Forensic Report

Nocatland Cat Possession Offense

Examiners' Name: Rashedun Nobi Chowdhury, Harin Wimalasiri, Anas Kwefati
Examination Number: Group_3

Examination Tasking:

On 30 September 2024 at 00:00, the task force manager assigned our team to the G3 task force to investigate a criminal case involving a suspect accused of petting a real cat and possessing cat-related photos, which violates laws 1.0, 2.0, 3.0, and 4.0 of Nocatland. As members of the task force, all three team members are authorized to examine, analyze, and present findings related to this case. The team structure assigns first responders to handle the identification and collection of digital evidence. In this instance, the first responder has utilized XRY to perform a physical acquisition of the suspect's smartphone.

Our task for the specified examination is to analyze the smartphone in the suspect's possession to determine their involvement in the alleged offenses. To reach a verdict, we will address the forensic questions outlined below, which are critical in determining whether the suspect is guilty. Additionally, we have been informed that intent and motive are significant factors, and as such, we will also examine any evidence that may indicate the suspect was coerced into taking the photos.

Chain of Custody:

Examination Number: Group_3
Examiners' Name: Rashedun Nobi Chowdhury, Harin Wimalasiri, Anas Kwefati

Date & Time	Action	Custodian	Location
October 17, 2024, 13:15	Download XRI files from the ftp link to a folder shared with Kali VM	Harin Wimalasiri	CS2 Lab, DSV
October 17, 2024, 13:47	Make SHA256 hash of the provided evidence	Rashedun Nobi Chowdhury	CS2 Lab, DSV
October 17, 2024, 14:05	Complete Imaging of the Evidence to another folder shared with Kali VM	Anas Kwefati	CS2 Lab, DSV

All actions taken on the evidence followed chain of custody protocols to ensure evidence integrity and prevent tampering.

Collection Details:

We have received three XRY files from the first responder. We are stating the file names and their respective **sha256** hash value below:

File Name	Hash Values
2023-03-29_16.43_cyfo_lab1----Samsung SM-G960f Galaxy S9 Duos TD-LTE--Google--01.xry	1b592b69551ba9ce8124ccb03821220fff4515952640a7f9e77db77ba00b7b17
2023-03-29_16.43_cyfo_lab1----Samsung SM-G960f Galaxy S9 Duos TD-LTE.xry	c15365096f29f8e334cfb762c970e78c26c65fa4829773f3d8e82c395adf1b2f
2023-03-29_16.43_cyfo_lab1.xrycase	e818d7d1be42a991c0e5ff357285520ad6f911df42b4c49c782a1d4bd59c7333

Evidence Details:

- **Android OS Version:** Android 10
- **Firmware Version:** G960FXXSHFUJ2
- **IMEI:**
  - 354663102138226
  - 35466310-213822-0
- **IMSI:** 240084718098318
- **ICCID:** 89460850027038455881
- **Phone Number:** +46767194924

Forensic Questions:

As part of our examination, we will seek to answer the following forensic questions:

1. **Presence of Cat-Related Photos**:

   Identify if the phone contains photos portraying real cats? If yes, how many?

2. **Source of Photos**:

   Of the identified cat photos, **individualize** how many were taken by the phone's camera as opposed to being downloaded from the internet or other external sources?

3. **AI-Generated Photos**:

   Does the phone contain any machine-learning-generated or AI-created cat images? If yes, how many?

4. **Petting Activity**:

   Has the petting of a cat occurred? If so, who was involved, when did it happen, where did it take place, and what were the circumstances? How many cats were involved? Has the same cat been petted multiple times, and if so, how many times?

5. **Obstruction of Justice**:

   Has the suspect attempted to deceive law enforcement by intentionally destroying, hiding, or tampering with evidence? If yes, how was this done?

6. **Accomplices**:

   Are there any suspected accomplices involved in the case? If so, who are they, and what is their potential role?

These questions will guide our forensic investigation and help determine the suspect's involvement and potential intent in the alleged activities.

Steps Taken:

In this section we will be briefing the steps we took to resolve the forensic questions. To ensure evidence integrity, all the steps mentioned in this section were performed on an image of the three files provided to us by the first responder.

Steps_FQ1: Presence of Cat-related images

Using the XAMN Viewer on the provided XRI file, we identified a collection of 71,970 images. This count includes cached files, thumbnails, and also deleted files.

We then loaded the pictures in the File Tree mode. We then looked at different folders under the userdata directory and were able to identify cat images on the following directories

1. **/media/Download**
2. **/media/DCIM**
3. **/media/picture**
4. **/media/android/data/com.discord/files/Pictures**

Note there are multiple **thumbnails and cached images** of cats. However, we are **not counting** them as cat images in possession.

Steps_FQ2: Source of Photos

In the course of our investigation, we followed the steps mentioned below to identify which cat images were captured by the phone:

1. We accessed **XAMN Viewer** and navigated to **Files & Media > Pictures** to locate the relevant images.
2. Using the **Report/Export** menu, we exported the filtered artifacts as files. In the export options, we deselected all unnecessary options and exported the files to a location shared with our Kali VM environment.
3. After switching to the **Kali VM**, we navigated to the directory where the files had been exported.
4. Inside the directory, we executed a Linux command using **exiftool** and **grep** to isolate the files captured by the specific phone camera. The command used was:
   ```
   exiftool *.jpg *.jpeg | grep 'File Name\|Camera Model Name' | grep 'SM-G960F' -B 1 | grep 'File Name'
   ```
5. Upon identifying the relevant file names, we returned to **XAMN**, where we applied a file name filter to locate the corresponding images.

6. Finally, within the **MetaData** panel in XAMN, we further refined the search by applying a filter based on the **software used** field.

After identifying the cat pictures taken from the phone, we used the process of elimination to identify the pictures that were downloaded from the internet or other external sources.

Steps_FQ3: AI Generated Photos

To identify if the evidence contained any cat images that were generated using AI or Machine Learning, we took the steps mentioned below:

1. Using the XAMN Viewer, we examined the suspect's search and browsing history on Chrome to determine if any searches were conducted for machine-learning-generated cat images.
2. Upon discovering that the suspect had visited the website https://thesecatsdonotexist.com/ , we navigated to this site.
3. On the website, we observed multiple cat images and proceeded to download one for comparison. It was noted that the downloaded image files followed a naming format similar to that of images found in the suspect's /media/Download folder, specifically cat**.jpg** (where **** denotes a number).
4. Recognizing this pattern, we copied the image address and identified a URL format for these images: xxxxx.cloudfront.net/0y/catzzzz.jpg, where y and z represent digits.
5. We systematically tested values of y from 1 to 7, while varying catzzzz.jpg between specific sets (cat4127, cat2252, cat2895).
6. Using the procedures outlined in Step 5, we identified three images with visual similarities to images on the suspect's phone. These images were subsequently downloaded and saved in a folder shared with our Kali VM.
7. To confirm if the images matched, we copied the three downloaded images from the suspect's phone, placing them in the folder where our reference images were stored.
8. We then executed the following Linux command in the Kali VM to analyze potential matches:
   ```
   ssdeep -d *.jpg
   ```

Steps_FQ4: Petting Activity

To verify if any petting had occurred, below steps were executed

1. **Image and Video Location:** We accessed XAMN Viewer and navigated to Files & Media > Pictures to locate the relevant images.
2. **Folder Navigation:** In File Tree view, we navigated to the folder /media/0/DCIM/Camera/, where we identified a video clip depicting the petting of a cat.
3. **Timestamp Verification:** We examined the creation timestamps of both the video and the cat petting image identified in Forensic Question 2 (FQ2) using XAMN Viewer.
4. **Location Extraction**: We used ExifTool on our Kali VM to extract the latitude and longitude coordinates embedded in the image metadata.
5. **Address Conversion**: The coordinates obtained were entered into https://gps-coordinates.org/coordinate-converter.php to determine the specific address where the incident occurred.

Steps_FQ5: Obstruction of Justice

In order to verify if the suspect had attempted to deceive the law enforcement by intentionally destroying, hiding, or tampering with evidence, we resorted to curving. Following steps were taken:

1. We followed the steps mentioned for FQ2 to identify if there are any cat images taken by the suspect's phone that have been deleted
2. We also looked at the communications apps present on the phone via XAMN viewer to see if there are any videos or images that were shared by the suspect to someone but had their original copies deleted from the phone
    a. Upon discovering a video in email attachment, we followed the steps mentioned in FQ4 to identify the location of the video recording.
3. We looked for traces of any communication app that the suspect would use to collect, transport, and store cat photos. In this step we also looked for apps that may have been deleted.
    a. We opened the phone in File Tree mode on XAMN Viewer
    b. We then navigated to the /data folder of /userdata directory and observed the list of packages available
4. We also looked at the com.sec.android.gallery3d on file tree mode to observe if there were traces of cat images as this folder often contains thumbnails for deleted images. (Athena Forensics, 2019)
5. By navigating to Web>Searches and Web>History on XAMN viewer we looked for any suspicious web searches related to evidence tampering

Steps_FQ6: Accomplices

We resorted to the following steps to identify if the suspect had any accomplices:

1. **Email Analysis**: Using the XAMN Viewer, we reviewed email communications on the suspect's device to identify any exchanges that may suggest collaboration with potential accomplices.
2. **SMS Examination**: We next examined SMS exchanges to verify if any messages indicated communication between the suspect and additional individuals.
3. **Chat Review**: Lastly, we analyzed the suspect's chat messages, focusing on Telegram conversations. Due to data limitations, only Telegram messages were accessible for review at this stage.

Results:

Suspect Identification:

Upon navigating to Device>Device Accounts from XAMN viewer we observed that the name of the device account is "**Foren Sics**". We believe this is the name the suspect used to set up the account. Additionally, we observed that the email account associated with the suspect to be fsics7581@gmail.com. This assumption is supported by the following premises:

1. Mentioned email was also used to set up the device as per email sent by googlecommunityteam-noreply@google.com at 11:49:52 on 3/26/23
2. The email was used to set up the discord account "**catlover420**"
    a. As per the mail sent from notifications@discord.com at 12:32:26 on 3/26/23
3. This is the email account that was used to communicate with "Johannes Olegard"

Examination Findings:

Image Possession and Petting:

We identified **12 images** of cats across various directories on the suspect's phone, with 3 images specifically depicting cat petting. The distribution of these images is as follows: 5 in the **Download** folder, 3 in the **DCIM** folder, 3 in the **Pictures** folder, and 1 in the **Discord** folder. We also found a few drawings and photorealistic images of cats as cached files. However, it is important to note that **thumbnails or cached images of cats were excluded from this count**.

Upon analyzing the dHash values of the images, we determined that the image in the Discord folder is identical to one in the Pictures folder. Consequently, the **unique count of cat images** on the **suspect's phone is 11**.

The steps mentioned in steps_fq2 allowed us to individualize 6 cat images that were taken by the suspect's phone. Note that we were also able to recover 3 cat images that were deleted by the suspect through carving; the other three were still on the phone. If we **count the deleted** files, the **total number of cats amounts to 14.**

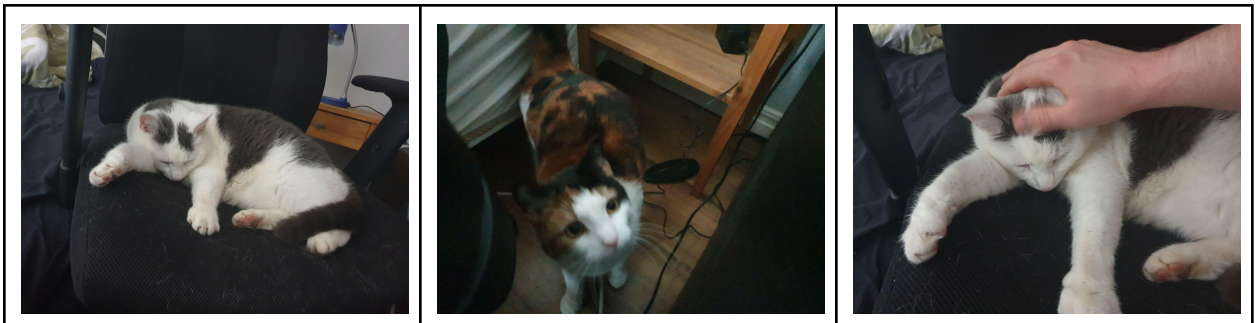

Table 1: Cat images captured by the suspect's phone

The suspect also had AI generated cat images on their phone. After following the steps mentioned in the Steps_FQ3, we found 100% matches between the images in the suspect's download folder and the sample machine learning generated images of cats of the site that the suspect visited.

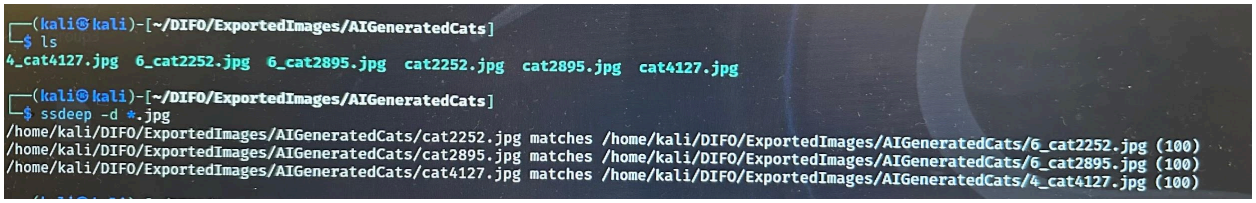

Fig 1.: Matches of Suspect's image and Sample AI Generated Cats

Table 2.: AI Generated Cats

Evidence also confirms that the petting of a cat by the suspect has occurred. This is substantiated by a video obtained through the steps outlined in Forensic Question 4 (Steps_FQ4) and an image recovered via the steps in Forensic Question 2 (Steps_FQ2).

Upon examining the video, it is clear that the suspect petted the cat **while wearing gloves.** Conversely, in the image identified in FQ2, the suspect is seen petting the cat **without gloves**,

suggesting that the incident took place on **at least two separate occasions.** Based on visual analysis, we conclude that the **same cat** was involved in both instances.

- **Video timestamp**: 2023-03-26 12:02:03
- **Image timestamp:** 2023-03-26 11:56:51
- **Image and Video location**: Lohäradsvägen 263, 761 72 Norrtälje, Sweden

Type of Images	Count
Total Cat Images	14
Petting Cats	4
Cat Images - Taken by Phone	6
Cat Images - Taken by Phone [Not Deleted]	3
Cat Images - Taken by Phone [Deleted]	3
Cat Images - Downloaded from External Sources	8
Petting Cats - Taken by Phone	2
Petting Cats - Taken by Phone [Not Deleted]	1
Petting Cats - Taken by Phone [Deleted]	1
Petting Cats - Downloaded from External Sources	2
AI Generated Cat Images	3

Table 3.: Breakdown of Cat Images

We also identified **two images of cat petting on the Downloads** folder. However, the image **metadata suggests** that these photos were not captured by the suspect's phone.

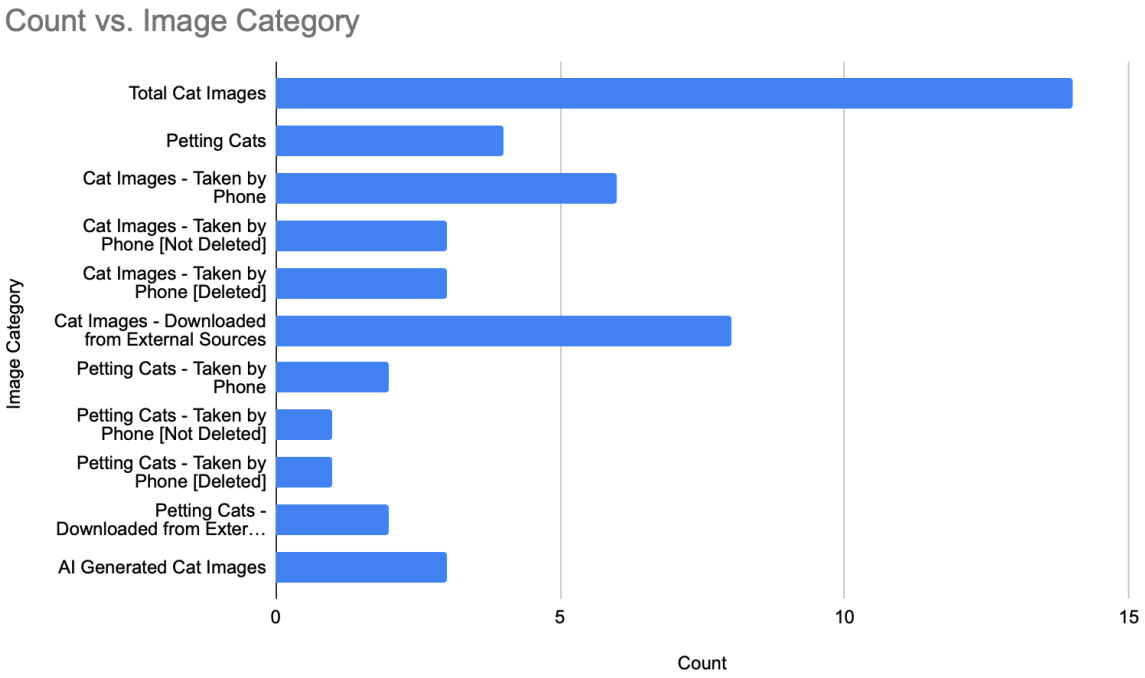

Fig 2: Distribution of Cat Images

Evidence Tampering:

Through our investigation, we came across multiple pieces of evidence that the suspect was deliberately trying to get rid of any evidence associated with the incident. We successfully recovered three carved files containing images of cats. These three images were deleted from the phone.

Additionally, in the **user's Gmail account**, we discovered a **video attachment** showing the suspect **discarding a glove previously used to pet the cat**. Using **ExifTool**, we determined that the video was **recorded at Stockholm University - Department of Computer and Systems Sciences (DSV), located at Borgarfjordsgatan 10, 164 55 Kista, Sweden**. The recording timestamp is **2023-03-27 12:52:06.**

We also uncovered a **Telegram message** sent to ID 5663170269 that read, "**You can prove NOTHING!**" This message suggests a deliberate intent by the suspect to destroy evidence.

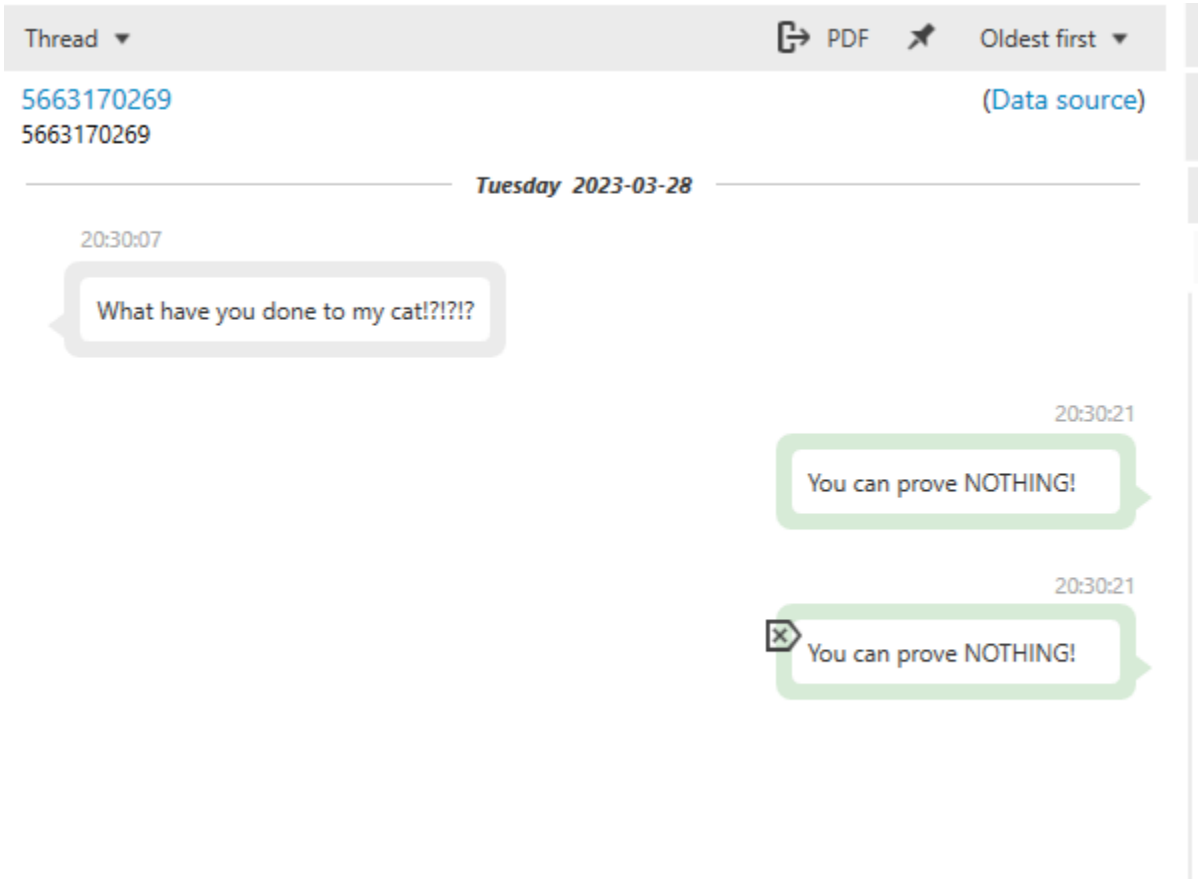

Fig 3.: Telegram conversation between the suspect and a victim

In reviewing the suspect's emails, we found that their email was used to register a **Discord account** under the **username** "**catlover420**". Although we did not find the Discord app on the suspect's phone, **file carving** in XAMN Viewer revealed the **com.discord package**. Further

carving efforts led to the recovery of several cat images saved in Discord's cache folder, indicating that the suspect likely used Discord to collect and share cat images.

Athena Forensics reports that "Even when the original version of the image is deleted, a copy within the com.sec.android.gallery3d folder remains." Following this lead, we navigated to the com.sec.android.gallery3d directory and recovered multiple copies of deleted cat images. Meaning the suspect was in possession of many cat images that he later deleted.

Finally, we observed that the suspect used Google Chrome to search "how to get away with petting cat" at 12:28:41 on 2023-03-26, an indicator that they were looking for ways on how to get away with the crime.

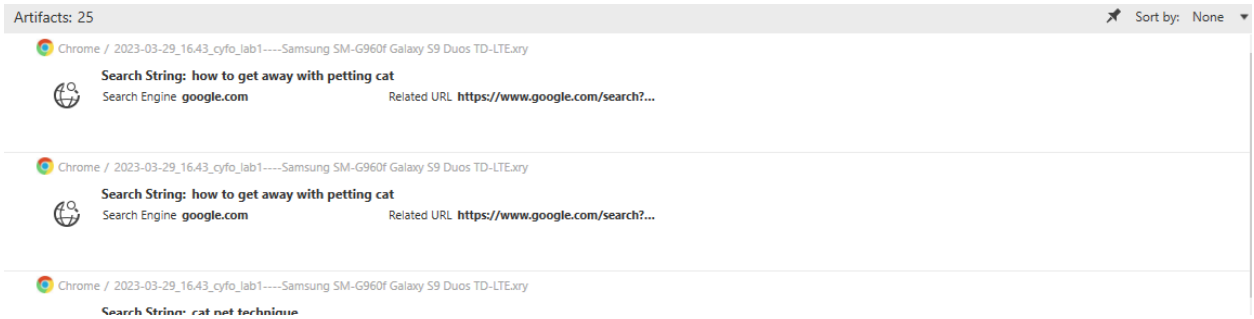

Fig 4.: Suspect's browser history

Accomplices:

Upon opening the XRY file handed to us by the first responder on XAMN viewer, we observed that there were multiple emails that were exchanged between the email address fsics7581@gmail.com and johannes.olegard@dsv.su.se

The first email we could recover from the evidence shows an email with the subject line "I did it" and the message body also contained the same message. We are unable to recover the exact time of when the email was sent.

On an email sent by "Johannes Olegard" on 3/27/23 12:47:42, (10:47:42 UTC) to the owner of the email address fsics7581@gmail.com , Mr. "Johannes Olegard" instructed the suspect to get rid of all the evidence. The email read "Get rid of all evidence".

To which the suspect replied "Done" on 3/27/23 12:51:19, (10:51:19 UTC). This email also contained a video clip of the suspect hiding a blue colored glove inside a white cupboard.

Upon receiving the email, Mr. "Johannes Olegard" further instructed the suspect via email on 12:52:55 of 3/27/23 to delete the video clip he had sent. This email contained general profanity, the word "idiot".

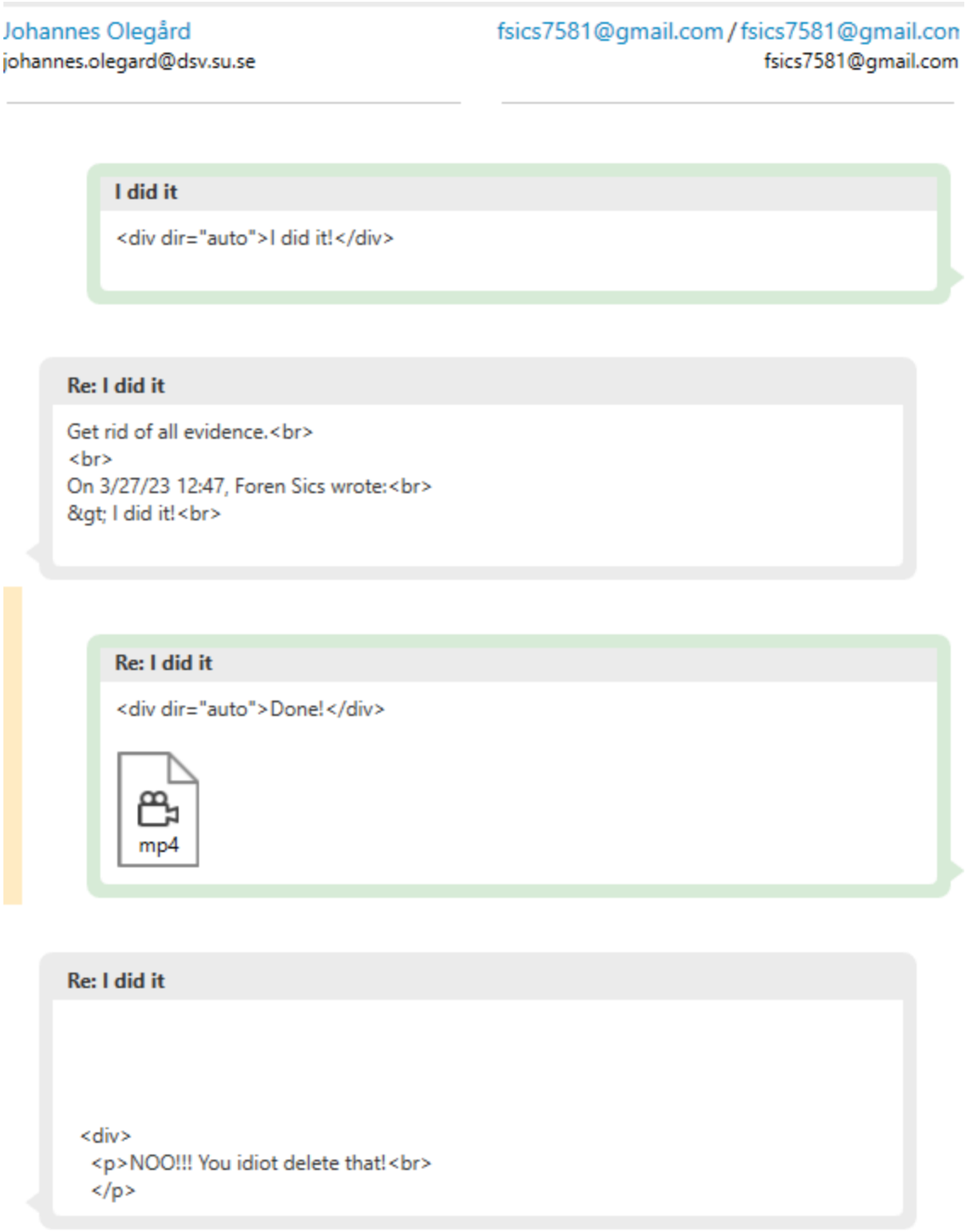

Fig 5.: Email exchanges between the suspect and Johannes Olegard

Based on the analysis of the email exchanges, it is our assessment that Mr. **"Johannes Olegard"** played a central role in the cat petting incident.

Additionally, we identified SMS communications between the suspect and a contact named "**Hallsta Rokeri**". The content of these messages suggests that "Hallsta Rokeri" may have been a victim in this case. We also uncovered communications with a Telegram account linked to the suspect. Although we were unable to retrieve the account owner's name, the context of the chat suggests that this individual may also have been a victim.

Conclusion:

Based on the evidence presented to us, we are able to prepare the following timeline of important events:

Date	Time	Event
3/26/2023	11:49:52	Completes account setup on the phone as per the email
	11:56:51	Takes a picture of him petting a cat
	12:02:03	Records a video of himself petting the cat wearing a glove
	12:28:41	Searches for how to get away with cat petting
	12:32:26	Creates an account on Discord
3/27/2023	12:47:42	Johannes Olegard instructs the suspect to get rid of the evidence
	12:51:19	Suspect sends an email saying evidence have been removed along with a video attachment
	12:52:55	Johannes Olegard instructs the suspect to delete the video sent as attachment
3/28/2023	20:30:07	A probable victim sends a message to the suspect, asking their cat's wherabouts
	20:30:21	The suspect responds saything that the victim will not be able to prove anything

Based on our forensic examination and analysis, we are able to conclude that, the suspect bearing the account name "Foren Sics" on the phone provided to us have violated the following laws of Nocatland:

1. **Law 1.0:** Possession of cat photos is illegal
2. **Law 2.0:** Capturing photos of cats is illegal
    a. **Law 2.1:** Capturing and Possessing cat photos
3. **Law 3.0:** Pet (or touch)ing a cat is illegal
4. **Law 4.1:** Petting one cat once is punishable by jail time.
5. **Law 4.2:** Petting two or more times (serial petting) is punishable by death (whether the same cat multiple times or multiple cats).
6. **Law 5.0:** If the suspect intentionally tries to obstruct the police, this can be held against them, possibly resulting in a more severe sentence.

Opinions:

In our assessment, “Johannes Olegard” appears to have played a significant role in the cat petting incident. However, there is **no conclusive evidence** to suggest that the suspect, “Foren Sics”, **was compelled** by Mr. Olegard to take the photos.

Additionally, we believe that the glove discarded by the suspect at **Stockholm University - Department of Computer and Systems Sciences (DSV), Borgarfjordsgatan 10, 164 55 Kista**, Sweden, is a **critical** piece of **non-digital evidence**. We recommend that the investigative team pursue this lead to further substantiate the case.