**Student Number:** 10005864 **Case Examined:** Suffolk

# Findings

The following evidence items were found:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Description of item** | **Significance to case** | **Full Provenance to include;** | **Method of discovery** |
| 1 | Six Yahoo IM chat logs (chat1.txt, chat2.txt, chat3.txt, chat4.txt, chat5a.txt, chat5b.txt). They contain messages between the owner of the suspect Richie Beans, Patsy Perovski and Tony T. | Sets the scene of the case. Richie is shown to be getting involved in smuggling ecstasy for a gang lead by Tony T. The gang is being watched by the police and Richie has been told to hide any evidence. | **Name:** chat1.txt  **Is Deleted:** No  **File Created**: 26/10/14 02:01:42  **Last Written:** 27/10/14 07:07:38  **Last Accessed:** 26/10/14 02:01:42  **Logical Size:** 714  **Physical Sector:** 3,039,183  **Full path:** C:/Documents and Settings/Administrator/My Documents/yahoo/IM/Chat logs/chat1.txt | Discovered when loading case into EnCase and looking through the user’s Documents folder. |
| 2 | A zip file containing a photo that was sent from Richie to Patsy. | The photo is likely of Richie holding ecstasy pills that he collected from Tony T’s gang. | **Name:** send2patsy.zip  **Is Deleted:** No  **File Created**: 26/10/14 02:13:05  **Last Written:** 27/10/14 17:22:12  **Last Accessed:** 26/10/14 02:13:05  **Logical Size:** 61,270  **Physical Sector:** 3,039,055  **Full path:** C:/Documents and Settings/NetworkService/ send2patsy.zip | The file was sent in one of the chat logs in item 01. A keyword search was used to find the file. |
| 3 | A deleted PDF that has had its extension changed to BMP. The file when the extension is corrected is an invoice. | An invoice showing a purchase of ziplock bags to sell drugs in. | **Name:** Dc3.bmp  **Is Deleted:** Yes  **File Created**: 28/10/14 ‏‎01:59:53  **Last Written:** 27/10/14 ‏‎12:43:00  **Last Accessed:** 28/10/14 ‏‎02:01:40  **Logical Size:** 14,966  **Physical Sector:** 1,094,575  **Full path:** C:/RECYCLER/S-1-5-21-1177238915-790525478-839522115-500/Dc3.bmp | Found looking through files with bad signatures. |
| 4 | An image of some zip lock bags. | The zip lock bags were mentioned in item 01 and are the item purchased for the invoice in item 03. They are the bags being used to hold the ecstasy that he is selling. | **Name:** bags.jpg  **Is Deleted:** No  **File Created**: 26/10/14 ‏‎02:20:45  **Last Written:** 27/10/14 ‏‎17:18:06  **Last Accessed:** 26/10/14 02:20:45  **Logical Size:** 4,656  **Physical Sector:** 1,366,695  **Full path:** C:/Documents and Settings/Administrator/My Pictures/bags.jpg | Found looking through pictures on the disk after finding item 01 and 03. |
| 5 | A text file with a bad extension. It has been modified to a jpg. | The file contains the string “password equivalent to Base64 format encoded to Base64 format” over and over. It implies that a password on the drive has been base64 encoded. | **Name:** bookmark.jpg  **Is Deleted:** No  **File Created**: 28/10/14 ‏‎01:42:26  **Last Written:** 27/10/14 ‏‎20:38:24  **Last Accessed:** 28/10/14 01:42:26  **Logical Size:** 3,339  **Physical Sector:** 1.093,103  **Full path:** C:/Documents and Settings/All Users/ Favorites/bookmark.jpg | The file was found when looking through all the files on the drive with bad signatures. |
| 6 | A capture of a web page Richie has visited. | Shows the website that was used to encode Richie’s password. | **Name:** bass.png  **Is Deleted:** Yes  **File Created**: 28/10/14 ‏‎08:10:10  **Last Written:** 28/10/14 08:08:54  **Last Accessed:** 28/10/14 08:10:10  **Logical Size:** 257,180  **Physical Sector:** 373,967  **Full path:** C:/Documents and Settings/Administrator/ Internet History/bass.png | Found when looking through the disks internet history. |
| 7 | A text file that appears empty, but contains another file inside of it. The inner file contains two strings. | Contains the two lines of text repeated:  squab.txt  SDNpbnpiZWVueg==  When the above is decoded it reveals a password, ‘H3inzbeenz’. | **Name:** squab.txt:hidden.txt  **Is Deleted:** No  **File Created**: 28/10/14 ‏‎03:36:29  **Last Written:** 28/10/14 03:37:43  **Last Accessed:** 28/10/14 03:36:29  **Logical Size:** 1,938  **Physical Sector:** 293,447  **Full path:** C:/Documents and Settings/All Users/ Favorites/squab.txt:hidden.txt | Found looking through the user folder after recovering the file using EnCase. |
| 8 | One of many captures of web pages that Richie has visited. | A series of how to be a drug dealer and how to deal with other drug dealers. This shows that Richie is likely new to dealing drugs and is learning how to do it. | **Name:** drukqs.jpg  **Is Deleted:** No  **File Created**: 28/10/14 ‏‎03:12:20  **Last Written:** 27/10/14 00:13:58  **Last Accessed:** 28/10/14 03:12:20  **Logical Size:** 308,844  **Physical Sector:** 1,089,311  **Full path:** C:/Documents and Settings/Administrator/ Internet History/drukqs.jpg | Found when looking through the disks internet history. |
| 9 | A screen capture of Richie’s desktop showing TrueCrypt open. | The screenshot shows not only that TrueCrypt has been used, but also the container file name. This can be used to find and unlock it. | **Name:** sceengrabber.png  **Is Deleted:** No  **File Created**: 28/10/14 ‏‎02:58:34  **Last Written:** 28/10/14 02:55:42  **Last Accessed:** 28/10/14 02:58:34  **Logical Size:** 70,800  **Physical Sector:** 316,431  **Full path:** C:/Documents and Settings/Administrator/My Pictures/sceengrabber.png | Found looking through the user’s picture folder. |
| 10 | A TrueCrypt container unlocked using the password found in item 7. | Contains a further chat log with Derek B on securing Richie’s computer. An image showing S-Tools and Slacker has likely been used. | **Name:** us.sys  **Is Deleted:** No  **File Created**: 28/10/14 ‏‎02:11:38  **Last Written:** 27/10/14 22:50:08  **Last Accessed:** 28/10/14 02:11:38  **Logical Size:** 16,777,216  **Physical Sector:** 497,799  **Full path:** C:/WINDOWS/system32/us.sys | Found using a keyword search after finding the name of the container in item 09. |
| 11 | One of many captures of web pages that Richie has visited. | Shows that a search on  For how to hide data within audio files was performed on Richie’s machine. | **Name:** goog.png  **Is Deleted:** No  **File Created**: 28/10/14 02:21:44  **Last Written:** 28/10/14 02:20:16  **Last Accessed:** 28/10/14 02:21:44  **Logical Size:** 14,148  **Physical Sector:** 1,094,655  **Full path:** C:/Documents and Settings /Administrator/Internet History/goog.png | Found when looking through the disks internet history. |
| 12 |  |  |  |  |

# Possible Scenario

## Based upon the evidence, a possible scenario is….

Richie Beans has contacted a friend Patsy Perovski asking for his help to put him in contact with some drug dealers so that he can start dealing himself. Patsy gives Richie an email address used by a gang lead by Tony T - [Tony.T@yahoo.com](mailto:Tony.T@yahoo.com). Richie spends time researching how to communicate with drug dealers and how to be one (item 8), then gets in contact with Tony. Tony sends him a USB drive containing a list of different drugs to deal and locations. With this information, Richie gets back in contact with Tony and arranges to pick up a sample of ecstasy called ‘Nintendo Pills’ at 9PM the day after the message was received. As these are copies and not originals, it is not clear what the exact date was.

Richie gets back in contact with Patsy after collecting the drugs and sends him a photo of them, as shown in item 2. He mentioned purchasing some zip lock bags to sell them in as well, as found in item 3 and 4. He also offers Patsy to get involved for a 60/40 percent cut, but Patsy doesn’t seem too interested in the offer, but doesn’t turn it down, just saying that he will think about it and get back to him.

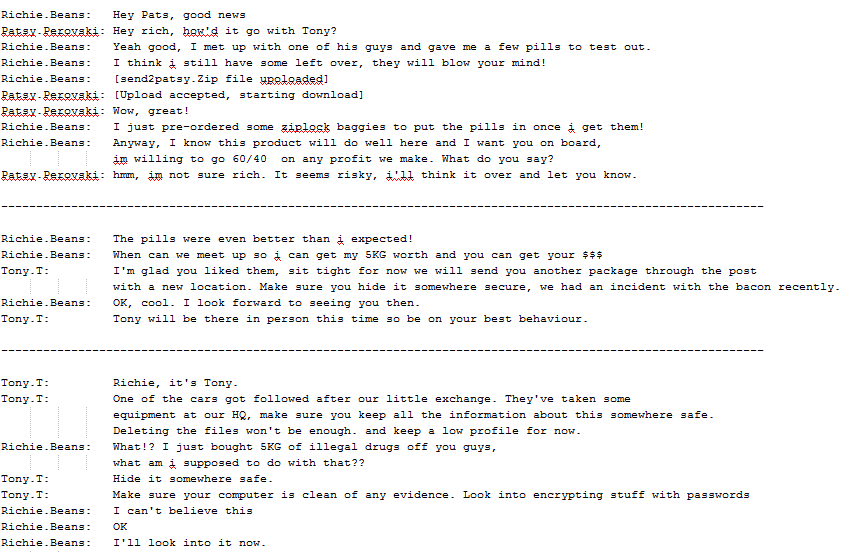
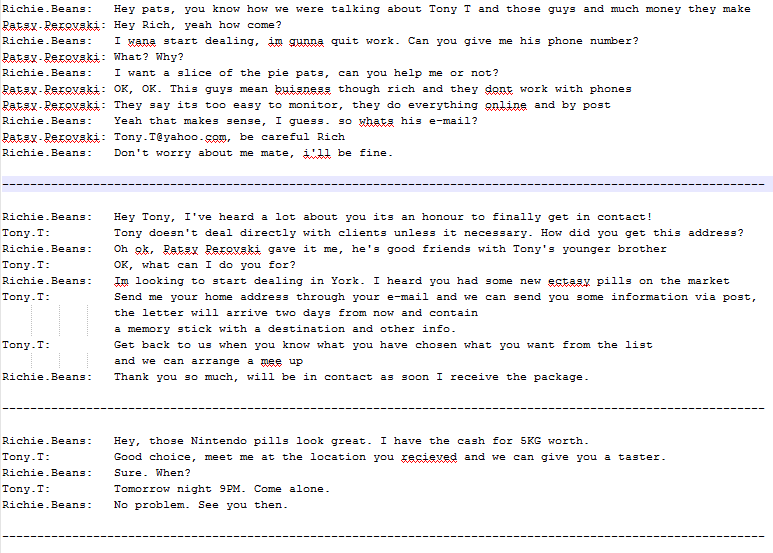
Richie contacts Tony again and is sent a second USB with a new location. He then meets up with Tony again, meeting Tony himself and not just his gang members. He collects 5kg of the ‘Nintendo Pills’ and returns home. He is then contacted by Tony saying that he has had involvement with the police and to hide any evidence of their communications and transactions.

Richie then contacts a friend who is knowledgeable in computer security, Derek B, who says he will get in contact with him shortly to help him secure his data. In the meantime he is told to research terms such as Steganography, file & volume slack, file extensions and bad clusters. Richie then installs Slacker and S-Tools and hides the chat log and a couple of screenshots within a TrueCrypt (item 10) container and puts a screenshot of the container name in his pictures folder (item 9).

He then attempts to hide the password he used for the TrueCrypt container on his computer. He visits <https://www.base64decode.org/> (item 6) and encodes the password using base64. He then adds the result to a file (item 7) which he attempts to hide inside another file. A note that he has done this is written up in a text document, which he then changes the extension to make it appear as a corrupt image (item 5).

# Description of Evidence Items

## Item 01



This set of Yahoo Instant Messages was found within the user’s document folder. As they are held in a pure text format it is likely they were retained as a log. The names of the users involved are:

* Richie Beans
* Patsy Perovski
* Tony T - Tony.T@yahoo.com

Richie.Beans: I wana start dealing, im gunna quit work. Can you give me his phone number?

Patsy.Perovski: Tony.T@yahoo.com, be careful Rich

These quotes from the first message shows that Richie Beans wants to get into drug dealing and knows that Pasty Perovski can put him in contact with someone. It is unclear if Patsy Perovski is involved, but certainly knows Tony T who is. He says that he is dangerous, but gives Richie his email address.

Richie.Beans: Im looking to start dealing in York. I heard you had some new ectasy pills on the market

Tony.T: Send me your home address through your e-mail and we can send you some information via post, the letter will arrive two days from now and contain a memory stick with a destination and other info.

Tony.T: Get back to us when you know what you have chosen what you want from the list and we can arrange a mee up

The second message shows Richie getting in contact with Tony T. However, it is not Tony who replies to the message, but one of his associates. From this it can be safely assumed there is more than one person involved, likely a larger gang.

Richie states that he wants to deal Ecstasy in York. One of Tony’s associates responds stating that he will send more information in the post on a USB stick containing a destination and a list of different options of drugs to deal.

Richie.Beans: Hey, those Nintendo pills look great. I have the cash for 5KG worth.

Tony.T: Tommorow night, 9PM. Come alone.

In the third message Richie tells Tony his choice of drugs, and says he wishes to purchase 5kg of ‘Nintendo Pills’. One of Tony’s associates then tells Richie to meet him at 9PM the next day to collect a small sample.

Richie.Beans: Yeah good, I met up with one of his guys and gave me a few pills to test out.

Richie.Beans: [send2patsy.Zip file upoloaded]

Richie.Beans: I just pre-ordered some ziplock baggies to put the pills in once i get them!

In the fourth message Richie contacts Pasty again confirming that he collected the drugs and sends him a zip, likely containing an image of the drugs. He also says that he ordered some ziplock bags to place them in.

Richie.Beans: When can we meet up so i can get my 5KG worth and you can get your $$$

Tony.T: I'm glad you liked them, sit tight for now we will send you another package through the post with a new location. Make sure you hide it somewhere secure, we had an incident with the bacon recently.

Tony.T: Tony will be there in person this time so be on your best behaviour.

The fifth message shows Richie getting in contact with Tony again to collect a 5KG batch of drugs and the money that he must have made selling the previous batch. One of Tony’s associates says he’ll send another package through the post with a new location. He also says to secure it as they’ve had an incident with the ‘bacon’, likely the police, recently. He also says that Tony will be there in person as well.

Tony.T: One of the cars got followed after our little exchange. They've taken some equipment at our HQ, make sure you keep all the information about this somewhere safe. Deleting the files won't be enough. and keep a low profile for now.

Richie.Beans: What!? I just bought 5KG of illegal drugs off you guys, what am i supposed to do with that??

Tony.T: Hide it somewhere safe. Make sure your computer is clean of any evidence. Look into encrypting stuff with passwords

In the final message, Tony states that one of his gang’s cars got followed after Richie picked up the second batch of drugs. He says to secure all the information Richie has and to hide the drugs. He also says to encrypt data on the computer with passwords.

### Summary

These messages show that Richie has become involved in drug dealing with a gang lead by Tony T. He has met the gang twice and Tony once and collected over 5kg of ecstasy pills named ‘Nintendo Pills’. He purchased zip lock bags to put them in and either used or sold the first sample of drugs somewhere in York. The gang has recently been followed and Richie has been told to secure all his personal data and to hide the drugs. Patsy is also in some way involved, but how far is currently unclear.

### What to search for next

* Further communication between Richie, Tony and Pasty.
* The zip folder send2patsy.zip
* Anything involving ecstasy
* Evidence of Nintendo pills
* Zip lock bags
* Encrypted files

## Item 02



Using a keyword search on send2patsy.zip the zip that had been sent in the previous evidence item was easily found. Unzipping it revealed this image, almost certainly the ‘Nintendo Pills’ ecstasy that Richie collected from Tony.

This image does not help lead to further items, but gives evidence of the possession of illegal drugs.

## Item 03

This item was found looking through files with a bad signature. It was labelled as a BMP file and had been deleted and held in the recycle bin. After finding an INFO2 file in the recycle bin containing the same name but with a pdf extension, it was easily modified to display correctly as an invoice.

The original file location was: C:/Documents and Settings/Administrator/My Documents/Invoice 8776874385734.bmp

The invoice is for the purchase of a hundred ziplock bags to put the drugs into. This was mentioned in the first evidence item and have almost certainly be purchased so that he can sell the drugs in small quantities.

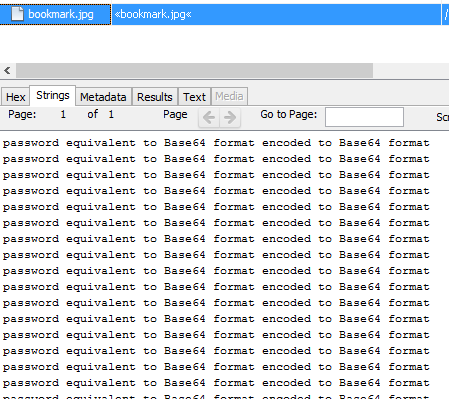
There will likely be an image of the bags located on the hard drive as they would have been viewed on a listing, so this will be searched for.

## Item 04



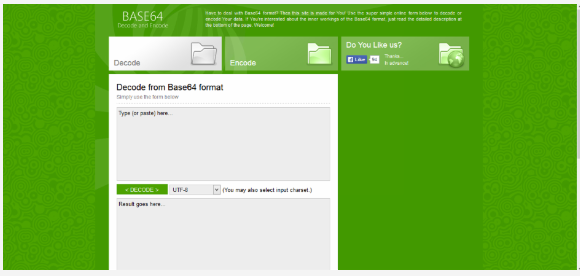
After finding the previous evidence item, I looked through all images looking for an image of the zip locked bags and found this. This, along with the image found for evidence item 2, helps confirm that bags were purchased to split the drugs between so that Richie could sell the drugs in smaller quantities.

## Item 05



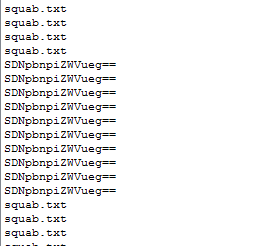
While looking through files with bad signatures I also found this. It looks as though there is a password somewhere on the hard drive that has been encoded using Base64. If I find a string that ends in one or two ‘=’s then it’s likely that it’s a password that has been encoded.

## Item 06



This screenshot confirms the item found above, that a Base64 encoder has been used to encode at least one password, if not more.

## Item 07

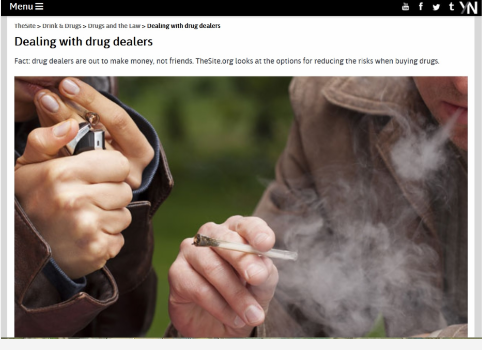
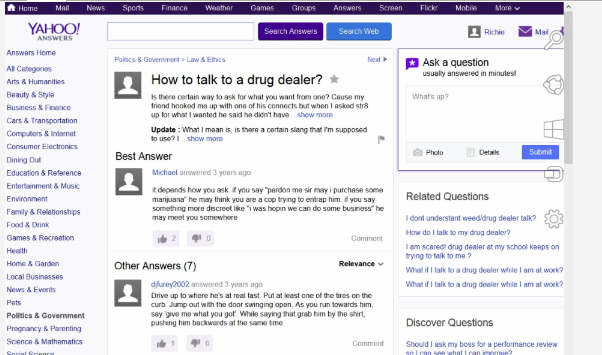
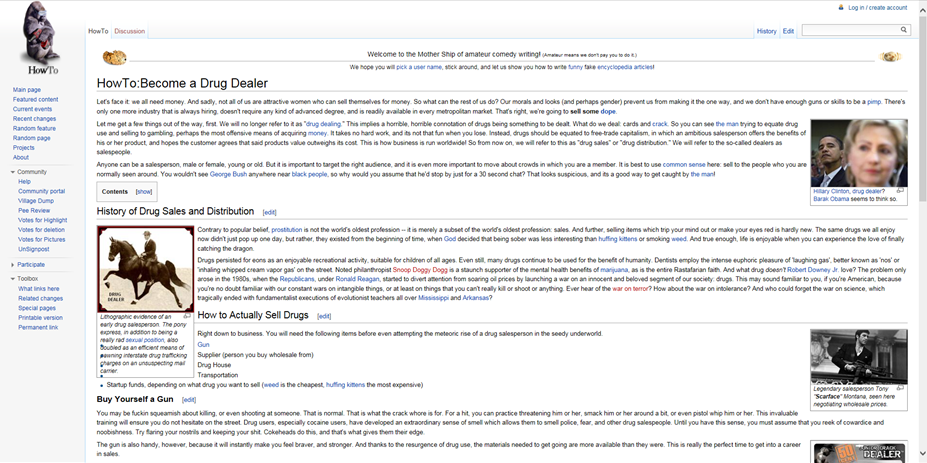


Looking through the favourite’s folder a file named ‘squab.txt’ was located. The file was empty, but appeared suspicious. After running the file carver in EnCase 7 the file squab.txt:hidden.txt was located in the same folder. Looking at the file squab.txt in FTK Imager, it appears almost as a folder, displaying the file hidden.txt inside of it.

Within a list of ‘squab.txt’, several lines contain a string with two ‘=’s after it, extremely likely to be base64 encoded as mentioned above.

Running the string through a decoder revealed the password ‘H3inzbeenz’. If a password is required for anything on the drive, this will likely be it.

## Item 08



The above are six examples of internet history looking how to become and how to talk to a drug dealer. This confirms all of the above and shows that Richie is new to drug dealing and is putting in a large amount of research before starting. He was also looking up how to deal with drug dealers, likely in preparation with his meeting with Tony.

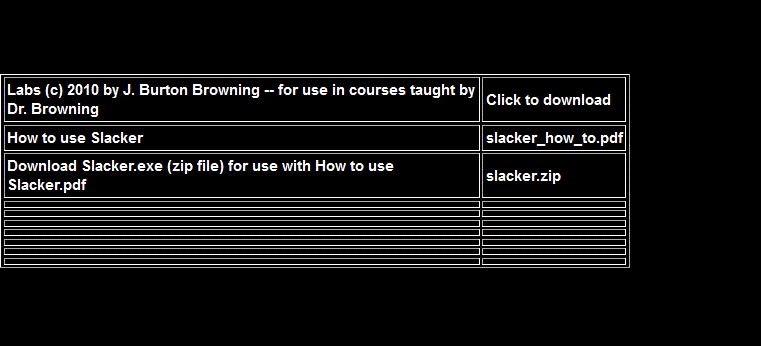
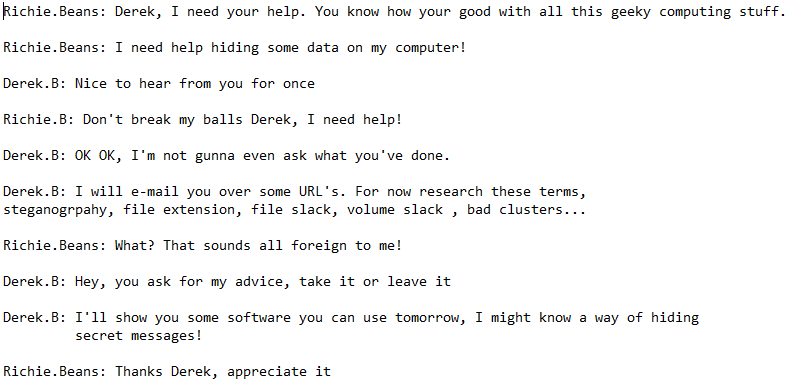
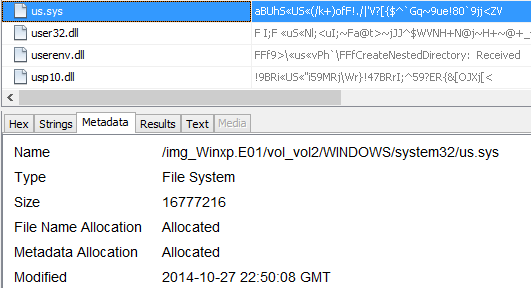
The items were found looking through internet history in Encase as well as when looking through images.

## C:\Users\David\Desktop\Suffolk\Evidence\08 - Item\sceengrabber.pngItem 09

This screenshot was found while looking through images on the hard drive. It is a screenshot showing that TrueCrypt was installed on the computer and that the container is named us.txt.

From this item I will need to install TrueCrypt and look for the file us.txt and attempt to mount it to see what it contains.

## Item 10



Although the TrueCrypt container ‘us.txt’ does not exist on the hard drive, a file named ‘us.sys’ does. The file size is large and it contains what appears to be completely random characters, unlike any other file. When loading it into TrueCrypt I used the password found earlier, ‘H3inzbeenz’. This successfully unlocked the TrueCrypt container and the three files displayer above were found within it.

The first is another chat log, this time between Richie and someone new named Derek B. It shows Richie asking for help securing data on his computer. The terms ‘steganography, file extension, file slack, volume slack, bad clusters’ are mentioned. The second file is an image of a program called Slacker which is used to hide data in file or volume slack. The last file is an image of a list of steganography tools, S-Tools being the term searched for.

### What to search for next

It is likely that slacker has been used to hide data in file or volume slack and that S-Tools has been used for steganography. File extension changes have been found. The hidden file found in item 7 may have been located in a bad cluster, but this needs to be looked into more.

## Item 11

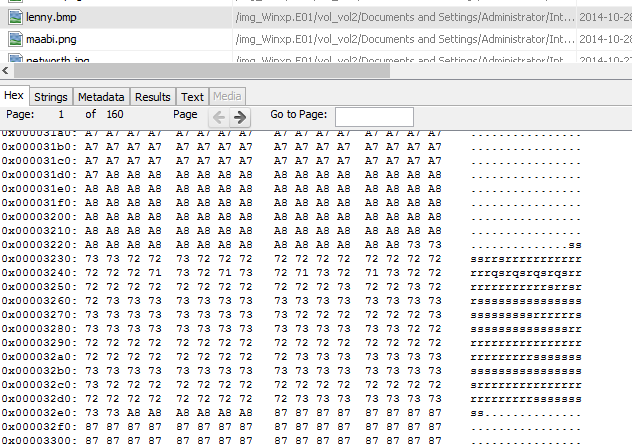
## 

This image was found when looking through images but was discarded as I was unable to read it, so assumed it was not important. However, after looking through the list of recently used documents it appeared again so I thought I would spend more time on it.

Increasing the size it is possible to just make out that it is a capture of Richie looking how to hide a message in an audio file.

As I am already looking for data hidden in slack and a use of steganography, one of these methods could potentially have been used to hide data in an audio files. There are only 11 audio files on the hard drive, so each will need to be analysed. Unfortunately none are listed on the list to the left, as that would likely have sped up the process.

## Item 12



|  |  |
| --- | --- |
| Suspect Details | Exhibit numbers, Computer details, HDD’s / Partitions / OS etc. |
| Richie Beans | Single hard drive recovered.  Operating System: Windows XP SP3 x86  Hard drive recovered: C: - NTFS  At least one Kingston USB was detected as E:/. It is likely there are a minimum of 2 from the evidence items found. |

|  |  |  |  |
| --- | --- | --- | --- |
| 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 | 20 November 2014 | Case Type | Coursework |
| Examiner | David Norton | Exam commenced | 01 December 2014 |
| Other relevant information |  | Software used, versions and licensing | * FTK 1.8.1 * EnCase 7 * Autopsy 3.1.1 * WinHex * S-Tools * SamInside * RegRipper * TrueCrypt |

| Action | Done | Date | Time | Notes | Initial | |
| --- | --- | --- | --- | --- | --- | --- |
| Load case & verify in EnCase | YES | 02/12/2014 | 13:01 | C:\Users\David\Desktop\Suffolk\Screenshots\01\Capture.PNG  Loaded into EnCase correctly. MD5 and SHA1 acquisition and verification hashes match so there has been no file alteration. |  | |
| Load case into FTK Imager | YES | 02/12/2014 | 13:21 | Loaded correctly into FTK imager. A bad cluster was found so will be worth pursuing. Nothing was found in unpartitioned space, but when looking through an INFO2 file in the recycle bin that didn’t display in EnCase, an Invoice pdf was found. This helped to find evidence item 3. |  | |
| Dual verification of key evidence items. | YES | 02/12/2014 | 13:41 | Folder structure remains constant between FTK, EnCase and Autopsy. Only difference is the format that unallocated space is displayed. Autopsy also discovered an additional volume, but it was empty.. |  | |
| Recover lost folders (FAT16 & 32). | YES | 03/12/2014 | 14:11 | C:\Users\David\Desktop\Suffolk\Screenshots\04\Capture.PNG    Recovered lost files using the ‘Recover Folder’ option in EnCase processor. Also used Autopsy to discover a total of 5834 deleted files. |  | |
| Mount archives; zip, thumbs.db, etc | YES | 03/11/2014 | 14:51 | C:\Users\David\Desktop\Suffolk\Screenshots\05\Capture.PNG    Mounted all archive files using the ‘Expand compound files’ option in EnCase processor. Found a key evidence item displayed above, although this was the only archive file found in EnCase. Autopsy found the files below. Tabs.rar is encrypted. Running a brute forcer found the password, but when trying to extract it, it returned the error below.  The password was correct but even when repairing the file I was unable to get past this error. |  | |
| File signature analysis, compute hash values | YES | 03/12/2014 | 15:12 | Ran File Signature Analysis, Protected File Analysis and Hash Analysis in EnCase processor. Helped to item (3) as it confirmed the file extension had been changed. The results could then be analysed in the Records tab in EnCase.  C:\Users\David\Desktop\Suffolk\Screenshots\06\Capture.PNG    Files with bad file extensions could also be easily viewed in FTK. |  | |
| Run filefinder | YES | 03/12/2014 | 15:32 | C:\Users\David\Desktop\Suffolk\Screenshots\07\Capture.PNG  Ran File Carver in EnCase’s Processor Options. Unfortunately this did not find any additional files of obvious interest that hadn’t already been discovered in Autopsy. |  | |
| Initialise Case script | YES | 03/12/2014 | 15:32 | Completed all processing options in EnCase 7.  Also used the Case Initializer script in EnCase 6, 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 | 03/12/2014 | 15:52 | C:\Users\David\Desktop\Suffolk\Screenshots\09\Capture.PNG  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 group together items such as squab.txt and squab.txt:hidden.txt. This helped to show the process of the user hiding the file, which would be much more difficult without the items sorted by activity. |  | |
| Log-on passwords – use SAMInside | YES | 03/12/2014 | 16:03 | C:\Users\David\Desktop\Suffolk\Screenshots\10\Capture.PNG  Neither EnCase or SAMInside were able to find passwords for the user accounts. It appears that none were set, as results came up as empty or disabled. |  | |
| Registry protected area  (Secret explorer) | YES | 03/12/2014 | 16:33 | 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.    However, although that didn’t work, RegRipper inside Autopsy did. I was able to find software on the machine and that was installed, such as CCleaner, which was used to wipe the majority of the drive. |  | |
| Internet History, favourites. Other browsers?  Netanalysis | YES | 03/12/2014 | 16:55 | C:\Users\David\Desktop\Suffolk\Screenshots\12\Capture.PNG  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 the file ‘armandosteg’, which has likely involved in some way with steganography and will be pursued further.  Unfortunately Browzar was used, meaning much of the user’s internet history is not available as no trace is left on the computer when using the software. |  | |
| Run relevant keyword searches | YES | 03/12/2014 | 17:08 | Keyword searches were run on EnCase and Autopsy numerous times throughout the project as more evidence items were discovered.  Using Autopsy I was able to find a list of email addresses as well as the Truecrypt volume, as the file name was the same but the extension had been changed. |  | |
| Emails, local & web-based. | YES | 03/12/2014 | 17:43 | No email history was discovered using EnCase, FTK or Autopsy. |  | |
| IM clients | YES | 03/12/2014 | 17:53 | C:\Users\David\Desktop\Suffolk\Screenshots\15\Capture.PNG  Yahoo Messenger chat logs were found above in plain text format. They give a good overall picture of what the case is about. The contents of each are documented thoroughly above.  A further chat log was discovered within a TrueCrypt, again documented above. No other IM clients were located on the drive. |  | |
| Export doc / office & exe files; look at Meta data if required | YES | 03/12/2014 | 18:08 | I ran a conditional search on EnCase to find Microsoft Office files. I also used Autopsy which catergories files by type, making it easy to view them together. Unfortunately there are no office files on the disk and no executables appeared to be of value. |  | |
| Clean-up utilities. Check log files | YES | 03/12/2014 | 18:08 | CCleaner was found in previous steps and evidence of its use can be found on the disk with thousands of deleted files marked as ZZZZ, as shown above. Apart from this no other clean up tools were found. The below pieces of software were also searched for: |  | |
| Encryption, Steg, use FTK | YES | 03/12/2014 | 18:21 | FTK didn’t find any encrypted files. However as mentioned above a locked RAR was found along with the password, but its contents couldn’t be extracted due to an error.  Inside the TrueCrypt folder a screenshot of a search for Stools was found, with a list of other steganography software. There was also a search for how to hide data within audio files. As S-Tools works with wav files the use of steganography in one is a possibility.  C:\Users\David\Desktop\Suffolk\Evidence\11 - Item\Startup\marked.jpgC:\Users\David\Desktop\Suffolk\Evidence\10 - Items\stools.pngThere are several suspect image files, such as a desktop image that is located multiple times on the disk in different formats. One version of the file is named ‘marked’ and I highly suspect, although at this point no other passwords have been found that link to steganography. |  | |
| Link files | YES | 03/12/2014 | 18:41 | C:\Users\David\Desktop\Suffolk\Screenshots\19\Capture.PNG  C:\Users\David\Desktop\Suffolk\Screenshots\19\Capture2.PNG  Using EnCase a full list of Link files was found using the Process Options. This revealed the chat logs, the screenshot containing the TrueCrypt container name and images of possible interest. |  | |
| Print artefacts | YES | 03/12/2014 | 19:14 | C:\Users\David\Desktop\Suffolk\Screenshots\20\Capture.PNG  No SPL, SHD or useful TMP files. |  | |
| CD/DVD burning apps; check log files | YES | 03/12/2014 | 19:24 | C:\Users\David\Desktop\Suffolk\Screenshots\21\Capture.PNG  No CD/DVD burning apps found. |  | |
| C:\Users\David\Desktop\Suffolk\Evidence\Internet History\winning.pngAdditional Notes This image shows the different devices that have been connected to the user’s computer. There are a number of logical drives and three physical drives, including a floppy drive. | | | | | |