

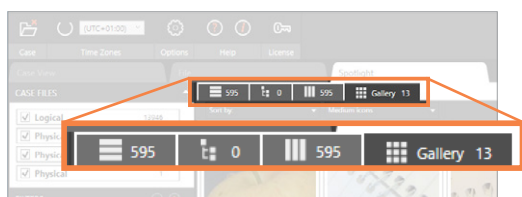
XAMN 1.0 [БЕТА] СВЕДЕНИЯ О ВЕРСИИ

Spotlight

ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ SPOTLIGHT ВЕРСИИ 1.0 [БЕТА]

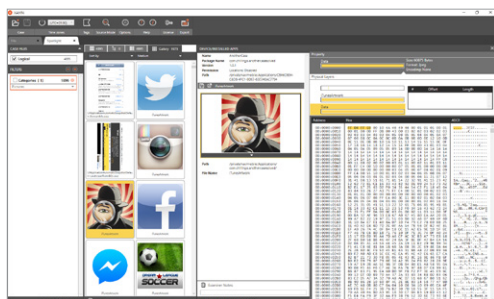
- » Режим сценария для одновременного просмотра нескольких извлечений
- » Представления «Grid» (Сетка), «List» (Список), «Gallery» (Галерея), «File Tree» (Файловая структура).
- » Одновременный последовательный анализ до 25 отдельных файлов XRY.
- » Режим первоисточника для просмотра исходных данных.
- » Режим настройки времени в формате UTC для локального времени.
- » Мощные функции наложения фильтров для отсеивания ненужных данных и подробного представления целевой информации.
- » Обзор страницы статистики сценария с быстрыми ссылками.
- » Отслеживание данных в разных представлениях

4 РАЗНЫХ СПОСОБА ПРОСМОТРА ДАННЫХ



Spotlight позволяет просматривать данные четырьмя разными способами: с помощью представлений «List» (Список), «File Tree» (Файловая структура), «Grid» (Сетка) и «Gallery» (Галерея). Представление «Grid» (Сетка) показывает, как данные отображались в программе Reader в XRY версии 6, и выводит элементы колонками. В представлении «List» (Список) данные отображаются вертикально, как в XRY Viewer. Представление «Gallery» (Галерея) специально предназначено для просмотра изображений. Наконец, новое представление «File Tree» (Файловая структура) показывает расположение данных в файловой системе исследуемого устройства.

РЕЖИМ ПЕРВОИСТОЧНИКА



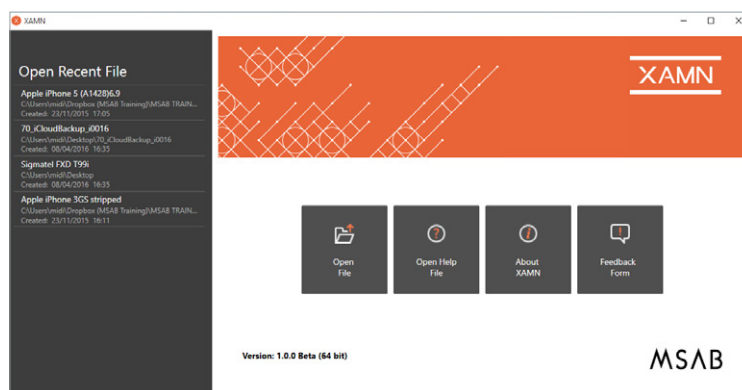
Режим первоисточника позволяет отслеживать и просматривать исходный шестнадцатеричный код данных, отображаемых в Spotlight. Пользователи могут видеть исходные данные в контексте извлеченных данных и изображений, что позволяет оценивать и интерпретировать данные. Просто нажмите кнопку «Source mode» (Режим первоисточника), или щелкните правой кнопкой мыши соответствующие данные на панели сведений и выберите параметр «Examine in Source Mode» (Исследовать в режиме первоисточника). Для оценки отобразятся исходные шестнадцатеричные данные, путь, слои и изменения.

СИЛА И ПРОИЗВОДИТЕЛЬНОСТЬ С XAMN SPOTLIGHT

XAMN Spotlight — это новое, фирменное программное обеспечение, разработанное с учетом требований экспертов. Оно имеет расширенные, по сравнению с XRY, возможности и направлено на просмотр данных, создание отчетов и анализ информации.

Линейка инструментов XAMN предназначена для повышения эффективности работы экспертов и улучшения производительности за счет более быстрой идентификации важной информации. ПО XAMN Spotlight удобно в использовании и имеет минимальные требования к оборудованию и установке. Любой эксперт может оценить его преимущества, которые позволяют быстрее раскрывать преступления, экономя время и облегчая обнаружение преступных деяний.

XAMN Spotlight построено на базе XRY Reader, и поэтому является невероятно мощным инструментом для поиска данных. Это 64-разрядное приложение работает на Windows 7, 8 или 10 и не требует предварительной установки. Для работы XAMN Spotlight необходимо лишь наличие .NET Framework версии 4.5 или выше.



РЕЖИМ СЦЕНАРИЯ

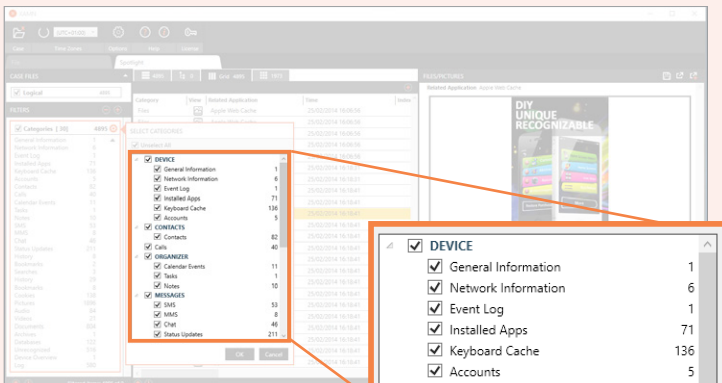
Режим сценария позволяет просматривать несколько файлов XRY, созданных при исследовании одного и того же устройства разными методами. Обычный файл сценария может содержать данные логического и физического извлечений, данные карты памяти, SIM-карты, камеры и облачные данные — все в одном месте. Spotlight может отображать результаты поиска с помощью нескольких разных представлений. Пользователи могут свободно переключаться между результатами, не делая новый запрос. Это позволяет просматривать одни и те же результаты поиска с разных точек зрения. Когда пользователь переключается на другое представление результатов, Spotlight запоминает последний выбранный элемент и отображает его в новом представлении результатов. Всего пользователи могут просматривать в Spotlight до 25 разных файлов XRY.

БЕСПЛАТНАЯ ЛИЦЕНЗИЯ XAMN SPOTLIGHT

На каждую имеющуюся лицензию XRY пользователи могут получить одну бесплатную копию XAMN Spotlight. Срок действия этих лицензий XAMN Spotlight будет соответствовать сроку действия текущей лицензии XRY.

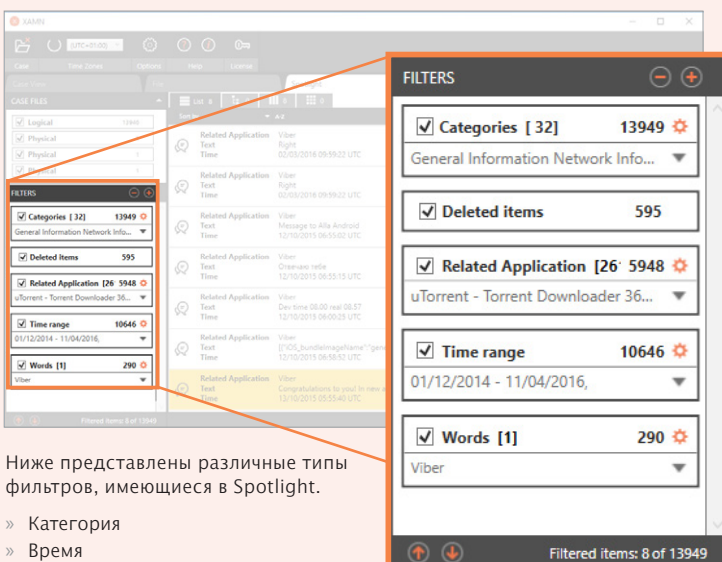
Для того чтобы активировать XAMN Spotlight, загрузите программное обеспечение с клиентского портала MSAB. Затем обновите лицензию XRY или запросите новую лицензию с license@msab.com

ФИЛЬТРЫ ПОМОГАЮТ НАЙТИ НАИБОЛЕЕ ПОДХОДЯЩИЕ ДАННЫЕ



Основная концепция в XAMN Spotlight — это эффективное использование фильтров. Эксперты могут создавать сложные поисковые запросы с помощью настройки фильтров. Результаты отображаются в одном из нескольких представлений, что облегчает сравнение данных. В поле фильтров отображаются текущие настройки фильтра, а также число элементов совпадения. Фильтры можно включать и отключать для быстрого изменения запроса.

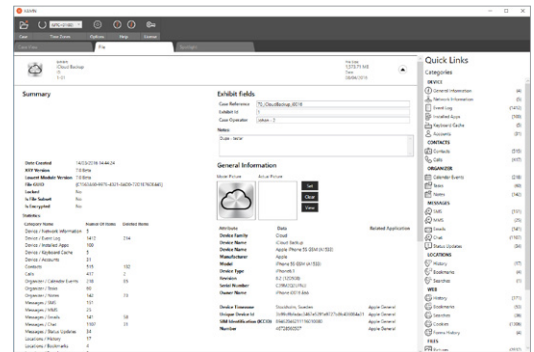
Фильтры работают совместно в комбинации. Элемент должен соответствовать всем фильтрам, чтобы попасть в результаты. Пользователь может объединять любое число фильтров. Также допускается объединение нескольких фильтров одного типа. Некоторые фильтры также включают в себя простую функцию OR (ИЛИ), позволяя вводить несколько значений. Например, фильтр текста допускает наличие нескольких строк, любая из которых будет рассматриваться как совпадение. Все эти функциональные фильтры помогают пользователям быстро и эффективно находить наиболее подходящие данные.



Ниже представлены различные типы фильтров, имеющиеся в Spotlight.

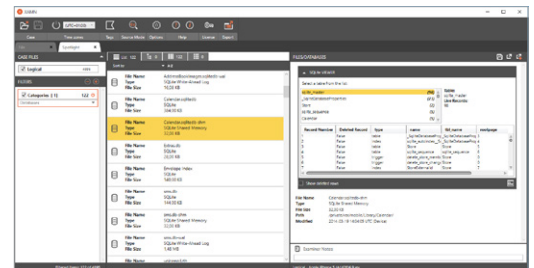
- » Категория
- » Время
- » Имя и размер файла
- » Имя папки
- » Удаленные файлы
- » Соответствующее приложение
- » Ярлыки
- » Список слов (импортируется как простой текст)

ВКЛАДКА ПРОСМОТРА ФАЙЛОВ



Это страница обзора, отображаемая в начале каждого файла сценария, на которой представлен комплексный обзор всех ключевых фактов и включенных в сценарий файлов XRY. Обзор сценария объединяет в себе итоговые сведения об устройстве, восстановленные данные и введенные пользователем подробности сценария. В отчете также имеется несколько быстрых ссылок, с помощью которых эксперты могут перейти непосредственно к определенной категории данных в отчете.

ТРИ СРЕДСТВА ПРОСМОТРА: SQLITE, XML И PLIST.



В XAMN Spotlight имеется три разных всплывающих средства просмотра для исследования содержимого смартфона: SQLite, XML и Plist. Для соответствующего типа файлов просто выберите доступное средство просмотра, представленное на панели сведений.

НАСТРОЙКА ВРЕМЕНИ В ФОРМАТЕ UTC



Уникальная функция XRY — способность упорядочивать отметки времени на нескольких поддерживаемых устройствах, что позволяет осуществлять по-настоящему точное сравнение отметок времени. Функция настройки времени в формате UTC еще больше расширяет возможности данного преимущества, предоставляя пользователям возможность устанавливать для сравнения все отметки времени на любой часовой пояс. Это позволяет экспертам видеть при исследовании локальное время событий.

ПРЕДСТОЯЩИЕ ВЕБИНАРЫ

Если вы хотите стать участником бесплатного вебинара на английском языке обо всех новых продуктах комплекса средств MSAB для экспертно-криминалистических исследований мобильных устройств, посетите веб-сайт: www.msab.com/training/webinars/