한국컴퓨터정보학회 하계학술대회 논문집 제26권 제2호 (2018. 7)

디렉토리 인덱스에 데이터 숨기기 방법을 적용하기 위한 필요한 요소들

조규상O
O동양대학교 테크노공공인재학부
e-mail: e-mail:cho@dyu.ac.krO

Analysis of Required Elements of a Directory Index Data Hiding Method

Gyu-Sang ChoO
ODept. of Human Resource of Technology, Dongyang University

● 요 약 ●

본 논문에서는 NTFS 파일시스템에서 디렉토리 인덱스의 구조내에 데이터를 숨기기 방법을 적용하는데 있어서 필요한 요소들에 대한 설명과 그것의 필요성에 대하여 논하기로 한다. 기존에 발표된 이 방법은 NTFS의 디렉토리 인덱스를 유지하기 위하여 B-tree방식으로 인덱스에 대한 데이터 구조를 운영하고 있는 점을 이용하여 인덱스의 정보를 담고 있는 인덱스 레코드 안에 저장되는 파일명을 이용하여 데이터 감추기를 수행하는 방법이다. 이것을 하기 위하여 필요한 몇가지 요소가 있는데 그 중에서 파일시스템, 작업 디렉토리, 위장 파일, 숨기려는 데이터, 사용할 수 없는 문자들, 앵커파일, 분석도구 등에 대한 것들을 나열하고 해당하는 요소들이 필요성과 그에 대한 의미를 기술하고자 한다.

키워드: 디렉토리 인덱스(directory index), NTFS파일시스템(NTFS file system), 데이터감추기(data hiding)

I. Introduction

NTFS는 Windows NT 3.1에서 부터 Windows의 기본 파일시스템으로 채택된 이후로 현재에 이르고 있는 동안에 안정적으로 사용되고 있다. Windows의 역사와 함께 개발 초기부터 적용된 기술과 기본사양을 바탕으로 Windows 10에 이르기까지 기본 형태를 그대로 유지하면서 큰 변화없이 안정적으로 잘 사용되고 있다[4].

Windows NTFS에 대한 구조와 원리에 대한 내용들은 여러 문헌들[5,6]에 잘 기술되어 있지만 디렉토리 인덱스에 관련된 내용들에 중에서 B-트리의 동작이나 구현 방법들은 소개가 잘되어 있지 않다. 최근 디렉토리 인덱스에 관한 연구는 Cho의 연구[1,2,3,4]에서 찾아볼 수 있다. 디렉토리 인덱스에 관한 디지털 포렌식 분석에 필요한 요소에 대한 설명과 함께 B-트리 인덱스 구조와 동작 방식을 잘 설명하고 있다[4]. 또 다른 연구[2]에서 디렉토리 목록 변화에 따른 인덱스 레코드의 흔적에 남게되는 파일명을 이용하여 데이터를 숨기는 방법을 제안하였다. 그 연구 결과를 응용한 후속 연구[3]에서 파일명으로 사용이 불가능하여 숨기려는 데이터에 사용할 수 없는 문제들이 있는 것을 극복하기 위한 방법으로 유니코드 변환 방법을 제안하였다.

이 연구에서는 기존에 발표된 NTFS의 B-tree방식을 사용하여 디렉토리 인덱스 안에 저장되는 파일명을 이용하여 데이터 감추기를 수행하는 방법[1]에서 필요한 요소들, 즉 파일시스템, 작업 디렉토리, 위장 파일, 숨기려는 데이터, 사용할 수 없는 문자들, 앵커파일, 분석도구 등에 대한 것들을 나열하고 해당하는 요소들이 필요성과 그에 대한 의미를 기술하고자 한다.

II. Essential Elements of a Directory Index Data Hiding Method

디렉토리 인덱스에 데이터를 숨기는 방법이 적용되기 위해서 필수적으로 사용되어야 하는 요소들이 있다. 아래에 필요한 요소들과 그에 대한 간단한 설명을 작성한다.

1. OS버전 : Windows XP/7/8/10
2. 파일시스템 버전 : NTFS v3.1
3. 최소 스토리지 소요공간
   1) MFT entry: 1KB
   2) 인덱스 엔트리 디스크 할당: 4KB
4. 작업 디렉토리(Working Directory) : 드라이브 상관없이 디스크내의 임의의 디렉토리에 적용가능하다.
5. 위장파일의 위치(Camoflage Direcotory) : 작업디렉토리와 마찬가지로 디스크내의 임의의 위치의 디렉토리에 적용 가능하다.

단, 작업디렉토리와 같은 디렉토리가 아니어야 한다. 예를 들면 “d:\otherDir”와 같이 적용될 수 있다[1].

6. 숨기려는 파일들: 파일명에 작성한 내용이 디렉토리 인덱스 레코드에 기록한다. 파일명에는 유니코드가 사용된다. 파일명의 길이는 1~255자까지 허용이 된다. 실제로는 디렉토리 경로를 포함한 파일명의 길이가 255자 이내이어야 한다. 경로명이 긴 경우는 숨기려는 데이터의 길이에서 경로 길이의 문자수 만큼 파일명 길이에서 제외되어야 한다[2,3].

7. 파일명에 사용할 수 없는 문자들: 파일명에는 다음과 같은 문자를 사용할 수 없다. “, *, /, :, <, >, ?, \, | 등의 문자는 사용할 수 없다[2,3].

8. 앵커파일(Anchor File): 디렉토리 인덱스가 유지되기 위해서는 최소 한 개의 파일이 디렉토리 안에 남아있어야 한다. 이것이 존재하지 않으면 할당되었던 인덱스 레코드가 해제되기 때문에 반드시 필요한 요소이다[1,2,3].

9. 디스크 분석도구: 숨겨진 데이터가 적절한 위치에 숨겨져 있는지를 확인하기 위하여 사용되는 툴로써 X-Ways WinHex/Forensics가 쓰이고, EnCase등의 포렌식 도구들을 사용하여 확인할 수 있다.

III. Conclusions

이 연구는 NTFS 파일 시스템의 디렉토리 인덱스의 구조를 이용하여 데이터를 숨기기 방법[1]을 적용할 때 필요한 요소들에 대한 필요한 요소들(파일시스템, 작업 디렉토리, 위장 파일, 숨기려는 데이터, 사용할 수 없는 문자들, 앵커파일, 분석도구 등)에 대하여 나열하고 해당하는 요소들이 필요성과 그에 대한 의미를 기술하였다.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2016R1D1A1B03935646)

REFERENCES

[1] Gyu-Sang Cho, “A New NTFS Anti-Forensic Technique for NTFS Index Entry”“, Journal of Korea Information Electron Communication Technology, Vol.8 No.4, pp.327-337, 2015.

[2] Gyu-Sang Cho, “A Problem Solving Method for Non-Admittable Characters of a Windows File Name in a Directory Index Anti-Forensic Technique”, KSDIM(Korea Society of Digital Industry & Information Management), Vol. 11, No. 4, pp. 69-79, 2015.

[3] Gyu-Sang Cho, “An Anti-Forensic Technique for Hiding Data in NTFS Index Record with a Unicode Transformation”, Journal of Korea Convergence Security Association, Vol. 15. No. 7, pp 76-84 2015.

[4] Gyu-Sang Cho, “Ordinary B-tree vs NTFS B-tree: A Digital Forensics Perspectives”, Journal of The Korea Society of Computer and Information), Vol. 22 No. 8, pp. 73-83, August 2017.

[5] B. Carrier, File System Forensic Analysis, Addison-Wesley, 2005, pp. 273-396.

[6] Microsoft TechNet, “How NTFS Works”, https://technet.microsoft.com/en-us/library/cc781134(v=ws.10).aspx.

[7] Wikipedia, “NTFS”, http://en.wikipedia.org/wiki /NTFS.