

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Кафедра: Цифрових Технологій в Енергетиці
Освітньо-професійна програма: «Цифрові технології в енергетиці»

Клієнт-серверний додаток моніторингу мережевого трафіку домашньої мережі

Презентація здобувача ступеня бакалавра,
студента групи ТР-12 Ковальова Олександра

Дипломний керівник: асистент, Кардашов Олександр Вадимович

Актуальність

- Оцінка завантаженості мережі
- Розмежування трафіку за типами застосунків
- Ручне виявлення аномалій



Мета:

Створити систему для моніторингу трафіку на обмежених за апаратними ресурсами маршрутизаторах із інтуїтивно зрозумілим інтерфейсом.

Система повинна вміти розрізняти трафік за застосунками, протоколами.

No.	Time	Source	Destination	Protocol	Length	Info
25	1.556532	216.34.181.45	172.16.11.12	TCP	1514	80 → 64581 [ACK] Seq=5793 Ack=470 Win=4832 Len=1448 T
26	1.556579	172.16.11.12	216.34.181.45	TCP	66	64581 → 80 [ACK] Seq=470 Ack=7241 Win=524176 Len=0 TS
27	1.571026	216.34.181.45	172.16.11.12	TCP	1514	80 → 64581 [ACK] Seq=7241 Ack=470 Win=4832 Len=1448 T
28	1.584432	172.16.11.12	216.34.181.45	TCP	66	64581 → 80 [ACK] Seq=470 Ack=8689 Win=524280 Len=0 TS
29	1.588048	216.34.181.45	172.16.11.12	TCP	1514	80 → 64581 [ACK] Seq=8689 Ack=470 Win=4832 Len=1448 T
30	1.602563	216.34.181.45	172.16.11.12	TCP	1514	80 → 64581 [ACK] Seq=10137 Ack=470 Win=4832 Len=1448
31	1.602646	172.16.11.12	216.34.181.45	TCP	66	64581 → 80 [ACK] Seq=470 Ack=11585 Win=524280 Len=0 T
32	1.604883	172.16.11.12	96.17.211.172	TCP	78	64582 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8
33	1.604952	172.16.11.12	96.17.211.172	TCP	78	64583 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8
34	1.630141	216.34.181.45	172.16.11.12	TCP	1514	80 → 64581 [ACK] Seq=11585 Ack=470 Win=4832 Len=1448
35	1.630675	172.16.11.1	172.16.11.12	DNS	81	Standard query response 0x152b AAAA e872.g.akamaiedge
36	1.630700	172.16.11.12	172.16.11.1	ICMP	70	Destination unreachable (Port unreachable)
37	1.660844	96.17.211.172	172.16.11.12	TCP	74	80 → 64582 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=
38	1.660895	172.16.11.12	96.17.211.172	TCP	66	64582 → 80 [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=4
39	1.660976	172.16.11.12	96.17.211.172	HTTP	572	GET /sd/idlecore-tidied.css?T_2_5_0_300 HTTP/1.1
40	1.661793	96.17.211.172	172.16.11.12	TCP	74	80 → 64583 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=
41	1.661826	172.16.11.12	96.17.211.172	TCP	66	64583 → 80 [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=4

Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)	0000	00 1f f3 3c e1 13 f8 1e df e5 84 3a 08 00 45 00	...
Ethernet II, Src: Apple_e5:84:3a (f8:1e:df:e5:84:3a), Dst: Apple_3c	0010	00 4f de 53 40 00 40 06 47 ab ac 10 0b 0c 4a 7d	..O.S@.@.G..
Internet Protocol Version 4, Src: 172.16.11.12, Dst: 74.125.19.17	0020	13 11 fc 35 01 bb c6 d9 14 d0 c5 1e 2d bf 80 18	...5.....
Transmission Control Protocol, Src Port: 64565, Dst Port: 443, Seq:	0030	ff ff cb 8c 00 00 01 01 08 0a 1a 7d 84 2c 37 c5
Transport Layer Security	0040	58 b0 15 03 01 00 16 43 1a 88 1e fa 7a bc 22 6e	X.....C...
	0050	e6 32 7a 53 47 00 a7 5d cc 64 ea 8e 92	..2zSG...].d..

Постановка задачі

- Захоплення пакетів
- Класифікація протоколів
- Персоналізація пристроїв
- Візуалізація даних
- Оптимізація ресурсів
- Базова безпека






Результати пошуку «TP-Link» В категорії «Маршрутизатори»

Знайдено 5470 товарів Очистити всі Маршрутизатори X

За релевантністю

Всі категорії
Комп'ютери та ноутбуки
Мережеве обладнання Всі
Маршрутизатори
Комутатори
Ретранслятори Wi-Fi
Бездротові точки доступу
Мережіві адаптери
Оптичне обладнання
Підсилювачі зв'язку
Пасивне мережеве обладнання
Обладнання PON

Продавець
Rozetka +
Інші продавці

 <p>ТОП ПРОДАЖІВ</p> <p>Маршрутизатор TP-LINK Archer A64 WiFi5/ AC1200/ 1 Гбіт/с</p> <p>★★★★★ 913</p> <p>Є в наявності</p> <p>1-599 ₪</p> <p>1 399 ₪</p>	 <p>ТІЛЬКИ В ROZETKA</p> <p>Маршрутизатор TP-LINK Archer AX1800 WiFi 6/ 1 Гбіт/с/</p> <p>★★★★★ 135</p> <p>Є в наявності</p> <p>2-499 ₪</p> <p>2 199 ₪</p>	 <p>ТОП ПРОДАЖІВ</p> <p>Маршрутизатор TP-LINK Archer AX12 WiFi6/ AX1500 / 1 Гбіт/с/</p> <p>★★★★★ 171</p> <p>Є в наявності</p> <p>1-999 ₪</p> <p>1 799 ₪</p>	 <p>ТОП ПРОДАЖІВ</p> <p>Маршрутизатор TP-Link Archer C64 WiFi5/ AC1200/ 1 Гбіт/с</p> <p>★★★★★ 771</p> <p>Є в наявності</p> <p>1-599 ₪</p> <p>1 399 ₪</p>	 <p>ТОП ПРОДАЖІВ</p> <p>Маршрутизатор TP-LINK Archer C6 v4 WiFi5/ AC1200 /1 Гбіт/с/</p> <p>★★★★★ 117</p> <p>Є в наявності</p> <p>1-699 ₪</p> <p>1 499 ₪</p>
---	--	---	---	--

Device Type: WiFi Router
Brand: TP-Link
Model: Archer A6
Target: ramips
Subtarget: mt7621
Package architecture: mipsel_24kc
CPU: MediaTek MT7621DAT
CPU Cores: 2
CPU MHz: 880
Flash MB: 16
RAM MB: 128

Існуючі рішення



ntop



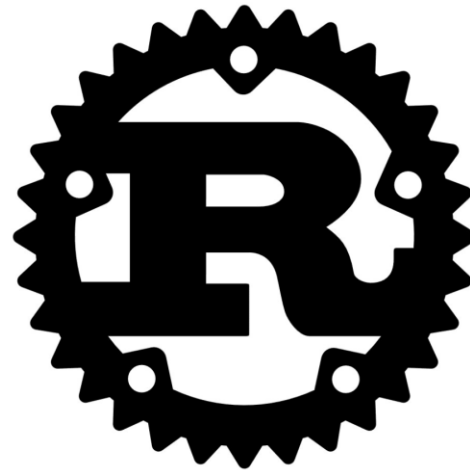
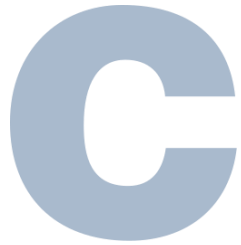
TCPDUMP & LIBPCAP



OpenSense®



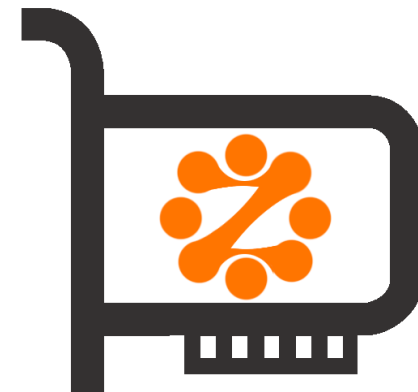
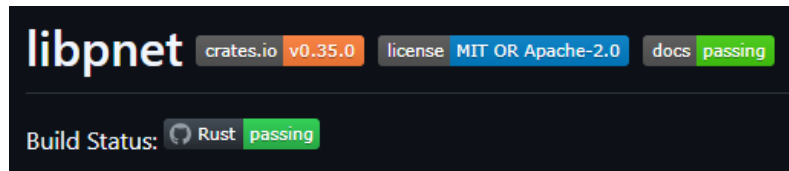
Мова програмування



**The Rust
Programming
Language**



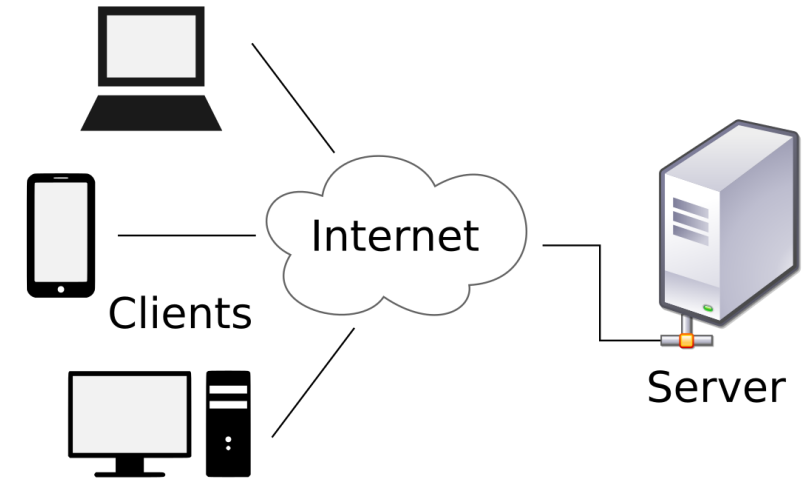
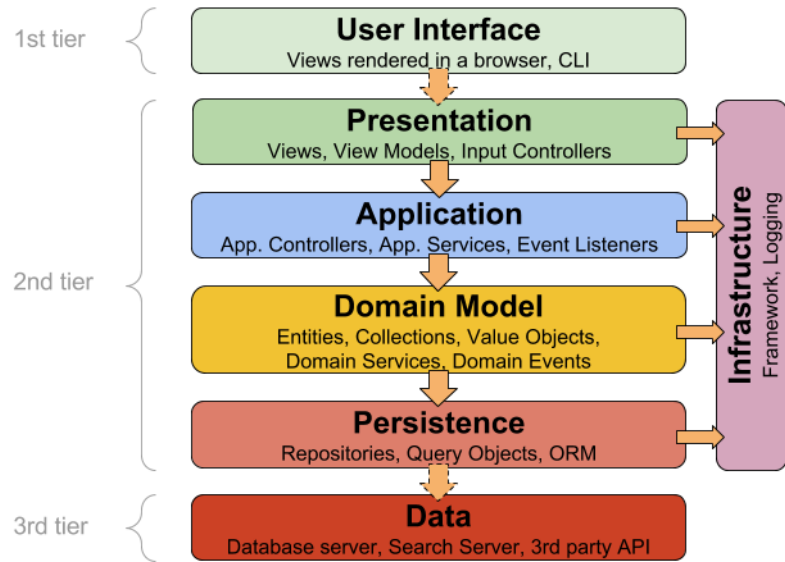
Захоплення пакетів



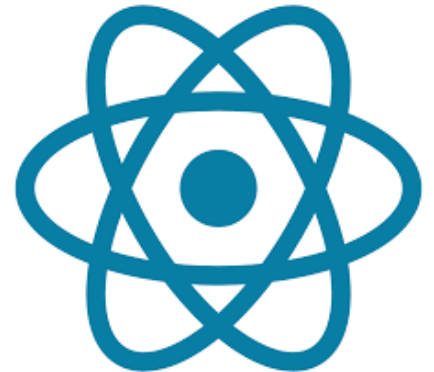
LIBPCAP



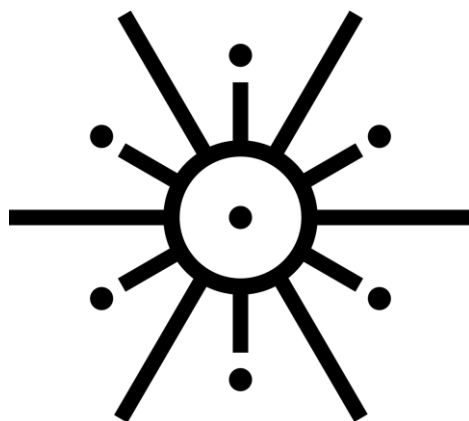
Програмна архітектура



egui



Комунікація між компонентами



Багатопотоковість

Threads

Arc

Mutex

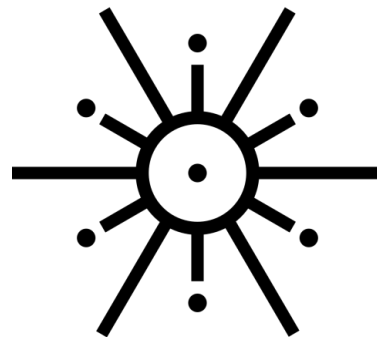
Atomics

Channels

RWLock

BroadcastChannel

Asynchronous

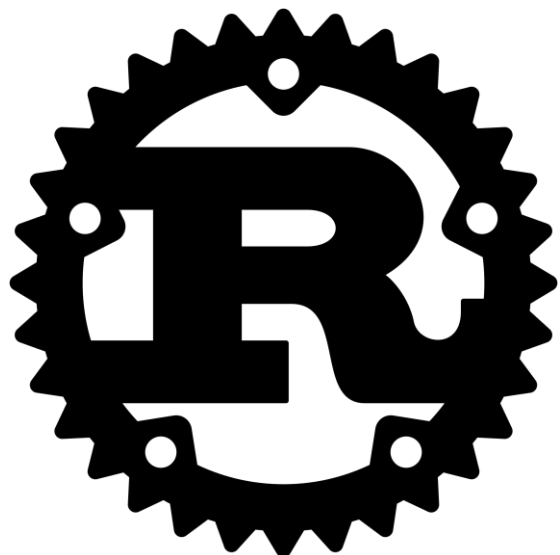


Runtime



GREEN THREADS

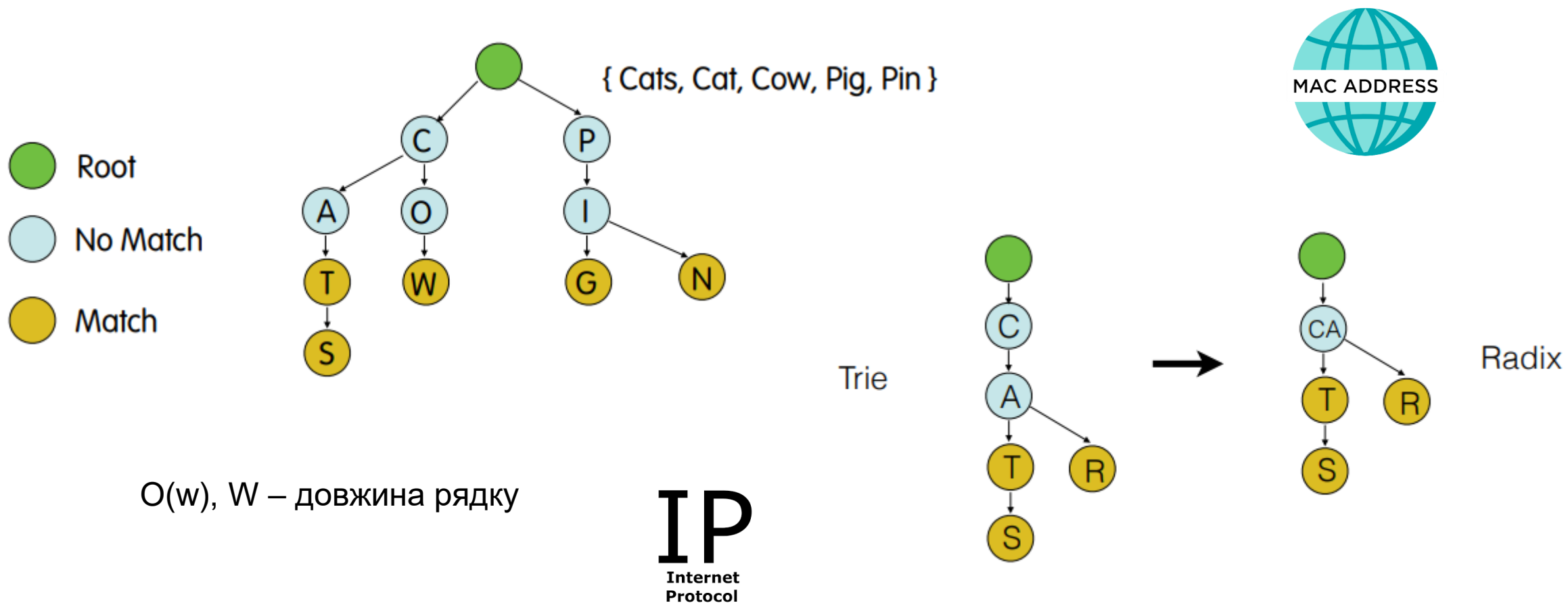
Парсери



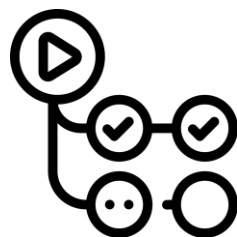
&[u8]

```
user@host:/tmp/segfault$ cat segfault.c
void main() {
    char *str = "Hello, world!";
    *str = 'A';
}
user@host:/tmp/segfault$ gcc segfault.c -o segfault
user@host:/tmp/segfault$ ./segfault
Segmentation fault
neil@snap:/tmp/segfault$
```

Зберігання префіксних сутностей (Radix Tree)

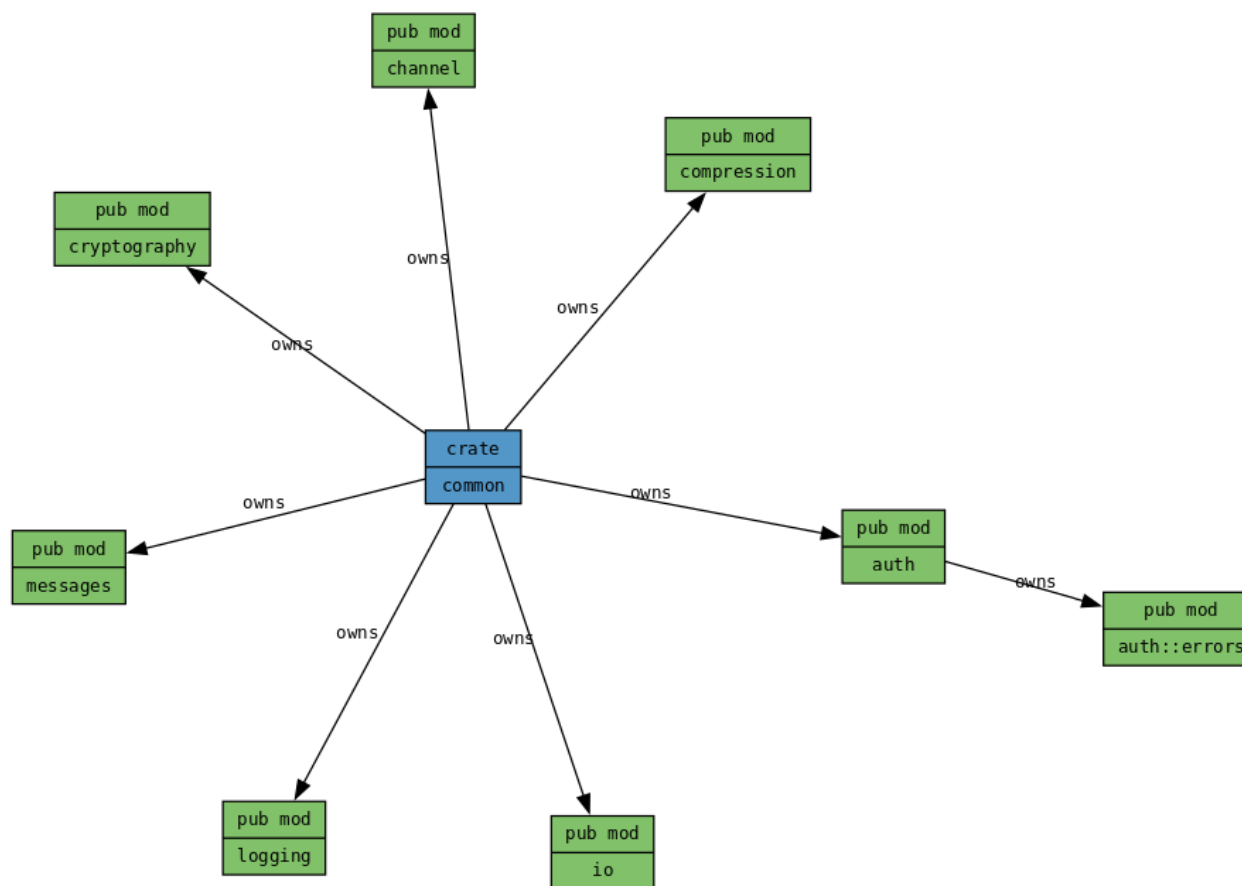


Зберігання коду, збірка

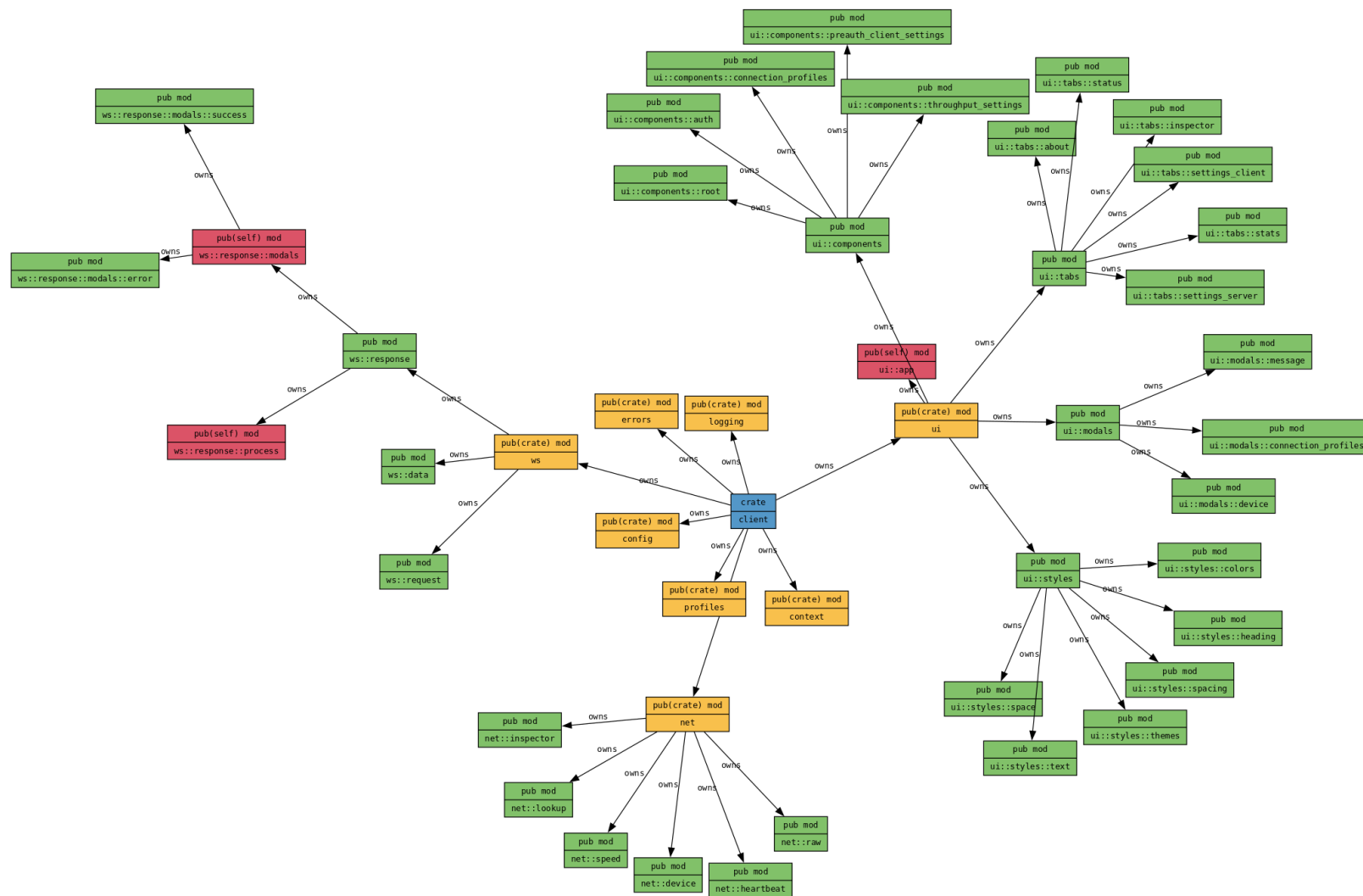


github.com/xairaven/xailyser

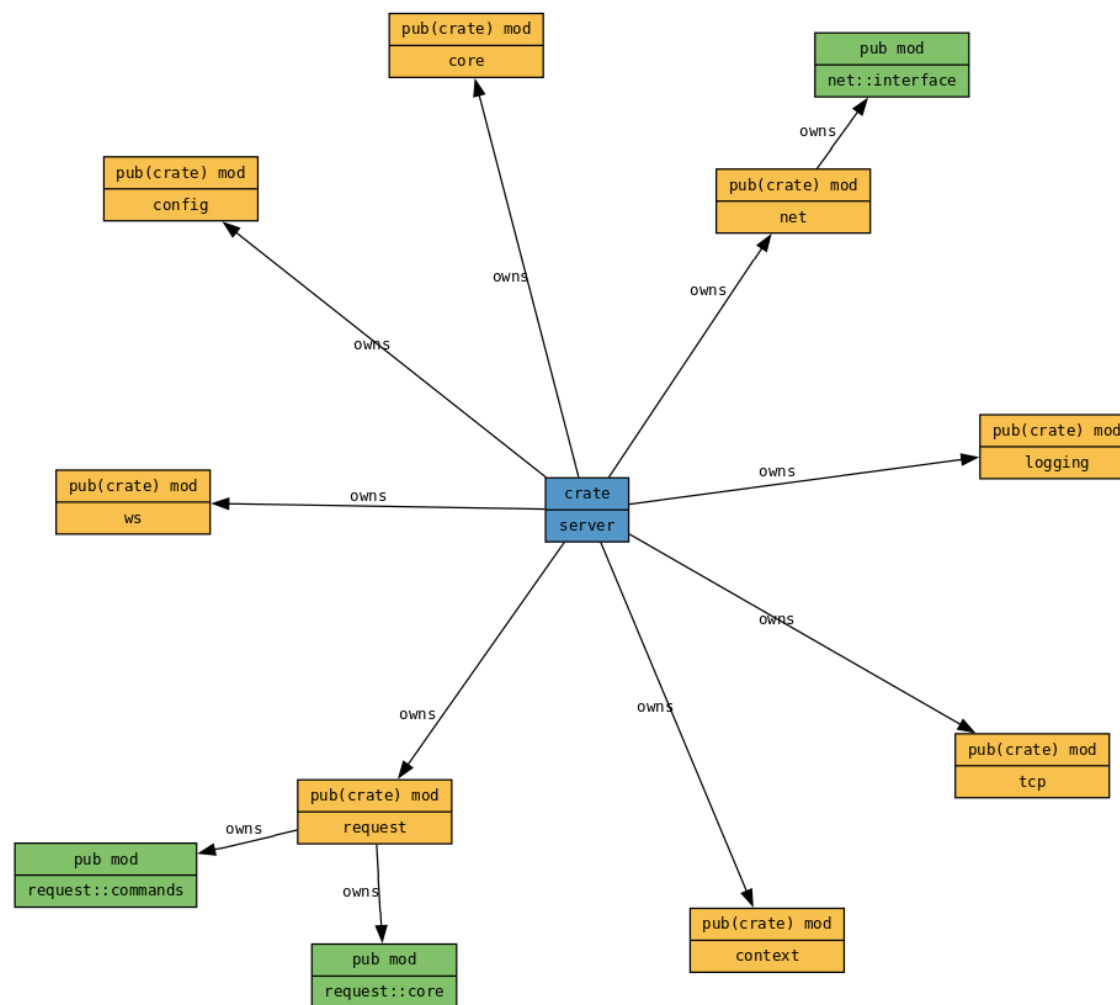
Спільний функціонал



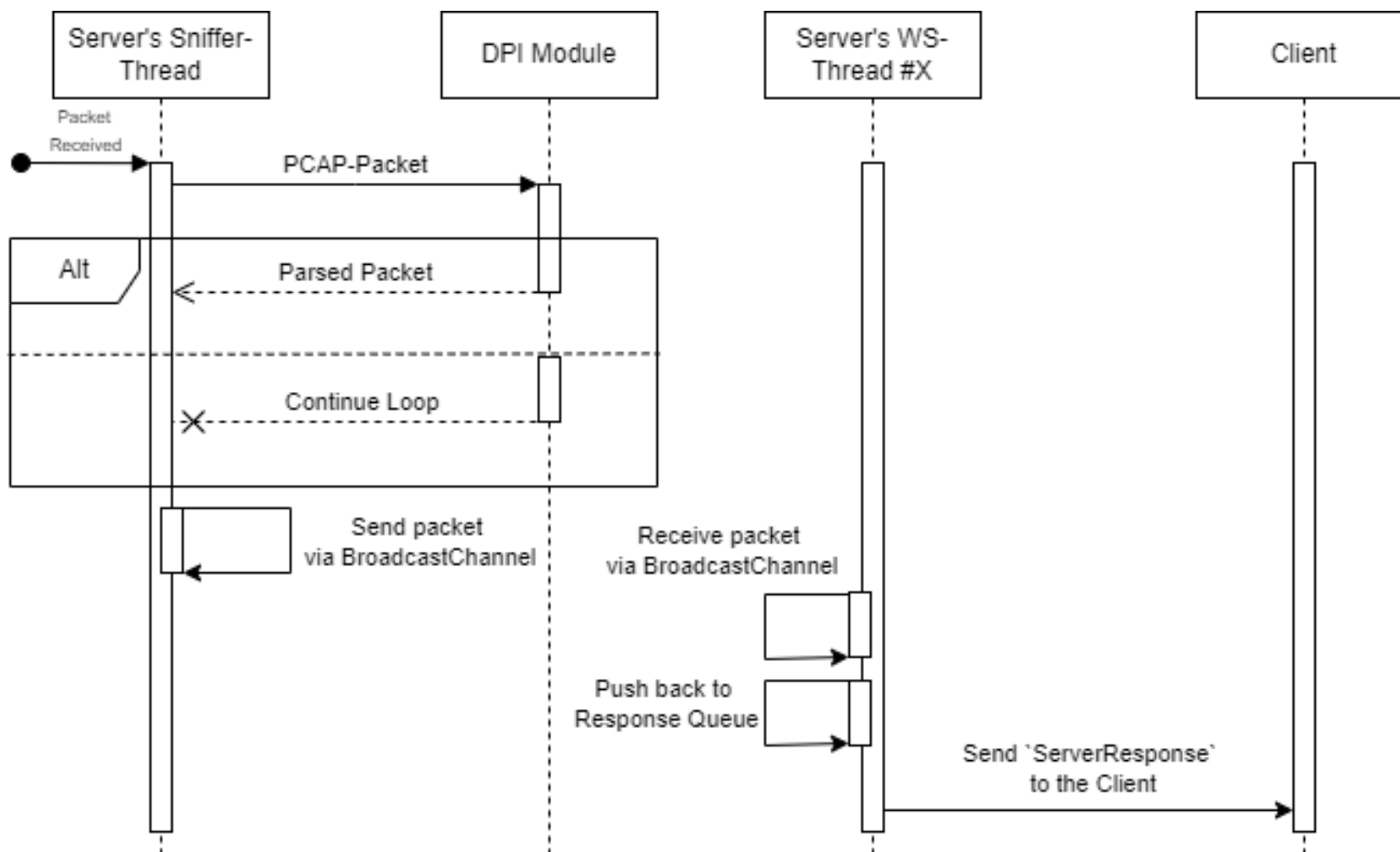
Клієнтський застосунок



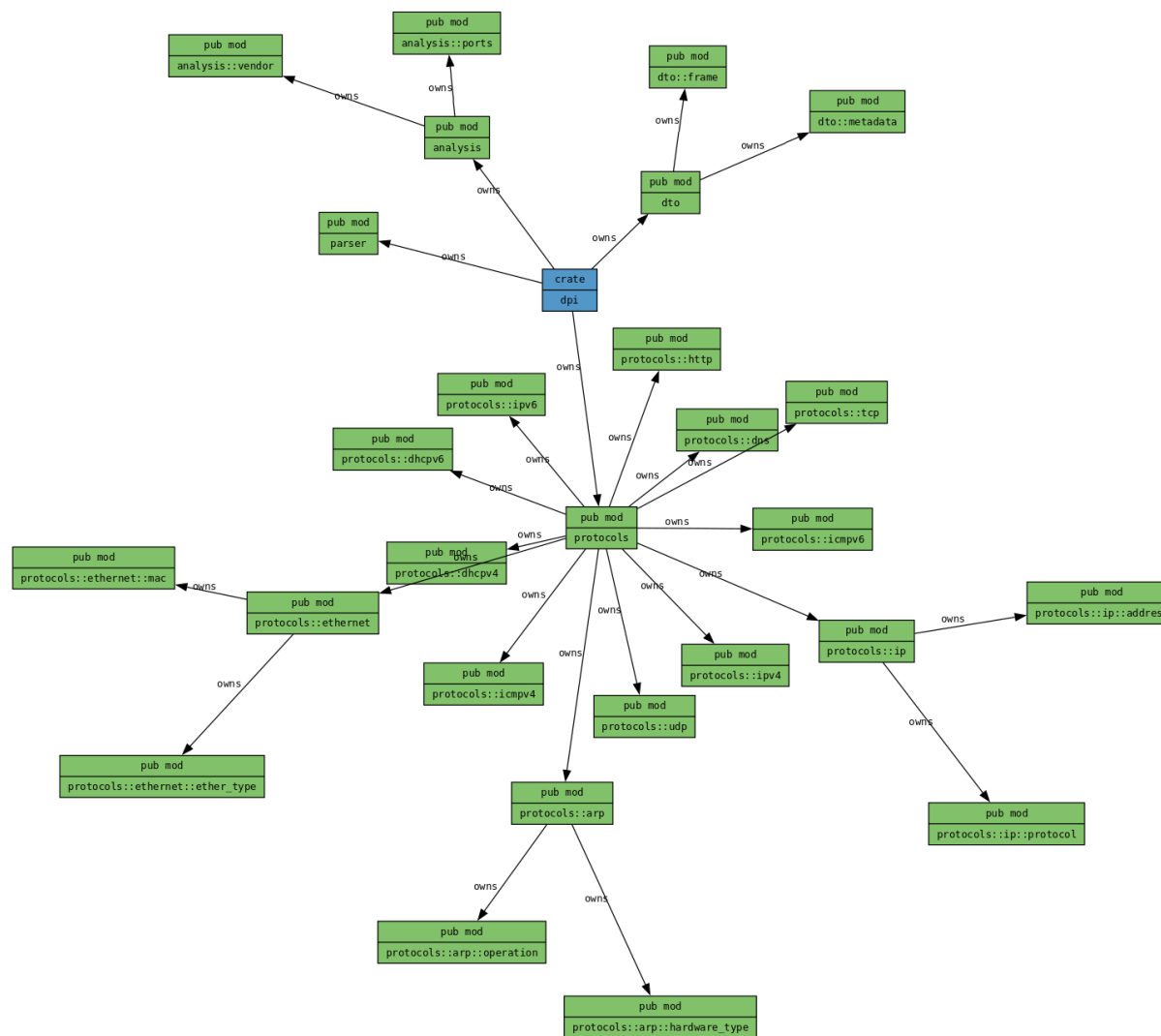
Сервер



Шлях отриманого пакету



Бібліотека DPI





Логін

IP:	<input type="text" value="127.0.0.1"/>
Порт:	<input type="text" value="8080"/>
Пароль:	<input type="password" value="....."/>

Підключитися



Профілі підключень: 1



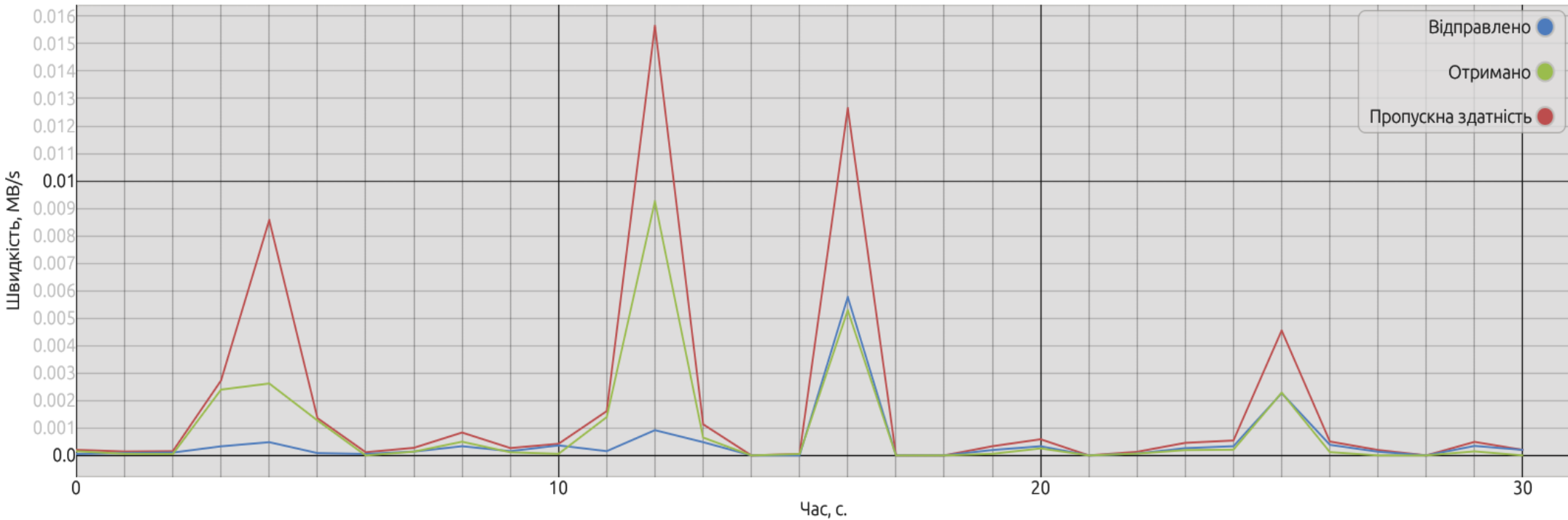
Main, Local

- ▶ Використати
- 🗑 Видалити
- ✎ Редагувати

Адреса: 127.0.0.1

Порт: 8080

- Статус
- Інспектор
- Статистика
- Клієнт
- Сервер
- Про програму
- Від'єднатись
- Вихід



Пік (MB/s): ➤ Загалом: 0.02 ↓ Отримано: 0.01 ↑ Відправлено: 0.01

Пристрої:

Зберегти псевдоніми

MyLaptop

MAC: 04:E8:B9:18:55:10
IPv4: 192.168.0.103
IPv6: -
Виробник: Intel Corporate

- Статус
- Інспектор
- Статистика
- Клієнт
- Сервер
- Про програму
- Від'єднатись
- Вихід

DNS

◀◀

◀

Page 1 of 1 total

▶

▶▶

Очистити

▼ DNS Packet #2

Тип повідомлення	Код операції	Авторитетна відповідь	Код відповіді
Query	StandardQuery	-	NoErrorCondition
Розділ питання (Записи: 1)			
№	Ім'я	Тип запису	Клас
1	frameworks.jetbrains.com	A	IN

▼ DNS Packet #3

Тип повідомлення	Код операції	Авторитетна відповідь	Код відповіді		
Response	StandardQuery	-	NoErrorCondition		
Розділ питання (Записи: 1)					
№	Ім'я	Тип запису	Клас		
1	frameworks.jetbrains.com	A	IN		
Розділ відповіді (Записи: 5)					
№	Ім'я	Тип запису	Клас	Час життя	Дані
1	frameworks.jetbrains.com	CNAME	IN	234	d1gyz2dzs4t2p.cloudfront.net
2	d1gyz2dzs4t2p.cloudfront.net	A	IN	60	18.66.122.72
3	d1gyz2dzs4t2p.cloudfront.net	A	IN	60	18.66.122.49

- Статус
- Інспектор
- Статистика
- Клієнт
- Сервер**
- Про програму
- Від'єднатись
- Вихід

Запитати активні налаштування05/25 22:51:36

Зберегти конфігурацію:Застосувати

Перезапустити сервер:Застосувати

Стиснення:ВимкненоУвімкнути

Змінити пароль:Застосувати

Відправка необроблених фреймів:ВимкненоУвімкнути

▼ Інтерфейси:

Активно: Intel(R) Wi-Fi 6 AX201 160MHz

Доступні інтерфейси:

Adapter for loopback traffic capture

Hyper-V Virtual Ethernet Adapter

Microsoft Wi-Fi Direct Virtual Adapter

Microsoft Wi-Fi Direct Virtual Adapter #2

Intel(R) Wi-Fi 6 AX201 160MHz

Панель керування

⚙️ Клієнт

🏠 Статус

🔍 Інспектор

📊 Статистика

⚙️ Клієнт

⚙️ Сервер

① Про програму

🔗 Від'єднатись

✖ Вихід

Відкинути нерозібрані пакети: ✓

Застосувати



Затримка синхронізації:

5 секунд

Застосувати



Зберегти конфігурацію:

Зберегти

Зберігати нерозібрані пакети: ✓

100 фреймів

Застосувати



Ліміт збереження фреймів: ✓

100000 фреймів

Застосувати



Мова:

Українська ▼

Застосувати



Рівень логування:

Інформація ▼

Застосувати



Стиснення:



Застосувати



Тема:

Standard Light ▼

Застосувати








Формат логування:

[\$Y-\$m-\$D \$H:\$M \$LEVEL \$TARGET]
\$MESSAGE

Застосувати



 Статус Інспектор Статистика Клієнт Сервер Про програму Від'єднатись Вихід

XAILYSER v1.0.0

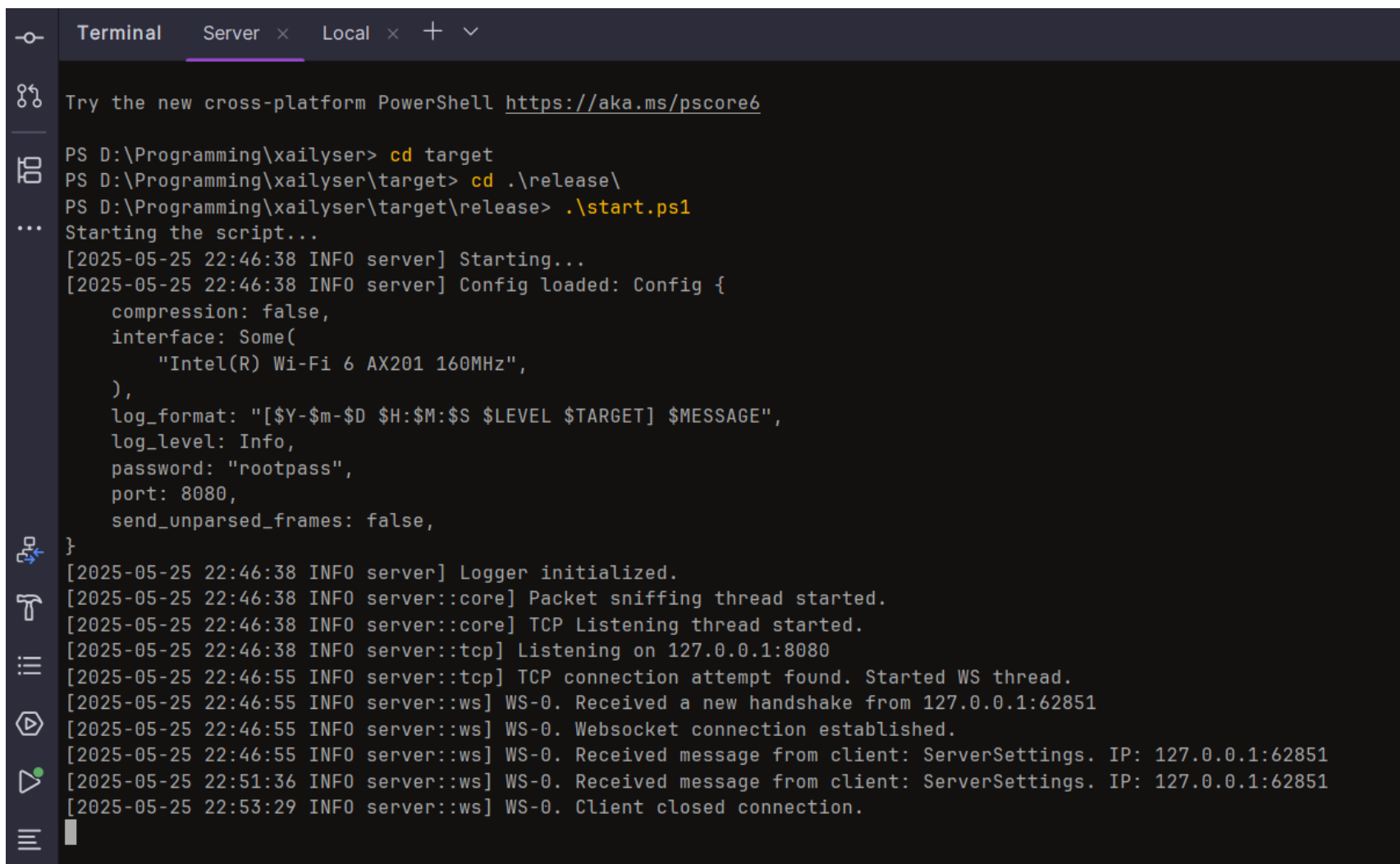
Клієнт-серверний аналізатор мережевого трафіку у домашній мережі.

Розробник: Ковальов Олександр

Перегляньте код на GitHub!

Останній реліз

Сервер



```
Terminal  Server x Local x + v

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS D:\Programming\xailyser> cd target
PS D:\Programming\xailyser\target> cd .\release\
PS D:\Programming\xailyser\target\release> .\start.ps1
Starting the script...
[2025-05-25 22:46:38 INFO server] Starting...
[2025-05-25 22:46:38 INFO server] Config loaded: Config {
    compression: false,
    interface: Some(
        "Intel(R) Wi-Fi 6 AX201 160MHz",
    ),
    log_format: "[Y-m-D H:M:S $LEVEL $TARGET] $MESSAGE",
    log_level: Info,
    password: "rootpass",
    port: 8080,
    send_unparsed_frames: false,
}
[2025-05-25 22:46:38 INFO server] Logger initialized.
[2025-05-25 22:46:38 INFO server::core] Packet sniffing thread started.
[2025-05-25 22:46:38 INFO server::core] TCP Listening thread started.
[2025-05-25 22:46:38 INFO server::tcp] Listening on 127.0.0.1:8080
[2025-05-25 22:46:55 INFO server::tcp] TCP connection attempt found. Started WS thread.
[2025-05-25 22:46:55 INFO server::ws] WS-0. Received a new handshake from 127.0.0.1:62851
[2025-05-25 22:46:55 INFO server::ws] WS-0. Websocket connection established.
[2025-05-25 22:46:55 INFO server::ws] WS-0. Received message from client: ServerSettings. IP: 127.0.0.1:62851
[2025-05-25 22:51:36 INFO server::ws] WS-0. Received message from client: ServerSettings. IP: 127.0.0.1:62851
[2025-05-25 22:53:29 INFO server::ws] WS-0. Client closed connection.
```

Тестування

The screenshot shows a test runner interface with a dark theme. On the left, a tree view shows the test results: 'Test Results' (1 sec 116 ms) is expanded, showing 'dpi' (1 sec 116 ms) which contains 'analysis' (992 ms) and 'protocols' (124 ms). 'protocols' is further expanded to show 'arp' (5 ms), 'dhcpv4' (5 ms), 'dhcpv6' (4 ms), 'dns' (27 ms), and 'ethernet' (24 ms). On the right, a summary bar indicates '33 tests passed' out of '33 tests total' in '1 sec 116 ms'. Below this, a terminal window shows the command 'C:/Users/Alex/.cargo/bin/cargo.exe test --color=always --' and the output 'Testing started at 23:41 ...'. The output continues with 'Finished `test` profile [unoptimized + debuginfo] target' and several 'Running unittests' entries for different components.

```

C:/Users/Alex/.cargo/bin/cargo.exe test --color=always --
Testing started at 23:41 ...

Finished `test` profile [unoptimized + debuginfo] target
Running unittests src\main.rs (target\debug\deps\cli
Running unittests src\lib.rs (target\debug\deps\comm
Running unittests src\lib.rs (target\debug\deps\dpi-
Running unittests src\main.rs (target\debug\deps\ser
  
```

Name	Status	42% CPU	81% Memory	0% Disk	0% Network
client.exe		28.1%	98.1 MB	0 MB/s	0 Mbps
server.exe		0%	2.3 MB	0 MB/s	0 Mbps

Висновки

- Продукт готовий до використання
- Тестування проведене
- Отримані нові знання щодо роботи з мережевими протоколами

Апробація

УДК 004.94

¹ Бакалаврант 4 курсу Ковальов О.О.

¹ Асист. Кардашов О.В.

<https://scholar.google.com.ua/citations?user=gtnZz4EAAAAJ&hl=uk>

¹ КПІ ім. Ігоря Сікорського

ПОРІВНЯННЯ ТЕХНОЛОГІЙ ЗАХОПЛЕННЯ МЕРЕЖЕВОГО ТРАФІКУ ДЛЯ РОЗРОБКИ СИСТЕМИ ГЛИБОКОГО АНАЛІЗУ ПАКЕТІВ

Постановка проблеми та її актуальність. У сучасному світі інформаційних технологій зростає потреба у високопродуктивних та безпечних системах аналізу мережевого трафіку, особливо коли йдеться про застосування технологій deep packet inspection (DPI, глибокий аналіз або інспекція пакетів, де пакет є будь-яким блоком даних відносно рівнів системи OSI) для забезпечення кібербезпеки, моніторингу мереж і оперативного виявлення аномалій. Використання DPI полягає не лише в обробці заголовків, а й самих даних, payload (корисне навантаження) та визначення протоколів.

Основною задачею є захоплення потоків пакетів із високою швидкістю та їх подальша обробка, що вимагає не лише високої продуктивності, але й надійності та

iate.kpi.ua/uploads/p_164_22642045.pdf