디지털포렌식을 이용한 아키텍처별 Windows11의 비교

김종도[O], 홍승표[*], 이훈재[**]
[O]동서대학교 일반대학원 디지털포렌식학과,
[*]동서대학교 일반대학원 컴퓨터공학과,
[**]동서대학교 정보보안학과
e-mail: jongdorai@naver.com[O], alfkdlthd@gmail.com[*], hjlee@gdsu.dongseo.ac.kr[**]

Comparison of Windows11 by Architecture Using Digital Forensics

Jong-Do Kim[O], Seoung-Pyo Hong[*], HoonJae Lee[**]
[O]Dept. of Digital Forensic, Graduate School, Dongseo University,
[*]Dept. Computer Engineering, Graduate School, Dongseo University,
[**]Dept. of Information Security, Dongseo University

● 요 약 ●

최근 프로세서 제조공정의 급속한 발전으로 프로세서의 종류에 상관없이 같은 운영체제를 설치 할 수 있게 되었다. 하지만 근본적으로 프로세서의 종류에 따라 차이점이 있고, 동작방식이 다르기 때문에 포렌식 할 경우 같은 운영체제라도 다른 결과가 나올 수 있다. 본 논문은 디지털포렌식을 이용하여 CISC 프로세서의 Windows 운영체제와 RISC 프로세서의 Windows운영체제를 비교하고, 프로세서 방식에 따른 차이점을 통해 후속 연구 방향을 제시한다.

키워드: 디지털포렌식(Digital Forensic), 프로세서(Processor), 윈도우11(Windows11)

I. Introduction

최근 프로세서 제조공정의 급속한 발전으로 인해 프로세서의 사용 방식이 변화하고 있다. 2017년 MicroSoft社에서 기존의 CISC 프로세서를 이용한 Windows 운영체제가 아닌 RISC 프로세서를 이용한 Windows 운영체제를 발표하였고, 2020년 Apple社에서 앞으로의 모든 Mac제품은 CISC 프로세서가 아닌 자체개발한 RISC 프로세서를 사용할 것이며, 자사의 모바일 디바이스에도 탑재할 예정이라고 발표를 함으로써 대중의 관심을 크게 이끌었다[1].

기존의 macOS에서는 BootCamp 기능을 이용하여 Windows OS를 설치할 수 있다. BootCamp기능은 파티션을 나누어 파티션마다 고유의 OS를 설치할 수 있게 해주는 기능이다. Apple社에서 RISC 프로세서를 사용함으로써 BootCamp 기능의 지원을 중단하였다[2]. 이로 인해 macOS 환경에서 가상 머신을 이용하여 Windows OS를 설치하는 사람이 증가하고 있으며, 설치하는 Windows OS의 경우 기존의 CISC 프로세서 방식이 아닌 RISC 프로세서의 방식으로 설치를 하게 됨으로써, 같은 소프트웨어라도 근본적으로 다르다. 이와 같은 이유로 포렌식을 할 경우 기존의 CISC 프로세서 Windows와 RISC 프로세서 Windows를 분석하였을 때 결과가 상이할 수 있다.

따라서, 본 논문에서는 CISC 프로세서 방식의 Windows와 RISC 방식의 Windows의 차이점에 관하여 연구한다.

II. Preliminaries

1. 아키텍처의 종류

1.1 CISC 방식의 아키텍처

CISC방식의 아키텍처는 Table. 1과 같이 복잡하고 많은 종류의 명령어를 사용하며 가변 길이 명령어 형식을 사용한다. 마이크로 프로그래밍 제어방식을 사용하기 때문에 호환성이 좋고, 명령어를 해석한 후에 명령어를 실행한 다는 특징이 있다. CISC 방식의 아키텍처는 복합 명령어를 가지고 있기 때문에 호환성이 뛰어나지만 전력소모가 크고 속도가 느리며 가격이 비싸다는 단점이 있다.

주로 데스크톱 환경에서 많이 사용되며 Intel社의 프로세서와 AMD社의 프로세서의 방식으로 x64 등이 있다.

Table 1. Architectural Features of the CISC Method

Item	CISC
Number of instructions	Many
Register	Less
Processing Speed	Slowly
Internal Structure	Complex
Power Consumption	Many

1.2 RISC 방식의 아키텍처

RISC 방식의 아키텍처는 Table. 2와 같이 간단하고 적은 종류의 명령어를 사용하며 고정 길이 명령어 형식이다. 하드와이어드 제어방식을 사용하기 때문에 호환성이 낮지만, 명령어의 길이가 고정이 되어있기 때문에 명령어 해석 속도가 빠르다는 특징이 있다.

RISC방식의 아키텍처는 프로세서의 명령어를 최소화 시켜 매우 효율적이고 전력소모가 적으며 가격이 저렴하다. 하드웨어가 간단하지만 소프트웨어가 복잡하며 호환성 위해 에뮬레이션 방식을 사용하지만 여전히 호환성이 부족하다는 단점이 있다.

주로 모바일 기기에서 많이 사용되며 Apple社의 프로세서와 퀄컴社의 프로세서의 방식으로 ARM 이라고 불린다.

Table 2. Architectural Features of the RISC Method

Item	RISC
Number of instructions	Less
Register	Many
Processing Speed	Fast
Internal Structure	Simple
Power Consumption	Less

2. Windows11 구축 및 분석방법

2.1 Windows11 환경구축

RISC 방식의 Windows 11과 CISC 방식의 Windows11을 똑같이 구축하기 위해 가상 머신을 이용하여 설치를 진행하였다. 하지만 RISC 방식의 Apple社의 Macbook Air M1은 VMware WorkStation 및 VM Fusion을 지원하지 않으므로 Paralles Desktop을 이용한다[3]. CISC 방식의 데스크톱에서는 VMware WorkStation을 이용하여 설치하였다. 분석대상의 OS들은 Table. 3과 같이 구성하였다.

CISC 방식의 Windows 11과 RISC 방식의 Windows 11은 단일 파티션으로 구성하였다.

Table 3. Windows 11 Implementation Environment by Architecture Method

Item	CISC Method	RISC Method
Local Machine	Desktop	Macbook Air M1
Virtual Machine Program	VMware WorkStation Pro ver.16.2.3 build-19376536	Parallels Desktop ver. 17.1.2
Windows11 Version	Windows11 21H2	Windows11 21H2
Windows11 Build	22000.652	22000.652
Windows11 Experience	1000.22000.652.0	1000.22000.652.0

2.2 분석방법

아키텍처별 구축한 Windows11을 분석하기 위해 가상 머신 내부에 FTK Imager를 설치하여 Physical 이미징 방식과 Logical 이미징을 진행하였다. 이미징 파일을 이용하여 차별점이 있는 폴더 및 파일을 찾고, 비교한다. 분석을 수행하는 PC의 환경과 도구는 Table. 4와 같다.

Table 4. Analysis Environment

Item	Analysis PC
Machine Form	Desktop
Local OS	Windows10 Pro 21H1
Imaging Tool	FTK Imager 4.5.0.3

III. The Proposed Scheme

3. Windows11 분석

3.1 Physical 이미징 Windows11

Physical 이미징을 했을 경우 CISC 방식의 Windows11과 RISC 방식의 Windows 11은 EFI 시스템 파티션, Microsoft 예약파티션, 파티션되지 않은 공간 GPT방식의 할당되지 않은 공간, 시스템을 관리하기 위한 NTFS 파티션이 공통적으로 존재하였고, CISC 방식의 Windows 11은 실제 데이터가 저장되는 파티션의 분석이 가능하였지만, RISC 방식의 Windows 11에는 실제 데이터가 저장되는 파티션의 분석이 불가능 하였다. Fig. 1은 CISC 방식의 Windows 11을 이미징 했을 때의 구조이며, Fig. 2는 RISC 방식의 Windows 11을 이미징 했을 때의 구조이다.

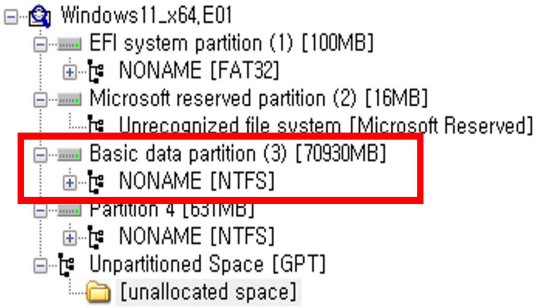

Fig. 1. Windows 11 Physical Imaging in CISC Method

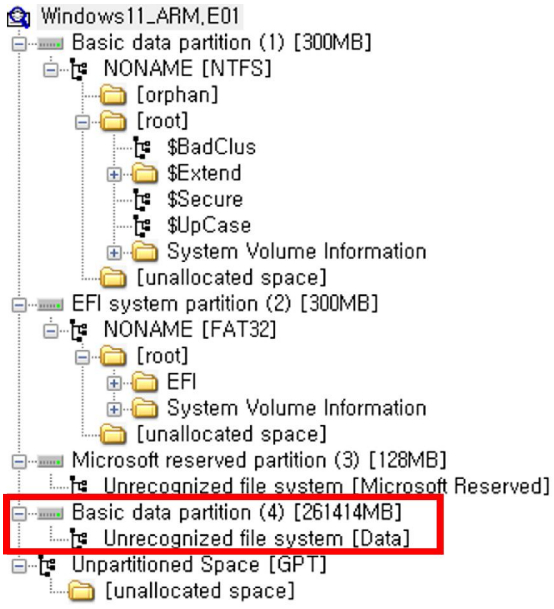

Fig. 2. Windows 11 Physical Imaging in RISC Method

3.2 Logical 이미징 Windows 11 분석

Physical 방식으로 이미징 했을 때 CISC 방식의 Windows 11은 분석할 수 있었으나 RISC 방식의 Windows 11은 파일시스템을 인식하지 못하였다. 따라서 Logical 방식으로 CISC 방식과 RISC 방식의 Windows를 이미징하여 분석을 진행하였으며 각각의 방식의 구조는 Fig. 3, Fig. 4와 같다.

RISC 방식의 Windows와 CISC 방식의 Windows의 차이가 나는 폴더는 $WINDOWS.~BT, $WinREAgent ,OneDrive Temp, Program Files(Arm), Windows.old가 있다. CISC 방식의 Windows11에만 존재하는 폴더로는 $WINDOWS.~BT, Windows.old, $WinREAgent, OneDrive Temp가 존재하는 대신 Program Files(Arm)이 없었다.

RISC 방식의 Windows11에는 $WINDOWS.~BT, Windows.old, $WinREAgent, OneDrive Temp 폴더가 없었지만, Program Files(Arm)이 존재하였다.

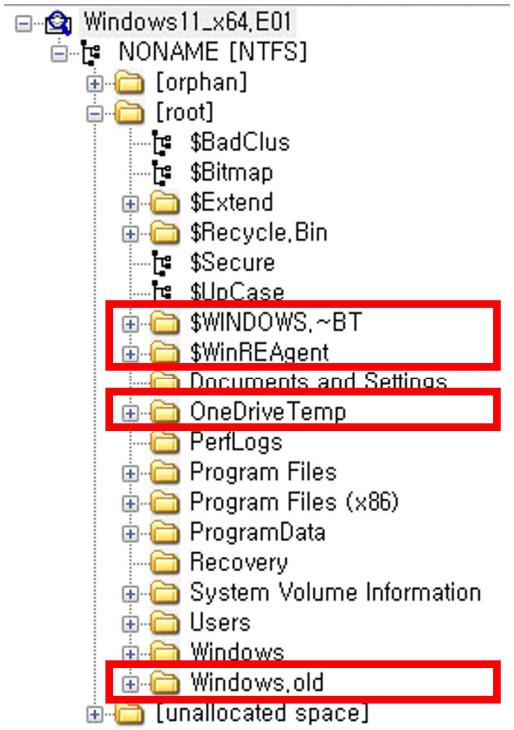

Fig. 3. Windows 11 Logical Imaging in CISC Method

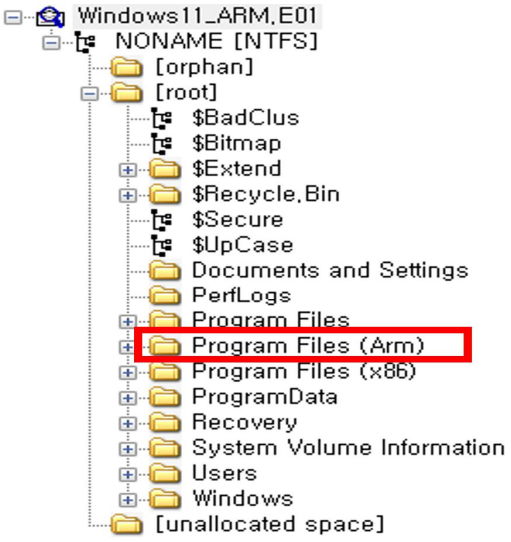

Fig. 4. Windows 11 Logical Imaging in RISC Method

IV. Conclusions

본 논문에서는 새로 발표된 Windows 11 운영체제에서 아키텍처의 동작 방식 차이로 발생하는 디스크 이미징 결과와 시스템 폴더의 차이를 알아보았다. FTK Imager의 Physical 디스크 이미징 기능을 이용했을 때 CISC 방식의 아키텍처에서 분석이 가능했던 것과 달리 RISC 방식의 아키텍처에서는 분석할 수 없었으며, Logical 디스크

이미징 기능을 사용했을 때는 두 방식 전부 분석이 가능한 것을 알 수 있었다.디지털포렌식의 관점에서 아키텍처의 동작 방식에 따라 아티팩트의 차이가 있을 수 있고 이에 따른 포렌식의 절차가 달라질 수 있다. 향후 연구계획은 Windows 11의 아티팩트를 포함하여 아키텍처별 Windows 11의 비교 분석을 진행하고, 차이점이 있을 시, 아키텍처별 Windows 포렌식 절차를 제안할 예정이다.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(grant number : NRF-2016R1D1A1B01011908).

REFERENCES

[1] Apple, “Apple announces mac transition to apple silicon” ,https://www.apple.com/kr/newsroom/2020/06/apple-announces-mac-transition-to-apple-silicon/,2020.

[2] Apple, ”What you need to install Windows 10 on your Mac,” https://support.apple.com/ko-kr/HT201468,2020.

[3] Ignatius Hall,, ”VMWare Fusion prepares to be compatible with Apple M1s”,https://www.soydemac.com/ko/vmware-fusion-se-prepara-para-ser-compatible-con-los-m1-de-apple/