Часопис Національного університету "Острозька академія". Серія "Право". – 2015. – №1(11)

УДК 343.1

Мате И. Ж.
судебно-информатический эксперт
(Докторская школа Юридического
факультета Университета Печа)

АНАЛИЗ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

Анализ доказательств - индивидуальная или командная работа?

Анализ и предварительная оценка доказательств являются первичным заданием и одновременно обязанностью прокурора и сотрудников органов, ведущих следствие в стадии расследования уголовного дела. Но при действиях, касающихся информатических систем, появились новые типы доказательств, которые в первую очередь касаются технических и инженерных наук, и робота с которими означает появление новых вызовов для дознавателей. В этой статье я ищу ответ на то, остаётся ли один в этом процессе специалист, ведущий следствие (дознаватель, прокурор, и т. д.), может ли он получить помощь, в какой форме и от кого?

Цифровое доказательство

В венгерском законодательстве отсутствует определение термина «цифровое доказательство». Но Закон XIX от 1998 года «Об уголовном процессе» абзац 115. § (1)), (2) З гласит:

«115. § (1) Вещественным доказательством является любой предмет (вещь), который пригоден для доказывания доказываемого факта, особенно тот, что носит следы преступника или возникает во время

▪ Анализ цифровых доказательств / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2015. – № 1(11) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles /2015/n1/15mizatd.pdf.

совершения преступления, который был использован как средство для совершения преступления, или по отношении к которому было совершено преступление.

(2) В применении этого закона вещественными доказательствами являются документы, рисунки и любые предметы, которые записывают данные, используя технические, химические или другие методы...»

Эта деталь в тексте «...записывают данные, используя технические, химические или другие методы» может быть применена и для цифровых доказательств, но для точного понимания этого понятия необходимо еще процитировать определение организации «Scientific Working Group on Digital Evidence», которая фокусирует своё внимание на том, что «цифровым доказательством есть информационные данные, имеющие доказательную силу, которые были сохранены или перенаправлены в бинарной форме».

Определения, данные той же самой организацией «SWGDE", мы будем использовать для обозначения других понятий, которые тесно связаны с использованием и анализом цифровых доказательств: «оригинальный экземпляр цифрового доказательства», «физические предметы и те данные, которые были связаны с этими предметами при конфискации», «дубликат цифрового доказательства», «точная цифровая репродукция всех данных, которые заключены в оригинальном физическом предмете», «копия цифрового доказательства», «точная, не связанная с оригинальным физическим предметом, репродукция сохранённой информации в объектах данных». [1]

Вышеупомянутые определения исходят из круга понятий, которые тесно связаны и с компьютерной наукой, и с юриспруденцией; они относятся к области «Digital Forensic Science» («Судебной информатики»). В этом контексте, судебно-информатический эксперт – это такой участник

▪ Анализ цифровых доказательств / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2015. – № 1(11) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles /2015/n1/15mizatd.pdf.

уголовного процесса, который подает информационные данные (факты), основанные на указанных понятиях, другим участникам процесса в соответствии с основным положением, известным из римского права «Da mihi factum, dabo tibi ius» (Дай мне факт и я дам тебе право.) [2].

Обнаружение и идентификация цифровых доказательств

На следственном этапе уголовного процесса органы следствия приступают к обнаружению и идентификации цифровых доказательств с помощью консультатора, потом эксперта. Этот момент решительно определяет их возможное употребление в дальнейшем, поэтому мы с полным правом можем считать этот момент также подготовительным этапом анализа цифровых доказательств. При проведении розыска участники могут использовать те обществоведческие наблюдения, которые мы можем и назвать народным обычаем виртуального пространства: размещение средств для ежедневного использования (в расстоянии вытянутой руки от компьютера), обычаи названия содержания (нелегальные копии софтвера в каталоге («взломанных программ»), удаление содержаний с носителя данных, предназначенных для скрывания.

После идентификации цифровых доказательств производится их конфискация (самое частое решение – их дупликация или их копирование, проводящиеся на месте действия, или обеспечение их охраны на месте (это не очень часто применяемый метод).

Но при любом из этих методов, которые используют органы следствия, должностное лицо должно поступать согласно юридическим законам – как напр. в Законе XLVII от 2005 года «О деятельности судебно-информатического эксперта», или в цитированном раньше законе «Об уголовном процессе». Это необходимо, потому что в данном моменте идентификации доказательств делается отправная точка цепочки надзора (Chain of Custody), при соблюдении которой цепь документов содержит

каждую операцию, связанную с доказательствами и причастных к этому делу лиц, место и время событий. В некоторых случаях уже на первом шагу нарушается закрытая цепь обработки доказательств: копирование съёмок камерой безопасности со стороны представителя нарушенного учреждения, удаление единицы хранения камерной системы следователями, и т. д. Все эти обстоятельства существенно влияют на более поздний экспертный анализ, который подробно обсуждается нами в дальнейшем.

Экспертная подготовка и экспертный анализ цифровых доказательств

В случае получения для обработки цифровых доказательств судебно-информатический эксперт рассматривает конфискованные средства, на которые был наложен арест органами следствия (типично, это компьютеры), в своей лаборатории.

Выбор способа фиксирования цифровых доказательств – не только экспертное, но также следственно-тактическое задание. Назначающее лицо может выбрать из широкого круга возможностей: дупликация содержания может быть судебной копией или полной копией, касающейся содержания, или копией, касающейся содержания после фильтрования по типам файлов, копией результата поиска по ключевым словам с упоминанием только самых частых. Практика показывает, что этот способ получения доказательств совершается часто по традициям, установленных органами, ведущими следствия и не привязан к конкретным обстоятельствам дела.

Пример: при производстве следственного действия, направленного на распространение данного процесса нет необходимости в моментальной полной дупликации носителей данных, а соответствующим методом является непосредственный анализ на месте результатов поиска по ключевым словам на релевантных типах файлов (в основном документы,

▪ Анализ цифровых доказательств / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2015. – № 1(11) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles /2015/n1/15mizatd.pdf.

электронные таблицы, базы данных), и конфискация носителей данных, содержащих важные данные с целью дальнейшего их изучения, расследования.

Если необходимо получить и удалённые данные, тогда может быть обоснованной их дупликация (обычным выражением клонирование) на месте или в лаборатории, через которую дальнейшее восстановление таких данных станет возможным.

Так как эти два выше представленных решения имеют различную потребность в средствах и времени, необходимо, чтобы сотрудники органов следствия поняли содержание отдельных операций и требование ресурсов. Например перед расследованием на месте (обыск в квартире) руководитель операции должен принять решение по следующим вопросам:

– имеются ли в распоряжении физические и личные условия, необходимые для расследования на месте или же они могут быть заменены,

~ имеется ли в распоряжении ёмкость для хранения, необходимая для сохранения данных;

~ имеются ли в распоряжении средства, поддерживающие достоверное сохранение (судебно-мост, дубликатор, и т.д.)

~ имеются ли в распоряжении аппаратные и программные компоненты обнаружения компьютерных сетей

~ есть ли достаточная численность экспертов (либо на месте либо в лаборатории);

~ касается ли расследование других физических или юридических лиц, кроме тех, которые вовлечены в процесс,

~ какими будут последствия остановки или последствия замедления, возникающие из-за расследования на месте / из-за конфискации

▪ Анализ цифровых доказательств / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2015. – № 1(11) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles /2015/n1/15mizatd.pdf.

~ возможна ли временная недоступность данных третьего лица или организации (напр. в случае расследования в бухгалтерских бюро). [3]

Таким образом, надлежащая подготовка определяет число полученных цифровых доказательств и степень возможности их постобработки и этим непосредственно также влияет на расходы уголовного дела. Этот последний фактор может хорошо осознаться при помощи сопоставления дупликации на месте с целенаправленным в лаборатории анализом. Настоящая ёмкость для хранения для одного компьютера приближается к терабайтной (ТБ) величине или превышает её (это соответствует ёмкости для хранения прибл. 220 ДВД дисков). Скорость передачи данных судебно-дублирующих оборудований 15 ГБ в минуту, из которых 70 минут/ ТБ идеальной скорости дублирования может быть вычислены. В случае нескольких устройств и продуктивных систем это решение влечёт за собой значительную затрату времени и невозможно без остановки системы.

При целенаправленном лабораторном анализе определённая часть рабочего времени эксперта может быть заменена машинным временем: фильтрование по файловым типам, копирование профильтрованных данных, поиск по ключевым словам в содержании файлов могут проводиться без личного присутствия эксперта.

Некоторые типы цифровых доказательств в отличие от предыдущих требуют дальнейшей экспертной работы или предварительной обработки. Из этих следует отметить базы данных электронной переписки (файлы PST, MS Outlook-a, Outlook Express, DBX ,Thunderbird, веб-системы электронной почты: Gmail, Freemail, и т. д.), которые не могут быть рассмотрены непосредственно, а только после экспертной подготовки. В этом случае эксперт не только получает, а может быть, восстанавливает содержание некоторых электронных писем из удалённого состояния, а

▪ Анализ цифровых доказательств / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2015. – № 1(11) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles /2015/n1/15mizatd.pdf.

также связанные с ними приложения, преимущественно в хронологическом порядке. Если имеются в распоряжении выражения для поиска (напр. имена, названия физических или юридических лиц), тогда эта операция также может принадлежать к кругу подготовки.

Эксперт проводит подобную деятельность и в случае исследования бухгалтерских баз данных, когда данные должны быть предоставлены в распоряжение органов следствия в оригинальном печатном формате данной программы, ввиду того, что их сотрудники, проводящие исследования судебно-бухгалтерского типа или другие исследования по экономической теме могут работать с такими данными.

Здесь мы подошли к моменту, который привел нас к приготовлению настоящего исследования: а именно, возможен ли анализ цифровых доказательств сотрудниками органов следствия самостоятельно без участия (поддержки) судебно-информатического эксперта. Ответ можно прочитать в заключительной главе исследования.

Сотрудничество органов следствия с экспертами

Анализ цифровых доказательств сотрудниками органов следствия зависит от ряда фундаментальных факторов: с одной стороны от компетенции сотрудника в области информатики, производящего расследование, от информационного оборудования, имеющегося в распоряжении (аспекты качества, содержания и применимости) и главным образом от количества рассматриваемых цифровых доказательств (то есть ёмкости хранения).

При проведении следствия в распоряжении органов следствия очень часто не хватает времени на анализ цифровых доказательств, во многих случаях достигающих 1-10 Тбайт ёмкости (при больших делах). Это обстоятельство усугубляется данными о требованиях технического оборудования: компьютеры исполнителей, находящиеся в контакте с

▪ Анализ цифровых доказательств / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2015. – № 1(11) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles /2015/n1/15mizatd.pdf.

цифровыми доказательствами, технически часто не пригодны на выполнения этой задачи, не имеют достаточных дополнительных средств (защита от записи для анализа жёсткого диска, и т. д.), ограничительные меры безопасности по использованию компьютеров (локальные сетевые правила внутреннего распорядка) тоже очень часто исключают работу с цифровым содержанием.

Последнее по счёту, но не по важности, что ИТ-навыков и знаний у лиц, производящих дознание, производящих исследование доказательств, часто не хватает даже для того, чтобы различать содержание цифровых доказательств, их проанализировать, а для возможного проведения более сложных операций – тем более (напр.: для добычи данных).

Следствием представленных фактов является то, что содержание, полученное и переработанное судебно-экспертной работой не используется в уголовном процессе из-за задерживающих обстоятельств. Это в раньше уже упомянутом экономическом аспекте (уголовные издержки) означает, что вложенные деньги (напр.: плата эксперта) не оправдаются в форме успешности процедуры.

Принимая во внимание тот факт, что цифровые доказательства всё чаще появляются в уголовном процессе, поиск ответов на поставленные вопросы не терпит замедления.

Есть несколько возможных решений, из этих мы фокусируем наше внимание на представлении двух конечных пунктов: сотрудники органов следствия должны быть подвержены всестороннему повышению квалификации и техники работы с цифровыми доказательствами, которая быть в их распоряжении на самом высоком актуальном уровне (что очень дорого и вероятно ведёт к конфликту). Или, судебно-информатических экспертов следует привлечь к работе через организационное изменение, и если нужно, через модификацию порядка процесса (это дешевле, но

▪ Анализ цифровых доказательств / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2015. – № 1(11) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles /2015/n1/15mizatd.pdf.

требуется более интенсивная организация и постоянное обновление системы средств судебных экспертов).

Таким образом, судебно-информатические эксперты являются уполномоченными помощниками органов, производящих расследования, которые кроме того, что подают результаты экспертизы, также могут помогать в исследовательской работе органов следствия своими советами или при профессиональном образовании работников следственных органов передачей своих профессиональных знаний, связанных с некоторыми видами дел. Для осуществления всего этого конечно также необходимы согласие и поддержка руководителей органов следствия, на получение которых можно надеяться.

Библиография

[1] Pollitt, Mark M. (ed.): Report on Digital Evidence. Lyon, 13th INTERPOL Forensic Science Symposium, 2001. p. D4-97.

[2] Феньвеши Чаба: Основные вопросы криминалистики. В.: Гаал Гюла, Хауцингер Золтан (ред.): Пограничные научные публикации в городе Печ 14. Печ : Венгерское Общество Военной Науки, Венгерское Отделение Пограничного Управления, 2013 – С.341-349.

[3] Мате Иштван Жолт: Обыск в квартире – судебно-информатический эксперт в уголовном процессе. В.: Конференция «Tavaszi szél» 2014 Труды научной конференции (в печати) Дебрецен, Университет Дебрецена 2014.

▪ Анализ цифровых доказательств / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2015. – № 1(11) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles /2015/n1/15mizatd.pdf.

Мате І. Ж.

Аналіз цифрових доказів

Після отримання цифрових доказів експерт передає докази співробітникам органів слідства, які аналізують, оцінюють і використовують їх у своїй роботі. Для аналізу цифрових доказів потрібно відповідні інформатичні знання, яких часто бракує у співробітників органів слідства. Судово-інформатичний експерт – це єдиний учасник кримінального процесу, який може допомогти і є компететний у цій ситуації. У цій статті аналізуються особливості співпраці судово-інформатичного експерта та органів слідства. Автором показані межі такої співпраці.

Ключові слова: цифровий доказ, судово-інформатичний експерт, аналіз цифрових доказів.

Мате И. Ж.

Анализ цифровых доказательств

После получения цифровых доказательств эксперт передаёт доказательства сотрудникам органов следствия, которые анализируют, оценивают и используют их в своей работе. Для анализа цифровых доказательств требуется соответствующее информатическое знание, часто не имеющееся в распоряжении у сотрудников органов следствия. Судебно-информатический эксперт – это такой единственный участник уголовного процесса, который умеет помочь и правомочен в этой ситуации. В этой статье представляется анализ особенностей сотрудничества судебно-информатического эксперта и органов следствия тесно сотрудничают друг с другом. Автором показаны пределы и границы такого сотрудничества.

Ключевые слова: цифровое доказательство, судебно-информатический эксперт, анализ цифровых доказательств.

▪ Анализ цифровых доказательств / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2015. – № 1(11) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles /2015/n1/15mizatd.pdf.

Mate I. Z.

The analysis of digital evidence

After acquisition of digital evidence forensic experts give them over to law enforcement officers, who analyze, evaluate and use them during their work. Analysis of digital evidence needs adequate IT knowledge and skills, although law enforcement officers often lack them. The forensic IT expert is the only participant in the penal procedure who can and is authorized to help. In this paper we can read some case studies, through them we introduce the process of analysis, presenting the close cooperation between IT experts and law enforcement officers. Finally, the author presents a suggestion how to treat the situation and makes a proposal for framework and borders of this cooperation.

Key words*:* digital evidence, forensic IT expert, analysis of the digital evidence.

▪ Анализ цифровых доказательств / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2015. – № 1(11) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles /2015/n1/15mizatd.pdf.