종합설계프로젝트2 11팀

디지털 포렌식

증거 시각화 프로젝트

디지털 기기는 당신의 모든 행동을 알고있다.

김예린 김경숙 이현섭 채한빈

팀원 업무 분장

beNX

김예린

- 전체 프로젝트 관리
- 시각화 UI/UX 연구 개발
- 논문 작성

김경숙

- 디스크 이미지 분석
- DB 연동
- 시각화 그래프 구현

강대명 멘토님

- beNX SW 엔지니어

이현섭

- 디스크 이미지 분석
- 타입 별 타임 스탬프 추출
- 논문 작성

채한빈

- DB 연동
- 시각화 그래프 구현
- 증거 Export 기능 구현

목차

1. 과제 수행 배경

Part 1

프로젝트 필요성

1 부족한 오픈소스 디지털 포렌식 툴

2 스토리지 대용량화에 따른 증거 수집 시간의 증대

3 선별수사 시 중요 데이터 수집 시간 단축의 필요성

4 수집된 메타데이터 시각화 제공으로 선별수사에 도움

Part 1

주제

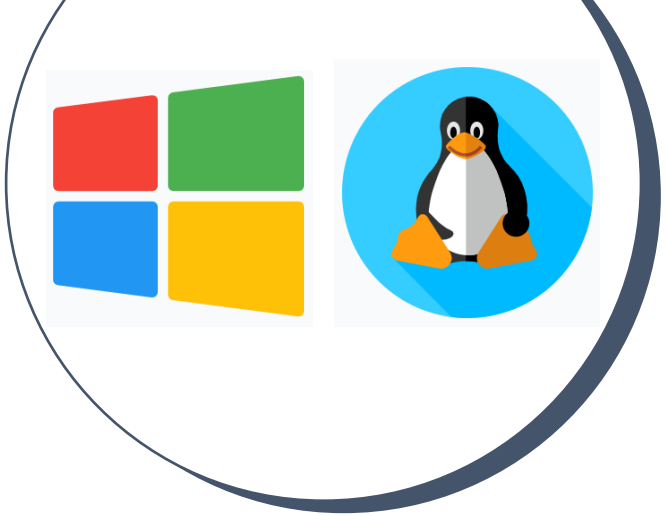
데이터 변화 추이나 접근 빈도와 같은 메타데이터를 **시각화** 하여 보여줌으로써 선별 압수 후 중요 데이터 수집 시 유용한 오픈소스 **디지털 포렌식 툴**

Part 1

목표

UI 구현을 통한 편리성

시각화 특화 도구



Portable한 툴

2. 과제 분석 및 설계 내용

Part 2

프로젝트 분석

1 레지스트리 하이브 파일 분석의 필요성

- 사용자 계정 정보, 시스템 정보, 응용프로그램 실행 흔적, 최근 접근 문서 등을 분석 가능
- 저장매체 사용 흔적 분석 (하드디스크, CD-ROM, USB 등)
- 시스템 안에서 파일이 변화된 모습을 보여줌

2 타임라인 분석

- 파일의 생성, 수정, 접근, 삭제 기록 등의 시간 정보 시각화
- 저장매체의 대용량화로 모든 파일의 시간 데이터를 일일이 확인하는 것이 불가능하기 때문에 한눈에 전체 시간 정보 확인이 가능한 기능이 요구됨

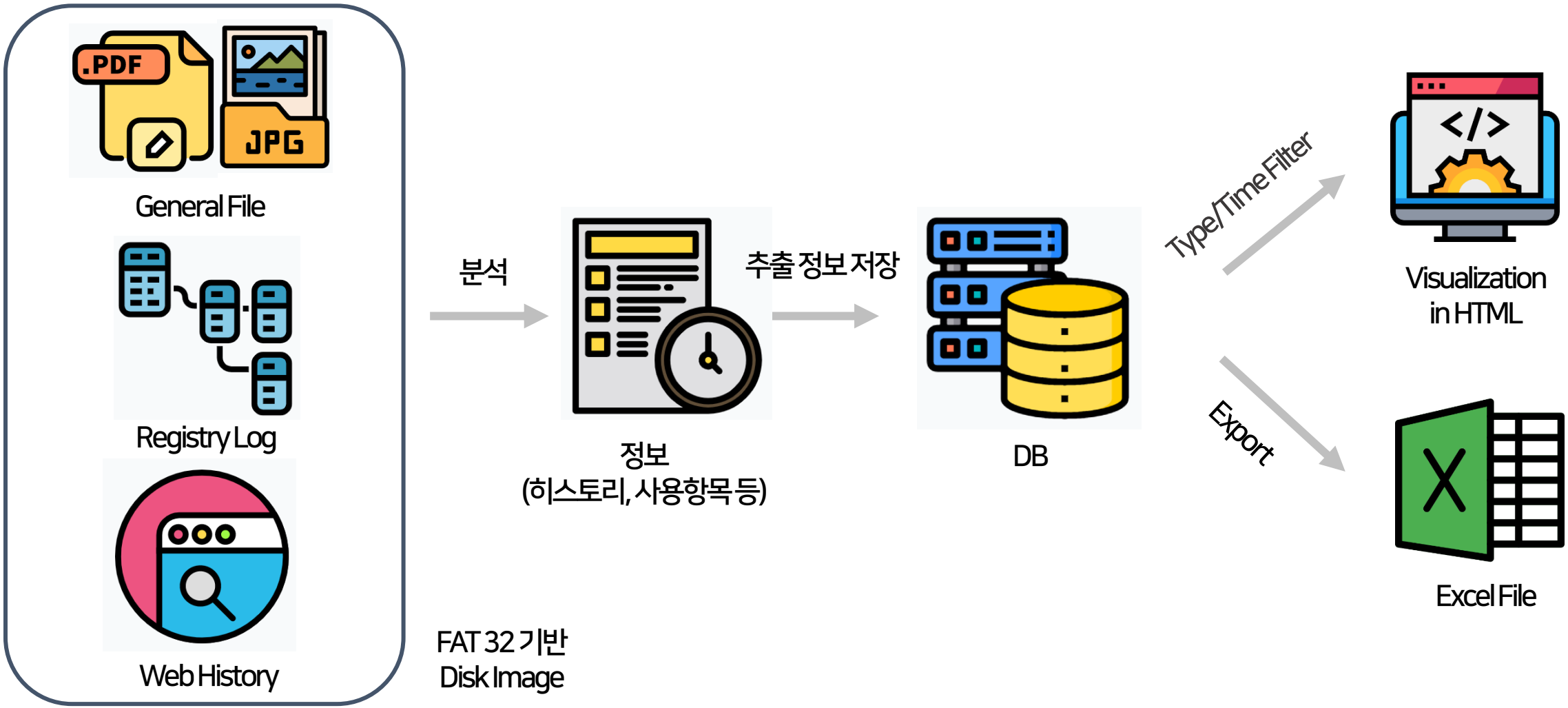
3 파일 정보 및 로그 분석

- 파일의 이름, 확장자, 크기, 위치 등의 세부 정보 제공
- 파일 변경 정보, 삭제 유무 등의 파일 로그 분석

Part 2

프로젝트 분석

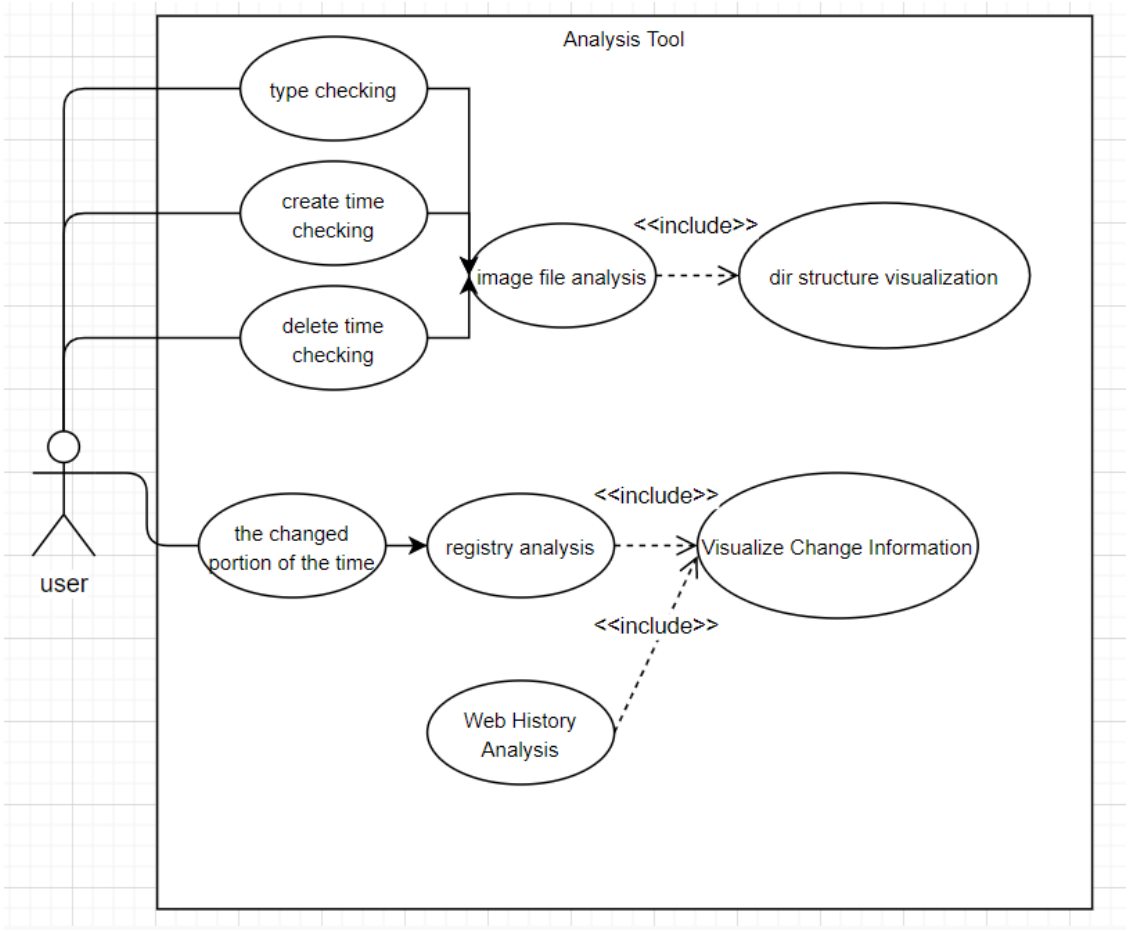
시스템 개요도



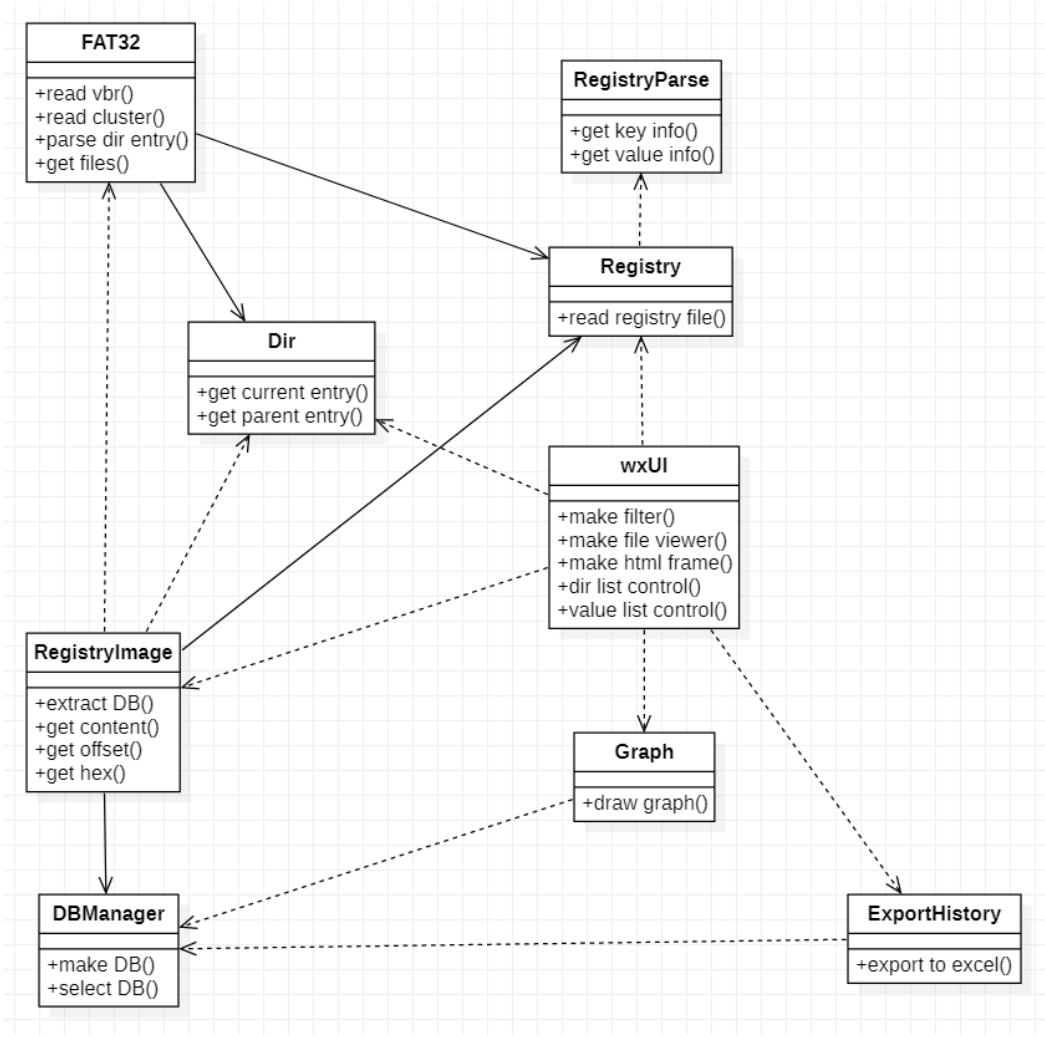
Part 2

프로젝트 설계

Use-Case Diagram



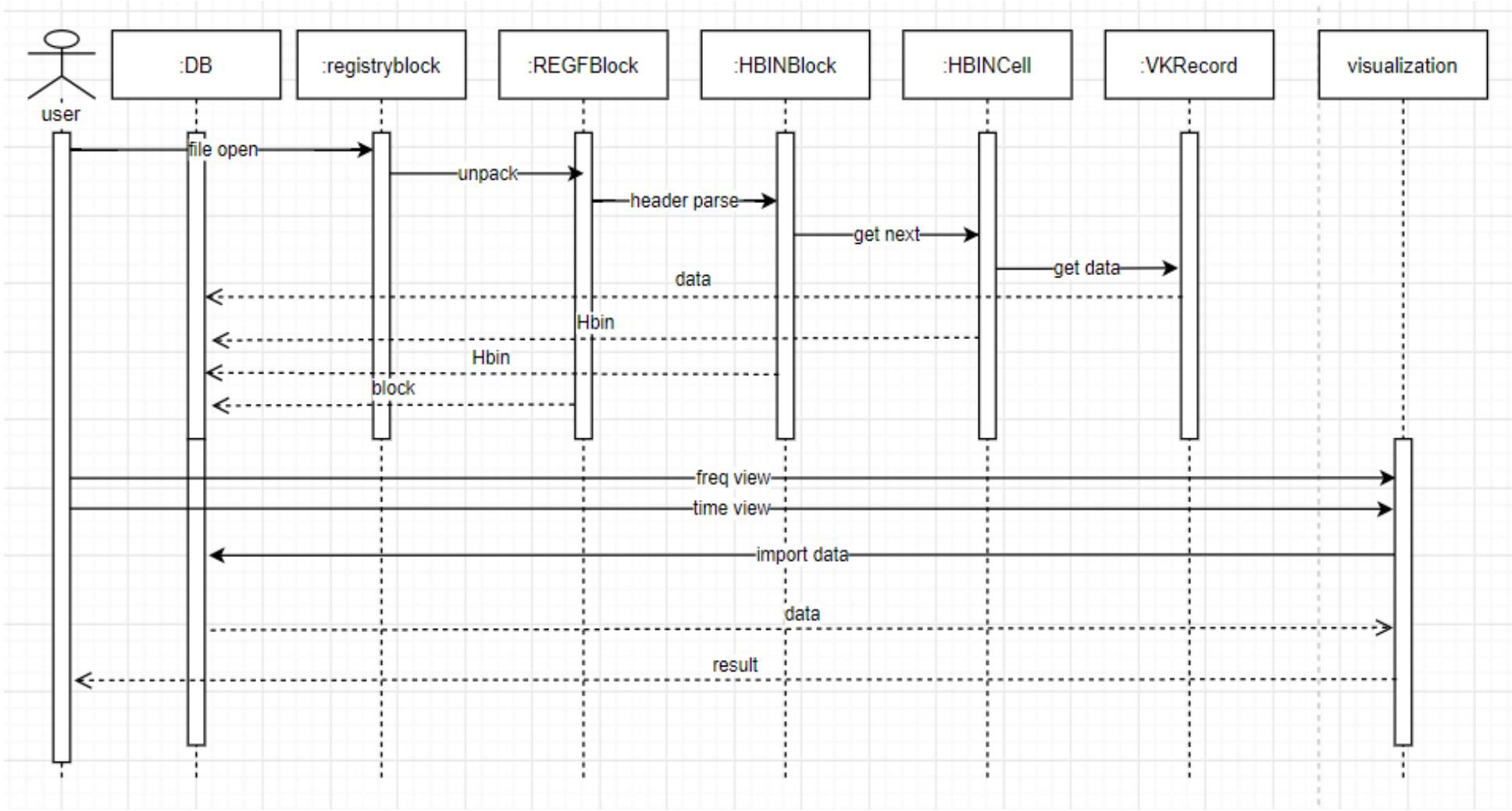
Class Diagram



Part 2

프로젝트 설계

Sequence Diagram – 하이브 파일 분석



3. 과제 수행 과정

Project Management Tool

Github	▪ 코드 공유 및 관리 ▪ 팀원 별 브랜치를 만들어 세부 기능 개발 후 병합하는 방식으로 구현 진행
Slack	▪ 멘토님과 정보 공유 ▪ 편한 자료 공유(ex. pdf 미리보기 기능)과 온라인 채팅기능 ▪ 일정 공유 가능
Hangout	▪ 서울에 계신 멘토님과 화상통화를 위해 사용 ▪ 오프라인 회의와 유사한 환경을 통해 회의의 quality 향상
Trello	▪ 월별 계획에 맞게 문서를 작성하여 올림 ▪ 업무의 진행상황을 정확하게 파악 할 수 있음

Part 3

프로젝트 환경 구축

1 프로젝트 환경

- 사용 OS : Windows
- 사용 언어 : Python
- UI : wx를 통해 제작

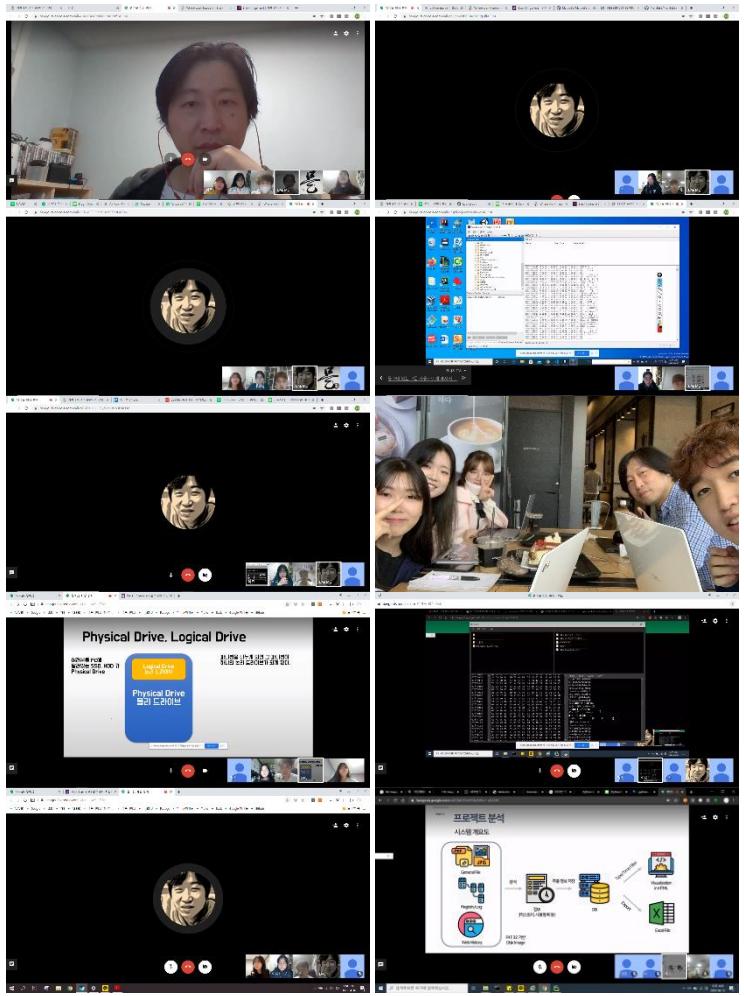
2 종합설계프로젝트 1 결과 기반 과제 진행

종합설계프로젝트1에서 개발한 FAT32 파일시스템 분석 툴을 기반으로 기존 툴에는 부족한 **시각화 기능**을 집중적으로 강화하여 디지털 포렌식 수사 시 더욱 효율적으로 증거 추출 및 정보 수집이 가능한 툴로 발전시키는 것이 이번 프로젝트의 목표입니다.

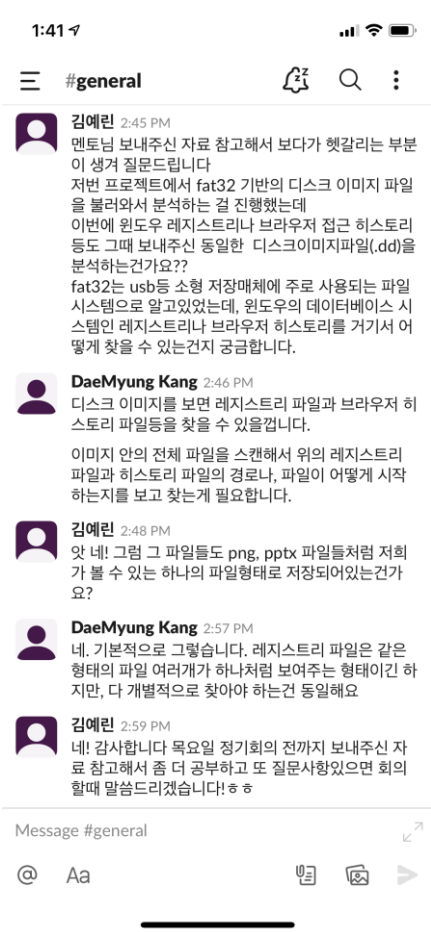
Part 3

멘토링

1 매주 목 PM 9:00 행아웃 + 오프라인 미팅



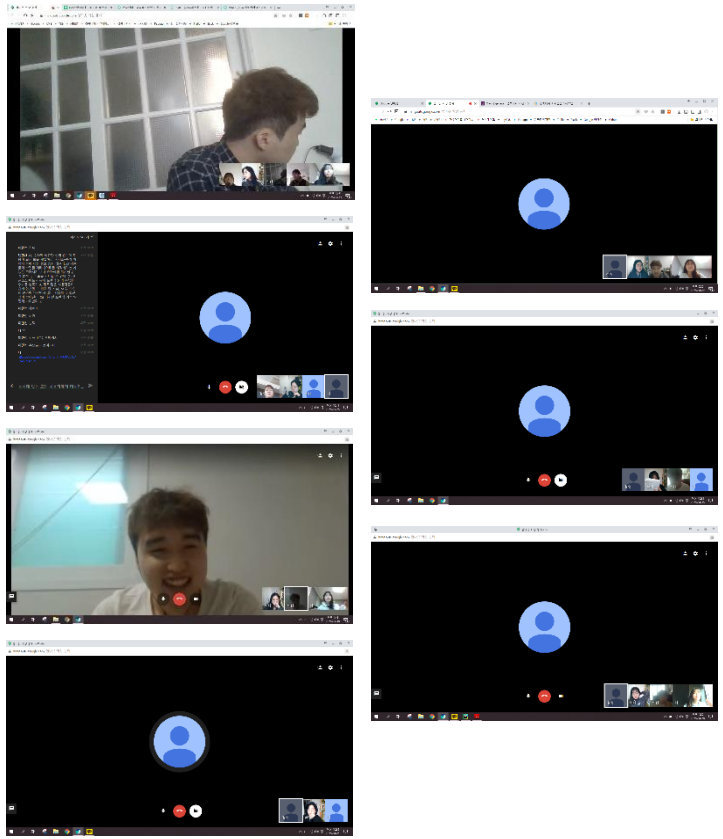
2 Slack



Part 3

팀원 회의

1 온라인 회의 (행아웃)

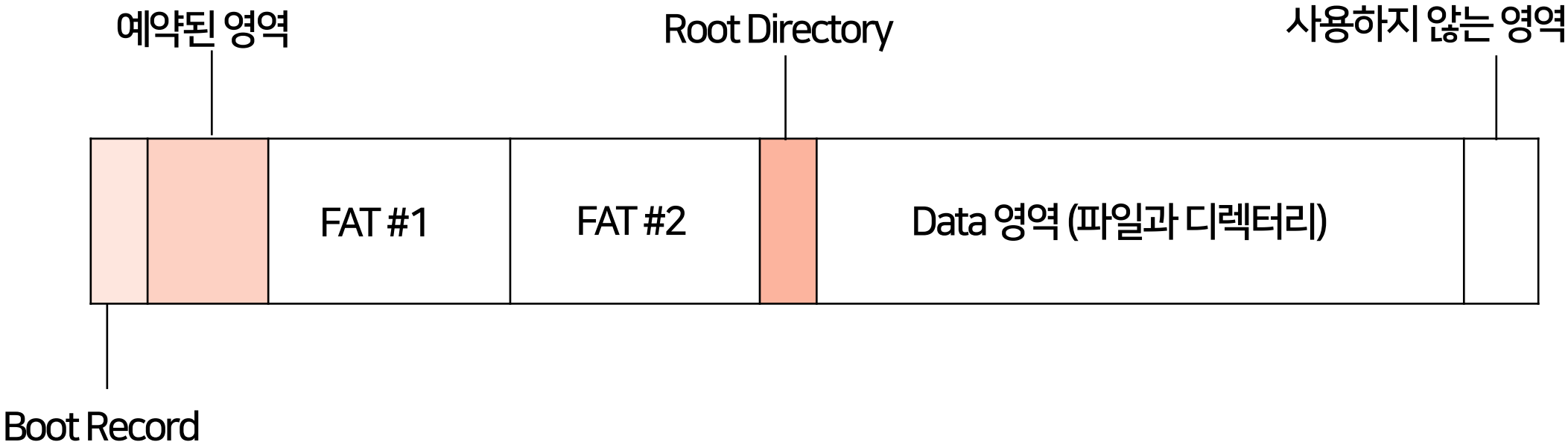


2 오프라인 회의 : 매주 월/수 AM 10:00

4. 과제 수행 결과

디스크 분석의 접근법

FAT32 파일 시스템 구조도



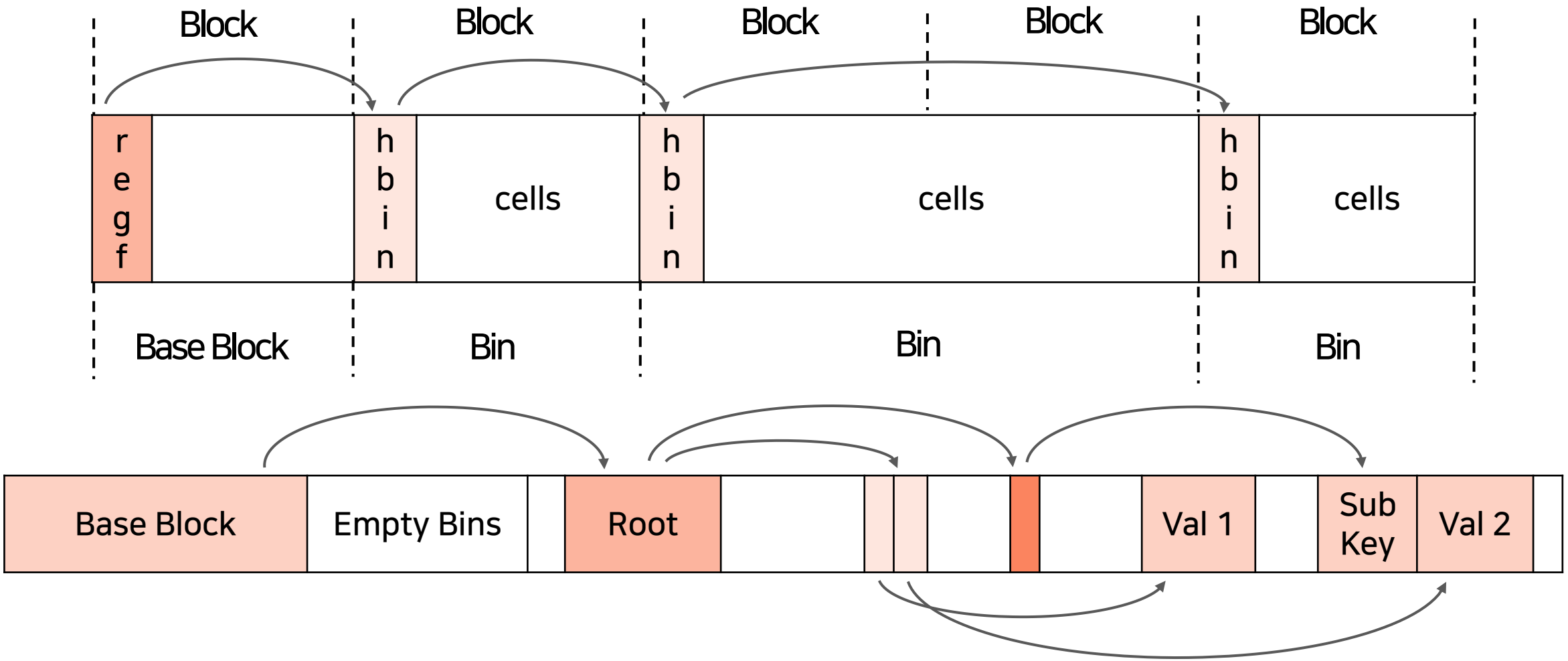
① VBR(Volume Boot Record) : 볼륨의 첫 번째 섹터에 해당하는 영역, FAT 파일시스템의 여러 설정 값 저장

② FAT 영역 : 클러스터(Linked List로 연결)들을 관리하는 테이블이 모여 있는 공간

③ Data 영역 : Directory Entry라 불리는 구조체들을 담고 있는 디렉터리와 파일 저장

레지스트리 정보 탐색 접근법

레지스트리(Registry) : 윈도우에서 사용하는 시스템 구성 정보를 저장한 데이터베이스



웹 히스토리 정보 탐색 접근법

웹 히스토리(Web History)

- 사용자의 검색기록, 방문 URL, 접속 시간 정보 추출
- 별도 분석 없이 윈도우 내 DB형태의 파일로 저장
- 인터넷 사용에 관한 빈도 시각화 제공

웹 브라우저	파일 위치
Chrome	C:₩Users₩[사용자이름]₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩
Whale	C:₩Users₩[사용자이름]₩AppData₩Local₩Naver₩Naver Whale₩User Data₩Profile 1₩
Internet Explorer	컴퓨터₩HKEY_CURRENT_USER₩Software₩Microsoft₩Internet Explorer₩TypedURLs
Firefox	C:₩Users₩[사용자이름]₩AppData₩Roaming₩Mozilla₩Firefox₩Profiles₩places.sqlite
Safari	~/Library/Safari/History.db

Part 4

주요 기능

1 디스크 이미지 구조 생성

디스크 이미지를 분석하고 저장

```
def tree_structure (self, cluster, parent):
    # TO GET OVERALL DIRECTORY TREE STRUCTURE
    data =self .get_content(cluster)
    for i in range (0, len(data), 32):
        # READ 32 BYTE
        attr =entry_data[11]
        is_LFN = attr & 0x0F == 0x0F
    if not is_LFN:
        # STORE
    else :
        # STORE PART
```

주요 기능

2 파일 및 value 정보 나열

분석한 디스크 이미지를 바탕으로
파일 및 value의 이름, 시그니처,
크기, 수정 날짜, 데이터 등을 제공

```
class RegistryFileView (wx.Panel):
    def __init__(self, parent, fileobj=None, filename=None):
        # UI
    def OnDirClicked (self, event):
        if directory:
            # READ VBR
        elif registry:
            # READ VALUE OF KEY
    def OnValueClicked (self, event):
        # UPDATE OFFSET AND HEX VIEW
    def print_hex_data (self, cluster):
        # DISPLAY HEX DATA
    def filename (self):
        # RETURN FILENAME
    def selected_path (self):
        # RETURN REGISTRY KEY PATH
    def select_path (self, path):
        # RETURN SPECIFIED REGISTRY KEY PATH
```

주요 기능

3 DB 관리

그래프 시각화와 파일 export에
필요한 데이터를 DB에 넣어 관리

```
class DBManager :
    def __init__(self, dbName):
        # CLASS COSTRUCTION
    def create_table (self, tableName):
        # GENERATE DB TABLE
    def drop_table (self, tableName):
        # DROP DB TABLE
    def insert_record (self, tableName, filename, type, key,
                       valType, valName, val, timeStamp, name,
                       ext, sig, size, create, write, access):
        # INSERT RECORDS INTO TABLE
    def order_by_date (self, tableName, date_from, date_to):
        # SELECT AND STORE RECORDS FOR DRAWING TIMELINE
        # RETURN RECORDS AS DICTIONARY TYPE
    def select_history (self, tableName, date_from, date_to):
        # SELECT AND STORE RECORDS FOR EXPORTING TO FILE
```

주요 기능

4 시각화

DBManager에서 받은 History 데이터로 타임라인 그래프 생성

```
class Graph :
    def __init__(self, date_from, date_to):
        # GET DATA FROM DBManager.order_by_date()
    def get_total_key (self):
        # RETURN total_key_list
    def get_hive_key (self):
        # RETURN hive_key_list
    def get_general_key (self):
        # RETURN general_key_list
    def get_url_key (self):
        # RETURN url_key_list
    def create_list (self, tablename, listname):
        # RETURN value_list
    def draw_graph_html (self, name):
        # DRAW GRAPH ABOUT TOTAL SYSTEM ACCESS USING ‘plotly’
        # DRAW GRAPH USING value_list USING ‘plotly’
```

Part 4

주요 기능

5 파일 export

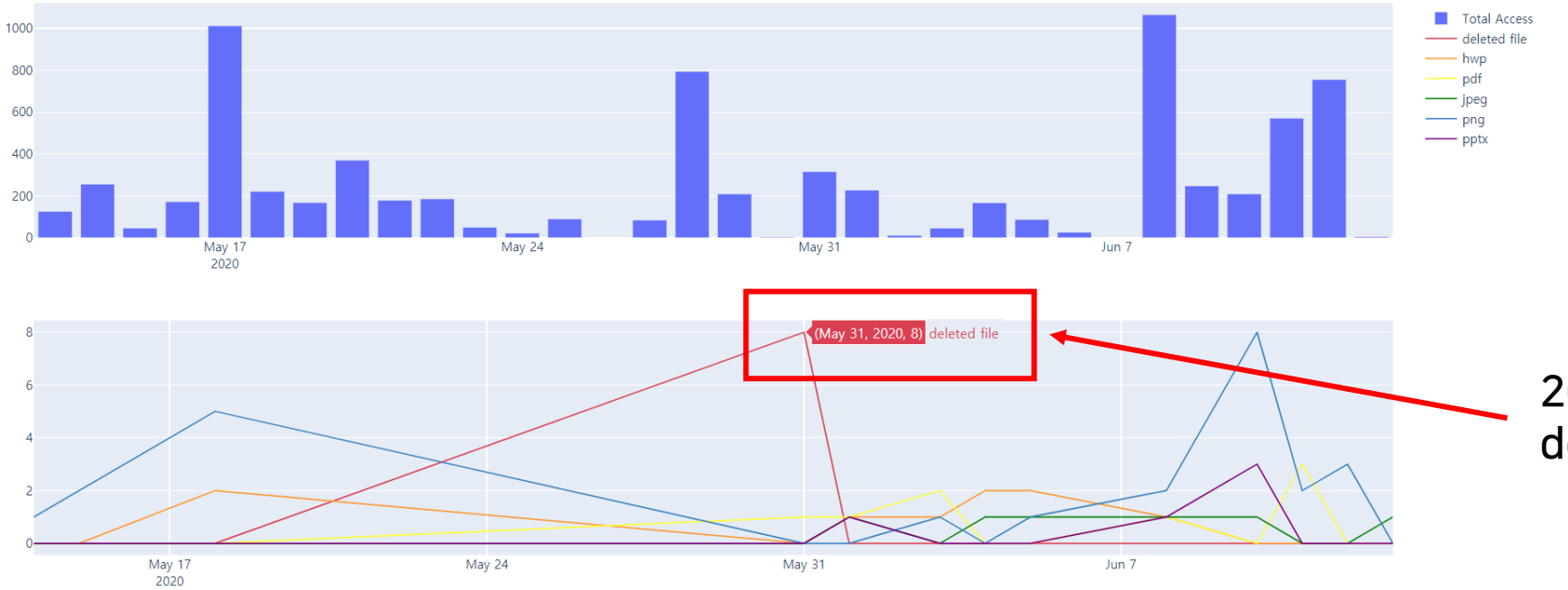
DBManager에서 받은 History
데이터를 엑셀 파일로 추출 및 저장

```
class ExportHistory :
    def __init__(self, tableName, date_from, date_to):
        # GET DATA FROM DBManager.select_history()
    def hiveExport2Excel (self, hive):
        # WRITE REGISTRY HISTORY TO EXCEL USING ‘openpyxl’
    def generalExport2Excel (self, general):
        # WRITE FILE HISTORY TO EXCEL USING ‘opnepyxl’
    def urlExport2Excel (self, chrome, whale):
        # WRITE URL HISTORY TO EXCEL USING ‘opnepyxl’
```

Part 4

실행 시나리오

1 회사 기밀 정보를 외부로 유출한 채모씨 2020-05-13 ~ 2020-06-13 General File 접근 기록을 조사



2020-05-31에 대량의 deleted file 발생 확인

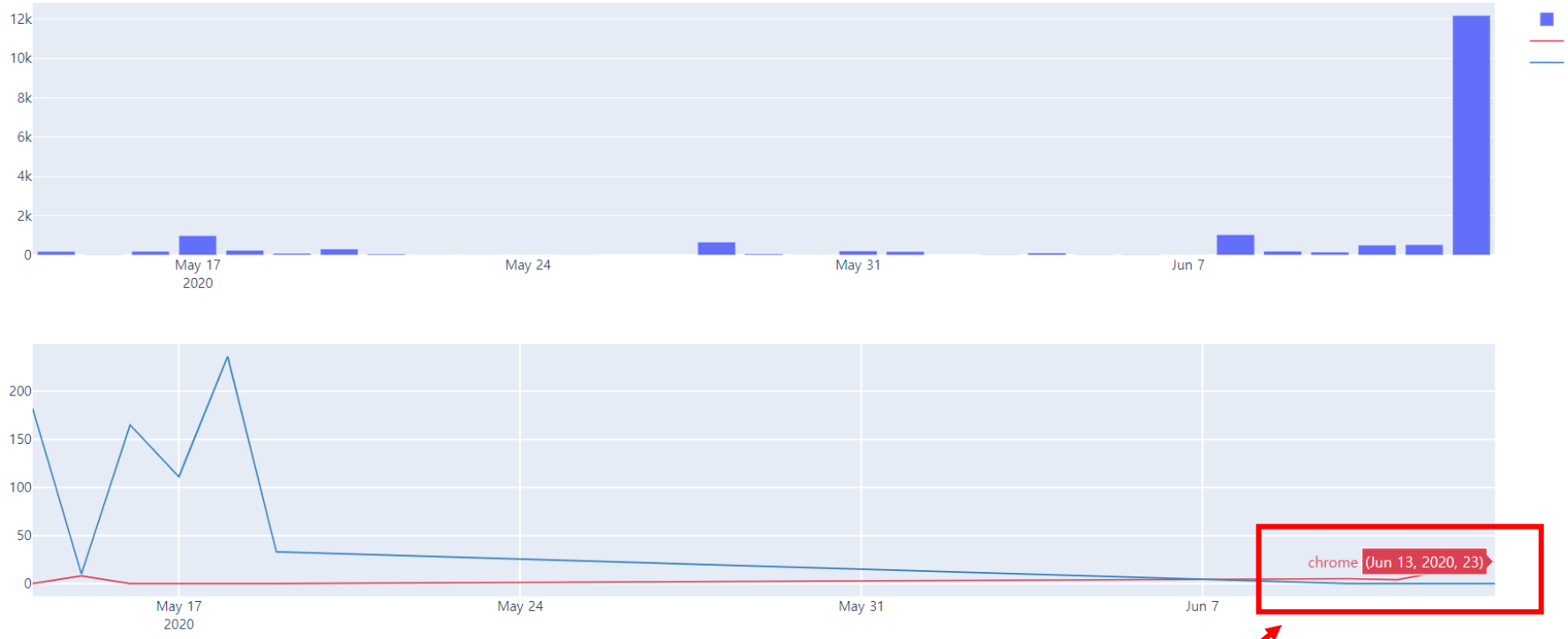
KakaoTalk_20200530_162337089	JPG	deleted file	29999	2020-05-3	2020-05-31 20:04:22	2020-05-31 20:04:22
KakaoTalk_20200530_162337089_01	JPG	deleted file	28168	2020-05-3	2020-05-31 20:04:56	2020-05-31 20:04:56
KakaoTalk_20200530_162337089_02	JPG	deleted file	24662	2020-05-3	2020-05-31 20:05:08	2020-05-31 20:05:08
KakaoTalk_20200530_162337089_03	JPG	deleted file	17834	2020-05-3	2020-05-31 20:05:21	2020-05-31 20:05:21
KakaoTalk_20200530_162337089_04	JPG	deleted file	37068	2020-05-3	2020-05-31 20:05:35	2020-05-31 20:05:35
KakaoTalk_20200530_162337089_05	JPG	deleted file	20834	2020-05-3	2020-05-31 20:05:46	2020-05-31 20:05:46
KakaoTalk_20200530_162337089_06	JPG	deleted file	16824	2020-05-3	2020-05-31 20:05:59	2020-05-31 20:05:59
KakaoTalk_20200530_162337089_07	JPG	deleted file	23577	2020-05-3	2020-05-31 20:06:13	2020-05-31 20:06:13

- 해당 기간 동안의 General File 접근 기록을 Export하여 조사한 결과, 카카오톡을 통해 여러 장의 이미지(JPG)를 전송 후 삭제했을 것으로 추측 가능

실행 시나리오

2 텔레그램을 통해 불법 음란물 유포에 가담한 김모씨

2020-05-14 ~ 2020-06-14 Web History 접근 기록을 조사



2020-06-13에 갑자기
Chrome 사용량 증가 확인

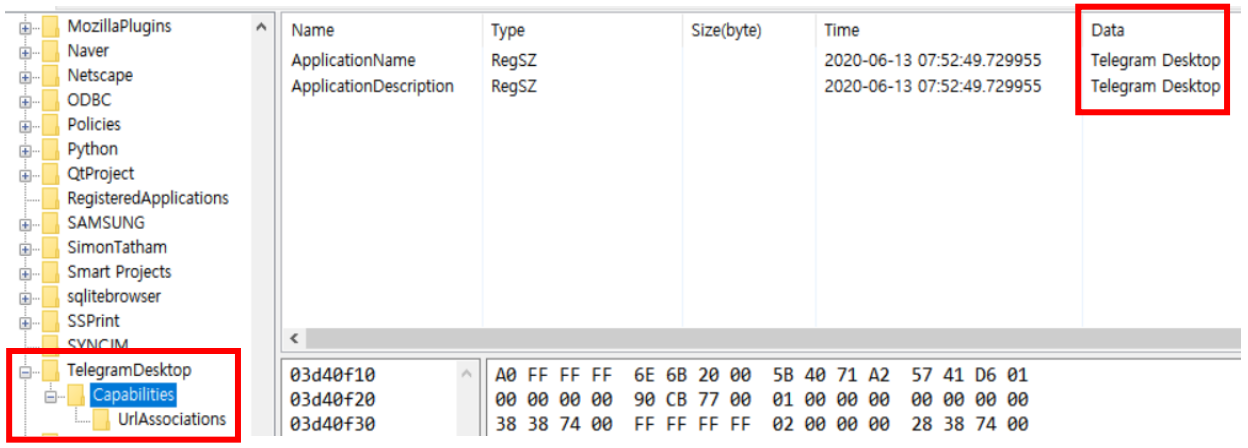
실행 시나리오

2 텔레그램을 통해 불법 음란물 유포에 가담한 김모씨

https://www.google.com/search?q=%ED%8	텔레그램 - Google 검색	2020-06-13 16:46:43
https://www.google.com/search?sxsrf=AL	텔레그램 다운로드 - Google 검색	2020-06-13 16:48:02
http://www.telegram.pe.kr/	텔레그램 한글사이트	2020-06-13 16:50:58
http://155.230.124.241/CPopupRequest	TA-PRS itstation	2020-06-13 16:46:49
http://www.telegram.pe.kr/index.php#t002	텔레그램 한글사이트	2020-06-13 16:50:30
http://www.telegram.pe.kr/index.php#t001	텔레그램 한글사이트	2020-06-13 16:51:39
https://www.google.com/search?sxsrf=AL	텔레그램 삭제 - Google 검색	2020-06-13 16:48:21
https://www.google.com/search?sxsrf=AL	텔레그램 삭제 방법 - Google 검색	2020-06-13 16:48:21
https://m.blog.naver.com/skdaksdptn/221	텔레그램 탈퇴 및 계정 삭제 방법 너무 쉽죠! : 네이버 블로그	2020-06-13 16:49:43
https://prolite.tistory.com/1464	텔레그램 탈퇴 계정 삭제하는 방법입니다.	2020-06-13 16:48:17
https://www.google.com/search?sxsrf=AL	텔레그램 계정 탈퇴 - Google 검색	2020-06-13 16:48:38
https://itons.net/%ED%85%94%EB%A0%8	텔레그램 탈퇴 계정 삭제하는 방법 Telegram Secession - 아	2020-06-13 16:48:30
https://ungdoli0916.tistory.com/274	(웅팁꿀팁) 텔레그램 1분 만에 탈퇴하는 방법 (웹/모바일)	2020-06-13 16:48:37
https://www.google.com/search?sxsrf=AL	텔레그램 기록 삭제 - Google 검색	2020-06-13 16:48:54
https://www.edaily.co.kr/news/read?newsI	"텔레그램 기록 지워지나요?"...쥐구멍 찾는 'n번방' 이용자들	2020-06-13 16:48:45
https://m.blog.naver.com/deadspirit13/22	텔레그램 탈퇴방법, 계정과 기록삭제 : 네이버 블로그	2020-06-13 16:48:51
https://my.telegram.org/auth?to=delete	Authorization	2020-06-13 16:48:52
https://www.google.com/search?sxsrf=AL	텔레그램 무료방 - Google 검색	2020-06-13 16:49:00
https://www.google.com/search?sxsrf=AL	텔레그램 회원탈퇴 - Google 검색	2020-06-13 16:49:43
https://blog.naver.com/PostView.nhn?blog	[Telegram] 텔레그램 탈퇴 / 계정삭제 방법(초간단!) : 네이버	2020-06-13 16:49:18
https://www.google.com/search?sxsrf=AL	텔레그램 - Google 검색	2020-06-13 16:49:47
http://www.telegram.pe.kr/?c=2	텔레그램 한글사이트 - 텔레그램 자주묻는질문(FAQ)	2020-06-13 16:50:02
http://www.telegram.pe.kr/index.php#t003	텔레그램 한글사이트	2020-06-13 16:50:47

- 해당 기간 동안의 Web History 접근 기록을 Export 하여 조사한 결과, 텔레그램 삭제 및 계정 탈퇴에 관한 검색을 한 기록이 확인
- 최근 이슈 된 텔레그램 N번방 사건과 관련하여 불법 음란물 유포에 가담하고 처벌이 두려워 계정 삭제를 하려한 정황을 짐작 가능

- 레지스트리에 텔레그램 프로그램 관련 기록이 남아 있는 것으로 보아 텔레그램을 사용했다고 추측 가능



Part 4

실행 동영상

5. 주요산출물

Part 5

주요 산출물

2020년 국제문화기술진흥원 국내 학술대회 논문집

디지털 포렌식 증거 시각화 방안

Digital Forensics Evidence Visualization Plan

김예린, 김경숙, 이현섭, 채한빈*, 고석주**, 강대명***

Ye-Rin Kim, Kyung-Sook Kim, Hyun-Sub Lee, Han-Bin Chae*,
Seok-Joo Koh**, Dae-Myeong Kang***

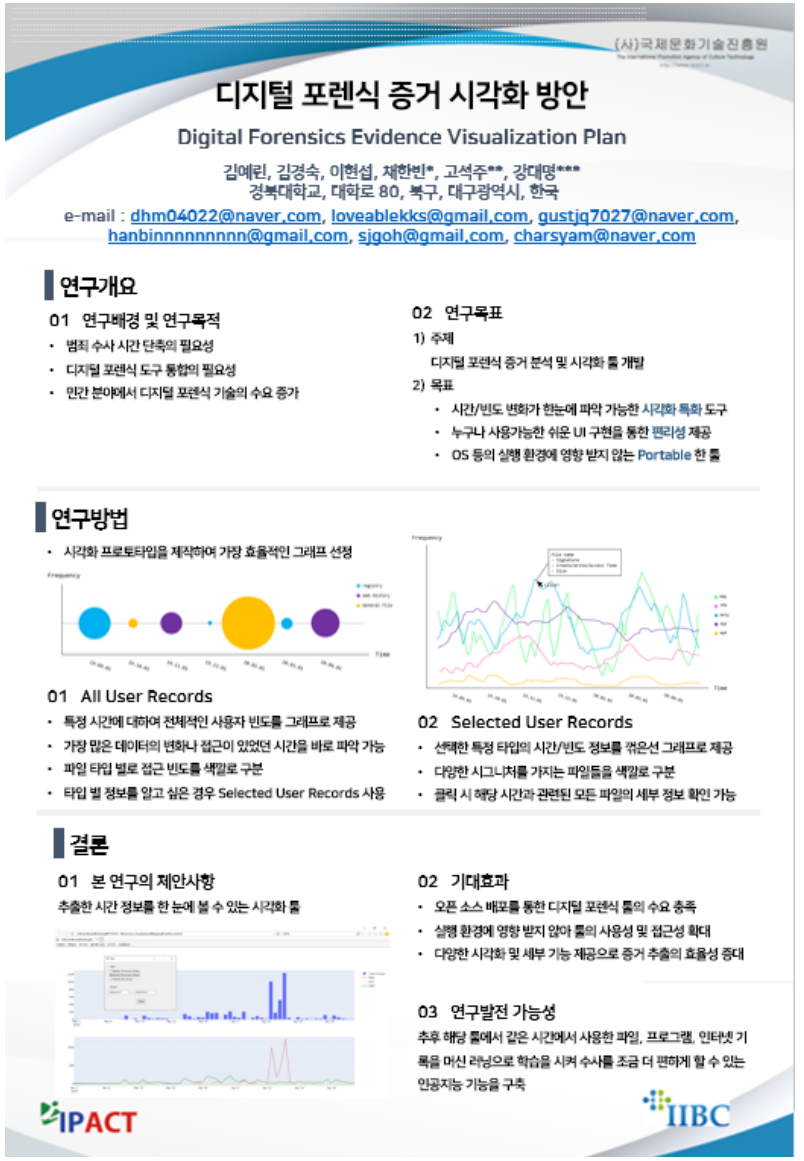
dhm04022@naver.com, lovablekks@gmail.com, gustjq7027@naver.com, hanbinnnnnnnnn@gmail.com,
sjkoh@gmail.com, charsyam@naver.com

요 약

스토리지의 대용량화가 점점 진행되고, 국내법에 따른 선별수사 정책에 따라 실제 압수 시에 필요한 데이터를 찾는데 시간을 줄이는 것이 중요한 시대가 되었다. 하지만 아직 오픈소스 디지털 포렌식 툴은 현저히 부족하고, 기존의 툴은 분석의 효율성과 접근성이 떨어져 여러 문제가 있다. 이에 본 논문은 FAT32 파일시스템 기반의 디스크 이미지를 분석하여 레지스트리, 웹 히스토리, 이미지, 문서 등과 같은 파일의 세부 정보를 추출하여 사용자에게 필요한 정보를 시각화를 통해 직관적으로 제공하는 것을 목표로 한다. 이를 위해 PyQt와 wx를 사용한 UI 구현을 통해 특정 시간대에 변화되거나 접근된 파일들의 접근 빈도 등을 보여줌으로써, 선별 압수 시에 도움이 되는 기능을 제공한다. 또한 수사 단계에서 사용자 행위 분석 시 효율성 증대를 위하여 다양한 프로토타입을 만들어 비교하는 단계를 거쳐 가장 효과적인 시각화 툴을 연구 개발 하였다.

IPACT 2020 국내학술대회 참가

- 2020.06.26 한국과학기술회관 강남



6. 기대효과

기대효과

1 선별 수사에 도움 제공

- 수사에 필요한 선별 압수 시 도움이 되는 툴 개발로 수사에 도움 제공
- 조사 목적에 따른 시각화 방법 적용으로 효율적인 디지털 증거 분석 기능 제공
- 사용자의 정보처리능력 향상으로 빠른 시간 내 많은 데이터 분석 가능

2 부족한 포렌식 툴 수요 충족

- 시각화가 특성화 된 포렌식 툴의 부족한 수요 충족
- 오픈 소스로 공개하여 누구나 포렌식 툴을 사용할 수 있도록 함

3 시각화 특화 포렌식 기술 발전 기여

- 데이터를 시각화 하는 Graph Theory 분야 중 포렌식 특화 시각화 기법은 미흡
- 이와 관련된 기술 발전에 기여 가능

감사합니다