Что такое программно-техническая экспертиза

Обзор

Программно-техническая экспертиза - это применение методов компьютерного анализа в интересах определения потенциальных юридических доказательств преступления. Доказательства могут быть найдены для широкого спектра компьютерных преступлений и злоупотреблений, в том числе, кражи коммерческой тайны, кражи или уничтожения информационной собственности и мошенничества. Компьютерные специалисты могут использовать множество методов для обнаружения необходимых для расследования данных, которые находятся в компьютерной системе, или восстанавливать удалённые, зашифрованные или повреждённые файлы. Эти сведения могут помочь во время расследования, присяги или фактического судебного разбирательства.

Преимущества методологии профессиональной экспертизы

- Беспристрастный компьютерный эксперт, который помогает во время расследования, как правило, имеет опыт работы с широким спектром аппаратного и программного обеспечения компьютеров.
- Это всегда полезно, когда ваше дело затрагивает аппаратное и программное обеспечение, с которым этот специалист непосредственно знаком.
- Но фундаментальная компьютерная и программная реализация часто очень похожи в разных системах, и опыт в одном приложении или операционной системе, часто легко применить в новой системе.

- В отличие от бумажных доказательств, компьютерные доказательства могут часто существовать в разных формах, с более ранними версиями, обычно они доступны на компьютерном диске.
- Зная возможность их существования, даже альтернативные форматы тех же данных могут быть обнаружены.
- Знающий эксперт может профессионально провести процедуру обнаружения и выявить больше данных, по сравнению с обычным расследованием.
- Кроме того, при локальной экспертизе, для случаев, когда компьютерные диски не конфискованы или не скопированы (см. ниже), такой эксперт может быстрее определить места, где стоит искать, подсказки, дополнительные источники информации для данного расследования .
- Они могут принять форму более ранних версий файлов (например, заметки, электронные таблицы), которые все еще существуют на диске компьютера или на резервном носителе, или по-разному форматированные версии данных, либо созданные или обработанные другими прикладными программами (например, для обработки текста , электронных таблиц, электронной почты, расписания или графики).

Защита доказательств крайне необходима

1. Никакие возможные доказательства не повреждаются, не уничтожаются и не компрометируются в течение экспертизы.
2. Для анализа не используются никакие компьютерные вирусы.
3. Полученные доказательства определённым образом сохраняются и защищаются от механического или электромагнитного воздействия.
4. Поддерживается постоянное наблюдение за сохранностью полученных данных.
5. Бизнес-операции затрагиваются на ограниченное количество времени, если потребуется.
6. Любой юридическая информация о клиенте, непреднамеренно приобретённая во время исследования является этически и юридически уважаемой и не разглашается.

Меры, предпринимаемые экспертом

- Защита данной компьютерной системы во время экспертизы от любых возможных изменений, повреждений, порчи данных, или вирусной атаки.
- Изучение всех файлов данной системы. Это включает в себя обычные файлы, удалённые еще оставшиеся файлы, скрытые файлы, защищенные паролем файлы и зашифрованные файлы.
- Восстановление всех (или столько, сколько возможно) из обнаруженных удаленных файлов.
- Чтение (по возможности) содержимого скрытых файлов, а также временных файлов или файлов подкачки, используемых прикладными программами и операционной системой.
- Доступ (если это возможно и если это юридически разрешено) к содержимому защищенных или зашифрованных файлов.

Меры, предпринимаемые экспертом

- Анализ всех относящихся к делу данных, найденных в специальных (и обычно недоступных) разделах диска. Например "нераспределенное" пространство на диске
- Общий анализ компьютерной системы, а также список всех возможно относящихся к делу файлов и обнаруженных данных.
- Кроме того, эксперт высказывает своё мнение о компоновке системы, обнаруженных файловых структурах, любых обнаруженных данных и информации об авторстве действий, любых попытках скрыть, удалить, защитить, зашифровать информацию, и обо всём остальном, что было обнаружено и имеет отношение к общей компьютерной экспертизе.
- Профессиональная консультация и / или свидетельство, по мере необходимости.

Кто может использовать программно-техническую экспертизу?

- Уголовное прокуроры могут используют компьютерные доказательства в различных преступлениях, где уличающие документы могут быть найдены: убийства, финансовое мошенничество, хищение наркотиков и протоколирование, и детской порнографии.
- В гражданских спорах полезны личные и деловые записи, найденные в компьютерных системах, которые имеют отношение к: мошенничеству, разводу, дискриминации и случаям домогательства.
- Страховые компании могут смягчить издержки с помощью обнаруженных доказательств возможного мошенничества при аварии, поджоге, случаях компенсации.
- Корпорации часто нанимают специалистов по программно-технической экспертизе чтобы выяснить доказательства, относящиеся к: сексуальным домогательствам, растрате, хищению или незаконному присвоению фирменных секретов и другой внутренней / конфиденциальной информации.
- Сотрудники правоохранительных органов часто нуждаются в помощи при проведении предварительной экспертизы или экспертизы после изъятия оборудования.
- Иногда нанимают специалистов программно-технической экспертизе в случае следующих претензий: неправомерное окончание срока действия, сексуальные домогательства или дискриминация по возрасту.