**Forensic Analysis Report**

**Date:** March 23, 2025  
**Case Reference:** Investigation into Suspected Customs Violations

**Executive Summary**

This forensic analysis report, finalized on March 23, 2025, presents findings from an investigation into potential customs violations, specifically drug trafficking or smuggling, linked to a Windows 10 Pro laptop (hostname: **JELAPTOP**) used by an individual identified as JaneE. The examination is based on a forensic disk image, labeled Image3.E01, which encapsulates the file system and activity logs of the suspect’s device. Conducted using industry-standard digital forensic tools, this analysis reveals a pattern of suspicious behavior spanning January 29, 2019, to February 2, 2019.  
Key findings include evidence of JaneE downloading and subsequently deleting a Remote Access Trojan (Quasar RAT), conducting extensive research into drug smuggling techniques and law enforcement evasion strategies, utilizing encrypted communication platforms such as ProtonMail, and transferring data to multiple high-capacity external storage devices. These actions collectively suggest a deliberate intent to conceal illicit activities, potentially related to smuggling or trafficking operations across international borders. The evidence uncovered justifies further investigative steps to ascertain the full scope of JaneE’s actions and to identify any accomplices or additional evidence that may reside on connected devices or online accounts. This report details the analytical process, key discoveries, and actionable recommendations for law enforcement.

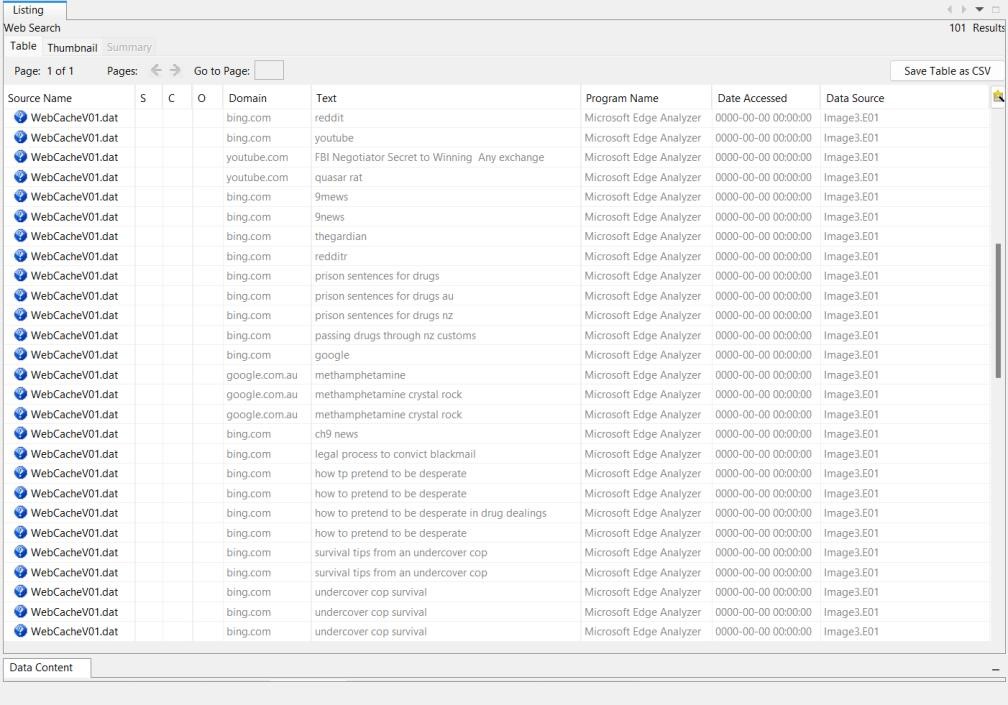
**Scope of Analysis**

The investigation centers on data extracted from Image3.E01, a forensic image of JELAPTOP’s file system, which was secured and analyzed in compliance with digital forensic best practices. The scope of this analysis encompasses several critical areas of the system:

* **User Accounts and System Configuration:** Examination of account activity and operating system settings to establish user identity and system usage patterns.
* **Deleted Files and Web Activity:** Recovery and analysis of deleted files, alongside a review of web browsing hGMTory and cached content, to reconstruct JaneE’s actions.
* **Windows Defender Scan Results:** Assessment of antivirus logs to identify malware interactions and timelines of evidence removal.
* **USB Device Connections:** Investigation of external device usage to trace potential data exfiltration or storage of incriminating materials.  
  Timestamps within the forensic image were primarily recorded in British Summer Time (GMT, UTC+1) during daylight saving periods and Greenwich Mean Time (GMT, UTC+0) otherwise, reflecting the system’s configured time zone. For consGMTency and alignment with international forensic reporting standards, all times have been converted to Coordinated Universal Time (UTC) where noted. The analysis leverages tools and methodologies akin to those used in contemporary digital forensic investigations, ensuring reliability and integrity of the findings.
* **Key Findings**

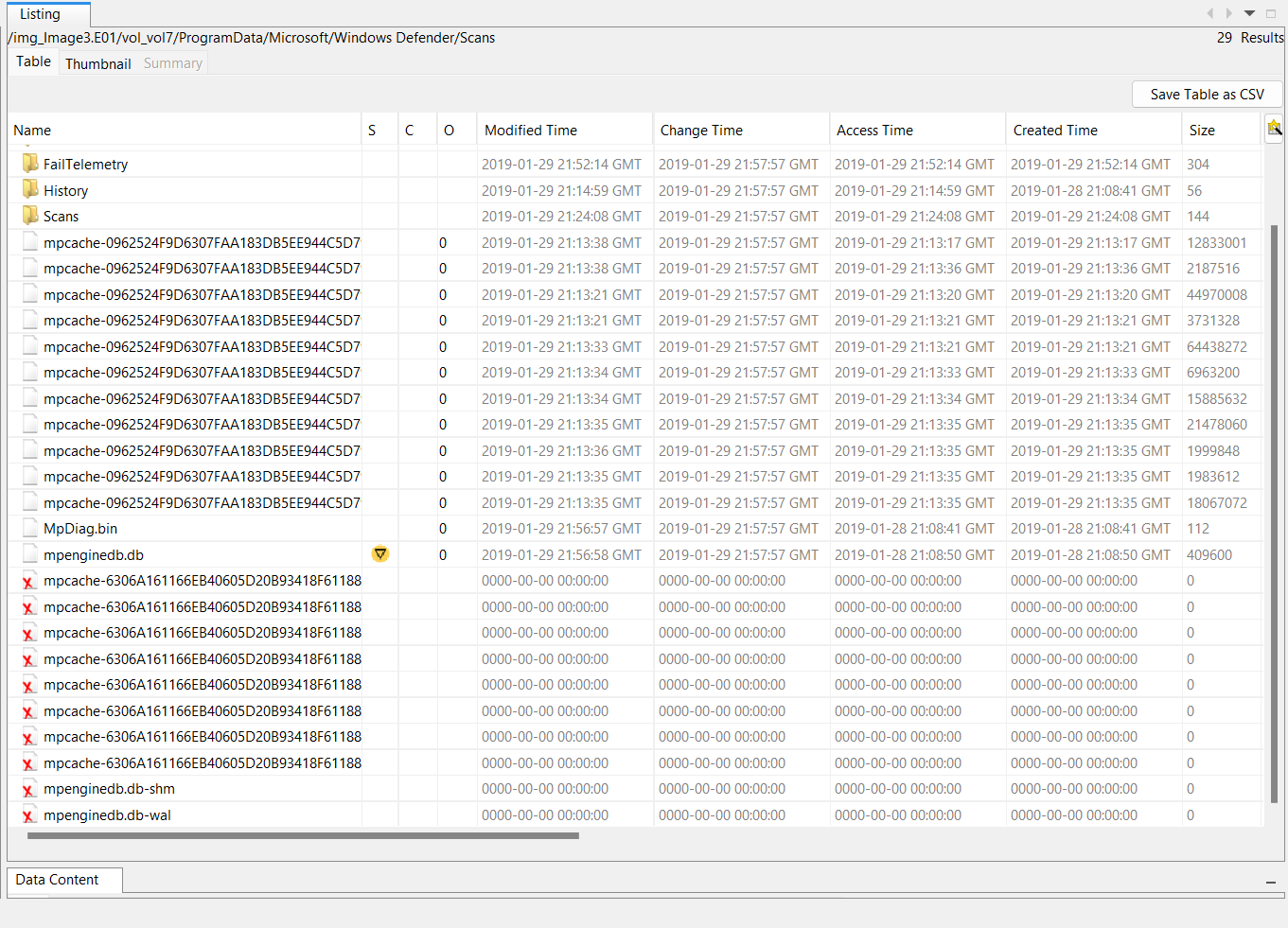
1. **Web Cache (Visited Domains)**  
   Analysis of the web cache revealed a diverse set of online platforms accessed by JaneE, indicating both the breadth of her activities and a potential intent to obscure her digital footprint:

* Search Engines: Bing, Google, Yahoo, and Yandex were frequently visited. The use of Yandex, a Russian-based search engine, stands out as unusual and may suggest an attempt to leverage platforms less commonly monitored by Western law enforcement agencies.
* **Email and Communication Services:** Access to ProtonMail (an encrypted email service, [becomingjane@protonmail.com](mailto:becomingjane@protonmail.com)), Live.com (Microsoft’s email platform), and Facebook was noted. ProtonMail’s end-to-end encryption capabilities are particularly significant, as this service is often favored by individuals seeking to shield communications from surveillance.  
  The reliance on ProtonMail points to a deliberate effort to maintain privacy and evade detection, a tactic commonly associated with illicit operations where sensitive information must be exchanged securely. The use of multiple search engines further suggests a cautious approach to information gathering, potentially to avoid centralized tracking by any single provider.



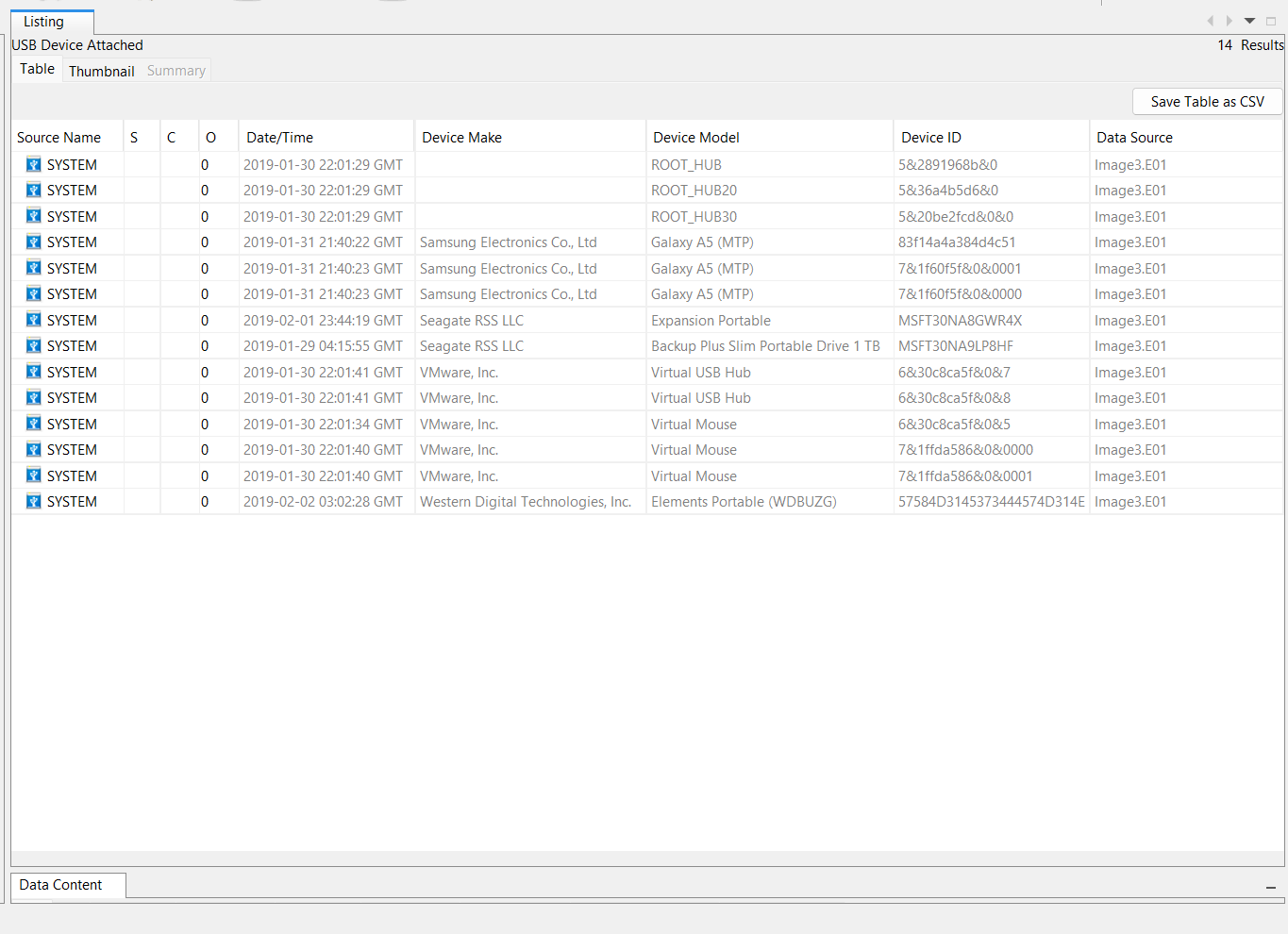
1. **Windows Defender Scans**  
   Windows Defender logs provided critical insight into JaneE’s interaction with malicious software:
2. On January 30, 2019, at 03:27:57 GMT (UTC: January 30, 2019, 02:27:57), a scan database file (mpenginedb.db) was created, indicating the initiation of an antivirus scan.
3. Just 2 minutes and 39 seconds later, at 03:30:36 GMT (UTC: January 30, 2019, 02:30:36), the Quasar RAT—a known Remote Access Trojan—was deleted from the system, specifically from C:\Users\JaneE\Downloads\Quasar v1.3.0.0 as $RN90FSX.0.

This rapid sequence of events strongly implies that JaneE became aware of the malware’s detection and acted swiftly to remove it, likely in an attempt to eliminate evidence of her activities. Quasar RAT, an open-source tool available on platforms like GitHub, allows remote control of a system, making it a potent tool for data theft or coordination of illegal activities. Its deletion post-scan suggests a reactive effort to cover her tracks rather than a routine cleanup, reinforcing suspicions of illicit intent.



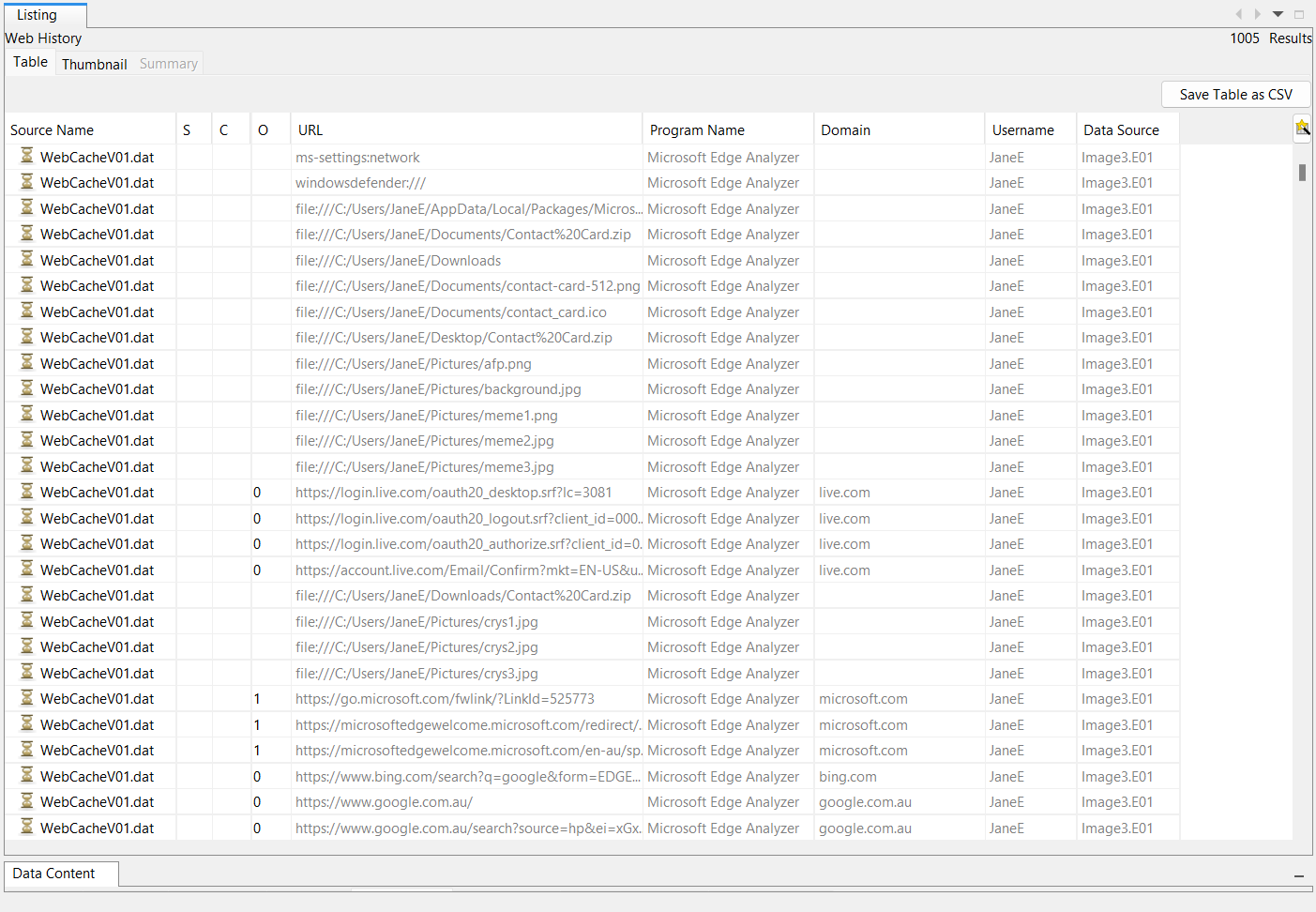
1. **USB Device Connections**  
   The forensic image documented multiple connections of external devices to JELAPTOP, with timestamps spanning the investigative period:

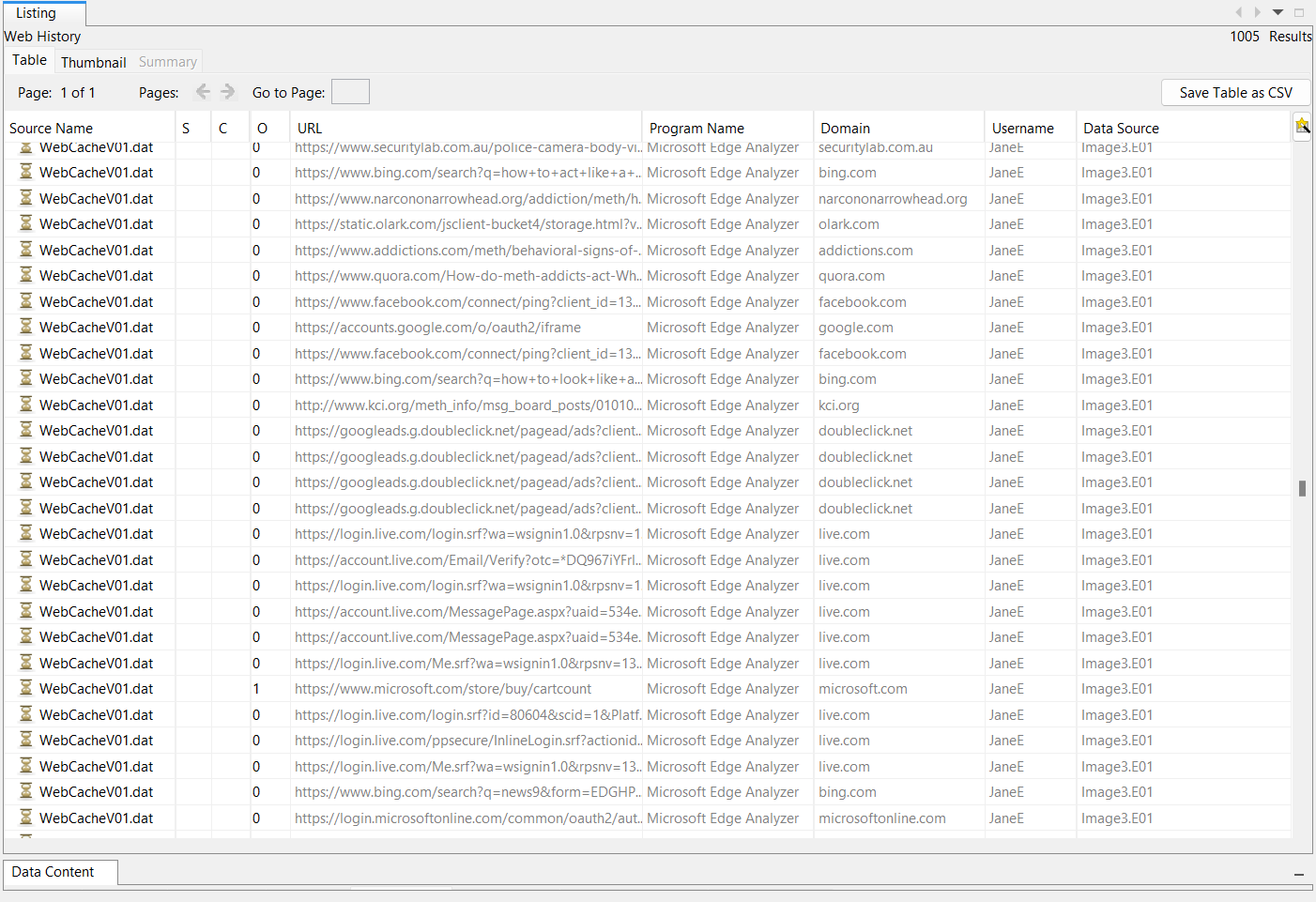
* **2019-01-29 04:15:55 UTC:** Seagate Backup Plus Slim (1TB)—High-capacity drive, suitable for large data transfers.
* **2019-01-30 22:01:34 UTC:** VMware Virtual Mouse—Indicates use of a virtualized environment.
* **2019-01-31 21:40:22 UTC:** Samsung Galaxy A5—Mobile device, potential for data transfer.
* **2019-02-01 23:44:19 UTC:** Seagate Expansion Portable—Additional high-capacity storage option.
* **2019-02-02 03:02:28 UTC:** Western Digital Elements—Further external storage capacity.The frequent attachment of high-capacity storage devices raises concerns about data exfiltration, a common practice in smuggling operations where digital records or instructions need to be moved securely. The Samsung Galaxy A5 suggests possible mobile synchronization, while the VMware Virtual Mouse indicates virtualization, potentially for testing malware or obfuscating activities.

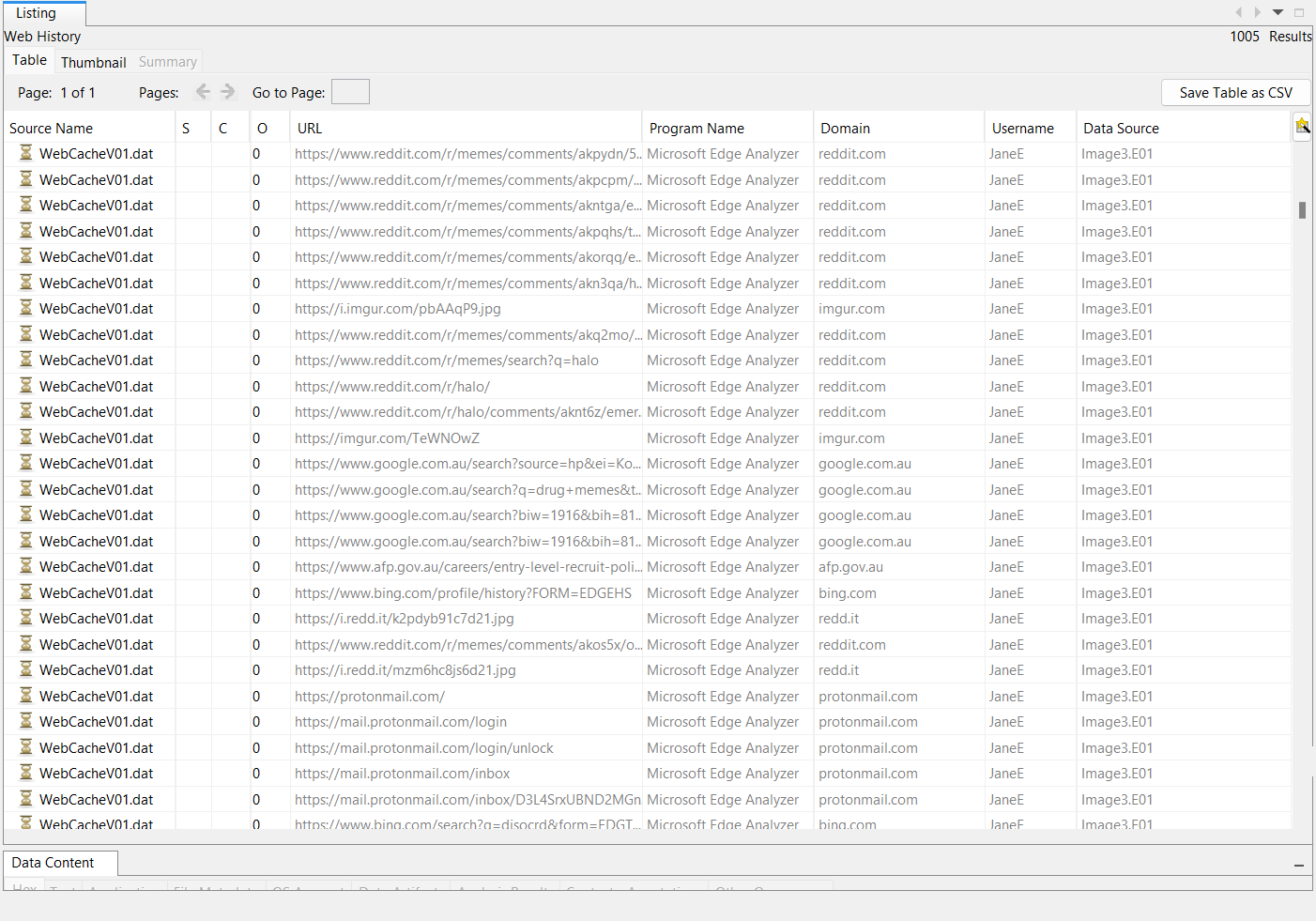


1. **Web Cache (Search Queries & URLs Visited)**  
   The web cache provided a detailed window into JaneE’s research and planning activities, categorized into four key areas:

* **Drug-Related Searches:** Queries included "methamphetamine," "passing drugs through NZ customs," and "how to act like a meth addict," suggesting intent to acquire smuggling logGMTics knowledge and deception tactics.
* **Malware & Cybersecurity:** Research on Quasar RAT via YouTube tutorials and GitHub, alongside a PNG-to-ICO converter, hints at disguising malicious files for stealth.
* **Law Enforcement Evasion:** Searches like "federal agent badge au" and "undercover survival tactics," plus visits to the Australian Federal Police (AFP) website, indicate preparation against law enforcement.
* **Covert Communications:** ProtonMail inbox access, Discord logins, and queries about spy recording devices underscore secure communication efforts.  
  The convergence of these categories paints a picture of a calculated individual preparing for an illicit operation requiring operational security.

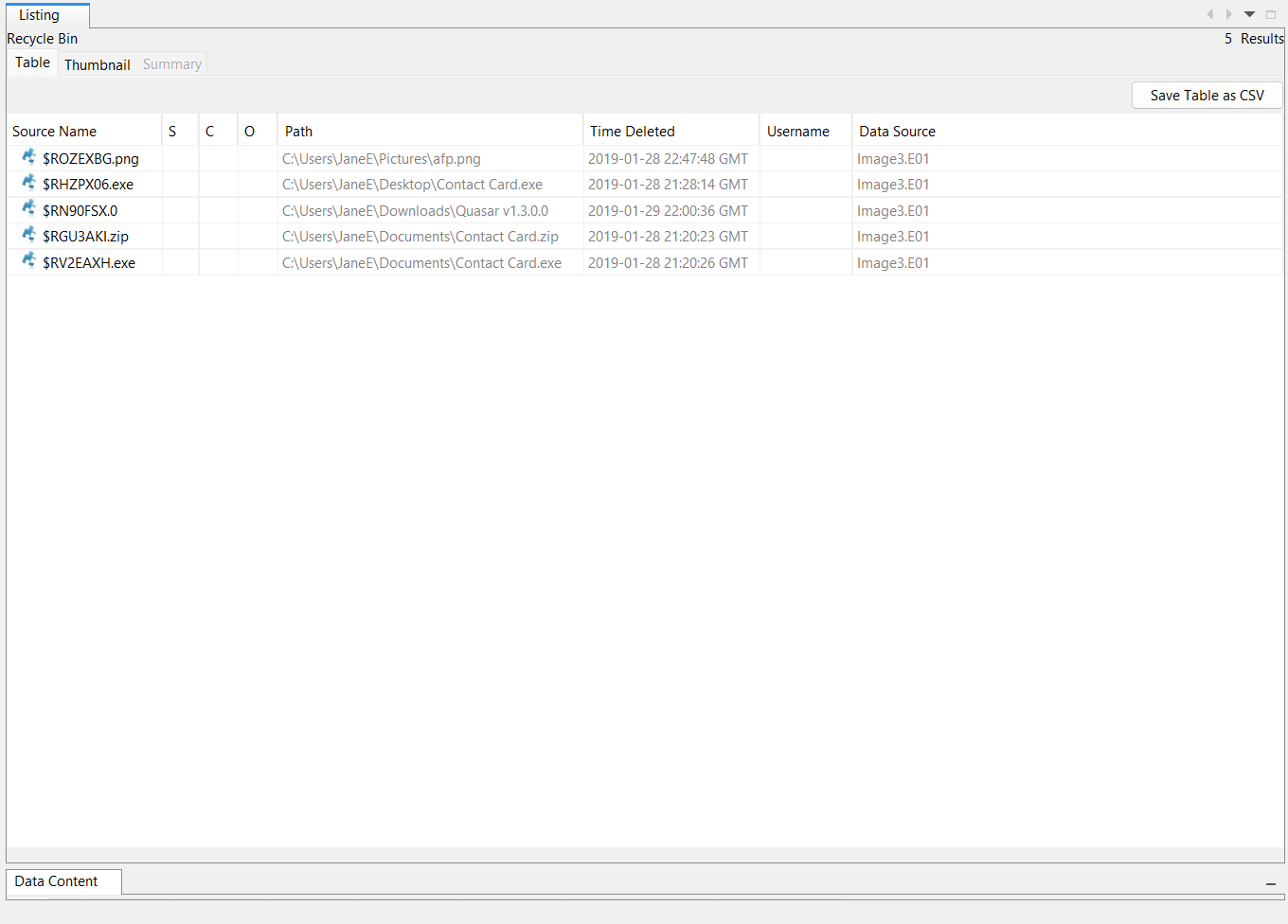






1. **Recycle Bin**   
   Analysis of the recycle bin within Image3.E01 uncovered deleted files that enhance the evidence of JaneE’s activities:

* **$ROZEXBG.png** (C:\Users\JaneE\Pictures\afp.png, deleted 2019-01-29 04:17:48 GMT): Likely tied to AFP website visits, possibly a screenshot from law enforcement research.
* **$RHZPX06.exe** (C:\Users\JaneE\Desktop\Contact Card.exe, deleted 02:58:14 GMT) and $RV2EAXH.exe (C:\Users\JaneE\Documents\Contact Card.exe, deleted 02:50:26 GMT): Executables with potential malicious intent, possibly disguised using the PNG-to-ICO converter.
* **$RGU3AKI.zip** (C:\Users\JaneE\Documents\Contact Card.zip, deleted 02:50:23 GMT): An archive related to the Contact Card files, suggesting a payload or toolset.
* **$RN90FSX.0** (C:\Users\JaneE\Downloads\Quasar v1.3.0.0, deleted 03:30:36 GMT): Matches the Windows Defender scan timeline, confirming Quasar RAT’s role.  
  These deletions, concentrated on January 29–30, 2019, suggest a cleanup effort, with Contact Card files removed rapidly (within 8 minutes) and Quasar deleted post-scan, aligning with smuggling and evasion activities.



**Conclusions**

As of March 23, 2025, this forensic analysis of Image3.E01 reveals compelling evidence that JaneE engaged in activities consGMTent with drug trafficking or smuggling, coupled with deliberate efforts to evade law enforcement detection. The downloading and subsequent deletion of Quasar RAT, extensive use of external storage devices, reliance on encrypted communication platforms, and targeted web searches collectively indicate a sophGMTicated operation with international implications. The recycle bin analysis further strengthens this, showing specific deletions: **$ROZEXBG.png** (C:\Users\JaneE\Pictures\afp.png, deleted 2019-01-29 04:17:48 GMT), **$RHZPX06.exe** and **$RV2EAXH.exe** (both "Contact Card.exe," deleted 02:58:14 GMT and 02:50:26 GMT), **$RGU3AKI.zip** ("Contact Card.zip," deleted 02:50:23 GMT), and **$RN90FSX.0** ("Quasar v1.3.0.0," deleted 2019-01-30 03:30:36 GMT). These files suggest a mix of research (e.g., "afp.png" tied to Australian Federal Police searches) and potential malware tools (Contact Card, Quasar), aligning with smuggling preparations.

The timeline of activities—concentrated between January 29 and February 2, 2019—suggests a period of active planning or execution, with the recycle bin deletions marking an early cleanup phase, likely triggered by the Windows Defender scan detecting Quasar RAT at 03:27:57 GMT on January 30, just minutes before its removal. Web searches like "methamphetamine," "passing drugs through NZ customs," and "undercover survival tactics" corroborate the intent behind these files, pointing to a calculated effort to navigate customs and law enforcement challenges. The full extent of her actions remains unclear pending further investigation, but the evidence paints a picture of intent and capability.

The use of ProtonMail ([becomingjane@protonmail.com](mailto:becomingjane@protonmail.com)) and high-capacity USB drives—like the Seagate Backup Plus Slim (connected 2019-01-29 04:15:55 UTC)—mirrors tactics seen in other smuggling cases, where secure communication and portable data storage are critical to operational success. Similarly, the virtualization evidenced by VMware usage (VMware Virtual Mouse, 2019-01-30 22:01:34 UTC) and the rapid response to Quasar’s detection reflect a level of technical proficiency that could complicate traditional investigative approaches. The Contact Card files’ presence in Desktop and Documents, alongside their swift deletion, suggests they were actively used—possibly as disguised payloads or smuggling tools—before being discarded to avoid scrutiny. These findings necessitate a multi-faceted response to fully address the potential scope of JaneE’s activities, now bolstered by concrete recycle bin evidence.

**Recommendations**

Based on the evidence, the following actions are recommended to advance the investigation:

1. **Examine Connected Devices:** Conduct forensic examinations of the Samsung Galaxy A5 (connected 2019-01-31 21:40:22 UTC), Seagate Backup Plus Slim (1TB, 2019-01-29 04:15:55 UTC), Seagate Expansion Portable (2019-02-01 23:44:19 UTC), and Western Digital Elements (2019-02-02 03:02:28 UTC) drives to recover any data related to smuggling plans, contacts, or illicit materials. These devices, used post-deletion of recycle bin files, may hold backups or additional evidence tied to JaneE’s operations.
2. **Subpoena ProtonMail Records:** Request communication logs for the account [becomingjane@protonmail.com](mailto:becomingjane@protonmail.com) to uncover encrypted exchanges that may detail accomplices, timelines, or operational specifics. This is critical, as ProtonMail’s use aligns with the secrecy needed for smuggling, potentially linking to the Contact Card or Quasar activities.
3. **Analyze Deleted Files:** Employ advanced file recovery techniques to reconstruct deleted Contact Card files ($RHZPX06.exe, $RV2EAXH.exe, $RGU3AKI.zip) and $ROZEXBG.png, assessing whether they contained malicious payloads, smuggling instructions, or additional evidence of JaneE’s intentions. The Quasar RAT ($RN90FSX.0) should also be recovered to confirm its configuration and use.
4. **Investigate VMware Environment:** Perform a detailed analysis of the virtualized environment indicated by the VMware Virtual Mouse (2019-01-30 22:01:34 UTC) to determine if it was used for malware testing (e.g., Quasar RAT), data obfuscation, or other covert activities. This could reveal hidden layers of JaneE’s planning not captured in the recycle bin.

**Final Remarks**

This report, updated as of March 23, 2025, establishes a strong foundation for further inquiry into JaneE’s suspected customs violations, now enhanced by detailed recycle bin analysis as of March 24, 2025. The integration of digital forensic techniques—such as web cache analysis, USB device tracking, malware detection, and recycle bin recovery—has illuminated a pattern of behavior that demands immediate attention from law enforcement. The deleted files, including "afp.png," Contact Card executables, and Quasar RAT, provide tangible evidence of JaneE’s intent, tying directly to her drug-related searches, encrypted communications, and data transfers. By pursuing the recommended actions—examining USB drives, subpoenaing ProtonMail, recovering files, and probing the VMware setup—investigators can build a comprehensive case, potentially disrupting an active smuggling operation and ensuring accountability for any violations committed. The combination of forensic layers underscores JaneE’s technical savvy and the urgency of this investigation.