Міністерство освіти і науки України

Національний університет «Запорізька політехніка»

кафедра програмних засобів

ЗВІТ

з лабораторної роботи № 6

з дисципліни «Безпека та захист програм і даних» на тему:

«ДОСЛІДЖЕННЯ РОБОТИ ПРОГРАМ-МОНІТОРІВ»

Виконав:

ст. гр. КНТ-113сп Іван ЩЕДРОВСЬКИЙ

Прийняв:

доцент Тетяна ЗАЙКО

2025

1 Мета роботи

Ознайомитись на практиці з основними програмними засобами, що використовуються зламниками для аналізу роботи захищеного програмного забезпечення. Навчитись обирати програмні засоби для аналізу системи захисту програм

2 Завдання до лабораторної роботи

Навчитись використовувати базові функції запропонованих програм, і заповнити таблицю характеристик

3 Відповіді на контрольні питання

Навести загальний порядок здійснення зламу захисту

Спочатку виконується запуск та спостереження за роботою програмного засобу. Перед виконанням зламу потрібно зрозуміти, що програма взагалі собою представляє, які функції виконує т.д.

Далі виконується відслідковування звернення програми до системного реєстру та власних файлів налаштувань. Інколи можна змінити щось в реєстрі, або ж в файлі налаштувань, щоб повністю зняти захист

Далі відслідковується звернення програми до ресурсів програмної системи, файлів та каталогів

Виконується аналіз виконуваних файлів на динамічних бібліотек на предмет запаковування виконуваних файлів, їх шифрування тощо

Далі виконується дизасемблювання і модифікація програмних модулів

Охарактеризувати програми-монітори звернень до файлів. Їх призначення

Програми-монітори звернень до файлів дозволяють зрозуміти з якими файлами взаємодіє програма, тобто які файли вона читає та записує. Наприклад, таким чином ми можемо знайти файли конфігурації та налаштувати, або навіть зламати, програму

Дати характеристику програмам стеження за системним реєстром. Їх використання для аналізу систем захисту

Програми-монітори стеження за системним реєстром дозволяють зрозуміти які саме налаштування використовує та змінює програма

Наприклад, в реєстрі можуть зберігатись налаштування застосунку, в тому числі параметри її захисту, змінюючи які ми можемо вимкнути його

Дати характеристику програмам для моніторингу процесів і вікон

Ці програми дають змогу спостерігати які процеси створюються/видаляються в процесі виконання програми

Наприклад, нові процеси можуть створюватись для якихось паралельних обчислень

Охарактеризувати програми-монітори API-викликів. Де і як їх можна застосувати?

Ці програми дозволяють зрозуміти які саме API-фукнції використовує програма та з якими даними

Це корисно знайти для майбутнього більш глибокого аналізу системи

Охарактеризувати особливості використання програм сканування портів, програм моніторингу мережевого обміну

Ці програми показують інформацію, яка передається через мережу, локальну чи глобальну. Наприклад, всі з’єднання, всі запити до інших серверів та обмін інформації між локальними програмами

Для чого можуть бути використані вказані програми при покращенні роботи операційних систем?

Для їх оптимізації. Ми не можемо оптимізувати, наприклад, роботу через мережу або процеси, якщо ми не побачимо як воно працює насправді

Як можуть бути використані програми моніторингу при дослідженні роботи систем захисту програмного забезпечення?

Програми-монітори показують як програма взаємодіє з частинами операційної системи, іншими програмами, файловими ресурсами і так далі. При дослідженні захисту програми це є дуже важливою інформацією, оскільки за допомогою неї можна зрозуміти як працює програма всередині, а тому зрозуміти як працює система захисту, якщо вона є, і як її вимкнути

4 Короткі відомості

Для аналізу було взято мій персональний проєкт який називається logical. Це застосунок який дозволяє візуалізувати логічні схеми, використовує Golang та ebitengine

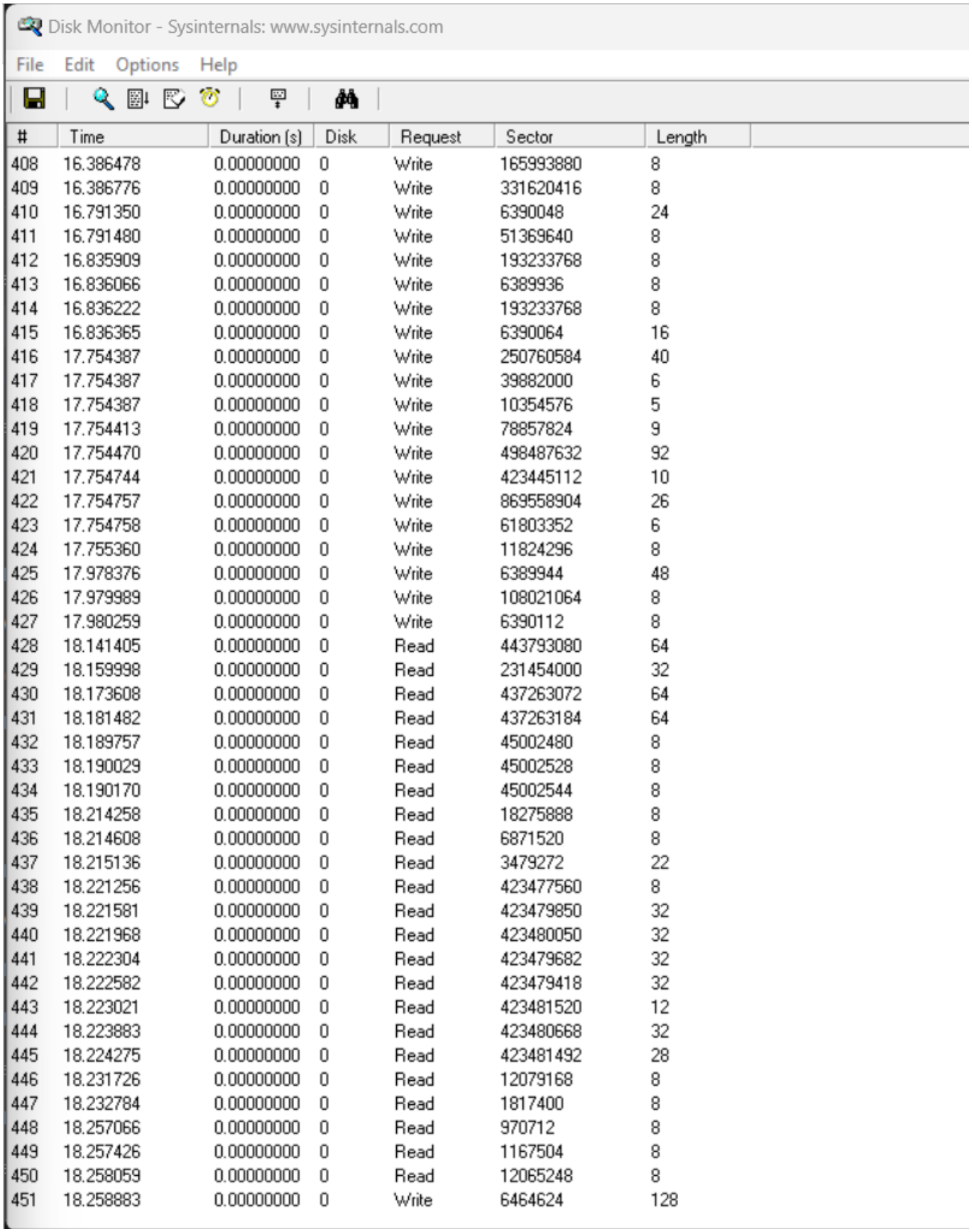
Згідно з офіційною документацією від Microsoft програми RegMon та FileMon більше не доступні для завантаження та використання. Вони були замінені на Process

Monitor починаючи з Windows Vista. Для виконання роботи використовується Windows 11

Ці програми все ще можна знайти в інтернеті, але при скачуванні чого завгодно з не офіційних ресурсів є великий шанс попасти на віруси/стилери т.д., тому в цій лабораторній роботі програми RegMon та FileMon аналізуватись не будуть

Також в роботі не буде виконуватись аналіз PortMon, оскільки цей застосунок не підтримується на Windows 11, а при запускі видає помилку Error 2 та повідомлення про безпеку драйверів

Першою програмою для аналізу було обрано DiskMon. Її використання показано на рисунку 1



#	Time	Duration (s)	Disk	Request	Sector	Length
408	16.386478	0.00000000	0	Write	165993880	8
409	16.386776	0.00000000	0	Write	331620416	8
410	16.791350	0.00000000	0	Write	6390048	24
411	16.791480	0.00000000	0	Write	51369640	8
412	16.835909	0.00000000	0	Write	193233768	8
413	16.836066	0.00000000	0	Write	6389936	8
414	16.836222	0.00000000	0	Write	193233768	8
415	16.836365	0.00000000	0	Write	6390064	16
416	17.754387	0.00000000	0	Write	250760584	40
417	17.754387	0.00000000	0	Write	39882000	6
418	17.754387	0.00000000	0	Write	10354576	5
419	17.754413	0.00000000	0	Write	78857824	9
420	17.754470	0.00000000	0	Write	498487632	92
421	17.754744	0.00000000	0	Write	423445112	10
422	17.754757	0.00000000	0	Write	869558904	26
423	17.754758	0.00000000	0	Write	61803352	6
424	17.755360	0.00000000	0	Write	11824296	8
425	17.978376	0.00000000	0	Write	6389944	48
426	17.979989	0.00000000	0	Write	108021064	8
427	17.980259	0.00000000	0	Write	6390112	8
428	18.141405	0.00000000	0	Read	443793080	64
429	18.159998	0.00000000	0	Read	231454000	32
430	18.173608	0.00000000	0	Read	437263072	64
431	18.181482	0.00000000	0	Read	437263184	64
432	18.189757	0.00000000	0	Read	45002480	8
433	18.190029	0.00000000	0	Read	45002528	8
434	18.190170	0.00000000	0	Read	45002544	8
435	18.214258	0.00000000	0	Read	18275888	8
436	18.214608	0.00000000	0	Read	6871520	8
437	18.215136	0.00000000	0	Read	3479272	22
438	18.221256	0.00000000	0	Read	423477560	8
439	18.221581	0.00000000	0	Read	423479850	32
440	18.221968	0.00000000	0	Read	423480050	32
441	18.222304	0.00000000	0	Read	423479682	32
442	18.222582	0.00000000	0	Read	423479418	32
443	18.223021	0.00000000	0	Read	423481520	12
444	18.223883	0.00000000	0	Read	423480668	32
445	18.224275	0.00000000	0	Read	423481492	28
446	18.231726	0.00000000	0	Read	12079168	8
447	18.232784	0.00000000	0	Read	1817400	8
448	18.257066	0.00000000	0	Read	970712	8
449	18.257426	0.00000000	0	Read	1167504	8
450	18.258059	0.00000000	0	Read	12065248	8
451	18.258883	0.00000000	0	Write	6464624	128

Рисунок 1 – Використання DiskMon

На рисунку 2 показано використання програми APIMon, а саме API Monitor v2 64-bit.

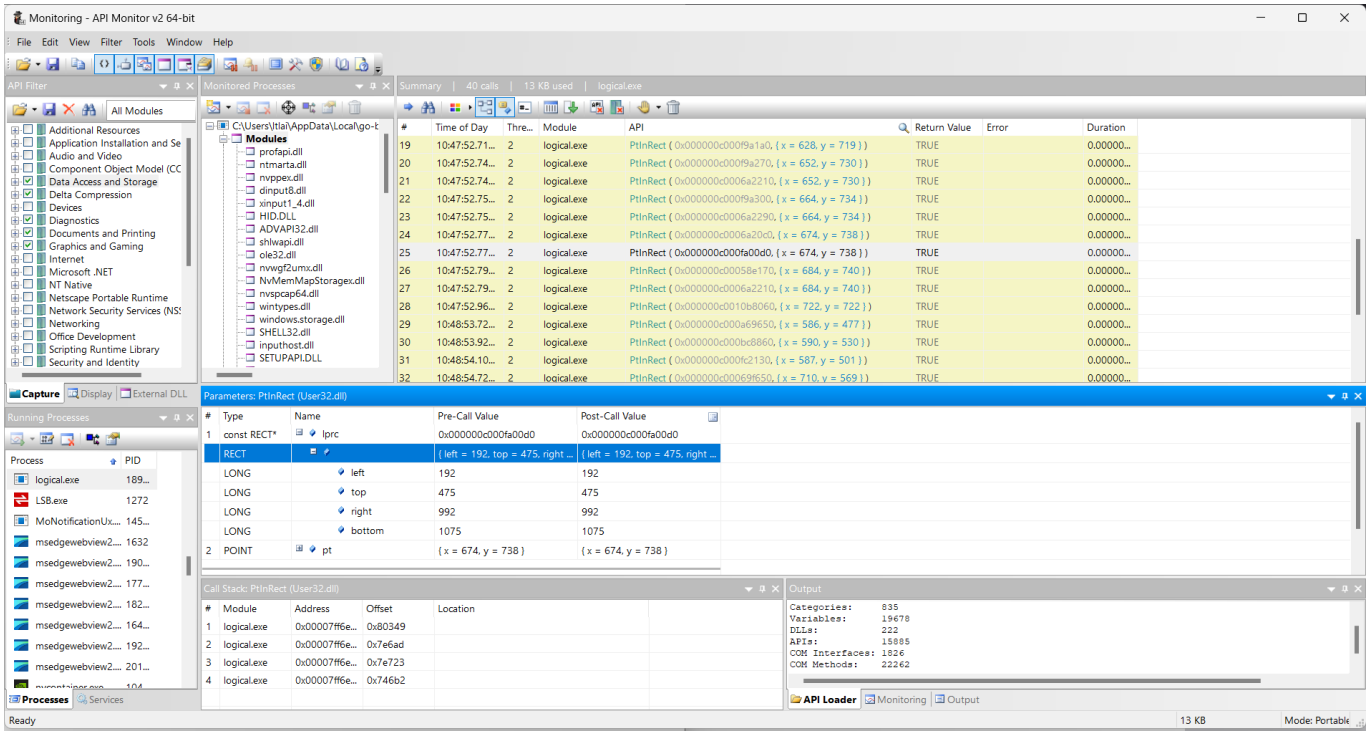


Рисунок 2 – Використання API Monitor v2

На рисунку 3 показано використання програми Process Monitor.

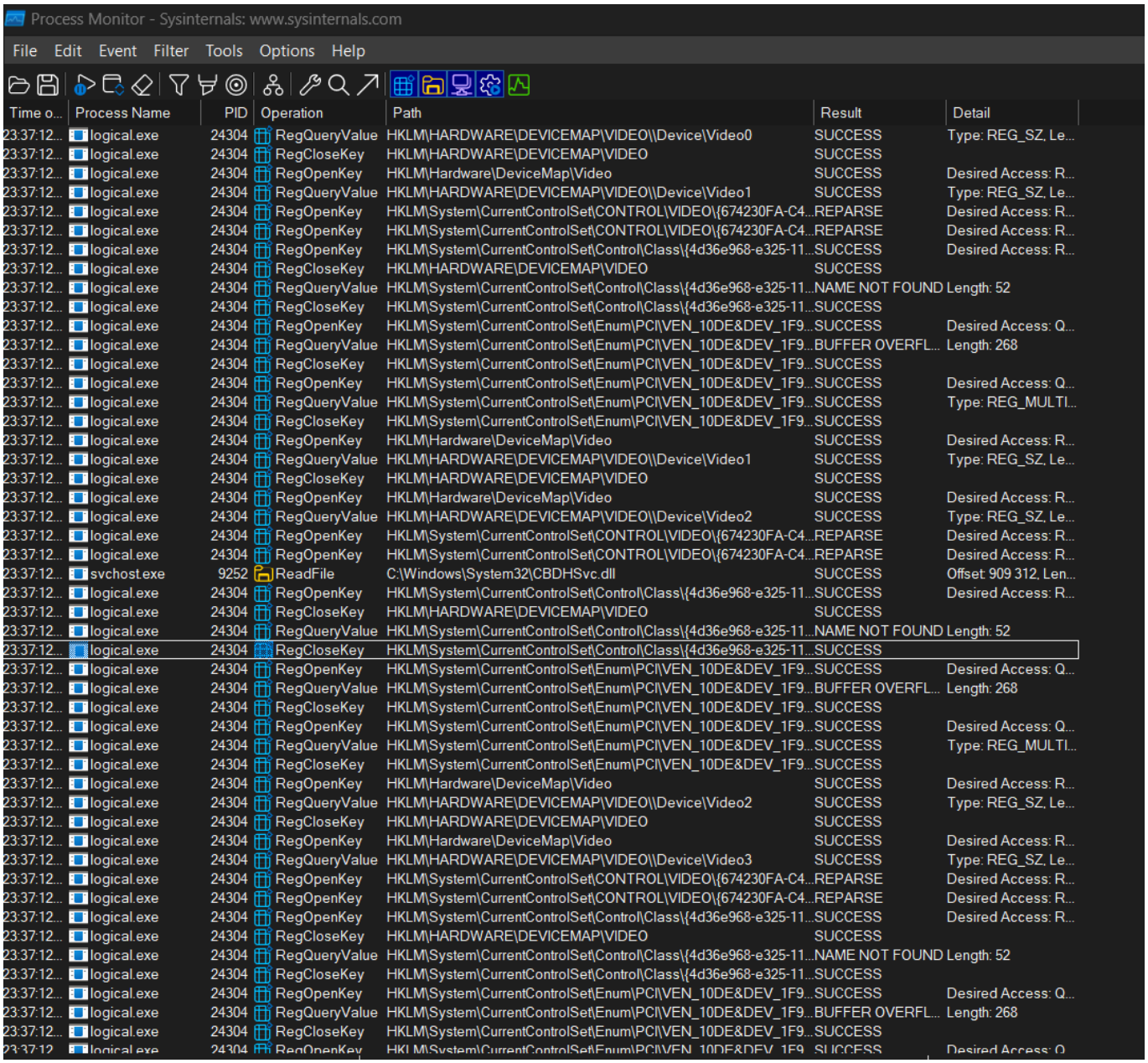


Рисунок 3 – Використання Process Monitor

На рисунку 4 показано використання програми Wireshark, яка є Network Traffic Monitor

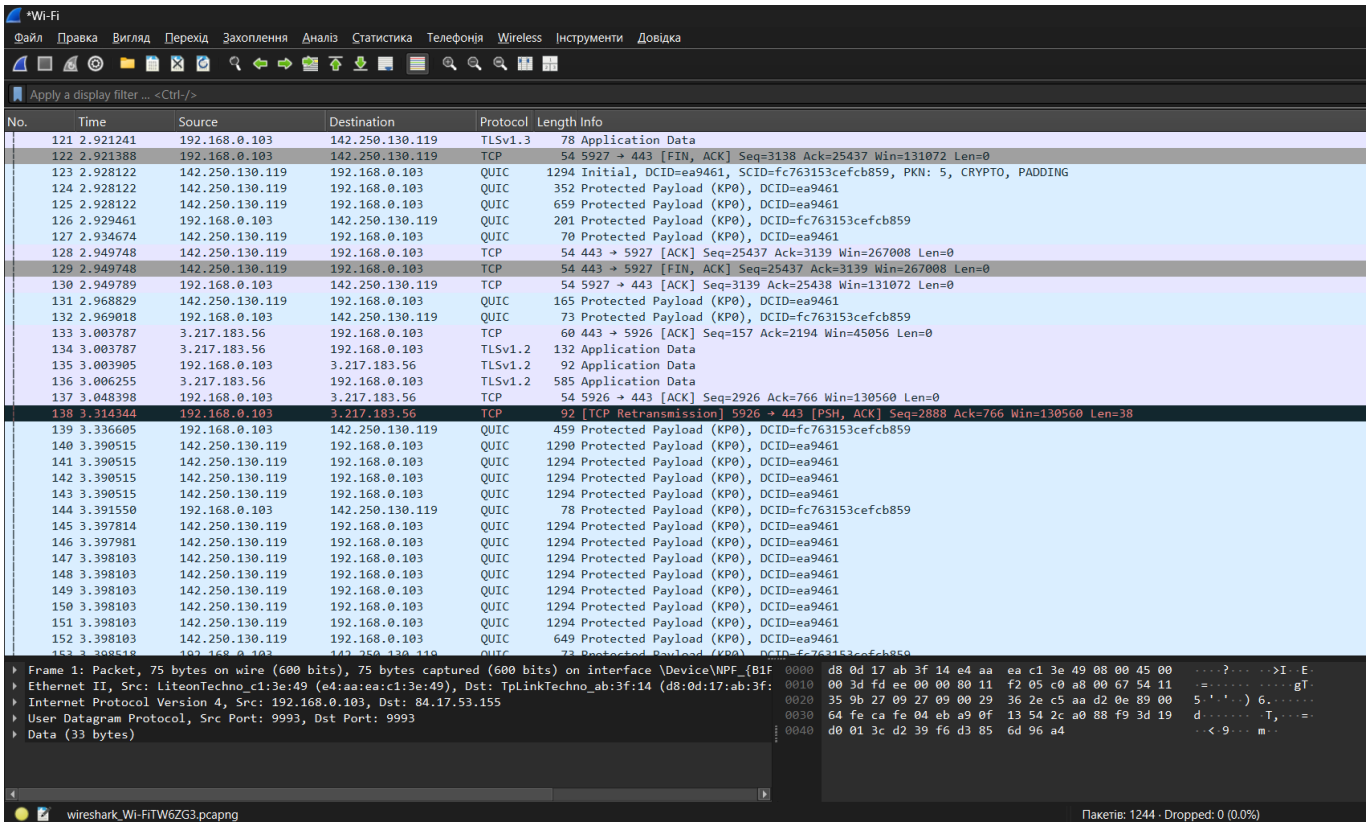


Рисунок 4 – Використання Wireshark

5 Таблиця з результатами

№	Назва програми	Призначення	Об’єкт дослідження	Результати дослідження	Оцінка	Висновки (позитивні і негативні)
1	**2**	**3**	**4**	**5**	**6**	**7**
1	DiskMon	Моніторинг звернень до дискової системи комп’ютера	Logical	Під час виконання програми виконується не велика кількість операцій, відносно інших програми, по запису та читанню інформації з диску	2	Позитивні: DiskMon показує всі записи та читання з диску Негативні: Для аналізу окремої програми потрібно або

						знати в які селектори дивитись, або запускати її в повній ізоляції, що зробити досить складно
2	APIMon	Моніторинг інформації про використовувані функції	Logical	В результаті аналізу вдалось побачити які саме API використовує програма для роботи, а також вдалось побачити інформацію, яка передається в них	5	Позитивні: Програма дає змогу побачити список API-функцій які використовує застосунок та дані, які туди передаються. Наприклад, якщо буде передаватись пароль, то його буде видно відразу Недоліки: Наразі не знайдено, треба більше часу використання
3	Process Monitor	Показ в реальному часі роботу файлової системи,	Logical	Програма показує всі взаємодії з файлами, всі взаємодії з реєстрами, роботу	5	Позитивні: Монітор показує велику кількість інформації, яка може бути

		взаємодії з реєстрами та активність процесів/тредів		тредів та взаємодію через мережу		використана в майбутньому для більш глибокого аналізу системи Недоліки: Швидкість роботи, але при 2 мільйонах подій за декілька хвилин це нормально
4	Wireshark	Моніторинг взаємодії через мережу	Firefox	Програма-монітор показує всі взаємодії через різні протоколи, наприклад ARP, QUIC, UDP, TCP, HTTP, DNS тощо	5	Позитивні: Монітор дозволяє аналізувати всі взаємодії через мережу Недоліки: Треба встановлювати додаткову бібліотеку, а також офіційне джерело має повільну швидкість скачування

6 Висновки

Я ознайомився на практиці з основними програмними засобами, що використовуються зламниками для аналізу роботи захищеного програмного забезпечення. Навчився обирати програмні засоби для аналізу системи захисту програм