# Poster: Mapping the Evidence: A Taxonomy for Satellite Digital Forensics

Owen Ramsey
*New Mexico State University*
*owenr@nmsu.edu*

Efrén López-Morales
*New Mexico State University*
*elopezm@nmsu.edu*

***Abstract*—Satellites underpin critical infrastructure, including communications, and navigation, yet their increasing connectivity has expanded their attack surface. While prior satellite cybersecurity research has focused on attack prevention and detection, post-incident investigation remains largely unexplored. In particular, there is no structured framework for digital forensic evidence analysis in satellite systems. In this work, we introduce the first taxonomy of satellite forensic artifacts that systematically structures evidence across space, ground, and communication segments. Our taxonomy captures 50 artifacts, and characterizes each artifact by its forensic properties, e.g., volatility. We demonstrate its feasibility using real-world flight software data, e.g., telemetry.**

## 1. Introduction

As satellites become more connected, e.g., Ground Station as a Service (GSaaS) [1], they face greater cybersecurity risks as shown by the 2022 Viasat cyberattack [2]. In response, satellite security research has been proposed to protect satellites [3], [4], [5]. However, this research focuses on detecting or preventing attacks, and largely ignore what happens after an incident occurs.

To address this problem, we propose a taxonomy of satellite forensic artifacts based on real mission data, system logs, and known attacker behaviors. The taxonomy categorizes which artifacts can provide useful evidence, what kind of forensic information they contain, and how that information connects to known cyberattack techniques using the SPARTA framework [6]. We implement this taxonomy in machine-readable format (YAML) and test it by simulating security incidents on a real flight software.

Our taxonomy includes data that can be collected from different components of a satellite system such as the space, ground and link segments and describe their forensic relevance. Each artifact includes details about its format, volatility, accessibility, and potential forensic utility.

We implement our taxonomy in a machine-readable format (YAML) so that it can be easily integrated into future automated forensic tools and analysis pipelines. Each artifact will follow a consistent schema that defines attributes such as data type, subsystem, example fields, and whether the data requires time synchronization or cryptographic hashing to maintain evidential integrity. The taxonomy also includes mappings to SPARTA Indicators of Behavior (IOBs) [6], which represent known patterns of malicious activity in space systems. By linking each forensic artifact to one or more IOBs, we can show how observable data can reveal traces of specific attack behaviors.

## 2. Methodology

**2.0.1. Literature Review Methodology.** To identify the relevant literature for the construction of the taxonomy of forensic evidence, we conduct a systematic search on multiple academic, industry, and government research platforms. 0ur primary sources include Google Scholar, IEEE Xplore, SpringerLink, supplemented by U.S. government and standards repositories and the Cybersecurity and Infrastructure Security Agency (CISA) technical report archives. Search keywords include "satellite digital forensics," "spacecraft telemetry evidence," "cybersecurity incident investigation in satellite systems," and "space system command authentication." Papers were filtered by relevance, technical rigor, and their applicability to either onboard (space segment) or ground-based (mission operations) forensic evidence sources. This methodology ensured a wide coverage of scientific research, gray literature, and agency guidance directly applicable to satellite cybersecurity forensics.

**2.0.2. Taxonomy Methodology.** We structured our taxonomy by dividing all forensic evidence into three main parts of a satellite system: the space segment, the ground segment, and the link segment. Within each of these segments, we organized the artifacts into subsystems to show what part of the system produces the data and how it relates to satellite operations. Each artifact in the taxonomy includes consistent fields such as volatility, forensic utility, accessibility, data format, and SPARTA Indicators of Behavior (IoBs). By using the same structure for every entry, the taxonomy makes it easy to compare artifacts, understand their forensic value, and map them to potential cyber behaviors or incidents. Overall, this approach creates a clear, organized, and traceable way to understand where evidence lives in a satellite system and how it can be used during a cybersecurity investigation.

Artifact: Attitude and Determination Telemetry

**Origin Domain:** Ground Segment
**Subsystem:** Software
**ID:** AOD_Telemetry_Records
**Volatility:** 3 days to 30 days

**Forensic Utility:**

- Detection of unauthorized orbit maneuvers or attitude changes
- Validation of spacecraft positional data against command timelines
- Identification of falsified or spoofed navigation telemetry
- Correlation of control system outputs with trajectory deviations

**Accessibility:** Stored within mission ground systems and navigation repositories; derived from telemetry downlinks and onboard sensor fusion products

**SPARTA IOBs:** SMSR-4, DISE-1

Figure 1. Example satellite forensic artifact showing structure and mapping to SPARTA IOBs.

## 3. Evaluation and Implementation Plan

Our evaluation focuses on measuring how accurate, complete, and useful our satellite forensic artifact taxonomy is when compared with real-world documentation, academic research, and known cyberattack behaviors.

First, we will evaluate the accuracy of each artifact by verifying that it appears in credible sources such as satellite mission documentation, peer-reviewed research papers, cybersecurity analyses, and operational system logs described in the literature. For each artifact, we will record the source(s) that mention it, its technical purpose within a subsystem, and how it could support a forensic investigation.

Second, we also evaluate consistency and structure through automated and manual checks. The YAML files are validated against the JSON schema to ensure that every artifact follows the same format and naming conventions. A well-structured taxonomy is one that passes all schema validation tests and maintains uniform categorization across the entire dataset.

## 4. Preliminary Results

Our preliminary results show that the proposed taxonomy is already feasible and useful for organizing satellite forensic evidence. First, we developed an initial taxonomy containing 50 detailed forensic artifacts spanning multiple parts of a satellite system. Fig. 1 provides an example artifact.

Second, we implemented a web-based visualization of the artifact taxonomy using YAML as the underlying machine-readable representation. This prototype interface allows artifacts to be browsed and inspected more easily, demonstrating that the taxonomy supports interactive exploration and future tool integration.

Finally, we collected initial example artifacts from a real-world flight software, the SUCHAI [7] flight software, focusing on telecommand-related data. Early examples include fields such as timestamps and event identifiers, which illustrate how operational spacecraft data can serve as forensic evidence during an investigation. These initial results suggest that real satellite software and mission data can be systematically mapped into the proposed taxonomy and used to support forensic analysis.

## 5. Conclusion and Future Work

We presented an initial taxonomy of satellite forensic artifacts and demonstrated its feasibility using real-world flight software data. Our results show that satellite systems expose meaningful forensic evidence that can be systematically organized and linked to adversarial behaviors.

In future work we will develop and publish a final version of our web-based taxonomy and an incident reconstruction pipeline that includes cryptographic such as hash functions to guarantee the forensic artifact's integrity.

## Acknowledgments

This work is partially supported by Startup Funds Grant from New Mexico State University and the UR2PhD program from the Computing Research Association.

## References

[1] Amazon Web Services, "Aws ground station," https://aws.amazon.com/ground-station/, 2026, accessed: 2026-03-20.

[2] "Case study: Viasat attack," https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat, accessed: 2025-05-24.

[3] E. López-Morales, U. Planta, G. Marra, C. González, J. Hopkins, M. Garoosi, E. Obreque, C. Rubio-Medrano, and A. Abbasi, "Honeysat: A network-based satellite honeypot framework," 2025. [Online]. Available: https://arxiv.org/abs/2505.24008

[4] J. Willbold, M. Schloegel, M. Vögele, M. Gerhardt, T. Holz, and A. Abbasi, "Space odyssey: An experimental software security analysis of satellites," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 1–19.

[5] G. Marra, U. Planta, P. Wüstenberg, and A. Abbasi, "On the feasibility of cubesats application sandboxing for space missions," *arXiv preprint arXiv:2404.04127*, 2024.

[6] The Aerospace Corporation, "Sparta — space attack research & tactic analysis," https://sparta.aerospace.org/, accessed: 2025-11-26.

[7] SPEL - Space and Planetary Exploration Laboratory, University of Chile, "Suchai flight software v2," https://gitlab.com/spel-uchile/flight-software/suchai-flight-software-v2, 2025, flight software for SUCHAI nanosatellites. Accessed: 2026-03-20.

# Mapping the Evidence: A Taxonomy for Satellite Digital Forensics

Owen Ramsey and Efrén López-Morales
Department of Computer Science, College of Arts and Sciences

BE BOLD. Shape the Future.
New Mexico State University

## Motivation

- Satellites are essential to our society, supporting critical infrastructure such as communications and navigation
- However, they have become more interconnected opening the door for potential cyber attacks
- In 2022 the Viasat satellite network was attacked affecting thousands of users

**Problem:** **Satellite cybersecurity research focuses on prevention and detection while post-attack forensics has been largely ignored**

## Research Questions:

1. What are the specific satellite digital artifacts required to perform post-attack forensics analysis?
2. How can we obtain satellite these digital artifacts while account for satellites' computational and physical limitations?

## Objectives

- Create a taxonomy of satellite digital forensic artifacts
- Describe each artifact's properties such as volatility, segment and format
- Collect artifacts through a real satellite flight software

## Methodology

1. **Data Collection:** Literature review of scientific literature and gray literature such as industry reports, whitepapers.
2. **Taxonomy Design**: Includes three sections across the satellite system
    1. **Ground:** artifacts from the ground station and
    2. **Space:** artifacts from the hardware on the satellite and the flight software
    3. **Link:** artifacts from the communication between space and ground segments.
3. **Evaluation:** To test the taxonomy in a realistic environment, we use forensic telecommands using a real-world satellite flight software called "SUCHAI" deployed in three satellites shown in Fig. 1.

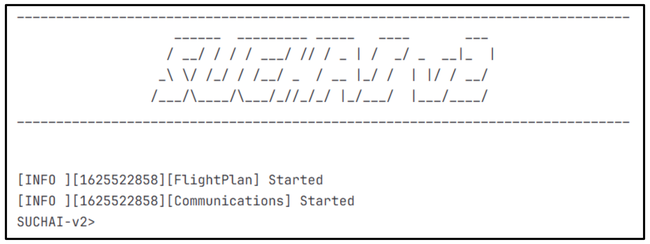


Figure 1: Satellite Ground station Console

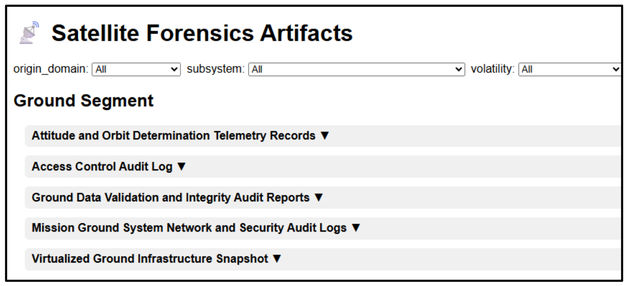


Figure 2: Web-based taxonomy

## Results

- Taxonomy with 50 detailed artifacts
- Web-based visualization of the artifact taxonomy using YAML (Fig. 2)
- Collected initial artifacts using the SUCHAI flight software via telecommand data, e.g., timestamp, and event ID

## Example Artifact: Telemetry Packet

Origin Domain: Space Segment
Subsystem: Telemetry
Volatility: 3 days
Accessibility: Downlink
Format: Binary data

## Conclusions

- A taxonomy with artifacts to perform post-attack forensics analysis
- Open-source flight software can support forensic investigation.
- Serves as a foundation for future satellite forensics methodologies

### Acknowledgements

This work is partially supported by Startup Funds Grant from New Mexico State University and the UR2PhD program from the Computing Research Association.