СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Судебно-экспертный центр

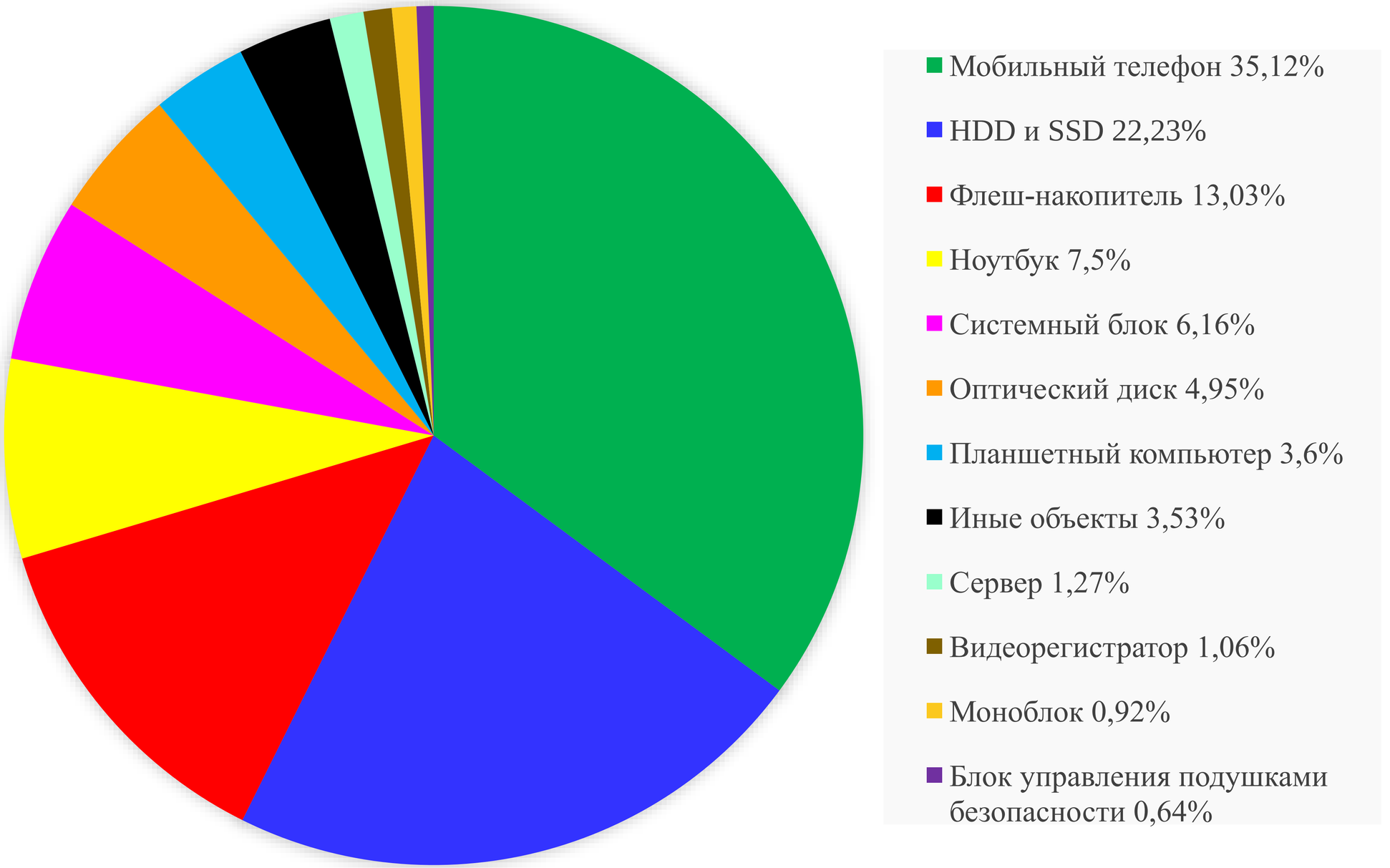
Положительный опыт криминалистического исследования мобильных устройств

Докладчик:
старший эксперт
Шавловский Андрей Борисович

E-mail: ashavlovsky@yandex.ru

Конференция «РусКрипто» 2022

Статистика по исследуемым объектам в 2021 году

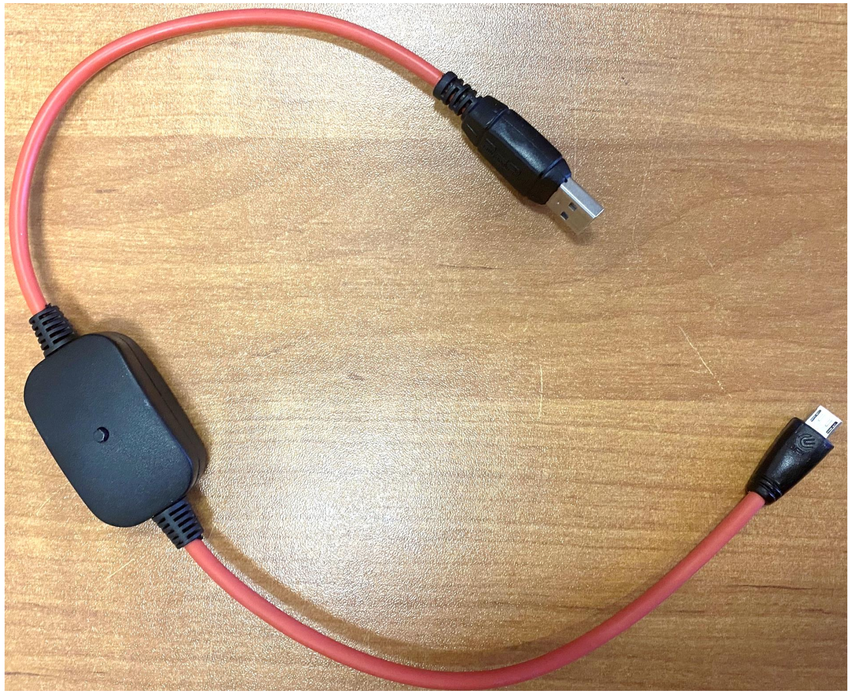


Работа с Android-устройствами на Qualcomm

Общие принципы работы:

- перевод устройства в сервисный режим аварийной загрузки EDL (mode 9008)
- использование доверенного файла-программера (протокол firehose)

prog_emmc_firehose_8937_ddr.mbn



Перевод в режим EDL:

- сервисная команда в терминале fastboot/adb;
- специализированный кабель (Xiaomi EDL);
- замыкание контактных площадок на системной плате;
- иные способы (зажатие определенных кнопок, перезагрузка в EDL из recovery и т.д.)

Планшетный компьютер Samsung Galaxy Tab A SM-T355, заблокированный цифровым паролем с частично неисправным экраном

Устройство*:

Марка: Samsung
Модель: Galaxy Tab A 8.0 SM-T355
ОС: Android 5.0, 6.0, 7.1
Процессор: Qualcomm Snapdragon 410 MSM8916
Встроенная память: 16 Гб

Возможности СПО по исследованию объекта:

Мобильный криминалист:

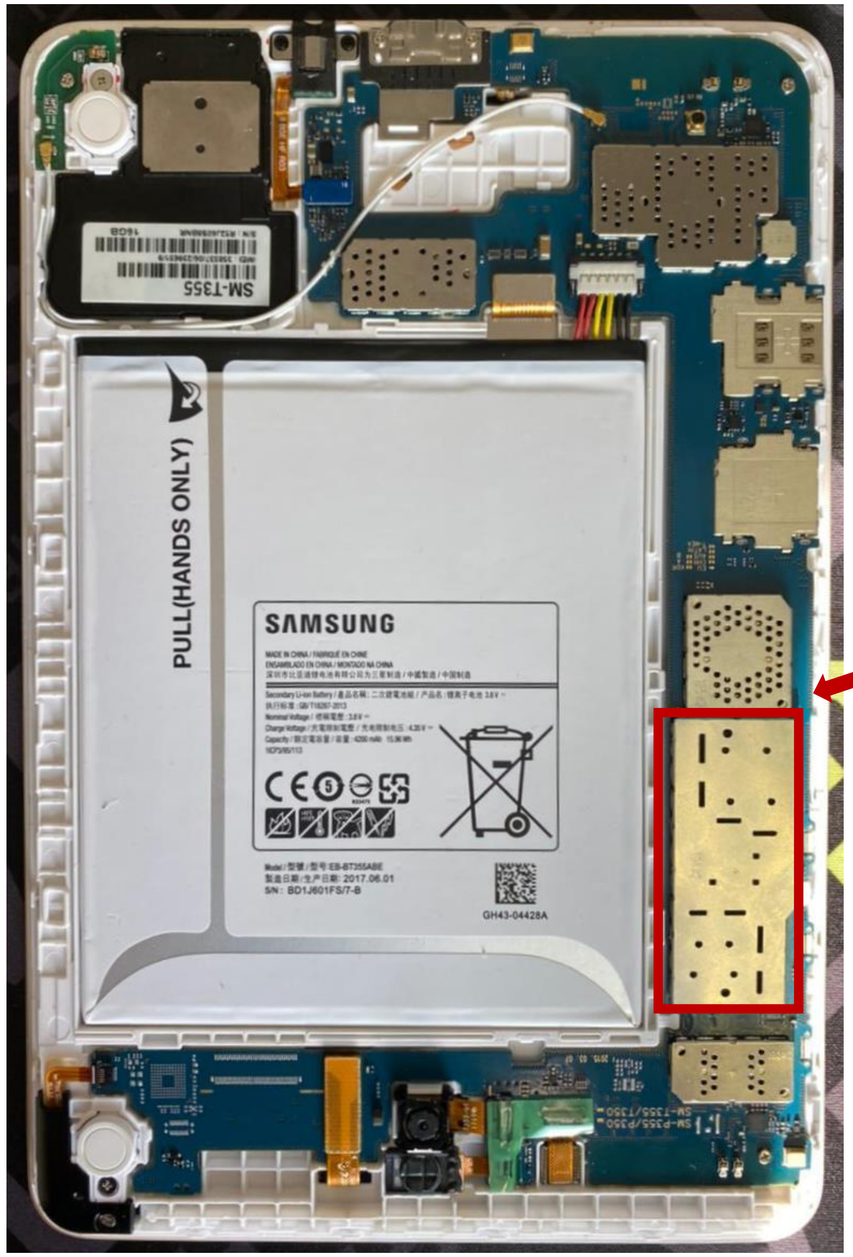
1. ✖ Установка модифицированного образа восстановления (метод Samsung Android) – отсутствует модифицированный образ для указанной модели.
2. ✖ Извлечение через Qualcomm EDL (процессор поддерживается) – отсутствуют сведения о контактных площадках для перевода в EDL.
3. ✖ Извлечение по ADB через уязвимость в операционной системе.

Cellebrite UFED:

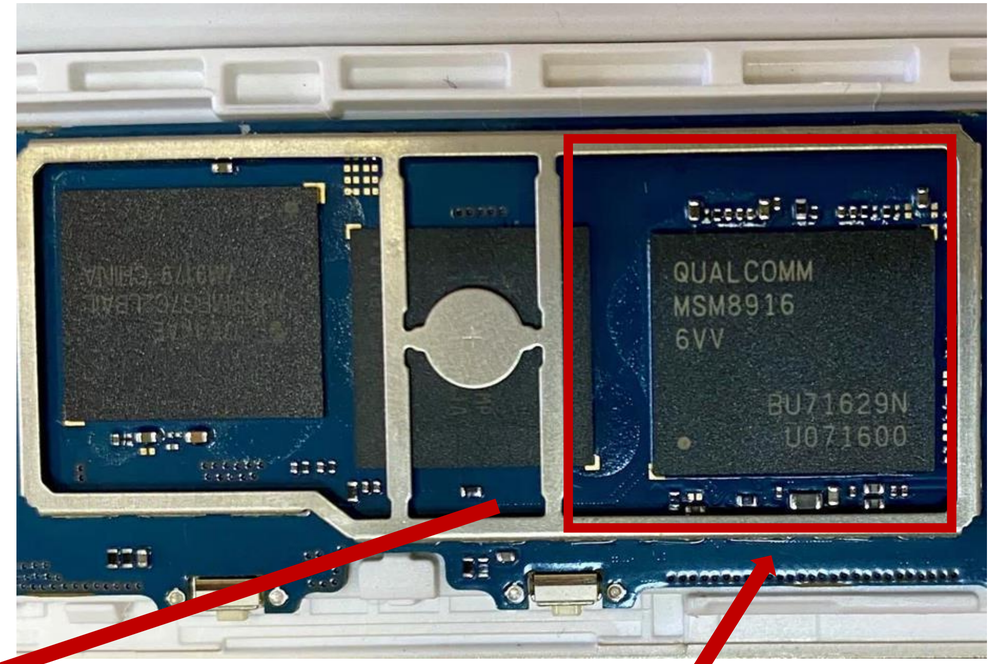
1. ✖ Отсутствует профиль извлечения для указанной модели. Имеется универсальная возможность извлечения для разблокированных устройств по ADB.
2. ✖ Извлечение через Decrypting EDL - отсутствуют сведения о контактных площадках для перевода в EDL.

*URL: https://4pda.to/

Поиск контактных площадок для перевода Samsung Galaxy Tab A SM-T355 в режим EDL

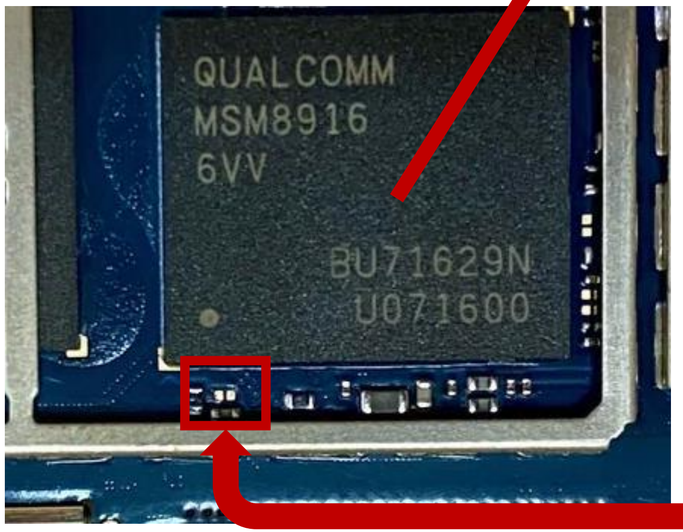


1

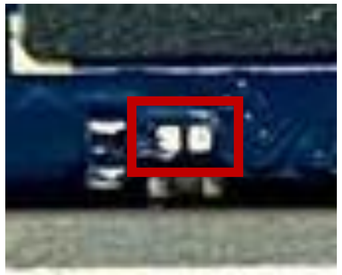


2

1. Поиск контактных площадок на похожих моделях.
2. Проверка контактных площадок при помощи резистора с сопротивлением 100 ОМ для предотвращения повреждения устройства



3



4

Контактные площадки на плате для перевода в режим EDL

Планшетный компьютер Samsung Galaxy Tab A SM-T355, заблокированный паролем с частично неисправным экраном

Устройство*:

Марка: Samsung
Модель: Galaxy Tab A 8.0 SM-T355
ОС: Android 5.0, 6.0, 7.1
Процессор: Qualcomm Snapdragon 410 MSM8916
Встроенная память: 16 Гб

Возможности СПО по исследованию объекта:

Мобильный криминалист:

1. ✖ Установка модифицированного образа восстановления (метод Samsung Android) – отсутствует модифицированный образ для указанной модели.
2. ✚ Извлечение через Qualcomm EDL (процессор поддерживается) – ~~отсутствуют сведения о контактных площадках для перевода в EDL.~~
3. ✖ Извлечение по ADB через уязвимость в операционной системе.

Cellebrite UFED:

1. ✖ Отсутствует профиль извлечения для указанной модели. Имеется универсальная возможность извлечения для разблокированных устройств по ADB.
2. ✚ Извлечение через Decrypting EDL - ~~отсутствуют сведения о контактных площадках для перевода в EDL.~~

*URL: https://4pda.to/

Мобильный телефон Honor 6C, заблокированный пользовательским паролем

Устройство*:

Марка: Honor
Модель: 6C
ОС: Android 6.0
Процессор: Qualcomm Snapdragon 435 MSM8940
Встроенная память: 32 Гб

Возможности СПО по исследованию объекта:

Мобильный криминалист:

✖ 1. Извлечение через Qualcomm EDL (процессор поддерживается) – отсутствует программер firehose.
✖ 2. Извлечение через Huawei Qualcomm EDL (процессор поддерживается) – отсутствует программер firehose.
✖ 3. Извлечение по ADB через уязвимость в операционной системе – для разблокированных устройств.

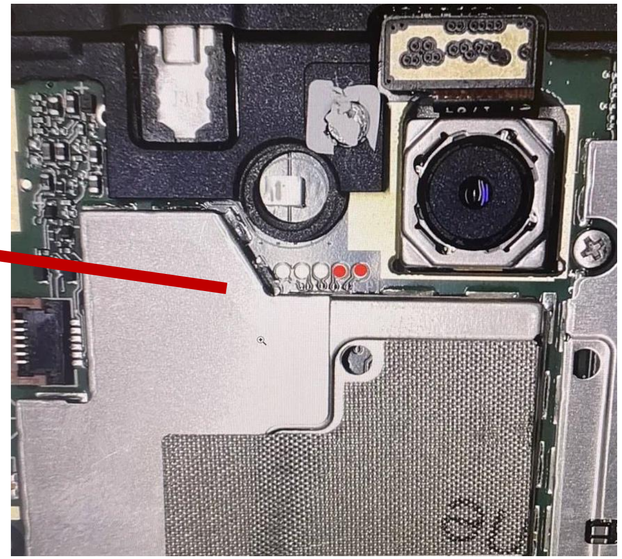
Cellebrite UFED:

✖ 1. Отсутствует профиль извлечения для указанной модели. Имеется универсальная возможность извлечения для разблокированных устройств по ADB (rooted) и Qualcomm Live.
✖ 2. Извлечение через Decrypting EDL – отсутствует программер firehose.

*URL: https://4pda.to/

Поиск файлов-программеров (firehose) к устройствам от Huawei

1

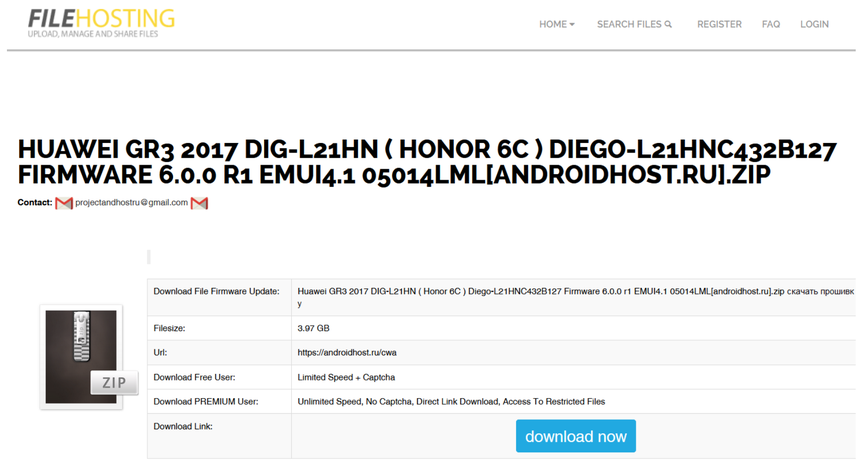


2 Контактные точки для перевода в режим EDL устройства Honor 6C

Поиск по ключевым словам: **firehose [модель устройства], programmer [модель устройства], firmware [модель устройства]**

Справочные ресурсы в сети Интернет:

- https://4pda.to/
- https://forum.xda-developers.com/
- https://www.gsmarena.com/
- https://gsmforum.ru/
- https://smartsworld.ru/
- https://androidhost.ru/
- Арабские, индийские и китайские сайты, посвященные сервису мобильных устройств (например, https://www.arabyfirmware.com/).



Мобильный телефон Nokia 5, заблокированный паролем

Устройство*:

Марка: Nokia
Модель: TA-1053
ОС: Android 7.1, 8.0, 8.1, 9
Процессор: Qualcomm Snapdragon 430 MSM8937
Встроенная память: 16 Гб

Возможности СПО по исследованию объекта:

Мобильный криминалист:

1. ? Извлечение через Qualcomm EDL (процессор поддерживается)

2. ✖ Извлечение по ADB через уязвимость в операционной системе – для разблокированных устройств.

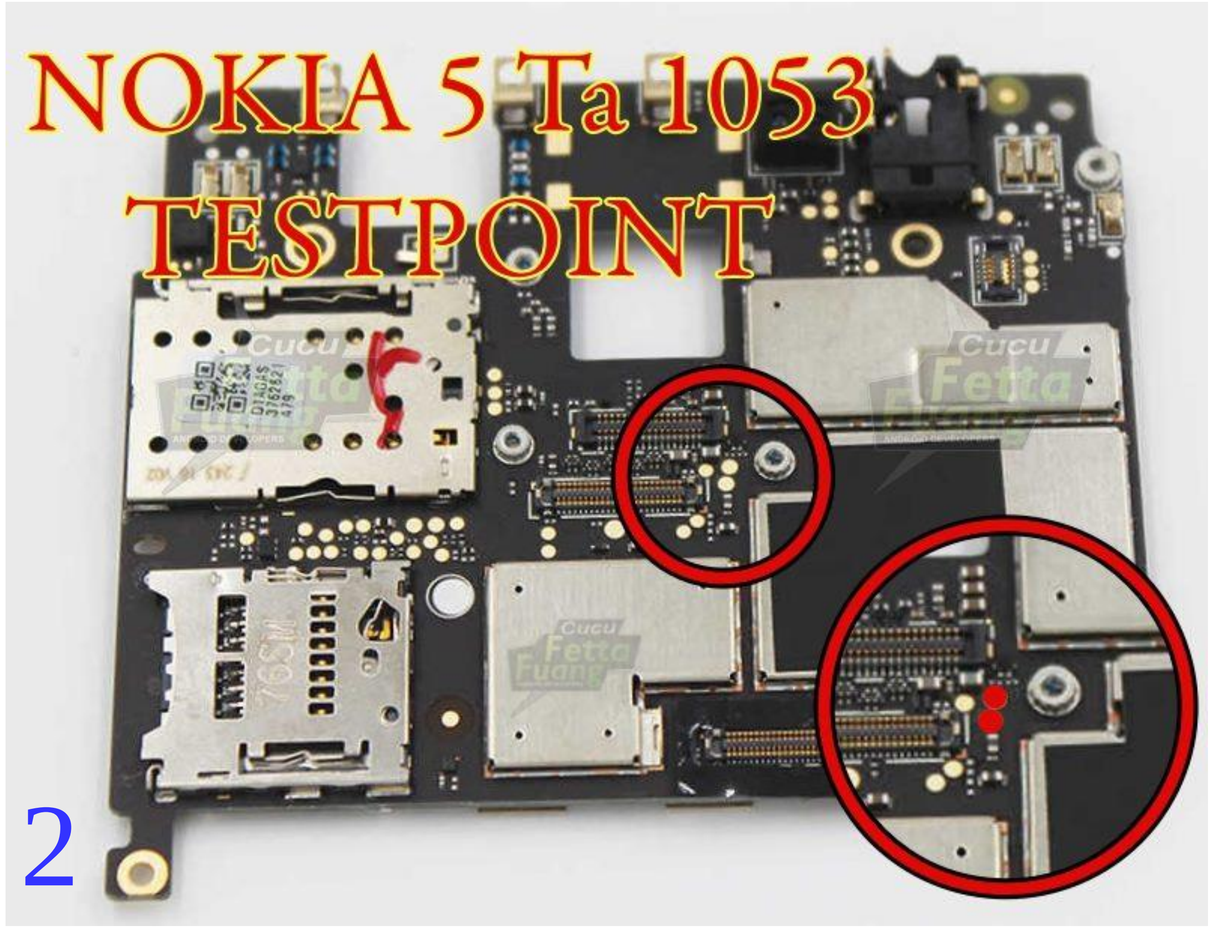
Cellebrite UFED:

1. ? Имеется профиль извлечения для указанной модели. Извлечение через BootLoader EDL.
2. ✖ Извлечение через ADB (rooted) и Smart ADB – для разблокированных устройств.

*URL: https://4pda.to/

Проведение исследования с Nokia 5, проблема перевода в режим EDL

1



2

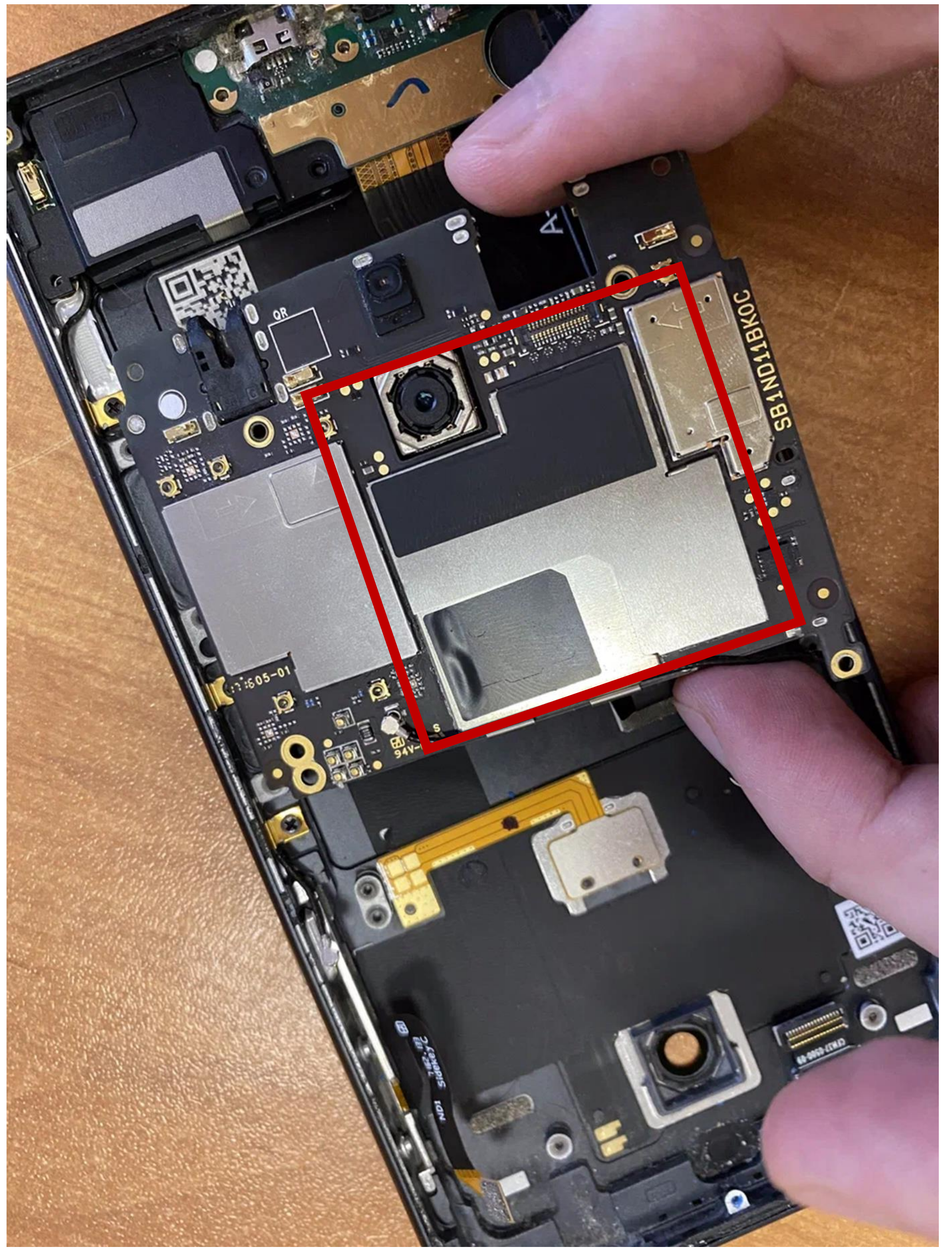
Контактные точки для перевода в режим EDL устройства Nokia TA-1053 на ОС Android 7.1

Мобильный телефон Nokia 5 в режиме EDL (mode 9008) не определился…

Возможные причины:

1. Отсутствие необходимого драйвера на компьютере.
2. Проблемы с интерфейсом подключения на компьютере или в мобильном устройстве.
3. Проблема с интерфейсным кабелем.
4. Внесение аппаратно-программных изменений в устройство производителем (например, изменение контактных площадок на системной плате и т.д.).

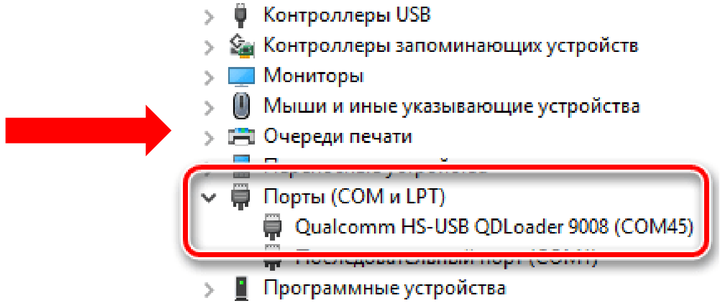
Проведение исследования с Nokia 5, проблема перевода в режим EDL

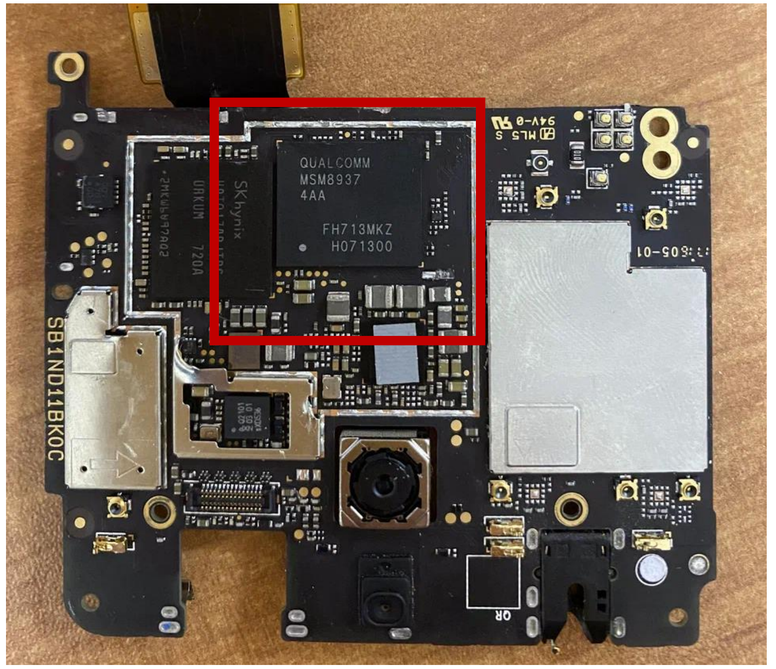


1

3

Замыкается контактная площадка № 2 на GND





2

Контактные точки для перевода в режим EDL устройства Nokia 5 на ОС Android 8.1 и выше

Спасибо за внимание!

Вопросы?

Докладчик:
старший эксперт Шавловский
Андрей Борисович

E-mail: ashavlovsky@yandex.ru