M57 Digital Forensics Report

Submitted By: Joel Ng, Sherwinna Chua, Aldric Chong,

Jovan Ho, Keith Tan

Examiner: Wayne Lim

A final report in partial fulfilment of the requirements of the ModularMaster in Cybersecurity (Digital Forensics)

2022

Table of Contents

1.0 Introduction

1.1 Overview

On 9th December 2009 1130am, Aaron Greene filed a police report claiming to have found Kitty exploitation movies and pictures on a computer (MT-2009-12-015-EV001). She claims to have purchased this computer from Craigslist as a secondary item. She proceeded to release the computer and upon recovering the computer, police forensics investigators determined that this computer formerly belonged to the company m57.biz.

On 10th December 2009 9.30am, Forensic tech team identified several known kitty exploitation videos on the recovered computer (MT-2009-12-015-EV001) and a possible owner, Jo Smith, who worked for the company M57 Patents. At 4.30pm, police contacted Pat McGoo, the CEO of M57 Patents who authorized the cooperation of the entire organization to assist with the investigation after speaking to a lawyer. At 5.00pm, there was a warrant (MT-2009-12-015-W0001) granted for the confiscation of the USB thumb drive owned by Jo (MT-2009-12-015-004). This thumb drive was believed to be u

We have been tasked to run an analysis for possible criminal charges and civil litigation with regards to the Kitty exploitation videos found on the computer (MT-2009-12-015-EV001). In addition, we were also tasked to find out if there were any other suspicious activities occurring in the organization based on the provided images. Regarding suspicious activities, we would classify anything related to gambling, alcohol, drugs or software which could be potentially used for malicious activities, or any executables/programs not normally found in a corporate environment as suspicious.

1.2 Executive Summary

This report includes the analysis of a Kitty exploitation case, which is analyzed by a team of investigators using mainly Magnet Axiom. The issue was first reported by Aaron Greene on 9th December 2009, where the police proceeded to retrieve the machine. It was confirmed that this machine was a corporate machine owned by user Jo Smith belonging to the company M57 Patents.

Our investigation confirms that there are Kitty exploitation pictures and videos in the aforementioned device, and have managed to trace it back to Jo Smith's personal USB, from which he transferred over to the purchased machine. We have also determined that this machine was sold by the IT administrator Terry Johnson on Craigslist. We would recommend that policies are put in place to deal with equipment disposal and to ensure that all machines when disposed are properly wiped and a proper procedure is followed to ensure that they do not compromise the company's business. To prevent future usage of corporate workstations for Kitty exploitation videos, a proper Acceptable Use Policy (AUP) should be drafted and approved, and each employee should acknowledge before being given a workstation.

Whilst conducting this investigation, several suspicious activities were found as well. One such activity was Terry Johnson, the IT Administrator installing keyloggers and capturing images and capturing the memory dumps of his colleagues' computers. While it is unclear whether such actions are illegal, we recommend the infrastructure team to come up with a list of approved software, and guidelines on how IT assistance should be provided so we can ascertain whether the VNC/Keylogging is malicious. While implementing these guidelines, we encourage the management team to follow the laws of their state as keylogging employees without their knowledge could be considered a breach of privacy in some states.

We have also discovered that the cause of Terry's actions are due to his lack of financial judgment. Depending on the budget of the company, it is encouraged that certain background checks, or hotlines be made available to employees such that they can seek help when they are facing problems, so that they do not end up harming the company for monetary benefits.

Lastly, we have also discovered that Charlie Brown is exfiltrating company patents in exchange for money. We have also noticed that he is conducting extortion on another user, Andy. We would recommend that legal action by the company to be taken if necessary based on what was lost due to the exfiltrated patents. Extortion in most states is considered illegal and necessary actions should be taken.

2.0 Forensic Examination

2.1 Tools Used

Tool	Function
Magnet Axiom 6.2.0.31	Axiom Process was used to load the memory and image files which were then processed and viewed in Axiom Examine. This was done for each of the personnel involved within this investigation. With the use of Magnet Axiom it allowed us to view system files, artifacts, etc.
Network Miner 2.7.3	Network Miner was used to analyze the network files and traffic going in and out of the company systems. When going through the network files available we were able to supplement some of the findings that were discovered through Magnet Axiom. For example, the notable email conversations that contained valuable information can also be identified within the network files.
Wireshark 3.6.2	Wireshark was used in conjunction with Network Miner to analyze network files and traffic going in and out of the company systems.

HxD 2.5.0.0	HxD was used to analyze the file “microscope1.jpg” which includes the password for decrypting the password protected zip file “01.zip”
Invisible Secrets	Invisible Secrets is a tool that was used to decrypt the steganography files found during investigation. One such file was the “astronaut1.jpg”

2.2 Evidence Acquired

Evidence Title	Evidence Type	Owners	Number of Files	Hashes(MD5)
charlie-2009-12-11.E01	Disk Image	Charlie Brown	1	a459f1aa45941ad4fa22d5cb9d35f7fc
jo-2009-12-11-002.E01	Disk Image	Jo Smith	1	17c63fd3ef3ed8b5b69c94dff2a2757f
pat-2009-12-11.E01	Disk Image	Pat McGoo	1	ccea8df1463b2adc8a9b6c8ab9563675
terry-2009-12-11-002.E01	Disk Image	Terry Johnson	1	cf383e86dc37d4d70c9ad1ce987b61be
charlie-2009-12-11.mddramimage.zip	Memory Image	Charlie Brown	1	ad652ee279bf819823818cc9b5444ff2
jo-2009-12-11.mddramimage.zip	Memory Image	Jo Smith	1	a46292ea7b5f548a04146dc6796bb88c

pat-2009-12-11.mddramimage.zip	Memory Image	Pat McGoo	1	773992cc4055352b5f498a726f1e1cfe
terry-2009-12-11.mddramimage.zip	Memory Image	Terry Johnson	1	c51f633ae9a6035601766c714357f83d
charlie-work-usb-2009-12-11.E01	Disk Image	Charlie Brown	1	8c23941655b3313f4a31a1a66085be86
jo-favorites-usb-2009-12-11.E01	Disk Image	Jo Smith	1	8cdc12e30af14e19533c58b3ffe840b5
jo-work-usb-2009-12-11.E01	Disk Image	Jo Smith	1	f9408bfcd292a7d8d60928a42806046f
terry-work-usb-2009-12-11.E01	Disk Image	Terry Johnson	1	941997b1b9e7a1217351d483c12dc29b
Multiple pcap Files zipped	Network Capture	Multiple users	49	A15CA7E2A823DC1B915751B6172DD756

2.3 Examination Preparation

On 7th September 2022 00:00:00 GMT+8, all files mentioned above were downloaded onto a secure storage device which was previously forensically wiped by Investigator Joel Ng, who proceeded to verify that all the MD5 hashes were correct when compared with the original evidence.

Subsequently, the files were then immediately distributed to each individual investigator Keith Tan, Sherwinna Chua, Aldric Chong, Jovan Ho who each proceeded to copy the files onto their own devices which they are conducting forensics on. They have also verified that the MD5/SHA1 hash is the same as the ones which were provided originally. All image files were processed with Magnet Axiom Process / Magnet Axiom Examine. All network files were processed with Network Miner, after being unzipped with Gunzip.

2.4 Role Delegation

The investigation was conducted mostly in pairs, with each person being the main investigator and the partner for peer review. Each investigator also verified that their Magnet Axiom version was the same as well as verifying all MD5/SHA1 hashes before they began their investigation.

Type Of Evidence	Details	Main Investigator	Co-Investigator
Drive/Memory Images	Jo Smith	Keith Tan	Jovan Ho
Drive/Memory Images	Terry Johnson	Joel Ng	Keith Tan
Drive/Memory Images	Pat McGoo	Aldric Chong	Sherwinna Chua
Drive/Memory Images	Charlie Brown	Jovan Ho	Aldric Chong

Network Files	All	Keith Tan	Joel Ng Sherwinna Chua Aldric Chong Jovan Ho

2.5 Personnel Under Investigation

Name	Designation	Remarks
Aaron Greene	Incident Reporter	Claims that the computer in question was purchased on the secondary market
Jo Smith	Patent Engineer	Previous owner of computer in question
Terry Johnson	IT Administrator of M57 biz	Maintains all IT equipment
Pat McGoo	CEO of M57 biz	Authorized full cooperation
Charlie Brown	Patent Engineer	Fellow Colleague of Jo Smith

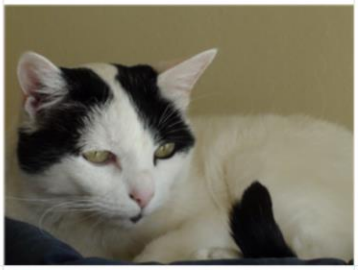
2.6 Evidence Cases

2.6.1 Jo's Case

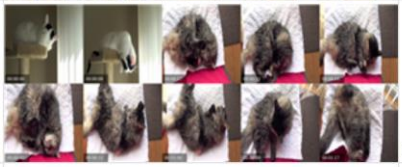
From detective investigations reports we have identified that Jo has Kitty exploitation pictures and movies. So we have decided to further our investigation starting with Jo's computer. There are 3 devices that Jo comes into contact with, his own desktop computer, work USB and his 'favourites' USB.

In investigating Jo's case, Axiom is used to load the evidences namely jo-2009-12-11.mddramimage, jo-2009-12-11.E01, jo-favourites-usb-2009-12-11.E01 jo-work-usb-2009-12-11.E01. The investigation led to the uncovering of evidence linking Jo and the Kitty exploitation pictures and movies.

The investigation started by first building media files to find evidence of Kitty exploitation pictures and videos. The screenshot below shows the evidence found on the Desktop. We can also see that the Kitty exploitation was created on Jo's Desktop from UTC+00 12/11/2009 4:37:23 PM to 12/11/2009 4:37:27 PM. These images were subsequently deleted from the source.

ecord	Tags	Comments	Category	Image	File Name	File Extensior	Created Date/Time - UTC+00:00 (M/d/	Last Ac
1	Evidence				hr_patent49.JPG	.JPG	12/11/2009 4:37:23 PM	12/11/2
2	Evidence				hr_patent50.JPG	.JPG	12/11/2009 4:37:23 PM	12/11/2
								

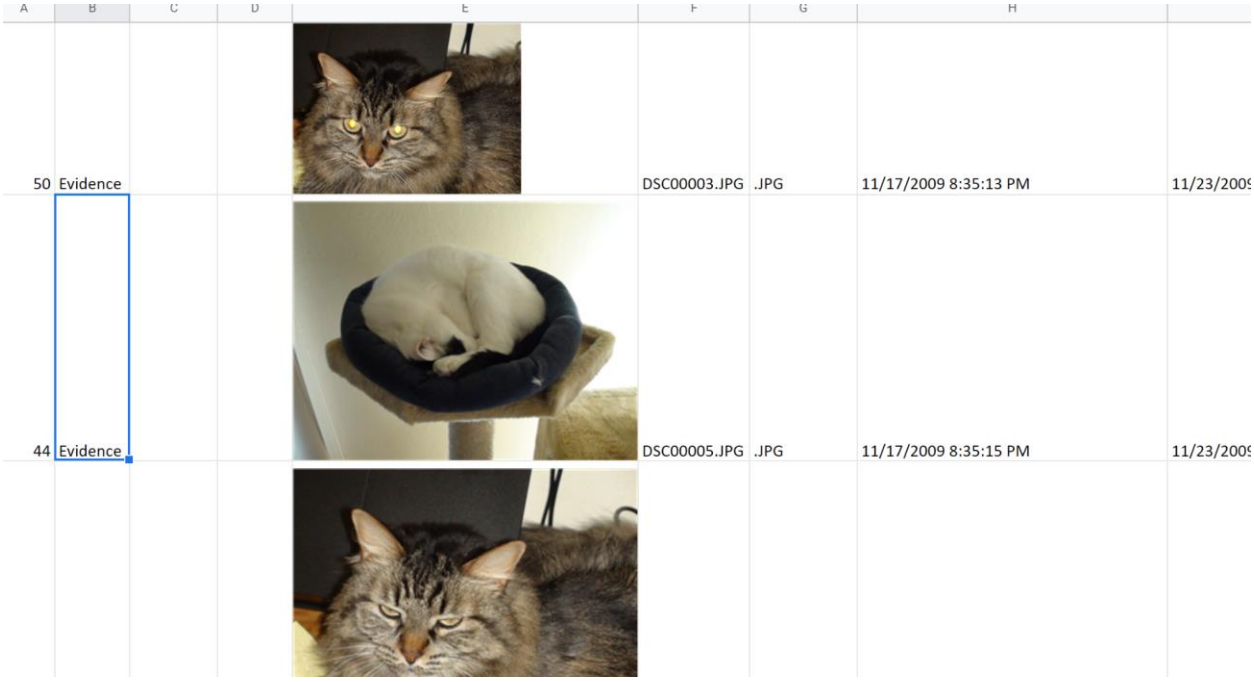
There were also Kitty videos that were found on his Desktop. They were created from 12/11/2009 4:37:28 PM to 12/11/2009 4:37:30 PM at Jo and they were subsequently deleted.

A	B	C	D	E	F	G	H
Record	Tags	Comments	Category	Image	File Name	File Extensior	Created Date/Time - UTC
1	Evidence				Cat.mov	.mov	12/11/2009 4:37:28 PM
2	Evidence				KittyMontage.mov	.mov	12/11/2009 4:37:30 PM

Next, we look into Jo's work USB. We find several encrypted images and videos on the USB. However, we have yet to find a way to decrypt these files in the work USB. The screenshot below shows a portion of the list of encrypted files in the work USB.

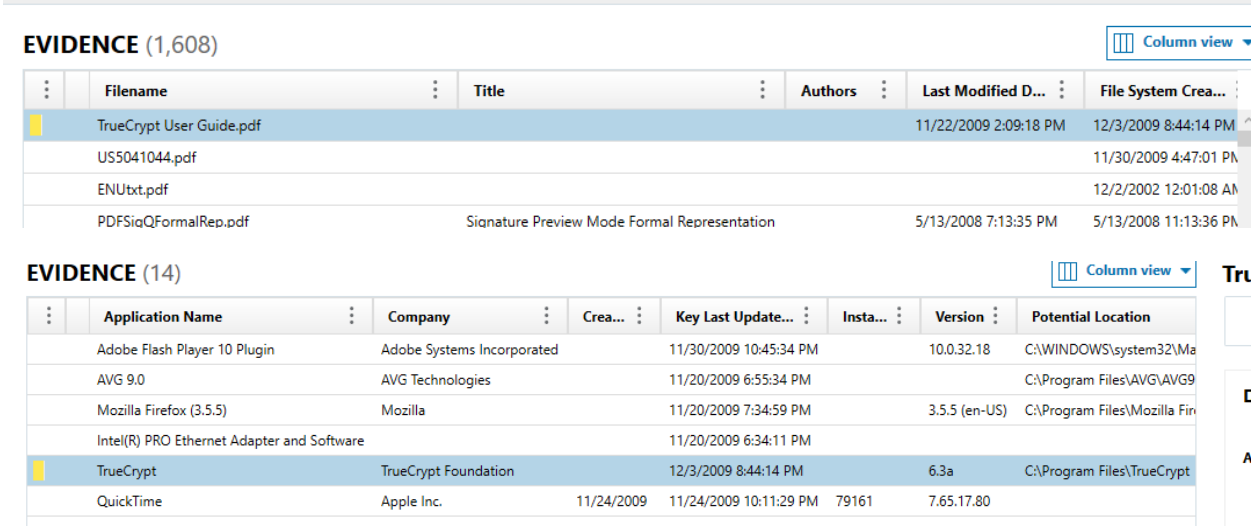
Tags	Comments	Image	File Name	File Extensior	Created Date/Time - UTC+00:00 (M/d/	Last Accessed Date/Time - UTC+0
		[Error Rendering Image]	σSC00009.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00010.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00012.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00011.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00015.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00017.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00016.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00014.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00020.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00018.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00019.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00021.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00025.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00022.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00024.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00023.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM
		[Error Rendering Image]	σSC00013.JPG	.JPG	11/20/2009 1:36:24 PM	11/19/2009 4:00:00 PM

Investigation into Jo's 'favourites' USB we see the earliest inception of the kitty exploitation pictures and movies. These are dated from 11/17/2009 8:35:13 PM to 11/17/2009 8:36:37 PM. The screenshot below shows a snippet of the images and videos found. The Kitty exploitation pictures and videos were likely transferred from his 'favourites' USB.



The full collection of evidence from his 'favourites' USB will be attached in the appendix of the report.

Within Jo's Desktop we find that there are some other files of interest, such as the TrueCrypt encryption software. There was also a TrueCrypt user guide found on his Desktop which indicated that he might have learnt how to use this encryption software to possibly encrypt the files on his work USB. The screenshots below show evidence of the TrueCrypt software on his Desktop.



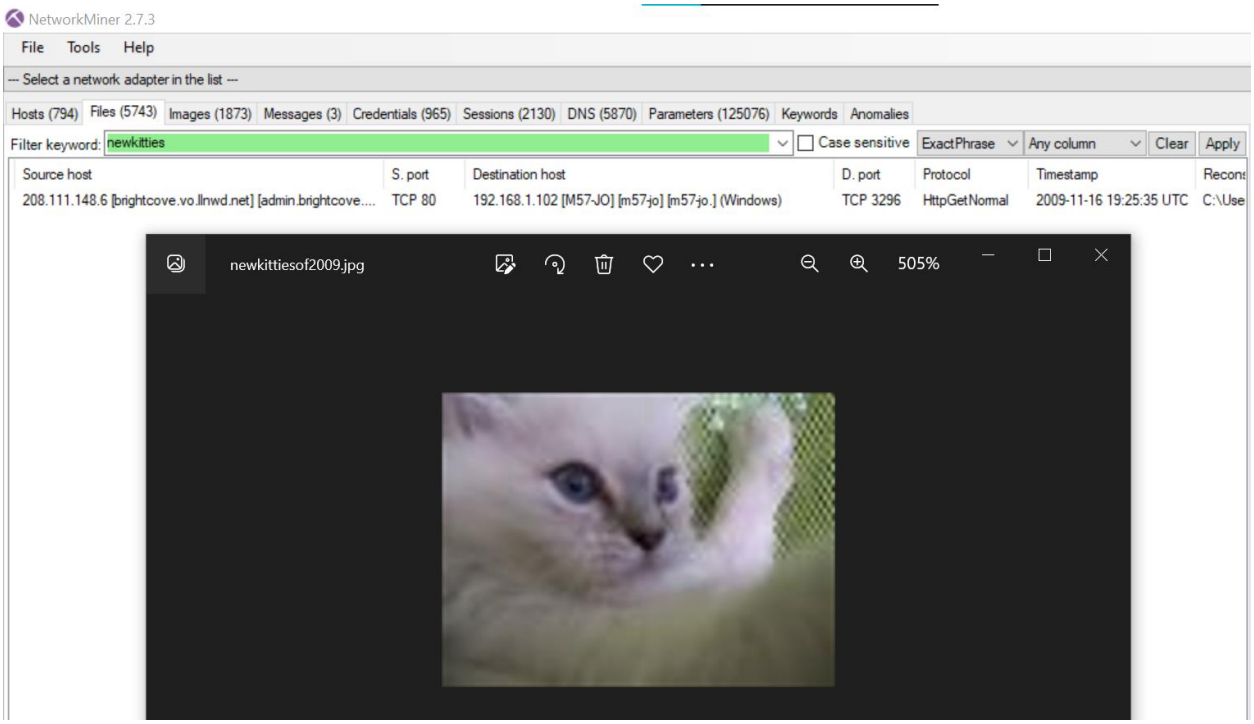
EVIDENCE (1,608) — Column view

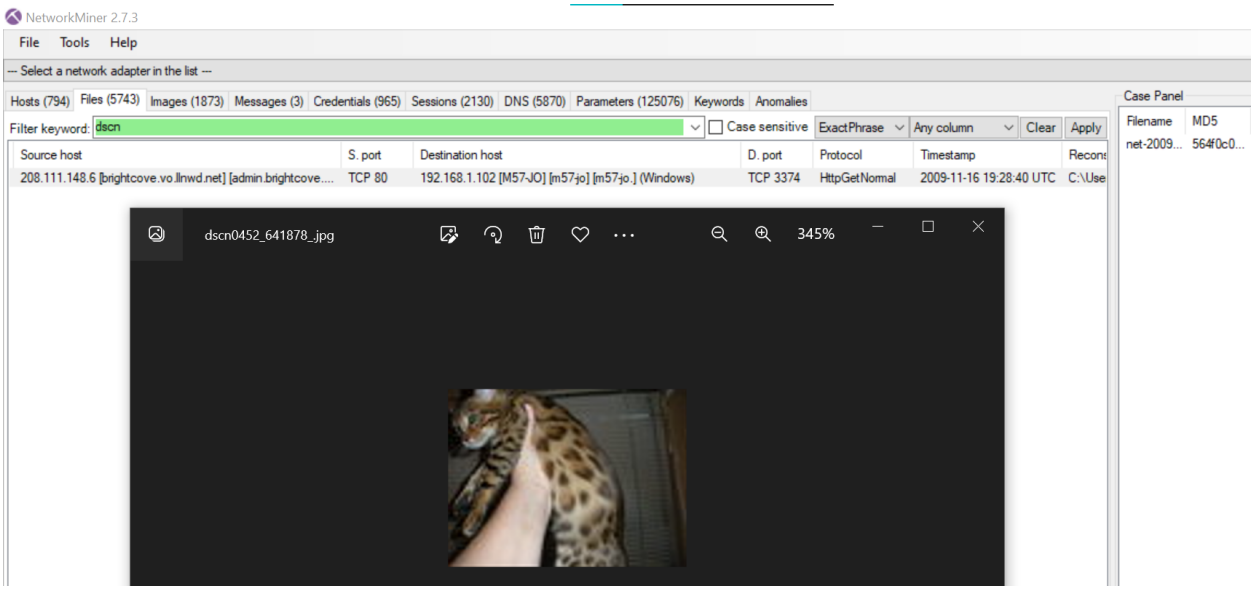
Filename	Title	Authors	Last Modified D...	File System Crea...
TrueCrypt User Guide.pdf			11/22/2009 2:09:18 PM	12/3/2009 8:44:14 PM
US5041044.pdf				11/30/2009 4:47:01 PM
ENUtxt.pdf				12/2/2002 12:01:08 AM
PDFSigQFormalRep.pdf	Signature Preview Mode Formal Representation		5/13/2008 7:13:35 PM	5/13/2008 11:13:36 PM

EVIDENCE (14) — Column view

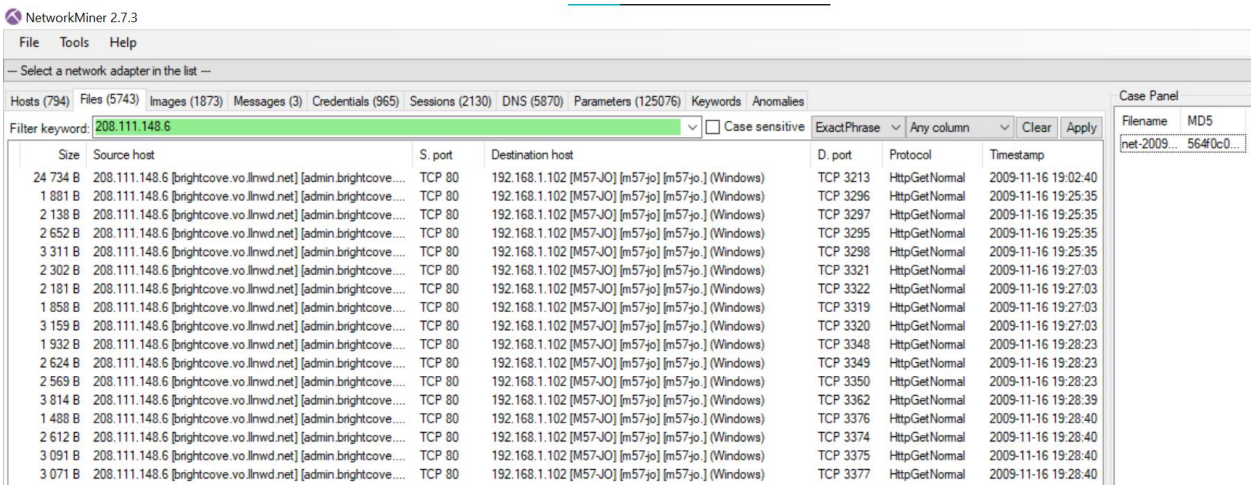
Application Name	Company	Crea...	Key Last Update...	Insta...	Version	Potential Location
Adobe Flash Player 10 Plugin	Adobe Systems Incorporated		11/30/2009 10:45:34 PM		10.0.32.18	C:\WINDOWS\system32\Ma
AVG 9.0	AVG Technologies		11/20/2009 6:55:34 PM			C:\Program Files\AVG\AVG9
Mozilla Firefox (3.5.5)	Mozilla		11/20/2009 7:34:59 PM		3.5.5 (en-US)	C:\Program Files\Mozilla Fir
Intel(R) PRO Ethernet Adapter and Software			11/20/2009 6:34:11 PM			
TrueCrypt	TrueCrypt Foundation		12/3/2009 8:44:14 PM		6.3a	C:\Program Files\TrueCrypt
QuickTime	Apple Inc.	11/24/2009	11/24/2009 10:11:29 PM	79161	7.65.17.80	

In addition, we find Jo downloaded kitty exploitation videos over the internet from 208.111.148.6, as seen from our NetworkMiner analysis:





Upon further investigation, we notice Jo has downloaded from the same IP address multiple times. However, not all of the downloads are kitty exploitation-related, some of them seem like harmless pictures. Despite this, he uses different TCP ports each time, presumably to evade detection by his sys admin. Therefore further investigation may be needed to check whether his other downloads are really harmless or not.

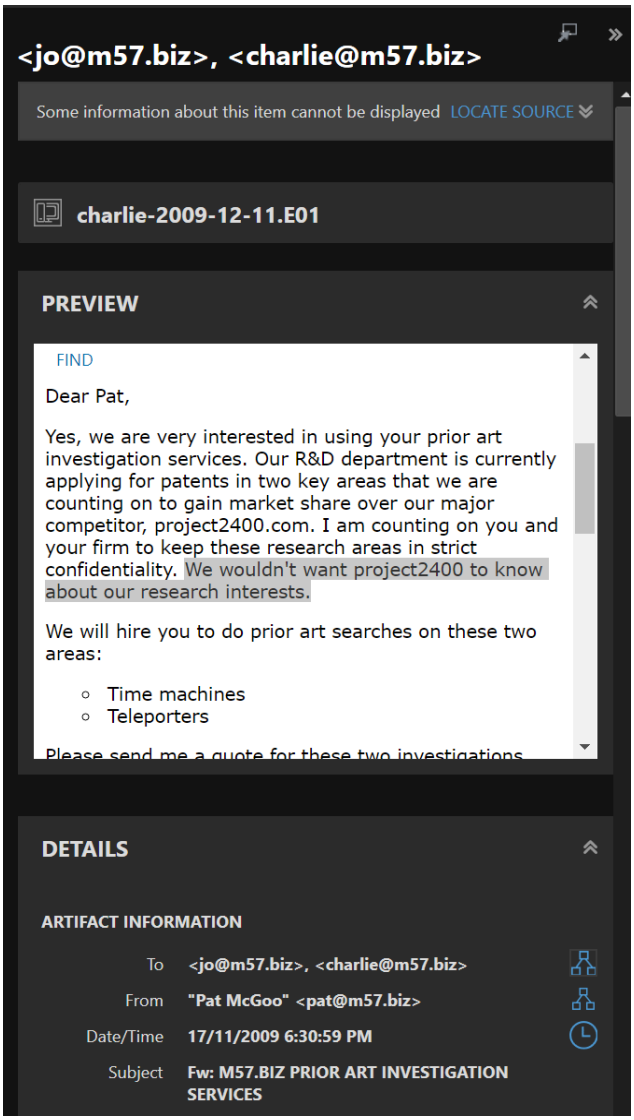

NetworkMiner 2.7.3
File
Tools
Help
-- Select a network adapter in the list --
Hosts (794)
Files (5743)
Images (1873)
Messages (3)
Credentials (965)
Sessions (2130)
DNS (5870)
Parameters (125076)
Keywords
Anomalies
Filter keyword:
208.111.148.6
Case sensitive
ExactPhrase
Any column
Clear
Apply
Case Panel
Filename
MD5
net-2009...
564f0c0...
Size
Source host
S. port
Destination host
D. port
Protocol
Timestamp
24 734 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3213 HttpGetNormal 2009-11-16 19:02:40
1 881 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3296 HttpGetNormal 2009-11-16 19:25:35
2 138 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3297 HttpGetNormal 2009-11-16 19:25:35
2 652 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3295 HttpGetNormal 2009-11-16 19:25:35
3 311 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3298 HttpGetNormal 2009-11-16 19:25:35
2 302 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3321 HttpGetNormal 2009-11-16 19:27:03
2 181 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3322 HttpGetNormal 2009-11-16 19:27:03
1 858 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3319 HttpGetNormal 2009-11-16 19:27:03
3 159 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3320 HttpGetNormal 2009-11-16 19:27:03
1 932 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3348 HttpGetNormal 2009-11-16 19:28:23
2 624 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3349 HttpGetNormal 2009-11-16 19:28:23
2 569 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3350 HttpGetNormal 2009-11-16 19:28:23
3 814 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3362 HttpGetNormal 2009-11-16 19:28:39
1 488 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3376 HttpGetNormal 2009-11-16 19:28:40
2 612 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3374 HttpGetNormal 2009-11-16 19:28:40
3 091 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3375 HttpGetNormal 2009-11-16 19:28:40
3 071 B 208.111.148.6 [brightcove.vo.llnwd.net] [admin.brightcove.... TCP 80 192.168.1.102 [M57-JO] [m57-jo] [m57-jo.] (Windows) TCP 3377 HttpGetNormal 2009-11-16 19:28:40

2.6.2 Charlie's Case

In investigating Charlie's case, Axiom is used to load all three pieces of evidence namely charlie-2009-12-11.mddramimage, charlie-2009-12-11.E01, charlie-work-usb-2009-12-11.E01. The investigation led to uncovering 2 cases of suspicious activities concerning Charlie. Both cases are as listed below:

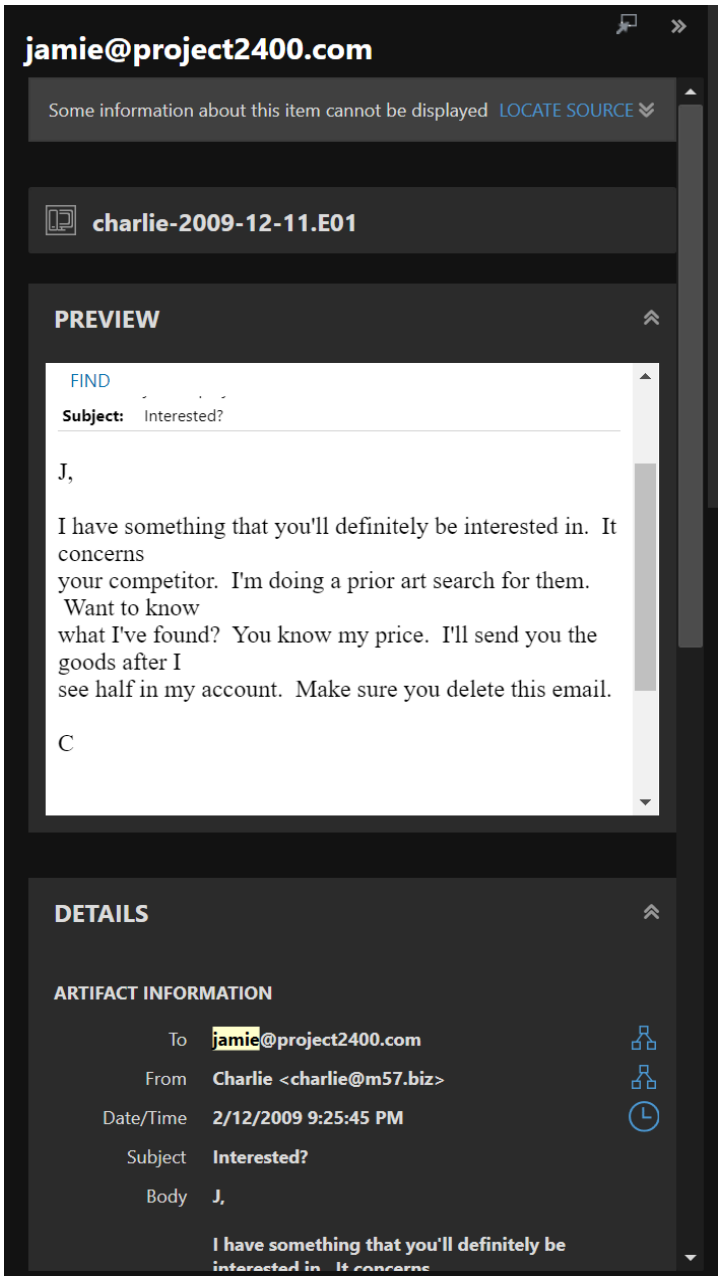
1. Charlie selling Nitroba's (M57's client) patent to Project2400 (Nitroba's competitor) for profit

    1.1. On 11-17-2009, Charlie is informed of Nitroba's interest and engagement with his company, M57.BIZ, for prior art investigation services through the forwarded email from Pat (Fw: M57.BIZ PRIOR ART INVESTIGATION SERVICES). Figure 1 below detailed down the Email by Alex, CEO of Nitroba, to express interest in Charlie's company and highlighted the need to be discreet with Nitroba's research interest, particularly against their competitor project2400.



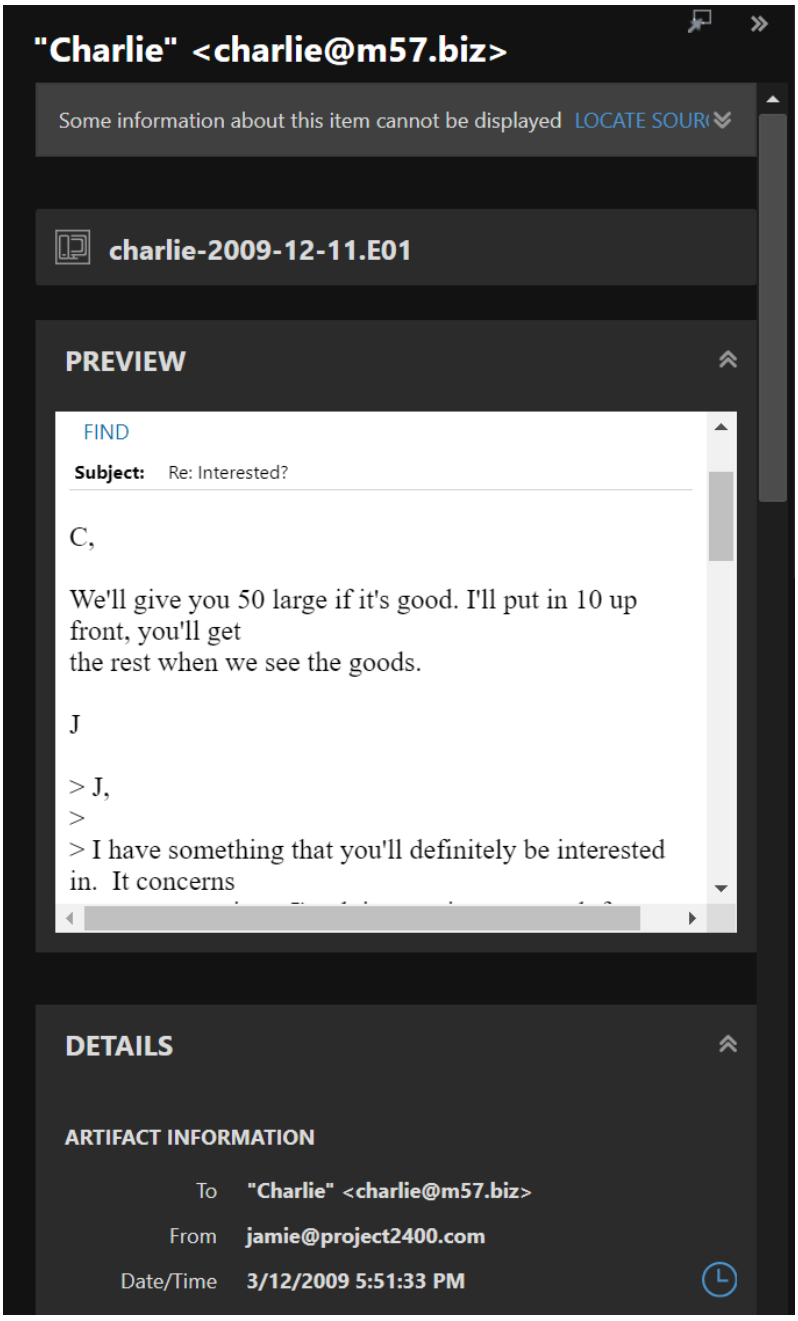
2.3.2. Figure 1: Charlie is informed of Nitroba's engagement with M57.biz and their concern with project2400

1.2 On 12-2-2009, Charlie emailed a recipient ("Jamie") with the email address jamie@project2400.com for sale of something of interest to Jamie. From the statement "You know my price" it seems that this is not the first time Charlie is engaging in such sales.



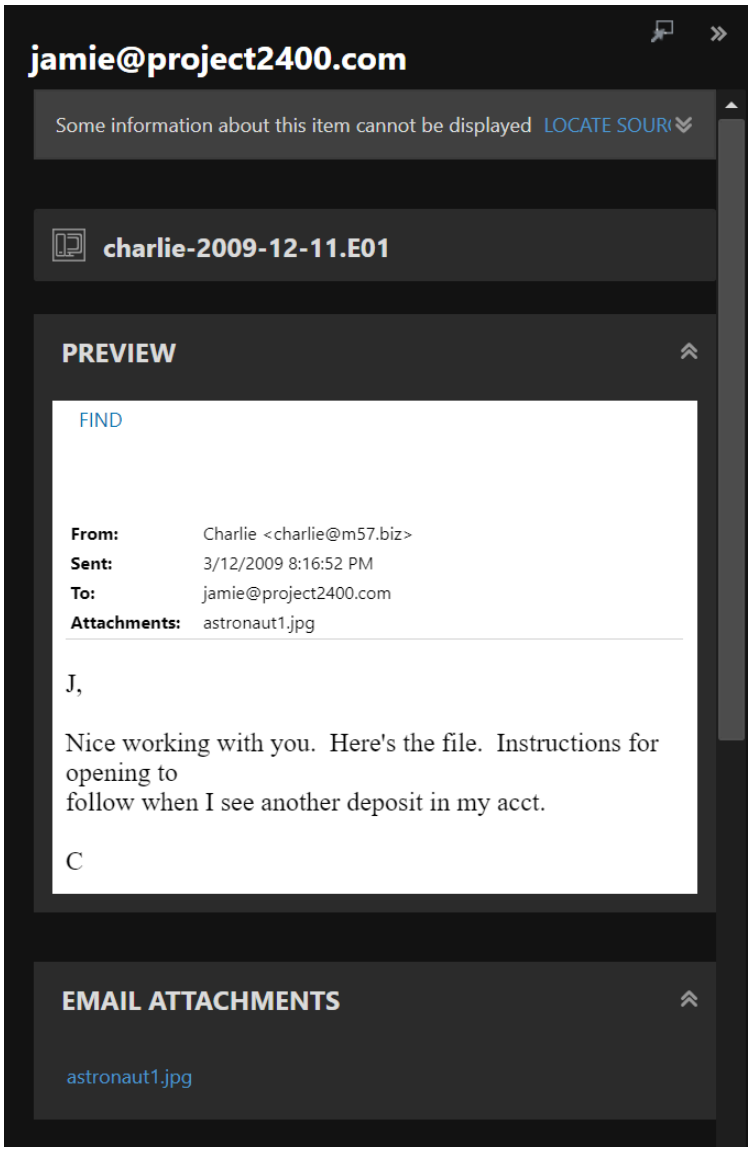
2.3.2. Figure 2: Initial contact with Jamie

1.3 On 3-12-2009, Jamie replied to Charlie expressing interest with upfront payment being made as shown in Figure 2.3.2. Figure 3.



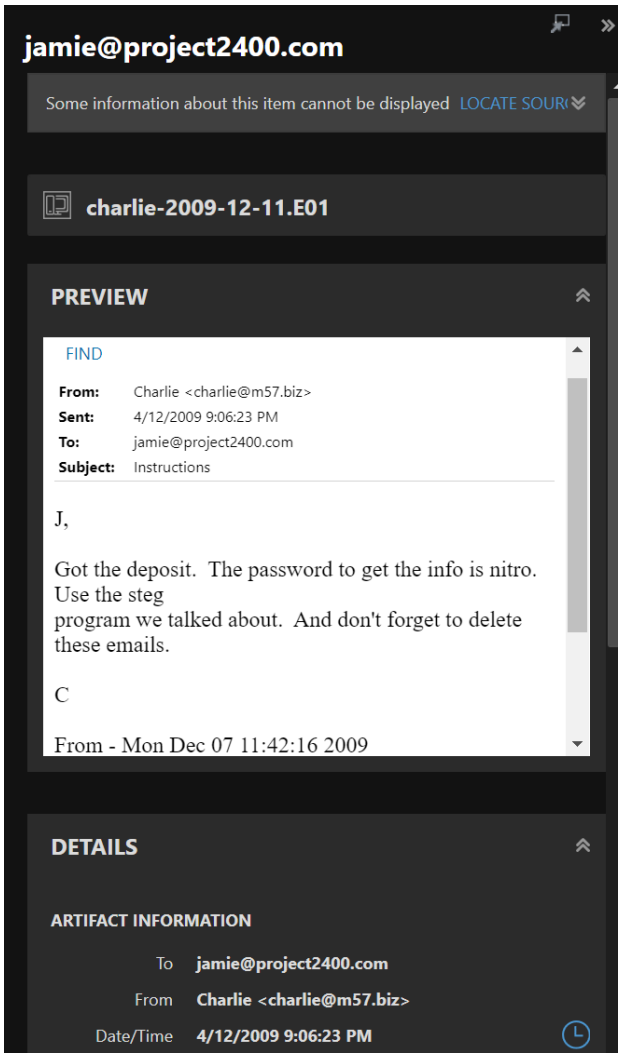
2.3.2. Figure 3: Jamie expresses interest with upfront payment

1.4 On the same day, 12-3-2009, Charlie replied to Jamie with an Email attachment named astronaut1.jpg with the instructions given to Jamie to open on receipt of another deposit.



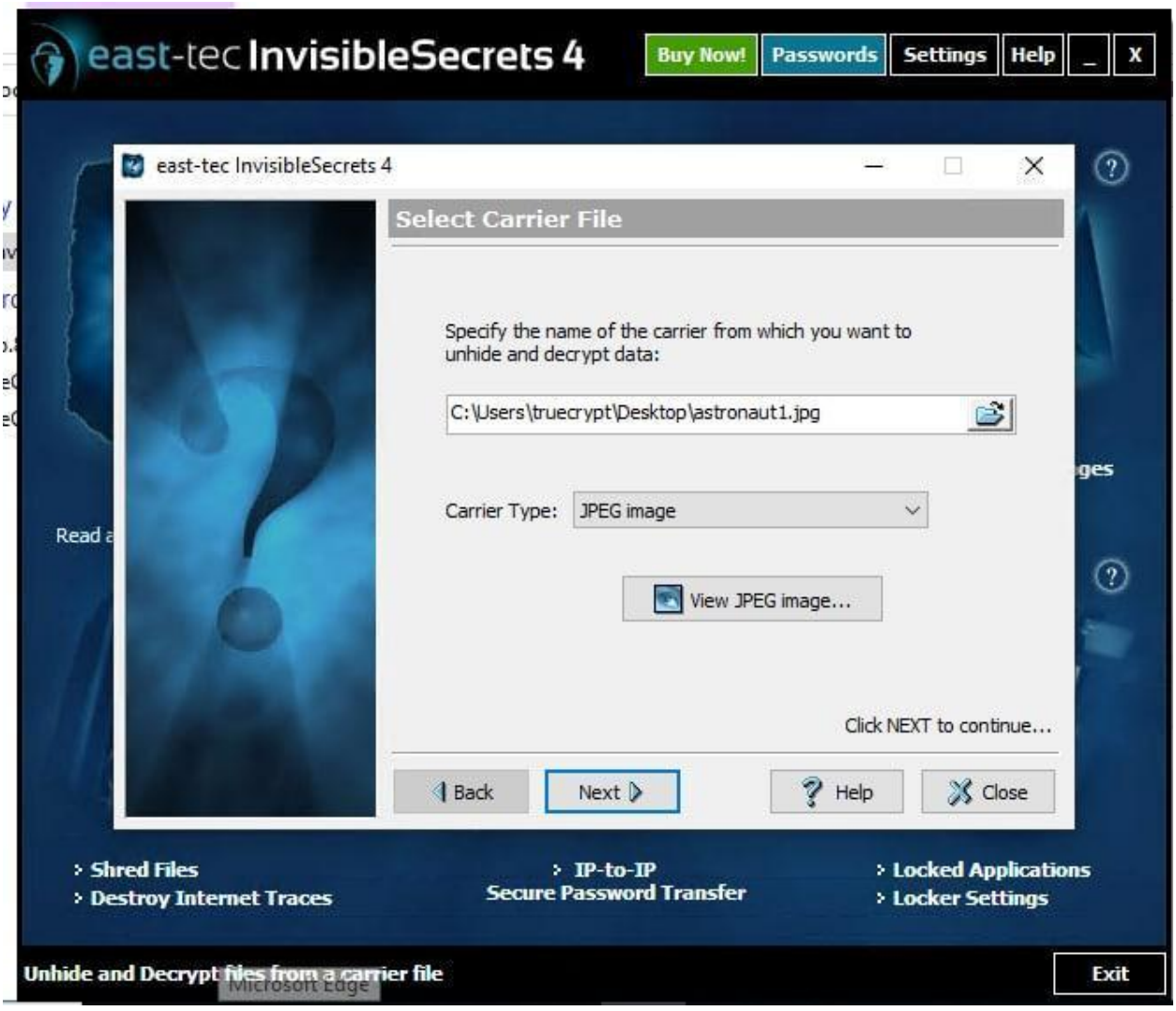
2.3.2. Figure 4: File sent to Jamie with request for another deposit

1.5 On 12-4-2009, Charlie replied to Jamie with the Email subject named as "*Instructions*" where the password to decrypt the initial astronaut1.jpg is given as "*nitro*" after confirmation of payment from Jamie.

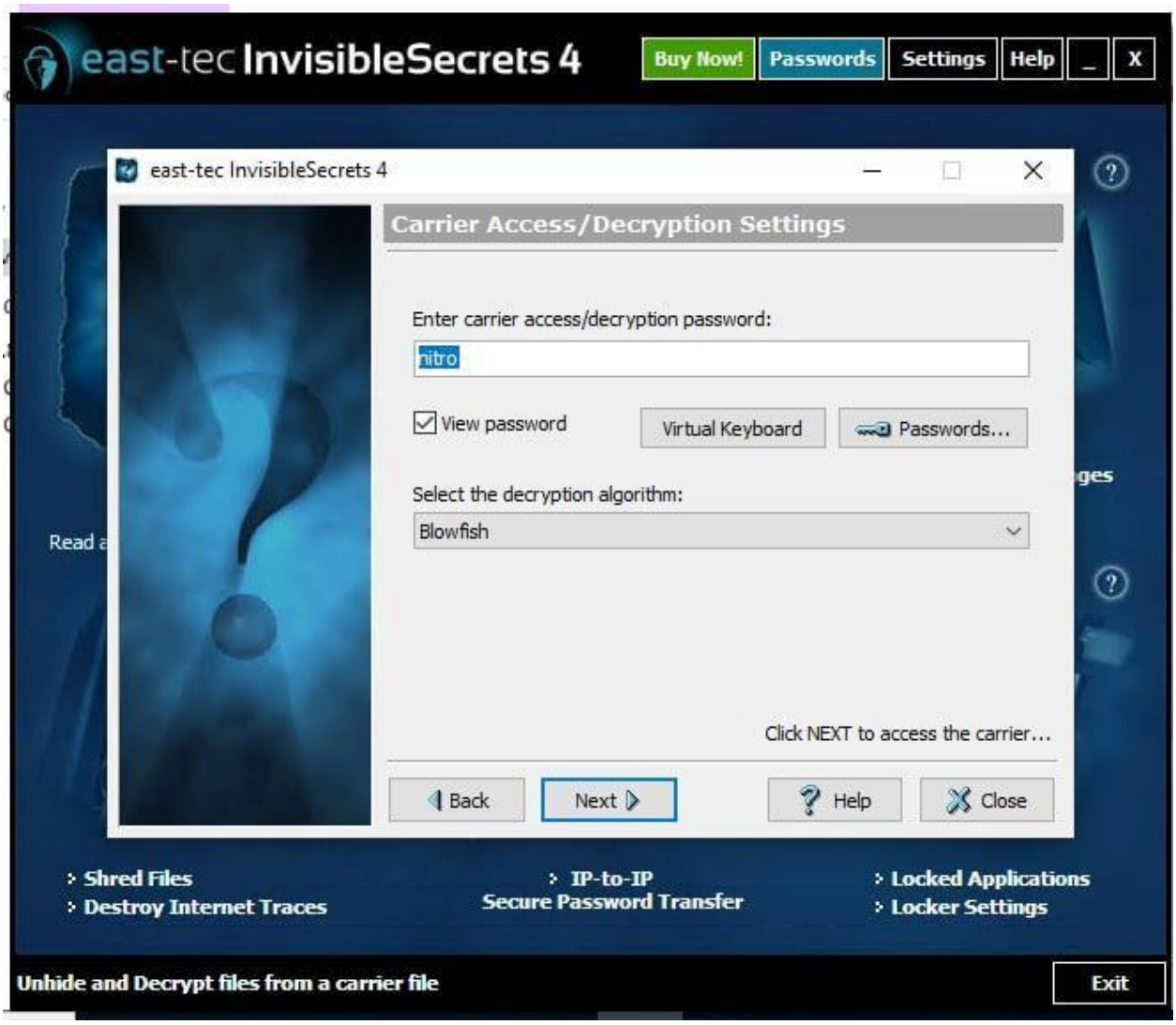


2.3.2. Figure 5: Password given to Jamie to decrypt after receiving payment

1.6 From the given evidence and password received, we were able to decrypt the astronaut1.jpg (MD5 hash: 45eade24b3a89b21fed303310ccbdc54) using the software InvisibleSecrets 4 with password set as "*nitro*" and decryption algorithm chosen as "*Blowfish*". This produced the odt file, "*Nitroba work.odt*" (MD5 hash: 56fd56fc40b7c6d7b7572711f863bc8d), which was sold to Jamie as seen in Figure 9. The detailed decryption process is shown from Figure 6 to 8 below.

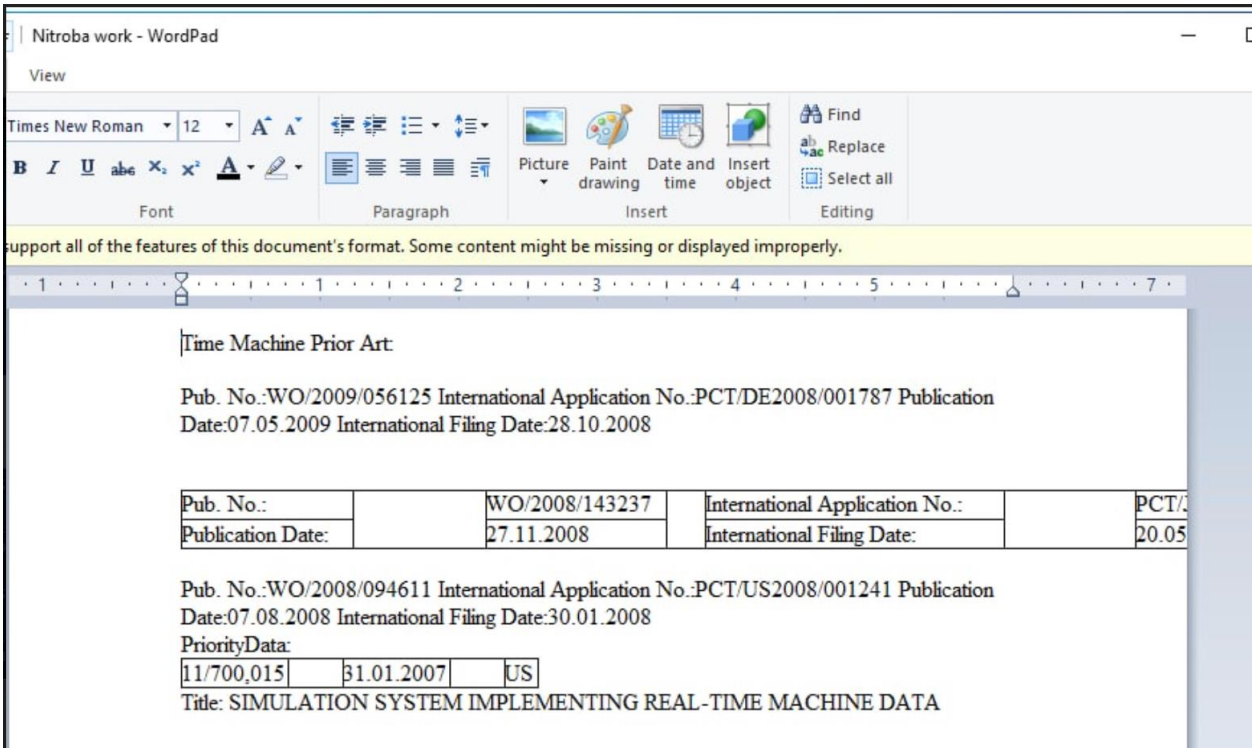


2.3.2. Figure 6: Loading astronaut1.jpg into InvisibleSecrets



2.3.2. Figure 7: Entering decryption password as "*nitro*" and decrypting algorithm as "*Blowfish*"

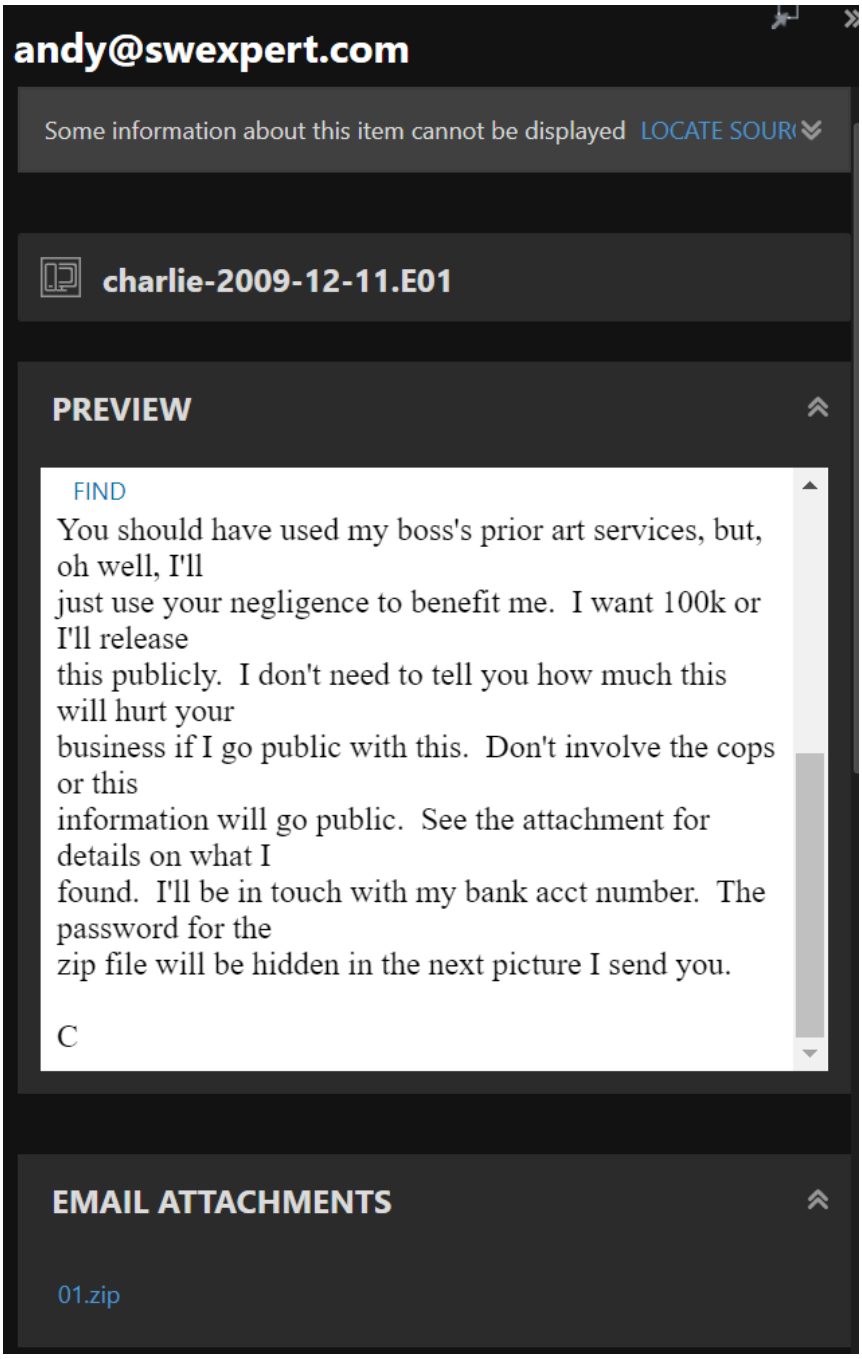
2.3.2. Figure 8: Unhide the file Nitroba work.odt



2.3.2. Figure 9: Decrypted patent (Nitroba work.odt) that is sold by Charlie to Jamie

2. Extortion case amounting to 100 thousand

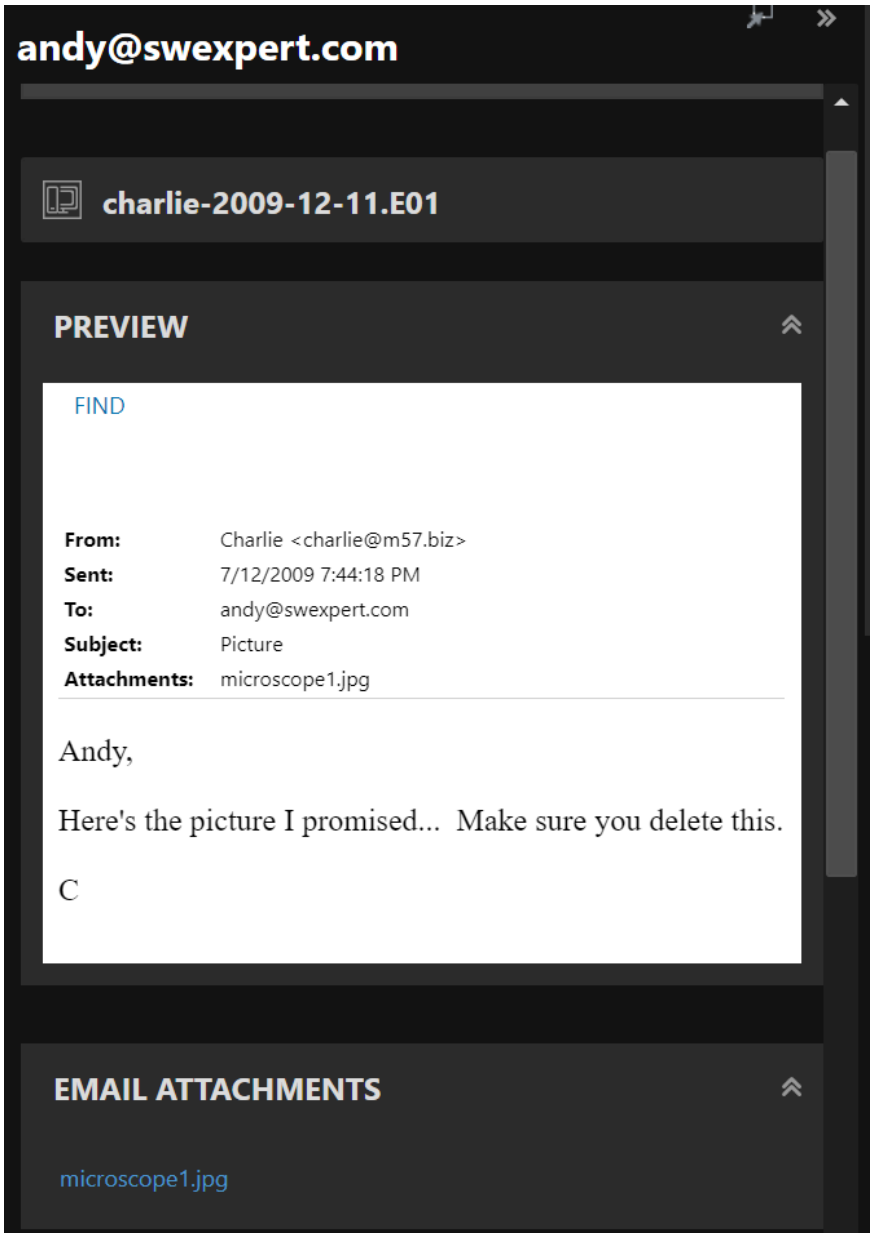
2.1 On 12-4-2009, Charlie sent an extortion Email to the recipient ("Andy") with the email address andy@swexpert.com demanding 100k in exchange for not disclosing private information that is attached in the email "*01.zip*" (MD5 hash: 4fa239c22e5fb7b934a1bf68e4e0e2e7) where the password to decrypt is in a separate Email in a picture.



2.3.2. Figure 10: Charlie extorting Andy for 100k

2.2 On 12-7-2009, Charlie emailed the picture that was mentioned in Figure 6 above which was named microscope1.jpg (MD5 Hash: 4be2c4abb48c4389ca798e6c21736ea1) in the Email

with the subject "*Picture*". The email conversation is seen below in Figure 11 with the jpeg file shown in Figure 12.

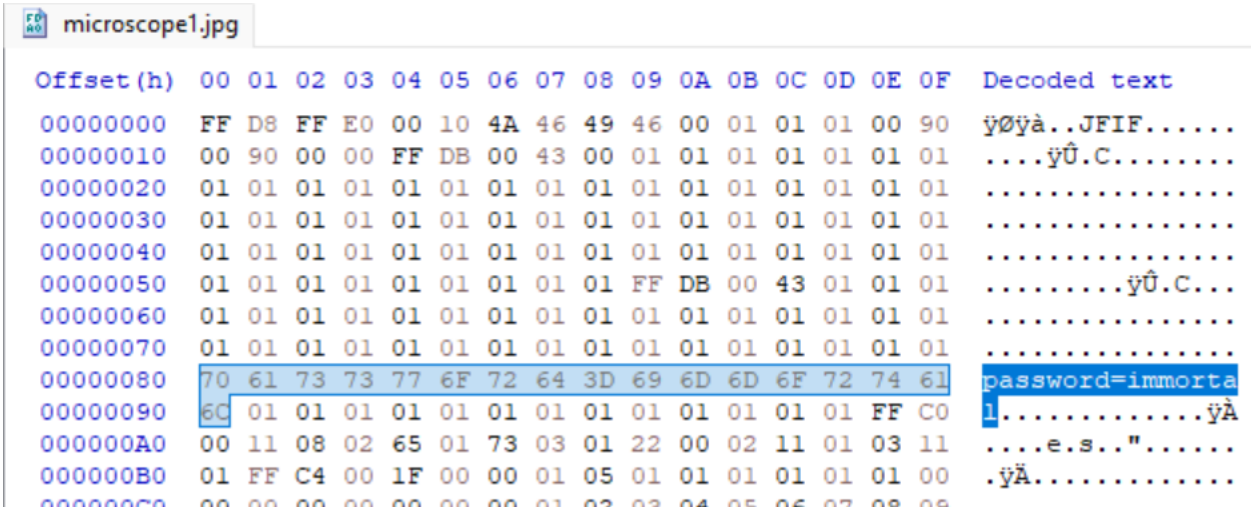


2.3.2. Figure 11: Email with microscope1.jpg as attachment

2.3.2. Figure 12: microscope1.jpg

2.3 Using HxD 2.5.0.0, the password to decrypt the file is obtained as “immortal” as shown in Figure 13 below. And upon unzipping the file with the password, we were able

to obtain 2. Patent files with the name us005026637-001.tif (MD5 hash: b526e6c7a244d62e7120f3f804d76d8d) and us006982168-001.tif (MD5 hash: c412dfcd8bca1333d9356d710dd7a01a) which Charles used to extort Andy shown in Figure 14 and 15 respectively.



2.3.2. Figure 13: Password for decrypting *01.zip* obtained from *microscope1.jpg*

United States Patent [19]

Soule et al.

[11] **Patent Number: 5,026,637**

[45] **Date of Patent: Jun. 25, 1991**

[54] **IMMORTAL HUMAN MAMMARY EPITHELIAL CELL LINES**

[76] Inventors: **Herbert Soule**, 6344 Jonathan, Dearborn, Mich. 48126; **Charles M. McGrath**, 6669 Beach, Troy, Mich. 48098

[21] Appl. No.: **317,610**

[22] Filed: **Feb. 28, 1989** (Under 37 CFR 1.47)

[51] **Int. Cl.**[5] **C12Q 1/02**; C12Q 1/18; C12N 5/06

[52] **U.S. Cl.** **435/29**; 435/32; 435/172.1; 435/240.1; 435/240.2; 436/63; 436/813

[58] **Field of Search** 435/29, 23, 7, 320, 435/6, 252.8, 219, 32, 172.1, 240.1, 240.2; 436/63, 813; 536/27; 935/9; 424/85.2, 85.1, 85.8, 85.91, 1.1; 514/317, 428, 648; 530/14, 395, 415, 829

[56] **References Cited**

PUBLICATIONS

Jones et al., Breast Cancer Research Group and Pathology Dept., Michigan Cancer Foundation, Detroit, Mich. 48201, Proceedings of AACR, vol. 29, (Mar. 1988).

In Vitro, vol. 20, No. 8, Aug. 1984, "Calcium Regulation of Normal Human Mammary Epithelial Cell Growth in Culture", Charles M. McGrath and Herbert D. Soule, pp. 653–662.

In Vitro Cellular & Developmental Biology, vol. 33, No. 1, Jan. 1986, "A Simplified Method for Passage and Long-Term Growth of Human Mammary Epithelial Cells", Herbert D. Soule and Charles M. McGrath, pp. 6–12.

Proceedings of AACR, vol. 29, Mar. 1988, #1780, p. 448.

Primary Examiner—Esther L. Kepplinger
Assistant Examiner—Toni R. Scheiner
Attorney, Agent, or Firm—Robert L. Kelly; Dykema Gossett

[57] **ABSTRACT**

Immortalized human epithelial cell sublines are provided. The novel cell lines do not undergo terminal differentiation and senescence upon exposure to high calcium concentrations. The novel cells exhibit positive reactivity with milk-fat globule membrane antigen and cytokeratin anti-serum. The cells are non-tumorigenic in athymic mice, and exhibit both three-dimensional growth in collagen and dome formation in confluent cultures. The cell sublines demonstrate growth control by hormones and growth factors. The novel cell sublines are useful in evaluating the capacity of preselected agents to bring about a change in epithelial cell growth and in the production of proteins.

3 Claims, 3 Drawing Sheets

2.3.2. Figure 14: First patent used for extortion

US006982168B1

(12) **United States Patent**
Topalian et al.

(10) **Patent No.: US 6,982,168 B1**
(45) **Date of Patent: Jan. 3, 2006**

(54) **IMMORTAL HUMAN PROSTATE EPITHELIAL CELL LINES AND CLONES AND THEIR APPLICATIONS IN THE RESEARCH AND THERAPY OF PROSTATE CANCER**

(75) Inventors: **Suzanne L. Topalian**, Brookeville, MD (US); **W. Marston Linehan**, Rockville, MD (US); **Robert K. Bright**, Portland, OR (US); **Cathy D. Vocke**, Germantown, MD (US)

(73) Assignee: **The United States of America as represented by the Department of Health and Human Services**, Washington, DC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **08/913,770**

(22) PCT Filed: **Jan. 30, 1997**

(86) PCT No.: **PCT/US97/01430**

§ 371 (c)(1),
(2), (4) Date: **Sep. 22, 1997**

(87) PCT Pub. No.: **WO97/28255**

PCT Pub. Date: **Aug. 7, 1997**

Related U.S. Application Data

(60) Provisional application No. 60/011,042, filed on Feb. 2, 1996.

(51) **Int. Cl.**
C12N 15/85 (2006.01)

(52) **U.S. Cl.** **435/325**; 435/366; 435/371; 435/384; 435/385; 435/386

(58) **Field of Classification Search** 424/184.1, 424/277.1, 93.7; 435/7.23, 325, 366, 378
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,026,637	A	6/1991	Soule et al.	435/29
5,376,542	A	12/1994	Schlegal	435/172.2
5,436,152	A	7/1995	Soule et al.	435/240.2
5,443,954	A	8/1995	Reddel et al.	435/7.21
5,462,870	A	10/1995	Chopra	435/240.2
5,576,206	A	11/1996	Schlegel	435/240.2
5,716,830	A	2/1998	Webber et al.	435/6
5,824,488	A	* 10/1998	Webber et al.	435/7.23

FOREIGN PATENT DOCUMENTS

WO	WO 92/16645	10/1992
WO	WO 95/29990	11/1995
WO	WO 95/29994	11/1995

OTHER PUBLICATIONS

Chiarello, E, Oncogene 16: 541–545, 1998.*
Kelemen. Genes Chromosomes Cancer 11:195–198, 1994.*
Drexler. Leukemia & Lymphoma 9:1–25, 1993.*
Embleton, Immunol. Ser. 23:181–207, 1984.*
Heu, In: Tissue Culture Meth & Applications, Kruse & Patterson, Eds, p. 764, 1973.*
Mustafa O. Intl. J. Oncol. 8(5):883–888, 1996.*
ATCC Catalogue of Cell Lines & Hybridomas, 6th edition, pp. 145 and 222, 1988.*
Bernardino et al. "Characterization of Chromosome changes in two human prostatic charcinoma cell lines (PC–3 and DU 145) using chromosome painting and comparative genomic hybridization" Cancer Genet. Cytogenet. vol. 96, pp. 123–128, 1997.*
Freshney, Culture of Animal Cells, A manual of basic technique chapter 13, p. 130, 1983.*
Smith, R. T. "Cancer and the immune system" Clinical Immunology. vol. 41 No. 4, pp. 841–850, Aug. 1994.*
McInerney J. M et al. Gene Therapy 7(8): 653–63, 2000.*
Parda et al, "Neoplastic Transformation of a Human Prostate Epithelial Cell Line by the v–Ki–ras Oncogene", *The Prostate* 23:91–98 (1993).
Hayward et al, "Establishment and Characterization of an Immortalized But Non–Transformed Human Prostate Epithelial Cell Line: BPH–1", *In Vitro Cell Dev. Biol.* 31A:14–24, Jan. 1995.
Castagnetta et al, "Prostate Long–Term Epithelial Cell Lines", *Annals of The New York Academy of Sciences*, vol. 595, pp. 149–164, 1990.
Boudou et al, "Distinct Androgen 5a–Reduction Pathways in Cultured Fibroblasts and Immortalized Epithelial Cells From Normal Human Adult Prostate", *The Journal of Urology*, vol. 152, 226–231, Jul. 1994.
Narayan et al, "Establishment and Characterization of a Human Primary Prostatic Adenocarcinoma Cell Line (ND–1)", *The Journal of Urology*, vol. 148, 1600–1604, Nov. 1992.
Rhim et al, "Stepwise immortalization and transformation of adult human prostate epithelial cells by a combination of HPV–18 and v–Ki–ras", *Proc. Natl. Acad. Sci. USA*, vol. 91, pp. 11874–11878, Dec. 1994.

(Continued)

Primary Examiner—Susan Ungar
Assistant Examiner—Minh-Tam Davis
(74) *Attorney, Agent, or Firm*—Leydig, Voit & Mayer, Ltd.

(57) **ABSTRACT**

The present invention relates to immortalized, malignant, human, adult prostate epithelial cell lines or cell lines derived therefrom useful in the diagnosis and treatment of prostate cancer. More particularly, the present invention relates to cloned, immortalized, malignant, human, adult prostate epithelial cell lines and uses of these cell lines for the diagnosis and treatment of cancer. Furthermore, the present invention provides for the characterization of said cell lines through the analysis of specific chromosomal deletions.

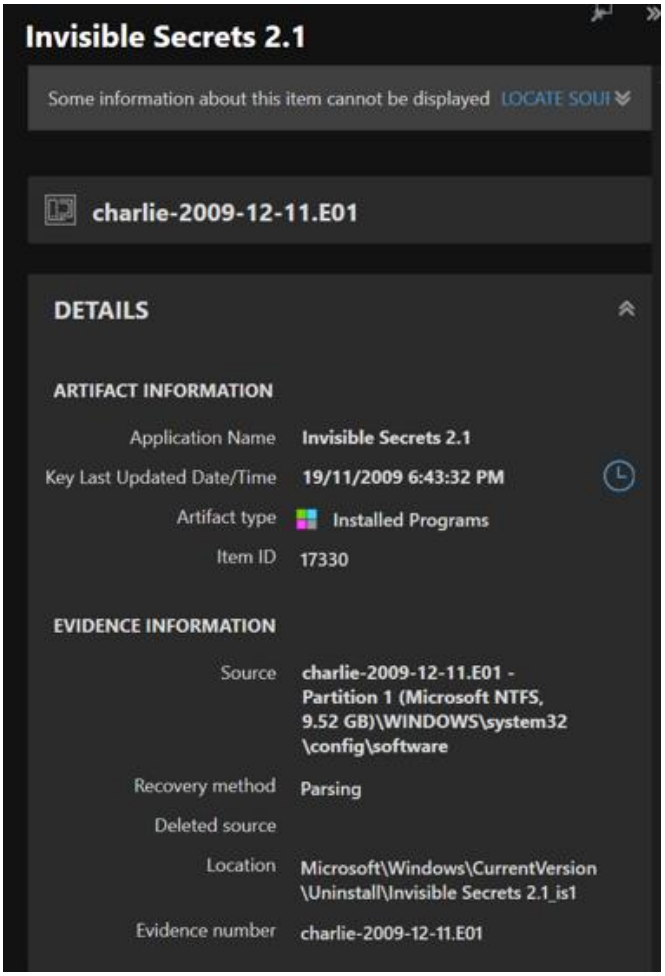
21 Claims, 6 Drawing Sheets

2.3.2. Figure 15: Second patent used for extortion

Other supporting evidences:

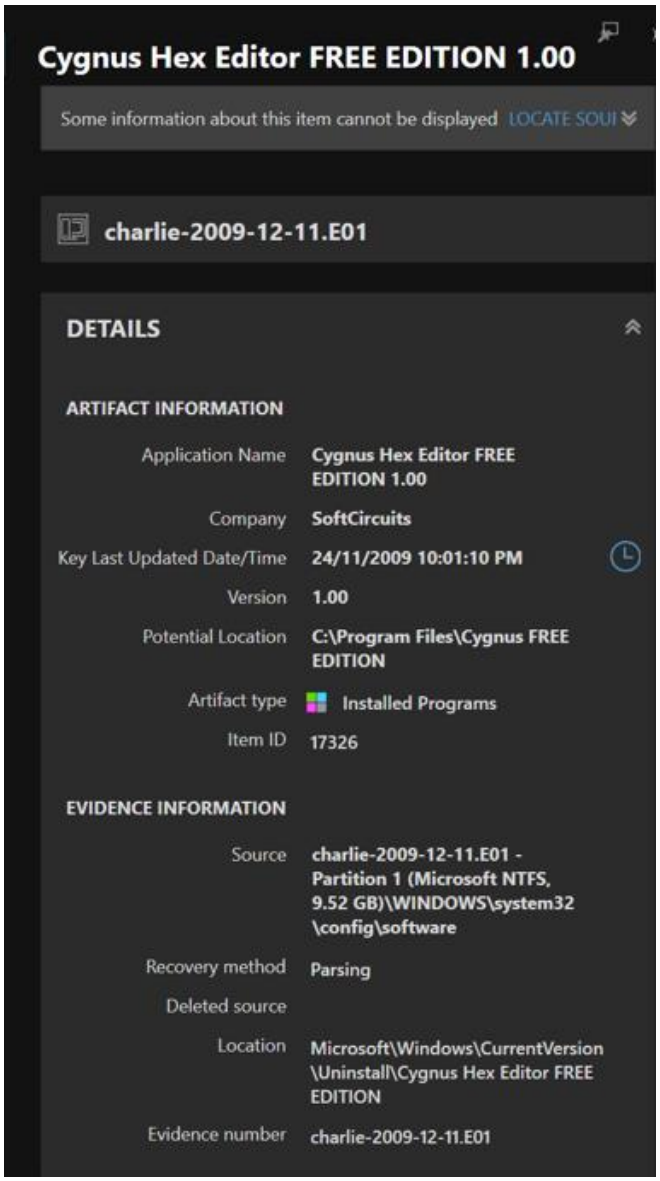
1. Installation of required software

We saw that on 11-19-2009, Charlie installed Invisible Secrets 2.1 which is a software that is used for the creation of astronaut1.jpg which uses steganography to hide "*Nitroba work.odt"*, the patent that was sold to Jamie from project2400.



2.3.2. Figure 16: Invisible Secrets software installed on 11-19-2009

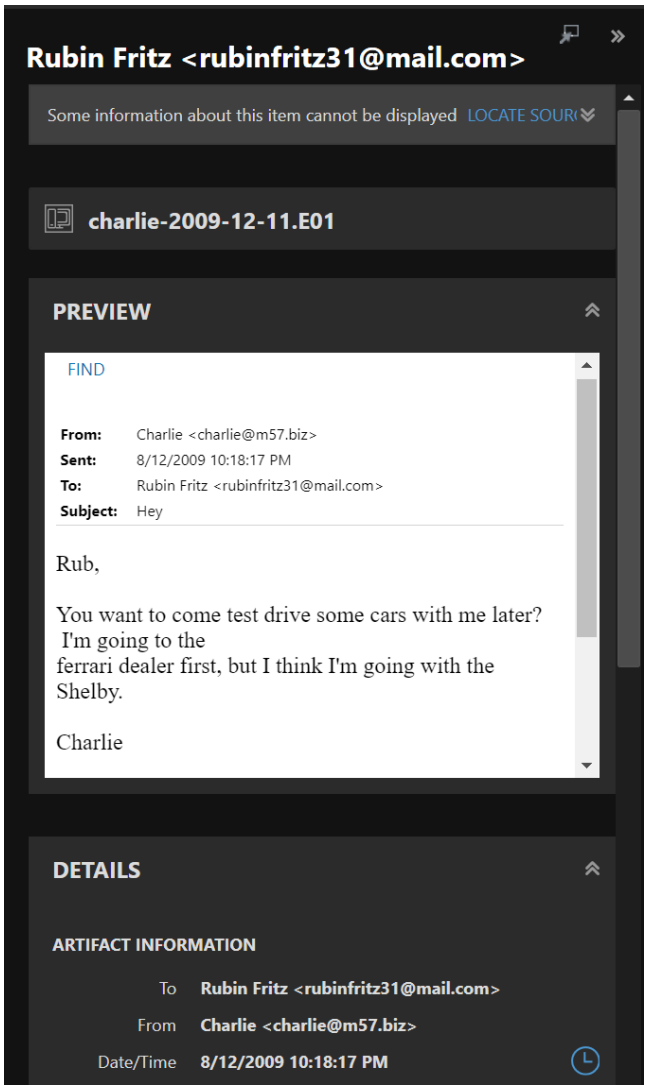
Furthermore, it is also recorded that on 11-24-2009 which is the date before Charlie sent microscope1.jpg to andy@swexpert.com, the software ("*Cygnus Hex Editor FREE EDITION 1.00*") which is used to embed the password to decrypt 01.zip is installed.



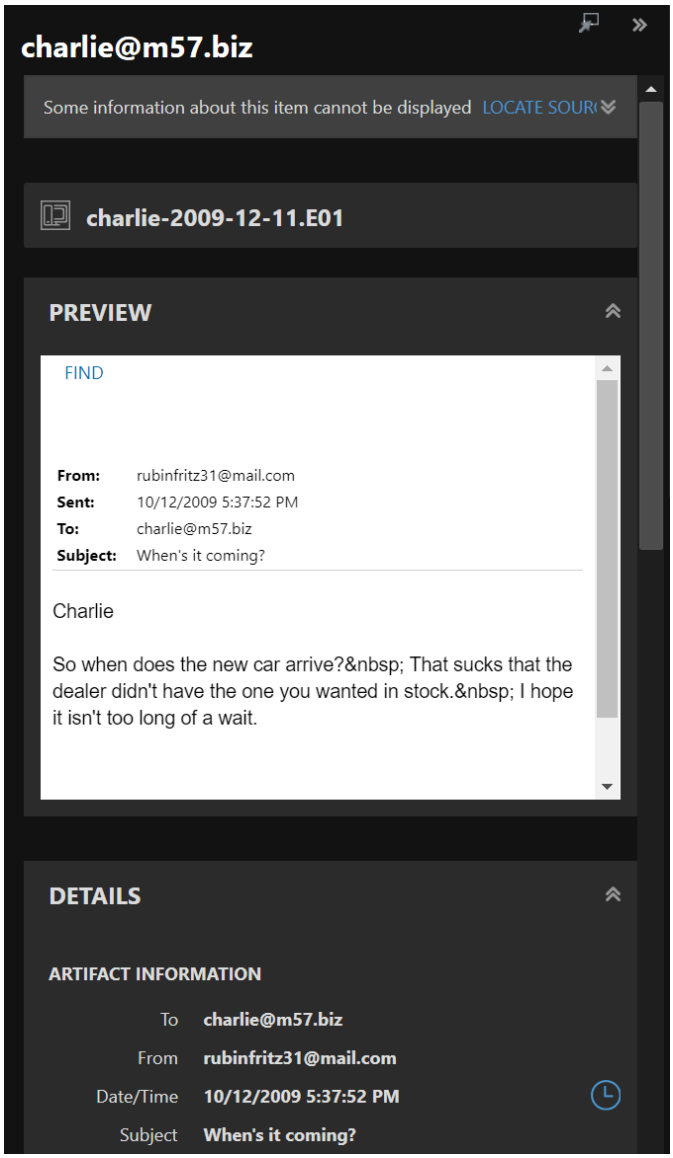
2.3.2. Figure 17: Cygnus Hex Editor FREE EDITION 1.00 software installed on 11-24-2009

2. Sudden change in lifestyle

We also observe that Charlie has a sudden significant change in lifestyle such as buying a luxury car which suggests a huge influx of money for Charlie.



2.3.2. Figure 18: Schedule for Ferrari test drive on 12-8-2009



2.3.2. Figure 19: Ferrari bought on 12-10-2009

2.6.3 Pat's Case

In investigating Pat's case, Axiom is used to load two pieces of evidence, namely pat-2009-12-11.E01 and pat-2009-12-11.mddramimage.

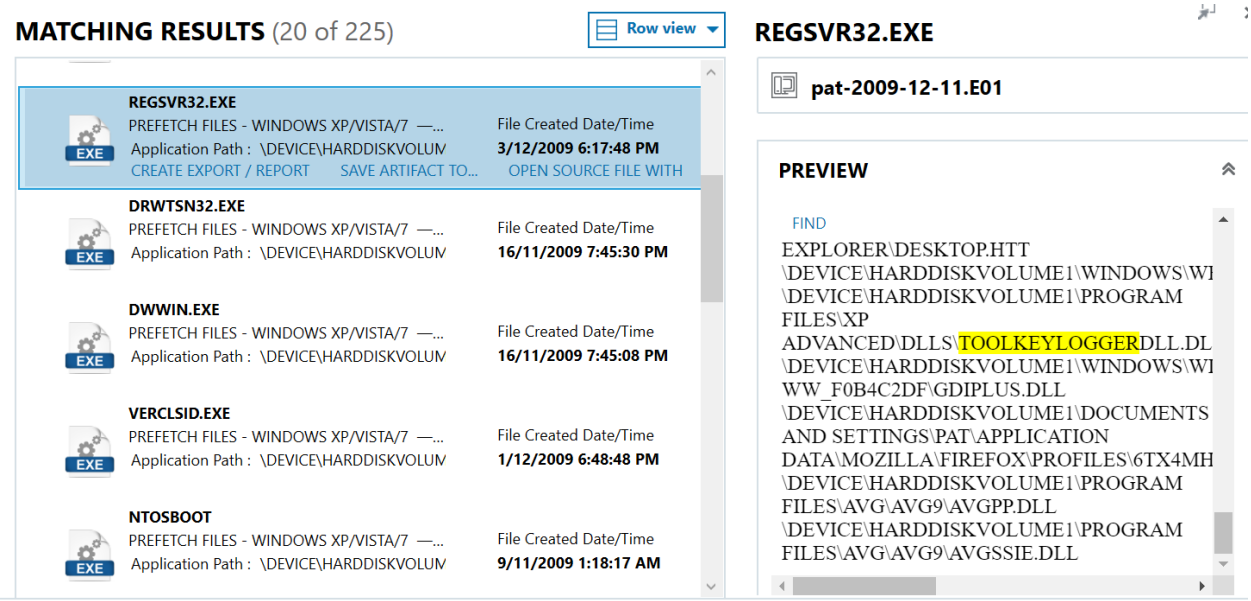
From the evidence, we built a basic timeline of what occurred to Pat's computer.

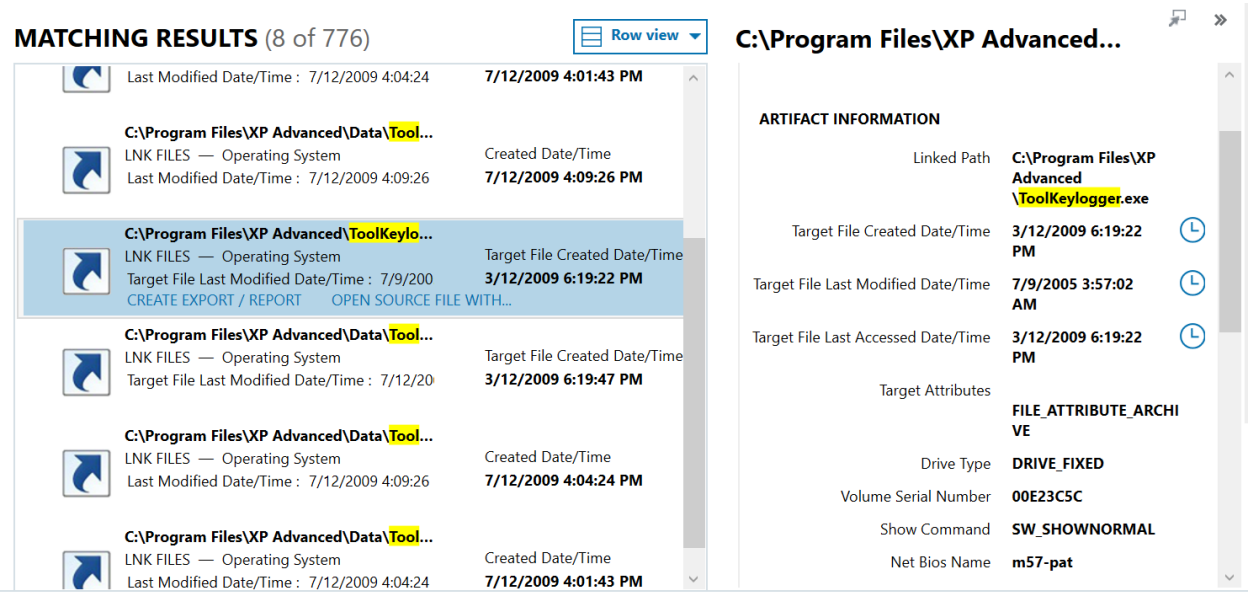
2.6.3.1 Evidence of Keylogger on Pat's computer

03/12

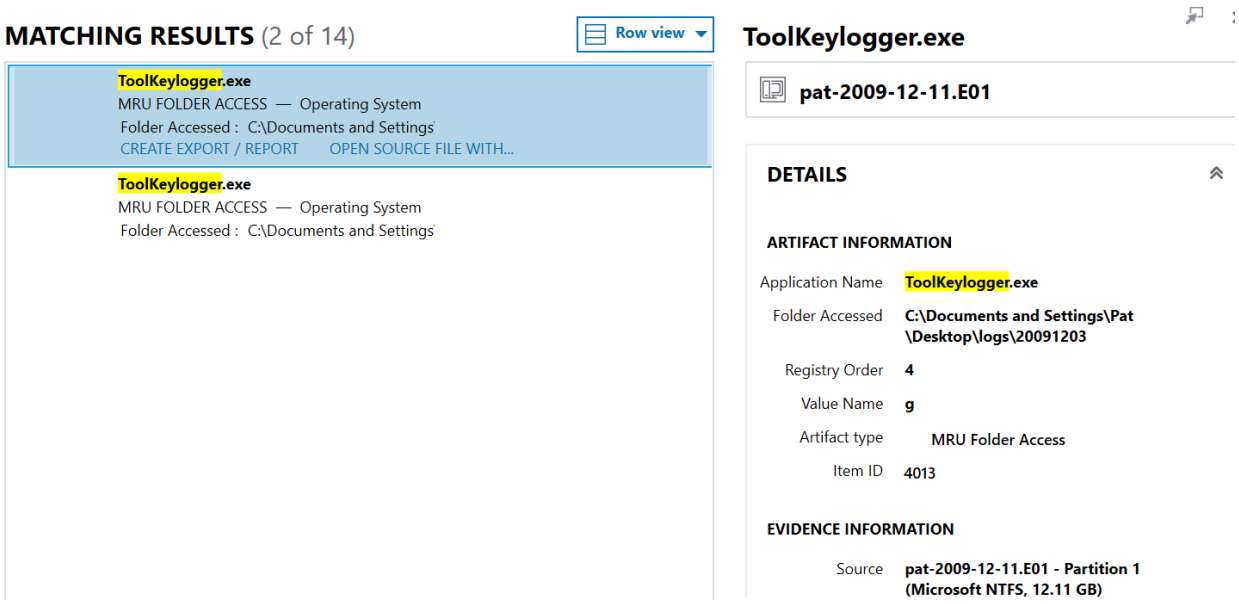
- XP Advanced Keylogger appears:
    - XP Advanced/DLLs/ToolKeyloggerDLL.dll
    - XP Advanced/SkinMagic.dll
    - XP Advanced/ToolKeylogger.exe

First mention of ToolKeylogger occurs on 03/12/2009. The file itself has been removed from the computer, but multiple artifacts remain that are linked to it, which suggests it was on Pat's computer starting from this date.



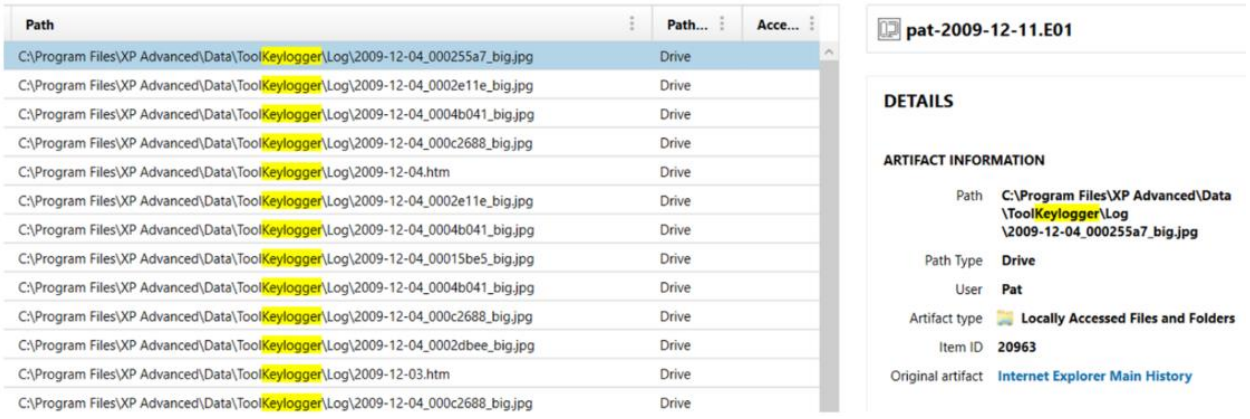


Keylogger is found in prefetch files and has a LNK file.



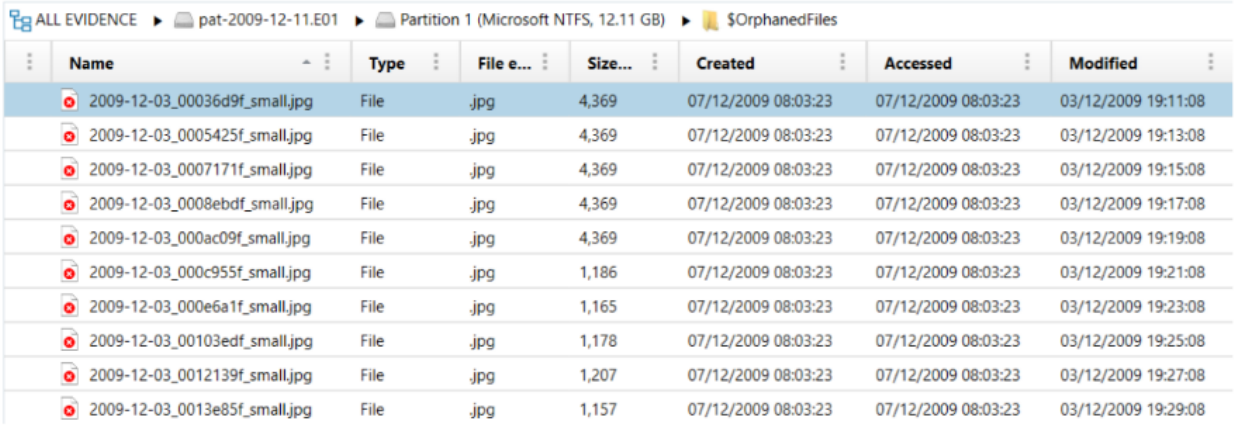
Keylogger appears in the Most Recently Used folder on 03/12/2009.

Therefore it is likely that a keylogger was secretly installed on Pat's computer, starting from 12/03/2009, to record his keystrokes.



Logs are also found, proving that the keylogger was recording and exfiltrating data. This is later linked to Terry's case, which shows that Terry was the one eavesdropping on Pat as the file naming conventions are the same as the one used here.

The original files are gone, but we managed to retrieve some data from the $OrphanedFiles folder, as such data remains on the computer even after the original copy is deleted:


ALL EVIDENCE ▸ pat-2009-12-11.E01 ▸ Partition 1 (Microsoft NTFS, 12.11 GB) ▸ $OrphanedFiles

Name	Type	File e...	Size...	Created	Accessed	Modified
2009-12-03_00036d9f_small.jpg	File	.jpg	4,369	07/12/2009 08:03:23	07/12/2009 08:03:23	03/12/2009 19:11:08
2009-12-03_0005425f_small.jpg	File	.jpg	4,369	07/12/2009 08:03:23	07/12/2009 08:03:23	03/12/2009 19:13:08
2009-12-03_0007171f_small.jpg	File	.jpg	4,369	07/12/2009 08:03:23	07/12/2009 08:03:23	03/12/2009 19:15:08
2009-12-03_0008ebdf_small.jpg	File	.jpg	4,369	07/12/2009 08:03:23	07/12/2009 08:03:23	03/12/2009 19:17:08
2009-12-03_000ac09f_small.jpg	File	.jpg	4,369	07/12/2009 08:03:23	07/12/2009 08:03:23	03/12/2009 19:19:08
2009-12-03_000c955f_small.jpg	File	.jpg	1,186	07/12/2009 08:03:23	07/12/2009 08:03:23	03/12/2009 19:21:08
2009-12-03_000e6a1f_small.jpg	File	.jpg	1,165	07/12/2009 08:03:23	07/12/2009 08:03:23	03/12/2009 19:23:08
2009-12-03_00103edf_small.jpg	File	.jpg	1,178	07/12/2009 08:03:23	07/12/2009 08:03:23	03/12/2009 19:25:08
2009-12-03_0012139f_small.jpg	File	.jpg	1,207	07/12/2009 08:03:23	07/12/2009 08:03:23	03/12/2009 19:27:08
2009-12-03_0013e85f_small.jpg	File	.jpg	1,157	07/12/2009 08:03:23	07/12/2009 08:03:23	03/12/2009 19:29:08

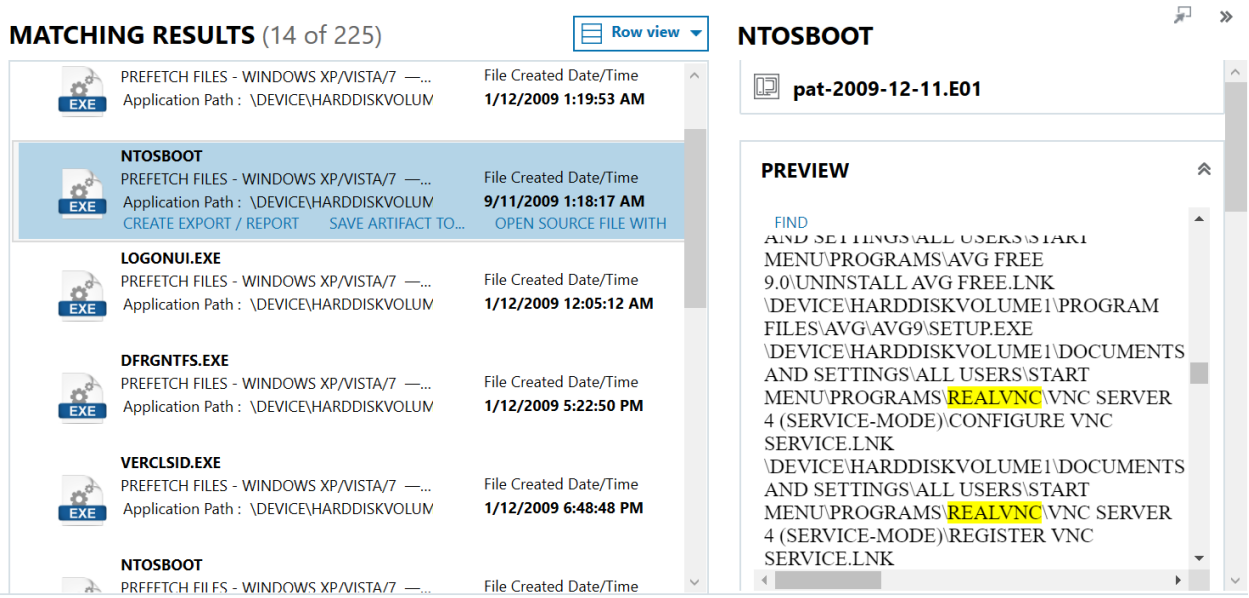
2.6.3.2 Evidence of Remote Desktop Software (RealVNC) on Pat's computer

07/12

- RealVNC VNC4 installed
    - RealVNC/VNC4/logmessages.dll
    - RealVNC/VNC4/winvnc4.exe
    - RealVNC/VNC4/wm_hooks.dll
    - RealVNC/VNC4/vncviewer.exe
    - RealVNC/VNC4/vncconfig.exe

RealVNC appears in multiple artifacts starting from 07/12/2009.

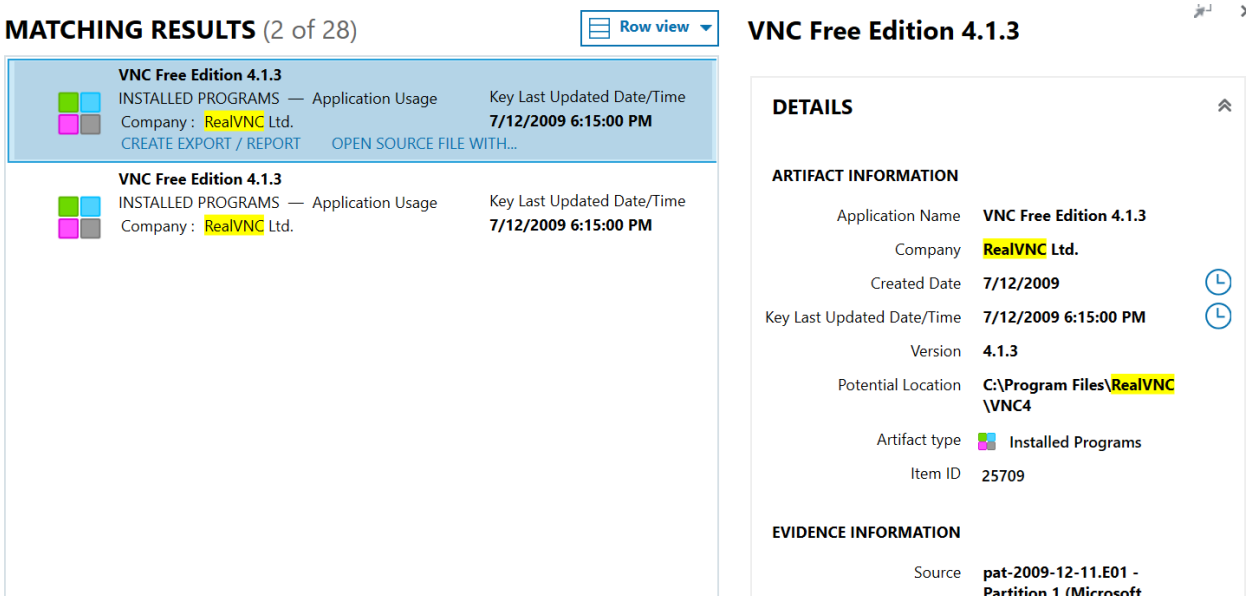
However, interestingly enough, RealVNC is mentioned in Prefetch files from as early as 9/11/2009.

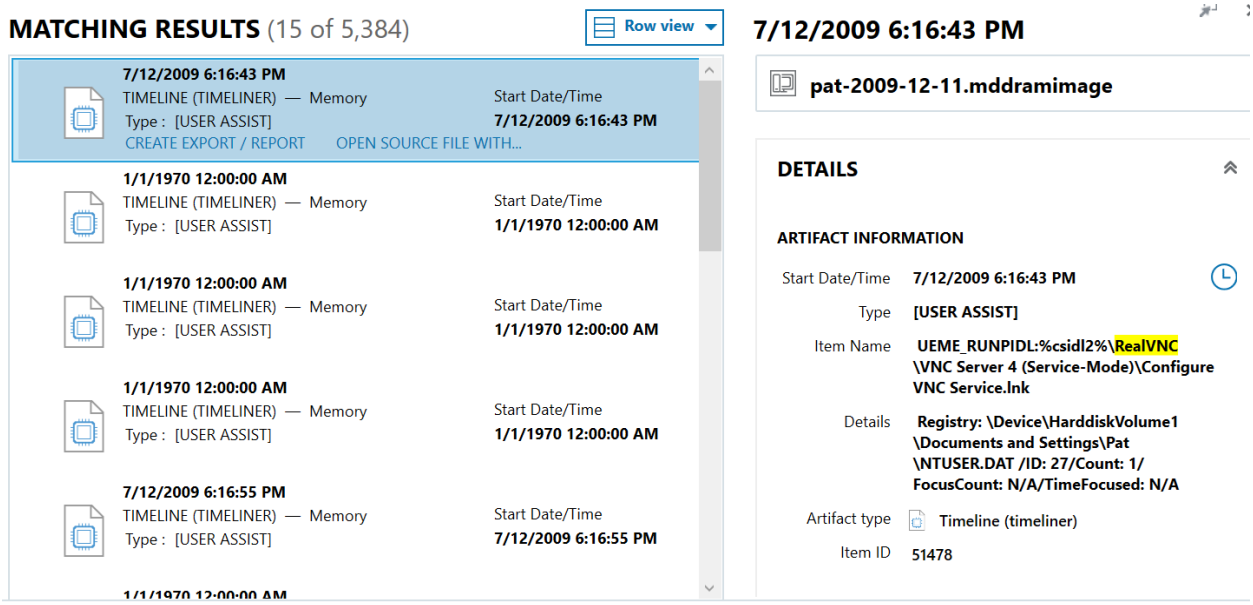


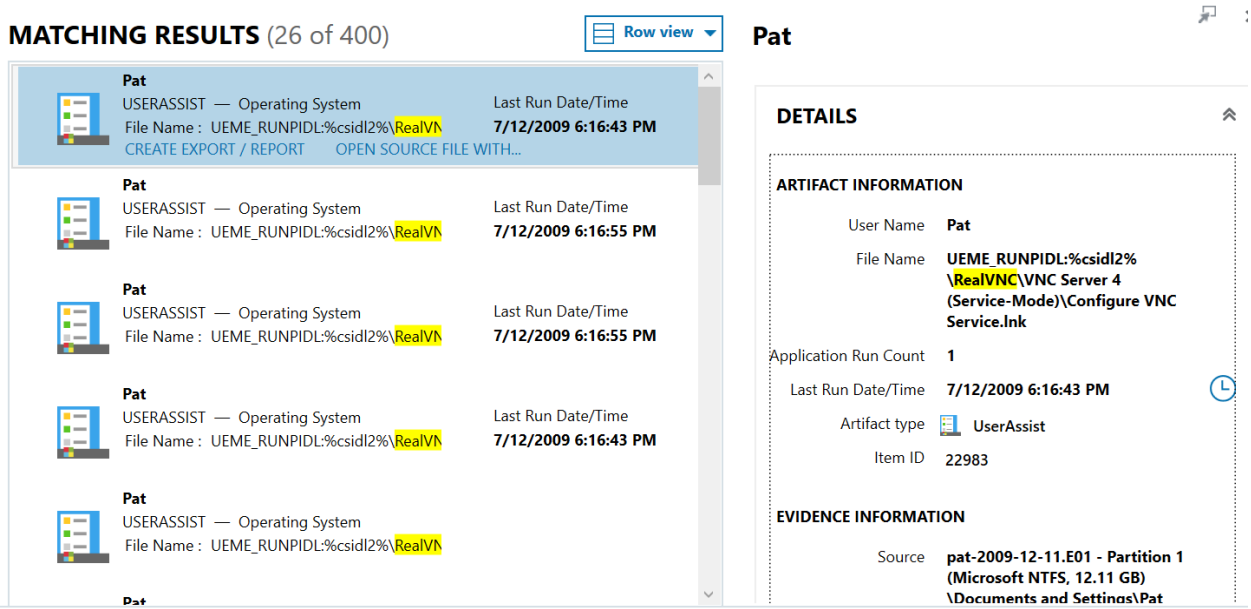
Despite this, we only found conclusive evidence that it was installed on a later date.

VNC Free Edition 4.1.3 was installed on Pat's laptop on 7/12/2009, as shown from the below screenshot. RealVNC is a company that provides remote access software. The software consists of a server and client application for the Virtual Network Computing protocol to control another computer's screen remotely.[1]

[1] https://www.realvnc.com/en/


MATCHING RESULTS (2 of 28)
Row view
VNC Free Edition 4.1.3
INSTALLED PROGRAMS — Application Usage
Company : RealVNC Ltd.
CREATE EXPORT / REPORT
OPEN SOURCE FILE WITH...
Key Last Updated Date/Time
7/12/2009 6:15:00 PM
VNC Free Edition 4.1.3
INSTALLED PROGRAMS — Application Usage
Company : RealVNC Ltd.
Key Last Updated Date/Time
7/12/2009 6:15:00 PM
VNC Free Edition 4.1.3
DETAILS
ARTIFACT INFORMATION
Application Name VNC Free Edition 4.1.3
Company RealVNC Ltd.
Created Date 7/12/2009
Key Last Updated Date/Time 7/12/2009 6:15:00 PM
Version 4.1.3
Potential Location C:\Program Files\RealVNC\VNC4
Artifact type Installed Programs
Item ID 25709
EVIDENCE INFORMATION
Source pat-2009-12-11.E01 -

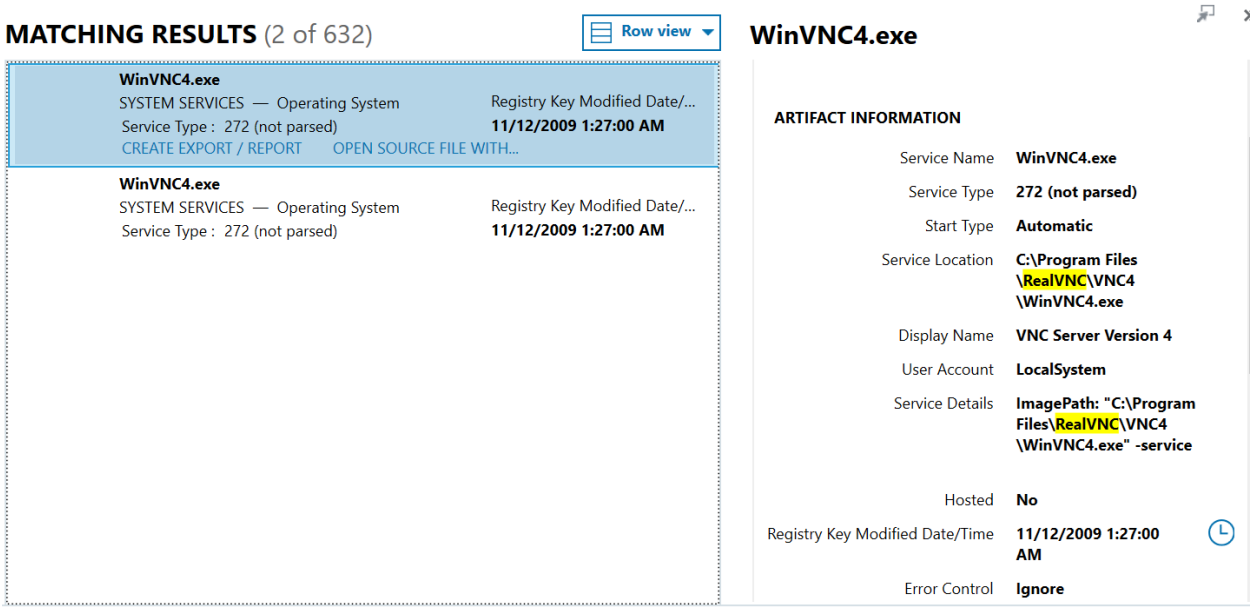

MATCHING RESULTS (15 of 5,384)
Row view
7/12/2009 6:16:43 PM
TIMELINE (TIMELINER) — Memory
Type : [USER ASSIST]
CREATE EXPORT / REPORT
OPEN SOURCE FILE WITH...
Start Date/Time
7/12/2009 6:16:43 PM
1/1/1970 12:00:00 AM
TIMELINE (TIMELINER) — Memory
Type : [USER ASSIST]
Start Date/Time
1/1/1970 12:00:00 AM
1/1/1970 12:00:00 AM
TIMELINE (TIMELINER) — Memory
Type : [USER ASSIST]
Start Date/Time
1/1/1970 12:00:00 AM
1/1/1970 12:00:00 AM
TIMELINE (TIMELINER) — Memory
Type : [USER ASSIST]
Start Date/Time
1/1/1970 12:00:00 AM
7/12/2009 6:16:55 PM
TIMELINE (TIMELINER) — Memory
Type : [USER ASSIST]
Start Date/Time
7/12/2009 6:16:55 PM
7/12/2009 6:16:43 PM
pat-2009-12-11.mddramimage
DETAILS
ARTIFACT INFORMATION
Start Date/Time 7/12/2009 6:16:43 PM
Type [USER ASSIST]
Item Name UEME_RUNPIDL:%csidl2%\RealVNC\VNC Server 4 (Service-Mode)\Configure VNC Service.lnk
Details Registry: \Device\HarddiskVolume1\Documents and Settings\Pat\NTUSER.DAT /ID: 27/Count: 1/FocusCount: N/A/TimeFocused: N/A
Artifact type Timeline (timeliner)
Item ID 51478



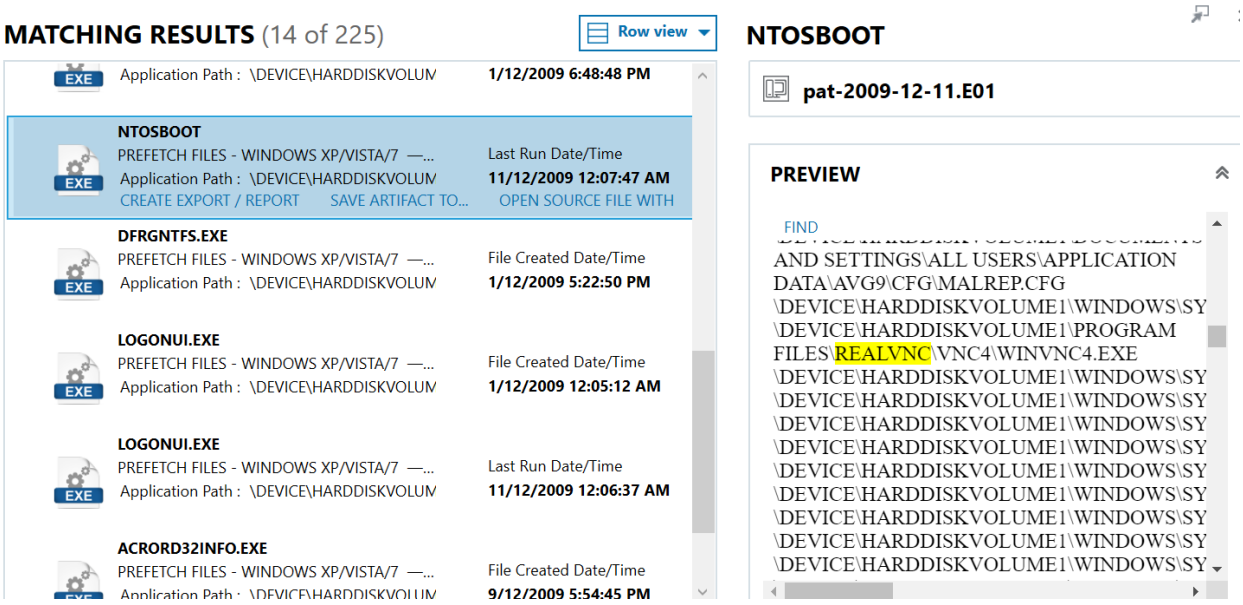
UserAssist utility displays a table of programs executed on a Windows machine, complete with running count and last execution date and time. From the above screenshot we observe that RealVNC runs on his computer from this time (7/12/2009, 6.16 PM).

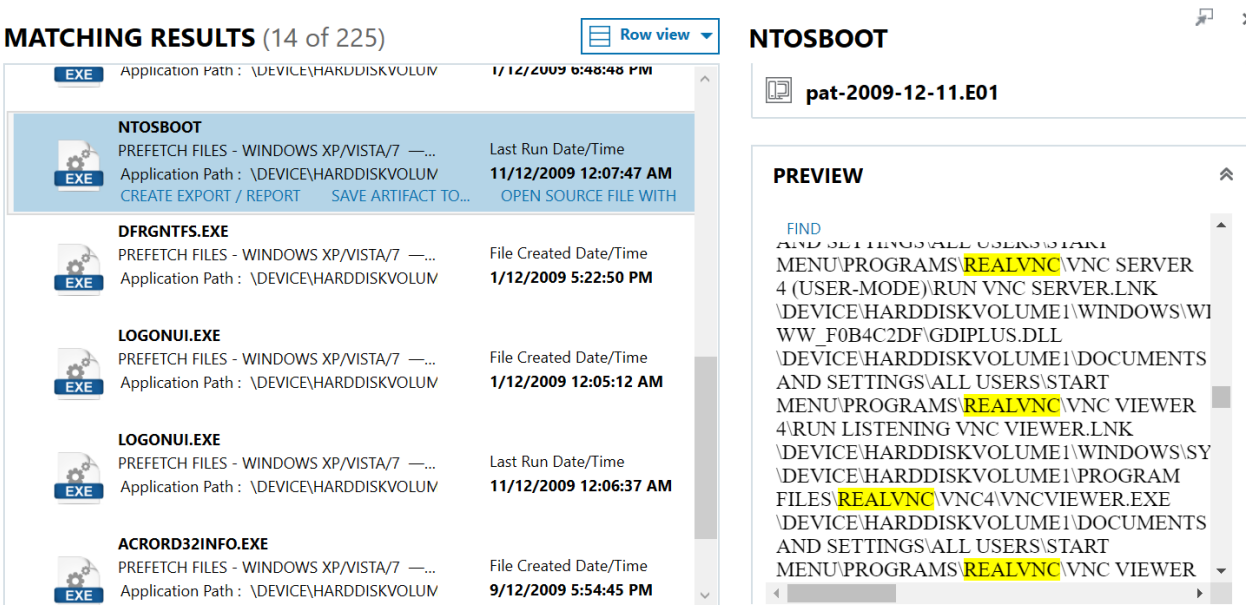
From this we can conclude that a Remote Desktop program was likely used to either control Pat's computer or eavesdrop on his communications.

Starting from 11/12/2009, it became a service that runs automatically with Pat's computer.



RealVNC was present on Pat's computer until at least 11/12/2009, as seen from the below prefetch files.





2.6.3.3 Attribution of above activities

Based on our forensic investigation, Terry is the one who installed the keylogger and remote desktop software on Pat's computer. The evidence found on Terry's computer matches the keylogger logs and remote desktop software found in Pat's computer. More details will be furnished in Terry's section.

2.6.3.4 Peculiarities in Pat's actions

One thing to note is that in the detective report, it is stated:

Outcome
McGoo has contacted a lawyer, and seems to intend to authorize a search. McGoo has promised not to tell employees, and will contact us with a decision tomorrow morning.

Despite his promise, Pat did in fact tell his employees that a search was imminent, as evidenced by the below email sent by Pat, which was found on Charlie's disk image:

From: "Pat McGoo" <pat@m57.biz>

Sent: 12/11/2009 4:55:53 PM

To: <terry@m57.biz>, <jo@m57.biz>, <charlie@m57.biz>

Subject: Important Meeting

Team,

we are going to have a meeting first thing this morning. As soon as you get in please come in to the conference room. I received a call yesterday from the Police - they are going to be here to talk to us.

Pat

Therefore we observe that Pat lied to the detective about not telling his employees. Despite this fact, we find no further evidence that Pat had any ill intentions, and therefore we only highlight this as a peculiarity.

2.6.4 Terry's Case

2.6.4.1 Usage of company's computer for personal use

Terry has been researching online gambling, as well as using his work laptop for research on sports scores and visiting anonymous gambling websites. This could be a breach of the company's AUP depending on the policies set by the management.

19	Of interest		http://www.gamblersanonymous.org/
20	Of interest		http://www.gamblersanonymous.org/mtgdirTOP.html
21	Of interest		http://www.gamblersanonymous.org/history.html
22	Of interest		http://www.gamblersanonymous.org/recovery.html

2.6.4.2 Usage of Cleaning software, VNC, Keylogging software

Terry has also been testing out various softwares on his own computer. These actions, depending on the company's policy on the usage of these software could determine if Terry was conducting illegal activities or not.

Cleaning software such as CCleaner and Eraser.exe were found on his computer. Further investigation is required to determine if he downloaded these for legitimate purposes such as wiping company's drives before disposing them

A	B	C	D	E	F	G
Record	Tags	Comments	Filename	Software	Created Date/Time - UTC+00:00 (M/d/	Last Accessed Date/Time - UTC+00:00 (M/d/
1	Of interest		CCleaner.exe	CCleaner	11/24/2009 9:49:10 PM	12/8/2009 9:09:23 PM
2	Of interest		Eraser.exe	Eraser	12/10/2009 4:28:29 PM	12/10/2009 4:28:29 PM

VNC software was also found to be tested in his drive (and subsequently found installed on Pat's computer). These softwares were previously found installed on Pat's computer. This once again depends on the company's AUP, as it is not uncommon for IT Support in companies to have

Remote Assistance software installed for troubleshooting purposes.

7	6	Of interest		http://www.realvnc.com/products/free/4.1/winvnc.html#Installatior	12/7/200
8	7	Of interest		http://www.realvnc.com/index.html	12/7/200
9	8	Of interest		http://www.realvnc.com/products/download.html	12/7/200
10	9	Of interest		http://www.realvnc.com/products/free/4.1/download.html	12/7/200
11	10	Of interest		http://www.realvnc.com/cgi-bin/download.cgi	12/7/200
12	11	Of interest		http://www.realvnc.com/products/free/4.1/index.html	12/7/200
13	12	Of interest		http://www.realvnc.com/products/free/4.1/winvnc.html	12/7/200
14	13	Of interest		http://www.realvnc.com/products/free/4.1/winvnc.html#Installatior	12/7/200
15	14	Of interest		http://www.realvnc.com/index.html	12/7/200
16	15	Of interest		http://www.realvnc.com/products/download.html	12/7/200
17	16	Of interest		http://www.realvnc.com/products/free/4.1/download.html	12/7/200
18	17	Of interest		http://www.realvnc.com/cgi-bin/download.cgi	12/7/200

2.6.4.3 Usage of Keylogging software

Keylogging software was also found on his drive, amongst which includes “skl0g”, “XPAdvancedKeylogger” as well as Github pages on latest keylogging apps like “Spyphone” where the open source code is hosted online. Once again, these software could be legitimate based on the company’s policy on whether employee’s usage of company devices are deemed to be monitored or not.

	B	C	D	E
ord	Tags	Comments	URL	User
1	Of interest		file:///C:/Users/terry/Documents/Downloads/skl0g/readme.tx	terry
2	Of interest		file:///C:/Users/terry/Documents/Downloads/keylogger.zip	terry
3	Of interest		file:///C:/Users/terry/Documents/Downloads/skl0g/readme.tx	terry
4	Of interest		file:///C:/Users/terry/Documents/Downloads/keylogger.zip	terry

A	B	C	
Record	**Tags**	**Comments**	**URL**
1	Of interest		http://www.google.com/search?rlz=1C1GGLS_enUS354US355&sourceid=chrome&ie=UTF-8&q=windows+xp+k
2	Of interest		http://www.blazingtools.com/bpk.html
3	Of interest		http://www.google.com/search?hl=en&rlz=1C1GGLS_enUS354US355&ei=c_UXS4jADIKGswPas7GsDg&sa=X&oi
4	Of interest		http://download.cnet.com/XP-Advanced-Keylogger/3000-27064_4-10434172.html
5	Of interest		http://dw.com.com/redir?edId=3&siteId=4&oId=3000-27064_4-10434172&ontId=27064_4&spi=8354bf713eec
6	Of interest		http://download.cnet.com/3001-27064_4-10434172.html?spi=8354bf713eedc6a715817465d93dd3a0
7	Of interest		http://www.google.com/search?hl=en&rlz=1C1GGLS_enUS354US355&q=free+windows+keylogger&revid=994
8	Of interest		http://www.kmint21.com/keylogger/
9	Of interest		http://www.kmint21.com/download.html
10	Of interest		http://threatpost.com/en_us/blogs/new-spyphone-iphone-app-can-harvest-personal-data-120409
11	Of interest		http://github.com/nst/spyphone/
12	Of interest		http://threatpost.com/en_us/blogs/new-spyphone-iphone-app-can-harvest-personal-data-120409

2.6.4.4 Sale of company equipment online

Terry has been selling the company's equipment online for quick cash. This depends on what the company policy has specified for retired equipment, we will however still present the findings in this report.

According to an inventory list (M57Inventory.xls) that was sent out to Pat, there were 2 items that were not assigned to anyone at that point in time.

M57.biz Computer Inventory List

Item Description	Assigned To	M57.biz Serial No.
HP Printer	N/A	P1111
ThinkVision Monitor	Terry	M1113
Dell Computer	Terry	C1112
Dell Computer	Pat	C1113
Dell Computer	N/A	C1111
Dell Computer	Charlie	C1114
Dell Monitor	Pat	M1112
Dell Monitor	Jo	M1111
Toshiba Monitor	Charlie	M1114
Dell Computer	Jo	C1115
Generic Printer	M57	P1112

We see that there are 2 devices that are not assigned to anyone, and likely that both were subsequently listed on Craigslist by Terry.

We determine that the computer S/N C1111 belonged to Jo previously as from an email file which Terry confirmed

```
Pat,

You are correct.

Terry
  ----- Original Message -----=20
  From: Pat McGoo=20
  To: terry@m57.biz=20
  Cc: jo@m57.biz=20
  Sent: Thursday, December 10, 2009 2:11 PM
  Subject: Computer Serial Number


  Terry,

    is this serial number from that computer Jo used to have?  C1111

  Pat
```

We see from Terry's email that there was also a sales for "HP Printer & Dell Monitor" which happens to be the same manufacturer (HP and Dell) as his company's equipment. Further investigation to determine if they are the company's devices such as ensuring that the individual S/N is logged properly in the inventory.

```
------=_NextPart_000_0059_01CA7999.B17AE960
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Jean,

The two items are still available.  I can sell you the two items for =
$200.  Give me a call for information about seeing the products tonight. =
831-233-2883

- Terry
  ----- Original Message -----=20
  From: Jean Sizemore=20
  To: t93940@gmail.com=20
  Sent: Thursday, December 10, 2009 11:26 AM
  Subject: HP Printer & Dell Monitor


  Hi,


  Would you be willing to sell me both the monitor and printer for $200 =
if they are still available?


  Thanks,
  Jean
```

We also see the computer C1111 of the main investigation being sold by Terry to Aaron Greene. It is highly probable that this was the computer previously owned by Jo, sold by Terry on Craigslist for $1000 USD.

```
>  Aaron,
>
> The computer is still available.  I'll give you a call later this afternoon
> with directions to my place.  Talk to you soon.
>
> - Terry
>
>
> ----- Original Message -----
> *From:* Aaron Greene <aarongreene12@gmail.com>
> *To:* t93940@gmail.com
> *Sent:* Monday, November 30, 2009 9:45 AM
> *Subject:* Dell Computer For Sale - $1000 (USA)
>
> Hi,
>
> Is the computer still available? I am extremely interested in the computer
> for sale. Please contact me at 831-555-5432 if you need to give me a call. I
> will be off at work at 5 tonight to check out the computer.
>
> Thanks,
>
> Aaron
>
```

This is likely how the computer ended up on the secondary market.

2.6.4.5 Forgery of Receipt

We find evidence of Terry making a quick $200 sent around 19th November 2009 13:01:30.

```
Subject: Re: How's It Going?
Date: Thu, 19 Nov 2009 13:01:30 -0800
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="----=_NextPart_000_0021_01CA6918.69CD3C30"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Windows Mail 6.0.6001.18000
X-MimeOLE: Produced By Microsoft MimeOLE V6.0.6001.18049

This is a multi-part message in MIME format.

------=_NextPart_000_0021_01CA6918.69CD3C30
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Cod,

Things are going well.  I am enjoying work right now, but we'll see.  My =
boss is a little weird.  There's something odd about him that I can't =
put my finger on. =20

I really shouldn't gamble anymore, but I just made a quick $200.  Sign =
me up for the tournament.  Hopefully I can win some big money.

Talk to you this weekend.

- Terry
```

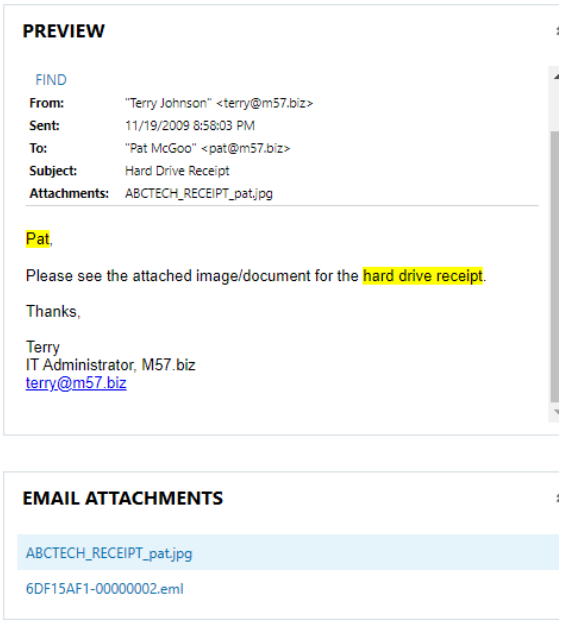
This incident was closely related to the hard disk issue of Pat commenting that there was a hard disk costing $300 as really pricey. We also see that Terry has previously requested a hard disk.

```
Terry,

You can go ahead an purchase the drive.  The company will re-imburse you =
on your next paycheck.  Please send me the receipt when you have =
purchased the drive.

Thanks,

Pat
  ----- Original Message -----=20
  From: Terry Johnson=20
  To: Pat McGoo=20
  Sent: Wednesday, November 18, 2009 9:43 AM
  Subject: Need Larger Hard Drive


  Pat,

  I need a larger hard drive since my Vista installation is taking up =
too much space.  Should I purchase the drive and the company can =
re-imburse me later?  Or are you going to purchase the drive?
```

According to his emails, we see that Terry has emailed from his personal email to his work email a file called “ABCTECH_RECEIPT.jpg” (md5:51A72BF38097A5FBD08ECC283E6F9C44)

```
Message-ID: <867c9858091119l128j748a306fr636efe0a5d389491@mail.gmail.com>
Subject: ABC Tech Receipt
From: Terry Terry <t93940@gmail.com>
To: terry@m57.biz
Content-Type: multipart/mixed; boundary=000e0cd253101ad62e0478be5d67

--000e0cd253101ad62e0478be5d67
Content-Type: multipart/alternative; boundary=000e0cd253101ad61e0478be5d65

--000e0cd253101ad61e0478be5d65
Content-Type: text/plain; charset=ISO-8859-1

Send receipt on to Pat.... :)

--000e0cd253101ad61e0478be5d65
Content-Type: text/html; charset=ISO-8859-1

Send receipt on to Pat.... :)<div><br></div>

--000e0cd253101ad61e0478be5d65--
--000e0cd253101ad62e0478be5d67
Content-Type: image/jpeg; name="ABCTECH_RECEIPT.jpg"
Content-Disposition: attachment; filename="ABCTECH_RECEIPT.jpg"
```

We subsequently see that when he sent the receipt to Pat, it was renamed to "ABCTECH_RECEIPT_pat.jpg" (md5:101880370D00BA48A1E0B7B93460A9A9)



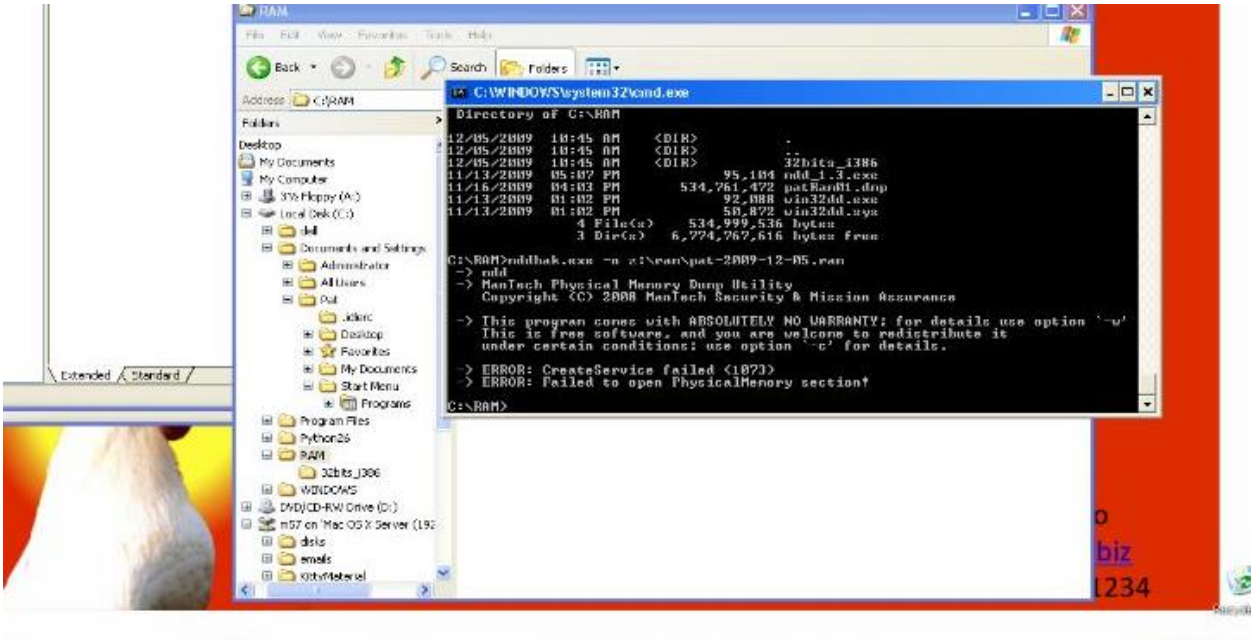
Logically speaking, the receipt should not have been changed but we have seen that the MD5 sum has changed, indicating that he submitted a different file from the original receipt.. Upon further investigation, we see that the value has been modified from $100 to $300

We can also see that in the email that follows, that even though Pat prompted Terry about the expensive hard disk, Terry agreed that the claim amount is correct of $300 which is different from the original receipt. This indicates that Terry is aware of himself claiming $300 for the hard disk.

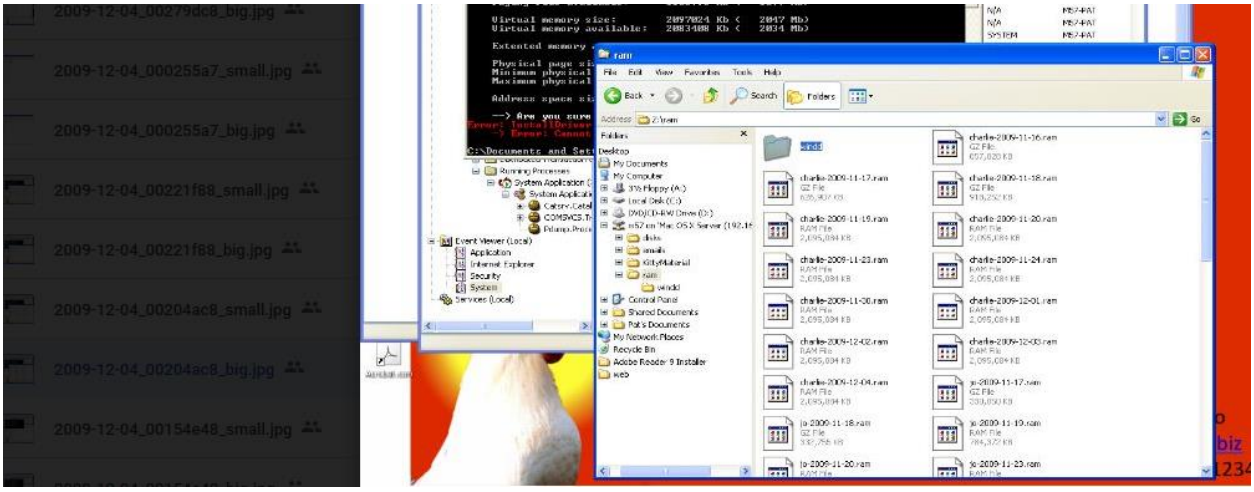
```
------=_NextPart_000_0038_01CA6919.1B5DC730
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Pat,

It costs more when you need a new hard drive immediatley.  Here's hoping =
to this drive being good.

Thanks,

Terry
IT Administrator, M57.biz
terry@m57.biz
  ----- Original Message -----=20
  From: Pat McGoo=20
  To: Terry Johnson=20
  Sent: Thursday, November 19, 2009 1:04 PM
  Subject: Re: Hard Drive Receipt


  Terry,

  It seems that $300 is a little expensive for a 40GB hard drive.  Oh =
well, at least work is getting done.

  Thanks,

  Pat
  CEO, M57.biz
  pat@m57.biz
```

2.6.4.6 Possession of Pat's desktop images

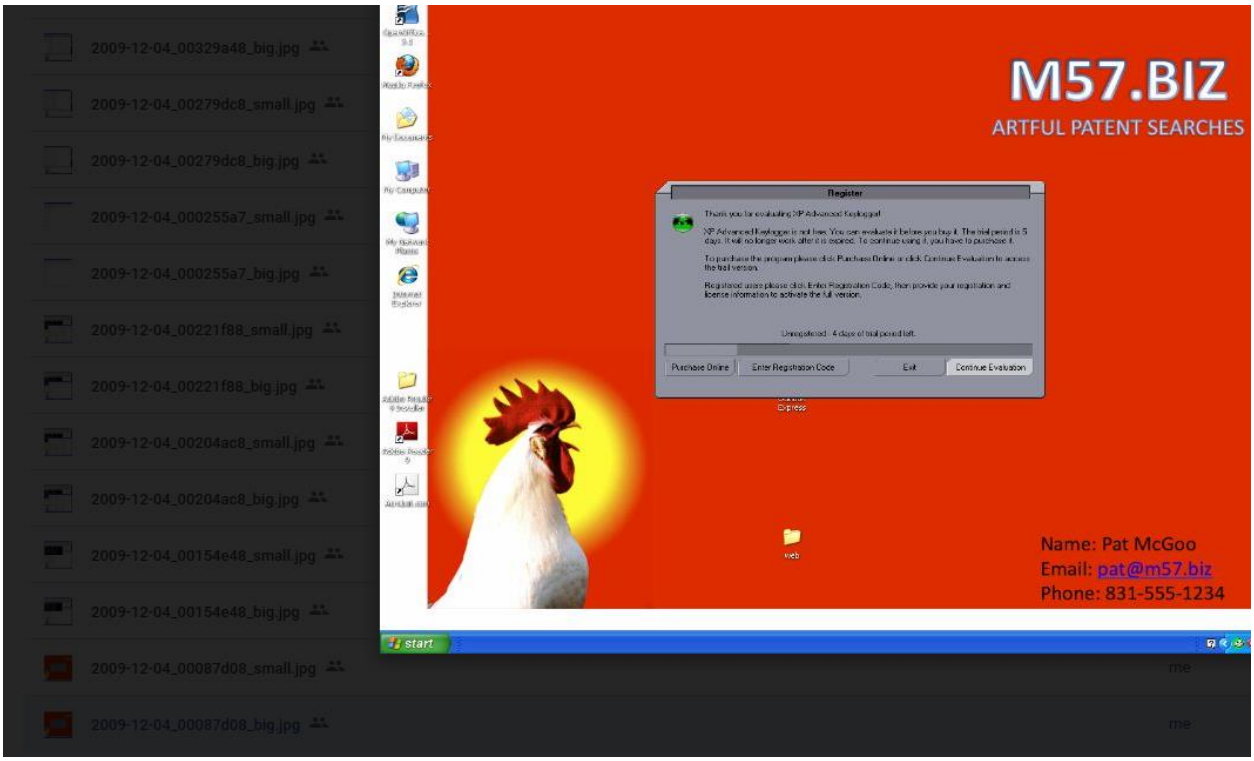
Previously, evidence of VNC and Keyloggers was found on Pat's drives. We can further see that Terry has captured screenshots of Pat's desktop, which hints at the possibility of Terry spying on Pat's actions.



Apart from screenshots of Pat's drives, we see that there is a ram capture software mddbak.exe that is used to capture not only Pat, but Charlie as well as Jo's desktop. Investigation should continue to verify whether this was approved by management.

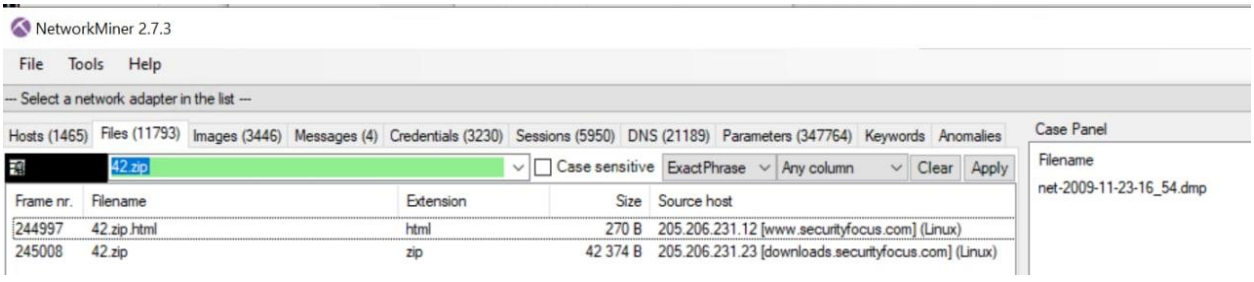


We can also see that keylogger has been successfully installed on Pat's computer via the GUI.



2.6.4.7 Downloading of malicious files

Upon inspecting the network files using NetworkMiner, we also found that Terry was downloading malicious files. Within 2009-11-23-15_54.dmp, we discovered that Terry downloaded a file named 42.zip that is a zip bomb. Upon researching it, we confirm that it is a fork bomb that crashes the computer via containing massive nested zip files for a total of 4.5 petabytes of unzipped data, which few computers can handle.[2]



[2] https://en.wikipedia.org/wiki/Zip_bomb

42.zip.html - File Details

Name	42.zip.html
MD5	96cab03e832e15dd3a7841204954d4f6
SHA1	1af6340cdd3f2b0e2c28c104b39682670dd5bde
SHA256	542db41690251f135800247eeb855d5aab2212b1ed0350f3dcf49f7f194d0130
Path	C:\Users\jovan\Downloads\NetworkMiner_2-7-3\NetworkMiner_2-7-3\AssembledFiles\205.206.231.12\TCP-80\data\vulnerabilities\exploits\42.zip.html
Size	270
LastWriteTime	25/11/2009 5:36 am
Source	205.206.231.12 [www.securityfocus.com] (Linux)
Destination	192.168.1.105 [ubuntu] [ubuntu-3.local] [M57-TERRY] [ubuntu.local] (Windows)

Max bytes to read: 256 Font size: 10 File type: HTML

```
3C21444F435459504520485 44D4C2050        <!DOCTYPE HTML P
55424C4943202 22D2F2F494554462F2F        UBLIC "-//IETF//
4454442048544D4C20322E302F2F454E         DTD HTML 2.0//EN
223E0A3C48544D4C3E3C484541443E0A         ">.<HTML><HEAD>.
3C5449544C453E333031204D6F766564         <TITLE>301 Moved
205065726D616E656E746C793C2F5449          Permanently</TI
544C453E0A3C2F484541443E3C424F44         TLE>.</HEAD><BOD
593E0A3C48313E4D6F76656420506572         Y>.<H1>Moved Per
6D616E656E746C793C2F48313E0A5468         manently</H1>.Th
6520646F63756D656E7420686173206D         e document has m
6F766564203C412048524546 3D226874        oved <A HREF="ht
74703A2F2F646F776E6C6F6164732E73         tp://downloads.s
65637572697479666F6375732E636F6D         ecurityfocus.com
2F76756C6E65726162696C6974696573         /vulnerabilities
2F65787 06C6F6974732F34322E7A6970        /exploits/42.zip
223E686572653C2F413E2E3C503E0A3C         ">here</A>.<P>.<
```

3.0 Summary of Conclusions Reached

After a lengthy investigation process we have come to a conclusion that Jo was indeed responsible for the files found on the purchased machine. We have also found evidence of the other employees within M57 engaging in suspicious activities.

Evidence from section 2.5.1 shows that the Kitty exploitation pictures and videos have originated from Jo and he was the one who subsequently transferred it to the purchased machine by means of a work USB. Jo has also deleted the files from this USB in an attempt to cover his tracks.

As for how this machine, which was originally office equipment belonging to M57, came into the secondary market was the work of another employee within M57. Terry Johnson, the IT administrator, has been selling office equipment for quick cash. From section 2.5.4.4 we have shown that the purchased machine, previously identified with serial number C1111 within M57, was sold by Terry did belong to Jo but has since been unused before the sale. This explains why the Kitty exploitation pictures and videos were found on this computer. The computer was not the only office equipment that was sold by Terry. He has also sold a monitor and printer for $200 as well as falsely reporting the cost of a hard drive so that he could pocket the difference.

Terry has not only been secretly selling office equipment he has also been spying on Pat's computer using a keylogger and remote desktop software. Further investigation showed that Terry has also used a ram capture software for both Charlie and Jo as well. It does not seem that this level of scrutinization from Terry was appropriate as an IT administrator, unless it is part of M57 company policy.

Charlie himself has also been engaging in suspicious activities. Charlie has been selling patents from his client's company Nitroba to Nitroba's competitor project2400 for large amounts of money to fund his own extravagant lifestyle. From section 2.6.2, we have evidence that Charlie is extorting large amount of money from swexpert which did not engage Charlie's company for their services previously.

In conclusion, it is unclear whether such actions are illegal, we would recommend the infrastructure team to come up with a list of approved software, and guidelines on how remote desktop assistance should be provided so we can ascertain whether the VNC/Keylogging is a malicious activity. While implementing these guidelines, we encourage the management team to follow the laws of their state as keylogging employees without their knowledge could be considered a breach of privacy in some states.

Most of the problems above can be solved with proper access control and monitoring put in place, as well as proper policies, guidelines and procedures to be followed. We recommend the following actions to be taken

1) Remove local administrator rights from corporate users so that they are not able to install software which is not needed in corporate environments.
2) Enforce the labeling of “Confidential/Restricted” on documents, and set up appropriate measures such as Mandatory Access Control to prevent confidential files from being copied out of the intranet environment.
3) Monitoring of network logs to ensure that there is no exfiltration of sensitive information, as well as downloading of unauthorized software.

4) Provide company issued storage media and prevent the use of personal thumb drives in the environment.

While the implementation of the above recommendations are not an unequivocal way of preventing incidents, it acts as a defense-in-depth and discourages future activities with malicious intents, as well as increasing the difficulty of it.

4.0 Appendix

Below are a list of files that we have created during the investigation into this case:

Terry's evidence:

Terry Gambling VNC.xlsx

Exported results.xlsx

Jo's evidence:

jo_allDesktop.xlsx

jo_desktopimage.xlsx

jo_favourites.xlsx

jo_workusb_interesting.xlsx

jo_workusbMEDIA.xlsx

Charlie's evidence:

Nitroba work.odt

us005026637-001.tif

us006982168-001.tif

Pat's evidence:

Shellbags.csv

LNK Files.csv

Shim Cache.csv

Timeline (timeliner).csv

Windows Event Logs.csv