IoT Environment: Implementing Security Measures

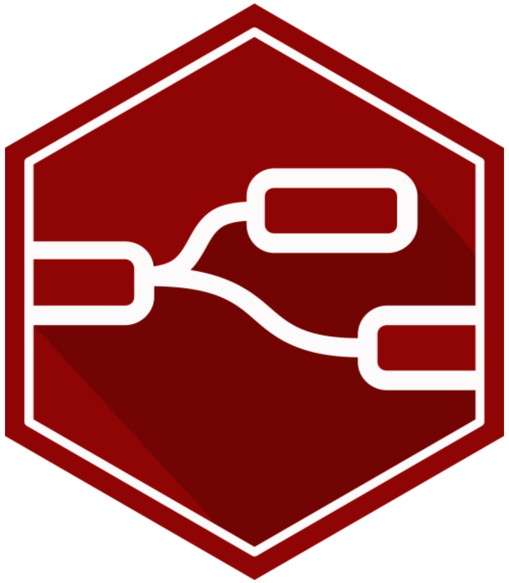
Enhancing IoT Security Through Authentication, Accounting, and Advanced Measurement Tools: A Comprehensive Approach Using Wireshark and BetterCap

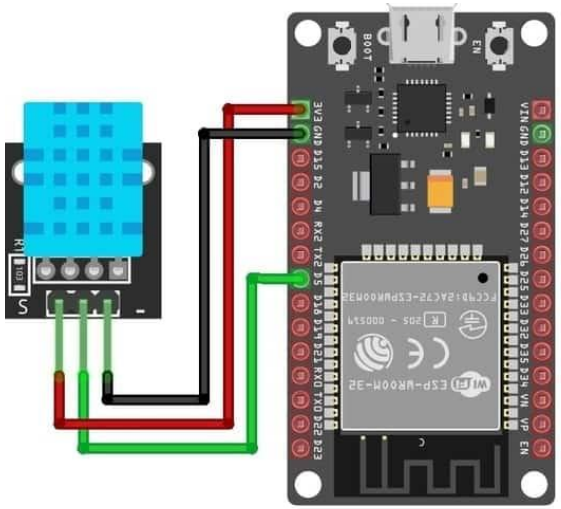
IoT Environment: Implementing Security Measures

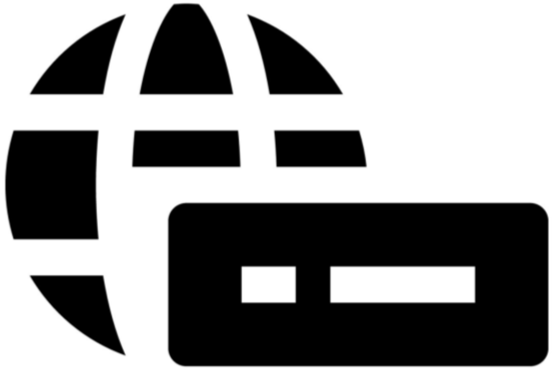
Mohammed Alramadan
muhammedarramadan@gmail.com
Mohammed Ali

University of Calabria

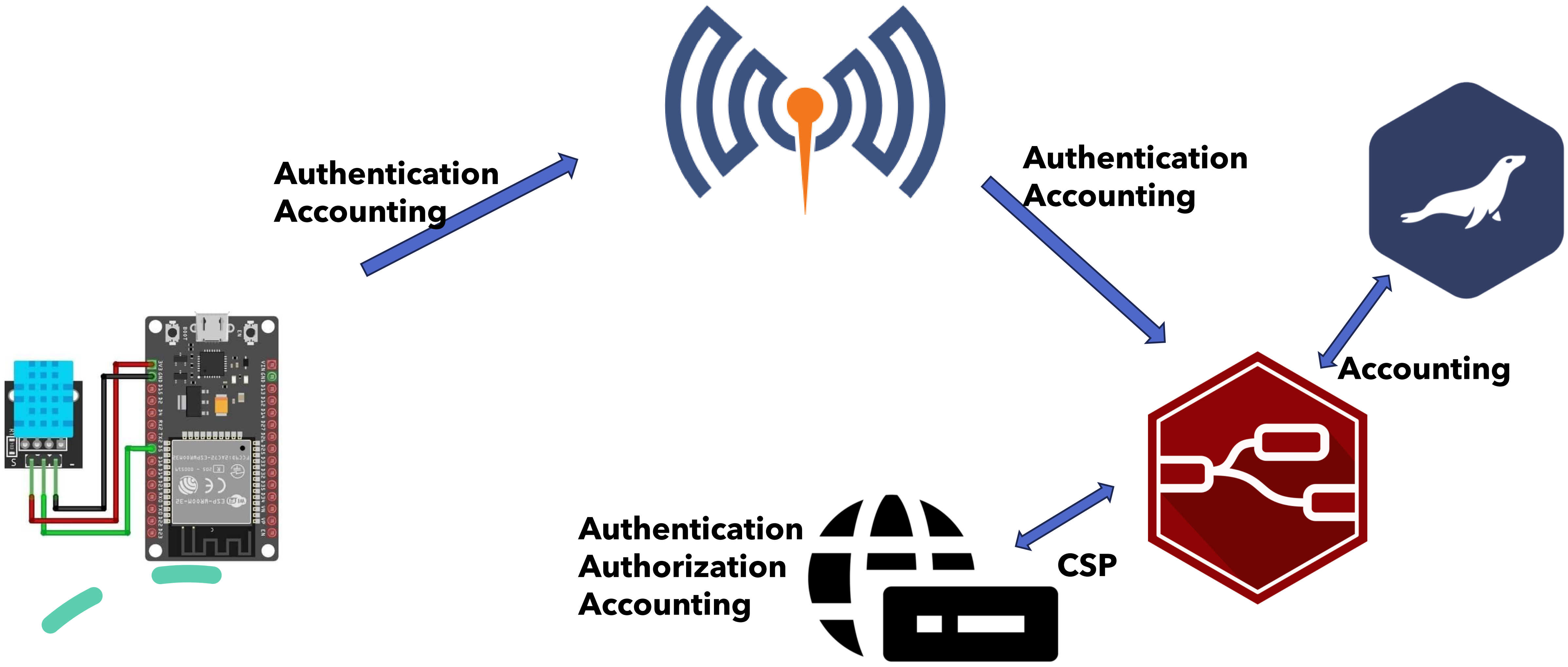
IoT Basic Architecture







IoT Basic Architecture: Security Implementation



Authentication
Accounting

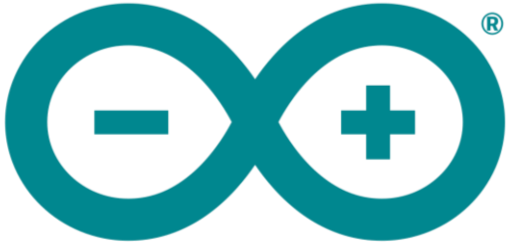
Authentication
Accounting

Accounting

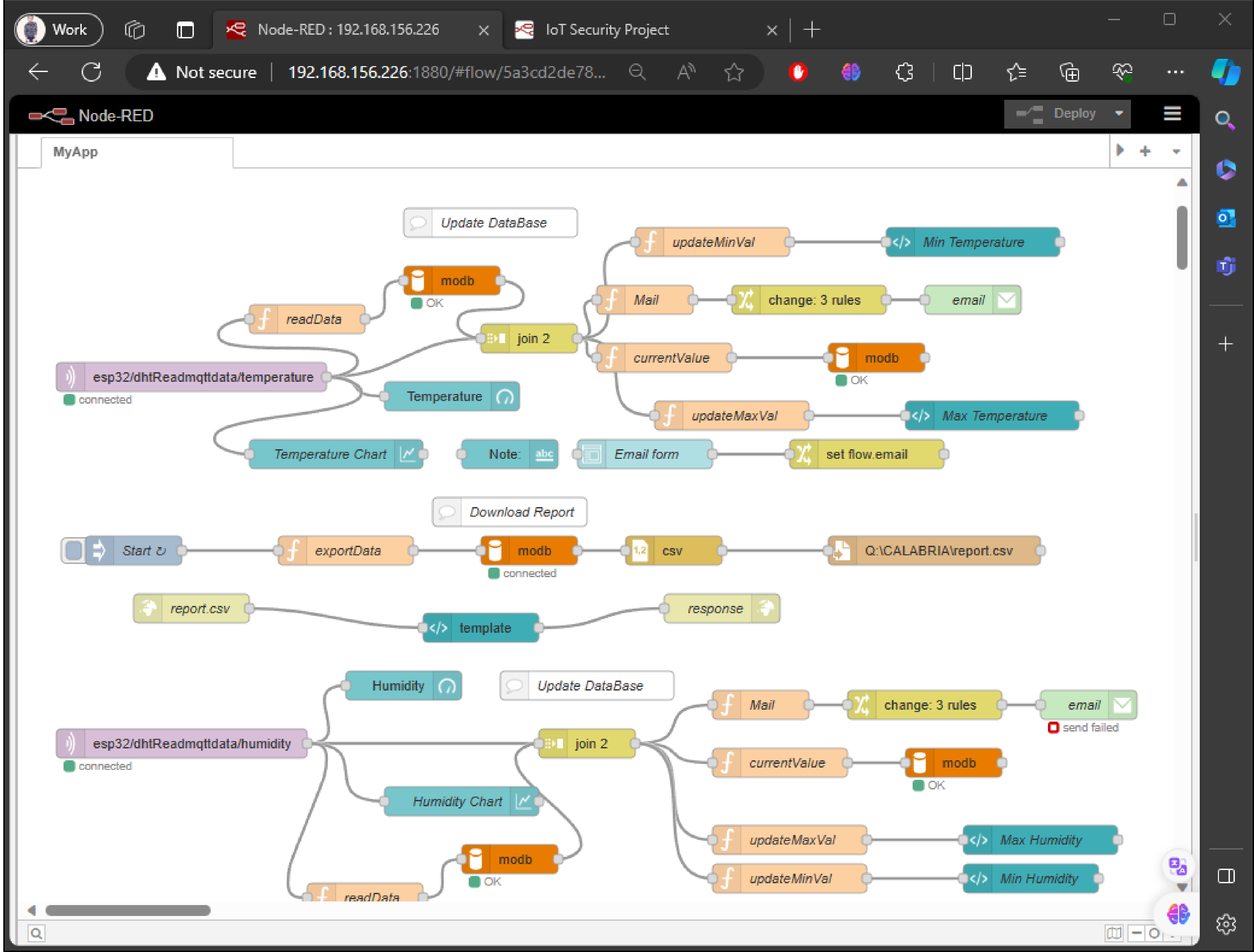
Authentication
Authorization
Accounting

CSP

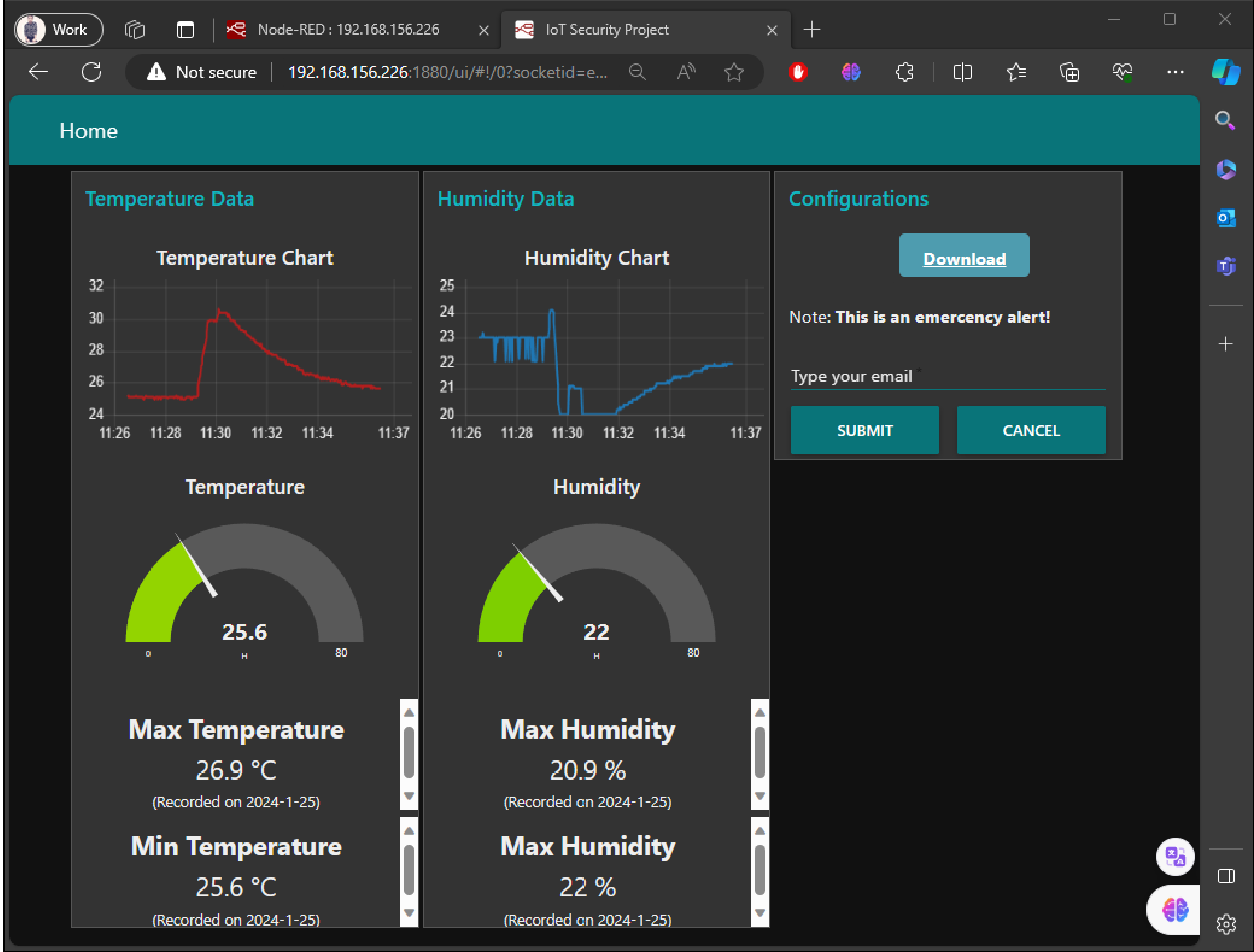
Monitoring IoT Security



Node Red Architecture



Dashboard Architecture



Note: **This is an emercency alert!**

Type your email *

Max Temperature

26.9 °C

(Recorded on 2024-1-25)

Min Temperature

25.6 °C

(Recorded on 2024-1-25)

Max Humidity

20.9 %

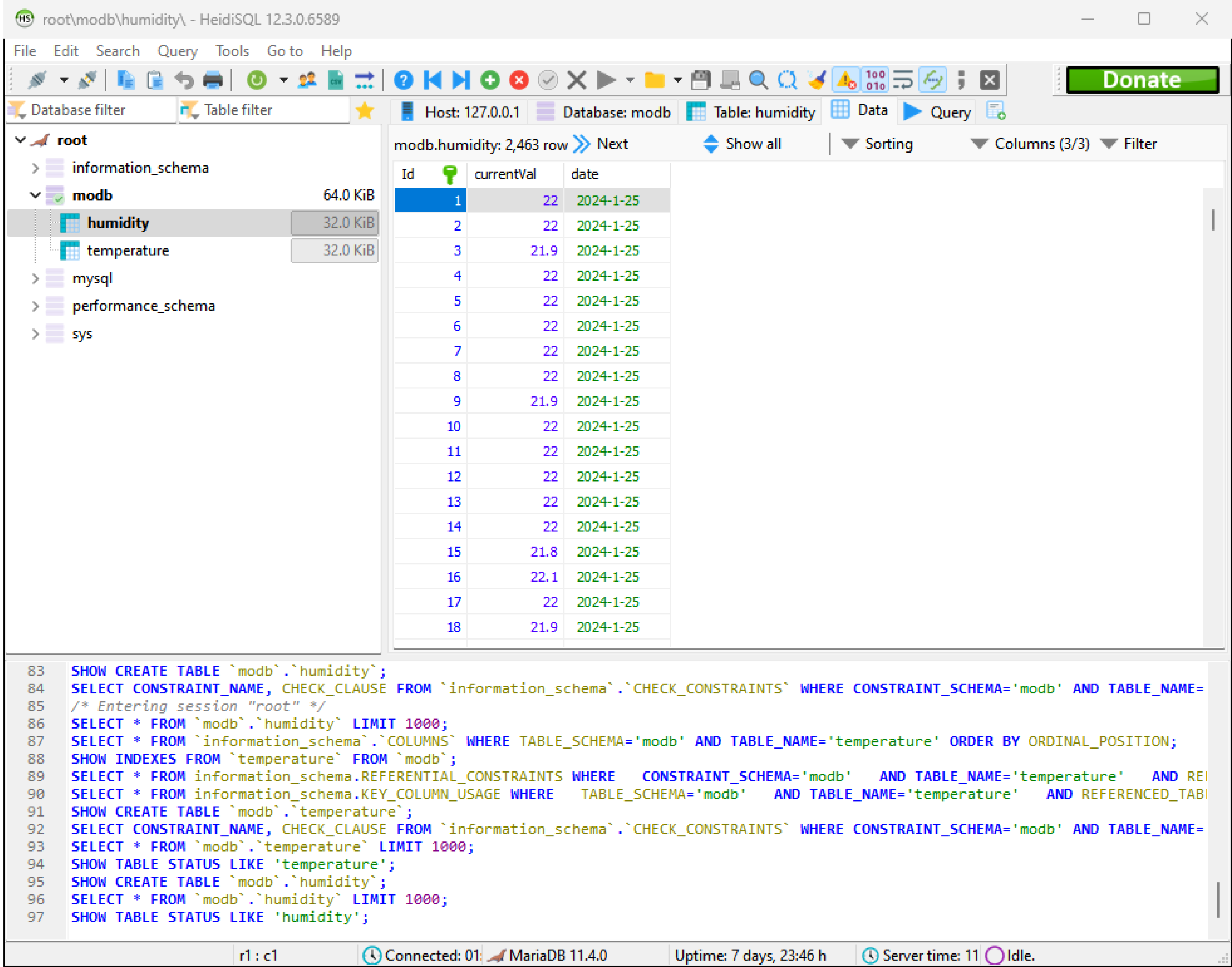
(Recorded on 2024-1-25)

Max Humidity

22 %

(Recorded on 2024-1-25)

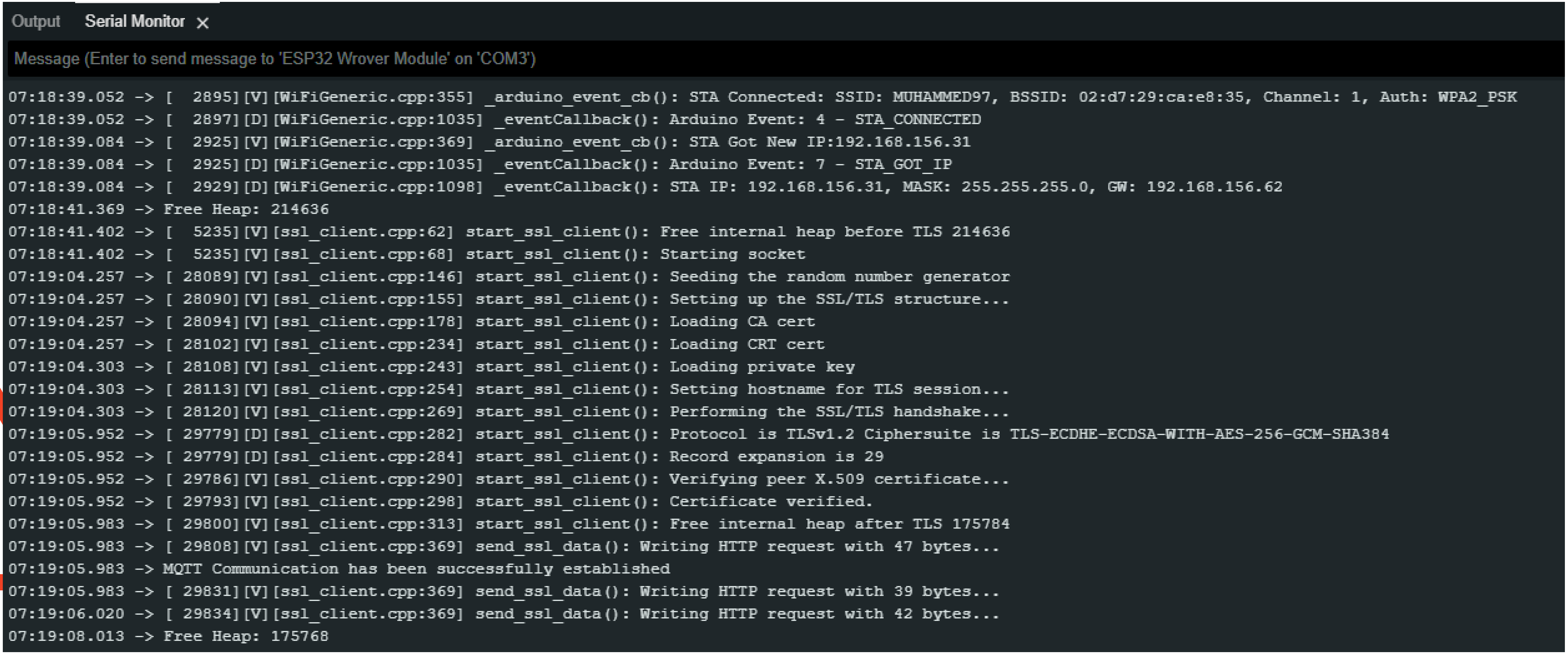
MariaDB HeidiSQL



Id	currentVal	date
1	22	2024-1-25
2	22	2024-1-25
3	21.9	2024-1-25
4	22	2024-1-25
5	22	2024-1-25
6	22	2024-1-25
7	22	2024-1-25
8	22	2024-1-25
9	21.9	2024-1-25
10	22	2024-1-25
11	22	2024-1-25
12	22	2024-1-25
13	22	2024-1-25
14	22	2024-1-25
15	21.8	2024-1-25
16	22.1	2024-1-25
17	22	2024-1-25
18	21.9	2024-1-25

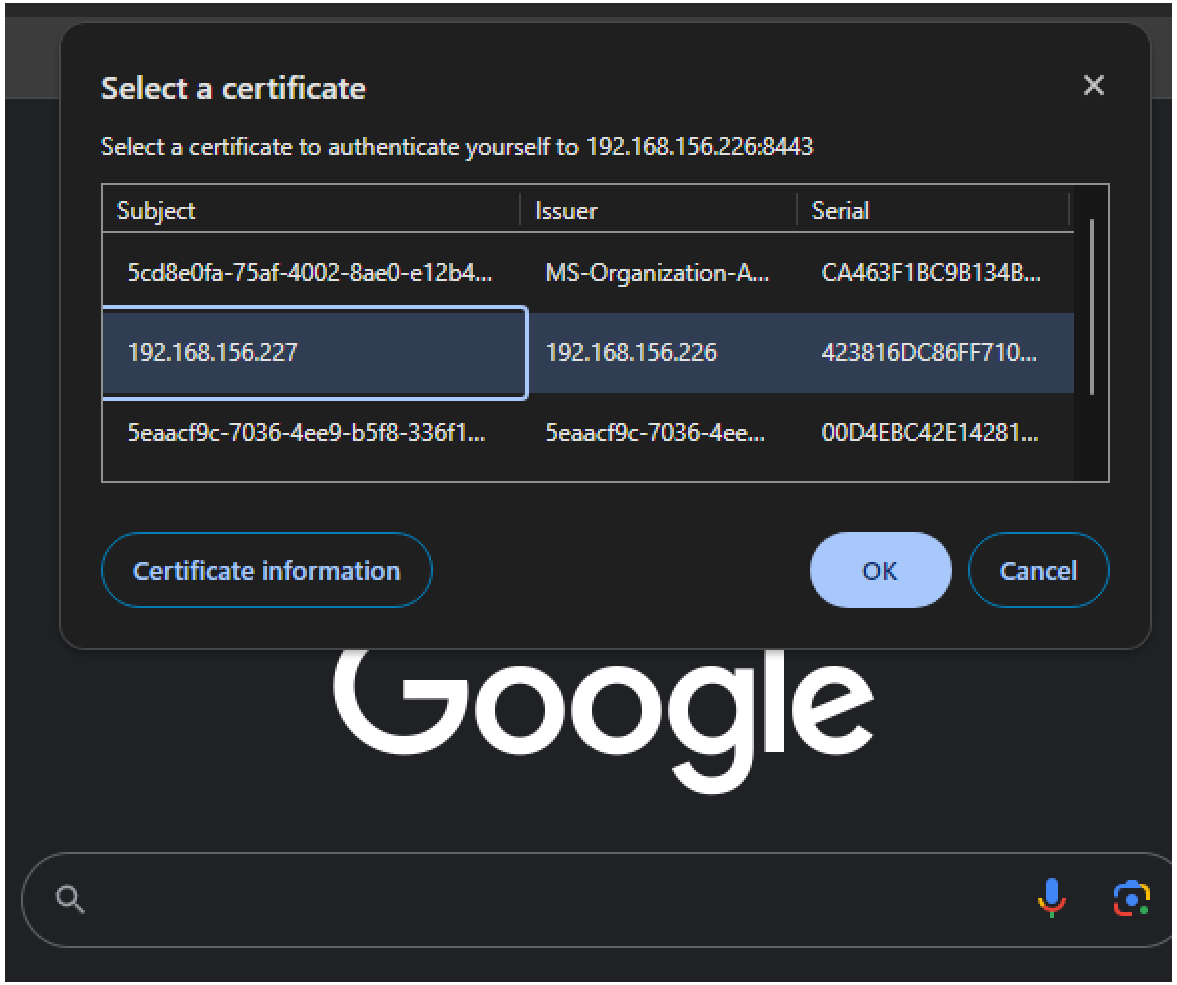
```
SHOW CREATE TABLE `modb`.`humidity`;
SELECT CONSTRAINT_NAME, CHECK_CLAUSE FROM `information_schema`.`CHECK_CONSTRAINTS` WHERE CONSTRAINT_SCHEMA='modb' AND TABLE_NAME=
/* Entering session "root" */
SELECT * FROM `modb`.`humidity` LIMIT 1000;
SELECT * FROM `information_schema`.`COLUMNS` WHERE TABLE_SCHEMA='modb' AND TABLE_NAME='temperature' ORDER BY ORDINAL_POSITION;
SHOW INDEXES FROM `temperature` FROM `modb`;
SELECT * FROM information_schema.REFERENTIAL_CONSTRAINTS WHERE   CONSTRAINT_SCHEMA='modb'   AND TABLE_NAME='temperature'   AND RE
SELECT * FROM information_schema.KEY_COLUMN_USAGE WHERE   TABLE_SCHEMA='modb'   AND TABLE_NAME='temperature'   AND REFERENCED_TAB
SHOW CREATE TABLE `modb`.`temperature`;
SELECT CONSTRAINT_NAME, CHECK_CLAUSE FROM `information_schema`.`CHECK_CONSTRAINTS` WHERE CONSTRAINT_SCHEMA='modb' AND TABLE_NAME=
SELECT * FROM `modb`.`temperature` LIMIT 1000;
SHOW TABLE STATUS LIKE 'temperature';
SHOW CREATE TABLE `modb`.`humidity`;
SELECT * FROM `modb`.`humidity` LIMIT 1000;
SHOW TABLE STATUS LIKE 'humidity';
```

Setting up SSL/TLS Communication ESP32


Output
Serial Monitor ×
Message (Enter to send message to 'ESP32 Wrover Module' on 'COM3')

```
07:18:39.052 -> [  2895][V][WiFiGeneric.cpp:355] _arduino_event_cb(): STA Connected: SSID: MUHAMMED97, BSSID: 02:d7:29:ca:e8:35, Channel: 1, Auth: WPA2_PSK
07:18:39.052 -> [  2897][D][WiFiGeneric.cpp:1035] _eventCallback(): Arduino Event: 4 - STA_CONNECTED
07:18:39.084 -> [  2925][V][WiFiGeneric.cpp:369] _arduino_event_cb(): STA Got New IP:192.168.156.31
07:18:39.084 -> [  2925][D][WiFiGeneric.cpp:1035] _eventCallback(): Arduino Event: 7 - STA_GOT_IP
07:18:39.084 -> [  2929][D][WiFiGeneric.cpp:1098] _eventCallback(): STA IP: 192.168.156.31, MASK: 255.255.255.0, GW: 192.168.156.62
07:18:41.369 -> Free Heap: 214636
07:18:41.402 -> [  5235][V][ssl_client.cpp:62] start_ssl_client(): Free internal heap before TLS 214636
07:18:41.402 -> [  5235][V][ssl_client.cpp:68] start_ssl_client(): Starting socket
07:19:04.257 -> [ 28089][V][ssl_client.cpp:146] start_ssl_client(): Seeding the random number generator
07:19:04.257 -> [ 28090][V][ssl_client.cpp:155] start_ssl_client(): Setting up the SSL/TLS structure...
07:19:04.257 -> [ 28094][V][ssl_client.cpp:178] start_ssl_client(): Loading CA cert
07:19:04.257 -> [ 28102][V][ssl_client.cpp:234] start_ssl_client(): Loading CRT cert
07:19:04.303 -> [ 28108][V][ssl_client.cpp:243] start_ssl_client(): Loading private key
07:19:04.303 -> [ 28113][V][ssl_client.cpp:254] start_ssl_client(): Setting hostname for TLS session...
07:19:04.303 -> [ 28120][V][ssl_client.cpp:269] start_ssl_client(): Performing the SSL/TLS handshake...
07:19:05.952 -> [ 29779][D][ssl_client.cpp:282] start_ssl_client(): Protocol is TLSv1.2 Ciphersuite is TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384
07:19:05.952 -> [ 29779][D][ssl_client.cpp:284] start_ssl_client(): Record expansion is 29
07:19:05.952 -> [ 29786][V][ssl_client.cpp:290] start_ssl_client(): Verifying peer X.509 certificate...
07:19:05.952 -> [ 29793][V][ssl_client.cpp:298] start_ssl_client(): Certificate verified.
07:19:05.983 -> [ 29800][V][ssl_client.cpp:313] start_ssl_client(): Free internal heap after TLS 175784
07:19:05.983 -> [ 29808][V][ssl_client.cpp:369] send_ssl_data(): Writing HTTP request with 47 bytes...
07:19:05.983 -> MQTT Communication has been successfully established
07:19:05.983 -> [ 29831][V][ssl_client.cpp:369] send_ssl_data(): Writing HTTP request with 39 bytes...
07:19:06.020 -> [ 29834][V][ssl_client.cpp:369] send_ssl_data(): Writing HTTP request with 42 bytes...
07:19:08.013 -> Free Heap: 175768
```

Setting up SSL/TLS Communication For the Web Server

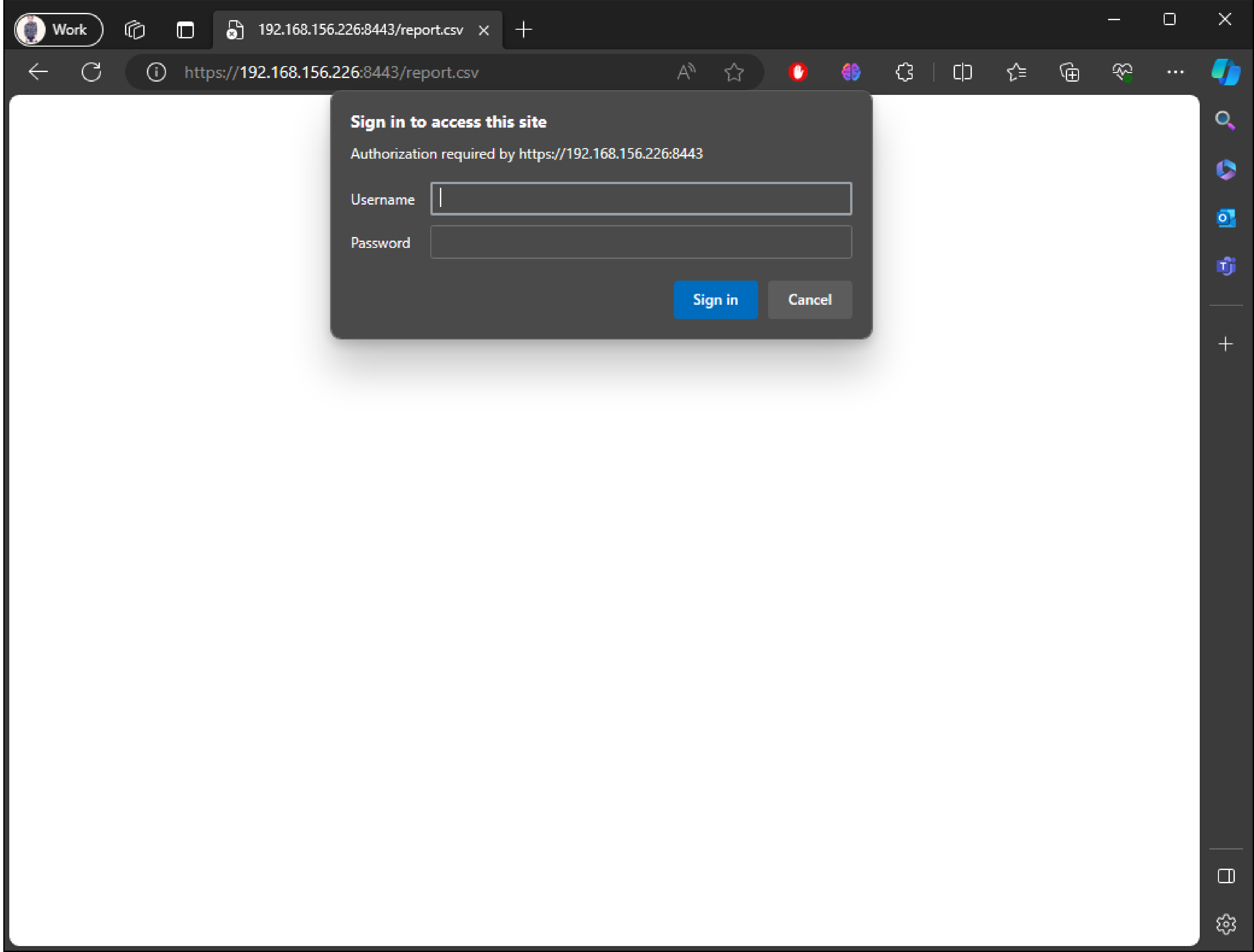


Select a certificate

Select a certificate to authenticate yourself to 192.168.156.226:8443

Subject	Issuer	Serial
5cd8e0fa-75af-4002-8ae0-e12b4...	MS-Organization-A...	CA463F1BC9B134B...
192.168.156.227	192.168.156.226	423816DC86FF710...
5eaacf9c-7036-4ee9-b5f8-336f1...	5eaacf9c-7036-4ee...	00D4EBC42E14281...

Setting up Accounting For the Web Server



Work
192.168.156.226:8443/report.csv
https://192.168.156.226:8443/report.csv

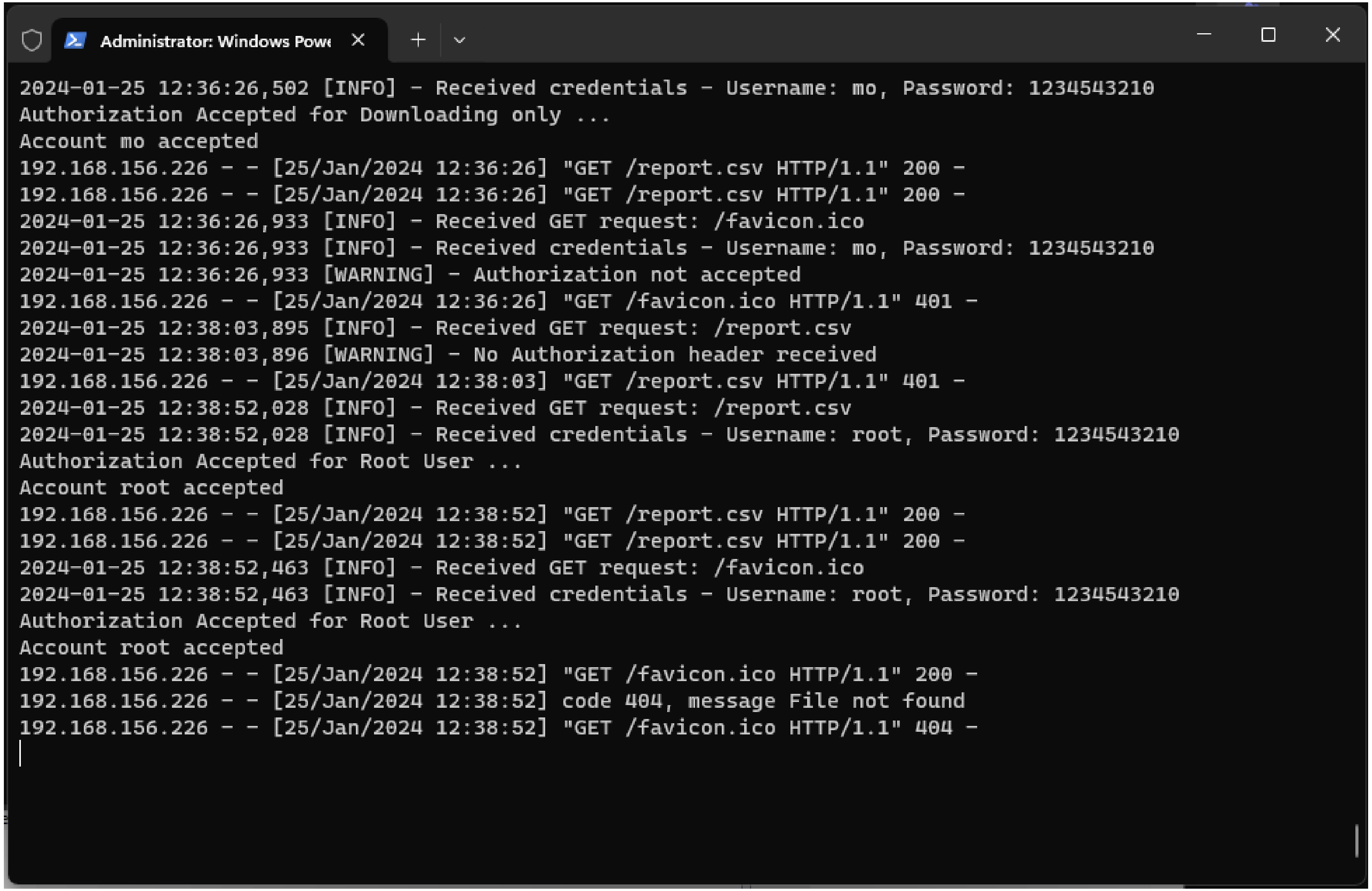
Sign in to access this site

Authorization required by https://192.168.156.226:8443

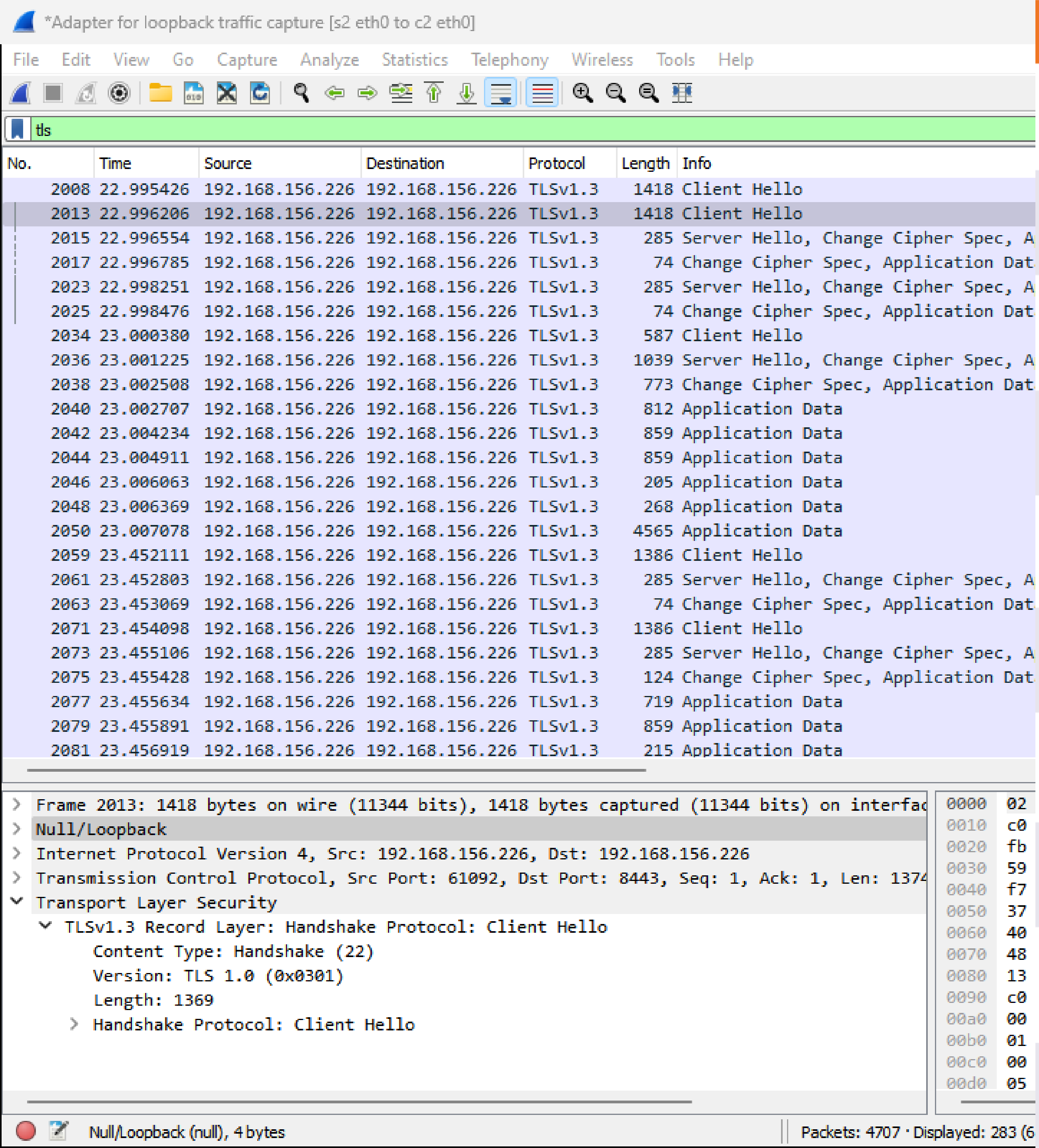
Username

Password

Connecting to the Web Server



```
2024-01-25 12:36:26,502 [INFO] - Received credentials - Username: mo, Password: 1234543210
Authorization Accepted for Downloading only ...
Account mo accepted
192.168.156.226 - - [25/Jan/2024 12:36:26] "GET /report.csv HTTP/1.1" 200 -
192.168.156.226 - - [25/Jan/2024 12:36:26] "GET /report.csv HTTP/1.1" 200 -
2024-01-25 12:36:26,933 [INFO] - Received GET request: /favicon.ico
2024-01-25 12:36:26,933 [INFO] - Received credentials - Username: mo, Password: 1234543210
2024-01-25 12:36:26,933 [WARNING] - Authorization not accepted
192.168.156.226 - - [25/Jan/2024 12:36:26] "GET /favicon.ico HTTP/1.1" 401 -
2024-01-25 12:38:03,895 [INFO] - Received GET request: /report.csv
2024-01-25 12:38:03,896 [WARNING] - No Authorization header received
192.168.156.226 - - [25/Jan/2024 12:38:03] "GET /report.csv HTTP/1.1" 401 -
2024-01-25 12:38:52,028 [INFO] - Received GET request: /report.csv
2024-01-25 12:38:52,028 [INFO] - Received credentials - Username: root, Password: 1234543210
Authorization Accepted for Root User ...
Account root accepted
192.168.156.226 - - [25/Jan/2024 12:38:52] "GET /report.csv HTTP/1.1" 200 -
192.168.156.226 - - [25/Jan/2024 12:38:52] "GET /report.csv HTTP/1.1" 200 -
2024-01-25 12:38:52,463 [INFO] - Received GET request: /favicon.ico
2024-01-25 12:38:52,463 [INFO] - Received credentials - Username: root, Password: 1234543210
Authorization Accepted for Root User ...
Account root accepted
192.168.156.226 - - [25/Jan/2024 12:38:52] "GET /favicon.ico HTTP/1.1" 200 -
192.168.156.226 - - [25/Jan/2024 12:38:52] code 404, message File not found
192.168.156.226 - - [25/Jan/2024 12:38:52] "GET /favicon.ico HTTP/1.1" 404 -
```



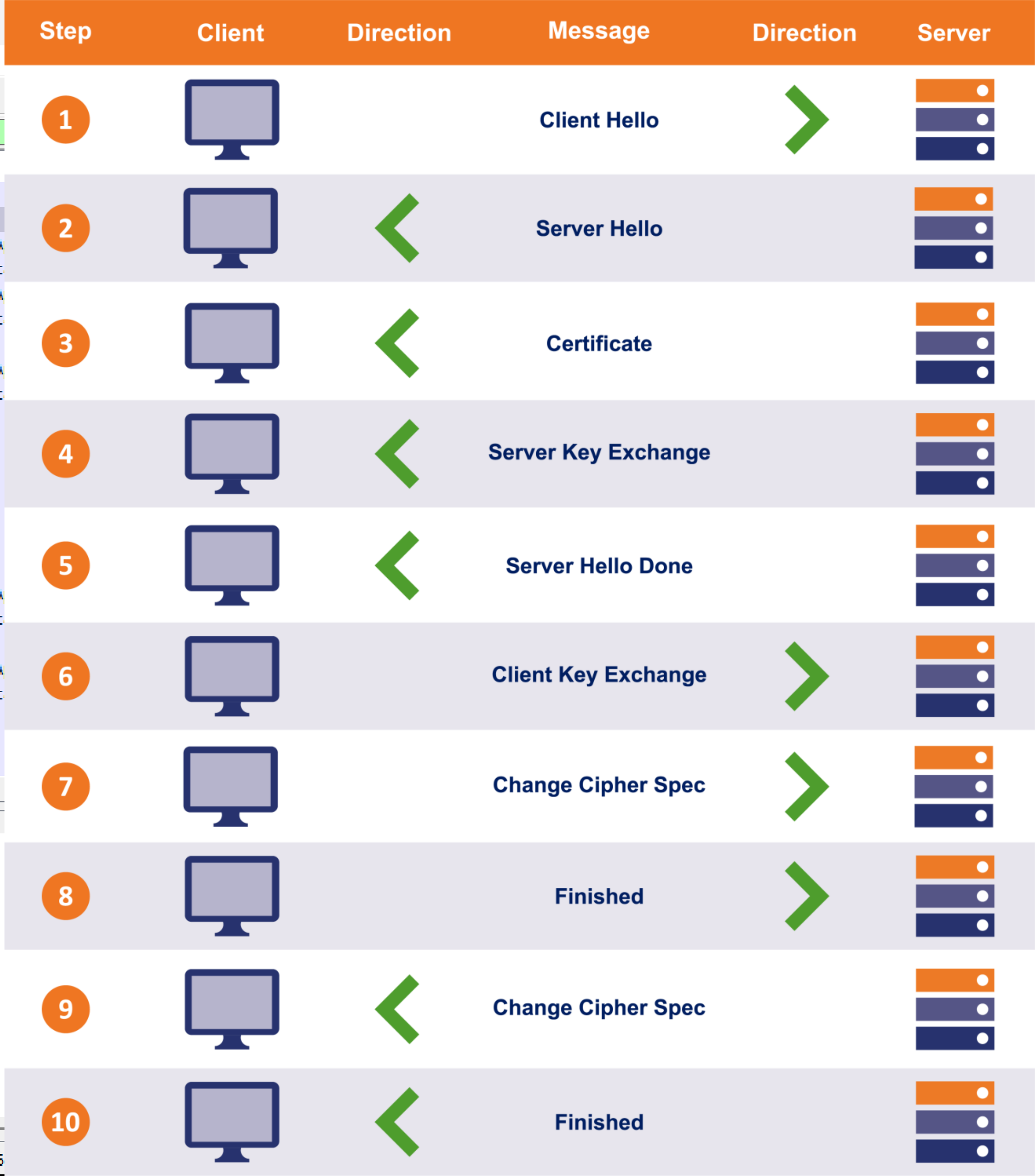
*Adapter for loopback traffic capture [s2 eth0 to c2 eth0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls

```
No.   Time      Source          Destination     Protocol Length Info
 2008 22.995426 192.168.156.226 192.168.156.226 TLSv1.3   1418 Client Hello
 2013 22.996206 192.168.156.226 192.168.156.226 TLSv1.3   1418 Client Hello
 2015 22.996554 192.168.156.226 192.168.156.226 TLSv1.3    285 Server Hello, Change Cipher Spec, A
 2017 22.996785 192.168.156.226 192.168.156.226 TLSv1.3     74 Change Cipher Spec, Application Dat
 2023 22.998251 192.168.156.226 192.168.156.226 TLSv1.3    285 Server Hello, Change Cipher Spec, A
 2025 22.998476 192.168.156.226 192.168.156.226 TLSv1.3     74 Change Cipher Spec, Application Dat
 2034 23.000380 192.168.156.226 192.168.156.226 TLSv1.3    587 Client Hello
 2036 23.001225 192.168.156.226 192.168.156.226 TLSv1.3   1039 Server Hello, Change Cipher Spec, A
 2038 23.002508 192.168.156.226 192.168.156.226 TLSv1.3    773 Change Cipher Spec, Application Dat
 2040 23.002707 192.168.156.226 192.168.156.226 TLSv1.3    812 Application Data
 2042 23.004234 192.168.156.226 192.168.156.226 TLSv1.3    859 Application Data
 2044 23.004911 192.168.156.226 192.168.156.226 TLSv1.3    859 Application Data
 2046 23.006063 192.168.156.226 192.168.156.226 TLSv1.3    205 Application Data
 2048 23.006369 192.168.156.226 192.168.156.226 TLSv1.3    268 Application Data
 2050 23.007078 192.168.156.226 192.168.156.226 TLSv1.3   4565 Application Data
 2059 23.452111 192.168.156.226 192.168.156.226 TLSv1.3   1386 Client Hello
 2061 23.452803 192.168.156.226 192.168.156.226 TLSv1.3    285 Server Hello, Change Cipher Spec, A
 2063 23.453069 192.168.156.226 192.168.156.226 TLSv1.3     74 Change Cipher Spec, Application Dat
 2071 23.454098 192.168.156.226 192.168.156.226 TLSv1.3   1386 Client Hello
 2073 23.455106 192.168.156.226 192.168.156.226 TLSv1.3    285 Server Hello, Change Cipher Spec, A
 2075 23.455428 192.168.156.226 192.168.156.226 TLSv1.3    124 Change Cipher Spec, Application Dat
 2077 23.455634 192.168.156.226 192.168.156.226 TLSv1.3    719 Application Data
 2079 23.455891 192.168.156.226 192.168.156.226 TLSv1.3    859 Application Data
 2081 23.456919 192.168.156.226 192.168.156.226 TLSv1.3    215 Application Data
```

```
> Frame 2013: 1418 bytes on wire (11344 bits), 1418 bytes captured (11344 bits) on interfac
> Null/Loopback
> Internet Protocol Version 4, Src: 192.168.156.226, Dst: 192.168.156.226
> Transmission Control Protocol, Src Port: 61092, Dst Port: 8443, Seq: 1, Ack: 1, Len: 1374
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 1369
    > Handshake Protocol: Client Hello
```

```
0000  02
0010  c0
0020  fb
0030  59
0040  f7
0050  37
0060  40
0070  48
0080  13
0090  c0
00a0  00
00b0  01
00c0  00
00d0  05
```

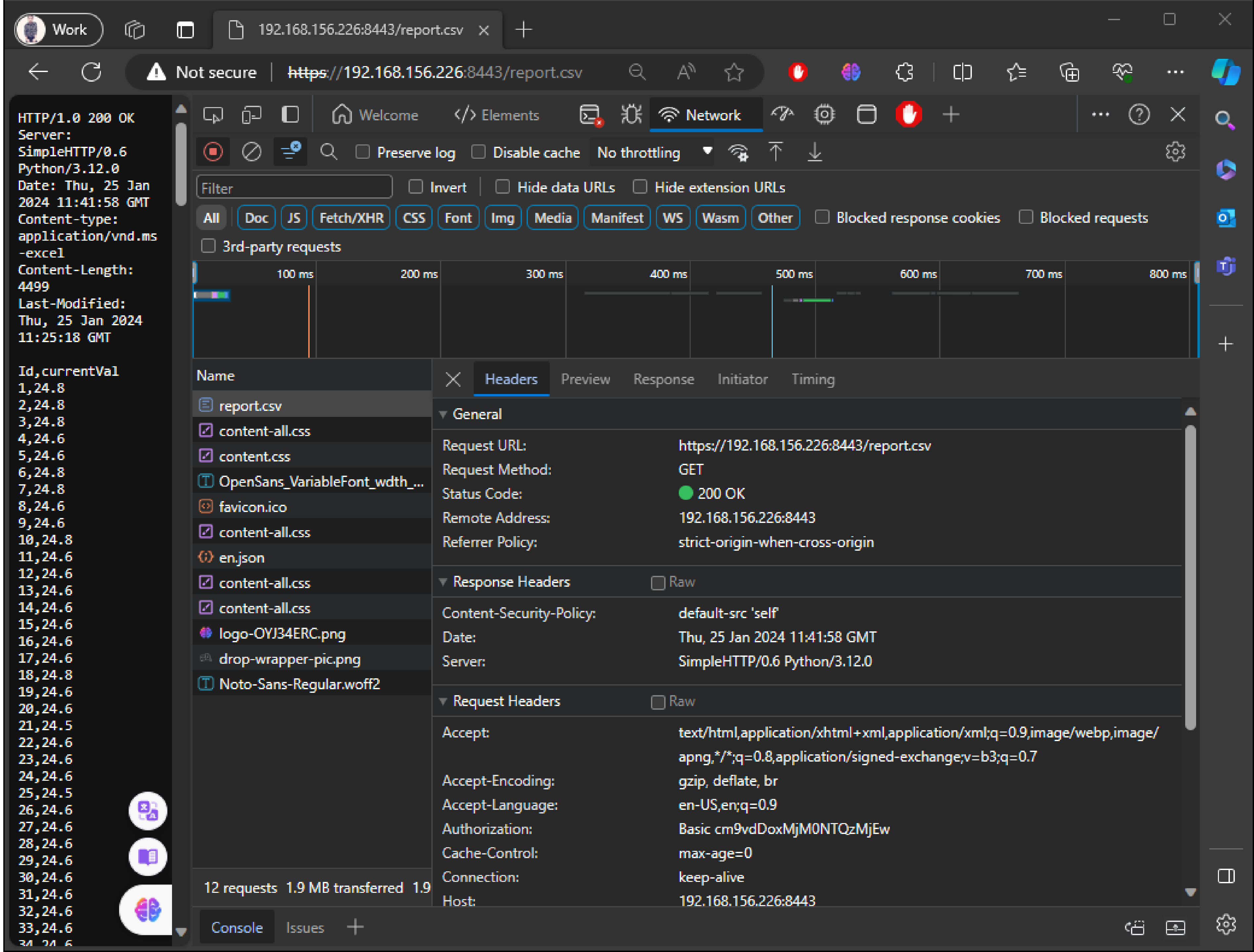
```
Null/Loopback (null), 4 bytes          Packets: 4707 · Displayed: 283 (6
```



Step	Client	Direction	Message	Direction	Server
1			Client Hello	>	
2		<	Server Hello		
3		<	Certificate		
4		<	Server Key Exchange		
5		<	Server Hello Done		
6			Client Key Exchange	>	
7			Change Cipher Spec	>	
8			Finished	>	
9		<	Change Cipher Spec		
10		<	Finished		

Confirming CSP Work

Preventing XSS Attack



```
HTTP/1.0 200 OK
Server:
SimpleHTTP/0.6
Python/3.12.0
Date: Thu, 25 Jan
2024 11:41:58 GMT
Content-type:
application/vnd.ms
-excel
Content-Length:
4499
Last-Modified:
Thu, 25 Jan 2024
11:25:18 GMT

Id,currentVal
1,24.8
2,24.8
3,24.8
4,24.6
5,24.6
6,24.8
7,24.8
8,24.6
9,24.6
10,24.8
11,24.6
12,24.6
13,24.6
14,24.6
15,24.6
16,24.6
17,24.6
18,24.8
19,24.6
20,24.6
21,24.5
22,24.6
23,24.6
24,24.6
25,24.5
26,24.6
27,24.6
28,24.6
29,24.6
30,24.6
31,24.6
32,24.6
33,24.6
34,24.6
```

Name

- report.csv
- content-all.css
- content.css
- OpenSans_VariableFont_wdth_...
- favicon.ico
- content-all.css
- en.json
- content-all.css
- content-all.css
- logo-OYJ34ERC.png
- drop-wrapper-pic.png
- Noto-Sans-Regular.woff2

12 requests 1.9 MB transferred 1.9

General

Request URL:	https://192.168.156.226:8443/report.csv
Request Method:	GET
Status Code:	● 200 OK
Remote Address:	192.168.156.226:8443
Referrer Policy:	strict-origin-when-cross-origin

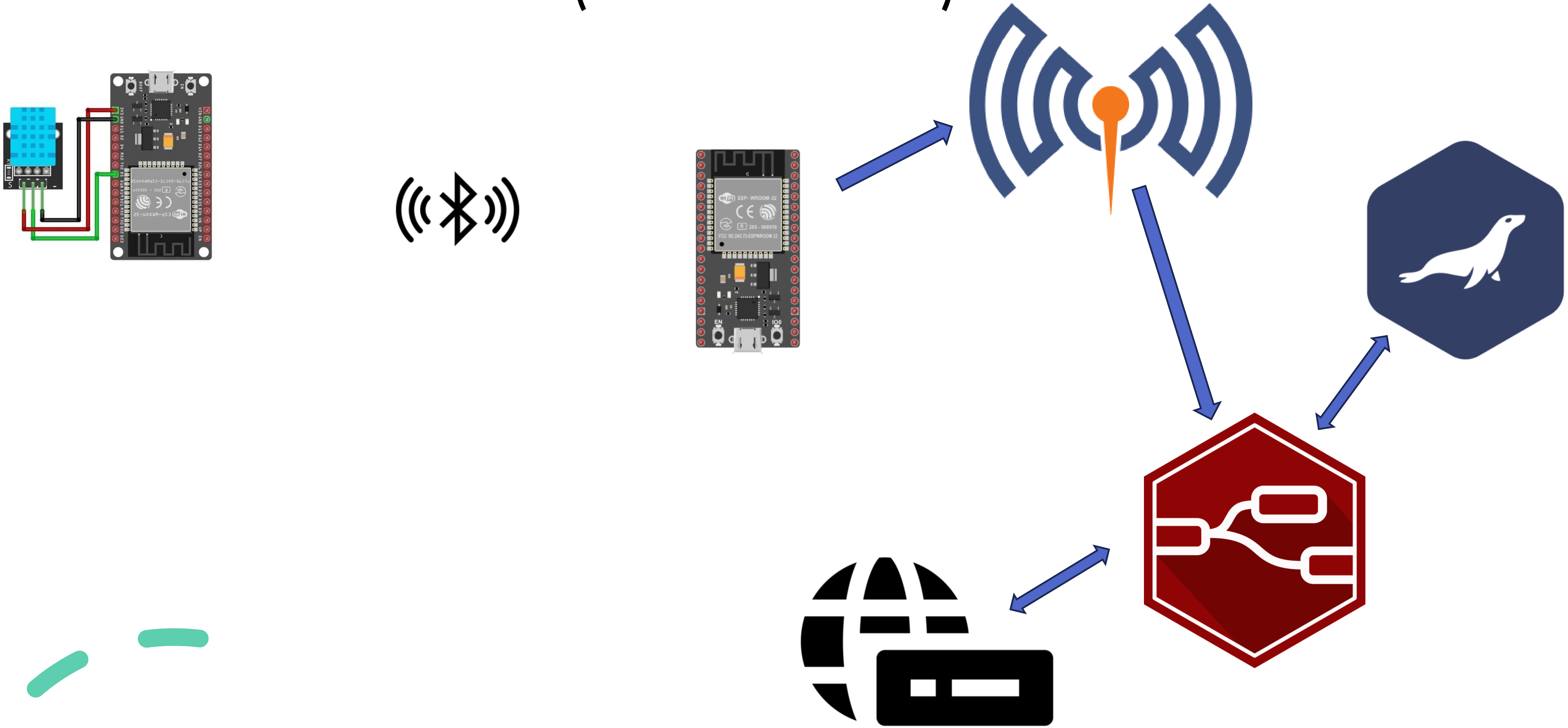
Response Headers □ Raw

Content-Security-Policy:	default-src 'self'
Date:	Thu, 25 Jan 2024 11:41:58 GMT
Server:	SimpleHTTP/0.6 Python/3.12.0

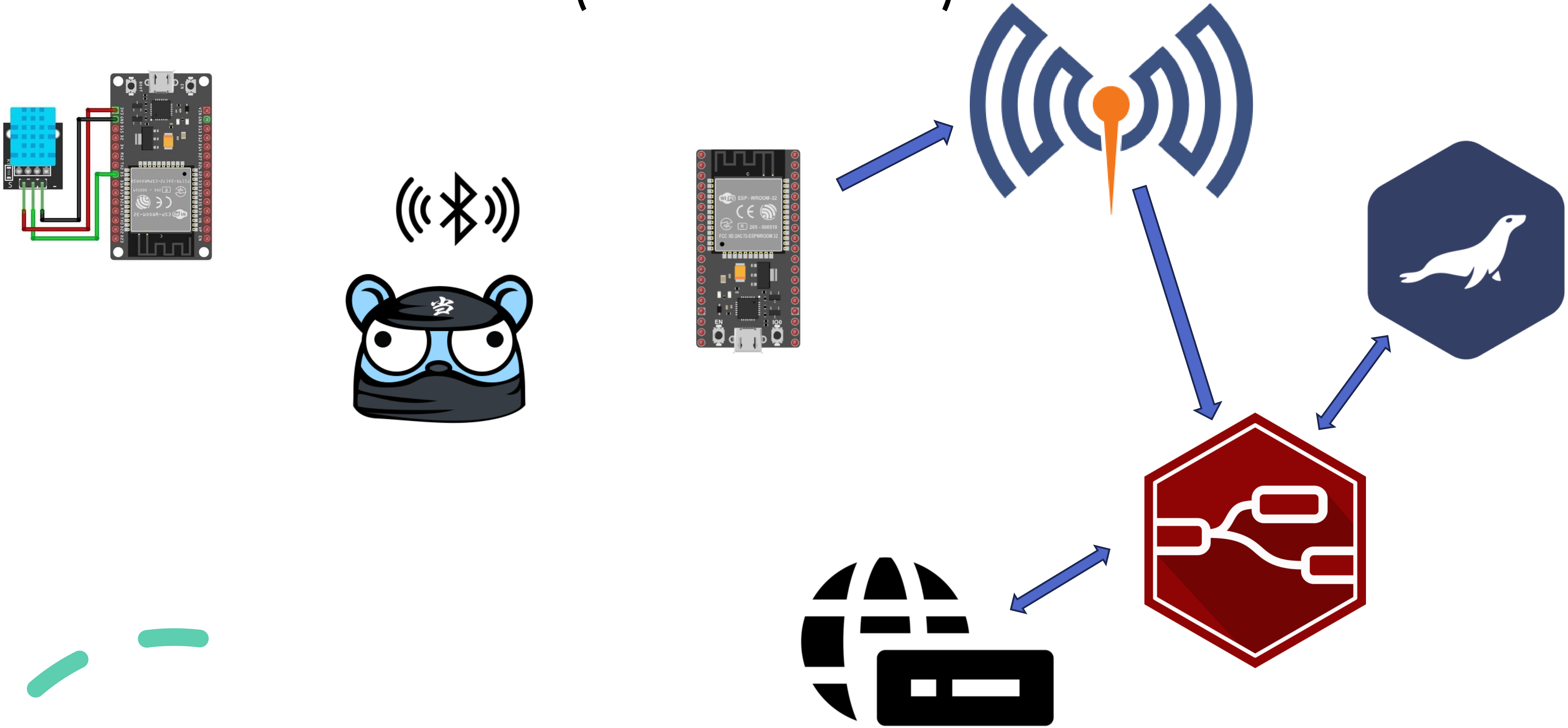
Request Headers □ Raw

Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding:	gzip, deflate, br
Accept-Language:	en-US,en;q=0.9
Authorization:	Basic cm9vdDoxMjM0NTQzMjEw
Cache-Control:	max-age=0
Connection:	keep-alive
Host:	192.168.156.226:8443

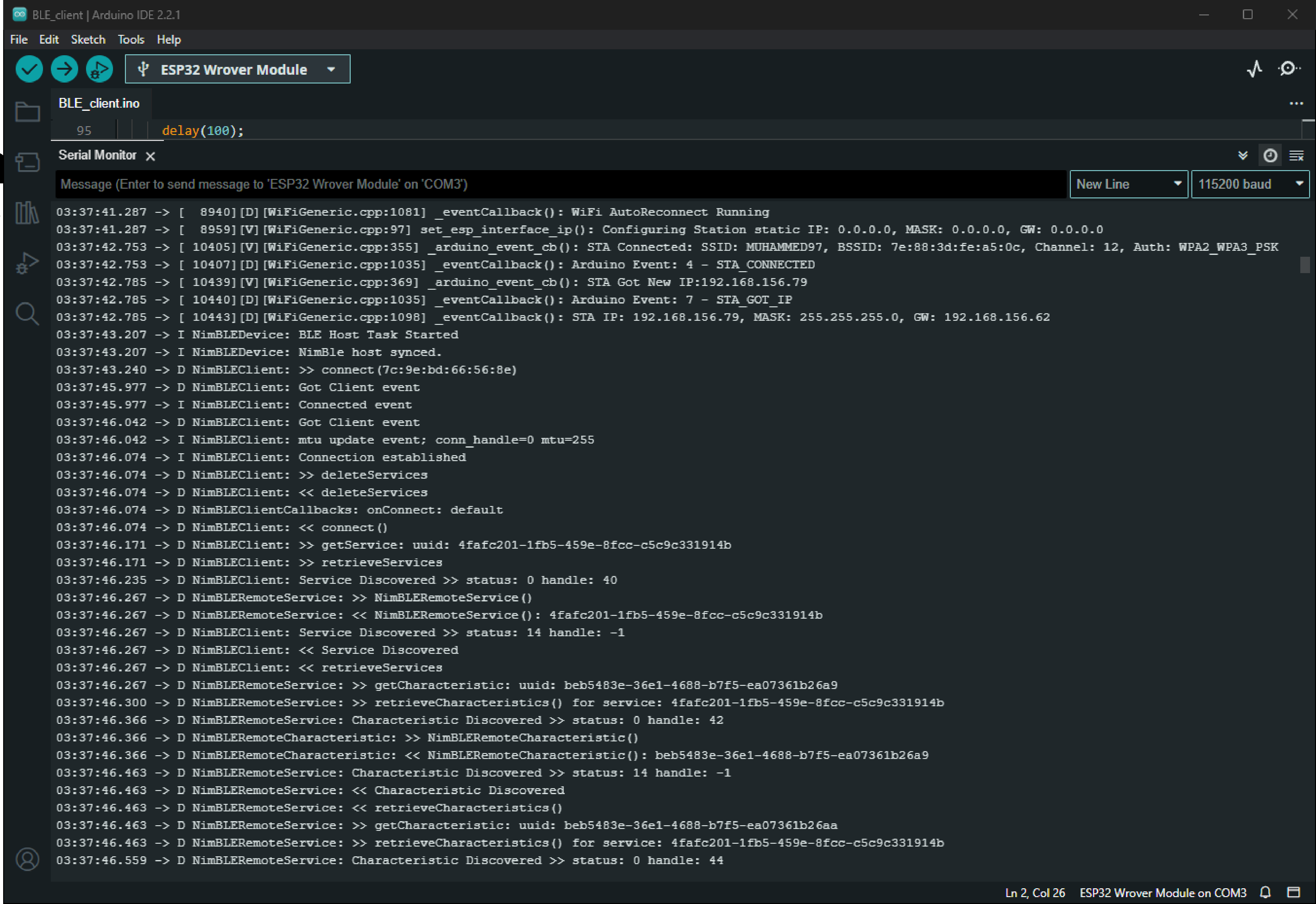
IoT Architecture (with Bluetooth)



IoT Architecture (with Bluetooth)



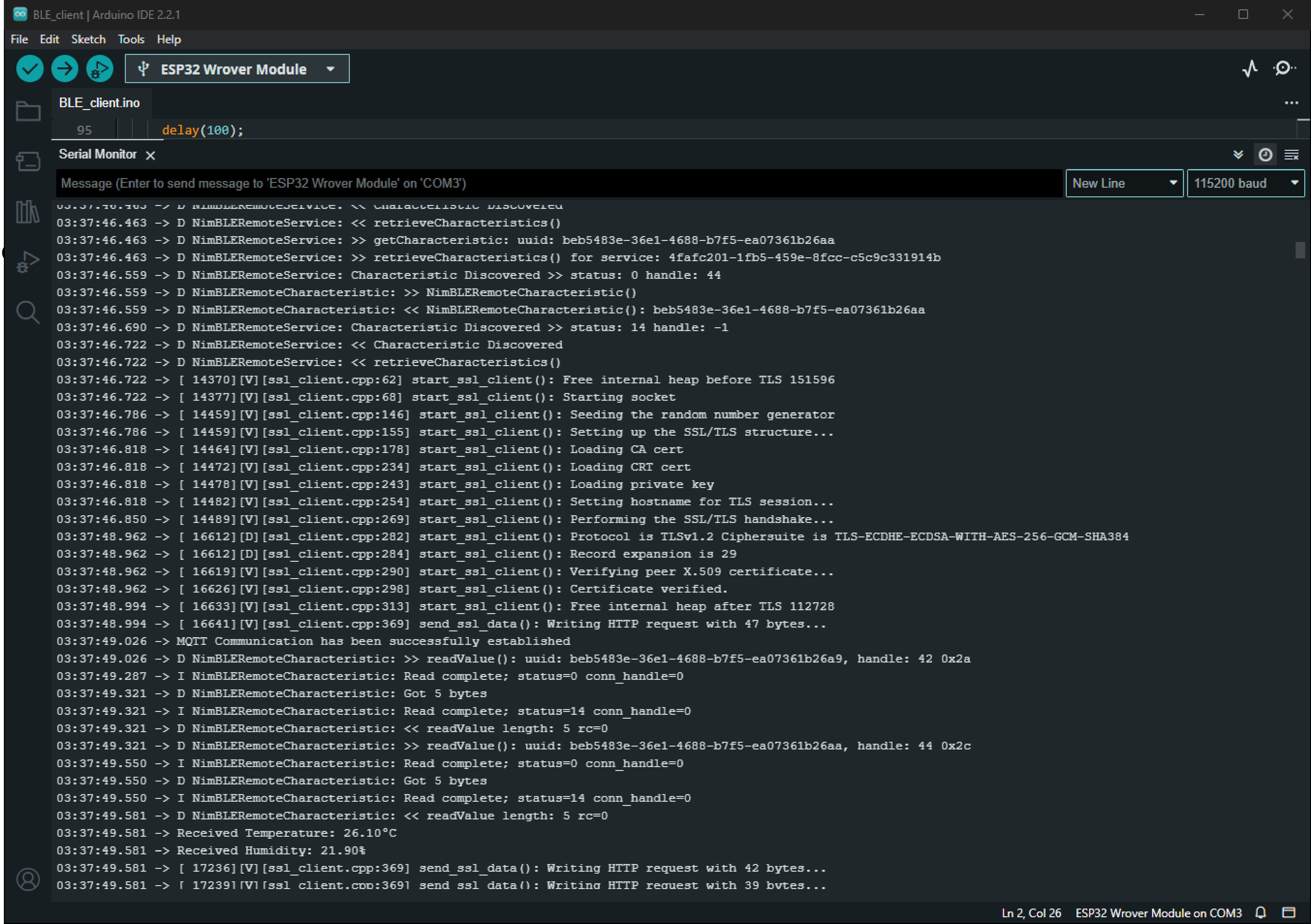
Setting Bluetooth Communi ESP32


BLE_client | Arduino IDE 2.2.1
File Edit Sketch Tools Help
ESP32 Wrover Module
BLE_client.ino
Serial Monitor ✕
Message (Enter to send message to 'ESP32 Wrover Module' on 'COM3')
New Line
115200 baud
Ln 2, Col 26 ESP32 Wrover Module on COM3

```
delay(100);
```

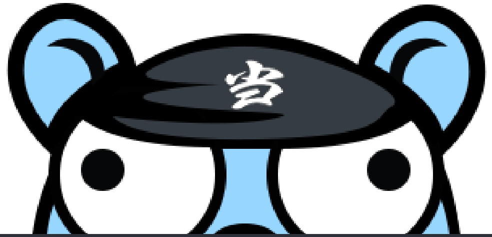
```
03:37:41.287 -> [  8940][D][WiFiGeneric.cpp:1081] _eventCallback(): WiFi AutoReconnect Running
03:37:41.287 -> [  8959][V][WiFiGeneric.cpp:97] set_esp_interface_ip(): Configuring Station static IP: 0.0.0.0, MASK: 0.0.0.0, GW: 0.0.0.0
03:37:42.753 -> [ 10405][V][WiFiGeneric.cpp:355] _arduino_event_cb(): STA Connected: SSID: MUHAMMED97, BSSID: 7e:88:3d:fe:a5:0c, Channel: 12, Auth: WPA2_WPA3_PSK
03:37:42.753 -> [ 10407][D][WiFiGeneric.cpp:1035] _eventCallback(): Arduino Event: 4 - STA_CONNECTED
03:37:42.785 -> [ 10439][V][WiFiGeneric.cpp:369] _arduino_event_cb(): STA Got New IP:192.168.156.79
03:37:42.785 -> [ 10440][D][WiFiGeneric.cpp:1035] _eventCallback(): Arduino Event: 7 - STA_GOT_IP
03:37:42.785 -> [ 10443][D][WiFiGeneric.cpp:1098] _eventCallback(): STA IP: 192.168.156.79, MASK: 255.255.255.0, GW: 192.168.156.62
03:37:43.207 -> I NimBLEDevice: BLE Host Task Started
03:37:43.207 -> I NimBLEDevice: NimBle host synced.
03:37:43.240 -> D NimBLEClient: >> connect(7c:9e:bd:66:56:8e)
03:37:45.977 -> D NimBLEClient: Got Client event
03:37:45.977 -> I NimBLEClient: Connected event
03:37:46.042 -> D NimBLEClient: Got Client event
03:37:46.042 -> I NimBLEClient: mtu update event; conn_handle=0 mtu=255
03:37:46.074 -> I NimBLEClient: Connection established
03:37:46.074 -> D NimBLEClient: >> deleteServices
03:37:46.074 -> D NimBLEClient: << deleteServices
03:37:46.074 -> D NimBLEClientCallbacks: onConnect: default
03:37:46.074 -> D NimBLEClient: << connect()
03:37:46.171 -> D NimBLEClient: >> getService: uuid: 4fafc201-1fb5-459e-8fcc-c5c9c331914b
03:37:46.171 -> D NimBLEClient: >> retrieveServices
03:37:46.235 -> D NimBLEClient: Service Discovered >> status: 0 handle: 40
03:37:46.267 -> D NimBLERemoteService: >> NimBLERemoteService()
03:37:46.267 -> D NimBLERemoteService: << NimBLERemoteService(): 4fafc201-1fb5-459e-8fcc-c5c9c331914b
03:37:46.267 -> D NimBLEClient: Service Discovered >> status: 14 handle: -1
03:37:46.267 -> D NimBLEClient: << Service Discovered
03:37:46.267 -> D NimBLEClient: << retrieveServices
03:37:46.267 -> D NimBLERemoteService: >> getCharacteristic: uuid: beb5483e-36e1-4688-b7f5-ea07361b26a9
03:37:46.300 -> D NimBLERemoteService: >> retrieveCharacteristics() for service: 4fafc201-1fb5-459e-8fcc-c5c9c331914b
03:37:46.366 -> D NimBLERemoteService: Characteristic Discovered >> status: 0 handle: 42
03:37:46.366 -> D NimBLERemoteCharacteristic: >> NimBLERemoteCharacteristic()
03:37:46.366 -> D NimBLERemoteCharacteristic: << NimBLERemoteCharacteristic(): beb5483e-36e1-4688-b7f5-ea07361b26a9
03:37:46.463 -> D NimBLERemoteService: Characteristic Discovered >> status: 14 handle: -1
03:37:46.463 -> D NimBLERemoteService: << Characteristic Discovered
03:37:46.463 -> D NimBLERemoteService: << retrieveCharacteristics()
03:37:46.463 -> D NimBLERemoteService: >> getCharacteristic: uuid: beb5483e-36e1-4688-b7f5-ea07361b26aa
03:37:46.463 -> D NimBLERemoteService: >> retrieveCharacteristics() for service: 4fafc201-1fb5-459e-8fcc-c5c9c331914b
03:37:46.559 -> D NimBLERemoteService: Characteristic Discovered >> status: 0 handle: 44
```

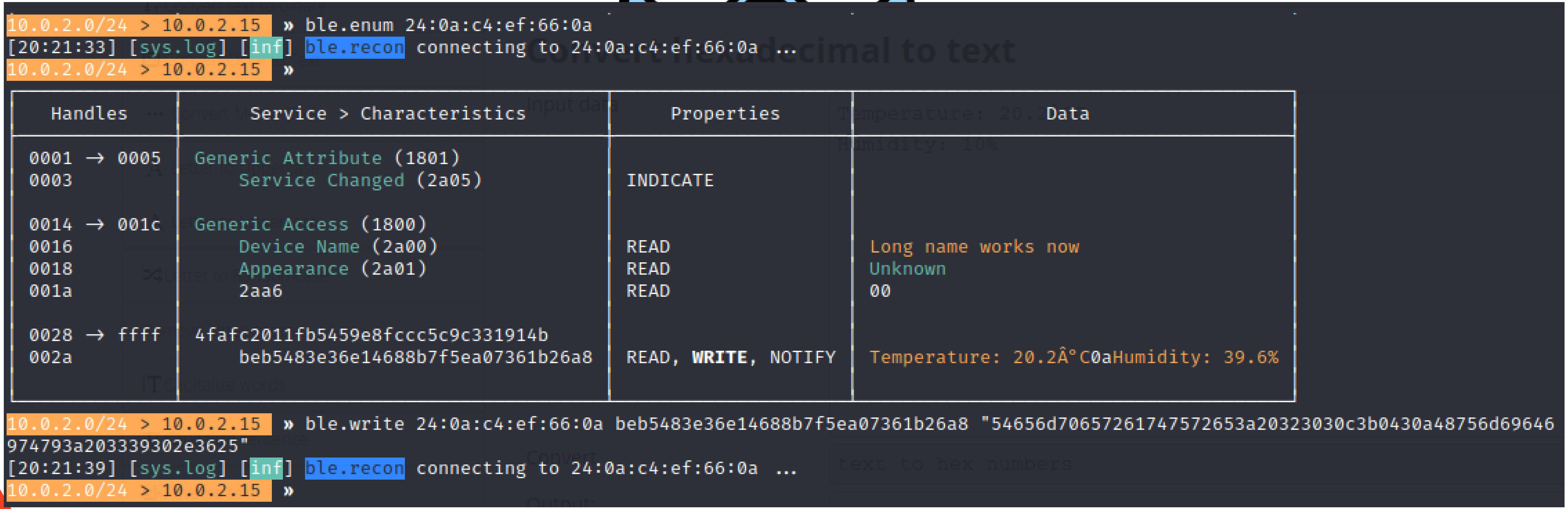
Setting Bluetooth Communic ESP32


BLE_client | Arduino IDE 2.2.1
File
Edit
Sketch
Tools
Help
ESP32 Wrover Module
BLE_client.ino
Serial Monitor
Message (Enter to send message to 'ESP32 Wrover Module' on 'COM3')
New Line
115200 baud
Ln 2, Col 26
ESP32 Wrover Module on COM3

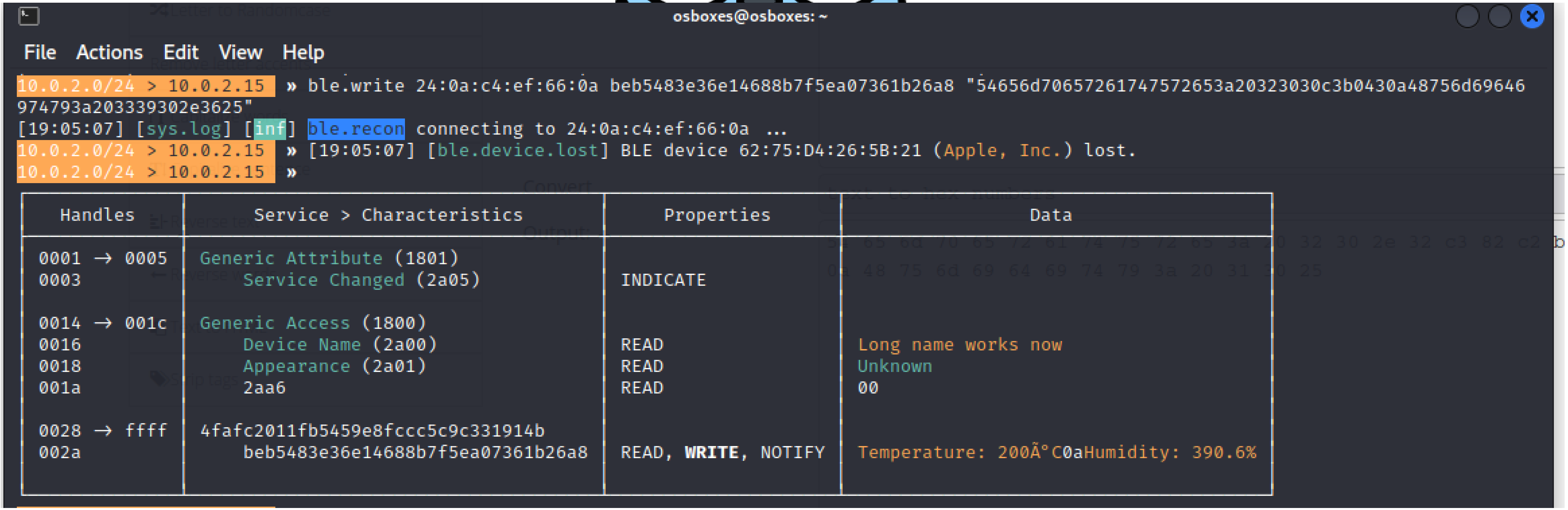
```
delay(100);
```

```
03:37:46.463 -> D NimBLERemoteService: << Characteristic Discovered
03:37:46.463 -> D NimBLERemoteService: << retrieveCharacteristics()
03:37:46.463 -> D NimBLERemoteService: >> getCharacteristic: uuid: beb5483e-36e1-4688-b7f5-ea07361b26aa
03:37:46.463 -> D NimBLERemoteService: >> retrieveCharacteristics() for service: 4fafc201-1fb5-459e-8fcc-c5c9c331914b
03:37:46.559 -> D NimBLERemoteService: Characteristic Discovered >> status: 0 handle: 44
03:37:46.559 -> D NimBLERemoteCharacteristic: >> NimBLERemoteCharacteristic()
03:37:46.559 -> D NimBLERemoteCharacteristic: << NimBLERemoteCharacteristic(): beb5483e-36e1-4688-b7f5-ea07361b26aa
03:37:46.690 -> D NimBLERemoteService: Characteristic Discovered >> status: 14 handle: -1
03:37:46.722 -> D NimBLERemoteService: << Characteristic Discovered
03:37:46.722 -> D NimBLERemoteService: << retrieveCharacteristics()
03:37:46.722 -> [ 14370][V][ssl_client.cpp:62] start_ssl_client(): Free internal heap before TLS 151596
03:37:46.722 -> [ 14377][V][ssl_client.cpp:68] start_ssl_client(): Starting socket
03:37:46.786 -> [ 14459][V][ssl_client.cpp:146] start_ssl_client(): Seeding the random number generator
03:37:46.786 -> [ 14459][V][ssl_client.cpp:155] start_ssl_client(): Setting up the SSL/TLS structure...
03:37:46.818 -> [ 14464][V][ssl_client.cpp:178] start_ssl_client(): Loading CA cert
03:37:46.818 -> [ 14472][V][ssl_client.cpp:234] start_ssl_client(): Loading CRT cert
03:37:46.818 -> [ 14478][V][ssl_client.cpp:243] start_ssl_client(): Loading private key
03:37:46.818 -> [ 14482][V][ssl_client.cpp:254] start_ssl_client(): Setting hostname for TLS session...
03:37:46.850 -> [ 14489][V][ssl_client.cpp:269] start_ssl_client(): Performing the SSL/TLS handshake...
03:37:48.962 -> [ 16612][D][ssl_client.cpp:282] start_ssl_client(): Protocol is TLSv1.2 Ciphersuite is TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384
03:37:48.962 -> [ 16612][D][ssl_client.cpp:284] start_ssl_client(): Record expansion is 29
03:37:48.962 -> [ 16619][V][ssl_client.cpp:290] start_ssl_client(): Verifying peer X.509 certificate...
03:37:48.962 -> [ 16626][V][ssl_client.cpp:298] start_ssl_client(): Certificate verified.
03:37:48.994 -> [ 16633][V][ssl_client.cpp:313] start_ssl_client(): Free internal heap after TLS 112728
03:37:48.994 -> [ 16641][V][ssl_client.cpp:369] send_ssl_data(): Writing HTTP request with 47 bytes...
03:37:49.026 -> MQTT Communication has been successfully established
03:37:49.026 -> D NimBLERemoteCharacteristic: >> readValue(): uuid: beb5483e-36e1-4688-b7f5-ea07361b26a9, handle: 42 0x2a
03:37:49.287 -> I NimBLERemoteCharacteristic: Read complete; status=0 conn_handle=0
03:37:49.321 -> D NimBLERemoteCharacteristic: Got 5 bytes
03:37:49.321 -> I NimBLERemoteCharacteristic: Read complete; status=14 conn_handle=0
03:37:49.321 -> D NimBLERemoteCharacteristic: << readValue length: 5 rc=0
03:37:49.321 -> D NimBLERemoteCharacteristic: >> readValue(): uuid: beb5483e-36e1-4688-b7f5-ea07361b26aa, handle: 44 0x2c
03:37:49.550 -> I NimBLERemoteCharacteristic: Read complete; status=0 conn_handle=0
03:37:49.550 -> D NimBLERemoteCharacteristic: Got 5 bytes
03:37:49.550 -> I NimBLERemoteCharacteristic: Read complete; status=14 conn_handle=0
03:37:49.581 -> D NimBLERemoteCharacteristic: << readValue length: 5 rc=0
03:37:49.581 -> Received Temperature: 26.10°C
03:37:49.581 -> Received Humidity: 21.90%
03:37:49.581 -> [ 17236][V][ssl_client.cpp:369] send_ssl_data(): Writing HTTP request with 42 bytes...
03:37:49.581 -> [ 17239][V][ssl_client.cpp:369] send_ssl_data(): Writing HTTP request with 39 bytes...
```

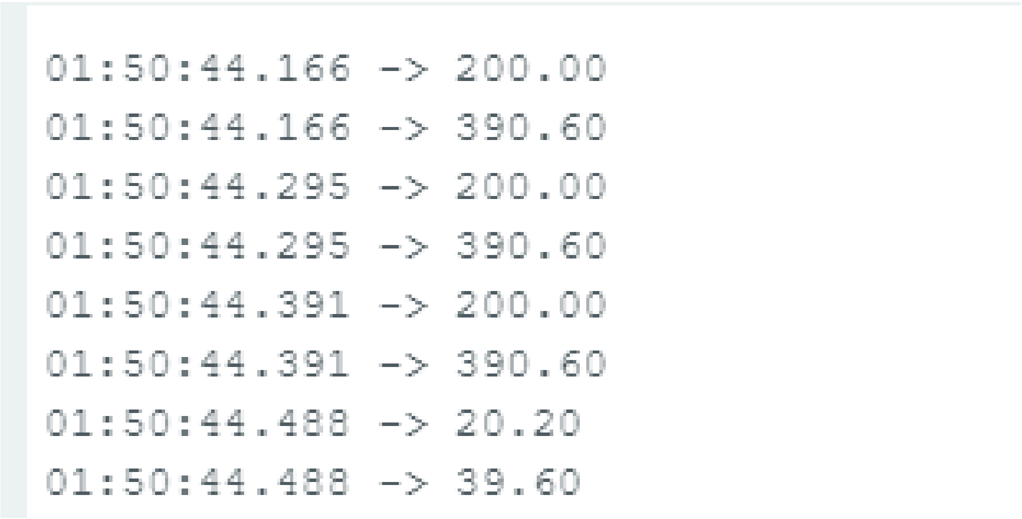




```
10.0.2.0/24 > 10.0.2.15  » ble.enum 24:0a:c4:ef:66:0a
[20:21:33] [sys.log] [inf] ble.recon connecting to 24:0a:c4:ef:66:0a ...
10.0.2.0/24 > 10.0.2.15  »

┌──────────────┬──────────────────────────────────────┬─────────────────────┬───────────────────────────────────────┐
│   Handles    │    Service > Characteristics         │     Properties      │              Data                     │
├──────────────┼──────────────────────────────────────┼─────────────────────┼───────────────────────────────────────┤
│ 0001 → 0005  │ Generic Attribute (1801)             │                     │                                       │
│ 0003         │     Service Changed (2a05)           │ INDICATE            │                                       │
│              │                                      │                     │                                       │
│ 0014 → 001c  │ Generic Access (1800)                │                     │                                       │
│ 0016         │     Device Name (2a00)               │ READ                │ Long name works now                   │
│ 0018         │     Appearance (2a01)                │ READ                │ Unknown                               │
│ 001a         │     2aa6                             │ READ                │ 00                                    │
│              │                                      │                     │                                       │
│ 0028 → ffff  │ 4fafc2011fb5459e8fccc5c9c331914b     │                     │                                       │
│ 002a         │     beb5483e36e14688b7f5ea07361b26a8 │ READ, WRITE, NOTIFY │ Temperature: 20.2Â°C0aHumidity: 39.6% │
│              │                                      │                     │                                       │
└──────────────┴──────────────────────────────────────┴─────────────────────┴───────────────────────────────────────┘

10.0.2.0/24 > 10.0.2.15  » ble.write 24:0a:c4:ef:66:0a beb5483e36e14688b7f5ea07361b26a8 "54656d706572617475726 53a20323030c3b0430a48756d69646
974793a203339302e3625"
[20:21:39] [sys.log] [inf] ble.recon connecting to 24:0a:c4:ef:66:0a ...
10.0.2.0/24 > 10.0.2.15  »
```



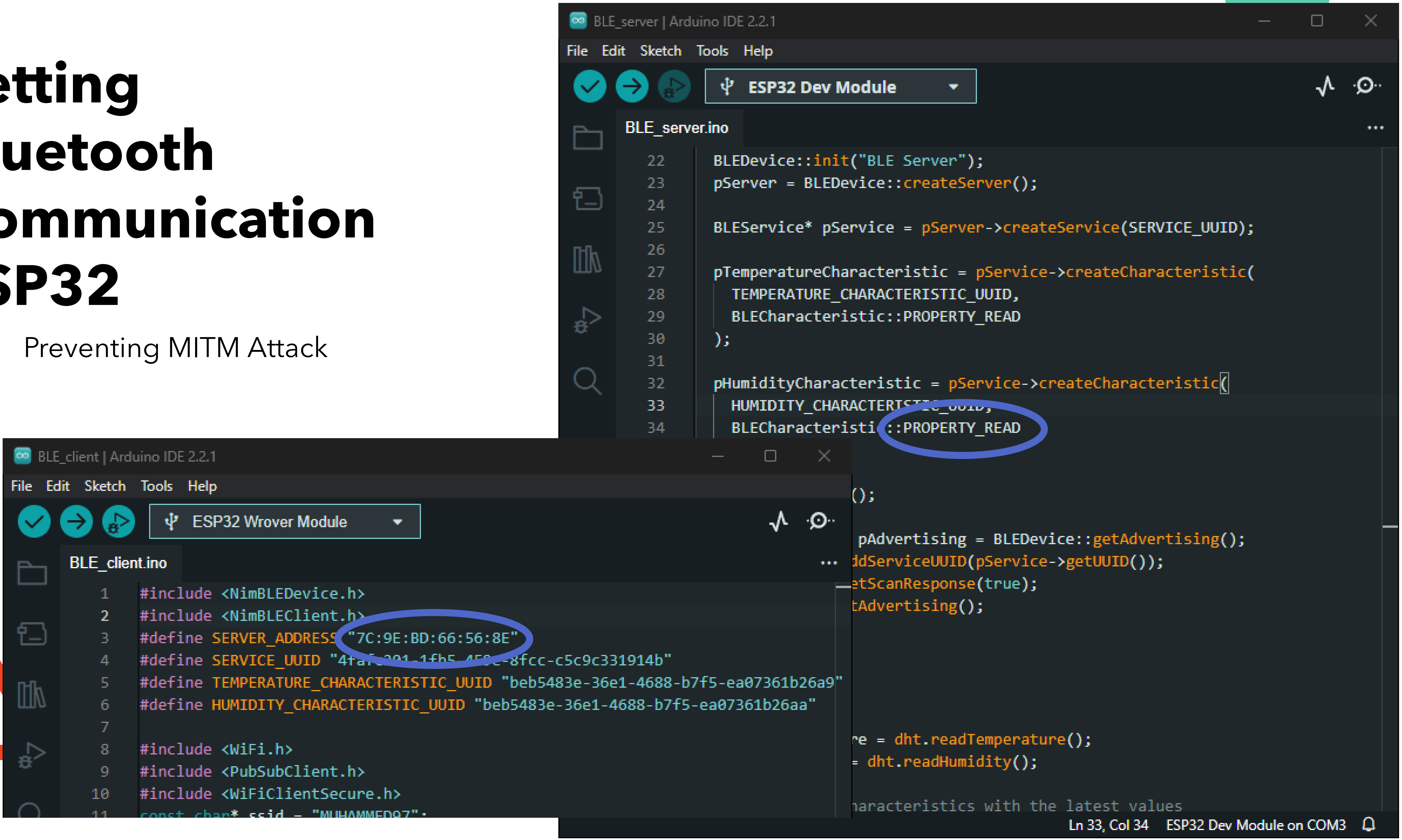
```
10.0.2.0/24 > 10.0.2.15  » ble.write 24:0a:c4:ef:66:0a beb5483e36e14688b7f5ea07361b26a8 "54656d7065726174757265a20323030c3b0430a48756d69646
974793a203339302e3625"
[19:05:07] [sys.log] [inf] ble.recon connecting to 24:0a:c4:ef:66:0a ...
10.0.2.0/24 > 10.0.2.15  » [19:05:07] [ble.device.lost] BLE device 62:75:D4:26:5B:21 (Apple, Inc.) lost.
10.0.2.0/24 > 10.0.2.15  »
┌──────────────┬───────────────────────────────────────┬──────────────────────┬─────────────────────────────────────────┐
│   Handles    │   Service > Characteristics           │      Properties      │                  Data                   │
├──────────────┼───────────────────────────────────────┼──────────────────────┼─────────────────────────────────────────┤
│ 0001 → 0005  │ Generic Attribute (1801)              │                      │                                         │
│ 0003         │     Service Changed (2a05)            │ INDICATE             │                                         │
│              │                                       │                      │                                         │
│ 0014 → 001c  │ Generic Access (1800)                 │                      │                                         │
│ 0016         │     Device Name (2a00)                │ READ                 │ Long name works now                     │
│ 0018         │     Appearance (2a01)                 │ READ                 │ Unknown                                 │
│ 001a         │     2aa6                              │ READ                 │ 00                                      │
│              │                                       │                      │                                         │
│ 0028 → ffff  │ 4fafc2011fb5459e8fccc5c9c331914b      │                      │                                         │
│ 002a         │     beb5483e36e14688b7f5ea07361b26a8  │ READ, WRITE, NOTIFY  │ Temperature: 200Â°C0aHumidity: 390.6%   │
│              │                                       │                      │                                         │
└──────────────┴───────────────────────────────────────┴──────────────────────┴─────────────────────────────────────────┘
```



```
01:50:44.166 -> 200.00
01:50:44.166 -> 390.60
01:50:44.295 -> 200.00
01:50:44.295 -> 390.60
01:50:44.391 -> 200.00
01:50:44.391 -> 390.60
01:50:44.488 -> 20.20
01:50:44.488 -> 39.60
```

Setting Bluetooth Communication ESP32

Preventing MITM Attack

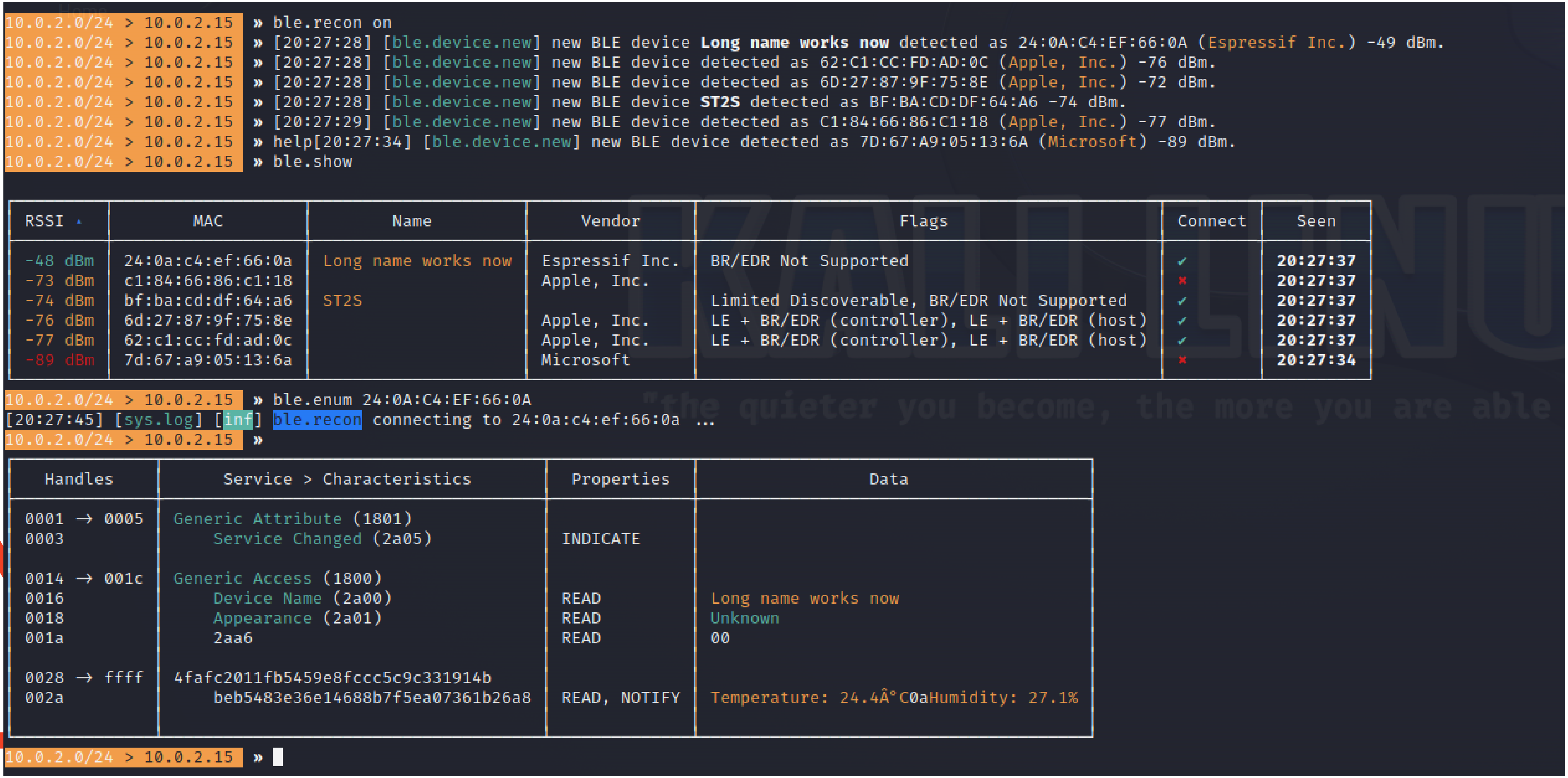


```
  BLEDevice::init("BLE Server");
  pServer = BLEDevice::createServer();

  BLEService* pService = pServer->createService(SERVICE_UUID);

  pTemperatureCharacteristic = pService->createCharacteristic(
    TEMPERATURE_CHARACTERISTIC_UUID,
    BLECharacteristic::PROPERTY_READ
  );

  pHumidityCharacteristic = pService->createCharacteristic(
    HUMIDITY_CHARACTERISTIC_UUID,
    BLECharacteristic::PROPERTY_READ
```

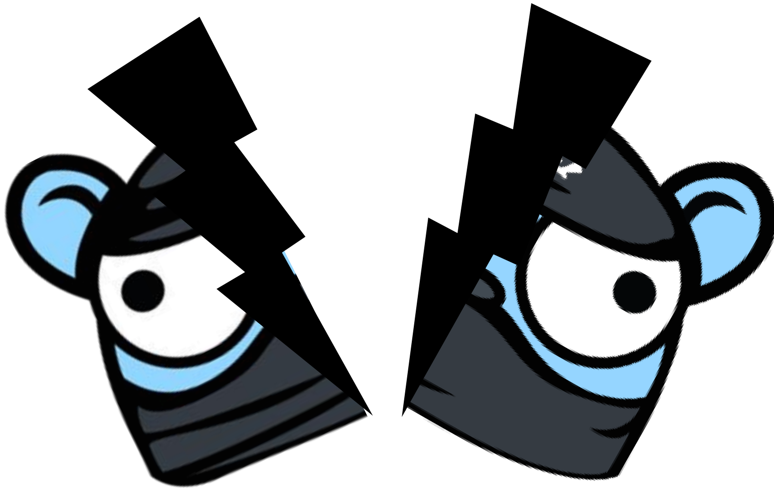
```
();

 pAdvertising = BLEDevice::getAdvertising();
ddServiceUUID(pService->getUUID());
etScanResponse(true);
tAdvertising();

re = dht.readTemperature();
= dht.readHumidity();

haracteristics with the latest values
```

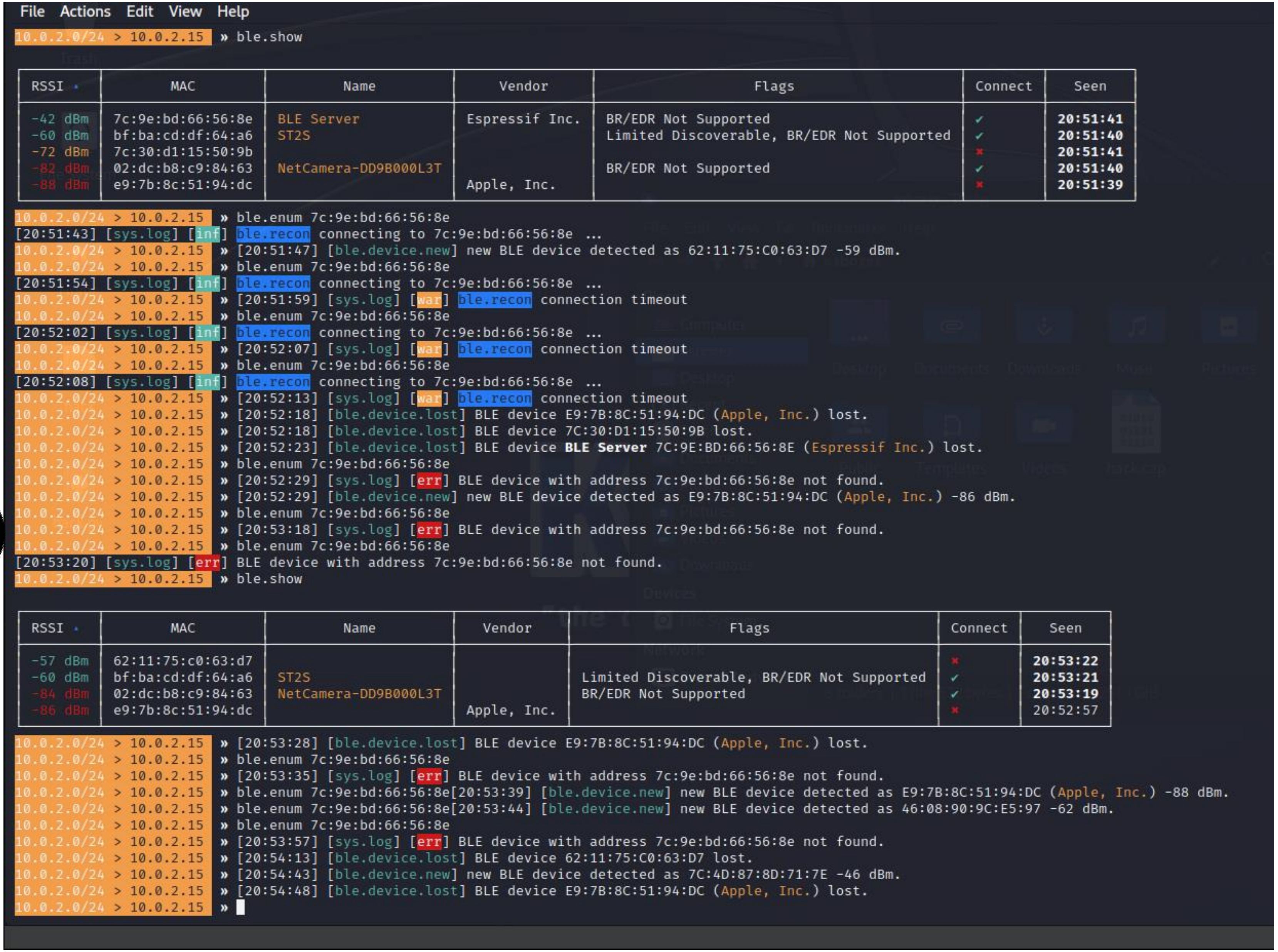
Ln 33, Col 34 ESP32 Dev Module on COM3
BLE_client | Arduino IDE 2.2.1
File Edit Sketch Tools Help
ESP32 Wrover Module
BLE_client.ino

```
#include <NimBLEDevice.h>
#include <NimBLEClient.h>
#define SERVER_ADDRESS "7C:9E:BD:66:56:8E"
#define SERVICE_UUID "4fafc201-1fb5-459e-8fcc-c5c9c331914b"
#define TEMPERATURE_CHARACTERISTIC_UUID "beb5483e-36e1-4688-b7f5-ea07361b26a9"
#define HUMIDITY_CHARACTERISTIC_UUID "beb5483e-36e1-4688-b7f5-ea07361b26aa"

#include <WiFi.h>
#include <PubSubClient.h>
#include <WiFiClientSecure.h>
const char* ssid = "MUHAMMED97";
```



```
10.0.2.0/24 > 10.0.2.15  » ble.recon on
10.0.2.0/24 > 10.0.2.15  » [20:27:28] [ble.device.new] new BLE device Long name works now detected as 24:0A:C4:EF:66:0A (Espressif Inc.) -49 dBm.
10.0.2.0/24 > 10.0.2.15  » [20:27:28] [ble.device.new] new BLE device detected as 62:C1:CC:FD:AD:0C (Apple, Inc.) -76 dBm.
10.0.2.0/24 > 10.0.2.15  » [20:27:28] [ble.device.new] new BLE device detected as 6D:27:87:9F:75:8E (Apple, Inc.) -72 dBm.
10.0.2.0/24 > 10.0.2.15  » [20:27:28] [ble.device.new] new BLE device ST2S detected as BF:BA:CD:DF:64:A6 -74 dBm.
10.0.2.0/24 > 10.0.2.15  » [20:27:29] [ble.device.new] new BLE device detected as C1:84:66:86:C1:18 (Apple, Inc.) -77 dBm.
10.0.2.0/24 > 10.0.2.15  » help[20:27:34] [ble.device.new] new BLE device detected as 7D:67:A9:05:13:6A (Microsoft) -89 dBm.
10.0.2.0/24 > 10.0.2.15  » ble.show

┌─────────┬───────────────────┬─────────────────────┬─────────────────┬───────────────────────────────────────────────┬─────────┬──────────┐
│ RSSI ▴  │        MAC        │        Name         │     Vendor      │                     Flags                     │ Connect │   Seen   │
├─────────┼───────────────────┼─────────────────────┼─────────────────┼───────────────────────────────────────────────┼─────────┼──────────┤
│ -48 dBm │ 24:0a:c4:ef:66:0a │ Long name works now │ Espressif Inc.  │ BR/EDR Not Supported                          │ ✔       │ 20:27:37 │
│ -73 dBm │ c1:84:66:86:c1:18 │                     │ Apple, Inc.     │                                               │ ✖       │ 20:27:37 │
│ -74 dBm │ bf:ba:cd:df:64:a6 │ ST2S                │                 │ Limited Discoverable, BR/EDR Not Supported    │ ✔       │ 20:27:37 │
│ -76 dBm │ 6d:27:87:9f:75:8e │                     │ Apple, Inc.     │ LE + BR/EDR (controller), LE + BR/EDR (host)  │ ✔       │ 20:27:37 │
│ -77 dBm │ 62:c1:cc:fd:ad:0c │                     │ Apple, Inc.     │ LE + BR/EDR (controller), LE + BR/EDR (host)  │ ✔       │ 20:27:37 │
│ -89 dBm │ 7d:67:a9:05:13:6a │                     │ Microsoft       │                                               │ ✖       │ 20:27:34 │
└─────────┴───────────────────┴─────────────────────┴─────────────────┴───────────────────────────────────────────────┴─────────┴──────────┘

10.0.2.0/24 > 10.0.2.15  » ble.enum 24:0A:C4:EF:66:0A
[20:27:45] [sys.log] [inf] ble.recon connecting to 24:0a:c4:ef:66:0a ...
10.0.2.0/24 > 10.0.2.15  »

┌──────────────┬───────────────────────────────────────┬───────────────┬────────────────────────────────────────┐
│   Handles    │       Service > Characteristics       │  Properties   │                  Data                  │
├──────────────┼───────────────────────────────────────┼───────────────┼────────────────────────────────────────┤
│ 0001 -> 0005 │ Generic Attribute (1801)              │               │                                        │
│ 0003         │     Service Changed (2a05)            │ INDICATE      │                                        │
│              │                                       │               │                                        │
│ 0014 -> 001c │ Generic Access (1800)                 │               │                                        │
│ 0016         │     Device Name (2a00)                │ READ          │ Long name works now                    │
│ 0018         │     Appearance (2a01)                 │ READ          │ Unknown                                │
│ 001a         │     2aa6                              │ READ          │ 00                                     │
│              │                                       │               │                                        │
│ 0028 -> ffff │ 4fafc2011fb5459e8fccc5c9c331914b      │               │                                        │
│ 002a         │     beb5483e36e14688b7f5ea07361b26a8  │ READ, NOTIFY  │ Temperature: 24.4Â°C0aHumidity: 27.1%  │
│              │                                       │               │                                        │
└──────────────┴───────────────────────────────────────┴───────────────┴────────────────────────────────────────┘

10.0.2.0/24 > 10.0.2.15  » █
```





```
10.0.2.0/24 > 10.0.2.15  » ble.show

┌─────────┬───────────────────┬──────────────────────┬──────────────────┬─────────────────────────────────────────────┬─────────┬──────────┐
│ RSSI ▴  │        MAC        │         Name         │      Vendor      │                    Flags                    │ Connect │   Seen   │
├─────────┼───────────────────┼──────────────────────┼──────────────────┼─────────────────────────────────────────────┼─────────┼──────────┤
│ -42 dBm │ 7c:9e:bd:66:56:8e │ BLE Server           │ Espressif Inc.   │ BR/EDR Not Supported                        │ ✔       │ 20:51:41 │
│ -60 dBm │ bf:ba:cd:df:64:a6 │ ST2S                 │                  │ Limited Discoverable, BR/EDR Not Supported  │ ✔       │ 20:51:40 │
│ -72 dBm │ 7c:30:d1:15:50:9b │                      │                  │                                             │ ✖       │ 20:51:41 │
│ -82 dBm │ 02:dc:b8:c9:84:63 │ NetCamera-DD9B000L3T │                  │ BR/EDR Not Supported                        │ ✔       │ 20:51:40 │
│ -88 dBm │ e9:7b:8c:51:94:dc │                      │ Apple, Inc.      │                                             │ ✖       │ 20:51:39 │
└─────────┴───────────────────┴──────────────────────┴──────────────────┴─────────────────────────────────────────────┴─────────┴──────────┘

10.0.2.0/24 > 10.0.2.15  » ble.enum 7c:9e:bd:66:56:8e
[20:51:43] [sys.log] [inf] ble.recon connecting to 7c:9e:bd:66:56:8e ...
10.0.2.0/24 > 10.0.2.15  » [20:51:47] [ble.device.new] new BLE device detected as 62:11:75:C0:63:D7 -59 dBm.
10.0.2.0/24 > 10.0.2.15  » ble.enum 7c:9e:bd:66:56:8e
[20:51:54] [sys.log] [inf] ble.recon connecting to 7c:9e:bd:66:56:8e ...
10.0.2.0/24 > 10.0.2.15  » [20:51:59] [sys.log] [war] ble.recon connection timeout
10.0.2.0/24 > 10.0.2.15  » ble.enum 7c:9e:bd:66:56:8e
[20:52:02] [sys.log] [inf] ble.recon connecting to 7c:9e:bd:66:56:8e ...
10.0.2.0/24 > 10.0.2.15  » [20:52:07] [sys.log] [war] ble.recon connection timeout
10.0.2.0/24 > 10.0.2.15  » ble.enum 7c:9e:bd:66:56:8e
[20:52:08] [sys.log] [inf] ble.recon connecting to 7c:9e:bd:66:56:8e ...
10.0.2.0/24 > 10.0.2.15  » [20:52:13] [sys.log] [war] ble.recon connection timeout
10.0.2.0/24 > 10.0.2.15  » [20:52:18] [ble.device.lost] BLE device E9:7B:8C:51:94:DC (Apple, Inc.) lost.
10.0.2.0/24 > 10.0.2.15  » [20:52:18] [ble.device.lost] BLE device 7C:30:D1:15:50:9B lost.
10.0.2.0/24 > 10.0.2.15  » [20:52:23] [ble.device.lost] BLE device BLE Server 7C:9E:BD:66:56:8E (Espressif Inc.) lost.
10.0.2.0/24 > 10.0.2.15  » ble.enum 7c:9e:bd:66:56:8e
10.0.2.0/24 > 10.0.2.15  » [20:52:29] [sys.log] [err] BLE device with address 7c:9e:bd:66:56:8e not found.
10.0.2.0/24 > 10.0.2.15  » [20:52:29] [ble.device.new] new BLE device detected as E9:7B:8C:51:94:DC (Apple, Inc.) -86 dBm.
10.0.2.0/24 > 10.0.2.15  » ble.enum 7c:9e:bd:66:56:8e
10.0.2.0/24 > 10.0.2.15  » [20:53:18] [sys.log] [err] BLE device with address 7c:9e:bd:66:56:8e not found.
10.0.2.0/24 > 10.0.2.15  » ble.enum 7c:9e:bd:66:56:8e
[20:53:20] [sys.log] [err] BLE device with address 7c:9e:bd:66:56:8e not found.
10.0.2.0/24 > 10.0.2.15  » ble.show

┌─────────┬───────────────────┬──────────────────────┬─────────────┬─────────────────────────────────────────────┬─────────┬──────────┐
│ RSSI ▴  │        MAC        │         Name         │   Vendor    │                    Flags                    │ Connect │   Seen   │
├─────────┼───────────────────┼──────────────────────┼─────────────┼─────────────────────────────────────────────┼─────────┼──────────┤
│ -57 dBm │ 62:11:75:c0:63:d7 │                      │             │                                             │ ✖       │ 20:53:22 │
│ -60 dBm │ bf:ba:cd:df:64:a6 │ ST2S                 │             │ Limited Discoverable, BR/EDR Not Supported  │ ✔       │ 20:53:21 │
│ -84 dBm │ 02:dc:b8:c9:84:63 │ NetCamera-DD9B000L3T │             │ BR/EDR Not Supported                        │ ✔       │ 20:53:19 │
│ -86 dBm │ e9:7b:8c:51:94:dc │                      │ Apple, Inc. │                                             │ ✖       │ 20:52:57 │
└─────────┴───────────────────┴──────────────────────┴─────────────┴─────────────────────────────────────────────┴─────────┴──────────┘

10.0.2.0/24 > 10.0.2.15  » [20:53:28] [ble.device.lost] BLE device E9:7B:8C:51:94:DC (Apple, Inc.) lost.
10.0.2.0/24 > 10.0.2.15  » ble.enum 7c:9e:bd:66:56:8e
10.0.2.0/24 > 10.0.2.15  » [20:53:35] [sys.log] [err] BLE device with address 7c:9e:bd:66:56:8e not found.
10.0.2.0/24 > 10.0.2.15  » ble.enum 7c:9e:bd:66:56:8e[20:53:39] [ble.device.new] new BLE device detected as E9:7B:8C:51:94:DC (Apple, Inc.) -88 dBm.
10.0.2.0/24 > 10.0.2.15  » ble.enum 7c:9e:bd:66:56:8e[20:53:44] [ble.device.new] new BLE device detected as 46:08:90:9C:E5:97 -62 dBm.
10.0.2.0/24 > 10.0.2.15  » ble.enum 7c:9e:bd:66:56:8e
10.0.2.0/24 > 10.0.2.15  » [20:53:57] [sys.log] [err] BLE device with address 7c:9e:bd:66:56:8e not found.
10.0.2.0/24 > 10.0.2.15  » [20:54:13] [ble.device.lost] BLE device 62:11:75:C0:63:D7 lost.
10.0.2.0/24 > 10.0.2.15  » [20:54:43] [ble.device.new] new BLE device detected as 7C:4D:87:8D:71:7E -46 dBm.
10.0.2.0/24 > 10.0.2.15  » [20:54:48] [ble.device.lost] BLE device E9:7B:8C:51:94:DC (Apple, Inc.) lost.
10.0.2.0/24 > 10.0.2.15  » █
```

Thanks ...