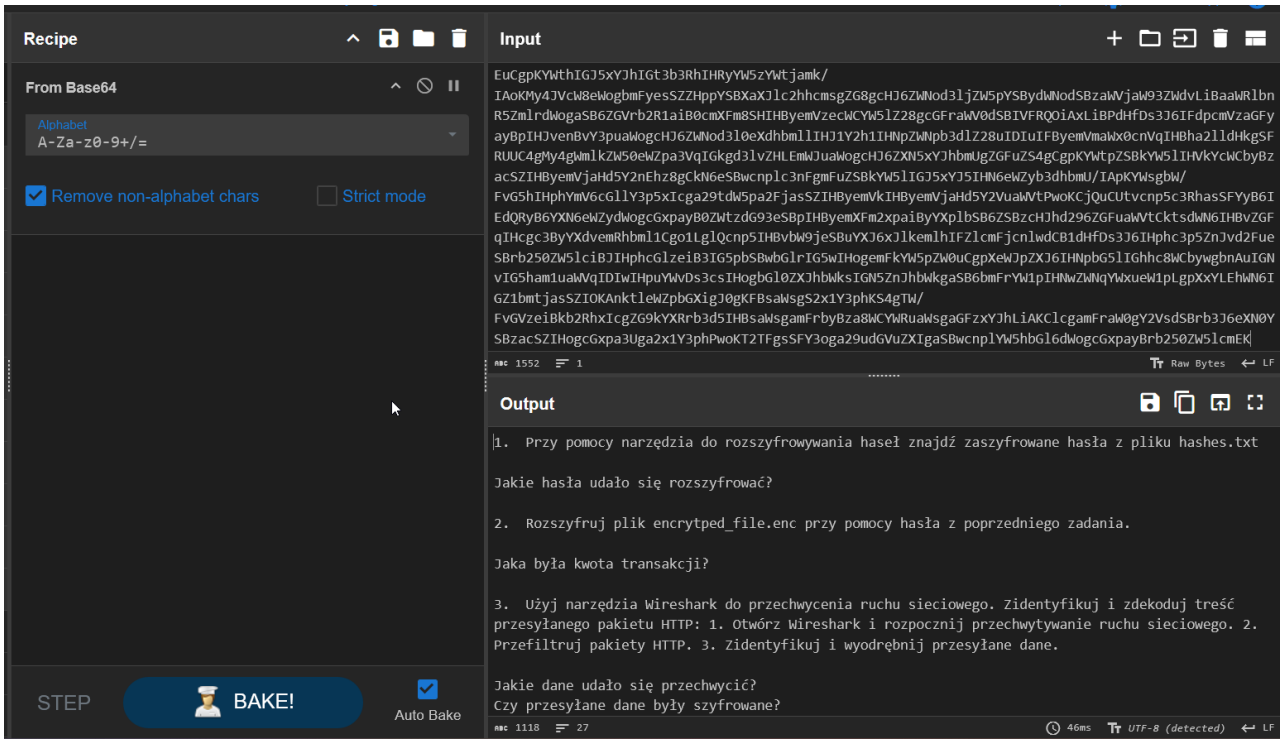
POLITECHNIKA WROCŁAWSKA  Wydział Informatyki i Telekomunikacji	Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30
CBESI0053G Informatyka śledcza – Laboratorium 3	
Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: 17.03.2025	
Data oddania sprawozdania: 23.03.2025	

1. Cel ćwiczenia

Szyfrowanie i deszyfrowanie plików oraz analiza ruchu sieciowego.

2. Odszyfrowanie instrukcji laboratoryjnej



Rysunek 1: Odszyfrowanie instrukcji za pomocą narzędzia CyberChef

Treść instrukcji:

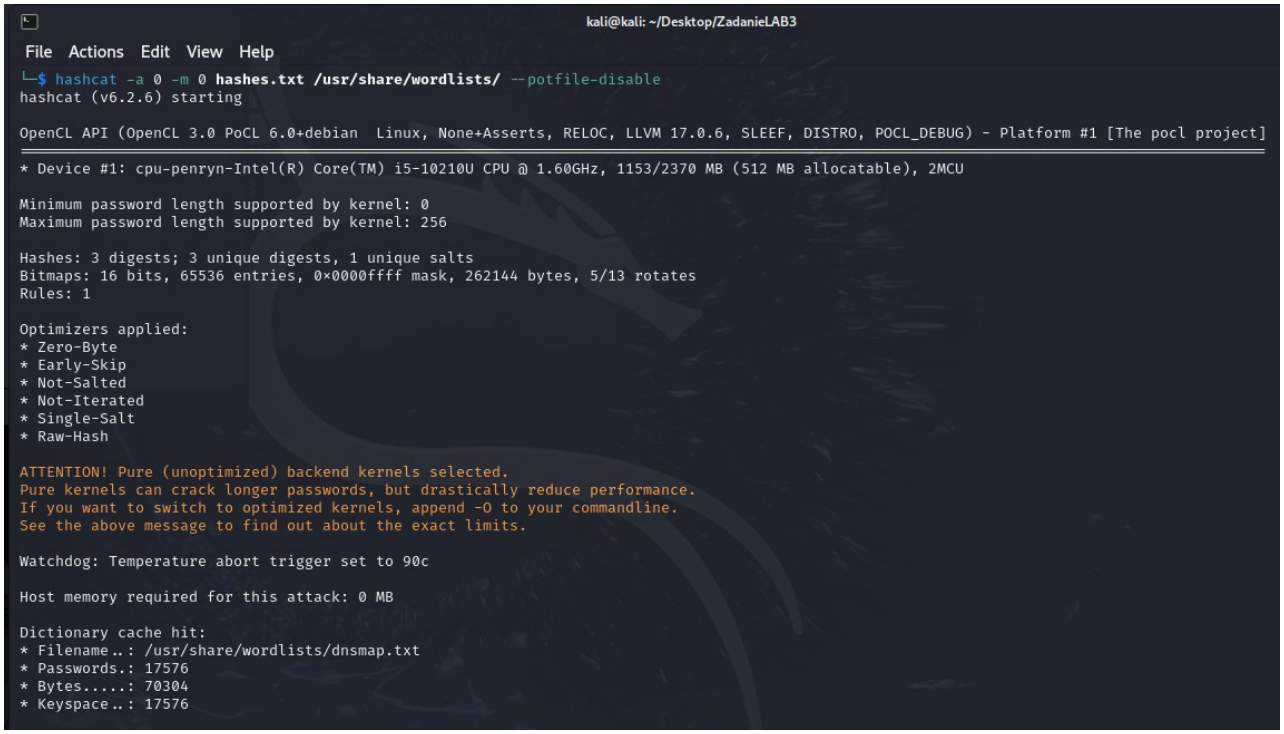
```
1.      Przy pomocy narzędzia do rozszyfrowywania haseł znajdź zaszyfrowane hasła z pliku
hashes.txt

Jakie hasła udało się rozszyfrować?

2.      Rozszyfruj plik encrytped_file.enc przy pomocy hasła z poprzedniego zadania.

Jaka była kwota transakcji?

3.      Użyj narzędzia Wireshark do przechwycenia ruchu sieciowego. Zidentyfikuj i zdekoduj
treść przesyłanego pakietu HTTP: 1. Otwórz Wireshark i rozpocznij przechwytywanie ruchu
sieciowego. 2. Przefiltruj pakiety HTTP. 3. Zidentyfikuj i wyodrębnij przesyłane dane.

Jakie dane udało się przechwycić?
Czy przesyłane dane były szyfrowane?
Jak można zabezpieczyć komunikację przed przechwyceniem?


4.      Korzystając z GPG zaszyfruj plik tekstowy i prześlij razem ze sprawozdaniem
Klucz podaj w sprawozdaniu

5.      Przy pomocy narzędzia Veracrypt utwórz zaszyfrowany kontener I zapisz w nim plik np
z zadaniem.

Wybierz silne hasło, np. co najmniej 20 znaków, z literami, cyframi i znakami specjalnymi.
Włącz funkcję „Keyfile” (Plik Klucza). Możesz dodać dodatkowy plik jako składnik hasła.

W jakim celu korzysta się z pliku klucza?

Odłącz kontener i przeanalizuj plik kontenera
```

Rysunek 2: odkodowana treść instrukcji

3. Realizacja zadań

Zadanie 1. Przy pomocy narzędzia do rozszyfrowywania haseł znajdź zaszyfrowane hasła z pliku hashes.txt

Hipoteza: hashe w pliku hashes.txt mają po 32 znaki, więc najprawdopodobniej są hashami MD5.



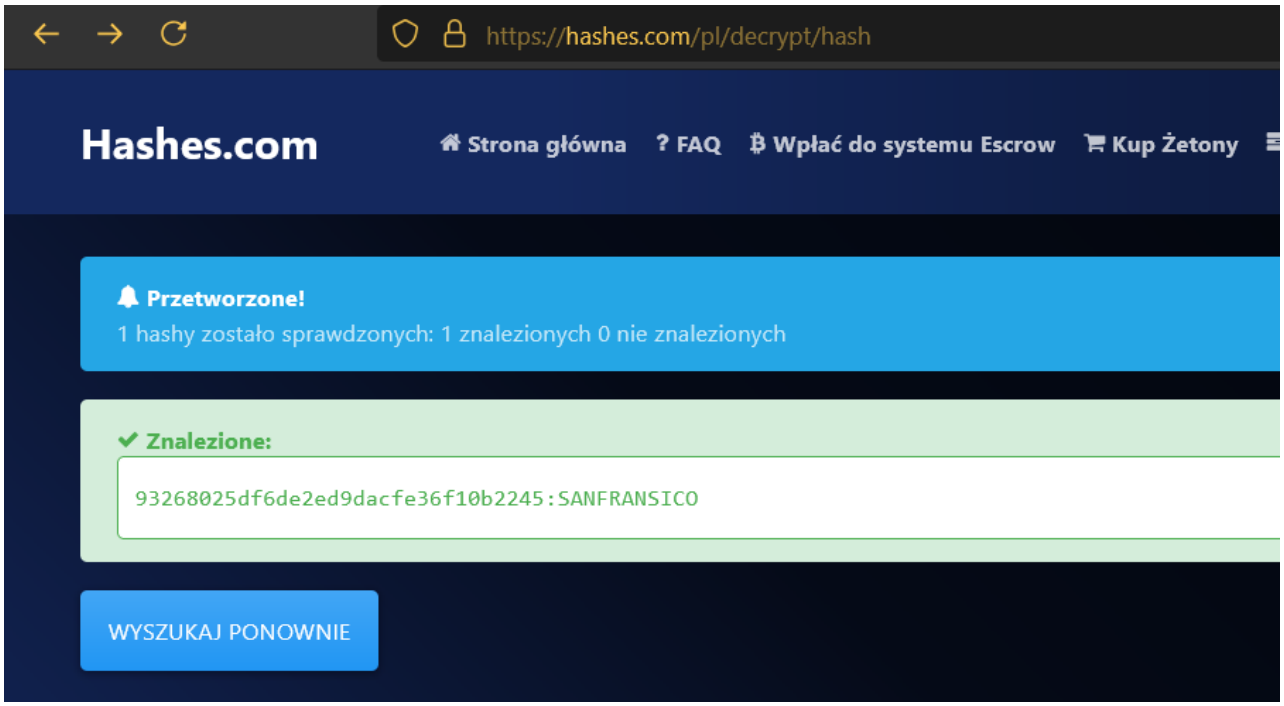
Rysunek 3: Atak słownikowy na plik hashes.txt

Atak słownikowy złamał dwa z trzech hashy w pliku:

79d8e340812f9db0bbfa508beb319dea:holiday

5cca9a53ece2fd6b499e035388db4171:rainb0ws

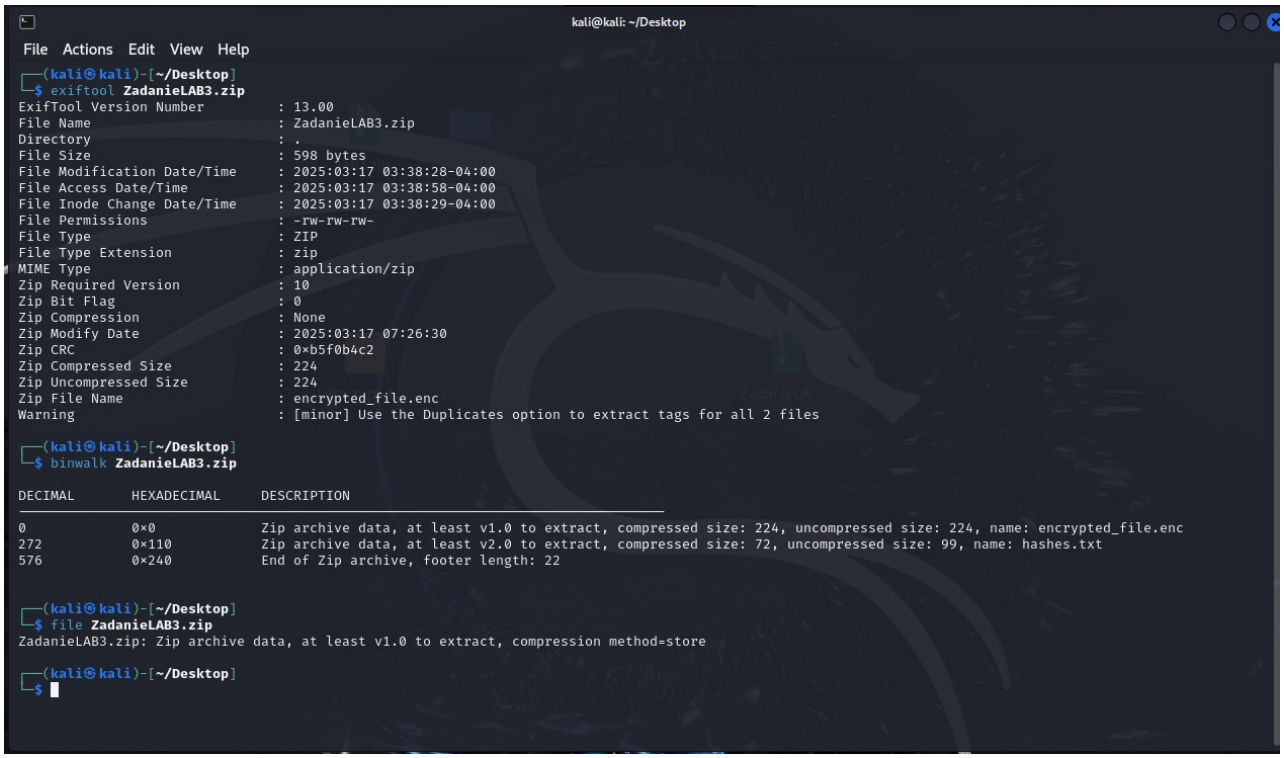
Ostatni hash został odkryty za pomocą narzędzia https://hashes.com/pl/decrypt/hash



Rysunek 4: Przeszukanie bazy hashy na hashes.com

Jakie hasła udało się rozszyfrować? – Udało się rozszyfrować hasła „holiday”, „rainb0ws”, „SANFRANCISCO”. Są to niebezpieczne hasła ponieważ są podatne na proste ataki słownikowe.

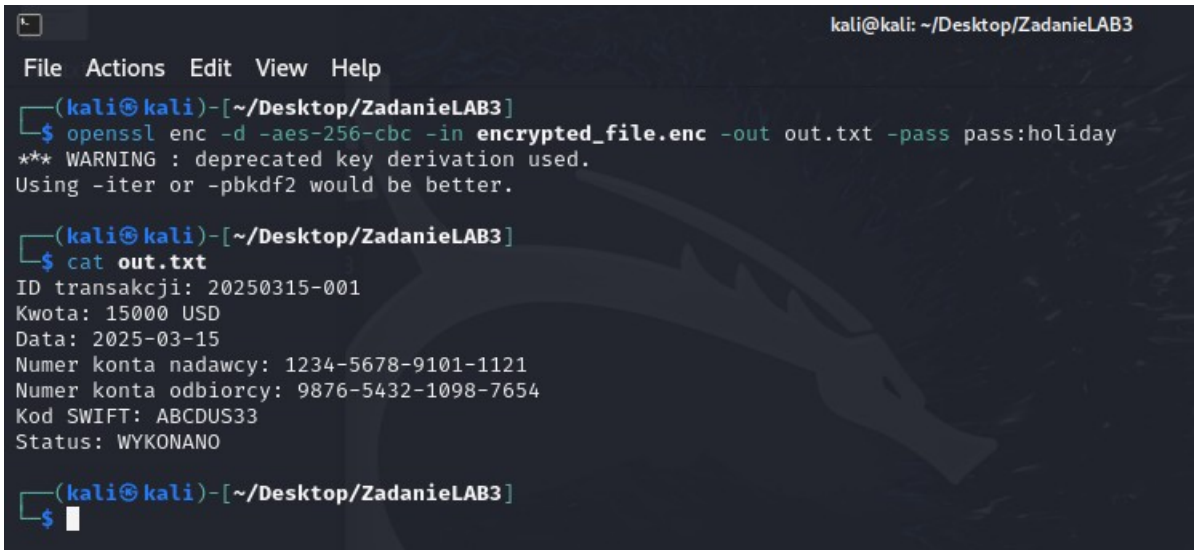
Analiza pliku przed odszyfrowaniem:



Rysunek 5: Analiza archiwum

Komentarz: Plik to archiwum zip zawierający pliki encrypted_file.enc oraz hashes.txt

Zadanie 2. Rozszyfruj plik encrytped_file.enc przy pomocy hasła z poprzedniego zadania.

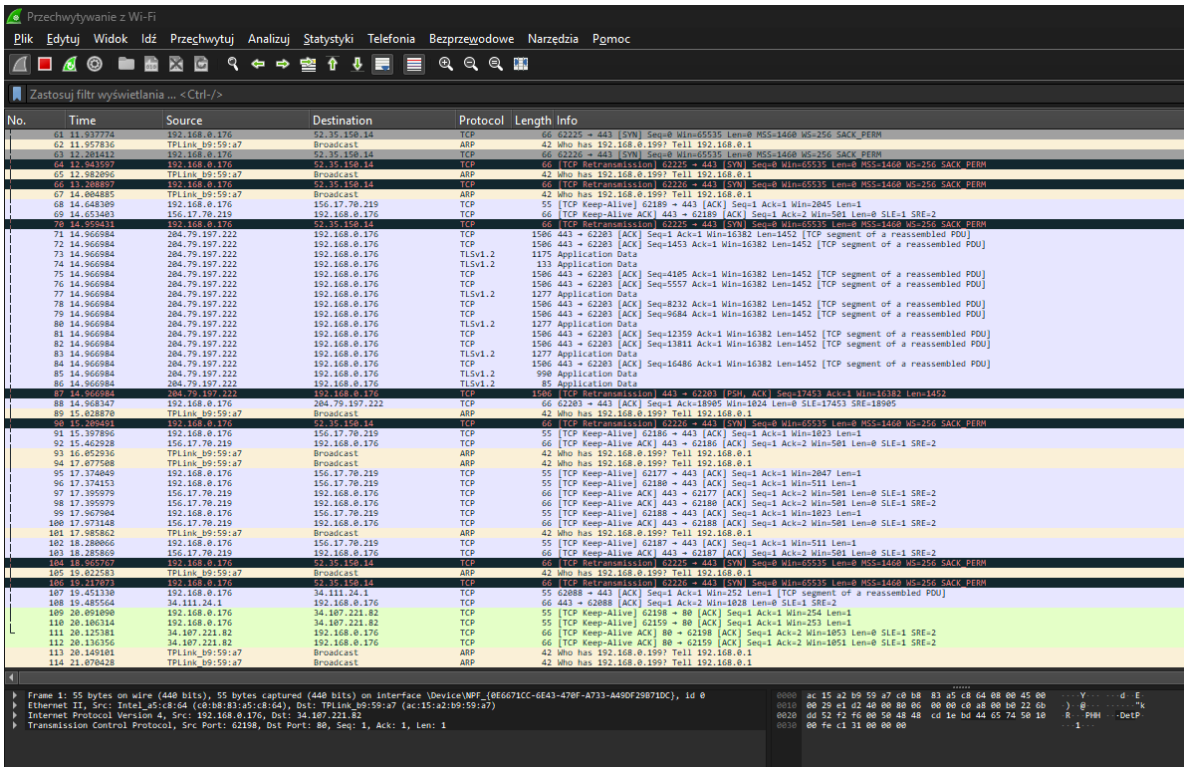


Rysunek 6: Rozszyfrowanie pliku encrypted_file.enc

Jaka była kwota transakcji? – 15000 USD

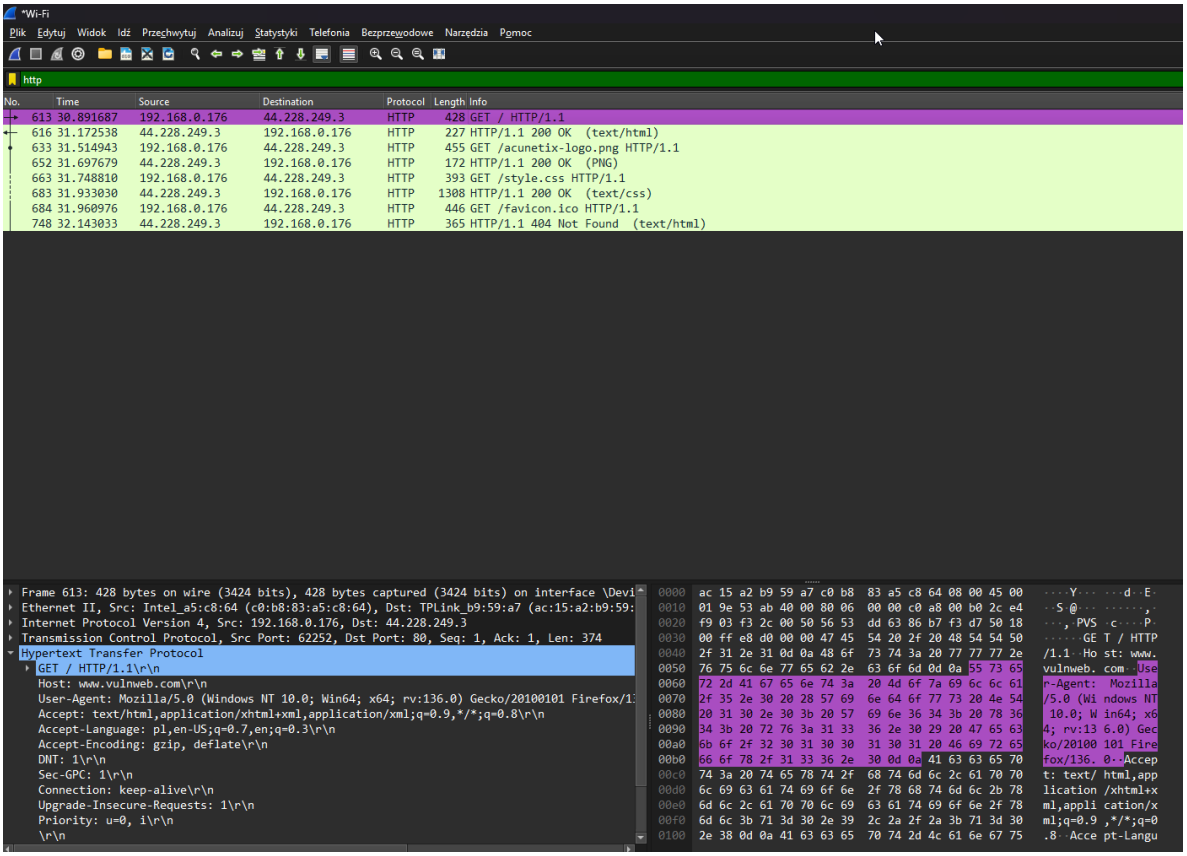
Zadanie 3. Użyj narzędzia Wireshark do przechwycenia ruchu sieciowego. Zidentyfikuj i zdekoduj treść przesyłanego pakietu HTTP:

1. Otwórz Wireshark i rozpocznij przechwytywanie ruchu sieciowego.



Rysunek 7: Rozpoczęcie przechwytywania ruchu sieciowego w programie Wireshark

2. Przefiltruj pakiety HTTP.

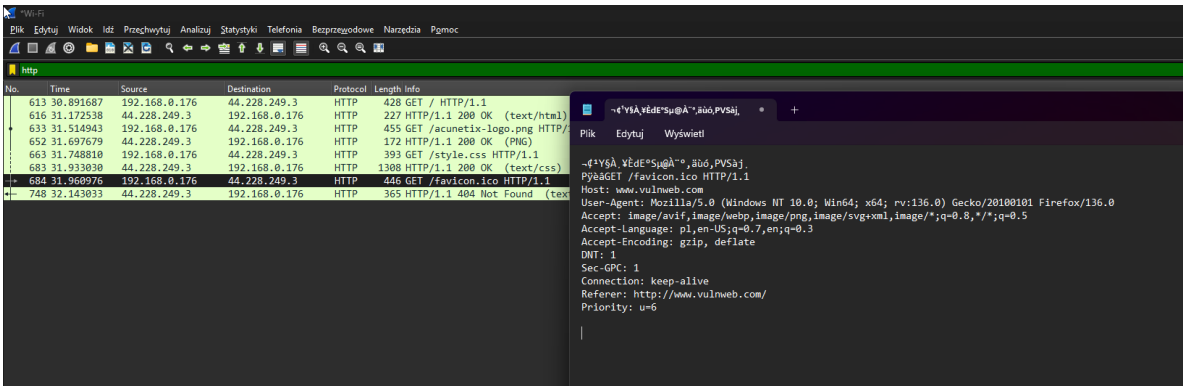


Rysunek 8: Filtrowanie pakietów http

Komentarz: Połączenie ze stroną http://www.vulnweb.com/.

3. Zidentyfikuj i wyodrębnij przesyłane dane.

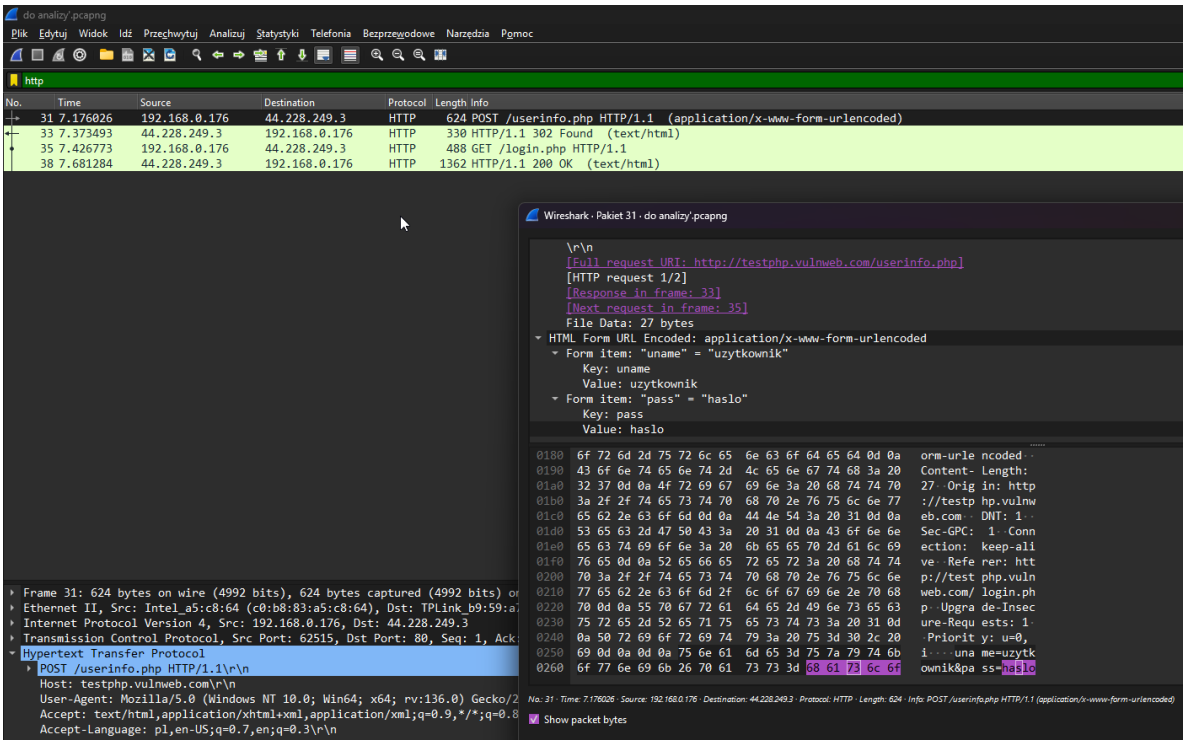
a. Strona bez logowania



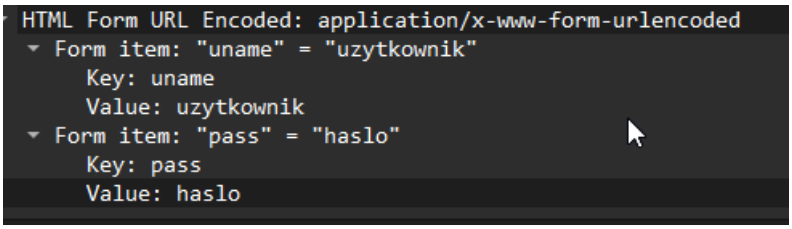
Rysunek 9: Wyodrębnienie danych z pakietu

Komentarz: W niezaszyfrowanym pakiecie HTTP można wyczytać szczegółowe informację o użytkowniku: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0 czy też typ żądania: GET /favicon.ico

b. Strona z logowaniem



Rysunek 10: Analiza pakietów przesłanych z/do strony z logowaniem



Rysunek 11: Zbliżenie rys. 9

Komentarz: W protokole HTTP nawet dane logowania nie są w żaden sposób chronione. Są dostępne w tekście jawnym jak widać na rys 9.

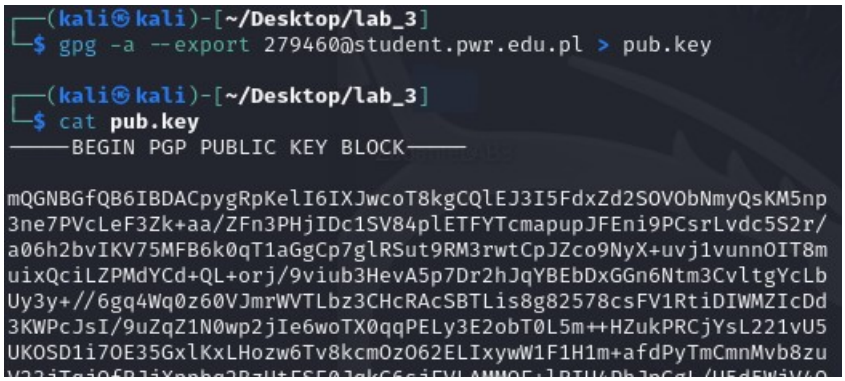
Jakie dane udało się przechwycić? - Np. dane logowania.

Czy przesyłane dane były szyfrowane? – Nie.

Jak można zabezpieczyć komunikację przed przechwyceniem? – Korzystać z protokołu HTTPS.

Zadanie 4. Korzystając z GPG zaszyfruj plik tekstowy i prześlij razem ze sprawozdaniem. Klucz podaj w sprawozdaniu

Rysunek 12: Szyfrowanie za pomocą klucza prywatnego (podpisanie)

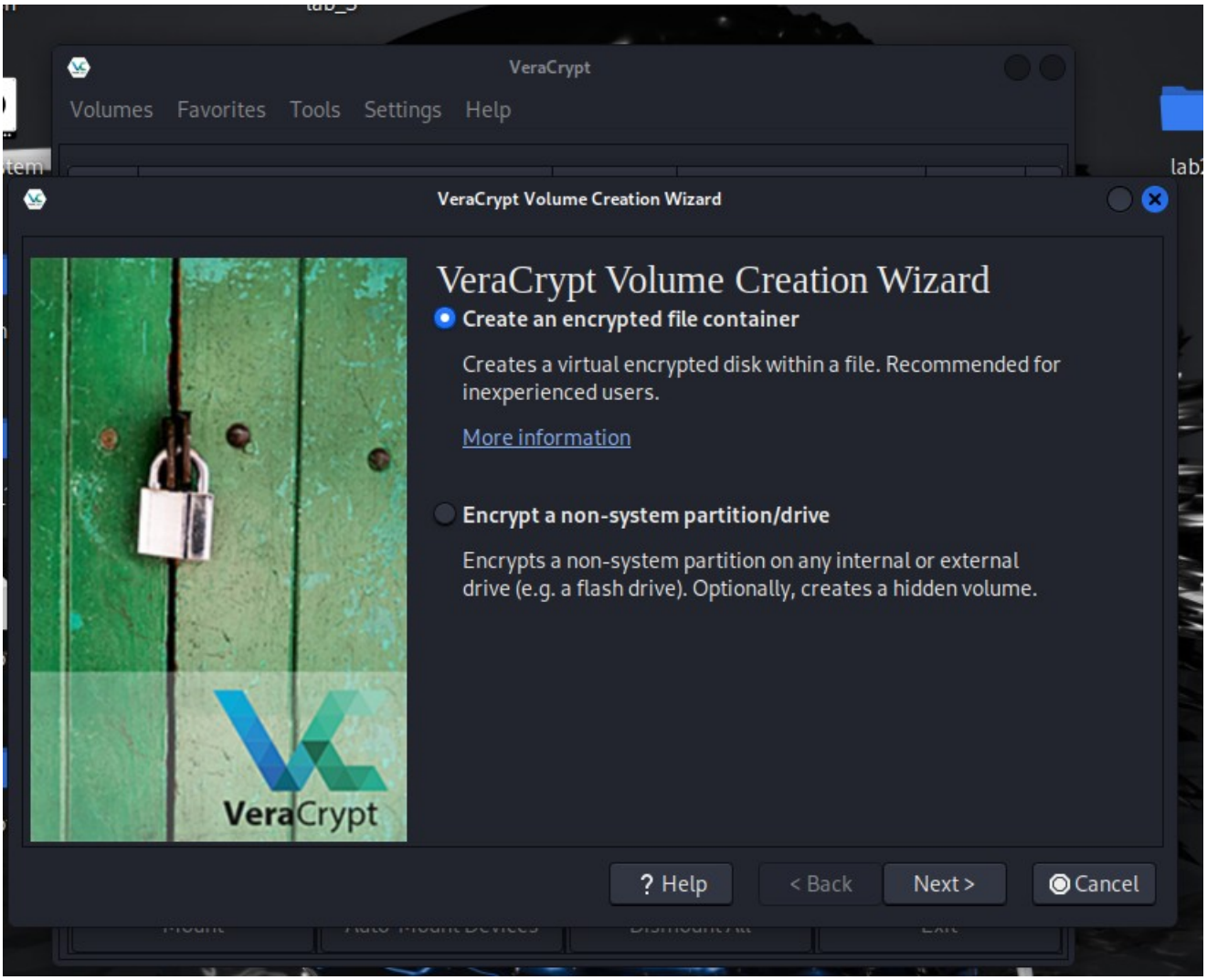


Rysunek 13: Eksport klucza publicznego

Komentarz: Klucz dołączony do sprawozdania

Zadanie 5. Przy pomocy narzędzia Veracrypt utwórz zaszyfrowany kontener i zapisz w nim plik np z zadaniem.

Wybierz silne hasło, np. co najmniej 20 znaków, z literami, cyframi i znakami specjalnymi.
Włącz funkcję „Keyfile” (Plik Klucza). Możesz dodać dodatkowy plik jako składnik hasła.
W jakim celu korzysta się z pliku klucza?
Odłącz kontener i przeanalizuj plik kontenera

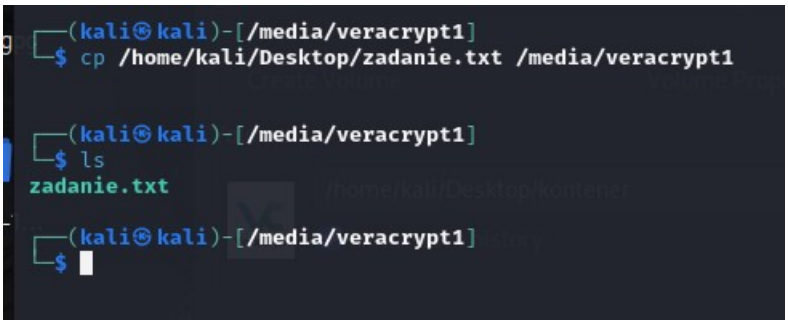


Rysunek 14: Tworzenie kontenera

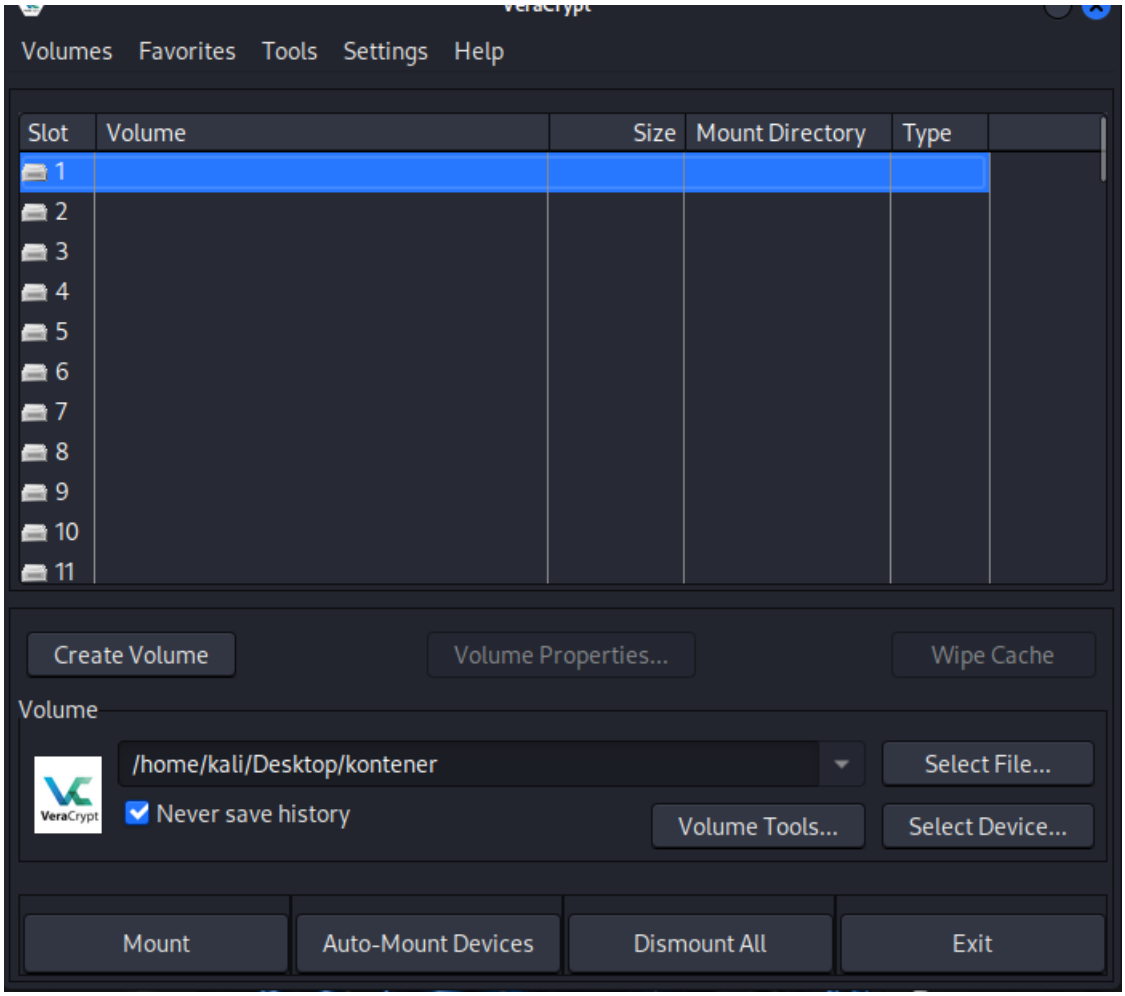
Rysunek 15: Ustawianie silnego hasła

Dodatkowo została zaznaczona opcja use keyfiles gdzie wybrany został plik tekstowy z pulpitu.

Po utworzeniu kontenera utworzył się jego plik, który przy użyciu VeraCrypt został zamontowany na pulpicie. Wymagało to podania hasła oraz odpowiedniego pliku tekstowego.

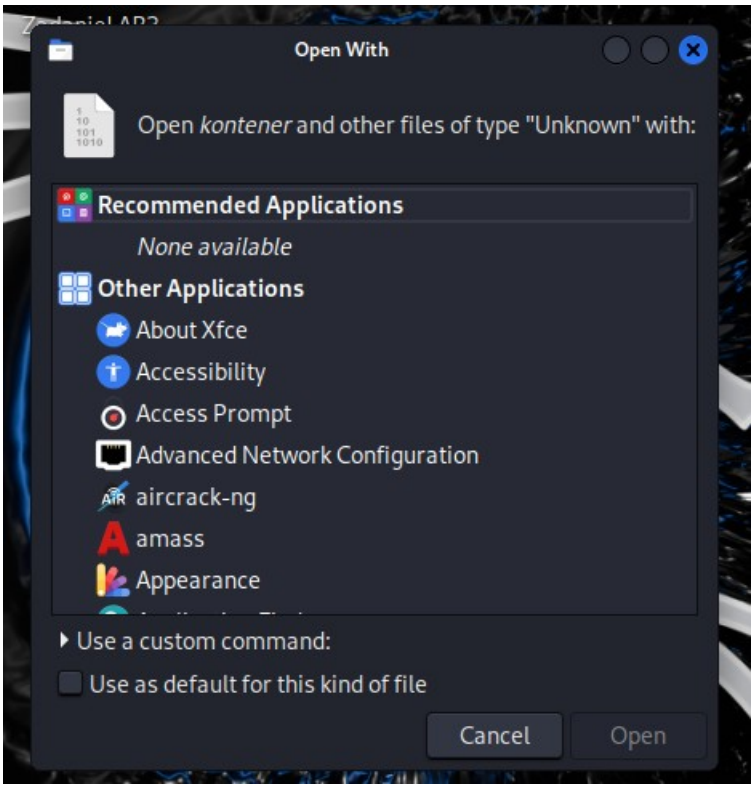


Rysunek 16: zapisanie pliku do kontenera

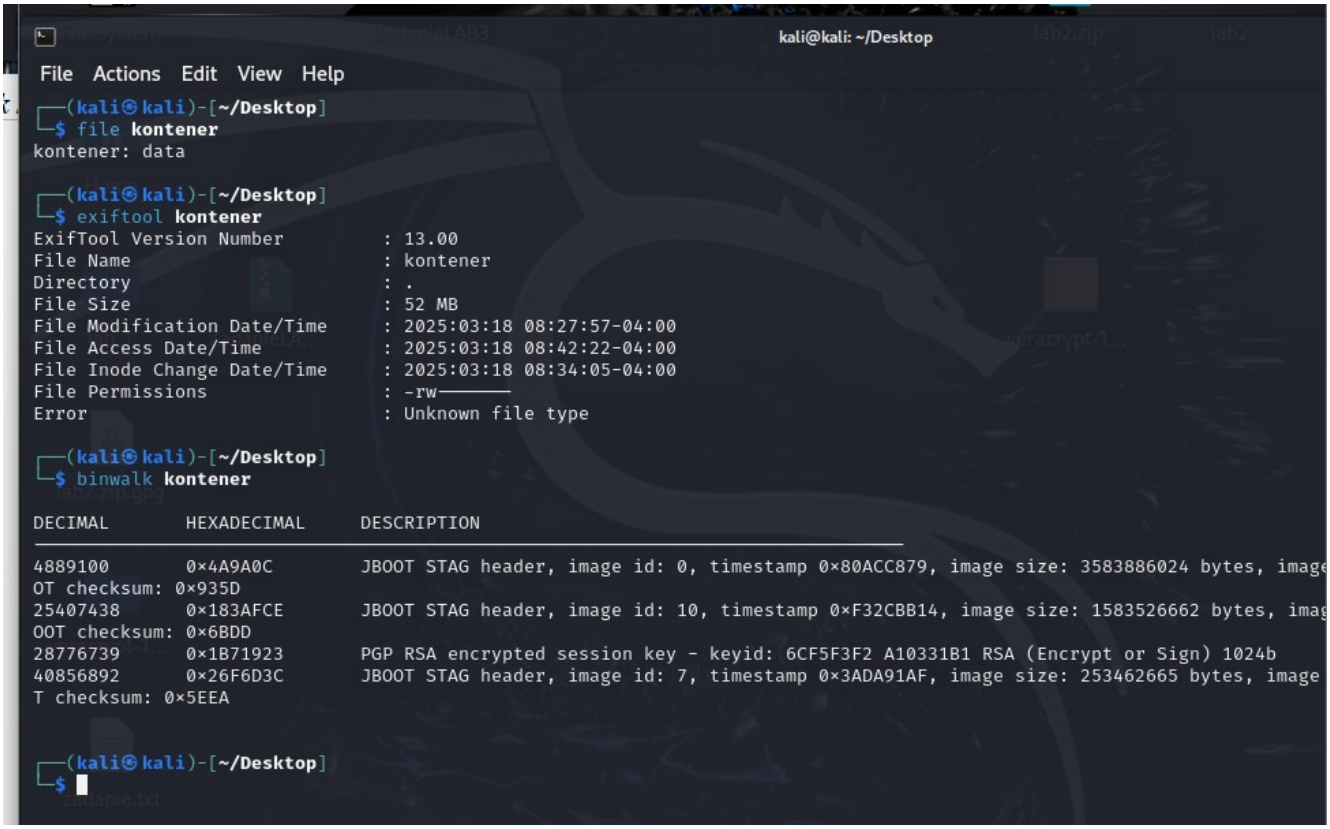


Rysunek 17: Odmontowanie kontenera

Po odmontowaniu kontenera pozostaje tylko jego plik, niezrozumiały dla zwykłego systemu operacyjnego. Dostęp do plików zapisanych na kontenerze byłby możliwy tylko dzięki ponownym podaniu hasła i odpowiednich plików w aplikacji VeraCrypt.



Rysunek 18: plik kontenera



Rysunek 19: analiza pliku kontenera

W jakim celu korzysta się z pliku klucza? – zwiększenie bezpieczeństwa poprzez wymaganie dodatkowego pliku poza hasłem.

4. Opis wykonanej pracy przez autora