



K-Shield Jr. 6기 프로젝트

모바일 포렌식 시각화 툴 개발

2조 티미룸 김석진 문재식 민서정 박귀수 송어진 이용하 이재훈 이지호 한택승

Contents

01 프로젝트 개요

02 기능 소개

03 시나리오 소개 및 시연

04 추후 연구 예정

05 Reference



01 프로젝트 개요

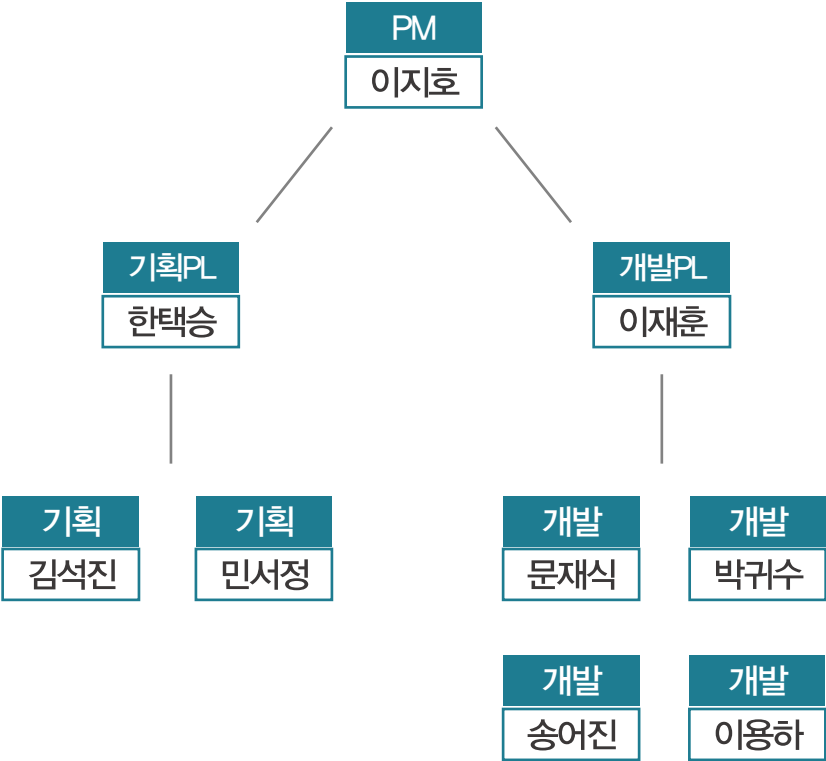
프로젝트명 및 기간

프로젝트명 : 모바일 포렌식 시각화 툴 개발

프로젝트 기간 : 2021.03 ~ 2021.06 (2.5개월)

프로젝트 수행 팀 : 티미룸

프로젝트 조직도



01 프로젝트 개요

주제 선정 배경



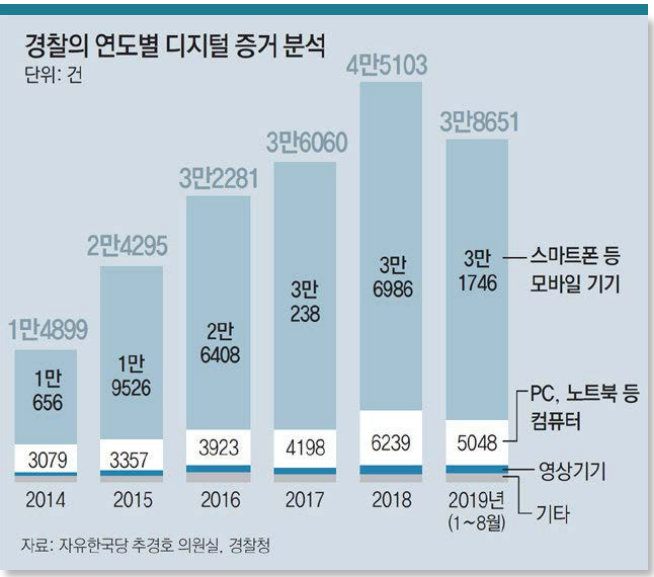
스마트폰, 태블릿PC 등의 다양한 모바일 기기들은 현대인의 생활을 편리하게 해줌과 동시에 **일상생활과 가장 밀접한 데이터들이 저장된 정보저장매체가 되었다**

모바일 기기에는 우리 일상생활과 밀접한 데이터가 가장 많이 저장되어 있기 때문에 디지털 포렌식 수사 시 **모바일 포렌식의 필요성이 크게 증가하고 있다**

김도현, 이상진 (2016). 모바일 포렌식 동향. 정보보호학회지, 26(5), 22-31.

01 프로젝트 개요

주제 선정 배경



디지털 포렌식은 수사를 위한 국가 기관뿐 아니라 기업, 법무법인 등에서 소송 관련 업무에도 활용되고 있으며 근래에는 보험 조사관이나 민간 수사, 조사 업체까지 확대되어 활용하므로 그 수요가 증가하고 있는 추세

나현대, 김창재 and 이남용. (2014). 디지털 포렌식 인력 양성을 위한 단계별대학 교과과정 설계에 관한 연구. 컴퓨터교육학회 논문지, 17(3), 75-84.

경찰, '택시기사 폭행' 이용구 차관 휴대폰 포렌식 완료

경찰, '아파트 세 모녀 살해' 피의자 휴대폰 포렌식

특수본, LH직원 휴대폰 포렌식 속도...조만간 소환조사

숙명여고 앞 시위 계속...'교무부장' 휴대폰 포렌식 조사

→ 모바일 기기의 사용이 증가하면서
모바일 포렌식에 대한 수요 및 중요도 증가

01 프로젝트 개요

프로젝트 목적

모바일 포렌식을 이용하는 사람들에게
기존에 있는 모바일 포렌식 도구들보다 보기 편하고 무료로 사용할 수 있는 툴을 제공하는 것

WHO?

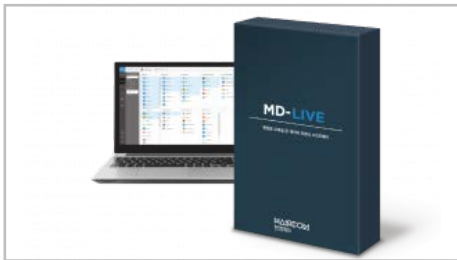
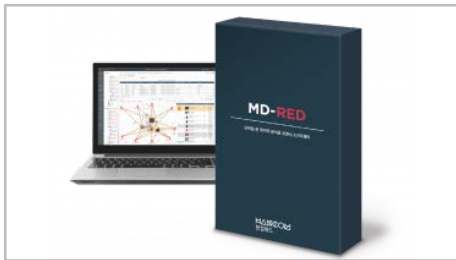
범죄 수사, 법적 분쟁 등에서 모바일 포렌식을 활용하는 사람

WHAT?

모바일 기기로부터 수집한 데이터를 다양한 방식으로 시각화

01 프로젝트 개요

기존 상용 도구 참조



기존 상용 도구 기능 참조

쉽고 간결한 사용자 인터페이스(UI) 제공

웹 상에서 대시보드를 통하여 데이터 분석 및 시각화 결과 제공

다양한 모바일 아티팩트 수집 및 시각화

메시지, 통화 기록, 인터넷 사용 기록, 미디어, 어플리케이션 등 다양한 모바일 아티팩트 데이터 수집 및 시각화

원하는 데이터 필터링 및 검색 가능

날짜 구간 지정 및 키워드 검색 가능

보고서 자동 생성 (추후 예정)

선택한 아티팩트에 대한 CSV 파일 및 보고서 자동 생성

01 프로젝트 개요

기존 무료 도구 참조

구분	세부 내용	도구			
		ALEAPP	Andriller CE	Autopsy	Timmy Room
분석	연락처		O	O	O
	메일		O	O	
	메시지	O	O	O	O
	WiFi 접속 기록	O	O		O
	사진			O	O
	동영상			O	O
	통화 기록		O	O	O
	계정 정보	O	O		
	인터넷 아티팩트	O	O	O	O
	GPS 아티팩트	O		O	O
	캘린더				O
	기기 정보	O	O		O
	APP 설치 현황	O			O
APP	Chrome	O	O		O
	Facebook		O		
	Facebook messenger		O		
	Kakaotalk				O
	Skype		O		
기타	타임라인			O	O
	키워드 검색	O		O	O
	키워드 추천				O



기존 무료 도구
기능 참조

분석 Analysis

- 연락처
- 기기 정보
- 메시지
- 사진, 동영상
- 통화 기록
- 캘린더
- WiFi 접속 기록
- 앱(APP) 설치 현황

앱 Application

- Chrome
- Kakaotalk (추가)

기타

- 타임라인
- 키워드 검색
- 키워드 추천 (추가)

프로젝트 목표



1 대상의 휴대폰에서 추출한 데이터를 이해하기 쉽도록 시각화하는 툴 개발

2 위치 정보와 시간 정보를 바탕으로 사용자의 행위를 파악하기 쉽게 시각화

→ 누구나 쉽고 편하게 사용할 수 있는, **진입 장벽이 낮은** 모바일 포렌식 도구 개발

→ 개발된 도구를 이용해 대상 휴대폰 **사용자의 행위 분석 및 추측 가능**

01 프로젝트 개요

기대 효과

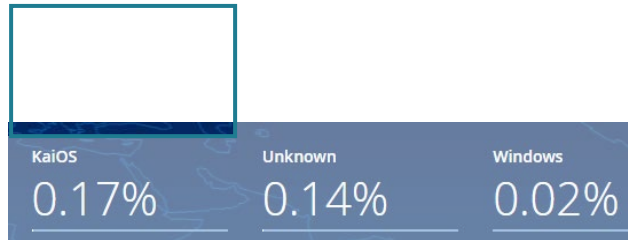


고도의 경험을 가진 숙련자 외에 입문자 또한 쉽게 모바일 포렌식 가능

모바일 포렌식 업을 하는 사람들이
보기 편하고 사용하기 편한 모바일 포렌식 도구를 이용 가능

01 프로젝트 개요

전제 조건






2021년 4월 기준 세계 모바일 OS 시장 점유율이 72.2%로 가장 높은 안드로이드 운영체제를 타깃으로 함



모바일 기기에서 추출한 이미징 파일(tar)을 분석하는 도구로, 이미징 파일을 이미 취득한 상태라고 가정

02 기능 소개

개발 스펙

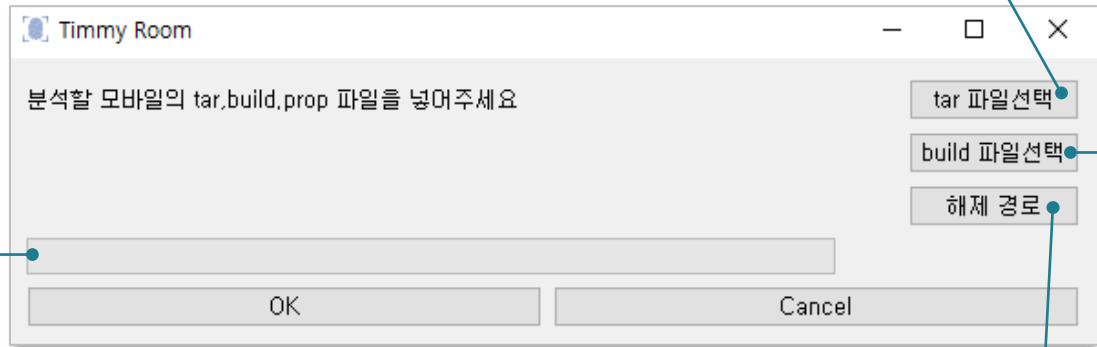
	Type	Spec
개발 언어	Python 	3.6.0
웹 프레임워크	Django 	3.2.2
오픈 API	Google map API 	

02 기능 소개

GUI 실행 창

- 분석할 모바일의 /data/ 폴더는 모바일 기기의 user data가 들어있는 폴더
- 위 폴더를 tar로 압축한 압축 파일 선택

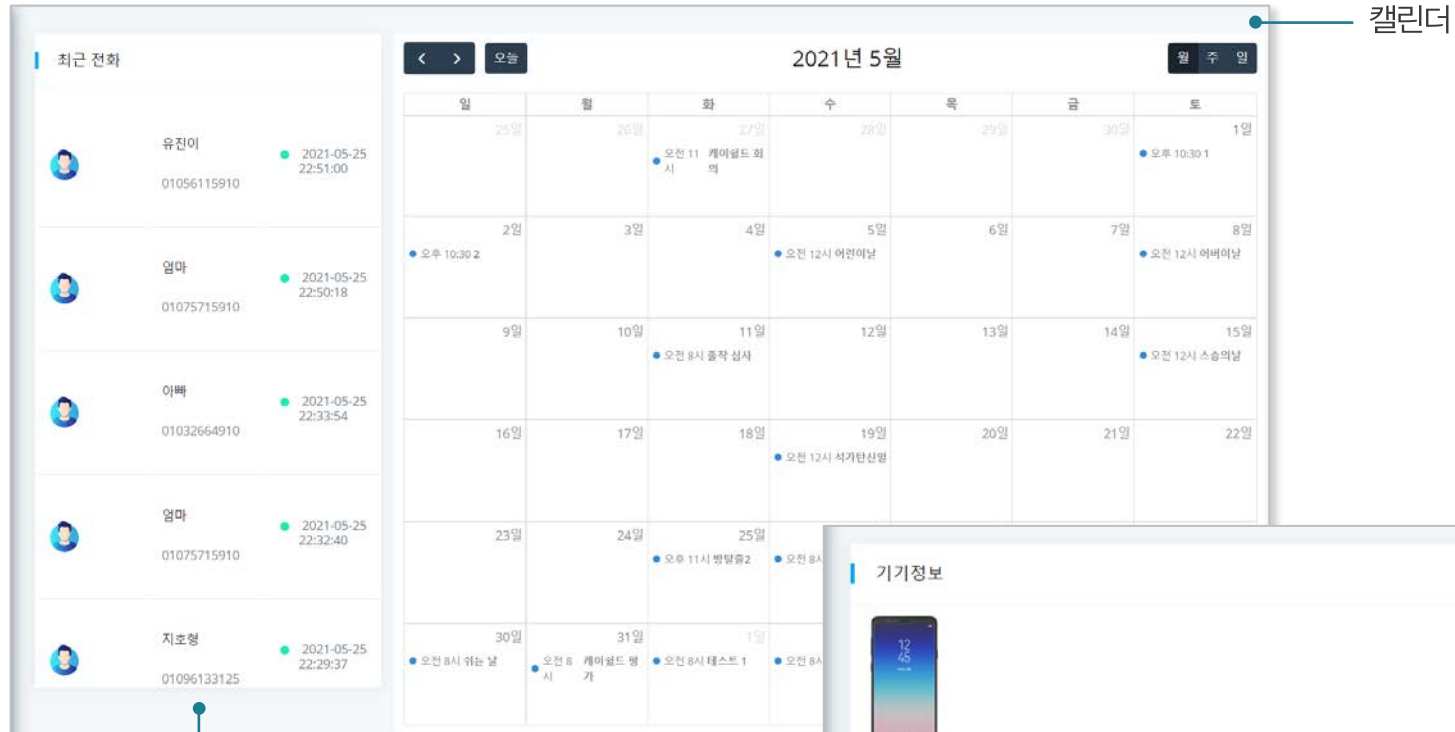
진행 표시줄(Progress bar)



- /system/ 아래에 위치
- 모바일 기기의 정보가 담겨있는 파일

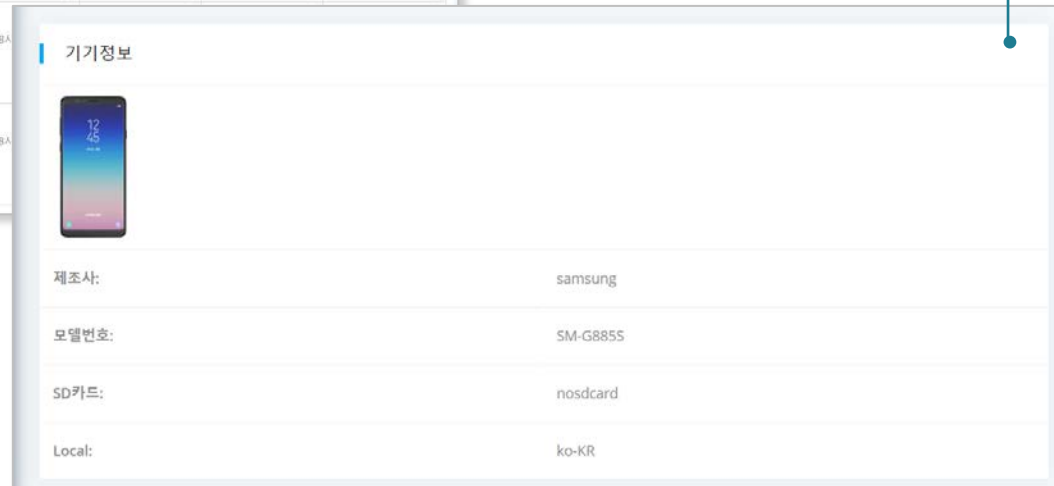
Tar 파일에서 필요한 파일들을 추출하여 저장할 위치 선택

메인 화면



크롤링을 사용하여 기기의 사진을 불러옴

최근 전화 목록



02 기능 소개

연락처 / 전화기록

이름 및 연락처 검색 가능

Contact

🏠 / 기본기능 / 연락처,전화기록

연락처

Search:

이름	연락처	전화 횟수 ↕
엄마	01075715910	7
유진이	01056115910	5
승현	01041509181	2
아빠	01032664910	2
지호형	01096133125	1
1	01026564345	0
2	01046465664	0
3	01056564487	0

전화기록

이름	상태	연락처	날짜	전화 시간
승현	발신	01041509181	2021-04-27 11:34:11	6분47초
승현	수신	01041509181	2021-04-27 11:41:04	11분49초
엄마	발신	01075715910	2021-05-12 23:45:05	부재중 통화
유진이	발신	01056115910	2021-05-12 23:45:26	부재중 통화
유진이	발신	01056115910	2021-05-12 23:48:03	부재중 통화
유진이	발신	01056115910	2021-05-12 23:50:36	부재중 통화
엄마	발신	01075715910	2021-05-12 23:50:51	0분1초
엄마	발신	01075715910	2021-05-12 23:51:38	0분16초
유진이	수신	01056115910	2021-05-12 23:52:15	0분24초

연락처 / 전화기록

Contact

🏠 / 기본기능 / 연락처, 전화기록

연락처

Search:

이름	연락처	전화 횟수
엄마	01075715910	7
유진이	01056115910	5
승현	01041509181	2
아빠	01032664910	2
지호형	01096133125	1
1	01026564345	0
2	01046465664	0
3	01056564487	0
4	01048797976	0

전화기록

이름	상태	연락처	날짜	전화 시간
엄마	발신	01075715910	2021-05-12 23:45:05	부재중 통화
엄마	발신	01075715910	2021-05-12 23:50:51	0분1초
엄마	발신	01075715910	2021-05-12 23:51:38	0분16초
엄마	발신	01075715910	2021-05-23 11:58:49	1분32초
엄마	수신	01075715910	2021-05-23 12:02:52	1분49초
엄마	수신	01075715910	2021-05-25 22:32:40	부재중 통화
엄마	발신	01075715910	2021-05-25 22:50:18	0분13초

이름, 연락처를 선택하여 특정 번호와의 전화기록만 열람 가능

02 기능 소개

메시지

키워드를 빈도수에 따라 워드클라우드 형태로 출력

검색 가능

Message

🏠 / 기본기능 / 메시지

시간(UTC+9)	상태	번호	내용
2021-04-22 22:14:31	발신	18114061	(uwZByEttLNik) Google SIM verification https://goo.gl/LHCS9W
2021-04-22 22:15:58	발신	01024353605	하이하이
2021-04-22 22:16:33	발신	+821092588393	라스트테스트
2021-04-22 22:16:47	발신	01024353605	하잉하잉
2021-04-24 23:16:33	발신	18114064	(6i4nJmYbn2T) Google SIM verification https://goo.gl/LHCS9W
2021-04-24 23:16:59	발신	01024353605	또 문자
2021-04-24 23:17:01	발신	01024353605	함
2021-04-27 11:07:43	수신	#CMAS#Severe	[하남시청] 4/27(화) 10시 기준 신규 확진자 8명 발생. 블로그, 홈페이지 참고하시기 바랍니다. c11.kr/ojmc
2021-04-27 11:30:19	수신	#CMAS#Severe	[서울시청] 04.27(화) 00시 기준 서울시 신규 확진자 116명 발생. 자치구 별 현황 및 동선 등은 bityl.co/6i7T 참고하시기 바랍니다. 120
2021-04-27 11:40:25	발신	01041509181	하이하이

이전
1
2
3
4
5
다음

02 기능 소개

브라우저 기록

브라우저 Browser



아티팩트 Artifact

■ 히스토리 History

■ 다운로드 Download

■ 검색 기록

02 기능 소개

미디어

원하는 행 클릭 시 해당 이미지 확인 가능

Media

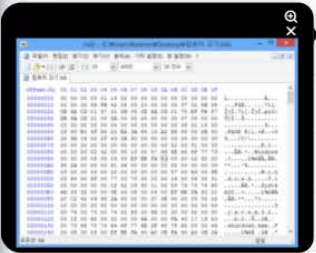
🏠 / 기본 기능 / 미디어

Search:

• 각 행 click시 미디어 자료확인 가능

날짜 및 시간 (UTC+9)	생성 도구	저장 위치
2021-04-27 10:15:37	com.android.chrome	/static/assets/images/media/0/Download/unnamed.png
	com.android.chrome	/static/assets/images/media/0/Download/cfile27.uf.26663142518DD8A1088F56.png
	Camera	/static/assets/images/media/0/DCIM/Camera/20210427_101935.jpg
	Camera	/static/assets/images/media/0/DCIM/Camera/20210427_102533.jpg
	Camera	/static/assets/images/media/0/DCIM/Camera/20210427_103827.mp4
2021-05-11 16:48:43	com.campmobile.snow	/static/assets/images/media/0/SNOW/20210511_164843_085.jpg
2021-05-11 16:48:57	com.campmobile.snow	/static/assets/images/media/0/SNOW/20210511_164856_973.jpg
2021-05-12 12:54:55	com.campmobile.snow	/static/assets/images/media/0/SNOW/20210512_125455_010.jpg
2021-05-12 18:36:06	com.campmobile.snow	/static/assets/images/media/0/SNOW/20210512_183606_708.jpg
2021-05-12 19:33:57	com.campmobile.snow	/static/assets/images/media/0/SNOW/20210512_193357_432.jpg

이전 1 2 3 4 5 다음

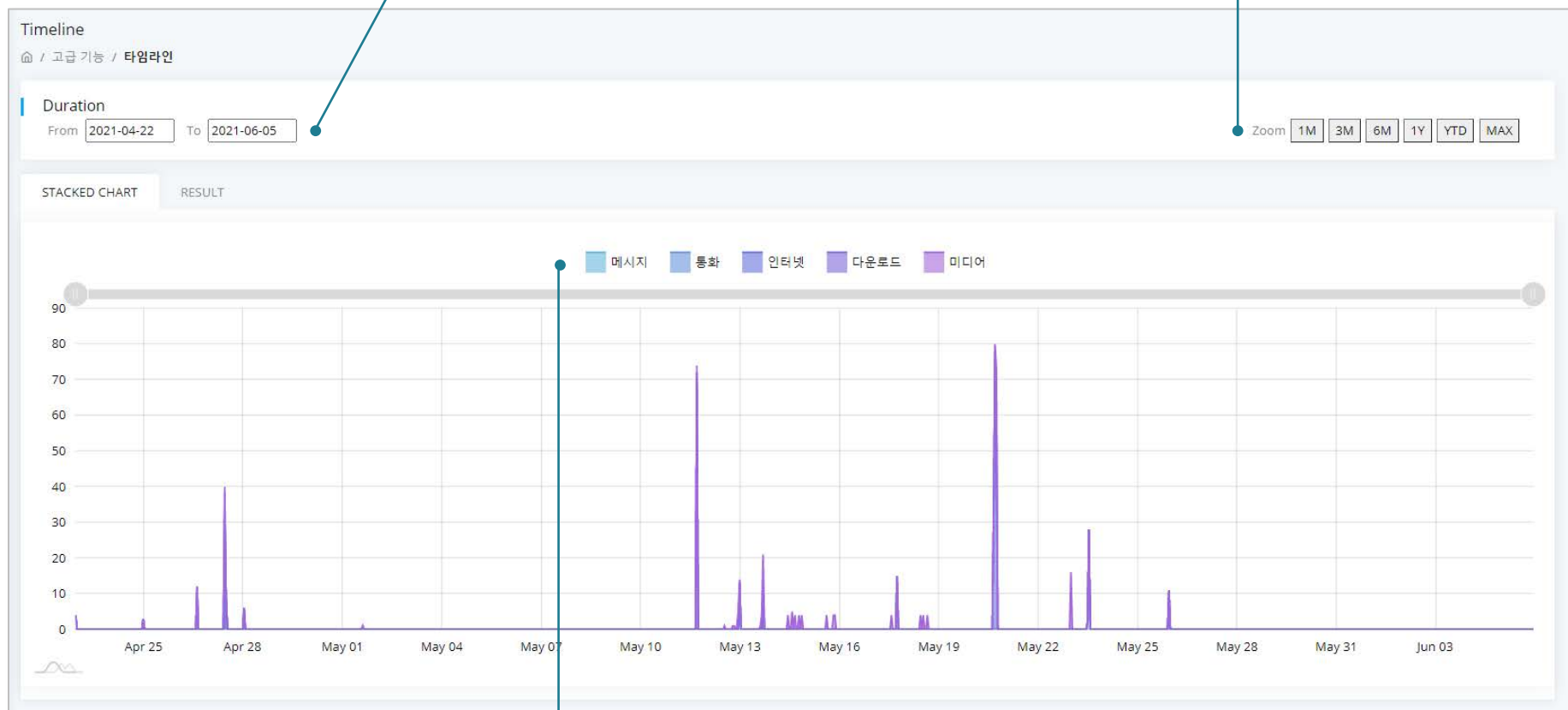


02 기능 소개

타임라인

출력할 날짜 구간 지정 가능

출력되는 날짜 구간의 단위 지정 가능

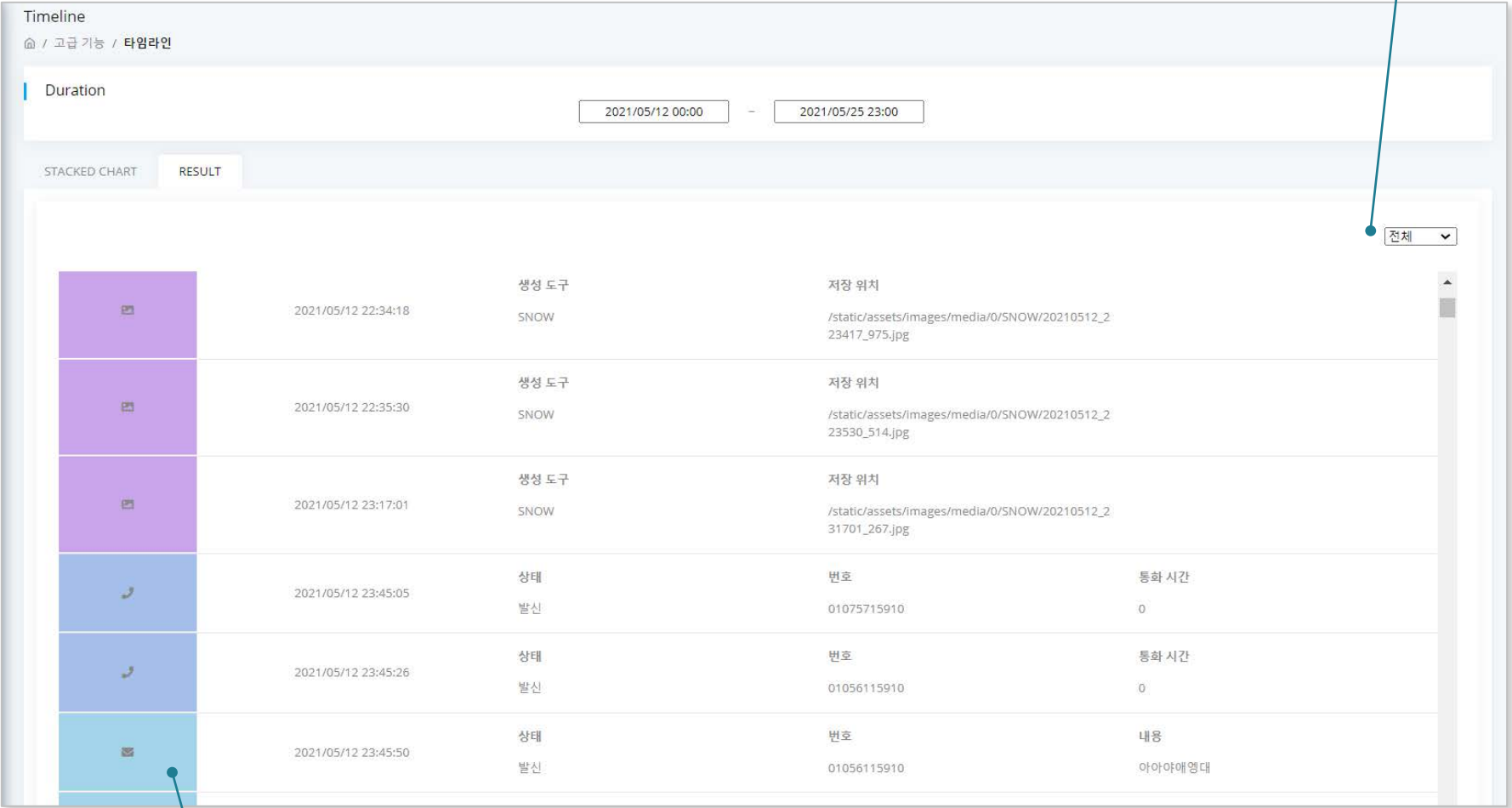


메시지, 통화, 인터넷, 다운로드, 미디어 기록을 통합해 각 횟수를 타임라인에 표시

02 기능 소개

타임라인

출력할 항목 지정 가능

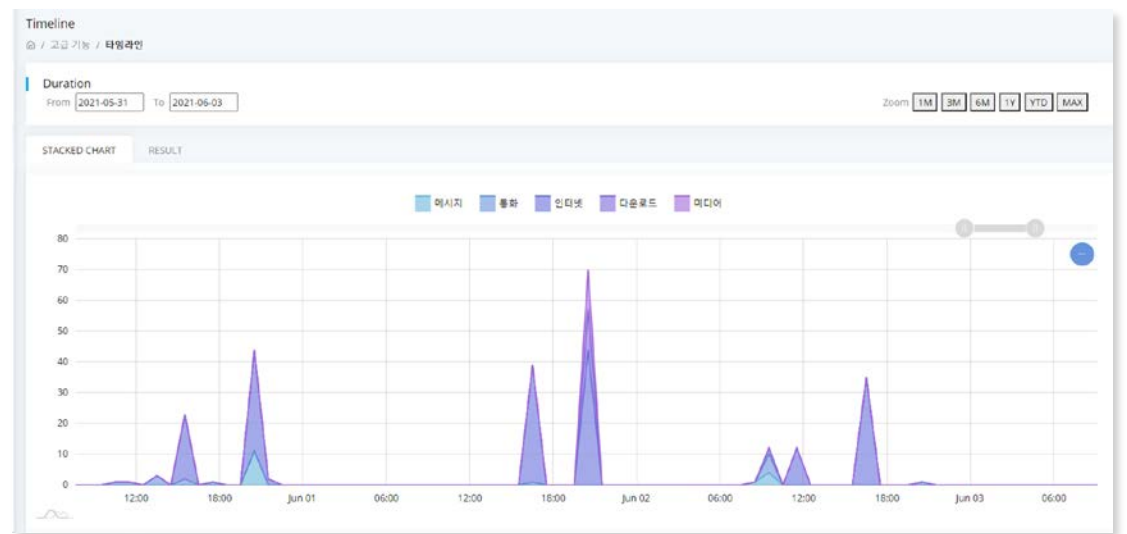
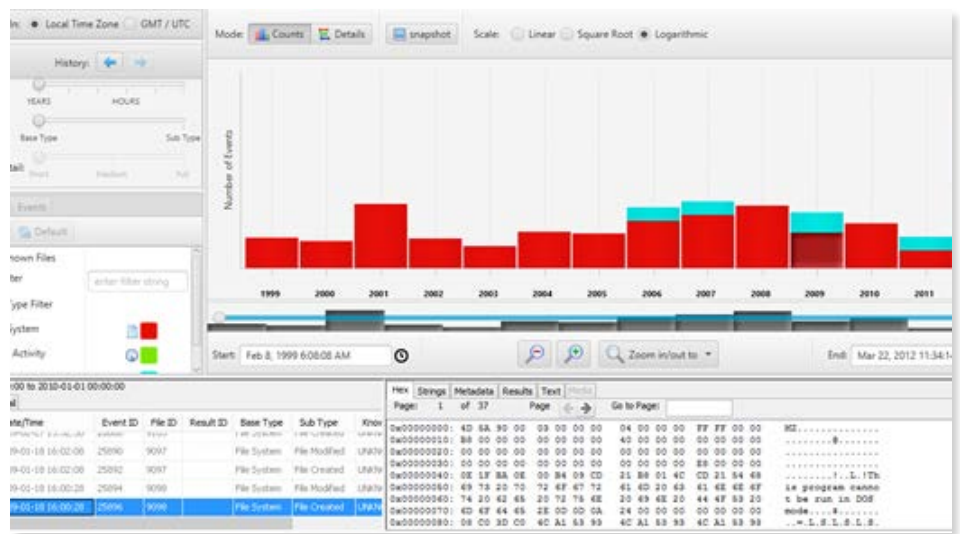


메시지, 통화, 인터넷, 다운로드, 미디어 기록을 통합해 시간 순서대로 출력

02 기능 소개

기존 무료 도구 보완

타임라인 Timeline



시각화 보완

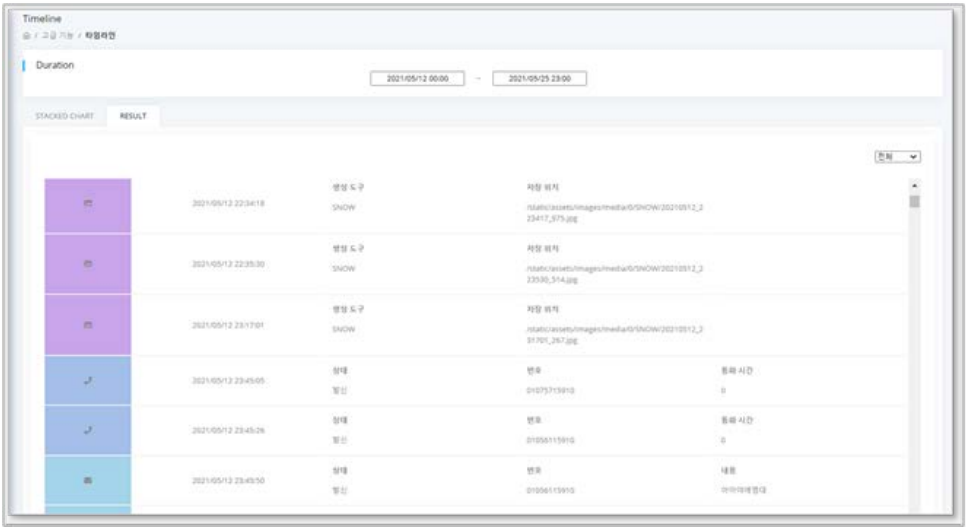
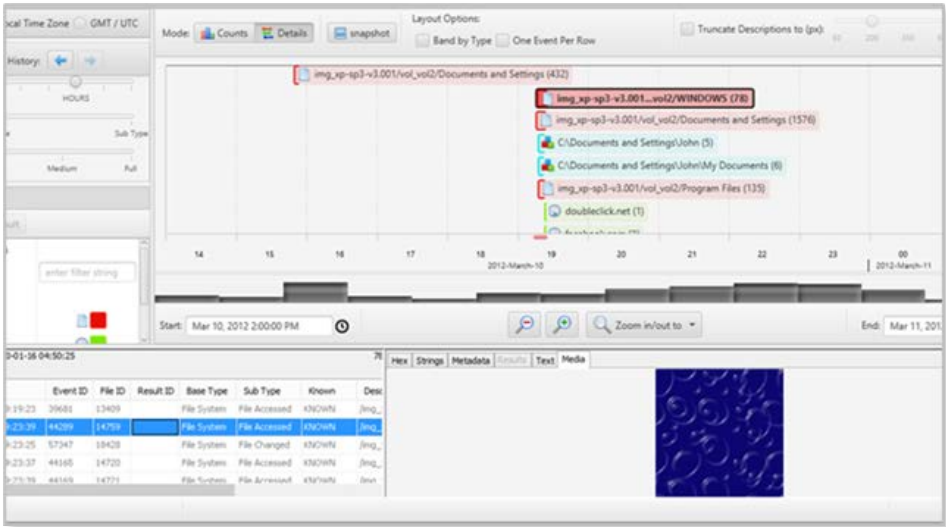
지정된 구간 내 이벤트 발생 빈도 변화 추이가 한눈에 파악되도록 선 그래프(Line Chart) 사용

출력하고자 하는 날짜 구간의 단위 선택 가능 (1M, 3M, 6M, 1Y, YTD, MAX)

02 기능 소개

기존 무료 도구 보완

타임라인 Timeline



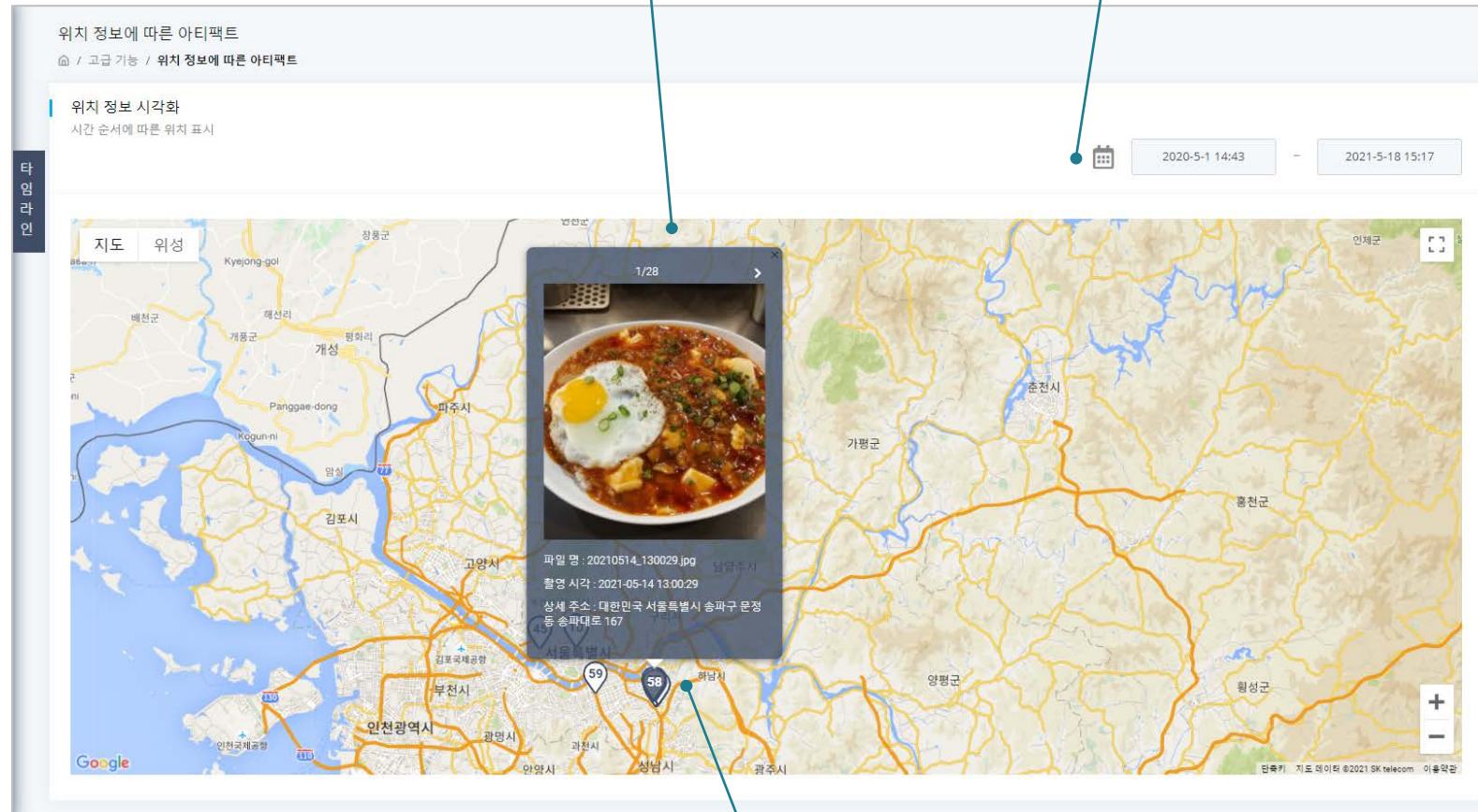
시각화 보완

- 지정된 날짜 구간 내 발생한 이벤트의 세부 내용을 시간 순으로 출력
- 발생한 이벤트를 항목별로 모아보기 가능
- 미디어의 경우 생성된 데이터 확인 가능

위치 정보에 따른 아티팩트

표시된 순서 마크 클릭 시 해당 미디어 확인 가능

출력할 날짜 구간 지정 가능

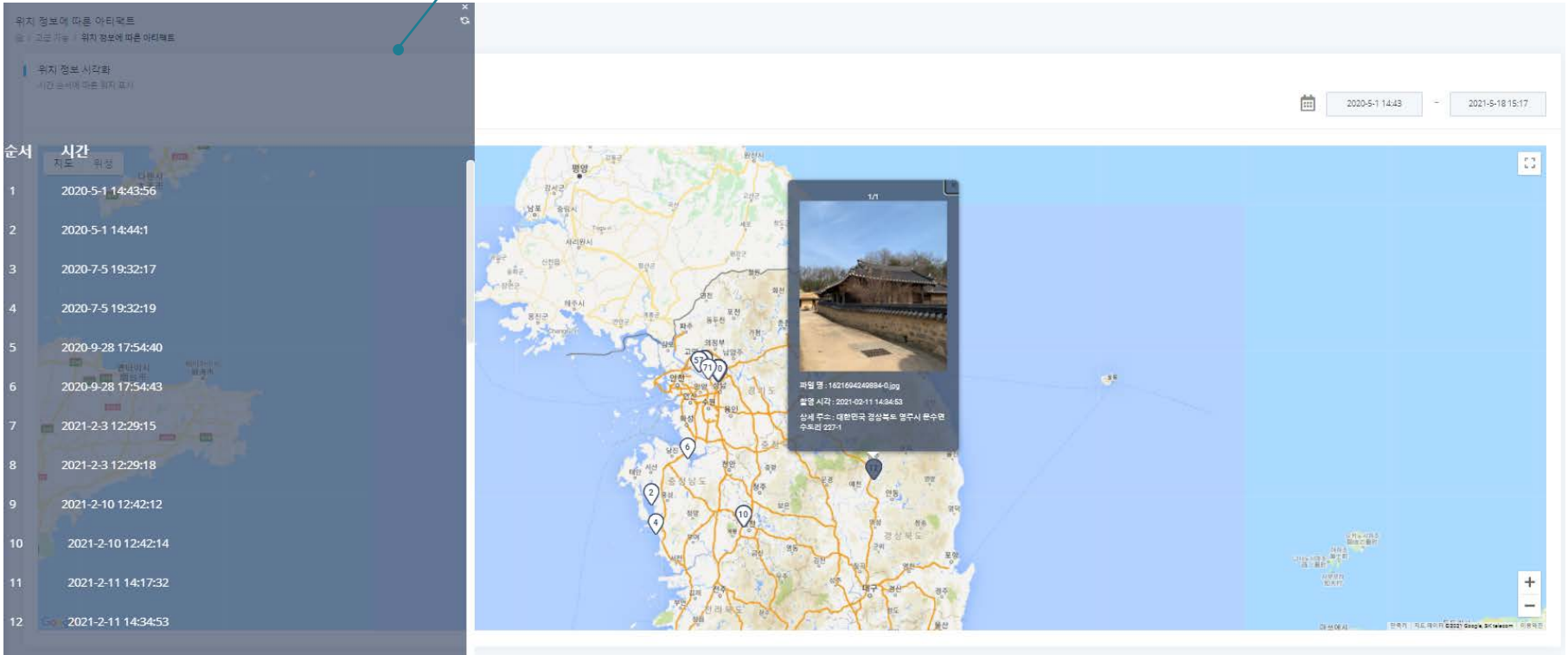


지정된 날짜 구간 내 생성된 미디어의 순서 표시

02 기능 소개

위치 정보에 따른 아티팩트

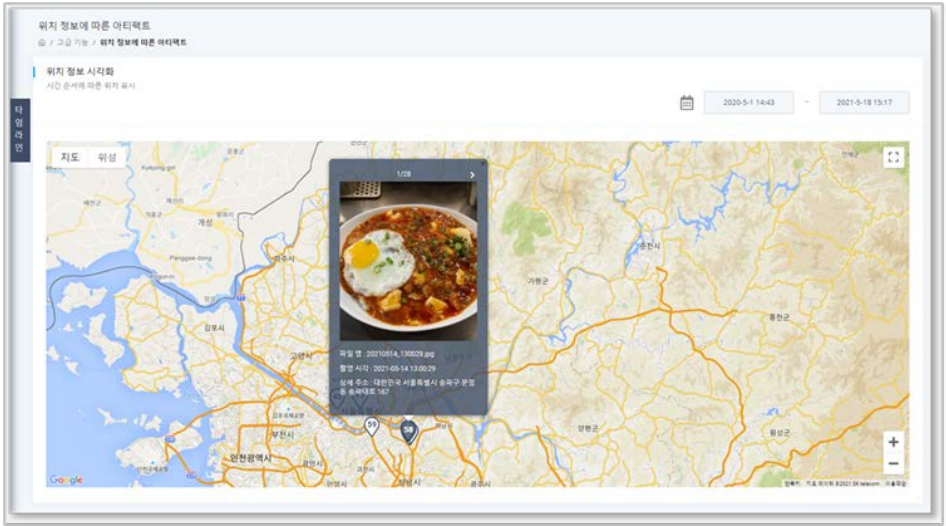
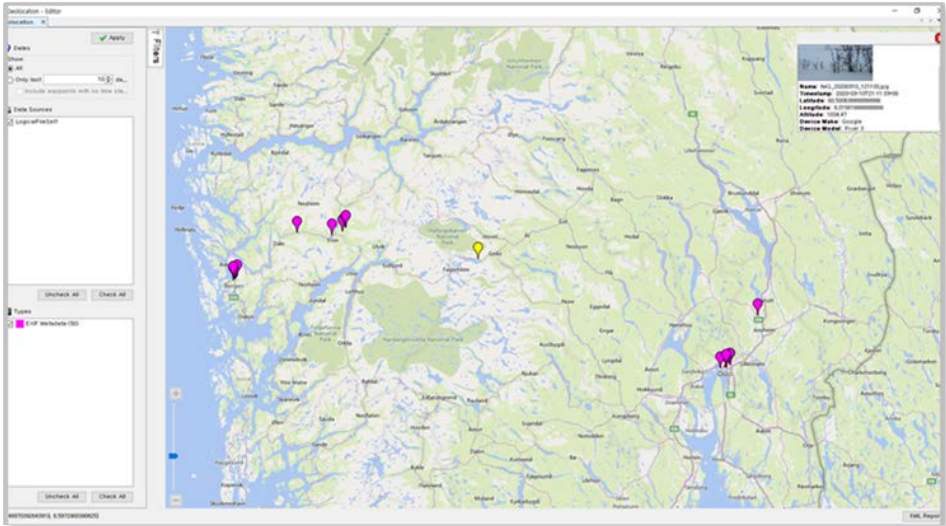
지정된 날짜 구간 내 미디어의 생성 시간 확인 가능



02 기능 소개

기존 무료 도구 보완

위치 정보



시각화 보완

GPS 데이터 생성 순서를 지도에 마크로 표시

표시하고자 하는 날짜 구간 지정 가능

02 기능 소개

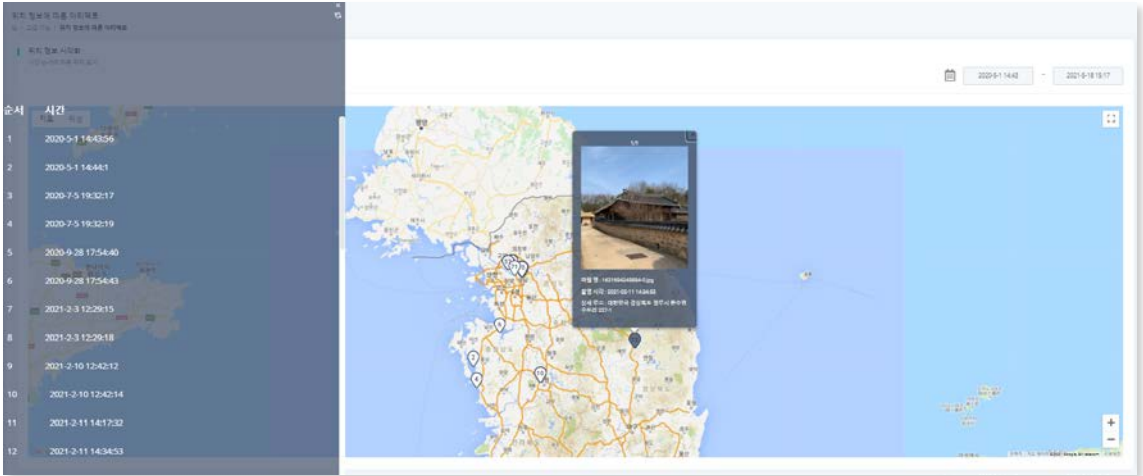
기존 무료 도구 보완

위치 정보

ALEAPP

Timestamp	Date Added	Date Modified	Title	Bucket Name	Latitude	Longitude	Address	URI
2021-04-27 01:15:37	2021-04-27 01:15:37	2021-04-27 01:15:37	unnamed	Download				
2021-04-27 01:15:44	2021-04-27 01:15:44	2021-04-27 01:15:44	cfile27.uf.2666314251BDD8A1088F56	Download				
2021-04-27 01:19:35	2021-04-27 01:19:35	2021-04-27 01:19:35	20210427_101935	Camera				
2021-04-27 01:25:33	2021-04-27 01:25:33	2021-04-27 01:25:33	20210427_102533	Camera	37.4832649230957	127.12284088134766	대한민국 서울특별시 송파구 문정동 316-6	content://secmedia
Timestamp	Date Added	Date Modified	Title	Bucket Name	Latitude	Longitude	Address	URI

Timmy Room



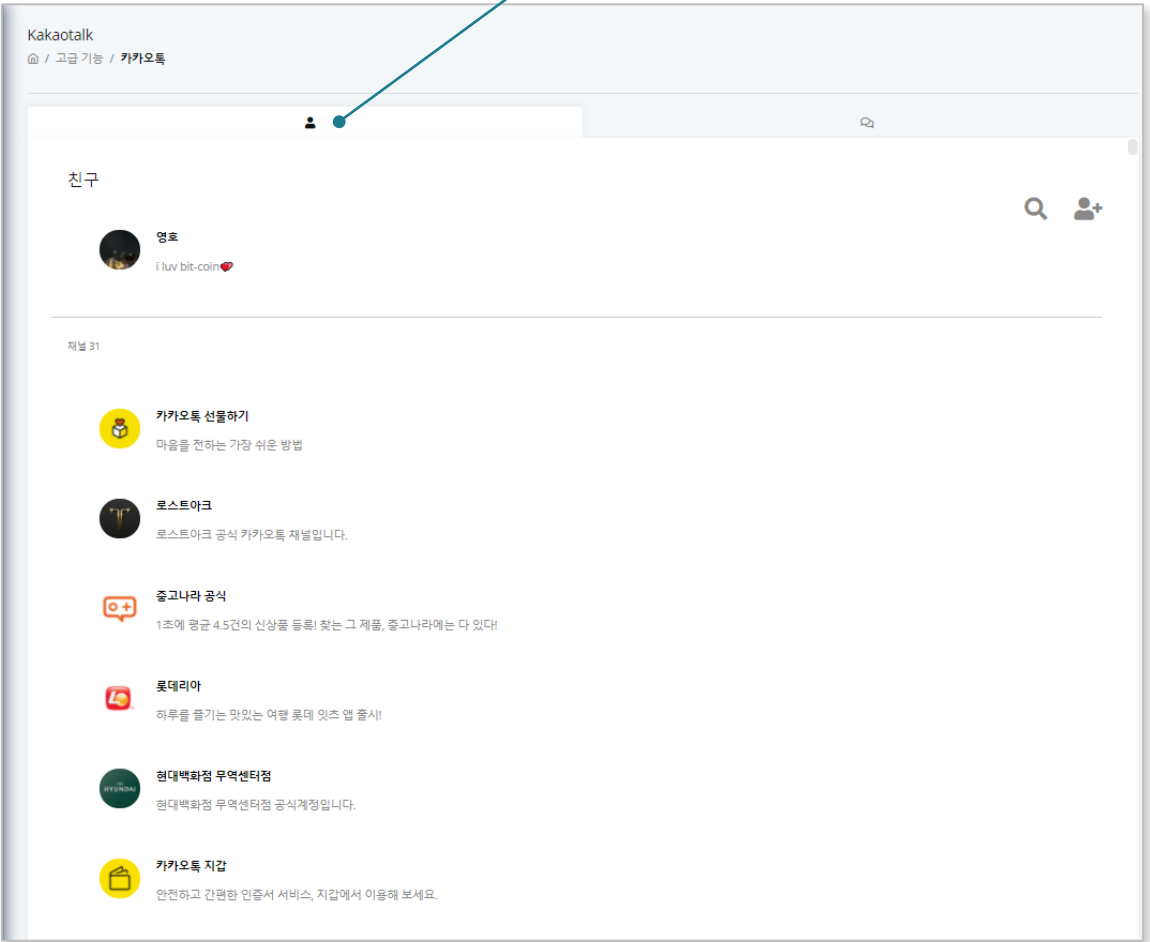
시각화 보완

GPS 데이터 타임라인 및 세부 사항을 지도에 표시

02 기능 소개

카카오톡

카카오톡에 저장된 친구 목록 확인 가능



03 시나리오 소개 및 시연

시나리오



1 같은 대학교 친구인 덕배와 진수는 학교 과제의 주제를 가상화폐로 결정



2 진수에게 가상화폐를 추천했던 군대 동기 영호에게 인터뷰 요청



3 2021년 6월 4일, 3명이 독섬유원지 역에 위치한 카페에서 모임을 가짐

03 시나리오 소개 및 시연

시나리오



4 근처 한강 공원 벤치에서 음주를 즐김



5 자정을 넘긴 시각에 영호는 화장실로, 덕배는 술을 사러 이동



6 영호가 돌아오지 않자 진수가 영호를 찾아 나섬

03 시나리오 소개 및 시연

시나리오



7 술을 사고 돌아온 덕배는 진수와 영호에게 전화를 걸었고, 받지 않자 찾으러 다님



8 덕배는 근처의 계단에서 넘어져 큰 부상을 입은 진수를 발견



9 영호가 계속 전화를 받지 않아 덕배와 진수는 병원으로 이동

03 시나리오 소개 및 시연

시나리오



10 이후에도 영호는 계속 연락을 받지 않음



11 덕배와 진수가 경찰에 신고



12 경찰은 강 근처에서 영호의 휴대폰을 발견해 모바일 포렌식 의뢰

03 시나리오 소개 및 시연

도구 시연



앞에서 소개된 시나리오 상황의 데이터를 Timmy Room 도구로 분석

03 시나리오 소개 및 시연

분석 결과

영호 휴대폰 데이터

– 실종 시각 06/05 01~02시경

확인할 수 있는 데이터

- 모델 번호: SM-G885S
- 캘린더: 06/04 20시 인터뷰 약속, 금전 관련 기록
- 마지막 메시지 수신 기록 : 06/05 01:30:17
- 마지막 메시지 발신 기록 : 06/05 00:58:52
- 마지막 통화 수신 기록 : 06/05 01:28:53 01089931596 덕배
- 마지막 인터넷 (삼성) 기록 : 06/05 01:06:10
- 마지막 미디어 기록 : 06/05 01:07:11
- 마지막 사진 위치 : 물가 근처 추정
- 가장 많은 전화기록 : 대출
- 메시지 키워드 추천 : 대출, 돈, 연락
- 삼성 브라우저 검색 기록 키워드 추천 : 빗, 코인, 대출



사건 전말 추정

영호는 대출과 친구들에게 빌린 돈을 가상화폐에 투자

– 메시지, 통화, 인터넷, SNS 채팅 기록 등을 통해 추측 가능

가상화폐의 가치가 점차 떨어지며 엄청난 스트레스를 받음

– 인터넷 기록 등을 통해 추측 가능

허영심이 있었던 영호는 겉으로 보이기에 많은 돈을 번 것처럼 포장

– 메시지, SNS 채팅, 인터넷 기록 등을 통해 추측 가능

빚 독촉이 심해지고 가상화폐의 가치가 계속해서 떨어지며 자살 생각

– 메시지, 통화, 인터넷, SNS 채팅 기록 등을 통해 추측 가능

덕배, 진수와의 모임 직전까지 극심한 빚 독촉 전화에 시달림

– 메시지, 통화, SNS 채팅 기록 등을 통해 추측 가능

모임 중 자살 시도

– GPS 기록, 인터넷 기록 등을 통해 추측 가능

04 추후 연구 예정

사용 환경

- 삼성 외의 다른 제조사 기기들도 실행할 수 있도록 개발
- DD 포맷의 파일에서 직접 추출 혹은 모바일 기기에서 라이브로 시각화 가능하도록 개발

기능 Feature

- 이미지 데이터를 바탕으로 인물 식별
- 영상, 음성 데이터의 소리를 텍스트로 변환하여 출력
- 추천된 키워드를 연관할 수 있는 카테고리 분석
- S노트 시각화 (삼성 노트 시리즈 한정)
- 원하는 데이터 CSV, PDF 등의 포맷으로 출력 가능

05 Reference

- statcounter GlobalStats, <https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-202103-202103-bar>
- statcounter GlobalStats, <https://gs.statcounter.com/os-market-share/mobile/south-korea#monthly-202103-202103-bar>
- W3 schools, <https://www.w3schools.com/>
- MDN Web Docs, <https://developer.mozilla.org/ko/docs/Web/JavaScript>
- 남우환. (2019). 안드로이드 에뮬레이터에 대한 포렌식 기법. 디지털포렌식연구, 13(4), 303–316.,
<https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView,kci?sereArticleSearchBean.artid=ART002550554>
- <https://digitalis.postype.com/post/2290617>
- Digital Forensics Wikipedia,
http://forensic.korea.ac.kr/DFWiki/index.php/%EC%8A%A4%EB%A7%88%ED%8A%B8_%EA%B8%B0%EA%B8%B0_%EC%95%B1
- 김도현, 이상진. (2016). 모바일 포렌식 동향. 정보보호학회지, 26(5), 22–31.,
<https://scienceon.kisti.re.kr/srch/selectPORSrchArticle.do?cn=JAKO201633056056055>
- 나현대, 김창재, 이남용. (2014). 디지털 포렌식 인력 양성을 위한 단계별 대학 교과과정 설계에 관한 연구. 컴퓨터교육학회 논문지, 17(3), 75–84.,
<https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE07480412>

An illustration of a hand holding a black smartphone against a teal background. The hand is light-skinned with orange-tinted fingers. The person holding the phone is wearing a dark suit jacket with a white shirt cuff visible. The smartphone screen is white and displays the Korean text '감사합니다' (Thank you) in a large, bold, black font, and '2조 팀이름' (2nd Division Team Name) in a smaller, regular black font below it.

감사합니다

2조 팀이름