Секция «Криминалистика»

Создание классификатора бесплатного и условно-бесплатного программного обеспечения для решения задач компьютерно-технической экспертизы

Научный руководитель – Яковлев Алексей Николаевич

Ульянова Мирослава Андреевна

Студент (специалист)

Московский государственный технический университет имени Н.Э. Баумана, Социально-гуманитарные науки, Кафедра Юриспруденции, интеллектуальной собственности и судебной экспертизы, Москва, Россия

E-mail: ulyanova.mira@yandex.ru

Ускоряющееся развитие информационных технологий приводит к появлению новых способов создания, хранения, изменения, копирования и удаления данных. Увеличивается разнообразие методов и средств совершения компьютерных преступлений, в связи с чем необходима соответствующая модернизация инструментария компьютерно-технических экспертов, содействующих расследованию подобных инцидентов. Однако при выборе оснащения возникает ряд проблем.

Еще на стадии планирования эксперт должен учитывать соответствие выбранного программного обеспечения утвержденной методике исследования, описывающей средства производства экспертизы и способ их применения. Использованные методики перечисляются в заключении эксперта, подтверждая обоснованность его действий, при этом ход исследования описывается с достаточной для производства повторной или дополнительной экспертизы степенью детализации. Требование об указании примененной методики содержится в ст. 204 Уголовно-процессуального кодекса Российской Федерации [1].

Тем не менее в ходе ознакомления с методической литературой некоторых государственных (ЭКЦ МВД России, РФЦСЭ при Минюсте России) и частных (Некоммерческого Партнерства Поставщиков Программных Продуктов) экспертных учреждений было установлено, что описываемые ею принципы и рекомендованные программные средства не являются актуальными - зачастую они малопригодны для использования при исследовании современных устройств, файловых систем и форматов. Подобное ведет не только к значительному затруднению процесса обнаружения и обработки электронных следов, но и создает предпосылки к экспертным ошибкам, если исследование проводит молодой специалист без опыта производства экспертиз нового для него вида объектов. Однако в экспертном сообществе принято считать, что методики не являются и не должны являться единственным источником актуальной технической и методической информации - это лишь источник наиболее проверенной, принятой экспертным сообществом информации, которой обязаны доверять участники судопроизводства. Таким образом, несовершенство методического обеспечения лишь говорит о необходимости создания альтернативных справочных материалов и соответствующей модернизации законодательства.

В экспертных учреждениях так же существует неформальная практика производства экспертиз, актуализирующая в том числе и инструментарий. Однако появляются иные проблемы. Так, используемые автоматизированные проприетарные продукты, не охватываемые методиками, но широко распространенные в ведомствах (EnCase, FTK, Мобильный Криминалист), недоступны для небольших экспертных организаций, частных экспертов и студентов, получающих образование по данной специальности, что заставляет искать альтернативы.

В настоящее время активно развивается свободное программное обеспечение, возможности которого вполне могут быть использованы для решения различных экспертных за-

дач. Однако же в русскоязычном сегменте сети «Интернет», являющейся одним из основных источников информации о подобном инструментарии, в основном лишь дублируется неактуальная и некорректная информация о подобных продуктах. Временные затраты эксперта на поиск и проверку оптимального программного средства препятствуют быстрому и эффективному исследованию.

Для решения обозначенной проблемы была поставлена задача систематизации перечня свободного программного обеспечения, использование которого можно назвать результативным при применении в различных областях компьютерно-технической экспертизы.

Так, считаем целесообразным начать работу по подготовке отечественного классификатора экспертного программного обеспечения, в котором должны учитываться возможности как проприетарного экспертного программного обеспечения, так и экспертных программ, распространяемых по свободной лицензии. При условии своевременного внесения актуальной и корректной информации такой классификатор может стать полезным источником информации об экспертном инструментарии, использование которого возможно в том числе в учебных целях. В указанном случае классификатор будет представлять собой постоянно обновляемый справочник для студентов, получающих образование по специальности «Компьютерно-техническая экспертиза», а также будет способствовать студенческой научно-исследовательской деятельности.

В ходе выполнения поставленной задачи было проведено тестирование свободно распространяемого программного обеспечения для производства полного цикла компьютерно-технической экспертизы как в статическом, так и в динамическом режиме анализа. Проприетарные программные продукты в данном исследовании не тестировались в силу специфики решаемой проблемы. Для визуализации результатов работы была выбрана табличная форма в виду её наглядности, удобства использования и модернизации. Учтено требование о сохранении целостности данных (приведены примеры программных блокираторов, программного обеспечения для создания полных копий электронных носителей информации), содержащееся в ст. 16 Федерального закона «О государственной судебно-экспертной деятельности в Российской Федерации» [2]. Приведены программные продукты, позволяющие эффективно решать задачи по восстановлению удаленных и поврежденных файлов. Подобраны инструменты для исследования содержимого оперативной памяти, сетевого трафика, баз данных. Программное обеспечение разделено на категории в зависимости от используемой операционной системы экспертного персонального компьютера, вида исследуемых объектов, решаемых задач. Указан способ получения доступа к файлам программных продуктов (источники в сети "Интернет") и вид интерфейса (графический или терминальный).

Классификатор не является завершенным, предполагается последующее дополнение и расширение. К примеру, планируется размещение в сети «Интернет» созданного нами тематического сайта, который будет содержать более полные сведения о протестированном программном обеспечении (в том числе демонстрацию работы с решением конкретной экспертной задачи). Наличие подобной информации на постоянной основе в открытых источниках способно так же обеспечивать свободный доступ к компьютерно-технической экспертизе для сторон судебного процесса, что увеличивает прозрачность судопроизводства.

Источники и литература

1) Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 11.10.2018) (с изм. и доп., вступ. в силу с 21.10.2018) // Собрание законодательства РФ, 24.12.2001. – N 52 (ч. I). – Ст. 4921.

2) Федеральный закон от 31.05.2001 N 73-ФЗ (ред. от 08.03.2015) «О государственной судебно-экспертной деятельности в Российской Федерации» // Собрание законодательства РФ, 04.06.2001. – N 23. – Ст. 22918.

Иллюстрации

№	Наименование	Платформа	Назначение	Отрасль	В составе дистрибутива	Интерфейс	Источник
1	USB Write Blocker for ALL Windows	Windows	Программный блокиратор записи	ЭФ, ЭМУ	-	CL	https://sourceforge.net/projects/usbwriteblockerforwindows8/
2	Linux-write-blocker	Linux			-	CL	https://github.com/msuhanov/Linux-write-blocker
3	dd, dcfldd, dc3dd, dd_rescue	Linux	Создание образов ЭНИ		Linux	CL	Репозитории Linux
4	Belkasoft Acquisition Tool	Windows			-	GUI	https://belkasoft.com/bat
5	AccessData FTK Imager	Windows			FORENSIC TOOLKIT (FTK)	GUI	https://accessdata.com/product-download/forensic-toolkit-ftk-version-6.4
6	Guymager	Linux			-	GUI	https://guymager.soft112.com/download.html
7	HDD Raw Copy Tool	Windows			-	GUI	http://123-box.ru/3670
8	EnCase Forensic Imager	Windows			-	GUI	https://www.guidancesoftware.com/encase-forensic-imager/forensic-imager-download
9	Belkasoft RAM Capturer	Windows	Дамп ОП		-	GUI	https://belkasoft.com/ru/memory-dump
10	LiME	Linux			-	CL	https://github.com/504ensicsLabs/LiME
11	Belkasoft Evidence Center (30-days Trial)	Windows	Дамп, анализ ОП	ЭФ	-	GUI	https://belkasoft.com/ec
12	FireEye RedLine	Windows	Анализ ОП		-	GUI	https://www.fireeye.com/services/freeware/redline.html
13	Autopsy	Windows/ Linux	Поиск, анализ данных		The Sleuth Kit	GUI/Web-API	http://www.sleuthkit.org/autopsy/download.php
14	Volatility Framework	Windows/ Linux/MacOS			-	GUI/CL	https://www.volatilityfoundation.org/releases
15	bulk_extractor	Windows/ Linux			-	GUI/CL	https://github.com/simsong/bulk_extractor
16	ExifTool	Windows/ Linux/MacOS	Извлечение метаданных		-	CL	https://sourceforge.net/projects/exiftool/
17	Runtime DiskExplorer	Windows/ Linux	Просмотр структуры файловой системы		-	GUI	https://www.runtime.org/diskexpl.htm
18	dfir_ntfs	Linux			-	CL	https://github.com/msuhanov/dfir_ntfs
19	R.saver	Windows	Поиск и восстановление удаленных файлов		-	GUI	https://rlab.ru/tools/rsaver.html
20	Scalpel	Linux			-	CL	https://pkgs.org/download/scalpel
21	Foremost	Linux			-	CL	https://pkgs.org/download/foremost
22	HxD	Windows	Просмотр файлов в HEX		-	GUI	https://mhnexus.de/en/downloads.php?product=HxD20

Рис. 1. Созданная таблица классификатора бесплатного и условно-бесплатного программного обеспечения (Часть 1).

23	Xxd	Linux	Просмотр файлов в HEX	ЭФ	Linux	CL	Репозитории Linux
24	Windows Registry Recovery	Windows	Просмотр реестра ОС Windows		-	GUI	http://www.mitec.cz/wrr.html
25	yarp	Linux			-	CL	https://github.com/msuhanov/yarp
26	LastActivityView	Windows	Просмотр сведений о действиях пользователя		-	GUI	https://www.nirsoft.net/utils/computectivity_view.html
27	CrowdStrike CrowdResponse	Windows	Поиск вредоносных программ		-	CL	https://www.crowdstrike.com/resourcommunity-tools/crowdresponse/
28	USB Historian	Windows	Просмотр сведений о подключении USB-устройств		-	GUI	http://www.4discovery.com/our-tool
29	FAW	Windows	Анализ веб-страниц	СЭ	-	GUI	https://en.fawproject.com/download/
30	Wireshark	Windows/ Linux/MacOS	Анализ сетевых пакетов		-	GUI	https://www.wireshark.org/downloadml
31	Xplico	Linux			-	CL	http://www.xplico.org/download
32	sqlite3	Windows/ Linux/MacOS	Работа с базами данных	ЭБД	-	CL	https://www.sqlite.org/index.html
33	Nirsoft NirLauncher	Windows	Многофункциональный набор утилит	ЭФ, СЭ	Nirsoft NirLauncher	GUI, CL	https://launcher.nirsoft.net/
34	Sysinternals Suite	Windows			Sysinternals Suite	CL	https://technet.microsoft.com/ru-ru/sysinternals/tcpview.aspx
35	CAINE	Linux	Многофункциональный дистрибутив	ЭФ, ЭМУ, СЭ, ЭБД	CAINE	GUI, CL	https://www.caine-live.net/
36	Santoku	Linux			Santoku	GUI, CL	http://santoku-linux.com/download/
37	SIFT	Linux			SIFT Workstation		https://digital-forensics.sans.org/community/downls
38	Parrot Security OS	Linux			Parrot Security OS		https://www.parrotsec.org/
39	Kali Linux	Linux			Kali Linux		https://www.kali.org/

Условные обозначения:

1. CL – command line (командная строка)
2. GUI – graphical user interface (графический интерфейс пользователя)
3. ЭНИ – электронный носитель информации
4. ОП – оперативная память
5. ЭФ – экспертиза файлов и файловых систем
6. ЭМУ – экспертиза мобильных устройств
7. СЭ – сетевая экспертиза

Рис. 2. Созданная таблица классификатора бесплатного и условно-бесплатного программного обеспечения (Часть 2).