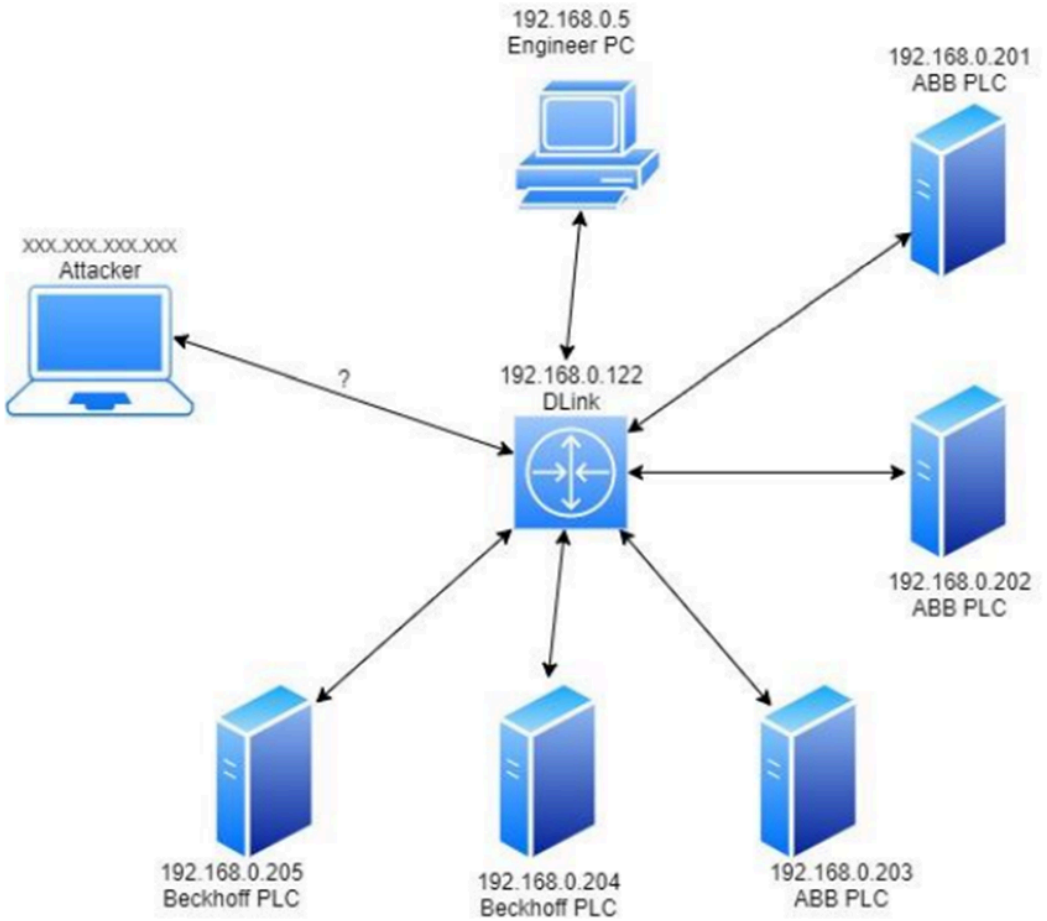
1. Введение.

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:

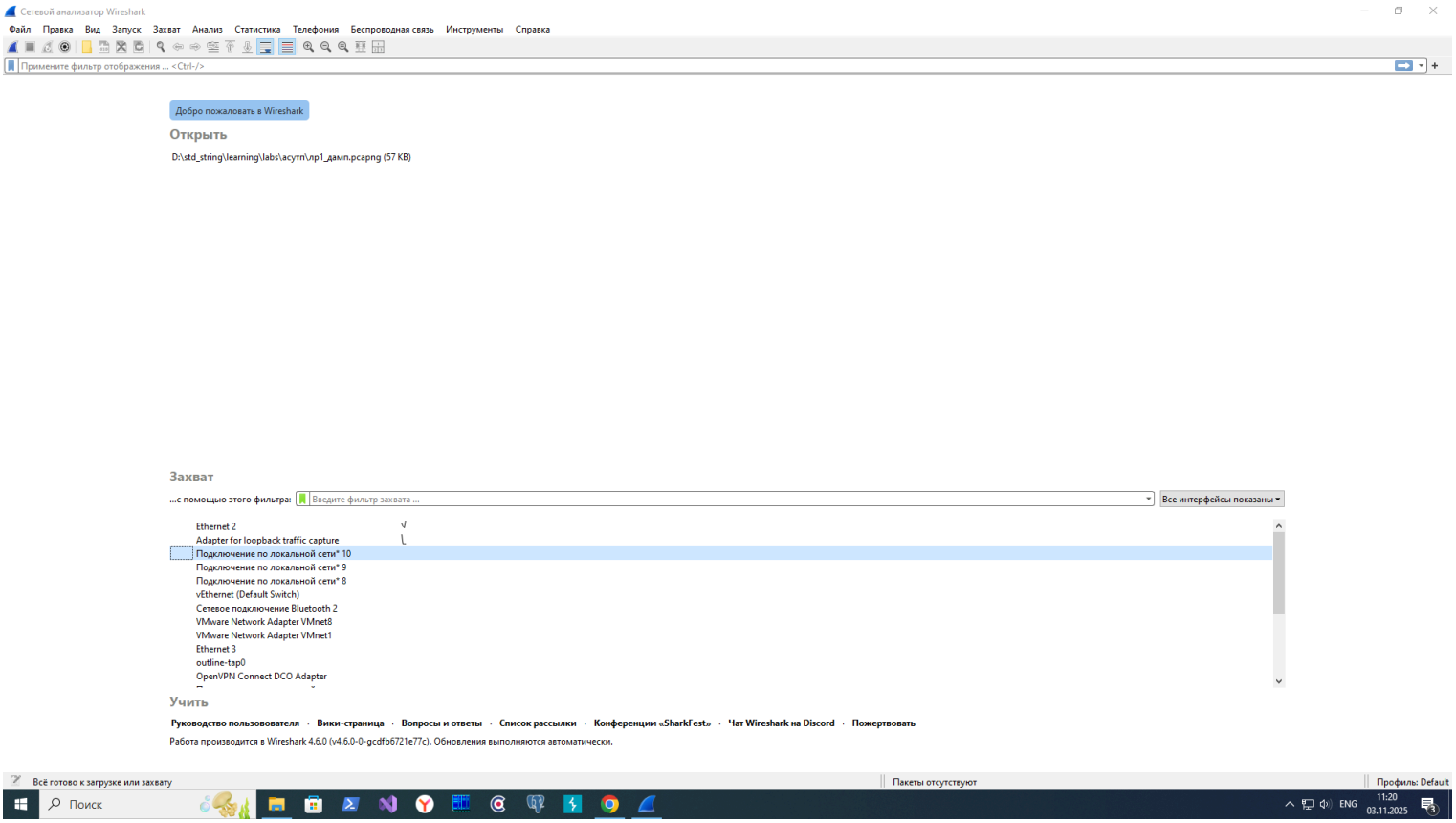


Немного информации о протоколе Modbus:
Контроллеры на шине Modbus взаимодействуют, используя модель ведущий — ведомый, основанную на транзакциях, состоящих из запроса и ответа.
Обычно в сети есть только одно ведущее client (по старой терминологии master) устройство, и несколько ведомых server (по старой терминологии slave) устройств. (Терминология верна, несмотря на противоположные значения в типичной

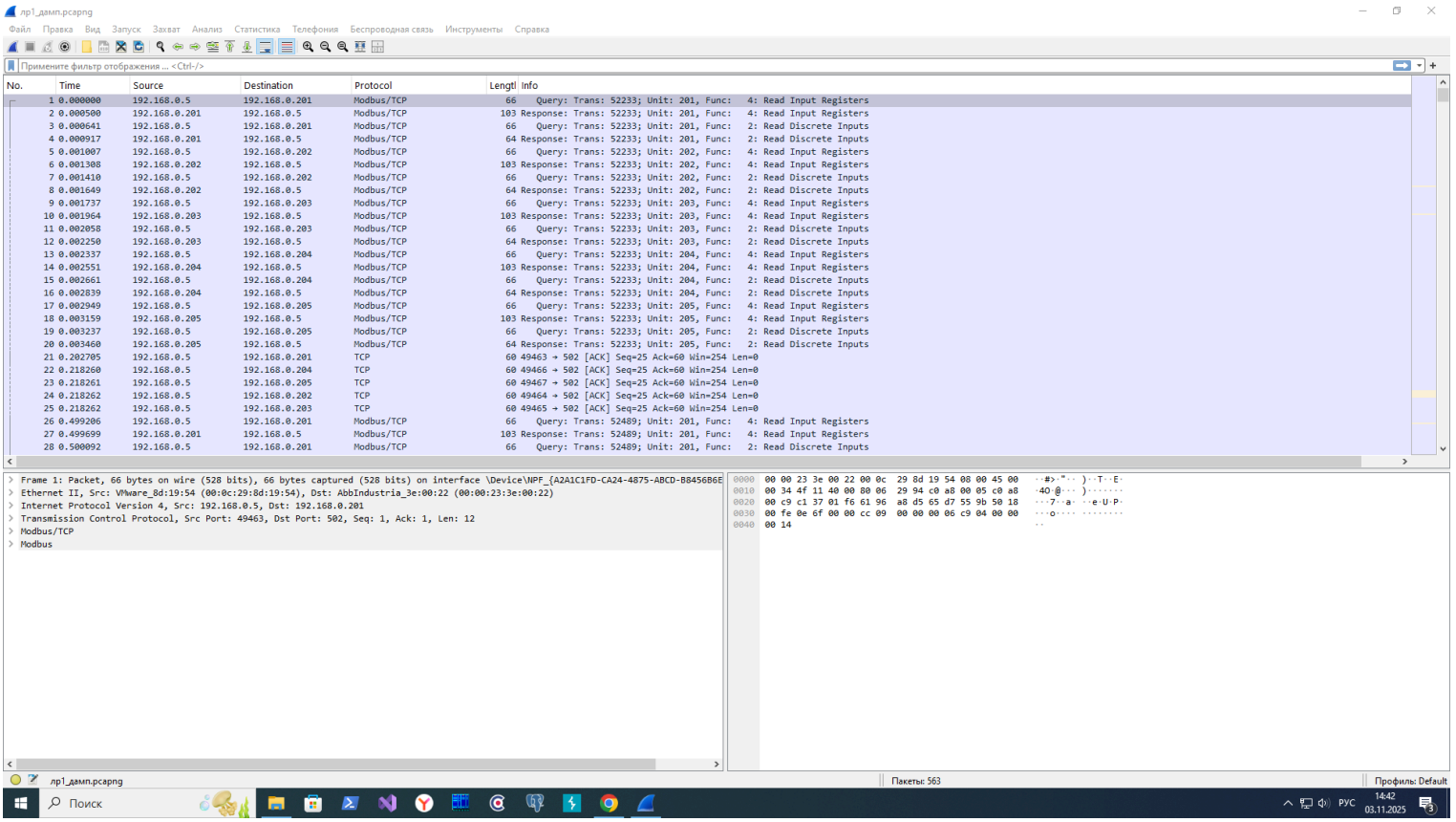
клиент-серверной архитектуре.) Ведущее устройство инициирует транзакции (передает запросы). Ведущий может адресовать запрос индивидуально любому ведомому или инициировать передачу широковещательного сообщения для всех ведомых устройств. Ведомое устройство, опознав свой адрес, отвечает на запрос, адресованный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

2. Анализ сетевого трафика.

Запускаю WireShark:

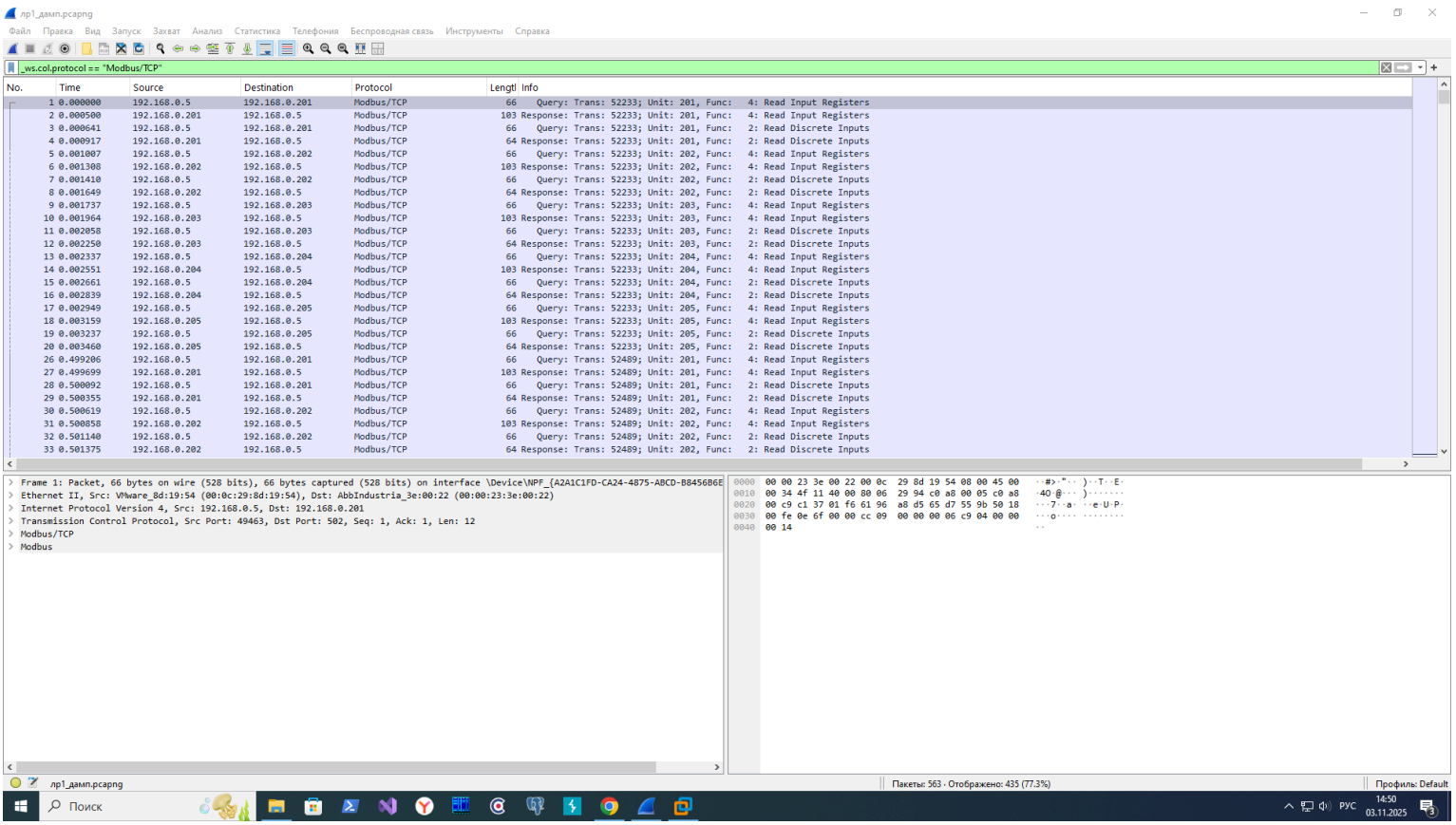


Загружаю дамп трафика:

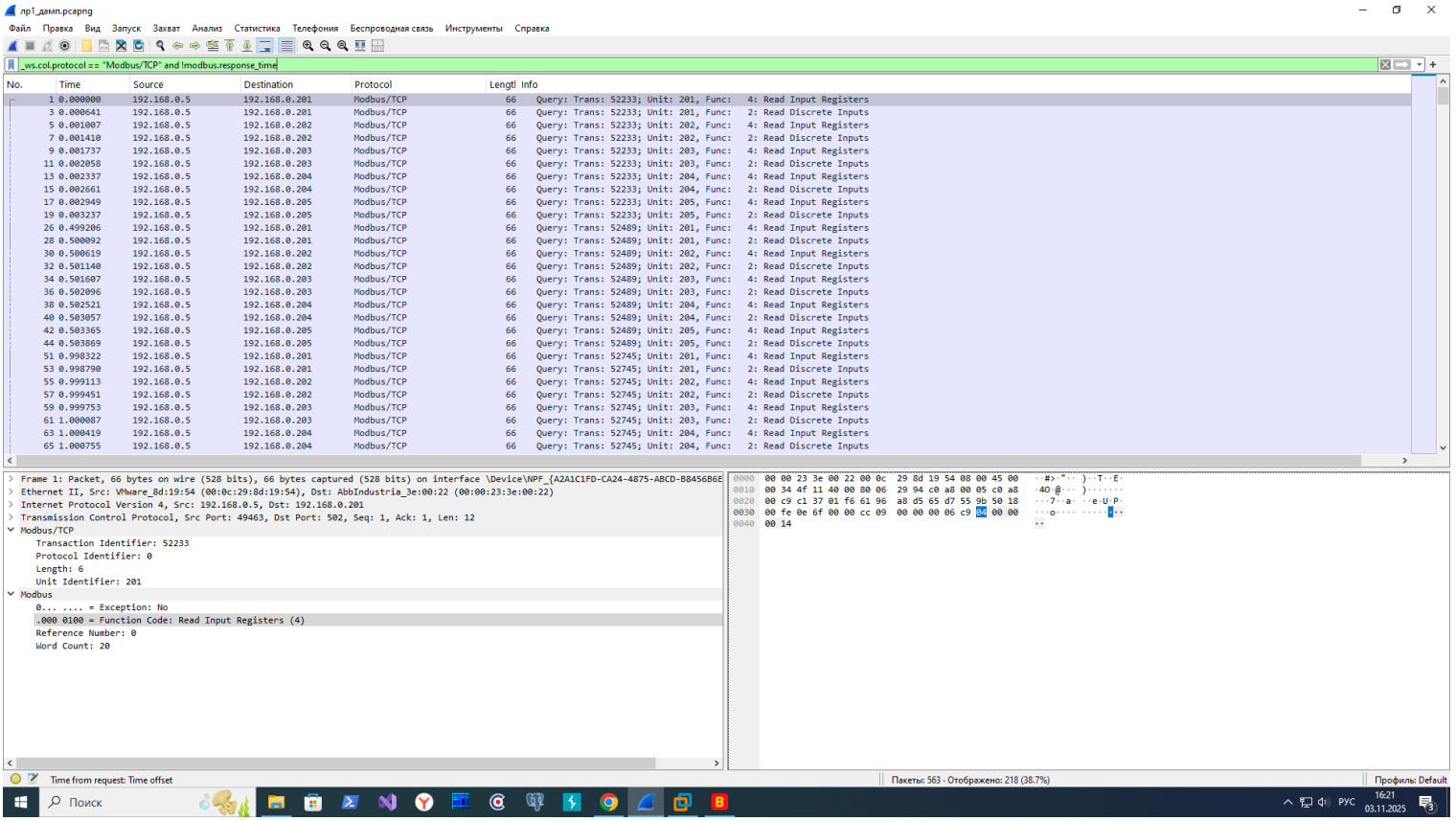


Видно, что WireShark распознал трафик, как Modbus/TCP, хотя временами встречаются и TCP, и ARP пакеты.

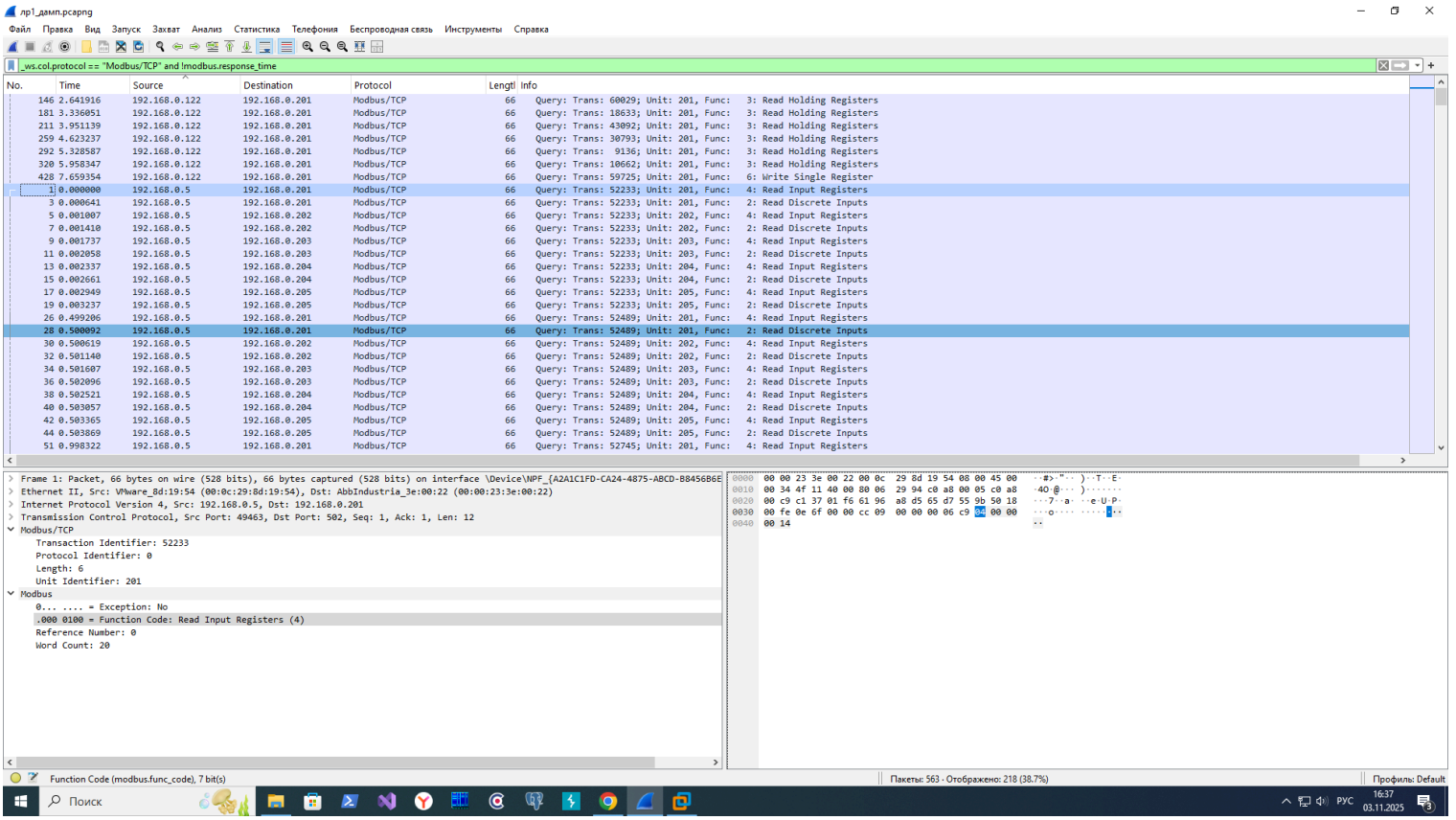
Чтобы работать только с Modbus/TCP пакетами, добавляю соответствующий фильтр:

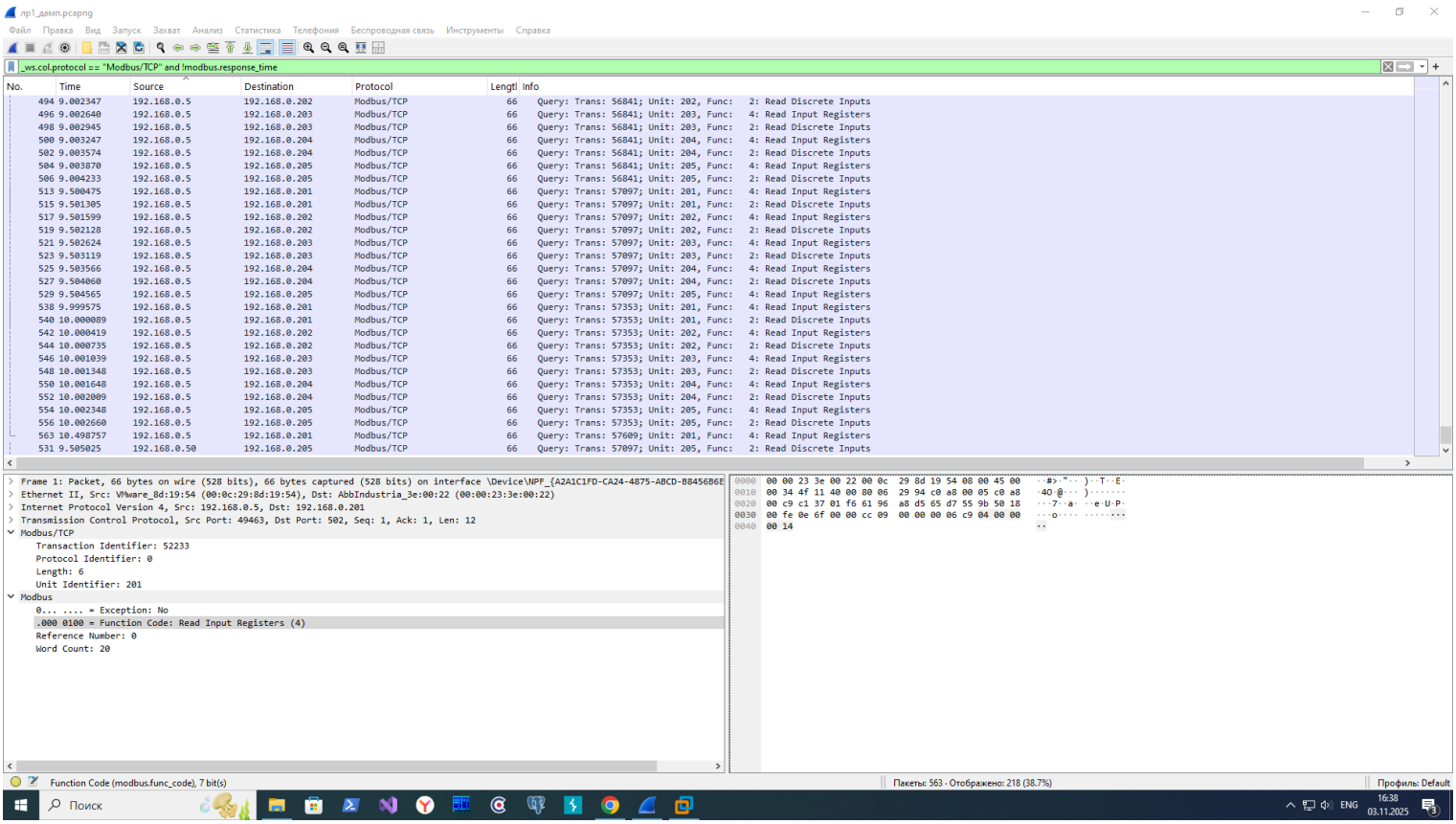


Для определения Master и Slave устройств воспользуемся тем фактом, что контроллеры на шине Modbus взаимодействуют, используя модель ведущий — ведомый; при этом именно ведущий инициирует запрос (Query).
Для определения Master устройств с помощью фильтра WireShark отфильтруем только запросы (Query):



Отсортируем отфильтрованные пакеты по столбцу Source:

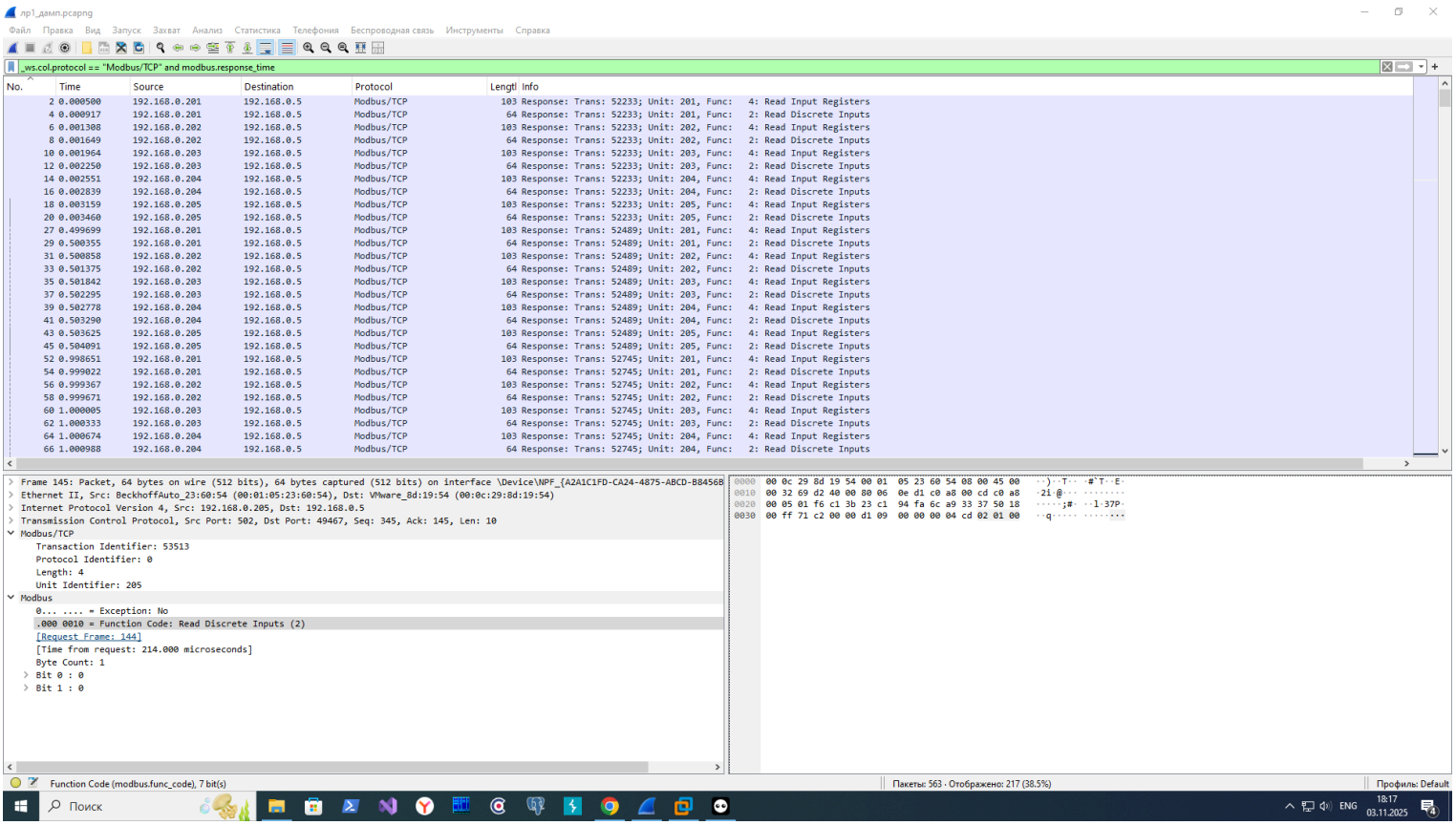




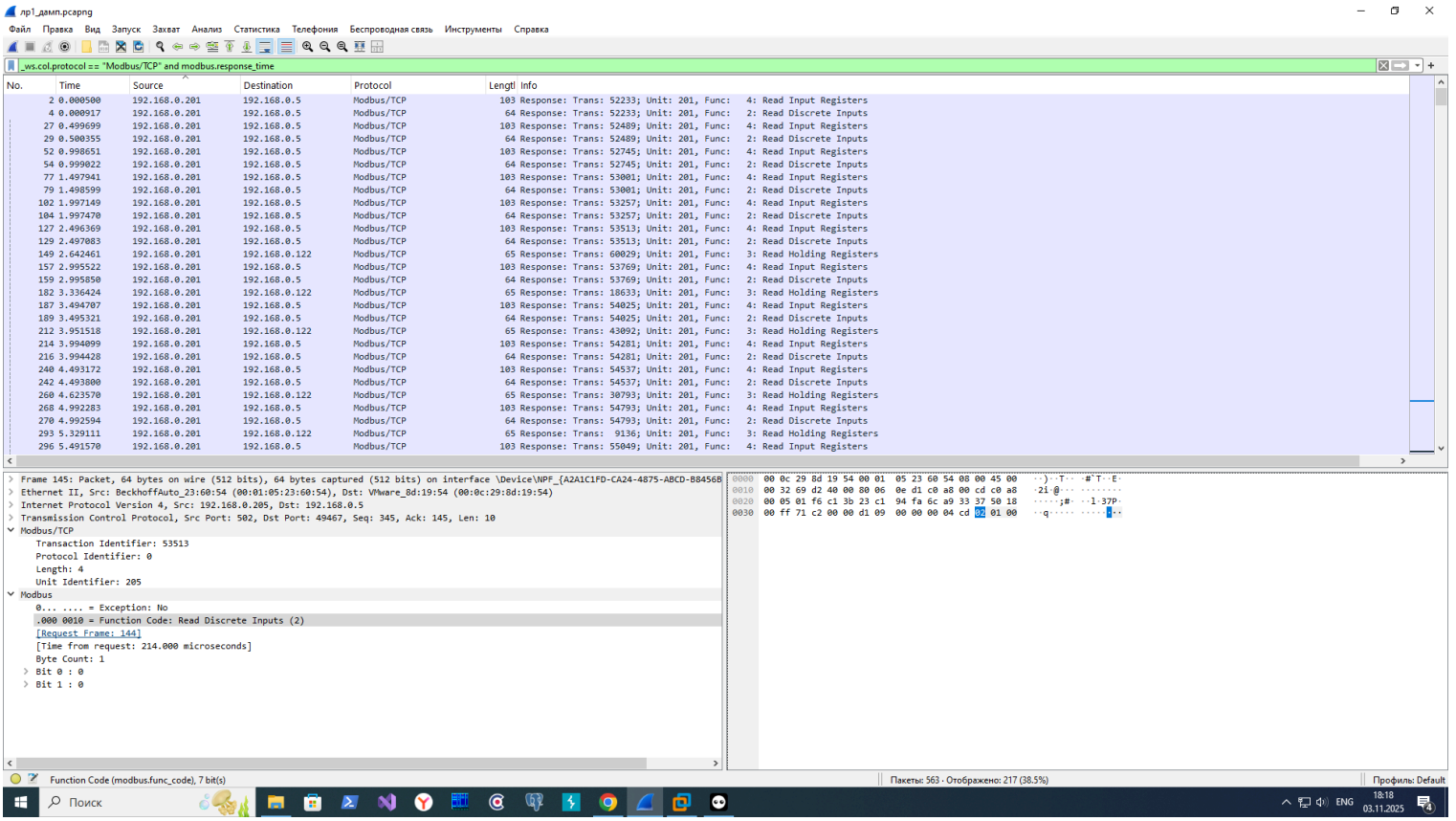
Видно, что устройствами, которые инициируют запросы являются устройства со следующими IP адресами: 192.168.0.122, 192.168.0.5 и 192.168.0.50. Устройство с IP адресом 192.168.0.5 - это Engineer PC (см. карту топологии сети), устройство с IP

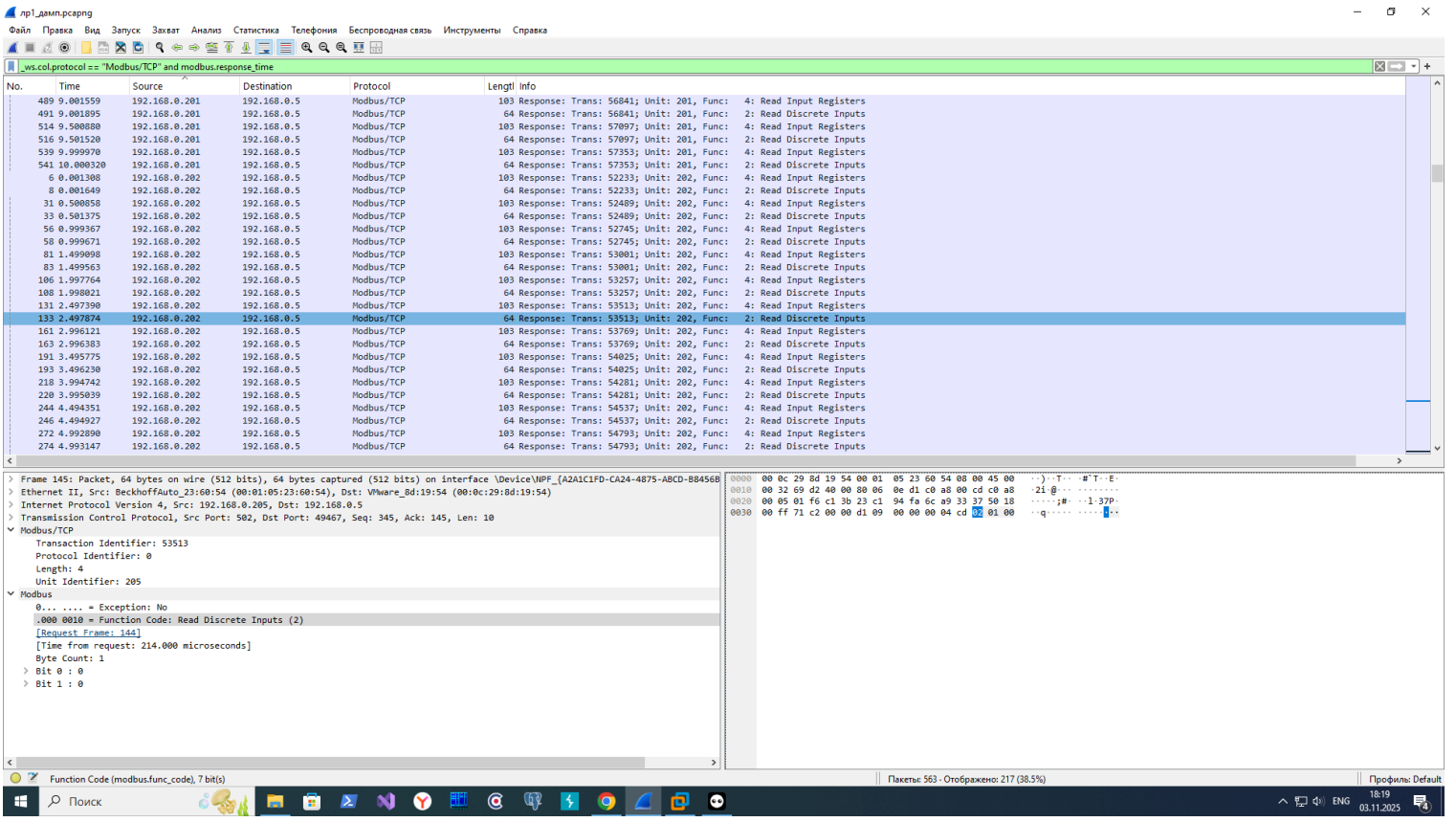
адресом 192.168.0.122 - это роутер DLink, а устройство с IP адресом 192.168.0.50 нам не известно (и от него идет всего один запрос). Поэтому Master устройствами мы можем считать Engineer PC (с IP адресом 192.168.0.5) и роутер DLink (с IP адресом 192.168.0.5).

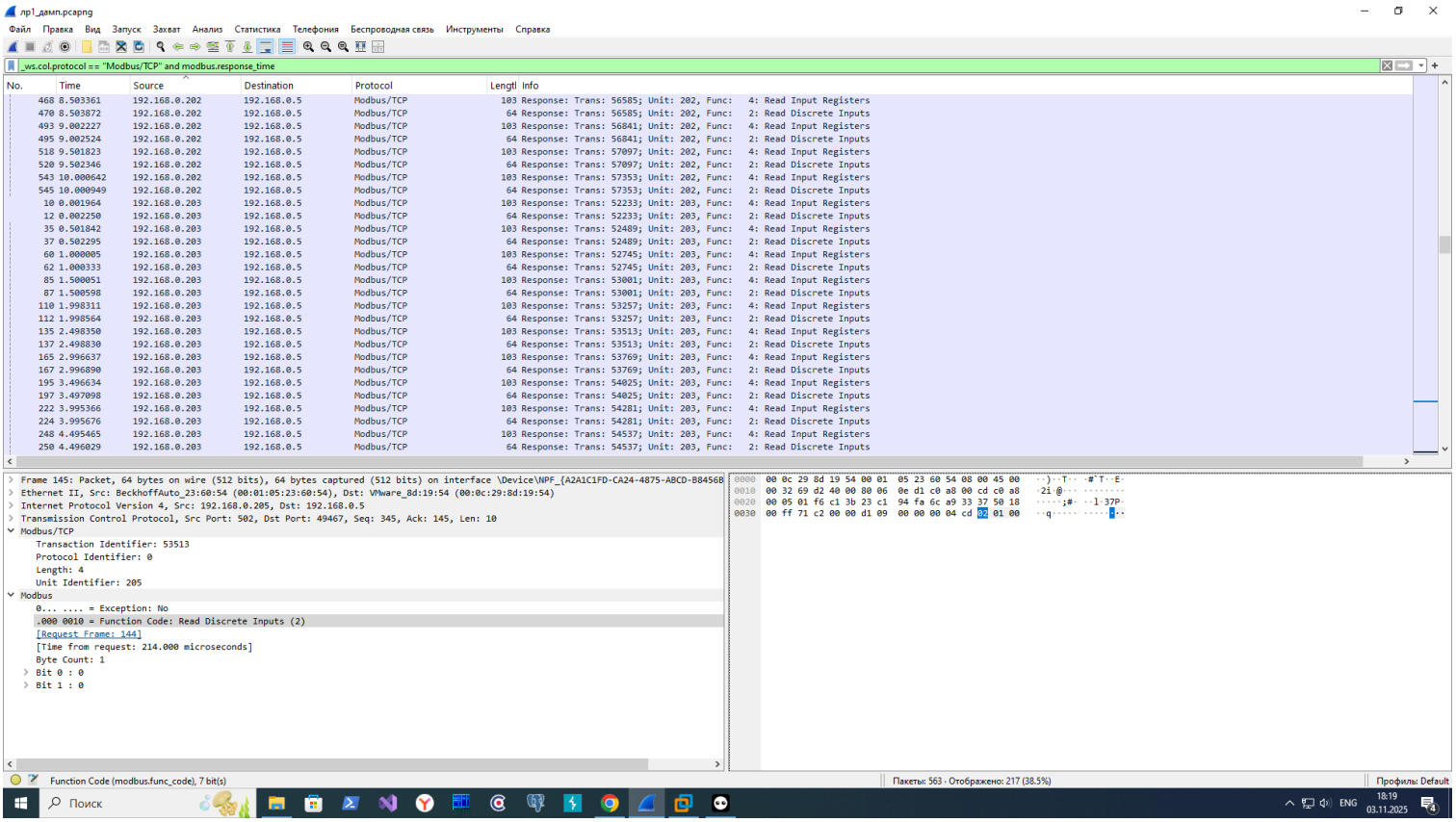
Для определения Slave устройств с помощью фильтра WireShark отфильтруем только ответы (Response):

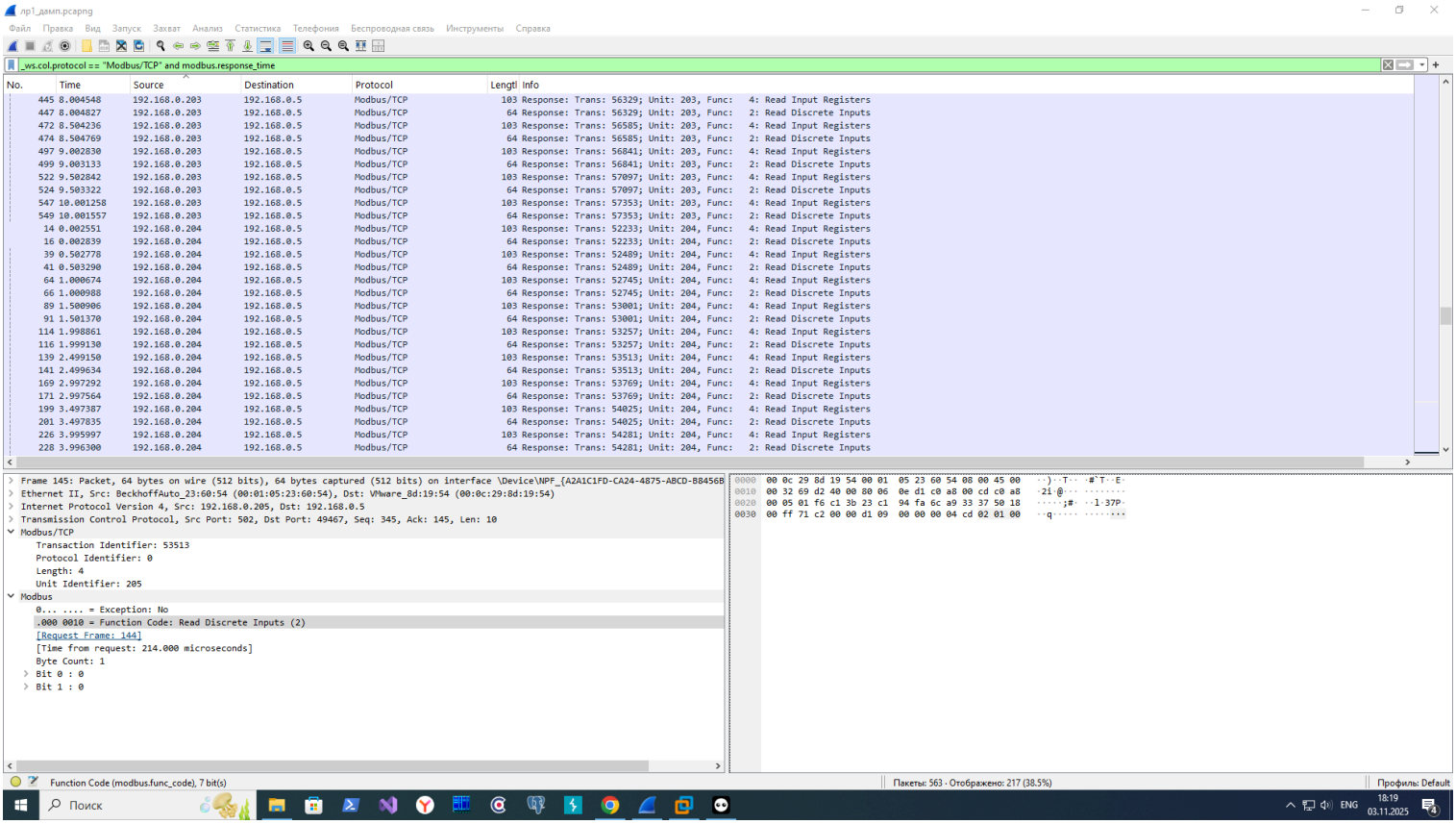


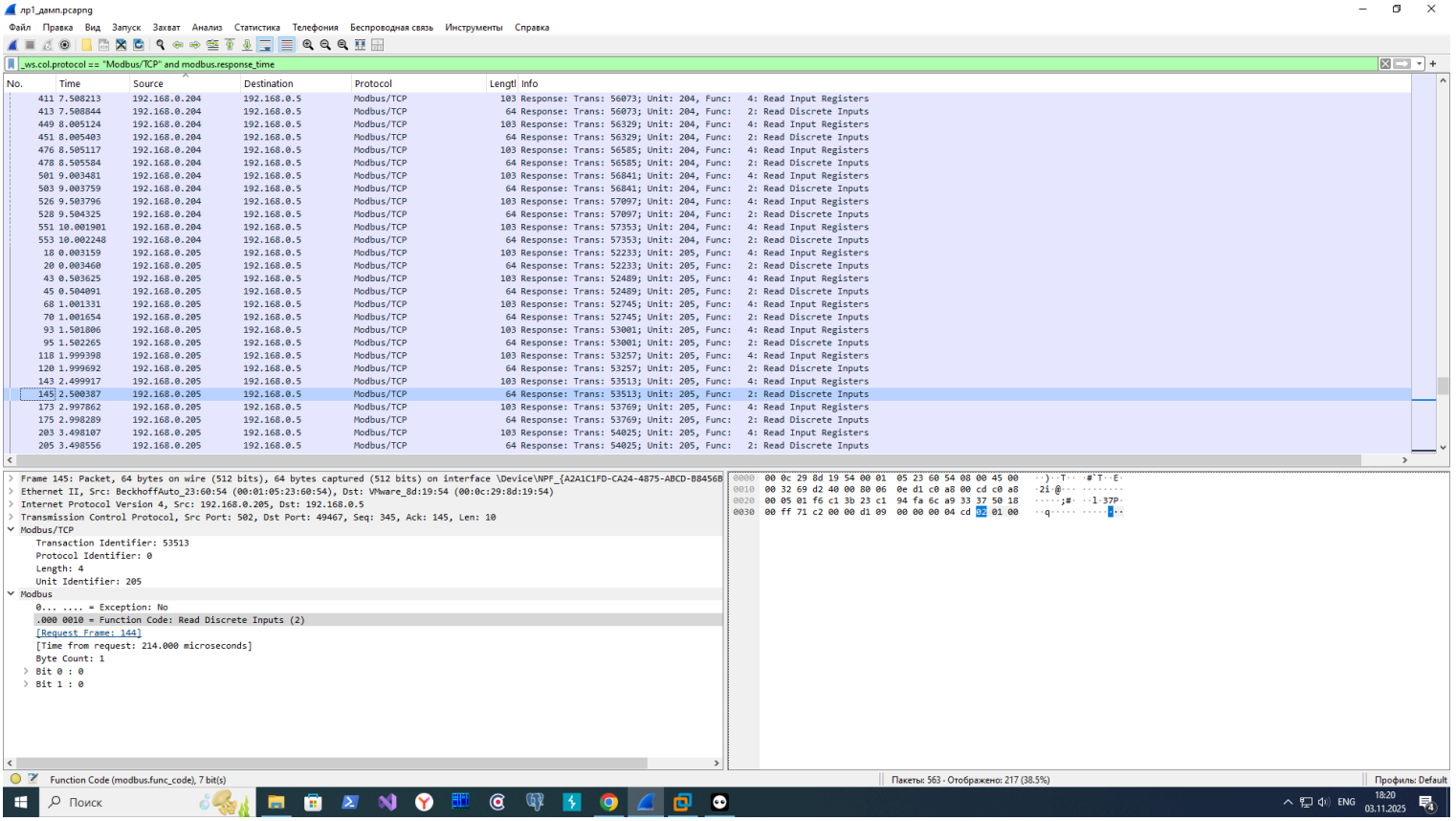
Отсортируем отфильтрованные пакеты по столбцу Source:


лр1_дамп.pcapng
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 Lengt Info
2 0.000500 192.168.0.201 192.168.0.5 Modbus/TCP 103 Response: Trans: 52233; Unit: 201, Func: 4: Read Input Registers
4 0.000917 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 0.998651 192.168.0.201 192.168.0.5 Modbus/TCP 103 Response: Trans: 52745; Unit: 201, Func: 4: Read Input Registers
54 0.999022 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
102 1.997149 192.168.0.201 192.168.0.5 Modbus/TCP 103 Response: Trans: 53257; Unit: 201, Func: 4: Read Input Registers
104 1.997470 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 2.497083 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 3.494707 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
240 4.493172 192.168.0.201 192.168.0.5 Modbus/TCP 103 Response: Trans: 54537; Unit: 201, Func: 4: Read Input Registers
242 4.493800 192.168.0.201 192.168.0.5 Modbus/TCP 64 Response: Trans: 54537; Unit: 201, Func: 2: Read Discrete Inputs
260 4.623570 192.168.0.201 192.168.0.122 Modbus/TCP 65 Response: Trans: 30793; Unit: 201, Func: 3: Read Holding Registers
268 4.992283 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 5.329111 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_8d: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
0000 00 0c 29 8d 19 54 00 01 05 23 60 54 08 00 45 00
0010 00 32 69 d2 40 00 80 06 0e d1 c0 a8 00 cd c0 a8
0020 00 05 01 f6 c1 3b 23 c1 94 fa 6c a9 33 37 50 18
0030 00 ff 71 c2 00 00 d1 09 00 00 00 04 cd 02 01 00
Function Code (modbus.func_code), 7 bit(s)
Пакеты: 563 · Отображено: 217 (38.5%)
Профиль: Default
Поиск
ENG
18:18
03.11.2025


лр1_дамп.pcapng
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 Lengt 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 9.500880 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 0.001308 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 0.500858 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 1.499098 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
106 1.997764 192.168.0.202 192.168.0.5 Modbus/TCP 103 Response: Trans: 53257; Unit: 202, Func: 4: Read Input Registers
108 1.998021 192.168.0.202 192.168.0.5 Modbus/TCP 64 Response: Trans: 53257; Unit: 202, Func: 2: Read Discrete Inputs
131 2.497390 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 2.996383 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 3.496230 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_8d: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
0000 00 0c 29 8d 19 54 00 01 05 23 60 54 08 00 45 00
0010 00 32 69 d2 40 00 80 06 0e d1 c0 a8 00 cd c0 a8
0020 00 05 01 f6 c1 3b 23 c1 94 fa 6c a9 33 37 50 18
0030 00 ff 71 c2 00 00 d1 09 00 00 00 04 cd 02 01 00
Function Code (modbus.func_code), 7 bit(s)
Пакеты: 563 · Отображено: 217 (38.5%)
Профиль: Default
Поиск
ENG
18:19
03.11.2025


лр1_дамп.pcapng
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 Lengt Info
468 8.503361 192.168.0.202 192.168.0.5 Modbus/TCP 103 Response: Trans: 56585; Unit: 202, Func: 4: Read Input Registers
470 8.503872 192.168.0.202 192.168.0.5 Modbus/TCP 64 Response: Trans: 56585; Unit: 202, Func: 2: Read Discrete Inputs
493 9.002227 192.168.0.202 192.168.0.5 Modbus/TCP 103 Response: Trans: 56841; Unit: 202, Func: 4: Read Input Registers
495 9.002524 192.168.0.202 192.168.0.5 Modbus/TCP 64 Response: Trans: 56841; Unit: 202, Func: 2: Read Discrete Inputs
518 9.501823 192.168.0.202 192.168.0.5 Modbus/TCP 103 Response: Trans: 57097; Unit: 202, Func: 4: Read Input Registers
520 9.502346 192.168.0.202 192.168.0.5 Modbus/TCP 64 Response: Trans: 57097; Unit: 202, Func: 2: Read Discrete Inputs
543 10.000642 192.168.0.202 192.168.0.5 Modbus/TCP 103 Response: Trans: 57353; Unit: 202, Func: 4: Read Input Registers
545 10.000949 192.168.0.202 192.168.0.5 Modbus/TCP 64 Response: Trans: 57353; Unit: 202, Func: 2: Read Discrete Inputs
10 0.001964 192.168.0.203 192.168.0.5 Modbus/TCP 103 Response: Trans: 52233; Unit: 203, Func: 4: Read Input Registers
12 0.002250 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 0.502295 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 1.500051 192.168.0.203 192.168.0.5 Modbus/TCP 103 Response: Trans: 53001; Unit: 203, Func: 4: Read Input Registers
87 1.500598 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: 53513; Unit: 203, Func: 4: Read Input Registers
137 2.498830 192.168.0.203 192.168.0.5 Modbus/TCP 64 Response: Trans: 53513; Unit: 203, Func: 2: Read Discrete Inputs
165 2.996637 192.168.0.203 192.168.0.5 Modbus/TCP 103 Response: Trans: 53769; Unit: 203, Func: 4: Read Input Registers
167 2.996890 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 3.995676 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-CA24-4875-ABCD-B8456B
Ethernet II, Src: BeckhoffAuto_23:60:54 (00:01:05:23:60:54), Dst: VMware_8d: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
0000 00 0c 29 8d 19 54 00 01 05 23 60 54 08 00 45 00
0010 00 32 69 d2 40 00 80 06 0e d1 c0 a8 00 cd c0 a8
0020 00 05 01 f6 c1 3b 23 c1 94 fa 6c a9 33 37 50 18
0030 00 ff 71 c2 00 00 d1 09 00 00 00 04 cd 02 01 00
Function Code (modbus.func_code), 7 bit(s)
Пакеты: 563 · Отображено: 217 (38.5%)
Профиль: Default
Поиск
ENG
18:19
03.11.2025

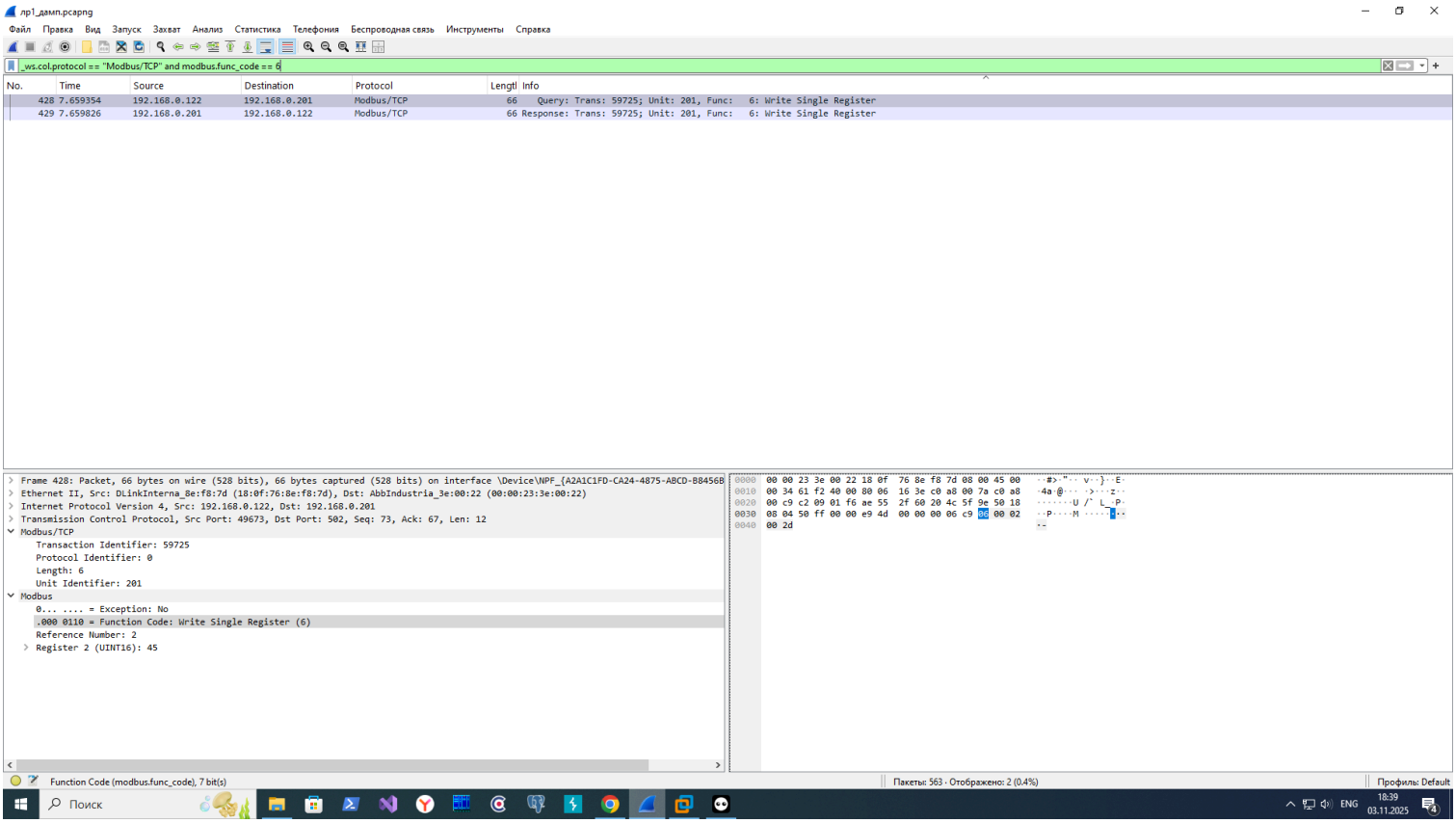

лр1_дамп.pcapng
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка
_ws.col.protocol == "Modbus/TCP" and modbus.response_time
No. Time Source Destination Protocol Lengt Info
445 8.004548 192.168.0.203 192.168.0.5 Modbus/TCP 103 Response: Trans: 56329; Unit: 203, Func: 4: Read Input Registers
447 8.004827 192.168.0.203 192.168.0.5 Modbus/TCP 64 Response: Trans: 56329; Unit: 203, Func: 2: Read Discrete Inputs
472 8.504236 192.168.0.203 192.168.0.5 Modbus/TCP 103 Response: Trans: 56585; Unit: 203, Func: 4: Read Input Registers
474 8.504769 192.168.0.203 192.168.0.5 Modbus/TCP 64 Response: Trans: 56585; Unit: 203, Func: 2: Read Discrete Inputs
497 9.002830 192.168.0.203 192.168.0.5 Modbus/TCP 103 Response: Trans: 56841; Unit: 203, Func: 4: Read Input Registers
499 9.003133 192.168.0.203 192.168.0.5 Modbus/TCP 64 Response: Trans: 56841; Unit: 203, Func: 2: Read Discrete Inputs
522 9.502842 192.168.0.203 192.168.0.5 Modbus/TCP 103 Response: Trans: 57097; Unit: 203, Func: 4: Read Input Registers
524 9.503322 192.168.0.203 192.168.0.5 Modbus/TCP 64 Response: Trans: 57097; Unit: 203, Func: 2: Read Discrete Inputs
547 10.001258 192.168.0.203 192.168.0.5 Modbus/TCP 103 Response: Trans: 57353; Unit: 203, Func: 4: Read Input Registers
549 10.001557 192.168.0.203 192.168.0.5 Modbus/TCP 64 Response: Trans: 57353; Unit: 203, Func: 2: Read Discrete Inputs
14 0.002551 192.168.0.204 192.168.0.5 Modbus/TCP 103 Response: Trans: 52233; Unit: 204, Func: 4: Read Input Registers
16 0.002839 192.168.0.204 192.168.0.5 Modbus/TCP 64 Response: Trans: 52233; Unit: 204, Func: 2: Read Discrete Inputs
39 0.502778 192.168.0.204 192.168.0.5 Modbus/TCP 103 Response: Trans: 52489; Unit: 204, Func: 4: Read Input Registers
41 0.503290 192.168.0.204 192.168.0.5 Modbus/TCP 64 Response: Trans: 52489; Unit: 204, Func: 2: Read Discrete Inputs
64 1.000674 192.168.0.204 192.168.0.5 Modbus/TCP 103 Response: Trans: 52745; Unit: 204, Func: 4: Read Input Registers
66 1.000988 192.168.0.204 192.168.0.5 Modbus/TCP 64 Response: Trans: 52745; Unit: 204, Func: 2: Read Discrete Inputs
89 1.500906 192.168.0.204 192.168.0.5 Modbus/TCP 103 Response: Trans: 53001; Unit: 204, Func: 4: Read Input Registers
91 1.501370 192.168.0.204 192.168.0.5 Modbus/TCP 64 Response: Trans: 53001; Unit: 204, Func: 2: Read Discrete Inputs
114 1.998861 192.168.0.204 192.168.0.5 Modbus/TCP 103 Response: Trans: 53257; Unit: 204, Func: 4: Read Input Registers
116 1.999130 192.168.0.204 192.168.0.5 Modbus/TCP 64 Response: Trans: 53257; Unit: 204, Func: 2: Read Discrete Inputs
139 2.499150 192.168.0.204 192.168.0.5 Modbus/TCP 103 Response: Trans: 53513; Unit: 204, Func: 4: Read Input Registers
141 2.499634 192.168.0.204 192.168.0.5 Modbus/TCP 64 Response: Trans: 53513; Unit: 204, Func: 2: Read Discrete Inputs
169 2.997292 192.168.0.204 192.168.0.5 Modbus/TCP 103 Response: Trans: 53769; Unit: 204, Func: 4: Read Input Registers
171 2.997564 192.168.0.204 192.168.0.5 Modbus/TCP 64 Response: Trans: 53769; Unit: 204, Func: 2: Read Discrete Inputs
199 3.497387 192.168.0.204 192.168.0.5 Modbus/TCP 103 Response: Trans: 54025; Unit: 204, Func: 4: Read Input Registers
201 3.497835 192.168.0.204 192.168.0.5 Modbus/TCP 64 Response: Trans: 54025; Unit: 204, Func: 2: Read Discrete Inputs
226 3.995997 192.168.0.204 192.168.0.5 Modbus/TCP 103 Response: Trans: 54281; Unit: 204, Func: 4: Read Input Registers
228 3.996300 192.168.0.204 192.168.0.5 Modbus/TCP 64 Response: Trans: 54281; Unit: 204, 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_8d: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
0000 00 0c 29 8d 19 54 00 01 05 23 60 54 08 00 45 00
0010 00 32 69 d2 40 00 80 06 0e d1 c0 a8 00 cd c0 a8
0020 00 05 01 f6 c1 3b 23 c1 94 fa 6c a9 33 37 50 18
0030 00 ff 71 c2 00 00 d1 09 00 00 00 04 cd 02 01 00
Function Code (modbus.func_code), 7 bit(s)
Пакеты: 563 · Отображено: 217 (38.5%)
Профиль: Default
Поиск
ENG
18:19
03.11.2025



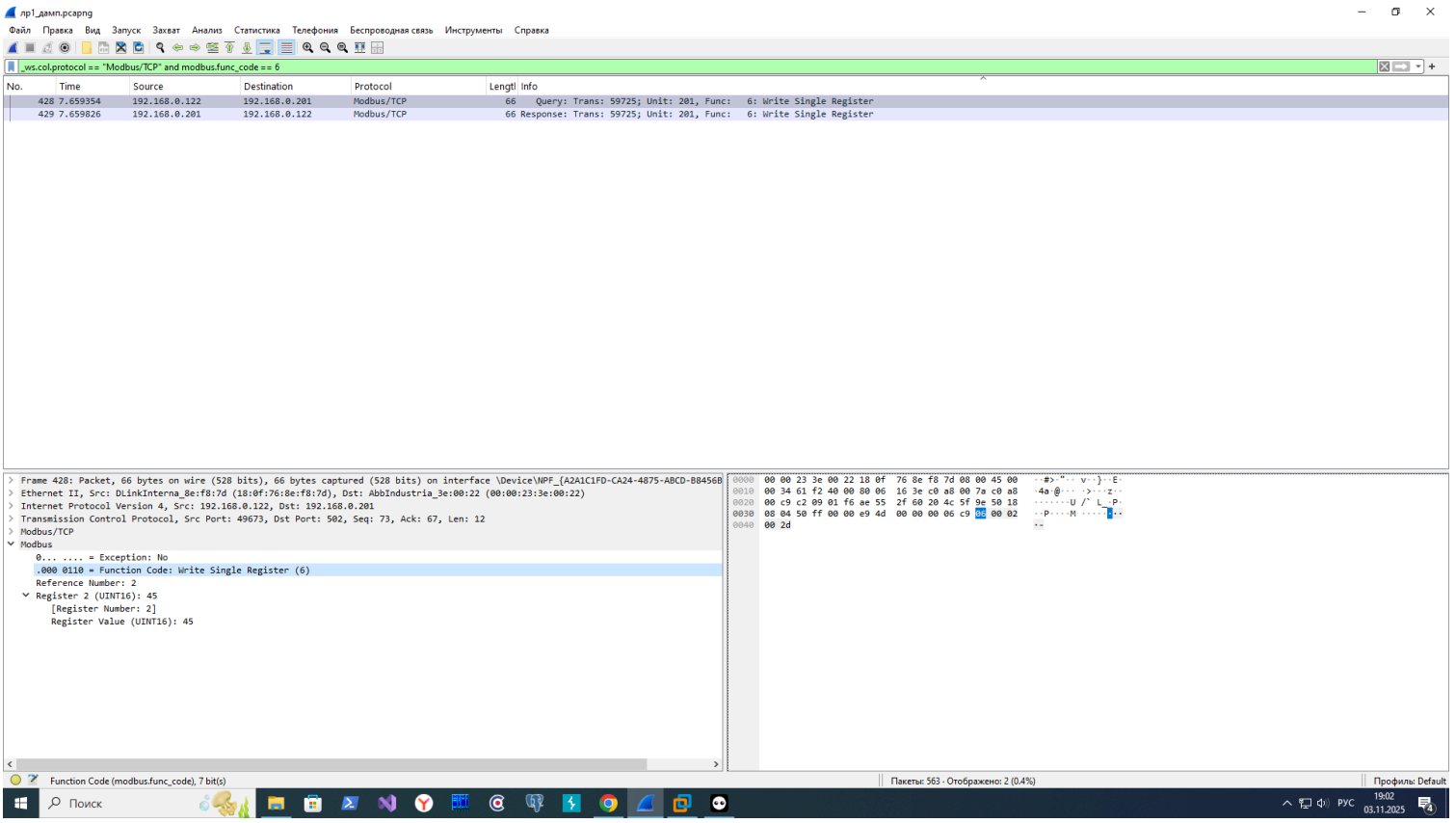
Видно, что устройствами, которые отправляют ответы являются устройства со следующими IP адресами: 192.168.0.201, 192.168.0.202, 192.168.0.203, 192.168.0.204 и 192.168.0.205. Все эти устройства являются PLC разного вида - поэтому всех их можно считать Slave устройствами.

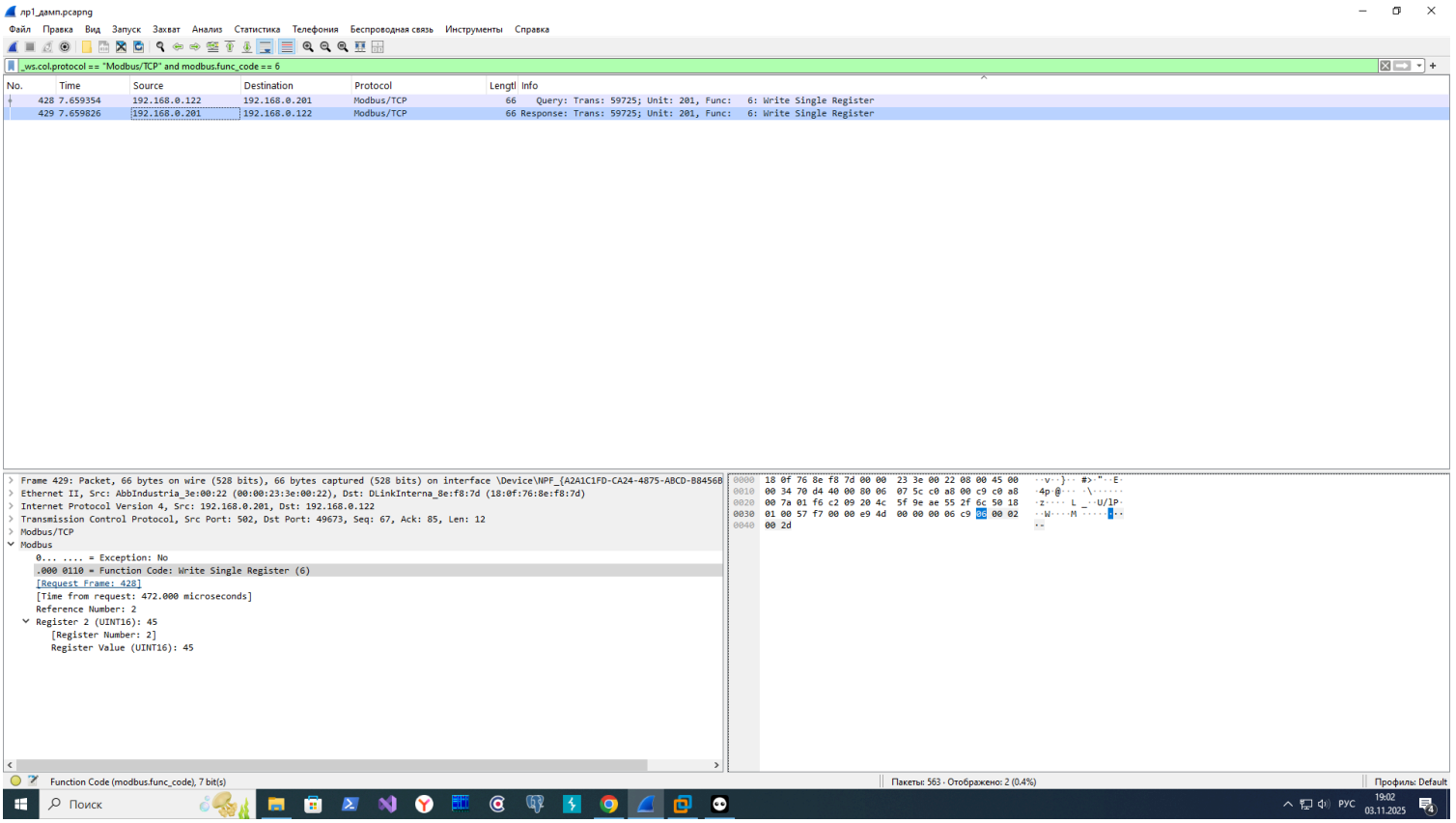
3. Идентификация пары «запрос-ответ».

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



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:

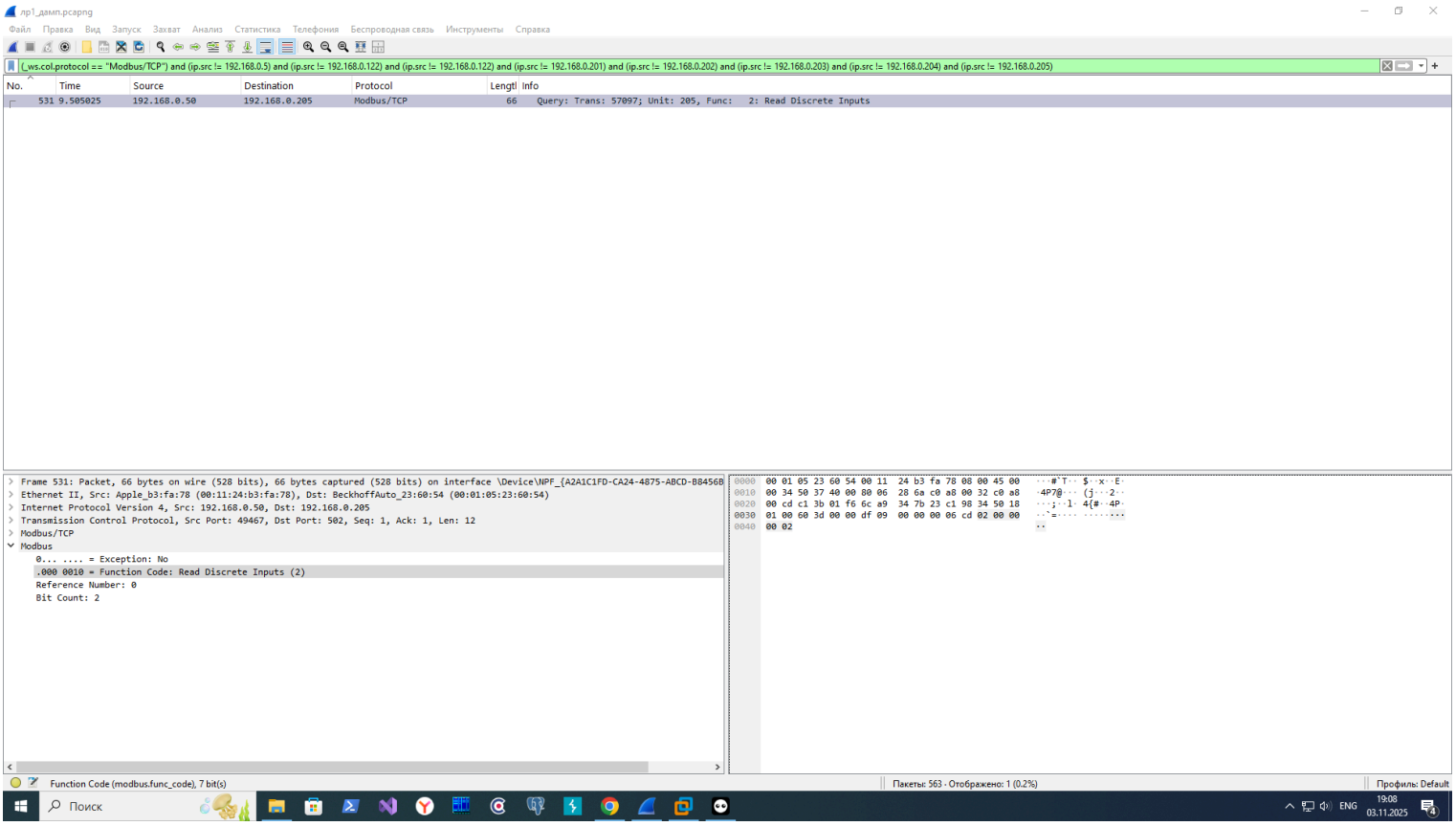




Видно, что в регистр 2 было записано значение 45

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.