Секция «Криминалистика»

Некоторые возможности обнаружения следов преступлений в облачных системах хранени

Закирова Ирина Вадимовна

Студент (бакалавр)

Уральская академия государственной службы при Президенте РФ, Екатеринбург, Россия

E-mail: irivadimovna@gmail.com

Активное внедрение компьютерных технологий в повседневную жизнь, их развитие и совершенствование неизбежно ведут не только к изменениям отдельных аспектов общественной жизни, но и к возникновению новых видов преступлений, совершенствованию способов их совершения. На протяжении нескольких лет сотрудниками отдела «К» МВД России отмечается динамика совершения преступлений с использованием информационных технологий. [3]

Особую сложность представляет обнаружение следов в набирающих все большую популярность системах онлайн-хранилища, как например в облачном хранилище данных. Облачная система хранения данных позволяет преступникам не хранить какие-либо файлы на своём электронном устройстве, а хранить их на веб-сервере, что затрудняет обнаружение следов как доказательств вовлечения в преступление. Но, при осведомленности о работе в облачной пространстве, обеспечения доступа к ней, представляется возможность их обнаружения, исследование и использование в качестве доказательств содеянного.

Независимо от места хранения какого-либо файла: на электронном устройстве, облачное платформе, - сама система электронных данных устроена таким образом, что образование, изменение, работа в файле, приложении, базе данных автоматически будет предполагать отражение изменения образа информации. Это может быть как дата создания, изменения документа, так и изменение какого-либо кода. Так, например, сведения об изменениях могут содержать так называемые «логи».

Лог - это журнал автоматической регистрации событий, которые фиксируются в рамках какой-либо программы. Каждому событию соответствует одна запись в логе. Почти каждое действие, производимое человеком, при взаимодействии с информационной системой, отражается в логе, иногда даже в нескольких логах одновременно. [1, С. 139] Исходя из вышесказанного лог будет являться своего рода следом, свидетельствующим об изменении. В зависимости от настроек сервера, можно будет увидеть IP-адрес, время доступа, идентификатор (логин) пользователя и другие поля. [1, С. 141]

К примеру, если лица работали на платформе Dropbox, после регистрации клиента на управляющих серверах clientX.dropbox.com, команда list получает изменения в метаданных, которые показывают разницу между локальной копией и тем, что находится на сервере. Как только происходит локальное изменение файлов, Dropbox вызывает команду commit_batch (client-lb.dropbox.com) и посылает измененные метаданные на сервер. После этого сервер отвечает, какие блоки ему необходимы, используя команду need_blocks, и клиент, на пример, отсылает эти блоки на Amazon (dl-clientX.dropbox.com). Сохранение каждого блока подтверждается командой OK. После этого локальный клиент еще раз посылает команду commit_batch на сервер и получает подтверждение, что все блоки получены. Все эти изменения будут автоматически отражены в файлах, представленных в формате, похожие на log_tcp_complete. [2] При анализе данных файлов возможно будет увидеть какие-либо отличия, иную информацию, сведения как след доступа и корректировки. В последующем это может быть использовано в качестве доказательства возможности совершения преступления конкретным лицом.

Помимо этого, выбрав платформу облачного хранения данных, пользователь должен пройти процедуру регистрации, подписания соглашения об использовании облачной платформы. Особый интерес будет представлять политика конфиденциальности. Так в рамках обеспечения политики организация, управляющая облачным веб-сервисом, приложением и т.д. в праве хранить и собирать персональную информацию, указанную при регистрации; файлы и сведения об ассоциации файлов, хранящихся на сервисе облачного хранилища; данные журналов событий; cookie (куки), тип браузера, дату и время, а также веб-страницу, которую посещали до перехода на Веб-сайт - облако. [См. например 4; 5]

Таким образом, при возможности получения всех этих данных представляется возможность установить круг лиц, причастных к совершению преступления, вычислить их IP-адрес, а затем и его принадлежность конкретному лицу, путем направления запросов в компании интернет-провайдеры. По сведениям об ассоциации файлов можно установить изменения, поскольку если файл, загруженный на сервис одним пользователем, частично совпадает с файлом, загруженный другим пользователем, то сохраняется не дубликат файла, а только изменения. В журнале событий как правило можно будет обнаружить сведения об устройствах, с которых производился доступ к услугам облачного хранения, сведения о программном обеспечении, установленном на этих устройствах и действия пользователя во время использования сервиса. [4]

Анализ сведений отдельных файлов, хранящихся на облачной платформе, как и при хранении в папке на компьютере, может содержать интересующие сведения и следы. Как и файлы Microsoft Office, облачная система OneDrive может отображать имя пользователя, который внес изменения и дату изменения файла. Например, система хранения GoogleDrive предусматривает возможность увидеть историю изменения документа, то есть его предыдущие версии, автора, дату и время. Даже при удалении какого-либо файла, папки из облачной среды, во многих программах предусмотрена возможность их восстановления в течение определенного времени, поскольку используется система резервного копирования. [См. например 6; 7]

Таким образом, при оперативности действий, в короткие сроки эксперты, органы предварительного расследования, имеют возможность обнаружить то, что лицо желало скрыть от следствия.

Источники и литература

1) Федотов Н.Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с.
2) Drago, I. and Mellia, M. and Munafò, M. M. and Sperotto, A. and Sadre, R. and Pras, A. (2012) Inside Dropbox: Understanding Personal Cloud Storage Services. Proceedings of the 12th ACM Internet Measurement Conference - IMC'12, Boston, Nov. 2012.
3) МВД отмечает рост киберпреступности в России: http://ria.ru/incidents/20160203/1369209245.html#ixzz40dxCjRoC
4) Политика конфиденциальности Dropbox: https://www.dropbox.com/privacy
5) Политика конфиденциальности Seagate Technology LLC: http://www.seagate.com/ru/ru/legal-privacy/privacy-policy/
6) Справочный центр – Редакторы Google Документов: https://support.google.com/docs#topic=1382883
7) Справочный центр Dropbox: https://www.dropbox.com/ru/help/296