DISTINCTIVE FEATURES OF DIGITAL EVIDENCE

Rasulev A. , Sobirov Sh.

Rasulev Abdulaziz
DSc., professor Abdulaziz RASULEV, Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Tashkent, Uzbekistan

Sobirov Shokhrukhbek
independent applicant, Tashkent State University of Law, Tashkent, Uzbekistan
e-mail: shokhrukhbek.sobirov@gmail.com

Information technology crimes do not differ in general terms from other types of crimes. However, when investigating computer crimes, you have to rely on evidence presented in digital form. This article focuses on the main distinguishing features of digital evidence.

Keywords: digital evidence, computer crimes, information technology

Никому не секрет, что всякое взаимодействие пользователя с информационно-коммуникационными технологиями порождает (генерирует) цифровые следы. При расследовании уголовных дел связанные с использование ИТК цифровые следы (цифровые доказательства) имеющие отношения к делу могут содержать гигабайты цифровой информации. Большой объем обрабатываемой информации, а также разнообразные программные и аппаратные оборудования искусственно задерживают процесс расследования уголовного дела.

Цифровая информация по-своему происхождения, считается не устойчивой и легко модифицируемой, что создает трудности в случаях, когда необходима аутентификация или проверка источников цифровой информации[1]. Правила и порядок сбора цифровых доказательств по сравнению с традиционными доказательства отличаются. Однако общие правила доказывания применимы при определении относимости, допустимости и достоверности к конкретному уголовному делу[2].

Во многих правовых системах предусматривается обязательное предъявление стороной, выдвигающей доказательства, сведений о качестве методов, примененных для поддержания целостности цифровой информации с момента ее создания до представления в суде. Целостность и подлинность цифровой информации имеют прямое отношение к весомости доказательств с точки зрения их надежности и достоверности. Сторона, стремящаяся выдвинуть доказательства, как правило, должна подтвердить устойчивость доказательств или их «порядок передачи и хранения» для удостоверения того, что доказательства не были подделаны или изменены любым другим способом. Устойчивость доказательств обычно является вопросом

[1] United States v Whitaker, 127 F3d 595, 602 (7th Cir. 1997).
[2] Jackson, J.D., and Summers, S.J., 2012. The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions. Cambridge: Cambridge University Press.

фактического характера, а порядок передачи и хранения представляет собой механизм ведения и документирования хронологии имеющихся доказательств по мере того, как они перемещаются из одного места в другое[3].

В случае с цифровой информацией устойчивость доказательств должна быть обеспечена как для физического носителя, содержащего информацию (при получении или выемке), так и для самой информации, хранящейся в устройстве[4]. В этой связи, выдвигающая доказательства сторона должна подтвердить, что:

цифровая информация, полученная с устройства, является достоверной и точно отражает исходные данные, содержащиеся на устройстве (достоверность);

устройство и информация, представляемые в качестве доказательств, идентичны с теми, которые были изначально обнаружены и впоследствии приняты на хранение (целостность).

Цель заключается в свидетельствовании факта, что устройство является тем, в качестве чего оно заявлено предъявившей его стороной, и что цифровая информация заслуживает доверия и не была подделана или изменена[5].

Надежность машинно-генерируемой и хранимой на компьютере информации также оспаривается в связи с ее уязвимостью с точки зрения безопасности операционных систем и программ, что может служить источником угроз для целостности цифровой информации.

Допустимость использования в суде машинно-генерируемой информации (например, записей в файле журнала), содержащей подробное описание выполненных на компьютере, в сети или на ином устройстве действий, может подвергаться сомнению, если генерирующая информацию система не оснащена усиленным контролем безопасности[6].

С учетом вышеизложенного, мы пришли к выводу, что цифровые доказательства имеют ряд уникальных характеристик и свойств:

1) Их не видно невооруженным глазом: Электронные доказательства зачастую спрятаны там, куда догадается заглянуть только специалист, либо там, куда можно добраться лишь с помощью специальных инструментов.

2) Они очень неустойчивые: На некоторых устройствах или в определенных обстоятельствах во время обычной эксплуатации устройства информация в его памяти (а значит и доказательства, которые оно содержит) может изменяться. Например, при разрядке устройства или нехватке памяти система накладывает (записывает) новую информацию поверх старой. Компьютерная память может быть повреждена или уничтожена под

[3] Casey, E., 2011. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. New York: Elsevier.

[4] U.S. Department of Justice, 2007. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. National Institute of Justice, p.16.

[5] Marcella Jr., A.J., Greenfield, R.S., (eds.), 2002. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes,
2nd edn. Boca Raton: CRC Press, p.136.

6 Chaikin, D., 2006. Network investigations of cyber attacks: the limits of digital evidence. Crime, Law and Social Change, 46(4-5):239- 256, 249.

воздействием физических факторов (большой влажности или высокой температуры) и электромагнитных полей.

3) Они могут быть изменены или уничтожены в процессе обычной эксплуатации устройства: Память компьютерных устройств постоянно изменяется по запросу пользователей («сохранить документ», «скопировать файл») либо операционной системы («выделить место для программы», «временно сохранить данные для обмена между устройствами»). Последнее происходит автоматически.

4) Их можно копировать без потери качества: Цифровые данные можно копировать неограниченное количество раз и любая последующая копия ничем не будет отличаться от оригинала. Благодаря этой уникальной особенности доказательства становятся разными. Поэтому следует неукоснительно соблюдать общие принципы работы с доказательствами.

5) Профессиональное обращение: Каждое электронное устройство обладает своими уникальными характеристиками, поэтому при работе с ними нужно соблюдать соответствующие процедуры. Одним из наибольших рисков, связанных с электронными доказательствами, является их непреднамеренная модификация. Нарушение установленных процедур может привести к тому, что целостность данных будет оспорена в суде, а это, в свою очередь, может уменьшить и даже уничтожить их доказательную силу.

6) Необходимые реквизиты для идентификации: Файл обладает рядом характерных свойств, пригодных для его идентификации с точки зрения криминалистики:

местонахождение или размещение (тип носителя, директория);

наименование (символьное название, позволяющее отличить файл от других);

расширение (содержит не больше трех символов, как правило, определяет тип информации, содержащейся в файле);

тип информации (графическая, текстовая, аудио-визуальная, программный код и др.);

атрибуты (системный, архивный, скрытый, только для чтения);

время создания, время изменения и т.д.

7) Стремительная эволюция источников электронных доказательств: Новые технологии появляются и развиваются с невероятной скоростью, поэтому методы и процедуры по работе с электронными доказательствами нужно постоянно пересматривать и обновлять.

8) Использование надлежащих процедур, методов и инструментов: Как и любые эксперты, специалисты в области компьютерной экспертизы используют в своей работе специальные методы и инструменты. Очень важно, чтобы в каждом конкретном случае эти методы и инструменты были выбраны правильно. Кроме того, чтобы полученная информация имела доказательную силу, процедуры должны быть составлены таким образом, чтобы другие специалисты могли воспроизвести и проверить описанные в них действия.

Приемлемость: Конечная цель использования электронных доказательств заключается в том, чтобы подтвердить или опровергнуть спорные факты.

Поэтому чтобы суд принял электронные доказательства к рассмотрению, порядок их получения должен соответствовать действующему законодательству и существующим практикам.