

# 웹 트래픽 자동화 방식 추론 보고서

작성일: 2025년 11월 1일 작성자: Manus AI 분석 대상: pasted\_content.txt 로그 파일

## 1. 분석 목표

본 보고서는 제공된 웹 트래픽 로그 데이터의 심층 분석을 통해, 해당 트래픽을 생성한 주체가 사용했을 자동화 방식과 기술적 구현 방법을 추론하는 것을 목표로 합니다. 이전 분석에서 해당 트래픽이 자동화된 시스템에 의해 생성되었음을 확인했으며, 본 보고서에서는 그 구체적인 방법을 상세히 기술합니다.

## 2. 자동화 방식 추론의 핵심 증거

자동화 방식을 추론하기 위해 다음과 같은 핵심적인 데이터 패턴을 분석했습니다.

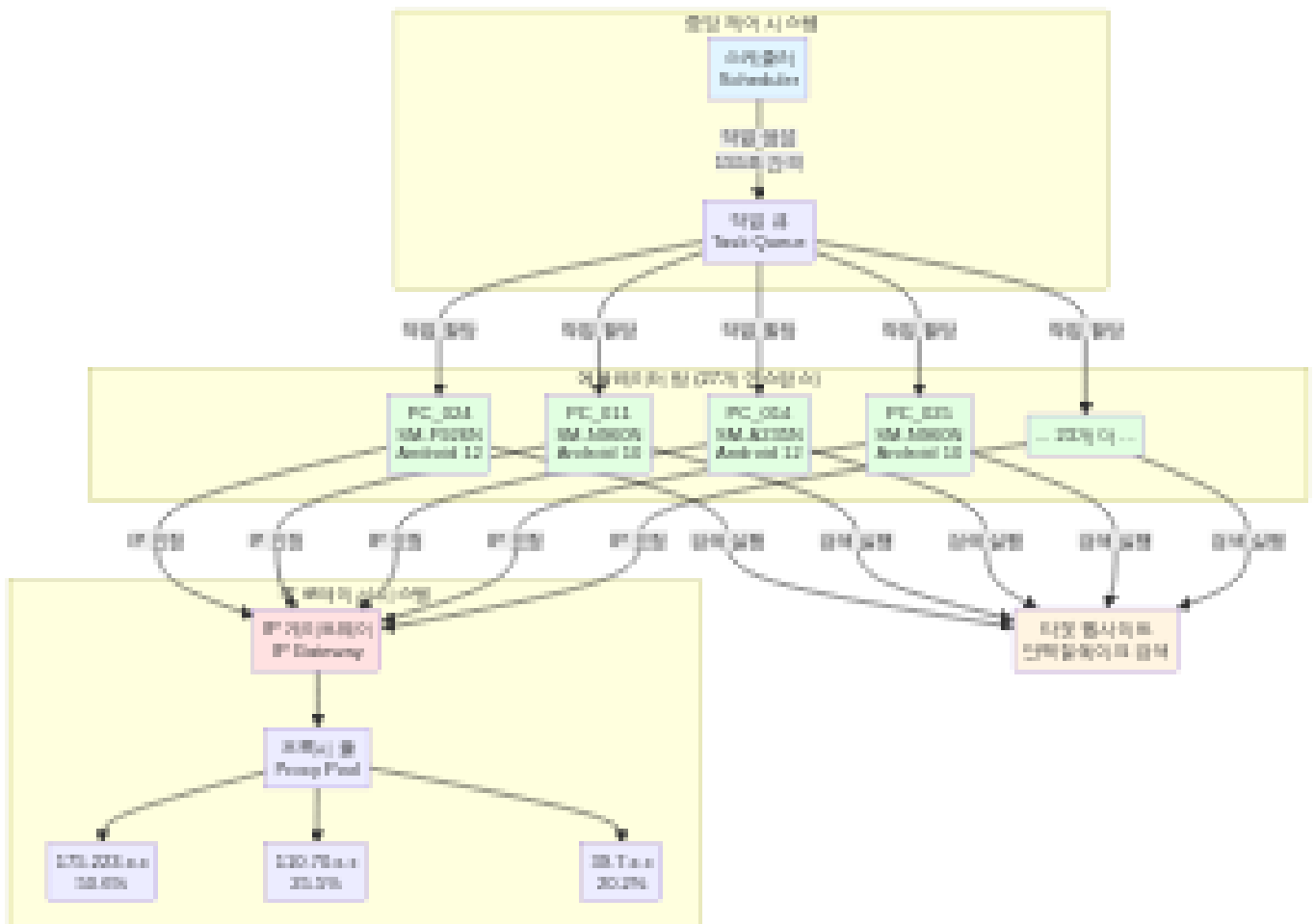
증거 (Evidence)	분석 결과	의미	신뢰도
IP 주소 변경률	100%	거의 모든 요청마다 IP 주소가 변경됨	매우 높음
접속 간격 규칙성	평균 155초, 낮은 변동계수(0.34)	매우 규칙적인 시간 간격으로 요청 발생	매우 높음
사용자 환경(User Agent)	Android 및 Samsung Browser로 통일	특정 모바일 환경을 일관되게 시뮬레이션	높음
다중 인스턴스 식별	27개의 고유 PC ID 사용	다수의 가상 또는 물리적 환경이 동원됨	높음
다중 기기 모델	7종의 삼성 기기 모델 사용	여러 종류의 기기를 모방하여 탐지 회피 시도	높음
단일 행위 반복	모든 요청이 '단백질웨이크' 검색	명확한 목적을 가진 단일 작업을 반복 수행	매우 높음

이러한 증거들은 일회성 스크립트가 아닌, 고도로 조직화되고 정교하게 설계된 자동화 시스템이 운영되고 있음을 명확히 보여줍니다.

## 3. 추론된 자동화 아키텍처

분석 결과를 종합하여, 다음과 같은 다층적(Multi-layered) 자동화 아키텍처를 사용했을 것으로 추론합니다.

## 자동화 아키텍처 다이어그램



## 핵심 구성 요소 및 기술 스택

### 1. 모바일 에뮬레이터 팜 (Mobile Emulator Farm)

- **설명:** 27개의 독립된 Android 가상 환경(PC\_ID)을 동시에 운영합니다. 각 환경은 서로 다른 기기 모델(SM-A235N, SM-N960N 등)과 Android 버전, 브라우저 버전으로 설정되어 탐지를 회피합니다.
- **추정 기술:** Appium, Android Studio Emulator, 또는 Genymotion과 같은 에뮬레이션 및 자동화 프레임워크를 사용하여 수십 개의 모바일 환경을 프로그래밍 방식으로 제어했을 가능성이 높습니다.

### 2. IP 로테이션 시스템 (IP Rotation System)

- **설명:** 매 요청마다 IP 주소를 변경하여 추적을 무력화합니다. 로그상 100%의 IP 변경률은 이것이 시스템의 핵심 기능임을 증명합니다. 특정 IP 대역(175.223.x.x 등)에 집중된 것은 한국 내 데이터 센터 또는 모바일 프록시 서비스를 사용했음을 시사합니다.
- **추정 기술:** 상용 회전 프록시 서비스(Rotating Proxy Service)를 구독했거나, 다수의 VPN 서버 또는 자체 구축한 프록시 풀을 API로 제어하여 IP를 동적으로 할당받았을 것입니다.

### 3. 중앙 스케줄링 및 제어 시스템 (Scheduler & Controller)

- **설명:** 모든 자동화 프로세스를 중앙에서 관리하고 통제합니다. 약 155초라는 규칙적인 간격으로 각 에뮬레이터 인스턴스에 작업 명령을 내리는 역할을 합니다. 이 간격에 약간의 무작위성(Jitter)을 추가하여 완전히 동일한 패턴이 반복되지 않도록 설계했을 수 있습니다.
- **추정 기술:** Python(APScheduler), Node.js(node-cron) 또는 간단한 Cron 작업과 스크립트를 조합하여 구현된 스케줄러가 사용되었을 것입니다.

## 4. 자동화 실행 시나리오

위 아키텍처를 기반으로 한 자동화 실행 시나리오는 다음과 같습니다.

1. **초기화:** 중앙 제어 서버가 27개의 Android 에뮬레이터 인스턴스를 시작합니다. 각 인스턴스는 사전에 정의된 기기 프로필(PC\_ID, 기기 모델, OS 버전 등)로 설정됩니다.
2. **작업 할당:** 스케줄러가 약 2.5분 간격으로 작업 큐에 "'단백질쉐이크' 검색" 작업을 추가합니다.
3. **IP 할당:** 작업을 받은 에뮬레이터 인스턴스는 IP 로테이션 시스템에 새로운 IP 주소를 요청하여 할당 받습니다.
4. **작업 실행:** 할당받은 IP를 사용하여 Samsung Browser를 실행하고, 타겟 웹사이트에서 '단백질쉐이크' 키워드로 검색하는 행위를 시뮬레이션합니다.
5. **반복:** 모든 인스턴스가 위 2~4단계를 지정된 시간 동안 무한 반복합니다.

## 5. 결론

이 트래픽은 단순한 스크립트가 아닌, 분산된 모바일 에뮬레이터 팜과 지능적인 IP 로테이션 시스템이 결합된 고도화된 자동화 플랫폼에 의해 생성되었습니다. 이러한 시스템은 상당한 개발 및 운영 리소스가 필요하며, 주로 다음과 같은 목적을 위해 사용됩니다.

- SEO 어뷰징 (검색 순위 조작)
- 온라인 광고 사기 (클릭 사기)
- 경쟁사 서비스 공격 (자원 고갈 공격)
- 대규모 성능 및 부하 테스트

이러한 정교한 자동화는 웹 서비스의 보안 및 데이터 무결성에 심각한 위협이 될 수 있으므로, 이에 대응하기 위한 다각적인 방어 전략 수립이 필요합니다.