情 報 保 護 學 會 誌
第 18 券 第 1 號, 2008. 2

소프트웨어 참조 데이터세트 구축 동향

김 기 범*, 박 상 서*

요 약

디지털 포렌식에서 증거 데이터 분석의 효율성을 높이기 위해서는 잘 알려진 파일을 분석 대상에서 제외하거나, 특정 파일의 존재여부에 대한 검사가 필요하다. 이를 위하여, 시스템 파일, 폰트 파일, 응용 프로그램 파일 등 분석 이 필요없는 파일 및 루트킷, 백도어, 익스플로잇 코드 등 악성 파일에 대한 해쉬 값을 미래 계산하여 저장해 둔 것을 소프트웨어 참조 데이터세트라고 한다. 이 논문에서는 소프트웨어 참조 데이터세트 구축에 대한 주요 동향에 대하여 살펴본다. 특히, 소프트웨어 참조 데이터세트 구축을 주도하고 있는 미국의 NSRL RDS에 대하여 활용가능성 측면에서 구체적으로 살펴본다. NSRL RDS에 대한 분석결과 실제 컴퓨터 포렌식 도구에서 활용하기 매우 어렵다는 사실을 알 수 있다.

Ⅰ. 서 론

급속히 지능화되는 범죄 및 불법 활동에 대한 철저한 수사를 위해서는 컴퓨터, 핸드폰, PDA, USB 메모리 등의 디지털 매체에 저장된 증거 자료에 대한 철저한 조사 및 분석이 요구된다. 이에 따라 디지털 증거 획득 및 분석 작업을 지원하는 디지털 포렌식 기술에 대한 활발한 연구가 진행 중이다. 디지털 포렌식은 획득된 증거 데이터를 효과적으로 빠른 시간 안에 찾을 수 있도록 지원해야 한다.

증거 데이터 분석의 효율성을 높이기 위해서는 잘 알려진 파일은 검색 대상에서 제외하여 주목해서 검색할 대상을 선정하는 기술이 필요하다. 이를 위한 기술로 사전에 시스템 및 폰트, 응용 프로그램 파일 등에 대한 해쉬 값을 계산해 두었다가 이를 참조 데이터세트(Reference Data Set: RDS)로 활용하여 검색 대상에서 제외하는 기법이 널리 이용되고 있다. 또한, 해킹 사고 조사를 원활히 수행하기 위해서는 해당시스템에 설치된 악성 파일을 정확히 식별할 수 있어야 한다. 이를 위하여 루트킷, 백도어, 익스플로잇코드, 웜바이러스 등을 구성하는 파일들에 대한 해쉬 값을 미리 계산하여 특정 시스템에 존재하는지 여부를 검사할 수 있어야 한다.

알려진 정상 파일에 대한 해쉬 값 정보 제공 기관으로 미국의 NIST(National Institute of Standard and Technology), NDIC(National Drug Intelligence Center) 및 SUN Microsystems사가 있다. NIST의 경우 NSRL(National Software Reference Library) RDS라는 프로젝트명으로 참조 데이터세트 구축사업을 수행하고 있다[1]. 즉, 2008년 1월 현재 RDS 2.18 버전이 최신 버전이며 4천4백만 여개의 파일에 대한 참조 데이터를 구축하여 일반에 공개하고 있다. 또한, 미국의 NDIC은 수사기관이 요청하는 경우 자체적으로 구축한 RDS를 제공하고 있다[2]. 뿐만 아니라, SUN사는 자사에서 발표하는 운영체제 및 패치 등의 파일에 대한 3백8십만 여개의 MD-5 해쉬 값을 인터넷에 공개하고 있다[3].

악성 파일에 대한 해쉬 값 정보는 Rootkit Hunter 프로젝트[4] 및 CyberAbuse RootkitID[5] 등이 있다. 현재 Rootkit Hunter만이 명맥을 유지하고 있는 현실이다.

국내에서는 아직까지 일반에 공개된 RDS 구축이 전무한 실정이다. 또한, NIST의 RDS의 경우 방대한 데이터 양에 비하여 국내에서 사용되는 소프트웨어에 대해서는 Windows 운영체제 정도가 구축되어 있는 상황이다. 이러한 현실로 인하여 국내 수사 환경에서 아직까지 RDS를 활용하여 수사의 효율성을 높이는 작업을 이루어지고 있지 않다.

이 논문에서는 소프트웨어 참조 데이터세트 구축 동향에 대하여 전반적으로 살펴본다. 또한, NSRL RDS를 활용성 측면에서 세부적으로 분석하여 국내 수사환경에

* ETRI 부설연구소 (kibom@ensec.re.kr, spark@ensec.re.kr)

서 실제 사용할 수 있는지를 분석한다.

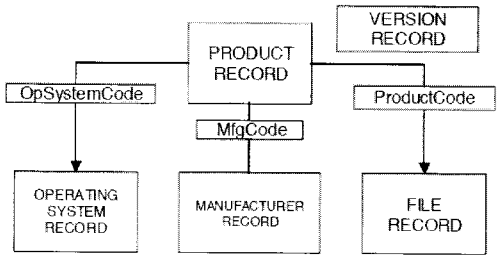
Ⅱ. RDS 구축 동향

디지털 포렌식의 효율성 향상을 위해서는 증거 분석 대상 중 특정 파일을 조사 대상에서 제외하거나 집중 검토 대상으로 선정하는 RDS 데이터 활용이 필수적이다. RDS는 자료의 특성상 중복 구축을 방지하기 위하여 미국의 경우 NIST를 전담기관으로 선정하고 있고, 유럽의 경우 NIST에서 생성한 데이터를 활용하고 있다. 이 장에서는 NIST에서 수행 중인 NSRL RDS에 대하여 살펴보고, 그 외 기관의 RDS 관련 동향을 기술한다.

2.1. NIST의 NSRL RDS

NSRL RDS는 미국의 NIST 산하 CFTT(Computer Forensics Tool Testing)에서 제공하는 국가 표준 소프트웨어 참조 데이터세트이다. NSRL RDS의 목적은 범죄에 사용되는 컴퓨터 파일의 식별 자동화와 증거에 포함된 파일 조사를 효율적으로 지원하는 것이다. 이를 위하여, 전세계 각종 S/W 및 알려진 파일을 수집 하여 이에 대한 정보와 해쉬 값을 DB로 구축하고 있다. 2008년 1월에 다운로드 가능한 최신 버전은 RDS 2.18로서, 44,334,490개의 파일에 대하여 SHA-1, MD5, CRC32로 계산된 해쉬 값을 인터넷에 공개하여 누구나 활용할 수 있도록 하고 있다.

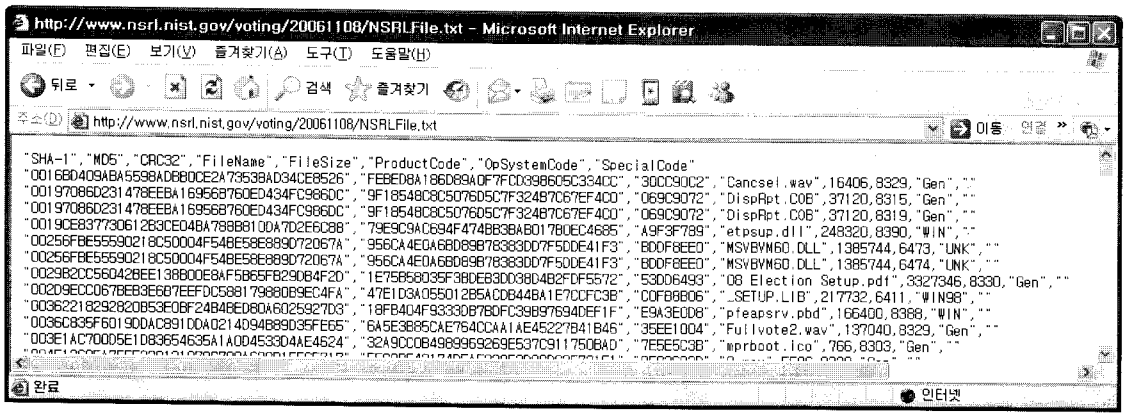
CFTT는 소프트웨어를 제조회사로부터 직접 기증 받거나, 불가능한 경우 구매를 통하여 RDS DB를 구축한다. 구축 대상은 인스톨 CD의 파일 및 컴퓨터에 설치된 파일로부터 해쉬 값을 계산한다. CFTT는 파일에 대한 해쉬 값 뿐만 아니라, 파일에 대한 운영체제 정보, 제조회사 정보, 제품정보에 해당하는 메타 데이터 정보를 함께 구축하고 있다. 또한, RDS 데이터 자체에 대한 버전 관리를 위하여 버전 정보를 포함하고 있다. 이에 따른 NSRL RDS의 논리적인 레코드간의 관계는 [그림 1]과 같다.



〔그림 1〕 NSRL RDS의 논리적 레코드 구조

[그림 1]에 도식화된 각각의 레코드는 참조 데이터 구축 대상 소프트웨어에 대한 주요 정보를 모두 포함하고 있는 것이며, 각각의 파일에 대한 해쉬 값을 포함하는 NSRL RDS의 파일레코드(NSRLFile.txt)는 [그림 2]와 같다. [그림 2]의 각각의 항목에 대하여 살펴보면 다음과 같다.

- SHA-1: 파일에 대하여 SHA-1 해쉬 알고리즘을 적용하여 계산한 값이다.
- MD5: 파일에 대하여 MD5 해쉬 알고리즘을 적용



〔그림 2〕 NSRL RDS의 해쉬 값 데이터

하여 계산한 값이다.

- CRC32: 파일에 대하여 CRC32 알고리즘을 적용하여 계산한 값이다.
- FileName: 파일에 대한 이름이다.
- FileSize: 파일의 크기이다.
- ProductCode: 파일이 포함된 제품에 대한 코드 값으로 정수형 숫자로 표현되며, NSRLProd.txt 파일로 공개된다.
- OpSystemCode: 파일이 운용되는 운영체제에 대한 정보로서, 범용인 경우 "Gen", Windows XP인 경우 "WinXP" 형태로 표현한다. NSRLOS.txt 라는 파일명으로 공개된다.
- SpecialCode: 파일의 악성인가 여부를 표시하기 위하여 사용되는 값으로 단일 문자로 표현한다.

CFTT는 인터넷에 4개의 iso 파일을 공개하고 있으며, 이는 각각 비영어권 소프트웨어, 운영체제, 어플리케이션 소프트웨어, 이미지&그래픽스이다. 각각의 파일에는 제조회사, 운영체제, 제품에 대한 메타데이터 파일 및 해쉬 값을 저장하는 RDS 파일로 구성된다.

2.2. NDIC의 HashKeeper

미국의 마약정보센터(NDIC)에서 컴퓨터 포렌식 수사에 사용할 수 있는 해쉬 셋을 제작하여 HashKeeper라는 이름으로 배포하고 있다. NDIC 홈페이지와 http://groups.yahoo.com/group/hashkeeper를 통하여 인증된 정부 기관에 대하여 해쉬 데이터를 제공한다. 300개 이상의 해쉬 셋을 보유한 것으로 알려져 있다.

2.3. SUN사의 Fingerprint 데이터

SUN 사에서 판매하는 운영체제(SunOS) 및 각종 프로그램에 대한 판매 버전 및 패치 버전에 대한 무결성 검증을 목적으로 인터넷을 통하여 파일에 대한 해쉬 값을 공개하고 있다. 해쉬 알고리즘은 MD-5만을 사용하고 있으며, 현재 3백8십만 여개의 파일에 대한 해쉬 값을 공개하고 있다.

2.4. HashDig

각종 형식의 해쉬 셋을 입력으로 받아 해쉬 셋에 대한 통합적인 참조가 가능하도록 만든 공개 도구이다[6]. PERL 언어로 작성되었으며, B-Tree를 이용하여 데이터를 저장하고 있다. 현재 NSRL RDS, Sun의 Fingerprint 데이터, HashKeeper 등에 대한 입력 기능을 제공한다.

2.5. Rootkit Hunter

유닉스 계열의 운영체제에서 악성 파일의 존재 여부를 찾기 위한 Rootkit Hunter 프로젝트에서는 루트킷, 백도어, 공격 코드에 대한 MD5 해쉬 값을 기반으로 자료를 찾는다. 즉, RDS 관점에서 보았을 때 악성 파일에 대한 MD5 해쉬 값 정보를 얻을 수 있다. Rootkit Hunter에서 제공하는 악성파일은 80여개로 디지털 포렌식에서 활용하기에는 상당히 부족하며, BSD 및 Linux 계열의 운영체제에 대한 정보만을 갖고 있다.

Ⅲ. NSRL RDS 데이터 상세 분석

NSRL RDS에 대한 상세 분석은 2007년 6월에 공개된 RDS 2.17 버전을 대상으로 수행한다. 상세 분석을 수행하기 위하여 RDS 2.17의 모든 데이터를 [그림 1]과 같은 레코드 구조로 스키마를 구성하고, MS-SQL DBMS에 제조회사 정보, 운영체제 정보, 제품정보를 차례를 입력하여 메타데이터 구성을 수행한다. 이를 바탕으로 4개로 분리된 NSRLFile.txt를 DB에 import하여 분석을 수행한다. 분석을 수행한 상세 결과를 살펴보면 다음과 같다.

3.1. 메타 데이터와 파일 레코드의 불일치

데이터 분석을 위하여, 제조회사 정보, 운영체제 정보, 제품정보를 차례를 입력하여 메타데이터를 구성하는 과정에는 데이터의 불일치가 발생하지 않는다. [표 1]은 메타 데이터 정보에 대한 입력 결과이다.

〔표 1〕 메타 데이터 입력 결과

파일	전체 개수	입력 개수
NSRLMfg.txt	1,277	1,277
NSRLOS.txt	340	340
NSRLProd.txt	17,504	17,504

반면 4개의 NSRLFile.txt를 DB에 입력하는 과정에서 [표 1]과 같은 메타데이터 부재에 따라 입력할 수 없는 데이터가 존재한다. 파일 A, B, C, D는 각각 NSRL에서 배포하는 4개의 iso 파일내의 압축을 해제하여 생성되는 NSRLFile.txt에 해당한다.

〔표 2〕 파일레코드 입력 현황

파일	전체 개수	입력 개수	입력 불가
A	12,253,935	11,983,710	270,225
B	4,053,716	3,238,424	815,292
C	21,700,239	19,869,329	1,830,910
D	5,095,602	4,978,200	117,402
계	43,103,492	40,069,663	3,033,829

[표 2]의 결과에서 알 수 있듯이 7%의 데이터는 메타데이터와 전혀 매핑할 수 없는 해쉬 값을 갖는 파일 레코드임을 알 수 있다. [표 2]에서 입력 불가인 데이터 각각에 대하여 어떤 메타데이터 정보가 존재하지 않는가를 분석한 결과를 살펴보면 [표 3]과 같다.

〔표 3〕 파일레코드 입력 불가 원인

파일	제품정보 부재	운영체제 정보 부재	모두 부재
A	204	270,225	204
B	83	815,292	83
C	2,919	1,830,910	2,919
D	177	117,402	177
계	3,383	3,033,829	3,383

[표 3]의 결과에 따른 입력 불가 원인을 살펴보면, 파일 레코드와 매핑되지 않는 운영체제 정보가 상당히 많음을 알 수 있다. 해당 데이터를 살펴보면 운영체제 코드 값이 대부분 "UNKNOWN", "UNK", "GEN" 등으로 특정 운영체제가 아닌 경우가 대부분이다. 이에 따라, 해쉬 값을 갖는 파일 레코드는 존재하지만 해당 레코드가 어떤 운영체제에서 동작하는 제품인지 여부를 파악할 수 없기 때문에 RDS 데이터로 활용할 수 없는 문제점이 발생하게 된다.

3.2. 제품명의 불명확성

메타 데이터와 파일 레코드의 불일치로 인하여 전체 43,103,492의 파일 레코드에 대한 분석은 불가능하다는 결론이 도출된다. 이에 따라, 지금부터 DBMS에 입력 가능한 40,069,663개의 파일 레코드에 대하여 분석한 결과를 기술한다.

〔표 4〕 파일레코드 상위 제품 리스트

코드 값	제품명	개수
388	1,300,000 Corel Gallery	1,166,269
228	Gallery	671,558
4690	The Big Box of Art	581,753
4987	MSDN Disc 2427.1	320,851
402	Art Explosion	302,641
8122	MSDN Disc 2427.3	264,507
2592	Platforms, SDK/DDK, Developer Tools	262,989
3269	MSDN Disc 2041	235,664
7395	MSDN Disc 2428.4	223,083
3361	MSDN Disc 2307	219,832
6478	MSDN Disc2428.3	218,542
3172	Windows XP	210,114
5029	MSDN Disc 2428.2	204,063
4875	MSDN Disc 2428.1	204,038
2939	Windows DDks	196,051
2603	Platforms, SDK/DDK	182,926
1561	Platforms SDKs/DDKs	179,672
2553	Platforms, Servers, Applications	175,527
3264	MSDN Disc 3264	166,808
2704	Platforms, SDK/DDK	164,843

파일 레코드의 모든 데이터에 대하여 동일한 제품코드를 갖는 상위 제품 20개에 대한 목록은 [표 4]와 같다.

[표 4]의 결과는 제품명 및 제품코드로 디지털 포렌식 도구에서 활용할 RDS 데이터 추출이 매우 어려움을 알 수 있다. 왜냐하면, "Platforms, SDK/DDK"의 경우 제품명은 동일한 데 반하여 제품 코드 값만 다르기 때문이다.

[표 4]에서 식별된 문제점을 보다 명확히하기 위하여 Windows XP를 제품명으로 갖는 파일 레코드를 추출한 결과는 [표 5]와 같다.

〔표 5〕 제품명이 Windows XP의 경우

코드 값	제품 명	개수
1449	Windows XP Multilingual User Interface	0
1455	Windows XP Home Edition Release Candidate 1	0
1456	Windows XP Professional Release Candidte 1	0
1457	Windows XP Professional Checked Build Release Candidate 1	0
1507	Windows XP Driver Developmet Kit	0
1510	Windows XP	0
1511	Windows XP Professional	0
1512	Windows XP Professional Checked/Debug Build	0
1543	Windows XP Home Edition	0
1544	Windows XP Professional	0
1567	Windows XP	16,361
1568	Windows XP Home Edition	16,361
1571	Windows XP	19,546
1572	Windows XP Professional	19,546
1697	Windows XP Multilingual Interface	53,562
1711	Windows XP MultiLingual User Interface Pack	2,465
1746	Windows XP eMbedded Evaluation Software	0
2321	Windows XP	16,458
2323	Windows XP	19,681
2470	Windows XP Tablet PC Edition	20,997
2471	Windows XP	1,398
2472	Windows XP Service Pack 1 Checked/Debug Build	0
2568	Windows XP	0
2589	Windows XP	0
2594	Windows XP versions	0
2605	Windows XP	0
2624	Windows XP	0
2638	Windows XP	0
2705	Windows XP	0
2706	Windows XP Tablet PC Edition	0
2742	Windows XP	0
2743	Windows XP Tablet PC Editition	0
2803	Windows XP	0
2808	Windows XP	65,790
2812	Windows XP Tablet PC Edition	0
2814	Windows XP	47,648
2815	Windows XP Tablet PC Edition	0
2891	Windows XP	0
2912	Windows XP	52,855
2913	Windows XP	0
2914	Windows XP	0
2944	Windows XP Tablet PC Edition Checked/Debug Build	0
2949	Windows XP Home Edition	157,085
2950	Windows XP Professional	0
2960	Windows XP Versions	0
2968	Windows XP Versions	0
2975	Windows XP Versions	0
3039	Windows XP Professional 2002 Service Pack 1	20,186
3126	Windows XP	19,614
3154	Windows XP	0
3155	Windows XP	0
3164	Windows XP	56,038
3165	Windows XP	0
3166	Windows XP	0
3172	Windows XP	210,114
3236	Windows XP	16,355
3292	Windows XP	23,483
3293	Windows XP	20,093
4917	Windows XP Professional	19,894
6461	Windows XP Service Pack 2	2,187
6788	Windows XP Service Pack 2	2,187

[표 5]에 따르면, 총 61개의 Windows XP에 대한 제품 정보 메타데이터가 존재하며, 이중 37개는 해당 제품코드를 갖는 해쉬 데이터가 전혀 존재하지 않는다. 즉, Windows XP 제품 중 약 61%가 관련된 파일 레코드가 존재하지 않음을 알 수 있다. 이에 따라, Windows XP 운영체제 데이터를 수사 대상에서 배제하기 위해서는 어떤 제품코드를 갖는 파일 레코드를 선택할 것인가를 선택하는 문제점에 봉착하게 된다.

3.3. 언어 코드가 Korean인 데이터 분석

제품에 대한 메타데이터 정보를 저장하는 NSRLProd.txt 파일에는 언어에 대한 정보가 있다. 즉, "English",

"Korean" 등으로 언어를 명시하고 있다. 우리나라의 수사 환경에서 활용가능성을 살펴보기 위하여, 언어 값에 "Korean"이 포함된 제품코드에 대한 파일레코드를 살펴보면 [표 6]과 같다.

〔표 6〕 언어가 Korean을 포함하는 경우

코드 값	제품 명	개수
1742	.NET Framework Service Pack 1	0
1836	Office 97	5,785
2464	.NET Framework	0
2551	Visual J#	62
2563	Platforms	136,810
2564	Internet Explorer	0
2565	Windows 98	0
2566	Windows Me	0
2567	Windows 2000	0
2568	Windows XP	0
2615	.NET Framework	0
2619	Applications, Platforms	138,444
2620	Internet Explorer	0
2621	Windows 98	0
2622	Windows Me	0
2623	Windows 2000	0
2624	Windows XP	0
2625	Visio 2002 Professional	0
2633	Applications, Platforms	139,370
2634	Internet Explorer	0
2635	Windows 98	0
2636	Windows Me	0
2637	Windows 2000	0
2638	Windows XP	0
2639	Visio 2002 Professional	0
2670	Developer Tools, Servers	48,511
2671	Visual Studio Enterprise Edition	0
2674	SQL Server	0
2711	Platforms, SDK/DDK	18,180
2712	Windows 2000	0
2713	.NET Framework SDK	0
2737	Developer Tools - Special Release	24,543
2738	Visual Studio .NET Enterprise Architect	0
2739	Visual Studio .NET	0
2740	Visual SourceSafe	0
2808	Windows XP	65,790
2809	Windows 2000	0
2810	Systems Management Server	0
2811	Publisher	0
2812	Windows XP Tablet PC Edition	0
2813	Office XP Professional with FrontPage	0
2817	Office XP Professional with FrontPage	0
2818	Systems Management Server	0
2838	Applications, SDK/DDK	50,409
2839	Project	0
2840	Publisher	0
2842	.NET Framework SDK	0
2843	Applications, SDK/DDK	24,864
2844	Project	0
2845	Publisher	0
2847	.NET Framework SDK	0
2903	Visual Studio Enterprise Edition	48,511
2906	SQL Server 2000	0
2964	Internet Explorer	141,352
2965	Windows 98 Versions	0
2966	Windows Me	0
2967	Windows 2000 Versions	0
2968	Windows XP Versions	0
2971	Visio 2002 Professional	0
3023	.NET Framework SDK	21,279
3024	Project Professional 2002	0
3025	Project Server 2002	0
3026	Publisher 2002	0
3027	Systems Management Server 2.0	0
3029	Office XP	0
3111	DVDit!	43
3188	MSDN Disc 2052	1,154
3264	MSDN Disc 3264	166,808
3290	Office XP	39,288
3291	Windows 2000	23,197
3292	Windows XP	23,483
3293	Windows XP	20,093
3294	BookShelf	20
3295	Visio	35
3330	Windows	10,493
3370	MSDN Disc 2321	0

3371	MSDN Library for Visual Studio .NET	0
3372	Visio Enterprise Architect	0
3492	MSDN MS Office XP Developer, Office XP Pro w FrontPage, SMS 2.0 w SP2, Project Pro 2002, Project Server 2002, Publisher 2002	22,239
3515	.NET Framework	12
3540	MSDN Disc 2470.1	9,260
4799	Solaris 7 Desktop	23,423
4945	MSDN Disc 2361	45,887
4958	MSDN Disc 2364	25,123
4968	MSDN Disc 2464.1	86,830
5417	MSDN Disc 2464	86,270
5924	MSDN Disc2365	141,352
5932	MSDN Disc2225	22,454
6524	MSDN Disc 2464.2	35,059
7351	MSDN Disc 2464.4	0
7380	MSDN Disc 2470.2	0
7382	MSDN Disc 2464.3	0
7397	MSDN Disc 2470.4	0
7418	MSDN Disc 2470.3	0
7933	Oracle8	6,265
8023	MSDN disc 2470	9,744
8055	MSDN Disc 2466.4	44,558
8059	MSDN Disc 3498	39,689
8081	MSDN Disc 2464.5	63,133
총 99개	파일 합계	1,809,822

[표 6]에 나타난 것처럼, RDS 2.17에는 총 1,809,822개의 파일에 대한 해쉬 값이 구축되어 있다. 또한, 총 99개의 한글 제품에 대한 제품 정보가 존재하며, 이중 59개는 관련된 해쉬 값 데이터가 존재하지 않는다. 즉, 약 60%의 제품 메타데이터 정보는 실제 연결된 파일 레코드가 전혀 존재하지 않음을 알 수 있다.

Ⅳ. 결 론

이 논문에서는 소프트웨어 참조 데이터세트 구축 동향에 대하여 살펴보았다. 그리고, NSRL RDS에 대한 세부 분석 결과, 데이터가 메타데이터와 해쉬 파일 데이터간 상당한 오류가 존재함을 알 수 있다. 전체 파일 레코드 중 7%가 관련된 메타데이터 정보가 존재하지 않았다. 또한, 메타데이터 중 약 60%의 메타데이터는 실제 관련된 파일 레코드가 한건도 존재하지 않음을 알 수 있었다. 이는 NSRL RDS를 실제 수사에 활용하기 매우 힘든 상황임을 나타낸다고 할 수 있다. 특히, RDS 데이터 활용을 위하여 어떤 제품 코드 값을 선택해야 정확한 것인가를 파악하기 매우 어렵다. 따라서, 활용성을 높이기 위해서는 NSRL RDS의 공개되는 데이터에 대한 지속적인 점검과 함께 별도의 데이터세트 구축이 필요할 것으로 사료된다.

참고문헌

[1] NIST의 NSRL RDS, http://www.nsrl.nist.gov/
[2] NDIC의 HashKeeper, http://groups.yahoo.com/group/hashkeeper
[3] SUN의 Fingerprint DB, http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl
[4] Rootkit Hunter, http://www.rootkit.nl
[5] CyberAbuse RootkitID, http://rk.cyberabuse.org
[6] HashDig, http://ftimes.sourceforge.net/FTimes/HashDig.shtml
[7] 표월성, 이상진, "컴퓨터 포렌식을 위한 한국형 RDS 구축," p. 545-p.550, 한국정보보호학회 하계 정보학술대회 논문집 Vol. 16, No. 1

〈著者紹介〉

김 기 범 (Kibom Kim)
정회원
1994년 2월 : 제주대학교 정보공학과 공학학사
1996년 8월 : 고려대학교 전산과학과 이학석사
2001년 2월 : 고려대학교 전산과학과 이학박사
2001년 1월 ~ 2004년 7월 : (주) 이씨오 개발부장
2004년 8월 ~ 현재 : ETRI 부설연구소 선임연구원
관심분야 : 정보보호, 디지털 포렌식, 분산시스템

박 상 서 (Sangseo Park)
정회원
1991년 2월 : 중앙대학교 전자계산학과 공학학사
1993년 2월 : 중앙대학교 전자계산학과 공학석사
1996년 8월 : 중앙대학교 컴퓨터공학과 공학박사
1996년 1월 ~ 1998년 12월 : 국방정보체계연구소 선임연구원
1999년 1월 ~ 2000년 1월 : 국방과학연구소 선임연구원
2000년 2월 ~ 현재 : ETRI 부설연구소 선임연구원
관심분야 : 정보보호, 디지털 포렌식