분류	경로	단위	기능ID	기능명	세부사항
EVENT	₩FindWall₩src₩core₩Sysmon	Sysmon	background	이벤트 수집 bat	sysmon 이벤트를 자동으로 수집하도록 스크립트를 작성 - 파일명 : Sysmon_Event_Collecter.py
			S1_01	count xml node	xml 파일에 기록된 첫 데이터를 기준으로, 30초 단위 시간 내에 기록된 Node 개수 기록 - 산출물 : time, count - 파일이름 : time_graph.json
			S1_02	Prcoess Tree	xml 기준으로 프로세스 트리를 구성하여 클래스로 작성 - 폴더명 : ProcessTree(모든 py파일)
			S1_03	Detected Process	탐지된 내역을 기준으로 해당 프로세스의 트리별 정보를 출력한다. 산출물 : Process path, PID, and Time 파일이름 : time_ps.json
MEMORY	₩FindWally₩src₩core₩memory	메모리 덤프	I2_03	메모리 덤프	라이브 상태에서 메모리를 덤프한다.
		Volatility		imageinfo plugin	현재 시스템 정보를 가져온다. 다른 플러그인을 사용할 때, 옵션으로 사용된다. 산출물 : Profile, Image date and time 파일 이름 : imageinfo_data.json
				pstree plugin	메모리에 상주된 프로세스들의 PID, PPID 등을 구분하여 출력해준다. 산출물: 프로세스명, PID, PPID, address 파일 이름 : pstree.json, sub_tree.json
				psxview plugin	Offset, 프로세스명, PID 등을 보여준다. 산출물 : Offset, 프로세스명, PID, Pslist, Psscan, thrdproc, pspcid, csrss, session, deskthrd 파일 이름 : psxview_process.json
				netscan plugin	네트워크 통신하는 목록들을 보여준다. 산출물 : Protocol, Local Address, Foreign Address, State, PID, 프로세스 명, Count 파일 이름 : netscan_process.json
				hivelist plugin	레지스트리 목록을 출력해준다. 산출물 : 레지스트리 경로, Virtual address 파일 이름 : hivelist.json
				printkey plugin	하이브 리스트 목록에 있는 레지스트리 키의 값을 출력해준다. 산출물 : Registry 경로, 이름, Last updated, Vurtual address, Values 파일 이름 : printkey_Run_process.json
				dlllist plugin	프로세스에서 로드한 dll들을 보여준다. 옵션을 사용하여 특정 프로세스가 로드한 dll들을 보여준다.
				ldrmodules plugin	링크되어 있지 않은 DLL들을 탐지해준다. dlllist에서 탐지하지 못한 dll들을 보여준다.
				yarascan plugin	커널/유저 메모리에서 바이트 순서와 유니코드 및 ANSI코드를 보여준다.
				malfind plugin	디스크에 있는 파일에 매핑되지 않은 'PAGE_EXECUTE_READWRITE' 메모리 섹션과 MZ 헤더 (실행가능한)의 존재 권한이 있는 메모리 섹션을 보여준다. 산출물 : 프로세스 명, PID, Signature
				Result hit process fucntion	여러 플러그인을 사용한 규칙에 따라 의심프로세스로 지정된 프로세스들을 한 파일에 모아주는 역할을 한다. 해당 파일을 기준으로 GUI에 의심프로세스들을 표현한다. 산출물 : 프로세스 명, PID 파일 이름 : Result_hit_process.json
DefenderLog		Defender Log	A1_01	lisk level	AMSI 에서 탐지한 위험의 심각도를 출력한다. 산출물 : Severity ID 파일이름 : EventLogParse.py
			A1_02	Latest Log	AMSI가 탐지한 로그 데이터 중 가장 최근 항목만 추려 출력한다. 보여줄 데이터에는 제공자, 탐지된 시간, 위협 이름, 위협 ID, 프로세스 이름, 경로 등이 해당된다. 산출물 : Product Name, Detection time, Treat Name, Threat ID, Severity Name, Severity ID, Category Name, Detection User, Path, Origin Name, Type Name 파일이름 : EventLogParse.py
			A1_03	Log List	하단에 리스트 형식으로 로그 데이터(최대 30개)를 날짜(최근이 우선) 순으로 불러와 정렬한다. 산출물 : Threat ID, Product Name, Detection time, Severity ID, Path 파일이름 : EventLogParse.py