|  |  |  |
| --- | --- | --- |
|  | BAN CƠ YẾU CHÍNH PHỦ  “HỌC VIỆN KỸ THUẬT MẬT MÃ” | Mẫu 2 |

BÁO CÁO CHUYÊN ĐỀ SỐ 5.2, 5.3, 5.4, 5.5

“Xây dựng hệ thống phát hiện mã độc trực tuyến sử dụng học sâu”

NHIỆM VỤ: “Nghiên cứu và ứng dụng nền tảng học sâu để xây dựng hệ thống phát hiện mã độc trực tuyến”.

Mã số: 06/2022/CB.

Cơ quan chủ trì: Học viện Kỹ thuật Mật mã

Chủ nhiệm: ThS. Lê Đức Thuận

Hà Nội - 2023

|  |  |  |
| --- | --- | --- |
|  | BAN CƠ YẾU CHÍNH PHỦ  “HỌC VIỆN KỸ THUẬT MẬT MÃ” |  |

BÁO CÁO CHUYÊN ĐỀ SỐ 5.2, 5.3, 5.4, 5.5

“Xây dựng hệ thống phát hiện mã độc trực tuyến sử dụng học sâu”

NHIỆM VỤ: “Nghiên cứu và ứng dụng nền tảng học sâu để xây dựng hệ thống phát hiện mã độc trực tuyến”.

Mã số: 06/2022/CB.

Cơ quan chủ trì: Học viện Kỹ thuật Mật mã

Chủ nhiệm: ThS. Lê Đức Thuận

|  |  |
| --- | --- |
| **Người thực hiện chuyên đề** | **Cơ quan chủ trì** |
| *(Họ tên và chữ ký)* | *(Họ tên và chữ ký)* |

Hà Nội - 2023

MỤC LỤC

[MỤC LỤC 1](#_Toc129761850)

[DANH MỤC HÌNH ẢNH 2](#_Toc129761851)

[5.2 Thiết kế, lập trình xây dựng mô-đun tiền xử lý mã độc 3](#_Toc129761852)

[5.3 Thiết kế, lập trình xây dựng mô-đun trích chọn đặc trưng 5](#_Toc129761853)

[5.4 Thiết kế, lập trình xây dựng mô-đun huấn luyện 7](#_Toc129761854)

[5.5 Thiết kế, lập trình xây dựng mô-đun phát hiện mã độc 8](#_Toc129761855)

# DANH MỤC HÌNH ẢNH

[Hình 1 Mô-đun tiền xử lý mã độc 3](#_Toc129761841)

[Hình 2 Toàn bộ đặc trưng sau khi tiền xử lý 4](#_Toc129761842)

[Hình 3 Mô-đun trích chọn đặc trưng 5](#_Toc129761843)

[Hình 4 Dữ liệu sau khi trích chọn đặc trưng 6](#_Toc129761844)

[Hình 5 Mô-đun huấn luyện 7](#_Toc129761845)

[Hình 6 Mô-đun phát hiện mã độc 8](#_Toc129761846)

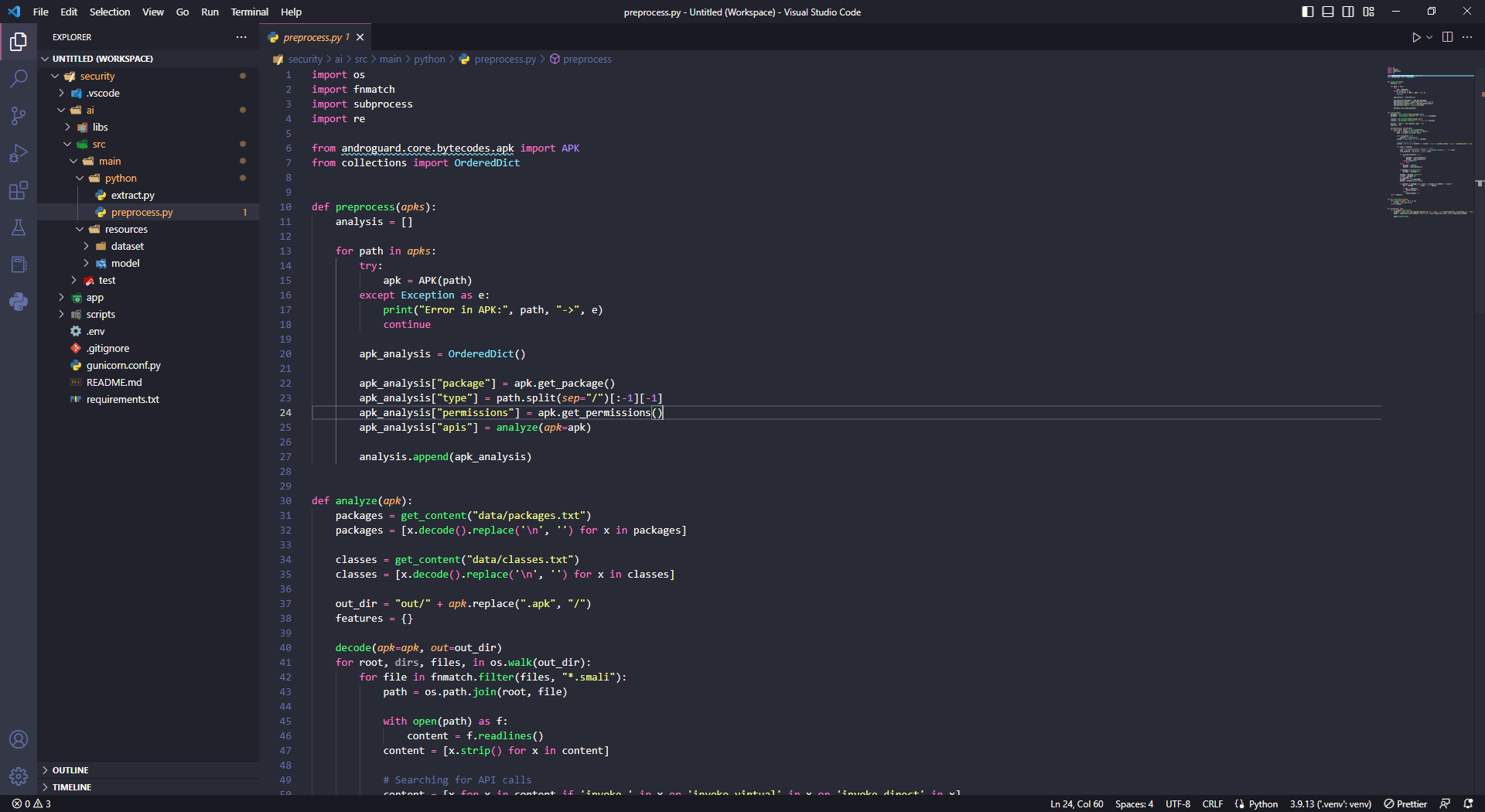
[Hình 7 Giao diện hiển thị danh sách ứng dụng đã cài đặt 9](#_Toc129761847)

[Hình 8 Giao diện hiển thị danh sách ứng dụng chưa cài đặt 10](#_Toc129761848)

[Hình 9 Giao diện hiển thị các thông tin chi tiết về ứng dụng 11](#_Toc129761849)

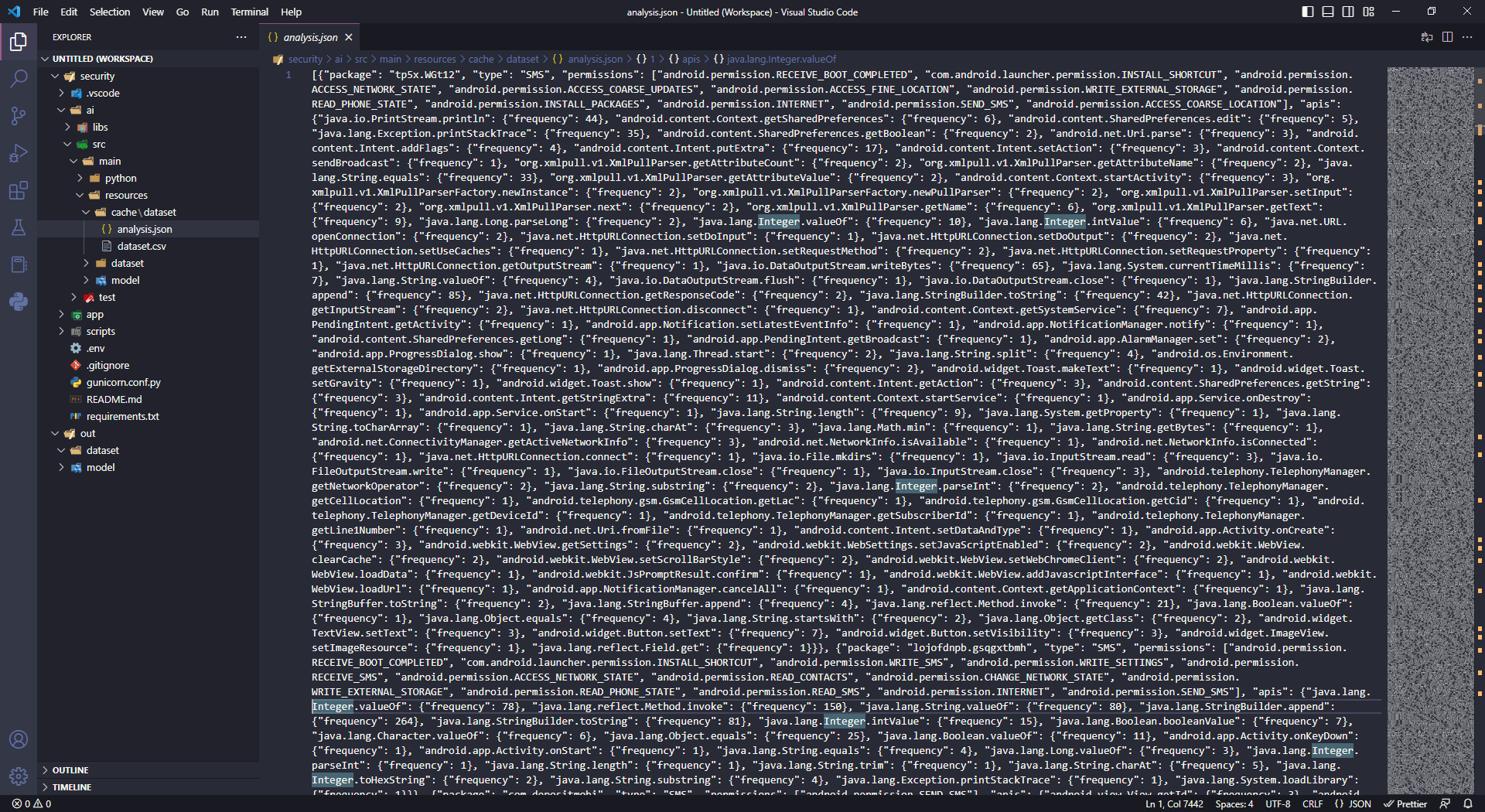
5.2 Thiết kế, lập trình xây dựng mô-đun tiền xử lý mã độc

Mô-đun tiền xử lý mã độc được xây dựng và đóng gói dưới dạng file *preprocess.py* và được đặt trong folder *ai/src/python.*



Hình 1 Mô-đun tiền xử lý mã độc

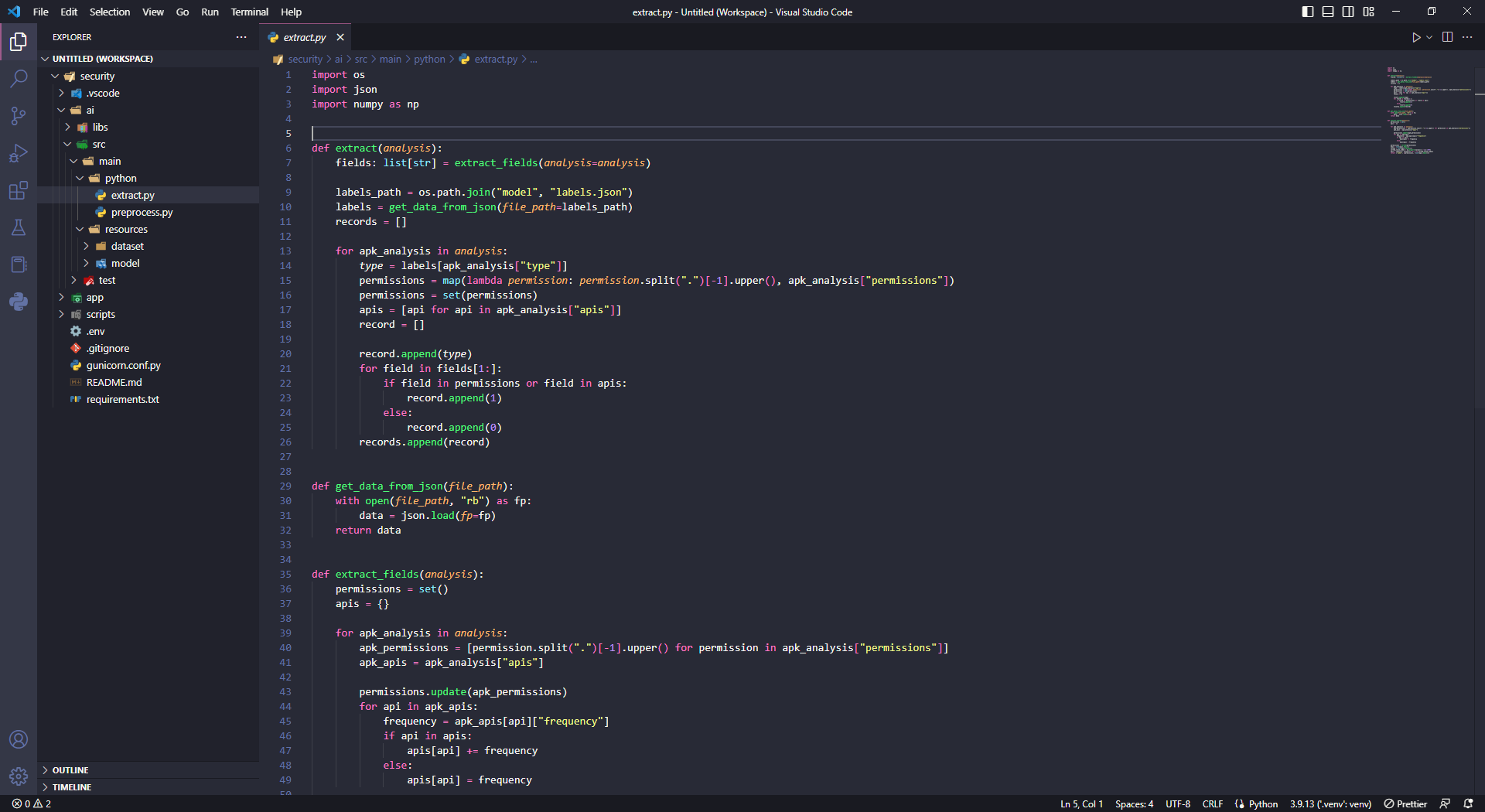
Mô-đun này có nhiệm vụ xử lý, trích xuất đặc trưng các mã độc đang được lưu trữ dưới dạng .apk thông qua lời gọi hàm preprocess() ở bên trong mô-đun. Kết quả đầu ra sau khi tiền xử lý là một đối tượng chứa toàn bộ các đặc trưng của các file mã độc được truyền từ tham số đầu vào được lưu vào file định dạng .json.



Hình 2 Toàn bộ đặc trưng sau khi tiền xử lý

5.3 Thiết kế, lập trình xây dựng mô-đun trích chọn đặc trưng

Mô-đun trích chọn đặc trưng được xây dựng và đóng gói dưới dạng file *extract.py* và được đặt trong folder *ai/src/python*.

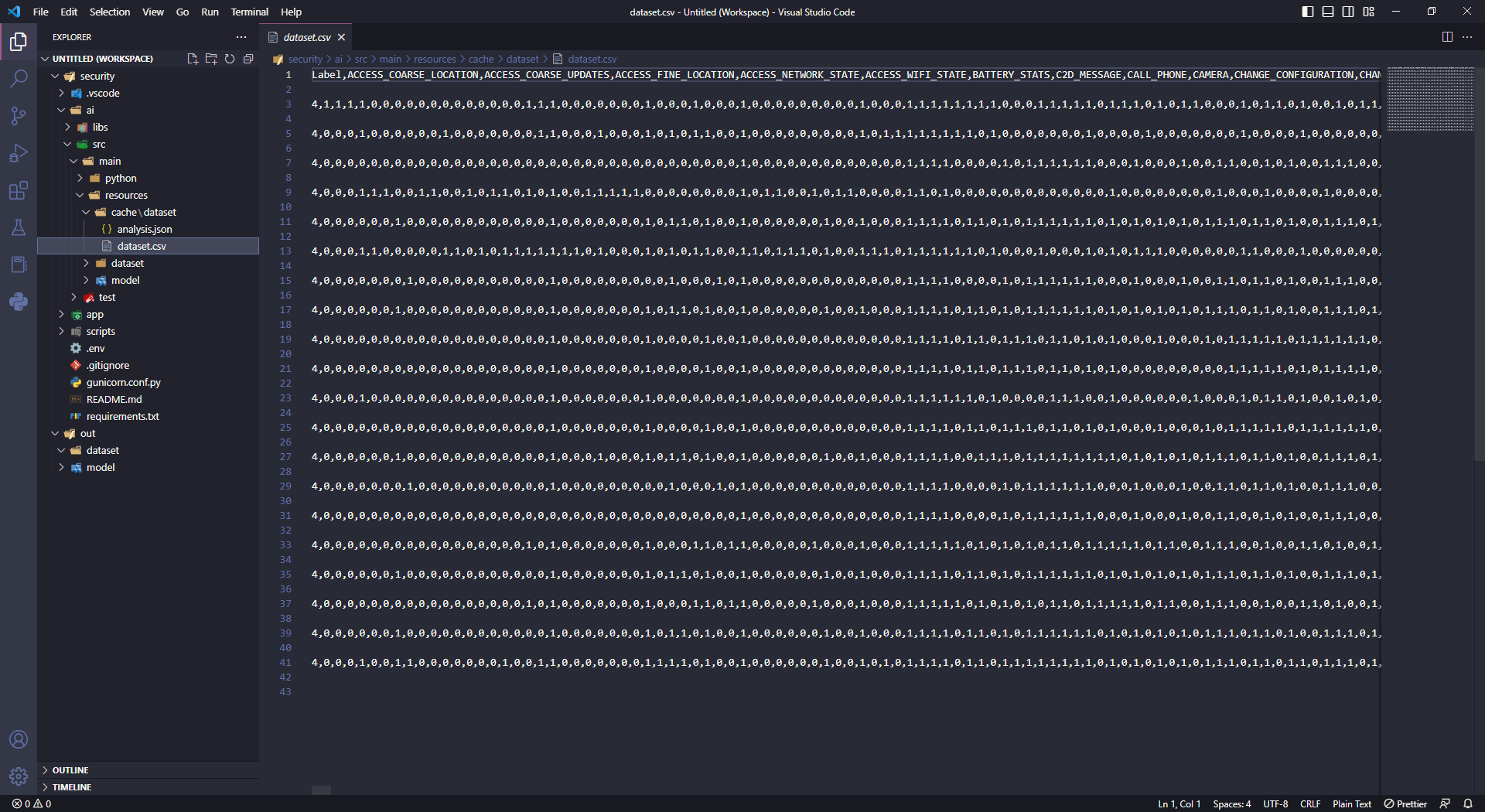


Hình 3 Mô-đun trích chọn đặc trưng

Mô-đun này có nhiệm vụ phân tích, trích chọn các đặc trưng của mã độc từ dữ liệu nhận được thông qua quá trình tiền xử lý. Quá trình trích chọn đặc trưng được thực dựa trên các tiêu chí bao gồm:

* Lấy tất cả các quyền mà ứng dụng yêu cầu có xuất hiện trong dữ liệu sau khi tiền xử lý;
* Lấy 1000 api có tần suất xuất hiện nhiều nhất mà các ứng dụng sử dụng, sắp xếp theo thứ tự giảm dần.

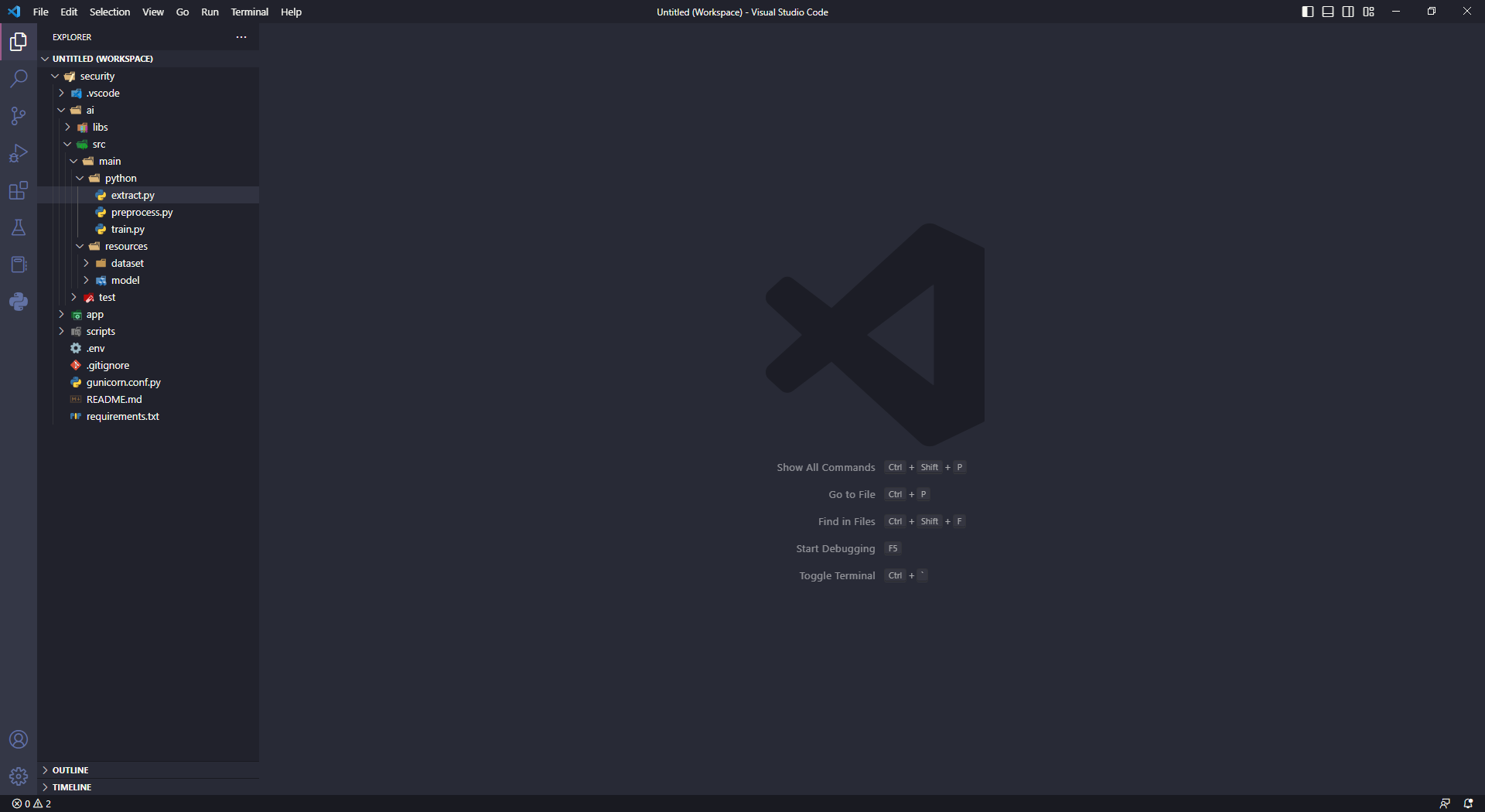
Kết quả đầu ra của mô-đun là dữ liệu đã được xử lý tưởng đối hoàn chỉnh, có thể dùng trong huấn luyện mô hình được lưu vào file định dạng .csv.



Hình 4 Dữ liệu sau khi trích chọn đặc trưng

5.4 Thiết kế, lập trình xây dựng mô-đun huấn luyện

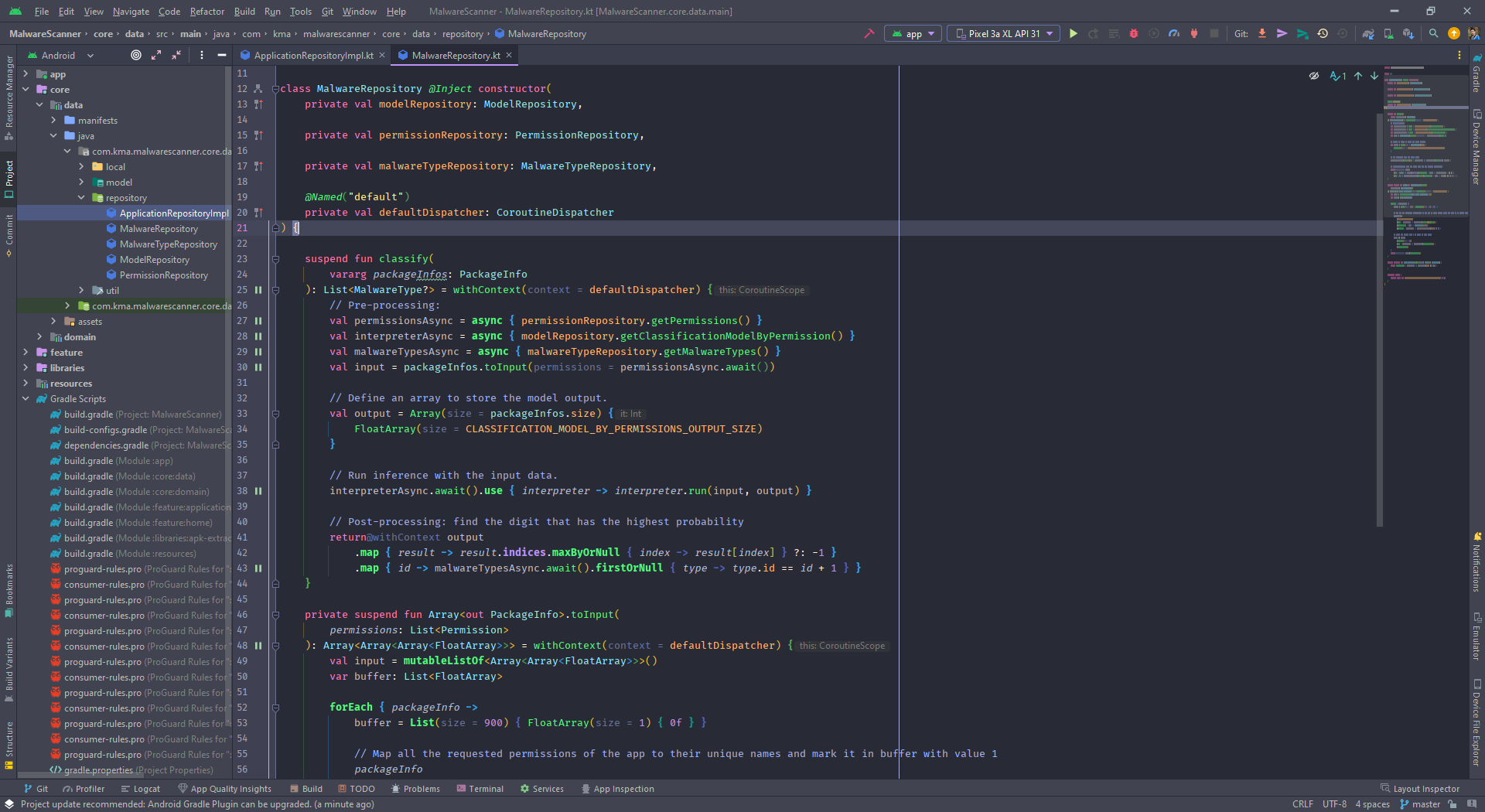
Mô-đun huấn luyện được xây dựng và đóng gói dưới dạng file *train.py* và được đặt trong folder *ai/src/python*.



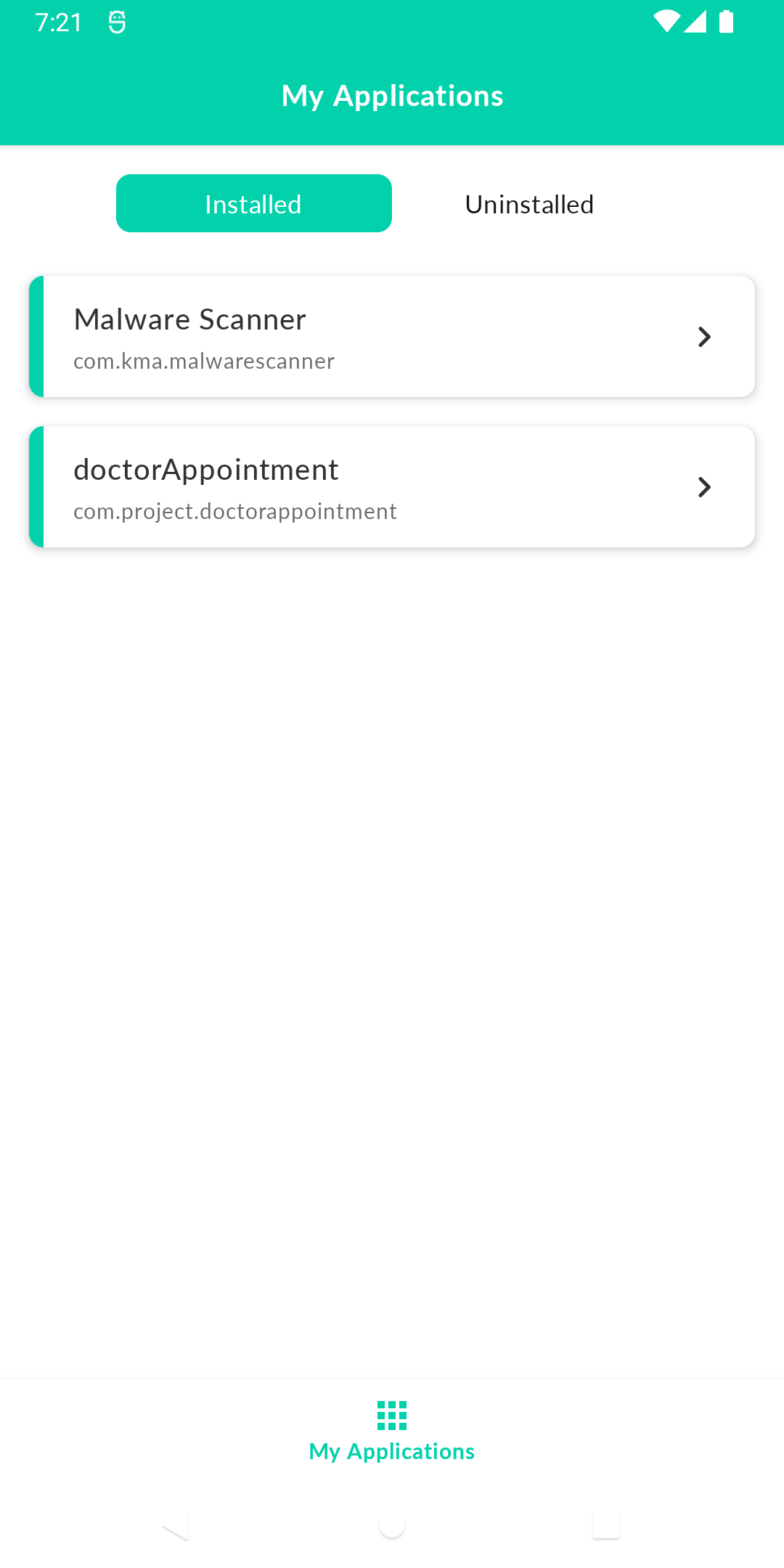
Hình 5 Mô-đun huấn luyện

5.5 Thiết kế, lập trình xây dựng mô-đun phát hiện mã độc

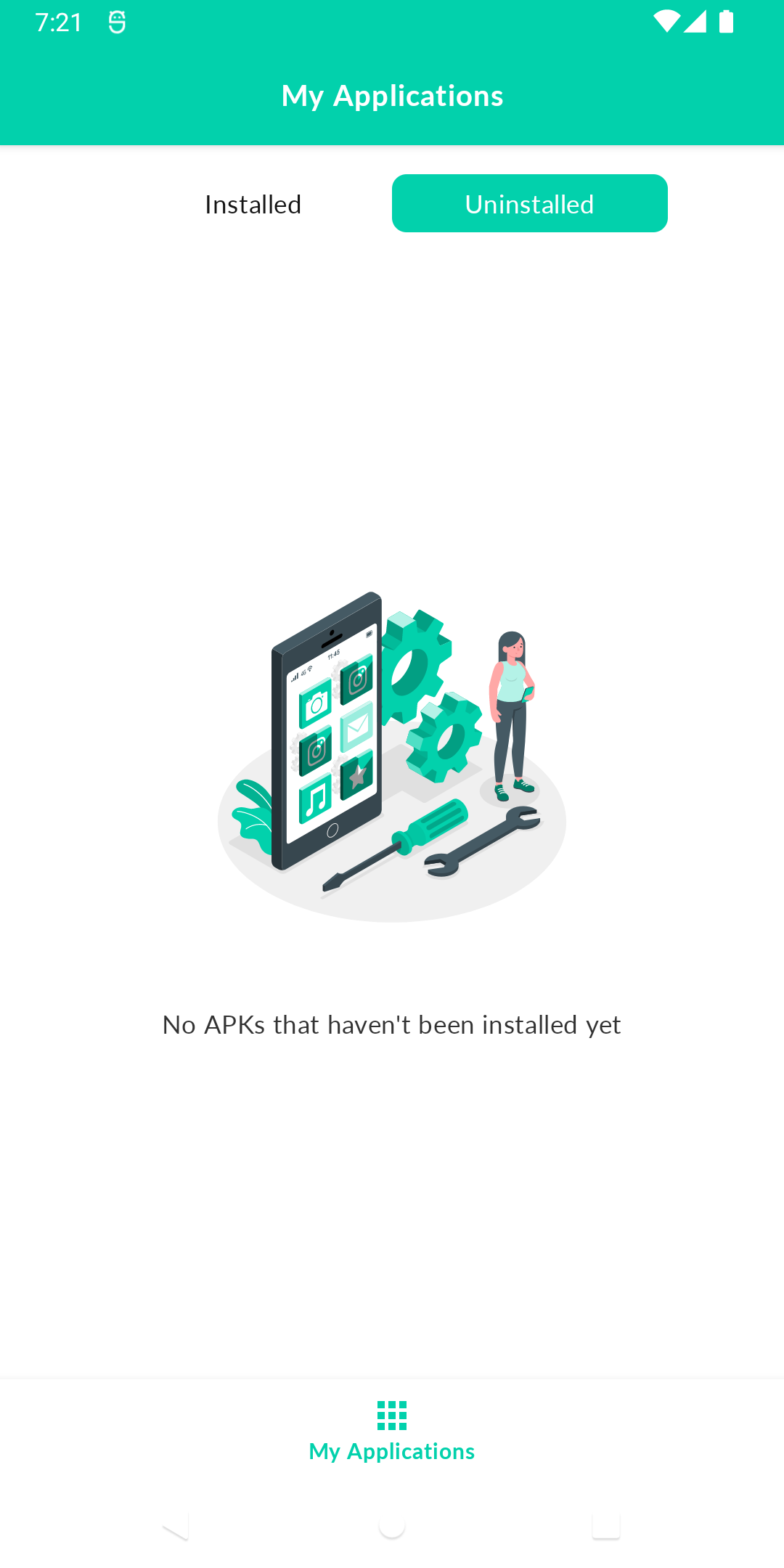
Mô-đun phát hiện mã độc được phát triển có thể chạy trực tiếp trên thiết bị Android dựa trên mô hình đã được huấn luyện và được sử dụng thông qua thư viện TensorFlow Lite.



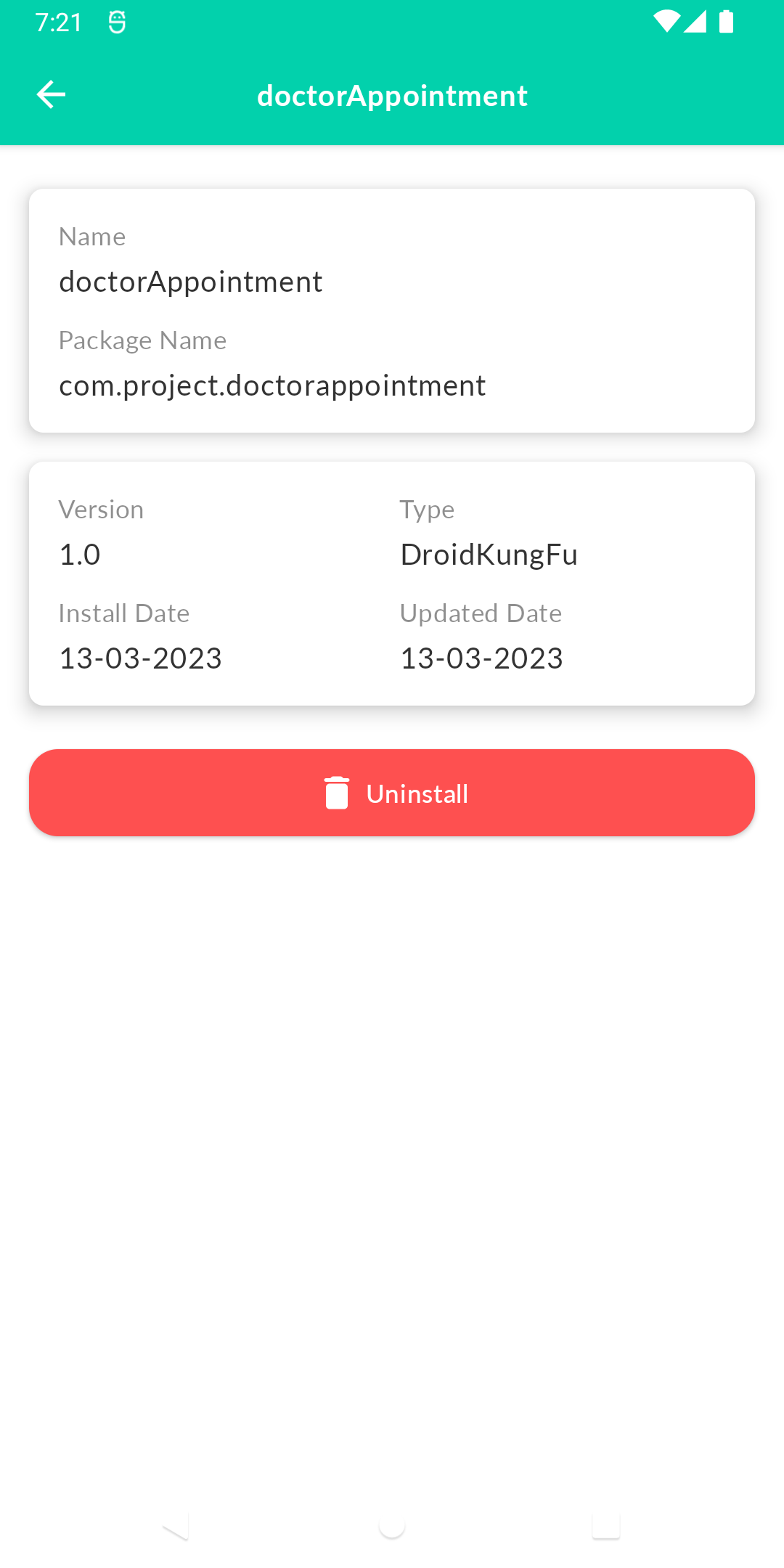
Hình 6 Mô-đun phát hiện mã độc



Hình 7 Giao diện hiển thị danh sách ứng dụng đã cài đặt



Hình 8 Giao diện hiển thị danh sách ứng dụng chưa cài đặt



Hình 9 Giao diện hiển thị các thông tin chi tiết về ứng dụng