Public PC Guard

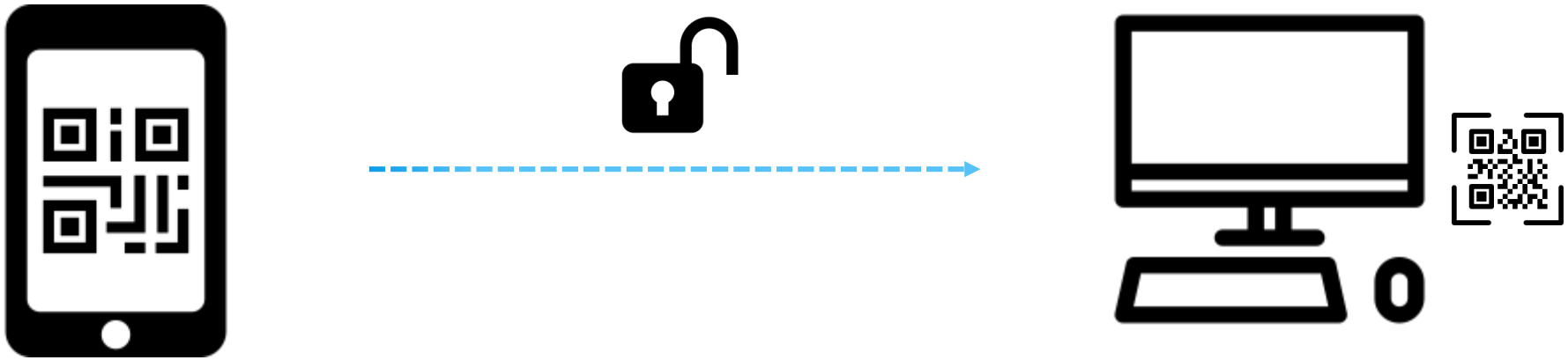
Team 4. GeonRyun Lee JaeKyung You KyungTae Kang
Yerim Chu WooJoo You

Index

Public PC Guard

1. Outline of Task

1. Outline of Task

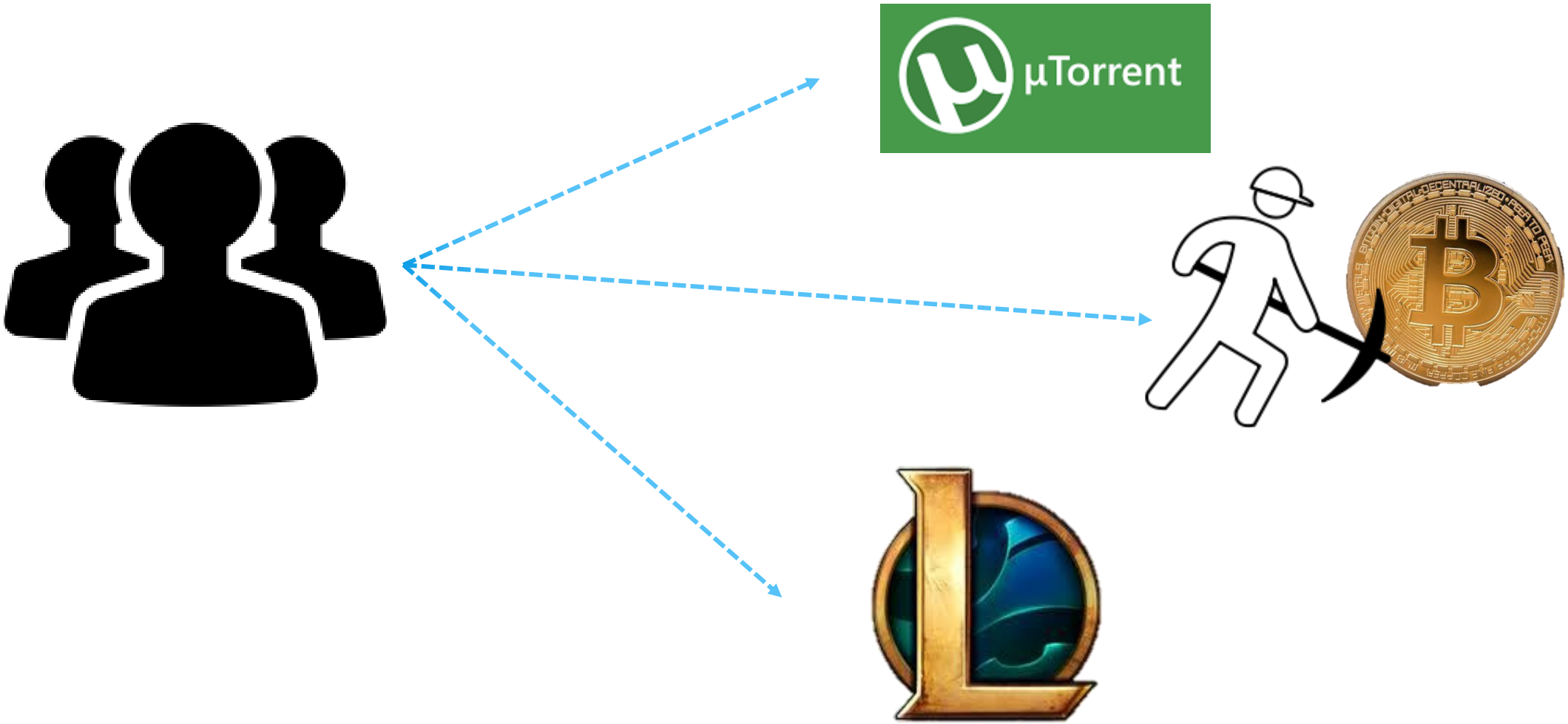


Public PC Guard

2. The Necessity and Expected Effect of Task

2. The Necessity and Expected Effect of Task

1) The Present Condition of Existing Technologies, Problems and Improvement Measures



2. The Necessity and Expected Effect of Task

1) The Present Condition of Existing Technologies, Problems and Improvement Measures

Who Are You?

2. The Necessity and Expected Effect of Task

2) Expected effects due to task development or production

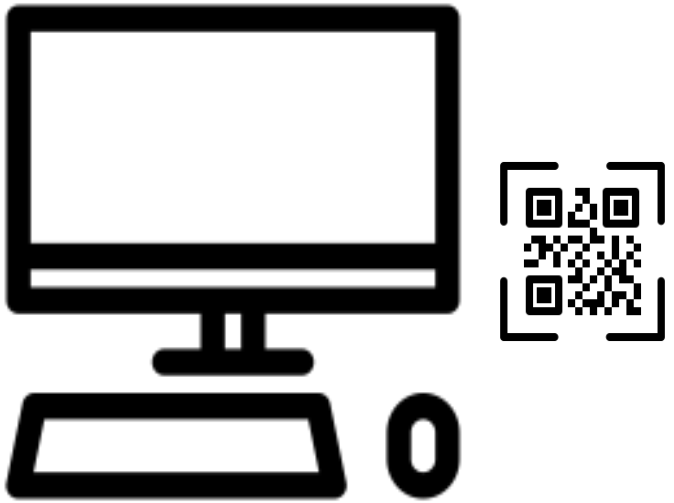
Public PC Guard

3. Task goals and content

3. Task goals and content

1-1) PC users

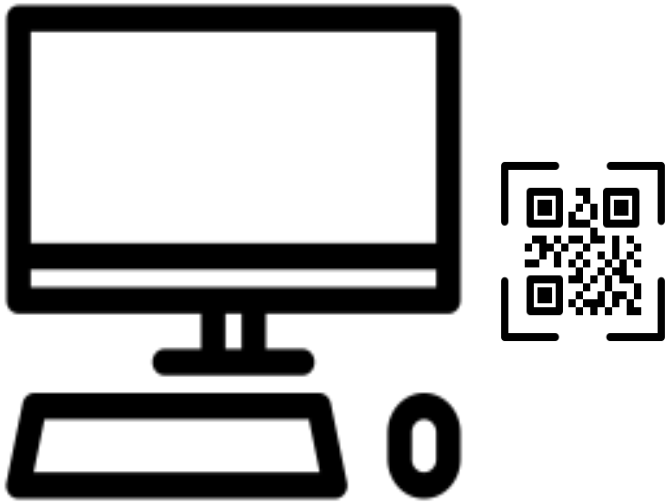
Only Authorized Users



Public PC

3. Task goals and content

1-2) Manage by collecting PC logs



Public PC

Index	Process	Start_proc
0	Chorme.exe	2019.04.18 132005
1	Cmd.exe	2019.04.18 135540

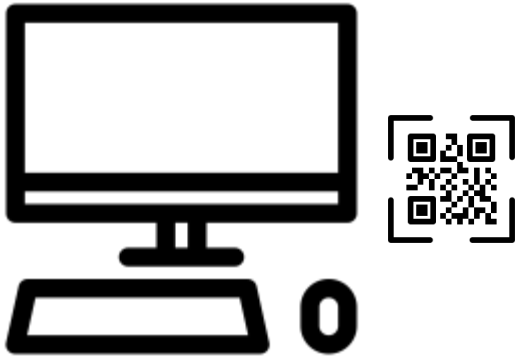
Log table

3. Task goals and content

2-1) Smart Application

1. User Authentification

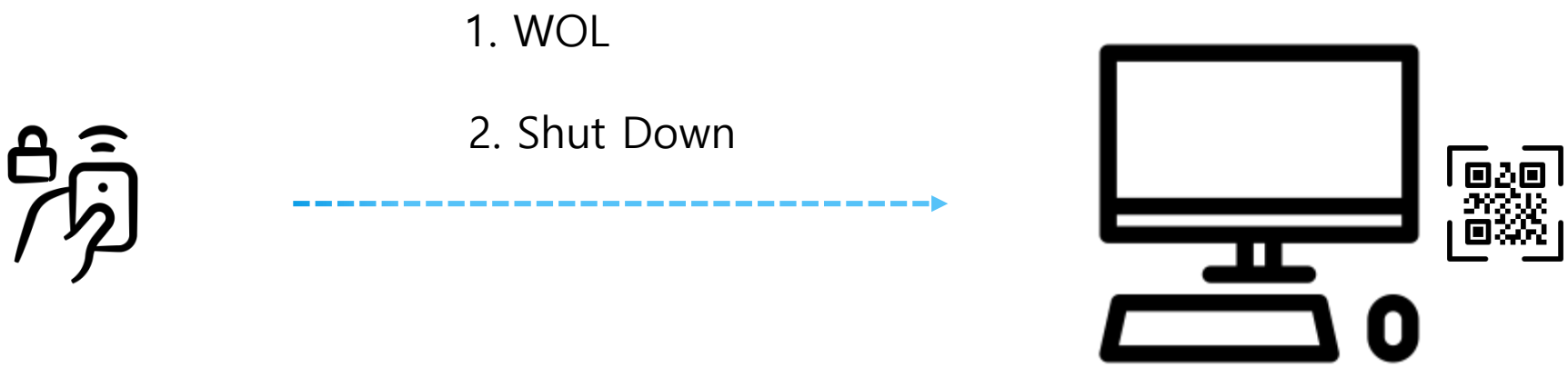
2. PC Information



We will check your identity through smart phone application.

3. Task goals and content

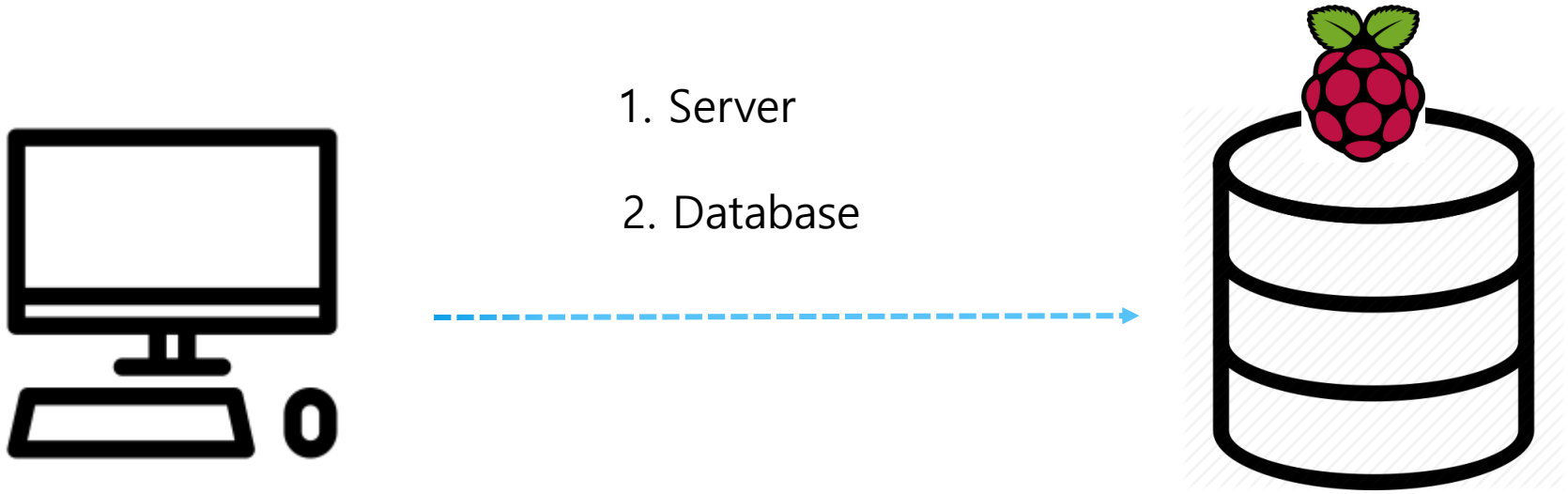
2-2) PC Remote control



The PC in the public pc room can be remotely booted and the user can shut down the system if the pc is terminated.

3. Task goals and content

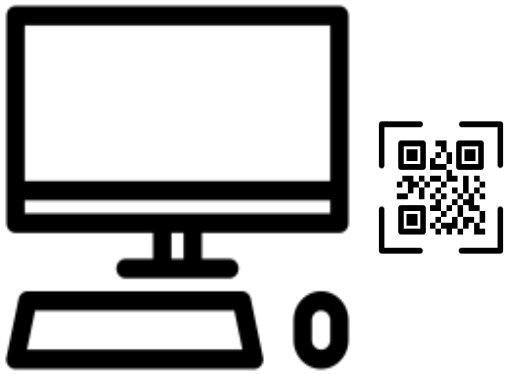
2-3) Raspberry Pi



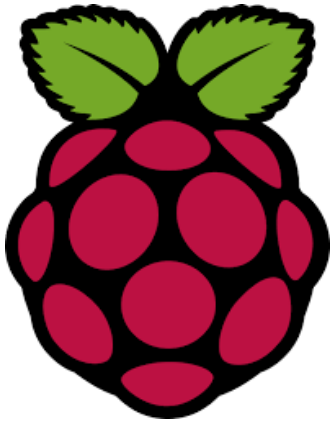
Applications will be installed on each PC to collect users' PC logs and send them to Raspberry Pi.

3. Task goals and content

2-4) Manage Logs

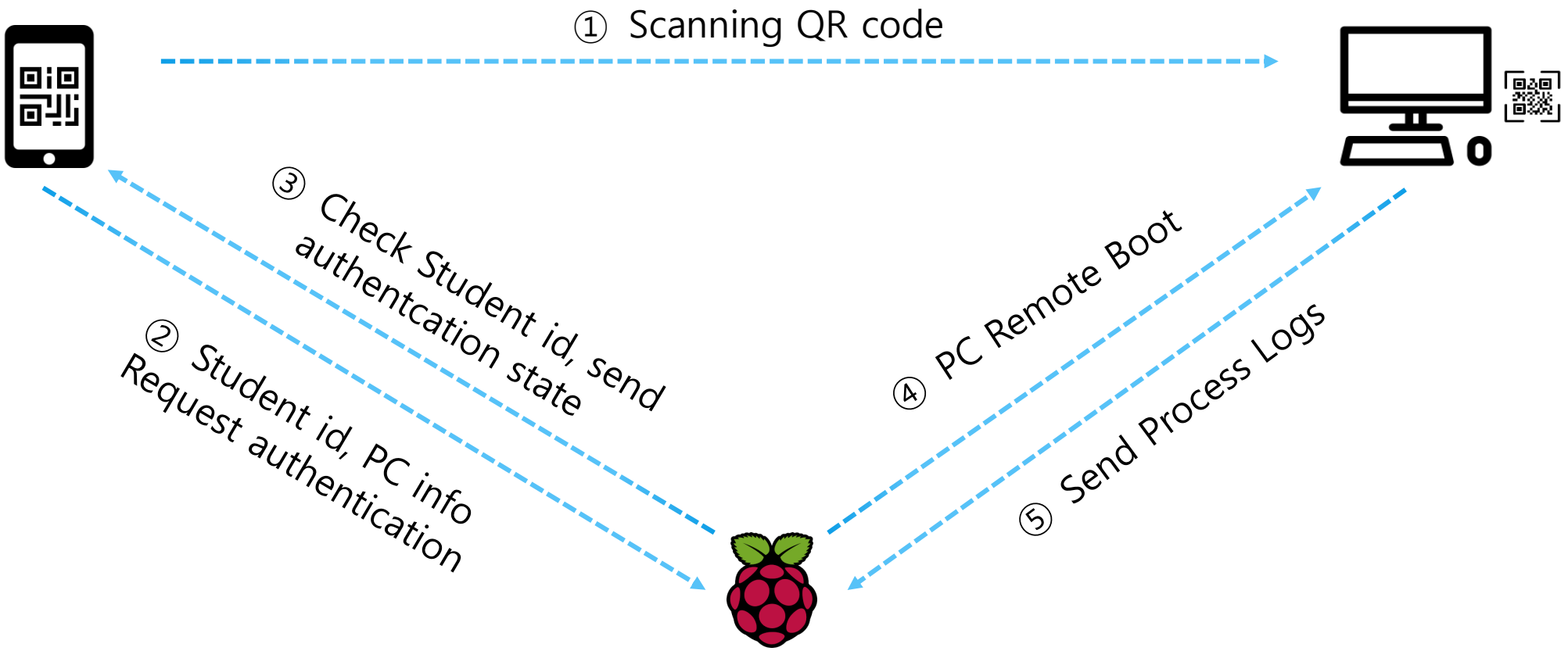


Transport Logs



3. Task goals and content

3) Summary

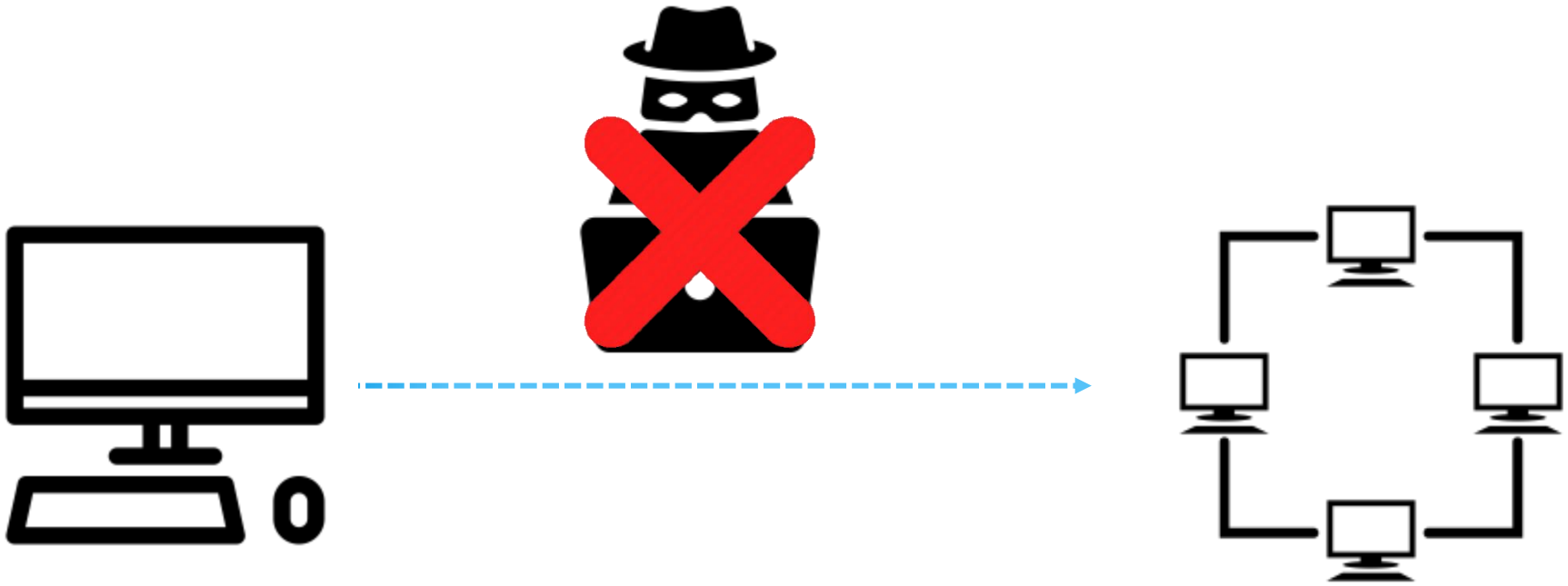


Public PC Guard

4. How to Perform a Task

4. How to Perform a Task

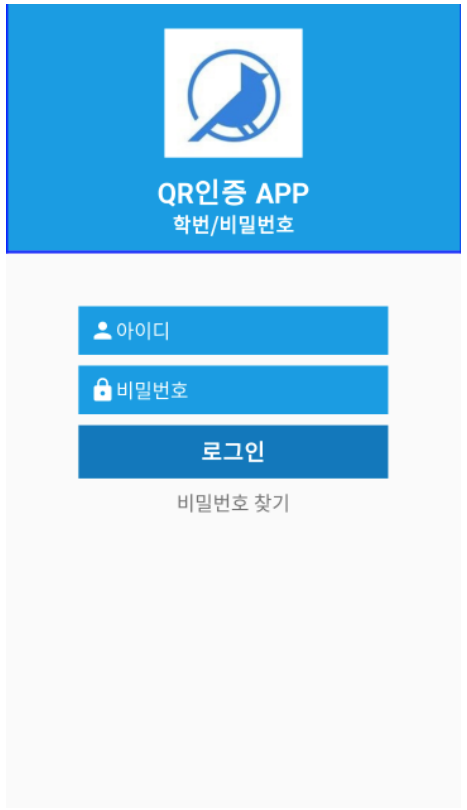
1) Task Performance



Prevents the user from using the PC indiscreetly.

4. How to Perform a Task

2-1) Detail - Application



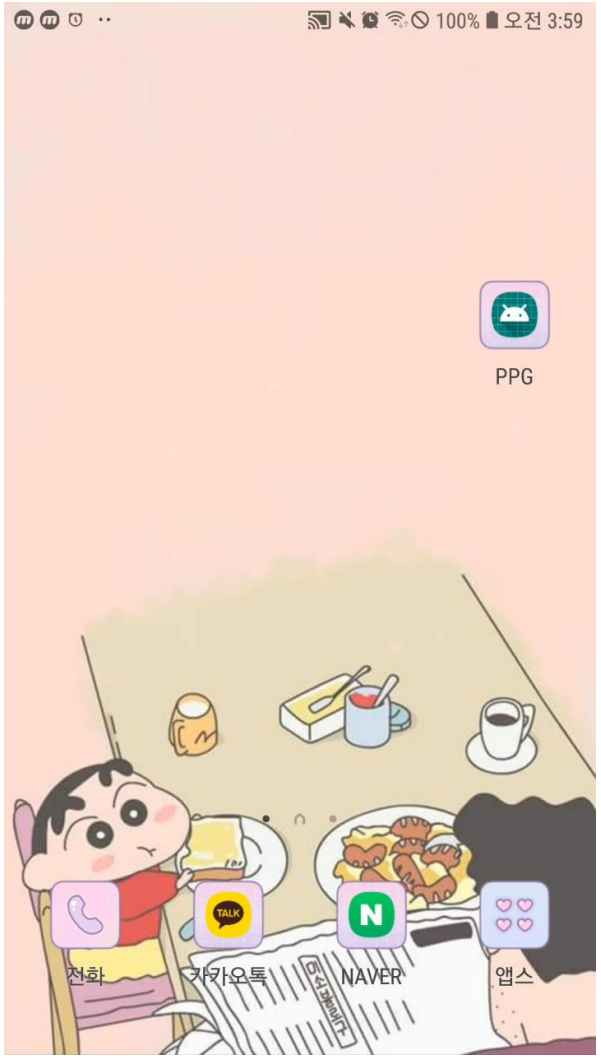
Log-in

Scanning QR code

PC Information

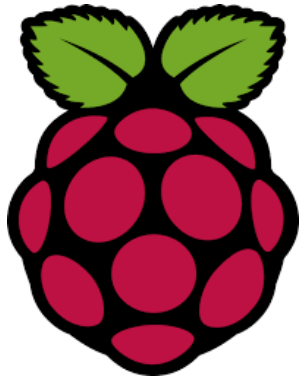
4. How to Perform a Task

2-1) Detail - Application

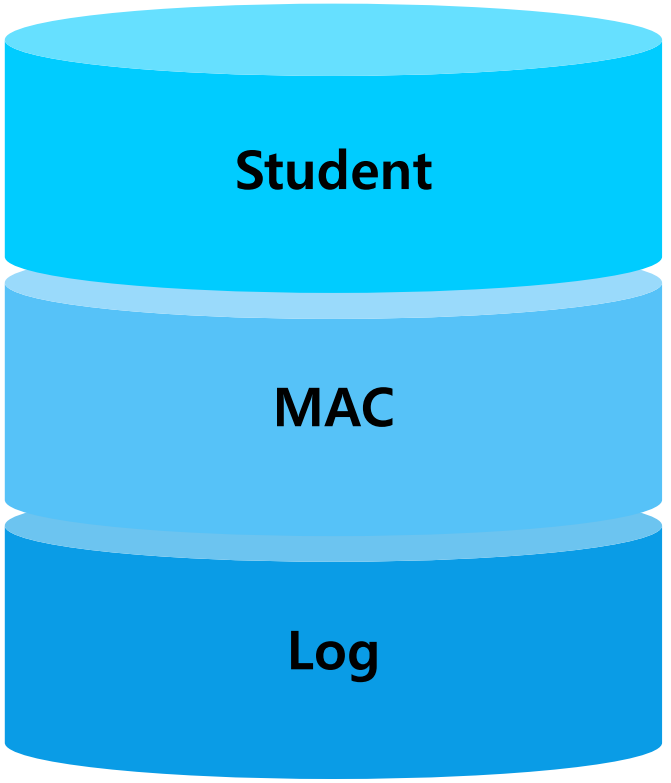


4. How to Perform a Task

2-2) Detail – Raspberry Pi

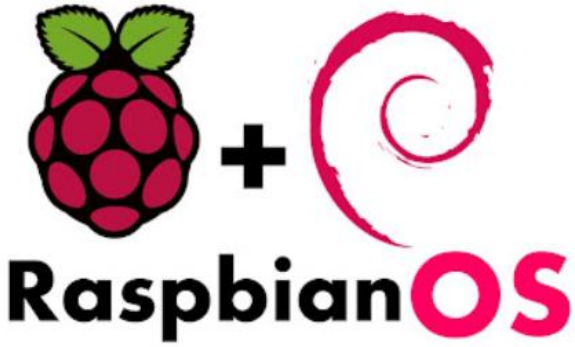


Store



4. How to Perform a Task

2-2) Detail – Raspberry Pi

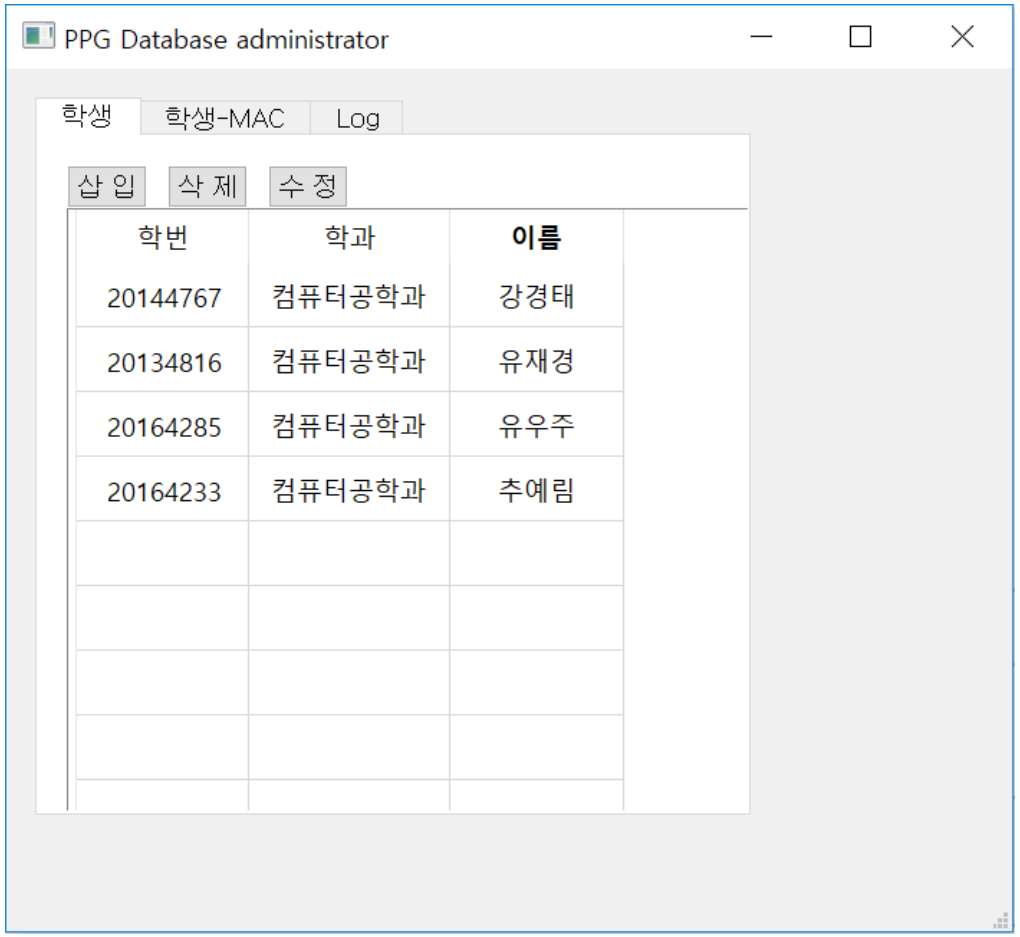


Raspbian install

Structure web server - Apache, MySQL, PHP

4. How to Perform a Task

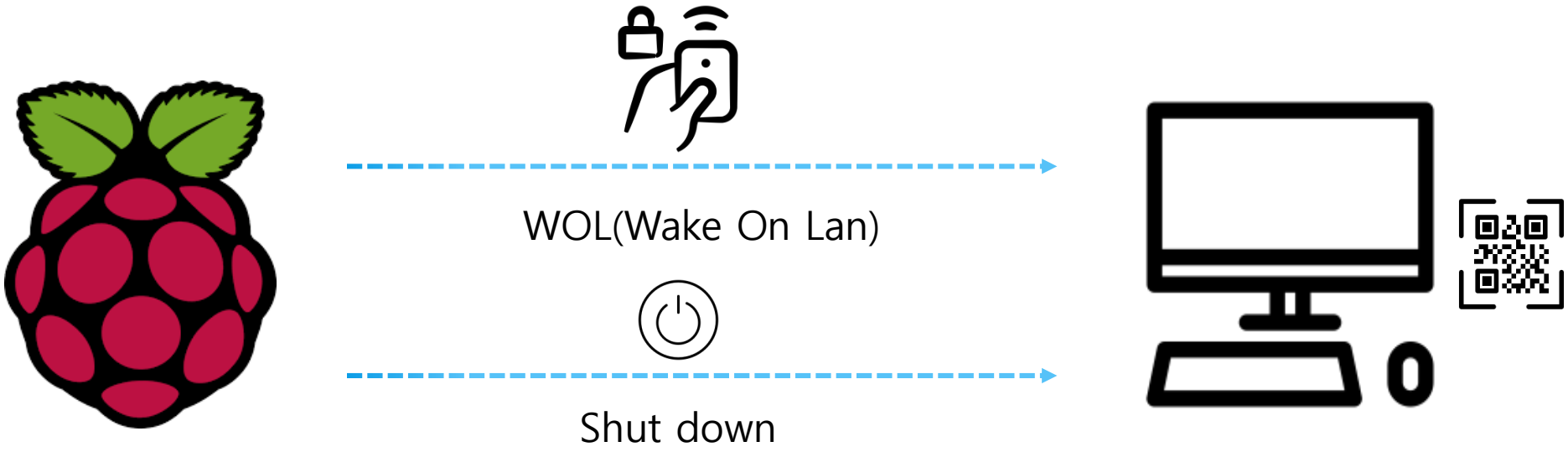
2-2) Detail – Raspberry Pi



[PPG Database administrator]

4. How to Perform a Task

2-3) Detail – PC Remote control

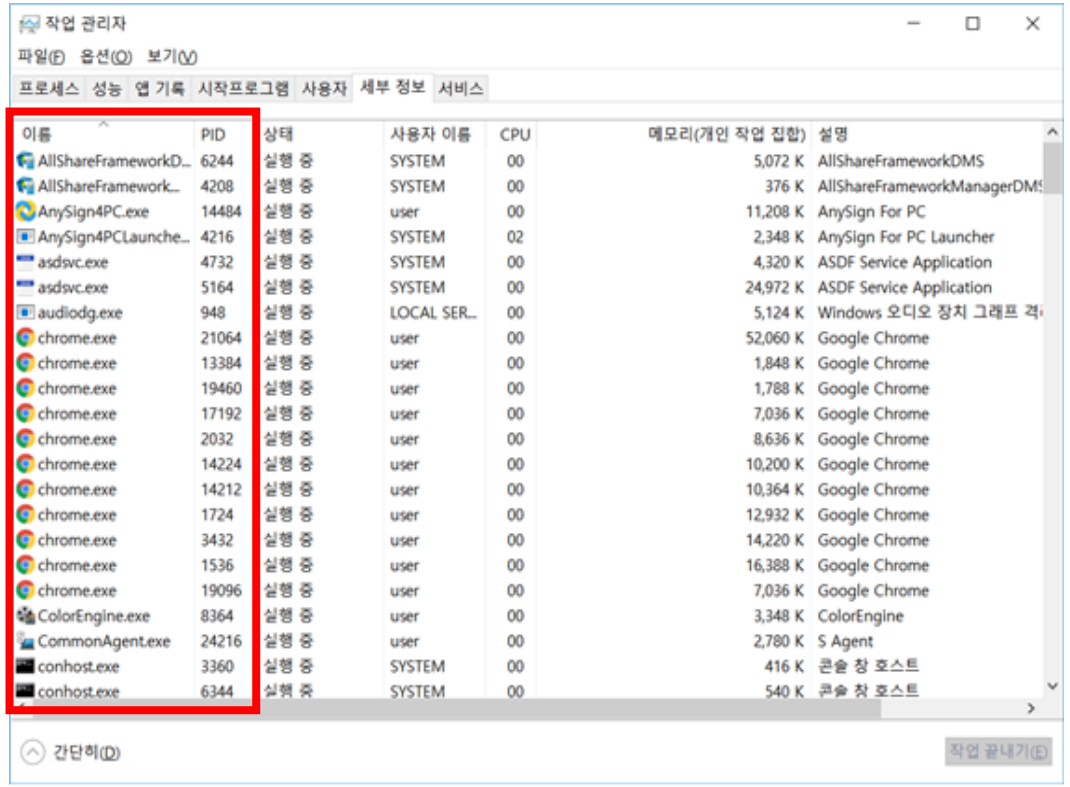


4. How to Perform a Task

2-3) Detail – PC Remote control

4. How to Perform a Task

2-4) Detail – PC Logs




```
C:₩Users₩user>tasklist

이미지 이름                     PID 세션 이름              세션#    메모리 사용
========================= ======== ================ =========== ============
System Idle Process               0 Services                   0          8 K
System                            4 Services                   0        148 K
Registry                         96 Services                   0     21,944 K
smss.exe                        376 Services                   0      1,000 K
csrss.exe                       544 Services                   0      4,304 K
wininit.exe                     636 Services                   0      4,944 K
csrss.exe                       644 Console                    1      5,632 K
services.exe                    716 Services                   0     12,360 K
lsass.exe                       736 Services                   0     15,832 K
svchost.exe                     844 Services                   0      3,056 K
₩UDFHost.exe                    868 Services                   0     11,144 K
svchost.exe                     876 Services                   0     27,444 K
fontdrvhost.exe                 912 Services                   0      2,488 K
svchost.exe                    1016 Services                   0     15,684 K
svchost.exe                     404 Services                   0      7,136 K
```

4. How to Perform a Task

2-4) Detail – PC Logs

```
def tasklist():
    wmic = subprocess.check_output('wmic path win32_process get caption,creationdate', shell=True) #process 시작시간 저장
    wmic = wmic.decode('euc-kr')

    return wmic
```

```
wmic = tasklist()

if re.findall(r'\w+.exe\b', wmic):      #.exe로 끝나는 모든 string을 저장, set() = 중복제거
    process_name = re.findall(r'\w+.exe', wmic)
    start_proc = re.findall(r'2019\w\w\w\w+\w\w\w\w\w\w', wmic)        #2019년도로 시작하는 문자열 검색

for i in range (0, len(process_name)):       #DB에 저장될 컨텐츠
    print("Index : " , i ,
        "MAC : " , arrinfo[2] ,
        "proc_name : " ,process_name[i] ,
        "start_proc : " ,start_proc[i])
```

4. How to Perform a Task

2-4) Detail – PC Logs

```
import subprocess, os, sys
import re

def getMacAddress():    #ipconfig에서 mac주소를 가져오는 함수
    arrinfo = {}
    isdevice = 0
    mk = 0
    if sys.platform == 'win32':
        for line in os.popen("ipconfig /all"):
            if line.lstrip().startswith('호스트'):
                host = line.split(':')[1].strip()
                arrinfo["host"] = host
            else:
                if line.lstrip().startswith('터널'):
                    isdevice = 0
                if line.lstrip().startswith('이더넷'):
                    isdevice = 1
                if line.lstrip().startswith('무선'):
                    isdevice = 1
                if isdevice == 1:
                    if line.lstrip().startswith('미디어 상태'):
                        desc = line.split(':')[1].strip()
                        if desc == '미디어 연결 끊김':
                            isdevice = 0
                    if line.lstrip().startswith('물리적'):
                        mac = line.split(':')[1].strip() #.replace('-',':')
                        arrinfo[mk] = mac
                        isdevice = 0
                        mk += 1
    return arrinfo
```

Output

```
Host : DESKTOP-6H67F89
MAC 1 : 00-50-56-C0-00-01
MAC 2 : 00-50-56-C0-00-08
MAC 3 : 00-C2-C6-D1-6F-37
```

4. How to Perform a Task

2-4) Detail – PC Logs

Output

```
Caption                          CreationDate
System Idle Process              20190416160553.816712+540
System                           20190416160553.816712+540
Registry                         20190416160551.552344+540
smss.exe                         20190416160553.824067+540
csrss.exe                        20190416160556.203471+540
```

```
Index :  0 MAC :  00-C2-C6-D1-6F-37 proc_name :  smss.exe start_proc :  20190416160553
Index :  1 MAC :  00-C2-C6-D1-6F-37 proc_name :  csrss.exe start_proc :  20190416160553
Index :  2 MAC :  00-C2-C6-D1-6F-37 proc_name :  wininit.exe start_proc :  20190416160551
Index :  3 MAC :  00-C2-C6-D1-6F-37 proc_name :  csrss.exe start_proc :  20190416160553
Index :  4 MAC :  00-C2-C6-D1-6F-37 proc_name :  winlogon.exe start_proc :  20190416160556
Index :  5 MAC :  00-C2-C6-D1-6F-37 proc_name :  services.exe start_proc :  20190416160556
```

Public PC Guard

5. Advance Schedule

5. Advance Schedule

Schedule																
	3				4				5				6			
Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Term
Idea Conference																2W
Android App Develope																4W
Raspberry Pi Server Develope																6W
Database Design																3W
PC Remote Boot / Control Application																5W
PC Log gathering and Transfer Application																5W
Synchronizing Raspberry Pie Android App / PC App																4W
Prototype Test																2W
Final Check / Presentation																2W

Public PC Guard

6. Expected effects and utilization measures

6. Expected effects and utilization measures

Effect

- Reduce administrative burden
- Use of public institutions
- An increase in student responsibility
- Application of Smart home system

Thank you for Listening!

Contact : https://github.com/chuyr/Cap4team_2019