

**WYŻSZA SZKOŁA HANDLOWA
W RADOMIU**



**RADOM
ACADEMY OF ECONOMICS**

Wydział Studiów Strategicznych i Technicznych

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

LABORATORIUM NR 1 PODSTAWY KRYPTOGRAFII

Prowadzący: dr Piotr Dobosz

Zespół laboratoryjny:

Magdalena Szafrńska, nr albumu: 18345

Spis treści

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

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)

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

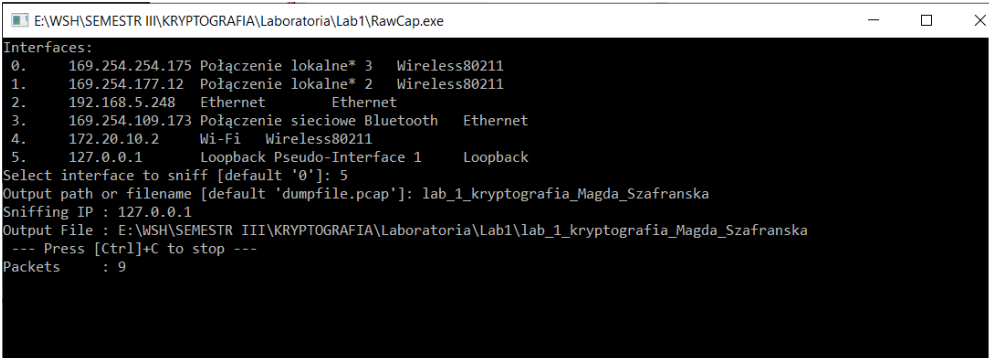
stron WWW, które nie posiadają klucza SSL. W tym celu można stworzyć prostą stronę formularza (HTML + PHP), uruchomić na serwerze stron WWW (np. na narzędziu XAMPP bądź na jakimkolwiek serwerze WWW - ja użyję Laragon) i spróbować kilkakrotnie wysłać informacje przez formularz.

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 wysłamy ją do kogoś innego (np. przez pomyłkę).

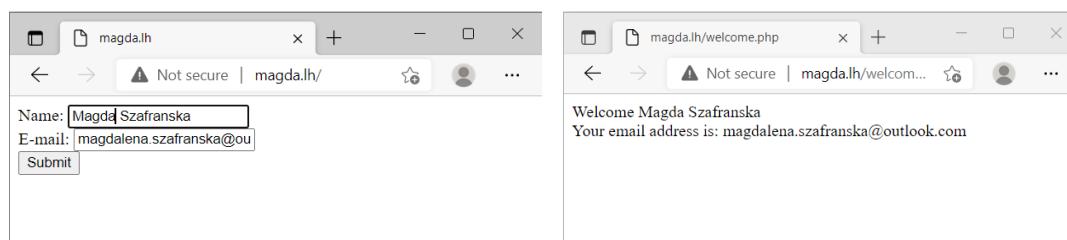
CZĘŚĆ I: Badanie ruchu sieci na stronie internetowej

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

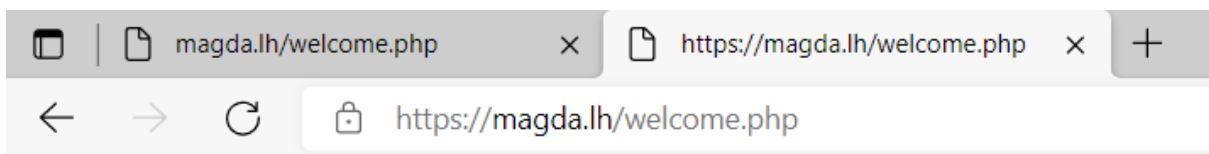
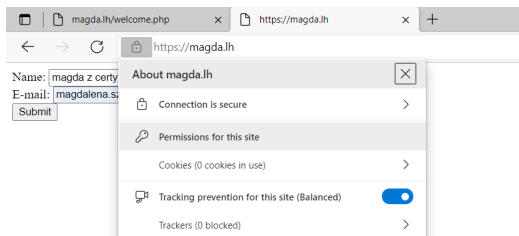
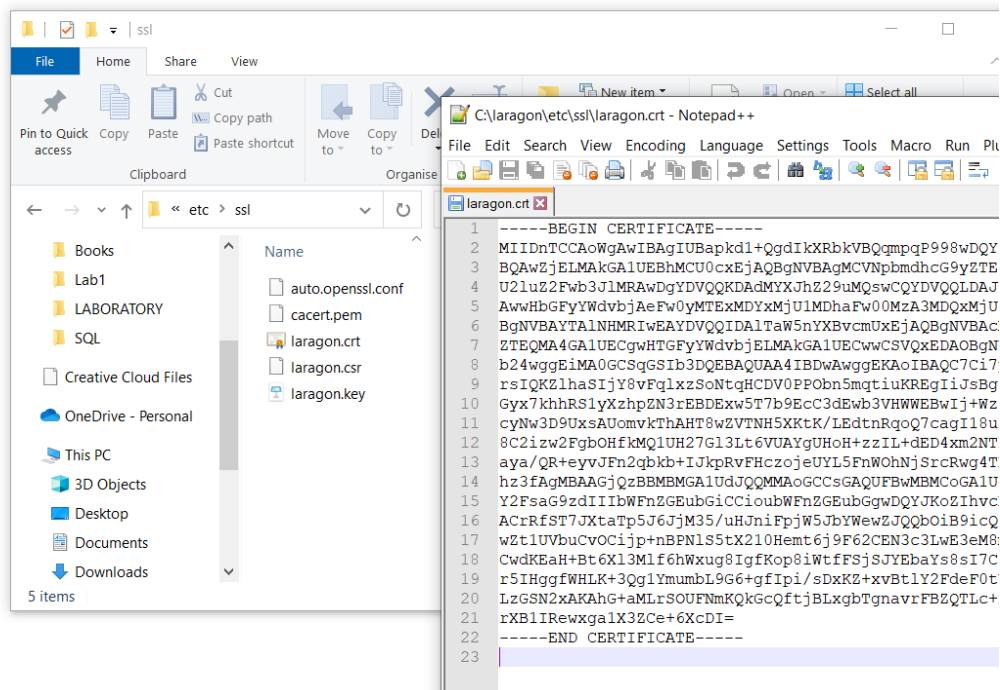
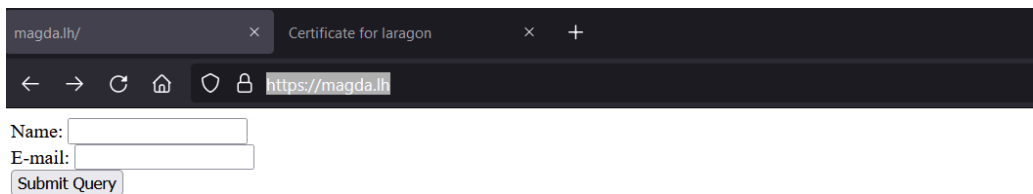


```
E:\WSH\SEMESTR III\KRYPTOGRAFIA\Laboratoria\Lab1\RawCap.exe
Interfaces:
0. 169.254.254.175 Połączenie lokalne* 3 Wireless80211
1. 169.254.177.12 Połączenie lokalne* 2 Wireless80211
2. 192.168.5.248 Ethernet Ethernet
3. 169.254.109.173 Połączenie sieciowe Bluetooth Ethernet
4. 172.20.10.2 Wi-Fi Wireless80211
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.

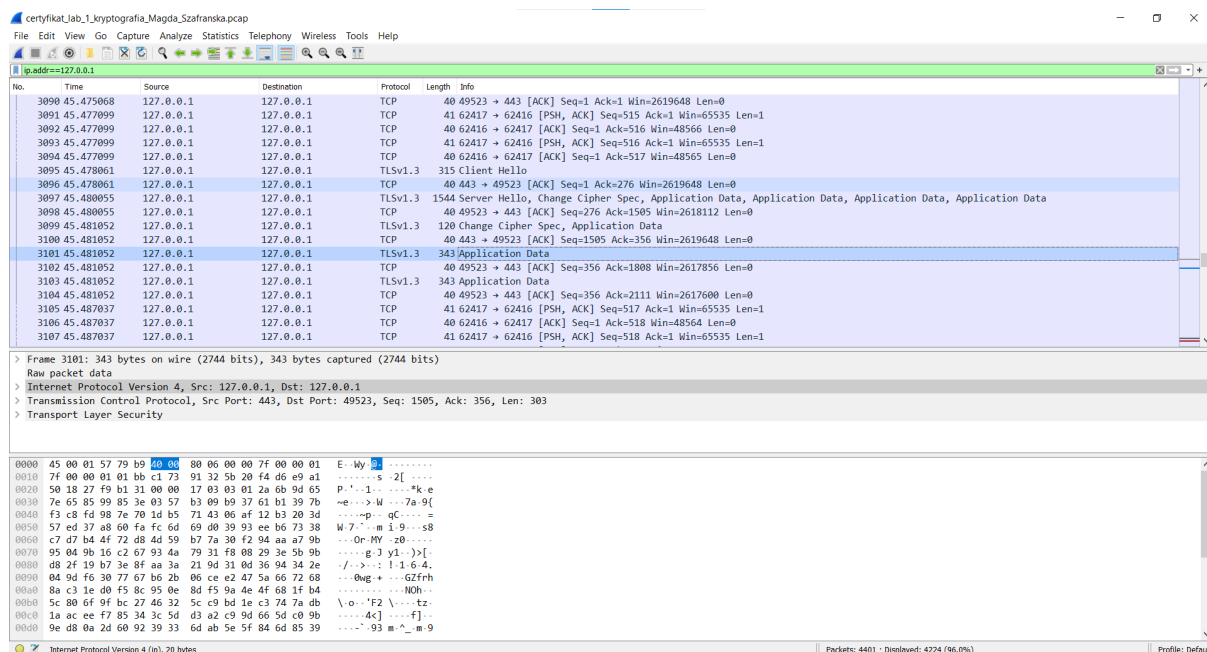


Welcome magda z certyfikatem
Your email address is: magdalena.szafranska@outlook.com

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
```

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

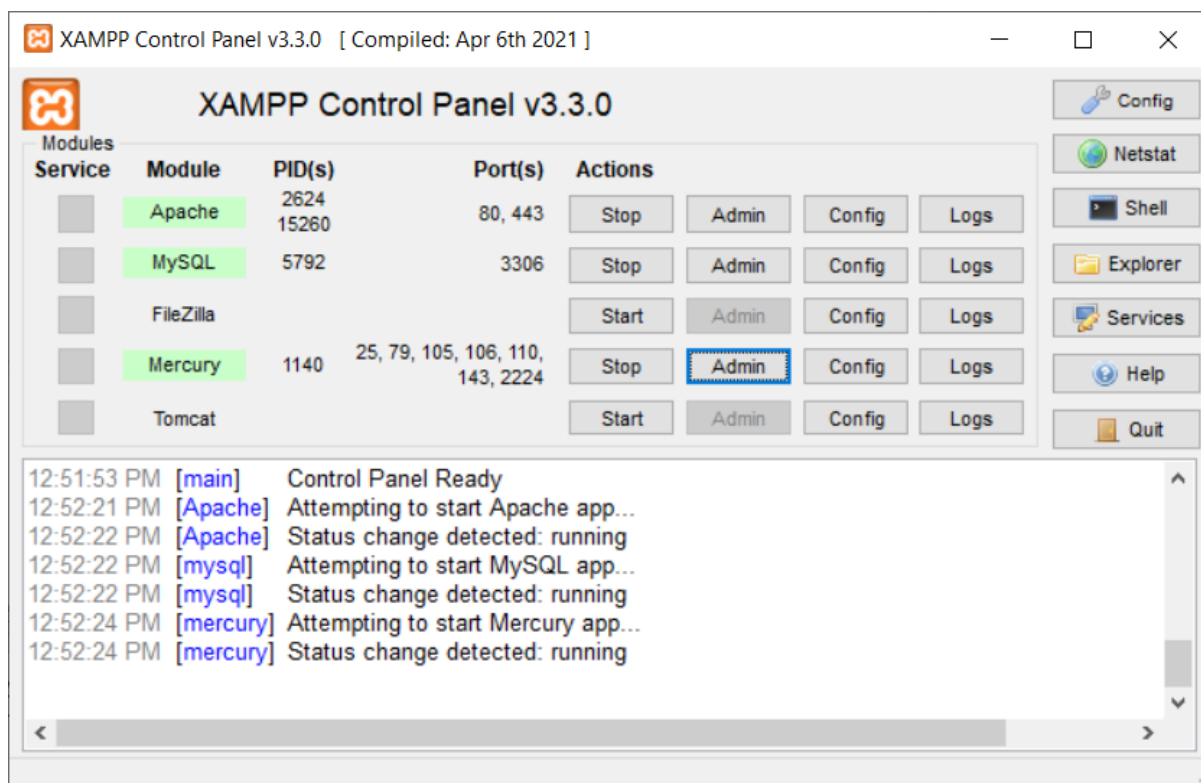


8. Przeanalizowałam wysłany pakiet. Jak widać przesłane w formularzu na zabezpieczonej stronie dane zostały zaszyfrowane. Nie da się ich odczytać w sposób jawny tak, jak działa się w przypadku wysłania formularza na stronie internetowej niezabezpieczonej certyfikatem SSL

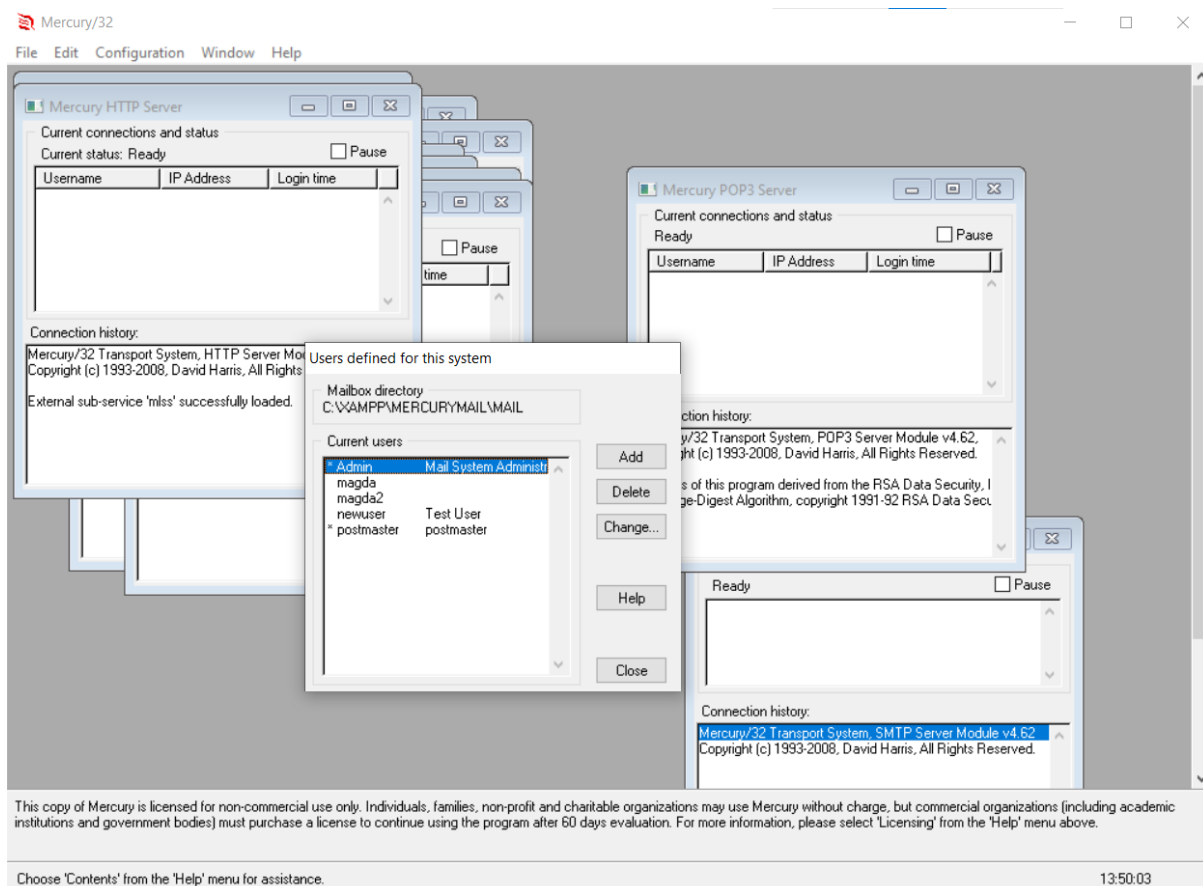
CZĘŚĆ II: Testowanie wysyłania wiadomości elektronicznej

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

1. 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

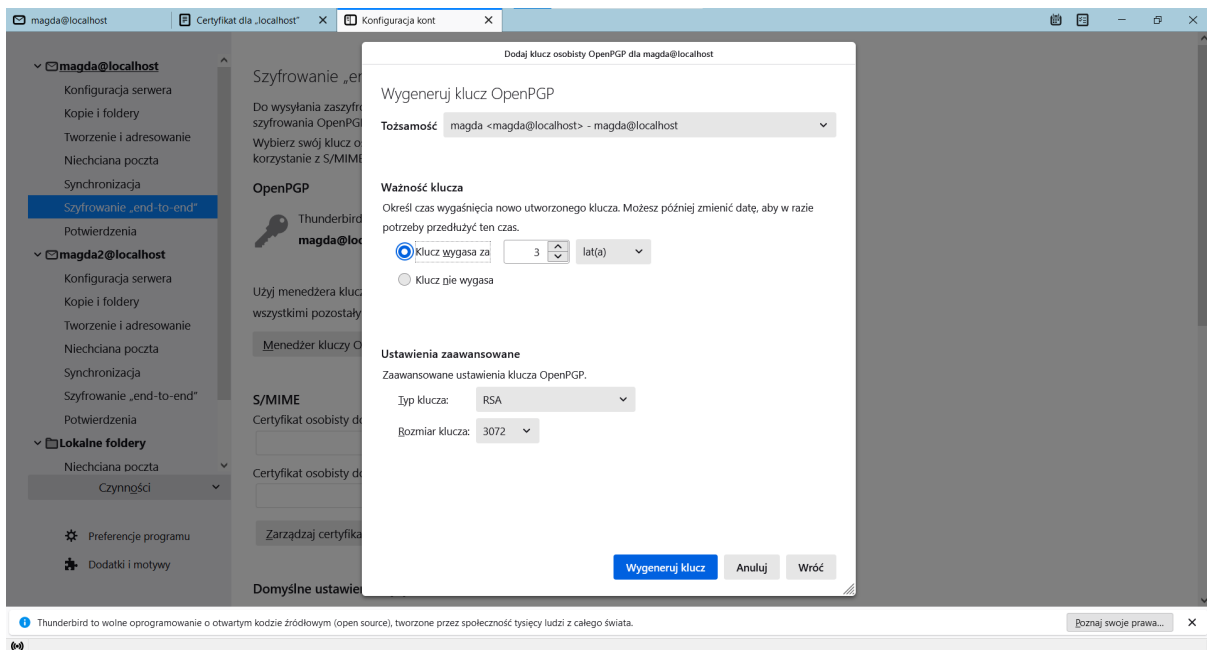
5. Przeanalizowałam w programie Wireshark ruch na serwerze SMTP przechwytyjąc wysłaną wiadomość i wybierając dany pakiet do analizy.

The screenshot displays the Wireshark interface with the following components:

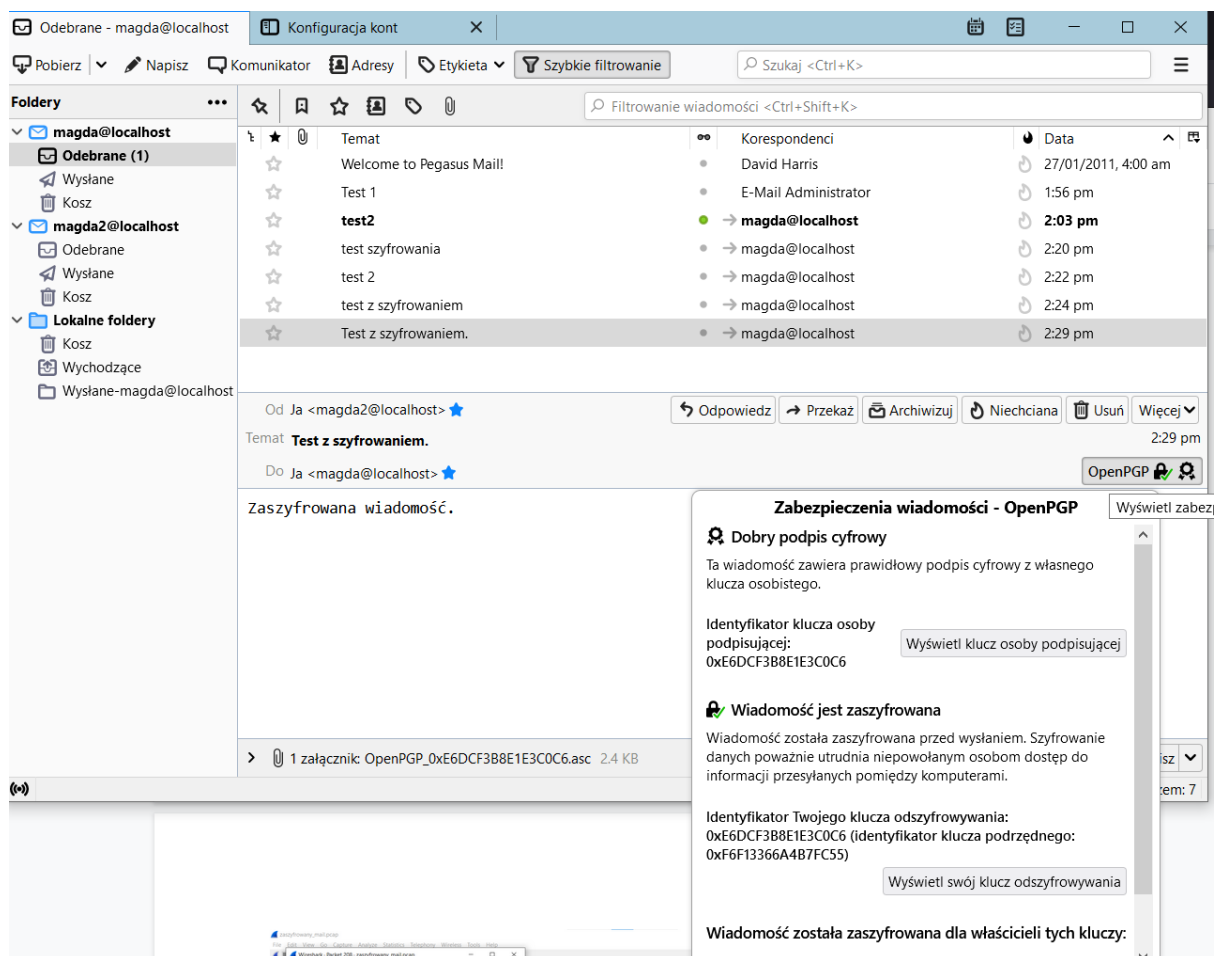
- Packet List:** Shows a series of SMTP packets. Packet 328 is highlighted, representing the final message transmission.
- Packet Details:** For packet 328, it shows the 'Internet Message Format' structure:
 - Message-ID: <94f02cb0-63b3-977e-d084-690300babb8f@localhost>
 - Date: Sat, 20 Nov 2021 14:02:10 +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)
- Raw Packet Data:** Shows the hexadecimal and ASCII representation of the captured data for the selected packet.

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

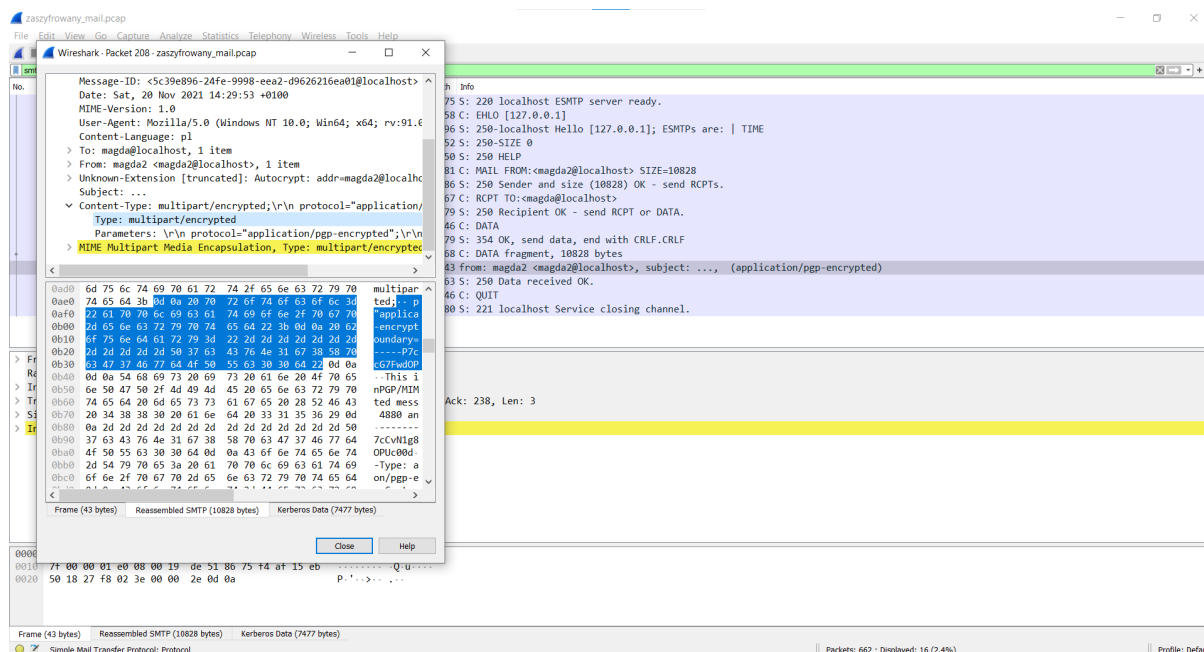


7. Wysłałam zaszyfowaną wiadomość



Jak można zauważyć, wiadomość została dostarczona jako zaszyfrowana.

- 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.