The Ways to Hack your Cell Phones

- Cho JooBong -

http://hacker.or.kr

Contents

Introduce

- **About 40 million Cell phone users in korea (80 % of the total population)**
- **Cell Phone Services**
  - Audio/Video call
  - SMS(Short Message Service)/MMS(Multimedia Messaging Service)
  - Internet/Email
  - Game
  - Music/Video/Camera
  - GPS
  - Electronic Settlement, Electronic Authentication

- **Cell Phone Crime**
  - 대포폰, 브릿지폰, 쌍둥이폰, 박스폰, 휴대폰깡, 명의 도용 등..

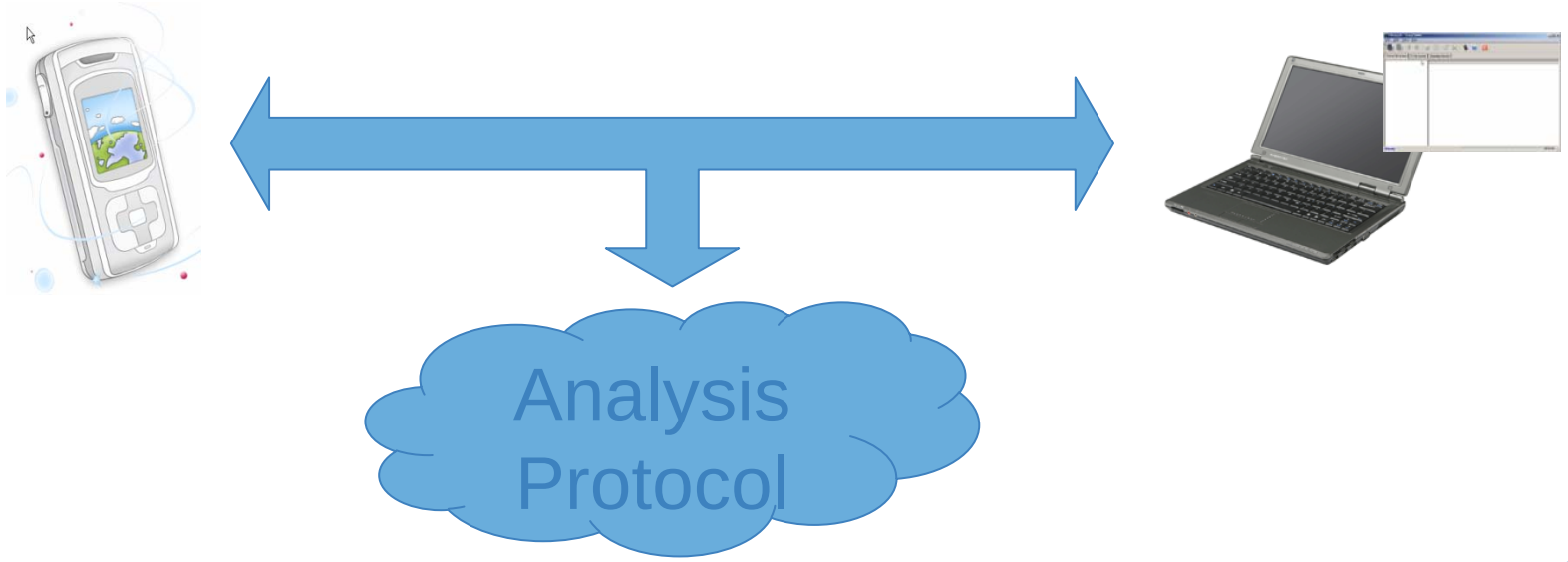
- **Mobile Phone Forensics**
  - Acquiring data from cell phones
  - Investigating cell phones

Phone Tools

- Phone Access Tools
  - QPST
  - BitPim
  - Easy CDMA
  - SIMCon
  - SIMIS
  - PhoneBase
  - MobileEdit

Protocol Analysis

- USB Device Monitoring Tools
  - Device Monitoring Studio
  - USBTrace
  - Advanced Serial Port Monitor



Protocol

- Protocol
  - BREW Protocol
    - BITPIM/QPST
  - EASY CDMA PROTOCOL
    - EASYCDMA
- What kind of operation is available on cell phones?
  - Accessing Cell phone’s embedded File System
  - Downloading/Uploading FILE List
  - Acquiring cell Phone information

Modem Protocol

Request	Response
ATQ0V1E0	Initializing Query
AT+GMM	Model ID. ITU-T V.250 recommendation can’t be applied for all models
AT+FCLASS=?	Available for only FAX class supporting modems
AT#CLS=?	Present whether the modem supports Rockwell voice command set
ATIn	Manufacturer information for n(1 ~ 7). Including port speed, testing result value, model information. Refer to the product specification
AT+GCI?	Country & region
AT+GCI=?	Countries and regions that supported by the modem

Root Directory Request/Response

Request

59	0A	02	00	00	00
brew command prefix	directory listing	index		dummy	
01	00	20	E9	7E	
directorypath length	directory pathname + null	crc Check value		brew terminator	

Response

59	0A	00	02	00	00	00
command prefix	directory listing	ok	index		dummy	

05	00	01	00	F4	F8	05	01	00	00	00	00	00
unknown												

00	00	00	00	00	05	4D	6F	76	69	65
unknown					length	M	o	v	i	e

A0	C0	7E	
crc		terminator	

File List Request/Response

Request

59		0B		02	00	00	00
command prefix		file listing		index		dummy	
14		56	6F	69	63	65	44	42
pathlength		V	o	i	c	e	D	B
2F	4C	61	6E	67	2F	4B	6F	72
/	L	a	n	g	/	K	o	r
65	61	6E	00	9C	3C	7E		
e	a	n	null	crc		terminator		

Response

59		0A		00	02	00	00	00
command prefix		directory listing		ok	index		dummy	
1F	00	00	00	00	B4	40	74	40	65	01	00
unknown				file created date/time				file size			
00	00	00	00	14		1F		56	6F
dummy				directory pathlength		fullpath length		V	o
69	63	65	44	42	2F	4C	61	6E	67	2F
i	c	e	D	B	/	L	a	n	g	/
6B	6F	72	64	61	74	31	2E	70	72	6D
k	o	r	d	a	t	1	.	p	r	m
83		EA		7E						
crc				terminator						

Request

File Open Request/Response

59	04	00	11	6E	76
command prefix	fileopen	index	fiepath length	n	v

6D	2F	73	6D	73	5F	30	32	38
m	/	s	m	s	_	0	2	8

36	00	7B	5A	7E	
6	null	crc		terminator	

59	04	01	D8	AF	7E
command prefix	file open	index	crc		terminator

Response

59	04	00	00	00	8C	00	00	00
command prefix	File open	ok	index		file size			

8C	00	1E	01	06	4F	00	0B	80	08	3E
data size	data stream									
~ 중략 ~										

0A	09	04	03	01	FE	B2	E5	7E
data stream		data/repeater				crc		terminator

Error Response

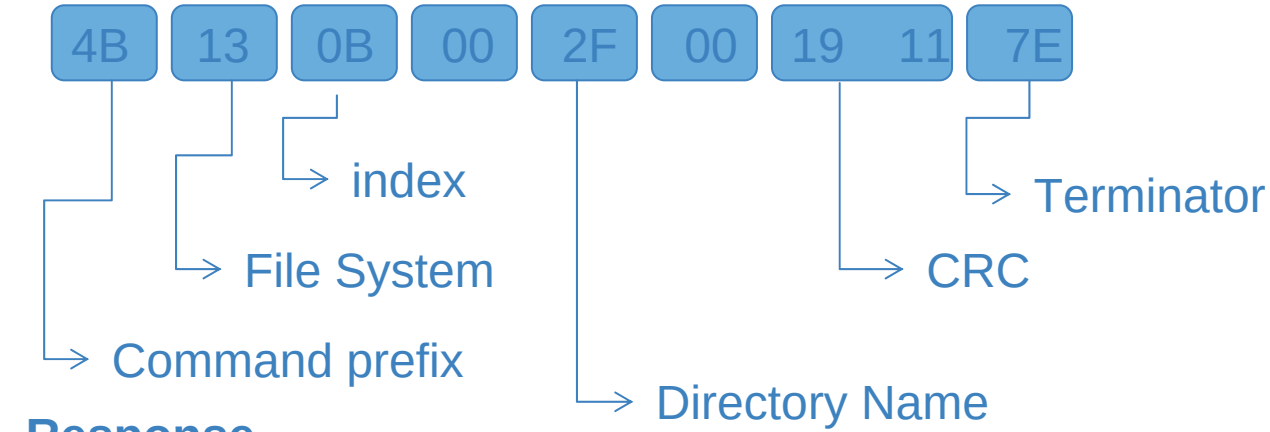
Response

59	0A[0B|04]	1C	AC	FE	7E
command prefix	command type	error signal	crc		terminator

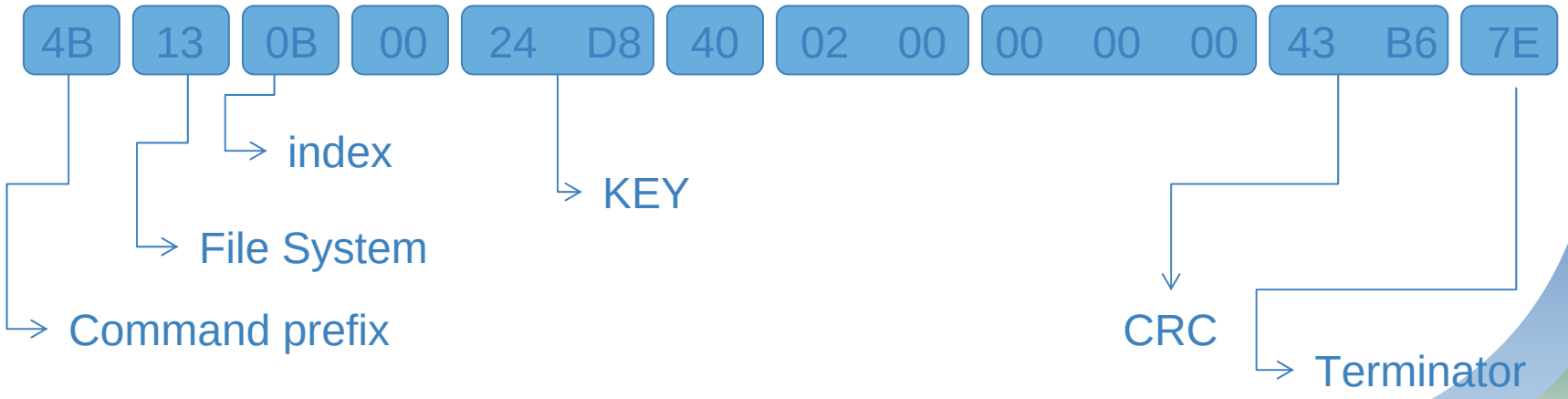
0x1C : NoMoreEntriesException
0x08 : NoSuchDirectoryException
0x06 : NoSuchFileException
0x1A : BadPathnameException
0x1B : NameTooLongException
0x07 : DirectoryExistException
0x100: CommandException
0x101: MalformedBrewCommandException
0x04 : AccessDeniedException
0x16 : FileSystemFullException

Directory Request/Response

Request

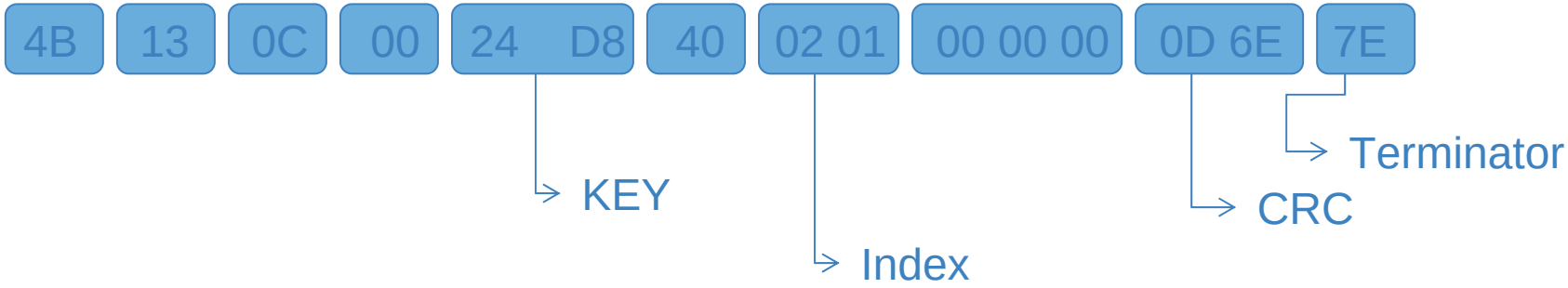


Response

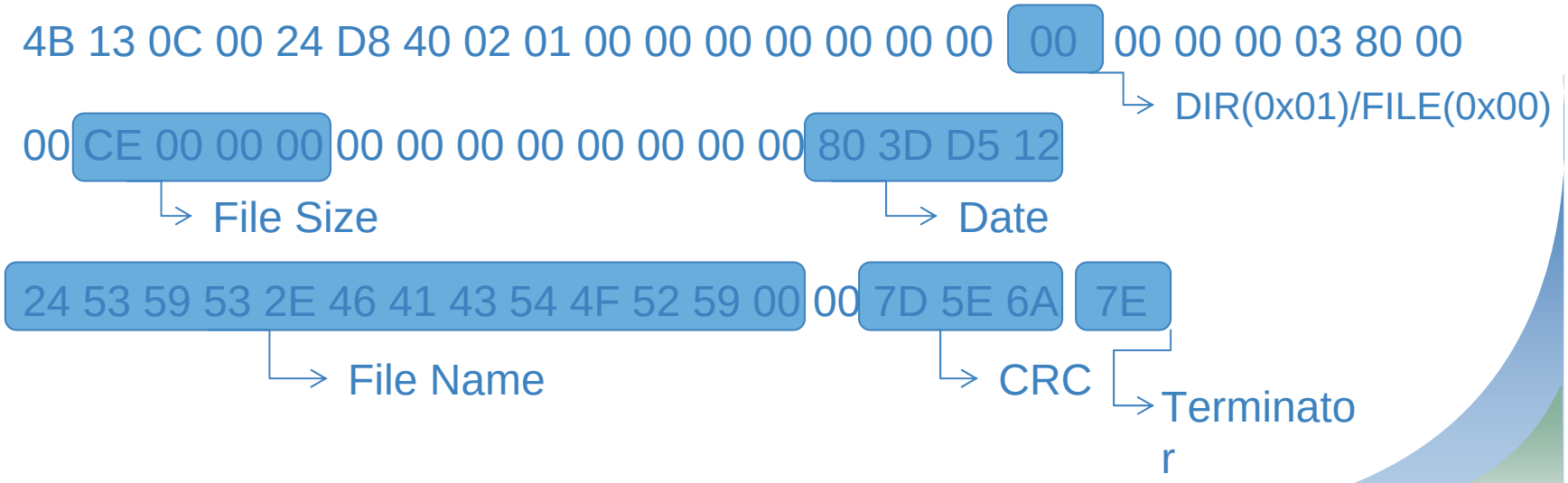


File List Request/Response

Request



Response



END(?) Request/Response

Request

[S] 4B 13 0D 00 24 D8 40 02 90 B8 7E

Response

[R] 4B 13 0D 00 00 00 00 00 96 69 7E

END(?) Request/Response

Request

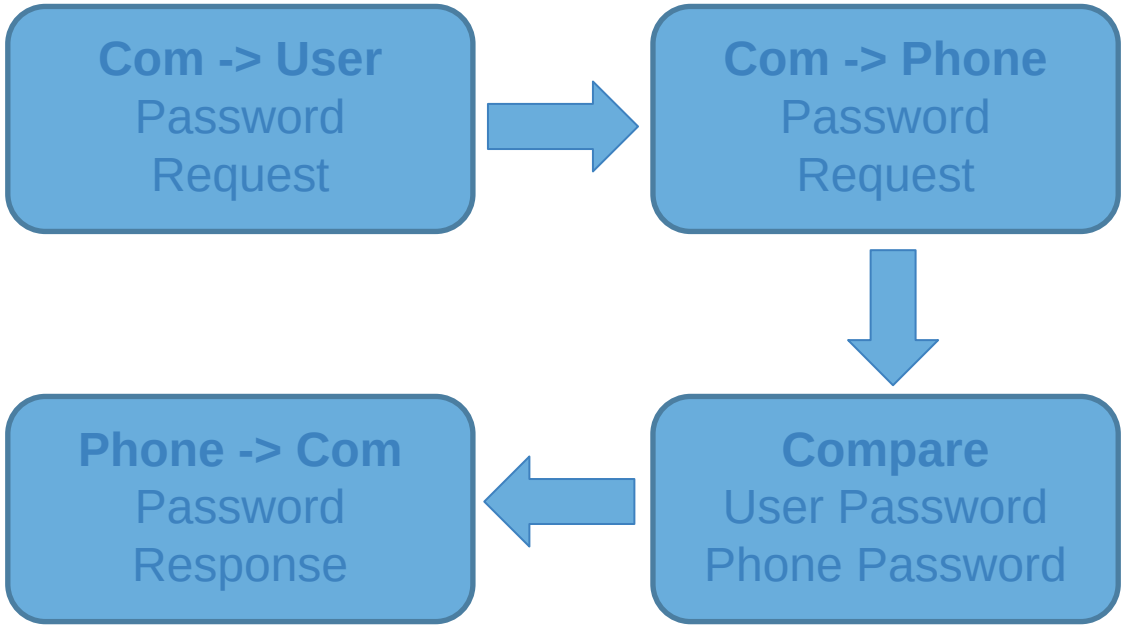
[S] 4B 13 0F 00 2F 00 F5 63 7E

Response

[R] 4B 13 0F 00 00 00 00 00 FF 41 00 00
0F 00 00 00 0D 00 00 00 00 00 00 00 80
3D D5 12 80 3D D5 12 EC 46 7E

Password Authentication

- Password comparison occurs on the side of the PC
- Password can be acquired from the query response



Phone Password

\x26\x52\x00**\x35\x31\x30\x31**\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x26\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x0C\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x34\xF6\x7E

Data Recovery

- Storing SMS
  - SMS messages within one file
  - One file for each SMS message
- Deleting SMS
  - Whether the SMS has been deleted or not can be known by checking flag
  - Data still exist after deleting
  - Can’t get Deleted time

SMS Data

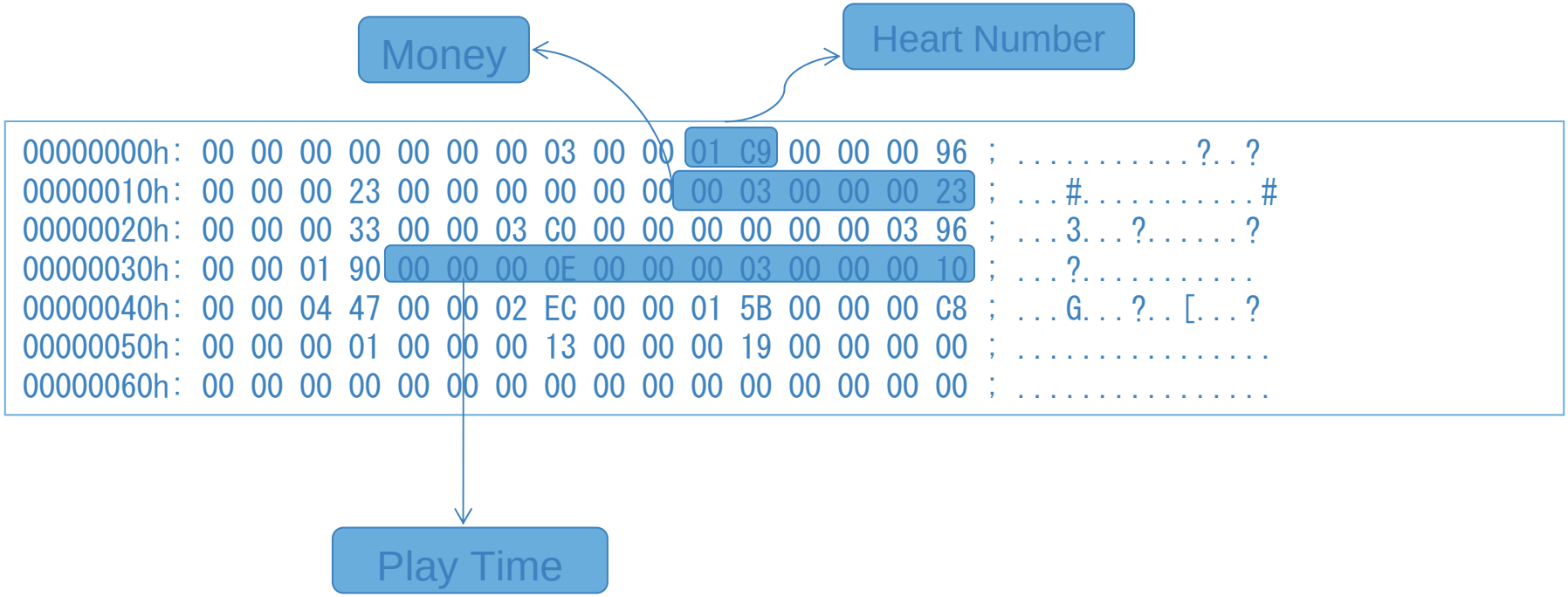
Total Message Size : 1377Byte
Message End : \x00\x00\x0a
First Byte : 7E (Live)
Other(Delete)

```
000060d2h: 7F A6 0D 00 00 07 00 09 29 11 13 31 00 00 00 00 ; □?.....)..1....
000060e2h: 00 F4 DC 00 00 00 00 00 00 00 00 0C 00 0B 00 00 ; .堞............
000060f2h: 00 01 08 3C 00 00 00 2A 00 01 00 01 F4 DC 00 00 ; ...<...*....堞..
00006102h: 00 00 C0 FC C8 AD BF AC B6 F4 BF E4 B8 C1 00 00 ; ..전화연락요망..
00006112h: 00 0B 30 31 30 33 31 37 37 39 39 31 38 07 09
29 ; ..01031779918..)
00006122h: 11 13 31 00 00 00 00 00 00 00 00 00 00 00       ; ..1..........
```

Game Score Data

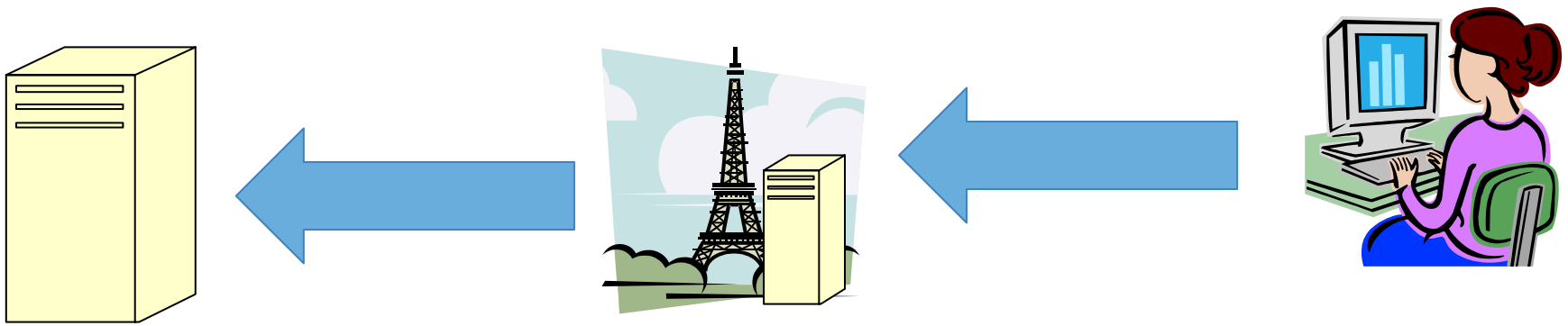
- Store Game Data as a file
- Data can be modified by using well-known method of game data hacking
- Analyzing data structure by comparing updated data from the old data
- On Games that connects servers, score data can be modified through direct connection to the phone

Game Score Data Patch



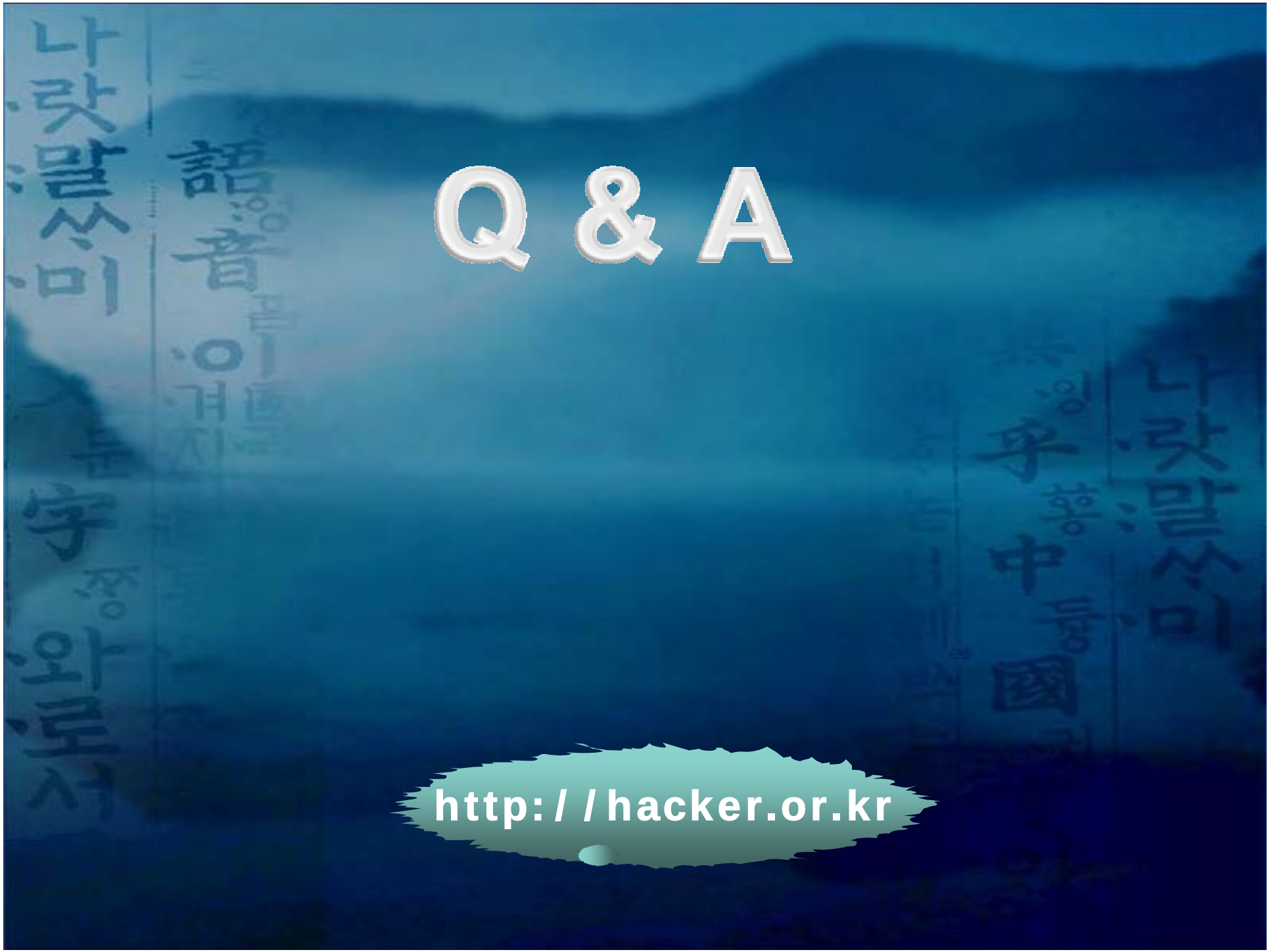
Etc…

- Web pages available only for Phones, PC web browser can’t access the web pages.
- Accessing by Modifying HTTP Header
- Incoming data from web pages can be modified (phone number/phone information)



HTTP Phone Header

multi-proxy: XXXX
http-proxy-info: PNAME:pasgw1;PTIME:20071030135941
host: xxx.xxx.xxx.xxx
user-agent: Mozilla/1.22 (compatible; SPH-V7400; CellPhone)
counter: 2
http-phone-number: 82 TTTEEELLLL
http-phone-system-parameter: BASE_ID:37314, NID:73, SID:2189, BASE_LAT:539867, BASE_LONG:1827750
http-device-info: LX:240,LY:320,CL:16
http-driver-info: IMG:NBMP|SIS2|JPEG|PNG|MNG|MCARD|MCOUPON,SND:MA5|SMAF64|MID|KMP|MSGR,VOD:HWVOD|MPEG4|H.263
http-platform-info: PNAME:KTFWIPI,PVER:V1.2,PID:1080
http-channel-info: CH:E
http-tab-version: 0
http-mnc-info: 04
http-mdn-info: TTTEEELLLL
proxy-connection: Keep-Alive


Q & A
http://hacker.or.kr