IP protocol

IP packets

Table 1: Extracted fields for the IP packets

Field	Label	Type	Description
Source IP address	src_ip	string	The source IP address of the packet (Anonymized)
Destination IP address	dst_ip	string	The destination IP address of the packet (Anonymized)
Source MAC	src_mac	string	The source MAC address of the packet (Anonymized) (N/A to PPP protocol)
Destination MAC	dst_mac	string	The destination MAC address of the packet (Anonymized) (N/A to PPP protocol)
Identification	id	int	The unique id of the IP packet. (N/A to PPP protocol)
Length	length	int	The length of the IP packet
Timestamp	timestamp	epoch time	The packet's timestamp in epoch format.
Transport protocol	transport	int	The transport protocol of the packet, e.g. TCP, UDP, ARP, ICMP.
Flags	flags	int	The flags of the packet's header (applicable only to TCP transport protocol). (N/A to PPP protocol)
Options	options	int	The options of the packet's header. (N/A to PPP protocol)
Source port	sport	int	The source port of the packet (N/A for transport protocols that do not have port, like ICMP).
Destination port	dport	int	The destination port of the packet (N/A for transport protocols that do not have port, like ICMP).

IP flows

Table 2: Extracted static and dynamic fields for the IP flows

Field	Label	Type	Description
Static data of IP traffic flows			
IP address of A	ip_a	string	The IP address of the first endpoint of the flow, that is the sender of the first packet of the flow. (Anonymized)
IP address of B	ip_b	string	The IP address of the second endpoint of the flow, that is the receiver of the first packet of the flow. (Anonymized)
MAC address of A	mac_a	string	The MAC address of the first endpoint of the flow, that is the sender of the first

			packet of the flow. (Anonymized) (N/A to PPP protocol)
MAC address of B	mac_b	string	The MAC address of the second endpoint of the flow, that is the receiver of the first packet of the flow. (Anonymized) (N/A to PPP protocol)
Port of A	port_a	int	The port used by the first endpoint of the flow.
Port of B	port_b	int	The port used by the second endpoint of the flow.
Application protocol	prot	string	The application protocol of the communication. Possible values are DNS, FTP, HTTP, IMAP, etc.
Transport protocol	tran_prot	int	The transport protocol of the connection, possible values are 6 for TCP or 17 for UDP.
Starting timestamp	ts_start	epoch time	The timestamp of the first packet of the flow.
Stopping timestamp	ts_end	epoch time	The timestamp of the last packet of the flow.
First 4 bytes from A	f4b_a	string	The first payload's four bytes of the first packet send by A.
First 4 bytes from B	f4b_b	string	The first payload's four bytes of the first packet send by B.
Size of first packet sent from A	sfp_a	int	The size of the first payload-bearing packet sent by the first endpoint.
Size of first packet sent from B	sfp_b	int	The size of the first payload-bearing packet sent by the second endpoint.
Dynamic data of IP traffic flows			
Packets from A	packets_a	int	Total number of packets sent from the first endpoint to the second endpoint.
Bytes from A	bytes_a	int	Total number of bytes sent from the first endpoint to the second endpoint.
Packets from B	packets_b	int	Total number of packets sent from the second endpoint to the first endpoint.
Bytes from B	bytes_b	int	Total number of bytes sent from the second endpoint to the first endpoint.
Min payload from A	min_load_a	int	Minimum payload size sent from first endpoint to second endpoint.
Mean payload from A	mean_load_a	float	Mean payload size sent from first endpoint to second endpoint.
Max payload from A	max_load_a	int	Maximum payload size sent from first endpoint to second endpoint.
Standard deviation payload from A	stdv_load_a	float	Standard deviation of the payload size sent from first endpoint to second endpoint.
Min payload from B	min_load_b	int	Minimum payload size sent from second endpoint to first endpoint.
Mean payload from B	mean_load_b	float	Mean payload size sent from second endpoint to first endpoint.
Max payload from B	max_load_b	int	Maximum payload size sent from second endpoint to first endpoint.

Standard deviation payload from B	stdv_load_b	float	Standard deviation of the payload size sent from second endpoint to first endpoint.
Min inter-arrival from A	min_iat_a	int	Minimum packet inter-arrival time for packets sent from first endpoint to second endpoint.
Mean inter-arrival from A	mean_iat_a	float	Mean packet inter-arrival time for packets sent from first endpoint to second endpoint.
Max inter-arrival from A	max_iat_a	int	Maximum packet inter-arrival time for packets sent from first endpoint to second endpoint.
Standard deviation inter-arrival from A	stdv_iat_a	float	Standard deviation of the packet inter-arrival time for packets sent from first endpoint to second endpoint.
Min inter-arrival from B	min_iat_b	int	Minimum packet inter-arrival time for packets sent from second endpoint to first endpoint.
Mean inter-arrival from B	mean_iat_b	float	Mean packet inter-arrival time for packets sent from second endpoint to first endpoint.
Max inter-arrival from B	max_iat_b	int	Maximum packet inter-arrival time for packets sent from second endpoint to first endpoint.
Standard deviation inter-arrival from B	stdv_iat_b	float	Standard deviation of packet inter-arrival time for packets sent from second endpoint to first endpoint.

Bluetooth Protocol

Bluetooth packets

Table 3 presents the fields that are common to every type of Bluetooth packets. Table 4 presents the fields unique for HCI Command packets, these packets have bt_type=1 as value. Table 5 presents the fields unique for ACL data packets which have bt_type=2 as value. Finally, Table 6 presents the fields for HCI event packets with bt_type=4.

Table 3: Common Fields extracted for Bluetooth packets

Field	Label	Type	Description
Type	bt_type	int	An integer value corresponding to the type of the packet, specifically 1 corresponds to HCI Command, 2 to HCI ACL data, and 4 to HCI event packets.
Direction	direction	int	Defines the direction of the packet. Packets sent by the gateway are denoted as 0, while packets received by the gateway as 1.

Time	timestamp	epoch time	The packet's timestamp in epoch format.
Length	length	int	The packet's length in bytes.
Taxonomy	taxonomy	string	Indicates whether the packet is management or data related, it takes two values, i.e., man and data. This is a custom defined taxonomy, where as 'man' are characterized the packets of HCI Command and HCI event. While, as 'data' are characterized the HCI ACL data packets.

Table 4: Fields extracted for HCI Command packets (bt_type=1)

Field	Label	Type	Description
Opcode	opcode	int	An integer corresponding to the command of the packet. It is built by a combination of the two following codes and it is unique for each command throughout the protocol.
Opcode_ogf	opcode_ogf	int	An integer corresponding to the group of the command. It is unique for each command subgroup and can be used to identify the general category of the command.
Opcode_ocf	opcode_ocf	int	An integer corresponding to the command of the packet. It is unique for each command only throughout its subgroup. If a command should explicitly identified, then this code is not appropriate as duplicate opcode_ocf may arise between commands of different subgroups.
Parameters length	param_length	int	The length of all the parameters measured in bytes.

Table 5: Fields extracted for ACL data packets (bt_type=2)

Field	Label	Type	Description
Source address	src_bd_addr	string	The source address of the packet (Anonymized)
Destination address	dst_bd_addr	string	The destination address of the packet (Anonymized)
Data length	data_length	int	The length of the packet's data in bytes
Opcode	btatt.opcode	int	Method of Bluetooth Attribute Protocol
Service	btatt.service_uuid16	int	Service UUID of Method of Bluetooth Attribute Protocol
Value	btatt.value	int	Value of Bluetooth Attribute Protocol

Table 6: Extracted fields for HCI event packets (bt_type=4)

Field	Label	Type	Description
Event code	event_code	int	The code related to the different types of events

Bluetooth Batches

Table 7: Extracted fields for Bluetooth batches

Field	Label	Type	Description
Source address	src_bd_addr	string	The address of the first endpoint of the batch. (Anonymized) (N/A for batches that contain management packets).
Destination address	dst_bd_addr	string	The address of the second endpoint of the batch. (Anonymized) (N/A for batches that contain management packets).
Taxonomy	taxonomy	string	Indicates whether the batch contains management or data related packets, it takes two values, i.e., “man” and “data”.
Start time	start_time	epoch time	The timestamp of the first packet of the batch stored in Linux time epoch format.
Stop time	stop_time	epoch time	The timestamp of the last packet of the batch stored in Linux time epoch format.
Duration	duration	float	The time duration of the batch in seconds.
Number of packets	number_of_packets	int	The total number of packets contained in the batch.
Batch id	batch_id	string	A string representing the series of type of packets in the batch.
Minimum size	min_size	int	The length in bytes of the smallest packet in the batch.
Maximum size	max_size	int	The length in bytes of the largest packet in the batch.
Average size	average_size	float	The average length in bytes of all the packets in the batch.
Packets from A	total_bytes_a	int	Total number of packets sent from the second endpoint to the first endpoint. (N/A for batches that contain management packets).
Bytes from A	total_bytes_b	int	Total number of bytes sent from the first endpoint to the second endpoint. (N/A for batches that contain management packets).
Packets from B	packets_a	int	Total number of packets sent from the second endpoint to the first endpoint. (N/A for batches that contain management packets).
Bytes from B	packets_b	int	Total number of bytes sent from the second endpoint to the first endpoint. (N/A for batches that contain management packets).
Total sum	sum_size	int	The total sum of the bytes of packets contained in the batch.

ZigBee Protocol

ZigBee packets

Table 8: Extracted fields for the ZigBee packets

Field	Label	Type	Description
Source address	src_zb_addr	string	The source address. (Anonymized)
Destination address	dst_zb_addr	string	The destination address. (Anonymized)
Destination PAN id	dst_zb_pan	string	The destination PAN id. (Anonymized)
Timestamp	timestamp	epoch time	The timestamp of the packet.
Packet length	packet_length	int	The length of the packet in bytes.
Data length	data_length	int	The length of the packet's payload in bytes.
Data	data	binary	The raw data of the payload.

ZigBee batches

Table 9: Extracted fields for the ZigBee batches

Field	Label	Type	Description
Source address	src_zb_addr	string	The source address. (Anonymized)
Destination address	dst_zb_addr	string	The destination address. (Anonymized)
Start time	start_time	epoch time	The timestamp of the first packet of the batch.
Stop time	stop_time	epoch time	The timestamp of the last packet of the batch.
Duration	duration	float	The batch duration in seconds.
Number of packets	number_of_packets	int	The number of the packets contained in the batch.
Minimum size	min_size	int	The length (in bytes) of the smallest packet in the batch.
Maximum size	max_size	int	The length (in bytes) of the largest packet in the batch.
Average size	average_size	float	The average length (in bytes) of the packets belonging to the batch.
Bytes from A	total_bytes_a	int	Total number of bytes sent from the first endpoint to the second endpoint.
Bytes from B	total_bytes_b	int	Total number of bytes sent from the second endpoint to the first endpoint.
Total bytes	sum_size	int	The total sum of the bytes of packets contained in the batch.

Packets from A	packets_a	int	Total number of packets sent from the second endpoint to the first endpoint.
Packets from B	packets_b	int	Total number of packets sent from the second endpoint to the first endpoint.

RF869 Protocol

RF869 packets

Table 10: Extracted fields for RF869 packets

Field	Label	Type	Description
Device address	address	string	The address of the device communicating with the gateway.
Timestamp	timestamp	epoch time	The timestamp of the packet.
Type	type	string	A bitmap that describes the functionality of the packet.
Data length	length	int	The length of the packet's payload in bytes.
Data	data	binary	The application data of the packet (possible empty).

RF869 batches

Table 11: Extracted fields for RF869 batches

Field	Label	Type	Description
Device address	address	string	The address of the device communicating with the gateway.
Start time	start_time	epoch time	The timestamp of the first packet of the batch.
Stop time	stop_time	epoch time	The timestamp of the last packet of the batch.
Duration	duration	int	The batch duration in seconds.
Number of packets	number_of_packets	int	The number of packets contained in the batch.
Minimum size	min_size	int	The length (in bytes) of the smallest packet in the batch.
Maximum size	max_size	int	The length (in bytes) of the largest packet in the batch.
Average size	average_size	float	The average length (in bytes) of the packets contained in the batch.