Task 02:

Digital Forensics Report

Hasnain Khan

Forensic Analysis Report:

Summary of Findings

This report outlines the results of a forensic examination into a data leak incident involving M57.biz, an online startup that curates a catalog of body art. A confidential document—specifically, a spreadsheet titled "m57plan.xls"—was discovered on a competitor's technical support forum. The spreadsheet originated from the device of the company's CFO, Jean. Digital forensic tools were used to analyze Jean's computer and the spreadsheet file itself to trace its origin and uncover how it was released without authorization. The investigation determined that Jean had unintentionally sent the file in response to a deceptive (spoofed) email. No evidence suggests that any other employees at M57.biz were involved in the leak. The report presents a detailed timeline, the forensic methods used, and suggestions to prevent future incidents.

Company Overview

M57.biz is a growing startup that recently secured $3 million in initial funding and is in the process of obtaining another $10 million. The team consists of 12 individuals, including co-founders Alison Smith (President) and Jean (CFO). There are four developers—Bob, Carole, David, and Emmy—who work remotely, with daily virtual meetings and weekly in-person gatherings. The marketing team (Gina and Harris) and the business development member (Indy) typically work from public spaces like cafes and hotels, meeting face-to-face every two weeks. Email is the primary medium for sharing and exchanging company documents.

The breach involved the unauthorized sharing of the "m57plan.xls" file on a competitor's platform. During interviews, Jean claimed Alison requested the file via email, while Alison denied both asking for and receiving the file. The investigation aimed to determine when the file was created, how it was transmitted, and whether anyone else within the company had a role in the incident.

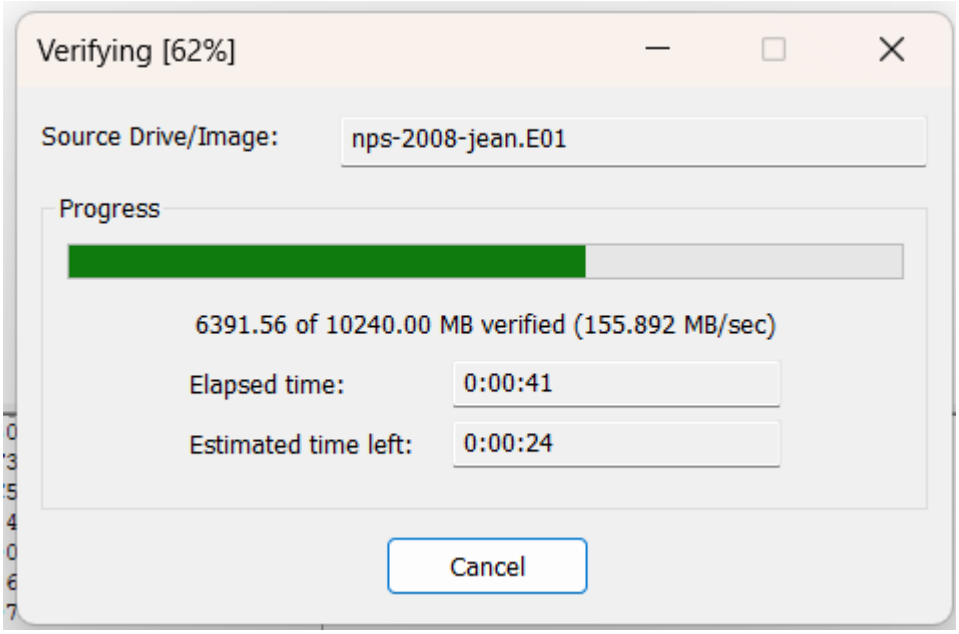
Summary of the Investigation

Specialized forensic tools such as EnCase and Autopsy were used to inspect both Jean's hard drive and the spreadsheet in question. Key discoveries include the following:

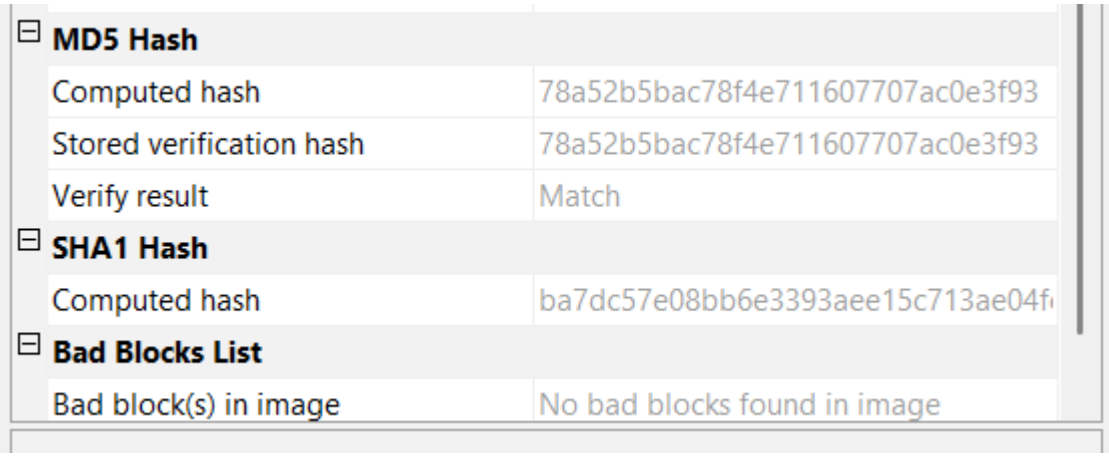
File and Disk Integrity

- An MD5 hash verification was conducted on Jean's hard drive to confirm that the data had not been modified or tampered with.

- The results showed no corruption or damaged sectors, verifying that the stored data was intact and dependable.

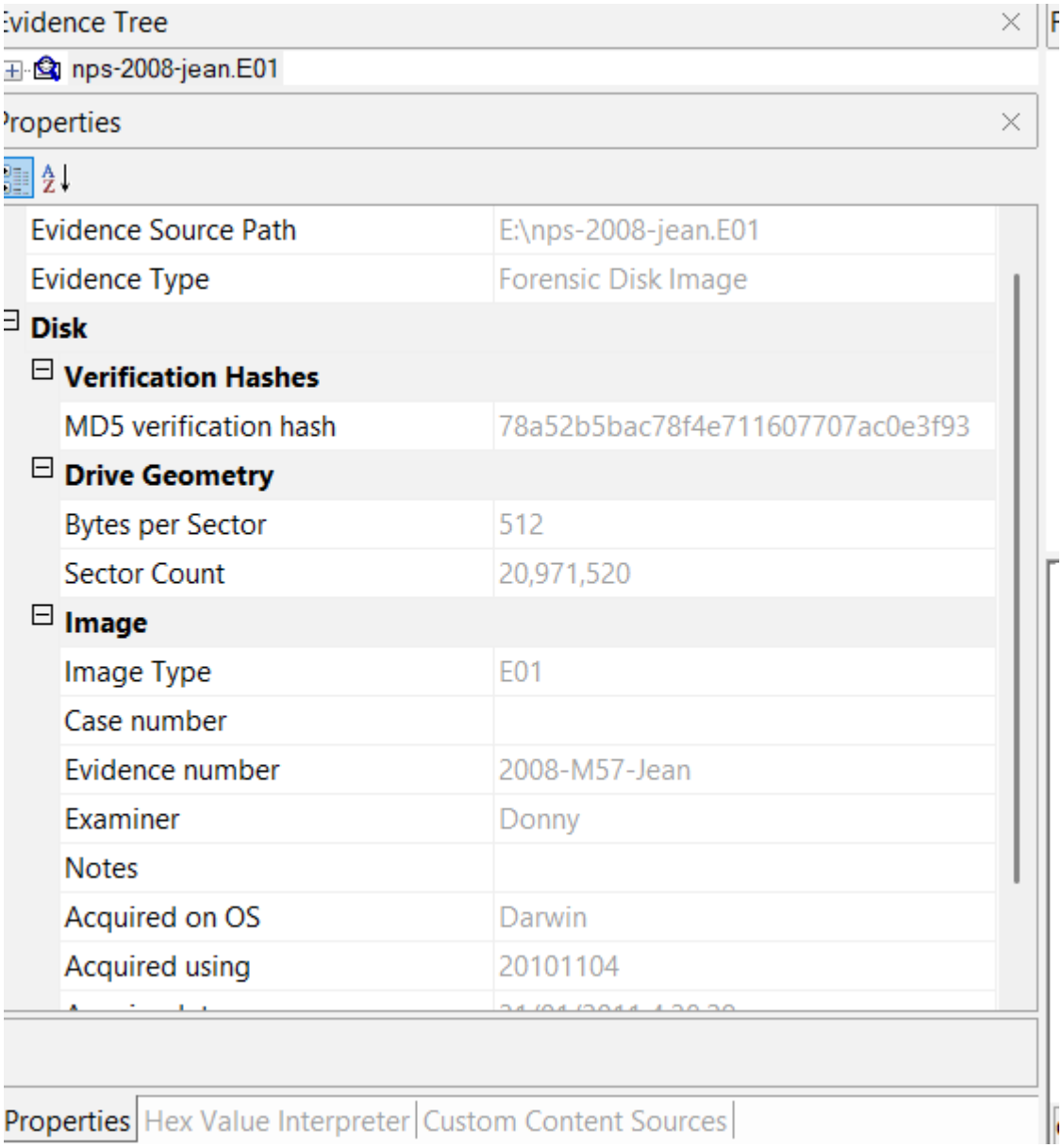


The MD5 hash verification confirmed data integrity, and no bad sectors were detected on the drive, ensuring the reliability of the stored information.

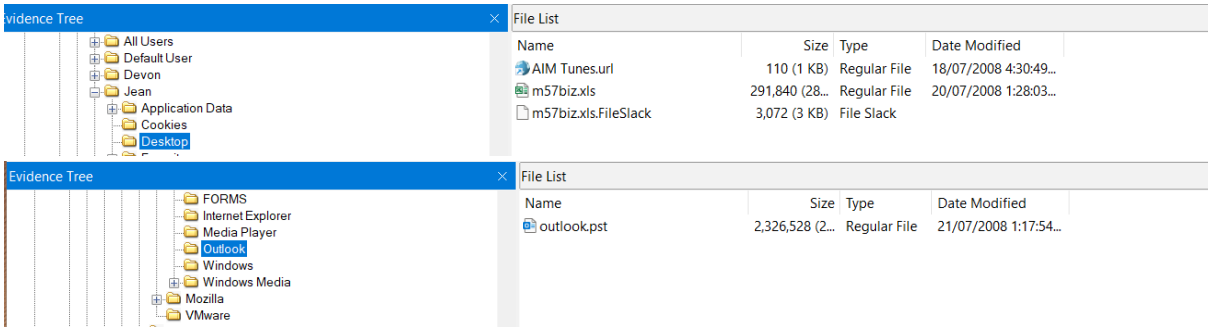


Finding the "m57plan.xls" file on Jean's desktop verified that her system was the origin of the document.

Metadata analysis of the "m57plan.xls" file indicated it was initially created on July 20, 2008, at 1:28:03 AM. Further forensic examination of timestamps may be required for more precise confirmation.



Examination of the Microsoft Outlook .pst file on Jean's computer revealed that she had sent an email containing the "m57plan.xls" attachment in response to a request, confirming the file was transmitted from her system.



Header analysis clearly confirmed that the email was spoofed, appearing to come from Alison's address (allison@m57.biz), which misled Jean into attaching and sending the file.

Transmission to Competitor's Website

It is likely that a third party, after receiving the file, uploaded it to the competitor's website. However, based solely on the analysis of Jean's system, it cannot be determined whether the upload was done directly or through an intermediary.

Employee Involvement

There is no evidence to suggest that any other employees of M57.biz—such as Alison, Bob, Carole, David, Emmy, Gina, Harris, or Indy—played a role in the breach.

The discovery that the email was spoofed clears Alison of any involvement, as she neither requested nor received the spreadsheet.

Ultimately, the root cause of the data leak was human error: Jean responded to a deceptive email without verifying its authenticity.

Event Timeline

- **July 20, 2008 – 1:28:03 AM**: Spreadsheet was created by Jean
- **July 20, 2008 – 5:39:47 AM**: Spoofed email was received by Jean
- **April 21, 2008**: File appeared on the competitor's website

Recovery Steps and Security Recommendations

1. Staff Awareness and Training

- Mandatory training should be conducted to help employees identify phishing attempts and spoofed emails, with emphasis on analyzing email headers.

2. Email Protection Mechanisms

- Implement email authentication protocols like SPF, DKIM, and DMARC to prevent spoofing.
- Deploy advanced email filters that can flag or block suspicious messages.

3. File Access and Sharing Controls

- Apply role-based access control policies and encrypt all sensitive data.
- Replace traditional email with secure file-sharing platforms for transmitting confidential documents.

4. Incident Response Strategy

- Establish a formal incident response plan.
- Perform regular security audits and reviews to identify vulnerabilities.

5. Actions After the Incident

- Notify stakeholders of the data leak.
- Request that the competitor’s website remove the unauthorized spreadsheet.
- Enhance remote work procedures and refine document handling policies.

alison@m57.biz

alison@m57.biz

20/07/2008 5:39:57 am

background checks

To: jean@m57.biz

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.

alison@m57.biz

tuckgorge@gmail.com

20/07/2008 7:22:45 am

Please send me the information now

To: jean@m57.biz

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

Jean User
jean@m57.biz
20/07/2008 7:28:47 am

RE: Please send me the information now
To: alison@m57.biz

m57biz.xls (288.51 KB)

I've attached the information that you have requested to this email message.

-----Original Message-----
From: alison@m57.biz
[mailto:tuckgorge@gmail.com]
Sent: Sunday, July 20, 2008 2:23 AM
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