Forensic Insights into SenseCAP: A Comprehensive Examination of Technical and LoRa Connectivity Dimensions

Nurettin Selcuk Senol and Amar Rasheed
Dept. of Computer Science, Sam Houston State University, Huntsville, Texas, USA

nss016@shsu.edu
axr249@shsu.edu

Abstract: The rapid expansion of Internet of Things (IoT) devices has reshaped various sectors by improving connectivity, efficiency, and convenience. Central to this transformation are LoRa (Long Range) and LoRaWAN (Long Range Wide Area Network) technologies, which provide reliable, low-power, long-range communication critical for IoT applications. As these systems evolve, examining security vulnerabilities and forensic challenges becomes increasingly essential. This paper explores digital forensics within IoT environments, focusing on the methodologies and tools required to secure and maintain the integrity of IoT deployments. By analyzing artifacts and log data from SenseCAP devices, the study offers insights into device operations and user interactions. Additionally, frequency analysis conducted via Software-Defined Radio (SDR) confirmed LoRa communication within expected frequency bands. The findings highlight the importance of robust forensic investigations to protect IoT ecosystems from cyber threats. Through an extensive literature review and empirical analysis, this paper contributes to advancing IoT device forensics, proposing strategies to address emerging challenges and enhance the resilience of IoT infrastructures in an increasingly interconnected world.

Keywords: Digital forensics, SenseCAP, LoRa, LoRaWAN, Browser forensics, Digital investigation

1. Introduction

The Internet of Things (IoT) has completely changed how we engage with technology in the modern world. IoT devices, which can be anything from industrial automation equipment to smart home systems, are becoming an essential part of our everyday lives since they facilitate smooth device connectivity and increase convenience, productivity, and efficiency. Over the past decade, there has been a significant transition from traditional to IoT-enabled devices, driven by the increasing demand for innovative technologies that boost connectivity and efficiency. As these devices proliferate across various sectors, healthcare, agriculture, logistics, and more—their importance continues to grow. By 2030, it is projected that IoT devices will account for 75% of all devices in use. This trend underscores the growing importance of IoT in shaping the future of technology and its applications in everyday life (Paolone 2022).

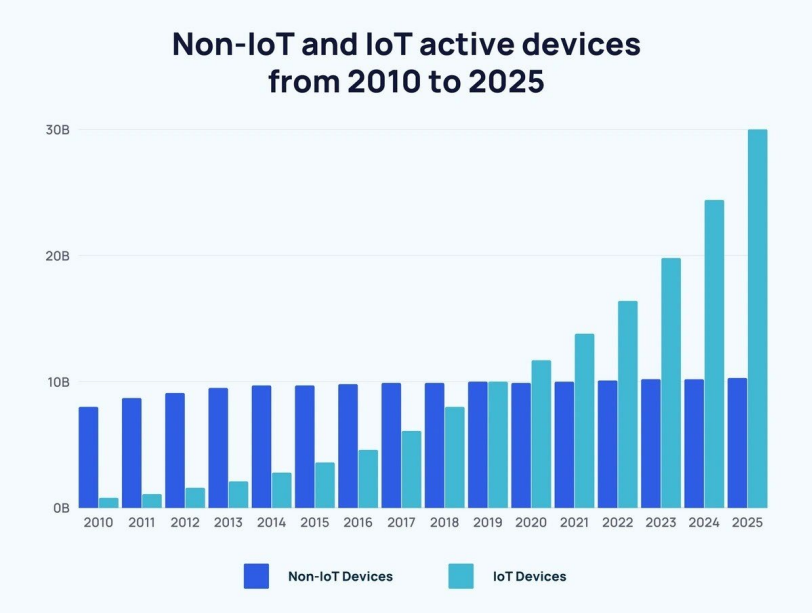

Figure 1: A comparison of active non-IoT and IoT devices from 2010 to 2025 (Paolone 2022)

The development of LoRa and LoRaWAN technologies is essential to the Internet of Things. LoRa is a modulation technology that is perfect for battery-operated devices since it provides long-range communication with low power consumption. In addition, LoRaWAN is a wide-area network system architecture and communication protocol that makes safe and effective long-distance data transfer possible.

Together, these technologies facilitate the deployment of IoT networks in remote and challenging environments, providing scalable and cost-effective connectivity solutions. SenseCAP, a product line from Seeed Studio, exemplifies the potential of LoRa and LoRaWAN in IoT applications. Designed for environmental monitoring, agriculture, and smart cities, SenseCAP devices offer robust performance and reliability. They come equipped with various sensors and connectivity options, making them versatile tools for data collection and analysis in diverse scenarios. The SenseCAP M2 Kit emphasizes the importance of LoRaWAN on the Internet of Things ecosystem by offering consumers a complete solution for configuring and maintaining LoRaWAN networks. With such a wide range of uses, the likelihood of finding these types of devices at crime scenes or their involvement in cybercrimes also increases. Digital forensics is essential to maintaining the integrity and security of the massive amounts of data that IoT devices, such as SenseCAP. Forensic investigation helps uncover vulnerabilities, validate functionality, and ensure compliance with security standards. By scrutinizing IoT devices from a forensic perspective, we can better understand their operational mechanics, detect potential threats, and safeguard against malicious activities. This enhances the overall security and reliability of IoT deployments, making digital forensics an indispensable part of the IoT landscape. Along with mentioning these points, this paper's contribution is as follows:

- Our investigation contributes to the understanding of IoT device forensics by providing insights into the operational dynamics and security implications of SenseCAP devices. Through artifact analysis, log examination, and frequency traffic analysis, we uncover valuable information about user interactions and device configurations.
- We created a dataset containing signals from LoRa transmissions, collected using SDR and the SenseCAP starter kit. This dataset offers real-world data for comprehensive analysis at the Autonomous Systems and IoT Lab in the Computer Science Department.

The purpose of this work is to advance IoT security and forensic practices by thoroughly analyzing SenseCAP devices' forensic artifacts and LoRa communication behaviors. By addressing key vulnerabilities and leveraging frequency analysis through Software-Defined Radio (SDR), this study highlights the importance of robust forensic methodologies in safeguarding IoT ecosystems against evolving cyber threats.

To address the critical challenges in IoT security and forensics, this study investigates the following research questions: **What are the key forensic artifacts and log data generated by SenseCAP devices during operation, and how can these be analyzed to uncover vulnerabilities and user interactions?** Additionally, **how effectively can frequency analysis using Software-Defined Radio (SDR) validate the integrity and expected behavior of LoRa communications within IoT networks?**

In this article, Section II covers the literature review, surveying related research papers and previous studies to provide a comprehensive background on the topic. Section III covers the methodology used in our investigation, outlining the processes and techniques employed. Section IV addresses our results in this study, Section V presents the conclusion and future work, summarizing the findings and their implications and future directions.

2. Literature Review

This section of our work provides a comprehensive overview of existing research related to IoT devices, LoRa, LoRaWAN technology, and digital forensics. It critically examines previous studies, highlighting the advancements and gaps in the current body of knowledge. By exploring various scholarly articles, technical reports, and case studies, this section aims to establish a solid foundation for understanding the context and significance of our investigation. Additionally, it identifies the key challenges and emerging trends in the field, setting the stage for the subsequent sections of this article.

LoRaWAN technology is employed in a wide range of applications, including health and wellbeing monitoring (Catherwood 2018), (Petäjäjärvi 2017), agricultural monitoring (Ilie-Ablachim 2016), (Sartori 2016), (Benaissa 2017), (Jawad 2017), wireless sensor networks (Lee 2018), (Wixted 2016) traffic monitoring (Sharma 2018), localization (Aernouts 2018), (Podevijn 2018), (Pasolini 2018) smart city projects (Pasolini 2018), and smart grids and telemeasurements (Del Campo 2018), (Rizzi 2017), (Varsier 2017), (De Castro Tomé 2018). Large-scale installations and non-latency-sensitive applications are their primary areas of suitability.

Adelantado et al. (Adelantado 2017) claim that while LoRaWAN is not ideal for video surveillance and is less suitable for real-time monitoring in big installations, it is feasible for smart-city applications, metering, and logistics tracking.

Using an Arduino platform. A testbed was created by Senol et al. (Senol, Rasheed 2023) to enable communication between two Arduino units via the LoRa protocol. An overview of the main characteristics of LoRa is given in this paper, along with a detailed explanation of the testbed setup and design. The study also includes experimental findings on packet loss, data throughput, and signal strength measures.

The work (Shalaginov 2020) examines the readiness and complexity of community-accepted smart devices for aiding criminal investigations. It describes a precise process and provides resources for Smart Applications while analyzing pertinent artifacts from the perspective of the digital forensics procedure. The study sheds light on the prospects and difficulties in IoT forensics, especially at the edge.

Using Wireshark and Netcut. Hildayantil et al. (Hildayanti 2019) examined router data flow prior to and during network disconnection to investigate digital data gathering. To simulate daily internet access through a router, the study first created scenarios. Numerous data categories, including the Internet Protocol, the accessed material, access times, and locations, were found by the research. The comparison of the router data flow prior to and following the network disconnection was the main emphasis since it showed variations in data packet transmission and demonstrated how network disruptions affect data flow.

Nawaf et al. (Nawaf 2024) explore router forensics, emphasizing the importance of extracting and analyzing data from routers, which are crucial in managing network information flow. It examines traditional and modern forensic techniques, highlighting the significance of router logs and volatile data. The research addresses the challenges of diverse router architectures and evolving cyber threats, advocating for standardized forensic protocols. Additionally, it discusses the potential of machine learning in enhancing forensic capabilities, aiming to strengthen the cybersecurity community against increasing cyber threats and ensuring a more secure digital environment.

The work in (Wiles 2007) provides an overview of router and network forensics, focusing on the practices of sniffing, recording, and analyzing network traffic and events to identify the origins of security incidents and attacks. A significant aspect of this field involves the expertise needed to distinguish between recurring issues and intentional malicious activities. Routers, whether hardware or software, play a pivotal role in directing data from local area networks to other networks, making decisions on the most optimal paths for network traffic. Positioned at layer three of the OSI model, known as the networking layer, routers manage routing between networks, define logical addressing, handle errors, regulate congestion, and sequence packets.

3. Methodology

In the methodology section, we offer a thorough exposition of extant research pertinent to IoT devices, LoRa, LoRaWAN technology, and digital forensics. This segment critically evaluates prior studies, delineating the strides made and lacunae present in the contemporary scholarly discourse. Through an examination of scholarly articles, technical reports, and case studies, our objective is to furnish a robust framework for comprehending the context and importance of our inquiry. Moreover, we spotlight key challenges and emergent trends in the domain, thus priming the terrain for the ensuing sections of this article.

3.1 The SenseCAP LoRaWAN Gateway

As a traditional LoRaWAN gateway, the SenseCAP M2 Multi-Platform LoRaWAN Gateway may communicate with several network servers. It is compatible with international LoRaWAN® frequency plans between 865 MHz to 923 MHz, making it appropriate for various LoRaWAN uses, including precision farming, environmental monitoring systems, smart building management, and more. With its wide range of coverage, strong signal output capabilities, and other cutting-edge characteristics, this gateway is a great option for building a durable LoRaWAN network (Seeed Studio 2023).

- Compatibility with Multiple LoRaWAN® Network Servers: Using the Packet Forwarder / Basics Station mode, the device supports multiple LNS, including AWS, TTN, ChirpStack, and others.
- Integrated LoRaWAN Network Server: The device provides a quick and dependable way to start a LoRaWAN network by using Chirp- stack.
- Integrated SenseCAP Local Console for Easy Configuration: Through an Ethernet and Wi-Fi AP-accessible Web UI, users may effortlessly setup the device.
- Support for Power-over-Ethernet (PoE): With PoE built-in, customers may power the gate via Ethernet, which improves deployment speed and reliability.
- Extensive Coverage and Strong Signal: The device provides robust LoRaWAN® coverage of up to 10km and a powerful signal, facilitating long-range data transmission at low data rates.

- Outstanding Performance: The gateway's Semtech SX1302 base-band long-range chip and well-established hardware solution, the MT7628, guarantee outstanding and reliable performance. In addition to Wi-Fi and Ethernet internet connections.
- Expert Management Tools and Cloud Services: An intuitive web interface makes it simple for users to configure and maintain the gateway. SenseCAP Portal and SenseCAP Local Console are supplementary resources designed to facilitate effective gatekeeping and oversight.

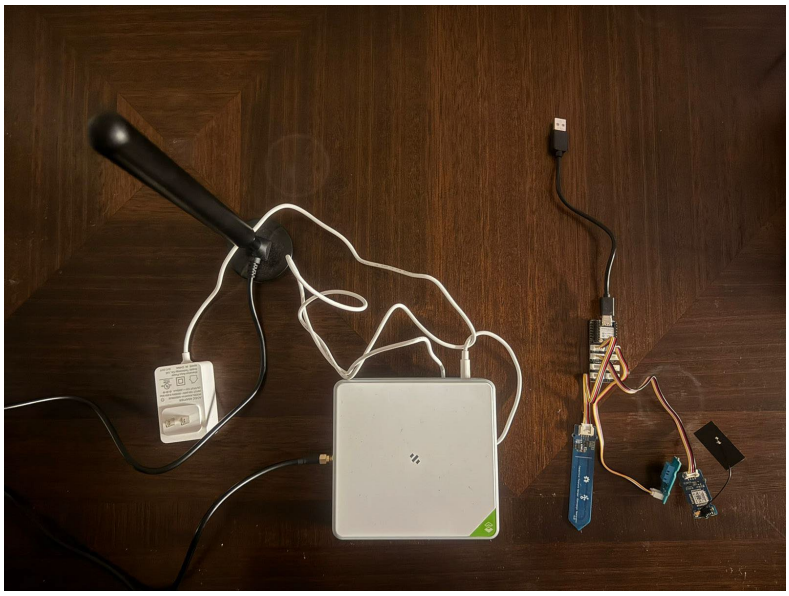

Figure 2: SenceCAP LoRa-LoRaWAN to Applications Hardware

3.2 Digital Forensic Investigation

The identification, preservation, analysis, and presentation of digital evidence kept on electronic devices or systems are all part of the field of digital forensics, a subfield of forensic science. It includes looking into digital artifacts to find out information about security lapses, cybercrimes, and other issues involving digital data. Experts in digital forensics retrieve and analyze data from networks, computers, mobile devices, and other electronic storage media using specific methods and instruments. Collecting evidence for use in incident response, court cases, or security investigations with the aim of attributing acts, reconstructing events, and assisting in decision-making is the aim of digital forensics (Damshenas 2025). The general framework of digital forensics is shown in Figure 3.

Figure 3: The general structure of Digital Forensics Investigation

3.2.1 Preservation

A controlled environment was established to maintain the integrity of the investigative process, and essential forensic tools like Forensic Toolkit (FTK) and Autopsy were procured for subsequent stages. The investigation proceeded with the acquisition of a forensic image of the computer that was connected to SenseCAP using FTK Imager. This step ensured the capture of all data stored on the device without altering its original content, and the integrity of the acquired image was verified through cryptographic hash functions. Subsequently, the acquired forensic image was ingested into Autopsy, an open-source digital forensic tool, for detailed examination.

3.2.2 Analyzing, investigation

Within Autopsy, a thorough analysis of the device's file system was conducted, delving into various artifacts, directories, and files stored on the device. System logs, configuration files, and other pertinent data were scrutinized to glean insights into the device's operation, configuration settings, and usage patterns. Special attention was paid to identifying any indications of security vulnerabilities, unauthorized access attempts, or anomalous activities that could pose risks to the device's security. Figure 4 shows the number of events by year.

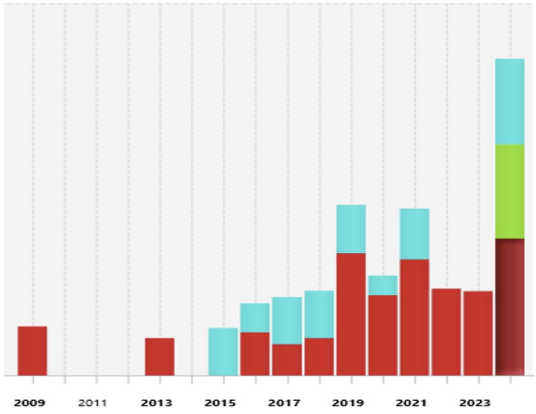

Figure 4: The number of Events (Logarithmic)

The methodology of this study involved several key steps to ensure a thorough forensic analysis of SenseCAP devices and their associated data. First, key forensic artifacts were extracted from the devices, including network communication logs, sensor data, firmware files, and system configuration parameters. This data was collected using forensic imaging tools to maintain integrity. The analysis began with a careful examination of timestamps, metadata, file attributes, and system logs to reconstruct the timeline of device operations. Communication logs were scrutinized for anomalies or unauthorized access, while sensor data was cross-verified against expected ranges to detect inconsistencies. Firmware files and system configurations were inspected for signs of tampering, such as unauthorized modifications or malicious injections. Additionally, frequency analysis was performed using Software-Defined Radio (SDR) to validate the integrity of LoRa communications, ensuring they fell within designated frequency bands and detecting any signs of tampering or interference.

3.2.3 Log files

000009.log and 000004.log contain logs related to interactions with the SenseCAP platform, specifically the SenseCAP Portal hosted at sensecap.seeed.cc. We believe these two logs are important to identify the user and associate the account with it. The log data analysis reveals pertinent insights into the operational dynamics of the SenseCAP gateway system. Through a systematic examination, key aspects such as gateway URL, login attempts, token generation, error handling, user interaction, device and gateway management, as well as IP address and user agent information, were scrutinized. Notably, the log indicates successful login attempts associated with a specific user identified by the email address "nss016@shsu.edu" and the corresponding user ID. Token generation and refresh token availability were observed, suggesting a secure authentication mechanism. Moreover, user interactions with chatbots on the SenseCAP website were

recorded, indicating user engagement for support or assistance purposes. Device and gateway management were also present, facilitating device registration and monitoring functionalities. Additionally, metadata such as IP address and user agent information provided insights into the user's browser environment. Overall, this investigation underscores the significance of log analysis in discerning system operations, identifying anomalies, and ensuring the integrity and security of the SenseCAP ecosystem.

- Gateway Information:
  - Gateway URL: https://sensecap.seeed.cc
  - Login Attempts:
    - sv0ccisLogin: true
    - sv0ccemail: nss016@shsu.edu
    - sv0ccnickname: nss016
    - sv0ccuser id: 435484262458960
    - sv0ccusernum: 435484262458960
  - Token Generation:
    - sv0cctoken: Token generated
    - sv0ccrefresh token: Refresh token available
  - Error Handling:
    - sv0ccisTokenError: No error reported
  - User Interaction: Messages exchanged with chatbots on the SenseCAP website, likely for assistance.
  - Device and Gateway Management:
    - sv0cctableVals: Contains information about gateway and device management, including device registration and last message time.

3.2.4 Chrome current tabs

Chrome Current Tabs artifacts provided consist of a series of URLs along with their corresponding last visited date and time and titles. These URLs represent various sections of the SenseCAP Portal and related web interfaces. The SenseCAP Portal, provided by Seeed Studio IIoT Solutions, serves as a comprehensive platform for device, data, and access key management. The records include different segments of the portal, such as the organization dashboard, security credentials, devices sensor node, and devices sensor node group. Additionally, there are entries for device development kits and multiple instances of the main dashboard. The SenseCAP LoRa Log and other administrative pages like the channel plan, system status, and device password management under the LuCI interface are also recorded. The visits are meticulously timestamped, all occurring on May 20, 2024, demonstrating a thorough exploration of the platform’s functionalities within a short timeframe. This detailed browsing history indicates an in-depth review of SenseCAP’s capabilities, likely for purposes of system management, data analysis, or software evaluation. Based on our investigation, we found:

- SenseCAP Portal by Seeed Studio IIoT Solutions:
  - URL: https://solution.seeedstudio.com/product/software-cloud-sensecap-portal/
  - Last Visited: 5/20/2024 4:17:16.937 AM
  - Title: SenseCAP Portal, for Device, Data, and Access

    Key Management - Seeed Studio IIoT Solutions
- Dashboard - SenseCAP CC Portal:
  - URL: https://sensecap.seeed.cc/portal/#/organization
  - Last Visited: 5/20/2024 4:23:26.765 AM

  - Title: Dashboard - SenseCAP CC Portal

- SenseCAP - Device Password - LuCI:
  - URL: https://607-771397f0x2dd9x11eex83c2xeb2cc4db137b-luci.sensecap-fleet.seeed.cc/cgi-bin/luci/admin/system/admin
  - Last Visited: 5/20/2024 4:22:32.156 AM
  - Title: SenseCAP - Device Password - LuCI
- SenseCAP - LoRa Log - LuCI:
  - URL: https://607-771397f0x2dd9x11eex83c2xeb2cc4db137b-luci.sensecap-fleet.seeed.cc/cgi-bin/luci/admin/system/admin
  - Last Visited: 5/20/2024 4:22:38.751 AM
  - Title: SenseCAP - LoRa Log – LuCI

The URL is complex and can be broken down to understand its various components. It begins with 'https://', indicating that it uses the secure HTTP protocol (HTTPS). The subdomain '607-771397f0x2dd9x11eex83c2xeb2cc4db137b- luci' appears to be a unique, auto-generated string, possibly assigned dynamically to represent a specific instance or session. The main domain, 'sensecap-fleet.seeed.cc ', shows that the service is hosted under the "seeed.cc" domain, which is associated with Seeed Studio, a platform for hardware innovation. The "sensecap-fleet" part indicates a service related to SenseCAP, Seeed Studio's brand for Industrial Internet of Things (IIoT) solutions. The path '/cgi-bin/luci/admin/lora/lora log' specifies the exact location of the resource on the server. This includes the '/cgi-bin' directory, which typically contains executable scripts, and '/luci', which likely refers to LuCI, a web interface for OpenWRT (an open-source router firmware). The '/admin/lora/lora log' part of the path shows that this resource is part of the administrative interface and is specifically for viewing LoRa (Long Range, a wireless communication technology) logs. This URL is thus accessing a particular administrative interface of the SenseCAP fleet management system, specifically targeting the LoRa log section. The complex subdomain string suggests a mechanism for session isolation or security, ensuring each user or session gets a unique and secure environment.

3.2.5 Chrome Fav Icons

Chrome FavIcons indicate that the user visited several SenseCAP-related URLs on 5/20/2024, within a close timeframe, suggesting a focused activity related to SenseCAP services. The URLs correspond to different facets of the SenseCAP ecosystem, including the main portal, specific product information, and administrative access points. The consistent timestamps and presence in the favicons database confirm these visits. The favicon URLs provide additional verification of the sites visited. This data helps build a timeline and context of the user's online behavior, potentially indicating an investigation or configuration activity related to SenseCAP services.

- Record 1:
  - Page URL: https://607-771397f0x2dd9x11eex83c2xeb2cc4db137b-luci.sensecap-fleet.seeed.cc/
  - Last Updated Date/Time: 5/20/2024 4:18:25 AM
  - Icon URL: https://607-771397f0x2dd9x11eex83c2xeb2cc4db137b-luci.sensecap-fleet.seeed.cc/luci-static/bootstrap/favicon.png
  - Location on Disk: Found in the user's Chrome browser favicons database, specifically within the file nvme0n1 Image.E01 - Partition 3 (Microsoft NTFS, 117.21 GB)\Users\Chuck\AppData\Local \ Google\Chrome\User Data\Default\Favicons, under the tables favicons, icon_mapping, and favicon_bitmaps.
- Record 2:
  - Page URL: https://solution.seeedstudio.com/product/software-cloud-sensecap-portal/
  - Last Updated Date/Time: 5/20/2024 4:17:21 AM

- Icon URL: https://sensecap-solution-upload.cdn.seeed.cn/cc/2022/03/cdc92bb1863427e6bfd2a378051806d1.png
- Location on Disk: Similarly located within the same favicons database as Record 1.

3.2.6 Identifiers, passwords and tokens

The investigation has identified a wireless network connection event to the SSID SenseCAP 1C63B7, logged in the Windows Event Logs under networking events. This information provides valuable insight into the connectivity history of the device in question. The event logs captured in the Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx file contain detailed records of network connections, including timestamps, connection statuses, and potentially even the hardware addresses of the connected devices.

- The SSID SenseCAP 1C63B7 can be used to infer the geographical location or the specific environment (e.g., a corporate office, laboratory, or field site) where the device was used.
- This can help in establishing the movement and usage patterns of the device over time.

The investigation has successfully identified user credentials stored in Google Chrome browser's login data. The encrypted format of the password/token suggests that while the credentials are present, they are protected and not directly accessible without decryption. The exact location of the artifact on the disk image has been noted, which is crucial for further analysis or for presenting findings in a legal context. The presence of these credentials in the Chrome logins database implies that the user nss016@shsu.edu has accessed the SenseCAP portal from the device associated with the disk image. This information could be pivotal in tracing user activities and understanding the scope of access and interactions with the SenseCAP platform.

3.2.7 Frequency analysis

At a crime scene, it may be observed that there are various electronic devices present. While the status of these devices—whether they are powered on or off—can be deduced by checking their LEDs, it is not always possible to determine if any data transmission is occurring. During the initial investigation, when digital devices are identified, and their labels are examined, it is possible to recognize what type of device they are and gain a general understanding of their functions. In this study, we aimed to identify whether data transmission is occurring in a properly functioning system using Software-Defined Radio (SDR).

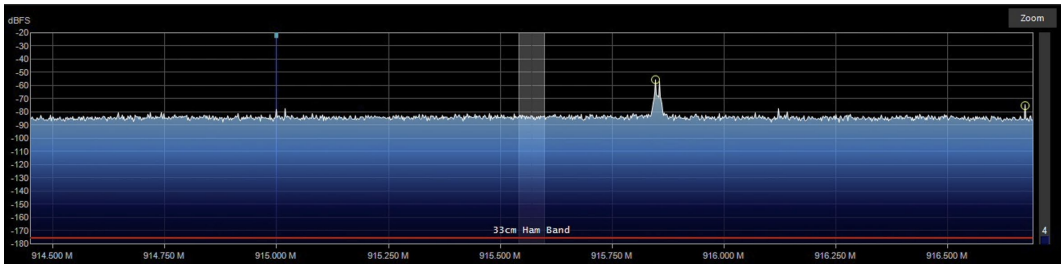

Figure 5: Frequency Spectrum

Figure 5 represents the frequency spectrum, showing signal activity between approximately 914.6 MHz and 916.0 MHz. The spikes in the spectrum indicate active transmissions, likely from a LoRa device or other radio frequency emitters operating in this range. The most notable feature in this spectrum is a clear signal spike around 915.750 MHz, suggesting active transmission. This could be a LoRa or other IoT device operating within this ISM band. The background noise floor is relatively stable, but the spike indicates a data transmission or broadcast happening at that frequency.

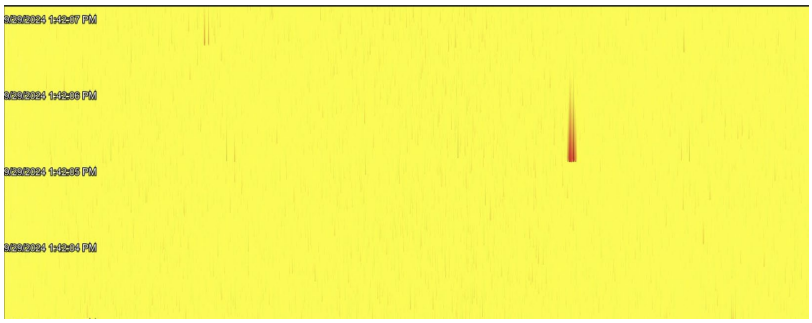

Figure 6. Waterfall plot with date and time information

Figure 6 shows a time-based visualization of frequency activity. Each horizontal line represents the signal strength at a particular moment, with brighter colors representing stronger signals. The red trace in the middle is a strong signal that has been consistently active over time, indicating ongoing communication or transmission. The timestamps on the left (1:42:05 PM, 1:42:06 PM, etc.) represent when these signals were captured, with each line representing a snapshot at a specific moment in time. To better detect the signal, the Waterfall display has been slowed down using the W-Delay feature. In this analysis, the SDR is tuned to the ISM band, commonly used for LoRa and other IoT communications, like those in the SenseCAP starter kit. The consistent spike and red signal in the waterfall plot indicate the presence of a transmission, which could be the SenseCAP gateway or sensor nodes sending data. The analysis can help determine if the system is actively transmitting data, and further investigation can reveal details about the type of communication (e.g., packet size, modulation type). The stable noise floor indicates a relatively clean spectrum with minimal interference, which is ideal for data transmission in IoT applications.

This setup is useful in detecting anomalies in transmissions, analyzing the quality of the communication, and confirming whether the data transfer is occurring between devices in real-time.

4. Results

The Autopsy analysis of the device's file system focused on identifying security vulnerabilities, unauthorized access, and anomalies through a detailed review of logs, configuration files, and artifacts. Key findings included the detection of device interactions with the SenseCAP Portal through log files such as "000009.log" and "000004.log." These logs revealed user activities, login attempts, and token generation for "nss016@shsu.edu." Examination of Google Chrome's browsing history confirmed visits to key sections of the SenseCAP Portal, including device management and security settings. Chrome FavIcons analysis supported these findings, showing a consistent timeline of SenseCAP-related activity. Additionally, the device connected to the wireless network SenseCAP 1C63B7, as recorded in the Windows Event Logs. User credentials were found encrypted in the Chrome login data, further linking the user to the platform. Frequency forensics using Software-Defined Radio (SDR) detected active transmissions in the 914.6 MHz to 916.0 MHz range, with a notable signal at 915.750 MHz, indicating data exchanges likely from a LoRa device. This spectrum analysis confirmed the device's operational communication, adding critical context to the investigation’s findings. This analysis provided a crucial layer of insight into the operational status of the device's communication systems. The frequency spectrum and waterfall plot visualizations offered a time-based view of the signal activity, with stronger signals highlighted over time, thereby confirming ongoing data transmissions. These findings were integral to the overall investigation, providing a thorough understanding of the device’s data flow and network interactions.

5. Conclusion and Future Work

In conclusion, our forensic investigation of SenseCAP devices has uncovered valuable insights into their operational dynamics. Through artifact analysis, log examination, and frequency analysis, we identified user interactions, device configurations, and possible threats, emphasizing the critical role of digital forensics in safeguarding the integrity and security of IoT deployments. However, several limitations must be acknowledged. Our study focused on specific devices, meaning that our findings may not be easily generalized to other SenceCAP IoT devices. Additionally, the rapidly evolving nature of IoT ecosystems presents ongoing challenges in addressing emerging technologies and vulnerabilities. Despite these limitations, this research provides a foundation for future investigations, particularly in enhancing the scalability and efficiency of forensic tools. Integrating machine learning and artificial intelligence could automate analysis processes and

improve threat detection. Moreover, the development of standardized protocols and collaborative frameworks will be essential to ensure consistency and interoperability across diverse IoT platforms. Future work must address challenges such as privacy, data integrity, and interoperability, bridging the gap between theory and practice to strengthen the security and resilience of IoT ecosystems in our increasingly connected world.

References

Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J. and Watteyne, T. (2017) 'Understanding the limits of LoRaWAN', *IEEE Communications Magazine*, 55(9), pp. 34–40.

Aernouts, M., Berkvens, R., Van Vlaenderen, K. and Weyn, M. (2018) 'Sigfox and LoRaWAN datasets for fingerprint localization in large urban and rural areas', *Data*, 3(2), p. 13.

Benaissa, S., Plets, D., Tanghe, E., Trogh, J., Martens, L., Vandaele, L., Verloock, L., Tuyttens, F.A., Sonck, B. and Joseph, W. (2017) 'Internet of animals: Characterisation of LoRa sub-GHz off-body wireless channel in dairy barns', *Electronics Letters*, 53(18), pp. 1281–1283.

Catherwood, P.A., Steele, D., Little, M., Mccomb, S. and McLaughlin, J. (2018) 'A community-based IoT personalized wireless healthcare solution trial', *IEEE Journal of Translational Engineering in Health and Medicine*, 6, pp. 1–13.

Damshenas, M., Dehghantanha, A. and Mahmoud, R. (2014) 'A survey on digital forensics trends', *International Journal of Cyber-Security and Digital Forensics*, 3(4), pp. 209–235.

De Castro Tomé, M., Nardelli, P.H. and Alves, H. (2018) 'Long-range low-power wireless networks and sampling strategies in electricity metering', *IEEE Transactions on Industrial Electronics*, 66(2), pp. 1629–1637.

Del Campo, G., Gomez, I., Sierra, S.C., Martinez, R. and Santamaria, A. (2018) 'Power distribution monitoring using LoRa: Coverage analysis in suburban areas', in *EWSN*, pp. 233–238.

Hildayanti, N. and Riadi, I. (2019) 'Forensics analysis of router on computer networks using live forensics method', *International Journal of Cyber-Security and Digital Forensics*, 8, pp. 74–81.

Ilie-Ablachim, D., Pătru, G.C., Florea, I.-M. and Rosner, D. (2016) 'Monitoring device for culture substrate growth parameters for precision agriculture: Acronym: Monisen', in *15th RoEduNet Conference: Networking in Education and Research*. IEEE, pp. 1–7.

Jawad, H.M., Nordin, R., Gharghan, S.K., Jawad, A.M. and Ismail, M. (2017) 'Energy-efficient wireless sensor networks for precision agriculture: A review', *Sensors*, 17(8), p. 1781.

Lee, H.-C. and Ke, K.-H. (2018) 'Monitoring of large-area IoT sensors using a LoRa wireless mesh network system: Design and evaluation', *IEEE Transactions on Instrumentation and Measurement*, 67(9), pp. 2177–2187.

Nawaf, M. (n.d.) 'Router forensics: Navigating the digital crossroads'. Available at: AEI EWAPublishing (Accessed: 15 October 2024).

Paolone, G., Iachetti, D., Paesani, R., Pilotti, F., Marinelli, M. and Di Felice, P. (2022) 'A holistic overview of the internet of things ecosystem', *IoT*, 3(4), pp. 398–434.

Pasolini, G., Buratti, C., Feltrin, L., Zabini, F., De Castro, C., Verdone, R. and Andrisano, O. (2018) 'Smart city pilot projects using LoRa and IEEE802.15.4 technologies', *Sensors*, 18(4), p. 1118.

Petäjäjärvi, J., Mikhaylov, K., Yasmin, R., Hämäläinen, M. and Iinatti, J. (2017) 'Evaluation of LoRa LPWAN technology for indoor remote health and wellbeing monitoring', *International Journal of Wireless Information Networks*, 24, pp. 153–165.

Podevijn, N., Plets, D., Trogh, J., Martens, L., Suanet, P., Hendrikse, K. and Joseph, W. (2018) 'TDOA-based outdoor positioning with tracking algorithm in a public LoRa network', *Wireless Communications and Mobile Computing*, pp. 1–9.

Rizzi, M., Ferrari, P., Flammini, A. and Sisinni, E. (2017) 'Evaluation of the IoT LoRaWAN solution for distributed measurement applications', *IEEE Transactions on Instrumentation and Measurement*, 66(12), pp. 3340–3349.

Sartori, D. and Brunelli, D. (2016) 'A smart sensor for precision agriculture powered by microbial fuel cells', in *IEEE Sensors Applications Symposium (SAS)*. IEEE, pp. 1–6.

Seeed Studio (2023) 'SenseCAP M2 multi-platform LoRaWAN indoor gateway (SX1302) - US915'. Available at: Seeed Studio (Accessed: 15 October 2024).

Senol, N.S. and Rasheed, A. (2023) 'A testbed for LoRa wireless communication between IoT devices', in *11th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1–6.

Shalaginov, A., Iqbal, A. and Olegård, J. (2020) 'IoT digital forensics readiness in the edge: A roadmap for acquiring digital evidence from intelligent smart applications', in Katangur, A., Lin, S.-C., Wei, J., Yang, S. and Zhang, L.-J. (eds.) *Edge Computing – EDGE 2020*. Cham: Springer International Publishing, pp. 1–17.

Sharma, V., You, I., Pau, G., Collotta, M., Lim, J.D. and Kim, J.N. (2018) 'LoRaWAN-based energy-efficient surveillance by drones for intelligent transportation systems', *Energies*, 11(3), p. 573.

Varsier, N. and Schwoerer, J. (2017) 'Capacity limits of LoRaWAN technology for smart metering applications', in *IEEE International Conference on Communications (ICC)*. IEEE, pp. 1–6.

Wixted, A.J., Kinnaird, P., Larijani, H., Tait, A., Ahmadinia, A. and Strachan, N. (2016) 'Evaluation of LoRa and LoRaWAN for wireless sensor networks', in *IEEE Sensors*. IEEE, pp. 1–3.

Wiles, J. and Reyes, A. (2007) 'Router Forensics and Network Forensics', in *The Best Damn Cybercrime and Digital Forensics Book Period*, pp. 553–567.