Where is the Potential for Large Language Models in Digital Forensic Investigation?

Akila Wickramasekara, Mark Scanlon

Forensics and Security Research Group, University College Dublin, Ireland
(akila.wickramasekara@ucdconnect.ie, mark.scanlon@ucd.ie)

ABSTRACT

In an era marked by a significant rise in various crimes, the integration of Large Language Models (LLMs) in digital forensic investigations presents a promising frontier [1]. This study explores the potential of LLMs to revolutionize digital forensics, addressing the growing challenges faced in the analysis of vast amounts of evidence and the need for specialized technical expertise. The adoption of LLMs promises to potentially enhance the efficiency of investigations across all types of crimes, offering improved evidence traceability and alleviating the technical and judicial barriers faced by law enforcement entities. By streamlining evidence analysis and adapting quickly to new tools and systems, LLMs could potentially mitigate the issues of time consumption, resource allocation, and investigator frustration, thereby reducing the backlog of digital forensic cases [1]. This exploration into LLMs' applicability in digital forensics aims to illuminate their role in transforming investigative methodologies and contributing to more effective and efficient crime-solving approaches.

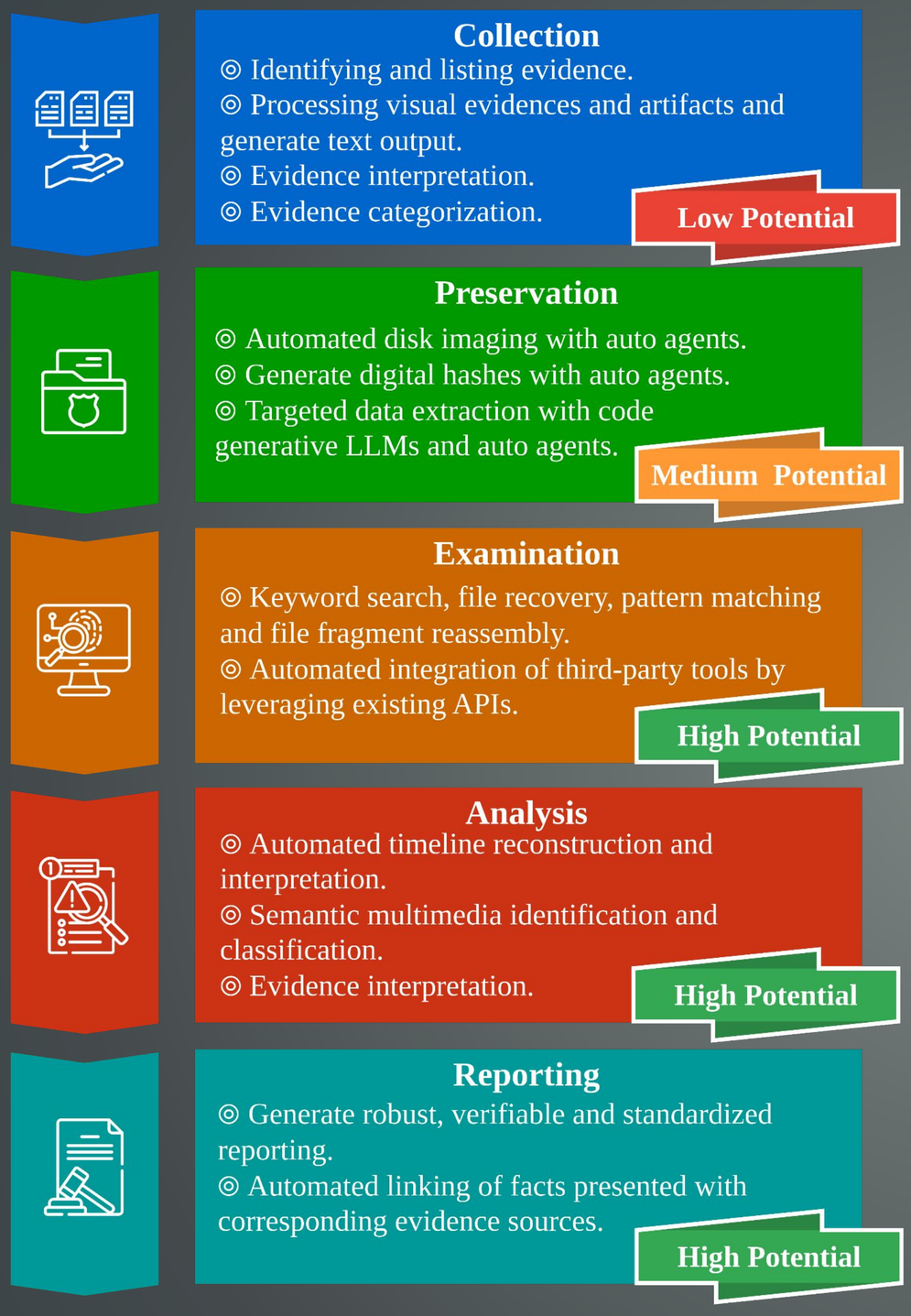

Figure 1. Potential of LLMs in the DF Process Model Phases

POTENTIAL IN DIGITAL FORENSICS

The Digital Forensic (DF) process model is structured into five principal phases: Collection and Seizure, Preservation, Examination, Analysis, and Reporting. Within these, the Examination phase further subdivides into sub-phases, including Recovery, Harvesting, Reduction, and Classification. Given the expansive capabilities of LLMs, there is significant potential for applying LLMs across all these phases in the DF process, enhancing efficiency and effectiveness in each step.
To assess the potential for applying LLMs in each phase of the DF process, a criterion defining the level of potential has been established as follows:

- Low Potential:
  - Requires a high level of human expert knowledge.
  - Often requires identifying/handling physical evidence.
  - Minimal or no scope for automation.
- Medium Potential:
  - Necessitates human expert knowledge, though it is not a critical component.
  - Focuses on handling digital evidence, with minimal involvement of physical evidence.
  - Automation is feasible and can be implemented.
- High Potential:
  - Demands minimal human expert knowledge.
  - Exclusively deals with digital evidence.
  - Fully amenable to automation.

Figure 1 illustrates the potential of employing LLMs in each phase of the DF process, using the defined criterion. It highlights the tasks within each phase where LLMs can be particularly beneficial. This depiction aids in understanding where LLMs can be most effectively integrated into the DF workflow.

CAPABILITIES OF LARGE LANGUAGE MODELS

Figure 2 highlights the evolution of LLMs across various fields, notably in coding and image processing. Fine-tuned LLMs excel in converting written instructions into executable code. Multimodal Large Language Models (MLLMs) are particularly effective in interpreting images and videos, aiding significantly in tasks like crime scene analysis and detailed video footage examination [2,3,4].

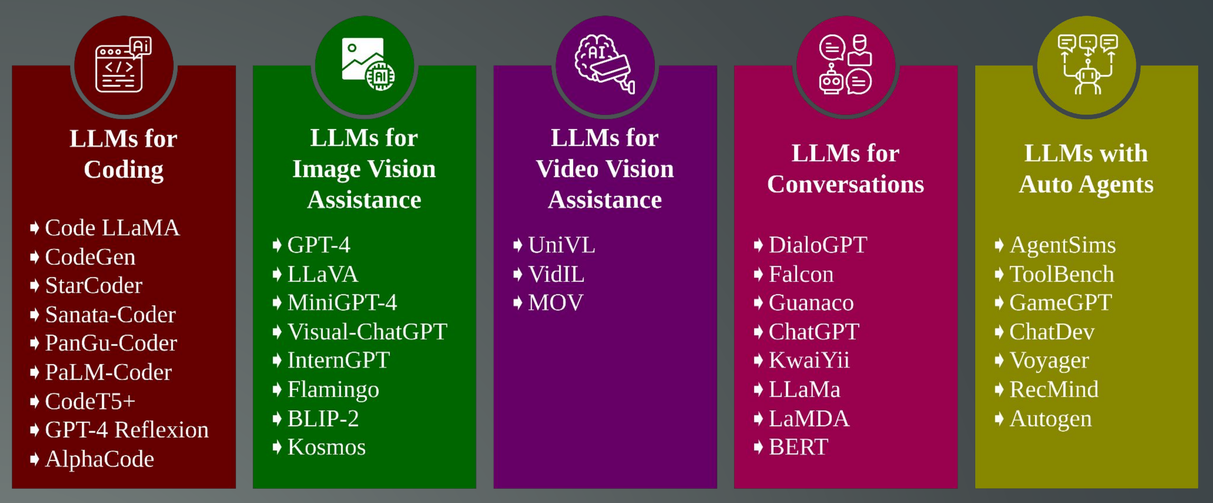

Figure 2. Example Fine-Tuned, Task-Specific LLMs.

LLMs ASSISTING IN DIGITAL FORENSIC INVESTIGATIONS

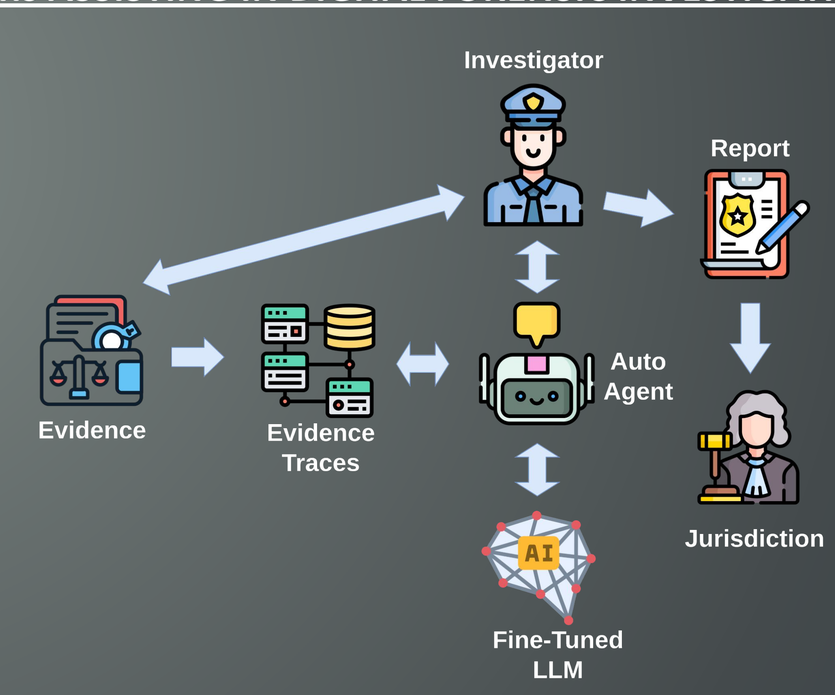

Figure 3. High Level Architecture of Fine-Tuned LLM-Aided DF Investigation.

The use of tailored LLMs and Artificial Intelligence (AI) Auto Agents in Digital Forensics, as shown in Figure 3, presents a significant opportunity to enhance the field's efficiency and effectiveness. Integrating LLMs into Digital Forensics as a Service (DFaaS) platforms, such as Hansken, enables more effective examination and analysis of evidence traces [5]. DF investigators can harness natural language inputs to efficiently extract information from these traces, and AI-driven auto agents can be employed to analyze evidence and develop incident hypotheses. The use of MLLMs and Augmented Large Language Models (ALLMs) is particularly promising for boosting automated investigative capabilities.

While the reporting phase greatly benefits from the precision and standardization offered by LLMs, reducing language errors and improving report accuracy, it's important to be mindful of the limitations of LLMs in phases like collection and preservation. These early stages of the DF process are critical, and maintaining a balance between human oversight and AI automation is essential for accurate and reliable outcomes. The potential for manpower and cost reduction through LLM automation is significant, but the integration of human expertise remains a crucial aspect of the process. Future research directions may explore the role of LLMs and general AI in enhancing decision-making within the realm of DF, further pushing the boundaries of technology in this field.

REFERENCES

1. M. Scanlon et al. ***ChatGPT for Digital Forensic Investigation: The Good, The Bad, and The Unknown***, Forensic Science International: Digital Investigation 46S, 301609, Proceedings of the Third Annual DFRWS APAC, ISSN 2666-2825. 2023.

2. R. Li et al. ***StarCoder: May the source be with you!*** arXiv preprint arXiv:2305.06161. 2023.

3. Y. Li et al. ***Competition-level code generation with alphacode.*** Science 378, 6624, 1092–1097. 2022.

4. F. Christopoulou et al. ***Pangu-coder: Program synthesis with function-level language modeling***. arXiv preprint arXiv:2207.11280. 2022.

5. H.M.A. van Beek et al. ***Digital Forensics as a Service: Game on.*** Digital Investigation 15, 20–38. Special Issue: Big Data and Intelligent Data Analysis. 2015.