1st Workshop on Digital Forensics (WDF26)*

Silvia Lucia Sanna[1,*,†], Sebastiano Battiato[2,†] and Luca Cadonici[3,†]

[1]University of Cagliari, Italy
[2]University of Catania, Italy
[3]European Forensics Institute

Abstract

This workshop provides a forum for digital forensic consultants (CTU/CTP), industry, law enforcement, judiciary, and academia to discuss current challenges and future directions in Digital Forensics. Unlike existing events with a mainly academic focus, it emphasizes practical issues and solutions relevant to real investigations. The program will explore limitations of current forensic tools and methodologies in areas such as mobile forensics, memory and computer acquisition, IoT, and open-source tools. Emerging challenges will also be addressed, including the forensic analysis of AI-generated content (e.g., deepfakes) and the application of AI techniques to support investigations. Both technical and legal perspectives will be considered to ensure solutions are effective and admissible in court. The workshop will include introductory talks, thematic discussions moderated among professionals, and paper presentations. Submissions are encouraged on novel methodologies, guidelines, and protocols for the forensic analysis of mobile, IoT, and AI-related data.

Keywords

Digital Forensics, Mobile Forensics, Emergent Forensics, AI Forensics, genAI-data Forensics

1. Preface

Digital forensics is the science of recovering information from any technological device. It is currently used in legal proceedings both when a device is involved as the main actor (e.g., cybercrime or accident) and in traditional cases where a device may contain information useful to the case under investigation. Nowadays, electronic devices are an integral part of all our lives and for this reason they often contain data that is fundamental to the resolution of court cases. First and foremost are mobile devices (smartphones) that can prove activities carried out, places visited, messages sent/received. At the same time, these devices must guarantee user privacy and security. Therefore, a combination of cybersecurity, data protection, and forensic analysis is essential. Secondly, there are desktop devices such as personal computers, servers, and industrial devices, which are analyzed in both industrial and private settings. In fact, the analysis of industrial devices often involves the use of specific techniques based on the proprietary system under examination, which are not often universal or easily adaptable and generalizable.

An emerging area of analysis is data created by Artificial Intelligence (AI), such as deepfake audio, video, and images. Such multimedia content, if created ad hoc, can accuse a person of a crime that was not actually committed. It is therefore essential to integrate forensic analysis techniques with these new types of data in order to prove whether the multimedia content under examination is genuine or created by AI algorithms. Not only that, but AI can be applied in various scenarios to assist analysts. Several industrial tools already apply it in data categorization. Due to the development of evasive techniques (adversarial attacks), it is essential to apply these techniques safely, also considering the legal validity of the automatic algorithm. At present, there is no protocol or methodology regulating the analysis of

1st Workshop on Digital Forensics (WDF 2026), co-located with the 2nd Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), February 09–13, 2026, Cagliari, Italy

*Corresponding author.
†These authors contributed equally.
silvial.sanna@unica.it (S. L. Sanna); sebastiano.battiato@unict.it (S. Battiato); luca.cadonici@isf.college (L. Cadonici)
https://kmitd.github.io/ilaria/ (S. Battiato); https://www.novaeraforensics.it/luca-cadonici/ (L. Cadonici)
0009-0002-8269-9777 (S. L. Sanna); 0000-0001-6127-2470 (S. Battiato)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).



published 2026-11-14

CEUR-WS.org/Vol-4329/preface-wdf26.pdf

such data. Therefore, the call for papers for this workshop will focus specifically on proposing new methodologies, guidelines, definitions, and protocols for the effective analysis of emerging technologies, with a focus on mobile devices, IoT, and the use of AI (both AI-generated content analysis and analysis using AI techniques). These issues must be addressed and resolved not only from a technical but also from a legal perspective.

The aim of the workshop is to bring together expert forensic consultants (CTU/CTP) with companies and law enforcement agencies to discuss current issues in digital forensics, debate the current limitations of tools and techniques, and identify effective solutions. Thanks to the collaboration of both industrial and academic research, it is necessary to identify possible solutions to these limitations from both a technical and legal point of view, as well as the future directions of digital forensics, such as the use of artificial intelligence or emerging branches such as IoT forensics. This workshop proposes a meeting point between various private professionals (CTUs, CTPs) as well as companies, criminologists, law enforcement agencies, and judicial authorities to discuss the current problems of digital forensics from both a technical and legal point of view (thus including not only technical personnel but also lawyers, judges, etc.). Subsequently, it is essential to understand how research can help overcome these problems and limitations. It is also essential to discuss new frontiers in digital forensics, such as the use of artificial intelligence and forensic analysis of the IoT and mobile devices, starting from the current state of affairs and considering possible future directions in terms of new legislation, technological updates, and security patches. The workshop received seven paper submissions. Each submission was evaluated by at least three members of the Program Committee through a peer-review process. Following the review process, four papers were accepted for presentation at the workshop and inclusion in the proceedings. The paper submission deadline was December 28, 2025. The accepted papers were notified on January 16, 2026. The camera-ready submission deadline was on February 28, 2026. The workshop took place on February 9, 2026.

2. Keynote

The workshop included three keynote speeches, one delivered by each of the three organizers:

- Sebastiano Battiato: *Media Authentication in Generative AI era*
- Luca Cadonici: *Passkeys-Over-Passwords: Improving Resistance to Phishing Attacks in Mobile Security*
- Silvia Lucia Sanna: *Towards AI in Digital Forensics: a mobile perspective*

3. Program Committee

- Fausto Galvan, University of Udine
- Marco Fontani, Amped Software
- Paolo Dal Checco, University of Turin
- Michele Ferrazzano, University of Modena e Reggio Emilia
- Andrea Oliveri, Eurecom

4. Acknowledgments

This work was partially supported by Project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

Declaration on Generative AI

During the preparation of this work, the authors used Grammarly for grammar and spelling check. The authors reviewed and edited the content, taking full responsibility for the publication's content.