CCIT 네트워크 발표

- 평문 사이트와 SSL 사이트,
- SSL strip과 데이터 변조를 이용한 로그인 취약점

정보보호학과

강보경
정영호

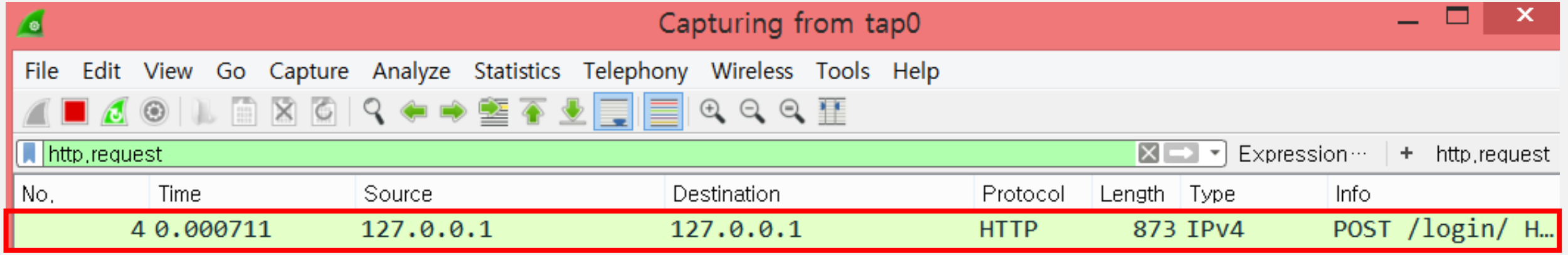
Contents

평문 사이트 로그인

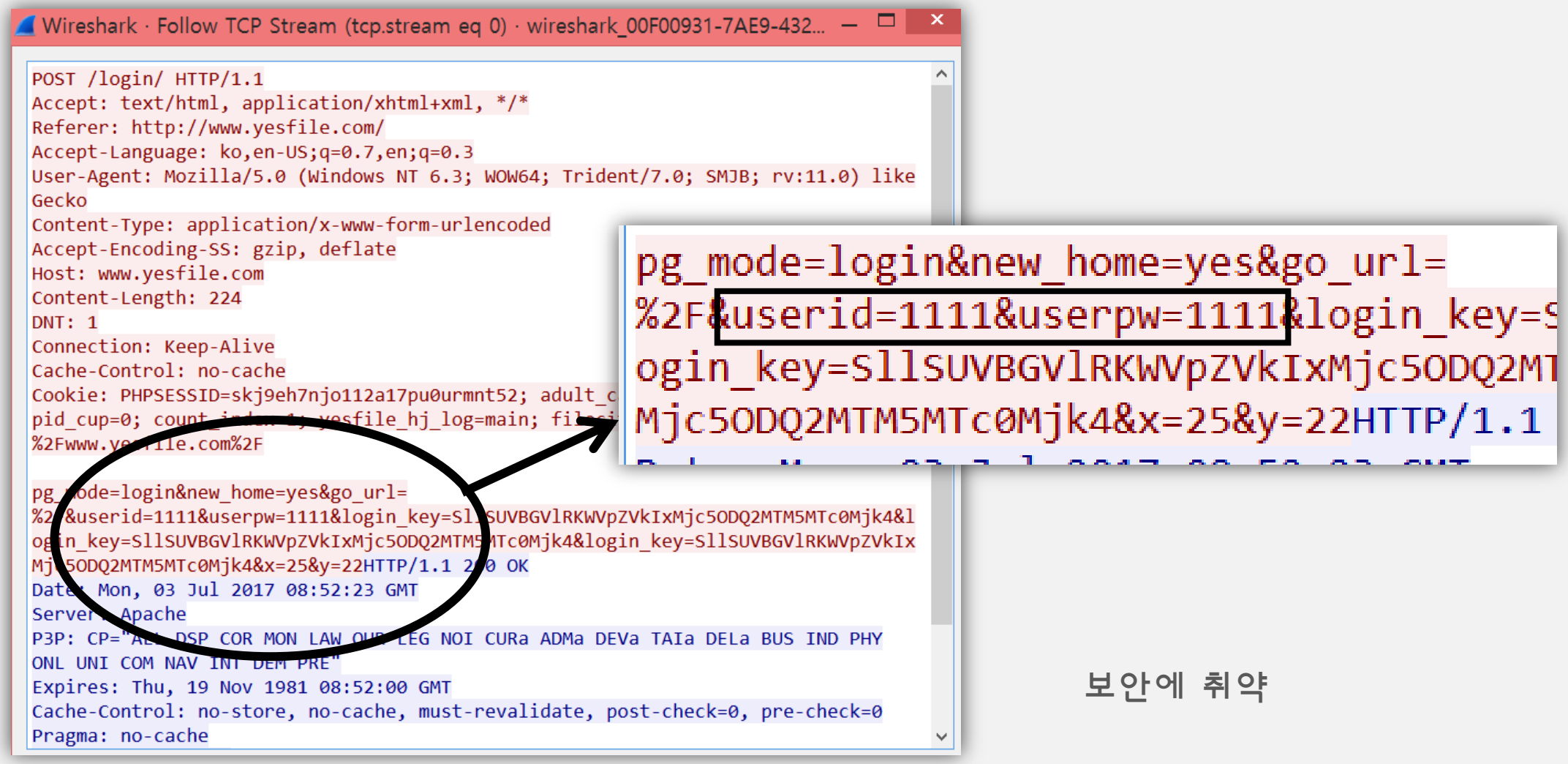
1. 평문 사이트 로그인

P2P 사이트 취약

2. 와이어샤크로 패킷 확인



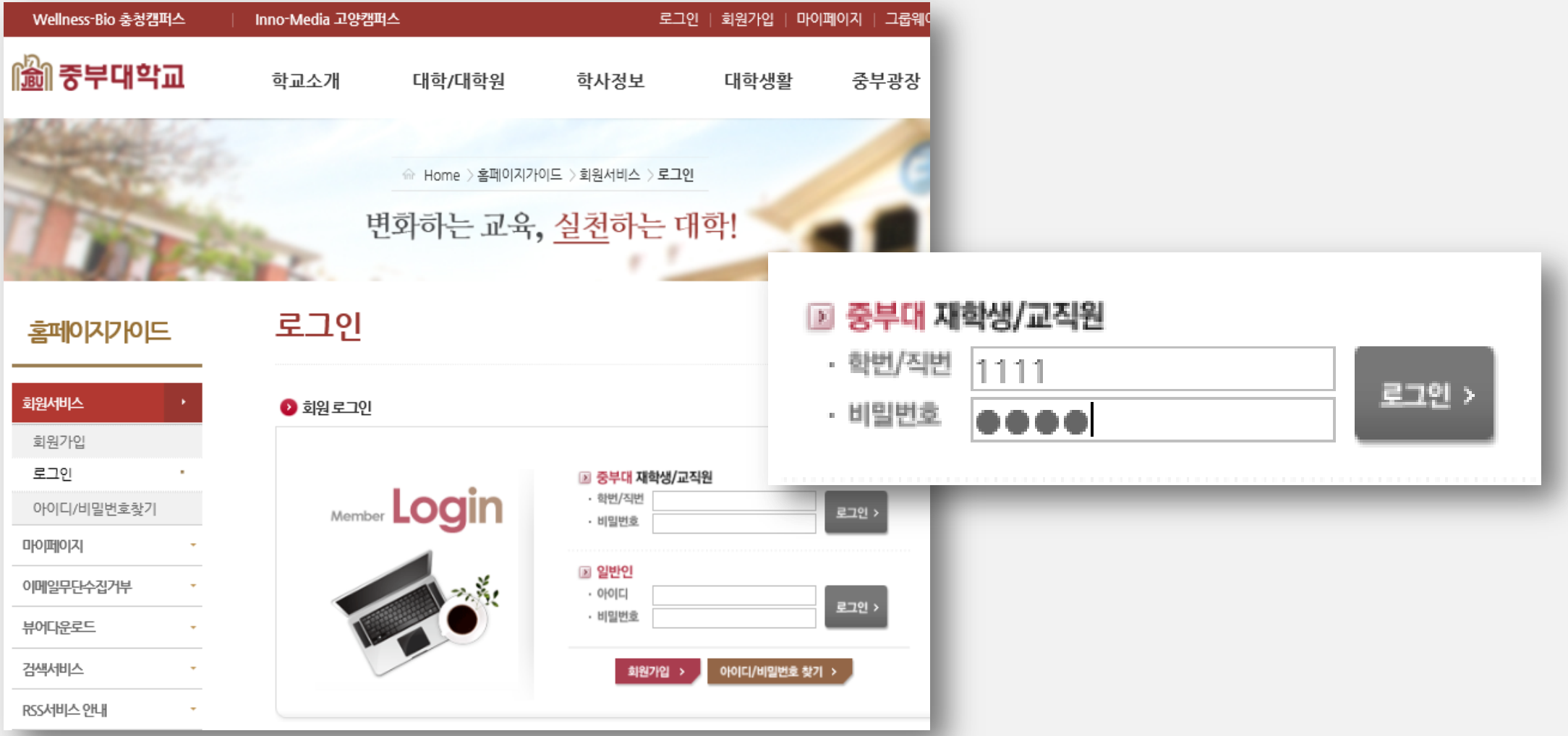
2. 와이어샤크로 패킷 확인



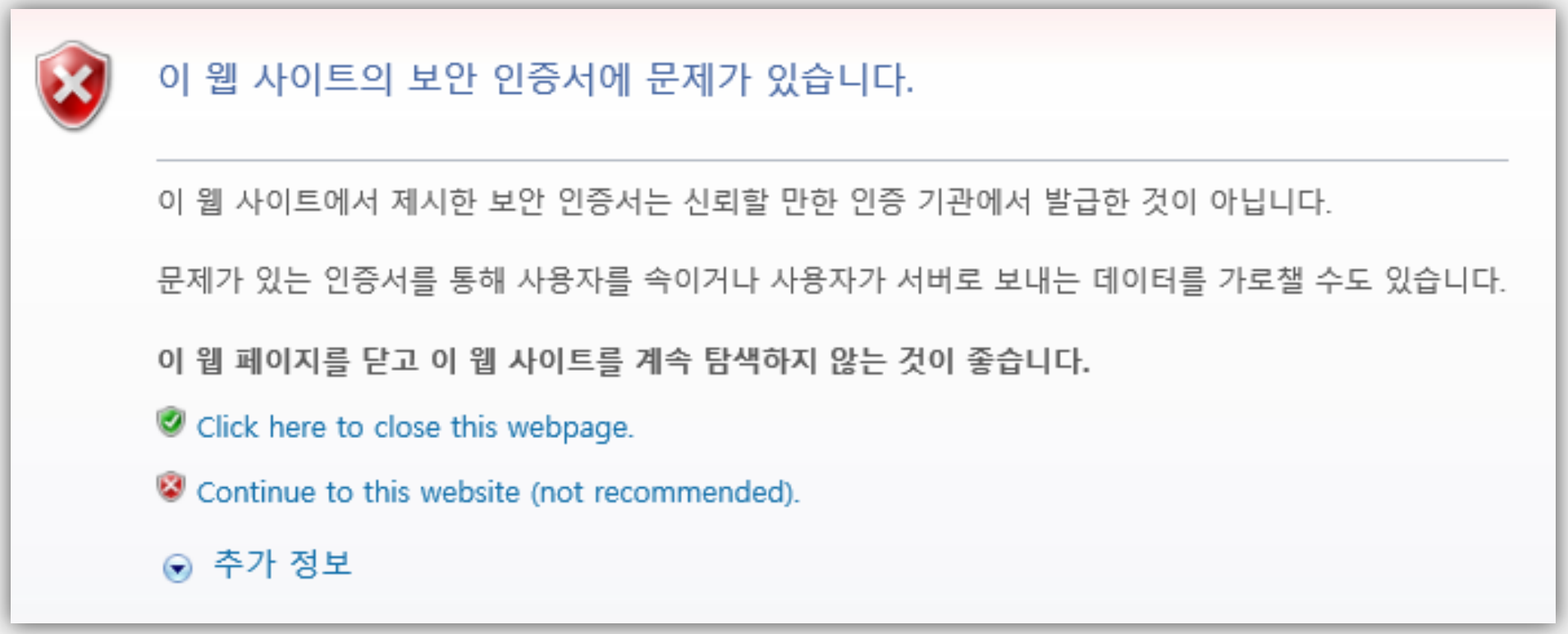
보안에 취약

SSL 통신

1. SSL 사이트 로그인

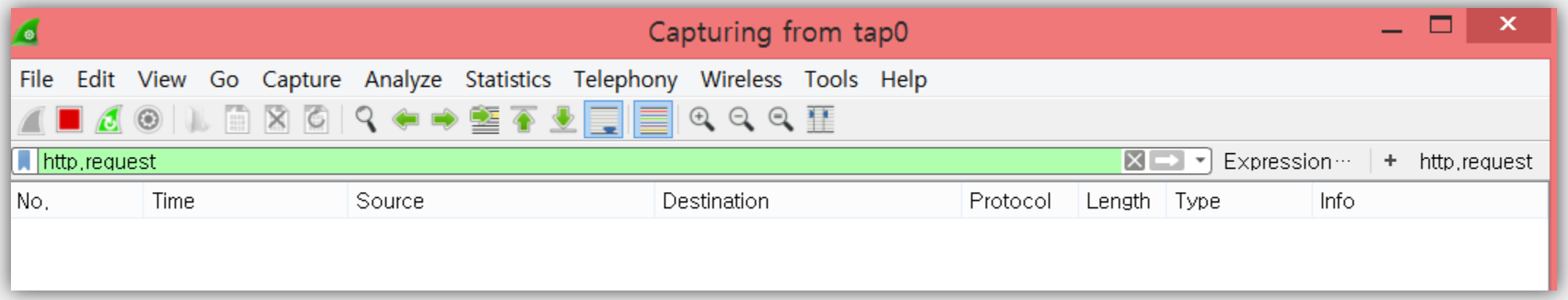

Wellness-Bio 충청캠퍼스
Inno-Media 고양캠퍼스
로그인 | 회원가입 | 마이페이지
중부대학교
학교소개
대학/대학원
학사정보
대학생활
중부광장
Home > 홈페이지가이드 > 회원서비스 > 로그인
변화하는 교육, 실천하는 대학!
홈페이지가이드
회원서비스
회원가입
로그인
아이디/비밀번호찾기
마이페이지
이메일무단수집거부
뷰어다운로드
검색서비스
RSS서비스 안내
로그인
회원 로그인
Member Login
중부대 재학생/교직원
학번/직번
비밀번호
로그인 >
일반인
아이디
비밀번호
로그인 >
회원가입 >
아이디/비밀번호 찾기 >
중부대 재학생/교직원
학번/직번
1111
비밀번호
로그인 >

1. SSL 사이트 로그인



사용자가 다음으로 넘어갈 수 있도록 선택할 수 있게 해주고

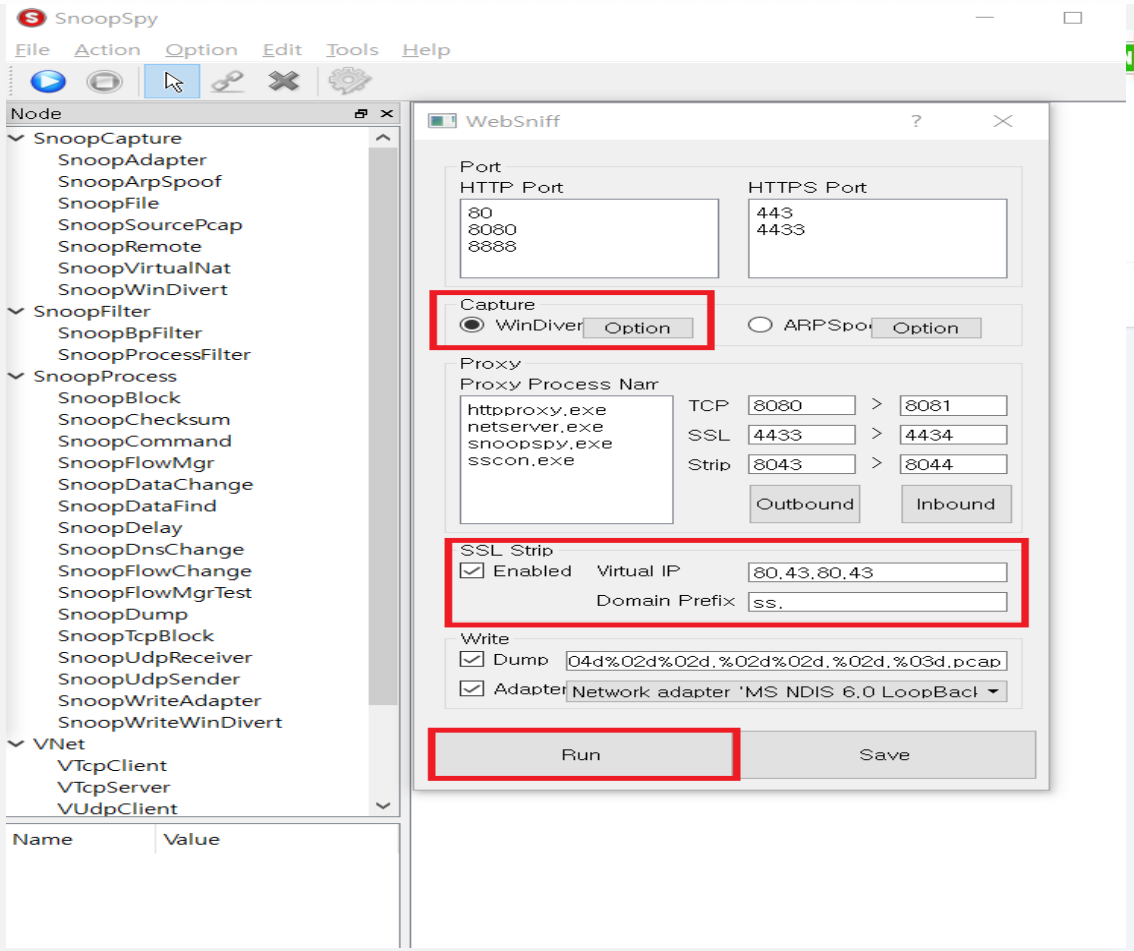
2. 와이어샤크로 패킷 확인



다음으로 넘어가지만 않는다면
SSL 통신이기 때문에 로그인 했을 때의 패킷이 보이지 않는다.

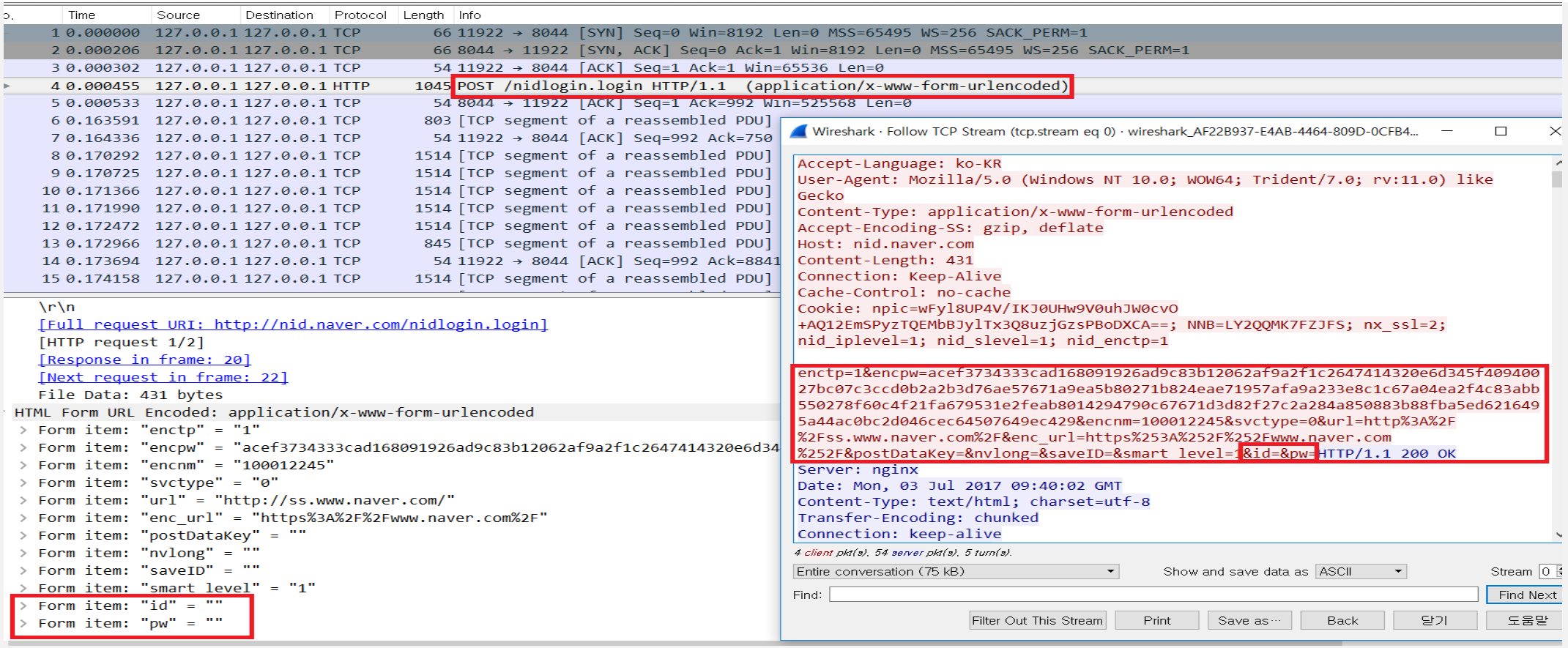
SSL Strip + 데이터 변조

1. SSL 사이트(네이버) 로그인



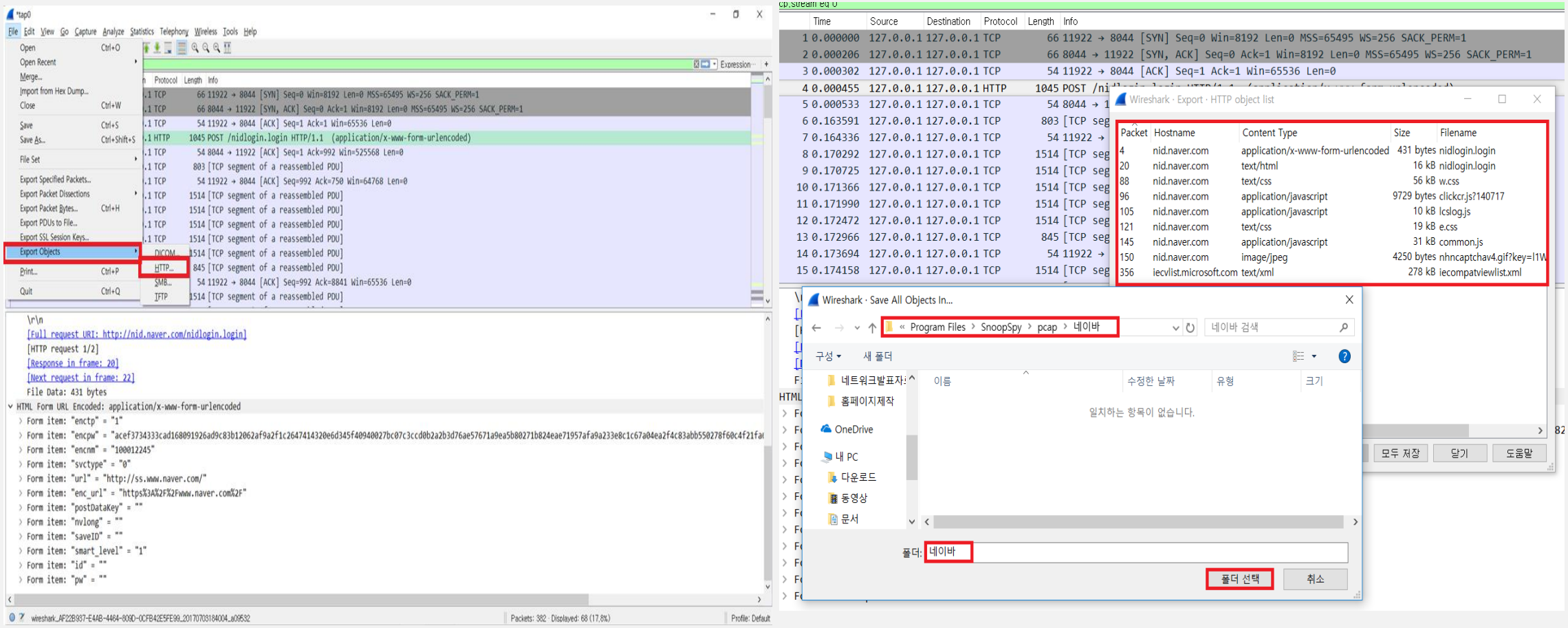
SSL Strip 공격으로 해당 ID(hohohohoho) 와 PW(0505050505)로 네이버에 로그인을 시도한다.

2. 와이어샤크로 패킷 확인

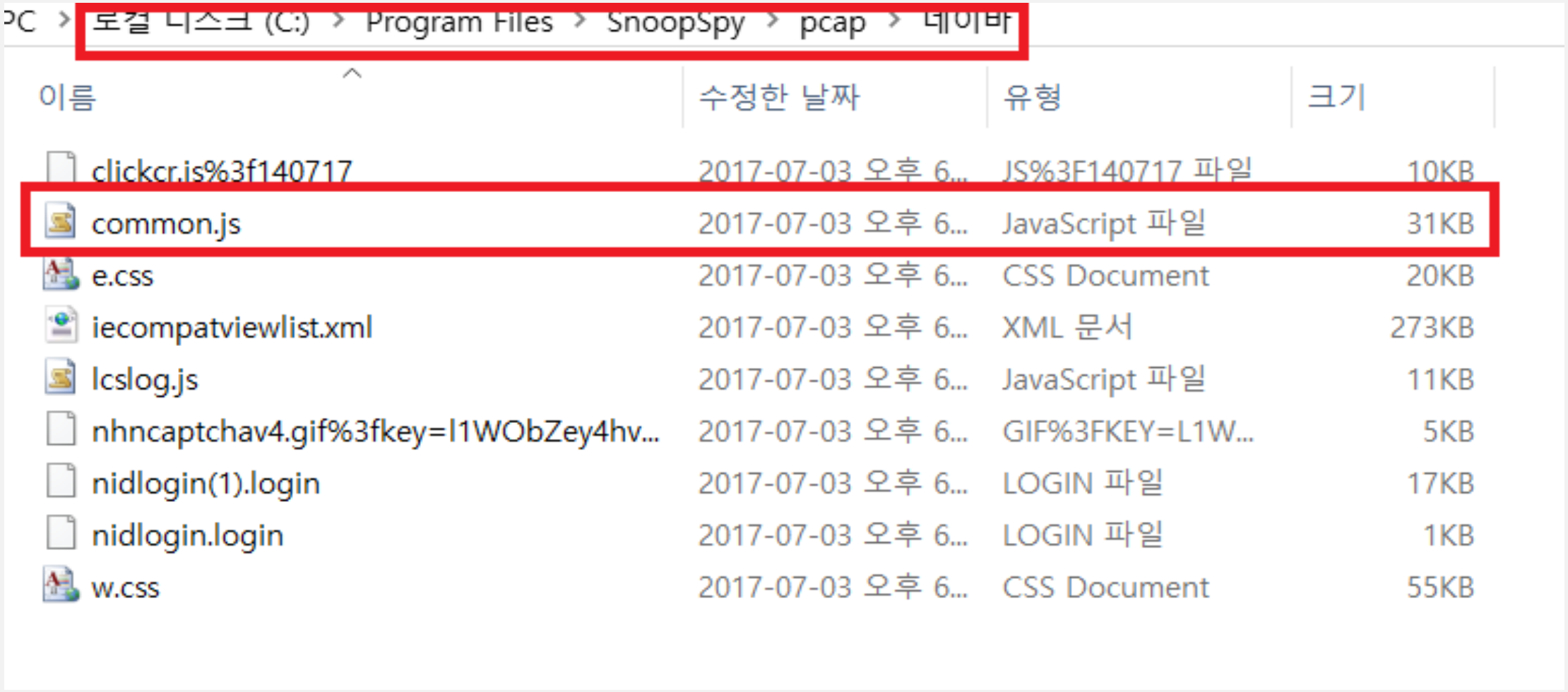


하지만 난독화가 되어있기 때문에 아이디와 패스워드가 보이지 않는다.

3. 오브젝트(http) 분석 및 수정



해당 오브젝트를 분석하기 위해 http로 Export 하여 네이바 폴더에 저장한다.



java script 파일을 열어서 코드를 분석해 본다.

```
function encryptIdPw() {
    var id = $("id");
    var pw = $("pw");
    var encpw = $("encpw");
    var rsa = new RSAKey;

    if (keySplit(session_keys)) {
        rsa.setPublic(evalue, nvalue);
        try{
            encpw.value = rsa.encrypt(
                getLenChar(sessionkey) + sessionkey +
                getLenChar(id.value) + id.value +
                getLenChar(pw.value) + pw.value);
        } catch(e) {
            return false;
        }
        $('enctp').value = 1;
        id.value = "";
        pw.value = "";
        return true;
    }
    else
    {
        getKeyByRuntimeInclude();
        return false;
    }

    return false;
}
function getKeyByRuntimeInclude() {
    try {
        var keyjs  = document.createElement('script');
        keyjs.type = 'text/javascript';
        keyjs.src = '/login/ext/keys_js2.nhn';
        document.getElementsByTagName('head')[0].appendChild(keyjs);
    } catch (e) {
    }
}
function clearErrorLayers() {
  var errors = new Array('err_empty_captcha', 'err_autologin', 'err_network_delay',
      'err_unsupport_browser', 'err_empty_id', 'err_empty_pw', 'err_idpw_incorrect',
```

encrpytIdPw 함수에 id.value와 pw.value 값을 공백으로 바꿔주는 코드가 확인되었다.

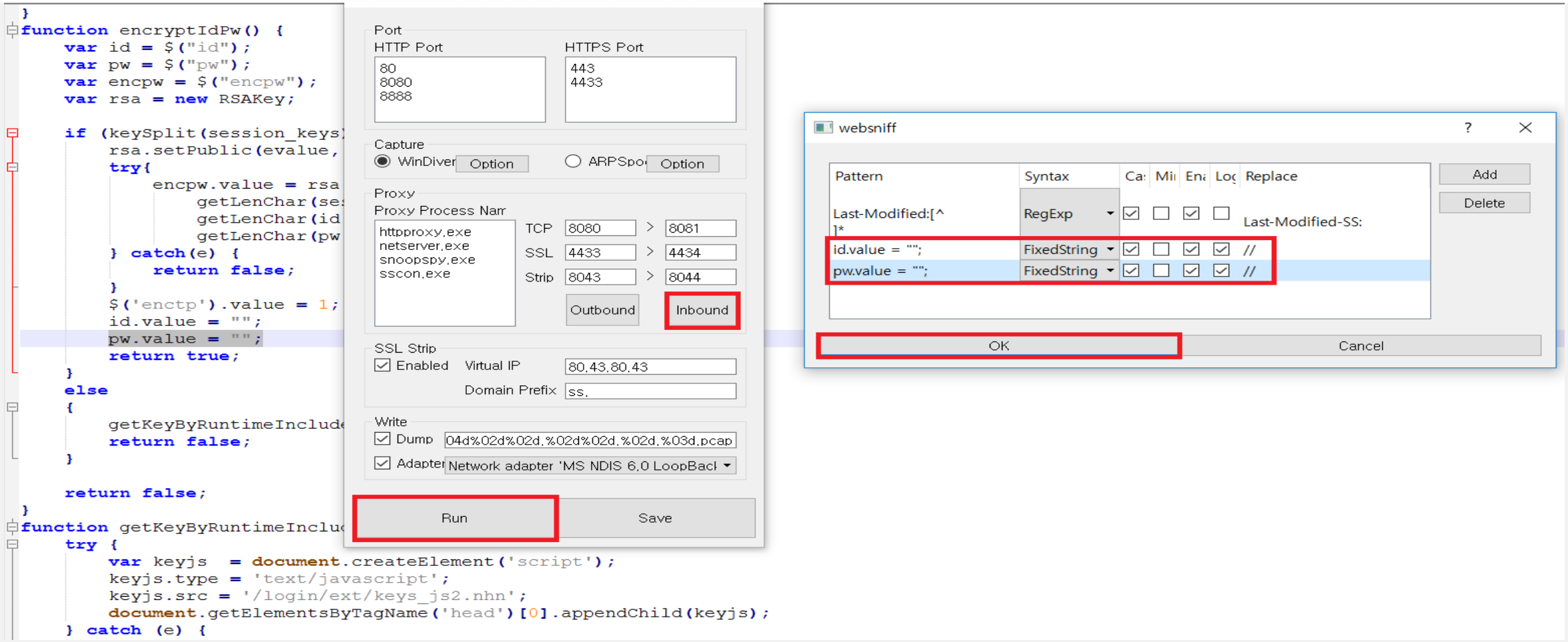
4. 암호화 코드 설명

```
function encryptIdPw() {
    var id = $("id");
    var pw = $("pw");
    var encpw = $("encpw");
    var rsa = new RSAKey;

    if (keySplit(session_keys)) {
        rsa.setPublic(evalue, nvalue);
        try{
            encpw.value = rsa.encrypt(
                getLenChar(sessionkey) + sessionkey +
                getLenChar(id.value) + id.value +
                getLenChar(pw.value) + pw.value);
        } catch(e) {
            return false;
        }
        $('enctp').value = 1;
        id.value = "";
        pw.value = "";
        return true;
    }
    else
    {
        getKeyByRuntimeInclude();
        return false;
    }

    return false;
}
```

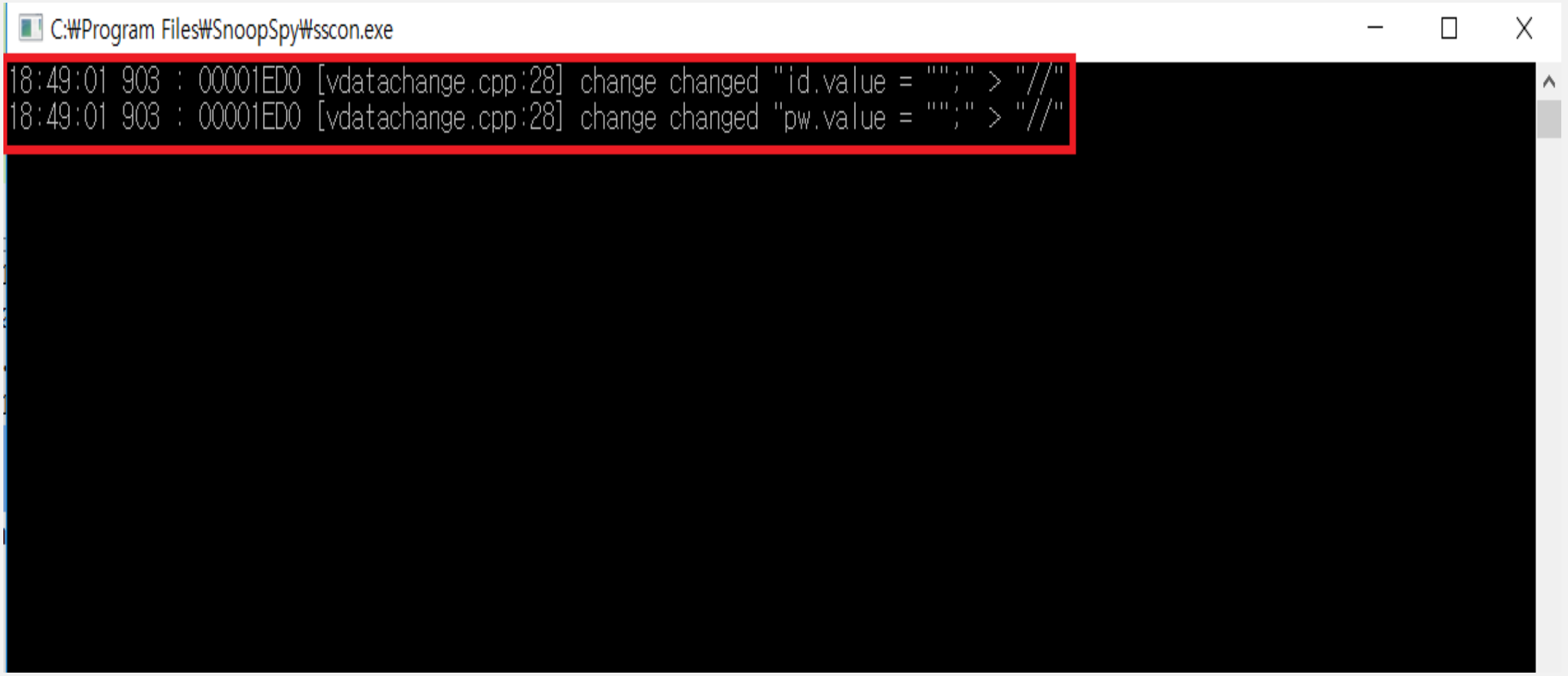
```
Content-Length: 431
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: npic=wFyl8UP4V/IKJ0UHw9V0uhJW0cvO
+AQ12EmSPyzTQEMbBJylTx3Q8uzjGzsPBoDXCA==; NNB=LY2QQMK7FZJFS; nx_ssl=2;
nid_iplevel=1; nid_slevel=1; nid_enctp=1

enctp=1&encpw=acef3734333cad168091926ad9c83b12062af9a2f1c2647414320e6d345f409400
27bc07c3ccd0b2a2b3d76ae57671a9ea5b80271b824eae71957afa9a233e8c1c67a04ea2f4c83abb
550278f60c4f21fa679531e2feab8014294790c67671d3d82f27c2a284a850883b88fba5ed621649
5a44ac0bc2d046cec64507649ec429&encnm=100012245&svctype=0&url=http%3A%2F
%2Fss.www.naver.com%2F&enc_url=https%253A%252F%252Fwww.naver.com
%252F&postDataKey=&nvlong=&saveID=&smart level=1&id=&pw=HTTP/1.1 200 OK
Server: nginx
Date: Mon, 03 Jul 2017 09:40:02 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive

4 client pkt(s), 54 server pkt(s), 5 turn(s).
```

예를 들어 id=AAA와 pw=BBB를 사용했을 경우 패킷이 id=AAA, pw=BBB이며 그 뒤에 해당 pw가 난독화된 문자가 들어간다. 난독화되기 전의 정보가 패킷 앞에 남아있으므로 해당 함수는 난독화되기 전의 정보인 AAA, BBB를 공백으로 만들어주는 함수이다. 그러므로 해당 부분을 제거해주면 아이디와 패스워드가 공백처리 되지 못하고 그대로 나타나게 된다.

5. 데이터 변조

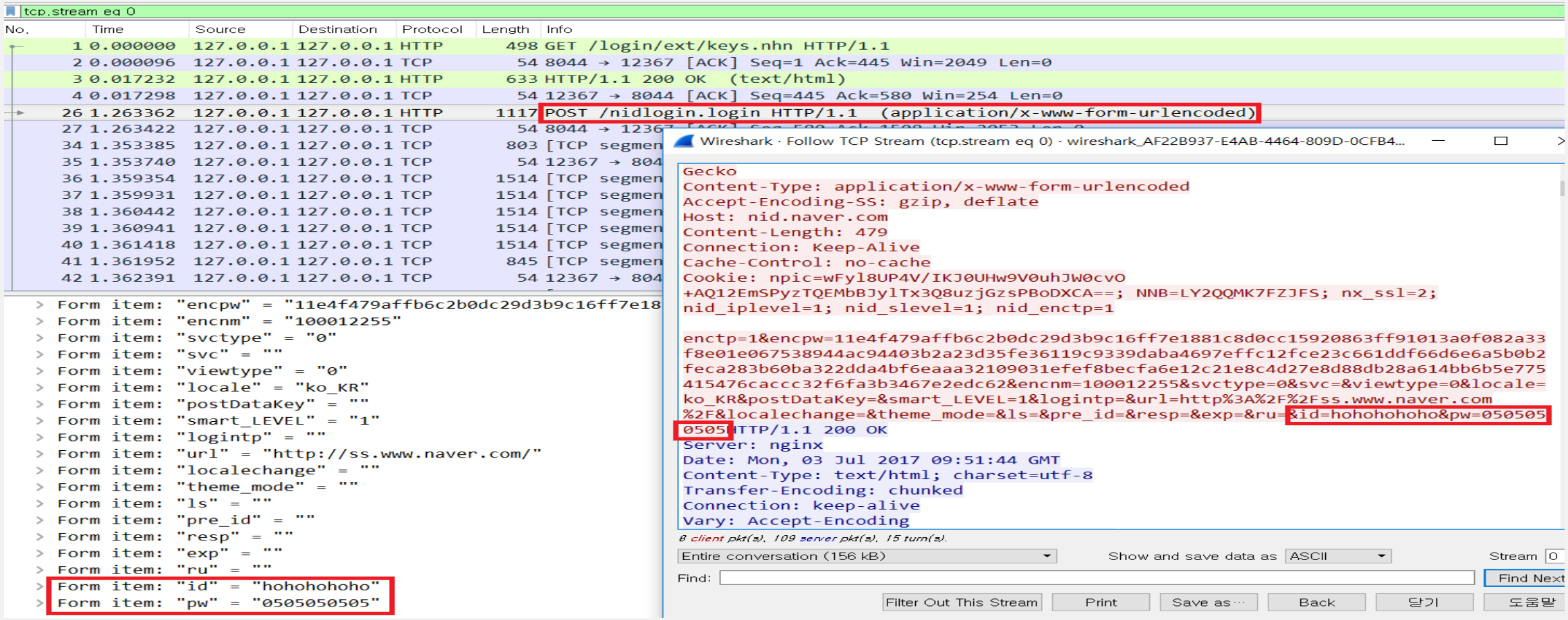


해당 코드를 데이터 변조를 사용하여 주석으로 바꿔준다. (해당코드 무효화)



다시 로그인 시, 데이터가 변조 되는 것을 확인

6. 와이어 샤크로 패킷 확인



SSL Strip 공격만으로 보이지않던 id, pw가 데이터 변조로 노출되는 것을 와이어 샤크에서 확인됨

7. 시연 영상

https://youtu.be/DoDnSt1Kggk