MEETING MINUTES

Project Summary

Meeting Number	3
Date and Time	27/11/ 25, 11.30
Project Name	Network Traffic Profiler Dashboard
Attendees	Timothy Birtles, Sophia Krasowski, Tomiris Ashim, Amelia Lee, Tomek Bergier

Key Discussion Topics	Discussion Points
Current progress	● Code has been developed to extract features from PCAP files. ● The system lists all flows and validates the data. ● After validation, the data is cleaned and converted into a .NPI file — a binary matrix suitable for machine learning.
Method to recognise the flows(Sophia)	● The model uses an Isolation Forest algorithm (unsupervised ML). Values are scaled before training: -1 = anomaly 1 = normal. ● If no flows are flagged, the ML model may not function correctly. If more than 50% are flagged, it may indicate too many anomalies detected. ● Standard scaling is used.
Test data concerns(Tomek)	The number of flows may include both flows and microflows. A single PCAP file may produce one large flow containing multiple microflows. Microflows represent user actions (e.g., clicking a button, subscribing, opening a link). Some flows are definitely action-based, and this may affect the dataset.
Validation	● The system performs validation tests before dataset creation. ● The output includes a “true/false” status indicating whether values fall within the expected range.
Machine Learning Aproach	● The team is using an unsupervised learning method. ● Any abnormal behaviour is flagged.

	● Machine learning must use features from flows, not directly from PCAP files (Tomek).
ACTION ITEMS	
Review action flow	
Complete dashboard prototype	