Journal scientific and applied research, vol. 22, 2022
International Journal

Original Contribution

ISSN 1314-6289

ANALYSIS AND MONITORING THE NETWORK TRAFFIC IN THE PROCESS OF CONNECTING TO INDUSTRIAL SIEMENS CONTROLLERS

Petar Kr. Boyanov

DEPARTMENT OF MANAGEMENT OF SECURITY SYSTEMS, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712,115, UNIVERSITETSKA STR,

E-MAIL: petar.boyanov@shu.bg

ABSTRACT: *In this paper analysis and monitoring of network traffic in the process of connecting to industrial Siemens controllers in the Faculty of Technical Sciences is made.*

KEY WORDS: *Analysis, Connection, Industrial controller, LAN, Monitoring, Network, Process, Siemens, Traffic.*

1. Introduction

The analysis and monitoring of the network traffic in the programming process of industrial controllers is an important and responsible task for every system administrator who maintains the production automation systems in the respective enterprise. The daily network scanning for suspicious networks connections and states, as well as the detection of anomalies in communication between devices will allow administrators to take the necessary measures to protect the proper working course of the technological process with the controllers. As it became known in the scientific community, one of the biggest weaknesses of Siemens controllers is the Stuxnet virus and in this regard, most Siemens controllers are used in critical infrastructure and infection with such a virus can cause great and irreparable technical and financial damages [11,12,15,16].

In this scientific research, the main emphasis on the presentation of the three-way network handshake is placed, when the initial network connection is made between programmer's workstation and the respective industrial controller in the local network of the enterprise [1,2,3,14]. The worldwide used and secure industrial controllers are Siemens and in this connection a real Siemens Simatic

S7-1200 controller with fully licensed Totally Integrated Automation Portal V13 SP1 Update 4 software is used [1,3,4,7,9,13].

2. Experiment

The experiment in the specialized computer network laboratory “Programming of Siemens controllers” in the Faculty of technical sciences is made. The free of charge network protocol analyzer “Wireshark” version Win64-3.6.5 is used. The operating system of the workstation for programing is Windows 8.1 x64, build 9600.

The laboratory is mainly designed for conducting courses with students in the professional field of Communication and Computer Engineering with an emphasis on design automation technologies and production automation technologies. It is equipped with 12 computer systems consisting of a server and "thin clients". Six models of Siemens Simatic S7-1200 industrial programmable controllers are located in the laboratory, and the Siemens software package necessary for working with the controllers is installed in the computer system. With the support of Siemens models and software, students studying in Computer Technology for Production Automation gain knowledge and skills for programming industrial controllers, which are actually used in modern production. There is a local computer network in the laboratory, connected to the rest of the network of the building, and from there to the entire network of the Shumen University. A projector is permanently installed in the lab. There is also a wireless internet access point.

The software program Wireshark consists of the following control future set components [2,4,5,6,8,10]:

- Deep inspection for various network protocols.
- Possibility for live capturing and offline analysis of the scanned network traffic.
- Live data reading from Ethernet, IEEE 802.11.
- The collected results can be exported to file with extensions as XML, PS, CSV or plain text.
- Possibility for reading and writing of various capture file formats as pcap, pcapng and etc.

3. Results

Once the program code has been compiled, then it is downloaded to the controller. After that is the setup of a dialog box that displays the following network information:

- Type of the PG/PC interface.
- PG/PC interface.
- Connection to interface/subnet
- Compatible devices in target subnet.

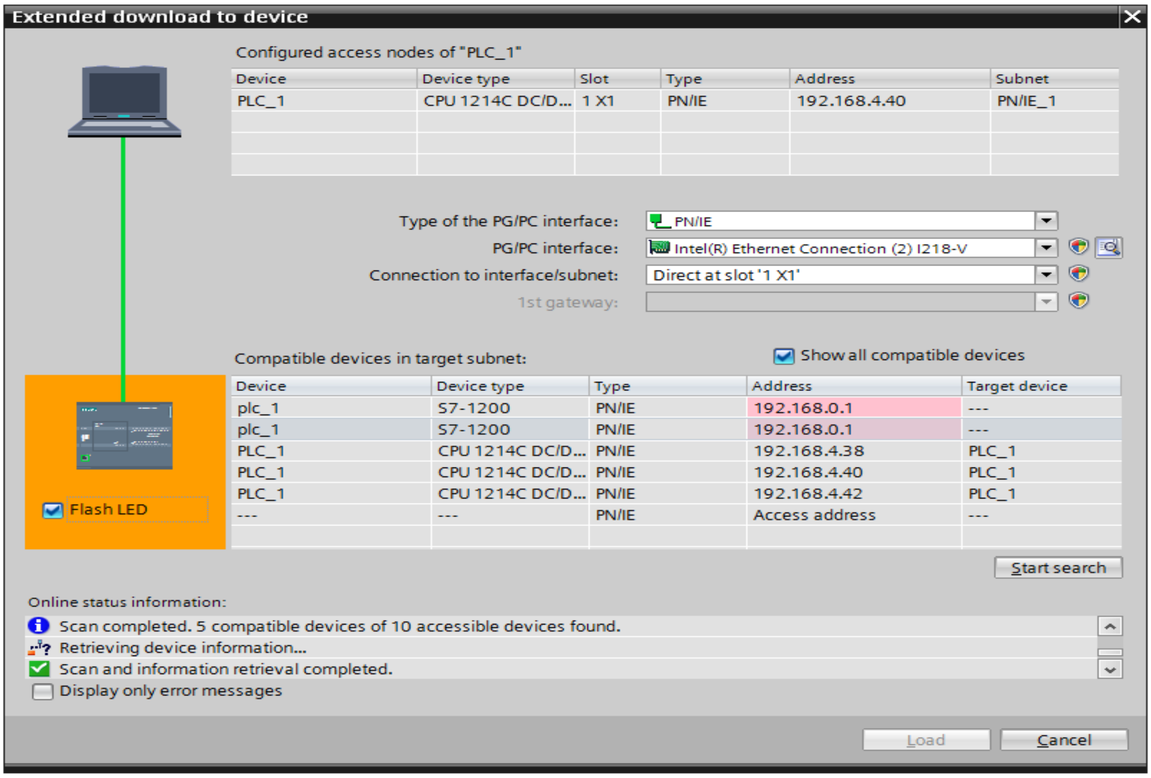
- Online status information.

It turned out that 5 compatible devices of 10 accessible devices were found. Every found device (controller) has got the following information:

- Device.
- Device type.
- Type.
- Address (IPv4).
- Target device.

Fig. 1 shows that 5 devices with the following IP addresses 192.168.0.1, 192.168.4.38, 192.168.4.40 and 192.168.4.42 were found. It can be seen that the first two devices the same IP shared and this is a prerequisite for a collision. In order to avoid it, it is necessary to change the IP address one of them.

It should be noted that even if the controllers have got the same IP addresses, then they can be checked for a physical connection by pressing the button "Flash LED".



Extended download to device

Configured access nodes of "PLC_1"

Device	Device type	Slot	Type	Address	Subnet
PLC_1	CPU 1214C DC/D...	1 X1	PN/IE	192.168.4.40	PN/IE_1

Type of the PG/PC interface: PN/IE

PG/PC interface: Intel(R) Ethernet Connection (2) I218-V

Connection to interface/subnet: Direct at slot '1 X1'

1st gateway:

Compatible devices in target subnet:

☑ Show all compatible devices

Device	Device type	Type	Address	Target device
plc_1	S7-1200	PN/IE	192.168.0.1	---
plc_1	S7-1200	PN/IE	192.168.0.1	---
PLC_1	CPU 1214C DC/D...	PN/IE	192.168.4.38	PLC_1
PLC_1	CPU 1214C DC/D...	PN/IE	192.168.4.40	PLC_1
PLC_1	CPU 1214C DC/D...	PN/IE	192.168.4.42	PLC_1
---	---	PN/IE	Access address	---

☑ Flash LED

Online status information:

Scan completed. 5 compatible devices of 10 accessible devices found.

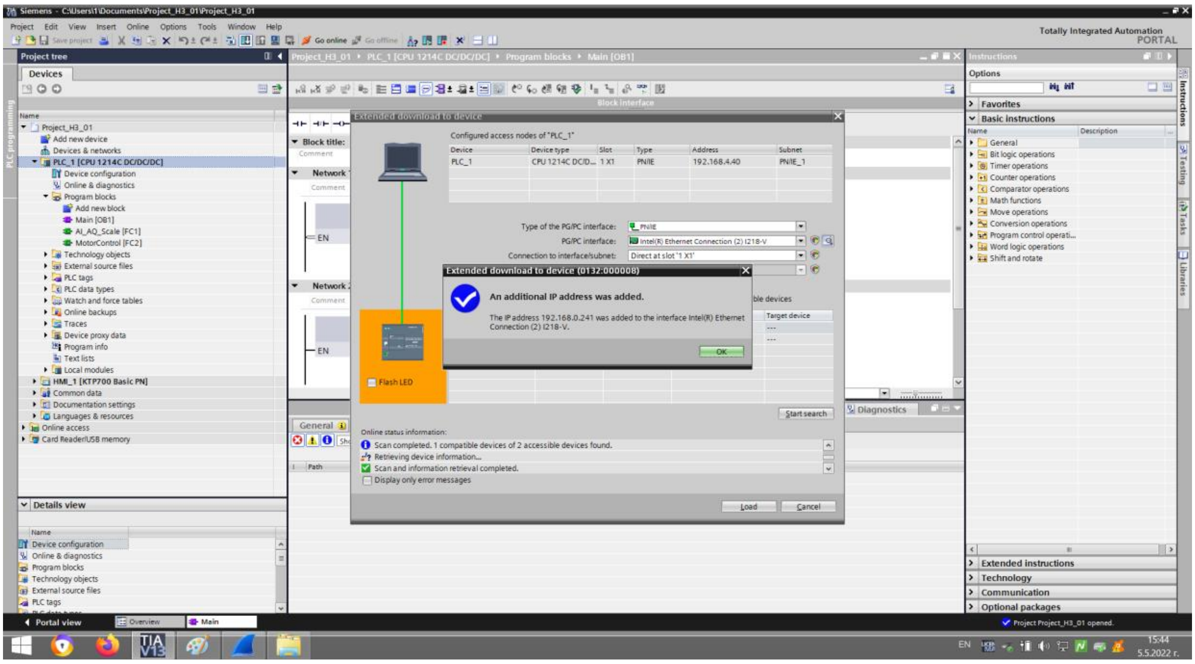
Retrieving device information...

Scan and information retrieval completed.

□ Display only error messages

Fig. 1. Extended download to device

Fig. 2 shows that the collision problem is successfully solved.



Extended download to device

Configured access nodes of "PLC_1"

Device	Device type	Slot	Type	Address	Subnet
PLC_1	CPU 1214C DC/D...	1 X1	PN/IE	192.168.4.40	PN/IE_1

Type of the PG/PC interface: PN/IE
PG/PC interface: Intel(R) Ethernet Connection (2) I218-V
Connection to interface/subnet: Direct at slot '1 X1'

Extended download to device (0132:000008)

An additional IP address was added.

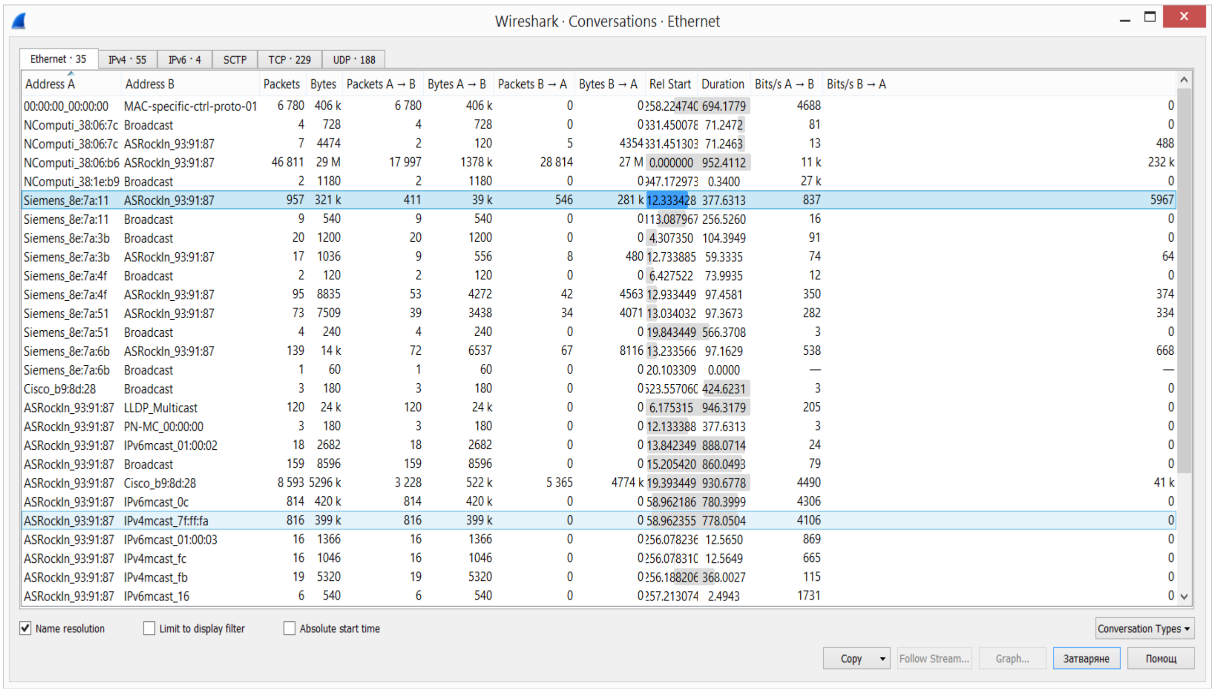
The IP address 192.168.0.241 was added to the interface Intel(R) Ethernet Connection (2) I218-V.

Online status information:
Scan completed. 1 compatible devices of 2 accessible devices found.
Retrieving device information...
Scan and information retrieval completed.
□ Display only error messages

Siemens - C:\Users\1\Documents\Project_H3_01\Project_H3_01
Totally Integrated Automation PORTAL
Project tree
Devices
Project_H3_01 ▸ PLC_1 [CPU 1214C DC/DC/DC] ▸ Program blocks ▸ Main [OB1]
Instructions
Flash LED
OK
Start search
Load
Cancel
Portal view
Overview
Main
Project Project_H3_01 opened.

Fig. 2. Solved collision problem

The scanning with the program is started by downloading the source code to the controller and fig. 3 shows the found Siemens controllers.



Wireshark · Conversations · Ethernet

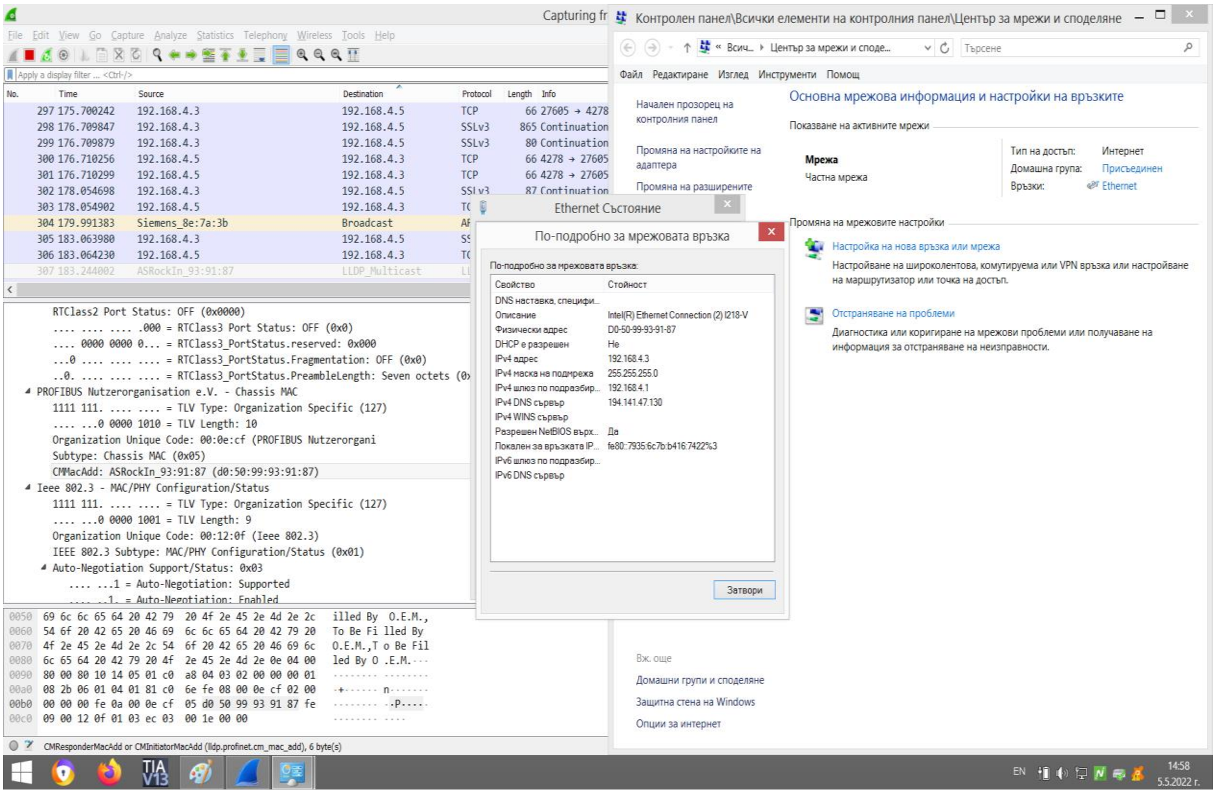
Ethernet · 35 | IPv4 · 55 | IPv6 · 4 | SCTP | TCP · 229 | UDP · 188

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00:00:00_00:00:00	MAC-specific-ctrl-proto-01	6 780	406 k	6 780	406 k	0	0	258.224740	694.1779	4688	0
NComputi_38:06:7c	Broadcast	4	728	4	728	0	0	331.450078	71.2472	81	0
NComputi_38:06:7c	ASRockIn_93:91:87	7	4474	2	120	5	4354	331.451303	71.2463	13	488
NComputi_38:06:b6	ASRockIn_93:91:87	46 811	29 M	17 997	1378 k	28 814	27 M	0.000000	952.4112	11 k	232 k
NComputi_38:1e:b9	Broadcast	2	1180	2	1180	0	0	947.172973	0.3400	27 k	0
Siemens_8e:7a:11	ASRockIn_93:91:87	957	321 k	411	39 k	546	281 k	12.333428	377.6313	837	5967
Siemens_8e:7a:11	Broadcast	9	540	9	540	0	0	113.087967	256.5260	16	0
Siemens_8e:7a:3b	Broadcast	20	1200	20	1200	0	0	4.307350	104.3949	91	0
Siemens_8e:7a:3b	ASRockIn_93:91:87	17	1036	9	556	8	480	12.733885	59.3335	74	64
Siemens_8e:7a:4f	Broadcast	2	120	2	120	0	0	6.427522	73.9935	12	0
Siemens_8e:7a:4f	ASRockIn_93:91:87	95	8835	53	4272	42	4563	12.933449	97.4581	350	374
Siemens_8e:7a:51	ASRockIn_93:91:87	73	7509	39	3438	34	4071	13.034032	97.3673	282	334
Siemens_8e:7a:51	Broadcast	4	240	4	240	0	0	19.843449	566.3708	3	0
Siemens_8e:7a:6b	ASRockIn_93:91:87	139	14 k	72	6537	67	8116	13.233566	97.1629	538	668
Siemens_8e:7a:6b	Broadcast	1	60	1	60	0	0	20.103309	0.0000	—	—
Cisco_b9:8d:28	Broadcast	3	180	3	180	0	0	523.557060	424.6231	3	0
ASRockIn_93:91:87	LLDP_Multicast	120	24 k	120	24 k	0	0	6.175315	946.3179	205	0
ASRockIn_93:91:87	PN-MC_00:00:00	3	180	3	180	0	0	12.133388	377.6313	3	0
ASRockIn_93:91:87	IPv6mcast_01:00:02	18	2682	18	2682	0	0	13.842349	888.0714	24	0
ASRockIn_93:91:87	Broadcast	159	8596	159	8596	0	0	15.205420	860.0493	79	0
ASRockIn_93:91:87	Cisco_b9:8d:28	8 593	5296 k	3 228	522 k	5 365	4774 k	19.393449	930.6778	4490	41 k
ASRockIn_93:91:87	IPv6mcast_0c	814	420 k	814	420 k	0	0	58.962186	780.3999	4306	0
ASRockIn_93:91:87	IPv4mcast_7f:ff:fa	816	399 k	816	399 k	0	0	58.962355	778.0504	4106	0
ASRockIn_93:91:87	IPv6mcast_01:00:03	16	1366	16	1366	0	0	256.078236	12.5650	869	0
ASRockIn_93:91:87	IPv4mcast_fc	16	1046	16	1046	0	0	256.078310	12.5649	665	0
ASRockIn_93:91:87	IPv4mcast_fb	19	5320	19	5320	0	0	256.188206	368.0027	115	0
ASRockIn_93:91:87	IPv6mcast_16	6	540	6	540	0	0	257.213074	2.4943	1731	0

☑ Name resolution □ Limit to display filter □ Absolute start time

Fig. 3. Found four Siemens controllers

Fig. 4 shows the IP address of the programing's workstation.



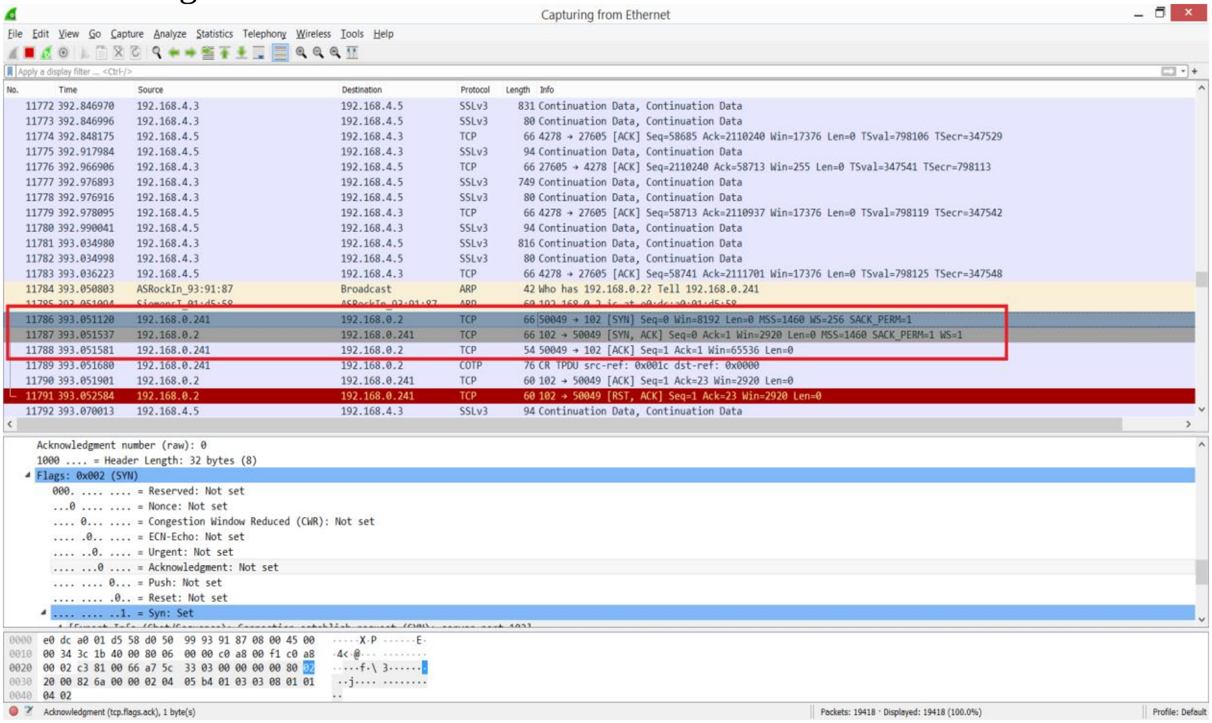
```
Capturing fr
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
Apply a display filter ... <Ctrl-/>
No.   Time        Source              Destination      Protocol  Length Info
  297 175.700242  192.168.4.3         192.168.4.5      TCP        66 27605 → 4278
  298 176.709847  192.168.4.3         192.168.4.5      SSLv3     865 Continuation
  299 176.709879  192.168.4.3         192.168.4.5      SSLv3      80 Continuation
  300 176.710256  192.168.4.5         192.168.4.3      TCP        66 4278 → 27605
  301 176.710299  192.168.4.5         192.168.4.3      TCP        66 4278 → 27605
  302 178.054698  192.168.4.3         192.168.4.5      SSLv3      87 Continuation
  303 178.054902  192.168.4.5         192.168.4.3      TC
  304 179.991383  Siemens_8e:7a:3b    Broadcast        AF
  305 183.063980  192.168.4.3         192.168.4.5      SS
  306 183.064230  192.168.4.5         192.168.4.3      TC
  307 183.244002  ASRockIn_93:91:87   LLDP_Multicast   LL

    RTClass2 Port Status: OFF (0x0000)
    .... .... .... .000 = RTClass3 Port Status: OFF (0x0)
    .... 0000 0000 0... = RTClass3_PortStatus.reserved: 0x000
    ...0 .... .... .... = RTClass3_PortStatus.Fragmentation: OFF (0x0)
    ..0. .... .... .... = RTClass3_PortStatus.PreambleLength: Seven octets (0x
  ◢ PROFIBUS Nutzerorganisation e.V. - Chassis MAC
    1111 111. .... .... = TLV Type: Organization Specific (127)
    .... ...0 0000 1010 = TLV Length: 10
    Organization Unique Code: 00:0e:cf (PROFIBUS Nutzerorgani
    Subtype: Chassis MAC (0x05)
    CMMacAdd: ASRockIn_93:91:87 (d0:50:99:93:91:87)
  ◢ Ieee 802.3 - MAC/PHY Configuration/Status
    1111 111. .... .... = TLV Type: Organization Specific (127)
    .... ...0 0000 1001 = TLV Length: 9
    Organization Unique Code: 00:12:0f (Ieee 802.3)
    IEEE 802.3 Subtype: MAC/PHY Configuration/Status (0x01)
  ◢ Auto-Negotiation Support/Status: 0x03
      .... ...1 = Auto-Negotiation: Supported
      .... ..1. = Auto-Negotiation: Enabled

0050  69 6c 6c 65 64 20 42 79  20 4f 2e 45 2e 4d 2e 2c   illed By  O.E.M.,
0060  54 6f 20 42 65 20 46 69  6c 6c 65 64 20 42 79 20   To Be Fi lled By
0070  4f 2e 45 2e 4d 2e 2c 54  6f 20 42 65 20 46 69 6c   O.E.M.,T o Be Fil
0080  6c 65 64 20 42 79 20 4f  2e 45 2e 4d 2e 0e 04 00   led By O .E.M.···
0090  80 00 80 10 14 05 01 c0  a8 04 03 02 00 00 00 01   ········ ········
00a0  08 2b 06 01 04 01 81 c0  6e fe 08 00 0e cf 02 00   ·+······ n·······
00b0  00 00 00 fe 0a 00 0e cf  05 d0 50 99 93 91 87 fe   ········ ·P·····
00c0  09 00 12 0f 01 03 ec 03  00 1e 00 00               ········ ····

CMResponderMacAdd or CMInitiatorMacAdd (lldp.profinet.cm_mac_add), 6 byte(s)
```

```
Контролен панел\Всички елементи на контролния панел\Център за мрежи и споделяне
« Всич… › Център за мрежи и споде…          Търсене
Файл  Редактиране  Изглед  Инструменти  Помощ

Начален прозорец на контролния панел
Промяна на настройките на адаптера
Промяна на разширените

Основна мрежова информация и настройки на връзките
Показване на активните мрежи
  Мрежа                Тип на достъп:    Интернет
  Частна мрежа         Домашна група:    Присъединен
                       Връзки:           Ethernet
Промяна на мрежовите настройки
  Настройка на нова връзка или мрежа
  Настройване на широколентова, комутируема или VPN връзка или настройване
  на маршрутизатор или точка на достъп.
  Отстраняване на проблеми
  Диагностика или коригиране на мрежови проблеми или получаване на
  информация за отстраняване на неизправности.

Вж. още
Домашни групи и споделяне
Защитна стена на Windows
Опции за интернет
```

```
Ethernet Състояние
По-подробно за мрежовата връзка
По-подробно за мрежовата връзка:
Свойство                      Стойност
DNS наставка, специфи…
Описание                      Intel(R) Ethernet Connection (2) I218-V
Физически адрес               D0-50-99-93-91-87
DHCP е разрешен               Не
IPv4 адрес                    192.168.4.3
IPv4 маска на подмрежа        255.255.255.0
IPv4 шлюз по подразбир…       192.168.4.1
IPv4 DNS сървър               194.141.47.130
IPv4 WINS сървър
Разрешен NetBIOS върх…        Да
Локален за връзката IP…       fe80::7935:6c7b:b416:7422%3
IPv6 шлюз по подразбир…
IPv6 DNS сървър
                                                      Затвори
```

Fig. 4. The IP address of the workstation (192.168.4.3)

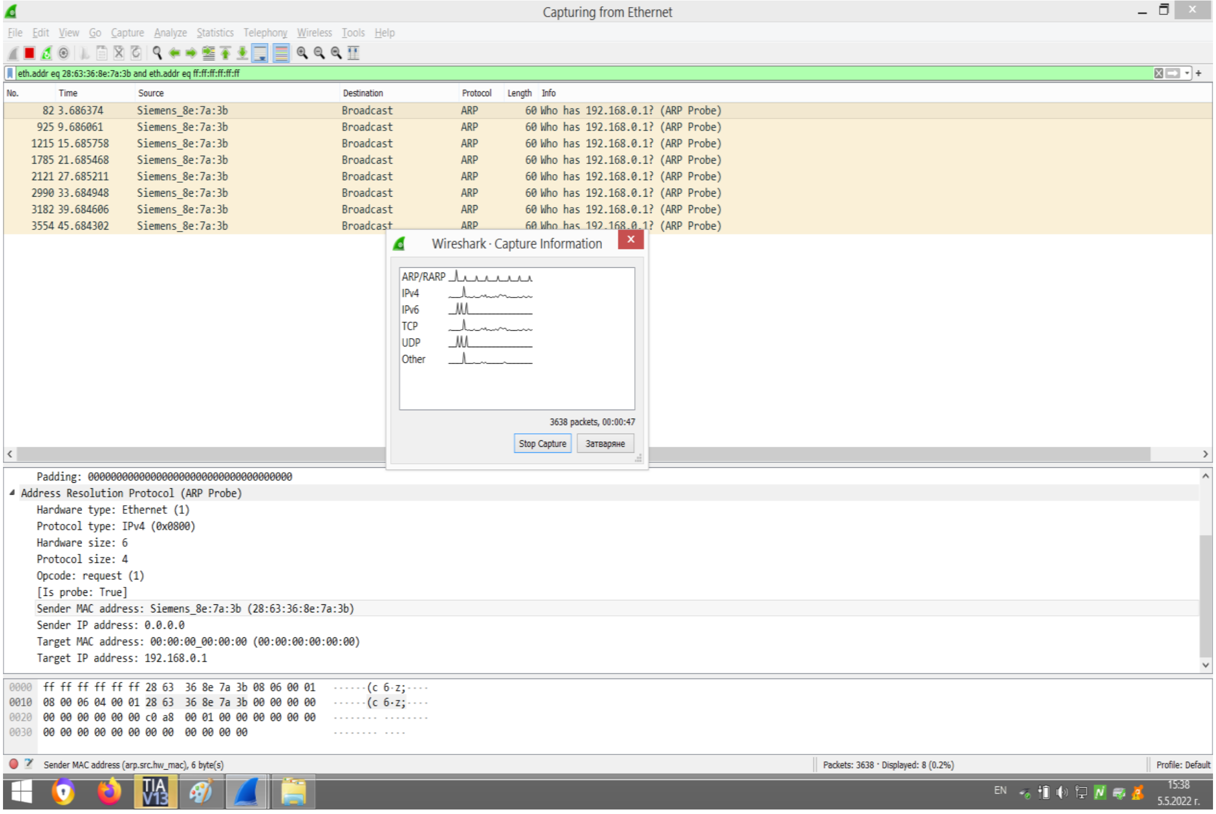
Lines 11786, 11787 and 11788 show that the three-way handshake between the hosts 192.168.0.241 and 192.168.0.2 is successfully established. This is shown on fig. 5.



```
Capturing from Ethernet
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
Apply a display filter ... <Ctrl-/>
No.     Time        Source              Destination        Protocol  Length Info
  11772 392.846970  192.168.4.3         192.168.4.5        SSLv3     831 Continuation Data, Continuation Data
  11773 392.846996  192.168.4.3         192.168.4.5        SSLv3      80 Continuation Data, Continuation Data
  11774 392.848175  192.168.4.5         192.168.4.3        TCP        66 4278 → 27605 [ACK] Seq=58685 Ack=2110240 Win=17376 Len=0 TSval=798106 TSecr=347529
  11775 392.917984  192.168.4.5         192.168.4.3        SSLv3      94 Continuation Data, Continuation Data
  11776 392.966906  192.168.4.3         192.168.4.5        TCP        66 27605 → 4278 [ACK] Seq=2110240 Ack=58713 Win=255 Len=0 TSval=347541 TSecr=798113
  11777 392.976893  192.168.4.3         192.168.4.5        SSLv3     749 Continuation Data, Continuation Data
  11778 392.976916  192.168.4.3         192.168.4.5        SSLv3      80 Continuation Data, Continuation Data
  11779 392.978095  192.168.4.5         192.168.4.3        TCP        66 4278 → 27605 [ACK] Seq=58713 Ack=2110937 Win=17376 Len=0 TSval=798119 TSecr=347542
  11780 392.990041  192.168.4.5         192.168.4.3        SSLv3      94 Continuation Data, Continuation Data
  11781 393.034980  192.168.4.3         192.168.4.5        SSLv3     816 Continuation Data, Continuation Data
  11782 393.034998  192.168.4.3         192.168.4.5        SSLv3      80 Continuation Data, Continuation Data
  11783 393.036223  192.168.4.5         192.168.4.3        TCP        66 4278 → 27605 [ACK] Seq=58741 Ack=2111701 Win=17376 Len=0 TSval=798125 TSecr=347548
  11784 393.050803  ASRockIn_93:91:87   Broadcast          ARP        42 Who has 192.168.0.2? Tell 192.168.0.241
  11785 393.051904  SiemensT_01:d5:58   ASRockIn_93:91:87  ARP        60 192.168.0.2 is at e0:dc:a0:01:d5:58
  11786 393.051120  192.168.0.241       192.168.0.2        TCP        66 50049 → 102 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  11787 393.051537  192.168.0.2         192.168.0.241      TCP        66 102 → 50049 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0 MSS=1460 SACK_PERM=1 WS=1
  11788 393.051581  192.168.0.241       192.168.0.2        TCP        54 50049 → 102 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  11789 393.051680  192.168.0.241       192.168.0.2        COTP       76 CR TPDU src-ref: 0x001c dst-ref: 0x0000
  11790 393.051901  192.168.0.2         192.168.0.241      TCP        60 102 → 50049 [ACK] Seq=1 Ack=23 Win=2920 Len=0
└ 11791 393.052584  192.168.0.2         192.168.0.241      TCP        60 102 → 50049 [RST, ACK] Seq=1 Ack=23 Win=2920 Len=0
  11792 393.070013  192.168.4.5         192.168.4.3        SSLv3      94 Continuation Data, Continuation Data

    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  ◢ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ◢ .... .... ..1. = Syn: Set
      ◢ [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 102]

0000  e0 dc a0 01 d5 58 d0 50  99 93 91 87 08 00 45 00   ·····X·P ······E·
0010  00 34 3c 1b 40 00 80 06  00 00 c0 a8 00 f1 c0 a8   ·4<·@··· ········
0020  00 02 c3 81 00 66 a7 5c  33 03 00 00 00 00 80 02   ·····f·\ 3·······
0030  20 00 82 6a 00 00 02 04  05 b4 01 03 03 08 01 01    ··j···· ········
0040  04 02                                              ··

Acknowledgment (tcp.flags.ack), 1 byte(s)    Packets: 19418 · Displayed: 19418 (100.0%)    Profile: Default
```

Fig. 5. Successfully established three-way handshake

Fig. 6 shows the captured information for the ARP protocol


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Capture Information
ARP/RARP
IPv4
IPv6
TCP
UDP
Other
Stop Capture
Затваряне

eth.addr eq 28:63:36:8e:7a:3b and eth.addr eq ff:ff:ff:ff:ff:ff

```
No.   Time      Source              Destination  Protocol  Length  Info
   82 3.686374  Siemens_8e:7a:3b    Broadcast    ARP          60 Who has 192.168.0.1? (ARP Probe)
  925 9.686061  Siemens_8e:7a:3b    Broadcast    ARP          60 Who has 192.168.0.1? (ARP Probe)
 1215 15.685758 Siemens_8e:7a:3b    Broadcast    ARP          60 Who has 192.168.0.1? (ARP Probe)
 1785 21.685468 Siemens_8e:7a:3b    Broadcast    ARP          60 Who has 192.168.0.1? (ARP Probe)
 2121 27.685211 Siemens_8e:7a:3b    Broadcast    ARP          60 Who has 192.168.0.1? (ARP Probe)
 2990 33.684948 Siemens_8e:7a:3b    Broadcast    ARP          60 Who has 192.168.0.1? (ARP Probe)
 3182 39.684606 Siemens_8e:7a:3b    Broadcast    ARP          60 Who has 192.168.0.1? (ARP Probe)
 3554 45.684302 Siemens_8e:7a:3b    Broadcast    ARP          60 Who has 192.168.0.1? (ARP Probe)
```

3638 packets, 00:00:47

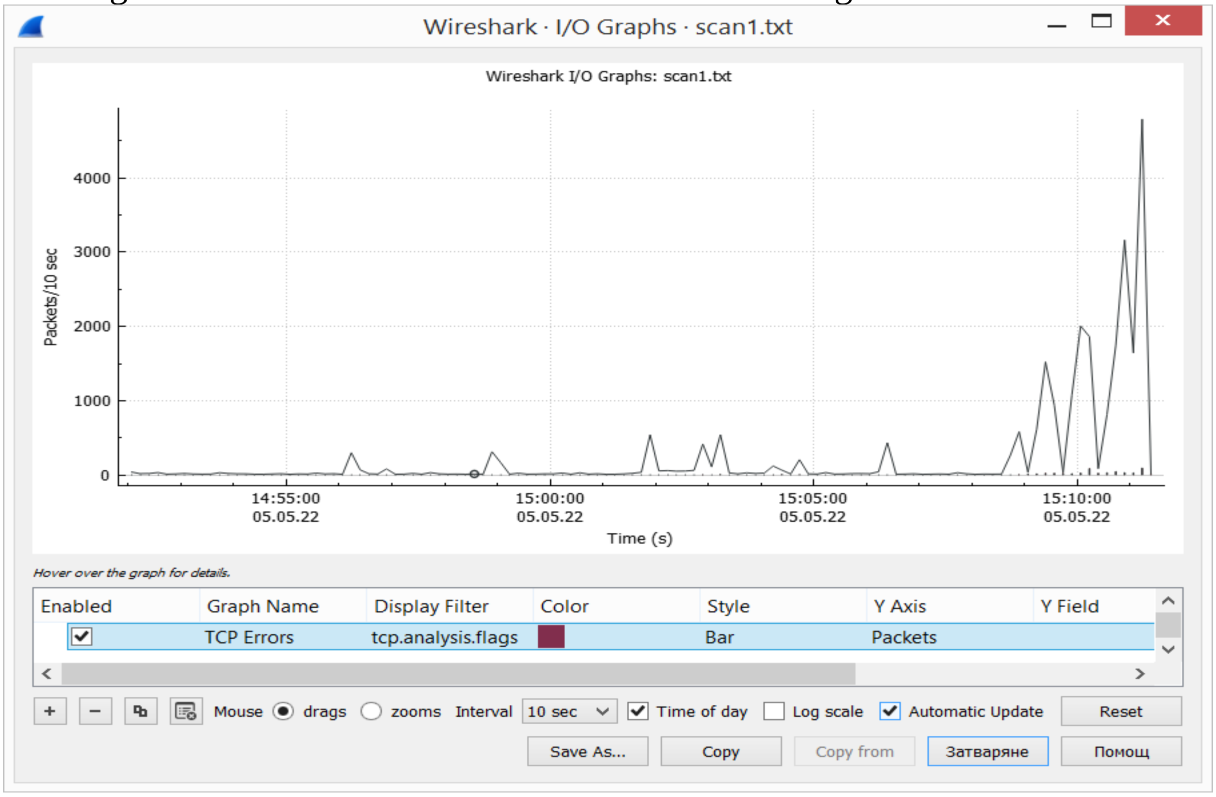
```
    Padding: 000000000000000000000000000000000000
◢ Address Resolution Protocol (ARP Probe)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is probe: True]
    Sender MAC address: Siemens_8e:7a:3b (28:63:36:8e:7a:3b)
    Sender IP address: 0.0.0.0
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.1
```

```
0000  ff ff ff ff ff ff 28 63  36 8e 7a 3b 08 06 00 01   ······(c 6·z;····
0010  08 00 06 04 00 01 28 63  36 8e 7a 3b 00 00 00 00   ······(c 6·z;····
0020  00 00 00 00 00 00 c0 a8  00 01 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Sender MAC address (arp.src.hw_mac), 6 byte(s) | Packets: 3638 · Displayed: 8 (0.2%) | Profile: Default

Fig. 6. ARP protocol information

Fig. 7 shows statistics for the found TCP errors flags.



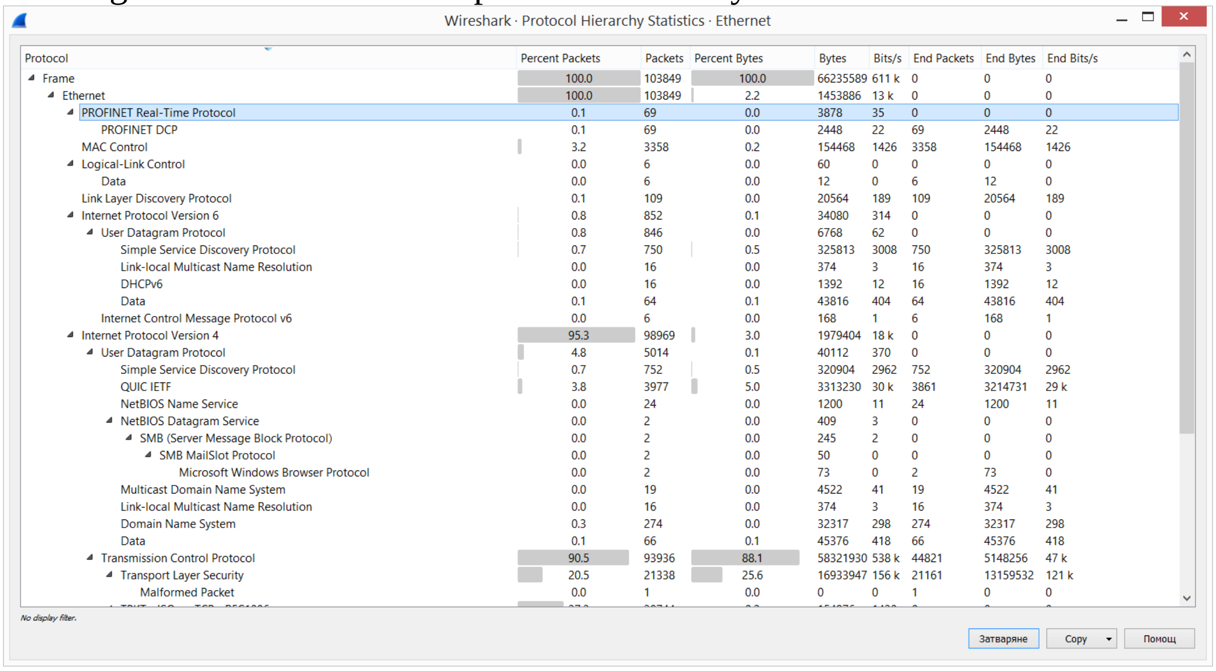
Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field
☑	TCP Errors	tcp.analysis.flags	■	Bar	Packets	

Mouse ● drags ○ zooms Interval 10 sec ☑ Time of day □ Log scale ☑ Automatic Update

Fig. 7. TCP errors flags

Fig. 8 shows the achieved protocol hierarchy statistics.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	103849	100.0	66235589	611 k	0	0	0
Ethernet	100.0	103849	2.2	1453886	13 k	0	0	0
PROFINET Real-Time Protocol	0.1	69	0.0	3878	35	0	0	0
PROFINET DCP	0.1	69	0.0	2448	22	69	2448	22
MAC Control	3.2	3358	0.2	154468	1426	3358	154468	1426
Logical-Link Control	0.0	6	0.0	60	0	0	0	0
Data	0.0	6	0.0	12	0	6	12	0
Link Layer Discovery Protocol	0.1	109	0.0	20564	189	109	20564	189
Internet Protocol Version 6	0.8	852	0.1	34080	314	0	0	0
User Datagram Protocol	0.8	846	0.0	6768	62	0	0	0
Simple Service Discovery Protocol	0.7	750	0.5	325813	3008	750	325813	3008
Link-local Multicast Name Resolution	0.0	16	0.0	374	3	16	374	3
DHCPv6	0.0	16	0.0	1392	12	16	1392	12
Data	0.1	64	0.1	43816	404	64	43816	404
Internet Control Message Protocol v6	0.0	6	0.0	168	1	6	168	1
Internet Protocol Version 4	95.3	98969	3.0	1979404	18 k	0	0	0
User Datagram Protocol	4.8	5014	0.1	40112	370	0	0	0
Simple Service Discovery Protocol	0.7	752	0.5	320904	2962	752	320904	2962
QUIC IETF	3.8	3977	5.0	3313230	30 k	3861	3214731	29 k
NetBIOS Name Service	0.0	24	0.0	1200	11	24	1200	11
NetBIOS Datagram Service	0.0	2	0.0	409	3	0	0	0
SMB (Server Message Block Protocol)	0.0	2	0.0	245	2	0	0	0
SMB MailSlot Protocol	0.0	2	0.0	50	0	0	0	0
Microsoft Windows Browser Protocol	0.0	2	0.0	73	0	2	73	0
Multicast Domain Name System	0.0	19	0.0	4522	41	19	4522	41
Link-local Multicast Name Resolution	0.0	16	0.0	374	3	16	374	3
Domain Name System	0.3	274	0.0	32317	298	274	32317	298
Data	0.1	66	0.1	45376	418	66	45376	418
Transmission Control Protocol	90.5	93936	88.1	58321930	538 k	44821	5148256	47 k
Transport Layer Security	20.5	21338	25.6	16933947	156 k	21161	13159532	121 k
Malformed Packet	0.0	1	0.0	0	0	1	0	0

No display filter.

Fig. 8. The achieved protocol hierarchy statistics

Fig. 9 shows the entire captured network traffic via interface Ethernet.

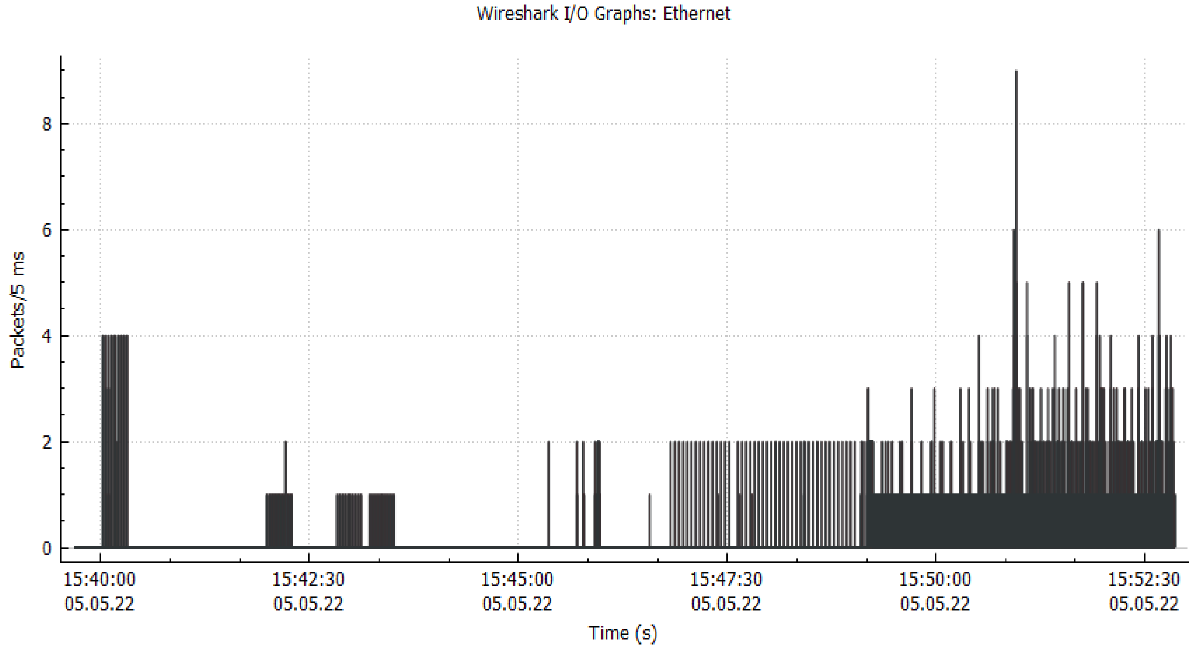


Fig. 9. The entire captured network traffic via interface Ethernet

ATTENTION: The scientific experiments and research works in this paper in a specialized computer laboratories at the Faculty of Technical Sciences of the Konstantin Preslavsky University of Shumen are made. Everything illustrated and explained in this paper is for research work and educational purposes and the authors are not responsible in cases of abuse.

3. Conclusion

All data obtained from this research are stored in files with the extension pcap and pcapng. In this way, all information can be analyzed and checked offline at any time in order to detect suspicious network connections and states. Thus the exceptionally well-equipped laboratories at the Faculty of Technical Sciences at the Konstantin Preslavsky University of Shumen give great opportunities to students majoring in "Communication and Information Systems", "Computer Technologies in Automated Manufacturing" and "Signal Security Systems and Technologies" to gain extensive theoretical and practical experience in the network analysis and monitoring the network traffic in the process of connecting to industrial controllers.

References:

[1] Asrodia P., & Patel H., Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis, International Journal of Electrical, Electronics and Computer Engineering 1(1): 55-58(2012).

[2] BAKRE, Ajay; BADRINATH, B. R. I-TCP: Indirect TCP for mobile hosts. In: Distributed Computing Systems, 1995., Proceedings of the 15th International Conference on. IEEE, 1995. p. 136-143.

[3] Dunaytsev, R. A., Krendzel A. V., Koucheryavy Y. A., & Harju J. J., Estimation of web traffic generated by users in home networks, Proceedings of the eighth IASTED IMSA', Kauai, Hawaii. Retrieved from/http://www.cs.tut.fi/tlt/npg/-icefin/documents/Hawaii-427-141_Final_Manuscript. pdf, 2004.

[4] Kahya-Özyirmidokuz E., Gezer A., & Ciflikli C., Characterization of Network Traffic Data: A Data Preprocessing and Data Mining Application, In DATA ANALYTICS 2012, The First International Conference on Data Analytics, 2012, September, pp. 18-23.

[5] Kumar P. S., & Arumugam S., Establishing a valuable method of packet capture and packet analyzer tools in firewall, International Journal of Research Studies in Computing, 2012 April, Volume 1 Number 1, 11-20.

[6] Paessler, Dirk. Server Virtualization and Network Management. Database and Network Journal, 2008, 38.5: 13.

[7] Park, Daihee, et al. NetCube: a comprehensive network traffic analysis model based on multidimensional OLAP data cube. International Journal of Network Management, 2013, 23.2: 101-118.

[8] SO-IN, Chakchai. A Survey of Network Traffic Monitoring and Analysis Tools. Cse 576m computer system analysis project, Washington University in St. Louis, 2009.

[9] Song, Yuqian, et al. Towards a framework to support novice users in understanding and monitoring of Home Area Networks. In: Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on. IEEE, 2012. p. 82-87.

[10] Singh G., & Singh A., Campus Network Security Policies: Problems And Its Solutions, International Journal of Innovative Research and Development, June, 2013, Vol 2 Issue 6, pp.294-306.

[11] Stoeva, D., Challenges to Building Critical Infrastructure Policies in a Complicated Cyber Environment, Globalization, the State and the Individual, No 2(14)/2017, pp. 263-267, ISSN 2367-4555.

[12] Stoeva, D., Security zones, Globalization, the State and the Individual, No 2(14)/2017, pp. 31-40, ISSN 2367-4555.

[13] Venkatramulu S., & Rao C. G., Various Solutions for Address Resolution Protocol Spoofing Attacks, International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013.

[14] Zaefferer M., Inanir Y. S., & Karanatsios T., Intrusion Detection, University of Applied Sciences Cologne, Faculty for Informatics and Engineering, Gummersbach, February 2012.

[15] Zagorcheva, D., Model of relationships in the management of educational institutions, SocioBrains, Issue 82/2021, pp. 58-64, Journal homepage: www.sociobrains.com, ISSN 2367-5721 (online).

[16] Zagorcheva, D., Pavlov, D., The need for elaboration of a new economic model for business environment analysis, Journal in Entrepreneurship and Innovation, Ruse, 2017, ISSN 1311-3321, c.19-27.