Analisi IOC Wireshark

• Identificare eventuali IOC o evidenze di tacchi in corso:
- Avendo analizzato il file scaricato da EPICODE è stato possibile identificare richieste anomale da una determinata sorgente

• Ipotesi su potenziali vettori di attacco:
- Dalle analisi effettuate le richieste sembrano indice di scansione proveniente dall'indirizzo ip: 192.168.200.100

• Azione per ridurre gli impatti dell' attacco:
- É importante a questo punto adottare contromisure nei confronti del IP indicato come ad esempio un blocco nelle policy del firewall, inserendolo eventualmente in blacklist. Essendo inoltre una scansione fatta in rete interna, tramite richiesta ARP è stato possibile visualizzare il Mac address del indirizzo IP associato e di conseguenza è possibile bloccare tramite firewall direttamente anche il Mac address