

1. Введение.

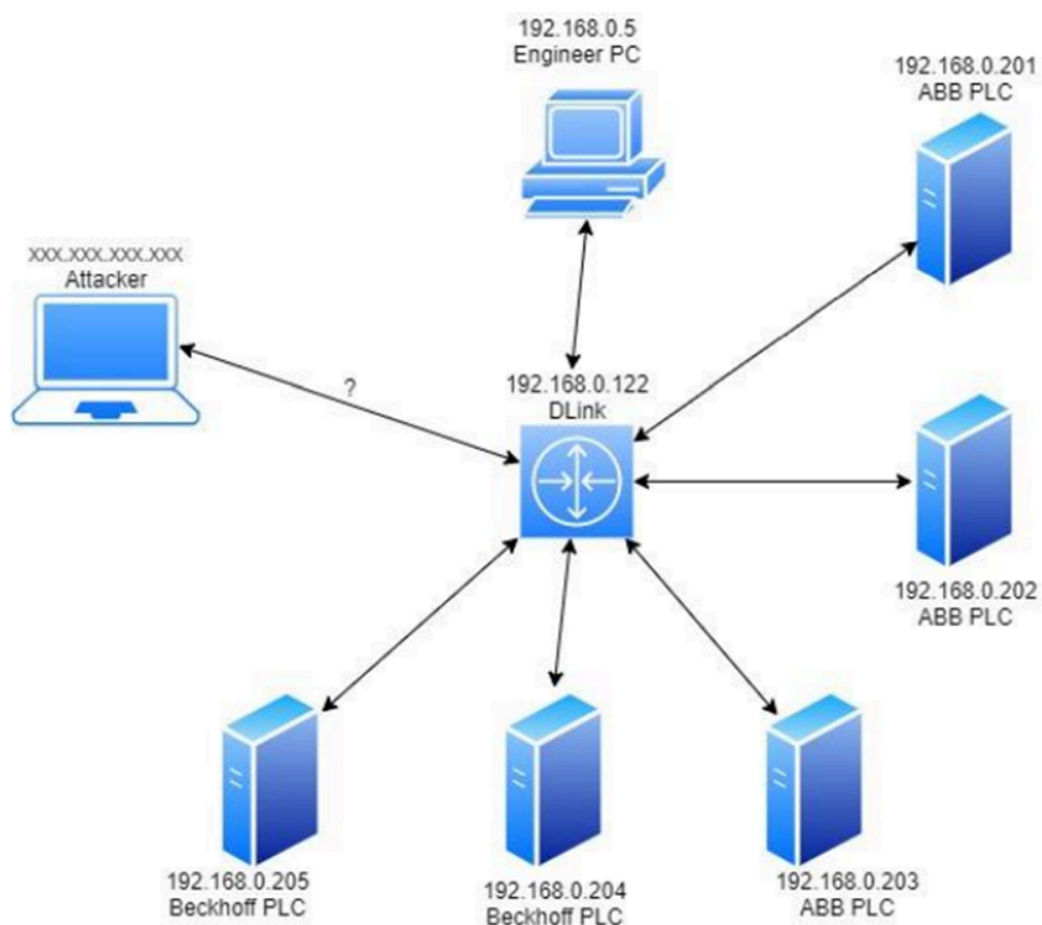
Цель и задачи задания.

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:

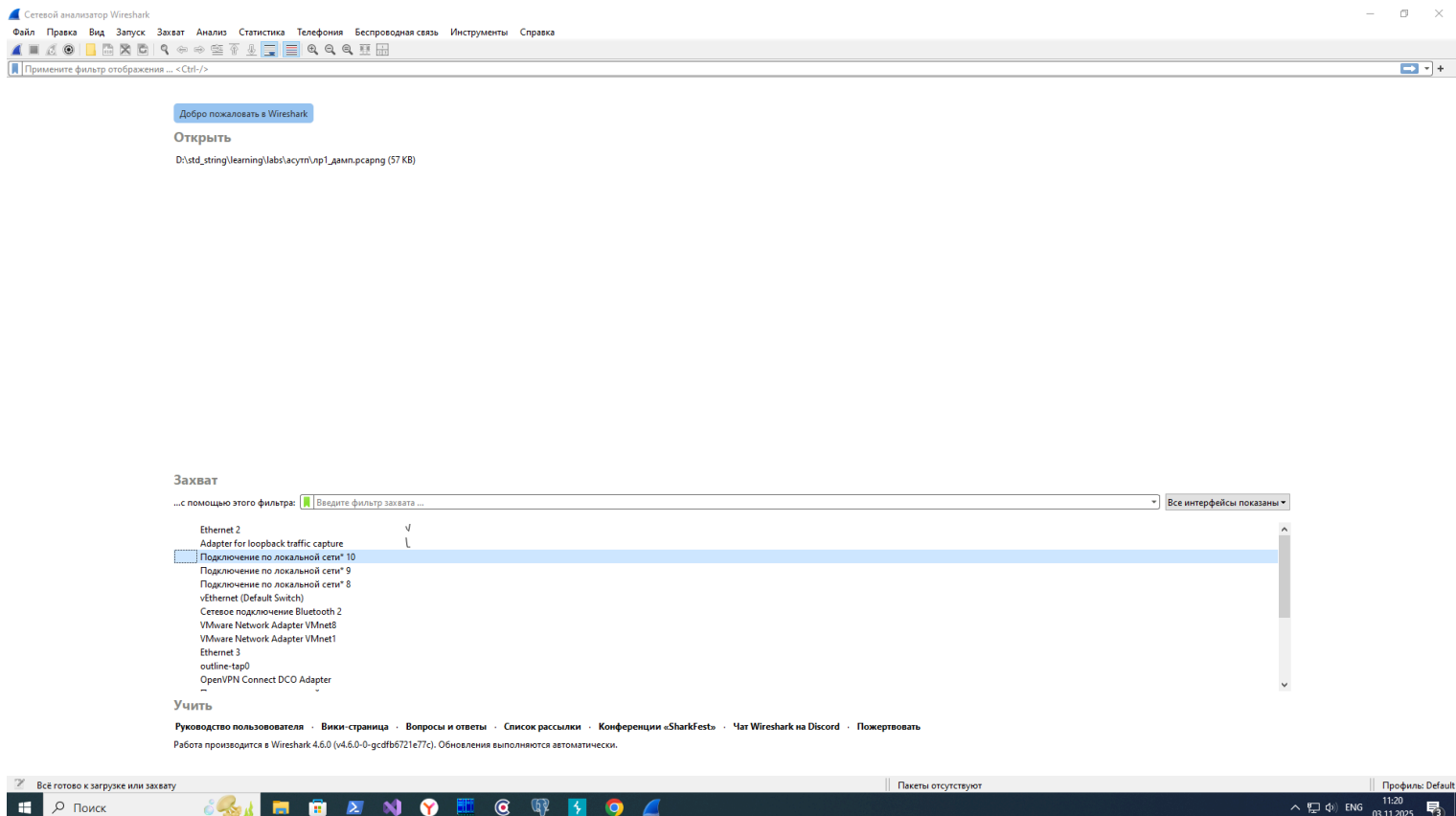
Контроллеры на шине Modbus взаимодействуют, используя модель ведущий — ведомый, основанную на транзакциях, состоящих из запроса и ответа.

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:

Скриншот интерфейса Wireshark, показывающий захваченный трафик. В таблице пакетов (Packet List) видны пакеты, идентифицированные как Modbus/TCP. Например, пакеты 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000, 1001, 1002, 1003, 1004, 1005, 1006, 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014, 1015, 1016, 1017, 1018, 1019, 1020, 1021, 1022, 1023, 1024, 1025, 1026, 1027, 1028, 1029, 1030, 1031, 1032, 1033, 1034, 1035, 1036, 1037, 1038, 1039, 1040, 1041, 1042, 1043, 1044, 1045, 1046, 1047, 1048, 1049, 1050, 1051, 1052, 1053, 1054, 1055, 1056, 1057, 1058, 1059, 1060, 1061, 1062, 1063, 1064, 1065, 1066, 1067, 1068, 1069, 1070, 1071, 1072, 1073, 1074, 1075, 1076, 1077, 1078, 1079, 1080, 1081, 1082, 1083, 1084, 1085, 1086, 1087, 1088, 1089, 1090, 1091, 1092, 1093, 1094, 1095, 1096, 1097, 1098, 1099, 1100, 1101, 1102, 1103, 1104, 1105, 1106, 1107, 1108, 1109, 1110, 1111, 1112, 1113, 1114, 1115, 1116, 1117, 1118, 1119, 1120, 1121, 1122, 1123, 1124, 1125, 1126, 1127, 1128, 1129, 1130, 1131, 1132, 1133, 1134, 1135, 1136, 1137, 1138, 1139, 1140, 1141, 1142, 1143, 1144, 1145, 1146, 1147, 1148, 1149, 1150, 1151, 1152, 1153, 1154, 1155, 1156, 1157, 1158, 1159, 1160, 1161, 1162, 1163, 1164, 1165, 1166, 1167, 1168, 1169, 1170, 1171, 1172, 1173, 1174, 1175, 1176, 1177, 1178, 1179, 1180, 1181, 1182, 1183, 1184, 1185, 1186, 1187, 1188, 1189, 1190, 1191, 1192, 1193, 1194, 1195, 1196, 1197, 1198, 1199, 1200, 1201, 1202, 1203, 1204, 1205, 1206, 1207, 1208, 1209, 1210, 1211, 1212, 1213, 1214, 1215, 1216, 1217, 1218, 1219, 1220, 1221, 1222, 1223, 1224, 1225, 1226, 1227, 1228, 1229, 1230, 1231, 1232, 1233, 1234, 1235, 1236, 1237, 1238, 1239, 1240, 1241, 1242, 1243, 1244, 1245, 1246, 1247, 1248, 1249, 1250, 1251, 1252, 1253, 1254, 1255, 1256, 1257, 1258, 1259, 1260, 1261, 1262, 1263, 1264, 1265, 1266, 1267, 1268, 1269, 1270, 1271, 1272, 1273, 1274, 1275, 1276, 1277, 1278, 1279, 1280, 1281, 1282, 1283, 1284, 1285, 1286, 1287, 1288, 1289, 1290, 1291, 1292, 1293, 1294, 1295, 1296, 1297, 1298, 1299, 1300, 1301, 1302, 1303, 1304, 1305, 1306, 1307, 1308, 1309, 1310, 1311, 1312, 1313, 1314, 1315, 1316, 1317, 1318, 1319, 1320, 1321, 1322, 1323, 1324, 1325, 1326, 1327, 1328, 1329, 1330, 1331, 1332, 1333, 1334, 1335, 1336, 1337, 1338, 1339, 1340, 1341, 1342, 1343, 1344, 1345, 1346, 1347, 1348, 1349, 1350, 1351, 1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359, 1360, 1361, 1362, 1363, 1364, 1365, 1366, 1367, 1368, 1369, 1370, 1371, 1372, 1373, 1374, 1375, 1376, 1377, 1378, 1379, 1380, 1381, 1382, 1383, 1384, 1385, 1386, 1387, 1388, 1389, 1390, 1391, 1392, 1393, 1394, 1395, 1396, 1397, 1398, 1399, 1400, 1401, 1402, 1403, 1404, 1405, 1406, 1407, 1408, 1409, 1410, 1411, 1412, 1413, 1414, 1415, 1416, 1417, 1418, 1419, 1420, 1421, 1422, 1423, 1424, 1425, 1426, 1427, 1428, 1429, 1430, 1431, 1432, 1433, 1434, 1435, 1436, 1437, 1438, 1439, 1440, 1441, 1442, 1443, 1444, 1445, 1446, 1447, 1448, 1449, 1450, 1451, 1452, 1453, 1454, 1455, 1456, 1457, 1458, 1459, 1460, 1461, 1462, 1463, 1464, 1465, 1466, 1467, 1468, 1469, 1470, 1471, 1472, 1473, 1474, 1475, 1476, 1477, 1478, 1479, 1480, 1481, 1482, 1483, 1484, 1485, 1486, 1487, 1488, 1489, 1490, 1491, 1492, 1493, 1494, 1495, 1496, 1497, 1498, 1499, 1500, 1501, 1502, 1503, 1504, 1505, 1506, 1507, 1508, 1509, 1510, 1511, 1512, 1513, 1514, 1515, 1516, 1517, 1518, 1519, 1520, 1521, 1522, 1523, 1524, 1525, 1526, 1527, 1528, 1529, 1530, 1531, 1532, 1533, 1534, 1535, 1536, 1537, 1538, 1539, 1540, 1541, 1542, 1543, 1544, 1545, 1546, 1547, 1548, 1549, 1550, 1551, 1552, 1553, 1554, 1555, 1556, 1557, 1558, 1559, 1560, 1561, 1562, 1563, 1564, 1565, 1566, 1567, 1568, 1569, 1570, 1571, 1572, 1573, 1574, 1575, 1576, 1577, 1578, 1579, 1580, 1581, 1582, 1583, 1584, 1585, 1586, 1587, 1588, 1589, 1590, 1591, 1592, 1593, 1594, 1595, 1596, 1597, 1598, 1599, 1600, 1601, 1602, 1603, 1604, 1605, 1606, 1607, 1608, 1609, 1610, 1611, 1612, 1613, 1614, 1615, 1616, 1617, 1618, 1619, 1620, 1621, 1622, 1623, 1624, 1625, 1626, 1627, 1628, 1629, 1630, 1631, 1632, 1633, 1634, 1635, 1636, 1637, 1638, 1639, 1640, 1641, 1642, 1643, 1644, 1645, 1646, 1647, 1648, 1649, 1650, 1651, 1652, 1653, 1654, 1655, 1656, 1657, 1658, 1659, 1660, 1661, 1662, 1663, 1664, 1665, 1666, 1667, 1668, 1669, 1670, 1671, 1672, 1673, 1674, 1675, 1676, 1677, 1678, 1679, 1680, 1681, 1682, 1683, 1684, 1685, 1686, 1687, 1688, 1689, 1690, 1691, 1692, 1693, 1694, 1695, 1696, 1697, 1698, 1699, 1700, 1701, 1702, 1703, 1704, 1705, 1706, 1707, 1708, 1709, 1710, 1711, 1712, 1713, 1714, 1715, 1716, 1717, 1718, 1719, 1720, 1721, 1722, 1723, 1724, 1725, 1726, 1727, 1728, 1729, 1730, 1731, 1732, 1733, 1734, 1735, 1736, 1737, 1738, 1739, 1740, 1741, 1742, 1743, 1744, 1745, 1746, 1747, 1748, 1749, 1750, 1751, 1752, 1753, 1754, 1755, 1756, 1757, 1758, 1759, 1760, 1761, 1762, 1763, 1764, 1765, 1766, 1767, 1768, 1769, 1770, 1771, 1772, 1773, 1774, 1775, 1776, 1777, 1778, 1779, 1780, 1781, 1782, 1783, 1784, 1785, 1786, 1787, 1788, 1789, 1790, 1791, 1792, 1793, 1794, 1795, 1796, 1797, 1798, 1799, 1800, 1801, 1802, 1803, 1804, 1805, 1806, 1807, 1808, 1809, 1810, 1811, 1812, 1813, 1814, 1815, 1816, 1817, 1818, 1819, 1820, 1821, 1822, 1823, 1824, 1825, 1826, 1827, 1828, 1829, 1830, 1831, 1832, 1833, 1834, 1835, 1836, 1837, 1838, 1839, 1840, 1841, 1842, 1843, 1844, 1845, 1846, 1847, 1848, 1849, 1850, 1851, 1852, 1853, 1854, 1855, 1856, 1857, 1858, 1859, 1860, 1861, 1862, 1863, 1864, 1865, 1866, 1867, 1868, 1869, 1870, 1871, 1872, 1873, 1874, 1875, 1876, 1877, 1878, 1879, 1880, 1881, 1882, 1883, 1884, 1885, 1886, 1887, 1888, 1889, 1890, 1891, 1892, 1893, 1894, 1895, 1896, 1897, 1898, 1899, 1900, 1901, 1902, 1903, 1904, 1905, 1906, 1907, 1908, 1909, 1910, 1911, 1912, 1913, 1914, 1915, 1916, 1917, 1918, 1919, 1920, 1921, 1922, 1923, 1924, 1925, 1926, 1927, 1928, 1929, 1930, 1931, 1932, 1933, 1934, 1935, 1936, 1937, 1938, 1939, 1940, 1941, 1942, 1943, 1944, 1945, 1946, 1947, 1948, 1949, 1950, 1951, 1952, 1953, 1954, 1955, 1956, 1957, 1958, 1959, 1960, 1961, 1962, 1963, 1964, 1965, 1966, 1967, 1968, 1969, 1970, 1971, 1972, 1973, 1974, 1975, 1976, 1977, 1978, 1979, 1980, 1981, 1982, 1983, 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 223

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

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

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like opening files, saving, and analyzing. The main window is divided into three panes:

- Packet List:** Displays a list of captured packets. The filter bar at the top shows the filter: `_ws.col.protocol == "Modbus/TCP" and !modbus.response_time`. The list includes columns for No., Time, Source, Destination, Protocol, and Length. The first packet (No. 1) is a Modbus/TCP query from 192.168.0.5 to 192.168.0.201.
- Packet Details:** Shows the hierarchical structure of the selected packet (No. 1). It includes Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Modbus/TCP. The Modbus/TCP section shows a Transaction Identifier of 52233, a Unit Identifier of 201, and a Function Code of Read Input Registers (4).
- Packet Bytes:** Displays the raw packet data in hexadecimal and ASCII. The first 14 bytes are shown, corresponding to the Ethernet II header.

The bottom status bar indicates the current time (03.11.2025) and the number of packets displayed (218 out of 563).

Отсортируем отфильтрованные пакеты по столбцу Source:

Скриншот программы Wireshark, отображающей сетевой трафик. В верхней панели меню и панели инструментов. Основная панель отображает список пакетов (No., Time, Source, Destination, Protocol, Length, Info). В нижней панели детализации (Packet Details) и панелей данных (Packet Bytes) и Hex-View.

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	3.336851	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 18633; Unit: 201, Func: 3: Read Holding Registers
211	3.951139	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 43092; Unit: 201, Func: 3: Read Holding Registers
250	4.623237	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: 9136; Unit: 201, Func: 3: Read Holding Registers
328	5.958347	192.168.0.122	192.168.0.201	Modbus/TCP	66	Query: Trans: 10662; 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
1	0.000000	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 52233; Unit: 201, Func: 4: Read Input Registers
3	0.000641	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: 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
7	0.001418	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	0.002940	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	0.499206	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: 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
30	0.500619	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	192.168.0.202	Modbus/TCP	66	Query: Trans: 52489; Unit: 202, Func: 2: Read Discrete Inputs
34	0.501607	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 52489; Unit: 203, Func: 4: Read Input Registers
36	0.502096	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 52489; Unit: 203, Func: 2: Read Discrete Inputs
38	0.502521	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 52489; Unit: 204, Func: 4: Read Input Registers
40	0.503057	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 52489; Unit: 204, Func: 2: Read Discrete Inputs
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

Детализация пакета 1 (Frame 1):

- Ethernet II, Src: VMware_Bd1:19:54 (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
 - 0000 0100 = Function Code: Read Input Registers (4)
 - Reference Number: 0
 - Word Count: 20

Пакеты: 563 - Отображено: 218 (38.7%)

Скриншот программы Wireshark, отображающей сетевой трафик. В верхней панели меню и панели инструментов. Основная панель отображает список пакетов (No., Time, Source, Destination, Protocol, Length, Info). В нижней панели детализации (Packet Details) и панелей данных (Packet Bytes) и Hex-View.

No.	Time	Source	Destination	Protocol	Length	Info
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	9.500475	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 57097; Unit: 201, Func: 4: Read Input Registers
515	9.501305	192.168.0.5	192.168.0.201	Modbus/TCP	66	Query: Trans: 57097; Unit: 201, Func: 2: Read Discrete Inputs
517	9.501599	192.168.0.5	192.168.0.202	Modbus/TCP	66	Query: Trans: 57097; Unit: 202, Func: 4: Read Input Registers
519	9.502128	192.168.0.5	192.168.0.202	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	9.503119	192.168.0.5	192.168.0.203	Modbus/TCP	66	Query: Trans: 57097; Unit: 203, Func: 2: Read Discrete Inputs
525	9.503566	192.168.0.5	192.168.0.204	Modbus/TCP	66	Query: Trans: 57097; Unit: 204, Func: 4: Read Input Registers
527	9.504060	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	9.999575	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	10.002009	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: 57089; Unit: 201, Func: 4: Read Input Registers
531	9.995925	192.168.0.50	192.168.0.205	Modbus/TCP	66	Query: Trans: 57097; Unit: 205, Func: 2: Read Discrete Inputs

Детализация пакета 1 (Frame 1):

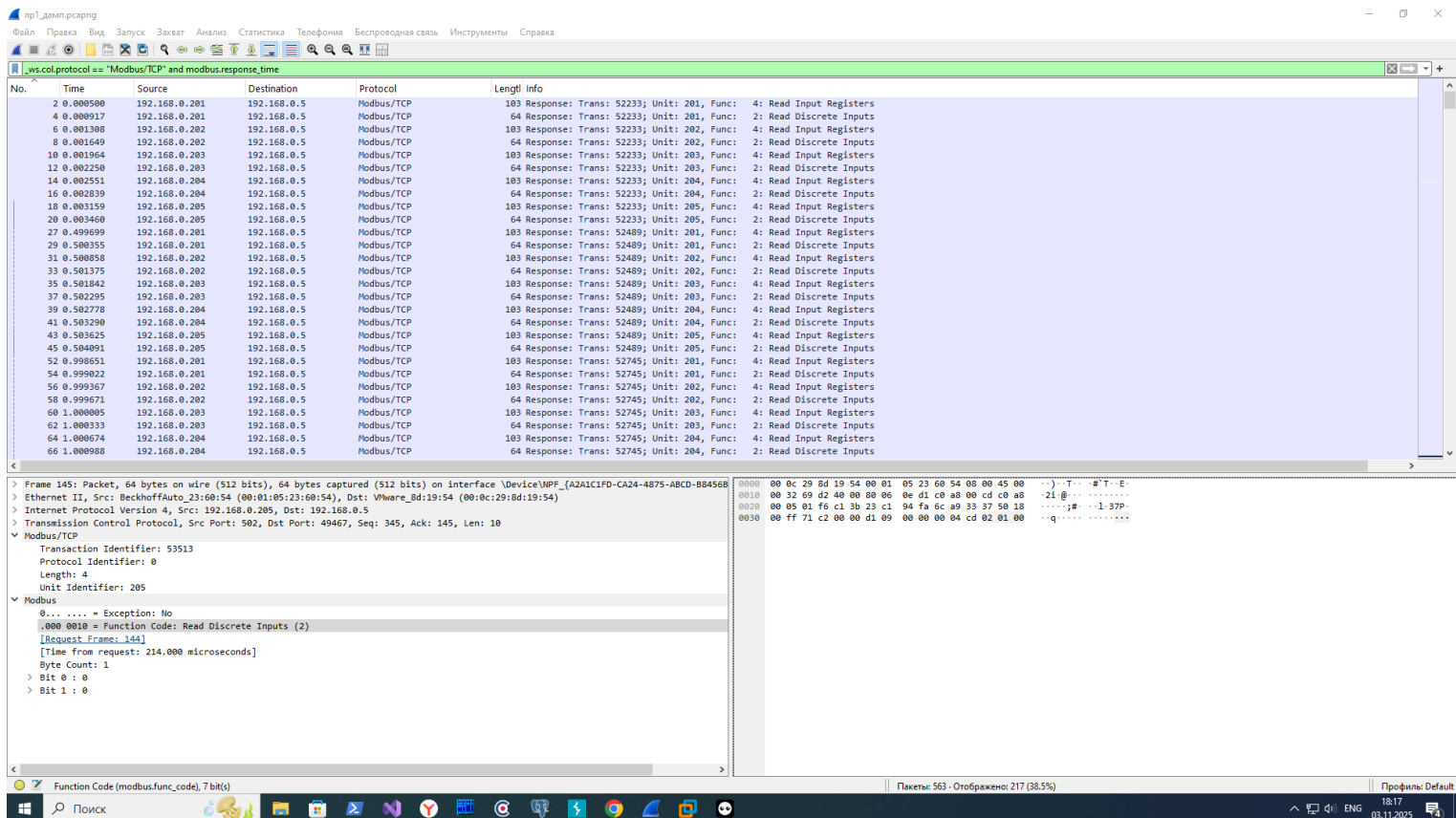
- Ethernet II, Src: VMware_Bd1:19:54 (00:0c:29:8d:19:54), Dst: AbbIndustria_3e:00:22 (00:00:23:3e:00:22)
- Internet Protocol Version 4, Src: 192.168.0.5, Dst: 192.168.0.201
- Transmission Control Protocol, Src Port: 49463, Dst Port: 502, Seq: 1, Ack: 1, Len: 12
- Modbus/TCP
 - Transaction Identifier: 52233
 - Protocol Identifier: 0
 - Length: 6
 - Unit Identifier: 201
 - Modbus
 - 0... = Exception: No
 - 0000 0100 = Function Code: Read Input Registers (4)
 - Reference Number: 0
 - Word Count: 20

Пакеты: 563 - Отображено: 218 (38.7%)

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):



The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like File, Edit, View, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The filter applied is `_ws.col.protocol == "Modbus/TCP" and modbus.response_time`. The list contains 66 packets, all of which are Modbus/TCP responses from various source IP addresses (192.168.0.201 to 192.168.0.204) to the destination 192.168.0.5.
- Packet Details:** Shows the hierarchical structure of the selected packet (Frame 145). It includes fields such as Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Modbus/TCP. The Modbus/TCP section is expanded, showing the Transaction Identifier (53513), Protocol Identifier (0), Unit Identifier (205), and the Modbus function code (Read Discrete Inputs (2)).
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII format.

The bottom status bar indicates that 563 packets are displayed, representing 217 (38.5%) of the total captured data.

Отсортируем отфильтрованные пакеты по столбцу Source:

npf_dmmr.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	Length	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	0.990651	192.168.0.201	192.168.0.5	Modbus/TCP	103	Response: Trans: 52745; Unit: 201, Func: 4: Read Input Registers
54	0.990922	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	3.494787	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
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: Beckhoff_Auto_23:68:54 (00:01:05:23:68:54), 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 0.000 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 18:18 03.11.2025

npf_dmmr.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	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	9.500800	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	1.499088	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: Beckhoff_Auto_23:68:54 (00:01:05:23:68:54), 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 0.000 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

нр1_дмпр.скарг

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
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
528	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
118	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-B84568} Ethernet II, Src: BeckhoffAuto_23:68:54 (00:01:05:23:68:54), 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, Len: 10

Modbus/TCP

Transaction Identifier: 53513

Protocol Identifier: 0

Length: 4

Unit Identifier: 205

Modbus

0... = Exception: No

0000 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

нр1_дмпр.скарг

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
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	10.002158	192.168.0.203	192.168.0.5	Modbus/TCP	103	Response: Trans: 57353; Unit: 203, Func: 4: Read Input Registers
549	10.002557	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-B84568} Ethernet II, Src: BeckhoffAuto_23:68:54 (00:01:05:23:68:54), 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

0000 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

Скриншот программы Wireshark, отображающей сетевой трафик. В верхней панели меню и панели инструментов. Основная панель отображает список пакетов, отсортированных по времени. В таблице ниже представлены данные из списка пакетов.

No.	Time	Source	Destination	Protocol	Length	Info
411	7.508213	192.168.0.204	192.168.0.5	Modbus/TCP	103	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
449	8.005124	192.168.0.204	192.168.0.5	Modbus/TCP	103	Response: Trans: 56329; Unit: 204, Func: 4: Read Input Registers
451	8.005403	192.168.0.204	192.168.0.5	Modbus/TCP	64	Response: Trans: 56329; Unit: 204, Func: 2: Read Discrete Inputs
476	8.505117	192.168.0.204	192.168.0.5	Modbus/TCP	103	Response: Trans: 56585; Unit: 204, Func: 4: Read Input Registers
478	8.505584	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	103	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	9.503796	192.168.0.204	192.168.0.5	Modbus/TCP	103	Response: Trans: 57097; Unit: 204, Func: 4: Read Input Registers
528	9.504325	192.168.0.204	192.168.0.5	Modbus/TCP	64	Response: Trans: 57097; Unit: 204, Func: 2: Read Discrete Inputs
551	10.001901	192.168.0.204	192.168.0.5	Modbus/TCP	103	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	103	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	103	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
60	1.001331	192.168.0.205	192.168.0.5	Modbus/TCP	103	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	1.501806	192.168.0.205	192.168.0.5	Modbus/TCP	103	Response: Trans: 53001; Unit: 205, Func: 4: Read Input Registers
95	1.502265	192.168.0.205	192.168.0.5	Modbus/TCP	64	Response: Trans: 53001; Unit: 205, Func: 2: Read Discrete Inputs
118	1.999398	192.168.0.205	192.168.0.5	Modbus/TCP	103	Response: Trans: 53257; Unit: 205, Func: 4: Read Input Registers
120	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	103	Response: Trans: 53513; Unit: 205, Func: 4: Read Input Registers
145	2.500387	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	103	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	3.498187	192.168.0.205	192.168.0.5	Modbus/TCP	103	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

В нижней панели отображены детали выбранного пакета (Frame 145). Вкладка "Ethernet II" показывает информацию о сетевом интерфейсе. Вкладка "Internet Protocol Version 4" показывает информацию о протоколе. Вкладка "Transmission Control Protocol" показывает информацию о портах и последовательности. Вкладка "Modbus/TCP" показывает детали транзакции, включая идентификатор транзакции (53513), длину (4) и единицу (205). Вкладка "Modbus" показывает детали функции (Read Discrete Inputs) и время отклика (214.000 микросекунд).

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:

np1_дмп.рсапг

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

Filter: _ws.col.protocol=="Modbus/TCP" and modbus.func_code==6

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-B8456B} (00:00:23:3e:00:22) on interface 0
> Ethernet II, Src: DLinkInterna_8e: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

0000 00 00 23 3e 00 22 18 0f 76 8e f8 7d 08 00 45 00 ..>...v...:E
0010 00 34 61 f2 40 00 00 06 16 3e c0 a8 00 7a c0 a8 4a @...>...z...
0020 00 c9 c2 09 01 f6 ae 55 2f 60 20 4c 5f 9e 50 18U /' L P
0030 08 04 50 ff 00 00 e9 4d 00 00 06 c9 00 00 02 ..P...M
0040 00 2d ..

Function Code (modbus.func_code), 7 bit(s)

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:

np1_дмп.рсапг

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

Filter: _ws.col.protocol=="Modbus/TCP" and modbus.func_code==6

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-B8456B} (00:00:23:3e:00:22) on interface 0
> Ethernet II, Src: DLinkInterna_8e: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

0000 00 00 23 3e 00 22 18 0f 76 8e f8 7d 08 00 45 00 ..>...v...:E
0010 00 34 61 f2 40 00 00 06 16 3e c0 a8 00 7a c0 a8 4a @...>...z...
0020 00 c9 c2 09 01 f6 ae 55 2f 60 20 4c 5f 9e 50 18U /' L P
0030 08 04 50 ff 00 00 e9 4d 00 00 06 c9 00 00 02 ..P...M
0040 00 2d ..

Function Code (modbus.func_code), 7 bit(s)

Пакеты: 563 · Отображено: 2 (0.4%)

Профиль: Default

19:02 03.11.2025

Wireshark capture of Modbus/TCP traffic. The packet list shows a query (428) and a response (429) for writing to register 2. The packet details pane shows the Modbus function code 6 (Write Single Register) and the register value 45. The packet bytes pane shows the raw data.

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

Packet 428 details:

- Frame 428: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A2A1C1FD-CA24-4875-ABCD-BB4568}
- Ethernet II, Src: AbiIndustria_3e:00:22 (00:00:12:3e:00:22), Dst: DLinkInterna_8e: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: 67, Ack: 85, Len: 12
- Modbus/TCP
 - 0... .. Exception: No
 - 0000 0110 = Function Code: Write Single Register (6)
 - [Request Frame: 428]
 - [Time from request: 472.000 microseconds]
 - Reference Number: 2
 - Register 2 (UINT16): 45
 - [Register Number: 2]
 - Register Value (UINT16): 45

Packet 429 details:

- 0000 18 0f 76 8e f8 7d 00 00 23 3e 00 22 08 00 45 00 ...v...E
- 0010 00 34 70 d4 40 00 06 07 5c c0 a8 00 c9 c0 a8 ...4p... \.....
- 0020 00 7a 01 f6 c2 09 20 4c 5f 9e ae 55 2f 6c 50 18 ...z... L...U/IP..
- 0030 01 00 57 f7 00 00 e9 4d 00 00 06 c9 00 02 ...M...M... ..
- 0040 00 2d

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:

np1_амп.рсарпг

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

Filter: [ws.col.protocol == "Modbus/TCP" and (ip.src == 192.168.0.5) and (ip.src == 192.168.0.122) and (ip.src == 192.168.0.201) and (ip.src == 192.168.0.202) and (ip.src == 192.168.0.203) and (ip.src == 192.168.0.204) and (ip.src == 192.168.0.205)]

No.	Time	Source	Destination	Protocol	Length	Info
531	9.585825	192.168.0.50	192.168.0.205	Modbus/TCP	66	Query: Trans: 57097; Unit: 205, Func: 2: Read Discrete Inputs

Frame 531: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A2A1C1F0-CA24-4875-ABCD-BB4568} (00:11:24:b3:fa:78) on interface 0

Ethernet II, Src: Apple_b3:fa:78 (00:11:24:b3:fa:78), Dst: BeckhoffAuto_23:68:54 (00:01:05:23:68:54)

Internet Protocol Version 4, Src: 192.168.0.50, Dst: 192.168.0.205

Transmission Control Protocol, Src Port: 49467, Dst Port: 502, Seq: 1, Ack: 1, Len: 12

Modbus/TCP

Modbus

0... = Exception: No

0000 0010 = Function Code: Read Discrete Inputs (2)

Reference Number: 0

Bit Count: 2

0000 00 01 05 23 68 54 00 11 24 b3 fa 78 08 00 45 00 ... #T... \$...x...E...
0010 00 34 50 37 40 00 00 06 20 6a c0 a0 00 32 c0 a0 ... 4P78... (j...2...
0020 00 cd c1 3b 01 fe 6c a9 34 7b 23 c1 50 34 50 18 ... j...1...4(#...4p...
0030 01 00 60 3d 00 00 df 09 00 00 00 06 cd 02 00 00
0040 00 02 ..

Function Code (modbus.func_code), 7 bit(s)

Пакеты: 563 - Отображено: 1 (0.2%)

Профиль: Default

1938 03.11.2025

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.