Feature Details

Feature extraction was carried out using CICFlowMeter (Lashkari et al., 2017).

In order to train and evaluate the machine learning models, flow-based features were extracted from captured network traffic using **CICFlowMeter** (Lashkari et al., 2017). These features represent statistical and behavioral properties of network flows rather than packet payloads, which is essential when dealing with encrypted communication such as TLS 1.3 or DNS-over-HTTPS. The complete set of **78 features** covers categories including basic flow identifiers, packet size statistics, timing intervals, flag counts, and flow activity ratios. By using these features, the models are able to capture patterns in encrypted C2 traffic without requiring access to the actual content of packets. The following table provides a detailed description of each feature used in this study.

Feature	Meaning (Simple Technical Explanation)
Src Port	Source port number used by the sender of the flow.
Dst Port	Destination port number where the traffic is directed.
Flow Duration	Total time (in microseconds) the flow lasted.
Total Fwd Packet	Total number of packets sent in the forward (source → destination) direction.
Total Bwd Packets	Total number of packets sent in the backward (destination → source) direction.
Total Length of Fwd Packet	Sum of the sizes (in bytes) of all forward packets.

Total Length of Bwd Packet	Sum of the sizes (in bytes) of all backward packets.
Fwd Packet Length Max	Largest size of a single forward packet.
Fwd Packet Length Min	Smallest size of a single forward packet.
Fwd Packet Length Mean	Average size of forward packets.
Fwd Packet Length Std	Variation (standard deviation) in forward packet sizes.
Bwd Packet Length Max	Largest size of a single backward packet.
Bwd Packet Length Min	Smallest size of a single backward packet.
Bwd Packet Length Mean	Average size of backward packets.
Bwd Packet Length Std	Variation in backward packet sizes.
Flow Bytes/s	Average number of bytes transmitted per second in the flow.
Flow Packets/s	Average number of packets transmitted per second in the flow.
Flow IAT Mean	Average time between two packets in the flow (Inter-Arrival Time).
Flow IAT Std	Variation in packet inter-arrival times in the flow.
Flow IAT Max	Longest gap between two consecutive packets in the flow.
Flow IAT Min	Shortest gap between two consecutive packets in the flow.
Fwd IAT Total	Total time spent between forward packets.
Fwd IAT Mean	Average time gap between forward packets.
Fwd IAT Std	Variation in the gaps between forward packets.

Fwd IAT Max	Longest gap between forward packets.
Fwd IAT Min	Shortest gap between forward packets.
Bwd IAT Total	Total time spent between backward packets.
Bwd IAT Mean	Average time gap between backward packets.
Bwd IAT Std	Variation in the gaps between backward packets.
Bwd IAT Max	Longest gap between backward packets.
Bwd IAT Min	Shortest gap between backward packets.
Fwd PSH Flags	Number of forward packets with the TCP “PSH” (push) flag set.
Bwd PSH Flags	Number of backward packets with the TCP “PSH” flag set.
Fwd URG Flags	Number of forward packets with the TCP “URG” (urgent) flag set.
Bwd URG Flags	Number of backward packets with the TCP “URG” flag set.
Fwd Header Length	Total length of headers in all forward packets.
Bwd Header Length	Total length of headers in all backward packets.
Fwd Packets/s	Average number of forward packets sent per second.
Bwd Packets/s	Average number of backward packets sent per second.
Packet Length Min	Smallest packet size in the entire flow.
Packet Length Max	Largest packet size in the entire flow.
Packet Length Mean	Average packet size in the entire flow.
Packet Length Std	Variation in packet sizes across the flow.

Packet Length Variance	Statistical variance of packet sizes in the flow.
FIN Flag Count	Number of packets in the flow with the TCP “FIN” flag set.
SYN Flag Count	Number of packets in the flow with the TCP “SYN” flag set.
RST Flag Count	Number of packets in the flow with the TCP “RST” (reset) flag set.
PSH Flag Count	Number of packets in the flow with the TCP “PSH” flag set.
ACK Flag Count	Number of packets in the flow with the TCP “ACK” flag set.
URG Flag Count	Number of packets in the flow with the TCP “URG” flag set.
CWR Flag Count	Number of packets with the TCP “CWR” (congestion window reduced) flag set.
ECE Flag Count	Number of packets with the TCP “ECE” (ECN echo) flag set.
Down/Up Ratio	Ratio of backward packets to forward packets (traffic balance).
Average Packet Size	Mean packet size across the flow (all directions).
Fwd Segment Size Avg	Average segment (packet payload) size in forward direction.
Bwd Segment Size Avg	Average segment size in backward direction.
Fwd Bytes/Bulk Avg	Average bytes sent per bulk transfer in forward direction.
Fwd Packet/Bulk Avg	Average packets per bulk transfer in forward direction.
Fwd Bulk Rate Avg	Average bulk data rate in forward direction.
Bwd Bytes/Bulk Avg	Average bytes per bulk transfer in backward direction.
Bwd Packet/Bulk Avg	Average packets per bulk transfer in backward direction.

Bwd Bulk Rate Avg	Average bulk data rate in backward direction.
Subflow Fwd Packets	Number of packets in forward sub-flows.
Subflow Fwd Bytes	Number of bytes in forward sub-flows.
Subflow Bwd Packets	Number of packets in backward sub-flows.
Subflow Bwd Bytes	Number of bytes in backward sub-flows.
FWD Init Win Bytes	Initial TCP window size used in the forward direction.
Bwd Init Win Bytes	Initial TCP window size used in the backward direction.
Fwd Act Data Pkts	Number of forward packets carrying actual data (not control only).
Fwd Seg Size Min	Minimum segment size in forward direction.
Active Mean	Average length of time the flow remained active (before idle).
Active Std	Variation in the length of active periods.
Active Max	Longest active period in the flow.
Active Min	Shortest active period in the flow.
Idle Mean	Average idle (inactive) time between bursts of packets.
Idle Std	Variation in idle times.
Idle Max	Longest idle period in the flow.
Idle Min	Shortest idle period in the flow.