

**WYŻSZA SZKOŁA HANDLOWA  
W RADOMIU**



**RADOM  
ACADEMY OF ECONOMICS**

## **Wydział Studiów Strategicznych i Technicznych**

**Kierunek: Informatyka, rok II, semestr III (2021/2022)**

# **LABORATORIUM Z PODSTAW KRYPTOGRAFII**

**Prowadzący: dr Piotr Dobosz**

**Zespół laboratoryjny:**

**Magdalena Szafrńska, nr albumu: 18345**

# Spis treści

<b>Spis treści</b>	<b>1</b>
<b>Cel ćwiczenia</b>	<b>2</b>
<b>Informacje wstępne</b>	<b>2</b>
<b>Użyte narzędzia i aplikacje</b>	<b>2</b>
<b>Przebieg ćwiczenia</b>	<b>3</b>
CZĘŚĆ I: Badanie ruchu sieci na stronie internetowej	3
CZĘŚĆ II: Testowanie wysyłania wiadomości elektronicznej	6
<b>Wnioski</b>	<b>11</b>

# Cel ćwiczenia

Podstawowym celem zadania jest przetestowanie podstawowych technik szyfrowania powszechnie użytkowanych technologii. Opisane narzędzia były testowane dla systemu Windows 10.

## Informacje wstępne

W obecnych czasach bezpieczeństwo danych w każdej instytucji musi stać na najwyższym poziomie. Szczególnie narażone są wiadomości przesyłane pocztą elektroniczną. W dobie rozporządzeń RODO należy dbać, aby wiadomość mogli odebrać jedynie adresaci. Ponadto warto mieć na uwadze wszelkiego rodzaju formularze logowania i/lub kontaktu na stronach WWW. Również tutaj istnieje bowiem ryzyko, że poufną treść przechwyci osoba niepożądana. Rozwiązaniem opisanych problemów będzie zastosowanie odpowiednich kluczy szyfrujących.

Klucze PGP są od dawna stosowanym elementem szyfrującym. Ze względu na używanie asymetrycznej architektury szyfrowania możemy część publiczną dostarczyć każdemu (np. wstawiając klucz na stronie WWW czy wysłać takowy nieszyfrowaną pocztą). Z drugiej strony posiadamy własny klucz prywatny, dzięki któremu możemy odszyfrować wiadomość. Z kolei w przypadku stron WWW od dłuższego czasu firmy i organizacje zajmujące się tworzeniem przeglądarek oraz wyszukiwarek internetowych forsują używanie przez wszystkie witryny kluczy uwierzytelniających witryny. Dzięki takiemu podejściu użytkownik końcowy otrzyma odpowiedni komunikat od strony WWW, że użyty klucz nie pasuje do wpisanego adresu (phishing). Po drugie, klucze SSL szyfrują przesyłane dane na linii klient-serwer. Dzięki temu dane przesyłane przez sieć nie będą widoczne dla osoby nasłuchującej sieć.

## Użyte narzędzia i aplikacje

- **Wireshark** - umożliwia przechwytywanie i nagrywanie pakietów danych, a także ich dekodowanie
- **Laragon/XAMPP** - lokalny serwer
- **RawCap** - zbiera ruch w sieci z komputera lokalnego
- **OpenSSL** - otwarta implementacja protokołów SSL i TLS oraz algorytmów kryptograficznych ogólnego przeznaczenia
- **poczta elektroniczna** - Mozilla Thunderbird
- **klucze PGP** - narzędzie służące do szyfrowania, odszyfrowywania i uwierzytelniania między innymi poczty elektronicznej
- **strona z formularzem** (skorzystałam z: [https://www.w3schools.com/php/php\\_forms.asp](https://www.w3schools.com/php/php_forms.asp))

## Przebieg ćwiczenia

Ćwiczenie podzielone jest na dwie części. W pierwszej kolejności w programie Wireshark należy sprawdzić ruch na sieci. Szczególnie należy zwrócić uwagę na działanie

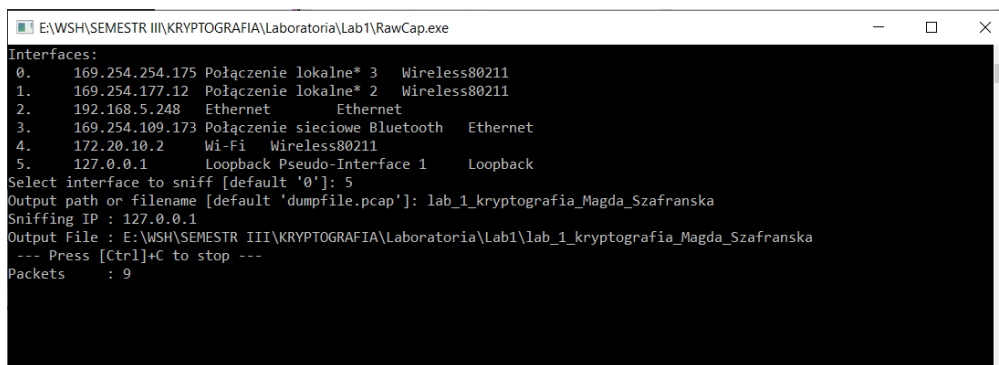
stron WWW, które nie posiadają klucza SSL. W tym celu można stworzyć prostą stronę formularza (HTML + PHP), uruchomić na serwerze stron WWW (np. na narzędziu XAMPP bądź na jakimkolwiek serwerze WWW - ja użyję Laragon) i spróbować kilkakrotnie wysłać informacje przez formularz.

Następnie należy wystawić certyfikat dla strony i ponownie spróbować przesłać dane. Sprawdzę, czy Wireshark był w stanie odczytać wartości przed wystawieniem certyfikatu oraz co stało się po uruchomieniu strony z certyfikatem.

W drugiej części ćwiczenia należy przetestować wysyłanie wiadomości elektronicznej. Następnie sprawdzę, czy Wireshark jest w stanie przechwycić wiadomości pocztowe. Kolejno stworzę i zastosuję klucz PGP. Ponownie sprawdzę, czy można przechwycić wiadomość LUB czy można taką pocztę otworzyć, jeżeli wyślemy ją do kogoś innego (np. przez pomyłkę).

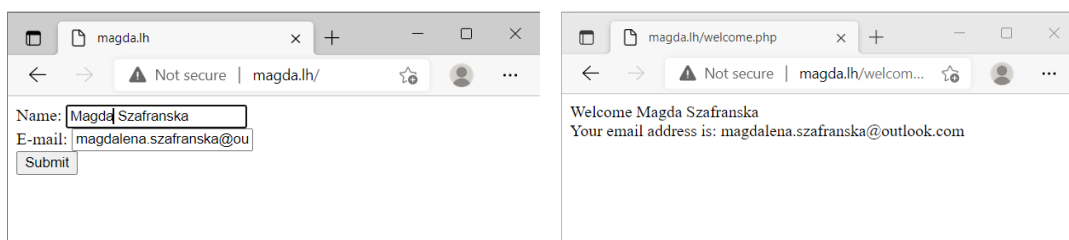
## CZĘŚĆ I: Badanie ruchu sieci na stronie internetowej

1. W programie RawCap utworzyłam plik, w którym przeanalizuję stronę niezabezpieczoną certyfikatem SSL



```
E:\WSH\SEMESTR III\KRYPTOGRAFIA\Laboratoria\Lab1\RawCap.exe
Interfaces:
0. 169.254.254.175 Połączenie lokalne* 3 Wireless80211
1. 169.254.177.12 Połączenie lokalne* 2 Wireless80211
2. 192.168.5.248 Ethernet Ethernet
3. 169.254.109.173 Połączenie sieciowe Bluetooth Ethernet
4. 172.20.10.2 Wi-Fi Wireless80211
5. 127.0.0.1 Loopback Pseudo-Interface 1 Loopback
Select interface to sniff [default '0']: 5
Output path or filename [default 'dumpfile.pcap']: lab_1_kryptografia_Magda_Szafranska
Sniffing IP : 127.0.0.1
Output File : E:\WSH\SEMESTR III\KRYPTOGRAFIA\Laboratoria\Lab1\lab_1_kryptografia_Magda_Szafranska
--- Press [Ctrl]+C to stop ---
Packets : 9
```

2. Wypełniłam formularz na stronie, którą stworzyłam na serwerze lokalnym i która to strona nie jest zabezpieczona certyfikatem SSL po czym wysłałam go.



3. Po zamknięciu RawCapa otworzyłam w narzędziu Wireshark wygenerowany podczas wysyłania formularza stworzony plik z analizą ruchu, który zebrał program RawCap.

No.	Time	Source	Destination	Protocol	Length	Info
933	27.804612	127.0.0.1	127.0.0.1	HTTP	510	GET / HTTP/1.1
935	27.807632	127.0.0.1	127.0.0.1	HTTP	498	HTTP/1.1 200 OK (text/html)
940	28.648772	127.0.0.1	127.0.0.1	HTTP	527	GET / HTTP/1.1
942	28.652753	127.0.0.1	127.0.0.1	HTTP	497	HTTP/1.1 200 OK (text/html)
944	28.691609	127.0.0.1	127.0.0.1	HTTP	464	GET /favicon.ico HTTP/1.1
946	28.692608	127.0.0.1	127.0.0.1	HTTP	477	HTTP/1.1 404 Not Found (text/html)
1056	30.503669	127.0.0.1	127.0.0.1	HTTP	510	GET / HTTP/1.1
1058	30.505674	127.0.0.1	127.0.0.1	HTTP	497	HTTP/1.1 200 OK (text/html)
1060	30.645409	127.0.0.1	127.0.0.1	HTTP	510	GET / HTTP/1.1
1062	30.646394	127.0.0.1	127.0.0.1	HTTP	497	HTTP/1.1 200 OK (text/html)
1069	30.828182	127.0.0.1	127.0.0.1	HTTP	510	GET / HTTP/1.1
1071	30.829219	127.0.0.1	127.0.0.1	HTTP	497	HTTP/1.1 200 OK (text/html)
1073	31.013742	127.0.0.1	127.0.0.1	HTTP	510	GET / HTTP/1.1
1075	31.014739	127.0.0.1	127.0.0.1	HTTP	497	HTTP/1.1 200 OK (text/html)
1211	47.628696	127.0.0.1	127.0.0.1	HTTP	705	POST /welcome.php HTTP/1.1 (application/x-www-form-urlencoded)
1213	47.629675	127.0.0.1	127.0.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)

4. Po unikatowym rodzaju informacji wybrałam do analizy dany pakiet, który został wysłany do strony internetowej. Jest to pakiet wypełnionego formularza na niezabezpieczonej certyfikatem SSL stronie.

The screenshot shows the Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows a series of HTTP GET requests followed by a POST request at packet 1211. The packet details pane for packet 1211 shows the raw packet data, the Internet Protocol version 4 header, the Transmission Control Protocol header, and the Hypertext Transfer Protocol section. The POST request is encoded in application/x-www-form-urlencoded and contains a form item with the name 'Magda Szafranska'.

No.	Time	Source	Destination	Protocol	Length	Info
933	27.804612	127.0.0.1	127.0.0.1	HTTP	510	GET / HTTP/1.1
935	27.807632	127.0.0.1	127.0.0.1	HTTP	498	HTTP/1.1 200 OK (text/html)
940	28.648772	127.0.0.1	127.0.0.1	HTTP	527	GET / HTTP/1.1
942	28.652753	127.0.0.1	127.0.0.1	HTTP	497	HTTP/1.1 200 OK (text/html)
944	28.691609	127.0.0.1	127.0.0.1	HTTP	464	GET /favicon.ico HTTP/1.1
946	28.692608	127.0.0.1	127.0.0.1	HTTP	477	HTTP/1.1 404 Not Found (text/html)
1056	30.503669	127.0.0.1	127.0.0.1	HTTP	510	GET / HTTP/1.1
1058	30.505674	127.0.0.1	127.0.0.1	HTTP	497	HTTP/1.1 200 OK (text/html)
1060	30.645409	127.0.0.1	127.0.0.1	HTTP	510	GET / HTTP/1.1
1062	30.646394	127.0.0.1	127.0.0.1	HTTP	497	HTTP/1.1 200 OK (text/html)
1069	30.828182	127.0.0.1	127.0.0.1	HTTP	510	GET / HTTP/1.1
1071	30.829219	127.0.0.1	127.0.0.1	HTTP	497	HTTP/1.1 200 OK (text/html)
1073	31.013742	127.0.0.1	127.0.0.1	HTTP	510	GET / HTTP/1.1
1075	31.014739	127.0.0.1	127.0.0.1	HTTP	497	HTTP/1.1 200 OK (text/html)
1211	47.628696	127.0.0.1	127.0.0.1	HTTP	705	POST /welcome.php HTTP/1.1 (application/x-www-form-urlencoded)
1213	47.629675	127.0.0.1	127.0.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)

Frame 1211: 705 bytes on wire (5640 bits), 705 bytes captured (5640 bits) on interface 0

Raw packet data

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Transmission Control Protocol, Src Port: 49497, Dst Port: 80, Seq: 1, Ack: 1, Len: 665

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: "name" = "Magda Szafranska"

0000 45 00 02 c1 37 63 40 00 80 06 00 00 7f 00 00 01 0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a0 73 74 73 3a 20 31 0d 0a 4f 72 69 6f 69 6e 3a 20 00b0 68 74 74 70 3a 2f 2f 6d 61 67 64 61 2e 6c 68 0d 00c0 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 00d0

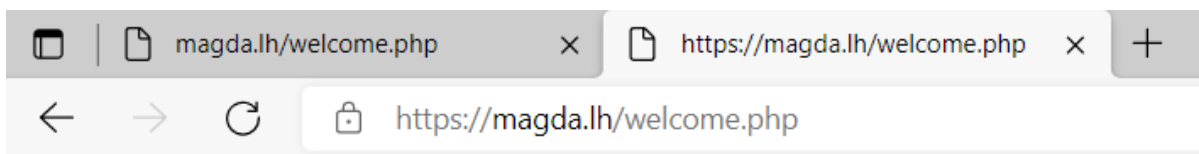
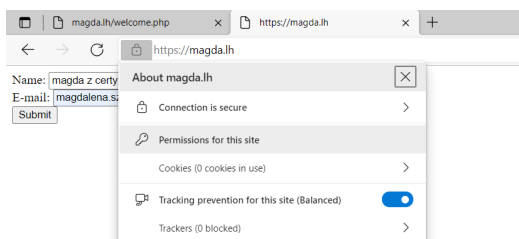
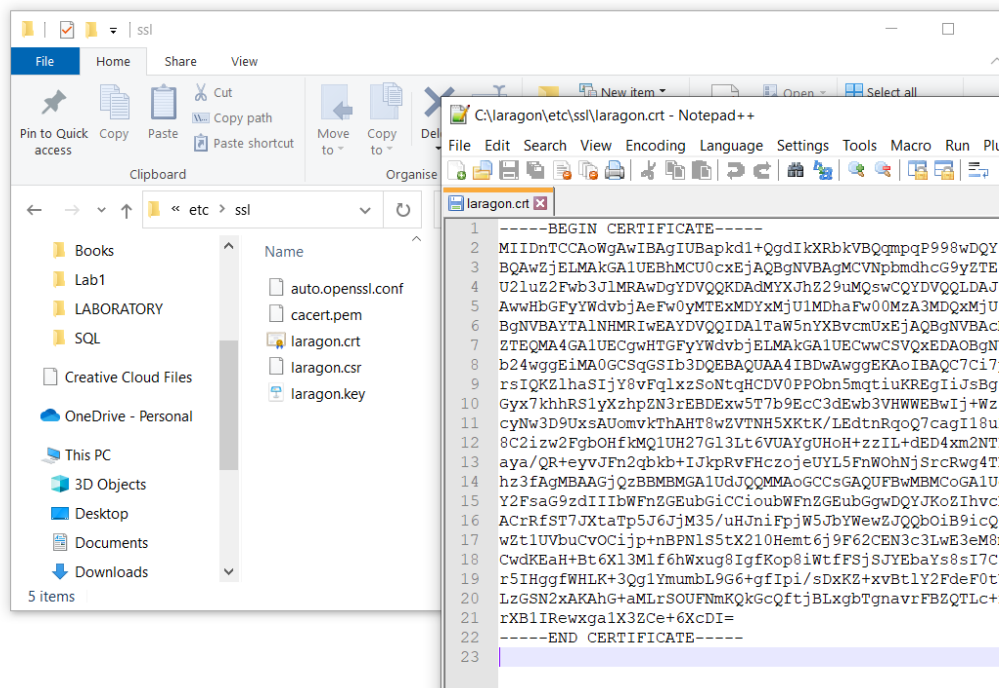
0000 7f 00 00 01 c1 59 00 50 7b c6 1a 52 ec d5 46 1a 0010 50 18 27 f9 b7 65 00 00 50 4f 53 54 20 2f 77 65 0020 6c 63 6f 6d 65 2e 70 68 70 20 48 54 54 50 2f 31 0030 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 67 64 61 2e 0040 6c 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0050 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 0060 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 32 0d 0a 0070 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 0080 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 0090 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 00a

magda.lh/ x Certificate for laragon x +

← → ↻ 🔒 https://magda.lh

Name:

E-mail:



Welcome magda z certyfikatem  
Your email address is: magdalena.szafranska@outlook.com

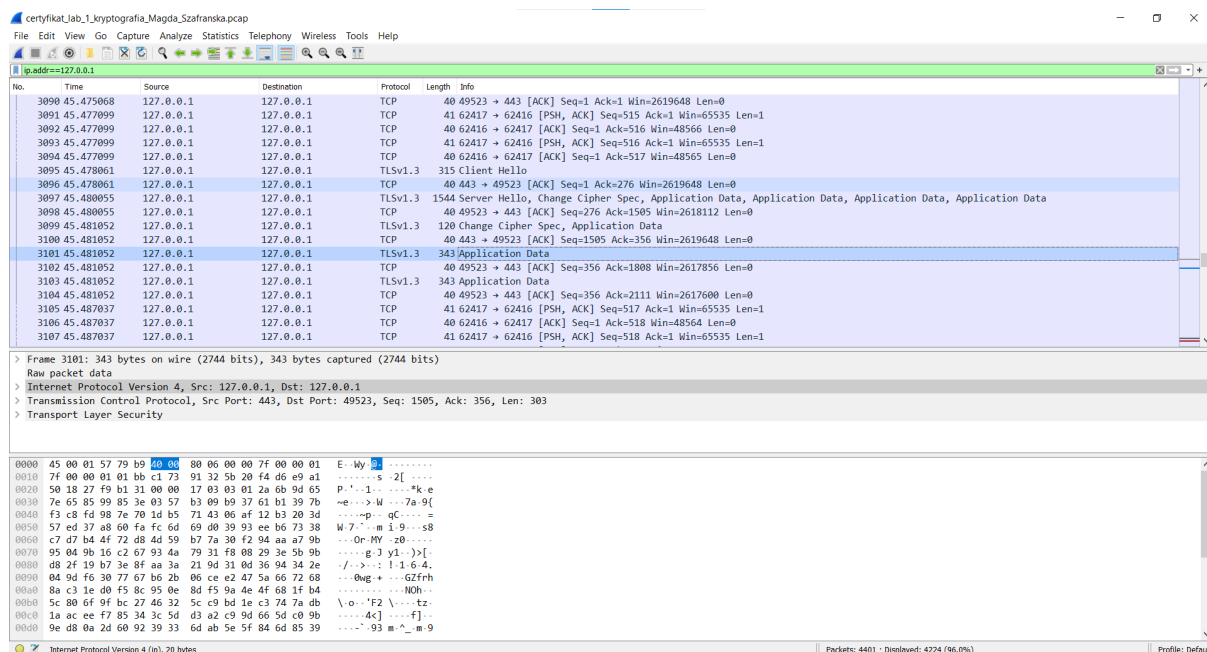
6. W programie RawCap stworzyłam plik, w którym przeanalizuję wybrany pakiet po wejściu na zabezpieczoną stronę.

```

E:\WSH\SEMESTR III\KRYPTOGRAFIA\Laboratoria\Lab1\RawCap.exe
Interfaces:
0. 169.254.254.175 Połączenie lokalne* 3 Wireless80211
1. 169.254.177.12 Połączenie lokalne* 2 Wireless80211
2. 192.168.5.248 Ethernet Ethernet
3. 169.254.109.173 Połączenie sieciowe Bluetooth Ethernet
4. 172.20.10.2 Wi-Fi Wireless80211
5. 127.0.0.1 Loopback Pseudo-Interface 1 Loopback
Select interface to sniff [default '0']: 5
Output path or filename [default 'dumpfile.pcap']: certyfikat_lab_1_kryptografia_Magda_Szafranska.pcap
Sniffing IP : 127.0.0.1
Output File : E:\WSH\SEMESTR III\KRYPTOGRAFIA\Laboratoria\Lab1\certyfikat_lab_1_kryptografia_Magda_Szafranska.pcap
--- Press [Ctrl]+C to stop ---
Packets : 23

```

- Po zamknięciu RawCapa otworzyłam wygenerowany plik w Wiresharku i sprawdziłam wygenerowany podczas wysyłania z zabezpieczonej strony formularza ruch.

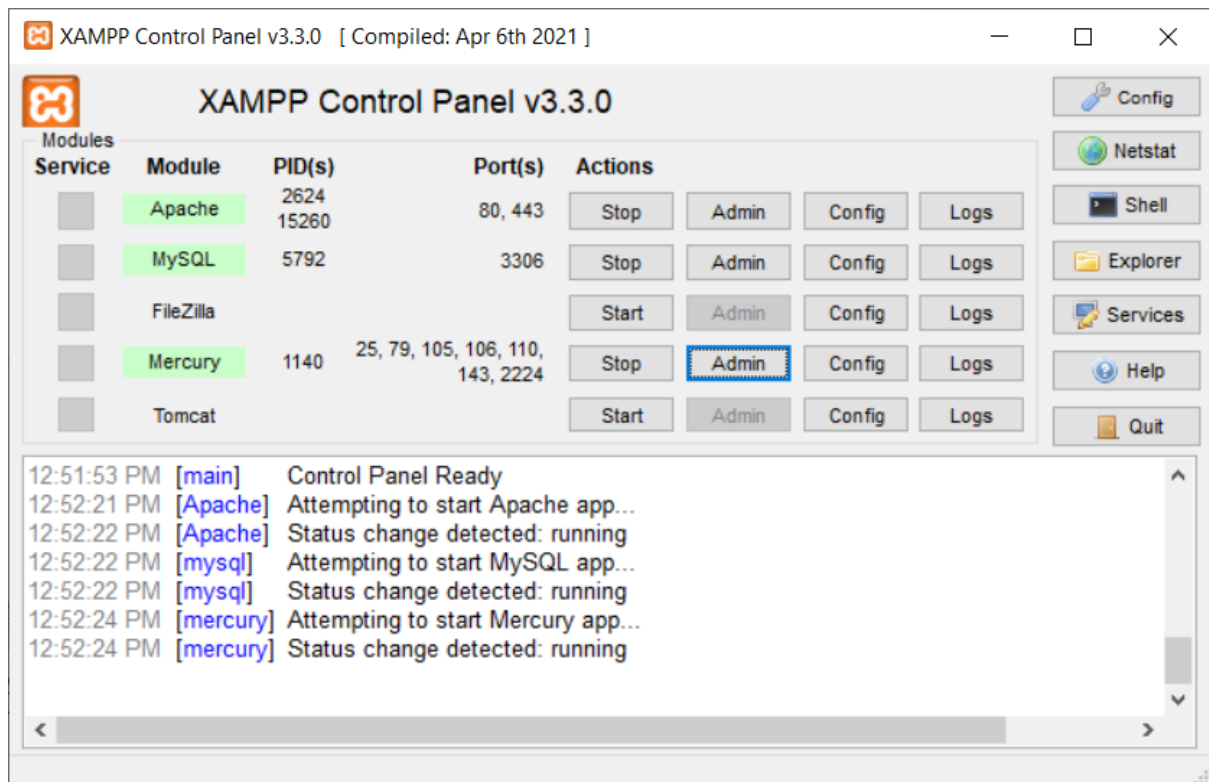


- Przeanalizowałam wysłany pakiet. Jak widać przesłane w formularzu na zabezpieczonej stronie dane zostały zaszyfrowane. Nie da się ich odczytać w sposób jawny tak, jak działa się w przypadku wysłania formularza na stronie internetowej niezabezpieczonej certyfikatem SSL

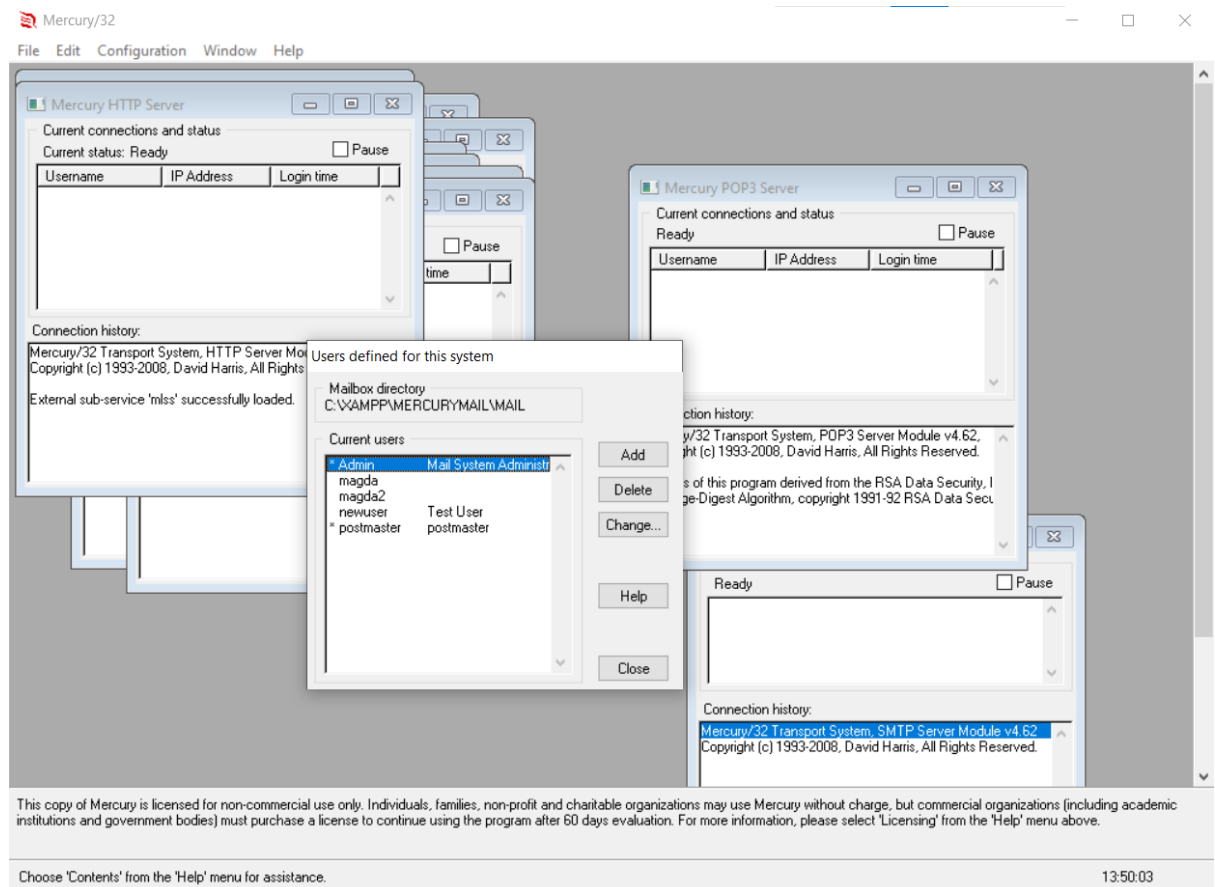
## CZĘŚĆ II: Testowanie wysyłania wiadomości elektronicznej

W drugiej części zadania sprawdzałam, czy Wireshark jest w stanie przechwycić wiadomości pocztowe.

- Uruchomiłam usługi Apache, MySQL i Mercury w narzędziu XAMPP.



2. Utworzyłam dwa adresy mailowe na serwerze lokalnym.



3. Zainstalowałam narzędzie Mozilla Thunderbird jako pocztę elektroniczną.



4. Wysłałam wiadomość mailową używając serwera lokalnego bez szyfrowania wiadomości.

Od Ja <magda@localhost> ★  
Temat test  
Do Ja <magda2@localhost> ★  
test

5. Przeanalizowałam w programie Wireshark ruch na serwerze SMTP przechwytyjąc wysłaną wiadomość i wybierając dany pakiet do analizy.

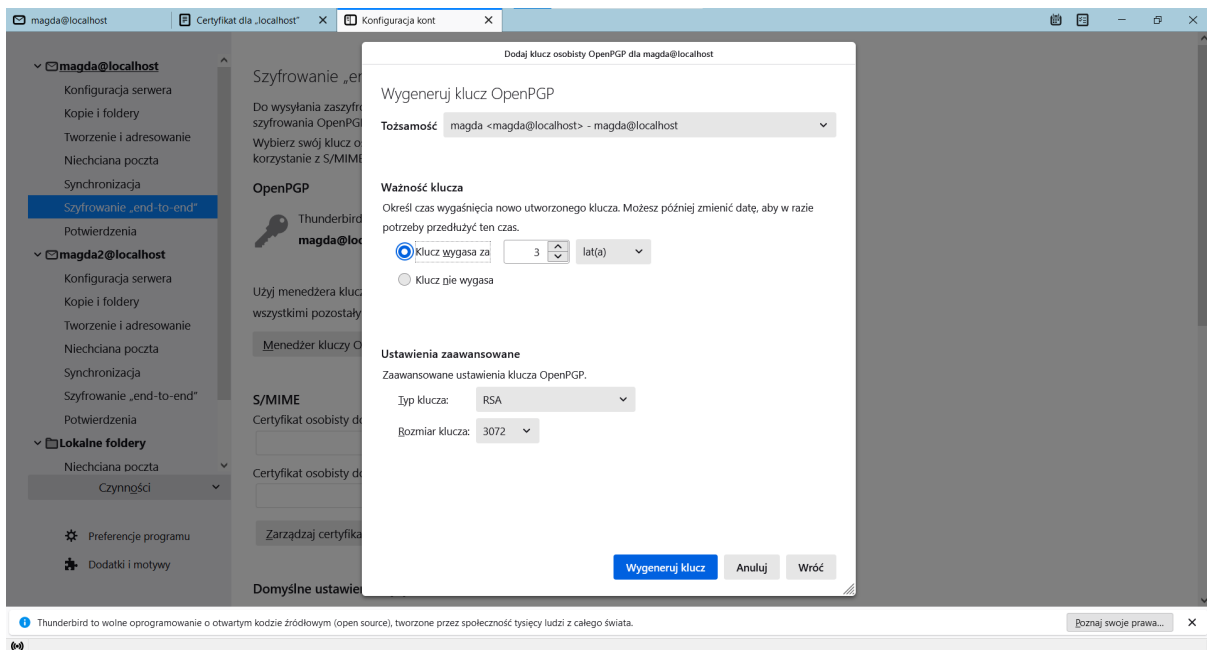
The screenshot shows the Wireshark interface with a packet capture of SMTP traffic. The main pane displays a list of packets, with packet 328 selected. The details pane on the right shows the structure of the selected packet, which is an Internet Message Format (IMF) message. The message details include the Message-ID, Date, MIME-Version, User-Agent, Content-Language, To, From, Subject, Content-Type, Content-Transfer-Encoding, and Line-based text data.

Packet 328 details:

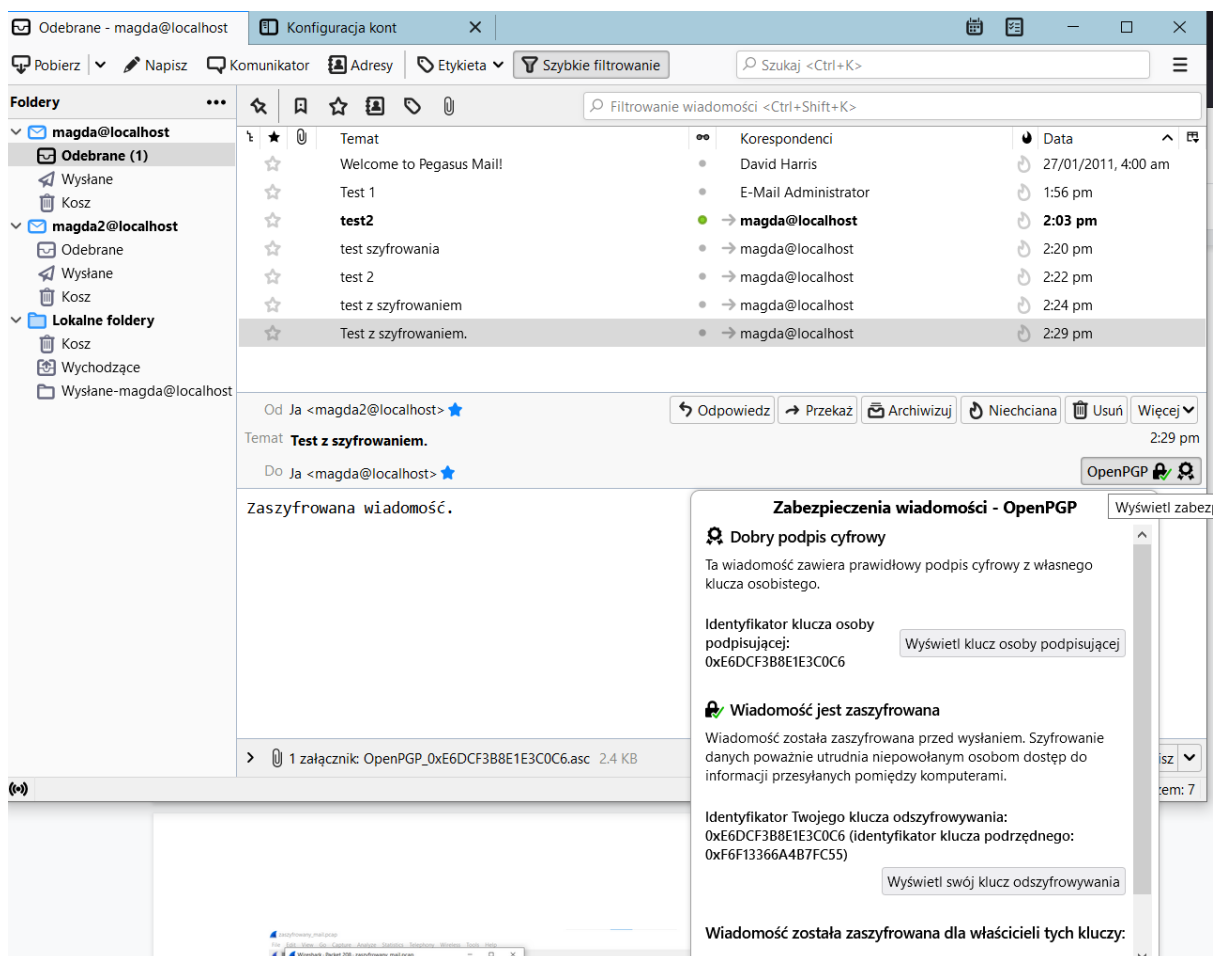
- Simple Mail Transfer Protocol
- Internet Message Format
  - Message-ID: <94f02cb0-63b3-977e-d084-690300b8db8f@localhost>
  - Date: Sat, 20 Nov 2021 14:02:10 +0100
  - MIME-Version: 1.0
  - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Thunderbird/91.3.2
  - Content-Language: pl
  - To: magda2@localhost, 1 item
  - From: magda <magda@localhost>, 1 item
  - Subject: test
  - Content-Type: text/plain; charset=UTF-8; format=flowed
  - Content-Transfer-Encoding: 7bit
  - Line-based text data: text/plain (2 lines)

Jak można zauważyć, sprawdzając wybrany pakiet mamy dostęp do dowolnych informacji wysłanych w ów wiadomości email, m.in. nadawcę i odbiorcę wiadomości, tytuł, treść czy chociażby dane odnośnie czasu i daty wysłania.

6. Wygenerowałam klucze PGP dla dwóch kont pocztowych i dodaję ich do konfiguracji poczty

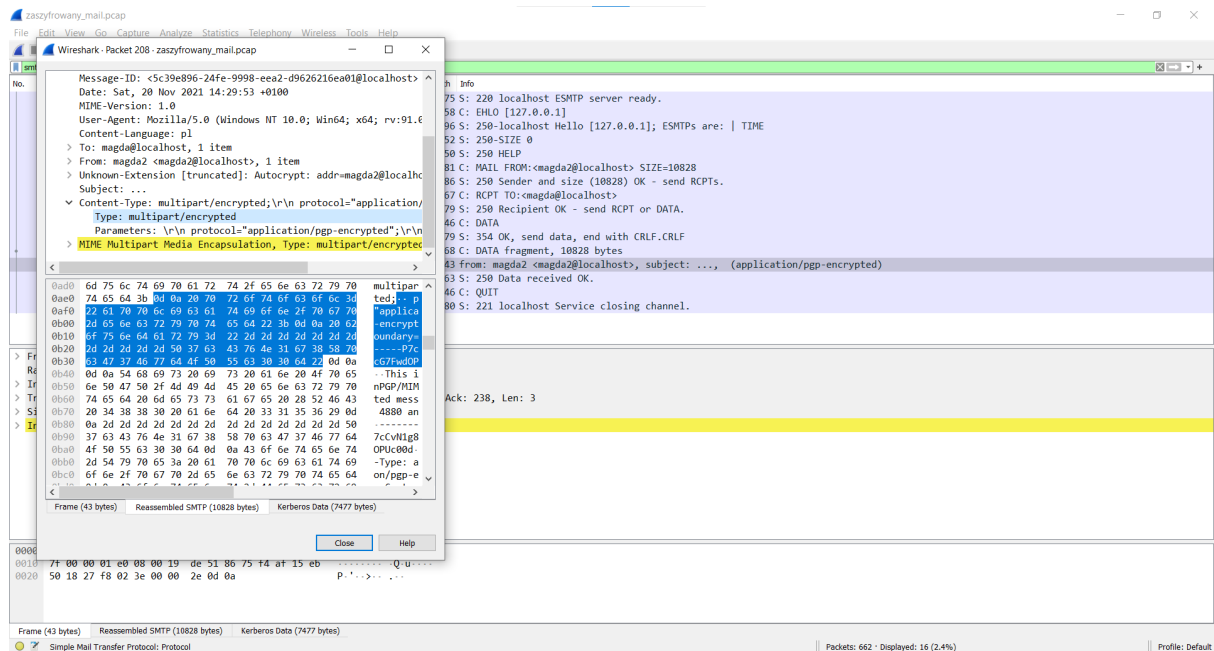


## 7. Wysłałam zaszyfowaną wiadomość



Jak można zauważyć, wiadomość została dostarczona jako zaszyfrowana.

8. Przeprowadziłam analizę pakietów zaszyfrowanej wiadomości w narzędziu Wireshark wybierając odpowiedni pakiet.



Jak widać, po zaszyfrowaniu wiadomości nie można już odczytać żadnych informacji typu jej treść czy tytuł - tak jak to miało miejsce przy wiadomości nieszyfrowanej. Ponadto, w nagłówku znajduje się komunikat, że wiadomość została zaszyfrowana.

# Wnioski

W pierwszej części zadania głównym wnioskiem, który wyraźnie widać po analizie pakietów narzędziem Wireshark jest bezproblemowe odczytanie przechwyconych informacji ze strony, która nie jest zabezpieczona certyfikatem SSL. Mamy możliwość podejrzenia szczegółowo wszystkich danych, jaki użytkownik przesłał odwiedzając daną witrynę przed zabezpieczeniem jej certyfikatem.

W odróżnieniu od powyższej, strona zabezpieczona certyfikatem SSL nie daje już takich możliwości. Narzędzie Wireshark widzi w przesyłanych pakietach jedynie zaszyfrowane dane. Poza informacją, że dane są zaszyfrowane, nie możemy nic więcej wyczytać.

W drugiej części zadania przekonujemy się, że narzędzie Wireshark jest w stanie przechwycić informacje przesyłane w wiadomości elektronicznej gdy nie jest ona zaszyfrowana. Po zaszyfrowaniu wiadomości kluczem PGP, wykorzystując ponownie Wireshark, nie możemy już nic odczytać z tak przesłanej wiadomości. Osoba nasłuchująca nie uzyska żadnych informacji bez odpowiedniego klucza.

Główna konkluzja tego ćwiczenia jest taka, że konieczne jest zabezpieczanie witryn, na których występują jakiekolwiek wrażliwe dane, które osoba niepowołana mogłaby przechwycić. Wysyłając bądź odbierając pocztę elektroniczną to obostrzenie jest równie ważne bo zabezpiecza nas przed wyciekiem informacji.