Для выполнения лабораторной использовано было: Bytecode viewer и android development studio.(а также winrar для того, чтобы получить dex файл)

Запустить получилось у меня на эмуляторе с конфигурацией

A screenshot of a black screen

AI-generated content may be incorrect.

Для начала поменяем расширение с apk на zip, после этого с помощью WinRar, посмотрел содержимое архива и перенес файл с расширением dex в Bytecode viewer. Там было потрачено довольно много времени для изучения структуры программы и примерного понимания, что как работает.

Первое, что можно отметить, что в программе в классе AesCrypt уже есть метод для дешифрования

A computer screen shot of a program code

AI-generated content may be incorrect.

Тут в этом классе можно посмотреть, что за алгоритм шифрования использовался и в целом его настройку (AES шифрование с использованием AES/CBC/PKCS7Padding).

A screen shot of a computer code

AI-generated content may be incorrect.

Тут используются стандартные пакеты java для шифрования. Видно, что в конструктор передается параметр, и то, где он используется дальше, говорит о том, что он похож на ключ-пароль, необходимый для настройки инстанса cipher. Посмотрим, где вызывается и инициализируется AesCrypt. В классе FilesEcryptor можно заметить, что там есть методы для получения файлов, которые нужно зашифровать и файлов, которые уже зашифрованы (рекурсивно). А также сами методы для де-шифрования файлов, который как раз создают наш класс AesCrypt и вызывают уже метод де-шифрования соответсвенно.

A computer screen shot of a program code

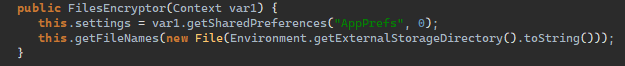
AI-generated content may be incorrect. A screen shot of a computer code

AI-generated content may be incorrect.

A screen shot of a computer program

AI-generated content may be incorrect.

Тут мы уже полуили пароль для дешифрования (jndlasf074hr)

Также из этого класса можно понять, где и какие файлы оно шифрует, оно 

Вызывает рекурсивную функцию и переадет туда в качестве начальной директории ExternalStorageDirectory. И там уже все файлы рекурсивно просматривает.

Интереса ради, посмотрел файл с константами A computer screen shot of a program code

AI-generated content may be incorrect.

Отсюда тоже можно много чего узнать, например пароль, файлы, которые это приложение шифрует, точнее их расширения. И другую информацию о клиенте, которую приложение использует и отправляет на удаленный сервер, используя TorService.

После проделанного анализа, мы знаем область файловой системы, где могут быть зашифрованы файлы, метод дешифрования и пароль. Теперь просто создадим приложение дешифратор (используя дисасссемблированный код).

В итоге для того, чтобы дешифровать файлы, достаточно просто установить Decryptor.apk. После Toast уведомления процесс дешифрования будет закончен. В логах можно посмотреть “какие файлы и их пути в хранилище” были дешифрованы.

Вот пример работы дешифровальщика:

До:

A screenshot of a computer program

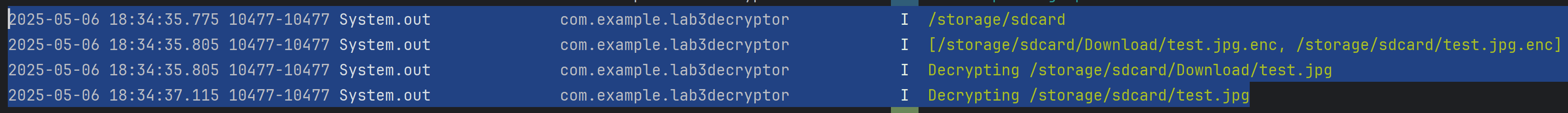
AI-generated content may be incorrect.

После:

A screenshot of a computer program

AI-generated content may be incorrect.

Содержимое логов:



Содержимое зашифрованного файла:

A green screen with white text

AI-generated content may be incorrect.