ІДЕНТИФІКАЦІЯ ТА РОЗТАШУВАННЯ IP-АДРЕС

Ломоносов Ю. В.
доцент кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого, кандидат технічних наук, доцент, м. Харків

Досить часто в ході розслідування у провадженнях, пов'язаних з мережею Інтернет, присутня задача: для заданої IP-адреси встановити, який комп'ютер її використовує і визначити місце розташування цього комп'ютера.

Зазвичай, ланцюг доказів полягає в наступному: (злочин) – (IP адреса) – (комп'ютер) – (людина). За допомогою використання різних технічних засобів виконуються наступні кроки:

1) фіксується IP-адреса, за допомогою якої здійснювалась кримінальна діяльність.

2) встановлюється комп'ютер, який використовував цю IP-адресу, факт такого використання закріплюється експертизою.

3) потрібно довести, що цей комп'ютер у відповідний час використовував підозрюваний.

Розгляду другого завдання (знайти комп'ютер за його IP-адресою) вважаємо доцільним приділити особливу увагу.

1) *Унікальність IP-адреси*. IP-адреса є унікальним ідентифікатором комп'ютера або іншого пристрою в мережі Інтернет. Це означає, що в межах всієї глобальної комп'ютерної мережі в кожний момент часу тільки один-єдиний комп'ютер може використовувати певну IP-адресу.

Винятки не розглядаються:

– приватні, або так звані «сірі» IP-адреси;

– колективні (multicast) IP-адреси;

– мережеві і широкомовні (broadcast) IP-адреси;

– не виділені або не присвоєні реєстратором IP-адреси.

2) *Реєстратори*. Виділенням і реєстрацією IP-адрес в Інтернеті займаються організації, іменовані реєстраторами IP-адрес (IP Registry). Це організації, які є органами самоврядування Інтернету. Реєстратори утворюють трирівневу ієрархію: IANA - RIR - LIR.

Організація IANA є головним реєстратором, вона виділяє найбільші блоки IP-адрес регіональним реєстраторам і великим організаціям. Регіональних реєстраторів (RIR) в даний час п'ять. Це ARIN (Північна Америка), RIPE (Європа і Центральна Азія), APNIC (Азіатсько-Тихоокеанський регіон), LACNIC (Латинська Америка), AfriNIC (Африка). Вони виділяють великі і середні блоки адрес місцевим реєстраторам (LIR), а також ведуть базу даних виділених IP-адрес і надають доступ до неї.

Місцеві реєстратори (LIR) виділяють дрібні блоки IP-адрес операторам зв'язку і споживачам і реєструють їх в базі даних свого регіонального реєстратора. Як правило, роль місцевого реєстратора виконує оператор зв'язку (інтернет-провайдер). Таких реєстраторів – кілька тисяч.

Всі виділені IP-адреси реєструються в спеціальній базі даних, яку підтримує регіональний реєстратор (RIR). Відомості з цієї бази даних (за винятком деяких полів) доступні будь-якій особі за протоколом whois. Звернутися до цієї бази досить просто. При наявності доступу в Інтернет треба набрати в командному рядку «whois <ip-адреса>». Така команда є в будь-якій операційній системі, крім Windows. На сьогоднішній день, існують численні веб-ресурси, які дозволяють отримати відповідь з відповідної бази даних по запитуваній IP-адресі.

3) *Встановлення приналежності IP-адреси через веб-форму.* Різниця між отриманням довідки через whois-клієнт і веб-форму невелика. Джерело таке ж. Просто в другому випадку додається ще один технічний посередник в особі чужого веб-сайту.

4) *Коректність.* Відомості про місцеві реєстратори (LIR) – вірні, оскільки LIR є членом регіонального реєстратора (RIR), має з ним договір, сплачує членські внески, постійно взаємодіє. А відомості про клієнта LIR'а, безпосереднього користувача IP-адреси, підлягають перевірці. Таким чином, та частина адреси, якій відповідають одиниці в масці, є адресою (ідентифікатором) підмережі. Її ще часто називають префікс. А частина, якій відповідають нулі в масці, – ідентифікатором хоста всередині підмережі. Саме префіксами оперують маршрутизатори, прокладаючи маршрути передачі трафіку по мережі.

5) *Трасування IP-адреси.* Також певну допомогу у встановленні місця розташування і приналежності IP-адреси може надати програма «traceroute», яка є в складі будь-якої операційної системи, навіть Windows. Принцип дії цієї програми такий. З комп'ютера дослідника випускаються IP-пакети, адресовані на цільову IP-адресу. Поле TTL кожного випущеного пакета виставляється послідовно рівним 1, 2, 3 і так далі. Це поле призначене для виключення перевантаження каналів на випадок утворення петель маршрутизації, тобто замкнутих маршрутів. При проходженні кожного маршрутизатора поле TTL зменшується на одиницю. При досягненні значення 0 цей IP-пакет скидається, а на адресу відправника надсилається спеціальне повідомлення. Отже, пакет з TTL = 1 буде скинутий на першому маршрутизаторі по шляху проходження, пакет з TTL = 2 – на другому маршрутизаторі і т.д. За зворотною адресою прийнятих ICMP-пакетів комп'ютер дослідника встановлює, через які вузли пролягає маршрут до цільового комп'ютера.

6) *Встановлення приналежності доменного імені.* Для справедливого розподілу простору доменних імен і забезпечення їх глобальної унікальності діє система реєстрації доменних імен. Підлягають реєстрації всі доменні імена

першого рівня (наприклад, org, info, ua), всі доменні імена другого рівня (наприклад, gprf.info, fnn.ru) і деякі виділені доменні імена третього рівня.

У переважній більшості випадків для проведення таких досліджень не потрібно спеціального устаткування або спеціальних програмних засобів. Цілком достатньо звичайних ресурсів, наявних у розпорядженні будь-якого оператора зв'язку.

Національний юридичний університет імені Ярослава Мудрого

Науково-дослідний інститут вивчення проблем злочинності
імені академіка В. В. Сташиса
Національної академії правових наук України

З нагоди 100-річчя від дня народження професора М. В. Салтевського

Збірник матеріалів круглого столу

30 жовтня 2017 р.

м. Харків
2017

УДК
ББК

З нагоди 100-річчя від дня народження професора М. В. Салтевського: Зб. матер. круглого столу, м. Харків, 30 жовтня 2017 р. – Харків: Нац. юрид. ун-т ім. Ярослава Мудрого, НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України, 2017. – 128 с.

ISBN

До збірника матеріалів круглого столу увійшли тези доповідей і повідомлень, які були предметом обговорення учасників круглого столу «З нагоди 100-річчя від дня народження доктора юридичних наук, професора, Заслуженого діяча науки і техніки України М. В. Салтевського», який було проведено у м. Харкові 30 жовтня 2017 р. в НАПрН України.

Матеріали круглого столу можуть становити інтерес для наукових працівників, викладачів, представників правоохоронних органів, суду, експертів, студентів, а також всіх, хто цікавиться науково-практичним доробком видатного вченого-криміналіста М. В. Салтевського, проблемами криміналістики, судової експертології та інших наук кримінально-правового циклу.

ISBN