In [ ]:

```
Training Day 14 Report– 6 July 2025
 Introduction
 Day 14 explored packet capture and traffic analysis as tools for both attacke
fenders. Understanding how data flows on a network enables detection of anomal
 vulnerabilities.
 Key Concepts Discussed
 We reviewed packet structure at a high level, the significance of headers and
 and how encryption affects visibility. The trainer discussed what information
 in cleartext flows and how to spot suspicious patterns.
 Lab Preparation in Theory
 A conceptual capture plan was described: identify capture points, manage stor
 large captures, and plan filters to reduce noise. Ethical constraints around
 traffic that contains private data were reiterated.
 Practical Understanding (Theory)
 We covered how defenders build detection rules and what telemetry is most use
 identifying attacks. The session stressed baseline profiling and anomaly dete
 valuable techniques.
 Key Takeaways
 Traffic analysis is a powerful diagnostic and detection tool; it must be used
 and with consent.
 Conclusion
 The next topic will be man-in-the-middle concepts and how TLS and certificate
ment mitigate those risks.
```