УДК 007.51:004.5

В. О. Головенько

СИСТЕМА ВИЯВЛЕННЯ ДЖЕРЕЛА ІНФОРМАЦІЙНОГО ВПЛИВУ В ІНТЕРНЕТ-ТРАФІКУ

Вінницький національний технічний університет

Анотація

Розроблено програмний засіб, що дозволяє виявити джерела інформаційного впливу серед інтернет-трафіку, а саме визначити належність IP-адреси до українських та присвоїти відповідні геолокаційні дані до кожної зі знайдених IP-адрес, такі як країна, область та місто.

Ключові слова: інформаційні війни, аналіз інтернет-трафіку, IP адреси, геолокаційні дані, модель передачі даних TCP/IP.

Abstract

The software that allows to detect the information influence sources,namely Ukrainian IP addresses among internet-traffic and to apply appropriate geolocation data to each of the found IP address was developed.

Keywords: information warfares, internet-traffic analysis, IP addresses, geolocation data, TCP/IP model of data transfer.

Вступ

Сьогодні, у час постійних інформаційних протиборств, існує проблема визначення країни та міста користувача, від імені якого було зроблено інформаційний вплив у вигляді текстового повідомлення, фотографій, відеоматеріалів тощо [1-4]. Важливим є завдання як знати, з якої IP-адреси була зроблена та чи інша дія, так і виявити, на які вузли було здійснено перехід користувача у процесі його інтернет-активності.

Результати дослідження

Розроблено систему виявлення українських IP-адрес в інтернет-трафіку, що складається з програмного засобу та бази даних українських IP-адрес. Інтернет-трафік – це файл великого розміру, який містить інформацію про пакет даних, на прикладному, транспортному, мережевому та канальному рівнях мережевої моделі передачі даних TCP/IP [5]. Зазвичай інтернет-трафік зберігається у файлі з розширенням *.pcap, тому програмний засіб аналізує трафік саме з файлів цього типу. Оскільки робота з IP-адресами відбувається на мережевому рівні за допомогою протоколу IP (Internet Protocol), інформація, що міститься на інших рівнях, фільтрується та не береться до уваги (рис. 1).

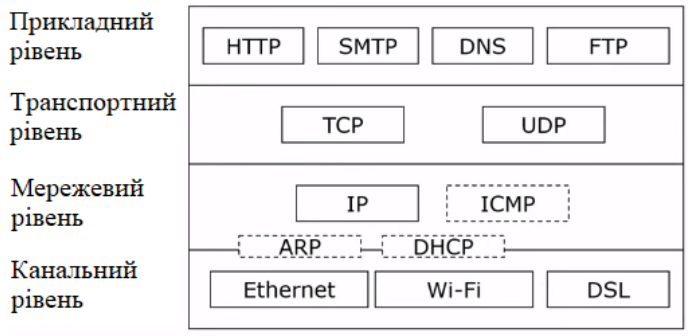

Рисунок 1 – Загальна схема мережевої моделі передачі даних TCP/IP

Протокол IP складається з наступних полів: версія (Version), довжина IP-заголовку (IP header Length — HLEN), тип обслуговування (Type of Service — TOS), загальна довжина (Total Length), ідентифікація (Identification), прапорці (Flags), зміщення фрагментації (Fragment Offset), час життя (Time-to-Live — TTL), протокол (Protocol), контрольна сума заголовку (Header Checksum), IP-адреса відправника (Source IP address), IP-адреса отримувача, опції (Options), підкладка (Padding), дані (Data)

[6]. Під час дослідження аналізуються IP-адреси, що знаходяться у двох полях: IP-адреса відправника та IP-адреса отримувача.

Пошук IP-адрес може відбуватися двома шляхами: за допомогою локальної бази даних IP-адрес, яку необхідно оновлювати раз на місяць для підтримування актуальності самої бази, а також за допомогою API, яке вимагає підключення до мережі Інтернет. Оскільки для дослідження використано безкоштовне API, швидкість пошуку IP-адрес, порівняно з пошуком у локальній базі даних, є значно меншою, що обумовлено обмеженою кількістю запитів до сервера API за певний проміжок часу.

Програмний засіб є простим та зручним у використанні. Для початку пошуку українських IP-адрес необхідно у програмному засобі вибрати файл з інтернет-трафіком та почати пошук.

Після завершення процесу пошуку українських IP-адрес на екран виводиться інформація у двох блоках: усі знайдені IP-адреси та власне усі знайдені українські IP-адреси. Для зручності обробки та збільшення швидкодії програмного засобу усі дублікати IP-адрес видаляються.

Для зручності подальшого аналізу отриманих результатів, українські IP-адреси записуються до файлу з розширенням *.csv, що являють собою базу даних, у форматі, що містить наступну інформацію: IP адреса, місто, область. Також програмний засіб має можливість оновлювати локальну базу даних та підтримувати її актуальність та показує час, що пішов на аналіз того чи іншого файлу з інтернет-трафіком.

Висновки

Розглянуто структуру мережевого рівня стеку протоколів TCP/IP, а саме протоколу IP (Internet Protocol). Розроблено програмний засіб, що дозволяє виявляти джерела інформаційного впливу під час інформаційних війн, а саме: аналізувати інтернет-трафік та виявляти українські IP-адреси з полів «IP-адреса відправника» та «IP-адреса отримувача» протоколу IP, а також визначати присвоєні їм відповідні геолокаційні дані, такі як країна, область та місто. Отримані результати записуються у файл для зручності подальшої роботи з ними.

REFERENCES

1. Лужецький В. А. Інформаційна безпека / Лужецький В. А., Войтович О. П., Дудатьєв А. В. // Навчальний посібник – Вінниця ВНТУ, 2009. – 240 с.
2. Voitovych O. Research of social networks as a source of information in warfare / Voitovych O., Holovenko V. // Inżynier XXI wieku projectujemy przyszlosc: monografia / pod red.: Jacek Rysiński. – Bielsko-Biała, 2016. – С. 111-119.
3. Войтович О.П., Дудатьєв А.В., Головенько В.О. Модель та засіб для виявлення фейкових облікових записів у соціальних мережах // Вчені записки таврійського національного університету ім. В.І. Вернадського. Серія: Технічні науки. Частина 1 – 2018. – № 1 Том 29 (68). – С. 112 – 119.
4. Дудатьєв А.В., Войтович О.П. Моделі інформаційної підтримки управління комплексною інформаційоною безпекою // Радіоелектроніка, інформатика, управління - 2017 - № 1 - С. 107-114.
5. The TCP/IP Protocol Stack [Електронний ресурс]. – Режим доступу до ресурсу : http://www.technologyuk.net/telecommunications/internet/tcp-ip-stack.shtml - назва з екрану.
6. IPv4 - Packet Structure [Електронний ресурс]. – Режим доступу до ресурсу : https://www.tutorialspoint.com/ipv4/ipv4_packet_structure.htm - назва з екрану.
7. Азарова А. О. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» / Азарова А. О., Карпінець В. В. // Методичні вказівки. – Вінниця : ВНТУ, 2013. – 44 с.

Головенько Віталій Олександрович — студент групи БС-18м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: torvald124@gmail.com

Науковий керівник: ***Войтович Олеся Петрівна*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Holovenko Vitalii O. — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: torvald124@gmail.com

Supervisor: ***Voitovych Olesia P.*** — Cand. Sc. (Eng), Assistant Professor of Cybersecurity, Vinnytsia National Technical University, Vinnytsia