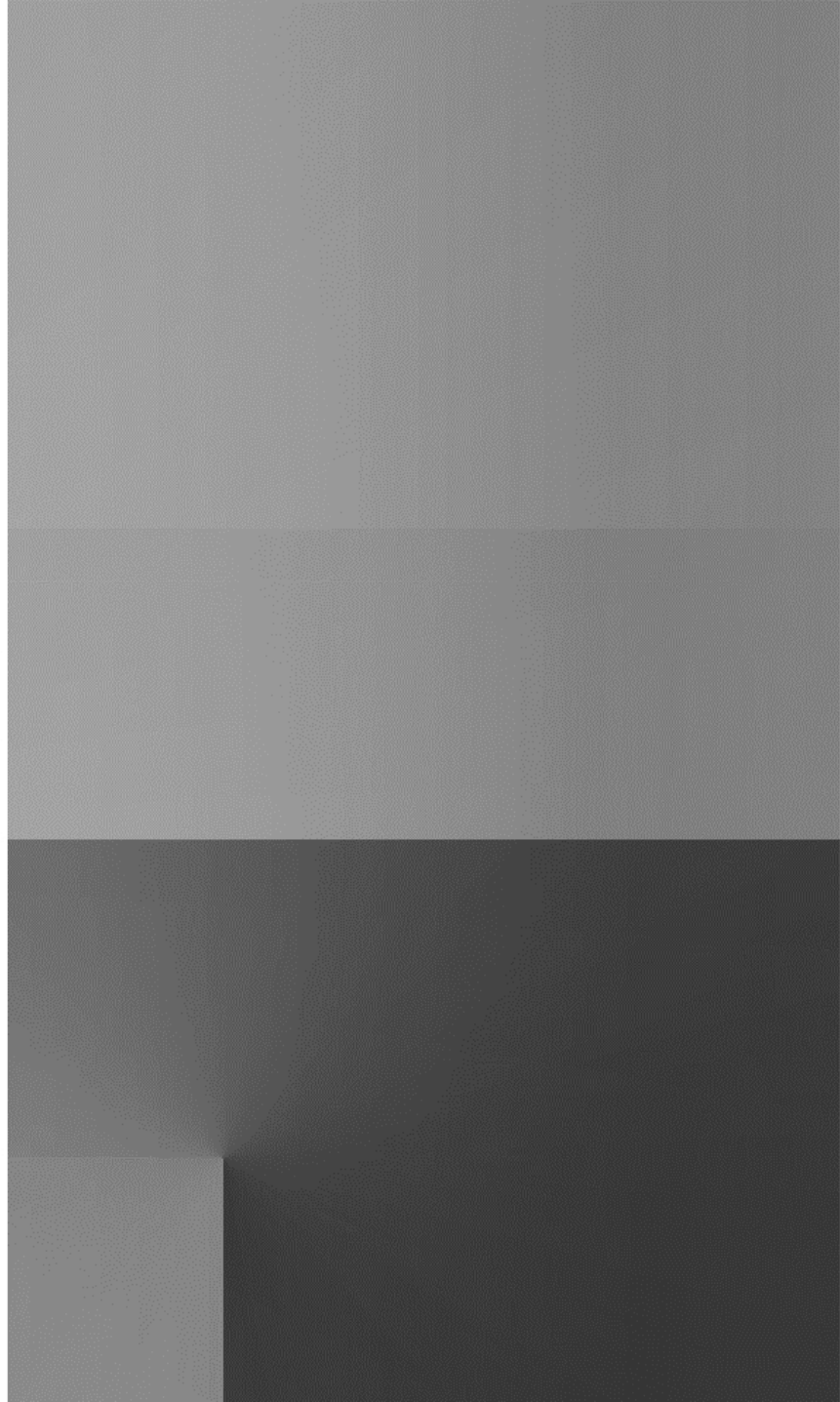
dongguk UNIVERSITY

정보보호 개론 “11주차 강의”

윤홍수

2025. 05. 15

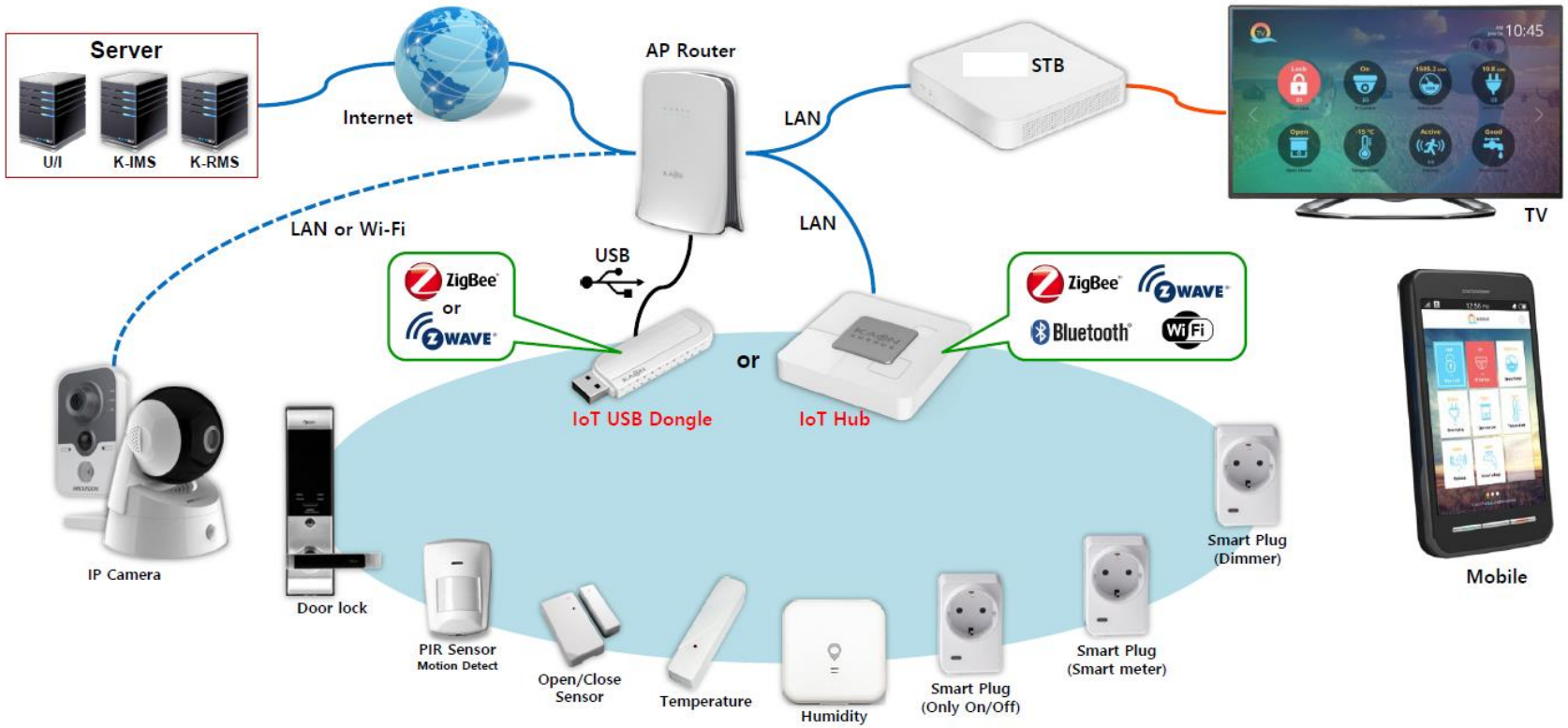
Table of Contents



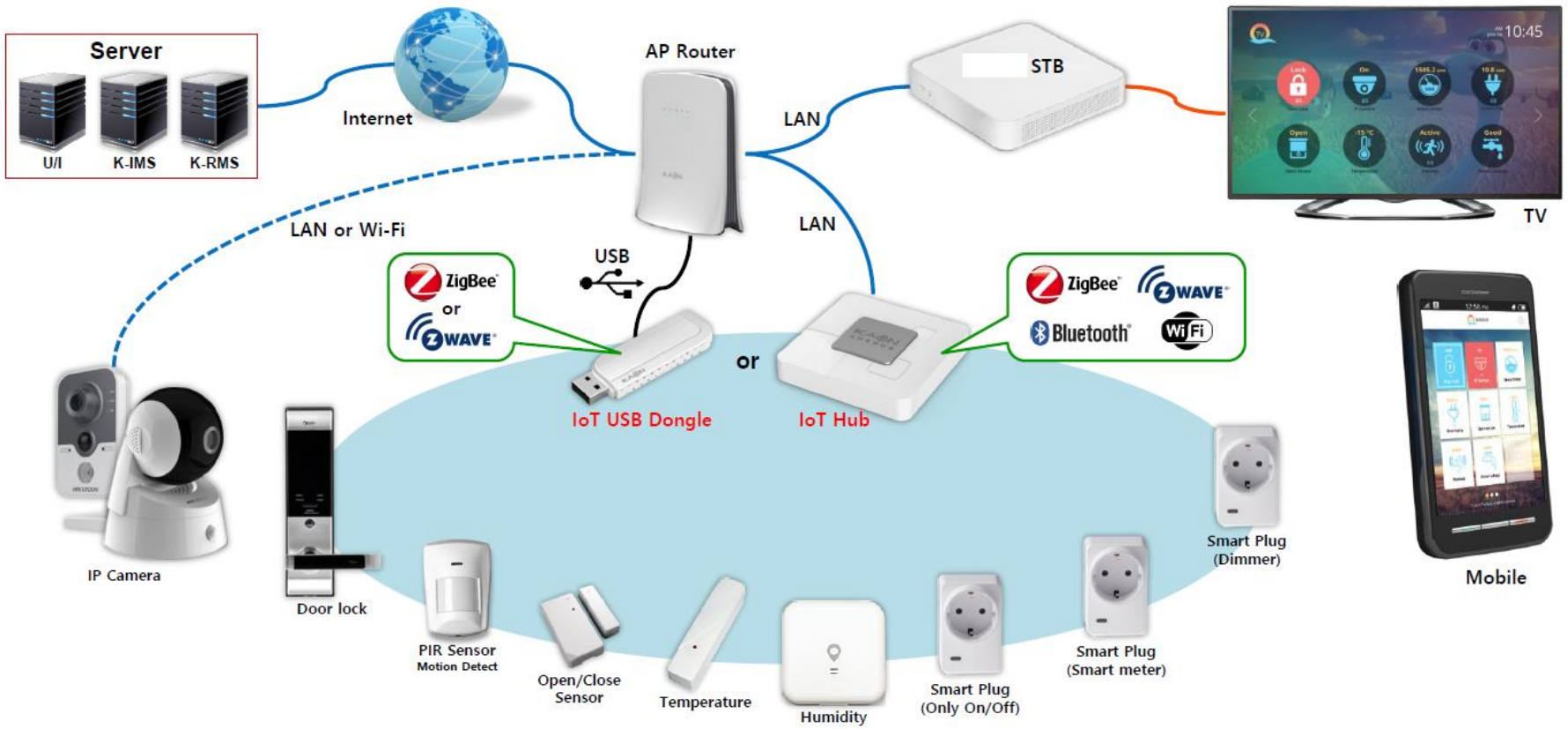
IoT 보안

✓ **IoT**

- Internet of Things의 줄임말, 우리말로 번역하면 사물 인터넷
- 모든 물건들이 인터넷에 연결되어 서로 정보를 주고받고 소통하는 기술



IoT 보안


Server
U/I
K-IMS
K-RMS
Internet
AP Router
STB
10:45
TV
LAN
LAN
LAN or Wi-Fi
USB
ZigBee
or
Z-WAVE
ZigBee
Z-WAVE
Bluetooth
Wi Fi
or
IoT USB Dongle
IoT Hub
Mobile
IP Camera
Door lock
PIR Sensor
Motion Detect
Open/Close
Sensor
Temperature
Humidity
Smart Plug
(Only On/Off)
Smart Plug
(Smart meter)
Smart Plug
(Dimmer)


Z-WAVE


zigbee


Wi Fi
TM


Bluetooth


NB-IoT


LoRa

IoT 보안

- 주로 가정용 자동화에 사용되는 무선 통신 프로토콜 (Silicon Labs의 라이선스)
- 저전력: 배터리로 작동하는 기기에 유리해서 오랫동안 사용할 수 있다
- 확장성 : Max 232개
- 스마트 조명 제어: 필립스 휴(Philips Hue) 일부 제품, 스마트 전구 등
- 스마트 도어락: Yale 스마트 잠금장치, August 스마트락 등
- 스마트 센서: 온도/습도 센서, 모션 센서, 누수 감지 센서 등 (SmartThings 등)

Z-Wave

국제 표준	800-900 MHz 무선 주파수
개발사	Zensys
도입일	1999년
산업	가정 자동화
물리적 범위	100미터
웹사이트	https://www.z-wave.com

IoT 보안

- 스마트홈에 사용되는 근거리 무선통신기술 프로토콜 (무료 프로토콜, 2.4G)
- 데이터 전송 속도가 Z-Wave보다 조금 더 빠름
- 다양한 제조사 지원: 많은 회사에서 Zigbee를 지원하는 제품을 만들고 있어서 호환성이 좋다
- 확장성 : Max 65,000개
- 스마트 조명: 필립스 휴(Philips Hue) 대부분 제품, IKEA Tradfri 등
- 스마트 플러그 및 스위치: Xiaomi Aqara, Sengled 등
- 스마트 센서: 모션 센서, 온도/습도 센서, 스마트 버튼 등 (SmartThings, Amazon Echo Plus 등)

직비

직비 모듈

국제 표준	IEEE 802.15.4
개발사	직비 얼라이언스[1]
산업	산업, 과학, 의학, IoT
물리적 범위	10 ~ 20미터
웹사이트	https://www.zigbee.org/

IoT 보안

- 매우 낮은 전력으로 아주 먼 거리까지 적은 양의 데이터를 전송하는데 특화된 통신 방식
- SK텔레콤 : 900 MHz 대역
- 저전력으로 장기리 통신을 가능하게 하며, 배터리 하나로 10년이상 사용 가능
- 16km 이상의 거리 커버 가능
- 스마트 미터링: 원격 수도/가스/전력 검침
- 환경 모니터링: 대기질 측정, 토양 센서 등
- 스마트 시티: 스마트 가로등, 주차 관리 등
- 자산 추적: 물류, 농업 등

IoT 보안

- 이동통신망(LTE)의 좁은 대역폭을 활용하여 저전력으로 넓은 범위까지 안정적인 통신
- 넓은 커버리지: 기존 LTE 기지국을 활용하여 넓은 지역에서 사용 가능
- 안정적인 통신: 면허 대역폭을 사용하므로 간섭에 강하고 안정적인 통신 품질을 제공
- 스마트 미터링: 원격 수도/가스/전력 검침
- 스마트 시티: 스마트 주차, 스마트 가로등
- 자산 추적: 물류, 보안
- 웨어러블 기기 (일부): 긴급 알림 등

IoT 보안

✓ IoT 사용 되는 곳

- 집: 스마트 전구, 스마트 스피커, 스마트 TV, 로봇 청소기, 스마트 냉장고, 월패드 등
- 학교: 스마트 교실 환경 제어 등
- 도시: 스마트 신호등, 스마트 주차 시스템, 스마트 가로, CCTV 등
- 병원: 웨어러블 건강 관리 기기, 원격 의료 시스템 등
- 공장: 스마트 팩토리, 자동화 설비 관리 등

IoT 보안

✓ IoT 역사

- ~ 1990 전 : 인터넷과 연결된 것은 아니지만, 기기들이 스스로 작동한다는 컨셉으로 이야기 됨 (아이디어)
- **1990년대 : Device to Device" 통신**
  - 기기(Device)와 기기(Device)가 직접적으로 서로 통신하는 방식
  - 중앙 집중형 장치(서버)를 거치지 않고, 가까이 있는 기기들이 직접 무선으로 연결
    - 인터넷과 연결되어 통신을 하려면, 서버가 있어야 하는데, D2D는 기기간 직접 연결

IoT 보안

✓ IoT 역사

- **기기(Device)와 기기(Device)가 직접적으로 서로 통신하는 방식**
- 통신 방식
  - 블루투스 (Bluetooth)
  - 와이파이 다이렉트 (Wi-Fi Direct) : 와이파이 공유기 없이 기기끼리 직접 연결
  - 지그비 (Zigbee), Z-Wave : 스마트 홈 기기들 간의 통신에 주로 사용되는 저전력, 저속 통신 기술
  - 근거리 무선 통신 (NFC, Near-Field Communication), NB-IOT, LoRA 등

IoT 보안

✓ IoT 역사

- **기기(Device)와 기기(Device)가 직접적으로 서로 통신하는 방식**
- 예
  - 스마트홈 : 움직임 감지 센서가 조명에 직접 신호를 보내 자동으로 켜지게 할 수 있다
  - 파일 공유: 와이파이 다이렉트를 이용하여 친구들과 사진이나 파일을 빠르게 공유
  - 긴급 통신: 재난 상황 발생 시, 통신망이 마비되었을 때 D2D 통신을 통해 주변 사람들과 긴급 메시지를 주고받을 수 있다

IoT 보안

✓ IoT 역사

- **기기(Device)와 기기(Device)가 직접적으로 서로 통신하는 방식**
- 보안
  - D2D 통신은 기기 간에 직접 데이터를 주고받기 때문에, 기존의 중앙 집중형 네트워크 보안 방식과는 다른 새로운 보안 위협에 노출될 수 있다
  - **도청 : 무선 채널을 사용하기 때문에, 통신 범위 내에 있는 악의적인 공격자가 무선 신호를 몰래 가로채 오가는 데이터를 엿들을 수 있다**
    - Software Defined Radio, SDR : 무선 통신 신호를 수신, 송신 분석 할 수 있다
      - RTL-SDR 동글, HackRF One, LimeSDR 등
    - Spectrum Analyzer : 넓은 주파수 범위의 무선 신호 강도를 시각적으로 표시해주는 전문 장비
      - Keysight, Rohde & Schwarz 등의 제품

IoT 보안

✓ IoT 역사

- **기기(Device)와 기기(Device)가 직접적으로 서로 통신하는 방식**
- 보안
  - D2D 통신은 기기 간에 직접 데이터를 주고받기 때문에, 기존의 중앙 집중형 네트워크 보안 방식과는 다른 새로운 보안 위협에 노출될 수 있다
  - **서비스 거부 공격 (Denial-of-Service, DoS):** 통신 채널에 불필요한 신호를 과도하게 보내 정상적인 기기 간의 통신을 방해하여 서비스 이용을 불가능하게 만들 수 있다
    - 과도한 신호 전송
    - 강력한 무선 신호를 지속적으로 특정 주파수 대역으로 방출
    - **공격자가 강력한 블루투스 신호를 주변에 계속해서 보내 다른 블루투스 기기들의 연결을 방해하거나, 와이파이 다이렉트 통신 주파수에 강한 노이즈를 발생**

IoT 보안

✓ IoT 역사

- **기기(Device)와 기기(Device)가 직접적으로 서로 통신하는 방식**
- 보안
  - D2D 통신은 기기 간에 직접 데이터를 주고받기 때문에, 기존의 중앙 집중형 네트워크 보안 방식과는 다른 새로운 보안 위협에 노출될 수 있다
  - **서비스 거부 공격 (Denial-of-Service, DoS) – WIFI / BT jammer**
    - **공격자가 강력한 블루투스 신호를 주변에 계속해서 보내 다른 블루투스 기기들의 연결을 방해하거나, 와이파이 다이렉트 통신 주파수에 강한 노이즈를 발생**

중국 신호 방해기, 오디오 방...
중국 사용자 정의 휴대용 ...

중국 신호 방해기, 오디오 방...
중국 사용자 정의 와이파이...

IoT 보안

✓ IoT 역사

- **기기(Device)와 기기(Device)가 직접적으로 서로 통신하는 방식**
- D2D 통신 보안 강화를 위한 대비책
  - 암호화 (Encryption): 내용을 숨기는 기술
  - 접근 제어 (Access Control): 허락된 대상만 접근하도록 제한
  - 보안 업데이트 및 패치 (Security Update & Patch): 취약점을 보완
  - 물리적 보안 강화 (Physical Security): 기기 자체를 안전하게 보호

IoT 보안

✓ IoT 역사

- **1999 ~ 2000년대 : "Internet of Things"라는 용어를 처음 사용**
- **2000년 초반 :**
  - 무선 통신 기술(Bluetooth, Wi-Fi 등)이 발전하면서, 실제로 사물을 인터넷에 연결하려는 시도들이 조금씩 나타나기 시작
  - 예 : 센서를 부착한 기기들이 데이터를 수집하고 네트워크를 통해 전송하는 초기 형태의 스마트 홈 시스템이나 산업 자동화 시스템들이 등장
  - 하지만 기술적인 제약과 높은 비용 때문에 널리 사용되지는 못함

IoT 보안

✓ IoT 역사

- **IoT의 폭발적인 성장과 대중화 (2010년대 이후)**
  - 2010년대: 스마트폰의 보급과 함께 무선 통신 기술, 센서 기술, 클라우드 컴퓨팅 기술이 눈부시게 발전하면서 IoT는 본격적으로 우리 생활 속으로 들어오기 시작함
  - 스마트 홈 기기: 스마트 전구, 스마트 스피커, 스마트 도어락 등 다양한 스마트 홈 기기들이 등장
  - 웨어러블 기기: 스마트 워치, 스마트 밴드와 같은 웨어러블 기기들이 건강 관리, 운동량 측정 등 다양한 기능을 제공하며 인기
  - 산업 IoT (IIoT): 제조업, 에너지, 농업 등 다양한 산업 분야에서 IoT 기술을 활용
  - 5G 통신: 빠른 속도와 낮은 지연 시간을 자랑하는 5G 통신 기술은 더욱 많은 기기를 안정적으로 연결

IoT 보안

https://www.youtube.com/watch?v=ZAIPemngLpE

정보통신망 침해 범죄(IoT 해킹)

IoT 보안

https://youtu.be/oF84ZOlRllY

정보통신망 침해 범죄(IoT 해킹)

IoT 보안

✓ 해킹 발생 주요 원인

- **취약한 초기 설정 및 관리 소홀**
  - 기본 비밀번호 사용 : 많은 사용자가 기기를 설치할 때 설정된 기본 비밀번호를 그대로 사용
  - 비밀번호 관리 부실 : 복잡하지 않은 쉬운 비밀번호를 사용하거나, 여러 계정에 동일한 비밀번호를 사용하는 경우, 한 번의 유출로 여러 기기가 위험에 노출될 수 있다 (**레인보우 테이블**)
  - 펌웨어 업데이트 소홀 : 제조사에서 제공하는 펌웨어 업데이트에는 보안 취약점을 해결하는 중요한 내용이 포함

IoT 보안

✓ 해킹 발생 주요 원인

- **레인보우 테이블**
  - 미리 계산된 가능한 수많은 비밀번호와 그 비밀번호를 특정한 방식으로 변환한 값(해시값)이 짝지어져서 저장
  - 해커 : 어떤 방법을 통해서 해시값을 획득 (해킹, 돈을 주고 사든)
  - 레인보우 테이블 검색 : 레인보우 테이블에서 획득한 해시값과 동일한 값 찾는다
  - 원래 비밀번호 추정
  - 제조사에서 미리 정해놓은 아주 흔하고 쉬운 비밀번호
  - 0000, 1234, admi과 같은 것들은 이미 레인보후 테이블에 모두 저장 되어 있음

IoT 보안

✓ **해킹 발생 주요 원인**

- **제조사의 보안 허술 및 취약점**
  - 소프트웨어/하드웨어 취약점 : 일부 저가형 또는 보안에 취약한 제조사의 제품에는 설계 단계부터 보안 취약점이 존재할 수 있다
    - HW 보안 : 인증 받은 부품 사용, 출처가 분명한 부품 사용, 물리적 잠금 장치 사용
    - SW 보안 : 중국 OEM, ODM 제품 사용하지 않기, 국내 통신 규격 인증 획득, 정식 SW 사용 라이선스 체크
  - 미흡한 보안 기능 : 암호화, 접근 제어 등 기본적인 보안 기능이 미흡하거나 제대로 구현되지 않은 제품도 있다
  - 사후 관리 부족 : 보안 취약점이 발견되었음에도 불구하고 제조사의 신속한 패치 제공 및 지원이 부족

IoT 보안

✓ **해킹 발생 주요 원인**

- **OEM, ODM**
  - OEM (Original Equipment Manufacturer)과 ODM (Original Design Manufacturer)
    - OEM : 대표 기업 => 애플(브랜드, 기획, 개발) / 생산 (외주)
    - ODM : 대표 기업=> 국내 네트워크 장비 업체들(브랜드, 기획) / 개발, 생산(외주)

IoT 보안

✓ **해킹 발생 주요 원인**

- **OEM, ODM**
  - OEM (Original Equipment Manufacturer)과 ODM (Original Design Manufacturer)
    - **저가 경쟁으로 인한 보안 투자 소홀**
    - **소프트웨어 업데이트 및 패치의 어려움**
    - **투명성 부족 및 검증 어려움** : 주문자가 ODM 방식으로 제품을 공급받는 경우, **제품 내부의 보안 구조나 개발 과정에 대한 투명성이 부족하여** 보안 취약점을 제대로 검증하기 어려울 수 있다
    - 공급망 보안 취약점 : IoT 기기는 다양한 부품과 소프트웨어 구성 요소로 이루어지는데, 이러한 요소들이 여러 하청업체를 거쳐 조립되는 경우가 많다. **각 공급업체의 보안 수준이 다르거나, 악의적인 부품이나 소프트웨어가 삽입될 가능성을 배제할 수 없다**

IoT 보안

✓ **해킹 발생 주요 원인**

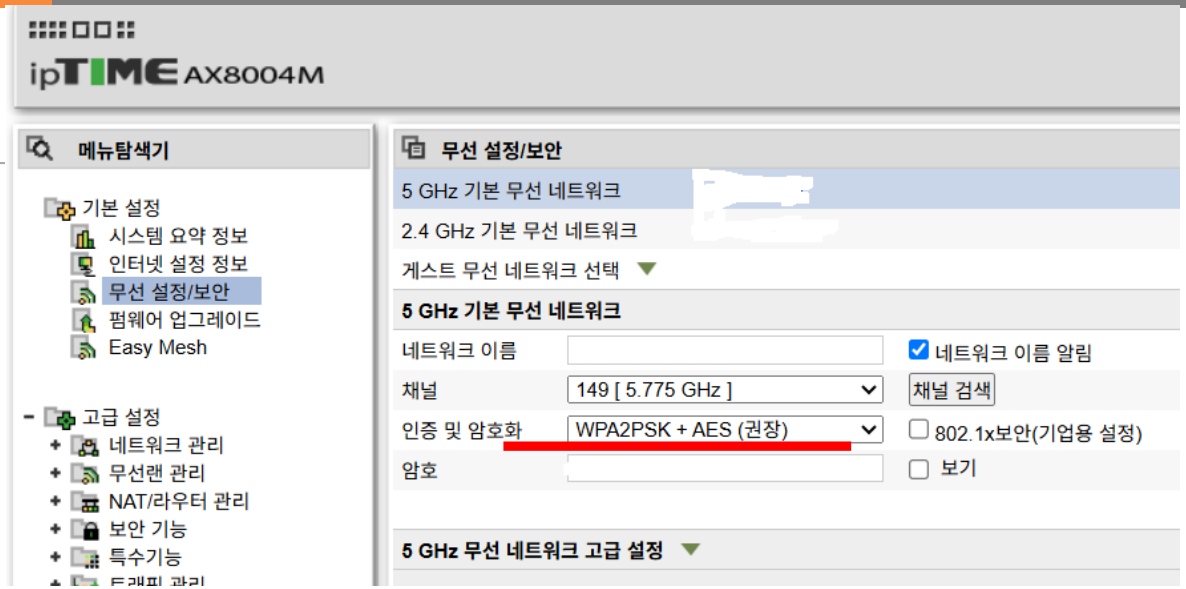
- **네트워크 보안 취약점**
  - 공유기 보안 설정 미흡
  - 개방된 포트
  - 취약한 와이파이 암호

IoT 보안

✓ **해킹 발생 주요 원인**

- **댁내 공유기 설정?**
  - 192.168.0.1 또는 192.168.1.1로 공유기 접속함.
  - 로그인 : admin/admin 또는 guest/guest 등으로 되어 있는 경우가 많디
  - 관리자 비번 변경
    - 설정 메뉴에서 "관리자 설정", "시스템 관리", "보안 설정" 등의 항목을 찾아 관리자 비밀번호를 새로운 비밀번호로 변경. 절대로 쉽게 추측할 수 없는 복잡한 비밀번호 (영문 대소문자, 숫자, 특수문자 조합)로 설정

IoT 보안



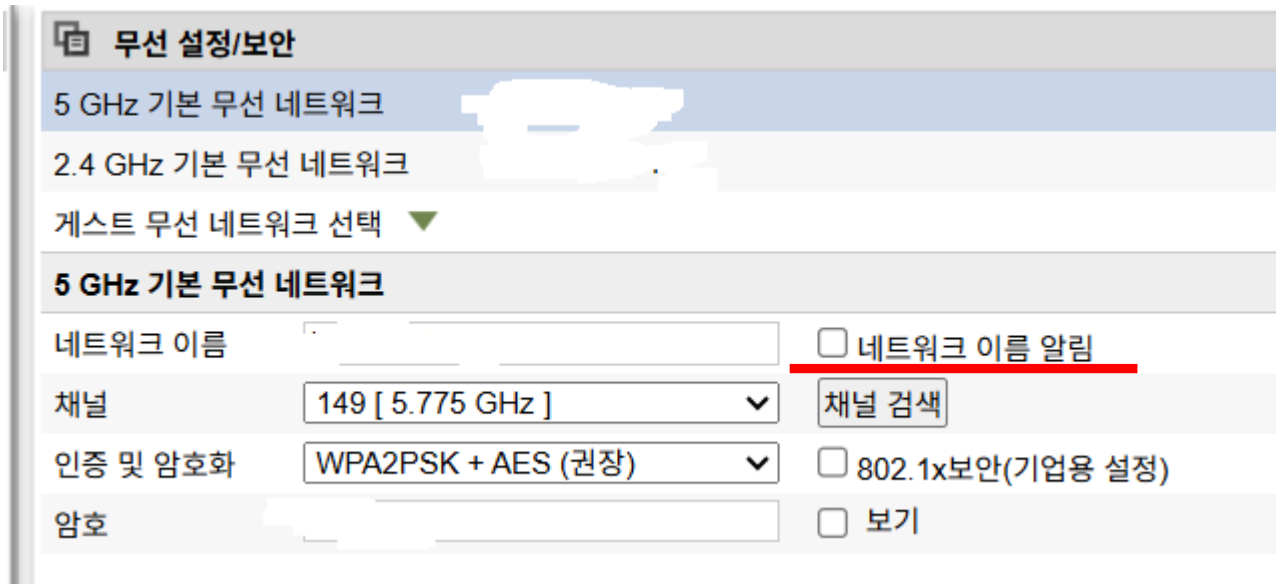
- ✓ **해킹 발생 주요 원인**
  - **댁내 공유기 설정?**
    - 와이파이 비밀번호 강력하게 설정
      - 비밀번호 등의 항목에서 현재 비밀번호를 확인하고, 새로운 강력한 비밀번호 (영문 대소문자, 숫자, 특수문자 조합, 최소 8자리 이상 권장)로 변경
      - 암호화 방식은 WPA2 또는 WPA3를 선택하는 것이 안전 (WEP 방식은 보안에 매우 취약하니 X)

WEP (Wired Equivalent Privacy) : 오래됨, 해커들이 쉽게 해킹함, 현재는 잘 사용하지 않음
WPA2 (Wi-Fi Protected Access 2) : 표준으로 사용될 만큼 안전성이 입증
WPA3 (Wi-Fi Protected Access 3) : 가능하다면 WPA3를 선택하는 것이 가장 안전한 방법

IoT 보안

✓ 해킹 발생 주요 원인

- **댁내 공유기 설정?**
  - SSID 숨기기
    - SSID를 숨기면 주변 와이파이 목록에 와이파이 이름이 보이지 않게 되어, 일반적인 방법으로는 연결 시도를 막을 수 있다

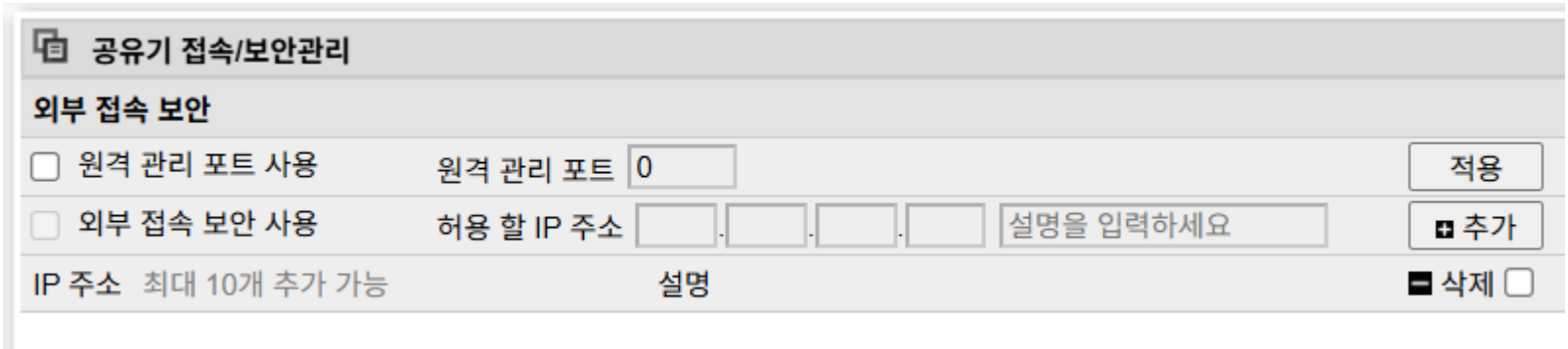


dongguk UNIVERSITY

IoT 보안

✓ **해킹 발생 주요 원인**

- **댁내 공유기 설정?**
  - 원격 관리 기능 끄기
    - 원격 관리 기능이 켜져 있으면 외부에서도 공유기 설정 페이지에 접속할 수 있게 되어 해킹 위험이 높아짐



IoT 보안

인증라벨

정보보호인증을 취득한 제품에 대하여 소비자 보호를 위해 인증 취득 사실을 홍보하기 위한 정보보호인증 라벨의 표시

정보보호인증을 취득한 자는 인증을 받은 기기 등에 부착이 가능하며, 효력이 상실되었거나 인증이 취소된 경우 인증에 대한 표시를 중지해야한다.

※ 인증을 획득한 자는 인증한 사실이 과장되거나 불명확한 표현을 사용하여 광고할 수 없으며, 허위사실을 표기·광고하거나, 인증받은 제품을 임의로 변경하는 경우 인증이 취소될 수 있다.

IoT 보안

인증체계도


과학기술정보통신부
정책 수립·시행
Korea Internet & Security Agency
한국인터넷진흥원
관리감독·시험의뢰
시험결과 검토요청
정책기관
인증기관
시험대행기관
상담요청·인증신청
인증서 발급·사후관리
인증시험 결과 적합 &
부적합 여부 심의 요청
신뢰성이 검증된
IoT 기기 공급
사용자
인증신청인
인증위원회

IoT 보안

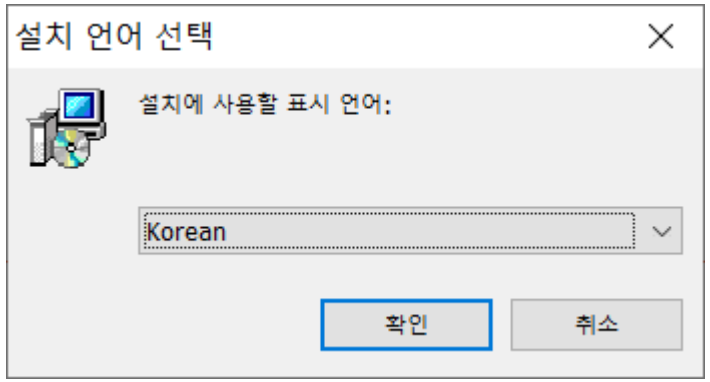
https://www.kisa.or.kr/1050608

헥사(Hex Editor) 에디터

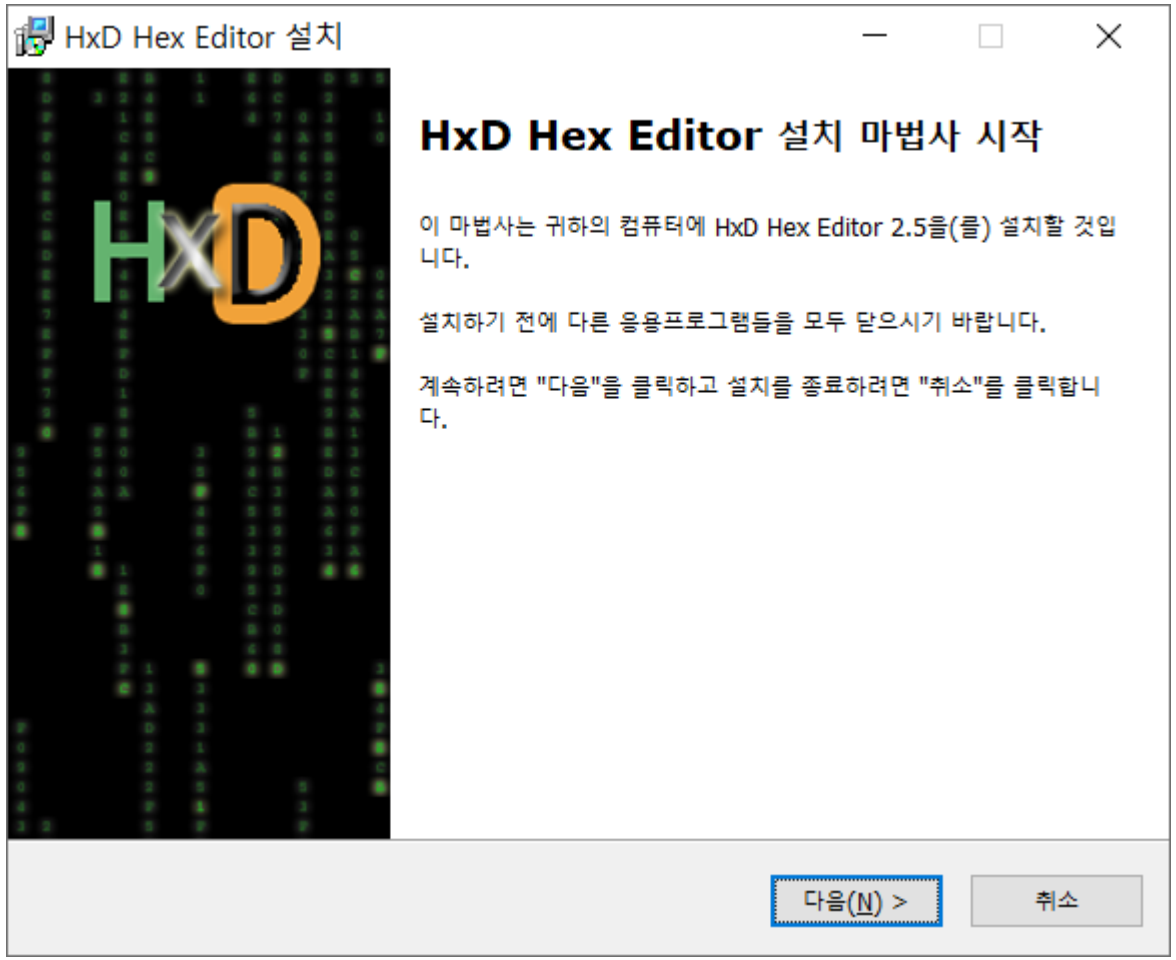
- 프로그램 설명
  - 파일의 원시(raw) 데이터 구조 확인
  - 삭제된 데이터 복원 가능성 분석
  - 스테가노그래피 및 악성코드 탐지
  - 이력 조작 여부 확인

헥사(Hex Editor) 에디터

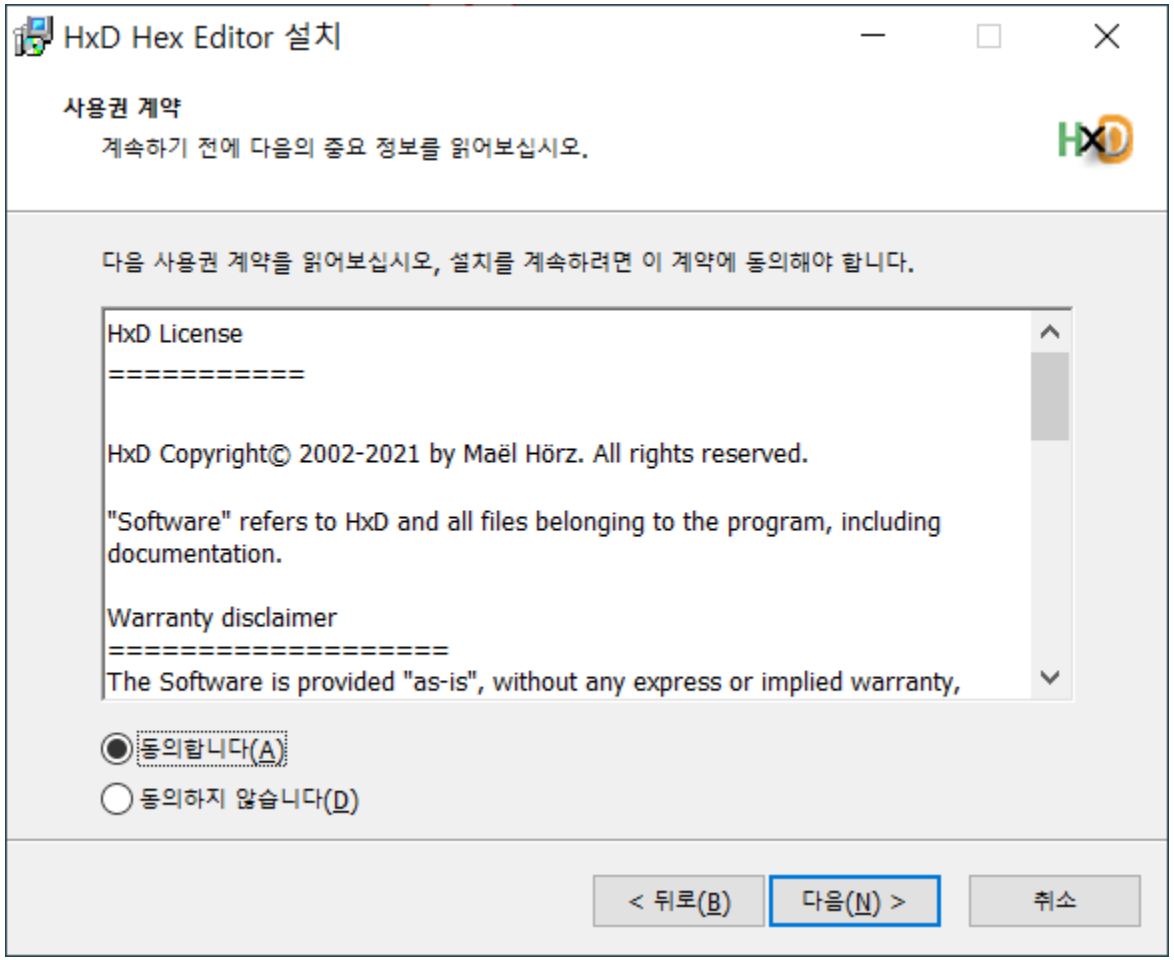
https://mh-nexus.de/en/downloads.php?product=HxD20



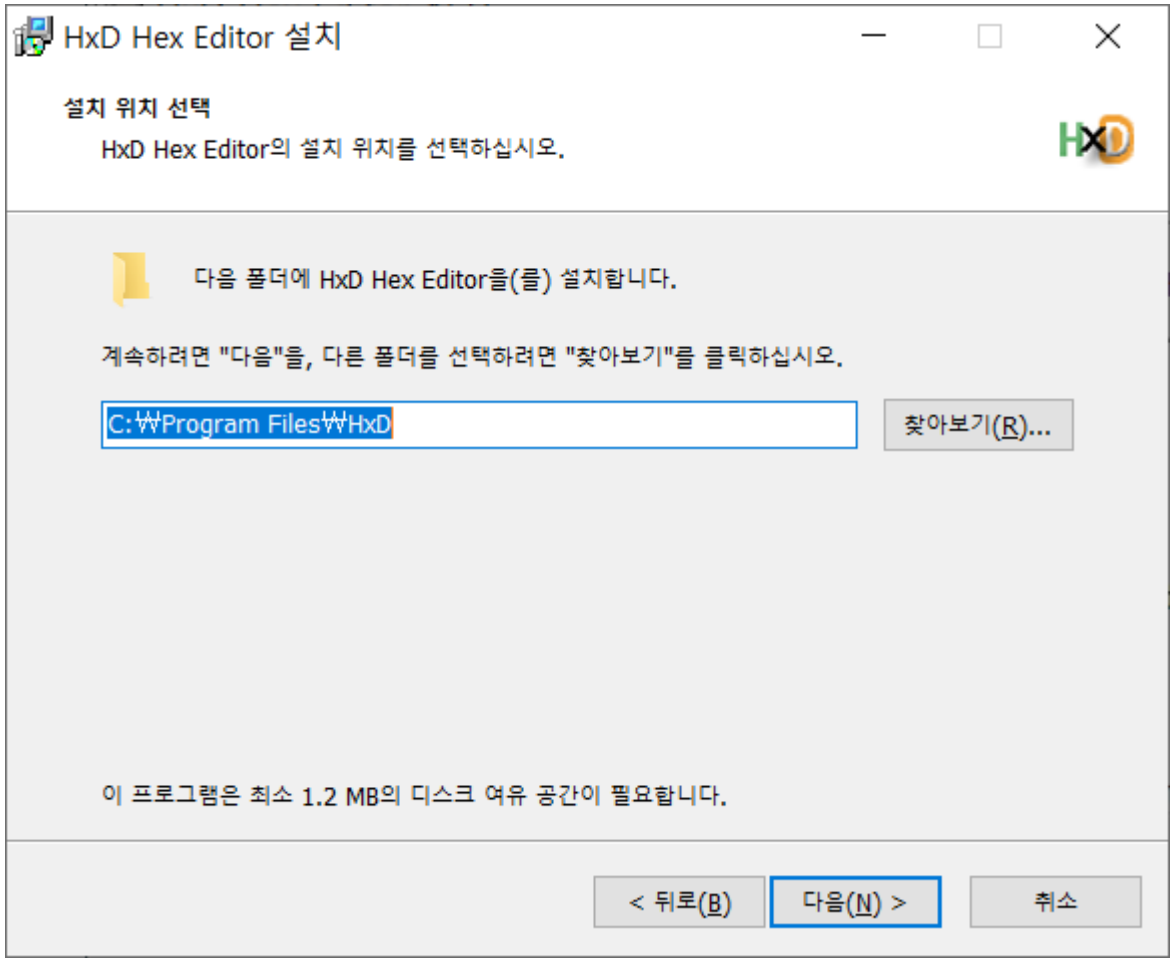
헥사(Hex Editor) 에디터



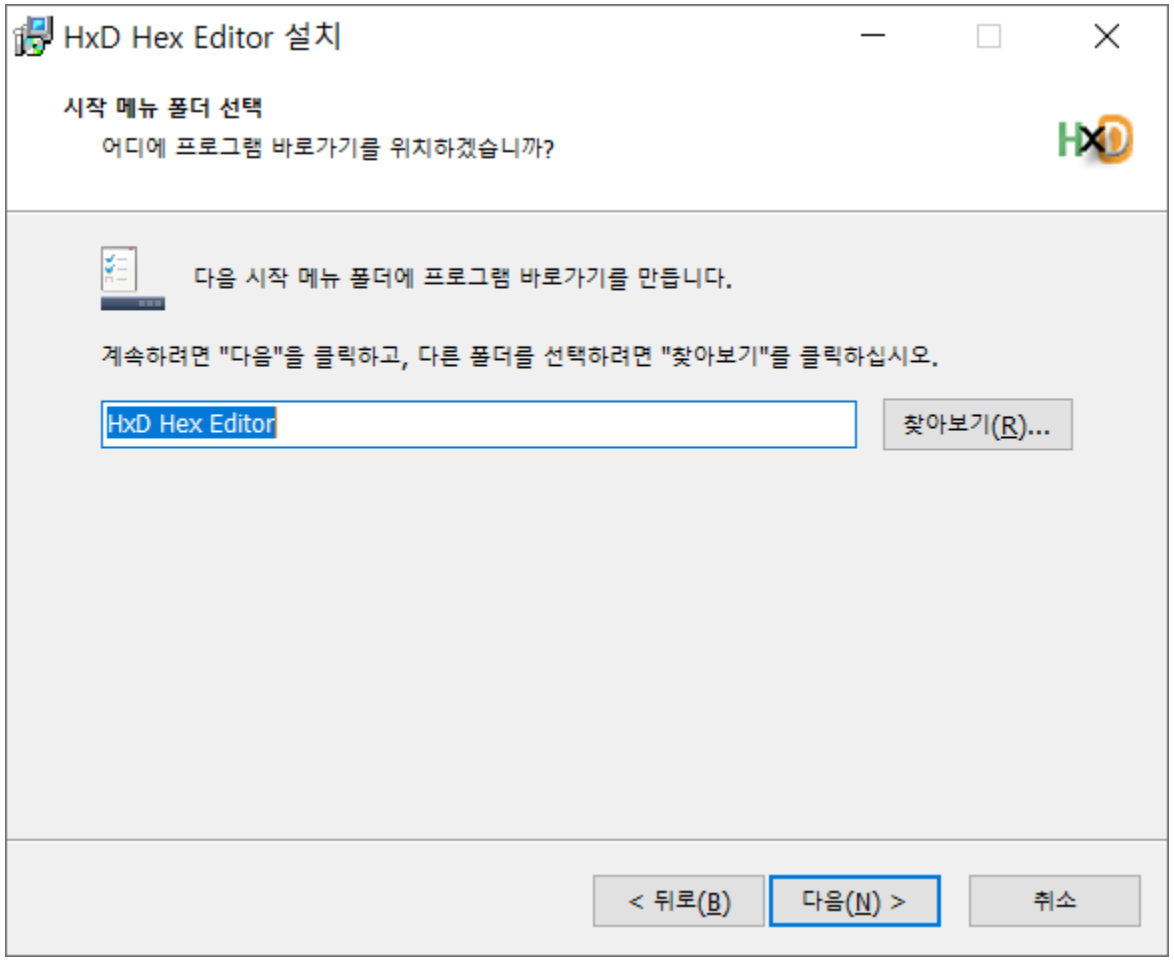
헥사(Hex Editor) 에디터



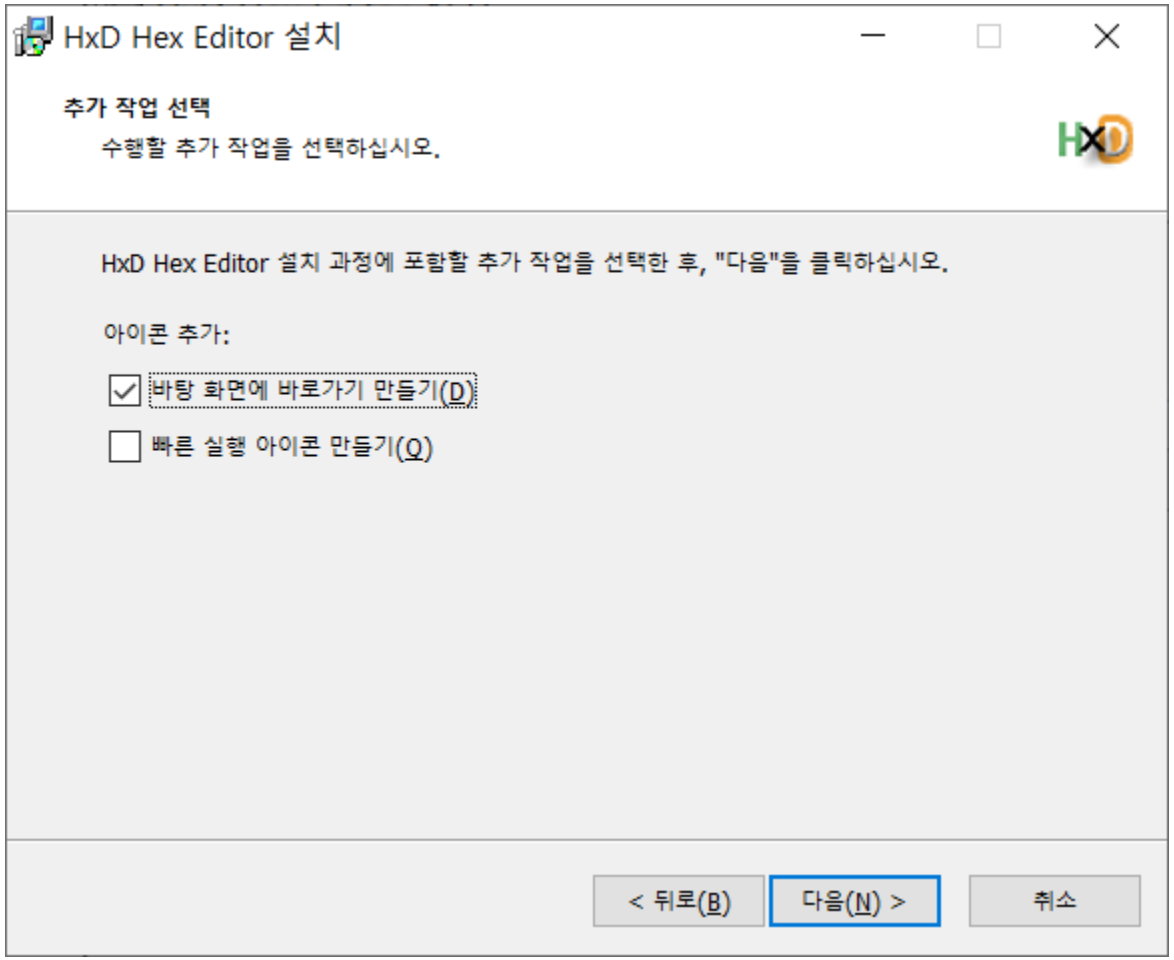
헥사(Hex Editor) 에디터



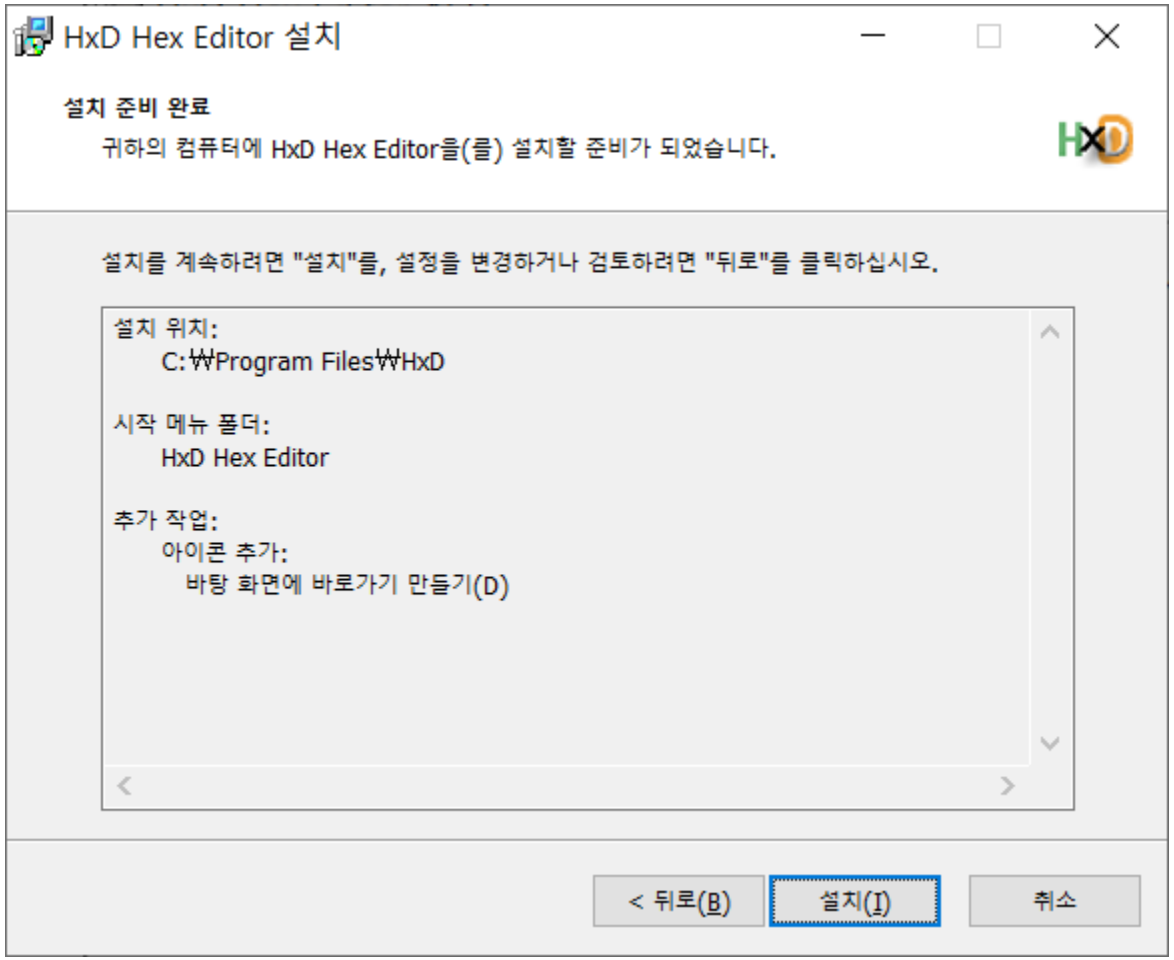
헥사(Hex Editor) 에디터



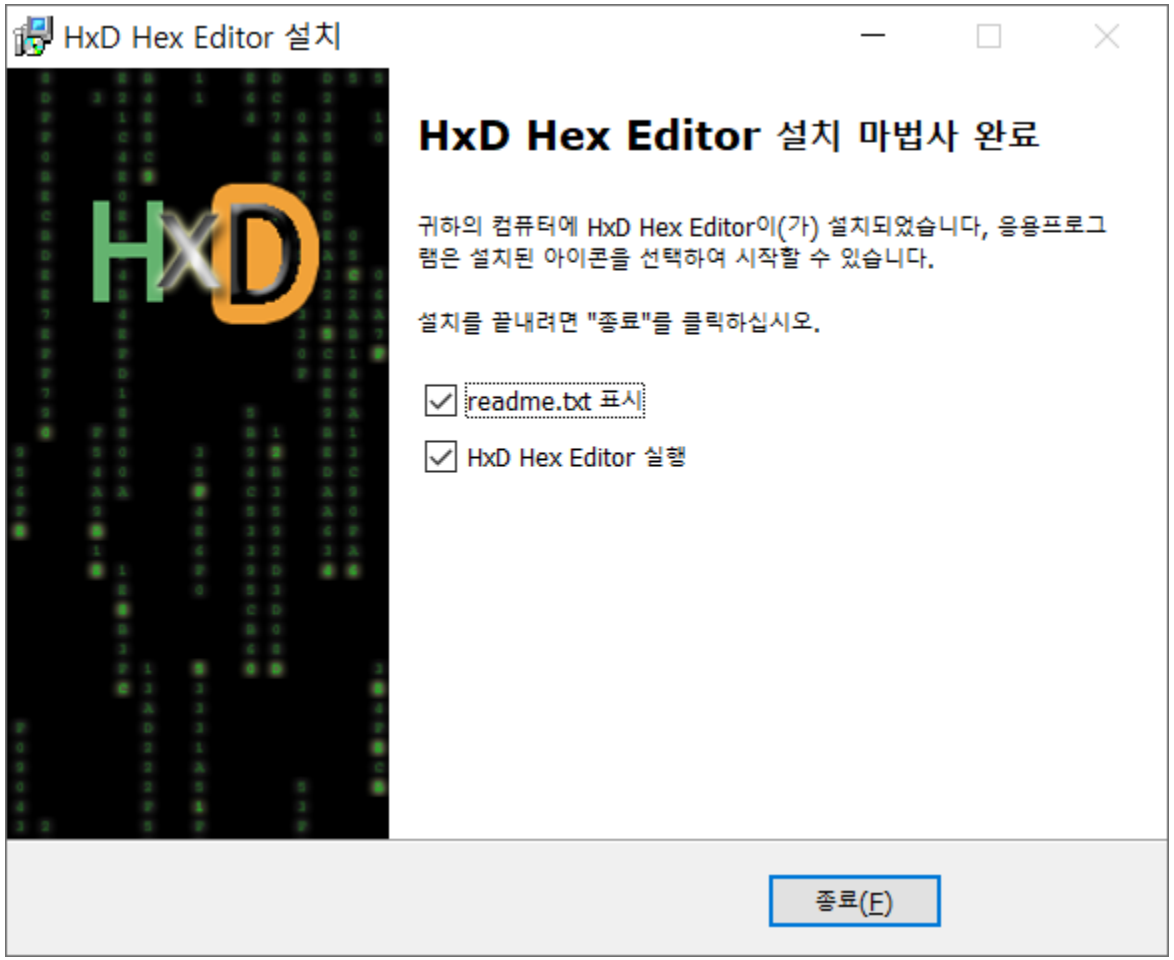
헥사(Hex Editor) 에디터



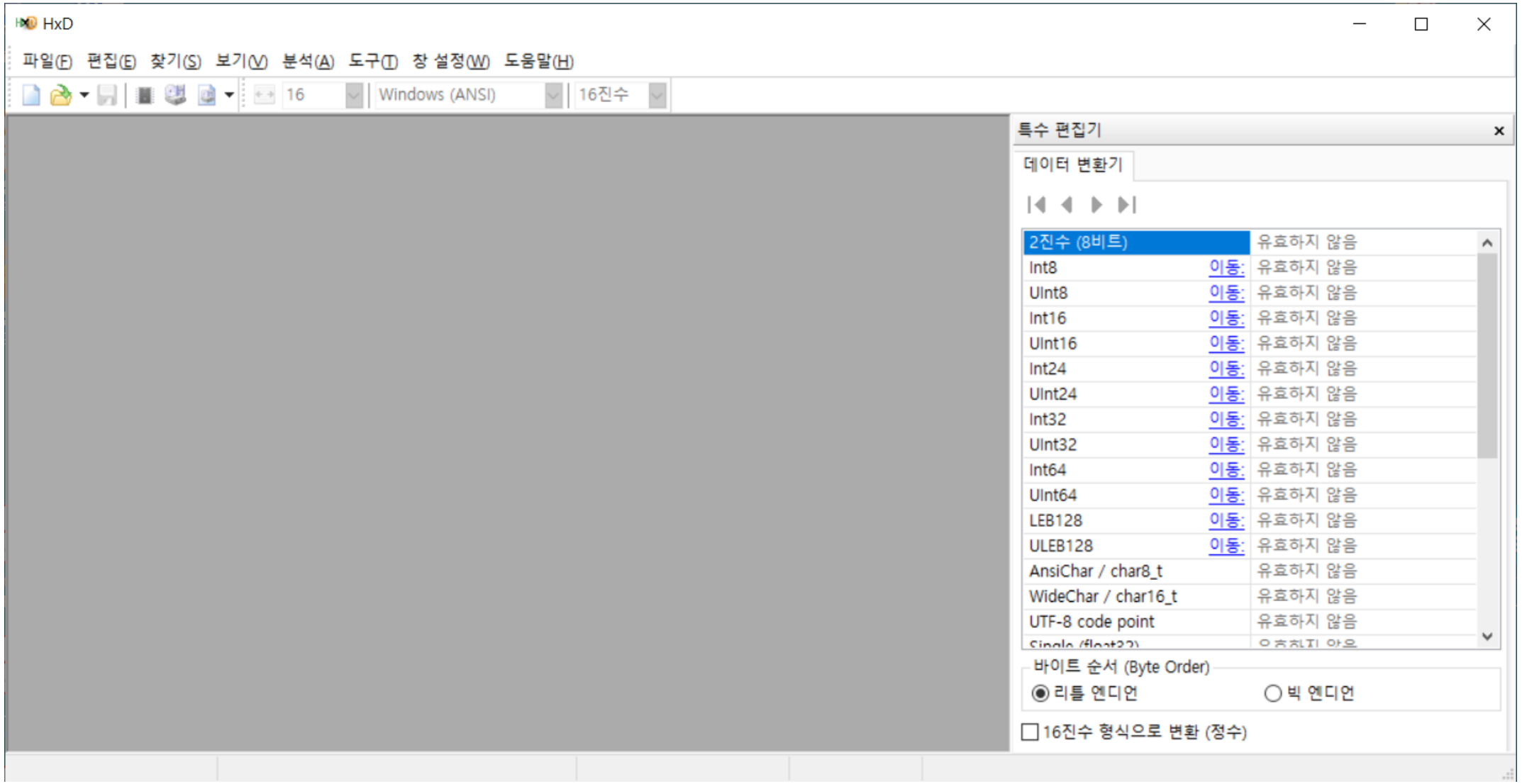
헥사(Hex Editor) 에디터



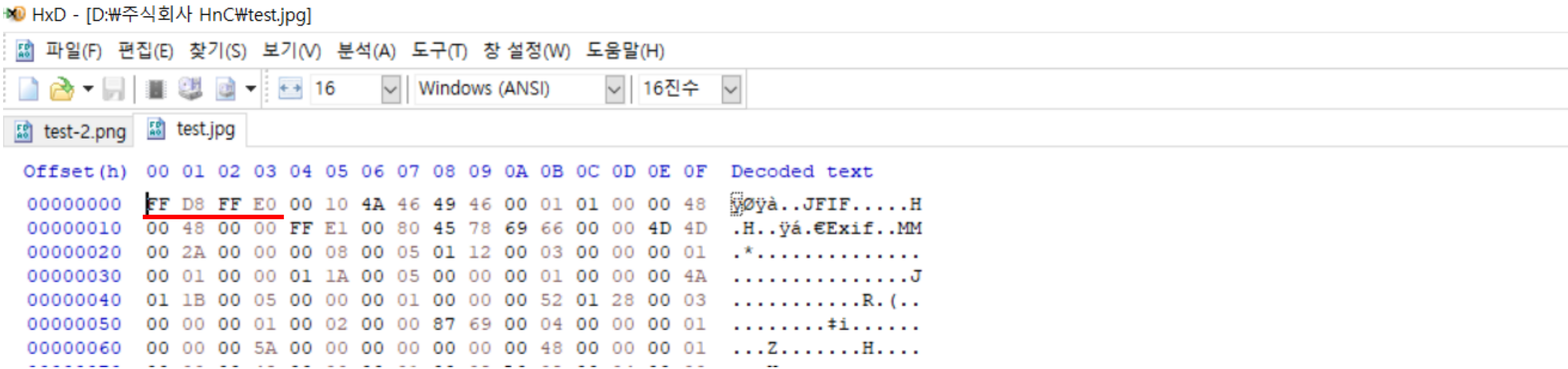
헥사(Hex Editor) 에디터



헥사(Hex Editor) 에디터



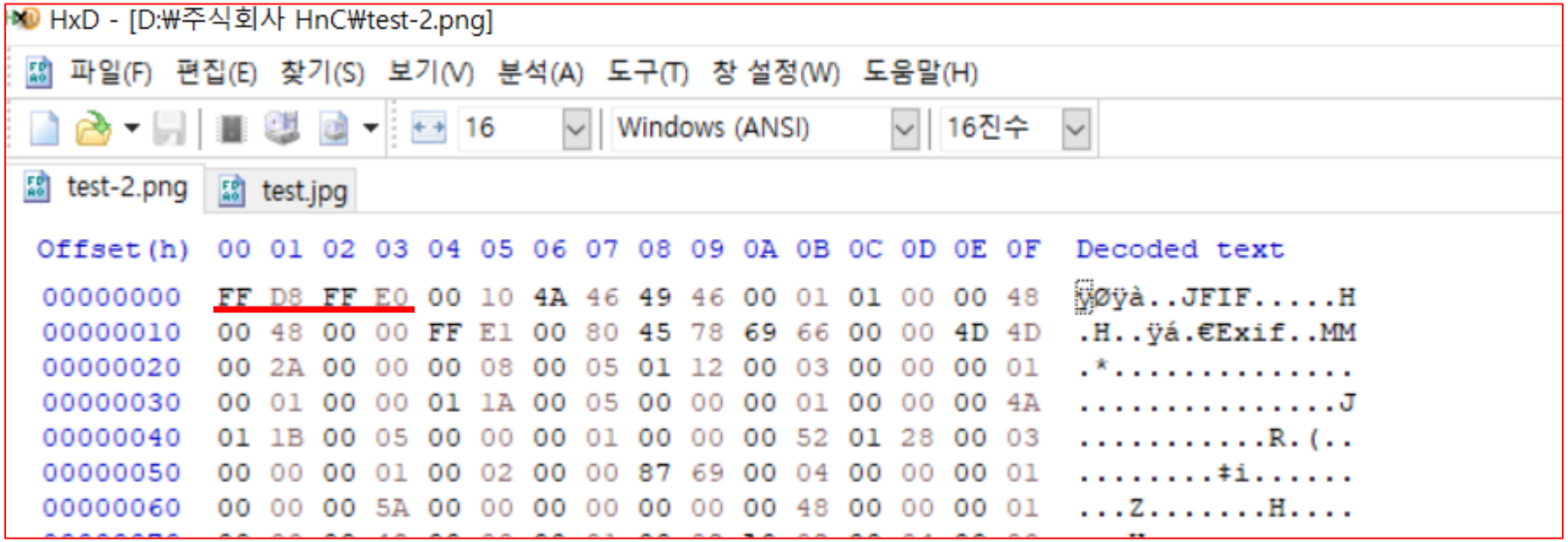
헥사(Hex Editor) 에디터 -확장자 찾기



Test.jpg 파일 open

HEX 시그니처 : FF D8 FF ➔ **jpg 파일임을 알 수 있음**

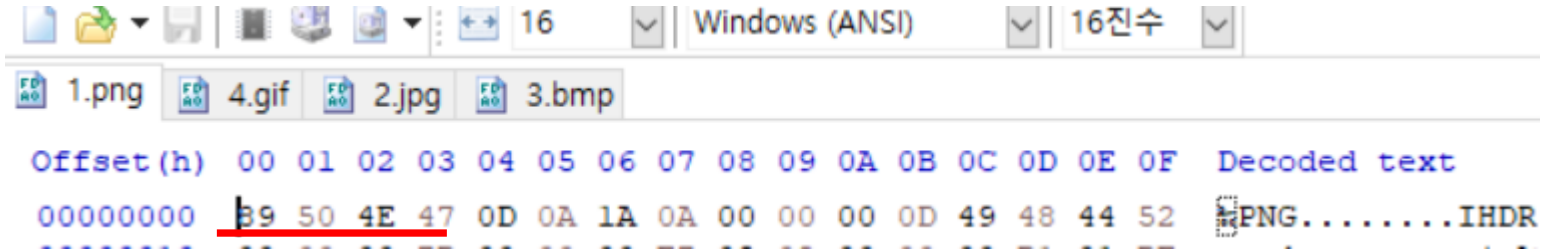
헥사(Hex Editor) 에디터 -확장자 찾기



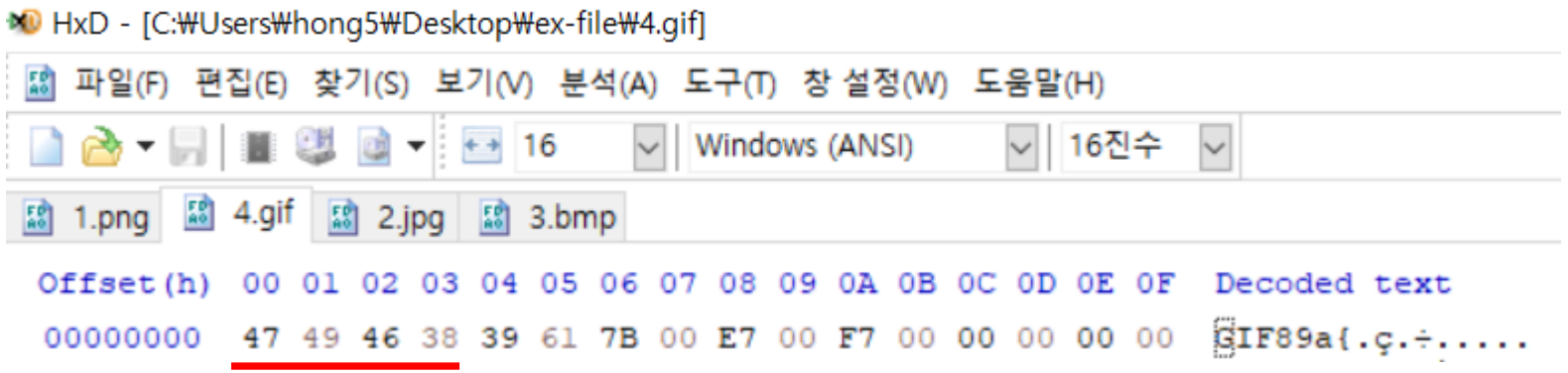
Test.png 파일 open

HEX 시그니처 : FF D8 FF ➔ ?????? ➔ 이해가 되십니까?

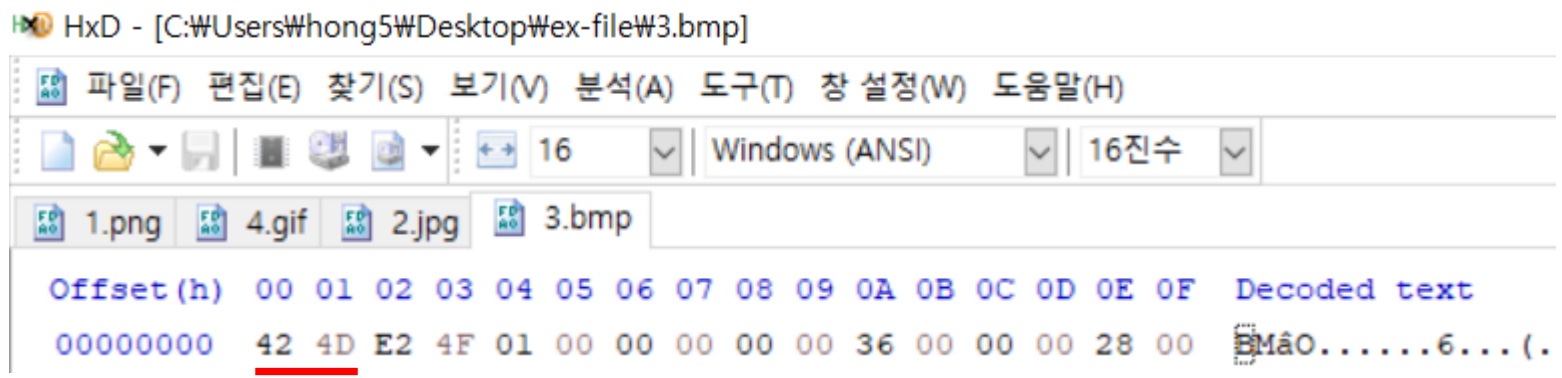
헥사(Hex Editor) 에디터 -메직 넘버



png

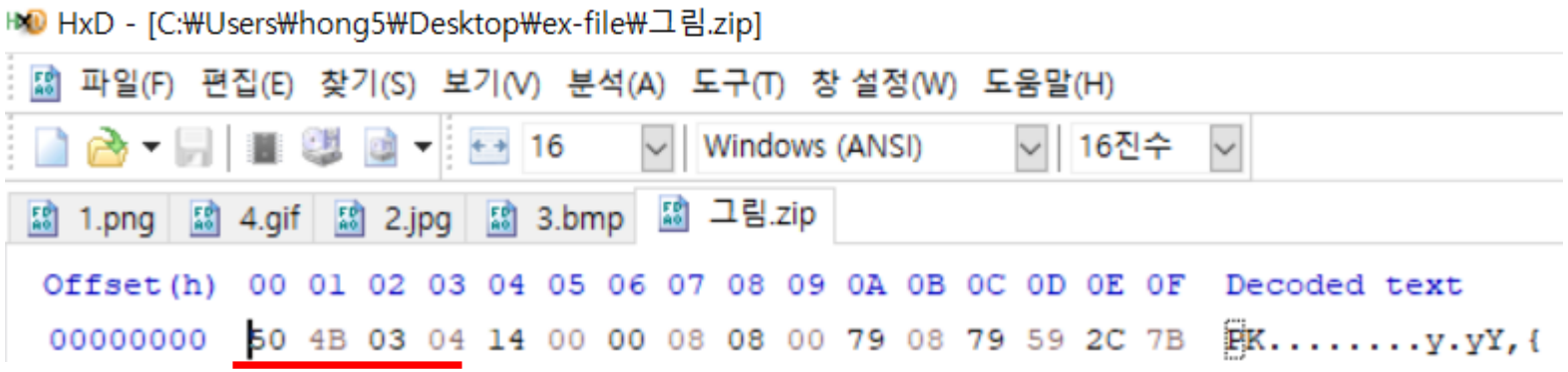


gif



bmp

헥사(Hex Editor) 에디터 -메직 넘버



zip

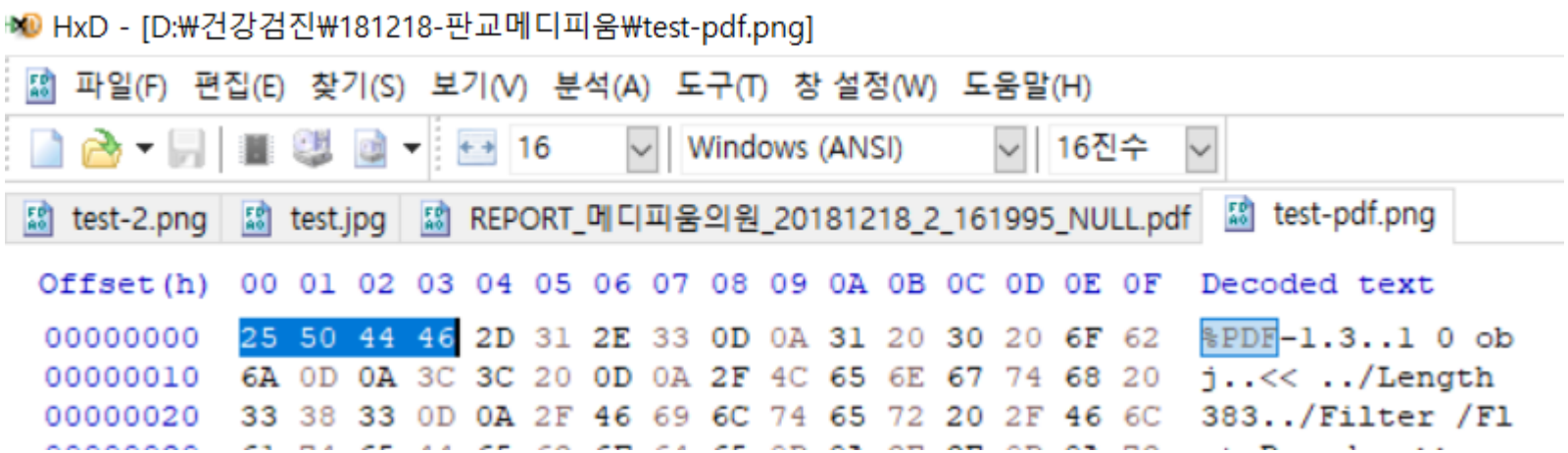
dongguk UNIVERSITY

헥사(Hex Editor) 에디터 -확장자 찾기

Pdf 파일 open

HEX 시그니처 : 25 50 44 46 ➔ **pdf 파일임을 알 수 있음**

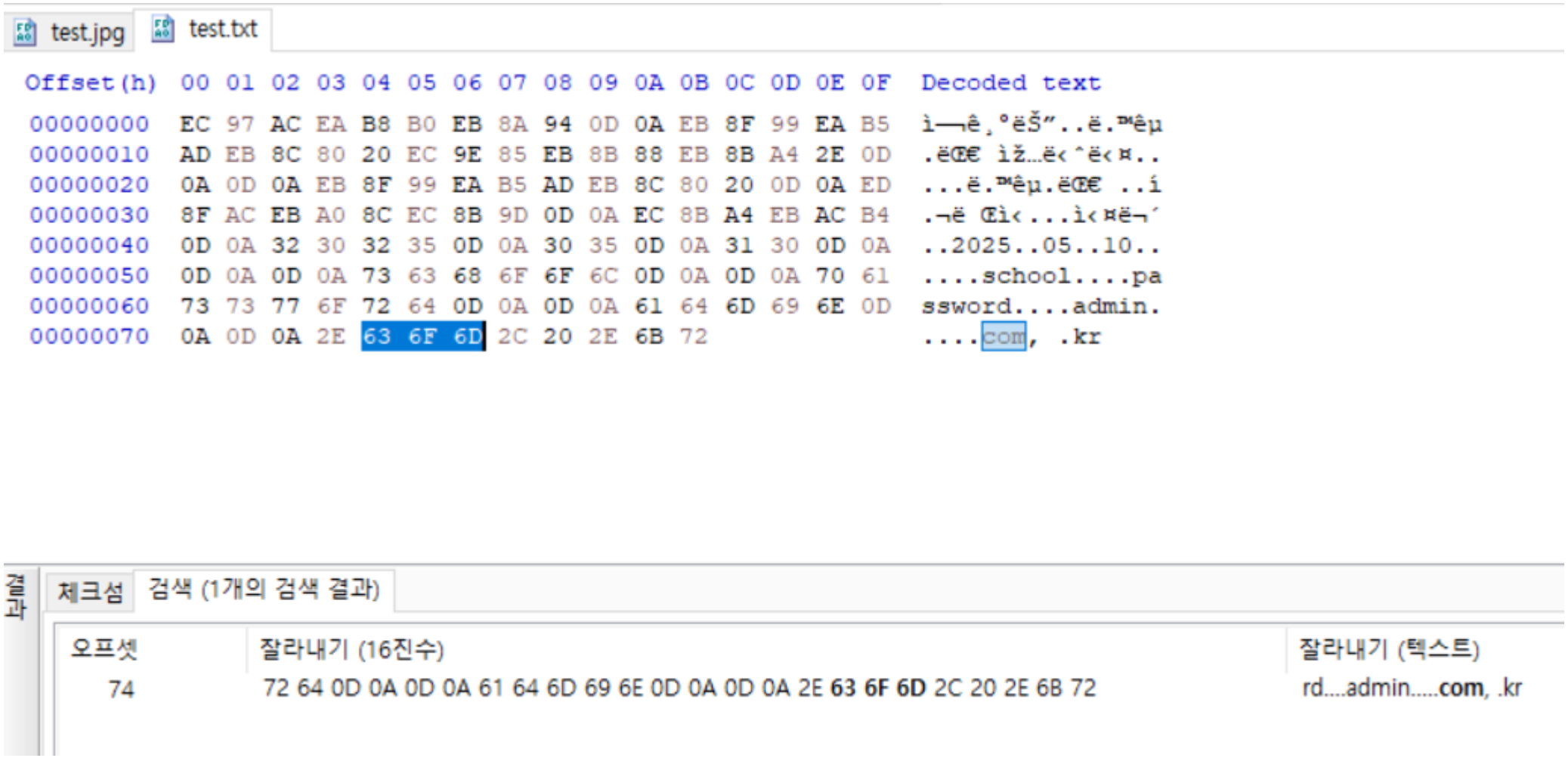
헥사(Hex Editor) 에디터 -확장자 찾기



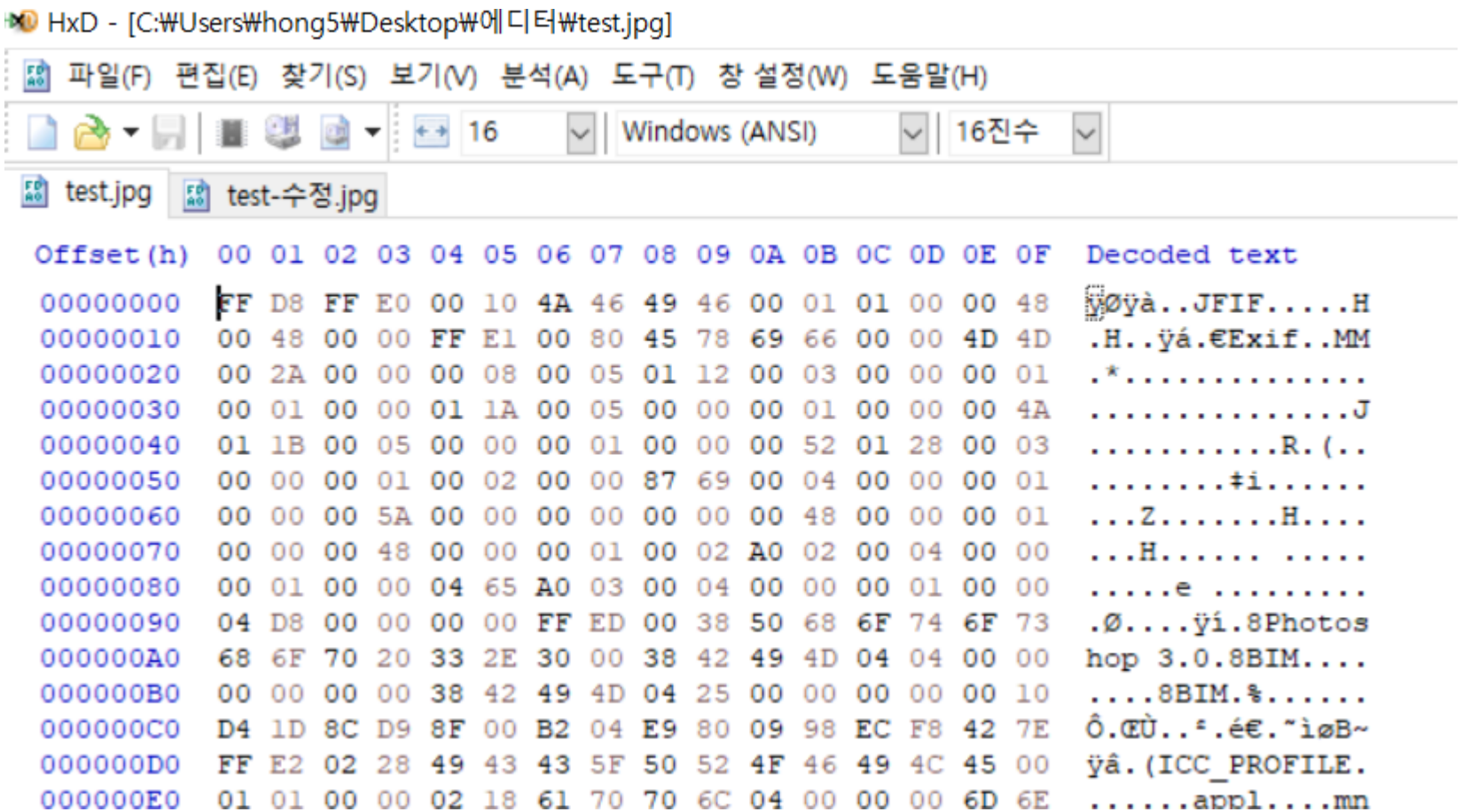
Test-pdf.png 파일 open

HEX 시그니처 : 25 50 44 46 ➔ ?????? ➔ 이해가 되십니까?

헥사(Hex Editor) 에디터 – 문자열 찾기 – ‘ctrl + f



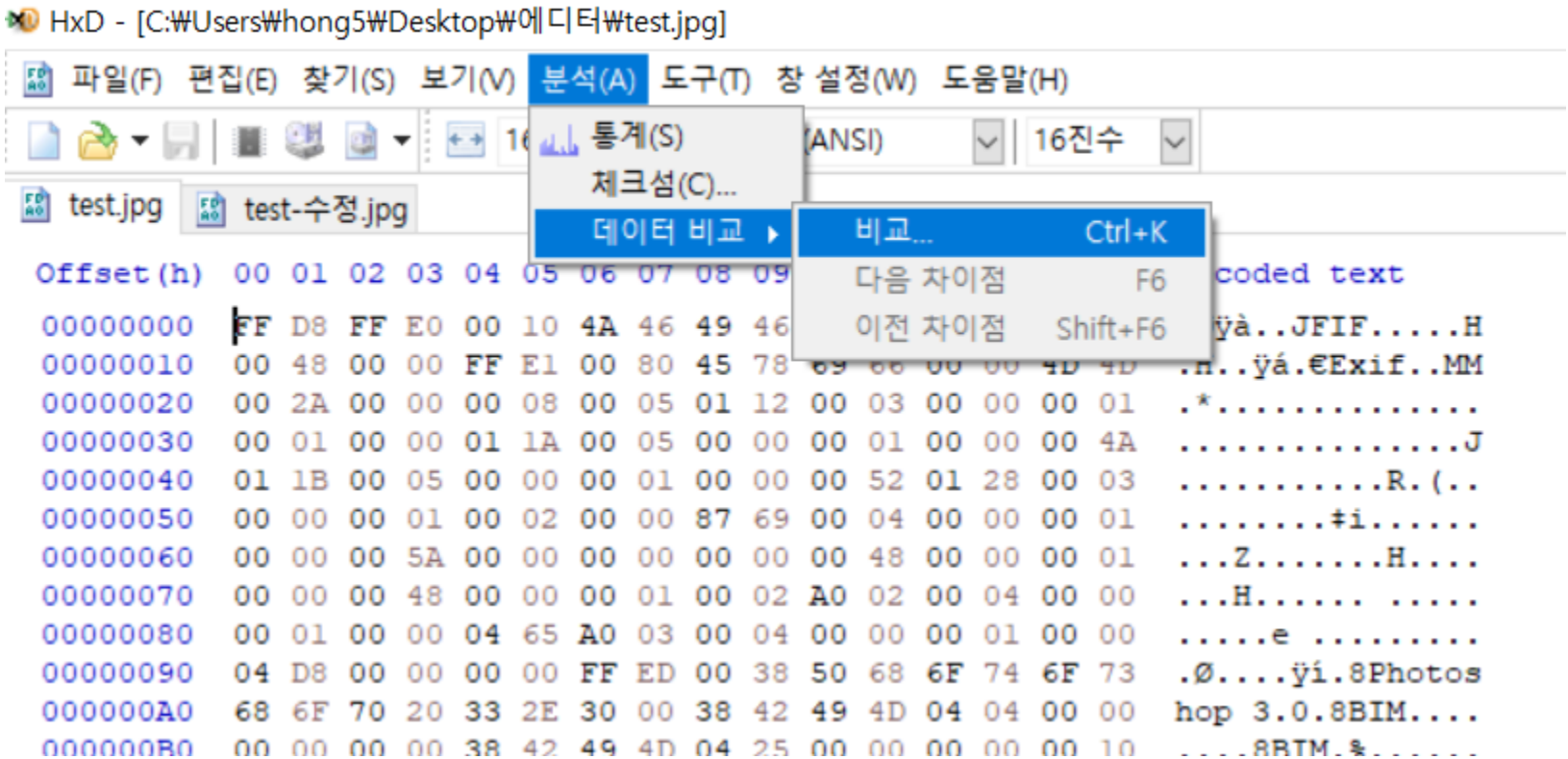
헥사(Hex Editor) 에디터 – 조작된 이미지 확인 하기



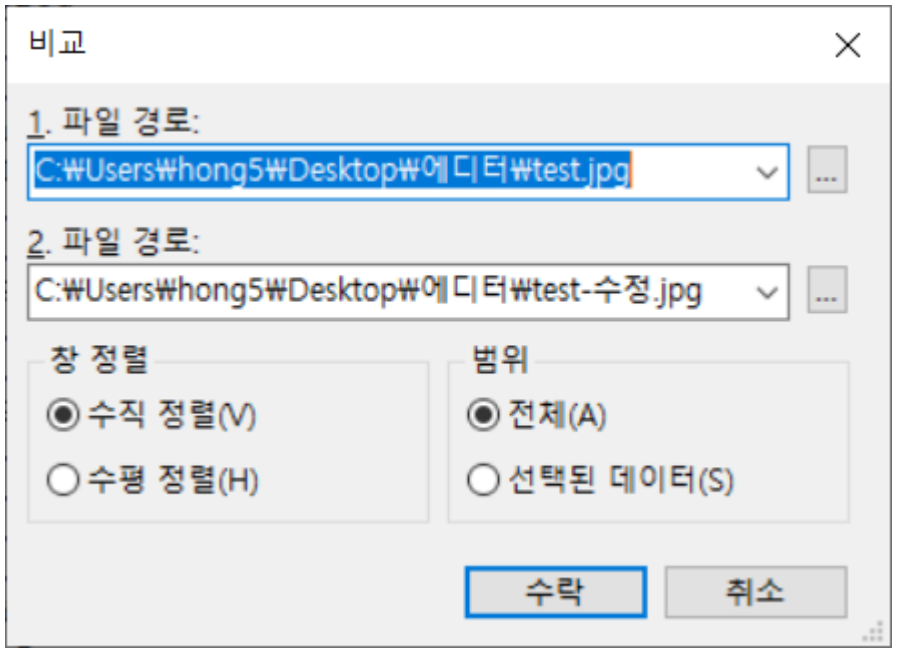
2개의 이미지를 open 함

dongguk UNIVERSITY

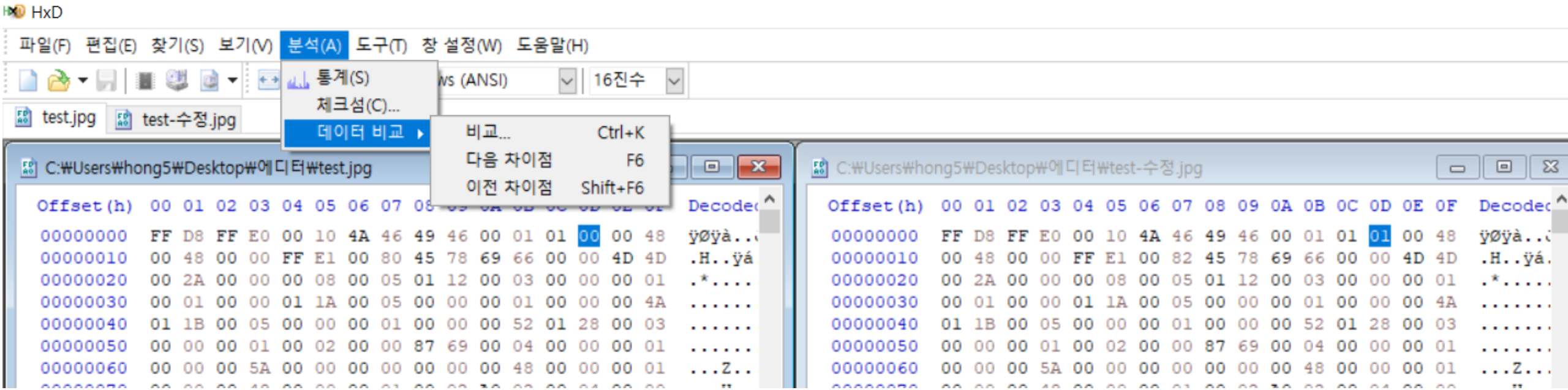
헥사(Hex Editor) 에디터 – 조작된 이미지 확인 하기



헥사(Hex Editor) 에디터 – 조작된 이미지 확인 하기



헥사(Hex Editor) 에디터 – 조작된 이미지 확인 하기



이미지가 변경된 것을 알 수 있음

헥사(Hex Editor) 에디터 – 데이터 은닉 -스테가노그래피

Steganography

https://youtu.be/uC-5pNNnaDo?si=r66hTN4zthfYlTIU

헥사(Hex Editor) 에디터 – 데이터 은닉 –스테가노그래피-1

Steganography

이미지 한 개를 준비 한다.

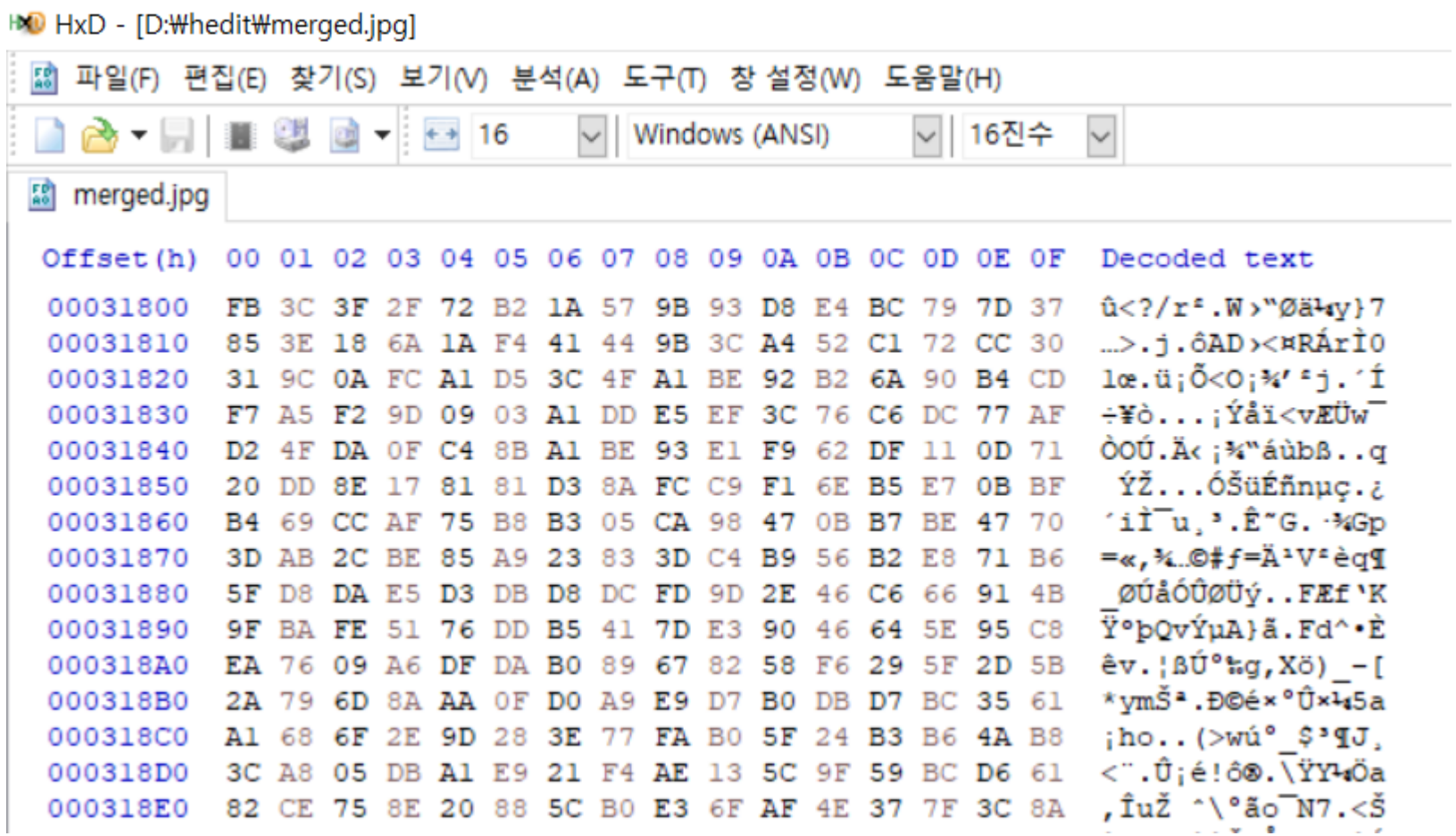
Text 파일 한 개를 준비 한다. (text 내용에는 school을 작성하고 저장 한다.)

같은 폴더에 위치 한다

D:\hedit>copy /b test.jpg + secert.txt merged.jpg

명령어 실행을하면 merged.jpg 파일이 생성이 된다

헥사(Hex Editor) 에디터 – 데이터 은닉 -스테가노그래피



은닉된 데이터를 찾는다

dongguk UNIVERSITY

헥사(Hex Editor) 에디터 – 데이터 은닉 –스테가노그래피-2

Steganography

이미지 한 개를 준비 한다.

Zip 파일 한 개를 준비 한다.

같은 폴더에 위치 한다

D:\hedit>copy /b test.jpg + pic.zip merged2.jpg

명령어 실행을하면 merged2.jpg 파일이 생성이 된다

헥사(Hex Editor) 에디터 – 데이터 은닉 –스테가노그래피-2

Steganography

이미지에서 zip 파일 추출하기

Ctrl+F → 16진수 모드 → 50 4B 03 04 검색

이 위치 부터 헥사 마지막까지 복사 함.

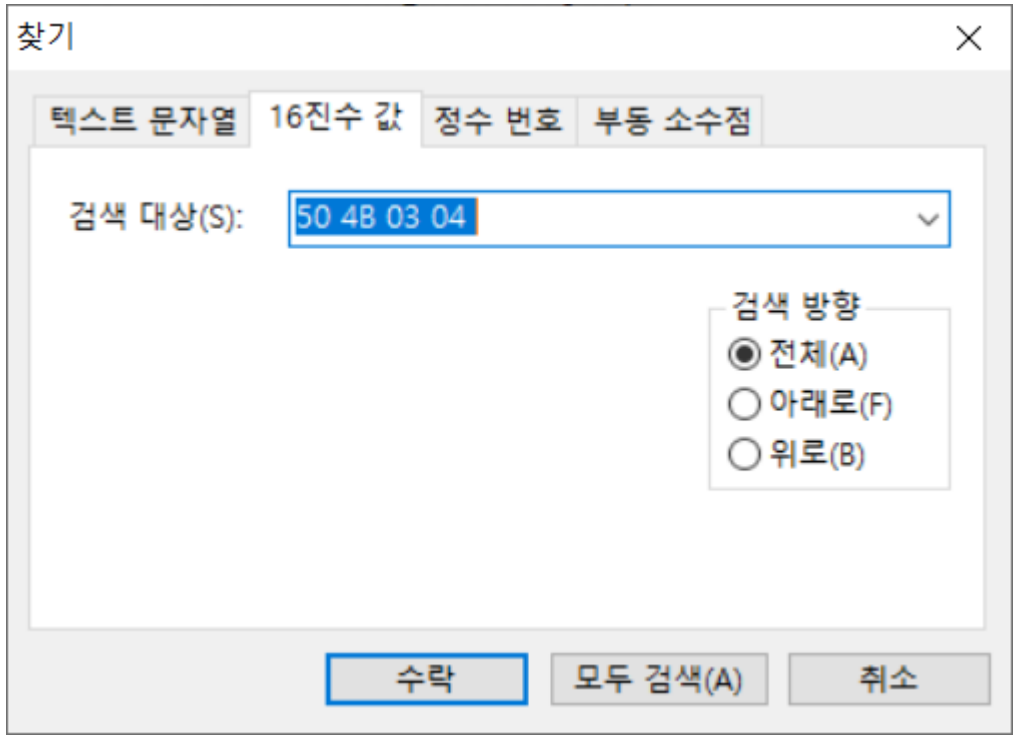
복사 하기 어려우면 ➔ 50위에 커서를 놓고 → 스크롤로 맨 마직까지 내리고-> shift 누르면서 마우스 클릭

카피 ➔ 새창 열고 ➔ 붙여넣기 ➔ 저장함.

파일이 생성됨. ➔ 내용을 확인 할수 있음.

헥사(Hex Editor) 에디터 – 데이터 은닉 –스테가노그래피-2

Steganography



헥사(Hex Editor) 에디터 – 데이터 은닉 –스테가노그래피-2

Steganography

```
00033650  AE A3 F9 0A D1 20 B6 63 6C 57 50 BB BE BC B2 9E  ®£ù.Ñ ¶clWP»¾¼²ž
00033660  FE 2B 37 82 4D C5 19 54 7F AC E7 03 20 9E 31 5A  þ+7‚MÅ.T.¬ç. ž1Z
00033670  BF D9 57 7F F4 1A B7 FC A3 FF 00 E2 6B 8F D5 3F  ¿ÙW.ô.·ü£ÿ.âk.Õ?
00033680  E4 73 D5 FF 00 DE 8F FF 00 41 34 B4 19 FB 34 7F  äsÕÿ.Þ.ÿ.A4´.û4.
00033690  FF D9 50 4B 03 04 14 00 00 08 08 00 79 08 79 59  ÿÙPK.........y.yY
000336A0  2C 7B 44 11 F7 EB 01 00 80 0B 02 00 0B 00 00 00  ,{D.÷ë..€.......
000336B0  EA B7 B8 EB A6 BC 2E 64 6F 63 78 EC 9A 53 73 25  ê·¸ë¦¼.docxìšSs%
000336C0  0C 12 86 63 DB B6 9D 13 DB CE 44 13 DB B6 6D DB  ..†cÛ¶..ÛÎD.Û¶mÛ
000336D0  36 26 13 4E 6C DB C6 09 4F F0 C5 FA 62 27 BB 5B  6&.NlÛÆ.OðÅúb'»[
```


dongguk UNIVERSITY

헥사(Hex Editor) 에디터 – 데이터 은닉 –스테가노그래피-2

Steganography

```
00033610  3A DE ED D5 55 ED 5A 28 81 CA 31 91 4B 46 31 C1  :ÞíÕUíZ(.Ê1'KF1Á
00033620  C0 20 E7 B0 FE 55 99 6A 2D 6C F5 06 B2 BF 9E 45  À ç°þU™j-lõ.²¿žE
00033630  68 9F 90 76 1D F9 C3 10 70 C4 9C F4 E6 BD 23 5B  hŸ.v.ùÃ.pÄœôæ½#[
00033640  FF 00 8F 96 FA CB FC EB C7 35 AF F9 1B E6 FF 00  ÿ..–úËüëÇ5¯ù.æÿ.
00033650  AE A3 F9 0A D1 20 B6 83 6C 57 50 BB BE BC B2 9E  ®£ù.Ñ ¶ƒlWP»¾¼²ž
00033660  FE 2B 37 82 4D C5 19 54 7F AC E7 03 20 9E 31 5A  þ+7‚MÅ.T.¬ç. ž1Z
00033670  BF D9 57 7F F4 1A B7 FC A3 FF 00 E2 6B 8F D5 3F  ¿ÙW.ô.·ü£ÿ.âk.Õ?
00033680  E4 73 D5 FF 00 DE 8F FF 00 41 34 B4 19 FB 34 7F  äsÕÿ.Þ.ÿ.A4´.û4.
00033690  FF D9 50 4B 03 04 14 00 00 08 08 00 79 08 79 59  ÿÙPK.........y.yY
000336A0  2C 7B 44 11 F7 EB 01 00 80 0B 02 00 0B 00 00 00  ,{D.÷ë..€.......
000336B0  EA B7 B8 EB A6 BC 2E 64 6F 63 78 EC 9A 53 73 25  ê·¸ë¦¼.docxìšSs%
000336C0  0C 12 86 63 DB B6 9D 13 DB CE 44 13 DB B6 6D DB  ..†cÛ¶..ÛÎD.Û¶mÛ
000336D0  36 26 13 4E 6C DB C6 09 4F F0 C5 FA 62 27 BB 5B  6&.NlÛÆ.OðÅúb'»[
000336E0  7B B5 55 FB 0F 76 DF 8B EE BE EE EE A7 BA BB AA  {uUû.vß‹î¾îî§º»ª
```


dongguk UNIVERSITY

헥사(Hex Editor) 에디터 – 데이터 은닉 –스테가노그래피-2

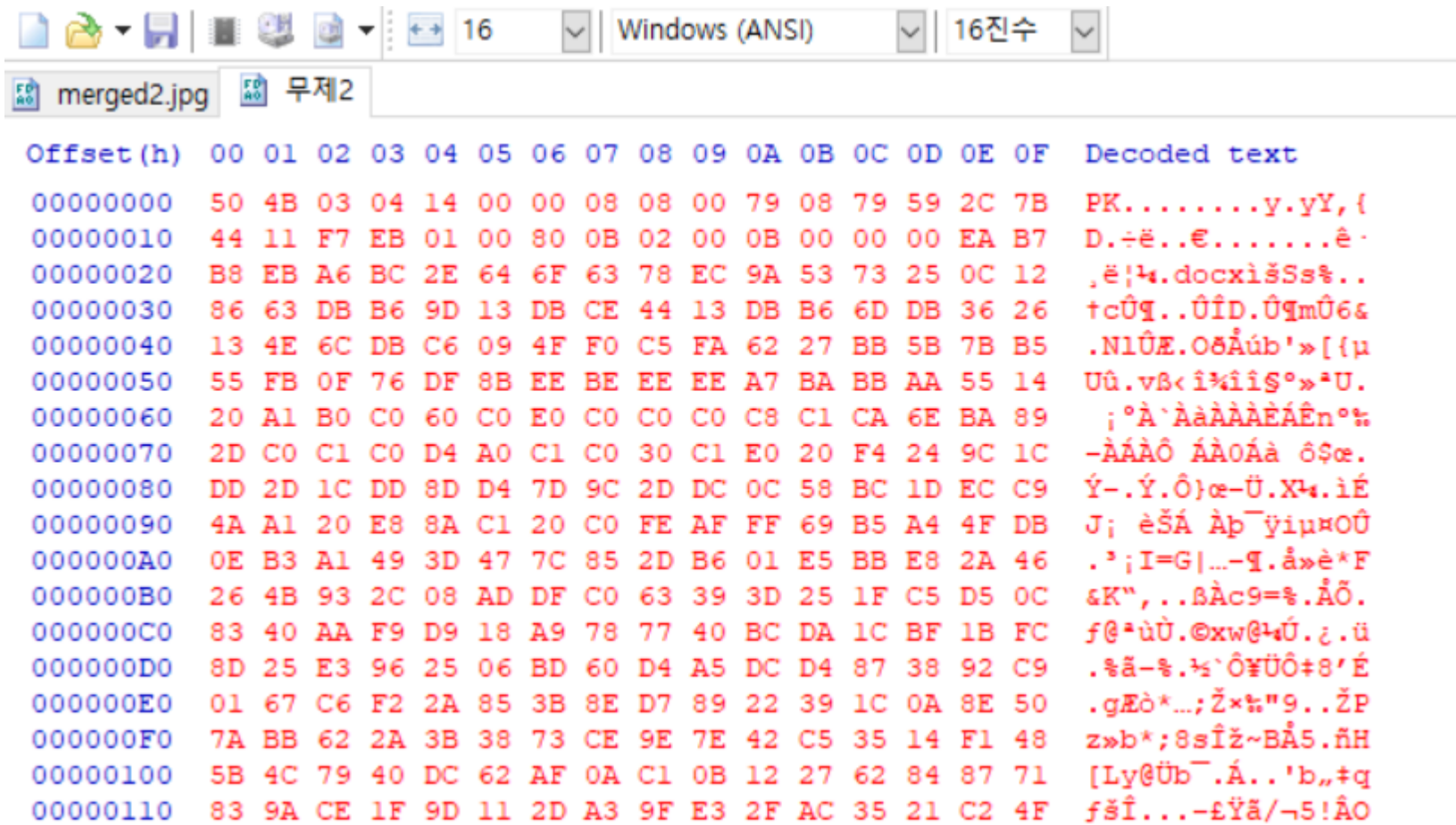
Steganography

```
000521F0  69 16 17 0A F0 01 03 F5 77 10 ED CB 7F 84 60 FB  i...ð..õw.íË.„`û
00052200  15 04 32 75 85 F9 35 30 07 D7 7F C8 05 C8 CE 1F  ..2u…ù50.×.È.ÈÎ.
00052210  21 DE FF 0A 22 8C B1 24 48 F9 13 08 08 50 7F 07  !Þÿ."Œ±$Hù...P..
00052220  41 7E F9 47 08 F6 5F 41 0C 9A 87 10 52 02 0B 3D  A~ùG.ö_A.š‡.R..=
00052230  50 7F 07 51 61 07 FA 07 08 8E 7F 40 FC EB 5D 8A  P..Qa.ú..Ž.@üë]Š
00052240  FF 10 98 4D D0 5F EF 59 FC 0B C4 BF DE 8F F2 0F  ÿ.˜MÐ_ïYü.Ä¿Þ.ò.
00052250  D1 DF 07 FD E3 EE 94 BF 98 FF EB E5 D7 7F 48 CD  ÑB.ýãî"¿˜ÿëå×.HÍ
00052260  09 E8 6F 16 63 7F 69 FC FB 31 D8 3F E4 F0 09 F4  .èo.c.iüû1Ø?äð.ô
00052270  97 23 B2 BF 20 FC EB A1 C2 3F 24 E0 05 F4 17 03  —#²¿ üë¡Â?$à.ô..
00052280  87 BF D8 FF AB 1E E2 6F 65 0C 04 0C E4 0F FD C5  ‡¿Øÿ«.âoe...ä.ýÅ
00052290  BF 98 FF AB 86 FB B7 E2 04 0E 34 FF 5D 33 2E 2F  ¿˜ÿ«†û·â..4ÿ]3./
000522A0  05 09 F5 33 0C 0D F8 B7 08 01 02 12 0B 05 06 BC  ..õ3..ø·.......¼
000522B0  FB 13 50 4B 01 02 3F 00 14 00 00 08 08 00 79 08  û.PK..?.......y.
000522C0  79 59 2C 7B 44 11 F7 EB 01 00 80 0B 02 00 0B 00  yY,{D.÷ë..€.....
000522D0  24 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00  $....... .......
000522E0  EA B7 B8 EB A6 BC 2E 64 6F 63 78 0A 00 20 00 00  ê·¸ë¦¼.docx.. ..
000522F0  00 00 00 01 00 18 00 80 E0 CC 72 8A 3E DB 01 80  .......€àÌrŠ>Û.€
00052300  E0 CC 72 8A 3E DB 01 80 E0 CC 72 8A 3E DB 01 50  àÌrŠ>Û.€àÌrŠ>Û.P
00052310  4B 05 06 00 00 00 00 01 00 01 00 5D 00 00 00 20  K..........]...
00052320  EC 01 00 00 00                                   ì....
```


dongguk UNIVERSITY

헥사(Hex Editor) 에디터 – 데이터 은닉 –스테가노그래피-2

Steganography

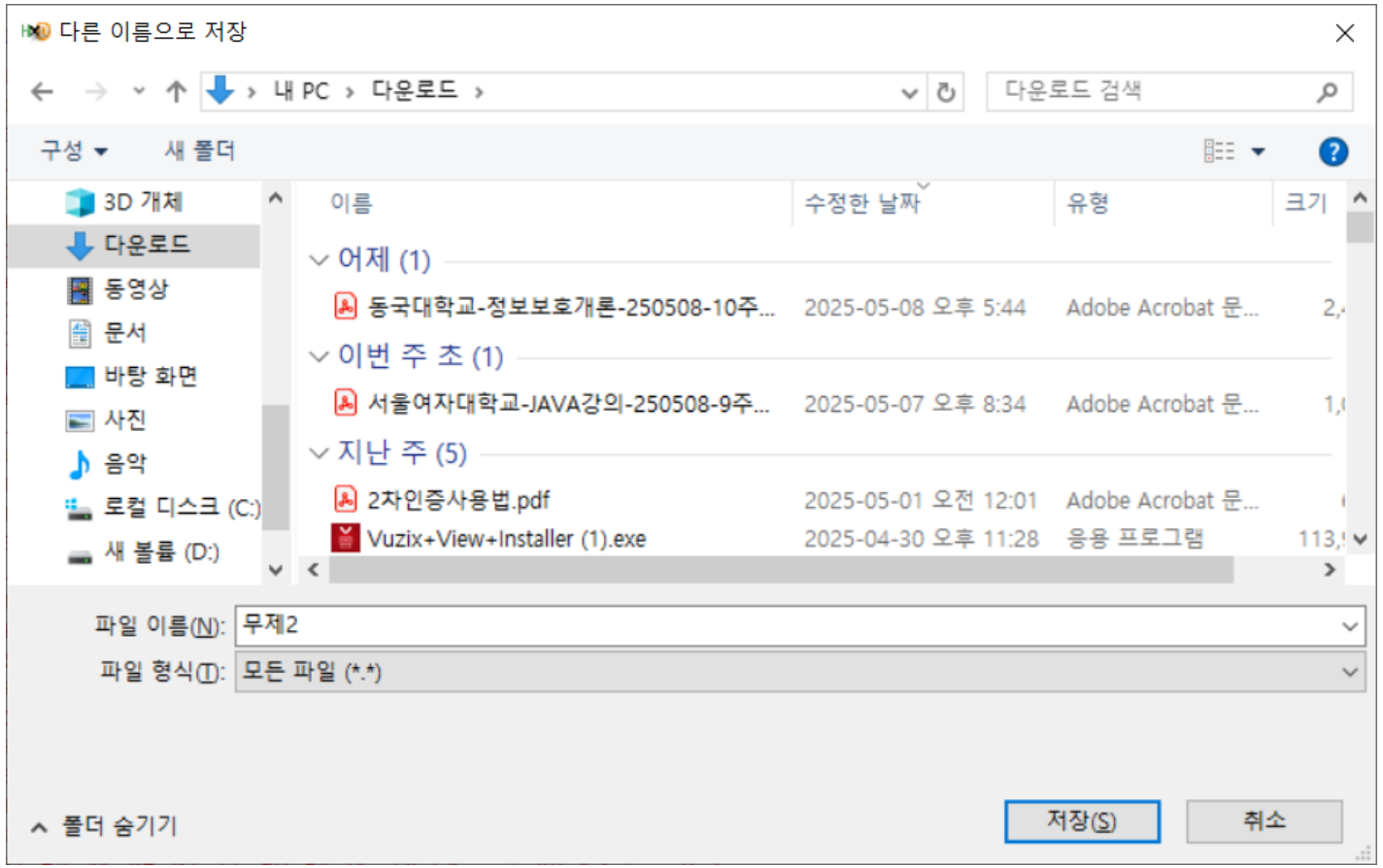


Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	50	4B	03	04	14	00	00	08	08	00	79	08	79	59	2C	7B	PK.....y.yY,{
00000010	44	11	F7	EB	01	00	80	0B	02	00	0B	00	00	00	EA	B7	D.÷ë..€.....ê·
00000020	B8	EB	A6	BC	2E	64	6F	63	78	EC	9A	53	73	25	0C	12	¸ë¦¼.docxìšSs%..
00000030	86	63	DB	B6	9D	13	DB	CE	44	13	DB	B6	6D	DB	36	26	†cÛ¶..ÛÎD.Û¶mÛ6&
00000040	13	4E	6C	DB	C6	09	4F	F0	C5	FA	62	27	BB	5B	7B	B5	.NlÛÆ.OðÅúb'»[{µ
00000050	55	FB	0F	76	DF	8B	EE	BE	EE	EE	A7	BA	BB	AA	55	14	Uû.vß‹î¾îî§º»ªU.
00000060	20	A1	B0	C0	60	C0	E0	C0	C0	C0	C8	C1	CA	6E	BA	89	¡°À`ÀàÀÀÀÈÁÊnº‰
00000070	2D	C0	C1	C0	D4	A0	C1	C0	30	C1	E0	20	F4	24	9C	1C	-ÀÁÀÔ ÁÀ0Áà ô$œ.
00000080	DD	2D	1C	DD	8D	D4	7D	9C	2D	DC	0C	58	BC	1D	EC	C9	Ý-.Ý.Ô}œ-Ü.X¼.ìÉ
00000090	4A	A1	20	E8	8A	C1	20	C0	FE	AF	FF	69	B5	A4	4F	DB	J¡ èŠÁ Àþ¯ÿiµ¤OÛ
000000A0	0E	B3	A1	49	3D	47	7C	85	2D	B6	01	E5	BB	E8	2A	46	.³¡I=G|…-¶.å»è*F
000000B0	26	4B	93	2C	08	AD	DF	C0	63	39	3D	25	1F	C5	D5	0C	&K",..ßÀc9=%.ÅÕ.
000000C0	83	40	AA	F9	D9	18	A9	78	77	40	BC	DA	1C	BF	1B	FC	ƒ@ªùÙ.©xw@¼Ú.¿.ü
000000D0	8D	25	E3	96	25	06	BD	60	D4	A5	DC	D4	87	38	92	C9	.%ã–%.½`Ô¥ÜÔ‡8'É
000000E0	01	67	C6	F2	2A	85	3B	8E	D7	89	22	39	1C	0A	8E	50	.gÆò*…;Ž×‰"9..ŽP
000000F0	7A	BB	62	2A	3B	38	73	CE	9E	7E	42	C5	35	14	F1	48	z»b*;8sÎž~BÅ5.ñH
00000100	5B	4C	79	40	DC	62	AF	0A	C1	0B	12	27	62	84	87	71	[Ly@Üb¯.Á..'b„‡q
00000110	83	9A	CE	1F	9D	11	2D	A3	9F	E3	2F	AC	35	21	C2	4F	ƒšÎ...-£Ÿã/¬5!ÂO

dongguk UNIVERSITY

헥사(Hex Editor) 에디터 – 데이터 은닉 –스테가노그래피-2

Steganography



Thank you for Listening

새로운 세상과 변화에 도전하는 동국대인이 되기를 바랍니다.