Компьютерно-техническая экспертиза — Lurkmore

Я нихуя не понял!

В этой статье слишком много мусора, что затрудняет её понимание. Данный текст необходимо очистить, ~~либо вообще снести нахуй~~

Компьютерно-техническая экспертиза (КТЭ) — род судебных экспертиз, объектами которых являются системные блоки персональных компьютеров, информационные носители (жесткие диски, дискеты и т. п.) и др.

Отдельно от КТЭ идет компьютерная экспертиза (КЭ), которую проводят в МВД.

Сферическая КТЭ в вакууме: жесткие диски, тысячи их!

В интернетах

КТЭ в этих ваших интернетах представлена популяциями судебных экспертов на форумах (в том числе и копирастских) и списках рассылок. В этой стране на первом месте по популярности мест обитания стоят форумы.

Троллинг

Троллинг судебных экспертов специфичен (ввиду их осведомленности о троллинге и троллях), но при грамотном подходе способен принести профит.

Судебный эксперт как объект троллинга

Судебный эксперт является хорошим объектом для троллинга. Для получения профита необходимо обладать достаточными познаниями в IT. Вброс, как правило, происходит путем создания провокационной темы. Приблизительный список наиболее удачных:

- Экспертиза зашифрованного раздела (рекомендация: необходимо в ходе обсуждения вброса давать рекомендации на тему правильной защиты данных от всевидящего ока судебных экспертов). Пример;
- Экспертиза распечаток принтеров (с целью доказать, что документ был распечатан именно на данном принтере);
- Сертификация судебного ПО (троллинг возможен даже в зале суда, если эксперт не знает как отвечать!);
- Лицензионность судебного ПО (иногда приводит к холивару на тему преимуществ пиратского ПО). Пример;
- Подброс «нелегального» ПО. Пример. Может использоваться в ходе троллинга «жертв правоохранительных органов».

Судебный эксперт как субъект троллинга

Невероятно, но факт: судебный эксперт тоже может троллить, причем и толсто, и тонко.

Одна из наиболее интересных тем для троллинга в англоязычной среде: может ли доказательство быть признано допустимым, если его аутентичность подтверждена при помощи MD5. Научной предпосылкой для подобного рода холиваров является ряд обнаруженных уязвимостей в алгоритме MD5.

При этом вопрос об аутентичности данных находится в сфере специальных знаний эксперта и, следовательно, как эксперт скажет, так и будет (почти. как скажет судья, так и будет. последний могет и в другого эксперта, ежели усомнитцо). Кроме этого, использование хеш-функций для подтверждения аутентичности данных не является обязательным (более того: иногда является нежелательным или, как в случае с этой страной, необоснованным). Такие дела.

Подобного рода троллинг эффективен **только** в зарубежных интернетах. Пара интересных для обсуждения тем:

- Контрафактность и признаки контрафактности.

Эксперт не может делать вывод о контрафактности той или иной копии программного продукта. Причина проста, однако некоторая часть экспертов ее не понимает: контрафактность экземпляра произведения —

юридический факт, а не технический. Отсюда вывод: эксперт может искать признаки контрафактности (например, наличие следов изменения кода программных продуктов или использование для активации продукта ключа из различных черных списков). Однако некоторые ученые считают, что «признаки контрафактности» являются антинаучной хуйней из ряда: «признаки адвоката». Ну ты понел.

- Вредоносность.

Так вышло, что вредоносность программы является то юридическим, то техническим понятием в зависимости от оратора (пруфлинки: [1], [2]). К счастью, до признаков вредоносности еще не дошло, но есть обратный эффект: некоторые эксперты любят признавать вредоносными программами различные кряки, кейгены и эмуляторы ключей. Короче, еще один повод для спора. Забавно бывает, когда при судебном преследовании некоторых скипт-кидисов вредоносными программами признают Internet Explorer и даже Notepad, так что засудить могут всех 100 % пользователей компьютера.

Заключение эксперта как источник лулзов

Заключение эксперта — документ, являющийся доказательством по уголовному или гражданскому делу, в котором экспертом даются ответы на вопросы, поставленные при назначении экспертизы. Мало того, что задачи эксперту часто ставят по определению идиотские (например, при экспертизе машин кулхацкеров очень часто отсутствует задача поиска скрытого ПО, позволяющего орудовать в сети от имени жертвы), так еще и на роль экспертов выбирают адово одаренных личностей. Все это рождает изрядное количество лулзов.

Примеры:

- Одиночные фразы, например, *«на основании собранных данных я догадался»*;
- Экспертизы целиком: [3], [4];
- Идиотские заключения об используемых вредоносных программах. В списке вредоносных программ были замечены: Internet Explorer, Notepad… На основании таких «заключений» можно кидать в кутузку абсолютно любого.

«Жертва правоохранительных органов» как объект троллинга

Типичная «жертва правоохранительных органов» — кулхацкер. Особо ценный поциент — кулхацкер, у которого вчера изъяли системный блок. Типичные обсуждаемые темы:

- Паяльник
- DriveCrypt раздел в руках ФСБ, смогут ли вскрыть? Или вот в таком ключе.

В подобных темах всегда присутствуют следующие личности: базовый набор кулхацкеров, более-менее грамотный специалист в обсуждаемых вопросах. Типичные лулзы:

> А допустим если есть ноут, на нем вся инфа и поставить пароль на биос. Катит такая тема или нет?

> про BestCrypt, перестал доверять программе после того, как из достоверных источников рассказали, про то как ФСБ ломали их крипты, пока вёлся допрос, а в конце допроса когда показывали скрытые файлы, народ просто был в шоке.

Обычно присутствующий в теме более-менее грамотный специалист пытается убедить всех, что шифрация данных проверенным ПО (читай: свободным ПО) спасет чуть более, чем во всех случаях. Наиболее выгодный вариант дискуссии с точки зрения тонкого тролля — попытка дискредитировать все позиции этого «специалиста» путем отсыла к различного рода «академическим исследованиям». Это, как правило, вызывает у кулхацкеров реакцию из разряда «ФСБ может все».

В связи с особой тонкостью данного вида троллинга и непредсказуемости дискуссии разрешается троллить с использованием реальных аккаунтов (при условии, что быстрый поиск в Гугле мигом выдаст вашу связь с КТЭ), что придаст вашему мнению еще больше веса, и попытки отослать вас учить матчасть будут заранее обречены на провал.

Иногда экспертные организации делают вброс сами (искать в тексте слово *PGP*).

- Отрицаемое шифрование (*deniable encryption*). Миниатюрный срач на ЛОРе.

Здесь наблюдается борьба здравого смысла и математики. Оппоненты тролля будут пытаться доказать, что отличить зашифрованные данные от псевдослучайных невозможно. Тролль опять же будет отсылать быдло к «академическим исследованиям» (пример). После прочтения оппонентами подобных исследований можно отсылать к различным документам с тегом LE only. Тем более, подобные документы по обсуждаемой теме действительно есть, я гарантирую это!

- Ментовский софт (речь в большинстве случаев идет об экспертном ПО). Пример на одном школьном портале.

- Эти ваши СОРМы и Эшелоны. Сугубо теоретическое обсуждение. А вот тут немного интереснее.

Одна из наиболее сытных тем. Отличается тем, что большинство людей никогда не видели технических спецификаций СОРМ, характеристик продуктов и нотариально заверенных скриншотов соответствующих систем. Основное направление троллинга — попытка переубедить специалистов по всему, утверждающих как ПРАВИЛЬНО шифровать переписку.

- Методики проведения экспертных исследований.

Параноик-криптолог как объект троллинга

Параноик-криптолог не является объектом троллинга. По крайней мере, в рамках тем КТЭ. Просто он УЖЕ знает, что Майкрософт внесла[*ЩИТО?*] в Свисту необходимый набор бекдоров для доступа к любым зашифрованным данным.

Еда

11 сентября Ache666 Alt-Right Avatar Beon.ru Boku no Pico Butthurt Championat.com Check you Chris-chan Cruel Addict Du Volon Fandom He Will Not Divide Us Leyla 22 Limp Bizkit Lingqiyan Linkin Park Megadeth MISS HOLLYWOOD Noize MC Project N.I.G.R.A. Pussy Riot Ray William Johnson Rsdn.ru Rutracker.org SupLisEr VIP X не умер Yandere Simulator Zeitgeist Аббатус Авраам Болеслав Покой Адольфыч АлисА Алкснис Аллан999 Альбац Альберт Акчурин Андерс Брейвик Андрей Лаптев Андрей Сковородников Анна Бешнова Апач Бабка АТС Багиров Бачинский Белоцерковская Белый Колонизатор Бобби Котик Бодибилдинг Болашенко Бурление говн Валерий Назаров Варракс Леонид Василевский Ватник Веганы Миша Вербицкий Винилофилия Виталик Вован Метал Высер Геноцид армян Германыч Глобальное потепление Гоблин Гага Говнарь Говно Город Снов Гринпис Гутник Дед ИВЦ Джеттейм Джигурда Джипсилиля Диванные войска Доброволец Друмба Дэниел Петрик Евровидение Еда Женя Духовникова Жертвы пранка Закон По Змагар Знаменитость российского уровня Иван Гамаз Иван Охлобыстин ИГИЛ Илья Фарафонов Император двачей Индусский код Инна Жиркова Кавказ-Центр Кактус Карикатуры на Мухаммеда Карина Будучьян Кинопоиск Коммуняки