|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Streamlined Forensic Reporting (SFR)** | | | **MG22B (SFR1)** | | |
| **FORENSIC RESULT REPORT – DIGITAL FORENSIC REPORT** | | | | | |
| Relates to (person): | **Ross Geller** | | Crime/Occ. No: | | **###################** |
| Location: | **Birmingham** | | Force Forensic Ref: | | **DFT-02-5321** |
| Date of Offence/Incident: | **Prior to 01/01/2021** | | Forensic Provider Ref: | | **BCU1012345** |
|  | | | | | |
| Report provided by: | **Umar Hussain** | Organisation: | | **Birmingham City University** | |
| Date of report: | **27/05/2024** | | | | |
| **Examined** | **Results / Findings** | | | | |
|  |  | | | | |
| **Evidence Type Supporting / Technical Information**  **Case Overview**  This case covers the potential theft of an IP (intellectual property) that is of value to a company. The IP is a prototype of the design of a new teddy bear, codenamed ‘Porche’. The evidence apart of this investigation, has been extracted in a forensically sound manner, following the latest forensic procedures. The evidence is made available in a UFDR file, alongside raw data. Whilst the original phone of interest in no longer available, these extractions provide crucial information for the case. In this report, the data available will be investigated to prove or disprove the alleged offense through the identification parties involved and the possible intentions of said party members.  **Method**  The purpose of this investigation was tailored to determine the involvement of ‘Ross’ (the device owner in which this data was extracted from) and uncovering other parties who are potentially involved in the alleged theft of an IP, specifically a teddy bear codenamed ‘Porche’. As stated before, the investigation was conducted using a prepared UFDR file alongside raw data, as the original device was unavailable. However a thorough investigation was still upheld, utilising key tools:   * Cellebrite Reader 7.67.0.15: For navigating the UFDR file. * Autopsy 4.21.0: Used for an in-depth examination files within the raw file data. * Rabbit Hole v2.2.5.0: For assessing databases within the raw data.   The data examined in this investigation covered key areas:   * Web-related data * App-related data * Message-related data * Times associated with key findings   In order to maintain forensic integrity, contemporaneous notes were taken to document each step of the investigation process, ensuring the reproducibility and verifiability of this investigation  **Exhibit Information**   |  |  | | --- | --- | | **Samsung GSM\_SM-A320FL** – **Mobile Phone Details** | | | Manufacturer | Samsung | | Model | SM-A320FL | | Named Device User | Ross Geller | | Operating System | Android 8.0.0 | | IMEI | 353118099497383 | | Serial Number | RF8JB3WXS8E | | Bluetooth Device Name | Galaxy A3 (2017) | | Password Protection | Android fingerprint | | Notes / Attribution linking device to suspect | | |  | |   **Results and findings**  Through this investigation, there is a solid establishment of the device’s ownership being to that of ‘Ross Geller’. A WhatsApp group chat was found relating to the teddy bear, where a plethora of users communicated in regard to the IP, one of which being ‘Ross’. An email uncovered through analysis of the raw files, yielded a conversation between ‘Ross’ and ‘Janice Litman-Gorlanik' in which stealing the IP was discussed as well as selling to ‘Vitality Blast’. ‘Vitality Blast’ is noted as a point of interest, as web data analysed reveals that ‘Ross’ had been looking into the subject. Further looking at the data, ‘Ross’ had planned to ‘leave Janice with nothing’ after cloning her card to take all of her money, boarding a plane as ‘Janice’ with intention to hide in a ‘non-extraditious’ country. Through these results, it is in my professional opinion that ‘Ross’, with the help of ‘Janice’ had meticulously planned to steal the IP and sell in the seeking of financial gain.  **Data Analysis**  Establishing identity  The identity of the owner of this device was verified through Cellebrite. Upon loading the extracted UFDR file into Cellebrite an extraction summary is presented along with a content table with a header called ‘Device Users’. This revealed ‘Ross Geller’ as the sole owner of this phone. Pairing this with ‘User Accounts’ it is beyond reasonable doubt that ‘Ross Geller’ is the owner of this device. The device itself is a ‘Samsung Galaxy A3’.  Messages  There was a total of 28 chats extracted for the purpose of this analysis, either utilising ‘WhatsApp’ (an end-to-end encryption-based messenger) or native messages to the ‘Samsung’ device. Of these chats, there is a WhatsApp group chat called ‘Big Bears’, created by ‘Gunthur’ on 03/09/2019 at 14:05:00. Upon creating this group, Gunthur added ‘447379079908’ which WhatsApp provides a name for, as part of its identifying process. This number belonged to ‘Ross’. The purpose of this group chat, as the name suggests, is to centre around the Teddy Bear. The group chat, excluding Ross, consisted of: Janice, Phoebe Buffay, Gunthur, Rachael Green, Monica Geller, David, Joey Tribbiani and Chandler Bing. An image of the bear was first sent by Gunthur at 14:09:46 on 03/09/2019. A question was then posed by Pheobe Buffay asking, ‘who’s bear’ in which Ross later replied ‘me and mona have a porche’. Porche in this case is a codename for the bear, as in this chat Joey Tribbiani refers to it as such. The point of focus, however, is Ross stating that he is in possession of a Porche.  Email  At precisely 14:13:01 on 3/09/2019 an email, extracted from rabbit hole, with ‘Janice Litman-Gorlanik' as the display name, is sent to Ross through an email associated to him - (practise.ccl.and.8@gmail.com). The content of this email clearly states the intention to steal the Porche patent and sell it to Vitality Blast for monetary gain. At 14:03:02 on 03/09/2019, Ross send an email to Janice’s email - (janice@gmail.com) - specifying the vitality blast in Amsterdam, suggesting to Janice to book a flight for 2 to Amsterdam. At 14:13:04, a response from Janice included a solidifying statement to their motive, stating ‘Let’s go make ourselves millionaires’.  The email associated with Ross can be seen used throughout the device, as it is linked to ‘Google Drive’, ‘Gmail’ and ‘Accounts’. An email sent from Ross at this email address is observed at 08:07:14 the following day on 04/09/2019. The email is sent to 8 different accounts, the same number as users in the WhatsApp Group chat the previous day, although the identity of the users behind the recipient accounts cannot be verified. The content of this email is asking for pictures of the Teddy Bear, which paired with the evidence of selling the bear, illudes to the potential reason as to why he is looking for more images.  Web Data  Through the application ‘Android Browser’ we can view search related data specific to Ross. Through Autopsy, specifically analysing the ‘history’ file within the raw data, a search containing ‘Vitality Blast’ in relation to Birmingham and Edgbaston, is found at 13:58:41 on 03/09/2019. This is before the establishment of the WhatsApp group chat and email records between Janice and Ross. As Vitality Blast is the intended buyer of the stolen IP, this further highlights Ross’s interest in this endeavor as well as explaining his email to Janice previously mentioned, where she was thinking of the Vitality Blast in Birmingham, whereas Ross was thinking of Amsterdam. This could potentially be a decision informed by research conducted in these findings, but it is not certain. What is, however, is the relationship between Vitality Blast, Ross and Janice.  Also, within the ‘history’ file, a search result containing ‘Amsterdam’ is yielded. This is in the context of a website called ‘lastminute’, a flight booking website. This was done at 18:46:37 on 03/09/2019, approximately 4 and a half hours after booking a flight to Amsterdam was mentioned by Ross to Janice over email. At 18:46:47 a new URL is present in the history file, stating ‘Your booking is confirmed!’, illuding to their intention stated, becoming reality.  The login data in regard to ‘lastminute.com’ can be found in the raw files. The email used for this website was ‘practice.ccl.8@gmail.com’, the same as the one Ross has been seen to use. The password for this account at the time was ‘CentralPerk1994’. This accounts existence was verified using autopsy, as user accounts are displayed. The password for the account was not shown on autopsy, however the website and related email were.  Flight  As suggested by the ‘history’ findings, the flight to Amsterdam was confirmed. This flight confirmation was downloaded to Ross’s phone, in the file ‘FlightConfirmed.txt’. Through traversing the raw file system by means of Autopsy, this file was retrieved, and its data presents the details of the flight. The flight was scheduled to leave on 06/09/2019 at 04:45:00, boarding at 04:15:00 and was set to arrive at its destination at 07:00:00, aligning with typical flight times to Amsterdam from the UK.  Further crimes  Additionally, to the evidence related to IP theft, a note found through the raw files within the Samsung notes version 2.1.02.27 application suggests that Ross intended to clone Janice’s cards in attempt to take all of her money, leaving her with ‘nothing’. He writes his intention to move to a ‘non-extraditious’ country and sneak onto a plane in Janice's name to get to this country. This was extracted from ‘personal\_notes.json’ and its content shows that Ross has been planning this as early as 18:46:37 on 03/09/2019. This conclusion is drawn from the bold opening statement, ‘DELETE AFTER FLIGHTS PAID’.  Conclusion  The motive for this crime is demonstrated and solidified in the findings. Ross and Janice planned the theft of the IP, codenamed Porche, for monetary gain. This money was intended to come from Vitality Blast which is highlighted through emails directly discussing this and web data proving the interest. Codename Porche is mentioned by users in the chat ‘Big Bears’ where the topic was openly discussed, leaving no room for misinterpretation of the intent when it comes to the emails between Janice and Ross. The email Ross used is seen to be used for more than just emailing Janice, as it communicated with 8 members, all with the same structure ‘practice.ccl.x@gmail.com’ where the x is a digit separating them all. There are 8 members in the WhatsApp group chat ‘Big Bear’, and although it cannot be verified with the data present, it could be assumed these were company emails. This email was used to make an account with ‘lastminute.com’ where a flight to Amsterdam was booked, and its details downloaded onto the device, proving the device owner, ruling out the possibility of an external force. This was according to the plan laid out by Janice and Ross, however information from the ‘Samsung Notes’ app illude to Ross crossing Janice, stealing all of her money, cloning her card, and subsequently moving to ‘Antarctica’. | | | | | |
| **Case management – To the court and to the defence**  The prosecution propose to rely on the forensic evidence contained in this SFR and if there is a trial, to adduce it by way of a s10 CJA 1967 admission to the general effect that the exhibit(s) listed were forensically examined and the examination produced the result(s) described. Therefore should there be a real issue in relation to this forensic evidence, such that the admission cannot be made, the prosecution ask that the defence identify the issue (Crim.PR.3.3 and Crim.PR 19.3(2)).  If this report contains expert evidence, then, in accordance with CPR 19.3(2), the defence is required to serve a response to this report as soon as practicable, and in any event not more than 10 business days after service of the report setting out which, if any of the conclusions in this report are admitted as fact, and where a conclusion is not admitted what are the disputed issues concerning that conclusion.  **This SFR is not a witness statement** to which the provisions of s9 CJA 1967 and Crim.PR 16 apply, nor is it an expert’s report to which the provisions of Crim. PR 19.4 apply, its purpose being to introduce any expert evidence contained therein as admitted fact. If this SFR contains expert opinion, it is a summary of that opinion served pursuant to Crim. PR 19.3(1).  SFRs assist courts to fulfil their duty to actively manage the case (Crim.PR 3.1) by ensuring that evidence is presented in the shortest and clearest way and by facilitating the early identification of the real issues. (Crim.PR 3.2). Each party must actively assist the court in fulfilling its duty (Crim.PR 3.3). | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Streamlined Forensic Reporting (SFR)** | | | | **MG22B (SFR1)** | | | | |
| **STATUS OF DIGITAL FORENSICS RELATED EXHIBITS** | | | | | | | | |
| Relates to (person): | **Ross Geller** | | | Crime/Occ. No: | | | **###################** | |
| Location: | **Birmingham** | | | Force Forensic Ref: | | | **DFT-02-5321** | |
| Date of Offence/Incident: | **Prior to 01/01/2021** | | | Forensic Provider Ref: | | | **BCU1012345** | |
|  | | | | | | | | |
| Report provided by: | | **Umar Hussain** | Organisation: | | | **Birmingham City University** | | |
| Date of report: | | **27/05/2024** | | | | | | |
| **Exhibits** | | **Status** | | | | | | |
| **Samsung GSM\_SM-A320FL** | |  | | | | | | |
| NB – Umar Hussain, Birmingham City University does not accept responsibility for the sensitivity or otherwise of this material. | | | | | | | | |
| **Additional information /** **Evidence Type Technical Information**  Please note the above list of exhibits relates only to exhibits submitted for examination and are relevant to my area of expertise and / or to the findings set out in the Results/Findings section of this report. The list was accurate at the time this report was generated. All exhibits will not necessarily be listed here. Should a comprehensive list of exhibits be required, please contact the Investigating Officer.  The prosecution will not ordinarily undertake further forensic analysis unless and until the exact issue that such analysis needs to address has been identified; and only if, in light of that issue, it is appropriate that the next stage of analysis should be undertaken by an expert instructed by the prosecution rather than an expert instructed by the defence. If appropriate a direction under Crim.PR 3.5(2)(h) as to the order in which the expert issues should be determined may be sought. | | | | | | | | |
| **Important:**  **Where real issue(s) are identified and if additional forensic work is necessary, please notify the agreed Force contact in writing, listing the issue(s) to be further addressed. Delivery dates for additional forensic work to be agreed on a case by case basis.** | | | | | Forensic Contact Details: | | | **Umar.Hussain5@mail.bcu.ac.uk** |