# Report

*by* Alish Mahat

**Submission date:** 27-Apr-2025 10:00PM (UTC+0545)
**Submission ID:** 2658288849
**File name:** Report_AlishMahat_23000965.docx (6.03M)
**Word count:** 1732
**Character count:** 10563

# Digital Forensic Investigation Report

Investigator: Alish Mahat
Date/Time of investigation: 2024/04/08, 8:26 AM
Place: Kathmandu, Nepal
Case: James Laptop

UWE Bristol | University of the West of England

# Contents

## Investigator Details

1. Investigator: Alish Mahat
2. Qualifications: Currently studying BSc (Hons) Cybersecurity and Digital Forensics
3. Experience: Skilled in using forensic tools such as Autopsy, FTK Imager, and Regripper to conduct digital forensic investigations.

## Summary

This report presents findings of forensic examination conducted on James laptop. The examination focused on identifying digital artifacts relevant to suspicions of international travel and possible creation of fake passports.

The analysis included the acquisition and analysis of James laptop disk image, Focusing on web browsing history, image metadata (EXIF data), deleted files, and USB device activity. The investigation found evidence, such as suspicious web searches related to fake passport creation, EXIF data from images indicating locations outside the United Kingdom, and recovered deleted files containing samples of passports.

Further, checking USB devices and recently downloaded files also showed the presence of encryption tools, Fake passport and some encrption suspected files. The evidences observed during the forensic analysis may support further investigation into unauthorized activities. However, this report is limited to factual findings based on the data recovered.

## Evidence Investigated

1. Web History

   I. Evidence: Reviewed James web browsing history to identify any suspicious activities.
   II. Findings: Several search terms were identified that indicated possible involvement in illegal activities, including:
      - "Create fake passport"
      - "Fake passport meme"
      - "Temporary email service"
      - "UK to Netherlands by car"
      - "Travel to France by car"
      - Visited website offering fake Ukrainian passports.
   III. Verification: Web history was retrieved from laptop using Autopsy. All data was cross verified with timestamps and metadata to ensure accuracy.

2. EXIF Data from Images

    I. Evidence: EXIF metadata from images found on James laptop was analysed to identify geolocation data of last 10 days that could indicate international travel.
    II. Findings:
        a. IMG_6325.JPG: Latitude: -22.478058, Longitude: 28.712825 (Botswana).
        b. IMG_4418.JPG: Latitude: -33.920005, Longitude: 18.422919 (Cape Town, South Africa).
    III. Verification: EXIF metadata was analysed. The locations identified in the EXIF data were also cross-checked in Google Maps to confirm the accuracy of the geolocation coordinates.

3. Recovered Deleted Files

    I. Evidence: Used data carving module where deleted files were recovered from James's laptop. It included images and documents that were potentially linked to fake passport.
    II. Findings: Multiple images of fake passports were recovered, including Ukrainian, Russian, and UK passport samples.
    III. Verification: The integrity of recovered files was validated using hash comparison methods, ensuring that no data was altered during the recovery process.

4. USB Devices and External Drives

    I. Evidence: Laptop was analysed for connected USB devices or external drives that might have been used to transfer any files.
    II. Findings: Two USB devices were detected, named USB Tablet and Robot_Hub. These devices were connected to laptop, and their activity was examined for relevant files.
    III. Verification: USB activity was examined, and file transfer logs were reviewed.

5. Recent Downloads

    I. Evidence: The download history was analysed to check for suspicious files related to passport creation or fraudulent activities was downloaded.
    II. Findings: A file passport-sample.jpg was downloaded from a suspicious site (img.pravda.com).
    III. Verification: The download activity was verified. File timestamps and domain names was cross-checked to ensure the legitimacy of the downloaded file and the website.

## Software Utilised

1. Evidence Acquisition: The device was acquired using Autopsy (Version 4.21.0).

   Description: Autopsy is an open-source digital forensics tool that provides a graphical interface for analyzing disk images. It is used for extracting web history, recovering deleted files, and analyzing file metadata.

2. Data Analysis: Examination was performed using Autopsy(4.21.0), FTK Imager (3.1.2.0), Regripper (4.0), and Windows Event Viewer.

   - FTK Imager (3.1.2.0): A forensic imaging tool used to create exact copies of devices, recover deleted files, and verify evidence integrity.
   - Regripper (4.0): A tool for extracting and analyzing data from Windows registry hives, useful for gathering user/system information.
   - Windows Event Viewer: A tool used to examine system, security, and application logs, useful for timeline analysis and user activity verification.

## Forensic Analysis

1) On 8th April 2025, I began the forensic acquisition of the laptop image "james_laptop_forensic_image.E01" . I verified the image by checking MD5 and SHA hash values to maintain integrity and verfired it on FTK Imager by checking MD5 and SHA.

2) After completing acquisition, I analyzed the extracted image using forensic tools focusing on web history, downloads, USB activity, encrypted files, user activity, EXIF metadata, and carved deleted files.

3) I used the following tools for forensic analysis, licensed for use:

- Autopsy v4.21.0
- AccessData FTK Imager v3.1.2.0
- Regripper v4.0
- Windows Event Viewer

## Relevant Findings

1. File System Information

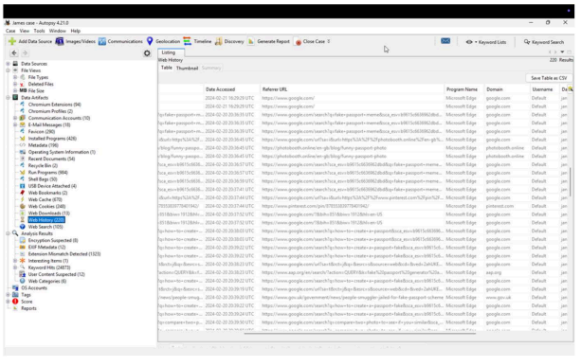
   Operating System: Windows 10 Enterprise was identified from the SOFTWARE registry hive.

   Timezone: The system timezone was set to GMT+00:00 UTC.

   Username: A single user account was identified with the username user. No password protection was applied to the account.

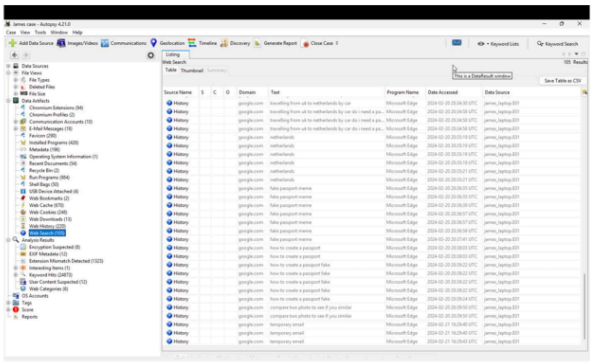
2. Web history

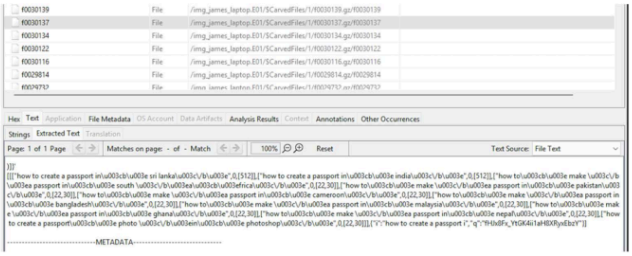
The web history analysis revealed that James performed multiple searches related to fake passport creation and temporary email services. Search queries included "fake passport meme," "how to create a fake passport," and "compare two photos to see if you are similar." The accessed websites were primarily through Google and photoabchi.online, using the Microsoft Edge browser. The activity indicates research towards document forgery and identity manipulation.

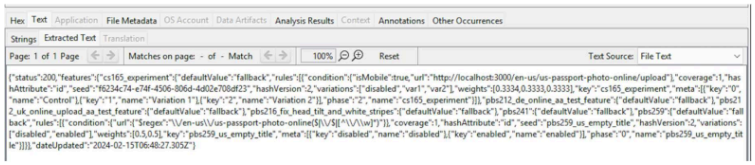


3. Web search

   The web search analysis showed that James performed multiple searches on topics related to international travel and fake document creation. Search terms included "travelling from UK to Netherlands by car," "do I need a passport to travel from UK to Netherlands," "fake passport meme," "how to create a passport," "temporary email," and "compare two photos to see if you are similar." All searches were conducted using Google through the Microsoft Edge browser. The search activity suggests efforts towards planning unauthorized travel and obtaining fraudulent documentation. Also found some searches in cache as the suspect searched for options to create passport in different countries and had also uploaded a picture in a site.

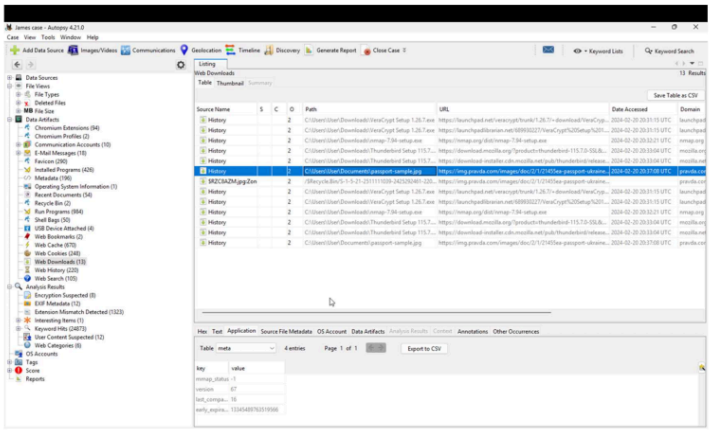






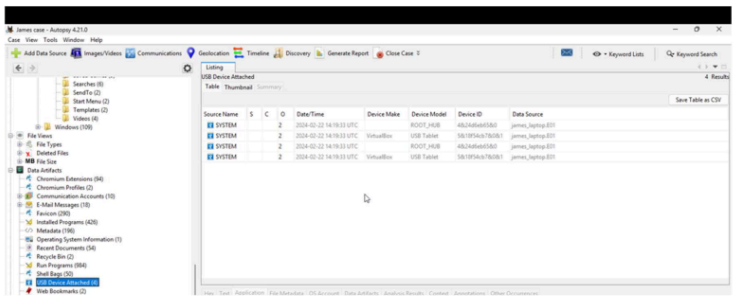
4. Web download

The web download analysis revealed that James downloaded multiple files, including an encryption tool, a messaging client, and a fake passport sample. The files included the VeraCrypt Setup installer, Thunderbird Setup installer, and a document named passport-sample.jpg. The passport-sample.jpg file was downloaded from the domain pravda.com, linking to a Ukrainian passport sample. These download activities suggest an intention to use encryption for securing files, a messaging tool for communication, and fake documents to facilitate identity forgery.



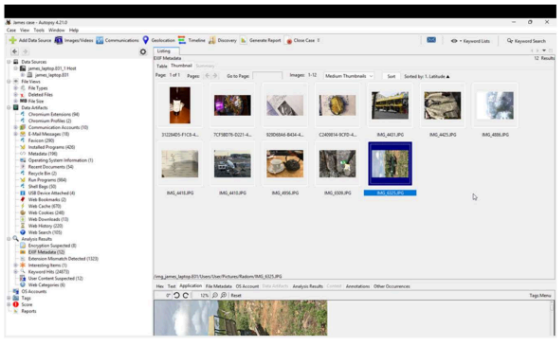
5. USB device found

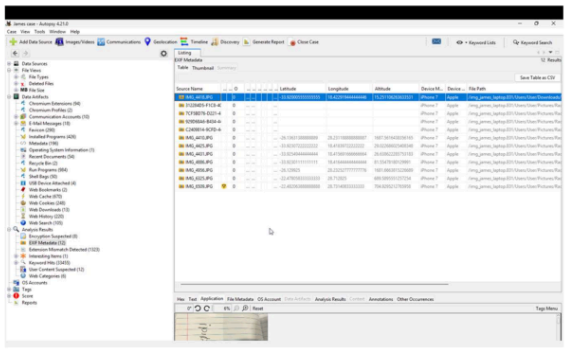
The analysis of USB device attachment history revealed that two external devices were connected to James' laptop. The devices identified were ROOT_HUB and USB Tablet, associated with VirtualBox. The connections occurred on 22nd February 2024. The activity suggests that external devices, possibly virtualized USB drives, were used during the investigation period, potentially for transferring or storing sensitive data.



6. Exif metadata

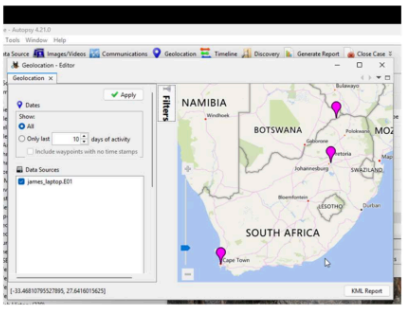
EXIF metadata was extracted from images found on James' laptop. Several images, including IMG_4418.JPG and IMG_6325.JPG, contained embedded GPS coordinates. The metadata revealed that the images were taken using Apple iPhone devices. Latitude and longitude values pointed to locations such as Botswana and Cape Town, South Africa. Other metadata fields confirmed device model and file storage paths under the user's Pictures directory.

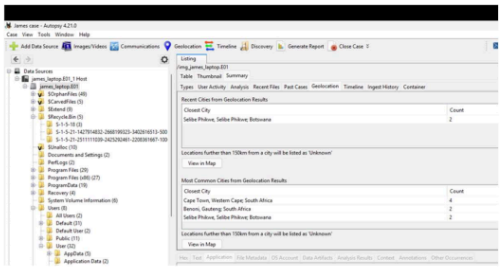




7. Geographical location

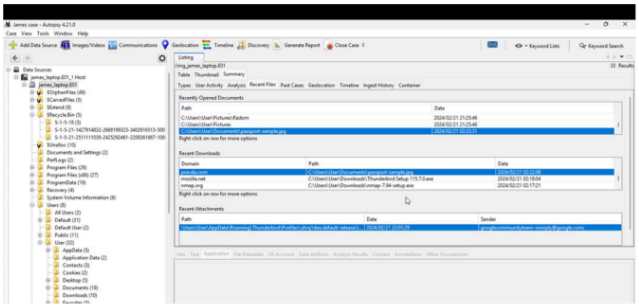
The geolocation analysis, based on extracted EXIF metadata, identified several international locations associated with James' activities. The most common cities detected were Cape Town (Western Cape, South Africa), Pretoria (Gauteng, South Africa), Gaborone (Botswana), and Selebi Phikwe (Botswana). The mapping of geolocation data further confirmed travel outside the United Kingdom during the period under investigation.



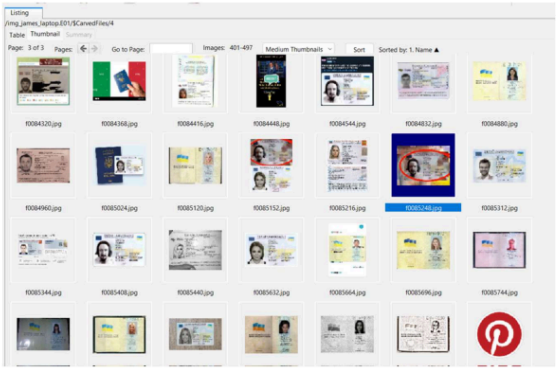
8. User activity

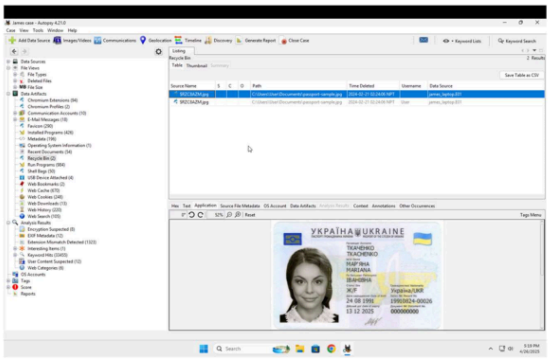
The user activity analysis revealed that James recently accessed files such as passport-sample.jpg stored in the Documents folder. Recent downloads included the VeraCrypt Setup installer, Thunderbird Setup installer, and nmap. Additionally, recent email attachment activity was detected through the Thunderbird email client, referencing an incoming message from a Google domain. These activities suggest active handling of encryption tools, messaging software, and potentially fraudulent documents.



9. Carved files

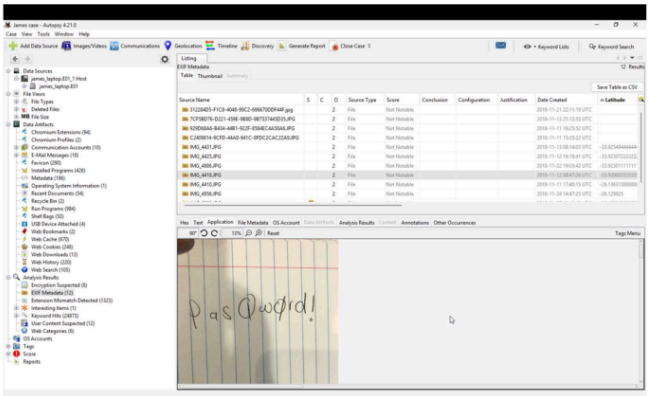
File carving module recovered significant number of deleted images from the laptop. Among the carved files there were multiple fake passport samples, including documents from Ukraine, Russia, and the United Kingdom. Additionally, a file named passport-sample.jpg, previously deleted, was identified in the Recycle Bin. The presence of these files indicates deliberate attempts to and conceal forged identification documents.





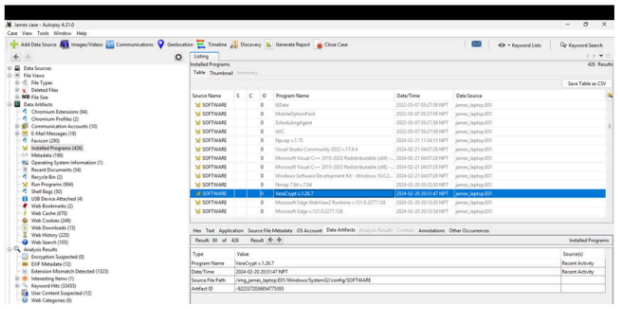
10. Password

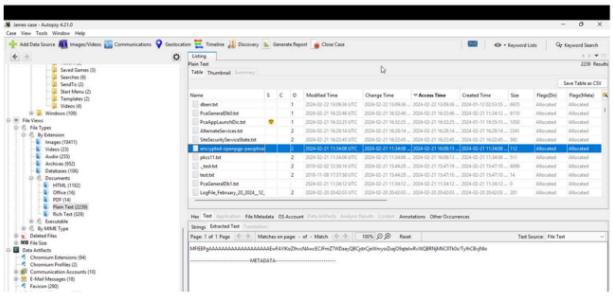
During the forensic process, one image was recovered showing a handwritten password “PasQword!”. EXIF metadata analysis revealed that the image was captured using an Apple iPhone device and was geotagged with coordinates pointing outside the United Kingdom. This image hints ,it could be password of some encrypted files, possibly through VeraCrypt, which was identified as downloaded and installed on the system. This finding directly connects user activity, encryption efforts, and geographical movements, supporting evidence of concealment and international travel.



11. Use of encryption tool

In investigation of system registry analysis it was confirmed of installation of VeraCrypt v1.26.7 on laptop. Additionally, a file named “encrypted-openpgppassphrase.txt” was recovered, containing non-readable high-entropy text consistent with encrypted data or key files. Presence of encryption software and encrypted files indicates attempting to protect s information, supporting the suspicion of concealment related to unauthorized activities.





## Forensic Examiner's Conclusion

Based on the analysis of James' laptop, multiple artifacts were recovered indicating activities consistent with unauthorized international travel and document forgery. Web browsing history and downloads revealed searches and downloads of fake passport samples and encryption tools. EXIF metadata extracted from images confirmed that the device was used in locations outside the United Kingdom, including Botswana and South Africa. User activity showed recent use of fake documents, and USB device analysis indicated the presence of external storage devices connected during the period.

Additionally, the installation of encryption software and presence of encrypted files, and a recovered handwritten password suggest data was encrpted on device. Carved files included numerous images of fake passports from different countries.

In conclusion, the artifacts recovered during the forensic examination are consistent with activities involving the creation of travel-related documents, international travel, and the use of encryption technologies to protect certain data. No final conclusions regarding the intent or legality of the activities are made in this report.

## Appendices

(Submitted in zip file)

1. James case html report
2. Case Notes

# Report

ORIGINALITY REPORT

| 6% | 2% | 0% | 5% |
| --- | --- | --- | --- |
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
| --- | --- | --- |
| 1 | Submitted to The British College<br>Student Paper | 4% |
| 2 | Submitted to University of Greenwich<br>Student Paper | 1% |
| 3 | www.investorcontacts.co.za<br>Internet Source | 1% |

| | | | |
| --- | --- | --- | --- |
| Exclude quotes | Off | Exclude matches | Off |
| Exclude bibliography | On | | |