АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

Институт повышения профессионального уровня

Кафедра следственно-оперативной работы

МЕТОДИКА
поиска информации, в том числе электронных следов в информационно-коммуникационной сети при расследовании киберпреступлений.

Калиев Аскар Абужанович

п. Косшы-2019 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Мировая тенденция широкого распространения современных информационно-коммуникационных технологий, неизбежно привела к росту компьютерных преступлений, которые отличаются от традиционных высоким показателем латентности и низким уровнем раскрываемости.

В большинстве своем проблема выявления и раскрытия данных преступлений связана с высокой профессиональной подготовкой преступника и сложной, с технической точки зрения, способом их совершения.

Поэтому раскрытие компьютерных преступлений зависит от профессиональных знаний сотрудника, занимающегося расследованием таких дел и умелым применением их на практике.

Однако, как показывает практика, далеко не всегда следователи, приступая к производству осмотра места преступления по делам данной категории, представляют себе, как он должен проводиться, с чего начинать, на что необходимо обращать внимание.

Особенно, трудности появляются при обследовании компьютерной техники и поиска электронных доказательств в компьютерных сетях.

Согласно правилам криминалистики, успех в раскрытии любого преступления во многом зависит от того, насколько полно удалось выявить, закрепить, исследовать и эффективно использовать следы, отражающие различные обстоятельства происшедшего криминального события [1].

Если по традиционным видам преступлений картина исследуемых объектов ясна, то по компьютерным преступлениям, органу уголовного преследования требуется специальные познания.

Данная методика описывает приемы и способы обнаружения электронных следов компьютерного преступления, а также проведения поисковых мероприятий в информационно-коммуникационной сети.

МЕТОДЫ ПОИСКА ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ ЭЛЕКТРОННЫХ СЛЕДОВ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СЕТИ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Стремительное развитие информационно - коммуникационных технологий способствовали широкому распространению интернета, который открыл человечеству не только новые возможности для саморазвития, но и создал благоприятные условия для совершения преступлений в сети.

Правоохранительные органы разных стран выдвигают киберпреступность на первое место среди других видов преступлений, поскольку она влияет на экономику государства, причиняя значительный материальный ущерб.

Среди киберпреступлений наиболее распространенными являются атаки на компьютерные системы, хищение информации, включая личные данные, распространение вредоносных программ и фишинг.

Каждое такое преступление совершается при помощи информационно-коммуникационных технологий и сети Интернет.

В целях эффективного их расследования сотрудникам правоохранительных органов необходимо знать приемы и способы обнаружения электронных следов компьютерных преступлений, а также понимать процесс их совершения.

Преступления, совершаемые в сети Интернет, всегда оставляют электронные следы. Это изменения, которые киберпреступник вносит в информационную систему, информацию или базу данных.

Любое компьютерное преступление должно начинаться с обследования компьютерной техники, где главная задача следователя или криминалиста является установления данных, позволяющих начать поиск предполагаемых компьютерных преступников.

Такими данными будет являться IP-адрес.

IP-адрес – это уникальный идентификатор компьютера в сети интернет.

Он имеет длину 4 байта и записывается в виде четырех групп цифр от 0 до 255, разделенных точками. Каждая группа обозначает сеть, группу узлов и идентификационный узел.

Другими словами IP-адрес фактически является виртуальным паспортом человека. Он может многое сказать о пользователе интернета:

выдать информацию о его провайдере, примерном месте нахождения и сообщить другие сведения.

В глобальной сети IP-адрес может быть двух видов (рис. 1):

1) статический - при новом подключении он остается неизменным;

2) динамический - при новом подключении он будет другим.

Рис. № 1

Таким образом, если нам необходимо найти человека, совершившего преступление через сеть интернет, первым делом следует искать IP-адрес его устройства, с помощью которого оно было совершено.

Получив информацию об IP-адресе можно предпринимать шаги для получения более детальной информации о нем.

УСТАНОВЛЕНИЕ ПОДОЗРЕВАЕМОГО ЛИЦА С ПОМОЩЬЮ IP-АДРЕСА.

Как узнать IP-адрес человека? Существуют разные способы его определения. В данной методике будет рассмотрено два способа установления IP-адреса: через почтовые сервисы интернет служб и с помощью специализированного программного обеспечения IP LOGGER.

Для начала давайте разберемся, как установить IP-адрес компьютера, с которого Вы начнете поиски IP-адреса предполагаемого преступника.

Нужно открыть командную строку *(открывается путем одновременного нажатия на клавиши «Windows» и «R»)* и в появившемся окошке набрать команду CMD, затем нажать клавишу ввода ENTER.

В открывшемся интерфейсе командной строки *(выглядит в виде черного экрана)* вводится команда: IPconfig, которая запускается клавишей ENTER.

В результате на экране появляется IP-адрес исследуемого компьютера, который может выглядеть следующим образом: **192.168.1.70**, где:

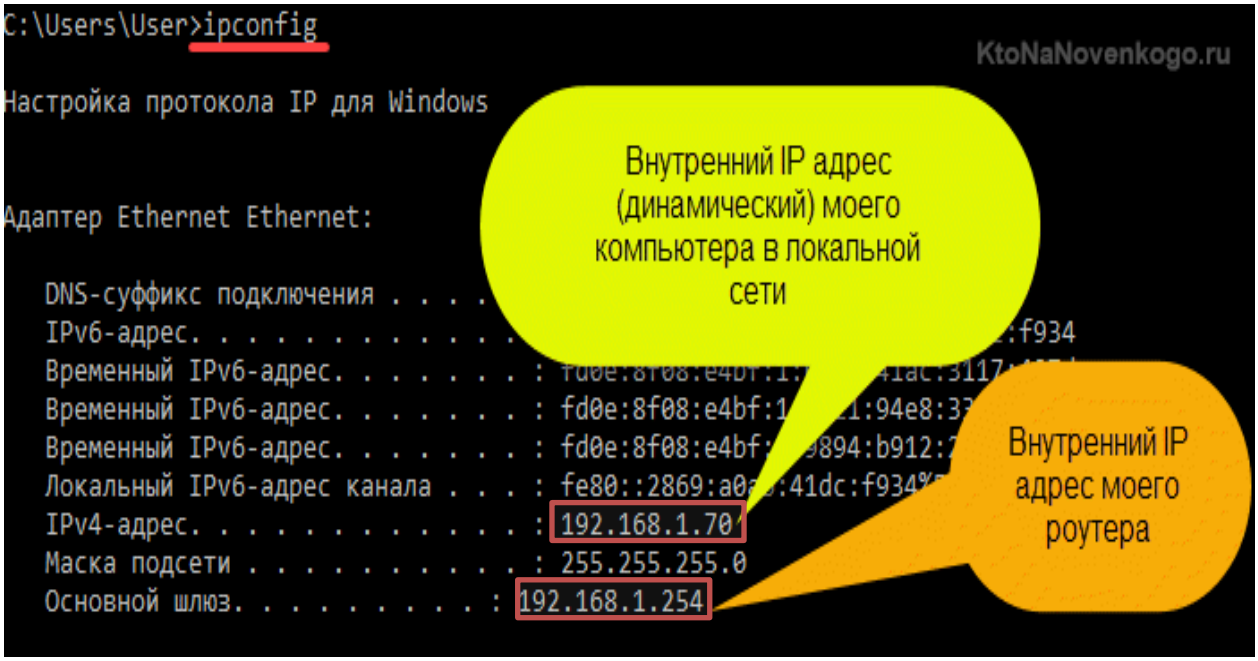
192.168 - адрес сети;

1 - адрес подсети;

70 - адрес компьютера.

Следует отметить, что одинаковых IP-адресов в сети Интернет не существует. Пример IP адреса компьютера и используемого роутера приведен на рисунке № 2.

Рис. № 2



Тем самым, узнать уникальный адрес компьютера в сети Интернет не сложно, специальных технических познаний в области IT технологий для этого не требуется.

Теперь давайте разберемся, как установить IP-адрес предполагаемого преступника, который оставил свои электронные следы в почтовом сообщении на компьютере потерпевшего.

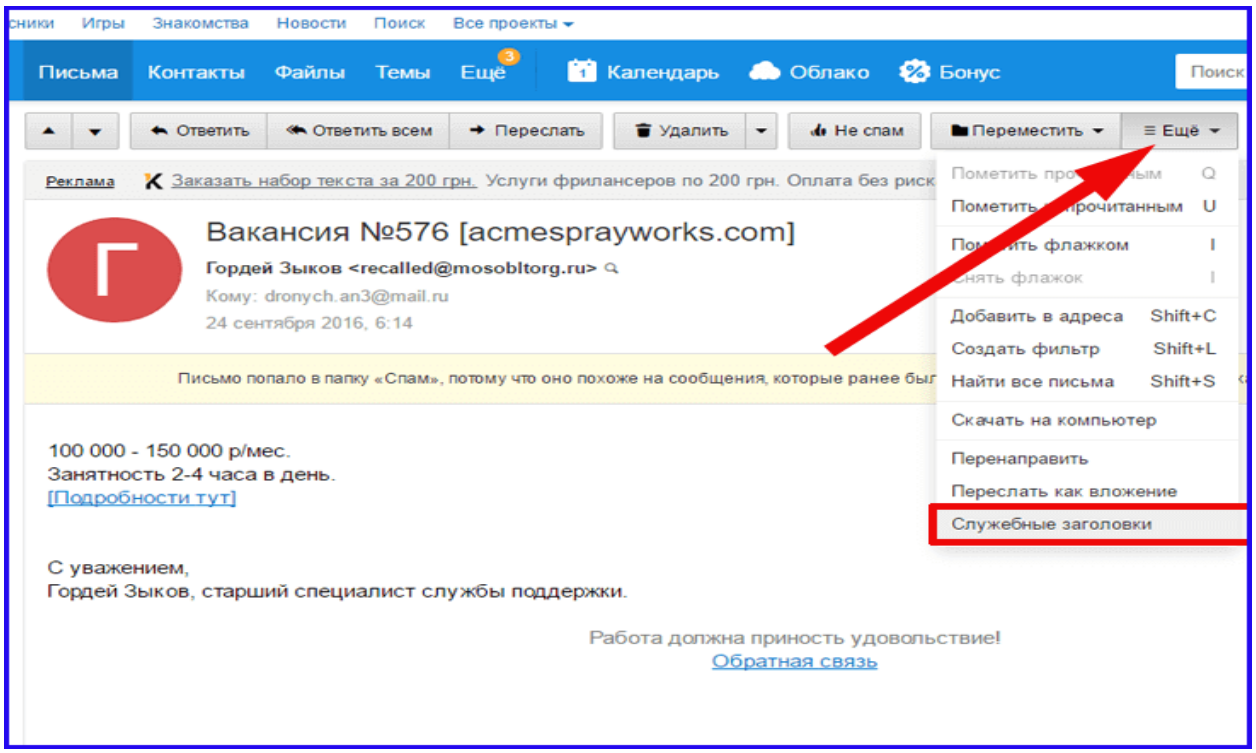
Способ № 1 – почтовые сервисы.

Для того чтобы нам установить **IP-адрес** в почтовом сообщении, например, на **MAIL.RU**, нам нужно зайти в почту (пароль и логин предоставляется потерпевшим), открыть там сообщение от подозреваемого нами лица и найти вкладку с названием «**ЕЩЁ**» (рис. № 3).

Нажав на данную вкладку, нам откроется небольшое меню, где мы должны выбрать раздел «Служебные заголовки». Он покажет нам

техническую информацию, которая является неотъемлемой частью любого письма (отправляемого или получаемого).

Рис. № 3



В представленной технической информации мы должны найти IP-адрес отправителя письма. Ниже приведен образец технических сведений, содержащих IP-адрес (рис. № 4).

Получив IP-адрес, Вы можете узнать, откуда идет соединение.

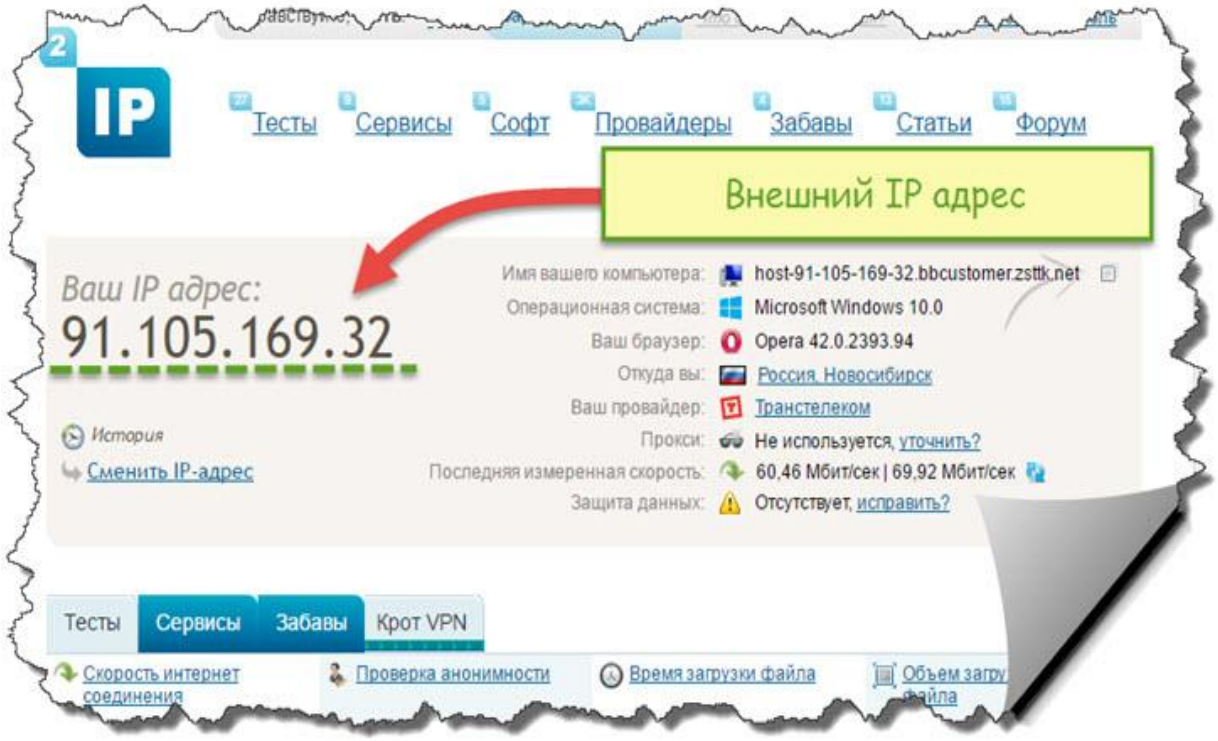
Необходимо сразу отметить, что эти простые инструменты не смогут точно сказать Вам, где находится киберпреступник, но зато они могут дать

нам представление о том, в каком городе он находятся и какого хостинг-провайдера он использует.

Далее копируем установленный нами IP-адрес и открываем специальный интернет - ресурс под названием «**2IP»** (рис. № 5) или аналогичные сервисы (например, whois). После чего проходим по вкладке «Информация по IP» и в открывшееся окошко вставляем скопированный ранее **IP-адрес,** затем наживаем проверить (найти).

Сайт сообщает нам важную информацию, которая содержит сведения о географическом месторасположении отправителя письма и названии провайдера, то есть организации предоставляющей услуги интернет.

Рис. № 5



Далее устанавливаем контакты данного провайдера и делаем ему запрос, с указанием IP-адреса, времени и даты направления письма.

Провайдер, обработав запрос, должен предоставить информацию о владельце компьютера, с которого пришло данное сообщение, указав адрес проживания и анкетные данные владельца квартиры или офиса, устройству которого выдавался данный IP-адрес (стационарный компьютер, ноутбук, планшет и т.д.).

Эти данные могут помочь Вам начать следственно-оперативные мероприятия в отношении подозреваемого лица.

Аналогичные поиски можно проводить и по другим почтовым сервисам и службам интернета, используя вышеуказанный алгоритм действий.

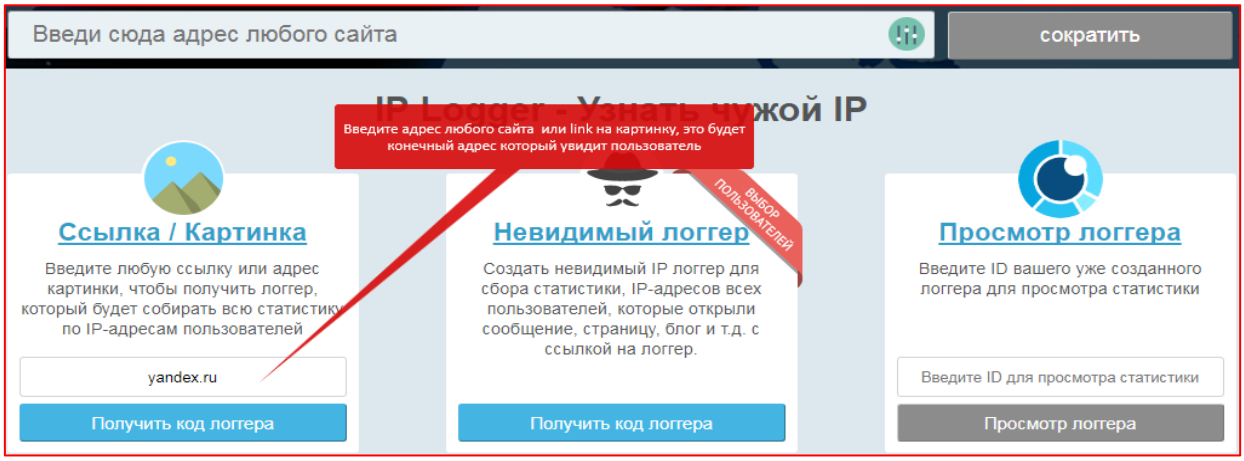
Способ № 2 –специальная программа «IP LOGGER»

Данная программа позволяет скрытно направить человеку ссылку, при переходе по которой будет считан его IP-адрес.

Ссылки могут быть абсолютно разными: изображения, видео или ссылки на любой сайт или личную страницу в социальной сети.

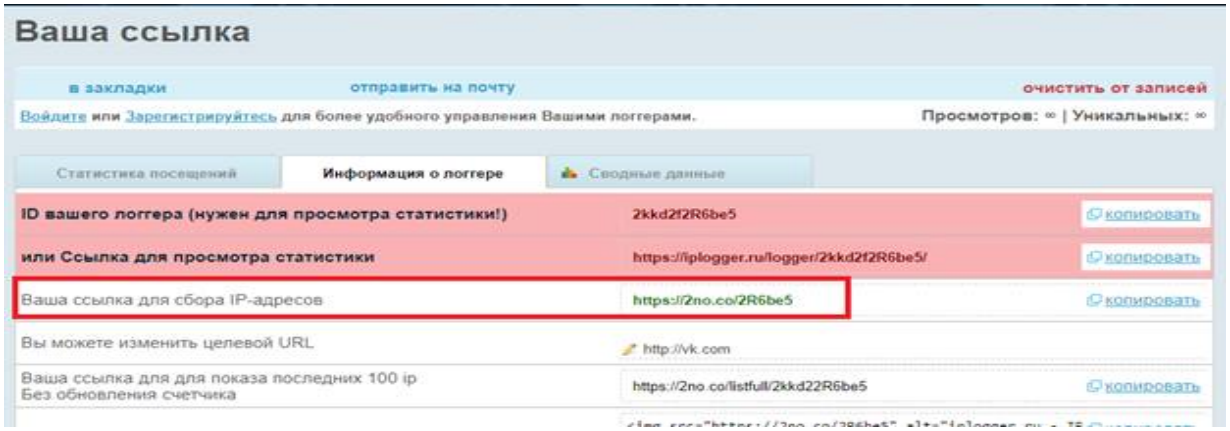
На рис. № 6 изображена главная страница данной программы.

Рис. № 6



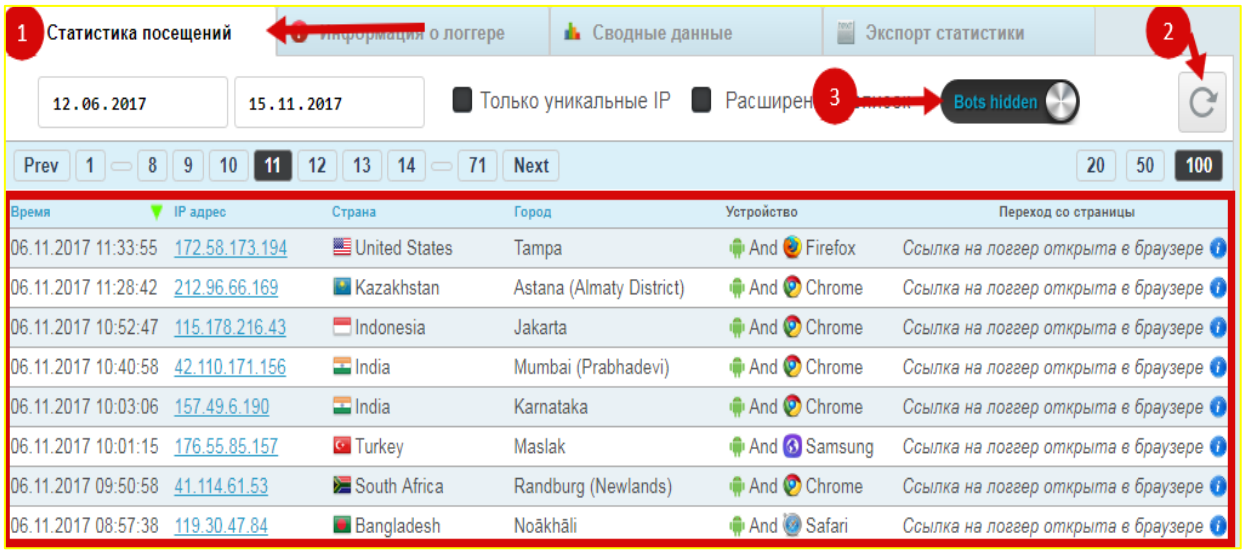
Главное, чтобы пользователь, которому будет направлена данная ссылка, не заподозрил вас в сборе информации о нем. Когда определитесь со ссылкой, нажмите на кнопку «Получить код логгера» и Вас переадресует в личный кабинет сбора информации о переходах по ссылке, где необходимо взять ссылку, которая будет указана в графе «Короткая ссылка от Google» (рис. № 7). Эту ссылку необходимо сбросить тому лицу, от которого мы хотим «скрытно» получить IP-адрес.

Рис. № 7



Когда пользователь сети, в отношении которого мы хотим собрать информацию, пройдет по нашей ссылке, сведения об его IP-адресе отобразится в разделе «Статистика посещений», где Вы сможете узнать ключевую информацию о человеке: IP-адрес, примерное местонахождение, устройство и браузер, которые были использованы для перехода по ссылке (рис. № 8).

Рис. № 8



Узнав IP-адрес интересующего нас человека, мы можем провести в отношении него следственно-оперативные мероприятия, направленные на установление его причастности к совершенному компьютерному преступлению.

УСТАНОВЛЕНИЕ ПОДОЗРЕВАЕМОГО ЛИЦА С ПОМОЩЬЮ MAC-АДРЕСА.

Вычислить местонахождение преступников, осуществляющих свою деятельность в сети Интернет можно и другими способами, о которых обязательно должен знать следователь или оперативный сотрудник.

Для установления человека в сети интернет будем использовать **MAC-адрес роутера,** находящегося в квартире или офисе организации.

Бывают случаи, когда в распоряжении следственно-оперативных подразделений попадает информация о MAC-адресе роутера, использованный в киберпреступлении или, например, которым пользуется в настоящее время интернет – преступник.

Алгоритм установления местонахождения преступника будет выглядеть следующим образом: следователь, используя данные **BSSID** – уникальный MAC-адрес беспроводной сети *(выглядит примерно так:* ***6A-28-5D-7B-78-D8)*****,**

вводит их в специальную строку сервиса геолокации WIFI сетей, который располагается по интернет - адресу:

HTTP://MOBILE.MAPS.YANDEX.NET/CELLID_LOCATION.....

В адресной строке ищем «wifinetworks=» и вписываем туда наш MAC-адрес без двоеточий и тире → 6A285D7B78D8.

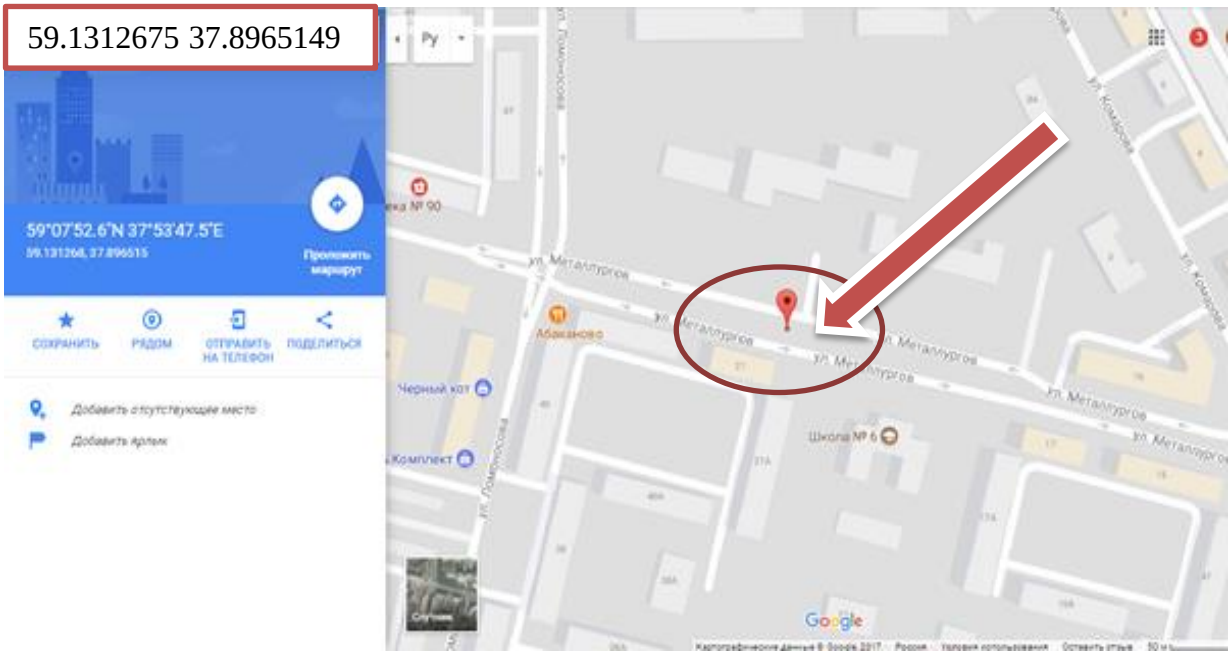
В итоге должно получиться вот так:

HTTP://MOBILE.MAPS.YANDEX.NET/CELLID_LOCATION/?CLID=1866854&LAC=-1&CELLID=-1&OPERATORID=NULL&COUNTRYCODE=NULL&SIGNALSTRENGTH=-1&WIFINETWORKS=**6A285D7B78D8:**-65&APP=YMETRO

Далее нажимаем на клавишу ENTER и получаем координаты mac-адреса: <coordinates latitude="**59.1312675**" longitude="**37.8965149**".

После этого мы заходим в **GOOGLE MAPS** или в любую другую интернет карту *(сервис геолокации)*, расположенную в интернете и устанавливаем географическое местонахождение интересующего нас человека (рис. № 9).

рис. № 9



Кроме **http://mobile.maps.yandex.net/cellid_location** могут применяться другие аналогичные службы геолокации: **https://alexell.ru/network/mac-geo**.

Все они направлены на установление местонахождения анализируемого субъекта и дальнейшего сбора информации по нему.

ЗАКЛЮЧЕНИЕ

Учитывая, что преступники стараются находить новые методы совершения компьютерных преступлений, правоохранительным органам необходимо совершенствовать свои навыки, разрабатывать более эффективные способы и приемы выявления преступлений данной категории.

В связи с чем, в данную методику периодически будут вноситься изменения и дополнения.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ.

1. Криминалистика. Учебник / Отв. ред. Н.П. Яблоков. — 3-е изд., перераб. и доп.— М.: Юристъ, 2005. — 781 с.

2. Криминалистика: тактика и методика. Учебник / И.В. Александров – М.: Юрайт, 2017 – 313 с.

3. http://www.neumeka.ru/poisk_lyudej.html. Поиск людей в интернете.

4. http://vhod.cc/raznoe/naiti-cheloveka/. Найти человека.

5. http://useroff.com/kak-najti-cheloveka-v-internete.html. Поиск человека в интернете.