



카카오톡으로 여친 만들기

김태훈

나이 : 22

취미 : 해킹

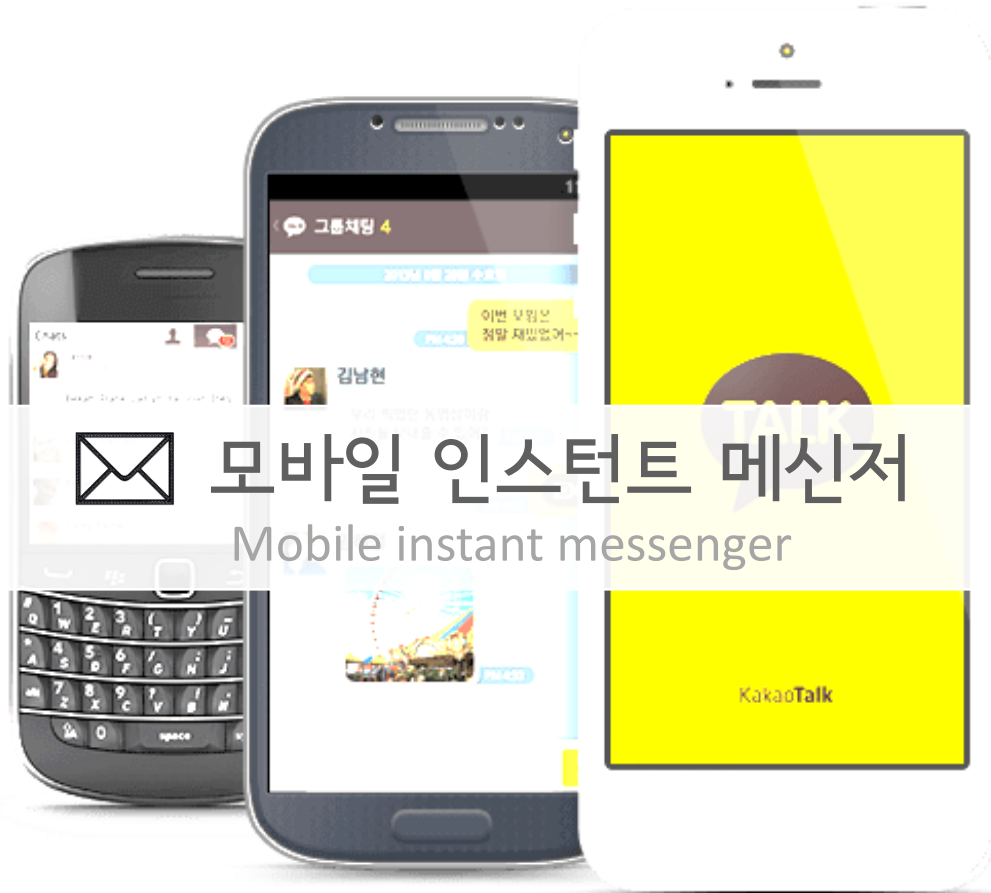
carpedm20

모조킬러, 로봇, 포탈봇, 식단봇, 헥사봇

카카오톡으로 여친 만들기

카카오톡으로 여친 만들기
카카오톡?

카카오톡?



모바일 인스턴트 메신저

Mobile instant messenger

카카오톡?

모바일 인스턴트 메신저



어떻게?

카카오톡?

모바일 인스턴트 메신저

프로토콜

Protocol

카카오톡?

모바일 인스턴트 메신저



통신을 원하는 두 개체간에 무엇을, 어떻게, 언제
통신할 것인가를 서로 약속한 규약

카카오톡?

모바일 인스턴트 메신저

대표적인 **프로토콜**

TCP/IP, HTTP, SSH, FTP

카카오톡?

모바일 인스턴트 메신저

카카오톡에서 사용하는 프로토콜?

TCP/IP? HTTP? SSH? FTP?

카카오톡?

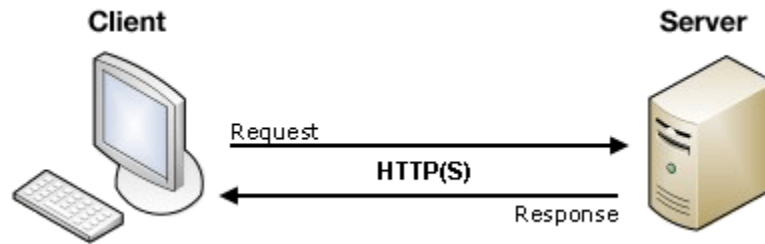
모바일 인스턴트 메신저

HTTP

2011.11 이전

카카오톡?

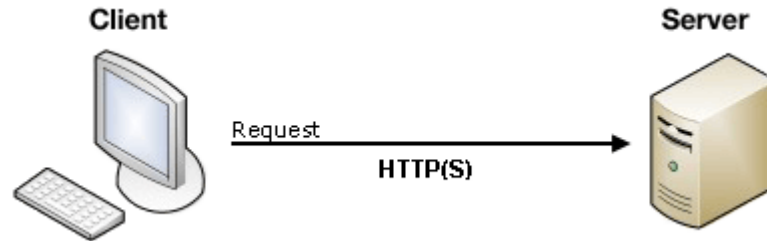
모바일 인스턴트 메신저



WWW 상에서 정보를 주고 받을 수 있는 프로토콜

카카오톡?

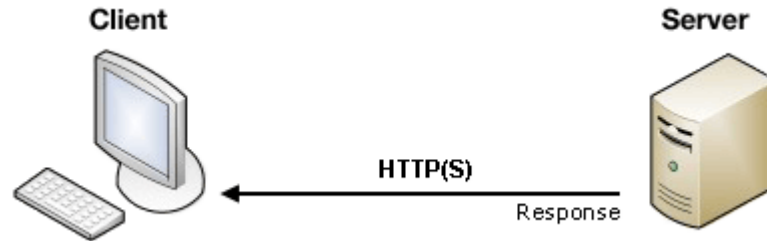
모바일 인스턴트 메신저



```
GET http://hexa.perl.sh/login?id=carpedm20&pw=secret HTTP/1.1
Host: hexa.perl.sh
Proxy-Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;
User-Agent: Chrome/29.0.1547.76
Accept-Encoding: sdch
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: PHPSESSID=oeilogqc1qf3g06aghh3qrekt3
```

카카오톡?

모바일 인스턴트 메신저



```
HTTP/1.1 200 OK
```

```
Date: Tue, 08 Oct 2013 04:48:07 GMT
```

```
Server: Apache/2.2.22 (Ubuntu)
```

```
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

```
Cache-Control: no-store, no-cache, must-revalidate
```

```
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
```

```
<head>
```

```
...
```

카카오톡?

모바일 인스턴트 메신저

```
POST /iphone/chats/write.json HTTP/1.1
Host: talk.kakao.com
User-Agent: KakaoTalk/2.3.1 CFNetwork/485.12.7 Darwin/10.4.0
A: ios/2.3.1/ko
S: < session key >
Content-Type: multipart/form-data; boundary=< boundary >
Accept: */*
Accept-Language: ko-kr
Accept-Encoding: gzip, deflate
Content-Length: 432
Connection: keep-alive
```

```
Content-Disposition: form-data; name="message"
```

카카오톡으로 여친 만들기

```
--< boundary >
```

```
Content-Disposition: form-data; name="chat_id"
```

```
55912035628534
```

```
--< boundary >--
```

카카오톡?

모바일 인스턴트 메신저



2011.11 이후

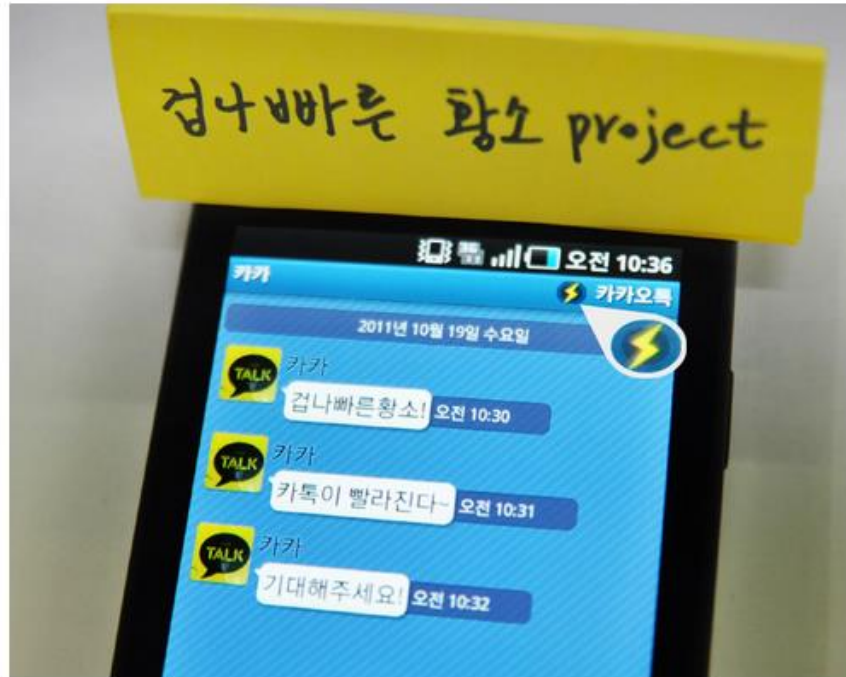
카카오톡?

모바일 인스턴트 메신저

지금, 겁나 빠른 황소가 갑니다.

공지사항/이벤트 2011/10/20 16:57

안녕하세요, 카카오톡입니다.



몇 차례 공지드렸던 겁나 빠른 황소 프로젝트, 본격적으로 가동 중에 있습니다. 벌써부터 겁나 빠른 황소에 올라탄 행운아의 후기가 이어지고 있는데요 :) 카카오톡 우측 상단에 번개가 나타났다면 당신의 카카오톡도 겁나 빠른 황소에 올라탄 것입니다.

카카오톡?

모바일 인스턴트 메신저

겁나 빠른 황소 프로젝트

2011.11 이후

카카오톡?

모바일 인스턴트 메신저

겁나 **빠른** 황소 프로젝트 = **LOCO** 프로토콜

2011.11 이후



Protocol



통신을 원하는 두 개체간에 무엇을, 어떻게, 언제
통신할 것인가를 서로 약속한 규약

Secret Protocol



통신을 원하는 두 개체간에 무엇을, 어떻게, 언제
통신할 것인가를 서로 약속한 **비공개** 규약

카카오톡으로 여친 만들기

카카오톡으로 여친 만들기

여친?

여친?



신화 속에서나 등장하는 상상의 동물

ASKY

The
Girlfriend



여친?

신화 속에서나 등장하는 상상의 동물

목표 : 여친을 만들자 (X)

가상의 여친을 만들자 (O)

Imaginary girlfriend

여친?

신화 속에서나 등장하는 상상의 동물

‘가상’의 여친, 조건 2가지

여친?

신화 속에서나 등장하는 상상의 동물

‘가상’의 여친, 조건 2가지

1. 나의 말을 들을 수 있다.

여친?

신화 속에서나 등장하는 상상의 동물

‘가상’의 여친, 조건 2가지

1. 나의 말을 들을 수 있다.
2. 나의 말에 대한 대답을 할 수 있다.

여친?

신화 속에서나 등장하는 상상의 동물

카카오톡에 살고 있는



‘가상’의 여친, 조건 2가지

1. 나의 메시지를 읽을 수 있다.
2. 나의 메시지에 대한 답장을 할 수 있다.

해킹을 시작해 봅시다

Let's start hacking

해킹을 시작해 봅시다



우리에게 필요한 것?

해킹을 시작해 봅시다
우리에게 필요한 것?

```
# include <stdio.h>
```

```
int kakaoTalk()
```

```
{
```

```
    sendMessage(“카카오톡으로 여친 만들기”);
```

```
    return 0;
```

```
}
```

해킹을 시작해 봅시다
우리에게 필요한 것?

카카오톡 오픈 소스

해킹을 시작해 봅시다
우리에게 필요한 것?

카카오톡 ≠ 오픈 소스

Life is short, you need HeXA

해킹을 시작해 봅시다
우리에게 필요한 것?

디컴파일

Decompile

해킹을 시작해 봅시다
우리에게 필요한 것?

카카오톡 초기 버전 어플리케이션

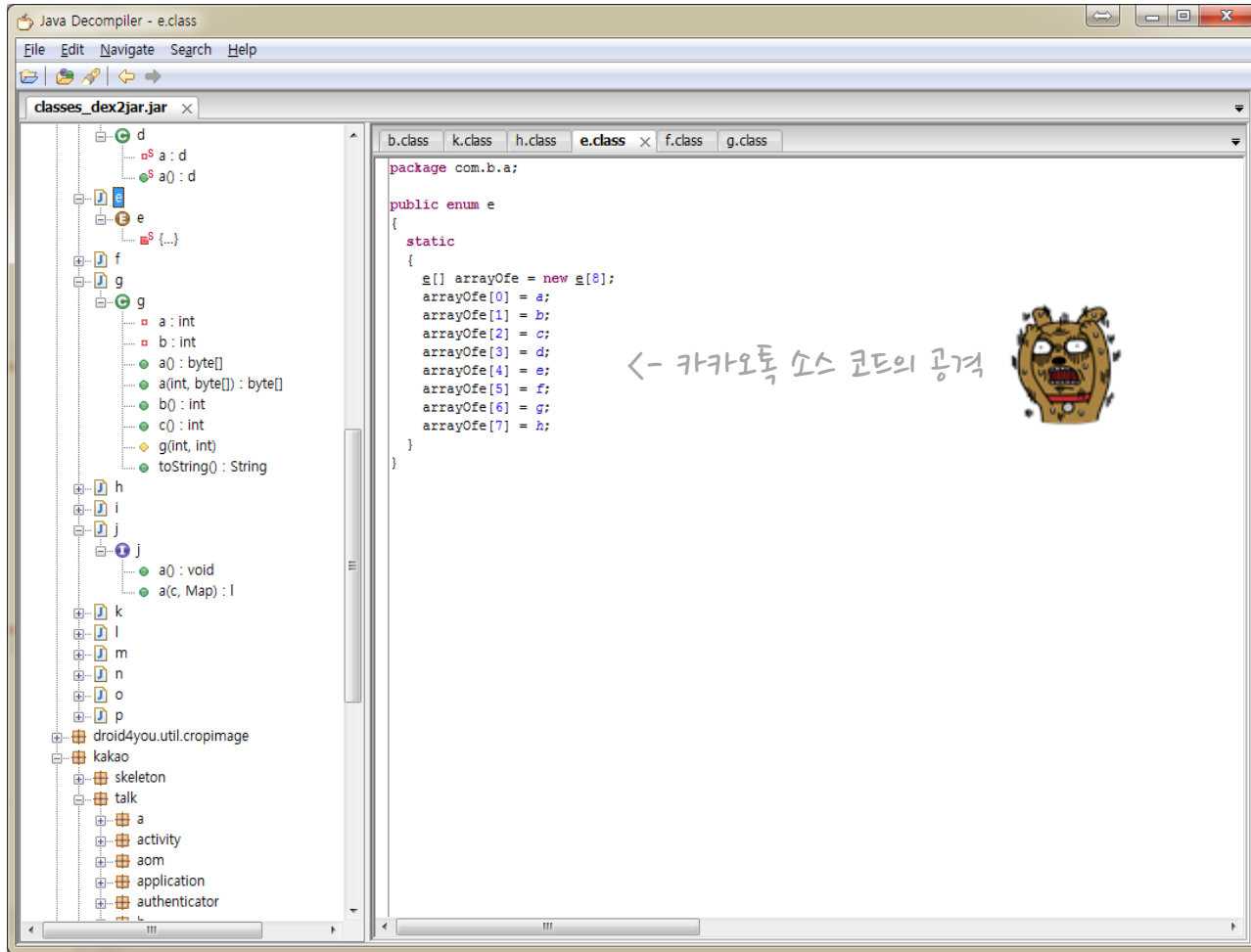
KakaoTalk application in 2006

해킹을 시작해 봅시다
우리에게 필요한 것?

소스 코드 난독화

Source code obfuscation

해킹을 시작해 봅시다
우리에게 필요한 것?



읽어볼 테면 읽어봐

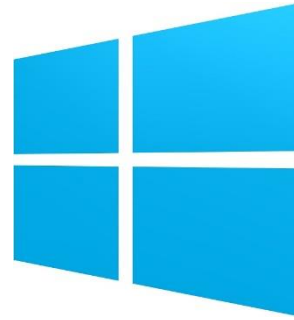
해킹을 시작해 봅시다
우리에게 필요한 것?



Java
.apk



Objective C
.ipa



C#
.xap



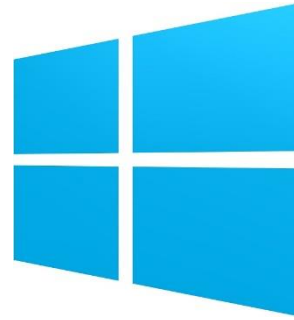
Java
.jar

해킹을 시작해 봅시다
우리에게 필요한 것?



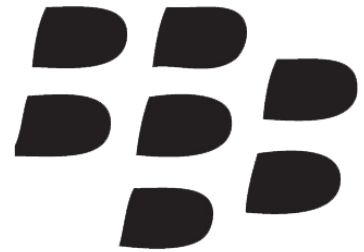
Java

상대적으로 구하기 쉬움



C#

상대적으로 분석하기 쉬움

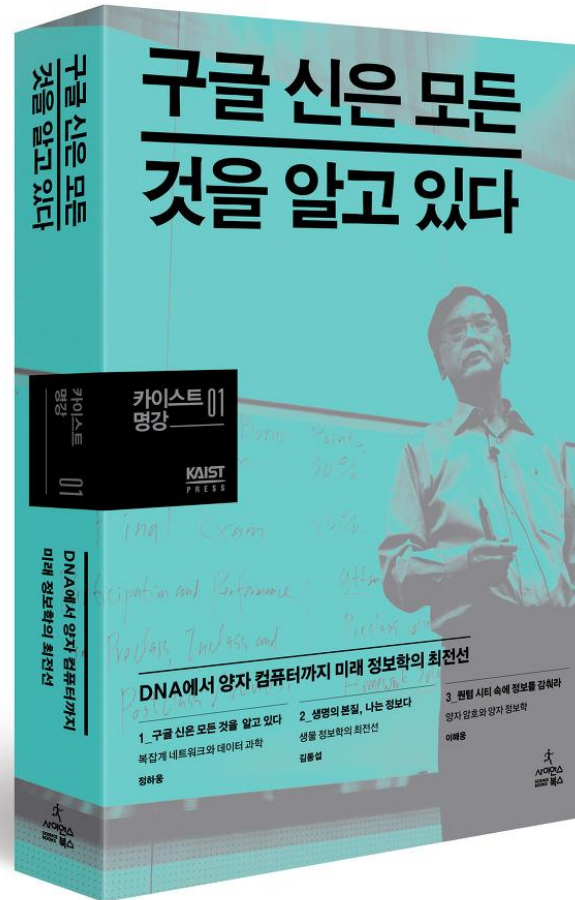


해킹을 시작해 봅시다



어떻게 구하지?

해킹을 시작해 봅시다
어떻게 구하지?



해킹을 시작해 봅시다
어떻게 구하지?

+Taeoon

Gmail

이미지



공유



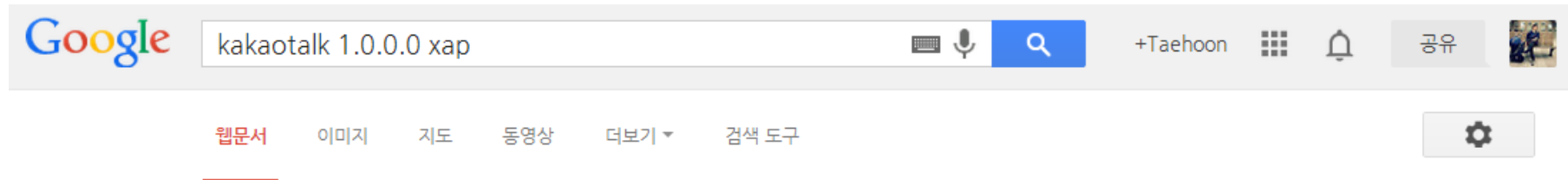
kakaotalk 1.0.0.0 xap



Google 검색

I'm Feeling Lucky

해킹을 시작해 봅시다 어떻게 구하지?



검색결과 약 1,820개 (0.15초)

관련검색: [kakaotalk xap](#)

[Animal Names 1.0.0.0 | Download Mobile Apps & Games ...](#)

[m.brothersoft.com](#) > [Social Networking](#) ▾ [이 페이지 번역하기](#)

Animal Names 1.0.0.0. Download Now (15 MB/xap). Description. You may know that a doe is a female ... [KakaoTalk 1.5.0.0](#) · [Kids Movies 2.0.0.0](#) · [Dora 1.0.0.0](#).

[Baby Learner 1.0.0.0 | Download Mobile Apps & Games | Brothersoft ...](#)

[m.brothersoft.com](#) > [Social Networking](#) ▾ [이 페이지 번역하기](#)

Baby Learner 1.0.0.0. Download Now (10 MB/xap). Description. The application let you move without ... [KakaoTalk 1.5.0.0](#) · [Kids Movies 2.0.0.0](#) · [Dora 1.0.0.0](#).

[Coloring book 1.0.0.0 | Download Mobile Apps & Games ...](#)

[m.brothersoft.com](#) > [Social Networking](#) ▾ [이 페이지 번역하기](#)

Coloring book 1.0.0.0. Download Now (1 MB/xap). Description ... [Instant Quack 1.0.0.0](#) · [Yahoo! Contacts 1.2.0.0](#) · [KakaoTalk 1.5.0.0](#) · [Kids Movies 2.0.0.0](#)

[DrawSomething 1.0.0.0 | Download Mobile Apps & Games ...](#)

[m.brothersoft.com](#) > [Social Networking](#) ▾ [이 페이지 번역하기](#)

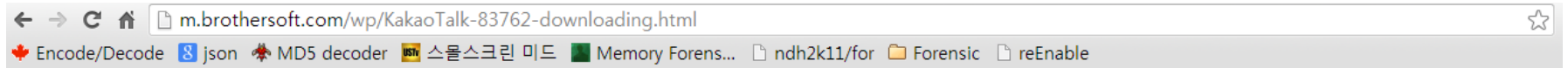
DrawSomething 1.0.0.0. Download Now (< 1 MB/xap). Description. Drawpad enables you to sketch ... [KakaoTalk 1.5.0.0](#) · [Google Talk 1.1.0.0](#). All Mobile Apps.

HOT 토픽

- 1 태풍 다나스 항공편 결항
- 2 백지영 눈을 악성 댓글
- 3 안녕하세요 집착 오빠
- 4 유리베 흥런 다저스
- 5 조영남 성형 후 얼굴 공개
- 6 北 군 동원태세 지시 위협
- 7 김형태 대체 왜 이러나
- 8 이청용 박주영 위건 감독
- 9 통진당 대리투표 무죄
- 10 美 해설진 일제히 류현진

해킹을 시작해 봅시다
어떻게 구하지?

그렇게 아무 일도 일어나지 않았다...



KakaoTalk 1.5.0.0
is downloading now, Please Wait...

Such as download failed, please
[Click Here](#) to download again.

Popular Apps for [Social Networking](#)

All Mobile Apps

[MP3 & Audio](#) (2,508)
[Communication](#) (1,014)
[Email & SMS](#) (203)
[Internet](#) (5,543)
[Action](#) (6,268)
[Adventure](#) (6,503)

[>>All Apps](#) [>>All Games](#)
[>>Essential Apps](#)
[>>Top Downloads](#)

[Home](#) > [Social Networking](#) > [KakaoTalk 1.5.0.0](#) > Downloading

해킹을 시작해 봅시다
어떻게 구하지?

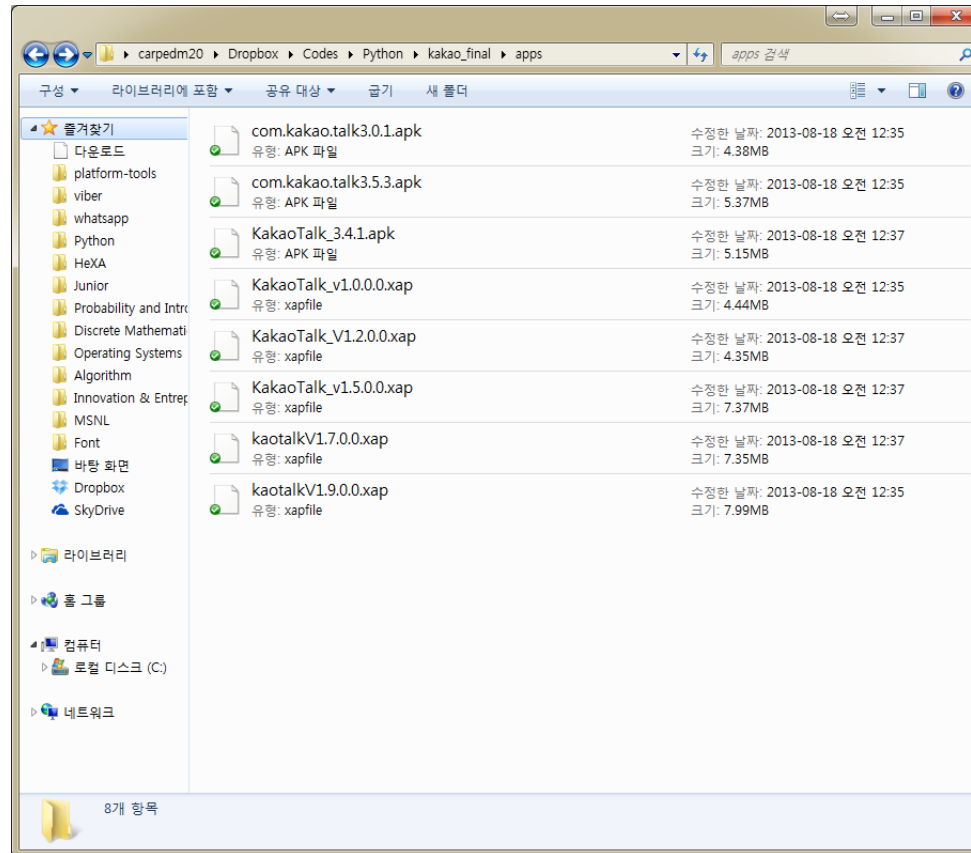


검색에 **왕도**는 없었다...

by carpdm20

해킹을 시작해 봅시다
어떻게 구하지?

결국... 성공!



해킹을 시작해 봅시다

소스코드를 읽어 봅시다

Reversing

해킹을 시작해 봅시다
소스코드를 읽어 봅시다



KakaoTalk_3.4.1.apk



KakaoTalk_v1.0.0.0.xap

얘네는 뭐지? C#, Java 인건 알겠는데...

해킹을 시작해 봅시다
소스코드를 읽어 봅시다



KakaoTalk_3.4.1.zip



KakaoTalk_v1.0.0.0.zip

그냥 zip 파일

해킹을 시작해 봅시다
소스코드를 읽어 봅시다



KakaoTalk_3.4.1



KakaoTalk_v1.0.0.0

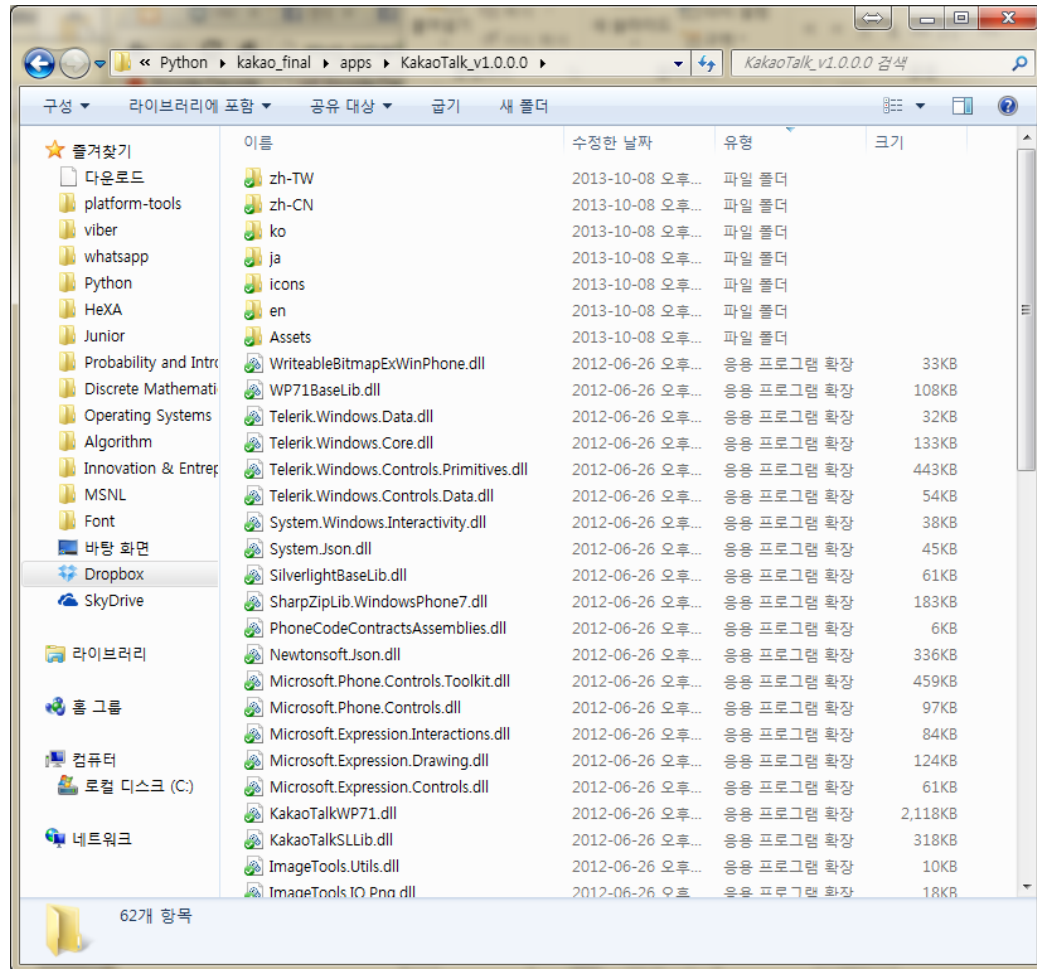


KakaoTalk_3.4.1.zip



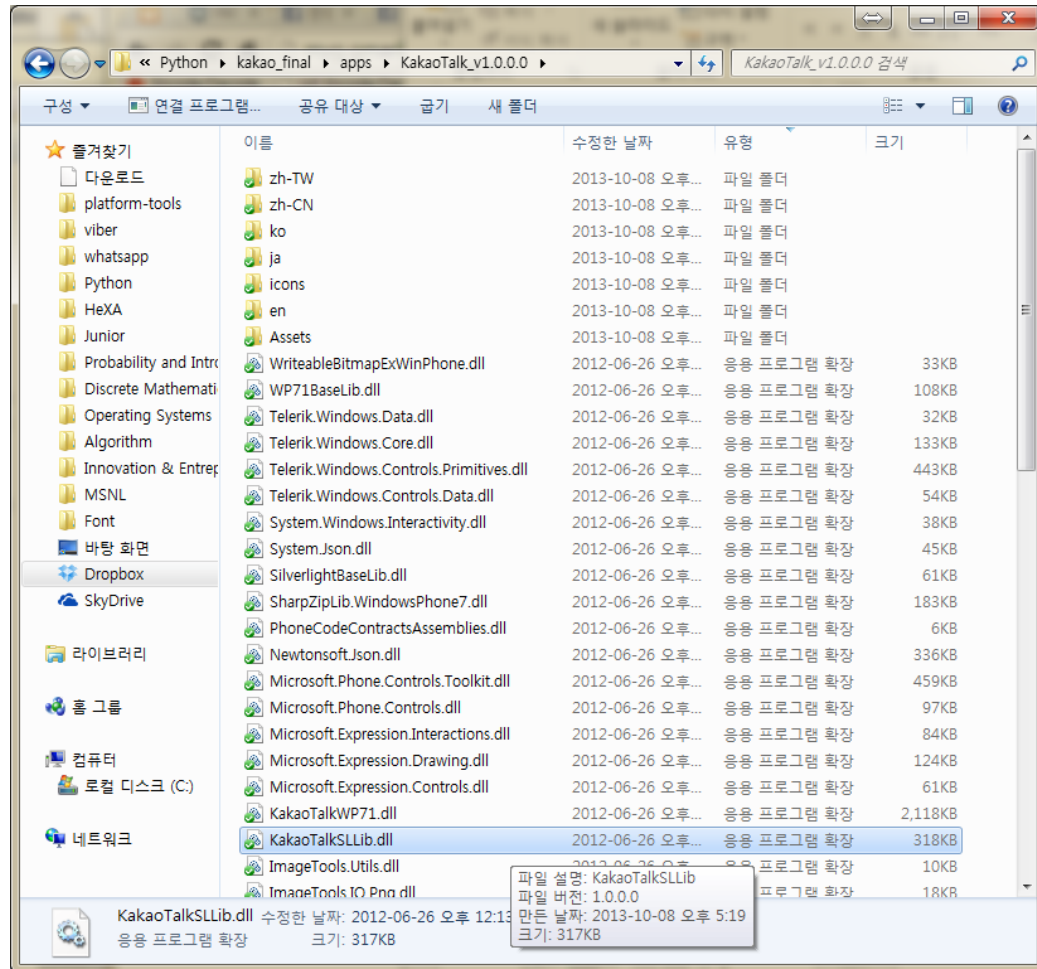
KakaoTalk_v1.0.0.0.zip

해킹을 시작해 봅시다
소스코드를 읽어 봅시다



음...

해킹을 시작해 봅시다
소스코드를 읽어 봅시다



찾음ㅋ

해킹을 시작해 봅시다

소스코드를 읽어 봅시다

.NET Reflector 8.2.0.42 - 10 days remaining

File Edit View Tools Help

Search Object Browser (Ctrl-F)

LocoClientAgent

- Base Types
- Derived Types
- _SendPacket_Timer
- _SendPendingPacket_Info
- ctor()
- _FireSendFailed(_SendPacket_Timer) : Void
- _SendPendingTimerCallBack(Object) : Void
- _TcpSocketClient_ConnectSucceeded(Object, EventArgs) : Void
- _TcpSocketClient_ReceivedFailed(Object, EventArgs) : Void
- _TcpSocketClient_ReceivedSucceeded(Object, EventArgs) : Void
- <_FireSendFailed>b_5(Object) : Void
- Connect(String, Int32) : Void
- Disconnect() : Void
- Send(LocoPacket) : Void
- Send(LocoPacket, String, Int32, Boolean) : Void

Current : LocoClientAgent

- IsSecureMode : Boolean
- SessionKeyBytes : Byte[]
- LocoPacketPushReceived
- LocoPacketReceived
- LocoPacketSendFailed
- SocketDisconnected
- _Current : LocoClientAgent
- _CurrentContext : SynchronizationContext
- _RecvPacketManager : LocoRecvPacketManager
- _SecureRecvPacketManager : LocoSecureRecvPacketManager
- _SendPacket_Timer_Map : Dictionary<Int32, _SendPacket_Timer>
- _SendPendingPacket_Infos : List<_SendPendingPacket_Info>
- _SessionKeyBytes : Byte[]
- _TcpSocketClient : TcpSocketClient
- <IsSecureMode>k__BackingField : Boolean

public void Send(LocoPacket sendPacket, string host, int port, bool isConnectionLessApi)

Declaring Type: KakaoTalkSLLib.LOCO.Base.LocoClientAgent

Assembly: KakaoTalkSLLib, Version=1.0.0.0

Search


LOGIN

Item	Owner	Assembly
RoleGroups	System.Web.UI.WebControls.LoginView	System.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
RunFileDialog	System.Windows.Forms.OpenFileDialog	System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561df3e698
RunFileDialog	System.Windows.Forms.SaveFileDialog	System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561df3e698
Send	KakaoTalkSLLib.LOCO.Base.LocoClientAgent	KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
SendPreLoginHandshake	System.Data.SqlClient.TdsParser	System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561df3e698

public void Send(LocoPacket sendPacket, string host, int port, bool isConnectionLessApi)

```
DebugEx.Assert(sendPacket != null);
DebugEx.Assert(host.Length > 0);
DebugEx.Assert(port > 0);
DebugEx.WriteLine(string.Format("LocoClientAgent.Send HostPort[{0}:{1}] Method[{2}] PacketId[{3}]", new object[] { host, port, sendPacket.Method, sendPacket.PacketId }));
if ((this._TcpSocketClient.IsConnected || (this._TcpSocketClient.Host != host)) || ((this._TcpSocketClient.Port != port) || isConnectionLessApi))
{
    _SendPendingPacket_Info item = new _SendPendingPacket_Info {
        SendPendingPacket = sendPacket,
        Host = host,
        Port = port,
        IsConnectionLessApi = isConnectionLessApi
    };
    this._SendPendingPacket_Infos.Add(item);
    this._TcpSocketClient.ConnectAsync(host, port);
}
else
{
    sendPacket.FillBuffer();
    _SendPacket_Timer state = new _SendPacket_Timer {
        SendPacketObj = sendPacket
    };
    this._SendPacket_Timer_Map[sendPacket.PacketId] = state;
    TimeSpan dueTime = TimeSpan.FromSeconds((double) KakaoLibModel.Current.LocoRetryItv);
    state.TimerObj = new Timer(new TimerCallback(this._SendPendingTimerCallBack), state, dueTime, dueTime);
    byte[] dst = null;
    if (this.IsSecureMode)
    {
        if (sendPacket.Method == "LOGIN")
        {
            LocoSecureHandshakePacket packet = new LocoSecureHandshakePacket();
            packet.FillBuffer();
```

<- 우왕! 코드가 보여요



.Net Reflector

해킹을 시작해 봅시다
소스코드를 읽어 봅시다

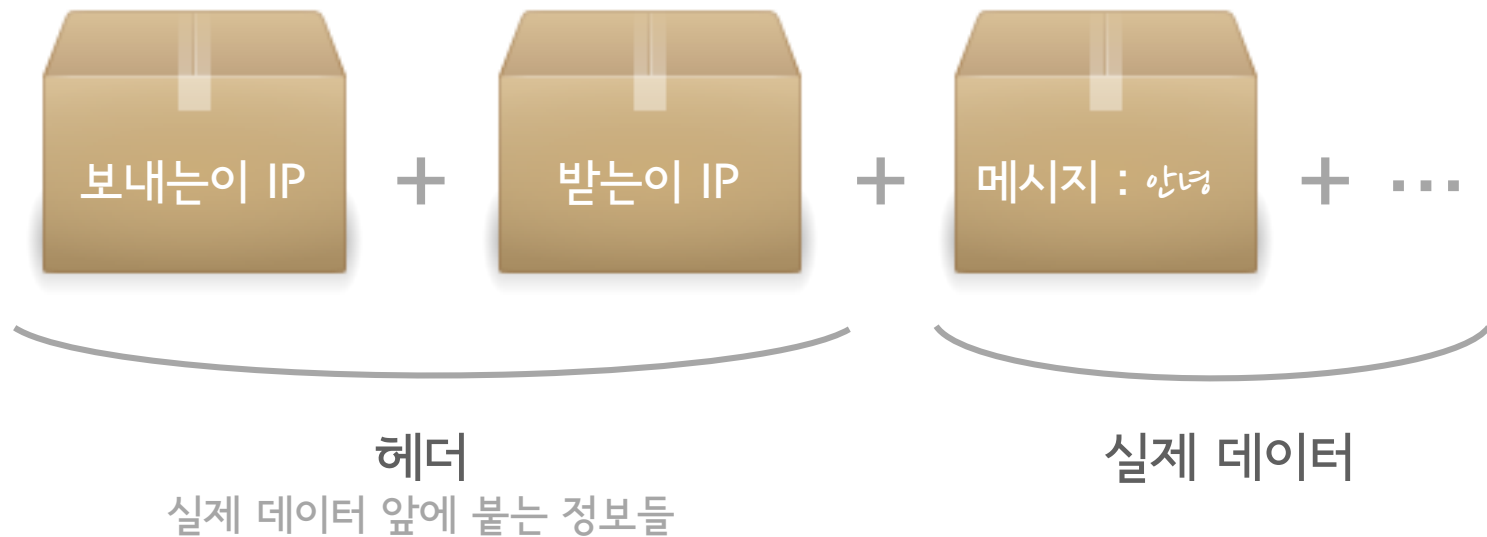
Network Packet



컴퓨터 네트워크가 전달하는 데이터의 형식화된 **블록**

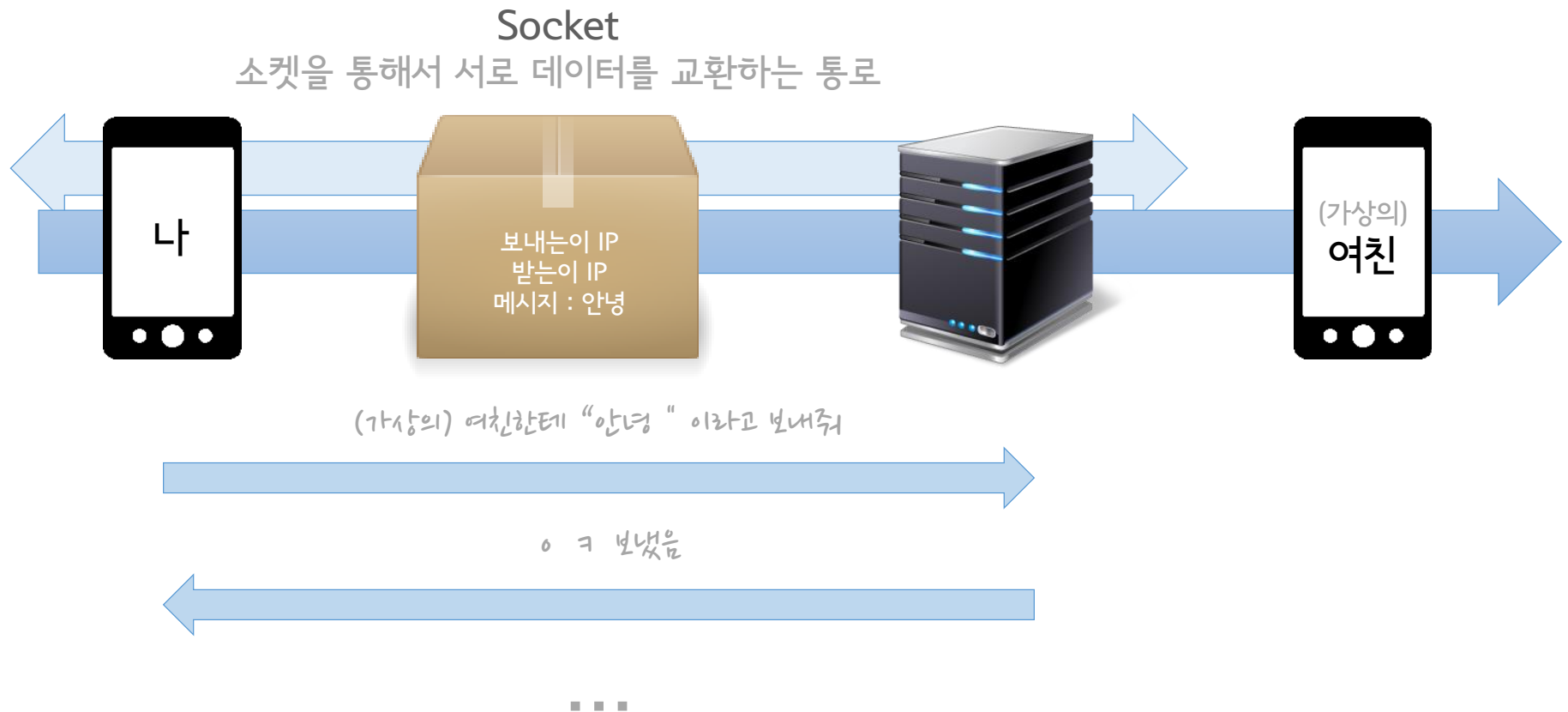
해킹을 시작해 봅시다
소스코드를 읽어 봅시다

Network Packet



해킹을 시작해 봅시다
소스코드를 읽어 봅시다

TCP 통신



해킹을 시작해 봅시다

소스코드를 읽어 봅시다

Network flow

- LOCO 서버와 TCP 소켓이 **연결**되어 있는지 **확인**
 - 그렇지 않다면 재 접속 시도
- 현재 **커맨드**에 해당하는 패킷 생성 (FillBuffer())
 - 커맨드 : 패킷이 메세징 과정에서 하는 역할
- if(isSecureMode)
 - True & Login : **handshake** 패킷 생성 후 암호화된 커맨드 패킷 앞에 붙이고 전송
 - True & !Login : 커맨드 패킷을 암호화 하고 전송
 - False: 그대로 전송

해킹을 시작해 봅시다
소스코드를 읽어 봅시다

커맨드 종류

- ADDMEM
- NOTIREAD
- LEAVE
- READ
- BUY
- CWRITE
- LOGIN
- PING
- WRITE
- BLOCK
- NCHATLIST
- CHATON
- CHATOFF
- UPDATECHAT
- UNBLOCK
- UPSEEN
- CHATLIST
- WRITE

해킹을 시작해 봅시다

소스코드를 읽어 봅시다

```
public void Send(LocoPacket sendPacket, string host, int port, bool isConnectionLessApi)
{
    DebugEx.Assert(sendPacket != null);
    DebugEx.Assert(host.Length > 0);
    DebugEx.Assert(port > 0);
    DebugEx.WriteLine(string.Format("LocoClientAgent.Send Host:Port[{0}:{1}] Method[{2}] PacketId[{3}]", new object[] { host, port, sendPacket.Method, sendPacket.PacketId }));
    if ((this._TcpSocketClient.IsConnected || (this._TcpSocketClient.Host != host)) || ((this._TcpSocketClient.Port != port) || isConnectionLessApi))
    {
        _SendPendingPacket_Info item = new _SendPendingPacket_Info {
            SendPendingPacket = sendPacket,
            Host = host,
            Port = port,
            IsConnectionLessApi = isConnectionLessApi
        };
        this._SendPendingPacket_Infos.Add(item);
        this._TcpSocketClient.ConnectAsync(host, port);
    }
    else
    {
        sendPacket.FillBuffer();
        _SendPacket_Timer state = new _SendPacket_Timer {
            SendPacketObj = sendPacket
        };
        this._SendPacket_Timer_Map[sendPacket.PacketId] = state;
        TimeSpan dueTime = TimeSpan.FromSeconds((double) KakaoLibModel.Current.LocoRetryItv);
        state.TimerObj = new Timer(new TimerCallback(this._SendPendingTimerCallBack), state, dueTime, dueTime);
        byte[] dst = null;
        if (this.IsSecureMode)
        {
            if (sendPacket.Method == "LOGIN")
            {
                LocoSecureHandShakePacket packet = new LocoSecureHandShakePacket();
                packet.FillBuffer();
                LocoSecureNormalPacket packet2 = new LocoSecureNormalPacket {
                    DecryptedDataBlock = sendPacket.Buffer
                };
                packet2.FillBuffer();
            }
        }
    }
}
```

해킹을 시작해 봅시다

소스코드를 읽어 봅시다

```
public void Send(LocoPacket sendPacket, string host, int port, bool isConnectionLessApi)
{
    DebugEx.Assert(sendPacket != null);
    DebugEx.Assert(host.Length > 0);
    DebugEx.Assert(port > 0);
    DebugEx.WriteLine(string.Format("LocoClientAgent Send Host:Port[{0}:{1}] Method[{2}] PacketId[{3}] new object[] { host, port, sendPacket.Method, sendPacket.
    if ((this._TcpSocketClient.IsConnected || (this._TcpSocketClient.Host != host)) || ((this._TcpSocketClient.Port != port) || isConnectionLessApi))
    {
        _SendPendingPacket_Info item = new _SendPendingPacket_Info {
            SendPendingPacket = sendPacket
            Host = host,
            Port = port,
            IsConnectionLessApi = isConnectionLessApi
        };
        this._SendPendingPacket_Infos.Add(item);
        this._TcpSocketClient.ConnectAsync(host, port);
    }
    else
    {
        sendPacket.FillBuffer();
        _SendPacket_Timer state = new _SendPacket_Timer {
            SendPacketObj = sendPacket
        };
        this._SendPacket_Timer_Map[sendPacket.PacketId] = state;
        TimeSpan dueTime = TimeSpan.FromSeconds((double) KakaoLibModel.Current.LocoRetryItv);
        state.TimerObj = new Timer(new TimerCallback(this._SendPendingTimerCallBack), state, dueTime, dueTime);
        byte[] dst = null;
        if (this.IsSecureMode)
        {
            if (sendPacket.Method == "LOGIN")
            {
                LocoSecureHandShakePacket packet = new LocoSecureHandShakePacket
                {
                    packet.FillBuffer();
                    LocoSecureNormalPacket packet2 = new LocoSecureNormalPacket
                    {
                        DecryptedDataBlock = sendPacket.Buffer
                    };
                    packet2.FillBuffer();
                }
            }
        }
    }
}
```

LOCО 서버에 대한 TCP 소켓이 연결되어 있는지 확인

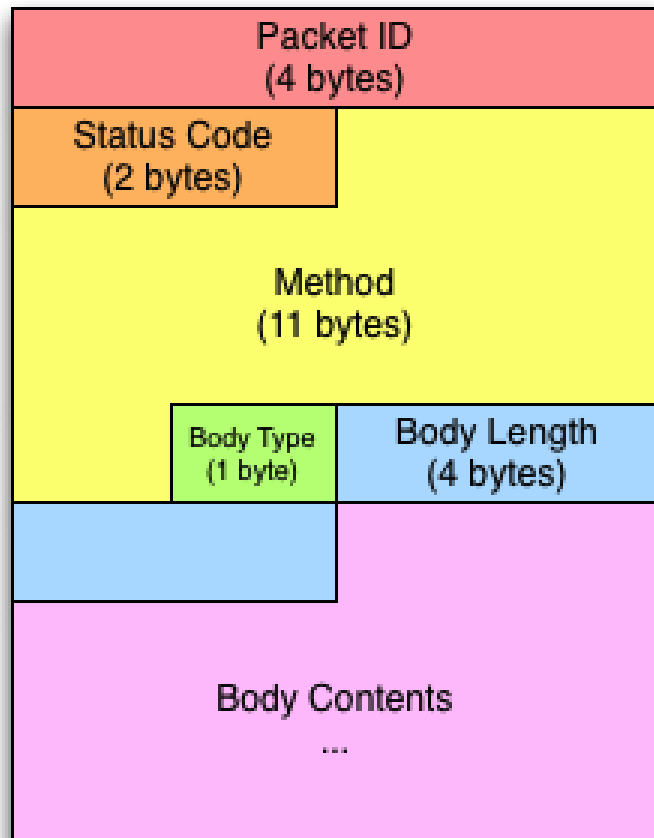
FillBuffer 함수를 통해 현재 커맨드에 해당하는 패킷 생성

True & Login : handshake 패킷 생성 후 암호화된 커맨드 패킷 앞에 붙이고 전송

해킹을 시작해 봅시다

소스코드를 읽어 봅시다

LocoPacket



- 가장 기본이 되는 패킷
- Packet ID : 패킷 번호
- Status Code : 보통 0
- Method = 커맨드

Ex) LOGIN, ADDMEM , ACHATLIST

- Body Type : 0
- Body Length
- Body Contents

- bson 형태로 전송됨

```
{ msg : “안녕”,  
  time : 20131012,  
  to : “(가상의) 여친” }
```

출처 : <http://www.bpak.org/>

해킹을 시작해 봅시다

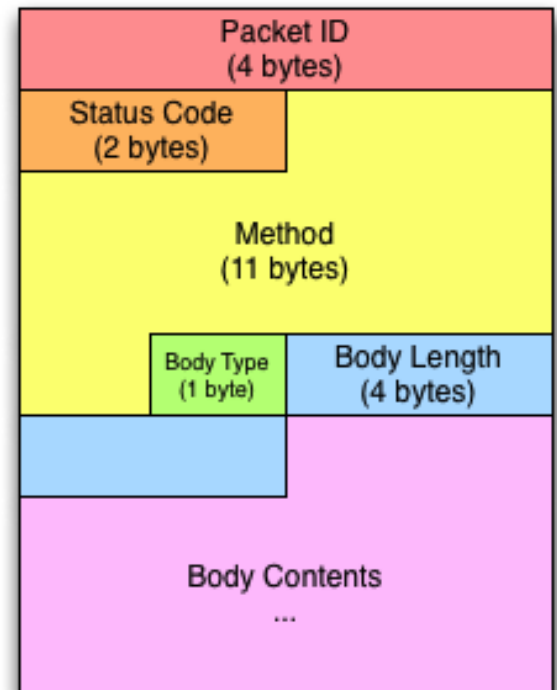
소스코드를 읽어 봅시다

```
public class LocoPacket : PacketBase, INotifyPropertyChanged
{
    // Fields
    private byte[] _Body;
    private int _BodyLength;
    private byte _BodyType;
    private static int _CurrentPacketId;
    private string _Method;
    private int _PacketId;
    private short _StatusCode;
    private static StringToAsciiEncodedBytesConverter _StringToAsciiEncodedBytesConverter;
    private PropertyChangedEventHandler PropertyChanged;

    // Events
    public event PropertyChangedEventHandler PropertyChanged;

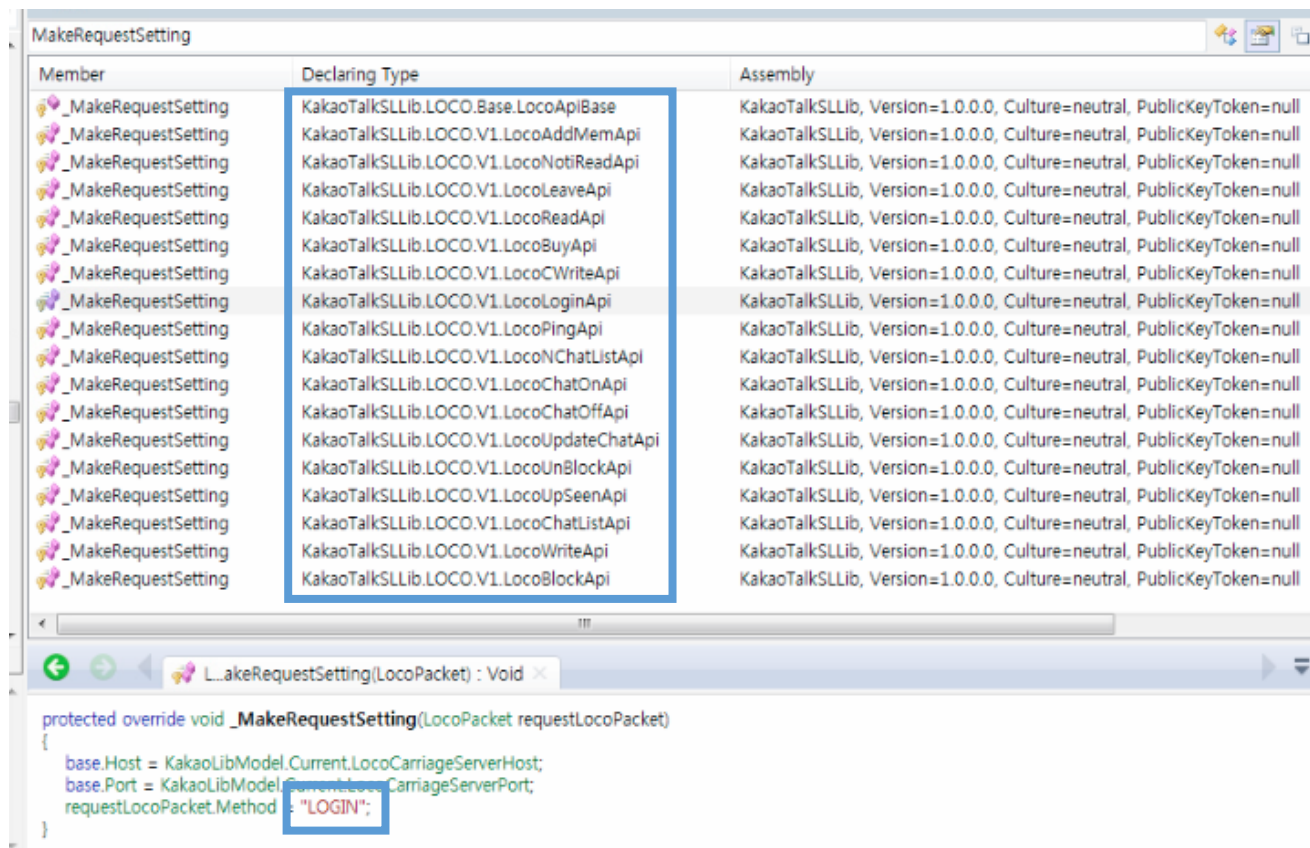
    // Methods
    static LocoPacket();
    public LocoPacket();
    public override void FillBuffer();
    public override int Parse(List<byte> recvData);
    private void This_PropertyChanged(object sender, PropertyChangedEventArgs e);

    // Properties
    public byte[] Body { get; set; }
    public int BodyLength { get; private set; }
    public byte BodyType { get; set; }
    public string Method { get; set; }
    public int PacketId { get; set; }
    public short StatusCode { get; set; }
}
```



해킹을 시작해 봅시다
소스코드를 읽어 봅시다

커맨드 종류



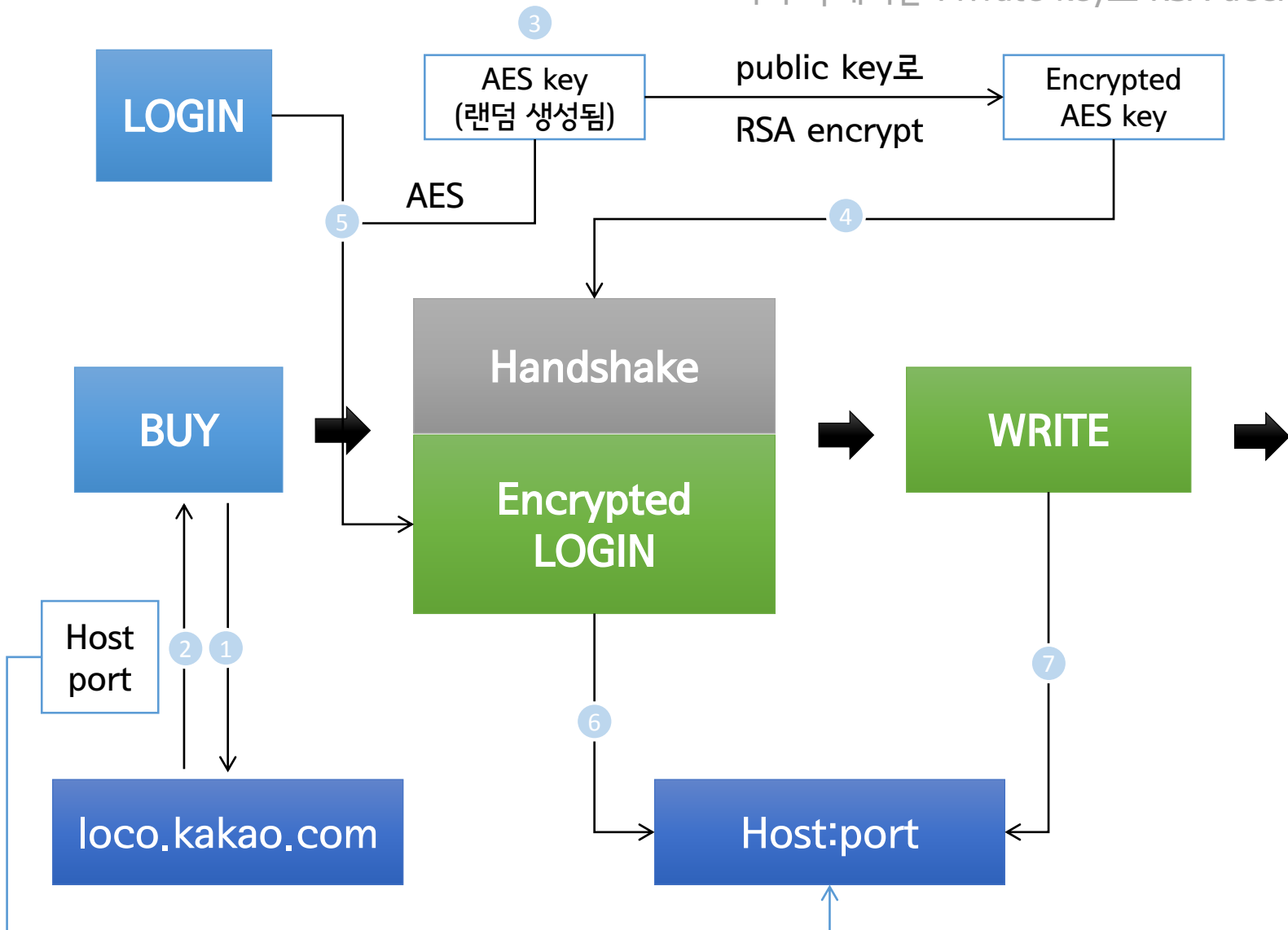
The screenshot displays the 'MakeRequestSetting' class in an IDE. The class list on the left shows various methods, with the 'Declaring Type' column highlighted by a blue box. The code snippet at the bottom shows the implementation of the `_MakeRequestSetting` method, with the `Method` property highlighted by a blue box.

Member	Declaring Type	Assembly
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.Base.LocoApiBase</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoAddMemApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoNotiReadApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoLeaveApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoReadApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoBuyApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoCWriteApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoLoginApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoPingApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoNChatListApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoChatOnApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoChatOffApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoUpdateChatApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoUnBlockApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoUpSeenApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoChatListApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoWriteApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>
<code>_MakeRequestSetting</code>	<code>KakaoTalkSLLib.LOCO.V1.LocoBlockApi</code>	<code>KakaoTalkSLLib, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null</code>

```
protected override void _MakeRequestSetting(LocoPacket requestLocoPacket)
{
    base.Host = KakaoLibModel.Current.LocoCarriageServerHost;
    base.Port = KakaoLibModel.Current.LocoCarriageServerPort;
    requestLocoPacket.Method = "LOGIN";
}
```

해킹을 시작해 봅시다
소스코드를 읽어 봅시다

서버 측에서는 Private key로 RSA decrypt



해킹을 시작해 봅시다



패킷패킷패킷 실제로 어떻게 생겼을까?

Network

해킹을 시작해 봅시다

패킷패킷패킷 실제로 어떻게 생겼을까?

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
123	11.522015	10.20.14.215	10.36.115.40	TCP	http > 62624 [SYN, ACK] Seq=0 Ack=1 Win=14600
124	11.522016	10.20.14.215	10.36.115.40	TCP	http > 62622 [SYN, ACK] Seq=0 Ack=1 Win=14600
125	11.522016	10.20.14.215	10.36.115.40	TCP	http > 62625 [SYN, ACK] Seq=0 Ack=1 Win=14600
126	11.522017	10.20.14.215	10.36.115.40	TCP	http > 62623 [SYN, ACK] Seq=0 Ack=1 Win=14600
127	11.522076	10.36.115.40	10.20.14.215	TCP	62622 > http [ACK] Seq=1 Ack=1 Win=65536 [TCP
128	11.522079	10.36.115.40	10.20.14.215	TCP	62624 > http [ACK] Seq=1 Ack=1 Win=65536 [TCP
129	11.522093	10.36.115.40	10.20.14.215	TCP	62625 > http [ACK] Seq=1 Ack=1 Win=65536 [TCP
130	11.522094	10.36.115.40	10.20.14.215	TCP	62623 > http [ACK] Seq=1 Ack=1 Win=65536 [TCP
131	11.583505	10.36.115.40	10.20.14.215	HTTP	GET / HTTP/1.1
132	11.589293	10.20.14.215	10.36.115.40	TCP	http > 62620 [ACK] Seq=1 Ack=344 Win=15680 Len=0
133	11.591566	8.8.8.8	10.36.115.40	DNS	Standard query response A 37.9.65.78
134	11.592496	10.36.115.40	8.8.8.8	DNS	Standard query A www.google.com
135	11.597601	8.8.8.8	10.36.115.40	DNS	Standard query response CNAME googleapis.l.google.com
136	11.656261	10.20.14.215	10.36.115.40	TCP	[TCP segment of a reassembled PDU]
137	11.657057	10.20.14.215	10.36.115.40	HTTP	HTTP/1.1 200 OK (text/html)
138	11.657095	10.36.115.40	10.20.14.215	TCP	62620 > http [ACK] Seq=344 Ack=2809 Win=65536 Len=0
139	11.672911	8.8.8.8	10.36.115.40	DNS	Standard query response A 74.125.235.80 A 74.125.235.80
140	11.801613	10.36.115.40	10.20.14.215	HTTP	GET /style.css HTTP/1.1
141	11.802405	10.20.14.215	10.36.115.40	TCP	http > 62620 [ACK] Seq=2809 Ack=812 Win=16768 Len=0
142	11.803171	10.20.14.215	10.36.115.40	HTTP	HTTP/1.1 304 Not Modified
143	11.852964	10.36.115.40	10.20.14.215	TCP	62620 > http [ACK] Seq=812 Ack=3021 Win=65280 Len=0
144	11.897850	10.36.115.40	74.125.31.95	TCP	62626 > http [SYN] Seq=0 Win=8192 [TCP CHECKSUM=0]
145	12.001080	Handream-00:19:72	MS-NLB-PhysServer-26_0xffff	Ethernet II	
146	12.014066	74.125.31.95	10.36.115.40	TCP	http > 62626 [SYN, ACK] Seq=0 Ack=1 Win=62920 Len=0
147	12.014259	10.36.115.40	74.125.31.95	TCP	62626 > http [ACK] Seq=1 Ack=1 Win=65536 [TCP

< Frame 131 (397 bytes on wire, 397 bytes captured)

Ethernet II, Src: 08:9e:01:c3:22:89 (08:9e:01:c3:22:89), Dst: 00:25:c3:cd:20:73 (00:25:c3:cd:20:73)

Internet Protocol, Src: 10.36.115.40 (10.36.115.40), Dst: 10.20.14.215 (10.20.14.215)

Transmission Control Protocol, Src Port: 62620 (62620), Dst Port: http (80), Seq: 1, Ack: 1, Len: 343

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Host: hexa.perl.sh\r\n

Connection: keep-alive\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n

User-Agent: Mozilla/5.0 (e5fac0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.69 Safari/537.36\r\n

Accept-Encoding: gzip,deflate,sdch\r\n

Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4\r\n

\r\n

0000 00 23 c3 cd 20 73 08 9e 01 c3 22 89 08 00 43 00 .%. SE.

0010 01 7f 65 26 40 00 80 06 00 00 0a 24 73 28 0a 14 ..e@.\$(.

0020 0e d7 f4 9c 00 50 c4 fb 82 19 1b a3 90 89 50 18P.P.

0030 01 00 97 a8 00 00 47 45 54 20 2f 20 48 54 54 50GE T / HTTP

File: C:\Users\WCARPED~1\AppData\Local\Temp\Wireshark.packets.174.Packets: 174 Displayed: 174 Marked: 0 Dropped: 0 Profile: Default



해킹을 시작해 봅시다

패킷패킷패킷 실제로 어떻게 생겼을까?

Follow TCP Stream

Stream Content

```
00000000 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a GET / HT TP/1.1..
00000010 48 6f 73 74 3a 20 68 65 78 61 2e 70 65 72 6c 2e Host: he xa.perl.
00000020 73 68 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 sh..Conn ection:
00000030 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 41 63 63 65 keep-ali ve..Acce
00000040 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 pt: text /html,ap
00000050 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plication n/xhtmll+
00000060 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f xml,appl ication/
00000070 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f xml;q=0. 9,image/
00000080 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a webp,*/* ;q=0.8..
00000090 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
000000A0 6c 6c 61 2f 35 2e 30 20 28 65 35 66 61 63 30 29 lla/5.0 (e5fac0)
000000B0 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 Applewe bKit/537
000000C0 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 .36 (KHT ML, like
000000D0 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 33 Gecko) Chrome/3
000000E0 30 2e 30 2e 31 35 39 39 2e 36 39 20 53 61 66 61 0.0.1599 .69 Safa
000000F0 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 ri/537.3 6..Accep
00000100 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 t-Encodi ng: gzip
00000110 2c 64 65 66 6c 61 74 65 2c 73 64 63 68 0d 0a 41 ,deflate ,sdch..A
00000120 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 ccept-La nguage:
00000130 6b 6f 2d 4b 52 2c 6b 6f 3b 71 3d 30 2e 38 2c 65 ko-KR,ko ;q=0.8,e
00000140 6e 2d 55 53 3b 71 3d 30 2e 36 2c 65 6e 3b 71 3d n-US;q=0 .6,en;q=
00000150 30 2e 34 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0.4....

00000000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.
00000010 0a 44 61 74 65 3a 20 53 61 74 2c 20 31 32 20 4f .Date: S at, 12 0
00000020 63 74 20 32 30 31 33 20 30 33 3a 32 31 3a 35 37 ct 2013 03:21:57
00000030 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT..Sel rver: Ap
00000040 61 63 68 65 2f 32 2e 32 2e 32 32 20 28 55 62 75 ache/2.2 .22 (Ubu
00000050 6e 74 75 29 0d 0a 58 2d 50 6f 77 65 72 65 64 2d ntu)..X- Powered-
00000060 42 79 3a 20 50 48 50 2f 35 2e 33 2e 31 30 2d 31 30 By: PHP/ 5.3.10-1
```

Find Save As Print Entire conversation (3831 bytes) [v] ☐ ASCII ☐ EBCDIC ☒ Hex Dump ☐ C Arrays ☐ Raw

Help Close Filter Out This Stream

HTTP Request

HTTP Response



Wireshark

해킹을 시작해 봅시다

패킷패킷패킷 실제로 어떻게 생겼을까?

BUY 커맨드

- LOCO 서버 정보 및 소켓 요청
- non-secure 모드
 - 암호화 되지 않고 **LocoPacket** 형태로 그대로 전송됨

00000000	01	00	00	00	00	00	42	55	59	00	00	00	00	00	00	00BU Y.....		
00000010	00	00	64	00	00	00	64	00	00	00	12	75	73	65	72	49	..d...d. ...userI		
00000020	64	00											02	6f	73	00	03	00	d..... ..os...
00000030	00	00	77	70	00	10	6e	74	79	70	65	00	03	00	00	00	..wp..nt ype.....		
00000040	02	61	70	70	56	65	72	00	06	00	00	00	31	2e	30	2e	.appver.1.0.		
00000050	31	00	02	4d	43	43	4d	4e	43	00	01	00	00	00	00	02	1..MCCMN C.....		
00000060	63	6f	75	6e	74	72	79	49	53	4f	00	03	00	00	00	55	countryI SO.....U		
00000070	53	00	08	76	6f	69	70	00	00	00							S..voip. ..		

해킹을 시작해 봅시다

패킷패킷패킷 실제로 어떻게 생겼을까?

Handshake + LOGIN 커맨드

```
00000000 80 00 00 00 01 00 00 00 01 00 00 00 52 bf 59 05 .....R.Y.
00000010 0c 99 c0 a0 4b af 35 ba 66 3e de 6e 6f 72 b1 c5 ....K.S. f>.nor..
00000020 1e d6 b3 48 23 54 b7 01 0a e9 fd e4 e0 11 ed bb ...H#T.. ....
00000030 4c e5 04 4f 32 d6 29 d4 fa 55 9a 9b 62 7b ed 7b L..02.). .U..b{.{
00000040 7e 06 f6 a9 f1 0a 4a 2f 4a 28 fb 24 14 e4 6d 4d ~.....J/ J(.$..mM
00000050 30 2e 43 d7 ff 3f 6d 95 5f c2 3f 1a 1a 62 f7 08 0.C..?m. _.?..b..
00000060 cd 50 c4 00 23 d8 9c be a0 e8 46 5d 21 af 5c f5 .P..#... .F]!\.
00000070 ee 1c 24 43 a5 3c 10 2a 25 62 5d 4c 1c 17 1f a5 ..$C.<.* %b]L....
00000080 d9 15 63 a1 b5 f5 8c 91 1e ae cd b8 .....C.....
0000008C 10 01 00 00 75 b7 25 ac 8f d7 b9 53 f1 4d 5a 76 ....u.%. ...S.MZv
0000009C 31 b7 8e 9c 9f 8d 5e 7a b5 a6 22 19 f7 3b 3f d3 1....^z .."....;?.
000000AC 6c cc 54 65 d5 7b c3 5f 58 aa ac 61 59 8a 25 0c l.Te.{. _ X..aY.%.
000000BC d8 c7 85 46 6f 05 2d b2 86 dc 55 e6 87 0f 40 f2 ...Fo.-. .U...@.
000000CC 1e d0 9a fd 3a e0 a4 29 0c e8 25 dc 8d a9 b5 d4 .....) ..%.....
000000DC d5 ac e9 57 d6 23 2d 4f 07 13 97 7c 15 81 a9 36 ...W.#-0 ...|...6
000000EC 1d 78 4a 6d 99 14 db c9 59 3d f8 c8 87 36 76 02 .xJm.... Y=...6v.
000000FC c1 23 6c 05 26 f3 24 e7 52 f9 59 39 33 98 b0 55 .#l.&$. R.Y93..U
0000010C 6e cd 71 73 ef 49 22 f7 f6 73 12 e9 9e a9 c7 cb n.qs.I". .s.....
0000011C 5f d6 6d 75 f7 c7 d3 c0 21 72 51 6d f7 b0 17 ff _mu.... !rQm....
0000012C 08 8f 23 e3 a0 66 3d d1 2e 93 41 61 67 23 8b 99 ..#...f=. ..Aag#..
0000013C 55 7c 80 c4 1f b5 54 9d dd 2c de d5 1b d4 14 ba U|....T. ,.....
0000014C aa 79 98 f5 b8 b6 60 96 19 01 d8 3a 21 59 e1 6a .y....` . ...!Y.j
0000015C d1 58 92 76 ce a3 e7 14 3d 20 ac a1 76 91 3f 42 .X.v.... = .v.?B
0000016C b4 38 f4 3a 25 57 05 30 b1 f2 7f e3 3f 48 16 78 .8.:%W.0 ....?H.x
0000017C 7f d2 21 eb d0 3f 62 88 34 7a 76 c7 b6 8e b3 03 ..!...?b. 4zv....
0000018C 77 97 53 cb 3c 90 eb f6 22 06 a9 05 a5 66 12 23 w.S.<.... "....f.#
0000019C e7 9f 94 e0 .....
00000000 60 00 00 00 75 b7 25 ac 8f d7 b9 53 f1 4d 5a 76 `....u.%. ...S.MZv
00000010 31 b7 8e 9c 7f b1 f4 37 b6 38 37 da 44 c2 fe bb 1.....7 .87.D...
00000020 56 5b ba d0 b5 09 37 03 b1 2e 8b 85 9d 78 5c 5b V[....7. ....x\[
00000030 57 bf 43 74 18 e1 9f 98 ab 54 37 37 10 8f df f6 w.Ct.... .T77....
00000040 f9 17 21 3c 22 57 6d 39 3f d1 a7 ca 1c 97 06 50 ..!<"Wm9 ?.....P
00000050 08 b4 81 44 f3 42 1f b4 ff 42 f0 ad 09 cd 36 39 ...D.B.. .B....69
00000060 3b 45 51 75 ;Equ
000001A0 60 00 00 00 7f 9c a3 31 f0 7a dd 5d 17 e6 c2 a7 `.....1 .z.]....
000001B0 63 96 1e ba b6 d6 43 ba de de 98 06 62 95 d7 ed c.....C. ....b...
```

Handshake
with RSA
encrypted
AES key

AES
Encrypted
Login

AES
Encrypted
Response

카카오톡으로 여친 만들기

이제 남은건?

이제 남은건?

카카오톡으로 여친 만들기

po코딩wer

이제 남은건?
po코딩wer

```
carpedm20@MSNL: ~/command

succ = send(s, data)
return succ

#[READ] {u'since': 0L, u'chatId': 55912035628534L}
def read(s, chatId = 50227792383031L, since = 462937779245527040L):
    print " [*] READ from " + str(chatId)

    data = '\x06\x00\x00\x00' # Packet ID
    data += '\x00\x00' # Status Code : when sending command -> 0
    data += 'READ\x00\x00\x00\x00\x00\x00' # Method
    data += '\x00' # Body Type : when sending command -> 0

    body = BSON.encode({u'chatId': chatId, u'since': since})

    data += body[:4]
    data += body

    succ = send(s, data)
    return succ

def write(s, chatId = 50227792383031L, msg = u'test'):
    try:
        print " [*] WRITE to " + str(chatId) + " : " + str(msg)
    except:
        print " [*] WRITE to " + str(chatId) + " : ???"

    data = '\x06\x00\x00\x00' # Packet ID
    data += '\x00\x00' # Status Code : when sending command -> 0
    data += 'WRITE\x00\x00\x00\x00\x00\x00' # Method
    data += '\x00' # Body Type : when sending command -> 0

    # print msg

    body = BSON.encode({u'chatId': chatId, u'msg': msg, u'extra': None, u'type':
1})

    data += body[:4]
    data += body

    succ = send(s, data)
    return succ

#http://dn-m.talk.kakao.com/talkm/oWduQM37UX/PLQiP0Jjbt4vSb1dKGdK0K/39qkgm.jpg
384,5 60%
```

이제 남은건?
po코딩wer

수많은것이
가능합니다.
헥사봇이
있기에.

!사진 명령어로 여러분이 보고싶은
사진을 카카오톡에서 바로 보세요.
헥사봇에게 말을 거세요. 물론 날씨와
버스 시간표도 물어볼 수 있습니다.
헥사봇보다 좋은건 헥사봇으로 즐기는
모든것 뿐입니다.

제작자 : 김태훈(carpedm20)

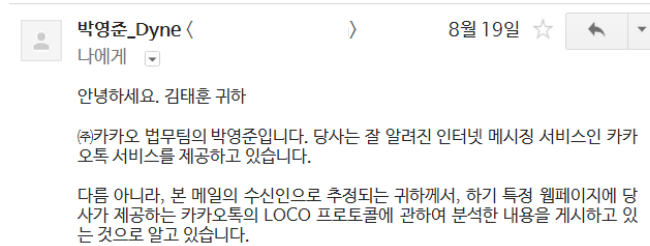


이제 남은건?
po코딩wer

Demo

소스코드는 안알라줌 ㅋ

이제 남은건?
po코딩wer



<https://pypi.python.org/pypi/kakao/1.0.0>

카카오톡한테는 비밀!



이제 남은건?
po코딩wer

끝

And?