Greater Omorose(

Section 1

Introduction

The investigation aims to gather evidence related to the armed robbery at West Monkseaton Post Office on 30th November 2016 to identify those responsible, their motivation, and plan.

Background information:

On the 30th of November, there was an armed robbery at West Monkseaton Post Office. Witnesses saw two individuals fleeing in a black car with the license plate NY54 KSO. After gaining photographic evidence of the car, police were led to Mr. Alan Redmond who was the last known owner of the car. Mr Redmond provided the details of the individuals who purchased the vehicle, leading to the identification of Mr. Lewis Scott, Mr. Carl Brown, and Mr. Eddie Young.

Scope and Limitations

Our investigation will focus on examining Mr. Scott's iPhone 4s,and his computer. I will analyse text messages, calls, images, videos, files, and web history.

The possible limitations in this investigation are:

- Difficulty in reconstructing deleted files, especially if secure deletion methods or special software were used.
- The forensic analysis must adhere to legal requirements and ethical standards, this may restrict the methods and extent of the examination, particularly regarding privacy concerns and the handling of sensitive or privileged information.
- The suspect might have used encryption software to hide his activity.
- Not all incriminated devices used by the suspects might have been collected by the police.
- The suspects were not captured immediately after the robbery, so they probably had enough time to conceal or destroy evidence.

Methodology

For this investigation I used Autopsy version 4.20.0, which is a digital forensics tool. I used Autopsy because its key functionalities such as metadata extraction, file analysis, keyword search, artifact analysis, and hash analysis allow investigators to find, document, and present findings in the juridical process. These functionalities enabled me to efficiently identify relevant evidence, and reconstruct the sequence of events leading up to the robbery.
During the investigation, I tagged evidence related to the robbery and examined internet history and search queries to uncover online research conducted by the suspect.
The logical phone extraction method recovered deleted files from Mr. Scott's iPhone 4s, revealing insights into his communications with accomplices.

Findings

The hard disk model is ST380215AS ATA, with Windows 7 Enterprise Service Pack 1 installed on 2016/10/4 at 10:44. The primary user accounts are "Student" and "Lewis Scott". Additionally, the system time zone is GMT, with a standard time bias of BST. Furthermore, I discovered that an iPhone 4s was connected to the computer on 2016-11-22 and this matches the phone model that has been confiscated by the police. The user account named Lewis Scott and the connection to the iPhone 4s and the time zone GMT, which suggests that it was likely used in the UK, suggests Lewis Scott's awareness of the computer's existence. Moreover, a M3 Portable

Hard Drive 1TB was connected on December 5th, 2016, potentially containing valuable evidence yet to be confiscated by the police.

Files

During the forensic investigation, it was discovered that Tor Browser, an anonymizing browser, was installed and accessed on Lewis Scott's computer on 2016-10-19 at 16:55:27. His familiarity with the software is evident from a custom jump list on Tor browser, indicating that he manually pinned the file to the start menu. Additionally, his search history includes queries about Tor browser and its benefits, demonstrating at least a basic understanding of the software's functions.

This use of Tor Browser can be indicative of Lewis Scott's attempts to conceal his online research, communications, or other activities related to the planning or execution of the robbery. It raises questions about what specific activities he was trying to hide and emphasizes the significance of further investigation into encrypted or hidden data and communications.

According to the report brief, a suspicious individual was caught on the CCTV while they were taking photos of the post office, and during my investigation on the computer, I found suspicious photos of the post office (interior and exterior including CCTV location) taken on 2016-11-21. This post office matched the location of the robbery, so this indicates that there was premeditation by Mr. Scott. He later then accessed these pictures; this is evident from the thumb caches found on his computer.

In the recycle bin, I recovered a PNG file and a password-protected docx file named "Master Plan”. The PNG contained the image of a car listed for 1,650 pounds. Mr. Scott knew this file's existence because he attempted to delete them, furthermore, I was able to find the thumb cache of this PNG as well which confirms that he opened these images. Mr. Scott had knowledge of the Master Plan.docx this is evident from the automatic jump list found, he also intentionally locked the document with a password. I know that he intentionally locked it because, in his browsing history, I found searches (2016-10-11) on ‘ways to password protect a document on Word’.

While examining the phone image I discovered a note(figure24) containing the password for the master plan.docx:’LewisMasterPlan2580’. He knew about the password because he searched for ways to encrypt notes(figure26)

Upon accessing Master plan.docx, I found out a lot:

- Firstly, it mentioned that the gateway vehicle was a BMW 7 series 740i e38 located in Queensbury BD13 in Bradford. This matches the description of the car found in the recycle bin and the black estate car captured on camera.
- Secondly, it mentions about buying fake number plates online. By checking the cookies and web history I found visits to numbe1plates.com, Demonplates.com, Proplates.co.uk,and Platecreator.com on 2016-11-02.
- Thirdly, the document said that they were targeting West Monkseaton Post Office and there were pictures from Google Maps showing its area. This is the same post office that got robbed on 30/11/2016.
- I found web links of equipment that could be linked to the robbery like a 3-hole balaclava, curved claw hammer, handguns, and a duffle bag. Lewis Scott knew about these because they were in his web history. This web links were also in a document called Gear.docx. Lewis Scott accessed Gear.docx because I found an automatic jump list.
- Lastly, it had a code to open the safe, and a map showing the post office layout, e.g. CCTV location etch. The document mentioned that the robbery was going to happen on 30/11/2016. Since the last time that Master plan.docx was opened was on 2016-11-25,

and the robbery date matches the actual robbery date, these show signs of premeditation by Lewis Scott.

In a folder labeled ‘Possible cars’ there are 4 images taken from Google Maps showing Low Lane Bradford BD13, Queensbury. If this matches Mr. Alan Redmon's address, then it could suggest that Lewis Scott engaged in the purchase of the black estate vehicle. Lewis Scott accessed the ‘Possible Cars’ folder because there is an automatic jump list to this folder and I also found thumb caches of the images in the folder. Within the ‘possible cars’ folder, I found another folder named ‘get rid of car loc’ that contains images that suggest plans to dispose of the car. Lewis Scott knew about this file because there is an automatic jump list that was created, and I found thumb caches of the pictures that are within this. Police can investigate these locations for the getaway car.
I found another document named ‘Potential Location.docx’ that shows post offices in Newcastle, Gateshead, and Whitley Bay including the West Monkseaton Post Office. Lewis Scott knew about this file because there is an automatic jump list to this docx file. There is another file called Doc1.docx that displays a loan screenshot from paydayluk.co.uk for £600. If the loan was signed by Lewis Scott, this could help police investigations because the Master Plan mentions taking a loan for the car.

Lastly, 'presentation1.pptx' contains a hate message towards Royal Mail. The presentation had a Royal Mail logo and a bin which were separated by the sentence ‘Should be,’ altogether this should mean ‘Royal Mail should be binned/trashed’. Lewis Scott knew about presentation 1.pptx because there is an automatic jump list that was created for this file and all the pictures I found in this file, are in the thumb cache as well.

In other findings, I discovered images of a machete on knifecentre.com and another image showing a total price of £35.94 for the machete. Additionally, I then found a video in which someone is recording himself burning the Royal Mail Logo while crying. The setting appears to be a garage, possibly belonging to Lewis Scott or his accomplice, as voices can be heard in the background, indicating at least two individuals present. Lewis Scott knew of this file because I found them in the thumb cache.
I found out that Lewis was looking for jobs, CV templates, ways to make money fast illegally, and articles on shop robbery. These searches show his desire to make quick money. Lastly, he searched for ‘People who hate Royal Mail’ and other hate content towards Royal Mail.

In the phone investigation, I found that Lewis Scott's phone number is +447564251570, along with Google searches regarding post offices in Newcastle, Whitley Bay, and South Shield on 17/11/2016(figure25). I found search queries on machete, ‘sacked from work getting them back’, ‘how to make money fast illegally’, and ‘Unfair dismissal’(figure22,23).
Contacts for Eddie Young and Carl Brown were also recovered, with Lewis saving Eddie Young's number as 'Youngy' and Carl Brown's as 'Carl' and their phone number are +447939968834 and +447564251569 respectively(figure3). Furthermore, Mr. Scott is friend with Mr. Brown and Carl on Facebook messager(figure1)(figure2). These informations imply that Lewis Scott knew about Mr. Young and Brown.
On 08/11/2016, I found out that ‘Youngy’ sent a message containing web links(figure4) to equipment which are the same as the web links I found in Gear.docx.
There was a group chat on Viber in which the participants were Mr Scott, Young, and Brown(figure3). This group chat gave me valuable information, for example in a message on 11/11/2016 'Youngy' called Lewis Scott the leader of their plans, with Carl saying he would join as long as he didn't get caught(figure5). Then, on 17/11/2016, they discussed future plans, and Lewis hinted they might attract police attention(figure6), suggesting they were up to no good. On

22/11/2016 'Youngy' mentioned 'Ami', confirming her involvement in the robbery(figure7) and giving them inside info, like floor plans and codes(figure8)(figure10). Facebook chats on 23/11/2016 showed that Lewis and Ami were romantically involved(figure9), and Ami admitted to helping Lewis and his friends(figure8). Furthermore, on 30/11/2016 there was a chat in which Ami confessed to leaving the exit door intentionally open on the day of the robbery for MR Scott and his accomplices(figure9). On 21/11/2016, Lewis admitted to taking photos of the building and CCTV(figure11), and later that day Carl sent pictures of where they could dump the car(figure12). These are the same pictures that I found on Lewis's computer file named 'potential location.docx'. Messages between Mr. Brown and Scott on 10/10/2016 showed Lewis talking about getting fired(figure13) from Royal Mail and hating the company. The reason he got fired, was because he did not wear a seat belt correctly(figure14). I also found messages in which Lewis's Mom reminded Mr. Scott that he still owes money to his grandpa(figure15)(figure16), and Carl talked about his money problems and wanting to spoil his kids. 'Youngy' agreed to join the plan on 18/10/2016, after Lewis convinced him that they could make easy money together(figure17). While investigating Scott's gallery. I found the same images I found on the computer, like the image of a machete, car dumping spots, and a Royal Mail video in which the logo is getting burned. I also found a lot of screenshots of job applications(figure18,19,20,21,).

Timeline Reconstruction

1. **10/10/2016:** Lewis Scott got fired from work, he then discusses his hate for Royal Mail with Carl Brown, and since he is in debt to his Grandpa he begins searching for jobs but soon looks for quick money-making schemes out of desperation.
2. **Mid-October-2016:** Mr. Brown is also desperate for money, and Mr. Young expresses interest in making easy money.
3. **Between October/November 2016:** Mr Scott, Brown, and Young formed a partnership and they started planning a robbery and identified West Monkseaton Post Office as their target. They begin searching for equipment needed for the robbery, such as hammers and guns, as documented in Gear.docx.
4. **Mid-November-2016:** They searched for a getaway car and locations to dispose of it after the robbery. They also secured a £600 loan to purchase the car.
5. **Late-November-2016:** With the help of insider Ami Louise, they obtained the safe code and layout of the post office.
6. **30/11/2016:** Scott, Young, and Brown executed the robbery at West Monkseaton Post Office, using the information and resources gathered during their preparation (Master plan.docx).

Potential Leads

- Locate the getaway car using the "location" I found in "get rid of car loc" folder.
- Track down Ami Louise to understand her involvement and gather a confession.
- Investigate the loan source (paydayluk.co.uk) used to purchase the car.
- Find M3 Portable Hard Drive 1TB.

The digital forensic analysis of Lewis Scott's devices provided significant evidence to support the investigation of the robbery. Incriminating documents like "Master Plan.docx" and message exchanges reveal that the device owner participated in the occurred events.

Section 2

This report aims to inform small businesses about possible cyber threats and possible mitigations. In my forensic investigation, two key themes emerged that facilitated Mr. Scott and his accomplices in executing a well-organized robbery: Insider help and OSINT.

The insider provided Mr. Scott with access to the floor plan and safe code, and on the day of the robbery, she intentionally left the door open for him and his accomplices. Based on the evidence I found earlier, Mr Scott performed passive reconnaissance. I know this because I found that he searched for the targeted post office on Google Maps and he did annotations of external areas to identify potential escape routes. Not only he performed passive reconnaissance but he also performed active reconnaissance by taking pictures of both the exterior and interior of the building, including the locations of CCTV cameras. the insider's actions and Mr. Scott's use of OSINT demonstrated how these vulnerabilities can be exploited to plan and execute criminal activities effectively on unprotected businesses. Unfortunately small/medium businesses have a limited budget, for these reasons they are vulnerable because they are not able to mitigate these risk effectively

Insider attack

Insider threats can be referred as malicious activities originating from individuals within an organization, to intentionally harm or compromise the organization's data, system, or operations. According to a 2020 global report [3, p.1], the average worldwide cost of insider threats increased by 31% over the past two years to $11.45 million, with incidents rising by 47% during that time. A 2018 survey by, the U.S. State of Cybercrime Survey indicates that 25% of cyberattacks are committed by insiders and 30% of people who replied to the survey indicated that incidents caused by insider attacks are more costly and damaging than outsider attacks [1, p.1]. Unfortunately, businesses frequently overlook protection against insider threats. For example, in the case of the post office robbery mentioned earlier, the establishment had CCTVs and safes to safeguard its assets. However, due to a lack of protection to prevent insider attacks, Mr. Scott was able to exploit this vulnerability and successfully carry out the robbery. Many other businesses employ similar security measures without adequate protection against insider threats, which makes them highly susceptible to such attacks. Insiders may have different goals but the most common objectives are fraud, sabotage of infrastructure, and theft of IP[3,p.4]:

- Inside fraud: This occurs when the insider is motivated by financial goals. This type of attacker can cause huge damage to small/medium organizations, financially, and reputation-wise, because it can discourage potential customers and partners.
- Insider threat sabotage: This is when the attacker's goal is to sabotage the organization's system and security by using for example malware, privilege escalation etc. Their motive could range from dissatisfaction to stress.
- IP theft: This occurs when the attacker steals source code or customer information without authorization. This type of insider attack could cause enormous damages to small/medium businesses because it may lead to a breach of trust, potentially leading to loss of customers[3,p.4]:.

Prevention of insider attack

To safeguard against insider attacks, small/medium companies should design a tailored training program to ensure employees understand and comply with security policies and recognize threats like malware and phishing. These trainings should focus on safeguarding data through encryption and regular backups and on creating strong passwords that need to be “renewed” as frequently as possible.[4, p.16]

Furthermore, it would be ideal if small/medium businesses could regularly review and communicate their security policies and guidelines for device and network usage to their employees. To further motivate employees to adhere to security policies, small/medium companies could offer small rewards for completing training or following protocol[4, p.20]. In the case of the forensics examination, if regular security checks were performed then someone could have easily spotted the door that the insider intentionally left open. If the open door had been spotted and locked on time, then this could have easily prevented Mr. Scott and his accomplice from escaping.

Managing ex-employees is another crucial aspect of preventing insider threats. An employee account should be terminated as soon as an employee leaves the company, this should effectively mitigate the risk from fired employees[4, p.20]. Furthermore, current employees should avoid directly communicating with the ex-employee regarding business matters or reactivating a former employee's account. In the forensic investigation I conducted, Ami continued communicating with Mr. Scott regarding business matters and this enabled him to exploit this relationship to his advantage and gather information about his target. Small/medium companies should also implement detection mechanisms. Some cybersecurity vendors offer services to create individual risk scores for employees based on factors like their role, online activity, and access level[4, p.20]. These risk scores help prioritize efforts in investigating and responding to insider attacks. If the small company can’t use risk scores, then they can pay attention to Insider threat indicators for example the use of new unapproved personal devices, without coordinating with IT, submitting requests to access drives, documents, or applications that were not previously required by the employee, and displaying sudden interest in the company security tools and policies.[4, p.20]

Small/medium businesses should frequently back up their data and ensure that systems are updated regularly to prepare themselves for potential breaches[4, p.26]. Another mitigation strategy to reduce insider threat risk is to only grant necessary access privileges based on the employee's job role. [4, p.25] Small organizations should start with minimal permissions for new employees and adjust permissions as necessary over time. For example, in the forensics investigation, I conducted, I found that Ami had the code to the safe that contained the post office’s assets, this should not have been the case because she was not the manager of that post office. For these reasons, we can conclude that limiting access to this information could have potentially prevented the robbery.

It is important to make sure that employees are happy and satisfied because when an employee is supported, he is less likely to cause harm to the organization[4, p.27].

OSINT

OSINT refers to the overall process of collecting and analyzing data based on publicly available information[5,p 1]. This process can be considered a double-edged sword because on one side the data gathered can be used to track down cyber criminals or prevent cyber-attacks from occurring but on the other side, data gathered can be used by cybercriminals to plan a cyber-attack against the target company[5,p 2]. For these reasons, small businesses should be cautious, as such attacks can be executed by individuals without hacking experience, and provide them with a lot of knowledge regarding the employees, the business, and its operations. In the case of the forensic investigation I conducted, I found a lot of evidence that proves that Mr. Scott used Google Maps to look up the post office and marked possible escape routes around it. He also took photographs of both the building's interior and exterior, including the locations of CCTV cameras. Without the online research he conducted, Mr. Scott would likely not have had sufficient information to plan the robbery.

To perform OSINT there are 4 steps. The first step is to understand where and how to get the information regarding the target. The second step is to gather every data based. The third step is to refine the collected data by filtering out irrelevant data. The last step is to summarise and analyse the findings.

OSINT prevention strategy

There are different ways to minimize the risks of OSINT for small/medium businesses [6,p.1]:

- As I mentioned earlier, Osint is used by attackers to gather information about a company, but companies can use this to their advantage too. Small companies can search for OSINT about their organization to see what information regarding their company is publicly available and based on the data they collect about their organization's network, systems, and employees, they can then utilize this information to pinpoint security vulnerabilities that could be exploited by attackers and then they could find solutions to fix these vulnerabilities.
- Even if vulnerabilities are identified and addressed, untrained employees can still pose significant risks to the organization, for these reasons, companies should train their employees to recognize and respond to potential cyber threats, establish SOPs, and promptly change compromised credentials.
- Lastly, it is also important to implement physical security measures such as having security staff because it can deter potential threats. If we consider the forensic investigation, Mr. Scott's ability to take photographs of the CCTV and post office layout without being detected or stopped suggests that a lack of physical security can allow attackers to freely perform active reconnaissance. Therefore, small companies should consider having at least a small team of security staff to improve their security measures.[4]

Other Cybersecurity risks

During my forensic investigation, I analysed the image of Mr. Scott computer and found all his deleted files, for these reasons, I think managing the risk of data recovery from disposed hard drives is essential for companies to protect their sensitive information. Without proper precautions, discarded hardware poses a risk, as someone could recover and exploit the data stored on it. To reduce this risk, companies should use specialized software to fully erase data from hard drives, they should encrypt the data and if possible, physically destroy the hard drive.

Unfortunately, insider attacks, OSINT, and deleted data are not the only concern for small/medium companies because by using information gathered from those attacks, the attacker can perform a phishing attack.

A phishing attack is when a cybercriminal pretends to be from a legitimate source and uses fake emails, messages, or websites to lure individuals into revealing sensitive information regarding their organization.

According to the 2020 Proofpoint annual report [7,p.15], phishing attacks are increasingly prevalent and have become a prominent tool in cybercrime. The study revealed that 90% of organizations have been targeted by phishing attacks. Within these organizations, 88% faced spear-phishing attacks, 83% encountered voice phishing, 86% experienced social media phishing, 84% dealt with SMS phishing, and 81% reported malicious USB drops. When comparing these figures to data from the 2019 Proofpoint annual report [7,p.15] and the 2021 APWG report [8, p.4], it shows that each year there is an exponential increase in phishing attacks specifically phishing email attacks. Phishing attacks via email pose a significant cybersecurity threat, and unfortunately, there have been many successful attacks. A notable example is the FACC attack [9, p.3], in which this company fell victim to a $61 million Business Email Compromise scam in 2016. An impostor posing as the president of a company deceived the CEO into transferring 61 million dollars to the attacker's account. Despite the company taking legal action and dismissing the CEO after the attack, the transferred money was irretrievable. This is one of the many cases in which organizations fell victim to this attack. Losing 61 million would be a huge loss for a small company for these reasons, companies should find mitigation strategies against this attack.

In a phishing attack, the attacker typically follows several stages. First, in the "Planning stage," they research potential targets using publicly available information, known as OSINT, to find individuals with valuable data. Next, in the "Creation stage," they craft deceptive emails, often targeting employees. These phishing emails usually exploit human vulnerabilities like curiosity, greediness, trust, inattention to details, and overreliance on technology. By using these vulnerabilities, the attacker can encourage the victim to click links, download infected attachments, and provide sensitive information regarding their organization. Lastly, in the "Collection/Covering Tracks stage," the attacker gathers the stolen information and attempts to erase any evidence of the phishing campaign.

Phishing mitigations

Even for this attack, the best effective mitigation strategy for organizations would be to offer employee training because offering additional cybersecurity training to employees can enhance their awareness, as a result, it decreases the likelihood of them becoming victims of a phishing scam. The issue with this approach is that small to medium-sized companies may lack the budget to invest in cybersecurity training. To address this, I found a paper [10] that proposes ways to optimize training costs while also being effective at reducing the risk of successful phishing. The solution is to use a Risk score to identify high-risk users and low-risk users. Based on this, high-risk users are assigned more training, and low-risk users are assigned less. For example, a company with 1000 employees that delivers 60-minute training per month to each employee, will have a total of 60000 minutes every month. By implementing the solution proposed earlier, the high-risk employee (top 10%) will be assigned 60 minutes per month and the low-risk employee will be assigned 20 minutes per month. This totals to 42,000 minutes of training per month for all employees, saving the company 18,000 minutes. This approach not only optimizes training time but also raises awareness among high-risk individuals about the vulnerabilities they pose to the organization, prompting them to be more cautious.

Conclusion

By implementing these strategies and fostering a culture of cybersecurity awareness, small businesses can significantly enhance their cyber defense posture, safeguard their assets and sensitive information, and maintain trust with their customers and partners.

References

[1] Shuhan Yuan, Xintao Wu, Deep learning for insider threat detection: Review, challenges and opportunities, Computers & Security, Volume 104, 2021. Available at: https://www.sciencedirect.com/science/article/pii/S0167404821000456

[2] A. Kim, J. Oh, J. Ryu and K. Lee, "A Review of Insider Threat Detection Approaches With IoT Perspective," in *IEEE Access*, vol. 8, pp. 78847-78867, 2020,Available at: https://ieeexplore.ieee.org/abstract/document/9078082

[3] Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., & Burnap, P. (2019, September 9). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. Available at: https://www.mdpi.com/2079-9292/9/9/1460

[4] Crowdstrike. (2022, August 10). Mitigating Insider Threats. Available at: https://www.crowdstrike.com/solutions/small-business/mitigating-insider-threats/

[5] Yong-Woon Hwang, Donghyun Kim ,Im-Yeong Lee ,HwankukKim ,Hyejung Lee .(2022, February). Current Status and Security Trend of OSINT. Available at: https://downloads.hindawi.com/journals/wcmc/2022/1290129.pdf?_gl=1*8f3uft*_ga*Mjg5NDk1MjU4LjE2OTkzODgyNDk.*_ga_NF5QFMJT5V*MTcxMzI4MTc0Ny40LjAuMTcxMzI4MTc0Ny42MC4wLjA.&_ga=2.47621922.482495170.1713263177-289495258.1699388249

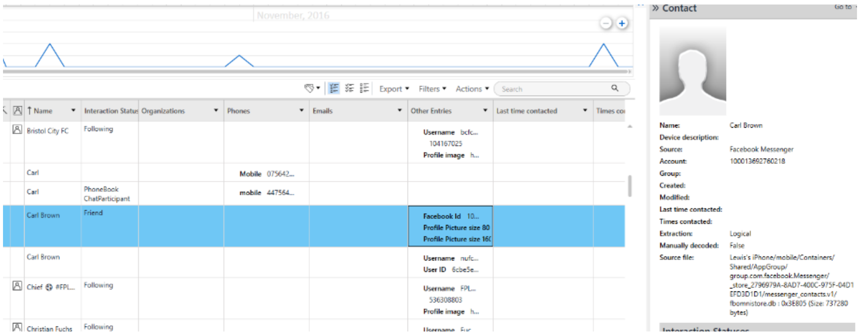
[6] Hiremath, O. (2021, August 26). Protecting Your Organization With Open-source Intelligence (OSINT). Available at :https://www.softwaresecured.com/post/protecting-your-organization-with-open-source-intelligence-osint

[7] proofpoint annual report(2020). State of the phish, An in-depth look at user awareness, vulnerability, and resilience. Available at https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf

[8]APWG(2021,8 June). Available at: https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf?_gl=1*1oi5pjf*_ga*MTkzMjAxODg4NS4xNzA1MzI2NTg2*_ga_55RF0RHXSR*MTcxNDc2OTQwNC40LjEuMTcxNDc2OTUyMi4wLjAuMA..

[9] Check Point Software Technologies Ltd. (2023, May 3). The Top 5 Phishing Scams of all Time . Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times

[10] Hossein Abroshan, Jan Devos, Geert Poels, and Eric Laermans. 2021. A phishing Mitigation Solution using Human Behaviour and Emotions that Influence the Success of Phishing Attacks. In Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization (UMAP '21). Association for Computing Machinery, New York, NY, USA, 345–350. Available at: https://dl.acm.org/doi/pdf/10.1145/3450614.3464472

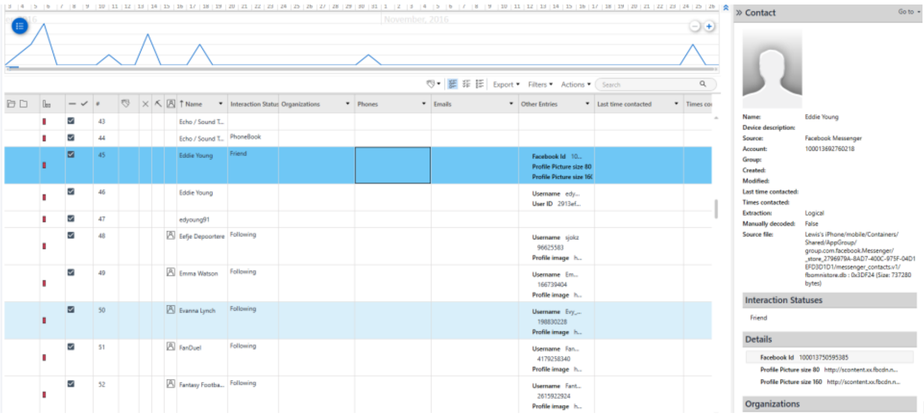


Name	Interaction Status	Organizations	Phones	Emails	Other Entries	Last time contacted	Times co
Bristol City FC	Following				Username bcfc... 104167025 Profile image h...		
Carl			Mobile 075642...				
Carl	PhoneBook ChatParticipant		mobile 447564...				
Carl Brown	Friend				Facebook Id 10... Profile Picture size 80 Profile Picture size 16(		
Carl Brown					Username nufc... User ID 6cbe5e...		
Chief ⊕ #FPL...	Following				Username FPL... 536308803 Profile image h...		
Christian Fuchs	Following				Username Fuc		

Name: Carl Brown
Device description:
Source: Facebook Messenger
Account: 100013692760218
Group:
Created:
Modified:
Last time contacted:
Times contacted:
Extraction: Logical
Manually decoded: False
Source file: Lewis's iPhone/mobile/Containers/Shared/AppGroup/group.com.facebook.Messenger/_store_2796979A-8AD7-400C-975F-04D1EFD3D1D1/messenger_contacts.v1/fbomnistore.db : 0x3E805 (Size: 737280 bytes)

Interaction Statuses

Figure 1



	#	Name	Interaction Status	Organizations	Phones	Emails	Other Entries	Last time contacted	Times co
☑	43	Echo / Sound T...							
☑	44	Echo / Sound T...	PhoneBook						
☑	45	Eddie Young	Friend				Facebook Id 10... Profile Picture size 80 Profile Picture size 16(		
☑	46	Eddie Young					Username edy... User ID 2913ef...		
☑	47	edyoung91							
☑	48	Eefje Depoortere	Following				Username sjokz 96625583 Profile image h...		
☑	49	Emma Watson	Following				Username Em... 166739404 Profile image h...		
☑	50	Evanna Lynch	Following				Username Evy_... 198830228 Profile image h...		
☑	51	FanDuel	Following				Username Fan... 4179258340 Profile image h...		
☑	52	Fantasy Footba...	Following				Username Fant... 2615922924 Profile image h...		

Name: Eddie Young
Device description:
Source: Facebook Messenger
Account: 100013692760218
Group:
Created:
Modified:
Last time contacted:
Times contacted:
Extraction: Logical
Manually decoded: False
Source file: Lewis's iPhone/mobile/Containers/Shared/AppGroup/group.com.facebook.Messenger/_store_2796979A-8AD7-400C-975F-04D1EFD3D1D1/messenger_contacts.v1/fbomnistore.db : 0x3DF24 (Size: 737280 bytes)

Interaction Statuses

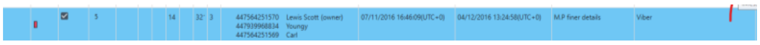
Friend

Details

Facebook Id 100013750595385
Profile Picture size 80 http://scontent.xx.fbcdn.n...
Profile Picture size 160 http://scontent.xx.fbcdn.n...

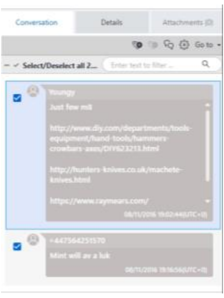
Organizations

Figure 2



☑	5	14	32'	3	447564251570 447939968834 447564251569	Lewis Scott (owner) Youngy Carl	07/11/2016 16:46:09(UTC+0)	04/12/2016 13:24:58(UTC+0)	M.P finer details	Viber

Figure 3



☑ Youngy
Just few mil

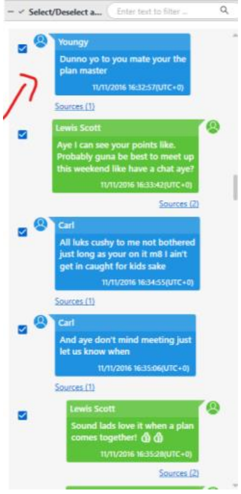
http://www.diy.com/departments/tools-equipment/hand-tools/hammers-crowbars-axes/DIY623213.html

http://hunters-knives.co.uk/machete-knives.html

https://www.raymears.com/
08/11/2016 19:02:44(UTC+0)

☑ +447564251570
Mint will av a luk
08/11/2016 19:16:56(UTC+0)

Figure 4



☑ Youngy
Dunno yo to you mate your the plan master
11/11/2016 16:32:57(UTC+0)
Sources (1)

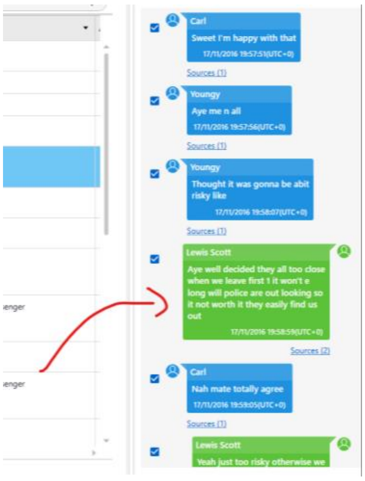
☑ Lewis Scott
Aye I can see your points like. Probably guna be best to meet up this weekend like have a chat aye?
11/11/2016 16:33:42(UTC+0)
Sources (2)

☑ Carl
All luks cushy to me not bothered just long as your on it m8 I ain't get in caught for kids sake
11/11/2016 16:34:55(UTC+0)
Sources (1)

☑ Carl
And aye don't mind meeting just let us know when
11/11/2016 16:35:06(UTC+0)
Sources (1)

☑ Lewis Scott
Sound lads love it when a plan comes together! 👍👍
11/11/2016 16:35:28(UTC+0)
Sources (2)

Figure 5



☑ Carl
Sweet I'm happy with that
17/11/2016 19:57:51(UTC+0)
Sources (1)

☑ Youngy
Aye me n all
17/11/2016 19:57:56(UTC+0)
Sources (1)

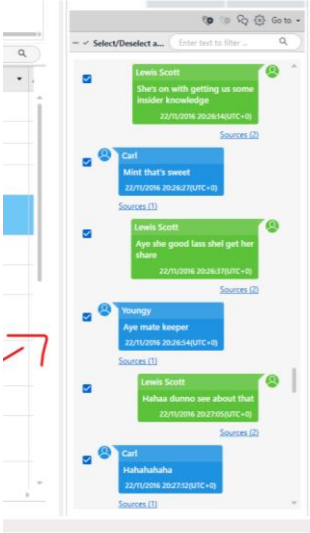
☑ Youngy
Thought it was gonna be abit risky like
17/11/2016 19:58:07(UTC+0)
Sources (1)

☑ Lewis Scott
Aye well decided they all too close when we leave first 1 it won't e long will police are out looking so it not worth it they easily find us out
17/11/2016 19:58:59(UTC+0)
Sources (2)

☑ Carl
Nah mate totally agree
17/11/2016 19:59:05(UTC+0)
Sources (1)

☑ Lewis Scott
Yeah just too risky otherwise we

Figure 6



☑ Lewis Scott
She's on with getting us some insider knowledge
22/11/2016 20:26:14(UTC+0)
Sources (2)

☑ Carl
Mint that's sweet
22/11/2016 20:26:27(UTC+0)
Sources (1)

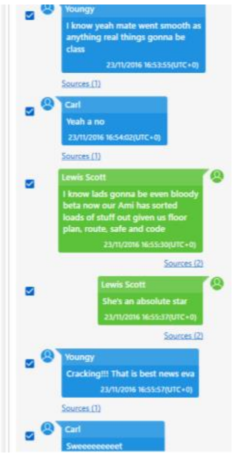
☑ Lewis Scott
Aye she good lass shel get her share
22/11/2016 20:26:37(UTC+0)
Sources (2)

☑ Youngy
Aye mate keeper
22/11/2016 20:26:54(UTC+0)
Sources (1)

☑ Lewis Scott
Hahaa dunno see about that
22/11/2016 20:27:05(UTC+0)
Sources (2)

☑ Carl
Hahahahaha
22/11/2016 20:27:12(UTC+0)
Sources (1)

Figure 7



☑ Youngy
I know yeah mate went smooth as anything real things gonna be class
23/11/2016 16:53:55(UTC+0)
Sources (1)

☑ Carl
Yeah a no
23/11/2016 16:54:02(UTC+0)
Sources (1)

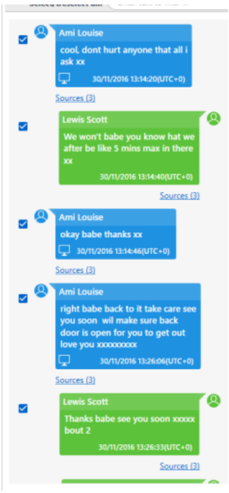
☑ Lewis Scott
I know lads gonna be even bloody beta now our Ami has sorted loads of stuff out given us floor plan, route, safe and code
23/11/2016 16:55:30(UTC+0)
Sources (2)

☑ Lewis Scott
She's an absolute star
23/11/2016 16:55:37(UTC+0)
Sources (2)

☑ Youngy
Cracking!!! That is best news eva
23/11/2016 16:55:57(UTC+0)
Sources (1)

☑ Carl
Sweeeeeeeeeet

Figure 8



☑ Ami Louise
cool, dont hurt anyone that all i ask xx
30/11/2016 13:14:20(UTC+0)
Sources (3)

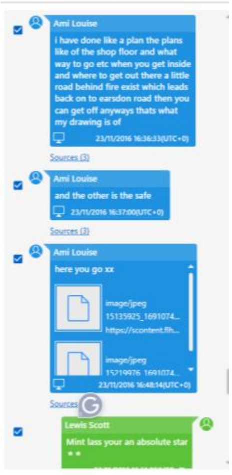
☑ Lewis Scott
We won't babe you know hat we after be like 5 mins max in there xx
30/11/2016 13:14:40(UTC+0)
Sources (3)

☑ Ami Louise
okay babe thanks xx
30/11/2016 13:14:46(UTC+0)
Sources (3)

☑ Ami Louise
right babe back to it take care see you soon wil make sure back door is open for you to get out love you xxxxxxxxx
30/11/2016 13:26:06(UTC+0)
Sources (3)

☑ Lewis Scott
Thanks babe see you soon xxxxx bout 2
30/11/2016 13:26:33(UTC+0)
Sources (3)

Figure 9



☑ Ami Louise

i have done like a plan the plans like of the shop floor and what way to go etc when you get inside and where to get out there a little road behind fire exist which leads back on to earsdon road then you can get off anyways thats what my drawing is of

23/11/2016 16:36:33(UTC+0)

Sources (3)

☑ Ami Louise

and the other is the safe

23/11/2016 16:37:00(UTC+0)

Sources (3)

☑ Ami Louise

here you go xx

image/jpeg
15135925_1691074...
https://scontent.fih...

image/jpeg
15219976_1691074...

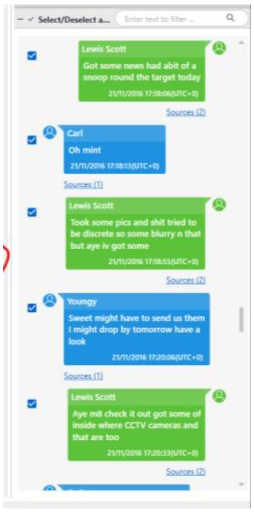
23/11/2016 16:48:14(UTC+0)

Sources

☑ Lewis Scott

Mint lass your an absolute star * *

Figure 10



☑ Lewis Scott

Got some news had abit of a snoop round the target today

21/11/2016 17:18:06(UTC+0)

Sources (2)

☑ Carl

Oh mint

21/11/2016 17:18:13(UTC+0)

Sources (1)

☑ Lewis Scott

Took some pics and shit tried to be discrete so some blurry n that but aye iv got some

21/11/2016 17:18:55(UTC+0)

Sources (2)

☑ Youngy

Sweet might have to send us them I might drop by tomorrow have a look

21/11/2016 17:20:06(UTC+0)

Sources (1)

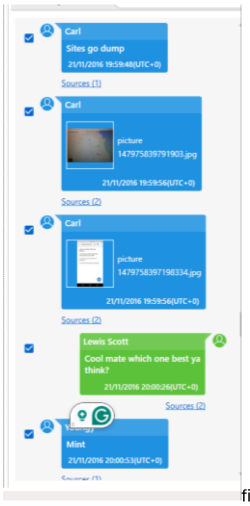
☑ Lewis Scott

Aye m8 check it out got some of inside where CCTV cameras and that are too

21/11/2016 17:20:33(UTC+0)

Sources (2)

figure 11



☑ Carl

Sites go dump

21/11/2016 19:59:48(UTC+0)

Sources (1)

☑ Carl

picture
147975839791903.jpg

21/11/2016 19:59:56(UTC+0)

Sources (2)

☑ Carl

picture
1479758397198334.jpg

21/11/2016 19:59:56(UTC+0)

Sources (2)

☑ Lewis Scott

Cool mate which one best ya think?

21/11/2016 20:00:26(UTC+0)

Sources (2)

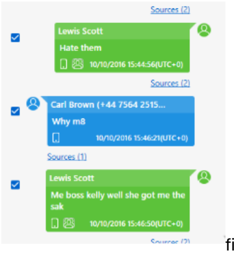
☑ Youngy

Mint

21/11/2016 20:00:53(UTC+0)

Sources (1)

figure 12



Sources (2)

☑ Lewis Scott

Hate them

10/10/2016 15:44:56(UTC+0)

Sources (2)

☑ Carl Brown (+44 7564 2515...

Why m8

10/10/2016 15:46:21(UTC+0)

Sources (1)

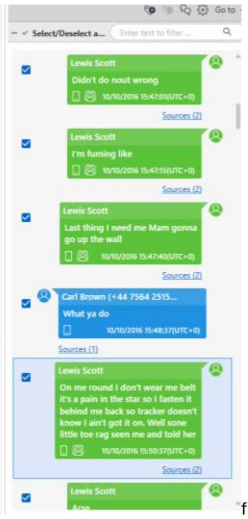
☑ Lewis Scott

Me boss kelly well she got me the sak

10/10/2016 15:46:50(UTC+0)

Sources (2)

figure 13



☑ Lewis Scott
Didn't do nout wrong
10/10/2016 15:47:01(UTC+0)
Sources (2)

☑ Lewis Scott
I'm fuming like
10/10/2016 15:47:15(UTC+0)
Sources (2)

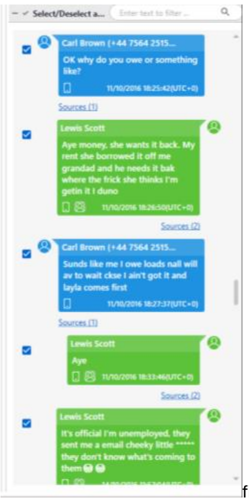
☑ Lewis Scott
Last thing I need me Mam gonna go up the wall
10/10/2016 15:47:40(UTC+0)
Sources (2)

☑ Carl Brown (+44 7564 2515...
What ya do
10/10/2016 15:48:37(UTC+0)
Sources (1)

☑ Lewis Scott
On me round I don't wear me belt it's a pain in the star so I fasten it behind me back so tracker doesn't know I ain't got it on. Well sone little toe rag seen me and told her
10/10/2016 15:50:37(UTC+0)
Sources (2)

☑ Lewis Scott
Arse

figure 14



☑ Carl Brown (+44 7564 2515...
OK why do you owe or something like?
11/10/2016 18:25:42(UTC+0)
Sources (1)

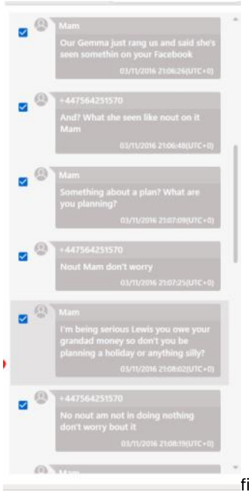
☑ Lewis Scott
Aye money, she wants it back. My rent she borrowed it off me grandad and he needs it bak where the frick she thinks I'm getin it I duno
11/10/2016 18:26:50(UTC+0)
Sources (2)

☑ Carl Brown (+44 7564 2515...
Sunds like me I owe loads nall will av to wait ckse I ain't got it and layla comes first
11/10/2016 18:27:37(UTC+0)
Sources (1)

☑ Lewis Scott
Aye
11/10/2016 18:33:46(UTC+0)
Sources (2)

☑ Lewis Scott
It's official I'm unemployed, they sent me a email cheeky little ***** they don't know what's coming to them 😁 😁

figure 15



☑ Mam
Our Gemma just rang us and said she's seen somethin on your Facebook
03/11/2016 21:06:26(UTC+0)

☑ +447564251570
And? What she seen like nout on it Mam
03/11/2016 21:06:48(UTC+0)

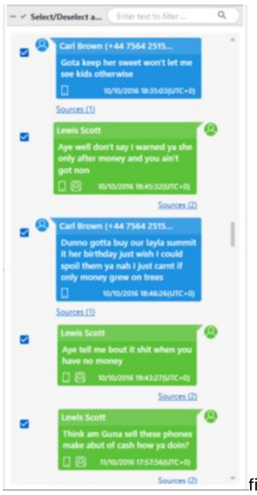
☑ Mam
Something about a plan? What are you planning?
03/11/2016 21:07:09(UTC+0)

☑ +447564251570
Nout Mam don't worry
03/11/2016 21:07:25(UTC+0)

☑ Mam
I'm being serious Lewis you owe your grandad money so don't you be planning a holiday or anything silly?
03/11/2016 21:08:02(UTC+0)

☑ +447564251570
No nout am not in doing nothing don't worry bout it
03/11/2016 21:08:19(UTC+0)

figure 16



☑ Carl Brown (+44 7564 2515...
Gota keep her sweet won't let me see kids otherwise
10/10/2016 18:35:03(UTC+0)
Sources (1)

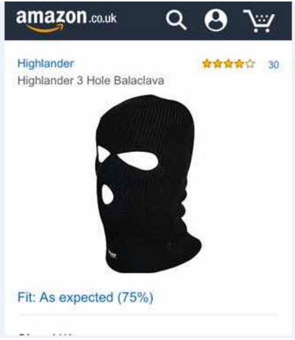
☑ Lewis Scott
Aye well don't say I warned ya she only after money and you ain't got non
10/10/2016 18:45:32(UTC+0)
Sources (2)

☑ Carl Brown (+44 7564 2515...
Dunno gotta buy our layla summit it her birthday just wish I could spoil them ya nah I just carnt if only money grew on trees
10/10/2016 18:46:26(UTC+0)
Sources (1)

☑ Lewis Scott
Aye tell me bout it shit when you have no money
10/10/2016 19:43:27(UTC+0)
Sources (2)

☑ Lewis Scott
Think am Guna sell these phones make abut of cash how ya doin?
11/10/2016 17:57:56(UTC+0)
Sources (2)

figure 17

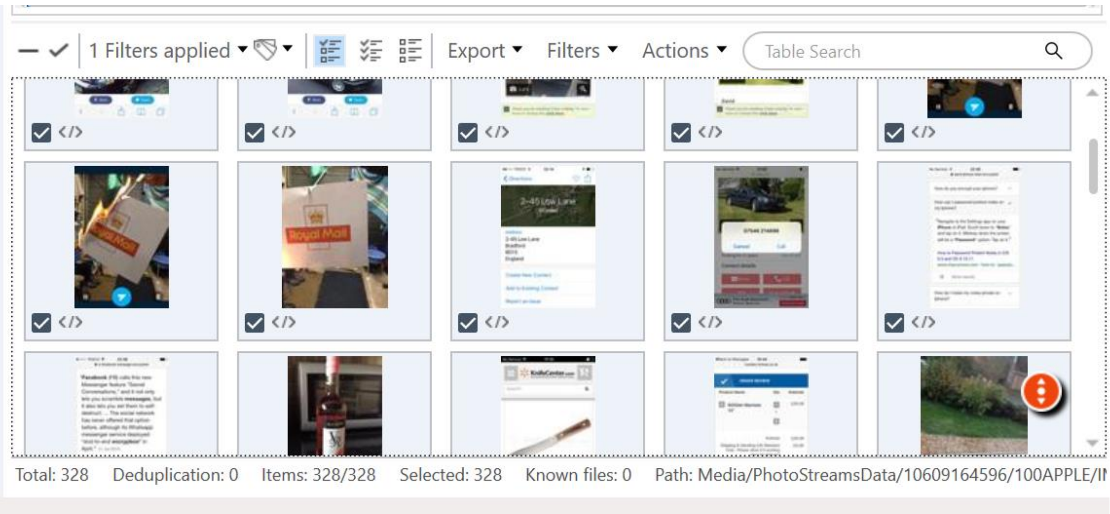


Highlander ★★★★☆ 30
Highlander 3 Hole Balaclava

Fit: As expected (75%)

figure 18

figure 19



Total: 328 Deduplication: 0 Items: 328/328 Selected: 328 Known files: 0 Path: Media/PhotoStreamsData/10609164596/100APPLE/II

Figure 20

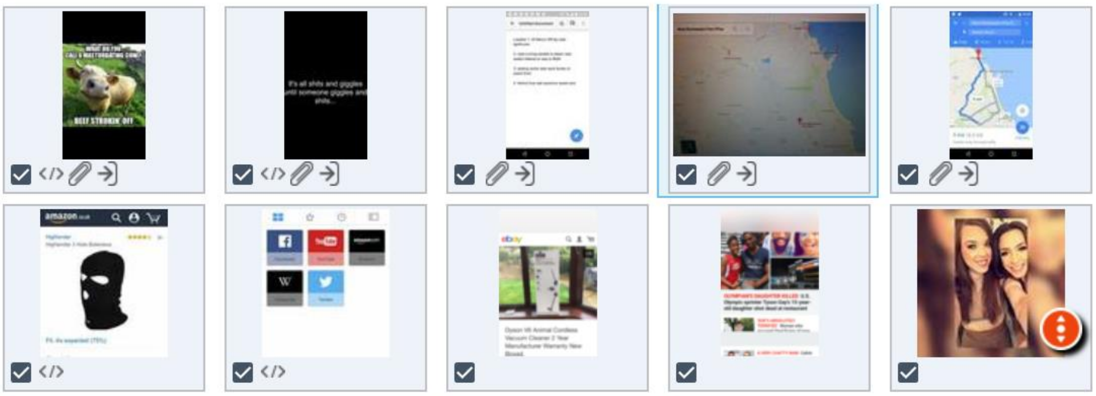
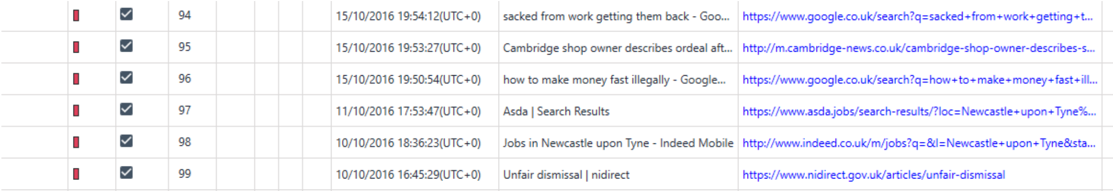
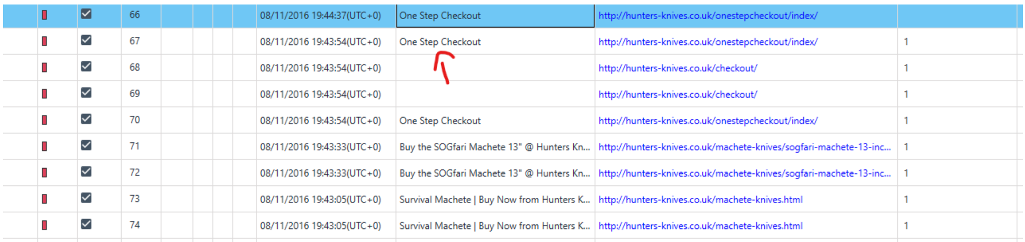

WHAT DO YOU CALL A MASTURBATING COW?
BEEF STROKIN' OFF
It's all shits and giggles until someone giggles and shits.
amazon.co.uk
ebay

Figure 21



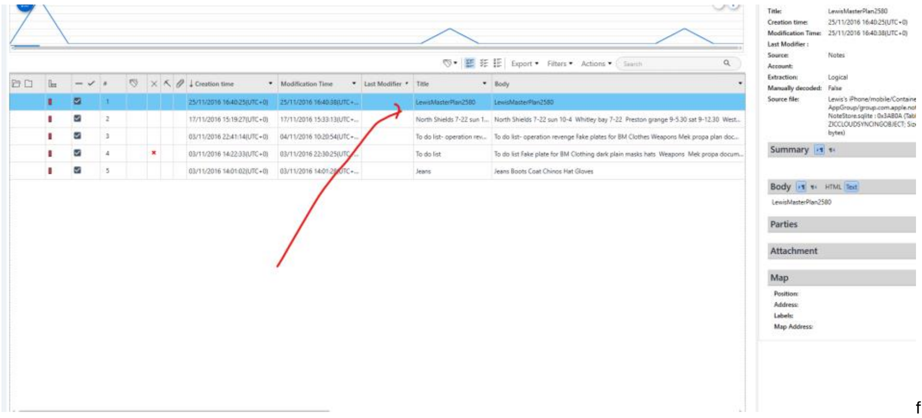
▮	☑	94	15/10/2016 19:54:12(UTC+0)	sacked from work getting them back - Goo...	https://www.google.co.uk/search?q=sacked+from+work+getting+t...
▮	☑	95	15/10/2016 19:53:27(UTC+0)	Cambridge shop owner describes ordeal aft...	http://m.cambridge-news.co.uk/cambridge-shop-owner-describes-s...
▮	☑	96	15/10/2016 19:50:54(UTC+0)	how to make money fast illegally - Google...	https://www.google.co.uk/search?q=how+to+make+money+fast+ill...
▮	☑	97	11/10/2016 17:53:47(UTC+0)	Asda | Search Results	https://www.asda.jobs/search-results/?loc=Newcastle+upon+Tyne%...
▮	☑	98	10/10/2016 18:36:23(UTC+0)	Jobs in Newcastle upon Tyne - Indeed Mobile	http://www.indeed.co.uk/m/jobs?q=&l=Newcastle+upon+Tyne&sta...
▮	☑	99	10/10/2016 16:45:29(UTC+0)	Unfair dismissal | nidirect	https://www.nidirect.gov.uk/articles/unfair-dismissal

figure 22



▮	☑	66	08/11/2016 19:44:37(UTC+0)	One Step Checkout	http://hunters-knives.co.uk/onestepcheckout/index/	
▮	☑	67	08/11/2016 19:43:54(UTC+0)	One Step Checkout	http://hunters-knives.co.uk/onestepcheckout/index/	1
▮	☑	68	08/11/2016 19:43:54(UTC+0)		http://hunters-knives.co.uk/checkout/	1
▮	☑	69	08/11/2016 19:43:54(UTC+0)		http://hunters-knives.co.uk/checkout/	1
▮	☑	70	08/11/2016 19:43:54(UTC+0)	One Step Checkout	http://hunters-knives.co.uk/onestepcheckout/index/	1
▮	☑	71	08/11/2016 19:43:33(UTC+0)	Buy the SOGfari Machete 13" @ Hunters Kn...	http://hunters-knives.co.uk/machete-knives/sogfari-machete-13-inc...	1
▮	☑	72	08/11/2016 19:43:33(UTC+0)	Buy the SOGfari Machete 13" @ Hunters Kn...	http://hunters-knives.co.uk/machete-knives/sogfari-machete-13-inc...	1
▮	☑	73	08/11/2016 19:43:05(UTC+0)	Survival Machete | Buy Now from Hunters K...	http://hunters-knives.co.uk/machete-knives.html	1
▮	☑	74	08/11/2016 19:43:05(UTC+0)	Survival Machete | Buy Now from Hunters K...	http://hunters-knives.co.uk/machete-knives.html	1

Figure23



		#	Creation time	Modification Time	Last Modifier	Title	Body
▮	☑	1	25/11/2016 16:40:25(UTC+0)	25/11/2016 16:40:38(UTC+...		LewisMasterPlan2580	LewisMasterPlan2580
▮	☑	2	17/11/2016 15:19:27(UTC+0)	17/11/2016 15:33:13(UTC+...		North Shields 7-22 sun 1...	North Shields 7-22 sun 10-4 Whitley bay 7-22 Preston grange 9-5.30 sat 9-12.30 West...
▮	☑	3	03/11/2016 22:41:14(UTC+0)	04/11/2016 10:20:54(UTC+...		To do list- operation rev...	To do list- operation revenge Fake plates for BM Clothes Weapons Mek propa plan doc...
▮	☑	4	03/11/2016 14:22:33(UTC+0)	03/11/2016 22:30:25(UTC+...		To do list	To do list Fake plate for BM Clothing dark plain masks hats Weapons Mek propa docum...
▮	☑	5	03/11/2016 14:01:02(UTC+0)	03/11/2016 14:01:28(UTC+...		Jeans	Jeans Boots Coat Chinos Hat Gloves

Title: LewisMasterPlan2580
Creation time: 25/11/2016 16:40:25(UTC+0)
Modification Time: 25/11/2016 16:40:38(UTC+0)
Last Modifier :
Source: Notes
Account:
Extraction: Logical
Manually decoded: False
Source file: Lewis's iPhone/mobile/Containe AppGroup/group.com.apple.not NoteStore.sqlite : 0x3A80A (Tab ZICCLOUDSYNCINGOBJECT; Siz bytes)

Summary

Body HTML Text

LewisMasterPlan2580

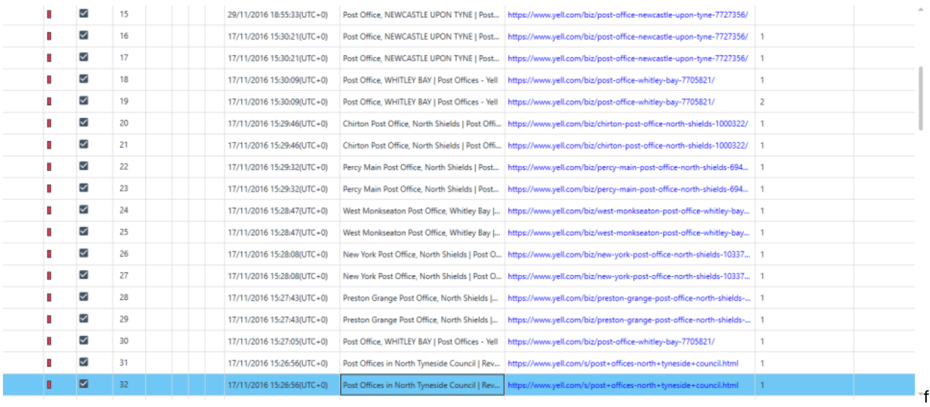
Parties

Attachment

Map

Position:
Address:
Labels:
Map Address:

figure24



▮	☑	15	29/11/2016 18:55:33(UTC+0)	Post Office, NEWCASTLE UPON TYNE | Post...	https://www.yell.com/biz/post-office-newcastle-upon-tyne-7727356/	
▮	☑	16	17/11/2016 15:30:21(UTC+0)	Post Office, NEWCASTLE UPON TYNE | Post...	https://www.yell.com/biz/post-office-newcastle-upon-tyne-7727356/	1
▮	☑	17	17/11/2016 15:30:21(UTC+0)	Post Office, NEWCASTLE UPON TYNE | Post...	https://www.yell.com/biz/post-office-newcastle-upon-tyne-7727356/	1
▮	☑	18	17/11/2016 15:30:09(UTC+0)	Post Office, WHITLEY BAY | Post Offices - Yell	https://www.yell.com/biz/post-office-whitley-bay-7705821/	1
▮	☑	19	17/11/2016 15:30:09(UTC+0)	Post Office, WHITLEY BAY | Post Offices - Yell	https://www.yell.com/biz/post-office-whitley-bay-7705821/	2
▮	☑	20	17/11/2016 15:29:46(UTC+0)	Chirton Post Office, North Shields | Post Offi...	https://www.yell.com/biz/chirton-post-office-north-shields-1000322/	1
▮	☑	21	17/11/2016 15:29:46(UTC+0)	Chirton Post Office, North Shields | Post Offi...	https://www.yell.com/biz/chirton-post-office-north-shields-1000322/	1
▮	☑	22	17/11/2016 15:29:32(UTC+0)	Percy Main Post Office, North Shields | Post...	https://www.yell.com/biz/percy-main-post-office-north-shields-694...	1
▮	☑	23	17/11/2016 15:29:32(UTC+0)	Percy Main Post Office, North Shields | Post...	https://www.yell.com/biz/percy-main-post-office-north-shields-694...	1
▮	☑	24	17/11/2016 15:28:47(UTC+0)	West Monkseaton Post Office, Whitley Bay |...	https://www.yell.com/biz/west-monkseaton-post-office-whitley-bay...	1
▮	☑	25	17/11/2016 15:28:47(UTC+0)	West Monkseaton Post Office, Whitley Bay |...	https://www.yell.com/biz/west-monkseaton-post-office-whitley-bay...	1
▮	☑	26	17/11/2016 15:28:08(UTC+0)	New York Post Office, North Shields | Post O...	https://www.yell.com/biz/new-york-post-office-north-shields-10337...	1
▮	☑	27	17/11/2016 15:28:08(UTC+0)	New York Post Office, North Shields | Post O...	https://www.yell.com/biz/new-york-post-office-north-shields-10337...	1
▮	☑	28	17/11/2016 15:27:43(UTC+0)	Preston Grange Post Office, North Shields |...	https://www.yell.com/biz/preston-grange-post-office-north-shields-...	1
▮	☑	29	17/11/2016 15:27:43(UTC+0)	Preston Grange Post Office, North Shields |...	https://www.yell.com/biz/preston-grange-post-office-north-shields-...	1
▮	☑	30	17/11/2016 15:27:05(UTC+0)	Post Office, WHITLEY BAY | Post Offices - Yell	https://www.yell.com/biz/post-office-whitley-bay-7705821/	1
▮	☑	31	17/11/2016 15:26:56(UTC+0)	Post Offices in North Tyneside Council | Rev...	https://www.yell.com/s/post+offices-north+tyneside+council.html	1
▮	☑	32	17/11/2016 15:26:56(UTC+0)	Post Offices in North Tyneside Council | Rev...	https://www.yell.com/s/post+offices-north+tyneside+council.html	1

figure 25