Noroff
University
College

# Memory Analysis of M57.biz

**Victor Sjo**

**Incident Response Fundamentals**

**UC3IRF05**

**Date:** October 25, 2023

# Contents

# List of Figures

# 1 Introduction

## 1.1 Case Background

This report is written in tandem with the police investigation of M57.biz, a patent searching company. It's CEO, Pat McGoo, was informed of a laptop containing confidential documents that had been sold on Craigslist and the laptop was later confirmed to have been stolen from the company. It is alleged someone in the company is selling confidential documents to an outside contact. Furthermore, there is suspicion that McGoo's computer is under illegal surveillance.

This report is based upon the provided data contained in the following files:

- charlie-2009-12-10.mddramimage
- charlie-2009-12-11.mddramimage
- pat-2009-12-10.mddramimage
- pat-2009-12-11.mddramimage
- terry-2009-12-10.winddramimage
- terry-2009-12-11.
- net-2009-12-10-12_00.dmp
- net-2009-12-11-12_00.dmp

The following individuals were identified and are considered people of interest to the investigation:

- Pat McGoo - CEO Of M57.biz
- Terry Johnson - IT Administrator of M57.biz
- Charlie Brown - Patent Researcher at M57.biz
- Jamie - Assumed employee at Project2400
- Aaron Greene - Purchaser of stolen computer
- Jo Smith - Patent Researcher at M57.biz
- Alex Pery - Assumed partner of Charlie Brown
- Jean Sizemore - Assumed potential buyer of printer
- Ruben Fritz - Friend of Charlie Brown
- Cod Williams - Friend of Terry Johnson, poker player
- Jesse - Employee of Norat Tech, friend of Terry Johnson

## 1.2 Executive Summary

The investigation and analysis revealed two distinct potential incidents. Its important to note that this analysis is not conclusive, as further investigation and collection of evidence is required. Nonetheless, the investigation has revealed incriminating evidence linking employee Charlie Brown to the illegal exfiltration and sale of sensitive information using steganography techniques to an outside contact, likely Jaime, an employee at Project2400. Further, the analysis uncovered evidence linking IT administrator Terry Johnson to multiple accounts of theft, embezzlement, and espionage. The report has split these two incidents, as while they to happen concurrently and at the same company, no evidence is present to link these incidents.

# 2 Evidence

## 2.1 Methodology

The data was analyzed on a Windows VM running Windows 10. The primary tool used was Volatility3, used to analyse and access the RAM images as well as retrieving the files referred to in this analysis. While the analysis of the network proved unfruitful, Wireshark and Brim were used for analysing the .dmp files. A hex editor was used in conjunction with traditional word processors to analyse the retrieved files, and for binary analysis AptDiff.exe was used. At times, powershell was used to automate file extraction from the images.

## 2.2 Evidence

The evidence used to draw conclusions are shown where relevant, and will use footnotes to refer back to the following table to ensure the use of evidence is clear, yet concise. Much like the timelines and analysis, the evidence will be divided as they relate to the two identified incidents.

| No. | Filename | MD5 Hash Value | Description | Source |
|---|---|---|---|---|
| 1 | file.0x988c5b8.0x | 721bc4e1da07da903134d42 | File: Charlie Mail Inbox | charlie-2009-12-10.mddramimage |
| 2 | file.0x9398b78.0x | 9595c383471b91b596bcdec | File: Form History | charlie-2009-12-10.mddramimage |
| 3 | Microscope.jpg | 484bc477fa1079452dbdd5e | Image: Microscope | charlie-2009-12-10.mddramimage |
| 4 | Microscope1.jpg | bb1509942924df3999a1766 | Image: Microscope Edited | charlie-2009-12-10.mddramimage |
| 5 | Astronaut.jpg | 484bc477fa1079452dbdd5e | Image: Astronaut | charlie-2009-12-10.mddramimage |
| 6 | Astronaut1.jpg | 2c9a0f66728920d1e0c3688 | Image: Astronaut Edited | charlie-2009-12-10.mddramimage |
| 7 | charlie_10_useras | e9ecf61fd533062a63a4fe61 | File: UserAssist information | charlie-2009-12-10.mddramimage |
| 8 | microscope_passv | 65b7bd66bc59aa77282ed86 | Image: Binary analysis of Microscope files | charlie-2009-12-10.mddramimage |

Table 1: Evidence relating to Charlie Brown

| No. | Filename | MD5 Hash Value | Description | Source |
|---|---|---|---|---|
| 1 | ABCTECH_RECEIPT_pat.jpg | 9446c86338fdbc873ab5b5a5f541b6ce | Image: Receipt for hard drive purchase | terry-2009-12-10.winddramimage |
| 2 | file.None.0x83b78f08.5815441D-00000027.eml.dat | 03377e1a14ba8c00102fef2f4aa3417a | Mail: Terry, Regarding receipt | terry-2009-12-10.winddramimage |
| 3 | file.None.0x840fb360.48F24E8B-0000004E.eml.dat | ae26810fbf8035e4d6cdcd0fe8a033a3 | Mail: Regarding new equipment | terry-2009-12-10.winddramimage |
| 4 | file.None.0x838002d8.1F064827-00000006.eml.dat | b63a9f5565a5df3f310b5aad030db0a3 | Mail: Regarding Jo Smith's computer | terry-2009-12-10.winddramimage |
| 5 | file.None.0x83b25740.6F3B01D5-0000004D.eml.dat | 9e58e435b8b36081d45f0a3c7a8a37da | Mail: Regarding Craigslist posting for printer | terry-2009-12-10.winddramimage |
| 6 | file.None.0x83627598.45AD3B66-0000003B.eml.dat | 351f4508f42c0719fa6d47f02d471023 | Mail: Regarding computer sale | terry-2009-12-10.winddramimage |
| 7 | file.None.0x83b16428.153C7E87-00000028.eml.dat | bbf357aa5734e77871f64a1c36005f51 | Mail: Regarding price of hard drive | terry-2009-12-10.winddramimage |
| 8 | file.None.0x83eb08c0.2FFF6C69-0000000F.eml.dat | 251c7ae942ac8db0ddbcef63198eceb1 | Mail: Regarding reimbursement | terry-2009-12-10.winddramimage |
| 9 | file.None.0x8536aa60.5E735A8A-00000052.eml.dat | dafa57827bdebbb6d58e613cc9c5f2a2 | Mail: Regarding inventory | terry-2009-12-10.winddramimage |
| 10 | file.0x7ec65288.0x838f1918.Data 0000004F.eml.dat | f6dd03bcc58c64ae863d30eb86312938 | Mail: Regarding HP Printer and Dell Monitor | terry-2009-12-10.winddramimage |
| 11 | file.0x69c4b0b8.0x83588d58.Data Index 2009-12.dat | 1849c66d7932fd8cfe13de79487a9c83 | File: Terry Johnson Chrome History | terry-2009-12-10.winddramimage |
| 12 | pat_10_userassist.txt | 1dae4c91a0fe1af879433fc491771345 | File: UserAssist info on Pat McGoo | pat-2009-12-10.mddramimage |
| 13 | terry_10_userassist.txt | 9e20120dd8c65ee02481652174e90f55 | File: UserAssist info on Terry Johnson | terry-2009-12-10.winddramimage |
| 14 | file.None.0x83bb34f0.M57Invento | 952b2625587d8bad1364f4b6a1f7b9d3 | Spreadsheet: Inventory of M57.biz | terry-2009-12-10.winddramimage |
| 15 | file.None.0x8373d5f0.320C23A5-0000000A.eml.dat | a822bf9cddf9dc0dbd1628346ed880ab | Mail: Regarding new printer | terry-2009-12-10.winddramimage |

Table 2: Evidence relating to the Terry Johnson Case

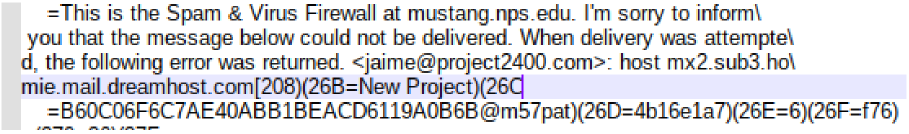
# 3 Incident: Data Exfiltration

| No. | Date and Time | Event | Persons Involved | Source |
|---|---|---|---|---|
| 1 | 16/Nov - 18/Nov | Pat McGoo announces first contract with Nitroba | Pat McGoo | Table 1(1) |
| 2 | 24/Nov | PatMcGoo annonces new contract on quantum cryptography | PatMcGoo | Table 1(1) |
| 3 | 30/Nov | Charlie Brown emails Jamie, at Project2400, concerning a new project | Charlie Brown<br>Jamie (Project2400) | Table 1(1) |
| 4 | 01/Dec | Charlie Brown informs Alix Pery about potential vacation in the Mediterranean | Charlie Brown<br>Alix Pery | Table 1(1) |
| 5 | 03/Dec | Jamie offers Charlie Brown $50 000 for "goods" | Charlie Brown<br>Jamie(Project2400) | Table 1(1) |

Table 3: Timeline of events relating to Charlie Brown

## 3.1 Exfiltration

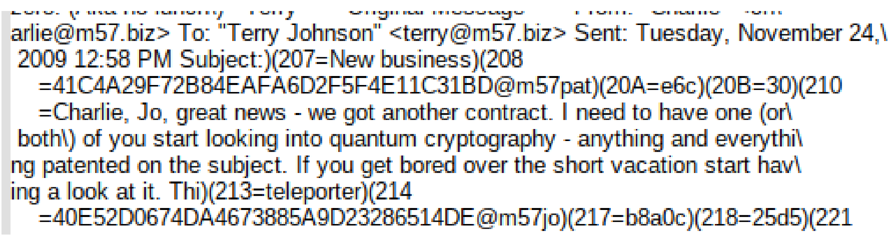
Charlie Brown is under suspicion for allegedly selling confidential information pertaining to Nitroba, a client of M57.biz, to Project2400, a competitor in the industry. This suspicion arose following an email attempted to be sent between 30/11/2009 and 01/12/2009 by Charlie to an individual at Project2400, using the email address <jaime@project2400.com>[1].



```
   =This is the Spam & Virus Firewall at mustang.nps.edu. I'm sorry to inform\
 you that the message below could not be delivered. When delivery was attempte\
d, the following error was returned. <jaime@project2400.com>: host mx2.sub3.ho\
mie.mail.dreamhost.com[208)(26B=New Project)(26C
   =B60C06F6C7AE40ABB1BEACD6119A0B6B@m57pat)(26D=4b16e1a7)(26E=6)(26F=f76)
```

Figure 1: Misspelt Email

It is worth noting that in the initial email attempt, the email address was misspelled, likely leading to its discovery as most other emails relating to the correspondence seems to have been deleted. The content of the email suggests that Charlie was discussing a new project, which is highly likely to be the quantum cryptography project he had been assigned to earlier that week[2].



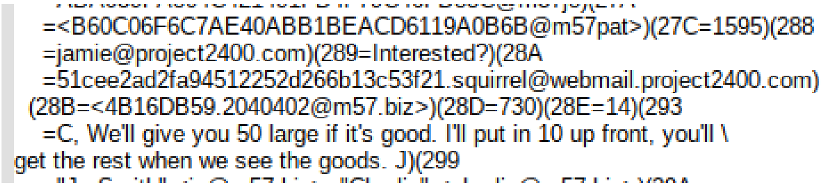
```
arlie@m57.biz> To: "Terry Johnson" <terry@m57.biz> Sent: Tuesday, November 24,\
 2009 12:58 PM Subject:)(207=New business)(208
   =41C4A29F72B84EAFA6D2F5F4E11C31BD@m57pat)(20A=e6c)(20B=30)(210
   =Charlie, Jo, great news - we got another contract. I need to have one (or\
 both\) of you start looking into quantum cryptography - anything and everythi\
ng patented on the subject. If you get bored over the short vacation start hav\
ing a look at it. Thi)(213=teleporter)(214
   =40E52D0674DA4673885A9D23286514DE@m57jo)(217=b8a0c)(218=25d5)(221
```

Figure 2: New Contract Announcement

[1] Ref: Table 1(1)

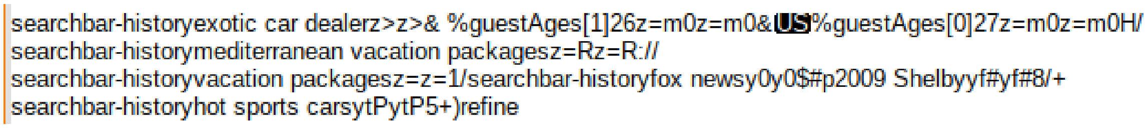
[2] Ref: Table 1(1)

Subsequently, between 01/12/2009 and 03/12/2009, Charlie received a response from Jaime, offering him a sum of $50,000 for unspecified "goods"[3]. It can be inferred that this exchange may be connected to the sale of confidential information. Around the same period, Charlie began planning a vacation to the Mediterranean for himself and Alix Pery, who is presumed to be his partner[4]. Charlie has also been looking at high end cars, and correspondance between him and his friend Ruben indicate Charlie is purchasing a new car[5]. These developments indicate a sudden and significant increase in Charlie's personal finances, which is likely a direct result of the suspected sale of confidential information.



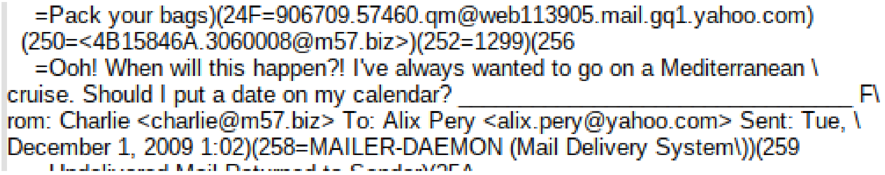
```
  =<B60C06F6C7AE40ABB1BEACD6119A0B6B@m57pat>)(27C=1595)(288
  =jamie@project2400.com)(289=Interested?)(28A
  =51cee2ad2fa94512252d266b13c53f21.squirrel@webmail.project2400.com)
 (28B=<4B16DB59.2040402@m57.biz>)(28D=730)(28E=14)(293
  =C, We'll give you 50 large if it's good. I'll put in 10 up front, you'll \
get the rest when we see the goods. J)(299
```

Figure 3: Offer for $50 000



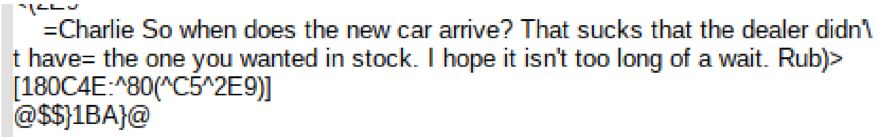
```
searchbar-historyexotic car dealerz>z>& %guestAges[1]26z=m0z=m0&US%guestAges[0]27z=m0z=m0H/
searchbar-historymediterranean vacation packagesz=Rz=R://
searchbar-historyvacation packagesz=z=1/searchbar-historyfox newsy0y0$#p2009 Shelbyyf#yf#8/+
searchbar-historyhot sports carsytPytP5+)refine
```

Figure 4: Luxury Searches



```
  =Pack your bags)(24F=906709.57460.qm@web113905.mail.gq1.yahoo.com)
 (250=<4B15846A.3060008@m57.biz>)(252=1299)(256
  =Ooh! When will this happen?! I've always wanted to go on a Mediterranean \
cruise. Should I put a date on my calendar? ______________________________ F\
rom: Charlie <charlie@m57.biz> To: Alix Pery <alix.pery@yahoo.com> Sent: Tue, \
December 1, 2009 1:02)(258=MAILER-DAEMON (Mail Delivery System\))(259
```

Figure 5: Vacation Plan



```
  =Charlie So when does the new car arrive? That sucks that the dealer didn'\
t have= the one you wanted in stock. I hope it isn't too long of a wait. Rub)>
[180C4E:^80(^C5^2E9)]
@$$}1BA}@
```

Figure 6: New Car

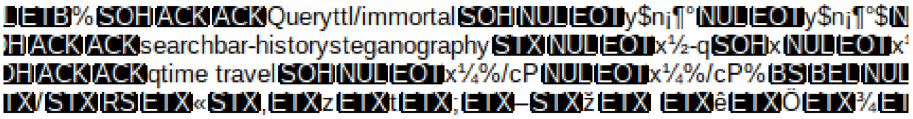
[3] Ref: Table 1(1)

[4] Ref: Table 1(1, 2)

[5] Ref: Table 1(1)

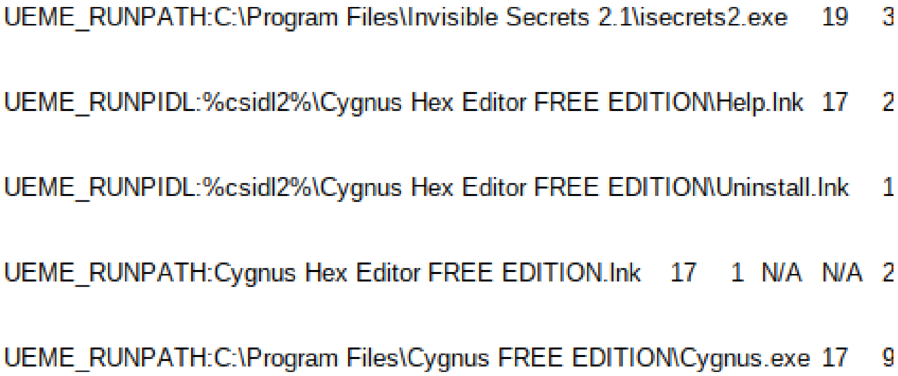
## 3.2 Methods And Techniques

Upon further investigation, it was discovered that Charlie had employed steganography techniques to exfiltrate data without detection. Steganography refers to the method of concealing sensitive information within seemingly unrelated or innocuous files(Bender et al., 1996). Evidence supporting this claim includes the presence of two software programs on his computer, Invisible Secrets 2(East-Tec, n.d.) and Cygnus Hex Editor(SoftCircuits, n.d.), both of which are known to facilitate steganographic techniques[6](phosphore, 2015). Moreover, the term "steganography" appears in Charlie's search history, further strengthening this suspicion[7].



```
LETB%SOHACKACKQueryttl/immortalSOHNULEOTy$n¡¶°NULEOTy$n¡¶°$N
)HACKACKsearchbar-historysteganographySTXNULEOTx½-qSOHxNULEOTx
)HACKACKqtime travelSOHNULEOTx¼%/cPNULEOTx¼%/cP%BSBELNUL
TX/STXRSETX«STX,ETXzETXtETX;ETX–STXžETX ETXêETXÖETX¾ET
```

Figure 7: Steganography Search

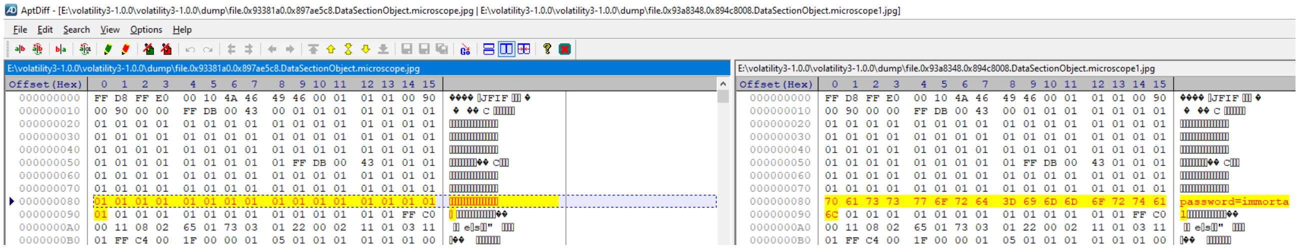


```
UEME_RUNPATH:C:\Program Files\Invisible Secrets 2.1\isecrets2.exe    19    3

UEME_RUNPIDL:%csidl2%\Cygnus Hex Editor FREE EDITION\Help.lnk  17    2

UEME_RUNPIDL:%csidl2%\Cygnus Hex Editor FREE EDITION\Uninstall.lnk    1

UEME_RUNPATH:Cygnus Hex Editor FREE EDITION.lnk    17    1  N/A   N/A  2

UEME_RUNPATH:C:\Program Files\Cygnus FREE EDITION\Cygnus.exe  17    9
```

Figure 8: Invisible Secrets 2 & Cygnus Hex Editor Presence

Additional verification was found in the form of multiple .jpg image files on Charlie's computer, depicting seemingly random and unrelated subjects, such as an astronaut and a microscope[8]. Each of these images has a secondary version, and upon conducting a binary analysis of the files, hidden information was discovered within the files[9]. Notably, a password, "Immortal," was embedded within the microscope1.jpg file but not present in the original microscope.jpg image[10]. Given that Charlie had access to confidential files related to M57.biz projects, it is highly plausible that he used steganography to secretly sell this information.

[6] Ref: Table 1(7)
[7] Ref: Table 1(2)
[8] Ref: Table 1(3, 5)
[9] Ref: Table 1(4, 6)
[10] Ref: Table 1(8)



AptDiff - [E:\volatility3-1.0.0\volatility3-1.0.0\dump\file.0x93381a0.0x897ae5c8.DataSectionObject.microscope.jpg | E:\volatility3-1.0.0\volatility3-1.0.0\dump\file.0x93a8348.0x894c8008.DataSectionObject.microscope1.jpg]

E:\volatility3-1.0.0\volatility3-1.0.0\dump\file.0x93381a0.0x897ae5c8.DataSectionObject.microscope.jpg

```
Offset(Hex)  0  1  2  3   4  5  6  7   8  9 10 11  12 13 14 15
000000000   FF D8 FF E0  00 10 4A 46  49 46 00 01  01 01 00 90   ���� ▯JFIF ▯▯▯ �
000000010   00 90 00 00  FF DB 00 43  00 01 01 01  01 01 01 01    �  �� C ▯▯▯▯▯▯▯
000000020   01 01 01 01  01 01 01 01  01 01 01 01  01 01 01 01   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
000000030   01 01 01 01  01 01 01 01  01 01 01 01  01 01 01 01   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
000000040   01 01 01 01  01 01 01 01  01 01 01 01  01 01 01 01   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
000000050   01 01 01 01  01 01 01 01  01 FF DB 00  43 01 01 01   ▯▯▯▯▯▯▯▯▯�� C▯▯▯
000000060   01 01 01 01  01 01 01 01  01 01 01 01  01 01 01 01   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
000000070   01 01 01 01  01 01 01 01  01 01 01 01  01 01 01 01   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
000000080   01 01 01 01  01 01 01 01  01 01 01 01  01 01 01 01   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
000000090   01 01 01 01  01 01 01 01  01 01 01 01  01 01 FF C0   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯��
0000000A0   00 11 08 02  65 01 73 03  01 22 00 02  11 01 03 11    ▯▯ e▯s▯▯"  ▯▯▯▯
0000000B0   01 FF C4 00  1F 00 00 01  05 01 01 01  01 01 01 00   ▯��   ▯▯▯▯▯▯▯▯
```

E:\volatility3-1.0.0\volatility3-1.0.0\dump\file.0x93a8348.0x894c8008.DataSectionObject.microscope1.jpg

```
Offset(Hex)  0  1  2  3   4  5  6  7   8  9 10 11  12 13 14 15
000000000   FF D8 FF E0  00 10 4A 46  49 46 00 01  01 01 00 90   ���� ▯JFIF ▯▯▯ �
000000010   00 90 00 00  FF DB 00 43  00 01 01 01  01 01 01 01    �  �� C ▯▯▯▯▯▯▯
000000020   01 01 01 01  01 01 01 01  01 01 01 01  01 01 01 01   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
000000030   01 01 01 01  01 01 01 01  01 01 01 01  01 01 01 01   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
000000040   01 01 01 01  01 01 01 01  01 01 01 01  01 01 01 01   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
000000050   01 01 01 01  01 01 01 01  01 FF DB 00  43 01 01 01   ▯▯▯▯▯▯▯▯▯�� C▯▯▯
000000060   01 01 01 01  01 01 01 01  01 01 01 01  01 01 01 01   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
000000070   01 01 01 01  01 01 01 01  01 01 01 01  01 01 01 01   ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
000000080   70 61 73 73  77 6F 72 64  3D 69 6D 6D  6F 72 74 61   password=immorta
000000090   6C 01 01 01  01 01 01 01  01 01 01 01  01 01 FF C0   l▯▯▯▯▯▯▯▯▯▯▯▯▯��
0000000A0   00 11 08 02  65 01 73 03  01 22 00 02  11 01 03 11    ▯▯ e▯s▯▯"  ▯▯▯▯
0000000B0   01 FF C4 00  1F 00 00 01  05 01 01 01  01 01 01 00   ▯��   ▯▯▯▯▯▯▯▯
```

Figure 9: Password hidden in image file

In summary, the evidence suggests that Charlie Brown has engaged in the illicit sale of confidential information to a competitor, Project2400, by employing steganographic techniques to exfiltrate data without detection. The sudden increase in his personal finances, as evidenced by his vacation plans and interest in purchasing a new car, further corroborates the suspicion that he has profited from these activities. The investigation into Charlie's actions should continue to ascertain the full extent of the potential breach and to ensure that the necessary steps are taken to mitigate any potential damage caused by the sale of sensitive information.

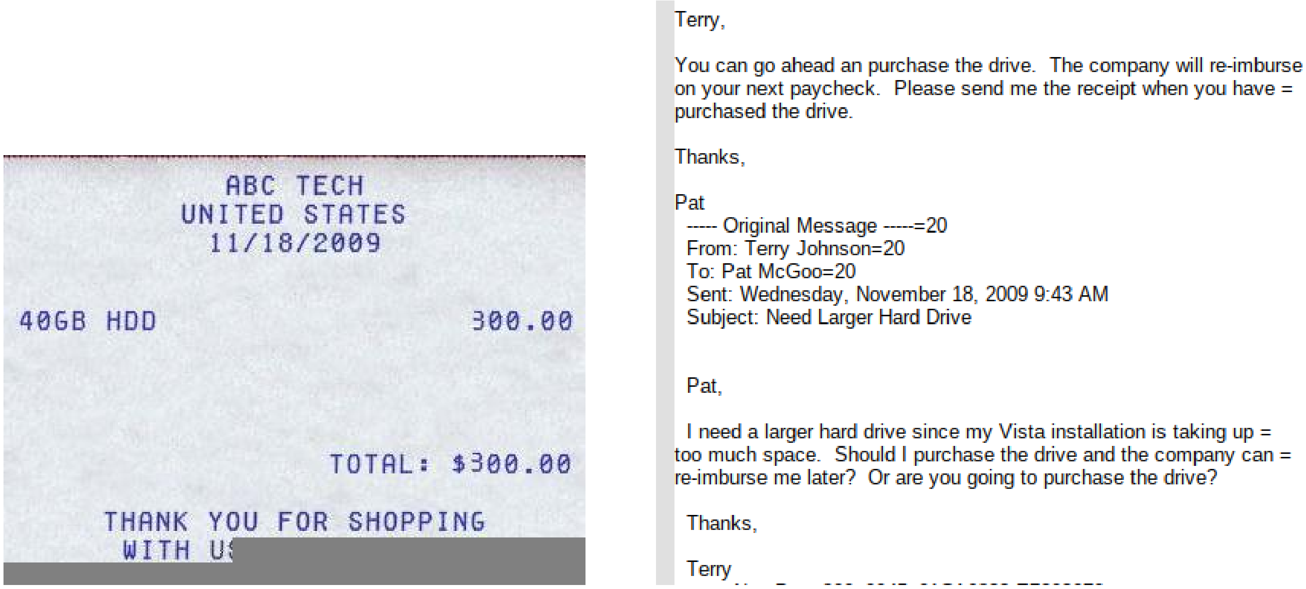
# 4 Incident: Theft

Terry, the Head of IT at M57.biz, appears to be engaging in embezzlement and theft of company resources. As the individual responsible for purchasing and installing computer hardware, as well as managing the inventory, Terry's actions and email correspondence suggest potential fraudulent activities.

| No. | Date and Time | Event | Persons Involved | Source |
|---|---|---|---|---|
| 1 | 18/Nov | Terry Johnson purchases hard drive at ABC Tech | Terry Johnson | Table 2(1) |
| 2 | 19/Nov | Terry Johnson emails receipt for hard drive to Pat McGoo | Terry Johnson<br>Pat McGoo | Table 2(2) |
| 3 | 20/Nov | Jo Smith's computer is replaced, Terry assumes responsibility for the computer | Terry Johnson<br>Jo Smith<br>Pat McGoo | Table 2(4) |
| 4 | 30/Nov | Terry Johnson announces setup of new printer for the office | Terry Johnson | Table 2(15) |
| 5 | 30/Nov | Terry Johnson sells computer to Aaron Greene on Craigslist | Terry Johnson<br>Aaron Greene | Table 2(6) |
| 6 | 03/Dec 17:30 | XP Advanced Keylogger is installed on Terry Johnson's computer | Terry Johnson | Table 2(13) |
| 7 | 03/Dec 18:19 | XP Advanced Keylogger is ran on Pat McGoo's computer from external E: drive | Pat McGoo | Table 2(12) |
| 8 | 04/Dec | Terry Johnson announces he will perform some software changes on the anti virus on Monday (07/Dec) | Terry Johnson | Table 1(1) |
| 9 | 07/Dec | VNC Software is installed on Pat McGoo's computer | Unclear | Table 2(12) |
| 10 | 09/Dec | Terry Johnson lists HP Printer for sale on Craigslist | Terry Johnson | Table 2(5) |
| 11 | 10/Dec | Pat McGoo requests a full inventory on M57.biz | Pat McGoo<br>Terry Johnson | Table 2(9) |
| 12 | 11/Dec 08:54 | Pat McGoo announces police investigation into M57.biz | Pat McGoo | Table 1(1) |
| 13 | 11/Dec 19:22 | CCleaner software is run on Terry Johnson's computer | Terry Johnson | Table 2(13) |

Table 4: Timeline of events relating to Terry Johnson

## 4.1 Embezzlement



ABC TECH
UNITED STATES
11/18/2009

40GB HDD 300.00

TOTAL: $300.00

THANK YOU FOR SHOPPING
WITH U

(a) ABC Tech Receipt

Terry,

You can go ahead an purchase the drive. The company will re-imburse 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?

Thanks,

Terry

(b) Terry Requesting Reimbursement

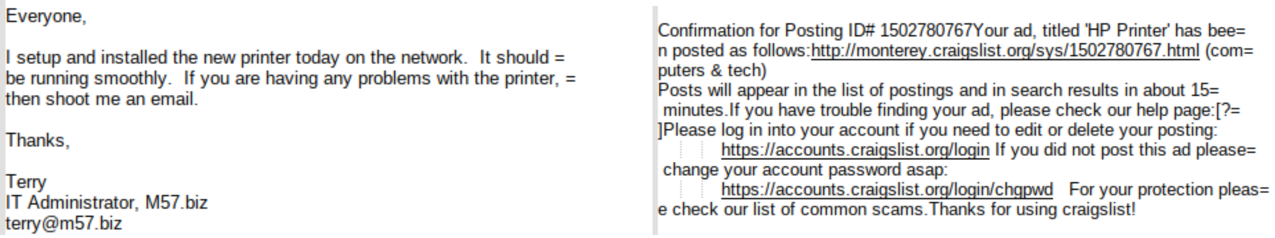
Figure 10: Request & Receipt For HDD

One suspicious incident involves the purchase of a 40GB hard drive from ABC Tech for a price of 300 USD, as mentioned in an email exchange with Pat McGoo[11]. The cost of the hard drive seems excessively high, especially considering its size(Klein, 2022). Although there is no direct evidence indicating that Terry altered the receipt or misrepresented the price, the presence of multiple versions of the receipt (ABCTECH_RECEIPT.jpg and ABCTECH_RECEIPT_pat.jpg) and the peculiar nature of the email correspondence raise suspicions[12]. Verification of the actual cost of the hard drive can be obtained through contacting ABC Tech or checking Terry's bank transactions.

[11] Ref: Table 2(2)
[12] Ref: Table 2(11)

## 4.2 Theft And Resale

Additionally, Terry seems to be stealing company property and reselling it for personal profit. After installing a new printer for the office on 30/11/2009[13], Terry listed a printer for sale on Craigslist a week later (09/12/2009)[14].



Everyone,

I setup and installed the new printer today on the network. It should =
be running smoothly. If you are having any problems with the printer, =
then shoot me an email.

Thanks,

Terry
IT Administrator, M57.biz
terry@m57.biz

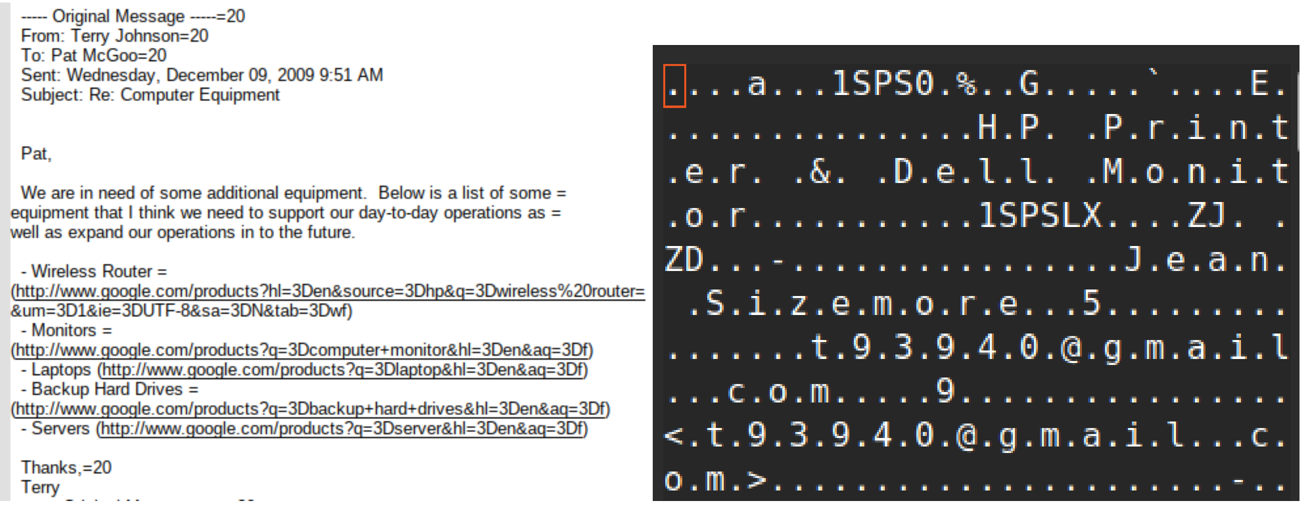
(a) New Printer Announcement

Confirmation for Posting ID# 1502780767Your ad, titled 'HP Printer' has bee=
n posted as follows:http://monterey.craigslist.org/sys/1502780767.html (com=
puters & tech)
Posts will appear in the list of postings and in search results in about 15=
 minutes.If you have trouble finding your ad, please check our help page:[?=
]Please log in into your account if you need to edit or delete your posting:
https://accounts.craigslist.org/login If you did not post this ad please=
 change your account password asap:
https://accounts.craigslist.org/login/chgpwd For your protection pleas=
e check our list of common scams.Thanks for using craigslist!

(b) Craigslist Post for HP Printer

Figure 11: New Printer & HP Printer For Sale

He further requested a new monitor and laptop on the same day[15], and there is an indication that he may have a monitor for sale alongside the printer[16].



----- Original Message -----=20
From: Terry Johnson=20
To: Pat McGoo=20
Sent: Wednesday, December 09, 2009 9:51 AM
Subject: Re: Computer Equipment

Pat,

We are in need of some additional equipment. Below is a list of some =
equipment that I think we need to support our day-to-day operations as =
well as expand our operations in to the future.

- Wireless Router =
(http://www.google.com/products?hl=3Den&source=3Dhp&q=3Dwireless%20router=
&um=3D1&ie=3DUTF-8&sa=3DN&tab=3Dwf)
- Monitors =
(http://www.google.com/products?q=3Dcomputer+monitor&hl=3Den&aq=3Df)
- Laptops (http://www.google.com/products?q=3Dlaptop&hl=3Den&aq=3Df)
- Backup Hard Drives =
(http://www.google.com/products?q=3Dbackup+hard+drives&hl=3Den&aq=3Df)
- Servers (http://www.google.com/products?q=3Dserver&hl=3Den&aq=3Df)

Thanks,=20
Terry

(a) Terry Requesting Equipment

```
....a...1SPS0.%..G.....`.....E.
...............H.P.  .P.r.i.n.t
.e.r.  .&.  .D.e.l.l.  .M.o.n.i.t
.o.r..............1SPSLX....ZJ. .
ZD...-.................J.e.a.n.
 .S.i.z.e.m.o.r.e...5.........
.......t.9.3.9.4.0.@.g.m.a.i.l
...c.o.m.....9...................
<.t.9.3.9.4.0.@.g.m.a.i.l...c.
o.m.>.....................-..
```

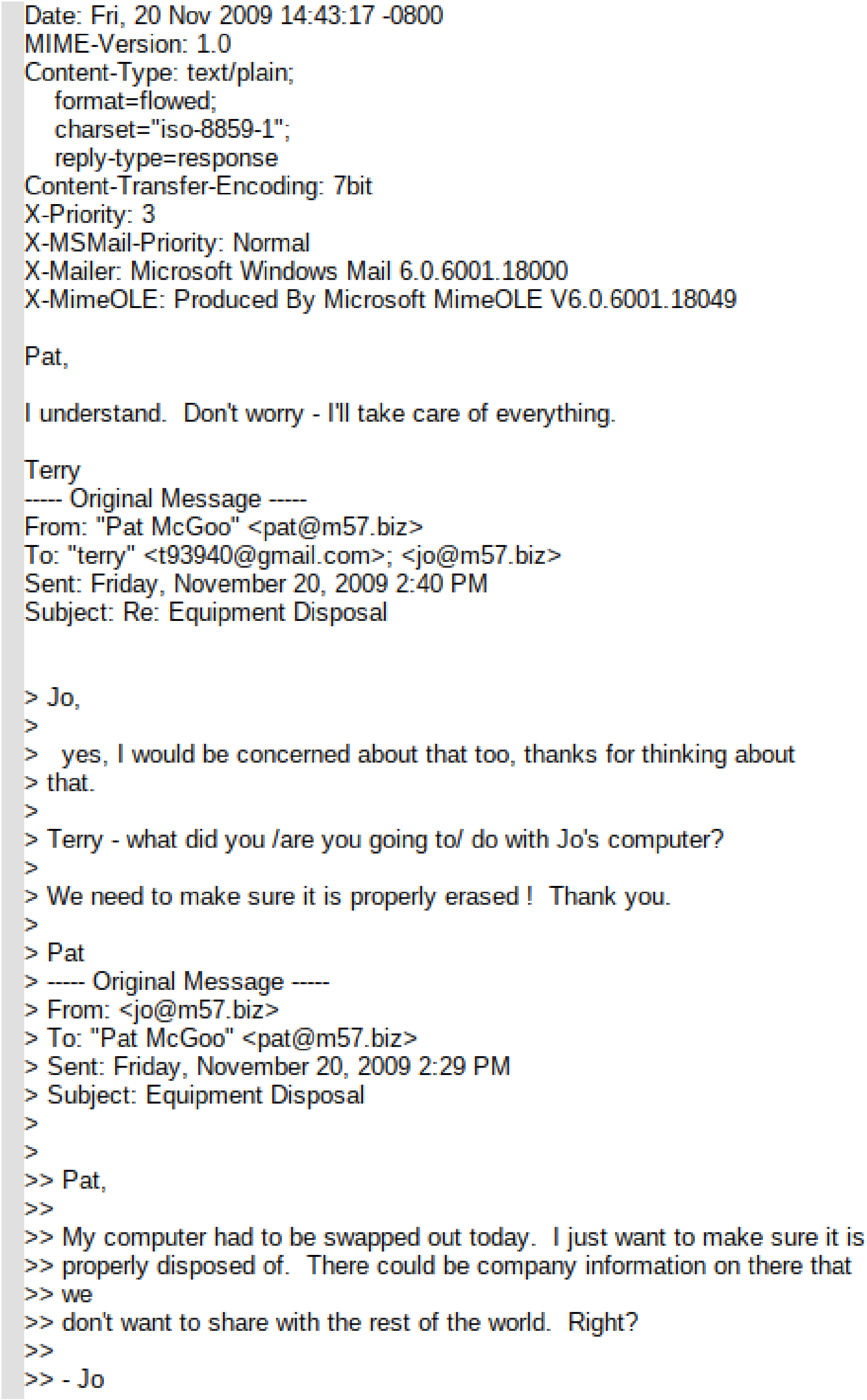
(b) Potential Craigslist Ad For Printer And Monitor

Figure 12: Monitor Request

The laptop request is particularly noteworthy due to the existence of a laptop in police inventory containing confidential information from M57.biz. Considering the email correspondance between Pat McGoo, Jo Smith, and Terry Johnson on 20/11 concerning the disposal of equipment shows Jo recieved a new computer and that she was concerned the old one would not be properly disposed of[17]. Terry assures both he will take care of it. Pat McGoo's email requesting serial numbers for Terry's recent inventory, specifically Jo Smith's computer (C111),

[13] Ref: Table 2(15)
[14] Ref: Table 2(5)
[15] Ref: Table 2(3)
[16] Ref: Table 2(10)
[17] Ref: Table 2(4)

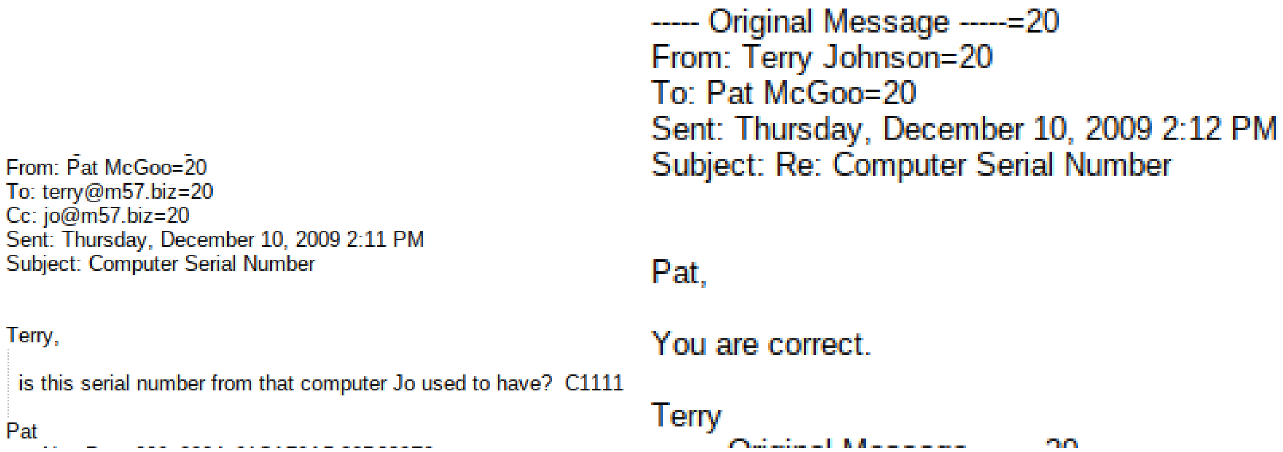
should be cross-referenced with the laptop recovered by the police[18]. Furthermore, it would be highly revealing if Aaron Greene, who purchased a computer from Terry on 30/11/2009, was found to be the buyer of the recovered laptop and if the laptop in police custody matches Jo Smith's computer.



```
Date: Fri, 20 Nov 2009 14:43:17 -0800
MIME-Version: 1.0
Content-Type: text/plain;
    format=flowed;
    charset="iso-8859-1";
    reply-type=response
Content-Transfer-Encoding: 7bit
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

Pat,

I understand.  Don't worry - I'll take care of everything.

Terry
----- Original Message -----
From: "Pat McGoo" <pat@m57.biz>
To: "terry" <t93940@gmail.com>; <jo@m57.biz>
Sent: Friday, November 20, 2009 2:40 PM
Subject: Re: Equipment Disposal


> Jo,
>
>   yes, I would be concerned about that too, thanks for thinking about
> that.
>
> Terry - what did you /are you going to/ do with Jo's computer?
>
> We need to make sure it is properly erased !  Thank you.
>
> Pat
> ----- Original Message -----
> From: <jo@m57.biz>
> To: "Pat McGoo" <pat@m57.biz>
> Sent: Friday, November 20, 2009 2:29 PM
> Subject: Equipment Disposal
>
>
>> Pat,
>>
>> My computer had to be swapped out today.  I just want to make sure it is
>> properly disposed of.  There could be company information on there that
>> we
>> don't want to share with the rest of the world.  Right?
>>
>> - Jo
```

Figure 13: Discussion On Jo Smith's Old Computer

[18] Ref: Table 2(9)



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

(a) Serial Number Request

----- Original Message -----=20
From: Terry Johnson=20
To: Pat McGoo=20
Sent: Thursday, December 10, 2009 2:12 PM
Subject: Re: Computer Serial Number

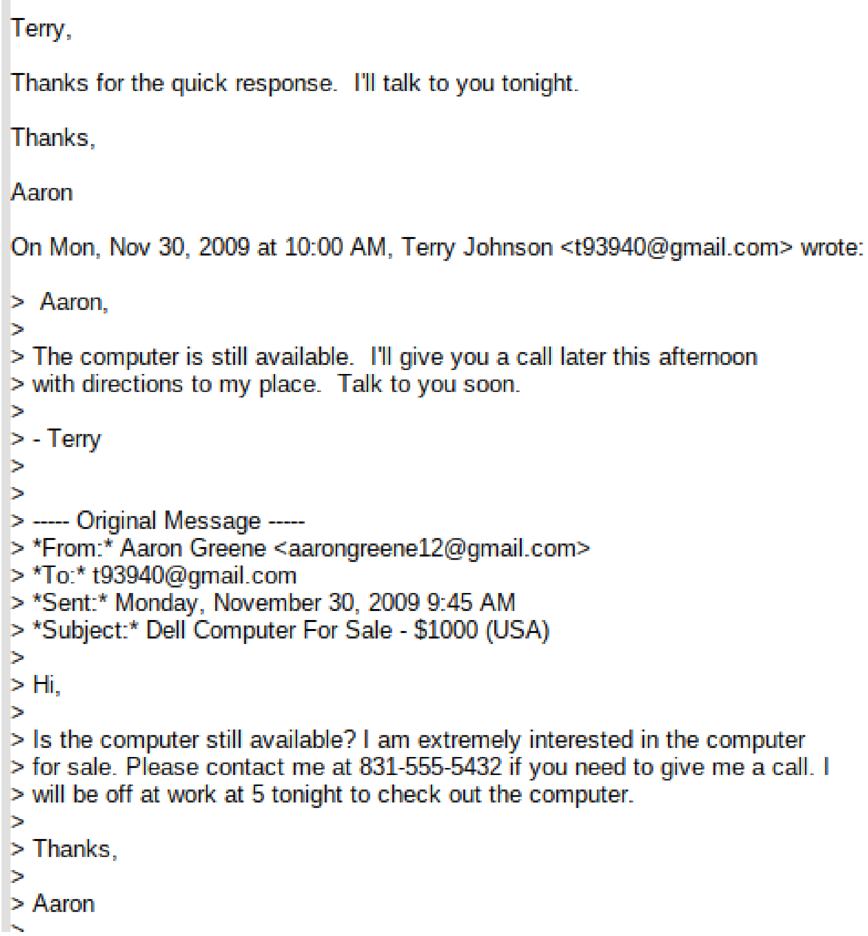
Pat,

You are correct.

Terry

(b) Serial Number Confirmation

Figure 14: Serial Number Discussion



Terry,

Thanks for the quick response.  I'll talk to you tonight.

Thanks,

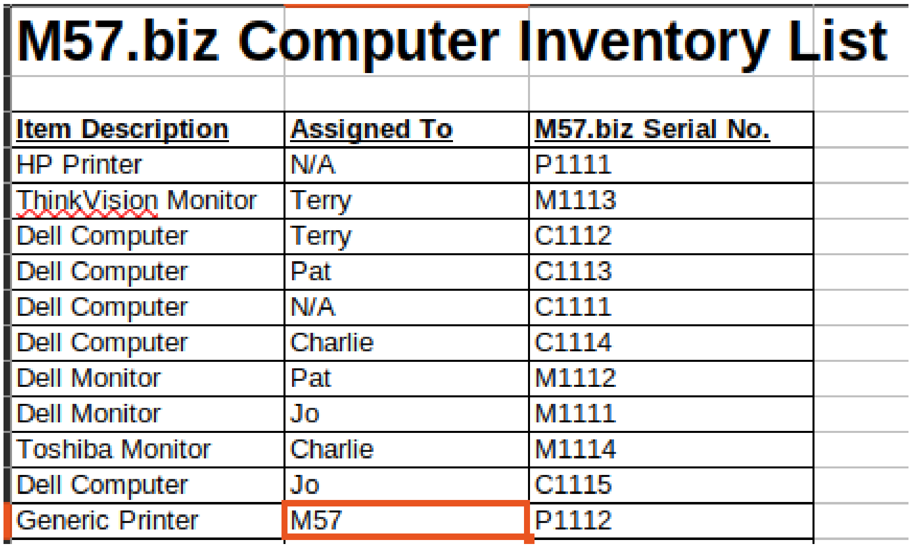
Aaron

On Mon, Nov 30, 2009 at 10:00 AM, Terry Johnson <t93940@gmail.com> wrote:

```
>  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
```

Figure 15: Discussion On Sale Of Computer

Pat McGoo requested a full inventory list of the M57.biz, and tasked Terry to do so[19]. This was following the discussion around Jo Smith's computer, and its serial number. This list is also available in the evidence collected, and could be considered quite telling. Here it lists, as confirmed by Terry Johnson, the serial number of Jo Smith's computer (C111), but it also shows a HP Printer assigned to N/A as well as listing C1111's owner to be N/A as well[20]. This inventory was done by Terry Johnson and cross referencing the serial number on the printer with the HP Printer Terry has for sale on craigslist should be done to further clarify the situation.



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 |

Figure 16: M57 Inventory

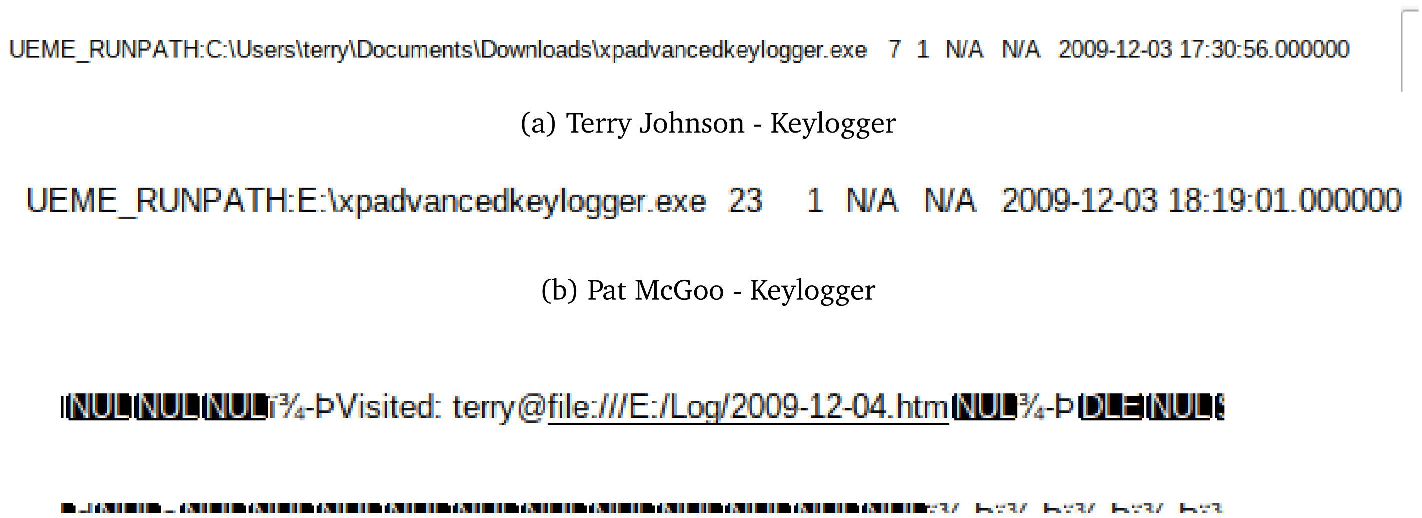
## 4.3 Espionage

Terry is also suspected of spying on Pat McGoo, presumably as a precautionary measure to conceal his illegal activities. Evidence for this suspicion includes the presence of keylogger software on both computers and the installation of VNC software (Lee, 2019 on Pat's computer, allowing Terry remote access to monitor Pat's activities[21]. On 03/12/2009, Terry executed the XP Advanced Keylogger from his downloads folder, and shortly after, the same keylogger software was run on Pat McGoo's computer from an external E: drive. Terry's file explorer history contains references to an E: drive, suggesting that he installed the keylogger on an external drive to discreetly run the software on Pat's system.

[19] Ref: Table 2(9)

[20] Ref: Table 2(14)

[21] Ref: Table 2(12, 13)



```
UEME_RUNPATH:C:\Users\terry\Documents\Downloads\xpadvancedkeylogger.exe   7   1   N/A   N/A   2009-12-03 17:30:56.000000
```

(a) Terry Johnson - Keylogger

```
UEME_RUNPATH:E:\xpadvancedkeylogger.exe   23    1   N/A   N/A   2009-12-03 18:19:01.000000
```

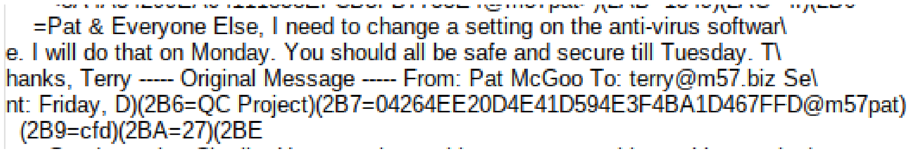
(b) Pat McGoo - Keylogger

```
NULNULNULï¾-ÞVisited: terry@file:///E:/Log/2009-12-04.htmNUL¾-ÞDLENUL
```

(c) Terry Johnson - E: Drive

Figure 17: Serial Number Discussion

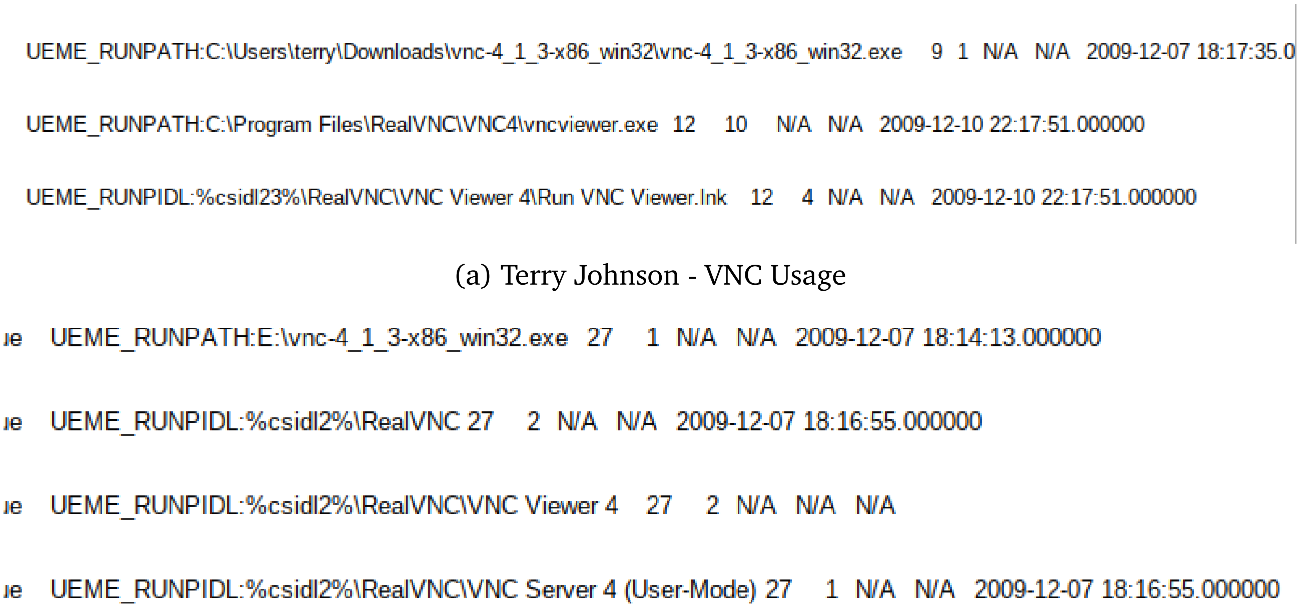
On 04/12/2009, Terry informed his colleagues about upcoming antivirus software updates, which he would perform on the following Monday (07/12/2009)[22]. On that day, VNC software was installed on Pat's computer from an external E: drive (18:14) and configured in server mode[23]. Later that evening (22:17), Terry ran the VNC viewer client, indicating that he used the antivirus update as a cover to install remote access tools on Pat's computer and monitor him from his own machine[24].



```
  =Pat & Everyone Else, I need to change a setting on the anti-virus softwar\
e. I will do that on Monday. You should all be safe and secure till Tuesday. T\
hanks, Terry ----- Original Message ----- From: Pat McGoo To: terry@m57.biz Se\
nt: Friday, D)(2B6=QC Project)(2B7=04264EE20D4E41D594E3F4BA1D467FFD@m57pat)
 (2B9=cfd)(2BA=27)(2BE
```

Figure 18: Terry Announcing Change In AV Software (Monday 07/12/2009)

[22] Ref: Table 1(1)
[23] Ref: Table 2(12)
[24] Ref: Table 2(13)



```
UEME_RUNPATH:C:\Users\terry\Downloads\vnc-4_1_3-x86_win32\vnc-4_1_3-x86_win32.exe    9  1  N/A   N/A   2009-12-07 18:17:35.0

UEME_RUNPATH:C:\Program Files\RealVNC\VNC4\vncviewer.exe  12    10    N/A  N/A  2009-12-10 22:17:51.000000

UEME_RUNPIDL:%csidl23%\RealVNC\VNC Viewer 4\Run VNC Viewer.lnk    12    4  N/A   N/A   2009-12-10 22:17:51.000000
```

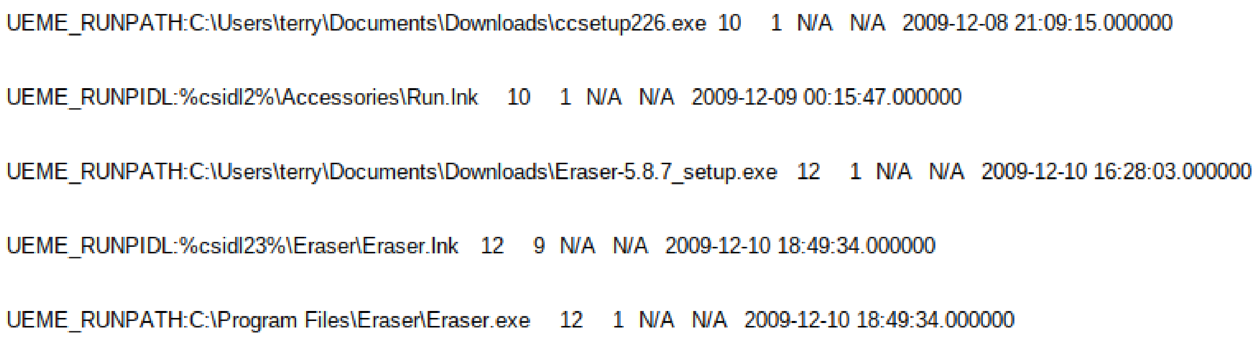
(a) Terry Johnson - VNC Usage

```
ıe  UEME_RUNPATH:E:\vnc-4_1_3-x86_win32.exe  27    1  N/A   N/A   2009-12-07 18:14:13.000000

ıe  UEME_RUNPIDL:%csidl2%\RealVNC 27    2  N/A   N/A   2009-12-07 18:16:55.000000

ıe  UEME_RUNPIDL:%csidl2%\RealVNC\VNC Viewer 4    27    2  N/A   N/A   N/A

ıe  UEME_RUNPIDL:%csidl2%\RealVNC\VNC Server 4 (User-Mode) 27    1  N/A   N/A   2009-12-07 18:16:55.000000
```

(b) Pat McGoo - VNC Usage

Figure 19: VNC Installation

Moreover, Terry has employed file deletion software, such as CCleaner and Eraser, likely to cover his tracks when engaging in illegal activities[25]. For instance, the VNC download is visible in the file explorer history but seems to be missing from the disk itself, possibly due to the use of file deletion software. Further investigation through disk analysis may reveal more information about Terry's activities.



```
UEME_RUNPATH:C:\Users\terry\Documents\Downloads\ccsetup226.exe  10    1  N/A   N/A   2009-12-08 21:09:15.000000

UEME_RUNPIDL:%csidl2%\Accessories\Run.lnk    10    1  N/A   N/A   2009-12-09 00:15:47.000000

UEME_RUNPATH:C:\Users\terry\Documents\Downloads\Eraser-5.8.7_setup.exe    12    1  N/A   N/A   2009-12-10 16:28:03.000000

UEME_RUNPIDL:%csidl23%\Eraser\Eraser.lnk    12    9  N/A   N/A   2009-12-10 18:49:34.000000

UEME_RUNPATH:C:\Program Files\Eraser\Eraser.exe    12    1  N/A   N/A   2009-12-10 18:49:34.000000
```

Figure 20: CCleaner & Eraser Software Presence

[25] Ref: Table 2(13)

# 5 Conclusion

## 5.1 Reccomendations

In light of the recent incident involving data exfiltration, employee theft, and espionage, its strongly recommended to implement the following security measures to protect the company's assets and reputation:

1. Create a formal process for approving and completing hardware and software purchases. Consider business accounts, and avoid employees personally purchasing resources. Implement additional oversight, particularly for IT department purchases, to ensure transparency and accountability.

2. Implement strict procedures for tracking and disposing of company equipment. This should include proper documentation and verification of disposal to prevent unauthorized sales or re-purposing of assets.

3. Enhance the monitoring of IT department activities by increasing oversight through more frequent audits and implementing monitoring systems to track actions such as software installations, hardware changes, and system access. This will help identify and prevent unauthorized activities.

4. Implement a secure and robust software update policy and routine. Ensure all actions are legitimate and logged for later audit or independent verification.

5. Regularly assess and improve the effectiveness of your security measures. Ensure the security measures are tested and audited, to uncover flaws or weaknesses.

Implementing such measures will help mitigate future incidents and ensure a higher level of safety and control over the actions of the company and its employees.

# References

Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, *35*(3.4), 313–336. https://doi.org/10.1147/sj.353.0313

East-Tec. (n.d.). Invisible Secrets [Accessed on: May 10, 2023].

Klein, A. (2022). *Hard drive cost per gigabyte*. Retrieved May 11, 2022, from https://www.backblaze.com/blog/hard-drive-cost-per-gigabyte/

Lee, J. (2019). How to protect yourself from unethical or illegal spying. *MakeUseOf*. Retrieved June 1, 2022, from https://www.makeuseof.com/tag/how-to-protect-yourself-from-unethical-or-illegal-spying/

phosphore. (2015). Steganography 101 [Accessed: May 10, 2023].

SoftCircuits. (n.d.). CygnusFE [Accessed: May 10, 2023].