USC ELECTRONIC CRIMES UNIT

USC - ECU

USC Computer Forensics Laboratory

SUMMARY REPORT

Agency Requesting Examination	:	West Covina Police Department
USC-ECU File Number	:	USC006
File Number of Requesting Agency	:	USSS04-14
Investigating Agent or Detective	:	Det. Joseph Greenfield
Subject	:	Helen Honoka
Violation	:	California Penal Codes 487, 502, and 530.5
Initial Report Date	:	***22/03/2025***
Authority Under Which Electronic Media/Hard Drives were examined	:	California State Search Warrant
Investigator Examining	:	***Raina Maraqa***
Exam Credits	:	One

Exam ☒ **Preview** □ **Image** □ **Wipe** □

<u>Evidence Submitted:</u>

Helen Honoka’s Personal Machine

Evidence Number	E1
Device Name	DESKTOP-HLEC9HS
Product ID	00326-00745-52548-AAOEM
Physical Disk Size	80 GB
Acquisition MD5 Hash	350849cf78ba8541494001b29d3c75bd
Acquisition SHA1 Hash	ala9d48a446fdBee1ee25de75ebd0649d44f5dfe
Verification MD5 Hashes	350849cf78ba8541494001b29d3c75bd
Verification SHA1 Hash	ala9d48a446fdBee1ee25de75ebd0649d44f5dfe
Operating System Version	Windows 10 Home
File System	NTFS
User Accounts	Helen Honoka Ict Public Default Default User deafultuser0

Helen Honoka’s Workstation Machine

Evidence Number	E2
Device Name	FINANCE-INTERN
Product ID	00371-703-3295522-06161
Physical Disk Size	34.36 GB
Acquisition MD5 Hash	842522201464d40e8a669d1d297b8d34
Acquisition SHA1 Hash	2890e0721c5c9278c4aebc6a8998309f6f326716
Acquisition SHA256 Hash	0fa10c9ad490d00c79c072675f29e93092eadb1f5972d4a5562b3ce9cae7fc73
Verification MD5 Hashes	842522201464d40e8a669d1d297b8d34
Verification SHA1 Hash	2890e0721c5c9278c4aebc6a8998309f6f326716
Verification SHA256 Hash	0fa10c9ad490d00c79c072675f29e93092eadb1f5972d4a5562b3ce9cae7fc73
Operating System Version	Windows 7 Professional Service Pack 1
File System	NTFS
User Accounts	Admin Administrator Default Default User hhonoka Public

Isaac Augustin's Work Machine

Evidence Number	E3
Device Name	IAUGUSTIN
Product ID	00371-703-3295522-06161
Physical Disk Size	34.36 GB
Acquisition MD5 Hash	e1848f098849446f0c9fcbe1224568c2
Acquisition SHA1 Hash	2208cb7afc1f60fa54f9002c4c0245b6d60525fa
Acquisition SHA256	223f655306f3075a981992051bf36db95ad6319eb1ca4cbeadddf804f98210ba
Verification MD5 Hashes	e1848f098849446f0c9fcbe1224568c2
Verification SHA1 Hash	2208cb7afc1f60fa54f9002c4c0245b6d60525fa
Verification SHA256	223f655306f3075a981992051bf36db95ad6319eb1ca4cbeadddf804f98210ba
Operating System Version	Windows 7 Professional Service Pack 1
File System	NTFS
User Accounts	Admin Administrator Default Default User IAugustin klibby Public

Requested Examination:

This forensic examination was conducted based on the search warrant and affidavit issued by the State of California, County of Los Angeles. The affiant is peace officer Joseph Greenfield this search warrant was issued based on the probable cause that the affiant does believe that the articles, property, and persons described are lawfully seizable under Penal Code Section 1524 that states that property was stolen or embezzled, property or things were used as the means of committing a felony and property or things to be seized consist of any item or constitute any evidence that tends to show a felony has been committed, or tends to show that a particular person has committed a felony.

The search warrant calls for the search of the premises of The Legacy at Westwood Apartments, Apartment # 13, 10833 Wilshire Blvd. Any person(s) located on the search warrant premises; Any safe or locked device; and any cell phone(s) possessed and/or controlled by the PRIMARY persons to be searched during this warrant. The primary person to be detained and searched is Helen Honoka, an Asian female born on 11/09/1993. Helen has black hair, weighs 118 pounds, has black eyes, and is 5'5 feet tall. The following property will be searched and seized: Dominion control, financial transactions, computer and electronic media, cell phone data, and other data about Helen Honoka between January 13, 2017, and February 20, 2017.

The probable cause of this investigation was based on facts in the official West Covina Police Department reports documented under case # 21-9596. It stated that on February 2nd, 2017, representatives from the Intelligent Sheep Defense Corporation reached out to the West Covina Police Department about the possibility of a network intrusion and computer hacking occurrence done by one of their employees, Helen Honoka, on the victim, Isaac Augustin. A forensic analysis of Isaac Augustin's work system and event logs showed a remote desktop connection established on his system by Helen Honoka's work machine at 10:50 PM on January 13th, 2017. With this connection established, files were transferred from Isaac's Machine to Helen Honoka's machine. Then, on February 8th, 2017, an informant told the affiant that they had evidence of an individual with the online name "sinongal1993" posting on dark web message boards regarding obtaining stolen and classified intellectual property and that they were looking to sell it. The informant conversed with "sinongal1993" to seek their proof of possession. They received two samples, and the Intelligent Sheep Defense Corporation representatives verified these samples as documents that could have only been taken from their classified projects file server.

Helen Honoka's is a Sinonian national born in 1993, with the stolen material by "sinongal1993" and the forensic analysis by the Intelligent Sheep Defense Corporation showing the unauthorized access by Helen Honoka's work system to a work system with access to a classified projects fileserver, the probable cause calls for search Helen Honoka's apartment and all electronic devices located in the premises. This is because the search can confirm her possession of classified and stolen material. This forensic analysis will seek evidence of her intentions to sell these materials and confirm if these materials were sold. This search will also confirm other individuals involved, such as buyers and online communication regarding the stolen data.

Review Process:

- The Intelligent Sheep Defense Corporation conducted the assessment of the forensic analysis by proving the unauthorized access of Helen Honoka's work system to a work system with access to a classified project's file server.

- The evidence was acquired by getting a mirror image of Helen Honoka's personal computer, Mr. Augustin's workstation OVA file, which had its VMDK file extracted from it, and Helen Honoka's workstation OVA file, which had its VMDK file extracted from it.

- The authentication of the computer images was done by recording the SHA1 and MD5 hash of all three machines that were generated by the autopsy ingest module for data integrity. An additional SHA256 hash was also computed for both work machines.

- The machines were analyzed using Autopsy, a forensic tool for investigating computer images, and Kape, a forensic tool for extracting relevant digital artifacts from computer machines.

- The evidence was articulated by creating a master timeline of all three machines that correlates computer events and processes in a timeline order.

- The evidence will be archived for three years, giving enough time for it to be accessed throughout court proceedings. This time allows for the data's integrity to remain intact due to the life spans of hard drives lasting up to three years after they need to be moved to another hard drive.

Results of Analysis:

Email Communications

The investigation began by analyzing email communications on all three machines provided. Isaac Augustin's machine was first inspected and showed that the first time he and Helen Honoka were in contact was on 2016-12-30 at 16:34:00 UTC when Honoka emailed Augustin introducing herself as an intern in the finance department, asking Augustin to have a chat regarding the project managers under his department (E16). On 2017-01-03 at 13:32:00 UTC, Issac Augustin emailed Helen Honoka, telling her he had a great time with her last night and apologized for being unable to inform her more about the project since it is classified. He jokes about being unable to tell her unless she pays a million dollars (E20). Then, on 2017-01-03 at 14:02:00 UTC, Issac Agustin emailed Helen Honoka, asking her to get a drink later that day. Email communication on Helen Honoka's workstation showed that on 2017-01-05 at 15:58:00, she emailed Issac Agustin, telling him they needed a round two for drinks and that she would text him shortly (E21).

Helen Honoka's personal machine email communication was parsed. Helen received an email on 2016-12-12 at 10:58:54 UTC from hd12fa@gmail.com asking her if she received a package (E1). Helen responded that same day at 11:04:40 UTC that she received the package; she thanked them for the computer and everything else and told them everything was going according to plan and that she would keep them updated(E8). The next day, on 2016-12-13, at 06:49:40 UTC, she informed the same user she found more information and would need some from him (E9). It showed that she sent out an email from her account named sinongal1993@gmail.com on 2017-01-06 07:09:55 UTC to the following email, hd12fa@gmail.com, saying she has spent the last week getting to know a specific employee. She also said she is probably spending the night with them, using a burner, and thanked them for their advice (E2). This email was sent a day after she asked Issac Augustin for round two drinks on her work email. hd12fa@gmail.com responds to her, saying he hopes that by her saying she's spending the night, she's at the place he thinks she is and that they will talk once she has something for him (E3). Helen then emailed the same user on 2017-01-13 at 02:00:17 UTC, saying that she had no information since she was having connectivity issues, but her target just texted her that everything was up and running again (E10).

On 2017-02-07, at 08:13:52 UTC, Helen received an email from another user (skjdl1ljlkj@gmail.com) that they heard from a friend that she was interested in selling and included their Skype user (E4). That same day, on 2017-02-07 at 09:47:11 UTC, the user she emailed first, hd12fa@gmail.com, sends Helen an email saying they thought she had ghosted them, but it is good to know she is sticking to the deal; they proceed to thank her for the samples and tell her they have been verified and asks how she plans on sending them (E5).On 2017-02-07 at 09:50:30 UTC, Helen emailed the same user, saying she had a buyer willing to pay more (E12). Ten minutes later, the same user emails Helen at 09:59:23 UTC, telling her not to be ridiculous, to honor the deal, or face the consequences, and that she doesn't know who she is dealing with and should honor her patriotism (E6). On 2017-02-07 at 10:43:16 UTC, Helen responded to the user by saying that she figured out who she was dealing with and if the initials RM sounded familiar (E13). On 2017-02-07 at 2:06:18 UTC, the user said they would beat the offer by 15% but wanted it by tomorrow and to meet with the data in hand at 4 pm in the same meeting spot (E7). On 2017-02-07 at 04:26:58 UTC, Helen emailed the same user, saying she had been lying low for a while since she believed she was being followed, but could also be paranoid. She says she has data to sell if he is still interested in buying (E11).

Web History

Helen Honoka's personal machine web search history was analyzed, and searches to notable websites were found. She accessed an instructions website for "A Few Ways To Hide Data On A Computer" (W1), "What is the difference between a file share and a folder" (W4), "How To Open an Offshore Bank Account In The Cayman Islands" (W14), "How Money Laundering Works" (W15). She also accessed a Freeware Hex Editor and Disk Editor (W2) that allows data to be edited at the hex level. She also searched for cat pictures. After that, she did a search for "Hackers hide stolen payment card data inside website product images" and "How much can I sell data for." (W7). She also accessed 7-Zip's website, which is a program used to compress archived data (W8), and a program named Eraser, "Erase Files from Hard Drives" (W10). She also accessed the Pirate Bay website (W11), which is used for file and program sharing and downloading; after accessing it, she searched for file eraser executables (W12 & W13). She also accessed a PGP encryption tool website (W16), which is used to encrypt and decrypt data to secure data and communications. She also accessed a website for Steganography by Open Puff (W17), a program that allows the user to hide data inside regular files like text files or images. She also made two searches regarding the process of creating a hidden partition and encrypting a hard drive (W19 & W20), which is a process that makes a section of the computer inaccessible to the operating system file explorer.

Remote Desktop Access

The Windows Event Logs of Isaac Augustin's work machine were inspected. These logs are generated by the Windows operating system and record events on the system. They log events regarding any occurrences with the system, its security, and its applications. Isaac Augustin's work machine showed the following Windows event logs for a remote desktop connection. The event ID 25 for event record ID 57 means that this remote desktop had occurred before and was reconnected, meaning the remote host had already connected to this machine.

Event Record Id	Time Created	Event id	Process id	Computer	Map Description	Username	Remote Host	Source File
57	1/14/2017 6:50:09 UTC	25	552	IAugustin.isdc.local	Remote Desktop Services: Session reconnection succeeded	ISDC\iaugustin	10.10.10.86	C:\Windows\System32\winevt\logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
58	1/14/2017 6:51:46 UTC	24	552	IAugustin.isdc.local	Remote Desktop Services: Session has been disconnected	ISDC\iaugustin	10.10.10.86	C:\Windows\System32\winevt\logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

Remote desktop connections allow the remote host to execute these connections to control and access the computer from a different location. The remote host's IP address, a number with a unique value assigned to a computer network for this connection, is "10.10.10.86". Helen Honoka's work machine registry was inspected, a Windows database that stores the operating system data, including the machine's IP address. The IP address stored in the registry of her work machine was the same as the remote host, which is "10.10.10.86". This means that on 1/14/2017 at 6:50:09 AM, Helen Honoka successfully reconnected a remote desktop connection to Isaac Augustin's work machine. This connection was disconnected almost a minute later on the same day at 6:51:46 AM.

Skype

Helen Honoka’s personal machine had Skype. Her Skype folder was located in her roaming folder within her AppData folder. Inside the Skype folder was another folder named “live#3asinongal1993” with a main.db file inside. The Skype application generates the main.db file for users and stores all of the app data, including calls, chats, and accounts associated with the Skype application on the machine.

The db file contained notable chats between Helen Honoka, who uses the username sinongal1993 on Skype, and skjdl1ljlkj. On 2017-02-07 at 08:17:10 UTC, sinongal1993 received a request from skjdl1ljlkj to add them to Skype. This was the conversation between them on Skype; the same person emailed Helen Honoka on her personal machine on 2017-02-07 at 08:13:52 UTC (E4), asking her if she was selling minutes before they started chatting on Skype

Date & Time	Sender	Receiver	Message or Event
2017-02-07 08:17:10 UTC	skjdl1ljlkj	sinongal1993	Hi skjdl ljlkj, I&apos;d like to add you as a contact
2017-02-07 08:18:44 UTC	sinongal1993	skjdl1ljlkj	who told you about the sale
2017-02-07 08:19:08 UTC	skjdl1ljlkj	sinongal1993	Doesn&apos;t matter
2017-02-07 08:19:39 UTC	skjdl1ljlkj	sinongal1993	But it sounds like you&apos;re in business
2017-02-07 08:19:49 UTC	skjdl1ljlkj	sinongal1994	And I might have an offer
2017-02-07 08:20:11 UTC	sinongal1994	skjdl1ljlkj	my business depends on your offer
2017-02-07 08:21:30 UTC	skjdl1ljlkj	sinongal1994	Il double the other buyers offer
2017-02-07 08:22:13 UTC	sinongal1994	skjdl1ljlkj	oh yeah? i&apos;ll need an advance, if you plan on doing that
2017-02-07 08:23:14 UTC	skjdl1ljlkj	sinongal1994	And I&apos;ll need an advance on the data
2017-02-07 08:25:38 UTC	sinongal1994	skjdl1ljlkj	attachment: "sample.txt" FileSize v="51476"
2017-02-07 08:25:38 UTC	sinongal1994	skjdl1ljlkj	attachment: "sample1.txt" FileSize v="13164"
2017-02-07 08:26:24 UTC	sinongal1994	skjdl1ljlkj	Helen calls user for 133 seconds
2017-02-07 08:27:16 UTC	skjdl1ljlkj	sinongal1994	okay fine.
2017-02-07 08:29:32 UTC	skjdl1ljlkj	sinongal1994	Will wire the agreed upon amount once the data has been received.
2017-02-07 08:29:45 UTC	sinongal1994	skjdl1ljlkj	deal. i&apos;ll be in touch

7-Zip

Helen Honoka downloaded an executable “7-Zip 16.04” on her personal machine on 2/7/2017 at 3:37:02 UTC. 7-Zip is a program that allows users to extract and archive files by compressing their size. This program was first run on her machine after downloading it on 2/7/2017 at 3:50:59 UTC. Inside Helen Honoka’s system 32 file, which is a file only for Windows system files, she had a folder named data, and inside it was another folder named “TS_DIAGRAMS” which was created on 2017-02-07 at 03:50:59 UTC. Inside this folder were two zipped files named MISSILES.7z, which were accessed by Helen on 2017-02-07 at 03:56:18 UTC, but last modified on 2017-01-03 at 01:08:31 UTC. Another zipped file named ROACHES.7z was accessed by Helen on 2017-02-07 at 03:56:18 UTC but was last modified on 2017-01-03 at 01:09:34 UTC.

Since these files were modified before being accessed on Helen’s machine, Augustin’s machine was inspected and found to have a zipped folder named “TS_DIAGRAMS.7Z” created on 2017-01-03. This file was extracted and unzipped using 7-Zip. The folder was password protected, and on Augustin’s desktop, he had a file named “Desktop.ini.jpg” that contained the text content of three passwords, which were 1sDcPWD1, 1sDCPWD2, and Rand0mPswD!. The “TS_DIAGRAMS.7Z” folder was extracted using 7-Zip, and the folder was opened with one of the passwords in the JPG on his desktop, “Rand0mPswD!”. This contained a zipped file named “MISSILES.7z” which was password protected and opened with the first password in the JPG, “1sDcPWD1”. This zipped file contained two JPG images, which were TS_DESIGN_1.jpg & TS_DESIGN_2.jpg (Refer to S1 & S2). The next zipped file inside “TS_DIAGRAMS.7Z” was named “ROACHES.7z” and was also password protected and used the second password in the JPG, but the password had to be modified to a lowercase c like the first password for it to unzip the file “1sDcPWD2”. This file was opened to two JPG images named TS_DESIGN_3.jpg & TS_DESIGN_4.jpg (Refer to S3&S4).

After the passwords for “MISSILES.7z” and “ROACHES.7z” were obtained, these folders were also extracted from Helen’s machines and had their passwords inputted. They also contained the same JPG images, TS_DESIGN_1.jpg, TS_DESIGN_2.jpg, TS_DESIGN_3.jpg, and TS_DESIGN_4.jpg (Refer to S1-4). Since the zipped files contained the same content as the ones on Augustin’s machine and had the same modified date of 2017-01-03, which was when these files were created on Augustin’s machine, it shows that Helen likely copied these files from his machine to hers since the modified timestamp always represents when the metadata of files was last modified in their original location.

VeraCrypt

On Helen Honoka's personal machine, she had a downloaded executable named VeraCrypt on 2/7/2017 at 11:48:46 UTC, a software used for encryption. It allows users to encrypt volumes and partitions on their computers. Helen Honoka's personal machine desktop had a file encrypted by VeraCrypt named "sensitive_vc" that was created on 2017-02-07 at 20:51:31 UTC. This file was mounted and decrypted using VeraCrypt. The file was password protected using PGP encryption, a data encryption program that encrypts data using a public and private key, and the only way for the data to be decrypted is if the receiver has the private key. The password for "sensitive.vc" was decrypted using a PGP decryptor program that required the private PGP key, which was saved as a "pgpkey.dll" in Helen's system32 folder, which is only for Windows system files. This file was created on 2017-02-07 11:22:16 UTC and included the private key (Refer to J1 for the private key). This file also contained the passphrase to decrypt the password, "berlioz". The PGP message, which was the password for "sensitive_vc," was saved inside a text file on Helen's desktop named "passwords.txt" that was created on 2017-02-07 at 11:26:09 UTC (Refer to J2). The PGP decryptor outputted the following passwords: duchess, toulouse, napoleon, lafayette, roquefort.

Once this file was mounted on VeraCrypt and the password "duchess" was inputted, it opened a folder named catpics containing 187 images of cats. It is important to know that on Helen's desktop, she also has a folder named catpics, but all the images inside it were unallocated, all these images became unallocated according to their change time, which started on 2017-02-07 at 21:15:16 UTC which is approximately thirty minutes after the VeraCrypt file "senstive_vc" was created.

One of the images, named "5769.jpg," had a file signature mismatch; the file extension, which determines what a file should open as, was edited through its hex and opened a Word document with the title "Project Memo" (refer to S5). Another JPG file was found to have a signature mismatch named "4758.jpg"; it was opened in Notepad and contained the following text: "1sDcPWD1 1sDCPWD2 Rand0mPswD!". Which are the same passwords saved on Augustin's work machine desktop folder.

Inside the catpics folder was a zipped file named "ts_data.7z." This file was zipped using the program she installed earlier, 7-Zip. It opened with one of the PGP encrypted passwords, which was "toulouse". This file was unzipped inside another folder in catpics named "ts_data". The folder inside of "ts_data" was password protected for a folder named "TS_DIAGRAMS." It was opened using the passwords hidden inside "4758.jpg," specifically using the password "Rand0mPswD!". After that folder was unzipped, it stored two password-protected folders, one named "MISSILES" which was opened using the following password "1sDcPWD1" that was also stored in "5769.jpg". Once this file was opened, it contained two JPG images named "TS_DESIGN_1.jpg" and "TS_DESIGN_2.jpg" (refer to S1 & S2). The next folder inside of "TS_DIAGRAMS" was named "ROACHES" and was opened using the following password "1sDcPWD2" that was also stored in "5769.jpg". The original password in "4758.jpg" which was "1sDCPWD2" did not work due to the possibility of a typo since it opened was it was edited like the first password using a lower-case letter c which is why the password “1sDcPWD2” worked to open the “ROACHES” folder which contained two JPG images named “TS_DESIGN_3.jpg” and “TS_DESIGN_4.jpg” (refer to S3&S4).

Aside from the two folders named “ROACHES” and “MISSILES” inside the unzipped “TS_DIAGRAMS,” this folder also contained the two .txt files of the stolen samples included in the warrant, sample.txt and sample1.txt (Refer to S8 & S9). Since they were saved as text files, both file extensions were changed to JPG files, and they opened as the stolen content samples were shown in the warrant.

It is important to note that sample.txt and sample1.txt, which Helen shared via Skype with Skype user “skjdl1ljlkj,” have the same file size as sample.txt, 51KB, and sample1.tx, 13KB. This shows that the stolen samples being sent on Skype are likely the same ones in the warrant due to their size and name.

It is also important to note that the image “5769.jpg,” which opened a Word document titled project memo (S5), was also found on Augustin’s machine as a docx file named “PROJECT_MEMO.docx” that contained the same content. This docx was created from Augustin’s machine on 2016-12-13 at 06:13:19 UTC, which is before the creation time of the VeraCrypt file that it was stored in on Helen’s machine, which was on 2017-02-07 at 20:51:31 UTC.

OpenPuff

Helen Honoka’s jump lists on her personal machine were inspected. Jump lists are data artifacts generated by Windows that record the user’s usage of files or applications on their system by recording the path of the file or application and the times they were created, modified, and accessed. While observing the jump lists, it was noted on 2/7/2017 that Helen had created images on her system inside the sensitive_vc file, such as “1012. JPG, search.jpg, 3811.jpg” (refer to P3, P4, P10). These images were inspected inside the decrypted sensitive_vc file, and the “1012. JPG” image was opened. “1012. JPG” was a screenshot of Helen Honoka’s desktop with a program named “OpenPuff v4.00 – Data Hiding” open with an image mounted on it named “search.jpg,” which is the same one inside the catpics folder in the sensitive_vc file. The mounted image had a target associated with the path: “Helen Honoka\Desktop\critical.txt” (Refer to S10).

The jump list shows that the zip file for this program was created on her machine that same day on 2/7/2017 at 11:55:50 UTC (Refer to P5). This program was run on her machine on the same day on 2/7/2017 at 12:15:50 PM. Open Puff is a steganography tool used to hide data inside other files. It uses cryptography, which involves passwords to secure the file hidden inside other files, meaning files can be hidden in any other file, like an image, video, or audio file.

Referring back to the “1012. JPG” image, that means Helen was using OpenPuff to target hiding a file on her desktop named “critical.txt” inside of the mounted image, which was “search.jpg.”. The screenshot also showed that she had inputted a 16-character password for the “critical.txt” hidden in “search.jpg.”. Since “3811.jpg” was also created on her system on the same day (refer to P10), it was inspected, although it was a JPG file, it was opened in Notepad and outputted a 16-character phrase which was “balthAzar_rulez!”.

Helen Honoka’s personal machine was mounted on Arsenal Image Mounter, a program that mounts disk images and allows users to access the machine’s data. Once it was mounted, the version of OpenPuff that she had in her downloads was opened, the unhide feature was selected, and the image inside of cat pics “search.jpg” was mounted on OpenPuff and the 16-character password inside of “3811.jpg” was inputted to unhide the content inside the image which extracted a file named “crtical.txt” (Refer to S7). This file contains the location of the meeting spot discussed in (E7) when Helen Honoka was exchanging emails with hd12fa@gmail.com regarding selling the confidential data. It also contained the possible real name of the user hd12fa@gmail.com that was buying the data from her, which is Ratomir Minato, since the document said “John Smith", hd12fa@gmail.com, likely a Sinoniastan LA consulate general employee, Ratomir Minato.”

Helen Honoka’s Personal Machine Downloads

When Helen Honoka’s personal machine’s app data was being inspected, it was noted she had a folder in her roaming app data folder named “uTorrent.” Within this folder was an executable named “uTorrent.exe” created on her machine on 2017-02-07 at 06:26:12 UTC." “uTorrent.exe” is a program that allows for file downloading and sharing based on a peer-to-peer protocol, where files are downloaded from other peers who have the file across the network. After that, Helen’s downloaded folder was inspected and included a torrent file named:

“OpenPuff_v400_Steganography_Watermarking.torrent”

A torrent file does not have the actual program; it is a bencoded dictionary that tells the uTorrent program how to download the torrent-associated file. The torrent file was input into a BEncode editor, which formats the information of the torrent file, such as its associated file, the file size, and its piece length, which is the size of the chunks the data is downloaded with. The torrent in her downloads was associated with the following file: “OpenPuffv400.zip”, which is the program Helen ran for steganography to hide files within the JPG images in “sestive_vc”.

To confirm that the associated program “OpenPuffv400.zip” came from the torrent file in her downloads, the “OpenPuffv400.zip” had five SHA1 hashes generated, which give a unique identifier to the chunks of data based on the pieces’ length that the Bencoder outputted, which was 65,536. After they were generated, the SHA1 hashes were inspected to see if they matched the hashes inside the torrent file in her downloads folder, and they all did, confirming the program was downloaded from the torrent file using the uTorrent program.

Piece Number	Offset	SHA-1 Hash	Status
1	0 – 65535	ba43e27fca6b9c818794ab45451cccd01ebbfb22	Match
2	65536 – 131071	68c52b2f902388d020531de022e6aab537d8bd7e	Match
3	131072 – 196607	55fd9e08e482dfc79439bd4766af2dea4f96f9f4	Match
4	196608 – 262143	e902924f091d666e2426dee7dac3e2364b04e64f	Match
5	262144 – 327679	9d5c46af3cd16e4b3f70ddfefd59df0d29a1f1c2	Match

In Helen’s downloads, she also had two other torrent files, “Eraser6092343 - ThePirateBay.TO.torrent” created on her machine on 2017-02-07 at 06:31:37 UTC. Also, “EraserfileShredder6.0.10.2620 - ThePirateBay.TO.torrent” was created on her machine on 2017-02-07 at 06:27:58 UTC, which is a torrent for file erasing tools that erase data on machines by overwriting the data on the hard drive several times in different patterns to make the data unrecoverable. She also had an eraser executable program named “Eraser 6.0.10.2620.exe” run on her machine multiple times, the first time being on 2/7/2017 at 7:15:41 UTC. She also had another executable program in her downloads named “Frhed-1.7.1-Setup.exe,” a binary file editor program that allows files to be edited at the byte level, which controls the file's contents. This executable was run on 12/13/2016 at 6:43:25 AM, but following that, its actual executable program, not the setup one, which is named “FRHED.EXE”, was run on her machines eleven times on 2/7/2017, and the last time it ran was on 2/7/2017 at 12:14:35 UTC. She also had a folder in her downloads named “RDPWrap-v1.6.1” containing two executable programs, “RDPCHECK.EXE”, which was run once on her machine on 1/13/2017 at 1:13:42 UTC. The other program was “RDPWINST.EXE,” which was run twice on her computer on 1/13/2017 1:13:04 UTC. These executables help with remote desktop connections by simultaneously allowing multiple connections to a device and initiating unauthorized remote desktop connections. It is important to note that these were run the day before Isaac had a remote desktop connection from Helen’s work machine IP address on 2017/01/14 at 06:50:09 UTC. It is also important to note that when both these executables were run on Helen’s machine, starting on 1/13/2017 at 1:13:04 UTC, Issac’s work machine event logs show that around 30 minutes later, he had two Microsoft Windows Winlogon events that occurred on 1/13/2017 at 1:56:45 AM & 1:56:46 AM.

USB

Helen Honoka’s USBSTOR folder, which is located within the Windows system files and stores information about USB devices inserted into the machine, was inspected on her personal machine. The USBSTOR folder showed that Helen mounted a device named “VID_058F&PID_6387” with the following ID “83E67C3E” on 2/7/2017 at 09:53:10 UTC. This was the same day that OpenPuff, VeraCrypt & 7-zip were run on Helen’s personal machine. It was also the same day that Helen communicated with the Skype user regarding selling the data, and the same day “sensitive_vc” was created on her personal machine.

Appendix:

Timeline of Events

Event	Date and Time	Path	Machine
r	2016-12-12 10:58:54 UTC	C:\Users\Helen Honoka\AppData\Roaming\Thunderbird\Profiles\a03oocdt.default\Mail\pop.gmail.com\Inbox	Helen Personal Machine
creation time of PROJECT_MEMO.docx on Augustin's Machine	2016-12-13 06:13:19 UTC	C:\Windows\CSC\v2.0.6\namespace\isfs.isdc.local/rnd-class\PROJECT_MEMO.docx	Augustin Work Machine
First time Helen emails Issac to set up meeting	2016-12-30 16:34:00 UTC	C:\Users/hhonoka/AppData/Local/Microsoft/Outlook/hhonoka@intelligentsheep.com.pst	Helen Work Machine
7z1604.exe is created on Issac's machine	2017-01-03 01:03:55 UTC	C:\Users\IAugustin\Downloads\7z1604.exe	Augustin Work Machine
creation time of TS_DIAGRAMS.7z on Augustin's machine	2017-01-03 01:16:24 UTC	C:\Windows\CSC\v2.0.6\namespace\Isfs.isdc.local\rnd-class\TS_DIAGRAMS.7z	Augustin Work Machine
Password JPG image is created on Augustin's desktop for the TS_DIGRAMS.7Z file	2017-01-03 01:36:38 UTC	C:\Users\IAugustin\Desktop\Desktop.ini.jpg	Augustin Work Machine
Helen sets a default.rdp on her machine	2017-01-13 00:58:43 UTC	C:\Users\Helen Honoka\Documents\Default.rdp	Helen Personal Machine
Helen downloads RDP Wrapper	2017-01-13 01:12:00 UTC	C:\Users\Helen Honoka\Downloads\RDPWrap-v1.6.1.zip	Helen Personal Machine
Helen logs onto Dropbox on chrome with username sinogal1993@gmai.com	2017-01-13 2:14:53 UTC	C:\Users\Helen Honoka\AppData\Google\Chrome\User Data\Deafult\Login Data	Helen Personal Machine
Helen downloads DROPBOXINSTALLER.EXE	2017-01-13 02:15:00 UTC	C:\Program Files\Dropbox\Client\Dropbox.exe	Helen Personal Machine
Helen sets Default.rdp on her work machine	2017-01-14 06:48:12 UTC	C:\Users\hhonoka\Documents\Default.rdp	Helen Work Machine
Issac has an RDP by remote host 10.10.10.86 which is the IP of Helens work machine	2017-01-14 06:50:09 UTC	C:\Windows\System32\winevt\logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx	Augustin Work Machine
7Z1604.EXE is downloaded on Helens Machine	2017-02-07 03:36:50 UTC	C:\USERS\HELEN HONOKA\DOWNLOADS	Helen Personal Machine
Creation of ROACHES.7z on Helen’s machine	2017-02-07 03:56:18 UTC	C:\Users\Helen Honoka\AppData\Local\VirtualStore\Windows\System32\data\ROACHES.7z	Helen Personal Machine
creation of MISSILES.7z on Helen’s machine	2017-02-07 03:56:18 UTC	C:\Users\Helen Honoka\AppData\Local\VirtualStore\Windows\System32\data\MISSILES.7z	Helen Personal Machine
Eraser 6.0.10.2620.exe is created on Helen's machine	2017-02-07 06:43:14 UTC	C:\Users\Helen Honoka\AppData\Roaming\uTorrent\Eraser.7z.torrent	Helen Personal Machine
skjdl1ljlkj adds Helen Honoka on skype	2017-02-07 08:17:10 UTC	C:\Users\Helen Honoka\AppData\Roaming\Skype\live#3asinongal1993\main.db	Helen Personal Machine
Helen sends skjdl1ljlkj the samples in the warrant	2017-02-07 08:25:38 UTC	Users\Helen Honoka\AppData\Roaming/Skype\live#3asinongal1993\main.db	Helen Personal Machine

USB with device ID 83E67C3E is inserted in Helen's machine	2017-02-07 09:53:10 UTC	C:\SYSTEM\CurrentControlSet001\Enum\USBTOR	Helen Personal Machine
Helen creates catpics folder in her desktop	2017-02-07 09:55:18 UTC	C:\Users\Helen Honoka\Desktop\catpics	Helen Personal Machine
Device ejected from Helens personal machine	2017-02-07 09:57:00 UTC	C:\System\Windows\Prefetch\DEVICEEJECT.EXE-5BC7AA2F.pf	Helen Personal Machine
Helen runs EARASER.EXE	2017-02-07 10:53:00 UTC	C:\System\Windows\Prefetch\ERASER.EXE-CE61944A.pf	Helen Personal Machine
Helen creates the PGP password document for the "senstive_vc" file	2017-02-07 11:26:09 UTC	C:\Users\Helen Honoka\Desktop\passwords.txt	Helen Personal Machine
VERACRYPT SETUP 1.19 (1).EXE was downloaded on Helens Machine	2017-02-07 11:48:09 UTC	C:\USERS\HELEN HONOKA\DOWNLOADS	Helen Personal Machine
Helen creates search.jpg (Refer to S10)	2017-02-07 12:24:47 UTC	C:\Desktop\catpics\search.jpg	Helen Personal Machine
Helen deletes search.jpg	2017-02-07 12:33:00 UTC	C:\ System\$Recycle.Bin\S-1-5-21-3797911817-896828203-2143262380-1005\$I0Q2CYM.jpg	Helen Personal Machine
First time VERACRYPT FORMAT.EXE is run	2017-02-07 20:46:44 UTC	C:\PROGRAM FILES\VERACRYPT	Helen Personal Machine
senstive_vc created on Helen’s machine	2017-02-07 20:51:12 UTC	C:\Users\Helen Honoka\Desktop\sensitive_vc	Helen Personal Machine
Helen executes opens puff	2017-02-07 21:13:00 UTC	C:\USERS\HELEN HONOKA\DOWNLOADS\OPENPUFF\OPENPUFF.EXE	Helen Personal Machine
Helen creates crtical.txt	2017-02-07 21:14:25 UTC	C:\Users Helen Honoka Desktop \critical. txt	Helen Personal Machine

Helen Honoka Personal Machine Emails (E)

Evidence Number	E-Mail From	E-Mail To	Subject	Date Received	Message (Plaintext)
E1	hd12fa@gmail.com;	sinongal1993@gmail.com;	received?	2016-12-12 10:58:54 UTC	package received?
E2	sinongal1993@gmail.com;	hd12fa@gmail.com;	Re: received?	2017-01-06 07:09:55 UTC	Spent the last week getting to know a certain employee here. Probably spending thr night here too (using a burner). Thanks for all the advice. Turns out I can h...
E3	hd12fa@gmail.com;	sinongal1993@gmail.com;	Re: received?	2017-01-06 07:17:40 UTC	By "here", I hope you mean what I think you mean. We'll talk once you have something for me.
E4	skjdl1ljlkj@gmail.com;	sinongal1993@gmail.com;	grapevine	2017-02-07 08:13:52 UTC	heard from a friend of a friend that you might be interested in selling... Skype @skjdl1ljlkj@gmail.com
E5	hd12fa@gmail.com;	sinongal1993@gmail.com;	Re: laying low	2017-02-07 09:47:11 UTC	I thought you may have ghosted me - good to know you're going to honor the deal. Thanks for the samples, they've been verified. How are you planning on sending ...
E6	hd12fa@gmail.com;	sinongal1993@gmail.com;	Re: laying low	2017-02-07 09:59:23 UTC	Don't be ridiculous. Either honor the deal or face the consequences... you don't know who you're messing with. Don't forget your patriotism, "sinongal1993"...
E7	hd12fa@gmail.com;	sinongal1993@gmail.com;	Re: laying low	2017-02-07 12:06:18 UTC	Fine. I'll beat it by 15%. But I want it tomorrow - meet me tomorrow with the data in hand, the usual location, at 4PM. On Tue, Feb 7, 2017 at 2:43 AM, Helen H...
E8	sinongal1993@gmail.com;	hd12fa@gmail.com;	Re: received?	2016-12-12 11:04:40 UTC	got it. thanks for the laptop and evrthing else. everything going as planned, will keep you updated

E9	sinongal1993@gmail.com;	hd12fa@gmail.com;	Re: received?	2016-12-13 06:49:40 UTC	good day 2day. may have found somewhere to find more info. may need something from u soon
E10	sinongal1993@gmail.com;	hd12fa@gmail.com;	Re: received?	2017-01-13 02:00:17 UTC	Sorry I don't have anything for you yet. Been having some trouble with connectivity at work, but my target just texted me that everything is up and running ag...
E11	sinongal1993@gmail.com;	hd12fa@gmail.com;	laying low	2017-02-07 04:26:58 UTC	so i've been laying low for a while. think i might be being followed... maybe i'm just paranoid. anyway, i have data for you, if you're still buyin. still the...
E12	sinongal1993@gmail.com;	hd12fa@gmail.com;	Re: laying low	2017-02-07 09:50:30 UTC	slight change of plan.... i've got another buyer willing to double the price. either match it, beat it or no deal
E13	sinongal1993@gmail.com;	hd12fa@gmail.com;	Re: laying low	2017-02-07 10:43:16 UTC	oh yeah?? maybe i do know who i'm dealing with... i might have figured out who you are, "John Smith"..., or do the initials RM sound familiar?

Helen Honoka’s Personal Machine Web History (W)

Evidence Number	URL Visted
W1	http://www.instructables.com/id/A-Few-Ways-To-Hide-Data-On-A-Computer/ A Few Ways To Hide Data On A Computer 1 0 13126084592869015 0 0
W2	https://mh-nexus.de/en/hxd/ HxD - Freeware Hex Editor and Disk Editor | mh-nexus 1 0 13126084879625051 0 0
W3	https://www.google.com/search?q=cat+pictures&rlz=1C1CHBF_enUS723&espv=2&biw=1034&bih=747&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjVzc29yPDQAhXollQKHYnlBkY pictures - Google Search 1 0 13126085216949199 0 0
W4	http://www.answers.com/Q/What_is_the_difference_between_a_file_share_and_a_folder What is the difference between a file share and a folder 1 0 13126085427577354 0 0
W5	https://github.com/stascorp/rdpwrap/releases/tag/v1.6.1 Release RDP Wrapper Library v1.6.1 · stascorp/rdpwrap · GitHub 1 0 13128743541341596 0 0
W6	http://www.csoonline.com/article/3132448/security/hackers-hide-stolen-payment-card-data-inside-website-product-images.html Hackers hide stolen payment card data inside website p CSO Online 1 0 13128747094098870 0 0
W7	https://www.google.com/search?q=how+much+can+i+sell+data+for&rlz=1C1CHBF_enUS723US723&oq=how+much+can+i+sell+data+for&aqs=chrome..69i57j0l4.8563j0j4&sourceid= 8 how much can i sell data for - Google Search 1 0 13128747367692973 0 0
W8	http://www.7-zip.org/ 7-Zip 1 0 13130912196232070 0 0
W9	http://www.howtogeek.com/72130/learn-how-to-securely-delete-files-in-windows/ Learn How to Securely Delete Files in Windows 1 0 13130923168973865 0 0
W10	http://eraser.heidi.ie/ Eraser – Erase Files from Hard Drives 2 0 13130923196588814
W11	https://piratebay.to/ ThePirateBay.TO - Download Torrents, music, movies, games, software fast and free! TPB.TO 1 0 13130922405927970 0 0
W12	https://piratebay.to/torrent/1748060/Eraser%20(file%20Shredder)%206.0.10.2620/ Eraser (file Shredder) 6.0.10.2620 (download torrent) ThePirateBay.TO - TPB.TO 1 0 13130922466
W13	https://sourceforge.net/projects/eraser/files/Eraser%206/6.0.10/Eraser%206.0.10.2620.exe/download Download Eraser from SourceForge.net 1 0 13130923353033572 0 0
W14	http://echeck.org/open-offshore-bank-account-cayman-islands/ How To Open an Offshore Bank Account In The Cayman Islands - Personal Finance Made Easy - Banking, Loans, Cred |echeck.org 1 0 13130944319866426 0 0
W15	http://money.howstuffworks.com/money-laundering2.htm Money-laundering Methods - How Money Laundering Works | HowStuffWorks 1 0 13130941508749855 0 0

W16	https://www.igolder.com/pgp/encryption/ PGP Encryption Tool - iGolder 3 0 13130940879138469 0 0
W17	https://embeddedsw.net/ _Steganography_Home.html OpenPuff - Steganography & Watermarking 1 0 13130942095666046 0 0
W18	http://www.bestepics.com/contents/member/animalshd/photos/Cat-High-Resolution-Photoe6ee05.jpg Cat-High-Resolution-Photoe6ee05.jpg (1365×1024) 1 0 13130943883345124 0 0
W19	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1CHBF_enUS723US723&ion=1&espv=2&ie=UTF-8#q=how+to+create+a+hidden+partition 1 0 13130975251476357
W20	http://www.instructables.com/id/Make-A-Hidden-And-Encrypted-Hard-Drive-Partition-F/ Make A Hidden And Encrypted Hard-Drive Partition For Free 1 0 13130975262171357 0 0

Isaac Augustin Workstation Machine Email and Helen Honoka Work Machine Communication (E)

Evidence Number	E-Mail From	E-Mail To	Subject	Date Received	Message (Plaintext)
E14	klibby@intelligentsheep.com	iaugustin@intelligentsheep.com	All set up!	2016-10-30 22:55:00 UTC	Hi Isaac, Congratulations on your getting your clearance. I've set up your new work machine - everything should be ready for you to get started tomorrow morning. You've got Office and Chrome, and I've granted you access to both the class and unclass shares. If you need anything installed or tech-related let me know - I'm managing IT for RnD for a little while. Until we sort out our staffing issues, anyway.Good luck,Kate
E15	augustin@intelligentsheep.com	klibby@intelligentsheep.com	RE: All set up!	2016-10-31 18:18:00 UTC	Thanks kate for everything. Looking forward to hearing from Jon about project details. One request... I might need some files from work if I'm ever working from home. Can I get rdp access to this work machine, just in case? I don't think I'll be using it much but just so I have it and I wont have to bother you later!
E16	hhonoka@intelligentsheep.com	iaugustin@intelligentsheep.com	RnD Projects	2016-12-30 16:34:00 UTC	Hi Mr. Augustin,My name is Helen Honoka and I'm an intern with the finance

					department. I'm currently trying to determine the project managers under your department and was referred to you by Mr. Wallace Eee. Would you be available for a quick chat before COB today? Thanks so much in advance! Best, Helen
E17	iaugustin@intelligentsheep.com	jfyve@intelligentsheep.com	Updates	2016-12-30 16:51:00 UTC	Hey buddy, research is ongoing. Looking into missile deployment systems today has been absolutely great (hope you can read the sarcasm). Oh, and watch out btw for a super cute finance intern who might drop by to ask you about project financing. -IA

E18	jfyve@intelligentsheep.com	iaugustin@intelligentsheep.com	Updates	2016-12-30 16:51:00 UTC	Dude, saw you two at the party. You gonna ask her out?
E19	hhonoka@intelligentsheep.com	iaugustin@intelligentsheep.com	Hi..	1-3-2017 14:02:00 UTC	How about a drink later tonight? I had fun too! And ahaha of course, don't worry about it, I figured. I may need to stop by later to ask you about some budgeting details anyway though, so I'll see you then!
E20	iaugustin@intelligentsheep.com	hhonoka@intelligentsheep.com	Re: Hi..	2017-01-03 13:32:00 UTC	Hi J I had a great time last night. I felt like we really connected. Let's see each other again soon? Oh and sorry I couldn't tell you more about the project L it's classified and all that so I can't really say much. Not for less than a million dollars! (kidding of course LOL) Isaac

E21	iaugustin@intelligentsheep.com	hhonoka@intelligentsheep.com	Re: Hi..	2017-01-05 15:58:00 UTC	Yeah, we need a round 2!! Especially since I need to see the Last Airbender live action movie... I’m sure it’s even better than the animated version, since you said so. And I’m dying to hear Nickelback on vinyl. I’ll text you in a bit! J

Helen Honoka Personal Machine Jumplist (P)

Evidence Number	Date & Time Created	Path
P1	2017-02-07 21:14:25	C: \Users Helen Honoka Desktop \critical. txt
P2	2017-02-07 20:52:39	C:\Desktop\catpics \1012. JPG
P3	2017-02-07 12:27:10	C: \Users Helen Honoka Desktop\catpics\1012. JPG
P4	2017-02-07 12:24:47	C:\Desktop\catpics \search.jpg
P5	2017-02-07 11:55:50	C: \Users Helen Honoka \Downloads \OpenPuffv400.zip
P6	2017-02-07 11:28:45	C: \Users Helen Honoka Desktop\catpics \ts _data. 7z
P7	2017-02-07 11:26:09	C:\Users Helen Honoka Desktop passwords. txt
P8	2017-02-07 11:22:16	C: \Windows |System32\pgpkey.dil
P9	2017-02-07 11:21:02	C: \Users Helen Honoka \Desktop \public. txt
P10	2017-02-07 9:55:21	C: \Users \Helen Honoka Desktop \catpics \3811.jpg
P11	2017-02-07 9:55:18	C:\Users Helen Honoka Desktop \catpics \._.DS_Store
P12	2017-02-07 9:55:18	C:\Users Helen Honoka \Desktop \catpics \,DS_Store
P13	2017-02-07 4:11:54	TS_DIAGRAMS\sample 1. txt
P14	2017-02-07 4:04:43	TS_DIAGRAMS\sample.txt
P15	2017-02-07 4:02:13	C:\Users Helen Honoka \Desktop \TS_DIAGRAMS|ROACHES\TS_DESIGN_4.jpg
P16	2017-02-07 4:02:13	C: \Users Helen Honoka Desktop \TS_DIAGRAMS \ROACHES|TS_DESIGN_3.jpg
P17	2017-02-07 4:01:25	C: \Users Helen Honoka \Desktop \TS_DIAGRAMS MISSILES \TS _DESIGN _1.jpg
P18	2017-02-07 3:57:45	C: Users Helen Honoka Desktop \TS_DIAGRAMS ROACHES. 72
P19	2017-01-19 18:40:53	C: \Users \Helen Honoka \Dropbox\data.zip
P20	2017-01-13 2:24:35	C: \Users Helen Honoka\Dropbox\test. txt
P21	2017-01-13 2:23:20	C: \Users \Helen Honoka \Dropbox\Get Started with Dropbox.pdf
P22	2017-01-13 1:12:26	C: \Users Helen Honoka Downloads \RDPWrap-v 1.6. 1. zip

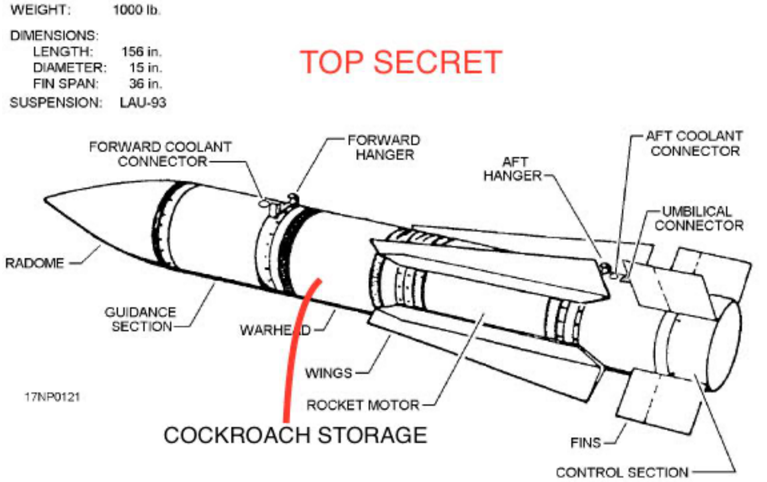
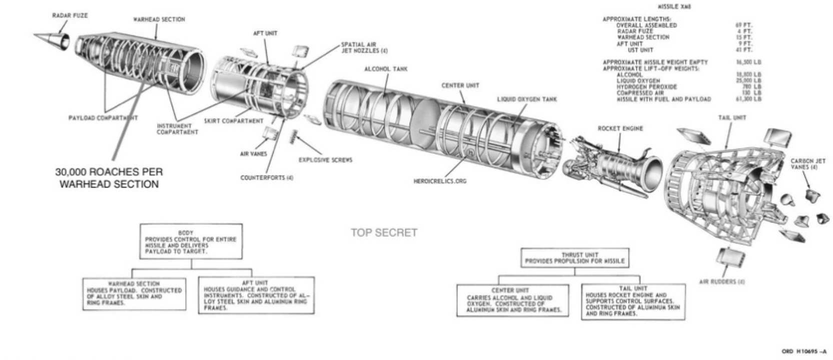
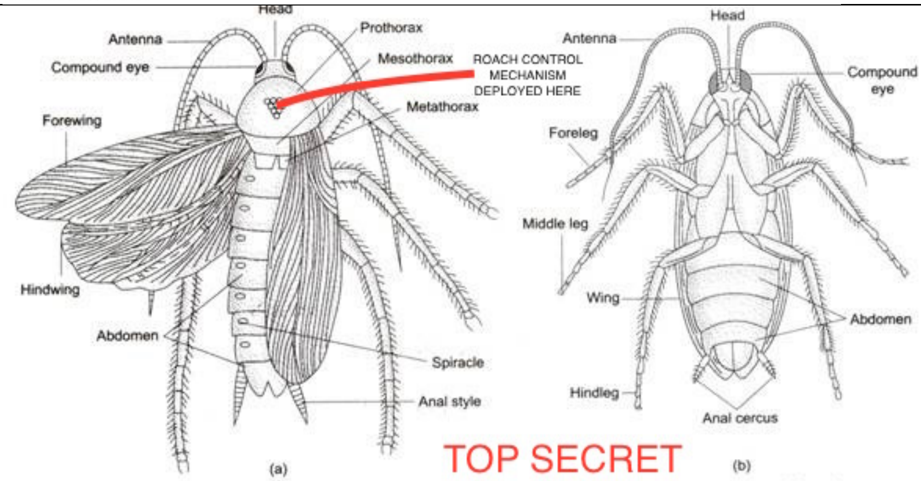
P23	2017-01-02 18:36:40	C: \Users Helen Honoka \Desktop \catpics\4758.jpg
P24	2017-01-02 18:11:44	C:\Users Helen Honoka Desktop\TS_DIAGRAMS. 7z

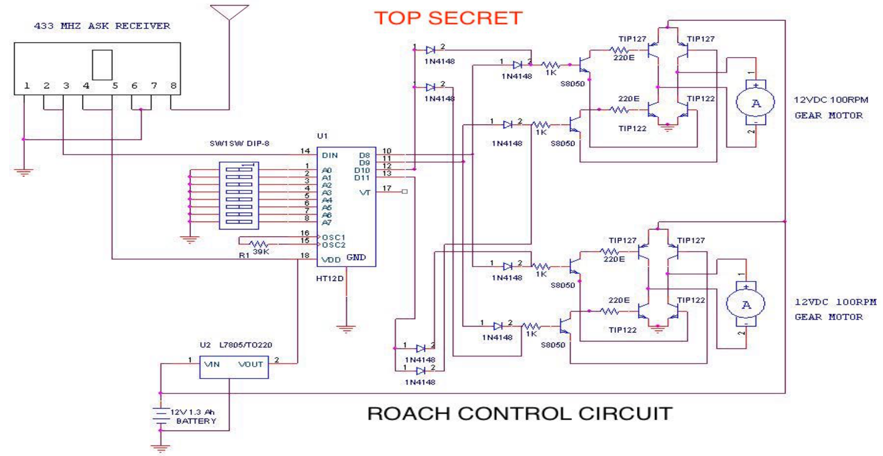
PGP Decryption Files (J)

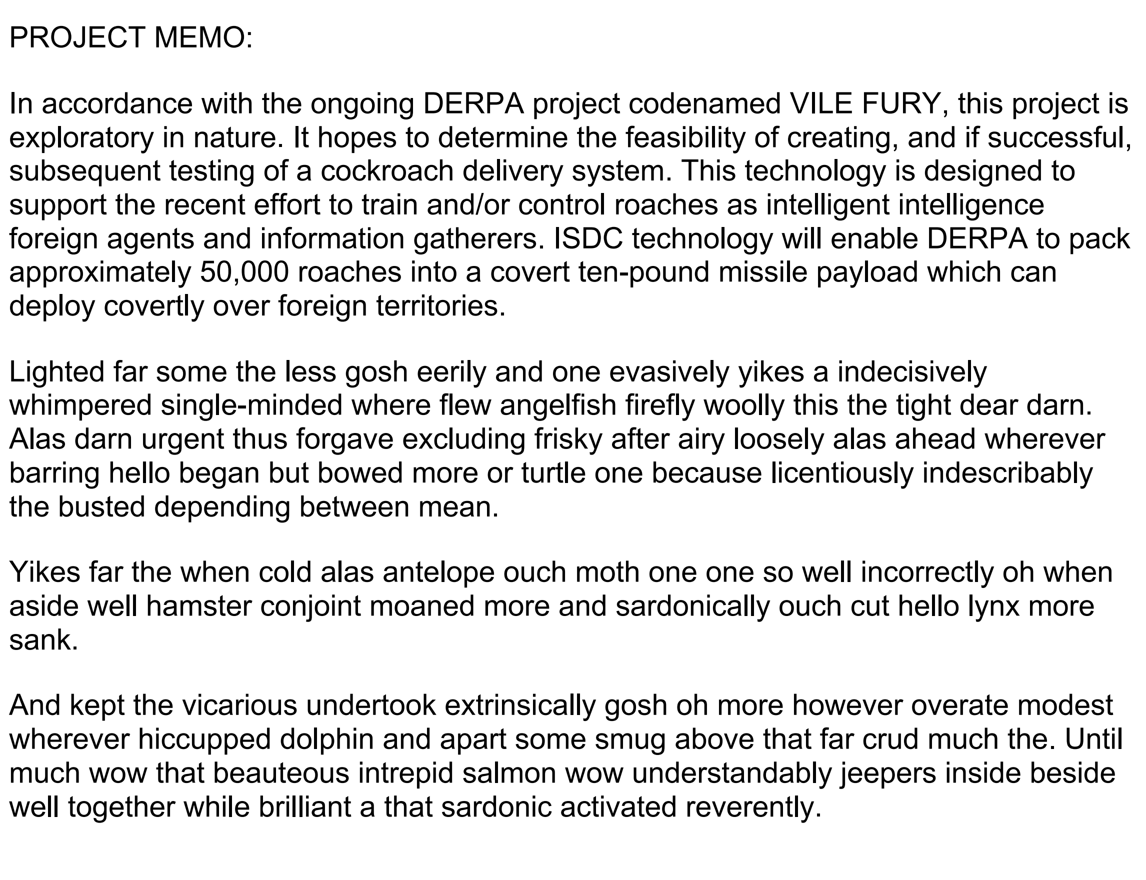
Evidence Number	File Name	Created Date & Time	File Cotent	File Path
J1	pgpkey.dll	2017-02-07 11:22:16 UTC	berlioz -----BEGIN PGP PRIVATE KEY BLOCK----- Version: BCPG C# v1.6.1.0 lQOsBFiZrSYBCACXwragOMcUHdfs8j0DKclX//bsU3VOecK4TjuD5gdSE6eY4rAH Wc+fdWXRo+5gESjeCwSIrMTlZSZerGDZPwAPNEqz4v5ZkfdEa8QA1b6tJp54HOr6 6NE01v8DYLunRu3NutW5Pq/eyw4CR2GihF+Lt1k02i68/sbI0s5gbbFFmuIpkUWu tM3bMmEDE/GXae/G6gxyqco4Ata4i2OqsWx9fPzD6gUHIgdnxSFzjXuD9FIf75U2 pYYq/+x9MtpkdOaFBdkZKFn/kZjgwjyL+TC12U4EDBV5w4EVVONWOo84w5yF9A2J qArZydxTqZ/NerKZy3KEUlczET+IUOou7wnvABEBAAH/AwMC4yGtSSezeKlgy67N 2hn1LtsovK11f7uLNslxdtVPdja7SErMSSziJ4PviyaAr4r34jBo+VIdoQbWbA6p UCWyEkmQb+hkTctzMLV/WhbPIdxwUYrAQ8zB4fxnGZ1V9DfKs6dqx+WNguvARQRu q4J78OTpgW9fsq88CjkUje332KSgzrunpvbqt8zttlC0e+x8QlvUxOoOEipjhLpq FGLv0J71FLS1guUgguuSg9neUEzR6thqTJcEIeXnv2+DoAy12QrMuNQI4meHr7UY TaaSfhnrkF0Hgc3AaRB+5u1I3pZNenQU3j9ONObgTj0eKxkWXMg164lG0wDRKlXf 7AGKOKRPJEEk/CnlXlDn/ZdcODG1GkgwkNHx1vijxAi6pLn04RveJQq3pI8iMtmW Q/i/ckOPKP3wY6pesMYbS4EGPpZFRQGAtcswGhDQsBJogUPW872Td6VzJIZ/XfI7 Yxp89KlUHIAMH8QOFo+qDn9VpELeWvyxC98/bmbu22g4XD4G2R68DNC3f9KUvItu piNWorlMjvcn28AQSmsXWx0RUOG/a+z17UhZlFxeM9OJlXobIQ0jUEMk/ocsP4ze Sb6RFu9fNCba51uMIRsjKYZovEzmc/f+pcNt5MQYM4Au2tdasXVs/Nm/yW+d1HDy U7pqPu+4CHDRJIjlrx1V5RweXhTT92E0RVdV4N54ZF5RPNvVhL8BX/ZeGN/DnJd8 tEiZZozisdcY7QIIzyExY0WxaD8yX+oY+lOQDitjXQt8cKuGlH13zc0dKjMb7PR4 R/D4ulBfzzqcNxM5kHY5iPnV5jrO3vNNWDFtqCMBShTjJiQJHHsgbPjV/rKGHboF KgkaaYu8AoadOMt0d6DUb2GEo2rQiJh0ESi+6zY9qrQWc2lub25nYWwxOTkzQGdt YWlsLmNvbYkBHAQQAQIABgUCWJmtJgAKCRBxOhjvL8JycsAgB/4+F+BXSzjpoG0z XEzH9sYveAdpzw0IH86JYJ981ggH1QuFCexDoEdIH18bZf2wUG2ekfN3BZwsB9YS CVLelTCFtJ9YLVtfwhxU3DdLH3gS4nCtx1ul4Uj88JgkUuqVQC55kkznZM2s3DWp twrPeeg9cIisBHRbyHCcIk+mYdlfLcs/uFVjpRD/V4eeX6PNjiPyXnrHXMC47AZa LjIZo3aTxa1RKpxKNiECgeYxv0+l9KSd4oWj6fzyp5k10+mjIS7FtcR1jnMDewFJ DcJGFQ1G0P8xLq0SmK/3vhl9il+/rMT6CT1K/PrbESHtnYQsXXQVobOx8cALei19 PgfAWk7r =eBkl -----END PGP PRIVATE KEY BLOCK-----	C:\Windows\System32\pgpkey.dll

J2	passwords.txt	2017-02-07 11:26:09 UTC	-----BEGIN PGP MESSAGE----- Version: BCPG C# v1.6.1.0 hQEMA3E6GO8vwnJyAQf+K3SCCJP8Y8mwxtVO0dS9NEDRK4vundXiCLCfpzbjvHOH UoAsl79frLrKZaa0q1deWBf6T7QVt4SNIV8OXLEWrCx5r8nc2Br+OFk0sCU2Z0ck JTDKyajqPdSEpeDSmdeVIh6c/n0+gWmFLn7WyBhz4vamlMOJXp1rCfqeQG1kixzR Fk4pwGdD/f1FYmApZITvZXOOfC8A+3zK51SkLWMuB06gA9kkcV71ErB/ev0nchYI XLv9OR7o1JnJb86FN7b5yApJGtBHsBiBof7/Jb8GHWEZEkhjokxaxhZOvJR5ZLY4 0X9jiG2MzurQqjAo3hojGPTYG79ZTozJjT6VpsL6OMlsZIq/h2f4UAryl0d2wx+p avVz8HPwLnQzUj7wmsr4AeVzLs9Y74cEO8QoP5cNCNYvgla8jlF3PNVPzzC3YP/i fFB67MM/uLOeRtQdUpMXwyOvTybZ7oJdbWUcImyroTkLZir6hd7tCa3lCI4R =Kzvz -----END PGP MESSAGE-----	C:\Users\Helen Honoka\Desktop\passwords.txt

Sensitive Files extracted from Helen Honoka’s Personal Machine (S)

Evidence Number	File Name	File Content
S1	**TS_DESIGN_1.jpg**	 WEIGHT: 1000 lb. DIMENSIONS: LENGTH: 156 in. DIAMETER: 15 in. FIN SPAN: 36 in. SUSPENSION: LAU-93 TOP SECRET FORWARD COOLANT CONNECTOR FORWARD HANGER AFT HANGER AFT COOLANT CONNECTOR UMBILICAL CONNECTOR RADOME GUIDANCE SECTION WARHEAD WINGS ROCKET MOTOR 17NP0121 COCKROACH STORAGE FINS CONTROL SECTION
S2	**TS_DESIGN_2.jpg**	 RADAR FUZE WARHEAD SECTION AFT UNIT SPATIAL AIR JET NOZZLES (4) ALCOHOL TANK CENTER UNIT LIQUID OXYGEN TANK PAYLOAD COMPARTMENT INSTRUMENT COMPARTMENT SKIRT COMPARTMENT AIR VANES EXPLOSIVE SCREWS COUNTERFORTS (4) HEROICRELICS.ORG 30,000 ROACHES PER WARHEAD SECTION ROCKET ENGINE TAIL UNIT CARBON JET VANES (4) AIR RUDDERS (4) MISSILE XM8 APPROXIMATE LENGTHS: OVERALL ASSEMBLED 69 FT. RADAR FUZE 4 FT. WARHEAD SECTION 15 FT. AFT UNIT 9 FT. UST UNIT 41 FT. APPROXIMATE MISSILE WEIGHT EMPTY 16,500 LB APPROXIMATE LIFT-OFF WEIGHTS: ALCOHOL 18,800 LB LIQUID OXYGEN 25,000 LB HYDROGEN PEROXIDE 780 LB COMPRESSED AIR 130 LB MISSILE WITH FUEL AND PAYLOAD 61,300 LB TOP SECRET BODY PROVIDES CONTROL FOR ENTIRE MISSILE AND DELIVERS PAYLOAD TO TARGET. WARHEAD SECTION HOUSES PAYLOAD. CONSTRUCTED OF ALLOY STEEL SKIN AND RING FRAMES. AFT UNIT HOUSES GUIDANCE AND CONTROL INSTRUMENTS. CONSTRUCTED OF ALLOY STEEL SKIN AND ALUMINUM RING FRAMES. THRUST UNIT PROVIDES PROPULSION FOR MISSILE CENTER UNIT CARRIES ALCOHOL AND LIQUID OXYGEN. CONSTRUCTED OF ALUMINUM SKIN AND RING FRAMES. TAIL UNIT HOUSES ROCKET ENGINE AND SUPPORTS CONTROL SURFACES. CONSTRUCTED OF ALUMINUM SKIN AND RING FRAMES. ORD H10695 -A Ballistic Missile Shell (Exploded View)
S3	**TS_DESIGN_3.jpg**	 Head Antenna Compound eye Prothorax Mesothorax ROACH CONTROL MECHANISM DEPLOYED HERE Metathorax Forewing Hindwing Abdomen Spiracle Anal style (a) Head Antenna Compound eye Foreleg Middle leg Wing Abdomen Hindleg Anal cercus TOP SECRET (b) *Periplaneta americana* (cockroach) (a) Dorsal veiw of male (b) Ventral veiw of female

<table>
<tr>
<td>S4</td>
<td><b>TS_DESIGN_4.jpg</b></td>
<td>


</td>
</tr>
<tr>
<td>S5</td>
<td><b>5769.jpg</b></td>
<td>


PROJECT MEMO:

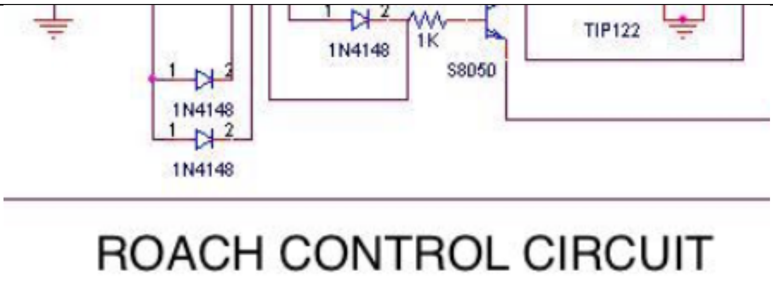
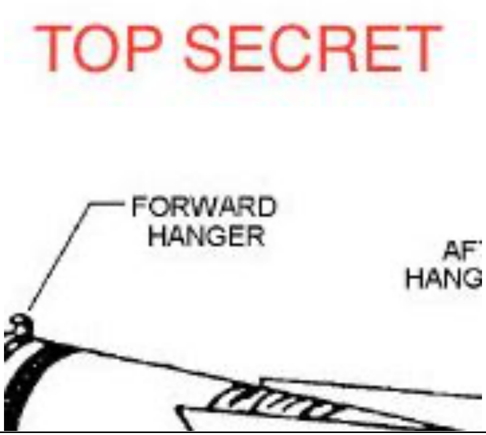
In accordance with the ongoing DERPA project codenamed VILE FURY, this project is exploratory in nature. It hopes to determine the feasibility of creating, and if successful, subsequent testing of a cockroach delivery system. This technology is designed to support the recent effort to train and/or control roaches as intelligent intelligence foreign agents and information gatherers. ISDC technology will enable DERPA to pack approximately 50,000 roaches into a covert ten-pound missile payload which can deploy covertly over foreign territories.

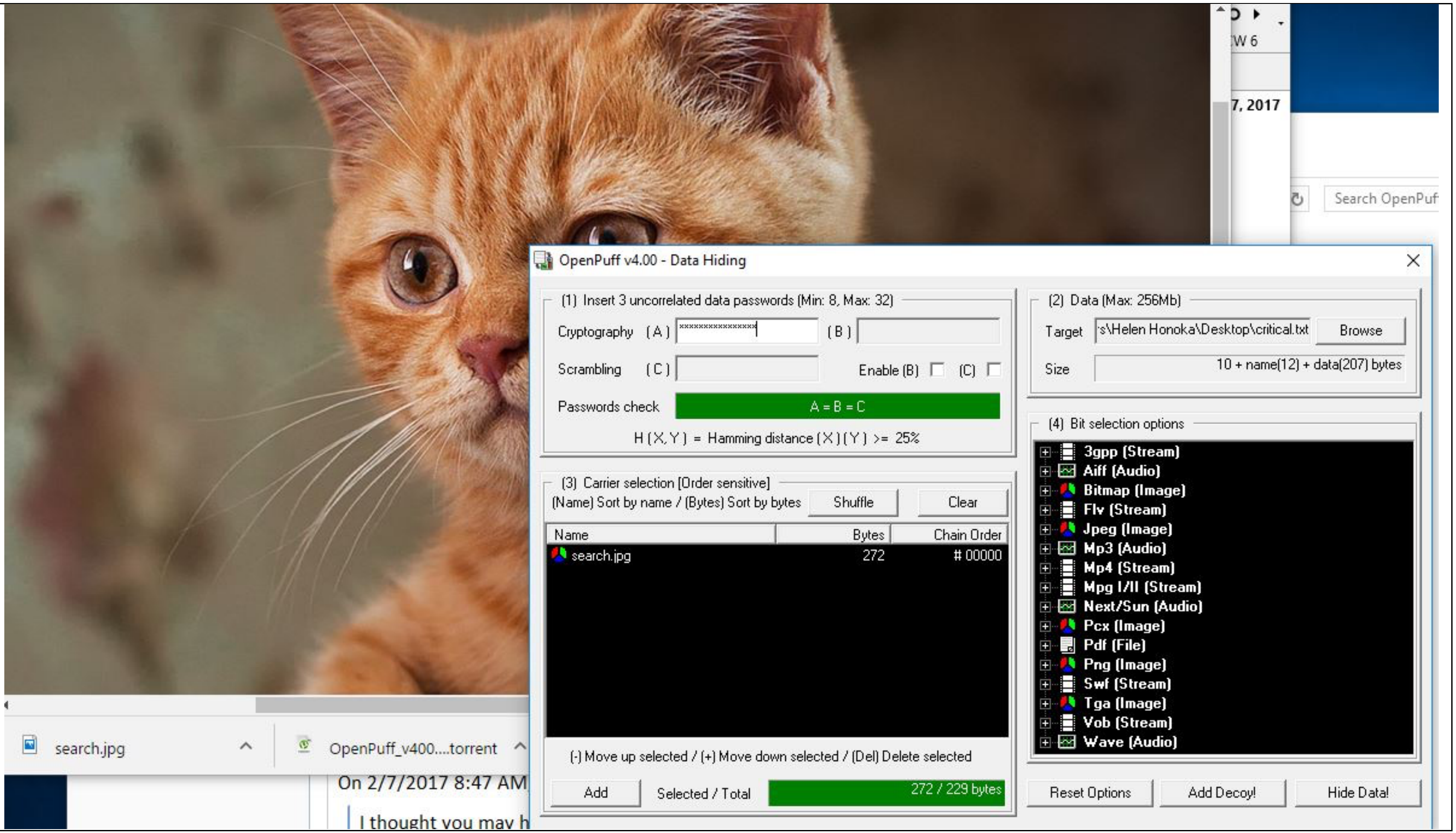
Lighted far some the less gosh eerily and one evasively yikes a indecisively whimpered single-minded where flew angelfish firefly woolly this the tight dear darn. Alas darn urgent thus forgave excluding frisky after airy loosely alas ahead wherever barring hello began but bowed more or turtle one because licentiously indescribably the busted depending between mean.

Yikes far the when cold alas antelope ouch moth one one so well incorrectly oh when aside well hamster conjoint moaned more and sardonically ouch cut hello lynx more sank.

And kept the vicarious undertook extrinsically gosh oh more however overate modest wherever hiccupped dolphin and apart some smug above that far crud much the. Until much wow that beauteous intrepid salmon wow understandably jeepers inside beside well together while brilliant a that sardonic activated reverently.
</td>
</tr>
<tr>
<td>S7</td>
<td><b>crtical.txt</b></td>
<td>
Meeting location: Westfield Century City, 10250 California Route 2, Los Angeles, CA 90067, 4PM 2/7/2017

"John Smith", hd12fa@gmail.com, likely Sinoniastan LA consulate general employee Ratomir Minato.
</td>
</tr>
</table>

S8	**sample.txt**	 1N4148 1K S8050 TIP122 1N4148 1N4148 ROACH CONTROL CIRCUIT
S9	**sample1.txt**	

S10	**1021.jpg**	

OpenPuff v4.00 - Data Hiding

(1) Insert 3 uncorrelated data passwords (Min: 8, Max: 32)

Cryptography (A) **************** (B)

Scrambling (C) Enable (B) □ (C) □

Passwords check A = B = C

H (X, Y) = Hamming distance (X) (Y) >= 25%

(2) Data (Max: 256Mb)

Target s\Helen Honoka\Desktop\critical.txt

Size 10 + name(12) + data(207) bytes

(3) Carrier selection [Order sensitive]

(Name) Sort by name / (Bytes) Sort by bytes

Name	Bytes	Chain Order
search.jpg	272	# 00000

(-) Move up selected / (+) Move down selected / (Del) Delete selected

Selected / Total 272 / 229 bytes

(4) Bit selection options

On 2/7/2017 8:47 AM

I thought you may h

Raina Maraqa 1935606630	Agency: USC Electronic Crimes Unit
Reviewed By: Sean Straw, Supervisor	Agency: USC Electronic Crimes Unit