



482-110 경기도 양주시 삼승로 31 (전화) 070-7797-2583 (문의) news.pcis@daum.net
대표 : 손영준 <http://cafe.daum.net/pcis>

수 신 : 각 언론사 경제, 사회부, NGO담당기자
발 신 : 정보화사회실천연합
문 의 : 손영준 T. 010-8677-9515
시 행 일 : 2013. 03. 14.(목)
제 목 : [보도자료] 소액결제시 개인정보보호 실태조사 (총 7페이지)

소액결제시 개인정보 여전히 불안

소액결제시 '집전화' 방식 절반의 안전 방통위의 실효적 행정조치 필요

1. 스미싱(Smishing)에 의한 휴대전화 소액결제 사기는 유출된 개인정보를 이용하여 인지도가 높은 기업을 사칭하여 '무료쿠폰' '모바일 상품권 도착' 등 메시지를 보내 사용자로 하여금 악성어플의 설치를 유도하여 피해자 몰래 게임아이템 등을 구매하여 소비자에게 금전적인 피해를 입히는 사례로서 개인정보유출로 인한 대표적인 2차 피해 사례로 개인정보보호의 중요성을 보여주는 사건입니다.

2. 이에 정보화사회실천연합(이하 정실련)은 기업의 개인정보보호에 대한 문제점 및 정보통신망법 위반행위 근절을 위하여 2013.02.20.부터(10일간) 20~30대가 가장 많이 이용하는 다운로드(P2P) 사이트 40개를 무작위로 선정하여 개인정보보호 실태조사를 하였습니다.

3. 실태조사는 외부에서 개인정보보호의 척도를 확인할 수 있는 유일한 방법인 "개인정보의 보호조치"사항 중 기술적 조치에 속하는 전송구간 암호화(보안서버구축, SSL) 적용 여부에 대하여 조사를 실시하였습니다.

4. 관련법령

- "정보통신망 이용촉진 및 정보보호 등에 관한 법률"(이하 정보통신망법)

제28조(개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

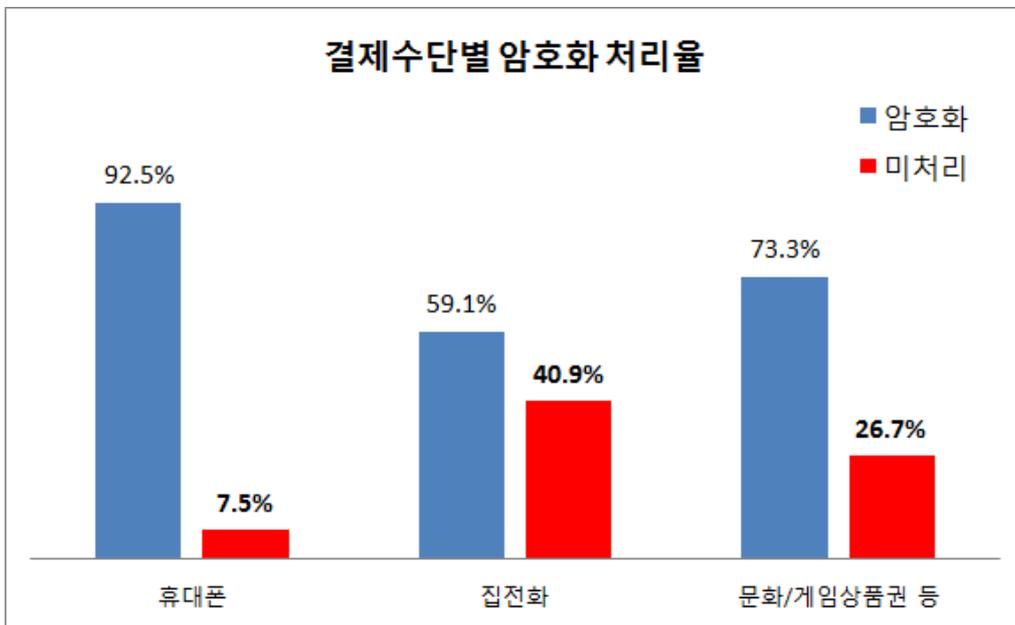
제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다. <개정 2011.3.29, 2012.2.17>

2. 제23조의2제1항을 위반하여 주민등록번호를 수집·이용하거나 같은 조 제2항에 따른 필요한 조치를 하지 아니한 자(제67조에 따라 준용되는 경우를 포함한다)
3. 제28조제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 아니한 자

5. 조사결과, 첫째, ‘집전화를 이용한 소액결제’의 암호 적용율이 59.1%를 보여 가장 심각한 사례로 나타났습니다.

- 소액결제수단의 전체 평균 암호화 처리율은 73.0%로 나타났으며, ‘휴대폰소액결제’는 최근 각 언론사의 스미싱 관련 언론보도 이후 많은 보완(조사기간 중 조치율 7.5%)이 이루어져 92.5%가 적용되었으나, ‘집전화’를 이용한 소액결제는 59.1%로 매우 저조한 암호화율을 보였습니다.

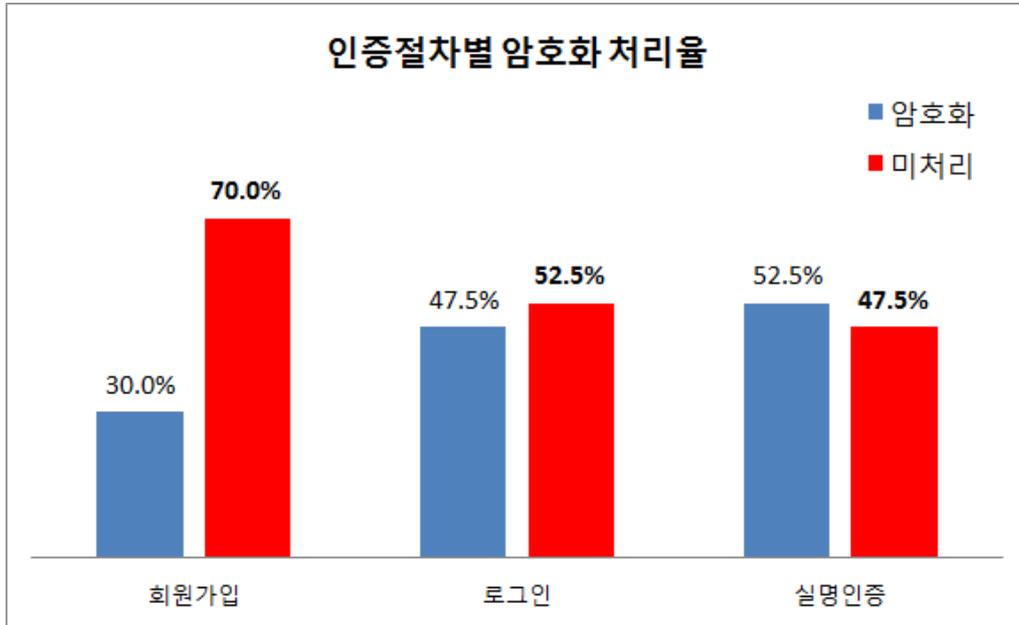
<도표 1. 결제수단별 개인정보 암호화 처리율>



6. 둘째, 인증절차별로는 회원가입시 30.0%의 암호화 처리율에 그친 것으로 나타났습니다.

- 인증절차별 평균 암호화 적용이 43.3%만이 준수하는 것으로 조사되었습니다. 다운로드(P2P)사이트의 특성상 ‘회원가입’시 민감한 개인정보는 취급하지 않으나 비밀번호는 암호화 대상임에도 기업의 개인정보보호에 대한 인식이 심각한 수준임을 보여주고 있습니다.

<도표 2. 인증절차별 개인정보 암호화 처리율>

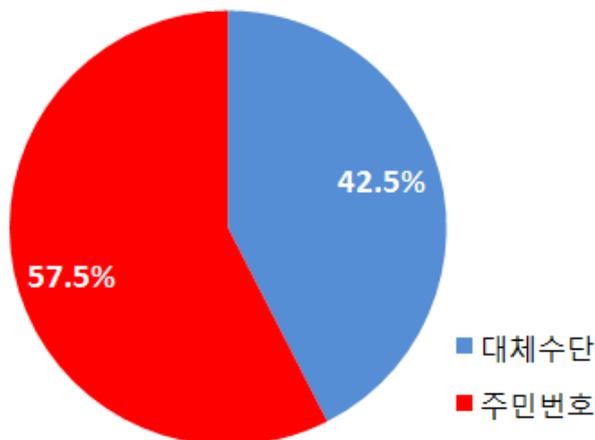


7. 셋째, “주민등록번호 수집 및 이용중단”의 경과조치기간(2013년2월17일) 이후 조사대상의 43%만이 대체수단을 제공하고 있습니다.

- 개정된 “정보통신망법 제23조의2(주민등록번호의 사용 제한) 경과조치(2012.2.17.)”이후 ‘주민등록번호’를 사용하지 않고 실명인증을 할 수 있도록 하는 대체수단(‘아이핀’, ‘휴대전화’, ‘신용카드’ 등)의 실명인증방식을 제공하는 사이트는 조사대상의 43%만이 제공하고 있었습니다.

<도표 3. 실명인증시 주민등록번호 대체수단 제공율>

실명인증 대체수단 제공율



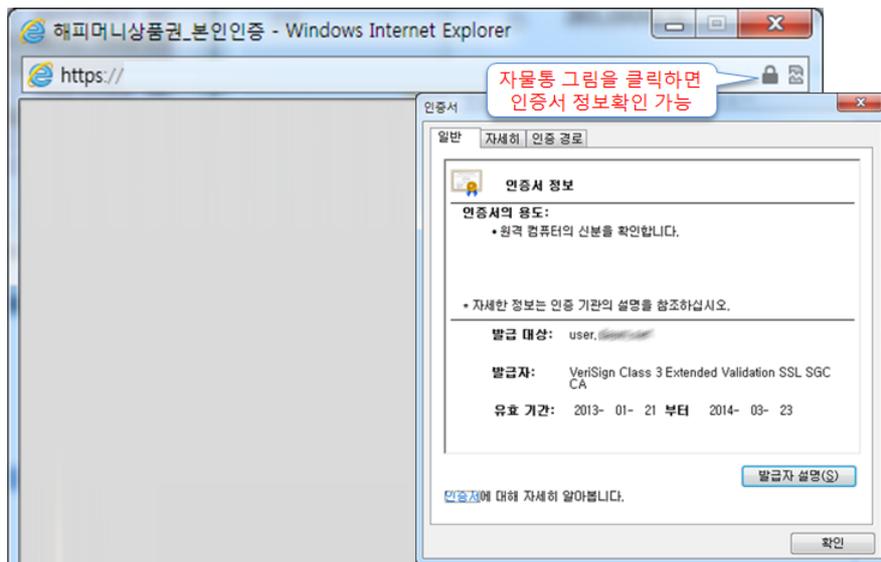
8. 소액결제시 입력된 개인정보를 암호화(https:..)처리를 안 하고 전송 하면 스니핑(Sniffing : 네트워크상에 흘러가는 정보를 수집하는 네트워크 도청 방법)과 같은 해킹방법에 의하여 손쉽게 대량의 개인정보가 수집될 수 있어 개인정보 유출의 위험성이 높은 보안 취약점입니다.

<그림 1. 전송구간 암호화 비교 도식>



또한 소비자에 대한 신뢰도를 높이기 위해서는 부분처리 암호화 방식(웹페이지 내의 개인정보 부분만 'https://'로 처리)이 아닌 웹페이지 암호화 방식(웹 페이지를 'https://'로 처리하면 브라우저에 '자물통 그림'이 나타남)으로 적용하여 암호화 처리 상태를 사용자가 가시적으로 확인할 수 있도록 처리하는 것이 기업의 신뢰도를 높이는 차원에서도 반드시 브라우저에 '자물통 그림' 나타나도록 처리하는 것을 권고합니다.

<그림 2. 전송구간 암호화 적용 화면 사례>



정실련은 이번 조사결과에서 나타났듯 기업의 개인정보보호에 대한 낮은 인식으로 인하여 또 다른 2차, 3차의 보이스포싱, 스미싱과 같은 피해사태가 일어나지 않을까 우려스럽습니다.

끝으로 국민의 개인정보보호를 위반하는 기업의 불법행위 근절에 대한 실효성 확보를 위하여 주무관청인 방송통신위원회는 실효성 있는 행정조치를 실천에 옮겨야 할 것입니다.

다운로드(P2P) 사이트의 개인정보보호 실태조사 (2013.02.20.~2013.03.02)

1. 조사배경 및 목적

- 최근 스미싱으로 휴대폰소액결제피해가 급증하여 소액결제의 이용이 높은 다운로드(P2P) 사이트에 대하여 긴급 실태조사를 실시하여 기업의 개인정보보호에 대한 인식을 높이며, 주무관청의 실효성 있는 행정권의 행사를 촉구함으로써 개인정보보호 위반행위가 줄어들기를 기대함.

2. 조사대상과 방법

1) 조사대상

- 2013년 2월 20일부터 2013년까지 03월 02일까지 포털 검색을 통하여 무작위로 선정한 다운로드(P2P) 사이트를 조사 대상으로 함.

2) 조사내용과 방법

- 선정된 다운로드(P2P) 사이트에 회원가입을 하여 개인정보를 취급하는 웹 페이지에 대하여 패킷수집도구('와이어샤크')를 사용하여 개인정보 처리 상태를 확인하는 방법으로 개인정보의 전송구간 암호화(https) 여부를 조사. 분석함.

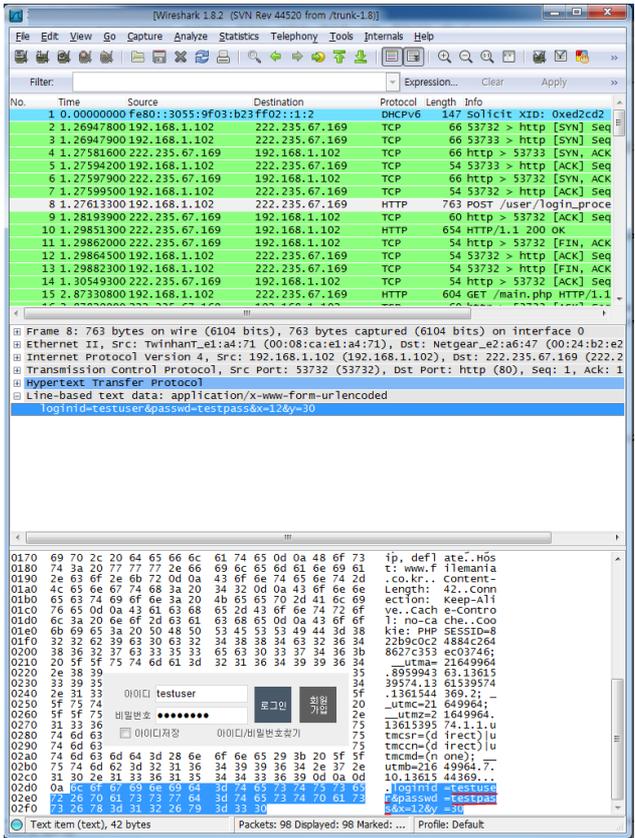
○ 조사내용

1. 인증절차(로그인, 회원가입, 실명인증)시 암호화 처리 여부
 2. 소액결제유형별 취급 개인정보의 암호화 처리 여부
 - 휴대폰소액결제 : 통신사, 휴대전화번호, 주민등록번호, 메일주소
 - 집전화결제 : 전화번호, 주민등록번호, 메일주소
 - 문화/도서상품권 결제 : 상품권 발행 업체 사이트의 아이디, 비밀번호
- *) 신용카드 등 금융권을 통한 링크방식은 암호화 처리를 하고 있어 대상에서 제외, 포인트(OK캐시백 등) 결제수단은 업체별로 적용빈도가 낮아 조사대상에 제외함.
3. 주민등록번호를 사용하지 않고 성인인증을 할 수 있는 대체수단의 제공 여부.

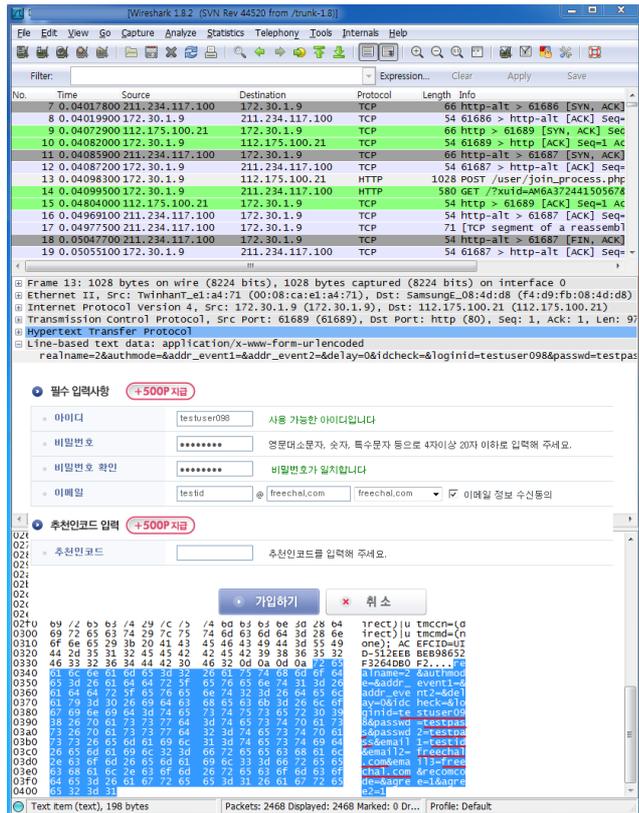
3) 위반 사례 화면

*) 파란색 내용에서 붉은색 언더라인 부분이 전송구간 암호화(SSL)를 적용하지 않아 개인정보가 노출된 부분입니다

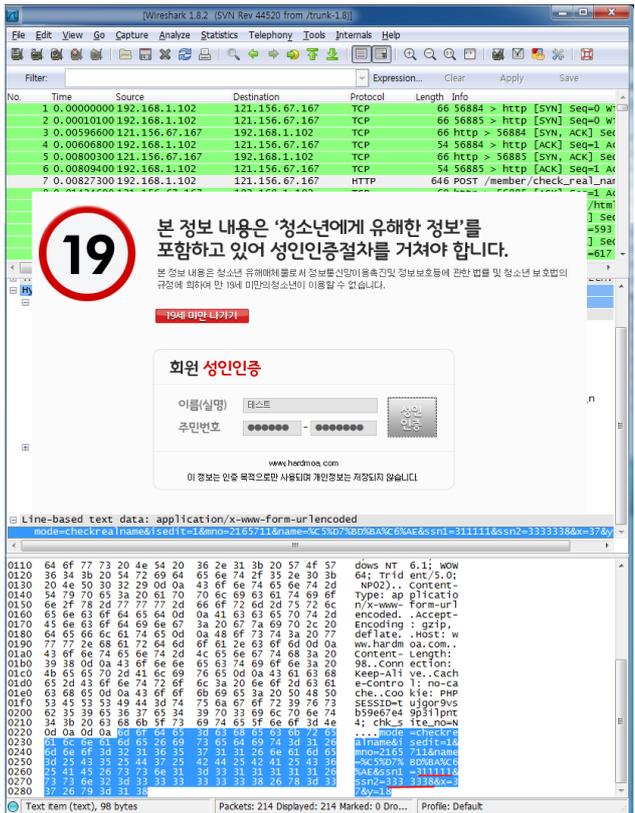
로그인



회원가입

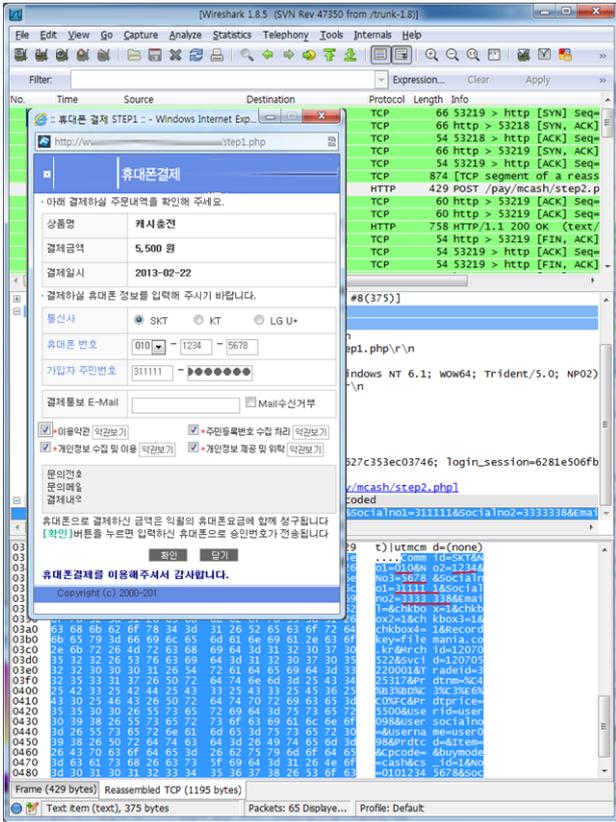


성인인증

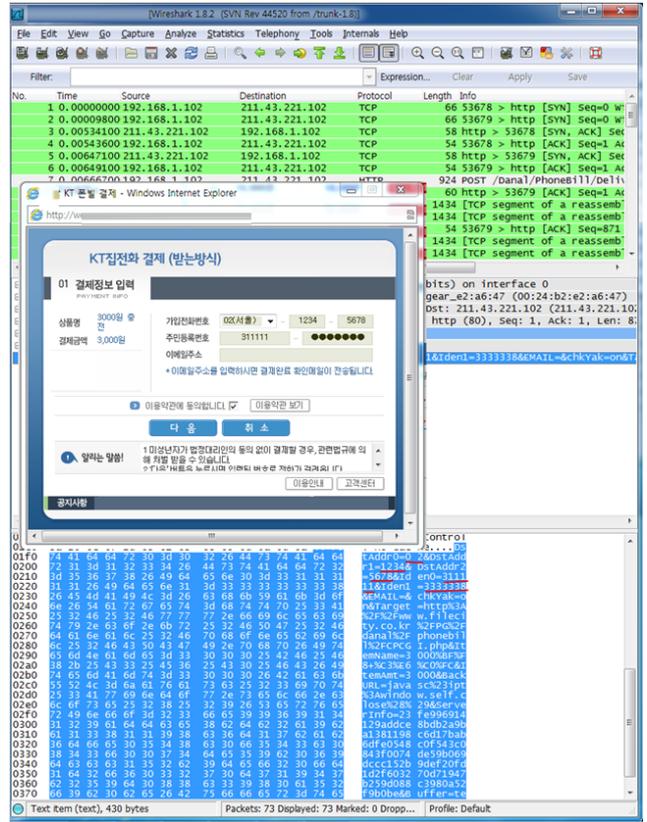


시민의 힘으로 안전한 정보화 사회 위하여 노력하는 시민단체

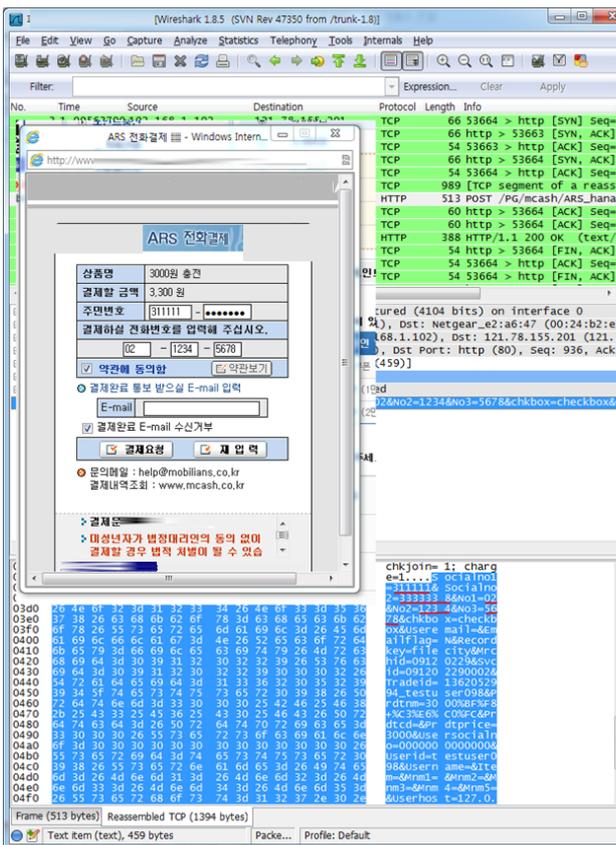
휴대폰소액 결제



집전화 결제



집전화 ARS 결제



문화상품권 결제

