Case Study Report

Subhikaran GANESH KUMAR - 10609551

Department of Science: Edith Cowan University

CSI6205 – Digital Forensics

Dr Patryk Szewczyk

17th Oct 2024

Table of Contents

[Summary 3](#_Toc179994083)

[Content related to offense 4](#_Toc179994084)

[Identification 5](#_Toc179994085)

[Intent 6](#_Toc179994086)

[Quantity of Evidence 8](#_Toc179994087)

[Installed Software 9](#_Toc179994088)

[Running Sheet 10](#_Toc179994089)

[Timeline 15](#_Toc179994090)

# Summary

This report highlights the findings from the digital forensic investigation the image 2024-2.dd image file obtained from Linda’s laptop. Linda had been accused of possessing illegal files (any files pertaining to turtles), document that contains employee’s usernames and passwords and a highly confidential document. The digital investigation focuses on to accuse or exonerate Linda by applying scientifically validated digital forensic method.

Initially, the process begins by checking the integrity of the image file (2024-2.dd) provided and to ensure the authenticity of the evidence. The image was verified by calculating the MD5 hash and was verified with the value **b7cb6e8ad2ed5b89014f4ee25c05087e** provided in the question. Regular verification of the image is done to ensure the integrity of the image throughout the investigation process. The main purpose of the investigation is to find out whether the suspect (Linda) intentionally accessed illegal files and possessed confidential documents. Also, the presence of any malware in the system as stated by the suspect should be proven. Time zone for the investigation is set to be Australian Western Standard Time (AWST).

Tools used for the investigation process:

* Autopsy 4.21.0 – To conduct forensic investigation
* OSForensics 11.0 – To verify the key findings from Autopsy
* FTK Imager 4.7.1.2 – To verify the key findings from Autopsy
* Registry Explorer 2.0.0.0 – To view DAT files
* HashCalc 2.02 – To find the hash of files

Investigation findings:

1. List of Active user accounts in the system

* fishbowl: active account with 11 login counts (not password protected)
* lenovo: active account with 2 login counts (password protected)

1. Presence of illegal content

* Illegal files and images were found in multiple folders linked with the account username fishbowl.
* The presence of encrypted files was present under the /Users/fishbowl folder indicating a strong link to the user fishbowl.
* There seems to be no presence of illegal content related to the user account lenovo.

1. Intention of the user account fishbowl

* The web search and web download artifacts of the image file clearly suggests that the user account fishbowl intentionally accessed and downloaded illegal turtle files from the internet.
* There were evidences of encryption software (used to hide file) installed from the web like TrueCrypt 7.1 and KeePass 1.28 software to store passwords safely.
* The user fishbowl had searched for ‘common password’ just before proceeding with the encryption of the documents. This might indicate that someone is trying to frame Linda.
* The user account fishbowl had run the encryption software to conceal illegal and confidential documents.
* The account fishbowl further generated a file named Database.kdb using KeePass1.28 software for storing passwords for an online turtle server and Linda’s bank account.

1. Malware detection : Linda claimed that her Laptop was infected by malware. Upon analysing the image file, there seems to be no presence of malware in the system as stated by the suspect.
2. Quantity of Evidence (Severity of Crime): Upon the forensic image analysis, it was found over 139 files ( jpg/jpeg, png, gif) pertaining to the images of turtles. Along with 2 encrypted files containing crucial evidence for this investigation. There have been instances of connection of external USB drives such as IBM Corp, Alcor Micro Corp and SanDisk Corp. These devices were attached around the same time the illegal and confidential content were accessed. Conclusively, the illegal documents are transferred in and out the system. The connection of multiple USB devices suggests the possibility of storing illegal files and confidential document. This might indicate a possibility of distributing illegal content.

In conclusion, the investigation found out over 139 illegal images, 2 encrypted files (which includes the 2 sensitive documents) on Linda’s Laptop. These evidences are strongly linked with the user account fishbowl and intention of fishbowl to access these illegal documents have been proven by analysing the web history and web searches. However, since the fishbowl user account is not password protected it is impossible to narrow it down to a specific person. Additionally, the web searches for the ‘common passwords’ conducted by fishbowl before the encryption of illegal files might indicate a possibility that the illegal actor was looking to frame Linda.

# Content related to offense

Table 1: *Evidence table*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  |  | | --- | --- | | Name: | ninja.jpg (**Evidence 1**) | | Location: | /img\_2024-2.dd/Users/fishbowl/Documents/ | | Filename Allocation : | Allocated | | Size: | 49.2KB | | Modified: | 2015-02-05 10:34:16 AWST | | Accessed: | 2015-02-06 10:23:56 AWST | | Created: | 2015-02-06 10:23:56 AWST | | Changed: | 2015-02-06 10:23:56 AWST | | MD5: | 9eeb2ca99874e935bf2afcc00d8c653e | | Analysis: | This image was copied from an external USB drive around 10:23 AM on 6th Feb 2015 and copied into Documents folder of fishbowl. | |
|  | |  |  | | --- | --- | | Name: | sendbinary.asp.jpg (**Evidence 2**) | | Location: | /img\_2024-2.dd/Users/fishbowl/Pictures/ | | Filename Allocation: | Unallocated | | Size: | 21.8KB | | Modified: | 2015-02-06 10:37:31 AWST | | Accessed: | 2015-02-06 06:25:01 AWST | | Created: | 2015-02-06 06:25:00 AWST | | Changed: | 2015-02-06 10:37:31 AWST | | MD5: | 6d1940668752b308c65e67aba28a49d5 | | Analysis: | This evidence was accessed and downloaded by fishbowl user in reptilepark.com.au website and encrypted into **filesafe** file using Truecrypt 7.1. | |
|  | |  |  | | --- | --- | | Name: | Turtle17.jpg (**Evidence 3**) | | Location: | /img\_2024-2.dd/Users/fishbowl/Pictures | | Filename Allocation: | Unallocated | | Size: | 183KB | | Modified: | 0000-00-00 00:00:00 | | Accessed: | 0000-00-00 00:00:00 | | Created: | 0000-00-00 00:00:00 | | Changed: | 0000-00-00 00:00:00 | | MD5: | f15bff69c02867ff0afbadba5d8b138a | | Analysis: | The evidence was accessed and copied into the Pictures folder of fishbowl from an online turtle server named photographyblogger.net. This file was encrypted into **filesafe** using Truecrypt 7.1. | |
|  | |  |  | | --- | --- | | Name: | names.pdf (**Evidence 4**) | | Location: | P:/ | | Filename Allocation: | Unallocated | | Size: | 44.6KB | | Modified: | 0000-00-00 00:00:00 | | Accessed: | 0000-00-00 00:00:00 | | Created: | 0000-00-00 00:00:00 | | Changed: | 0000-00-00 00:00:00 | | MD5: | d954ebdcdb5fdf34de10813de8f3af3c | | Analysis: | This evidence contains usernames and password of employees and was copied from an external USB drive and was encrypted into **work** file. | |

# Identification

Firstly, it is important to analyse the total number of user accounts using the laptop. As this piece of information helps us to narrow down the investigation. Upon analysing the 2024-2.dd, the list of user account details has been identified and their details are listed down the below table. From the table 2, Linda’s laptop has 4 user accounts (Administrator, Guest, lenovo and fishbowl).

Table 2: User account details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Users | Login Counts | Creation Date | Last Login date | Settings |
| Administrator | 1 | 2015-01-20 09:56:36 | 2006-11-02 21:03:49 | Disabled |
| Guest | 0 | 2015-01-20 09:56:36 | N/A | Disabled |
| lenovo | 2 | 2015-02-05 10:41:42 | 2015-02-08 10:38:45 | Active |
| fishbowl | 11 | 2015-01-20 09:56:23 | 2015-02-08 10:42:00 | Active |

From the analysis, it was found that for the user account **fishbowl** is not password protected and the account has been logged in for 11 times. On the other hand, the user account **lenovo** is password protected and was logged in for 2 times. **Administrator** account has been logged once and is password protected. Furthermore, it can be inferred from the Table 2 that lenovo account is created after the fishbowl account and lenovo’s last login date is before fishbowl’s.

Evidence 1 (ninja.jpg), Evidence 2(sendbinary.asp.jpg) and Evidence 3(Turtle17.jpg) was linked with the user fishbowl. Evidence 1 was found in /img\_2024-2.dd /Users/fishbowl /Documents folder. Evidence 2 was deleted but a recycle bin artifact suggests that the Evidence 2 was present in Pictures folder of fishbowl user. Similarly, Evidence 3 was present in the Pictures folder of fishbowl user.

The encrypted files **filesafe** and **work** which contains evidences mentioned in the section *Content Relating to Offence* (Evidence 2, Evidence 3 and Evidence 4) and have been found in **/Users/fishbowl/Desktop/** and **/Users/fishbowl/Documents/** respectively. Encryption related contents were discussed in section *Encrypted files*.

Additionally, **/Users/fishbowl/Favorites** folder contains strong presence of turtle related websites and video URL had been present indicating a strong link with the user fishbowl.More number of illegal images (relating to turtles) have been found in **/Users/fishbowl/ Documents/**.

In conclusion, fishbowl user account has been linked with all the confidential documents and files pertaining to turtle which is deemed as illegal. From the forensics analysis using autopsy, it was also found out that the account fishbowl is not password protected. This implies that the account can be accessed by anyone and not be restricted to a single user.

# Intent

The forensic analysis of the image shows that the user account fishbowl intentionally accessed images or files regarding turtles and the highly confidential sensitive documents. By observing the web search of the user, fishbowl accessed the illegal content. From the figure 1, fishbowl intentionally searched for content relating to turtles in Internet Explorer and Firefox browsers.

Figure 1: Web search by fishbowl

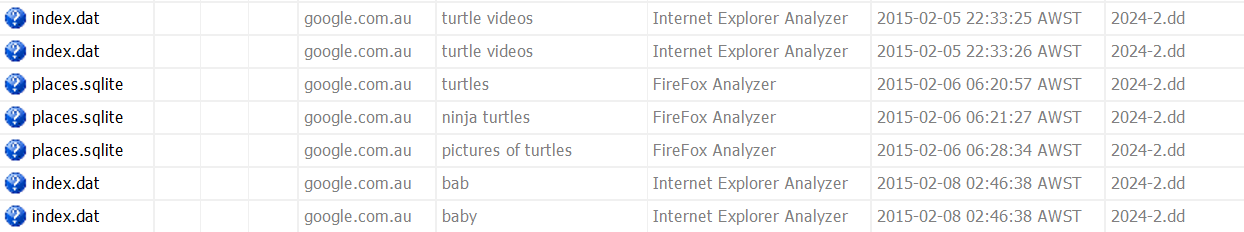


Figure 2: Web download artifact for **Evidence 2(sendbinary.asp.jpg)**

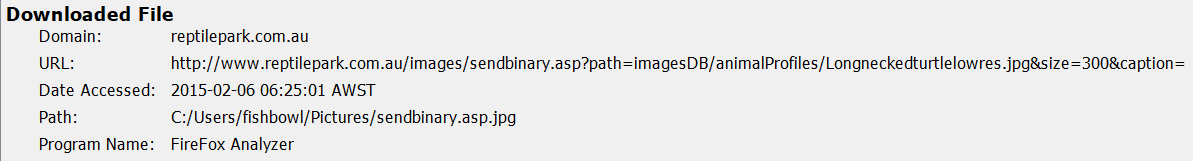


Figure 2 indicates that fishbowl downloaded the **Evidence 2** from **reptilepark.com.au** website. Evidently, the fishbowl intentionally accessed an illegal image and downloaded it from FireFox.

By reviewing the metadata of **Evidence 1**, the modified date is before the created date of the file. Consequently, this discrepancy in a metadata file can mean that this image file is copied from an external device like an USB drive. The image is created on the system on 10:23 AM at 6th Feb 2015. Around same time, external devices named IBM Corp, Alcor Micro Corp and Sony Corp had been attached to the system. Conclusively, Evidence 1 was transferred was transferred from the external devices connected. Also, this indicates the intention of the user trying to access illegal images. Similarly, around the same time names.pdf file (**Evidence 4**) is accessed by fishbowl user indicating that this file is transferred from external devices. From analysing the web history artifacts, **Evidence 3**(Turtle17.jpg) was accessed by fishbowl from an online turtle server named **photoblogger.net** user around 10:17 PM on 5th Feb 2015 (*Refer the timeline logs of TL5,TL6,TL7,TL12,TL13,TL14,TL18 and TL21)*.

By analysing the web search artifacts, the user account fishbowl searched how to hide files in web. Furthermore, encryption programs such as encryption programs such as KeePass 1.28 and TrueCrypt7.1 program have been installed from the internet on 5th Feb 2015. Interestingly, the fishbowl user also searched for common used passwords before running the encryption programs.

The password file generated using KeePass 1.28 which was Database.kdb contained information about Linda's bank account details and online turtle server password (Refer **RS10** log in Running sheet)

In conclusion, this shows the intent of the user fishbowl to access illegal content by looking at the web histories, searches artefacts. Since the fishbowl account is not password protected and the fishbowl user’s intentional search of common passwords before encryption might suggests that the illegal actor was trying to take advantage of the no password protected account and to frame Linda.

# Quantity of Evidence

The below table shows the quantity of evidence found out during the forensic analysis process. The total illegal number of evidences (images/files) is found out to be **142**.

Table 3: *Quantity of Evidence*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| File Type | Total Number | Number of evidence files | Percentage of Evidence | Relevance to the investigation |
| Database files | 43 | 1 | 2.33% | Database.kdb file is used to store the passwords for online turtle server and Linda’s bank account. |
| PDF documents | 22 | 4 | 18.4% | These files consist of techniques required to guide the user to conceal the information using encryption software. |
| Image files (jpg/jpeg, gif, png) | 1983 | 139 | 7.01% | These image files comprise of turtle images which is deemed as illegal. |
| Encrypted files | 2 | 2 | 100% | These encrypted files contain the sensitive information of usernames and passwords of employee’s and a highly confidential report. |
| HTML  files | 413 | 13 | 3.15% | HTML files indicates the user activities. In the 13 files there were evidences of turtle related websites visited |

# Installed Software

The below table list the software used on the system and their corresponding relevance to the case.

Table 3:*Installed Software*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Software | Used for | Date/Time (AWST) | Counts | Relevance to the investigation |
| Mozilla FireFox | To browse and download content from internet | 2015-02-08 11:06:00 | 4 | The user account fishbowl used this application to search and access content related to turtles. |
| Internet Explorer | To browse and content from internet | 2015-02-08  11:05:52 | 5 | The user account fishbowl used this application to search and access content related to turtles. |
| Adobe Reader | To view the files | 2015-02-08  10:47:24 | 10 | The user account fishbowl used the application to read guide documents on how to encrypt illegal files. |
| TrueCrypt 7.1 | To encrypt or conceal information | 2015-02-08  10:58:14 | 2 | This software is used to encrypted 2 confidential documents and some turtle images by fishbowl user. |
| KeePass 1.28 | To store passwords | 2015-02-08  10:59:15 | 1 | fishbowl account used this software to store the passwords for online turtle server and Linda’s bank account password. |
| Steghide | To conceal secret files using stenography | 2015-02-05  10:51:25 | 4 | fishbowl account used this software to conceal a confidential document in an image file. |
| Media Player | To view and play videos | 2015-02-08  10:56:25 | 14 | Fishbowl used this software to view video files pertaining to turtles. |

# Running Sheet

|  |  |  |  |
| --- | --- | --- | --- |
| Event logs (RS\*) | Time (AWST)  and Duration | Method | Result/ Analysis |
| RS1 | 08/09/2024  17:00  15 mins | Accessed the 2024-2.dd file from DF242 DO NOT DELETE folder and checked the hash of the file to verify the integrity using HashCalc software  ***Software Used:*** HashCalc 2.02 | **b7cb6e8ad2ed5b89014f4ee25c05087e** is the MD5 hash of the file and matches with the hash given in the question |
| RS2 | 08/09/2024  17:15  15 mins | Opened the existing case file created using 2024-2.dd in Autopsy software and opened the 242.aut file in Desktop/DF-CaseStudy/242/ folder in remote PC.  ***Software Used:*** Autopsy 4.21.0 | Opened the case successfully and were able to navigate through the file system of the 2024-2.dd file. |
| RS3 | 08/09/2024  17:30  15 mins | Analysed the Operating System user accounts in the given image file in autopsy 4.21.0. Selected the OS accounts section in the left pane of the Autopsy software to check the details of the login users  ***Software Used:*** Autopsy 4.21.0 | From Analysing, it was found there were 2 active accounts (fishbowl and lenovo). The user account fishbowl had over 11 logins and was not password protected. |
| RS4 | 08/09/2024  18:00  30 mins | Verified the Security Identifier (SID) of the active user accounts fishbowl and lenovo.  Navigated to the UsrClass.dat files in 2024- 2.dd /Users/fishbowl/ AppData/Local/Microsoft/Windows and 2024-2.dd /Users/ lenovo/AppData/Local /Microsoft/Windows and extracted to the desktop. Uploaded the extracted files to Registry Software  ***Software Used:*** Registry Explorer 2.0.0.0 | S-1-5-21-870810913-3780417518-2558847328-1000 – fishbowl  S-1-5-21-870810913-3780417518-2558847328-1001 – lenovo  These have been verified by using Registry Explorer 2.0.0.0 |
| RS5 | 08/09/2024  18:30  30 mins | Analysed the directories of 2024-2.dd in Autopsy 4.21.0 to find the illegal content in fishbowl user account. Navigated to 2024-2.dd/Users/fishbowl/ folder and browsed through it.  The MD5 hash value of **Evidence 1** was calculated by HashCalc  ***Software Used:*** Autopsy 4.21.0, HashCalc 2.02 | Found 9 jpg files (**Evidence 1 – ninja.jpg**) and 1 gif file related to turtles in the Documents folders of fishbowl user and found turtle-downloader-malware.exe and HIDING IMAGES OF TURTLES FOR DUMMIES.pdf in the Desktop folder.  MD5 hash of ninja.jpg **9eeb2ca99874e935bf2afcc00d8c653e** |
| RS5 | 08/09/2024  19:00  15 mins | Opened the case study file 2024-2.dd file in FTK Imager tool to verify the metadata and file properties of **Evidence 1**. Opened the case study and browsed through the evidence tree of 2024-2.dd image file. Extracted the Evidence 1 to the desktop and verified the hash of the evidence.  ***Software Used:*** FTK Imager 4.7.1.2, HashCalc 2.02 | The metadata of ninja.jpg has been verified by using FTK Imager tool.  MD5 hash of ninja.jpg **9eeb2ca99874e935bf2afcc00d8c653e**. Also, similar results were obtained as the RS4 event. |
| RS6 | 08/09/2024  19:15  30 mins | Analysed the directories of 2024-2.dd in Autopsy 4.21.0 and FTK Imager evidence tree to find the illegal content in lenovo user account. Navigated to 2024-2.dd/Users/lenovo/ folder and browsed through it  ***Software Used:*** Autopsy 4.21.0, FTK Imager 4.7.1.2 | No illegal documents were found linking to the user account lenovo in both Autopsy and FTK imager software. |
| RS7 | 09/09/2024  13:00  15 mins | Opened the case study and analysed to identify the presence of any encryption software provided in the image. Clicked on the Web downloads in Data artifacts section in left pane in Autopsy case file. Navigated to Users/fishbowl/Downloads.  ***Software Used:*** Autopsy 4.21.0 | Found Steghide.exe and KeePass.exe in Data artifacts.  Found TrueCrypt7.1 and KeePass 1.28 downloaded in /Users/fishbowl/Downloads/ folder. |
| RS8 | 09/09/2024  13:15  15 mins | Opened the Autopsy case study and analysed for any encrypted files in the image file. Clicked the Encryption suspected in Analysis results in left pane of autopsy case study and searched for any files with .kdb file extension.  ***Software Used:*** Autopsy 4.21.0, HashCalc 2.02 | Found 2 encrypted files named filesafe and work located in  /img\_2024-2.dd/ Users/fishbowl/Desktop and /img\_2024-2.dd/Users/fishbowl/Documents/work and Database.kdb file was found in /img\_2024-2.dd/Users/fishbowl.  MD5 hash of filesafe document **e256b9bd6333a5fc53f8cb826246710f**  MD5 hash of work document –  **7d593386f7e931d1ecedb6908471627a**  MD5 hash of Database.kdb –  **54fdc6ef06b0f6c80830325869b09f6b** |
| RS9 | 09/09/2024  13:30  15 mins | Opened the 2024-2.dd file in FTK Imager and extracted the the encrypted files **filesafe**, **work** and **Database.kdb** and check the hash of them using HashCalc to verify the files.  ***Software Used:*** HashCalc 2.02, FTK Imager 4.7.1.2 | MD5 hash of filesafe document **e256b9bd6333a5fc53f8cb826246710f**  MD5 hash of work document –  **7d593386f7e931d1ecedb6908471627a**  MD5 hash of Database.kdb –  **54fdc6ef06b0f6c80830325869b09f6b**  The integrity of the encrypted files was verified by using both FTK Imager and Autopsy software |
| RS10 | 09/09/2024  13:45  60 mins | Used truecrack 3.6 in kali to break the password of the 2 files (filesafe and work) by using brute force dictionary attack using rockyou.txt word list. And use john the ripper tool to crack the password storage file Database.kdb.  By running the following commands  ***truecrack -t filesafe -w /usr/share/wordlists/rockyou.txt***  ***truecrack -t work -w /usr/share/wordlists/rockyou.txt***  ***keepass2john Database.kdb > hash.txt***  ***john --wordlist=/user/share/wordlists/rockyou.txt hash.txt***  ***Software Used:*** Truecrack 3.6, john the ripper (v1.90) | The password for filesafe document is **“password1”**  The password for work document is **“leonardo”**  The username and password for online turtle server is **turtles** and **turtles1** respectively.  The username and password for Linda’s bank account is **12345678** and **turtles12** |
| RS11 | 09/09/2024  14:45  15 mins | Mounted the **work** file and analysed the content in the files using Truecrypt 7.1 software using the cracked passwords from the RS10 Event log.  ***Software Used:*** TrueCrypt 7.1 | * Found names.pdf (**Evidence 4**) which contains the usernames and password of employees of the organisation. * Found topsecret.doc which is deemed as confidential document * Found an illegal picture of turtle named bing\_baby\_turtle-t2.jpg |
| RS12 | 09/09/2024  15:00  15 mins | Mounted the **filesafe** file and analysed the content in the files using Truecrypt 7.1 software using the cracked passwords from the RS10 Event log.  ***Software Used:*** TrueCrypt 7.1 | * Found Turtle17.jpg (**Evidence 2**)containing Turtle image deemed as illegal * Found sendbinary.asp.jpg (**Evidence 3**) containing Turtle image deemed as illegal |
| RS13 | 10/09/2024  13:00  60 mins | Opened the case study and selected the keyword search feature of Autopsy in top right hand and searched for sendbinary.asp.jpg, Turtle 17.jpg and names.pdf and analysed the status and source of the files.  ***Software Used:*** Autopsy 4.21.0 | - sendbinary.asp.jpg file is linked with the user account fishbowl as the location of the file is /img2024-2.dd/Users/fishbowl/Pictures folder. The status of the sendbinary.asp.jpg file is unallocated in the memory. The recent document artifacts further suggest that this image was recently accessed. A web download artifact suggest that this image was downloaded from [www.reptilepark.com.au](http://www.reptilepark.com.au) website.  - Upon Analysing Turtle17.jpg search results, it is found that this image was unallocated and deleted in the system. Also, this image was found accessed in an online turtle server named [www.photoblogger.net](http://www.photoblogger.net) by fishbowl user account.  - Upon Analysing names.pdf search results, it is identified that the names.pdf is recently accessed by fishbowl account and was deleted. |
| RS14 | 10/09/2024  14:00  60 minutes | Analysed the intention of fishbowl user to access illegal content. Clicked the Web search, Web history artifacts and Web downloads in the Data artifacts section in the left pane on Autopsy case software.  ***Software Used:*** Autopsy 4.21.0 | Several web searches in google, firefox and Internet Explorer browsers and downloads – shows the intention of the fishbowl user account to access illegal content. Also, fishbowl user before encrypting the files had searched for the common passwords in web. |
| RS15 | 11/09/2024  13:00  15 minutes | Opened the case study and analysed the metadata of **Evidence 1** in the Users folder of fishbowl in Autopsy. Select the tree view in the left pane of autopsy and navigate to /Users/fishbowl/Documents/ folder and selected ninja.jpg file.  ***Software Used:*** Autopsy 4.21.0 | The metadata of ninja.jpg (Evidence 1)  Modified: 2015-02-05 10:34:16 AWST  Accessed: 2015-02-06 10:23:56 AWST  Created: 2015-02-06 10:23:56 AWST  Changed: 2015-02-06 10:23:56 AWST  There is some discrepancy in the metadata as the created date is after modified data stating the possibility of getting the images from external devices like USB drive. Suggesting that USB is connected around 10:30 6th Feb 2015. |
| RS16 | 11/09/2024  13:15  30 mins | Analysed for external devices attached to the system. Clicked on USB Device Attached in Data artifacts in left pane in autopsy  ***Software Used:*** Autopsy 4.21.0 | Sony Corp, IBM Corp and Alcor Micro Corp devices have been attached on 2015-02-06 10:43:53 AWST  ROOT\_HUB and ROOT\_HUB20 have been attached on 2015-02-08 10:38:21 AWST  SanDisk Corp have been attached on 2015-02-08 10:39:40 AWST  Sony Corp, IBM Corp and Alcor Micro Corp devices have been attached on 2015-02-06 10:55:42 AWST  ROOT\_HUB and ROOT\_HUB20 have been attached on 2015-02-08 20:23:58 AWST  Evidence 1 and Evidence 4 are potentially transferred from SONY Corp, IBM Corp and Alcor Micro Corp external devices. By viewing RS15 event log, the created time of ninja.jpg (Evidence 1) in the system is around 10:30 AM 6th Feb 2015 same time when the external devices are connected. The connected devices also indicate that backup of illegal images and documents were taken. |
| RS17 | 11/09/2024  13:45  15 mins | Analysed if the system was affected by malware. Navigated to 2024-2.dd/ ProgramData/Microsoft/ Windows Defender/Support/ folder and accessed the file **MPLog-11022006-050253.log**  ***Software Used:*** Autopsy 4.21.0 | The output of the scan file:  Start Time:Tue Jan 20 2015 10:09:28  End Time:Tue Jan 20 2015 10:09:28  Explicit resource to scan  Resource Schema:service  Resource Path:{18760F63-13E1-4432-BBF7-AB56C537608D}  Threat Count:1  Threat Name:Unknown  ID:2147483646  Severity:0  Number of Resources:1  Resource Schema:service  Resource Path:{18760F63-13E1-4432-BBF7-AB56C537608D}  End Scan  \*\*\*\*\*\*\*\*\*\*\*  This indicates that the system is not infected by any severe malware as claimed by Linda. |
| RS18 | 11/09/2024  14:00  15 mins | Navigated to 2024-2.dd/ ProgramData/Microsoft/ Windows Defender/Support/ folder and accessed the file **MPLog-11022006-050253.log**  ***Software Used:*** OSForensics 11.0 | RS17 Results were verified using OSForensics tool. |
| RS19 | 11/09/2024  14:15  15 mins | Closed the case study in Autopsy, FTK imager and OSForensics software |  |

# Timeline

|  |  |  |  |
| --- | --- | --- | --- |
| Event Logs  (TL\*) | Date/Time (AWST) | Events | Relevance |
| TL1 | 20-01-2015  09:56 | User accounts of fishbowl, Administrator and Guest were created | The user fishbowl is seen as the main user since the login counts are 11. Also, fishbowl account is not password protected. |
| TL2 | 05-02-2015  02:09:46 | KeePass – 1.28 zip file was installed in fishbowl user account | Encryption software had been installed by fishbowl used to hide sensitive/illegal files |
| TL3 | 05-02-2015  10:41:42 | User account lenovo was created | lenovo is also an active user with password protected with 2 login counts |
| TL4 | 05-02-2015  10:46:53 | TrueCrypt 7.1 exe file is installed in the system by the user fishbowl | Truecrypt is used to hide sensitive files |
| TL5 | 05-02-2015  22:15:26 | Web search of **pictures of turtles** by fishbowl user. | Fishbowl intention to access illegal pictures from the internet |
| TL6 | 05-02-2015  22:17:33 | Turtle19.jpg , Turtle17.jpg (**Evidence 3**) and Turtle20.jpg were accessed from [www.photoblogger.net](http://www.photoblogger.net) website by fishbowl | Fishbowl intention to access illegal pictures |
| TL7 | 06-02-2015  02:37:11 | Sendbinary.asp.jpg (**Evidence 2**) (turtle image is downloaded (Web history artifact) by fishbowl from [www.reptilepark.com.au](http://www.reptilepark.com.au) | Fishbowl intention to access illegal picture |
| TL8 | 06-02-2015  06:20:57 | Google search ‘turtles’ by the user account fishbowl (Web history accessed) | Intention to access turtle image (illegal) |
| TL9 | 06-02-2015  06:22:56 | Deep sea turtles in google by the user account fishbowl (Web history artifact) | Intention to access turtle images (illegal) |
| TL10 | 06-02-2015  06:23:56 | The user account fishbowl visited [www.reptilepark.com.au](http://www.reptilepark.com.au) website and accessed to eastern long necked turtle page | Intention to access turtle images (illegal) |
| TL11 | 06-02-2015  06:31:28 | Downloaded European-pond-turtle-132801.jpg from naturephoto-cz website linked with fishbowl | Intention to download turtle image (illegal) |
| TL12 | 06-02-2015  10:23:56 | **Evidence 1**(ninja.jpg) is copied from external drives to fishbowl the fishbowl user account in Documents folder. | Illegal image of turtle is copied to the system from external drives. |
| TL13 | 06-02-2015  10:37:46 | Truecrypt.exe have been run to encrypt the files and generate the **work** and **filesafe** files which are encrypted. | Encryption of sensitive and illegal files. |
| TL14 | 06-02-2015  10:43:53 | USB devices IBM Corp, Sony Corp and Alcor Micro Corp attached to transfer names.pdf in P:/ folder (**Evidence 4**) and topsecret.doc to the system | confidential documents are transferred using external devices. |
| TL15 | 06-02-2015  10:51:25 | Steghide.exe was run to conceal a data file accessed from the external devices to generate secret.jpg | Concealment of a confidential file. |
| TL16 | 08-02-2015  02:46:42 | Baby turtles google search by fishbowl | Intention to access and download illegal files |
| TL17 | 08-02-2015  02:58:48 | Searched in web ‘how to hide files’ by the user account fishbowl. | Intention to conceal sensitive data |
| TL18 | 08-02-2015  03:05:57 | The user account fishbowl searched for common passwords in google. | Intention to frame Linda by using weak passwords to encrypt important information. |
| TL19 | 08-02-2015  10:38:21 | External devices attached ROOT\_HUB20. | To transfer sensitive data and get a backup |
| TL20 | 08-02-2015  10:55:42 | External devices attached Sony Corp, Alcon Micro Corp and SanDisk Corp | To Transfer sensitive data and get a backup |
| TL21 | 08-02-2015  10:58:14 | KeePass 1.28 and Truecrypt program have been run. Database.kbd file (containing usernames and passwords for Linda’s bank account and online turtle server) has been generated | Encryption of sensitive data |
| TL23 | 08-02-2015  11:06:21 | Turtle dancing video watched in youtube linked to fishbowl (Web history artifact) | Intention to access illegal content |
| TL24 | 08-02-2015  20:33:58 | External device name ROOT\_HUB was connected | Backing up of illegal data and potential distribution of illegal content. |