Mollet

한글날 기념 프로젝트 · Agentic AI Hackathon 2026

한글동행 HANGUL DONGHAENG

한글로 잇는 한국의 문화와 역사

걸으며 비추기만 하면 랜드마크를 알아보고,
이야기와 주변 맛집을 여행자의 언어로

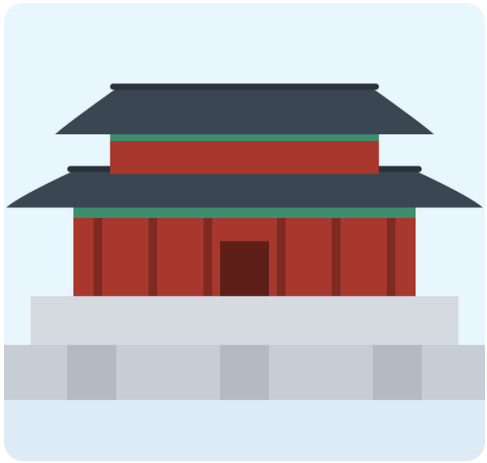
외국인 여행자 · 한국어 · English

NVIDIA OpenShell · Nemotron VL

2026.10.07 · Team Mollet

랜드마크마다

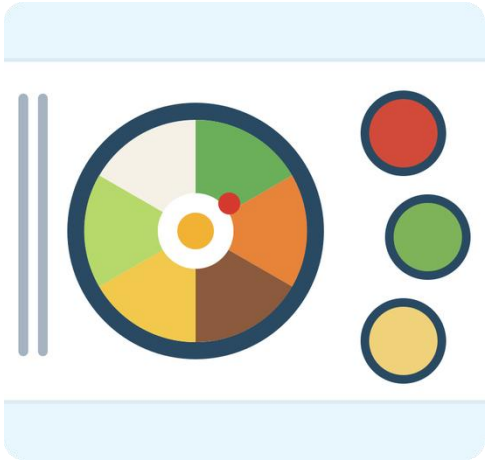
1



영상으로 랜드마크 인지

걸으며 보는 경복궁 ·
남산타워를 바로 알아보고
이야기

2



보는 곳의 주변 맛집

지금 보고 있는 랜드마크 주변
음식점을 지도로

일러스트 · 실제 화면 아님

텍스트만으로 알 수 없는 맥락을 판단, 다음 걸음까지 동행

대회 미션

사용자의 상황을 이해하고, 맥락과 신뢰성을 판단해 실제 사용 가능한 경험으로 잇는 AI Agent

배경 · 2025년 방한 외래객 약 1,894만 명(한국관광공사 한국관광통계)

한글동행의 답

눈앞의 장면에서 시작

카메라로 본 경복궁·남산타워를 질문의 대상으로

다음 목적까지

현재 랜드마크를 위치 기반으로 주변 식당 추천

한글동행 한자 현판 앞에서도, 그 문이 품은 역사를 사용자의 언어에 맞게 풀어 주는 문화·역사 동행 Agent

걸으며 보는 영상에서 랜드마크를 알아봅니다

실시간 촬영	선택 프레임	랜드마크 인식	선제 질문	자료 조회	근거 검증	음성 안내 · 카드
기기에서 연속 표시 · 분석과 분리	≥20초 간격 · 이전 응답 완료 후	Nemotron VL 관찰	“설명해 드릴까요?” · 사용자 언어	허용된 도구 · 등록 자료	broker: 형식 · 인용 · 소유권	검증된 결과만 저장

랜드마크 인식

에이전트가 전달 받은 프레임의 랜드마크 여부를 인식

먼저 말 걸기

여행자의 언어로 “설명해 드릴까요?”, 원하면 이어서 설명

음성 안내 및 후속 추천

질문에 대해 음성으로 설명 및 랜드마크 주변 식당 추천

장점 보고 있는 장면이 곧 질문 · 연속 미리보기는 기기에서, 분석은 필요한 프레임만 골라서

비추면 알아보고, 여행자의 언어로 먼저 말을 겁니다

대화 예시



경복궁

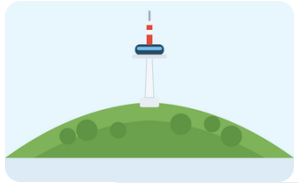
카메라로 비춤 · 한국어 사용자

경복궁에 오셨네요. 설명해 드릴까요?

응, 알려줘

경복궁은 1395년에 세워진 조선의 중심 궁궐이에요. 정문 광화문의 세 문 가운데 문은 왕이 지나던 통로였어요. 현판 '光化門'은 한자라서, 그 이야기를 쉬운 한글로 풀어 드릴게요.

서울관광재단 · 한국관광공사 · 국립한글박물관



남산타워

카메라로 비춤 · English user

This is Namsan Seoul Tower. Shall I tell you about it?

Yes, please

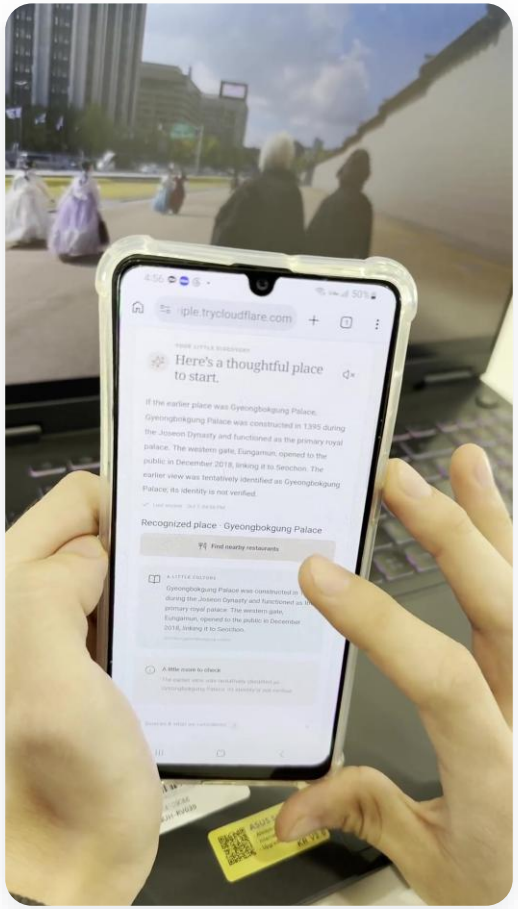
It was the first multipurpose tower in Korea, adding a sightseeing observatory to a broadcasting tower. The observatory offers an unobstructed view of the whole city.

VISITKOREA (English)

이어서 "주변 맛집 추천해줘" → 탐색한 랜드마크 주변 음식점을 거리순 최대 3곳, 지도와 OSM 출처로

대화 속 사실 문장은 공식 관광·전시 자료 기준(영어 문장은 VISITKOREA 영문 원문 요약) · 확인된 지원 언어는 한국어·영어 · 일러스트는 실제 사진 아님 · 확인 2026-10-07

안내에서 추천까지: 실제 데모



경복궁 인식 → 영어 문화 안내
주변 음식점 지도 확인

01 랜드마크에서 먼저 말 걸기

"설명해 드릴까요?" → (승인 시) 쭉 설명

02 사진 전송 및 안내

사용자가 촬영한 사진에 대해서 요청된 내용 답변

03 주변 식당 추천

랜드마크 위치 기반 주변 식당 추천

시연 영상은 별도 MP4로 첨부

모델이 판단하고, 정책이 경계를 정합니다

브라우저
로컬 미리보기
선택 프레임 전송

trusted broker
세션·소유권 검사
결과 검증·영구 저장

OpenShell
에이전트 worker
허용된 도구 호출

NVIDIA L40S
Nemotron Nano
12B v2 VL · BF16

nvidia/NVIDIA-Nemotron-Nano-12B-v2-VL-BF16 · vLLM 0.12.0 · 실제 호출에서 설정·응답 모델 일치 3회 기록

통제	검사 대상
앱의 도구·자료 허용 목록	승인한 출처·장소 ID와 제한된 카탈로그 조회
OpenShell 실행 정책	worker 프로세스의 파일·목적지·HTTP 요청 권한
모델 출력 검증	JSON·스키마, 승인 근거·인용 ID, 장소 일치, 요청·세션·실제/가상 모드
영구 산출물 작성	broker가 현재 요청을 검사한 뒤 카드 저장 · worker는 내용만 제안
주변 음식점 조회	broker가 고정 Nominatim·Overpass 조회 · 모델은 URL·쿼리를 정하지 않음 · 거리순 최대 3곳

실행 **L40S에서 Nemotron VL 실제 호출 · 설정·응답 모델 일치 확인**

Nemotron Nano 12B v2 VL BF16 모델 카드(v1.0): 지원 하드웨어 L40S, 카드상 지원 언어 English only · 스키마·인용 통과가 문장의 의미·역사 사실을 증명하지는 않음

정책으로 경계를 정하고, 실제 기록으로 확인했습니다

정책 요약

코드·자료 읽기 전용 | 임시 경로만 쓰기 | Landlock 필수 | 비루트 실행 | REST enforce 모드

실제 기록 확인 · 자체 시험

허용된 상태 조회

200

허용 GET 요청 성공

독립 수신기에서 1회 확인

허용하지 않은 전송

403 · 수신 0

예약 POST 차단

비허용 목적지도 수신 0

제한된 파일 동작

차단

읽기·쓰기·삭제 시험

보호 파일의 전후 해시 동일

정책 로그와 수신 기록을 대조했고, 경계 결합 판정 11개 조건을 통과했습니다.
자체 무해한 시험 파일·수신기로 검증한 결과이며, 모든 경로의 안전성을 뜻하지 않습니다.

결과 OpenShell 0.1.2 · 통제된 경계 시험 11개 조건 통과

OpenShell Sandbox Policies: 파일 접근은 Landlock, 네트워크 목적지·요청은 정책으로 통제하고 명시적으로 허용되지 않은 접근은 거부 · 카메라·마이크·위치·지도는 worker 샌드박스 밖

한국의 문화와 일상을 한글로 이어 갑니다

확인된 동작

- 전체 시연: 영상 속 경복궁 인지 → 영어 설명 → 주변 음식점 3곳 지도
- 실제 HTTPS UI 기본 흐름 PASS · 한국어·영어 음성 입력과 TTS
- OpenShell 통제 시험 11조건 PASS

다음 확장

- 더 많은 랜드마크와 언어로 확장
- 메뉴 추천과 음식→문화 안내까지

함께 이해할 것

눈앞의 장소
경복궁 · 남산타워

한국의 문화와 역사
출처와 함께 이해할 맥락

이어 가는 동행
방문한 랜드마크에서, 식사까지 추천

한글날 기념 · 눈앞의 장면에서 문화·역사와 생활의 이야기로.

감사합니다

Mollet