ASSIGNMENT - 6

Examination of Jean’s Computer

11/19/2019

-ARVIND PONNARASSERY JAYAN
(aponnar1)

Examination of Evidence Item 650-457-42715-1: Hard Drive Containing the Evidence Image Copy

Introduction

A request for service was issued to conduct a digital forensic examination of the evidence image of the computer identified as belonging to Jean Jones, evidence item 650-457-42715-1, also known as nps-2008-jean.E01 and nps-2008-jean.E02. The request for examination was issued by Special Agent G. Mann to provide any and all information that suggests Jean Jones either was or was not involved in extortion, any and all information regarding the spreadsheet identified as “m57biz.xlsx” either was or was not created on the computer identified as the computer of Jean Jones and to get from the computer of Jean Jones to being published on a competitors web site and also to provide any and all information that suggests whether or not anyone else from m57.biz should be investigated in support of this criminal investigation.

The report was written by Arvind Ponnarassery Jayan, a digital forensic examiner, the examination uncovered information suggesting if there was an involvement of Jean Jones in the extortion, more information about creation and movement of the spreadsheet file “m57biz.xlsx” and possibility for investigating other users involved.

Evidence Summary

The evidence item 650-457-42715-1, also known as nps-2008-jean.E01 and nps-2008-jean.E02, was examined on the days 11/15/2019 to 11/18/2019. It should be noted that the evidence file nps-2008-jean.E02 could not be examined, this is due to the fact that the image file was not supported by the forensic tool that had been used for the examination. With the consultation from the case inspector and legal counsel the examination was proceeded and only inspected the evidence image nps-2008-jean.E01.

The information regarding the suspicious file “m57biz.xlsx” were found by checking the meta data of the the excel file on 11/17/2019. Also by going through the E-Mail messages that were sent and received by the user, one possible method for information leaking was realized. The registry files of the system and the users, and also data regarding all the users were inspected on the same day. The whole evidence image was examined, looking for other possible evidences for realizing a whole picture and also considered other possible attack vectors which helped in establishing hypothesis, following which they were tested and resolved on 11/18/2019 before returning the evidence.

The hash value that was provided in the chain of custody was “78cf 5a38 b39d cd16 c1b6 c1fa 1746 d6f5”, while the hash value obtained during the examination of the evidence was “78a5 2b5b ac78 f4e7 1160 7707 ac0e 3f93”, this mismatch was caused because only the first evidence image was used for examination.The other significant hashes include the MD5 hash of the excel file, which was found to be “e23a 4eb7 f256 2f53 e88c 9dca 8b26 a153” during the examination, this file was suspected to be leaked to the competitor company.

The evidence hard drive contains an image copy of a SYX Sytemax, computer tower, black with grey front panel with s/n 3XCD54ZX89 was released by John Anderson on 11/15/2019 at 10:00 AM to the digital forensic examiner and the same was returned on 11/18/2019 at 05:00 PM. The evidence image "nps-2008-jean.E02" could not be examined due to the standard tool used for the examination did not accept the image format. Other tools were not used for further inspection of this image since a digital examination requires usage of well-known and accepted standard tools for a legal inspection.

Examination Summary

The tools used for the examination includes Autopsy (v 4.13.0) an open source digital forensic platform for examination, RegRipper(v 2.8) an open source tool for extracting/parsing information (keys, values, data) from the Registry and presenting it for analysis, OpenStego (v 0.7.3) a steganography application that provides functionalities for embedding data and watermarking. These tools are used because of their standards and acceptance in the digital forensic community.

Autopsy was used to examine the digital evidence "nps-2008-jean.E01" and recover evidence. RegRipper was used to examine the registry files in the system and this includes SAM, Software, Security, System registry files and the NTUSER.DAT files of the users of the system. OpenStego tool was used for the purpose Steganalysis, for recovering hidden data embedded in images.

The important data present such as the E-Mail messages sent and received, the suspected excel file, the overall behavior of the user and the other relevant information regarding the files in the evidence image were found by going through the logical file system. The files that were suspected of encryption were checked for the possibility of hidden data. The data that was supposed to be deleted by the user were also inspected, since the forensic tool could recover these files from the hard disk even though the user has deleted them.

The irrelevant files such as the program files used by the Operating System, the downloads required for the the functioning of applications, etc. Sample pictures and pictures and videos with small file size were avoided from Steganalysis.

File System Examination

There were many files and directories in the evidence image that has a lot of importance:

- m57biz.xls

  This excel spreadsheet contains the confidential information like salary and SSN of the employees of the business "m57.biz". The data was found to be leaked and appeared in the competitor's website. This file can be found in the locations "/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/

Microsoft/Outlook/outlook.pst" and "/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop/m57biz.xls". The MD5 hash value of this file in both these locations are "e23a 4eb7 f256 2f53 e88c 9dca 8b26 a153". The author and the creator of the file is "Alison Smith". This file that was created by Alison on "2008-06-12" was saved to the Jeans's Desktop on "2008-07-19" and last modified on "2008-07-20". There is an absence of sufficient data to understand how Jean got this spreadsheet to begin with.

- SAM registry file:

  The SAM (Security Accounts Manager) registry file is in the location "Windows/system32/config", it was extracted and analyzed using RegRipper tool. Through the analyzes it was found that there are various other users for the same system and there is one other user other than Jean, namely Devon, who has actually accessed his/her account on the same system. The users have not changed their passwords and never had a failed attempt in logging in.

- SOFTWARE registry file:

  Similar to SAM registry file, this file is also in the location "Windows/system32/config", and contains the softwares installed and executed. During the month of July (07), it was found that the application Microsoft Office specifically EXCEL.exe software was used very recently.

- SYSTEM registry file:

  This file is also in the location "Windows/system32/config", and shows that several removable devices were attached to the system during the period of July 20 and July 21.

- E-Mail Messages:

  This folder lists all the emails present in the evidence image. This is obtained through forensic examination of the evidence using the Autopsy tool. The email messages have shed light into the actual occurrences of the events that have progressed on days July 20 and 21. The email messages include the conversation threads between the email ids jean@m57.biz, alison@m57.biz and other relevant employees, possible attackers and other non-employee users.

Analysis

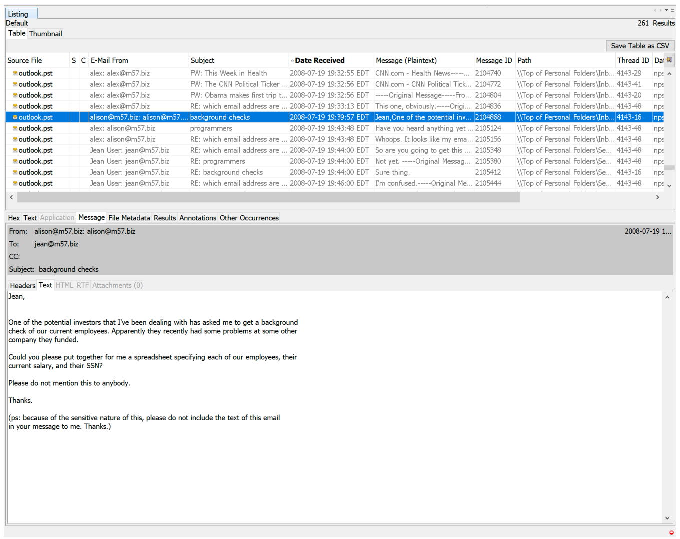
Temporal Analysis

Chronological list of relevant events:

1. From the Request for Examination, we understand that, On **5 July 2008**, Alison Smith, the President of a business known as m57.biz (M 57 dot biz) reported to law enforcement that she was receiving telephone calls from someone attempting to extort money from her in exchange for not disclosing confidential information about m57.biz to a competitor. Ms. Smith dismissed these threats as not being serious. This event and what has followed shows that m57 business was targeted by an attacker, or is a possible foreshadowing of the attack and also the attacker can be possibly an insider or an outsider.

2. At **2008-07-19 19:31:00 EDT** jean@m57.biz noticed that alison@m57.biz is sending her email under the username "alex" and sends an email suggesting the same to "alex".

3. At **2008-07-19 19:39:57 EDT**, an email from alison@m57.biz to jean@m57.biz requests her to provide the excel sheet including the SSN for background checks under the subject "background checks". No tampering or spoofing of this mail was observed, but this mail could not have come from the real alison@m57.biz since her emails are coming under the username "alex", shown in Figure 1.



Source File	S	C	E-Mail From	Subject	Date Received	Message (Plaintext)	Message ID	Path	Thread ID	Da
outlook.pst			alex: alex@m57.biz	FW: This Week in Health	2008-07-19 19:32:55 EDT	CNN.com - Health News-----...	2104740	\\Top of Personal Folders\Inb...	4143-29	nps
outlook.pst			alex: alex@m57.biz	FW: The CNN Political Ticker ...	2008-07-19 19:32:56 EDT	CNN.com - CNN Political Tick...	2104772	\\Top of Personal Folders\Inb...	4143-41	nps
outlook.pst			alex: alex@m57.biz	FW: Obama makes first trip t...	2008-07-19 19:32:56 EDT	-----Original Message-----Fro...	2104804	\\Top of Personal Folders\Inb...	4143-20	nps
outlook.pst			alex: alex@m57.biz	RE: which email address are ...	2008-07-19 19:33:13 EDT	This one, obviously.-----Origi...	2104836	\\Top of Personal Folders\Inb...	4143-48	nps
outlook.pst			alison@m57.biz: alison@m57....	background checks	2008-07-19 19:39:57 EDT	Jean,One of the potential inv...	2104868	\\Top of Personal Folders\Inb...	4143-16	nps
outlook.pst			alex: alison@m57.biz	programmers	2008-07-19 19:43:48 EDT	Have you heard anything yet ...	2105124	\\Top of Personal Folders\Inb...	4143-48	nps
outlook.pst			alex: alison@m57.biz	RE: which email address are ...	2008-07-19 19:43:48 EDT	Whoops. It looks like my ema...	2105156	\\Top of Personal Folders\Inb...	4143-48	nps
outlook.pst			Jean User: jean@m57.biz	RE: which email address are ...	2008-07-19 19:44:00 EDT	So are you going to get this ...	2105348	\\Top of Personal Folders\Se...	4143-48	nps
outlook.pst			Jean User: jean@m57.biz	RE: programmers	2008-07-19 19:44:00 EDT	Not yet. -----Original Messag...	2105380	\\Top of Personal Folders\Se...	4143-48	nps
outlook.pst			Jean User: jean@m57.biz	RE: background checks	2008-07-19 19:44:00 EDT	Sure thing.	2105412	\\Top of Personal Folders\Se...	4143-16	nps
outlook.pst			Jean User: jean@m57.biz	RE: which email address are ...	2008-07-19 19:46:00 EDT	I'm confused.-----Original Me...	2105444	\\Top of Personal Folders\Se...	4143-48	nps

From: alison@m57.biz: alison@m57.biz
2008-07-19 1...
To: jean@m57.biz
CC:
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.

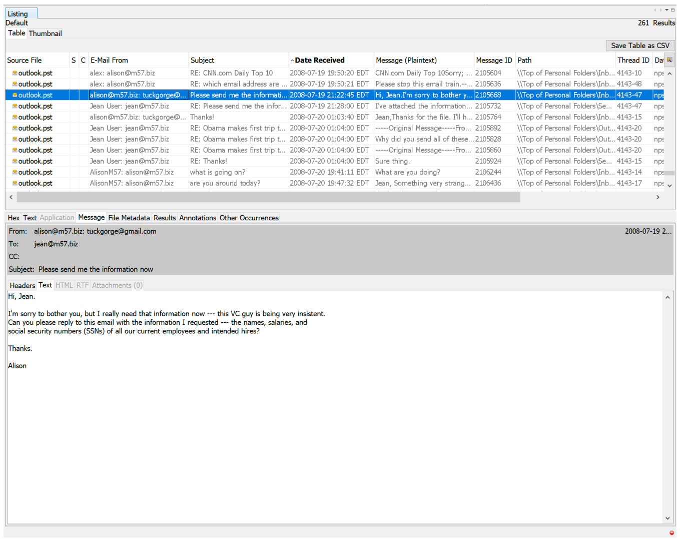
Thanks.

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

Figure 1: Original mail requesting the excel sheet; 2008-07-19 19:39:57 EDT

4. At **2008-07-19 19:43:48 EDT**, user alison@m57.biz acknowledges that the user's mail was misconfigured and notifies jean@m57.biz with the mail "`My email is alison@m57.biz, not alex. Sorry about that.`". This further indicates that previous message might not be from the real user alison@m57.biz.

5. At **2008-07-19 21:22:45 EDT**, jean@m57.biz receives another mail from alison@m57.biz, requesting for the specified document again. But here it was observed that the email id is spoofed, and the mail is actually from `tuckgorge@gmail.com`. No signs in the email messages show that Jean is aware of this miscommunication. Also it is observed that this user tuckgorge@gmail.com has never made any contact before or after this event.



Source File	S	C	E-Mail From	Subject	Date Received	Message (Plaintext)	Message ID	Path	Thread ID	Da
outlook.pst			alex: alison@m57.biz	RE: CNN.com Daily Top 10	2008-07-19 19:50:20 EDT	CNN.com Daily Top 10Sorry; ...	2105604	\\Top of Personal Folders\Inb...	4143-10	nps
outlook.pst			alex: alison@m57.biz	RE: which email address are ...	2008-07-19 19:50:21 EDT	Please stop this email train.--...	2105636	\\Top of Personal Folders\Inb...	4143-48	nps
outlook.pst			alison@m57.biz: tuckgorge@...	Please send me the informati...	2008-07-19 21:22:45 EDT	Hi, Jean.I'm sorry to bother y...	2105668	\\Top of Personal Folders\Inb...	4143-47	nps
outlook.pst			Jean User: jean@m57.biz	RE: Please send me the infor...	2008-07-19 21:28:00 EDT	I've attached the information...	2105732	\\Top of Personal Folders\Se...	4143-47	nps
outlook.pst			alison@m57.biz: tuckgorge@...	Thanks!	2008-07-20 01:03:40 EDT	Jean,Thanks for the file. I'll h...	2105764	\\Top of Personal Folders\Inb...	4143-15	nps
outlook.pst			Jean User: jean@m57.biz	RE: Obama makes first trip t...	2008-07-20 01:04:00 EDT	-----Original Message-----Fro...	2105892	\\Top of Personal Folders\Out...	4143-20	nps
outlook.pst			Jean User: jean@m57.biz	RE: Obama makes first trip t...	2008-07-20 01:04:00 EDT	Why did you send all of these...	2105828	\\Top of Personal Folders\Out...	4143-20	nps
outlook.pst			Jean User: jean@m57.biz	RE: Obama makes first trip t...	2008-07-20 01:04:00 EDT	-----Original Message-----Fro...	2105860	\\Top of Personal Folders\Out...	4143-20	nps
outlook.pst			Jean User: jean@m57.biz	RE: Thanks!	2008-07-20 01:04:00 EDT	Sure thing.	2105924	\\Top of Personal Folders\Se...	4143-15	nps
outlook.pst			AlisonM57: alison@m57.biz	what is going on?	2008-07-20 19:41:11 EDT	What are you doing?	2106244	\\Top of Personal Folders\Inb...	4143-14	nps
outlook.pst			AlisonM57: alison@m57.biz	are you around today?	2008-07-20 19:47:32 EDT	Jean, Something very strang...	2106436	\\Top of Personal Folders\Inb...	4143-17	nps

From: alison@m57.biz: tuckgorge@gmail.com 2008-07-19 2...
To: jean@m57.biz
CC:
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?

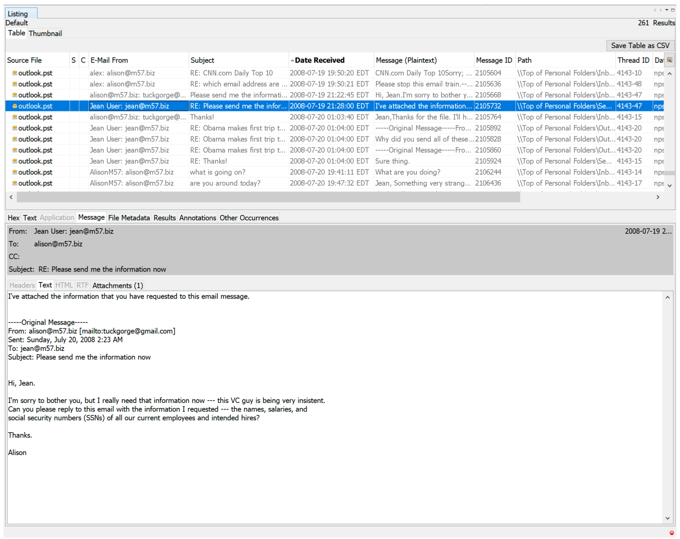
Thanks.

Alison

Listing
Default
261 Results
Table Thumbnail
Save Table as CSV
Hex Text Application Message File Metadata Results Annotations Other Occurrences
Headers Text HTML RTF Attachments (0)

Figure 2: Spoofed mail requesting the excel sheet; 2008-07-19 21:22:45 EDT

6. It is observed that jean@m57.biz replies to this spoofed email id with the excel sheet at **2008-07-19 21:28:00 EDT**.



Source File	S	C	E-Mail From	Subject	Date Received	Message (Plaintext)	Message ID	Path	Thread ID	Da
outlook.pst			alex: alison@m57.biz	RE: CNN.com Daily Top 10	2008-07-19 19:50:20 EDT	CNN.com Daily Top 10Sorry; ...	2105604	\\Top of Personal Folders\Inb...	4143-10	nps
outlook.pst			alex: alison@m57.biz	RE: which email address are ...	2008-07-19 19:50:21 EDT	Please stop this email train.--...	2105636	\\Top of Personal Folders\Inb...	4143-48	nps
outlook.pst			alison@m57.biz: tuckgorge@...	Please send me the informati...	2008-07-19 21:22:45 EDT	Hi, Jean.I'm sorry to bother y...	2105668	\\Top of Personal Folders\Inb...	4143-47	nps
outlook.pst			Jean User: jean@m57.biz	RE: Please send me the infor...	2008-07-19 21:28:00 EDT	I've attached the information...	2105732	\\Top of Personal Folders\Se...	4143-47	nps
outlook.pst			alison@m57.biz: tuckgorge@...	Thanks!	2008-07-20 01:03:40 EDT	Jean,Thanks for the file. I'll h...	2105764	\\Top of Personal Folders\Inb...	4143-15	nps
outlook.pst			Jean User: jean@m57.biz	RE: Obama makes first trip t...	2008-07-20 01:04:00 EDT	-----Original Message-----Fro...	2105892	\\Top of Personal Folders\Out...	4143-20	nps
outlook.pst			Jean User: jean@m57.biz	RE: Obama makes first trip t...	2008-07-20 01:04:00 EDT	Why did you send all of these...	2105828	\\Top of Personal Folders\Out...	4143-20	nps
outlook.pst			Jean User: jean@m57.biz	RE: Obama makes first trip t...	2008-07-20 01:04:00 EDT	-----Original Message-----Fro...	2105860	\\Top of Personal Folders\Out...	4143-20	nps
outlook.pst			Jean User: jean@m57.biz	RE: Thanks!	2008-07-20 01:04:00 EDT	Sure thing.	2105924	\\Top of Personal Folders\Se...	4143-15	nps
outlook.pst			AlisonM57: alison@m57.biz	what is going on?	2008-07-20 19:41:11 EDT	What are you doing?	2106244	\\Top of Personal Folders\Inb...	4143-14	nps
outlook.pst			AlisonM57: alison@m57.biz	are you around today?	2008-07-20 19:47:32 EDT	Jean, Something very strang...	2106436	\\Top of Personal Folders\Inb...	4143-17	nps

From: Jean User: jean@m57.biz 2008-07-19 2...
To: alison@m57.biz
CC:
Subject: RE: Please send me the information now

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

Listing
Default
261 Results
Table Thumbnail
Save Table as CSV
Hex Text Application Message File Metadata Results Annotations Other Occurrences
Headers Text HTML RTF Attachments (1)

Figure 3: sending the file to wrong user; 2008-07-19 21:28:00 EDT

7. The user tuckgorge@gmail.com responds to the email with subject "`Thanks`" at **2008-07-20 01:03:40 EDT**, confirming that the confidential information has reached an unauthorized user. This user would have posted the confidential information on the competitor's website. The user could have been part of the competitor's company, hired worker or a disgruntled employee.

8. At **2008-07-20 20:10:26 EDT**, carol@m57.biz starts an email thread regarding exposing of confidential data. Also at **2008-07-20 20:11:45 EDT**, bob@m57.biz

inquires jean@m57.biz, regarding her confidential information like SSN and salary. This email thread reveals that the confidential information was revealed on a website around **2008-07-20 20:10:20**.

9. The Request for examination states that "On about **21 July 2008 (exact date uncertain)**, Alison Smith noticed confidential information regarding m57.biz employees posted on a competitors web site. This information consists of names, Social Security Numbers, and current salary information at m57.biz.", since there were no other attack vector observed or a conclusive approach for the information to be leaked, it is highly likely that the malicious user tuckgorge@gmail.com has spoofed an email, obtained and leaked the the attached information.

Relational Analysis

The intruder could have been a disgruntled employee of m57.biz, hired attacker, or a user from the competitors's company. This malicious user, in this case tuckgorge@gmail.com, has spoofed the email id of alison@m57.biz and requested for this file enclosing the confidential information. The malicious user would have initially initiated a phishing attack of sorts to reconfigure the mail id of alison@m57.biz and send a mail to jean@m57.biz requesting for the spreadsheet. Attacker takes advantage of the confusion of the email ids and the username, and sends a spoofed email with sender id as alison@m57.biz requesting for the spreadsheet again. This is might be to obtain the reply with the attachment directly to the inbox of the malicious user. The user jean@m57.biz would have fallen for the trap and send the requested information as a reply to the malicious user, leading to the information leakage. The attacker would have then posted the same information in the competitor's website.

Functional Analysis

The capability for the attack to be performed according to the evidence is highly likely. This can be understood with the help of both the temporal and relational analysis. It is observed that at 2008-07-19 19:31:00 EDT, the email id alison@m57.biz got misconfigured, at 2008-07-19 19:39:57 EDT, jean@m57.biz receives an email from alison@m57.biz even though it was misconfigured requesting for the spreadsheet. At 2008-07-19 19:43:48 EDT, the misconfiguration was acknowledged, but the email regarding the spreadsheet was never acknowledged in the same thread. At 2008-07-19 21:22:45 EDT, jean@m57.biz receives the spoofed email, the user replies with the attachment leading to the success of the attack.

Technically the attack is feasible. A malicious user can trick the user of the email id alison@m57.biz using a phishing attack that can lead to these events. Further information should be collected regarding all the involved users especially tuckgorge@gmail.com, alison@m57.biz, for the completeness of the case, the mail servers used by the business should be examined to verify the capability of the attack.

Conclusions

- The user jean@m57.biz is responsible for sending the attachment encasing the excel spreadsheet m57biz.xls that has the confidential information like SSN and salary of the employees. But it is highly likely that the user was unaware of who the message was actually sent to. Especially since there were no evidence showing that user was aware of the fact that the user was communicating to the wrong email id.

- The spreadsheet identified as "m57biz.xls" was found in 2 locations: "/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst" and "/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop/m57biz.xls", that is in the user Jean's desktop and in an attachment in of the mail belonging to the user jean@m57.biz. The file was authored ans created by "Alison Smith" on "2008-06-12" and possibly transferred to the user Jean's desktop on "2008-07-19" and it was last modified on "2008-07-20".

- The spoofed emails from tuckgorge@gmail.com as alison@m57.biz to the user jean@m57.biz, proves that it is highly likely that the user jean@m57.biz was taken advantage in order to leak this confidential information and making it appear on the competitor's website. The attacker would have had the capacity to reconfigure the email id alison@m57.biz using a spear phishing attack and following which he uses email spoofing to obtain the required information from the user jean@m57.biz.

- From the evidence it is probable that the employees of the business m57, were not aware that they were being attacked by a malicious user. But to obtain a complete understanding of the events that have occurred, the best practice is to examine the devices of alison@m57.biz to understand more about the email misconfiguration that have occurred during the period of July 19^{th} and 20^{th} of 2008. This is to confirm how the spear phishing attack and the misconfiguration of the email id took place, to help complete the picture and remove any doubt from the user alison@m57.biz.

Examination Notes

Examiner Name: Arvind Ponnarassery Jayan **Examiner Signature:_________APJ____________**

Date	Notes
11/15/2019	
11/15/2019	I initially checked the search warrant issued for this case, case number : 650-457-42715, authorized by Honorable Joseph Albert Wapner, the Magistrate Judge.By reviewing the Search Warrant and I found it to provides sufficient legal authority to perform the requested examination.
11/15/2019	I obtained evidence image 650-457-42715-1 from Evidence Clerk John Anderson at 10:17 AM. The evidence image is an image copy of mage copy of a SYX Sytemax computer tower, black with grey front panel, s/n 3XCD54ZX89. I signed and dated the Chain of Custody (We both signed and dated the chain of custody at 10:17 AM, 11/15/2019). I reviewed the Chain of Custody and found all of the time periods in the chain to be properly accounted for. There is a minute discrepency with the file name of the images end with extension ".E01" instead of "nps-2008-jean.E01" and "nps-2008-jean.E02". The case investigator and the legal counsel were alerted of the same and they directed me to continue.
11/15/2019	I reviewed the Request for Examination document from Special Agent G. Mann. The request is signed and dated properly. The request for service was to conduct a digital forensic examination of the evidence image of the computer identified as belonging to Jean Jones.
11/16/2019	
11/16/2019	I powered on my examination system, the computer conducted a “Power On Self-Test” and computer booted without any issues.
11/16/2019	I created the following folders "C:\Users\Arvind P Jayan\Desktop\A6" and "C:\Users\Arvind P Jayan\Desktop\A6\Evidences" copied the following images nps-2008-jean.E01 and nps-2008-jean.E02 image file into the folder "C:\Users\Arvind P Jayan\Desktop\A6\Evidences".
11/16/2019	I suspended the system for the day to resume activities the following day.
11/17/2019	
11/17/2019	I started the forensic tool Autopsy v4.13.0 and created a new case file. I provided the case information, I filled the Case Name as "Jean1" and the base directory as "C:\Users\Arvind P Jayan\Desktop\A6". I provided the case number as 1000 and the Examiner Name as "Arvind P Jayan". After the database for the case was created by the tool I had to selected the option 'Disk Image or VM file' for the type of data. Then I provided the path of the data source as "C:\Users\Arvind P Jayan\Desktop\A6\Evidences\nps-2008-jean.E01". The time zone was automatically set. In the configure Ingest Modules settings, I selected to run all ingest modules and then the data source was added to the local database previousy created. I clicked finish and waited for the ingest module to run completely.

Examination Notes

Examiner Name: Arvind Ponnarassery Jayan **Examiner Signature:_________APJ____________**

11/17/2019	After the running the ingest modules, I checked the hash value of the image, it was found as 78a5 2b5b ac78 f4e7 1160 7707 ac0e 3f93, and this was cross referenced with the hash value provided in the Chain of custody, which is 78cf 5a38 b39d cd16 c1b6 c1fa 1746 d6f5. This difference was reported to legal counsel. This discrepancy must have occurred because the evidence files were split into 2 files and only .E01 was loaded for the current forensic inspection.
11/17/2019	Then I added the second evidence file using the Add Data Source tab in the left top of the tool. By clicking the option, we will repeat the process of adding the second Disk image. This time the source of the file is provided as "C:\Users\Arvind P Jayan\Desktop\A6\Evidences\nps-2008-jean.E02". But this was not possible since, Autopsy is expecting a file with an extension .E01 and not .E02, hence only the first evidence image was loaded into the Autopsy tool.
11/17/2019	I initially went to Jean's desktop which was at the Location "/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop". I found a suspicious file "m57biz.xls", which is an excel spreadsheet containing the information regarding the employees with the confidential details susch as SSN and salary of each employee. The MD5 hash of the file was e23a 4eb7 f256 2f53 e88c 9dca 8b26 a153.
11/17/2019	I inspected this file more closely. I checked the properties of the file and found that the create time for this file as "Created Time 2008-07-19 21:28:03 EDT", and this is the create time of the file in the Jean's Desktop. This cannot be blindly trusted since it can be spoofed. The excel file contians an image "image_0.png" which depicts soliers carrying the US flag. The create time of the image was Created Time "0000-00-00 00:00:00". This is not unusual since the data that is found in the evidence is not always consistent. I was able to check the meta data of the associated to the file "m57biz.xls" and found that the author and the creator of the file is "Alison Smith", I also found that Alison Smith created the file on "2008-06-12" and that it was last modified on "2008-07-20". Hence this file that was created by Alison on "2008-06-12" was saved to the Jeans's Desktop on "2008-07-19" and last modified on "2008-07-20".q
11/17/2019	Now I inspect the registry files of the image, for this I'm using the tool RegRipper V 2.8. For this I extract the SAM, system, software and security registry files from the location "Windows/system32/config" to the directories "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\sam registry", "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\system registry", "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\system registry" and "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\security registry" respectively. Then I extracted the NTUSER file from the location "Documents and Settings/Jean" to "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\ntuser registry".

Examination Notes

Examiner Name: Arvind Ponnarassery Jayan **Examiner Signature:_________APJ____________**

11/17/2019	I now inspect the SAM file extracted by running the "RegRipper tool". I first create a SAMreport .txt in the folder "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\sam registry". Then I provide the source location of the SAM file in RegRipper tool, the destination of the report is provided as "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\sam registry\SAMreport.txt", profile is set as "sam" and then I clicked “Rip It”. Now checking the SAMreport.txt (with the bigger size), I find that there are various users for this system including "Kim", "Addison", "Jean", "Abijah", "Devon" and "Sacha". But at a closer inspection, I found that the only 2 users that have accessed the system and they are Jean and Devon. Jean has accessed the system 80 times without a password fail and last login was at July 20 2008 and Devon has accessed 4 times without a password fail and the last login was at July 12 2008.
11/17/2019	I now inspect the SECURITY file extracted by running the "RegRipper tool". I first create a SECURITYreport .txt in the folder "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\security registry". Then I provide the source location of the SECURITY file in RegRipper tool, the destination of the report is provided as "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\security registry\SECURITYreport.txt", profile is set as "security" and then I clicked “Rip It”. Unfortunately, this particular report has very sparse information and perhaps is not an ideal example to look for evidence.
11/17/2019	I now inspect the SOFTWARE file extracted by running the "RegRipper tool". I first create a SOFTWAREreport .txt in the folder "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\software registry". Then I provide the source location of the SOFTWARE file in RegRipper tool, the destination of the report is provided as "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\software registry\SOFTWAREreport.txt", profile is set as "software" and then I clicked “Rip It”. It was found that during the month of July several tools related to Microsoft Office was executed.
11/17/2019	I now inspect the SYSTEM file extracted by running the "RegRipper tool". I first create a SYSTEMreport .txt in the folder "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\system registry". Then I provide the source location of the SYSTEM file in RegRipper tool, the destination of the report is provided as "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\system registry\SYSTEMreport.txt", profile is set as "system" and then I clicked “Rip It”. By going through the report it was found that several removable devices were used to connect to the system during the period of July 20 and July 21.
11/17/2019	I now inspect the NTUSER.DAT file of Jean, extracted, by running the "RegRipper tool". I first create a NTUSERreport .txt in the folder "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\ntuser registry". Then I provide the source location of the NTUSER file in RegRipper tool, the destination of the report is provided as "C:\Users\Arvind P Jayan\Desktop\A6\Registry FIles\ntuser registry\NTUSERreport.txt", profile is set as "ntuser" and then I clicked “Rip It”. The report mentions that recent files accessed at July 20 was contains the file "m57biz.xls".
11/17/2019	I repeated the process to obtian the NTUSER.DAT that is associated to the user Devon, since he also had accessed the system 4 other times. But the report did not have any mentions of the excel file in focus. This could be infered as the user Devon didn't directly have the file in his system.

Examination Notes

Examiner Name: Arvind Ponnarassery Jayan **Examiner Signature:_________APJ____________**

11/17/2019	Now I resume inspection of the image using the Autopsy tool. I extracted the image previously discovered in the excel sheet into the directory "C:\Users\Arvind P Jayan\Desktop\A6\Extract". Then I used the tool OpenStego v0.7.3, to detect the steganography in the extracted image. I suspected this due to blurriness of the picture. The tool couldnt verify whether there is an embedded data in the image.
11/17/2019	Now I inspect the E-mail Messages, and checked the messages in the default tab. I initially noticed the descrepancy regarding the email ID alison@m57.biz and the username associated with it as alex instead of alison. jean@m57.biz noticed this and send emails suggesting this descrepancy to alison@m57.biz at 2008-07-19 19:31:00 EDT, but from the replies to the thread with message IDs 2104836, 2105156, 2105348, 2105508, 2105636, we understand that there is misconfiguration and this was resolved by 2008-07-19 19:51:00 EDT. This misconfiguration could be one of the reason the events following occured. The reason for the misconfiguration
11/17/2019	I found an email from alison@m57.biz to jean@m57.biz asking her to provide the excel sheet including the SSN for background checks under the subject "background checks". This message with message ID "2104868" was sent 2008-07-19 19:39:57 EDT, and I didn't find any tampering or spoofing of the email. The user jean@m57.biz replied confirming that she will provide the data at 2008-07-19 19:44:00 EDT, the message ID was 2105412. But we by observing the timeline when mail misconfiguration has occured, we can confirm that these threads were happening parallely and some issue has happned to the mail accounts.
11/17/2019	Following this, another mail was recieved to the email id jean@m57.biz at 2008-07-19 21:22:45 EDT, from the email id alison@m57.biz, but here I observe that there is spoofing and the user tuckgorge@gmail.com has spoofed this email and sent this message masking himself as alison@m57.biz. The message id of this spoofed email is 2105668. It is observed that jean@m57.biz replies to the spoofed email, it has the message ID 2105732, and sends the excel sheet "m57biz.xls" intended for alison@m57.biz reaches tuckgorge@gmail.com. I cross referenced the MD5 hash of the file sent it was an exact match of the file present in the user's desktop, which was e23a 4eb7 f256 2f53 e88c 9dca 8b26 a153, this shows that the same file was sent as an reply without any alteration. The user tuckgorge@gmail.com replies to the mail thanking jean@m57.biz for sending her the data and asking her to keep this confidential, this message with message id 2105764 was recieved at 2008-07-20 01:03:40 EDT. Hence we can understand that the user tuckgorge@gmail.com has successfully received the confidential data.
11/17/2019	It is observed that Bob on 2008-07-20 has come across the information regarding the leak of confidential data, through email with message id 2106468. This email confirms that the data is put in the website. Carol also questions Jean with her concern of leaking confidential data on the same day, and this can be seen on the email with the message id 2107330. This confirms that the confidentail data send on the 19th was leaked on the next day that is the 20th.

Examination Notes

Examiner Name: Arvind Ponnarassery Jayan **Examiner Signature:_________APJ____________**

11/17/2019	I went through the tab "Extensions mismatched detected". I found several .bmp files, which I extracted into the folder "C:\Users\Arvind P Jayan\Desktop\A6\Extract" and tried the approach of steganalysis since these files seemed suspicious. But the results were inconclusive.
11/17/2019	I did a keyword search of "tuckgorge" to understand whether there were any previous connections, but there were only 3 mails in the search results, which shows that this the only point of contact for tuckgorge@gmail.com.
11/17/2019	I did a keyword search of "alison@m57.biz" to understand whether there relation, the mails included both professional and social content. This defines their relation as friendly.
11/17/2019	I suspended the examination system for the day to resume activities the following day.
11/18/2019	
11/18/2019	I went through the folder "Encryption Suspected" which had supected encrypted files. But these were binary files and are not actually encrypted.
11/18/2019	I went through the "Web Bookmarks", "Web Downloads"and "Web Searches" section and found nothing suspicious. It mainly included searches for albums.
11/18/2019	I went through the "Deleted Files" where recovered files are present, and checked for suspicious files, the result was inconclusive.
11/18/2019	I went through the "USB devices Attached" section and noticed that an iphone was attached at 07/10/2019, this raised a suspicion since, from the evidence list Jean had a Motorola and no iphone devices. This can be disregarded since the suspicious file was not present in the system during that time. Considering our timeline, I checked the devices that could have been attached during 07/19/2019 or after that day, I found that there were several ROOT HUBs, virtual USB Hub and a Flash Disk belonging to iCreate Technologies Corp. These were not also present in the posession of Jean and is also a possible angle in which something the user of the system could act maliciously.
11/18/2019	I went through the folder Recent in the location "/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Recent", to check the recent files accessed and nothing seems to be out of the ordinary. The recent access included inconclusive images and the excel file in focus.
11/18/2019	I went through the folder My Music and My Pictures in the location "/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/My Documents/My Music" and "/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/My Documents/My Pictures" respectively. The My Pictures folder did have different pictures, but these folders were also safe.
11/18/2019	Next I moved back to the directories in Volume 2 of the evidence image. I discovered that there was an image "Dc1.jpg" in the Location "/img_nps-2008-jean.E01/vol_vol2/RECYCLER/S-1-5-21-484763869-796845957-839522115-1004/", but it was not supicious.
11/18/2019	I went through the various Program Files, it included fairly familiar software like "Microsoft Office", "Mozilla Firefox 3 Beta", "Windows Media Player" etc and they were not suspicious.

Initials:_____APJ______________

Examination Notes

Examiner Name: Arvind Ponnarassery Jayan **Examiner Signature:_________APJ____________**

11/18/2019	I went through the folder Cookies in the location "/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Cookies", to verify if the user has visited cached any malicious cookie. There were none in my regard.
11/18/2019	I went throught the folders owned by the user Devon, and it didn’t have any suspicious data.
11/18/2019	I checked the hash value of the image and found it to be 78a5 2b5b ac78 f4e7 1160 7707 ac0e 3f93. This is an exact match before the forensic examination confirming that the inspection didn’t change any value.
11/18/2019	I shut-downAutopsy and shut-down the examination station. I returned the evidence image (650-457-42715-1) to the evidence room.
11/18/2019	<<EXAMINATION COMPLETE>>

Request for Examination

Case Number: 650-457-42715

From: Special Agent G. Mann

To: <Your Name Here>

Background Information:

On 5 July 2008, Alison Smith, the President of a business known as m57.biz ("M 57 dot biz") reported to law enforcement that she was receiving telephone calls from someone attempting to extort money from her in exchange for not disclosing confidential information about m57.biz to a competitor. Ms. Smith dismissed these threats as not being serious.

On about 21 July 2008 (exact date uncertain), Alison Smith noticed confidential information regarding m57.biz employees posted on a competitor's web site. This information consists of names, Social Security Numbers, and current salary information at m57.biz.   Ms. Smith reported this event to law enforcement and provided information that suggests the Chief Financial Officer, identified as Jean Jones, might be involved.

On 22 July 2008, an Affidavit was submitted and sworn in front of the Honorable Magistrate Joseph Albert Wapner. A Search Warrant was issued for the search of the location identified as the residence of Jean Jones. (m57.biz has a very liberal "work from home" policy, which allows many employees to conduct much of their work from their own residence. Thus, a "work computer" assigned to Jean Jones by m57.biz is maintained at the residence of Jean Jones.) Several computers were seized, including several portable hard drives.

In August 2008, a digital forensic examination was completed on the seized evidence by Forensic Examiner Dewey Cheatem. The examination produced a copy of a file identified as m57biz.xlsx. This file appears to contain a copy of the information found posted on the competitor's web site. As a result of this finding, Jean Jones was charged with extortion. In 2009, Jean Jones underwent a trial and was found guilty of extortion. She is currently serving her sentence in a federal prison.

Recently, new evidence has been identified regarding this criminal investigation. Jean Jones might be given a new trial. In support of the possibility of a new trial, a second examination of the computer belonging to Jean Jones has been requested. You are to perform another examination of the evidence copy of the computer belonging to Jean Jones. You will be asked to testify about your findings in court.

Request for Service:

Conduct a digital forensic examination of the evidence image of the computer identified as belonging to Jean Jones (evidence item 650-457-42715-1, also known as nps-2008-jean.E01 and nps-2008-jean.E02).

In a standard digital forensic examination report, provide the following information;

1. Provide any and all information that suggests Jean Jones either was or was not involved in extortion, as it relates to this investigation.

2. Provide any and all information that suggests the spreadsheet identified as “m57biz.xlsx” either was or was not created on the computer identified as the computer of Jean Jones.

3. Provide any and all information that suggests how it was possible or not possible for the spreadsheet identified as “m57biz.xlsx” to get from the computer of Jean Jones to being published on a competitor’s web site.

4. Provide and all information that suggests whether or not anyone else from m57.biz should be investigated in support of this criminal investigation.

Instructor’s note:

To be clear, you are not only expected to answer the four questions above, but you are expected to review every file within the computer system to support your conclusion. Remember, as an unbiased examiner, you should also be considering scenarios that might find the accused innocent of the charges. Thus, do a very thorough analysis of EVERYTHING. If you find an encrypted file, decrypt it! If you find suspicious emails, investigate them further. If you suspect a file of containing steganography, do what you can with it (at least mention it in your notes if you cannot find a tool to assist you.)

This is a two week assignment. Please spend two weeks on it. Make sure your notes are very detailed and very inclusive. Make sure your FTK report is perfect and all of the links work. (Review the AccessData Training manual if needed.). Make sure your written report is excellent! You will get much more out of this course if you put a great deal of effort into this assignment.

To be clear, we will be discussing how you perform this examination in class, during Moot Court. Please prepare well by doing an excellent exam and writing a perfect report.

Signature:___ **// Signed by George A. Mann //** ______ Date: **(assume a current date)**

United States District Court

Central District of Maryland

In the Matter of the Search of

(Name, address or Brief description of person, property or premises to be searched)

The residence of Jean Jones, 498 Apple Creek Lane, Pig Snout, MD 21047. A single family, single story residence, light green in color with dark green trim and natural wood ornamental window shutters. The residence is the second house south of Main St., on the east side of the street. The front door faces the west and has number 498 located to the left of it on the house.

SEARCH WARRANT

CASE NUMBER: 650-457-42715

TO: Special Agent G. Mann, and any Authorized Officer of the United States

Affidavit(s) having been made before me by Special Agent G. Mann who has reason to believe that on the premises known as the residence of Jean Jones, 498 Apple Creek Lane, Pig Snout, MD 21047, in the Central District of Maryland, is now concealed property identified as computer(s), digital storage media, digital communication equipment, and general office equipment that supports computing, storage, and/or transmission of digital data. The equipment and the data that it contains are believed to contain evidence of extortion and the transferring of data and/or documents that support extortion. The residence is identified as a single family, single story residence, light green in color with dark green trim and natural wood ornamental window shutters. The residence is the second house south of Main St., on the east side of the street. The front door faces the west and has number 498 located to the left of it on the house.

(See Attachment A)

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before 27 July, 2008 (not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search (in the daytime - 6:00 A.M. to 10:00 P.M.) (at any time in the day or night as I find reasonable cause has been established) and if the person or property be found there to seize same, leaving copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to Magistrate Joseph Albert Wapner of the Central District of Maryland, as required by law.

__ // Signed by Joseph A. Wapner //__ **___ 22 July 2008 ___________________**

Honorable Joseph Albert Wapner, US Magistrate Judge Date and Time Issued

AO 93 (Rev. 5/85) Search Warrant

RETURN

DATE WARRANT RECEIVED **22 July 2008**	DATE AND TIME WARRANT EXECUTED **22 July 2008, 10:05 AM**	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH **Jean Jones**

INVENTORY OF PERSON OR PROPERTY TAKEN PURSUANT TO THE WARRANT

Zine ZN5 Motorola Cell Phone.

SYX Sytemax computer tower, black with grey front panel, s/n 3XCD54ZX89.

200 GB Western Seagate external USB hard drive.

16 GB Kingston Data Transfer USB thumbdrive.

Two (2) DVD’s, each labeled as “m57.biz client list”.

CERTIFICATION

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

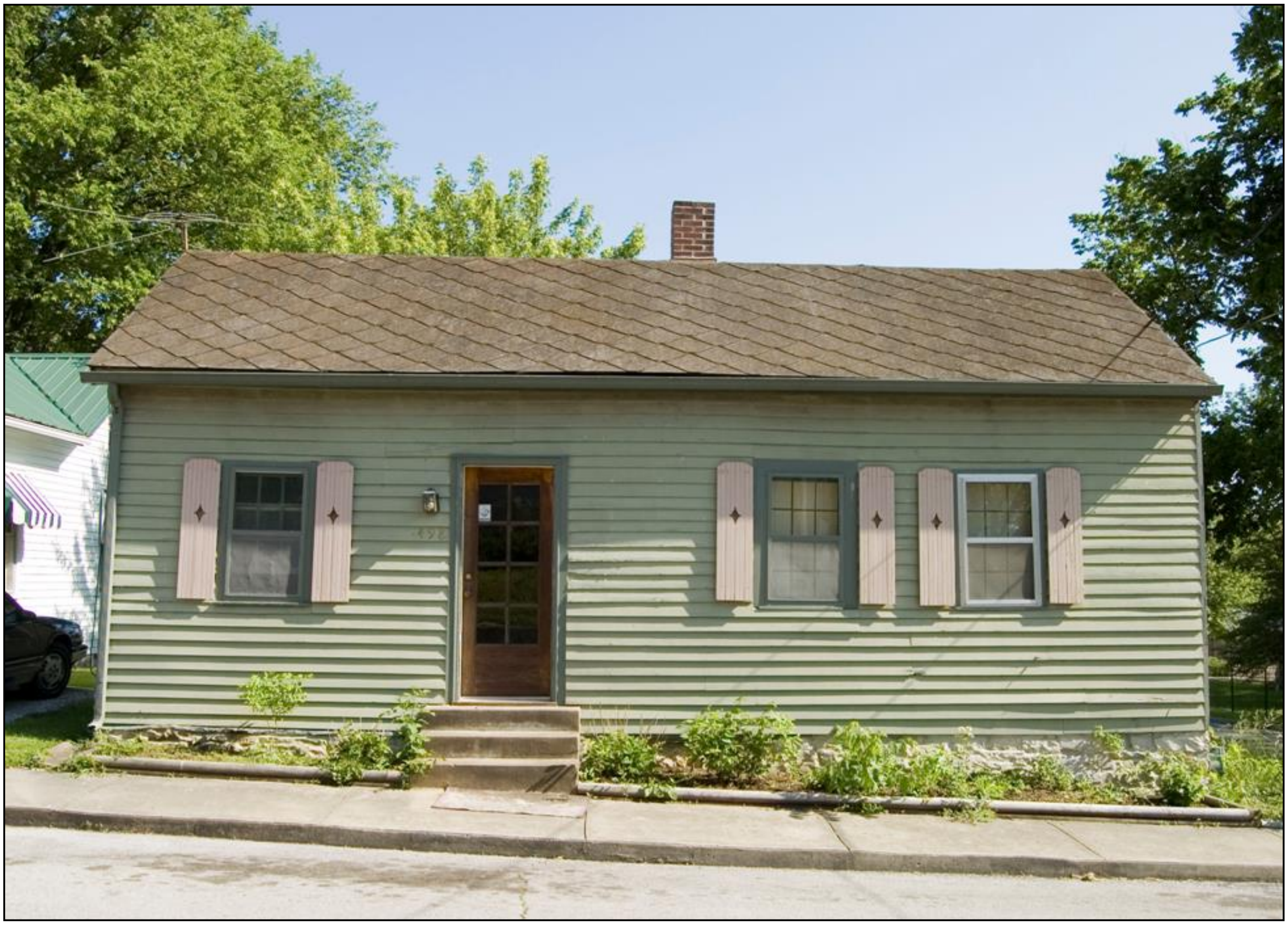
__ // Signed by George Mann // __
Special Agent G. Mann

Subscribed, sworn to, and returned before me this date.

__// Signed by Joseph A. Wapner //__
Honorable Joseph Albert Wapner, Magistrate Judge

Date: **7/22/2008**

Attachment A



Picture taken 20 June 2008 by Special Agent Ima U. Friend.

The residence of Jean Jones, 498 Apple Creek Lane, Pig Snout, MD 21047 a single family, single story residence, light green in color with dark green trim and natural wood ornamental window shutters. The residence is the second house south of Main St., on the east side of the street. The front door faces the west and has number 498 located to the left of it on the house.

Chain of Custody

Evidence Name: __ Image copy 650-457-42715-1 ______________________________
____

Evidence Description: ___ Hard drive containing an image copy of a SYX Sytemax _____
computer tower, black with grey front panel, s/n 3XCD54ZX89. The image ________
copy is identified as item 650-457-42715-1 (nps-2008-jean.E01 and _____________
nps-2008-jean.E01). The MD5 value of this image copy is ______________________
78cf 5a38 b39d cd16 c1b6 c1fa 1746 d6f5__________________________________

Received	Released
Date: 7/22/2008 Name: _____John Anderson _______ Time: 2:05 PM Signature: // Signed by John Anderson //	Date: 7/23/2008 Name: _____John Anderson _______ Time: 9:16 AM Signature: // Signed by John Anderson //
Date: 7/23/2008 Name: ___ Dewey Cheatem _______ Time: 9:16 AM Signature: // Signed by Dewey Cheatem //	Date: 8/12/2008 Name: ____ Dewey Cheatem ______ Time: 4:55 PM Signature: // Signed by Dewey Cheatem //
Date: 8/12/2008 Name: _____John Anderson _______ Time 4:55 PM Signature: // Signed by John Anderson //	Date: 8/13/2008 Name: _____John Anderson _______ Time: 9:20 AM Signature: // Signed by John Anderson //
Date: 8/13/2008 Name: ___ Dewey Cheatem _______ Time: 9:20 AM Signature: // Signed by Dewey Cheatem //	Date: 8/16/2008 Name: ___ Dewey Cheatem _______ Time: 11:56 AM Signature: // Signed by Dewey Cheatem //
Date: 8/16/2008 Name: _____John Anderson _______ Time: 11:56 AM Signature: // Signed by John Anderson //	Date:_____*_____ Name: _____John Anderson _______ Time:_____*_____ Signature: // Signed by John Anderson //
Date:__________ Name: ____________________________ Time:__________ Signature: _________________________	Date:__________ Name: ____________________________ Signature: _________________________

(* Assume this date and time is correct and that it corresponds to the date and time that John Anderson released this evidence to you.)