

PREVIEW PREVIEW PREVIEW PREVIEW

eForensics

VOL. 12

NO. 01

ISSN 2300-6986



# SATELLITE FORENSICS

DIGITAL  
FORENSICS  
IN SATELLITE  
AND **UAV**  
**TECHNOLOGY**

THE WORLD  
OF SATELLITES:  
**UNLOCKING**  
**MYSTERIES**  
BEYOND EARTH

TOOLS  
USED  
FOR  
**SPACE**  
**SATELLITE**

WINDOWS  
DIGITAL  
**CYBER-CRIME**  
FORENSICS  
INVESTIGATION

PREVIEW PREVIEW PREVIEW PREVIEW

# EDITOR'S WORD

---

Dear Readers,

Satellite technology has become a ubiquitous feature of modern life, providing integral services such as communication, navigation, streaming, Earth observation, and scientific research. Alongside this growing dependence, however, comes a corresponding increase in vulnerabilities. Consequently, the field of satellite forensics has emerged as a specialized discipline concerned with the gathering and analysis of satellite data to investigate incidents such as unauthorized access, security breaches, and collisions with space debris. As the number of satellite-related incidents continues to rise, so does the importance of satellite forensics in mitigating the risks associated with this technology. We would like to introduce these subjects to you in this issue. You can see where all of this led us by looking through a few truly fascinating articles that we gathered. Kate Libby wrote the article that presents all topics in general, and you will see how interesting this topic is and how useful knowing this technology can be. DR. Sapna V M tells you how Satellite forensics, a quite promising field, involves the investigation and analysis of satellite images and data to track information pertinent to legal and investigative processes. George Antoniou, in his article, delineates the potential digital forensic challenges and discusses the state of digital forensic readiness in the context of 6G satellite and IoT networks. And Rhonda Johnson, in her article, delves into space satellite forensics, exploring the challenges faced, and the tools used to investigate satellite hacking incidents. Moreover, in this issue, you can read fantastic articles written by Alameen Karim Merali, Harsh Behl, and Daniele Ferreira. Our last great source of knowledge is the interviews with two famous experts: Brett Shavers and Barry Grundy. Definitely, you will find your favourite article and a new piece of knowledge in this issue. This publication would not have been possible without the contributions of our authors, reviewers, editors, and proofreaders. It has been a pleasure working with you and learning from your insights.

We look forward to continuing to collaborate and inviting others to create more exceptional content with us. Together, let's make a meaningful impact in our field.

Don't miss out on this must-read issue!

**Ewa & eForensics Team**

[ewa.dudzic@eforensicsmag.com](mailto:ewa.dudzic@eforensicsmag.com)

**Cover Image**  
Wiktoria Bukowska

**Cover Design**  
Wiktoria Bukowska

<b>04</b>	SATELLITE FORENSICS
<b>21</b>	UNLOCKING MYSTERIES BEYOND EARTH FROM ABOVE: THE WORLD OF SATELLITE
<b>25</b>	UNLOCKING THE ORBITAL DOMAIN: DIGITAL FORENSICS IN SATELLITE AND UAV TECHNOLOGIES
<b>33</b>	TOOLS USED FOR SPACE SATELLITE FORENSICS
<b>40</b>	WINDOWS DIGITAL CYBER-CRIME FORENSICS INVESTIGATION
<b>50</b>	FOUR WAYS TO CRAFT A DEFENSIBLE NARRATIVE WITH DIGITAL FORENSICS
<b>55</b>	CYBER THREAT INTELLIGENCE 101
<b>63</b>	INTERVIEW WITH BRETT SHAVERS
<b>67</b>	INTERVIEW WITH BARRY GRUNDY

All trademarks, trade names, or logos mentioned or used are the property of their respective owners. The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

# SATELLITE FORENSICS

KATE LIBBY

Satellites have become indispensable elements of modern-day life. This technology is playing a vital role in communication, navigation, streaming services, Earth observation, and scientific research. As our dependence on satellite technology grows, the number of vulnerabilities grows with it; so does the need for satellite forensics, a specialized field focused on gathering and analyzing data from satellites to investigate incidents, such as space debris collisions, unauthorized access, or security breaches.

## ***Significance of Satellite Forensics***

Satellite forensics is a specialized field that has grown in importance as our reliance on satellite technology expanded across various sectors.

Satellite forensics plays a crucial role in investigating incidents and maintaining the integrity, security, and functionality of satellites. The significance of satellite forensics can be understood in the following points:

**Protecting Critical Infrastructure:** Satellites are an integral part of critical infrastructure, including telecommunications, navigation, weather monitoring, and national defense. Any compromise in the functionality of these satellites can have far-reaching consequences. Satellite forensics helps safeguard these systems by identifying and addressing vulnerabilities and threats.

**Space Debris Mitigation:** The increasing amount of space debris in Earth's orbit poses a substantial risk to operational satellites. Satellite forensics can help investigate incidents involving space debris collisions, providing valuable insights into the causes and potential ways to mitigate such risks. By understanding these incidents, the field contributes to the safe operation of satellites in space.

**Security and Data Integrity:** In an era of increased cyber threats, satellite systems are not immune to cybersecurity risks. Unauthorized access, data breaches, and other forms of interference can compromise satellite functionality.

# CALL FOR PAPERS

**FOR OUR MAGAZINE,  
WE ARE LOOKING FOR  
TUTORIALS, CASE  
STUDIES, STEP-BY-  
STEP GUIDES, AND  
ARTICLES THAT  
WOULD INTEREST  
INTERMEDIATE AND  
ADVANCED READERS.**

**SEND YOUR EMAIL TO:**

[hello@eforensicsmag.com](mailto:hello@eforensicsmag.com)

**MORE INFORMATION:**

[www.eforensicsmag.com](http://www.eforensicsmag.com)



# UNLOCKING MYSTERIES BEYOND EARTH FROM ABOVE: THE WORLD OF SATELLITE

DR. SAPNA VM

## So....What is a Satellite?

Satellites, sometimes called “Digital Television”, orbiting high above the Earth's atmosphere, have become essential tools for communication, navigation, weather monitoring, and national security, but there are also natural satellites. For example, Earth is a satellite because it orbits the sun, and the moon is a satellite because it orbits the Earth. Figure 1 shows the typical satellite architecture. Dotted orange arrows denote radio links; solid black arrows denote ground network links. While their main functions are recognized, they also play a vital role in forensic investigations, helping unravel mysteries from above and provide valued insights into numerous events and occurrences. Satellite forensics, a quite promising field, involves the investigation and analysis of satellite images and data to track information pertinent to legal and investigative processes.

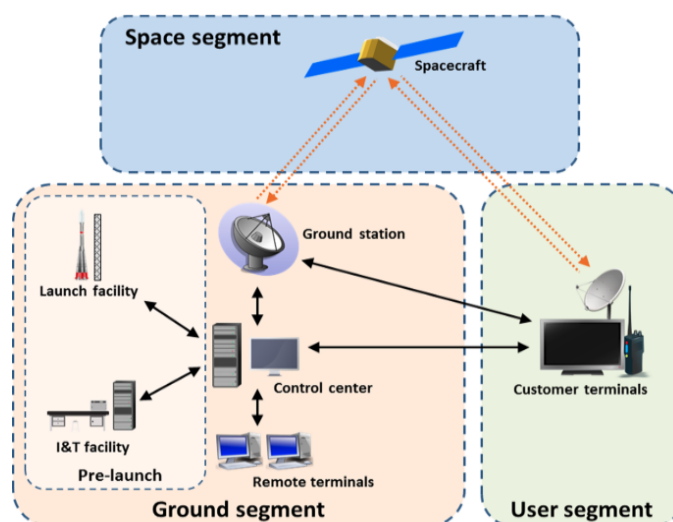


Figure 1. [https://commons.wikimedia.org/wiki/File:Ground\\_segment.png](https://commons.wikimedia.org/wiki/File:Ground_segment.png)

# UNLOCKING THE ORBITAL DOMAIN: DIGITAL FORENSICS IN SATELLITE AND UAV TECHNOLOGIES

*GEORGE ANTONIOU, PH.D.*

The evolution of digital technology has significantly broadened the scope of digital forensics, a field traditionally tethered to terrestrial digital systems. The advent of satellite and Unmanned Aerial Vehicle (UAV) technologies has opened up new frontiers, marking a significant stride towards a global digital ecosystem. These technologies are the linchpins in a gamut of critical sectors including global communication, navigation, and surveillance. The imperative to safeguard these systems against burgeoning cyber threats has catalyzed the emergence of satellite and UAV digital forensics. This discourse endeavors to traverse the nascent field of satellite and UAV digital forensics, elucidating on the symbiotic relationship between emerging digital forensic tools, methodologies, and the inherent challenges.

## **Background**

A plethora of studies have surfaced over the years, delineating the trajectory of digital forensics in satellite and UAV technologies. For instance, Akinbi (2023) explored the vicissitudes of satellite digital forensics in the digital epoch, highlighting both the opportunities and challenges that lie therein. Similarly, Thornton and Bagheri Zadeh (2022) unveiled a new horizon in digital investigation through UAV digital forensics. These studies elucidate the burgeoning digital forensic tools and methodologies tailored for these novel domains. However, a discernible lacuna exists in addressing the nuanced technical and legal challenges, and the evolving threat landscape. A comparative scrutiny of these seminal works reveals a pressing need for a robust legal and technical framework to bolster digital forensic investigations in satellite and UAV domains.

The impending evolution of sixth generation (6G) wireless networks, projected to be operative by the 2030s, heralds a new epoch of technological innovation characterized by ultra-high-speed data transmission and superior network performance over the extant fifth generation (5G) networks.

# TOOLS USED FOR SPACE SATELLITE FORENSICS

*RHONDA JOHNSON*

Satellites are crucial in modern communication, navigation, weather forecasting, and national security. As our dependence on satellite technology grows, so does the potential for malicious activities, including hacking and unauthorized access. Space satellite forensics has emerged as a vital field for investigating and mitigating the impact of satellite attacks.

In this article, we delve into space satellite forensics, exploring the challenges faced, and the tools used to investigate satellite hacking incidents.

## ***Challenges in Space Satellite Forensics***

Satellite hacking investigations require a multidisciplinary approach combining space technology, cybersecurity, and digital forensics expertise. Professionals in this field must navigate the complexities of space systems, understanding the intricacies of satellite hardware, software, and communication protocols. Analyzing satellite data and identifying signs of compromise demand specialized knowledge, as traditional digital forensic tools may not be directly applicable in the extraterrestrial context. The scarcity of physical evidence and the remote nature of satellite operations necessitate innovative approaches to collect, preserve, and analyze data, requiring experts to adapt and develop new methodologies.

## ***Tools for Space Satellite Hacking Investigation***

### **Satellite Communication Interception Tools**

Satellite Ground Stations are pivotal in satellite communications, serving as the primary link between Earth and orbiting satellites. In forensic investigations, analyzing the activities at ground stations becomes crucial. For instance, investigators can scrutinize communication logs to trace data flow between ground stations and satellites, identifying unauthorized access or unusual patterns. Frequency data, which indicates the specific radio frequencies used for communication, is another valuable resource for forensic analysts. Unusual frequency shifts or unexpected changes may signal a potential intrusion or compromise. Moreover, studying transmission timings can reveal irregularities that may suggest a hacking attempt, as deviations from established schedules could indicate unauthorized activities.

Software-defined radios (SDRs) represent a versatile tool for satellite hacking investigations, offering the capability to intercept and analyze satellite signals. These radios can be



programmed to receive and decode signals from various frequencies, making them essential for monitoring satellite communications. In a forensic context, investigators employ SDRs to capture transmissions between ground stations and satellites, enabling them to scrutinize the data for anomalies or signs of compromise. For example, if an SDR intercepts an unusual signal that does not conform to the expected communication protocols, it could indicate a potential security breach. Additionally, the ability of SDRs to adapt and tune to different frequencies allows investigators to stay ahead of evolving hacking techniques, providing a dynamic and responsive approach to satellite forensic analysis.

Beyond ground stations and SDRs, artificial intelligence (AI) and machine learning (ML) in satellite forensic investigations are gaining prominence. AI algorithms can sift through vast amounts of satellite data, automatically identifying patterns or anomalies that may elude human analysts. For instance, machine learning models can learn the typical patterns of satellite communications and raise alerts when deviations occur. This advanced technology enhances the efficiency and effectiveness of satellite hacking investigations, allowing for real-time analysis and proactive threat detection.

### **Telemetry Analysis Tools**

Telemetry decoders play a crucial role in satellite hacking investigations by providing insights into the health and status of satellites. Telemetry data encompasses various parameters, such as temperature, power levels, and system diagnostics, allowing investigators to understand the satellite's operational status comprehensively. Decoding telemetry signals enables forensic experts to interpret this data, identifying standard patterns and detecting anomalies that may indicate unauthorized interference. For example, sudden power consumption fluctuations or unexpected temperature reading changes could indicate a cyberattack on the satellite's systems. By closely examining telemetry data, investigators can reconstruct the events leading up to a potential compromise, aiding in the attribution and resolution of satellite hacking incidents.

In satellite cybersecurity, Simple Network Management Protocol (SNMP) tools are instrumental for monitoring and managing network devices, including satellites. SNMP allows administrators to gather information about the performance and status of networked devices, making it a valuable resource for investigators. By analyzing SNMP data, forensic experts can detect irregularities that may signify unauthorized access attempts or abnormal network behavior. For instance, an investigator might notice a spike in SNMP requests originating from an unfamiliar source, suggesting a potential hacking attempt. Additionally, changes in configuration settings through SNMP, such as alterations to access controls or network parameters, could raise red flags during a forensic analysis. Implementing robust SNMP monitoring practices enhances the ability to identify and respond promptly to security threats in the satellite communication infrastructure.

As technology advances, the integration of blockchain technology in satellite communication security is becoming an area of exploration. With its decentralized and tamper-resistant nature, blockchain offers the potential to enhance the integrity and authenticity of telemetry and SNMP data. By recording telemetry and SNMP information on a blockchain, investigators can establish a secure and immutable audit trail, ensuring the integrity of critical data. Any attempt to tamper with or manipulate telemetry signals or SNMP records would leave a trace on the blockchain, providing a transparent and trustworthy record of satellite activities. This innovative approach adds an extra layer of security to satellite forensic investigations, addressing data tampering concerns and ensuring evidence's reliability in legal proceedings.

### **Cybersecurity Tools**

Intrusion Detection Systems (IDS) serve as a vital component in space satellite forensics, offering a proactive means to monitor and identify potential security threats. These systems can be strategically deployed on ground stations or within satellite networks to continuously analyze network traffic and detect anomalous patterns or activities that may signify a hacking attempt. For example, if an IDS identifies a sudden surge in data transfer rates or unexpected communication patterns, it could indicate a potential cyber intrusion. By setting up rules and signatures that define normal network behavior, investigators can configure IDS to raise alerts or take automated actions when deviations occur. The use of anomaly-based detection methods within IDS allows for the identification of novel and previously unseen attack patterns, enhancing the system's capability to thwart sophisticated hacking attempts in space satellite communication.

Firewall logs are instrumental in space satellite forensics for uncovering unauthorized access attempts and patterns of communication within satellite networks. Firewalls act as a critical line of defense, regulating incoming and outgoing network traffic based on predetermined security rules. Analyzing firewall logs provides investigators with valuable insights into the flow of data, revealing any suspicious activities that might indicate a security breach. For instance, repeated failed login attempts or unusual requests to access restricted areas of the satellite network could be flagged through careful examination of firewall logs. Furthermore, firewall logs can assist in reconstructing the sequence of events during an attack, aiding investigators in understanding the methods employed by hackers and facilitating the attribution process.

To enhance the capabilities of Intrusion Detection Systems and firewall logs, the integration of threat intelligence feeds is becoming increasingly important in space satellite forensics. Threat intelligence feeds provide real-time information about emerging cyber threats, allowing IDS and firewalls to adapt quickly to evolving attack methods. By incorporating threat intelligence data into these tools, investigators gain a proactive defense mechanism that can identify and mitigate potential threats before they manifest into full-blown attacks. For example, if a threat intelligence feed reports a new type of malware targeting satellite communication systems, IDS can be configured to recognize and block such threats based on the latest threat intelligence, bolstering the overall resilience of space satellite networks against cyber threats.

## **Satellite Imaging and Remote Sensing**

Satellite Imagery Analysis is a powerful tool in space satellite forensic investigations, enabling investigators to scrutinize high-resolution satellite imagery to identify potential physical tampering or unauthorized objects in space. By comparing current imagery with historical data, investigators can detect subtle changes around satellites or anomalies that may suggest interference. For instance, if unauthorized modifications or additions are observed on a satellite's exterior, it could indicate tampering or potential sabotage. Additionally, the capability to analyze satellite imagery in real-time enhances the responsiveness of forensic investigations. If an irregularity is identified, investigators can swiftly deploy countermeasures to address security concerns, demonstrating the importance of satellite imagery analysis in maintaining the integrity of space assets.

Ground-based telescopes complement satellite imagery analysis by providing an alternative means of observing satellites in orbit. These telescopes can capture valuable data, such as the satellite's position, trajectory, and behavior, aiding forensic analysts in reconstructing events leading up to a potential security incident. For example, anomalies in a satellite's orbit or unexpected changes in its movement patterns could be indicative of a cyberattack or physical interference. Ground-based telescopes also offer the advantage of continuous monitoring, allowing investigators to track a satellite's movements over extended periods and providing a more comprehensive view of its operational behavior. The combination of satellite imagery analysis and ground-based telescope observations presents a holistic approach to space satellite forensics, enhancing the ability to detect and respond to security threats from multiple perspectives.

Advancements in artificial intelligence (AI) and machine learning (ML) further contribute to the effectiveness of satellite imagery analysis and ground-based telescope observations in space satellite forensic investigations. AI algorithms automate the analysis of vast amounts of satellite imagery, rapidly identifying anomalies or patterns that may indicate tampering or unauthorized activities. Machine learning models can also predict normal behavior based on historical data, enabling quicker detection of deviations that may signal a security breach. Integrating AI and ML into space satellite forensics enhances the efficiency of analysis. It enables continuous improvement as these algorithms learn from new data, staying ahead of emerging threats in the ever-evolving landscape of satellite security.

## **Cryptographic Analysis Tools**

Encryption Key Analysis is a critical tool in space satellite forensic investigations, especially considering the reliance on encryption to secure satellite communications. Investigative tools can meticulously analyze cryptographic data to identify any compromises in encryption keys or attempts to decrypt secure channels. For instance, if an unauthorized entity gains access to a satellite's encryption keys, it could eavesdrop on sensitive communications or even

manipulate data. Investigators can use specialized tools to scrutinize key management protocols, monitor changes in encryption key configurations, and identify any anomalies that may indicate a security breach. By conducting thorough encryption critical analysis, forensic experts can trace the source of compromised keys, assess the extent of unauthorized access, and implement corrective measures to safeguard satellite communication integrity.

Steganography detection tools are crucial in uncovering covert communication within satellite data. Steganography involves concealing information within seemingly innocuous files or transmissions, making detecting it challenging. In space satellite forensic investigations, tools capable of detecting steganographic methods are employed to uncover hidden messages or malicious payloads embedded in satellite communications. For example, a steganography detection tool may identify subtle alterations in image or signal data that deviate from expected patterns, suggesting hidden information. By revealing these concealed elements, investigators can uncover potential threats, such as covert channels used by attackers to transmit malicious commands or exfiltrate sensitive data. The continuous advancement of steganography detection tools ensures that forensic analysts remain equipped to identify and counter increasingly sophisticated covert communication techniques in satellite networks.

In addition to encryption critical analysis and steganography detection, integrating blockchain technology in satellite communication security adds an extra layer of protection. Blockchain can securely manage and authenticate encryption keys, ensuring their integrity and preventing unauthorized alterations. Additionally, blockchain's transparent and decentralized nature can assist in maintaining an immutable record of cryptographic activities, making it more challenging for malicious actors to manipulate encryption-related data. As space satellite communication technologies evolve, leveraging encryption critical analysis, steganography detection, and blockchain-based security measures provides a comprehensive approach to safeguarding satellite communications from potential cyber threats.

### **Conclusion**

*Space satellite forensics* is an evolving field that plays a critical role in maintaining the integrity and security of satellite systems. As technology advances, so does the need for sophisticated tools and techniques to investigate satellite hacking incidents.

The collaboration between space agencies, cybersecurity experts, and forensic investigators is crucial for developing and refining the tools needed to secure our presence in space. As we venture further into the cosmos, safeguarding our satellite infrastructure becomes paramount for the continued success of space exploration and satellite-dependent applications on Earth.

### **References**

Fleron, R. W. (2019). Satellite Forensics: Analysing Sparse Beacon Data to Reveal the Fate of DTUsat-2. *International Journal of Aerospace Engineering*, 2019, Article 8428167. <https://doi.org/10.1155/2019/8428167>

Manulis, M., Bridges, C.P., Harrison, R. *et al.* Cyber security in New Space. *Int. J. Inf. Secur.* **20**, 287–311 (2021). <https://doi.org/10.1007/s10207-020-00503-w>

Horváth, J., Xiang, Z., Cannas, E. D., Bestagini, P., Tubaro, S., & Delp III, E. J. (2022, May). Sat U-Net: a fusion based method for forensic splicing localization in satellite images. In *Multimodal Image Exploitation and Learning 2022* (Vol. 12100, p. 1210002). SPIE.

Horvath, J. (2022). *Manipulation Detection and Localization for Satellite Imagery* (Doctoral dissertation, Purdue University).

Straub, J., Swartwout, M., Nunes, M., & Lappas, V. (2019). CubeSats and small satellites. *International Journal of Aerospace Engineering*, 2019, 1-3.

### **About the Author**

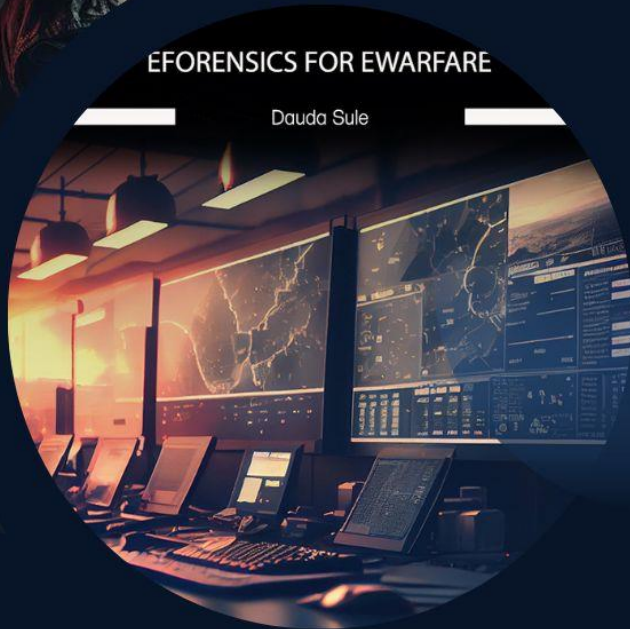
*Rhonda Johnson has Certified Digital Forensics Examiner and Certified Penetration Testing Engineer certifications from Mile2. She serves as e-learning manager/course creator for Ogun Drone Forensics Training LLC in Houston, TX ([ogunforensics.com](http://ogunforensics.com)). She has a Master's in Computer and Information Security, and she is currently on the editorial review board for the International Journal of Cyberwarfare and Terrorism and a Peer Reviewer for the International Journal of Digital Crime and Forensics.*

Join Us!

# eForensics

magazine & courses

## ONLINE COURSES



[eforensicsmag.com](http://eforensicsmag.com)

# WINDOWS DIGITAL CYBER-CRIME FORENSICS INVESTIGATION

*ALAMEEN KARIM MERALI*

## ***What exactly is Digital Cyber-Crime Forensics?***

Digital Cyber-Crime Forensics is a discipline that investigates and identifies processes, inspecting and analyzing data to obtain information or evidence that leads to a suspect of a cyber-crime. As a certified Computer Hacking Forensic Investigator myself, I am aware that there's plenty of information that needs to be taken into consideration when acquiring data, as we shall see below.

## ***How is it done?***

Digital data forensics could take many formats; one is when investigators need to be aware that some data is latent, which normally means that they can't be seen as obvious and requires deeper analysis. Performing forensics itself is a tedious task since it really depends on how much information you have to start working from.

## ***What does the court consider as evidence?***


In order to present data that adheres to strict investigation procedures, an acceptable and approved chain of custody pathway needs to be followed. Data obtained in such a manner should be presented in a tested and proven evidence register suitable for court proceedings. The chain of custody is normally only for the eyes of a specific number of people, who are supposed to sign the document in order to view the evidence. No one else has access. This is how tough integrity of digital evidence needs to be kept because any tampering would cause the evidence to be disproved by the court. Some other ways of proving integrity include hashing.

While keeping the chain of custody, it's important that information or data that was analyzed pertaining to obtaining evidence isn't exposed publicly by third parties that have signed the chain of custody document. A suspect of a cyber-crime could be brought into trial years after evidence has been gathered and sent to the court.

# GET YOUR COPY NOW!

eForensics | VOL. 11  
NO. 09

ISSN 1733-7186



**THE COMPLETE GUIDE  
TO USING AUTOPSY**

---

LEARN HOW TO PERFORM A <b>FORENSIC ANALYSIS</b> USING AUTOPSY 4.21.0	EXPLORE HOW TO USE AUTOPSY, FROM STARTING A CASE TO <b>MANAGING ARTIFACT CONTENTS</b>	<b>HUNT HACKERS</b> USING AUTOPSY ON A MACOS IMAGE	USING AI AND <b>HIGH-TECH TOOLS</b> , REDEFINE THE LIMITS OF CASE SOLVING
----------------------------------------------------------------------	---------------------------------------------------------------------------------------	----------------------------------------------------	---------------------------------------------------------------------------

WITH THE HELP OF ALL THIS KNOWLEDGE, YOU WILL BE ARMED TO SOLVE EVERY CASE AND RANK AMONG THE INDUSTRY'S TOP EXPERTS.



# FOUR WAYS TO CRAFT A DEFENSIBLE NARRATIVE WITH DIGITAL FORENSICS

*HARSH BEHL*

Every prosecutor understands that in order to secure a conviction, they must present the evidence in a compelling narrative. Whether it's a murder trial or a financial crime, absent a well-constructed narrative arc, even the most talented prosecutor will struggle to hold the attention of their audience. It's how the story is told and the way in which it's presented to a jury that can make the difference between a guilty or not-guilty verdict.

As many digital investigators have come to appreciate firsthand, the primary challenge of a modern investigation is not the scarcity of evidence in a case but rather the overwhelming abundance of it. To secure a conviction is not simply a matter of gathering and preserving mountains of digital evidence, but also connecting a constellation of data points so that a prosecutor or trial lawyer can reveal the story that's hidden within the data. In this context, small but telling details like a defendant's location on a specific date and time or the last phone call the defendant made just minutes before the incident occurred can become crucial to creating a logical narrative that is defensible in court.

## ***Complexity of Modern Investigations***

The nature and scope of investigations has changed dramatically over the past decade. It's hardly an exaggeration to say that every investigation has a digital component of some type. As we continue to incorporate digital devices into our daily lives, each of us leaves a trail of unique and traceable digital activity, or digital footprints, everywhere we go. These footprints include a variety of actions and communications that are manifested on these devices or the Internet. Whether it's through our use of smartphones, tablets, laptops, our social media activity, or even through the various IoT (Internet of Things) devices that we interact with daily, individuals generate a vast amount of digital data daily.

# CYBER THREAT INTELLIGENCE 101

DANIELE FERREIRA

Cyber Threat Intelligence, or CTI, emerged with the creation of the first Military Intelligence departments in the mid-19th century. However, this concept is much older and is intrinsic to the evolution of humanity, demonstrated by numerous espionage cases during the period of globalization and territorial conflicts. During major wars, this need evolved, and to gain a military advantage, it was not enough to merely know but rather to know everything about the enemy. The definition of intelligence is a subject that has been debated for years by academics who, apparently, have not reached a conclusion. Michael Warner cites in his paper "Wanted: A Definition of Intelligence" a definition that states, "*Intelligence deals with all the things which should be known in advance of initiating a course of action.*" But let's return to the fundamentals. When we talk about Cyber Threat Intelligence, we refer to a discipline within the field of cybersecurity that is based on the above-mentioned concept (prior knowledge) to proactively address threats to computer networks. CTI thus represents the convergence of two communities: intelligence and cybersecurity. CTI focuses on the collection and analysis of information from internal and external sources to gain a better understanding of vulnerabilities or potential threats to ensure the protection of assets according to their value to the company.

But what is a threat? We may define a threat as any circumstance or event with the potential to exploit vulnerabilities in environments, systems, and people, causing a negative impact on operations, assets, and individuals within a private organization or public entity. The information generated in CTI, aimed at combating or minimizing threats, has three levels, strategic, tactical, and operational, described below:

## **Strategic Information**

High-level information is consumed by senior management and decision-making areas regarding threats, trends, and cyber attacks. In general, these decisions have financial implications and guide investments in prevention.

# INTERVIEW WITH BRETT SHAVERS

*Brett Shavers is a former law enforcement detective and currently is a digital forensics consultant to law firms in civil litigation along with an occasional government engagement in high profile investigations. Brett has been assigned to local state, and federal task forces working all types of cases, including international and national security matters. He has been trained by several US federal agencies, quite a few forensic software companies, and higher educational schools. Brett has published several books, including *Placing the Suspect Behind the Keyboard*, *Hiding Behind the Keyboard*, and the *X-Ways Forensics Practitioner's Guide*. Brett's greatest teachers have been those he wined and dined with while undercover. You can find him rambling away at [www.brettshavers.com](http://www.brettshavers.com).*



**Could you please introduce yourself to our readers? Let us know who you are.**

Hi. My name is Brett Shavers and I have been in the digital forensics field since 2004 as a student, practitioner, consultant, expert witness, author, and adjunct professor. I've worked in law enforcement for the better part of 2 decades in SWAT, bicycle patrol, undercover, detectives, and as a computer forensics investigator. Before that, I jumped out of airplanes and walked around the woods a lot.

**Can you provide more information about your background and experiences?**

I got my start in forensics while working as an undercover officer assigned to a federal task force. I had my first exposure to digital forensics in that assignment, and brought back experience, training, and gear to propose a digital forensic capability to my police department. It took more than a year for approval, but I finally was allowed to create the unit, operating out of a storage closet.

# INTERVIEW WITH BARRY GRUNDY

*A U.S. Marine Corps veteran, Barry Grundy has been working in the field of digital forensics since the mid-1990s. Starting at the Ohio Attorney General's office as a criminal investigator, and eventually joining U.S. Federal Law Enforcement as a digital forensics analyst and computer crimes investigator in 2001.*

*He holds a Bachelor of Science in Forensic Science from Ohio University, and a Master's Degree in Forensic Computing and Cybercrime Investigations from*

*University College Dublin. Barry is the author and maintainer of the Law Enforcement and Forensic Examiner's Introduction to Linux ([LinuxLEO])(<https://linuxleo.com>)).*

*This practical beginner's guide to Linux as a digital forensics platform has been available for over 20 years and has been used by a number of academic institutions and law enforcement agencies around the world to introduce students of DFIR to Linux. Teaching, particularly Linux forensics and open source DFIR tools, is his passion. Barry retired from federal service in 2023, and continues to teach and contribute to the DFIR community where possible.*

**Could you please share some information about yourself and your career?**

I left the United States Marine Corps in 1990 and attended Ohio University in Athens, Ohio where I studied forensic chemistry and physical anthropology. My goal at the time was a career in forensic science. It was here where I was first exposed to Linux and UNIX as part of my studies and research. After college, I spent four years as a forensic chemist working in Ohio. It did not take long for me to decide that working in a lab full time (doing chemistry, at least) was not for me.



# PRESALE OUT NOW!

## MICRO-DRONE WARFARE

CYBERSECURITY IMPLICATIONS AND COUNTERMEASURES

Rhonda Johnson



DELVE INTO THE VARIOUS TYPES AND CAPABILITIES OF MICRO-DRONES, THEIR COMMUNICATION AND NETWORKING TECHNOLOGIES, AND THE ASSOCIATED CYBERSECURITY VULNERABILITIES!