[WHS-3] 포렌식빵

프로젝트 킥오프

PM 정지윤 외 7명

CONTENTS

1. 프로젝트 팀 소개

1. 프로젝트 팀 소개 - 1. 팀 소개

팀 이름	포렌식빵
팀 소개	윈도우 포렌식에 관심이 많고 프로젝트에 열정이 있는 팀입니다.

PROJECT OUTLINE

Mentor	PL	Team
문현지 멘토님	심주완 PL님	[PM] 31반 정지윤 12반 배영혜 / 14반 전소현 / 17반 서연정 26반 김예은 / 31반 강지민 / 33반 김신아 38반 안서진

1. 프로젝트 팀 소개 -2. 역할 분배

역할	이름	내용
PM	정지윤	프로젝트 총괄 및 일정 정리
회의 기록	강지민	회의 내용 정리 및 회의록 작성
발표	김신아	프로젝트 결과 발표 준비 및 발표 진행
보고서 취합	김예은	팀원별 작업 내용 통합 및 보고서 정리
피피티 제작	배영혜	발표 자료 구성 및 PPT 형식의 보고서 제작
깃허브 관리	서연정	소스코드 및 산출물 버전 관리
노션 관리	안서진	프로젝트 기록 및 자료 정리
자료 취합	전소현	외부 자료 및 참고문헌 수집 및 정리

2. 프로젝트 개요

2. 프로젝트 개요

1. 프로젝트 정의

- 평소에는 정상적으로 사용되지만, 특정 조건에서 악의적으로 이용될 수 있는 프로그램 탐지 및 분석
- Windows 환경에서 사용자 행위 기반의 아티팩트 분석 기법을 확립 후 디지털 흔적을 기반으로 악용된 프로그램 아티팩트를 탐지하고 분석하여 포렌식 자동화 툴 제작

2. 프로젝트 필요성

기술적 능력 향상

- 악용이 가능한 정상적인 기능을 가진 프로그램의 아티팩트를 분석하여 범죄 증거를 수집하는 능력 학습 가능
- 아티팩트 분석 도구 개발 경험과 함께 논리적 사고, 문제 해결력, 협업 능력, 발표 역량까지 종합적 성장 가능
- 추후 논문 작성 및 자료 준비를 통해 결과물의 학술적 가치 증대 가능

2. 프로젝트 개요

3. 프로젝트 목표

윈도우 아티팩트 기반 악용 프로그램 탐지

- 정상 프로그램의 악용 행위를 식별하기 위한 아티팩트 기반 탐지 능력 향상

윈도우 아티팩트 기반 악용 프로그램 분석

- 윈도우 시스템 환경에서 생성되는 주요 디지털 아티팩트에 대한 이해 및 분석 역량 확보
- 정상적인 기능을 가진 프로그램을 악용하는 아티팩트를 분석

윈도우 아티팩트 기반 악용 프로그램 탐지 아티팩트 분석 도구 제작

- 자동화 도구를 활용한 악용된 정상 프로그램의 아티팩트를 신속하게 식별 가능
- 이를 통해 문제의 원인 분석, 범죄 증거물 수집

3. 프로젝트 계획

3. 프로젝트 계획 - 1. WBS

- 프로젝트 기획 및 시나리오 확정

담당자	세부 작업	5월											
		1차											
		1주차					2주차				3주차		
1 프로젝트 기획													
공통	Kick-off, WBS												
2. 포렌식 도구 분석 및 메뉴얼 작성													
공통	탐색 및 메뉴얼 공유												
3. 논문 탐색													
공통	논문 탐색												
공통	소프트웨어의 악성 활동 시나리오 조사												
공통	참고 논문 분석 및 시나리오 작성												
4. 설계 단계													
공통	실제 프로그램 메신저 아티팩트 분석												

3. 프로젝트 계획 - 1. WBS

- 프로그램 분석

담당자	세부 작업	5월					6월																				
		2차					3차										4차										
		4주차					5주차					6주차					7주차					8주차					
1. 프로그램 분석																											
공통	실제 프로그램 분석(추후 프로그램 선택 예정)																										
2. 아티팩트 분석 도구 설계																											
시나리오 바탕의 아티팩트 분석 도구 설계(개발 1주차)																											
공통	- 주요 분석 아티팩트 선정																										
개발팀(6)	- 도구 구조 및 기능 정의 및 기능 명세서 작성																										
3. 중간 발표																											
김신아, 배영혜	중간 발표 자료 제작 및 발표 준비																										
김신아	중간 발표																										

3. 프로젝트 계획 - 2. 정기 모임

- 회의 방식
  - 주 1회 회의 진행
    - 학기 중 : 격주에 한 번 오프라인 회의
    - 방학 : 매주 오프라인 회의
- 회의 시간
  - 매주 토요일 오후 14시
- 회의 장소
  - 잠실 스터디룸 (1순위)
  - 강남 스터디룸 (2순위)

3. 프로젝트 계획 - 3. 세부 프로젝트 계획

- 포렌식 도구 분석 및 메뉴얼 작성_도구 분석 담당자

분석 카테고리	담겨 있는 정보	분석 도구	담당자
메신저 아티팩트	전송 기록, 캐시, 채팅 로그, 실행 기록	FTK Imager, WinPrefetchView, Registry Explorer, SQLite Browser	김예은, 김신아
네트워크 아티팩트	방문 기록, 세션 토큰, 네트워크 연결	Wireshark	배영혜
시스템 설치/실행 아티팩트	prefetch, 레지스트리, 이벤트 로그, LNK 파일	WinPrefetchView, Registry Explorer, Event Viewer	안서진, 정지윤, 서연정
파일 사용/조작 아티팩트	MFT, MAC 타임	FTK Imager, LogFileParser	전소현
메모리 아티팩트	프로세스 메모리, 명령어 이력	Volatility	안서진
사용자 행위 아티팩트	최근 명령어, 로그인 기록, 탐색 기록	Windows Event Viewer	강지민

3. 프로젝트 계획 - 3. 세부 프로젝트 계획

- 설계 단계_분석 파일 담당자

툴 이름	간단한 소개	담당
Rega	윈도우 레지스트리 뷰어	정지윤
Hashcat	비밀번호 해시 크래킹 도구	정지윤
DCode	시간 포맷 변환 도구	정지윤
MailView	Outlook 메일 아티팩트 분석	강지민
EventLog Explorer	이벤트 로그 분석 도구	강지민
HxD	파일의 헥스값 분석 도구	김신아
Audacity	mp3 파일 분석	김예은
pdfstreamdumper	PDF 분석 도구	김신아
FTK Imager	디스크 이미지 분석 도구	김예은
WinMerge	파일 및 디렉토리 비교 및 병합 도구	김예은
Volatility	메모리 덤프 파일 분석 도구	배영혜
ChromeCacheView	크롬 브라우저 캐시 분석 도구	김예은
Wireshark	pcap 파일 분석 도구	배영혜
Autopsy	디스크 이미지 분석 도구	서연정
KAPE	특정 아티팩트 추출 자동화 도구	안서진
WinPrefetchView	프리패치 아티팩트 분석 도구	안서진
DB Browser	SQLite DB 분석 도구	전소현
JumpList Explorer	점프 리스트 분석 도구	전소현
ntfslogtracker	시스템 파일 내 ntfs 파일 분석	김신아

3. 프로젝트 계획 - 3. 세부 프로젝트 계획

- 도구 개발 단계

1. 개발 역할 분담표

역할	주요 책임	구성원	세부 내용
총괄 / 통합 관리	전체 구조 설계, 통합 테스트, 코드 리뷰 및 발표 자료	강지민	전반 관여
아티팩트 처리팀	Registry, Prefetch, USN 등 아티팩트 파싱 함수 전담	정지윤, 안서진	서로 다른 아티팩트를 병렬로 구현
출력 및 인터페이스팀	CLI 출력 / WPF GUI 설계 / 로그 저장 등 사용자 인터페이스 구현	김예은, 배영혜	CLI/GUI 구현
탐지 로직 및 자동화팀	탐지 알고리즘 구현 / 테스트	강지민, 서연정	파싱 함수와 병렬로 탐지 테스트 가능

3. 프로젝트 계획 - 3. 세부 프로젝트 계획

- 도구 개발 단계

2. 개발 사이클

3. 프로젝트 계획 - 3. 세부 프로젝트 계획

- 도구 개발 단계

3.개발 세부 계획

담당자	세부 작업	7월																	
		5차							6차										
		9주차					10주차				11주차				12주차				
도구 기본 모듈 구현(개발 2주차)																			
개발팀(2)	- 레지스트리 파싱 함수 구현																		
개발팀(2)	- prefetch 등 파일 추출 가능한 함수 구현																		
개발팀(2)	- CLI 환경에서 초기 출력 구현																		
도구 기능 확장(개발 3주차)																			
개발팀(2)	- 로그 파일 읽기 함수 구현																		
개발팀(2)	- 메타데이터/ USN 저널 읽기 함수 구현																		
개발팀(2)	- CLI 내 통합 출력 테스트 진행																		
범죄 아티팩트 인식 기능 개발(개발 4주차)																			
개발팀(2)	- 모듈 통합 및 아티팩트 패턴 인식 로직 구현																		
개발팀(2)	- 탐지 패턴 자동화 함수 추가																		
개발팀(2)	- CLI 최종 구현																		
테스트 및 최종 점검(개발 5주차)																			
개발팀(6)	- 직접 만든 이미징 파일로 도구 테스트																		
개발팀(6)	- 기능 개선 및 오류 수정																		
개발팀(6)	- CLI 기반 GUI 개발(WPF 연동)																		
문서화 및 발표 준비(개발 6주차)																			
개발팀(2)	- 기능 명세서 및 매뉴얼 작성																		
강지민, 배영혜	- 결과 정리 및 ppt 제작																		
피드백 및 분석 도구 개발 마무리																			

3. 프로젝트 계획 - 3. 세부 프로젝트 계획

- 도구 개발 단계

4. 도구 개발 방향성 (아티팩트 파싱 도구)

4.1 목적

디지털 포렌식 아티팩트를 효과적으로 파싱하고 사용 흔적을 탐지할 수 있는 통합 도구를 개발

4.2 핵심기능

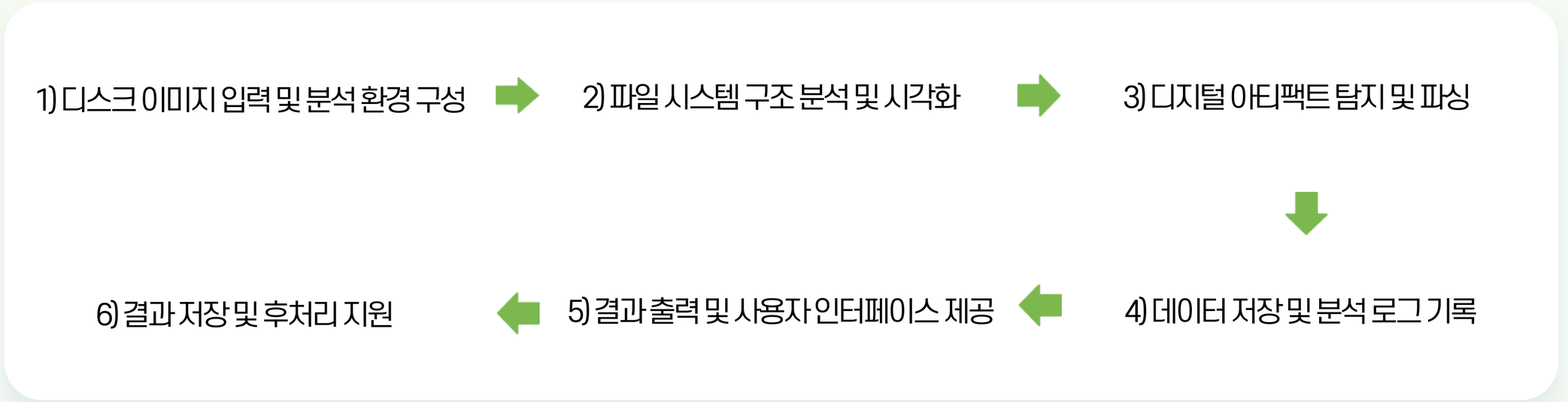
1) 아티팩트 파싱 기능
2) 디스크 이미지 (E01, raw) 분석기능
3) 탐지 패턴 적용 기능
4) CLI 인터페이스 제공
5) GUI 인터페이스 제공
6) 로깅 및 결과 저장 기능

3. 프로젝트 계획 - 3. 세부 프로젝트 계획

- 도구 개발 단계

4. 도구 개발 방향성 (아티팩트 파싱 도구)

4.3 예시 흐름



3. 프로젝트 계획 - 3. 세부 프로젝트 계획

- 도구 개발 단계

4. 도구 개발 방향성 (아티팩트 파싱 도구)

영역	기술 스택	설명
개발 언어	C, C++	성능 최적화 및 저수준 접근 용이
디스크 이미지 처리	LibEWF / Sleuth Kit (TSK)	.E01, .raw 등의 디스크 이미지 분석
파일 시스템 분석	Sleuth Kit (TSK)	NTFS, FAT 등 파일 시스템 트리 탐색
디지털 아티팩트 파싱	WinAPI, Windows Registry API, WMI	레지스트리, Prefetch, USN 등 파싱
데이터베이스	SQLite3 (C API)	경량화된 DB로 아티팩트 저장 및 관리
로그 관리	spdlog / log4cplus	분석 과정 로그 기록
CLI 구현	Getopt, WinAPI (Console)	명령행 인터페이스 구현
GUI 구현	Win32 API	WPE 기반 GUI 지원
네트워크 지원 (옵션)	WinSock API	원격 디스크 이미지 접근
멀티스레딩	Windows Threads API, PThreads for Win	멀티스레드 아티팩트 분석
작업 관리	github	

3. 프로젝트 계획 - 3. 세부 프로젝트 계획

- 논문 작성

1. 논문 역할 분담표

역할	주요 책임	구성원
총괄 / 통합 관리	전체 리뷰 및 교정	전소현
개발팀 자료 취합	개발팀과의 커뮤니케이션을 통한 자료 취합	전소현
연구 관련 자료 시각화	논문 작성 시에 필요되는 시각화 자료 제작	김신아
피드백 의견 정리	피드백 의견 취합 및 정리	김신아
논문 작성	논문 작성	전소현, 김신아

3. 프로젝트 계획 - 3. 세부 프로젝트 계획

- 논문 작성

2. 논문 작성 세부 계획

담당자	세부 작업	7월																			
		5차							6차												
		9주차					10주차					11주차				12주차					
논문 기획(논문 1주차)																					
논문팀(1)	- 개발팀 분석 자료 취합																				
논문팀(2)	- 논문 구조 및 목차 초안 작성 (논문 구조 아웃라인)																				
논문팀(2)	- 관련 연구 정리 및 비교 분석																				
논문팀(1)	- 서론 초안 작성																				
연구 배경 조사(논문 2주차)																					
논문팀(2)	- 논문 구조 및 목차 확정																				
논문팀(2)	- 서론 마무리 및 본론 초안 작성																				
연구 방법 정리(논문 3주차)																					
논문팀(1)	- 개발팀 문서 및 분석 결과 자료 취합																				
논문팀(2)	- 본론 작성																				
연구 결과 분석(논문 4주차)																					
논문팀(1)	- 실험 결과 정리 및 시각화																				
논문팀(2)	- 본론 마무리 및 결론 작성																				
논문 최종 정리 및 피드백(논문 5주차)																					
논문팀(2)	- 전체 원고 통합 및 표절 검사																				
논문팀(2)	- 참고문헌 및 인용 정리																				
피드백 및 분석 도구 개발 마무리																					
김신아, 배영혜	기말 발표 자료 제작 및 발표 준비																				
김신아	기말 발표																				

4. 프로젝트 산출물

4. 프로젝트 산출물

단계	산출물
관리	WBS
	Kick-Off 보고서
	중간 보고서
	최종 보고서
	회의록
	Notion
	Github
분석	분석 기록 및 아티팩트 추출 결과
	분석 방법 습득 리포트
	각 소프트웨어별 분석 결과
	시나리오 기반 아티팩트 목록화
	분석 도구 개발 계획서
제작	아티팩트 파싱 분석 도구
	논문
	발표 PPT

감사합니다.

포렌식빵