Yeungnam University

SysMiner

-Analysis-

Student No	22112133
Name	서주형
Email	blane7777@naver.com

[Revision history]

Revision date	Version #	Description	Author
2025/05/07	1.00	초기 버전	서주형

= Contents =

1. Introduction

1) Executive Summary

정보화 시대가 도래함으로써 사이버 공간에서의 위협과 공격은 점점 더 진화하고, 잦아지고 있다. 침해사고는 예방과 빠른 초기 대응이 중요하지만, 컴퓨터에 대한 지식이 없는 사람들은 어떻게 예방해야할지, 사고 발생 시 어떻게 대응해야할 지에 대해 무지하다. 결국 많은 사람들이, 침해사고 발생 시에 포맷을 하여 기존의 컴퓨터 파일을 포기한다.

그리하여 "SysMiner"는 통해 사용자가 신속하게 대응할 수 있도록 데이터 추출 및 시스템 정보 백업 기능을 제공한다. 또한, 침해사고 전조 증상 감지 기능을 제공하여 사용자가 선제적으로 대응할 수 있도록 한다.

2) Busniess Goals

"SysMiner"는 사용자가 컴퓨터 공격을 받았을 때 즉시 조치를 할 수 있는 도구를 제공한다. 컴퓨터에 대한 전문 지식이 없는 사용자도 컴퓨터 공격에 초기에 대응할 수 있도록 지원하여 데이터 손상 전에 중요한 파일과 정보를 추출할 수 있도록 한다. 이렇게 함으로써 복구 확률을 올릴 수 있다. 시스템 정보 백업 및 공격의 조기 경고 징후를 제공하여 사전에 예방할 수 있도록 한다.

3) Technical Goals

"Sys Miner"는 사고 발생 전에는 주기적으로 시스템 정보를 추출하고, 한 곳에 모아주는 기능이 있다. 또한, CPU 사용량이 급격하게 증가하거나 혹은 가장 최근 정보 추출 일로부터 사용자가 지정한 기한이 지나면 프로그램이 사용자에게 알람을 주어 상기시키도록 한다.

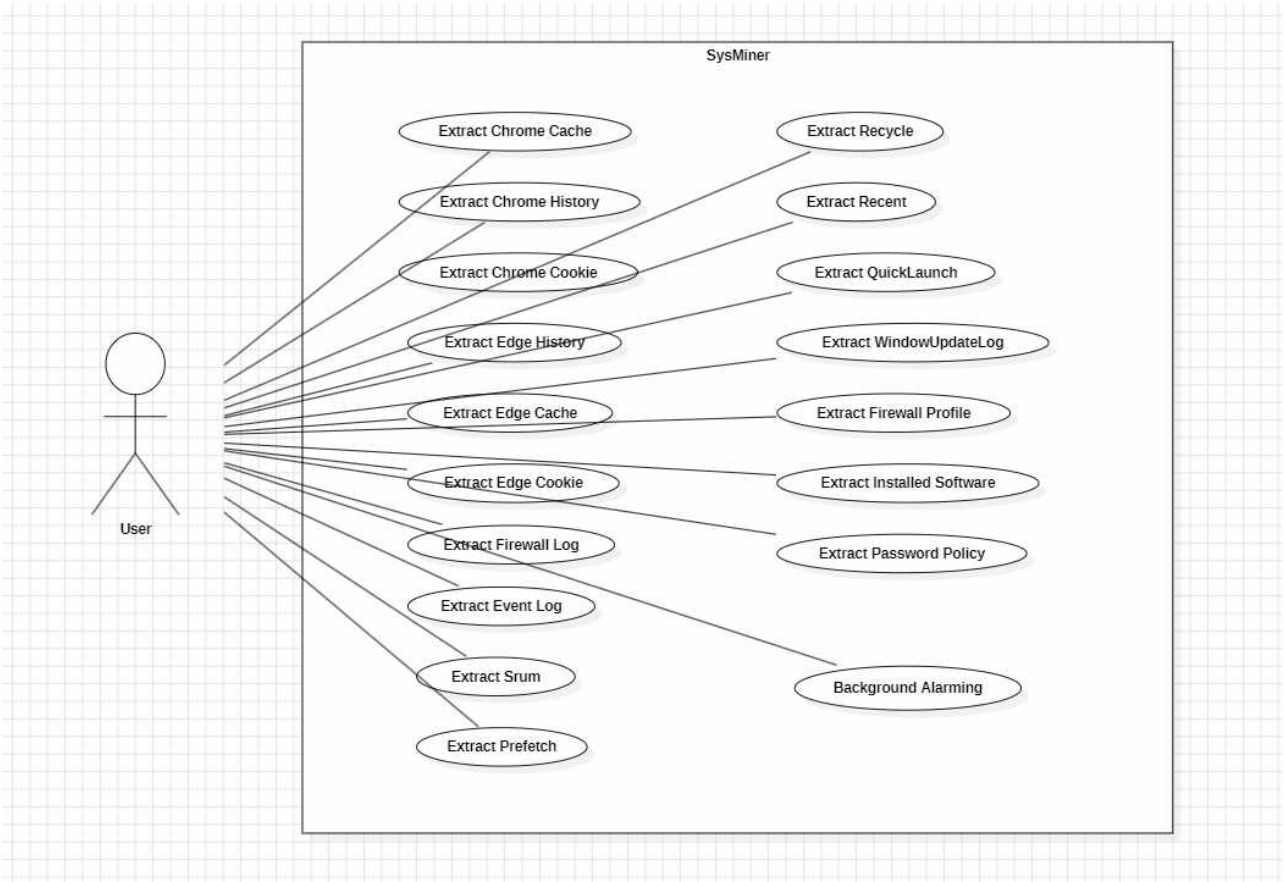
사고 발생 후에는 수집한 데이터를 통해 전문가에게 도움을 줄 수 있도록 한다. 공격으로 인해 손상되기 전의 정보들을 통해 사고를 해결하는 데 도움을 줄 수 있다.

친화적이고 직관적인 GUI를 통해 사용하기 쉽도록 한다.

시스템 정보를 추출 후, 추출 결과를 html 파일로 나타내어 한 눈에 알아 보기 쉽도록 한다.

2. Introduction

1) Usecase Diagram



"SysMiner"는 개인 사용자를 위한 프로그램임으로 Actor는 User 한 명이다. 그 외에 각종 시스템 정보를 추출하는 usecase들과 사용자에게 알람 기능을 하는 Background Alarming usecase가 있다.

2) Usecase Description

Usecase #1 : Extract Chrome History	
GENERAL CHARACTERISTICS	
Summary	인터넷 브라우저 'Chrome'의 방문 기록을 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'크롬 방문기록'란을 체크한다.
Success Post Condition	수집 창에서 "크롬 방문기록 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "크롬 방문기록 수집 실패 X"가 표시된다. "Report.html"에서 "크롬 방문기록 (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "크롬 방문기록"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "크롬 방문기록 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "Chrome_Info" 폴더 → "Chrome_History" 폴더에 방문기록 파일이 저장

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다. 4b. 사용자 컴퓨터에 "Chrome" 프로그램이 설치되어 있지 않은 경우 추출에 실패한다. 4b1. 수집 창에서 "크롬 방문기록 수집 실패 X"가 표시된다. 4b2. "Report.html"에서 "크롬 방문기록 (수집되지 않음)"으로 표시된다. 4c. 사용자가 현재 "Chrome" 프로그램을 실행 중이면 추출에 실패한다. 4c1. 프로그램을 종료해야한다는 문구를 띄운다. 4c2. 프로그램을 강제로 종료한다.

RELATED INFORMATION	
Performance	≤3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #2 : Extract Chrome Cache	
GENERAL CHARACTERISTICS	
Summary	인터넷 브라우저 'Chrome'의 캐시를 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'크롬 캐시'란을 체크한다.
Success Post Condition	수집 창에서 "크롬 캐시 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "크롬 캐시 수집 실패 X"가 표시된다. "Report.html"에서 "크롬 캐시 (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "크롬 캐시"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "크롬 캐시 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "Chrome_Info" 폴더 → "Chrome_Cache" 폴더에 방문기록 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다. 4b. 사용자 컴퓨터에 "Chrome" 프로그램이 설치되어 있지 않은 경우 추출에 실패한다. 4b1. 수집 창에서 "크롬 방문기록 수집 실패 X"가 표시된다. 4b2. "Report.html"에서 "크롬 방문기록 (수집되지 않음)"으로 표시된다. 4c. 사용자가 현재 "Chrome" 프로그램을 실행 중이면 추출에 실패한다. 4c1. 프로그램을 종료해야한다는 문구를 띄운다. 4c2. 프로그램을 강제로 종료한다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #3 : Extract Chrome Cookie	
GENERAL CHARACTERISTICS	
Summary	인터넷 브라우저 'Chrome'의 쿠키를 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'크롬 쿠키'란을 체크한다.
Success Post Condition	수집 창에서 "크롬 쿠키 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "크롬 쿠키 수집 실패 X"가 표시된다. "Report.html"에서 "크롬 쿠키 (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "크롬 쿠키"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "크롬 쿠키 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "Chrome_Info" 폴더 → "Chrome_Cookie" 폴더에 방문기록 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다. 4b. 사용자 컴퓨터에 "Chrome" 프로그램이 설치되어 있지 않은 경우 추출에 실패한다. 4b1. 수집 창에서 "크롬 방문기록 수집 실패 X"가 표시된다. 4b2. "Report.html"에서 "크롬 방문기록 (수집되지 않음)"으로 표시된다. 4c. 사용자가 현재 "Chrome" 프로그램을 실행 중이면 추출에 실패한다. 4c1. 프로그램을 종료해야한다는 문구를 띄운다. 4c2. 프로그램을 강제로 종료한다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #4 : Extract Edge History	
GENERAL CHARACTERISTICS	
Summary	인터넷 브라우저 '엣지'의 방문 기록을 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'엣지 방문기록'란을 체크한다.
Success Post Condition	수집 창에서 "엣지 방문기록 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "엣지 방문기록 수집 실패 X"가 표시된다. "Report.html"에서 "엣지 방문기록 (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "엣지 방문기록"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "엣지 방문기록 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "Edge_Info" 폴더 → "Edge_History" 폴더에 방문기록 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다. 4b. 사용자 컴퓨터에 "Edge" 프로그램이 설치되어 있지 않은 경우 추출에 실패한다. 4b1. 수집 창에서 "엣지 방문기록 수집 실패 X"가 표시된다. 4b2. "Report.html"에서 "엣지 방문기록 (수집되지 않음)"으로 표시된다. 4c. 사용자가 현재 "Edge" 프로그램을 실행 중이면 추출에 실패한다. 4c1. 프로그램을 종료해야한다는 문구를 띄운다. 4c2. 프로그램을 강제로 종료한다.

RELATED INFORMATION	
Performance	≤3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #5 : Extract Edge Cache	
GENERAL CHARACTERISTICS	
Summary	인터넷 브라우저 '엣지'의 캐시를 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'엣지 캐시'란을 체크한다.
Success Post Condition	수집 창에서 "엣지 캐시 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "엣지 캐시 수집 실패 X"가 표시된다. "Report.html"에서 "엣지 캐시 (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "엣지 캐시"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "엣지 캐시 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "Edge_Info" 폴더 → "Edge_Cache" 폴더에 방문기록 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다. 4b. 사용자 컴퓨터에 "Edge" 프로그램이 설치되어 있지 않은 경우 추출에 실패한다. 4b1. 수집 창에서 "엣지 방문기록 수집 실패 X"가 표시된다. 4b2. "Report.html"에서 "엣지 방문기록 (수집되지 않음)"으로 표시된다. 4c. 사용자가 현재 "Edge" 프로그램을 실행 중이면 추출에 실패한다. 4c1. 프로그램을 종료해야한다는 문구를 띄운다. 4c2. 프로그램을 강제로 종료한다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #6 : Extract Edge Cookie	
GENERAL CHARACTERISTICS	
Summary	인터넷 브라우저 '엣지'의 쿠키를 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'엣지 쿠키'란을 체크한다.
Success Post Condition	수집 창에서 "엣지 쿠키 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "엣지 쿠키 수집 실패 X"가 표시된다. "Report.html"에서 "엣지 쿠키 (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "엣지 쿠키"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "엣지 쿠키 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "Edge_Info" 폴더 → "Edge_Cookie" 폴더에 방문기록 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다. 4b. 사용자 컴퓨터에 "Edge" 프로그램이 설치되어 있지 않은 경우 추출에 실패한다. 4b1. 수집 창에서 "엣지 방문기록 수집 실패 X"가 표시된다. 4b2. "Report.html"에서 "엣지 방문기록 (수집되지 않음)"으로 표시된다. 4c. 사용자가 현재 "Edge" 프로그램을 실행 중이면 추출에 실패한다. 4c1. 프로그램을 종료해야한다는 문구를 띄운다. 4c2. 프로그램을 강제로 종료한다.

RELATED INFORMATION	
Performance	≤3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #7 : Extract Firewall Log	
GENERAL CHARACTERISTICS	
Summary	방화벽을 통하는 트래픽의 기록을 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'방화벽 로그'란을 체크한다.
Success Post Condition	수집 창에서 "방화벽 로그 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "방화벽 로그 수집 실패 X"가 표시된다. "Report.html"에서 "방화벽 로그 (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "방화벽 로그"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "방화벽 로그 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "Firewall_Logs" 폴더에 로그 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다. 4b. 사용자 컴퓨터에 방화벽 로깅 기능이 설정 되어있지 않은 경우 추출에 실패한다. 4b1. 수집 창에서 "방화벽 로그 수집 실패 X"가 표시된다. 4b2. "Report.html"에서 "방화벽 로그 (수집되지 않음)"으로 표시된다. 4b3. 방화벽 로깅 기능을 설정하는 방법을 표시한다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #8 : Extract Event Log	
GENERAL CHARACTERISTICS	
Summary	컴퓨터 내에서 발생한 이벤트 로그를 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'이벤트 로그'란을 체크한다.
Success Post Condition	수집 창에서 "이벤트 로그 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "이벤트 로그 수집 실패 X"가 표시된다. "Report.html"에서 "이벤트 로그 (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "이벤트 로그"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "이벤트 로그 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "Event_Logs" 폴더에 로그 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #9 : Extract Srum	
GENERAL CHARACTERISTICS	
Summary	어떤 프로그램의 실행 시간, 네트워크 사용량, CPU 사용량 등에 대한 정보를 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'Srum'란을 체크한다.
Success Post Condition	수집 창에서 "Srum 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "Srum 수집 실패 X"가 표시된다. "Report.html"에서 "Srum (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "Srum"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "Srum 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "Srum" 폴더에 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #10 : Extract Prefetch	
GENERAL CHARACTERISTICS	
Summary	처음 실행된 프로그램의 초기 로딩 정보를 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'Prefetch'란을 체크한다.
Success Post Condition	수집 창에서 "Prefetch 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "Prefetch 수집 실패 X"가 표시된다. "Report.html"에서 "Prefetch (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "Prefetch"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "Prefetch 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "Prefetch" 폴더에 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #11 : Extract Recycle	
GENERAL CHARACTERISTICS	
Summary	사용자 컴퓨터의 휴지통 폴더를 복사한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'휴지통'란을 체크한다.
Success Post Condition	수집 창에서 "휴지통 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "휴지통 수집 실패 X"가 표시된다. "Report.html"에서 "휴지통 (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "휴지통"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "휴지통 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "RecycleBin" 폴더에 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #12 : Extract Recent	
GENERAL CHARACTERISTICS	
Summary	사용자 컴퓨터의 최근 접근한 폴더를 정보를 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'최근 파일'란을 체크한다.
Success Post Condition	수집 창에서 "최근 파일 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "최근 파일 수집 실패 X"가 표시된다. "Report.html"에서 "최근 파일 (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "최근 파일"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "최근 파일 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "Recent" 폴더에 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #13 : Extract QuickLaunch	
GENERAL CHARACTERISTICS	
Summary	사용자 컴퓨터의 바로가기로 설정된 정보를 추출한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	'QuickLaunch'란을 체크한다.
Success Post Condition	수집 창에서 "QuickLaunch 수집 완료 ✓"가 표시된다.
Failed Post Condition	수집 창에서 "QuickLaunch 수집 실패 X"가 표시된다. "Report.html"에서 "QuickLaunch (수집되지 않음)"으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 "QuickLaunch"란을 체크한다.
3	사용자가 "다음"버튼을 클릭한다.
4	수집 창에서 "QuickLaunch 수집 완료 ✓"가 표시된다.
5	사용자 컴퓨터의 바탕화면 → "Result" 폴더 → "Data_Hub" 폴더 → "QuickLaunch" 폴더에 파일이 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 폴더를 복사할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #14 : Extract WindowUpdateLog	
GENERAL CHARACTERISTICS	
Summary	파워쉘 명령어 “Get-WindowsUpdateLog”를 실행시킨 결과를 .txt 파일로 저장한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	‘윈도우 업데이트 기록’란을 체크한다.
Success Post Condition	수집 창에서 “윈도우 업데이트 기록 수집 완료 ✓”가 표시된다.
Failed Post Condition	수집 창에서 “윈도우 업데이트 기록 수집 실패 X”가 표시된다. “Report.html”에서 “윈도우 업데이트 기록 (수집되지 않음)”으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 “윈도우 업데이트 기록”란을 체크한다.
3	사용자가 “다음”버튼을 클릭한다.
4	수집 창에서 “윈도우 업데이트 기록 수집 완료 ✓”가 표시된다.
5	사용자 컴퓨터의 바탕화면 → “Result” 폴더 → “Data_Hub” 폴더 → “Security_Check” → “Windows_Update.log”와 “Windows_Update.txt” 로 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 명령어를 실행할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다. 4b. “Get-WindowsUpdateLog”명령어를 수행하면 별도로 파워쉘에서 제공하는 텍스트 파일이 바탕화면에 생성된다. 4b1. 바탕화면에 생성된 파일을 Data_Hub 파일로 이동시킨다.

RELATED INFORMATION	
Performance	≤3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #15 : Extract Firewall Profile	
GENERAL CHARACTERISTICS	
Summary	파워쉘 명령어 “Get-NetFirewallProfile | Select-Object -Property Name, Enabled”를 실행시킨 결과를 .txt 파일로 저장한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	‘방화벽 상태확인’란을 체크한다.
Success Post Condition	수집 창에서 “방화벽 상태확인 수집 완료 ✓”가 표시된다.
Failed Post Condition	수집 창에서 “방화벽 상태확인 수집 실패 X”가 표시된다. “Report.html”에서 “방화벽 상태확인 (수집되지 않음)”으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 “방화벽 상태확인”란을 체크한다.
3	사용자가 “다음”버튼을 클릭한다.
4	수집 창에서 “방화벽 상태확인 수집 완료 ✓”가 표시된다.
5	사용자 컴퓨터의 바탕화면 → “Result” 폴더 → “Data_Hub” 폴더 → “Security_Check” → “Firewall_Status.txt”로 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 명령어를 실행할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #16 : Extract Password Policy	
GENERAL CHARACTERISTICS	
Summary	파워쉘 명령어 “Get-LocalUser | Select-Object -Property Name, PasswordNeverExpires, UserMayNotChangePassword”를 실행시킨 결과를 .txt 파일로 저장한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	‘패스워드 정책’란을 체크한다.
Success Post Condition	수집 창에서 “패스워드 정책 수집 완료 ✓”가 표시된다.
Failed Post Condition	수집 창에서 “패스워드 정책 수집 실패 X”가 표시된다. “Report.html”에서 “패스워드 정책 (수집되지 않음)”으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 “패스워드 정책”란을 체크한다.
3	사용자가 “다음”버튼을 클릭한다.
4	수집 창에서 “패스워드 정책 수집 완료 ✓”가 표시된다.
5	사용자 컴퓨터의 바탕화면 → “Result” 폴더 → “Data_Hub” 폴더 → “Security_Check” → “Password_Policy.txt”로 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 명령어를 실행할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다.

RELATED INFORMATION	
Performance	≤ 3 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #17 : Extract Installed Software	
GENERAL CHARACTERISTICS	
Summary	파워쉘 명령어 “Get-WmiObject -Class Win32_Product | Select-Object -Property Name, Version”를 실행시킨 결과를 .txt 파일로 저장한다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	시스템이 실행 되어 있어야한다.
Trigger	‘설치된 소프트웨어’란을 체크한다.
Success Post Condition	수집 창에서 “설치된 소프트웨어 수집 완료 ✓”가 표시된다.
Failed Post Condition	수집 창에서 “설치된 소프트웨어 수집 실패 X”가 표시된다. “Report.html”에서 “설치된 소프트웨어 (수집되지 않음)”으로 표시된다.

Main SUCCESS SCENARIO	
Step	Action
1	사용자가 시스템을 실행한다.
2	사용자가 “설치된 소프트웨어”란을 체크한다.
3	사용자가 “다음”버튼을 클릭한다.
4	수집 창에서 “설치된 소프트웨어 수집 완료 ✓”가 표시된다.
5	사용자 컴퓨터의 바탕화면 → “Result” 폴더 → “Data_Hub” 폴더 → “Security_Check” → “Installed_Software.txt”로 저장된다.

EXTENSION SCENARIOS	
Step	Branching Action
4	4a. 프로그램이 관리자 권한으로 실행되지 않으면 명령어를 실행할 수 없다. 4a1. 프로그램을 실행할 경우 관리자 권한으로 다시 실행한다고 사용자에게 알려주는 문구를 띄우고 관리자 권한으로 다시 실행시킨다.

RELATED INFORMATION	
Performance	≤ 10 Seconds
Frequency	프로그램 실행 당 0번 혹은 1번
Concurrency	None
Other	None

Usecase #18 : Background Alarming	
GENERAL CHARACTERISTICS	
Summary	사용자에게 시스템 정보를 추출하라고 알림을 주며, 사고 전조증상이 확인된 경우 경고 문구를 띄운다.
Scope/Level	SysMiner/User Level
Author	서주형
Last Update	2025.05.06
Status	Analysis
Primary Actor	User
Preconditions	컴퓨터가 실행되어 있어야 한다.
Trigger	사용자가 설정한 기한이 지난 경우, CPU사용량이 급격히 늘어난 경우, 바탕화면에 파일이 잠긴 것을 감지한 경우
Success Post Condition	1) 사용자가 설정한 기한이 지난 경우, 사용자에게 정보를 백업하라고 알람 문구를 띄운다. 2) CPU 사용량이 급격하게 늘어난 경우, CPU 사용량이 급격히 늘어났다고 경고 문구를 띄운다. 3) 바탕화면에 파일이 잠긴 것을 감지한 경우, 잠긴 파일명과 확장자가 바뀌었다고 경고 문구를 띄운다.
Failed Post Condition	-

Main SUCCESS SCENARIO	
Step	Action
1	사용자의 컴퓨터를 사용하고 있다.
2	사용자가 설정한 기한이 지난 경우, CPU 사용량이 급격하게 늘어난 것을 감지한 경우, 바탕화면에 잠긴 파일이 생겼을 경우 프로그램이 문구를 띄운다.

EXTENSION SCENARIOS	
Step	Branching Action
-	-

RELATED INFORMATION	
Performance	≤ 1 Seconds
Frequency	1) 사용자가 설정한 기한이 지난 경우: 하루마다 백업 권고 알람 문구를 띄운다. 2) CPU 사용량이 급격히 늘어난 경우: 1분마다 CPU 사용량을 확인하고, CPU 사용량이 80% 이상이 될 경우 1분마다 경고 문구를 띄운다. 3) 바탕화면에 파일이 잠긴 것을 감지한 경우: 2시간마다 바탕화면의 파일들의 확장자를 검사하고, 확장자가 잠긴 것으로 감지되면 경구 문구를 띄운다.
Concurrency	None
Other	None

3. Domain analysis

1) SysMiner

SysMiner 시스템의 전체적인 기능을 총괄하는 클래스이다.

2) Admin

프로그램이 관리자 권한으로 실행되었는지 확인하는 클래스이며, 관리자 권한으로 실행되지 않았을 경우 강제적으로 프로그램을 관리자 권한으로 다시 실행시킨다.

3) BrowserHistories

“SysMiner”의 “크롬 방문기록”, “크롬 캐시”, “크롬 쿠키”, “엣지 방문기록”, “엣지 캐시”, “엣지 쿠키” 기능을 담당하는 클래스이며, 크롬과 엣지 브라우저의 각각 방문기록, 캐시, 쿠키 정보를 수집하는 클래스이다.

4) SystemLogs

“SysMiner”의 “방화벽 로그”, “이벤트 로그” 기능을 담당하는 클래스이며, 방화벽 로그와 이벤트 로그를 추출하는 클래스이다.

5) ApplicationCache

“SysMiner”의 “프리패치”, “Srum” 기능을 담당하는 클래스이며, “Srum”과 “Prefetch” 정보를 추출하는 클래스이다.

6) UserActivities

“SysMiner”의 “휴지통”, “최근 파일”, “QuickLaunch” 기능을 담당하는 클래스이며, 사용자 컴퓨터의 “휴지통”, “최근 파일”, “QuickLaunch” 정보를 추출하는 클래스이다.

7) SecurityCheck

“SysMiner”의 “윈도우 업데이트 기록”, “방화벽 상태확인”, “패스워드 정책”, “설치된 소프트웨어” 기능을 담당하는 클래스이며, 각 기능마다 파워쉘 명령어를 실행시키고, 그 결과를 .txt 파일로 저장하는 클래스이다.

8) Background Alarming

사용자가 컴퓨터를 사용중일 때, 백그라운드에서 사용자가 지정한 기한이 지났거나 CPU 사용량이 급격히 늘어나거나, 확장자가 갑자기 바뀌었을 경우 알람을

주는 기능을 가지는 클래스이다.

9) FinalReport

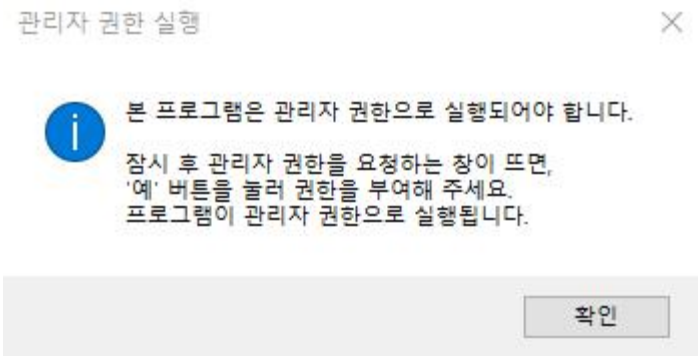
사용자가 “SysMiner”를 통해 정보를 추출하고, 추출한 정보들의 결과와 현재 컴퓨터의 상태에 대하 보기 쉽게 html 파일로 정리해주는 기능을 가진 클래스이다.

10) SysMinerGUI

“SysMiner”의 GUI를 담당하는 클래스이며, 사용자가 알아보기 쉽도록 GUI를 만드는 기능을 하는 클래스이다.

4. User Interface prototype

1) 관리자 권한 실행



"SysMiner"를 실행할 때, 프로그램이 관리자 권한으로 실행되지 않은 경우, 사용자에게 관리자 권한으로 실행되어야 한다는 문구와 함께 강제로 관리자 권한으로 다시 실행하도록 알람을 준다.

2) Main GUI

"SysMiner"의 Main GUI이다. 왼쪽에는 프로그램을 사용하는 방법에 대해 간략히 설명이 적혀있으며, "검사 주기 설정 (일)"에 수를 적고 "설정" 버튼을 누르면, 마지막으로 시스템 정보를 추출한 시간으로부터 설정한 수만큼 지난 날에 정보를 백업하

는 날이라고 알람 문구를 띄워준다. 오른쪽에는 추출 가능한 정보들을 체크박스로 나열한 것이고, 선택한 정보만 추출할 수 있다. “전체 선택”과 “전체 해제”버튼을 통해 모든 체크박스를 한 번에 선택, 해제할 수 있다. “다음”버튼을 누르면 체크한 정보들을 수집하기 시작한다.

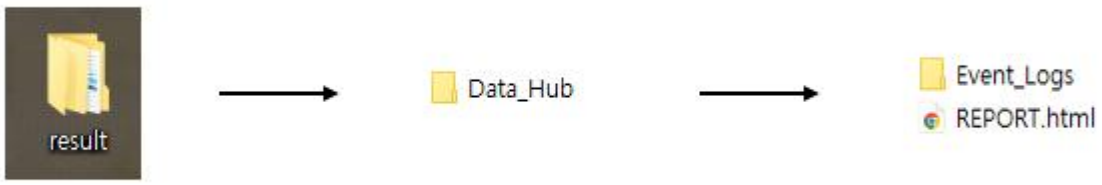
3) 수집 화면

수집 화면이다. 체크한 정보들의 수집현황에 대해 사용자에게 알려주는 화면이다. 정보 수집이 진행될수록 바가 초록색으로 차면서 진행률에 대해 알려준다.

4) 수집 현황

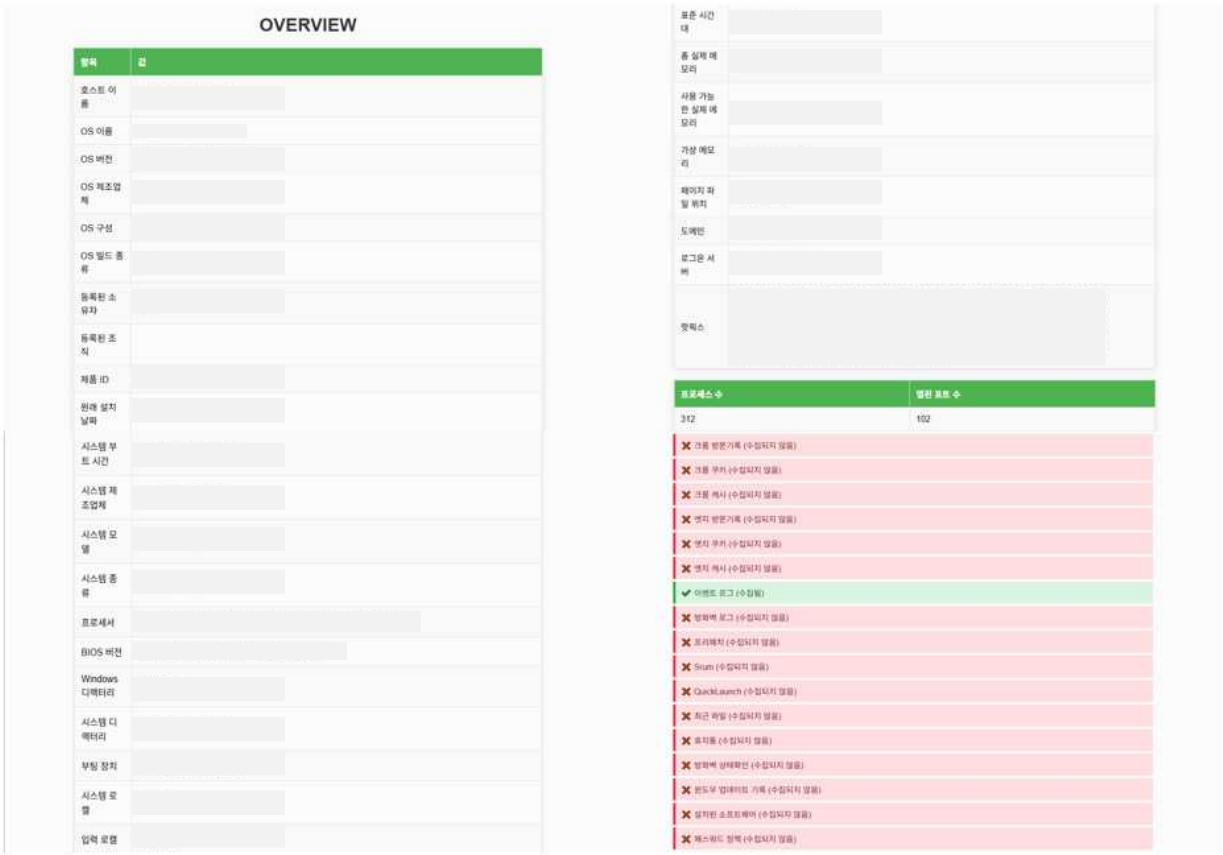
예시로 “이벤트 로그”와 “방화벽 로그”란을 체크한 결과이다. 수집을 정상적으로 성공한 정보는 초록색으로 표시되며 수집을 실패한 정보는 빨간색으로 표시되어 가독성 올렸다. 또한 수집이 완료된 경우 결과 페이지 html 리포트가 열린다고 사용자에게 알린다.

5) 수집 결과



“이벤트 로그”와 “방화벽 로그” 기능을 사용한 경우, 이벤트 로그만 수집을 성공했으므로 바탕화면의 “Result” 폴더 → “Data_Hub”에 “Event_Logs” 폴더와, “REPORT.html”파일이 저장된다.

6) REPORT.html



프로그램이 추출 작업이 완료되고, 사용자가 확인할 수 있는 HTMl 파일이다. 현재 컴퓨터에 대한 정보, 추출 성공한 정보, 추출 실패한 정보에 대해서 알아보기 쉽게 정리되어 있다.

5. Glossary

Terms	Description
CPU	컴퓨터의 중앙처리장치로, 연산과 명령 실행을 담당
HTML	웹페이지 구조를 정의하는 언어
Cache	데이터를 임시로 저장해 속도 향상을 돕는 저장소
Cookie	웹사이트가 사용자 정보를 저장하는 작은 파일
이벤트 로그(Event Log)	Windows의 시스템, 보안, 앱 이벤트를 기록
방화벽(Firewall)	네트워크 접근을 통제하는 보안 시스템
방화벽 로그(Firewall Log)	방화벽이 허용/차단한 연결 기록
Prefetch	Windows가 프로그램 실행정보를 미리 저장해 빠르게 로딩하도록 돕는 기능
Srum	Windows의 시스템 자원 사용 모니터링
Recycle(휴지통)	삭제한 파일이 임시로 보관되는 곳
Recent	최근 열어본 파일이나 폴더 기록
QuickLaunch	작업 표시줄에 자주 쓰는 앱을 빠르게 실행하는 영역
파워쉘	Windows 자동화 및 관리용 명령줄 프로그램