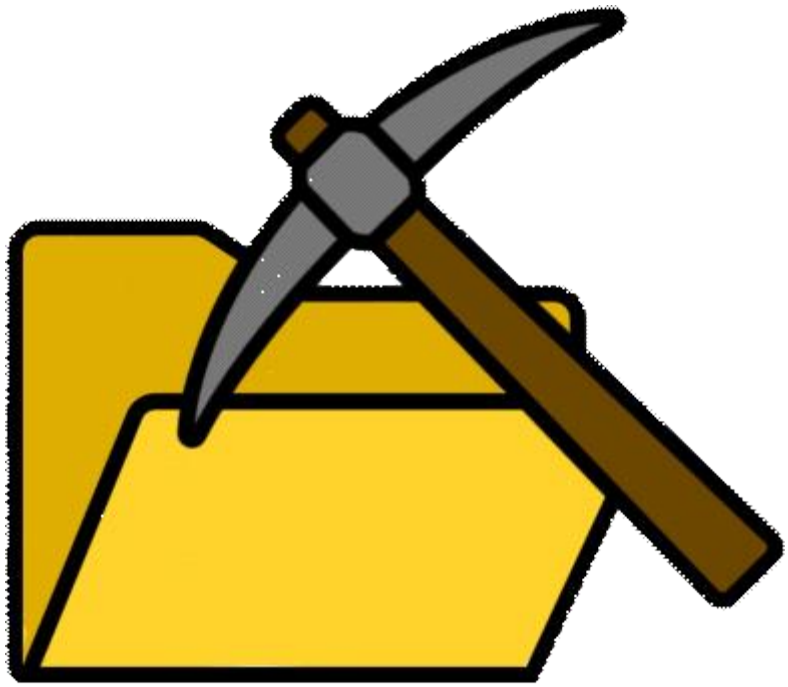
Yeungnam University

SysMiner

-Design-



Student No	22112133
Name	서주형
Email	blane7777@naver.com

[Revision history]

Revision date	Version #	Description	Author
2025/05/19	1.0.0	초기 버전	서주형
2025/06/15	1.0.1	기능 추가 및 최신화	서주형

= Contents =

1. Introduction

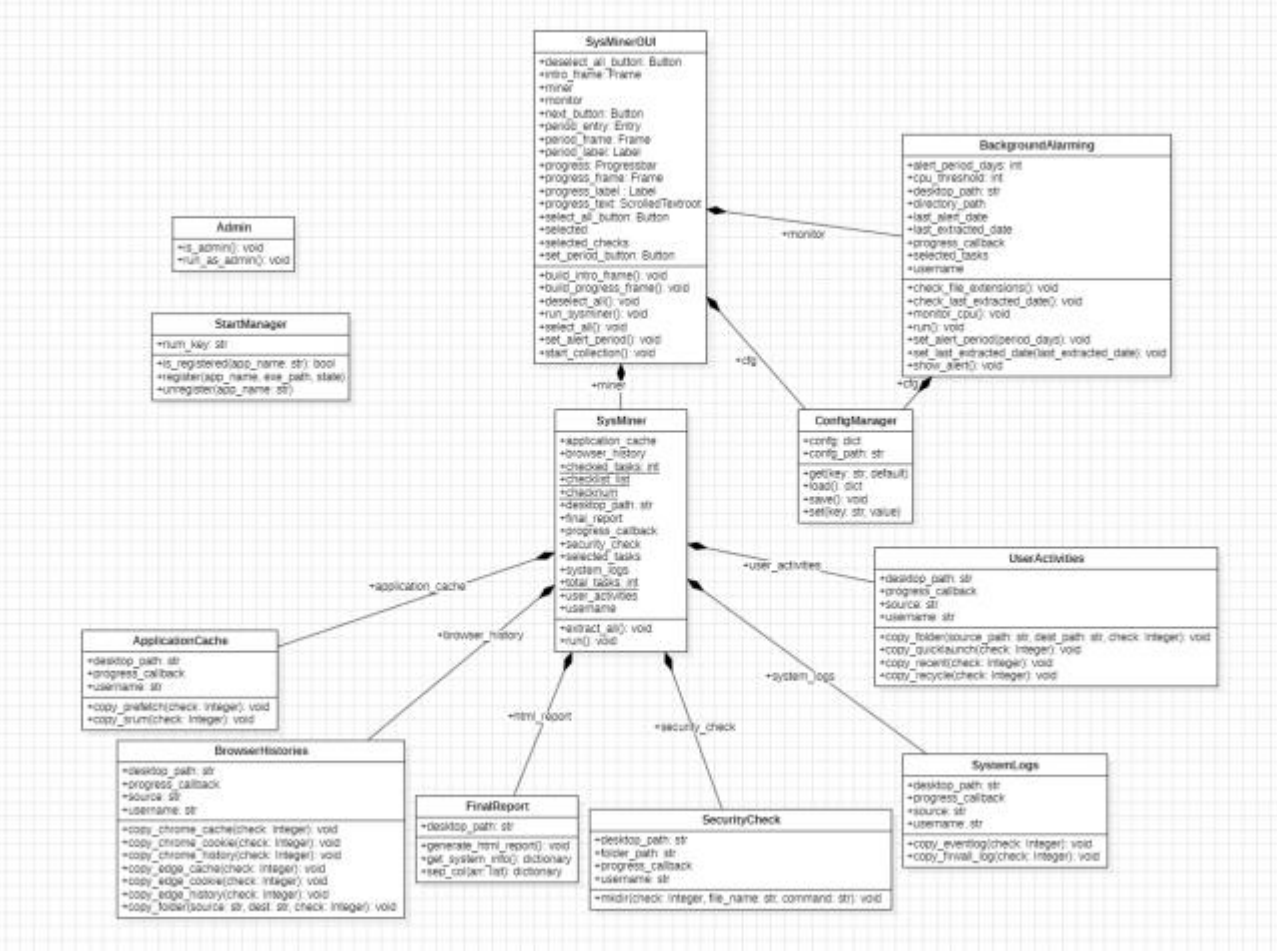
인터넷 기술이 많이 발달한 지금, 그만큼 많은 침해사고가 발생하고 있다. 침해사고의 문제점은 행위 자체에 관한 문제도 있지만, 침해사고 발생 시 복구가 어려우며 컴퓨터 공학에 대해 무지한 일반 사람들은 대처하는 방법에 대해서도 알지 못한다. 또한, 침해사고는 발생 전 사전예방과 발생 후 초기 대응이 중요한데, 예방 혹은 초기 대응을 어떻게 해야하는 지에 대해 무지한 사람들이 많다. 따라서 컴퓨터공학에 대해 무지한 사람들도 침해사고를 사전에 예방하도록 또, 발생 후 초기에 대응할 수 있도록 도와주는 “SysMiner”를 개발하게 되었다.

이 프로그램이 이루고자하는 첫 번째 목표는 신속하게 초기에 대응할 수 있도록 하는 것이다. 침해사고 발생 후, 정보가 더욱 손상되고 잠기기 전에 최대한 빠르게, 간편하게 몇 번의 클릭만으로 컴퓨터 정보를 수집할 수 있도록 도와준다. 또한 발생 전에는 주기적으로 컴퓨터의 상태를 백업할 수 있도록 도와주며, 사용자가 잊고 백업한 지 오랜 시간이 지나면 프로그램이 알람 문구를 띄워주는 등의 도움을 준다. 정보를 추출한 후, 추출된 정보를 한 곳에 모아주고, 결과 창을 띄워 추출 결과물에 대한 쉬운 관리와 접근이 가능하도록 한다.

아래 내용들은 “SysMiner”의 개발 전 Design에 관한 내용으로, “SysMiner” 구현에 직접적으로 관여하는 요소들의 관계를 정리하고, 구체적으로 프로그램이 제공하는 기능이 어떻게 동작하는지에 관한 내용을 다루고 있다.

2. Class diagram

아래 그림은 시스템을 Class Diagram으로 나타낸 그림이다.



아래 표는 위 Class Diagram의 각 클래스들에 대한 설명이다.

Class Name	Explanation
SysMiner	메인 컨트롤러 클래스, 사용자 경로를 설정하고 하위 수집 클래스들을 초기화하며, 선택된 작업들을 실행한다. - extract_all(): 체크된 수집 항목에 따라 각 기능별 클래스의 복사 기능을 실행한다. - run(): 전체 수집을 실행한 뒤, FinalReport를 통해 리포트를 생성한다.

BrowserHistories	Chrome/Edge의 방문기록, 쿠키, 캐시 데이터를 사용자 데스크탑 경로로 복사하는 기능을 담당한다. - copy_chrome_cache(check: Integer): 크롬의 캐시 파일들을 복사한다. - copy_chrome_cookie(check: Integer): 크롬의 쿠키 DB를 복사한다. - copy_chrome_history(check: Integer): 크롬브라우저의 히스토리 DB를 지정된 폴더로 복사한다. - copy_edge_cache(check: Integer): 엣지의 캐시 파일들을 복사한다. - copy_edge_cookie(check: Integer): 엣지의 쿠키 DB를 복사한다. - copy_edge_history(check: Integer): 엣지 브라우저의 히스토리를 복사한다. - copy_folder(source: str, dest: str, check: Integer): 복사하고자 하는 정보를 복사한다.
SystemLogs	윈도우 이벤트 로그 및 방화벽 로그 파일을 백업 경로로 복사하는 기능을 제공한다. - copy_eventlog(check: Integer): Windows 이벤트 로그 디렉토리를 전체 복사한다. - copy_firewall_log(check: Integer): 방화벽 로그와 이전 로그를 모두 복사한다.
ApplicationCache	Windows에서 실행된 앱 관련 캐시(Prefetch, SRUM)파일을 수집하는 기능을 제공한다. - copy_prefetch(check: Integer): 프리패치 폴더 전체를 복사한다. - copy_srum(check: Integer): SRU 데이터 디렉토리를 복사한다.

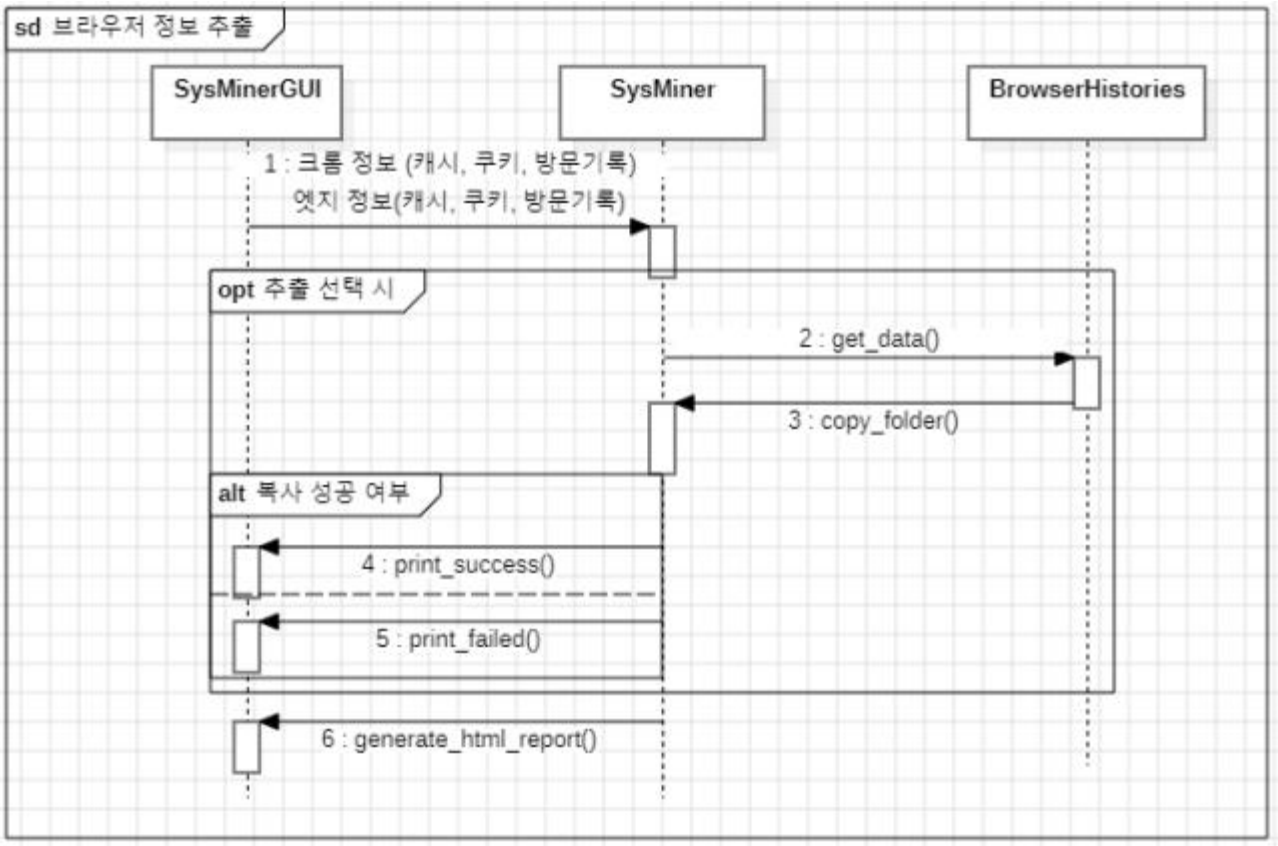
UserActivities	사용자의 작업 흔적(최근 문서, 바로가기, 휴지통 등)을 수집하는 클래스이다. - copy_folder(source_path: str, dest_path: str, check: Integer): 인자로 받은 source_path에 있는 폴더를 dest_path로 복사하는 기능이다. - copy_quicklaunch(check: Integer): 바로가기로 지정된 파일들을 모아놓은 폴더를 복사한다. - copy_recent(check: Integer): 최근 사용된 팡리 목록을 복사한다. - copy_recycle(check: Integer): 윈도우 휴지통 경로에서 데이터를 복사한다.
SecurityCheck	PowerShell 명령어를 이용해 보안 설정(방화벽, 업데이트, 비밀번호 정책 등)을 텍스트로 저장한다. - mkdir(check: Integer, file_name: str, command: str): command 인자로 들어온 명령어를 PowerShell 명령어로 실행시키고 결과를 파일로 저장한다.
FinalReport	시스템 정보 및 프로세스/포트 리스트를 분석하고 HTML 형식의 리포트를 생성하는 기능이다. - get_system_info(): systeminfo 명령과 psutil을 이용해 시스템 상태 및 프로세스를 수집한다. - generate_html_report(): 수집된 정보를 기반으로 HTML 리포트를 생성하고 저장한다. - sep_col(arr: list): systeminfo 명령어를 실행시킨 결과를 딕셔너리에 정보별로 저장하고, 그 딕셔너리를 반환한다.

BackgroundAlarming	CPU 사용률, 파일 확장자, 마지막 추출일 등을 주기적으로 감시하고 알람창을 띄우는 기능이다. - monitor_cpu(): 10분 단위로 CPU 사용률을 체크하고 임계치 초과 시 알림을 띄운다. - check_file_extension(): 감시 디렉토리 내 비정상 확장자 파일을 감지하면 경고 알림을 띄운다. - check_last_extracted_date(): 마지막 추출일 기준으로 경과일을 체크하고 설정한 기간보다 오래 지났다면 알림을 띄운다. - show_alert(): 사용자에게 알람을 띄운다. - set_last_extracted_date(): 사용자가 마지막으로 시스템 정보를 추출한 날을 저장한다. - set_alert_period(): 사용자가 지정한 알림 기간을 저장한다. - run(): CPU 사용률, 파일 확장자, 마지막 추출일 모니터링 기능을 각각 쓰레드로 실행한다.
Admin	프로그램이 관리자 권한으로 실행중인지 확인하고, 아니라면 권한 상승 요청을 수행하는 클래스이다. - is_admin(): 현재 사용자가 관리자 권한인지 확인한다. - run_as_admin(): 관리자 권한 실행이 아닐 경우 권한 상승을 요청하고 프로그램을 재실행한다.

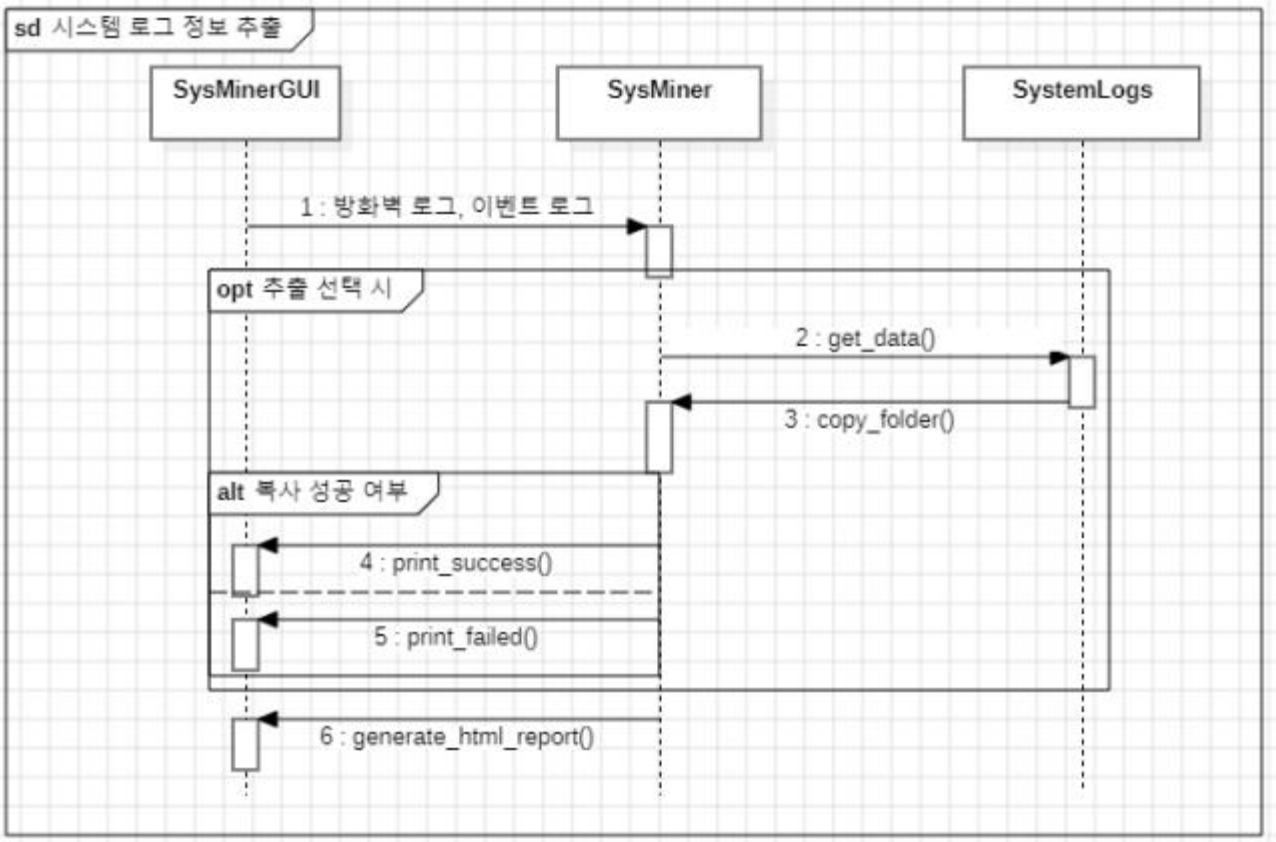
SysMinerGUI	시스템의 전체 GUI를 관리하며 사용자 선택 인터페이스, 프로그래스 바, 로그 출력을 관리하는 클래스이다. - build_intro_frame(): GUI 상단의 설명 영역과 체크리스트 구성 UI를 생성한다. - build_progress_frame(): 추출 시 올라가는 프로그래스 바 UI를 생성한다. - deselect_all(): 모든 정보의 체크를 풀어주는 버튼을 생성한다. - run_sysminer(): SysMiner클래스의 run() 메소드를 실행하고 완료 후 HTML 리포트를 자동으로 연다. - select_all(): 모든 정보를 체크하는 버튼을 생성한다. - set_alert_period(): 알림을 띄워주는 기간을 설정하도록 하는 공간을 생성한다. - start_collection(): 체크된 작업을 기반으로 수집을 시작하며, 쓰레드를 사용해 병렬처리하도록 한다.
ConfigManager	사용자가 설정한 기한을 유지할 수 있도록 별도로 json 파일에 저장해놓고, 프로그램이 실행될 때마다 정보를 읽어오도록 한다. - load(): 저장된 json 파일을 불러온다. - save(): json 파일에 바뀐 설정을 저장한다. - get(): json 파일의 key에 저장된 값을 불러온다. - set(): json 파일의 key에 새로 값을 저장한다.
StartManager	사용자가 자동 검사 버튼 체크시, 윈도우 시작프로그램으로 등록해주는 클래스이다. - is_registered(): 현재 시작프로그램으로 등록되어있는지 확인한다. - register(): 시작프로그램애 등록한다. - unregister(): 사용자가 체크를 해제하면 시작프로그램에서 제거한다.

3. Sequence diagram

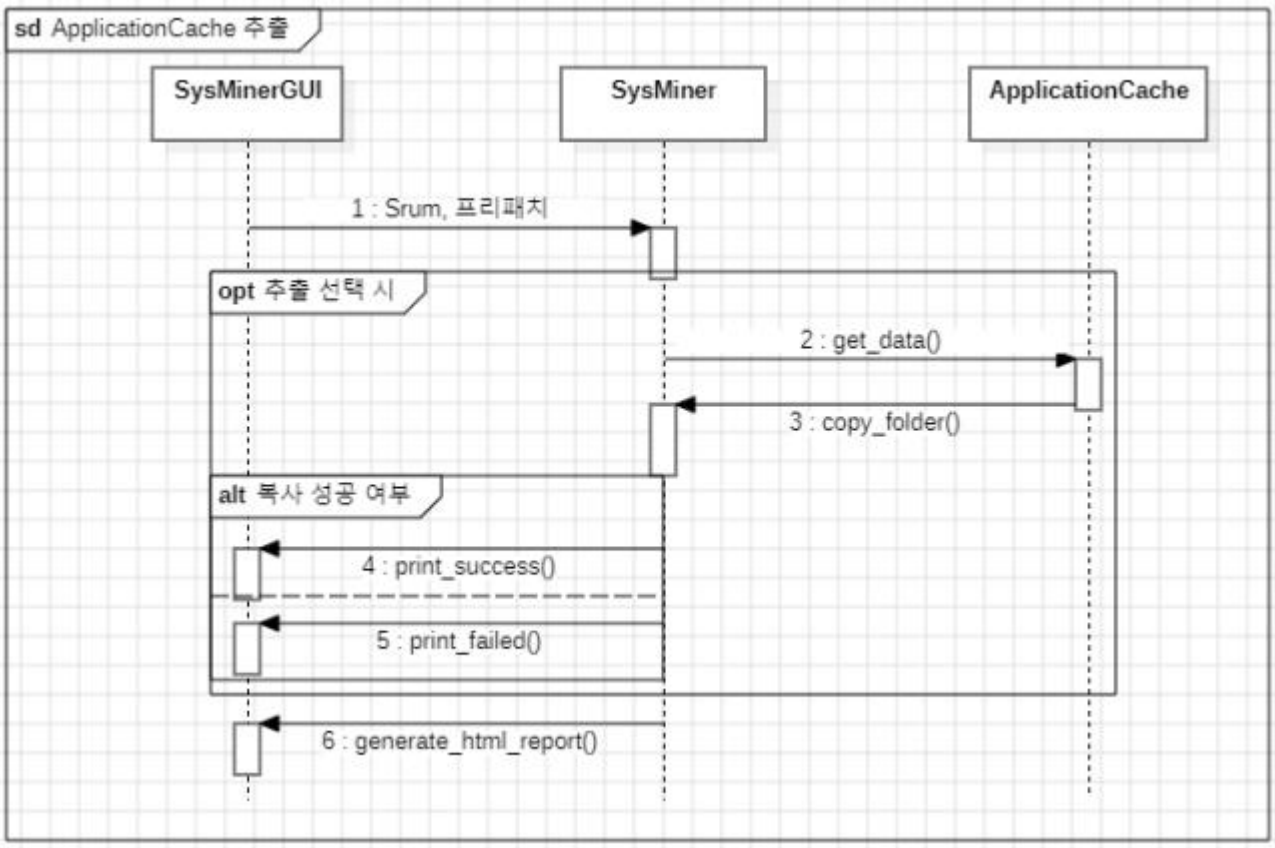
아래 나오는 그림들은 Conceptualization에서 표현한 기능들을 Sequence Diagram으로 표현한 그림들이다.



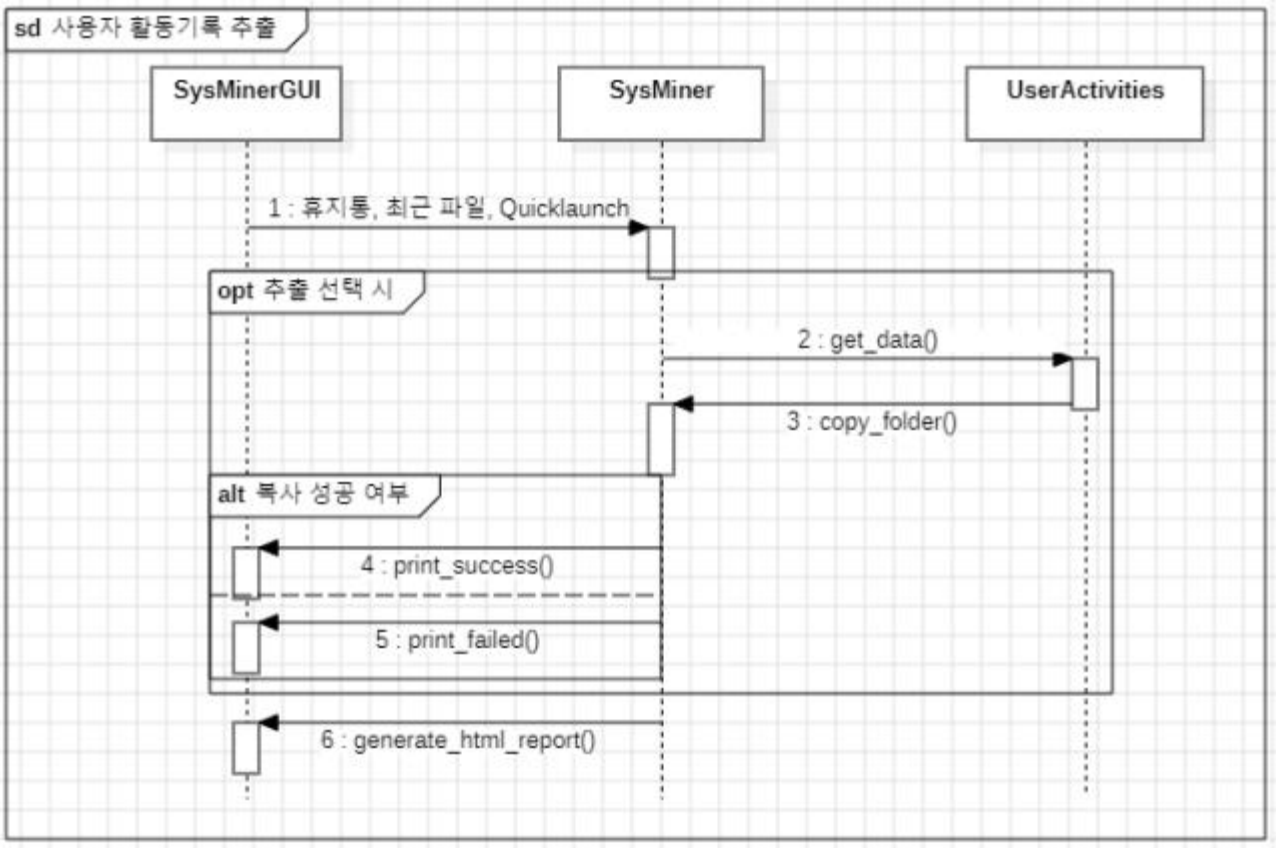
위의 그림은 시스템 실행 후 “크롬 캐시”, “크롬 쿠키”, “크롬 방문기록”, “엣지 캐시”, “엣지 쿠키”, “엣지 방문기록” 기능을 수행할 때를 표현한 Sequence Diagram이다. 위 6개의 목록 중, 체크된 정보들 각각은 get_data()를 통해 폴더 혹은 파일 위치를 찾고 copy_folder()를 통해 바탕화면의 “Data_Hub” 폴더에 모이게 된다. 만약 추출에 성공했다면 GUI에 print_success()를 하고, 실패했다면 print_failed()를 실행한다. 후에 generate_html_report()를 통해 결과를 html로 저장한 파일을 생성한다.



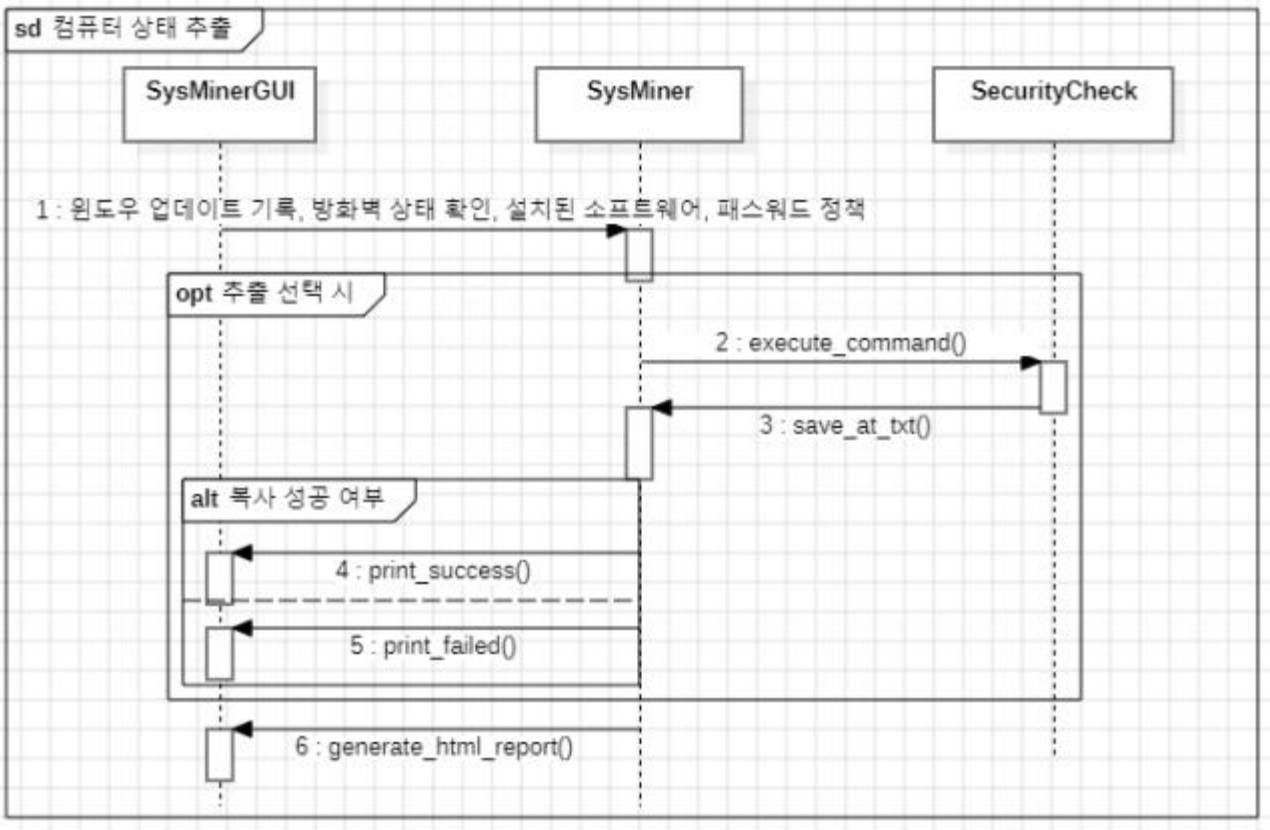
메인 메뉴에서 “방화벽 로그”, 혹은 “이벤트 로그” 정보를 선택했을 때를 표현한 Sequence Diagram이다. 두 개의 목록 중, 체크된 정보들은 get_data()를 통해 파일 혹은 폴더의 위치를 찾고 바탕화면의 “Data_Hub” 폴더에 저장된다. 추출에 성공했을 경우 GUI에 print_success()를 수행하고, 실패했다면 print_failed()를 수행한다. 후에 generate_html_report()를 통해 결과를 html로 저장한 파일을 생성한다.



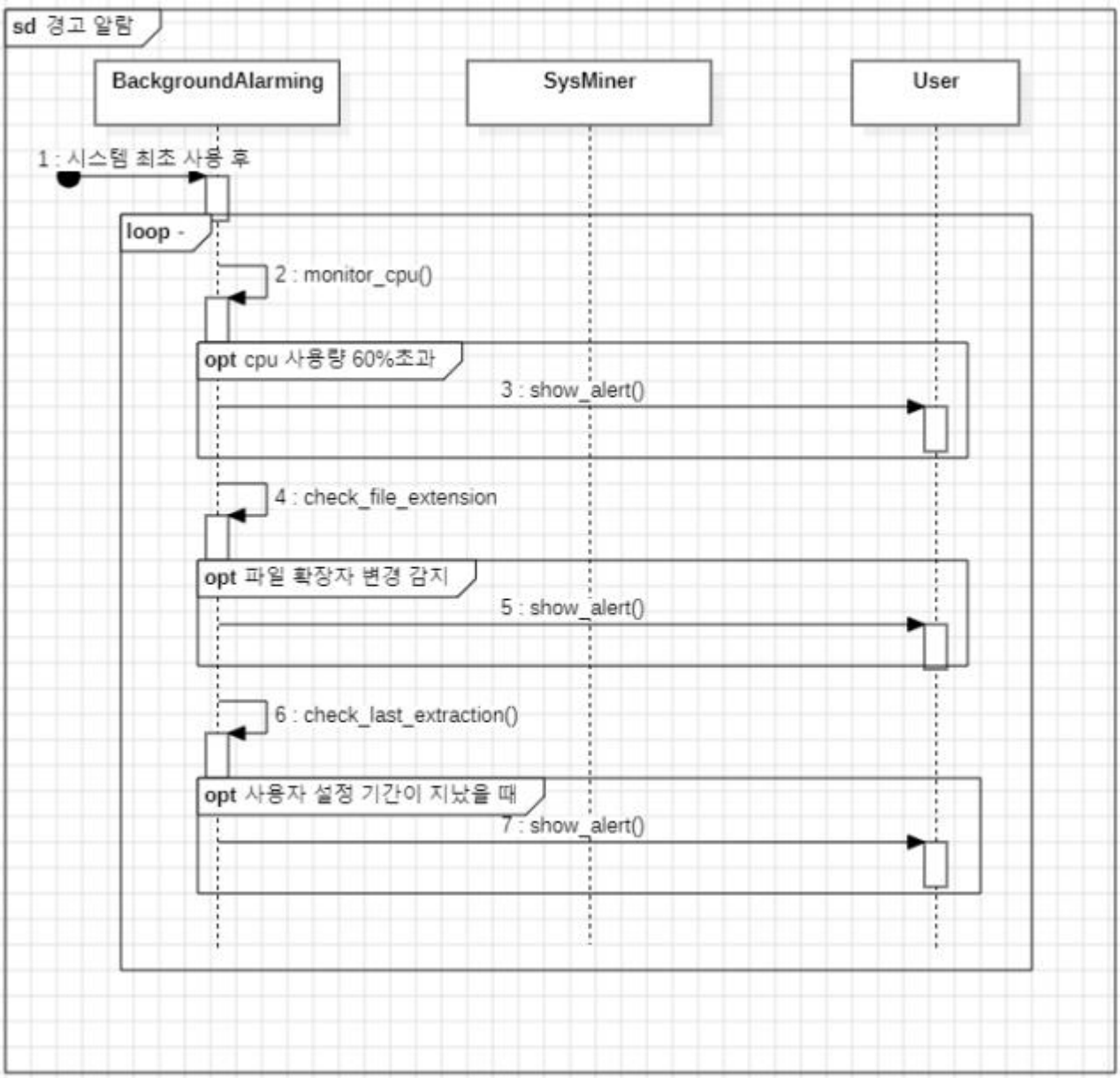
메인 메뉴에서 “Srum” 혹은 “프리패치”를 선택했을 경우, 각각 파일들을 get_data()를 통해 파일 혹은 폴더를 찾고 copy_folder()를 통해 바탕화면의 “Data_Hub”에 저장된다. 후에 추출에 성공한 정보는 GUI에 print_success()를 수행하고 실패한 정보는 print_failed()를 수행한다. 후에 generate_html_report()를 통해 결과를 html로 저장한 파일을 생성한다.



메인 메뉴에서 “휴지통”, “최근 파일”, “QuickLaunch”를 선택했을 경우, 각각 폴더 혹은 파일들을 get_data()를 통해 파일 혹은 폴더를 찾고, copy_folder()를 통해 바탕화면의 “Data_Hub”에 저장된다. 추출에 성공한 정보들은 GUI에 print_success()를 수행하고 실패한 정보들은 print_failed()를 수행한다. 후에 generate_html_report()를 통해 결과를 html로 저장한 파일을 생성한다.



메인 메뉴에서 ”윈도우 업데이트 기록“, ”방화벽 상태 확인“, ”패스워드 정책“, ”설치된 소프트웨어“ 항목을 선택했을 경우, 각 항목에 따른 알맞은 PowerShell 명령어를 execute_command()를 통해 수행한 뒤, save_at_txt()를 통해 바탕화면의 ”Data_Hub“ 폴더에 메모장 파일로 저장된다. 후에 generate_html_report()를 통해 결과를 html로 저장한 파일을 생성한다.



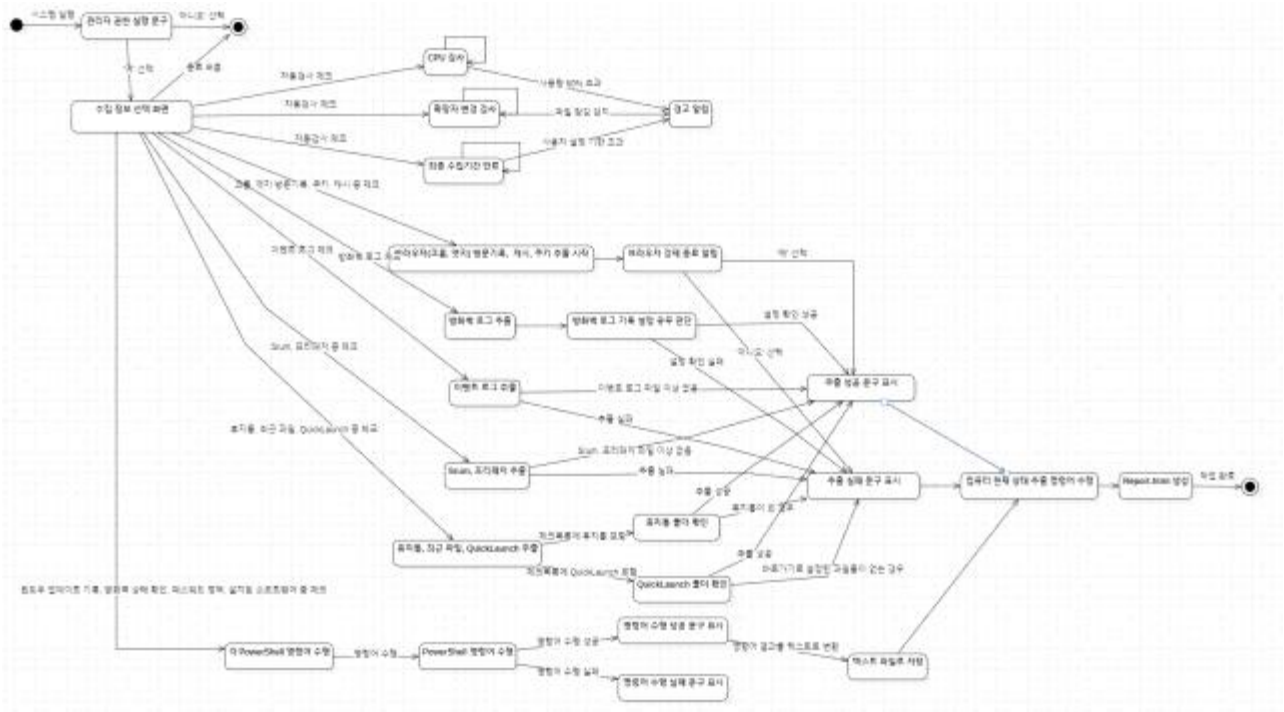
시스템이 백그라운드에서도 실행되며, 수시로 CPU 사용량과 확장자명 변경을 검사하며, 둘 중 하나라도 감지된 경우 사용자에게 알람을 띄우도록 한다.

monitor_cpu() 함수를 통해 10분마다 CPU 사용량을 측정하며, 임계값인 60%를 넘을 경우 사용자에게 알람을 준다.

check_file_extensions() 함수를 통해 2시간마다 바탕화면에 있는 파일의 확장자를 검사하며, 파일이 잠겨지는 확장자로 변경됐을 경우 사용자에게 알람을 준다.

check_last_extraction()을 통해 하루마다 검사하며, 사용자가 알람을 주도록 설정한 기간보다 날짜가 지났다면 사용자에게 프로그램을 사용하여 컴퓨터 정보를 백업하라고 알람을 띄운다.

4. State machine diagram



위 그림은 전체적인 시스템 수행 과정을 나타낸 State Machine diagram이다. 사용자는 프로그램을 실행하면 관리자 권한으로 실행하도록 알람을 띄워 권한을 허가받는다. 후에 GUI에 들어서면 사용자는 자동 검사 체크박스를 체크할 수 있는데, 체크를 하면 자동으로 윈도우 실행 프로그램에 등록되며, 백그라운드에서 CPU 검사, 확장자 검사, 기한 만료 여부를 검사한다. 이상이 감지되면 사용자에게 알람을 띄운다.

후에 기능 선택창에선 각 기능에 대해 알맞은 동작을 수행 후, 최종적으로 사용자 컴퓨터의 현재 상태에 대한 정보를 추출하는 명령어를 수행한 후, 최종 보고서를 수행해 추출 결과와 현재 컴퓨터 상태에 대해 한 눈에 알아보기 쉽도록 한다.

5. Implementation requirements

1) H/W platform requirements
   (1) CPU: Intel Core i3 또는 동급 AMD 프로세서
   (2) RAM: 4GB
   (3) SSD: 128GB 이상

2) S/W platform requirements
   (1) OS: Microsoft Window 7 이상
   (2) Implementation Language: Python

6. Glossary

Terms	Description
Class Diagram	객체지향 프로그래밍에서의 클래스 간의 관계를 시각적으로 표현한 UML 다이어그램
메인 컨트롤러	전체 기능 실행을 제어하는 클래스
DB	데이터가 저장되어있는 공간
Integer	정수인 숫자
HTML	웹 문서를 구조화하는데 사용되는 언어
딕셔너리	파이썬 등에서 사용되는 key-value 쌍으로 구성된 자료형
확장자	파일의 유형을 나타내는 파일 이름 끝의 문자열