

5조 프로젝트 중간 발표

-Windows Sentinel-

2416110232 김기원

2416110242 안지훈

2416110252 정재윤

Windows Sentinel 프로젝트 개요

목적

Windows 시스템의 보안 상태

모니터링, 관리

보안 프로그램 복구

주요 기능

- 설치된 프로그램 관리
- 시스템 변경 이력 추적
- 보안 로그 모니터링
- 보안 설정 관리
- 보안 프로그램 복구 기능

기술 스택

- C#
- WPF (Windows Presentation Foundation)
- XAML
- Windows 관리자 권한 관리 (Manifest)
- Segoe MDL2 Assets 폰트 활용 (아이콘 생성)

주요 기술 구현

관리자 권한 구현

애플리케이션
매니페스트 파일을
통한 관리자 권한 요청

Windows 보안 기능
접근을 위한 필수 권한
설정

사용자 계정
컨트롤(UAC) 통합

UI/UX 개선

Windows 네이티브
디자인 시스템 적용

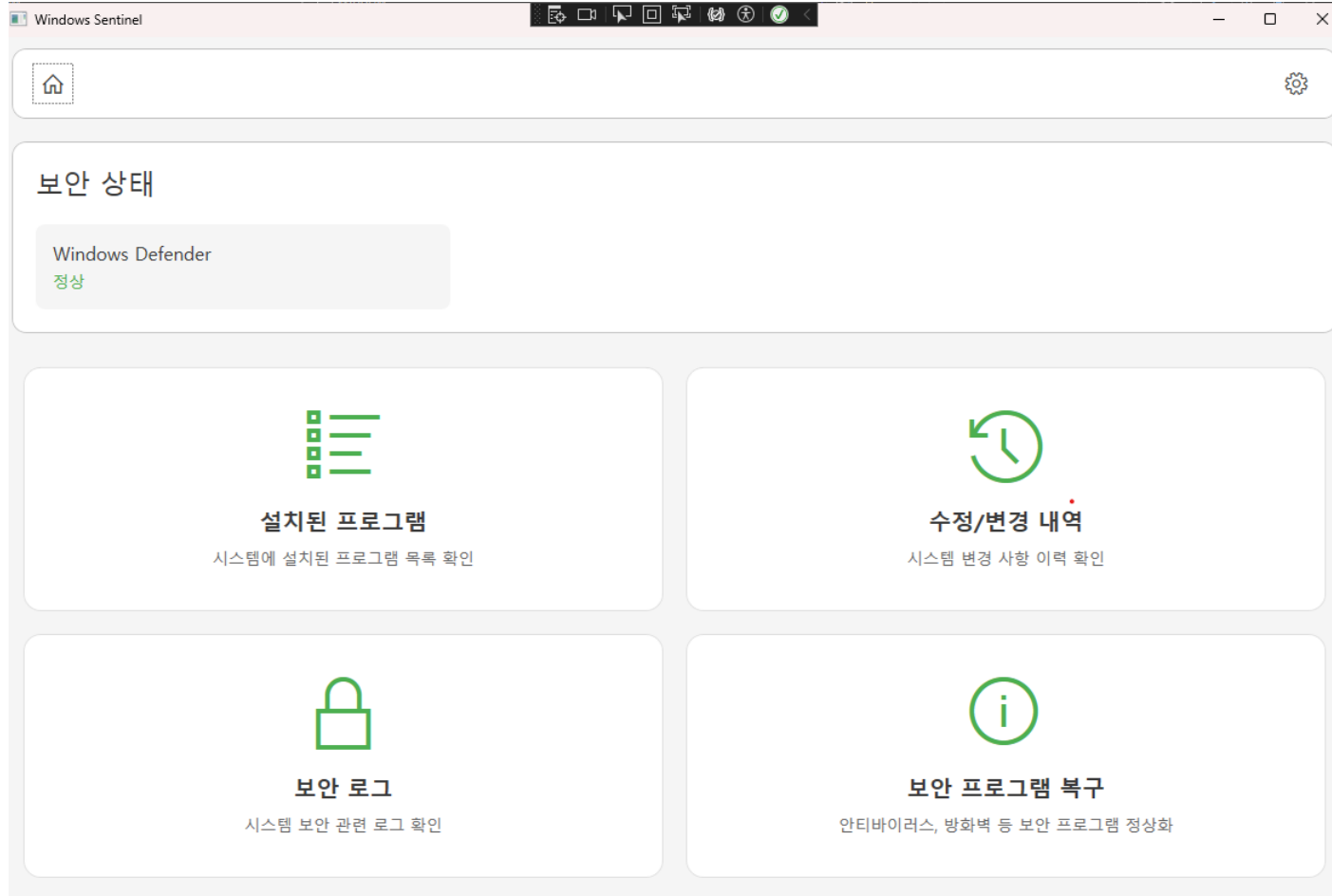
Segoe MDL2 Assets
폰트를 활용한 아이콘
구현

시스템 리소스 효율적
사용

Windows 디자인
가이드라인 준수

일관된 시각적 경험
제공

개발 현황 - 메인 UI



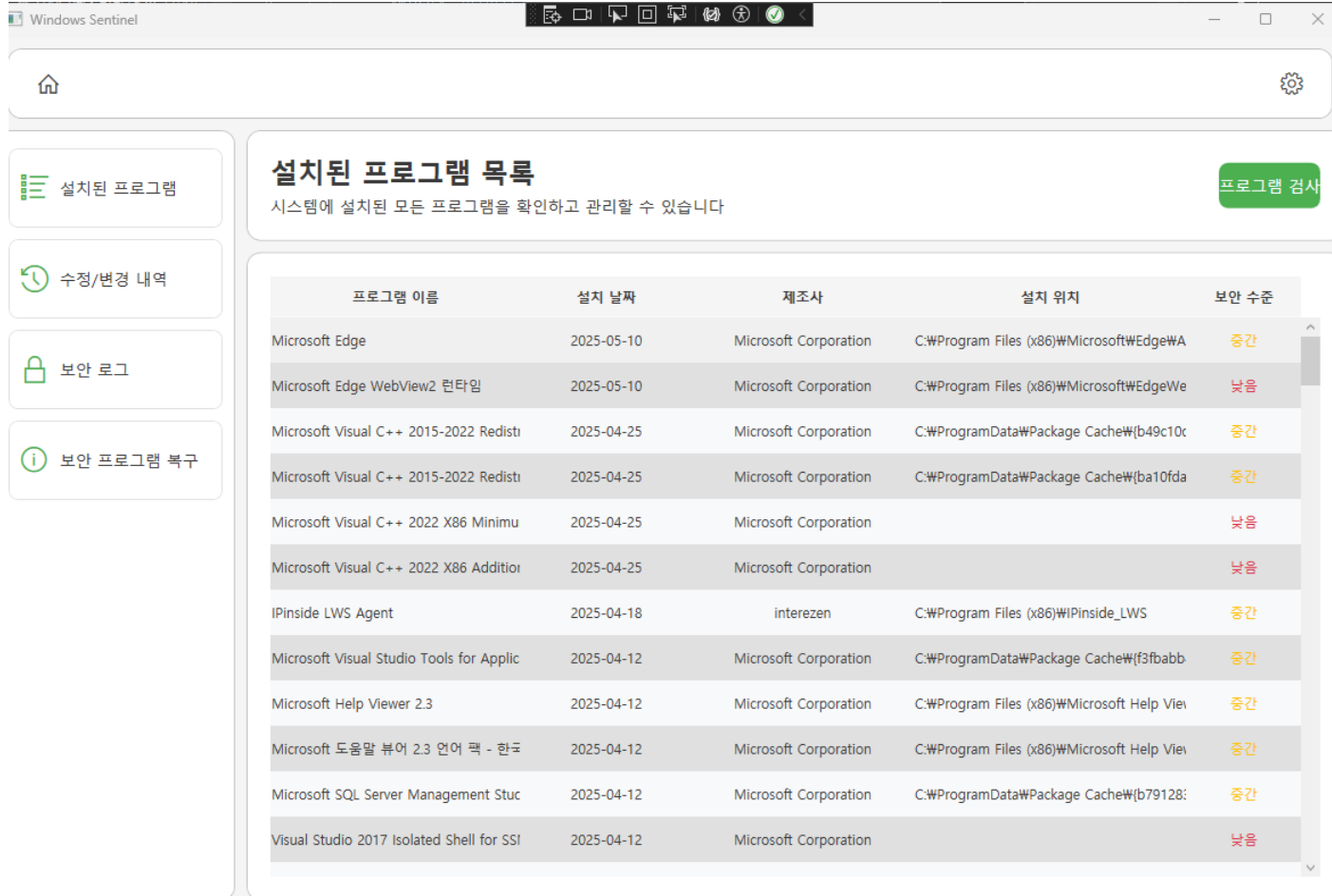
구현된 기능

- 메인 대시보드 UI 구현
- 페이지 네비게이션 시스템 구축

다음 섹션들의 기본 구조 구현

- 설치된 프로그램 관리
- 수정/변경 이력 관리
- 로그 모니터링
- 보안 프로그램 복구 (미구현)

개발 현황 - 설치 프로그램 검사



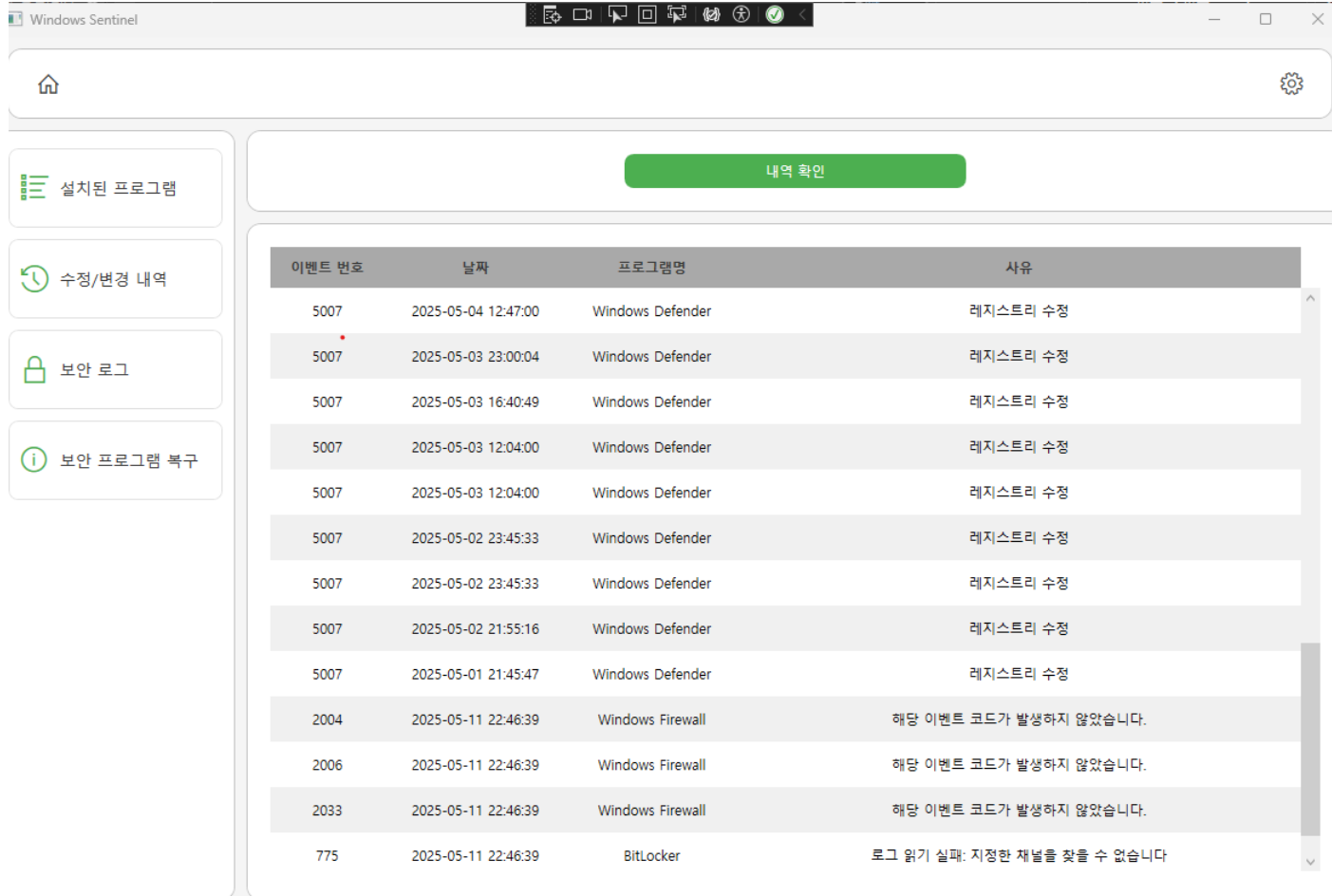
The screenshot shows the Windows Sentinel application window. On the left is a sidebar with navigation icons and labels: '설치된 프로그램' (Installed Programs), '수정/변경 내역' (Modification History), '보안 로그' (Security Log), and '보안 프로그램 복구' (Recover Security Programs). The main area is titled '설치된 프로그램 목록' (Installed Programs List) with a subtitle '시스템에 설치된 모든 프로그램을 확인하고 관리할 수 있습니다' (You can check and manage all programs installed on the system). A green button labeled '프로그램 검사' (Check Programs) is in the top right. Below is a table listing installed programs with columns for Name, Date, Manufacturer, Location, and Security Status.

프로그램 이름	설치 날짜	제조사	설치 위치	보안 수준
Microsoft Edge	2025-05-10	Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\A	중간
Microsoft Edge WebView2 런타임	2025-05-10	Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeWe	낮음
Microsoft Visual C++ 2015-2022 Redist	2025-04-25	Microsoft Corporation	C:\ProgramData\Package Cache\{b49c10c	중간
Microsoft Visual C++ 2015-2022 Redist	2025-04-25	Microsoft Corporation	C:\ProgramData\Package Cache\{ba10fda	중간
Microsoft Visual C++ 2022 X86 Minimu	2025-04-25	Microsoft Corporation		낮음
Microsoft Visual C++ 2022 X86 Addition	2025-04-25	Microsoft Corporation		낮음
IPinside LWS Agent	2025-04-18	interezen	C:\Program Files (x86)\IPinside_LWS	중간
Microsoft Visual Studio Tools for Applic	2025-04-12	Microsoft Corporation	C:\ProgramData\Package Cache\{f3fbabb	중간
Microsoft Help Viewer 2.3	2025-04-12	Microsoft Corporation	C:\Program Files (x86)\Microsoft Help Vie	중간
Microsoft 도움말 뷰어 2.3 언어 팩 - 한국	2025-04-12	Microsoft Corporation	C:\Program Files (x86)\Microsoft Help Vie	중간
Microsoft SQL Server Management Stuc	2025-04-12	Microsoft Corporation	C:\ProgramData\Package Cache\{b79128:	중간
Visual Studio 2017 Isolated Shell for SSI	2025-04-12	Microsoft Corporation		낮음

기능 개요

- 시스템에 설치된 모든 프로그램을 검사하고 보안 수준을 평가하는 기능
- 프로그램의 상세 정보와 보안 상태를 한눈에 확인 가능
- 검사 프로세스
- "프로그램 검사" 버튼 클릭
- 로딩 오버레이 표시 ("검사 중...")
- 검사 완료 후 결과 테이블에 표시
- 보안 수준에 따른 색상 구분 표시

개발 현황 - 보안 수정/변경 내역



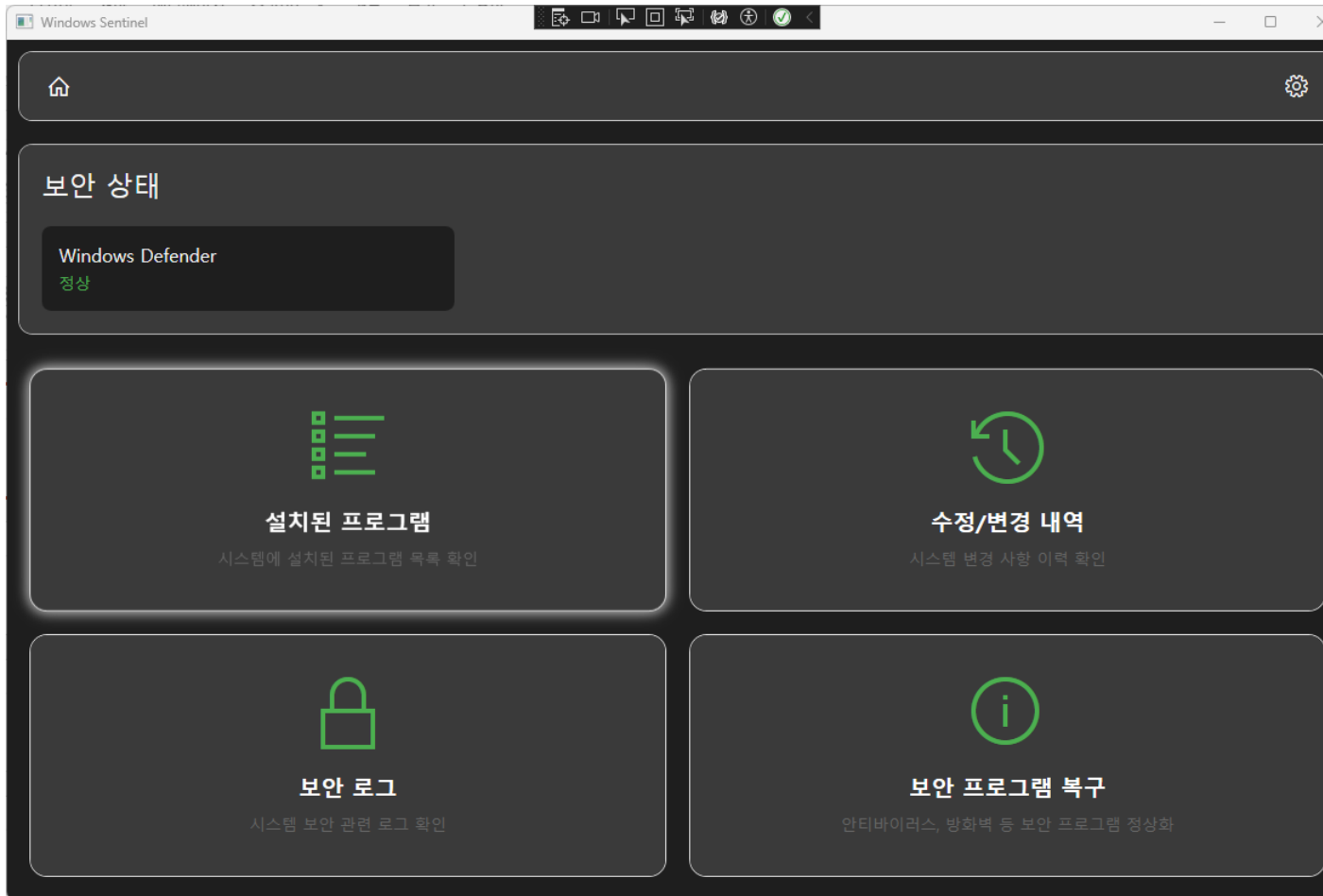
The screenshot shows the Windows Sentinel application window. On the left is a sidebar with navigation icons and labels: '설치된 프로그램' (Installed Programs), '수정/변경 내역' (Modification/Change History), '보안 로그' (Security Log), and '보안 프로그램 복구' (Recovery of Security Programs). The main area has a green '내역 확인' (Check History) button. Below it is a table of events.

이벤트 번호	날짜	프로그램명	사유
5007	2025-05-04 12:47:00	Windows Defender	레지스트리 수정
5007	2025-05-03 23:00:04	Windows Defender	레지스트리 수정
5007	2025-05-03 16:40:49	Windows Defender	레지스트리 수정
5007	2025-05-03 12:04:00	Windows Defender	레지스트리 수정
5007	2025-05-03 12:04:00	Windows Defender	레지스트리 수정
5007	2025-05-02 23:45:33	Windows Defender	레지스트리 수정
5007	2025-05-02 23:45:33	Windows Defender	레지스트리 수정
5007	2025-05-02 21:55:16	Windows Defender	레지스트리 수정
5007	2025-05-01 21:45:47	Windows Defender	레지스트리 수정
2004	2025-05-11 22:46:39	Windows Firewall	해당 이벤트 코드가 발생하지 않았습니다.
2006	2025-05-11 22:46:39	Windows Firewall	해당 이벤트 코드가 발생하지 않았습니다.
2033	2025-05-11 22:46:39	Windows Firewall	해당 이벤트 코드가 발생하지 않았습니다.
775	2025-05-11 22:46:39	BitLocker	로그 읽기 실패: 지정된 재료를 찾을 수 없습니다

기능 개요

- 시스템의 보안 관련 변경 사항을 추적하고 기록하는 기능
- 프로그램 설치, 제거, 수정 등 보안에 영향을 미치는 모든 변경사항을 모니터링
- 기본적인 변경 내역 표시
- 보안 수준 평가 시스템
- 실시간 검사 기능
- 직관적인 UI/UX 구현

개선 예정 사항 - 메인 UI



현재 다소 아쉬운 다크 모드

- 다크 모드 개선
- 시스템 테마 연동
- 눈의 피로도 감소
- 애니메이션 효과 추가
- 부드러운 전환 효과
- 로딩 애니메이션 개선
- 사용자 피드백 강화

개선 예정 사항 - 설치 프로그램 검사

- 심층 보안 분석
- 프로그램 서명 검증
- 취약점 데이터베이스 연동
- 악성코드 패턴 검사
- 필터링 및 정렬
- 보안 수준별 필터링
- 설치 날짜순 정렬
- 제조사별 그룹화
- 검색 기능 강화
- 위험도 계산
- 가중치 기반 평가
- 다중 요소 통합 분석
- 동적 위험도 조정
- 트렌드 분석

개선 예정 사항 - 보안 수정/변경 내역

- 개선 예정 사항
- 변경 내역 필터링 기능
- 상세 변경 내용 표시
- 변경 이력 백업 기능
- 실시간 알림 시스템

개선 예정 사항 - 보안 프로그램 복구

• 복구 기능 설계

- 자동 복구 시스템
- Windows Defender 자동 복구
- 방화벽 설정 복구
- 보안 업데이트 자동 설치
- 시스템 보안 정책 복구

• 수동 복구 옵션

- 선택적 복구 기능
- 단계별 복구 프로세스
- 복구 이력 관리
- 롤백 기능

개선 예정 사항 - 기타

- 프로그램 대표 아이콘 디자인
- 설정에서 사용자가 선택할 수 있는 요소 추가
 - 사용자 매뉴얼, 문제 해결 가이드, 폰트 크기, 언어 선택 등
- 개발자 지원
 - 디버깅 지원, 오류 추적

THANK YOU!
감사합니다!

FeedBack Us
Github

<https://github.com/gkwp1216/WindowsSentinel>

E-mail
rabbia1216@gmail.com
