ИНФОРМАЦИОННОЕ ПРАВО

УДК 343.1

Фам За Хюи
Волгоградская академия МВД Российской Федерации
Факультет подготовки иностранных специалистов
Россия, Волгоград
huyphamhhnbk@gmail.com
Фам Ньы Хан
Академия народной безопасности
Кафедры профессионального фундаментального
Вьетнам, Ханой
nik.fam.89@mail.ru
Pham Gia Huy
Volgograd Academy of the Ministry of Internal Affairs of Russia
Faculty of training foreign specialists
Russia, Volgograd
Pham Nhu Han
People's security academy
Department of professional fundaments
Vietnam, Hanoi

СБОР ЭЛЕКТРОННЫХ СЛЕДОВ С МОБИЛЬНЫХ УСТРОЙСТВ В ХОДЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ВО ВЬЕТНАМЕ

Аннотация: в последние годы в мире, а также во Вьетнаме, наряду с непрерывным развитием технологий, все большее развитие получают мобильные телефоны, которые становятся основным средством общения и работы людей. Вместе с появлением многофункциональных смартфонов увеличилось и количество дел, связанных с мобильными телефонами. Во многих случаях мобильные телефоны используются в качестве криминального оружия.

Преступники могут использовать телефоны для сохранения личной информации, обмена письмами, чата, доступа к социальным сетям, сайтам ставок на футбол, игре в онлайн-лотерею. В данной статье рассматривается проблема сбор следов с мобильных устройств для расследования преступлений.
Ключевые слова: след, сбор, преступник, уголовное дело, моби́льный телефо́н, криминальный.

COLLECTING ELECTRONIC TRACES FROM MOBILE DEVICES DURING CRIME INVESTIGATION IN VIETNAM

Annotation: In recent years in the world, and also in Vietnam, along with the continuous development of technology, mobile phones have become increasingly developed and are becoming the main means of communication and work for people. Along with the emergence of multifunctional smartphones, the number of cases involving mobile phones has also increased. In many cases, mobile phones are used as a criminal weapon. Criminals may use phones to store personal information, exchange emails, chat, access social media, football betting sites, play online lotteries... This article discusses the problem of collecting traces from mobile devices for the investigation of crimes.
Key words: trace, collection, criminal, criminal case, mobile phone, criminal.

Во Вьетнаме, в некоторых случаях, при сборе и использовании информации с мобильных устройств, можно найти много важных доказательств, которые невозможно получить традиционными методами расследования. Поэтому понимание того, как хранятся данные и их используются операционные системы в современных телефонах, поможет в сборе данных и управлении ими, тем самым повышая эффективность борьбы с преступностью.

В настоящее время электронные данные в телефонах очень разнообразны, поэтому существует множество критериев классификации для улучшения сбора

и анализа данных для расследования. Одна из популярных классификаций заключается в том, что на основе операционной системы телефона можно классифицировать типы телефонов, использующих операционную систему, такие как IOS, ANDROID, WINDOWPHONE, BLACKBERRY, FUNTOUCH... Или может быть основаны на расположении хранения данных, которые можно разделить на внутренней памяти, на SIM-карте, в картах памяти, либо основаны на форме существования телефонных данных, которые делятся на данные в виде символов, изображений, звуков... Кроме того, существует множество других классификаций, основанных на конкретных критериях, таких как: на основе типа извлекаемых и восстанавливаемых данных (сообщения, изображения, местоположения, история звонков...); на основе статуса электронных данных (скрытые, удаленные, существующие) или также могут быть основаны на цели использования данных (данные передаваемы, данные получаемые).

Статья 99 Уголовно-процессуального кодекса Вьетнама 2015 г. (в дальнейшем - УПК Вьетнама 2015 г.) гласит: Электронные данные - как источник доказательств, определяемые как «символы, буквы, числа, изображения, звуки или аналогичные форматы, созданные, сохраненные; переданных или полученных с помощью электронными средств» [1]. Это положение демонстрирует последовательность и конкретизирует понятие «данные» в Законе об электронных сделках 2006 года: «Данные — это информация в виде символов, букв, цифр, изображений, звуков и т. д. в штриховом или аналогичном формате» [2]. Однако только после выхода УПК Вьетнама 2015 г. электронные данные были узаконены в качестве одного из источников доказательств.

Так что можно сказать, что информационные на телефонах как один из источников доказательств и должны собираться в соответствии с ст. 107 и ст.196 УПК Вьетнама 2015 г., во время расследования уголовного дела.

Статья 107 УПК Вьетнама 2015 г. — «Сбор электронных средств и электронных данных». В пункте 1 этой статьи еще раз гласит: «Электронные носители должны быть изъяты своевременно и в полном объеме, с точным описанием фактического положения и опломбированы сразу же после изъятия. Опломбирование и снятие пломб осуществляются в соответствии с законодательством.

Статья 196 УПК Вьетнама 2015 г., регулирует изъятие электронных носителей и электронных данных следующим образом: «Изъятие электронных средств и электронных данных производится лицом, компетентным в ведении процессуальных действий, и может быть предметом судебного разбирательства…».

Следственные органы должны собирать данные, полученные с мобильных телефонов, записаны в протоколе, и сразу опечатаны [3, с. 20].

По сути, электронные данные — это символы, буквы, изображения, звуки и тому подобное, которые создаются, сохраняются, передаются или получаются с помощью электронных средств, включая данные, которые были удалены, перезаписаны, скрыты, зашифрованы и сделаны читаемыми, видимыми, перезаписываемыми для использования в качестве доказательств [4, с.124].

Поэтому для повышения эффективности обнаружения и сбора электронных данных с мобильных телефонов, необходимо понять механизм формирования и характеристики электронных данных на мобильных телефонах.

Механизм формирования электронных данных на телефоне формируется из взаимодействия между физическими объектами, которые является результатом операций на телефоне программного обеспечения обработки ввода пользователя.

Основные стадии совершения преступления с использованием мобильных телефонов:

- Приготовление к преступлению: это период получения информации извне в мобильный телефон с помощью клавиатуры, камеры, микрофона и т.д. Большинство электронных следов правонарушений формируется в этот период.

- Обеспечения обработки данных: на этом периоде программное обеспечение может создавать свои собственные данные для хранения данных во время обработки и в тоже время может записывать промежуточные результаты или записывать обработку. Этот шаг формирует электронные следы, о которых пользователь может не знать. Окончанием этого периода является сохранение обработанных данных в электронной памяти телефона или их передача [5, с.43].

- Покушение на преступление: это период, на котором электронные данные передаются с одного телефона на другой телефон или другое электронное устройство через телекоммуникационную сеть или Интернет. На этом периоде злоумышленники могут использовать различные методы и уловки для незаконного доступа к телефону, искажения данных, искажения управляющих программ и передачи вирусов в систему.

- Оконченное преступление: данные, хранящиеся в памяти, могут быть преобразованы в читаемую, понятную форму. На этом периоде саботажа мало, но как только данные будут украдены, злоумышленники могут получить ценную информацию при отображении или печати.

Из изучения механизма формирования видно, что электронные данные на телефоне имеют такую характеристику, что не существуют в обычном физическом виде, а существуют в виде электронной информации и хранятся в памяти телефона. Кроме того, электронные данные имеют динамический характеристики. Динамический характер электронных данных выражаются в способности копировать, перемещаться из одного места в другое, с одного телефона на другой телефон или устройство, из одного формата в другой...

В уголовных и оперативных расследованях розыск электронных данных с телефона обычно начинается с личной проверки изъятого телефона преступника,

чтобы найти файлы, которые содержащие значимую информацию, доказывающую истинность дела. Особое внимание следует уделить документам, таблицам, изображениям, информации, электронным письмам, чатам, отражающим размещение и загрузку объектов. Это могут быть ценными доказательствами в борьбе с преступниками [6, с.31].

Сбор данных — это использование всей информации на телефоне, включая сохранную информацию и удаленную информацию. Телефонная сим-карта также является устройством, которое хранит много информации. На сим-карте часто сохраняются MMS-сообщения, контакты... Поэтому в процессе интеллектуального анализа данных на сим-карте также является важным шагом. Интеллектуальный анализ данных на сим-карте может проводиться непосредственно через телефон или подключиться к компьютеру с помощью устройства чтения сим-карты [7]. У каждого типа телефона будет свой метод интеллектуального анализа данных, в зависимости от типа полученного телефона, который технические специалисты решат, какой метод использовать.

На практике, для эффективной работы все методы должны следовать следующей последовательности:

Шаг 1: Арестуйте телефон в соответствии с законом, чтобы избежать потери информации на телефоне и обеспечить правильную юридическую процедуру.

Шаг 2: когда телефон находится в режиме энергосбережения, кажется, что выключен, но на самом деле телефон включен. Нажмёте любую кнопку на телефоне, чтобы проверить ее статус.

Шаг 3: Проверьте, есть ли в телефоне сим-карта. Если телефон использует сим-карту, перейдите к процедуре интеллектуального анализа данных сим-карты. Если телефон использует технологию CDMA, интеллектуальный анализ данных проводится только на телефоне.

Шаг 4: включите питание и перейдите к следующим шагам, чтобы использовать информацию на телефоне.

Шаг 5: Проверьте характеристики телефона, изучите спецификации, чтобы придумать разумный метод сбора данных. Этот шаг требует от технического специалиста обладал знаниями и пониманием типов телефонов и их характеристик.

Шаг 6: Составьте план анализа.

Шаг 7: Проверьте, поддерживает ли телефон подключение к компьютеру? Какие инструменты интеллектуального анализа данных можно использовать?

Шаг 8: Используйте инструменты для сбора, анализа и восстановления данных на телефоне. В зависимости от данных, которые будут использоваться, выберите правильный инструмент для сбора, чтобы достичь максимальной эффективности.

Шаг 9: Используйте методы интеллектуального анализа данных для выполнения процесса интеллектуального анализа данных на мобильных телефонах.

Шаг 10: после использования всей информации на устройстве выключите питание и извлеките сим-карту из устройства, чтобы переключиться на процесс оценку сим-карты.

При создании электронной копии трассировки для анализа необходимо использовать зашифрованные хэш-значения (MD5, SHA). Целью хеш-значения является проверка подлинности и целостности данных в качестве точной копии исходных данных [8]. Значение хэша очень важно, особенно когда оно используется в качестве доказательства в суде, потому что изменение даже самого маленького бита данных создает совершенно новое значение хэша.

Таким образом, мобильные телефоны содержат много ценной информации для следственной деятельности. Однако это данные, которые легко потерять, много данных просто отключают питание, данные больше не существуют.

Поэтому процесс проведения оперативно-розыскных, таких как: осмотр места, обыск, сбор электронных данных... требует тщательной подготовки кадров и технических средств; Процесс резервного копирования должен полностью резервировать содержимое, такое как: Объекты для резервного копирования, объекты хранения, методы резервного копирования и присваивать значения хэша для резервного копирования. Любой недостаток в процессе сбора и хранения, может вызвать юридические проблемы.

В целях повышения эффективности расследования и разрешения дел необходимо полностью и более подробно дополнить порядок извлечения и оценки источников доказательств, указанные в статьях 87, 88, 99, 107 УПК Вьетнама 2015 г.

Список литературы

1. Bộ luật Tố tụng hình sự nước Cộng hòa xã hội chủ nghĩa Việt Nam, số: 101/2015/QH13 ngày 27.11.2015 /Уголовно-процессуальный кодекс Социалистической Республики Вьетнам №101/2015/QH13 27 ноября 2015 г. URL: https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Bo-luat-to-tung-hinh-su-2015-296884.aspx (Дата обращения: 18.07.2023)

2. Luật Giao dịch điện tử nước Cộng hoà xã hội chủ nghĩa Việt Nam Số: 51/2005/QH11 ngày 29 tháng 11 năm 2005/ Законе об электронных сделках Социалистической Республики Вьетнам №51/2005/QH11, 29 ноября 2005 года. URL: https://thuvienphapluat.vn/van-ban/Thuong-mai/Luat-Giao-dich-dien-tu-2005-51-2005-QH11-6922.aspx (Дата обращения: 17.07.2023)

3. Nguyễn Quang Lộc, Các biện pháp điều tra tố tụng đặc biệt quy định trong BLTTHS 2015, Tạp chí Tòa án nhân dân, số 21/2017, tr. 20. / Нгуен Куанг Лок, Специальные следственные и процессуальные меры, предусмотренные Уголовно-процессуальным кодексом 2015 года, Журнал народного суда, № 21/2017, с.20.

4. Nguyễn Văn Huyên, Lê Lan Chi, Bình luận khoa học BLTTHS 2015, Nxb Lao động 2016, tr.124. / Нгуен Ван Хуен, Ле Лан Чи, Научный комментарий к Уголовно-процессуальному кодексу 2015 г., Издательство труда, 2016 г., с.124.

5. Phạm Minh Tuyên, Thu thập, kiểm tra, đánh giá và nguyên tắc sử dụng chứng cứ trong tố tụng hình sự, Tạp chí kiểm sát số 21/2017, tr.43./ Фам Минь Туен, Сбор, исследование, оценка и принципы использования доказательств в уголовном процессе, Журнал прокуратуры № 21/2017, с. 43.

6. Bùi Việt Hùng, Chứng minh và chứng cứ trong Bộ luật tố tụng hình sự 2015, Tạp chí kiểm sát số 5/2018, tr.31/ Буй Вьет Хунг, Доказательства в Уголовно-процессуальном кодексе 2015 года, Журнал прокуратуры № 5/2018, с.31.

7. Một số vấn đề về sử dụng chứng cứ trong luật tố tụng hình sự Việt Nam [Электронный ресурс] URL: http://luatsuquangthai.vn/mot-so-van-de-ve-su-dung-chung-cu-trong-luat-to-tung-hinh-su-viet-nam-129-a3id (Дата обращения: 10.07.2023)

8. Hash Là Gì Và Hash Dùng Để Làm Gì? [Электронный ресурс] URL: https://codelearn.io/sharing/hash-la-gi-va-hash-dung-de-lam-gi (Дата обращения: 18.07.2023)