CS433, Spring 2026
Homework: BLE Packets

This is an **individual** assignment. Submission is through Gradescope. You can submit a scanned version of this document, a computer edited version, or simply paper with the answers. Please be careful to ensure that answers are labeled and legible.

The goal of this homework is to practice interacting with BLE advertisement payloads. Useful aspects of this are decoding TLV data, interpreting fields, and investigating meaningful BLE values (Assigned Numbers).

I don't want busy work, so we're going to keep this assignment fairly short. Long enough to force you to engage a little, but hopefully doesn't take more than an afternoon. If you run into issues on this homework, please reach out to the course staff for help.

BLE Advertisement Background & Resources

- Advertisement TLV format
    - For BLE advertisements, the format of data is Length-Type-Value
        - Where Length is the number of bytes for the Type + Value (doesn't count itself)
        - These "Advertisement Data" TLVs are concatenated together to create a full advertisement payload.
    - Type numbers are defined in the Generic Access Profile document
    - Value fields have their own layout, defined in the Core Specification Supplement
        - 16-bit Service UUIDs are defined in the 16-bit UUID Numbers document
        - From the Core Specification Supplement: "All numerical multi-byte entities and values associated with the following data types shall use little-endian byte order."
    - Company Identifiers are in the Assigned Numbers document
        - Be sure to determine *which* company is identified.
        - Additional manufacturer-specific data can't be translated unless the company provides documentation for it. You probably can't translate it and that's okay.
        - The same is true for some Service Data, especially if it's a company-specific service.

- Advertisement decoding example: https://community.silabs.com/s/article/kba-bt-0201-bluetooth-advertising-data-basics?language=en_US

- To determine what a device is, you will likely have to do a little googling. Usually, a name of a device, or the service UUID and the word "BLE", can get you pretty far.

- Eddystone URL beacon encoding
    - Eddystone payloads use the service UUID 0xFEAA. The service data attached is then further specified by protocol documentation:
    - https://github.com/google/eddystone/blob/master/protocol-specification.md
    - https://github.com/google/eddystone/tree/master/eddystone-url

Q1: Simple BLE Advertisements [15pts]

These are hexadecimal byte values from the payload of a BLE advertisement:

Offset	0	1	2	3	4	5	6	7
0	04	09	48	69	21	02	0A	00
8	--	--	--	--	--	--	--	--
16	--	--	--	--	--	--	--	--
24	--	--	--	--	--	--	--	--

1. What Types are included in this BLE advertisement? Add names from the documentation, not just the numbers.

2. For each type, what information is associated with it? Translate from raw data into meaningful information: for names the name in ASCII, for services the meaning of the service, etc. Include units when meaningful.

Q2: Real-world BLE Advertisement 1 [20pts]

These are hexadecimal byte values from the payload of a BLE advertisement:

Offset	0	1	2	3	4	5	6	7
0	03	03	03	FE	0E	09	4C	45
8	5F	57	48	2D	31	30	30	30
16	58	4D	34	--	--	--	--	--
24	--	--	--	--	--	--	--	--

1. What Types are included in this BLE advertisement? Add names from the documentation, not just the numbers.

2. For each type, what information is associated with it? Translate from raw data into meaningful information: for names the name in ASCII, for services the meaning of the service, etc. Include units when meaningful.

3. What is this device and why does it have that service?

Q3: Real-world BLE Advertisement 2 [20pts]

These are hexadecimal byte values from the payload of a BLE advertisement:

Offset	0	1	2	3	4	5	6	7
0	02	01	02	0B	FF	1B	01	00
8	00	EC	67	94	71	D4	40	0F
16	09	4A	4C	36	36	31	41	2D
24	2D	2D	2D	2D	2D	2D	2D	--

1. What Types are included in this BLE advertisement? Add names from the documentation, not just the numbers.

2. For each type, what information is associated with it? Translate from raw data into meaningful information: for names the name in ASCII, for services the meaning of the service, etc. Include units when meaningful.

3. What is this device? Why does it even have BLE support?

Q4: Real-world BLE Advertisement 3 [20pts]

These are hexadecimal byte values from the payload of a BLE advertisement:

Offset	0	1	2	3	4	5	6	7
0	02	01	06	05	16	61	FE	00
8	02	13	09	4D	65	65	74	55
16	70	20	53	6F	66	74	20	52
24	65	6D	6F	74	65	--	--	--

1. What Types are included in this BLE advertisement? Add names from the documentation, not just the numbers.

2. For each type, what information is associated with it? Translate from raw data into meaningful information: for names the name in ASCII, for services the meaning of the service, etc. Include units when meaningful.

3. What is this device? Why does it even have BLE support?

Q5: Eddystone Advertisement [25pts]

These are hexadecimal byte values from the payload of a BLE advertisement:

Offset	0	1	2	3	4	5	6	7
0	02	01	06	03	03	AA	FE	0F
8	16	AA	FE	10	BA	03	78	6B
16	63	64	00	32	30	35	35	--
24	--	--	--	--	--	--	--	--

1. What Types are included in this BLE advertisement? Add names from the documentation, not just the numbers.

2. For each type, what information is associated with it? Translate from raw data into meaningful information: for names the name in ASCII, for services the meaning of the service, etc. Include units when meaningful.

3. What is the Eddystone URL here?