Bachelor of Science with Honours in Computing Science/ Bachelor of Science with Honours in Cyber Security

COURSEWORK No. 2

Module Name : Computer Forensics FT

Module Code : CU T225 PSB501IT

Weighting : 66.7%

Due Date : 29th August 2025

SUBMITTED BY

NAME : DON LOO BOON KIAT

CU Index No. : 504EHLOC

Word Count : 2197 (1649 words for report)

Contents

INTRODUCTION 3

METHODOLOGY 4

CASE SCENARIO 6

IDENTITIES 7

EVIDENCE 9

CONCLUSION 22

TIMELINE OF EVENTS 23

APPENDIX 24

REFERENCES 26

Introduction

The forensic analysis report that will be covered will present the main findings from the case files of Washer17.E01 and Mantooth.E01. All research gathered for the report was done in a controlled environment using a virtual machine to ensure the integrity of the evidence presented.

This report highlights the key findings found on the suspect's device. This report will explain the process of uncovering the truth behind the cybercrime, the methods that were used by the culprits, the identification of the culprits and the evaluation of the extracted evidence.

Evidence materials used for the report:

S/N	File name	file type	File Creation date	file size	Hash value (MD5)
1	Mantooth17.E01	E01 File	06/03/2014	38,801kb	9AB5FE980D66B0452479321EC96D3D10
2	Washer17.E01	E01 File	06/03/2014	76,580kb	E353444DC210368A34CA571898E14EBB

Digital Tool(s) used for the report:

1. Autopsy
2. Forensics Toolkits
3. John The Ripper

Methodology

When investigating the evidence, the application of digital forensic methodologies in cybercrime investigations was applied in accordance with UK law and UK police investigations principles. The following steps were taken:

1. **Identification (Obtaining of Evidence)**

   The evidence material provided for the investigation named Washer17.E01 and Mantooth.E01, were obtained and verified with no modification. A virtual machine was then used to isolate the working space which ensures no external material will alter the evidence or affect any personal data.

2. **Tools and Techniques**

   Several tools were incorporated in this investigation to uncover and analyse the evidence file:

   - Autopsy: Used to analyse the evidence file and uncover hidden, deleted and encrypted files.
   - Forensics Toolkits (FTK): Used to enhance email discoverability and efficiently extract associated attachments.
   - John The Ripper: Used for decrypting passwords attached to protected files to access them.

3. **Analysing Data**

   The investigation commenced with the extraction of relevant data from the evidence file provided. This process includes the acquisition of emails, attachments and associated miscellaneous documents for subsequent analysis. All recovered artifacts were examined for

criminal activities with particular focus on the term of credit cards and ATMs. Files that were found to be encrypted or access-restricted were subjected to decryption procedures.

4. **Linking of Evidence**

   A comprehensive correlation of findings was conducted across diverse digital evidence sources, including email communications, file attachments and encrypted files. This diverse spread allowed for the identification of relative links between individuals and their involvement in the cybercrime. The individuals identified are as follows: Wes Mantooth, Rasco Badguy, John Washer, Skimmerman (David Thomas). These individuals exhibited behavioural patterns corresponding to the suspicious activities found in the evidence files. With the information obtained, all connections were cross-referenced to validate their associations and to identify their identity via the evidence photos found in the case file.

5. **Report and Documentation**

   All forensic findings were documented, incorporating screenshots and descriptive narratives to preserve context and support interpretation. Aligning with the best practices for forensic integrity and legal admissibility.

Case Scenario

After conducting an in-depth forensic analysis of the digital evidence contained within the files *Mantooth.E01* and *Washer17.E01*, the criminal activity uncovered is centred around a sophisticated credit card fraud operation. The primary method of execution appears to involve the strategic manipulation of ATM machines.

The investigation has identified three key individuals as the main perpetrators: Wes Mantooth, John Washer, and Rasco Badguy. Their communications reveal a calculated plan to install covert cameras and magnetic stripe readers on targeted ATMs, enabling them to capture both the physical card data and PIN entries of users.

Further analysis of the email threads indicates that the group was not operating in isolation. A fourth individual, known by the alias “Skimmerman,” was also involved in the operation. Skimmerman, later identified as David Thomas, was found to be in contact with the trio.

Identities

After scanning through the evidence file, I have managed to identify the individuals and provide photo evidence. Explanation of how the individuals were identified will be stated further into the report.

	File Name	Wes.jpg
	File Type	JPG File | .jpg
	File Owner	Mantooth.E01
	File Size	78.7KB (80,671 bytes)
	File Creation Date	Unknown
	Hash Value (MD5)	263f7296ad28e1a69a28802d3426728c
Analysis:	An image of Wes Mantooth	

	File Name	Dc5.jpg
	File Type	JPG File | .jpg
	File Owner	Washer17.E01
	File Size	443KB (454,197 bytes)
	File Creation Date	2007-08-04 09:31:58 SGT
	Hash Value (MD5)	6a990blb8950f2bff2d495c142fleefb
Analysis:	An image of Rasco Badguy	

	File Name	Dc6.jpg
	File Type	JPG File | .jpg
	File Owner	Washer.E01
	File Size	377KB (386,922 bytes)
	File Creation Date	2007-08-04 09:31:58 SGT
	Hash Value (MD5)	a005ecd81f9ee3106907cb9cf006b071
Analysis:	An image of John Washer	

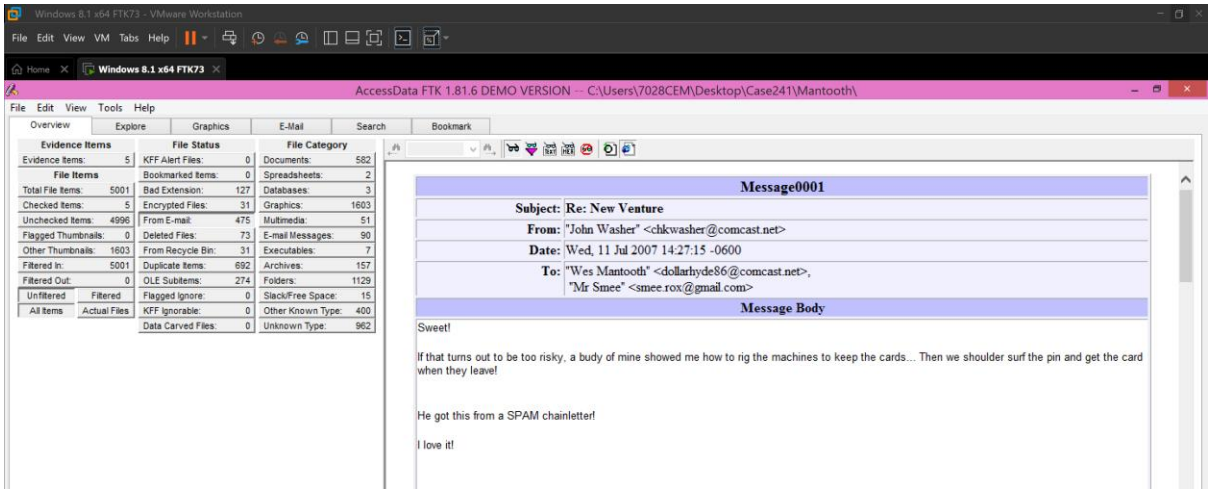
	File Name	Skimmerman Photo
	File Type	JPG File | .jpg
	File Owner	Washer17.E01
	File Size	33.8KB (34,613 bytes)
	File Creation Date	Unknown
	Hash Value (MD5)	Unknown
Analysis:	An image of Skimmerman (David Thomas)	

	File Name	Skimmerman Girlfriend Photo
	File Type	JPG File | .jpg
	File Owner	Washer17.E01
	File Size	76.6KB (78,521 bytes)
	File Creation Date	Unknown
	Hash Value (MD5)	Unknown
Analysis:	An image of Skimmerman's Girlfriend	

Evidence

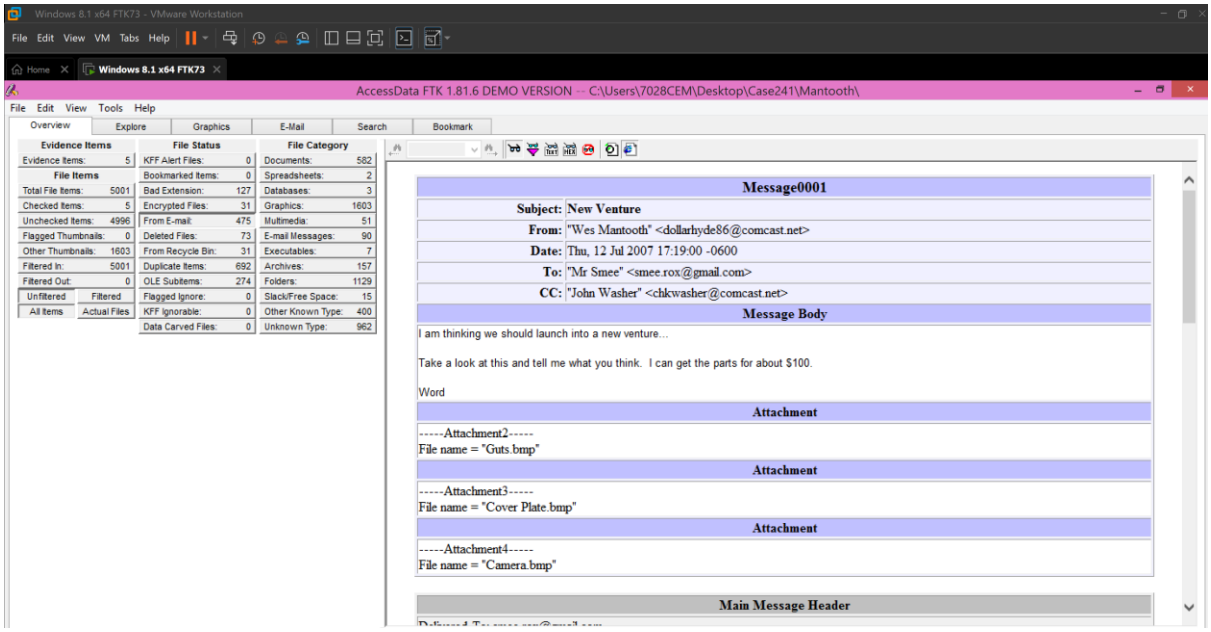
This segment of the report will cover and present the findings through a series of screenshots and images related to the crime. The report will detail the events leading up to the fraudulent activities and the actions taken during the crime.

Firstly, the image “Screenshot 1” of the email below dated 11st July 2007, is what I believe to be the starting point of the communication between the culprits for the beginning of the plotting for the credit card fraud.



*Screenshot 1

Referring to the follow up email “Screenshot 2” below dated 12nd July 2007, the key method of their plan was introduced. Listed as attachments in the email are Gut.bmp, Cover Plate.bmp and Camera.bmp. analysing the images will give a rough understanding of the method they were going to employ to perform their credit card fraud.



*Screenshot 2

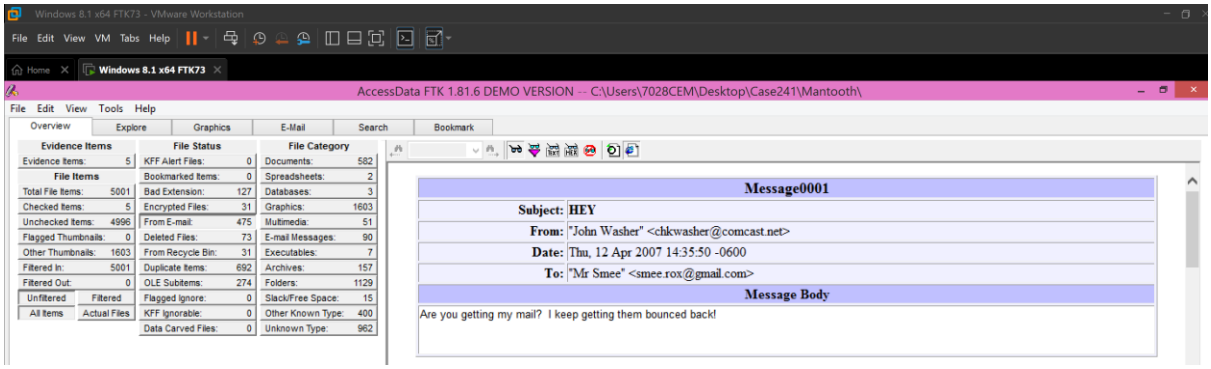
Referring below are the 3 images extracted from the email above. From my understanding, the plan would involve installing a covert camera as seen in ***image A*** and magnetic stripe readers as seen on ***image B and C*** on targeted ATMs, enabling them to capture both the physical card data and PIN entries of users.

	File Name	Camera.bmp
	File Type	BMP File | .bmp
	File Owner	Mantooth.E01
	File Size	366KB (375,030 bytes)
	File Creation Date	Unknown
	Hash Value (MD5)	c708c59b9db8007983a03fead10b3898
Analysis:	Image A	

	File Name	Guts.bmp
	File Type	BMP File | .bmp
	File Owner	Mantooth.E01
	File Size	411KB (421,878 bytes)
	File Creation Date	Unknown
	Hash Value (MD5)	56a0856e955784f8332a8affd1a2a4cf
Analysis:	Image B	

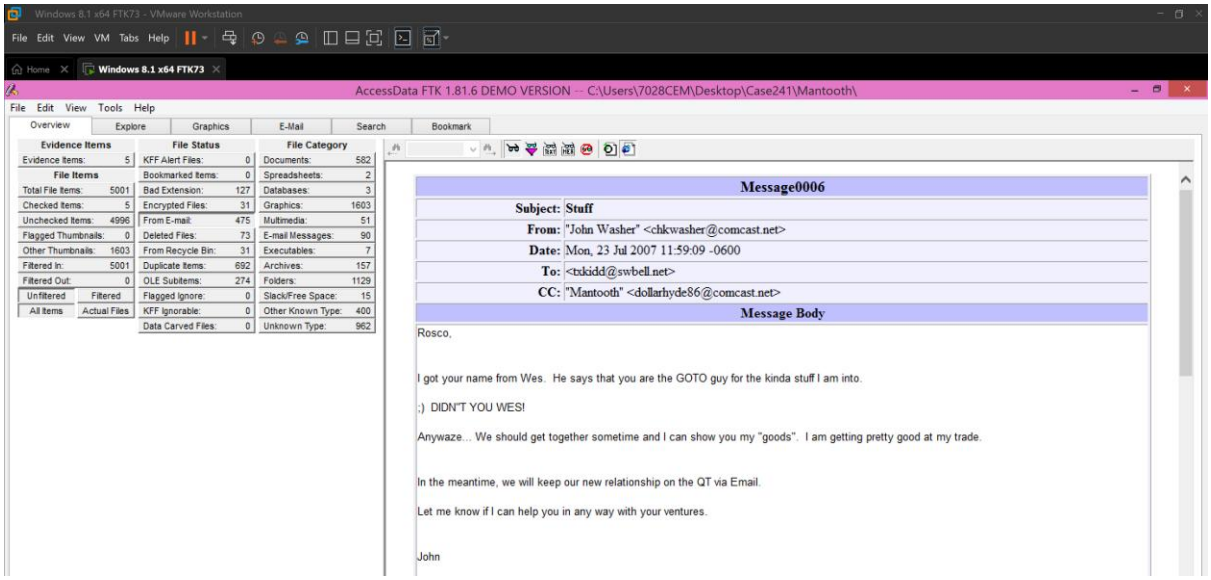
	File Name	Cover Plate.bmp
	File Type	BMP File | .bmp
	File Owner	Mantooth.E01
	File Size	397KB (406,854 bytes)
	File Creation Date	Unknown
	Hash Value (MD5)	989d320c9a9b13f197c98156935b7fb9
Analysis:	Image C	

Circling back to the email labelled “Screenshot 3”, it was sent to a “Mr Smee” whose identity is still unknown. Referring to the email below dated 12th April 2007 will show that John Washer had lost contact with Mr Smee awhile back resulting in him being excluded from future emails.



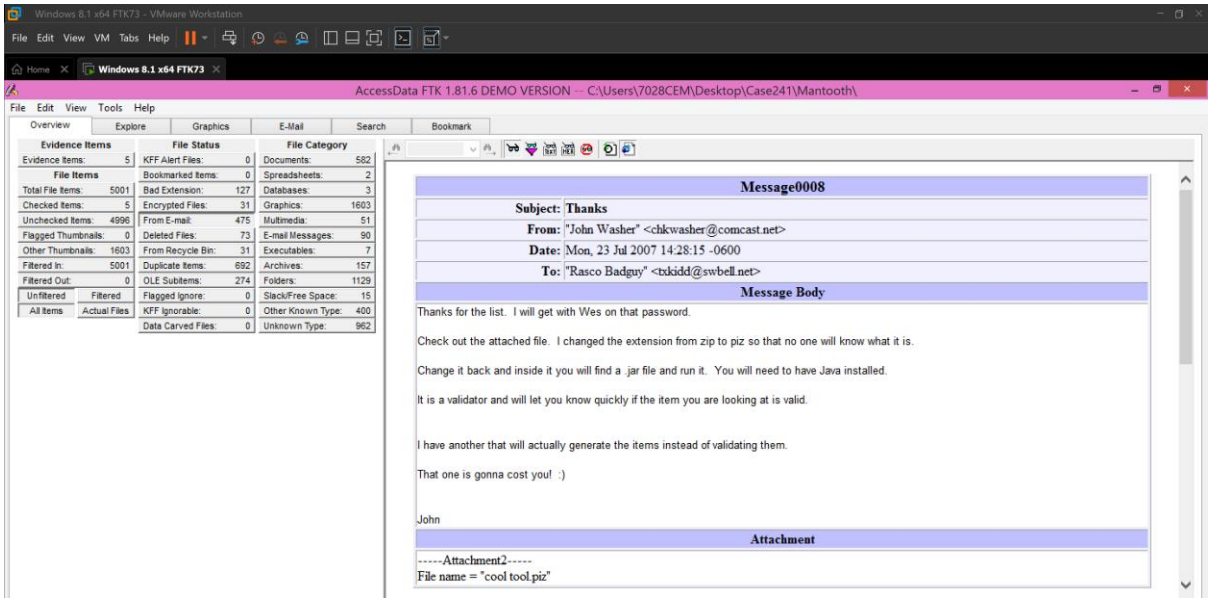
*Screenshot 3

This in turn got John Washer and Wes Mantooth to search for another accomplice to aid them in the fraud. Referring to the email below “Screenshot 4” dated 23rd July 2007, it is shown that Wes Mantooth had recommended Rasco Badguy to John Washer.



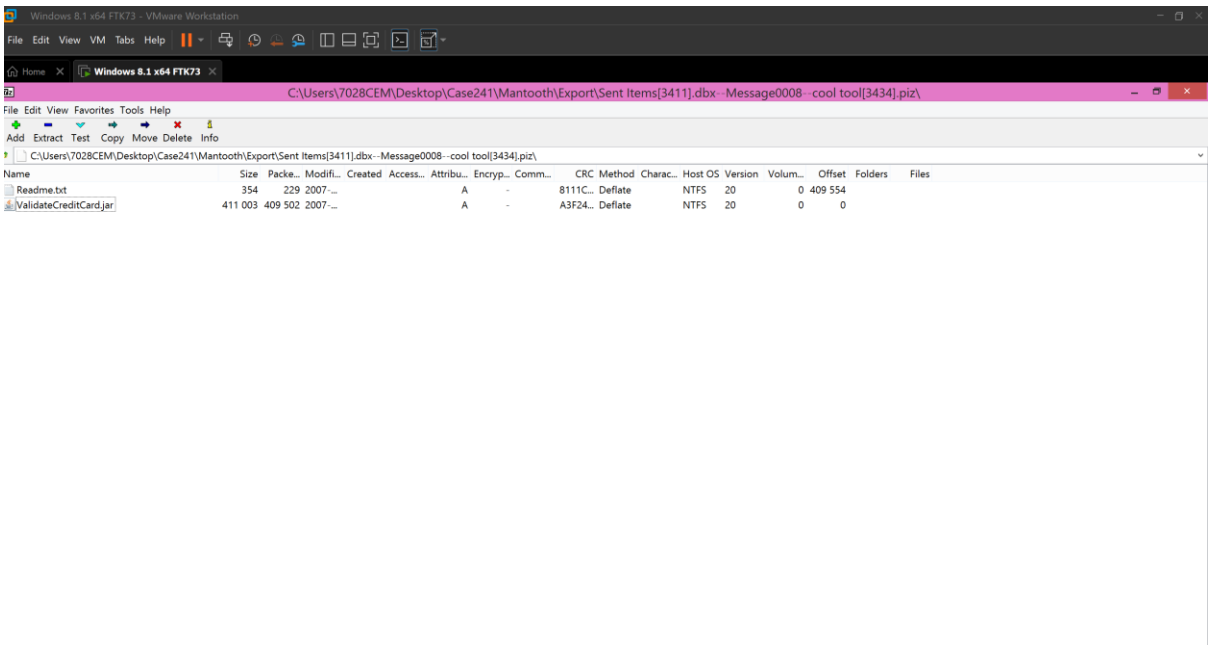
*Screenshot 4

After the introduction of Rasco Badguy, he proceeded to share a file in an email dated “Screenshot 5” on 23rd July 2007. The file named “cool tool.piz”.



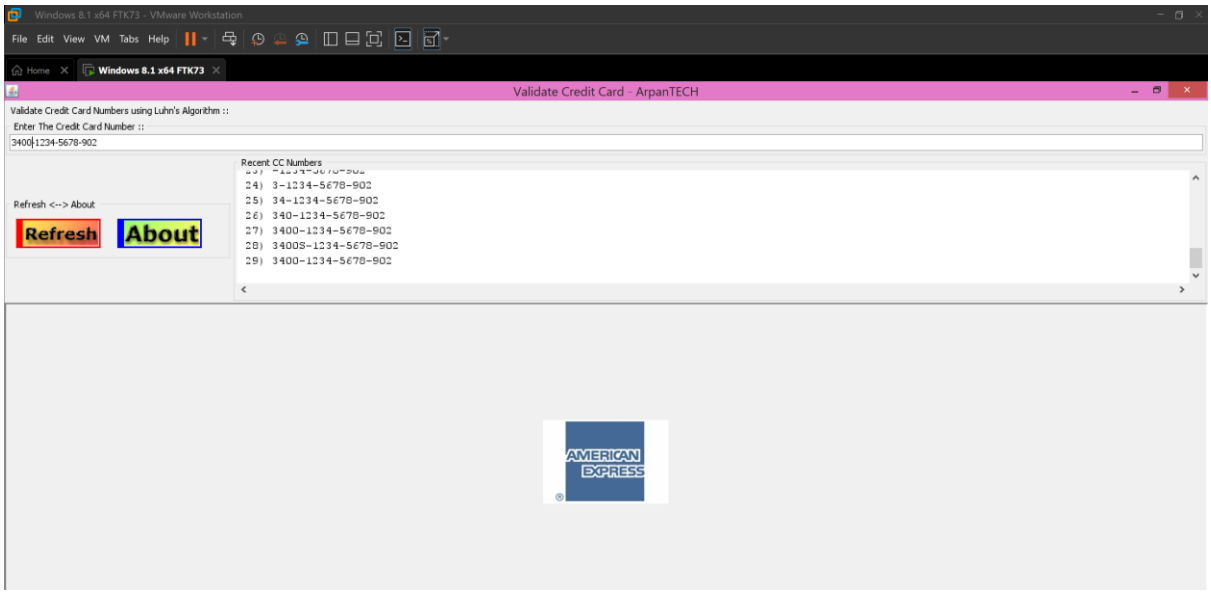
*Screenshot 5

Opening the zip file “Screenshot 6 and 7” will grant access to the “ValidateCreditCard” application.



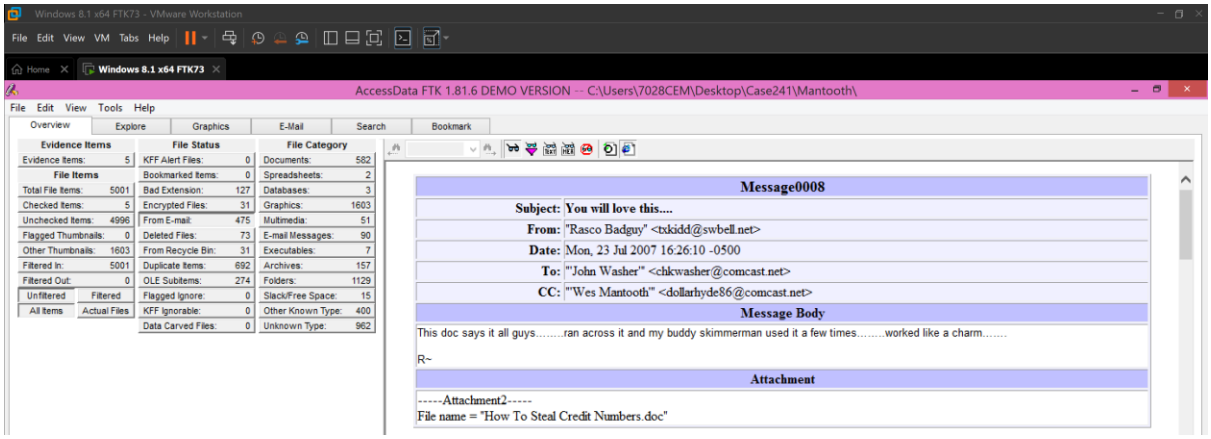
*Screenshot 6

The application main purpose is to validate credit card numbers.



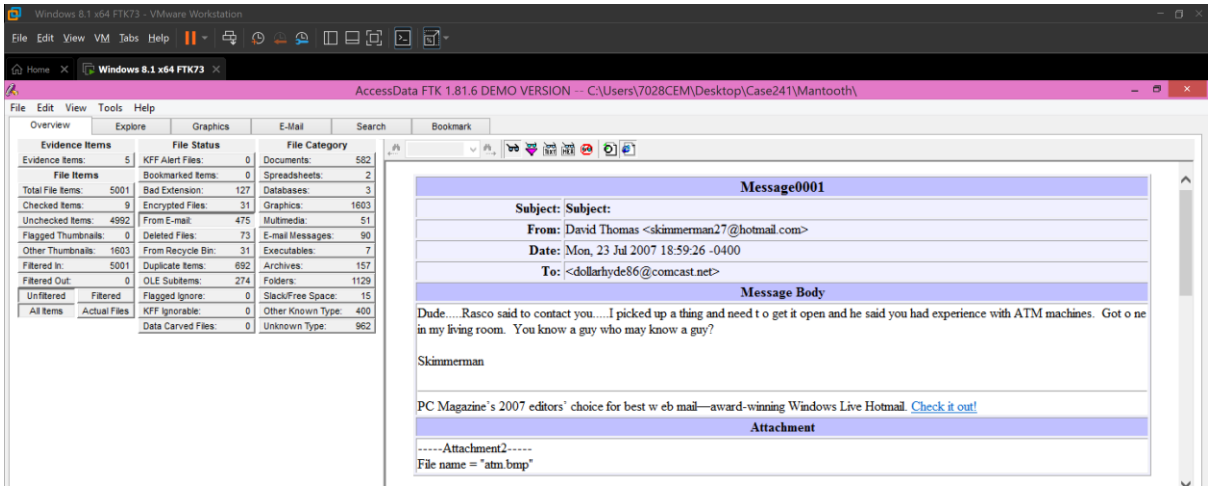
*Screenshot 7

Referring to the screenshot below “Screenshot 8” will show an email dated 23rd July 2007, the contents of the email is mainly about the attached file. Additionally, this is also the first mention of David Thomas aka skimmerman.



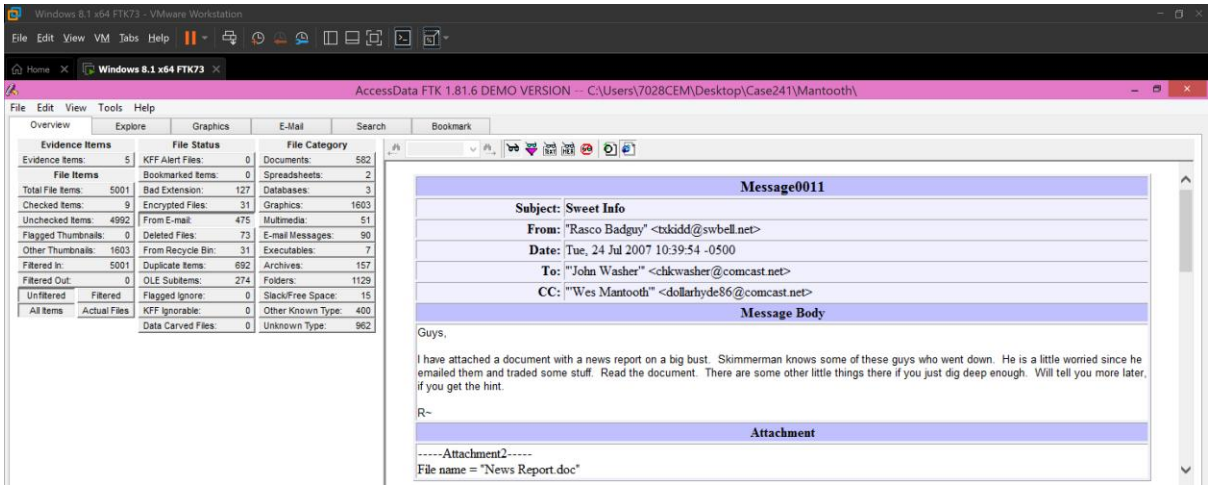
*Screenshot 8

David Thomas (Skimmerman) then seeked help from Wes Mantooth “Screenshot 9” pertaining to an ATM machine which he had obtained and needed help with.



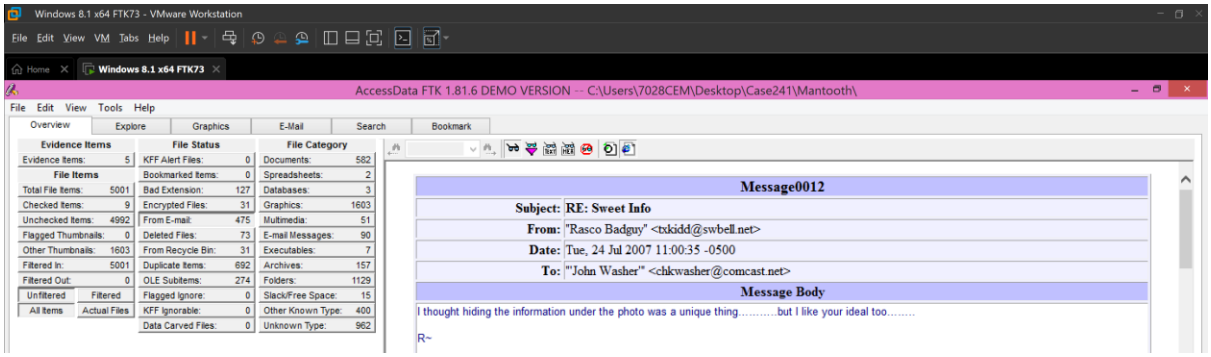
*Screenshot 9

The next email thread “Screenshot 10” listed below dated 24th July 2007, shows Rasco Badguy linking an attachment which describes the “big bust” incident.



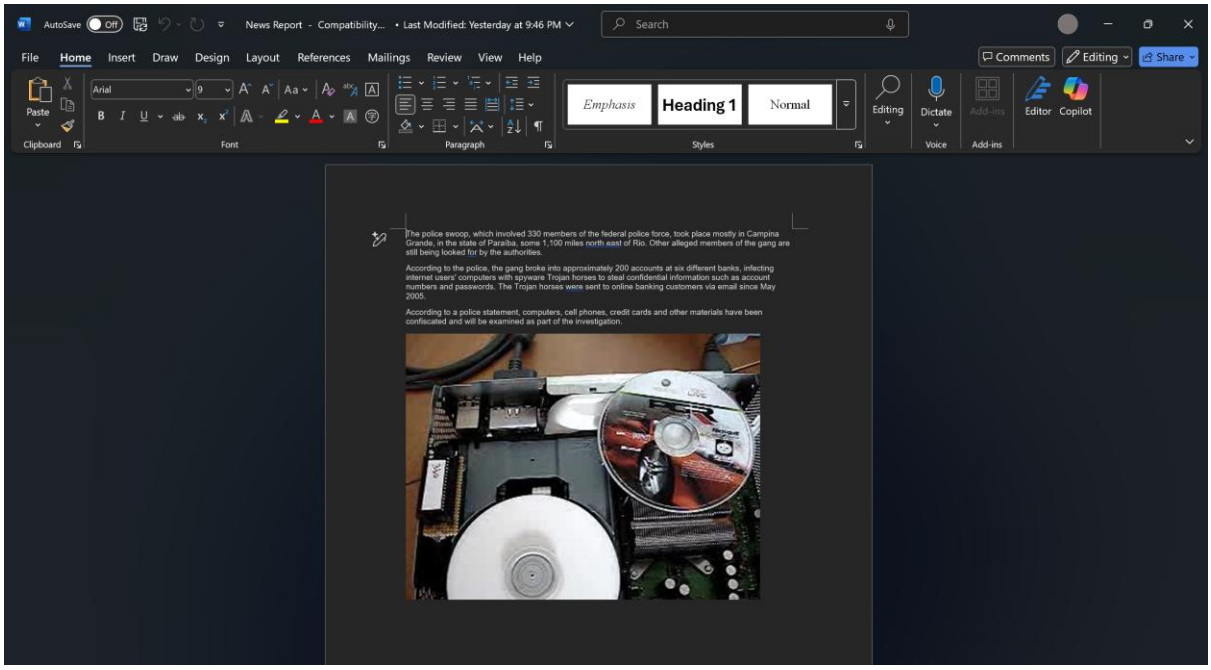
*Screenshot 10

Opening the document shows nothing out of the ordinary at first glance, however an email “Screenshot 11” dated on the same day 24th July 2007 states that moving the photo will reveal some hidden texts underneath.

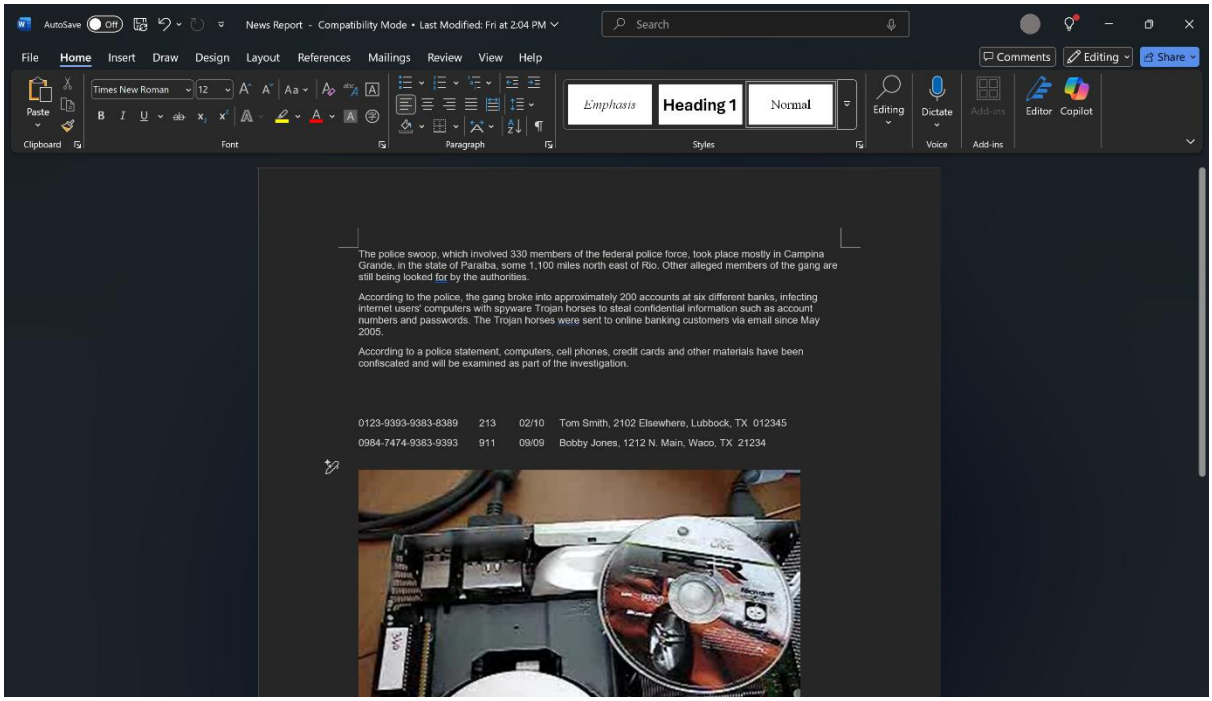


*Screenshot 11

Referring to the 2 screenshots “Screenshot 12 and 13”, it is shown the before and after of moving the image. Moving it reveals 2 sets of credit card information that belongs to a “Tom Smith” and “Bobby Jones”.

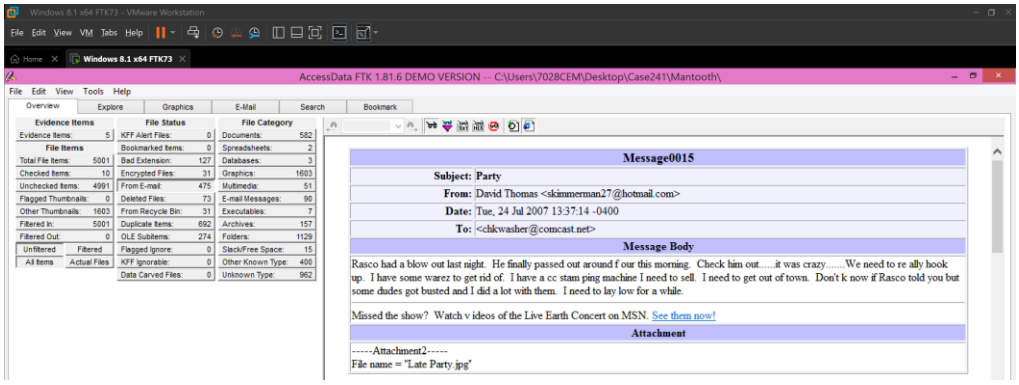


*Screenshot 12

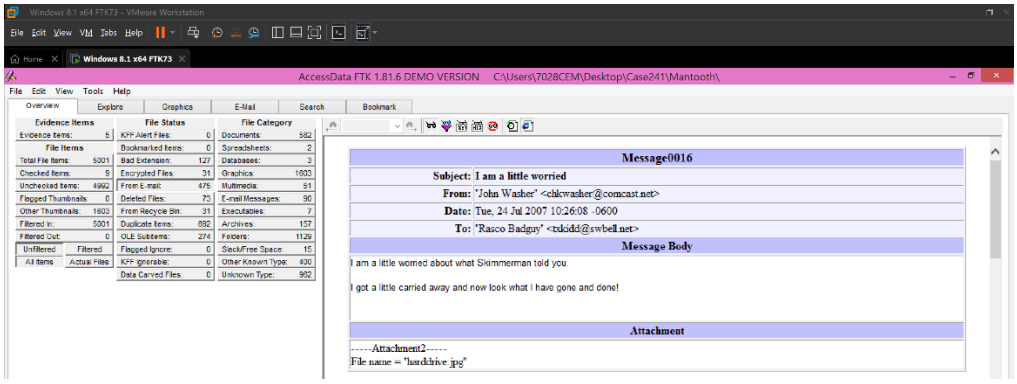


*Screenshot 13

It is to note that in the news article above, the content led me to the conclusion for the emails listed below “Screenshot 14 and 15” dated 24th July 2007, on why John Washer was afraid and was seen trying to get rid of his hard disk by physically destroying it. He was afraid of being traced for being in communication with David Thomas (Skimmerman).



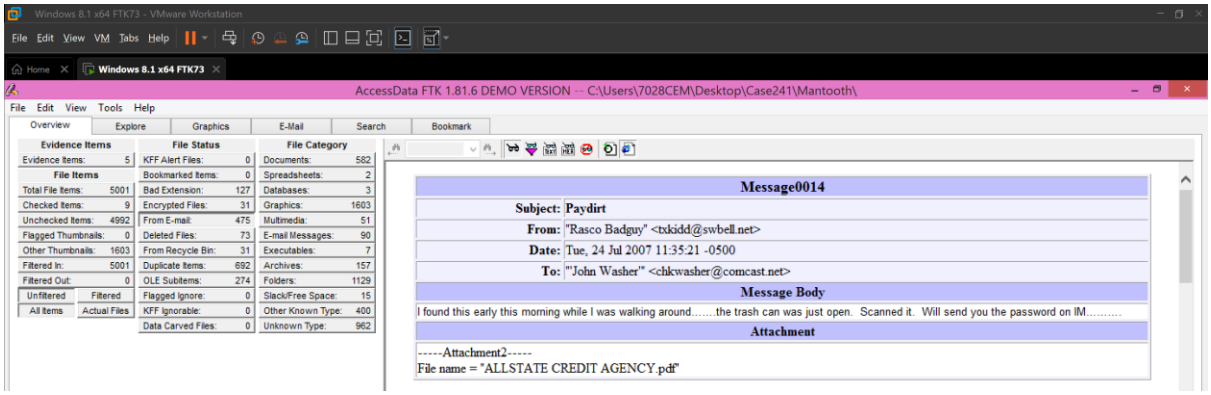
*Screenshot 14



*Screenshot 15

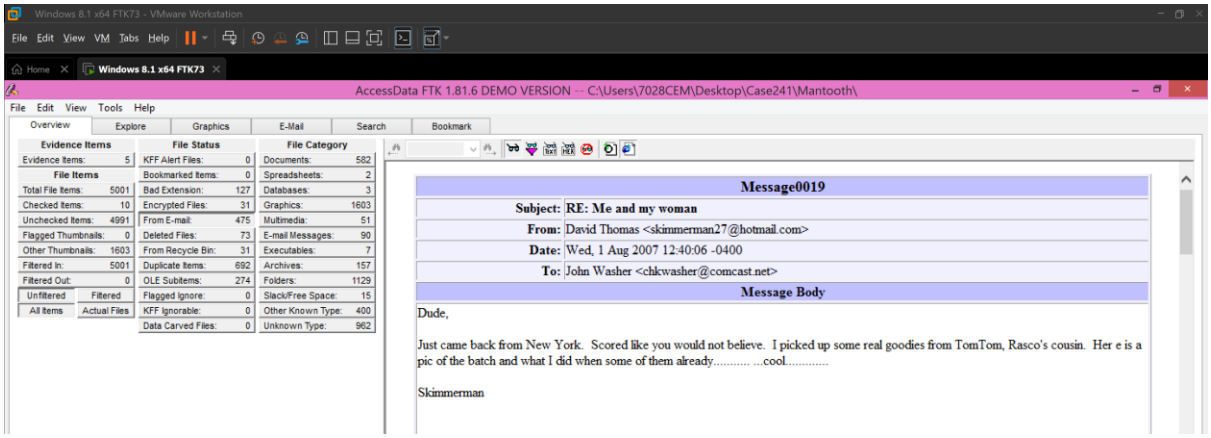
	File Name	harddrive.jpg
	File Type	JPG File | .jpg
	File Owner	Washer17.E01
	File Size	551KB (564,356 bytes)
	File Creation Date	Unknown
	Hash Value (MD5)	Unknown
Analysis:	John Washer’s Destroyed Hard Drive	

Next up is an email “Screenshot 16” dated 24th July 2007, the contents of the email is a file which reads “ALLSTATE CREDIT AGENCY.pdf”. Unfortunately, I am unable to decrypt this file.



*Screenshot 16

Here’s an email “Screenshot 17” dated 1st August 2007, which states that Skimmerman brought back some “goodies”. After opening the attachment, it is shown that said “goodies” were blank cards and stolen credit cards.

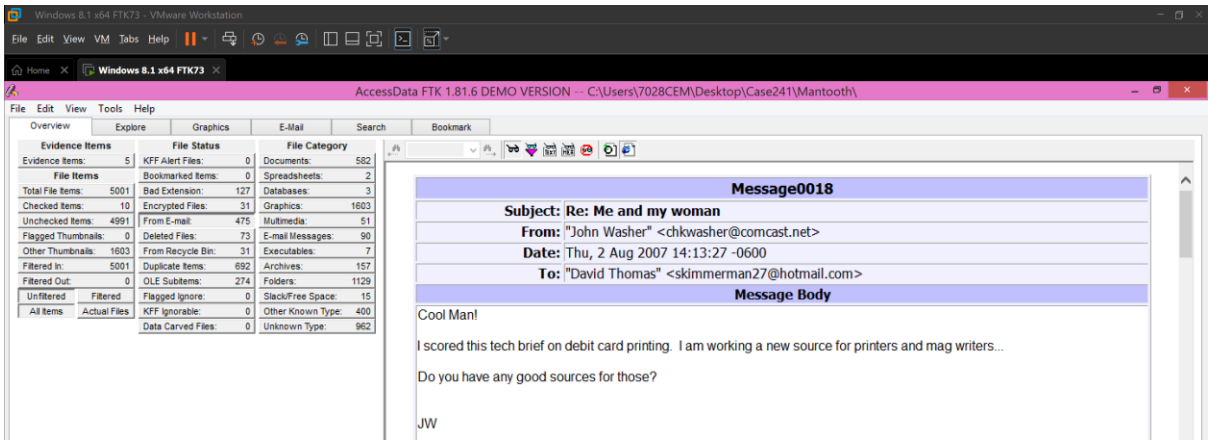


*Screenshot 17

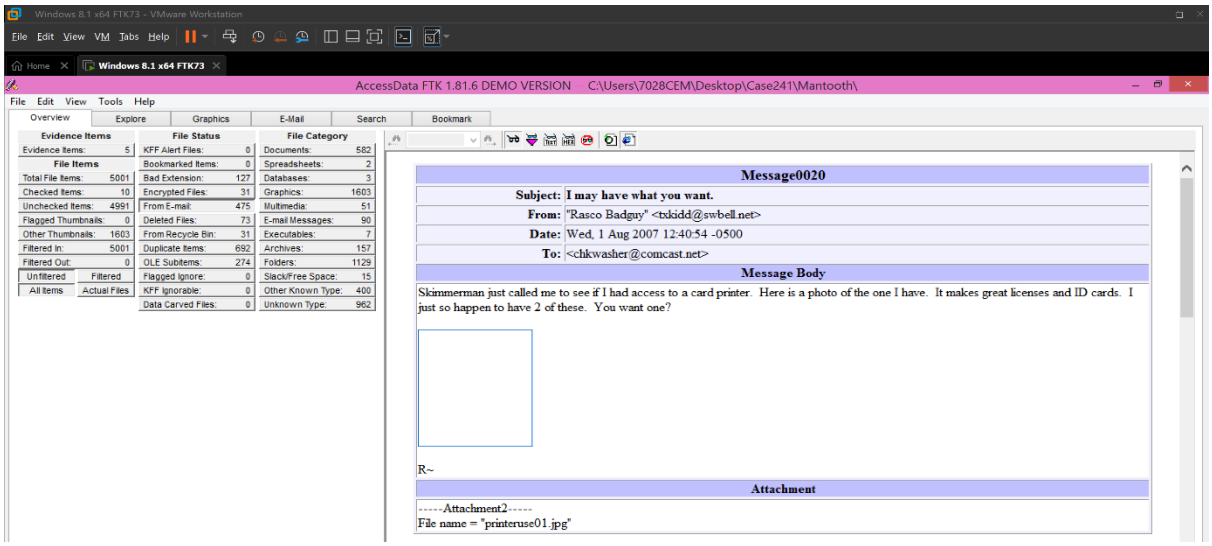
	File Name	blank-cards-250.jpg
	File Type	JPG File | .jpg
	File Owner	Washer17.E01
	File Size	7KB (7,168 bytes)
	File Creation Date	Unknown
	Hash Value (MD5)	Unknown
Analysis:	Blanks cards brought back from NYC by Skimmerman	

	File Name	See what I did.jpg
	File Type	JPG File | .jpg
	File Owner	Washer17.E01
	File Size	18.5KB (18,944 bytes)
	File Creation Date	Unknown
	Hash Value (MD5)	Unknown
Analysis:	Stolen credit cards from NYC by Skimmerman	

Afterwards, David Thomas (Skimmerman) can be seen asking Rasco Badguy “Screenshot 18 and 19” about a card printing machine. Armed with the newly obtained blank cards, this would be where the start of the credit card printing began.



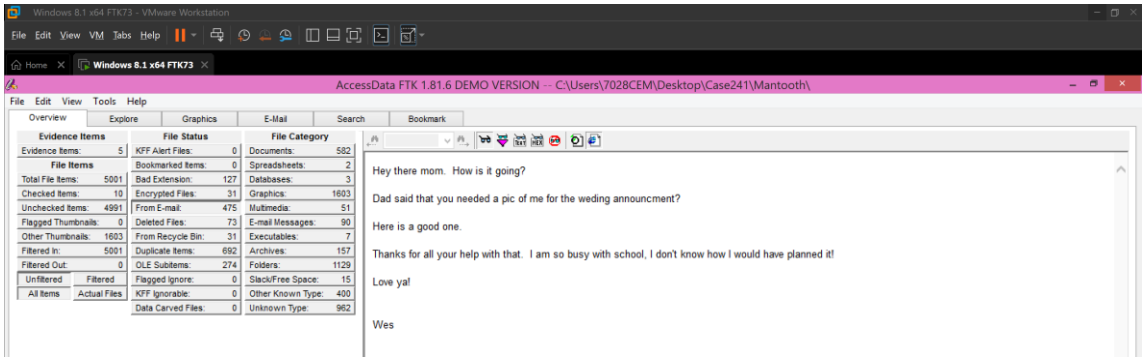
*Screenshot 18



*Screenshot 19

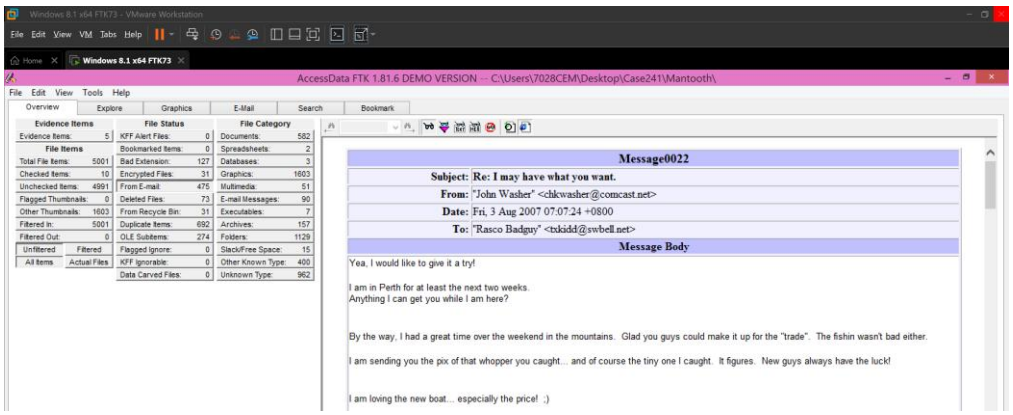
	File Name	printeruse01.jpg
	File Type	JPG File | .jpg
	File Owner	Washer17.E01
	File Size	1.48KB (1,519 bytes)
	File Creation Date	Unknown
	Hash Value (MD5)	Unknown
Analysis:	Rasco Badguy's credit card printing machine	

Lastly, I will now go over how I was able to identify the individuals who were involved in the case. Firstly, for Wes Mantooth, an image file titled "Wes" was believed to be Wes not only due to the file name, but the context of why the file was needed as it was supposedly sent to Wes's mother for a wedding announcement "Screenshot 20".



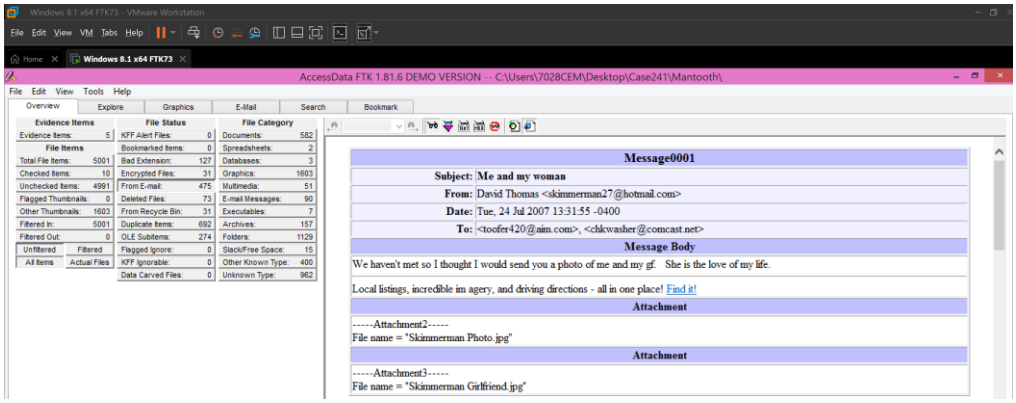
*Screenshot 19

Secondly, for John Washer and Rasco Badguy, an email "Screenshot 20" describes John going on a trip to Perth, however continuing to read the email. One sentence says, "I am sending you the pix of that whopper you caught… and of course the tiny one I caught." Circling back to the images presented earlier in the report, the "whopper" and "tiny" ones refer to fishes that the 2 men can clearly be seen carrying.



*Screenshot 20

Lastly, for David Thomas (Skimmerman) and his girlfriend, an email “Screenshot 21” describes Skimmerman sending two images, one of himself and one of his girlfriend’s.



*Screenshot 21

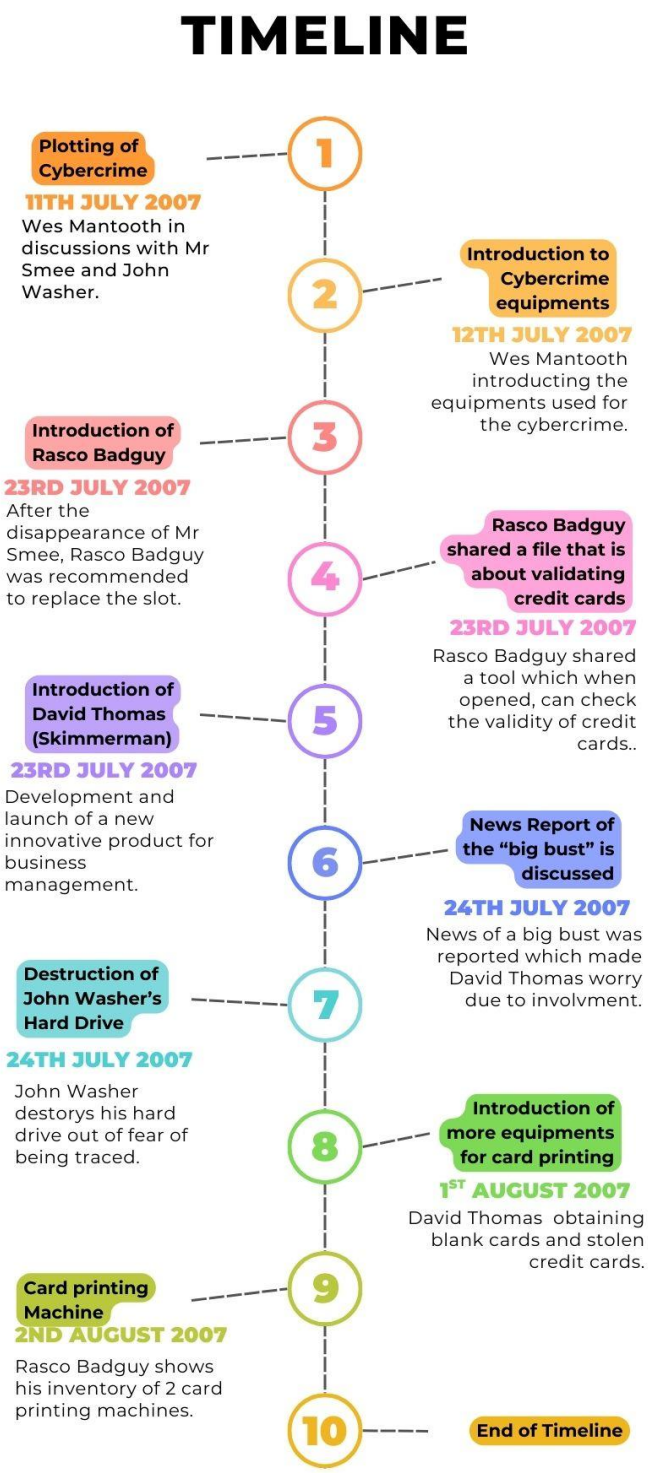
Conclusion

Following a comprehensive examination of the available digital evidence, including all recovered email communications and image files. I have concluded the evidence collection phase for this case. Based on the findings, the cybercrime uncovered is about credit card fraud. The individuals identified are as follows, John Washer, Wes Mantooth, Rasco Badguy and David Thomas, also known by the alias “Skimmerman”. These names emerged repeatedly across multiple sources of evidence, with corroborating indicators linking them to the orchestration and execution of the illicit activities.

It became apparent that John Washer engaged in deliberate attempts to obstruct forensic analysis. Specifically, he sought to eliminate incriminating data by physically destroying his personal hard drive. This act of evidence tampering was likely intended to hinder investigative efforts and conceal digital traces of his involvement. Notably, the compromised storage device was found to contain several encrypted files, suggesting the presence of sensitive or potentially incriminating information that he intended to keep inaccessible.

Thus, some evidence couldn’t be analysed in this report due to strong file encryption.

Timeline Of Events



Appendix

Property Record Number: _____

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: 241_____ Offense: Credit Card Fraud_____
Submitting Officer: (Name/ID#)
Don_____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)
1	1	Hard Disk (Mantooth.E01)
1	1	Hard Disk (Washer17.E01)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**
1	21 Aug'25	**Don**		Seized
2	22 Aug'25	**Don**	**Alice**	Disk Image (FTK)
3	23 Aug'25	**Alice**	**Martin**	Analysis (Autopsy)
4	24 Aug'25	**Martin**	**Luis**	Report
5	25 Aug'25	**Luis**	**Don**	Report

PE003_v.1 (12/2012) Page 1 of 2 pages (See bac

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers*. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM

(Continued)

Final Disposal Authority

Authorization for Disposal

Item(s) #: _____ on this document pertaining to (suspect): _____
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

☐ Return to Owner ☐ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: _____ Signature: _____Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ID#:_____ in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian _____ID#:_____ to
Name _____
Address: _____ City: _____State: _____ Zip Code: _____
Telephone Number: (____) _____
Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: _____ Date: _____

Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers*. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

References

Articles:

- What is the Chain of Custody
- Police and Criminal Evidence Act 1984
- 5 Stages of Digital Forensics Investigation
- John the Ripper Password Cracker
- Importance of Timeline in a Forensic Investigation
- How to find MD5 hash in Windows Powershell