Современные возможности криминалистического исследования компьютеризированных элементов автомобилей.

АНАЛИЗ ГОЛОВНЫХ УСТРОЙСТВ

И.А. Бережной, Следственный комитет РФ

П.И. Лосев, НТЦ «Информационная безопасность»

И.Б. Пугачёв, НТЦ «Информационная безопасность»

Цели анализа

- Получение информации, хранящейся в головном мультимедийном устройстве автомобиля:
  - телефонная книга
  - история звонков
  - сообщения (если поддерживается)
- Информация о перемещении автомобиля (при наличии навигации)
  - маршруты перемещения
  - история поиска
- Информация о самом автомобиле (при наличии механизмов защиты)
  - VIN
  - марка, модель

Объект анализа

Ключевые характеристики

Расположение искомой информации:

- файловая система, расположенная в энергонезависимой памяти
- Текстовые файлы/реляционная база данных/бинарные файлы

Аппаратные

- многопроцессорность (минимум два: прикладной (взаимодействие с пользователем) и периферийный
- Несколько микросхем энергонезависимой памяти с разными интерфейсами (NAND,SPI,MMC,UFS)

Программные

- Одна или несколько операционных систем
- Различные виды ОС: Linux, Android, iTron, QNX, Windows CE и производные от них

Демонтаж микросхем памяти

Основные операции

- демонтаж микросхемы памяти/подключение на плате
- считывание на программаторе

Достоинства

- универсальность метода
- типовые файловые системы

Недостатки

- информация может располагаться в нескольких микросхемах
- наличие защитного покрытия на печатной плате (компаунд, силикаты)
- фиксация микросхем на клею
- специализированное оборудование эксперта

Технологические интерфейсы автопроизводителя

Основные операции

- подключение к отладочному интерфейсу(чаще всего UART)

Достоинства

- унифицированы
- доступ к файловой системе
- относительно легко можно самостоятельно найти

Недостатки

- Интерфейс может работать только на вывод отладочной информации
- Режим ввода может активироваться специальной последовательностью/установкой дополнительных элементов/изъят на программном уровне

Технологические интерфейсы производителя ГУ

Основные операции

- Выполнение специфических процедур/подключение специфических устройств

Достоинства

- Альтернативный доступ к файловой системе
- Автопроизводитель не подозревает о таком доступе

Недостатки

- Зависит от производителя ГУ/сборочного автозавода

Hyundai I30 (GD)

- Операционная система: Windows CE
- Навигационная программа: запуск с uSD (внешний носитель)
- Технологическая консоль: нет.

- Доступ к навигационным данным
- Сохраняются на карте uSD
- Доступ к телефонной книге и истории звонков
- Через интерфейс выбрать навигационной программой EXPLORER.EXE

Audi A6 (Harman)

- Операционная система: QNX 6.5
- Навигационная программа: встроенная
- Технологическая консоль: только на вывод

- Доступ к файловой системе
- Подключение специализированного UART или Ethernet адаптера открывает отладочную консоль. Для доступа нужно знать пароль пользователя root. После получения доступа к файловой системе, можно найти и скопировать требуемые файлы. Формат файлов - MySQL.

Hyundai Solaris (LG)

- Операционная система: Android 4
- Навигационная программа: внешняя (SD)
- Технологическая консоль: только на вывод

- Доступ к файловой системе
- Скрытые точки в интерфейсе, «простукивание» которых открывает меню включения ADB. При включенном ADB можно осуществить подключение к внутреннему usb-разъему adb-кабеля либо к внешнему USB — специализированного Ethernet-адаптера. Через ADB получаем доступ к файловой системе. Формат файлов - MySQL/бинарный.

Спасибо за внимание!

Докладчик	Почта
И.А. Бережной	
П.И. Лосев И.Б. Пугачёв	ntc-ib@yandex.ru