

# 암호화폐 채굴 증거 수집을 위한 윈도우 아티팩트 분석 기술 연구

박 시 현\*, 한 성 훈\*, 박 원 형\*\*

## 요 약

최근 암호화폐 가격 급증과 동시에 암호화폐 채굴과 관련된 사회적인 이슈가 지속 발생하고 있다. 특히, 암호화폐는 암호 연산을 통해 취득할 수 있어서 컴퓨터만 있다면 누구나 쉽게 채굴을 시도할 수 있으며, Bitcoin, Ethereum 등 주요 암호화폐들의 자산가치가 증가함에 따라 대중들의 관심은 증가하고 있다. 또한, 높은 사양의 컴퓨터를 소유하고 있는 개인이 가정이나 회사 등 다양한 장소에서 암호화폐를 채굴하는 사례가 늘어나고 있다. 일부 채굴자들은 많은 전기에너지를 소모하는 컴퓨터의 발열 문제로 가정이 아닌 회사나 공공장소 등에서 채굴하여 개인의 도덕적 문제뿐만 아니라 기업에서도 여러 가지 문제들을 발생시키고 있다. 따라서, 본 연구는 암호화폐를 채굴한 컴퓨터들의 윈도우 아티팩트를 이용하여 채굴을 시도한 흔적들에 대해서 증거를 획득하는 기술에 관해 연구한다. 이를 통해 기업의 보안 강화를 위해 내부감사에 활용할 수 있도록 기대한다.

## Windows Artifacts Analysis for Collecting Cryptocurrency Mining Evidence

Si-Hyeon Park\*, Seong-Hun Han\*, Won-hyung Park\*\*

### ABSTRACT

Recently, social issues related to cryptocurrency mining are continuously occurring at the same time as cryptocurrency prices are rapidly increasing. In particular, since cryptocurrency can be acquired through cryptographic operation, anyone with a computer can easily try mining, and as the asset value of major cryptocurrencies such as Bitcoin and Ethereum increases, public interest is increasing. In addition, the number of cases where individuals who own high-spec computers mine cryptocurrencies in various places such as homes and businesses are increasing. Some miners are mining at companies or public places, not at home, due to the heat problem of computers that consume a lot of electrical energy, causing various problems in companies as well as personal moral problems. Therefore, this study studies the technology to obtain evidence for the traces of mining attempts using the Windows artifacts of the computers that mined cryptocurrency. Through this, it is expected that it can be used for internal audit to strengthen corporate security.

**Keywords : Digital Forensics, Windows Artifacts, Cryptocurrency, Mining, Internal Audit**

접수일(2022년 3월 29일), 수정일(2022년 3월 30일),  
게재확정일(2022년 3월 31일)

\* 상명대학교 정보보안공학과 학부생 (주저자, 공동저자)  
\*\* 상명대학교 정보보안공학과 교수 (교신저자)

## 1. 서 론

암호화폐의 등장 이후 급격한 가격상승에 따라 블록체인 네트워크의 거래내역이 담긴 블록을 생성하고 암호화폐로 보상을 얻는 채굴자들이 증가하기 시작했다. 채굴자들이 주로 채굴하는 암호화폐 종류는 크게 Bitcoin과 Ethereum이 있다. 암호화폐를 채굴하는 방법은 CPU 또는 GPU의 연산으로 블록체인 네트워크에 등록 대기 중인 거래기록을 전달받아, 거래기록 내부에 담긴 해시값이 올바른지에 대한 여부를 판단하고, 올바르다면 거래기록을 바탕으로 블록을 생성하여 네트워크에 등록한다. 그 이후 채굴된 암호화폐를 전달받는 형식이다. 이때 CPU와 GPU는 해시 연산을 진행하게 되는데, 해시 연산을 하는 데 소모되는 시간과 전력량이 상당하여, 여러 GPU를 사용하여 병렬처리를 하거나 채굴기를 사용하여 채굴하는 일이 빈번하게 발생하고 있다. 채굴에 사용되는 CPU와 GPU의 사용량이 늘어날수록 소비전력량도 증가하게 되는데, 소비전력량이 늘어날수록 전기요금도 함께 상승한다. 상승하는 전기요금을 회피하고자 가정용 전기보다 저렴하게 공급되는 농업 또는 산업용 전기로 채굴을 하는 불법 채굴자들이 등장하기 시작했다. 영국에서는 올해 5월 경찰이 대마 재배 농장으로 알고 기습단속에 나섰다가 주변 전력망에서 전기를 훔쳐 쓴 불법 채굴 현장을 적발하고 채굴에 사용된 컴퓨터를 압수한 사례가 있었다. 국내에서는 2017년 11월 중순부터 2018년도 3월 초까지 경기도 남양주시 개발제한구역에서 불법으로 암호화폐 채굴장을 운영하다 적발된 사례가 있다[1]. 이뿐 아니라 UNIST에서도 학생이 채굴 프로그램을 설치해 불법으로 채굴하여 적발[2]되는 등 산업, 농사용 전기를 사용하는 불법 채굴이 증가하는 상황이다. 따라서, 본 논문에서는 과도한 농업 또는 산업용 전기 사용이 발견되었을 때 윈도우 아티팩트를 이용하여 암호화폐 채굴을 하였다는 증거를 발견할 수 있는 방법을 제안한다. 본 논문의 순서는 제2장에서 암호화폐에 대한 이해를 위한 블록체인 등록과정, 마이닝 풀(Mining pool)에 대하여 설명한다. 3장에서는 암호화폐

채굴을 위한 실험 환경과 4장에서는 본 논문에서 제안하는 윈도우 아티팩트를 이용한 채굴 증거 획득기술을 제안한다. 마지막 5장에서는 결론을 내린다.

## 2. 관련 연구

### 2.1 암호화폐 관련 동향

최근에 Bitcoin의 가격이 아래 (그림 1)과 같이 8000만 원을 돌파하며 역대 최고가를 갱신하고 있다. 암호화폐의 가격이 높아지면서 전 세계적으로 사람들의 관심도가 높아졌고 하드웨어의 발전으로 매우 뛰어난 컴퓨터 사양이나 환경이 필요하지 않기에 암호화폐를 개인이 채굴하는 사람들이 증가하고 있다. 또한, 중국의 경우 시간당 150MW를 소모하여 불법으로 채굴하는 사례도 있었다고 한다[4]. 이렇게 불법으로 암호화폐를 채굴하는 데 소모되는 전력이 증가하는 것에 반해 이를 색출하는 방법이 발전되는 속도는 상당히 더딘 편이다. 일반적으로 불법 채굴로 의심되는 경우는 전기사용량 추이를 보고 평년, 평월 등의 사용량과 비교하여 상대적으로 급증하는 경우 불법 채굴로 의심할 수 있다. 하지만 의심을 피하고자 산업용 공장 등으로 쓰이던 건물을 인수하는 방법 등으로 회피를 하는 경우가 발생한다. 이러한 방법으로는 불법 채굴자를 색출하기에는 어려움이 있다. Felipe Ribas Coutinho 외에는 불법 채굴자 색출을 위해 Wireshark, Tcpdump를 활용한 물리적 탐지, “Bitcoin”, “Monero” 또는 “Crypto”같은 문자열을 가진 디렉터리 또는 파일을 찾는 방법과 인터넷 검색기록을 통한 색출 방법 등이 연구되고 있다[4][5].



(그림 1) Bitcoin Price trend. 21.11.12. 업비트 기준

## 2.2 암호화폐 채굴 원리

암호화폐를 채굴하는 방법은 다음과 같다. 블록체인 네트워크에 등록할 블록을 생성하려면 네트워크에서 검증되지 않은 거래내역을 수집한다. 수집한 거래 내역의 정상 여부를 판단하고, 정상이면 블록체인 네트워크에 수집한 블록을 등록한다. 정상 여부를 판단하는 기준은 수집한 블록에서 일회용 암호인 Nonce를 발견하느냐에 따라 달려있다. Nonce는 블록체인 네트워크 유지를 위해 단순한 연산으로 접근하기 어렵게 충분히 큰 수를 가진 해시값을 가진다.

## 2.3 해시 함수를 사용한 Nonce 생성

CPU 또는 GPU를 사용한 연산으로 Nonce를 발견하면 네트워크에 등록할 수 있게 되는데, 일반적으로 Nonce는 SHA256, Keccak256 같은 해시 함수를 사용하여 생성한다. 이러한 SHA256과 Keccak256은 입력된 문자열을 기반으로 고정길이의 문자열을 출력하게 된다. 이렇게 생성된 고정길이의 문자열은 서로 다른 문자열 2개를 입력으로 같은 해시 함수를 사용하여 연산을 진행했을 때 입력 문자열끼리 단 1bit라도 다르다면 값이 크게 바뀌게 된다.

## 2.4 마이닝 풀(Mining pool)

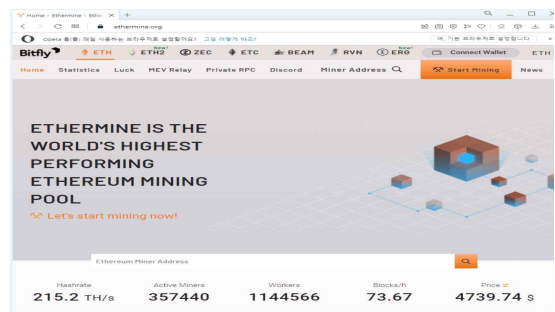
SHA256은 64바이트의 고정된 크기를 가지는 문자열을 생성하게 되는데, 64바이트에서 서로 다른 입력으로 같은 출력을 갖게 되는 해시 충돌이 발생하려면 약  $2^{130}$ 개의 입력으로 했을 경우

99.8% 확률로 발생한다고 한다. Nonce값을 찾는 연산을 단일 PC를 사용해서 진행하려면 상당한 시간이 소요된다. Nonce를 발견하기까지 소모되는 시간과 연산량을 줄이기 위해 다수의 사용자가 검증에 참여할 수 있게 구현한 시스템을 마이닝 풀(Mining pool)이라 한다.

## 3. 채굴 증거 획득을 위한 연구 환경

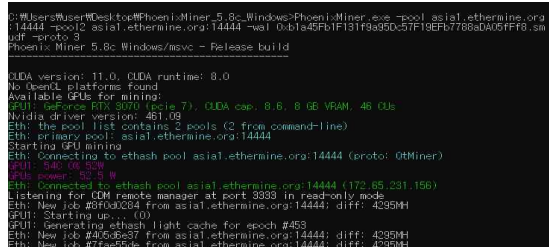
### 3.1 연구 환경

암호화폐를 채굴하기 위해서는 우선 (그림 2)와 같이 채굴 사이트에 접속하여 채굴 프로그램을 다운로드한다. 이후에는 마이닝 풀(Mining pool)에서 채굴이 끝나고 보상을 나눠 가질 받을 지급 주소를 설정하면 채굴을 할 수 있다.



(그림 2) Mining pool site

실험은 다음과 같은 환경에서 이루어졌다. 채굴 프로그램으로 PhoenixMiner, Desktop GPU는 RTX 3070을 사용하여 (그림 3)과 같이 채굴을 진행하였으며 채굴 종료 후 PC에서 다양한 Artifacts를 수집했다.

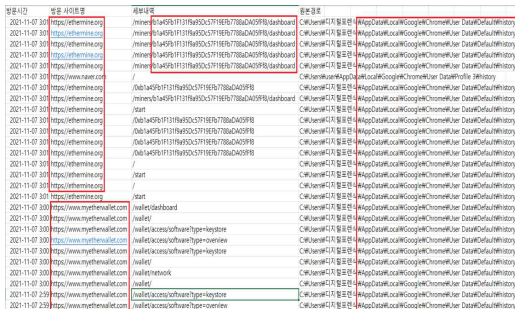


(그림.3) Phoenix Minor execution screen.

### 4. 채굴 증거 획득을 위한 윈도우 아티팩트

#### 4.1 웹 브라우저 기록을 통한 증거 탐색

채굴자가 채굴에 따른 보상받을 암호화폐 지갑 관리와 채굴량을 확인할 수 있는 사이트에 접속했다면 그 증거를 웹 브라우저 기록을 통해 찾아볼 수 있다. 웹 브라우저에 관련된 기록이 남는 경로는 Google Chrome 기준으로 C:\Users\W{사용자계정명}\AppData\Local\Google\Chrome\User Data\default\History이며 경로에서 사용자가 방문한 웹 사이트 및 검색기록을 확인할 수 있다. 위 경로를 따라 웹 브라우저 방문 기록을 확인한 결과 (그림 4)처럼 채굴 관련 사이트 접근 기록을 확인할 수 있다.



(그림 4) Web Browser, Visiting website record.



(그림 5) Web Browser, Portal search word record.

또한, 채굴 관련 사이트 중 ethermine.org/에서는 대시보드(Dashboard) 기능을 활용하여 채굴 진행사항을 볼 수 있다. 사이트 속 Dashboard 메뉴의 URL은 구조는 ethermine.org/miners/{지갑주소}/dashboard 형태로 되어있다. 위 URL 구조를 가진 곳을 방문한 기록이 있다면 채굴 진행도를 확인하기 위해 사이트를 방문하였다는 것을 유추할 수 있다. 그 외에도 아래 (그림 5)와 같이 검색기록에서 채굴과 관련된 "https://ethermine.org/", "https://miningpoolhub.com/"와 오버클럭(overclocking)을 위한 프로그램을 검색한 기록도 해당 채굴자가 어떤 Pool을 사용하였는지 알아볼 수 있다.

History 경로에는 파일 또는 프로그램을 다운로드 기록도 남아있는데, 이 역시 결정적 증거자료가 될 수 있다. 채굴 관련 프로그램 다운로드 기록과 암호화폐 지갑 생성 시 본인인증용 인증키를 파일 형식으로 다운로드 기록이 있다면 채굴 여부를 확인하는데 중요한 증거가 될 수 있다. 인증키 파일의 이름은 지갑 생성 시각을 UTC timezone으로 정해지기 때문에 다운로드 기록에서 아래 (그림 6)과 같이 UTC로 시작하는 파일을 찾아야 한다. 단, 채굴보상을 받을 암호화폐 지갑에 접근하려면 본인인증을 하는 방법이 필요한데 앞서 언급한 내용처럼 인증키 파일을 이용하여 인증하는 방식 이외에도 비밀번호를 입력하거나 Application을 이용하여 인증하는 등 여러 방법이 있다. 다른 방법을 이용하여 본인인증을 진행했다면 인증키 파일은 존재하지 않을 수 있다.



(그림 6) Web Browser, Download record.

앞서 언급한 경로 이외에 아래 (그림 7)과 같이 C:\Users\W{사용자계정명}\AppData\Local\Google\Chrome\User Data\Cache\data에서도 웹 캐시 기록들로 채굴과 관련된 사이트에 접근한 증거들을 볼 수 있다. 위 경로에서는 Mining pool 등 채굴과 관련된 키워드를 위주로 증거 수집해야 한다.



(그림 7) Web browser, cache record.

### 4.2 채굴 관련 프로그램 실행 기록 분석

사용자에 의해 실행된 응용프로그램과 해당 프로그램의 실행 횟수, 응용프로그램의 마지막 실행 시간 등의 정보를 포함하고 있는 “Prefetch”와 “UserAssist”를 통해 아래 (그림 8)과 같이 채굴 프로그램과 오버클럭(overclocking) 프로그램 실행 여부를 확인할 수 있다. 위 Artifacts에서는 프로그램 실행 횟수, 최종 실행 시간 등 기록을 확인할 수 있다. Artifact에서 발견된 프로그램 실행 기록 중 채굴 관련 프로그램 실행 기록을 획득한다면 해당 PC는 채굴에 사용되었다는 증거가 될 수 있다.

최종 실행 시간	프로그램명	실행 수	프로그램 경로	원본 경로
2023-11-07 20:25:33	chrome.exe	4	C:\Users\*~1\AppData\Local\Google\Chrome\Application\chrome.exe	C:\Users\*~1\AppData\Local\Google\Chrome\Application\chrome.exe
2023-11-07 20:25:33	chrome.exe	4	C:\Users\*~1\AppData\Local\Google\Chrome\Application\chrome.exe	C:\Users\*~1\AppData\Local\Google\Chrome\Application\chrome.exe
2023-11-07 20:25:33	chrome.exe	4	C:\Users\*~1\AppData\Local\Google\Chrome\Application\chrome.exe	C:\Users\*~1\AppData\Local\Google\Chrome\Application\chrome.exe
2023-11-07 20:25:33	chrome.exe	4	C:\Users\*~1\AppData\Local\Google\Chrome\Application\chrome.exe	C:\Users\*~1\AppData\Local\Google\Chrome\Application\chrome.exe
2023-11-07 20:25:33	chrome.exe	4	C:\Users\*~1\AppData\Local\Google\Chrome\Application\chrome.exe	C:\Users\*~1\AppData\Local\Google\Chrome\Application\chrome.exe

(그림 8) Prefetch, UserAssist Analysis.

### 4.3 Windows Event Logs를 이용한 분석

<표 1> Windows Artifacts related to cryptocurrency mining.

Windows Artifacts	증거	원본 경로	설명
Google Chrome Cache, Web History, Download File List	방문한 사이트, 다운로드 파일들, 웹 페이지 데이터	C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\	Google Chrome을 통하여 Miner 프로그램과 암호화폐 지갑 인증키를 다운로드 기록 및 채굴과 관련된 사이트들을 방문한 기록을 확인할 수 있다.
Prefetch, UserAssist	실행 프로그램, 실행 횟수, 실행 시간	C:\Windows\Prefetch\Microsoft\Windows\CurrentVersion\Explorer\UserAssist	채굴 관련 프로그램들을 마지막으로 실행한 시간과 실행 횟수 등을 알 수 있다. 시스템 On/Off 기록과 대조하여 채굴 프로그램을 실행 기록을 알 수 있다.
Windows Event Logs	Windows 로그인, 시스템 on/off, 응용프로그램 로그	C:\Windows\System32\winevt\Logs	시스템의 On/Off 시간과 응용프로그램의 실행 로그를 볼 수 있다. 해당 정보는 다른 Artifacts를 조합하여 추론이 가능하다.
JumpList	실행프로그램	C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\	최근 또는 자주 열람되는 파일리스트, 채굴, 오버클럭(overclocking) 프로그램과 지갑 인증키 프로그램의 사용 여부를 알 수 있다.

C:\Windows\System32\winevt\Logs\Security.evtx에서 보안 관련된 Event log와 Windows 로그인, 로그아웃 기록, 네트워크 등 다양한 Log 기록을 볼 수 있다. 또한, 전문적인 포렌식 도구를 활용하여 시스템의 On/Off 기록과 프로그램의 실행 시간을 대조하여 해당 컴퓨터가 채굴에 사용된 시간대와 활동 시간을 알 수 있다. 아래 (그림 9)은 보안감사 전문 도구인 더존 DFAS 프로그램을 활용하여 타임라인 분석 및 시스템 On/Off 정보를 확인 및 분석한 결과이다.



(그림 9) System On/Off information and timeline analysis.

### 4.4 JumpList를 이용한 실행 프로그램

JumpList는 응용프로그램을 통해 최근 열람했거나 자주 열람되는 파일들의 리스트이며 대상 파일들의 경로 등 정보를 확인할 수 있다. 사용자

행위 파악, 최근에 사용한 문서, 프로그램 정보 및 실행 여부 또한 알 수 있다. 채굴에 사용된 컴퓨터의 JumpList를 확인한다면 오버클럭(overclocking) 프로그램과 채굴과 관련된 start.bat 등의 프로그램들이 아래 (그림 10)과 같이 JumpList에 증거로 남을 것이다.

파일명	경로
start.bat	C:\Users\디지털포렌식\Desktop\PhoenixMiner_5.8c
PhoenixMiner_5.8c_Windows	C:\Users\디지털포렌식\Desktop\
start.txt	C:\Users\디지털포렌식\Desktop\PhoenixMiner_5.8c
UTC--2021-11-02T14:51:38.587Z--b1a45fb1f13	C:\Users\디지털포렌식\Desktop\비트코인 지갑\

(그림 10) Extracting programs related to mining through JumpList.

#### 4.5 윈도우 아티팩트 종합 결과

앞서 채굴 증거 획득을 위해 불법 채굴자가 설치한 다양한 증거들에 대해 4가지 윈도우 아티팩트를 종합해서 <표 1>과 같이 정리 할 수 있다. 이러한 4가지 아티팩트들만 가지고도 불법 채굴자를 색출 할 수 있는 내부 감사도구도 제작 할 수 있을 것으로 판단한다.

## 5. 결론

암호화폐에 대한 이슈는 국내뿐만 아니라 세계적으로도 큰 이슈이다. 현재와 같이 암호화폐의 자산이 증가함에 따라 단순 가상자산으로 바라보는 것이 아니라 베네수엘라와 같이 암호화폐를 국가 통화로써 인정하는 등 현실 세계에서도 사용할 수 있는 사례가 증가하고 있다. 이에 따라 향후, 암호화폐에 대한 자산은 더욱 증가하고 있으며 암호화폐를 채굴하는 채굴자 역시 증가할 것으로 예측된다. 또한, 내부 보안의 관점에서 비인가 장비 설치 및 노트북 반출입, 비인가 통신 등의 문제는 기관의 사이버 보안에서도 가장 중요한 문제가 된다. 이러한 문제는 불법 채굴행위를 할 때 사용되는 Miner 프로그램이 안티바이러스 백신에서 악성코드로 감지되어 내부 인터넷망에 문제가 될 가능성 있다. 본 연구를 통해 채굴자가 설치한 불법 채굴기를 발견하는 등 내부 보안을 강화하는데 활

용되길 기대한다. 향후, 새로운 암호화폐와 채굴 방법이 발전함에 따라 관련된 윈도우 아티팩트에 대한 추가 연구가 필요하다.

## 참고문헌

- [1] Kyung-Man Park, "Illegal Mining of Virtual Currency in Factories and Farm Buildings in Northern Gyeonggi-Do", 2018.04.19., [https://www.hani.co.kr/arti/area/area\\_general/841224.html#csidxa1fec1fd8f16f21bebae7123a61c850](https://www.hani.co.kr/arti/area/area_general/841224.html#csidxa1fec1fd8f16f21bebae7123a61c850).
- [2] Shin-Young Yoon, "A Student Caught Mining Cryptocurrency in a University Computer Lab", 2019.02.08, <https://www.dongascience.com/news.php?idx=26705>
- [3] Gul, Omer. "The Detection of Illicit Cryptocurrency Mining Farms in Electrical Distribution Systems with Innovative Approaches." (2021).
- [4] Ribas Coutinho, F., Pires, V., Miceli, C., Menasche, D. S. Crypto-Hotwire. ACM SIGMETRICS Performance Evaluation Review, 48(4), 4-7, (2021).
- [5] Hyo-Seok Jo. "Analysis and Performance of Virtual Currency Artificial Intelligence." Bachelor's degree in 2019.
- [6] Jeong-Hoon Jeon. "Study on the Carbon Dioxide Emission from Crypto currency Mining." Convergence security journal v.18 no.3. pp.45 - 51, 2018.
- [7] F. Ribas Coutinho, V. Pires, C. Miceli, and D. S. Menasche, "Crypto-Hotwire," ACM SIGMETRICS Performance Evaluation Review, vol. 48, no. 4. Association for Computing Machinery (ACM), pp. 4&#8211;7, 17-May-2021.
- [8] Recent Advances in Cryptovirology: State-of-the-Art Crypto Mining and Crypto Ransomware Attacks," KSII Transactions on Internet and Information Systems, vol. 13, no. 6. Korean Society for Internet Information

(KSII), 30-Jun-2019.

- [9] S. Ghimire, H.Selvaraj, "A Survey on Bitcoin Cryptocurrency and its Mining," A Survey on Bitcoin Cryptocurrency and its Mining Systems Engineering (ICSEng), 2018 26th International Conference on 2018 Dec, pp.1-6, Dec-2018
- [10] V. Vesely and M. &#381;adnik, "How to detect cryptocurrency miners? By traffic forensics!," Digital Investigation, vol. 31. Elsevier BV, p. 100884, Dec-2019.

---

[ 저 자 소 개 ]

---



박 시 현 (Si-Hyeon Park)  
2018년 3월 ~ 현재 : 상명대학교 정보  
보안공학과 학사  
email : number3341@naver.com



한 성 훈 (Seong-Hun Han)  
2018년 3월 ~ 현재 : 상명대학교 정보보  
안공학과 학사  
email : ab5682@nate.com



박 원 형 (Won-Hyung Park)  
2002년 서울과학기술대 산업정보시스템 학사  
2005년 서울과학기술대 정보산업공학과 석사  
2009년 경기대학교 정보보호학 박사  
2015년 성균관대학교 컴퓨터교육학 박사수료  
2020년 호주 다즈매니아대학교 컴퓨터사이언스  
박사수료  
2020년 극동대학교 사이버보안학과 학과장  
현재 상명대학교 정보보안공학과 부교수  
email : whpark@smu.ac.kr