113-1
ICS CYBERSECURITY

FINAL REPORT

B10209040 陳彥倫

TASK DESCRIPTION

: Plot PLC(192.168.1.19)'s register 0 value --- the water level, and its trend.

TOOL

Programming language: Python

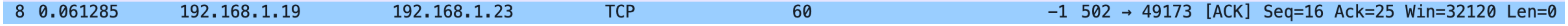
Library: Scapy, Panda, Matplotlib, Numpy ···

APPROACH

According to the provided tips, I set up some filters such as source and destination ip (192.168.1.19 & 192.168.1.23) and protocol (Modbus). To find the values of water levels, we can find those request packets with **Reference number = 0**, and then we can read the **Register 0** of their corresponding response packets.

APPROACH

For my first approach, I found out that I was not able to get all the Register 0 values. And it turned out that the method I chose to catch the packets right after the request packets was wrong, because I forgot to add “function code != none” as one of the filters. As a result, the program may return some void value from time to time.



```
8 0.061285      192.168.1.19        192.168.1.23        TCP                 60                                  -1  502 → 49173 [ACK] Seq=16 Ack=25 Win=32120 Len=0
```

Figure 1. The example packet that could be counted in if the filter is not correct.

CODE STRUCTURE

- Import libraries
- Functions to get important values (Reference number, Register 0)
- Functions to execute the filter process (store valid packets as a new pcap file, and then do another round of filtering)
- Plot the result

RESULT

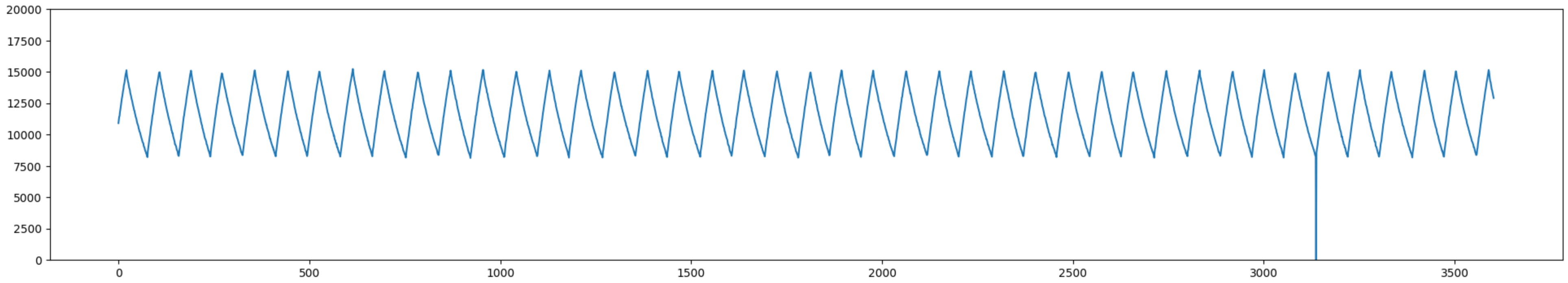
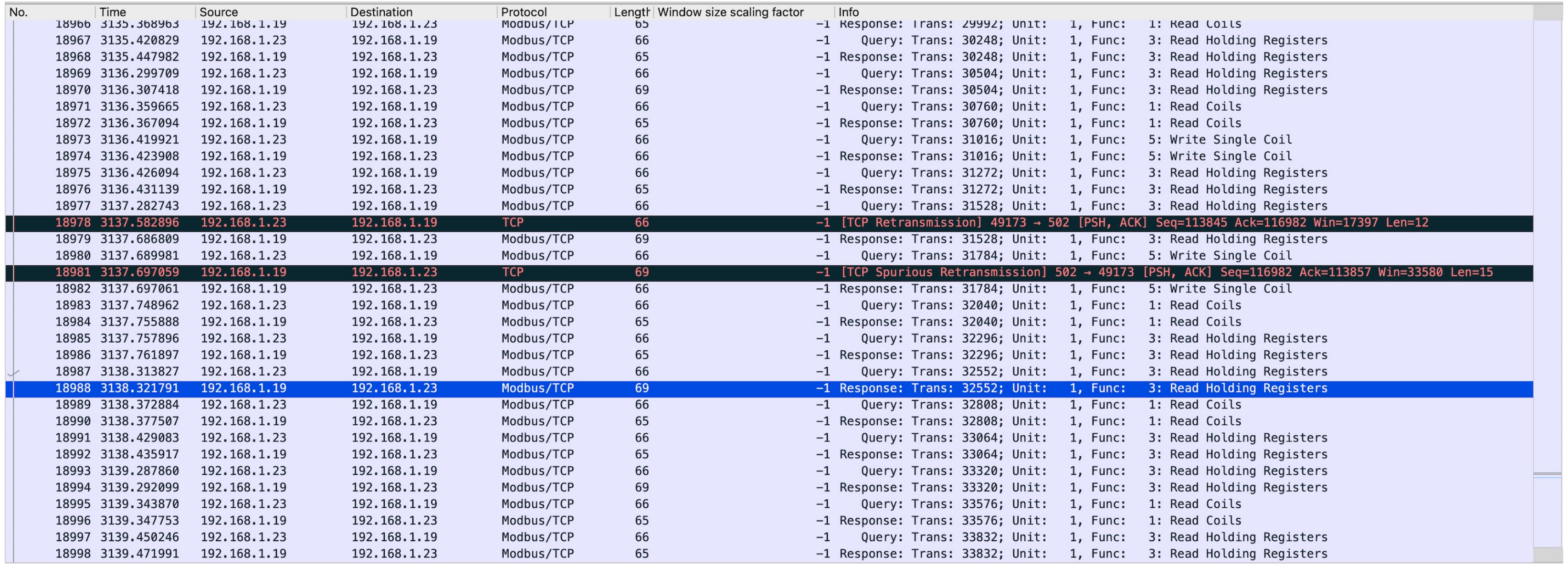


Figure 2. The water level trend

RESULT

From Figure 2, we can spot that there is a 0 around t = 3100.



No.	Time	Source	Destination	Protocol	Length	Window size scaling factor	Info
18966	3135.368963	192.168.1.19	192.168.1.23	Modbus/TCP	65	-1	Response: Trans: 29992; Unit: 1, Func: 1: Read Coils
18967	3135.420829	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 30248; Unit: 1, Func: 3: Read Holding Registers
18968	3135.447982	192.168.1.19	192.168.1.23	Modbus/TCP	65	-1	Response: Trans: 30248; Unit: 1, Func: 3: Read Holding Registers
18969	3136.299709	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 30504; Unit: 1, Func: 3: Read Holding Registers
18970	3136.307418	192.168.1.19	192.168.1.23	Modbus/TCP	69	-1	Response: Trans: 30504; Unit: 1, Func: 3: Read Holding Registers
18971	3136.359665	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 30760; Unit: 1, Func: 1: Read Coils
18972	3136.367094	192.168.1.19	192.168.1.23	Modbus/TCP	65	-1	Response: Trans: 30760; Unit: 1, Func: 1: Read Coils
18973	3136.419921	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 31016; Unit: 1, Func: 5: Write Single Coil
18974	3136.423908	192.168.1.19	192.168.1.23	Modbus/TCP	66	-1	Response: Trans: 31016; Unit: 1, Func: 5: Write Single Coil
18975	3136.426094	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 31272; Unit: 1, Func: 3: Read Holding Registers
18976	3136.431139	192.168.1.19	192.168.1.23	Modbus/TCP	65	-1	Response: Trans: 31272; Unit: 1, Func: 3: Read Holding Registers
18977	3137.282743	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 31528; Unit: 1, Func: 3: Read Holding Registers
18978	3137.582896	192.168.1.23	192.168.1.19	TCP	66	-1	[TCP Retransmission] 49173 → 502 [PSH, ACK] Seq=113845 Ack=116982 Win=17397 Len=12
18979	3137.686809	192.168.1.19	192.168.1.23	Modbus/TCP	69	-1	Response: Trans: 31528; Unit: 1, Func: 3: Read Holding Registers
18980	3137.689981	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 31784; Unit: 1, Func: 5: Write Single Coil
18981	3137.697059	192.168.1.19	192.168.1.23	TCP	69	-1	[TCP Spurious Retransmission] 502 → 49173 [PSH, ACK] Seq=116982 Ack=113857 Win=33580 Len=15
18982	3137.697061	192.168.1.19	192.168.1.23	Modbus/TCP	66	-1	Response: Trans: 31784; Unit: 1, Func: 5: Write Single Coil
18983	3137.748962	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 32040; Unit: 1, Func: 1: Read Coils
18984	3137.755888	192.168.1.19	192.168.1.23	Modbus/TCP	65	-1	Response: Trans: 32040; Unit: 1, Func: 1: Read Coils
18985	3137.757896	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 32296; Unit: 1, Func: 3: Read Holding Registers
18986	3137.761897	192.168.1.19	192.168.1.23	Modbus/TCP	65	-1	Response: Trans: 32296; Unit: 1, Func: 3: Read Holding Registers
18987	3138.313827	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 32552; Unit: 1, Func: 3: Read Holding Registers
18988	3138.321791	192.168.1.19	192.168.1.23	Modbus/TCP	69	-1	Response: Trans: 32552; Unit: 1, Func: 3: Read Holding Registers
18989	3138.372884	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 32808; Unit: 1, Func: 1: Read Coils
18990	3138.377507	192.168.1.19	192.168.1.23	Modbus/TCP	65	-1	Response: Trans: 32808; Unit: 1, Func: 1: Read Coils
18991	3138.429083	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 33064; Unit: 1, Func: 3: Read Holding Registers
18992	3138.435917	192.168.1.19	192.168.1.23	Modbus/TCP	65	-1	Response: Trans: 33064; Unit: 1, Func: 3: Read Holding Registers
18993	3139.287860	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 33320; Unit: 1, Func: 3: Read Holding Registers
18994	3139.292099	192.168.1.19	192.168.1.23	Modbus/TCP	69	-1	Response: Trans: 33320; Unit: 1, Func: 3: Read Holding Registers
18995	3139.343870	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 33576; Unit: 1, Func: 1: Read Coils
18996	3139.347753	192.168.1.19	192.168.1.23	Modbus/TCP	65	-1	Response: Trans: 33576; Unit: 1, Func: 1: Read Coils
18997	3139.450246	192.168.1.23	192.168.1.19	Modbus/TCP	66	-1	Query: Trans: 33832; Unit: 1, Func: 3: Read Holding Registers
18998	3139.471991	192.168.1.19	192.168.1.23	Modbus/TCP	65	-1	Response: Trans: 33832; Unit: 1, Func: 3: Read Holding Registers

Figure 3. Wireshark record at t = 3137

RESULT

Clearly, the outlier comes from the spurious tcp retransmission and the write function. Since the MAC address are the same as the rest of the packets, so this might not be a Man-in-the-middle attack. For those normal results, we can see that the water level shows a periodical up-and-down pattern.