파이널 프로젝트 결과물-노현석

앱 링크 : https://ai.studio/apps/drive/12xaJGI-wjAyazaL6DEARR3A4IY2kd2D8

github : https://github.com/oasisc1205/aiweb.git

👥 팀 정보

- **팀명:** expuser group (사용자 경험 기반팀)
- **팀원 역할:**
  - PM/기획 및 발표 담당 (프로젝트 총괄 책임 영역)
  - UI/UX 및 디자인 담당 (디자인 전체 구현)
  - 백엔드 (비즈니스 로직 및 API 구현)
  - 앱개발 (네이티브 앱개발 구현)
  - 인프라 (서버 및 인프라 구성, CI/CD 구현)
  - 데이터베이스 (데이터베이스 설계 및 구현)
  - 노현석 (PM / 발표 담당 / UI-UX / 디자인 / 백엔드 / 앱개발 / 인프라, 데이터베이스)

❓ 문제 정의

- **우리가 해결하려는 문제는?:**
  - **심리적으로 불안하고 충격 상태**에 있으며,
  - 확보한 **외도 증거 자료가 유실되거나 삭제될 위험**을 걱정하고,
  - **법적 절차(상간소송, 이혼소송 등)에 대한 지식이 부족**해 어떻게 대처해야 할지 막막하다.

  현재 시장에는 이러한 위기 상황에서 **증거를 안전하게 보존**하고 **법률적 대응을 체계적으로 안내**해주는 신뢰할 수 있는 앱이 부재하다.

  “외도 증거를 안전하게 관리하고, 법적 대응을 위한 단계별 가이드를 제공함으로써 사용자의 심리적·재정적 피해를 최소화” 하는 것을 목표로 한다.

- **왜 지금 이 문제를 해결해야 하나?:**
  - 외도 관련 법률 분쟁 증가 추세 : 디지털 기기의 발달로 외도 증거(카톡, 사진, 위치 기록 등)가 쉽게 확보되지만, 동시에 삭제·유출 위험도 증가하고 있다.
  - 법률 및 심리적 지원의 정보 비대칭 : 일반 사용자는 외도 관련 법적 절차나 대처 방법을 알기 어렵고, 검색으로 얻는 정보는 단편적이며 신뢰성이 낮다.
  - 프라이버시 보호의 필요성 확대 : 배우자나 타인에게 앱 사용 사실이 노출될 경우, 사용자는 2차 피해를 입을 수 있다. 따라서 **보안성과 위장 기능**을 갖춘 안전한 솔루션이 시급하다.

- **대상(사용자/고객)은 누구인가?:**
  - 핵심 사용자 : 배우자의 외도를 인지한 후, 증거를 확보했지만 보관·활용 방법을 몰라 불안한 일반인
  - 연령대 : 20대 후반 ~ 50대
  - 성별 : 무관함

💡 해결 아이디어

- **프로젝트 이름 :** 프로젝트 페이스(당신의 불안한 현실에, 안전한 믿음을 더하다.)
- **한 줄 요약:** 배우자의 외도 사실을 인지한 사용자가 **증거를 안전하게 보관하고**, **법적 대응 절차를 단계별로 안내받으며**, **긴급 상황에서도 자신의 프라이버시를 지킬 수 있는** 보안 중심의 위기 대응 앱.
- **주요 기능(bullet point):**

구분	기능명	설명
🔒 **증거 보존 및 관리**	**이중화 백업 시스템**	사진, 동영상, 녹음 등 외도 증거를 AES-256 암호화하여 스마트폰 내부 저장소와 클라우드에 동시 저장. 네트워크 불안 시 자동 동기화.
📚 **법률 절차 가이드**	**단계별 법률 대응 가이드**	외도 인지 → 증거 수집 → 법률 상담 → 소송 준비 및 진행까지, 각 단계별로 필요한 서류와 절차를 상세 안내.
🕵️ **프라이버시 보호**	**앱 위장 기능**	앱 아이콘과 화면을 '날씨 앱' 등으로 위장하여 타인에게 노출되지 않도록 보호. 비밀 코드로만 원래 화면 진입 가능.

구분	기능명	설명
🔐 **보안 접근 제어**	**앱 잠금 기능**	PIN, 패턴, 지문, Face ID 등 다양한 인증 방식으로 앱 접근을 제한하고 자동 잠금 기능 제공.
💬 **전문가 연결**	**법률/탐정 광고 연동**	검증된 법률 전문가 및 탐정의 광고를 안전하게 노출하여, 사용자가 즉시 상담 및 의뢰 가능.

🔎 아이디어 구체화

1) 사용자 페르소나

- 핵심 사용자 : 배우자의 외도를 인지한 후, 증거를 확보했지만 보관·활용 방법을 몰라 불안한 일반인
- 주요 페르소나 : 김지영 (30대 후반, 회사원) — 외도 사실을 알게 된 후 증거 유실과 법적 절차에 대한 불안을 겪는 인물
- 연령대 : 20대 후반 ~ 50대
- 성별 : 무관 (다만 여성 비율이 높을 것으로 예상)
- 지역 : 대한민국
- 특징 : 외도 증거를 확보 중이거나 확보 계획 중, 법적 대응을 고려하지만 절차를 모름, 프라이버시와 보안을 가장 중요하게 생각함

2) 사용자 시나리오

- 외도 증거 확보 및 안전 보관

- 상황 : 김지영(38세)은 배우자의 외도 정황을 발견하고, 휴대폰으로 대화 캡처 및 사진을 확보했다.

- 행동 :

1. 앱 *페이스(FAITH)* 를 실행한다.
2. '증거 보관함' 메뉴에서 캡처 이미지를 업로드한다.
3. 앱은 파일을 즉시 **AES-256 암호화** 후, **로컬 + 클라우드에 이중 백업**한다.
4. 업로드 완료 후, "안전하게 보관되었습니다"라는 알림이 표시된다.

- 결과: 김지영은 배우자가 스마트폰을 보더라도, 앱이 위장되어 노출되지 않으며, 증거 자료는 안전하게 보존된다.

- 법적 대응 가이드 확인

- **상황**: 김지영은 증거를 모았지만, 이후 어떤 법적 절차를 밟아야 할지 몰라 막막하다.

- **행동**:

  1. '법률 가이드' 메뉴에서 "상간소송 절차"를 선택한다.
  2. 앱은 단계별 절차(소장 접수 → 증거 제출 → 재판 → 판결)를 시각적으로 안내한다.
  3. 각 단계마다 필요한 서류와 주의사항을 함께 보여준다.

- **결과**: 사용자는 스스로 상황을 파악하고, 불안감 대신 **명확한 행동 계획**을 세울 수 있다.

- 긴급 상황에서의 앱 위장

- **상황**: 배우자가 휴대폰을 보여달라고 요구하는 긴급 상황.

- **행동**:

  1. 김지영은 미리 설정해둔 "위장 모드"를 활성화한다.
  2. 앱 아이콘이 '날씨 앱'으로 변경되고, 실행 시 날씨 정보 화면이 표시된다.
  3. 비밀 코드 입력 시에만 본래의 증거 관리 화면으로 복귀할 수 있다.

- **결과**: 배우자는 앱의 존재를 눈치채지 못하고, **개인 정보와 증거 자료가 완벽히 보호된다.**

3) 예상 효과

구분	효과	설명
🔒 **보안 강화**	증거 유실 및 유출 방지	로컬·클라우드 이중화 저장과 암호화로 데이터 손실률 0% 목표.
🧠 **심리 안정**	불안감 완화 및 통제감 회복	명확한 법률 가이드와 안전한 보관 시스템으로 사용자의 심리적 안정감 제공.
⚖️ **법적 준비도 향상**	법률 절차 이해 및 준비도 향상	체계적인 단계별 가이드를 통해 변호사 상담 전에도 대응 전략 수립 가능.
👁️ **프라이버시 보호**	배우자 등 제3자로부터의 노출 방지	위장 모드 및 앱 잠금으로 외부 노출 위험 최소화.
💵 **경제적 가치 창출**	전문가 광고 수익 모델	법률 전문가 및 탐정 광고 연동으로 수익 확보, 사용자에게 실질적 연결 제공.

🛠️ 기술 스택 (예상)

- 클라이언트 (모바일 앱)

- **프레임워크**: **Flutter** (단일 코드베이스, 보안·UI 일관성, 빠른 MVP에 유리)

  대안: React Native (기존 JS/웹 인력 재사용 시)

- **로컬 보안 저장소**

  iOS: Keychain + File Protection (NSFileProtectionComplete)

  Android: EncryptedFile/EncryptedSharedPreferences + **Android Keystore**

  공통: **SQLCipher**(옵션, 메타데이터까지 암호화), 앱 내 캐시 최소화

- **암호화**

  대칭: **AES-256-GCM**

  키 파생: **Argon2id**(또는 PBKDF2-HMAC-SHA256, 파라미터 강화)

  전송: **TLS 1.3**, HSTS, 인증서 고정(핀닝) 옵션

- **위장/보안 UX**

  아이콘/이름 위장:

  - iOS: alternate app icons
  - Android: activity alias로 런처 아이콘 스위칭

  가짜 첫 화면(날씨/계산기): Feature flag로 온·오프

  스크린샷 방지: Android FLAG_SECURE, iOS UISecure

  생체 인증: iOS Face ID / Android BiometricPrompt

- **미디어 처리**

  EXIF/메타데이터 제거, 썸네일 로컬 생성(메모리 격리)

- **알림**

  민감정보 비노출, **silent push** 위주, OS 설정 가이드

- 백엔드 / API
  - **런타임/프레임워크**: **Node.js + NestJS** (의존성 주입/모듈화, 테스트 용이)

    대안: Python **FastAPI**(ML/콘텐츠 파이프라인 친화)

  - **API 설계**: REST(핵심) + 추후 gRPC(업로드 파이프라인), OpenAPI 스키마 관리
  - **인증/인가**

    OIDC(Auth0/Cognito/Keycloak) + JWT(짧은 수명) / refresh token 회전

첨부 다운로드는 **서명된 URL(단명)**, IP/UA 바인딩 옵션

관리자 콘솔은 RBAC + IP 제한

- **저장소 / 데이터**
  - **객체 스토리지(증거 원본)**: **AWS S3(ap-northeast-2)** + **SSE-KMS**

    버전닝/무결성 체크(ETag, S3 Object Lock(Compliance/WORM 옵션))
  - **DB(메타데이터/가이드)**: **PostgreSQL** (RLS 적용, pgcrypto 선택적)
  - **캐시/큐**: **Redis**(세션/레이트리밋) / **SQS**(비동기 업로드 재시도)
  - **검색(가이드/도움말)**: **OpenSearch/Algolia**(비민감 텍스트만)
- **인프라 / DevOps**
  - **클라우드**: **AWS 서울 리전** (또는 NCP 선택 가능)
  - **컨테이너**: EKS(표준) 또는 **ECS Fargate**(운영 단순화, MVP 권장)
  - **CDN**: 개인 데이터는 CDN 미사용 원칙. 정적 가이드만 **CloudFront**
  - **CI/CD**: **GitHub Actions** → IaC 배포
  - **IaC**: **Terraform**(+ Terragrunt), 환경 분리(dev/stage/prod)
  - **비밀관리**: **AWS Secrets Manager** / Parameter Store
- 보안 / 컴플라이언스
  - **키 관리**: KMS CMK, 키 회전 정책, BYOK 검토
  - **접근제어/감사**: IAM 최소권한, CloudTrail, S3 Access Logs
  - **민감정보 처리 원칙**: 서버 로그에 PII/파일 경로/해시 미기록
  - **DLP**: 업로드 시 MIME·헤더 검증, 안티바이러스(Lambda + ClamAV)
  - **법규**: **개인정보보호법(PIPA)** 준수, 데이터 국내 리전 저장 원칙, 파기 정책(지침 포함)
  - **침투테스트**: 릴리즈 전 외부 모의해킹 / 정기 SAST/DAST
- **관제 / 모니터링 / 품질**
  - **로그/모니터링**: CloudWatch + **OpenTelemetry**(Trace), 구조화 로그(JSON)
  - **APM**: AWS X-Ray / Datadog(대안)
  - **크래시/이슈**: **Sentry**(모바일/서버), Privacy Mode
  - **분석**: **PostHog(자가호스팅)**(개인정보 비수집 설정), 이벤트 최소화

- 콘텐츠 / 운영 도구
  - **가이드 CMS**: **Headless CMS(Strapi)**(자가호스팅) 또는 Contentful(비민감)
  - **번역/현지화**: i18n(ko 우선), 앱 스트링 키 암호화
  - **광고/전문가 연결**: 내부 광고 슬롯 + 서드파티 연동(추가 검증 후), 서버사이드 클릭 트래킹(PII 없이)
- 관리자 콘솔 (디자인 가이드 반영)
  - **웹 스택**: **Next.js + TypeScript**
  - **UI**: **Tailwind CSS + shadcn/ui** (블루 톤, 눈에 편한 테이블형 리스트)
  - **Auth**: 사내 SSO/OIDC, 2FA 필수
  - **기능**: 신고/요청 티켓 조회, 가이드 콘텐츠 관리, 광고 슬롯 운영, 감사 로그 뷰어(읽기 전용)
- **테스트 전략**
  - **단위**: Jest(NestJS) / Flutter test
  - **통합**: Pact(Consumer-driven), Testcontainers(Postgres/S3 mock)
  - **E2E**: Playwright(관리 콘솔) / Flutter integration tests
  - **보안**: SAST(semgrep), DAST(ZAP), 종속성 취약점 스캔(Dependabot)
- 업로드 파이프 라인
  - 앱 → **암호화 후 청크 업로드**(Resumable) → S3 멀티파트 → Lambda 무결성 검증 → 메타데이터 DB 트랜잭션 → 서명URL 발급(단명)
  - 네트워크 불안 시: 로컬 대기열 + 백오프 재시도, 앱 재시작 안전 복구
- MVP 대비 선택 / 대안 요약
  - **MVP 채택**: Flutter, NestJS, S3+KMS, Postgres, Auth(OIDC), S3 Object Lock(옵션), Sentry, PostHog(자가호스팅), CloudWatch
  - **차기 고려**: E2EE(사용자 단말 키로 서버 무지식 모드), KMS BYOK, 오프라인 용 암호화 공유(큐알/비밀단어), 기기 침해 탐지(Jailbreak/Root 감지)

🗓️ 실행 로드맵

✅ Phase 1 — 기획 및 설계 (1개월차)

목표: 문제 정의 명확화 및 MVP 범위 확정, UX 프로토타입 완성

기간	주요 목표	세부 실행 항목	담당
1주차	프로젝트 킥오프	• 요구사항 검토 및 범위 확정• UX 리서치(사용자 인터뷰, 경쟁 서비스 조사)	PM, 기획
2주차	정보 구조 설계	• 사용자 여정 지도(User Journey Map)• IA(Information Architecture) 및 기능 우선순위 정의	기획, UX
3주차	UX/UI 프로토타입	• 앱 핵심 흐름 와이어프레임 제작• 위장 UI 컨셉 시안 제작(날씨·계산기 UI 포함)	디자인
4주차	기술 아키텍처 확정	• 기술 스택 및 클라우드 인프라 결정• 데이터 모델 및 암호화 정책 확정	개발리드, 보안엔지니어

성과물:

- UX 프로토타입 (Figma)
- 시스템 아키텍처 다이어그램
- 기능 정의서 및 API 설계 초안

✅ Phase 2 — 핵심 기능 개발 (2개월차)

목표: MVP 3대 핵심 기능 완성 (증거 업로드/백업, 위장 모드, 법률 가이드)

기간	주요 목표	세부 실행 항목	담당
1주차	증거 업로드 시스템	• 파일 암호화/이중 저장 구현• 로컬·클라우드 동기화 모듈 개발	모바일, 백엔드
2주차	보안/인증 기능	• 앱 잠금(비밀번호·생체인증)• 세션 관리 및 만료 정책 구현	모바일, 백엔드
3주차	위장 기능	• 아이콘·앱명 스위칭 구현• 위장용 첫 화면(날씨/계산기) 제작	모바일, 디자인
4주차	법률 절차 가이드	• CMS 기반 콘텐츠 통합• 단계별 프로세스 UI 완성	콘텐츠, 프론트엔드

성과물:

- 내부 테스트 가능한 MVP 버전
- 암호화·백업 기능 안정성 검증 리포트

- 법률 가이드 1차 콘텐츠 세트

✅ Phase 3 — 테스트 및 베타 런칭 (3개월차)

목표: 안정성 확보, 보안 점검, 실사용자 피드백 수집

기간	주요 목표	세부 실행 항목	담당
1주차	통합 테스트	• 기능/보안/성능 테스트• QA 자동화 스크립트 구축	QA, 개발
2주차	클로즈드 베타	• 20~30명 테스트 사용자 모집• UX 피드백 수집 및 개선	PM, 디자인
3주차	보안 강화	• 모의해킹 및 취약점 점검• 앱 스토어 심사용 빌드 준비	보안, 개발
4주차	MVP 런칭	• 앱스토어/플레이스토어 등록• 초기 광고주(법률/탐정) 연동 시작	PM, 마케팅

성과물:

- 정식 출시 가능한 MVP 버전 (v1.0)
- 테스트 리포트 및 보안 인증 보고서
- 초기 사용자 후기 및 개선 계획

🔄 Phase 4 — 확장 및 최적화 (4~6개월차 이후)

목표: 사용자 유지율 강화 및 수익 모델 고도화

영역	주요 방향	세부 내용
💬 사용자 유지	• 심리상담/커뮤니티 기능 추가• 자동 백업 상태 알림, 안심 리포트 제공	
💰 수익 모델	• 전문가 광고 자동 매칭• 프리미엄(암호화 공유, 변호사 상담 연결) 출시	
🧩 기술 확장	• E2EE(종단 간 암호화) 적용• 클라우드 비용 절감 및 서버리스 전환	
📈 데이터 분석	• 사용자 행동 분석 기반 UX 개선• 리텐션/이탈 분석 대시보드 구축	

📍 전체 일정 요약

월	주요 마일스톤
1개월차	기획/디자인/아키텍처 확정
2개월차	핵심 기능 개발 완료
3개월차	테스트 및 MVP 런칭
4~6개월차	피드백 반영 + 확장 기능 개발