Digital Incident Scene Investigation and Analysis

CST2580

Final Report

M0087021 I

M00857972

M0087401 3

M008643208

M0091 1983

M0087275I

Executive Summary

This report presents the findings from a comprehensive digital forensic investigation into an incident involving a suspected data breach from a computer system registered to an individual named Jean. The investigation was prompted by the discovery of sensitive information on a competitor's website, which appeared to originate from M57, an online art catalogue company. The primary suspect in the case is the company's CFO, Jean Jones, who had exclusive access to the breached data.

A critical piece of evidence, Jean's hard drive, was meticulously imaged using AccessData® FTK® Imager to ensure the authenticity of the data. The imaging tools and software were carefully selected for their robustness and compliance with forensic standards. Additionally, a USB drive was found and documented, which could potentially provide further insights into the incident.

The root of our discovery was rooted in the analysis of specific emails that were identified as instrumental in the dissemination of the spreadsheet. Through the employment of advanced digital forensic techniques and tools, we were able to reconstruct the sequence of events leading up to the breach. It became evident that the spreadsheet was attached to an email sent by Jean, underlining her direct involvement in the transmission of the data.

This critical email was scrutinized for its metadata, including the timestamp, which provided insights into the timing of the breach, and the recipient list, which revealed the intended targets of the information. The forensic analysis extended to the examination of the email's path across the network, tracing its route from Jean's computer to the external recipient, thereby mapping out the trajectory of the data leak.

Contents

1. Case Background

Our team, consisting of Case Officer Muhaned Ali Nouman, Warrant Officer Hanzala Qadir, Exhibit Officer Sulayman Ali, and Forensic Investigator Deen, was tasked with conducting a thorough digital investigation to identify how a confidential spreadsheet ended up on a rival firm's website. This spreadsheet, which contained the names, salaries, and social security numbers of the 10 employees at M57.Biz, an online art catalogue company, was believed to be exclusively accessed and managed by Jean Jones, the Chief Financial Officer (CFO). Despite Jean Jones' denial and claim of being hacked, as she had no knowledge of how the spreadsheet was leaked, our investigation aimed to uncover:

1. The pathway through which the documents were transferred to the competitor's website.
2. The timestamp of when Jean Jones initially created the spreadsheet.
3. The potential involvement of any other employees from M57.Biz in this incident.

This investigation involved inspecting Jean's computer and its surrounding area, where the spreadsheet was reportedly stored, and conducting interviews with both Jean and Allison Smith, the President, to determine the method of data theft.

2. Investigation

2.1 Search Warrant

3

Obtaining a search warrant for the investigation at Room H104, The Burroughs, Hendon, London, at Middlesex University (NW4 4BT), was a key step in our lawful and methodical evidence gathering. To get this warrant, we had to prove to a judge that there was strong evidence to justify the search. This process ensures our investigative methods are both legal and precise, showing our commitment to following the law and respecting individual rights.

A search warrant is a crucial legal document that a judge or magistrate issues. It allows police or other law enforcement to search a specific place, vehicle, or person for evidence related to a crime. Officers must present a detailed affidavit to a judicial officer to get this warrant. This affidavit must convincingly argue, based on facts, that a crime has occurred, and that evidence of this crime is likely to be found in a certain location. It should clearly state where the search will take place and what items they are looking to find and seize. This careful process helps protect people's privacy while allowing justice to be pursued when there's strong evidence of criminal activity.

2.2 International Standards, Guidelines and Procedures

4

In the investigation of M57.Biz, the adherence to international standards ISO/IEC 27037:2012 and ISO/IEC 17025:2015 played a pivotal role in ensuring the correct management and preservation of

5

digital evidence. These standards offer a comprehensive framework for handling digital evidence across various devices and ensuring the credibility and reliability of forensic investigations. Below are guidelines and procedures that align with these standards, as well as additional bullet points for a deeper understanding:

ISO/IEC 27037:2012 Guidelines:

- **Device Identification and Handling:**
  - Ensure the immediate and secure collection of all digital devices, including computers, USB drives, and mobile phones.
  - Document the physical condition of each device upon collection.
- **Data Acquisition:**
  - Utilize appropriate tools and methods for data extraction, ensuring no alteration of data during the process.
  - Employ write-blocking devices to prevent any write operations to the storage media.
- **Evidence Preservation:**
  - Store digital evidence in a secure environment, protected from magnetic fields, physical damage, and unauthorized access.
  - Maintain a controlled chain of custody for all evidence, documenting every individual who accesses the evidence.

ISO/IEC 17025:2015 Procedures:

- **Qualification and Calibration:**
  - Ensure all equipment used in forensic examinations is regularly calibrated and maintained according to manufacturer specifications.
  - Technicians and forensic analysts must be qualified and trained in the use of this equipment and the interpretation of results.
- **Sample Handling and Analysis:**
  - Adopt standardized methods for the collection, analysis, and storage of digital evidence.
  - Ensure samples are handled in a way that prevents contamination or loss of data.
- **Data Management:**
  - Implement robust data management policies, including secure storage, backup, and restricted access to forensic data.
  - Ensure all analytical procedures and results are fully documented, with an audit trail for quality control.

2.3 Search of the premises and Digital Imaging

On January 16, 2024, led by Hanzala Qadir and Sulayman Ali, our team initiated a meticulously planned search operation at precisely 13:30 GMT. The first step in our procedure was to secure the incident scene, a crucial measure to ensure that no unauthorized individuals could tamper with or alter the potential evidence. This not only involved physically securing the area but also establishing a clear log of all individuals who entered or exited the scene, maintaining the integrity of the environment where the digital evidence was located.

Following the security measures, our attention turned to identifying potential evidence within t 7 secured perimeter. The process began with an examination of the computer's BIOS setup, a foundational system that controls the initialization and diagnostics of hardware components. Capturing an image of the BIOS screen allowed us to document vital details such as the current date, time, and specific configurations of the computer system. This information was essential for completing the necessary documentation associated with our search and for understanding the state of the computer at the time of the incident.

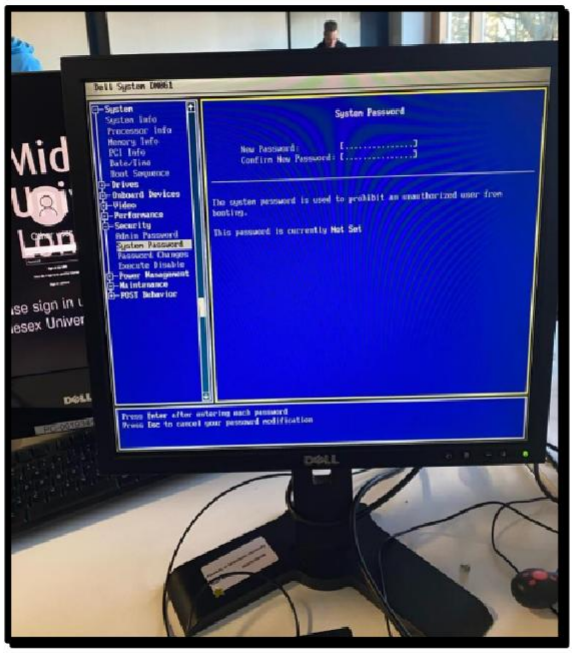


Figure 1 | Jean's Computer's Desktop

By 13:48 GMT, having documented the preliminary information, we progressed to the next critical phase: focusing on the computer's hard drive. To prepare for its digital imaging, we first powered down the computer to ensure the data remained static and unchanged during the imaging process. We took precautionary steps such as securing the power button to avoid accidental reactivation and carefully disconnected all cables and components from the computer, ensuring a thorough approach to preserving the evidence in its original state.

During this preparation, a USB drive was discovered on the opposite side of the room, prompting an immediate extension of our evidence-collection efforts. Photographs of the USB drive were taken quickly, ensuring it was accurately documented as potential evidence before proceeding with the digital imaging of Jean's computer hard drive.

Figure 2 | USB found during search

The discovery of Jean's computer and the USB device signaled the beginning of an intensive digital imaging operation. This step was critical, as it involved creating exact replicas of the digital data found on the hard drive and USB device, ensuring the preservation of data integrity for thorough analysis. By employing recognized forensic software and reliable hardware, we were able to guarantee that the data remained unaltered, thus maintaining the authenticity of our investigative process.

Selection of Imaging Tools and Software

For the imaging of Jean's computer hard drive and USB drive, we chose tools recognized for their reliability and adherence to forensic standards:

Table 1: Tools and Software used for the investigation

Category	Tool/Equipment	Description
Software	AccessData® FTK® Imager 4.7.1.2	Used for creating exact digital copies without altering the original data. Operated on a machine running Windows 11 Enterprise. Serves dual purposes: hosting FTK® Imager and as the OS for imaging.
Hardware	Tableau T35U Write Blocker	Utilized to image the hard disk, preventing any potential data modification during the process.
	Legion Pro 5i PC	The machine used for the operation, features an i7-7700 processor and 16GB of RAM, ensuring efficient imaging performance.

Figure 3

These selections were guided by the need to adhere to best practices in digital forensics, ensuring that our evidence-handling process is both secure and reliable.

11

Procedure for Imaging Jean's Hard Drive

The critical component of our investigation centred around Jean's computer, specifically the hard drive suspected to contain crucial evidence.

- **Preliminary Steps and Discovery**: At 13:44 GMT, we located Jean's computer in BIOS mode, which provided essential system information. To avoid any risk of data alteration, we disconnected the power at 13:49 GMT.
- **Access and Preparation for Imaging**: After powering down the computer, we opened the tower for direct access to the hard drive. This process required us to detach the SATA and power cables, enabling us to securely remove the hard drive.
- **Imaging Process**: The imaging began at 14:00 GMT, with the hard drive connected to our Dell PC host via the Tableau T35U write blocker. This setup ensured no data on the hard drive was altered, maintaining the original state of the evidence. The FTK® Imager software played a crucial role in this process, helping to preserve the evidence's integrity for potential legal scrutiny.

Figurrc 4 /Write blockn used for imaging

Figurrc 5/Jean's Computer's Hard drive

Hash Verification Process

As a critical step in the digital forensic examination, the hash verification process was carried out to ensure the integrity and authenticity of the digital evidence obtained from Jean's computer. The following hash values were computed at the conclusion ofthe imaging process and were then meticulously verified to confirm their accuracy:

- **MDS Checksum:** 78a52b5bac78f4e711607707ac0e3f93
- **SHA1 Checksum:** ba7dc57e08bb6e3393aee1Sc713ae04feadcd181

```
Image Verification Results:
 verification started: sun Mar 17 15:24:54 2024
 Verification finished: sun Mar 17 15:25:56 2024
 MD5 checksum:   78a52b5bac78f4e711607707ac0e3f93 :  verified
 SHA1 checksum:    ba7dc57e08bb6e3393aee15c713ae04feadcd181 :  verified
```

Figurrc 3 / Hash verification

The verification process commenced on Sun Mar 17 at 15:24:54, 2024, and successfully concluded within a minute, affirming that the computed hashes of the imaged data precisely matched the original data'shashes. The matching checksums - MDS and SHA1 - stand as a testament to the data's unchanged state from the time of acquisition to the time of analysis. This match verified the data's integrity, ensuring that no alterations occurred, and that the evidence is forensically sound for subsequent examination and potential legal proceedings.

Upon successful completion of the digital imaging process and hash verifications, our team

transitioned to the crucial phase of evidence preservation. Each item of potential digital evidence, including Jean's hard drive and the USB drive discovered at the scene, was systematically 'bagged and tagged' — a meticulous procedure that ensures the chain of custody is maintained.

For the hard drive, we employed anti-static packaging, which guards against electrostatic discharges that could damage the data stored within. A unique evidence label was then securely affixed to the packaging, detailing the evidence number, [illegible]mber, item description, date and time of collection, and the initials of the handling officer, ensuring every piece of evidence could be accurately traced back to its source.

The USB drive, given its compact size and vulnerability to magnetic fields, was similarly placed in a protective anti-static pouch. It received an evidence tag with correlating details that mirror those on the hard drive's label, maintaining consistency across all evidentiary items.

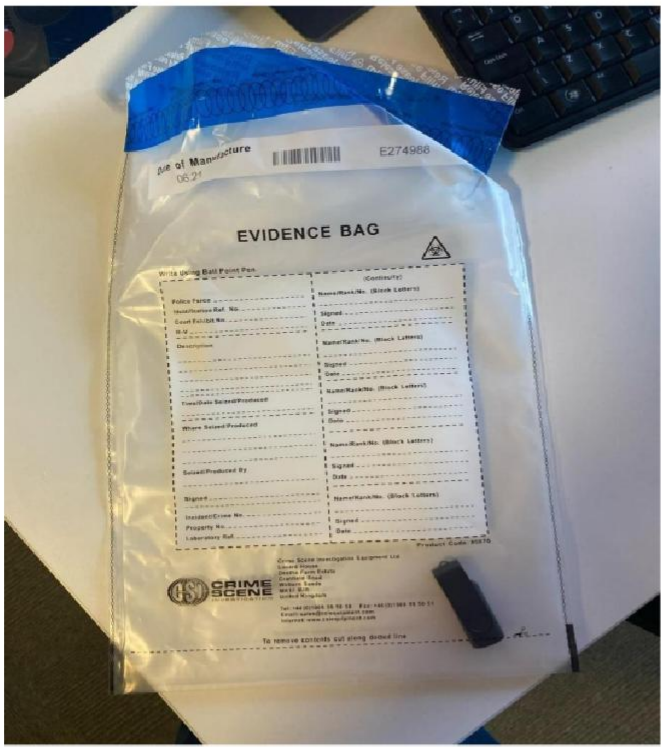


Figure 4| USB bagged and tagged

Once securely enclosed and labeled, the evidence was transported to a dedicated evidence storage facility. This location is specifically designed for the safekeeping of digital evidence, featuring environmental controls to preserve the integrity of the devices and their data. Access to this facility is strictly regulated, requiring authorization and documentation for entry, which is critical for preserving the evidence's forensic value and ensuring it remains untainted.

Figure 5 | Evidence storage location

15

Each item was then logged into the facility's evidence management system, which tracks the location and status of the evidence, providing an auditable trail that documents the entire lifecycle of the evidence — from collection to potential presentation in a court of law. This careful and systematic approach to evidence handling is integral to the foundation of trust and reliability upon which the legal process depends.

Interviews during investigation

Interview Transcript

16

Date: January 16, 2024
Location: [Middlesex University, London, Room H104]
Interviewers: Deen and Amir
Subject: Investigation into Data Breach Incident

Interview 1: Jean, Chief Financial Officer (CFO)

Deen: Good morning, Jean. Thank you for meeting with us today. To start, can you confirm your role within the company and your access level to the company's financial data?

Jean: Yes, I'm the CFL here. I have full access to all our financial data, including the spreadsheets in question.

Amir: We noticed that you've been quite firm in your responses. However, there are a few questions you've opted not to answer. Could you tell us who else has access to the breached spreadsheets?

Jean: Myself, Alison, and the head of the IT department.

Deen: [Notes Jean's attempts to divert the conversation and whistle] Despite some diversions, we managed to get a straightforward answer regarding access to the breached spreadsheets.

Interview 2: The Individual Claiming to be Jean

Amir: Can you confirm your identity and your role within the company?

"Jeana": I'm Jeana, just a caretaker here with very limited access to company data. 17

Deen: But you've mentioned working here for nearly two years. Does your role involve any interaction with company data or computers?

"Jeana": Well, I sometimes work from my hotel room... It's possible someone could've accessed my computer when I left it unattended.

Amir: [Notes inconsistencies and changes in "Jeana's" story] Your account seems to fluctuate. This inconsistency raises some questions about your involvement and access.

Interview 3: The Individual Claiming to be Billy, the Janitor

Deen: Please, could you tell us about your access to the company's sensitive information?

"Billy": I'm just a janitor. I don't have access to anything important.

Amir: And you're certain there's no way you could inadvertently come into contact with company data?

"Billy": Absolutely not. I know nothing about the data breach.

Interview 4: Alison, President of the Company

Amir: Alison, as president, you'd have comprehensive access to all company data, correct?

Alison: Yes, that's correct. There's nothing within the company I can't access if needed.

Deen: Have there been any financial difficulties within the company that might incentivize someone to leak documents?

Alison: No comment.

Amir: [Observes Alison's shock upon learning about their access to documents] You seem surprised we have these documents. Did you know the spreadsheet was created by Jean?

Alison: Yes, Jean handled that spreadsheet.

This transcript highlights several key points relevant to the investigation:

1. **Access and Potential Motives:** Jean and Alison are confirmed to have access to the breached data. Alison's "no comment" to financial difficulties could imply undisclosed motivations behind the data breach.
2. **Suspicious Behaviour:** "Jean's" inconsistent statements and unwillingness to confirm his real name raise suspicions. His changing story and admission that his computer, left unattended, could have been accessed, suggest a possible vector for the breach.

3. **Unreliable Testimonies:** "Billy's" insistence on being a janitor with no access to digital files may be true but requires verification given the context of other misleading testimonies.

Details of items submitted for examination

Jean's Hard drive

Table 2: information about the hard drive

18

Attribute	Details
Software Used	AccessData® FTK® Imager 4.7.1.2
Case Information	M57
Imaging Tool Version	ADI4.7.0.31
Case Number	001
Evidence Number	1
Item Description	Jean's hard drive/M57
Examiner	Muhaned Nouman
Acquisition Date	31/01/2011 16:38:29
Acquisition OS	Windows
Image Type	E01
Image Size	10240 MB
Sector Count	20,971,520
MD5 Checksum	78a52b5bac78f4e711607707ac0e3f93
SHA1 Checksum	ba7dc57e08bb6e3393aee15c713ae04feadcd181
Verification Status	MD5 and SHA1 checksums verified
Acquisition Start	Sun Mar 17 15:23:19 2024
Acquisition Finish	Sun Mar 17 15:24:49 2024
Verification Start	Sun Mar 17 15:24:54 2024
Verification Finish	Sun Mar 17 15:25:56 2024

USB

Table 3: information about the USB

Attribute	Details

Software Utilized	AccessData®FTK®Imager4.7.l.2
Case Information	M57 ADI4.2.0.13 001
Evidence Number	2
Evidence Description	USB device imaging
Examiner	Hanzala Qadir
Acquisition Date and Time	Wed Feb 3 20:53:44 2021to Wed Feb 3 20:54:20 2021
Image File Location	C:\Users\Me\Desktop\cwk2_usb_image.001
Drive Model	General UDisk USB Device
Drive Interface Type	USB
Drive Removability	True
Physical Drive Size	507 **MB**
Sector Count	1,039,616
Drive Geometry	64 Cylinders, 255 Tracks/Cylinder, 63 Sectors/Track
	a5ecc193830f0a9480bflf2c27a4a881
SHAl Checksum	2fded8289c6d25e5977e43b5f577643791aaef52
Checksum Verification	MD5 and SHAl checksums verified

Figure 9

Examination and Analysis

In this investigation, our primary focus was to meticulously analyse the evidence contained within a specific spreadsheet that had been accessed by an unauthorized external party. Our objective was to uncover the truth behind the data leak and arrive at well-founded conclusions. To narrow our scope, we concentrated on areas directly related to the potential breach, including the spreadsheet itself, important emails, images, and the USB device involved. While these elements were our main focus, the investigation's nature meant we remained open to exploring additional areas for deeper analysis as required.

To conduct a thorough analysis, we employed a variety of software tools and devices, each chosen for its specific capabilities and role in the investigative process:

Table 4: software used in the investigation

Software	Version	Purpose
AccessData® Forensic Toolkit	4.7.1.2	Making disk images accessible and for conducting in-depth analysis
Autopsy	4.21.0	Extra tool for verifying findings
Google Chrome	-	Performing online searches to provide context to findings
Microsoft Outlook	-	Examining relevant email communications
Microsoft OneDrive	-	Storage and sharing of investigative findings with the team
Microsoft Excel	16.0.13901.20148	Examining the contents of spreadsheets
Windows 11 Home	-	The operating system of the Legion Pro used in the analysis

Figure 10

Devices Used

Table 5: the devices that were used in the investigation

Device	Model	Description
Huawei Matebook	Laptop D15 2022	Primary machine for analysis
Samsung	LAPTOP-OC4HLA9Q 12th Gen Intel(R) Core(TM) i7-1255U	The main device for investigation tasks

Figure 11

The software and devices we used played a crucial role in examining the digital evidence. Particularly, the Forensic Toolkit software was key in making the collected images viewable. We started looking into the evidence in a case folder we called "Forensic processing". This folder was set up with standard options like creating hash values and showing deleted files, and it could also spot copies of files. We then added the digital image we were investigating to this folder, kicking off our in-depth review.

This methodical way of looking into the data, with the help of specific forensic tools and techniques, made sure our investigation was thorough yet efficient. It helped us go through the massive amount of information, focusing on the parts that were directly linked to the data breach. This setup also kept us flexible to explore any new directions that might come up as we dug deeper.

Examining Digital Photographs

During the meticulous examination of Jean's computer, our team also analysed various digital images stored on the system. Using advanced forensic imaging software, we carefully reviewed the visual content for any clues that could shed light on the incident. Despite our thorough scrutiny of these images, which included looking for hidden metadata and steganographic content, no substantive information relevant to the case was uncovered. The absence of incriminating evidence within these files suggests that, if Jean was involved in the data breach, the pertinent details were not left within the image files on this computer.

Registry information

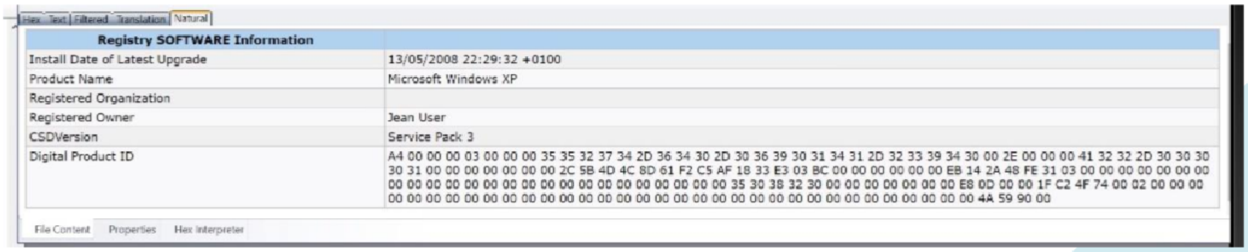
Registry information refers to data stored in the Windows Registry, a database that Windows operating systems use to store system, application, and user settings. This information is vital for forensic investigators because it provides a wealth of details about the configuration and use of a computer system, which can be crucial in understanding the actions and behaviours of users on the system. It can include:

Table 6: information about the registry

Registry Information	Description
User Activity	Tracks applications run, files accessed, and settings altered by users.
System Information	Contains OS configurations, installed software, startup scripts, and hardware details.
Network Configuration	Stores details on network settings and the history of connected networks.
USB Device History	Records identifiers and connection times of USB devices connected to the computer.
User Accounts and Password Policies	Maintains information on user login times and password management policies.

Upon thorough examination of Jean's computer, the inquiry into the system registry files was particularly enlightening. Situated in the \Windows\System32\config\ directory, essential registry hives including SAM, Security, Software, and System were identified and analysed.

Registry SOFTWARE Information



Registry SOFTWARE Information	
Install Date of Latest Upgrade	13/05/2008 22:29:32 +0100
Product Name	Microsoft Windows XP
Registered Organization	
Registered Owner	Jean User
CSDVersion	Service Pack 3
Digital Product ID	A4 00 00 00 03 00 00 00 35 35 32 37 34 2D 36 34 30 2D 30 36 39 30 31 34 31 2D 32 33 39 34 30 00 2E 00 00 00 41 32 32 2D 30 30 30 30 31 00 00 00 00 00 00 00 2C 5B 4D 4C 8D 61 F2 C5 AF 18 33 E3 03 BC 00 00 00 00 00 00 EB 14 2A 48 FE 31 03 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 35 30 38 32 30 00 00 00 00 00 00 00 E8 0D 00 00 1F C2 4F 74 00 02 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 4A 59 90 00

Figure 6| Software registry information

A careful examination of the registry on Jean's computer has provided invaluable information that aids in our understanding of the system's configuration and ownership:

- **Ownership and Usage**: The registry confirms that the operating system, Microsoft Windows XP Service Pack 3, was installed on the 13th of May, 2008. Notably, the system is registered to an individual named Jean User, which establishes a direct link to our main suspect.
- **System Updates**: The last update was applied on the same day as the installation, indicating that the system was maintained up to a certain point, which can be relevant for understanding the system's vulnerabilities or security at the time of the incident.
- **Computer Name**: The designated name of the system is JEAN-13FBF038A3. This unique identifier not only corroborates Jean's usage of the machine but can also be cross-referenced with network logs for potential activity related to the case.

Registry SYSTEM Information

File Content

Hex | Text | Filtered | Translation | Natural

Registry SYSTEM Information	
Active Control Set	ControlSet001
Computer Name	JEAN-13FBF038A3
Shutdown Time	21/07/2008 02:31:32 +0100
Time Zone BIAS	0
Time Zone Active Time BIAS	-60
Standard Bias	0
Daylight Bias	-60
Time Zone Standard Name	GMT Standard Time
Time Zone Daylight Name	GMT Daylight Time

Figure 7| System registry hive

The SYSTEM registry hive provided pivotal insights into the computer's configura 26 d usage. The registry revealed that the computer, identified by the name JEAN-13FBF038A3, was last shut down on the 21st of July, 2008 at 02:31:32 GMT+1. This specific shutdown time is particularly significant as it may align with the timeline of the unauthorized access incident under investigation. Establishing that the computer was active close to the time of the breach can help us pinpoint potential user actions leading up to the event and can corroborate alibi claims or other timeline-based evidence.

Furthermore, the registry indicates that the system was configured to operate in the GMT Standard Time zone, a detail that ensures the accuracy of all time-stamped logs analysed during the investigation. Such consistency in time zone settings is crucial for correlating the logged events with the incident chronology accurately. The Active Control Set, identified as ControlSet001, confirms the system settings in use, which could indicate normal operations or, if altered close to the time of the incident, might suggest tampering or unusual activity.

SAM registry

Upon analysis, the SAM registry suggested several critical points:

1. **User Accounts and Access Controls**: It provided a detailed list of all user accounts present on Jean's computer. This allowed us to scrutinize the access level of each account, identifying those with administrative privileges versus standard user accounts.
2. **Password Policies:** The SAM registry also holds information about the password policies enforced on the system, such as password length, complexity requirements, and expiration intervals. This is crucial for assessing the system's stance against unauthorized access and brute-force attacks.
3. **Last Login Times:** We were able to extract data on the last login times for each account, which is invaluable for constructing a timeline of user activity. This cou 27 ntially correlate user logins with the timing of the unauthorized access or breach.
4. **Failed Login Attempts**: The registry tracks the number of unsuccessful login attempts, which can indicate attempted unauthorized access. Analyzing these entries helped us identify any anomalies or patterns suggestive of a security threat.

Spreadsheets metadata

STILL IN PROGRESS

Emails

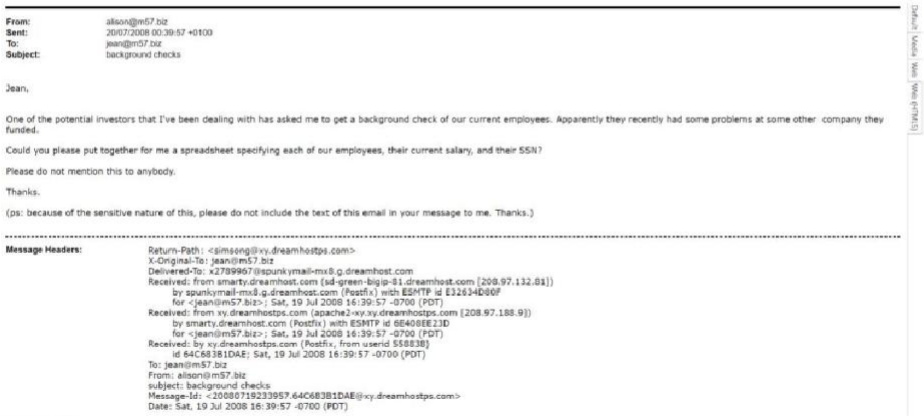
Analysis of emails is an essential part of any investigation, especially in organizations such as M57.Biz where email is the main form of communication. Data security is given top priority by M57.Biz, guaranteeing secure and expert communication within its own domain. A detailed examination of email headers was done during the investigation, particularly those that came from Jean's PC. Email origins and paths inside the M57.Biz network may be traced back to these headers, which contain crucial metadata like sender details, timestamps, and routing information. Keywords were used to quickly and effectively extract relevant data from the large dataset to expedite the research process. However, how well this process works is largely dependent on how well M57.Biz's email system indexes emails.

28

29

30

1st Email



From: alison@m57.biz
Sent: 20/07/2008 00:39:57 +0100
To: jean@m57.biz
Subject: background checks

Jean,

One of the potential investors that I've been dealing with has asked me to get a background check of our current employees. Apparently they recently had some problems at some other company they funded.

Could you please put together for me a spreadsheet specifying each of our employees, their current salary, and their SSN?

Please do not mention this to anybody.

Thanks.

(ps: because of the sensitive nature of this, please do not include the text of this email in your message to me. Thanks.)

Message Headers:

Return-Path: <simseng@xy.dreamhostps.com>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx8.g.dreamhost.com
Received: from smarty.dreamhost.com (sd-green-bigip-81.dreamhost.com [208.97.132.81])
by spunkymail-mx8.g.dreamhost.com (Postfix) with ESMTP id E32634D80F
for <jean@m57.biz>; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
Received: from xy.dreamhostps.com (apache2-xy.xy.dreamhostps.com [208.97.188.9])
by smarty.dreamhost.com (Postfix) with ESMTP id 6E408EE23D
for <jean@m57.biz>; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
Received: by xy.dreamhostps.com (Postfix, from userid 55883E)
id 64C6831DAE; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
To: jean@m57.biz
From: alison@m57.biz
subject: background checks
Message-Id: <20080719233957.64C6831DAE@xy.dreamhostps.com>
Date: Sat, 19 Jul 2008 16:39:57 -0700 (PDT)

31

Figure 13

explanation:

This is an email from Alison to Jean asking her to make a spreadsheet with all the employers with all their salaries as they have investors, and they want to do a background check on them. Only Jean and Alison know about this spreadsheet no one else in the company knows about it, it appears to be unreliable for several reasons in verification.

Verification:

32

-The Return-path and the message-ID are matching as: "@xy.dreamhostps.com". it appears to be unreliable because Alison's Message-ID is ending with @m57.biz, and the Message-ID of the Email above is @xy.dreamhostps.com it seems possible that this email has been sent by a third party

33

Return-Path	@xy.dreamhostps.com
Message-ID	@xy.dreamhostps.com
From	alison@m57.biz

-The X-Original-To header & To header are matching as jean@m57.biz and that shows that the email delivered successfully.

X-Original-To	jean@m57.biz
To	jean@m57.biz

-Both Received headers "from" and "by" show the sender's email address as xy.dreamhostps.com, only the Received header "from" includes an IP address (208.97.188.9), which can be verified to see the stability of the connection. The two headers also have different IDs: "by" header has "64C683B1DAE," which cannot be verified, while "from" header has "ESMTP id 6E408EE23D." Since Received headers are crucial in

determining the reliability of the email server, the inconsistency between headers 'from and 'by' suggests that the email might be suspicious and need further investigation.

From	xv.dreamhostm.com
Bv	xy.dreamhostps.com
From "'IP address•	208.97.188.9
From "'ESMTP"	6E408EE23D
bv "'ESMTP"	64C683B1DAE

2nd Email

Frnm: ak!:ic< !57.IIW-
Sent! 20,I[J7fIOQII00:50:11I +OHIO
TQ; Jv,a11 UMr <iNn@m57 bit'>
SuDJtct: RE: wnkn emil!l aocnu are Ullng?

Ve:s. I ,;otthl:temaiL

-----Or1,glnal MMSil'ijll!·····
F :)ean User [m-1llto:Jean@m57.biz]
Sent; Sund,11v, Jul:v 20, 2008 12.:46 AM
To: ;iilu
Subj.a; RE: whict, •m•il 1ddr1u 11r11y1ou usai.-.g7

So are you going to get this email?

-----01'1QInal MM!IlilOl!:-----
From! a1ex [mallto:al n@m57.biz)
SiMt: Sunday, July 20, 2CI08 12:44 AM
To: ,e.an u,er
S-.ibjKt FtE: whld1 em.all addr■H -1r111 yo1,1 1alr.lil'

Whoops. It looks like my email was misconfigured.

My &<'ntli1 i,t Ali:sOl"l(l'lr'n57 bi:t, nor 11111,f,,:r_Snr'ljl' :lllbout tl'lllt

-----OrhJInal Me.551191!:-----
frcm: a1ex [mallto:aleA@-mS7.biz]
SIM[: Sund11y, July 20, 2008 12:3] iliM
To: Je.an U"er; allson@mS:?.bi..z
Subject: RE: which em-11 addrl!n are vou u,lr.g?

This one, obviously.

-----ortg,nal Mri age-••··
From: IH,n user (mailta:JunOm57.bi%]
Sl!-nt: Sunday. July 2□. 2008 12:32 AM
T : a.11"onC,m57.blt
SubjKt: while:!, email add,..:H ar• you u1lng?

Are you going to use alex@m57.biz or alison@m57.biz?

M-tlIN91' HHdl!ra:
Fl.et\lm-Pilltl1: -c.illi0fl@m57,blz>
X•Ong1n•l•To; JHn@m57,br;r:
O.lii.t1r1d•To: :ic2789967@59unl;.ym•il• 2.g,drHmhg:i;t,,om
R.1i;ei ; from ie;iin1lfbfOJ81J (unl;.nawn {70.134.85.172})
by -'?1Jnlcym:iiil■-112.g.d;,e111onho .c,;im (Pti-1:tfi:r) with ESMTP id EF"C68 1C9
for <j.,.,nfl-mS7.btZ>; Sat, 19 Jul 2008 16:SO:19 -0700 {POT)
Fram: "ale:ii:" <aliioer'l@m57.bi.t►
To: •Jean Utcr" <Jean,UmS7.blz:>
Subject: RE: whldi email addre arercuusing?
Dae@: Sun, 20 Jul 2008 DO:SO:19 +0100
Me:!lsage-10: c:KAEEIACF'IHe.POJt,,IPKHIPIEAGCAAA.atlscn@ImS?.bl:z>
MIME-Ven;lon: 1.0
Cont@nt•l'"l'PII!!: tot/pla.ln;
charMt• "150-8859-1"
C t-Tr.an,f.,-..Em;;odin.i: 7bit
X•Pri...-i1y: 3 (Noflffill)
X•MSM•lI•Priority: Norm..
:ic-M.lifl,irr: M1cro$0l't Outlaol IMO, t!luil(I 'ill.O.l4lllo(-0-l:SHO.O)
Importancll:!: Normal
){,Mime-OLE: Produ ByMietosoft Mi OLEVIS.00.2900.5512
111- ply-Ta: c:NNEEKAKACNPOIIMAAIIKAECACAAA.J i!lnRmS7.bi.t>

Figure 14

explanation:

-The email chain implies that M57.Biz staff members are confused or misinformed about using email addresses. When jean first asks Alison/Alex what email address they are using, Alex responds “this one” Aison responds “not Alex” then jean asked Alison for conforming, Alison respond and answering yes so Alison is using alison@M57.biz, This might to appears to be unreliable for several reasons in verification.

Verification:

-The Return-path and the message-ID are matching as Alison account belong to M57.biz company but it is already clear that the person is unreliable because Alison's email address has been replaced with Alex's, as his message-ID, which is shows in the table below:

Return-Path	**alison@m57.biz**
Message-ID	KAEEIACFIHBPDJMPKNIPAEAHCAAA.alison@m57.biz
Alex’s Message-ID - 2ND Emile	KAEEIACFIHBPJDJMPKNIPOEACCAAA.alex@m57.biz

-The X-Original-To header & To header are matching as jean@m57.biz and that shows that the email delivered successfully.

X-Original-To	**jean@m57.biz**
To	jean@m57.biz

- The Received header & the Delivered-to header matches the same sender’s email address which known as dreamhost.com used to send the Emile, There’s also **Unknown** IP address known as: 70.134.85.172 which be verified by using DNS(Domain-Name- System) to see the stability of the connection, , there’s also a ESMTP(Extended-Simple-Mail –Transfer-Protocol) know as : 2780588164, The email can be considered to be unreliable because the router is **unknown** and also because user Alison have been replaced by the user Alex, who is not an employee at M57.biz.

Received	**dreamhost.com**
Delivered-to	dreamhost.com
IP address (Unknown)	70.134.85.172
ESMTP	EFC68881C9

3rd Email

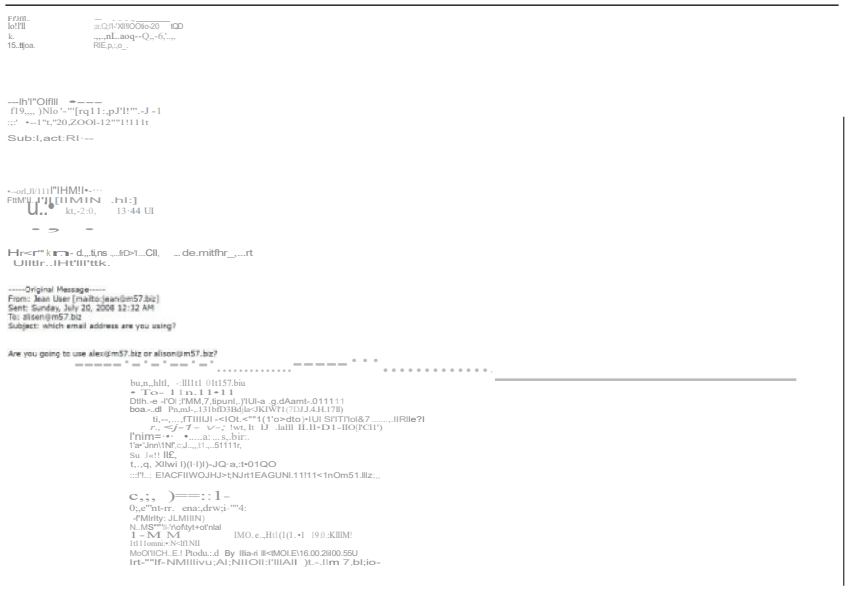


Figure 15

explanation:

-This is an email from Alison/Alex to Jean asking her if she heard anything from Alice, Bob and Carol which seems they are employee in M57, Jean responds Not yet, Alison/Alex respond Well, make it happen, this might to appears to be unreliable for several reasons in verification.

Verification:

-The Return-path and the message-ID are matching as Alison account belong to M57.biz company but it is already clear that the person is unreliable because Alison's email address has been replaced with Alex's, as his message-ID, which is shows in the table below:

Return-Path	**alison@m57.biz**
Message-ID	KAEEIACFIHBPDJMPKNIPAEAHCAAA.alison@m57.biz
Alex's Message-ID - 2ND Emile	KAEEIACFIHBPJDJMPKNIPOEACCAAA.alex@m57.biz

-The X-Original-To header & To header are matching as jean@m57.biz and that shows that the email delivered successfully.

X-Original-To	**jean@m57.biz**
To	jean@m57.biz

- The Received header & the Delivered-to header matches the same sender's email address which known as dreamhost.com used to send the Emile, There's also **Unknown** IP address known as: 70.134.85.172 which be verified by using DNS(Domain-Name- System) to see the stability of the connection, , there's also a ESMTP(Extended-Simple-Mail –Transfer-Protocol) know as : 67491881C9, The email can be considered to be unreliable because the router is **unknown** and also because user Alison have been replaced by the user Alex, who is not an employee at M57.biz.

Received	**dreamhost.com**
Delivered-to	dreamhost.com
IP address (Unknown)	70.134.85.172
ESMTP	EFC68881C9

4th Email

From: alison@m57.biz
Sent: 20/07/2008 02:22:45 +0100
To: jean@m57.biz
Subject: Please send me the information now

Hi, Jean.

I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent. Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires?

Thanks.

Alison

Message Headers:

```
Return-Path: <simsong@xy.dreamhostps.com>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx2.g.dreamhost.com
Received: from smarty.dreamhost.com (sd-green-bigip-66.dreamhost.com [208.97.132.66])
        by spunkymail-mx2.g.dreamhost.com (Postfix) with ESMTP id 2D1DC7278E
        for <jean@m57.biz>; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
Received: from xy.dreamhostps.com (apache2-xy.xy.dreamhostps.com [208.97.188.9])
        by smarty.dreamhost.com (Postfix) with ESMTP id 138E5EE221
        for <jean@m57.biz>; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
Received: by xy.dreamhostps.com (Postfix, from userid 55838)
        id 177343B1DA8; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
To: jean@m57.biz
From: tuckgorge@gmail.com (alison@m57.biz)
subject: Please send me the information now
Message-Id: <20080720012245.177343B1DA8@xy.dreamhostps.com>
Date: Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
```

Figure 16

explanation:

-This is an email from Alison to Jean asking that she need the information which is the "spreadsheet" as soon as possible, This might to appears to be unreliable for several reasons in verification.

Verification:

-The Return-path and the message-ID are matching as @xy.dreamhostps.com account but it is already clear that the person is unreliable because Alison's email address end with alison@m57.biz while the Emile above ends with @xy.dreamhostps.com It is possible to believe that the email was sent by either her personal email, which could be "tuckgorge@gmail.com" as well as to her business email, or it may have been a spam message from a third-party account.

as it shows in the table below:

Return-Path	**@xy.dreamhostps.com**
Message-ID	@xy.dreamhostps.com
3rd party Emile	tuckgorge@gmail.com / alison@m57.biz

-The X-Original-To header & To header are matching as jean@m57.biz and that shows that the email was delivered successfully.

X-Original-To	**jean@m57.biz**
To	jean@m57.biz

-Both Received headers "from" and "by" show the sender's email address is xy.dreamhostps.com, only Received header "from" have an IP address (208.97.188.9), which can be verified using DNS to see the stability of the connection. The two headers also have different IDs: "by" header has "177343B1DA8," which cannot be verified, while "from" header has "ESMTP id 138E5EE221" Since Received headers are crucial in determining the reliability of the email server, the inconsistency between headers 'from and 'by' suggests

that the email might be suspicious and sent from third party and it need further investigation as there The Delivered-to header with Emile dreamhost.com with the IP address 208.97.132.66 and ESMTP 2D1DC7278E that confirm and increase the probability that the Emile been sent from 3rd party.

From	xv.draamhostm.com
y	xy.dreamhostps.com
From "'IP address"	208.97.188.9
From "'E5MTP"	2D1DC7278E
by "ESMTP"	138ESEE221
-- ....ta	dreamhost.com
Dellv.,.Mfl-talP	208.97.132.66
Delivered-to ESMTP	177343B1DA8

5th Email

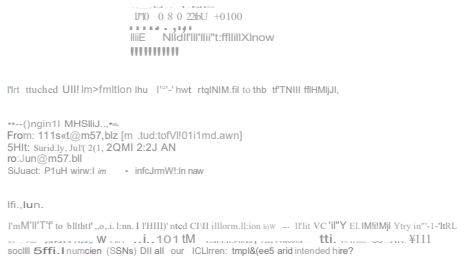


Figure 17

explanation:

This is a confirmation email from Jean saying that the spreadsheet has been attached in this Email.

6th Email

Figu 18

explanation:

This is a confirmation email from what to appear Alison thanking Jean for the file.

Verification:

-The Return-path and the message-ID are matching as@xy.dreamhostps.com account but it is already clear that the person is unreliable because Alison's email address end with alison@m57.biz while the Emile above ends with@xy.dreamhostps.com It is possible to believe that the email was sent by either her personal email, which could be "tuckgorge@gmail.com" as well as to her business email, or it may have been a spam message from a third-party account.

as it shows in the table below:

Return-Path	@xy.dreamhostps.com
Message-ID	@xy.dreamhostps.com
3rd party Emile	tuckgorge@gmail.com / alison@m57.biz

-The X-Original-To header & To header are matching as jean@m57.biz and that shows that the email delivered successfully.

X-Original-To	jean@m57.biz
To	jean@m57.biz

-Both Received headers “from” and “by” show the sender's email address is xy.dreamhostps.com, only Received header “from” have an IP address (208.97.188.9), which can be verified using DNS to see the stability of the connection. The two headers also have different IDs: “by” header has "39FD03B1DAE," which cannot be verified, while “from” header has "ESMTP id 3E257EE236” Since Received headers are crucial in determining the reliability of the email server, the inconsistency between headers ‘from and ‘by’ suggests that the email might be suspicious and sent from third party

From	xy.dreamhostps.com
by	xy.dreamhostps.com
From “IP address”	208.97.188.9
From “ESMTP”	3E257EE236
by “ESMTP”	39FD03B1DAE

7th Email

Figure 19

explanation:

-This Emile between jean and Bob, Bob asking jean about any info belong to M57 contain sensitive info posted in the internet.

Verification:

-The Return-path and the message-ID are matching as Bob account belong to M57.biz company account as it shows in the below table:

Return-Path	Bob@m57.biz
Message-ID	52778.70.134.85.172.1216598579.squirrel@webmail.m57.biz.
3rd party Emile	tuckgorge@gmail.com / alison@m57.biz

-The X-Original-To header & To header are matching as jean@m57.biz and that shows that the email delivered successfully.

X-Original-To	jean@m57.biz
To	jean@m57.biz

-Received header "From" utilizing IP address 70.134.85.172 as a means of transmission across the router, the message can be interpreted as erratic spam email. Although it is useless, a verify can be done to check that the connection is stable. Furthermore, no ESMTP id is present The IP address 127.0.0.1 and the sender's email address webmail.m57.biz are used in the received header "by". a verify can be done to check that the connection is stable. SMTP address 8F4FB5BEE8 increases the reliability of the email as it is the record of the device's server while it has been already established to be a spam email. The sender's IP address, 208.97.132.81, and email address, spunkymail-mx5.g.dreamhost.com, are included in the Received header "from" and the Delivered-to header. To verify the consistency of the connection, even if it has already been determined that the email is spam, its ESMTP id of 9C3741CE4 enhances its credibility as it is a record of the device's server.

From	bob@m57.biz
by	webmail.m57 (127.0.0.1)
From "IP address"	70.134.85.172
From "ESMTP"	N/A
by "IP address"	127.0.0.1
by "ESMTP"	8F4FB5BEE8
To "Sender"	spunkymail-mx5.g.dreamhost.com
To "Sender" IP address	208.97.132.81
To "Sender" ESMTP"	9C3741CE4

Timelines of Emails

Date/Time	Subject	From	To	Message
20/07/2008 at 00:39:57	'Background checks'	jean@m57.biz	jean@m57.biz	Creating the file
20/07/2008 at 00:50:19	'Which email address are you using?'	Alex as alison@m57.biz	jean@m57.biz	Email has been misconfigured
20/07/2008 at 00:50:20	'programmers'	Alex as alison@m57.biz	jean@m57.biz	Programmers are not working
20/07/2008 at 02:22:45	'Please send me the information now'	alison@m57.biz	jean@m57.biz	requesting the files "spreadsheet"
20/07/2008 at 02:28:47	'Please send me the information now'	jean@m57.biz	alison@m57.biz	Spreadsheet been sent
20/07/2008 at 08:03:40	'Thanks'	alison@m57.biz as tuckgorge@gmail.com	jean@m57.biz	Spreadsheet been received
21/07/2008 at 01:02:59	'Hi Jean'	bob@m57.biz	jean@m57.biz	M57 employee info been leaked

Table 7: chronological order of the important emails between Jean and Alison

Conclusion

Appendix

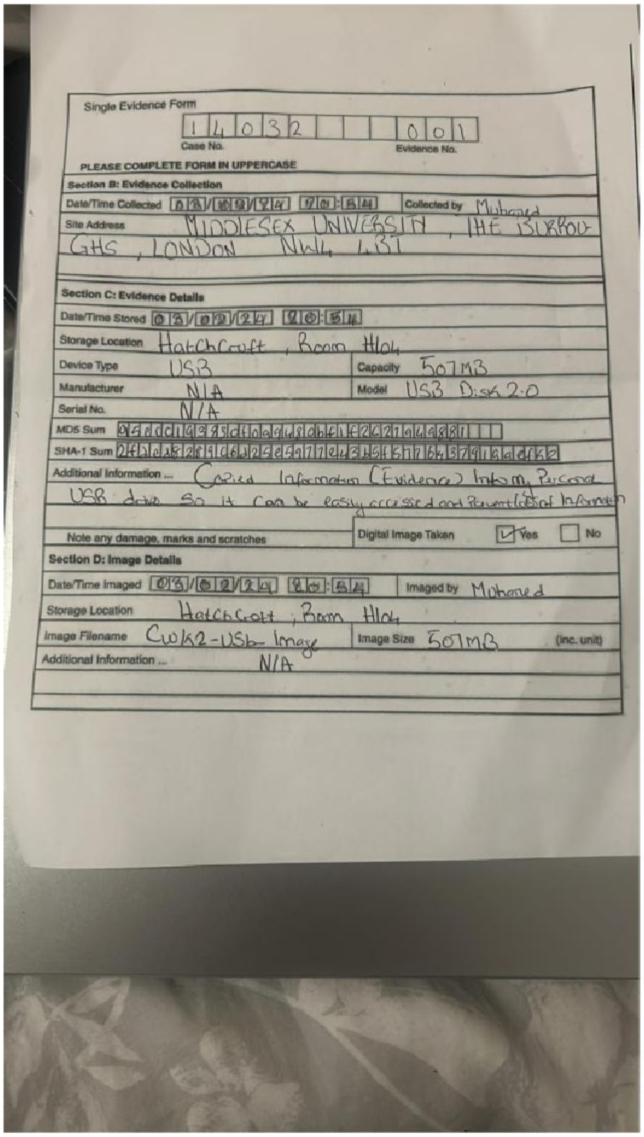
Form 1: Chain of Custody

Chain of Custody Form

Evidence Item Details			
Case Name	M57. Biz	Date	16/01/2024
Case No.	140321	Evidenuteag No.	E274988
Time of Seizure	1:30	Seizure Location	H104
Seized From	Jean room	Seized By	Sulayman
Description	I Found two types of evidence one was a hard drive and a USB		
Unique Marking	N A		

Custody Log					
#	Date	Time	Released By	Received By	Action Taken
1	16/01/24	5:00	Ali		took the hard drive out of the bag and started to image it
2	20/01/24	11:00	Ali	Muhaned	took the USB out of the bag and started to investigate
6					

Form 2: Acquisition form of the USB



Single Evidence Form

Case No. 14032 Evidence No. 001

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 03/02/24 20:54	Collected by Muhamed
Site Address MIDDLESEX UNIVERSITY, THE BURROUGHS, LONDON NW4 4BT	

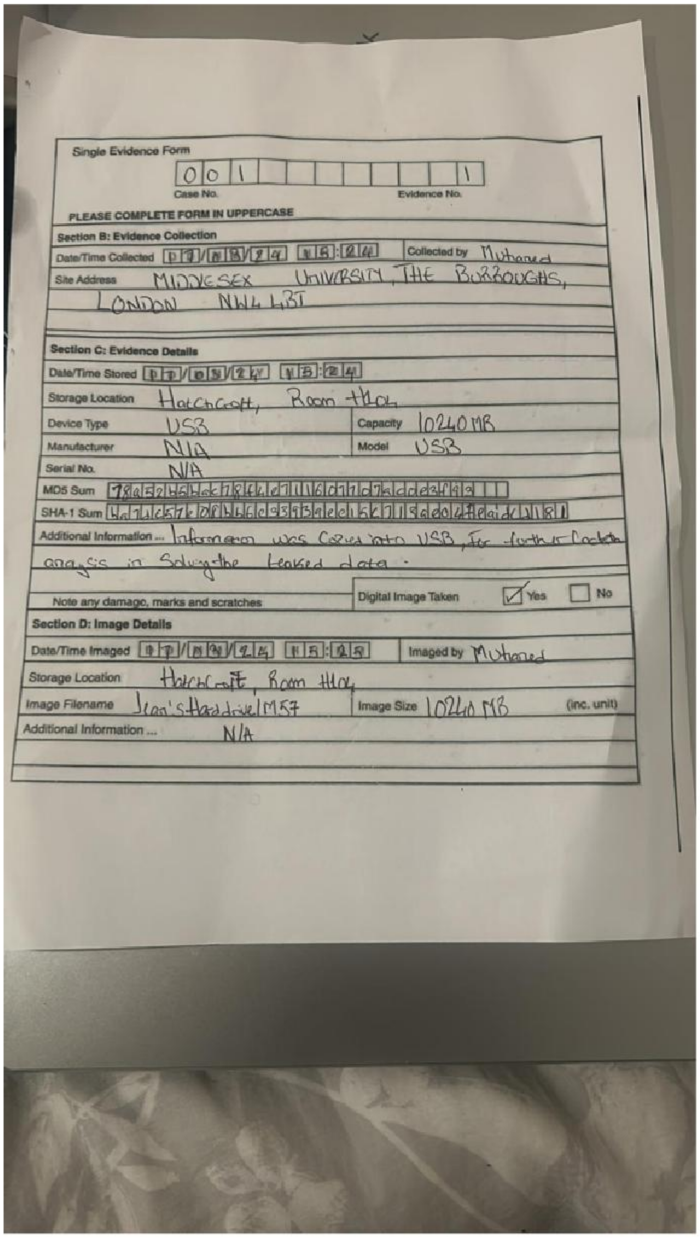
Section C: Evidence Details

Date/Time Stored 03/02/24 20:54	
Storage Location Hatchcroft, Room H104	
Device Type USB	Capacity 507MB
Manufacturer N/A	Model USB Disk 2.0
Serial No. N/A	
MD5 Sum [illegible]	
SHA-1 Sum [illegible]	
Additional Information ... Copied Information (Evidence) Into my Personal USB drive So it Can be easily accessed and Prevent loss of Information	
Note any damage, marks and scratches	Digital Image Taken ☑ Yes ☐ No

Section D: Image Details

Date/Time Imaged 03/02/24 20:54	Imaged by Muhamed
Storage Location Hatchcroft, Room H104	
Image Filename CW2-USB-Image	Image Size 507MB (inc. unit)
Additional Information ... N/A	

Form 3: Acquisition form of Hard drive



Single Evidence Form

Case No. 001 | Evidence No. 1

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected [illegible]	Collected by Muhamed
Site Address MIDDLESEX UNIVERSITY, THE BURROUGHS, LONDON NW4 4BT	

Section C: Evidence Details

Date/Time Stored [illegible]	
Storage Location Hatchcroft, Room [illegible]	
Device Type USB	Capacity 10240 MB
Manufacturer N/A	Model USB
Serial No. N/A	
MD5 Sum [illegible]	
SHA-1 Sum [illegible]	
Additional Information ... Information was Copied onto USB, For further [illegible] analysis in Solving the Leaked data.	
Note any damage, marks and scratches	Digital Image Taken ☑ Yes ☐ No

Section D: Image Details

Date/Time Imaged [illegible]	Imaged by Muhamed
Storage Location Hatchcroft, Room [illegible]	
Image Filename [illegible]'s Hard drive/M57	Image Size 10240 MB (inc. unit)
Additional Information ... N/A	