# Article information:

IoT forensic challenges and opportunities for digital traces - ScienceDirect
<https://www.sciencedirect.com/science/article/pii/S1742287619300222>

# Article summary:

1. The growth of the Internet-of-Things (IoT) presents challenges and opportunities for investigators of cyberattacks and physical assaults.

2. IoT devices generate valuable digital traces that can be used as evidence, but managing the quantity and variety of data is a challenge.

3. A methodology in six steps was developed to study IoT devices, including preliminary analysis, testbed setup, network analysis, smartphone application analysis, vulnerability analysis, and physical analysis. Traces can be extracted from multiple locations including device memory, network traffic, and smartphone applications.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article "IoT forensic challenges and opportunities for digital traces" discusses the growing use of Internet-of-Things (IoT) devices in smarthomes and other environments, and the challenges and opportunities they present for investigators of crimes. The article highlights the potential value of IoT devices as digital witnesses, capturing traces of activities that can be used in investigations. However, it also notes the challenges associated with managing the quantity of data generated by these devices, as well as their distributed nature and heterogeneity of protocols used.

The article presents a methodology for studying IoT devices that involves preliminary analysis, testbed setup, network analysis, smartphone application analysis, vulnerability analysis, and physical analysis. The authors argue that this approach extends existing methods for forensic processing of mobile devices to deal with new types of traces.

While the article provides useful insights into the potential value of IoT devices as sources of evidence in investigations, it has some limitations. For example, it focuses primarily on smarthomes and other consumer-oriented environments rather than industrial IoT applications. Additionally, while it acknowledges the need for legal authorization to obtain data from cloud service providers related to IoT devices, it does not explore the potential risks associated with accessing such data without proper authorization.

Furthermore, while the article notes that vulnerabilities were discovered on two devices during their study and reported to vendors, it does not provide details about these vulnerabilities or how they were addressed. This lack of information makes it difficult to assess the significance of these vulnerabilities or their potential impact on users.

Overall, while "IoT forensic challenges and opportunities for digital traces" provides valuable insights into the potential value of IoT devices as sources of evidence in investigations, its focus on consumer-oriented environments limits its applicability to other contexts. Additionally, more information is needed about vulnerabilities discovered during their study to fully assess their significance.

# Topics for further research:

* Industrial IoT applications and forensic challenges
* Legal authorization for accessing cloud data related to IoT devices
* Risks associated with unauthorized access to IoT device data
* Vulnerabilities discovered in IoT devices and their impact on users
* Forensic processing of IoT devices in non-consumer environments
* Best practices for securing IoT devices and data in investigations

# Report location:

<https://www.fullpicture.app/item/40b1d7ad67aa6bf1e0375b80ec66d31a>