# DIFPILOT

Leveraging Large Language Models to Automate and Enhance Digital Forensics Workflows

| | | | |
|---|---|---|---|
| **Programm / Ausschreibung** | KS 24/26, KS 24/26, Bridge 2024/02 | **Status** | laufend |
| **Projektstart** | 01.01.2026 | **Projektende** | 30.06.2028 |
| **Zeitraum** | 2026 - 2028 | **Projektlaufzeit** | 30 Monate |
| **Keywords** | LLM, Digital Forensics | | |

## Projektbeschreibung

Mit der zunehmenden Komplexität digitaler Ermittlungen stoßen traditionelle manuelle forensische Werkzeuge an ihre Grenzen. Das enorme Datenvolumen und die Verflechtung von Fällen machen die Hinzunahme weiterer personeller Ressourcen unpraktikabel. Fortschritte bei großen Sprachmodellen (LLMs), wie beispielsweise Microsofts Co-Pilot, bieten vielversprechende Lösungen, indem sie die Automatisierung von Code- und Arbeitsabläufen ermöglichen und so die Effizienz und Wirtschaftlichkeit der digitalen Forensik steigern.

Obwohl LLMs im Bereich der Softwareentwicklung erfolgreich eingesetzt werden, wurden sie bisher nicht systematisch an die spezifischen Herausforderungen der digitalen Forensik angepasst – insbesondere in Bezug auf die Automatisierung von Arbeitsabläufen und die Interpretation von Ergebnissen forensischer Analysetools. Diese Lücke bietet die Chance, digitale Ermittlungen grundlegend zu verbessern.

Das DIFPILOT-Projekt zielt darauf ab, diese Lücke zu schließen, indem es einen neuartigen Ansatz entwickelt und evaluiert, um digitale forensische Ermittler bei der Automatisierung von Arbeitsabläufen und der Analyse von Daten mithilfe von LLMs zu unterstützen. Das Projekt wird (1) bestehende forensische Prozesse in zwei spezifischen Anwendungsfällen systematisch untersuchen und bewerten, (2) algorithmische Methoden und Modelle entwickeln, um die Erstellung und Interpretation forensischer Arbeitsabläufe zu erleichtern, und (3) eine kontrollierte Laborumgebung einrichten, um die Effizienz und Wirksamkeit der vorgeschlagenen Lösungen zu evaluieren.

Die Neuheit von DIFPILOT liegt in der gezielten Anwendung von LLMs auf die spezifischen Herausforderungen der digitalen Forensik, wodurch sowohl technologische Innovationen als auch praktische Relevanz geboten werden. Die Forschungsergebnisse werden in hochrangigen wissenschaftlichen Publikationen veröffentlicht und innerhalb von 3–5 Jahren nach Projektabschluss für die kommerzielle Verwertung durch den Industriepartner aufbereitet.

## Abstract

As digital investigations become increasingly complex, traditional manual forensic tools struggle to scale effectively. The vast volume of data and the interconnectedness of cases make adding human resources impractical. Recent advancements

in Large Language Models (LLMs), such as Microsoft’s Co-Pilot, offer promising solutions by enabling coding and workflow automation, thereby enhancing the efficiency and affordability of digital forensics.

Despite their success in software development, LLMs have not been systematically adapted to the specific challenges of digital forensics, particularly in automating workflows and interpreting results from forensic analysis tools. This gap presents an opportunity to revolutionize digital forensic investigations.

The DIFPILOT project aims to bridge this gap by developing and evaluating a novel approach to assist digital forensic investigators in automating workflows and analyzing data using LLMs. The project will (1) systematically study and assess existing forensic processes in two specific use cases, (2) develop algorithmic methods and models to support the creation and interpretation of forensic workflows, and (3) establish a controlled laboratory environment to evaluate the efficiency and effectiveness of the proposed solutions.

The novelty of DIFPILOT lies in its targeted application of LLMs to the unique challenges of digital forensics, offering both technical innovation and practical relevance. Research outcomes will be disseminated through high-quality scientific publications and prepared for commercial exploitation by the project’s industry partner within 3–5 years of completion.

## Projektkoordinator

- Complexity Science Hub Vienna CSH - Verein zur Förderung wissenschaftlicher Forschung im Bereich komplexer Systeme

## Projektpartner

- Iknaio Cryptoasset Analytics GmbH