is Deleted:</b> No <b>File Created:</b> - <b>Last Written:</b> 26/10/14 12:43:00 <b>Last Accessed:</b> - <b>Logical Size:</b> 11,639 <b>Physical Sector:</b> 600,103 <b>Full path:</b> 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.	<b>Name:</b> important.jpeg <b>Is Deleted:</b> No <b>File Created:</b> 27/10/14 15:48:01 <b>Last Written:</b> 27/10/14 02:28:46 <b>Last Accessed:</b> 26/10/14 00:00:00 <b>Logical Size:</b> 1,692 <b>Physical Sector:</b> 665,535 <b>Full path:</b> 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: <a href="https://uk-mg42.mail.yahoo.com/neo/launch?.rand=26gc824uahof&amp;action=otepad#4932827028">https://uk-mg42.mail.yahoo.com/neo/launch?.rand=26gc824uahof&amp;action=otepad#4932827028</a> 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.	<b>Name:</b> Movements.xls <b>Is Deleted:</b> No <b>File Created:</b> 27/10/14 15:47:59 <b>Last Written:</b> 27/10/14 13:36:40 <b>Last Accessed:</b> 26/10/14 00:00:00 <b>Logical Size:</b> 11,741 <b>Physical Sector:</b> 601,255 <b>Full path:</b> 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.	<b>Name:</b> Memo1.odt <b>Is Deleted:</b> No <b>File Created:</b> 27/10/14 15:47:59 <b>Last Written:</b> 27/10/14 15:00:04 <b>Last Accessed:</b> 26/10/14 00:00:00 <b>Logical Size:</b> 11,741 <b>Physical Sector:</b> 600,063 <b>Full path:</b> 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.	<b>Name:</b> turf5.bmp <b>Is Deleted:</b> No <b>File Created:</b> 27/10/14 15:48:01 <b>Last Written:</b> 24/10/14 20:09:02 <b>Last Accessed:</b> 26/10/14 00:00:00 <b>Logical Size:</b> 15,116,598 <b>Physical Sector:</b> <b>Full path:</b> 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.	<b>Name:</b> suitcase.bmp <b>Is Deleted:</b> No <b>File Created:</b> 27/10/14 16:48:01 <b>Last Written:</b> 24/10/14 16:19:38 <b>Last Accessed:</b> 26/10/14 00:00:00 <b>Logical Size:</b> 15,116,598 <b>Physical Sector:</b> 670,104 <b>Full path:</b> 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.

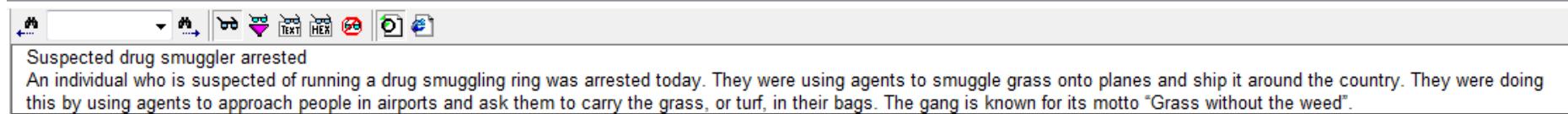
The type, stock and price that they were selling the drugs were located, along with the names of agents who have previously transported the drugs, the date, amounts, destinations and amount of profit the gang made from each. The structure of the gang was discovered, along with full names, addresses and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



Suspected drug smuggler arrested  
An individual who is suspected of running a drug smuggling ring was arrested today. They were using agents to smuggle grass onto planes and ship it around the country. They were doing this by using agents to approach people in airports and ask them to carry the grass, or turf, in their bags. The gang is known for its motto "Grass without the weed".

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 : thisisprivate
Yahoo username : lordturf
Yahoo password : Grass123
Locations steg password : stayOut! 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](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

The screenshot shows a list of chat histories on the left and a search interface on the right.

**Chat History:**

- hollywoodtomcat: 24 Oct 13:26 apprenticeTurf: hey
- hollywoodtomcat: 24 Oct 13:26 apprenticeTurf: is the meeting for the location hosts at yours?
- hollywoodtomcat: 24 Oct 13:09 hi babes
- hollywoodtomcat: 24 Oct 13:17 😞
- lordturf: 24 Oct 13:26 im bust
- lordturf: 24 Oct 13:17 busy
- hollywoodtomcat: 24 Oct 13:17 ffs
- lordturf: 24 Oct 13:17 trying to hide information
- hollywoodtomcat: 24 Oct 13:17 i thought you were solid
- lordturf: 24 Oct 13:17 from any nosy investigators
- hollywoodtomcat: 24 Oct 13:17 gg
- hollywoodtomcat: 24 Oct 13:17 such wo
- hollywoodtomcat: 24 Oct 13:17 w

**Search Results:**

Conversation History

9 results

Refined by Instant messages ×

Add More Filters

Sender	Date
hollywoodtomcat	2014
Joe Blogs	
joe.blogsss	
lordturf	

Sender: Date

hollywoodtomcat hollywoodtomcat... 2014  
Joe Blogs joe.blogsss@yahoo.co.uk  
Turf Apprentice apprenticeTurf@yah...

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 who were planning on cutting communication with them. This could prove relevant to the case if more information is found.

## Item 06

<u>Date</u>	<u>Amount</u>	<u>Type</u>	<u>From</u>	<u>To</u>	<u>Profit</u>	<u>Agent</u>
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



The screenshot shows a software window with a menu bar (File, Window, Help) and a sidebar titled 'Revealed files:' containing a single item: 'Listoflocations.xls' (Size: 14,336). The main area displays a table with columns: Location number, Location name, Host, Supervisor, Address, and Contact no.

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 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](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

PK LJ ¶■•YE...19\$..mimetypeapplication/vnd.oasis.opendocument.spreadsheetPK LJ ¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
1 PK LJ ¶■•YE...19\$..mimetypeapplication/vnd.oasis.opendocument.spreadsheetPK LJ ¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
2 +  
3  
4 IHDR¾ ¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
5 It=D1x ¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
6 aeÁt+¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
7 ±iCEÜl"n‡yÁ"±t(xTÉ EÉ)¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
8 /yñys¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
9 ¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
10 ¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
11 ¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
12 cAföüp~¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
13 Øà Çn}¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
14 ↪t(BüGÜz←-G Yéo@-Mfcj-çM-←@-Of |aæte|¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
15 L^N2&a)&←#I-E-%œùT9AíkH Ü, Qbc|fA@Gvç|Æø#œù, áB?Y-Y'èÍyudüñ"Z"fc+ò1,j, c|ø-th-u|p,,døxùÖÙ%éö1#-m-A~VI]åJ Á-+aç'èMÅäfaé%o|p)e|uäö?<Ö]§|ceZ4Ø)yæ  
16 8Á)qgäqu m" Ö|EzD|LéUë8rñ+3+2"m, l"!!"yÄz@xÜùåsÜ4s<xQ"u"ùC!%o, t"!,"C|j, j"7EEZvc¶■•YE|Configurations2/fniu"aiOG"RTy@%>-é/ä|Téx3+2"m{}v12ä"Z-i, iøeiuAz"6"o%L"ç, t, äU...åñ  
17 øÈÜ;"nñjA N,kjYñnf GØ, èžj@THÜ"  
18 su\_¶■•YE|Configurations2/floater/PK LJ ¶■•YE|Configurations2/accelerator/current.xml  
19 Z→wibl@S-åñ"ñYÓŒ#(uul(ÀEýE\_1/Y@1:D?i-#u"iiA@%o|gœa|åG%é', JCE| |žpA?G, öežj+ø'ø"m)|#|1:D?#u'G, ÚÙÜYd,-iUÁ| |'wµZÖC4A\* →@&G-ÜSÅ3oÀLr(\*uér"1Ü%  
20 5AEj-ZY"-ÅKü6"çcöOB%, T"styþBç, öä

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.

The screenshot shows a file browser window on the left and two overlapping 'Go To Sector' dialog boxes on the right.

**File Browser Data:**

important.jpg	jpg	1.7 KB	10/27/2014	16:48:01	10/27/2014	03:28:46	A	665472				
Sample Pictures.lnk	Ink	0.7 KB	10/27/2014	16:48:01	10/12/2014	13:13:02	A	663304				
spacepak_suitcase1_1.bmp	bmp	732 KB	10/27/2014	16:48:01	10/25/2014	19:01:48	A	663312				
suitcase.bmp	bmp	732 KB	10/27/2014	16:48:01	10/27/2014	16:19:38	A	670104				
Turfylicious.jpg	jpg	341 KB	10/27/2014	16:48:01				664784				

**Go To Sector Dialogs:**

The first dialog box (foreground) has the title 'Go To Sector' and contains the following fields:

- Logical: Sector: 670104
- = Cluster: B1717

The second dialog box (background) has the title 'Go To Sector' and contains the following fields:

- Logical: Sector: 670104
- = Cluster: B1717

Both dialogs have OK and Cancel buttons at the bottom.

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.

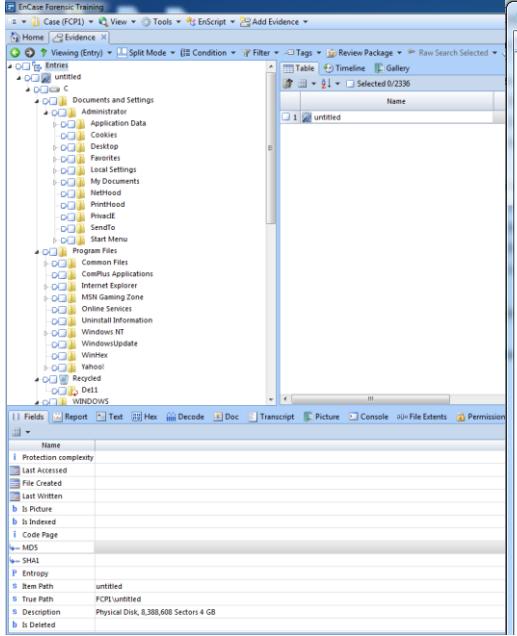
It appears that LordTurf made a mistake, hiding the wrong file within the image. In the chat log it stated that he wanted to hide a list of passwords and it's clear that this is the image that it was intended to be hidden within.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	/	?
00054410	05	3F	01	00	06	3F	01	00	07	3F	01	00	08	3F	01	00	?	?
00054420	09	3F	01	00	0A	3F	01	00	0B	3F	01	00	0C	3F	01	00	?	?
00054430	0D	3F	01	00	0E	3F	01	00	0F	3F	01	00	10	3F	01	00	?	?
00054440	11	3F	01	00	12	3F	01	00	13	3F	01	00	14	3F	01	00	?	?
00054450	15	3F	01	00	16	3F	01	00	17	3F	01	00	18	3F	01	00	?	?
00054460	FF	FF	FF	OF	1A	3F	01	00	1B	3F	01	00	1C	3F	01	00	ÿÿ	ÿÿ
00054470	1D	3F	01	00	1E	3F	01	00	1F	3F	01	00	20	3F	01	00	?	?
00054480	21	3F	01	00	22	3F	01	00	23	3F	01	00	24	3F	01	00	!?	"?
00054490	25	3F	01	00	26	3F	01	00	27	3F	01	00	28	3F	01	00	%?	&?
000544A0	29	3F	01	00	2A	3F	01	00	2B	3F	01	00	2C	3F	01	00	)?	*?
000544B0	2D	3F	01	00	2E	3F	01	00	2F	3F	01	00	30	3F	01	00	-?	.
000544C0	31	3F	01	00	32	3F	01	00	33	3F	01	00	34	3F	01	00	1?	2?
000544D0	FF	FF	FF	OF	36	3F	01	00	37	3F	01	00	38	3F	01	00	ÿÿ	6?
000544E0	39	3F	01	00	3A	3F	01	00	3B	3F	01	00	3C	3F	01	00	9?	:?
000544F0	3D	3F	01	00	3E	3F	01	00	3F	3F	01	00	40	3F	01	00	=?	>?
00054500	41	3F	01	00	42	3F	01	00	43	3F	01	00	44	3F	01	00	??	??

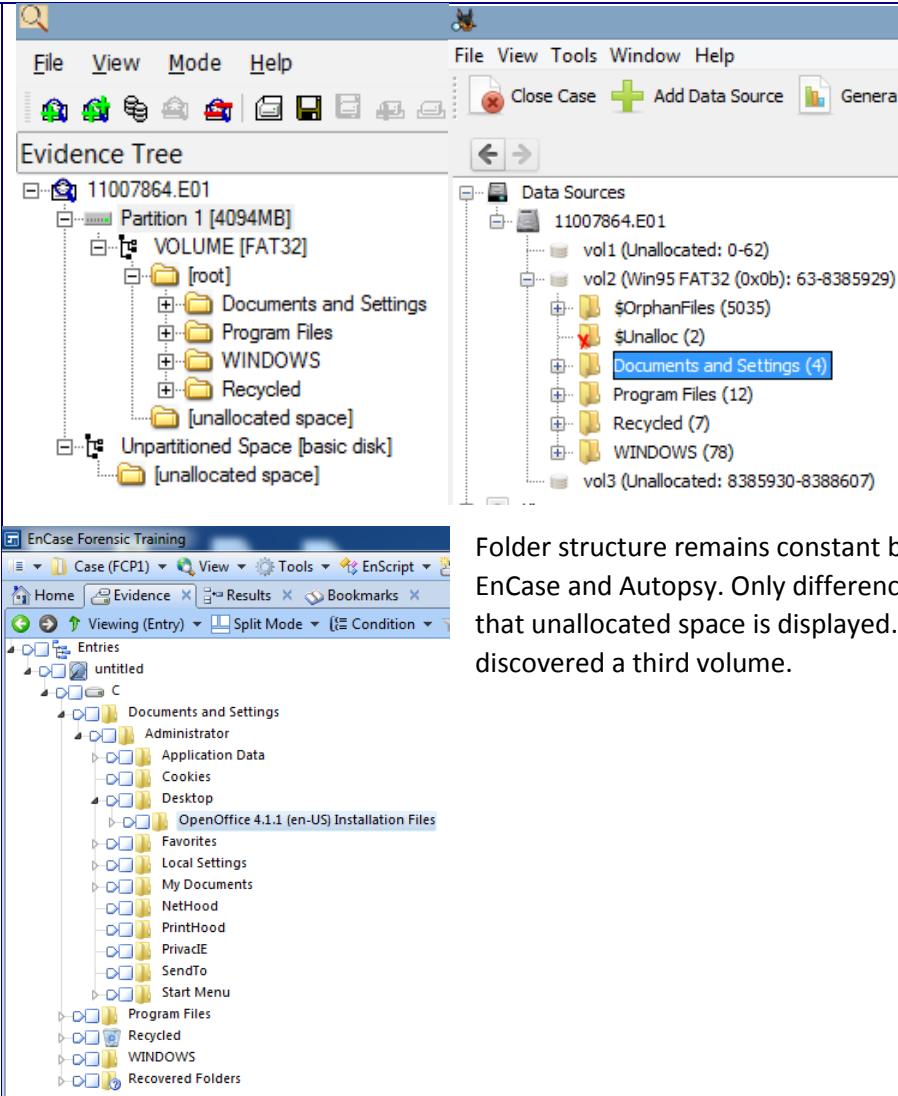
Unfortunately, this now ends the trail, as no other leads can be located using the items recovered and no other items can be located.

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	<ul style="list-style-type: none"> <li>• FTK 1.8.1</li> <li>• EnCase 7</li> <li>• Autopsy 3.1.1</li> <li>• WinHex</li> <li>• S-Tools</li> <li>• OpenPuff</li> <li>• OSFMount</li> <li>• SamInside</li> <li>• RegRipper</li> </ul>

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

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

Dual verification of key evidence items.	YES	08/11/2014	18:48	 <p>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.</p>	
--	-----	------------	-------	--	--

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

The screenshot displays two windows side-by-side, both showing file comparison results between two volumes.

**Top Window (EnCase Forensic 7):**

- Left pane:** Shows a tree view of the 'My Case' volume structure, including 'Documents and Settings', 'Program Files', 'Recycled', 'Windows', and 'VOLUME'. A file named 'TheCase.txt' is selected.
- Right pane:** A table view comparing files from 'My Case' and 'VOLUME'. The table includes columns for Name, Tag, File Date, Logical Size, Category, Signature Analysis, File Type, Protected, Protection Complexity, Last Accessed, and Last Modified.
- Bottom pane:** A detailed view of the selected file 'TheCase.txt', showing its properties such as Name, File Ext, Logical Size, Category, File Type, Protection Complexity, and a large list of file metadata.

**Bottom Window (AccessData FTK 18.0 DEMO VERSION):**

- Left pane:** Shows a tree view of the 'Case 11007864' volume structure, including 'Part\_1', 'VOLUME-FAT32', and various sub-folders like 'Documents and Settings', 'Program Files', 'Recycled', 'Windows', 'System Volume Information', and 'Temp'.
- Right pane:** A text editor window containing the contents of 'TheCase.txt'. The text discusses a drug smuggler arrested for smuggling grass onto planes.
- Bottom pane:** A table view comparing files from 'Case 11007864' and 'VOLUME-FAT32'. The table includes columns for File Name, Full Path, Cr Date, Mod Date, Acc Date, L-Size, P-Size, MD5 Hash, and SHA1 Hash.

**Taskbar:** Both windows show the taskbar with icons for Internet Explorer, Google Chrome, File Explorer, and other system icons.

**Exif Editor - Viewing File**

File Home Evidence View Tools Exchange Add Evidence

File Edit View Tools Help

Overview

Documents and Settings

- Administrator
- Application Data
- Cookies
- Desktop
- Favorites
- Local Settings
- My Computer
- Network
- Temporary Internet Files
- User Profile

Selected 1000/1003

Name	Tag	Mod Date	Logical Size	Category	Signature Analysis	File Type	Protected	Previous completely	Last	
111.zip	ZIP Unknown	Unknown	0B Unknown	Unknown		ZIP Archive			10/27/14 12:00:00 AM	10/27/14 12:00:00 AM
111_JH	ZIP Unknown	10/27/14 4:51:52 PM	0B Unknown	Unknown		ZIP Archive			10/27/14 12:00:00 AM	10/27/14 12:00:00 AM
75401968	ZIP Unknown	10/27/14 4:51:52 PM	276 0	Unknown		ZIP Archive			10/27/14 12:00:00 AM	10/27/14 12:00:00 AM
75401968	ZIP Unknown	10/27/14 4:51:52 PM	276 0	Unknown		ZIP Archive			10/27/14 12:00:00 AM	10/27/14 12:00:00 AM

Fields Report Text Hex Decode Doc Transcript Picture Console File Extents Permissions Hash Sets Attributes

Value

Protection complexity

File Access 10/27/14 12:00:00 AM

File Created 10/27/14 04:50:00 PM

Last Written 10/27/14 04:51:12 PM

Is Readable

Is Shared

Code Page 29464 (Windows-1252)

File System C:\Windows\system32\cmd.exe

File Type ZIP Archive

File Version 10.0.9600.16384

Filepath C:\Windows\system32\cmd.exe

Description File.Demand\_Access

Is Deleted

Is Encrypted

File Acquired 10/27/14 11:04:58 AM

Filesize 256

Filetype ZIP

Starting Offset 0C-C3570A

File Extents 1

Filegroup

Physical Location 312,343,036

Physical Sector 1,532,703

Physical Volume 1

File Identifier 2524

GUID 4420042b9fa4205ab4d1f82f747ed

Volume Name 1

VFS Name

Original Path

Symbolic Link

Case Untitled (C:\Documents and Settings\Administrator\My Documents)\13

AccessData FTV 1.8.0 (DRAFT VERSION) - C:\Windows\Temp\Case 01\111007864

File Edit View Tools Help

Overview

Documents and Settings

- Administrator
- Application Data
- Cookies
- Desktop
- Favorites
- Local Settings
- My Computer
- Network
- Temporary Internet Files
- User Profile

excel sheet in zip folder : thisisaprototype

Yahoo username : lonturf

Yahoo password : 12345678901234567890

Locations step password : stayout! type = IDEA image of a garden

Transactions step transactionz type = IDEA changed first FAT cluster from 36 3F to FF F7

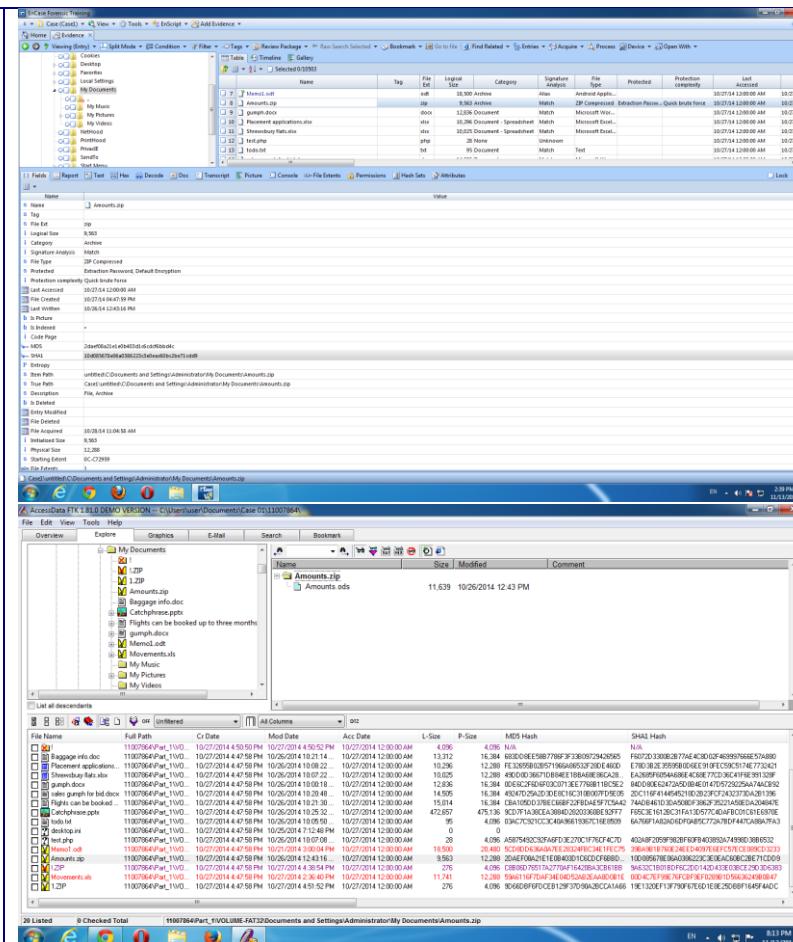
File Name Full Path Cr Date Mod Date Acc Date L-Size P-Size MD5 Hash SHA1 Hash

111.zip	11007864\Part_1\100	10/27/2014 4:51:50 PM	10/27/2014 4:51:52 PM	0	0	294642618AC19A41904A547A7E705	7C9B977ED514D1D7E1C167924B234AC27097
111_JH	11007864\Part_1\100	10/27/2014 4:51:50 PM	10/27/2014 4:51:52 PM	0	0	294642618AC19A41904A547A7E705	7C9B977ED514D1D7E1C167924B234AC27097
75401968	11007864\Part_1\100	10/27/2014 4:51:50 PM	10/27/2014 4:51:52 PM	276	0	294642618AC19A41904A547A7E705	7C9B977ED514D1D7E1C167924B234AC27097
75401968	11007864\Part_1\100	10/27/2014 4:51:50 PM	10/27/2014 4:51:52 PM	276	0	294642618AC19A41904A547A7E705	7C9B977ED514D1D7E1C167924B234AC27097

4 Listed 0 Checked Total 11007864\Part\_1\VOLUME-FAT32\Documents and Settings\Administrator\My Documents\13

EN 8:07 PM 11/13/2014

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



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

The screenshot displays three windows illustrating the analysis of a file named "important.jpg".

**Top Window:** A forensic tool interface showing the file's details. The file is a 1,682 byte Windows Picture and Image File (JPG). It was last modified on 10/27/14 at 12:00:00 AM and has a SHA1 hash of E0746C8F92004960B7F25E9779E5039A252C.

Name	Tag	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected	Protection Complexity	Last Accessed
important.jpg	JPG	JPG	1,682	Windows Picture	Match	Microsoft Photo			10/27/14 12:00:00 AM
Sensor Pictures.lnk	LNK	LNK	793,914	Picture	Match	Microsoft Photo L			10/27/14 12:00:00 AM
TurboNoobs.jpg	JPG	JPG	245,360	Picture	Match	JPG Image Sta...			10/27/14 12:00:00 AM
important.jpg	JPG	JPG	1,682	Windows	N/A	Registry Data			10/27/14 12:00:00 AM

**Middle Window:** A file browser showing the file's location in the "My Pictures" folder. The file is a 1,682 byte file with a SHA1 hash of E0746C8F92004960B7F25E9779E5039A252C.

**Bottom Window:** A file browser showing the file's location in the "My Pictures" folder. The file is a 1,682 byte file with a SHA1 hash of E0746C8F92004960B7F25E9779E5039A252C.

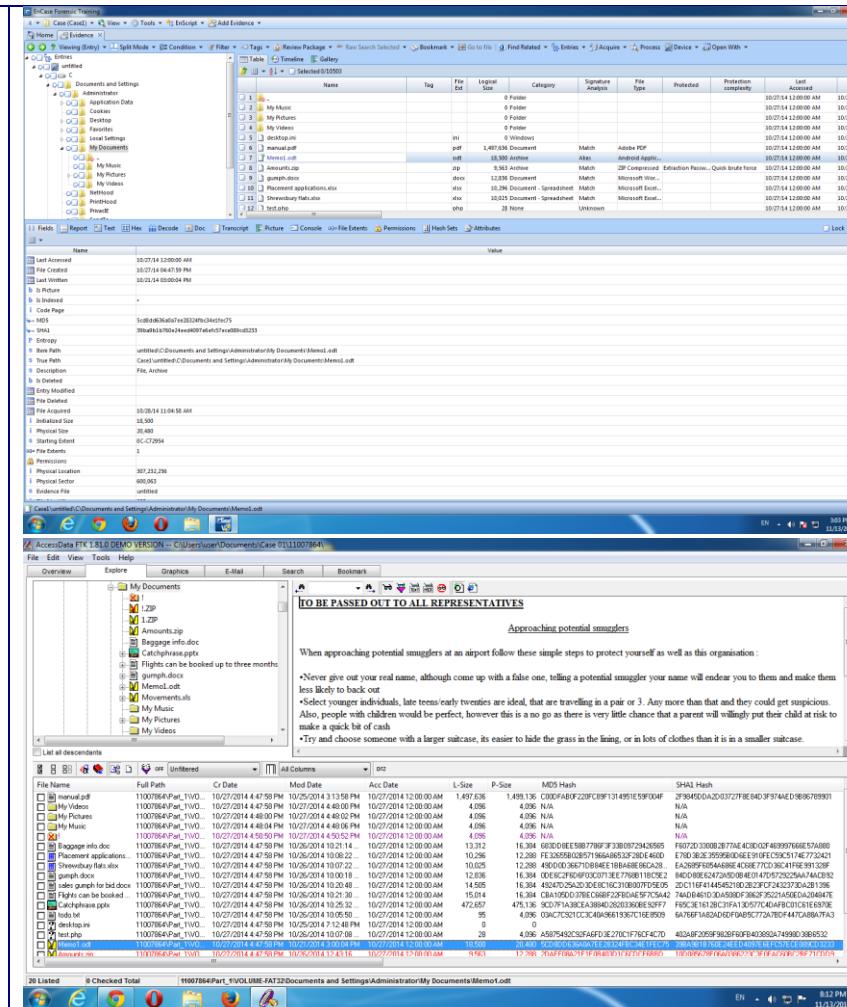
**Item 4: Location, Size, MD5 & SHA1 Hash all match.**

The screenshot displays three windows side-by-side, illustrating a forensic analysis process:

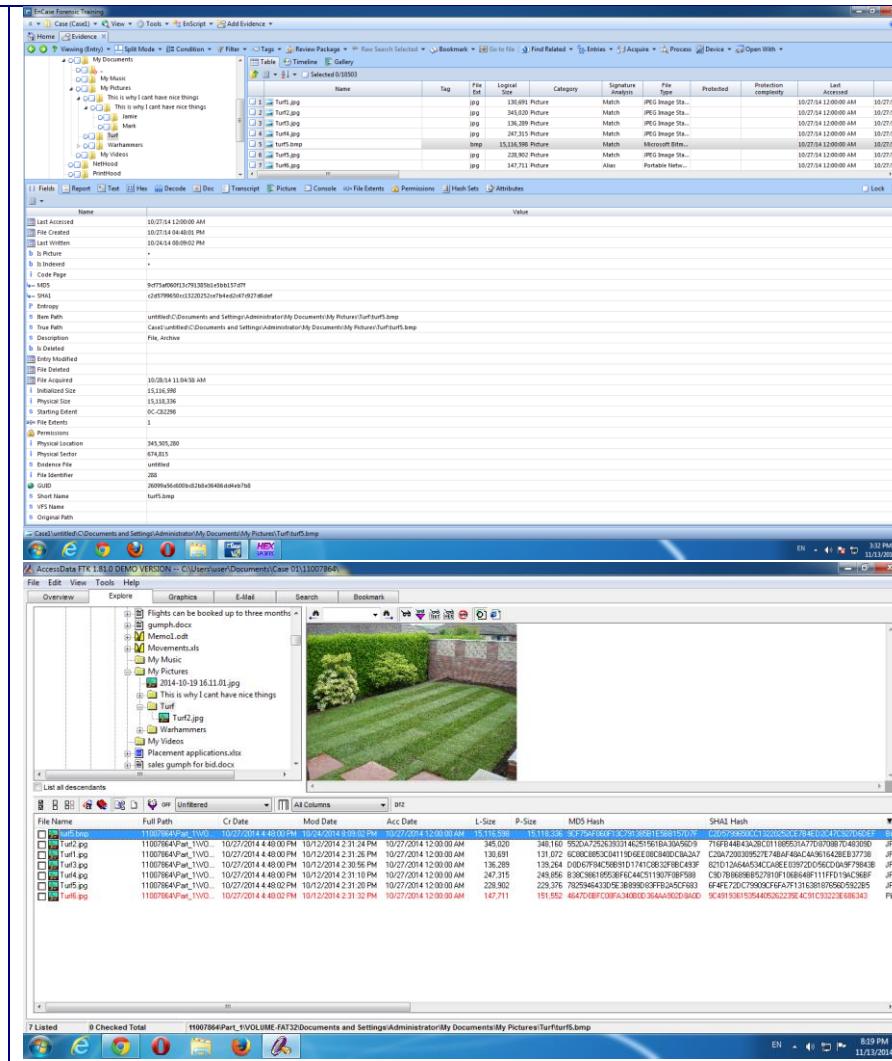
- Top Window:** A file browser titled "Case Evidence - Forensic". It shows a tree view of evidence items under "Case (CaseID: 1)". One item is selected: "My Documents" (CaseID: 1). This item is expanded to show sub-folders like "Administrator", "Application Data", "Cookies", "Desktop", "Favorites", "Local Settings", and "My Documents". A detailed table view on the right lists files with columns: Name, Tag, File Date, Logical Size, Category, Signature Analysis, File Type, Protected, Protection Complexity, and Last Accessed. Key entries include:
 

Name	Tag	File Date	Logical Size	Category	Signature Analysis	File Type	Protected	Protection Complexity	Last Accessed
todo.txt		10/27/2014 4:50:59 PM	15 Document	Match	Microsoft Word...	docx		10/27/2014 12:00:00 AM	10/27/2014 12:00:00 AM
sales.gragh		10/27/2014 4:50:59 PM	13,245 Document	Match	Microsoft Word...	docx		10/27/2014 12:00:00 AM	10/27/2014 12:00:00 AM
Baggage.info.doc		10/27/2014 4:47:59 PM	472,900 Document	Match	Microsoft Word...	docx		10/27/2014 12:00:00 AM	10/27/2014 12:00:00 AM
Movements.xls		10/27/2014 4:47:59 PM	13,054 Document	Match	Microsoft Word...	docx		10/27/2014 12:00:00 AM	10/27/2014 12:00:00 AM
ZIP		10/27/2014 4:47:59 PM	276 Archive	Match	ZIP Compressed	zip		10/27/2014 12:00:00 AM	10/27/2014 12:00:00 AM
1.zip		10/27/2014 4:47:59 PM	15,743 Archive	Match	Android applic...	apk		10/27/2014 12:00:00 AM	10/27/2014 12:00:00 AM
- Middle Window:** A detailed file information window for "Movements.xls". It shows various metadata fields such as Name, Value, File Name, File Created, Last Written, Is Archived, Is Indexed, Code Page, Last Read, SHA1, Entropy, File Path, True Path, Description, Is Deleted, Is Encrypted, File Modified, File Acquired, Physical Size, Starting Offset, File Allocation, Permissions, Physical Location, File Protection, Evidence File, and Case ID. The file was last modified on 10/27/2014 at 4:50:59 PM.
- Bottom Window:** A file viewer titled "AccessData FTV 1.8.0.0 (Build Version: 1.8.0.0) - C:\Users\user\Documents\Case 0131107304". It displays the contents of "Movements.xls" in a spreadsheet-like interface. The table includes columns: Date, Amount, Type, From, To, Profit, Agent, and Status. The "Status" column contains entries like "Flight can be booked up to three months in advance", "Sales can be booked up to one month in advance", and "Sales can be booked up to three months in advance". The bottom status bar indicates the file was last modified on 14/12/13.

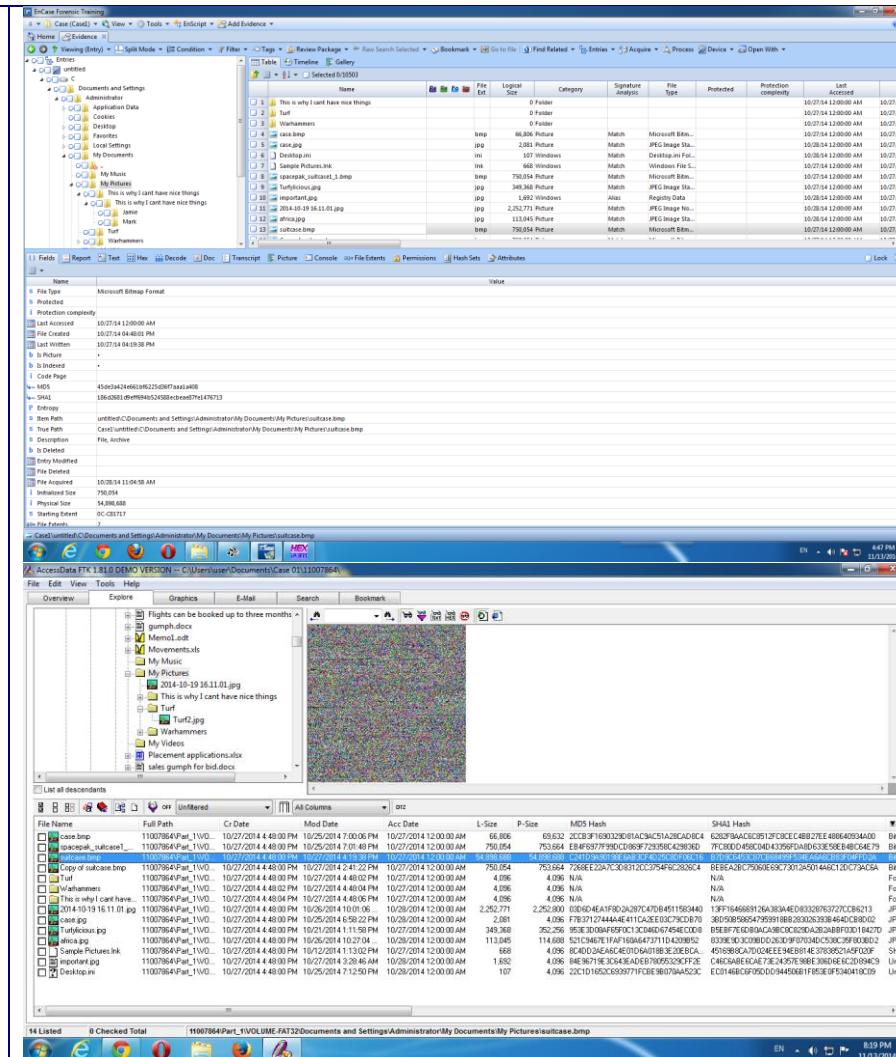
**Item 6: Location, Size, MD5 & SHA1 Hash all match.**



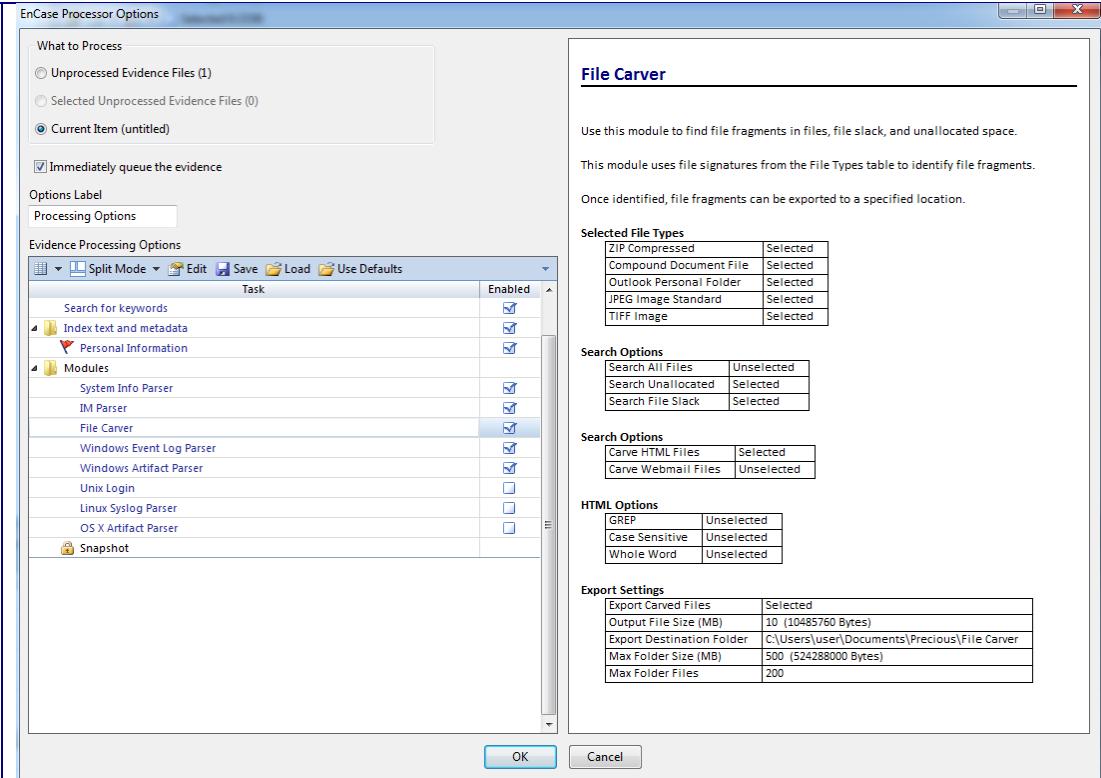
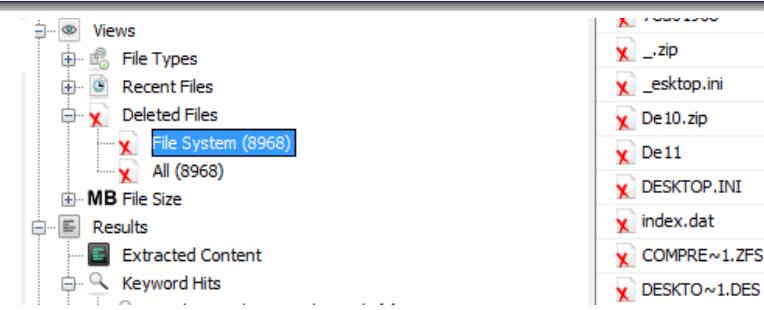
**Item 7:** Location, Size, MD5 & SHA1 Hash all match.



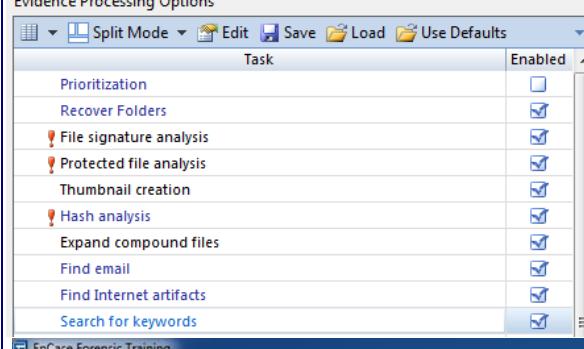
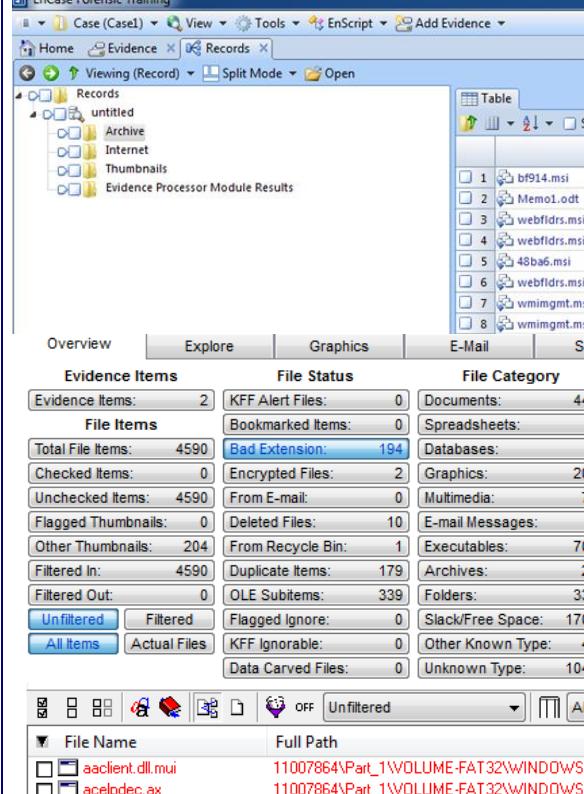
**Item 8:** Location, Size, MD5 & SHA1 Hash all match.

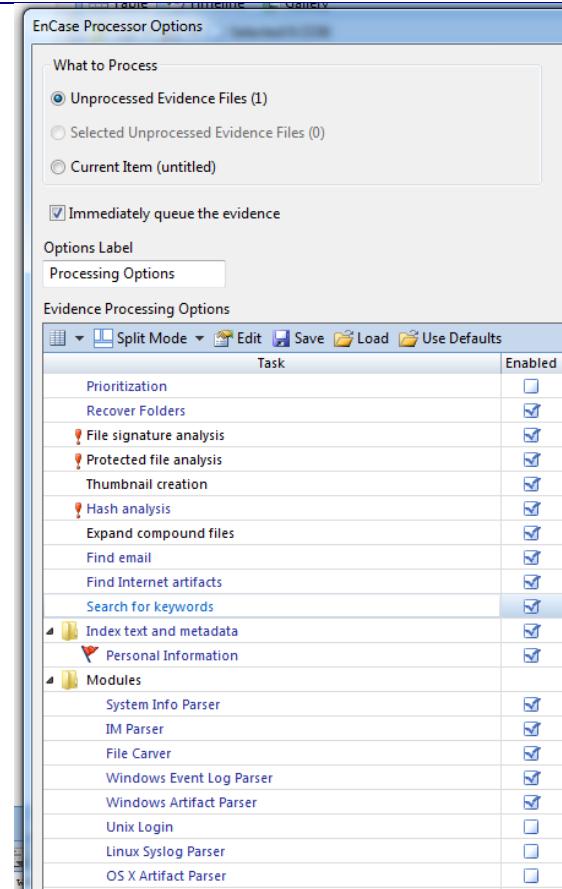


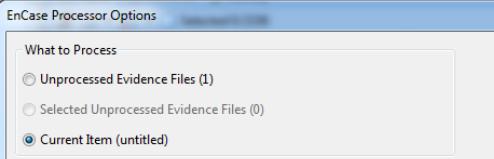
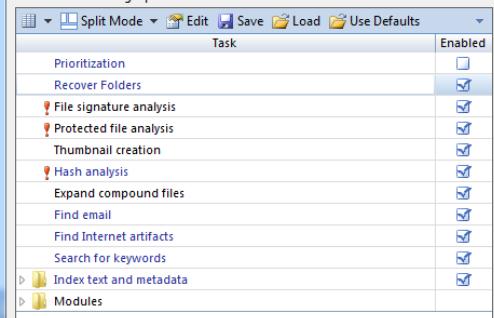
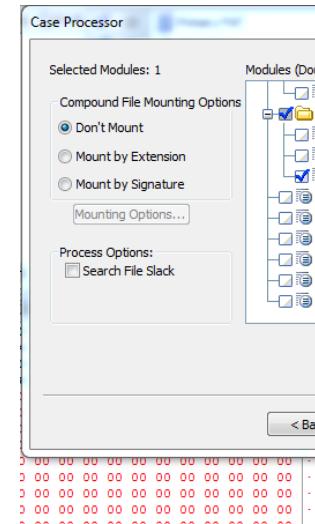
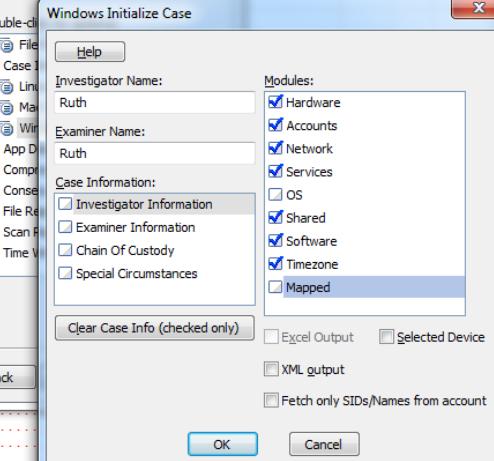
**Item 9:** Location, Size, MD5 & SHA1 Hash all match.

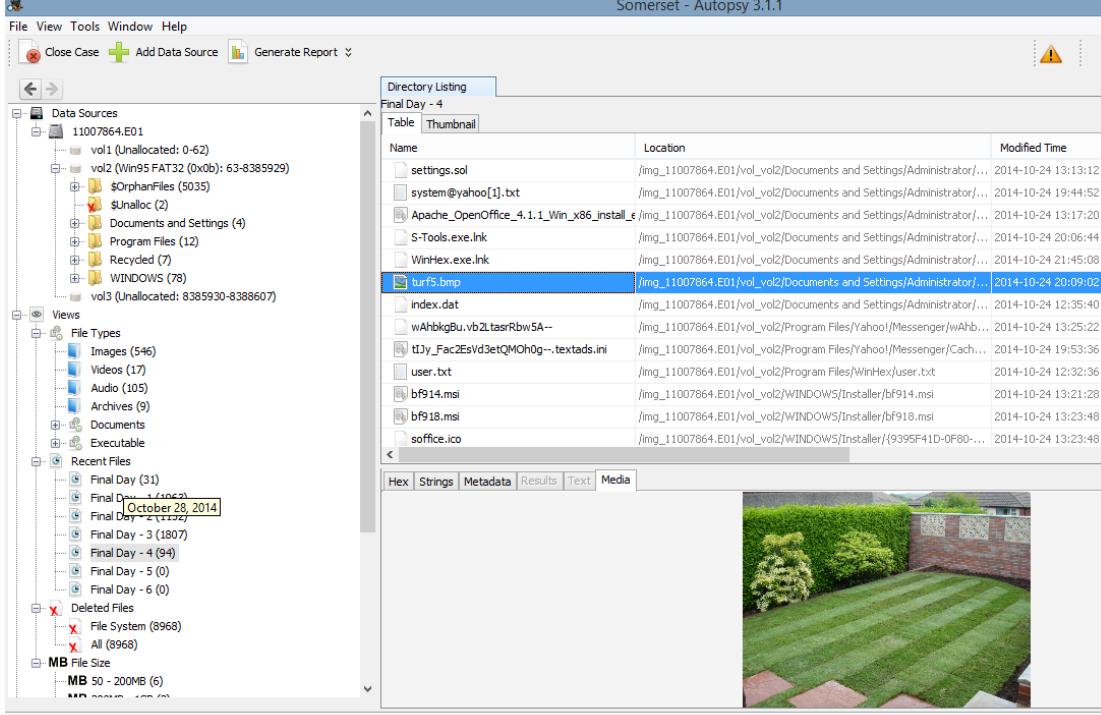
Recover lost folders (FAT16 & 32).	YES	03/11/2014	11:41	<p><b>Recovered Folders</b></p> <p>Recovered lost files using the 'Recover Folder' option in EnCase processor. Also used Autopsy to discover a total of 8968 deleted files.</p>  

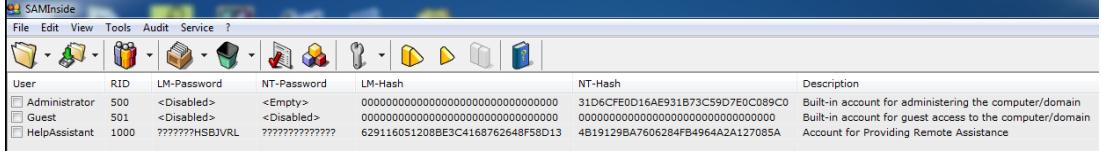
				<p><b>Evidence Processing Options</b></p> <table border="1"> <thead> <tr> <th>Task</th><th>Enabled</th></tr> </thead> <tbody> <tr> <td>Prioritization</td><td><input type="checkbox"/></td></tr> <tr> <td>Recover Folders</td><td><input checked="" type="checkbox"/></td></tr> <tr> <td>File signature analysis</td><td><input checked="" type="checkbox"/></td></tr> <tr> <td>Protected file analysis</td><td><input checked="" type="checkbox"/></td></tr> <tr> <td>Thumbnail creation</td><td><input checked="" type="checkbox"/></td></tr> <tr> <td>Hash analysis</td><td><input checked="" type="checkbox"/></td></tr> <tr> <td>Expand compound files</td><td><input checked="" type="checkbox"/></td></tr> <tr> <td>Find email</td><td><input checked="" type="checkbox"/></td></tr> <tr> <td>Find Internet artifacts</td><td><input checked="" type="checkbox"/></td></tr> <tr> <td>Search for keywords</td><td><input checked="" type="checkbox"/></td></tr> </tbody> </table> <p>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.</p>	Task	Enabled	Prioritization	<input type="checkbox"/>	Recover Folders	<input checked="" type="checkbox"/>	File signature analysis	<input checked="" type="checkbox"/>	Protected file analysis	<input checked="" type="checkbox"/>	Thumbnail creation	<input checked="" type="checkbox"/>	Hash analysis	<input checked="" type="checkbox"/>	Expand compound files	<input checked="" type="checkbox"/>	Find email	<input checked="" type="checkbox"/>	Find Internet artifacts	<input checked="" type="checkbox"/>	Search for keywords	<input checked="" type="checkbox"/>	
Task	Enabled																										
Prioritization	<input type="checkbox"/>																										
Recover Folders	<input checked="" type="checkbox"/>																										
File signature analysis	<input checked="" type="checkbox"/>																										
Protected file analysis	<input checked="" type="checkbox"/>																										
Thumbnail creation	<input checked="" type="checkbox"/>																										
Hash analysis	<input checked="" type="checkbox"/>																										
Expand compound files	<input checked="" type="checkbox"/>																										
Find email	<input checked="" type="checkbox"/>																										
Find Internet artifacts	<input checked="" type="checkbox"/>																										
Search for keywords	<input checked="" type="checkbox"/>																										
Mount archives; zip, thumbs.db, etc	YES	03/11/2014	11:41																								

				<p><b>Evidence Processing Options</b></p>  <p>The screenshot shows the 'Evidence Processing Options' dialog box. Under the 'Task' column, several items are checked, including 'File signature analysis', 'Protected file analysis', 'Thumbnail creation', 'Hash analysis', 'Find email', 'Find Internet artifacts', and 'Search for keywords'. The 'Enabled' column has a dropdown arrow icon.</p> <p><b>EnCase Forensic Training</b></p>  <p>The screenshot shows the EnCase interface with the 'Records' tab selected. On the left, there's a tree view of evidence items under 'untitled'. On the right, a table provides a detailed breakdown of evidence items:</p> <table border="1"> <thead> <tr> <th colspan="2">Evidence Items</th> <th colspan="2">File Status</th> <th colspan="2">File Category</th> </tr> </thead> <tbody> <tr> <td>Evidence Items:</td> <td>2</td> <td>KFF Alert Files:</td> <td>0</td> <td>Documents:</td> <td>442</td> </tr> <tr> <td>File Items</td> <td></td> <td>Bookmarked Items:</td> <td>0</td> <td>Spreadsheets:</td> <td>2</td> </tr> <tr> <td>Total File Items:</td> <td>4590</td> <td>Bad Extension:</td> <td>194</td> <td>Databases:</td> <td>2</td> </tr> <tr> <td>Checked Items:</td> <td>0</td> <td>Encrypted Files:</td> <td>2</td> <td>Graphics:</td> <td>204</td> </tr> <tr> <td>Unchecked Items:</td> <td>4590</td> <td>From E-mail:</td> <td>0</td> <td>Multimedia:</td> <td>76</td> </tr> <tr> <td>Flagged Thumbnails:</td> <td>0</td> <td>Deleted Files:</td> <td>10</td> <td>E-mail Messages:</td> <td>0</td> </tr> <tr> <td>Other Thumbnails:</td> <td>204</td> <td>From Recycle Bin:</td> <td>1</td> <td>Executables:</td> <td>701</td> </tr> <tr> <td>Filtered In:</td> <td>4590</td> <td>Duplicate Items:</td> <td>179</td> <td>Archives:</td> <td>27</td> </tr> <tr> <td>Filtered Out:</td> <td>0</td> <td>OLE Subitems:</td> <td>339</td> <td>Folders:</td> <td>338</td> </tr> <tr> <td>Unfiltered</td> <td></td> <td>Flagged Ignore:</td> <td>0</td> <td>Slack/Free Space:</td> <td>1708</td> </tr> <tr> <td>All Items</td> <td></td> <td>Actual Files:</td> <td>KFF Ignorable:</td> <td>Other Known Type:</td> <td>45</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>Data Carved Files:</td> <td>1045</td> </tr> </tbody> </table> <p>Below the table, a list of files is shown with columns for 'File Name' and 'Full Path'.</p>	Evidence Items		File Status		File Category		Evidence Items:	2	KFF Alert Files:	0	Documents:	442	File Items		Bookmarked Items:	0	Spreadsheets:	2	Total File Items:	4590	Bad Extension:	194	Databases:	2	Checked Items:	0	Encrypted Files:	2	Graphics:	204	Unchecked Items:	4590	From E-mail:	0	Multimedia:	76	Flagged Thumbnails:	0	Deleted Files:	10	E-mail Messages:	0	Other Thumbnails:	204	From Recycle Bin:	1	Executables:	701	Filtered In:	4590	Duplicate Items:	179	Archives:	27	Filtered Out:	0	OLE Subitems:	339	Folders:	338	Unfiltered		Flagged Ignore:	0	Slack/Free Space:	1708	All Items		Actual Files:	KFF Ignorable:	Other Known Type:	45					Data Carved Files:	1045	
Evidence Items		File Status		File Category																																																																															
Evidence Items:	2	KFF Alert Files:	0	Documents:	442																																																																														
File Items		Bookmarked Items:	0	Spreadsheets:	2																																																																														
Total File Items:	4590	Bad Extension:	194	Databases:	2																																																																														
Checked Items:	0	Encrypted Files:	2	Graphics:	204																																																																														
Unchecked Items:	4590	From E-mail:	0	Multimedia:	76																																																																														
Flagged Thumbnails:	0	Deleted Files:	10	E-mail Messages:	0																																																																														
Other Thumbnails:	204	From Recycle Bin:	1	Executables:	701																																																																														
Filtered In:	4590	Duplicate Items:	179	Archives:	27																																																																														
Filtered Out:	0	OLE Subitems:	339	Folders:	338																																																																														
Unfiltered		Flagged Ignore:	0	Slack/Free Space:	1708																																																																														
All Items		Actual Files:	KFF Ignorable:	Other Known Type:	45																																																																														
				Data Carved Files:	1045																																																																														

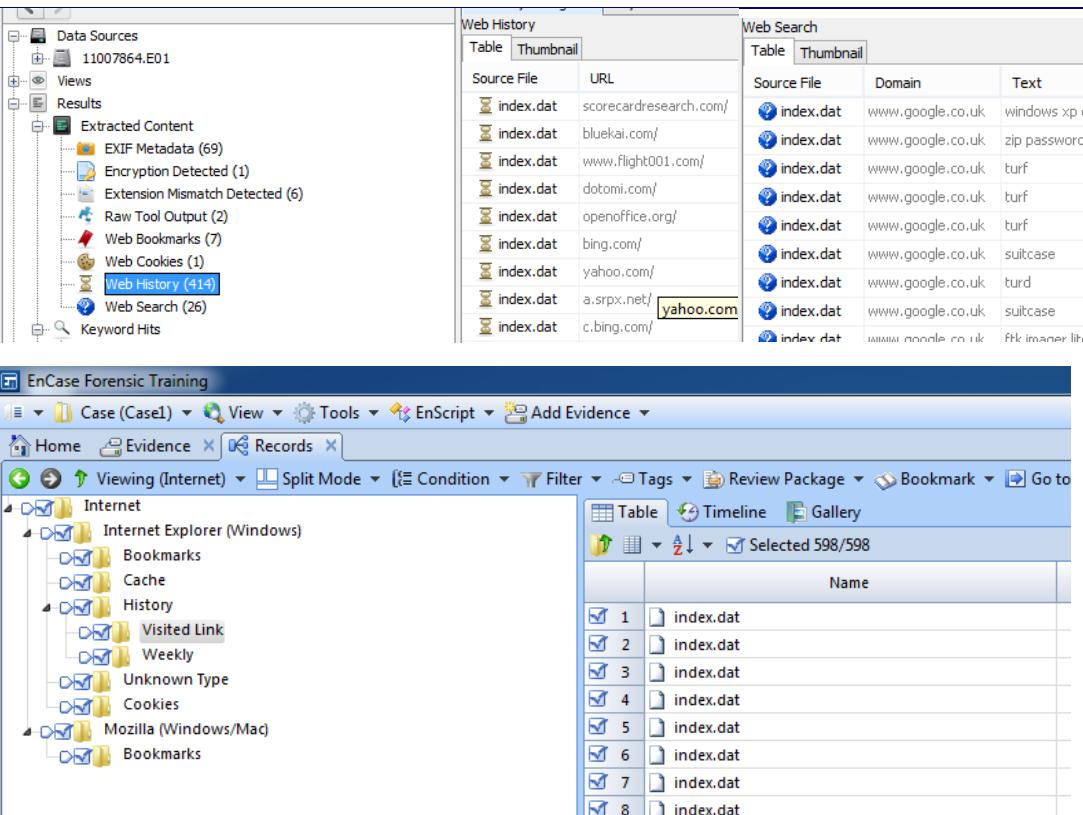
				Ran File Carver in EnCase's Processor Options. Unfortunately this did not find any additional files of obvious interest.	
Run filefinder	YES	03/11/2014	11:41		

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

				 <p>Timeline analysis, date of last activity</p> <p>YES    08/11/2014    21:24</p> <p>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.</p>	
--	--	--	--	---	--

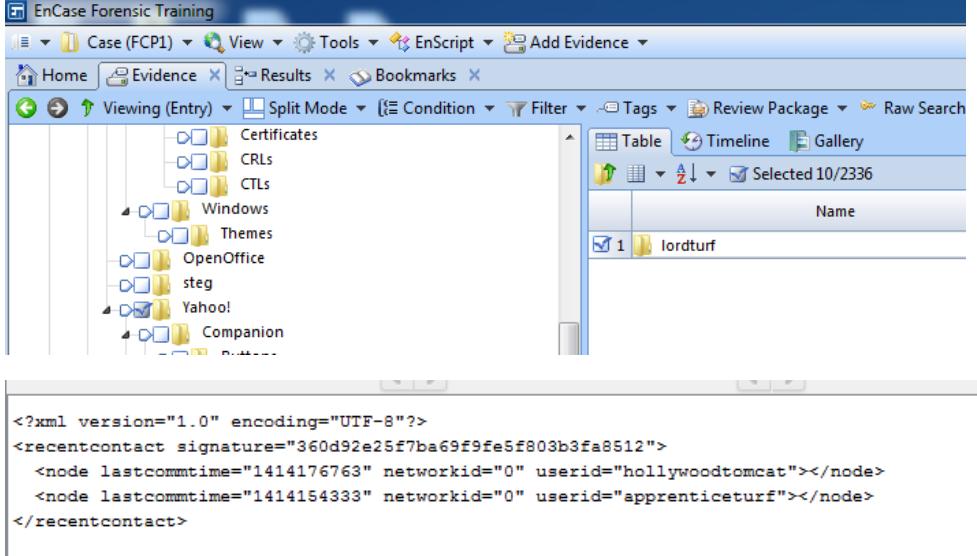
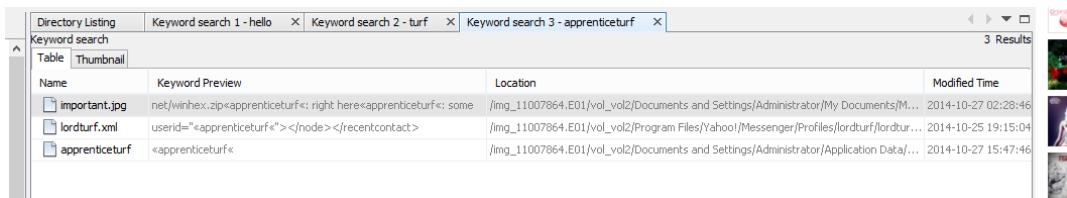
				 <p>SAMInside found that there was no password set for the administrator account and was only able to find part of the HelpAssistant password. No other useful user account was detected.</p>	
Log-on passwords – use SAMInside	YES	09/11/2014	00:26		

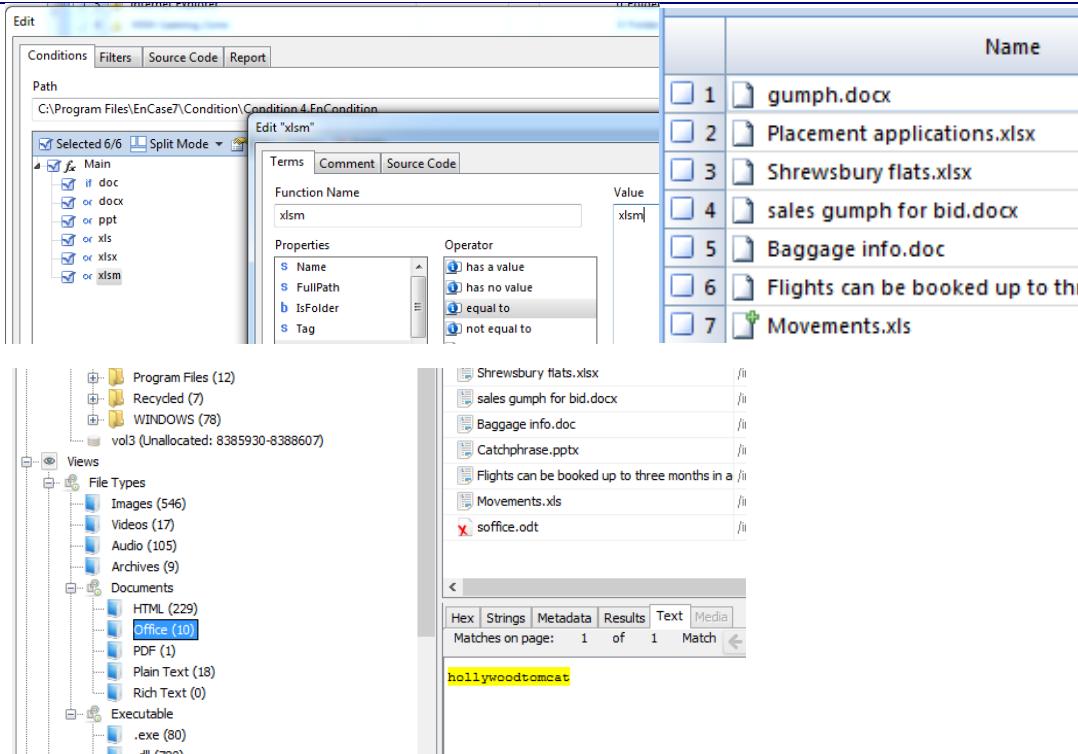
Registry protected area (Secret explorer)	YES	09/11/2014	00:57	<p>Profile List Populated.</p> <p>Import Alien Registry (READ CAREFULLY!)</p> <p>Use Import Alien Registry function to read Protected Storage of another computer. Since Protected Storage is located in Windows registry, you should specify alien registry file. This file is named ntuser.dat if target system is operated under Windows NT/2000/XP or system.dat if it is run under Win 95/98/Me</p> <p>Secret Explorer</p> <p>Selected file is not accessible. Please select valid unlocked file.</p> <p>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.</p>
--	-----	------------	-------	---

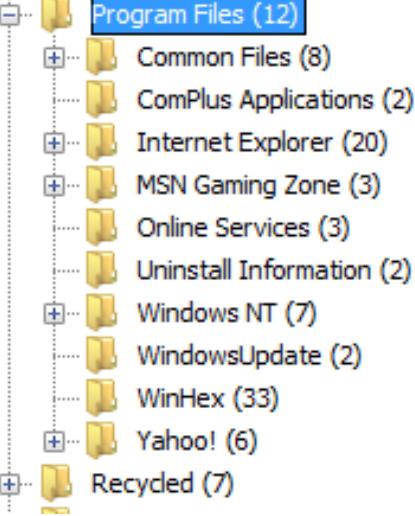
Internet History, favourites. Other browsers?  Netanalysis	YES	09/11/2014	16:55	 <p>The screenshot shows the EnCase Forensic Training software interface. On the left, a tree view under 'Extracted Content' shows categories like EXIF Metadata, Encryption Detected, Extension Mismatch Detected, Raw Tool Output, Web Bookmarks, Web Cookies, and Web History (414). The 'Web History' node is selected. To the right, there are two tables: 'Web History' and 'Web Search'. The 'Web History' table lists source files (index.dat) and URLs visited, including scorecardresearch.com/, bluekai.com/, www.flight001.com/, dotomi.com/, openoffice.org/, bing.com/, yahoo.com/, a.spx.net/, and c.bing.com/. The 'Web Search' table lists source files, domains, and search terms, including www.google.co.uk, zip password, turf, suitcase, and turd. Below these tables is a larger pane titled 'EnCase Forensic Training' showing a list of files under 'Internet' (Internet Explorer (Windows), Mozilla (Windows/Mac)) and their sub-components like Bookmarks, Cache, History, Visited Link, Weekly, Unknown Type, and Cookies.</p> <p>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.</p>	

				<p><b>Search for keywords</b></p> <hr/> <p>Use this facility to search raw text for specific keywords. The keywords and their settings are specified below.</p> <p><b>Current processing options</b></p> <table border="1"> <tr><td>password</td></tr> <tr><td>pass</td></tr> <tr><td>pa55wrd</td></tr> <tr><td>pa55word</td></tr> <tr><td>pa55w0rd</td></tr> <tr><td>pa55</td></tr> <tr><td>crime</td></tr> <tr><td>drug</td></tr> <tr><td>police</td></tr> <tr><td>agent</td></tr> <tr><td>airport</td></tr> <tr><td>Grass</td></tr> <tr><td>weed</td></tr> </table> <p>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.</p> <table border="1"> <thead> <tr> <th colspan="2">Directory Listing</th> <th>Keyword search 1 - hello</th> <th>X</th> <th>Keyword search</th> </tr> <tr> <th colspan="2">Keyword search</th> <th colspan="3"></th> </tr> <tr> <th>Table</th> <th>Thumbnail</th> <th colspan="3"></th> </tr> </thead> <tbody> <tr> <th>Name</th> <th></th> <th colspan="3">Keyword Preview</th> </tr> <tr> <td> TheCase.txt</td> <td></td> <td colspan="3">grass, or «turf», in b</td> </tr> <tr> <td> index.dat</td> <td></td> <td colspan="3">uk/search?q=&lt;turf&lt;</td> </tr> <tr> <td> Unalloc_11969_4038770176_4293596160</td> <td></td> <td colspan="3">uk/search?q=&lt;turf&lt;</td> </tr> <tr> <td> TheCase.txt</td> <td></td> <td colspan="3">grass, or «turf», in b</td> </tr> <tr> <td> TheCase.txt</td> <td></td> <td colspan="3">grass, or «turf», in b</td> </tr> <tr> <td> Turf</td> <td></td> <td colspan="3">«Turf«</td> </tr> <tr> <td> index.dat</td> <td></td> <td colspan="3">uk/search?q=&lt;turf&lt;</td> </tr> </tbody> </table>	password	pass	pa55wrd	pa55word	pa55w0rd	pa55	crime	drug	police	agent	airport	Grass	weed	Directory Listing		Keyword search 1 - hello	X	Keyword search	Keyword search					Table	Thumbnail				Name		Keyword Preview			TheCase.txt		grass, or «turf», in b			index.dat		uk/search?q=<turf<			Unalloc_11969_4038770176_4293596160		uk/search?q=<turf<			TheCase.txt		grass, or «turf», in b			TheCase.txt		grass, or «turf», in b			Turf		«Turf«			index.dat		uk/search?q=<turf<			
password																																																																									
pass																																																																									
pa55wrd																																																																									
pa55word																																																																									
pa55w0rd																																																																									
pa55																																																																									
crime																																																																									
drug																																																																									
police																																																																									
agent																																																																									
airport																																																																									
Grass																																																																									
weed																																																																									
Directory Listing		Keyword search 1 - hello	X	Keyword search																																																																					
Keyword search																																																																									
Table	Thumbnail																																																																								
Name		Keyword Preview																																																																							
TheCase.txt		grass, or «turf», in b																																																																							
index.dat		uk/search?q=<turf<																																																																							
Unalloc_11969_4038770176_4293596160		uk/search?q=<turf<																																																																							
TheCase.txt		grass, or «turf», in b																																																																							
TheCase.txt		grass, or «turf», in b																																																																							
Turf		«Turf«																																																																							
index.dat		uk/search?q=<turf<																																																																							

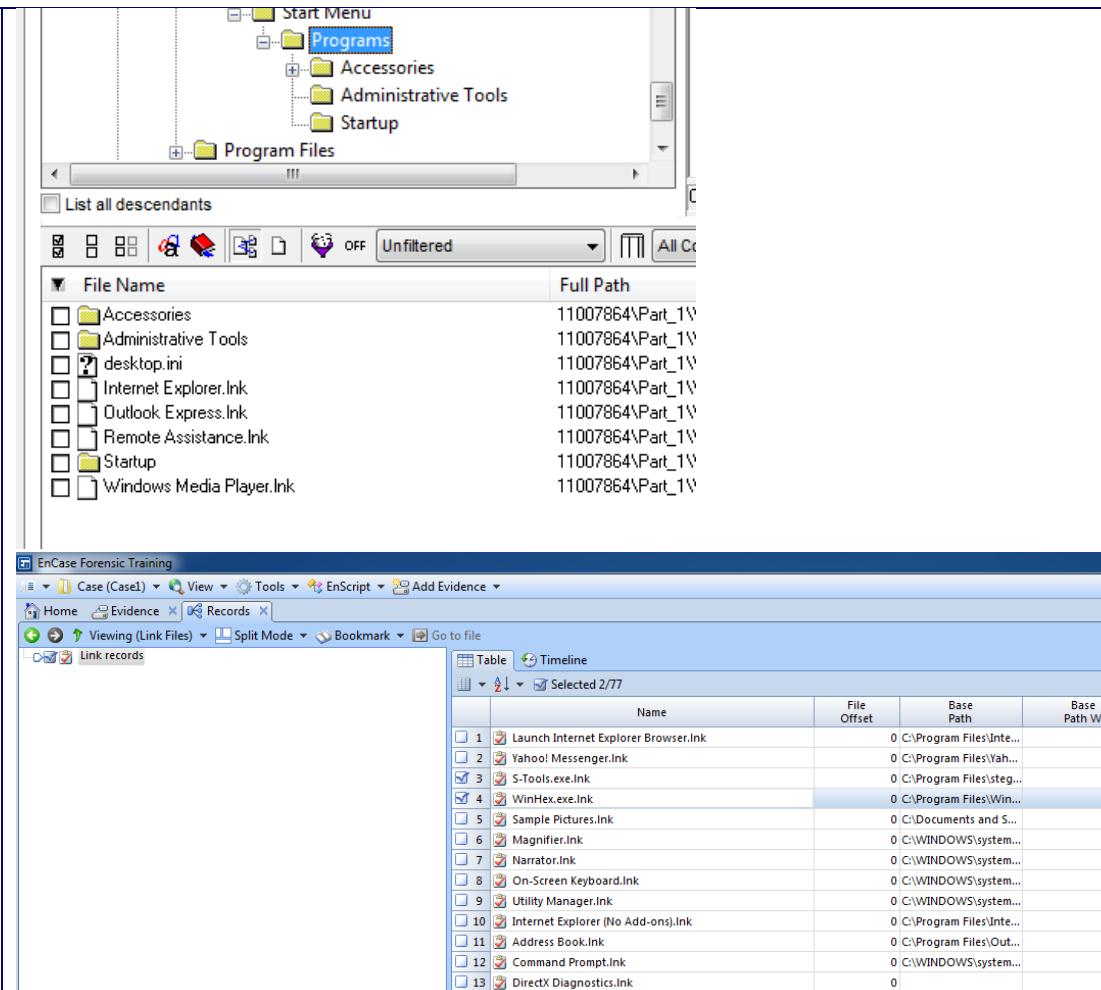
Emails, local & web-based.	YES	09/11/2014	17:43	<p>Somerset2 - Autopsy 3.1.1</p> <p>Directory Listing Keyword search 1 - hello × Keyword search 2 - turf ×</p> <p>E-Mail Messages</p> <p>Table Thumbnail</p> <p>Source File</p> <p>Extracted Content</p> <ul style="list-style-type: none"> <li>EXIF Metadata (69)</li> <li>Encryption Detected (1)</li> <li>Extension Mismatch Detected (6)</li> <li>Raw Tool Output (2)</li> <li>Web Bookmarks (7)</li> <li>Web Cookies (1)</li> <li>Web History (414)</li> <li>Web Search (26)</li> </ul> <p>Keyword Hits</p> <ul style="list-style-type: none"> <li>Single Literal Keyword Search (39)</li> <li>Single Regular Expression Search (0)</li> <li>Email Addresses (721)</li> </ul> <p>Hashset Hits</p> <ul style="list-style-type: none"> <li>E-Mail Messages</li> </ul> <p>Interesting Items</p> <p>Tags</p> <p>Reports</p> <p>No email history was discovered using EnCase, FTK or Autopsy.</p>	
----------------------------	-----	------------	-------	---	--

Action	Done	Date	Time	Notes	Initial
IM clients	YES	09/11/2014	17:53	<p></p> <p>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.</p> <p></p> <p>However, running a keyword search on the names did reveal an evidence item.</p>	

Export doc / office & exe files; look at Meta data if required	YES	09/11/2014	18:08	 <p>I ran a conditional search on EnCase to find a list of Microsoft Office files. I also used Autopsy which categorizes 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.</p>

				 <p>A screenshot of a Windows File Explorer window. The left pane shows a tree view of folders under 'Program Files (12)'. The right pane is empty. The visible items are:</p> <ul style="list-style-type: none"><li>Common Files (8)</li><li>ComPlus Applications (2)</li><li>Internet Explorer (20)</li><li>MSN Gaming Zone (3)</li><li>Online Services (3)</li><li>Uninstall Information (2)</li><li>Windows NT (7)</li><li>WindowsUpdate (2)</li><li>WinHex (33)</li><li>Yahoo! (6)</li><li>Recycled (7)</li></ul>	
Clean-up utilities. Check log files	YES	09/11/2014	18:11	<p>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.</p>	

				<p>Encryption Detected</p> <table border="1"> <thead> <tr> <th>Source File</th><th>Name</th><th>Data Source</th></tr> </thead> <tbody> <tr> <td> Amounts.zip</td><td>Full Encryption</td><td>11007864.E01</td></tr> </tbody> </table> <p>Using Autopsy an encrypted file Amounts was found. Further keyword searches found the password to unlock it.</p> <p> install.txt Files\«steg» contains the S-Tools executable and some</p> <p>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.</p>	Source File	Name	Data Source	Amounts.zip	Full Encryption	11007864.E01	
Source File	Name	Data Source									
Amounts.zip	Full Encryption	11007864.E01									
Encryption, Steg, use FTK	YES	09/11/2014	18:21								

						
Link files	YES	09/11/2014	18:41		<p>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.</p>	

Print artefacts	YES	09/11/2014	19:14	\core.sol \settings.sol \local\settings.sol	sep Unknown Fil... Unknown sig Unknown Fil... Unknown sig Unknown Fil... Unknown sol Unknown Fil... Unknown sol Unknown Fil... Unknown sol Unknown Fil... Unknown spd Unknown Fil... Unknown sql Unknown Fil... Unknown swf Audio Flash Multimedia swf Audio Flash Multimedia	10/27/2014 4:48:26 ... 9/25/2010 10/27/2014 4:48:24 ... 9/25/2010 10/27/2014 4:48:24 ... 9/25/2010 10/27/2014 4:47:44 ... 10/25/2010 10/27/2014 4:47:44 ... 10/24/2010 10/27/2014 4:47:44 ... 10/16/2010 10/27/2014 4:48:08 ... 9/25/2010 10/27/2014 4:48:22 ... 9/25/2010 10/27/2014 4:48:04 ... 2/16/2012 10/27/2014 4:48:06 ... 10/16/2010 10/27/2014 4:48:06 ... 10/16/2010 10/27/2014 4:48:06 ... 10/16/2010 10/27/2014 4:48:06 ... 10/16/2010 10/27/2014 4:48:06 ... 10/16/2010	9/25/2010 9/25/2010 9/25/2010 10/25/2010 10/24/2010 10/16/2010 9/25/2010 9/25/2010 2/16/2012 10/16/2010 10/16/2010 10/16/2010 10/16/2010 10/16/2010 10/16/2010
					No SPL, SHD or useful TMP files.		

				<p>The screenshot shows the Autopsy file browser interface. On the left, there's a sidebar with a 'File Types' section containing 'Program Files (12)' and other categories like 'Common Files', 'ComPlus Applications', etc. Below this is a 'No CD/DVD burning apps found.' message. On the right, there's a '1100/864.E01' section showing three volumes: 'vol1 (Unallocated: 0-62)', 'vol2 (Win95 FAT32 (0x0b): 63-8385929)', and 'vol3 (Unallocated: 8385930-8388607)'. The 'vol1' volume is highlighted with a blue selection bar.</p> <p>CD/DVD burning apps; check log files</p> <p>No CD/DVD burning apps found.</p> <p>1100/864.E01</p> <ul style="list-style-type: none"><li>vol1 (Unallocated: 0-62)</li><li>vol2 (Win95 FAT32 (0x0b): 63-8385929)</li><li>vol3 (Unallocated: 8385930-8388607)</li></ul> <p>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.</p>	
--	--	--	--	---	--

Action	Done	Date	Time	Notes	Initial
Additional Notes					