Introduction

This report serves to develop and apply an incident response plan (IRP) for YouClan university in order to acquire forensically sound evidence from both live and dead-box systems.

The scope of this report covers the procedures for collecting this evidence, analysing it, and the handling of evidence once it has been acquired as well as the legal and ethical guidelines within each procedure.

Task 1: Image Acquisition Plan

ACPO PRINCIPLES

“No action must be taken that will change data held on a digital device that could later be relied on as evidence in Court”

The first ACPO principle ensures data integrity throughout investigations, promoting forensically sound methods when acquiring data such as the use of write blockers and hashing to ensure evidence remains unaltered when presented in court.

“If it’s necessary to access original data held on a digital device, you must be both competent to do so and able to explain your actions, as well as explain the impact of them on any digital evidence used in Court”

This principle requires that only qualified individuals may interact with original data. Actions taken along with reasoning must be recorded as and when they happen. This is crucial for the defence of actions if the evidence is later presented in court, as any discrepancy with the methods of acquisition can lead to the dismissal of the evidence.

“A trail or record of all the actions taken and applied to the digital evidence must be created and kept safely and securely. If an independent third party examines the processes they should be able to come to the same conclusion”

The third principle emphasises proper documentation. Every action that is taken, transfer of evidence and relevant dates/times should be thoroughly documented. An audit trail created using methods such as chain-of-custody forms and logging tools strengthens credibility of the investigation as the actions can be repeated and verified by a third party.

“The person in charge of the investigation has the overall responsibility of making sure these principles are followed”

The final principle serves to reinforce non-repudiation within the investigation. The leader of the investigation is charged with ensuring that all relevant laws and guidelines are followed throughout. This elevates the other ACPO principles and ensures that all evidence is found in a defensible and credible manner.

Incident Response Plan for Live and Dead-box Systems

Preparation

When a system is identified to be part of an incident, the investigator must make an informed decision whether or not to perform a live or dead-box acquisition. Nature of the evidence, risk of data loss if left powered on and time pressure are some examples of factors to consider when weighing the options between live or dead-box acquisition.

Before imaging, prepare a chain-of-custody form for each drive and audit trail with relevant information (time, location, name, etc) with space to record actions with descriptions as and when you take them **(Fig.1)**. This reinforces non-repudiation and both the second and third ACPO principles.

You should review the system to determine the physical contents, including drives directly connected to the motherboard and any removable drives. Make notes on the chain-of-custody form(s) of descriptions of the drives as well as any physical flaws.

Live box

Live image acquisition involves taking an image of a system whilst it is still powered on. This is mainly used when potential evidence is stored within volatile data that is temporarily stored and will be lost if the system is powered off (e.g. RAM, running processes and network connections).

Prior to interacting with the system, prepare a removable drive with a portable imaging software such as FTK imager. This should be done on a separate, secure system.

Once these appropriate measures are in place, you may proceed to image the volatile data that has been identified using the drive with FTK imager, outputting the dumps to the removable drive and updating your audit trail with every action you take alongside reasoning.

When all volatile data has been imaged, you may proceed to image the entire system for non-volatile data, however it is recommended that the system is powered off before this as certain elements such as malware may modify non-volatile data if the system is left running.

Finally, remove the drive and immediately create an MD5 and SHA256 hash of the images using a secure device, logging them on the audit trail and chain-of-custody forms. Once the data has been hashed and verified as non-corrupted the drive may be placed within a safe container attached to the chain-of-custody form.

Dead box

When approaching a system that has already been powered off and isolated, the consideration is no longer on the volatile data but on the integrity of the non-volatile data contained within. This is where a dead-box acquisition should be performed.

Prior to interaction with the system, prepare an additional drive for every identified drive within the system, ensuring they have larger capacities than the drives you are imaging.

Prepare another drive on a secure system with a live environment such as CAINE that can be booted without installation. Check the target system's BIOS settings before powering on to ensure it is not pin-coded and that the boot drive can be changed. If the system BIOS is pin-coded each drive will have to be removed, decrypted and imaged separately.

Once the CAINE loaded drive is prepared alongside chain-of-custody and audit trail forms, plug the drive into the system and change the boot drive to the CAINE distribution.

Once CAINE has loaded, change the date and time to match the your own, this ensures that photographs can be taken throughout that serve to reinforce the information found of the audit trail.

Proceed to image each drive using Guymager (a built in forensics tool within CAINE), outputting each image to the appropriate additional drive prepared prior to interaction. Guymager will allow you to input relevant information such as case numbers, evidence numbers and investigator names which serve to further reinforce the information on the audit trail and chain-of-custody forms.

Using Guymager, produce MD5 and SHA256 hashes for each image and log them on the audit trail and chain of custody forms. The drives should then be placed in the appropriate containers linked to the relevant chain-of-custody forms.

Acquired MD5 HASH: 644e0e2a62b85dc2c25e7a595b173b6b

Task 2: Incident Response Procedures

Preparing EnCase for Analysis

Once an image has been acquired via live or dead-box acquisition, you will be able to analyse it securely using EnCase. Take a copy of the image to analyse (In line with the first ACPO principle), ensuring hashes match those on the chain-of-custody form , confirming it has not been modified from acquisition to now. Prepare an audit trail to record your actions.

Prepare EnCase by creating a new case with an appropriate name. Fill out the information with a relevant case number matching that on the chain-of-custody form, your name and a description of the case. (Fig.1)

Adding Evidence

Evidence can be added from the home page of the case, under the 'Add Evidence' tab, you can then add the image or raw image file depending on the method of acquisition.

Confirming MBR Validity

In cases where the device is corrupt or has been maliciously tampered with, the MBR should be examined for partition information. Using EnCase navigate to the image file, select it and from the taskbar at the top select 'Disk View' to view the device by its sectors.

Device boot information and partition information is found in the first sector, the relevant information being located in the byte range 446-509 within the first sector. Select the first sector then using the tab at the bottom and change from 'Text' to 'Hex'.

Each partition is contained within 16 bit ranges between 446-509, using Fig.3 you may manually analyse each partition to determine its values. EnCase can perform this for you by highlighting the 16 byte range for each partition and selecting Partition Entry in the Decode tab.

If a partition is not automatically picked up by EnCase, you may run Case Processor from the Enscript tab on the top taskbar to find partitions, which you may then manually mount by selecting Partitions->Add Partition and defining the information you have found.

Parsing for Evidence

Once all partitions are mounted, create a key word list based on the incident. From the Evidence tab select the entire drive and from the top task bar select Raw Search Selected, then run a search based on your key word list. EnCase will then return all hits on each word in the list. Any hits may then be inspected, tagged and bookmarked as possible evidence for the report.

EnCase offers automatic features to expedite evidence searches, from the Evidence tab select Process Evidence->Process to select a range of tasks for EnCase to run. For incidents where there may be evidence within internet files you can specify to find history, bookmarks, cookies, etc within the drive. This is then viewable within the artifacts tab where new evidence can be analysed.

Legal/Ethical and Good Practice Guidelines

As with the imaging of the original device, all steps you are performing to examine the evidence should be recorded within the audit trail (Fig.1), alongside relevant information such as your name, time etc allowing a third party to replicate the same results at a later date. This ensures the third ACPO principle is being maintained throughout.

Throughout the course of the investigation,it should be consistent that all four ACPO principles as well as UK laws on data protection, privacy etc are maintained, as if they are not the credibility of the investigation will significantly decrease and any evidence may be dismissed.

Reporting

Once all partitions have been analysed, EnCase can generate a report based on all bookmarked evidence along with file paths, tags and comments, allowing third parties to easily locate the same evidence at a later date. This can be done by navigating to the bookmark folder of all found evidence, right clicking it and adding it to the report. This report can then be exported to various file formats (PDF, HTML) for presentation. Ensure you re-hash the drive to verify integrity.

Task 3: Evaluation of Procedures and Findings

The following is a representation of what to fill out on an audit trail to justify actions, with figures representing screenshots that would go in the log.

(Fig.2) - Creation of an EnCase File, filled in with my own relevant information to this scenario, with myself as the investigator.

From the home page, I selected 'Add Device' (Fig.4), selected 'Raw Image' (Fig.5), then filled in the information with the .dd file and named it appropriately (Fig.6).

Once added, I navigated to the 'Evidence' tab and selected 'Disk View' on the drive to view sectors of the drive. (Fig.7)

Highlighting the first sector, I view the bytes in Hex and highlighted 446-509 (Fig.8), selecting Partition Entry in the Decode tab to expedite the process (Fig.9). This showed an additional partition to the two that EnCase automatically mounted.

Using Enscript->Case Processor, I found an Unused Disk Area which matched the partition information I had found for the additional partition (Fig.10).

I then navigated to the start sector, selected Partitions->Add Partition and manually filled in the information, mounting the partition and allowing me to view it inside the Evidence tab (Fig.11).

I then ran a keyword search by selecting all partitions, then selecting Raw Search Selected and inputting my list of keywords (Fig.12), returning hits which I then inspected (Fig.13).

As this investigation found evidence of emails and internet searches it was relevant to run an artefact search by selecting Process Evidence->Process and selecting Find email and Find Internet Artifacts (Fig.14) This yielded information on history and cookies relevant to the investigation (Fig.15)

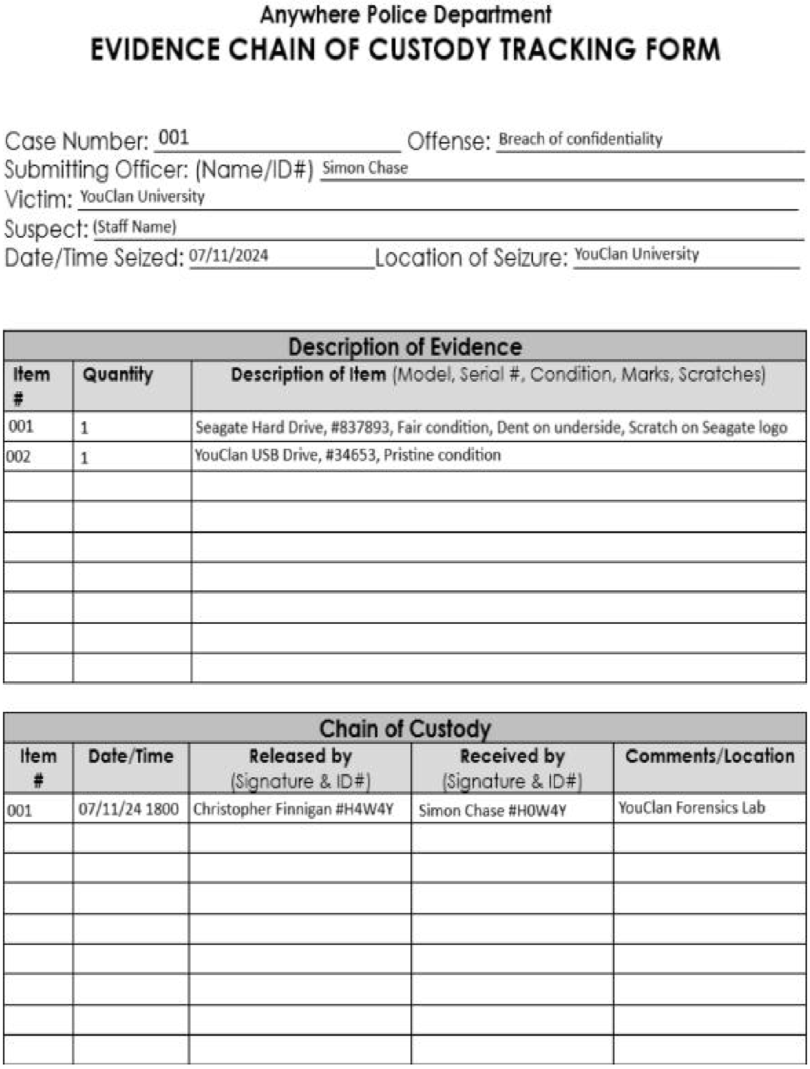
Verification Hash (Fig.24): 644e0e2a62b85dc2c25e7a595b173b6b

8. Recovered Evidence/Artifacts

Figures 16-22 provide evidence included in the final report, along with the relevant descriptions attached to them, with Figure 23 being the final report exported from EnCase.

Appendices

Figure 1



Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: 001 Offense: Breach of confidentiality

Submitting Officer: (Name/ID#) Simon Chase

Victim: YouClan University

Suspect: (Staff Name)

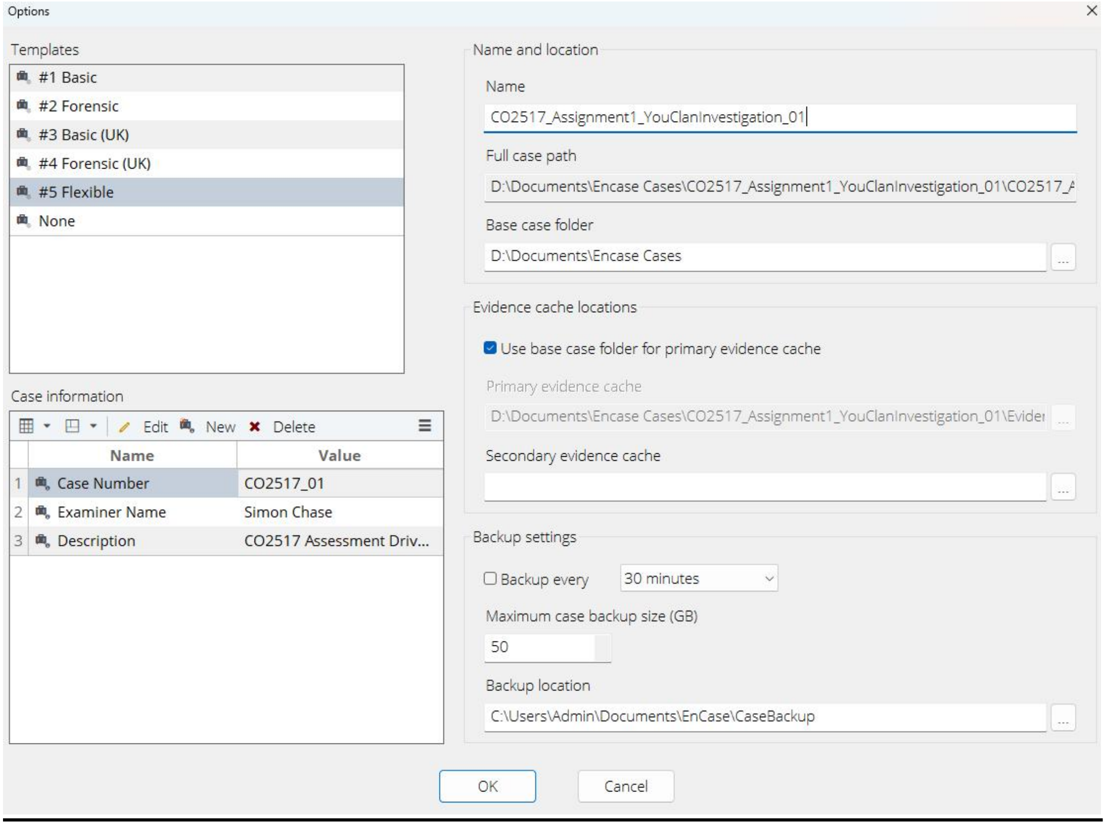
Date/Time Seized: 07/11/2024 Location of Seizure: YouClan University

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)
001	1	Seagate Hard Drive, #837893, Fair condition, Dent on underside, Scratch on Seagate logo
002	1	YouClan USB Drive, #34653, Pristine condition

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**
001	07/11/24 1800	Christopher Finnigan #H4W4Y	Simon Chase #H0W4Y	YouClan Forensics Lab

Fig.1 - An example template of a chain of custody form

Figure 2



Options

Templates

- #1 Basic
- #2 Forensic
- #3 Basic (UK)
- #4 Forensic (UK)
- #5 Flexible
- None

Case information

	Name	Value
1	Case Number	CO2517_01
2	Examiner Name	Simon Chase
3	Description	CO2517 Assessment Driv...

Name and location

Name: CO2517_Assignment1_YouClanInvestigation_01

Full case path: D:\Documents\Encase Cases\CO2517_Assignment1_YouClanInvestigation_01\CO2517_A

Base case folder: D:\Documents\Encase Cases

Evidence cache locations

☑ Use base case folder for primary evidence cache

Primary evidence cache: D:\Documents\Encase Cases\CO2517_Assignment1_YouClanInvestigation_01\Evider

Secondary evidence cache:

Backup settings

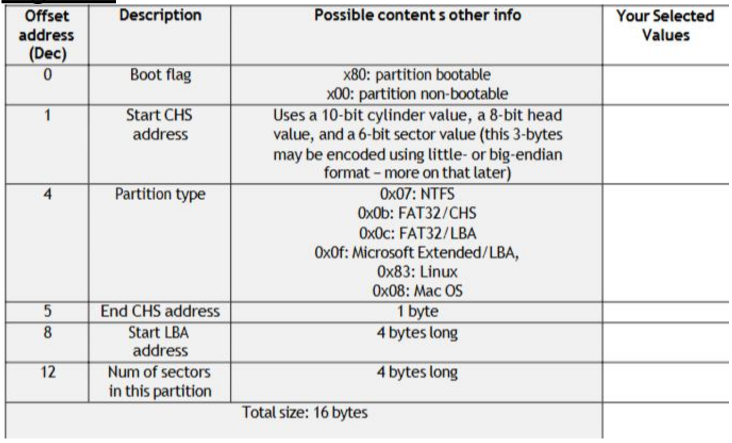
□ Backup every 30 minutes

Maximum case backup size (GB): 50

Backup location: C:\Users\Admin\Documents\EnCase\CaseBackup

Fig.2 - A filled out page for the creation of an EnCase case

Figure 3



Offset address (Dec)	Description	Possible content s other info	Your Selected Values
0	Boot flag	x80: partition bootable x00: partition non-bootable	
1	Start CHS address	Uses a 10-bit cylinder value, a 8-bit head value, and a 6-bit sector value (this 3-bytes may be encoded using little- or big-endian format – more on that later)	
4	Partition type	0x07: NTFS 0x0b: FAT32/CHS 0x0c: FAT32/LBA 0x0f: Microsoft Extended/LBA, 0x83: Linux 0x08: Mac OS	
5	End CHS address	1 byte	
8	Start LBA address	4 bytes long	
12	Num of sectors in this partition	4 bytes long	
		Total size: 16 bytes	

Fig.3 - A table allowing for the manual analysis of partition information

Figure 4

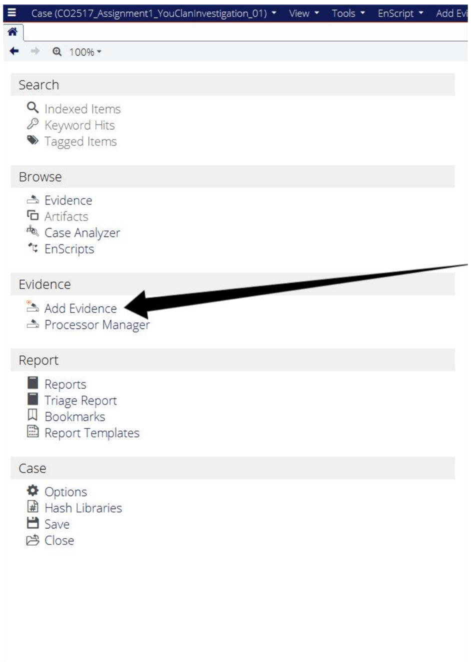


Fig.4 - A pointer to where to access the 'Add Evidence' tab from the home page of an EnCase case

Figure 5

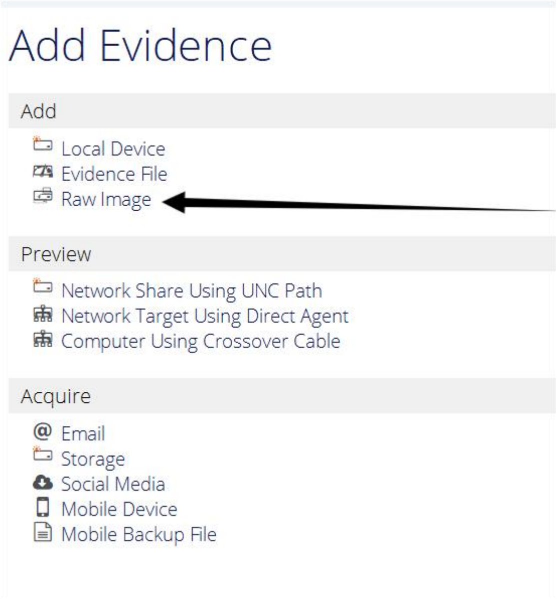
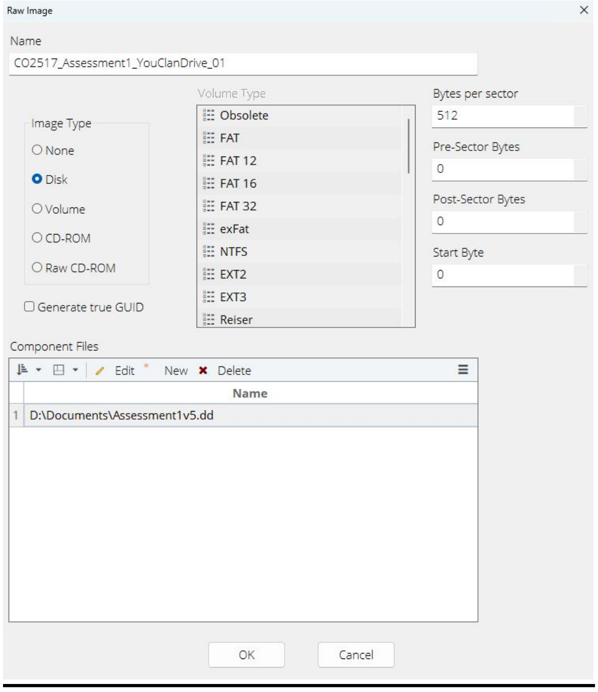


Fig.5 - A pointer to where to add a raw image file as acquired in the scenario, if using an evidence file select the option above 'Raw Image'

Figure 6



Name: CO2517_Assessment1_YouClanDrive_01

Image Type: ○ None ● Disk ○ Volume ○ CD-ROM ○ Raw CD-ROM

□ Generate true GUID

Bytes per sector: 512

Pre-Sector Bytes: 0

Post-Sector Bytes: 0

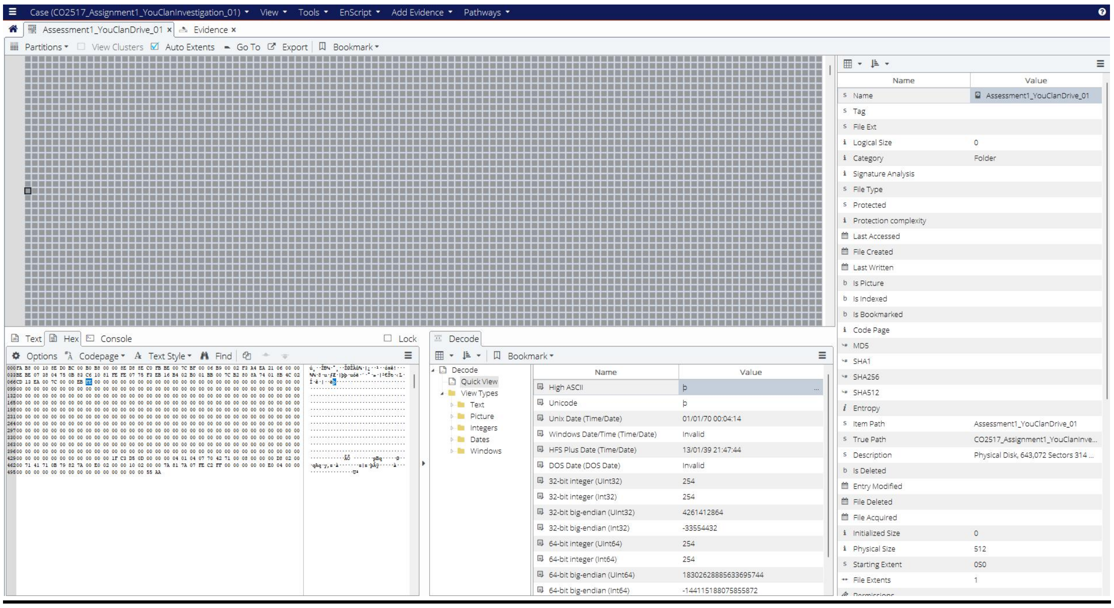
Start Byte: 0

Component Files

	Name
1	D:\Documents\Assessment1v5.dd

Fig.6 - A filled out page for adding a Raw Image file, complete with path to file, image type and name

Figure 7

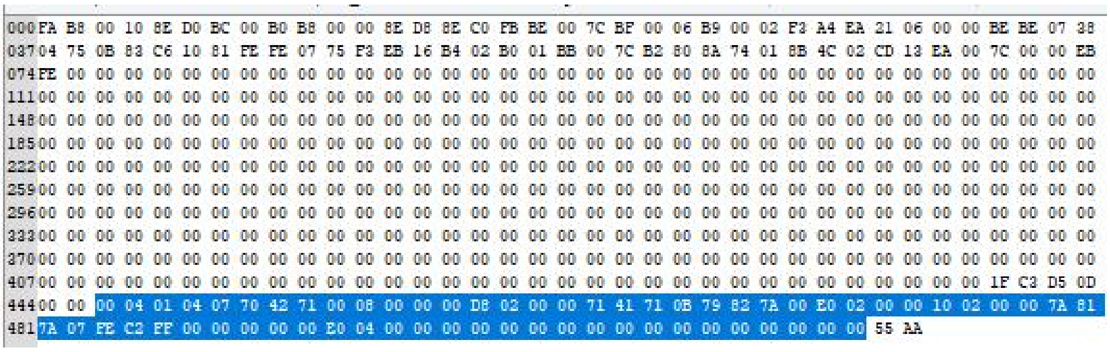


Name	Value
High ASCII	þ
Unicode	þ
Unix Date (Time/Date)	01/01/70 00:04:14
Windows Date/Time (Time/Date)	Invalid
HFS Plus Date (Time/Date)	13/01/39 21:47:44
DOS Date (DOS Date)	Invalid
32-bit integer (UInt32)	254
32-bit integer (Int32)	254
32-bit big-endian (UInt32)	4261412864
32-bit big-endian (Int32)	-33554432
64-bit integer (UInt64)	254
64-bit integer (Int64)	254
64-bit big-endian (UInt64)	18302628885633695744
64-bit big-endian (Int64)	-144115188075855872

Name	Value
Name	Assessment1_YouClanDrive_01
Tag	
File Ext	
Logical Size	0
Category	Folder
Signature Analysis	
File Type	
Protected	
Protection complexity	
Last Accessed	
File Created	
Last Written	
Is Picture	
Is Indexed	
Is Bookmarked	
Code Page	
MD5	
SHA1	
SHA256	
SHA512	
Entropy	
Item Path	Assessment1_YouClanDrive_01
True Path	CO2517_Assignment1_YouClanInve...
Description	Physical Disk, 643,072 Sectors 314 ...
Is Deleted	
Entry Modified	
File Deleted	
File Acquired	
Initialized Size	0
Physical Size	512
Starting Extent	0S0
File Extents	1

Fig.7 - A full page screenshot of the sector view page of the acquired device

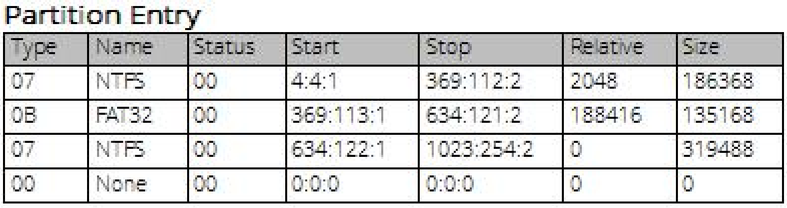
Figure 8



```
000FA B8 00 10 8E D0 BC 00 B0 B8 00 00 8E D8 8E C0 FB BE 00 7C BF 00 06 B9 00 02 F3 A4 EA 21 06 00 00 BE BE 07 38
03704 75 0B 83 C6 10 81 FE FE 07 75 F3 EB 16 B4 02 B0 01 BB 00 7C B2 80 8A 74 01 8B 4C 02 CD 13 EA 00 7C 00 00 EB
074FE 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
11100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
14800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
18500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
22200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
25900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
29600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
33300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
37000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
40700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1F C3 D5 0D
44400 00 00 04 01 04 07 70 42 71 00 08 00 00 00 D8 02 00 00 71 41 71 0B 79 82 7A 00 E0 02 00 00 10 02 00 00 7A 81
4817A 07 FE C2 FF 00 00 00 00 00 E0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA
```

Fig.8 - Highlighted bytes 446 - 509 containing partition information

Figure 9

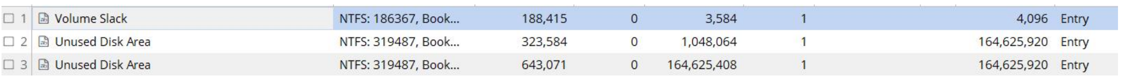


Partition Entry

Type	Name	Status	Start	Stop	Relative	Size
07	NTFS	00	4:4:1	369:112:2	2048	186368
0B	FAT32	00	369:113:1	634:121:2	188416	135168
07	NTFS	00	634:122:1	1023:254:2	0	319488
00	None	00	0:0:0	0:0:0	0	0

Fig.9 - Table of partition information acquired through EnCase's Decode->Windows->Partition Entry view when bytes 446 - 509 are highlighted

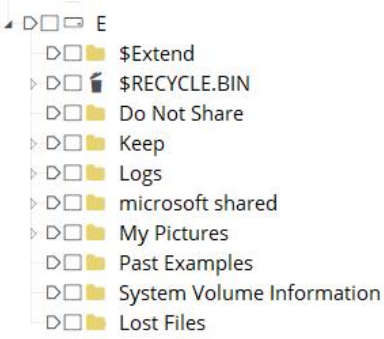
Figure 10



□ 1	Volume Slack	NTFS: 186367, Book...	188,415	0	3,584	1	4,096	Entry
□ 2	Unused Disk Area	NTFS: 319487, Book...	323,584	0	1,048,064	1	164,625,920	Entry
□ 3	Unused Disk Area	NTFS: 319487, Book...	643,071	0	164,625,408	1	164,625,920	Entry

Fig.10 - The output of using Enscript->Case Processor showing Unused Disk Area in line with the additional partition information in Fig.9

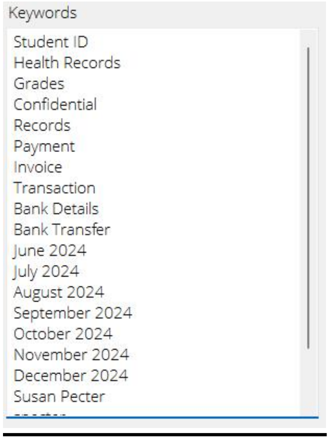
Figure 11



```
E
    $Extend
    $RECYCLE.BIN
    Do Not Share
    Keep
    Logs
    microsoft shared
    My Pictures
    Past Examples
    System Volume Information
    Lost Files
```

Fig.11 - The folders contained within the additional partition, shown in evidence view after the additional partition has been mounted

Figure 12

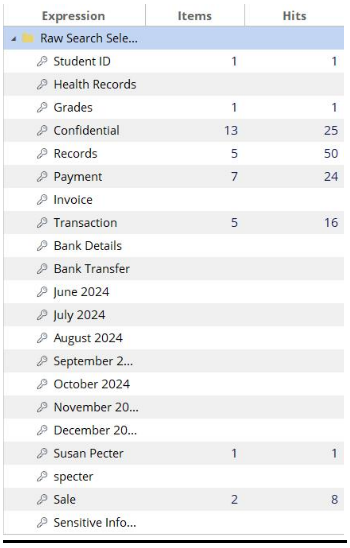


Keywords

Student ID
Health Records
Grades
Confidential
Records
Payment
Invoice
Transaction
Bank Details
Bank Transfer
June 2024
July 2024
August 2024
September 2024
October 2024
November 2024
December 2024
Susan Pecter

Fig.12 - Keyword list used within the keyword search of all partitions

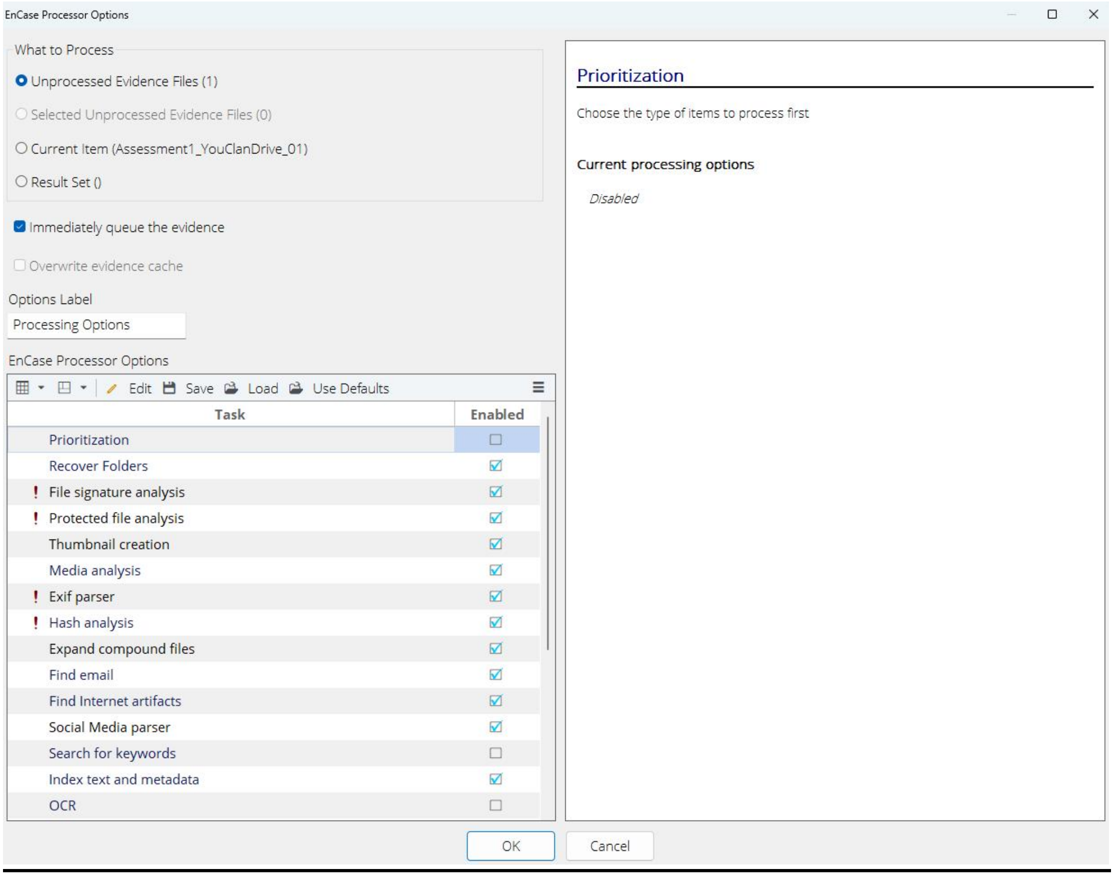
Figure 13



Expression	Items	Hits
Raw Search Sele...		
Student ID	1	1
Health Records		
Grades	1	1
Confidential	13	25
Records	5	50
Payment	7	24
Invoice		
Transaction	5	16
Bank Details		
Bank Transfer		
June 2024		
July 2024		
August 2024		
September 2...		
October 2024		
November 20...		
December 20...		
Susan Pecter	1	1
specter		
Sale	2	8
Sensitive Info...		

Fig.13 - The list of keyword hits found after the keyword search

Figure 14



EnCase Processor Options

What to Process

● Unprocessed Evidence Files (1)

○ Selected Unprocessed Evidence Files (0)

○ Current Item (Assessment1_YouClanDrive_01)

○ Result Set ()

☑ Immediately queue the evidence

☐ Overwrite evidence cache

Options Label

Processing Options

EnCase Processor Options

	Task	Enabled
	Prioritization	☐
	Recover Folders	☑
!	File signature analysis	☑
!	Protected file analysis	☑
	Thumbnail creation	☑
	Media analysis	☑
!	Exif parser	☑
!	Hash analysis	☑
	Expand compound files	☑
	Find email	☑
	Find Internet artifacts	☑
	Social Media parser	☑
	Search for keywords	☐
	Index text and metadata	☑
	OCR	☐

Prioritization

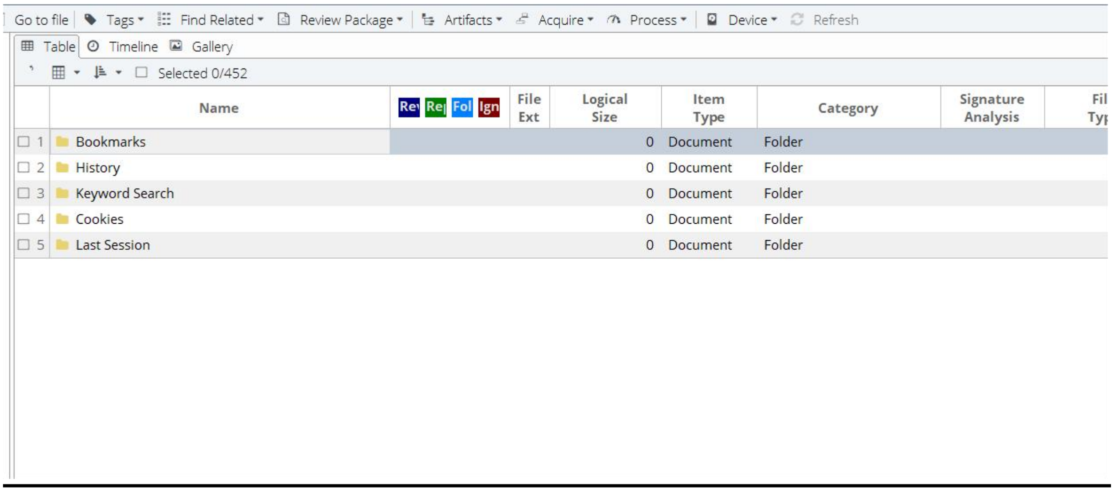
Choose the type of items to process first

Current processing options

Disabled

Fig.14 - The filled out page for running Process Evidence->Process in order to find Internet Artifacts

Figure 15

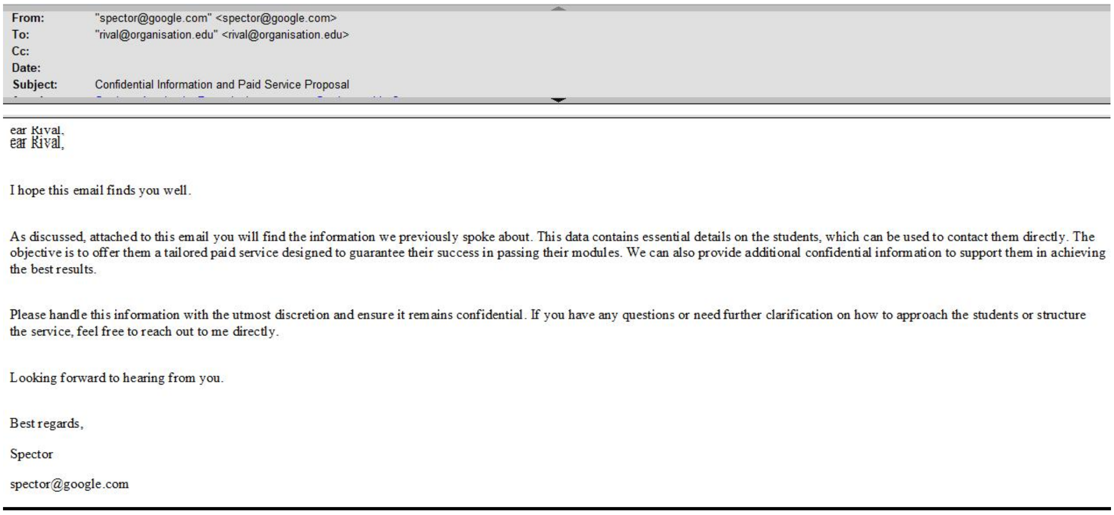


Selected 0/452

	Name	Rev	Rej	Fol	Ign	File Ext	Logical Size	Item Type	Category	Signature Analysis	Fil Typ
☐ 1	Bookmarks						0	Document	Folder		
☐ 2	History						0	Document	Folder		
☐ 3	Keyword Search						0	Document	Folder		
☐ 4	Cookies						0	Document	Folder		
☐ 5	Last Session						0	Document	Folder		

Fig.15 - The results of the artefact search conducted in Fig.14

Figure 16



From: "spector@google.com" <spector@google.com>
To: "rival@organisation.edu" <rival@organisation.edu>
Cc:
Date:
Subject: Confidential Information and Paid Service Proposal

ear Rival,
ear Rival,

I hope this email finds you well.

As discussed, attached to this email you will find the information we previously spoke about. This data contains essential details on the students, which can be used to contact them directly. The objective is to offer them a tailored paid service designed to guarantee their success in passing their modules. We can also provide additional confidential information to support them in achieving the best results.

Please handle this information with the utmost discretion and ensure it remains confidential. If you have any questions or need further clarification on how to approach the students or structure the service, feel free to reach out to me directly.

Looking forward to hearing from you.

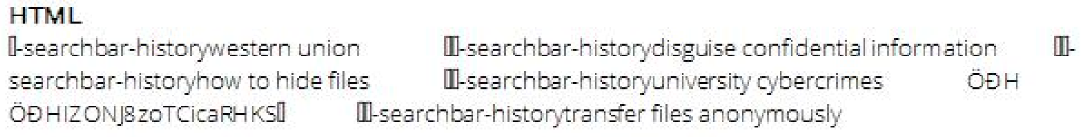
Best regards,

Spector

spector@google.com

Fig.16 - Email from "spector@google.com" to rival organisation regarding sending private student data in order to target them with specific paid services and additional confidential info (E/Keep/This/Folder/For_Transferring_Funds/New_File.keep)

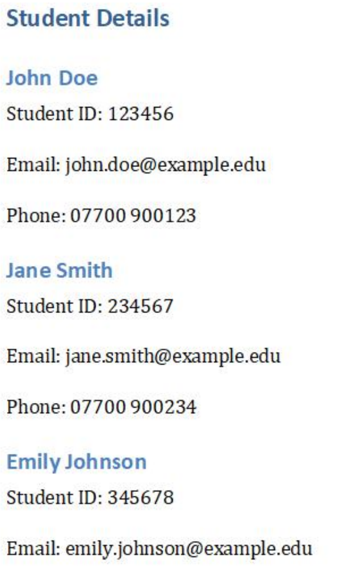
Figure 17



```
HTML
□-searchbar-historywestern union          □□-searchbar-historydisguise confidential information      □□-
searchbar-historyhow to hide files        □□-searchbar-historyuniversity cybercrimes              ÖÐH
ÖÐHIZONJ8zoTCicaRHKS□        □□-searchbar-historytransfer files anonymously
```

Fig.17 - Search bar history located in formhistory.sqlite related to Fig.22, found in internet artefact search.

Figure 18



Student Details

John Doe

Student ID: 123456

Email: john.doe@example.edu

Phone: 07700 900123

Jane Smith

Student ID: 234567

Email: jane.smith@example.edu

Phone: 07700 900234

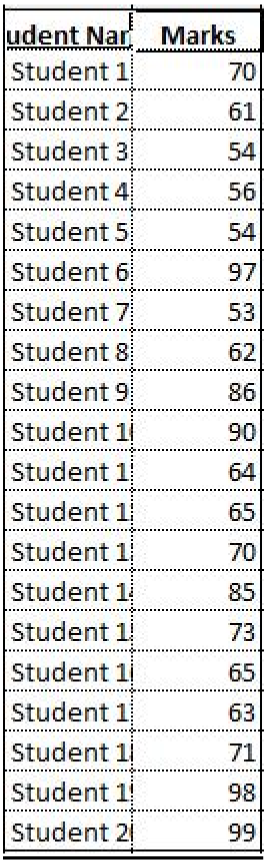
Emily Johnson

Student ID: 345678

Email: emily.johnson@example.edu

Fig.18 - File containing confidential student information found on corrupt partition

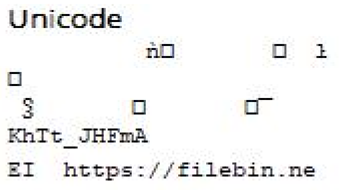
Figure 19



udent Nar	Marks
Student 1	70
Student 2	61
Student 3	54
Student 4	56
Student 5	54
Student 6	97
Student 7	53
Student 8	62
Student 9	86
Student 1	90
Student 1	64
Student 1	65
Student 1	70
Student 1	85
Student 1	73
Student 1	65
Student 1	63
Student 1	71
Student 1	98
Student 2	99

Fig.19 - File containing student marks found on Susan Pector's corrupt pratition, linked to other confidential information

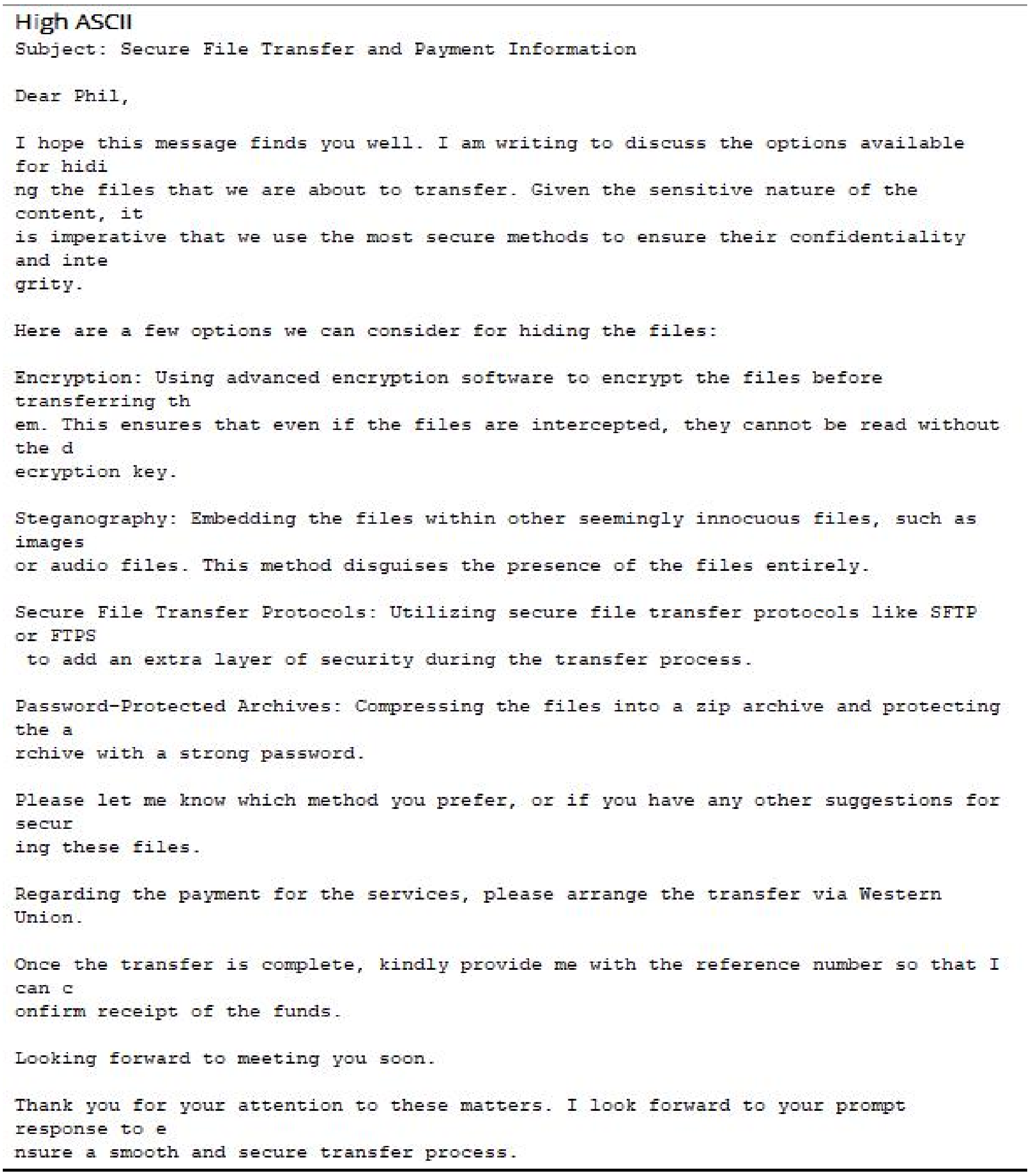
Figure 20



```
Unicode
          ǹ□       □  ł
□
 Ȿ       □        □¯
KhTt_JHFmA
EI  https://filebin.ne
```

Fig.20 - Found in places.sqlite links to a website for anonymously sharing files, acquired in internet artefact search

Figure 21

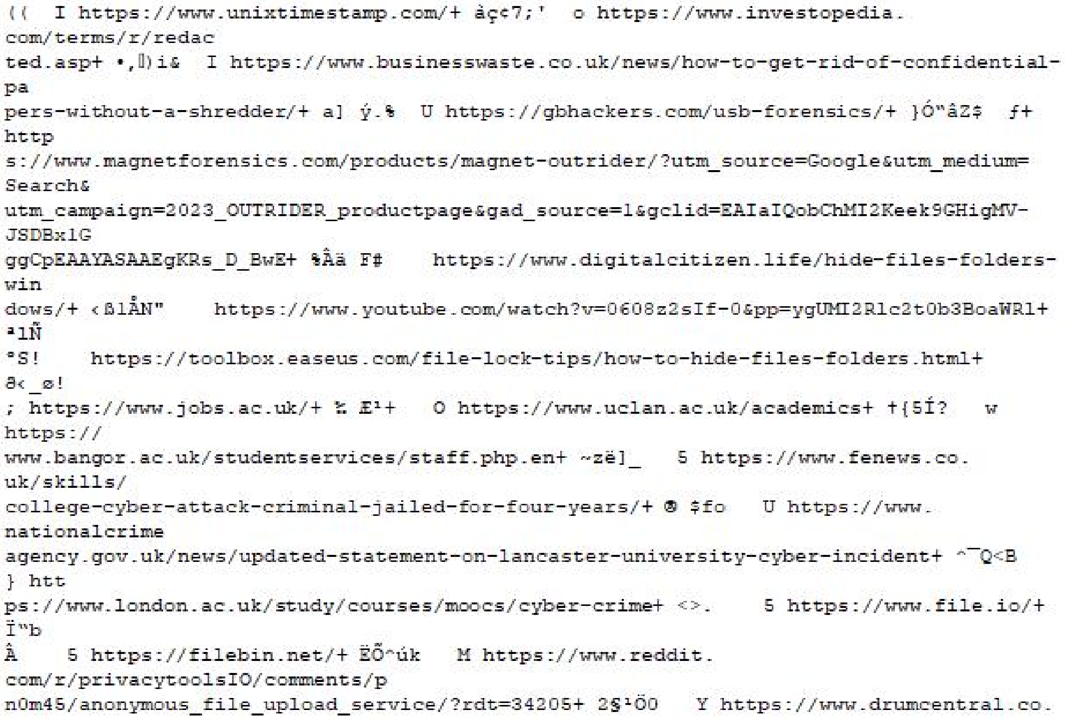


High ASCII

```
Subject: Secure File Transfer and Payment Information

Dear Phil,

I hope this message finds you well. I am writing to discuss the options available
for hidi
ng the files that we are about to transfer. Given the sensitive nature of the
content, it
is imperative that we use the most secure methods to ensure their confidentiality
and inte
grity.

Here are a few options we can consider for hiding the files:

Encryption: Using advanced encryption software to encrypt the files before
transferring th
em. This ensures that even if the files are intercepted, they cannot be read without
the d
ecryption key.

Steganography: Embedding the files within other seemingly innocuous files, such as
images
or audio files. This method disguises the presence of the files entirely.

Secure File Transfer Protocols: Utilizing secure file transfer protocols like SFTP
or FTPS
 to add an extra layer of security during the transfer process.

Password-Protected Archives: Compressing the files into a zip archive and protecting
the a
rchive with a strong password.

Please let me know which method you prefer, or if you have any other suggestions for
secur
ing these files.

Regarding the payment for the services, please arrange the transfer via Western
Union.

Once the transfer is complete, kindly provide me with the reference number so that I
can c
onfirm receipt of the funds.

Looking forward to meeting you soon.

Thank you for your attention to these matters. I look forward to your prompt
response to e
nsure a smooth and secure transfer process.
```

Fig.21 - Correspondance discussing securely transferring sensitive files as well as payment for services through Western Union (Search History in Fig.17), found in E/Past_Examples/blockout.txt

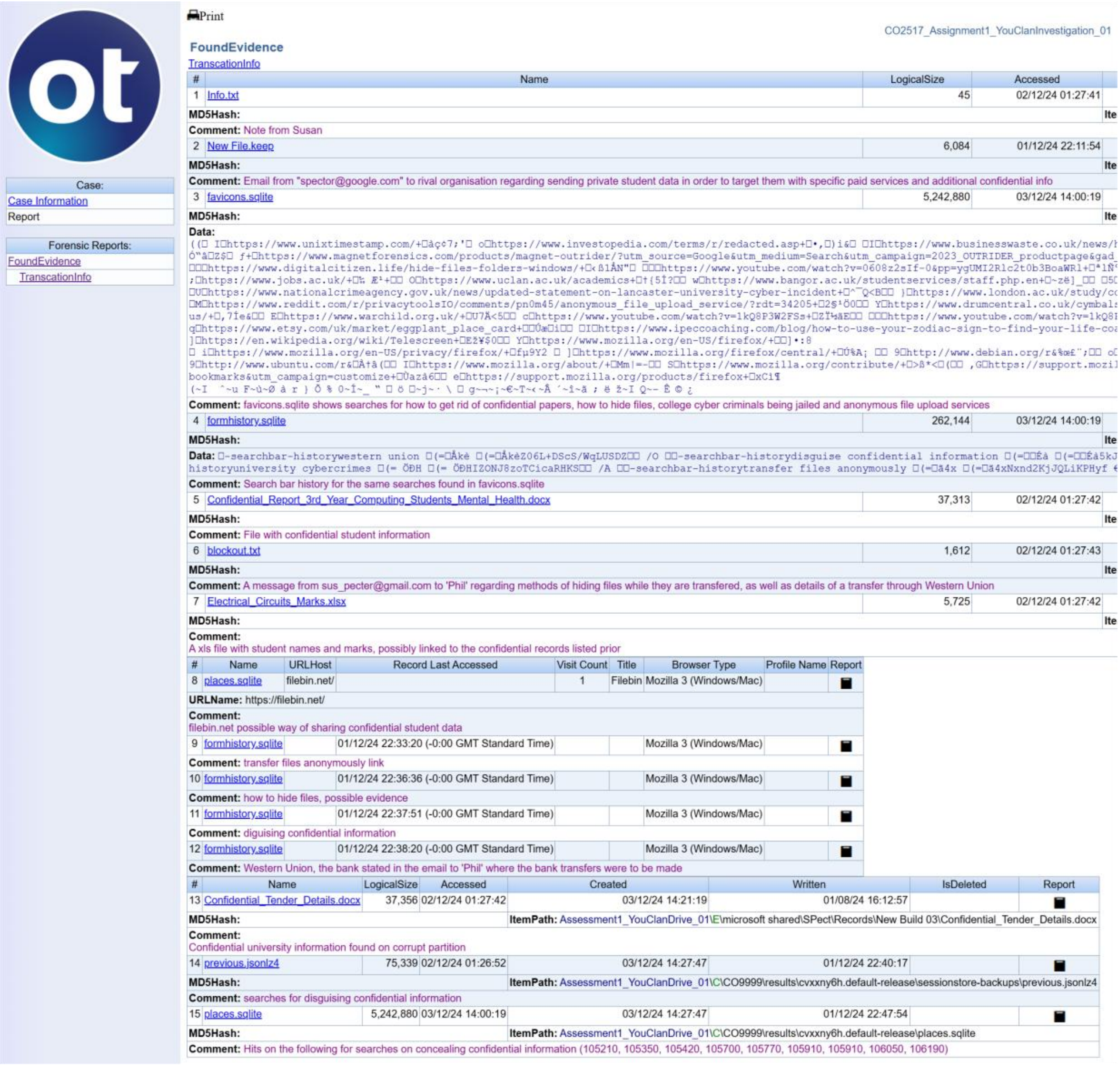
Figure 22



```
(( I https://www.unixtimestamp.com/+ àç¢7;'  o https://www.investopedia.
com/terms/r/redac
ted.asp+ •,)i&  I https://www.businesswaste.co.uk/news/how-to-get-rid-of-confidential-
pa
pers-without-a-shredder/+ a] ý.%  U https://gbhackers.com/usb-forensics/+ }Ó"âZ$  ƒ+
http
s://www.magnetforensics.com/products/magnet-outrider/?utm_source=Google&utm_medium=
Search&
utm_campaign=2023_OUTRIDER_productpage&gad_source=1&gclid=EAIaIQobChMI2Keek9GHigMV-
JSDBx1G
ggCpEAAYASAAEgKRs_D_BwE+ %Âä F#    https://www.digitalcitizen.life/hide-files-folders-
win
dows/+ <ß1ÅN"    https://www.youtube.com/watch?v=0608z2sIf-0&pp=ygUMI2R1c2t0b3BoaWR1+
ª1Ñ
°S!    https://toolbox.easeus.com/file-lock-tips/how-to-hide-files-folders.html+
ð<_ø!
; https://www.jobs.ac.uk/+ % Æ¹+   O https://www.uclan.ac.uk/academics+ †{5Í?   w
https://
www.bangor.ac.uk/studentservices/staff.php.en+ ~zë]_   5 https://www.fenews.co.
uk/skills/
college-cyber-attack-criminal-jailed-for-four-years/+ ® $fo   U https://www.
nationalcrime
agency.gov.uk/news/updated-statement-on-lancaster-university-cyber-incident+ ^¯Q<B
} htt
ps://www.london.ac.uk/study/courses/moocs/cyber-crime+ <>.    5 https://www.file.io/+
Ï"b
Â    5 https://filebin.net/+ ËÕ^úk   M https://www.reddit.
com/r/privacytoolsIO/comments/p
n0m45/anonymous_file_upload_service/?rdt=34205+ 2§¹Ö0   Y https://www.drumcentral.co.
```

A set of search history detailing getting rid of confidential information, hiding folders, college cyber crime, as well as staff services from other universities, potentially linked as the rivals corresponded with in Fig.21 and Fig.16, found in internet artefact search

Figure 23



Case:
Case Information
Report

Forensic Reports:
FoundEvidence
TranscationInfo

Print

CO2517_Assignment1_YouClanInvestigation_01

FoundEvidence

TranscationInfo

#	Name	LogicalSize	Accessed
1	Info.txt	45	02/12/24 01:27:41

MD5Hash: Ite

Comment: Note from Susan

#	Name	LogicalSize	Accessed
2	New File.keep	6,084	01/12/24 22:11:54

MD5Hash: Ite

Comment: Email from "spector@google.com" to rival organisation regarding sending private student data in order to target them with specific paid services and additional confidential info

#	Name	LogicalSize	Accessed
3	favicons.sqlite	5,242,880	03/12/24 14:00:19

MD5Hash: Ite

Data:

```
((□ I□https://www.unixtimestamp.com/+□àç¢7;'□ o□https://www.investopedia.com/terms/r/redacted.asp+□•,□)i&□ □I□https://www.businesswaste.co.uk/news/h
Ó"â□Z$□ ƒ+□https://www.magnetforensics.com/products/magnet-outrider/?utm_source=Google&utm_medium=Search&utm_campaign=2023_OUTRIDER_productpage&gad_
□□□https://www.digitalcitizen.life/hide-files-folders-windows/+□‹ß1ÅN"□ □□□https://www.youtube.com/watch?v=0608z2sIf-0&pp=ygUMI2Rlc2t0b3BoaWRl+□ª1Ñ
;□https://www.jobs.ac.uk/+□‰ Æ¹+□□ O□https://www.uclan.ac.uk/academics+□†{5Î?□□ w□https://www.bangor.ac.uk/studentservices/staff.php.en+□-zë]_□□ □5□
□U□https://www.nationalcrimeagency.gov.uk/news/updated-statement-on-lancaster-university-cyber-incident+□^¯Q<B□□ }□https://www.london.ac.uk/study/co
□M□https://www.reddit.com/r/privacytoolsIO/comments/pn0m45/anonymous_file_upload_service/?rdt=34205+□2§¹Ö0□□ Y□https://www.drumcentral.co.uk/cymbals
us/+□,7Ïe&□□ E□https://www.warchild.org.uk/+□U7Ă<5□□ c□https://www.youtube.com/watch?v=1kQ8P3W2FSs+□ZÏ¼ãE□□ □□□https://www.youtube.com/watch?v=1kQ8P
q□https://www.etsy.com/uk/market/eggplant_place_card+□□Úæ□i□□ □I□https://www.ipeccoaching.com/blog/how-to-use-your-zodiac-sign-to-find-your-life-coa
]□https://en.wikipedia.org/wiki/Telescreen+□Ež¥$0□□ Y□https://www.mozilla.org/en-US/firefox/+□□]•:8
□ i□https://www.mozilla.org/en-US/privacy/firefox/+□fµ9Y2 □ ]□https://www.mozilla.org/firefox/central/+□Ú%A; □□ 9□http://www.debian.org/r&%œ£";□□ o□
9□http://www.ubuntu.com/r&□Á†â(□□ I□https://www.mozilla.org/about/+□Mm|=-□□ S□https://www.mozilla.org/contribute/+□>ß*<□(□□ ,G□https://support.mozil
bookmarks&utm_campaign=customize+□Ùazä6□□ e□https://support.mozilla.org/products/firefox+□xCi¶
(~I  ˆ~u F~ù~Ø à r } Õ % 0~Î~_ " □ ö □~j~· \ □ g~¬~¡~€~T~‹~Å ´~î~ã ; ë ž~I Q~- Ê © ¿
```

Comment: favicons.sqlite shows searches for how to get rid of confidential papers, how to hide files, college cyber criminals being jailed and anonymous file upload services

#	Name	LogicalSize	Accessed
4	formhistory.sqlite	262,144	03/12/24 14:00:19

MD5Hash: Ite

Data:

```
□-searchbar-historywestern union □(=□Åkè □(=□ÅkèZ06L+DScS/WqLUSDZ□□ /O □□-searchbar-historydisguise confidential information □(=□□Éà □(=□□Éà5kJ
historyuniversity cybercrimes □(= ÕĐH □(= ÕĐHIZONJ8zoTCicaRHKS□□ /A □□-searchbar-historytransfer files anonymously □(=□ä4x □(=□ä4xNxnd2KjJQLiKPHyf €
```

Comment: Search bar history for the same searches found in favicons.sqlite

#	Name	LogicalSize	Accessed
5	Confidential_Report_3rd_Year_Computing_Students_Mental_Health.docx	37,313	02/12/24 01:27:42

MD5Hash: Ite

Comment: File with confidential student information

#	Name	LogicalSize	Accessed
6	blockout.txt	1,612	02/12/24 01:27:43

MD5Hash: Ite

Comment: A message from sus_pecter@gmail.com to 'Phil' regarding methods of hiding files while they are transfered, as well as details of a transfer through Western Union

#	Name	LogicalSize	Accessed
7	Electrical_Circuits_Marks.xlsx	5,725	02/12/24 01:27:42

MD5Hash: Ite

Comment:
A xls file with student names and marks, possibly linked to the confidential records listed prior

#	Name	URLHost	Record Last Accessed	Visit Count	Title	Browser Type	Profile Name	Report
8	places.sqlite	filebin.net/		1	Filebin	Mozilla 3 (Windows/Mac)		■

URLName: https://filebin.net/

Comment:
filebin.net possible way of sharing confidential student data

#	Name	URLHost	Record Last Accessed	Visit Count	Title	Browser Type	Profile Name	Report
9	formhistory.sqlite		01/12/24 22:33:20 (-0:00 GMT Standard Time)			Mozilla 3 (Windows/Mac)		■

Comment: transfer files anonymously link

#	Name	URLHost	Record Last Accessed	Visit Count	Title	Browser Type	Profile Name	Report
10	formhistory.sqlite		01/12/24 22:36:36 (-0:00 GMT Standard Time)			Mozilla 3 (Windows/Mac)		■

Comment: how to hide files, possible evidence

#	Name	URLHost	Record Last Accessed	Visit Count	Title	Browser Type	Profile Name	Report
11	formhistory.sqlite		01/12/24 22:37:51 (-0:00 GMT Standard Time)			Mozilla 3 (Windows/Mac)		■

Comment: diguising confidential information

#	Name	URLHost	Record Last Accessed	Visit Count	Title	Browser Type	Profile Name	Report
12	formhistory.sqlite		01/12/24 22:38:20 (-0:00 GMT Standard Time)			Mozilla 3 (Windows/Mac)		■

Comment: Western Union, the bank stated in the email to 'Phil' where the bank transfers were to be made

#	Name	LogicalSize	Accessed	Created	Written	IsDeleted	Report
13	Confidential_Tender_Details.docx	37,356	02/12/24 01:27:42	03/12/24 14:21:19	01/08/24 16:12:57		■

MD5Hash: **ItemPath:** Assessment1_YouClanDrive_01\E\microsoft shared\SPect\Records\New Build 03\Confidential_Tender_Details.docx

Comment:
Confidential university information found on corrupt partition

#	Name	LogicalSize	Accessed	Created	Written	IsDeleted	Report
14	previous.jsonlz4	75,339	02/12/24 01:26:52	03/12/24 14:27:47	01/12/24 22:40:17		■

MD5Hash: **ItemPath:** Assessment1_YouClanDrive_01\C\CO9999\results\cvxxny6h.default-release\sessionstore-backups\previous.jsonlz4

Comment: searches for disguising confidential information

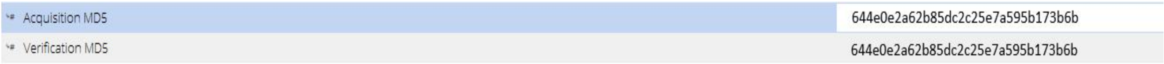
#	Name	LogicalSize	Accessed	Created	Written	IsDeleted	Report
15	places.sqlite	5,242,880	03/12/24 14:00:19	03/12/24 14:27:47	01/12/24 22:47:54		■

MD5Hash: **ItemPath:** Assessment1_YouClanDrive_01\C\CO9999\results\cvxxny6h.default-release\places.sqlite

Comment: Hits on the following for searches on concealing confidential information (105210, 105350, 105420, 105700, 105770, 105910, 105910, 106050, 106190)

Fig.23 - The outputted report of all found evidence and artefacts

Figure 24



Acquisition MD5	644e0e2a62b85dc2c25e7a595b173b6b
Verification MD5	644e0e2a62b85dc2c25e7a595b173b6b

Fig.24 - Acquisition and Verification MD5sums of the drive to verify integrity