

Introduction

This report serves as a medium to communicate the results of an investigation into suspicions of Bob's involvement in illegal online activities. The report comprises the discovery of evidence, here referred to as 'issues,' which involves comprehensive analysis and a breakdown of detailed procedures. These procedures encompass hypotheses, strategies, and techniques employed by investigators to uncover facts. A timeline of events is included at the end of the report to assist the reader in visualizing the chronological sequence of occurrences.

Background

Bob is suspected of engaging in illegal online activities. Prior intelligence reports are vague, conflicting and lacking sufficient detail. A warrant was issued, and an officer was able to covertly access and perform a logical acquisition of Bob's computer. You have been assigned the task of investigating Bob's computer to extract evidence and formulate a series of conclusions as to what crimes (if any), Bob was engaging in.

Investigation Approach

Given the limited information available regarding Bob, the investigative approach chosen revolves around an in-depth examination of the system image. The initial focus is on ascertaining the number of users associated with the computer. This step is pivotal, as it provides clarity regarding the quantity of individuals potentially involved in the allegations, aiding in the investigation's scope and direction.

Following the identification of the number of users, the investigation proceeded with an examination of specific folders known to be common storage locations. Drawing from personal experience, these folders include Desktop, Downloads, and Documents. The Desktop folder is often used for storing easily accessible and frequently used material. Downloads, on the other hand, serves as the default directory for downloaded content from the internet. Meanwhile, Documents typically functions as the designated repository for files considered 'formal documents' by the user.

In the next phase of the investigation, given its focus on online activities, a more detailed examination will center around fragments of information extracted from web browsing activity. This entails scrutinizing artifacts derived from web browsing history, downloads, and bookmarks in order to identify and understand the extent of Bob's online activities.

To enhance the investigative process, it is imperative to also employ an approach that involves the inspection of Windows registry files and security event logs. These sources offer a lower risk of contamination, thus rendering the extracted data reliable and valuable for the formulation of events with greater accuracy.

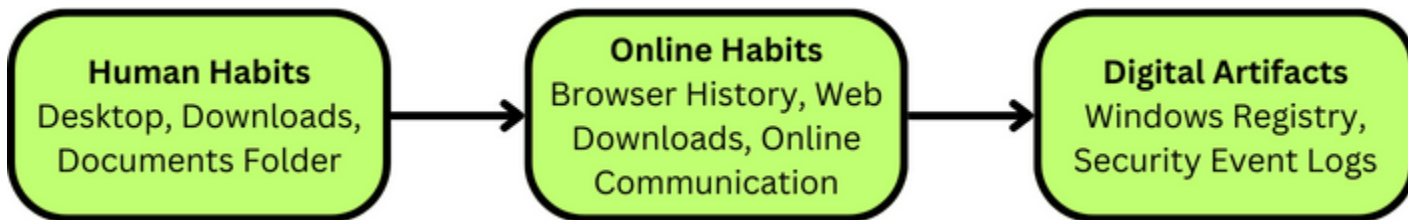


Figure 1 Investigation Approach Illustration

Resources

This investigation will maximize the use of freely available tools on the internet and harness the full potential of trial or demo version tools. The tools are:

- Autopsy 4.20.0
- AccessData Registry Viewer (Demo Mode)
- Event Viewer 1.0
- PassMark OSForensics v 10.0.1015 (Trial version)

Findings

1. Hexchat Conversation Log – [Issue#1 Artifact 4](#)

A log file containing conversations initiated by Bob has been discovered, and it serves as a crucial link to several other pieces of evidence. From this conversation, it can be inferred that Bob paid an entity known as SovereignClassCitizen to

create specific documents. Within the documents, Bob also expressed his intention of earning money through identity theft.

2. Potential Passport Forgery – [Issue#1 Artifact 3](#)

Subsequent to the conversation, it was observed that three passport documents, each bearing the name and a strikingly similar photograph of an individual identified as Bob Sacamano, were downloaded from a link provided by SovereignClassCitizen to Bob. The notable similarities between these three copies strongly suggest an act of identity fraud through forgery.

3. Unauthorized Identity Acquisition – [Issue#1 Artifact 2](#)

Within the conversation, another link was also present. Upon investigation, it was found that the link provided led to the discovery of a file named 'PassportScans.zip,' containing a total of 89 copies of passports, each associated with unique identities. The unusually high number of files in this archive strongly suggests that these documents were acquired without the owners' consent. Considering the context of the HexChat conversation, it is apparent that these 89 copies may be intended for use in identity fraud-related offenses in the future.

4. Identity Theft attempt through Phishing Email – [Issue#1 Artifact 1](#)

Further investigation into alternative means of communication revealed that Bob may have attempted to engage in identity theft through phishing emails. In one such email, Bob endeavored to defraud his colleague, Leonardo, by employing a PayPal scam template with the intention of extracting vital information, including credit card numbers.

Assumptions made.

This investigation was conducted based on the assumption that Bob lives alone, with no one else having access to his computer. Additionally, it is noted that Bob's account, containing evidence relevant to the allegations, is not protected by a password. Furthermore, it is assumed that Bob lacks expertise in both social engineering attacks and the Windows operating system.

Analysis of the severity of crimes committed.

There is currently no conclusive evidence to support the claim that Bob has used the illegally obtained documents for identity fraud, and as such, it cannot be definitively established that he has broken the law. However, it's important to note that, should Bob proceed with identity fraud in the future, he would be in violation of the Criminal Code Part VI, Chapter LI, Section 490, which carries a potential penalty of up to 7 years of imprisonment.

In the case of Bob's attempted attack on Leonardo, it's noteworthy that this action does not presently amount to a committed crime, as the email did not reach Leonardo due to a misspelled email address. Nevertheless, it's essential to stress that engaging in such activities can have legal implications, as outlined in the Spam Act 2003. While Bob's current action remains within a legal gray area, it is crucial to recognize that pursuing similar actions in the future may lead to a violation of the Spam Act and associated legal consequences.

Formal conclusion.


There is no concrete evidence to support the assertion that Bob has misused the multiple copies of passports he obtained. Furthermore, the phishing email may be viewed as a failed attempt, and the fact that there is only one specimen of a phishing email diminishes its significance. It is also noteworthy that the computer accounts are not password protected, potentially exposing them to unauthorized access. In conclusion, there is no concrete evidence to substantiate the accusations against Bob.

Issue #1 - Contents Relating to Offence


Artifact 1 - Identity Theft through Phishing Email

	<p>Dear Leonardo,</p> <p>We have faced some problems with your account. Please update the account. If you do not update will be closed.</p> <p>To update your account, just confirm your information below:</p> <p>Name:</p> <p>Date Birth:</p> <p>Credit Card Number associated with Paypa.</p> <p>Street address.</p> <p>We thank you.</p>
File Name	Sent-1 – Sent Email Archive
Timestamp	Mon, 1 May 2023 10:57:06 AWST
IP Address	[192.168.1.50]
Type	Email - Text
Location	/img_DF232.dd/Users/Bob/AppData/Roaming/Thunderbird/Profiles/zscn2vzd.default-release/ImapMail/outlook.office365-1.com/Sent-1
Status	Allocated
MD5	74c42a529441bd2f60c579d838a99a29
Modified	2023-05-01 10:57:39 AWST
Accessed	2023-07-18 07:34:15 AWST
Created	2023-04-24 07:47:39 AWST
Changed	2023-05-01 10:57:39 AWST
Cluster (length)	965618 (4), 2172518 (2), 2250430 (1), 2254507 (4)
Logged User	Bob
Email Client	Thunderbird v.102.10.0
Analysis	This email exhibits classic characteristics of a phishing email, notably including typos and a clear intention to extract Leonardo's details related to his PayPal account. Of particular concern is the request for Leonardo's credit card number, which has raised red flags.

Artifact 2 - Unauthorized Identity Acquisition

	
File Name	PassportScans.zip
Type	Compressed Zip File
Content	89 copies of individual identity in format .jpg, .pdf, .bmp, .gif, .png and .tif
Origin	https://cloudstor.aarnet.edu.au/plus/s/W1zEz0tUffNEx9
Location	/img_DF232.dd/Users/Bob/Music/Classical Music/60s Music/Incomplete/PassportScans.zip
Status	Allocated
MD5	52bc1b6e02f00772ab5a161e22a03ae4
Modified	2023-04-03 08:02:29 AWST
Accessed	2023-04-03 08:07:52 AWST
Created	2023-04-03 08:02:22 AWST
Changed	2023-04-03 08:07:43 AWST
Cluster (Length)	6415029 (36130)
Logged User	Bob
Analysis	The file was located together with the unzipped content of the file in folder PassportScans. This zip file was downloaded from a link given to Bob from SovereignClassCitizen on HexChat application.

Artifact 3- Passport Modification / Forgery

	
File Name	ID.pdf
Type	Picture (.jpg) and PDF files
Origin	https://cloudstor.aarnet.edu.au/plus/s/bNAiHRCswZFyWt
Location	/img_DF232.dd/Users/Bob/Documents/SECRET/
Status	Allocated
MD5	5f8cfa1e17b711b5a5fb335c051d95cf
Modified	2023-04-03 07:59:44 AWST
Accessed	2023-04-03 08:00:28 AWST
Created	2023-04-03 07:59:43 AWST
Changed	2023-04-03 07:59:44 AWST
Cluster (Length)	5927649 (8); 579567 (41)
Logged user	Bob
Analysis	3 passport copies for a person named Bob Sacamano. 2 out of 3 have the same photograph of Bob, while the other one has a moustache. All three have different details pertaining to Bob. Varied passport details for identical names suggests forgery. The link to download the files were given by SovereignClassCitizen user in HexChat application.

Artifact 4 - Identity Theft Intent Confession

	<p>[SovereignClassCitizen has address ~SovereignClassCitizen@139.230.02E3C3.288C92]</p> <p>Apr 03 07:52:21 <SovereignClassCitizen> hello again</p> <p>Apr 03 07:52:38 <Bobthebuilder> Do you have the files I needed?</p> <p>Apr 03 07:52:48 <SovereignClassCitizen> I do</p> <p>Apr 03 07:55:01 <SovereignClassCitizen> With great power, comes great responsibility, remember that!</p> <p>Apr 03 07:55:05 <SovereignClassCitizen> What is your aim?</p> <p>Apr 03 07:55:12 <SovereignClassCitizen> Why do you want these identities?</p> <p>Apr 03 07:55:49 <Bobthebuilder> I lost my job and discovered easier ways to make money through identity theft</p> <p>Apr 03 07:56:08 <SovereignClassCitizen> I understand</p> <p>Apr 03 07:59:13 <SovereignClassCitizen> Use this to start with: https://cloudstor.aarnet.edu.au/plus/s/bNAiHRCswZFyWt</p> <p>Apr 03 08:00:40 <Bobthebuilder> Received, thank you</p> <p>Apr 03 08:00:53 <SovereignClassCitizen> I will kill the data soon, so take it quicky</p> <p>Apr 03 08:02:08 <SovereignClassCitizen> I hope you find the following usefuf for your adventure</p> <p>Apr 03 08:02:10 <SovereignClassCitizen> https://cloudstor.aarnet.edu.au/plus/s/W1zEz0tUffNEx9</p> <p>***** ENDING LOGGING AT Mon Apr 3 08:04:06 2023</p>
File Name	SovereignClassCitizen.log
Type	Log - Text File
Timestamp	2023-03-04 07:52:21 – 08:02:10
Location	/img_DF232.dd/Users/Bob/AppData/Roaming/HexChat/logs/AustNet/SovereignClassCitizen.log
Status	Allocated
MD5	7aa9cea3824b783f45e493cb575ecf49
Modified	2023-04-03 08:04:06 AWST
Accessed	2023-04-03 08:04:06 AWST
Created	2023-03-27 10:16:58 AWST
Changed	2023-04-03 08:04:06 AWST
Cluster (length)	926952 (1)
User	Bob
Analysis	A conversation between Bob and SovereignClassCitizen expressing his intention of earning money by Identity Theft. Earlier in the conversation, there is indication that Bob paid SovereignClassCitizen to forge the passports. Links to previous downloads are recorded in this document. The close timestamp and last access date hint at this being Bob's final conversation with SovereignClassCitizen.

Issue #2 – Identification

Number of user profiles

Evidence: SAM file

Type: Windows Registry file

In the SAM file extracted from the DF232.dd image, data pertaining to the quantity of user profiles within the image can be extracted. This data aids in the identification of individuals with system access. It's worth noting that although usernames may not necessarily correspond to real names, data can still be organized according to the usernames linked to them.

Username	Last Login Time	Account Disabled	Password Required
Bob	18/7/2023 7:49:53	False	False
secret	18/7/2023 7:50:49	false	false

Analysis:

Utilizing the registry viewer, profile details indicate the presence of two active accounts, namely Bob and 'secret.' Interestingly, the last login times for these two accounts differ by just one minute, suggesting that Bob could be associated with the 'secret' profile. Furthermore, both accounts lack password protection, indicating a high level of trust between these two users if there are more than one.

Logged User at Event

Evidence: Security.evtx

Type: Windows Security Event Log file

Utilizing Event Viewer to retrieve user logon information from file security.evtx allows us to pinpoint the individual who was in control at the time when the evidence was either downloaded or introduced into the computer.

Event	User	Logon Time	Logoff Time	Last Accessed/Timestamp
SoverignClassCitizen.log	Bob	3/4/2023 7:51:01 AWST	3/4/2023 8:09:20 AWST	3/4/2023 8:04:06 AWST
Download Scan_epson.jpg	Bob	3/4/2023 7:51:01 AWST	3/4/2023 8:09:20 AWST	3/4/2023 8:00:06 AWST
Download passport.jpg	Bob	3/4/2023 7:51:01 AWST	3/4/2023 8:09:20 AWST	3/4/2023 8:00:17 AWST
Download ID.pdf	Bob	3/4/2023 7:51:01 AWST	3/4/2023 8:09:20 AWST	3/4/2023 8:00:28 AWST
Download PassportScan.zip	Bob	3/4/2023 7:51:01 AWST	3/4/2023 8:09:20 AWST	3/4/2023 8:07:52 AWST
Phishing Email	Bob	1/5/2023 10:27:29 AWST	1/5/2023 10:57:51 AWST	1/5/2023 10:57:01 AWST

Analysis:

Hexchat communication and Passports Download - The event log analysis reveals that on 3/4/2023 at 7:51:01 AWST, 5 activities occurred when Bob logged in. He initiated communication with SoverignClassCitizen and subsequently downloaded the following files: "ID.pdf," "Scan_epson.jpg," "passport.jpg," and "PassportScan.zip." The minimal time gaps between the last accessed timestamps of these files suggest that they were downloaded in succession. The synchronization between the timestamps of Bob's conversation with SoverignClassCitizen and the last accessed metadata of the files strongly indicates Bob's involvement in downloading the files. Additionally, the origin of these files aligns with the links provided by SoverignClassCitizen in the HexChat conversation, further substantiating the connection between the two events.

Phishing Email - Upon comparing the email header timestamp with Bob's logon and logoff times, it strongly suggests that the email was sent while Bob was actively logged on. Furthermore, the email was sent from the address bobthecoolbuilder@outlook.com. Further examination of the Sent-1 file revealed that this particular email account is consistently used by Bob for his personal communication purposes.

Issue #3 – Intent

Unconventional File Location

Evidence: places.sqlite - FireFox

Type: Sqlite Database

Analysis: The unconventional location of the file implies a deliberate effort by Bob to conceal its existence. Places.sqlite is the file archive of FireFox web browser. Using Autopsy as tool to process the database, it is evident that PassportScans.zip was downloaded at 3/4/2023 8:02:22 AWST. This matches with the Created Time of the file. According to Autopsy directory of Data Artifacts/Web Downloads, PassportScans.zip is supposed to be stored at folder Downloads. Upon using keyword search, it was discovered the location [of PassportScans.zip](#) is at [/img_DF232.dd/Users/Bob/Music/Classical Music/60s Music/Incomplete/PassportScans.zip](#).

Web Searches & Web Downloads

Evidence: History – Microsoft Edge

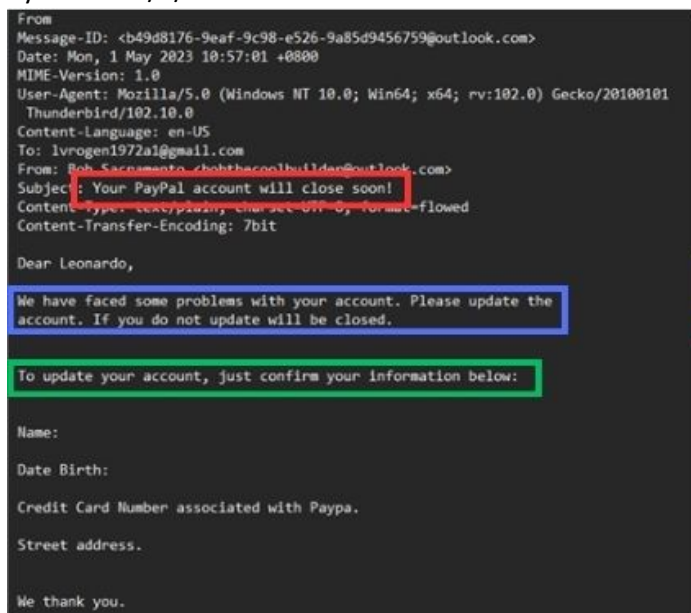
Type: Sqlite Database

Analysis: Storing these files discreetly within a folder named 'Windowz,' Bob exhibited an intention to obscure the downloaded files within the computer's typical 'Windows' directory. This move could potentially sow confusion for anyone accessing the system. History is a file archive of Microsoft Edge web browser. Using Autopsy as tool to process, it allows the investigator to analyze the history of Web Searches and Downloads. This examination unveiled a significant event on 1/5/2023 at 07:52:22 AWST when Bob initiated a web search using the keywords 'common phishing email.' The search led him to the website at [Log10PhishingEmailCrafting](#). During his visit to the website, Bob downloaded six files related to scam examples.

Evidence: Example of a Pay Pal Scam.webp

Type: Image

Among the 6 files discovered, the file [Example of a Pay Pal Scam.webp](#) is interestingly similar to [the Phishing Email](#) sent by Bob on 1/5/2025.



Attention! **Your PayPal account will close soon!**

Dear Member,

We have faced some problems with your account Please update the account .if you do not update will be Closed.

To Update your account, just confirm your informations.(only takes a minute.)

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm that you're the owner of the account, and then follow the instructions.

[Relog in your account now](#)

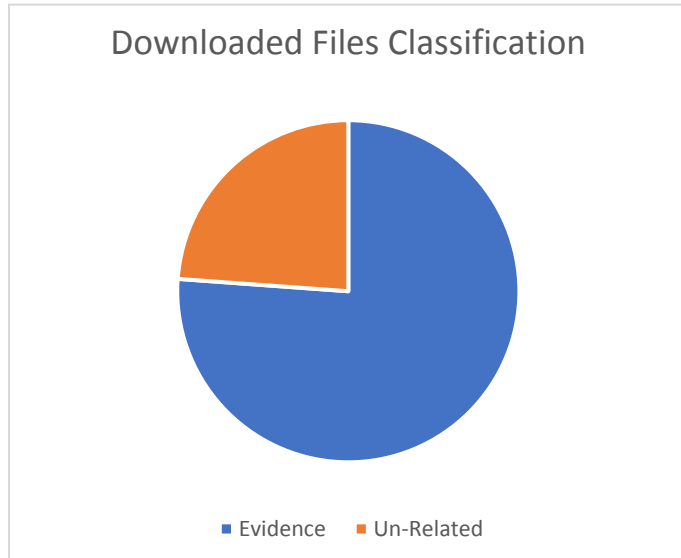
Analysis: The striking similarity between the email's subject and body strongly suggests that Bob employed the downloaded file as a template for crafting the phishing email.

Issue#4 Quantity of Evidence

Total Downloaded files vs Illegal Natured Files

Evidence: Web Downloads extracted by Autopsy

Numerous downloaded and extracted files were organized in a table to assess their relevance. This allowed for a clear distinction between the weight of pertinent downloads compared to unrelated ones.



Passport Scans of Individuals	Evidence	89	Files
Bob Sacamano's Passport	Evidence	3	Files
Phishing Email	Evidence	1	Files
Examples of scam	Evidence	6	Files
	Total	99	Files
.jpg downloaded	Un-related	16	Files
.exe downloaded	Un-related	2	Files
.png downloaded	Un-related	4	Files
.torret downloaded	Un-related	1	Files
.webp downloaded	Un-related	6	Files
.zip downloaded	Un-related	2	Files
	Total	31	Files

Analysis: Data above is extracted from the number of files downloaded and decompressed files from web and stored into the computer. It is distinct the number of evidences outweigh the number of un-related downloads.

Total images and pdfs Vs. Illegal Natured Files

Evidence:

- Autopsy: Data Artifact /File Views/File Types/By Extension/Images
- Autopsy: Data Artifact /File Views/File Types/Documents/PDF

Types	In Computer	Illegal Natured	(%)
Images & PDF	21357	99	0.464%

Analysis: There are 21,272 image files and 85 PDF documents discovered within the computer. Comparing the numbers to illegal natured files, the number is not significant.

Issue #5 – Installed Software

Evidence: SOFTWARE

Type: Windows Registry

- **HexChat v.2.16.1** – Installed

Analysis: HexChat is an open-source communication tool. This tool was used by Bob to communicate with SovereignClassCitizen on 27/3/2023 and 3/4/2023, where Bob was able to obtain 3 copies of Bob Sacamano's Passport and 89 other passport copies.

- **Thunderbird v.102.10.0** – Installed.

Analysis: Thunderbird is the email client application which is installed in the computer that Bob used to launch his phishing email to Leonardo at lvrogen1972a1@gmail.com

- **7-zip 22.01(x64) v.22.01** – Installed

Analysis: 7 zip is a free and open-source file archiver. The existence of this software complements Bob's intention in downloading the Kali Linux torrent as the outcome of the download is a .7z file and it will require 7-zip to decompress and extract the content.

Evidence: Web Downloads extracted from places.sqlite – Firefox

Type: Sqlite Database

- **Social Engineer Toolkit Master** – Downloaded

Analysis: The Social Engineer Toolkit Master is a framework tool employed by penetration testers for security assessments. Within this framework, there are tools designed for sending phishing emails with the objective of illicitly obtaining personal information from the target without their consent. This toolkit is designed to run on a Linux environment. However, there is no evidence that the toolkit or even the Linux environment is installed in the computer. The discovery of this aligned to the suspicion that Bob might be engaging in identity theft themed crime.

- **Kali Linux Torrent** – Downloaded

Analysis: It is evident that Bob visited Kali Linux website, and leads to downloading a torrent file for Kali Linux called kali-linux-2023.1-vmware-amd64.7z.torrent. Torrent file is a BitTorrent file that allows users to download and share files with users all around the internet. There is no evidence that a BitTorrent client was installed on the computer. However, the discovery of Kali Linux torrent file, complement the discovery of Social Engineering Toolkit. The outcome of a successful download from the torrent file will a zipped Kali Linux installation file called linux-2023.1-vmware-amd64.7z. The particular file was discovered on Bob's Desktop, however the content is not Kali Linux, but repeated strings of "Thank you for supporting Thunderbird, which is funded by users like you! Producing Thunderbird requires software engineers, designers, system administrators and server infrastructure. So if you like Thunderbird, the best way to ensure Thunderbird remains available is to make a donation."

Evidence: /img_DF232.dd/Users/Bob/Documents/TC/TrueCrypt.exe

Type: Executable

- **True Crypt v.3.0** – Discovered

Analysis: TrueCrypt is a free encryption software that is widely available on the internet. A folder called TC was discovered, which contains True Crypt applications and supporting files. The time of Last Accessed of the TrueCrypt.exe is 18/7/2023 7:36:52 AWST, which implies Bob had executed the application to perform encryption. The purpose of encryption might be to conceal files or drives which may hold valuable information to prevent any unauthorized access.

Running Sheet

	Date & Time	Hypothesis, Strategy, Technique and Tools	Steps & Result									
Log #1	18/10/2023 10:30 PM – 19/10/2023 12:40 AM	<p>Hypothesis: Bob is the user of the computer.</p> <p>Strategy: Discover how many users registered to the machine. Investigate if any of the users are related to Bob.</p> <p>Technique: Extract SAM file from the machine and extract the username, last logon time and password required.</p> <p>Tools: Autopsy, Registry Viewer</p>	<p>Using Autopsy, locate and extract the Security Account Manager (SAM) file at /img_DF232.dd/Windows/System32/config/SAM</p> <p>Open SAM file using Registry Viewer to path: /SAM/Domains/Account/Users</p> <p>Result:</p> <p>2 Enabled Account: Bob, secret</p> <table><tr><th>Username</th><th>Last Logon Time</th><th>Password Required</th></tr><tr><td>Bob</td><td>17/09/2023 23:49:53</td><td>false</td></tr><tr><td>secret</td><td>17/09/2023 23:50:49</td><td>false</td></tr></table> <p>Username Bob which highly relatable to the suspect was found, and judged my last logon time suggest Bob and secret are active users of the computer.</p>	Username	Last Logon Time	Password Required	Bob	17/09/2023 23:49:53	false	secret	17/09/2023 23:50:49	false
Username	Last Logon Time	Password Required										
Bob	17/09/2023 23:49:53	false										
secret	17/09/2023 23:50:49	false										
Log #2	19/10/2023 12:50 AM – 01:00 AM	<p>Hypothesis: Bob uses the computer to engage in illegal activities.</p> <p>Strategy: Discover contents from Bob’s account that may seem illegal in nature.</p> <p>Technique: Start exploring with personalized folder such as Desktop, Documents and Downloads.</p> <p>Tools: Autopsy</p>	<p>Start with Bob Account:</p> <p>Explore the content and identify folder or file in folder Desktop, Documents and Downloads.</p> <p>Result:</p> <p>Folder: /img_DF232.dd/Users/Documents/SECRET</p> <p>Files: ID.pdf, passport.jpg, scan_epson.jpg</p> <p>Three passport copies with identical name and similar portrait might indicate forgery.</p>									
Log #3	19/10/2023 01:00 AM – 01:17 AM	<p>Hypothesis: Files were downloaded by Bob.</p> <p>Strategy: Discover how the files appeared on the computer. Was it downloaded from internet or created by Bob. If downloaded, it aligns with allegation of illegal online activity.</p> <p>Technique: Perform keyword search on Autopsy to identify potentially traces of the file’s origin.</p> <p>Tools: Autopsy</p>	<p>Perform keyword search for ID.pdf, passport.jpg, and scan_epson.jpg</p> <p>Result:</p> <p>All 3 of the keywords appeared with Web Downloads and Web History Artifact.</p> <p>Origin URL: https://cloudstor.aarnet.edu.au/plus/s/bNAihIRCSwZFyWt</p> <p>This result support the hypothesis that the files were downloaded by Bob.</p>									
Log #4	19/10/2023 09:30 AM – 09:45 AM	<p>Hypothesis: Bob found the URL online.</p> <p>Strategy: Find traces of the origin URL. If traces were discovered, Bob might have obtained the URL online. Otherwise, the URL might have been obtained offline.</p>	<p>Perform keyword search to identify origin of URL.</p> <p>Keyword: https://cloudstor.aarnet.edu.au/plus/s/bNAihIRCSwZFyWt</p> <p>Result:</p> <p>/img_DF232.dd/Users/Bob/AppData/Roaming/HexChat/logs/AustNet/SoverignClassCitizen.log</p>									

		<p>Technique: Perform a keyword search with origin URL as the keyword.</p> <p>Tools: Autopsy</p>	<p>A conversation log belonging to HexChat application was discovered containing the URL. Within the log, it was discovered that Bob was communicating with an online entity called SovereignClassCitizen on 3rd April 2023 at 07:52:21 AWST. The URL link is given by SovereignClassCitizen to Bob to support his intention to perform identity theft.</p>
Log #5	19/10/2023 09:55 AM – 10:07 AM	<p>Hypothesis: SovereignClassCitizen is Bob's supplier of illegal documents.</p> <p>Strategy: Explore the log and discover additional information that may support the hypothesis.</p> <p>Tools: Autopsy</p>	<p>Inspect the content of the log.</p> <p>Result: A URL: https://cloudstor.aarnet.edu.au/plus/s/W1zEz0tIUffNEx9</p> <p>Within the log, SovereignClassCitizen supplied Bob the link above and wishes Bob it will aid Bob's adventure.</p>
Log #6	19/10/2023 10:10 AM – 10:15 AM	<p>Hypothesis: The link contains illegal documents.</p> <p>Strategy: Discover traces of where the link might lead Bob to. Remnants of downloads will give more clarity to Bob's intentions.</p> <p>Technique: Perform a keyword search with the URL link. Explore laterally to discover what was downloaded and locate the file(s).</p> <p>Tools: Autopsy</p>	<p>Perform keyword search to identify potentially traces of file downloaded from the link.</p> <p>Results: Web Bookmarks Artifact Web Downloads Artifact – C:/Users/Bob/Downloads/PassportScans.zip Web Downloads Artifact – C:/Users/Bob/Music/Classical Music/60s Music/Incomplete/PassportScans.zip</p> <p>Expand directory: /img_DF232.dd/Users/Bob/Music/Classical Music/60s Music/Incomplete/ Result: PassportScans folder contains 89 passport scans and copies with multiple extensions.</p> <p>Given the absence of any information regarding possession consent from the owners of the passports, this event can be categorized as the illegal acquisition of identity through theft.</p>
Log #7	19/10/2023 10:20 AM – 11:30 AM	<p>Hypothesis: Bob is the user who downloads these illegal documents.</p> <p>Strategy: Validate the user who downloads the contents by auditing the log file. Security.evtx is a windows registry file that logged security events such as time of user logs on or logs off, failed attempts to log in, etc.</p> <p>Each file has meta data which records the time of last accessed, last modified, last changed and the created date. If files were downloaded, the last accessed date will reflect the time they were obtained, which can later be compared to the user's logged-on and logged-off times.</p> <p>If these timestamps fall within the period when the user was logged in and logged off, it strongly suggests that the user is the one who downloaded the files.</p>	<p>Locate the time of Bob log into Hexchat in the HexChat log file SovereignClassCitizen.log Result: 3/4/2023 7:52:21 AWST</p> <p>Locate the Modify Time of the file ID.pdf, passport.jpg, scan_epson.jpg to identify the time the file downloaded. Result: ID.pdf – 3/4/2023 7:59:44; passport.jpg – 3/4/2023 7:59:49; scan_epson.jpg – 3/4/2023 7:59:53</p> <p>Locate the Modify Time of the file PassportScans.zip to identify the time the file downloaded. Result: 3/4/2023 8:02:09 AWST</p> <p>Locate and extract the security.evtx file from /img_DF232.dd/Windows/System32/winevt/Logs/Security.evtx</p> <p>Load Security.evtx to Event Viewer. Filter the current log to display entries from 3/4/2023 12:00:01 AM to 11:59:59 AM to display events occurred during the whole day.</p> <p>Apply the filter with EventID 4647, 4648.</p>

		<p>Technique: Extract the log security.evtx and load it to Event Viewer. Apply filter of EventID 4647.4648. EventID 4647 is associated with Logoff events, whereas EventID 4648 is associated with Logon Events.</p> <p>Tools: Autopsy, Event Viewer</p>	<p>Result: EventID 4648: 3/04/2023 7:51:01 AM Account Name: Bob EventID 4647: 3/04/2023 8:09:20 AM Account Name: Bob</p> <p>Bob logged in before the hexchat conversation and log off after Passportscans.zip last accessed.</p>
Log #8	19/10/2023 01:30PM – 02:00 PM	<p>Hypothesis: Bob has other methods of online communication.</p> <p>Strategy: Discover alternate method of communications such as Email or social media. Online communication logs might provide trails to illegal online activity.</p> <p>Technique: Use Autopsy to locate email client and email account associated to the email client.</p> <p>Tools: Autopsy</p>	<p>Using Autopsy, load image file DF232.dd, expand the directory tree to Data Artifacts/Installed Programs</p> <p>Result: Mozilla Thunderbird (x86 en-US) v.102.10.0</p> <p>Using Autopsy, expand the directory tree to Data Artifacts/ E-Mail Messages/Default Using the listing tab, sort the emails by Source Name, and locate email from source Sent-1.</p> <p>Result: bobthecoolbuilder@outlook.com</p> <p>Bob uses bobthecoolbuilder@outlook.com account to communicate with his contacts personally or to receive ads.</p>
Log #9	19/10/2023 02:00 PM – 02:12 PM	<p>Hypothesis: Allegation of illegal online activities might involve email communications.</p> <p>Strategy: Inspect email mailbox for contents might have illegal implications. Browse through Inbox, Sent mails, and deleted email.</p> <p>Technique: Use autopsy to browse the email. Visually identify suspicious email.</p> <p>Tools: Autopsy</p>	<p>Inspect email by expanding directory tree in autopsy to /Data Artifacts/E-Mail Messages/Default/Default</p> <p>Results: Potential Phishing Email in Sent-1</p> <p>File location: <img_df232.dd appdata="" bob="" imapmail="" outlook.office365-1.com="" p="" profiles="" roaming="" sent-1<="" thunderbird="" users="" zscn2vzd.default-release=""> <p>There is evidence suggesting that Bob attempted to scam Leonardo by sending a phishing email, which falsely warned of the closure of a PayPal account. The email exhibits classic phishing characteristics, notably the typos.</p> </img_df232.dd></p>
Log #10	19/10/2023 07:35 PM – 07:40 PM	<p>Hypothesis: Bob engaged in identity theft through phishing email.</p> <p>Strategy: Search for Phishing content related item. If there is evidence that the phishing email is a follow up action from a series of phishing related event, then the phishing email is legit. Otherwise, Bob might just want to remind Leonardo about his Pay Pal account.</p>	<p>Expand the directory tree of Data Artifacts to path: Data Artifacts/Web History Locate entries with Date Accessed 1/5/2023</p> <p>Result: A web search with keyword “common phishing email” at 1/5/2023 07:52:22 AWST using Microsoft Edge A visit to website with URL https://blog.usecure.io/the-most-common-examples-of-a-phishing-email</p>

		<p>Technique: Perform a keyword search with “phishing” as keyword and trace the follow up action initiated by Bob.</p> <p>Tools: Autopsy</p>	<p>Bob initiated a web search for common phishing email, and landed on a website that contains examples of scams. One of the examples is Pay Pal scams, which aligned with the content and structure of the identified email.</p>
Log #11	19/10/2023 07:42 PM – 07:54 PM	<p>Hypothesis: Bob uses examples from his web searches to craft a Pay Pal phishing email.</p> <p>Strategy: Discover if there is follow up action after accessing the website. If Bob downloads the examples, there is strong indication that Bob intentionally saved the content.</p> <p>Compare the timestamp of the sent mail to last accessed date of the Pay Pal scam example. If Bob downloaded the images from the web and used them as samples, the last accessed date of the image will align with the timestamp of the sent phishing mail.</p> <p>Technique: Use autopsy and expand the web downloads, locate the entries that relate to Pay Pal. Extract the file, open with Paint. Compare the email with example visually.</p> <p>Tools: Autopsy, Paint</p>	<p>Expand the directory tree of Data Artifacts to path: DataArtifacts/Web Downloads Locate entries with Date Accessed on 1/5/2023 and URL origin that matches: https://blog.usecure.io/the-most-common-examples-of-a-phishing-email</p> <p>Result: 6 files were downloaded from blog.usecure.io and saved at path: C:/Windowz Example of an email account upgrade scam.webp Example of a fake invoice scam.webp Example of a Nigerian scam.jpg Example of a Pay Pal scam.webp Example of a Drop box scam.webp Example of an unusual activity scam.webp</p> <p>Extract file Example of a Pay Pal scam.webp from locations /img_232.dd/Windowz/ and open the file with Paint application. Paint application able to open an image with .webp extension.</p> <p>Use Autopsy, expand the directory of Data Artifacts Open the sent email which located at: /img_DF232.dd/Users/Bob/AppData/Roaming/Thunderbird/Profiles/zscn2vzd.default-release/ImapMail/outlook.office365-1.com/Sent-1 Compare the two files visually.</p> <p>Result: Email and example are almost identical in structure. Bob did use the example as template.</p>
Log #12	19/10/2023 08:33 PM – 08:40 PM	<p>Technique: Compare the email timestamps and the example last accessed date.</p>	<p>Locate the file Example of a Pay Pal scam.webp, and identify the last access date. Result: 1/5/2023 10:55:28 AWST</p> <p>Compare with Email timestamp with Last Accessed date of the example. Result: 1/5/2023 10:57:01 AWST The example opened with a 1 minute 27 second difference. Highly likely that the email is crafted using the example as template.</p>

Log #13	20/10/2023 02:23 PM – 02:45 PM	<p>Hypothesis: Bob sent the phishing email using his computer.</p> <p>Strategy: Leverage the email header to identify the email client, and the origin IP address. If the header specifies the exact version of email client installed in the computer and the same IP address of the computer. It supports the hypothesis that the email is sent from Bob's computer.</p> <p>Technique: Use autopsy, locate the header of the phishing email. Inspect the header and identify the email client and the IP address.</p> <ol style="list-style-type: none"> 1. Compare the Email client version with the one installed in the machine. 2. Compare the IP Address origin with the machine's IP Address. <p>Tools: Autopsy, Registry Viewer</p>	<p>Email Client Steps On the selected email, select the Headers tab to view the email's header.</p> <p>Result: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Thunderbird/102.10.0</p> <p>Email client matched with previously identified application.</p> <p>IP Address Steps Inspect the Email Header and locate the IP address origin in the email header Result: 192.168.1.50</p> <p>Identify Machine IP Address Using Autopsy, extract file SYSTEM from /img_DF232.dd/Windows/System32/config/SYSTEM Using Registry Viewer, open SYSTEM file. Expand directory tree to SYSTEM/ControlSet001/Services/Tcpip/Parameters/Interfaces/{1aa607f1-afbc-4383-bdc2-2ae44165f9e5} Result: DhcpIPAddress 192.168.1.50 IP Address Matched</p> <p>Bob sent the email using the seized machine.</p>
Log #14	20/10/2023 06:25 PM – 07:32 PM	<p>Hypothesis: Bob is the one that sent the Phishing Email and downloads the examples.</p> <p>Strategy: Use event viewer to identify If the email is sent between the time when Bob logged on and logged off. This validate that Bob is in control of the machine when the examples were downloaded and the email was sent.</p> <p>Technique: Extract security.evtx from autopsy, and lot it to event viewer. Filter the log with EventID 4647 and 4648 to identify the logon and logoff activity.</p> <p>Tools: Autopsy, EventViewer.</p>	<p>Locate and load Security.evtx from /img_DF232.dd/Windows/System32/winevt/Logs/Security.evtx to Event Viewer. Filter the current log to display entries from 1/05/2023 12:00:01AM to 1/05/2023 11:59:59PM to display events occurred during the whole day.</p> <p>Apply the filter with input EventID 4647, 4648.</p> <p>Result: EventID 4648: 1/05/2023 7:40:08 AM EventID 4647: 1/05/2023 7:55:35 AM Example of Pay Pal scam.webp Created Time: 1/05/2023 07:54:15 AM</p> <p>Example of Pay Pal scam.webp is created/downloaded while Bob is logged on the computer.</p> <p>Result: EventID 4648: 1/05/2023 10:27:29 AM Account Name: Bob EventID 4647: 1/05/2023 10:57:51 AM Account Name: Bob Email timestamp: 1/05/2023 10:57:06 AM</p> <p>Phishing email was sent while Bob is logged on the computer.</p>

Timeline of Events

Time (AWST)	Event	Analysis	Evidence
3/4/2023 Event			
3/4/2023 7:51:01	Bob Log in to computer	Bob's login time before Artifact 2, 3, and 4 appears appears.	Running sheet log#7
3/4/2023 7:52:21	Bob converse with SovereignClassCitizen	Bob's logs in to HexChat.	Artifact #4
3/4/2023 7:59:20	Bob access link to https://cloudstor.aarnet.edu.au/plus/s/bNAihIRCSwZFyWt from log	The link is given by SovereignClassCitizen to Bob within the chat.	Places.SQLite
3/4/2023 7:59:44	Bob downloads ID.pdf and store it to /Users/Bob/Documents/SECRET	Bob intentionally downloaded and saved ID.pdf	Artifact #3 , Log#2
3/4/2023 7:59:49	Bob downloads passpot.jpg and store it to /Users/Bob/Documents/SECRET	Bob intentionally downloaded and saved passport.jpg	Artifact #3 , Log#2
3/4/2023 7:59:53	Bob downloads scan_epson.jpg and store it to /Users/Bob/Documents/SECRET	Bob intentionally download and saved scan_epson.jpg	Artifact #3 , Log#2
3/4/2023 8:02:14	Bob access link https://cloudstor.aarnet.edu.au/plus/s/W1zEz0tUffNEx9 from the log	Additional link which is also mentioned in the log.	Artifact #4 , Log#5
3/4/2023 8:02:22	Bob downloads PassportScans.zip to /Users/Bob/Downloads folder	Initially Bob downloaded PassportScans.zip to Downloads.	Evidence #13
3/4/2023 8:03:08	Classical Music Folder created		Issue #3 , Log#6
3/4/2023 8:07:04	60s Music Folder created within Classical Music		Issue #3 , Log#6
3/4/2023 8:07:13	Incomplete Folder created within 60s Music		Issue #3 , Log#6
3/4/2023 8:07:45	File PassportScan.zip moved to /Users/Bob/Music/Classical Music/60s Music/Incomplete/	PassportScans.zip moved to an unconventional location.	Issue #3 , Log#6
3/4/2023 8:07:45	Bob Extracted PassportScans.zip	Bob initiate extraction of the folder.	Issue #3 , Log#6
3/4/2023 8:07:50	PassportScans folder created at /Users/Bob/Music/Classical/Music/60s Music/Incomplete/PassportScans	Zip file extraction process created a folder with the name of the zip file.	Issue #3 , Log#6
3/4/2023 8:07:50 – 8:07:52	89 files pictures in .jpg and .pdf form placed in PassportScans folder	Content of the zip file placed inside the folder.	Issue #3 , Log#6 , Issue#4
3/4/2023 8:09:20	Bob log off out of the computer	Log off time after PassportScans.zip extracted.	Log#7
1/5/2023 Event			
1/5/2023 7:40:08	Bob logs in to Computer.	Bob's login time before Examples in Issue#3 appeared.	Log #14
1/5/2023 7:52:22	Bob searches for "Common Phishing Email" using Microsoft Edge	Bob begins researching for Phishing Email template.	Issue#3 , Log#10
1/5/2023 7:52:24	Bob visited https://blog.usecure.io/the-most-common-examples-of-a-phishing-email	Bob accessed the website intentionally.	Log#10

1/5/2023 7:54:14	Bob downloads Example of a Pay Pal scam.webp from https://blog.usecure.io/the-most-common-examples-of-a-phishing-email and save it to /img_DF232.dd/Windowz folder	Bob downloaded the examples and saved it on Windowz folder which might have intention to obscure it, confusing reader with "Windows" folder.	Issue#3 , Log#11
1/5/2023 7:55:35	Bob log off out of computer	Time Bob logs off the computer after examples in Issue#3 were downloaded.	Log#14
1/5/2023 10:27:29	Bob log in to Computer at	Time Bob logs on before phishing email in Artifact#1 sent.	Log#14
1/5/2023 10:50:34	Mozilla Thunderbird v.102.10.0 installed.	Bob installed Thunderbird v.102.10.0 before sending the email.	Issue#5 , Log#8
1/5/2023 10:51:22	Bob access https://www.kali.org/		Issue#5
1/5/2023 10:51:52	Bob downloaded a Kali Linux torrent from https://cdimage.kali.org/kali-2023.1/kali-linux-2023.1-vmware-amd64.7z.torrent using microsoft EDGE and saved it to /img_DF232.dd/Users/Bob/Desktop/LOL	Bob has intention of installing Kali Linux by downloading the installation image of Kali Linux. Downloaded file will be a 7z file.	Issue #5
1/5/2023 10:53:13	Bob searches for 7Zip using Firefox		Issue#5
1/5/2023 10:53:23	Bob downloaded 7z2201-x64.exe using Firefox	Bob downloads 7-zip installation file to extract Kali Linux image file downloaded.	Issue#5 , Issue#4
1/5/2023 10:53:28	Bob searches for social engineering toolkit		Issue#4
1/5/2023 10:53:32	Bob access https://github.com/trustedsec/social-engineer-toolkit		Issue#4 , Issue#5
1/5/2023 10:54:36	Bob downloaded social-engineer-toolkit-master.zip using Firefox		Issue#5
1/5/2023 10:55:28	Bob open Example of Pay Pal scam.webp with MSPAINT.exe	Bob uses paint application to open Example of a Pay Pal scam.webp	Evidence #9
1/5/2023 10:57:01	Bob sends out the Phishing Email.	This is the time when Bob sent the phishing email in attempt to scam Leonardo.	Artifact#1
1/5/2023 10:57:51	Bob logs off out of computer.	The time Bob logs off after Bob sent the phishing email.	Log#14