УДК 343.98:004.77

НІЗОВЦЕВ Ю.Ю., *кандидат юридичних наук*, головний судовий експерт Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-7641-6403.

ПАРФИЛО О.А., *кандидат юридичних наук*, *старший науковий співробітник*, начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-8787-7478.

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ WI-FI МАРШРУТИЗАТОРІВ ДЛЯ ВСТАНОВЛЕННЯ МОБІЛЬНОГО ТЕРМІНАЛУ ТА ЙОГО МЕРЕЖЕВОЇ АКТИВНОСТІ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Анотація. *Досліджено можливості Wi-Fi маршрутизаторів для встановлення мобільного терміналу та його мережевої активності під час розслідування кіберзлочинів. Зокрема розкрито такі проблемні питання: яка доказова інформація може бути виявлена у Wi-Fi маршрутизаторі, як її зафіксувати і вилучити, а також обставини, що можуть перешкоджати пошуку зловмисника та доведенню його провини. Висвітлено роль та значення проведення експертизи електронних комунікацій або судової комплексної експертизи електронних комунікацій та комп'ютерно-технічної експертизи для аналізу лог-файлів на предмет відображення в них ознак кібератаки. Деталізовано особливості пошуку, фіксації та вилучення інформації про MAC-адресу мережевого інтерфейсу Wi-Fi-передавача.*

Ключові слова: *маршрутизатори, мобільні термінали, цифрові сліди, кіберзлочини, розслідування, спеціальні знання, дослідження, судова експертиза, методичні рекомендації.*

Summary: *The possibilities of Wi-Fi routers for establishing a mobile terminal and its network activity during the investigation of cybercrimes were investigated. In particular, the following problematic issues are revealed: what evidentiary information can be found in a Wi-Fi router, how to record and remove it, as well as circumstances that can hinder the search for an intruder and proving his guilt. The role and importance of electronic communications expertise or forensic comprehensive electronic communications expertise and computer-technical expertise to analyze log files for signs of a cyber attack are highlighted. The peculiarities of searching, fixing and extracting information about the MAC address of the network interface of the Wi-Fi transmitter are detailed.*

Keywords: *routers, mobile terminals, digital traces, cybercrimes, investigations, special knowledge, research, forensic examination, methodological recommendations.*

Постановка проблеми. Стрімкий розвиток сучасних цифрових технологій породжує пропорційно і кількість уразливостей в інформаційно-комунікаційних системах та відповідно зростає статистика вчинених кіберзлочинів із застосуванням комп'ютерних і телекомунікаційних пристроїв, особливо з використанням активного мережевого обладнання та можливостей Інтернет.

Наслідки цієї злочинності зачіпають не тільки інтереси окремих осіб, що стали жертвами, але й підприємства, установи, організації, державні органи і суспільство в цілому. Кіберзлочинність найчастіше ставить під загрозу критично важливі об'єкти

інфраструктури, які в багатьох країнах не контролюються публічним сектором, і такі посягання можуть вчиняти дестабілізуючий вплив як на окремих громадян, так і на національну безпеку держави.

Ефективність протидії злочинам, вчиненим у кіберпросторі, значною мірою визначається розумінням криміналістичної сутності способів їх вчинення та специфіки слідової картини. Крім того, потребує подальшого дослідження криміналістична характеристика правопорушень, що вчиняються з використанням комп'ютерних та мережевих технологій.

Слід зазначити, що використання інформації з Wi-Fi маршрутизаторів є актуальним під час розслідування різних злочинів. Наприклад, це може бути використання кіберзлочинцем публічної Wi-Fi мережі задля приховування слідів кібератаки. Або торговець речами, що мають обмеження обігу (зброя, наркотичні засоби тощо), може намагатись анонімізувати своє місцезнаходження під час переписки з покупцями, підключаючись до різних Wi-Fi мереж. Або це може бути просте користування мережею Wi-Fi на місці події, і встановлення факту такого користування буде доказом, що особа знаходилась на цьому місці.

Враховуючи актуальність описаної тематики, в Українському науково-дослідному інституті спеціальної техніки та судових експертиз СБ України було розроблено для спеціалістів та судових експертів методичні рекомендації "Використання можливостей Wi-Fi маршрутизаторів для встановлення мобільного терміналу та його мережевої активності" (далі – Методичні рекомендації) [1]. Основні положення вказаної науково-методичної праці буде представлено далі.

Результати аналізу наукових публікацій. Дослідженням проблемних аспектів використання спеціальних знань при фіксації, вилученні та збереженні цифрових (віртуальних) слідів, які утворюються під час вчинення правопорушення у кіберпросторі, присвячували свої праці такі науковці, як: Г.К. Авдєєва [2], Н.М. Ахтирська [3], В.Д. Басай [4], І.О. Крицька [5], Я. Найдьон [6], О.С. Омельян [7], О. А. Самойленко [8], А.В. Скрипник [9], Є.С. Хижняк [10] та інші.

Однак можна констатувати, що тема огляду та дослідження комп'ютерних і телекомунікаційних засобів (активного мережевого обладнання) під час розслідування злочинів, вчинених у кіберпросторі, досі залишає багато питань. Це й не дивно, враховуючи її об'єм та технічну складність. При цьому якісь аспекти залишаються невисвітленими повністю, якісь розкриті лише частково, а певну частину показано не зовсім коректно.

Зокрема, М.В. Кобець та Р.М. Кобець, описують використання можливостей Wi-Fi роутерів під час виявлення та розслідування кримінальних правопорушень [11]. Автори стверджують, що "...для автентифікації входу до інтерфейсу роутера необхідно в пошуковій колонці ввести пароль: http://192.168.0.1 або http://192.168.1.1. Проте, у даному випадку мова йде не про пароль, а про IP-адресу, і вона може бути різною у різних роутерів навіть за базовими налаштуваннями від виробника. Так само їх твердження "...далі вводиться ім'я користувача: admin і пароль: admin" може бути вірним лише за умови, якщо такі дані були надані виробником роутера і вони не змінювались користувачем. Втім найбільш не обґрунтованим нам здається твердження, що "слідчий (оперативний працівник) на підставі ухвали слідчого судді суду першої інстанції направляє запит до мережевих операторів стільникового радіозв'язку з метою перевірки MAC-адрес, встановлених під час огляду місця події, і встановлення даних користувача (IMEI, номера телефону та інші дані), які є в системі баз даних постачальника електронних комунікаційних послуг стільникового радіозв'язку". Але

оператори стільникового зв'язку не мають інформації про MAC-адреси абонентських терміналів. Ця інформація їм не потрібна, вона ніяк не впливає на надання послуг стільникового зв'язку і не передбачена специфікацією. Для стільникового зв'язку використовується інший радіоінтерфейс, який має інший ідентифікатор – IMEI, а не MAC-адресу. Щоб це з'ясувати, достатньо подивитись офіційну специфікацію протоколів стільникового зв'язку.

Метою статті є визначення можливостей Wi-Fi маршрутизаторів для встановлення мобільного терміналу та його мережевої активності під час розслідування кіберзлочинів, зокрема отримання відповідей на такі питання: яка доказова інформація може бути виявлена у Wi-Fi маршрутизаторі, як її зафіксувати і вилучити, а також обставини, які можуть перешкоджати пошуку зловмисника та доведенню його провини.

Виклад основного матеріалу. Нерідко для приховування слідів кіберзлочинів зловмисники використовують публічний доступ до мережі Wi-Fi. Це може бути, наприклад, кафе чи готель. Разом з тим, можливі й інші варіанти підключення, які не мають принципових технічних відмінностей – Wi-Fi мережа офісу, власної квартири чи квартири сусідів або знайомих.

Для розуміння особливостей функціонування Wi-Fi маршрутизатора, до якого під'єднався мобільний термінал підозрюваної особи, для встановлення вказаного пристрою та його подальшого розшуку, розглянемо основні теоретичні положення, викладені в Методичних рекомендаціях [1].

Використання зафіксованої Wi-Fi маршрутизатором інформації про підключені мобільні термінали можливе у випадку, якщо маршрутизатор підтримує логіювання мережевих з'єднань і якщо таке логіювання активоване. Логіювання або журналювання – це функція автоматичної фіксації службової та статистичної інформації про дії програмного забезпечення або користувачів у хронологічному порядку. Така інформація зберігається у лог-файлах (лог-файл або просто лог, англ. Log file) походить від грец. logos – слово, смисл, думка, мова), які можуть бути різних форматів – від звичайних текстових з простою структурою до бінарних файлів та баз даних. У лог-файлах може фіксуватись різна інформація, все залежить від програмного забезпечення, якого стосується логіювання, та налаштувань цього логіювання.

У розглянутому випадку інтерес для розслідування будуть становити два види інформації:

1. Інформація, що характеризує безпосередньо під'єднані до Wi-Fi-мережі мобільні термінали. Фактично, ці дані є цифровими (електронними) слідами, за якими можна (не завжди, про це далі) ідентифікувати мобільний термінал підозрюваної особи.

2. Інформація, яка характеризує мережеву активність під'єднаних до Wi-Fi-мережі мобільних терміналів. Ця інформація може містити цифрові сліди конкретних протиправних дій зловмисника.

Конкретний перелік даних, що накопичуються у логах, залежить від моделі маршрутизатора, версії його програмного забезпечення та налаштувань (у маршрутизаторів побутового рівня, як правило, відсутні налаштування логіювання подій, є лише можливість активації/деактивації логіювання).

У випадку виявлення в логах необхідних даних, їх потрібно належним чином документувати та процесуально оформити задля набуття ними статусу доказів.

Аби успішно оперувати описаною вище інформацією у процесі доказування, варто розуміти доказове значення кожних даних. Розглянемо їх детальніше.

Інформація, що характеризує безпосередньо під'єднані до Wi-Fi-мережі мобільні термінали, зазвичай може містити дані про мережеву назву такого терміналу, його MAC-адресу, IP-адресу, час підключення до мережі та тривалість сеансу.

Мережева назва мобільного терміналу зазвичай збігається з його моделлю – це встановлюється заводом-виробником. Але цю назву може змінити користувач у налаштуваннях мобільного терміналу. Нерідко нова назва також тим чи іншим чином може ідентифікувати користувача, наприклад, містити його ім'я. Але може бути і цілком нейтральною, наприклад, просто "smartphone".

MAC-адреса (від англ. Media Access Control – управління доступом до середовища) – це унікальний ідентифікатор мережевого інтерфейсу. У мережевій моделі OSI (від англ. The Open Systems Interconnection model) MAC-адреса використовується на другому (канальному) рівні. Іноді цю адресу ще називають апаратною чи фізичною (англ. Hardware Address). MAC-адреса надається мережевому інтерфейсу заводом-виробником, при цьому адресний простір розподілений між виробниками. Використовуючи довідкові дані, за MAC-адресою зазвичай можна визначити виробника мобільного терміналу, а в окремих випадках – конкретну модель. Можливість визначення конкретної моделі залежить від того, чи відкрив виробник загальний доступ до такої інформації, інакше доведеться направляти офіційний запит до виробника. Проте слід враховувати певні особливості MAC-адреси. По-перше, цю адресу можна змінити у налаштуваннях мобільного терміналу або використовуючи спеціальне програмне забезпечення. Наприклад, сучасні смартфони мають функцію генерації випадкової MAC-адреси при кожному підключенні до мережі (див. Рис. 1). По-друге, MAC-адреса не передається разом з мережевим трафіком глобально. В рамках Wi-Fi-мережі MAC-адреса передається від терміналу лише до маршрутизатора, не далі. А отже, відслідкувати у глобальній мережі мобільний термінал за його MAC-адресою зазвичай неможливо.

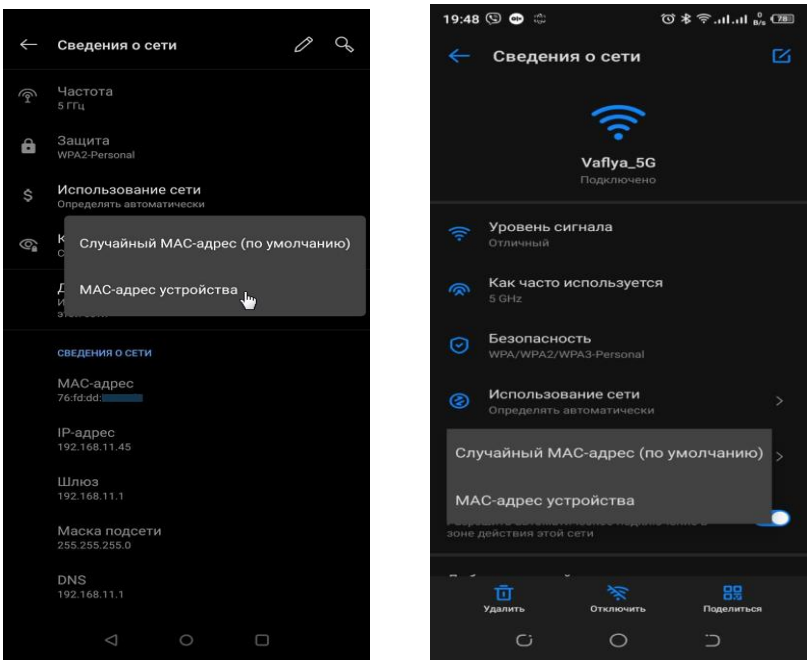

Рис. 1. Приклади налаштувань Wi-Fi-мережі у смартфоні, що функціонує під керуванням ОС Android.

IP-адреса (від англ. Internet Protocol address) – це також унікальний ідентифікатор мережевого інтерфейсу, який використовується для адресації комп'ютерів чи інших

пристроїв у мережах, які побудовані з використанням стеку протоколів TCP/IP, у тому числі – Інтернет. У мережі Інтернет потрібна глобальна унікальність адрес, а у разі роботи в локальній мережі – унікальність у межах цієї мережі (існують заздалегідь визначені адресні простори для локальних мереж). На відміну від MAC-адреси, IP-адреса використовується на третьому (мережевому) рівні моделі OSI. Ця адреса використовується для адресації пакетів інформації, а отже, може передаватись глобально. При цьому слід враховувати, що адреса вузла локальної мережі не передається назовні. Для взаємодії з глобальною мережею використовується технологія NAT (від англ. Network Address Translation – перетворення мережевих адрес), яка дозволяє змінювати IP-адресу у заголовку пакету інформації під час його проходу через пристрій маршрутизації трафіку (маршрутизатор). IP-адреса надається мережевому інтерфейсу вручну адміністратором чи користувачем, або автоматично з використанням протоколу DHCP (англ. Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла). У мережах Wi-Fi у переважній більшості випадків використовується саме динамічне розподілення IP-адрес, при цьому це адреси локальної мережі, які не передаються назовні.

Час підключення до мережі та тривалість сеансу дозволяють локалізувати в часі знаходження мобільного терміналу в межах покриття Wi-Fi-мережі. Також слід враховувати, що термінал міг знаходитись на цій же території і в інший час, але не будучи підключеним до Wi-Fi.

Інформація, яка характеризує мережеву активність під'єднаних до Wi-Fi-мережі мобільних терміналів, може містити дані про доменне ім'я та/або IP-адресу ресурсу, до якого звертався термінал, порт, тип протоколу, тип пакету, дату та час звернення тощо. Таким чином якщо, наприклад, зловмисник через публічну мережу Wi-Fi намагався підключитись до віддаленого сервера за протоколом SSH (від англ. Secure SHell – "безпечна оболонка" – мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів). Схожий за функціональністю з протоколом Telnet і rlogin, проте шифрує весь трафік, в тому числі і паролі, що передаються) і використовуючи його IP-адресу, у логах може відобразитись встановлення з'єднання з 22 TCP-портом мережевого вузла з відповідною IP-адресою.

Разом з тим, якщо зловмисник використовує сервіс VPN (від англ. Virtual Private Network – віртуальна приватна мережа), весь мережевий трафік у зашифрованому вигляді буде йти на адресу VPN-сервера. У логах, скоріше за все, відображатиметься лише IP-адреса та/або доменне ім'я цього сервера. А всю іншу інформацію доведеться запитувати у власника сервісу VPN.

Пошук, фіксація та вилучення інформації про MAC-адресу.

Якщо є підозра, що зловмисник у певному місці користувався Wi-Fi-мережею (зокрема, публічною) для вчинення протиправних дій, перш за все, слід з'ясувати, чи дійсно на місці події функціонує якась Wi-Fi-мережа. Для цього можна використати як спеціалізоване обладнання (наприклад, аналізатор частот), так і спеціальні утиліти (Wi-Fi аналізатори), які можна встановити на звичайний смартфон. Такі додатки дозволяють не лише виявити Wi-Fi-мережу, але й встановити ще багато даних: MAC-адреса мережевого інтерфейсу Wi-Fi-передавача, канал, потужність сигналу, наявність та вид шифрування каналу тощо (див. Рис. 2, 3). При застосуванні додатку потрібно враховувати апаратні можливості смартфона, адже якщо смартфон підтримує мережу Wi-Fi лише на частоті 2,4 ГГц, то мережа 5 ГГц у додатку не відобразиться.

Рис. 2. Вікно додатку Wifi Analyzer (розробник – farproc), доступного для завантаження з Google Play, працює під керуванням ОС Android.

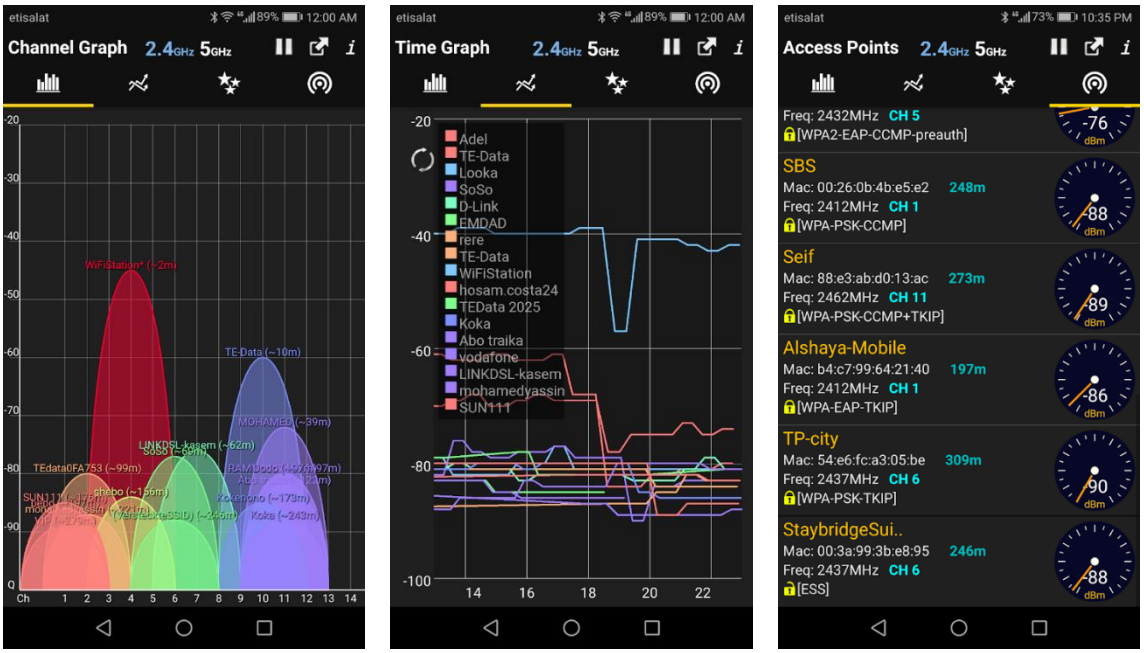

Рис. 3. Вікно додатку WiFi Analyzer (розробник – olgor.com), доступного для завантаження з Google Play, працює під керуванням ОС Android.

Якщо на місці події виявлено функціонуючу Wi-Fi-мережу, наступним етапом слід з’ясувати місце знаходження мережевого обладнання Wi-Fi та схему побудови мережі в цілому. Це може бути один пристрій – Wi-Fi маршрутизатор (характерно для домашніх помешкань), Wi-Fi маршрутизатор та декілька додаткових передавачів (точок доступу, ретрансляторів/повторювачів (або репітерів, від англ. repeater)) для розширення зони покриття (вони можуть поєднуватись у мережу як дротовим, так і бездротовим з’єднанням), декілька Wi-Fi маршрутизаторів або Wi-Fi маршрутизатор, який не має відповідного радіоінтерфейсу, а функціонує через окремі Wi-Fi-передавачі, що виступають як точки доступу (такий варіант більш характерний для професійного застосування, наприклад, забезпечення мережею Wi-Fi громадського місця – зали

ресторану, великого офісу тощо). В цілому варіантів побудови мережі безліч. Наприклад, останнім часом набувають поширення так звані Wi-Fi Mesh мережі. Найбільш складними є, зазвичай, корпоративні мережі. Крім того, логіювання може здійснюватися не лише на локальний носій інформації маршрутизатора, але й на сторонній носій (наприклад, окремий комп'ютер чи хмарне сховище).

Наступним кроком слід вжити заходів задля збереження логів Wi-Fi маршрутизатора. Якщо мережа корпоративна, слід звернутись до адміністратора цієї мережі, повідомивши йому про необхідність забезпечення збереження журналу подій для його подальшого вилучення у процесуальному порядку. У випадку огляду домашнього помешкання слід виявити місцезнаходження Wi-Fi маршрутизатора. Зазвичай у квартирах Wi-Fi маршрутизатор встановлюють біля входу до квартири, щоб не тягнути кабель всередину квартири, або приблизно посередині квартири, щоб забезпечити найкраще покриття. У всіх випадках бажано обмежити доступ будь-яких осіб до мережевого устаткування, аби уникнути будь-яких маніпуляцій (навмисних, ненавмисних чи випадкових) з ним: від'єднання (роз'єднання), вимкнення, перезавантаження, знеструмлення, переналаштування тощо. Для проведення будь-яких дій з маршрутизатором варто залучити спеціаліста (відповідно до ст. 71 КПК України "особу, яка володіє спеціальними знаннями та навичками…") [12], який допоможе професійно розібратися в особливостях комп'ютерного та телекомунікаційного обладнання, виявити носії інформації та запобігти умисному або випадковому знищенню інформації на них, проконсультує слідчого щодо інформації, яка підлягає копіюванню тощо. Профіль і кваліфікація спеціаліста, якого необхідно залучити до огляду, визначається, перш за все, об'єктом огляду (у розглянутому випадку це Wi-Fi маршрутизатор), а також залежно від мети і завдань слідчої (розшукової) дії, зважаючи на первинні дані про характер кримінального правопорушення.

На початковій стадії проведення слідчих (розшукових) дій, таких як огляд, обшук, а також виїмка, слідчому або оперативному працівнику на місці події, якщо виявлено Wi-Fi мережу, необхідно:

1. Прибувши на місце проведення слідчої (розшукової) дії заборонити всім особам, що перебувають у приміщенні, торкатися до комп'ютерної та/чи телекомунікаційної техніки, носіїв інформації, телекомунікаційних та електродротів, вмикати і вимикати пристрої й енергоживлення.

2. Провести фото-, відеозйомку приміщення, у якому здійснюється огляд або тимчасовий доступ до комп'ютерного та/чи телекомунікаційного обладнання.

3. У процесі огляду або тимчасового доступу до телекомунікаційного обладнання спеціаліст у присутності понятих має:

3.1. Встановити схему мережі, з'ясувати, які пристрої забезпечують функціонування мережі (мережеве обладнання) та які до неї під'єднані постійно та тимчасово (стаціонарні та мобільні термінали – стаціонарні комп'ютери, ноутбуки, смартфони тощо).

3.2. Зафіксувати дані, які зазвичай містяться у маркувальних позначеннях на корпусі пристроїв: марку, модель, серійний номер, MAC-адресу, стандартні дані автентифікації (ім'я користувача та пароль). Як правило, маркування містять й інші дані, але вони зазвичай не є суттєвими.

3.3. Підключитись до мережі. Для цього під'єднати до Wi-Fi-мережі службовий ноутбук (бажаний варіант) або використати вже під'єднаний до мережі "місцевий" комп'ютер. Використання "місцевого" комп'ютера має свої переваги і недоліки. Перевагою є те, що він вже підключений до мережі, а також можлива наявність у ньому

автентифікаційних даних (якщо з нього здійснювалось адміністрування маршрутизатора). Недоліком може бути внесення змін до інформаційного вмісту носіїв інформації комп'ютера, оскільки в окремих випадках це небажано. У випадку підключення службового ноутбуку чи іншого мобільного терміналу до Wi-Fi-мережі потрібно знати її назву (SSID, від англ. Service Set Identifier) та, якщо мережа захищена, пароль. При цьому слід враховувати, що SSID може бути скритим та/або підключення до мережі дозволене лише за білим списком MAC-адрес. Значна частина Wi-Fi маршрутизаторів підтримує підключення до Wi-Fi-мережі за допомогою WPS (від англ. Wi-Fi Protected Setup), що значно спрощує під'єднання до мережі і реалізується одним з таких способів: за допомогою PIN (зазвичай вказаний на етикетці маршрутизатора), з натисканням push-кнопки, з використанням NFC або з використанням флеш-накопичувача для перенесення налаштувань з маршрутизатора на ноутбук. Також не слід відкидати можливість підключення до мережі за допомогою дротового з'єднання, адже більшість Wi-Fi-маршрутизаторів мають також і дротові інтерфейси для локальної мережі. В останньому випадку SSID та пароль не знадобляться.

3.4. Здійснити вхід до інтерфейсу головного мережевого пристрою (Wi-Fi маршрутизатора). Слід враховувати, що вхід до адміністративного меню Wi-Fi маршрутизатора може бути заблокований з бездротової мережі (дозволено лише з дротової локальної мережі), може бути дозволений вхід лише за білим списком MAC-адрес тощо. Для входу до веб-інтерфейсу маршрутизатора за допомогою Інтернет-браузера необхідно в адресний рядок ввести адресу маршрутизатора. Для побутових маршрутизаторів це зазвичай "http://192.168.0.1" або "http://192.168.1.1", але не для всіх. Наприклад, для маршрутизаторів ASUS це може бути "http://192.168.50.1", а для маршрутизаторів MikroTik – це "http://192.168.88.1". Також слід враховувати, що ця адреса може бути змінена у налаштуваннях. У випадку професійного мережевого обладнання доцільно з'ясувати параметри входу у системного адміністратора. У низці випадків може бути неможливо увійти до меню маршрутизатора через веб-інтерфейс. У такому випадку, якщо маршрутизатор підтримує доступ через термінал, можна використати доступ за протоколами Telnet чи SSH (останній краще, бо використовує зашифрований канал зв'язку) (див. Рис. 4). Крім того, слід враховувати, що частина маршрутизаторів підтримують адміністрування за допомогою спеціального програмного забезпечення (фірмової утиліти).

3.5. Здійснити візуальний огляд відображеної інформації на екрані комп'ютера з подальшою її фіксацією;

3.6. Ввести автентифікаційні дані адміністратора. У багатьох Wi-Fi маршрутизаторів виробниками задаються стандартні параметри входу: ім'я admin і пароль admin. Разом з тим, стандартною є рекомендація змінити ці параметри відразу після першого входу. Нерідко система може навіть не пропустити користувача до меню, доки він не змінить стандартні автентифікаційні дані. Крім того, для автентифікації може знадобитись ключ HASP (від англ. Hardware Against Software Piracy). Отже, бажано дізнатися параметри входу у власника Wi-Fi маршрутизатора або системного адміністратора. Вказані параметри слід зафіксувати у протоколі.

3.7. У разі успішного входу до адміністративного меню варто спочатку переглянути налаштування логіювання, а потім – наявність логів за потрібний проміжок часу.

3.8. Виявлені дані слід вивести на екран та переглянути учасникам слідчої (розшукової) дії, зокрема, понятим.

3.9. Вказані дані слід зафіксувати у протоколі слідчої (розшукової) дії, до якого доцільно долучити роздруківки відповідних знімків екрану (скріншотів).

3.10. Після цього виявлені логи слід вилучити. В залежності від моделі Wi-Fi маршрутизатора та наявного криміналістичного обладнання це можна зробити шляхом копіювання лог-файлу, експорту логів у текстовий чи табличний файл, виділенням та копіюванням необхідної інформації у текстовий файл або скріншотами (останній варіант є найгіршим з точки зору подальшого використання вказаної інформації, зокрема, для проведення судової експертизи).

3.11. Отриманий файл або декілька файлів слід підписати з використанням кваліфікованого електронного підпису слідчого або обрахувати хеши цих файлів, які вписати до протоколу. У випадку, якщо файлів значна кількість, їх можна помістити до архіву та підписати (обрахувати хеш) лише цього одного архівного файлу. Файл записати на носій інформації (оптичний диск, флеш-носій, карта пам'яті тощо), який додати до протоколу слідчої (розшукової) дії.

Всі дії на екрані комп'ютера рекомендується фіксувати не лише у протоколі, але й шляхом створення знімків екрану (скріншотів), які потім можна роздрукувати та записати на цифровий носій інформації.

Враховуючи, що до Wi-Fi маршрутизатора у цей самий час могли бути підключені інші мобільні термінали (інших присутніх осіб), варто провести огляд цих терміналів та зафіксувати їх MAC-адреси. Виокремивши ці MAC-адреси зі списків адрес у логах можна встановити MAC-адресу мобільного терміналу підозрюваної особи (або декілька адрес, серед яких – адреса терміналу зловмисника).

```
C:\>
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
C:\>
C:\>
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
merionetSw1>en
% No password set.
merionetSw1>
% Connection timed out; remote host not responding
C:\>
C:\>
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
merionetSw1>en
Password:
merionetSw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
merionetSw1(config)#hostname merionSwitch1
merionSwitch1(config)#
```

Рис. 4. Вікно терміналу з відображенням входу до адміністративних налаштувань маршрутизатора Cisco за допомогою протоколу Telnet.

4. На завершальній стадії необхідно оформити протокол огляду або тимчасового доступу, у якому поетапно описати усі дії спеціаліста (рекомендується під його диктовку та у присутності понятих, супроводжуючи роздруківками скріншотів усіх дій на екрані комп'ютера, які разом з схемами та матеріалами фото-, відеозйомки додаються до протоколу).

Можливості встановлення мобільного терміналу за MAC-адресою.

Після оформлення протоколу на місці події провадять подальші слідчі (розшукові) дії зі встановлення місцезнаходження мобільних терміналів, MAC-адреси яких виявлено на місці події. Оператори стільникового зв'язку не мають інформації щодо MAC-адрес мобільних терміналів, а отже, і не зможуть таку інформацію надати на відповідний запит слідчого, навіть оформлений з дотриманням усіх процесуальних вимог. Оператори мобільного зв'язку отримують лише ідентифікатор стільникового радіоінтерфейсу мобільного терміналу (IMEI, від англ. International Mobile Equipment Identity – міжнародний ідентифікатор мобільного обладнання), а також ідентифікатор абонента (IMSI, від англ. International Mobile Subscriber Identity – міжнародний ідентифікатор користувача мобільного зв'язку), який міститься у SIM/USIM/R-UIM картці. Якщо телефон має декілька слотів для SIM/USIM/R-UIM карток, то і IMEI та IMSI буде декілька, по одній парі IMEI+IMSI на кожен слот. Віртуальна (цифрова) SIM/USIM/R-UIM картка також має власний IMSI.

IMEI та IMSI є унікальними номерами. IMEI надається мобільному терміналу його виробником, IMSI – виробником SIM/USIM/R-UIM картки, зазвичай, оператором стільникового зв'язку (заводом на його замовлення). Отже, виробник мобільного терміналу має інформацію і про IMEI (який відстежується операторами стільникового зв'язку), і про MAC-адресу терміналу. Цим можна скористатись під час пошуку мобільного терміналу. Перш за все, слід встановити через довідникові джерела у мережі Інтернет-виробника терміналу, що має виявлену MAC-адресу. Зазначимо, що якщо за IMEI у довідникових Інтернет-джерелах можна, зазвичай, встановити точну модель терміналу, то за MAC-адресою – лише виробника. Маючи інформацію щодо виробника мобільного терміналу у певних випадках попередньо можна припустити, що то був за пристрій – смартфон, планшетний комп'ютер, ноутбук, окремий мережевий інтерфейс (плата) тощо. Але таке можливо в обмеженій кількості випадків, бо, наприклад, Xiaomi Communications Co Ltd виготовляє значну кількість різних типів пристроїв: смартфони, планшетні комп'ютери, ноутбуки, мережеве обладнання тощо, і все це має мережеві інтерфейси з MAC-адресами. Отже, за точною інформацією доведеться звернутись до виробника. Якщо запитуваний мобільний термінал має стільниковий мережевий інтерфейс (тобто, окрім Wi-Fi також може підключитись до стільникової мережі, наприклад, ноутбук чи планшетний комп'ютер – через вбудований 3G/4G модем), від виробника можна отримати інформацію про IMEI вказаного терміналу.

Отримавши цю інформацію, стає можливим отримати від операторів телекомунікацій інформації про зв'язок (абонента, надання електронних комунікаційних послуг, їх тривалість, зміст, маршрути передавання трафіку тощо). Для цього на підставі ухвали слідчого судді суду першої інстанції направляється запит до операторів стільникового радіозв'язку з метою перевірки отриманого від виробника IMEI і встановлення даних користувача, які є в системі баз даних постачальника електронних комунікаційних послуг стільникового радіозв'язку.

Наступним кроком може бути проведення такої негласної слідчої (розшукової) дії, як установлення місцезнаходження радіоелектронного засобу, що може дати можливість установити місцезнаходження мобільного терміналу, який був підключений до мережі (маршрутизатора) у момент вчинення кримінального правопорушення.

Можливості дослідження цифрових слідів кібератак у лог-файлах.

Паралельно з встановленням терміналу, інформації про його володільця та місця знаходження терміналу може здійснюватися аналіз лог-файлів на предмет відображення в них ознак кібератаки.

При цьому послідовно здійснюються наступні операції:

- встановлення наявності у лог-файлах інформації про мережеву активність в цілому і конкретного терміналу зокрема;
- визначення наявності чи відсутності ознак використання сервісу VPN чи інших механізмів маскування трафіку;
- виявлення ознак кібератаки;
- встановлення механізму кібератаки, її класифікація.

Зазвичай дослідження лог-файлів на предмет виявлення ознак кібератаки, встановлення її механізму і віднесення до певного типу (класифікація) доцільно здійснювати шляхом експертизи електронних комунікацій або судової комплексної експертизи електронних комунікацій та комп'ютерно-технічної експертизи. При цьому для встановлення механізму кібератаки можуть знадобитись додаткові матеріали, наприклад, лог-файли атакованої електронної комунікаційної системи.

Висновки.

Використання зафіксованої Wi-Fi маршрутизатором інформації про підключені мобільні термінали можливе у випадку, якщо маршрутизатор підтримує логіювання мережевих з'єднань і якщо таке логіювання активоване. Інтерес для розслідування буде становити інформація щодо під'єднаних до Wi-Fi-мережі мобільних терміналів, що зазвичай може містити дані про мережеву назву пристрою, його MAC-адресу, IP-адресу, час підключення до мережі та тривалість сеансу, а також щодо мережевої активності, що може містити дані про доменне ім'я та/або IP-адресу ресурсу, до якого звертався термінал, порт, тип протоколу, тип пакету, дату та час звернення тощо.

Під час огляду здійснюється виявлення Wi-Fi-мережі, з'ясовується місце знаходження мережевого обладнання Wi-Fi та схема побудови мережі в цілому. Наступним кроком вживаються заходи задля збереження логів Wi-Fi маршрутизатора та їх вилучення у процесуальному порядку. Отримавши з логів MAC-адресу мобільного терміналу, слід встановити IMEI цього пристрою, що можливо зробити через довідкові дані або звернувшись до виробника терміналу. З цією інформацією (IMEI) можна звернутись до операторів стільникового зв'язку для отримання даних користувача, які є в системі баз даних постачальника електронних комунікаційних послуг стільникового радіозв'язку. Також можна, відповідно до положень ст. 268 КПК України [12], провести негласну слідчу (розшукову) дію – установлення місцезнаходження радіообладнання (радіоелектронного засобу).

Одночасно зі встановленням терміналу, інформації про його володільця та місця знаходження терміналу може здійснюватися аналіз лог-файлів на предмет відображення в них ознак кібератаки, що доцільно здійснювати шляхом проведення експертизи електронних комунікацій або судової комплексної експертизи електронних комунікацій та комп'ютерно-технічної експертизи. При цьому для встановлення механізму кібератаки можуть знадобитися додаткові матеріали, наприклад, лог-файли атакованої електронної комунікаційної системи.

Використана література

1. Нізовцев Ю. Ю. Використання можливостей Wi-Fi маршрутизаторів для встановлення мобільного терміналу та його мережевої активності: методичний посібник. Київ: Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України, 2022. 18 с.

2. Авдєєва Г.К. Сутність цифрових слідів в криміналістиці: зб. матеріалів міжнар. наук.-практ. конфер. *Актуальні питання судової експертизи та криміналістики,* м. Харків, 10 – 11

жовт. 2018 р. Харків, 2018. С. 90-93. URL: http://dspace.nlu.edu.ua/bitstream/123456789/15677/1/Avdeeva_90-93.pdf (дата звернення: 17.09.2023).

3. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів: навч. посіб. Київ: ВПЦ "Київський університет", 2018. 229 с.

4. Басай В.Д., Томин С.В. Дослідження віртуальних слідів – перспективний напрямок криміналістичного слідознавства. *Актуальні проблеми держави і права*. 2008. Вип. 44. С. 220-223. URL: http://nbuv.gov.ua/UJRN/apdp_2008_44_44

5. Крицька І.О. Доріжка цифрових слідів: доказове значення й окремі аспекти збирання та дослідження у кримінальному провадженні: зб. наук. пр. НДІ ПЗІР НАПрН України № 1 за матеріалами круглого столу *Цифрові трансформації України 2020: виклики та реалії,* м. Харків, 18 верес. 2020 р. С. 92-97. URL: http://openarchive.nure.ua/handle/document/13917 (дата звернення: 17.09.2023).

6. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право.* 2019. № 5. С. 304-307.

7. Омельян О.С. Поняття та ознаки цифрових слідів, що утворюються під час вчинення кіберзлочинів. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 457-466. DOI:10.33994/kndise.2020.65.45.

8. Самойленко О.А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.

9. Скрипник А.В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Харків: Право, 2022. 408 с. DOI:https://doi.org/10.31359/9789669982940.

10. Хижняк Є.С. Поняття віртуальних слідів та їх значення у процесі розслідування злочинів: зб. наукових праць *"Актуальні проблеми держави і права".* 2017. № 79. С. 159-166.

11. Кобець М.В., Кобець Р.М. Використання можливостей Wi-Fi роутерів під час виявлення та розслідування кримінальних правопорушень. *Криміналістичний вісник*. Київ: ДНДЕКЦ МВС України, НАВС, 2022. № 2(38). С. 36-47.

12. Кримінальний процесуальний кодекс України: Закон України від 13.04.12 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 17.09.2023).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~