

Digital Forensics Project

Done By:
Sherwinna Chua
Joel Ng
Keith Tan
Aldric Chong
Jovan Ho



Background Introduction

- Aaron Greene found Kitty exploitation movies and pictures on computer (MT-2009-12-015-EV001) purchased from Craigslist.
- Computer belongs Johnson Smith from M57 Patents.
- Police spoke to CEO Pat McGoo before confiscating Jo USB thumb drive which used for transferring kitty exploitation material.

Employees of interest:

- o CEO: Pat McGoo
- o IT Administrator: Terry
- o Patent Researchers: Jo, Charlie



Our Task

Analyze criminal charges and civil litigation on kitty exploitation videos

Investigate other suspicious activities based on image provided



Timeline

09-11-2009

Joined the company



16-11-2009

First day in Company



17-11-2009

Downloaded software to
computer



18-11-2009

Jo's computer slow
down



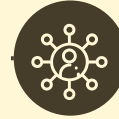
21-11-2009

Terry swap out Jo's
computer. Also put
PDF in Pat computer.



24-11-2009

Terry told Charlie suit case
bought from poker money.
Also created Craigslist account



11-12-2009

Jean buy both listed items. While
Cod asked Terry join for poker. Pat
is also suspicious of Terry work.



12-12-2009

Pat called for urgent
meeting after police
called



10-12-2009

Terry post Dell monitor and
HP printer on craigslist over
the course of 2 days



4-12-2009

Pat computer slow
down and Terry fix it.



30-11-2009

Aaron purchase computer for
\$1000



TABLE OF CONTENTS

01 Intro

Background, Task,
Timeline

02 Jo

Kitty Exploitation!

03 Pat

Victim of
eavesdropping

04 Charlie

- Corporate espionage
- Extortion

05 Terry




- Receipt forgery
- Eavesdropping on Pat

06 Conclusion

Kitty Exploitation Found

From 12/11

- Jo's Computer
 - Kitty exploitation pictures and movies found
 - Pictures created on 12/11/2009 at 4:37:23 PM
 - Videos created on 12/11/2009 4:37:28 PM

cord	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
							

Kitty Exploitation Found

From 11/20

- Jo's Work USB:
 - Encrypted Images and videos found

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

Kitty Exploitation Found

From 11/17

- Jo's Favourites USB:
 - First appearance of Kitty exploitations found on the Favourites USB
 - 11/17/2009 8:35:13 PM

A	B	C	D	E	F	G	H
							
50	Evidence				DSC00003.JPG .JPG	11/17/2009 8:35:13 PM	11/23/2009
							
44	Evidence				DSC00005.JPG .JPG	11/17/2009 8:35:15 PM	11/23/2009
							

Kitty Exploitation Found

From 11/17

- Jo's Favourites USB:
 - Matching hashes for files on Favorites USB and Jo's Computer

File Name	hr_patent69.JPG
File Extension	.JPG
Created Date/Time	11/12/09 08:37:25 AM
Last Accessed Date/Time	11/12/09 08:37:25 AM
Last Modified Date/Time	08/11/09 11:28:28 AM
Size (Bytes)	622799
Skin Tone Percentage	81.1
Original Width	2304
Original Height	1296
Exif Extraction Status	Complete
Created Date/Time - Local Time	08/11/09 11:28:29 AM (Local time)
Modified Date/Time - Local Time	08/11/09 11:28:29 AM (Local time)
Make	SONY
Model	HDR-SR10
Exif Data	Extraction Result: Complete ImageWidth: 2304 ImageHeight: 1296 DateTimeOriginal: 11/08/2009 11:28:29 CreateDate: 11/08/2009 11:28:29 ModifyDate: 11/08/2009 11:28:29 Make: SONY Model: HDR-SR10
MD5 Hash	34a248ffbc03c1b96e2225b788f71fd6
SHA1 Hash	7276959a00da00c00022c2bf869a710cb6eb2cc2

ARTIFACT INFORMATION

File Name	DSC00071.JPG
File Extension	.JPG
Created Date/Time	17/11/09 12:36:15 PM
Last Accessed Date/Time	23/11/09 08:00:00 AM
Last Modified Date/Time	07/11/09 07:28:28 PM
Size (Bytes)	622799
Skin Tone Percentage	81.1
Original Width	2304
Original Height	1296
Exif Extraction Status	Complete
Created Date/Time - Local Time	08/11/09 11:28:29 AM (Local time)
Modified Date/Time - Local Time	08/11/09 11:28:29 AM (Local time)
Make	SONY
Model	HDR-SR10
Exif Data	Extraction Result: Complete ImageWidth: 2304 ImageHeight: 1296 DateTimeOriginal: 11/08/2009 11:28:29 CreateDate: 11/08/2009 11:28:29 ModifyDate: 11/08/2009 11:28:29 Make: SONY Model: HDR-SR10
MD5 Hash	34a248ffbc03c1b96e2225b788f71fd6
SHA1 Hash	7276959a00da00c00022c2bf869a710cb6eb2cc2
Artifact Name	EXIF Data



03

Pat






Keylogger Found!

From 03/12

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

MATCHING RESULTS (20 of 225)

Row view

	REGSVR32.EXE PREFETCH FILES - WINDOWS XP/VISTA/7 ... Application Path : \DEVICE\HARDDISKVOLUM CREATE EXPORT / REPORT SAVE ARTIFACT TO... OPEN SOURCE FILE WITH	File Created Date/Time 3/12/2009 6:17:48 PM
	DRWTSN32.EXE PREFETCH FILES - WINDOWS XP/VISTA/7 ... Application Path : \DEVICE\HARDDISKVOLUM	File Created Date/Time 16/11/2009 7:45:30 PM
	DWWIN.EXE PREFETCH FILES - WINDOWS XP/VISTA/7 ... Application Path : \DEVICE\HARDDISKVOLUM	File Created Date/Time 16/11/2009 7:45:08 PM
	VERCLSID.EXE PREFETCH FILES - WINDOWS XP/VISTA/7 ... Application Path : \DEVICE\HARDDISKVOLUM	File Created Date/Time 1/12/2009 6:48:48 PM
	NTOSBOOT PREFETCH FILES - WINDOWS XP/VISTA/7 ... Application Path : \DEVICE\HARDDISKVOLUM	File Created Date/Time 9/11/2009 1:18:17 AM

REGSVR32.EXE

pat-2009-12-11.E01

PREVIEW

FIND

EXPLORER\DESKTOP.HTT
\DEVICE\HARDDISKVOLUME1\WINDOWS\WI
\DEVICE\HARDDISKVOLUME1\PROGRAM
FILES\XP
ADVANCED\DLLS\TOOLKEYLOGGER.DLL.DL
\DEVICE\HARDDISKVOLUME1\WINDOWS\WI
WW_F0B4C2DF\GDIPLUS.DLL
\DEVICE\HARDDISKVOLUME1\DOCUMENTS
AND SETTINGS\PAT\APPLICATION
DATA\MOZILLA\FIREFOX\PROFILES\6TX4MH
\DEVICE\HARDDISKVOLUME1\PROGRAM
FILES\AVG\AVG9\AVGPP.DLL
\DEVICE\HARDDISKVOLUME1\PROGRAM
FILES\AVG\AVG9\AVGSSIE.DLL







Keylogger Found!

From 03/12

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

MATCHING RESULTS (8 of 776)

Row view

	Last Modified Date/Time : 7/12/2009 4:04:24	7/12/2009 4:01:43 PM
	C:\Program Files\XP Advanced\Data\Tool... LNK FILES — Operating System Last Modified Date/Time : 7/12/2009 4:09:26	Created Date/Time 7/12/2009 4:09:26 PM
	C:\Program Files\XP Advanced\ToolKeylo... LNK FILES — Operating System Target File Last Modified Date/Time : 7/9/200 CREATE EXPORT / REPORT OPEN SOURCE FILE WITH...	Target File Created Date/Time 3/12/2009 6:19:22 PM
	C:\Program Files\XP Advanced\Data\Tool... LNK FILES — Operating System Target File Last Modified Date/Time : 7/12/20	Target File Created Date/Time 3/12/2009 6:19:47 PM
	C:\Program Files\XP Advanced\Data\Tool... LNK FILES — Operating System Last Modified Date/Time : 7/12/2009 4:09:26	Created Date/Time 7/12/2009 4:04:24 PM
	C:\Program Files\XP Advanced\Data\Tool... LNK FILES — Operating System Last Modified Date/Time : 7/12/2009 4:04:24	Created Date/Time 7/12/2009 4:01:43 PM

C:\Program Files\XP Advanced...

ARTIFACT INFORMATION

Linked Path	C:\Program Files\XP Advanced\ToolKeylogger.exe
Target File Created Date/Time	3/12/2009 6:19:22 PM
Target File Last Modified Date/Time	7/9/2005 3:57:02 AM
Target File Last Accessed Date/Time	3/12/2009 6:19:22 PM
Target Attributes	FILE_ATTRIBUTE_ARCHIVE
Drive Type	DRIVE_FIXED
Volume Serial Number	00E23C5C
Show Command	SW_SHOWNORMAL
Net Bios Name	m57-pat

Keylogger Found!

From 03/12

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

MATCHING RESULTS (2 of 14)

Row view ▼

ToolKeylogger.exe

MRU FOLDER ACCESS — Operating System

Folder Accessed : C:\Documents and Settings\

CREATE EXPORT / REPORT OPEN SOURCE FILE WITH...

ToolKeylogger.exe

MRU FOLDER ACCESS — Operating System

Folder Accessed : C:\Documents and Settings\

ToolKeylogger.exe



pat-2009-12-11.E01

DETAILS

ARTIFACT INFORMATION

Application Name	ToolKeylogger.exe
Folder Accessed	C:\Documents and Settings\Pat\Desktop\logs\20091203
Registry Order	4
Value Name	g
Artifact type	MRU Folder Access
Item ID	4013

EVIDENCE INFORMATION

Source pat-2009-12-11.E01 - Partition 1
(Microsoft NTFS, 12.11 GB)

Keylogger Found!

From 03/12

- File format for logs matches the files found on Terry's computer

Path	Path...	Acce...
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_000255a7_big.jpg	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_0002e11e_big.jpg	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_0004b041_big.jpg	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_000c2688_big.jpg	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04.htm	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_0002e11e_big.jpg	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_0004b041_big.jpg	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_00015be5_big.jpg	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_0004b041_big.jpg	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_000c2688_big.jpg	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_0002dbee_big.jpg	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-03.htm	Drive	
C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_000c2688_big.jpg	Drive	

pat-2009-12-11.E01

DETAILS











ARTIFACT INFORMATION

Path	C:\Program Files\XP Advanced\Data\ToolKeylogger\Log\2009-12-04_000255a7_big.jpg
Path Type	Drive
User	Pat
Artifact type	Locally Accessed Files and Folders
Item ID	20963
Original artifact	Internet Explorer Main History

Keylogger Found!

From 03/12

- File format for logs matches the files found on Terry's computer
- Files were deleted, but we managed to locate them in \$OrphanedFiles

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	

Remote Desktop Software!

From 07/12

RealVNC's VNC4

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.









Remote Desktop Software!

From 07/12

- First appearance: 9/11/2009

MATCHING RESULTS (14 of 225)

Row view

	PREFETCH FILES - WINDOWS XP/VISTA/7 —...	File Created Date/Time 1/12/2009 1:19:53 AM
	NTOSBOOT PREFETCH FILES - WINDOWS XP/VISTA/7 —... Application Path : \DEVICE\HARDDISKVOLUM CREATE EXPORT / REPORT SAVE ARTIFACT TO... OPEN SOURCE FILE WITH	File Created Date/Time 9/11/2009 1:18:17 AM
	LOGONU!.EXE PREFETCH FILES - WINDOWS XP/VISTA/7 —... Application Path : \DEVICE\HARDDISKVOLUM	File Created Date/Time 1/12/2009 12:05:12 AM
	DFRGNTFS.EXE PREFETCH FILES - WINDOWS XP/VISTA/7 —... Application Path : \DEVICE\HARDDISKVOLUM	File Created Date/Time 1/12/2009 5:22:50 PM
	VERCLSID.EXE PREFETCH FILES - WINDOWS XP/VISTA/7 —... Application Path : \DEVICE\HARDDISKVOLUM	File Created Date/Time 1/12/2009 6:48:48 PM
	NTOSBOOT PREFETCH FILES - WINDOWS XP/VISTA/7 —...	File Created Date/Time

NTOSBOOT

pat-2009-12-11.E01

PREVIEW

FIND
AND SETTINGS\ALL USERS\START
MENU\PROGRAMS\AVG FREE
9.0\UNINSTALL AVG FREE.LNK
\DEVICE\HARDDISKVOLUME1\PROGRAM
FILES\AVG\AVG9\SETUP.EXE
\DEVICE\HARDDISKVOLUME1\DOCUMENTS
AND SETTINGS\ALL USERS\START
MENU\PROGRAMS\REALVNC VNC SERVER
4 (SERVICE-MODE)\CONFIGURE VNC
SERVICE.LNK
\DEVICE\HARDDISKVOLUME1\DOCUMENTS
AND SETTINGS\ALL USERS\START
MENU\PROGRAMS\REALVNC VNC SERVER
4 (SERVICE-MODE)\REGISTER VNC
SERVICE.LNK

Remote Desktop Software!

From 07/12

- VNC Free Edition 4.1.3 installed on 7/12/2009

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 -**
Partition 1 (Microsoft







Remote Desktop Software!

From 07/12


- VNC Free Edition 4.1.3 installed on 7/12/2009

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
	1/1/1970 12:00:00 AM	

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

Remote Desktop Software!






From 07/12

- VNC Free Edition 4.1.3 ran on 7/12/2009

MATCHING RESULTS (26 of 400)

Row view ▼

Pat


	Pat USERASSIST — Operating System File Name : UEME_RUNPIDL:%csidl2%\RealVN CREATE EXPORT / REPORT OPEN SOURCE FILE WITH...	Last Run Date/Time 7/12/2009 6:16:43 PM
	Pat USERASSIST — Operating System File Name : UEME_RUNPIDL:%csidl2%\RealVN	Last Run Date/Time 7/12/2009 6:16:55 PM
	Pat USERASSIST — Operating System File Name : UEME_RUNPIDL:%csidl2%\RealVN	Last Run Date/Time 7/12/2009 6:16:55 PM
	Pat USERASSIST — Operating System File Name : UEME_RUNPIDL:%csidl2%\RealVN	Last Run Date/Time 7/12/2009 6:16:43 PM
	Pat USERASSIST — Operating System File Name : UEME_RUNPIDL:%csidl2%\RealVN	

DETAILS

ARTIFACT INFORMATION

User Name **Pat**
File Name **UEME_RUNPIDL:%csidl2%\RealVNC\VNC Server 4 (Service-Mode)\Configure VNC Service.Ink**

Application Run Count **1**
Last Run Date/Time **7/12/2009 6:16:43 PM**

Artifact type  UserAssist
Item ID **22983**

EVIDENCE INFORMATION

Source **pat-2009-12-11.E01 - Partition 1 (Microsoft NTFS, 12.11 GB) \Documents and Settings\Pat**

Remote Desktop Software!

From 11/12

- Persistence via inclusion as startup service

MATCHING RESULTS (2 of 632)

Row view ▼

WinVNC4.exe

SYSTEM SERVICES — Operating System

Service Type : 272 (not parsed)

[CREATE EXPORT / REPORT](#) [OPEN SOURCE FILE WITH...](#)

Registry Key Modified Date/...

11/12/2009 1:27:00 AM

WinVNC4.exe

SYSTEM SERVICES — Operating System

Service Type : 272 (not parsed)

Registry Key Modified Date/...

11/12/2009 1:27:00 AM

WinVNC4.exe

ARTIFACT INFORMATION

Service Name **WinVNC4.exe**

Service Type **272 (not parsed)**

Start Type **Automatic**

Service Location **C:\Program Files
RealVNC\VNC4
WinVNC4.exe**

Display Name **VNC Server Version 4**

User Account **LocalSystem**

Service Details **ImagePath: "C:\Program
Files\RealVNC\VNC4
WinVNC4.exe" -service**

Hosted **No**

Registry Key Modified Date/Time **11/12/2009 1:27:00
AM**

Error Control **Ignore**



04

Charlie

Case 1: Corporate Espionage Involving Charlie & Jamie

17 November 2009

Charlie is informed of Nitroba's interest in engaging M57.biz for their services and confidentiality concerns with project2400 through a forwarded email from Pat

03 December 2009

Jamie replied with her offer of "50 large" should the "goods" be good with "10" paid upfront

04 December 2009

Charlie responded to Jamie with the password "nitro" for the "steg program" that they discussed earlier

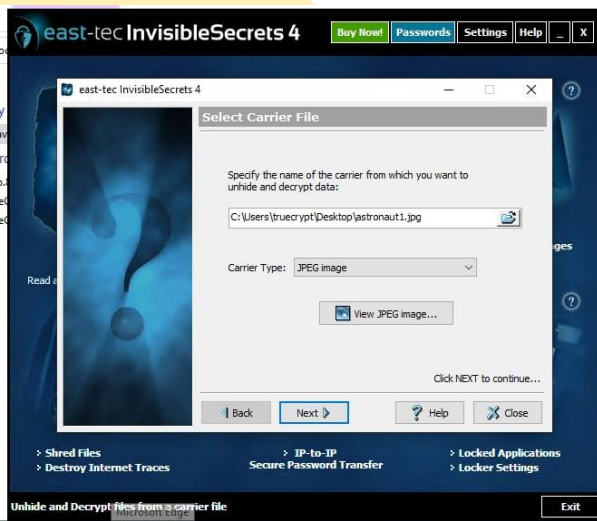
02 December 2009

Charlie initiated an email conversation with Jamie from project2400 for sale of something on interest to project2400

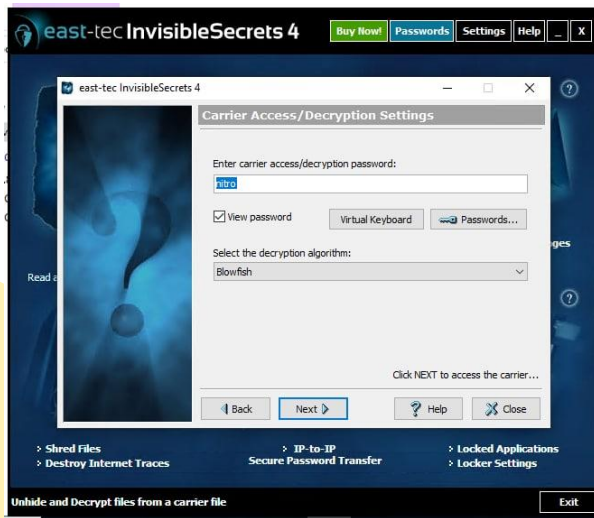
03 December 2009

Charlie sent Jamie a follow-up email with the "astronaut1.jpg" attachment with instructions to decrypt the file on receipt of another deposit

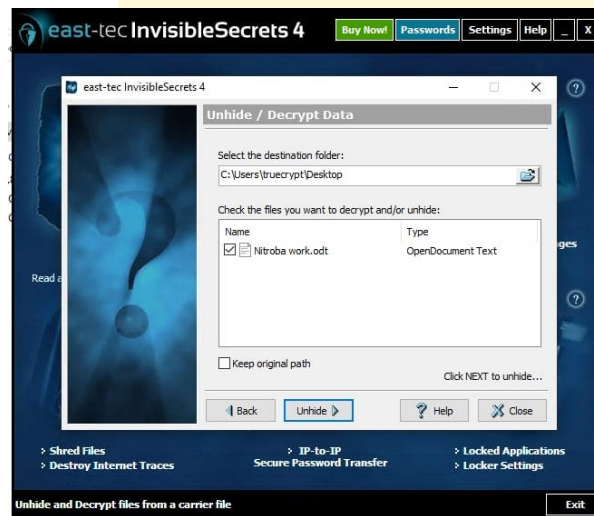
Invisible Secret Program



Loading astronaut1.jpg into InvisibleSecrets

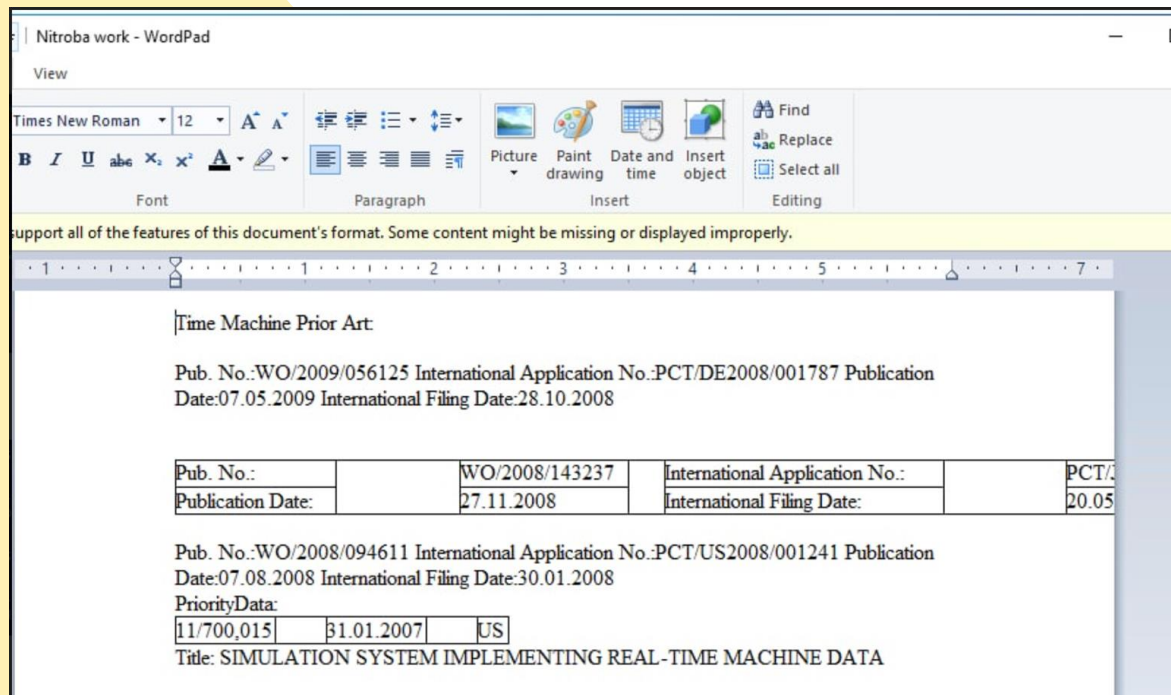


Entering decryption password as “nitro” and decrypting algorithm as “Blowfish”



Unhide the file Nitroba work.odt

Decrypted file



File “*Nitroba work.odt*” sent out by Charlie to Jamie

Case 2: Extortion Involving Charlie & Andy



04 December 2009

Charlie's emailed Andy from swexpert to demand 100k for not disclosing information (attachment: 01.zip) that will invalidate their current patent publicly



07 December 2009

Charlie attached 'microscope1.jpg' in the email to Andy which contains the password for the zip file (01.zip)



Decrypting 01.zip

Analyzing microscope1.jpg using HxD, password is uncovered to be
"immortal"

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	90	yøya..JFIF.....
00000010	00	90	00	00	FF	DB	00	43	00	01	01	01	01	01	01	01yÛ.C.....
00000020	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000030	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000040	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000050	01	01	01	01	01	01	01	01	01	01	FF	DB	00	43	01	01yÛ.C...
00000060	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000070	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000080	70	61	73	73	77	6F	72	64	3D	69	6D	6D	6F	72	74	61	password=immorta
00000090	6C	01	01	01	01	01	01	01	01	01	01	01	01	01	FF	C0	l.....yÀ
000000A0	00	11	08	02	65	01	73	03	01	22	00	02	11	01	03	11e.s..."....
000000B0	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00	.yÄ.....
000000C0	00	00	00	00	00	00	00	01	03	03	04	05	06	07	08	08	

Files used to extort Andy

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.³ 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



US06982168B1

(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, Brookville, MD (US); W. Martin Linshan, Rockville, MD (US); Robert K. Bright, Portland, OR (US); Cathy D. Voelke, 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/US97/01450

§ 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 15/05 (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, 53/7, 435/23, 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 12/1991 Schlegel et al. 435/172.1
5,436,152 A 7/1995 Soule et al. 435/240.2
5,443,954 A 8/1995 Reddel et al. 435/7.1
5,460,870 A 10/1995 Chopin 435/240.2
5,576,206 A 11/1996 Schlegel 435/240.2
5,716,830 A 2/1998 Webber et al. 435/8
5,824,488 A 10/1998 Webber et al. 435/7.23

FOREIGN PATENT DOCUMENTS

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

OTHER PUBLICATIONS

Chiarelli, E. Oncogene 16: 541-545, 1998.*
Kakman, Geens Chromosome 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 & Petersen, Eds., p. 764, 1973.*
Mustafa O. Int. 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 carcinoma 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(9): 653-663, 2000.*
Pardo 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 5 α -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-17)", The Journal of Urology, vol. 148, 1600-1604, Nov. 1992.
Rhin 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—Mub-Tam Davis

(74) Attorney, Agent, or Firm—Leydig, Voil & Mayer, Ltd.

(57) ABSTRACT

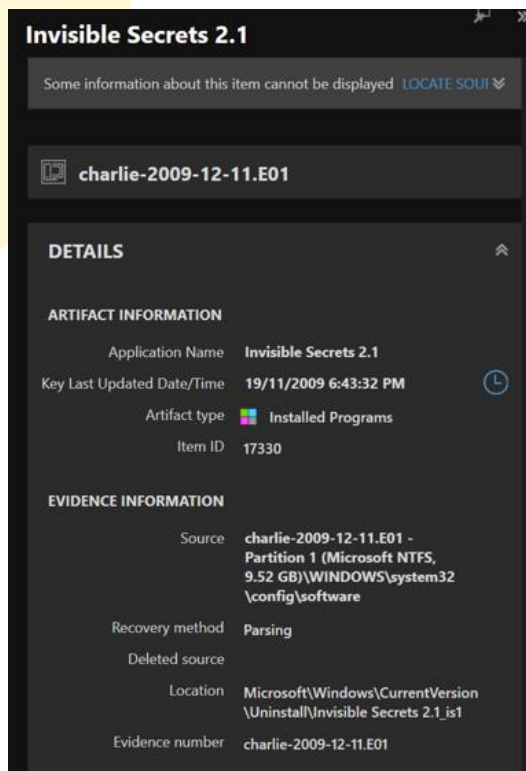
The present invention relates to immortalized, malignant, human, adult prostate epithelial cell lines or cell lines derived therefrom useful in the diagnosis and treatment of prostate cancer. More particularly, the present invention relates to cloned, immortalized, malignant, human, adult prostate epithelial 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

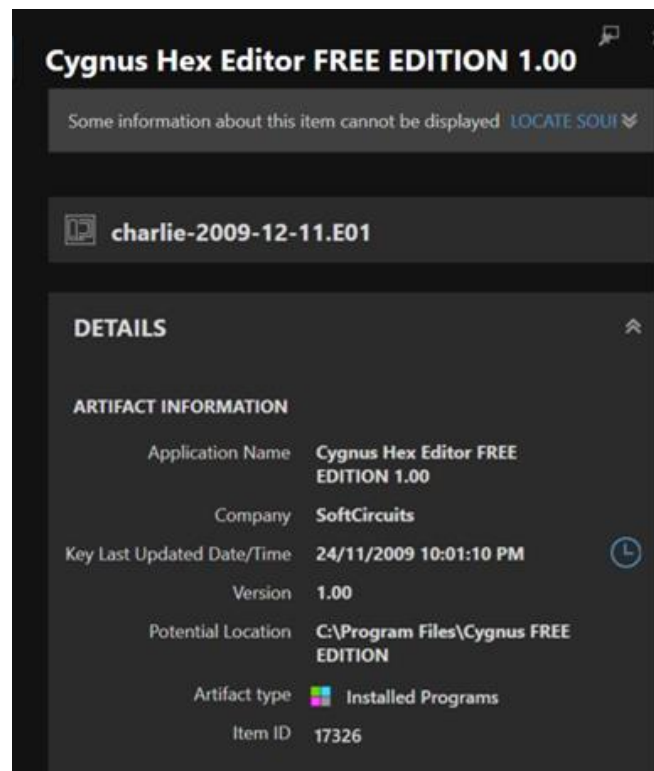
Patent 1 used for extortion

Patent 2 used for extortion

Supporting Evidence - Software Required

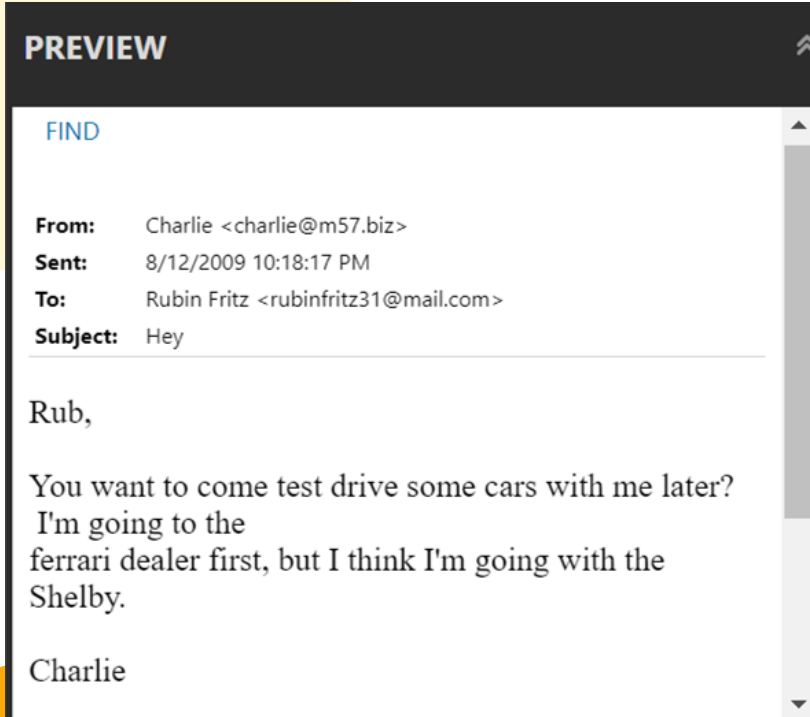


Installed on 19 Nov 2009

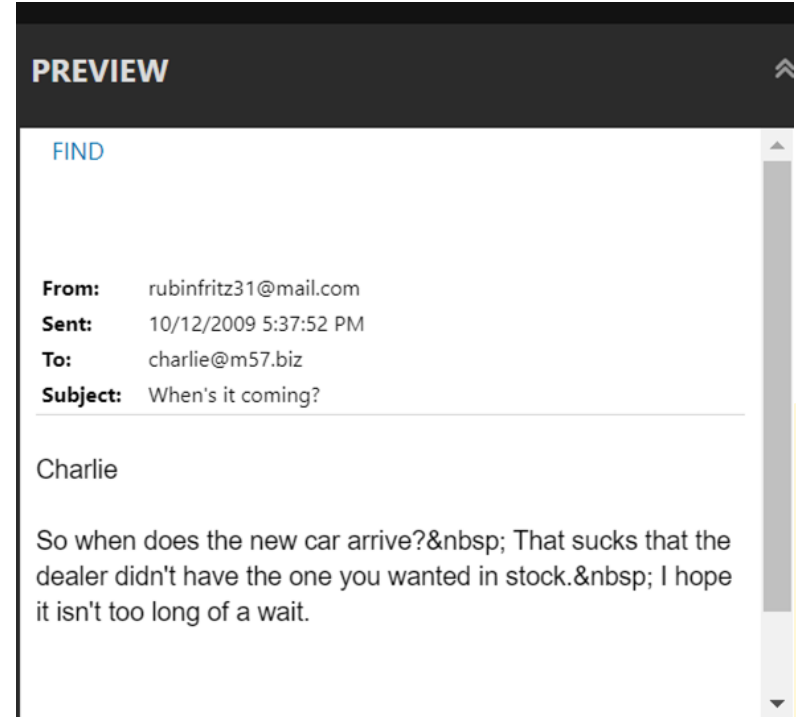


Installed on 24 Nov 2009

Supporting Evidence - Change in lifestyle



8 December 2009 - Ferrari test drive



10 December 2009 - Ferrari bought



05 Terry

Case 1: Selling office equipment on Craigslist

20th Nov 2009

Terry Johnson swapped out
Jo's computer

24th Nov 2009

Dell computer was listed
for sale

9th Dec 2009

Dell Monitor and HP
Printer was listed as well

20th Nov 2009

Terry assured both Jo and
Pat that the equipment will
be properly disposed of

30th Nov 2009

Aaron Greene negotiated
with Terry to meet that
night to deal Jo's computer



Computer belonging to Jo

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

Inventory List as claimed by Terry

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

Serial Number that Jo used to have matches
the N/A

Equipment being sold

```
> 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 <aarongreenel2@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
```

Dell Computer deal

```
-----=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
```

Monitor and Printer deal

Case 2: Forgery of receipt

18th Nov 2009

Terry requested for a larger Hard Drive.

19th Nov 2009

Terry has claimed \$300 from Pat

19th Nov 2009

Pat questioned the \$300 and Terry confirmed that the price is correct.

18th Nov 2009

Terry has a purchase receipt for the Hard Drive for \$100.

19th Nov 2009

Terry emailed Cod saying he made a quick \$200

Forgery of Receipt

Terry,

You can go ahead and 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,

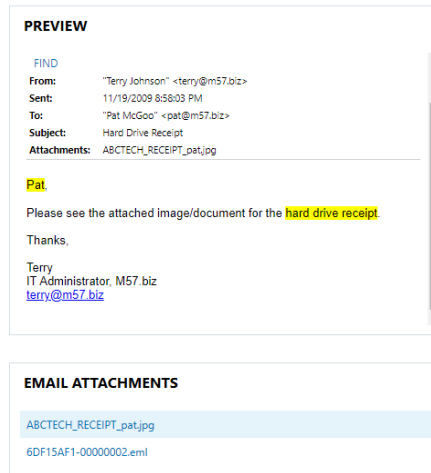
I need a larger hard drive since my Vista installation is taking up = too much space. Should I purchase the drive and the company can = re-imburse me later? Or are you going to purchase the drive?

Terry Requesting for a hard disk



Original Hard Disk Receipt

Forgery of Receipt



Terry claiming for the hard drive



Modified Hard Disk Receipt

Forgery of Receipt

```
-----=_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

Terry confirming that the hard drive costs
\$300



o
biz
1234

Other activities: Using office computer for recreational activities

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

Firefox / Internet Explorer Web History

Other activities: Downloading keylogging software

	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

Downloading keylogging software

Other activities: Downloading malicious files

NetworkMiner 2.7.3

File Tools Help

-- Select a network adapter in the list --

Hosts (1465) Files (11793) Images (3446) Messages (4) Credentials (3230) Sessions (5950) DNS (21189) Parameters (347764) Keywords Anomalies

42.zip ☐ Case sensitive ExactPhrase Any column Clear Apply

Frame nr.	Filename	Extension	Size	Source host
244997	42.zip.html	html	270 B	205.206.231.12 [www.securityfocus.com] (Linux)
245008	42.zip	zip	42 374 B	205.206.231.23 [downloads.securityfocus.com] (Linux)

Case Panel

Filename

net-2009-11-23-16_54.dmp

42-zip downloaded using Terry's IP address

Other activities: Downloading malicious files

42.zip.html - File Details

Name	42.zip.html
MD5	96cab03e832e15dd3a7841204954d4f6
SHA1	1af6340cdd3f2b0e2c28c104b39682670fdd5bde
SHA256	542db4169025f1135800247eeb855d5aab2212b1ed0350f3dcf49f7194d0130
Path	C:\Users\jovan\Downloads\Network Miner_2-7-3\Network Miner_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] [MS7-TERRY] [ubuntu.local] (Windows)

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

```
3C21444F43545950452048544D4C2050
55424C494320222D2F2F494554462F2F
4454442048544D4C20322E302F2F454E
223E0A3C48544D4C3E3C484541443E0A
3C5449544C453E333031204D6F766564
205065726D616E656E746C793C2F5449
544C453E0A3C2F484541443E3C424F44
593E0A3C48313E4D6F76656420506572
6D616E656E746C793C2F48313E0A5468
6520646F63756D656E7420686173206D
6F766564203C4120485245463D226874
74703A2F2F646F776E6C6F6164732E73
65637572697479666F6375732E636F6D
2F76756C6E65726162696C6974696573
2F6578706C6F6974732F34322E7A6970
223E686572653C2F413E2E3C503E0A3C
<!DOCTYPE HTML P
UBLIC "-//IETF//
DTD HTML 2.0//EN
">.<HTML><HEAD>
<TITLE>301 Moved
Permanently</TI
TLE>.</HEAD><BO
DY>.<H1>Moved Per
manently</H1>.Th
e document has m
oved <A HREF="ht
tp://downloads.s
ecurityfocus.com
/vulnerabilities
/exploits/42.zip
">here</A>.<P>.<
```

Contents of 42.zip

Conclusion



Jo indeed responsible for the files found on the purchased machine.



Charlie has been selling patents from his client's company (Nitroba) to their competitor (project2400) for large amounts of money to fund his own extravagant lifestyle while also extorting money from swexpert



- Terry Johnson, the IT administrator, has been selling office equipment for quick cash.
- Terry secretly spy on Pat computer using keylogger and remove desktop software.



We recommend the infrastructure team to come up with a list of approved software, and guidelines on how remote desktop assistance should be provided

THANKS

Do you have any questions?

