

## 1. Введение.

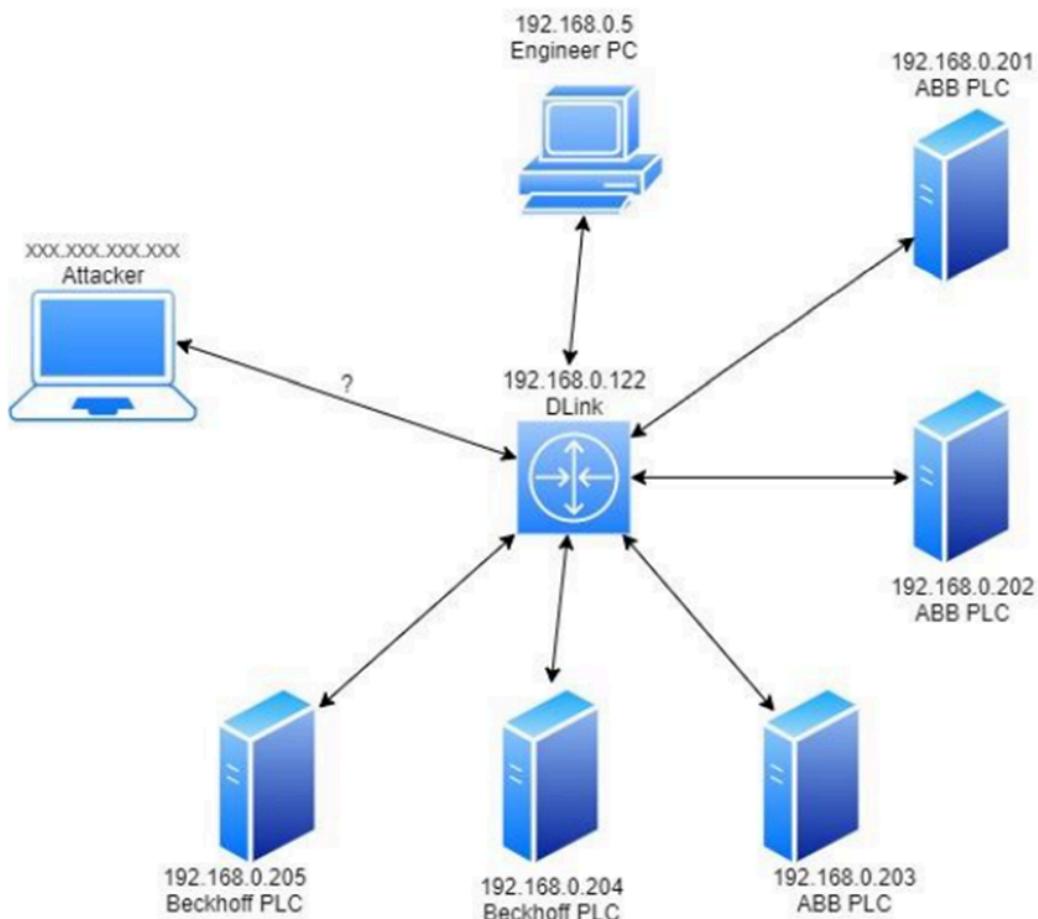
Цель и задачи задания.

В рамках данной лабораторной работы вам предстоит провести анализ дампа трафика, собранного в промышленной сети, где используется протокол Modbus. В сети существует топология, в которой одно устройство выполняет роль Master, а другие устройства — Slave.

Вам нужно:

- Определить, какие из устройств в трафике являются Master и Slave.
- Найти уникальную пару «запрос-ответ», где происходит операция записи регистров, так как в остальном трафике содержатся только запросы на чтение.
- На основе топологической карты сети и данных анализа трафика оценить, могло ли происходить вторжение на момент записи трафика.

Карта топологии сети:



Немного информации о протоколе Modbus:

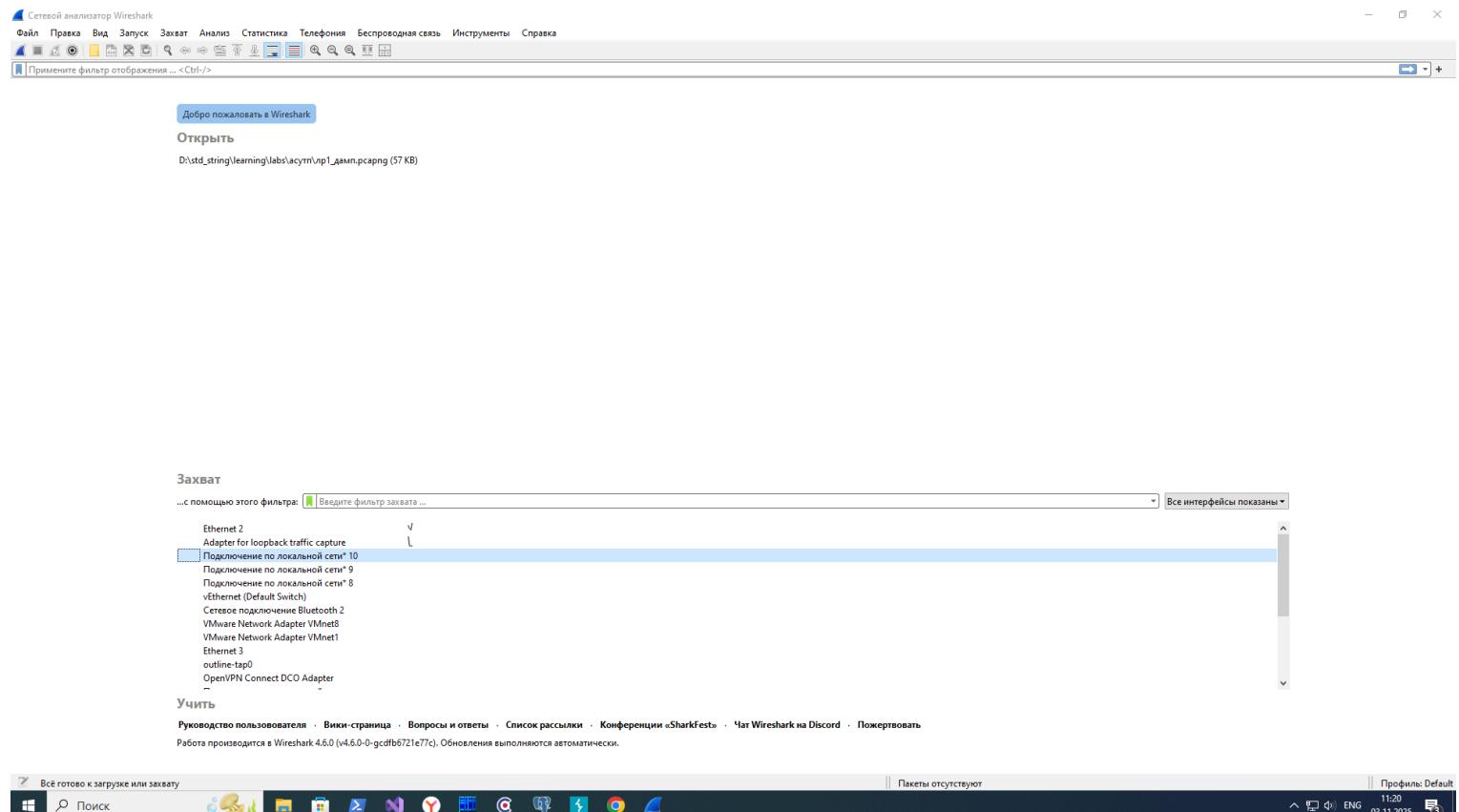
Контроллеры на шине Modbus взаимодействуют, используя модель ведущий — ведомый, основанную на транзакциях, состоящих из запроса и ответа.

Обычно в сети есть только одно ведущее client (по старой терминологии master) устройство, и несколько ведомых server (по старой терминологии slave) устройств. (Терминология верна, несмотря на противоположные значения в типичной

клиент-серверной архитектуре.) Ведущее устройство инициирует транзакции (передает запросы). Ведущий может адресовать запрос индивидуально любому ведомому или инициировать передачу широковещательного сообщения для всех ведомых устройств. Ведомое устройство, опознав свой адрес, отвечает на запрос, адресованный именно ему. При получении широковещательного запроса ответ ведомыми устройствами не формируется.

## 2. Анализ сетевого трафика.

Запускаю Wireshark:



Загружаю дамп трафика:

Примените фильтр отображения ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52233; Unit: 201, Func: 4: Read Input Registers
2	0.000050	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 201, Func: 4: Read Input Registers
3	0.000641	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52233; Unit: 201, Func: 2: Read Discrete Inputs
4	0.000917	192.168.0.201	192.168.0.5	Modbus/TCP	66	Response: Trans: 52233; Unit: 201, Func: 2: Read Discrete Inputs
5	0.001007	192.168.0.5	192.168.0.202	Modbus/TCP	66	Query: Trans: 52233; Unit: 202, Func: 4: Read Input Registers
6	0.001388	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 202, Func: 4: Read Input Registers
7	0.001418	192.168.0.5	192.168.0.202	Modbus/TCP	66	Query: Trans: 52233; Unit: 202, Func: 2: Read Discrete Inputs
8	0.001649	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 202, Func: 2: Read Discrete Inputs
9	0.001737	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 52233; Unit: 203, Func: 4: Read Input Registers
10	0.001964	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 203, Func: 4: Read Input Registers
11	0.002055	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 52233; Unit: 203, Func: 2: Read Discrete Inputs
12	0.002259	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 203, Func: 2: Read Discrete Inputs
13	0.002337	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 52233; Unit: 204, Func: 4: Read Input Registers
14	0.002551	192.168.0.204	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 204, Func: 4: Read Input Registers
15	0.002661	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 52233; Unit: 204, Func: 2: Read Discrete Inputs
16	0.002839	192.168.0.204	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 204, Func: 2: Read Discrete Inputs
17	0.002949	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 52233; Unit: 205, Func: 4: Read Input Registers
18	0.003159	192.168.0.205	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 205, Func: 4: Read Input Registers
19	0.003237	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 52233; Unit: 205, Func: 2: Read Discrete Inputs
20	0.003468	192.168.0.205	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 205, Func: 2: Read Discrete Inputs
21	0.202795	192.168.0.5	192.168.0.201	TCP	66	049463 + 592 [ACK] Seq=25 Ack=69 Win=254 Len=0
22	0.218268	192.168.0.5	192.168.0.204	TCP	66	049466 + 582 [ACK] Seq=25 Ack=69 Win=254 Len=0
23	0.218261	192.168.0.5	192.168.0.205	TCP	66	049467 + 582 [ACK] Seq=25 Ack=69 Win=254 Len=0
24	0.218262	192.168.0.5	192.168.0.202	TCP	66	049464 + 582 [ACK] Seq=25 Ack=69 Win=254 Len=0
25	0.218262	192.168.0.5	192.168.0.203	TCP	66	049465 + 582 [ACK] Seq=25 Ack=69 Win=254 Len=0
26	0.499266	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52489; Unit: 201, Func: 4: Read Input Registers
27	0.499699	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 52489; Unit: 201, Func: 4: Read Input Registers
28	0.500092	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52489; Unit: 201, Func: 2: Read Discrete Inputs

```
> Frame 1: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A2A1C1FD-C424-4875-ABCD-B8456B6E
> Ethernet II, Src: VMware_8d:19:54 (00:0c:29:8d:19:54), Dst: AbbIndustria_3e:00:22 (00:00:23:3e:00:22)
> Internet Protocol Version 4, Src: 192.168.0.5, Dst: 192.168.0.201
> Transmission Control Protocol, Src Port: 49463, Dst Port: 502, Seq: 1, Ack: 1, Len: 12
> Modbus/TCP
> Modbus
```

Видно, что Wireshark распознал трафик, как Modbus/TCP, хотя временами встречаются и TCP, и ARP пакеты.

Чтобы работать только с Modbus/TCP пакетами, добавляю соответствующий фильтр:

Примените фильтр отображения ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52233; Unit: 201, Func: 4: Read Input Registers
2	0.000050	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 201, Func: 4: Read Input Registers
3	0.000641	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52233; Unit: 201, Func: 2: Read Discrete Inputs
4	0.000917	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 201, Func: 2: Read Discrete Inputs
5	0.001007	192.168.0.5	192.168.0.202	Modbus/TCP	66	Query: Trans: 52233; Unit: 202, Func: 4: Read Input Registers
6	0.001388	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 202, Func: 4: Read Input Registers
7	0.001418	192.168.0.5	192.168.0.202	Modbus/TCP	66	Query: Trans: 52233; Unit: 202, Func: 2: Read Discrete Inputs
8	0.001649	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 202, Func: 2: Read Discrete Inputs
9	0.001737	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 52233; Unit: 203, Func: 4: Read Input Registers
10	0.001964	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 203, Func: 4: Read Input Registers
11	0.002055	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 52233; Unit: 203, Func: 2: Read Discrete Inputs
12	0.002259	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 203, Func: 2: Read Discrete Inputs
13	0.002337	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 52233; Unit: 204, Func: 4: Read Input Registers
14	0.002551	192.168.0.204	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 204, Func: 4: Read Input Registers
15	0.002661	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 52233; Unit: 204, Func: 2: Read Discrete Inputs
16	0.002839	192.168.0.204	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 204, Func: 2: Read Discrete Inputs
17	0.002949	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 52233; Unit: 205, Func: 4: Read Input Registers
18	0.003159	192.168.0.205	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 205, Func: 4: Read Input Registers
19	0.003237	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 52233; Unit: 205, Func: 2: Read Discrete Inputs
20	0.003468	192.168.0.205	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 205, Func: 2: Read Discrete Inputs
21	0.202795	192.168.0.5	192.168.0.201	Modbus/TCP	66	049463 + 592 [ACK] Seq=25 Ack=69 Win=254 Len=0
22	0.218268	192.168.0.5	192.168.0.204	Modbus/TCP	66	049466 + 582 [ACK] Seq=25 Ack=69 Win=254 Len=0
23	0.218261	192.168.0.5	192.168.0.205	Modbus/TCP	66	049467 + 582 [ACK] Seq=25 Ack=69 Win=254 Len=0
24	0.218262	192.168.0.5	192.168.0.202	Modbus/TCP	66	049464 + 582 [ACK] Seq=25 Ack=69 Win=254 Len=0
25	0.218262	192.168.0.5	192.168.0.203	Modbus/TCP	66	049465 + 582 [ACK] Seq=25 Ack=69 Win=254 Len=0
26	0.499266	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52489; Unit: 201, Func: 4: Read Input Registers
27	0.499699	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 52489; Unit: 201, Func: 4: Read Input Registers
28	0.500092	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52489; Unit: 201, Func: 2: Read Discrete Inputs

```
> Frame 1: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A2A1C1FD-C424-4875-ABCD-B8456B6E
> Ethernet II, Src: VMware_8d:19:54 (00:0c:29:8d:19:54), Dst: AbbIndustria_3e:00:22 (00:00:23:3e:00:22)
> Internet Protocol Version 4, Src: 192.168.0.5, Dst: 192.168.0.201
> Transmission Control Protocol, Src Port: 49463, Dst Port: 502, Seq: 1, Ack: 1, Len: 12
> Modbus/TCP
> Modbus
```

Пакетов: 563 · Обработано: 435 (77.3%)

Профиль: Default  
14:50  
РУС 03.11.2025

Для определения Master и Slave устройств воспользуемся тем фактом, что контроллеры на шине Modbus взаимодействуют, используя модель ведущий — ведомый; при этом именно ведущий инициирует запрос (Query).

Для определения Master устройств с помощью фильтра Wireshark отфильтруем только запросы (Query):

Wireshark screenshot showing captured Modbus/TCP traffic. The left pane lists 66 captured frames, mostly Query messages from source 192.168.0.5 to destination 192.168.0.201. The right pane displays the hex and ASCII representation of frame 1, which is a Modbus/TCP Read Input Registers request.

Frame 1: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{A2A1C1FD-CA24-4875-ABCD-B8456B86E

Modbus/TCP

Transaction Identifier: 52233

Protocol Identifier: 0

Length: 6

Unit Identifier: 201

Modbus

0... .... = Exception: No

.000 0108 = Function Code: Read Input Registers (4)

Reference Number: 0

Word Count: 20

Hex View:

000000	00	00	23	3e	00	22	00	0c	2d	8d	19	54	08	00	45	00	#>^_`-	-T-E:	
000001	00	34	4f	11	40	00	00	06	20	94	03	00	00	05	00	00	44	8	-
000002	00	c9	c1	37	01	f6	61	96	a8	d5	d7	55	9b	50	18	..	7	a-e-U-P:	
000003	00	fe	0e	00	00	cc	09	00	00	00	06	c9	00	00	00	00	00	00	
000004	00	14	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	

ASCII View:

```
00000000: 00 00 23 3e 00 22 00 0c 2d 8d 19 54 08 00 45 00 #>^_`- -T-E:  
00000001: 00 34 4f 11 40 00 00 06 20 94 03 00 00 05 00 00 44 8  
00000002: 00 c9 c1 37 01 f6 61 96 a8 d5 d7 55 9b 50 18 .. 7 a-e-U-P:  
00000003: 00 fe 0e 00 00 cc 09 00 00 00 06 c9 00 00 00 00 00 00  
00000004: 00 14 .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. ..
```

Отсортируем отфильтрованные пакеты по столбцу Source:

No.	Time	Source	Destination	Protocol	Length	Info
146	2.641916	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 60029; Unit: 201, Func: 3: Read Holding Registers
181	3.236851	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 18653; Unit: 201, Func: 3: Read Holding Registers
211	3.295119	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 43093; Unit: 201, Func: 3: Read Holding Registers
259	5.632327	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 30793; Unit: 201, Func: 3: Read Holding Registers
292	5.328587	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 9126; Unit: 201, Func: 3: Read Holding Registers
320	5.958347	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 18662; Unit: 201, Func: 3: Read Holding Registers
428	7.659354	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 59725; Unit: 201, Func: 6: Write Single Register
11	0.000000	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52233; Unit: 201, Func: 4: Read Input Registers
3	0.009641	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52233; Unit: 201, Func: 2: Read Discrete Inputs
5	0.001087	192.168.0.5	192.168.0.202	Modbus/TCP	66	Query: Trans: 52233; Unit: 202, Func: 4: Read Input Registers
7	0.001410	192.168.0.5	192.168.0.202	Modbus/TCP	66	Query: Trans: 52233; Unit: 202, Func: 2: Read Discrete Inputs
9	0.001737	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 52233; Unit: 203, Func: 4: Read Input Registers
11	0.002058	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 52233; Unit: 203, Func: 2: Read Discrete Inputs
13	0.002337	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 52233; Unit: 204, Func: 4: Read Input Registers
15	0.002661	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 52233; Unit: 204, Func: 2: Read Discrete Inputs
17	0.002949	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 52233; Unit: 205, Func: 4: Read Input Registers
19	0.003237	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 52233; Unit: 205, Func: 2: Read Discrete Inputs
26	0.49208	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 52489; Unit: 201, Func: 4: Read Input Registers
28	0.508092	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52489; Unit: 201, Func: 2: Read Discrete Inputs
30	0.508019	192.168.0.5	192.168.0.202	Modbus/TCP	66	Query: Trans: 52489; Unit: 202, Func: 4: Read Input Registers
32	0.501140	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 52489; Unit: 203, Func: 4: Read Input Registers
34	0.501140	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 52489; Unit: 203, Func: 2: Read Discrete Inputs
36	0.509096	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 52489; Unit: 203, Func: 4: Read Input Registers
38	0.509251	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 52489; Unit: 204, Func: 2: Read Discrete Inputs
40	0.509387	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 52489; Unit: 204, Func: 4: Read Input Registers
42	0.503365	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 52489; Unit: 205, Func: 4: Read Input Registers
44	0.503869	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 52489; Unit: 205, Func: 2: Read Discrete Inputs
51	0.998322	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52745; Unit: 201, Func: 4: Read Input Registers
Frame 1: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A2A1C1FD-CA24-4875-ABCD-B8456B6E						
> Ethernet II, Src: VMware_8d:19:54 (00:0c:29:8d:19:54), Dst: AbbIndustria_3e:00:22 (00:00:23:3e:00:22)						
> Internet Protocol Version 4, Src: 192.168.0.5, Dst: 192.168.0.201						
> Transmission Control Protocol, Src Port: 49463, Dst Port: 502, Seq: 1, Ack: 1, Len: 12						
Modbus/TCP						
Transaction Identifier: 52233						
Protocol Identifier: 0						
Length: 6						
Unit Identifier: 201						
Modbus						
0... .... = Exception: No						
.000 0100 = Function Code: Read Input Registers (4)						
Reference Number: 0						
Word Count: 20						
Function Code (modbus.func_code), 7 bit(s)						
0000 00 00 23 3e 00 22 00 0c 29 8d 19 54 08 00 45 00 ..> .. ) - T - E						
0010 00 34 4f 11 40 00 00 06 29 8d c8 a8 00 05 c9 a8 ..40 @ - ) - - - - -						
0020 00 c9 c1 37 01 f6 61 96 a8 d5 65 d7 55 9b 50 18 ..7 - a - e U P -						
0030 00 fe 0e 6f 00 00 cc 09 00 00 00 06 c9 04 00 00 ..o - - - - -						
0040 00 14 ..						
Пакеты: 563 - Отображено: 218 (38.7%)						
Профиль: Default						
16:37 03.11.2025						
лр1.дамп.расп						
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка						
<a href="#">ws.col.protocol == "Modbus/TCP" and modbus.response_time</a>						
No.						
494	9.002347	192.168.0.5	192.168.0.202	Modbus/TCP	66	Query: Trans: 56841; Unit: 202, Func: 2: Read Discrete Inputs
496	9.002640	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 56841; Unit: 203, Func: 4: Read Input Registers
498	9.002945	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 56841; Unit: 203, Func: 2: Read Discrete Inputs
500	9.003247	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 56841; Unit: 204, Func: 4: Read Input Registers
502	9.003574	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 56841; Unit: 204, Func: 2: Read Discrete Inputs
504	9.003870	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 56841; Unit: 205, Func: 4: Read Input Registers
506	9.004233	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 56841; Unit: 205, Func: 2: Read Discrete Inputs
513	9.508475	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 57097; Unit: 201, Func: 4: Read Input Registers
515	9.501306	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 57097; Unit: 201, Func: 2: Read Discrete Inputs
517	9.501590	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 57097; Unit: 202, Func: 4: Read Input Registers
519	9.502124	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 57097; Unit: 202, Func: 2: Read Discrete Inputs
521	9.502624	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 57097; Unit: 203, Func: 4: Read Input Registers
523	9.503110	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 57097; Unit: 203, Func: 2: Read Discrete Inputs
525	9.503656	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 57097; Unit: 204, Func: 4: Read Input Registers
527	9.504860	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 57097; Unit: 204, Func: 2: Read Discrete Inputs
529	9.504565	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 57097; Unit: 205, Func: 4: Read Input Registers
538	9.099575	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 57353; Unit: 201, Func: 4: Read Input Registers
540	10.000089	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 57353; Unit: 201, Func: 2: Read Discrete Inputs
542	10.000419	192.168.0.5	192.168.0.202	Modbus/TCP	66	Query: Trans: 57353; Unit: 202, Func: 4: Read Input Registers
544	10.000735	192.168.0.5	192.168.0.202	Modbus/TCP	66	Query: Trans: 57353; Unit: 202, Func: 2: Read Discrete Inputs
546	10.001039	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 57353; Unit: 203, Func: 4: Read Input Registers
548	10.001348	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 57353; Unit: 203, Func: 2: Read Discrete Inputs
550	10.001648	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 57353; Unit: 204, Func: 4: Read Input Registers
552	10.002089	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 57353; Unit: 204, Func: 2: Read Discrete Inputs
554	10.002348	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 57353; Unit: 205, Func: 4: Read Input Registers
556	10.002660	192.168.0.5	192.168.0.205	Modbus/TCP	66	Query: Trans: 57353; Unit: 205, Func: 2: Read Discrete Inputs
563	10.498757	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 57689; Unit: 201, Func: 4: Read Input Registers
531	9.505025	192.168.0.50	192.168.0.205	Modbus/TCP	66	Query: Trans: 57097; Unit: 205, Func: 2: Read Discrete Inputs
Frame 1: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A2A1C1FD-CA24-4875-ABCD-B8456B6E						
> Ethernet II, Src: VMware_8d:19:54 (00:0c:29:8d:19:54), Dst: AbbIndustria_3e:00:22 (00:00:23:3e:00:22)						
> Internet Protocol Version 4, Src: 192.168.0.5, Dst: 192.168.0.201						
> Transmission Control Protocol, Src Port: 49463, Dst Port: 502, Seq: 1, Ack: 1, Len: 12						
Modbus/TCP						
Transaction Identifier: 52233						
Protocol Identifier: 0						
Length: 6						
Unit Identifier: 201						
Modbus						
0... .... = Exception: No						
.000 0100 = Function Code: Read Input Registers (4)						
Reference Number: 0						
Word Count: 20						
Function Code (modbus.func_code), 7 bit(s)						
0000 00 00 23 3e 00 22 00 0c 29 8d 19 54 08 00 45 00 ..> .. ) - T - E						
0010 00 34 4f 11 40 00 00 06 29 8d c8 a8 00 05 c9 a8 ..40 @ - ) - - - - -						
0020 00 c9 c1 37 01 f6 61 96 a8 d5 65 d7 55 9b 50 18 ..7 - a - e U P -						
0030 00 fe 0e 6f 00 00 cc 09 00 00 00 06 c9 04 00 00 ..o - - - - -						
0040 00 14 ..						
Пакеты: 563 - Отображено: 218 (38.7%)						
Профиль: Default						
16:38 03.11.2025						
лр1.дамп.расп						
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка						
<a href="#">ws.col.protocol == "Modbus/TCP" and modbus.response_time</a>						
No.						

адресом 192.168.0.122 - это роутер DLink, а устройство с IP адресом 192.168.0.50 нам не известно (и от него идет всего один запрос). Поэтому Master устройствами мы можем считать Engineer PC (с IP адресом 192.168.0.5) и роутер DLink (с IP адресом 192.168.0.5).

Для определения Slave устройств с помощью фильтра Wireshark отфильтруем только ответы (Response):

The screenshot shows the NetworkMiner interface with the following details:

- Title Bar:** "пр1.димм.распрг" - File, Правка, Вид, Запуск, Анализ, Статистика, Телефония, Беспроводная связь, Инструменты, Справка.
- Search Bar:** ".ws.col.protocol == "Modbus/TCP" and modulus.response\_time".
- Table View:** Shows a list of captured Modbus/TCP frames. Each row contains: No., Time, Source, Destination, Protocol, Length, and Info. The Info column provides detailed information about the Modbus function code and unit identifier for each response.
- Frame Details:** Frame 145 is selected, showing its bytes on wire and bytes captured. It includes fields like Source MAC, Destination MAC, Type, and Content.
- Protocol Tree:** A tree view showing the structure of the Modbus/TCP frame, including Transaction Identifier, Protocol Identifier, Length, and Unit Identifier.
- Hex/ASCII/Payload:** Displays the raw bytes of the selected frame in hex, ASCII, and as a payload.
- Bottom Status Bar:** "Пакеты: 563 - Отображено: 217 (38.5%)" and "Профиль: Default" along with system icons.

Отсортируем отфильтрованные пакеты по столбцу Source:

пр1\_дамп.рарсиг

Файл Правка Вид Запуск Заверк Анализ Статистика Телефония Беспроводная связь Инструменты Справка

\_ws.col.protocol == "Modbus/TCP and modbus.response\_time"

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000588	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 201, Func: 4: Read Input Registers
4	0.000817	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 201, Func: 2: Read Discrete Inputs
27	0.499699	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 52489; Unit: 201, Func: 4: Read Input Registers
29	0.500355	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 52489; Unit: 201, Func: 2: Read Discrete Inputs
52	0.998551	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 52745; Unit: 201, Func: 4: Read Input Registers
54	0.999822	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 52745; Unit: 201, Func: 2: Read Discrete Inputs
77	1.497941	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 53001; Unit: 201, Func: 4: Read Input Registers
79	1.498599	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 53001; Unit: 201, Func: 2: Read Discrete Inputs
182	1.997149	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 53257; Unit: 201, Func: 4: Read Input Registers
184	1.997474	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 53257; Unit: 201, Func: 2: Read Discrete Inputs
127	2.496369	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 53513; Unit: 201, Func: 4: Read Input Registers
129	2.497883	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 53513; Unit: 201, Func: 2: Read Discrete Inputs
149	2.642461	192.168.0.201	192.168.0.122	Modbus/TCP	65	Response: Trans: 60029; Unit: 201, Func: 3: Read Holding Registers
157	2.995522	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 53769; Unit: 201, Func: 4: Read Input Registers
159	2.995850	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 53769; Unit: 201, Func: 2: Read Discrete Inputs
182	3.336424	192.168.0.201	192.168.0.122	Modbus/TCP	65	Response: Trans: 18633; Unit: 201, Func: 3: Read Holding Registers
187	3.494787	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 54025; Unit: 201, Func: 4: Read Input Registers
189	3.495321	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 54025; Unit: 201, Func: 2: Read Discrete Inputs
212	3.951518	192.168.0.201	192.168.0.122	Modbus/TCP	65	Response: Trans: 43092; Unit: 201, Func: 3: Read Holding Registers
214	3.994099	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 54281; Unit: 201, Func: 4: Read Input Registers
216	3.994428	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 54281; Unit: 201, Func: 2: Read Discrete Inputs
248	4.493172	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 54537; Unit: 201, Func: 4: Read Input Registers
242	4.493888	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 54537; Unit: 201, Func: 2: Read Discrete Inputs
266	4.623279	192.168.0.201	192.168.0.122	Modbus/TCP	64	Response: Trans: 54093; Unit: 201, Func: 3: Read Holding Registers
268	4.992263	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 54793; Unit: 201, Func: 4: Read Input Registers
270	4.992594	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 54793; Unit: 201, Func: 2: Read Discrete Inputs
293	5.320911	192.168.0.201	192.168.0.122	Modbus/TCP	65	Response: Trans: 9136; Unit: 201, Func: 3: Read Holding Registers
296	5.491570	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 55049; Unit: 201, Func: 4: Read Input Registers

> Frame 145: Packet, 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF\_{A2A1C1FD-CA24-4875-ABCD-B8456B

> Ethernet II, Src: BeckhoffAuto\_23:60:54 (00:01:05:23:60:54), Dst: VMware\_Bd:19:54 (00:0c:29:8d:19:54)

> Internet Protocol Version 4, Src: 192.168.0.205, Dst: 192.168.0.5

> Transmission Control Protocol, Src Port: 502, Dst Port: 49467, Seq: 345, Ack: 145, Len: 10

Modbus/TCP

Transaction Identifier: 53513

Protocol Identifier: 0

Length: 4

Unit Identifier: 205

Modbus

0... .... = Exception: No

.000 0010 = Function Code: Read Discrete Inputs (2)

[Request Frame: 144]

[Time from request: 214.000 microseconds]

Byte Count: 1

> Bit 0 : 0

> Bit 1 : 0

Function Code (modbus.func\_code), 7 bit(s)

Пакеты: 563 - Отображено: 217 (38.5%)

Профиль: Default

пр1\_дамп.рарсиг

Файл Правка Вид Запуск Заверк Анализ Статистика Телефония Беспроводная связь Инструменты Справка

\_ws.col.protocol == "Modbus/TCP and modbus.response\_time"

No.	Time	Source	Destination	Protocol	Length	Info
489	9.001559	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 56841; Unit: 201, Func: 4: Read Input Registers
491	9.001895	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 56841; Unit: 201, Func: 2: Read Discrete Inputs
514	9.500888	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 57097; Unit: 201, Func: 4: Read Input Registers
516	9.501520	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 57097; Unit: 201, Func: 2: Read Discrete Inputs
539	9.999970	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 57353; Unit: 201, Func: 4: Read Input Registers
541	10.000320	192.168.0.201	192.168.0.5	Modbus/TCP	64	Response: Trans: 57353; Unit: 201, Func: 2: Read Discrete Inputs
6	0.001386	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 202, Func: 4: Read Input Registers
8	0.001649	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 202, Func: 2: Read Discrete Inputs
31	0.508588	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 52489; Unit: 202, Func: 4: Read Input Registers
33	0.501375	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 52489; Unit: 202, Func: 2: Read Discrete Inputs
56	0.999367	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 52745; Unit: 202, Func: 4: Read Input Registers
58	0.999671	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 52745; Unit: 202, Func: 2: Read Discrete Inputs
81	1.499988	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 53001; Unit: 202, Func: 4: Read Input Registers
83	1.499563	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 53001; Unit: 202, Func: 2: Read Discrete Inputs
104	1.999424	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 53277; Unit: 202, Func: 4: Read Input Registers
108	1.999821	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 53277; Unit: 202, Func: 2: Read Discrete Inputs
131	2.497790	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 53513; Unit: 202, Func: 4: Read Input Registers
133	2.497874	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 53513; Unit: 202, Func: 2: Read Discrete Inputs
161	2.996121	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 53769; Unit: 202, Func: 4: Read Input Registers
163	2.996833	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 53769; Unit: 202, Func: 2: Read Discrete Inputs
191	3.495775	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 54025; Unit: 202, Func: 4: Read Input Registers
193	3.496232	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 54025; Unit: 202, Func: 2: Read Discrete Inputs
218	3.994742	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 54281; Unit: 202, Func: 4: Read Input Registers
220	3.995039	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 54281; Unit: 202, Func: 2: Read Discrete Inputs
244	4.494351	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 54537; Unit: 202, Func: 4: Read Input Registers
246	4.494927	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 54537; Unit: 202, Func: 2: Read Discrete Inputs
272	4.992890	192.168.0.202	192.168.0.5	Modbus/TCP	103	Response: Trans: 54793; Unit: 202, Func: 4: Read Input Registers
274	4.993147	192.168.0.202	192.168.0.5	Modbus/TCP	64	Response: Trans: 54793; Unit: 202, Func: 2: Read Discrete Inputs

> Frame 145: Packet, 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF\_{A2A1C1FD-CA24-4875-ABCD-B8456B

> Ethernet II, Src: BeckhoffAuto\_23:60:54 (00:01:05:23:60:54), Dst: VMware\_Bd:19:54 (00:0c:29:8d:19:54)

> Internet Protocol Version 4, Src: 192.168.0.205, Dst: 192.168.0.5

> Transmission Control Protocol, Src Port: 502, Dst Port: 49467, Seq: 345, Ack: 145, Len: 10

Modbus/TCP

Transaction Identifier: 53513

Protocol Identifier: 0

Length: 4

Unit Identifier: 205

Modbus

0... .... = Exception: No

.000 0010 = Function Code: Read Discrete Inputs (2)

[Request Frame: 144]

[Time from request: 214.000 microseconds]

Byte Count: 1

> Bit 0 : 0

> Bit 1 : 0

Function Code (modbus.func\_code), 7 bit(s)

Пакеты: 563 - Отображено: 217 (38.5%)

Профиль: Default

18:19 03.11.2025

No.	Time	Source	Destination	Protocol	Length	Info
468	8.593861	192.168.0.203	192.168.0.5	Modbus/TCP	64	103 Response: Trans: 56585; Unit: 203, Func: 4: Read Input Registers
470	8.593872	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 56585; Unit: 203, Func: 2: Read Discrete Inputs
493	9.002227	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 56841; Unit: 203, Func: 4: Read Input Registers
495	9.002524	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 56841; Unit: 203, Func: 2: Read Discrete Inputs
518	9.501823	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 57097; Unit: 203, Func: 4: Read Input Registers
520	9.502346	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 57097; Unit: 203, Func: 2: Read Discrete Inputs
543	10.000642	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 57353; Unit: 203, Func: 4: Read Input Registers
545	10.000949	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 57353; Unit: 203, Func: 2: Read Discrete Inputs
10	10.001964	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 52233; Unit: 203, Func: 4: Read Input Registers
12	0.002259	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 203, Func: 2: Read Discrete Inputs
35	0.501842	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 52489; Unit: 203, Func: 4: Read Input Registers
37	0.502299	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 52489; Unit: 203, Func: 2: Read Discrete Inputs
60	1.000005	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 52745; Unit: 203, Func: 4: Read Input Registers
62	1.000333	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 52745; Unit: 203, Func: 2: Read Discrete Inputs
85	1.500501	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 53001; Unit: 203, Func: 4: Read Input Registers
87	1.500595	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 53001; Unit: 203, Func: 2: Read Discrete Inputs
110	1.998311	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 53257; Unit: 203, Func: 4: Read Input Registers
112	1.998564	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 53257; Unit: 203, Func: 2: Read Discrete Inputs
135	2.498350	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 53511; Unit: 203, Func: 4: Read Input Registers
137	2.498830	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 53511; Unit: 203, Func: 2: Read Discrete Inputs
149	2.499090	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 53769; Unit: 203, Func: 4: Read Input Registers
167	2.499890	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 53769; Unit: 203, Func: 2: Read Discrete Inputs
195	3.496634	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 54025; Unit: 203, Func: 4: Read Input Registers
197	3.497098	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 54025; Unit: 203, Func: 2: Read Discrete Inputs
222	3.995366	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 54281; Unit: 203, Func: 4: Read Input Registers
224	3.995673	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 54281; Unit: 203, Func: 2: Read Discrete Inputs
248	4.495465	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 54537; Unit: 203, Func: 4: Read Input Registers
250	4.496029	192.168.0.203	192.168.0.5	Modbus/TCP	64	Response: Trans: 54537; Unit: 203, Func: 2: Read Discrete Inputs

> Frame 145: Packet, 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{A2A1C1FD-CA48-4B75-ABCD-B8456B	0000 00 0c 29 8d 19 54 00 01 05 23 60 54 08 00 45 00 ...-T-#T-E
> Ethernet II, Src: BeckhoffAuto_23:60:54 (00:01:05:23:60:54), Dst: VMware_8d:19:54 (00:0c:29:8d:19:54)	0010 00 32 60 d2 40 00 00 0e d1 c0 a8 00 cd c0 a8 21 @-----
> Internet Protocol Version 4, Src: 192.168.0.205, Dst: 192.168.0.5	0020 00 05 01 f6 c1 3b 23 0c 94 fa 6c a9 33 37 50 18 ...;#-1.37P
> Transmission Control Protocol, Src Port: 502, Dst Port: 49467, Seq: 345, Ack: 145, Len: 10	0030 00 ff 71 c2 00 00 d1 09 00 00 00 04 cd 01 00 ...q-----
Modbus/TCP	
Transaction Identifier: 53513	
Protocol Identifier: 0	
Length: 4	
Unit Identifier: 205	
Modbus	
0... .... = Exception: No	
.000 0010 = Function Code: Read Discrete Inputs (2)	
[Request Frame: 144]	
[Time from request: 214.000 microseconds]	
Byte Count: 1	
> Bit 0 : 0	
> Bit 1 : 0	
Function Code (modbus.func_code), 7 bit(s)	

Пакеты 563 · Отображено: 217 (38.5%)      Профиль: Default      18:19 03.11.2025

лр1.дамп.расп

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

ws.col.protocol == "Modbus/TCP" and modbus.response\_time

No.	Time	Source	Destination	Protocol	Length	Info
411	7.508213	192.168.0.204	192.168.0.5	Modbus/TCP	183	Response: Trans: 56073; Unit: 204, Func: 4: Read Input Registers
413	7.508844	192.168.0.204	192.168.0.5	Modbus/TCP	64	Response: Trans: 56073; Unit: 204, Func: 2: Read Discrete Inputs
409	8.0005124	192.168.0.204	192.168.0.5	Modbus/TCP	183	Response: Trans: 56329; Unit: 204, Func: 4: Read Input Registers
451	8.0005124	192.168.0.204	192.168.0.5	Modbus/TCP	64	Response: Trans: 56329; Unit: 204, Func: 2: Read Discrete Inputs
476	8.509117	192.168.0.204	192.168.0.5	Modbus/TCP	183	Response: Trans: 56585; Unit: 204, Func: 4: Read Input Registers
478	8.509584	192.168.0.204	192.168.0.5	Modbus/TCP	64	Response: Trans: 56585; Unit: 204, Func: 2: Read Discrete Inputs
501	9.003481	192.168.0.204	192.168.0.5	Modbus/TCP	183	Response: Trans: 56841; Unit: 204, Func: 4: Read Input Registers
503	9.003759	192.168.0.204	192.168.0.5	Modbus/TCP	64	Response: Trans: 56841; Unit: 204, Func: 2: Read Discrete Inputs
526	9.50379	192.168.0.204	192.168.0.5	Modbus/TCP	183	Response: Trans: 57097; Unit: 204, Func: 4: Read Input Registers
528	9.50432	192.168.0.204	192.168.0.5	Modbus/TCP	64	Response: Trans: 57097; Unit: 204, Func: 2: Read Discrete Inputs
551	10.001981	192.168.0.204	192.168.0.5	Modbus/TCP	183	Response: Trans: 57353; Unit: 204, Func: 4: Read Input Registers
553	10.002248	192.168.0.204	192.168.0.5	Modbus/TCP	64	Response: Trans: 57353; Unit: 204, Func: 2: Read Discrete Inputs
18	0.003159	192.168.0.205	192.168.0.5	Modbus/TCP	183	Response: Trans: 52233; Unit: 205, Func: 4: Read Input Registers
20	0.003460	192.168.0.205	192.168.0.5	Modbus/TCP	64	Response: Trans: 52233; Unit: 205, Func: 2: Read Discrete Inputs
43	0.503625	192.168.0.205	192.168.0.5	Modbus/TCP	183	Response: Trans: 52489; Unit: 205, Func: 4: Read Input Registers
45	0.504091	192.168.0.205	192.168.0.5	Modbus/TCP	64	Response: Trans: 52489; Unit: 205, Func: 2: Read Discrete Inputs
68	1.001331	192.168.0.205	192.168.0.5	Modbus/TCP	183	Response: Trans: 52745; Unit: 205, Func: 4: Read Input Registers
70	1.001654	192.168.0.205	192.168.0.5	Modbus/TCP	64	Response: Trans: 52745; Unit: 205, Func: 2: Read Discrete Inputs
93	1.501808	192.168.0.205	192.168.0.5	Modbus/TCP	183	Response: Trans: 53081; Unit: 205, Func: 4: Read Input Registers
95	1.502265	192.168.0.205	192.168.0.5	Modbus/TCP	64	Response: Trans: 53081; Unit: 205, Func: 2: Read Discrete Inputs
118	1.99939	192.168.0.205	192.168.0.5	Modbus/TCP	183	Response: Trans: 53257; Unit: 205, Func: 4: Read Input Registers
128	1.999692	192.168.0.205	192.168.0.5	Modbus/TCP	64	Response: Trans: 53257; Unit: 205, Func: 2: Read Discrete Inputs
143	2.499917	192.168.0.205	192.168.0.5	Modbus/TCP	183	Response: Trans: 53513; Unit: 205, Func: 4: Read Input Registers
145	2.508387	192.168.0.205	192.168.0.5	Modbus/TCP	64	Response: Trans: 53513; Unit: 205, Func: 2: Read Discrete Inputs
173	2.997862	192.168.0.205	192.168.0.5	Modbus/TCP	183	Response: Trans: 53769; Unit: 205, Func: 4: Read Input Registers
175	2.998289	192.168.0.205	192.168.0.5	Modbus/TCP	64	Response: Trans: 53769; Unit: 205, Func: 2: Read Discrete Inputs
203	3.498107	192.168.0.205	192.168.0.5	Modbus/TCP	183	Response: Trans: 54025; Unit: 205, Func: 4: Read Input Registers
205	3.498556	192.168.0.205	192.168.0.5	Modbus/TCP	64	Response: Trans: 54025; Unit: 205, Func: 2: Read Discrete Inputs

```

> Frame 145: Packet, 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{A2A1C1FD-CA24-4875-ABCD-BB456B
> Ethernet II, Src: BeckhoffAuto_23:60:54 (00:01:00:23:60:54), Dst: VMware_8d19:54 (00:0c:29:8d:19:54)
> Internet Protocol Version 4, Src: 192.168.0.205, Dst: 192.168.0.5
> Transmission Control Protocol, Src Port: 502, Dst Port: 49467, Seq: 345, Ack: 145, Len: 10
Modbus/TCP
  Transaction Identifier: 5313
  Protocol Identifier: 0
  Length: 4
  Unit Identifier: 205
Modbus
  0... .... = Exception: No
  .000 0010 = Function Code: Read Discrete Inputs (2)
  [Request Frame: 144]
  [Time from request: 214.000 microseconds]
  Byte Count: 1
  > Bit 0 : 0
  > Bit 1 : 0

```

Пакеты: 563 - Отображено: 217 (38.5%)      Профиль: Default

18:20 ENG 03.11.2025

Видно, что устройствами, которые отправляют ответы являются устройства со следующими IP адресами: 192.168.0.201, 192.168.0.202, 192.168.0.203, 192.168.0.204 и 192.168.0.205. Все эти устройства являются PLC разного вида - поэтому всех их можно считать Slave устройствами.

### 3. Идентификация пары «запрос-ответ».

Согласно документации, запись одного значения в регистр - это функция с кодом 6 (0x06). Отфильтруем запросы по значению кода функции, равного 6:

Лог сеанса (пр1\_дамп.срарп)

No.	Time	Source	Destination	Protocol	Length	Info
428	7.659354	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 59725; Unit: 201, Func: 6: Write Single Register
429	7.659826	192.168.0.201	192.168.0.122	Modbus/TCP	66	Response: Trans: 59725; Unit: 201, Func: 6: Write Single Register

Frame 428: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{A2A1C1FD-CA24-4875-ABCD-BB456B

> Ethernet II, Src: DlinkInterna\_Be:f8:7d (18:0f:76:8e:f8:7d), Dst: Abbindustria\_3e:00:22 (00:00:23:3e:00:22)

> Internet Protocol Version 4, Src: 192.168.0.122, Dst: 192.168.0.201

> Transmission Control Protocol, Src Port: 49673, Dst Port: 502, Seq: 73, Ack: 67, Len: 12

Modbus/TCP

- Transaction Identifier: 59725
- Protocol Identifier: 0
- Length: 6
- Unit Identifier: 201

Modbus

- 0... .... = Exception: No
- .000 0110 = Function Code: Write Single Register (6)
- Reference Number: 2
- Register 2 (UINT16): 45

Frame 429: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{A2A1C1FD-CA24-4875-ABCD-BB456B

> Ethernet II, Src: Abbindustria\_3e:00:22 (00:00:23:3e:00:22), Dst: DlinkInterna\_Be:f8:7d (18:0f:76:8e:f8:7d)

> Internet Protocol Version 4, Src: 192.168.0.201, Dst: 192.168.0.122

> Transmission Control Protocol, Src Port: 502, Dst Port: 49673, Seq: 73, Ack: 67, Len: 12

Modbus/TCP

- Transaction Identifier: 59725
- Protocol Identifier: 0
- Length: 6
- Unit Identifier: 201

Modbus

- 0... .... = Exception: No
- .000 0110 = Function Code: Write Single Register (6)
- Reference Number: 2
- Register 2 (UINT16): 45
- [Register Number: 2]
- Register Value (UINT16): 45

Пакеты: 563 · Отображено: 2 (0.4%)

Профиль: Default

18:39 03.11.2025

Видим, что единственный запрос на запись значения в регистр был от Master устройства с IP адресом 192.168.0.122 на Slave устройство с IP адресом 192.168.0.201:

Лог сеанса (пр1\_дамп.срарп)

No.	Time	Source	Destination	Protocol	Length	Info
428	7.659354	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 59725; Unit: 201, Func: 6: Write Single Register
429	7.659826	192.168.0.201	192.168.0.122	Modbus/TCP	66	Response: Trans: 59725; Unit: 201, Func: 6: Write Single Register

Frame 428: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{A2A1C1FD-CA24-4875-ABCD-BB456B

> Ethernet II, Src: DlinkInterna\_Be:f8:7d (18:0f:76:8e:f8:7d), Dst: Abbindustria\_3e:00:22 (00:00:23:3e:00:22)

> Internet Protocol Version 4, Src: 192.168.0.122, Dst: 192.168.0.201

> Transmission Control Protocol, Src Port: 49673, Dst Port: 502, Seq: 73, Ack: 67, Len: 12

Modbus/TCP

- Transaction Identifier: 59725
- Protocol Identifier: 0
- Length: 6
- Unit Identifier: 201

Modbus

- 0... .... = Exception: No
- .000 0110 = Function Code: Write Single Register (6)
- Reference Number: 2
- Register 2 (UINT16): 45
- [Register Number: 2]
- Register Value (UINT16): 45

Frame 429: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{A2A1C1FD-CA24-4875-ABCD-BB456B

> Ethernet II, Src: Abbindustria\_3e:00:22 (00:00:23:3e:00:22), Dst: DlinkInterna\_Be:f8:7d (18:0f:76:8e:f8:7d)

> Internet Protocol Version 4, Src: 192.168.0.201, Dst: 192.168.0.122

> Transmission Control Protocol, Src Port: 502, Dst Port: 49673, Seq: 73, Ack: 67, Len: 12

Modbus/TCP

- Transaction Identifier: 59725
- Protocol Identifier: 0
- Length: 6
- Unit Identifier: 201

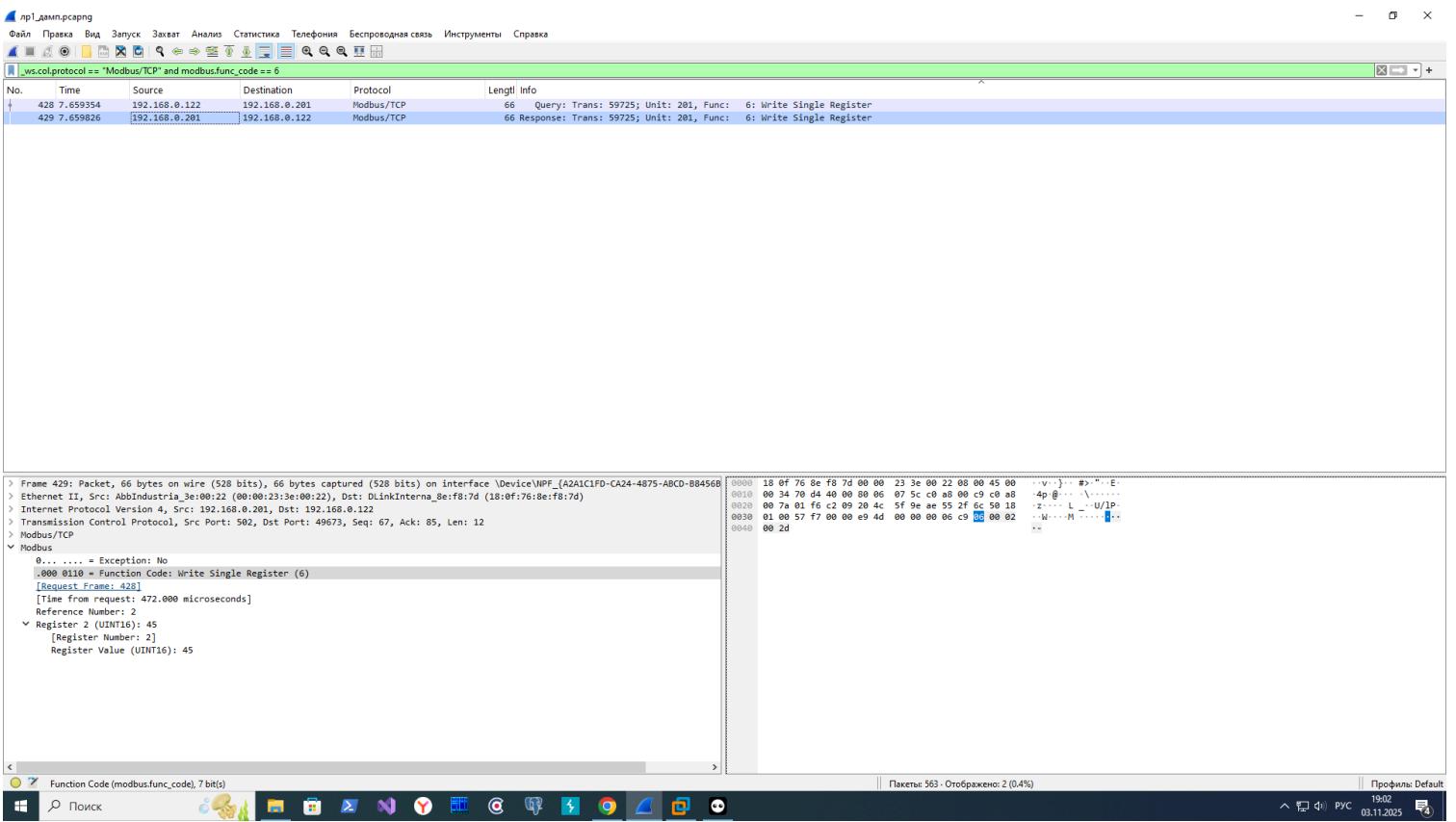
Modbus

- 0... .... = Exception: No
- .000 0110 = Function Code: Write Single Register (6)
- Reference Number: 2
- Register 2 (UINT16): 45
- [Register Number: 2]
- Register Value (UINT16): 45

Пакеты: 563 · Отображено: 2 (0.4%)

Профиль: Default

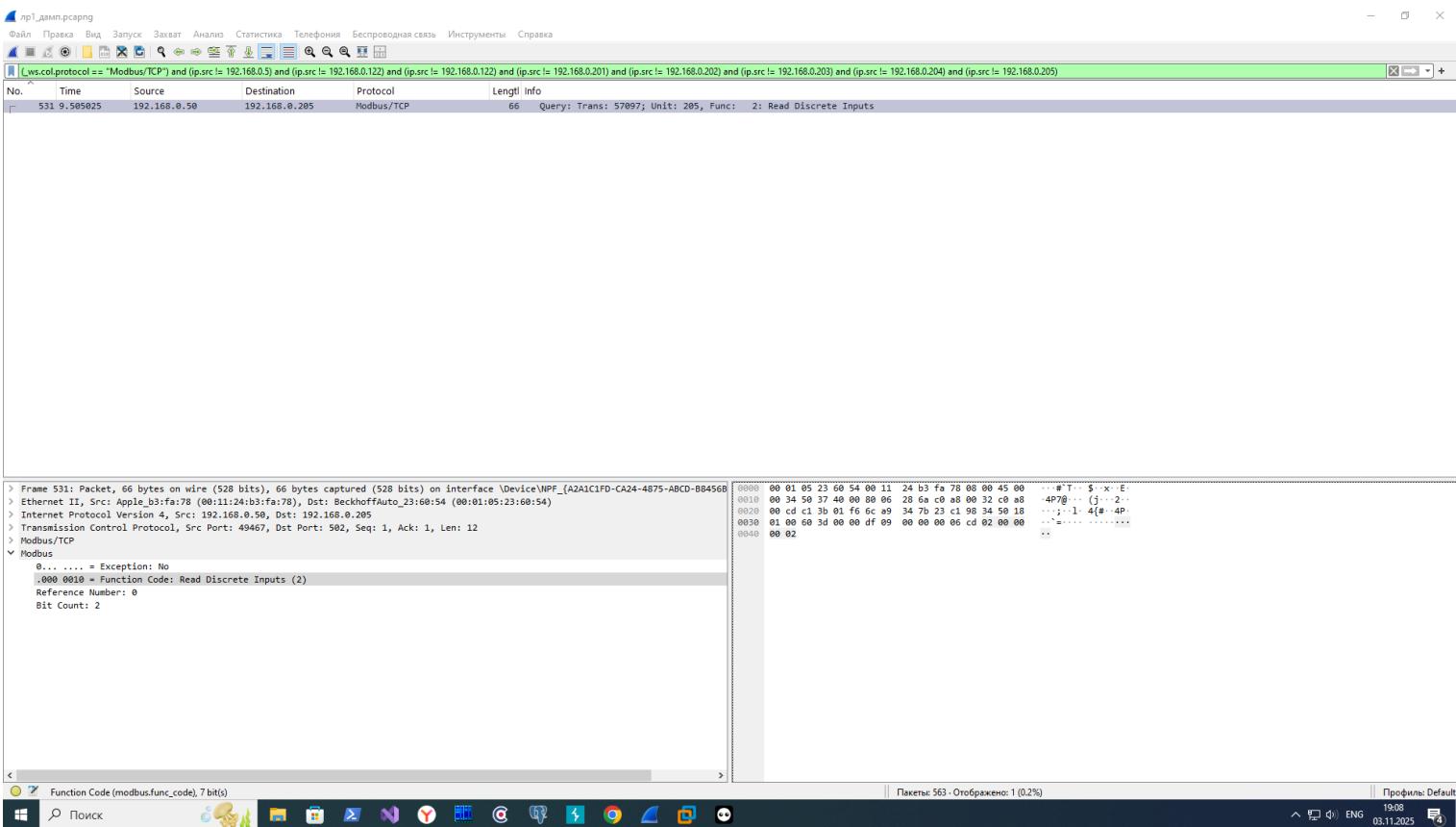
19:02 03.11.2025



Видно, что в регистр 2 было записано значение 45

#### 4. Анализ соответствия топологии сети.

Согласно топологии сети, у нас есть устройства со следующими IP адресами: 192.168.0.5, 192.168.0.122, 192.168.0.201, 192.168.0.202, 192.168.0.203, 192.168.0.204 и 192.168.0.205. Отфильтруем запросы по IP адресу источника запроса (Source IP) так, чтобы IP адрес источника запроса не совпадал с известными нам адресами:



Видно, что у нас есть запрос (на чтение значений из нескольких дискретных входов) с неизвестного для нашей топологии сети IP адреса - 192.168.0.50. Можно сделать вывод, что это какая-то попытка вторжения.

## 5. Выводы.

- 1) Мы выяснили, что устройства с IP адресами 192.168.0.5 и 192.168.0.122 являются Master устройствами; устройства с IP адресами 192.168.0.201, 192.168.0.202, 192.168.0.203, 192.168.0.204 и 192.168.0.205 являются Slave устройствами.
- 2) Мы обнаружили, что запрос на запись значения в регистр был только один: от Master устройства с IP адресом 192.168.0.122 на Slave устройство с IP адресом 192.168.0.201.
- 3) Мы обнаружили запрос (на чтение значений из нескольких дискретных входов) с неизвестного для нашей топологии сети IP адреса - 192.168.0.50. Из этого можно сделать вывод, что это начало попытки вторжения.