Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Бойченка Олександра Олександровича

академічної групи *125-20-1*

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему Дослідження безпеки використання соціальної мережі «Instagram» та месенджерів «Telegram» і «WhatsApp»

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Начовний І.І.			
економічний	к.е.н., доц. Пілова Д.П.	85	добре	

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту Бойченку О.О. **академічної групи** ***125-20-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему Дослідження безпеки використання соціальної мережі «Instagram» та месенджерів «Telegram» і «WhatsApp»

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Огляд соціальної мережі «Instagram» та месенджерів «Telegram» і «WhatsApp», їх функцій та випадків злому облікових записів користувачів	15.03.2024
Розділ 2	Дослідження передачі та шифрування текстових та голосових повідомлень, які надсилаються через десктопні додатки для клієнтів соціальної	10.05.2024
Розділ 3	Розрахунки витрат на проведення дослідження, можливих експлуатаційних витрат після вивчення матеріалів цього дослідження, можливих збитків від злому облікового запису працівника приватної компанії	11.06.2024

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 15.01.2024 р.

Дата подання до екзаменаційної комісії: 28.06.2024 р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 84 с., 32 рис., 3 табл., 4 додатка, 49 джерел.

Об'єкт дослідження: соціальна мережа «Instagram» та месенджери «Telegram» і «WhatsApp».

Предмет дослідження: випадки злому облікових записів користувачів «Instagram», «Telegram» і «WhatsApp», шифрування текстових та голосових повідомлень.

Мета роботи: перевірка захисних методів в «Instagram», «Telegram» і «WhatsApp», перевірка безпеки використання службовими працівниками.

У першому розділі було розглянуто соціальну мережу «Instagram» та месенджери «Telegram» і «WhatsApp», їх загальний функціонал, інформацію, що створюється та обробляється в них. Було розглянуто найвідоміші випадки злому облікових записів користувачів соціальної мережі «Instagram» та месенджерів «Telegram» і «WhatsApp».

У другому розділі було задокументовано результати проведення дослідження шифрування текстових та голосових повідомлень, надісланих через десктопні додатки для клієнтів «Instagram», «Telegram» і «WhatsApp», за допомогою сніферу пакетів «Wireshark». За допомогою утиліти «JPEGsnoop» було перевірено фотографії, що надсилаються, на наявність метаданих.

У третьому розділі було розраховано витрати на проведення дослідження, можливі річні експлуатаційні витрати для національних служб та приватних компаній, можливі економічні збитки від злому облікового запису працівника приватної компанії.

Практична цінність дослідження полягає у виявленні ризиків, які можливі під час використання зазначених соціальної мережі та месенджерів.

ДОСЛІДЖЕННЯ, МЕРЕЖЕВІ ПАКЕТИ ДАНИХ, МЕСЕНДЖЕР, МЕТАДАНІ, СОЦІАЛЬНА МЕРЕЖА, ШИФРУВАННЯ, INSTAGRAM, TELEGRAM, WHATSAPP, WIRESHARK.

ABSTRACT

Explanatory note: 84 pp., 32 pic., 3 table, 4 app, 49 sources.

Research object: social network «Instagram» and messengers «Telegram» and «WhatsApp».

Research subject: cases of hacking of «Instagram», «Telegram» and «WhatsApp» user accounts, encryption of text and voice messages.

The purpose of the work: verification of protective methods in «Instagram", «Telegram» and «WhatsApp», verification of the security of use by employees.

In the first section, the social network «Instagram» and messengers «Telegram» and «WhatsApp», their general functionality, the information created and processed in them were considered. The most famous cases of hacking of accounts of users of the social network «Instagram" and messengers «Telegram» and «WhatsApp» were considered.

The second chapter documented the results of a study of encrypting text and voice messages sent through the «Instagram», «Telegram», and WhatsApp» desktop applications using the «Wireshark» packet sniffer. Submitted photos were scanned for metadata using «JPEGsnoop».

In the third section, the costs of conducting the study, the possible annual operating costs for national services and private companies, and the possible economic losses from hacking the account of an employee of a private company were calculated.

The practical value of the research lies in identifying the risks that are possible when using the specified social network and messengers.

RESEARCH, NETWORK DATA PACKAGES, MESSENGER, METADATA, SOCIAL NETWORK, ENCRYPTION, INSTAGRAM, TELEGRAM, WHATSAPP, WIRESHARK.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДСНС - Державна служба з надзвичайних ситуацій

ОС - операційна система;

ПЗ - програмне забезпечення;

ПК - персональний комп'ютер;

ШІ - штучний інтелект;

API - Application Program Interface;

IP - Internet Protocol;

SSL - Secure Sockets Layer;

TCP - Transmission Control Protocol;

TLS - Transport Layer Security;

UDP - User Datagram Protocol.

ЗМІСТ

ВСТУП

Соціальні мережі та месенджери стали невід'ємною частиною нашого життя. Вони спрощують комунікацію між людьми в різноманітних сферах діяльності людства (навчання, робота тощо), допомагають нам завжди тримати зв'язок з рідними та близькими, а для когось вони є джерелом заробітку, отже, не дивно, що для зловмисників заволодіння чиїмось акаунтом від соцмережі. Для успішної реалізації та просування додатку для спілкування необхідно переконати та надати впевненість користувачам у тому, що їх персональні дані не будуть викрадені та використані проти них і що їх конфіденційна інформація не буде розповсюджена. З цієї причини вивчення, детальне дослідження та постійна розробка та покращення методів захисту конфіденційної інформації в соціальних мережах є однією з галузей сфери кібербезпеки у сучасному світі.

Спеціалісти з кібербезпеки регулярно працюють над збільшенням завадостійкості до різного роду зламів в програмному забезпеченні для спілкування, які розробляють різноманітні компанії, наприклад, «Telegram FZ-LLC»[1)], «Meta Platforms Inc.»[2)] та інші. Покращені криптографічні шифри для шифрування повідомлень, хешування паролів, двофакторна автентифікація, наскрізне шифрування повідомлень, аудіозв'язку та відеозв'язку, періодичне видалення повідомлень через деякий проміжок часу - це далеко не весь список методів захисту, які відомі на сьогоднішній день, що використовуються для збереження приватності спілкування користувачів та від несанкціонованого доступу до акаунтів користувачів соціальних мереж, які і надалі продовжують розвиватися та стають великою перепоною для зловмисників.

Взявши до уваги такі непереборні методи та алгоритми захисту конфіденційної інформації користувачів, які в останній час набули великого розвитку, хакери почали стрімко розвивати атаки за допомогою соціальної інженерії. За до-

[1)] Є розробником та власником відомого месенджеру «Telegram».

[2)] Є власником соціальних мереж «Instagram» та «Facebook» та месенджеру «WhatsApp»

помогою методів соціальної інженерії, а саме фішинг, цільовий фішинг, спуфінг

електронної пошти, претекст, атака «Щось за щось» («Quid pro quo»), атака через програми-вимагачі, які можуть поширюватися через банери в клонах популярних вебсайтів та вішинг, злочинці, які навіть можуть не мати практичних навичок створення шкідливого ПЗ, можуть отримати доступ до конфіденційної інформації цілі, до якої було здійснено неправомірні дії.

Примітки:

1 Відмінність цільового фішингу від звичайного полягає в тому, що для його здійснення потрібна більш складніша та якісніша підготовка.

2 Претекст - підміна особи з метою отримання інформації про особу, яку підмінили.

3 Сутність атаки «Щось за щось» - отримання важливих послуг або інформації жертвою та отримання конфіденційної інформації про жертву хакером або іншим порушником.

4 Вішинг - вид шахрайства, пов'язане з виманюванням конфіденційної інформації про жертву в телефонному режимі або за допомогою завчасно записаних голосових повідомлень.

Злочинці не обмежуються лише соціальною інженерією. Вони вивчають новітні захисні методи, а отже, і покращують ПЗ, яке викрадає та передає зловмиснику інформацію, що цікавить його. Прикладом є кейлогери, які фіксують, наприклад, у встановлений алгоритмом файл, введену на клавіатурі жертвою інформацію, до якої можна віднести логіни та паролі від облікових записів соціальних мереж, та передають її до зловмисника за допомогою Інтернету. Також хакери можуть використати бекдори - віруси, які набули за останні 10 років великої популярності та які під виглядом драйвера одного із основних компонентів ПК дозволяють розробнику шкідливого ПЗ віддалено керувати ПК жертви. Хоч найрозповсюдженішою причиною використання бекдору є створення ботнету[1)], проте за допомогою цього вірусу порушники можуть отримати і доступ до облікових даних користувачів соцмережами.

У свою чергу, користувачі, які не навчені кібергігієні, мають низький рівень технічних знань та знань про сучасні кіберзагрози, дуже вразливі до атак, що ґрунтуються на методах соціальної інженерії та потребують захисту від атак

[1)] Ботнет - логічна комп'ютерна мережа, що складається з хостів, на яких запущено автономне ПЗ.

даного виду. Навіть ті, хто має знання про забезпечення своєї безпеки від кібершахрайства, все одно вразливі до впиву таких атак, адже соціальна

інженерія спирається не лише на необізнаність та неграмотність цілі, до якої виконуються неправомірні дії. Усі найвідоміші соціальні мережі та месенджери, наприклад, «Telegram», «Viber», «Instagram», «Facebook», все ще залишаються вразливими до зламів через програмні засоби, проте в меншій мірі, ніж до атак, що ґрунтуються на методах соціальної інженерії, оскільки випадки заволодіння акаунтом таким чином більш поширені. Розвиток і поширення зламу у такий спосіб вказує на те, що соцмережі потребують новітніх методів захисту.

З розвитком штучного інтелекту та технології машинного навчання описана вище проблема може отримати програмне вирішення. ШІ може стати потужним інструментом для запобігання шахрайствам та обману, оскільки він має великий потенціал з пошукової та аналітичної роботи, яку може виконувати людина. За допомогою технології машинного навчання Одними з нових досліджень та відкриттів в галузі кібербезпеки можуть стати використання ШІ для запобігання злочинам різних видів у кіберпросторі.

Метою цієї кваліфікаційної роботи є не лише дослідження та вивчення існуючих методів захисту конфіденційної інформації користувачів в соціальних мережах, а також і надання початківцям та професіоналам в галузі кібербезпеки та захисту інформації нових ідей з використання ШІ та технології машинного навчання, наприклад, використання ШІ для захисту користувача від атаки «Щось за щось».

Завданням цієї роботи є дослідження шифрування текстових та голосових повідомлень та наявності метаданих в фотографіях, що надсилаються в соціальній мережі «Instagram» та месенджерах «Telegram» та «Viber».

Отримані в цій роботі результати можуть слугувати ґрунтом для створення нового стартапу, сутність якого полягає у створенні українського новітнього продукту, месенджеру або соцмережі, який не лише забезпечить надійний зв'язок та розважить людей, а також захистить від шахраїв та зловмисників у кіберпросторі. Це дослідження дозволить зрозуміти, як фахівці з кібербезпеки можуть використовувати штучний інтелект та технологію машинного навчання для захисту персональних даних користувачів у вже наявних соцмережах та

месенджерах та що можна покращити у вже наявних програмних та криптографічних методах захисту інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

У цьому розділі буде зроблено загальний огляд соціальної мережі «Instagram» та месенджерів «Telegram» та «WhatsApp», їх можливості та призначення, загальну структуру їх функціонування. Буде розглянуто види інформації, що використовується та обробляється в них, а також останні новини про випадки зломів або збоїв цієї соцмережі та цих месенджерів. Буде розроблено загальну інструкцію з вивчення методів та механізмів захисту інформації та персональних даних користувачів.

1.1 Стан питання

1.1.1 Огляд соціальної мережі «Instagram» та її функціональні можливості

«Instagram» - соціальна мережа, створена 6 жовтня 2010 року компанією «Instagram Inc.» та яка має закритий вихідний код. Базується на обміні фотографіями, дозволяє користувачам робити фотографії, застосовувати до них фільтри, а також поширювати їх через свій сервіс і низку інших соціальних мереж та месенджерів. Належить компанії «Meta Platforms». Є одним із найпопулярніших сервісів у мистецтві мобілографії[1)]. Фотографії у «Instagram» мають квадратну форму - як в камерах компаній «Eastman Kodak Company»[2)] і «Polaroid Corporation»[3)], тоді як більшість мобільних фоторедакторів використовує співвідношення сторін 3:2.

Застосунок на мобільних пристроях сумісний зі специфікацією «IPhone», «IPad» і «IPod» на ОС «IOS» версії 4.0 і вище, а також зі смартфонами на ОС «Android» версії 4.2.2 і вище з підтримкою «OpenGL ES» версії 2.0 і вище, а також

[1)] Мобілографія - різновид фотографічного мистецтва, в якому інструментом слугують портативні електронні прилади з вбудованою цифровою фотокамерою, основним призначенням яких не є фотографування.

[2)] «Eastman Kodak Company» - американська компанія, всесвітньо відомий виробник фототехніки та фото- і кінотоварів.

[3)] «Polaroid Corporation» - американська компанія, що виробляє фототехніку й побутову електроніку (LCD-телевізори, портативні DVD-плеєри, цифрові фоторамки). Широко знана як виробник фотоапаратів, що дозволяють робити моментальні фотознімки.

доступний для смартфонів, на яких встановлена ОС «Windows Phone» версій 8 та

8.1. Офіційна та актуальна версія застосунку для мобільних пристроїв на ОС «IOS» поширюється через «App Store», на ОС «Android» - «Google Play», на ОС «Windows Phone» - «Windows Marketplace». Також існує вебверсія для браузерів «Google Chrome», «Microsoft Edge», «Opera», «Mozilla Firefox», «Safari», починаючи з версій, в яких є підтримка «JavaScript».

На рисунку 1.1 зображено сторінку користувача соціальної мережі «Instagram» на мобільному пристрої «IPhone 11».

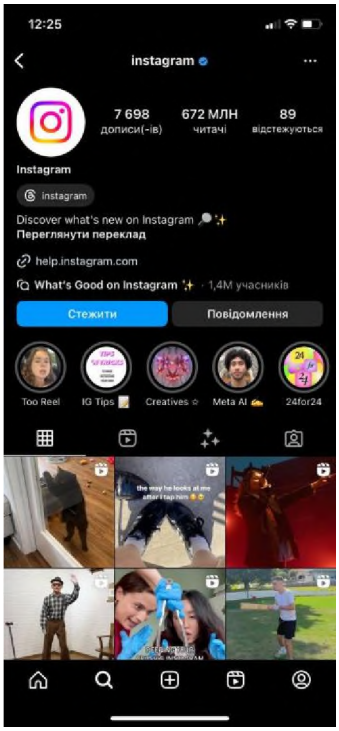


Рисунок 1.1 - Сторінка користувача соціальної мережі «Instagram»

Серед можливостей «Instagram» можна виділити наступні основні функції:

· редагувати властивості профілю облікового запису після реєстрації;

· створювати, публікувати, редагувати, видаляти дописи в стрічку профілю;

• додавати до дописів місцерозташування;

• обмежувати перегляд вмісту власної стрічки профілю для інших користувачів (приватний обліковий запис);

- пошук інших користувачів;
- надсилати, керувати та видаляти повідомлення, в тому числі відеоповідомлення та голосові повідомлення, надіслані іншим користувачам та переглядати повідомлення від інших користувачів;
- виконувати та приймати аудіо- та відеовиклики;
- створювати групові чати, в яких може бути до 250 користувачів;
- створювати чати, що захищені наскрізним шифруванням, в яких доступне надсилання, керування та видалення повідомлень, в тому числі відео-повідомлень та голосових повідомлень, надіслані іншим користувачам та переглядання повідомлень від інших користувачів, здійснення та прийняття аудіо- та відео-викликів;
- починати та планувати трансляцію в реальному часі (далі пряма трансляція), переглядати прямі трансляції інших користувачів.

Примітка. В соціальній мережі «Instagram» існує декілька видів дописів: одинарні фото або відео; публікація, що складається з декількох фото або відео та яка називається «карусель»; короткі відео, що називаються «Instagram Reels»; розповіді, що називаються «Instagram Stories» - короткі вертикальні відео або фото, які зникають з профілю користувача за 24 години та більше недоступні для перегляду іншим користувачам; вибрані розповіді, що називаються «Highlights» - це розповіді, які користувач зберіг у своєму профілі й які можна переглядати за посиланням в профілі; запис прямої трансляції, що зберігається у стрічку профілю користувача.

В «Instagram» створюється та обробляється різноманітна інформація, яку можна класифікувати за декількома категоріями. Основні категорії класифікації, види інформації в категорії та назви інформації, що відносяться до наведеного виду, наведені в таблиці 1.1.

Таблиця 1.1 - Класифікація інформації, що створюється та обробляється в соціальній мережі «Instagram»

Назва категорії класифікації	Вид інформації	Назва інформації
За формою подання	Текстова	Описи дописів, імена користувачів (ніки), імена та прізвища профілів користувачів, якщо вказані, описи профілів користувачів (біографії), контактні дані користувачів, статистична інформація, назва та опис опцій налаштувань, текстове повідомлення
	Графічна	Фотографії, основна фотографія профілю, діаграми, графічне повідомлення (фотографія, скріншот тощо), емоджі, 3D-моделі, піктограми пунктів налаштувань, QR-коди
	Візуальна	Відео без звуку, відеоповідомлення без звуку, GIF
	Звукова	Музичне супроводження дописів, голосове повідомлення
	Візуально-звукова	Відео зі звуком, допис із музичним супроводженням
За призначенням	Особисте спілкування	Текстові повідомлення, голосові повідомлення, відеоповідомлення
	Розважальна	Дописи користувачів з професійним типом облікового запису, які входять до наступних категорій: «Митець», «Блогер», «Спільнота», «Автор цифрового контенту», «Особистий блог», «Геймер»
	Професійна	Дописи та контактна інформація користувачів з професійним типом облікового запису
	Статистична	Рекламна статистика, статистика переглядів дописів, статистика часу, проведеного в «Instagram»
За режимом доступу	Відкрита	Імена користувачів (ніки), біографії, основні фотографії профілів; дописи та контактні дані користувачів, доступ до яких дозволений користувачами
	Конфіденційна	Дописи та контактні дані користувачів, доступ до яких обмежений користувачами, особиста інформація користувачів

1.1.2 Випадки злому «Instagram»

Випадки злому та отримання несанкціонованого доступу до акаунту користувача «Instagram» хакерами - розповсюджене явище. З 2016 року кількість зломів облікових записів «Instagram» щороку невпинно зростає. За даними від компанії «ITRC», серед одного мільйону звернень до цієї компанії за 2021 рік 85% звернень мали ідентичну тематику - втрата доступу або злом акаунту «Instagram». Основна причина втрати - довіра та неграмотність в сфері кібербезпеки, типові

риси, на які спираються хакери та шахраї, здійснюючи атаки, що ґрунтуються на методах соціальної інженерії. Зловмиснику достатньо дізнатись про адрес електронної пошти або мобільний номер телефону користувача, щоб заволодіти обліковим записом.

На початку весни 2024 року генеральний прокурор штату Пенсильванія Сполучених Штатів Америки Мішель Генрі повідомила, що вона разом з 40 іншими генеральними прокурорами штату надіслали лист до компанії «Meta», власника «Instagram». У листі було прохання провести розслідування збільшення випадків злому акаунтів «Instagram» та «Facebook», що призводить до викрадення зламаних облікових записів, їх блокування, викрадення особистої інформації та розміщення через них шкідливого контенту. У проханні генеральний прокурор наводить дані, які свідчать про те, що активність зловмисників значно зросла за останні роки - у Пенсільванії злам акаунтів «Instagram» та «Facebook» зросли на 270% з 2022 по 2023 рік - водночас запитуючи компанію, що вона робить, щоб запобігти зламам і як реагує на скарги від жертв. Жертви неправомірних дій з боку хакерів у свої зверненнях до прокуратури щодо втрати облікового запису скаржаться на те, що під час звернення до служби підтримки клієнтів компанії «Meta» їм відповідає автоматизована система, а не консультант. Можливо, збільшення кількості викрадень акаунтів «Instagram» та «Facebook» пов'язане з тим, що нещодавно компанія-власник цих соціальних мереж звільнила близько 11 тис. працівників, серед яких більшість, за словами самої компанії, становили працівники сектору безпеки, конфіденційності та цілісності.

Одним з найвідоміших випадків злому акаунтів користувачів «Instagram» став інцидент, що відбувся наприкінці серпня 2017 року. Тоді група хакерів скористувалася помилкою в API Instagram, яка дозволяла отримати адрес електронної пошти та номер телефону користувача, які використовуються в обліковому записі. За результатами зловмисних дій була створена база даних, що називалася «Doxagram» та в якій знаходилися дані про 6 мільйонів облікових записів, серед яких були акаунти знаменитостей, серед яких була і Селена Гомес.

1 вересня 2017 року технічний директор «Instagram» Майк Крігер опублікував заяву , в якій говориться, що команда соціальної мережі виправила помилку, і, на їхню думку, вона вплинула лише на «низький відсоток облікових записів «Instagram». Але для програми з 700 мільйонами користувачів (станом на 19 вересня 2017 року) навіть низький відсоток облікових записів все одно є великою цифрою. Якщо вірити творцям бази даних «Doxagram», то цей інцидент торкнувся 0,8% відсотка від загальної кількості користувачів.

1.1.3 Огляд месенджеру «Telegram»

«Telegram» - багатоплатформовий месенджер, що надає можливість користувачам миттєво обмінюватись текстовими, аудіо- та відео-повідомленнями, здійснювати дзвінки та відео-дзвінки тощо. Розробниками та власниками є компанії «Telegram FZ LLC» та «Telegram Messenger Inc.». Був запущений для мобільних телефонів та планшетів з ОС «IOS» 14 серпня 2013 року та для мобільних телефонів та планшетів з ОС «Android» 20 жовтня 2013 року. Має відкритий вихідний код, окрім серверної частини, оскільки вона використовує власні криптографічний протокол «MTProto» та мережевий протокол «MTProxy», тому ця частина має закритий вихідний код і є власністю компаній-розробників. У серпні 2023 року кількість щомісячних активних користувачів месенджером перевищив 800 мільйонів. Є найпопулярнішим додатком для обміну миттєвими повідомленнями в Україні.

Месенджер має наступні клієнтські застосунки:

- «Telegram Messenger» - мобільний клієнт для ОС «IOS» версії 9.0 і вище, присутні регулярні оновлення та клієнтська підтримка, робота над застосунком підтримується;
- «Telegram» - мобільний клієнт для ОС «Android» версії 4.1 і вище, присутні регулярні оновлення та клієнтська підтримка, робота над застосунком підтримується;
- «Telegram X» - мобільний клієнт для ОС «Android» версії 4.1 і вище та для ОС «IOS» версії 8.0 і вище, присутні

регулярні оновлення та клієнтська підтримка, робота над застосунком підтримується (окрім застосунку для ОС «IOS»);

· «Telegram Messenger» - мобільний клієнт для ОС «Windows Phone» версії 8.1 і вище, присутні регулярні оновлення та клієнтська підтримка, робота над застосунком підтримується;

· «Telegram Desktop» - десктопний клієнт для ОС «Windows» версії 7 та вище, для ОС «macOS» версії 10.10 і вище, для дистрибутивів ОС «Linux», присутні регулярні оновлення та клієнтська підтримка, робота над застосунком підтримується;

· «Telegram» - спеціальний десктопний клієнт для ОС «macOS» версії 10.11 і вище, присутні регулярні оновлення та клієнтська підтримка, робота над застосунком підтримується;

• «Telegram Web» - старий вебзастосунок, який заміняється новим вебзастосунком, відсутні регулярні оновлення, присутня клієнтська підтримка, робота над застосунком не відбувається;

· «Telegram Web A» - новий вебзастосунок, який перебуває на стадії альфа-тестування та доступний за посиланням web.telegram.org, присутні регулярні оновлення та клієнтська підтримка, робота над застосунком підтримується;

· «Telegram» - вебзастосунок для браузера «Google Chrome», який розроблений на основі «Telegram Web», присутні регулярні оновлення та клієнтська підтримка, робота над застосунком підтримується;

На рисунку 1.2 можна побачити головну сторінку з останніми активними чатами в десктопному додатку «Telegram Desktop» версії 1.0.

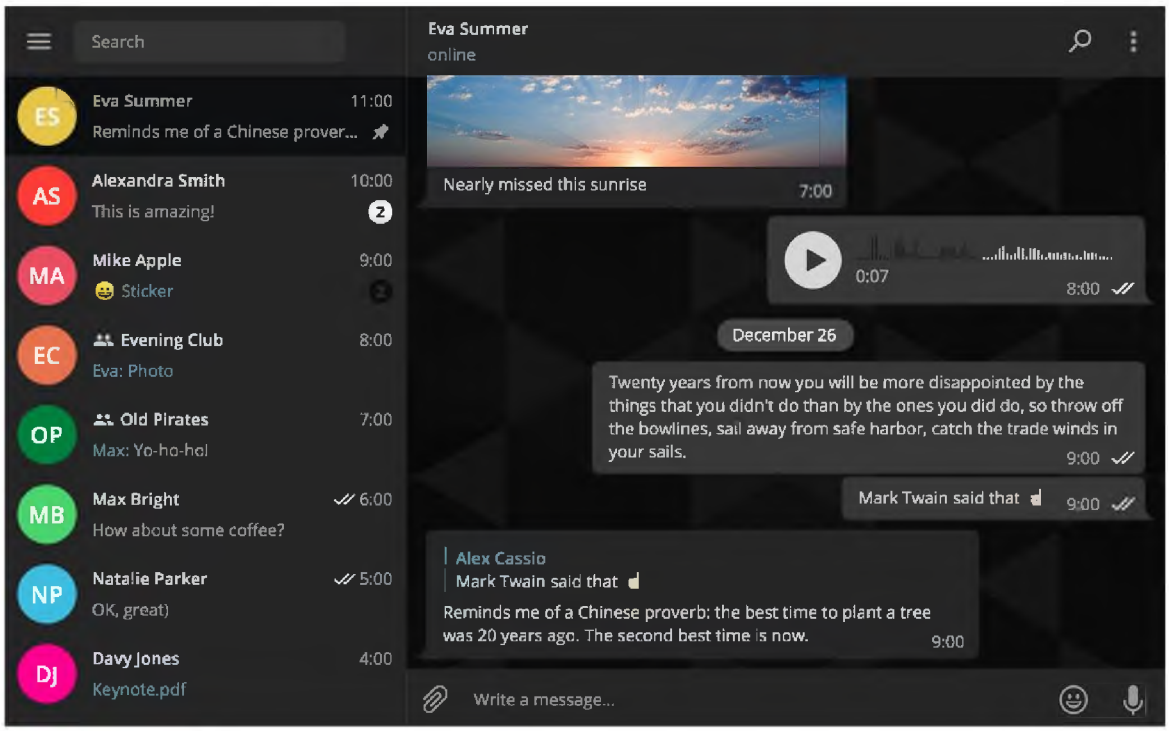


Рисунок 1.2 - Головна сторінка додатку «Telegram Desktop»з останніми активними чатами

Месенджер «Telegram» надає багатий вибір можливостей, що спрощує його використання, комунікацію з іншими користувачами та робить спілкування приємним. Серед усіх його можливостей основними можна визначити наступні:

- редагування властивостей профілю облікового запису після реєстрації;
- надсилати, редагувати, видаляти, переглядати, прикріпляти текстові повідомлення;
- створювати «секретні чати», що захищені наскрізним шифруванням;
- надсилати, видаляти, переглядати прикріпляти голосові повідомлення та відеоповідомлення;
- надсилати, видаляти, завантажувати файли розміром до 2 ГБ для звичайних користувачів, для користувачів підписки «Telegram Premium» - до 4 ГБ;

- пошук інших користувачів, каналів, чатботів[1)], повідомлень за ключовими словами;
- створювати групові чати на 200 000 учасників;
- поширювати іншим користувачам в приватних та групових чатах власну геопозицію;
- створювати публічні, тобто мають необмежений доступ та можуть бути знайдені через пошук додатка, та приватні, тобто доступ до яких здійснюється через згенероване посилання та які неможливо знайти через пошук, канали, що являють собою стрічку з повідомлень та мають елементи блогу. Користувачі підписуються на канал та отримують повідомлення, надсилати повідомлення можуть лише адміністратори каналу;
- здійснювати аудіо- та відеодзвінки та відповідати на них;
- створювати та приймати участь в групових відеочатах;
- створювати та використовувати чатботів у приватних, групових чатах та каналах;
- створювати, видаляти свої та переглядати створені іншими користувачами історії;
- обмежувати можливість перегляду персональних даних, таких як мобільний телефон, дату народження, основне та інші фото профілю, а також обмежувати можливість надсилання повідомлень до користувача від інших користувачів;
- керування активними сесіями на різних пристроях, де виконаний вхід до облікового запису.

Примітки.

1 Прикріплення повідомлення - це створення посилання на повідомлення, яке візуально закріплюється вгорі віджету повідомлень. Посилання має текст повідомлення, на яке воно

створене, і при натисканні на нього чат автоматично прокручується до повідомлення, на яке вказане посилання, і виділяє його кольоровим ефектом.

2 Історія в месенджері «Telegram» - це опубліковане в профілі фото та відео, які можуть містити текстові написи та які зникають через певний проміжок часу.

[1)] Чат-бот - це програма штучного інтелекту, яка імітує інтерактивну розмову людини за допомогою ключових, заздалегідь розрахованих фраз користувача, та слухових або текстових

«Telegram» є найпопулярнішим месенджером в Україні, отже, в ньому створюється та обробляється велика кількість різної інформації, яку можна класифікувати за великою кількістю категорій. Класифікацію інформації за основними категоріями, їх види та назву приведено в таблиці 1.2.

Таблиця 1.2 - Класифікація інформації, що створюється та обробляється в соціальній мережі «Telegram»

Назва категорії класифікації	Вид інформації	Назва інформації
За формою подання	Текстова	Імена користувачів, імена та прізвища профілів користувачів, описи профілів (біографія), назви групових чатів або каналів, контактні дані користувачів, текстові повідомлення, назви пунктів та опис налаштувань, статистична інформація
	Графічна	Основні та інші фото профілів та групових чатів, фото каналів, фото історій, діаграми, емодзі, піктограми пунктів налаштувань, графічне повідомлення (фотографія, скріншот тощо), QR-коди
	Візуальна	Відео без звуку, відеоповідомлення без звуку, відео без звуку в історіях GIF
	Звукова	Аудіоповідомлення, музичний або аудіо супровід історій
	Візуально-звукова	Відео зі звуком в повідомленнях або історіях, відеоповідомлення зі звуком
За призначенням	Особисте спілкування	Текстові повідомлення, голосові повідомлення, відеоповідомлення в групових та приватних чатах
	Розважальна	Текстові, голосові повідомлення та відеоповідомлення в каналах
	Статистична	Інформація про розмір кешованих голосових повідомлень, відеоповідомлень, фото та відео з чатів та каналів інформація про використання інтернет мережі та мобільного інтернету.
За режимом доступу	Відкрита	Імена користувачів, імена та прізвища профілів користувачів; основні та інші фото профілів, контактні дані, описи профілів (біографія), дати народження, якщо доступ

		до них дозволений користувачами; фото, відео, текстові повідомлення в каналах та групових чатах, фото та відео з історій

Продовження таблиці 1.2

Назва категорії класифікації	Вид інформації	Назва інформації
	Конфіденційна	Основні та інші фото профілів, контактні дані, описи профілів (біографія), дати народження, якщо доступ до них обмежений користувачами, фото, відео, текстові та голосові повідомлення в каналах та приватних чатах

1.1.4 Випадки злому «Telegram»

З 2013 року, з року заснування месенджеру, не було зафіксовано масштабних випадків злому акаунтів користувачів, проте поодинокі випадки злому все ще виникають. Хакери та представники спеціальних служб безпеки певних країн (яких саме буде розглянуто нижче) через методи соціальної інженерії, зокрема SMS-спуфінг, намагаються отримати доступ до облікових записів користувачів.

Спробу злому декількох акаунтів російських журналістів в месенджері «Telegram» представниками Федеральної Служби Безпеки Російської Федерації було зафіксовано в 2019 році та про яку доповів один із засновників месенджеру російський підприємець Павло Дуров. За словами Дурова, причиною спроби стали висловлювання журналістів про протести проти будування православного храму на місці скверу в Єкатеринбурзі. Ця спроба не мала успіху, оскільки жертви мали в своїх облікових записах мали налаштовану двофакторну аутентифікацію, проте чому в цьому замасі на отримання несанкціонованого доступу до акаунтів підозрюються саме працівники ФСБ РФ, він не пояснив.

Також про спроби злому в 2019 році повідомляли низка російських опозиційних журналістів, такі як головний редактор єкатеринбурзького видання «Znak.com» Дмитро Колєзєв, заступник головного редактора єкатеринбурзького видання «Znak.com» Антон Ольшанніков, журналіст видання «Meduza» Дмитро Андрєєв та позаштатний кореспондент видання «Радіо Свобода» в Псковській області РФ Людмила Савицька. Ці спроби здійснювались з іспанської IP-адреси.

Також на початку 2024 року були зафіксовані спроби злому акаунтів білоруських користувачів месенджеру «Telegram» представниками білоруської

спеціальної служби безпеки. Користувачі, у яких не налаштована функція двофакторної аутентифікації, є в групі ризику й існує можливість, що їх конфіденційна інформація з їх облікових записів може бути відома представникам силових структур Білорусі.

1.1.5 Зв'язок «Telegram» з Федеральною Службою Безпеки Російської Федерації

Месенджер «Telegram», як було з'ясоване раніше, має російське походження, тому є можливість перехоплення повідомлень російськими силовими структурами через політичний режим Російської Федерації. Незважаючи на заяви одного із власників месенджеру Павла Дурова, що «Telegram» є втіленням ідеї їхньої команди про світ, в якому кожен має право бути вільним, останнім часом виникають доволі суперечливі ситуації навколо платформи для моментального обміну повідомленнями.

В дослідженні видання «Wired» вказано детальну історію розвитку відносин між ФСБ РФ та «Telegram». У 2018 році Роскомнагляд заблокував месенджер через відмову за наказом ФСБ надати ключі шифрування, що використовуються для російських користувачів. Проте в 2020 році, можливо, влада Російської Федерації домовилась з керівниками «Telegram» щодо розблокування на тлі фінансових проблем компанії-розробника платформи для обміну повідомленнями. З початком повномасштабної агресії Росії проти України, за словами видання, «Telegram» стає основним інструментом розповсюдження російської пропаганди. «Wired» з'ясувало, що за два тижні до блокування Роскомнаглядом соціальної мережі «Facebook», в телеграм-каналі російського уряду було підведено підсумок зустрічі віце-прем'єра Дмитра Чернишенка з лідерами IT-індустрії, на якій він заявив, що держорганам рекомендовано створювати акаунти в Telegram і «ВКонтакті». Також це видання з'ясувало, що, можливо, працівники силових структур РФ використовують API «Telegram» для збору інформації про користувачів та про їхню діяльність на цій платформі, оскільки API надає широкий спектр можливостей і немає обмежень з

використання користувачами, бо будь-який користувач, маючи відповідний ключ, він же токен API, може його використовувати.

Про можливий зв'язок ФСБ з «Telegram» можуть вказувати блокування ботів в месенджері, що є протидіючими засобами проти влади РФ. У 2021 році, за день до виборів був заблокований бот, створений командою російського опозиціонера Олексія Навального з метою організованого голосування за альтернативних кандидатів на виборах у Державну думу РФ. За словами керівників месенджеру, блокування відбулось через недотримання командою опозиціонера «дня тиші»[2)]. У кінці квітня 2024 року «Telegram» заблокував низку ботів, створених урядовими органами та структурами України для протидії російській військовій агресії та збору інформації про неї, зокрема таких ботів, як «єВорог» та «Головний бот розвідки», проте через декілька годин розблокував лише тих ботів, які були призначені лише для збору інформації. В своїй заяві команда месенджеру повідомила, що вони блокують облікові записи та ботів, які призначені для цільових ударів або закликів до насильства, оскільки не бажають розповсюджувати через «Telegram» насильництво.

Примітки.

1 «єВорог» - бот в месенджері «Telegram», створений Міністерством цифрової трансформації України з метою збору інформації про пересування російських військ.

2 «Головний бот розвідки» - бот в месенджері «Telegram», створений Головним управлінням розвідки Міністерства оборони України з метою створення офіційного каналу зв'язку для жителів тимчасово окупованих територій України з Головним управління розвідки МО України.

Месенджер також використовується російськими службами спеціального призначення для вербування українців з метою створення провокацій та

[1)] «День тиші» - неформальна назва дня безпосередньо перед виборами, коли заборонена агітація. «День тиші» у виборчій практиці також позначають термінами «період тиші» або «день роздумів».

диверсійної діяльності. Восени 2023 року Служба безпеки України виявила мережу з каналів в «Telegram», які вербували українських підлітків віком від 13 до 17 років для створення антисемітських провокацій та псування пам'ятників, що присвячені Голокосту.

1.1.6 Огляд месенджеру «WhatsApp»

«WhatsApp» - багатоплатформовий месенджер, що має закритий вихідний код, права на який належать компанії «Meta Platforms Inc.» та створений в 2009 році програмістами Яном Кумом і Браяном Ектоном. До 2016 року використовувався лише на мобільних пристроях з операційними системами «IOS», «Android», «Symbian Series 40»[1)] та «Windows Phone». У 2016 році були створені перші десктопні версії клієнтів для комп'ютерів з операційними системами «Windows» та «macOS». Месенджер працює лише через номери мобільних телефонів та використовує їх для встановлення ідентифікації та унікальності користувача

На сьогоднішній час «WhatsApp» доступний для мобільний пристроїв та комп'ютерів та має клієнтські додатки для таких ОС:

- «IOS» версії 12.0 та вище;
- «Android» версії 4.0.3 та вище;
- «macOS» версії 11 та вище;
- «Windows» версії 10 та вище.

Також існує вебзастосунок, що доступний за посиланням web.whatsapp.com та запускається на браузерах «Google Chrome», «Opera», «Mozilla Firefox», «Microsoft Edge», «Safari», починаючи з версій, в яких наявна підтримка «JavaScript».

На рисунку 1.3 продемонстровано головну сторінку з останніми активними чатами десктопного додатку месенджеру «WhatsApp».

[1)] Symbian Series 40 - операційна система та інтерфейс користувача, що використовувалась в деяких мобільних пристроях «Nokia».

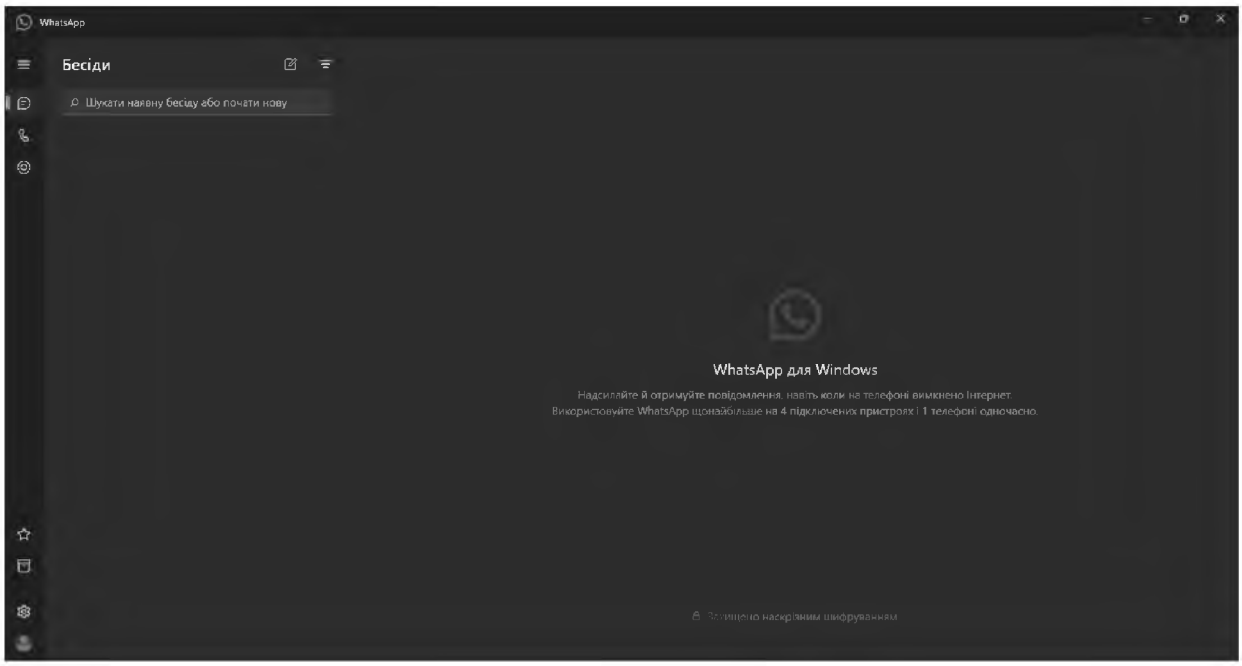


Рисунок 1.3 - Головна сторінка десктопного додатку месенджеру «WhatsApp»

«WhatsApp» має великий спектр можливостей для спрощення процесу комунікації та забезпечення безпеки цього процесу, що робить його комфортною та досить безпечною платформою для обміну миттєвими повідомленнями. Головна риса месенджеру - встановлення за замовчуванням для всіх чатів використання наскрізного шифрування, яке неможливо вимкнути. Серед всіх можливостей WhatsApp можна виділити такі основні функції:

- редагувати номеру телефону та ім'я користувача профілю облікового запису;
- надсилати, видаляти, переглядати текстові, голосові повідомлення та відеоповідомлення;
- надсилати, видаляти, завантажувати файли розміром до 2 ГБ;
- здійснювати та приймати аудіо- та відеодзвінки;
- створювати, видаляти спільноти, що складаються з груп, та приєднуватись до них;

· створювати та приймати участь в групових відеочатах до 32 одночасних учасників;

· створювати, видаляти та підписуватись на канали;

• пошук повідомлень за видом, тобто знайти тільки фото, відео, посилання тощо, пошук за ключовими словами та пошук користувачів серед власних контактів;

• створювати, видаляти та переглядати статуси.

Примітка. Статус в «WhatsApp» є аналогом історій в «Telegram» - через 24 години фото, відео або текст, опублікований в статусі, зникне.

«WhatsApp» надає можливості для обробки та створення різноманітної інформації, яка класифікується за різними категоріями. Основні категорії класифікації, види та назви інформації в месенджері наведено в таблиці 1.3.

Таблиця 1.3 - Класифікація інформації, що створюється та обробляється в соціальній мережі «WhatsApp»

Назва категорії класифікації	Вид інформації	Назва інформації
За формою подання	Текстова	Імена профілів користувачів, персональні дані користувачів, назви спільнот та каналів, назви та опис пунктів налаштувань, опис статусів, текст в статусах користувачів, текстові повідомлення в приватних та групових чатах і каналах, статистична інформація
	Графічна	Фото профілів, спільнот та каналів, фото статусів, діаграми, емодзі, піктограми пунктів налаштувань, графічне повідомлення (фотографія, скріншот тощо), 3D-моделі, QR-коди
	Візуальна	Відеоповідомлення без звуку, відео в повідомленні або в статусі без звуку
	Звукова	Аудіоповідомлення
	Візуально-звукова	Відеоповідомлення зі звуком, відео в повідомленні або в статусі зі звуком
За призначенням	Особисте спілкування	Текстові повідомлення, голосові повідомлення, відеоповідомлення в приватних чатах та спільнотах
	Розважальна	Текстові, голосові повідомлення та відеоповідомлення в каналах

Продовження таблиці 1.3

Назва категорії класифікації	Вид інформації	Назва інформації
	Статистична	Інформація про розмір кешованих голосових повідомлень, відеоповідомлень, фото та відео з чатів, спільнот та каналів
За режимом доступу	Відкрита	Фото, відео, текст в каналах
	Конфіденційна	Персональні дані користувачів; фото, відео, текстові та голосові повідомлення з приватних чатів та спільнот

1.1.7 Випадки злому «WhatsApp»

З моменту заснування месенджеру «WhatsApp», він завжди був одною з центральних фігур в новинах про кібербезпеку різних газет та журналів, проте останнім часом випадків злому цієї платформи для обміну повідомленнями стало менше і вони набули менш масштабного характеру, як це було на початку.

У вересні 2012 року була виявлена можливість отримання несанкціонованого доступу до акаунтів «WhatsApp» за допомогою «WhatsAPI», неофіційного API цього месенджеру, серійного номеру пристрою (IMEI) для смартфонів та планшетів з ОС «Android» або MAC-адреси інтерфейсу мережі Wi-Fi для смартфонів та планшетів з ОС «IOS». Було з'ясовано, що IMEI або MAC-адрес використовуються клієнтським додатком для внутрішнього генерування пароля для входу на сервер. Зловмисники, зробивши сценарії з використанням «WhatsAPI» та підставивши в ці сценарії IMEI або MAC-адрес пристроя жертви, можуть надсилати від імені облікового запису жертви та отримувати повідомлення, що надходять до облікового запису жертви, при цьому жертва на своєму пристрої не могла побачити надісланих та отриманих повідомлень. Після повідомлення про цей інцидент керівництво «WhatsApp» надіслало розробникам API ультиматум, що вимагав від розробників інтерфейсу переведення його в автономний режим, та в разі невиконання цього ультиматуму компанія зробить судовий позов проти них. Ультиматум був виконаний, і робота над «WhatsAPI» була припинена.

У грудні 2014 року два індійські незалежні дослідники безпеки, 17-річні Індраджит Бхуян і Саурав Кар повідомили та надали відеопідтвердження про вразливість мобільного додатку «WhatsApp». Вона полягає в тому, що повідомлення, складене з певних символів, надіслане жертві та яке має розмір 2 КБ, змушує аварійно завершити роботу мобільного застосунку, окрім того, після першого аварійного завершення роботи, повторне відкриття чату зі шкідливим повідомленням все одно викликає програмний збій. Лише повне видалення чату

зі шкідливим повідомленням вирішує проблему. Станом на зараз ця проблема вирішена та не є актуальною.

У січні 2015 року після першого запуску вебзастосунку «WhatsApp Web» дослідник безпеки Індраджит Бхуян повідомив про вразливості забезпечення конфіденційності користувачів в ньому. За його словами, перша вразливість полягає в тому, що якщо в налаштуваннях конфіденційності зображення профілю встановити пункт «Лише контакти», тобто бачити фото профілю можуть лише ті користувачі, які наявні в книзі контактів користувача, користувачі, що не перебували в цій книзі, все одно могли побачити зображення профілю через вебзастосунок. Друга вразливість була пов'язана із функцією синхронізації фото між вебзастосунком та мобільним додатком. Після того, як користувач видаляє фотографію, надіслану через мобільну версію програми «WhatsApp», вона стає недоступною для перегляду. Однак те саме фото, яке вже було видалено користувачем із мобільного застосунку, може бути доступним у «WhatsApp Web», оскільки фото не видаляється з нього, що вказувало на те, що мобільний клієнт та вебклієнт месенджеру не синхронізовано належним чином.

У кінці серпня 2018 року Наталі Сільванович виявила чергову вразливість в «WhatsApp» - хакери могли заволодіти обліковим записом жертви, коли вона відповідала на вхідний відеодзвінок в застосунку. Вона також опублікувала інструкцію для реалізації вразливості. Ця вразливість стосувалась лише додатків для мобільних пристроїв з ОС «Android» та «IOS», і була пов'язана з неправильним пакетом транспортного протоколу реального часу «RTP». Команда розробників «WhatsApp» виправила проблему в наступному оновленні, що вийшло 28 вересня.

У жовтні 2018 року в Ізраїлі був спалах зломів акаунтів «WhatsApp». Хакери намагались увійти до облікового запису жертви, намагаючись ввести одноразовий код після вводу номеру телефону жертви. Після невдалих спроб вводу месенджер пропонував повторення одноразового коду через дзвінок на мобільний номер телефону. Якщо жертва не приймає дзвінок, він потрапляє до голосової пошти, доступ до якої більшість ізраїльських мобільних провайдерів

надавали віддалено та надається після вводу паролю від облікового запису голосової пошти. Якщо пароль є шаблонним або простим, зловмисник міг отримати доступ до голосової пошти жертви та відтворити одноразовий код для входу в акаунт «WhatsApp», після чого хакер отримує доступ до акаунту. Вперше про цей метод злому повідомив ще у 2017 році Ран Бар-Зік.

У 2016 році шахраї за допомогою обману змушували користувачів «WhatsApp» завантажувати їх додаток. Вони пропонували, за їх словами, зареєструватись через вебсайт і отримати ексклюзивні версії месенджеру під назвою «WhatsApp Gold» або «WhatsApp Plus», які нібито були доступні знаменитостям та мали розширений функціонал: відеодзвінки, нові емоджі, розширені функції безпеки тощо. Після завантаження та встановлення псевдо-месенджерів на пристрій жертвою, злочинці мали доступ до конфіденційної інформації жертви, яку вони могли передавати третім особам. Після скарг від користувачів команда «WhatsApp» почала блокувати користувачів, в яких були встановлені фальшиві версії месенджеру та закликати користувачів не встановлювати їх.

1.2 Постановка задачі

Для проведення дослідження та вивчення існуючих методів захисту конфіденційної інформації користувачів в соціальних мережах, використовувалась наступна інструкція:

- перевірка шифрування текстового повідомлення у десктопному додатку соціальної мережі «Instagram» через перевірку мережевих пакетів даних в сніфері пакетів «Wireshark»;
- перевірка шифрування голосового повідомлення у десктопному додатку соціальної мережі «Instagram» через перевірку мережевих пакетів даних в сніфері пакетів «Wireshark»;
- перевірка наявності метаданих в фотографіях та відео, що надсилаються та публікуються через десктопний додаток соціальної мережі «Instagram», за допомогою програми «JPEGsnoop»;

- перевірка шифрування текстового повідомлення у десктопному додатку месенджеру «Telegram» через перевірку мережевих пакетів даних в сніфері пакетів «Wireshark»;
- перевірка шифрування голосового повідомлення у десктопному додатку месенджеру «Telegram» через перевірку мережевих пакетів даних в сніфері пакетів «Wireshark»;
- перевірка наявності метаданих в фотографіях та відео, що надсилаються та публікуються через десктопний додаток месенджеру «Telegram», за допомогою програми «JPEGsnoop»;
- перевірка шифрування текстового повідомлення у десктопному додатку месенджеру «WhatsApp» через перевірку мережевих пакетів даних в сніфері пакетів «Wireshark»;
- перевірка шифрування голосового повідомлення у десктопному додатку месенджеру «WhatsApp» через перевірку мережевих пакетів даних в сніфері пакетів «Wireshark»;
- перевірка наявності метаданих в фотографіях та відео, що надсилаються та публікуються через десктопному додатку месенджеру «WhatsApp», за допомогою програми «JPEGsnoop».

1.3 Висновки

Огляд соціальної мережі «Instagram» та месенджерів «Telegram» та «WhatsApp» надав розуміння про сучасний масштаб виникнення кіберінцидентів в них, про періодичність та причини виникнення кібератак та вразливостей, на які ці атаки направлені, а також про реакцію компаній власників або команд розробників соцмереж та месенджерів на проблеми, що виникають в їх мобільних, десктопних та вебдодатках або на платформі в цілому. За минулий рік в оглянутих месенджерах не було виявлено масштабних зломів облікових записів користувачів, які б призвели до витоку їхньої конфіденційної інформації, проте в соцмережі «Instagram» частішають випадку злому, про що свідчить звернення суддів штату Пенсильванія, США. Це може свідчити про те, що використання популярного та відомого сервісу для обміну фотографіями може стати небезпечним та загрозливим, натомість месенджери рекомендують себе як безпечні для використання через відсутність відомостей про масштабні зломи облікових записів їхніх користувачів.

Огляд також надав розуміння про те, які методи та засоби можуть використовувати хакери та шахраї в кіберпросторі для отримання несанкціонованого доступу до облікових записів жертв або їхньої конфіденційної інформації. Основними програмними чинниками, що сприяють зловмисникам в їх неправомірних діях, стають недоліки в додатках платформ та супроводжуваних програмних засобах, наприклад API, але не ці чинники не є переважними серед хакерів в останній час. Перевагу злочинці надають різноманітним засобам та методам злому, що ґрунтуються на основі соціальної інженерії. Прикладом цього є описаний випадок з псевдо-розширеною версією «WhatsApp» в 2016 році.

Підсумовуючи огляд соціальної мережі «Instagram», хочеться зазначити про низький рівень клієнтської підтримки та відсутність нормальної реакції компанії власника цієї платформи для обміну фотографіями на інциденти, які пов'язані зі зломом або викраденням облікового запису користувача. Незважаючи на оперативність виправлення, наявність помилки в API призвела до витоку конфіденційної інформації близько 7 мільйонів користувачів, що є неприйнятним

для популярної соцмережі. На велику небезпеку використання цього сервісу для обміну фотографіями також вказує нещодавнє скорочення працівників, серед яких більшість склали працівники в сфері забезпечення кібербезпеки, в компанії «Meta», яка є власником «Instagram», що може призвести до подальшого зросту випадків злому та викрадень облікових записів користувачів.

Огляд месенджеру «Telegram» показав, що за всю історію його існування не було масштабних випадків злому чи викрадень облікових записів або витоку конфіденційної інформації користувачів, що свідчить про достатній рівень захисту та надійності цього сервісу для обміну повідомленнями для, насамперед, незалежних користувачів. Зважаючи на походження, сумнівну діяльність та дивну реакцію команди розробників на оглянуті ситуації, які вказували на зв'язок месенджеру з спеціальними службами Російської Федерації, можна зробити висновок, що месенджер є небезпечним для використання працівниками Державної служби з надзвичайних ситуацій України, Національної поліції України, Національної гвардії України та Збройних Сил України, оскільки листування та обмін повідомленнями через «Telegram» може загрожувати національній безпеці України.

Останній в загальному огляді в цьому розділі був месенджер «WhatsApp». Після його огляду та огляду кіберінцидентів, що виникали з цим месенджером, важко зробити однозначний висновок. З самого початку масштабного користування мобільним додатком та вебдодатком цього сервісу для обміну повідомленнями виникали вразливості, які були спричинені помилками під час розробки цих додатків. Звісно, ці вразливості майже одразу були скомпрометовані, але або через відкритість команди розробників до критики, або через заохочення, це було зроблено білими хакерами або ентузіастами, які одразу доповіли про наявну вразливість в додатках. Після виявлення таких вразливостей команда розробників «WhatsApp» одразу приймала міри щодо усунення виявлених недоліків, що свідчить про достатній рівень підтримки роботи над месенджером. Проте назвати цілком безпечним месенджер «WhatsApp» не можна,

незважаючи на те, що в останній час не було відомостей про злом через програмні недоліки в додатках цього сервісу для обміну повідомленнями.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

У цьому розділі буде проведено дослідження існуючих методів захисту конфіденційної інформації користувачів в соціальній мережі «Instagram» та месенджерах «Telegram» та «Instagram» за інструкцією, котра написана у пункті 1.2 цієї кваліфікаційної роботи. По завершенню дослідження буде виконано огляд та вивчення отриманих результатів та методів захисту, що використовуються для захисту конфіденційної інформації користувачів. У дослідженні приймало участь троє добровольців. Усі добровольці виявили бажання не розповсюджувати про себе інформацію, тому на деяких рисунках, що продемонстровані у пунктах цього розділу, буде замазана та не буде вказана інформація, що є конфіденційною.

Технічні засоби, що були використанні для проведення дослідження:

- маршрутизатор безпровідного зв'язку «TP-Link WR740N», що під'єднаний до провайдера інтернет-зв'язку за допомогою Ehternet-кабелю;
- ноутбук «Acer Nitro 5 AN515-45».

Програмні засоби та вебсервіси, що використовувалися в дослідженні та для аналізу результатів дослідження:

- операційна система «Windows 11» версії 23H2, що поширюється за платною ліцензією;
- сніфер пакетів «Wireshark» версії 4.2.5, що поширюється за безкоштовною ліцензією;
- десктопний додаток для клієнта соціальної мережі «Instagram» версії 42.0.23.0, що поширюється за безкоштовною ліцензією;
- вебзастосунок для клієнта соціальної мережі «Instagram», який використовується через браузер «Google Chrome» та поширюється за безкоштовною ліцензією;
- десткопний додаток для клієнта месенджеру «Telegram» версії 5.1.7, що поширюється за безкоштовною ліцензією;

· десктопний додаток для клієнта месенджеру «WhatsApp» версії 2.2423.10.0, що поширюється за безкоштовною ліцензією.

· утиліта «JPEGsnoop»[1)] версії 1.8.0 що поширюється за безкоштовною ліцензією та призначена для сканування внутрішньої інформації в файлах формату «JPEG» та «JPG»;

· вебсервіс «2IP»[2)], доступ до якого є безкоштовним та який дозволяє отримати різну інформацію про введений IP-адрес.

2.1 Перевірка шифрування текстового повідомлення у десктопному додатку соціальної мережі «Instagram»

Для виконання цього експерименту одному з добровольців дослідником було надіслане текстове повідомлення розміром 2042 байти через десктопний додаток месенджеру «Telegram». Процес надсилання текстового повідомлення було перехоплено сніфером «Wireshark».

На рисунку 2.1 зображено список перехоплених мережевих пакетів даних з текстовим повідомленням, що був надісланий добровольцю.

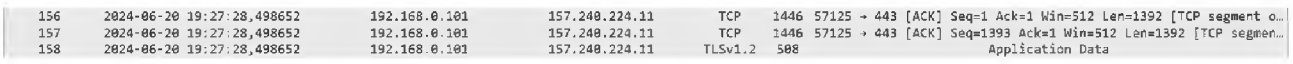


Рисунок 2.1 - Список перехоплених пакетів даних з текстовим повідомленням, що були надіслані добровольцю

На рисунку 2.1 зображені загальні відомості про пакети даних з текстовим повідомленням у вигляді таблиці, стовпці якої зліва направо мають такі назви:

· номер пакету за весь час процесу перехоплення пакетів;

· дата та час (враховуючи мілісекунди) надсилання пакету;

· IP-адресу джерела пакету;

· IP-адресу кінцевої точки пакету;

[1] «JPEGsnoop» — це детальний інструмент для декодування та аналізу зображень JPEG, виявлення всіх метаданих зображення, визначення оригінальності зображення.

[2] «2IP» — це веб-сервіс для аналізу IP-адрес. Дозволяє перевірити IP-адресу пристрою, з якого виходять до інтернет-мережі та отримати відомості про будь-яку IP-адресу.

- назва протоколу пакету;
- розмір пакету;
- загальна інформація про пакет.

Як можна побачити з рисунку 2.1, надсилання повідомлення відбувається з використанням пакетів за протоколом TCP та TLS версії 1.2, які потрапили до хосту за IP-адресою 157.240.224.11. За допомогою вебсервісу «2IP» було встановлено, що цей хост є сервером, який належить компанії «Meta Platforms Inc.», яка є власником соціальної мережі «Instagram», а також що сервер знаходиться у місті Менло Парк, штат Каліфорнія, США. Вже від цього серверу повідомлення було надіслане до добровольця.

На рисунках 2.2 та 2.3 зображено фрагмент байтів та детальну інформацію про складові початкового та проміжкового мережевих пакетів даних за протоколом «TCP» відповідно.

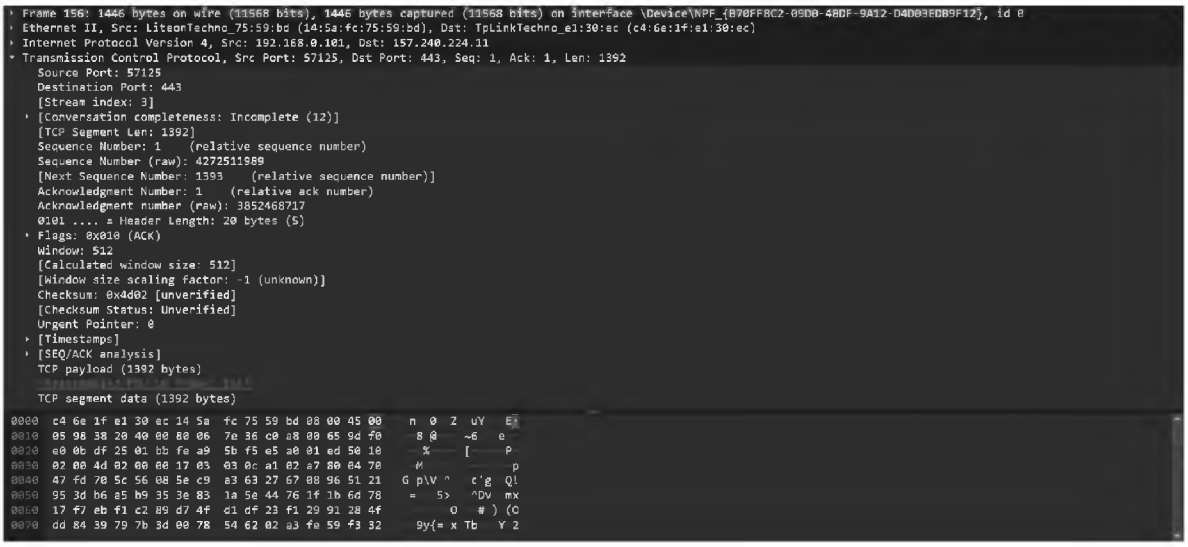


Рисунок 2.2 - Фрагмент байтів та складові початкового пакету даних

На продемонстрованих рисунках 2.2 та 2.3 зверху зображено складові пакетів даних, знизу - фрагмент байтів пакету даних. Також на зазначених

рисунках зображені деталі складових «Transmission Control Protocol», в яких присутній сегмент текстового повідомлення.

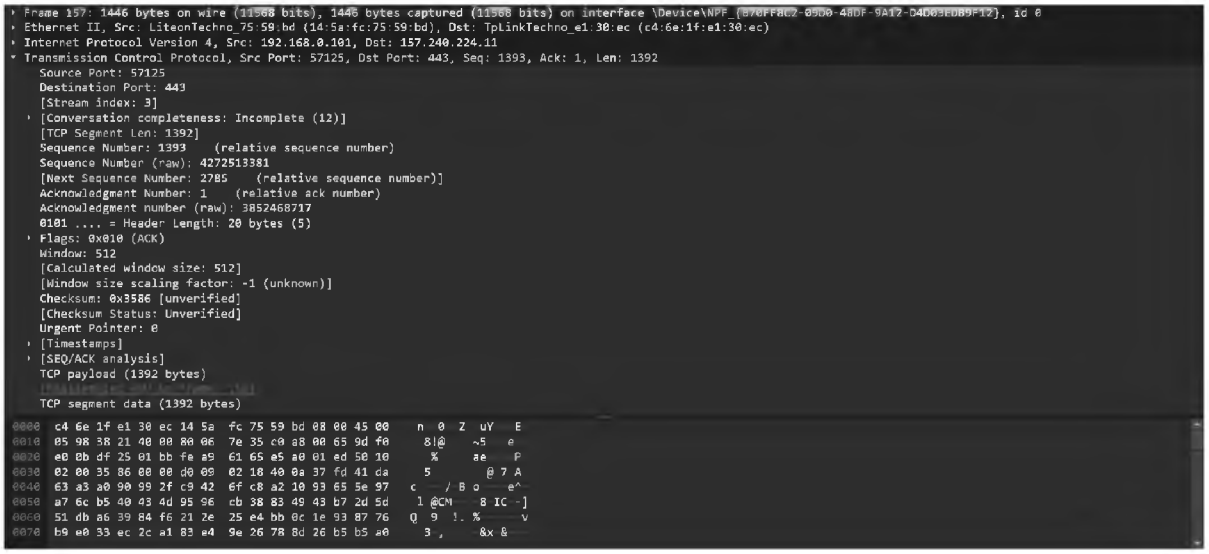


Рисунок 2.3 - Фрагмент байтів та складові проміжкового пакету даних

Мережеві пакети даних за протоколом «TCP» у цьому випадку використовувались для передачі сегментів текстового повідомлення, оскільки розмір повідомлення не дозволяє надіслати його за один пакет «TCP». На рисунку 2.2 у полі «Sequence Number» в складовій «Transmission Control Protocol» можна побачити, що початковий індекс даних в пакеті даних дорівнює 1, що вказує на те, що зображений пакет даних є початковим. На рисунку 2.3 у полі «Sequence Number» в складовій «Transmission Control Protocol» можна побачити, що початковий індекс даних в пакеті даних дорівнює 1393, що вказує на те, що зображений пакет даних є проміжковим.

Через деталі складової «Transmission Control Protocol» неможливо отримати сегмент повідомлення, проте через байти пакету це можливо. Фрагмент байтів повідомлення зображено на рисунку 2.4.

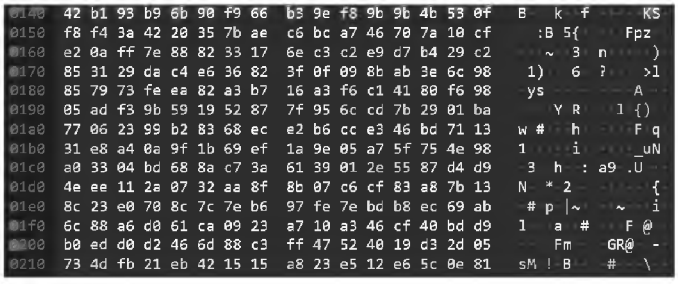


Рисунок 2.4 - Фрагмент байтів проміжкового пакету даних за протоколом «TCP»

На рисунку 2.5 зображено мережевий пакет даних за протоколом «TLS» з його складовими та частиною його байтів.

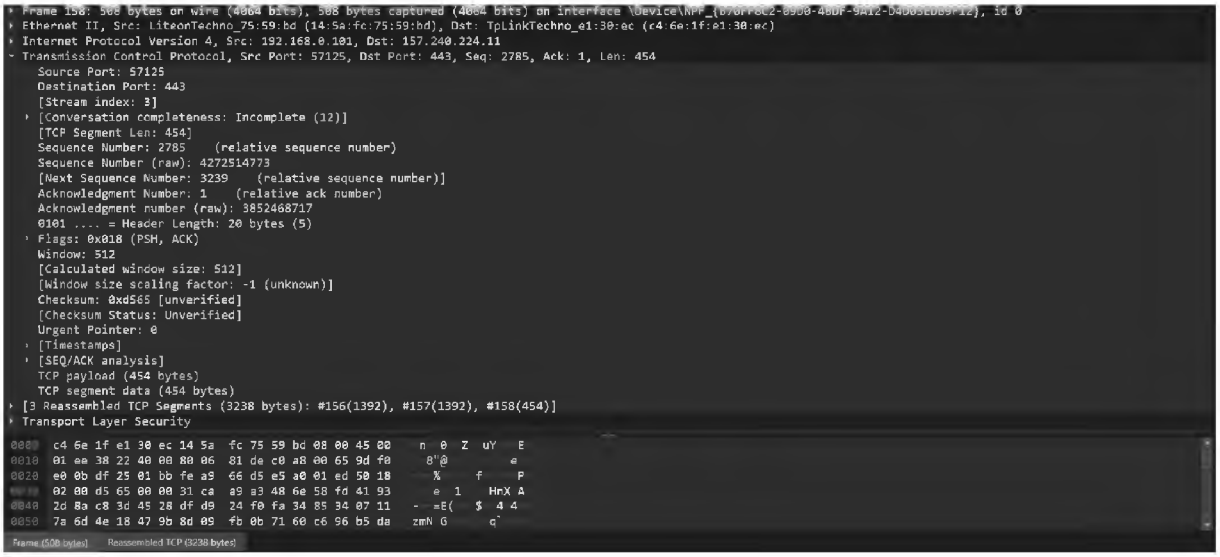


Рисунок 2.5 - Фрагмент байтів та складові пакету даних за протоколом «TLS»

На рисунку 2.5 у верхній частині знаходяться складові пакетів даних, у нижній - фрагмент байтів пакету даних. Також на цьому рисунку зображено деталі складової «Transmission Control Protocol».

З деталей складової «Transmission Control Protocol» зображеного на рисунку 2.5 пакету даних видно, що у полі «Sequence Number» початковий індекс відправлених даних дорівнює 2785 та у полі «TCP payload» розмір надісланих даних дорівнює 454, що вказує на те, що зображений пакет даних є фінальним.

З рисунку 2.5 видно, що передостання складова зображеного пакету даних має відомості про розподілення фрагментів надісланого текстового повідомлення по пакетах даних за протоколом «TCP», включно з пакетом даних, що розглядається. На рисунку 2.6 зображено складову «Transport Layer Security» пакету даних за протоколом «TLS».

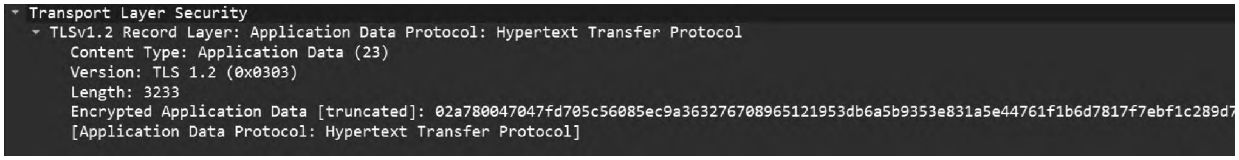


Рисунок 2.6 - Складова «Transport Layer Security» мережевого пакету даних

На рисунку 2.6 можна побачити версію пакету даних за протоколом «TLS» у полі «Version», розмір пакету даних у «Length», а також у полі «Encrypted Application Data» зашифровані дані, якими є надіслане дослідником текстове повідомлення до добровольця. З фрагменту зашифрованих даних у полі «Encrypted Application Data» можна зробити висновок, що у протоколі «TLS» використовується симетричний алгоритм блокового шифрування «AES».

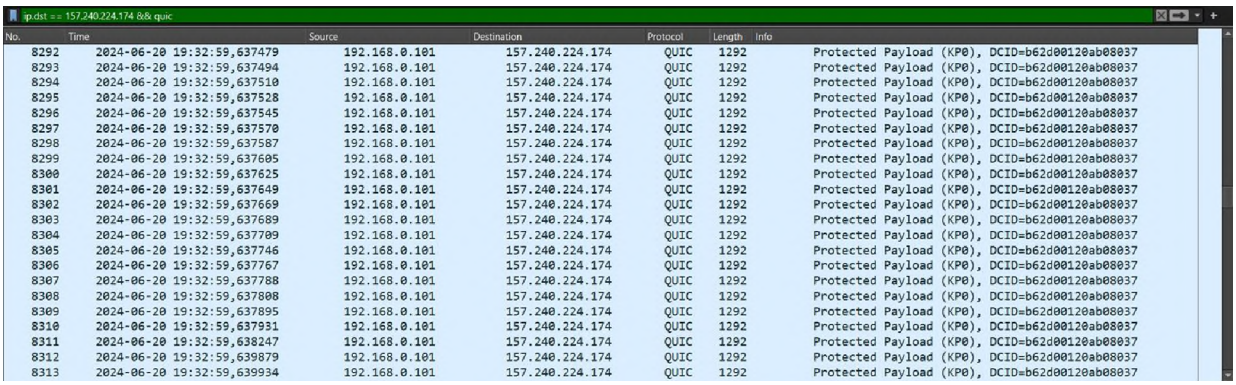
На рисунках 2.2, 2.3 та 2.5 у полях «TCP payload» складових «Transmission Control Protocol» зображених пакетів даних продемонстровано розмір надісланих даних. Якщо скласти значення цих полів, отримуємо 3 238 байтів, проте вихідне текстове повідомлення має розмір 2042 байти. Цей факт може вказувати на обробку вихідного текстового повідомлення, а саме його шифрування, що призвело до збільшення обсягу даних, які потрібно надіслати.

Розглянуті мережеві пакети даних, які використовує десктопний додаток соціальної мережі «Instagram» та які відповідають текстовому повідомленню, показують, що текстові повідомлення перед надсиланням шифруються.

2.2 Перевірка шифрування голосового повідомлення у десктопному додатку соціальної мережі «Instagram»

Для виконання цього експерименту одному з добровольців дослідником було надіслане голосове повідомлення розміром 457 кілобайт, або 467393 байтів, через десктопний додаток соціальної мережі «Instagram». Процес надсилання голосового повідомлення було перехоплено сніфером «Wireshark».

На рисунку 2.7 зображено частину списку перехоплених мережевих пакетів даних з голосовим повідомленням, що був надісланий добровольцю.



ip.dst == 157.240.224.174 && quic

No.	Time	Source	Destination	Protocol	Length	Info
8292	2024-06-20 19:32:59,637479	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8293	2024-06-20 19:32:59,637494	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8294	2024-06-20 19:32:59,637510	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8295	2024-06-20 19:32:59,637528	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8296	2024-06-20 19:32:59,637545	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8297	2024-06-20 19:32:59,637570	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8298	2024-06-20 19:32:59,637587	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8299	2024-06-20 19:32:59,637605	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8300	2024-06-20 19:32:59,637625	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8301	2024-06-20 19:32:59,637649	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8302	2024-06-20 19:32:59,637669	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8303	2024-06-20 19:32:59,637689	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8304	2024-06-20 19:32:59,637709	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8305	2024-06-20 19:32:59,637746	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8306	2024-06-20 19:32:59,637767	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8307	2024-06-20 19:32:59,637788	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8308	2024-06-20 19:32:59,637808	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8309	2024-06-20 19:32:59,637895	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8310	2024-06-20 19:32:59,637931	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8311	2024-06-20 19:32:59,638247	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8312	2024-06-20 19:32:59,639879	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037
8313	2024-06-20 19:32:59,639934	192.168.0.101	157.240.224.174	QUIC	1292	Protected Payload (KP0), DCID=b62d00120ab08037

Рисунок 2.7 - Частина списку перехоплених мережевих пакетів даних голосового повідомлення

На рисунку 2.7 зображені загальні відомості про пакети даних з текстовим повідомленням у вигляді таблиці, стовпці якої зліва направо мають такі назви:

- номер пакету за весь час процесу перехоплення пакетів;
- дата та час (враховуючи мілісекунди) надсилання пакету;
- IP-адресу джерела пакету;
- IP-адресу кінцевої точки пакету;
- назва протоколу пакету;
- розмір пакету;
- загальна інформація про пакет.

Також на рисунку 2.7 у верхній частині є поле для виразу, що фільтрує мережеві пакети даних, які були перехоплені за весь час перехоплення. У цьому полі було введено вираз для фільтрування пакетів даних за весь час перехоплення. Фільтрування відбувалось за пунктом призначення та назвою пакетів даних. Фільтрування надає користувачу сніфером «Wireshark» відфільтрований список пакетів даних, що спрощує аналіз.

На рисунку 2.7 можна побачити, що всі пакети надсилались до хосту за IP-адресою 157.240.224.174. За допомогою вебсервісу «2IP» було встановлено, що цей хост є сервером, який належить компанії «Meta Platforms Inc.», яка, як було зазначено вище, є власником соціальної мережі «Instagram», а також що сервер знаходиться у місті Менло Парк,

штат Каліфорнія, США. Від цього серверу голосове повідомлення було надіслане добровольцю.

Продемонстровані на рисунку 2.7 пакети були надіслані за протоколом «QUIC». Серед продемонстрованого списку мережевих пакетів даних немає початкового та кінцевого пакетів даних, які відповідають надісланому голосовому повідомленню. На рисунках 2.8 та 2.9 зображено початковий та кінцевий пакети даних надісланого голосового повідомлення.

Примітка. «QUIC» - транспортний мережевий протокол, що альтернативою зв'язці протоколів «TCP» та «TLS». Він розв'язує проблеми з великим часом встановлення та узгодження з'єднань в «TCP» і усуває затримки при втраті пакетів в процесі передачі даних. «QUIC» є надбудовою над протоколом «UDP», що підтримує мультиплексування декількох з'єднань і забезпечує методи шифрування, еквівалентні тим, що використовуються в протоколі «TLS».

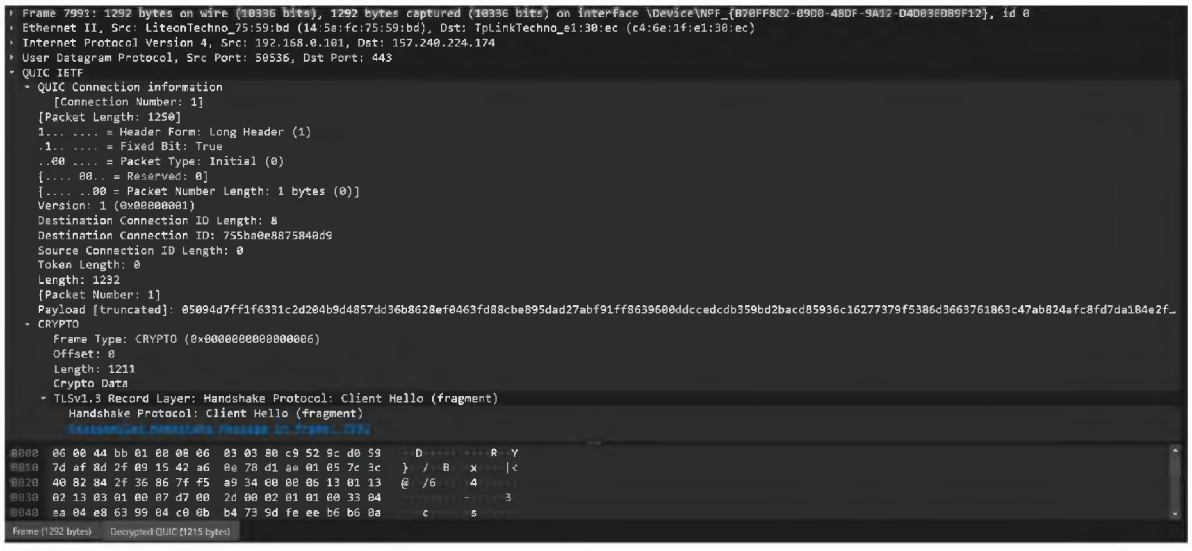


Рисунок 2.8 - Початковий мережевий пакет даних надісланого голосового повідомлення

На рисунках 2.8 та 2.9 у верхній частині зображено складові пакетів даних, у нижній частині - фрагмент байтів пакетів даних.

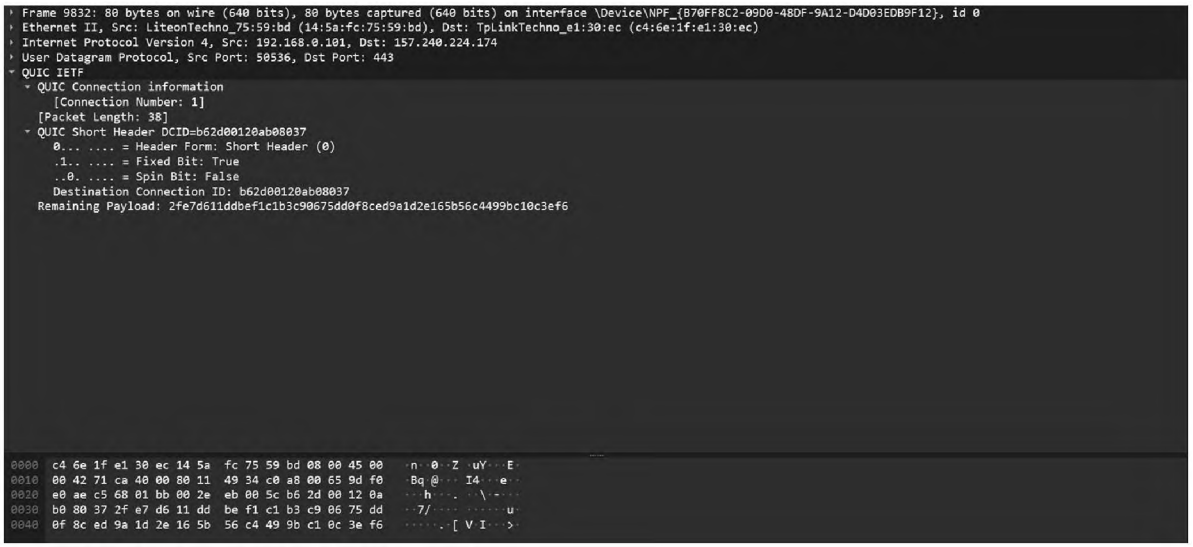


Рисунок 2.9 - Кінцевий мережевий пакет даних надісланого голосового повідомлення

На рисунку 2.8 можна побачити, що у детальній інформації складової «QUIC IEFT» пакету даних у деталях поля «CRYPTO» надсилається запит на встановлення TLS-з'єднання з використанням протоколу «TLS» версії 1.3. Також можна побачити, що в цьому ж пакеті даних у детальній інформації складової «QUIC IEFT» у полі «Payload» початковий фрагмент зашифрованого голосового повідомлення.

На рисунку 2.9 продемонстровано, що у детальній інформації складової «QUIC IEFT» зображеного мережевого пакету даних у полі «Remaining Payload» знаходиться останній фрагмент зашифрованого голосового повідомлення.

Висновок про те, що голосове повідомлення є зашифрованим, було зроблено на основі трьох отриманих відомостей:

· у початковому пакеті даних за протоколом «QUIC» надісланого голосового повідомлення є відомості про відкриття TLS-з'єднання за протоколом «TLS» версії 1.3, що свідчить про те, передача даних відбувається у зашифрованому вигляді;

· вигляд фрагментів голосового повідомлення в зображених на рисунках 2.8 та 2.9 пакетах даних вказує на те, що повідомлення було зашифроване за алгоритмом, який у результаті повертає рядок

даних, який має вигляд чисел у шістнадцятковій системі числення. Прикладом такого алгоритму шифрування може бути «AES»;

· після підрахунку кількості надісланих даних, які були надіслані за допомогою мережевих пакетів даних за протоком «QUIC» та які стосуються голосового повідомлення, розмір склав 710435 байтів, проте розмір вихідного голосового повідомлення складає 467393 байтів, що вказує на шифрування повідомлення, і цей процес викликав збільшення обсягу даних, які необхідно надіслати.

2.3 Перевірка наявності метаданих в фотографіях та відео, що надсилаються та публікуються через десктопний додаток соціальної мережі «Instagram»

Десктопний додаток соціальної мережі «Instagram» не підтримує завантаження дописів або фотографій, що були надіслані в чатах, проте завантаження можливе через мобільний додаток та інструменти розробника браузера, в якому відкритий вебзастосунок «Instagram». Дослідником було завантажено фотографії з двох довільних дописів з вебзастосунку «Instagram», використовуючи інструменти розробника браузера «Google Chrome».

За допомогою утиліти «JPEGsnoop» відбулася перевірка завантажених фотографій. Звіт від зазначеної утиліти з результатами перевірки першої завантаженої фотографії з вебзастосунку представлені на рисунку 2.10, другої завантаженої фотографії - на рисунку 2.11.

Звіти містять в собі відомості про назву перевіряємого файлу, розмір перевіряємого файлу та версію файлу.

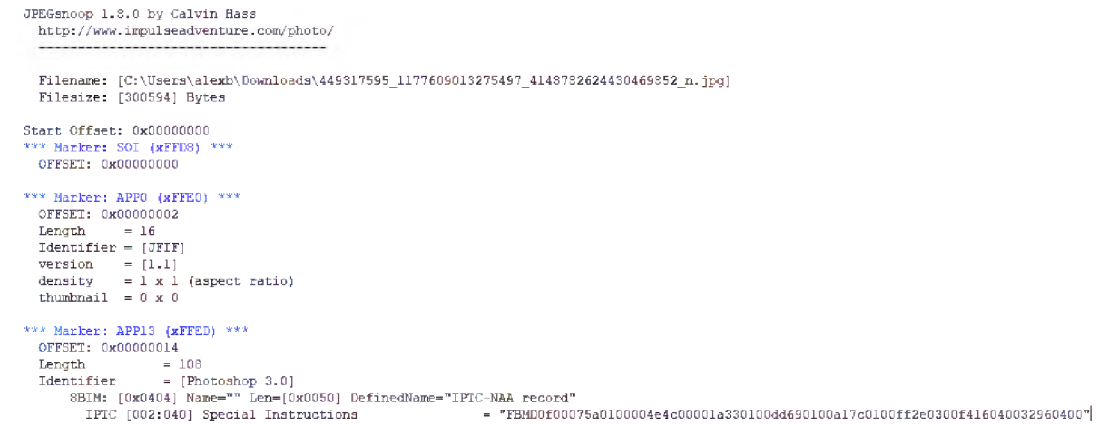


Рисунок 2.10 - Звіт з результатами перевірки першої завантаженої фотографії з вебзастосунку «Instagram»

Рисунок 2.11 - Звіт з результатами перевірки другої завантаженої фотографії з вебзастосунку «Instagram»

З рисунку 2.10 та 2.11 з розділу «Marker: APP13 (xFEED)» з поля «Identifier» можна побачити, що перед публікацією дописів фотографії були оброблені програмою «Photoshop» версії 3.0. Також можемо побачити, що у завантажених фотографіях відсутні метадані.

2.4 Перевірка шифрування текстового повідомлення у десктопному додатку месенджеру «Telegram»

Для виконання цього експерименту одному з добровольців дослідником було надіслане текстове повідомлення розміром 39 байтів через десктопний додаток месенджеру «Telegram». Процеси запуску додатка, надсилання текстового повідомлення та закриття додатка було перехоплено сніфером «Wireshark».

На рисунку 2.12 зображено початок списку перехоплених пакетів даних, що були надіслані до серверів «Telegram».

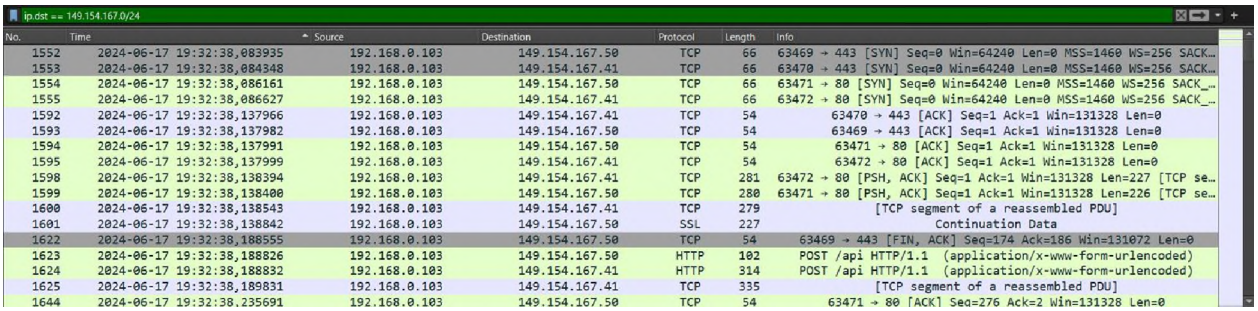


Рисунок 2.12 - Початок списку перехоплених пакетів даних, що були надіслані до серверів «Telegram»

На рисунку 2.12 зображені загальні відомості про пакети даних у вигляді таблиці, стовпці якої зліва направо мають такі назви:

- номер пакету за весь час процесу перехоплення пакетів;
- дата та час (враховуючи мілісекунди) надсилання пакету;
- IP-адресу джерела пакету;
- IP-адресу кінцевої точки пакету;
- назва протоколу пакету;
- розмір пакету;
- загальна інформація про пакет.

Також на рисунку 2.12 у верхній частині є поле для виразу, що фільтрує мережеві пакети даних, які були перехоплені за весь час перехоплення. У цьому полі було введено вираз для фільтрування пакетів даних за весь час перехоплення. Фільтрування відбувалось лише за пунктом призначення. Фільтрування надає користувачу сніфером «Wireshark» відфільтрований список пакетів даних, що спрощує аналіз.

На рисунку 2.12 зображені пакети, як було зазначено вище, надсилаються до серверів «Telegram», а саме сервери за IP-адресами 149.154.167.41 та

149.154.167.50. За допомогою вебсервісу «2IP» було з'ясовано, що ці сервери належать компанії «Telegram Messenger LLP», яка є розробником «Telegram», та знаходяться у Лондоні, Великобританія.

Серед зображених пакетів даних на рисунку 2.12 є пакет даних під номером 1601, що був надісланий за протоколом «SSL» до серверу за IP-адресою 149.154.167.50, який і містить надіслане дослідником текстове повідомлення добровольцю. Детальну інформацію про цей пакет зображено на рисунку 2.13.

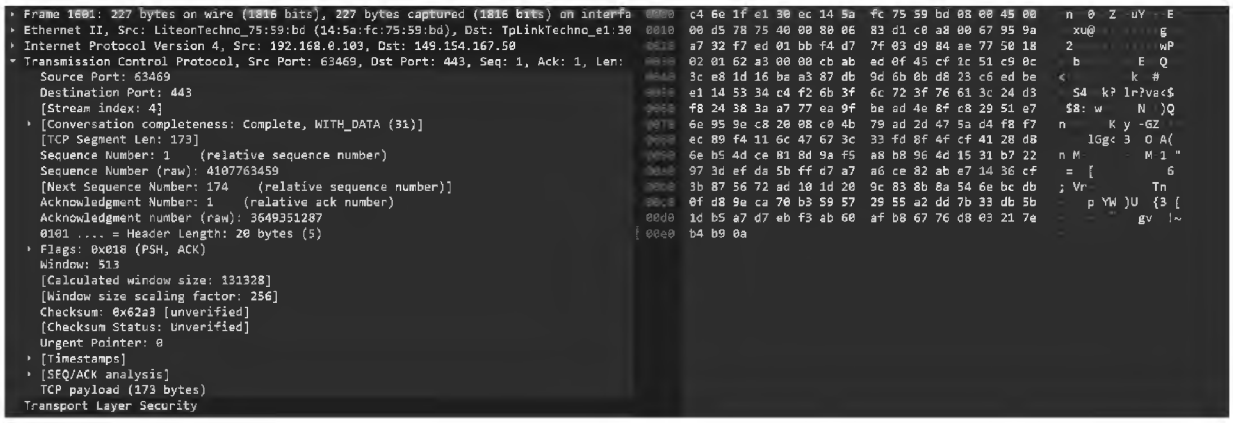


Рисунок 2.13 - Детальна інформація про мережевий пакет даних з текстовим повідомленням

На рисунку 2.13 ліворуч знаходиться віджет з інформацією про складові пакету даних, праворуч віджет з байтами пакету даних. Також у віджеті з інформацією про складові зображено деталі складової «Transmission Control Protocol» зображеного пакету даних.

Розмір надісланих даних становить 173 байти. Це стало відомо з поля «TCP payload» складової «Transmission Control Protocol». Зважаючи на те, що розмір вихідного текстового повідомлення становить 39 байтів, збільшений розмір надісланих даних свідчить про те, що повідомлення було зашифровано перед надсиланням.

Можна побачити, що деталі про дані, які знаходяться у складовій «Transport Layer Security» пакету даних з текстовим повідомленням неможливо переглянути взагалі. Це пов'язано з тим, що для шифрування текстових повідомлень десктопний додаток «Telegram» використовує власний криптографічний

протокол «MTProto», який є власністю компанії-розробника, і деталі якого є закритими, тому переглянути вигляд зашифрованого повідомлення неможливо та можна лише робити припущення, який саме вигляд має зашифровані текстові дані.

З розглянутих мережевих пакетів даних можна зробити висновок, що текстові повідомлення, надіслані через десктопний додаток месенджеру «Telegram», передаються у зашифрованому вигляді.

2.5 Перевірка шифрування голосового повідомлення у десктопному додатку месенджеру «Telegram»

Для виконання цього експерименту одному з добровольців дослідником було надіслане голосове повідомлення розміром 23 286 байтів через десктопний додаток месенджеру «Telegram». Процес надсилання голосового повідомлення було перехоплено сніфером «Wireshark».

На рисунку 2.14 зображено список перехоплених пакетів даних з голосовим повідомленням.

2650	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2651	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2652	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2653	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2654	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2655	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2656	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2657	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2658	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2659	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2660	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2661	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2662	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2663	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2664	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2665	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2666	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2667	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1294	Continuation Data
2668	2024-06-17 20:55:59,282839	192.168.0.103	149.154.167.41	SSL	1202	Continuation Data

Рисунок 2.14 - Список перехоплених пакетів з голосовим повідомленням

На рисунку 2.14 зображені загальні відомості про пакети даних у вигляді таблиці, стовпці якої зліва направо мають такі назви:

- номер пакету за весь час процесу перехоплення пакетів;
- дата та час (враховуючи мілісекунди) надсилання пакету;
- IP-адресу джерела пакету;

- IP-адресу кінцевої точки пакету;
- назва протоколу пакету;
- розмір пакету;
- загальна інформація про пакет.

На рисунку 2.14 зображені пакети надсилаються до хосту за IP-адресою 149.154.167.41. За допомогою вебсервісу «2IP» було з'ясовано, що цей хост є сервером, який належить компанії «Telegram Messenger LLP», яка є розробником «Telegram», та знаходиться у Лондоні, Великобританія.

З рисунку 2.14 можна побачити, що пакети даних, які містять голосове повідомлення, були надіслані за протоколом «SSL». На рисунку 2.15 та 2.16 зображено початковий та кінцевий мережевий пакет даних відповідно.

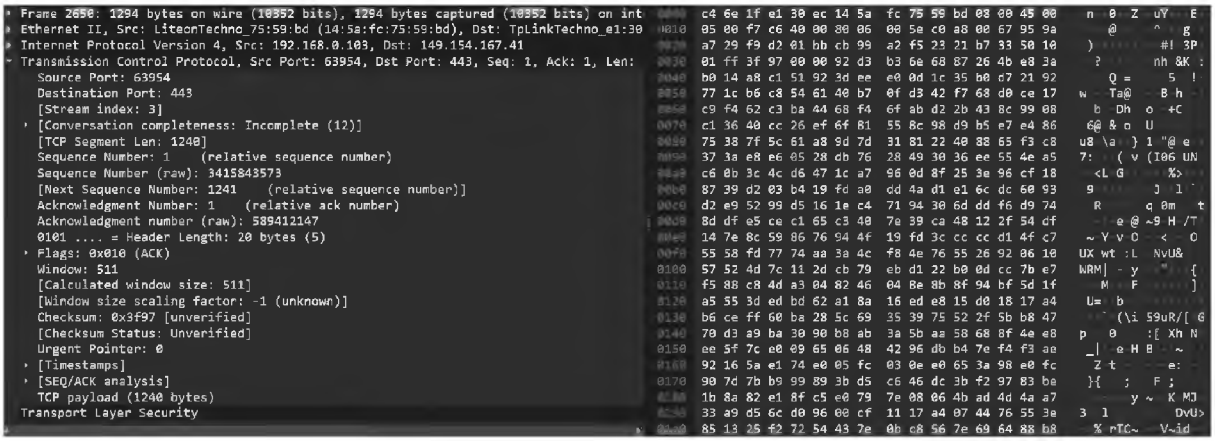


Рисунок 2.15 - Початковий мережевий пакет даних надісланого голосового повідомлення

На рисунках 2.15 та 2.16 ліворуч знаходиться віджет з інформацією про складові пакету даних, праворуч віджет з байтами пакету даних. Також у віджеті з інформацією про складові зображено деталі складової «Transmission Control Protocol» зображених пакетів даних.

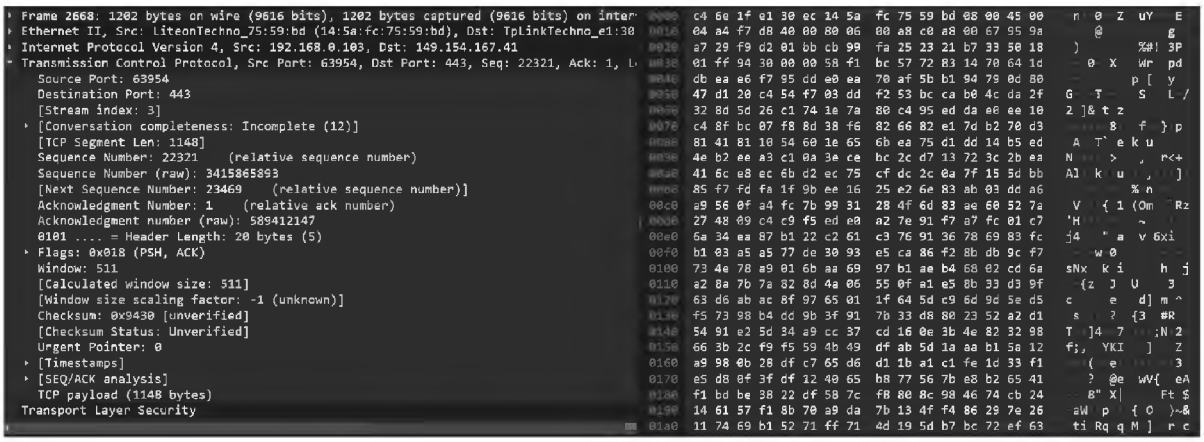


Рисунок 2.16 - Кінцевий мережевий пакет даних надісланого голосового повідомлення

На рисунку 2.15 у полі «Sequence Number» складової «Transmission Control Protocol» вказано початковий індекс надісланих сегментованих даних, який дорівнює 1, що вказує на те, що зображений пакет даних є початковим у загальному списку пакетів даних, що відповідають голосовому повідомленню. На рисунку 2.16 у полі «Sequence Number» складової «Transmission Control Protocol» вказано початковий індекс надісланих сегментованих даних, який дорівнює 22321, та порівнюючи значення у полях «TCP payload» складової «Transmission Control Protocol» між початковим та зображеним пакетом даних, зображений мережевий пакет даних має зменшений обсяг надісланих даних, що вказує на те, що зображено саме кінцевий пакет даних у загальному списку пакетів даних, що відповідають голосовому повідомленню.

Після підрахунку розміру всіх даних, надісланих за допомогою пакетів даних, список яких зображено на рисунку 2.14, розмір надісланого голосового повідомлення склав 23 468 байтів. Порівнюючи з розміром вихідного голосового повідомлення, який дорівнює 23 286 байтів, невелике збільшення обсягу надісланих даних може вказувати на попередню обробку повідомлення, а саме на шифрування, яке і збільшило обсяг даних, які необхідно надіслати.

На рисунках 2.15 та 2.16 можна побачити, що деталі про дані, які знаходяться у складовій «Transport Layer Security» початкового та кінцевого пакетів даних з голосовим повідомленням неможливо переглянути взагалі. Це

пов’язано з тим, що для шифрування голосових повідомлень десктопний додаток «Telegram» використовує власний криптографічний протокол «MTProto», який є власністю компанії-розробника, і деталі якого є закритими, тому переглянути вигляд зашифрованого повідомлення неможливо та можна лише робити припущення, який саме вигляд має зашифровані текстові дані.

З розглянутих мережевих пакетів даних можна зробити висновок, що голосові повідомлення, надіслані через десктопний додаток месенджеру «Telegram», передаються у зашифрованому вигляді.

2.6 Перевірка наявності метаданих в фотографіях та відео, що надсилаються та публікуються через десктопний додаток месенджеру «Telegram»

Для виконання цього експерименту одним з добровольців досліднику була надіслана фотографія двома способами: як зображення та як файл. Дослідником було завантажено через десктопний додаток «Telegram» 2 файли: фотографія, яка була надіслана як зображення та фотографія, яка була надіслана як файл. Обидві завантажені фотографії були перевірені на допомогою утиліти «JPEGsnoop» на наявність метаданих.

На рисунку 2.17 зображено звіт з результатами перевірки на наявність метаданих завантаженої фотографії, яка була надіслана як зображення.

```
JPEGsnoop 1.8.0 by Calvin Hass
  http://www.impulseadventure.com/photo/
  ------------------------------------

  Filename: [C:\Users\alexb\Downloads\photo_2024-06-27_12-27-46.jpg]
  Filesize: [77341] Bytes

Start Offset: 0x00000000
*** Marker: SOI (xFFD8) ***
  OFFSET: 0x00000000

*** Marker: APP0 (xFFE0) ***
  OFFSET: 0x00000002
  Length      = 16
  Identifier  = [JFIF]
  version     = [1.1]
  density     = 1 x 1 (aspect ratio)
  thumbnail   = 0 x 0
```

Рисунок 2.17 - Звіт з результатами перевірки завантаженої фотографії, яка була надіслана як зображення

З рисунку 2.17 можна побачити з поля «Filesize», що завантажена фотографія, яка надіслана як фотографія, має розмір 77341 байт. Також перевірка не показала наявності метаданих.

На рисунку 2.18, 2.19 та 2.20 зображено частини звіту з результатами перевірки на наявність метаданих завантаженої фотографії, яка була надіслана як файл.

```
JPEGsnoop 1.8.0 by Calvin Hass
  http://www.impulseadventure.com/photo/
  ---------------------------------------

  Filename: [C:\Users\alexb\Downloads\20240621_210104.jpg]
  Filesize: [2304460] Bytes
```

Рисунок 2.18 - Частина звіту з результатами перевірки на наявність метаданих завантаженої фотографії, яка була надіслана як файл

```
EXIF GPSIFD @ Absolute 0x000003C2
  Dir Length = 0x0009
  [GPSVersionID                    ] =
  [GPSLatitudeRef                  ] =
  [GPSLatitude                     ] =
  [GPSLongitudeRef                 ] =
  [GPSLongitude                    ] =
  [GPSAltitudeRef                  ] =
  [GPSAltitude                     ] =
  [GPSTimeStamp                    ] =
  [GPSDateStamp                    ] =
```

Рисунок 2.19 - Частина звіту з результатами перевірки на наявність метаданих завантаженої фотографії, яка була надіслана як файл

```
EXIF SubIFD @ Absolute 0x000000E2
  Dir Length = 0x0024
  [ExposureTime                    ] = 1/16 s
  [FNumber                         ] = F1.7
  [ExposureProgram                 ] = Normal program
  [ISOSpeedRatings                 ] = 200
  [ExifVersion                     ] = 02.20
  [DateTimeOriginal                ] = "2024:06:21 21:01:04"
  [DateTimeDigitized               ] = "2024:06:21 21:01:04"
  [ComponentsConfiguration         ] = [Y Cb Cr .]
  [ShutterSpeedValue               ] = 399/100
  [ApertureValue                   ] = 153/100
  [BrightnessValue                 ] = -59/100
  [ExposureBiasValue               ] = 0.00 eV
  [MaxApertureValue                ] = 153/100
  [MeteringMode                    ] = CenterWeightedAverage
  [Flash                           ] = Flash did not fire
  [FocalLength                     ] = 4 mm
  [MakerNote                       ] = @ 0x0336
  [UserComment                     ] = ""
  [SubSecTime                      ] = "0717"
  [SubSecTimeOriginal              ] = "0717"
  [SubSecTimeDigitized             ] = "0717"
  [FlashPixVersion                 ] = 01.00
  [ColorSpace                      ] = sRGB
  [ExifImageWidth                  ] = 0x[00000FC0] / 4032
  [ExifImageHeight                 ] = 0x[000008DC] / 2268
  [ExifInteroperabilityOffset      ] = @ 0x0398
```

Рисунок 2.20 - Частина звіту з результатами перевірки на наявність метаданих завантаженої фотографії, яка була надіслана як файл

З рисунку 2.18 видно, що фотографія, яка була надіслана як файл, має розмір 2304460 байт, що значно більше за розмір фотографії, яка була надіслана як зображення.

На рисунку 2.20 можна побачити, що за результатами перевірки було виявлено метадані у фотографії, зокрема час фотографування. На рисунку 2.19 можна побачити, що серед знайдених метаданих присутні дані про місцерозташування пристрою під час фотографування, тобто були виявлені GPS-дані, які містились в фотографії.

2.7 Перевірка шифрування текстового повідомлення у десктопному додатку месенджеру «WhatsApp»

Для виконання цього експерименту одному з добровольців дослідником було надіслане текстове повідомлення розміром 74 байти через десктопний додаток месенджеру «WhatsApp». Процес надсилання текстового повідомлення було перехоплено сніфером «Wireshark».

У результаті процесу перехоплення було перехоплено лише один пакет даних за протоколом «TCP», який відповідає надісланому текстовому повідомленню. На рисунку 2.21 зображено деталі мережевого пакету даних, який відповідає текстовому повідомленню.

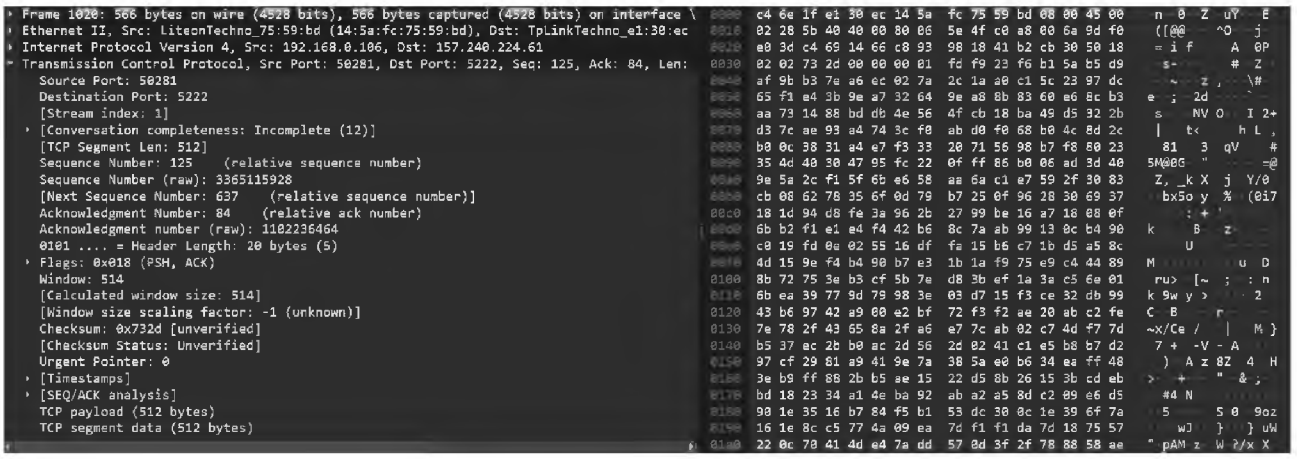


Рисунок 2.21 - Мережевий пакет даних за протоколом «TCP», який відповідає текстовому повідомленню

На рисунку 2.21 у лівій частині знаходяться складові зображеного пакету даних, у правій частині - фрагмент байтів пакету даних. Також серед складових пакету даних зображено деталі складової «Transmission Control Protocol».

З рисунку 2.21 з опису складової «Internet Protocol Version 4» видно, що зображений пакет даних був надісланий до хосту за IP-адресою 157.240.224.61. За допомогою вебсервісу «2IP» було з'ясовано, що цей хост є сервером, який належить компанії «Meta Platforms Inc.», яка є власником «WhatsApp», та який знаходиться у Менло Парк, США.

Як можна побачити з рисунку 2.21, в деталях складової «Transmission Control Protocol» неможливо переглянути вигляд надісланих даних, проте з поля «TCP payload», яке вказує на розмір надісланих даних та значення якого дорівнює 512 байтів, що свідчить про те, що перед надсиланням текстове повідомлення зазнало попереднього оброблення даних зі збільшенням їх обсягу, що вказує на процес шифрування, оскільки розмір вихідного текстового повідомлення складає 74 байти.

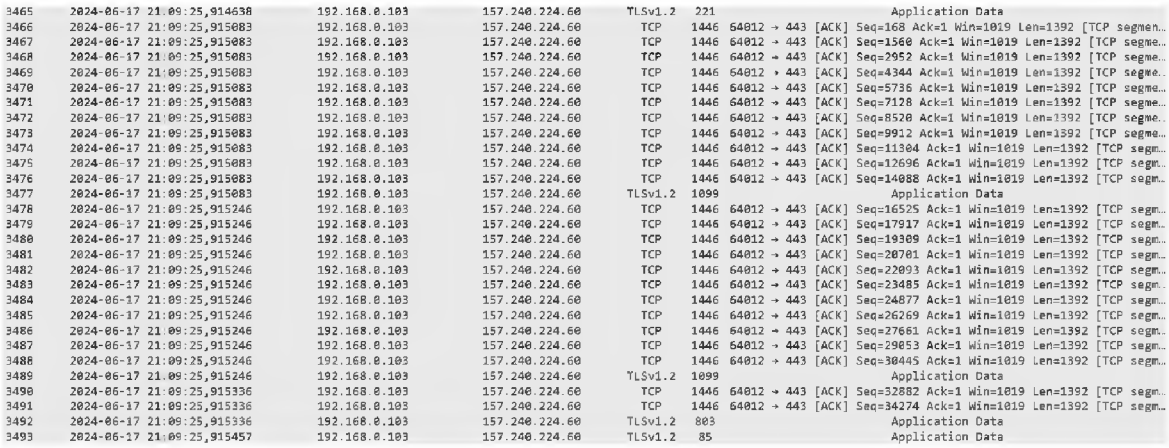
Наявність лише одного пакету даних для текстового повідомлення та наявність його шифрування, як було з'ясовано вище, свідчить про те, що для передачі тестових повідомлень в месенджері «WhatsApp» використовується технологія наскрізного шифрування - процес шифрування повідомлень, коли лише власники ключів шифрування мають доступ до вихідного повідомлення.

З розглянутого мережевого пакету даних за протоколом «TCP» можна зробити висновок, що текстові повідомлення, надіслані через десктопний додаток месенджеру «WhatsApp», передаються у зашифрованому вигляді.

2.8 Перевірка шифрування голосового повідомлення у десктопному додатку месенджеру «WhatsApp»

Для виконання цього експерименту одному з добровольців дослідником було надіслане голосове повідомлення розміром 36 134 байти через десктопний додаток месенджеру «WhatsApp». Процес надсилання голосового повідомлення було перехоплено сніфером «Wireshark».

На рисунку 2.22 зображено список перехоплених мережевих пакетів даних, що містять відправлене дослідником добровольцю голосове повідомлення через десктопний додаток «WhatsApp».



3465	2024-06-17 21:09:25,914638	192.168.0.103	157.240.224.60	TLSv1.2	221		Application Data
3466	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=168 Ack=1 Win=1019 Len=1392 [TCP segmen…	
3467	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=1560 Ack=1 Win=1019 Len=1392 [TCP segme…	
3468	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=2952 Ack=1 Win=1019 Len=1392 [TCP segme…	
3469	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=4344 Ack=1 Win=1019 Len=1392 [TCP segme…	
3470	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=5736 Ack=1 Win=1019 Len=1392 [TCP segme…	
3471	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=7128 Ack=1 Win=1019 Len=1392 [TCP segme…	
3472	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=8520 Ack=1 Win=1019 Len=1392 [TCP segme…	
3473	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=9912 Ack=1 Win=1019 Len=1392 [TCP segme…	
3474	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=11304 Ack=1 Win=1019 Len=1392 [TCP segm…	
3475	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=12696 Ack=1 Win=1019 Len=1392 [TCP segm…	
3476	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=14088 Ack=1 Win=1019 Len=1392 [TCP segm…	
3477	2024-06-17 21:09:25,915083	192.168.0.103	157.240.224.60	TLSv1.2	1099		Application Data
3478	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=16525 Ack=1 Win=1019 Len=1392 [TCP segm…	
3479	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=17917 Ack=1 Win=1019 Len=1392 [TCP segm…	
3480	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=19309 Ack=1 Win=1019 Len=1392 [TCP segm…	
3481	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=20701 Ack=1 Win=1019 Len=1392 [TCP segm…	
3482	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=22093 Ack=1 Win=1019 Len=1392 [TCP segm…	
3483	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=23485 Ack=1 Win=1019 Len=1392 [TCP segm…	
3484	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=24877 Ack=1 Win=1019 Len=1392 [TCP segm…	
3485	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=26269 Ack=1 Win=1019 Len=1392 [TCP segm…	
3486	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=27661 Ack=1 Win=1019 Len=1392 [TCP segm…	
3487	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=29053 Ack=1 Win=1019 Len=1392 [TCP segm…	
3488	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=30445 Ack=1 Win=1019 Len=1392 [TCP segm…	
3489	2024-06-17 21:09:25,915246	192.168.0.103	157.240.224.60	TLSv1.2	1099		Application Data
3490	2024-06-17 21:09:25,915336	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=32882 Ack=1 Win=1019 Len=1392 [TCP segm…	
3491	2024-06-17 21:09:25,915336	192.168.0.103	157.240.224.60	TCP	1446	64012 → 443 [ACK] Seq=34274 Ack=1 Win=1019 Len=1392 [TCP segm…	
3492	2024-06-17 21:09:25,915336	192.168.0.103	157.240.224.60	TLSv1.2	803		Application Data
3493	2024-06-17 21:09:25,915457	192.168.0.103	157.240.224.60	TLSv1.2	85		Application Data

Рисунок 2.22 - Перехоплені мережеві пакетів даних, що містять голосове повідомлення

На рисунку 2.22 зображені загальні відомості про пакети даних у вигляді таблиці, стовпці якої зліва направо мають такі назви:

- номер пакету за весь час процесу перехоплення пакетів;
- дата та час (враховуючи мілісекунди) надсилання пакету;
- IP-адресу джерела пакету;
- IP-адресу кінцевої точки пакету;
- назва протоколу пакету;
- розмір пакету;
- загальна інформація про пакет.

На рисунку 2.22 зображені пакети надсилаються до хосту за IP-адресою 157.240.224.60. За допомогою вебсервісу «2IP» було з'ясовано, що цей хост є сервером, який належить компанії «Meta Platforms Inc.», яка є власником месенджеру «WhatsApp», та знаходиться у Менло Парк, США.

З рисунку 2.22 стало відомо, що відправлення голосового повідомлення в десктопному додатку месенджеру «WhatsApp» відбувається партіями пакетів даних за протоколами «TCP» та «TLS».

На рисунках 2.23, 2.24 та 2.25 зображено детальна інформація про початковий, проміжковий та кінцевий пакет даних за протоколом «TLS», які відповідають надісланому голосовому повідомленню, відповідно.

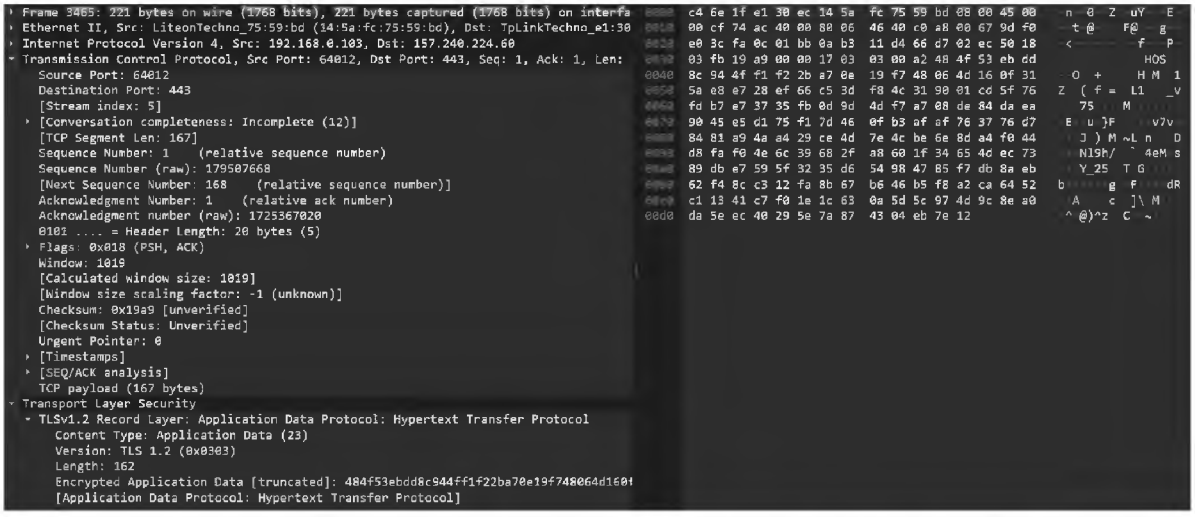


Рисунок 2.23 - Початковий пакет даних надісланого голосового повідомлення

Рисунок 2.24 - Проміжковий пакет даних надісланого голосового повідомлення

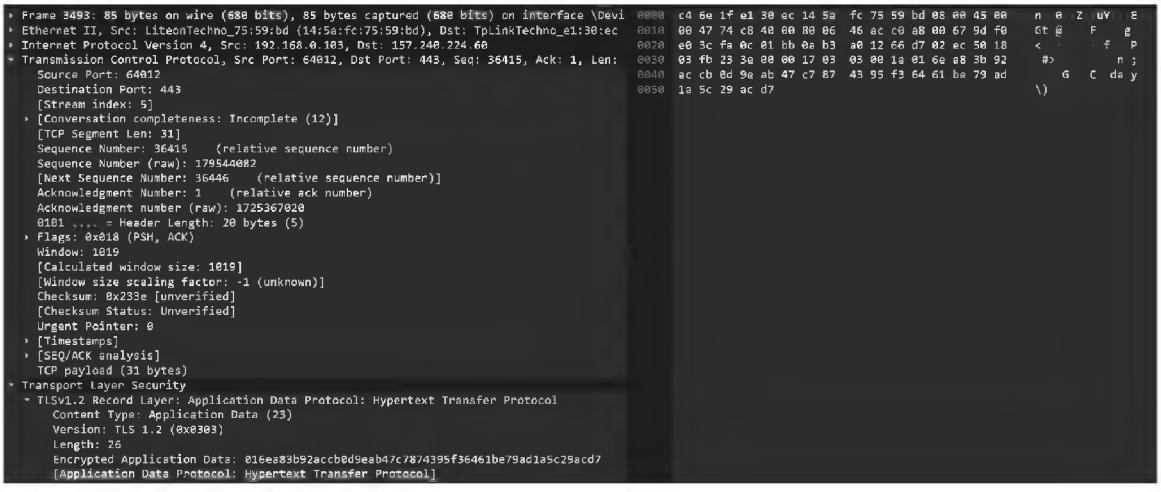


Рисунок 2.25 - Кінцевий пакет даних надісланого голосового повідомлення

На рисунках 2.23, 2.24 та 2.25 в лівій частині зображено складові зображених пакетів даних, а в правій частині - байти пакетів даних. Також на зазначених рисунках зображено деталі складових «Transmission Control Protocol» та «Transport Layer Security».

На рисунку 2.23 у складовій «Transmission Control Protocol» є поле «Sequence Number», значення якого дорівнює 1, що вказує на те, що на зазначеному рисунку зображений пакет даних є початковим у списку пакетів даних, які відносяться до голосового повідомлення. На рисунку 2.24 у складовій «Transmission Control Protocol» є поле «Sequence Number», значення якого дорівнює 15480, що вказує на те, що на зазначеному рисунку зображений пакет даних є проміжковим у списку пакетів даних, які відносяться до голосового повідомлення. На рисунку 2.25 у складовій «Transmission Control Protocol» є поле «Sequence Number», значення якого дорівнює 36415, а також зменшений обсяг надісланих даних вказують на те, що на зазначеному рисунку зображений пакет даних є кінцевим у списку пакетів даних, які відносяться до голосового повідомлення.

На рисунку 2.23, 2.24 та 2.25 у складовій «Transport Layer Security» є поле «Encrypted Application Data», значеннями яких є рядки чисел за шістнадцятковою системою числення, та які розподіленні по пакетах даних за протоколом «TCP». Це вже вказує на те, що голосове повідомлення надсилається у зашифрованому вигляді.

Після розрахунку всього об'єму надісланих даних, розмір яких склав 36 420 байтів, було зроблено порівняння з розміром вихідного голосового повідомлення, розмір якого склав 36 134 байти. За результатами порівняння можна стверджувати, що голосове повідомлення було попередньо оброблено, що призвело до збільшення обсягу надісланих даних, що свідчить про те, що голосове повідомлення відправляється в зашифрованому вигляді.

З розглянутих мережевих пакетів даних можна зробити висновок, що голосові повідомлення, надіслані через десктопний додаток месенджеру «WhatsApp», передаються у зашифрованому вигляді.

2.9 Перевірка наявності метаданих в фотографіях та відео, що надсилаються та публікуються через десктопному додатку месенджеру «WhatsApp»

Для виконання цього експерименту одним з добровольців досліднику була надіслана фотографія двома способами: як зображення та як файл. Дослідником було завантажено через

десктопний додаток «WhatsApp» 2 файли: фотографія, яка була надіслана як зображення та фотографія, яка була надіслана як файл. Обидві завантажені фотографії були перевірені на допомогою утиліти «JPEGsnoop» на наявність метаданих.

На рисунку 2.26 зображено звіт з результатами перевірки на наявність метаданих завантаженої фотографії, яка була надіслана як зображення.

```
JPEGsnoop 1.8.0 by Calvin Hass
  http://www.impulseadventure.com/photo/
  ---------------------------------------

  Filename: [C:\Users\alexb\Downloads\Зображення WhatsApp, дата_ 2024-06-20 о 11.27.29_4810d05c.jpg]
  Filesize: [175498] Bytes

Start Offset: 0x00000000
*** Marker: SOI (xFFD8) ***
  OFFSET: 0x00000000

*** Marker: APP0 (xFFE0) ***
  OFFSET: 0x00000002
  Length     = 16
  Identifier = [JFIF]
  version    = [1.1]
  density    = 1 x 1 (aspect ratio)
  thumbnail  = 0 x 0
```

Рисунок 2.26 - Звіт з результатами перевірки завантаженої фотографії, яка була надіслана як зображення

З рисунку 2.26 можна побачити з поля «Filesize», що завантажена фотографія, яка надіслана як фотографія, має розмір 175498 байт. Також результат перевірки не показав наявності метаданих.

На рисунку 2.27 та 2.28 зображено звіт з результатами перевірки на наявність метаданих завантаженої фотографії, яка була надіслана як файл.

```
JPEGsnoop 1.8.0 by Calvin Hass
  http://www.impulseadventure.com/photo/
  ---------------------------------------

  Filename: [C:\Users\alexb\Downloads\IMG_20240608_101251.jpg]
  Filesize: [2873892] Bytes
```

Рисунок 2.27 - Частина звіту з результатами перевірки завантаженої фотографії, яка була надіслана як файл

Рисунок 2.28 - Частина звіту з результатами перевірки завантаженої фотографії, яка була надіслана як файл

З рисунку 2.27 видно, що фотографія, яка була надіслана як файл, має розмір 2873892 байт, що значно більше за розмір фотографії, яка була надіслана як зображення. На рисунку 2.28 можна побачити, що за результатами перевірки було виявлено метадані у фотографії, зокрема час фотографування.

2.10 Висновки

За результатами проведеного дослідження було підтверджено наявність шифрування текстових та голосових повідомлень під час їх обміну в приватних чатах соціальної мережі «Instagram» та месенджерів «Telegram» і «WhatsApp». За допомогою сніферу «Wireshark» було з’ясовано, яким чином надсилаються текстові та голосові повідомлення та які протоколи використовуються для транспортування даних.

Текстові повідомлення, що надсилаються через десктопний додаток «Instagram», передаються через мережеві пакети даних за протоколами «TCP» та «TLS» версії 1.2. «TCP» використовуються для транспортування даних, «TLS» для шифрування повідомлень за допомогою вбудованих алгоритмів шифрування. Текстові повідомлення, що надсилаються через десктопний додаток «Telegram», передаються та шифруються за допомогою мережевих пакетів даних за протоколом «MTProto», який є розробкою та власністю розробників «Telegram». Текстові повідомлення, що надсилаються через десктопний додаток «WhatsApp», передаються за допомогою мережевих пакетів даних за протоколом «TCP», а шифруються за допомогою вбудованих алгоритмів шифрування.

Голосові повідомлення, що надсилаються через десктопний додаток «Instagram», транспортуються та шифруються за допомогою мережевих пакетів даних за протоколом «QUIC». Голосові повідомлення, що надсилаються через десктопний додаток «Telegram», передаються та шифруються за допомогою мережевих пакетів даних за протоколом «MTProto», який є розробкою та власністю розробників «Telegram». Голосові повідомлення, що надсилаються через десктопний додаток «WhatsApp», передаються через мережеві пакети даних за протоколами «TCP», в свою чергу шифруються за допомогою алгоритмів шифрування протоколу «TLS» версії 1.2.

Під час проведення дослідження було перевірено наявність метаданих в фотографіях, що надсилаються через месенджери «Telegram» і «WhatsApp» та які публікуються в соціальній мережі «Instagram». За результатами перевірки було виявлено, що фотографії, які надіслані як файл через «Telegram» і «WhatsApp», містять в собі метадані, які можуть вказувати на час фотографування та місцерозташування під час фотографування. Натомість було з'ясовано, що фотографії, які опубліковані в «Instagram» та фотографії, які відправленні як зображення через «Telegram» і «WhatsApp», не мають метаданих.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

У цьому розділі буде проведено розрахунок трудомісткості дослідження для розрахунку витрат на проведення дослідження. Буде проведено детальний розрахунок витрат на проведення дослідження. Для національних служб та комерційних компаній буде проведено розрахунок можливих річних експлуатаційних витрат, які б виникли через вивчення та аналізу результатів описаного в цій кваліфікаційній роботі дослідження. Буде зроблено огляд на можливі збитки, які виникнуть через використання соціальної мережі «Instagram» та месенджерів «Telegram» і «WhatsApp».

3.1 Розрахунок трудомісткості проведення дослідження

Трудомісткість проведення дослідження визначається часом, що було витрачено:

- на складання інструкції для проведення дослідження;
- на визначення технічних та програмних засобів, що використовувались для проведення дослідження;
- на пошук добровольців, що приймали участь у проведенні дослідження;
- на проведення дослідження;
- на аналіз отриманих результатів проведеного дослідження;
- на документування результатів проведеного дослідження та висновків, що були отримані після аналізу результатів.

Трудомісткість проведеного дослідження буде вирахувано за формулою:

$$t = t_{\text{ін}} + t_{\text{вз}} + t_{\text{пд}} + t_{\text{прд}} + t_{\text{ар}} + t_{\text{др}}, \text{годин}, \quad (3.1)$$

де t - це шукана трудомісткість проведеного дослідження;

$t_{ін}$ - це час, витрачений на складання інструкції проведення дослідження та дорівнює 2 годинам;

$t_{вз}$ - це час, витрачений на визначення технічних та програмних засобів та дорівнює 4 годинам;

$t_{пд}$ - це час, витрачений на пошук добровольців та дорівнює 48 годинам;

$t_{прд}$ - це час, витрачений на проведення дослідження та дорівнює 24 годинам;

$t_{ар}$ - це час, витрачений на аналіз результатів дослідження та дорівнює 96 годинам;

$t_{др}$ - це час, витрачений на документування результатів дослідження та аналізу та дорівнює 144 годинам.

За формулою (3.1), підставивши значення, знайдемо шукану трудомісткість проведення дослідження:

$$t = 2 + 4 + 48 + 24 + 96 + 144 = 318 \text{годин.}$$

Отже, трудомісткість проведення дослідження дорівнює 318 годинам.

3.2 Розрахунок витрат на проведення дослідження

Витрати на проведення дослідження визначаються заробітною платою спеціаліста з кібербезпеки, яку необхідно заплатити за проведення цього дослідження, аналізу та документування результатів дослідження та аналізу, а також вартістю машинного часу, потрібного для проведення дослідження, його аналізу та документування.

Витрати на проведення дослідження буде вирахувано за формулою:

$$В_д = З_{кб} + З_{мч} + З_{дв}, \text{грн,} \quad (3.2)$$

де $В_д$ - це витрати на проведення дослідження, грн;

$З_{кб}$ - це заробітна плата спеціаліста з кібербезпеки, яку отримає спеціаліст за проведення дослідження, аналіз та документування результатів дослідження та аналізу, грн;

$З_{мч}$ - це вартість машинного часу, потрібного для проведення дослідження, його аналізу та документування, грн;

$З_{дв}$ - це витрати на грошове заохочення добровольців, грн.

Заробітна плата спеціаліста з кібербезпеки, яку отримає спеціаліст за проведення дослідження, аналіз та документування результатів дослідження та аналізу визначається за формулою:

$$З_{кб} = t \cdot З_{гкб}, грн, \quad (3.3)$$

де $З_{кб}$ - це заробітна плата спеціаліста з кібербезпеки, яку отримає спеціаліст за проведення дослідження, аналіз та документування результатів дослідження та аналізу, грн;

t - це трудомісткість проведення дослідження, годин;

$З_{гкб}$ - це середньогодинна заробітна плата спеціаліста з кібербезпеки, грн.

Середньогодинна заробітна плата спеціаліста з кібербезпеки визначається середньою заробітною платою спеціаліста з кібербезпеки, розділеною на середню кількість діб у місяці та кількість годин у добі та знаходиться за формулою:

$$З_{гкб} = \frac{З_{скб}}{720}, грн, \quad (3.4)$$

де $З_{гкб}$ - це середньогодинна заробітна плата спеціаліста з кібербезпеки, грн;

$З_{скб}$ - це середня заробітна плата спеціаліста з кібербезпеки, грн.

Середня заробітна плата спеціаліста з кібербезпеки в Україні за місяць становить 30000 гривень. Знайдемо за формулою (3.4) середньогодинну заробітну плату спеціаліста з кібербезпеки:

$$З_{гкб} = \frac{30000}{720} = 41{,}67грн.$$

За формулою (3.3) знайдемо заробітну плату спеціаліста з кібербезпеки, яку отримає спеціаліст за проведення дослідження, аналіз та документування результатів дослідження та аналізу:

$$З_{кб} = 318 \cdot 41{,}67 = 13251{,}06грн$$

Вартість машинного часу, потрібного для проведення дослідження, його аналізу та документування, визначається за формулою:

$$З_{мч} = t \cdot С_{мч}, грн, \quad (3.5)$$

де $З_{мч}$ - це вартість машинного часу, потрібного для проведення дослідження, його аналізу та документування, грн;

t - це трудомісткість проведення дослідження, годин;

$С_{мч}$ - це вартість 1 години машинного часу ПК, грн;

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = P \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{грн}, \quad (3.6)$$

де $C_{мч}$ - це вартість 1 години машинного часу ПК;

P - це потужність ПК, кВт;

C_e - це тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ - це залишкова вартість ПК на поточний рік проведення дослідження, грн;

$Н_а$ - це річна норма амортизації на ПК, частка одиниці;

$К_{лпз}$ - це вартість ліцензійного програмного забезпечення, грн;

$Н_{апз}$ - це річна норма амортизації на ліцензійне програмне забезпечення, частка одиниці;

$F_р$ - це річний фонд робочого часу за 40-годинного робочого тижня та дорівнює 1920 годинам.

Потужність ПК, що використовується в дослідженні, дорівнює 0,18 кВт. Тариф на електричну енергію дорівнює 4,32 грн/кВт·година. Вартість ліцензійного програмного забезпечення визначається лише вартістю ОС «Windows» версії 11 та дорівнює 6800 грн. Залишкова вартість ПК визначається первісною вартістю ПК та накопиченою амортизацією ПК. Накопичена амортизація ПК визначається річною амортизацією ПК та кількістю минулих років використання ПК. Річна амортизація ПК визначається різницею між первісною вартістю ПК та ліквідаційною вартістю ПК, поділеною на строк служби ПК. Отже, залишкову вартість ПК знайдемо за формулою:

$$Ф_{зал} = В_п - \frac{В_п - В_л}{С_{сл}} \cdot К_{мр}, \text{грн}, \quad (3.7)$$

де $Ф_{зал}$ - це залишкова вартість ПК на поточний рік проведення дослідження, грн;

$В_п$ - це первісна вартість ПК та дорівнює 50000 грн;

$В_л$ - це ліквідаційна вартість ПК та дорівнює 20000 грн;

$С_{сл}$ - це строк служби ПК та дорівнює 10 років;

$К_{мр}$ - це кількість минулих років використання ПК та дорівнює 2 роки.

За формулою (3.7) знайдемо залишкову вартість ПК на поточний рік проведення дослідження:

$$Ф_{зал} = 50000 - \frac{50000 - 20000}{10} \cdot 2 = 44000грн.$$

Річна норма амортизації на ПК визначається за формулою:

$$Н_а = 1 - \frac{1}{К_{мр}}, \quad (3.8)$$

де H_a - це річна норма амортизації на ПК;

$K_{мр}$ - це кількість минулих років використання ПК та дорівнює 2 роки.

За формулою (3.8) знайдемо річну норму амортизації на ПК:

$$Н_а = 1 - \frac{1}{2} = 0,5.$$

Річна норма амортизації на ліцензійне програмне забезпечення визначається за формулою:

$$Н_{апз} = 1 - \frac{1}{К_{мрпз}}, \quad (3.8)$$

де $H_{апз}$ - це річна норма амортизації на ліцензійне програмне забезпечення;

$K_{мрпз}$ - це кількість минулих років використання ліцензійного програмного забезпечення та дорівнює 0,5 року.

За формулою (3.9) знайдемо річну норму амортизації на ПК:

$$Н_{апз} = 1 - \frac{1}{0,5} = -1.$$

За формулою (3.6) знайдемо вартість 1 години машинного часу ПК:

$$С_{мч} = 0,18 \cdot 4,32 + \frac{44000 \cdot 0,5}{1920} + \frac{6800 \cdot -1}{1920} = 8,7грн$$

За формулою (3.5) знайдемо вартість машинного часу, потрібного для проведення дослідження, його аналізу та документування:

$$З_{мч} = 318 \cdot 8,7 = 2766,6грн.$$

Витрати на грошове заохочення добровольців склали 650 грн. За формулою (3.2) знайдемо витрати на проведення дослідження:

$$В_д = 13251,06 + 2766,6 + 650 = 16667,66грн.$$

Отже, витрати на проведення дослідження дорівнюють 16667,66 грн.

3.3 Розрахунок можливих річних експлуатаційних витрат за результатами проведення дослідження

Результати дослідження, яке представлене в цій кваліфікаційній роботі, можуть спонукати приватні компанії та національні служби, такі як Державна служба з надзвичайних ситуацій (ДСНС), до запровадження змін та навчання працівників.

Для національних служб можливі річні експлуатаційні витрати визначаються за формулою:

$$С = С_{нк} + С_{рп}, \quad (3.9)$$

де *С* - можливі експлуатаційні витрати;

$С_{нк}$ - це витрати на навчальні курси з кібербезпеки;

$С_{рп}$ - це витрати на розробку правил або політик, що стосуються кібербезпеки.

Для приватних компаній можливі річні експлуатаційні витрати визначаються за формулою:

$$С = С_{нк} + С_{рп} + С_{пк}, \quad (3.10)$$

де *С* - можливі експлуатаційні витрати;

$С_{нк}$ - це річні витрати на навчальні курси з кібербезпеки;

$С_{рп}$ - це витрати на розробку правил або політик, що стосуються кібербезпеки;

$С_{пк}$ - це річні витрати на покращення, що стосуються комфортності користування соціальними мережами або месенджерами.

Для національних служб річні витрати на навчальні курси з кібербезпеки та інформаційної безпеки буде вирахувано за умови, що навчальні курси проводяться раз на рік та були придбані за середньою ціною. Для приватних компаній річні витрати на навчальні курси з кібербезпеки та інформаційної

безпеки буде вирахувано за умови, що навчальні курси проводяться 2 рази на рік. Середня ціна на курси з кібербезпеки складає 2000 грн. Отже, витрати на навчальні курси визначаються за формулою:

$$С_{нк} = n \cdot В_к, грн, \quad (3.11)$$

де $С_{нк}$ - це витрати на навчальні курси з кібербезпеки;

n - це кількість разів проходження курсів за рік;

$В_к$ - це середня вартість на курси з кібербезпеки.

З формули (3.11) знайдемо витрати на навчальні курси з кібербезпеки для національних служб:

$$С_{нк} = 1 \cdot 2000 = 2000грн$$

З формули (3.11) знайдемо витрати на навчальні курси з кібербезпеки для приватних компаній:

$$С_{нк} = 2 \cdot 2000 = 4000грн$$

Витрати на розробку правил або політик, що стосуються кібербезпеки та інформаційної безпеки, визначаються за формулою:

$$С_{рп} = (t_р + t_д) \cdot С_{мч}, грн, \quad (3.12)$$

де $С_{рп}$ - це витрати на розробку правил або політик;

$t_р$ - це час, витрачений на розробку правил або політик та дорівнює 96 годин;

$t_д$ - це час, витрачений на документування розроблених правил або політик та дорівнює 24 години;

$С_{мч}$ - це вартість 1 години машинного часу.

З пункту 3.2 відомо, що вартість 1 години машинного часу дорівнює 8,7 грн. Отже, за формулою (3.12) знайдемо витрати на розробку правил або політик з кібербезпеки та інформаційної безпеки:

$$С_{рп} = (96 + 24) \cdot 8,7 = 304,8грн.$$

Для приватних компаній додатковими річними експлуатаційними витратами може бути придбання преміум-аккаунтів в соціальних мережах або месенджерах для працівників. Отже, витрати на покращення, що стосуються комфортності користування соціальними мережами або месенджерами, визначаються за формулою:

$$С_{пк} = N_п \cdot В_{па}, \quad (3.13)$$

де $C_{пк}$ - це витрати на покращення, що стосуються комфортності користування соціальними мережами або месенджерами;

$N_п$ - це кількість працівників в компанії;

$B_{па}$ - це вартість преміум-аккаунтів, грн.

За середню кількість працівників в приватній компанії було встановлено 100 працівників. Серед можливих преміум-аккаунтів можливе лише придбання підписки «Telegram Premium»[1)] на місяць для месенджеру «Telegram», яка коштує 115 грн. За формулою (3.13) знайдемо витрати на покращення, що стосуються комфортності користування соціальними мережами або месенджерами:

$$С_{пк} = 100 \cdot 115 = 11500грн.$$

За формулою (3.9) знайдемо можливі річні експлуатаційні витрати для національних служб:

$$С = 2000 + 304{,}8 = 2304{,}8грн.$$

За формулою (3.10) знайдемо можливі річні експлуатаційні витрати для приватних компаній:

$$С = 2000 + 304{,}8 + 11500 = 13804{,}8грн.$$

Отже, можливі річні експлуатаційні витрати для національних служб складає 2304,8 грн, а для приватної компанії - 13804,8 грн.

3.4 Можливі економічні збитки від злому облікового запису працівника

Можливі економічні збитки від злому облікового запису працівника розглянемо на прикладі працівника приватної компанії, яка є власницею вебзастосунку, який надає детальну фінансову статистику власникам інтернет-магазинів.

[1)] «Telegram Premium» — це необов'язкова підписка, що надає доступ до додаткових

Можливі економічні збитки, що розглядаються, визначаються за формулою:

$$З_е = В_{ві} + В_{зд} + В_с, грн, \quad (3.14)$$

де $З_е$ - можливі економічні збитки;

$В_{ві}$ - витрати на повторне введення інформації, що була втрачена, грн;

$В_{зд}$ - втрати від зниження очікуваного доходу, грн;

$В_с$ - судові витрати, грн.

Через злом та отримання несанкціонованого доступу до облікового запису від соціальної мережі або месенджеру зловмисник може отримати доступ до баз даних, де зберігаються облікові дані та інші дані користувачів вебзастосунком компанії. Зловмисник може їх видалити, що призведе до її повторного введення, якщо відсутні актуальні копії баз даних. Витрати на повторне введення інформації, що була втрачена, визначається за формулою:

$$В_{ві} = t_{ві} \cdot З_{п}, грн, \quad (3.15)$$

де $В_{ві}$ - витрати на повторне введення інформації, що була втрачена;

$t_{ві}$ - час, потрібний для повторного введення інформації, годин;

$З_п$ - годинна заробітна плата працівника, яка дорівнює 41,67 грн.

Час, потрібний для повторного введення інформації, залежить від масштабу втрачених даних і визначається за формулою:

$$t_{ві} = n_{вз} \cdot t_{вз}, годин, \quad (3.16)$$

де $t_{ві}$ - час, потрібний для повторного введення інформації;

$n_{вз}$ - кількість записів, які потрібно відновити;

$t_{вз}$ - час, потрібний на відновлення одного запису, годин.

Для розрахунку часу, потрібного для повторного введення інформації, було визначено, що необхідно відновити 10000 записів, та потрібно 5 хвилин на відновлення одного запису.

За формулою (3.16) було розраховано час, потрібний для повторного введення інформації:

$$t_{ві} = 10000 \cdot 5 = 50000хв = 833годин.$$

За формулою (3.15) було розраховано витрати на повторне введення інформації, що була втрачена:

$$В_{ві} = 833 \cdot 41{,}67 = 34711{,}11грн.$$

Злом облікового запису працівника приватної компанії може зменшити довіру користувачів до вебзастосунку компанії, і вони можуть припинити користування ним, що призведе до зменшення доходу від вебзастосунку. Втрати від зниження очікуваного доходу визначаються за формулою:

$$В_{зд} = n_{к} \cdot В_{п}, грн, \quad (3.17)$$

де $В_{зд}$ - втрати від зниження очікуваного доходу, грн;

$n_к$ - кількість користувачів;

$B_п$ - вартість місячної підписки на вебзастосунок, грн.

Для розрахунку втрат від зниження очікуваного доходу, було визначено, що 800 користувачів відмовились від підписки. Вартість місячної підписки на вебзастосунок складає 1200 грн.

За формулою (3.17) було розраховано втрати від зниження очікуваного доходу:

$$В_{зд} = 800 \cdot 1200 = 960000 грн.$$

Судові витрати викликані розслідуванням та позовом до суду з метою виявлення та притягнення зловмисника до відповідальності та визначаються за формулою:

$$В_с = З_с + В_{юп} + В_е + В_с + В_а, грн, \quad (3.18)$$

де $B_с$ - судові витрати;

$З_с$ - судовий збір, який дорівнює 3028 грн;

$B_{юп}$ - витрати на юридичні послуги, грн;

$B_е$ - витрати на проведення експертизи, грн;

$B_с$ - витрати, що пов'язані зі свідками, грн;

$B_а$ - витрати на адміністративні справи.

Для розрахунку судових витрат було визначено, що витрати на проведення експертизи дорівнює 10000 грн, витрати, що пов'язані зі свідками, дорівнюють 5000 грн, витрати на адміністративні справи, а саме витрати на копіювання документів, поштові витрати, нотаріальне засвідчення документів тощо, дорівнюють 2000 грн.

Витрати на юридичні послуги визначаються за формулою:

$$В_{юп} = В_к + В_{поз} + В_{пс}, грн, \quad (3.19)$$

де $B_{юп}$ - витрати на юридичні послуги;

$B_к$ - витрати на консультацію, які дорівнюють 10000 грн;

$B_{поз}$ - витрати на підготовку та подачу позову, які дорівнюють 40000 грн;

$B_{пс}$ - витрати на представництво в суді, які дорівнюють 30000 грн.

За формулою (3.19) розрахуємо витрати на юридичні послуги:

$$В_{юп} = 10000 + 40000 + 30000 = 80000грн.$$

За формулою (3.18) розрахуємо судові витрати:

$$В_с = 3028 + 10000 + 5000 + 2000 + 80000 = 100028грн.$$

За формулою (3.14) розрахуємо можливі економічні збитки від злому облікового запису працівника:

$$З_е = 34711,11 + 960000 + 100028 = 1094739,11грн.$$

Отже, можливі економічні збитки від злому облікового запису працівника дорівнюють 1094739,11 грн.

3.5 Висновки

У цьому розділі було проведено розрахунок трудомісткості дослідження та детальний розрахунок витрат на проведення дослідження. Розрахована трудомісткість дослідження складає 318 годин, розраховані витрати на проведення дослідження, що описане в цій кваліфікаційній роботі, склали 16667,66 грн.

Для національних служб та приватних компаній було проведено розрахунок можливих річних експлуатаційних витрат, які б виникли через вивчення та аналізу результатів описаного в цій кваліфікаційній роботі дослідження. Для національних служб вони склали 2304,8 грн, для комерційних компаній - 13804,8 грн.

Для приватної компанії, яка є власницею вебзастосунку, який надає детальну фінансову статистику власникам інтернет-магазинів, було розраховано можливі економічні збитки від злому облікового запису працівника. Вони склали 1094739,11 грн.

ВИСНОВКИ

Під час проведення дослідження було проведено загальний огляд функціоналу та інформації, що оброблюється та створюється в соціальній мережі «Instagram» та месенджерах «Telegram» і «WhatsApp». Було досліджено мережевий трафік, який виникає під час обміну текстовими та голосовими повідомленнями, а також наявність метаданих в надісланих фотографіях.

На основі результатів дослідження було зроблено висновок, що використання месенджеру «Telegram» є небезпечним для працівників національних служб, такі як ДСНС України та Національна поліція України, та військових, оскільки було встановлено, що розробники та власники цього месенджеру можуть мати зв'язки з спеціальними службами Російської Федерації. Використання «Telegram» зазначеними категоріями людей може нести небезпеку національній безпеці та суверенітету України. Рекомендованим до використання серед розглянутих є месенджер «WhatsApp», проте і він має недолік, який полягає в тому, що фотографії та інші медіа, надіслані через нього як файл, містять метадані. Для незалежних користувачів розглянуті соціальна мережа та месенджери є безпечними для використання з огляду на програмну складову розглянутих сервісів для обміну повідомленнями та публікації фотографій.

Розглянуті випадки злому облікових записів вказують неповноцінність захисних методів, які направлені лише на захист повідомлень від перехоплень та злому, проте не захищають користувачів від атак, що ґрунтуються на методах соціальної інженерії. Подальші розробки та дослідження в галузі кібербезпеки повинні ґрунтуватись на забезпеченні захисту користувачів від атак, наприклад, за допомогою технологій штучного інтелекту та машинного навчання, які б у реальному часі визначали б шахрайські дії.

ПЕРЕЛІК ПОСИЛАНЬ

1. Соціальна інженерія - що це?. GridinSoft. Дата оновлення: 06.10.2023. URL: https://gridinsoft.ua/social-engineering (дата звернення: 05.06.2024);

2. Що таке Бекдор? Визначення, приклади, бекдор-атаки. GridinSoft. Дата оновлення: 06.10.2023. URL: https://gridinsoft.ua/backdoor (дата звернення: 05.06.2024);

3. Ботнет. Вікіпедія. Дата оновлення: 30.05.2024. URL: https://uk.wikipedia.org/wiki/Ботнет (дата звернення 05.06.2024);

4. Instagram. Вікіпедія. Дата оновлення: 07.06.2024. URL: https://uk.wikipedia.org/wiki/Instagram (дата звернення: 08.06.2024);

5. Eastman Kodak. Вікіпедія. Дата оновлення: 05.08.2023. URL: https://uk.wikipedia.org/wiki/Eastman_Kodak (дата звернення: 08.06.2024);

6. Polaroid. Вікіпедія. Дата оновлення: 05.09.2023. URL: https://uk.wikipedia.org/wiki/Polaroid (дата звернення: 08.06.2024);

7. Мобілографія. EverybodyWiki. Дата оновлення: 28.03.2023. URL: https://uk.everybodywiki.com/Мобілографія (дата звернення: 08.06.2024);

8. Як цитувати допис з «Instagram»?. Grafiati. Дата оновлення: 01.02.2023. URL: https://www.grafiati.com/uk/blogs/how-to-cite-an-instagram-post/ (дата звернення: 08.06.2024);

9. 2022 Consumer Impact Report. Identity Theft Resource Center. Дата оновлення: 01.09.2022. URL: https://www.idtheftcenter.org/wp-content/uploads/2022/09/2022-Consumer-Impact-Report_V3.4_Final_Linked.pdf (дата звернення: 09.06.2024). С. 37;

10. Hacked Instagram Account: 3 Ways To Protect Yourself. Format. Дата оновлення: 19.09.2017. URL: https://www.format.com/magazine/resources/photography/hacked-instagram-account-protect (дата звернення: 09.06.2024);

11. How to Recover a Hacked Instagram Account [Step by Step]. Aura. Дата оновлення: 16.01.2023. URL: https://www.aura.com/learn/my-instagram-was-hacked-what-to-do (дата звернення: 09.06.2024);

12. AG HENRY IN LETTER TO META: INVESTIGATE CAUSES OF SPIKE IN "ACCOUNT TAKEOVERS," INCREASE PROTECTION FOR CONSUMERS. Pennsylvania Attorney General Michelle A. Henry. Дата оновлення: 06.03.2024. URL: https://www.attorneygeneral.gov/taking-action/ag-henry-in-letter-to-meta-investigate-causes-of-spike-in-account-takeovers-increase-protection-for-consumers/ (дата звернення 09.06.2024);

13. Identity Theft Resource Center. Wikipedia. Дата оновлення: 22.01.2024. URL: https://en.wikipedia.org/wiki/Identity_Theft_Resource_Center (дата звернення 09.06.2024);

14. Telegram. Вікіпедія. Дата оновлення: 09.06.2024. URL: https://uk.wikipedia.org/wiki/Telegram (дата звернення: 10.06.2024);

15. Чат-бот. Вікіпедія. Дата оновлення: 26.11.2023. URL: https://uk.wikipedia.org/wiki/Чат-бот (дата звернення: 10.06.2024);

16. Telegram-канал. Вікіпедія. Дата оновлення: 06.05.2024. URL: https://uk.wikipedia.org/wiki/Telegram-канал (дата звернення: 10.06.2024);

17. SMS-spoofing: як розпізнати шахрайство та захиститися від нього. Decision Telecom. Дата оновлення: 01.05.2024 URL: https://decisiontele.com/uk/news/sms-spoofing.html (дата звернення 13.06.2024);

18. Дуров обвинил власти РФ в попытках взлома телеграм-аккаунтов журналистов. Радио Свобода. Дата оновлення: 26.05.2019. URL: https://www.svoboda.org/a/29963567.html (дата звернення 13.06.2024);

19. Осторожно, происходят массовые попытки взлома телеграм-аккаунтов белорусов. UDF. Дата оновлення: 20.01.2024. URL: https://udf.name/news/main_news/264865-ostorozhno-proishodjat-massovye-popytki-vzloma-telegram-akkauntov-belorusov.html (дата звернення: 13.06.2024);

20. The Kremlin Has Entered the Chat. Wired. Дата оновлення: 27.04.2024. URL: https://www.wired.com/story/the-kremlin-has-entered-the-chat/ (дата звернення: 13.06.2024);

21. День тиші. Вікіпедія. Дата оновлення: 17.09.2023. URL: https://uk.wikipedia.org/wiki/День_тиші (дата звернення: 13.06.2024);

22. Telegram blocks then unblocks chatbots used by Ukraine's security services to get info on Russian activities. Euromaidan Press. Дата оновлення: 29.04.2024. URL: https://euromaidanpress.com/2024/04/29/telegram-blocks-then-unblocks-chatbots-used-by-ukraines-security-services-to-get-info-on-russian-activities/ (дата звернення: 13.06.2024);

23. ГУР: Telegram заблокував низку офіційних ботів, зокрема чат-бот української розвідки. Радіо Свобода. Дата оновлення: 29.04.2024. URL: https://www.radiosvoboda.org/a/news-telegram-boty-hur/32924640.html (дата звернення: 13.06.2024);

24. SSU exposes russian intelligence services on recruiting Ukrainian teenagers for anti-Semitic provocations. Security Service of Ukraine. Дата оновлення: 25.10.2023. URL: https://ssu.gov.ua/en/novyny/sbu-vykryla-spetssluzhby-rf-na-verbuvanni-ukrainskykh-pidlitkiv-dlia-antysemitskykh-provokatsii-u-riznykh-rehionakh-ukrainy (дата звернення: 13.06.2024);

25. Допоможи ЗСУ знищити окупанта: Мінцифра запускає чатбот єВорог. Міністерство цифрової трансформації України. Дата оновлення: 10.03.2022. URL: https://thedigital.gov.ua/news/dopomozhi-zsu-znishchiti-okupanta-mintsifra-zapuskae-chatbot-evorog (дата звернення: 13.06.2024);

26. Головний бот розвідки. Головне управління розвідки Міністерства оборони України. Дата оновлення: 13.06.2024. URL: https://gur.gov.ua/content/tg-bot.html (дата звернення: 13.06.2024);

27. WhatsApp. Вікіпедія. Дата оновлення: 25.05.2024. URL: https://uk.wikipedia.org/wiki/WhatsApp (дата звернення: 14.06.2024);

28. Series 40. Вікіпедія. Дата оновлення: 23.02.2023. URL: https://uk.wikipedia.org/wiki/S40 (дата звернення: 14.06.2024);

29. Symbian. Вікіпедія. Дата оновлення: 13.06.2024. URL: https://uk.wikipedia.org/wiki/Symbian (дата звернення: 14.06.2024);

30. Завантажити WhatsApp. WhatsApp. Дата оновлення: 14.06.2024. URL: https://www.whatsapp.com/download (дата звернення: 14.06.2024);

31. Нові функції статусу у WhatsApp. WhatsApp Blog. Дата оновлення: 07.02.2023. URL: https://blog.whatsapp.com/new-ways-to-enjoy-whatsapp-status (дата звернення: 14.06.2024);

32. Представляємо канали WhatsApp. Приватний спосіб стежити за тим, що дійсно важливо. WhatsApp Blog. Дата оновлення: 08.06.2023. URL: https://blog.whatsapp.com/introducing-whatsapp-channels-a-private-way-to-follow-what-matters (дата звернення: 14.06.2024);

33. Наше бачення спільнот у WhatsApp. WhatsApp Blog. Дата оновлення: 14.04.2022. URL: https://blog.whatsapp.com/sharing-our-vision-for-communities-on-whatsapp (дата звернення: 14.06.2024);

34. WhatsApp accounts almost completely unprotected. The H. Дата оновлення: 04.09.2012. URL: http://www.h-online.com/security/news/item/WhatsApp-accounts-almost-completely-unprotected-1708545.html (дата звернення: 15.06.2024);

35. WhatsApp threatens legal action against API developers. The H. Дата оновлення: 25.09.2012. URL: http://www.h-online.com/security/news/item/WhatsApp-threatens-legal-action-against-API-developers-1716912.html (дата звернення: 15.06.2024);

36. Crash Your Friends`WhatsApp Remotely with Just a Message. The Hacker News. Дата оновлення: 01.12.2014. URL: http://thehackernews.com/2014/12/crash-your-friends-whatsapp-remotely_1.html (дата звернення: 15.06.2024);

37. 17-Year-Old Found Bugs in WhatsApp Web and Mobile App. The Hacker News. Дата оновлення: 29.01.2015. URL: http://thehackernews.com/2015/01/whatsapp-web-mobile-app.html (дата звернення: 15.06.2024);

38. Уразливість в WhatsApp дозволяла зламувати акаунти через відеодзвінок. РБК-Україна. Дата оновлення: 10.10.2018. URL:

https://www.rbc.ua/ukr/news/uyazvimost-whatsapp-pozvolyala-vzlamyvat-1539181675.html (дата звернення: 15.06.2024);

39. WhatsApp fixes bug that let hackers take over app when answering a video call. ZDNet. Дата оновлення: 09.10.2018. URL: https://www.zdnet.com/article/whatsapp-fixes-bug-that-let-hackers-take-over-app-when-answering-a-video-call/ (дата звернення: 15.06.2024);
40. Recent wave of hijacked WhatsApp accounts traced back to voicemail hacking. ZDNet. Дата оновлення: 04.10.2018. URL: https://www.zdnet.com/article/recent-wave-of-hijacked-whatsapp-accounts-traced-back-to-voicemail-hacking/ (дата звернення: 15.06.2024);
41. WhatsApp Gold: Scammers trick mobile phone users into downloading malware. Independent. Дата оновлення: 25.05.2016. URL: https://www.independent.co.uk/tech/whatsapp-gold-plus-scam-malware-download-get-message-a7045606.html (дата звернення: 15.06.2024);
42. JPEGsnoop. GitHub. Дата оновлення: 19.07.2018. URL: https://github.com/ImpulseAdventure/JPEGsnoop (дата звернення 20.06.2024);
43. Огляд сервісу 2ip. Cityhost.ua. Дата оновлення: 10.01.2020. URL: https://cityhost.ua/uk/blog/obzor-servisa-2ip.html (дата звернення: 20.06.2024);
44. Наскрізне шифрування. Вікіпедія. Дата оновлення: 24.10.2023. URL: https://uk.wikipedia.org/wiki/Наскрізне_шифрування (дата звернення: 22.06.2024);
45. QUIC. Вікіпедія. Дата оновлення: 08.12.2023. URL: https://uk.wikipedia.org/wiki/QUIC (дата звернення: 22.06.2024);
46. STUN. Вікіпедія. Дата оновлення: 23.10.2022. URL: https://uk.wikipedia.org/wiki/STUN (дата звернення: 22.06.2024);

47. Transport Layer Security. Вікіпедія. Дата оновлення: 19.02.2024. URL: https://uk.wikipedia.org/wiki/Transport_Layer_Security (дата звернення: 22.06.2024);

48. Advanced Encryption Standard. Вікіпедія. Дата оновлення: 17.04.2024. URL: https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard (дата звернення: 22.06.2024);

49. Судові витрати:поняття, види, порядок оплати. WikiLegalAid. Дата оновлення: 31.01.2024. URL: https://wiki.legalaid.gov.ua/index.php/Судові_витрати:поняття,_види,_порядок_оплати (дата звернення: 25.06.2024).

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	1	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	4	
5	А4	1 Розділ	23	
6	А4	2 Розділ	27	
7	А4	3 Розділ	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	6	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Пояснювальна_записка.odt

2 Пояснювальна_записка.pdf

3 Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 85 б. «добре».

Керівник розділу _____ Д.П. Пілова

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:

Дослідження безпеки використання соціальної мережі «Instagram» та месенджерів «Telegram» і «WhatsApp»

студента групи 125-20-1

Бойченка Олександра Олександровича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 84 сторінках та містить 32 рисунка, 3 таблиці, 49 джерел та 4 додатка.

У роботі було продемонстровано володіння знаннями про класифікацію інформації, пошук та аналіз інформації в галузі кібербезпеки, вміння використовувати спеціалізоване ПЗ, вміння аналізувати результати, що повертає спеціалізоване ПЗ, знання з мережевих пакетів даних, знання з алгоритмів шифрування.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою, відповідає вимогам положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка». Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник