Module 7: The Final Project

Vincent Gervasi

University of San Diego

27 November 2018

Abstract

This report intends to supplement the evidentiary packet submitted to the court system regarding the M57.biz organization. The report will outline the following considerations;

- Readiness - Forensic readiness is an important and occasionally overlooked stage in the examination process. Readiness will include appropriate training, regular testing and verification of their software and equipment, familiarity with legislation, dealing with unexpected issues and ensuring that the on-site acquisition (data extraction) kit is complete and in working order.
- Evaluation - The evaluation stage includes the receiving of instructions, the clarification of those instructions if unclear or ambiguous, risk analysis and the allocation of roles and resources.
- Collection - If the acquisition is to be carried out on-site rather than in a computer forensic laboratory, then this stage would include identifying and securing devices which may store evidence and documenting the scene.
- Analysis - Analysis must be accurate, thorough, impartial, recorded, repeatable and completed within the timescales available and resources allocated.
- Presentation - This stage usually involves the examiner producing a structured report on their findings, addressing the points in the initial instructions along with any subsequent instructions.
- Review - A review of an examination can be simple, quick and can begin during any of the above stages. It may include a basic analysis of what went wrong, what went well, and how the learning from this can be incorporated into future examinations. Any lessons learned from this stage should be applied to the next examination and fed into the readiness stage.

Contents

Computer Forensic Examination Report

This case revolves around confidential information in the form of personally identifiable information (PII) and salary ranges for personnel employed at M57.biz. This information was leaked from a company asset belonging to Jean an employee at M57.biz; the leaked information was later discovered to have been leaked on a competitors website.

Computer Forensics Report

The report will outline the readiness and qualifications of the investigators on the case, in addition to the evaluation, collection, and analysis of the forensic information found on the user's asset. Finally, a presentation of the findings including a final review and conclusion of the evidence found.

Readiness and Qualification

Readiness is the preparatory portion of the investigation. Investigators should be aware of procedures and policies in place for digital forensic acquisition. During forensic acquisition, investigators should utilize established forensic methodology, in combination with proven tools and software to ensure that data is preserved and is collected in a matter that is legally defensible (SANS, 2010). Readiness is not limited to the collection; readiness should include procedures that include intake of evidence into evidence lockers and computer storage, including but not limited to local storage and backup, digital jump boxes, or cloud storage or any combination of the pre-mentioned methods.

Management.

Case management, evidence handling and retention, case processing, and procedures both technical and procedural are imperative to be legally defensible. Also, forensics investigators must also be ready and capable of handling the meticulous handling of digital evidence. Part and

partial, to readiness, ensuring that software and evidence gathering tools are of the latest version and licensed properly. Analysts must be familiar with standard operating procedures (SOP), can provide, and prove a proper chain of custody (COC) (USDOJ, 2004).

M57.biz.

In the case of M57.biz, PII was leaked from corporate asset and found its way onto the internet on a competitor's website. No one is aware of any wrongdoing, only that a request for that very same data, the m57bix.xls spreadsheet was sent via email to Alison Smith president of m57.biz. Jean the Chief Financial Officer (CFO) and the asset owner claims that a request for the m57biz.xls came from Alison Smith.

Evaluation Methods

The scope of this data breach was limited to one asset the legal parameters were straightforward permission was granted by the organization to collect and evaluate the information on the asset belonging to the CFO Jean. During the interview process as mentioned earlier, it was unclear as to how the competitor gained access to the data that had been stolen. The only real information confirmed by Jean the CFO was that an email was sent to Alison, but Alison claims she never received the information. In short, our investigators would focus on email and follow the evidence to where it leads.

Collection Methods

- Collecting evidence includes the procedures below;
- Safely seize computer systems and files to avoid contamination and/or interference.
- Safely collect data and software.

- Safe and non-contaminating copying of disks and other data media.
- Review and report on data media. (Sadgune, 2017)

For the M57.biz investigation evidence was collected in the form of FTK Imager file and uploaded to the University of San Diego evidence file server. The nps-2008-jean.E01 and the nps-2008-jean.E02 file was downloaded from the USD file server to the investigator's lab computer for analysis. A copy of the file was made, and hashes were compared to ensure data integrity. Please see images 1 and 2 for hash comparison of duplicated evidence file.

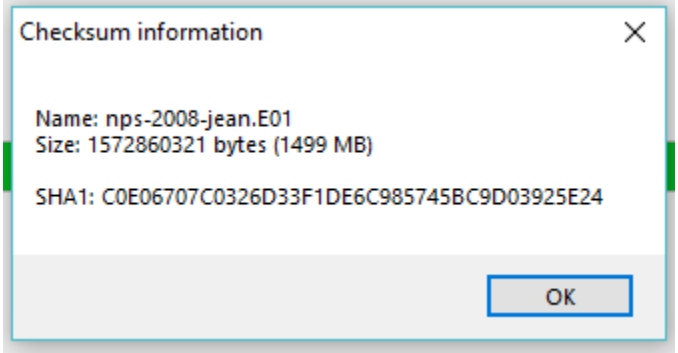


Figure 1: Original evidence file hash.

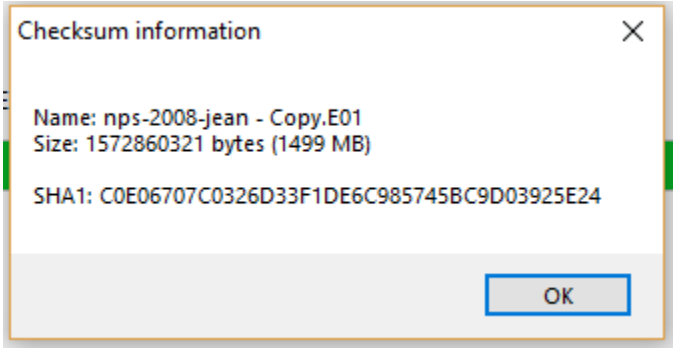


Figure 2: Copied evidence file hash.

Duplicating the file original evidence file is required to protect the integrity of the evidence for court submission. The replicated data will be the file analyzed by analysts during the investigation.

Forensic Analysis

As mentioned earlier forensic analysis was performed on the copied evidence file, to reiterate the original file remained unmolested to protect the integrity of the evidence so maintain admissibility to the courts. During the interview, it was mentioned that Jean had received an email from Alison requesting the m57biz.xls file which Alison denies ever sending the request.

The investigator began the investigation with Jean's outlook.pst file; the outlook.pst file is the email file associated with the Microsoft Outlook email client. Outlook is the interface in which m57.biz personnel communicate with for email transaction. Extracting the outlook.pst file from the copied evidence file (nps-2008-jean.E01) and viewing the evidence file with PST Viewer from Nucleus Technologies, email transactions were found between Jean and Alison.

Presentation of Evidence

Upon extracting the email from the outlook.pst file, and examining the evidence, an email was sent to Jean by Alison, or so it would seem, Alison's email had been spoofed and found to be an email from an anonymous account. The email was generated from a Gmail server, and the email domain is identified to have been a gmail.com account. Figure 3, shows email header information generated on 19 July 2008 at 6:22 PM the "from" line in the header shows alison@m57.biz email address, the "mail to" address clearly shows the email address as tuckgorge@gmail.

MIME-Version:·1.0¶
Date:·Sat,·19·Jul·2008·18:22:45·-0700·(PDT)¶
Message-ID:·<20080720012245.177343B1DA8@xy.dreamhostps.com>¶
Content-Type:·text/plain;·charset=utf-8¶
Content-Transfer-Encoding:·quoted-printable¶
X-Priority:·Normal¶
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·558838)·id·177343B1DA8;¶
→ ·Sat,·19·Jul·2008·18:22:45·-0700·(PDT)¶
Subject:·Please·send·me·the·information·now¶
TO:·jean@m57.biz¶
From:·"alison@m57.biz"·<tuckgorge@gmail.com>¶
CKX-Bounce-Address:·tuckgorge@gmail.com¶

Figure 3, Email header information.

The email timeline is presented below describing the events of when the email was sent to the threat actors email account.

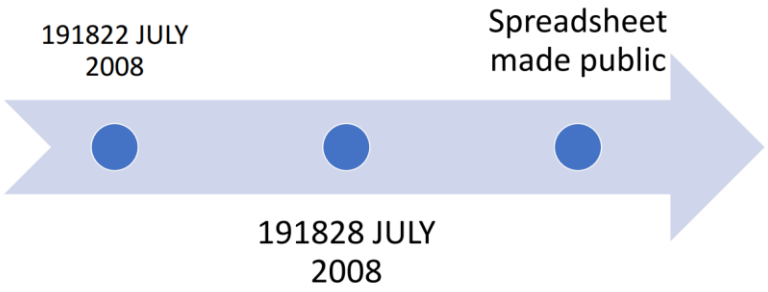
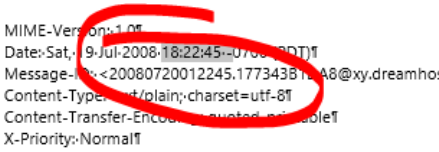


Figure 4 Timeline



MIME-Version:·1.0¶
Date:·Sat,·19·Jul·2008·18:22:45·-0700·(PDT)¶
Message-ID:·<20080720012245.177343B1DA8@xy.dreamhostps.com>¶
Content-Type:·text/plain;·charset=utf-8¶
Content-Transfer-Encoding:·quoted-printable¶
X-Priority:·Normal¶
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·558838)·id·177343B1DA8;¶
→ ·Sat,·19·Jul·2008·18:22:45·-0700·(PDT)¶
Subject:·Please·send·me·the·information·now¶
TO:·jean@m57.biz¶
From:·"alison@m57.biz"·<tuckgorge@gmail.com>¶
CKX-Bounce-Address:·tuckgorge@gmail.com¶

Figure 5 Spoofed account and "mail to" address.

```
MIME-Version: 1.0
Date: Sat, 19 Jul 2008 18:28:47 -0700
Message-ID: <NNEEKAKACNPOIIMAAIIKIECBCAAA.jean@m57.biz>
Content-Type: multipart/mixed;
    → boundary="----------080400030204090409050606"
X-Priority: Normal
To: alison@m57.biz
From: "Jean User" <jean@m57.biz>
CKX-Bounce-Address: jean@m57.biz
Subject: RE: Please send me the information now

----------080400030204090409050606
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: quoted-printable

I've attached the information that you have requested to this email message=
=2E

```

Figure 6 Header information for Jean's reply at 06:28 PM with attachment.

Review and Conclusion

After reviewing the evidence, it was clear that the data exfiltration was not malicious in intent by the CFO, Jean. Jean had sent the email upon the request of Alison, the president of the M57.biz. The spoofed not hidden very well and if Jean had not been so hasty in the reply, could have identified the email as being a phishing attempt.

It is recommended based on the evidence that the personnel of M57.biz, attend cybersecurity training to and human firewall training in addition to conducting an acceptable use class. Also, M57.biz should provide reparation to its staff and provide credit monitoring for their employees affected by the data breach. The level of severity regarding the PII posted on the open web could prove to be devastating to the affected individuals.

References;

SANS Institute (2010 January 5) "Integrating Forensic Investigation Methodology into eDiscovery" retrieved from <https://www.sans.org/reading-room/whitepapers/incident/paper/33448> on 05 December 2018

U.S. Department of Justice (USDOJ) (2004 April) "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" retrieved from <https://ole.sandiego.edu/bbcswebdav/pid-1260139-dt-content-rid-4005592_1/courses/CSOL-590-MASTER/M7/Forensic_Exam.pdf> on 30 November 2018

Sadgune, Rohit D. (2017 September 09)"Digital Forensic Checklist." Detect Defeat Cyber Threat. retrieved from <http://hackforlab.com/digital-forensic-checklist/> on 05 December 2018

Pettinari, Dave. Hackers: Computer Outlaws. Accessed December 05, 2018. http://www.crime-research.org/library/Forensics.htm.