화이트햇 스쿨 2단계 팀 프로젝트 보고서

차세대 보안리더 양성 프로그램

한국정보기술연구원 BoB 교육센터

멘토명 / PL명	문현지/심주완	팀 명	포렌식빵
프로젝트 주제	윈도우 악성 프로그램 탐지 및 분석	회차	3회차
팀원	정지윤(PM) , 강지민, 김신아, 김예은, 배영혜, 서연정, 안서진, 전소현		
추진현황	<목차> 1. 프로젝트 진행 현황 1.1. 개요 1.2. ChatGPT 프로그램 분석 1.3. Perplexity 프로그램 분석 1.4. 논문 주제 제안 2. 향후 진행 방향 3. 산출물 3.1. ChatGPT 조작 보고서 3.2. ChatGPT 분석 보고서 3.3. Perplexity 조작 보고서 3.4. Perplexity 조작 보고서 4. 활동 사진		

KITRI
한국정보기술연구원

White Hat School

1. 프로젝트 진행 현황

1.1. 개요

3회차 프로젝트에서는 LLM 범주에 해당하는 프로그램들을 분석하였습니다. 분석 대상 프로그램을 선정할 때에는 Windows 환경에서 설치가 가능한지 여부와 기존 선행 연구와 주제가 중복되지 않는지를 고려하였습니다. 이러한 기준을 바탕으로 3~4주차 분석 대상 프로그램으로는 ChatGPT, Perplexity, Claude, Grok을 선정하였습니다. 3회차 프로젝트에는 ChatGPT, Perplexity을 조작하여 분석하였으며, 해당 회차의 산출물은 ChatGPT, Perplexity의 조작 보고서 및 분석 보고서가 제시됩니다.

1.2. ChatGPT 프로그램 분석

해당 분석 과정에서는 메신저 아티팩트, 네트워크 아티팩트, 캐시, 채팅 로그, 메모리 덤프를 중심으로 분석을 진행하였습니다. 로컬 사용자 계정 경로 내 AppData₩Local및 Roaming디렉터리에 저장된 캐시 및 로그 파일을 통해 사용자 정보와 네트워크 사용 정보 등을 확인할 수 있었으며, Wireshark를 활용하여 네트워크 트래픽 정보도 확인할 수 있었습니다. 이를 종합하여 분석 요약 표를 제시합니다.

아티팩트 유형	경로	설명
시스템 설치/실행 아티팩트	C:₩Windows₩Prefetch₩CHATGPT INSTALLER.EXE-FFA711B3.pf	설치파일이 실행된 시간과 실행 횟수 파악 가능
	C:₩Windows₩Prefetch	CHATGPT.EXE 실행 시각 및 누적 실행 횟수 확인 가능
	C:₩Users₩forensic₩Downloads₩ChatGPT Installer.exe	다운로드된 ChatGPT 설치 파일 경로 및 시

			간 확인가능
	사용자 행위 아티팩트	C:/Users/forensic/AppData/Local/Packages/OpenAI.ChatGPT Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Cache/Cache_Data	사용자 토큰, 구독 상태, 계정 생성일, 이메일, 이름, 전화번호, 프로필 사진 등의 정보 확인 가능
		C:/Users/forensic/AppData/Local/Packages/OpenAI.ChatGPT Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Local Storage/leveldb/00003.log	sessionID, 세션 시작 시각, 마지막 갱신 시각 등을 통해 세션 유지 시간과 사용자 활동 추적 가능
		C:/Users/forensic/AppData/Local/Packages/OpenAI.ChatGPTDesktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Local State	환경설정 및 암호화 관련 메타데이터 포함. 내부 데이터 암호화 및 복호화에 필요한 정보 포함
		C:₩Users₩forensic₩AppData₩Roaming₩Microsoft₩Windows₩Recent	사용자가 최근 접근한 이미지, 문서, 폴더 등의 흔적 확인 가능
		HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩ProfileList	SID 값과 사용자 계정명이 연결된 경로를 통해 분석 대상 사용자 계정 식별
		/Users/forensic/AppData/Local/Microsoft/Edge/User Data/Default/History	로그인 페이지에 접속한 기록과 로그인 관련 URL 경로 접근 확인

		C:Users/forensic/AppData/Local/Packages/OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Cache/Cache_Data/data_1	OAuth 인증 최종 단계에서 callback URL 호출과 함께 인증 코드가 기록된 로그 확인
		C:Users/forensic/AppData/Local/Packages/OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Cache/Cache_Data/data_1	사용자가 사용한 모델의 변경 시각, 모델명 등의 기록을 통해 모델 전환 내역 확인 가능
	파일 사용/조작 아티팩트	C:₩Users₩forensic₩Desktop₩ocr_test_invisible_id.png	파일이 삭제된 시간, 위치, 파일의 이름 등 확인 가능
		/$Recycle.Bin/S-1-5-21-1233276306-1788545777-16298427 36-1001	.csv, .docx, .zip, .png 등 삭제된 파일 목록과 삭제 경로 확인 가능
		C:₩Users₩forensic₩Desktop	ABC_Corp 파일 확인 가능
		MFT (Master File Table) : C:₩₩$MFT USN Journal : C:₩₩$Extend₩$UsnJrnl NTFS 로그 파일 : C:₩₩$LogFile	MFT/USN Journal/NTFS 로그 분석을 통해 파일 생성, 열람, 수정, 삭제 등 조작 시간 및 행위 확인 가능
		C:root₩Users₩forensic₩NTUSER.DAT, C:root₩Users₩forensic₩ntuser.dat.LOG1, C:root₩Users₩forensic₩ntuser.dat.LO	레지스트리 경로를 통해 ChatGPT의 설치 버전 및 설치 경로를 식별할 수 있음

		G2	
		C:root₩Users₩forensic₩NTUSER.DAT, C:root₩Users₩forensic₩ntuser.dat.LOG1, C:root₩Users₩forensic₩ntuser.dat.LOG2	실행 횟수, 마지막 실행 시각, 아키텍처 코드, 파일 크기 + 실행 여부 등 UserAssist, AppCompatCache 통해 확인 가능
	메모리 아티팩트	python vol.py -f gpt.vmem windows.pstree (명령어)	ChatGPT 프로세스, PID, 설치 경로 등 확인 가능
		python vol.py -f gpt.vmem windows.handles --pid 6484 (명령어)	ChatGPT 프로세스 내 열려있는 리소스(파일 핸들 등) 확인 가능
		python vol.py -f gpt.vmem windows.registry.hivelist (명령어)	ChatGPT 관련 레지스트리 경로 확인 가능
	네트워크 아티팩트	C:/Users/forensic/AppData/Local/Packages/OpenAI.ChatGPTDesktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Network/TransportSecurity	HTTPS 접속 기록, 적용 도메인, 서브도메인 포함 여부, 최초 적용 시각, 만료 시각 등의 정보 확인
		Users/forensic/AppData/Local/Packages/OpenAI.Chat GPT-Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Cache/Cache_Dat	ChatGPT API 호출 로그를 통해 offset/limit 파라미터로 과거 대화 목록 불러오기 기능

	네트워크 아티팩트	a/data_1	확인 가능능
		Users/forensic/AppData/Local/Packages/OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Network/Cookies	Cloudflare 기반 인증 쿠키 및 세션 키 기록 확인 가능
		Users/forensic/AppData/Local/Packages/OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Network/NetworkPersistent State	접속한 서버 주소, 프로토콜, 포트, 서버 응답 기록 등 확인 가능
		C:₩Users₩forensic₩AppData₩Local₩Packages₩OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0₩LocalCache₩Roaming₩ChatGPT₩Cache₩Cache_Data	csrf.json 내 토큰 값 확인 가능
		C:/Users/spdlq/AppData/Local/Packages/OpenAI.ChatGPTDesktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Network₩Network Persistent State	로컬 네트워크 IP 주소와 기록된 접속 주소 비교를 통해 동일성 확인 가능
		Wireshark 캡처	내부 IP가 OpenAI 인프라와 통신한 정황 확인 가능

	Wireshark 캡처	TLS 1.3 또는 QUIC 프로토콜을 통한 Client Hello~Key Exchange 핸드셰이크 흐름 확인 가능
메신저 아티팩트	C:/Users/forensic/AppData/Local/Packages/OpenAI.ChatGPTDesktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/LocalStorage/leveldb	대화 ID, 제목, 생성/수정 시각, 아카이브 여부, 메모리 사용 여부 등 메타데이터 확인 가능
	C:₩Users₩forensic₩AppData₩Local₩Packages₩OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0₩LocalCache₩Roaming₩ChatGPT₩Cache₩Cache_Data	employee_leak.csv 등 프롬프트 내 업로드한 파일명, 시각 등 확인 가능
	MFT (Master File Table) : C:₩₩$MFT USN Journal : C:₩₩$Extend₩$UsnJrnl NTFS 로그 파일 : C:₩₩$LogFile	ABC_com_Email_Password_Leak.csv 등 ChatGPT 생성 파일의 다운로드 흔적 확인 가능

[표1. ChatGPT 아티팩트 분석 요약표]

1.3. Perplexity 프로그램 분석

Perplexity 프로그램을 분석하는 과정에서는 ChatGPT 분석 과정에서는 발견하지 못했던 채팅 로그를 LevelDB 폴더를 분석함으로써 복구할 수 있었습니다. 채팅 로그를 포함하여 캐시 파일에서 사용자 행위에 대한 정보를 확인할 수 있었고, wireshark를 사용하여 해당 프로그램의 ip 정보 확인과 접속 도메인, 서버 연결 정보 등의 확인이 가능하였습니다. 이를 종합하여 분석 요약 표를 제시합니다.

아티팩트 유형	경로	설명
	C:₩Windows₩Prefetch	Perplexity 설치 및 실행

	시스템 설치/실행 아티팩트		기록
		C:Users₩forensic₩AppData₩Roaming₩Perplexity₩logs₩main.log	Perplexity 실행 로그
		C:Users₩forensic₩AppData₩Local₩Programs₩Perplexity	Perplexity 설치 디렉터리
		C:Users₩forensic₩Downloads	Perplexity 다운로드 파일
		C:Users₩forensic₩Desktop	Perplexity 바로가기 파일
		C:Users₩forensic₩AppData₩Local₩perplexity-updater	update 진행 기록
	사용자 행위 아티팩트	C:Users₩forensic₩AppData₩Roaming₩Perplexity₩logs₩main.log	Perplexity 사용자 이메일, 앱 실행 로그, 프롬포트 로그, 페이지 로그, 스페이스 로그, 스레드 이름 변경 로그, 익명 모드 로그
		C:₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Cache₩Cache_Data₩data_3	Perplexity 사용자 메타정보
		C:Users₩forensic₩AppData₩Roaming₩Perplexity₩Cache₩Cache_Data₩data_1	csrf 토큰, 로그인 인증 시도, 사용자 설정/계정 활동 리소스 접근 (Google Drive 연동)

		C₩Users₩forensic₩Roaming₩Perplexity₩Local Storage₩leveldb₩000005/ldb	사용자 도메인 접근 흔적
	파일 사용/조작 아티팩트	C:₩<root>₩$MFT , C:₩<root>₩$Extend₩$UsnJrnl , C:₩<root>₩$LogFile	파일 생성 및 파일 조작 흔적
	네트워크 아티팩트	C:₩root₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Network₩Network Persistent State	접속 도메인
		C:₩root₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Network₩Network Persistent State	서버 연결 정보
		C:₩root₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Network₩TransportSecurity	Perplexity HSTS 정책 정보
		C:₩root₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Network₩Cookies	Perplexity 쿠키 정보
		C:₩root₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Local Storage₩leveldb₩000038.log	채팅 내역
		C₩Users₩forensic₩App	로그 정보

메신저 아티팩트	Data₩Roaming₩Perplexity₩logs₩main.log	
	C₩Users₩forensic₩Roaming₩Perplexity₩Cache₩Cache_Data₩f_00002b	이미지 모델 정보

[표2. Perplexity 아티팩트 분석 요약표]

1.4. 논문 주제 제안

ChatGPT 분석 과정에서는 메신저 아티팩트에 해당하는 채팅 로그를 복구하지 못하였기 때문에 해당 프로그램으로 논문 작성을 진행하기에는 어려움이 있다고 생각하였습니다. 그러나 Perplexity에 대한 분석을 진행하며 Perplexity의 아티팩트에 대하여 분석한 논문이 없고, 분석 과정에서 기존 선행 연구에서는 진행하지 못하였던 대화 삭제 및 로그아웃 상황에서의 잔존 로그와 메타데이터를 확인할 수 있었기 때문에 '윈도우 환경에서의 Perplexity 애플리케이션 아티팩트 분석'를 논문 주제로 제시하였습니다.

2. 향후 진행 방향

Perplexity에 대한 분석 과정에서 선행 연구들과의 뚜렷한 차이점이 발견됨에 따라, '윈도우 환경에서의 Perplexity 애플리케이션 아티팩트 분석'을 주제로 선정한 논문을 2025년 7월 8일에 개최하는 한국디지털포렌식학회 하계학술대회에 투고할 예정입니다. 또한, 4회차 프로젝트에서는 LLM 범주 중 Claude 와 Grok에 대한 조작과 분석을 진행할 예정입니다. 해당 회차의 예상 산출물로는 각각 프로그램의 조작 보고서와 분석 보고서가 예상됩니다.

3. 산출물

3.1. ChatGPT 조작 보고서

https://github.com/forensicbread/WHS_forensicbread/blob/2204b88564608eed

02d5cdb16e991dbb5e68fc42/%EC%82%B0%EC%B6%9C%EB%AC%BC/3%EC%B0%A8%20%EC%82%B0%EC%B6%9C%EB%AC%BC/ChatGPT%20%EC%A1%B0%EC%9E%91%20%EB%B3%B4%EA%B3%A0%EC%84%9C/ChatGPT%20%EC%A1%B0%EC%9E%91%20%EB%B3%B4%EA%B3%A0%EC%84%9C.pdf

3.2. ChatGPT 분석 보고서

https://github.com/forensicbread/WHS_forensicbread/blob/2204b88564608eed02d5cdb16e991dbb5e68fc42/%EC%82%B0%EC%B6%9C%EB%AC%BC/3%EC%B0%A8%20%EC%82%B0%EC%B6%9C%EB%AC%BC/ChatGPT%20%EB%B6%84%EC%84%9D%20%EB%B3%B4%EA%B3%A0%EC%84%9C/ChatGPT%20%EB%B6%84%EC%84%9D%20%EB%B3%B4%EA%B3%A0%EC%84%9C.pdf

3.3. Perplexity 조작 보고서

https://github.com/forensicbread/WHS_forensicbread/blob/2204b88564608eed02d5cdb16e991dbb5e68fc42/%EC%82%B0%EC%B6%9C%EB%AC%BC/4%EC%B0%A8%20%EC%82%B0%EC%B6%9C%EB%AC%BC/Perplexity%20%EC%A1%B0%EC%9E%91%20%EB%B3%B4%EA%B3%A0%EC%84%9C/Perplexity%20%EC%A1%B0%EC%9E%91%20%EB%B3%B4%EA%B3%A0%EC%84%9C.pdf

3.4. Perplexity 분석 보고서

https://github.com/forensicbread/WHS_forensicbread/blob/2204b88564608eed02d5cdb16e991dbb5e68fc42/%EC%82%B0%EC%B6%9C%EB%AC%BC/4%EC%B0%A8%20%EC%82%B0%EC%B6%9C%EB%AC%BC/Perplexity%20%EB%B6%84%EC%84%9D%20%EB%B3%B4%EA%B3%A0%EC%84%9C/Perplexity%20%EB%B6%84%EC%84%9D%20%EB%B3%B4%EA%B3%A0%EC%84%9C.pdf

KITRI
한국정보기술연구원

White Hat School

1

활동사진 **(회의 사진 등)**

[그림1. 2025_05_31 온라인 회의 사진]

[그림2. 2025_06_07 오프라인 회의 사진]