SOC_Shark.py
Proof of Concept

This tool can help analyst quickly identify ARP Spoofing, Port Scanning, Brute Force attacks, and suspicious behavior within packets. The CSV export generated by the python script helps by giving a more user friendly view, if unfamiliar with Wireshark.

How the CSV helps

Speeds up triage workflows by automatically extracting:

- Source & destination IPs
- MAC addresses
- Ports and protocols
- DNS queries
- Connection status
- Packet sizes
- Network direction
- Flow identifiers
- GeoIP country enrichment (Optional)
- HTTP request details (GET/POST)
- Potential plaintext credential exposure

CSV Output Columns

Column	Description
timestamp	Human-readable packet time (local timezone)
src_ip / dst_ip	Source and destination IP addresses
src_mac / dst_mac	Ethernet addresses
src_port / dst_port	Transport layer ports
protocol	IP protocol name
tcp_flags	TCP flag values
packet_size	Packet length in bytes
dns_query	Extracted DNS query
connection_status	attempt / success / failed / udp / other
direction	inbound / outbound / internal / external
flow_id	MD5 hash representing a flow
geoip_country	Destination country (optional)
http_method	HTTP method detected
http_host	Host header
http_uri	Requested URI
http_user_agent	Browser/client string
http_cookie	Cookie header
http_body	HTTP request body
http_credentials	Detected credential-like POST data