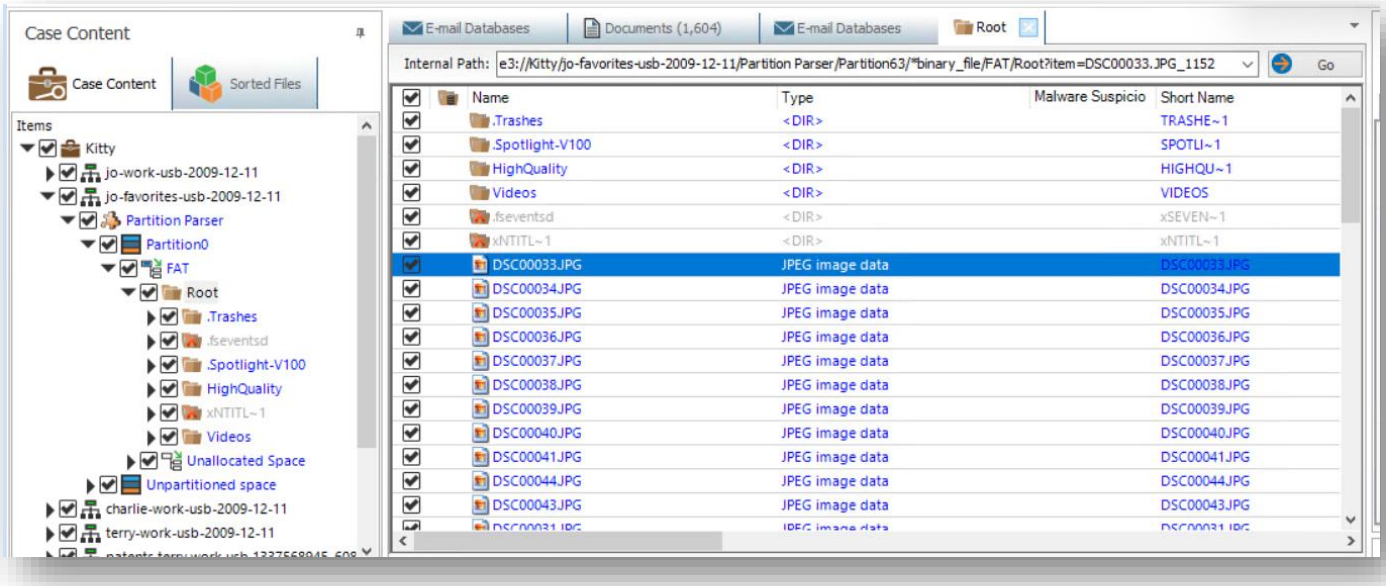
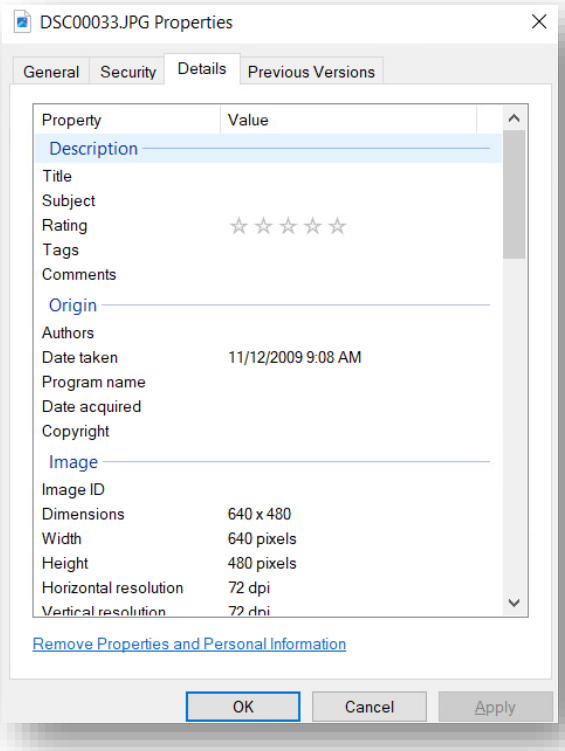
1. Is Jo the owner of the files you found from the USB drives? What evidence is there to confirm or reject this?

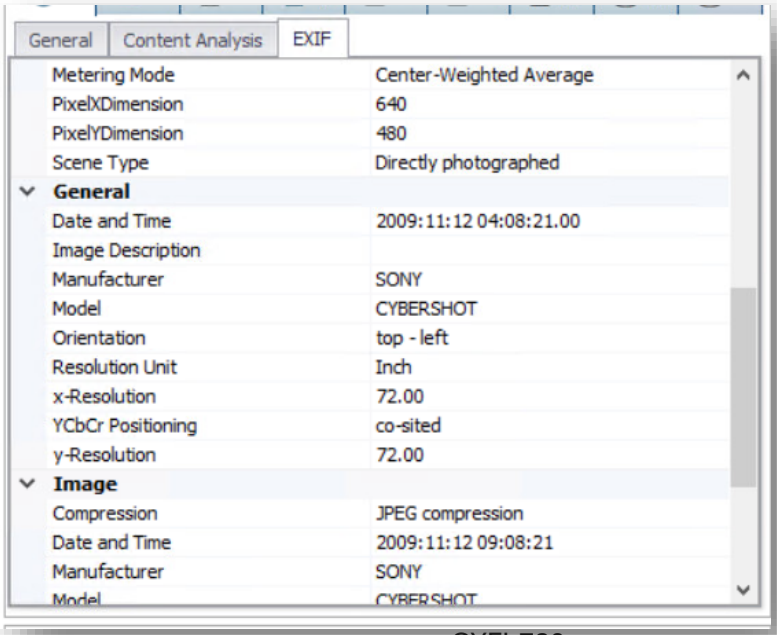
Answer: **Yes,** the owner of the files available on the USB drive is **Jo Smith**.

Approach-1: Evidence Used: Evidence Used: USB drive images of Jo (jo-work-usb-2009-12-11.E01, jo-favorites-usb-2009-12-11.E01), RAM images of Jo and the images of Jo's old and new PC

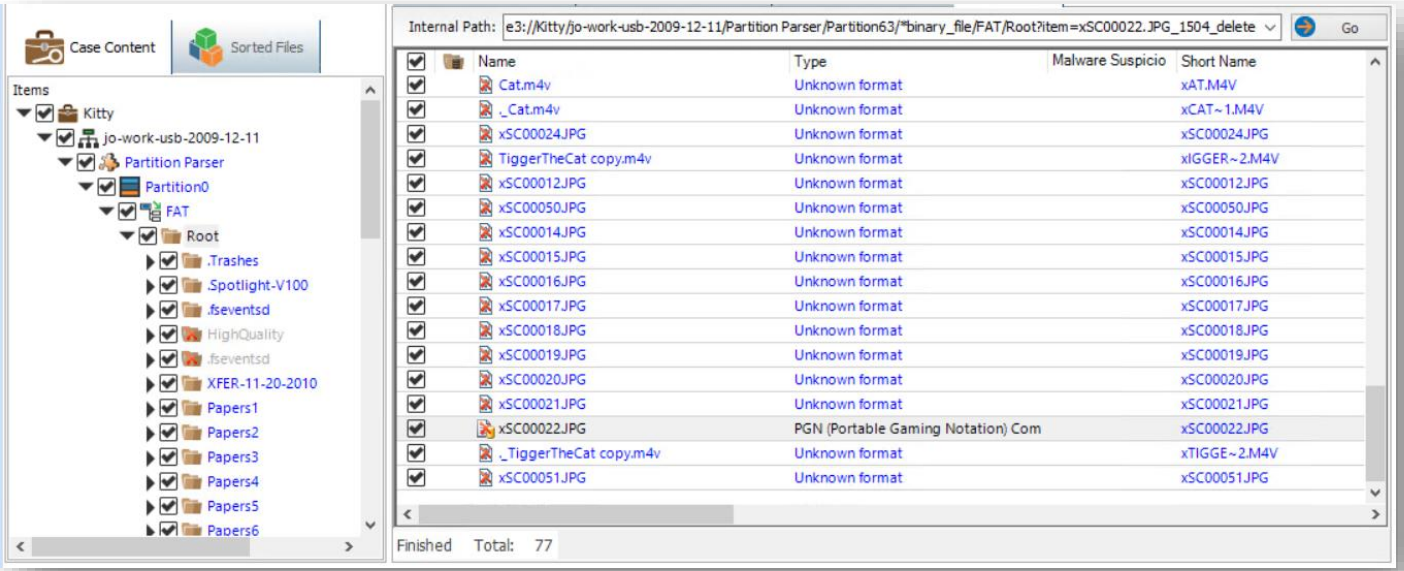


Kitty images were discovered on a USB image with the name 'jo-favorites-2009-12-11.E01,' indicating that it is possibly Jo's favourite USB. This drive, along with others, was seized from M57 Patents. The initial assumption was that the USB drive and its contents belonged to an employee named Jo. Several pieces of circumstantial evidence support this assumption. First, the USB drive's volume label clearly indicates Jo's ownership. Second, it's generally accepted that individuals are responsible for the contents of their personal USB drives. Third, similar "kitty" images, though marked as deleted, were also found on another USB drive associated with Jo, labelled "jo-work-usb-2009-12-11.E01."



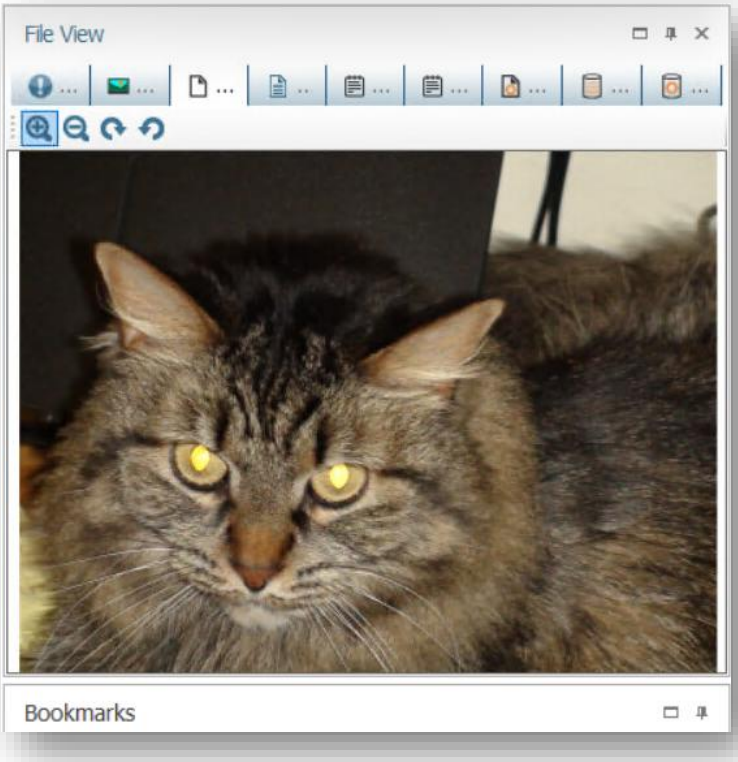


While examining the file metadata (mentioned in above images) of the "kitty" images, specifically the "Author" field, no conclusive evidence directly linked Jo as the owner. While analysing the images' EXIF data, it reveals SONY CYBERSHOT camera was used and photos were clicked on 5th November 2009 between 5 PM to 6:30PM. However, the combined circumstances—the images being present on Jo's personal USB drive, the drive's label clearly identifying ***Jo*** as the owner, the presence of similar deleted images on Jo's work USB, and the general expectation of personal responsibility for USB drive contents—strongly suggest that Jo is the likely owner of the images



Further analysis of Jo's old computer also revealed the presence of "kitty" images, strengthening the case for Jo's ownership. These images were exclusively found on Jo's devices and were not present on any other employee's computers or USB drives.

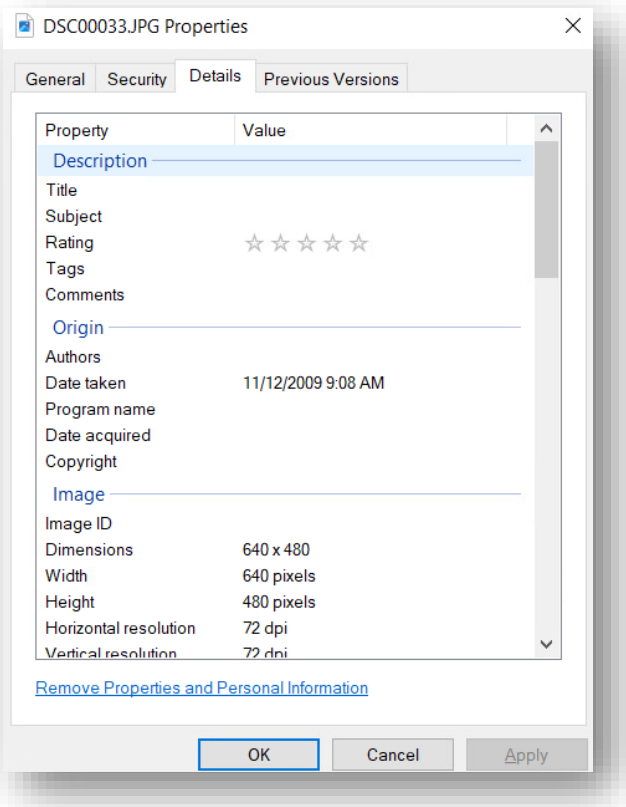
In conclusion, while direct evidence from file metadata might be lacking, the combined circumstantial evidence points towards Jo being the owner of the "kitty" images. The images were found on his personal USB drive, which was clearly labelled with his name, and similar deleted images were present on his work USB. Additionally, the images were also found on his old computer and were exclusive to his devices. This, coupled with the general principle of personal responsibility for USB drive contents, strongly suggests Jo's ownership of the illicit images.

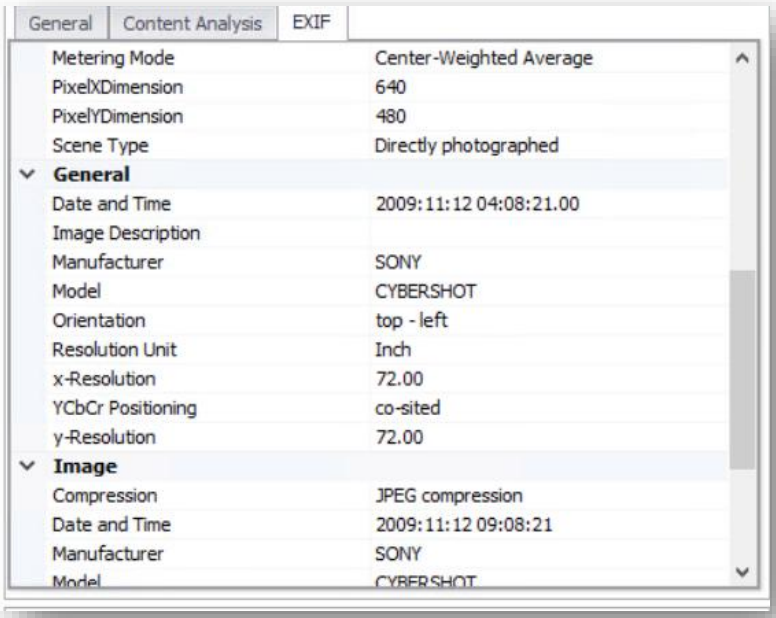


Approach-2

I. Image Creation:

- The EXIF data extracted from the kitty images reveals that they were taken with a SONY CYBERSHOT camera on November 5th, 2009, between 5:00 PM and 6:30 PM. This establishes the initial creation of the images.
- **Path**: e3://Kitty/jo-favorites-usb-2009-12-11/Partition Parser/Partition63/*binary_file/FAT/Root/HighQuality_384?item=DSC00003.JPG_64

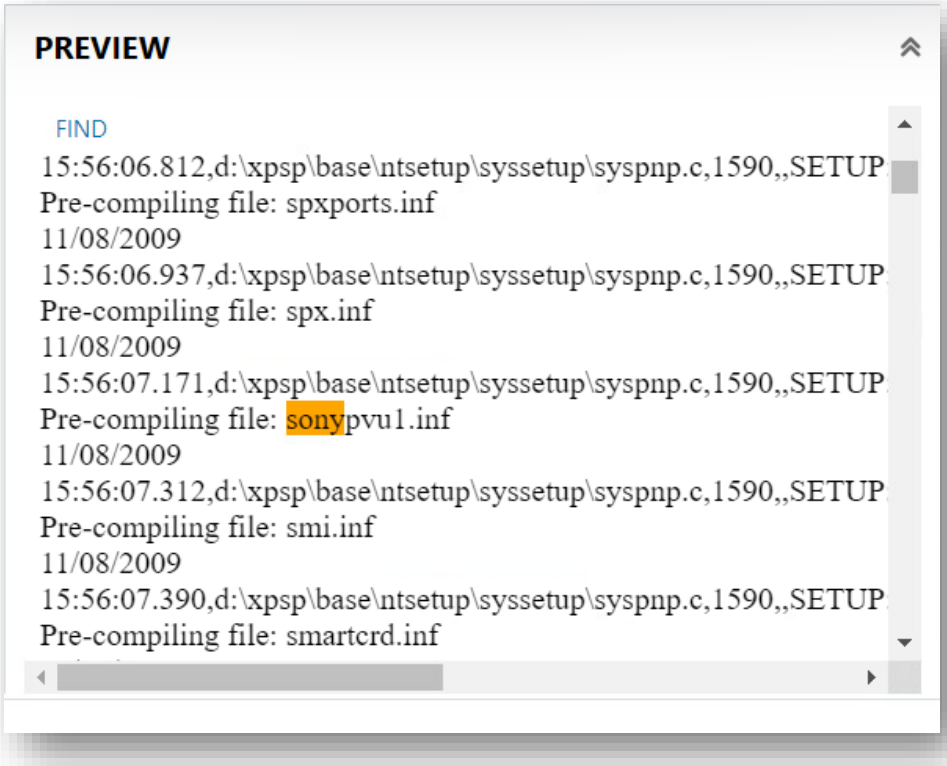




II. Camera Connection and Image Transfer:

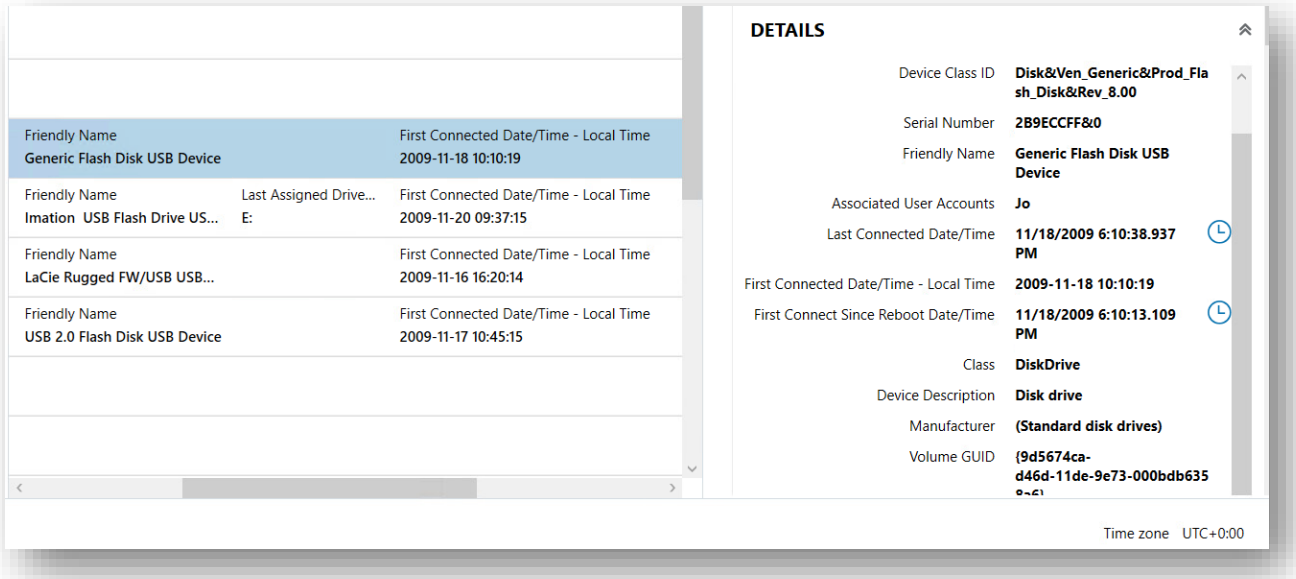
- The Windows setup log file **(sonypvu1.inf)** from Jo's old computer (jo-2009-11-20-01dComputer.E01) shows that the SONY CYBERSHOT camera was connected to the computer on November 8th, 2009, at 3:56:07 PM. This suggests that the images were likely transferred from the camera to the computer at this time. This evidence was located by making a keyword search of word "SONY" as it is the camera make found in the image EXIF data.
- Further analysis of the image metadata indicates that the images were created on the computer on November 11th, 2009, supporting the theory that they were transferred from the camera around this time.
- **Path:** jo-2009-11-20-oldComputer.E01 - Partition 1 (Microsoft NTFS, 12.11 GB)\WINDOWS\setuplog.txt

This log entry, extracted from the Windows setup log file (`sonypvu1.inf`) of Jo's PC, provides evidence of a device installation during the Windows setup process. The timestamp '15:56:07.171' indicates that on November 8th, 2009, at approximately 3:56:07 PM, a Sony device, possibly a camera, was connected to the computer for the first time. This suggests that the user was installing or configuring the necessary drivers for the Sony device, likely in preparation for its use. The pre-compilation of the `.inf` file (`sonypvu1.inf`) further supports this conclusion, as it indicates the system was optimizing the driver installation for future use. This event is relevant to the investigation as it establishes a timeline for the connection of the Sony device and suggests the user's intent to utilize it, potentially for transferring or accessing data.

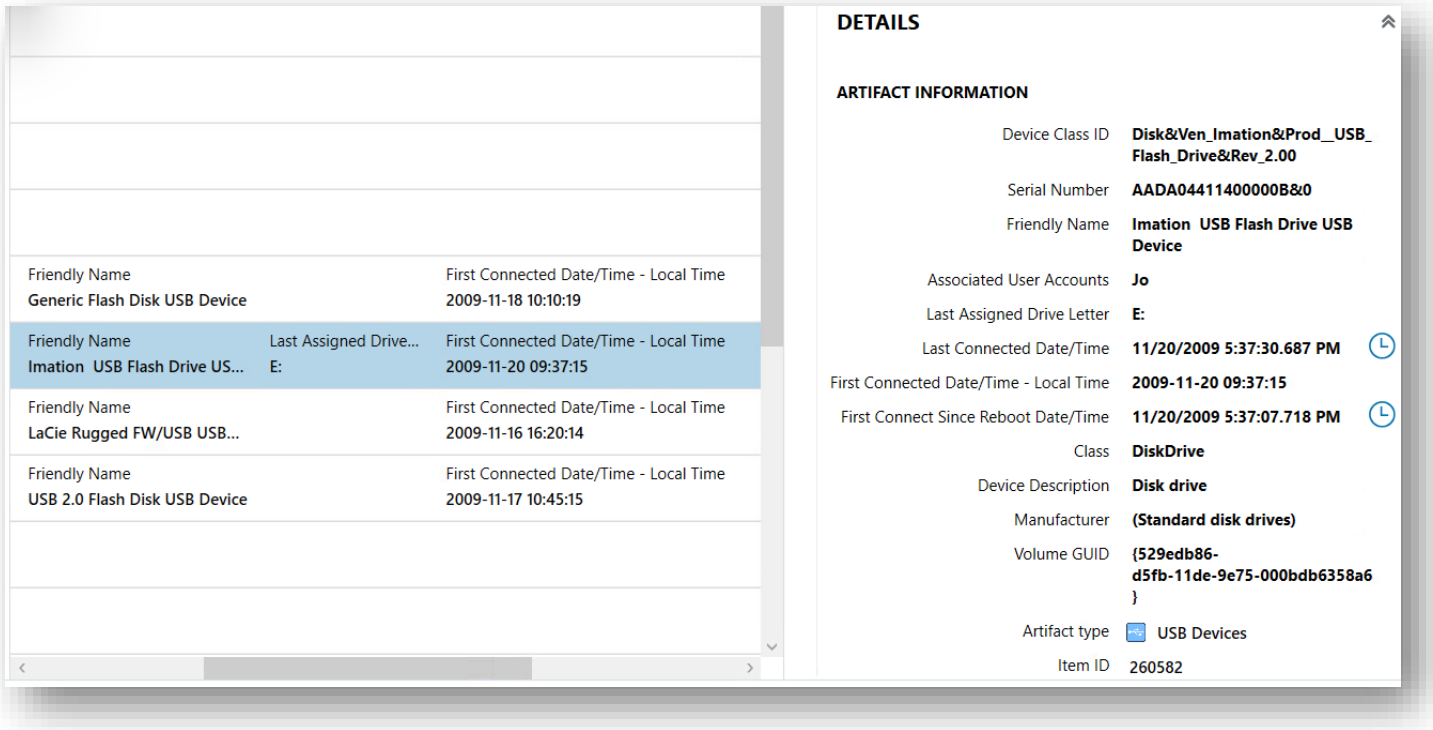


III. Transfer to USB Drive:

- Based on the image creation dates and the first and last connection timestamps of the USB drive, it appears that the images were transferred from Jo's old PC to his favorite USB drive ("Generic Flash Disk USB Device," serial number: 2B9ECCFF&0) on November 18th, 2009, between 10:10:19 AM and 6:10:38 PM UTC.

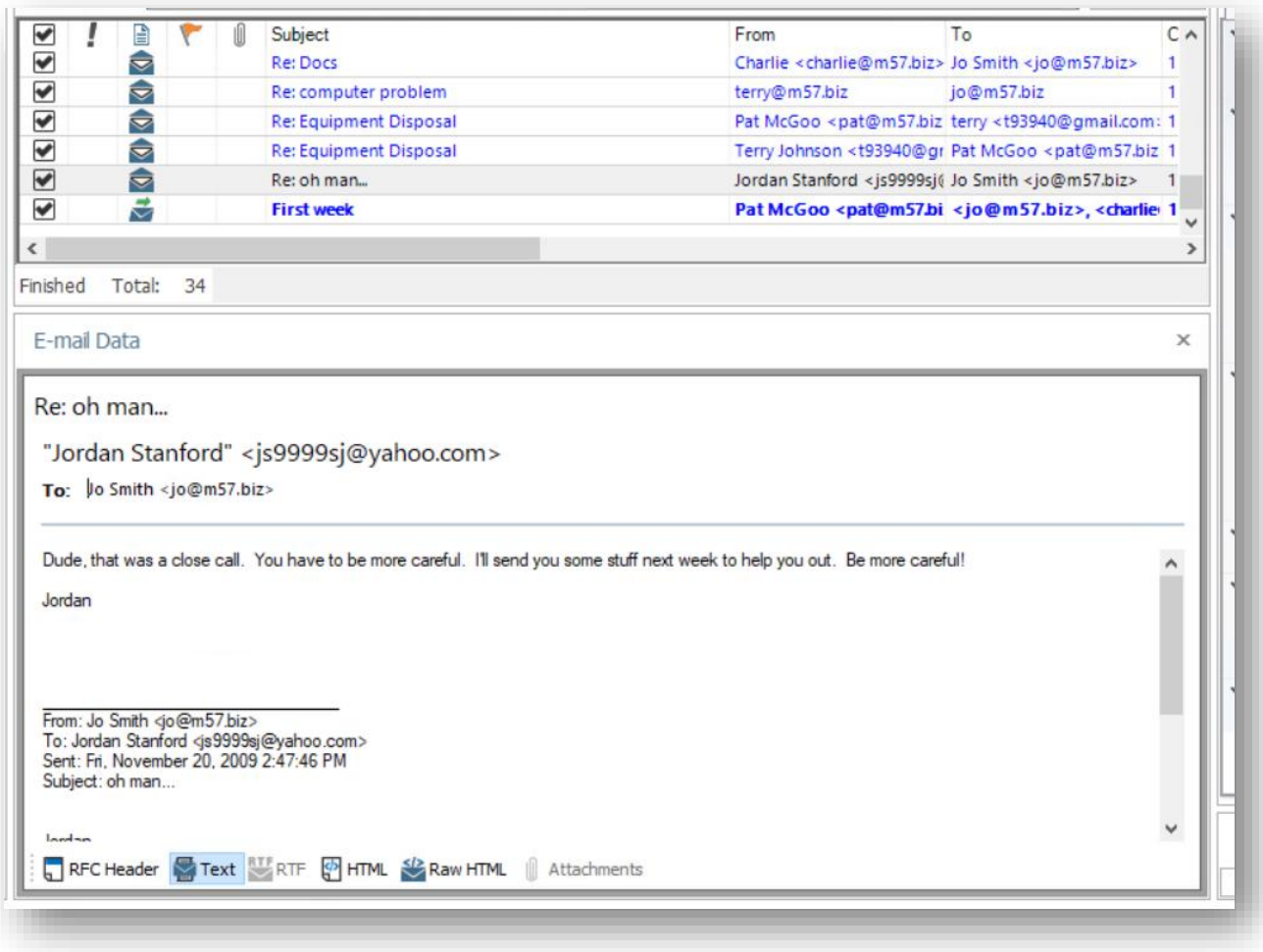


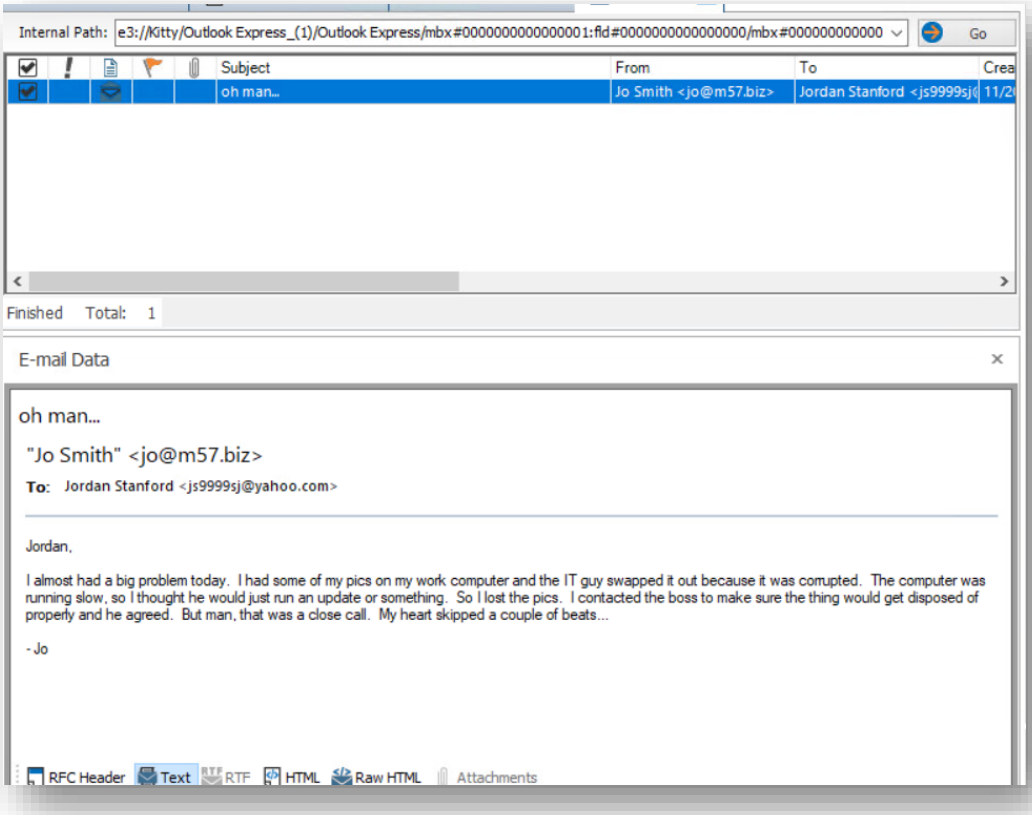
- It's likely that Jo mistakenly transferred the images to his work USB drive ("Imation USB Flash Drive USB Device," serial number: AADA04411400000B&0). This is supported by the image access dates and the connection timestamps of the work USB drive to the old PC.
- Subsequently, Jo deleted the images from the work USB drive around 9:35 PM UTC on November 20th, 2009, possibly to remove them from the work environment.



IV. Email Exchange with Jordan:

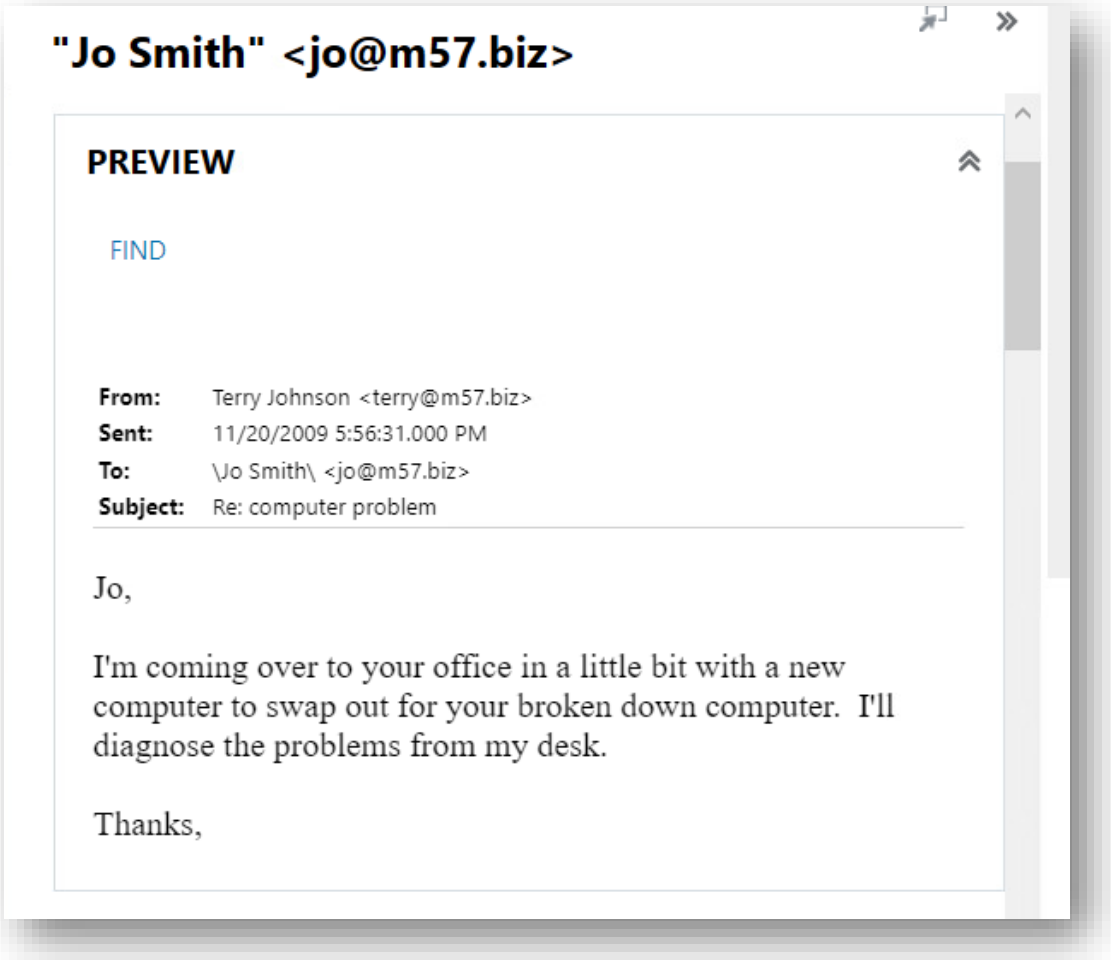
- On November 20th, 2009, at 5:47:46 PM, Jo sent an email to his friend Jordan (js9999sj@yahoo.com) using his work email account (jo@m57.biz). In this email, Jo expresses concern about almost having a "big problem" due to having personal pictures on his work computer, which was replaced by the IT person, Terry. This email exchange further strengthens the connection between Jo and the "kitty" images.
- To get this evidence, I found the email database folder (Outlook) from the Jo's new computer (jo-2009-11-20-oldComputer.E01) and extracted the database to analyse it using the Paraben's email database analyser.
- **Path**: e3://Kitty/Outlook Express_(1)/Outlook Express/mbx#0000000000000001:fld#0000000000000000/mbx#0000000000000001:fld#0000000000000002?item=fld#0000000000000001:msg#0000000000000020


Subject From To C
Re: Docs Charlie <charlie@m57.biz> Jo Smith <jo@m57.biz> 1
Re: computer problem terry@m57.biz jo@m57.biz 1
Re: Equipment Disposal Pat McGoo <pat@m57.biz terry <t93940@gmail.com: 1
Re: Equipment Disposal Terry Johnson <t93940@gr Pat McGoo <pat@m57.biz 1
Re: oh man... Jordan Stanford <js9999sj(Jo Smith <jo@m57.biz> 1
First week Pat McGoo <pat@m57.bi <jo@m57.biz>, <charlie 1
Finished Total: 34
E-mail Data
Re: oh man...
"Jordan Stanford" <js9999sj@yahoo.com>
To: Jo Smith <jo@m57.biz>
Dude, that was a close call. You have to be more careful. I'll send you some stuff next week to help you out. Be more careful!
Jordan
From: Jo Smith <jo@m57.biz>
To: Jordan Stanford <js9999sj@yahoo.com>
Sent: Fri, November 20, 2009 2:47:46 PM
Subject: oh man...
RFC Header Text RTF HTML Raw HTML Attachments


Internal Path: e3://Kitty/Outlook Express_(1)/Outlook Express/mbx#0000000000000001:fld#0000000000000000/mbx#000000000000
Go
Subject From To Crea
oh man... Jo Smith <jo@m57.biz> Jordan Stanford <js9999sj(11/2
Finished Total: 1
E-mail Data
oh man...
"Jo Smith" <jo@m57.biz>
To: Jordan Stanford <js9999sj@yahoo.com>
Jordan,
I almost had a big problem today. I had some of my pics on my work computer and the IT guy swapped it out because it was corrupted. The computer was running slow, so I thought he would just run an update or something. So I lost the pics. I contacted the boss to make sure the thing would get disposed of properly and he agreed. But man, that was a close call. My heart skipped a couple of beats...
- Jo
RFC Header Text RTF HTML Raw HTML Attachments

V. **New Computer and Continued Activity:**

- Jo requested a new computer from Terry, the IT person, due to issues with his old computer. The email exchange with Jordan originated from this new computer. This suggests that Jo continued his activities related to the "kitty" images even after his old computer was replaced.
- **Path**: jo-2009-11-20-newComputer.E01 - Partition 1 (Microsoft NTFS, 14.32 GB)\Documents and Settings\Jo\Local Settings\Application Data\Identities\{BC112AB3-3F86-4D46-A9E4-73A00E67A426}\Microsoft\Outlook Express\Inbox.dbx


"Jo Smith" <jo@m57.biz>

PREVIEW

FIND

From: Terry Johnson <terry@m57.biz>
Sent: 11/20/2009 5:56:31.000 PM
To: \Jo Smith\ <jo@m57.biz>
Subject: Re: computer problem

Jo,

I'm coming over to your office in a little bit with a new computer to swap out for your broken down computer. I'll diagnose the problems from my desk.

Thanks,

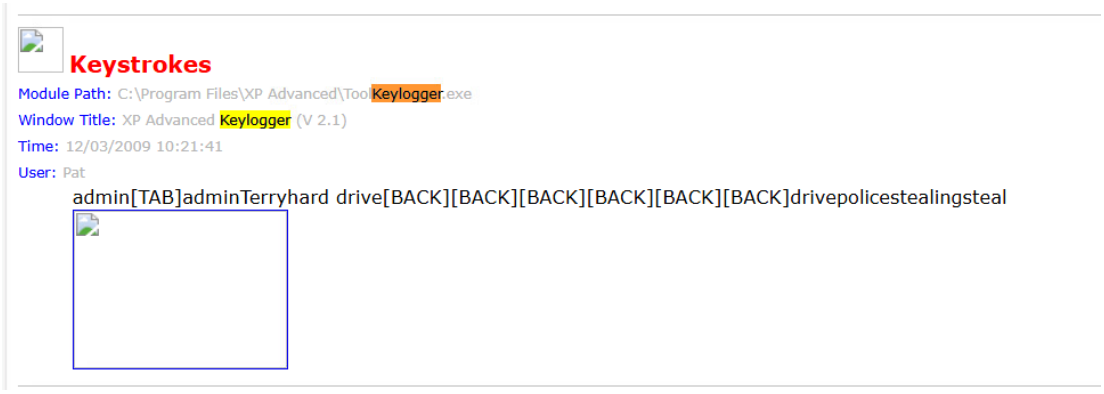
The combined evidence from image metadata, system logs, USB drive connection timestamps, and email correspondence strongly suggests that Jo is the owner of the "kitty" images and videos. The timeline reconstructed from this evidence demonstrates Jo's consistent interaction with these files, from their initial creation to their transfer and subsequent deletion from various devices. This analysis provides a compelling narrative for inclusion in a forensic report, linking Jo to the illicit images and supporting potential legal action.

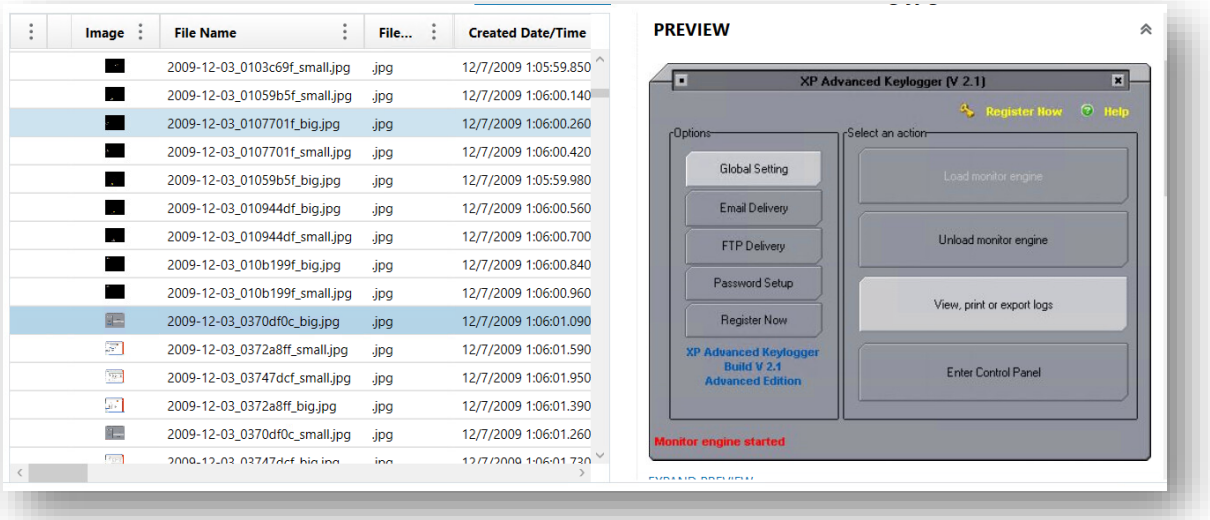
2. Are there any other suspicious activities occurring within M57?

Answer: **Yes**, there are several suspicious activities occurring within M57, as evidenced by the analyses of the company's systems and employee activities.

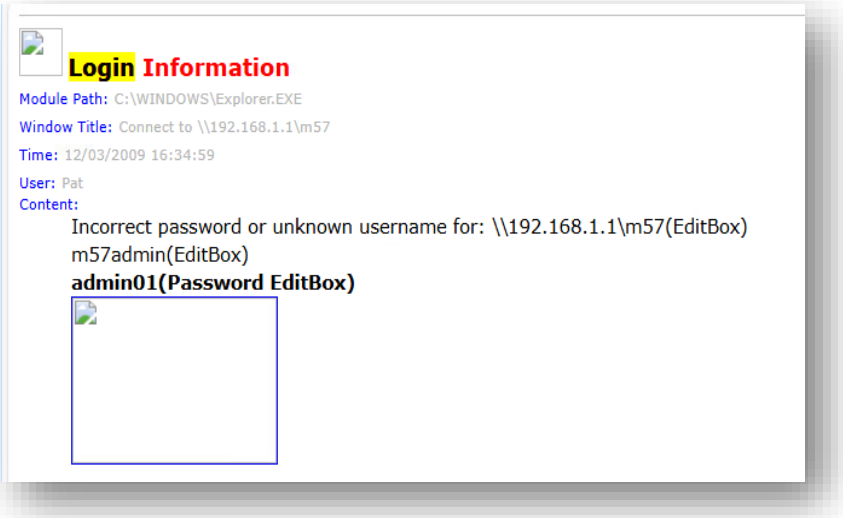
- **Keylogging Activity**: Analysis of Terry's RAM and matching it with a "LOG"folder, reveals evidence of a keylogger installed on his machine. By comparing the executables in memory with those from the baseline disk image, a keylogger ("XP Advanced Keylogger") was identified as present on December 3rd. This suggests someone was actively monitoring Pat's activities. Further analysis indicates the keylogger was removed on December 7th. However, the presence of "RealVNC VNC4" in the RAM snapshots from December 7th onwards raises concerns about potential remote access and surveillance. If Pat did not install RealVNC, it could have been used by an unauthorized individual to monitor his actions in real-time. This finding warrants further investigation to determine who installed the keylogger and RealVNC and their intentions behind these actions.

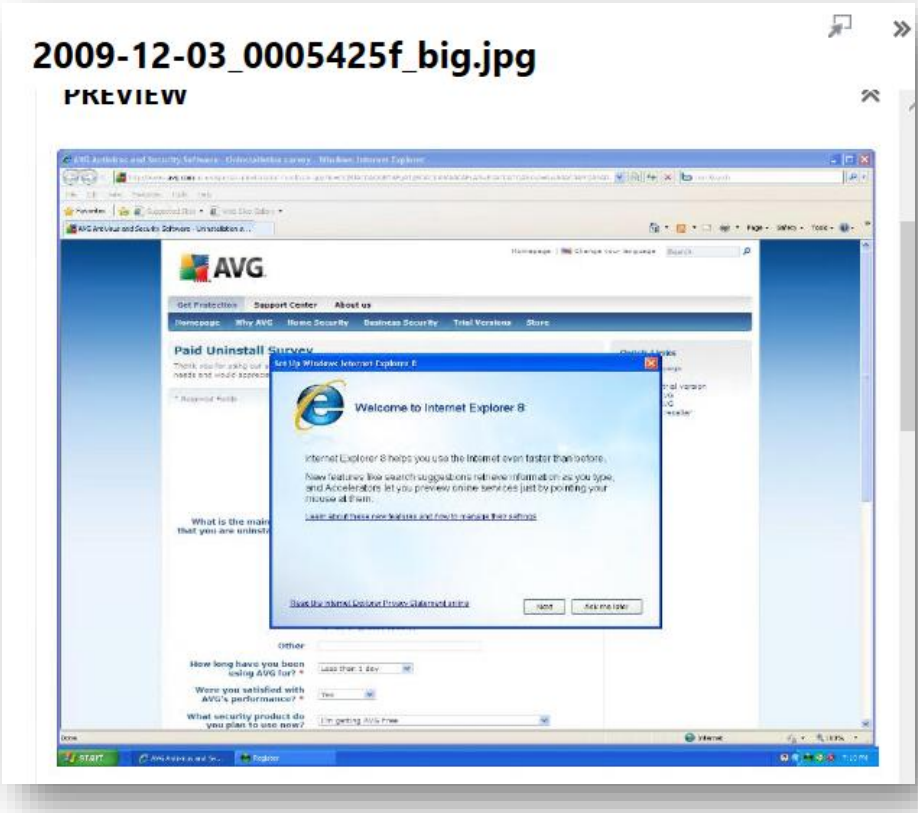
  - **Path**: patents terry work usb 1337568945_608350.E01 - Partition 1 (Microsoft FAT32, 1.95 GB) TERRYS WORK\Log\2009-12-03.htm
  - **Evidence:**





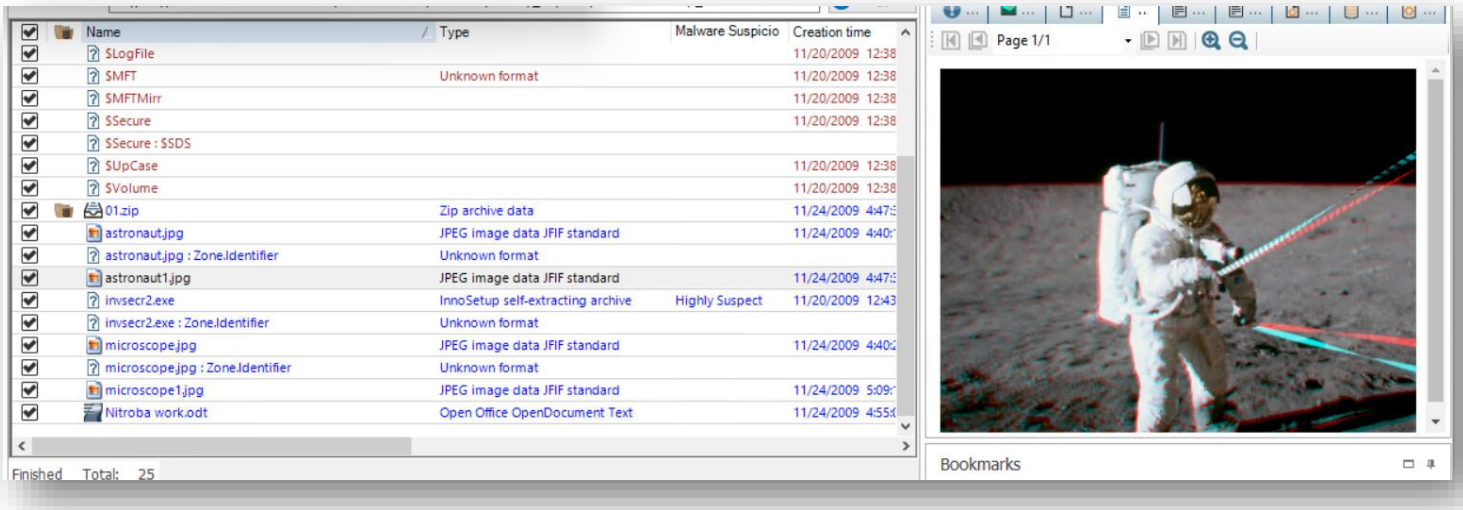
Pat's Unauthorized Access to User Accounts and Failed Login Attempts: Pat's activity logs from the keylogging activity show that he tried to access several user accounts without authorization, including those for Outlook Express, Task Manager, Control Panel, and User Accounts. He performed actions such as entering login credentials, typing messages, and opening applications, which raises serious concerns about data security and employee privacy. Additionally, Pat tried multiple times to connect to a network resource ("\192.168.1.1\m57"), but failed, suggesting potential unauthorized access attempts. These actions warrant further investigation.

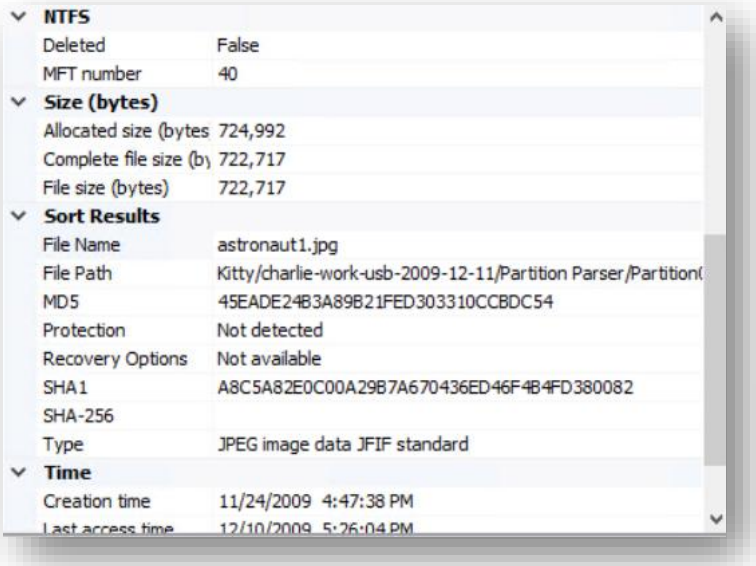




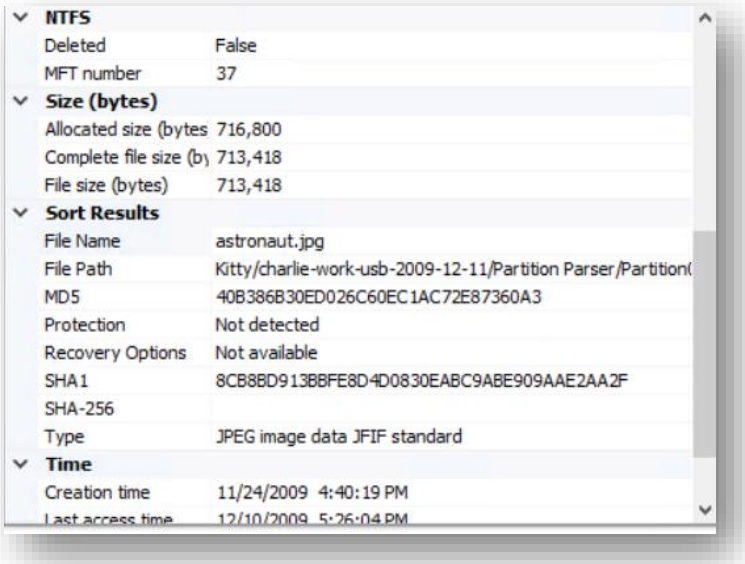
Charlie's Activities:

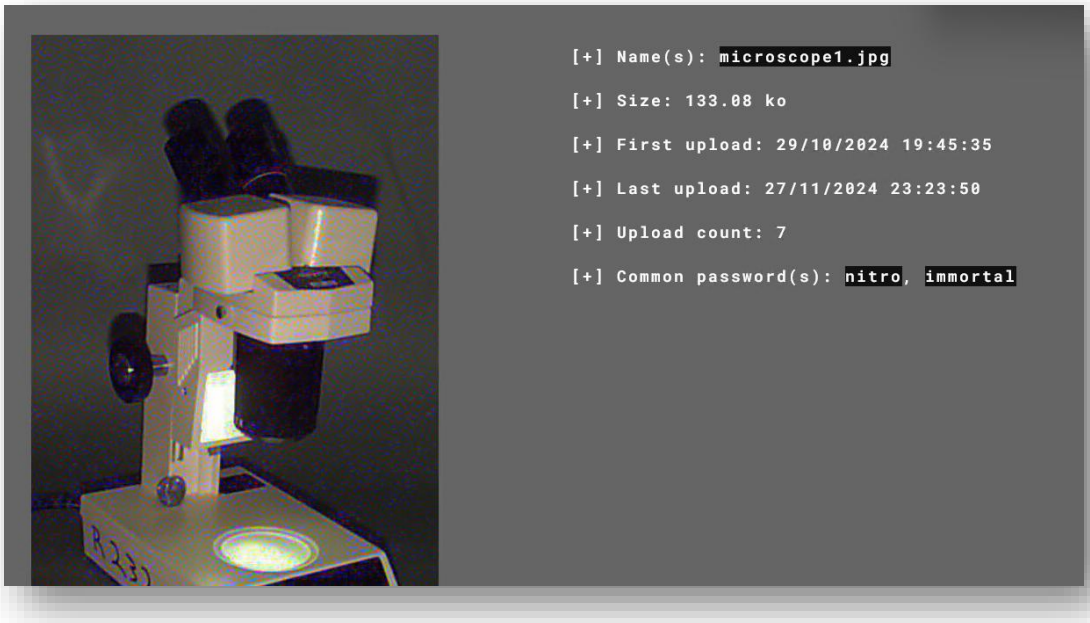
- **Steganography**: Charlie is suspected of hiding password for the zip file that was sent as an attachment in email, as suggested by the discovery of "**microscope1.jpg**" and "**astronaut1.jpg**" image pairs that appear identical but have different hashes, indicating embedded data.
    - **Path**: e3://Kitty/charlie-work-usb-2009-12-11/Partition Parser/Partition1/*binary_file/NTFS/Root?item=01.zip_39
    - **Evidence**:



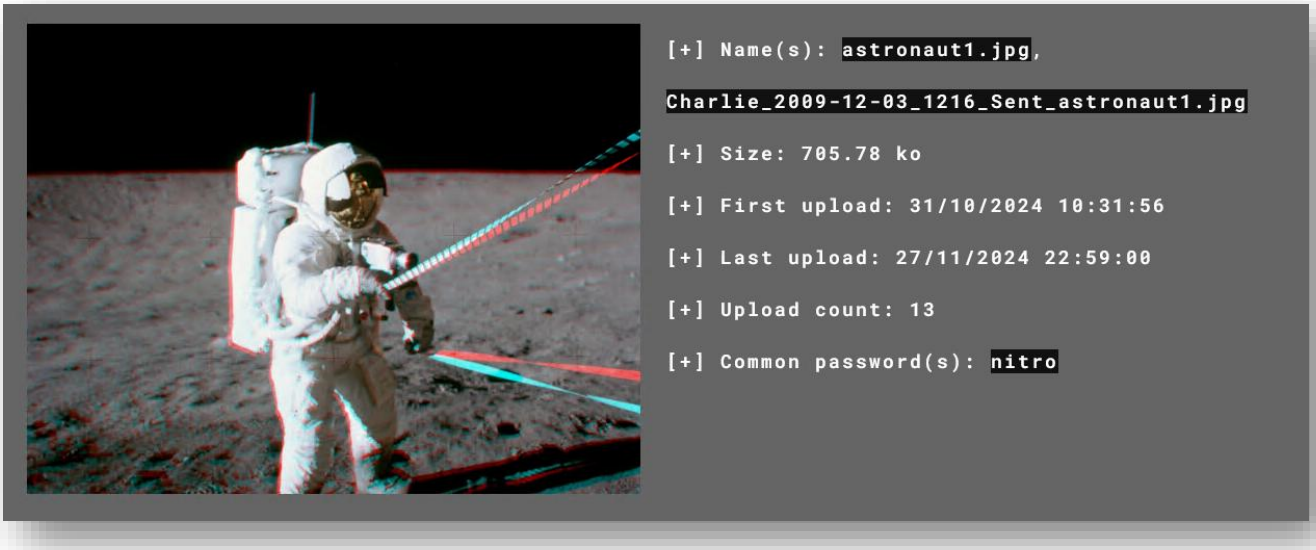


Difference in file size and MD5 hash values between the **astronaut.jpg** and **astronaut1.jpg** suggest potential evidence of steganography.





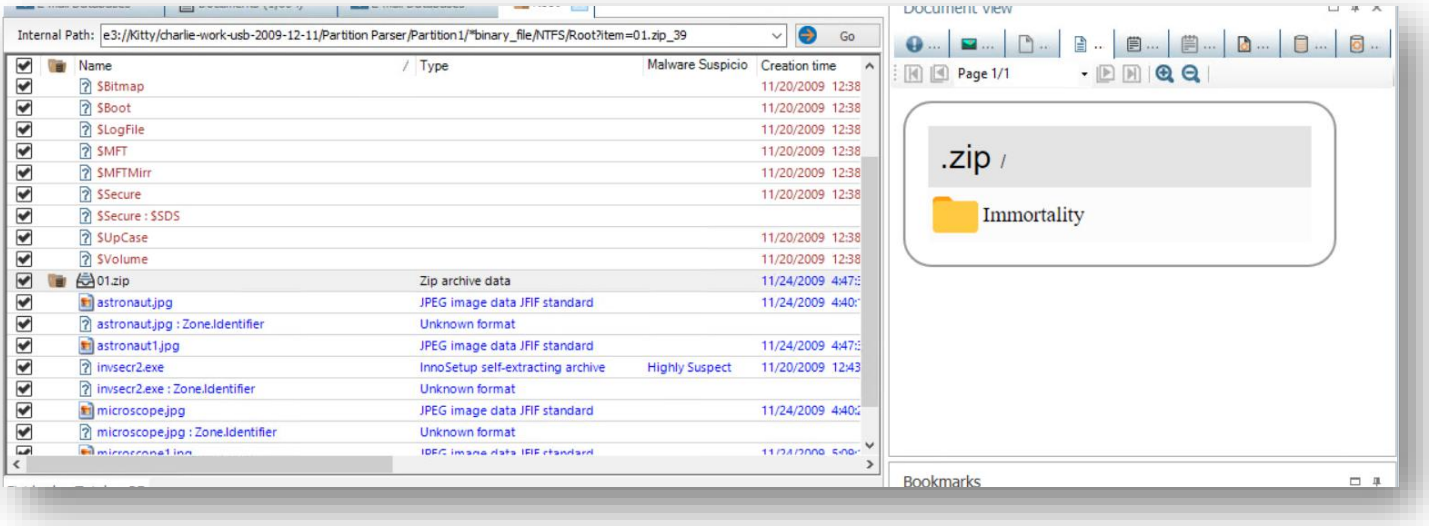
Charlie sent an email containing a password-protected ZIP file and hinted that the password was hidden within separate image attachment (microscope1.jpg and astronaut1.jpg).

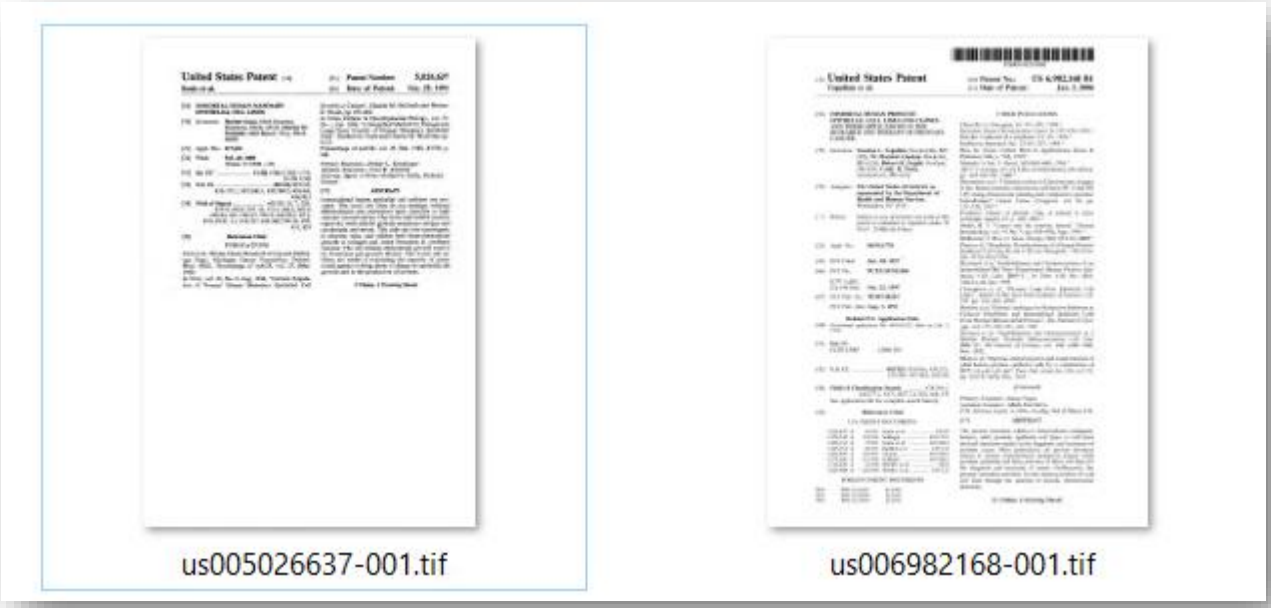


Charlie is potentially involved in an extortion scheme, as evidenced by the password-protected archive "01.zip" found on his USB drive and the presence of the associated files in his RAM images and email correspondence. The password of this file “immortal” as extracted from this

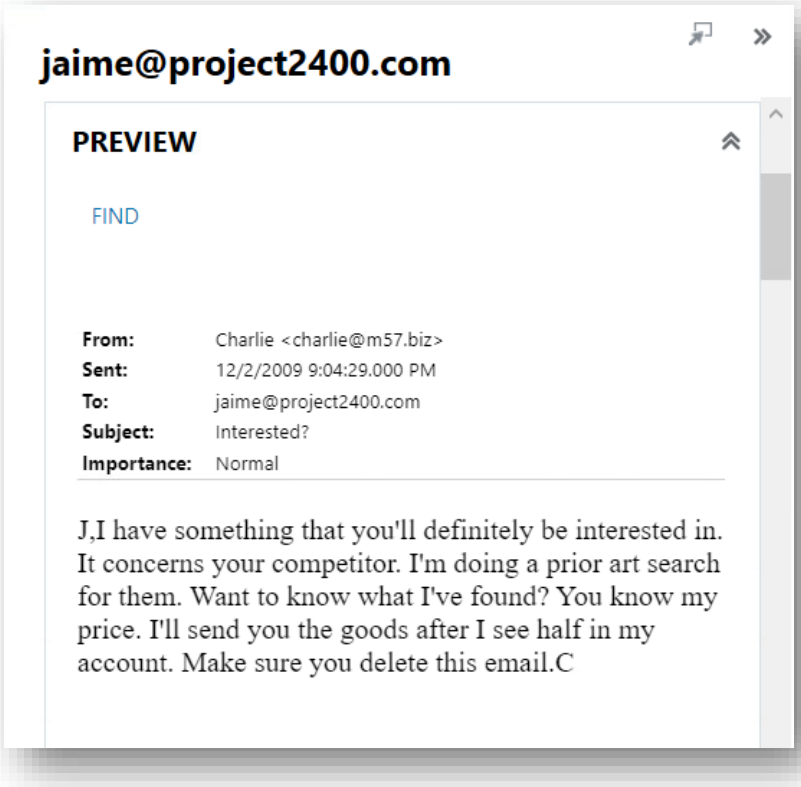
- **Path:** e3://Kitty/charlie-work-usb-2009-12-11/Partition Parser/Partition1/*binary_file/NTFS/Root?item=01.zip_39
- **Evidence**:

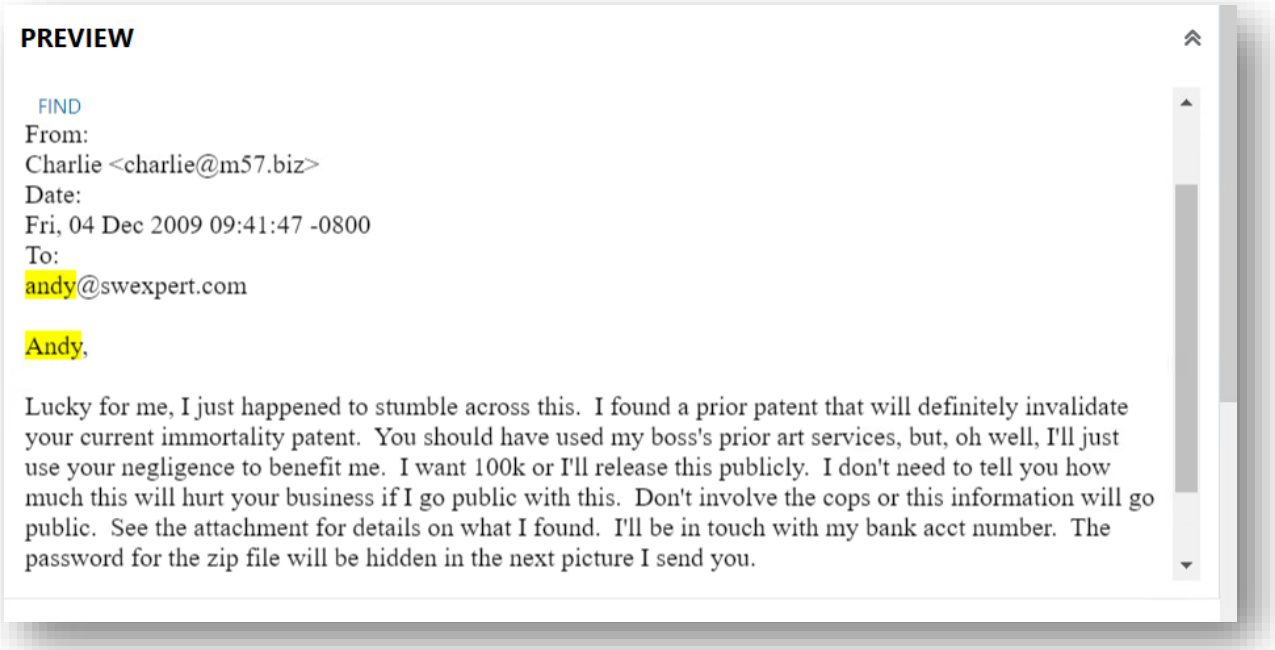
The ZIP file was password-protected and required the password "immortal" to be extracted. Inside, a folder named "immortality" contained two password-protected TIF images. After entering the same password, the images were accessed, revealing content related to a U.S. Patent, as described in an email from Charlie to Andy.





- **Data Exfiltration:** Charlie's emails to people outside the company raises concerns and make him a suspect of data exfiltration. He talked about everyday things with Rubin and Alix, like movies, dinner, cars, and vacations. But his emails with Jaime and Andy are much more worrisome as he demands money in order his company secrets and data to their competitor.
    - **Path:** charlie-work-usb-2009-12-11.E01 - Partition 1 (Microsoft NTFS, 0.99 GB) charliework\Email\Charlie_Email.zip\Charlie_2009-12-02_1305_Received_Interested-.eml
    - **Evidence:**



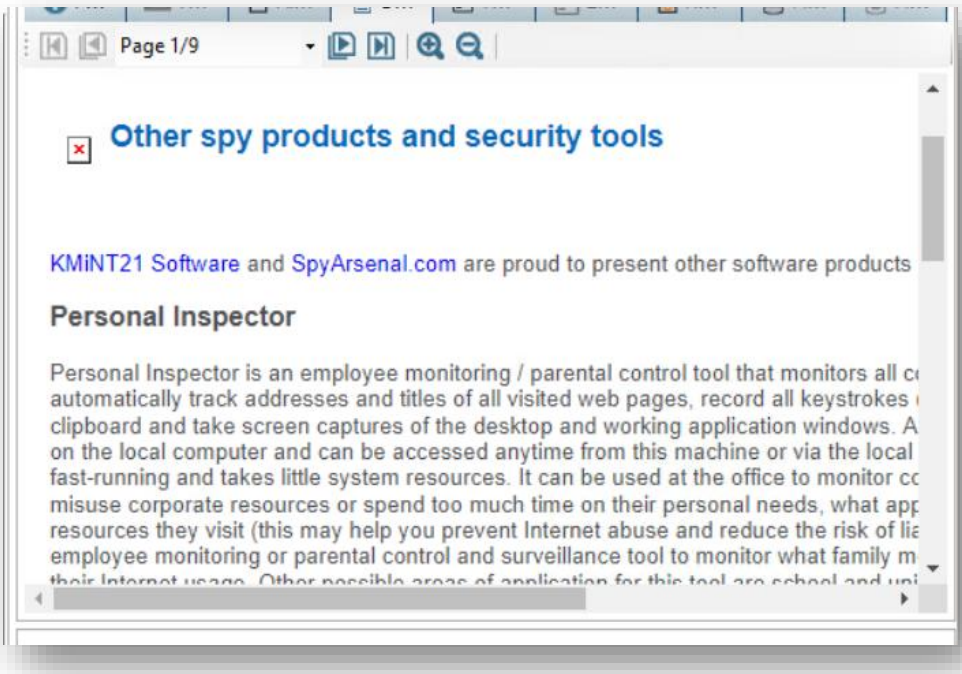


Terry's Activities:

- **Personal Use of Work Computer**: Terry is also suspected of using his work computer for personal activities, including online gambling and accessing dating websites, as evidenced by his web browsing history and email correspondence.
  - **Path**: terry-2009-12-04.E01 - Partition 1 (Microsoft NTFS, 38.28 GB) (Unallocated Clusters)
  - **Evidence**:

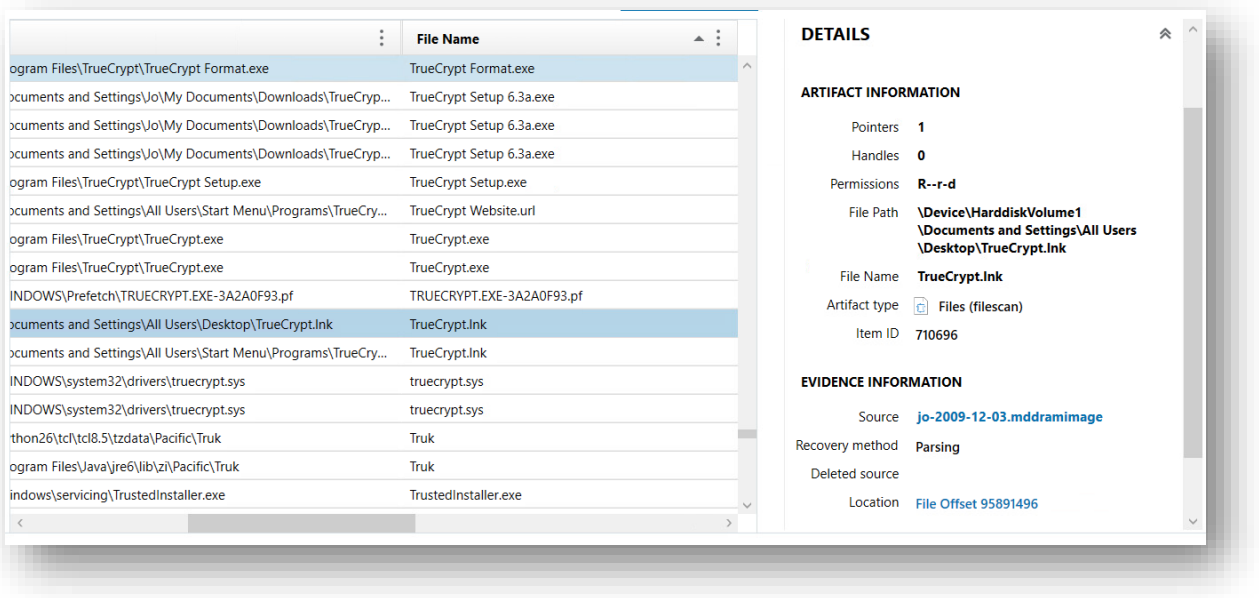
12/4/2009 11:31:19.211 PM	Gamblers Anonymous International Dir...	6	No	Firefox Web History	te
12/3/2009 7:21:32.425 PM	Gamblers Anonymous International Dir...	4	No	Firefox Web History	te
12/1/2009 11:35:30.120 PM	Gamblers Anonymous International Dir...	3	No	Firefox Web History	te
12/1/2009 11:35:30.120 PM	Gamblers Anonymous International Dir...	3	No	Firefox Web History	te
11/30/2009 11:47:23.182...	Gamblers Anonymous International Dir...	1	No	Firefox Web History	te
12/4/2009 11:31:19.211 PM	Gamblers Anonymous International Dir...	6	No	Firefox Web History	te
12/4/2009 7:13:45.478 PM	Gamblers Anonymous International Dir...	5	No	Firefox Web History	te
12/4/2009 11:24:27.402 PM	Gamblers Anonymous Official Home P...	6	No	Firefox Web History	te
12/3/2009 7:19:18.823 PM	Gamblers Anonymous Official Home P...	4	No	Firefox Web History	te
12/1/2009 11:34:53.444 PM	Gamblers Anonymous Official Home P...	3	No	Firefox Web History	te
12/1/2009 11:34:53.444 PM	Gamblers Anonymous Official Home P...	3	No	Firefox Web History	te
11/30/2009 11:39:35.384...	Gamblers Anonymous Official Home P...	1	No	Firefox Web History	te
12/4/2009 11:24:27.402 PM	Gamblers Anonymous Official Home P...	6	No	Firefox Web History	te

  - **Path**: e3://Kitty/terry-2009-12-04/Partition Parser/Partition40/*binary_file/FAT/Partition::Free::Spaces/Partition::Free::Spaces::Detected/unallocated_blocks_0_999?item=unallocated_block_9564_16



Jo's Activities:

- **Downloading and Installing Unauthorized Software**: Jo is found to have downloaded and installed unauthorized software, including "TrueCrypt," which could be used to hide or encrypt data.
    - **Path**: jo-2009-12-03.mddramimage
    - **File Path**: \Device\HarddiskVolume1\Documents and Settings\All Users\Desktop\TrueCrypt.lnk
    - **Evidence:**



These suspicious activities suggest potential misconduct, policy violations, and even criminal behavior within M57. Further investigation is needed to determine the full extent of these activities and their implications.

3. Terry has attempted to eliminate evidence of criminal activity by deleting old emails. How did he do this? Was it successful? Can emails be recovered from the drive image in police evidence?

Answer:

- **Path:** terry-2009-12-04.E01 - Partition 1 (Microsoft NTFS, 38.28 GB)\Users\terry\AppData\Local\Microsoft\Windows Mail\Local Folders\Deleted Items\041C5ED6-00000007.eml
    - **Deleted Items Folder:** The data clearly indicates that these files were found in the Deleted Items folder. This suggests that Terry deleted emails by simply moving them from his inbox or sent folder to the Deleted Items folder. In Windows Mail, when an email is moved to the Deleted Items folder, it's not immediately deleted from the drive. Instead, it's marked as "allocated" to the Deleted Items folder.
    - **Not Successful:** This method of deletion was not successful in permanently removing the emails. The files are still present in the Deleted Items folder and can be recovered using forensic tools like Autopsy.

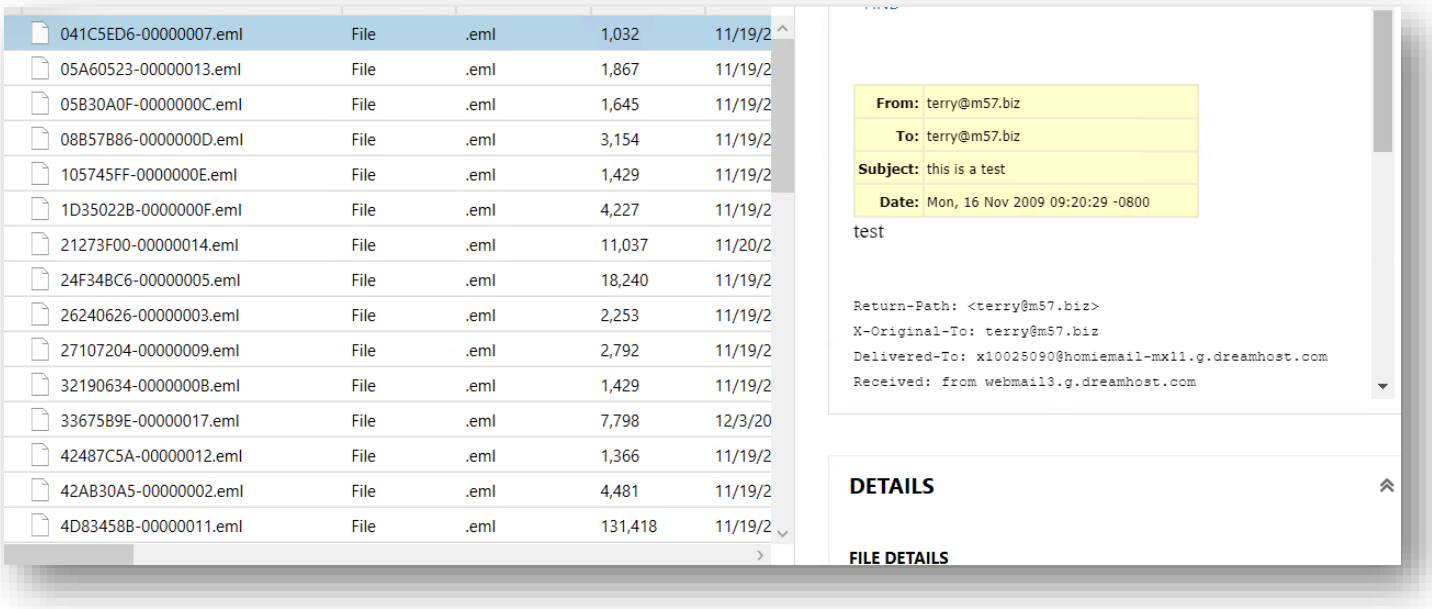
- **.eml and .eml:OECustomProperty Files:** The list shows pairs of .eml files (containing the email content) and .eml:OECustomProperty files (containing email metadata). The presence of both types of files indicates that the emails were not completely erased.

Name	Created Time	Extension
041C5ED6-00000007.eml	2009-11-19 14:49:50 EST	eml
winmail.fol	2009-11-19 14:40:06 EST	fol
62954DC8-00000001.eml:OECustomProperty	2009-11-19 14:40:08 EST	eml
62954DC8-00000001.eml	2009-11-19 14:40:08 EST	eml
041C5ED6-00000007.eml:OECustomProperty	2009-11-19 14:49:50 EST	eml
27107204-00000009.eml:OECustomProperty	2009-11-19 14:49:51 EST	eml
05A60523-00000013.eml:OECustomProperty	2009-11-19 14:49:51 EST	eml
05A60523-00000013.eml	2009-11-19 14:49:51 EST	eml
27107204-00000009.eml	2009-11-19 14:49:51 EST	eml
08B57B86-0000000D.eml:OECustomProperty	2009-11-19 14:49:52 EST	eml
7C436D22-00000010.eml:OECustomProperty	2009-11-19 14:49:52 EST	eml
08B57B86-0000000D.eml	2009-11-19 14:49:52 EST	eml
7C436D22-00000010.eml	2009-11-19 14:49:52 EST	eml
4D83458B-00000011.eml:OECustomProperty	2009-11-19 14:49:54 EST	eml
4D83458B-00000011.eml	2009-11-19 14:49:54 EST	eml
42AB30A5-00000002.eml:OECustomProperty	2009-11-19 15:00:32 EST	eml
42487C5A-00000012.eml:OECustomProperty	2009-11-19 15:00:32 EST	eml
26240626-00000003.eml:OECustomProperty	2009-11-19 15:00:32 EST	eml
42487C5A-00000012.eml	2009-11-19 15:00:32 EST	eml
26240626-00000003.eml	2009-11-19 15:00:32 EST	eml
42AB30A5-00000002.eml	2009-11-19 15:00:32 EST	eml
105745FF-0000000E.eml:OECustomProperty	2009-11-19 15:00:33 EST	eml
32190634-0000000B.eml:OECustomProperty	2009-11-19 15:00:33 EST	eml
1D35022B-0000000F.eml:OECustomProperty	2009-11-19 15:00:33 EST	eml
663E7D55-0000000A.eml:OECustomProperty	2009-11-19 15:00:33 EST	eml
05B30A0F-0000000C.eml:OECustomProperty	2009-11-19 15:00:33 EST	eml
69285545-00000006.eml:OECustomProperty	2009-11-19 15:00:33 EST	eml

24F34BC6-00000005.eml:OECustomProperty	2009-11-19 15:00:33 EST	eml
783F5579-00000004.eml:OECustomProperty	2009-11-19 15:00:33 EST	eml
59883E0D-00000008.eml:OECustomProperty	2009-11-19 15:00:33 EST	eml
105745FF-0000000E.eml	2009-11-19 15:00:33 EST	eml
32190634-0000000B.eml	2009-11-19 15:00:33 EST	eml
663E7D55-0000000A.eml	2009-11-19 15:00:33 EST	eml
05B30A0F-0000000C.eml	2009-11-19 15:00:33 EST	eml
1D35022B-0000000F.eml	2009-11-19 15:00:33 EST	eml
69285545-00000006.eml	2009-11-19 15:00:33 EST	eml
59883E0D-00000008.eml	2009-11-19 15:00:33 EST	eml
783F5579-00000004.eml	2009-11-19 15:00:33 EST	eml
24F34BC6-00000005.eml	2009-11-19 15:00:33 EST	eml
21273F00-00000014.eml:OECustomProperty	2009-11-20 12:13:43 EST	eml
21273F00-00000014.eml	2009-11-20 12:13:43 EST	eml
68E45DF7-00000015.eml:OECustomProperty	2009-11-20 12:43:45 EST	eml
68E45DF7-00000015.eml	2009-11-20 12:43:45 EST	eml
1CFA4233-0000001E.eml:OECustomProperty	2009-11-24 16:27:13 EST	eml
1CFA4233-0000001E.eml	2009-11-24 16:27:13 EST	eml
5FBA4750-00000016.eml:OECustomProperty	2009-12-01 13:01:27 EST	eml
5FBA4750-00000016.eml	2009-12-01 13:01:27 EST	eml
33675B9E-00000017.eml:OECustomProperty	2009-12-03 14:24:55 EST	eml
33675B9E-00000017.eml	2009-12-03 14:24:55 EST	eml
45895FCF-0000001B.eml:OECustomProperty	2009-12-07 11:27:38 EST	eml
45895FCF-0000001B.eml	2009-12-07 11:27:38 EST	eml
1D3B7188-0000001C.eml:OECustomProperty	2009-12-07 13:41:27 EST	eml
1D3B7188-0000001C.eml	2009-12-07 13:41:27 EST	eml
053223F3-0000001A.eml:OECustomProperty	2009-12-08 11:22:36 EST	eml
14DA26E5-00000019.eml:OECustomProperty	2009-12-08 11:22:36 EST	eml
053223F3-0000001A.eml	2009-12-08 11:22:36 EST	eml
14DA26E5-00000019.eml	2009-12-08 11:22:36 EST	eml

26E509E4-0000001D.eml:OECustomProperty	2009-12-08 16:04:49 EST	eml
26E509E4-0000001D.eml	2009-12-08 16:04:49 EST	eml
45B128E6-00000018.eml:OECustomProperty	2009-12-09 14:37:37 EST	eml
45B128E6-00000018.eml	2009-12-09 14:37:37 EST	eml
7C436D22-00000010.eml	0000-00-00 00:00:00	eml

Thus, Terry tried to delete emails by moving them to the "Deleted Items" folder, but this didn't get rid of them.



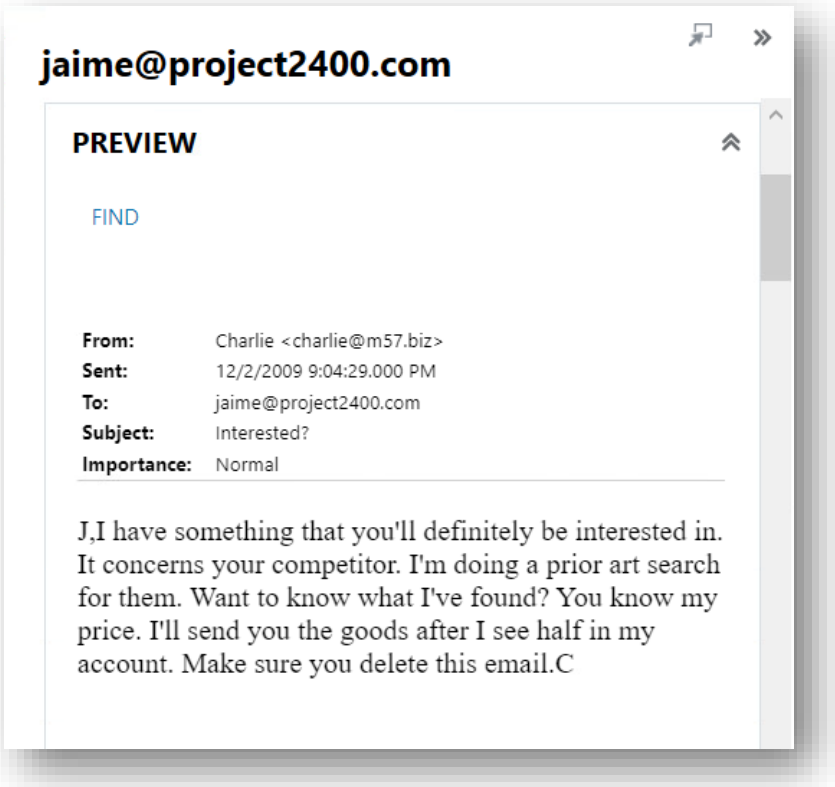
4. We know that Terry, Jo, Charlie, and Pat McGoo work for m57 Patents. A number of other personas appear in the email histories for the employees. Who are they, and which of them (if any) are involved in criminal activity?

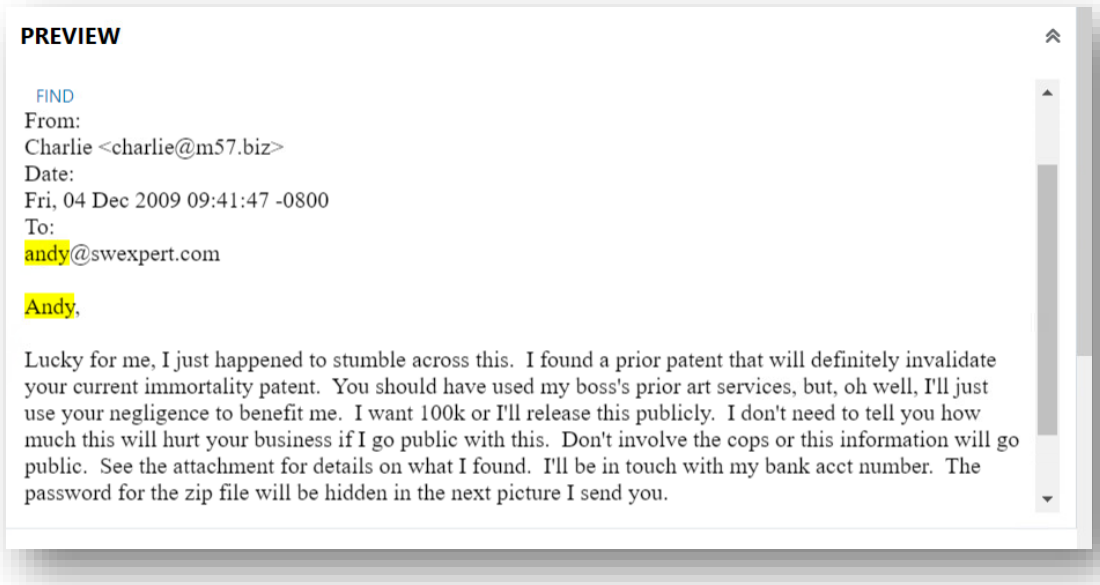
Answer: There were multiple entities who were in contact with the employe of M57 patents while some were for professional communication while some were planning something illegal and against the companies policy and ethics. Here are the people associated with each employee:

- ***Charlie Brown: from Charlie's USB Drive Image (Charlie-work-usb-2009-12-11-001.E01)***
  - Charlie's is in email communication with 4 people outside the organization. They are:

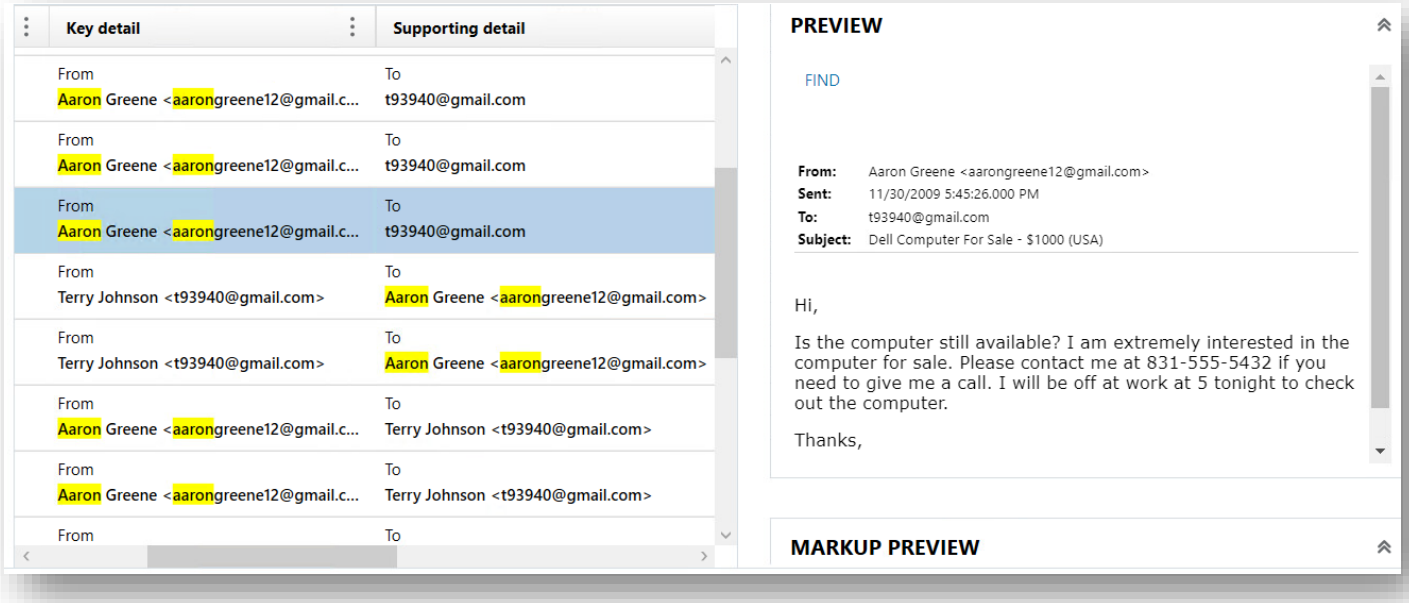
Name	Email	Communication Type
Rubin Fritz	rubinfritz31@mail.com	Discussions about movie nights, dinners, and casual topics
Alix Pery	alix.pery@yahoo.com	Conversations related to cars, cruises, and vacations
Jaime	jaime@project2400.com	Illegal activities
Andy	andy@swexpert.com	

This conversations reveals interactions with external individuals, particularly Jaime and Andy. Charlie appears to be involved in illegal activities, including industrial espionage and blackmail. He offers to sell sensitive information to Jaime and threatens to disclose Andy's patent unless paid a hefty sum. These actions raise serious concerns about Charlie's conduct and potential criminal liability. While it looks like Jaime might be involved in something illegal, the evidence suggests that Charlie is blackmailing Andy, perhaps because Andy used a patent that doesn't belong to him. While Charlie is communicating with Jaime and is planning data exfiltration.

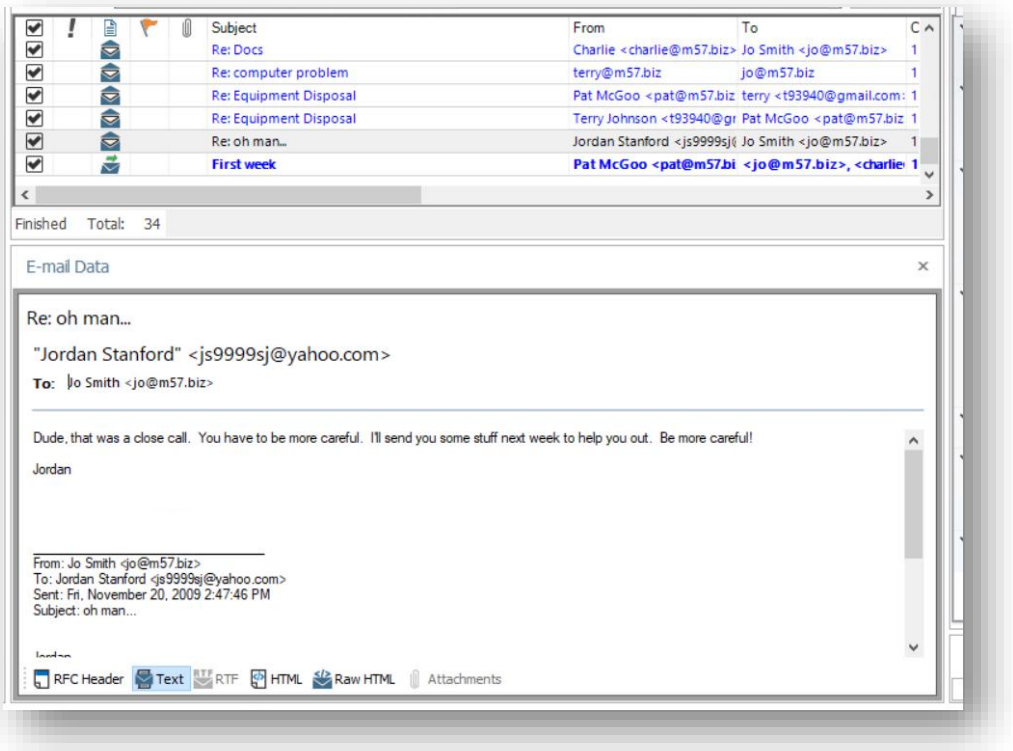


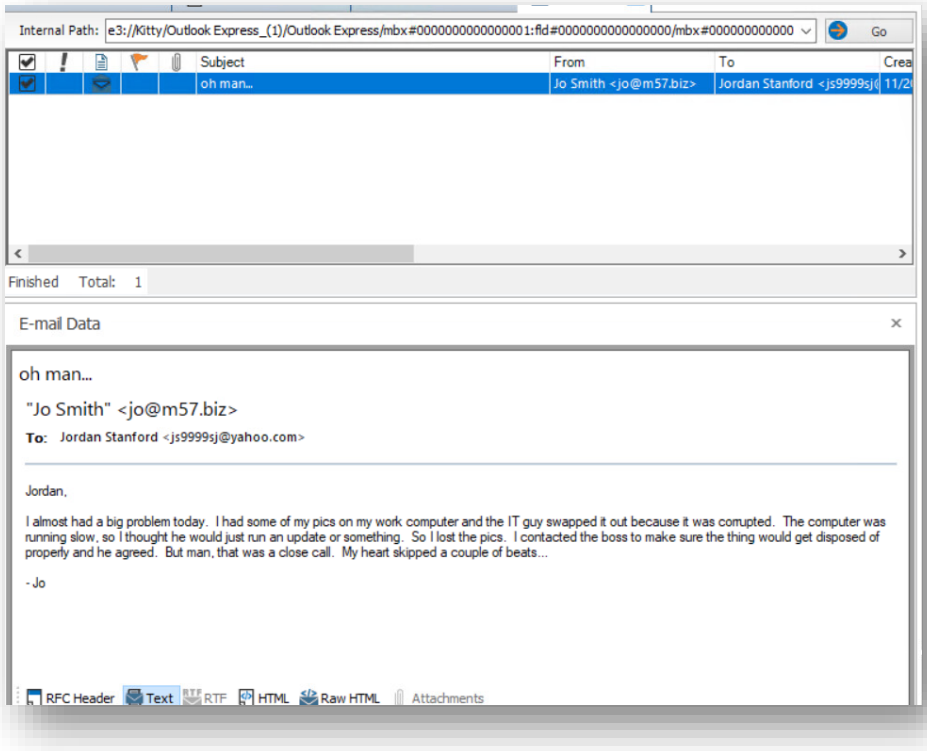


- ***Terry Johnson: Terry's USB Drive Image (Terry-2009-12-04-001.E01)***
  - **Path:** terry-2009-12-04.E01 - Partition 1 (Microsoft NTFS, 38.28 GB)\Users\terry\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox\34B940E9-0000003A.eml
  - Terry had posted an advertisement on craigslist to sell the old PC of Jo. Following that advertisement, a person named Aaron Greene contacted Terry to buy the PC. Terry's emails show he was involved in selling Jo's old computer to Aaron. This is a problem because the computer had explicit content on it, which means selling it could be seen as helping Jo commit a crime. Before selling the computer, Terry should have wiped the hard drive to delete all the data. Emails between Jo, Pat, and Terry confirm this was supposed to happen. Jo even told them there was company data on the computer and talked about how to get rid of it properly. Pat trusted Terry, as the IT person, to handle this correctly.



- ***Jo Smith:***
  - Jo was in contact with one of his friends named Jordan Stanford who is involved in storing of the kitty exploitation images and videos along with Jo Smith.
  - **Path:** e3://Kitty/Outlook Express_(1)/Outlook Express/mbx#0000000000000001:fld#0000000000000000/mbx#0000000000000001:fld#0000000000000004?item=fld#0000000000000001:msg#0000000000000000





5. Charlie sends a number of emails with attachments that have been protected or otherwise obfuscated. What are they? Can the original information be recovered? 10ptw

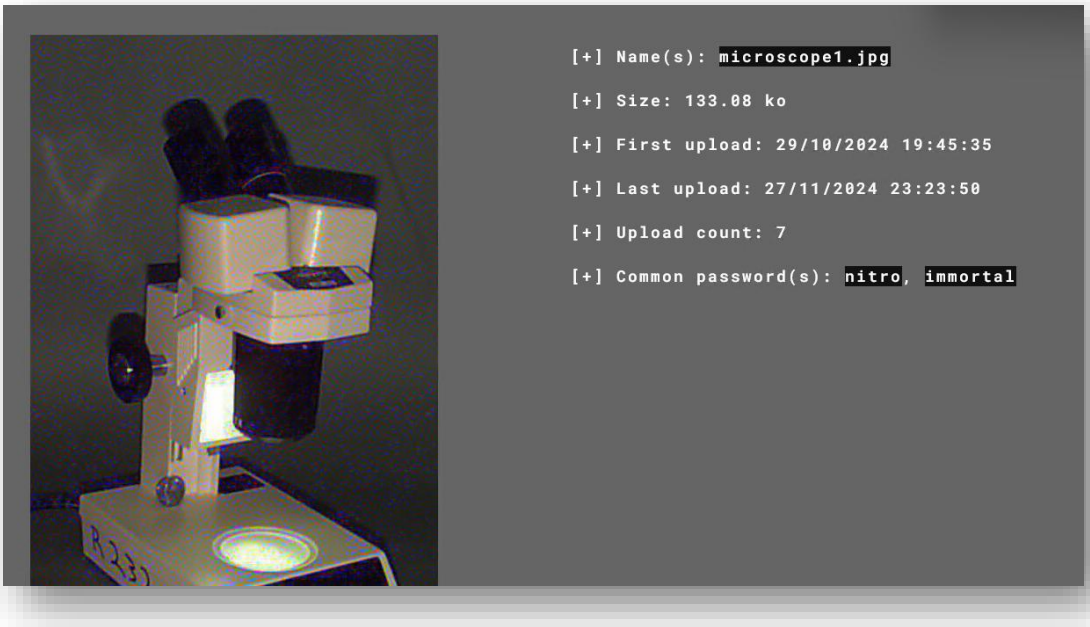
Answer: Charlie sent three emails with protected or obfuscated attachments:

- **To Jaime**: An image file named `astronaut1.jpg` which was protected using steganography. The password, "nitro," was recovered using the online tool "Aperi' Solve."
- **To Andy**: A password-protected ZIP file named `immortality.zip`. The password, "immortal," was hidden within another image file (`microscope1.jpg`) and recovered using "Aperi' Solve." The ZIP file contained two password-protected TIF images, also protected with the password "immortal." These images, when accessed, revealed content related to a U.S. Patent.

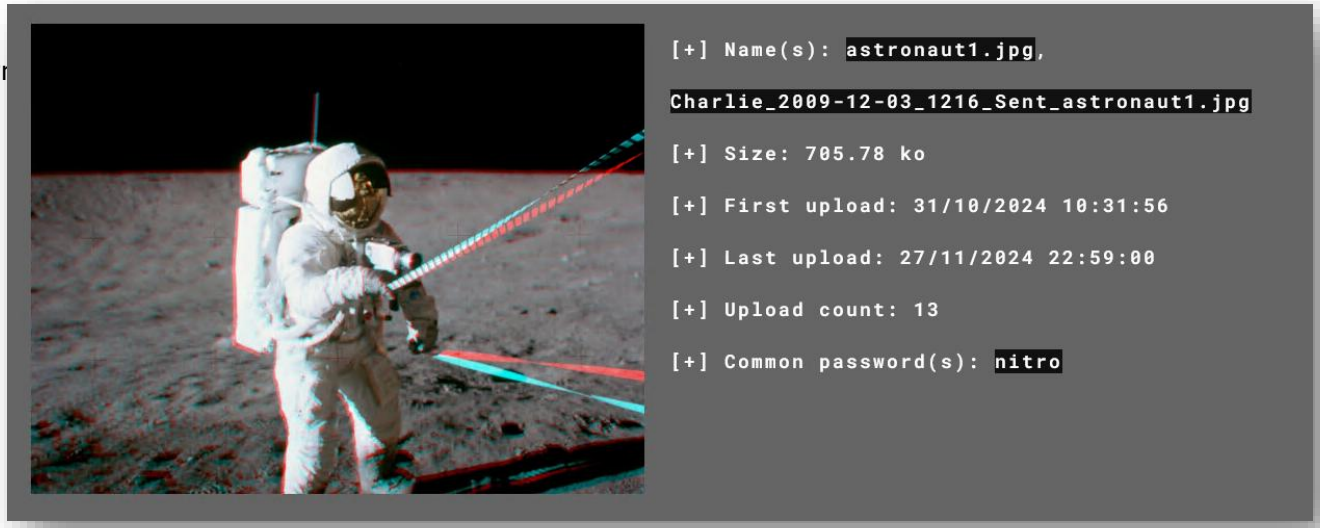
In summary, Charlie's emails contained attachments secured with passwords and steganography. However, using appropriate tools like "Aperi' Solve" and password recovery techniques, the original information within these attachments was successfully recovered.

- **Evidence:** Charlie sent an email containing a password-protected ZIP file and hinted that the password was hidden within separate image attachment (microscope1.jpg and astronaut1.jpg).

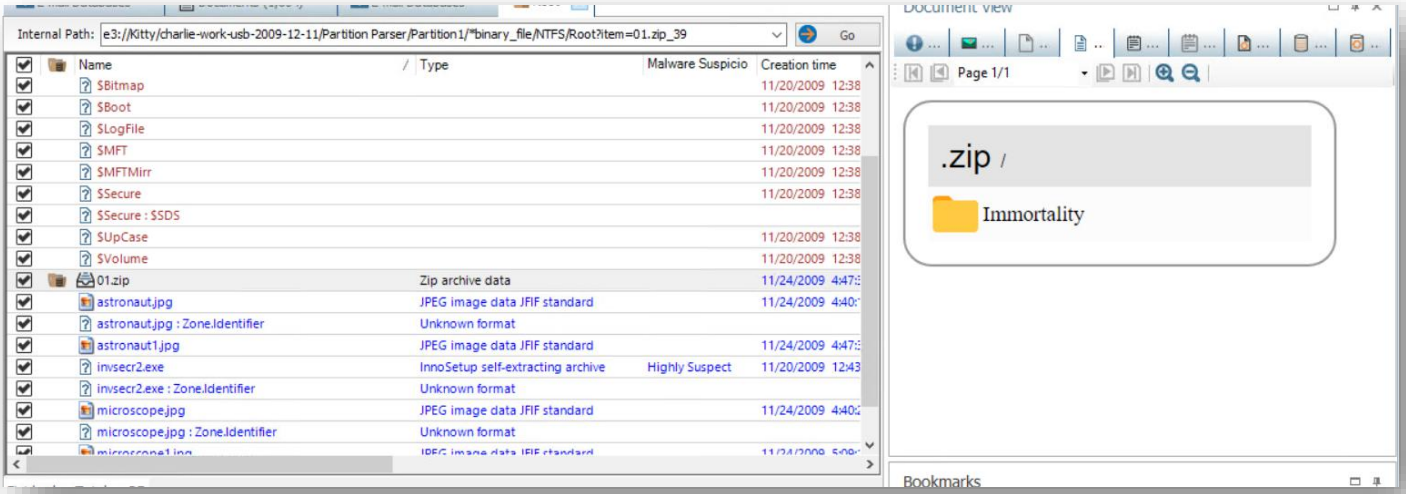
To	Date	Attachment	Description
Jaime (jaime@project2400.com)	Thu, 03 Dec 2009 12:16:52	**atraonaut1.jpg**	Charlie sends a picture of an astronaut with password hidden inside it is using a steganography
Andy (andy@swexpert.com)	Fri, 04 Dec 2009 09:41:47	**immortality.zip**	Charlie sends a password-protected zip file
Andy (andy@swexpert.com)	Mon, 07 Dec 2009 11:44:18	**microscope1.jpg**	Charlie sends another stereographed image

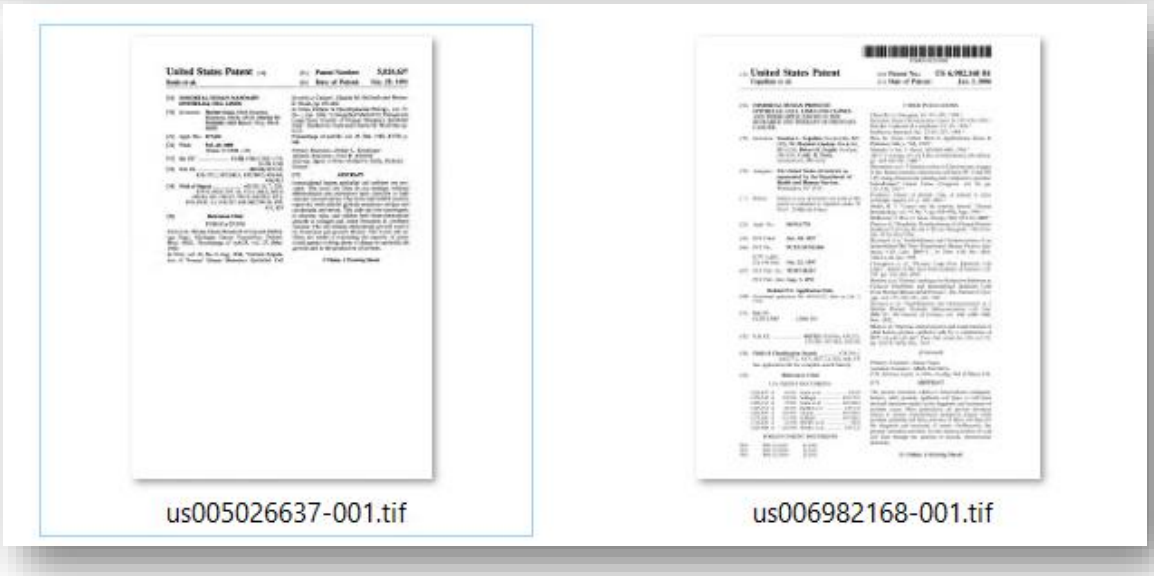


Pr

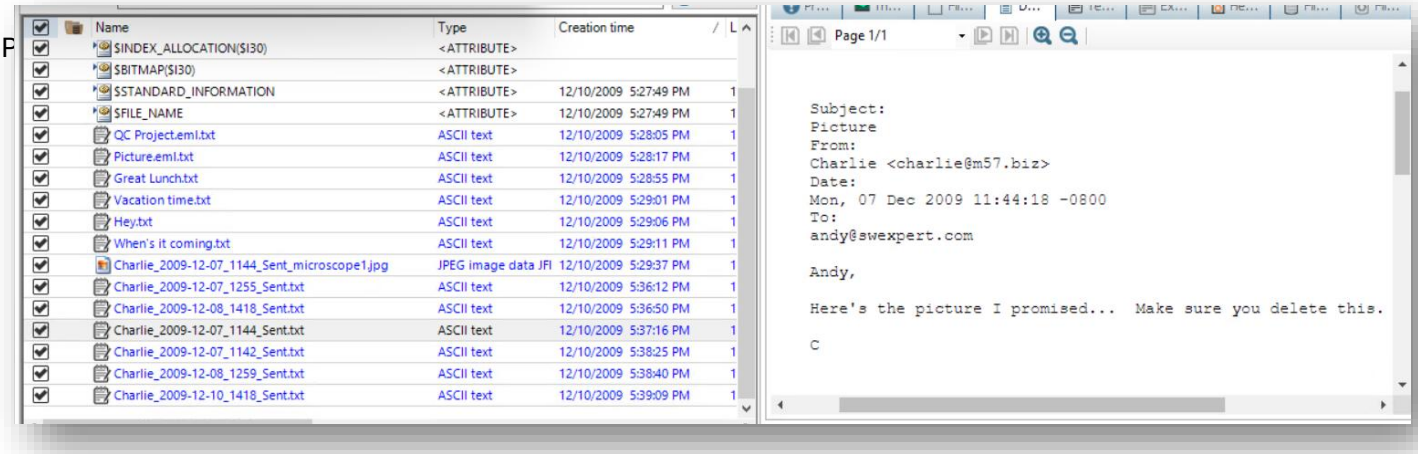


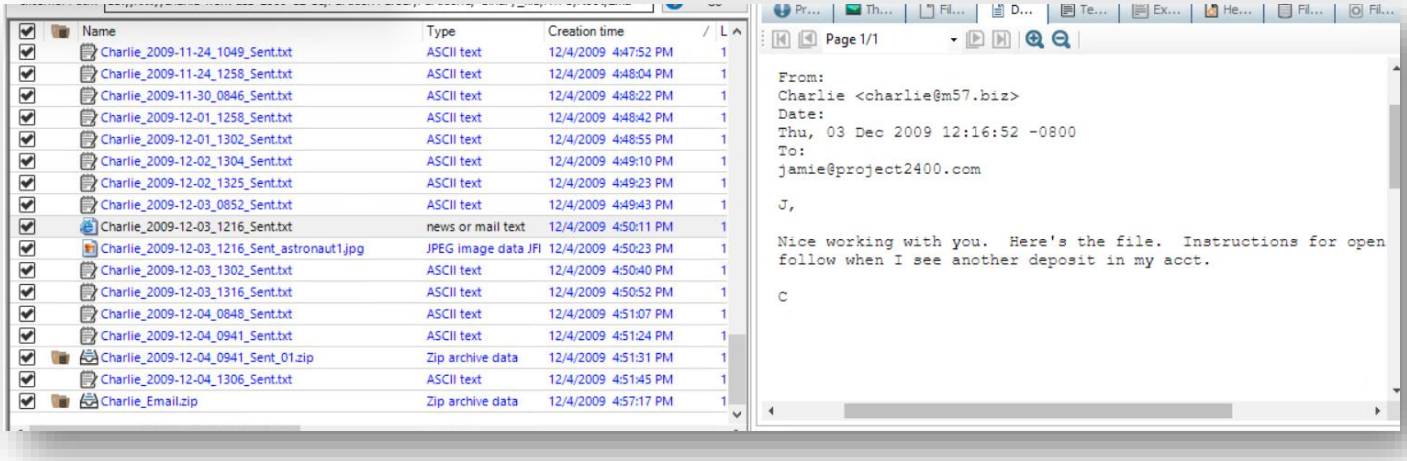
The ZIP file (01.zip) was password-protected and required the password "immortal" to be extracted. Inside, a folder named "immortality" contained two password-protected TIF images. After entering the same password, the images were accessed, revealing content related to a U.S. Patent, as described in an email from Charlie to Andy.

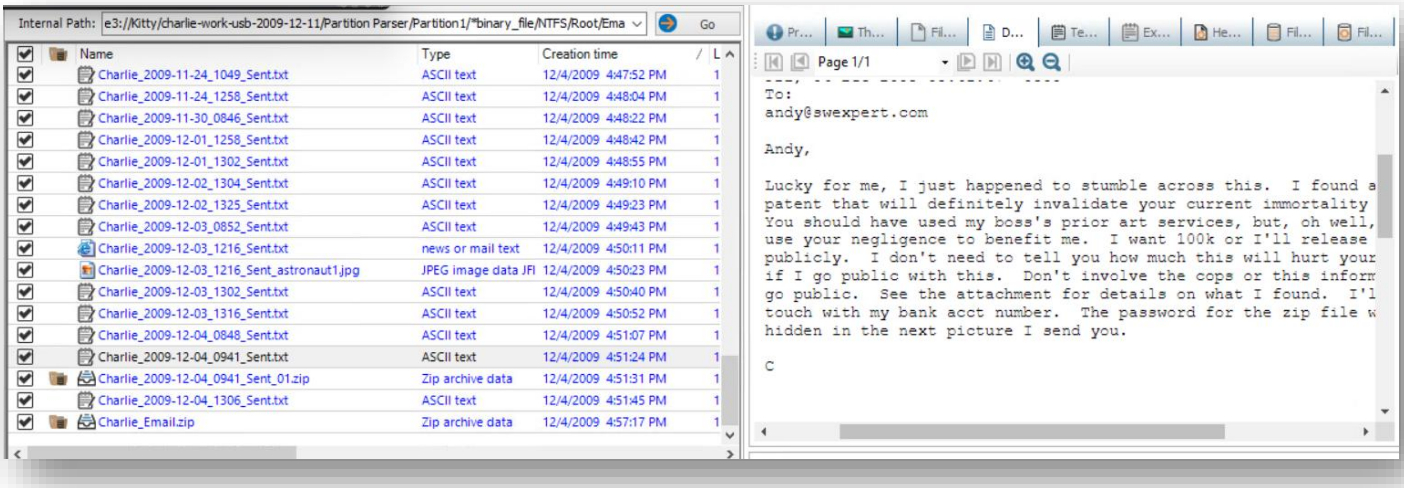




P


Name
Type
Creation time
$INDEX_ALLOCATION($I30) <ATTRIBUTE>
$BITMAP($I30) <ATTRIBUTE>
$STANDARD_INFORMATION <ATTRIBUTE> 12/10/2009 5:27:49 PM
$FILE_NAME <ATTRIBUTE> 12/10/2009 5:27:49 PM
QC Project.eml.txt ASCII text 12/10/2009 5:28:05 PM
Picture.eml.txt ASCII text 12/10/2009 5:28:17 PM
Great Lunch.txt ASCII text 12/10/2009 5:28:55 PM
Vacation time.txt ASCII text 12/10/2009 5:29:01 PM
Hey.txt ASCII text 12/10/2009 5:29:06 PM
When's it coming.txt ASCII text 12/10/2009 5:29:11 PM
Charlie_2009-12-07_1144_Sent_microscope1.jpg JPEG image data JFI 12/10/2009 5:29:37 PM
Charlie_2009-12-07_1255_Sent.txt ASCII text 12/10/2009 5:36:12 PM
Charlie_2009-12-08_1418_Sent.txt ASCII text 12/10/2009 5:36:50 PM
Charlie_2009-12-07_1144_Sent.txt ASCII text 12/10/2009 5:37:16 PM
Charlie_2009-12-07_1142_Sent.txt ASCII text 12/10/2009 5:38:25 PM
Charlie_2009-12-08_1259_Sent.txt ASCII text 12/10/2009 5:38:40 PM
Charlie_2009-12-10_1418_Sent.txt ASCII text 12/10/2009 5:39:09 PM
Page 1/1
Subject:
Picture
From:
Charlie <charlie@m57.biz>
Date:
Mon, 07 Dec 2009 11:44:18 -0800
To:
andy@swexpert.com
Andy,
Here's the picture I promised... Make sure you delete this.
C


Name
Type
Creation time
Charlie_2009-11-24_1049_Sent.txt ASCII text 12/4/2009 4:47:52 PM
Charlie_2009-11-24_1258_Sent.txt ASCII text 12/4/2009 4:48:04 PM
Charlie_2009-11-30_0846_Sent.txt ASCII text 12/4/2009 4:48:22 PM
Charlie_2009-12-01_1258_Sent.txt ASCII text 12/4/2009 4:48:42 PM
Charlie_2009-12-01_1302_Sent.txt ASCII text 12/4/2009 4:48:55 PM
Charlie_2009-12-02_1304_Sent.txt ASCII text 12/4/2009 4:49:10 PM
Charlie_2009-12-02_1325_Sent.txt ASCII text 12/4/2009 4:49:23 PM
Charlie_2009-12-03_0852_Sent.txt ASCII text 12/4/2009 4:49:43 PM
Charlie_2009-12-03_1216_Sent.txt news or mail text 12/4/2009 4:50:11 PM
Charlie_2009-12-03_1216_Sent_astronaut1.jpg JPEG image data JFI 12/4/2009 4:50:23 PM
Charlie_2009-12-03_1302_Sent.txt ASCII text 12/4/2009 4:50:40 PM
Charlie_2009-12-03_1316_Sent.txt ASCII text 12/4/2009 4:50:52 PM
Charlie_2009-12-04_0848_Sent.txt ASCII text 12/4/2009 4:51:07 PM
Charlie_2009-12-04_0941_Sent.txt ASCII text 12/4/2009 4:51:24 PM
Charlie_2009-12-04_0941_Sent_01.zip Zip archive data 12/4/2009 4:51:31 PM
Charlie_2009-12-04_1306_Sent.txt ASCII text 12/4/2009 4:51:45 PM
Charlie_Email.zip Zip archive data 12/4/2009 4:57:17 PM
Page 1/1
From:
Charlie <charlie@m57.biz>
Date:
Thu, 03 Dec 2009 12:16:52 -0800
To:
jamie@project2400.com
J,
Nice working with you. Here's the file. Instructions for open
follow when I see another deposit in my acct.
C

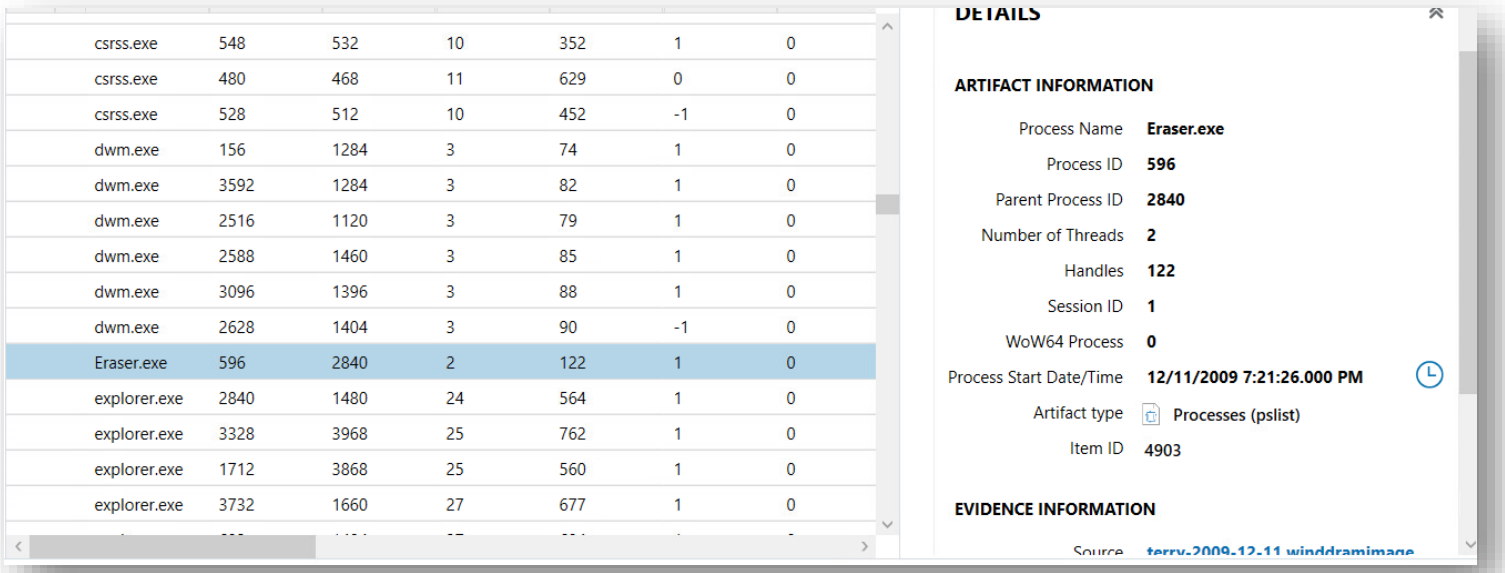

Internal Path: e3://Kitty/charlie-work-usb-2009-12-11/Partition Parser/Partition1/*binary_file/NTFS/Root/Ema
Go
Name
Type
Creation time
Charlie_2009-11-24_1049_Sent.txt ASCII text 12/4/2009 4:47:52 PM
Charlie_2009-11-24_1258_Sent.txt ASCII text 12/4/2009 4:48:04 PM
Charlie_2009-11-30_0846_Sent.txt ASCII text 12/4/2009 4:48:22 PM
Charlie_2009-12-01_1258_Sent.txt ASCII text 12/4/2009 4:48:42 PM
Charlie_2009-12-01_1302_Sent.txt ASCII text 12/4/2009 4:48:55 PM
Charlie_2009-12-02_1304_Sent.txt ASCII text 12/4/2009 4:49:10 PM
Charlie_2009-12-02_1325_Sent.txt ASCII text 12/4/2009 4:49:23 PM
Charlie_2009-12-03_0852_Sent.txt ASCII text 12/4/2009 4:49:43 PM
Charlie_2009-12-03_1216_Sent.txt news or mail text 12/4/2009 4:50:11 PM
Charlie_2009-12-03_1216_Sent_astronaut1.jpg JPEG image data JFI 12/4/2009 4:50:23 PM
Charlie_2009-12-03_1302_Sent.txt ASCII text 12/4/2009 4:50:40 PM
Charlie_2009-12-03_1316_Sent.txt ASCII text 12/4/2009 4:50:52 PM
Charlie_2009-12-04_0848_Sent.txt ASCII text 12/4/2009 4:51:07 PM
Charlie_2009-12-04_0941_Sent.txt ASCII text 12/4/2009 4:51:24 PM
Charlie_2009-12-04_0941_Sent_01.zip Zip archive data 12/4/2009 4:51:31 PM
Charlie_2009-12-04_1306_Sent.txt ASCII text 12/4/2009 4:51:45 PM
Charlie_Email.zip Zip archive data 12/4/2009 4:57:17 PM
Page 1/1
To:
andy@swexpert.com
Andy,
Lucky for me, I just happened to stumble across this. I found a
patent that will definitely invalidate your current immortality
You should have used my boss's prior art services, but, oh well,
use your negligence to benefit me. I want 100k or I'll release
publicly. I don't need to tell you how much this will hurt your
if I go public with this. Don't involve the cops or this inform
go public. See the attachment for details on what I found. I'l
touch with my bank acct number. The password for the zip file w
hidden in the next picture I send you.
C

6. A large number of processes are running on a typical Windows machine. However, the machines used by the m57 employees are not identical. Were there unusual or noteworthy processes running on any of the machines during the police capture?

Answer: To see what programs were running on the employees' computers at M57, a careful analysis of the snapshot of the RAM image till December 11th, 2009, was made. The following are the process running on the PC's of all the employees:

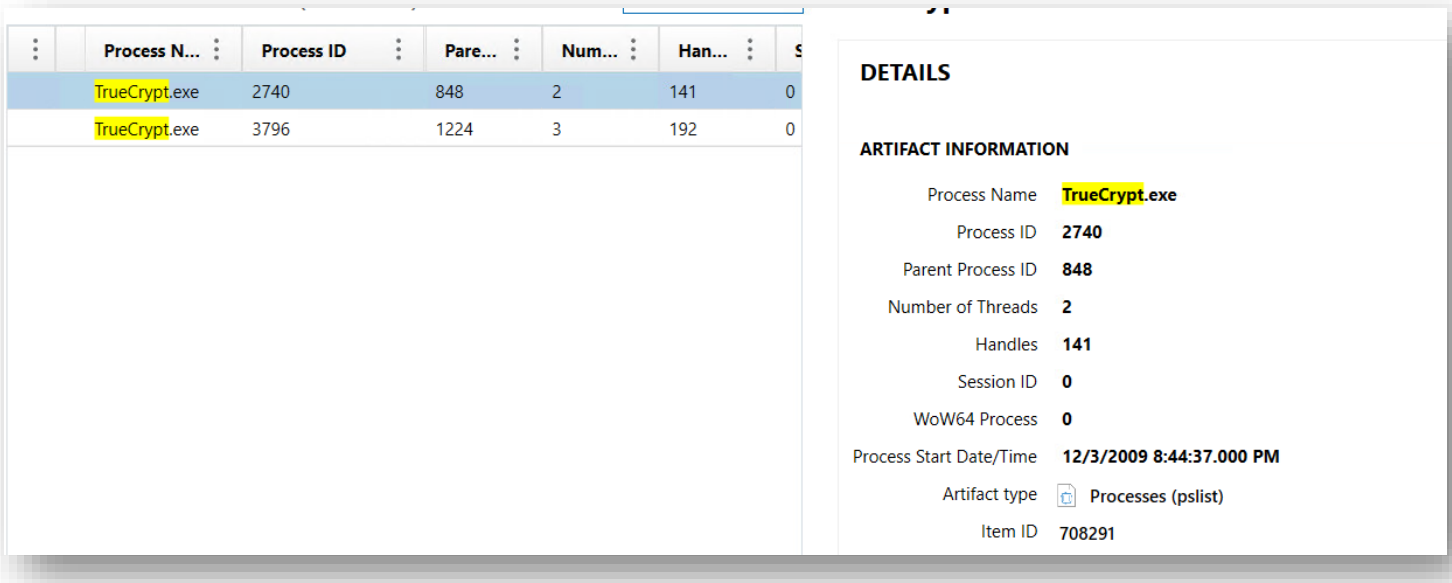
- ***Terry Johnson:***
  - Most of the programs running were typical Windows programs or common applications. However, one program called "Eraser.exe" stood out. This program is often used to securely delete files, which raises concerns about why it was running. It might mean someone was trying to hide or permanently delete information.
  - The **Process List** artifact under the **Memory** section in Magnet AXIOM is a key forensic artifact that provides insights into the processes running on a system at the time the memory (RAM) was captured.
  - **Path:** terry-2009-12-11.winddramimage > file offset 2127382976
  - **Evidence:**

Service Name	Process ID	Process Date	Process Time
Eraser.exe	596	12/11/2009	7:21:26 PM



- ***Jo Smith:***
  - There are no evidence of Jo using any kind of evidence elimination tools but as per the evidence available in the Jo's RAM image from 10 December 2009, there is an encryption tool named "**Truecrypt**" which is a legitimate disk encryption software but can be used to hide evidence by encryption.
  - **Path:** jo-2009-12-03.mddramimage
  - **Evidence:**

Service Name	Process ID	Process Date	Process Time
TrueCrypt.exe	2740	12/3/2009	8:44:37.000 PM
TrueCrypt.exe	3796	12/10/2009	10:42:53.000 PM



- ***Charlie Brown:***
  - To see what programs were running on Charlie's computer, RAM snapshots were taken from December 11th, 2009, and examined. It was noted that there was no illegal or suspicious process running on Charlie's computer during the evidence collection time as he was not involved in any illegal activity going on in the company related to the case.
  - Charlie had only one steganography application used as he was trying to sell company patents which is a suspected case of data exfiltration.
  - **Path**: charlie-2009-11-20.mddramimage
  - **Evidence**:

Item Name	Details
\??\C:\Program Files\Invisible Secrets 2.1\isecrets2.exe	End: 2009-11-19 18:43:34 UTC+0000
UEME_RUNPIDL:%csidl2%\Invisible Secrets 2.1\Invisible Secrets 2.1.lnk	Registry: \Device\HarddiskVolume1\Documents an...
UEME_RUNPATH:C:\Program Files\Invisible Secrets 2.1\isecrets2.exe	Registry: \Device\HarddiskVolume1\Documents an...
UEME_RUNPIDL:%csidl2%\Invisible Secrets 2.1	Registry: \Device\HarddiskVolume1\Documents an...
\??\C:\Program Files\Invisible Secrets 2.1\isecrets2.exe	End: 2009-11-30 16:48:17 UTC+0000
UEME_RUNPIDL:%csidl2%\Invisible Secrets 2.1\Invisible Secrets 2.1.lnk	Registry: \Device\HarddiskVolume1\Documents an...
UEME_RUNPATH:C:\Program Files\Invisible Secrets 2.1\isecrets2.exe	Registry: \Device\HarddiskVolume1\Documents an...
UEME_RUNPIDL:%csidl2%\Invisible Secrets 2.1	Registry: \Device\HarddiskVolume1\Documents an...
\??\C:\Program Files\Invisible Secrets 2.1\isecrets2.exe	End: 2009-11-30 16:48:17 UTC+0000

- ***Pat McGoo:***
  - There are no active suspicious services running on Pat's computer as evident from the RAM analysis from November 16, 2009 till December 11, 2009.
  - **Path**: pat-2009-11-16.mddramimage > file offset 37530056

  - **Evidence:**

Process N...	Proc...	Pare...	Num...	Han...	Ses
System	4	0	58	504	-1
smss.exe	828	4	3	19	-1
csrss.exe	924	828	14	683	0
winlogon.exe	948	828	18	640	0
services.exe	992	948	19	360	0
lsass.exe	1004	948	21	355	0
svchost.exe	1176	992	17	196	0
svchost.exe	1264	992	10	289	0
svchost.exe	1388	992	76	1607	0
svchost.exe	1452	992	5	80	0
avgchsvx.exe	1612	948	23	281	0
avgrsx.exe	1680	948	28	240	0
svchost.exe	1748	992	12	166	0
avgcsrvx.exe	1848	1680	8	168	0
spoolsv.exe	268	992	10	105	0

DETAILS

ARTIFACT INFORMATION

Process Name	**explorer.exe**
Process ID	**488**
Parent Process ID	**444**
Number of Threads	**12**
Handles	**601**
Session ID	**0**
WoW64 Process	**0**
Process Start Date/Time	**11/13/2009 10:04:52.000 PM**
Artifact type	**Processes (pslist)**
Item ID	161573

EVIDENCE INFORMATION

Source	pat-2009-11-16.mddramimage

Apart from the programs running on Terry's and Jo's computer, nothing else unusual was found running on Pat and Charlie's computers. It's important to note that Terry, the IT person, was using Windows Vista, while the others were using Windows XP. Also, Terry, being knowledgeable about computers, was the only one using the "Eraser.exe" program, which is a more specialized tool.

7. Read and analyze the search warrant and affidavit. Establish and document the general nature of the crime(s) which appear to have been committed and prioritize analysis of the available images accordingly.

Answer: The affidavit and search warrant reveal that the investigation involves suspected crimes of possessing and distributing illegal pornographic images and videos. Key details include:

Nature of the Crime: Aaron Greene purchased a used computer through Craigslist from Terry Johnson. Upon using the device, Greene found illegal pornographic material on the hard drive and reported it to the City of Monterey Police Department. The computer was subsequently handed over for forensic analysis.

Probable Cause: Detective Joe Friday established probable cause based on the presence of illegal content on the computer. He emphasized that operating system logs and metadata could provide critical insights into the creation, modification, and access history of the files, potentially identifying the responsible user. Secondary storage devices, such as USB thumb drives, were also considered critical to the investigation.

Legal Framework: The search warrant was issued under California Penal Code Section 1524, which permits the seizure of property believed to be linked to criminal activities. The suspected crimes include violations under Section 311.3(a), which pertains to the exploitation of non-consenting entities.

Forensic Analysis: The warrant prioritizes the analysis of specific digital evidence, including:

- Subscriber and account information.
- RAM images and hard disk drive images from computers assigned to Jo Smith.
- USB thumb drives associated with Jo Smith.
- The focus timeframe is from November 13, 2009, to December 12, 2009.

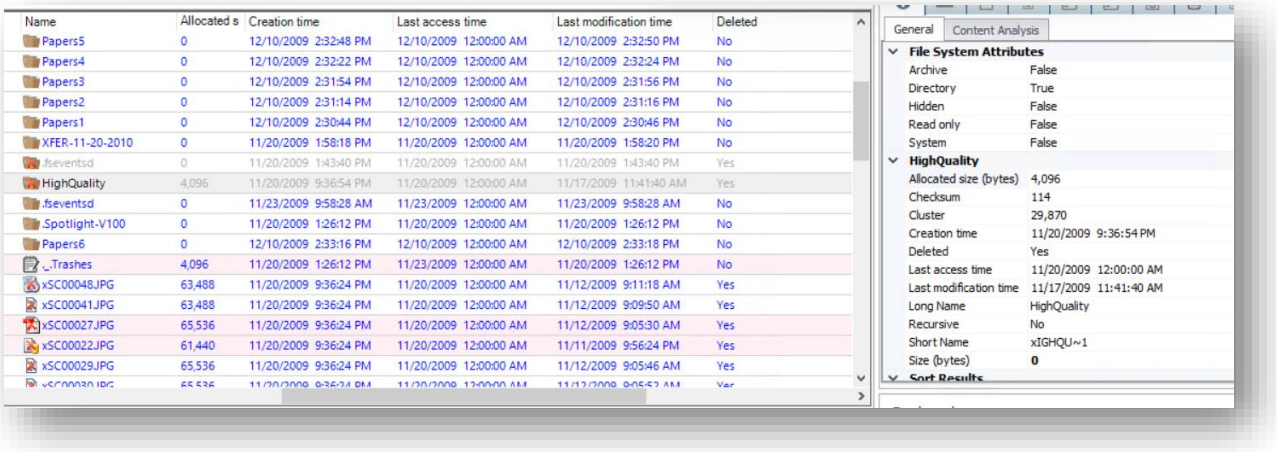
8. Identify a pattern of activity for Jo. Jo appears to have overwritten a large selection of files on one of the thumb drives. Are any of these files recoverable?

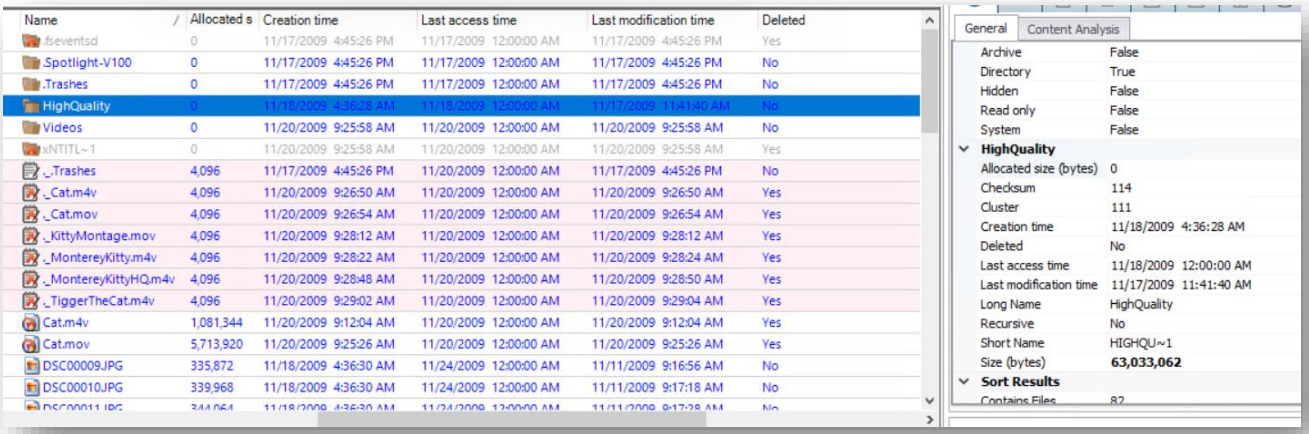
Answer: Jo's activity reveals a pattern of transferring and then deleting files, likely in an attempt to conceal his possession of the "kitty" images and videos. Evidence suggests that Jo copied the "HIGHQUALITY" folder containing these illicit materials from his favourite USB drive to his work USB drive, and subsequently deleted the folder from the work drive. However, despite the deletion, the files within the "HIGHQUALITY" folder may be recoverable through forensic techniques. Evidence of transfer and deletion**:**

Two USB Drives: Jo possesses two USB drives: a "favourite" drive and a "work" drive.

Deleted Folder: The "HIGHQUALITY" folder, containing the explicit content, is found on both drives, but is marked as deleted on the work USB drive. Analysis of the timeline for Jo's computer shows that on November 20th, he connected a USB drive and engaged in copying/creating files, aligning with the suspected transfer of the "HIGHQUALITY" folder.

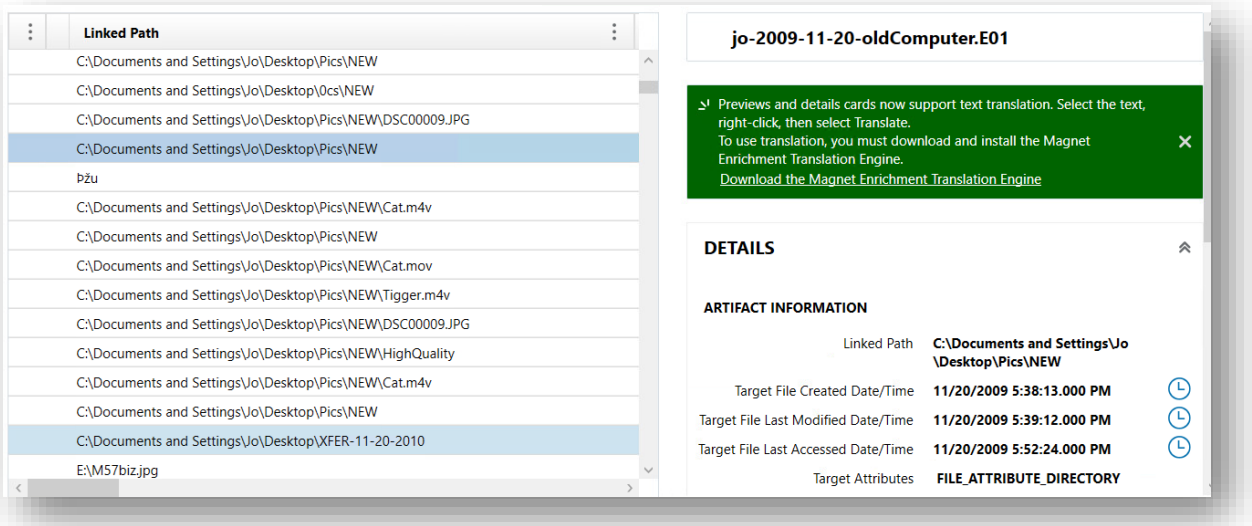
Jo's actions of transferring and deleting the "HIGHQUALITY" folder suggest an attempt to conceal his possession of the illicit content. Despite the deletion, the files might be recoverable from the unallocated space on his work USB drive using forensic techniques. Further analysis and data recovery attempts are recommended to confirm the presence and recoverability of the deleted files.





Evidence of Jo copying the kitty files from USB to his computer on Nov 20 which is the last day of use of his old computer.

Path: jo-2009-11-20-oldComputer.E01 - Partition 1 (Microsoft NTFS, 12.11 GB)\$LogFile



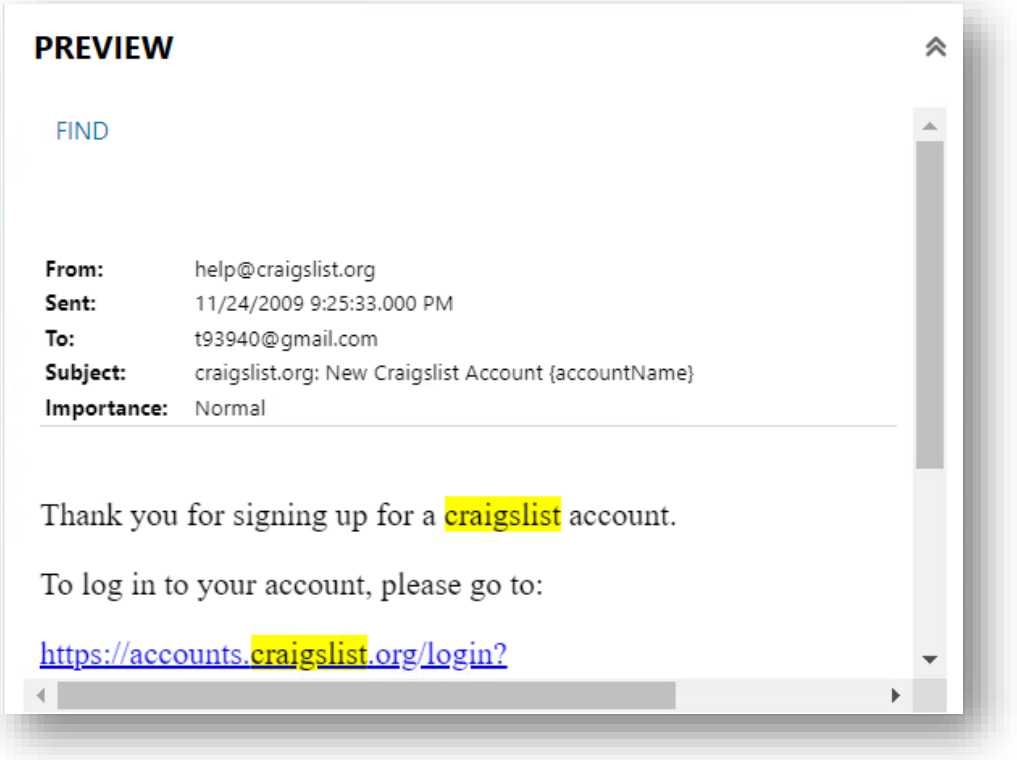
9. Identify a pattern of activity for Terry. Terry is involved in the sale of Jo's old computer. How? Is there evidence of this on his machine?

Answer: Terry's involvement in the sale of Jo's old computer is evident through his email correspondence. His interaction with online content related to a Craigslist post advertising the sale of a Dell computer, which is later confirmed to be Jo's old computer, points to his active participation in the sale. Furthermore, email communication between Terry and Aaron Greene, the eventual buyer of the computer, reveals Terry's direct involvement in facilitating the sale. The fact that the Craigslist account used to advertise the computer was created by Terry on November 24, 2009, further strengthens this assertion.

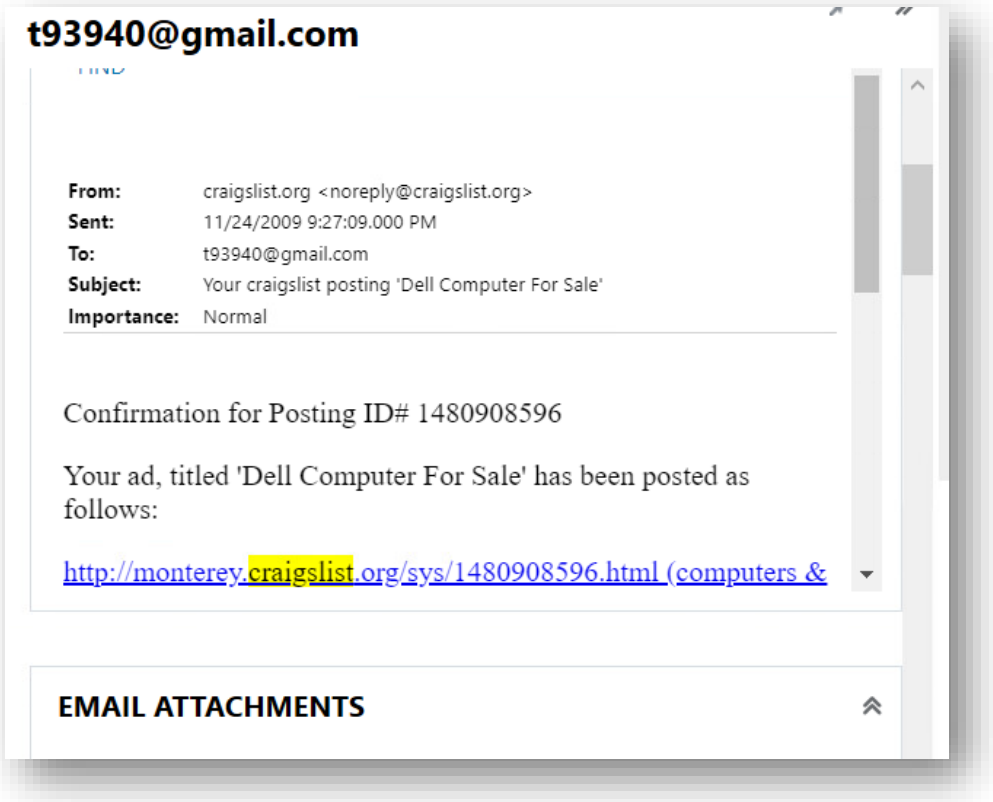
Path: terry-2009-12-04.E01 - Partition 1 (Microsoft NTFS, 38.28 GB)\Users\terry\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox\

Communication	Date	Sender	Receiver	Content
Email	11/24/2009 9:25 PM	help@craigslist.com	t93940@gmail.com	Account creation and confirmation
Email	11/24/2009 9:27 PM	noreply@craigslist.com	t93940@gmail.com	Confirmation for Posting the ads for computer on Craigslist
Email	11/30/2009 5:45 PM	aarongreene12@gmail.com	t93940@gmail.com	Aaron contacting terry for the first time
Email	11/30/2009 6:00PM	t93940@gmail.com	aarongreene12@gmail.com	Terry responding to Aaron and acknowledging the sale
Email	11/30/2009 6:04PM	aarongreene12@gmail.com	t93940@gmail.com	Aaron is acknowledging Terry's response and expressing anticipation for further communication

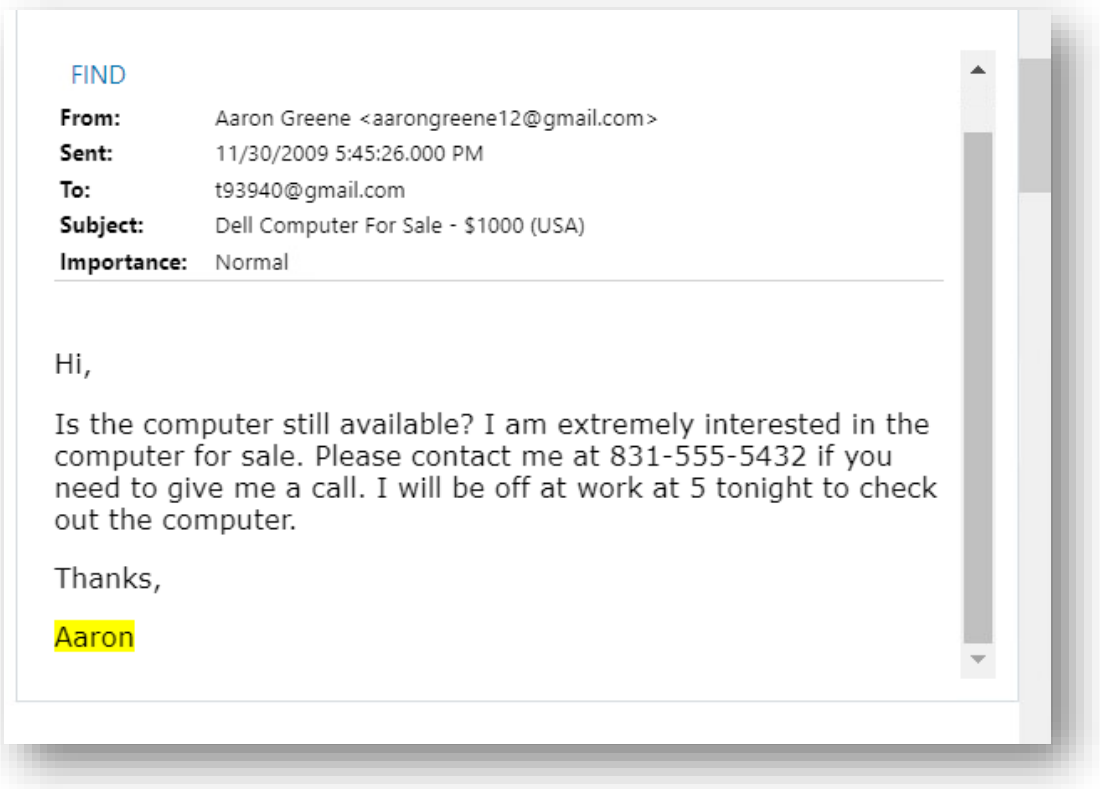
- **ACCOUNT CREATION**



- **ADVERTISE POSTING CONFIRMATION**



- **AARON CONTACTING TERRY FOR THE FIRST TIME**



FIND

From: Aaron Greene <aarongreene12@gmail.com>
Sent: 11/30/2009 5:45:26.000 PM
To: t93940@gmail.com
Subject: Dell Computer For Sale - $1000 (USA)
Importance: Normal

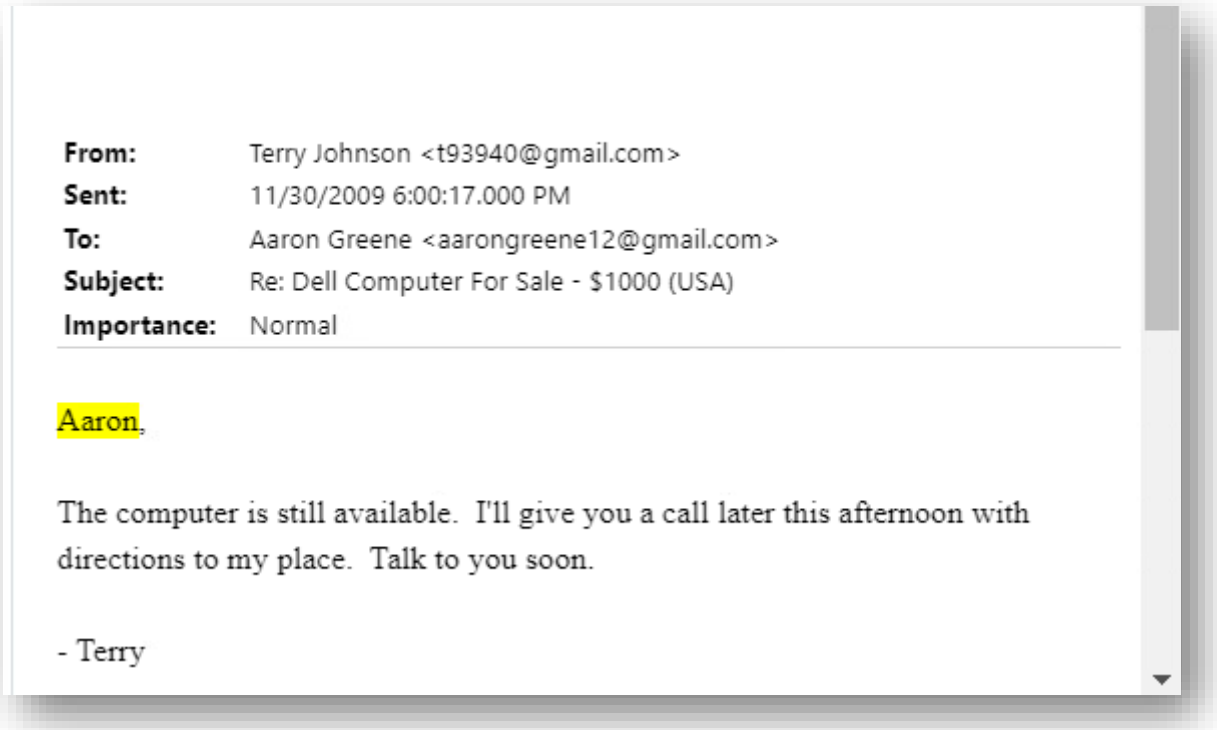
Hi,

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

- **TERRY RESPONDING TO AARON AND ACKNOWLEDGING THE SALE**



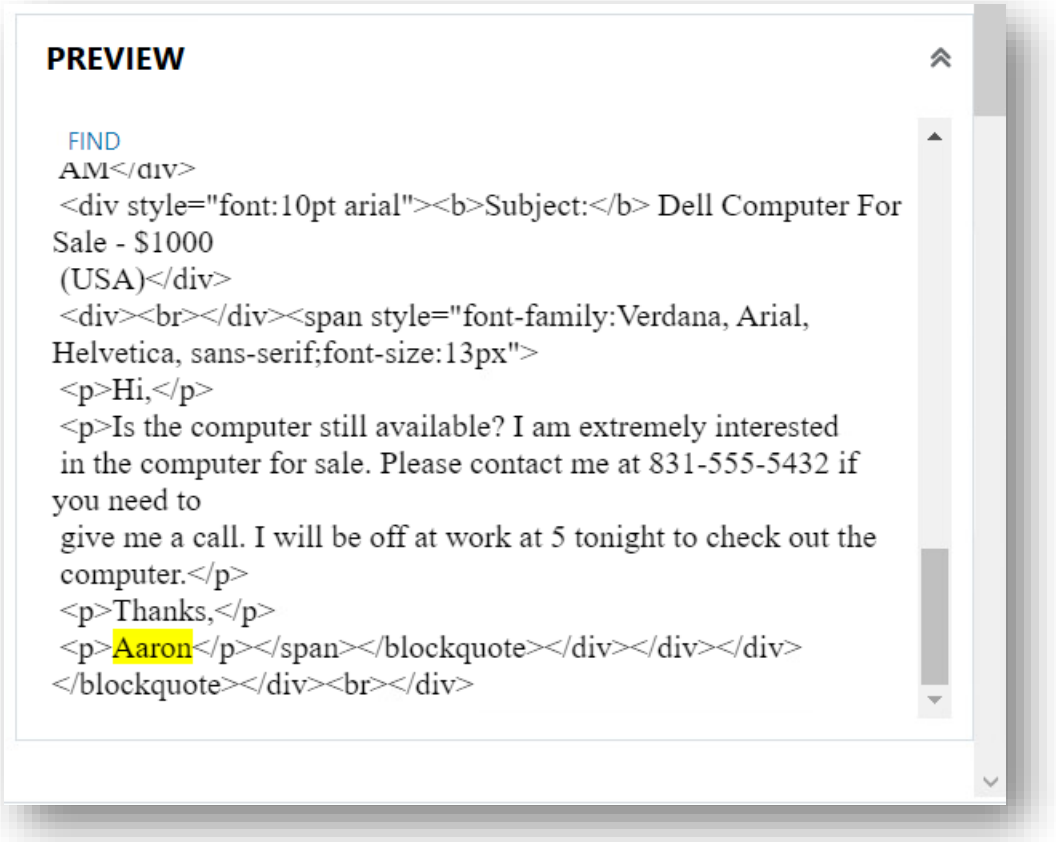
From: Terry Johnson <t93940@gmail.com>
Sent: 11/30/2009 6:00:17.000 PM
To: Aaron Greene <aarongreene12@gmail.com>
Subject: Re: Dell Computer For Sale - $1000 (USA)
Importance: Normal

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

- **ARRON SHOWING INTEREST:**

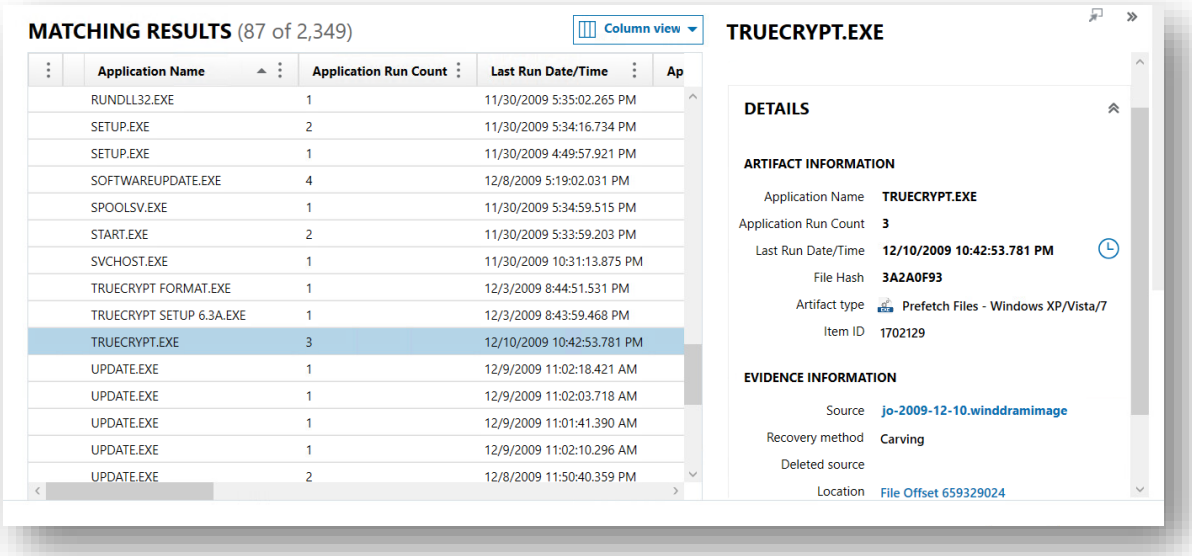


10. Identify use of evidence elimination tools. Which tools have been used, and by whom? Have they been successful?

Answer: The use of evidence elimination tools by each employee of M57 are as follows:

I. ***Jo Smith:*** There are no evidence of Jo using any kind of evidence elimination tools but as per the evidence available in the Jo's RAM image from 10 December 2009, there is an encryption tool named "**Truecrypt**" which is a legitimate disk encryption software but can be used to hide evidence by encryption.

a. **Path:** jo-2009-12-10.winddramimage > file offset 659329024

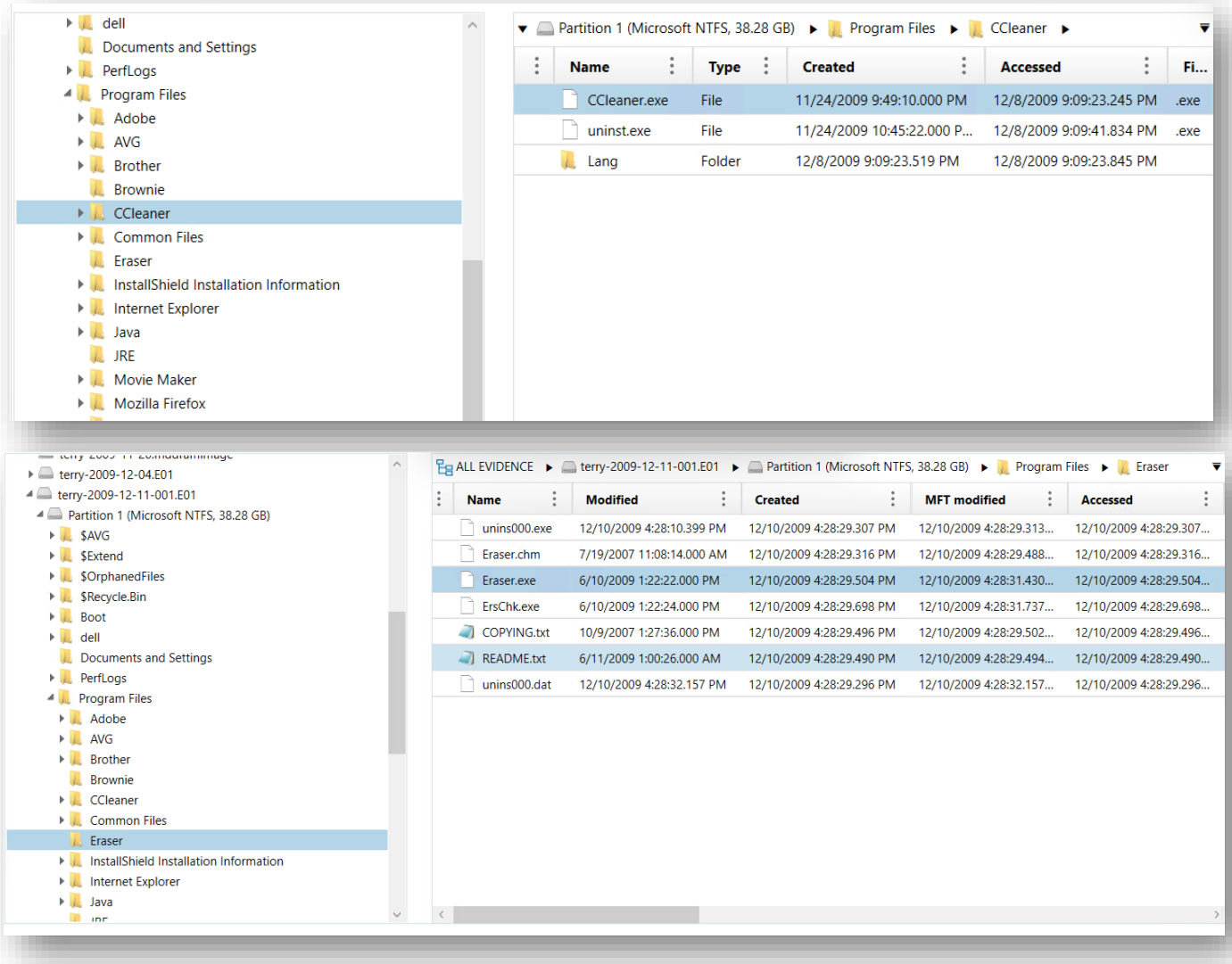


- **What is TrueCrypt:** TrueCrypt is a discontinued source-available freeware utility used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file or encrypt a partition or the whole storage device (pre-boot authentication). On-the-fly encryption (OTFE) means that data is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention.

II. ***Terry Johnson:*** Terry is suspected of using 2 evidence elimination tools named "**CCLEANER**" and "**ERASER.**"

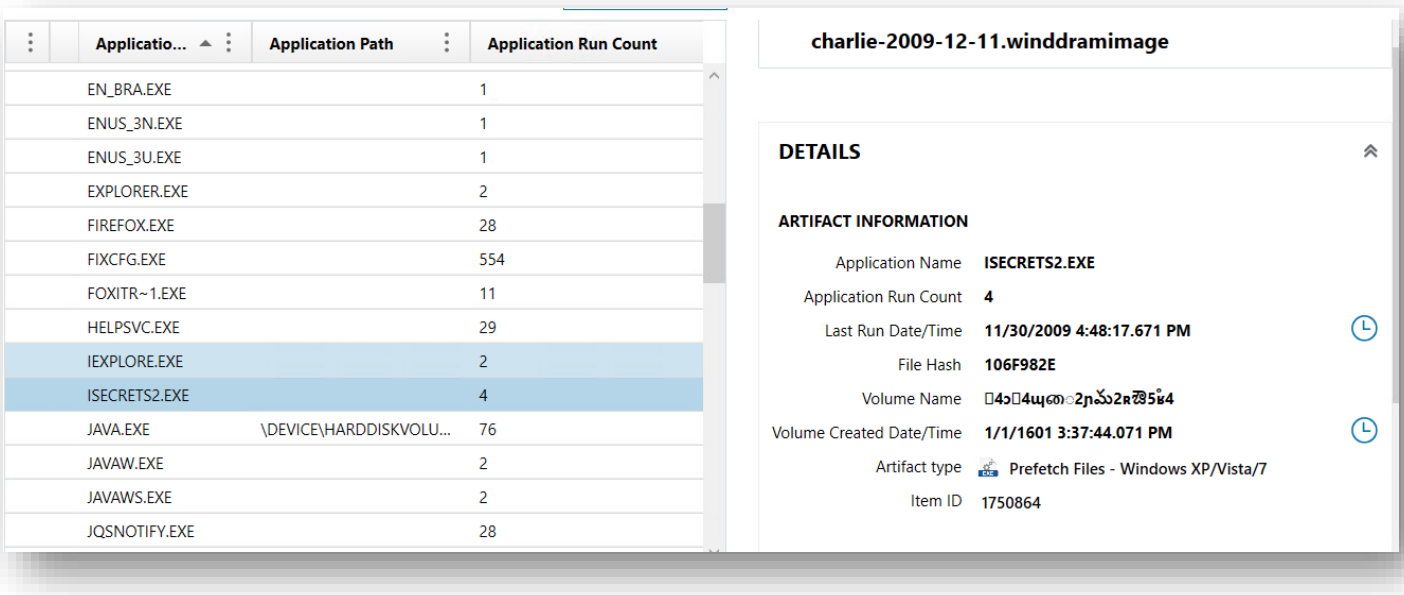
a. Path: terry-2009-12-11-001.E01 - Partition 1 (Microsoft NTFS, 38.28 GB) (Unallocated Clusters)

Tool	Location	Usage Count	Last Access Date	Last Access Time
Ccleaner.exe	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\CCLEANER\CCLEANER.EXE	3	12/8/2009	9:09:49.787 PM
Eraser.exe	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\ERASER\ERASER.EXE	3	12/10/2009	6:49:34.850 PM



III. ***Charlie Brown:*** There are no evidence of Charlie using any kind of evidence elimination tools but as per the evidence available in the Charlie's RAM image from 11 December 2009, but the presence of the "**Invisible Secrets**" software indicates a potential alternative method for concealing data. Invisible Secrets is a software application that provides both encryption and steganography capabilities.

- **Encryption**: It allows users to encrypt files and folders, protecting them with a password.
- **Steganography**: It enables users to hide files within other files, such as images or audio files. This technique is known as steganography, where the data is concealed within another file, making it less obvious that sensitive information is being stored or transmitted.



Applicatio...	Application Path	Application Run Count
EN_BRA.EXE		1
ENUS_3N.EXE		1
ENUS_3U.EXE		1
EXPLORER.EXE		2
FIREFOX.EXE		28
FIXCFG.EXE		554
FOXITR~1.EXE		11
HELPSVC.EXE		29
IEXPLORE.EXE		2
ISECRETS2.EXE		4
JAVA.EXE	\DEVICE\HARDDISKVOLU...	76
JAVAW.EXE		2
JAVAWS.EXE		2
JQSNOTIFY.EXE		28

IV. ***Pat McGoo:*** There are no evidence of Pat using any kind of evidence elimination tools but as per the evidence available in the Pat's RAM image.

➢

QUIZ – 2

1. Write a one-page report (500 words min) describing the evidence the police/detectives found and explain whether they had enough information for a search warrant. Did the information justify taking all the computers and USB drives? Why or Why not?

Answer:

City of Monterey, CA Police Department

Case Number: MT-2009-12-015

Date: 10 December 2009

Time: 5:00 PM

Incident: Suspected Child Exploitation Material

Summary

This report details the investigation into a case of suspected child exploitation material found on a computer. The investigation involved the recovery of a computer, forensic analysis, interviews, and the execution of a search warrant.

Initial Report and Evidence Collection

On December 9, 2009, the department received a call from Aaron Greene, who reported finding child exploitation material on the hard drive of a computer he recently purchased online. Officers were dispatched to Mr. Greene's residence, where he voluntarily surrendered the computer. The computer was then logged as evidence (MT-2009-12-015-EV001) and sent to the forensics lab for analysis.

Forensic Analysis and Identification of Suspect

The forensic lab conducted an analysis of the computer's hard drive and determined that it had been used by a local company, M57 Patents. The primary user of the computer was identified as an employee named Jo (last name unavailable). Further investigation revealed that the owner of M57 Patents is Pat McGoo.

Interview with Pat McGoo

Detectives Friday and Gannon conducted an interview with Mr. McGoo at the M57 Patents office. During the interview, Mr. McGoo stated that he believed the computer in question had likely been stolen, as he had been informed it was non-functional. Mr. McGoo confirmed that Jo was an employee of the company. While cooperative, Mr. McGoo requested to consult with his attorney before consenting to a search of company property.

Warrant for USB Thumb Drive

Forensic technologists, during their analysis of the computer, found evidence suggesting the use of a USB thumb drive to transfer the child exploitation material. Based on this finding, a search warrant (MT-2009-12-015-W001) was requested and granted for the seizure of the USB thumb drive, with the assumption that it belonged to Jo.

Execution of Warrant and Search Authorization

Mr. McGoo contacted the department the following morning and authorized a voluntary search of the company's computers and any USB thumb drives belonging to Jo. During the search, the USB thumb drive in question was located and seized.

Legality of Search and Seizure

The initial recovery of the computer was lawful due to its voluntary surrender by Mr. Greene. The subsequent search and seizure of the USB thumb drive were also legal, as they were based on a valid warrant and conducted with the authorization of the company owner, Mr. McGoo.

However, it's important to note that the seizure of all computers and USB thumb drives at M57 Patents, as initially considered, would have been unlawful. The information obtained from the initial computer did not provide probable cause to believe that other company devices were involved in the crime. Seizing these items would have violated the Fourth Amendment, which protects against unreasonable searches and seizures.

Conclusion

The investigation successfully recovered a computer and a USB thumb drive potentially containing child exploitation material. The evidence gathered will be further analyzed to determine the extent of Jo's involvement in the alleged crimes. The investigation will continue to be conducted in accordance with all applicable laws and regulations, ensuring the protection of individual rights while pursuing justice in this sensitive case.

2. Are there any other suspicious activities occurring within M57?

Answer: EXPLAINED IN QUIZ 3 (Page-7)

3. A number of professional contacts and outside persons (friends of the employees) may appear in this scenario. Who are they? Are they involved in any of the activities uncovered?

Answer: The following is the professional contacts outside the organization that the employees had:

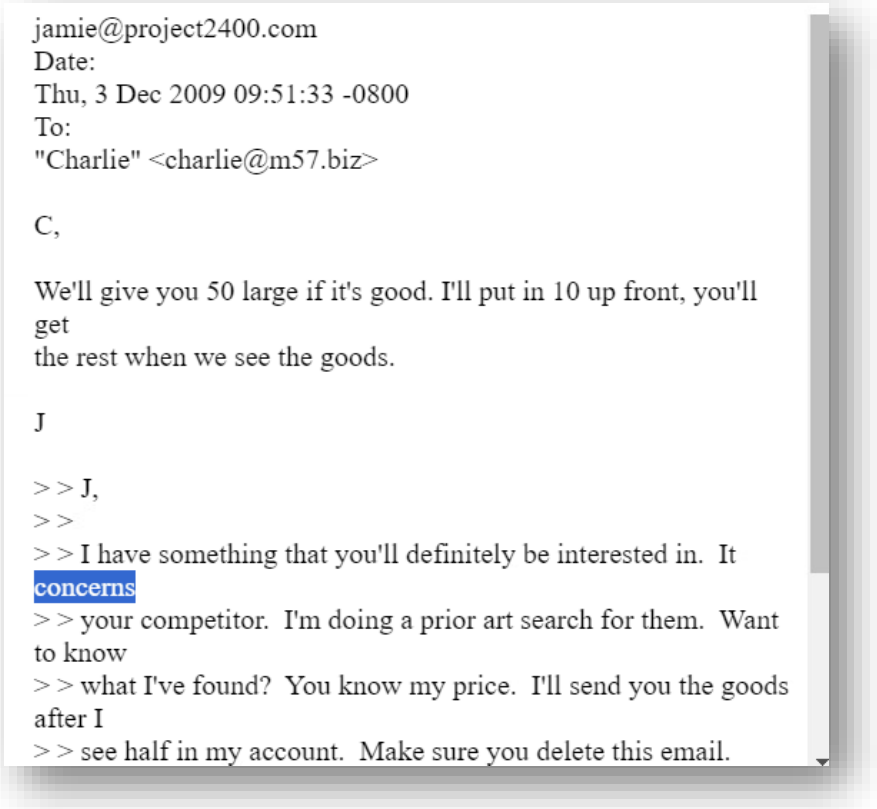
- ***Charlie Brown:***

Charlie's emails show he talked to both coworkers at M57 and people outside the company. His emails to coworkers were about normal work stuff, but his emails to people outside the company raise concerns about possible illegal activity.

While his chats with Rubin and Alix seem harmless, focusing on things like movies, dinner, cars, and vacations, his emails with Jaime and Andy are much more worrisome and suggest he might be involved in criminal activities.

Path: charlie-work-usb-2009-12-11.E01 - Partition 1 (Microsoft NTFS, 0.99 GB) charliework\Email\

i. **Rubin Fritz (rubinfritz31@mail.com):** - Discussions about movie nights, dinners, and casual topics
ii. **Alix Pery (alix.pery@yahoo.com):** - Conversations related to cars, cruises, and vacations
iii. **Jaime (jaime@project2400.com):** - Charlie claims to possess sensitive information about Jaime's competitor obtained through a prior art search



jamie@project2400.com
Date:
Thu, 3 Dec 2009 09:51:33 -0800
To:
"Charlie" <charlie@m57.biz>

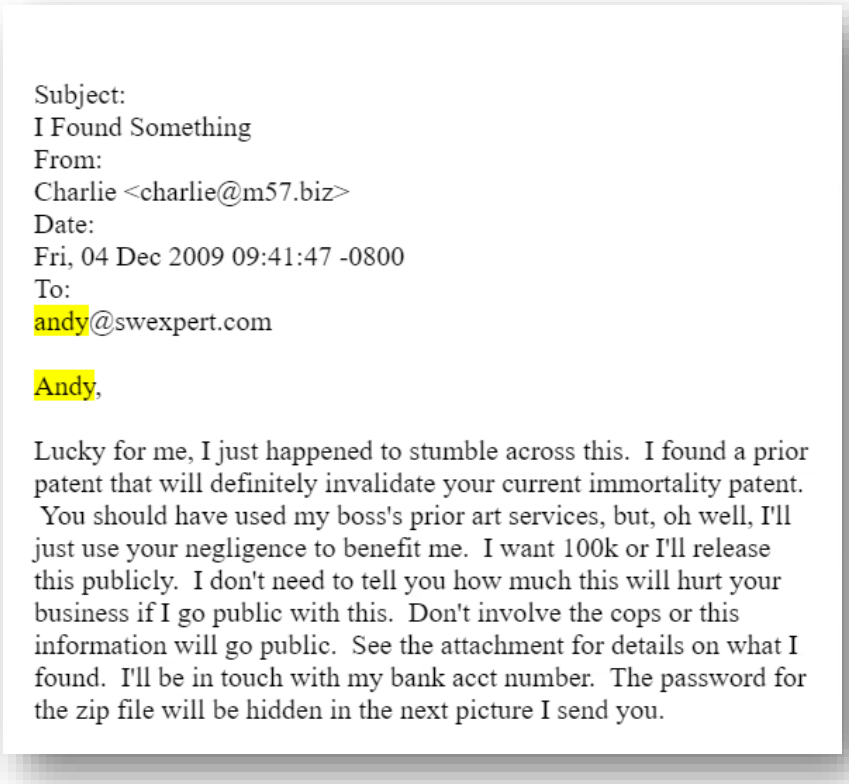
C,

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

> > J,
> >
> > I have something that you'll definitely be interested in. It concerns
> > your competitor. I'm doing a prior art search for them. Want to know
> > what I've found? You know my price. I'll send you the goods after I
> > see half in my account. Make sure you delete this email.

iv. **Andy (andy@swexpert.com):** - Charlie contacts Andy, claiming to have found a prior patent that could invalidate Andy's immortality patent



Subject:
I Found Something
From:
Charlie <charlie@m57.biz>
Date:
Fri, 04 Dec 2009 09:41:47 -0800
To:
andy@swexpert.com

Andy,

Lucky for me, I just happened to stumble across this. I found a prior patent that will definitely invalidate your current immortality patent. You should have used my boss's prior art services, but, oh well, I'll just use your negligence to benefit me. I want 100k or I'll release this publicly. I don't need to tell you how much this will hurt your business if I go public with this. Don't involve the cops or this information will go public. See the attachment for details on what I found. I'll be in touch with my bank acct number. The password for the zip file will be hidden in the next picture I send you.

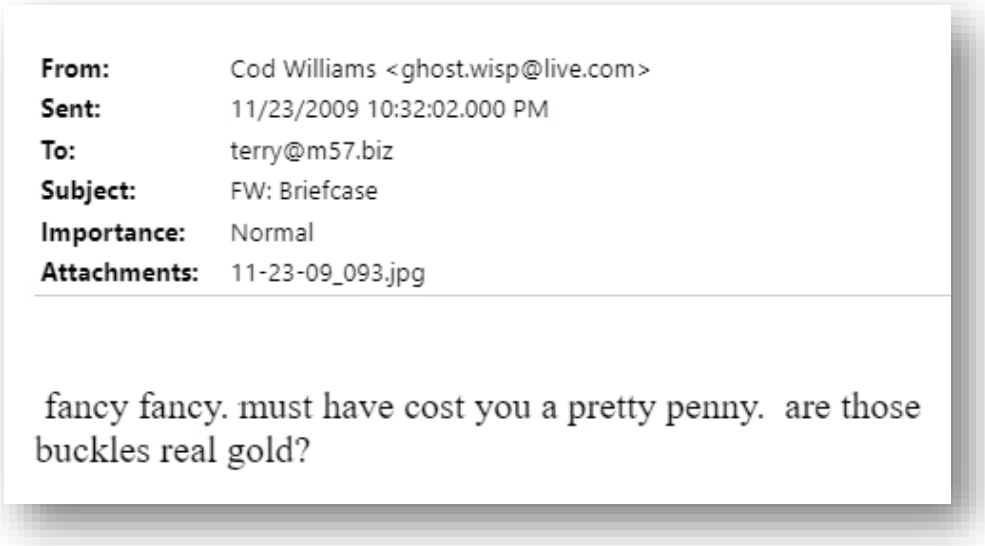
This email conversations are not directly related with the kitty images and videos but are part of illegal activities going on in the company which no one is aware of.

➢ ***Terry Johnson:***

Terry's emails show he talked to both coworkers at M57 and people outside the company. His emails to coworkers were about normal work stuff, while his emails to people outside the company were also not raising any kind of threat concerns to the company as all his chats were normal and casual.

Path: terry-2009-12-11-001.E01 - Partition 1 (Microsoft NTFS, 38.28 GB)\Users\terry\AppData\Local\Microsoft\Windows Mail\Local Folders\Sent Items\

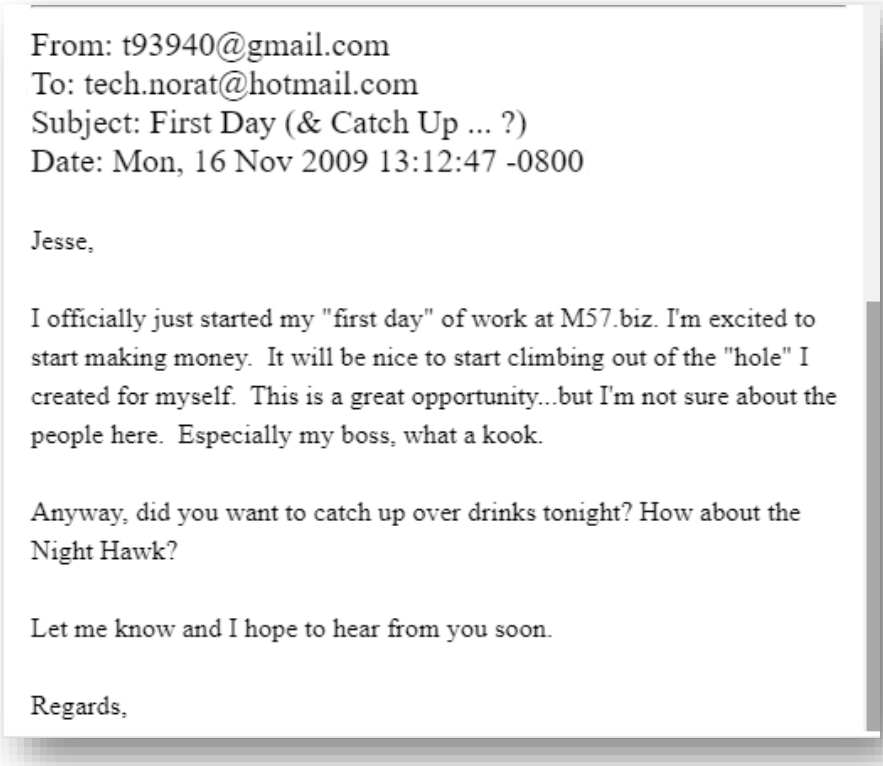
I. **Jean Sizmore (jeansizemore3@gmail.com):** Related to buying of PC posted on Craigslist
II. **Cod Williams (ghost.wisp@live.com):** Terry's friend asking for poker and games



From: Cod Williams <ghost.wisp@live.com>
Sent: 11/23/2009 10:32:02.000 PM
To: terry@m57.biz
Subject: FW: Briefcase
Importance: Normal
Attachments: 11-23-09_093.jpg

fancy fancy. must have cost you a pretty penny. are those buckles real gold?

III. tech.norat@hotmail.com**: Terry's friend**



From: t93940@gmail.com
To: tech.norat@hotmail.com
Subject: First Day (& Catch Up ... ?)
Date: Mon, 16 Nov 2009 13:12:47 -0800

Jesse,

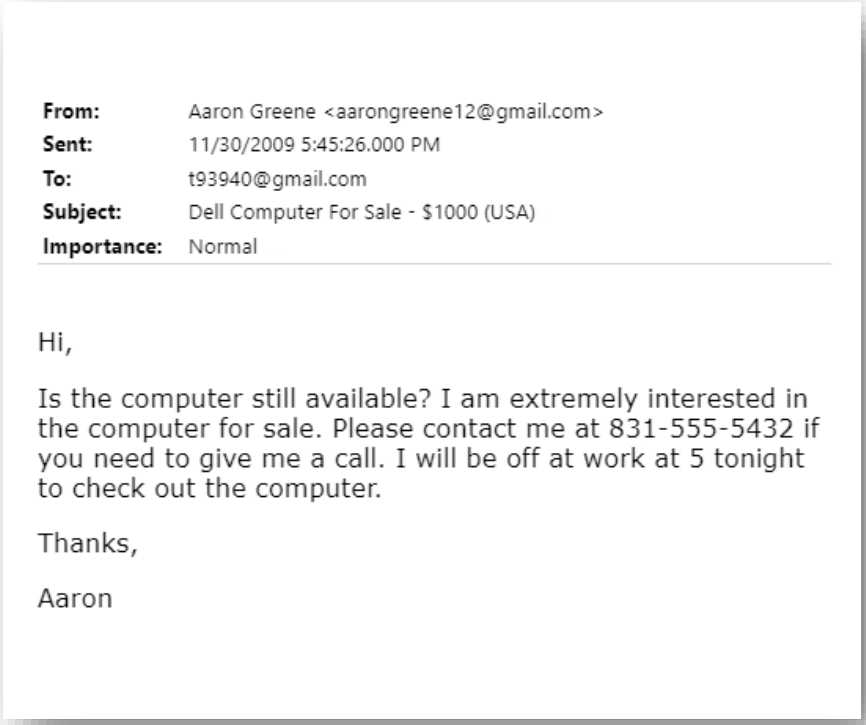
I officially just started my "first day" of work at M57.biz. I'm excited to start making money. It will be nice to start climbing out of the "hole" I created for myself. This is a great opportunity...but I'm not sure about the people here. Especially my boss, what a kook.

Anyway, did you want to catch up over drinks tonight? How about the Night Hawk?

Let me know and I hope to hear from you soon.

Regards,

IV. **Aaron Greene (aarongreene12@gmail.com):** The person who actually bought the computer from Craigslist and he is the actual person who found and reported the kitty images



From: Aaron Greene <aarongreene12@gmail.com>
Sent: 11/30/2009 5:45:26.000 PM
To: t93940@gmail.com
Subject: Dell Computer For Sale - $1000 (USA)
Importance: Normal

Hi,

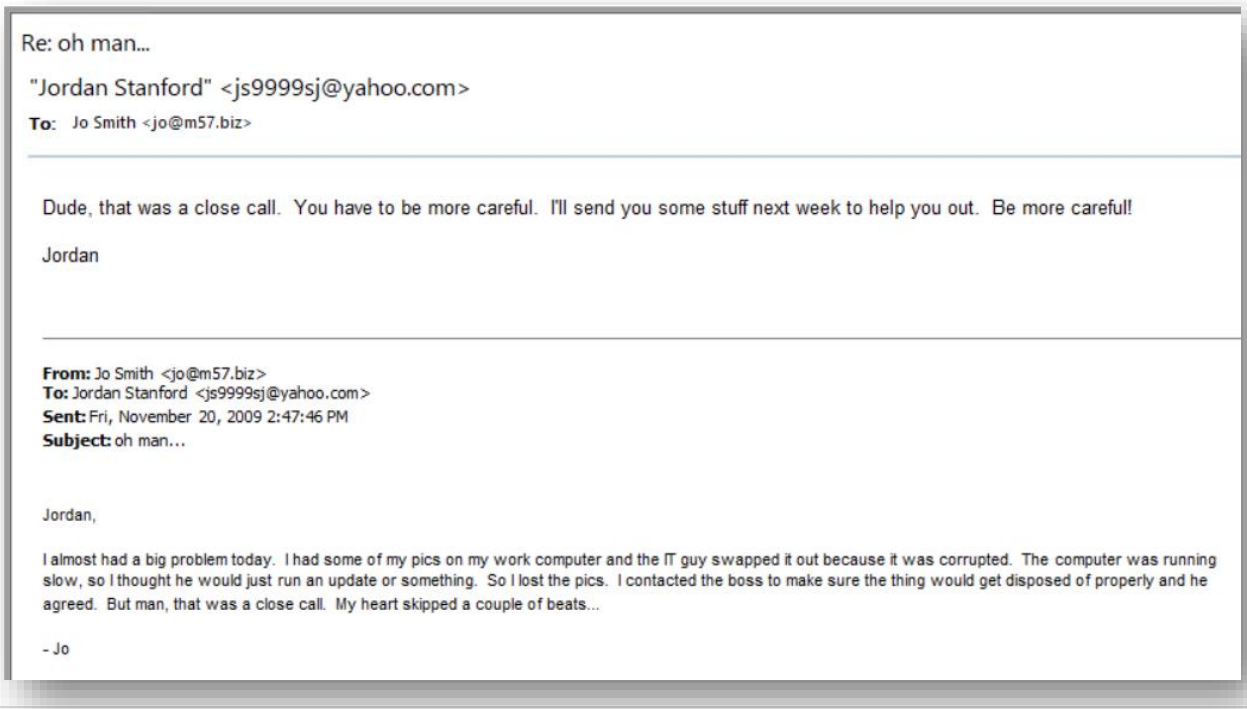
Is the computer still available? I am extremely interested in the computer for sale. Please contact me at 831-555-5432 if you need to give me a call. I will be off at work at 5 tonight to check out the computer.

Thanks,

Aaron

These are the few personalities with whom terry was in contact and out of all, Aaron was the person who is the main complainant about the images from the PC he bought, and this is where the case started.

- ***Jo Smith:*** Jo's emails show he talked to both coworkers at M57 and people outside the company. His emails to coworkers were about normal work stuff, but his he was only in contact of 1 person outside the company which raise concerns about possible illegal activity. This comes from the email database found from the new PC that Terry brought for Jo as his old PC was not working.
  - **I. Path:** e3://Kitty/Outlook Express_(1)/Outlook Express/mbx#0000000000000001:fld#0000000000000000/mbx#0000000000000001:fld#0000000000000002



Re: oh man...

"Jordan Stanford" <js9999sj@yahoo.com>
To: Jo Smith <jo@m57.biz>

Dude, that was a close call. You have to be more careful. I'll send you some stuff next week to help you out. Be more careful!

Jordan

From: Jo Smith <jo@m57.biz>
To: Jordan Stanford <js9999sj@yahoo.com>
Sent: Fri, November 20, 2009 2:47:46 PM
Subject: oh man...

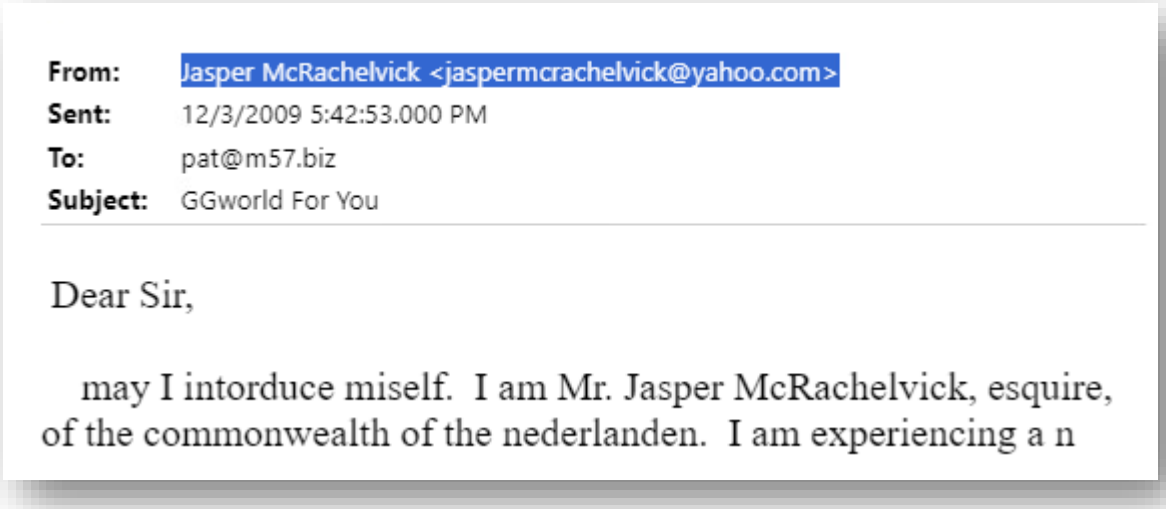
Jordan,

I almost had a big problem today. I had some of my pics on my work computer and the IT guy swapped it out because it was corrupted. The computer was running slow, so I thought he would just run an update or something. So I lost the pics. I contacted the boss to make sure the thing would get disposed of properly and he agreed. But man, that was a close call. My heart skipped a couple of beats...

- Jo

- ***Pat McGoo:*** Pat's emails show he talked to both coworkers at M57 and people outside the company. His emails to coworkers were about normal work stuff and also about having lunch and coffee, while his outside the company contacts were also related to work and had no relation to the case neither anything illegal related the M57 company. Here are some of the persons Pat was in contact with:
  - **Path:** PhysicalDrive0 VMware Virtual disk SCSI Disk Device (365 GB).zip\C\Users\student\Downloads\Pat\pat-2009-11-20.mddramimage

II. Jasper McRachelvick (jaspermcrachelvick@yahoo.com): A professional contact

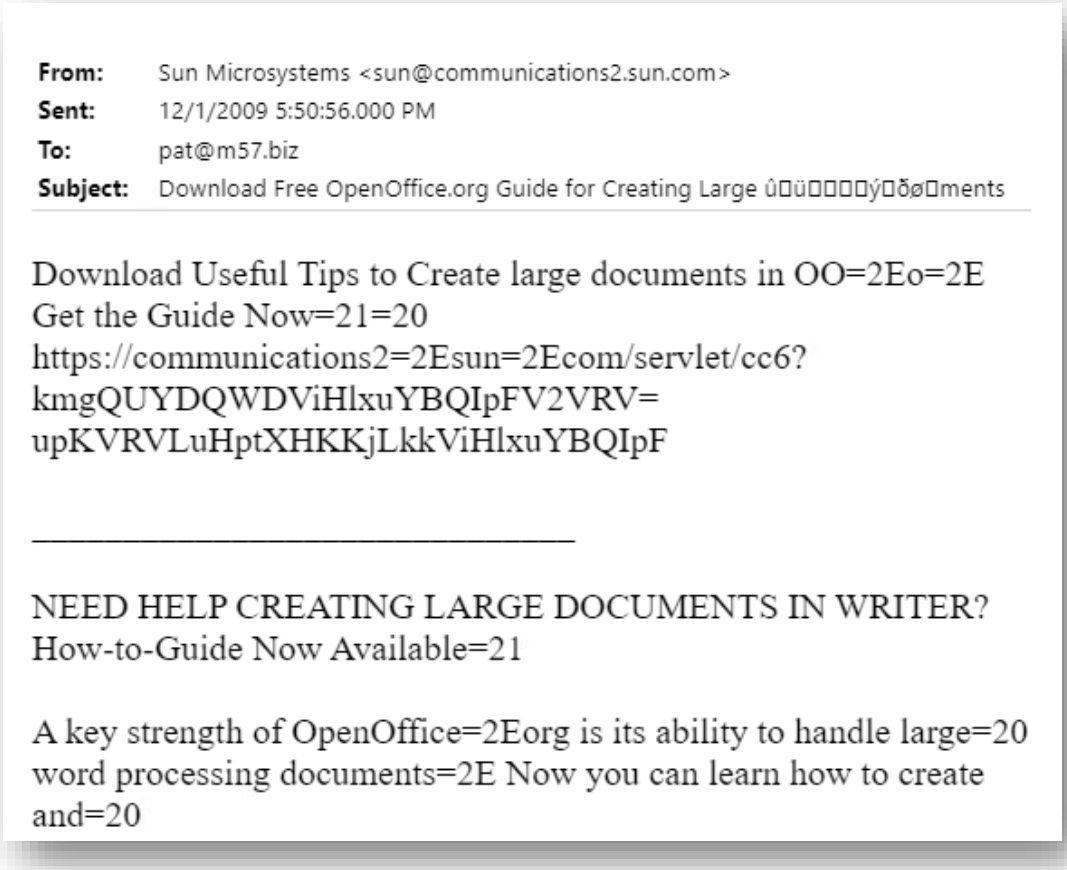


From: Jasper McRachelvick <jaspermcrachelvick@yahoo.com>
Sent: 12/3/2009 5:42:53.000 PM
To: pat@m57.biz
Subject: GGworld For You

Dear Sir,

may I intorduce miself. I am Mr. Jasper McRachelvick, esquire, of the commonwealth of the nederlanden. I am experiencing a n

III. Sun Microsystems sun@communications2.sun.com: A regular system generated email from sun microsystems.



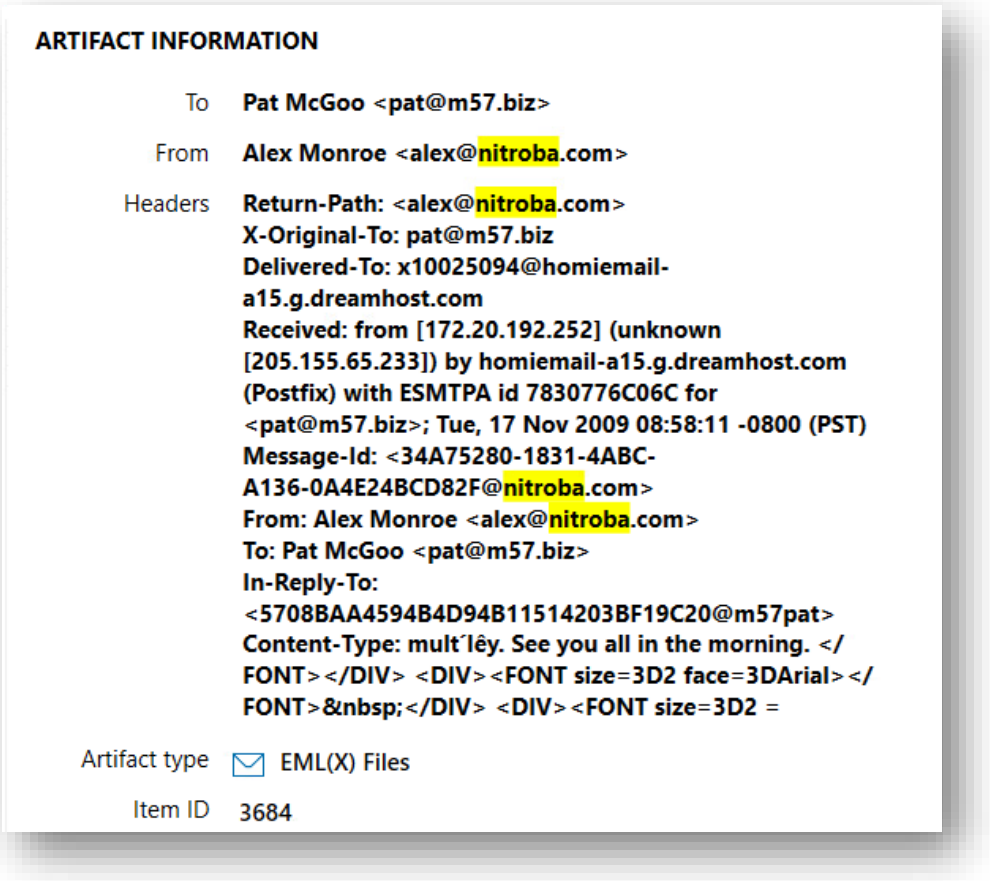
From: Sun Microsystems <sun@communications2.sun.com>
Sent: 12/1/2009 5:50:56.000 PM
To: pat@m57.biz
Subject: Download Free OpenOffice.org Guide for Creating Large û□ü□□□□ý□ðø□ments

Download Useful Tips to Create large documents in OO=2Eo=2E
Get the Guide Now=21=20
https://communications2=2Esun=2Ecom/servlet/cc6?
kmgQUYDQWDViHlxuYBQIpFV2VRV=
upKVRVLuHptXHKKjLkkViHlxuYBQIpF

NEED HELP CREATING LARGE DOCUMENTS IN WRITER?
How-to-Guide Now Available=21

A key strength of OpenOffice=2Eorg is its ability to handle large=20 word processing documents=2E Now you can learn how to create and=20

IV. Alex Monroe (alex@nitroba.com): A person from nitroba asking for patent related information

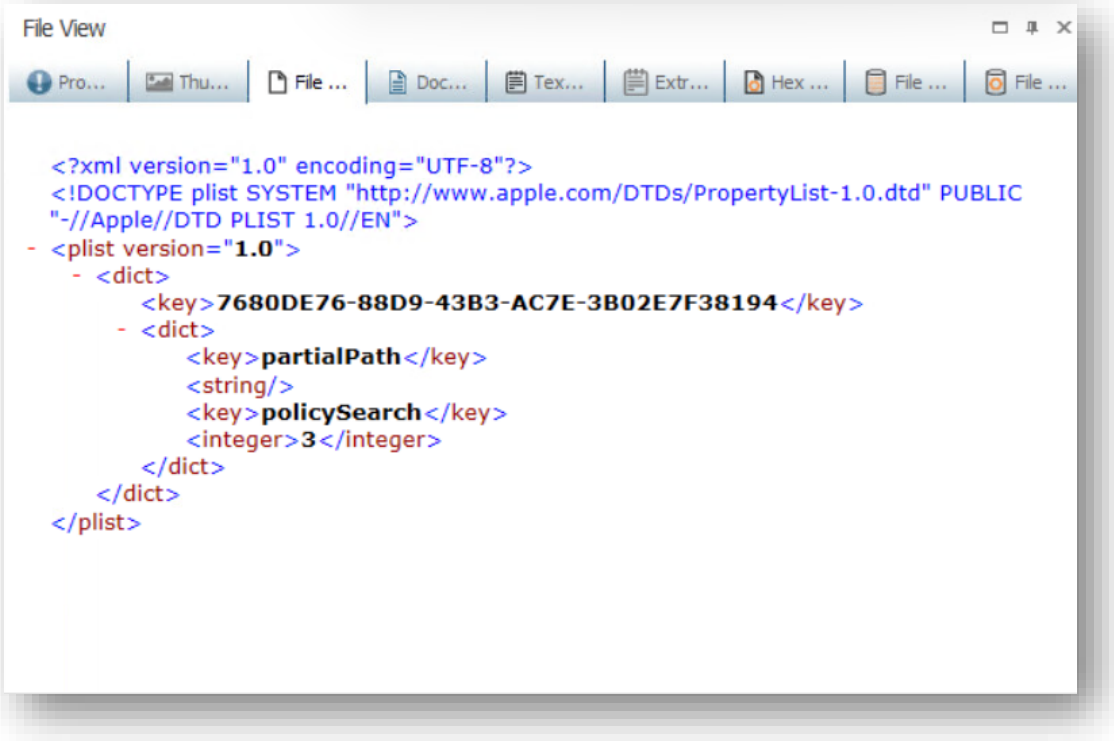


Not all the people who are in contact with everyone in the company are part of the case but some people like Jo, Jordan, Terry are directly related to storing and distribution of Kitty exploitation image, which is the actual case while others like Charlie, Jaime, Andy are involved in other criminal and illegal activities going on in the company which is not noticed by anyone.

4. Note: Terry's phone is not available in the evidence. However, several files that originated from the phone exist somewhere in the evidence. Can you find them? Are they related to the case?

Answer: Yes, there is a file available on Terry's work USB. The name of file is VolumeConfig.plist.

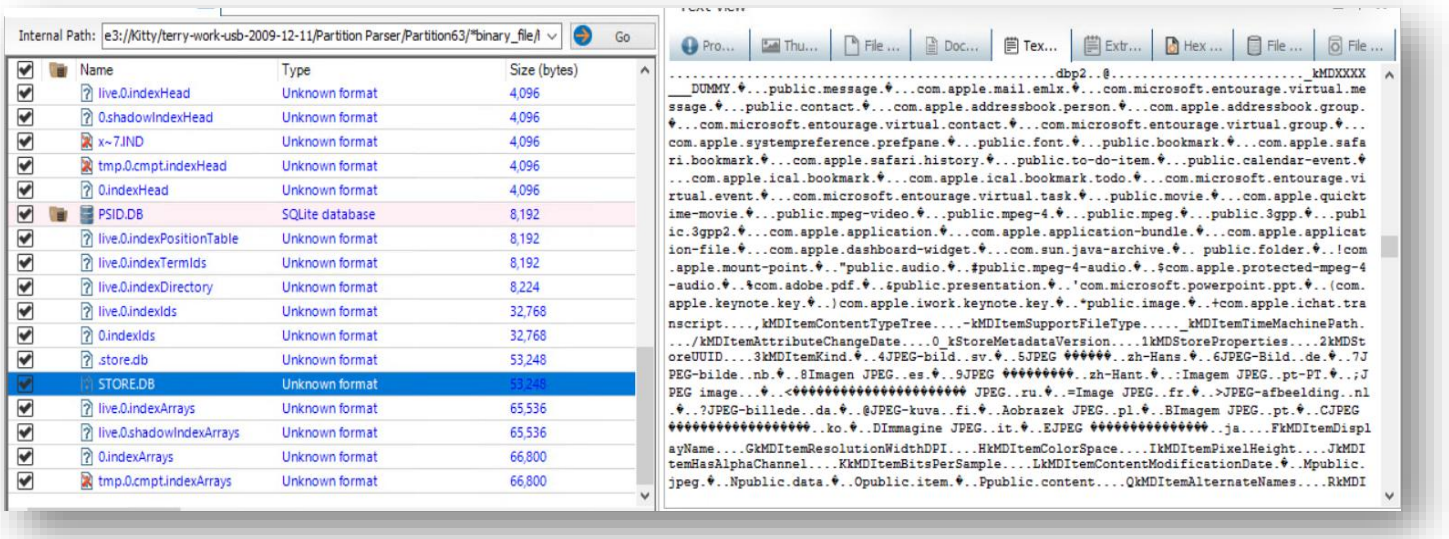
- **Path:** e3://Kitty/terry-work-usb-2009-12-11/Partition Parser/Partition63/*binary_file/FAT/Root/.Spotlight-V100_320/Store-V1_96?item=VolumeConfig.plist_128
- **Evidence:**



The first file, named "VolumeConfig.xml," exhibits the structure and characteristics of a plist (Property List) file, a format commonly used in Apple's macOS and iOS operating systems. While plist files are typically associated with Apple devices, the specific keys and values within this file suggest it might be related to a Windows feature, possibly search or indexing functionality. Further analysis is needed to determine the exact nature and origin of this file.

The second file is a database file named "stores.db." This file contains references to several Apple applications, including Mail, Safari, Address Book, and Calendar, suggesting it may be associated with application data from an Apple device.

Interestingly, both "VolumeConfig.xml" and "stores.db" share a unique identifier, linking them together. This strengthens the hypothesis that "stores.db" is connected to an Apple device, potentially Terry's iPhone.



5. Is Terry involved in anything illicit or against policy? If so, describe in detail what he did.

Answer: EXPLAINED IN QUIZ 3 (Page-3)