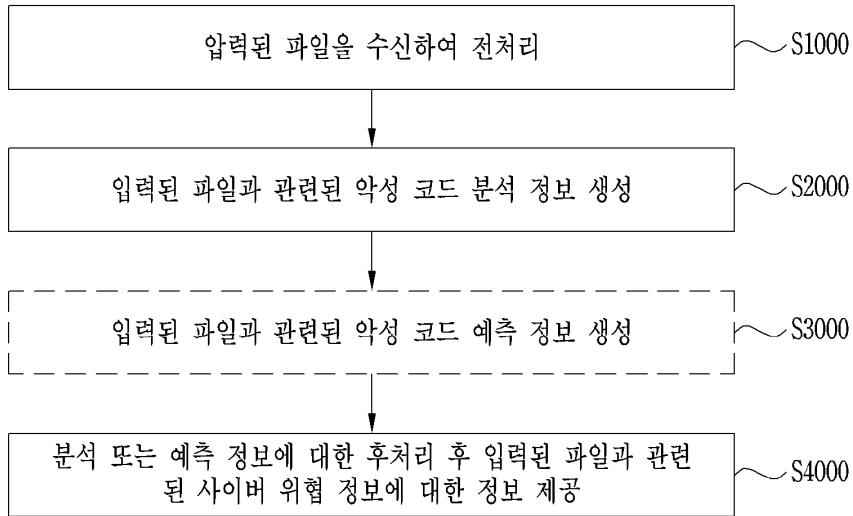
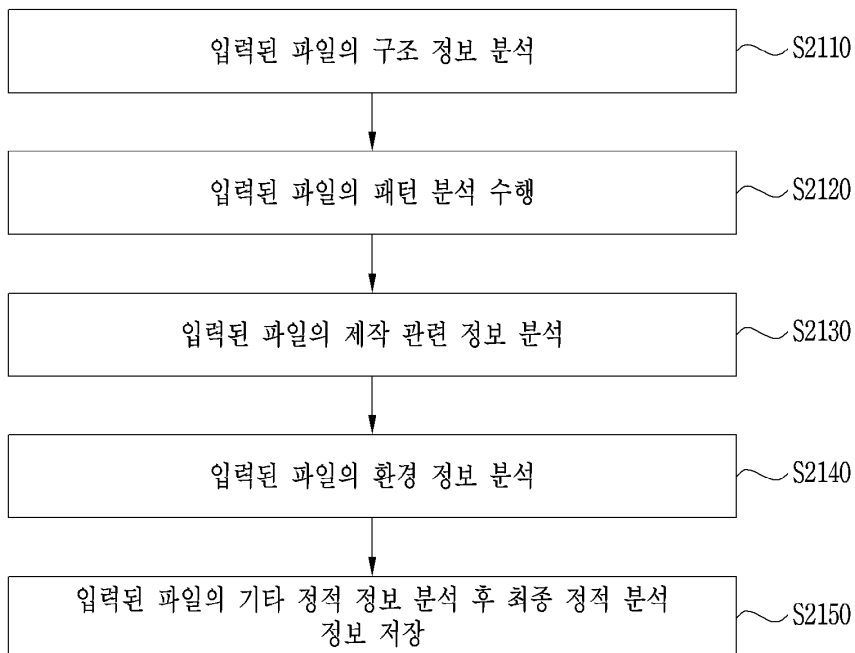


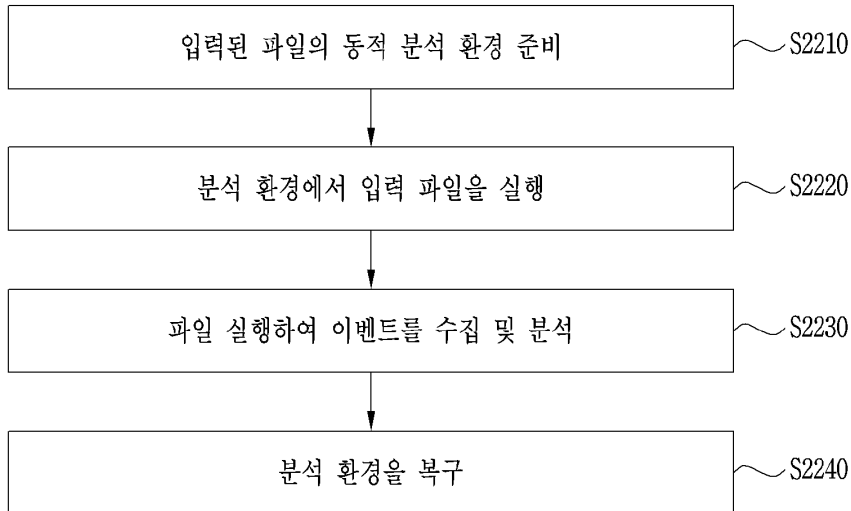
[도1]



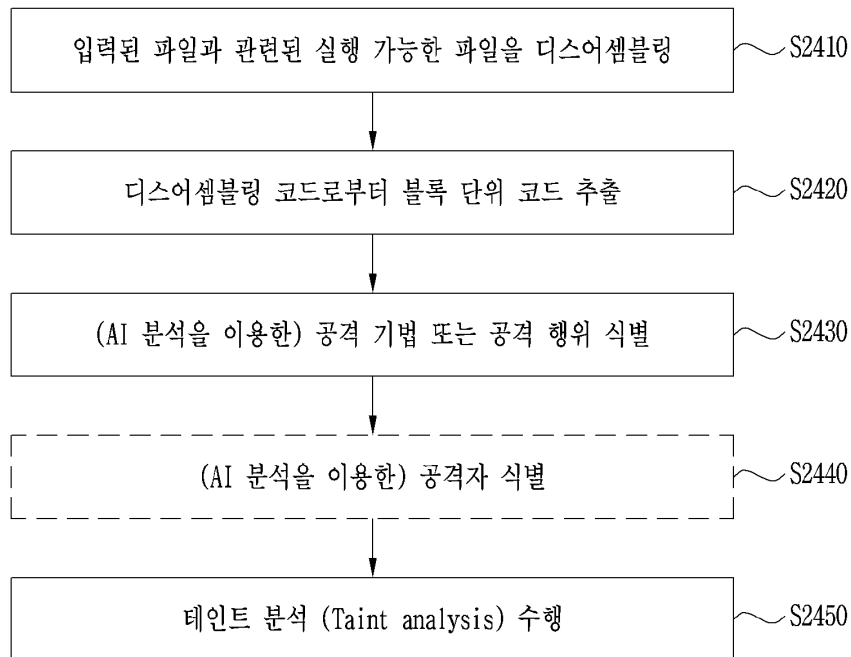
[도2]



[도3]



[도4]



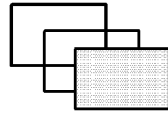
WO 2023/017931

PCT/KR2022/000955

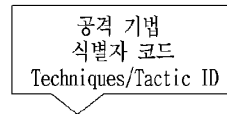
[도5]



EXE 파일

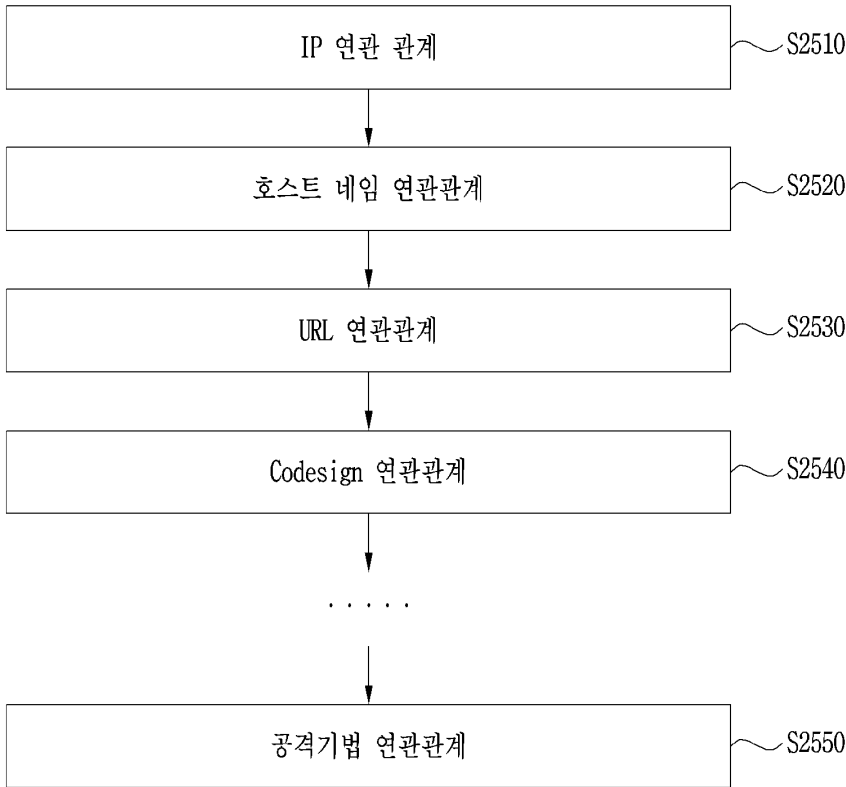


Disassembled code set

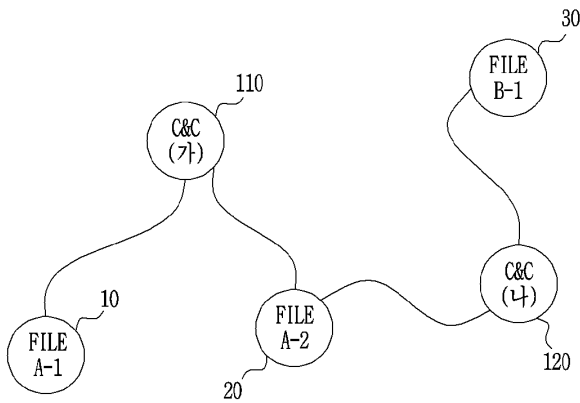


파일	OP 코드	T-ID	설명
malware.exe	MOV DWORD PTR SS: [EBP-4], 1 MOV DWORD PTR SS: [EBP-8], 2 MOV EDX, DWORD PTR SS: [EBP-8] LEA EAX, DWORD PTR SS: [EBP-4]	1022	시스템 주요 레지스트리 변경
	PUSH EBP MOV EBP, ESP SUB ESP, 18 AND ESP, FFFFFFF0 MOV EAX, 0	1077	시작 프로그램 등록
	LEA EAX, DWORD PTR SS: [EBP-4] MOV EDX, DWORD PTR SS: [EBP-8] LEA EAX, DWORD PTR SS: [EBP-4] LEA EAX, DWORD PTR SS: [EBP-4]	1034	윈도우 방화벽 해제
	PUSH EBP MOV EBP, ESP MOV EAX, DWORD PTR SS: [EBP+B] AND EAX, DWORD PTR SS: [EBP+C] POP EBP RETN	1090	신규 유저 추가
	CMP DWORD PTR SS: [EBP-4], 2 JNZ SHORT if. 00401035 PUSH if. 0040C008 CALL if.printf ADD ESP, 4 JMP SHORT if. 00401042	2011	백도어 생성
	CMP DWORD PTR SS: [EBP-B], 1 JE SHORT switch. 00401027 CMP DWORD PTR SS: [EBP-B], 2 JE SHORT switch. 00401036 CMP DWORD PTR SS: [EBP-B], 3 JE SHORT switch. 00401045 JMP SHORT switch. 00401054	3744	보안 프로그램 동작 중지

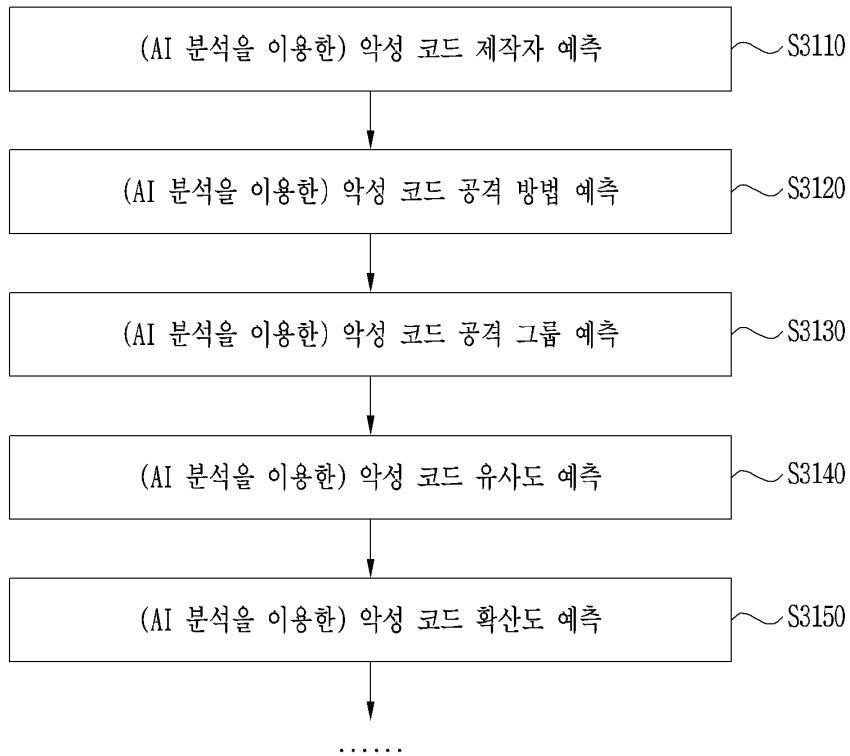
[도6]



[도7]



[도8]



[도9]

Query (A)

"2020년 3월 1일 오후 4시 ~ 2020년 3월 2일 오전 9시
사이에 Anti-Virus 40개 이상 탐지한 악성코드 중에
탐지한 Anti-virus 탐지명 중에 "*ransomware*" 라는
단어가 들어가 있고 EXE 파일 타입이면서 유포지(ITW)가
"*go.kr*"이고 CodeSign 서명 정보가 존재하는
파일 크기 10MB 이하의 파일"

Query (B)

"2020년 3월 1일에 Anti-Virus 10개 이하 탐지한 파일
중에 HWP, DOC, PPT, PDF, XLS 파일 타입이면서
유포지가 존재하고 행위 분석 결과 "powershell.exe" 또는
"vbscript.exe"가 실행되는 파일 크기 10MB 이하의 파일"

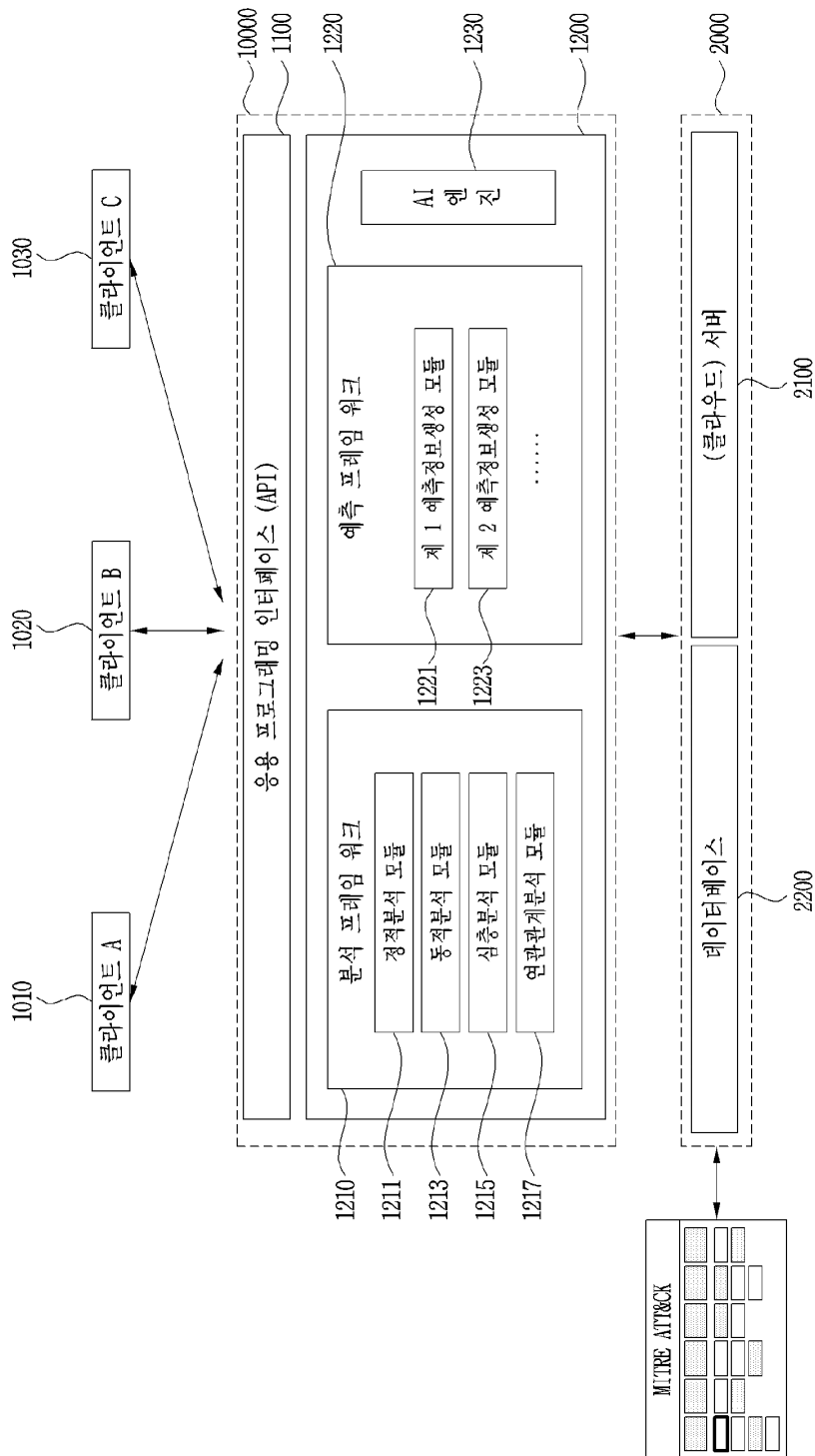
Query (C)

"2019년 1월 ~ 12월에 Anti-Virus 5개 이상 탐지한 파일
중에 EXE_32, EXE_64 파일 타입이면서 유포지가 존재하고
유포지 주소가 "nexon.com"이 아니면서 파일명에 "nexon"
이라는 단어가 들어가며 행위 분석 결과 "방화벽 설정을 수정"
또는 "시작 프로그램에 등록" 행위가 실행되면서 184.55.38.2에
접속 시도를 하는 파일 크기 100KB 이상의 파일"

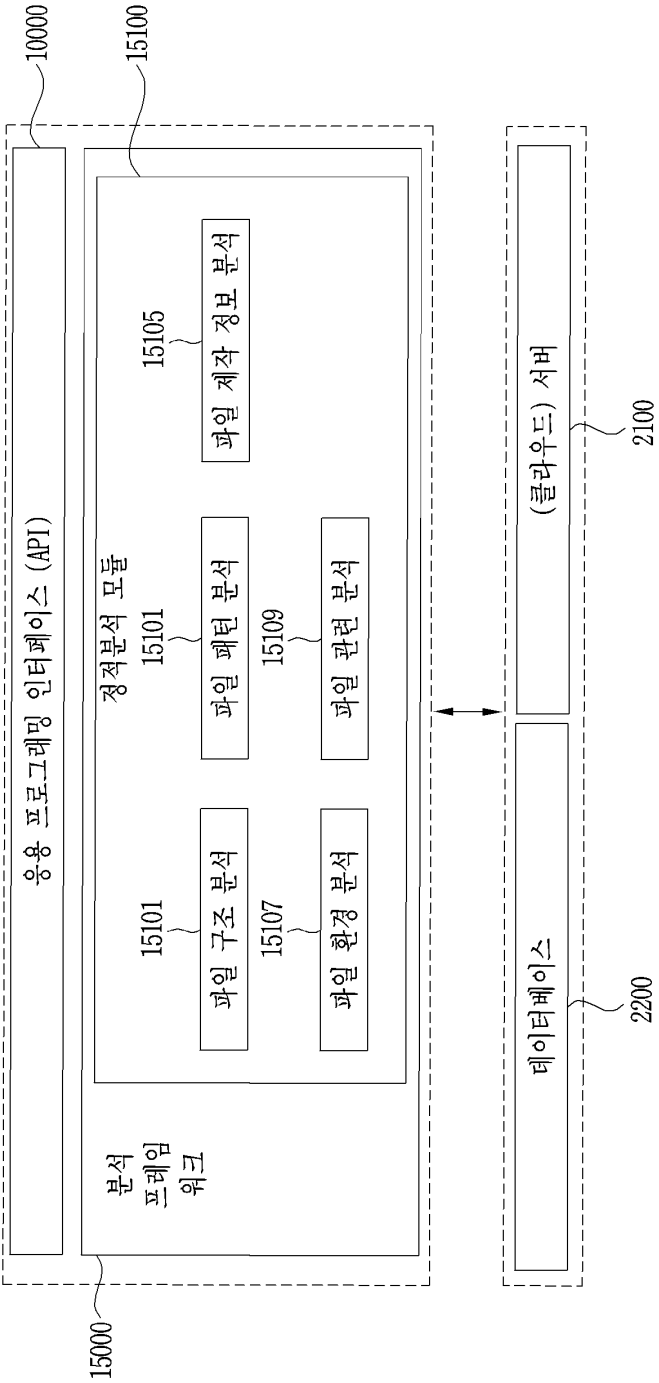
Query (D)

"2019년 1월 ~ 12월에 Anti-Virus 20개 이상 탐지한 파일 중에
문서 (hwp, doc, ppt, xls, pdf) 파일 타입이면서 kaspersky의
탐지명에 "not-virus"가 들어가지 않고 유포지 주소가 "*.kr*"이
들어가는 파일의 매일 통계 정보"

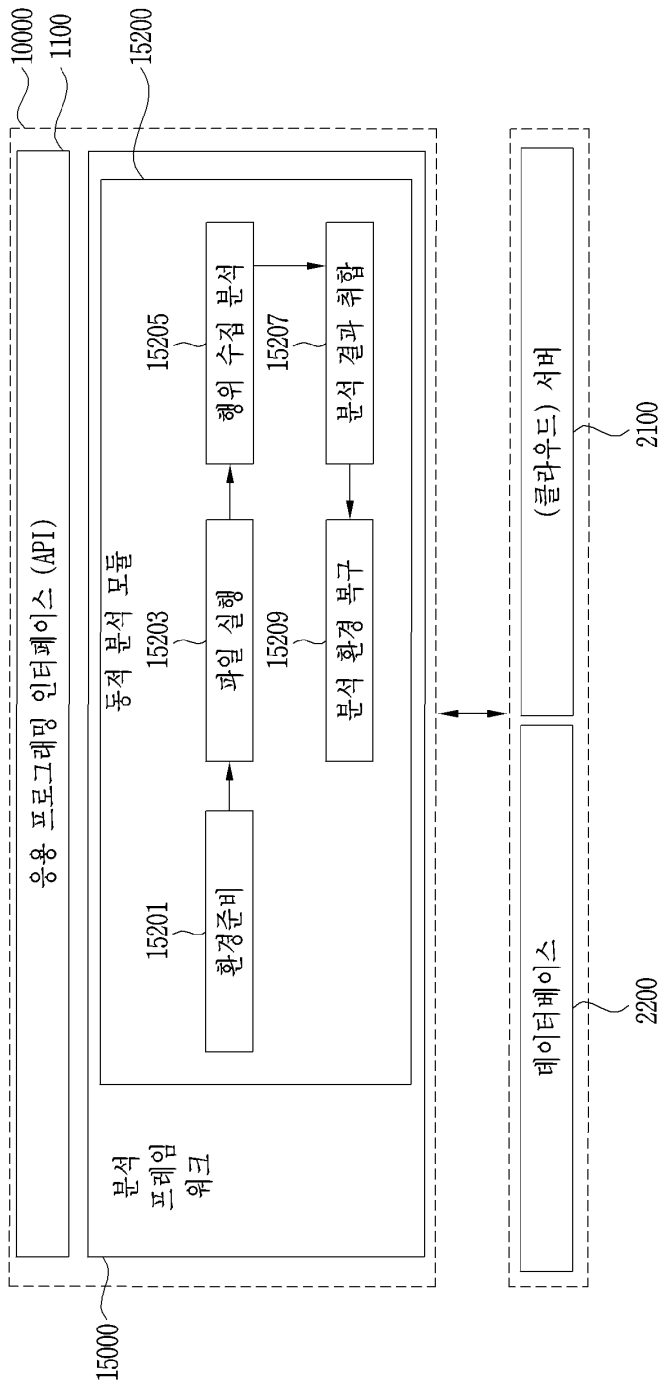
[도 10]



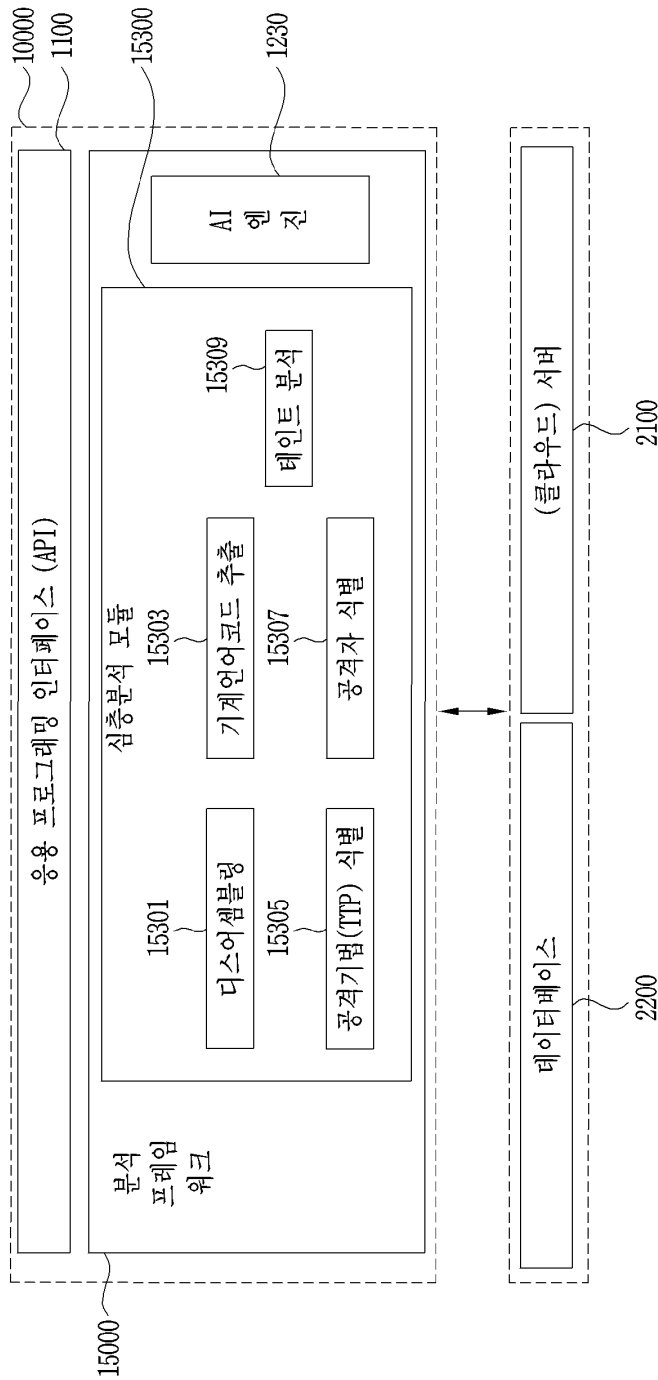
[도11]



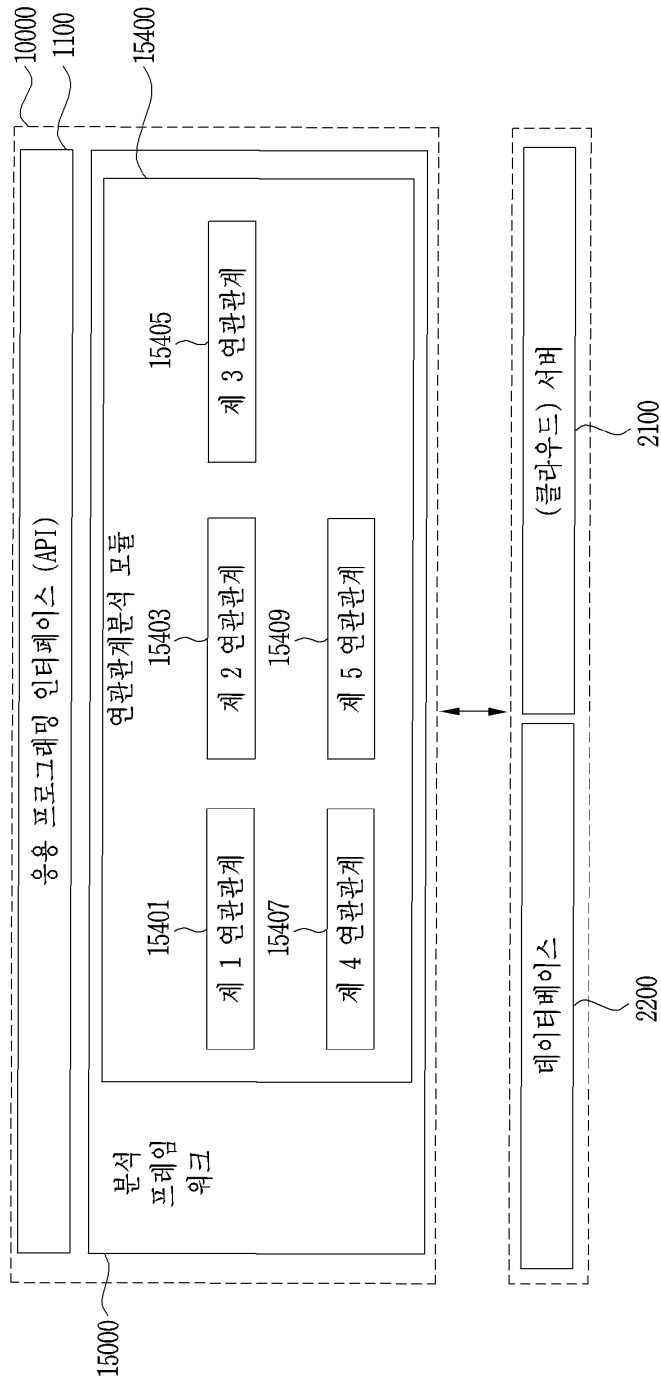
[도12]



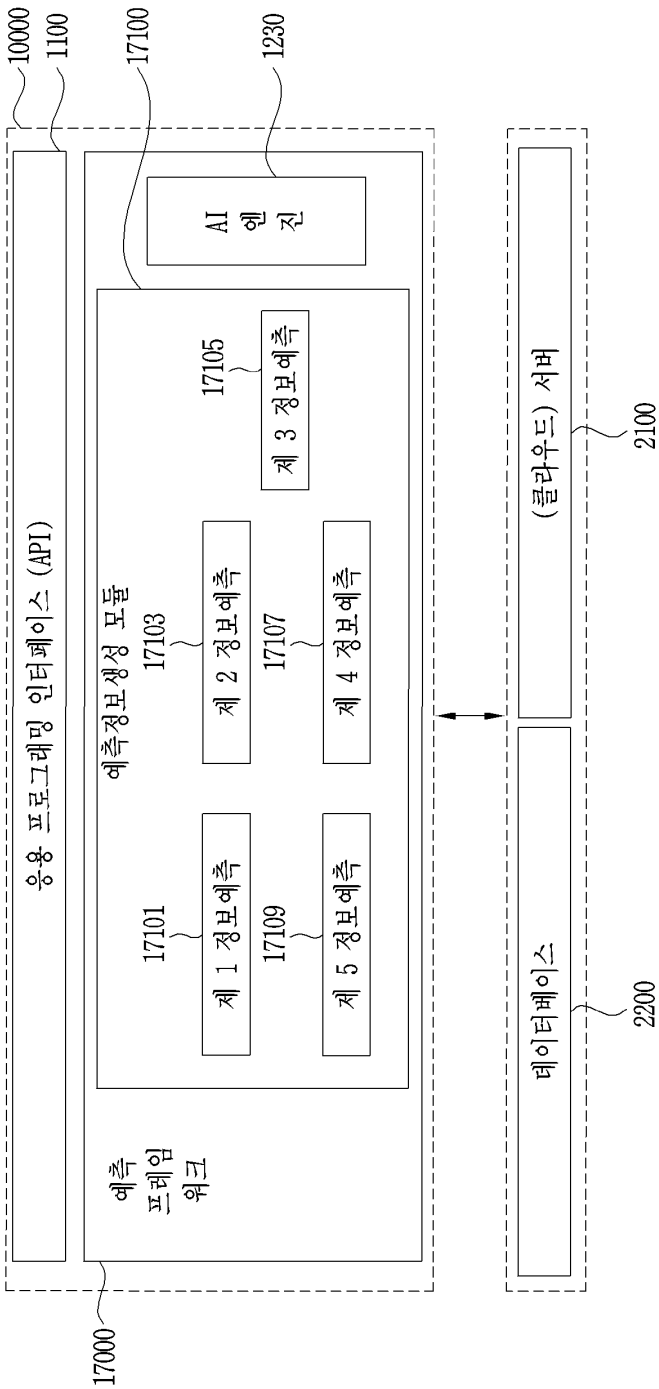
[도 13]



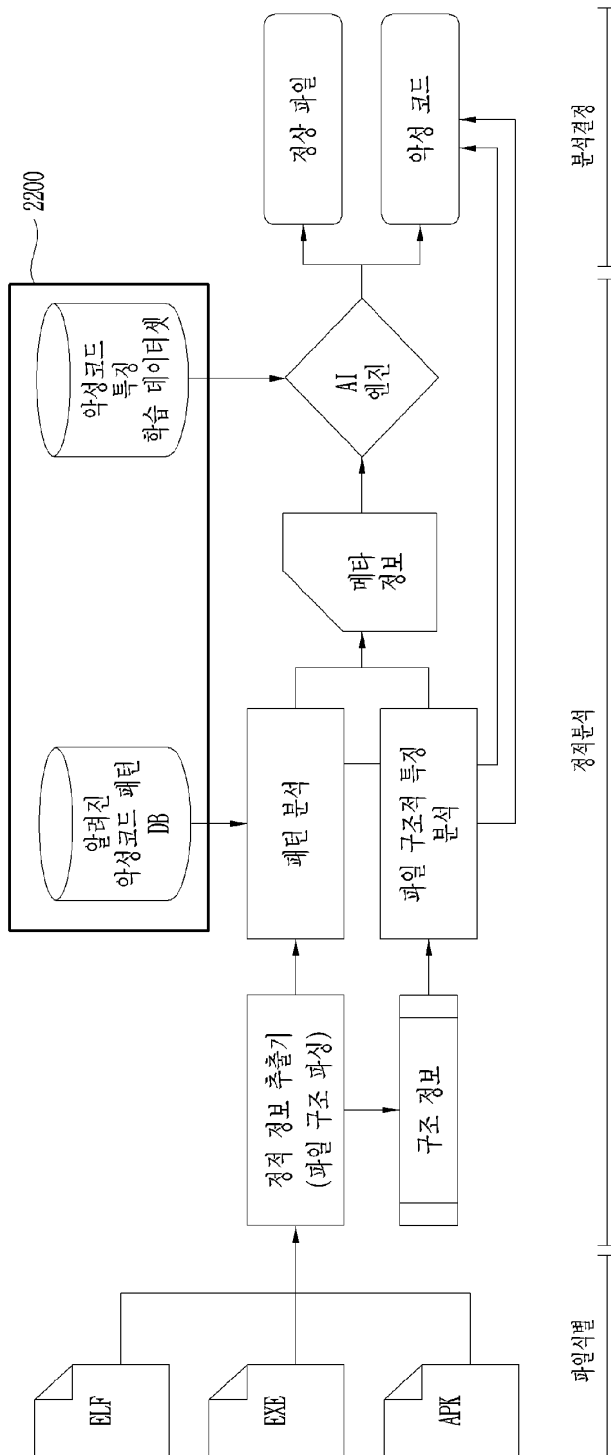
[도14]



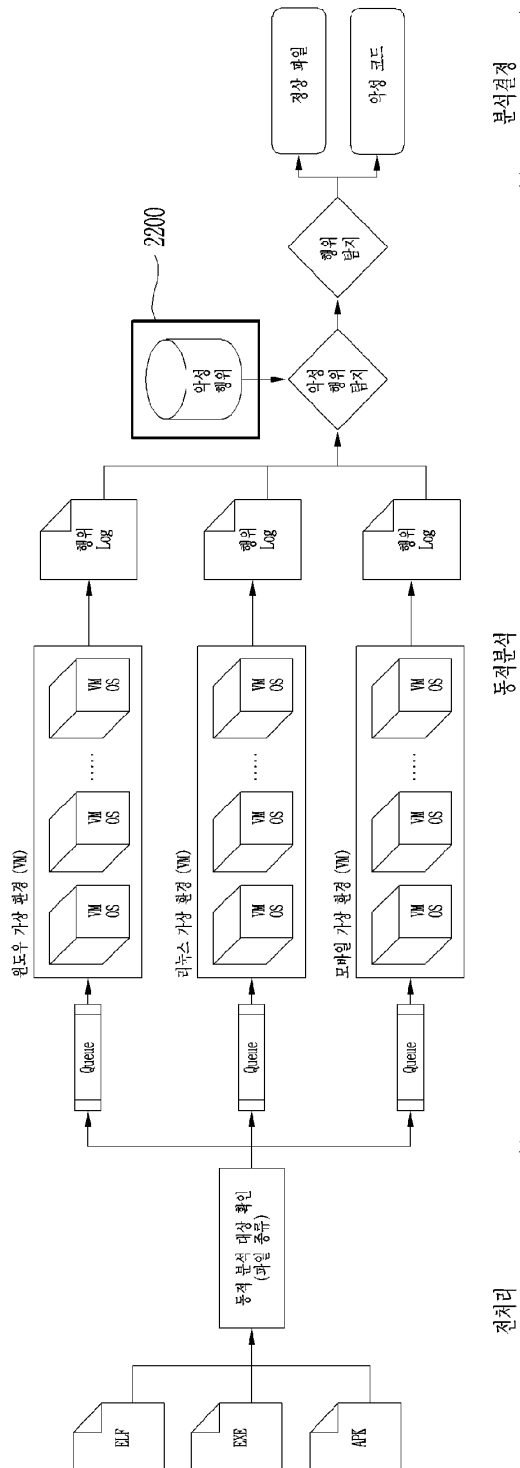
[도15]



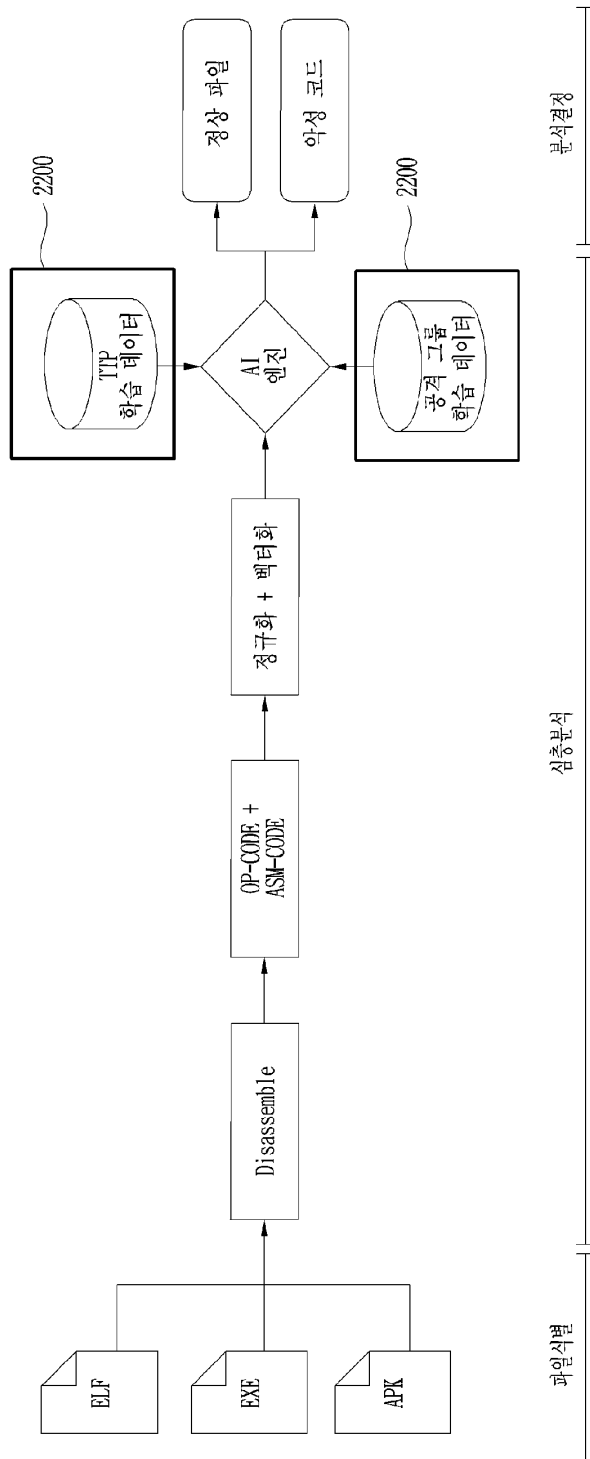
[도16]



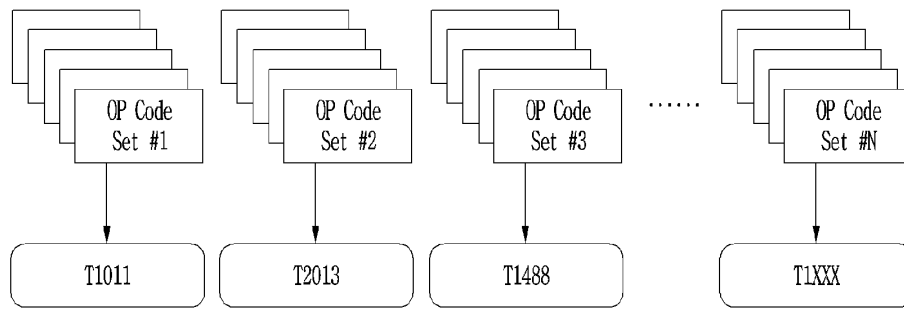
[도17]



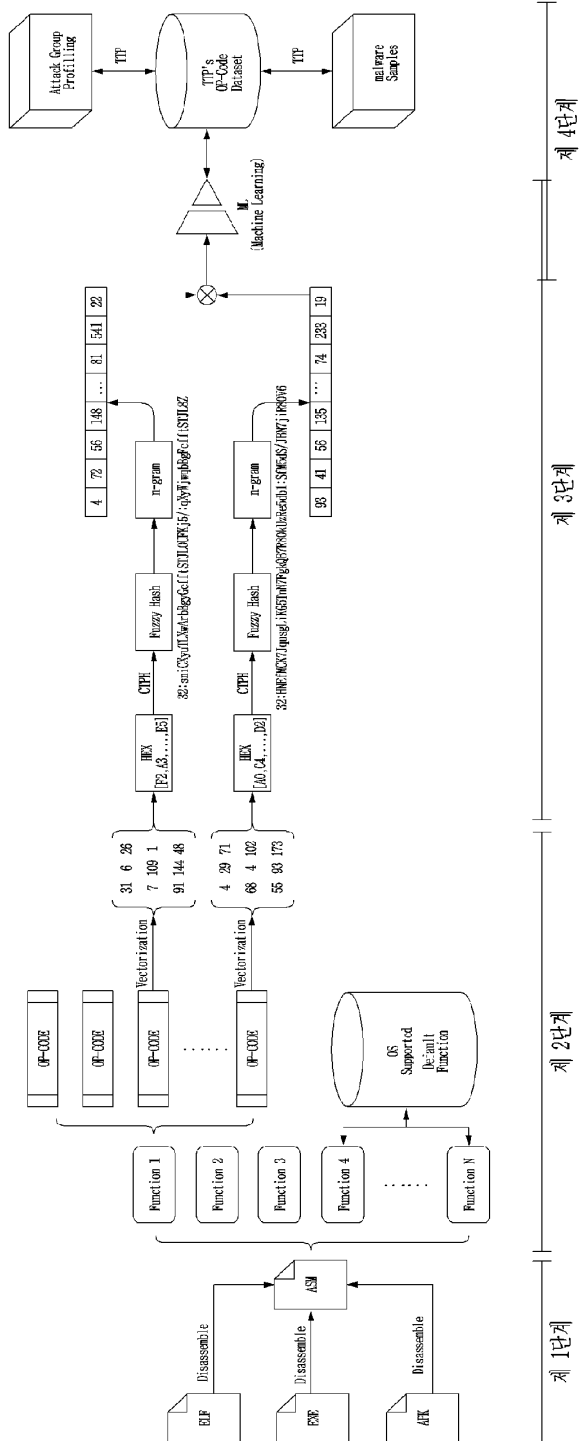
[도18]



[도 20]



[도 21]



[도 22]

OP-CODE`	OP-CODE → CRC-16	ASM-CODE	ASM-CODE → CRC-32
push	0x45E9	55	0xC9034AF6
mov	0x10E3	8B EC	0x3012FD2C
lea	0xAACE	8D 45 0C	0x9214A6AA
push	0x45E9	50	0xB969BE79
push	0x45E9	6A 00	0xDECB91D2
push	0x45E9	FF 75 08	0x1D4AE87E
push	0x45E9	6A 01	0xA9CCA144
call	0x09F8	FF 15 B0 20 40 00	0x284055E2
pop	0x7117	59	0xC0B506DD
push	0x45E9	50	0xB969BE79
call	0x09F8	E8 AB FF FF FF	0x4452C315
add	0x8B0B	83 C4 10	0xAE137EE5
pop	0x7117	5D	0xC7D8C2C4
retn	0x12B3	C3	0xD06F7C87

WO 2023/017931

PCT/KR2022/000955

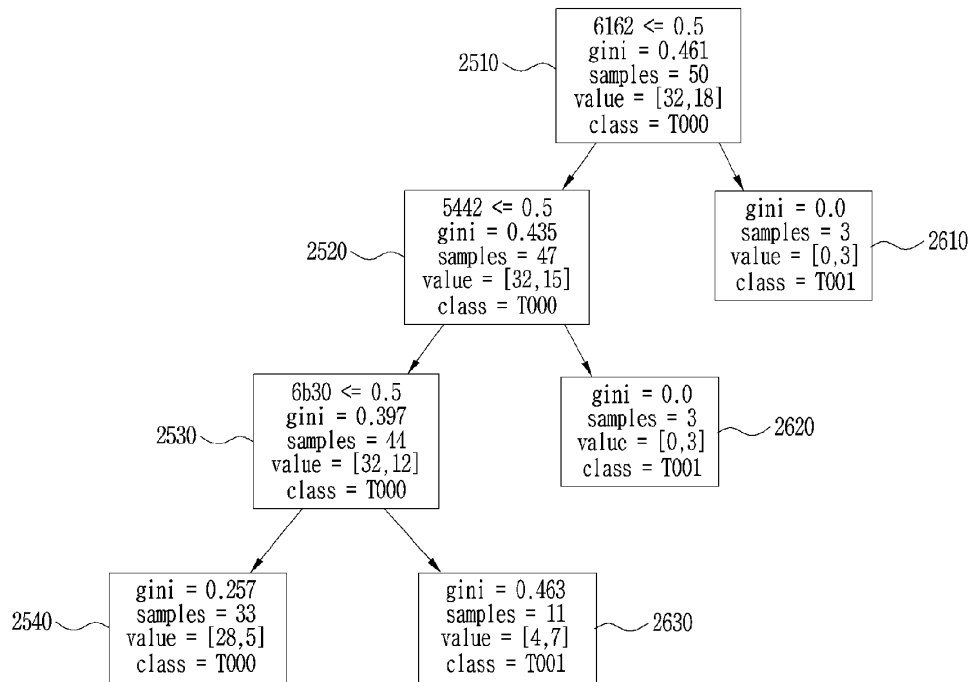
[도 23]

OP-CODE Vector	ASM-CODE Vector
17897	201 3 74 246
4323	48 18 253 44
43726	146 20 166 170
17897	185 105 121 44
17897	222 203 145 210
17897	29 74 232 126
17897	169 204 161 68
2552	40 64 85 226
28951	192 181 6 221
17897	185 105 190 121
2552	68 82 195 21
35595	174 19 126 229
28951	199 216 194 196
4787	208 111 124 135

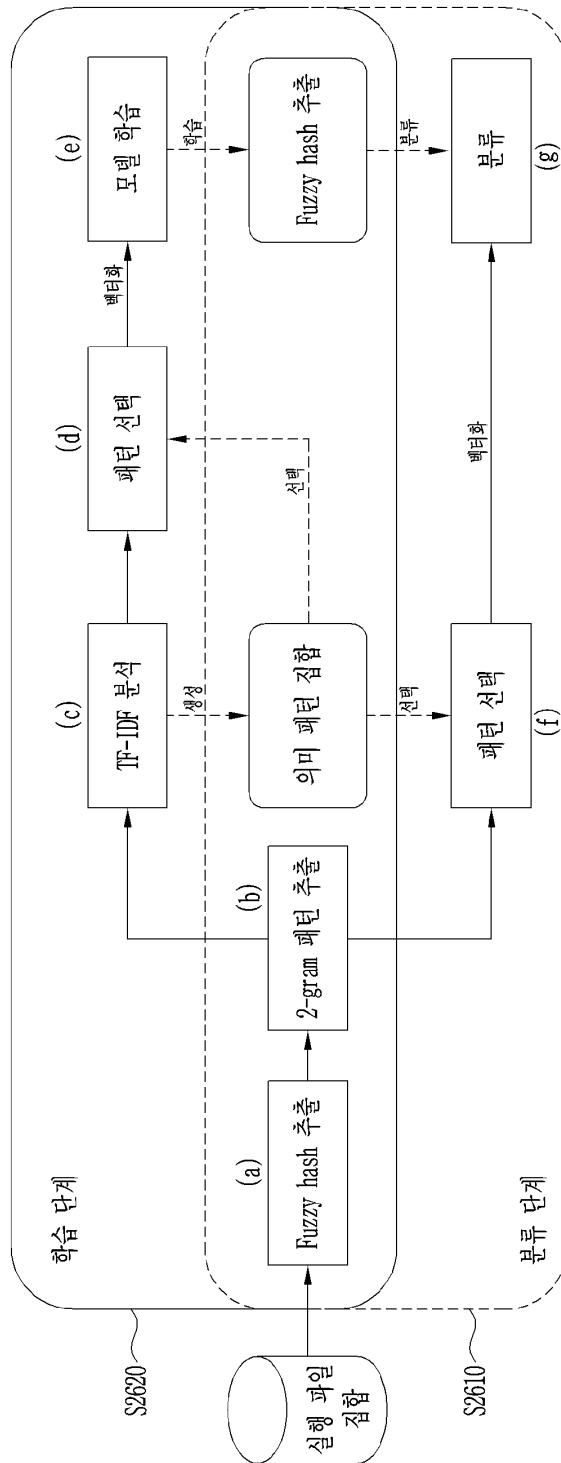
[도24]

Fixed block Original	content	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1
	ascii val	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	48	49
	ascii sum	394		410		426		442		458		474		340															
KaQ6KaU	b64 char	K		a		q		6		K		a		U															

[도 25]



[도26]

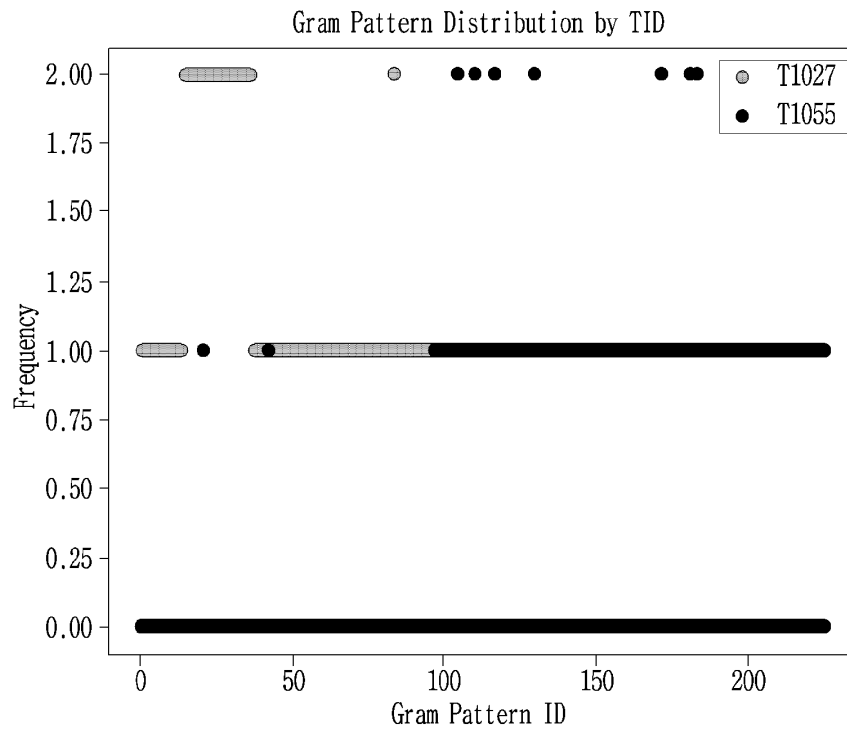


Label		SHA-256 (size)	N-gram
T-ID	Attacker (or Group)	(OP-CODE + ASM-CODE)'s Fuzzy Hash	
T10XX	TA504	389E03B1A1FD1C5....	{ "3736":1, "3645":1, "4563":1, "6344":1, "4472":1, "7255":1
		32:76EcDrURBPQk58t...	
	TA504	E3EC2AA04AFEC6...	{ "3736":1, "3645":1, "4563":1, "6344":1, "4472":1, "7255":1, "5552":1, "5242":1, "4250":1.....
		32:76EcDrURBPQk58tGcoHE...	

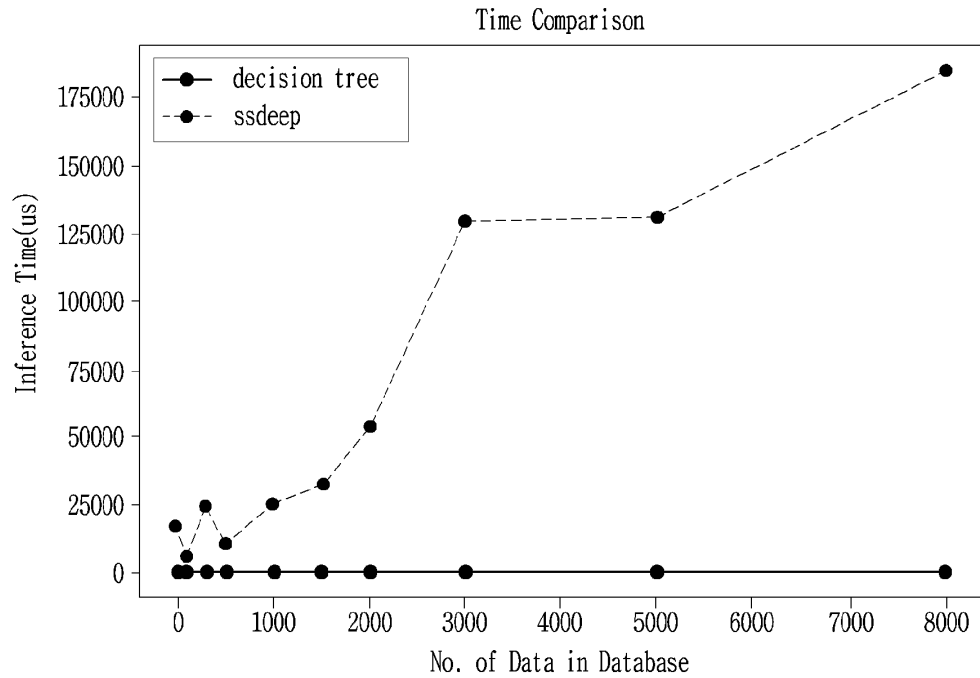
The figure displays a Euclidean Distance Matrix (D-matrix) for five samples: T1027(T), T1027(K), T1055(T), T1055(K), and T1055(L). The matrix is symmetric, with the diagonal elements representing a distance of 0. The color scale ranges from 0 (dark gray) to 14 (light gray). The matrix shows that T1027(T) and T1027(K) are relatively close (distance ~2-4), while T1055(T) and T1055(K) are also close (distance ~2-4). The distances between T1027 and T1055 samples are higher, ranging from ~6 to ~14.

	T1027(T)	T1027(K)	T1055(T)	T1055(K)	T1055(L)
T1027(T)	0	~2	~14	~14	~14
T1027(K)	~2	0	~14	~14	~14
T1055(T)	~14	~14	0	~2	~14
T1055(K)	~14	~14	~2	0	~14
T1055(L)	~14	~14	~14	~14	0

[도29]



[도30]



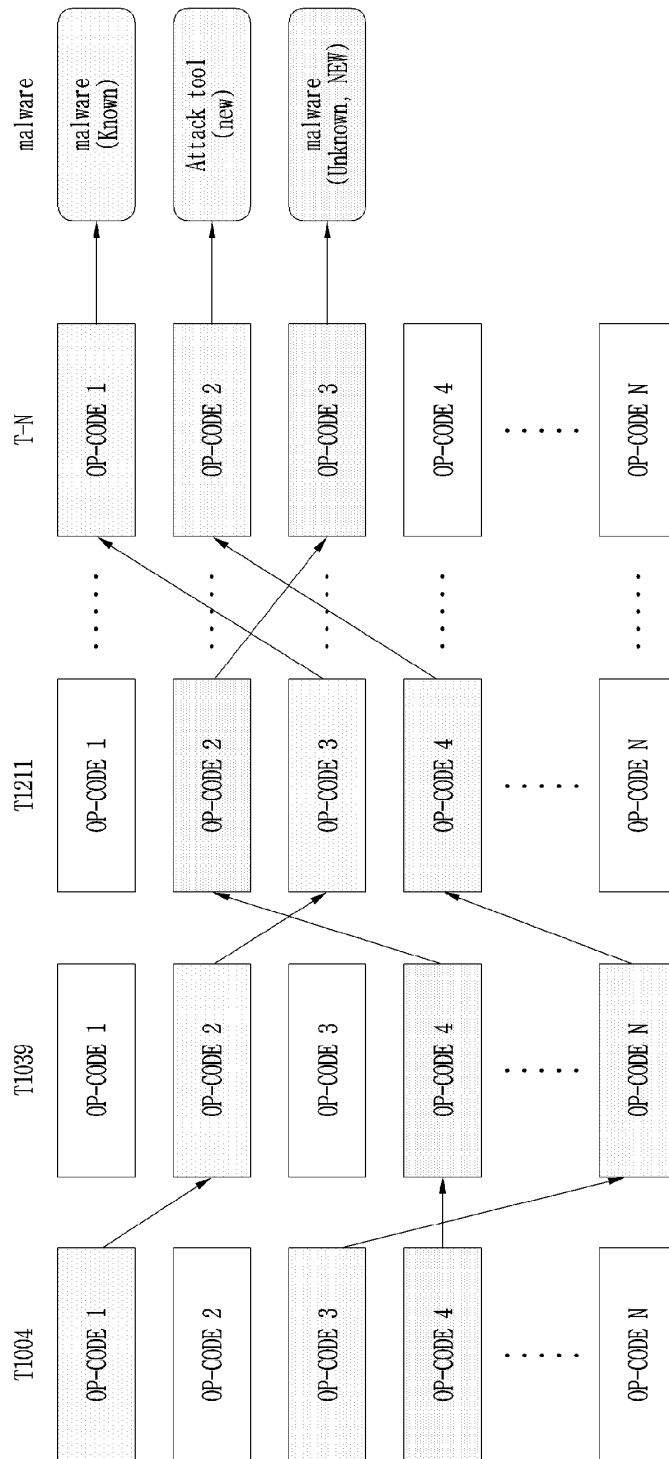
[도31]

Cylance	① Unsafe
eGambit	① Unsafe.AI_Score_100%
SentinelOne (Static ML)	① Static AI-Malicious PE
Symantec	① ML.Attribute.HighConfidence
SecureAge APEX	① Malicious
AVG	① FileRepMalware
Bkav Pro	① W32.AIDetect.malware1
Cynet	① Malicious (score:99)
Sophos	① ML/PE-A

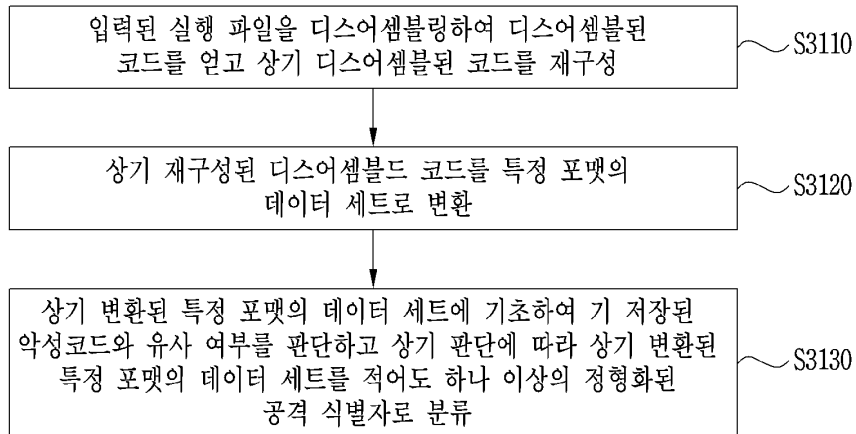
3210

3220

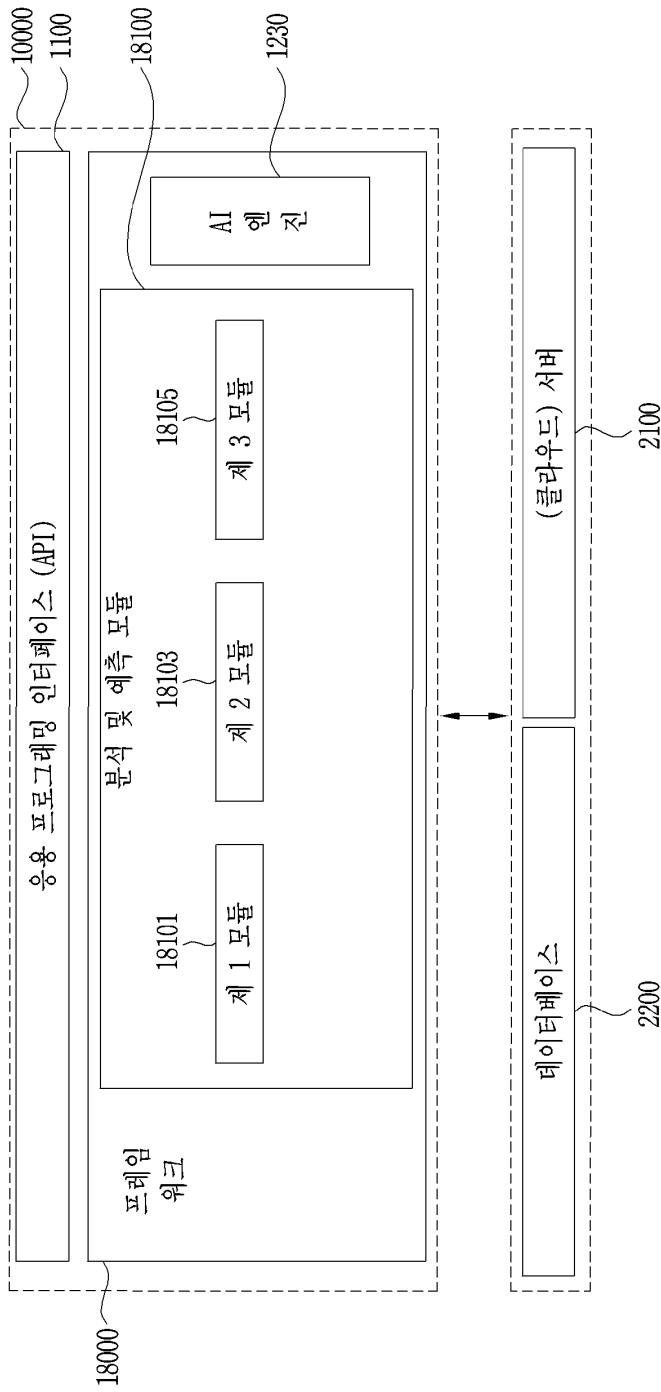
[도 32]



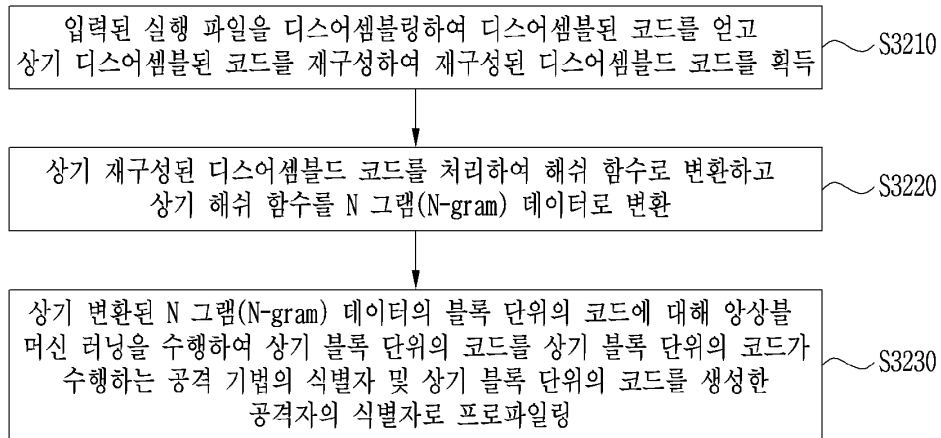
[도33]



[도34]



[도35]



[도36]

