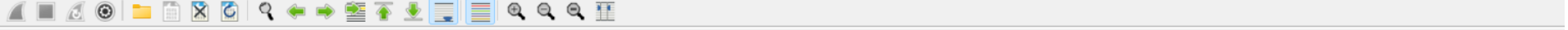

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1566	30.418993	192.168.0.202	192.168.0.102	Modbus/TCP	66	Response: Trans: 44002; Unit: 255, Func: 16: Write Multiple Registers
1567	30.426386	192.168.0.102	192.168.0.202	Modbus/TCP	66	Query: Trans: 44003; Unit: 255, Func: 3: Read Holding Registers
1568	30.433075	192.168.0.202	192.168.0.102	Modbus/TCP	67	Response: Trans: 44003; Unit: 255, Func: 3: Read Holding Registers
1569	30.442520	192.168.0.102	192.168.0.202	Modbus/TCP	77	Query: Trans: 44004; Unit: 255, Func: 16: Write Multiple Registers
1570	30.449074	192.168.0.202	192.168.0.102	Modbus/TCP	66	Response: Trans: 44004; Unit: 255, Func: 16: Write Multiple Registers
1571	30.453376	192.168.0.102	192.168.0.202	Modbus/TCP	66	Query: Trans: 44005; Unit: 255, Func: 3: Read Holding Registers
1572	30.460050	192.168.0.202	192.168.0.102	Modbus/TCP	67	Response: Trans: 44005; Unit: 255, Func: 3: Read Holding Registers
1573	30.463326	Dataindustri_07:19:…	SiemensIndus_b0:8d:6f	ARP	60	Who has 192.168.0.202? Tell 192.168.0.102 (duplicate use of 192.168.0.102 detected!)
1574	30.463326	Dataindustri_07:19:…	SiemensIndus_b0:8d:ce	ARP	60	Who has 192.168.0.102? Tell 192.168.0.202 (duplicate use of 192.168.0.202 detected!)
1575	30.465291	SiemensIndus_b0:8d:…	Dataindustri_07:19:98	ARP	60	192.168.0.202 is at e0:dc:a0:b0:8d:6f (duplicate use of 192.168.0.102 detected!)
1576	30.465291	SiemensIndus_b0:8d:…	Dataindustri_07:19:98	ARP	60	192.168.0.102 is at e0:dc:a0:b0:8d:ce (duplicate use of 192.168.0.202 detected!)
1577	30.465291	192.168.0.102	192.168.0.202	Modbus/TCP	66	Query: Trans: 44006; Unit: 255, Func: 3: Read Holding Registers
1578	30.605050	192.168.0.102	192.168.0.202	TCP	66	[TCP Retransmission] 504 → 502 [PSH, ACK] Seq=4088 Ack=3434 Win=8192 Len=12
1579	30.611111	192.168.0.202	192.168.0.102	Modbus/TCP	67	Response: Trans: 44006; Unit: 255, Func: 3: Read Holding Registers
1580	30.616690	192.168.0.202	192.168.0.102	TCP	67	[TCP Retransmission] 502 → 504 [PSH, ACK] Seq=3434 Ack=4100 Win=8192 Len=13
1581	30.622640	192.168.0.102	192.168.0.202	Modbus/TCP	77	Query: Trans: 44007; Unit: 255, Func: 16: Write Multiple Registers
1582	30.629033	192.168.0.102	192.168.0.202	TCP	77	[TCP Retransmission] 504 → 502 [PSH, ACK] Seq=4100 Ack=3447 Win=8192 Len=23
1583	30.635179	192.168.0.202	192.168.0.102	Modbus/TCP	66	Response: Trans: 44007; Unit: 255, Func: 16: Write Multiple Registers
1584	30.640932	192.168.0.202	192.168.0.102	TCP	66	[TCP Retransmission] 502 → 504 [PSH, ACK] Seq=3447 Ack=4123 Win=8192 Len=12
1585	30.645534	192.168.0.102	192.168.0.202	Modbus/TCP	66	Query: Trans: 44008; Unit: 255, Func: 3: Read Holding Registers
1586	30.653066	192.168.0.102	192.168.0.202	TCP	66	[TCP Retransmission] 504 → 502 [PSH, ACK] Seq=4123 Ack=3459 Win=8192 Len=12
1587	30.659163	192.168.0.202	192.168.0.102	Modbus/TCP	67	Response: Trans: 44008; Unit: 255, Func: 3: Read Holding Registers
1588	30.665147	192.168.0.202	192.168.0.102	TCP	67	[TCP Retransmission] 502 → 504 [PSH, ACK] Seq=3459 Ack=4135 Win=8192 Len=13
1589	30.675397	192.168.0.102	192.168.0.202	Modbus/TCP	77	Query: Trans: 44009; Unit: 255, Func: 16: Write Multiple Registers

Gói tin Modbus TCP truyền nhận giữa hai PLC trước khi hệ thống bị tấn công

Bản tin giả mạo địa chỉ gửi đến hai PLC

Các gói tin Modbus TCP đã được gửi đến thiết bị tấn công

Các gói tin Modbus TCP được chuyển tiếp đến PLC còn lại