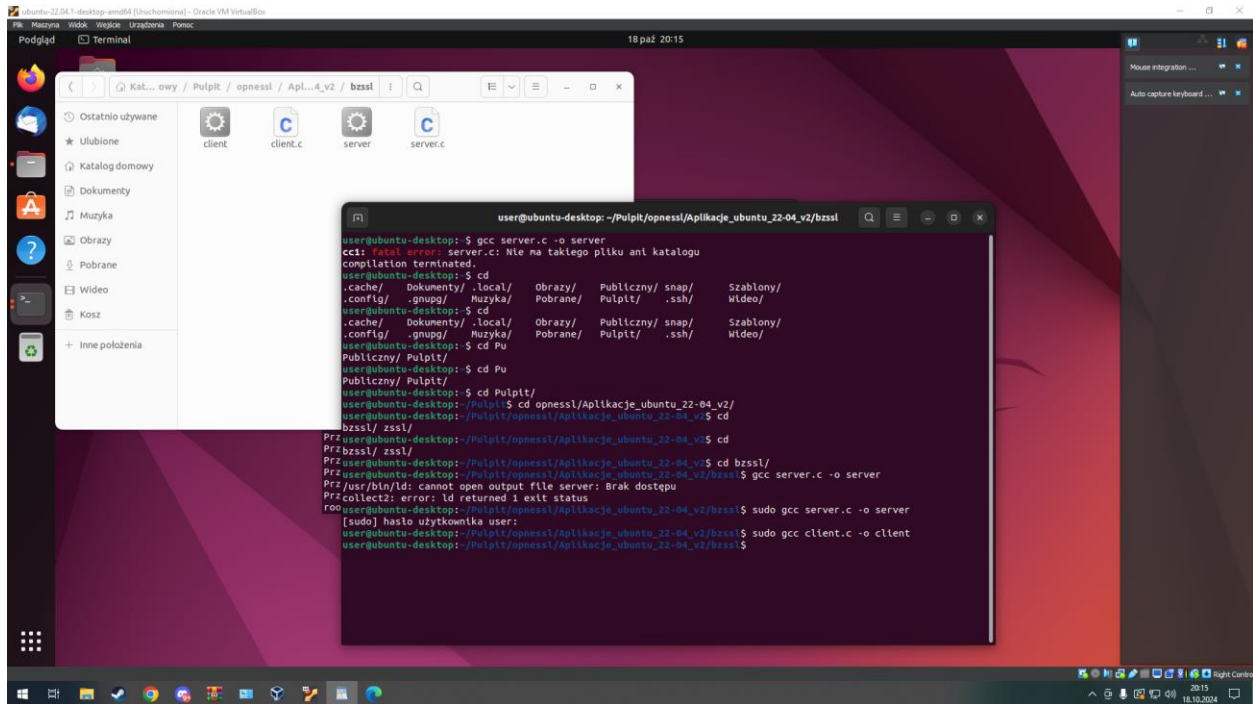
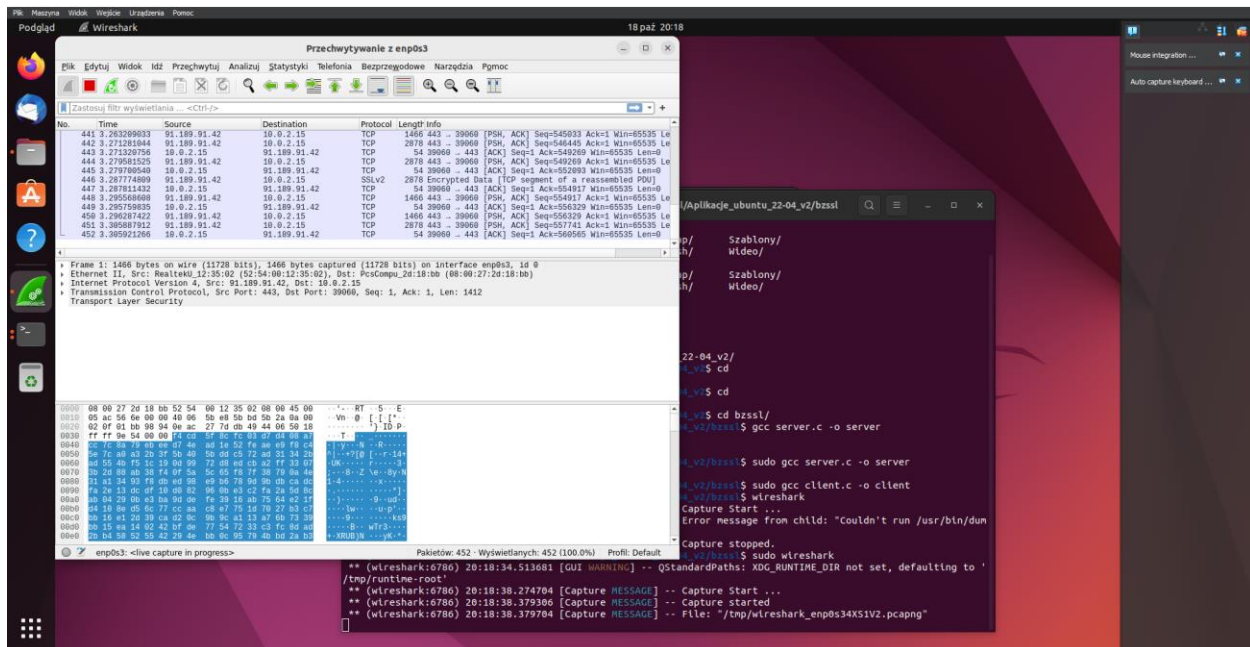


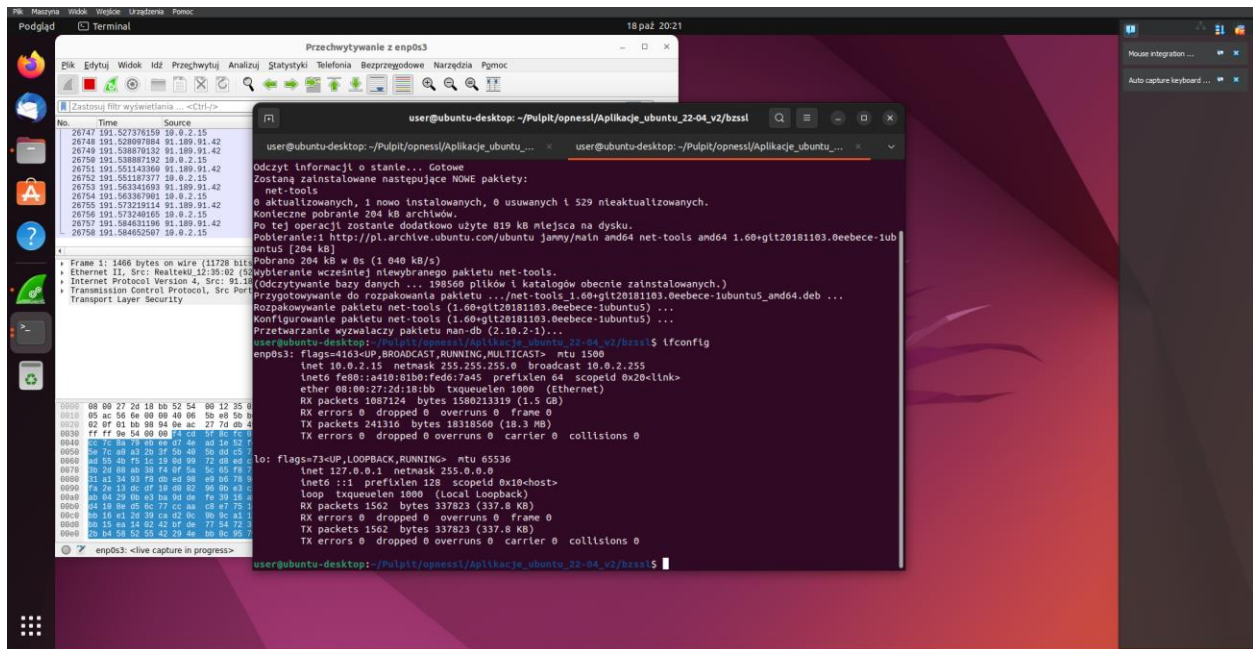
```
~/Pulpit/openssl/Aplikacje/bzssl $gcc server.c -o server ~/Pulpit/openssl/Aplikacje/bzssl $gcc
client.c -o client (jeżeli pojawią się ostrzeżenia, należy je zignorować)
```



2. Uruchom program Wireshark z prawami administratora i rozpocznij podsłuchiwanie swojej karty sieciowej. Z menu Capture wybierz opcję “start”, a następnie wybierz interfejs sieciowy i kliknij „ok.”. W tym momencie program Wireshark odczytuje wszystkie informacje przechodzące przez kartę sieciową Twojego komputera.



3. Odczytaj i zapisz adres IP swojego komputera wpisując polecenie `ifconfig` (jeżeli brakuje polecenia to zainstaluj: `sudo apt install net-tools`) Aby móc uruchomić program, należy zmienić tryb dostępu dla pliku – dodać tryb wykonywania `chmod +x server` Czynność tą należy wykonać tylko w przypadku, gdy plik wykonywalny nie posiada odpowiednio ustawionych praw wykonania. UWAGA! Aby uruchomić program w systemie Linux należy przed jego nazwą dodać znaki `./`, np. `./server`



4. Dwa pierwsze pliki client.c i server.c są odpowiednio oprogramowaniem klienta umożliwiającego połączenie się z podanym adresem IP i portem, na którym nasłuchuje serwer. Po nawiązaniu połączenia można odczytać wiadomość, która jest przesyłana tekstem otwartym do serwera.

5. Uruchom program server: ./server 1101 Program server nasłuchuje na porcie określonym w argumente wykonania.

```
user@ubuntu-desktop: ~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/bzssl
Zostaną zainstalowane następujące NOWE pakiety:
net-tools
0 aktualizowanych, 1 nowo instalowanych, 0 usuwanych i 529 nieaktualizowanych.
Konieczne pobranie 204 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 819 kB miejsca na dysku.
Pobieranie:1 http://pl.archive.ubuntu.com/ubuntu jammy/main amd64 net-tools amd64 1.60+git20181103.0eebece-1ub
untu5 [204 kB]
Pobrano 204 kB w 0s (1 040 kB/s)
Wybieranie wcześniej niewybranego pakietu net-tools.
(Odczytywanie bazy danych ... 198560 plików i katalogów obecnie zainstalowanych.)
Przygotowywanie do rozpakowania pakietu .../net-tools_1.60+git20181103.0eebece-1ubuntu5_amd64.deb ...
Rozpakowywanie pakietu net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Konfigurowanie pakietu net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Przetwarzanie wyzwalaczy pakietu man-db (2.10.2-1)...
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/bzssl$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a410:81b0:fed6:7a45 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:2d:18:bb txqueuelen 1000 (Ethernet)
    RX packets 1087124 bytes 1580213319 (1.5 GB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 241316 bytes 18318560 (18.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

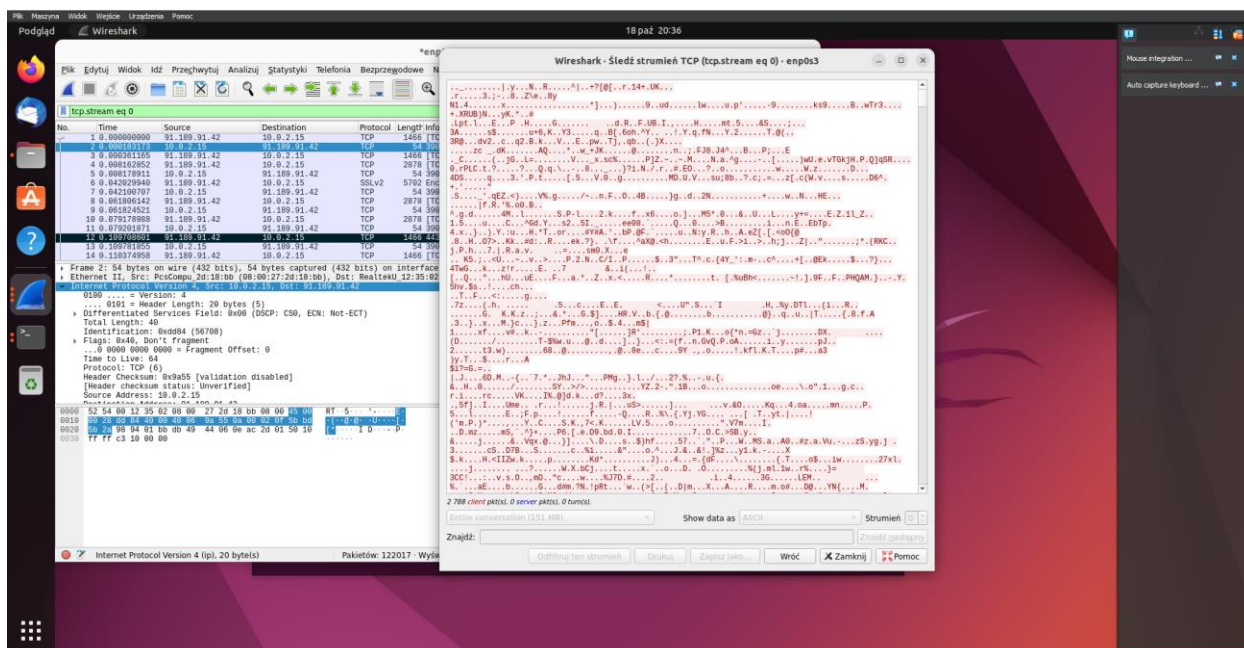
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1562 bytes 337823 (337.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1562 bytes 337823 (337.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/bzssl$ ./server 1101
```

6. Utwórz nową konsolę. Aby móc uruchomić program klienta, należy zmienić tryb dostępu dla pliku – dodać tryb wykonywania: `chmod +x client`

7. Uruchom program klienta i wyślij wiadomość na serwer: `./client 127.0.0.1 1101` 8. W programie zakończ przechwytywanie. Spróbuj odczytać jakie informacje zostały przesłane pomiędzy klientem a serwerem. Czy jest to możliwe? Możesz kliknąć prawym przyciskiem myszy na jednym z pakietów i wybrać opcję Podążaj->Strumień TCP to Wireshark połączy i wyświetli dane przesyłane w ramach połączenia.

```
user@ubuntu-desktop: ~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/bzssl
user@ubuntu-desktop: ~/Pulpit/op... x user@ubuntu-desktop: ~/Pulpit/op... x user@ubuntu-desktop: ~/Pulpit/opn... x
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/bzssl$ chmod +x client
chmod: nie można zmienić uprawnień do 'client': Operacja niedozwolona
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/bzssl$ sudo chmod +x client
[sudo] hasło użytkownika user:
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/bzssl$ ./client 10.0.2.15 1101
Polaczenie nawiązane
Podaj tekst do wysłania: benzema
Wysłano 7 bajtów
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/bzssl$
```




```
user@ubuntu-desktop: ~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/bzssl
0 aktualizowanych, 1 nowo instalowanych, 0 usuwanych i 529 nieaktualizowanych.
Konieczne pobranie 204 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 819 kB miejsca na dysku.
Pobieranie:1 http://pl.archive.ubuntu.com/ubuntu jammy/main amd64 net-tools amd64 1.60+git20181103.0eebece-1ub
untu5 [204 kB]
Pobrano 204 kB w 0s (1 040 kB/s)
Wybieranie wcześniej niewybranego pakietu net-tools.
(Odczytywanie bazy danych ... 198560 plików i katalogów obecnie zainstalowanych.)
Przygotowywanie do rozpakowania pakietu .../net-tools_1.60+git20181103.0eebece-1ubuntu5_amd64.deb ...
Rozpakowywanie pakietu net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Konfigurowanie pakietu net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Przetwarzanie wyzwalaczy pakietu man-db (2.10.2-1)...
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/bzssl$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a410:81b0:fed6:7a45 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:2d:18:bb txqueuelen 1000 (Ethernet)
    RX packets 1087124 bytes 1580213319 (1.5 GB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 241316 bytes 18318560 (18.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1562 bytes 337823 (337.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1562 bytes 337823 (337.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/bzssl$ ./server 1101
połączono z: 10.0.2.15
serwer tcp odebrał: benzema
```

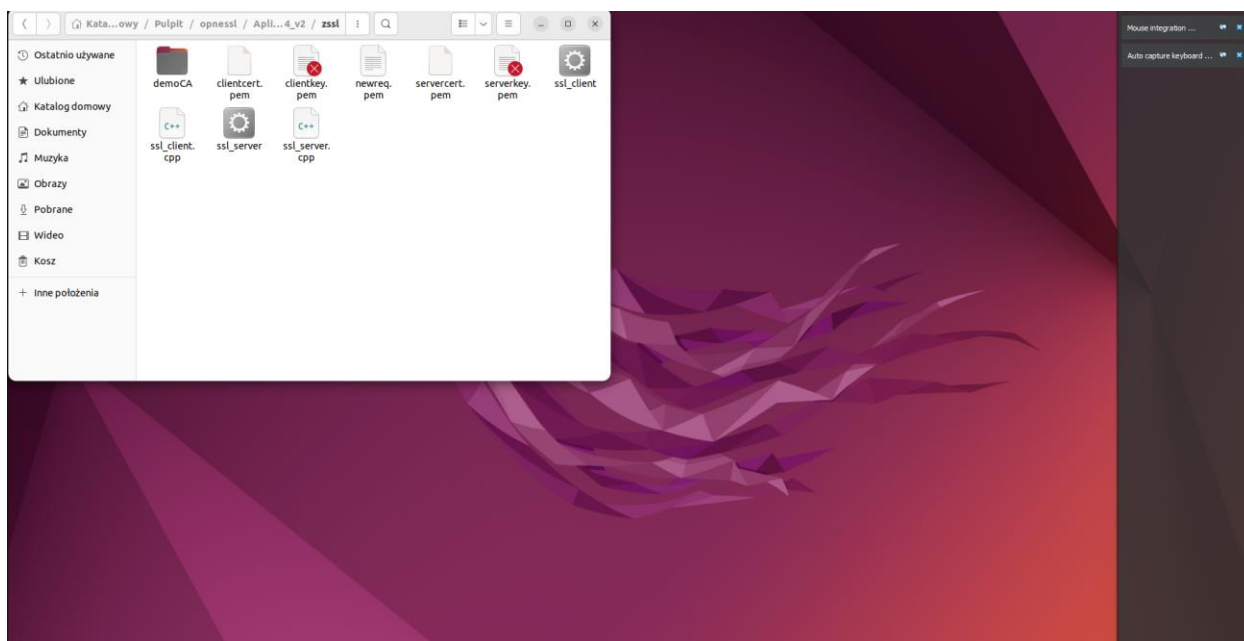
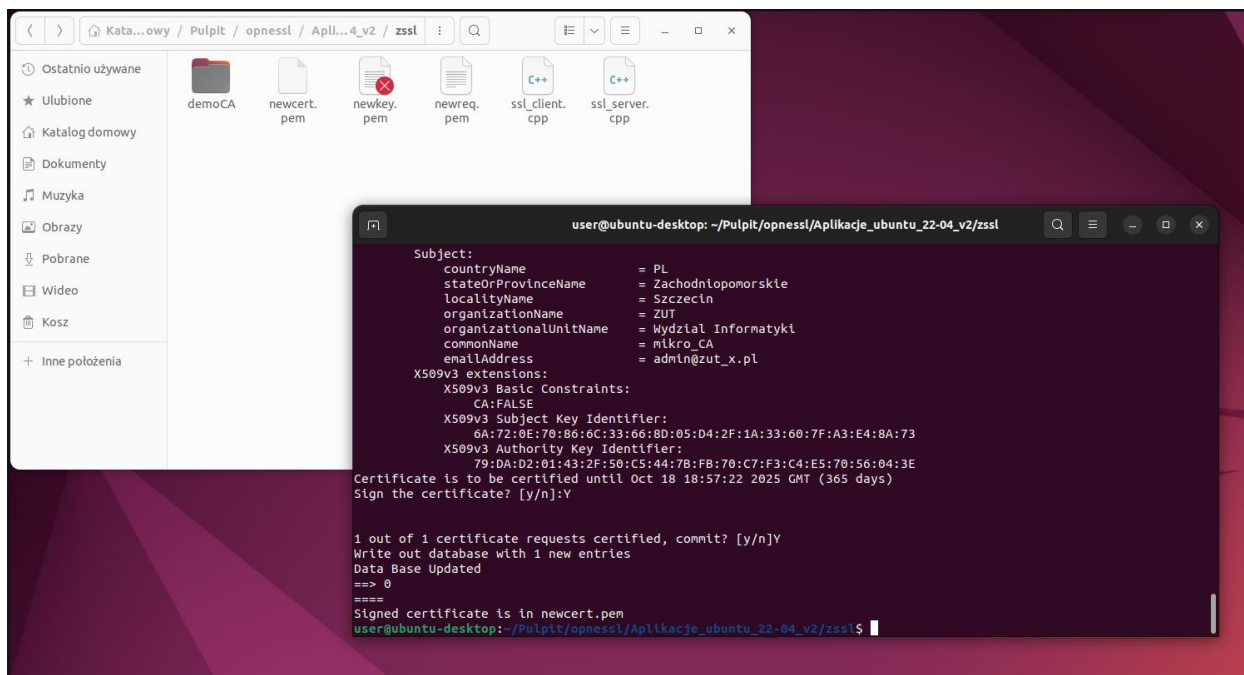
1. Utwórz własny mikro urządzenie certyfikacji przy pomocy biblioteki OpenSSL (patrz rozdz. 4.1).
Desktop/openssl/Aplikacje/zssl#/usr/lib/ssl/misc/CA.pl -newca

```
user@ubuntu-desktop: ~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl
40:21:b2:e0:4c:4b:71:60:e7:bd:48:71:49:ed:1a:64:14:5c:eb:57
Validity
  Not Before: Oct 18 18:53:01 2024 GMT
  Not After : Oct 18 18:53:01 2027 GMT
Subject:
  countryName          = PL
  stateOrProvinceName  = Zachodniopomorskie
  organizationName      = ZUT
  organizationalUnitName = Wydział Informatyki
  commonName            = mikro_CA
  emailAddress          = admin@zut_x.pl
X509v3 extensions:
  X509v3 Subject Key Identifier:
    79:DA:D2:01:43:2F:50:C5:44:7B:FB:70:C7:F3:C4:E5:70:56:04:3E
  X509v3 Authority Key Identifier:
    79:DA:D2:01:43:2F:50:C5:44:7B:FB:70:C7:F3:C4:E5:70:56:04:3E
  X509v3 Basic Constraints: critical
    CA:TRUE
Certificate is to be certified until Oct 18 18:53:01 2027 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
==> 0
====
CA certificate is in ./demoCA/cacert.pem
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$
```

2. Wygeneruj żądania wystawienia certyfikatu dla serwera (program ssl_server), patrz rozdz. 4.2. Desktop/openssl/Aplikacje/zssl#/usr/lib/ssl/misc/CA.pl –newreq 3. Wystaw certyfikat dla serwera (patrz rozdz. 4.3).

Desktop/openssl/Aplikacje/zssl#/usr/lib/ssl/misc/CA.pl –sign



4. Zamień nazwy newcert.pem na servercert.pem oraz newkey.pem na serverkey.pem 5. Kroki 2 i 3 powtórz także dla oprogramowania ssl_klient. Dwa pliki newkey.pem i newcert.pem zamień na clientkey.pem i clientcert.pem

1.Odpalam serwer na porcie 1101

```
user@ubuntu-desktop: ~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl
user@ubuntu-desktop: ~/P... x user@ubuntu-desktop: ~/P... x user@ubuntu-desktop: ~/P... x user@ubuntu-desktop: ~/P... x
/ciphercommon_block.c:124:
0F7273D9F7F0000:error:11800074:PKCS12 routines:PKCS12_pbe_crypt_ex:pkcs12 cipherfinal error:../crypto/pkcs12/p12_decr.c
86:maybe wrong password
0F7273D9F7F0000:error:1C800064:Provider routines:ossl_cipher_unpadblock:bad decrypt:../providers/implementations/cipher
/ciphercommon_block.c:124:
0F7273D9F7F0000:error:11800074:PKCS12 routines:PKCS12_pbe_crypt_ex:pkcs12 cipherfinal error:../crypto/pkcs12/p12_decr.c
86:maybe wrong password
0F7273D9F7F0000:error:0A080009:SSL routines:SSL_CTX_use_PrivateKey_file:PEM lib:../ssl/ssl_rsa.c:384:
ser@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ sudo ./ssl_server 1101
Enter PEM pass phrase:
321
321
321
C
ser@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ sudo ./ssl_server 1101
Enter PEM pass phrase:
321
321
321
C
ser@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ sudo ./ssl_server
usage: server port
ser@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ sudo ./ssl_server
usage: server port
ser@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ sudo ./ssl_server 4321
Enter PEM pass phrase:
C
ser@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ sudo ./ssl_server 1101
[sudo] hasło użytkownika user:
Enter PEM pass phrase:
```

2.Podajemy komunikat do przesłania


```
user@ubuntu-desktop: ~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl

Podaj komunikat: ^C
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ ip config
Object "config" is unknown, try "ip help".
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a410:81b0:fed6:7a45 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:2d:18:bb txqueuelen 1000 (Ethernet)
    RX packets 1276167 bytes 1856981436 (1.8 GB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 332956 bytes 23829118 (23.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1736 bytes 356130 (356.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1736 bytes 356130 (356.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ sudo ./ssl_client 127.0.0.1 1101
Enter PEM pass phrase:
polaczenie SSL uzywa TLS_AES_256_GCM_SHA384
Certyfikat serwera:
    temat: /C=PL/ST=Zachodniopomorskie/L=Szczecin/O=ZUT/OU=Wydzial Informatyki/CN=mikro_CA/emailAddress=admin@zut_x.pl
Wydany przez: /C=PL/ST=Zachodniopomorskie/O=ZUT/OU=Wydzial Informatyki/CN=mikro_CA/emailAddress=admin@zut_x.pl

Podaj komunikat: benzema
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$
```

3. Otrzymujemy wyslany komunikat.

```
user@ubuntu-desktop: ~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl

user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ ./ssl_server
usage: server port
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ sudo ./ssl_server
usage: server port
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ ls
clientcert.pem demoCA servercert.pem ssl_client ssl_server
clientkey.pem newreq.pem serverkey.pem ssl_client.cpp ssl_server.cpp
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ sudo wireshark
[sudo] haslo uzytkownika user:
** (wireshark:8595) 21:34:22.860932 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
** (wireshark:8595) 21:34:25.048582 [Capture MESSAGE] -- Capture Start ...
** (wireshark:8595) 21:34:25.114399 [Capture MESSAGE] -- Capture started
** (wireshark:8595) 21:34:25.115755 [Capture MESSAGE] -- File: "/tmp/wireshark_enp0s3K6GW2.pcapng"
** (wireshark:8595) 21:59:58.664868 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:8595) 21:59:58.668302 [Capture MESSAGE] -- Capture stopped.
** (wireshark:8595) 22:00:46.918323 [Capture MESSAGE] -- Capture Start ...
** (wireshark:8595) 22:00:47.022743 [Capture MESSAGE] -- Capture started
** (wireshark:8595) 22:00:47.022771 [Capture MESSAGE] -- File: "/tmp/wireshark_enp0s3STW7V2.pcapng"
** (wireshark:8595) 22:01:02.441832 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:8595) 22:01:02.444696 [Capture MESSAGE] -- Capture stopped.
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$ sudo ./ssl_server 1101
[sudo] haslo uzytkownika user:
Enter PEM pass phrase:
Polaczenie z 100007f, port d2ca
polaczenie TLS uzywa TLS_AES_256_GCM_SHA384
Certyfikat klienta:
    temat: /C=PL/ST=Zachodniopomorskie/L=Szczecin/O=ZUT/OU=Wydzial Informatyki /CN=mikro_CA/emailAddress=admin@zut_x.pl
Wydany przez: /C=PL/ST=Zachodniopomorskie/O=ZUT/OU=Wydzial Informatyki/CN=mikro_CA/emailAddress=admin@zut_x.pl
Otrzymano 7 znakow: 'benzema'
user@ubuntu-desktop:~/Pulpit/opnessl/Aplikacje_ubuntu_22-04_v2/zssl$
```

55

*enp0s3

Plik Edytuj Widok Idź Przechwytyj Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pgmoc

ludp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.168.1.1	DNS	89	Standard query 0xfd27 AAAA connectivity-check.ubuntu.com
2	0.000005894	192.168.1.1	10.0.2.15	DNS	537	Standard query response 0xfd27 AAAA connectivity-check.ubuntu.com AAAA 2620:2d:4000:1::2b AAAA 2001:67c

Frame 2: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface enp0s3, id 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_2d:18:bb (08:00:27:2d:18:bb)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 55139
Domain Name System (response)

```
0000 08 00 27 2d 18 bb 52 54 00 12 35 02 08 00 45 00  ... RT  ... E
0010 02 0b 78 9e 00 00 40 11 32 8c c0 a8 01 01 0a 00  ...x... 2...
0020 02 0f 00 35 d7 63 01 f7 e3 eb fd 27 81 80 00 01  ...5...
0030 00 0c 00 03 00 03 12 63 6f 0e 0e 65 53 74 69 76  ...c onnectiv
0040 69 74 79 2d 63 68 65 63 6b 00 75 62 75 6a 74 75  ity-check k ubuntu
0050 03 63 6f 6d 00 00 1c 00 01 c9 0c 00 1c 00 01 00  com...
0060 00 00 2f 00 10 26 20 00 2d 40 00 00 01 00 00 00  /...& ...-
0070 00 00 00 00 2b c0 0c 00 1c 00 01 00 00 00 2f 00  ...+... /-
0080 10 20 01 06 7c 15 62 00 00 00 00 00 00 00 00  ...| b...
0090 23 c0 0c 00 1c 00 01 00 00 00 2f 00 10 26 20 00  #... /-&
00a0 2d 40 02 00 01 00 00 00 00 00 00 01 00 c0 0c 00  ~@...
00b0 1c 00 01 00 00 00 2f 00 10 26 20 00 2d 40 00 00  ... /-& --@-
```