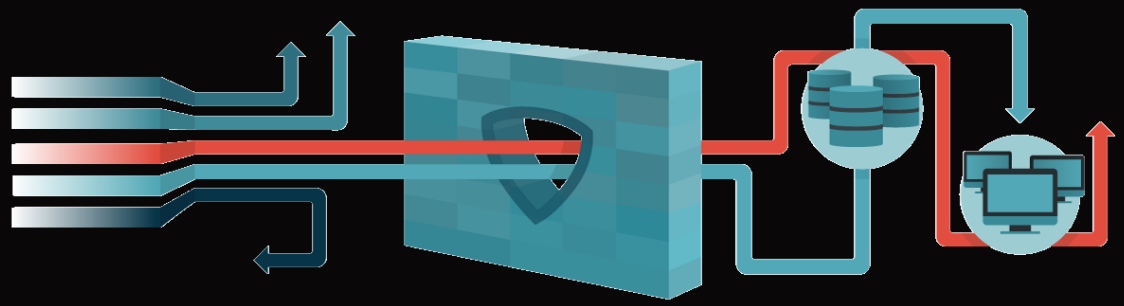
강의실 컴퓨터

X

Crypto Mining



Just for fun | SCP | CCIT

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

>__ Contents

[Extra] Bug Bounty - 첫 번째 발표

- 발표 이 후 학교 웹 자체 진단 점검 팀 개설
- XSS(2), SQLI(1), File Upload(1), 정보유출(3) 추가
- 정보유출(1) 패치
- 학교 웹은 Feed는 있으나 Back은 없다.

ining

[7월 기준] 1XMR = 120$ = \130,000

Q 어느 정도의 채산성?

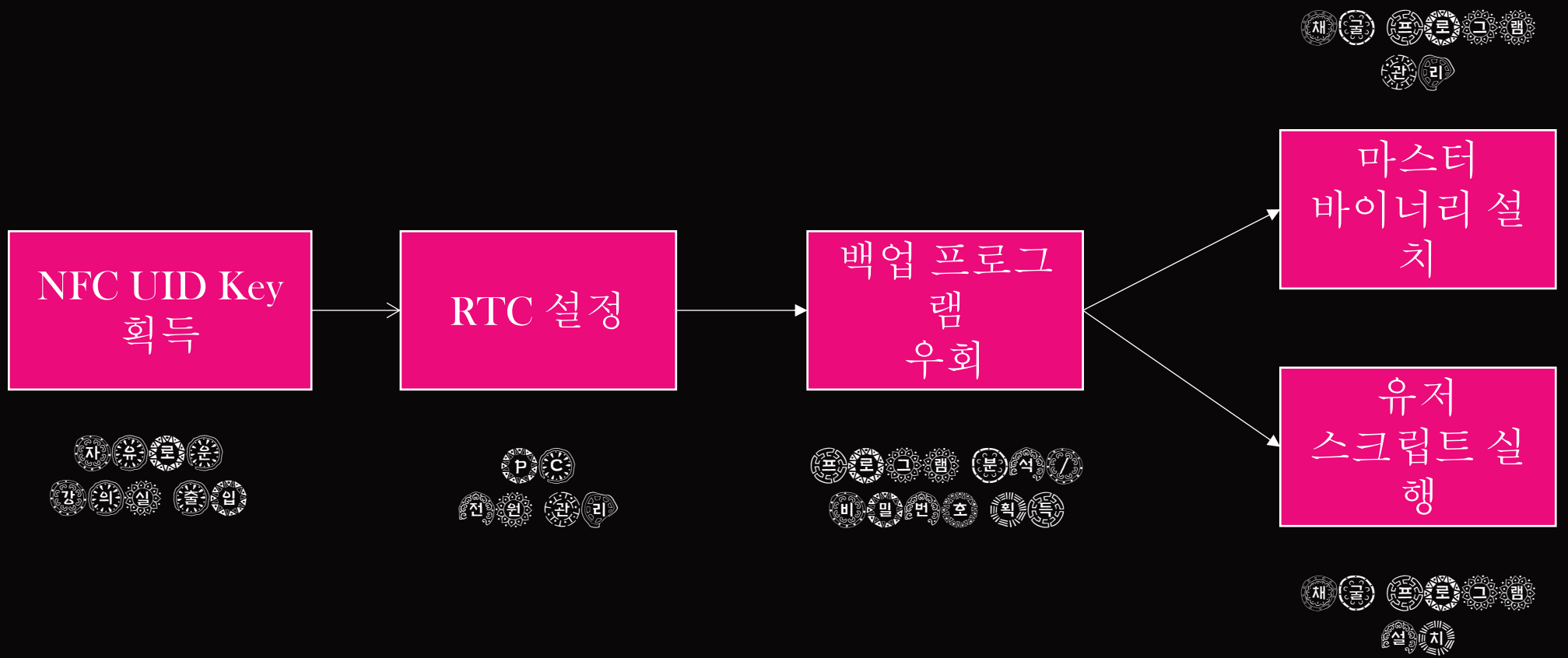
* i5 3330 hastrate = 0.2 KH/S (강의실에 설치 되어있는 일반적인 PC)

180 KH/S	1 XMR	(24 Hours)	13만원
18 KH/S	0.1 XMR	(24 Hours)	1만 3천 원
18 KH/S	0.05 XMR	(12 Hours)	6천 5백 원

x90

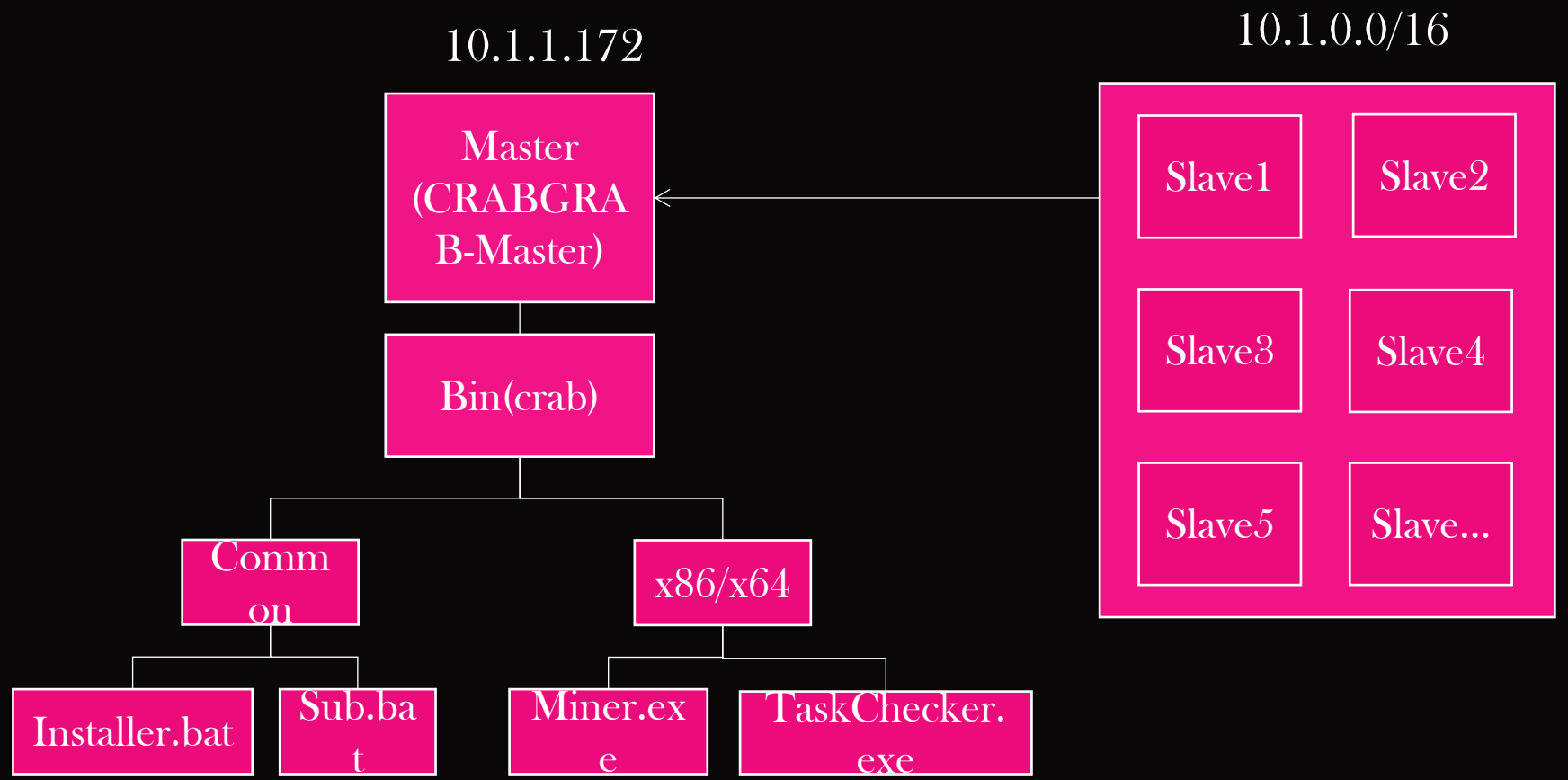
=> i5 PC에 90대를 설치하면 하루에 6,500원, 한 달(30일) 195,000원을 벌 수 있습니다

[1] Scenario

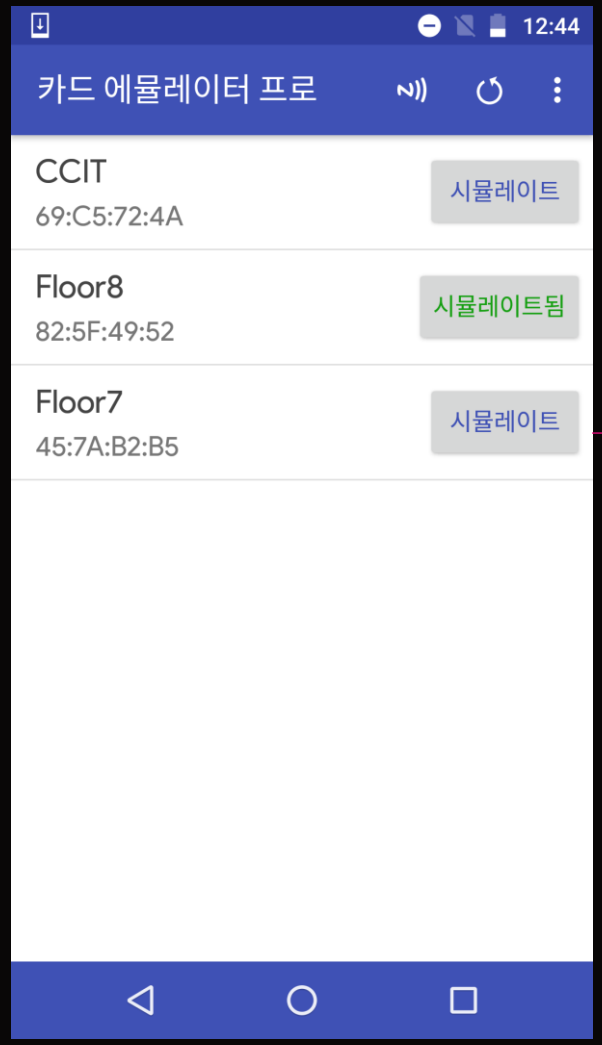

NFC UID Key 획득
RTC 설정
백업 프로그램 우회
마스터 바이너리 설치
유저 스크립트 실행
채굴 프로그램 관리
자유로운 강의실 출입
PC 전원 관리
프로그램 분석 / 비밀번호 획득
채굴 프로그램 설치

[1] Scenario_마스터 바이너리 구조

XMR은 ASIC(최적화된 채굴용 머신)를 대비하여 잦은 하드포크를 합니다.
하드포크 이후에는 채굴 알고리즘이 바뀌게 되는데 이에 따라 채굴 프로그램도 업데이트 하여야 합니



[2] NFC UID Cloning — Card Emulat



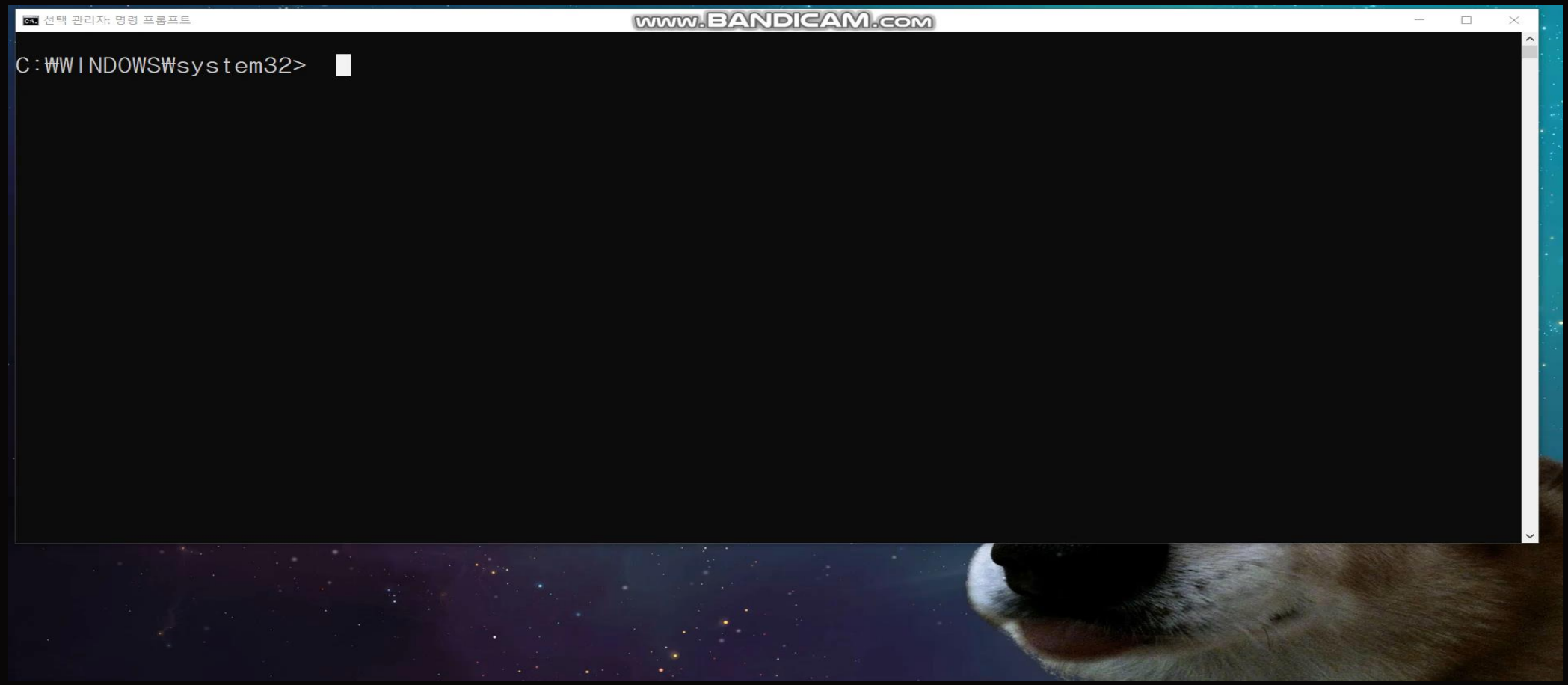
- 현재 학교는 NFC Mifare Classic 1k 버전을 사용 하고 있음.
- 유명한 컨퍼런스(BlackHat, HITCON등)에서 많이 발표 되었음.
- 휴대폰에 내장된 NFC 칩의 UID를 바꿀 수 있는 어플리케이션 존재 (Thx. 정재훈)

Supported Phones (with stock ROM)
Xiaomi, Huawei, OnePlus, Sony, Samsung (S4, S5, Note3), Google Phone (Nexus and Pixel)
, Meizu, LG, HTC, Nubia, Letv, Moto, Lenvo and maybe more?

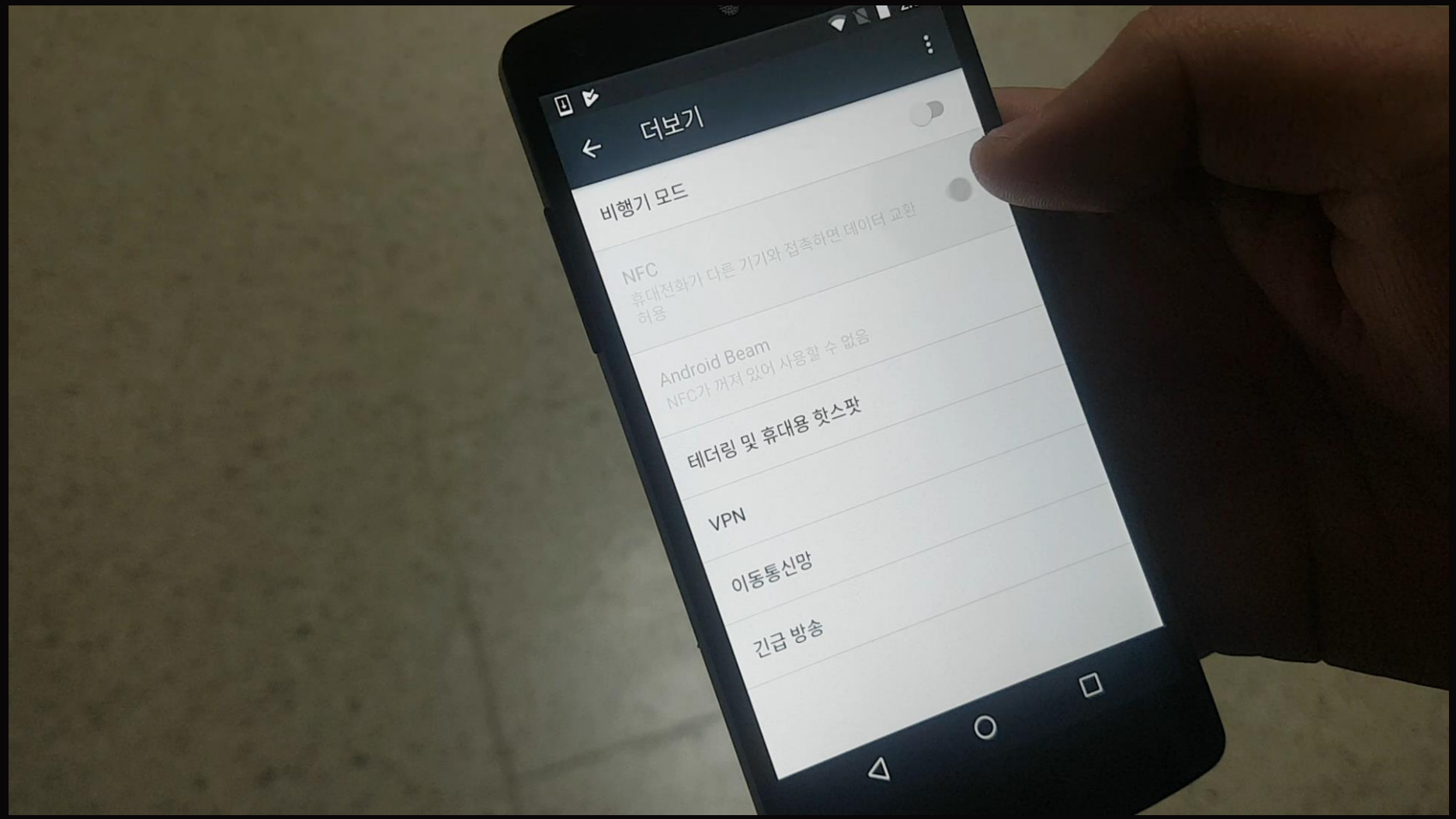
Unsupported Phones
Samsung S6, S6 edge, S7, S7 edge, S8, S8+ and above.
NOTE: Some unsupported phone DO work with a custom ROM such as Aurora or LineageOS.

[2] NFC UID Cloning - 어떻게 동작하는 걸까요

- etc/libnfc-brcm-13414.conf
- NFA_DM_START_UP_CFG = { LENGTH:BL:AH:BL:AH:33:04:82:5F:49:52 }



[2] NFC UID Cloning



[2] NFC UID Cloning

- 그렇다면 UID는 어떻게 얻을 수 있을까요?

HackRF 13.56Mhz Recording

USB RFID Reader

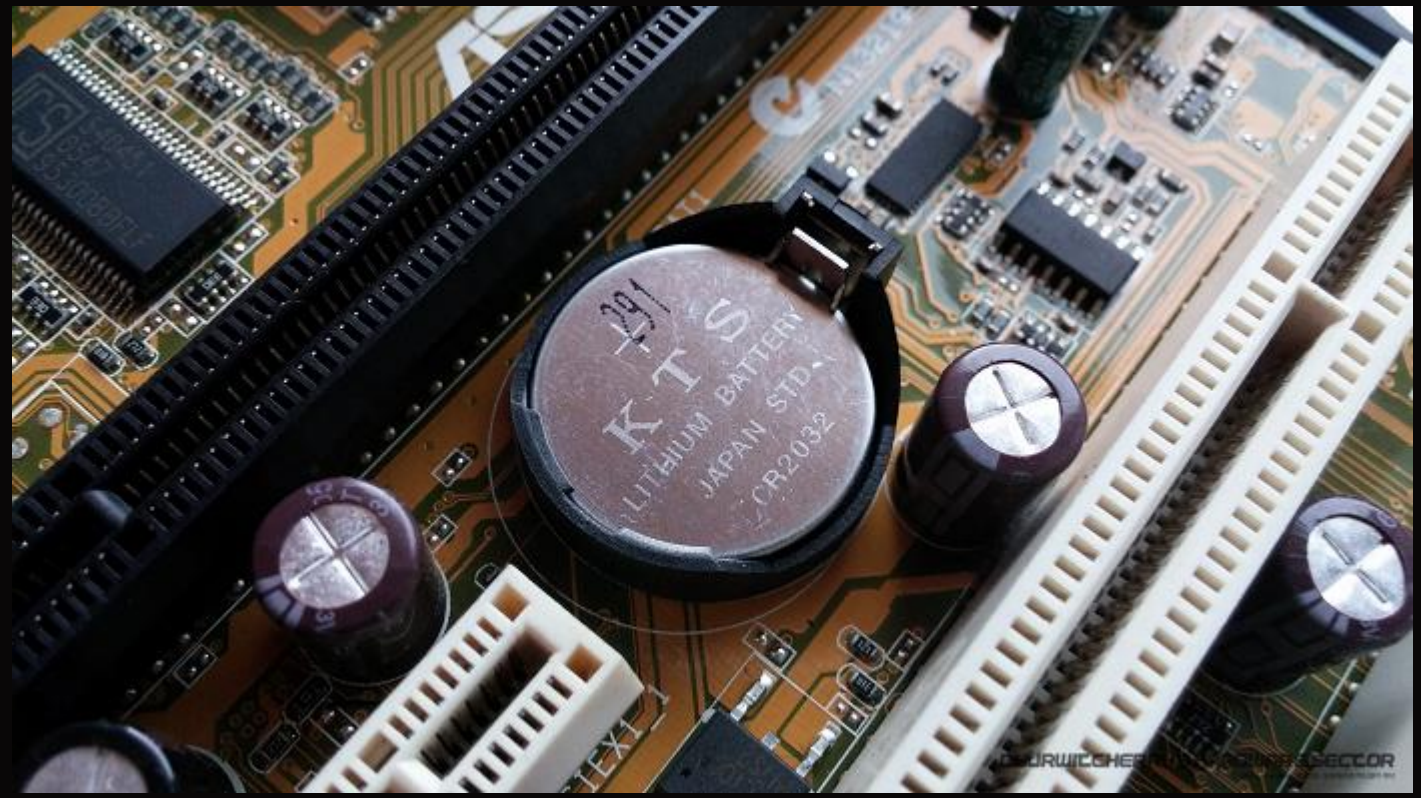
[2] NFC UID Cloning

- HackRF 13.56Mhz Recording and Decoding
  - Replay는 불가
  - NFC 스펙상 최대거리가 10~15cm이라 리더기와 벽 사이를 잡아 낼 수 없음

- Reader
  - 리더기 뒤에 비어 있는 공간, 혹은 옆에 리더기를 설치하여 획득

[3] Automation - RTC Alarm

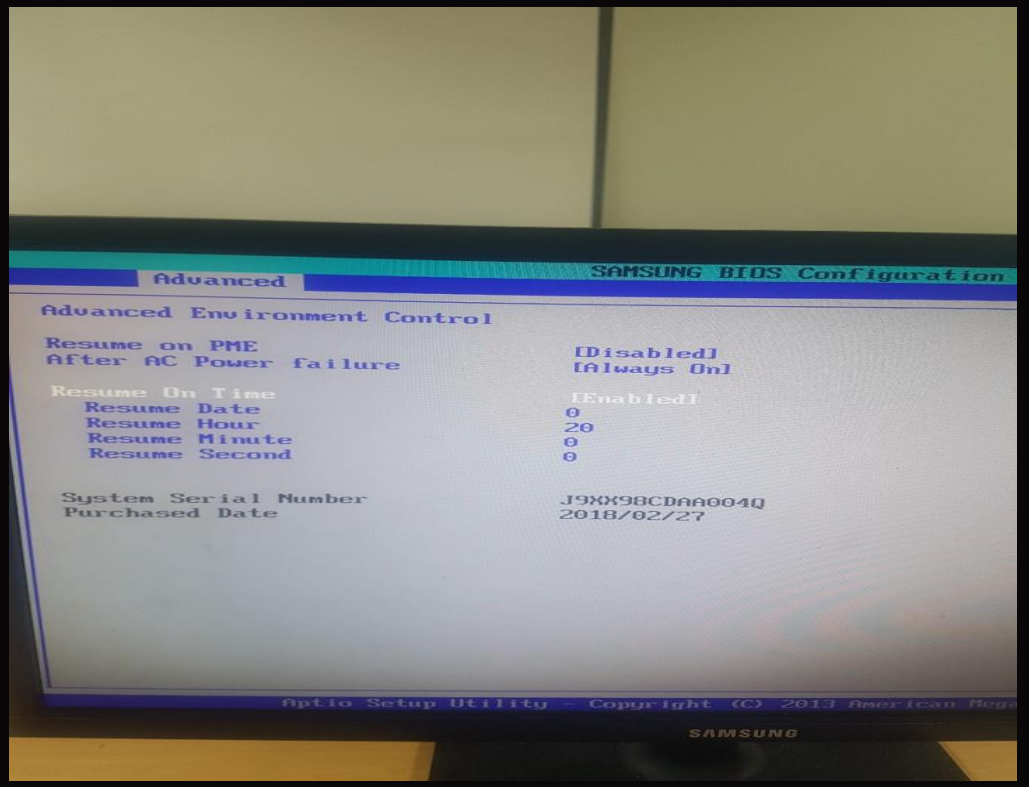
- 메인보드에서 지원하는 RTC(RealTimeClock) Alarm을 사용



[3] RTC Alarm 설정 방법

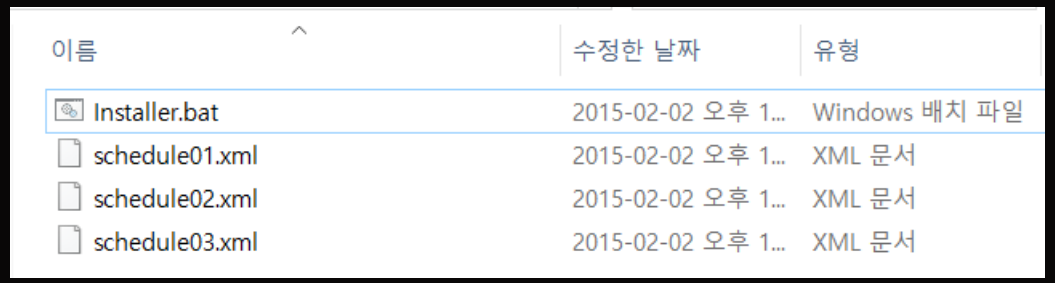
(*_*)

제조사 메인보드마다 방법이 살짝 틀리다



[3] Automation – 작업 스케줄러

- 등록 요소 : 프로그램 시작 및 컴퓨터 종료
- 등록 방법 : 배치 스크립트로 시간과 조건이 설정된 XML 파일을 스케줄러로 로딩



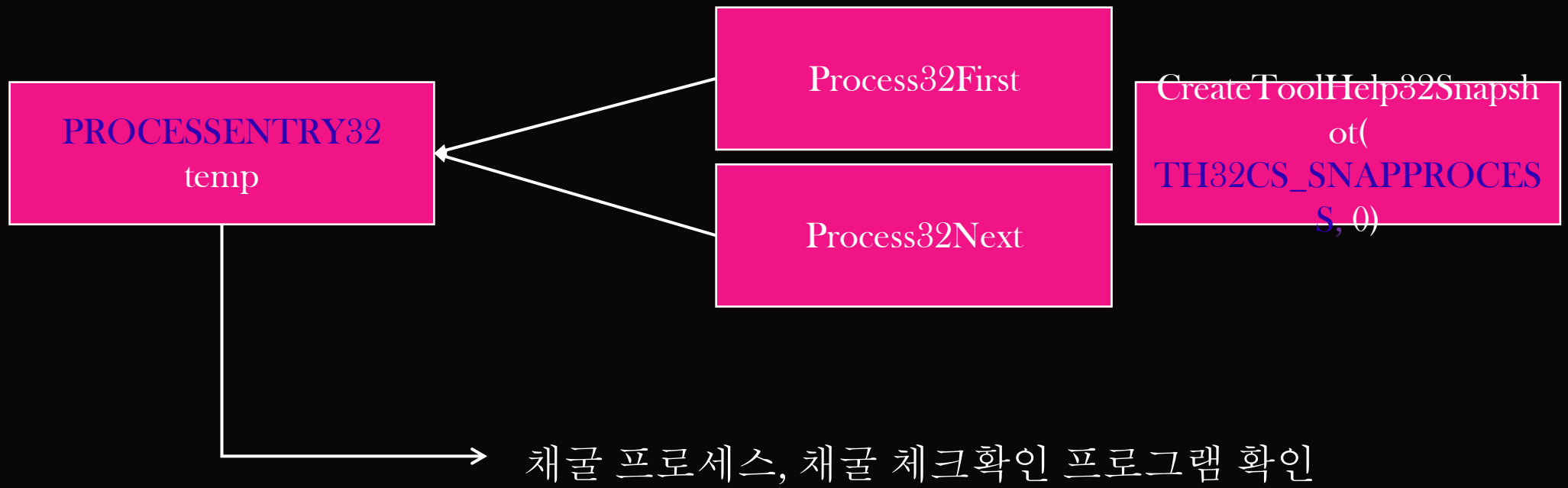
SCHTASKS /Create /TN schedule_pc_on /XML \\PC_NAME\crab\common\CPU_N_Installer\schedule01.xml

SCHTASKS /Create /TN schedule_pc_off /XML \\PC_NAME\crab\common\CPU_N_Installer\schedule02.xml

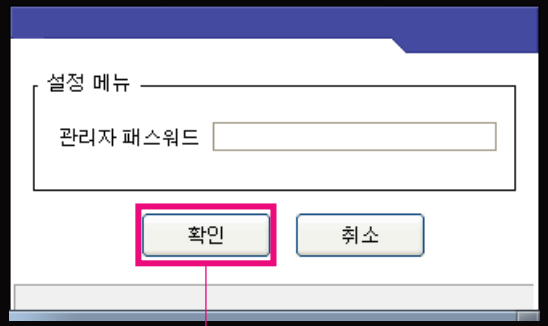
SCHTASKS /Create /TN schedule_fastboot_disable /XML \\PC_NAME\crab\common\CPU_N_Installer\schedul

[4] 작업관리자 모니터링 / 마우스 좌표 모니터링

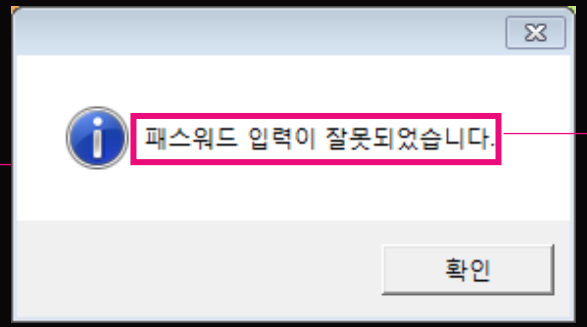
- TaskMgr 프로세스 확인 시 감시 프로그램과 채굴 프로그램 종료
- TlHelp32 Library 사용
- GetCursorPos API로 처음 좌표 변화 감지



[5] 백업 프로그램 우회



Good Result

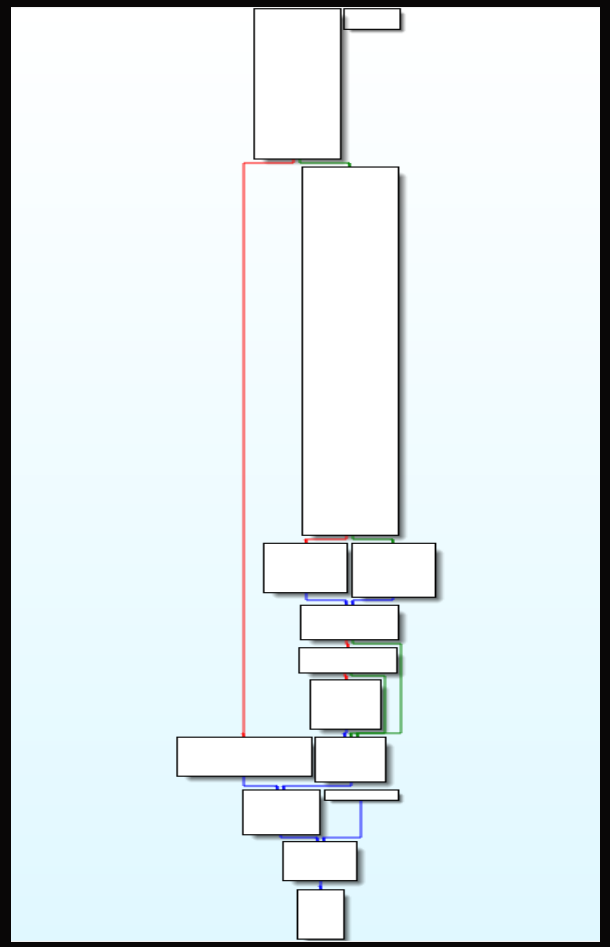


Encoding Type: EUC-KR

\xC6\xD0\xBD\xBA\xBF\xF6
\xB5\xE5\x20\xC0\xD4\xB7
\xC2\xC0\xCC

[5] 백업 프로그램 우회 (1)

- GRAPH VIEW -



```
0050F1B0  C6 D0 BD BA BF F6 B5 E5  20 C0 D4 B7 C2 C0 CC 20   패·스·워·드··입·력·이··
0050F1C0  C0 DF B8 F8 B5 C7 BE FA  BD C0 B4 CF B4 D9 2E 00   잘·못·되·었·습·니·다···
0050F1D0  FF FF FF FF 01 00 00 00  31 00 00 00 FF FF FF FF   ........1.......
```

```
; Attributes: bp-based frame

sub_50EF1C proc near

var_8= dword ptr -8
var_4= dword ptr -4

push    ebp
mov     ebp, esp
push    0
push    0
push    ebx
mov     ebx, eax
xor     eax, eax
push    ebp
push    offset loc_50F186
push    dword ptr fs:[eax]
mov     fs:[eax], esp
lea     edx, [ebp+var_8]
mov     eax, [ebx+344h]
call    sub_45C888
mov     eax, [ebp+var_8]
lea     edx, [ebp+var_4]
call    sub_408950
mov     edx, [ebp+var_4]
mov     eax, [ebx+3B8h]
call    sub_404694
jz      short loc_50EF7A
```

→ No Obfuscation

MessageBox Call

```
push    40h                 ; uType
mov     ecx, offset dword_50F194 ; lpCaption
mov     edx, offset dword_50F1B0 ; lpText
mov     eax, ds:off_51A2D4
mov     eax, [eax]
call    sub_47C7F4
jmp     loc_50F168
```

[5] 백업 프로그램 우회 (2)

#DEMO — 815

#Result

잔고

코인	일반 지갑	환전용 지갑	환전 중	
Monero	0.97653240	0	0	지갑 관리

모네로/Monero (XMR)

₩61,974 -8.3%
0.01439275 BTC -0.80%

KRW | 구매 / 판매 | Crypto Loan | Wallet

웹사이트 getmonero.org
탐험가 monerovision.com moneroblocks.info
커뮤니티 Reddit Twitter Facebook forum.getmonero.org bitcointalk.org
소스 코드 Github
Tags Privacy Coins

시가총액 (순위 #11)
₩1,028,983,306,084

24 Hour Trading Vol
₩88,665,780,116

24h Low / 24h High
₩61,795 / ₩69,386

Available Supply
16,617,596 / 18,400,000

XMR	0.9765324	⇄	KRW	60519.27717126

#Result

- 특정 IP에 대한 트래픽 증가 여부 확인
- 강의실 컴퓨터에 대한 관리/관리 솔루션 필요
- 여러 마이닝 풀에서 사용하는 포트 차단

Q a