



Course Project

Large Language Models and Digital Forensics: A Survey

Cybercrime Investigation and Digital Evidence

MSCS 630 - Fall 2026

Dr. ElMouatez Billah Karbab

1 PROJECT OVERVIEW

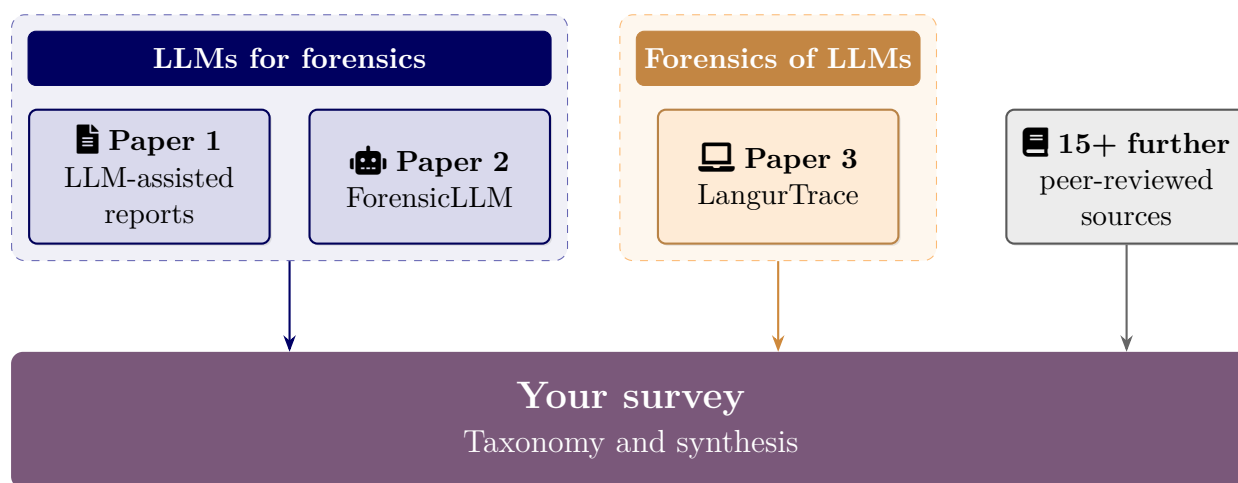


Figure 1: **Project overview.** The three core papers cover two directions: LLMs used as tools for forensics, and forensic analysis of LLM applications. Your survey extends them with further literature and synthesizes both.

Large Language Models (LLMs) now reach digital forensics from two sides. Investigators try them as tools, for example to draft reports or to answer domain questions. At the same time, suspects and victims run LLM applications on their own machines, so these applications become a new source of evidence.

YOUR MISSION: You will write an **individual survey paper** on large language models and digital forensics. The project has no hands-on part. You start from three core papers,

extend them with the wider literature, organize the field into a clear taxonomy, and analyze critically what the research shows and what remains open.

2 CORE PAPERS

PAPER 1: LLM-ASSISTED REPORT WRITING. Michelet and Breitingner [2] ask to what extent LLMs such as ChatGPT and Llama, including locally run models, can assist the writing of forensic reports. They first examine forensic reports to find their general structure, then use a case study to evaluate the strengths and limitations of LLMs for generating each part of a report. They conclude that, combined with thorough proofreading and correction, LLMs may assist practitioners in report writing but cannot replace them at this point. Open access: <https://www.sciencedirect.com/science/article/pii/S2666281723002020>

PAPER 2: A LOCAL MODEL SPECIALIZED FOR FORENSICS. Sharma et al. [3] note that general LLMs lack specialization for digital forensics, that cloud APIs and high-end hardware limit their use, and that hallucinations threaten forensic use. They introduce ForensicLLM, a 4-bit quantized LLaMA-3.1-8B model fine-tuned on question-and-answer samples drawn from digital forensics research articles and curated digital artifacts. In their evaluation ForensicLLM outperformed both the base model and a Retrieval Augmented Generation (RAG) model, and it attributed sources correctly 86.6% of the time. A survey of digital forensics professionals also found clear improvements of both ForensicLLM and RAG over the base model. Open access: <https://www.sciencedirect.com/science/article/pii/S2666281725000113>

PAPER 3: FORENSIC ANALYSIS OF LOCAL LLM APPLICATIONS. Jeong et al. [1] take the reverse direction and treat LLM applications as evidence sources. They propose a framework that divides LLM application environments into backend runtime, client interface and integrated platform components. Through experiments on representative applications they identify and classify artifacts such as chat records, uploaded files, generated files and model setup histories, and they release LangurTrace, an open-source tool that automates the collection and analysis of these artifacts. Open access: <https://www.sciencedirect.com/science/article/pii/S2666281725001271>

3 WHAT THE SURVEY MUST COVER

Your paper must address at least the following themes. Each theme should draw on the core papers and on the further literature you find.

1. **Taxonomy.** A clear classification of the field into the two directions, LLMs *for* forensics and forensics *of* LLMs, with sub-categories that you define and justify.

2. **Report writing and its risks.** The use of LLMs in forensic reporting and its evidentiary and legal risks: hallucination, verification of every generated statement, and disclosure of AI use to courts and other parties.
3. **Local versus cloud models.** Privacy of case data, confidentiality, and the effect on chain of custody when evidence or case details leave the forensic workstation.
4. **Fine-tuning versus RAG.** How each approach specializes a model for forensics, how they compare, and why source attribution matters for forensic work.
5. **Artifacts of local LLM applications.** What traces these applications leave, where they are stored, and how investigators can collect and interpret them.
6. **Open problems.** Gaps in evaluation, datasets, reproducibility, legal admissibility and tool support, with concrete directions for future research.

4 EXTENDING THE LITERATURE

The three core papers are a starting point, not the whole survey.

- Cite **at least 15 further peer-reviewed sources** (journal articles and conference papers). Preprints, blogs and vendor pages may support your argument but do not count toward the 15.
- Use **backward search** (the references of the three core papers) and **forward search** (later papers that cite them, for example through Google Scholar or Semantic Scholar).
- Good venues to search include the DFRWS conferences and *Forensic Science International: Digital Investigation*.

5 DELIVERABLES

1. **Final survey paper (8 pages, IEEE format, excluding references):**
 - **Abstract and Introduction:** scope and contributions.
 - **Background:** the core papers and key concepts.
 - **Taxonomy and Synthesis:** the field organized by theme.
 - **Critical Analysis and Open Problems.**
 - **Conclusion and References.**
2. **Presentation (10 minutes):** the main findings of your survey, followed by questions.

6 EVALUATION CRITERIA

Total Points: 100

Component	Points	Description
Core papers	20	Coverage and depth of the three core papers.
Literature breadth	15	Quality and range of the further sources.
Taxonomy and synthesis	20	A clear, justified structure that connects the work.
Critical analysis	15	Strengths, weaknesses and open problems.
Writing quality	15	Clarity, structure and academic quality.
Citation correctness	5	Every reference real, complete and accurately cited.
Presentation	10	Delivery of the talk and handling of questions.

7 RULES

1. **Individual work:** each student writes and presents their own survey.
2. **AI use:** you may use AI tools, but you must disclose how you used them in a short statement at the end of the paper. You are responsible for every claim; check each statement and each reference against its original source. This is the same verification problem the core papers discuss.
3. **Citation integrity:** every cited work must exist and must support the sentence that cites it. A fabricated or misattributed reference is treated as academic misconduct.
4. **Plagiarism:** copying text from any source without quotation and citation is not accepted.

8 TIMELINE

- ☐ **Week 7:** Annotated bibliography checkpoint.
- ☐ **Week 10:** Draft for feedback.
- ☐ **Week 13:** Final submission and presentations.

REFERENCES

- [1] Sungjo Jeong, Sangjin Lee, and Jungheum Park. LangurTrace: Forensic analysis of local LLM applications. *Forensic Science International: Digital Investigation*, 54:301987, 2025. DFRWS APAC 2025, presented at the 5th Annual Digital Forensics Research Conference APAC.
- [2] Gaëtan Michelet and Frank Breitingner. ChatGPT, Llama, can you write my report? An experiment on assisted digital forensics reports written using (local) large language models. *Forensic Science International: Digital Investigation*, 48:301683, 2024. DFRWS EU 2024, Selected Papers from the 11th Annual Digital Forensics Research Conference Europe.
- [3] Binaya Sharma, James Ghawaly, Kyle McCleary, Andrew M. Webb, and Ibrahim Baggili. ForensicLLM: A local large language model for digital forensics. *Forensic Science International: Digital Investigation*, 52:301872, 2025. DFRWS EU 2025, Selected Papers from the 12th Annual Digital Forensics Research Conference Europe.