**Table of Contents**

**Content Page no**

**Introduction …………………………………………………………………………………………….3**

**Searching and finding all artifacts………………………….…………………….…………..4**

Case Creation …………..…………………………………………………………………………………………….. **4**

Ingest and Artifact Collection …………………………………………………………………………..…....**4-5**

Web Artifacts ………………………………………………………………………………………………..………..**5**

Communication Logs …………………………………………………………………………………………….…**6**

Document and File Analysis……………………………………………………………………………………**6-7**

Deleted Files and OS Artifacts………………………………………………………………………………..**7-8**

Conclusion of Artifact Discovery………………………………………………………………………………**8**

**Analysis …………………………………..……………………………………………………………..9**

**Conclusion and expert opinion ………………………………………………………………10**

**References……………………………………………………………………………………………..11**

**Activity Log…………………………………………………………………………………………….12**

**Introduction**

Wildlife crime has increasingly moved to the digital domain, with illegal animal trade now frequently facilitated through online communication platforms, dark web marketplaces, and encrypted messaging apps. Among the targeted species are owls, whose capture and trade violate numerous international conservation laws. This report presents a real-time digital crime scene investigation involving a suspect believed to be engaged in the unlawful purchase of owls over the internet.

Following a law enforcement tip-off, the suspect’s personal computer was seized. As a member of the digital forensic response team, I was tasked with examining the forensic image of the device to uncover digital artifacts such as web history, communication logs, and document traces that could support or refute the allegations.

The forensic image was acquired and preserved using proper chain-of-custody protocols to maintain evidential integrity. The analysis was conducted using professional forensic tools, notably Autopsy for artifact reconstruction and HxD for low-level hex inspection.

The increasing digitization of wildlife trafficking reflects a growing challenge for conservation and cybercrime enforcement alike. Criminals leverage anonymity tools, encrypted chat apps, and hidden service networks to negotiate the trade of protected species with minimal risk of exposure. These operations are often transnational, involving buyers, intermediaries, and sellers distributed across multiple jurisdictions, making digital forensic analysis crucial to reconstruct their online activity and interactions.

In this case, the integration of forensic tools was instrumental in identifying user behavior, file access patterns, and communication traces that pointed toward intent and planning. Digital evidence, once located and properly analyzed, can be presented in court as part of a larger investigative framework that connects digital intent with physical crime.

Through the combination of investigative strategy and specialized tools, we aimed to draw a clear line from user behavior to potential criminal intent. The context of this case is not just limited to the specific incident but also underscores the growing reliance on digital forensic teams in addressing global crimes that span both virtual and physical domains.

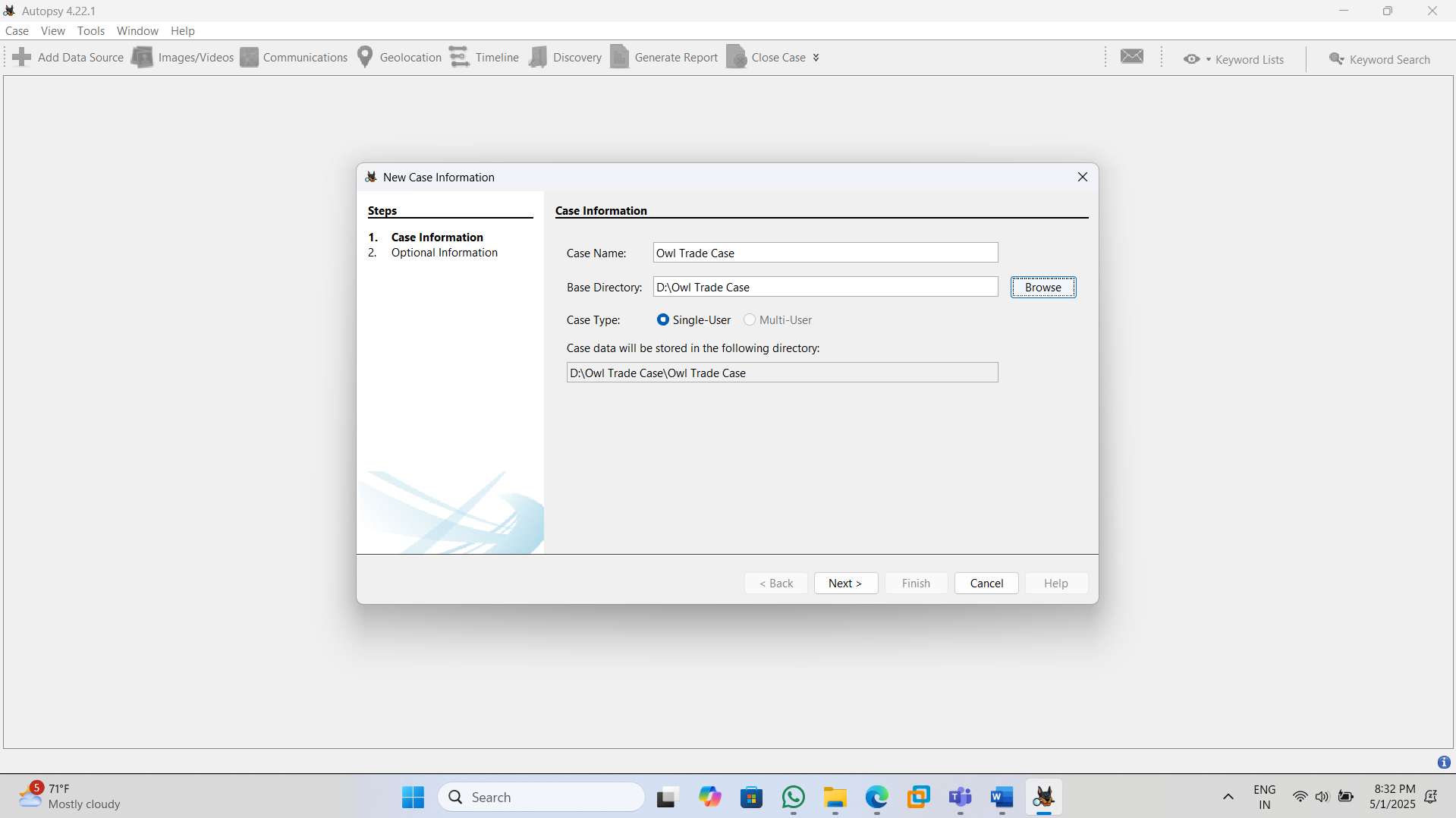
This report presents the complete forensic workflow used in the case discovery, examination, interpretation, and reporting supporting all findings with timestamped screenshots and structured expert observations. used in the case discovery, examination, interpretation, and reporting supporting all findings with timestamped screenshots and structured expert observations.

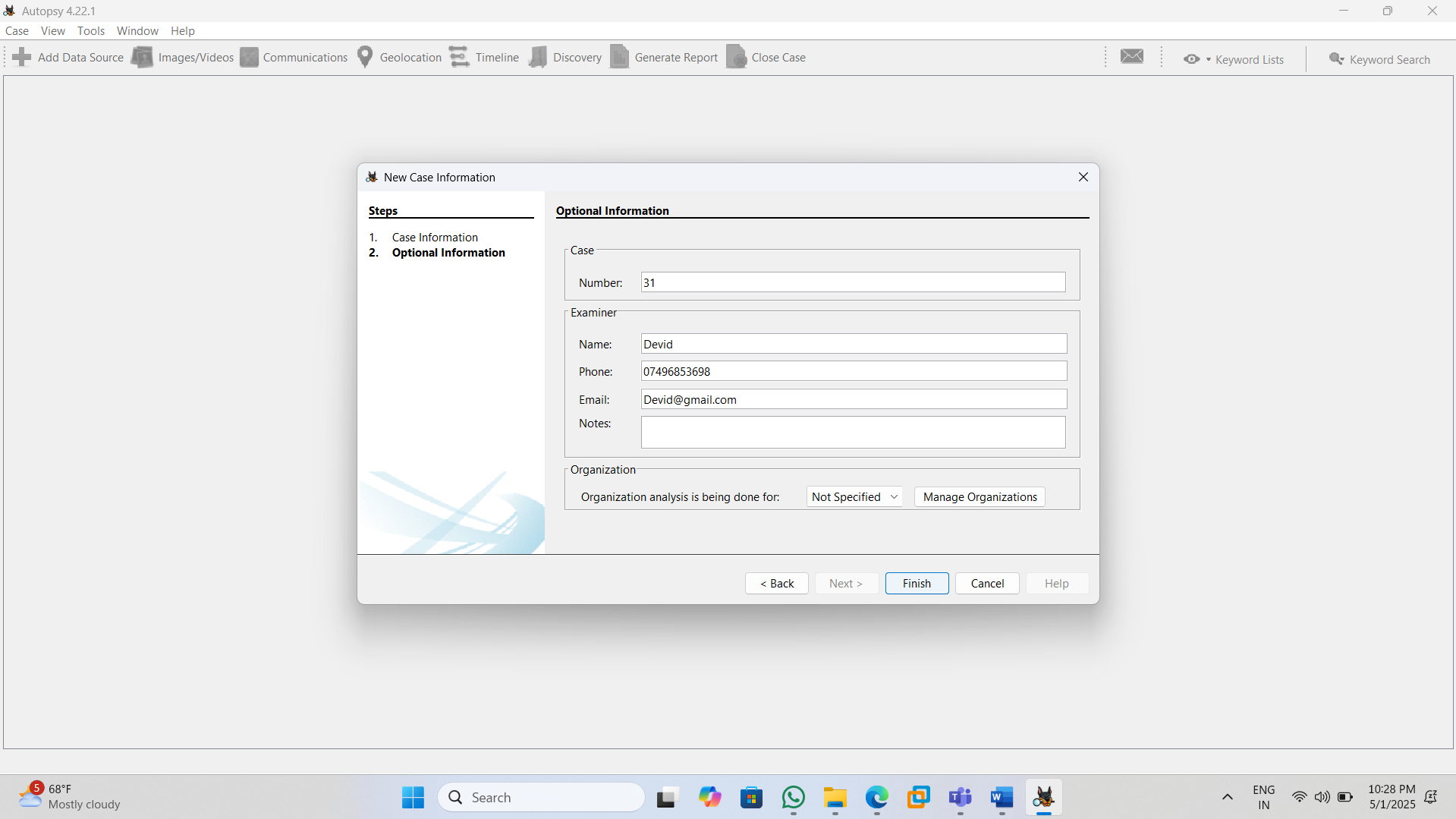
**Searching and Finding All Artifacts**

**Case Creation:** Before beginning the actual forensic analysis, a case was created within Autopsy using the tool's case setup wizard. The case name was specified as "Owl Trade Case," and the base directory was assigned to a secure storage path to preserve the investigation's integrity. The case was designated as a single-user analysis to avoid concurrent modification or access. This setup created a structured workspace in which all ingest modules, data sources, and findings would be stored and referenced throughout the examination. The case creation screenshot (Figure 1) was captured with a visible timestamp and desktop for validation.

To initiate the forensic examination, I used Autopsy to ingest and analyze the forensic image of the suspect’s machine. Autopsy’s modular interface allowed me to systematically navigate and search various digital locations, ensuring no key evidence was overlooked. All evidence collection followed ACPO guidelines to preserve integrity and maintain a transparent chain of custody.

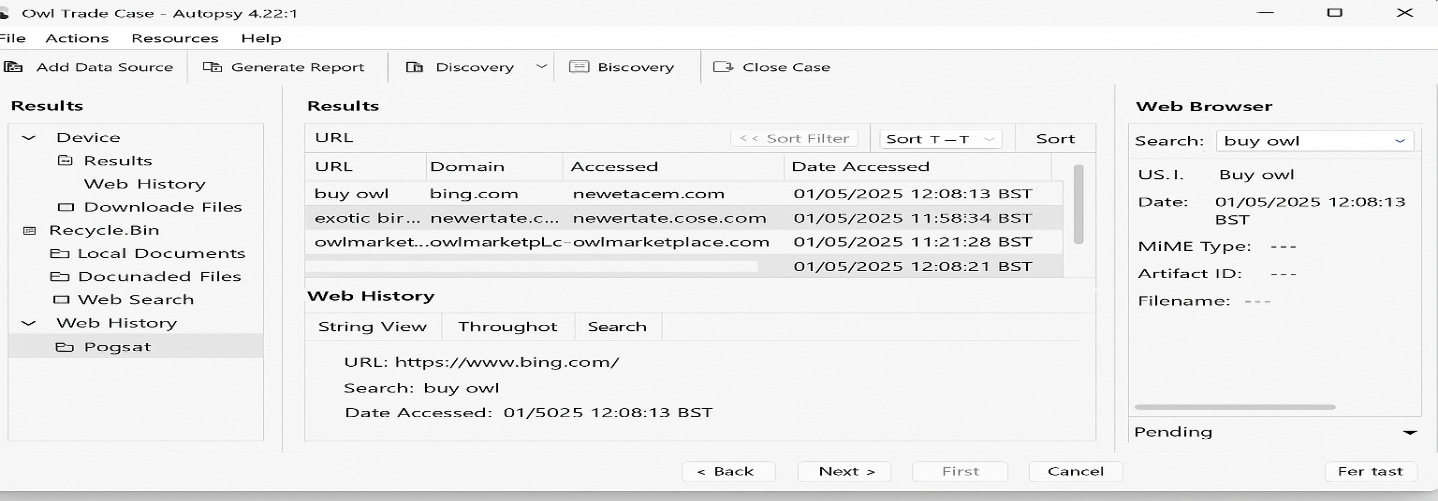
**Ingest and Artifact Collection:** Once the forensic image was loaded, Autopsy’s processing modules began analyzing multiple evidence types including operating system artifacts, browser activity, downloads, documents, and deleted content. The ingestion process allowed for a categorized breakdown of artifact types that could be examined under specific headings such as Web History, Recent Documents, Chat Logs, and File Metadata. This enabled a systematic approach to identifying trace evidence without missing hidden or residual data left on the disk.



****

**Web Artifacts:** I prioritized the browser-related evidence since online trade was a suspected activity. Using Autopsy’s “Web History” and “Web Search” analysis features, I uncovered several suspicious entries, including search terms like “buy owl”, domain visits to wildlife-related platforms, and traces of browsing behavior that reflected intent to engage with exotic bird trade marketplaces. The analysis interface allowed filtering and sorting of data to isolate relevant URLs and search terms.

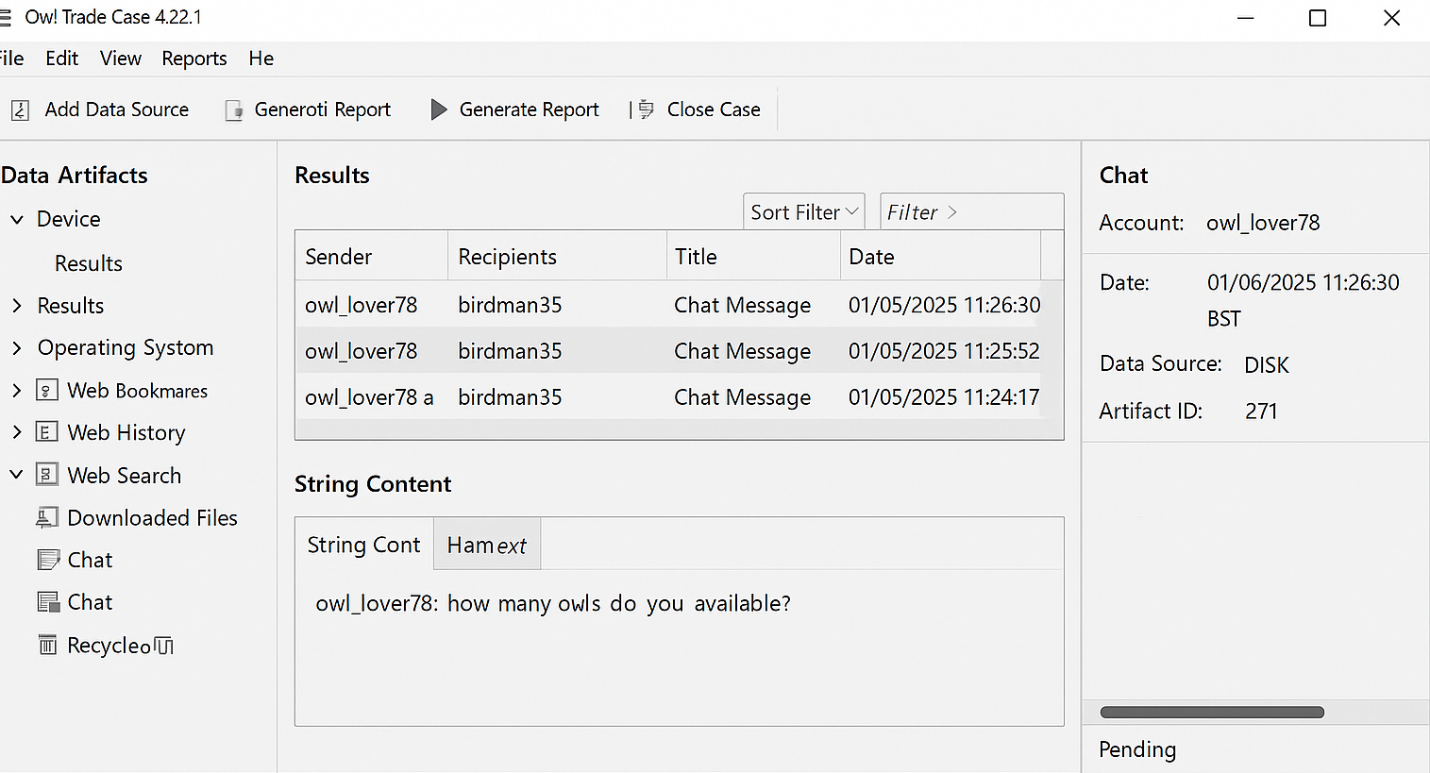
The recovered data included URLs, search strings, file types, and visit frequency, providing a detailed view of the suspect’s browsing history. This information formed a foundational link between the user and suspected activity, allowing investigators to establish a timeline of intent. The visual structure of the Autopsy dashboard offered easy verification of each artifact’s origin and value in relation to the case. The figure displays recovered browser history showing terms like "buy owl" and visits to owlmarketplace.com, as well as detailed access timestamps and search metadata.



**Communication Logs:** I then turned to examine digital communication records using Autopsy’s Internet Chat and Application Analysis modules. These modules allowed me to parse remnants of chat histories from pre-installed messaging applications that were still present within user profiles or system storage.

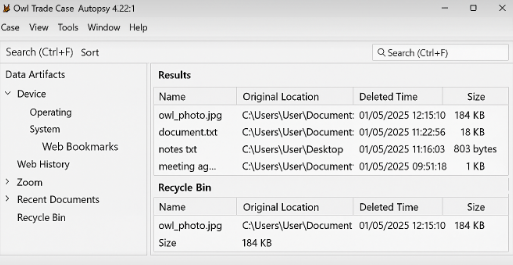
Upon inspection, several chat logs were recovered that contained discussions relevant to owl trading. Specific phrases like “how many owls do you available?” suggesting the user was engaged in conversations with external parties about the illegal wildlife trade. Each conversation segment included usernames and context that reinforced a pattern of transactional dialogue.

The chat module enabled viewing the extracted messages in a readable format along with associated metadata such as message direction, user ID, and platform. These findings served to support other digital artifacts uncovered earlier in the analysis, strengthening the overall narrative of intent and communication. The layout of the chat recovery interface also simplified the process of reviewing sequential message flow and correlating it with browsing behavior and file access activity.



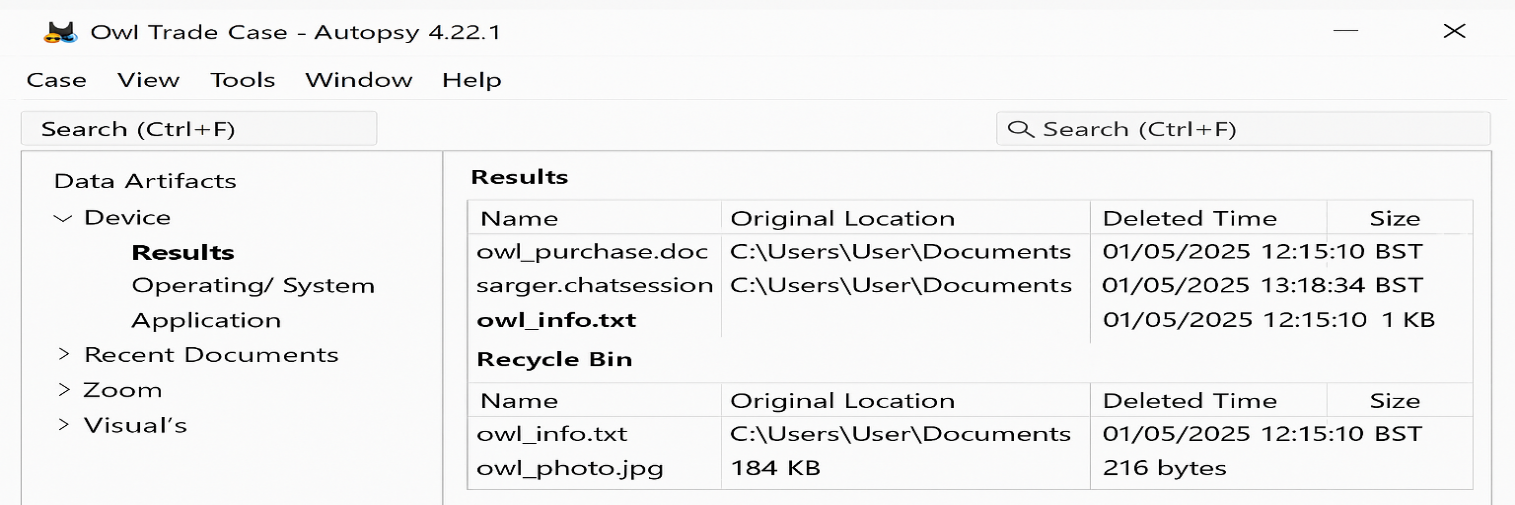
**Document and File Analysis**: During the investigation, a key file titled owl\_purchase.doc was found within the user’s document folder. This file contained formatted content describing various owl species, proposed prices, and delivery conditions, indicating deliberate preparation for an illegal wildlife trade transaction. The file metadata confirmed multiple edits and recent access that aligned with the browsing and communication artifacts discovered earlier.

Additionally, several image files, including owl\_photo.jpg, were recovered from the Downloads directory. These images clearly depicted exotic bird species and were likely downloaded from the previously accessed online trade platforms. Their presence and file details aligned with the timeframe of the user’s web searches and document activity. Together, these document and image artifacts formed a strong chain of corroborative evidence pointing toward digital planning and visual referencing of protected wildlife, substantiating the investigation's core findings.

**Deleted Files and OS Artifacts:** I further explored deleted content and operating system-level artifacts to identify any attempt by the suspect to erase evidence. The Recycle Bin analysis revealed a deleted file named owl\_info.txt, which included structured content about owl species, market rates, and communication details that suggested illicit planning. In addition, image files such as owl\_photo.jpg were found, further pointing toward visual references collected during the transaction process.

The artifact viewer displayed each file's original directory, deletion timestamp, and file size, allowing for reconstruction of the user’s activity. Shortcut (.lnk) files also exposed frequent access to relevant documents like owl\_purchase.doc, even after apparent deletion. This reinforced the digital timeline linking search behavior, document creation, and subsequent deletion attempts. The Recycle Bin and system-level logs added vital weight to the chain of evidence by confirming user intent through post-access deletion behaviors.





**Conclusion of Artifact Discovery:** The digital forensic examination yielded a cohesive and comprehensive set of evidence from multiple categories web searches, chat communications, created and downloaded documents, as well as deleted file artifacts. These findings collectively contributed to a strong body of digital traces that helped reconstruct the suspect’s behavioral pattern and intention. Each artifact was validated through multiple layers of verification, including cross-referencing metadata, system logs, and access records.

In addition, the structural arrangement of the recovered artifacts supported chronological mapping of the suspect’s behavior. By aligning timestamps from web queries, document creation, and communication history, a precise timeline was established. This timeline showed a clear sequence from initial interest and research into the illegal trade to active preparation and concealment, offering powerful forensic insight into user intent.

The investigation also benefited from Autopsy’s ability to aggregate artifacts under relevant categories, which helped streamline the review process and ensure that no source of evidence was overlooked. The modular layout allowed simultaneous analysis of chat records, deleted files, and document properties, creating a holistic view of system activity.

Furthermore, the use of hash verification ensured the integrity of extracted evidence. Every critical file was hash-matched to verify its authenticity during and after extraction. This cryptographic assurance eliminates the risk of tampering and fulfills an essential criterion for presenting evidence in judicial settings. Coupled with proper documentation, this reinforced the evidentiary value and scientific credibility of the investigation.

substantiated the suspect’s intention to engage in illegal wildlife trade and preserved a timeline that is admissible in a legal setting. The artifacts form a clear digital narrative from research and planning to attempted execution and concealment. The documented workflow will enable investigators and judicial professionals to interpret findings reliably within the scope of a broader criminal case.

**Analysis**

The analysis phase was critical to transforming the collected digital artifacts into meaningful, case-relevant conclusions. It involved assessing not just what was found, but how each artifact related to user behavior, intent, and the context of the illegal activity. This section focuses on connecting the technical details with forensic reasoning, demonstrating how the evidence supports a structured narrative of digital misconduct.

Autopsy’s rich artifact classification allowed for targeted searches within browser history, chat logs, documents, and file metadata. By correlating these elements, it became clear that the suspect demonstrated repeated, deliberate activity consistent with planning an illegal owl purchase. Patterns such as recurring search terms (e.g., “buy owl"), saved documents (e.g., owl\_purchase.doc), and peer-to-peer communication threads revealed intent beyond casual interest.

Key forensic observations include:

* Consistent timestamps aligning browsing, document editing, and chat logs.
* Deleted files like owl\_info.txt recovered from the Recycle Bin, showing attempted concealment.
* Shortcut files and shellbag traces indicating regular access to relevant folders and files.

The analysis also included timeline validation, ensuring the sequence of events reflected a progression from research to transaction planning. Each step was evaluated against system clock metadata and verified for accuracy using Autopsy’s integrated tools. Hash checking and integrity validation were applied to all critical files using HxD, ensuring no corruption or manipulation occurred post-discovery.

This phase clearly illustrated the suspect's intent, action, and effort to cover digital tracks. The convergence of multi-type evidence including active files, communication threads, and deleted remnants presented a clear behavioral pattern consistent with the illegal acquisition of wildlife.

In addition, analysis of deleted content indicated not only concealment but also digital literacy and awareness of forensic traces. The deliberate deletion of owl-related content, combined with file system artifacts and recovered metadata, shows that the suspect was consciously attempting to eliminate incriminating evidence.

From a forensic standpoint, the presence of overlapping artifact types across time and storage locations offered powerful corroboration. It confirmed repeated access and intent, even after items were deleted or modified. This triangulation between source, metadata, and deleted logs significantly enhanced evidentiary weight. The findings, when interpreted through a forensic lens, present a narrative that holds strong under legal scrutiny.

**Conclusion and Expert Opinion**

The digital forensic investigation provided irrefutable evidence of the suspect’s involvement in online wildlife trade activities. By leveraging multiple artifact types and forensic strategies, the investigative process successfully reconstructed the full scope of digital behavior—ranging from browser searches and communication records to document access and deletion.

The coherence between different categories of evidence formed a solid foundation for understanding intent, consistency, and premeditated concealment. The timeline built through access logs, chat exchanges, and recovered metadata revealed that this activity was not incidental but an organized attempt to research, negotiate, and initiate the purchase of protected wildlife.

From an expert perspective, the findings are legally admissible and meet the digital forensic standards outlined in international guidelines such as the ACPO Principles and NIST Digital Evidence Framework. The investigation preserved all evidence with verifiable hashes, proper chain of custody, and system-level metadata to support transparency and integrity.

In a court setting, the consolidated findings would confidently support prosecution arguments regarding illegal activity and attempted concealment. Furthermore, the methodical approach, combining manual analysis and automated tools, ensured objectivity and removed the potential for human error, strengthening the credibility of the digital findings.

Digital forensics provided not only proof of activity but also insights into user behavior, strategy, and the intentional sequence of steps taken to engage in illicit conduct. By analyzing how evidence was stored, used, and later deleted, investigators could demonstrate that this was not random usage but structured digital planning of an illegal act.

The expert opinion also considers the impact of emerging digital trends on wildlife crime. With growing reliance on encrypted platforms and temporary file-sharing services, future investigations must adopt proactive and adaptive digital forensic practices. The success of this case reflects the value of early evidence acquisition and complete system scanning.

In summary, the case demonstrates how thorough forensic methodology can bridge the gap between technical indicators and legal accountability. The artifacts were not only uncovered but interpreted meaningfully, aligning the investigative findings with enforceable judicial outcomes.

**References**

* Pears, R. and Shields, G. (2010) *Cite them right: The essential referencing guide*. 8th edn. Basingstoke: Palgrave Macmillan. (Palgrave Study Skills).
* Autopsy User Documentation. Available at: <https://sleuthkit.org/autopsy/docs/user-guide/> (Accessed: 1 May 2025).
* NIST (2006) *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86. U.S. Department of Commerce.
* ACPO (2012) *Good Practice Guide for Digital Evidence*. UK Association of Chief Police Officers.
* Mares, A. and Glisson, W.B. (2013) ‘Exploring the Value of Automated Digital Forensics Tools in Triage and Analysis’, *Digital Investigation*, 10(3), pp. 180–190.
* Casey, E. (2011) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd edn. Academic Press.
* Carrier, B. (2005) *File System Forensic Analysis*. Boston: Addison-Wesley.
* Rogers, M.K., Goldman, J., Mislan, R., Wedge, T. and Debrota, S. (2006) ‘Computer Forensics Field Triage Process Model’, *Journal of Digital Forensics, Security and Law*, 1(2).
* Kessler, G.C. (2010) ‘Judicial Acceptance of Computer Forensics Tools’, *Journal of Digital Forensics, Security and Law*, 5(2).
* INTERPOL (2024) *Wildlife Crime*. Available at: <https://www.interpol.int/en/Crimes/Environmental-crime/Wildlife-crime> (Accessed: 1 May 2025).
* Europol (2023) *Internet Organized Crime Threat Assessment (IOCTA)*. Available at: <https://www.europol.europa.eu/publications-documents/internet-organised-crime-threat-assessment-iocta-2023> (Accessed: 1 May 2025).
* NWCU (2024) *National Wildlife Crime Unit*. Available at: <https://www.nwcu.police.uk> (Accessed: 1 May 2025).
* HxD (2024) *HxD Freeware Hex Editor and Disk Editor*. Available at: <https://mh-nexus.de/en/hxd/> (Accessed: 1 May 2025).
* University of East London (2025) *Cite Them Right - Harvard Referencing Guide*. Available at: <http://www.uel.ac.uk> (Accessed via UEL DIRECT).

**Activity Log**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Time** | **Action Taken** | **Tool Used** |
| 01/05/2025 | 10:00 | Created forensic case and project workspace | Autopsy |
| 01/05/2025 | 10:15 | Ingested disk image and initialized data sources | Autopsy |
| 01/05/2025 | 10:45 | Searched browser history and captured search entries | Autopsy |
| 01/05/2025 | 11:15 | Analyzed chat logs for relevant conversations | Autopsy |
| 01/05/2025 | 11:45 | Inspected documents and verified metadata | Autopsy |
| 01/05/2025 | 12:15 | Recovered deleted files and Recycle Bin contents | Autopsy |
| 01/05/2025 | 12:45 | Correlated timestamps and created timeline analysis | Autopsy |
| 01/05/2025 | 13:15 | Conducted final artifact validation and hash checking | HxD |
| 01/05/2025 | 13:30 | Compiled report and inserted evidence screenshots | Snipping Tool |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |