EXPERT WITNESS REPORT

Case: Disappearance of William B. “Willy” Yeats

Report by: Atharva Deshpande

Email ID: deshpana@oregonstate.edu

Student ID: 934418172

Table of Contents

INTRODUCTION & QUALIFICATIONS

I am Atharva Deshpande. I am a master's student with an opportunity for the role of a digital forensic investigator at Oregon State University. I have expertise in forensic analysis, particularly in registry analysis, shell bag analysis, event log analysis, and file carving.

I have developed skills in timeline reconstruction which is crucial for establishing sequences of events and identifying relevant information. I also get different opportunities to apply my theoretical knowledge to practical scenarios at the Laboratory. My business address is 1500 SW Jefferson Way Corvallis, OR 97331.

The following represents my Report in the matter of Willy Yeats. It is based on review of materials submitted to me, my education and experience as a forensic investigator and my experience designing and using different forensic tools. I reserve the right to amend this report if other evidence becomes available.

SUMMARY OF INCIDENT

William B also known as "Willy" Yeats was a 38-year-old man who was the Vice President of IT for Rose City, a software company based in Portland. Willy was an Oregon State University Alumnus with a BS in CS and, along with Maude Gonne and Jack Spicer, founded Rose City soon after graduating.

The US Coast Guard found Willy's sailboat, a Vancouver 34, capsized at sea off the shore near Cape Disappointment on Wednesday, March 10, 2021. Nobody was found near the wreckage. Known as an avid sailor with open ocean experience, Willy was last seen by locals on the evening of March 8th at the Rogue Pier 39 Public House. He was seen leaving the establishment at around 10pm. Willy's truck, a 2019 Toyota Tundra, was found at his dock in Portland.

Near the Lake Oswego PD, there was a tip by neighborhood watch member who saw a "young man in a hoodie" throwing" something heavy in the dumpster—stolen goods," late in the evening of March 7th. The police recovered a HP Z230 in a bag of trash in a dumpster near Yeats' apartment. The serial number indicated that it was originally purchased by Rose City and was recently replaced during a refresh cycle. Yeats purchased it at a cost of $50 for his personal use. Fingerprints on the computer matched prints from Yeats' apartment. A forensically-sound image of the hard drive was extracted and provided to the investigators.

METHODS AND PROCEDURES

CASE EVALUATION

- A thorough examination of the case details and requirements was conducted to establish the scope and objectives of the investigation. This involved reviewing relevant documentation, discussing the requirements, and determining the specific areas of interest for the analysis. A constructed timeline for the case can be found in the Appendix.

EVIDENCE AQUISITION

- All necessary digital evidence was identified, acquired, and preserved using recognized forensic techniques to maintain the chain of custody. The acquisition process involved creating forensic images of the hard disk devices using validated tools and methodologies. Hash values were calculated for each acquired image to ensure data integrity. Copies of evidence were made as well to ensure integrity of the original data file.

FORENSIC ANALYSIS

- The acquired digital evidence was subjected to comprehensive analysis using industry-standard forensic tools and techniques. Various methods were employed to examine the evidence, including keyword searches, registry analysis, event log analysis, shell bag analysis, metadata examination, and file carving. These procedures aimed to identify relevant artifacts, uncover hidden or deleted information, and establish a timeline of events. The tools used to perform this analysis include Autopsy, Registry explorer, Shell bags explorer, Hex Editor and Event Log Explorer.

DOCUMENTS REVIEWED

As part of my assignment, I have reviewed Case presentation file shared with us. I have also reviewed the associated information provided to us during the investigation. Moreover, there was a phishing email sent to Rose City that was documented in the evidence. It was sent to Ms. Maude Gonne by Theodore Roethke, Sr. Vice President at Byzantium Construction. I reviewed a copy of this email as well.

FINDINGS AND ANALYSIS

REGISTRY ANALYSIS

- Registry analysis involves the examination and interpretation of data stored within the Windows Registry, a central database in Windows operating systems. It aims to extract valuable information related to user activity, system configuration, installed software, recent usage history, and persistence mechanisms utilized by malware.
- A domain account was created and accessed on the computer with 'yeatsw' as the user. Timestamps for the last shutdown time of the system were extracted by conversion of hexadecimal values to date time values which came out to be 13-12-2020 at 14:07:25. The last logged on user on the computer system was BYZANTIUMUS/yeatsw which belonged to Willy B.
- Data from Yeats' system was accessed the very day when he was last seen. There is evidence of a USB drive with serial number '38A261A4&0' being accessed the same day at 01:06:10 when Willy B went missing.
- All URLs accessed before 08-12-2020 at 06:48:30 were either deleted or someone did not make use of Internet Explorer to perform actions on the internet. The last typed URL from

the system was made to the Microsoft default home page, which justifies the above stated claim.

SHELLBAG ANALYSIS

- Shellbag analysis is a forensic technique used to examine the Windows Registry and analyze the artifacts known as "shellbags." Shellbags are data structures that store information about folder navigation and file access within the Windows operating system. Analyzing shellbags helps us to reconstruct a user's file and folder access patterns, including timestamps, names, and paths, providing insights into a user's activities, navigation history, and potentially revealing evidence of file manipulation or access to sensitive information. Shellbags are stored in two files (Ntuser.dat & Usrclass.dat).
- The user BYZANTIUMUS/YeatsW was last accessing D drive on the computer system on 2021-03-08 01:16:24. Upon examining the Usrclass.dat file for the user, I was able to view 12 shellbags with an empty directory located on the desktop named ‘Canada’ which was last accessed on 2021-03-07 08:16:24 (a day prior when the laptop was tossed into a dumpster). This could imply deletion of files in that directory.
- The user BYZANTIUMUS/WillyB last accessed the C drive on the computer system on 2020-11-08 00:14:07. Upon examining the Usrclass.dat file for the user, I was able to view sixteen shellbags. The actions performed pointed to log files which were observed to be a NTFS file.

EVENT LOG ANALYSIS

- Event log analysis involves examining and interpreting the records of significant events, errors, warnings, and activities generated by computer systems and applications. By analyzing event logs, digital forensic analysts can reconstruct timelines, identify anomalies and security breaches, detect malware, analyze system health and performance, and monitor user activities.
- I observed that the user ‘Willy B’ was trying to join the domain and access other user accounts from it. But, since all users did not have access to the domain, they were given

restricted access by the administrator. This led to the change in the computer host name. Having looked into the system log file, I saw that the NETBIOS name and the host name of the machine was changed from 'DESKTOP-4ADMS82' to 'WILLYB-DESKTOP' at 11/7/2020 16:14:58.

- Willy B attempted to join the domain 'BYZANTIUMUS.COM.' After successfully joining it, a new account 'yeatsw' accessed the domain account by logging into it at 11-7-2020 at 16:13:59. Examining the security log file helped me to understand that the user account 'WillyB' did attempt to join the domain controller and later using administration access, added a new account to this system. Furthermore, moments after the account were added to a local security group, I observed it logging into the system and the account whose credentials were used belonged to 'yeatsw.'

EMAIL AND METADATA ANALYSIS

- Email and metadata analysis involves examining the content, headers, and associated metadata of email messages. It helps extract valuable information, identify communication patterns, establish timelines, detect anomalies, and gather evidence of illegal or unauthorized activities.
- Having examined the email conversations between Willy and Maude, I was able to extract images of them being together in a relationship. A flight ticket to Port Vila from San Francisco via Mexico City was attached in an email conversation along with images of Canadian passports. Moreover, I accessed the images in a Hex Editor and observed that there were hidden files present in images, which were extracted by file carving. File carving involves searching for and reconstructing file fragments based on specific file signatures or patterns. By analyzing the binary content of the storage media, file carving can recover deleted, damaged, or hidden files.
- There was presence of multiple steganographic images (particularly images of a Canadian birth certificate for a person named Mary Ellen Lee, two Canadian passports and a spreadsheet containing bank information i.e., account number, routing number and available balance) in the email conversations between Willy and Maude.

WEB HISTORY ANALYSIS

- During the investigation of the system image in Autopsy, I extracted important artifacts pertaining to web browsing history, web cookies and traces of Tor browser being accessed.
- I was able to find browser cookies for byzantiumus.com. Information accessed through x-sqlite3 database was modified on 7th March 2021. This was the last login to the domain account database.
- Tor browser was used to conduct private and untraceable transactions over the internet. This access was made just before an email mentioning bitcoin transfer. There was presence of web cookies for the domain controller account, web history of the domain and traces of Tor browser being accessed that justify the analysis made above.

EXPERT OPINION & CONCLUSION

Upon investigating, I observed that four user accounts (John McCrae, Ted Roethke, WillyB and YeatsW) were created on the system and given access to the domain account of 'ByzantiumUS.' 'ByzantiumUS/yeatsw' was the last logged on account on the system. There were traces of steganographic images and money transfer in email conversations. An empty directory named 'Canada' was accessed a day prior when Yeats was last seen. The server of ByzantiumUS was migrated to an AWS server and user accounts were given administrative access for the same. To conclude, the evidence gathered from different analyses points towards suspicious activities, including unauthorized access, file deletion, potential involvement in illegal activities, and attempts to conceal online transactions.

GLOSSARY OF TERMS

- **Autopsy** - Autopsy is a digital forensics platform used for analyzing and investigating computer systems and storage devices. Main purpose of this tool is to analyze and extract files from the image for application analysis of emails, photograph, etc.
- **Registry explorer** - Registry Explorer is a software tool that allows users to access and modify the Windows Registry on a Microsoft Windows operating system. It is used to examine windows registry for different key values, hives, data evidence, logs, etc.
- **Shell bags explorer** – Shell bags Explorer is a tool used to analyze and manage the "shell bags" in the Windows Registry. Its purpose is to examine a computer system for directory usage in the past, including timestamps of files being created, accessed, and modified.
- **Hex editor** - A hex editor is a software tool used for viewing and editing binary files at a low-level. It can be used to identify specific data patterns and recover steganographic files.
- **Event log explorer** - Event Log Explorer is a software tool designed to facilitate the analysis and management of event logs on Microsoft Windows operating systems. It can be used to view, search, and analyze event (system, application, and security) log entries.
- **Domain account** - A domain account is a user account that is managed and authenticated by a centralized domain controller in a Windows domain network.
- **Domain controller** - A domain controller account is a privileged account that manages and controls access to resources within a Windows domain network.
- **NTUser.dat** - NTUser.dat stores user related settings, preferences, and configuration data, such as desktop settings, application settings, user-specific registry keys, and various user-related preferences.
- **Usrclass.dat** - Usrclass.dat stores information related to the user's classes, including file associations, shell extensions, and other user-specific settings for various applications.
- **Web cookies** - Web cookies are small pieces of data stored by a website on a user's web browser to remember user preferences and enable personalized browsing experiences.

APPENDIX

- Timeline of events for Willy B's case –

Incident	Timestamp	Comments and significance
creditsuisseag.xlsx file last modified	3/24/2021 20:17	Contains the details of the offshore account
Last login user	3/8/2021 1:22	This was the last user to ever log in to the system. This user was BYZANTIUMUS/yeatsw
USBSTOR: Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07	3/8/2021 1:06	Last time the USB was attached to the system
Shellbags: Last modified for D drive	3/7/2021 20:16	12 Shellbags were found. The timestamps of more than 1 folders were found to be 7th March 2021
Shellbags: Last write time for My Computer	3/7/2021 20:16	4 child bags were found for My Computer. Last write time was of interest as it was around the time of disappearance of Willy B.
Shellbags: Last write time for Home	3/7/2021 20:16	Last write time was of interest as it was around the time of disappearance of Willy B.
Shellbags: Last write time for F drive	3/7/2021 20:16	Last write time was of interest as it was around the time of disappearance of Willy B.
Shellbags: Last write time for Canada folder	3/7/2021 20:16	Empty directory named Canada was accessed. Last write time was of interest as it was around the time of disappearance of Willy B.
The Windows Management Instrumentation service has detected an inconsistent system shutdown.	3/7/2021 17:23	Inconsistent system shutdown for the WILLYB-DESKTOP.byzantiumus.com
cookies for byzantiumus.com	3/7/2021 17:21	Browser cookies were found for byzantiumus.com. Access was through x-sqlite3 database
web history login to domain account ByzantiumUS	3/7/2021 17:21	There was a login to the official website belonging to ByzantiumUS. The URL was: https://byzantiumus.com:8443/Login/Index. The login was using samba- a single sign on platform
Web data modified for Microsoft edge	3/7/2021 17:21	Information for x-sqlite3 database access was modified on 7th March 2021
Money Transferred. Tickets attached. Drive from Astoria to make the flight. rendezvous at Malvanua. -15.359212, 167.193547	3/7/2021 17:17	

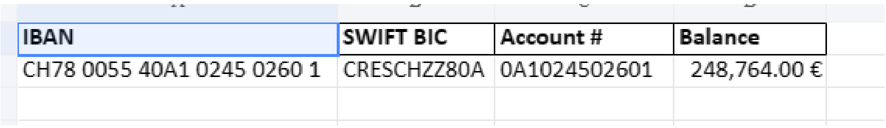
Password changed for domain controller \\byzdc1.byzantiumus.com	3/7/2021 17:05	Password changed for the domain through the system found
Shellbags: Last modified for Windows application	2/26/2021 11:46	This is the last modified timestamp reported in Shellbags for user account Willy B. Other Shellbag dates from 2020 - Not significant
Network connectivity status log	2/26/2021 8:13	The “Home” network was the most recently accessed network
Unmanaged Network: 3	12/14/2020 7:18	Network profiles that are public or non-associated with byzantiumus.com
Unmanaged Network: 2	12/13/2020 17:12	Network profiles that are public or non-associated with byzantiumus.com
Last Shutdown time	12/13/2020 14:07	The time when the system was last shut down.
Authentication failure for active directory service on domain controller	12/13/2020 9:12	There was some error in LDAP bind function call leading to the failure
Logon attempt using explicit credentials	12/13/2020 9:11	Account name WILLYB-DESKTOP$ tried to login using credentials of yeatsw
name resolution for byzdc1.byzantiumus.com timed out	12/13/2020 9:11	Attempt to log into or make connection to the website timed out
Unmanaged Network: 1	12/10/2020 1:52	Network profiles that are public or non-associated with byzantiumus.com
Last write time: Ted Roethke	12/8/2020 6:52	The last write time signifies the time that they made any kind of changes to the ntuser.dat file
Last write time: John McCrae	12/8/2020 6:48	The last write time signifies the time that they made any kind of changes to the ntuser.dat file
Time for last typed URLs in Internet explorer	12/8/2020 6:48	Internet explorer was not used that frequently or not used at all since the timestamp is too old. The timestamp and URL was same for all the 4 user accounts.
Account created for Ted Roethke	12/7/2020 22:52	New account created for ted
New user was created: John McCrae	12/7/2020 22:48	New user was created on the same system
indicating that money will be moved soon	12/7/2020 22:44	Steganographic financial document xlsx document found in image attachment
Attempt was made to query the existence of blank password for the account	12/7/2020 22:39	A possible attempt to check security loopholes in the system
Willy emails: team thinks he is in Baja. Will head out to VLI via Sydney - 1 day layover. Moves server to AWS. No future communications.	12/7/2020 20:48	

Accounts(bank) set up. The domain changed. Bit coins used		
email from Maude asking when will willy head out.	12/7/2020 20:15	
tor.exe accessed	12/7/2020 19:26	Tor browser was accessed to do certain activities on the web (bitcoin?)
Willy heading out to Vancouver. Drive a car back to Redmond. Commissioner meeting at 4. Marriage. Save $180k	12/5/2020 3:46	
Web data created in Microsoft edge	12/5/2020 3:46	Accessed x-sqlite3 database using Microsoft edge.
Maude indicated upcoming marriage and not meeting in public as a ruse for new building construction	11/23/2020 15:24	
confession of 2 birth records forged and certificates ordered. Collected passports in person. Discussed Vancouver trip	11/23/2020 15:03	Indicates a trip to Canada
Got an email? Hint of steganography. Attached passports	11/23/2020 14:45	Birth certificate was found
Last write time: Willy B	11/19/2020 8:09	The last write time signifies the time that they made any kind of changes to the ntuser.dat file
USBSTOR: Disk&Ven_SanDisk&Prod_Ultra &Rev_1.00	11/16/2020 23:36	Last time the USB was attached to the system
Mention of CS373 (steganography) hidden images	11/16/2020 15:43	Willy and Maude had a history. Steganographic passport image found in 1st image attachment. Steganographic birth certificate image found in 2st image attachment
email from willy: Canada is taken care of. Might need to go again. Talks about trip down to equator. $200k needed. Bonuses. Need to make house down payment	11/11/2020 20:20	
email from Maude: I am an early bird. Asks about bonus	11/8/2020 17:17	Some money is to come in
email back from Willy saying hard drive died	11/8/2020 15:18	No communication before this time

email from Maude asking if Willy was okay	11/8/2020 6:16	
Last write time: BYZANTIUMUS\yeatsw	11/8/2020 0:20	The last write time signifies the time that they made any kind of changes to the ntuser.dat file
Managed Network	11/8/2020 0:15	Network profile managed by byzantiumus.com
Shellbags: Control panel and networks and internet folder accessed	11/7/2020 23:59	Shellbags found for WillyB. Probably adjusted while trying to connect to ByzantiumUS network
Shellbags: Last write time	11/7/2020 19:14	This is the last write time of shell bags for the user account Willy B
Change in NETBIOS name and the host name of the machine	11/7/2020 16:14	The NETBIOS name and host name was changed from 'DESKTOP-4ADMS82' to 'WILLYB-DESKTOP'
Identification of IP of domain controller	11/7/2020 16:14	The IP address of the domain name controller was 192.168.0.4. IP address of this system was 192.168.0.3
Successfully joined the domain - byzantiumus.com	11/7/2020 16:13	The machine 'DESKTOP-4ADMS82' joined the domain byzantiumus.com
User logged in using the new account created	11/7/2020 16:13	The new user account was 'yeatsw' and the domain was BYZANTIUMUS.COM
New account was added to local security group	11/7/2020 16:13	Administrator access was used to add a new user to the security group
Attempt to join the domain account. Attempt failed due to wrong username of password	11/7/2020 16:10	Machine - 'DESKTOP-4ADMS82' attempts to join the domain byzantiumus.com
Logs cleared	11/7/2020 11:24	Audit logs were cleared by DESKTOP-4ADMS82

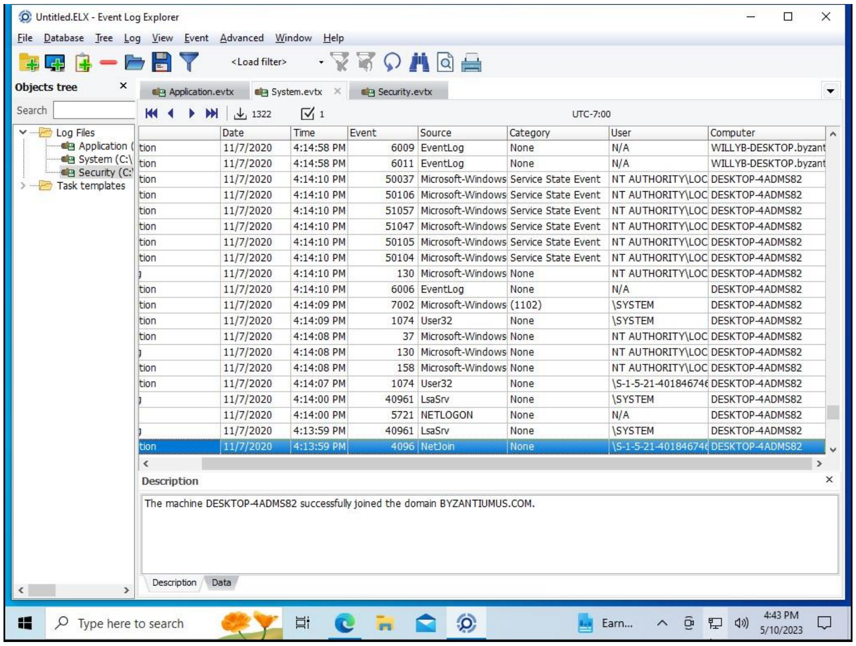
Note*: Timestamps are of the format mm/dd/yyyy hh:mm*

- Images/ screenshots of evidence relevant to the case –



IBAN	SWIFT BIC	Account #	Balance
CH78 0055 40A1 0245 0260 1	CRESCHZZ80A	0A1024502601	248,764.00 €

Bank Information extracted by File Carving on a Steganographic image.

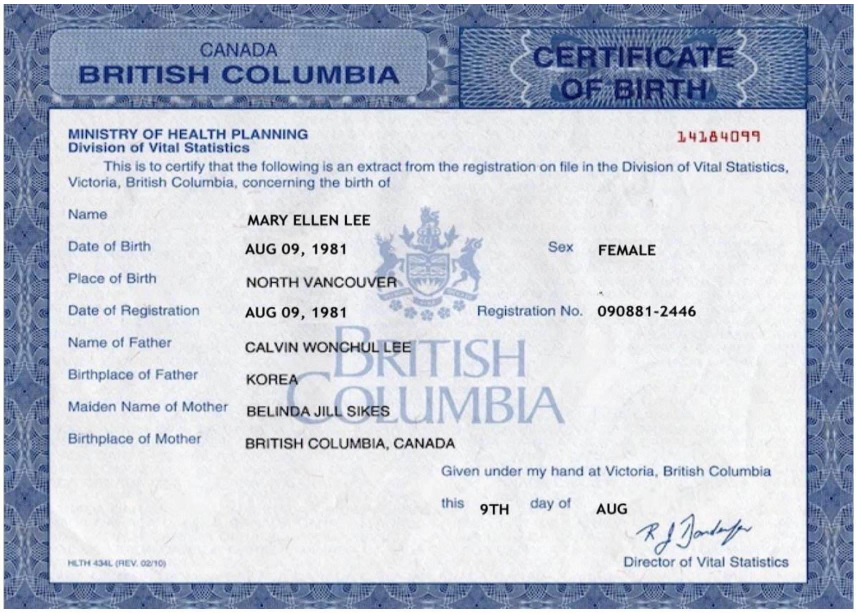


	Date	Time	Event	Source	Category	User	Computer
tion	11/7/2020	4:14:58 PM	6009	EventLog	None	N/A	WILLYB-DESKTOP.byzant
tion	11/7/2020	4:14:58 PM	6011	EventLog	None	N/A	WILLYB-DESKTOP.byzant
tion	11/7/2020	4:14:10 PM	50037	Microsoft-Windows	Service State Event	NT AUTHORITY\LOC	DESKTOP-4ADMS82
tion	11/7/2020	4:14:10 PM	50106	Microsoft-Windows	Service State Event	NT AUTHORITY\LOC	DESKTOP-4ADMS82
tion	11/7/2020	4:14:10 PM	51057	Microsoft-Windows	Service State Event	NT AUTHORITY\LOC	DESKTOP-4ADMS82
tion	11/7/2020	4:14:10 PM	51047	Microsoft-Windows	Service State Event	NT AUTHORITY\LOC	DESKTOP-4ADMS82
tion	11/7/2020	4:14:10 PM	50105	Microsoft-Windows	Service State Event	NT AUTHORITY\LOC	DESKTOP-4ADMS82
tion	11/7/2020	4:14:10 PM	50104	Microsoft-Windows	Service State Event	NT AUTHORITY\LOC	DESKTOP-4ADMS82
j	11/7/2020	4:14:10 PM	130	Microsoft-Windows	None	NT AUTHORITY\LOC	DESKTOP-4ADMS82
tion	11/7/2020	4:14:10 PM	6006	EventLog	None	N/A	DESKTOP-4ADMS82
tion	11/7/2020	4:14:09 PM	7002	Microsoft-Windows	(1102)	\SYSTEM	DESKTOP-4ADMS82
tion	11/7/2020	4:14:09 PM	1074	User32	None	\SYSTEM	DESKTOP-4ADMS82
tion	11/7/2020	4:14:08 PM	37	Microsoft-Windows	None	NT AUTHORITY\LOC	DESKTOP-4ADMS82
j	11/7/2020	4:14:08 PM	130	Microsoft-Windows	None	NT AUTHORITY\LOC	DESKTOP-4ADMS82
tion	11/7/2020	4:14:08 PM	158	Microsoft-Windows	None	NT AUTHORITY\LOC	DESKTOP-4ADMS82
tion	11/7/2020	4:14:07 PM	1074	User32	None	\S-1-5-21-40184674€	DESKTOP-4ADMS82
j	11/7/2020	4:14:00 PM	40961	LsaSrv	None	\SYSTEM	DESKTOP-4ADMS82
	11/7/2020	4:14:00 PM	5721	NETLOGON	None	N/A	DESKTOP-4ADMS82
j	11/7/2020	4:13:59 PM	40961	LsaSrv	None	\SYSTEM	DESKTOP-4ADMS82
tion	11/7/2020	4:13:59 PM	4096	NetJoin	None	\S-1-5-21-40184674€	DESKTOP-4ADMS82

Description

The machine DESKTOP-4ADMS82 successfully joined the domain BYZANTIUMUS.COM.

The computer system successfully joined the domain BYZANTIUMUS.COM.



CANADA
BRITISH COLUMBIA

CERTIFICATE OF BIRTH

MINISTRY OF HEALTH PLANNING
Division of Vital Statistics

14184099

This is to certify that the following is an extract from the registration on file in the Division of Vital Statistics, Victoria, British Columbia, concerning the birth of

Name	MARY ELLEN LEE		
Date of Birth	AUG 09, 1981	Sex	FEMALE
Place of Birth	NORTH VANCOUVER		
Date of Registration	AUG 09, 1981	Registration No.	090881-2446
Name of Father	CALVIN WONCHUL LEE		
Birthplace of Father	KOREA		
Maiden Name of Mother	BELINDA JILL SIKES		
Birthplace of Mother	BRITISH COLUMBIA, CANADA		

BRITISH COLUMBIA

Given under my hand at Victoria, British Columbia

this 9TH day of AUG

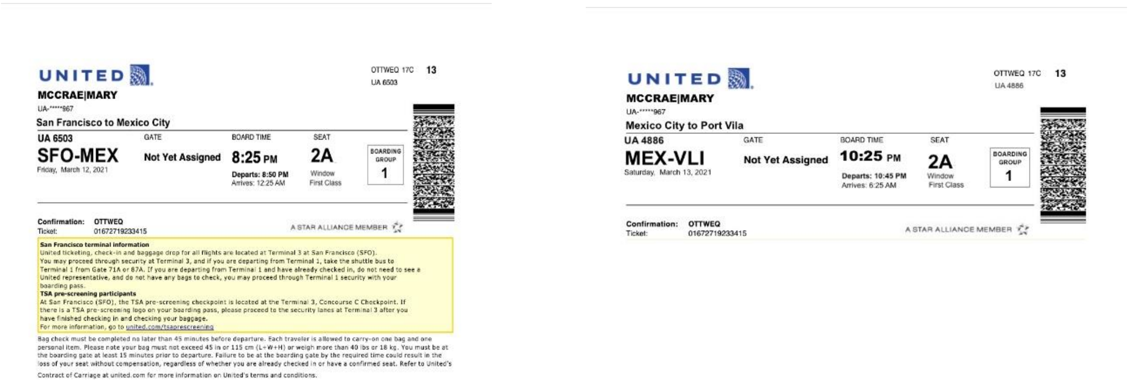
R J Jordan

Director of Vital Statistics

HLTH 434L (REV. 02/10)

Birth Certificate Information extracted by File Carving on a Steganographic image.

Passports extracted by conducting Email Analysis



UNITED

OTTWEQ 17C 13
UA 6503

MCCRAE|MARY
UA-*****967

San Francisco to Mexico City

UA 6503	GATE	BOARD TIME	SEAT	BOARDING GROUP
SFO-MEX Friday, March 12, 2021	**Not Yet Assigned**	**8:25 PM** **Departs: 8:50 PM** Arrives: 12:25 AM	**2A** Window First Class	1

Confirmation: **OTTWEQ**
Ticket: 01672719233415

A STAR ALLIANCE MEMBER

San Francisco terminal information
United ticketing, check-in and baggage drop for all flights are located at Terminal 3 at San Francisco (SFO).
You may proceed through security at Terminal 3, and if you are departing from Terminal 1, take the shuttle bus to Terminal 1 from Gate 71A or 87A. If you are departing from Terminal 1 and have already checked in, do not need to see a United representative, and do not have any bags to check, you may proceed through Terminal 1 security with your boarding pass.
TSA pre-screening participants
At San Francisco (SFO), the TSA pre-screening checkpoint is located at the Terminal 3, Concourse C Checkpoint. If there is a TSA pre-screening logo on your boarding pass, please proceed to the security lanes at Terminal 3 after you have finished checking in and checking your baggage.
For more information, go to united.com/tsaprescreening

Bag check must be completed no later than 45 minutes before departure. Each traveler is allowed to carry-on one bag and one personal item. Please note your bag must not exceed 45 in or 115 cm (L+W+H) or weigh more than 40 lbs or 18 kg. You must be at the boarding gate at least 15 minutes prior to departure. Failure to be at the boarding gate by the required time could result in the loss of your seat without compensation, regardless of whether you are already checked in or have a confirmed seat. Refer to United's Contract of Carriage at united.com for more information on United's terms and conditions.

UNITED

OTTWEQ 17C 13
UA 4886

MCCRAE|MARY
UA-*****967

Mexico City to Port Vila

UA 4886	GATE	BOARD TIME	SEAT	BOARDING GROUP
MEX-VLI Saturday, March 13, 2021	**Not Yet Assigned**	**10:25 PM** **Departs: 10:45 PM** Arrives: 6:25 AM	**2A** Window First Class	1

Confirmation: **OTTWEQ**
Ticket: 01672719233415

A STAR ALLIANCE MEMBER

Flight ticket extracted by conducting Email Analysis

REFERENCES

- Grammarly – To verify and correct vocabulary of words used.
- Chatgpt – To understand technical terms and definitions.
- Seak Expert Witness Company – To understand structure, expected format and view sample expert witness reports.