Acta Scientific COMPUTER SCIENCES

Volume 7 Issue 4 July 2025

Short Communication

Digital Forensics and Incident Response (DFIR) in Satellite and Space Technologies

Talha Riaz*

DFIR, MSSP, REM, Innovator, Keynote Speaker, Principal DFIR Consultant at Cyberani by Aramco Digital, Saudi Arabia

***Corresponding Author:** Talha Riaz, DFIR, MSSP, REM, Innovator, Keynote Speaker, Principal DFIR Consultant at Cyberani by Aramco Digital, Saudi Arabia.

Received: May 27, 2025

Published: June 18, 2025

© All rights are reserved by **Talha Riaz.**

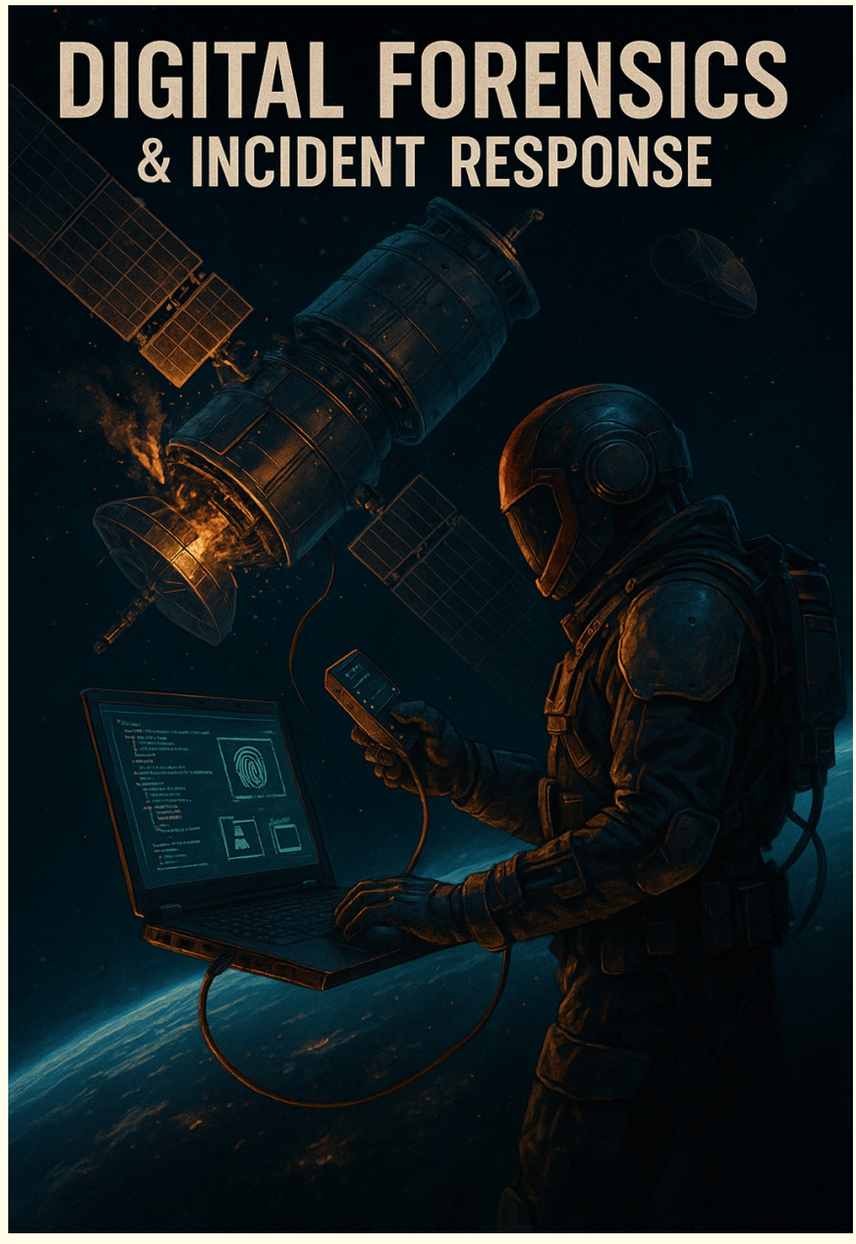

Figure 1

The increasing reliance on satellite and space technologies for critical infrastructure, communication, navigation, scientific research, and national security has brought a new, complex dimension to cybersecurity: Digital Forensics and Incident Response (DFIR). As orbital assets and ground control systems become more interconnected and reliant on standard terrestrial network protocols, their attack surface expands, making them lucrative targets for state-sponsored actors, cybercriminals, and hacktivists. This article delves into the unique challenges of performing DFIR in this domain, explores real-world cybersecurity tools and notable case studies, and examines the future of space DFIR in an era of advanced AI and rapidly evolving space exploration.

The unique challenges of DFIR in space

Performing digital forensics and incident response on satellite and space technologies presents a distinct set of challenges not typically encountered in terrestrial environments:

- **Remote and Inaccessible Environments:** Physical access to compromised assets (satellites in orbit) is often impossible. Investigations rely heavily on telemetry data, command logs, and ground system artifacts.
- **Data Volume and Velocity:** Satellites generate vast amounts of telemetry and payload data. Sifting through this to find forensic evidence requires specialized tools and techniques.
- **Proprietary and Legacy Systems:** Many satellites operate on custom-built, proprietary hardware and software, or older, legacy systems that may lack modern security logging and forensic capabilities.
- **Limited Bandwidth and High Latency:** Communicating with and retrieving data from distant space assets can be slow and constrained, hampering timely incident response.
- **Harsh Operating Environment:** The space environment (radiation, temperature extremes) can cause data corruption or system malfunctions that might mimic cyberattacks, complicating diagnosis.
- **Complex Interdependencies:** Space systems involve intricate networks of satellites, ground stations, user terminals, and data links. An incident in one segment can cascade and impact others.
- **Attribution Difficulties:** The global nature of space operations and the potential for sophisticated state-level actors can make attributing attacks exceptionally challenging.

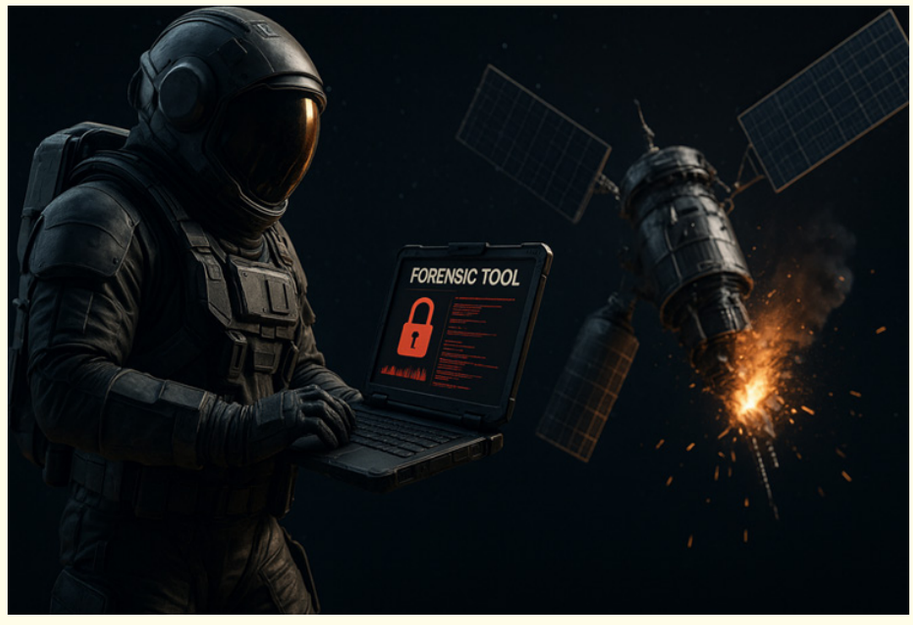

Figure 2

Real-world cybersecurity tools and techniques in Space DFIR

While a dedicated "Space DFIR Toolkit" is still an emerging concept, practitioners adapt and utilize a range of cybersecurity and forensic tools, often focusing on specific segments of the space ecosystem.

Ground segment and network analysis

- **Security Information and Event Management (SIEM) Systems:** (e.g., Splunk, IBM QRadar, Microsoft Sentinel) are crucial for collecting and correlating logs from ground control stations, network devices, and communication links.
- **Network Forensics Tools:** (e.g., Wireshark, tcpdump, NetworkMiner) are used to capture and analyze network traffic between ground control and satellites, and within ground networks, to identify anomalous patterns or malicious communications.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** Deployed at ground stations to monitor for and block known threats.
- **Industrial Control System (ICS)/SCADA Security Tools:** Since ground control systems often share characteristics with ICS/SCADA environments, tools designed for monitoring and securing these systems (e.g., Nozomi Networks, Dragos Platform) are increasingly relevant for identifying vulnerabilities and detecting attacks.

Satellite and payload data analysis

- **Telemetry Analysis Tools:** Custom or specialized tools are often required to parse and analyze satellite bus and payload telemetry. AI and Machine Learning (ML) are increasingly used to establish baseline behaviors and detect anomalies that could indicate a compromise.
- **Memory Forensics Tools:** (e.g., Volatility Framework) While direct memory acquisition from an orbiting satellite is highly complex, analysis of memory dumps from emulated environments or recovered components (if possible) can provide insights.
- **Specialized Data/File Analysis Tools:** For incidents involving data exfiltration or manipulation from satellite payloads (e.g., imagery, scientific data), tools like ExifTool (for metadata analysis), hexadecimal editors (e.g., HxD), and image forensic tools (e.g., Forensically) can be employed on the received data.
- **Satellite Communication Interception and Analysis Tools:** Specialized hardware and software are used to monitor and analyze the radio frequency (RF) spectrum for unauthorized transmissions, jamming, or spoofing of satellite signals. This involves analyzing communication logs and frequency data from ground stations.

General digital forensics platforms

- Standard forensic suites (e.g., EnCase Forensic, AccessData FTK, Autopsy) are used to analyze compromised workstations, servers, and user devices within ground control facilities or organizations involved in space operations.
- **Threat Intelligence Platforms:** Subscribing to and integrating threat intelligence feeds specific to aerospace and critical infrastructure helps in proactively identifying potential threats, indicators of compromise (IOCs), and attacker tactics, techniques, and procedures (TTPs).

Figure 3

Case studies: Cyber incidents in the space domain

Several incidents have highlighted the real-world cybersecurity threats to space technologies:

- **Viasat KA-SAT Attack (February 2022):** Just hours before Russia's invasion of Ukraine, a sophisticated cyberattack targeted Viasat's KA-SAT satellite network. The attack deployed a wiper malware variant named "AcidRain" against tens of thousands of satellite broadband modems, rendering them inoperable. This disrupted internet services for individuals, businesses, and critical infrastructure (including wind farms in Germany) across Ukraine and other parts of Europe. The primary goal appeared to be service disruption. DFIR efforts involved analyzing modem firmware, network traffic, and ground system logs to identify the malware and its propagation mechanisms.
- **NASA Jet Propulsion Laboratory (JPL) Hack (April 2018):** An attacker utilized an unauthorized and unsecured Raspberry Pi computer connected to the JPL network to gain access. They moved laterally within the network and exfiltrated approximately 500 megabytes of data related to Mars missions. The breach also compromised JPL's Deep Space Network (DSN) satellite dish network. The intrusion went undetected for nearly a year, highlighting weaknesses in IT asset inventory, network segmentation, and incident detection. The investigation involved network log analysis and system forensics to trace the attacker's path and identify the compromised device.
- **Interference with US Government Satellites (Landsat-7 and Terra AM-1) (2007-2008):** According to a U.S. congressional commission report, hackers, allegedly operating through a ground station in Svalbard, Norway (which relies on internet connectivity), interfered with two NASA-managed Earth observation satellites: Landsat-7 (for 12+ minutes in Oct 2007 and July 2008) and Terra AM-1 (for 2 minutes in June 2008 and 9 minutes in Oct 2008). For the Terra AM-1, attackers reportedly achieved all steps necessary to command the satellite, though they did not issue any commands. This incident demonstrated the vulnerability of ground station internet connections and the potential for unauthorized satellite command.
- **National Oceanic and Atmospheric Administration (NOAA) Satellite Breach (Reported November 2014):** Hackers, reportedly based in China, breached NOAA's satellite network, which provides critical weather and environmental data. The intrusion forced NOAA to temporarily shut down some of its services and take primary forecasting satellites offline to contain the threat. This attack underscored the vulnerability of critical government satellite infrastructure providing essential public services. Forensic investigations focused on identifying the intrusion vector and the extent of data access.
- **ROSAT X-Ray Satellite Hack (1998):** In one of the earliest documented satellite cyberattacks, hackers reportedly gained access to the German ROSAT X-ray satellite's control systems at the Goddard Space Flight Center. They allegedly commanded the satellite to turn its sensitive solar panels and optical sensors directly towards the sun. This action is believed to have severely damaged or destroyed the satellite's sensors and batteries, rendering the multi-million dollar scientific instrument largely unusable. This case highlighted the potential for destructive attacks on space assets.

The future of DFIR in space technologies: The AI revolution and beyond

The future of DFIR in space will be inextricably linked with advancements in Artificial Intelligence (AI) and the increasing complexity of space missions, including mega-constellations and commercial space exploration.

- **AI-Powered Anomaly Detection and Threat Hunting:** AI and ML algorithms will be indispensable for sifting through the enormous volumes of telemetry, sensor data, and network logs generated by space assets. These systems can learn baseline behaviors of satellites and ground systems, automatically flagging anomalies that could indicate a cyberattack, malfunction, or precursor to an incident. AI will also power automated threat hunting, proactively searching for subtle signs of compromise that human analysts might miss.
- **Autonomous Incident Response:** Given communication delays and potential "blind zones" where direct human intervention is not immediately possible, on-orbit AI/ML solutions will be crucial for autonomous detection and initial mitigation of threats. Satellites may need to self-heal or enter safe modes based on AI-driven threat assessments.
- **Predictive Forensics:** AI could enable predictive forensics by analyzing trends, vulnerabilities, and threat intelligence to anticipate potential attack vectors and prepare defensive and DFIR strategies in advance.

- **Enhanced Simulation and Digital Twins:** Creating high-fidelity digital twins of satellites and ground control systems will allow for realistic simulation of cyberattacks. This enables testing of DFIR plans, training of response teams, and forensic analysis of simulated incidents without risking live assets. AI can enhance these simulations by creating more sophisticated and adaptive adversaries.
- **Standardization and Collaboration:** As the space domain becomes more democratized, there will be a greater need for standardized DFIR procedures, data formats, and secure information sharing protocols (like those facilitated by the Space ISAC) to enable collaborative response to widespread threats.
- **Zero Trust Architectures:** Implementing Zero Trust security models, where no user or system is implicitly trusted, will become more critical. This will require robust identity and access management and continuous verification, which AI can help manage and monitor across distributed space networks.
- **Quantum Computing's Double-Edged Sword:** While quantum computing poses a future threat to current encryption standards, quantum-resistant cryptography (QRC) and potentially Quantum Key Distribution (QKD) will be vital for securing future space communications. DFIR techniques will need to adapt to these new cryptographic realities.
- **DFIR for AI Systems:** As AI itself becomes more integrated into satellite operations, DFIR will also need to address incidents involving compromised or misbehaving AI systems, requiring new techniques to understand AI decision-making processes and identify malicious manipulation.

The journey towards robust DFIR capabilities for satellite and space technologies is ongoing. It requires a multi-disciplinary approach, blending traditional cybersecurity and digital forensics expertise with specialized knowledge of space systems and a forward-looking adoption of advanced technologies like AI. As humanity's reach extends further into space, ensuring the resilience and security of these vital assets will be paramount.