UNIVERSITY OF NEW HAVEN

Department Of Cyber Security & Networks

Final Forensics Challenge

Report

Submitted in partial fulfilment

Of the requirements for the degree of

MASTERS IN CYBERSECURITY AND NETWORKS

Submitted by-Team-1

AKSHITH RAO- 00952448

AMANI PONNAM- 00863409

OLUWATOYOSI KEHINDE- 00836634

VINUSHA GOUD POTTOLLA-00941796

YADLAPALLI LAKSHMIDHAR- 00964282

December 2024

Advisor

Prof. Mathew Jackson

University *of*
New Haven

Item		Points
1	Provide a written summary not to exceed two pages that describes what took place within the systems pertaining to the potential exfiltration.	
1a	The summary is clear and easy to follow.	5 points
1b	The summary is written in an objective format versus subjective.	5 points
1c	The relevant aspects of the scenario/findings are represented.	3 points for each element
1d	The written summary is free of grammatical, syntax, and spelling errors, *e.g.*, consistent verb tense, pronoun-antecedent agreement, correct use of parallelism, *etc*.	1 point deduction for each error
2	Provide a written description not to exceed four pages of the forensic methodology used to analyze the evidence files and obtain the results identified in the summary. The methodology does not need to provide step-by-step instructions on how software was used; however, it should provide sufficient description for the judges to reproduce the participant's findings.	
2a	The methodology is clear and easy to follow.	5 points
2b	The methodology is written in an objective format versus subjective.	5 points
2c	The methodology is forensically sound and is defensible.	10 points
2d	The methodology is reproducible, *i.e.*, another forensic examiner could follow the procedures and obtain the same results.	10 points
2e	The methodology and table of findings supports the conclusions presented in the summary. There are no gaps in the methodology, *i.e.*, there are findings in the conclusion or the Table of Findings, which are not supported by the methodology.	5 points
2f	The forensic methodology is free of grammatical, syntax, and spelling errors, *e.g.*, consistent verb tense, pronoun matching, correct use of parallelism, *etc*.	1 point deduction for each error
3	Provide a Table of Findings, which contains a list of recovered artifacts	
3a	Identify the names of all installed operating systems	2 points each
3b	Identify the versions of all operating systems present	3 points each
3c	Identify each system by its hostname and its matching IP address	2 points each
3d	Identify all user accounts on all systems	3 points each
3e	Identify all passwords for all user accounts on all systems	5 points each
3f	Identify all websites accessed/visited by each system	1 point each
3g	Identify any suspicious files on the computer systems	3 points each
3h	Identify all instances of stolen website credentials for www.crazywickedawesome.com. Each instance should be identified by listing the file(s) that contained the credentials. Identification must include: the file's name, hash of file, path to file, and logical offset.	7 points each
3i	If information was exfiltrated from The HiTeK Company, then identify the exfiltrated information. List relevant files by name and MD5 and SHA1 hashes. Describe the contents of the files.	10 points each
3j	If information was exfiltrated from The HiTeK Company, then list the time of the exfiltration(s).	10 points

Table-1 Cyber Forensic Challenge Scoring

CONTENTS

1.EXECUTIVE SUMMARY

The investigation of a digital forensic data breach involving the unlawful exfiltration of private data from HiTeK Company is described in this report. The responding agency gathered evidence for analysis, such as picture files and a network capture. The evidence, Which included 2 disk images and network PCAP file, it was examined by the UNHCFREG Cyberteam Investigation Unit in order to verify the information, examine its contents, and determine the exfiltration technique.

Autopsy, a potent forensic tool that made it possible to extract digital evidence and possibly uncover indications of data modification, deletion, or unauthorized access, was used to perform a thorough analysis of the disk images. Examiners are able to reconstruct crucial info which made clear the type and scope of the suspected breach by utilizing Autopsy's sophisticated features.

Not only this, network forensics were used in the investigation concentrating on the network pcap file's analysis using Wireshark. This method made it possible to examine network traffic in great detail, which helped reconstruct the attack timeline. Investigators discovered possible access points, data exfiltration routes, and suspicious activity patterns through packet-level analysis.

Disk and network forensic techniques had to be integrated in order to fully comprehend the incident. Consistent with the core principles of cyber forensics, this systematic approach highlighted the importance of producing reliable and legally admissible evidence.

The investigation's overall goal was to find important evidence to back up court cases and guide strategic cybersecurity measures. The importance of cyber forensics for safeguarding digital assets and preserving the integrity of the investigation was illustrated by the use of state-of-the-art forensic tools.

2. APPARATUS

Table 1: Apparatus used in Investgation

ITEM/PART	MODEL NUMBER	VERSION	USAGE
Lenovo	N/A	Windows 11	Used for analysis of disk images in autopsy
Wireshark	N/A	V4.4.2	Used for network analysis of the .pcap file
Virtual Machine	N/A	V7.1.4	Used for running the virtual opera ng system
Autopsy	N/A	V4.21.0	Used to analyze and extract data from image files
John the Ripper	N/A	V1.9.0	Used to bypass password from computer 2.E01 Linux user account
fcrackzip	N/A	V1.3	Used to bypass password of zip files such as BusinessStrategy.zip and Secrets.zip
CertUtil	N/A	Inbuilt in Windows Command Prompt	Used to generate MD5 and SHA1 hashes of the images and evidence
FTKImager	N/A	V4.3	Used to extract reports for Acquisiton.txt files

3. PROCEDURES

3.1.Procedure

On November 28, 2015, investigators started looking into the possibility that sensitive information might have come from HiTek Company. After examining the supplied PCAPNG file, which included multiple IP addresses linked to the business network, the first important hints became apparent. As a result, investigators found that some private IP addresses, such as those mentioned below, were increasingly being targeted. Computer One's hostname was determined to be DESKTOP-A8B0TBH, and its IP address was 192.168.0.6. Furthermore, this computer's virtual machine had the IP address 192.168.0.7 and the hostname DESKTOPA8B0TBH. The IP address 192.168.0.8 and hostname Web-srv-02 were allocated to Machine Two.

An investigation into the server with IP address 192.168.0.6 on November 25, 2018, found that the server at 192.168.0.8 could be accessed using the username "webmaster" and a matching password. The STOR command was used to upload the files secrets.zip and businessstrategy.zip to the server. The CHMOD644 command was then used to change the server's file permissions, limiting access for other user groups while granting the file owner read and write access. Afterwards, the DELE command was used to remove the files from the server. Another questionable IP address, 192.168.0.4, was discovered during this procedure; however, its hostname was not revealed. The downloaded files were associated with this IP address.

Further analysis of log files from machine 1.E01 revealed additional critical data. Investigators employed steganography techniques to recover internet passwords for the website "www.crazywickedawesome.com," which had been concealed within several images. These findings suggested that data exfiltration had occurred, potentially leading to the compromise of sensitive information. The investigation also determined that carlson have installed another version of vmware on each system, that contributed to system instability and potential vulnerabilities.

Through the careful gathering and analysis of all evidence, investigators concluded that sensitive data had been successfully exfiltrated from the network. The findings highlight the complexity of the incident and the importance of thorough forensic analysis in identifying and understanding data breaches.

4.METHODOLOGY

Investigators started their inquiry by entering the disk pictures into the Autopsy Sleuth Kit software after acquiring disk images for both computers and hard drives.

4.1. Computer 01 Procedure

Investigators began analyzing the disc image for computer 1 after importing eight disc pictures of the system into Autopsy. Creating MD5 hash values for the system and its image and comparing them to make sure the disc had not been tampered with was the first step in confirming the data's integrity. Investigators started examining the information included in the Computer1.E01 picture after the hashes were verified. Important system parameters like the hostname, IP address, operating system, and account information were included in this data. It was discovered from the windows/system32/config/system file that, it was determined that the hostname and computer name were both Desktop-A8botbh. The operating system was identified as Windows 10 Pro from the SYSTEM and SOFTWARE records.

Further investigation into the system's files led to the discovery of the SAM file, which contains sensitive user account and password information. To access and decipher these user credentials, investigators mounted the image of computer 1 using FTK Imager. Once mounted, they created a virtual machine file using the ".vmdk" format via the command prompt and then loaded it into Oracle VirtualBox to boot the image. With Windows 10 successfully booted up, investigators were able to install Mimikatz.exe, a tool designed to extract user data from the SAM file, including NTLM password hashes.

By running Mimikatz.exe with administrative privileges, investigators successfully retrieved the NTLM hashes of the system’s user accounts. These hashes were then decrypted using the online platform "crackstation.net," which allowed the investigators to identify the plaintext passwords associated with the accounts. The recovered credentials revealed the passwords as "letmein," "Monkey," & "123456," which corresponded to the users carlson, jonathan, and tester, respectively.

In addition to examining the system image, investigators also reviewed VMware files related to the system and discovered that a virtual machine running the Linux Ubuntu operating system was installed under the "tester" user account. By utilizing FTK Imager and Autopsy, investigators extracted the vmdk files associated with the Ubuntu virtual machine and found the "shadow.bak" file, which stores encrypted password information. This file was further analyzed using Kali Linux to extract the usernames and password hashes, which were later cracked using the "john the ripper" tool, revealing the password for the Ubuntu user.

While continuing the investigation into computer 1’s disc image, investigators found that the system had both Google Chrome and Mozilla Firefox installed, with web search histories revealing non-suspicious websites like the Star Wars website. However, they also found search queries related to "MMC," a term that appeared frequently in searches. Further investigation of the MMC file in the Autopsy-loaded data revealed login credentials for the website crazywickedawesome.com, including Username "laslow" and password "frito-Lay".

The examination of the SQLite history database, which tracked the web searches of users "tester"

and "Carlson," continued to yield valuable information. The investigators also reviewed the "place.sqlite3" database, which contained detailed logs of the users' search activities, further corroborating the investigation. Among the important findings was the discovery of Credentials for the website www.Crazywickedawesome.com, with the username "henchman" and the password "P@ssw0rd!@."

The investigators also found a second file, "grays.png," in the image's hex code that contained more sensitive information, such as the credentials "evil henchman" and the secret key "MyP@ssw0rd!@." Another file found during the investigation was called "a.zip," and it contained a text file called "a.txt" that contained a list of the letter "a." This suggested that anti-forensic methods might be used, perhaps to encrypt or conceal data. Investigators discovered proof that the user used encryption software, specifically the VeraCryptSetup1.16.exe file, which raises the possibility that the system was using encrypted data storage and concealment techniques.

4.2.Procedure of Computer 02

The investigation of computer 2 began when investigators loaded the image file Computer2.E01 into Autopsy. To ensure the integrity of the image and verify that no tampering had occurred, both the MD5 hash value of the computer and the value for the image file were generated and compared. After confirming the image's authenticity, investigators identified the operating system as Ubuntu 12.0.4, located under the path vol_vol2/etc/issue. Additionally, the hostname was identified as "websrv02" in the vol_vol2/etc/hostname file. With this information in hand, investigators proceeded to review the user account details found in the vol_vol2/home directory. To retrieve the passwords for the user accounts on the system, the investigators navigated to the vol_vol2/var/backups directory, where they discovered a file named "shadow.bak." This file was downloaded from Autopsy and copied to a kali Linux virtual machine for further analysis. By executing the "john the ripper" tool with the command "john," investigators were able to crack the password hashes stored in the shadow file, which revealed the user credentials on the system.

During the ongoing investigation, investigators uncovered several log files that provided valuable information. One of these was the "vsfipd.log" file, which contained logs from the FTP server. The second log file, "access.log," stored Apache web server logs. These files helped the investigators understand the activities and interactions that had occurred on the system, particularly with respect to the accessed websites and files.

Moreover examination of the autopsy-loaded files revealed two encrypted zip files: "BUSINESSSTRATEGY.ZIP" AND "SECRETS.ZIP." The investigators attempted to crack the passwords for these files using the Fcrackzip application, which performed a brute-force attack. However, despite the failed attempts to decrypt the files with Fcrackzip, the investigators conducted a manual search through the server logs and weblogs. These searches revealed the websites that had been visited and the files that had been accessed, as well as important user data, such as names and email addresses.

Lastly, the investigators compiled a timeline that detailed the server's activities. Using Autopsy's Timeline application, they created two distinct timelines. The first timeline covered activities from

Jan to Nov, marking the specific dates when sensitive data was exfiltrated. The second timeline focused on the months of September to November, with November being the most active month, particularly on November 28, 2015, when significant events occurred. This comprehensive timeline helped investigators pinpoint the exact moments of the data breach and other suspicious activities.

4.3.Network.pcapng

To investigate potential data exfiltration, investigators began by loading the network.pcapng file into Wireshark to analyze the network traffic. They enhanced the readability of the PCAP file by expanding the stream id(Emphtcp.stream) and Host (Emphhttp.host) columns. By examining the DHCP query data, investigators found four IP addresses and hostnames. Using commands such as "Ip.Add == 192.168.0.6" and "ip.add == 192.168.0.8," they filtered the network traffic by IP address. Additionally, commands like "Ip.Src == 192.168.0.8" and "tcp.port==21" were used to examine the interactions between these addresses, which appeared suspicious.

Investigators followed the TCP stream flow to track several suspicious exchanges between the identified IP addresses. They discovered that the user "webmaster" had Logged into the server hosted on IP 192.168.0.6, using the same IP address for the connection. The investigation revealed that the source had requested the password and username associated with the user account. Investigators also located the "authentication.ICEauthority" file and observed that the source had accessed the directory to save "Secrets.zip" to the destination. Following this, the source modified the permissions for both "BusinessStrategy.zip" and "Secrets.zip" before ultimately deleting them from the server.

In order to comprehend how and when the "BusinessStrategy.zip" and "Secrets.zip" files were moved from HiTeK Company, the investigators' study was essential. It became crucial to put together the circumstances surrounding their exfiltration because the source had removed these data from the destination. Investigators were able to track the communication between IPs 192.168.0.8 and 192.168.0.4 by filtering traffic on the IP address 192.168.0.8, which was connected to Linux Computer 2. To learn more about the interaction, this tracing was carried out by right-clicking on the pertinent data and tracing the HTTP stream.

In the end, the agents discovered that the user on IP 192.168.0.4 had requested the files from the web server. confirming that the exfiltration of data had occurred. This critical discovery was made while the investigation was ongoing, allowing the team to piece together the flow of sensitive data from the HiTeK network. By analyzing the filtered traffic and traces within Wireshark, investigators were able to identify the exact moments of unauthorized access and file deletion, reinforcing their findings of data theft from the company's systems.

5.PROBLEM SOLVING AND TROUBLESHOOTING

PB 1: The examination of the Computer1.E01 file in Autopsy was extremely slow, with the process freezing at 98%. Despite multiple attempts, the file took several hours, even overnight, to process each time.

Sol 1: To resolve this issue, increasing the allocated resources for VirtualBox, such as adding more CPU cores and RAM, could significantly enhance processing power. Additionally, closing unnecessary applications on the host machine would free up system resources, allowing VirtualBox to run more efficiently.

PB 2: The virtual machine on the computer failed to open, preventing the extraction of the "shadow.bak" file. The hypervisor was disabled, and vM machine would not start due to an incompatibility with the Hyper-version. Despite searching for solutions to enable Windows 10's Hypervisor within the virtual machine, no viable methods were found.

Sol 2: To resolve this, the autopsy virtual machine files (.vmdk) were downloaded and extracted. After unzipping the files, the "shadow.bak" file was successfully retrieved using FTK Imager, which allowed the virtual machine files to be read and analyzed.

6.FINDINGS

no.	operating system	hostname	version	ip address
1	windows	desktop-a8b0tbh	windows 10 pro	192.168.0.6
2	debian	linux (debian)	-	
3	isb-release	linux (ubuntu)	ubuntu	

table 2: table of installed operating systems

no.	hostname	logical count	md5 hash	password
1	tester	8	f2477a144dff4f216ab81f2ac3e3207d	monkey
2	administrator	1	-	-
3	jonathon	0	becedb42ec3c5c7f965255338be4453c	letmein
4	carlson	8	32ed87bdb5fdc5e9cba88547376818d4	123456
5	guest	0	-	-

table 3: table of user accounts

no	file name	md5 hash values	location
1	sam	d41dcd9f00b20469009 ecf427e	/imp_computer1.e01/ vol_vol3/windows/ system32/config/regbac/sam
2	secrets.zip	8168c5f9cf2924562d2f63a1c982a94e	/img_computer2.e01/ vol_vol2/var/www/ se-crets.zip

3	businessstrategy.zip	95d8a102ec775a8712b098b 43d2a1b4e	/img_computer2.e01/ vol_vol2/var/www/ businessstrategy.zip
4	shadow.bak	95d8a102ec775a8712b098b 43d2a1b4e	/img_computer2.e01/ vol_vol2/var/backups/ shadow.bak
5	access.log	e528633057c5323df661639 1708ad797	/img_computer2.e01/ vol_vol2/var/backups/ access.log
6	vsftp.log	c722724afdcaecf0a309cdb1 50627e1a	/img_computer2.e01/ vol_vol2/var/log/ vs-ftpd.log

table 4: list of suspicious files

no.	file name	location
1	a.zip	/img_computer1.e01/ vol_vol3/a.zip/a.txt
2	next-character.docx	/img_computer1.e01/ vol_vol3/users/tester/ documents/nextcharacter.docx
3	shadow.bak	/img_computer2.e01/ vol_vol2/var/backups/ shadow.bak
4	x3fw.ncf	/img_computer2.e01/ vol_vol2/lib/firmware/ vxge/x3fw.ncf
5	x3fw-pxe.ncf	/img_computer2.e01/ vol_vol2/lib/firmware/ vxge/x3fw-pxe.ncf

table 5: stolen files

no	file name	md5 hash value	sha-256 hash value	location
1	grays.jpg	05fce143ef07910a2328 8ff d841df32a	6bb44a3f213934b0e911b 62fbc3 70d9705dbe3c0b83836c0 e50a 91bc6b1cc3bc	/img_computer1.e01/ vol_vol3/users/tester/ documents/grays.jpg
2	grays.pn g	bf298fd9197b2fa17b22 7ddc71 d61765	1a5c371340b9dda7880cc 29284d ca216df47d514351567c9 e53a9 498d9a5a276	/img_computer1.e01/ vol_vol3/users/tester /pictures/grays.png
3	mmc.exe	54e04095b1dea240a8c 0778b4f3 4cab1	2b730c42d947f64968276 3886f	/img_computer1.e01/ vol_vol3/windows/mm

			47dd0a5c0d6bf6c4dc9d5881 0576714db10e2d	c.exe

table 6: credentials for crazywickedawesome.com

no.	file name	md5 hash value	sha1 hash value	date	time
1	secrets.zip	8168c5f9cf2924562d2f63a 1c982a94e	bf04c2e2da0dc9d84ed33f0b0583814d2aefcc09028e10a98a2306474c327043	sat, 28 nov 2015	22:48:25 gmt
2	businessstrategy.zip	bf04c2e2da0dc9d84ed33f0b0583814d2aefcc09028e10a98a2306474c327043	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	sat, 28 nov 2015	22:48:46 gmt

table 7: list of ex-filtered files

no.	name	password	location	password hash
1	cknight	popcorn	img_computer2.e01/var/backups/shadow.bak	6n7fu15mvga8laf5l$60lkm/e3sgljskfwfks3o91iiidii9i0xg3mnkq0x2t/pztql56oveizbashpkdifkhuxiunkwukmt9g5j7fi/:16767:0:99999:7:::
2	webmaster	password	img_computer2.e01/var/backups/shadow.bak	6yivb3tix$kp.b3u0jj8kwagkk05.g5mb/qreydj9xtrnmmnflekymsupsq6.d.ctoloeyr3wi32tqeww01hg2o..unodrr.:167 67:0:99999:7:::
3	jhathoway	n/a	img_computer2.e01/var/backups/shadow.bak	$6$375qz16zalvujatr$ijthis3efpqs4rxvg0annwt01ap66/.8lkiyefbocpua4mqcfonhawg.zrhla8occqqa104pau5bxivrxvm6i.:16767:0:99999:7::

table 8: useraccountsofcomputer2

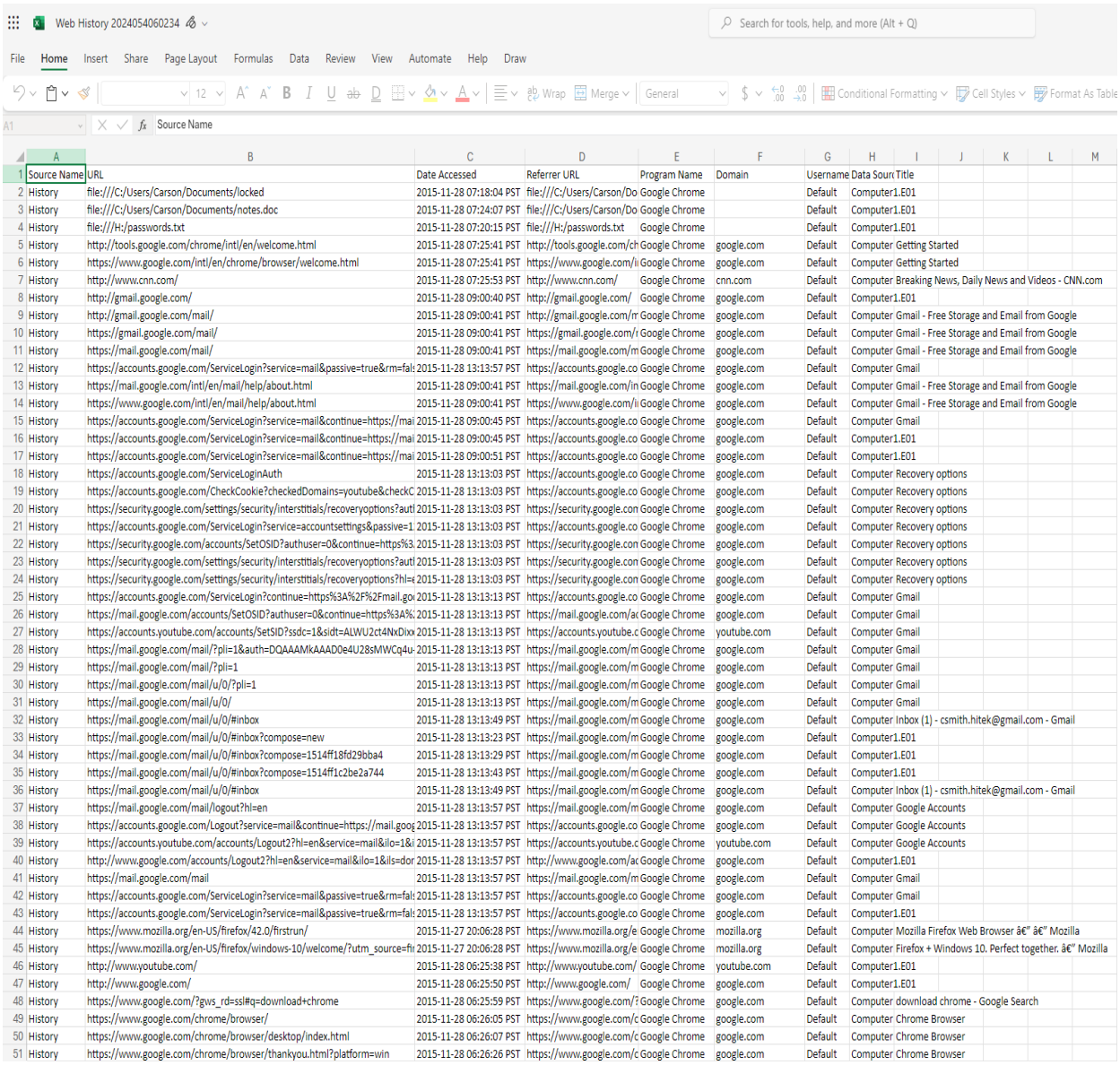
no.	websites	username	passwords	path
1	crazywickedawesome.com	laslow	fritolay	/windows/mmc.exe

2	www.crazywickedawesome.com	evilhenchman	myp@ssw0rd!@	users/tester/desktop/openoffice 4.1.2 (en-us) installation files/grays.png
3	crazywickedawesome.com	henchman	p@ssw0rd!@	users/ tester/pictures/ grays.jpg

table 9: logindetailsforcrazywickedawesome.com

no.	host	operating system	version
1	192.168.0.9	windows	windows 10
2	192.168.0.10	windows	n/a
3	192.168.0.200	windows	windows 7 or windows server 2008 r2

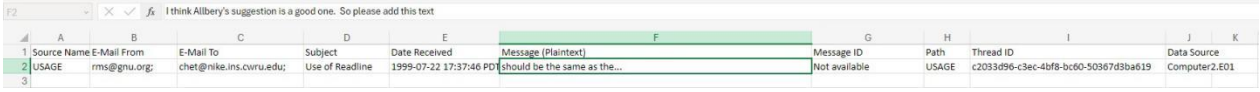
table 10: other host's operating system and version present on the network



Web History 2024054060234

Source Name	URL	Date Accessed	Referrer URL	Program Name	Domain	Username	Data Sour	Title
History	file:///C:/Users/Carson/Documents/locked	2015-11-28 07:18:04 PST	file:///C:/Users/Carson/Do	Google Chrome		Default	Computer1.E01	
History	file:///C:/Users/Carson/Documents/notes.doc	2015-11-28 07:24:07 PST	file:///C:/Users/Carson/Do	Google Chrome		Default	Computer1.E01	
History	file:///H:/passwords.txt	2015-11-28 07:20:15 PST	file:///H:/passwords.txt	Google Chrome		Default	Computer1.E01	
History	http://tools.google.com/chrome/intl/en/welcome.html	2015-11-28 07:25:41 PST	http://tools.google.com/ch	Google Chrome	google.com	Default	Computer	Getting Started
History	https://www.google.com/intl/en/chrome/browser/welcome.html	2015-11-28 07:25:41 PST	https://www.google.com/i	Google Chrome	google.com	Default	Computer	Getting Started
History	http://www.cnn.com/	2015-11-28 07:25:53 PST	http://www.cnn.com/	Google Chrome	cnn.com	Default	Computer	Breaking News, Daily News and Videos - CNN.com
History	http://gmail.google.com/	2015-11-28 09:00:40 PST	http://gmail.google.com/	Google Chrome	google.com	Default	Computer1.E01	
History	http://gmail.google.com/mail/	2015-11-28 09:00:41 PST	http://gmail.google.com/m	Google Chrome	google.com	Default	Computer	Gmail - Free Storage and Email from Google
History	https://gmail.google.com/mail/	2015-11-28 09:00:41 PST	https://gmail.google.com/r	Google Chrome	google.com	Default	Computer	Gmail - Free Storage and Email from Google
History	https://mail.google.com/mail/	2015-11-28 09:00:41 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer	Gmail - Free Storage and Email from Google
History	https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=fal	2015-11-28 13:13:57 PST	https://accounts.google.co	Google Chrome	google.com	Default	Computer	Gmail
History	https://mail.google.com/intl/en/mail/help/about.html	2015-11-28 09:00:41 PST	https://mail.google.com/in	Google Chrome	google.com	Default	Computer	Gmail - Free Storage and Email from Google
History	https://www.google.com/intl/en/mail/help/about.html	2015-11-28 09:00:41 PST	https://www.google.com/i	Google Chrome	google.com	Default	Computer	Gmail - Free Storage and Email from Google
History	https://accounts.google.com/ServiceLogin?service=mail&continue=https://mai	2015-11-28 09:00:45 PST	https://accounts.google.co	Google Chrome	google.com	Default	Computer	Gmail
History	https://accounts.google.com/ServiceLogin?service=mail&continue=https://mai	2015-11-28 09:00:45 PST	https://accounts.google.co	Google Chrome	google.com	Default	Computer1.E01	
History	https://accounts.google.com/ServiceLogin?service=mail&continue=https://mai	2015-11-28 09:00:51 PST	https://accounts.google.co	Google Chrome	google.com	Default	Computer1.E01	
History	https://accounts.google.com/ServiceLoginAuth	2015-11-28 13:13:03 PST	https://accounts.google.co	Google Chrome	google.com	Default	Computer	Recovery options
History	https://accounts.google.com/CheckCookie?checkedDomains=youtube&checkC	2015-11-28 13:13:03 PST	https://accounts.google.co	Google Chrome	google.com	Default	Computer	Recovery options
History	https://security.google.com/settings/security/interstitials/recoveryoptions?autl	2015-11-28 13:13:03 PST	https://security.google.con	Google Chrome	google.com	Default	Computer	Recovery options
History	https://accounts.google.com/ServiceLogin?service=accountsettings&passive=1	2015-11-28 13:13:03 PST	https://accounts.google.co	Google Chrome	google.com	Default	Computer	Recovery options
History	https://security.google.com/accounts/SetOSID?authuser=0&continue=https%3	2015-11-28 13:13:03 PST	https://security.google.con	Google Chrome	google.com	Default	Computer	Recovery options
History	https://security.google.com/settings/security/interstitials/recoveryoptions?autl	2015-11-28 13:13:03 PST	https://security.google.con	Google Chrome	google.com	Default	Computer	Recovery options
History	https://security.google.com/settings/security/interstitials/recoveryoptions?hl=e	2015-11-28 13:13:03 PST	https://security.google.con	Google Chrome	google.com	Default	Computer	Recovery options
History	https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fmail.go	2015-11-28 13:13:13 PST	https://accounts.google.co	Google Chrome	google.com	Default	Computer	Gmail
History	https://mail.google.com/accounts/SetOSID?authuser=0&continue=https%3A%2	2015-11-28 13:13:13 PST	https://mail.google.com/ac	Google Chrome	google.com	Default	Computer	Gmail
History	https://accounts.youtube.com/accounts/SetSID?ssdc=1&sidt=ALWU2ct4NxDixx	2015-11-28 13:13:13 PST	https://accounts.youtube.c	Google Chrome	youtube.com	Default	Computer	Gmail
History	https://mail.google.com/mail/?pli=1&auth=DQAAAMkAAAD0e4U28sMWCq4u-	2015-11-28 13:13:13 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer	Gmail
History	https://mail.google.com/mail/?pli=1	2015-11-28 13:13:13 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer	Gmail
History	https://mail.google.com/mail/u/0/?pli=1	2015-11-28 13:13:13 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer	Gmail
History	https://mail.google.com/mail/u/0/	2015-11-28 13:13:13 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer	Gmail
History	https://mail.google.com/mail/u/0/#inbox	2015-11-28 13:13:49 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer	Inbox (1) - csmith.hitek@gmail.com - Gmail
History	https://mail.google.com/mail/u/0/#inbox?compose=new	2015-11-28 13:13:23 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer1.E01	
History	https://mail.google.com/mail/u/0/#inbox?compose=1514ff18fd29bba4	2015-11-28 13:13:29 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer1.E01	
History	https://mail.google.com/mail/u/0/#inbox?compose=1514ff1c2be2a744	2015-11-28 13:13:43 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer1.E01	
History	https://mail.google.com/mail/u/0/#inbox	2015-11-28 13:13:49 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer	Inbox (1) - csmith.hitek@gmail.com - Gmail
History	https://mail.google.com/mail/logout?hl=en	2015-11-28 13:13:57 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer	Google Accounts
History	https://accounts.google.com/Logout?service=mail&continue=https://mail.goo	2015-11-28 13:13:57 PST	https://accounts.google.co	Google Chrome	google.com	Default	Computer	Google Accounts
History	https://accounts.youtube.com/accounts/Logout2?hl=en&service=mail&ilo=1&i	2015-11-28 13:13:57 PST	https://accounts.youtube.c	Google Chrome	youtube.com	Default	Computer	Google Accounts
History	http://www.google.com/accounts/Logout2?hl=en&service=mail&ilo=1&ils=dor	2015-11-28 13:13:57 PST	http://www.google.com/ac	Google Chrome	google.com	Default	Computer1.E01	
History	https://mail.google.com/mail	2015-11-28 13:13:57 PST	https://mail.google.com/m	Google Chrome	google.com	Default	Computer	Gmail
History	https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=fal	2015-11-28 13:13:57 PST	https://accounts.google.co	Google Chrome	google.com	Default	Computer	Gmail
History	https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=fal	2015-11-28 13:13:57 PST	https://accounts.google.co	Google Chrome	google.com	Default	Computer1.E01	
History	https://www.mozilla.org/en-US/firefox/42.0/firstrun/	2015-11-27 20:06:28 PST	https://www.mozilla.org/e	Google Chrome	mozilla.org	Default	Computer	Mozilla Firefox Web Browser â€" â€" Mozilla
History	https://www.mozilla.org/en-US/firefox/windows-10/welcome/?utm_source=fi	2015-11-27 20:06:28 PST	https://www.mozilla.org/e	Google Chrome	mozilla.org	Default	Computer	Firefox + Windows 10. Perfect together. â€" Mozilla
History	http://www.youtube.com/	2015-11-28 06:25:38 PST	http://www.youtube.com/	Google Chrome	youtube.com	Default	Computer1.E01	
History	http://www.google.com/	2015-11-28 06:25:50 PST	http://www.google.com/	Google Chrome	google.com	Default	Computer1.E01	
History	https://www.google.com/?gws_rd=ssl#q=download+chrome	2015-11-28 06:25:59 PST	https://www.google.com/?g	Google Chrome	google.com	Default	Computer	download chrome - Google Search
History	https://www.google.com/chrome/browser/	2015-11-28 06:26:05 PST	https://www.google.com/c	Google Chrome	google.com	Default	Computer	Chrome Browser
History	https://www.google.com/chrome/browser/desktop/index.html	2015-11-28 06:26:07 PST	https://www.google.com/c	Google Chrome	google.com	Default	Computer	Chrome Browser
History	https://www.google.com/chrome/browser/thankyou.html?platform=win	2015-11-28 06:26:26 PST	https://www.google.com/c	Google Chrome	google.com	Default	Computer	Chrome Browser

IMAGE 1: WEB SEARCH HISTORY



I think Allbery's suggestion is a good one. So please add this text

Source Name	E-Mail From	E-Mail To	Subject	Date Received	Message (Plaintext)	Message ID	Path	Thread ID	Data Source
USAGE	rms@gnu.org;	chet@nike.ins.cwru.edu;	Use of Readline	1999-07-22 17:37:46 PDT	should be the same as the...	Not available	USAGE	c2033d96-c3ec-4bf8-bc60-50367d3ba619	Computer2.E01

IMAGE 2: EMAIL MESSAGE

	Name	Modified Time	Change Ti	Access Tin	Created Ti	Size	Flags(Dir)	Flags(Met	Known	Location	MD5 Hash	SHA-256 H	MIME Typ	Extension
2	f_00000f	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
3	f_000010	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
4	f_000013	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
5	f_000015	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
6	f_000023	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
7	f_000024	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
8	f_000038	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
9	f_00004c	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
10	f_000060	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
11	f_000075	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
12	f_000085	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
13	f_00008a	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
14	f_00008c	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
15	f_00008e	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
16	f_0000a0	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
17	gl	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
18	nl	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
19	Temp	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
20	History-journal	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
21	Preferences	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
22	Safe Browsing Cookies	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
23	SqmWrapper.dll	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	applicatio	dll
24	{5A6CE3BF-741D-4BE	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	applicatio	png
25	iconcache_256.db	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	applicatio	db
26	Microsoft.Windows.Sh	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
27	TempState	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
28	AAA_SettingsGroupEa	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
29	AAA_SystemSettings_	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
30	AAA_SettingsGroupPe	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
31	AAA_SettingsPageAcc	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
32	AAA_SettingsPageDev	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
33	AAA_SettingsPageMa	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
34	AAA_SettingsPageNet	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
35	AAA_SettingsPagePriv	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
36	AAA_SettingsPageRes	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
37	AAA_SystemSettings_	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
38	AAA_SystemSettings_	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
39	AAA_SystemSettings_	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
40	AAA_SystemSettings_	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
41	AAA_SystemSettings_	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
42	AAA_SystemSettings_	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
43	AAA_SystemSettings_	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
44	AAA_SystemSettings_	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	
45	AAA_SystemSettings_	0000-00-00 00:00:00	0000-00-0	0000-00-0	0000-00-0	0	Unallocated		unknown	/img_Computer1.E01/vol_vol3/User	d41d8cd9	e3b0c442	application/octet-stream	

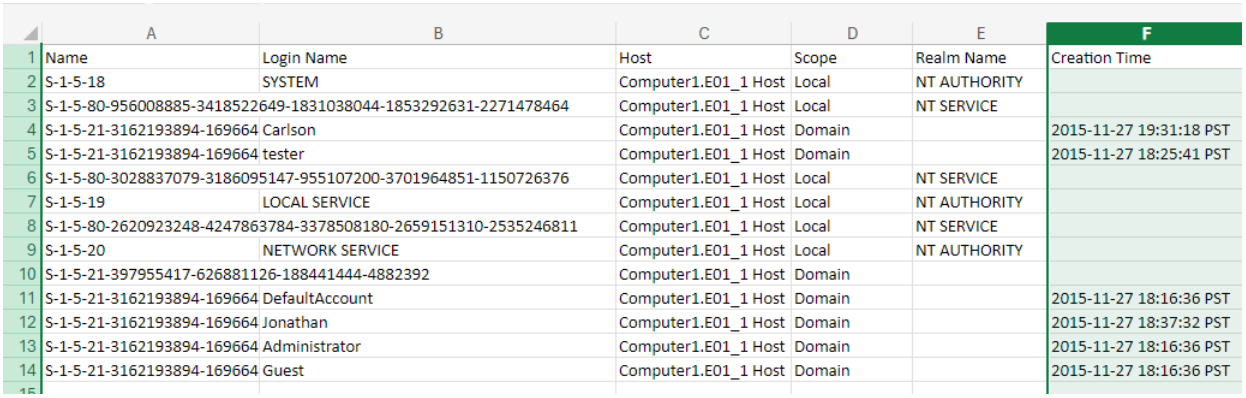
IMAGE 3: RECENTLY DEL FILES

	Source Na	Name	Program Name	Processor	Temporary File	Path	Product ID	Owner	Data Source
2	Computer	DESKTOP-	Windows 10 Pro	AMD64	%SystemRoot%	C:\Windows	00331-10000-000	tester	Computer1.E01

IMAGE 4: OS INFORMATION

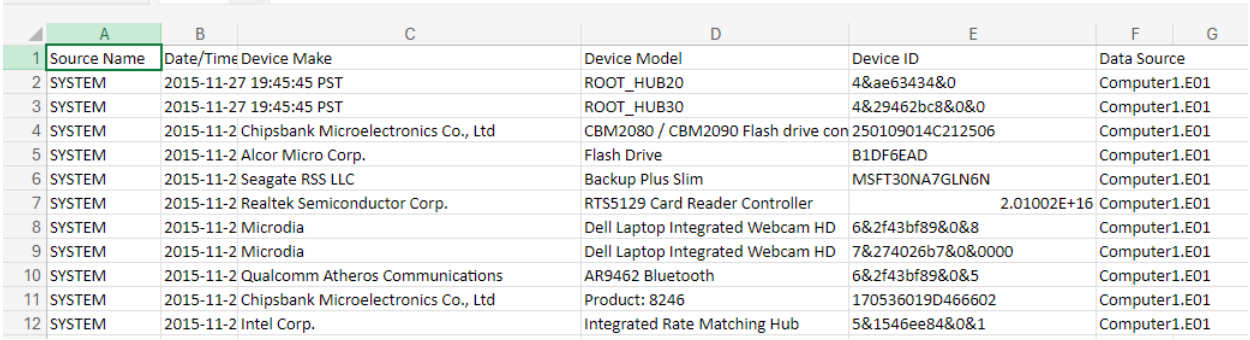
	Source Name	Program Name	Data Source
2	debian_version	Linux (Debian)	Computer2.E01
3	lsb-release	Linux (Ubuntu)	Computer2.E01

IMAGE 5: OS FOUND



	A	B	C	D	E	F
1	Name	Login Name	Host	Scope	Realm Name	Creation Time
2	S-1-5-18	SYSTEM	Computer1.E01_1 Host	Local	NT AUTHORITY	
3	S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464		Computer1.E01_1 Host	Local	NT SERVICE	
4	S-1-5-21-3162193894-169664	Carlson	Computer1.E01_1 Host	Domain		2015-11-27 19:31:18 PST
5	S-1-5-21-3162193894-169664	tester	Computer1.E01_1 Host	Domain		2015-11-27 18:25:41 PST
6	S-1-5-80-3028837079-3186095147-955107200-3701964851-1150726376		Computer1.E01_1 Host	Local	NT SERVICE	
7	S-1-5-19	LOCAL SERVICE	Computer1.E01_1 Host	Local	NT AUTHORITY	
8	S-1-5-80-2620923248-4247863784-3378508180-2659151310-2535246811		Computer1.E01_1 Host	Local	NT SERVICE	
9	S-1-5-20	NETWORK SERVICE	Computer1.E01_1 Host	Local	NT AUTHORITY	
10	S-1-5-21-397955417-626881126-188441444-4882392		Computer1.E01_1 Host	Domain		
11	S-1-5-21-3162193894-169664	DefaultAccount	Computer1.E01_1 Host	Domain		2015-11-27 18:16:36 PST
12	S-1-5-21-3162193894-169664	Jonathan	Computer1.E01_1 Host	Domain		2015-11-27 18:37:32 PST
13	S-1-5-21-3162193894-169664	Administrator	Computer1.E01_1 Host	Domain		2015-11-27 18:16:36 PST
14	S-1-5-21-3162193894-169664	Guest	Computer1.E01_1 Host	Domain		2015-11-27 18:16:36 PST

IMAGE 6: OPERATING SYSTEM ACCOUNTS



	A	B	C	D	E	F	G
1	Source Name	Date/Time	Device Make	Device Model	Device ID	Data Source	
2	SYSTEM	2015-11-27	19:45:45 PST	ROOT_HUB20	4&ae63434&0	Computer1.E01	
3	SYSTEM	2015-11-27	19:45:45 PST	ROOT_HUB30	4&29462bc8&0&0	Computer1.E01	
4	SYSTEM	2015-11-2	Chipsbank Microelectronics Co., Ltd	CBM2080 / CBM2090 Flash drive con	250109014C212506	Computer1.E01	
5	SYSTEM	2015-11-2	Alcor Micro Corp.	Flash Drive	B1DF6EAD	Computer1.E01	
6	SYSTEM	2015-11-2	Seagate RSS LLC	Backup Plus Slim	MSFT30NA7GLN6N	Computer1.E01	
7	SYSTEM	2015-11-2	Realtek Semiconductor Corp.	RTS5129 Card Reader Controller	2.01002E+16	Computer1.E01	
8	SYSTEM	2015-11-2	Microdia	Dell Laptop Integrated Webcam HD	6&2f43bf89&0&8	Computer1.E01	
9	SYSTEM	2015-11-2	Microdia	Dell Laptop Integrated Webcam HD	7&274026b7&0&0000	Computer1.E01	
10	SYSTEM	2015-11-2	Qualcomm Atheros Communications	AR9462 Bluetooth	6&2f43bf89&0&5	Computer1.E01	
11	SYSTEM	2015-11-2	Chipsbank Microelectronics Co., Ltd	Product: 8246	170536019D466602	Computer1.E01	
12	SYSTEM	2015-11-2	Intel Corp.	Integrated Rate Matching Hub	5&1546ee84&0&1	Computer1.E01	

IMAGE 7: ATTACHED DEVICES

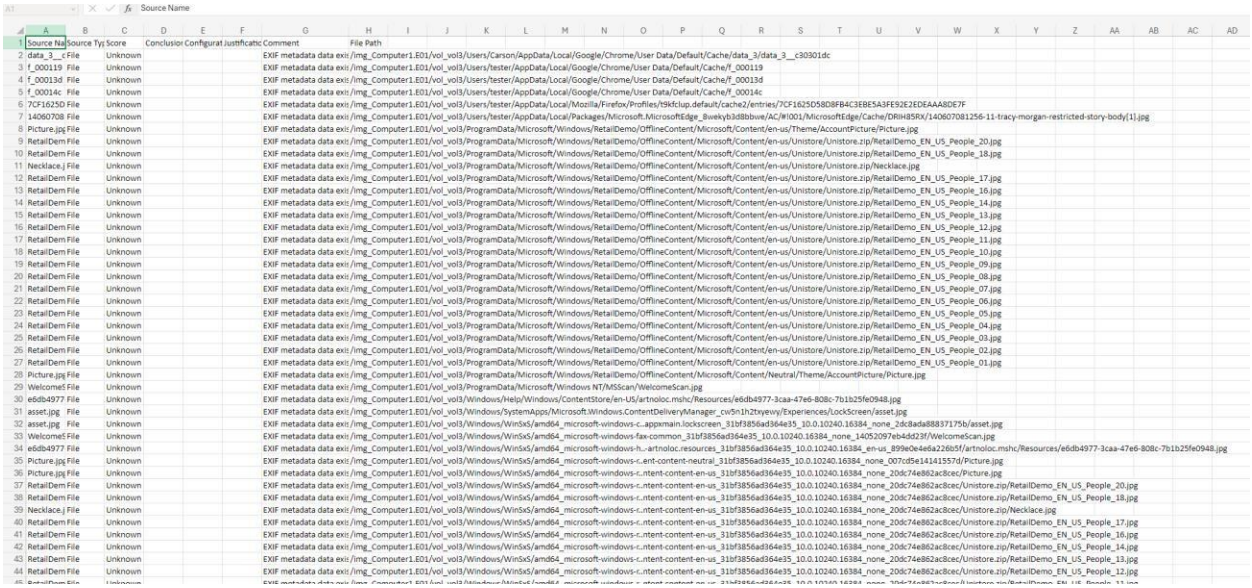
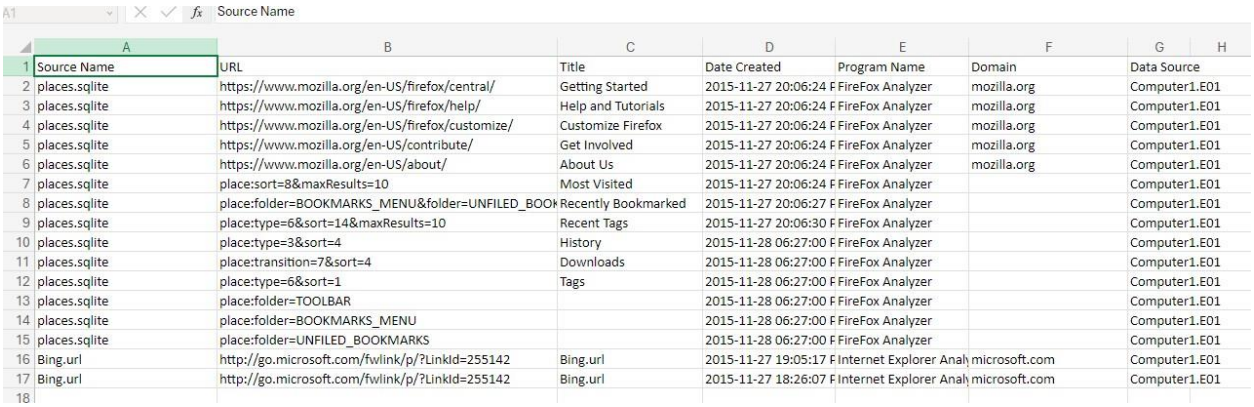
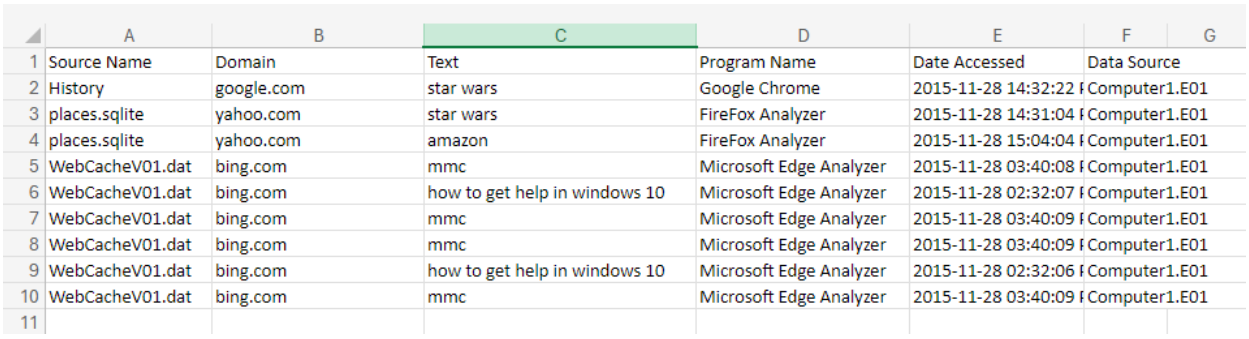


IMAGE 8: USERS CONTENT SUSPECTED



Source Name	URL	Title	Date Created	Program Name	Domain	Data Source
places.sqlite	https://www.mozilla.org/en-US/firefox/central/	Getting Started	2015-11-27 20:06:24 F	FireFox Analyzer	mozilla.org	Computer1.E01
places.sqlite	https://www.mozilla.org/en-US/firefox/help/	Help and Tutorials	2015-11-27 20:06:24 F	FireFox Analyzer	mozilla.org	Computer1.E01
places.sqlite	https://www.mozilla.org/en-US/firefox/customize/	Customize Firefox	2015-11-27 20:06:24 F	FireFox Analyzer	mozilla.org	Computer1.E01
places.sqlite	https://www.mozilla.org/en-US/contribute/	Get Involved	2015-11-27 20:06:24 F	FireFox Analyzer	mozilla.org	Computer1.E01
places.sqlite	https://www.mozilla.org/en-US/about/	About Us	2015-11-27 20:06:24 F	FireFox Analyzer	mozilla.org	Computer1.E01
places.sqlite	place:sort=8&maxResults=10	Most Visited	2015-11-27 20:06:24 F	FireFox Analyzer		Computer1.E01
places.sqlite	place:folder=BOOKMARKS_MENU&folder=UNFILED_BOOK	Recently Bookmarked	2015-11-27 20:06:27 F	FireFox Analyzer		Computer1.E01
places.sqlite	place:type=6&sort=14&maxResults=10	Recent Tags	2015-11-27 20:06:30 F	FireFox Analyzer		Computer1.E01
places.sqlite	place:type=3&sort=4	History	2015-11-28 06:27:00 F	FireFox Analyzer		Computer1.E01
places.sqlite	place:transition=7&sort=4	Downloads	2015-11-28 06:27:00 F	FireFox Analyzer		Computer1.E01
places.sqlite	place:type=6&sort=1	Tags	2015-11-28 06:27:00 F	FireFox Analyzer		Computer1.E01
places.sqlite	place:folder=TOOLBAR		2015-11-28 06:27:00 F	FireFox Analyzer		Computer1.E01
places.sqlite	place:folder=BOOKMARKS_MENU		2015-11-28 06:27:00 F	FireFox Analyzer		Computer1.E01
places.sqlite	place:folder=UNFILED_BOOKMARKS		2015-11-28 06:27:00 F	FireFox Analyzer		Computer1.E01
Bing.url	http://go.microsoft.com/fwlink/p/?LinkId=255142	Bing.url	2015-11-27 19:05:17 F	Internet Explorer Analy	microsoft.com	Computer1.E01
Bing.url	http://go.microsoft.com/fwlink/p/?LinkId=255142	Bing.url	2015-11-27 18:26:07 F	Internet Explorer Analy	microsoft.com	Computer1.E01

IMAGE 9: WEB BOOKMARKS



Source Name	Domain	Text	Program Name	Date Accessed	Data Source
History	google.com	star wars	Google Chrome	2015-11-28 14:32:22 F	Computer1.E01
places.sqlite	yahoo.com	star wars	FireFox Analyzer	2015-11-28 14:31:04 F	Computer1.E01
places.sqlite	yahoo.com	amazon	FireFox Analyzer	2015-11-28 15:04:04 F	Computer1.E01
WebCacheV01.dat	bing.com	mmc	Microsoft Edge Analyzer	2015-11-28 03:40:08 F	Computer1.E01
WebCacheV01.dat	bing.com	how to get help in windows 10	Microsoft Edge Analyzer	2015-11-28 02:32:07 F	Computer1.E01
WebCacheV01.dat	bing.com	mmc	Microsoft Edge Analyzer	2015-11-28 03:40:09 F	Computer1.E01
WebCacheV01.dat	bing.com	mmc	Microsoft Edge Analyzer	2015-11-28 03:40:09 F	Computer1.E01
WebCacheV01.dat	bing.com	how to get help in windows 10	Microsoft Edge Analyzer	2015-11-28 02:32:06 F	Computer1.E01
WebCacheV01.dat	bing.com	mmc	Microsoft Edge Analyzer	2015-11-28 03:40:09 F	Computer1.E01

IMAGE 10: WEB SEARCHES CONTENT

7.EVIDENCE AND FIGURES :

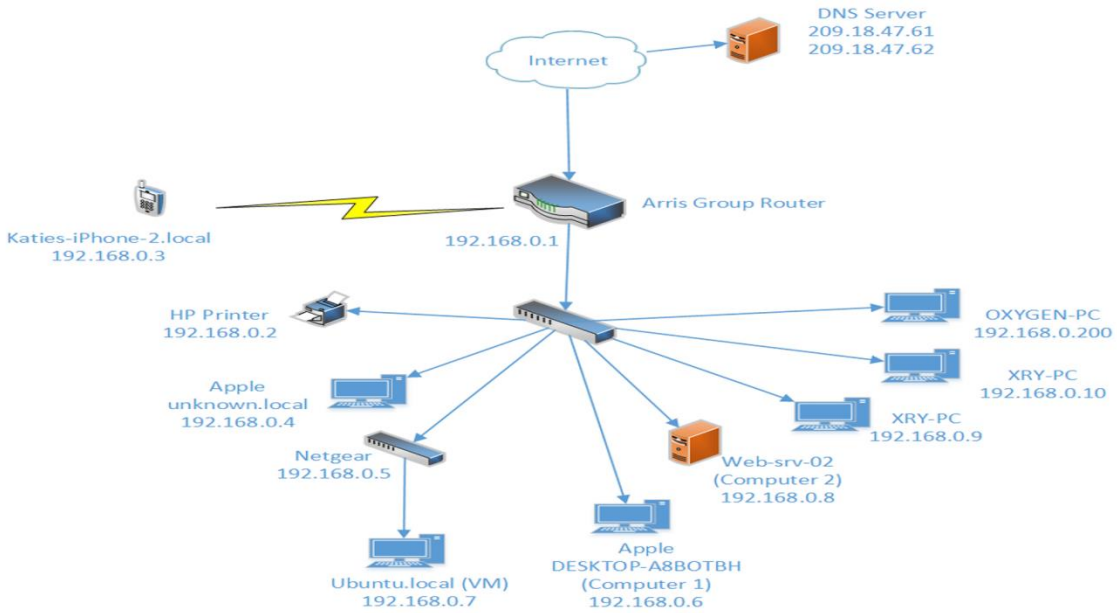


Figure 1: NETWORK DESIGN OF THE HITEK COMPANY

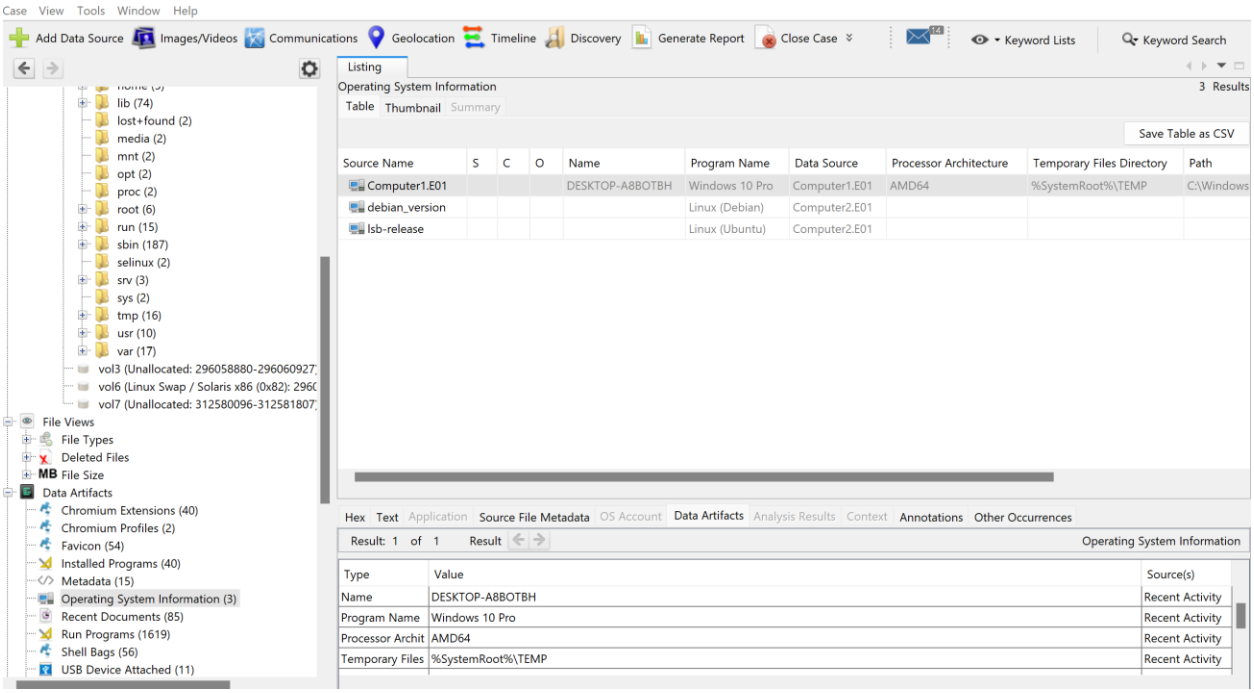


FIGURE 2: SYSTEM INFORMATION OF COMPUTER1

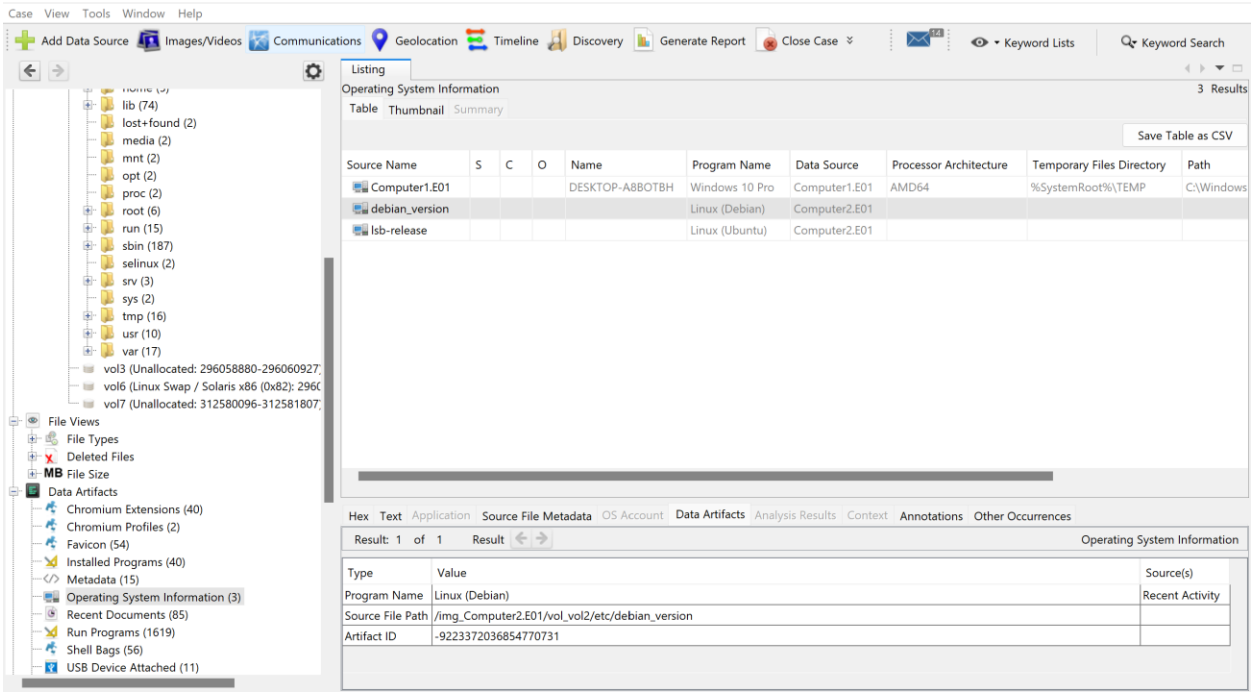


FIGURE 3: SYSTEM INFORMATION OF COMPUTER2

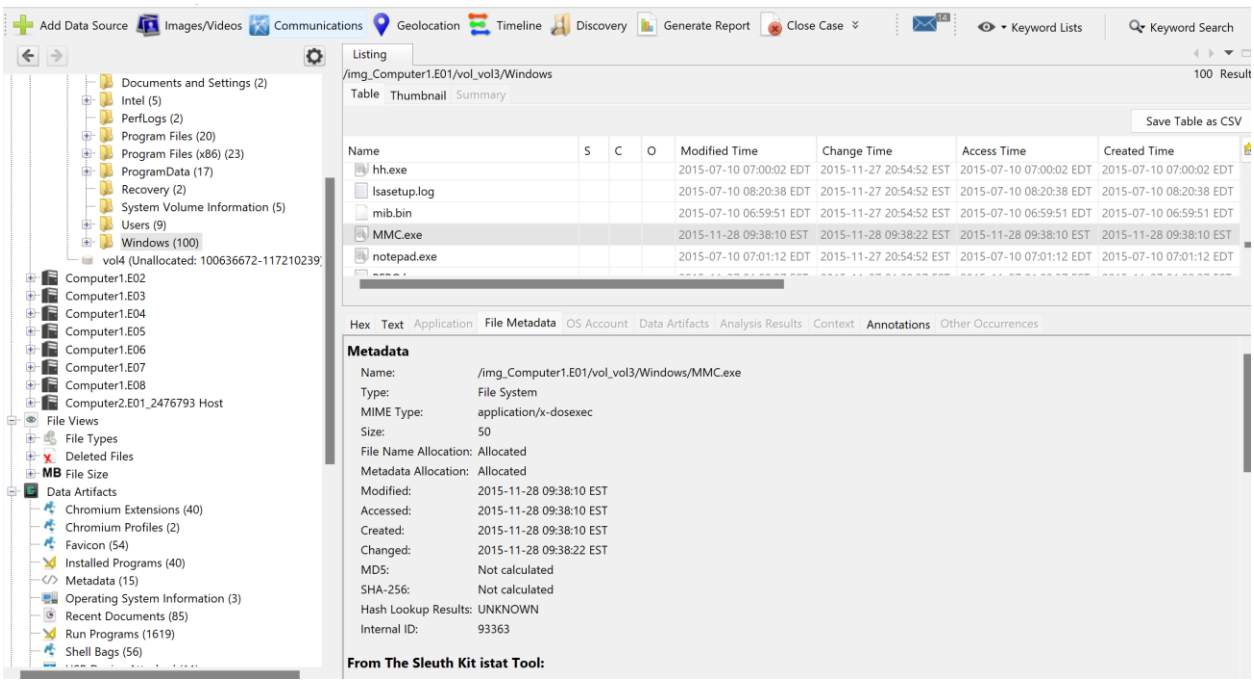


FIGURE 4: MMC.EXE FILE

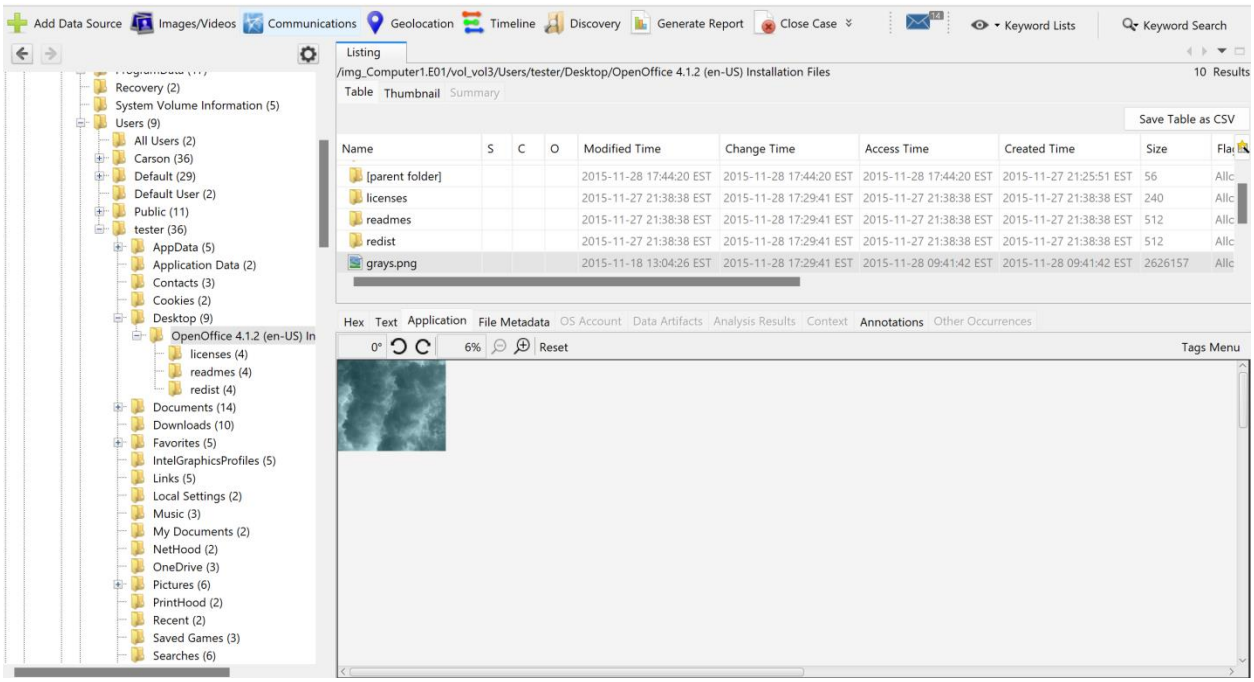


FIGURE 5: GRAYS.PNG FILE

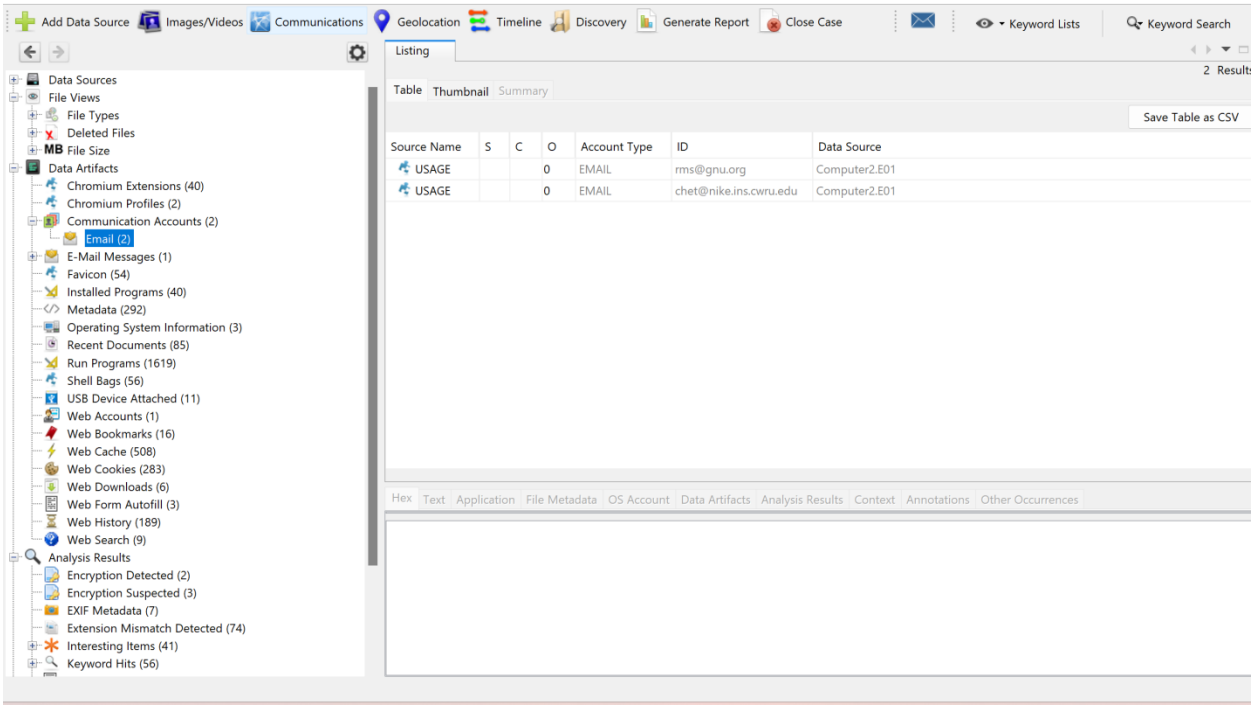


FIGURE 6: SUSPICIOUS EMAILS FOUND

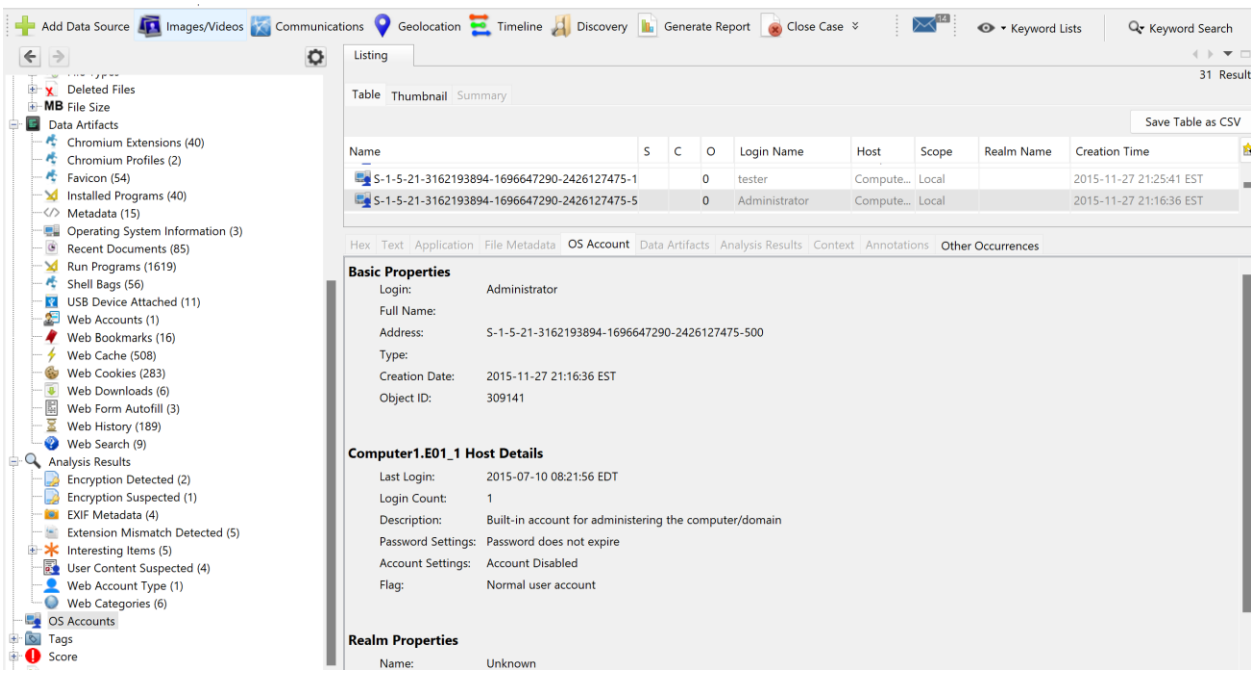


FIGURE 7: USER ACCOUNT OF ADMINISTRATOR

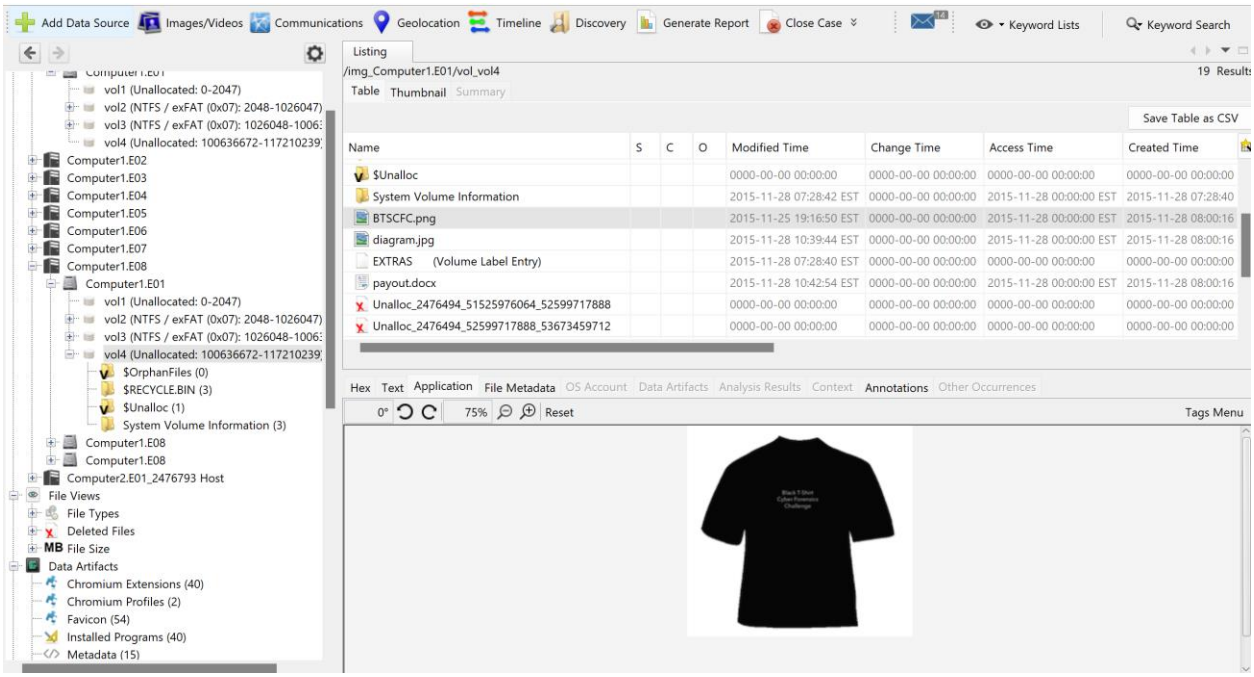


FIGURE 8: SUSPICIOUS IMAGE

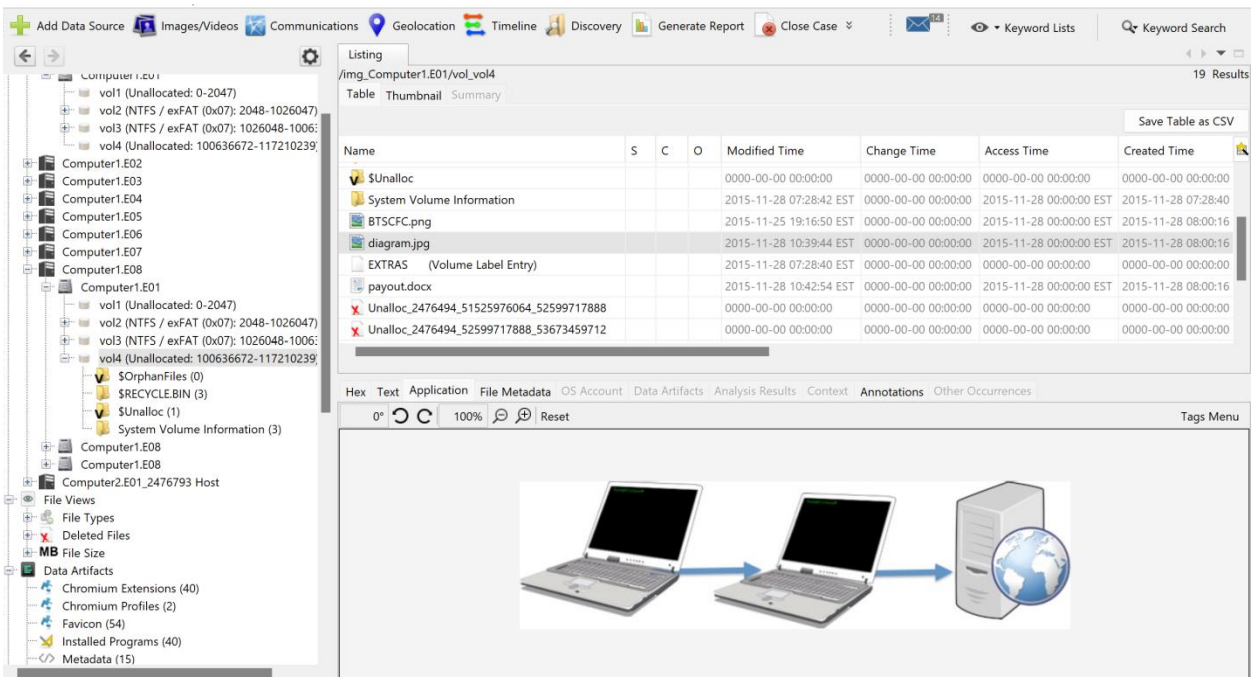


FIGURE 9: SUSPICIOUS IMAGE

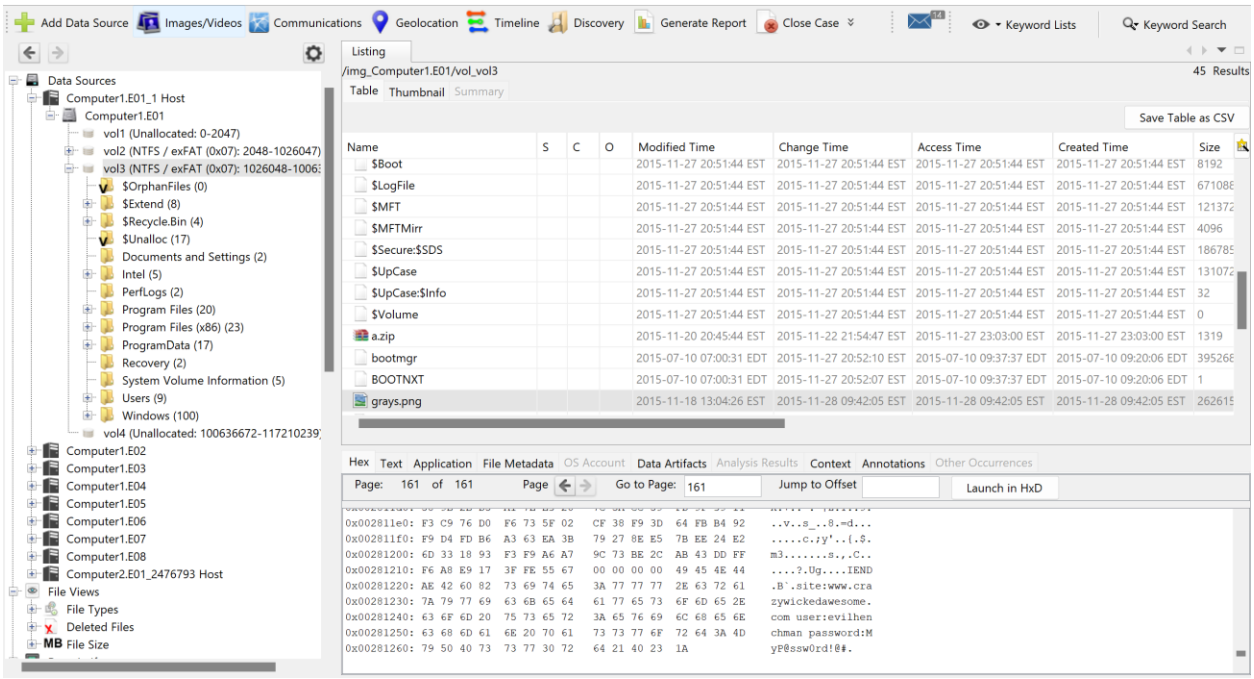


FIGURE 10: HIDDEN LOGIN CREDENTIALS FOR CRAZYWICKEDAWESOME.COM IN HEXCODE

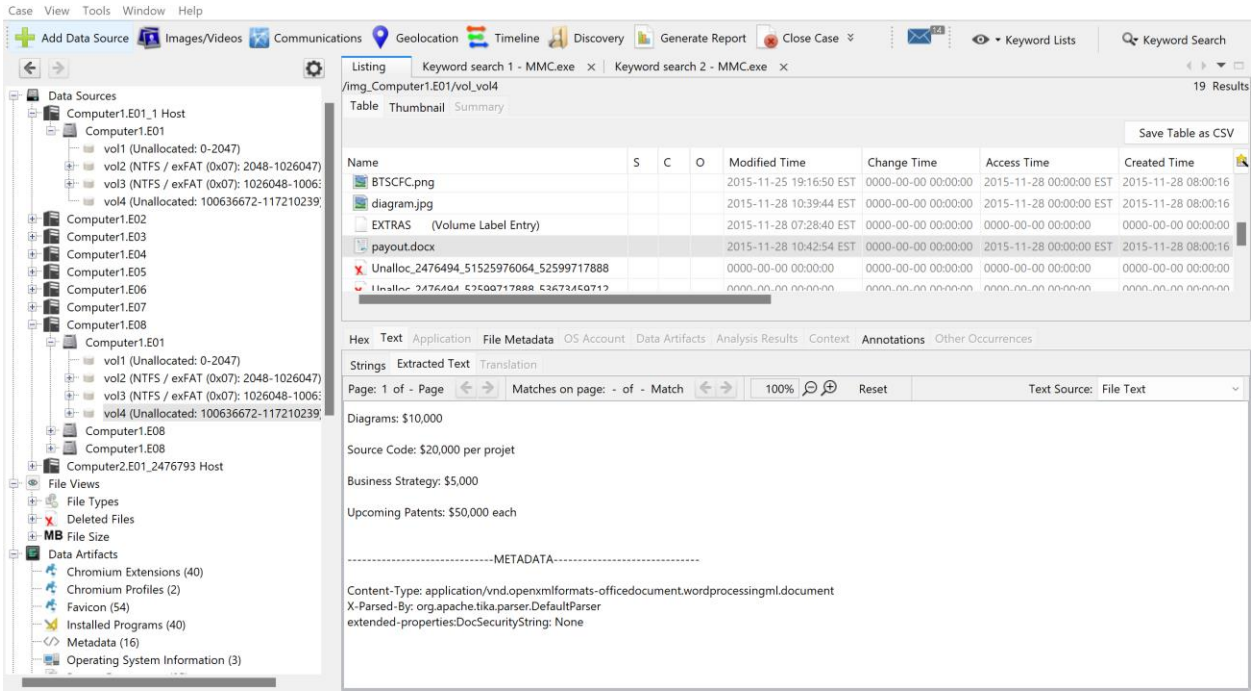


FIGURE 11: PAYOUT.DOCX

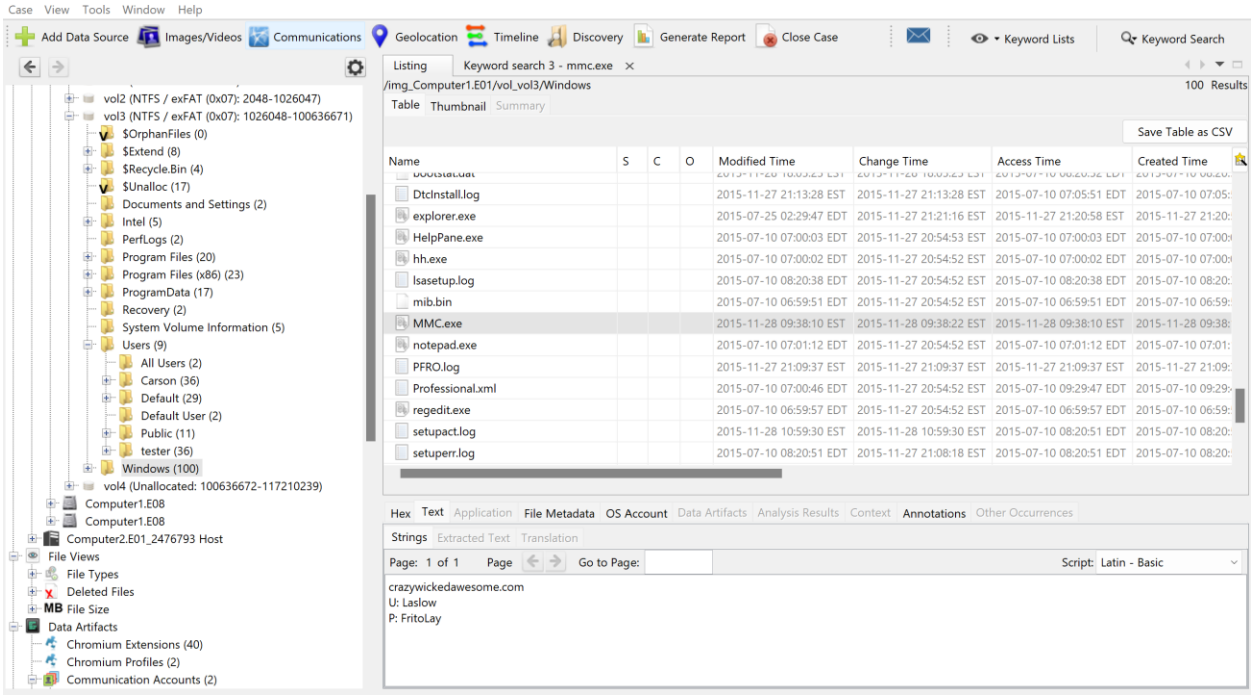


FIGURE 12: LOGIN DETAILS ARE CONTAIN IN EXECUTABLE FILE FOR CRAZYWICKEDAWESOME.COM

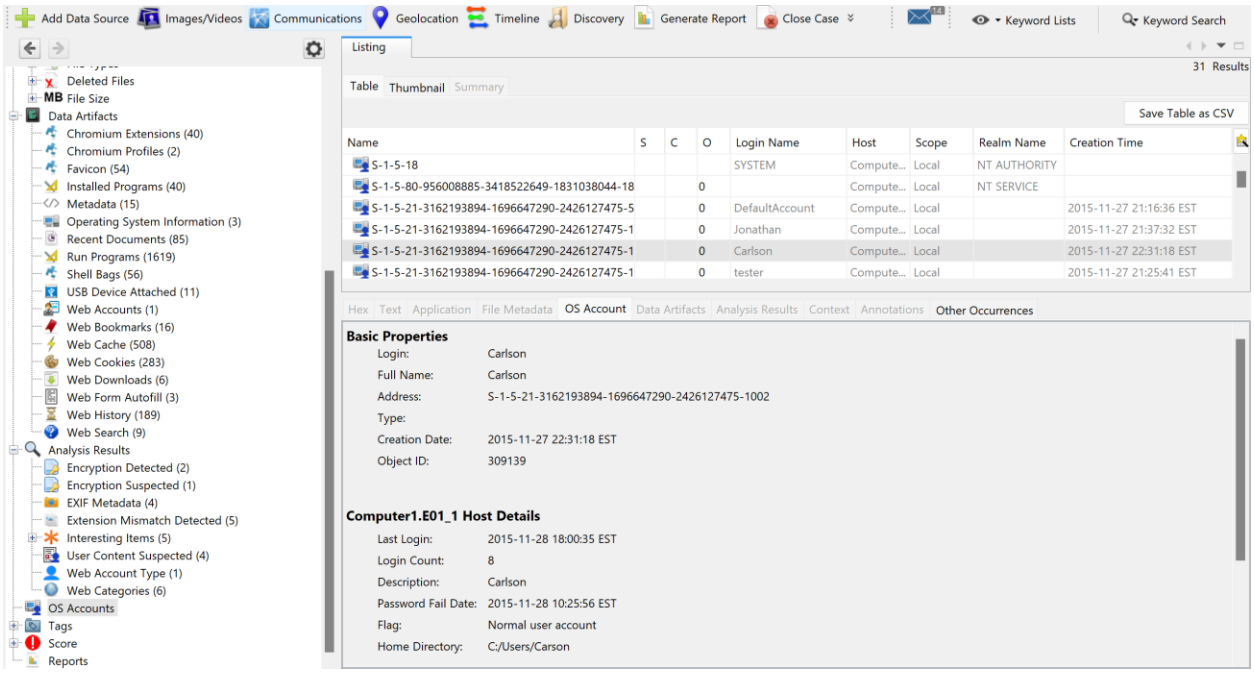


FIGURE 13: USER ACCOUNT OF CARLSON

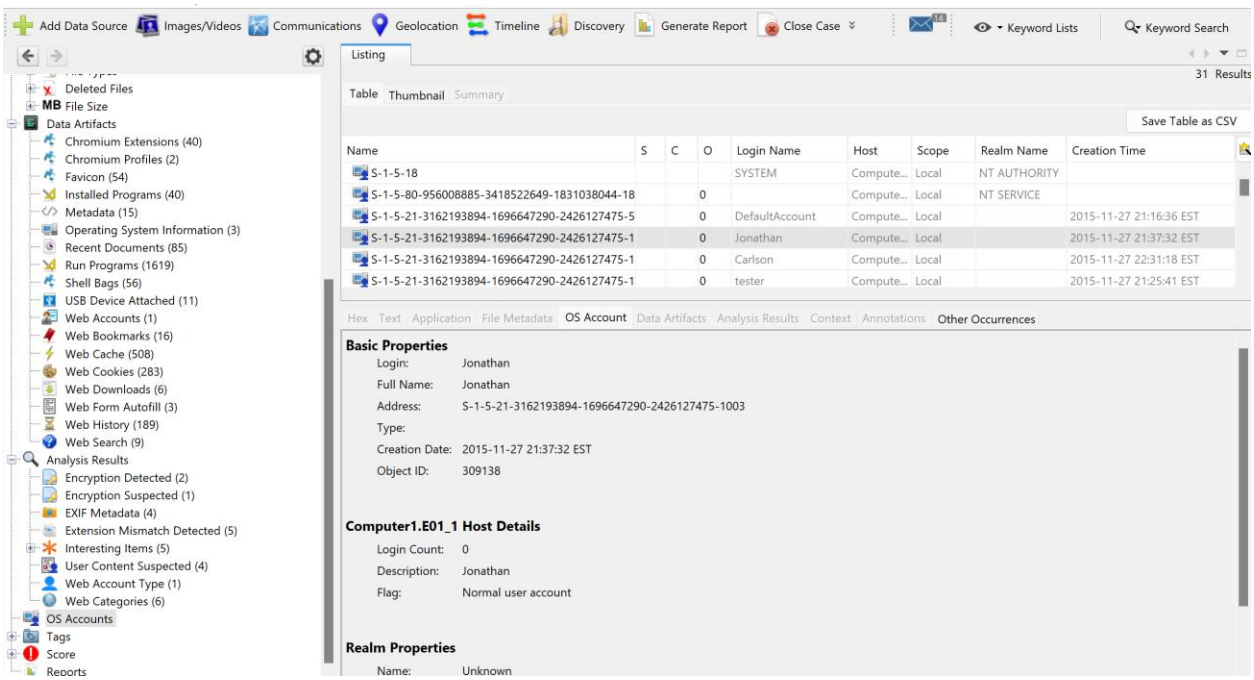


FIGURE 14: USER ACCOUNT OF JONATHAN

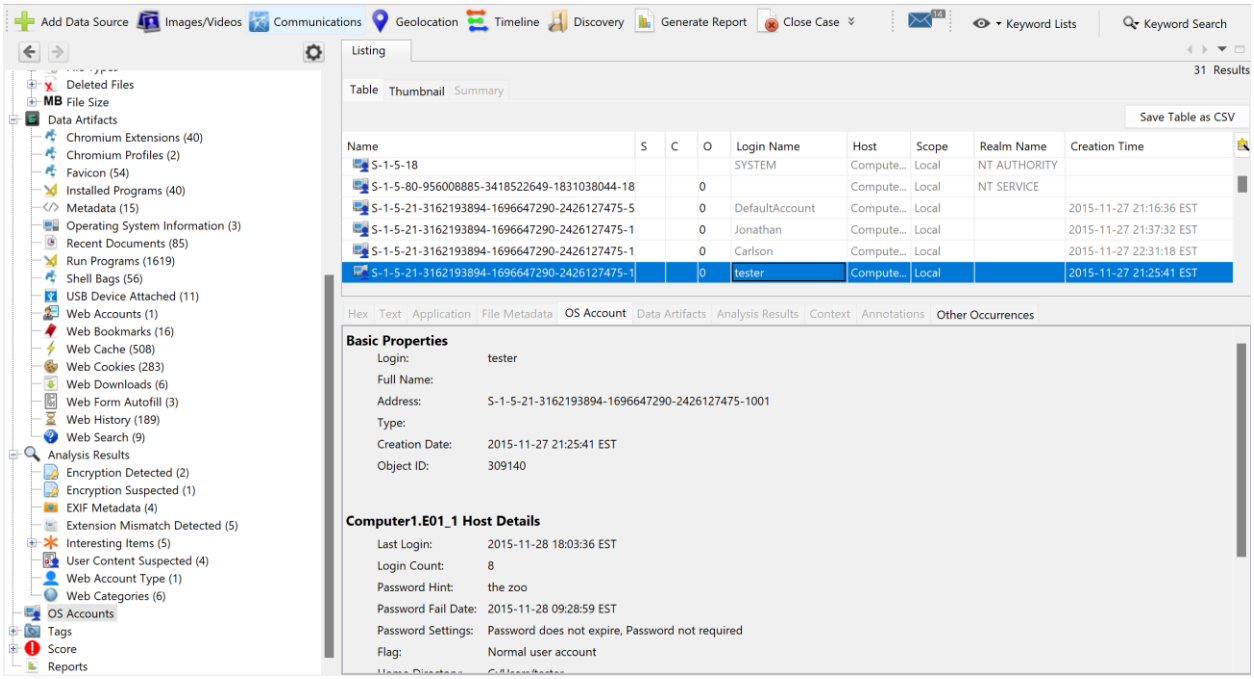


FIGURE 15: USER ACCOUNT OF TESTER

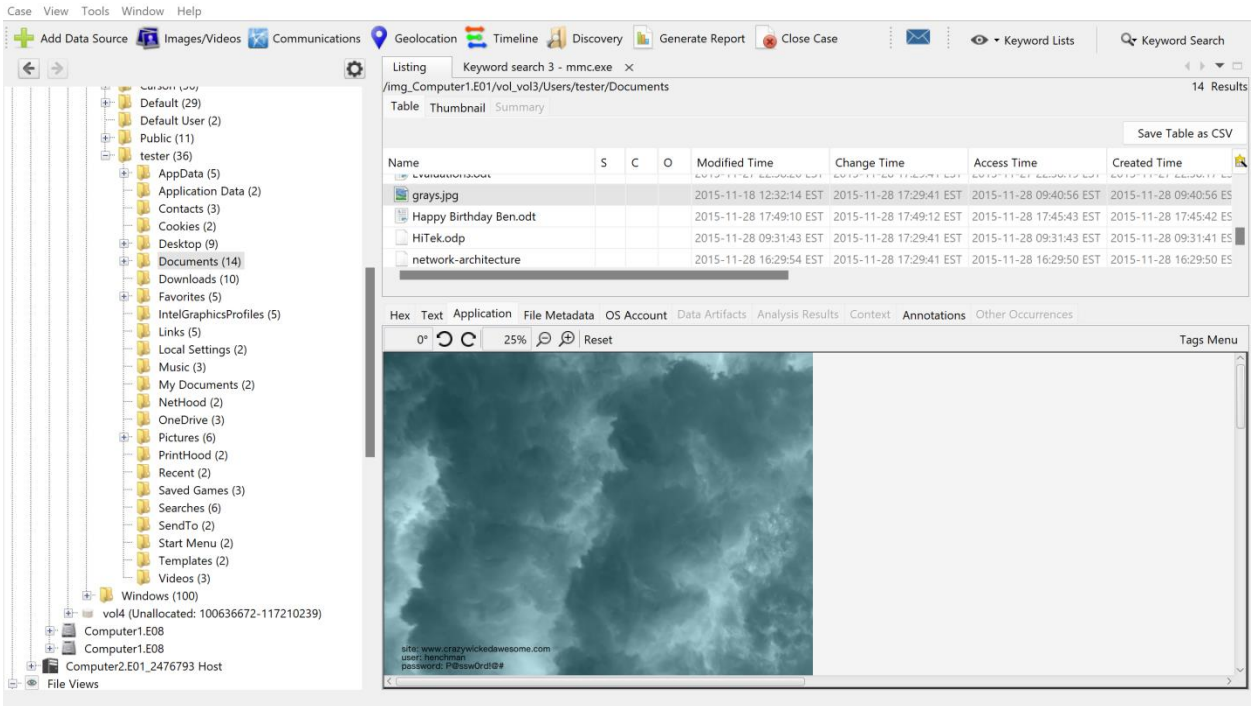


FIGURE 16: LOGIN CREDENTIALS FOR CRAZYWICKEDAWESOME.COM IN PICTURE

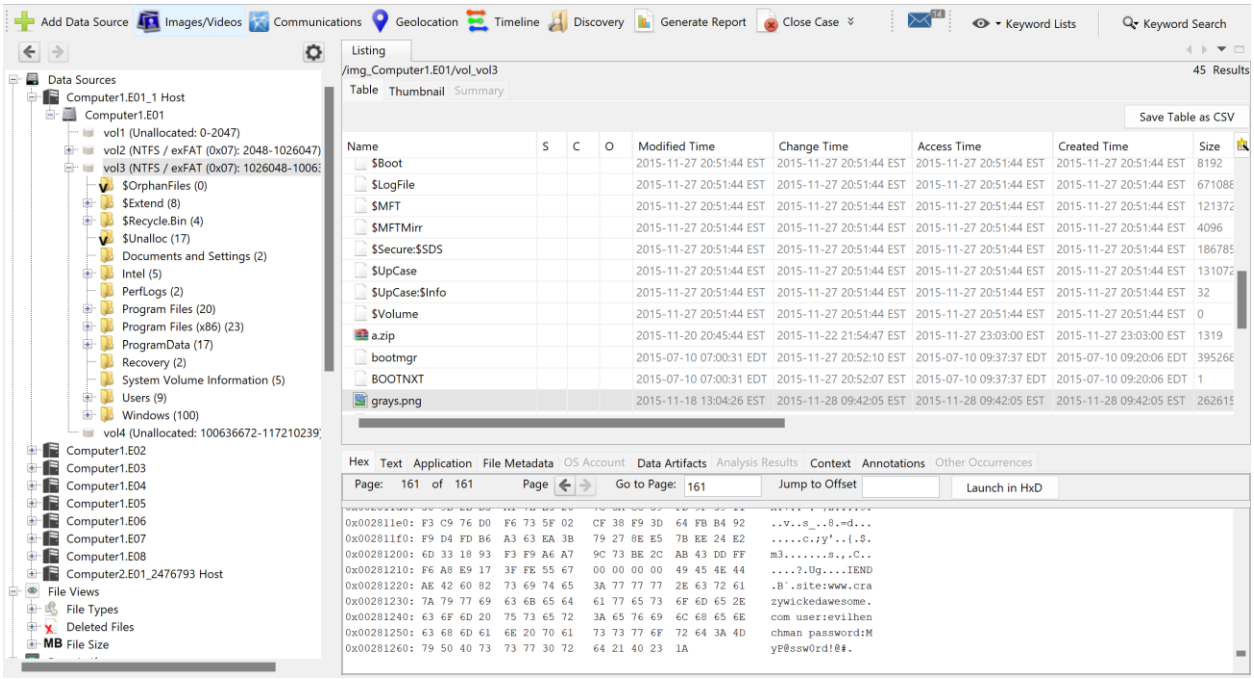


FIGURE 17: HIDDEN LOGIN CREDENTIALS FOR CRAZYWICKEDAWESOME.COM IN HEXCODE

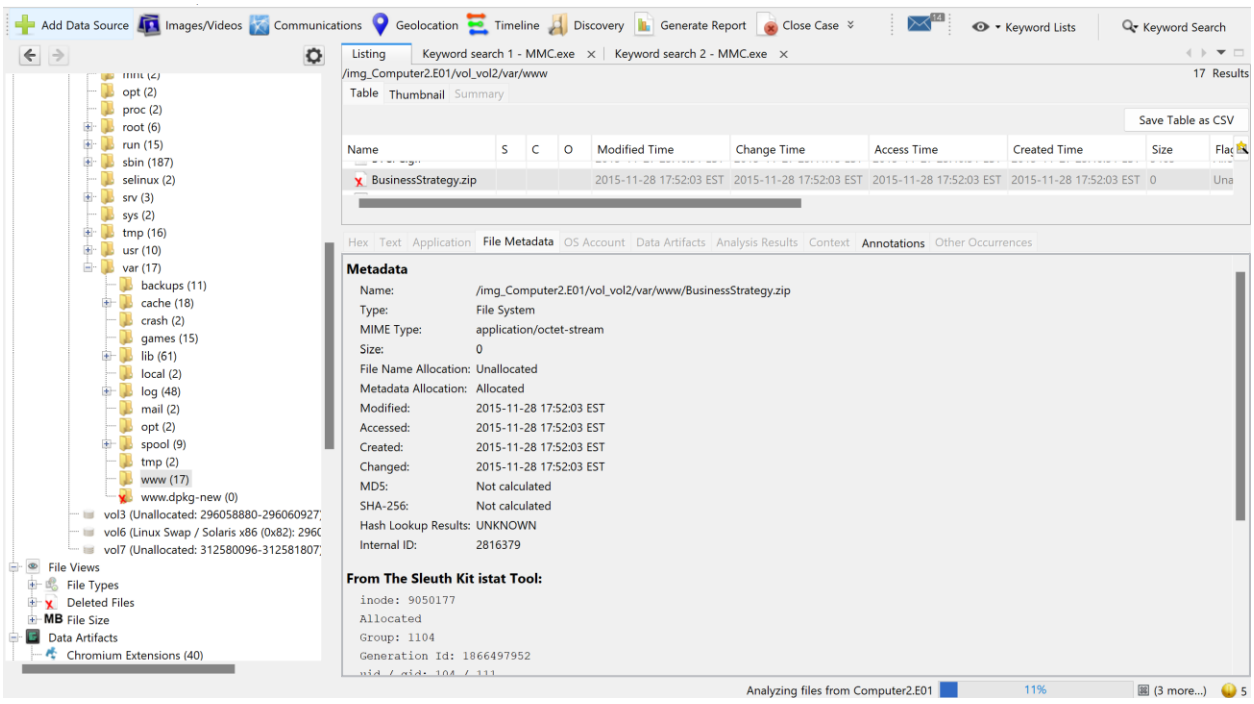


FIGURE 18: USER ACCOUNTS OF COMPUTER 2

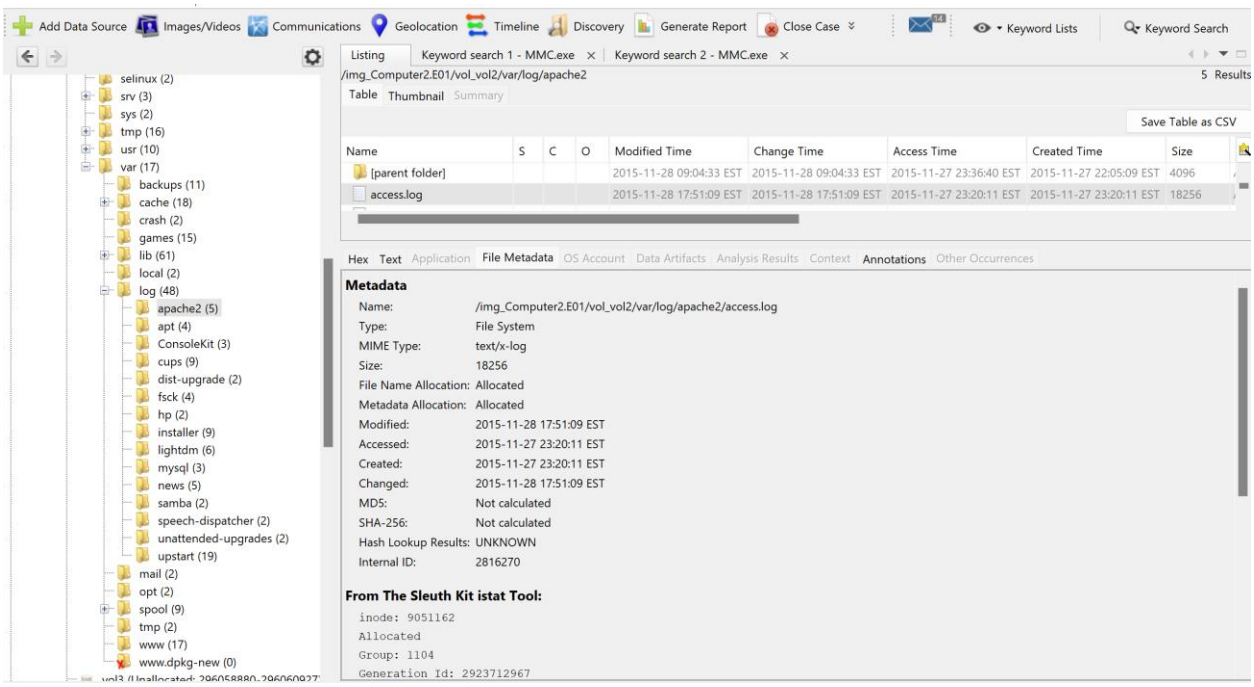


FIGURE 19: ACCESS LOG FILES FROM COMPUTER2

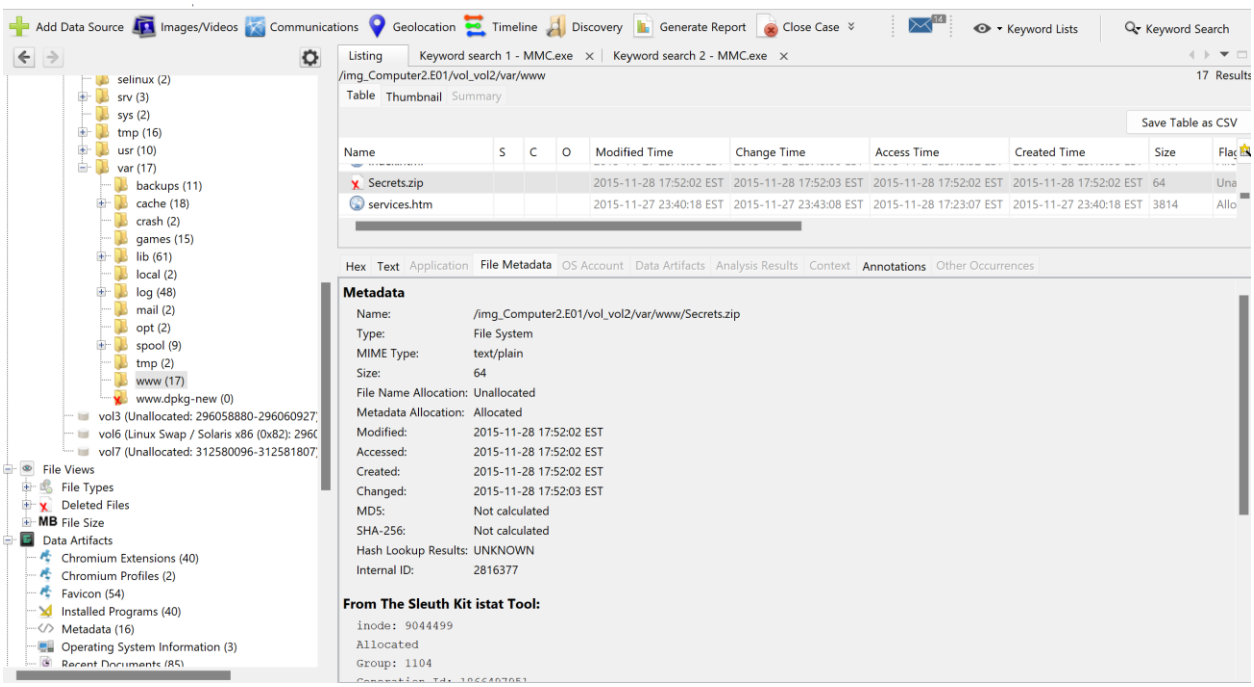


FIGURE 20: SECRET.ZIP FILE FROM COMPUTER2

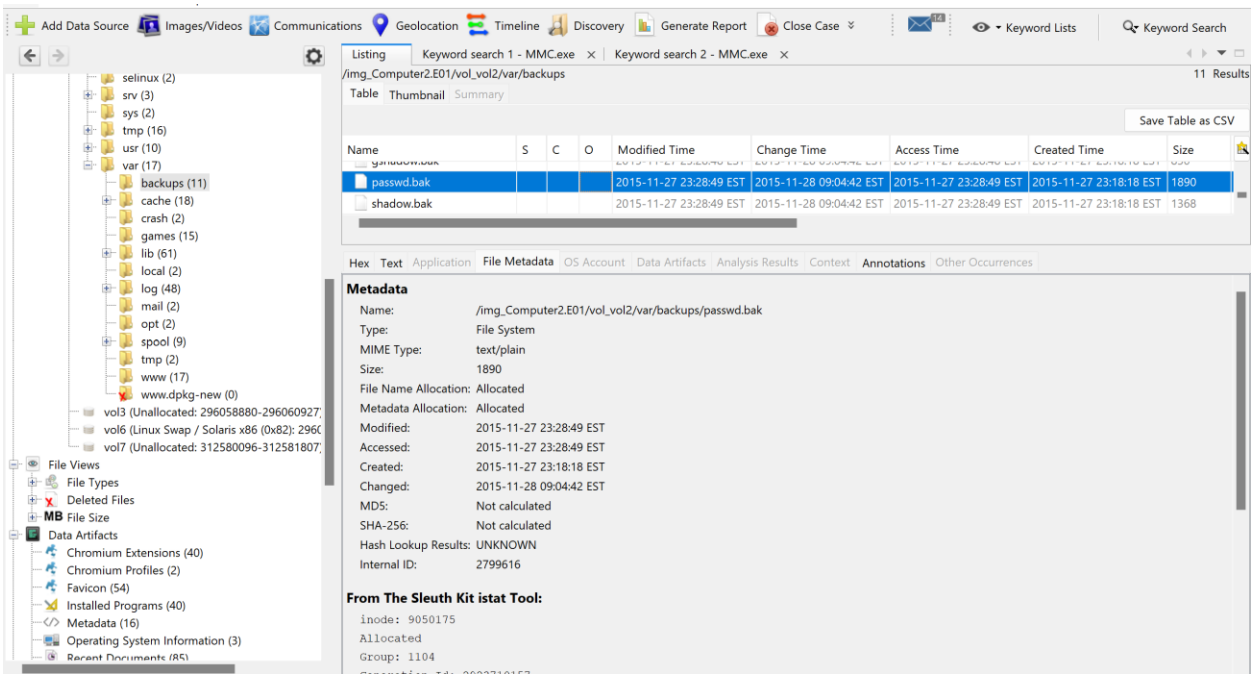


FIGURE 21: SHADOW FILES FROM COMPUTER2

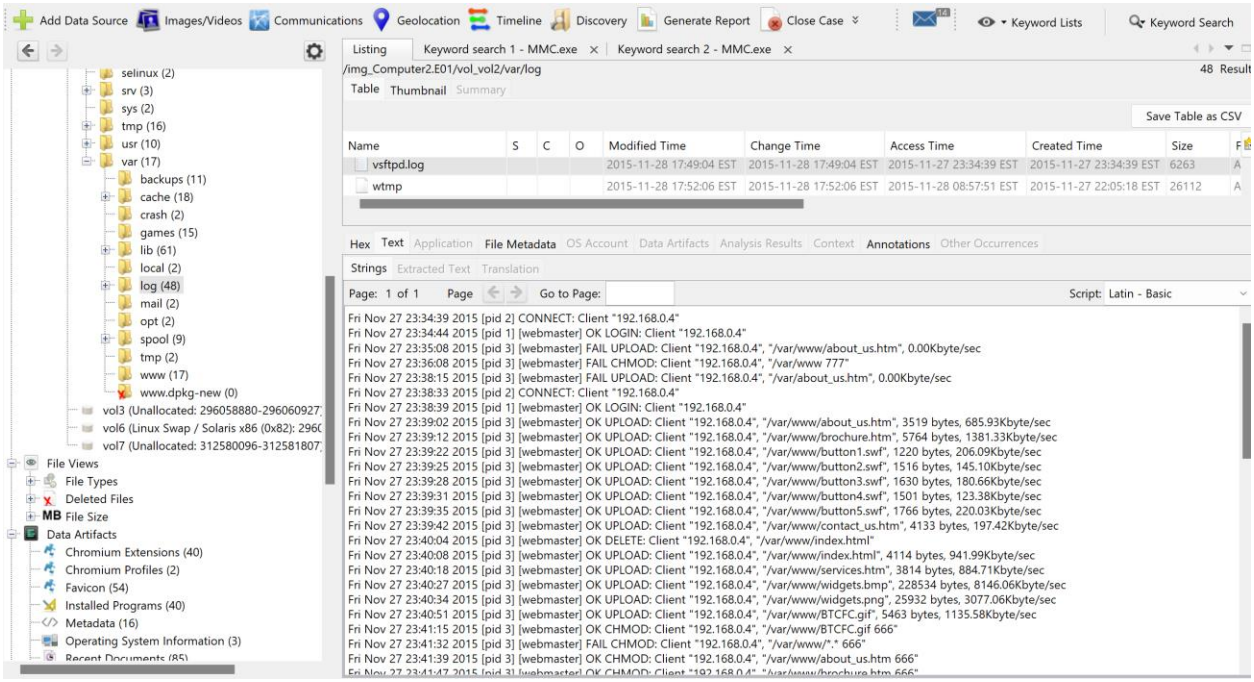


FIGURE 22: VSFTPD.LOG FILES FROM COMPUTER2

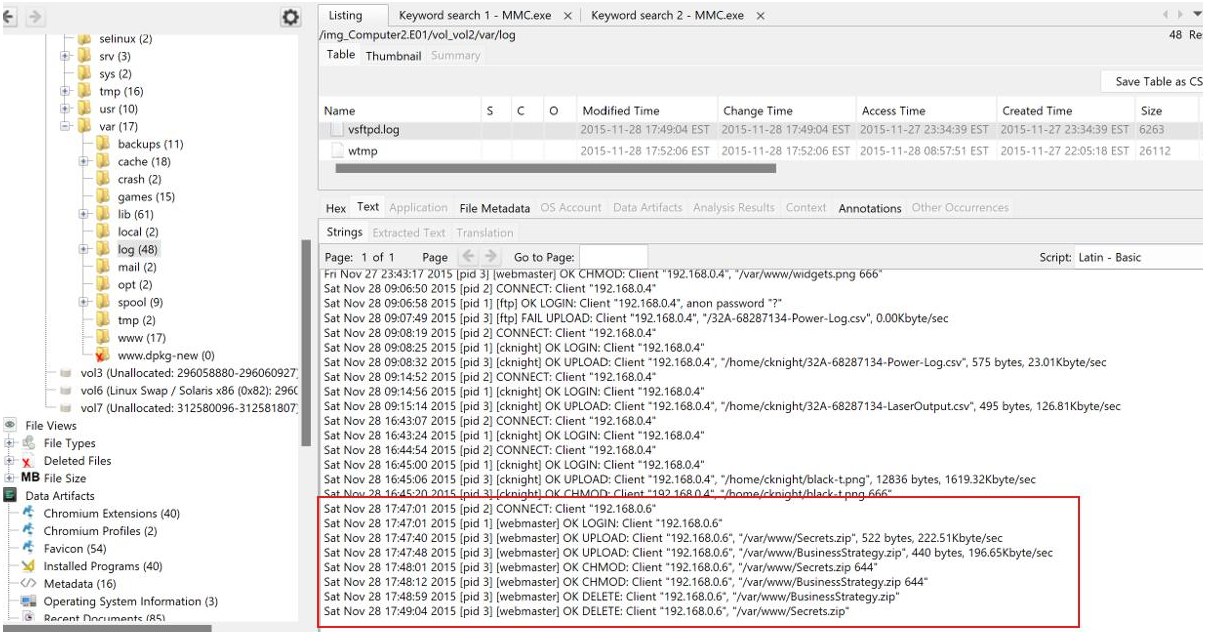


FIGURE 23: ACTIVITY OF USER "WEBMASTER" FOUND IN VSFTPD.LOG

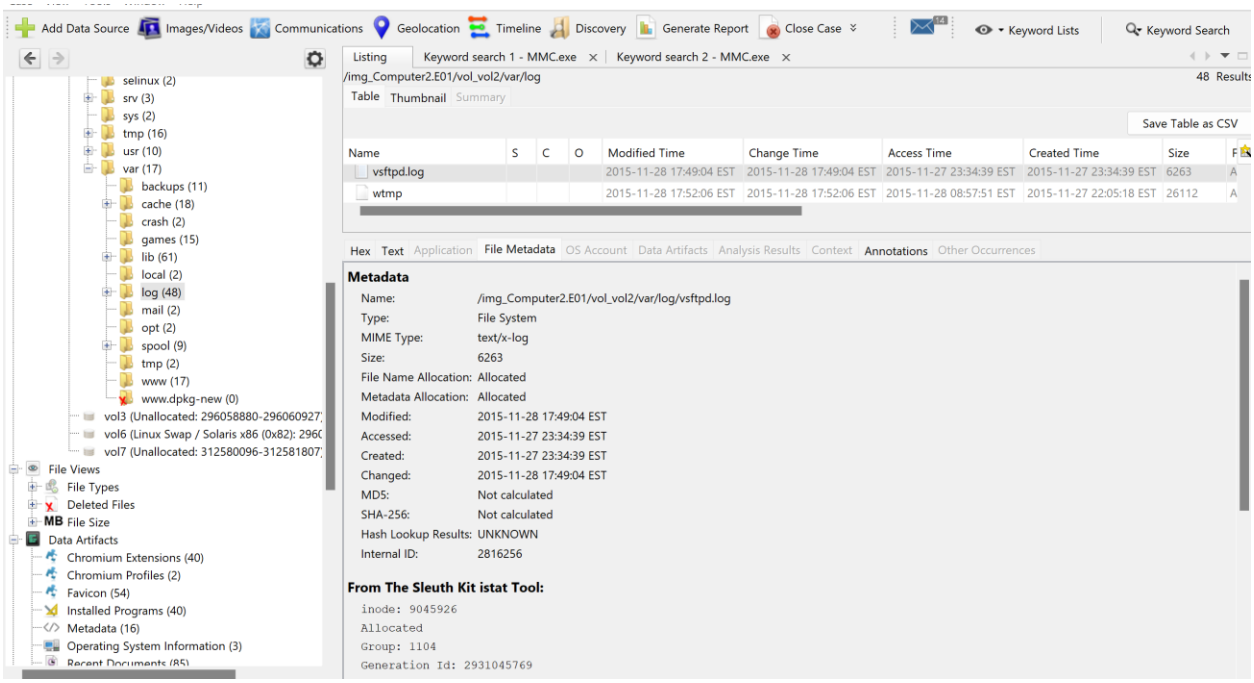


FIGURE 24: FILE METADATA OBSERVED IN THE VSFTPD.LOG

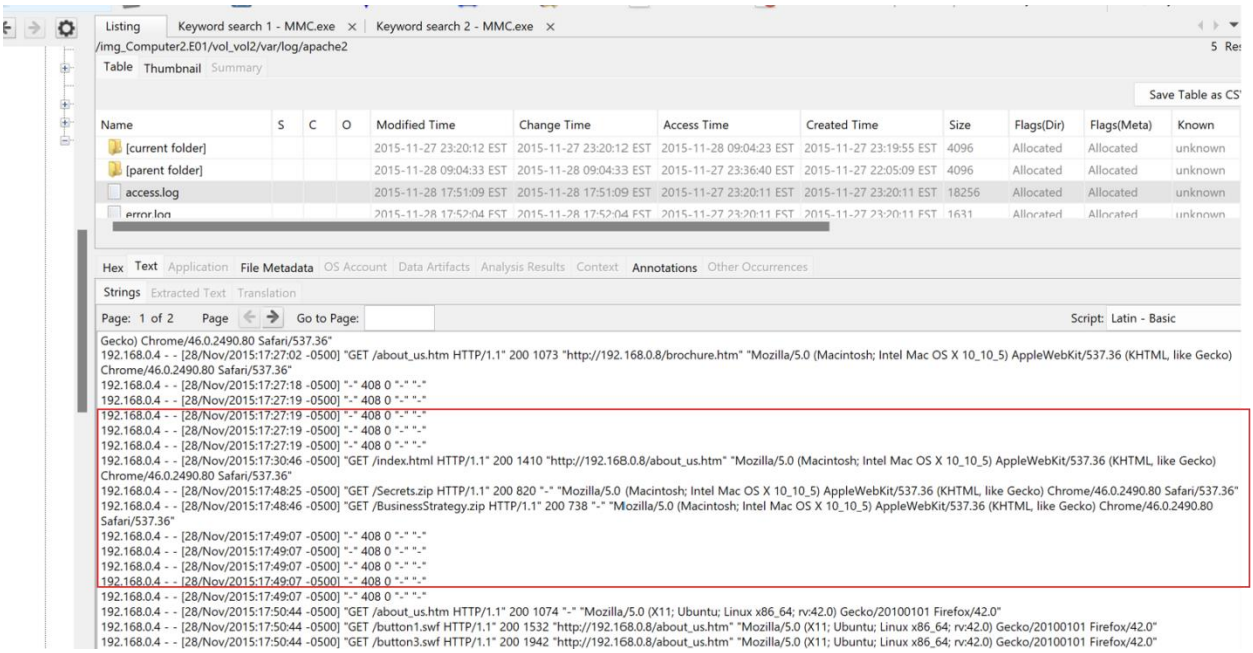


FIGURE 25: ACTIVITY OF DOWNLOADING "BUSINESSSTRATEGY.ZIP" AND "SECRET.ZIP"

```
GET /button4.swf HTTP/1.1
Host: 192.168.0.8
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:42.0) Gecko/20100101 Firefox/42.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.8/
Connection: keep-alive
```

FIGURE 26: HTTP REQUEST EXPLOITING VULNERABILITY IN [VULNERABILITY NAME]

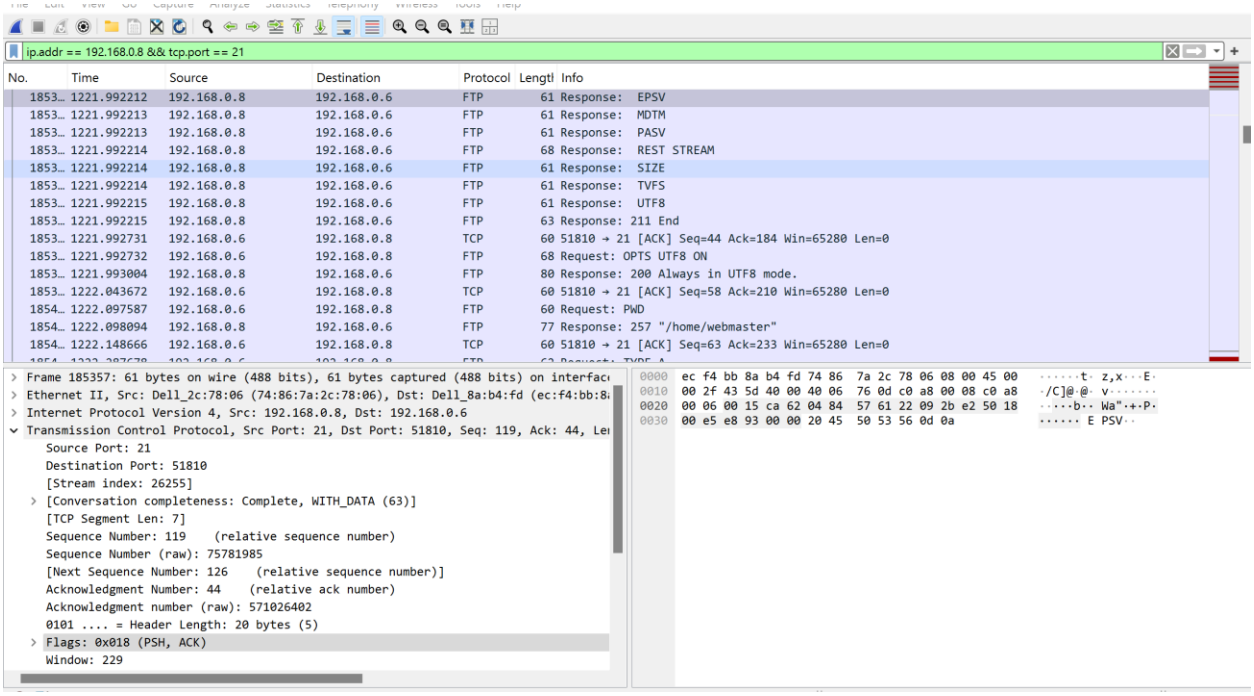


FIGURE 27: FTP DATA TRANSFER SESSION

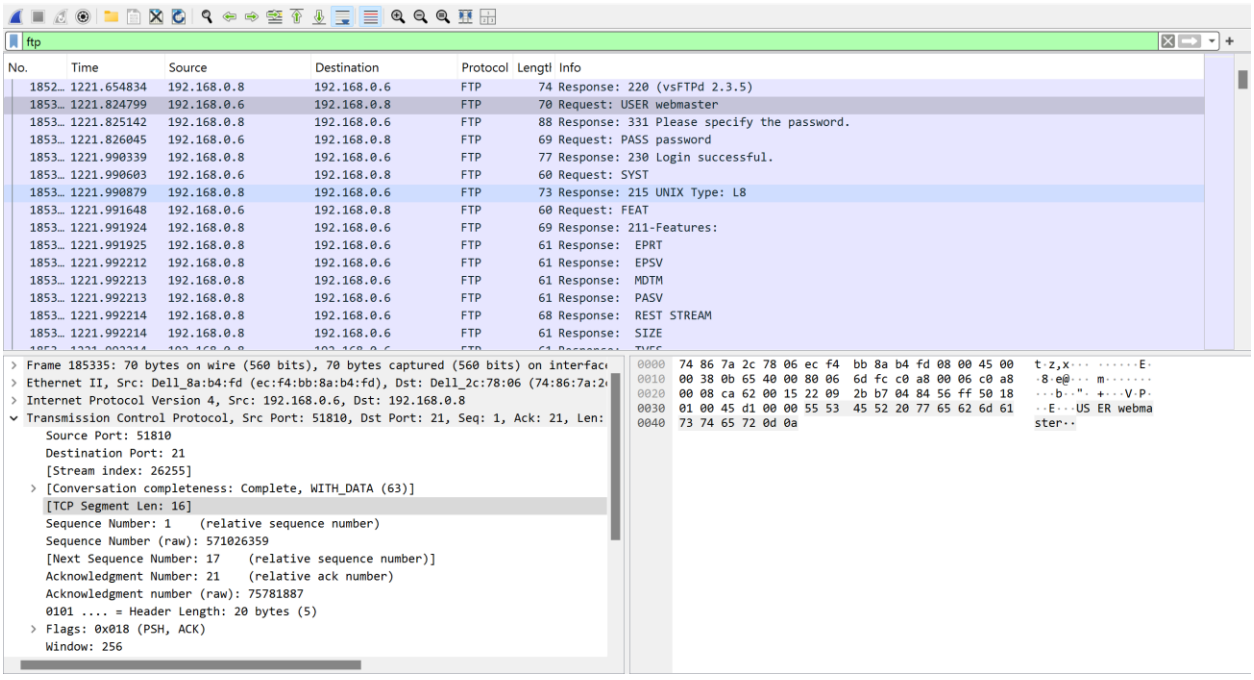


FIGURE 28: FTP LOGIN AUTHENTICATION AND COMMAND EXCHANGE (WIRESHARK ANALYSIS)

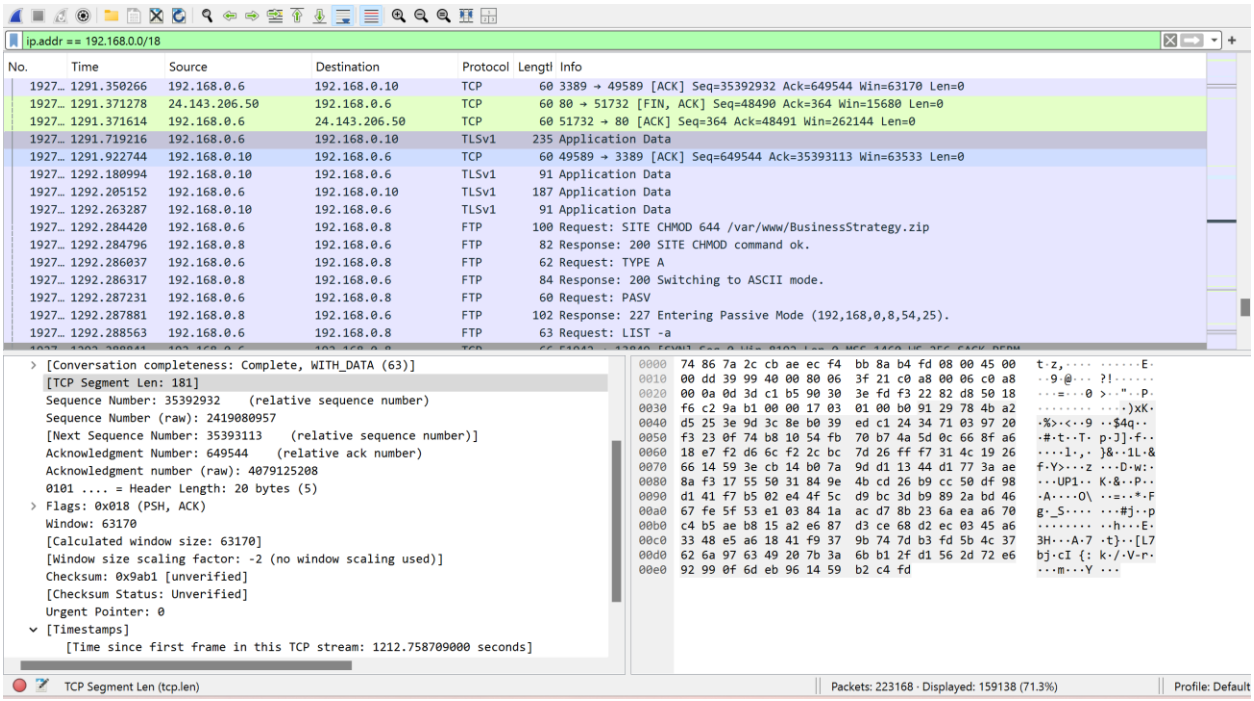


FIGURE 29: FILE PERMISSION MODIFICATION AND NETWORK TRAFFIC ANALYSIS (WIRESHARK)

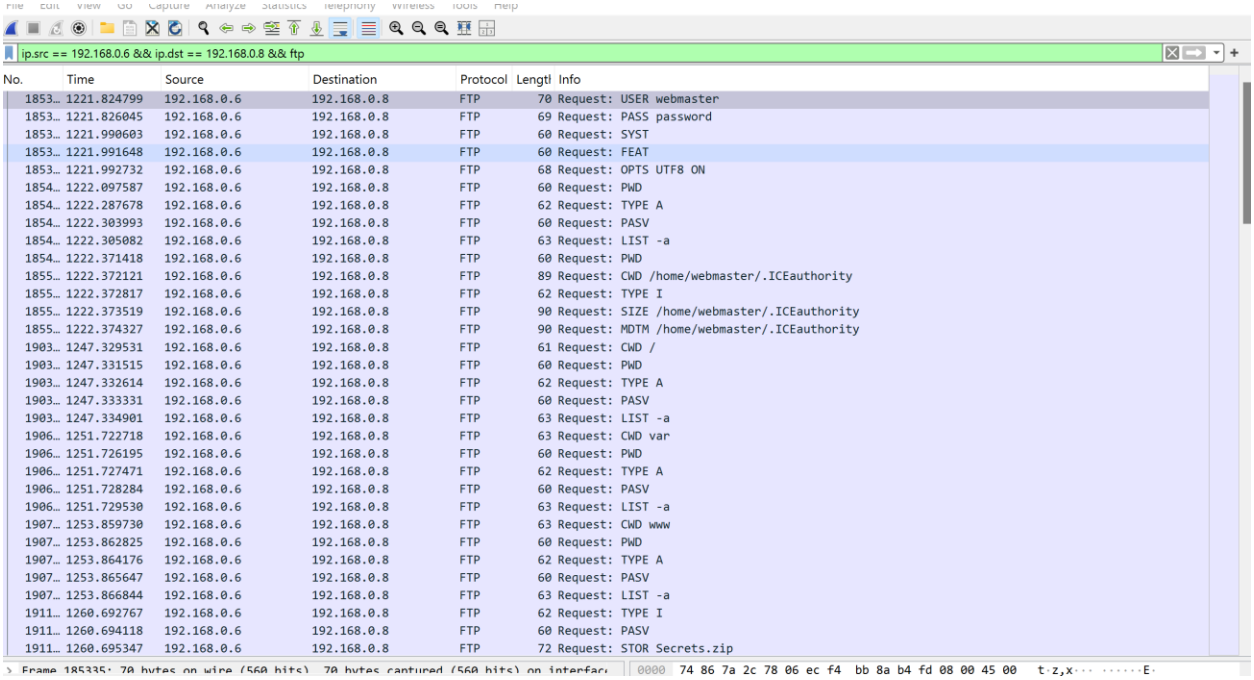
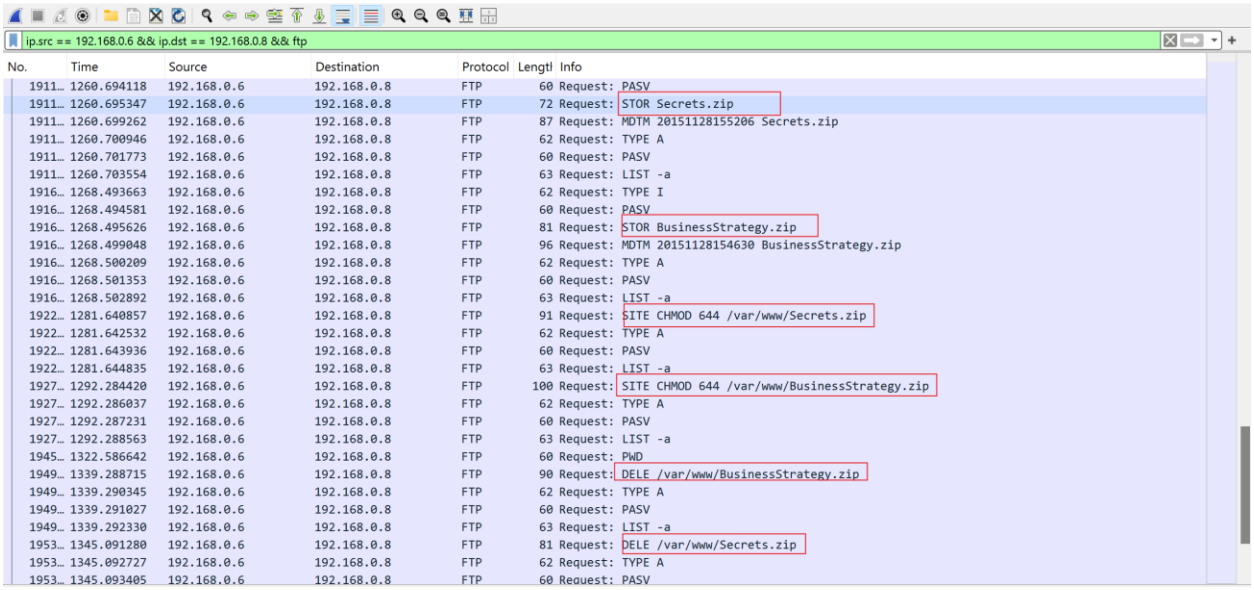


FIGURE 30: CONVERSATION BETWEEN 192.168.0.6 AND 192.168.0.8 USING FTP

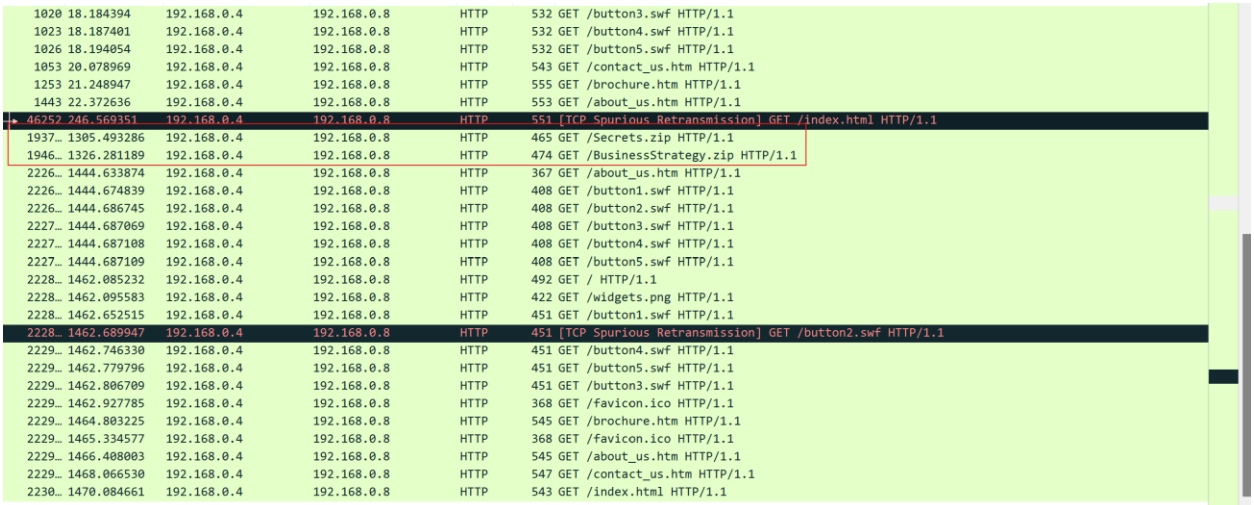
PROTOCOL



ip.src == 192.168.0.6 && ip.dst == 192.168.0.8 && ftp

No.	Time	Source	Destination	Protocol	Lengtl	Info
1911…	1260.694118	192.168.0.6	192.168.0.8	FTP	60	Request: PASV
1911…	1260.695347	192.168.0.6	192.168.0.8	FTP	72	Request: STOR Secrets.zip
1911…	1260.699262	192.168.0.6	192.168.0.8	FTP	87	Request: MDTM 20151128155206 Secrets.zip
1911…	1260.700946	192.168.0.6	192.168.0.8	FTP	62	Request: TYPE A
1911…	1260.701773	192.168.0.6	192.168.0.8	FTP	60	Request: PASV
1911…	1260.703554	192.168.0.6	192.168.0.8	FTP	63	Request: LIST -a
1916…	1268.493663	192.168.0.6	192.168.0.8	FTP	62	Request: TYPE I
1916…	1268.494581	192.168.0.6	192.168.0.8	FTP	60	Request: PASV
1916…	1268.495626	192.168.0.6	192.168.0.8	FTP	81	Request: STOR BusinessStrategy.zip
1916…	1268.499048	192.168.0.6	192.168.0.8	FTP	96	Request: MDTM 20151128154630 BusinessStrategy.zip
1916…	1268.500209	192.168.0.6	192.168.0.8	FTP	62	Request: TYPE A
1916…	1268.501353	192.168.0.6	192.168.0.8	FTP	60	Request: PASV
1916…	1268.502892	192.168.0.6	192.168.0.8	FTP	63	Request: LIST -a
1922…	1281.640857	192.168.0.6	192.168.0.8	FTP	91	Request: SITE CHMOD 644 /var/www/Secrets.zip
1922…	1281.642532	192.168.0.6	192.168.0.8	FTP	62	Request: TYPE A
1922…	1281.643936	192.168.0.6	192.168.0.8	FTP	60	Request: PASV
1922…	1281.644835	192.168.0.6	192.168.0.8	FTP	63	Request: LIST -a
1927…	1292.284420	192.168.0.6	192.168.0.8	FTP	100	Request: SITE CHMOD 644 /var/www/BusinessStrategy.zip
1927…	1292.286037	192.168.0.6	192.168.0.8	FTP	62	Request: TYPE A
1927…	1292.287231	192.168.0.6	192.168.0.8	FTP	60	Request: PASV
1927…	1292.288563	192.168.0.6	192.168.0.8	FTP	63	Request: LIST -a
1945…	1322.586642	192.168.0.6	192.168.0.8	FTP	60	Request: PWD
1949…	1339.288715	192.168.0.6	192.168.0.8	FTP	90	Request: DELE /var/www/BusinessStrategy.zip
1949…	1339.290345	192.168.0.6	192.168.0.8	FTP	62	Request: TYPE A
1949…	1339.291027	192.168.0.6	192.168.0.8	FTP	60	Request: PASV
1949…	1339.292330	192.168.0.6	192.168.0.8	FTP	63	Request: LIST -a
1953…	1345.091280	192.168.0.6	192.168.0.8	FTP	81	Request: DELE /var/www/Secrets.zip
1953…	1345.092727	192.168.0.6	192.168.0.8	FTP	62	Request: TYPE A
1953…	1345.093405	192.168.0.6	192.168.0.8	FTP	60	Request: PASV

FIGURE 31: UPLOADING, CHANGING PERMISSION AND DELETING THE EXFILTRATED FILE



1020	18.184394	192.168.0.4	192.168.0.8	HTTP	532	GET /button3.swf HTTP/1.1
1023	18.187401	192.168.0.4	192.168.0.8	HTTP	532	GET /button4.swf HTTP/1.1
1026	18.194054	192.168.0.4	192.168.0.8	HTTP	532	GET /button5.swf HTTP/1.1
1053	20.078969	192.168.0.4	192.168.0.8	HTTP	543	GET /contact_us.htm HTTP/1.1
1253	21.248947	192.168.0.4	192.168.0.8	HTTP	555	GET /brochure.htm HTTP/1.1
1443	22.372636	192.168.0.4	192.168.0.8	HTTP	553	GET /about_us.htm HTTP/1.1
46252	246.569351	192.168.0.4	192.168.0.8	HTTP	551	[TCP Spurious Retransmission] GET /index.html HTTP/1.1
1937…	1305.493286	192.168.0.4	192.168.0.8	HTTP	465	GET /Secrets.zip HTTP/1.1
1946…	1326.281189	192.168.0.4	192.168.0.8	HTTP	474	GET /BusinessStrategy.zip HTTP/1.1
2226…	1444.633874	192.168.0.4	192.168.0.8	HTTP	367	GET /about_us.htm HTTP/1.1
2226…	1444.674839	192.168.0.4	192.168.0.8	HTTP	408	GET /button1.swf HTTP/1.1
2226…	1444.686745	192.168.0.4	192.168.0.8	HTTP	408	GET /button2.swf HTTP/1.1
2227…	1444.687069	192.168.0.4	192.168.0.8	HTTP	408	GET /button3.swf HTTP/1.1
2227…	1444.687108	192.168.0.4	192.168.0.8	HTTP	408	GET /button4.swf HTTP/1.1
2227…	1444.687109	192.168.0.4	192.168.0.8	HTTP	408	GET /button5.swf HTTP/1.1
2228…	1462.085232	192.168.0.4	192.168.0.8	HTTP	492	GET / HTTP/1.1
2228…	1462.095583	192.168.0.4	192.168.0.8	HTTP	422	GET /widgets.png HTTP/1.1
2228…	1462.652515	192.168.0.4	192.168.0.8	HTTP	451	GET /button1.swf HTTP/1.1
2228…	1462.689947	192.168.0.4	192.168.0.8	HTTP	451	[TCP Spurious Retransmission] GET /button2.swf HTTP/1.1
2229…	1462.746330	192.168.0.4	192.168.0.8	HTTP	451	GET /button4.swf HTTP/1.1
2229…	1462.779796	192.168.0.4	192.168.0.8	HTTP	451	GET /button5.swf HTTP/1.1
2229…	1462.806709	192.168.0.4	192.168.0.8	HTTP	451	GET /button3.swf HTTP/1.1
2229…	1462.927785	192.168.0.4	192.168.0.8	HTTP	368	GET /favicon.ico HTTP/1.1
2229…	1464.803225	192.168.0.4	192.168.0.8	HTTP	545	GET /brochure.htm HTTP/1.1
2229…	1465.334577	192.168.0.4	192.168.0.8	HTTP	368	GET /favicon.ico HTTP/1.1
2229…	1466.408003	192.168.0.4	192.168.0.8	HTTP	545	GET /about_us.htm HTTP/1.1
2229…	1468.066530	192.168.0.4	192.168.0.8	HTTP	547	GET /contact_us.htm HTTP/1.1
2230…	1470.084661	192.168.0.4	192.168.0.8	HTTP	543	GET /index.html HTTP/1.1

FIGURE 32: DOWNLOADING SECRETS.ZIP AND BUSINESSSTRATEGY.ZIP FROM HOST "192.168.0.4"

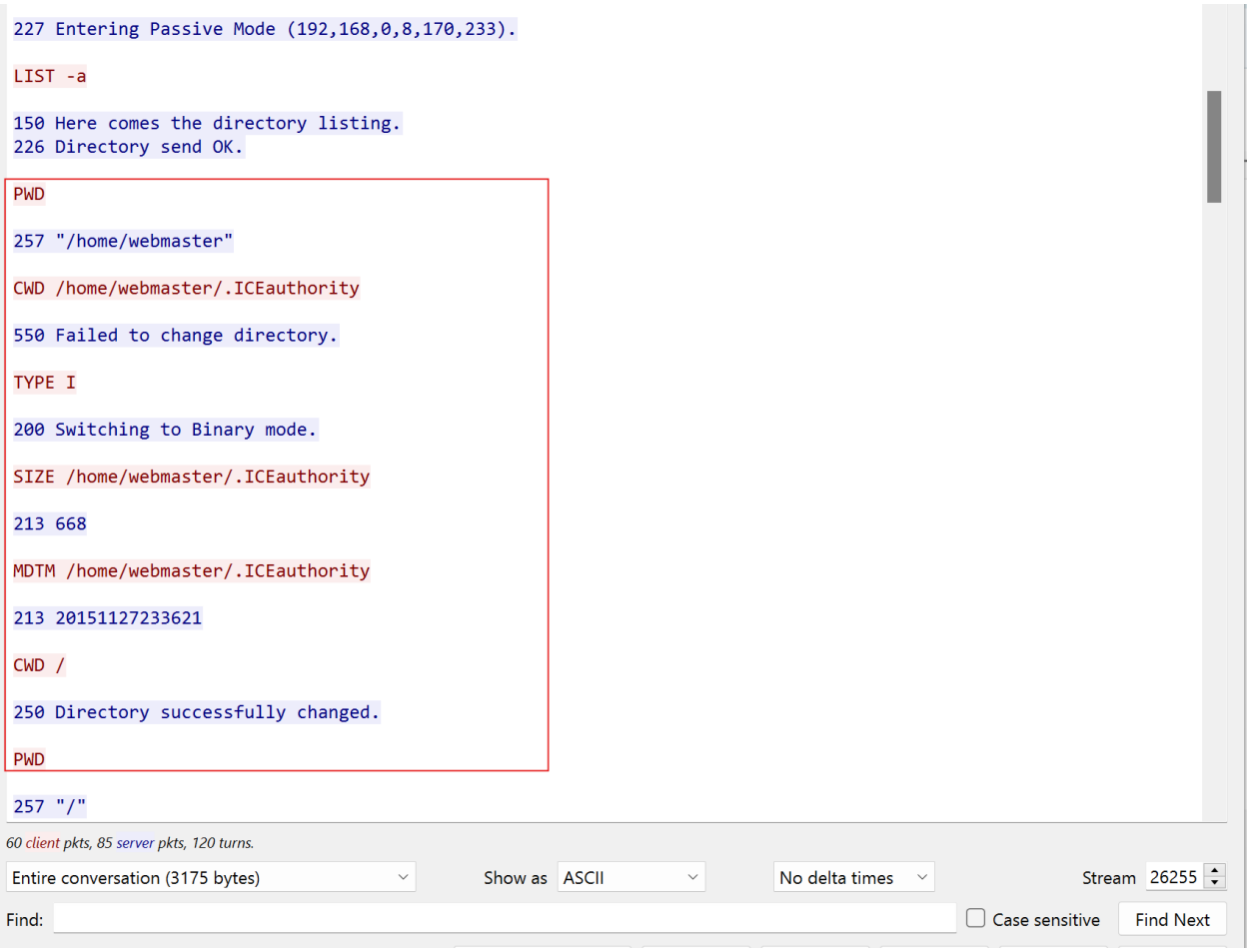


FIGURE 33: TRYING TO ACCESS AUTHENTICATION FILE

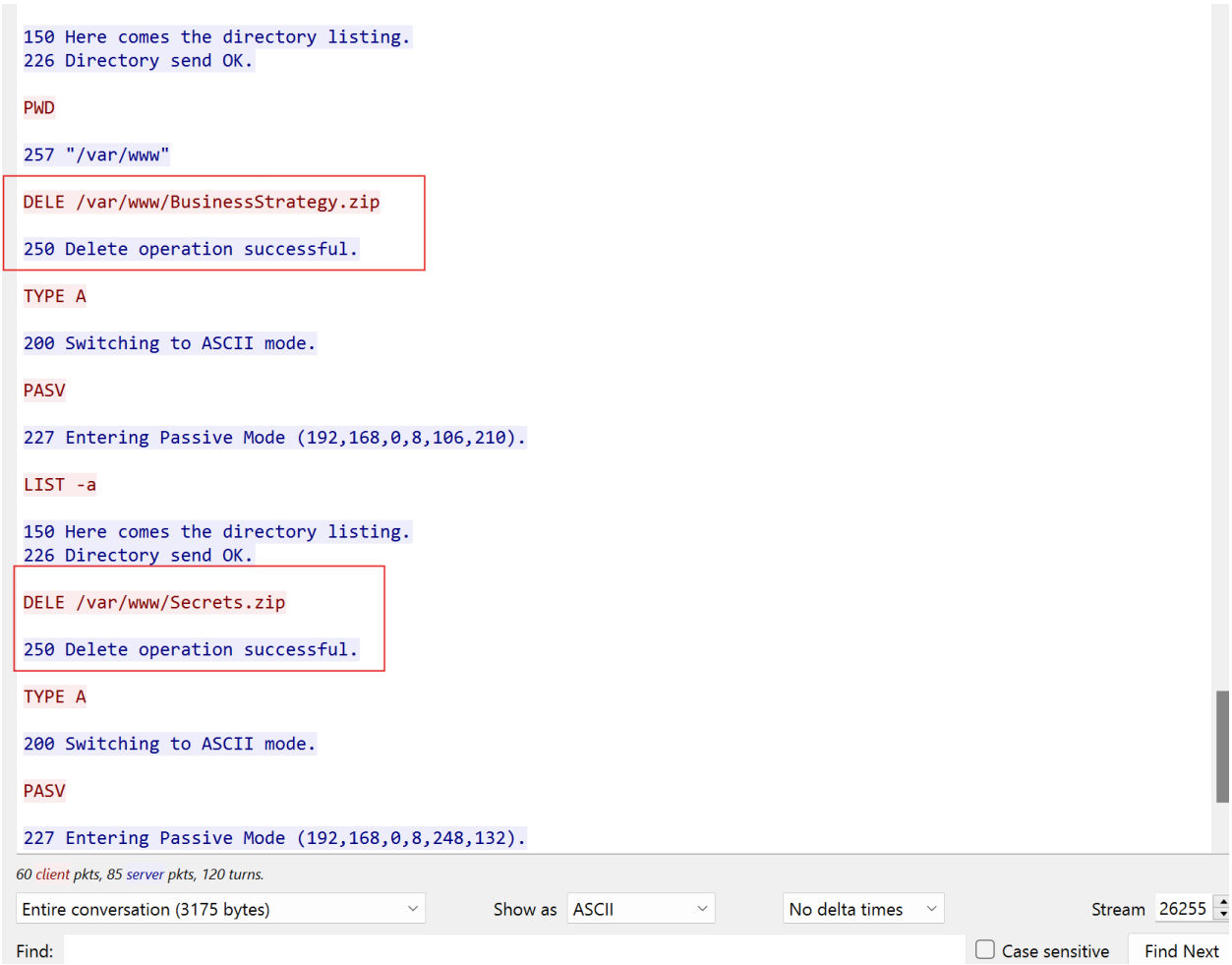


FIGURE 34: DELETION OF SECRETS.ZIP AND BUSINESSSTRATEGY.ZIP FROM WEB SERVER

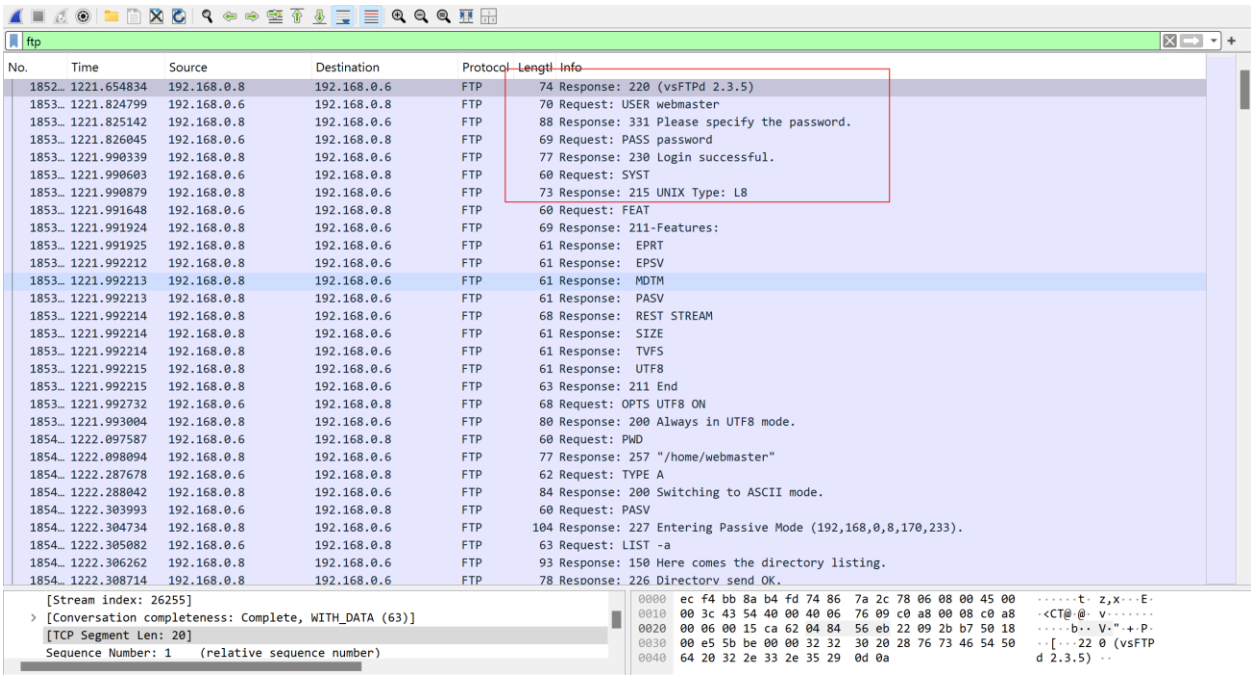


FIGURE 35: ACCESSING WEB SERVER USING WEBMASTER AND PASSWORD

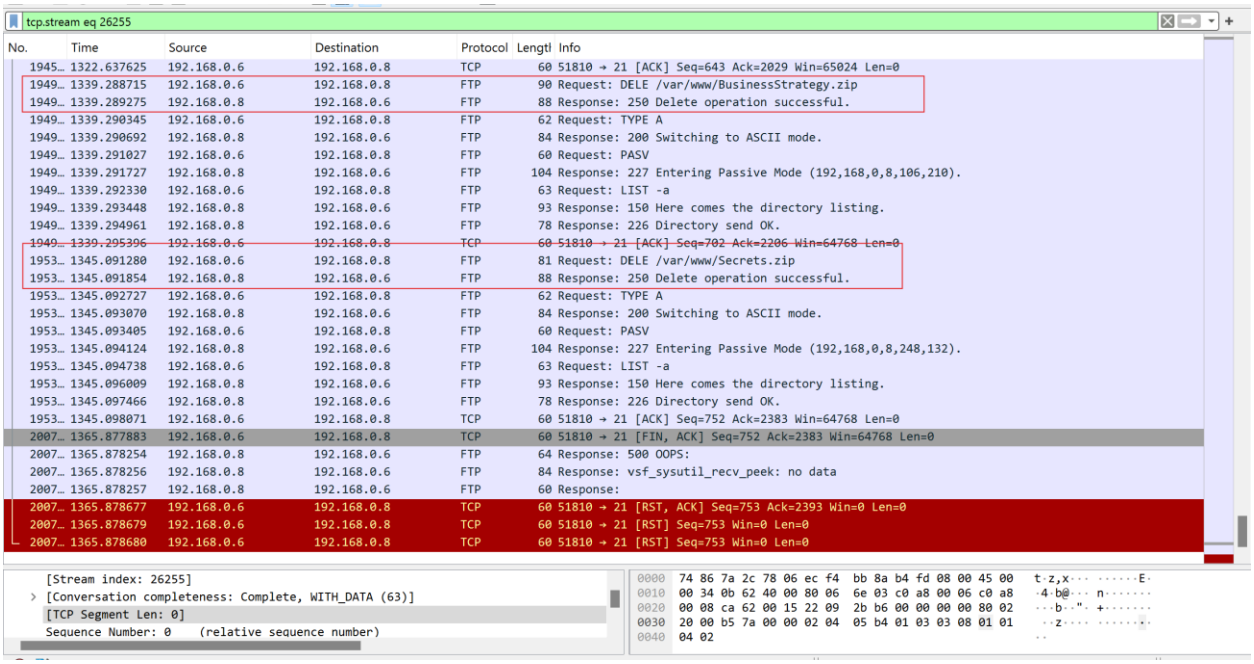


FIGURE 36: FTP COMMANDS AND FILE DELETION ACTIVITY IN CAPTURED NETWORK TRAFFIC (WIRESHARK ANALYSIS)

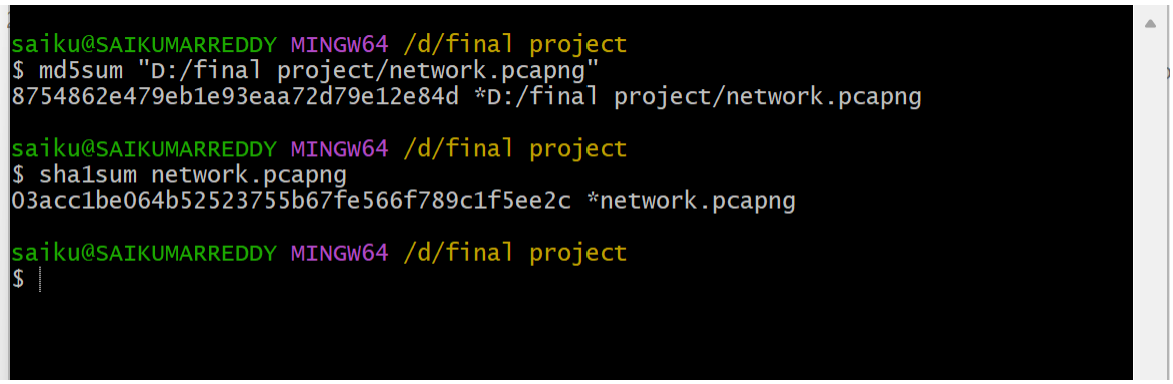


FIGURE 37: MD5 AND SHA1 FOR NETWORK.PCAPNG(USING GIT BASH)

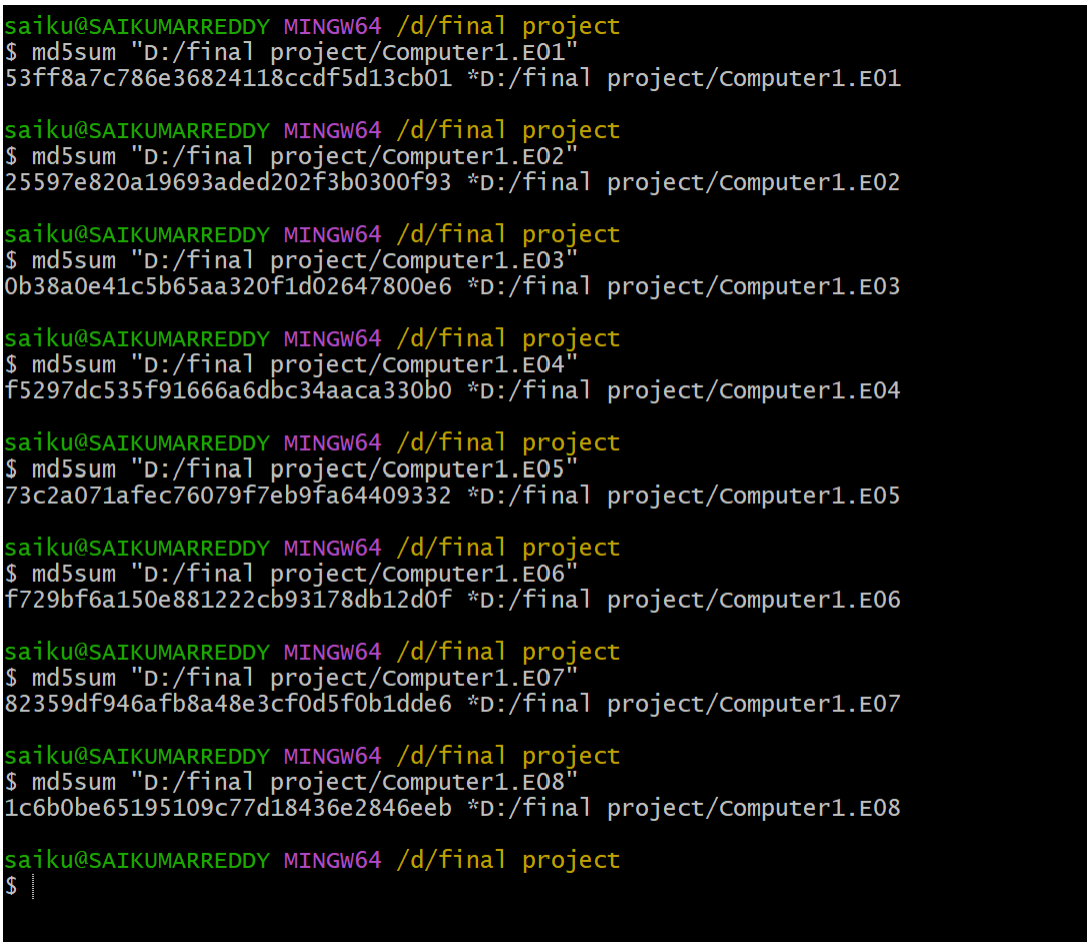


FIGURE 38:MD5 HASHES OF COMPUTER 1 USING GIT BASH

```
saiku@SAIKUMARREDDY MINGW64 /d/final project
$ sha1sum Computer1.E01
62badc2b2b27095db51408f46931c51ad289dbb3 *Computer1.E01

saiku@SAIKUMARREDDY MINGW64 /d/final project
$ sha1sum Computer1.E02
4eb10332a7876e39d8153624d7d365b67ccf6630 *Computer1.E02

saiku@SAIKUMARREDDY MINGW64 /d/final project
$ sha1sum Computer1.E03
b7d9f4d5fab03e30c21a2bb845bb6052c38b480a *Computer1.E03

saiku@SAIKUMARREDDY MINGW64 /d/final project
$ sha1sum Computer1.E04
32d20dfd9218cc03dd6ac2a936aa1d8192613a91 *Computer1.E04

saiku@SAIKUMARREDDY MINGW64 /d/final project
$ sha1sum Computer1.E05
fff112b45673b759d950ff0fa8e240adfbf5cd77 *Computer1.E05

saiku@SAIKUMARREDDY MINGW64 /d/final project
$ sha1sum Computer1.E06
5d1b4c35a28edd43d48ae2c2a290f89a055632c8 *Computer1.E06

saiku@SAIKUMARREDDY MINGW64 /d/final project
$ sha1sum Computer1.E07
7493f7b667f2f305452bb3fd874688c6923eda9e *Computer1.E07

saiku@SAIKUMARREDDY MINGW64 /d/final project
$ sha1sum Computer1.E08
85e88b711c089fe8635a68e68438e32bf3790ac3 *Computer1.E08

saiku@SAIKUMARREDDY MINGW64 /d/final project
$
```

FIGURE 39: SHA1 HASHES OF COMPUTER 1 USING GIT BASH

```
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

D:\final project\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64\run>john --format=NT hashes.txt --word
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=16
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (Carlson)
                 (Administrator)
letmein          (Jonathan)
monkey           (tester)
4g 0:00:00:00 DONE (2024-12-06 19:00) 235.2g/s 11294p/s 11294c/s 45176C/s 123456..knight
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed

D:\final project\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64\run>
```

FIGURE 40: PASSWORDS OF USER ACCOUNTS OF COMPUTER 1(USING JOHN THE RIPPER)

```
D:\final project\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64\run>john --wordlist=rockyou.txt shadow-
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (webmaster)
popcorn          (cknight)
```

FIGURE 41: PASSWORDS OF ACCOUNTS IN COMPUTER 2 (USING JOHN THE RIPPER)

8.CONCLUSION AND RECOMMENDATIONS

8.1. Conclusion

The investigation into the data exfiltration incident at HiTek Corporation on November 28, 2015, at 17:47 EST, confirmed that sensitive information, including 2 Zip files—Secrets.Zip And Businessstrategy.Zip—was stolen from the company's internal network . The attacker exploited multiple vulnerabilities, beginning with the use of SSDP packets to identify network devices. Gaining remote desktop access to Computer 1 using the administrator credentials of "Carlson," the attacker subsequently accessed the web server via FTP using the "webmaster" account from 192.168.0.6 to upload the stolen files. The files were later downloaded through HTTP by an unknown individual from 192.168.0.4 using an Apple device. To cover their tracks, the attacker erased the directories containing the uploaded files.

The investigation utilized advanced forensic tools, including Wireshark, FTK Imager, and Autopsy, to analyze artifacts from network captures and disk images (Computer1.E01 and Computer2.E01). These tools enabled investigators to uncover stolen credentials, suspicious file transfers, and a detailed timeline of the exfiltration. Despite challenges in processing the vast amount of data, the integrity of the evidence was maintained, providing critical insights into the attack methodology.

This breach could have been prevented with stronger password policies across the organization, stricter access controls, and comprehensive monitoring of user permissions. It is recommended that HiTek Corporation implement these measures alongside reliable forensic and monitoring tools to safeguard against future incidents of data exfiltration.

8.2. RECOMMENDATIONS

1.Comprehensive Evidence Gathering: Collect all potential sources of evidence to ensure a thorough understanding of the incident.
2.Adequate Time Allocation: Dedicate sufficient time for resource-intensive tasks like password cracking to uncover valuable insights.
3.Optimal Use of Resources: Leverage a wide range of forensic tools and techniques to enhance the chances of recovering encrypted or hidden data.
4.Proactive Security Practices: Organizations should enforce stricter access policies, maintain robust logging systems, and conduct regular audits to minimize vulnerabilities and swiftly detect unauthorized activities.

9. REFERENCE

[1] WIKIPEDIA SIMPLE SERVICE DISCOVERY PROTOCOL RETRIEVED FROM: HTTPS://EN.WIKIPEDIA.ORG/WIKI/SIMPLE_SERVICE_DISCOVERY

_

[2] WIRESHARK TIP 4: FINDING SUSPICIOUS TRAFFIC IN PROTOCOL HIERARCHY RETRIEVED FROM HTTPS://WWW.YOUTUBE.COM/WATCH?V=OWQMWBD1UIST=8S

[3] WIRESHARK USER'S GUIDE RETRIEVED FROM: HTTPS://WWW.WIRESHARK.ORG/DOCS/WSUG_HTML/

[4] WIRESHARK FOR PENTESTER: PASSWORD SNIFFING RETRIEVED FROM:

[5] HTTPS://WWW.HACKINGARTICLES.IN/WIRESHARK- FOR-PENTESTERPASSWORD-SNIFFING/

[6] BRUTE FORCE ATTACK DETECTION AND PREVENTION ON A NETWORK USING WIRESHARK ANALYSIS RETRIEVED FROM: HTTP://WWW.IJESRT.COM/ISSUES%20PDF%20FILE/ARCHIVE2017/JUNE-2017/4.PDF

[7] HOW TO INSTALL JOHN THE RIPPER ON UBUNTU RETRIEVED FROM: HTTPS://LINUXHINT.COM/JOHN_RIPPER_UBUNTU/
HTTPS://LINUXHINT.COM/JOHN_RIPPER_UBUNTU/