LLM et analyse Wireshark — automatise

16 mai 2026 • Mis à jour le 17 mai 2026 • 15 min de lecture • 3254 mots • v

Utilisez les LLM pour analyser automatiquement des captures Wireshark :
detection DNS, pipeline PCAP vers alertes. Guide complet pour analystes

À RETENIR

A retenir -- LLM et analyse Wireshark

Les **LLM pour l'analyse Wireshark** revolutionnent le travail des analystes rese
PCAP complexes en analyses en langage naturel compréhensibles. Le pipeli
une summarization automatique des flux, une detection du Shadow IT via les
des anomalies OT/ICS. Les limites principales sont la taille du contexte (les g
agregation prealable) et le risque de hallucinations sur des protocoles peu re
d'entrainement. L'integration Zeek/Suricata + LLM offre le meilleur equilibre

L'analyse des captures reseau est l'une des taches les plus fastidieuses et les plus
capture Wireshark d'une heure sur un reseau d'entreprise peut contenir des millio

d'analyse experte pour en extraire les informations pertinentes. Les **LLM pour l'an** changent fondamentalement cette equation. En transformant les flux reseau en re LLM, il devient possible de generer des summaries intelligents en quelques secon comportements anormaux (Shadow IT, tunnels couverts, communications C2), et passe reellement sur le reseau. En 2026, des pipelines complets allant du PCAP b disponibles open source. Cet article vous presente l'architecture complete, le cod deployer efficacement ces capacites dans votre SOC ou vos engagements de per

Architecture pipeline PCAP vers LLM vers alerte

Le **pipeline d'analyse reseau par LLM** se decompose en quatre etapes sequentiel

- **Extraction tshark** : convertir le fichier PCAP en JSON structure avec tshark (CL pertinents par protocole (IP src/dst, ports, DNS names, TLS SNI, HTTP Host, pa
- **Agregation et contexte** : aggreger les flux par paires IP, par domaine DNS, par taille du contexte a analyser par le LLM
- **Analyse LLM** : soumettre l'agregation au LLM avec un prompt structure deman classification des flux et les recommandations
- **Alerting** : formatter les sorties LLM en alertes SIEM (JSON CEF ou Syslog) pou

Flow summarization automatique par LLM

La **summarization automatique des flux reseau** est le premier cas d'usage acces lignes de logs, l'analyste recoit un resume structure :