교환하는 가게(?)들이 장을 펼치는 상상을 해본다.

괴물은 계속 형태를 바꾸고 학습하고 자라고 있다. 그리고 지금 여기로부터 내용적으로 시간적으로 장소적으로 더 멀리 자랄 것이다.

무명씨를 위하여

226 익명의 권리를 허하라 / 바리
235 아이덴터티? 아이덴터티. 아이덴터티! / 김지성
244 Tor: 익명네트워크 / 김승욱

무명씨를 위하여

익명의 권리를 허하라

바리 | 진보네트워크센터 활동가 della@jinbo.net

또다시 인터넷 실명제가 화두이다. 물론 인터넷 실명제는 2004년 도입된 직후부터 내내 논란의 대상이었다. 관련 법률조항이 발효하자마자 헌법소원이 제기되었고, 선거시기면 인터넷 언론사들의 실명제 거부가 이어졌다. 첫 헌법소원은 법률조항이 개정되었다는 이유로 각하되었지만, 2007년 대통령 선거에서 인터넷 실명제 시스템 설치를 거부한 참세상이 과태료 재판에서 위헌법률심판 제청을 신청하였고 한 네티즌은 인터넷 실명제가 기본권을 침해하고 있다며 또다시 헌법소원심판을 청구하기도 했다. 다른 한편으로는 인터넷 실명제가 소위 '악플', 즉 명예훼손과 같은 인권 침해에 대해 예방 효과를 가질 것이라고 기대하는 여론이 존재해 왔고, P2P 등 디지털 음원 공유 사이트에도 인터넷 실명제를 적용하자는 주장이 제기되었다.

논란의 재시동을 당긴 것은 촛불집회였다. 2008년 5월 촛불집회가 시작되자 인터넷이 소위 '광우병 괴담' 의혹에 휘둘린다는 보수 언론의 지적이 일었고 때맞춰 인터넷 실명제를 확대하려는 정부 움직임이 포착되었다. 7월 22일 정부는 제한적 본인확인제, 즉 인터넷 실명제를 현행 37개 사이트에서 대폭 늘려 210

개 사이트에 의무화하겠다는 방침을 공식적으로 밝혔다. 다만 개인정보 보호를 위해 주민등록번호를 사용하지 못하도록 하겠다는 친절함(?)을 덧붙였다.

누구를 위한 실명제인가

그러나 주민등록번호가 아니라 하더라도 아이핀, 휴대전화번호 등을 통해 실명 정보가 수집된다는 점은 마찬가지이다. 실명제 대상인 210개 사이트는 일일 방문자수 10만 명 이상의 사이트를 추산한 것인데, 이 정도 규모면 대다수 국민이 이용하는 사이트를 거진 아우른다. 가장 큰 의문점은 이것이다. **어째서 인터넷에서는 실명을 사용해야만 하는가?** 술집이나 버스나 지하철 등 일상생활 곳곳의 대중 공간에서는 이름표를 달지 않고도 지낼 수 있는데 왜 유독 인터넷에서는? 모든 국민이 악플러일 가능성 때문에? 과연 그런가? 네티즌들의 게시물을 삭제할지 말지 여부를 결정하는 방송통신심의위원회의 공적인 의사결정 과정은 익명으로, 비공개로 진행하면서 네티즌들은 왜 늘 발가벗을 것을 요구당하는가. **누구를 위해서?**

악플러를 막아야 한다고 치자. 그러나 어떤 행위도 하지 않았는데 당신이 악플을 올릴지 모르니 민증을 까라고 요구하는 것은 국가의 폭력이며 사전 검열이다. 다른 사람의 권리를 침해하는 악플이 발생하였으면 발생한 '후'에 현행법률에 따라 공정하게 처리하면 될 일이다. 실명이 아니어서 사법 처리가 어렵다는 말은 엄살이다. 그런 이유대로라면 주민등록번호가 없는 다른 나라들은 모두 인터넷 범죄에 속수무책일 것이다. 인터넷 실명제가 도입되었는데도 정부 속이 시원할 만큼 악플이 줄지 않는 데에는 그럴만한 이유가 있다. 청소년들이 거친 어휘를 쓴다고 해서 신원을 추적하고 경찰서를 들락거리게 한다고 악플이 줄지 않을 거라는 말이다. 이것은 형사적으로 일벌백계할 일이 아니라 우리 인터넷 토

론 문화의 문제이고 그런 차원에서의 정책적 접근이 필요하다. 그러나 지금까지 이런 주장은 크게 주목받지 않았다.

인터넷 실명제 논쟁은 표현의 자유 대 표현의 책임론으로 대비되어 왔기 때문이다. 이러한 논쟁 구도 설정은 흔히 익명 표현이 실명 표현보다 책임감이 없고 윤리적으로 바람직하지 않다고 규정한다는 점에서 문제이다.

익명도 권리다

우리 헌법이 보장하고 있는 표현의 자유에는 '익명표현의 자유'가 보장되어 있다고 보아야 한다. 왜냐하면 표현의 자유가 완전히 구현되기 위해서는 자신의 의사를 '자유롭게' 표현할 수 있어야 하는데, 이러한 자유로운 의사표현은 익명성이 보장되는 경우에만 가능하기 때문이다. 물론 의견을 개진하고자 하는 자는 실명으로 자신의 의사를 표현할 수 있다. 문제는 국가가 강제력을 동원하여 '실명으로만' 의사를 표현하도록 하거나 혹은 본인임이 확인된 사람에 대해서만 의사표현의 기회를 부여하는 방식은 안 된다는 것이다. 국가가 강제력을 동원하여 '실명으로만' 의사를 표현하도록 하거나 혹은 본인임이 확인된 사람에 대해서만 의사표현의 기회를 부여하는 경우에는, 그 '위축효과(chilling effect)'로 인하여 '자유로운' 의사표현이 불가능할 것이기 때문이다.

이러한 익명표현의 자유는 특히 정치적 표현과 관련될 때는 상당한 정도로 보장된다. 왜냐하면 정치적 표현의 특성이라든지 지금까지의 역사적 경험에 비추어 볼 때, 특정 정부나 정치세력에 대한 비판은 익명의 형태로 행해지는 것이 일반적이었고, 또한 원활하게 이루어지기 때문이다. 물론 익명표현의 자유가 절대적인 권리는 아니어서 일정한 공익을 위해서 제한할 수 있지만, 이러한 제한은 기존의 민형사수단에 의해서도 충분히 이루어지고 있다.

또 익명의 자유는 특히 사회적 소수자에게 중요한 인권이다. 익명 표현은 자신의 표현으로 말미암은 불이익에 대한 두려움 없이 소신껏 자신의 의견을 표현할 수 있도록 해준다. 때문에 민주사회에서 비판의 자유는 익명표현의 자유가 인정되어야만 비로소 완전해질 수 있다. 특히 내부고발은 익명표현이 보장되지 않는다면 이루어지기 어렵다. 이름을 밝히기 어려운 내부자에 의한 고발은 사회의 부정과 비리를 청산하는 데 기여했고, 익명의 제보는 역사의 실체적 진실에 대한 접근을 가능하게 했다. 미국의 독립, 나아가 프랑스 혁명 등 근대혁명을 태동케 한 역사적인 글인 토마스 페인의 '상식(Common sense)'은 '한 영국인'이라는 필명으로 발표되었으며, 그 외에 역사를 바꾼 수많은 글들이 익명표현물들이었다. 따라서 익명표현물은 규제되어야 할 비겁한 글쓰기가 아니라, 옹호되어야 할 민주주의의 전통이다. 표현의 자유에 있어서 익명성의 보장은 다수 위주의 사회질서 내에서 소수의 가장 강력하고 유용한 도구로서의 의미를 갖는 것이며, 따라서 익명성으로 인한 폐해를 시정하기 위한 법제도 속에도 이러한 익명성의 헌법적 의미와 역할은 반드시 제고되어 투영되어야만 한다.

소수자에게 절실한 익명성

우리는 최근 인터넷 실명제가 소수자의 표현의 자유를 침해했다고 볼 수 있는 사례를 볼 수 있었다. 예를 들어 지난 2007년 대통령 선거운동기간 중에 벌어졌던 사건을 들어보자. 12월에 '차별금지법' 논란이 발생하였는데 이 시기는 공직선거법상 모든 인터넷언론 게시판에 실명제가 의무실시되는 기간이었다. 차별금지법은 정치나 선거와 직접 관련이 없는데도 관련 기사 게시판에 실명으로만 댓글을 달 수 있었다는 말이다. 결과적으로 성소수자를 비롯한 장애, 이주노동

자, 청소년, 비혼자 등 사회적 약자와 소수자들이 강력한 문제의식을 갖고 차별금지법 반대운동을 벌였으나, 정작 이 문제를 다룬 인터넷 언론의 기사에 댓글을 달거나 토론을 할 수는 없었다. 실명을 확인받고 댓글을 달거나 토론을 할 경우 자신이 성소수자이거나 이주노동자라는 사실이 알려진 가능성이 있었기 때문이다.

또한 2008년 국회의원 선거운동기간 중에는 'J고'에서 일어난 인권침해 사건이 논란이 되었다. 이 사건은 익명인이 학내 문제점을 동영상으로 고발한 사건으로, 인터넷 언론 다수에서 기사로 다루었다. 만약 실명을 써야만 했다면 이런 고발이 어려웠을 것이다. 불이익을 받을 것이 자명한 상황이기 때문이다. 그러나 문제의 J고 학생이나 J고와 유사한 사례에 대하여 문제의식을 가지고 있는 이들은 이 사건에 대한 포털의 게시물이나 기사에 댓글을 달 수 없었다. 선거운동기간 중이라 모든 인터넷 언론 기사에 인터넷 실명제가 실시되고 있었고, 논란이 벌어진 포털 등 주요 인터넷 사이트에서는 상시적인 인터넷 실명제가 실시되고 있었기 때문이다. 생각해보라. 이들에게 실명을 밝혀야만 글을 쓸 수 있다고 말하는 것은 얼마나 큰 국가적 폭력인가!

다른 나라는 어떠한가? 세계 어느 나라에도 인터넷 실명제라는 건 존재하지 않는다! 그뿐만이 아니다. 익명의 권리를 인정하는 국가도 있다.

글로벌 스탠다드와 거리가 먼 실명제

1992년 캐나다의 통신 프라이버시 원칙에서는 통신서비스에 있어서 보호되어야 할 프라이버시 원칙으로, 원하지 않는 개입으로부터 보호받을 권리, 혼자 있을 권리, 감시되지 않을 권리, 자신과 자신의 행동에 대한 정보를 통제할 권리, 익명으로 남아 있을 권리를 못박았다. 1997년 미국과학발전협회(American Association for the Advancement of Science)는 인터넷에서 익명성이 사용자의 권리로 받아들여져야 한다며 그 근거가 되는 4가지 원칙을 제시하였다. 그 중의 하나는 익명적 커뮤니케이션이 도덕적으로 중립적이라는 원칙이다. 익명성이 부정적 결과를 양산하기도 하지만 그 자체가 해로운 것으로 규정할 수 없다는 것이다. 즉 해악적인 익명성을 규제하는 것은 정당한 익명성의 권리를 침해할 수 있다는 의미이다. 협회는 익명적 커뮤니케이션은 1948년 세계인권선언 제12조와 제19조에 근거한 인권으로서, "온라인상의 익명적 커뮤니케이션에 대한 어떠한 금지도 자유로운 의견표출을 침해하며, 개인의 사생활과 안전을 침범할 것"이라고 주장했다.

미국 연방대법원은 실명제의 문제를 표현의 자유의 문제로 보고 있다. 헌법 제정 전부터 익명이나 가명에 의한 팜플렛은 정치 뿐만 아니라 사회문화적 이념을 주도해 왔고 지금까지도 각종 언론보도에서 그 정보원을 고위층이나 X 등 익명화된 형식으로 표기하는 관행이 존재하는 것을 감안한다면 익명성이 표현의 자유에서 차지하는 비중은 작지 않다고 하면서, 익명의 팜플렛이나 전단, 브로슈어 또는 책자 등은 인류의 진보에 중요한 역할을 수행해 왔다고 판시한 바 있는 것이다. 대체로 미국의 법원은 익명은 한번 상실되면 다시 회복할 수 없다는 점을 강조하고 있다. 그렇기 때문에, 표현자의 익명성을 훼손하기에 앞서, 불법행위의 주장이 어떤 무게를 싣고 있는지 여부를 미리 결정하는 것이 필수적이라는 입장을 취하고 있다.

인터넷과 관련해서는 1996년 미국의 조지아주가 인터넷에서 익명표현을 금하는 법률을 제정했다가 연방지방법원의 위헌판결을 받은 후 폐기한 바 있고, 2001년 7월 뉴저지주 항소법원이 명예훼손 소송에서 익명의 인터넷 표현자의 권리를 인정하는 판결을 한 바 있다.

유럽에서도 익명적 커뮤니케이션은 표현의 자유의 한 측면으로 간주되는 경향이 있다. 유럽 의회 '정보보호분과'의 "인터넷 프라이버시: 온라인 정보보호에 대한 유럽의 통합적 접근"(Privacy on the internet: An integrated EU approach to online data protection, 5063/00/EN/FINAL) 보고서에 따르면, "특히 공공 영역에서의 인터넷 익명성과 관련해서 '가상 정체성'(익명성)은 개인 정보의 보호와 그 오용에 대한 법률적 규제 사이의 균형을 잡을 수 있는 대안적인 해결책이다"고 밝히고 있다. 대부분의 유럽 국가에서는 비용 지불의 목적을 제외하고 익명성의 권리를 인정하고 있다. 왜냐하면 익명성이 개인정보보호법에서 요구하고 있는 개인정보의 보호의 매우 중요한 수단으로 간주되고 있기 때문이다. 벨기에, 프랑스, 독일, 영국에서 익명성이나 가명의 사용을 권장하고 있다고 되어 있다.

당신들을 위한 인터넷 실명제

한마디로 국제적으로 익명성이 주목받고 있는 것은 프라이버시 때문이다. 실명을 확인하기 위해서는 인터넷 서비스 업체들이 주민등록번호와 같은 실명 개인정보를 수집할 수 밖에 없고, 이는 개인정보에 대한 자기결정권과 프라이버시권을 침해한다는 것이다. 개인정보 보호의 가장 기본적인 원칙은 '최소 수집의 원칙'이다. 꼭 필요하지 않은 개인정보는 수집하지 않는 것이 유출될 일도 없도록 만든다.

2008년 4월 옥션과 하나로텔레콤 등 주요 인터넷 서비스 회사에서 대규모로 개인정보가 유출된 것으로 밝혀지면서 이로 인한 명의도용이나 불이익, 사생활과 안전 상의 위협에 대한 우려가 커졌다. 그런데 이런 개인정보 유출사태에는 인터넷 실명제 의무화로 업계의 주민등록번호 수집을 정당화한 정부에도 책임이 있다는 비판이 제기되었다. 그런데도 정부는 계속해서 인터넷 실명제를 확대하려고 시도하고 있다. 다시 한번 묻지 않을 수 없다. 도대체 210개 사이트가 왜 모두 실명 개인정보를 수집해야 하는가? **누구를 위하여?**

최근 인터넷 실명제가 누구를 위한 정책인지 서서히 드러나고 있다. 일반 국민의 입장에서는 인터넷 실명제의 도입 이후에도 악플이 크게 줄지 않았다며 정책 무용론을 제기하고 있건만, 정부 입장에서는 인터넷 실명제로 꼭 뿌리뽑아야 할 '악플'이 있단다. 이명박 대통령을 '2MB'라고 표현한 국민의 표현이 악플이라는 것이다. 정부와 국민의 '악플'에 대한 개념이 완전히 다른 것이다. 그리고 인터넷 실명제는 정부 입맛대로 도입되고 있다.

인터넷 실명제의 이면에는 수사 편의를 확대하겠다는 꿍꿍이가 자리잡고 있다. 현행 전기통신사업법 제54조에서는 이용자의 실명 정보를 정권과 경찰이 원할때 언제든 확인할 수 있도록 보장하고 있다. 이는 이용자의 통신내역을 요구할때 법원의 허가를 받도록 한 현행 통신비밀보호법과도 균형이 맞지 않을 뿐더러, 이런 감시와 추적이 인터넷 여론을 위축시키는 효과를 낳을 것이라는 점에서 크게 우려스럽지 않을 수 없다. 평소 이용자의 실명 개인정보를 수집해 두었다가 그 정보를 수사기관이 마구 사용하도록 하는 정책이 '정보 보호'라는 명분으로 추진된다는 점이 기가 막힐 따름이다.

이명박 대통령은 지난 OECD 장관회의에서 "인터넷은 독"이라고 단언하는가 하면, 국회 개원연설에서는 "정보전염병"을 운운하기도 하였다. 그야말로 인터넷을 "부정적 여론의 진원지"로 보고 있는 발언이 아니라 할 수 없다. 인터넷은 마땅한 자기 표현 매체를 가지기 어려운 일반 국민들에게 유일하고도 강력한 표현 매체이다. 따라서 인터넷을 부정적으로 본다는 것은 국민 여론을 부정적으로 본다는 것과 다름이 없다. 이 대목에서 최근 인터넷의 힘을 빌어 확산되었다고

하는 촛불집회와 대통령의 악연이 떠오르는 것은 당연하다.

그러나 인터넷을 틀어쥐면 국민 여론이 잠잠해질 것이라는 것은 오산이다. 사람이 움직이기 때문에 인터넷이 움직이는 것이다. 그걸 깨닫지 못한다면 남은 4년 임기가 내내 순탄치 않을 것이다. 당신만을 위한, 당신들의 인터넷 실명제를 즉각 폐지하라!

아이덴터티? 아이덴터티. 아이덴터티!

김지성 | 진보네트워크센터 활동가 to.jisung@gmail.com

아이덴터티(identity)라는 단어를 영어사전에서 뜻을 찾아보면 동일성, 신원, 독자성의 의미를 갖고있다고 나온다. 솔직히 우리말로 바꾸어도 그 뜻이 심오하고 다양하게 쓰인다는 것을 알 수 있다. 이글에서는 온라인 세계에서 아이덴터티와 관련된 문제가 어디에서 발생하는지, 문제가 얼마나 복잡한지, 그리고 이와 관련된 여러가지 해결책(?)에 대한 모색과 논의가 어떤 것들이 있는지 거칠게나마 살펴보도록 한다.

우리는 이미 온라인 세계와 오프라인 세계의 경계가 허물어지고 과거에는 오프라인에서만 가능했던 일들과 관계들이 온라인에서 가능해지는 것을 경험하고 있다. 이제 온라인 세계는 단지 자신의 생각과 지식을 글로써 올려놓는 곳이 아니다. 온라인 쇼핑몰을 통해 전자상거래를 하고, 전자정부 서비스를 이용하여 민원 처리를 하기도 하고, 온라인 게임을 통해 여가 시간을 보내고, 싸이월드나 페이스북 같은 서비스를 이용해 사회적 관계망을 관리하고, 인터넷 뱅킹이나 주식거래로 돈을 관리하고, 위키피디아에서 공동으로 지식을 모으고, 또는 개인 블로그를 통해 자신의 전문 분야에 속하는 지식과 견해를 공표하기도 한다.

자신이 얼마나 많은 시간을 온라인 세계에서 보내는가 생각해본다면 경계가 무너지고 있는 것이 얼마나 급격하게 그리고 광범위하게 일어나고 있는지 쉽게 알 수 있다.

정보의 집합으로서의 아이덴터티

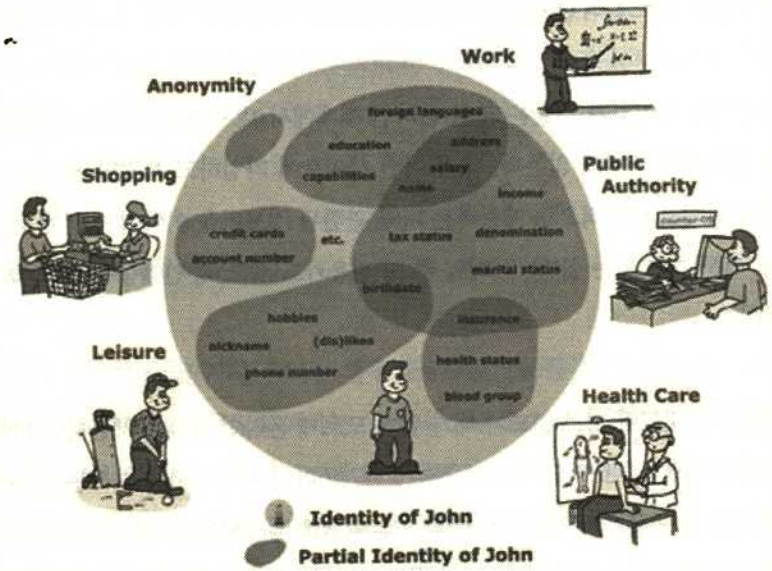
앞서 열거한 여러 가지 온라인 업무 (transaction)를 하기 위해서는 그러한 활동을 할 수 있는 권한을 부여하는 '승인 (authorization)' 과정이 있어야 하고 승인을 하기 위해서는 그 사이트에 그 사용자가 그러한 권한을 가진 주체가 맞는지를 확인하는 '인증 (authentication)' 과정을 거쳐야 한다. 순서로 보면 인증이 이루어지고 나야 권한을 부여하는 승인이 이루어지는 것이라 생각할 수 있다. 예를 들어 내가 가입한 온라인 카페에 가서 로그인 아이디와 암호를 입력하는 것은 인증을 위한 과정이다. 암호를 알고 있는 사람은 나뿐이라는 가정에서 암호는 내가 그 로그인 아이디를 쓰는 사람이라는 것을 인증하는 수단이 된다. 그리고 나면 카페의 사용자 등급에 따라 나는 글을 쓸 수 있는지 없는지 다른 사람이 쓴 글을 관리할 권한이 있는지 등이 부여되는 승인의 과정이 해당 사이트의 내부적으로 이루어진다. 대단히 간단한 구조다. 이것은 간단한 예고 만약 인터넷 뱅킹을 한다면 인증과 승인하는 과정은 훨씬 복잡해진다. 공인인증서나 비밀번호 카드가 필요할 수도 있다.

내가 온라인 세계에서 하고자 하는 업무에 따라서 필요한 승인의 절차와 그때 제공해야할 나와 관련된 정보(이름이나 신용카드 정보와 같이 오프라인 세계와 연결이 가능한 정보일 수도 있고 아니면 이메일주소와 같이 온라인 세계에서만 의미 있는 정보일 수도 있다.)도 달라진다. 완전하게 온라인 세계에서만 통용되는 또는 온라인 세계에서도 영역이 달라지면 전혀 의미를 갖지 않는 그런 익명성의 공간으로 온라인 세계를 이해할 수 없다.

지금까지 이야기된 것들은 사실 온라인 세계에서 내 아이덴터티와 관련해서 아주 일부분에 지나지 않는다. 내가 어떤 사이트에 가입하고 특정한 서비를 이용하기 위해서 명시적으로 제공하는 나와 관련된 정보만을 이야기한 것에 불과하다. 이름(가명 또는 실명), 이메일 주소, 신용카드 정보, 공인인증서 등과 같은 것들이다.

그렇다면 이러한 정보 정도가 내가 알게 모르게 온라인 세계에 제공하는 나의 아이덴터티의 일부로서의 정보의 전부일까? 온라인 세계에서 처리하는 업무가 많아 지고 그 종류가 다양해지는 만큼 기본적으로 제공해야 할 내 오프라인에서의 실체에 대한 정보도 늘어난다. 예를 들어 세금, 의료 보험, 대출 등과 같은 업무를 온라인에서 처리하기 위해서는 더욱 많은 정보를 내가 명시적으로 제공해야 한다.

그렇다면 이런 명시적으로 내가 제공하는 정보만이 있을까? 전자상거래 사이트에서 내가 판매자라면 나에 대한 구매자들의 평가도 내 아이덴터티의 일부가 된다. 당연히 내가 이제까지 팔아온 상품에 대한 이력도 아이덴터티 정보다. 내 블로그에 등록된 다른 블로거의 링크들이나 내 개인 페이지에 등록된 일촌 페이지 등도 나의 아이덴터티 정보다. 나와 관련된 사람들이나 물건들을 통해서 나의 아이덴터티가 일부 들어난다. 또 내가 검색엔진을 이용하거나 포털 사이트를 이용하면서 남기는 검색질의어나 페이지 이동에 관련된 정보는 대부분의 비즈니스 사이트에서는 자신들의 영업을 위해 개인 또는 집단에 대한 프로파일 (profile) 형태로 만들어진다. 내가 어떤 물건, 어떤 종류의 사회 이슈, 어떤 집단에 관심이 있는지를 프로파일을 통해 파악하게 된다.



신뢰성과 사생활의 문제

온라인 세계에서 아이덴터티의 문제는 크게 신뢰성과 사생활의 문제로 나누어 살펴볼 수 있다. 내 가 온라인에서 어떤 업무를 하는데 있어서 이러한 업무를 처리하기 위해 맺는 관계에 대해서 신뢰할 수 있는지 판단하기 위해서는 나 자신뿐만이 아니라 나와 관계 맺고 상호작용을 하는 상대의 아이덴터티에 대한 정보가 어느 수준 이상이 필요해진다. 그리고 그러한 정보가 정확한 것인지 확인해줄 방법 또한 필요해진다. 동시에 이렇게 제공되고 보관되는 아이덴터티에 관한 정보가 나의 사생활을 침해하지 않도록 정보를 제어할 수단 또한 필요해진다.

신뢰성의 문제를 온라인 쇼핑몰의 경우를 통해 살펴보자. 물건을 사기 위해서 온라인 쇼핑몰에 가서 나는 나에 대한 어떤 정보를 판매자에게 제공하고 나는

판매자로부터 판매자에 대한 어떤 정보를 얻어서 돈을 주고 물건을 살 것을 결정하는가? 왜 우리는 내가 돈을 지불하면 판매자가 판매한다고 사이트에 올린 물건을 정확히 받을 수 있다고 믿을까? 불안해하면서도 우리는 값싸다는 장점과 물건을 사기위해 매장을 찾을 필요가 없다는 점 때문에 온라인으로 물건을 산다. 아마도 대부분의 사람들이 물건을 구매할 때 정말로 판매자를 믿을 수 있는가를 판단하기 위해서 다른 구매자들의 판매자에 대한 평가나 물건에 대한 평가를 볼 것이다. 우리는 이러한 평가를 판매자가 자신이 공개하는 자신에 대한 정보보다 더 중요한 정보로 판단한다. 판매자가 자신에 대해서 자신이 누구라고 믿을 수 있다고 '주장' 하는 것보다 다른 이들이 그 판매자에 대해서 평가한 것을 더 '객관적' 이라고 보는 것은 합리적인 판단이다. 이러한 '명성 시스템(reputation system)' 은 온라인 세계에서의 아이덴터티를 구성하는데 중요하고도 일반화된 방법이다. 하지만 이 명성 시스템에서도 문제는 역시 존재한다. 이미 많은 온라인 쇼핑몰에서 판매자가 여러 개의 아이디를 만들어 구매자로 위장하여 좋은 평가를 올려서 구매자를 속이는 경우도 있고, 초기에는 진짜 물건을 정확하게 발송하여 좋은 평가를 받은 다음 이를 이용해서 물건을 파는 척하고는 돈을 챙겨 달아나기도 하고, 아니면 해당하는 아이디를 버리고 새로운 아이디를 만들기도 한다.

온라인 쇼핑몰의 사기 사건들과는 다른 분야에서도 신뢰성의 문제는 다양하게 발생하고 있다. 최근에 촛불집회와 관련해서 대학강사가 자신이 전경이라고 말하고 시위 진압 업무를 거부한다고 글을 올렸던 적이 있다. 대단히 민감한 정치적 사안에서 우리는 온라인에 올라온 글을 작성하는 사람들의 아이덴터티를 어떻게 믿고 이를 판단의 근거로 삼아야 하는가의 문제가 있다. 민주주의에 관련해서도 온라인의 아이덴터티의 신뢰성은 중요하다. 온라인 상에서 가상으로 특정한 계층에게 매력적으로 보일 가공의 아이덴터티를 만들어 이를 바탕으로 사기를 치는 사람 또한 많다. 문제가 생기면 이런 사람들은 온라인의 다른 사이

트로 옮겨가거나 또는 같은 사이트에서 쉽게 새로운 아이디를 만들고 새로운 가공의 인물을 창조하면서 사기 행각을 이어갈 수 있다. 위키피디아에서 자신을 전문가로 위장하고 엄청난 양의 항목을 만들었던 사건에서 우리는 소위 말하는 인터넷을 통한 "집단 지성"이라는 것에서 신뢰성의 문제가 역시 존재함을 알 수 있다.

우리는 온라인에서 이곳 저곳에서 나의 아이덴터티와 관련된 정보를 다양하게 남기고 살아가고 있다. 온라인에서 실명을 쓰느냐 아니면 가명을 쓰느냐의 문제를 넘어서서 나는 내 존재와 나에 대해서 여러 가지 정보를 남긴다. 내 스스로 사생활을 지키기 위해 가능하면 가명을 쓰고 내 물리적인 존재와 관련된 정보는 남기지 않고, 사이트 가입 때마다 다른 가명을 쓴다고 해서 해결 가능하지 않은 문제가 너무나 많다. 다시 여러 예를 들어가면서 우리가 온라인 세계에서 사생활과 관련해서 겪는 문제를 따져보자.

취업을 하려고 할때, 해당하는 기업의 인사담당자는 내가 제출한 이력서와 자기소개서만을 보고 나를 판단할 것이라고 생각한다면 오해다. 나는 내가 쓰는 사이트는 다 가명으로 되어있으니 안심을 해도 돼라고 생각하고 있다면 다시 생각해보아야 한다. 인사담당자는 아마도 검색 엔진에 당신의 이름으로 검색을 해볼 것이다. 검색 결과에 우연히도 내 친구 중에 하나가 내 실명과 내 블로그나 개인 홈페이지를 링크를 해두었다면 인사담당자는 쉽게 내가 어떤 것에 관심이 있고 어떤 생각을 가지고 있고 어떤 사람들과 관계를 맺고 있는지 알 수 있다. 외국의 사례의 경우에 기업이 자신의 회사에서 일하는 직원의 블로그의 글이 기업의 입장과 위배된다고 해서 해고를 한 경우도 있다.

이메일 주소는 명함에, 내 홈페이지에, 또는 내가 속한 공동체 사이트에 연락을 위해 쉽게 적어둔다. 이메일 주소만 알아도 그 사람에 대한 정보를 얻기란 너

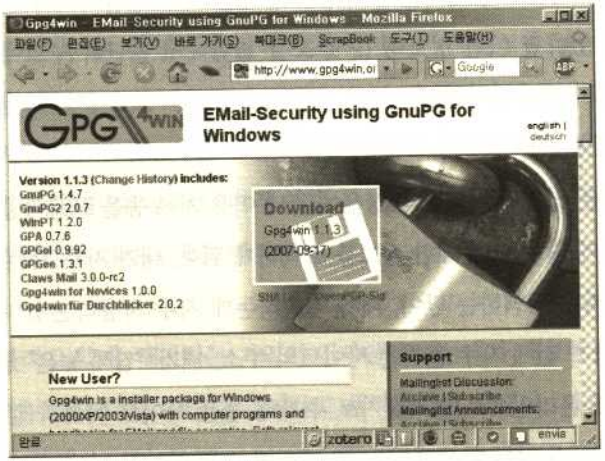
무나 쉽다. 내가 생각하는 익명성이라는 것이 얼마나 허술한지 쉽게 알 수 있다. 악성 스패머들은 또한 이렇게 쉽게 수집할 수 있는 이메일 주소를 이용해서 스팸을 수십만통씩 내 이름으로 보낼 수도 있다. 덕분에 나는 하루 아침에 악성 스패머가 될 수도 있다. 내가 조그만 공동체 사이트의 운영자라면 웹서버에 남는 로그를 통해 IP 주소를 바탕으로 어떤 사용자가 대충 어디에 살거나 일하는지 알 수 있다. 해당 사용자가 게시물 등에 자신에 관한 몇 가지 정보를 제공하고 있다면 심한 경우는 그 사람의 이름과 소속 단체 등은 쉽게 유추가 가능하다. 예를 들어 해당 사용자가 게시물에 특정한 단체를 자주 언급하거나 졸업한 학교 등을 적어두었다면 이런 정보와 IP 주소를 결합해서 판단하면 그에 해당하는 사람의 폭은 대단히 좁아진다.

포탈과 같은 상업적 서비스의 경우에는 내 이용 기록 등을 프로파일하는 과정에서 엄청나게 많은 나에 대한 정보를 축적하게 된다. 내가 자주 가는 카페나 블로그, 내가 자주 검색하는 단어, 내가 접속하는데 자주 사용하는 IP 주소, 내가 그 포탈을 가기 전에 자주 들리는 사이트의 주소, 내가 "찜해 놓은" 물건 · 책 · 여행지, 내가 온라인으로 즐겨찾기로 추가해 놓은 사이트 목록과 같은 것들이 쉽게 생각해볼 수 있는 것이다. 하지만 포털이 수집 가능한 나에 대한 정보의 목록은 훨씬 더 길어질 것이다. 나 이외의 누군가가 이러한 포탈의 정보의 접근할 수만 있다면 나라는 사람에 대해서 내 사랑하는 가족이나 애인보다 어쩌면 더 은밀한 또는 나와 관계 맺고 살아가는 어떤 한 사람보다 더 많이 알고 있다고 할 수도 있지 않을까 싶다.

해결은 어디서부터?

앞에서 거칠게 열거해본 신뢰성과 사생활에 관련한 문제들만으로도 문제가

얼마나 복잡한지 쉽게 알 수 있다. 어떤 이들은 이런 상황을 두고 인터넷에서는 어떤 것도 믿지 말고 사생활이 보호 받는 것은 불가능하니 그만 포기하라고 말하기도 한다. 아마도 아이덴터티의 문제를 해결할 수 없다면 인터넷 공간은 지금까지와 같은 발전을 더 이상 기대할 수 없게 될지도 모른다. 그것은 사이버 공간을 통한 더욱 다양해진 소통과 관계 맺기라는 희망을 더 이상 갖기 어려운 공간이 될 위험도 있다. 하지만 아직은 많은 이들은 인터넷에서 신뢰성의 보장이나 사생활의 보호를 포기할 무엇으로 판단하고 있지는 않다.



Gnu 사생활 지킴이

Tor와 같이 IP 주소를 익명화하는 시스템도 이러한 사생활 보호를 위한 하나의 수단으로서 탄생했다. 이와 유사한 시스템으로는 이메일을 익명화하거나 검색을 익명화하는 시스템들도 이미 존재한다. 또한 온라인 상에서의 데이터 이동이나 데이터베이스의 보관에 있어서 암호화하는 기술도 일종의 사생활 보호 도구로서 이용되고 있다. 다양한 개별 사이트에서 멋대로 이루어지고 있는 아이덴터티 관리를 사용자가 제어가능한 형태로 통합하여 관리하는 '연합 아이덴터티 (federated identity)' 시스템이 개발되고 도입되기도 하고 있다.

유럽연합의 경우는 'Future of Identity in the Information Society (FIDIS)'라는 연구 프로젝트를 통해 "아이덴터티의 아이덴터티(Identity of Identity)", "아이덴터티와 아이덴터티 관리 시스템의 상호호환성 (Interoperability of Identities and Identity Management Systems)", "프로파일링 (profiling)", "아이덴터티 시스템의 수사와 관련한 의미 (Forensic Implications of Identification Systems)", "사생활과 아이덴터티의 법률 · 사회적 내용 (Privacy and the legal-social content of Identity)", "이동성과 아이덴터티 (Mobility and Identity)"의 7가지 영역을 주요 대상으로 연구를 진행하고 있다.

현존하는 어떤 기술이나 정책 한두 가지로 아이덴터티와 관련한 문제를 해결하기에는 부족하다고 보는 것이 현 상황에 대한 적절한 판단일 것이다. 하지만, 나는 문제가 어디에 존재하는지에 대해서 이미 많은 온라인 세계의 시민들은 깨닫고 있다는 것에서 이미 문제 해결의 실마리는 존재한다고 생각한다. 이미 다양한 측면에서의 해결책을 제시하고 있는 개인과 집단이 존재하는 것 또한 사실이다. 문제는 우리가 온라인 세계의 시민으로서 그렇다면 공통으로 겪고 있는 문제에 대해서 집단으로서 대응할 수 있는 능력과 의지가 있는가가 관건이다. 정부나 기업은 자신들의 필요에 의해서 자신들의 입맛에 맞는 아이덴터티 관리 시스템을 만들고 이를 이용하도록 강제 또는 권유하고 있다. 자신의 아이덴터티를 자신이 관리할 수 있어야 한다고 우리가 믿는다면 이를 만족하는 관리 시스템을 우리가 기획하고 제안할 수 있어야 한다. 누군가에 맡기기에는 아이덴터티에 관한 정보를 통해 얻을 수 있는 또는 잃을 수 있는 것이 각자의 입장에 따라서는 너무나 많다. 이런 상황에서 대리인은 자신의 이익을 극대화하는 방향으로 행동할 가능성이 너무나 크다.

Tor: 익명네트워크

김승욱 | 진보네트워크센터 활동가 saakan99@jinbo.net

Tor(발음: 토어)는 인터넷에서의 프라이버시와 보안을 위한 일종의 가상 네트워크입니다. 우리는 웹브라우저, 메신저 등의 프로그램을 사용할 때 Tor를 통해 통신을 하도록 설정할 수 있으며, 이것이 프라이버시를 지키는데 도움이 됩니다. Tor 네트워크는 지구 곳곳의 Tor 이용자들이 자발적으로 제공하는 트래픽에 의해 구성됩니다. Tor는 Tor 네트워크 속으로 이용자의 통신요청을 순환시킴으로써, 프라이버시와 보안을 가능케 합니다. Tor를 사용하면 다음과 같은 효과를 기대할 수 있습니다:

- 제 3자가 당신이 어떤 사이트에 방문하는지 알 수 없도록 한다.
- 당신이 방문하는 사이트에서 당신의 물리적 위치를 알 수 없도록 한다.

그래서 Tor는 다음과 같이 사용되고 있습니다. : 기자들은 내부고발자나 정부에 저항하는 운동을 하는 사람들과 좀 더 안전하게 소통을 하기 위해서 Tor를 사용합니다. 독재국가의 국민들은 정부를 비판하는 글을 올리기 위해서 Tor를 사용합니다. 이 밖에도, 인권활동가, 노동자, 내부고발자, 지구 곳곳의 저항세력들이 Tor를 사용하고 있으며, 온라인에서의 권리를 지키고 싶어하는 많은 사람들이 Tor를 사용하고 있습니다.

Tor를 사용하는 사람들의 다양성이 사실 Tor를 가능하게 하는 중요한 요소입니다. 우리는 Tor의 사용자들 속에 무표정하게 서있음으로 인해서, 익명화되고 안전해질 수 있습니다. 따라서 더 많은 사람들이 Tor를 사용할수록, 더 많은 프라이버시가 가능해집니다.

IP주소의 익명화

오늘날의 웹사이트들은 통신과정에서 발생하는 일련의 행위들을 모두 기록(log)해두고 있습니다. 예를 들어, 검색을 제공하는 포털이나 서비스들의 경우 검색창을 통해 입력된 그 동안의 모든 검색어를 보관해두고 있습니다. 그리고 그 기록들은 검색어를 입력했던 IP주소에 연결되어 있습니다. 즉, 어느 IP주소에서 어떤 검색을 했는지 파악하는 것이 가능합니다. 그리고 IP주소는 당신과 연결되어 있지요. 빙고!

한국 정부는 작년에 통신비밀보호법 개정을 통하여, 위와 같은 IP주소의 보관을 사업자들에게 강제하려는 시도를 한 적이 있습니다. IP주소와 통신기록을 보관하다가 수사기관이 요청하면, 즉각 제공하도록 한 법안입니다. 다행히 작년의 통신비밀보호법은 진보넷과 몇몇 사회단체들의 강력한 반대 때문에 국회를 통과하지 못했지만, 이런 시도는 앞으로 계속될 것입니다.

사실 법으로 강제되고 있지 않은 지금도 인터넷 서비스 제공자들은 IP주소와 통신기록을 보관합니다. 사용자들의 성향을 분석하는 것이 마케팅의 기본이기

때문입니다. 보관되는 기록들은 수사기관에도 끊임없이 제공되고 있습니다. 몇 개의 작은 서비스를 운영하고 있는 진보넷에도 IP주소를 넘겨달라는 경찰의 전화가 자주 걸려옵니다. 2006년 한 해에만 IP주소와 통신기록에 대한 경찰의 요청은 총 41,681건이었습니다. 하루에 114건 꼴입니다.

Tor의 기능 중 하나는 IP주소의 익명화입니다. (정확히 말하면 이것은 Tor 통합배포판에 포함되어 있는 Privoxy의 기능입니다.) 이것은 웹사이트에서 개인의 물리적 위치를 알지 못하도록 해주며, 또 IP주소별로 통신기록을 기록/분류/분석하는 것을 무력화시킵니다. 경찰과 정보기관은 여전히 정보제공을 요청할 수 있지만, 그들이 그 기록을 신뢰한다면 정부정책에 반대의견을 내거나 소비자 운동을 하기 위해 인터넷에 글을 올린 사람을 뒤쫓기 위해 유럽이나 미국으로 날아가야 할 것입니다. Tor는 지구적인 프로젝트입니다.

반대로 Tor를 이용하여 서버를 익명화하는 것도 가능합니다. "랑데뷰 포인트"라는 숨겨진 기능을 이용하면 다른 Tor 사용자를 통해 웹사이트를 제공할 수 있습니다. 이 경우 누가 서비스를 제공하고 있는지 알 수 없고, 따라서 수사기관의 정보제공 요청이나 감시 등은 애초부터 불가능해집니다.

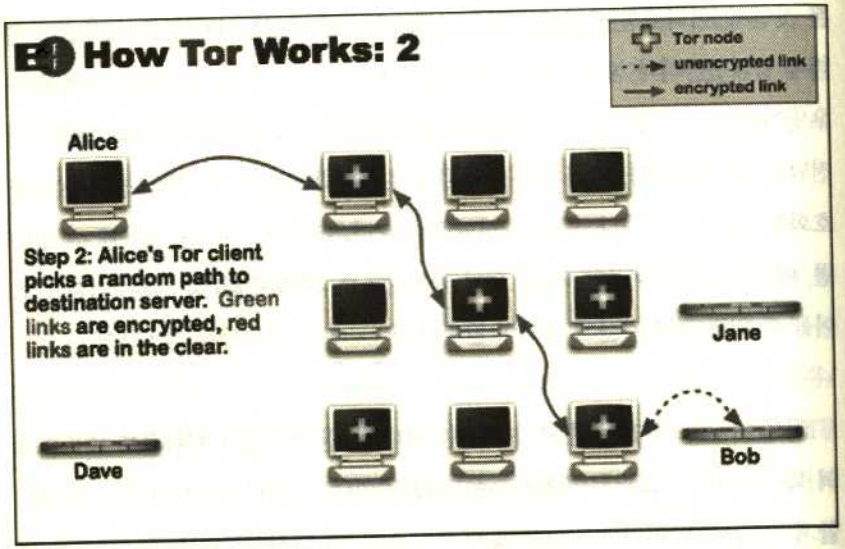
트래픽 분석과 Tor

Tor의 가장 중요한 기능은 "트래픽 분석"이라고 불리는 웹 감시기술을 무력화시키는 것입니다. 인터넷 데이터 패킷(정보전송의 최소단위)은 헤더와 데이터로 구성되어 있습니다. 데이터는 말 그대로 우리가 전송하고자 하는 그 무엇입니다. 데이터는 이메일일수도, 동영상일수도, 사진일수도 있습니다. 헤더는 이러한 데이터를 잘 전송하기 위한 일종의 메타데이터입니다. 이 데이터가 어디서 온 것인지, 어디로 전달되어야 하는지, 크기는 어느 정도인지 등등의 정보가 헤더에 담겨있습니다. 인터넷에서 패킷을 원하는 목적지까지 전달하는 행위를 라우팅이라고 하는데, 각각의 라우터는 헤더정보를 보고 패킷을 올바른 목적지로 전달할 수 있습니다. 따라서 데이터를 암호화한다고 한다 하더라도, 헤더는 암호화를 할 수 없습니다. 중간에 전달해주는 라우터들이 헤더를 열어볼 수 없다면, 어디로 전달해야 하는지 알 수가 없으니까요. 그래서 헤더는 누구나 쉽게 읽어볼 수 있고, 감시자들의 표적이 됩니다.

ISP같이 권한이 있는 사람[기관]뿐만 아니라, 권한이 없는 사람들도 네트워크의 특정지점에서 오가는 패킷들, 헤더들을 열어보고 인터넷에서의 통신을 감시할 수 있습니다. 이러한 작업을 통해 통신주체, 즉 당신의 위치는 물론, 자주 접속하는 사이트, 관심사, 인터넷 사용 패턴 등을 알아낼 수 있습니다. 특히 정보기관이 당신에 대한 수사를 시작하기라도 했다면 말이죠. 당신의 전용선은 지금 안전할까요?

Tor는 다음과 같은 방법으로 트래픽 분석을 불가능하게 만듭니다.:

1. 패킷을 목적지까지 바로 전달하지 않고, Tor 네트워크 속으로 전송합니다.
2. Tor 네트워크 안에서, 패킷은 의미 없는 랜덤경로를 따라 전송이 됩니다.
3. 각각의 노드들은 패킷이 어디서 출발했고, 최종 목적지는 어디인지 알 수 없습니다.
4. 어느 노드도 전체 통신을 추적하거나 알아 낼 수 없습니다.
5. 패킷은 Tor 네트워크의 출구노드(Exit node)를 통해 최종목적지로 전달됩니다.
6. Tor 네트워크 안에서 패킷이 순환되었던 기록은 주기적으로 삭제됩니다.



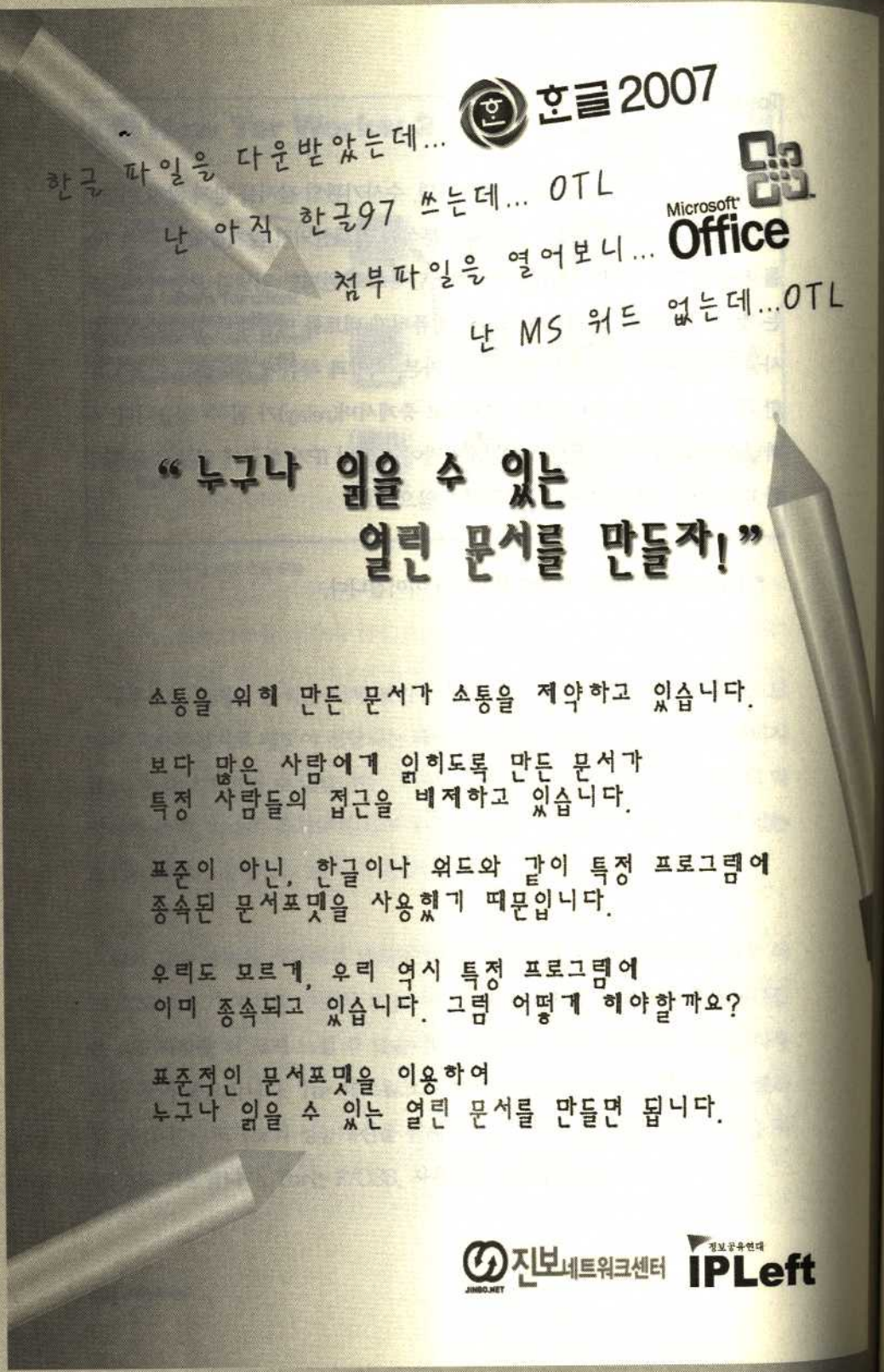
Tor 네트워크에서의 패킷 전송 모습

대부분의 트래픽 분석은 이제 불가능해집니다. 다만, 위의 과정 중 출구노드에서 최종목적지로 패킷이 전달되는 과정(위 그림의 붉은선 부분)은 암호화되지 않고, 따라서 보호될 수 없습니다. 그러나 이미 Tor의 다른 기능인, IP주소의 익명화를 통해, 당신의 위치나 당신이 누구인지 알기가 어렵기 때문에, 의미 있는 트래픽 분석은 힘들다고 볼 수도 있습니다.

위와 같은 방법을 사용하기 때문에 Tor를 이용하여 인터넷을 사용할 경우 어느 정도 속도가 저하될 수밖에 없습니다. 특히 전용선에 익숙한 한국 네티즌들은 속도저하를 더 크게 느낄 수 있습니다. 그래서 더 많은 사람들이 Tor를 사용하는 것이 중요합니다. Tor 네트워크가 더욱 방대해질수록 Tor의 속도도 빨라질 것입니다. 또 Tor의 성능개선을 위해서 Tor의 개발에 참여하거나 후원을 하는 것도 가능합니다. Tor는 F/OSS, 자유소프트웨어입니다.

이제 당신의 통신이 안전하길 원한다면, 수사기관의 감시를 받지 않길 원한다면, 기업들의 마케팅 자료로 보관되고 분석되고 계산되지 않기를 원한다면 Tor를 사용할 것을 권장드립니다. (단, Tor 단독으로 완벽한 익명과 보안이 보장되는 것은 아닙니다) 또 당신과 당신의 컴퓨터가 네트를 마음대로 항해하는 마법사들의 빗자루가 되고 싶다면, 국가와 자본, 억압과 착취에 저항하는 이들을 위한 무기가 되고 싶다면, Tor를 설치하고 중계서버(relay)가 될 수 있습니다! 사파티스타를 추적하는 멕시코의 정보기관이 그들의 IP가 한국에 있는 것을 확인한 다면 어떤 기분이 들까요? 궁금하지 않으세요?

* Tor 설치매뉴얼은 F/OSS 꼭지에서 이어집니다.



F/OSS가 함께하길

252 그누 사생활 지킴이를 만나보세요 / Envia
276 촛불생중계: 자유소프트웨어로 보고, 재전송도 하기 / 조동원
286 Tor 설치매뉴얼 / 김승욱

그누 사생활 지킴이를 만나보세요

Envia

GnuPG

요약

이 문서는 윈도 환경에서 GnuPG(GNU Privacy Guard, 그누 사생활 지킴이)를 이용하여 이메일과 파일의 내용을 암호화하고 푸는 방법을 설명합니다.

강조

비밀 열쇠와 비밀문구는 소중한 것입니다.

소개

GnuPG는 무엇인가

GnuPG는 문서와 파일의 내용을 암호화할 때 사용하는 프로그램입니다.

이름에 대해 조금 더 알아 보면, GnuPG(그누피지)는 GNU Privacy Guard를 줄인 이름입니다. 더 줄여서 GPG(지피지)라고 부르기도 합니다. GNU Privacy Guard는 보통 그누 사생활 경비원으로 옮기는데, 그누 사생활 지킴이라고 부르는 것이 더욱 친근할 것 같습니다.

암호화는 무엇인가

암호화는 어떠한 정보를 알아볼 수 어렵게 만드는 것을 말합니다. 사실 그냥 알아보기 어렵게 만드는 것은 아닙니다. 비밀 번호를 가진 사람은 쉽게 알아볼 수 있지만, 그렇지 않은 사람은 알아보기 어렵게 만듭니다. 비밀 번호를 가진 사람이 암호화를 해제해서 암호화된 정보를 원래 정보로 돌려놓는 것을 복호화라고 합니다. 암호화를 하고 해제하는 것이 자물쇠로 잠그고 열쇠로 여는 것과 비슷하기 때문에 비밀 번호를 열쇠라고 부릅니다.

암호화와 복호화를 하는 방법에는 크게 두 가지가 있습니다. 첫번째 방법은 대칭 암호입니다. 대칭 암호는 열쇠가 하나이고, 암호화를 할 때와 해제할 때 같은 열쇠를 사용합니다.예를 들어 비밀 번호 "1234"로 이메일을 암호화해서 보냈다면, 상대방은 "1234"를 이용해서 암호화를 해제할 수 있습니다. 대칭 암호에서 쓰는 열쇠를 비밀 열쇠라고 부르기도 합니다.

대칭 암호는 혼자서 사용하거나 자주 만나는 사람과 사용할 때에는 괜찮지만, 쉽게 만나기 어려운 사람과 사용할 때에는 문제가 있습니다. 비밀번호 "ABCD"로 이메일을 암호화해서 보냈다고 합시다. 상대방이 이메일을 읽을 수 있도록 하려면 비밀번호를 전달해 주어야 하는데, 안전하게 비밀번호를 전달하기가 쉽지가 않습니다. 비밀번호를 이메일로 전달하면 기껏 암호화한 것이 의미가 없어집니다. 누군가가 이메일을 가로챈다면 이메일에 있는 비밀번호를 이용해서 암호화된 이메일을 읽을 수 있기 때문입니다.

그래서 나온 것이 두번째 방법인 공개 열쇠 암호라고도 하는 비대칭 암호입니다. 비대칭 암호에서는 열쇠가 두 개입니다. 하나는 공개 열쇠이고, 다른 하나는 개인 열쇠라 고도 하는 비공개 열쇠입니다. 하나로 암호화 한 것은 다른 하나로 해제할 수 있지만, 하나를 이용해서 다른 하나를 알아내는 것은 어렵게 설계되어 있습니다. 예를 들어 공개 열쇠가 "ABCD"이고 비밀 열쇠가 "1234"라면, "ABCD"로 암호화 한 것은 "1234"로 해제할 수 있고, "1234"로 암호화 한 것은 "ABCD"로 해제할 수 있지만, 공개 열쇠가 "ABCD"라는 것을 이용해서 비밀 열쇠가 "1234"라는 것을 알아내는 것은 어렵게 되어 있습니다. 개인 열쇠는 개인이 가지고 있고, 공개 열쇠는 아무나 알 수 있도록 공개해 놓습니다. 공개 열쇠 암호를 이용해서 이메일을 보낼 때에는 상대방의 공개 열쇠를 이용해서 암호화를 합니다. 그러면 상대방은 자신의 개인 열쇠를 이용해서 암호화를 해제하고 내용을 읽을 수 있습니다.

나의 비밀 열쇠로 암호화를 하는 경우도 생각해 봅시다. 이 때 상대방은 나의 공개 열쇠를 이용해서 암호를 해제할 수 있습니다. 나의 공개 열쇠는 아무나 알 수 있도록 공개되어 있기 때문에 암호화의 효과는 거둘 수 없지만, 나의 비밀 열쇠로 암호화한 것만 나의 공개 열쇠로 암호화를 해제할 수 있기 때문에 상대방은 이메일을 보낸 사람이 나의 비밀 열쇠를 가진 사람인 나 자신이라는 것을 알 수 있게 됩니다. 이것은 편지에 서명을 해서 내가 보낸 편지라는 것을 증명하는 것과 비슷하기 때문에 서명이라고 합니다.

GnuPG가 한글화가 되어 있지 않기 때문에 영어 용어들도 함께 알아 두시면 좋겠습니다. 암호화는 encryption, 복호화는 decryption, 서명은 signature입니다. 그리고 "암호화 하다"는 encrypt, "복호화 하다"는 decrypt, "서명하다"는 sign이 되겠습니다.

암호화는 왜 하는가

비밀 정보를 주고받기 위해 필요합니다. 비밀 정보라고 하니 무엇인가 대단한 것 같지만, 사실 그렇지만은 않습니다. 개인적으로 주고 받는 이메일에 담겨 있는 내용이 새어 나가지 않기를 바란다면 비밀이라고 할 수 있습니다. 업무와 관련되어 주고 받는 자료들도 다른 사람들이 보기를 원하지 않는다면 비밀이라고 생각할 수 있습니다.

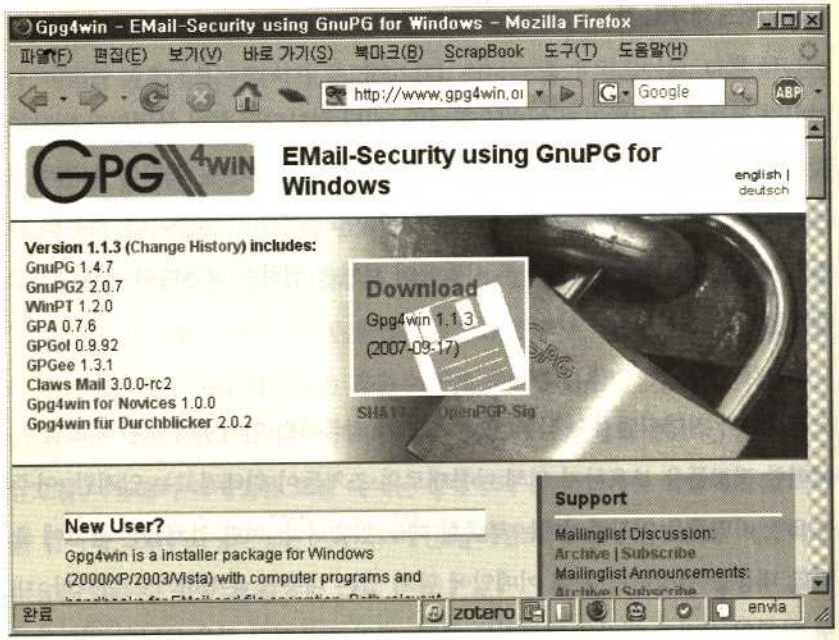
정보화가 진행되면서 점점 더 많은 정보가 컴퓨터와 인터넷에 보관되고 있고, 이러한 정보들을 보호하기 위해 나름대로의 조치들이 취해지고는 있지만, 아주 중요한 비밀들을 저장하기에는 부족할 때도 있습니다. 어떤 업체들은 광고에 출력할 내용을 결정하기 위해 이메일에 담겨 있는 내용을 분석하기도 합니다. 대형 업체의 서버가 해킹을 당하기도 하고, 개인 컴퓨터의 경우 도난의 위험까지 있습니다. 암호화를 이용하면 정보가 유출되더라도 해독이 어렵기 때문에 비밀과 프라이버시를 지킬 수 있습니다.

설치하기

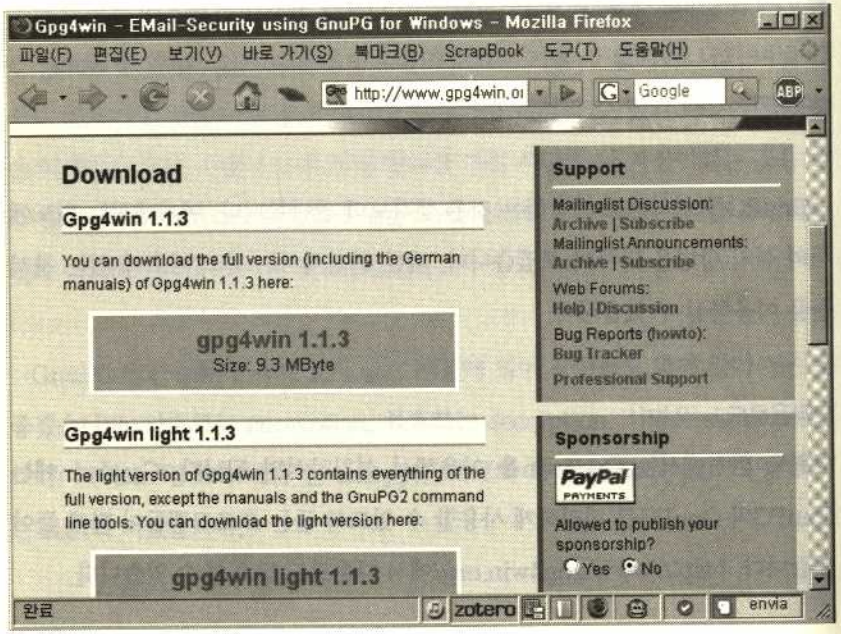
GnuPG를 설치하고 사용하는 것은 생각보다 간단합니다. 여기에서는 윈도에서의 설치 방법을 다루어 보겠습니다. 다른 환경에서는 참고 자료에 있는 문서들을 이용하실 수 있습니다.

다운로드

윈도 환경에서는 Gpg4win을 이용해서 설치하시면 됩니다. Gpg4win에는 GnuPG와 GnuPG를 편리하게 사용할 수 있도록 돕는 프로그램들이 함께 들어 있습니다. http://www.gng4win.org/에서 다운로드 받으실 수 있습니다.



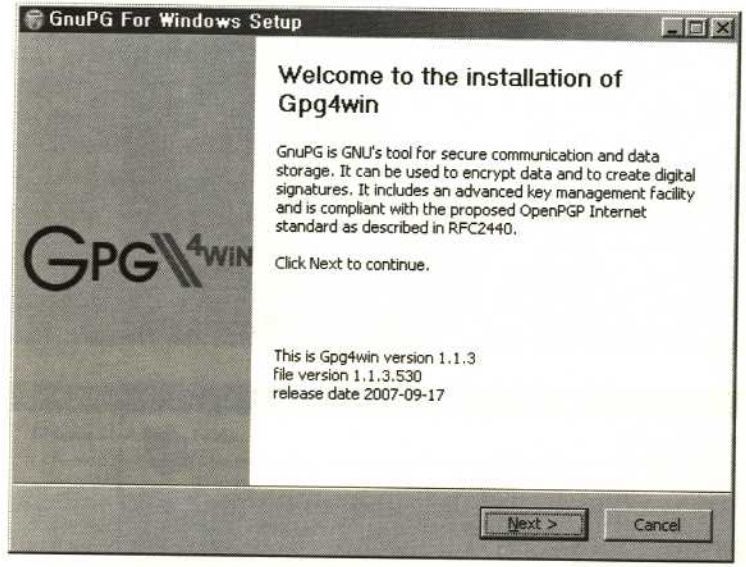
Download를 누릅니다.

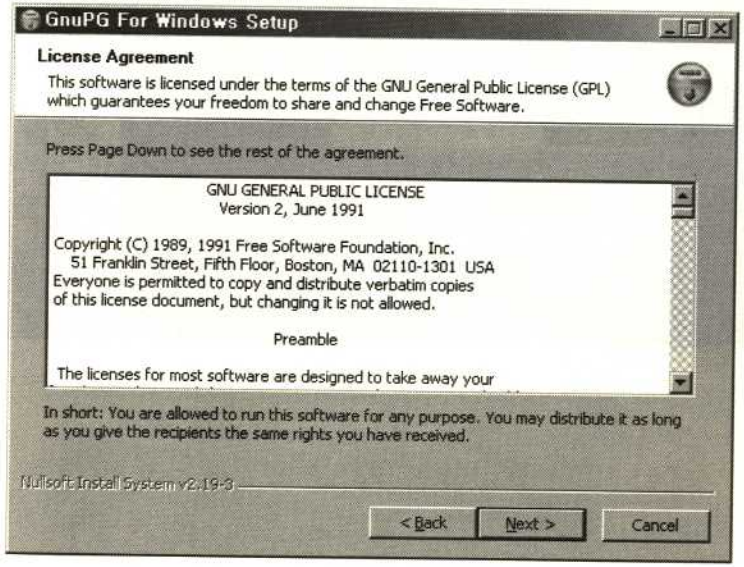


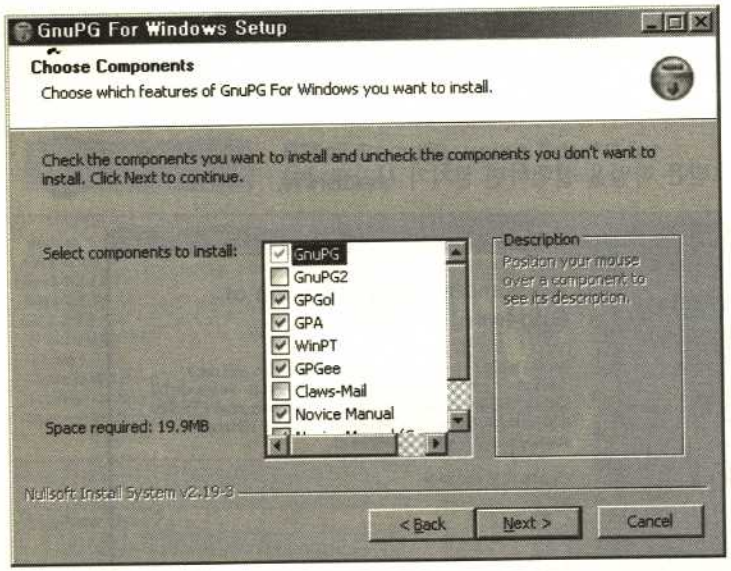
gpg4win을 누릅니다. gpg4win light를 누르셔도 됩니다.

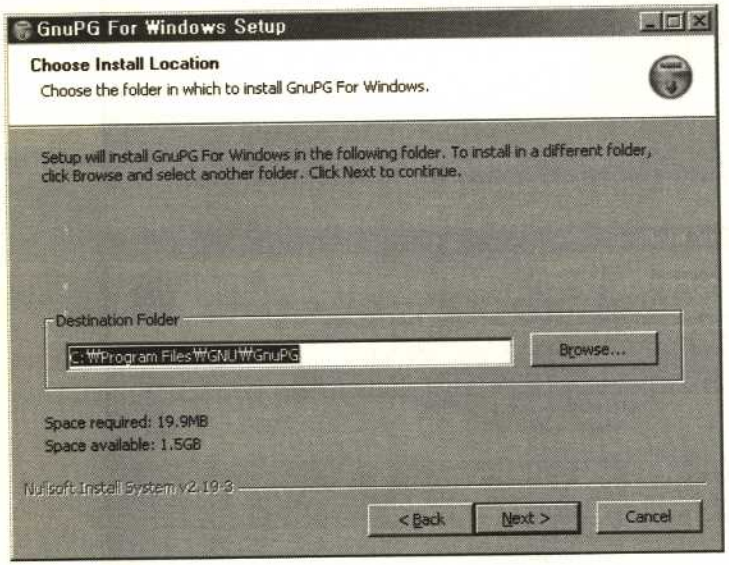
설치

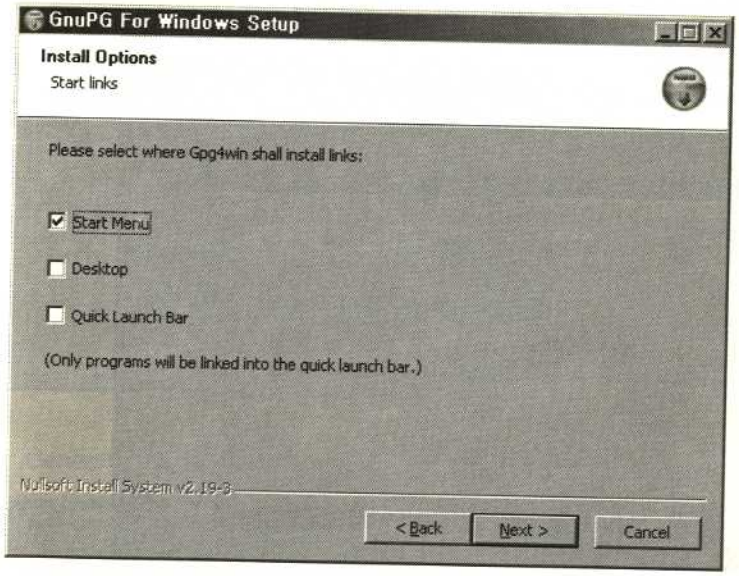
다운로드 받은 파일을 실행하면 설치가 시작됩니다.

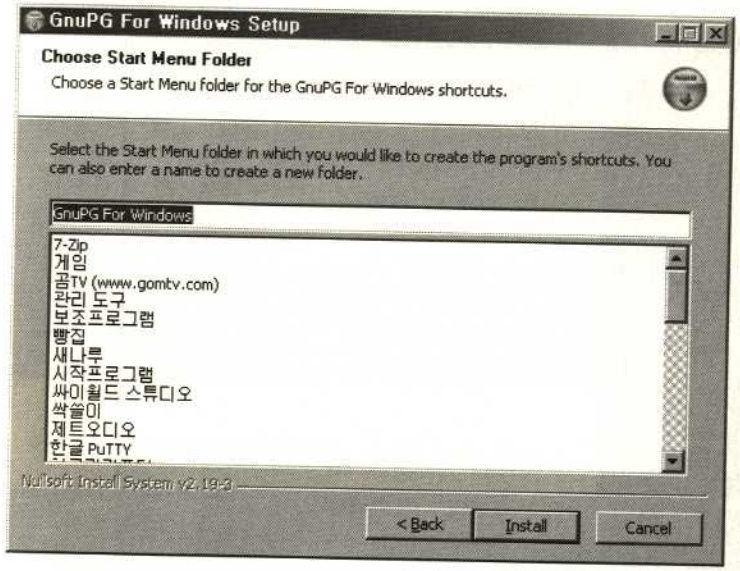


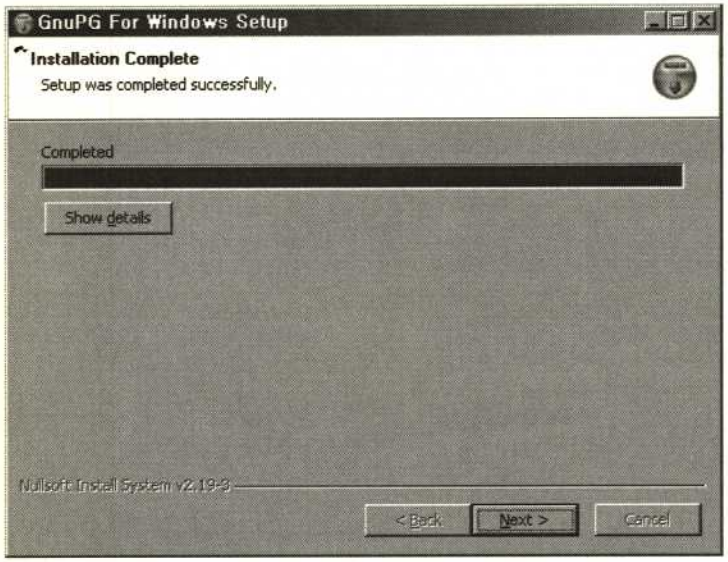


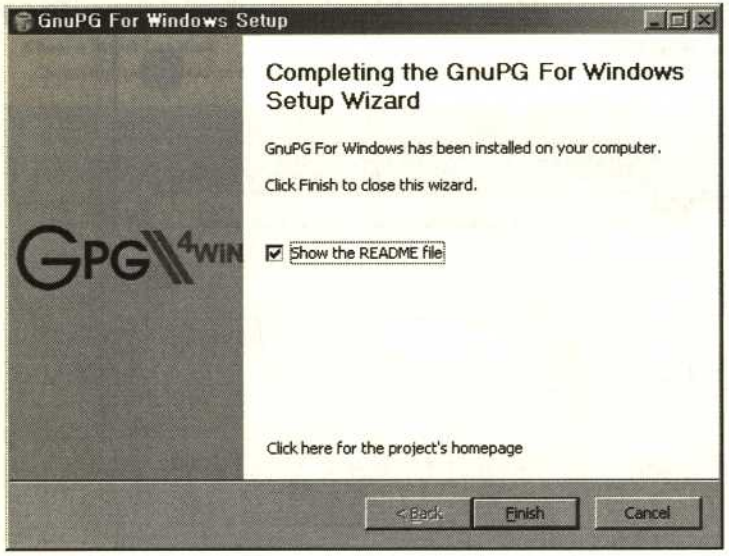

GnuPG For Windows Setup
Choose Components
Choose which features of GnuPG For Windows you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
GnuPG
GnuPG2
GPGol
GPA
WinPT
GPGee
Claws-Mail
Novice Manual
Description
Position your mouse over a component to see its description.
Space required: 19.9MB
Nullsoft Install System v2.19-3
< Back
Next >
Cancel


GnuPG For Windows Setup
Choose Install Location
Choose the folder in which to install GnuPG For Windows.
Setup will install GnuPG For Windows in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:₩Program Files₩GNU₩GnuPG
Browse...
Space required: 19.9MB
Space available: 1.5GB
Nullsoft Install System v2.19-3
< Back
Next >
Cancel


GnuPG For Windows Setup
Install Options
Start links
Please select where Gpg4win shall install links:
Start Menu
Desktop
Quick Launch Bar
(Only programs will be linked into the quick launch bar.)
Nullsoft Install System v2.19-3
< Back
Next >
Cancel


GnuPG For Windows Setup
Choose Start Menu Folder
Choose a Start Menu folder for the GnuPG For Windows shortcuts.
Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.
GnuPG For Windows
7-Zip
게임
곰TV (www.gomtv.com)
관리 도구
보조프로그램
빵집
새나루
시작프로그램
싸이월드 스튜디오
싹쓸이
제트오디오
한글 PuTTY
Nullsoft Install System v2.19-3
< Back
Install
Cancel

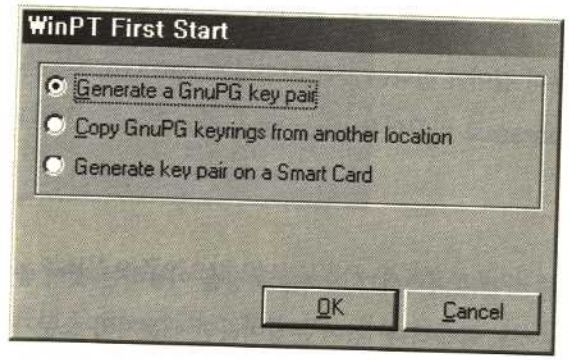




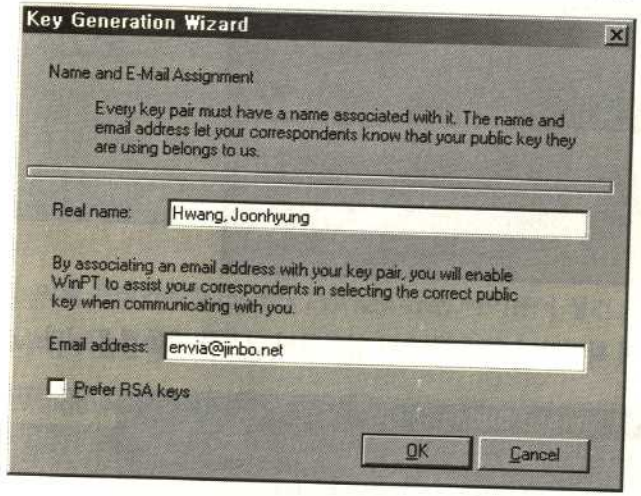
열쇠 만들기

설치가 끝났으면 시작 〉 프로그램 〉 GnuPG For Windows 〉 WinPT를 선택

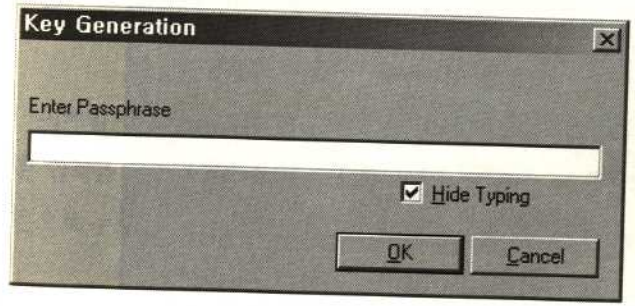
합니다. 열쇠가 없기 때문에 다음과 같은 화면이 나옵니다.



Generate a GnuPG key pair를 누르고 OK를 누릅니다.

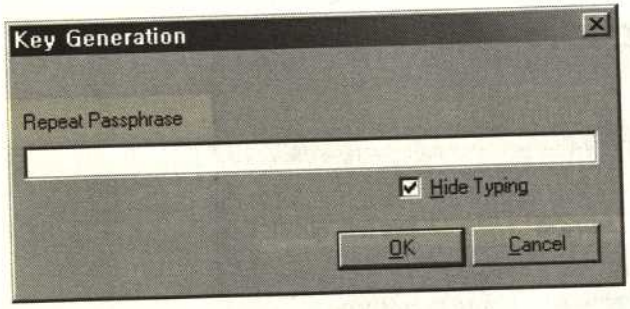


이름과 이메일 주소를 입력하고 OK를 누릅니다.

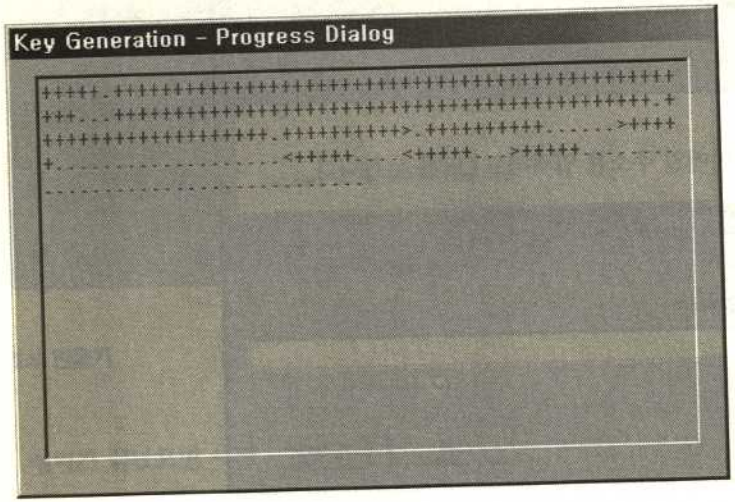


비밀문구를 입력합니다. 비밀문구는 비밀 열쇠를 암호화할 때 쓰는 비밀번호입니다. 비밀문구는 영어로 passphrase라고 합니다. 비밀번호를 영어로 password라고 하는데, 충분히 길어야 한다는 것을 강조하기 위해 단어라는 뜻의 word를 어구라는 뜻의 phrase로 바꾸어서 passphrase라고 부르는 것입니다.

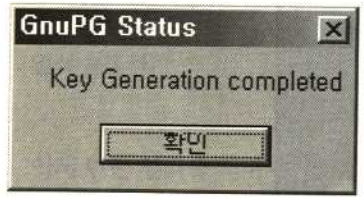
나는 기억하기 쉽지만 다른 사람은 예측하기 어려운 문장을 이용하는 것이 좋고, 중간에 특수문자를 섞는 것도 좋습니다. 영어 문장이라면 대문자와 소문자를 적절히 섞는 것이 바람직합니다.



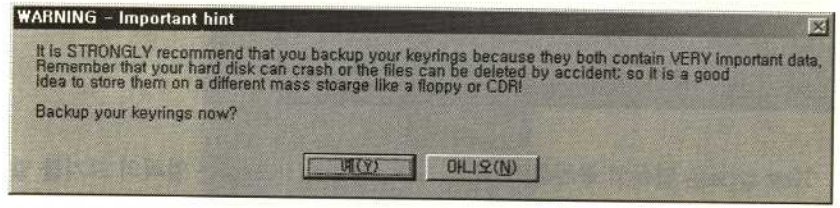
올바로 입력했는지 확인하기 위해 한번 더 입력하면 열쇠를 만들게 됩니다.



잠시 기다리면 열쇠가 만들어집니다.



열쇠를 만들었으면 열쇠 목록에 추가하게 됩니다. 열쇠 목록을 열쇠 고리라는 뜻의 keyring이라고 부릅니다. 열쇠 목록에 추가할 때 만약에 대비하기 위해 백업을 만들 생각이 있느냐고 물어보는데, 지금은 특별히 백업할 내용이 없으므로 아니오를 눌러줍니다. 나중에는 백업을 위해 예를 누르는 것이 좋겠습니다.

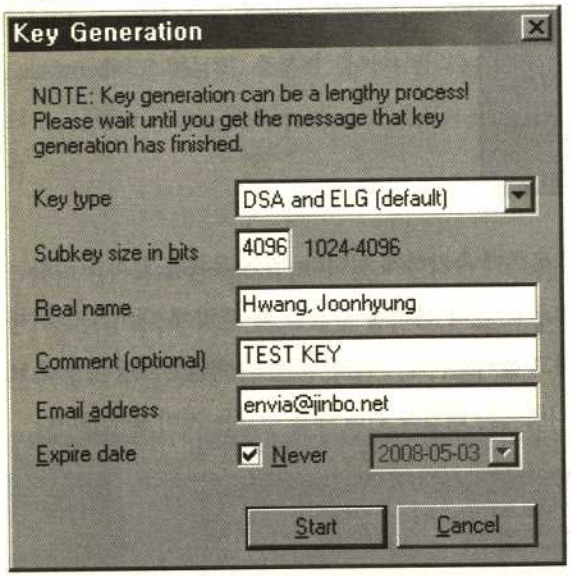


이제 트레이에 Windows Privacy Tray 아이콘이 생긴 것을 확인할 수 있습니다. 더블클릭하면 Key Manager가 실행됩니다.

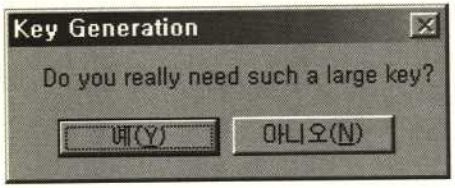
열쇠 더 만들기

이메일 주소가 더 있다면 열쇠를 더 만들고 싶을 것입니다. 여기서는 방금 만든 열쇠를 지우고 새로 만들어 보겠습니다. 방금 만든 열쇠를 마우스 오른쪽 버튼으로 누르고 Delete를 선택하면 열쇠를 지울 수 있습니다.

이제 Key Manager의 메뉴에서 Key 〉 New 〉 Expert를 골라봅시다.



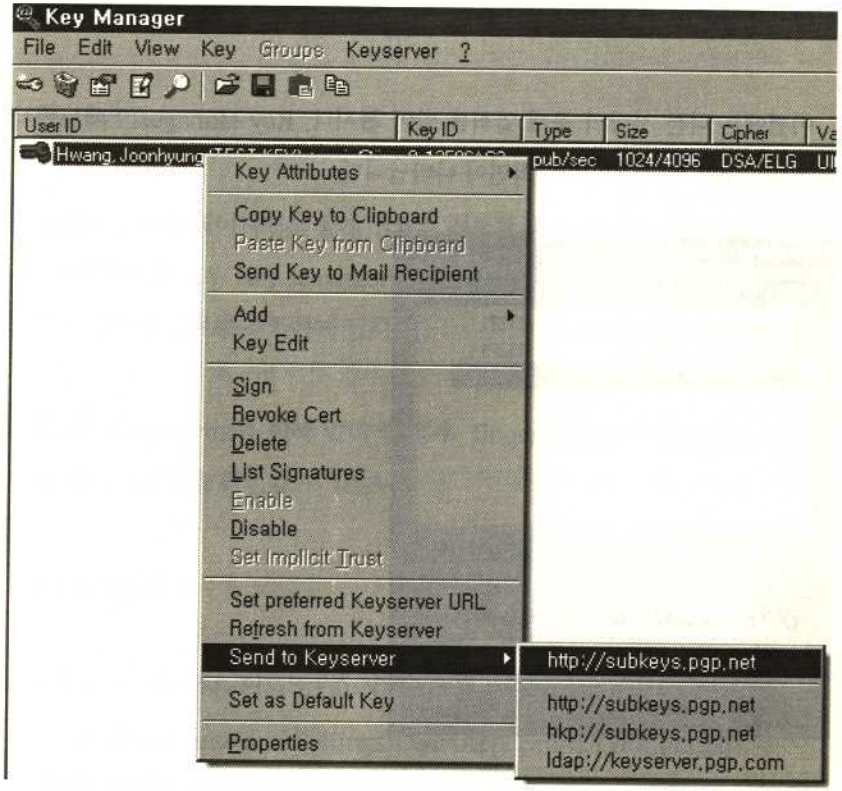
Key type은 열쇠의 종류를 말하고, Subkey size in bits는 열쇠의 크기를 말합니다. 큰 열쇠일수록 좋은 열쇠이지만, 만드는 데 시간은 오래 걸립니다. 기본값은 2048입니다. 여기서는 4096을 이용해 보도록 하겠습니다. Real name은 이름, Comment는 추가로 담고 싶은 말, Email address는 이메일 주소입니다. Expire date는 유효기간입니다. 적절한 정보를 입력한 다음, Start를 누릅시다.



열쇠 크기를 4096으로 정해서 만드는 데 시간이 오래 걸리기 때문에 정말로 그렇게 큰 열쇠를 원하는지 물어봅니다. 예를 선택합시다. 비밀문구를 입력하고 기다리면 열쇠가 만들어집니다. 열쇠 크기가 2048일 경우 1분 정도 걸리고, 4096일 경우 5분 이상 걸릴 수도 있습니다.

열쇠 등록하기

이제 만든 열쇠를 서버에 등록해 봅시다. 등록은 꼭 할 필요는 없지만, 등록하면 다른 사람이 쉽게 내 공개 열쇠를 받아갈 수 있습니다.

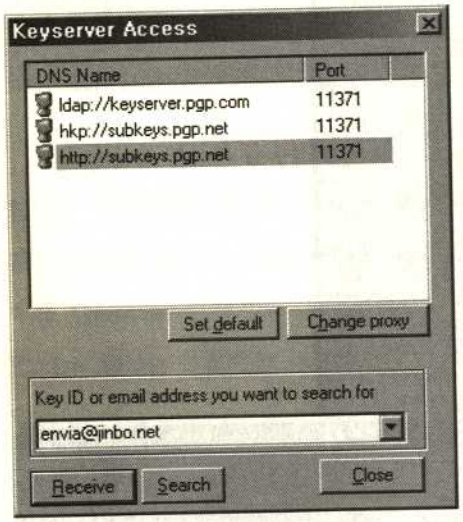


Key Manager에서 열쇠를 마우스 오른쪽 버튼으로 누르고 Send to keyserver를 누른 다음 아무 서버나 선택하면 됩니다. 서버들끼리 정보를 주고받기 때문에 아무 서버나 선택해도 괜찮습니다.

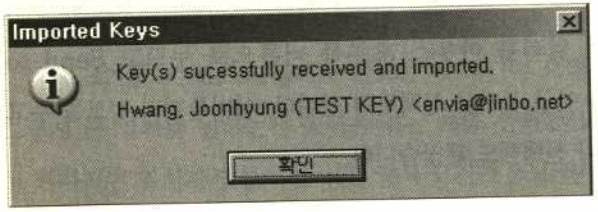
예를 누르면 열쇠가 서버에 등록됩니다.

열쇠 받아오기

이번에는 다른 사람의 공개 열쇠를 받아 봅시다. Key Manager의 메뉴에서 Keyserver를 선택하면 다음 화면이 나타납니다.



이메일 주소나 Key ID를 입력하면 열쇠를 받을 수 있습니다.



열쇠 내보내기

공개 열쇠를 서버에 올려 놓을 수도 있지만, 내 홈페이지에 올려 놓거나 이메일로 주고 받을 수도 있습니다. 이를 위해서는 공개 열쇠의 정보를 담은 파일을 만들어야 합니다. Key Manager에서 열쇠를 고른 다음 Key 〉 Export를 선택하면 열쇠를 저장할 수 있습니다. 이 파일을 홈페이지에 올려 놓거나 이메일로 보내면 됩니다.

열쇠 가져오기

다른 사람의 홈페이지에서 공개 열쇠의 정보를 담은 파일을 받았거나, 이메일을 통해 받았을 경우 Key Manager에서 Key 〉 Import를 선택한 다음 파일을 고르면 열쇠의 정보를 추가하게 됩니다.

열쇠와 fingerprint를 함께 알려 줄 경우, fingerprint를 이용해서 열쇠가 올바른 것이라는 것을 확인할 수 있습니다.

열쇠가 저장된 곳

방금 만든 열쇠들은 윈도 2000, XP의 경우

C:\Documents and Settings\User\Application Data\gnupg

에 저장되어 있습니다. 윈도 비스타의 경우

C:\Users\User\AppData\Roaming\gnupg

에 저장되어 있습니다. 여기에서 User는 윈도의 사용자 이름입니다.

주의 사항

비밀 열쇠를 잃어버릴 경우 암호화된 메일을 읽을 수 없게 됩니다. 비밀 열쇠를 실수로 지우는 일이 없도록 조심하시고, 백업해 두도록 하십시오.

비밀 열쇠를 다른 사람이 얻게 되면 암호화된 메일을 읽을 수 있게 됩니다. 비밀 열쇠를 특별한 처리 없이 저장해 놓으면 컴퓨터를 도둑맞거나 해킹을 당했을 경우 상대방은 비밀 열쇠를 얻게 되고, 암호화를 해제할 수 있습니다. 이것을 막기 위한 최후의 보루가 비밀문구입니다. 비밀 열쇠는 비밀문구로 암호화 된 상태로 저장되며, 비밀 열쇠가 필요할 때마다 비밀문구를 입력받아 암호화를 해제해서 사용합니다.

비밀문구를 잊어버릴 경우 비밀 열쇠의 암호화를 해제할 수 없기 때문에, 암호화된 메일을 읽을 수 없게 됩니다. 비밀문구를 잊지 않도록 주의하십시오.

비밀 열쇠와 비밀문구가 유출되지 않도록 주의하십시오.

GPGee 설정

GPGee는 파일을 암호화하고 해제하는 프로그램입니다. Gpgee에서 열쇠들을 사용할 수 있도록 설정을 해 봅시다. 아무 파일이나 마우스 오른쪽 버튼으로 누른 다음 GPGee 〉 configure를 선택합니다.

Set program path는 보통

C:\Program Files\GNU\GnuPG\gpg.exe

로 설정하면 됩니다. Set options file, Set public keyring, Set secret keyring은 위에 나와 있는 열쇠들이 들어있는 디렉토리 안을 찾아서 선택하면 됩니다. 윈도 2000, XP의 경우 보통

C:\Documents and Settings\User\Application Data\gnupg\gpg.conf

C:\Documents and Settings\User\Application Data\gnupg\pubring.gpg

C:\Documents and Settings\User\Application Data\gnupg\secring.gpg

에 있습니다.

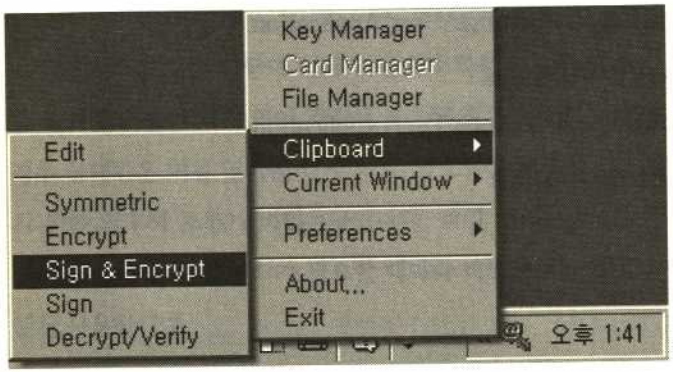
사용하기

여기까지 오시느라 수고하셨습니다. 이제 암호화된 메일을 보내고 받아 봅시다.

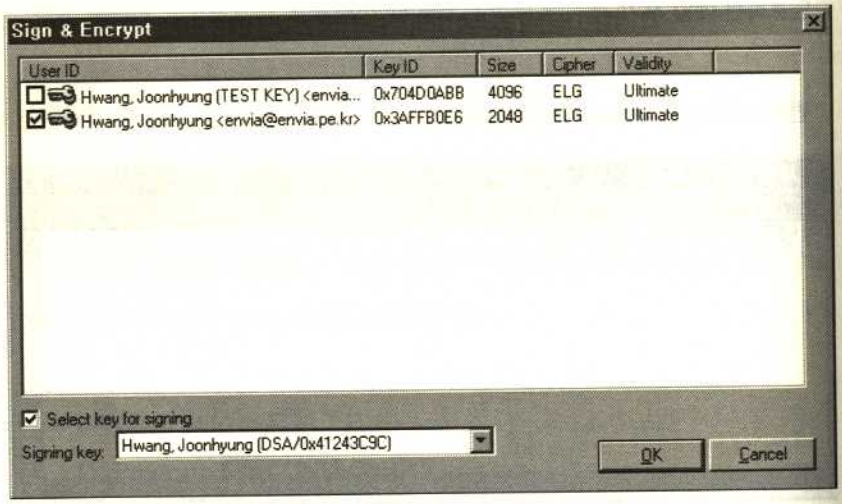
암호화된 메일 쓰기

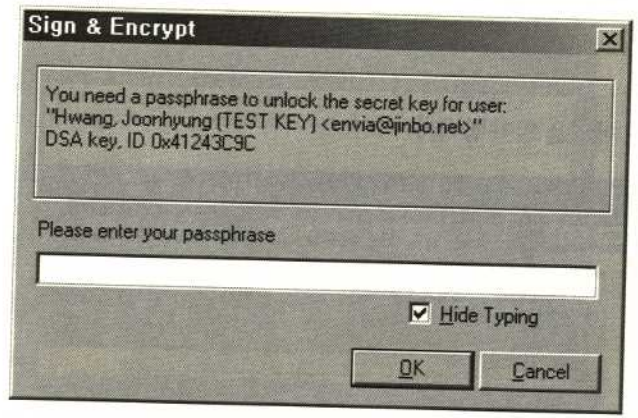
먼저 이메일의 내용을 작성합니다.

작성이 끝나면 보낼 내용 전체를 선택한 다음, 클립보드로 복사합니다. 보통 메뉴에서 편집 〉 복사를 선택하시거나 Ctrl+C를 누르시면 됩니다. 그 다음 트레이에 있는 아이콘을 마우스 오른쪽 버튼으로 누른 다음, Clipboard 〉 Sign & Encrypt를 누릅니다.

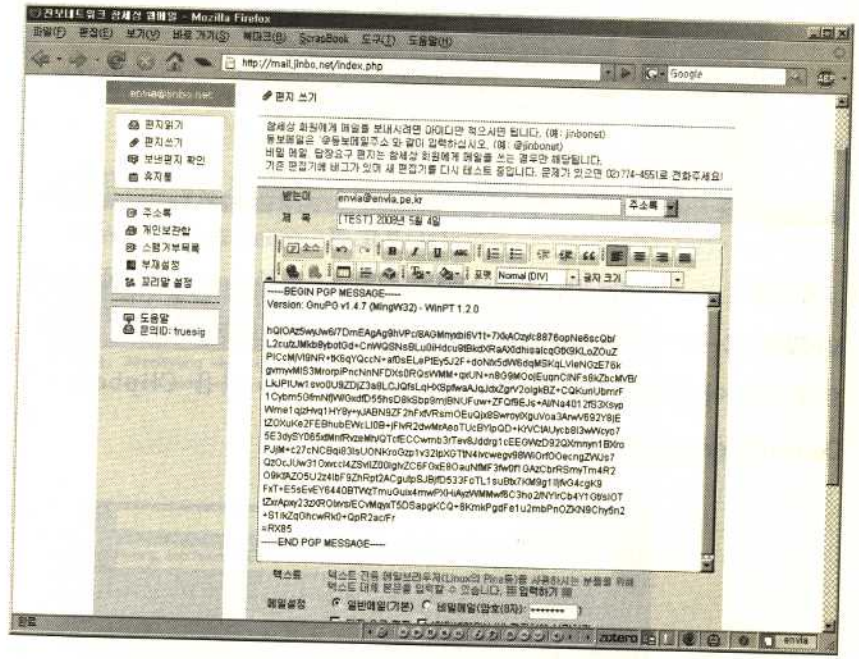


열쇠를 선택합니다. 암호화에 사용할 수 있는 열쇠의 목록이 나오는데, 상대방의 열쇠를 선택해야 합니다. 자신의 열쇠는 아래의 Select key for signing에서 선택해 줍니다.





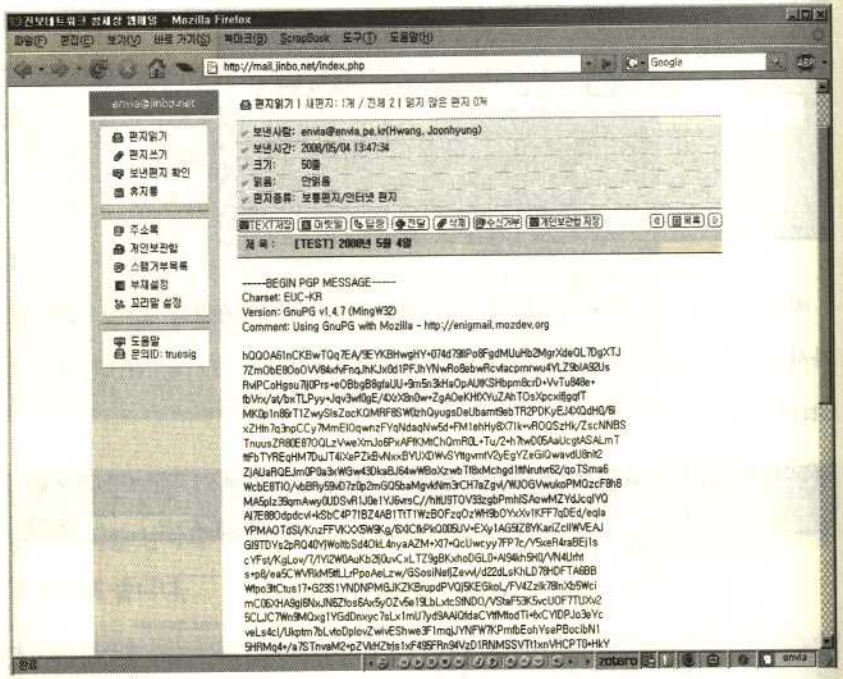
비밀문구를 입력하면 암호화가 이루어집니다. 이제 이메일을 보내는 화면에 가서 클립보드의 내용을 붙여넣으면 됩니다. 편집 〉 붙여넣기를 선택하시거나 Ctrl+V를 누르시면 됩니다.



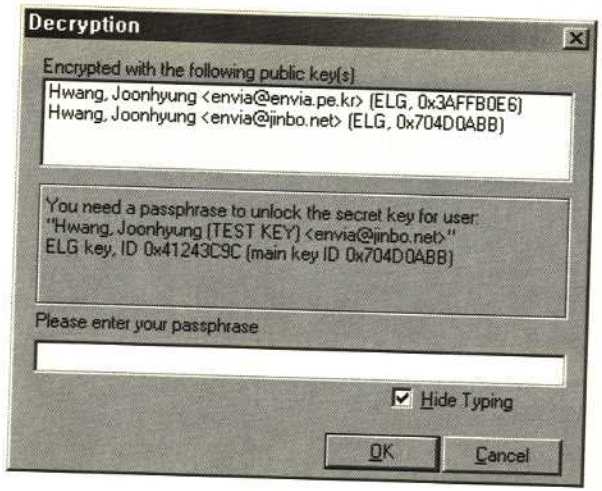
편지의 제목은 암호화 할 수 없습니다. 적절히 입력해 주시면 됩니다.

암호화된 메일 읽기

이번에는 암호화된 메일을 읽어 봅시다.



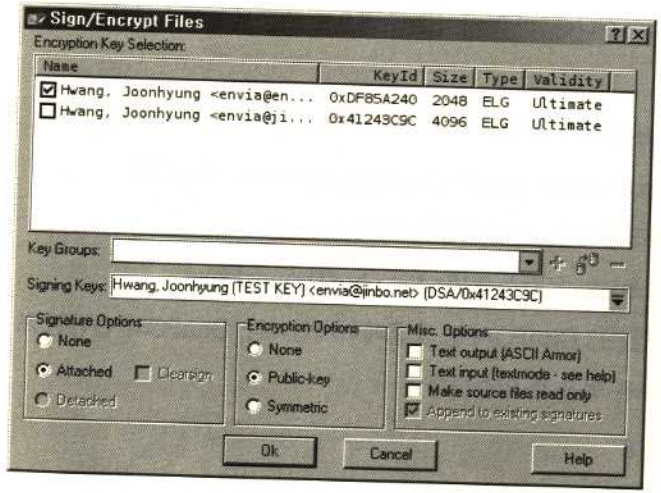
메일에서 -----BEGIN PGP MESSAGE-----부터 -----END PGP MESSAGE-----까지의 내용을 선택한 다음 클립보드로 복사합니다. 그 다음 트레이의 아이콘을 마우스 오른쪽 버튼으로 누른 다음 Clipboard 〉 Decrypt/Verify를 선택합니다.



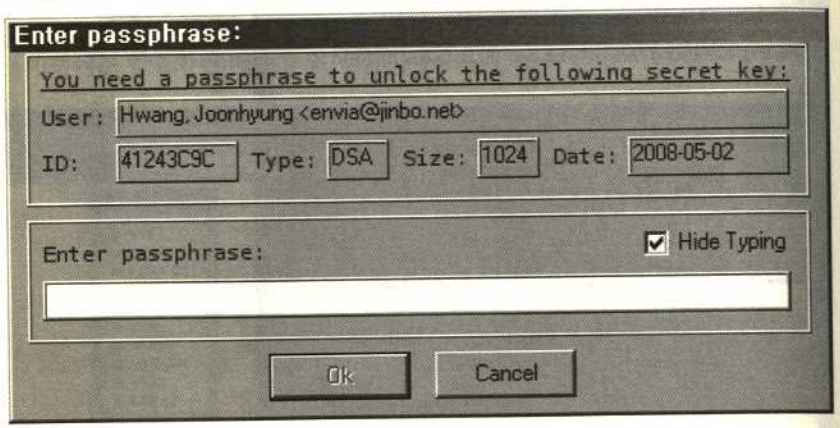
비밀문구를 입력한 후, 클립보드의 내용을 적절한 곳에 붙여넣으면 메일을 읽을 수 있습니다.

파일 암호화

암호화하고 싶은 파일을 마우스 오른쪽 버튼으로 누릅니다. 나타나는 메뉴에서 Gpgee 〉 Sign & Encrypt를 고릅니다.



암호화에 사용하고 싶은 열쇠를 선택합니다.



비밀문구를 입력하면 암호화된 파일이 생깁니다. 암호화를 풀 때에는 마우스 오른쪽 버튼으로 누른 다음, Gpgee > Verify/Decrypt를 선택하면 됩니다.

참고자료

이 문서는 Use PGP with any Windows Email Client를 읽고 아이디어를 얻어서 작성하게 되었습니다. 다음 사이트의 내용도 도움이 되었습니다.

* GnuPG mini HOWTO (국문)

http://wiki.kldp.org/wiki.php/DocbookSgml/GnuPG-TRANS

* 모질라 썬더버드에서 GnuPG 사용하기 (국문)

http://www.docbook.or.kr/wiki/index.php/ThunderBird

* GnuPG.org (영문) : GnuPG의 공식 홈페이지입니다. GnuPG와 관련된 프로그램에 대한 정보를 얻을 수 있습니다.

http://gnupg.org

* Gpg4win (영문) : GnuPG를 윈도에서 사용할 때 필요한 프로그램들을 다운로드 받을 수 있습니다.

http://www.gpg4win.org

암호에 관한 이론을 알고 싶으시다면 다음 책을 참고하실 수 있습니다.

* 한국정보보호학회 편, 현대 암호학 및 응용. 한국정보보호진흥원. (국문)

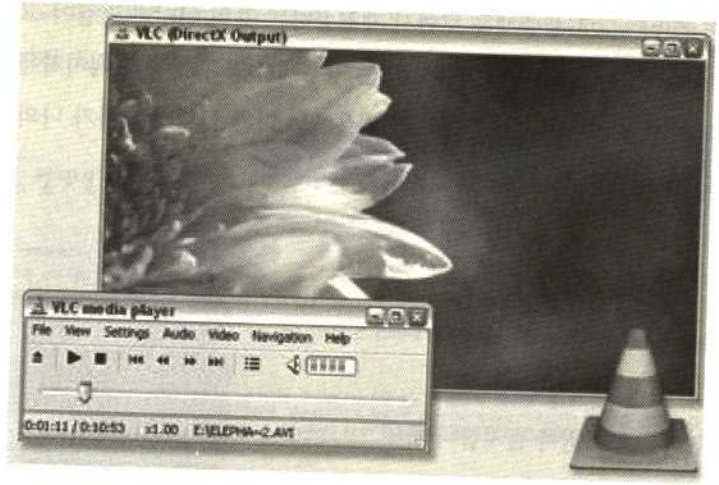
* Johannes Buchmann, Introduction to Cryptography, Second Edition, Springer. (영문)

촛불생중계: 자유소프트웨어로 보고, 재전송도 하기

조동원 | jonair@riseup.net

촛불집회 생중계 – 비디오 스트리밍의 시청 규모도 엄청난 것 같습니다. (어느 정도 시청하는지, 주로 어떤 생중계 서비스를 보는지에 대한 분석도 나오는지 모르겠습니다. 이에 대한 정보 아시는 분?) 광화문–시청 일대에서 매일 밤 벌어지는 집회 시위와 문화 난장은 – 직접 가서 보고 참여할 수 없다면 – 밤잠을 설치게 하는 볼거리일 텐데요, 생중계를 하는 곳들의 행복한 고민의 하나는 이 수많은 접속자들을 서버가 감당을 못하는 지경에 이르고 있다는 점일 것입니다. 그런 만큼, 인터넷 생중계 "방송"에 대한 (자발적) "시청료" 개념의 후원도 활발하게 이루어지는데, "스타"(?)를 이용하여 인기 있거나 마케팅 실력을 발휘하는 곳들에 편중되어 있어 보입니다.

이런 상황들을 보면서, 서버의 부담을 줄이면서도 "시청자"들이 "시청료"라는 후원 이외에 이 인터넷TV 시스템에 참여할 수 있는 방법을 생각해 보게 됩니다. 검색해 보면 p2p 기반의 비디오 스트리밍을 위한 자유소프트웨어나 오픈소스소프트웨어, 그리고 웹서비스들도 여럿 나옵니다.



그 중에서 VLC(Video Lan Client)라는 멀티미디어 플레이어 (자유소프트웨어입니다)를 사용하면, – 생중계되는 것을 시청할 수 있고, – 시청하고 있는 생중계를 동시에 재전송할 수도 있습니다. 내가 재전송하는 IP주소로 다른 사람이 생중계를 볼 수 있게 되고, 처음의 – (서버 없이) 이 플레이어만을 이용해서 현장에서 생중계를 할 수 있습니다.: vlc, 인터넷 접속, 웹캠을 갖춘 노트북 하나로!

즉, vlc는 비디오 스트리밍 서버가 필요 없이, 그 자체로 서버로 기능하는 훌륭한 기능을 가진 자유소프트웨어입니다. 이것으로 p2p 방식의 인터넷 실시간 TV가 가능한 것인데요, 하지만, 현재 "재전송"을 하는데 몇 가지 한계가 있습니다.:

– 이 자유소프트웨어인 vlc를 이용해서 생중계를 보고 재전송할 수 있는 촛불집회 생중계 서비스는 "민중언론 참세상"(http://newscham.net) 밖에 없는 듯합니다. 왜냐하면, 참세상을 제외하고 비디오 스트리밍 소스를 손쉽게 확인하기 힘들기 때문입니다.

– 재전송의 경우, vlc로 생중계를 보면서 재전송하는 곳의 인터넷 연결이 고정IP여야 합니다. 혹은, 모뎀–공유기를 쓰시는 경우에는 공유기 관리 페이지에 가서 포트 포워딩을 하면 됩니다. 유동IP인 경우에는 다른 곳의 접속자가 나의 vlc 재전송의 주소를 제대로 알 수 없게 되기 때문입니다.

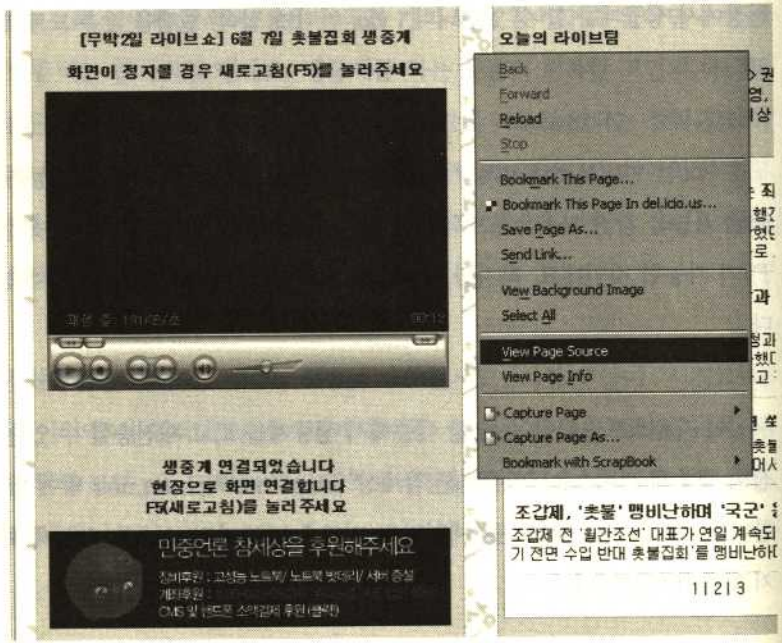
참세상의 촛불 생중계를 보면서 재전송 하기

우선, vlc를 다운로드 받아 설치합니다.

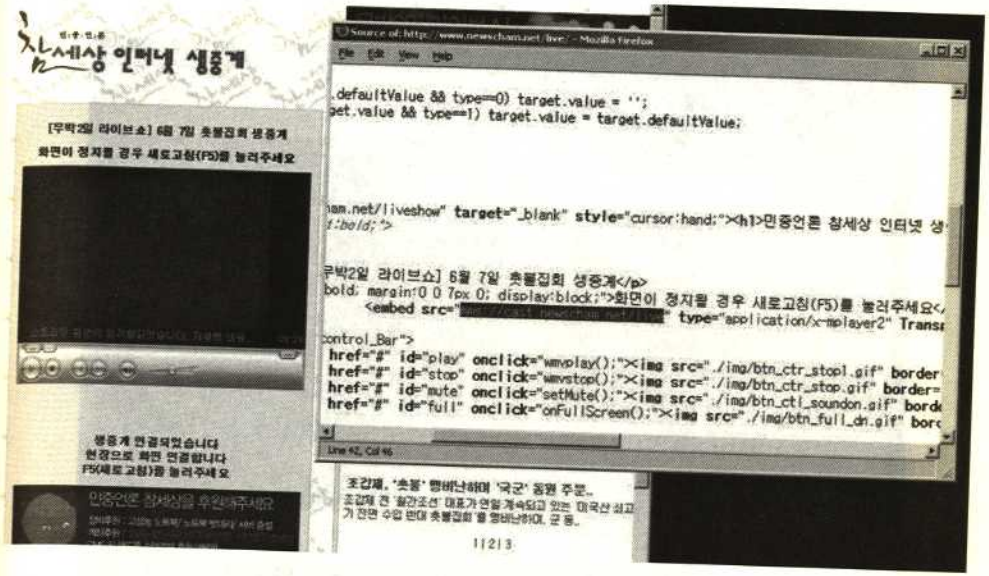
vlc 다운로드: http://www.videolan.org

그리고 나서, 민중언론 참세상의 생중계하는 곳

(http://www.newscham.net/live/)으로 가 아래와 같은 화면에서, 오른쪽 클릭을 해보면 "View Page Source" 혹은 "소스 보기" 메뉴가 나옵니다. 그것을 열면...

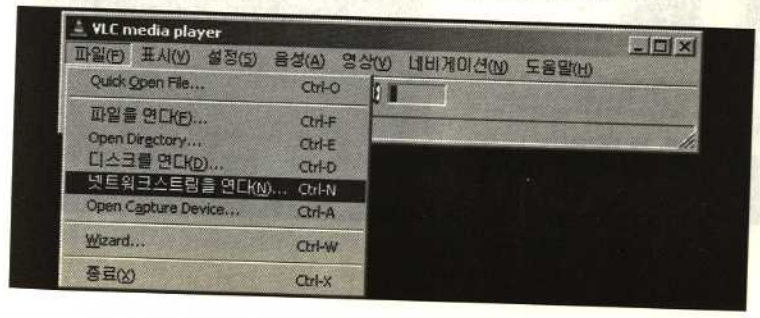


그것을 열면, html 소스들이 텍스트 파일로 나타나는데, 거기에 "비디오 스트리밍 소스"를 찾을 수 있습니다: mms://cast.newscham.net/live

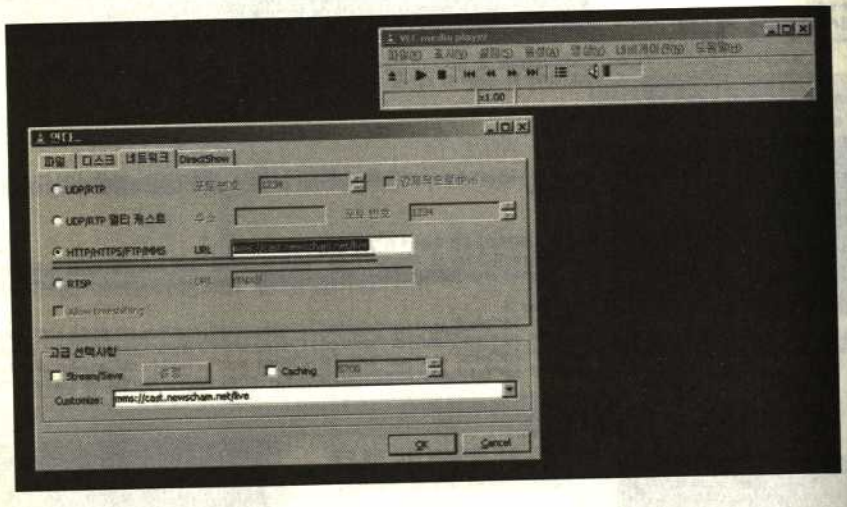


자, 이제 vlc를 엽니다.

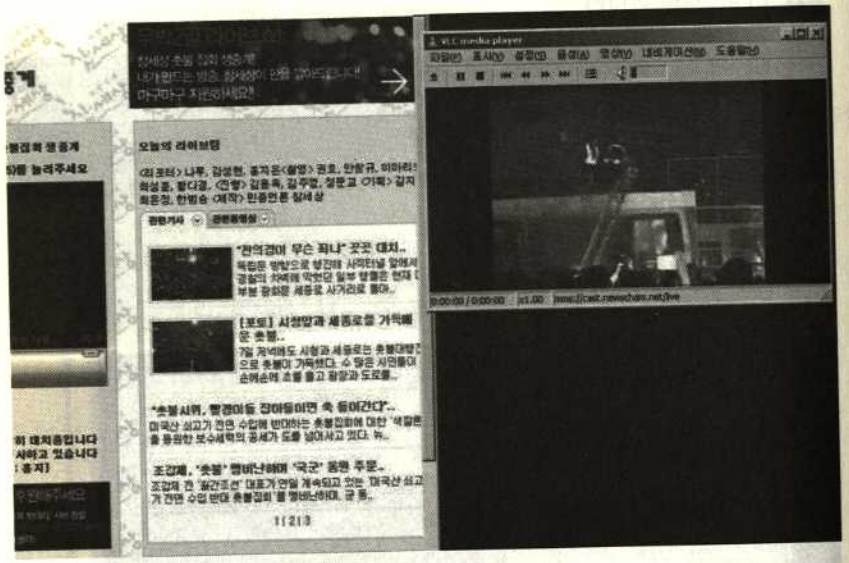
아주 단순하게 보입니다만... 우선 참세상의 촛불집회 생중계를 보기 위해서, "파일(F)" 메뉴를 열고 "넷트워크스트림을 연다"를 클릭합니다.



그러면, 아래 그림과 같이 "연다..." 창이 나오고, 앞서 확인한 참세상의 생중계 소스(mms://cast.newscham.net/live)를 아래 그림과 같이 HTTP/HTTPS/FTP/MMS의 URL에 넣습니다.

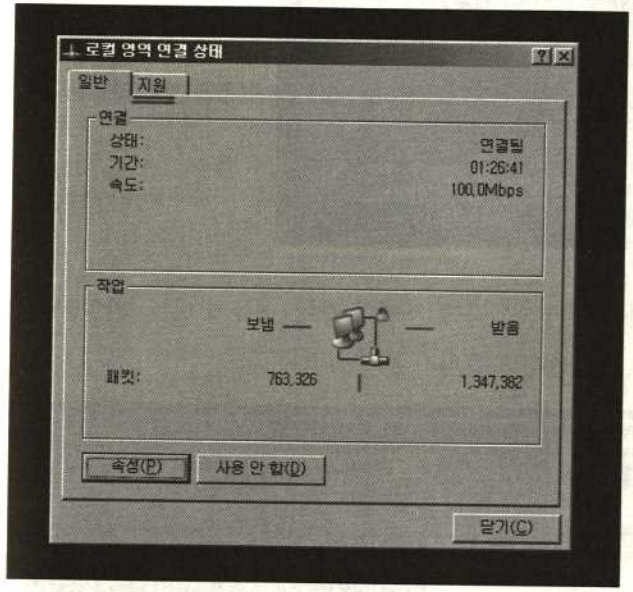


그리고 OK를 누르면 잠시 신호를 확인하면서 생중계가 나오게 됩니다.:

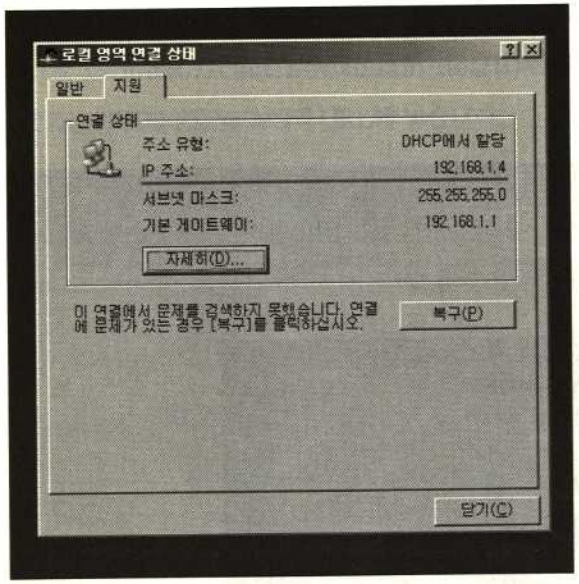


자, 그러면 이제 이렇게 참세상의 생중계를 보면서, 동시에 재전송해보겠습니다.

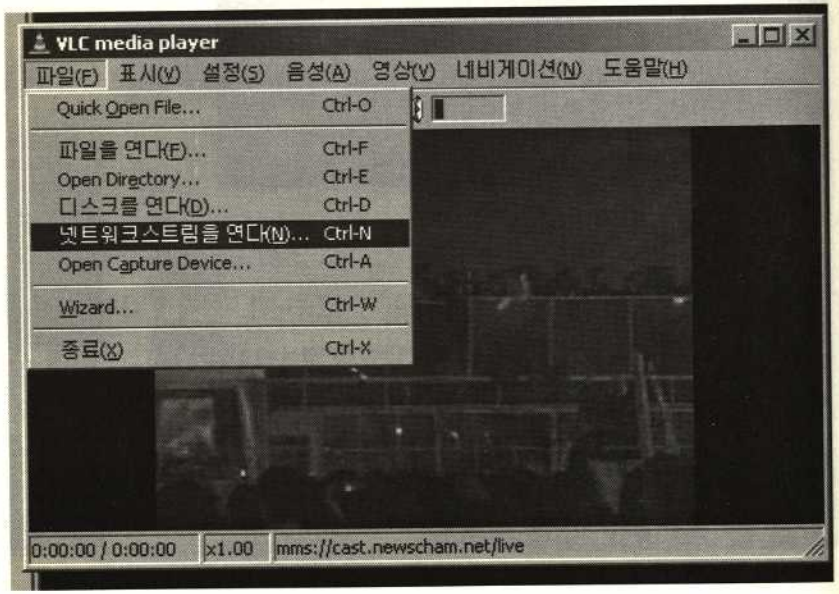
우선, 자신의 컴퓨터의 IP주소를 알아야 합니다. 이를 확인하는 방법은, 제어판이나 오른쪽 아래의 실행 아이콘 등에 있는 인터넷 연결 메뉴를 통해 "로컬 영역 연결 상태"라는 아래와 같은 창을 엽니다.:



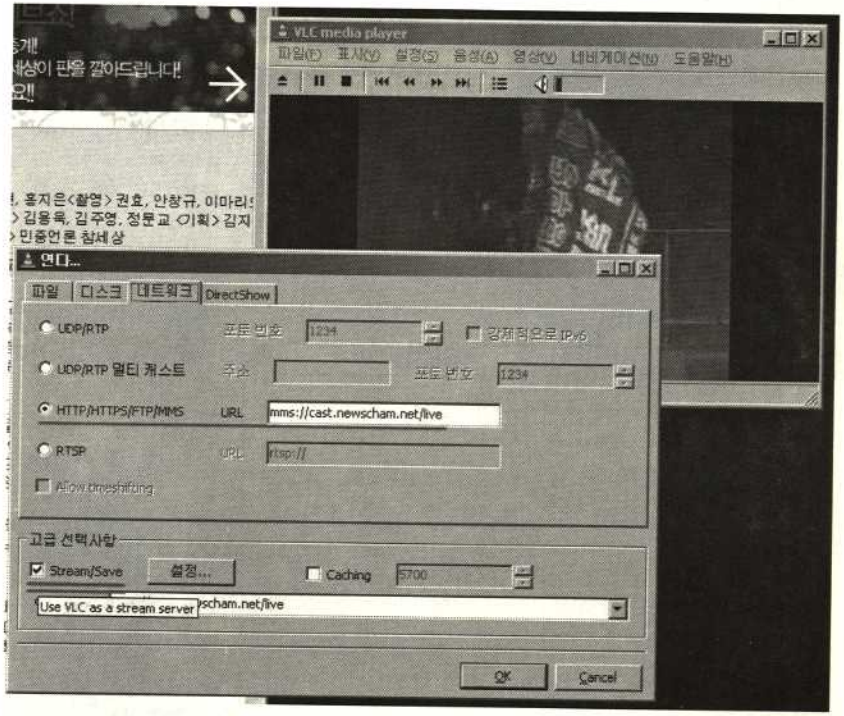
위의 그림의 윗부분에 있는 "지원"이라는 탭을 클릭하게 되면, 아래와 같은 그림이 나오고, 여기에서 IP주소를 확인할 수 있습니다. (아래에 나와 있는 ip는 유동 ip라 실제로는 재전송에 적합하지 않은 정보이긴 합니다. 고정ip를 사용하실 경우에 고정 ip를 확인하여 입력하시거나, 모뎀-공유기를 쓰시는 경우에 공유기 관리 페이지에 가서 포트 포워딩하셔야 합니다.)



자신의 ip 주소가 확인이 되었다면, 아까와 같이, 메뉴에 있는 "파일(F)"에 있는 "넷트워크스트림을 연다..."를 다시 클릭합니다.



"연다..."의 창이 다시 나오고, 제일 아래를 보면 "고급 선택 사항" 중에 "Stream/Save" 항목을 선택하면 됩니다. 그리고 그 옆에 있는 "설정"을 클릭합니다.



아래와 같은 "스트림 출력"이라는 창이 나오는데요...

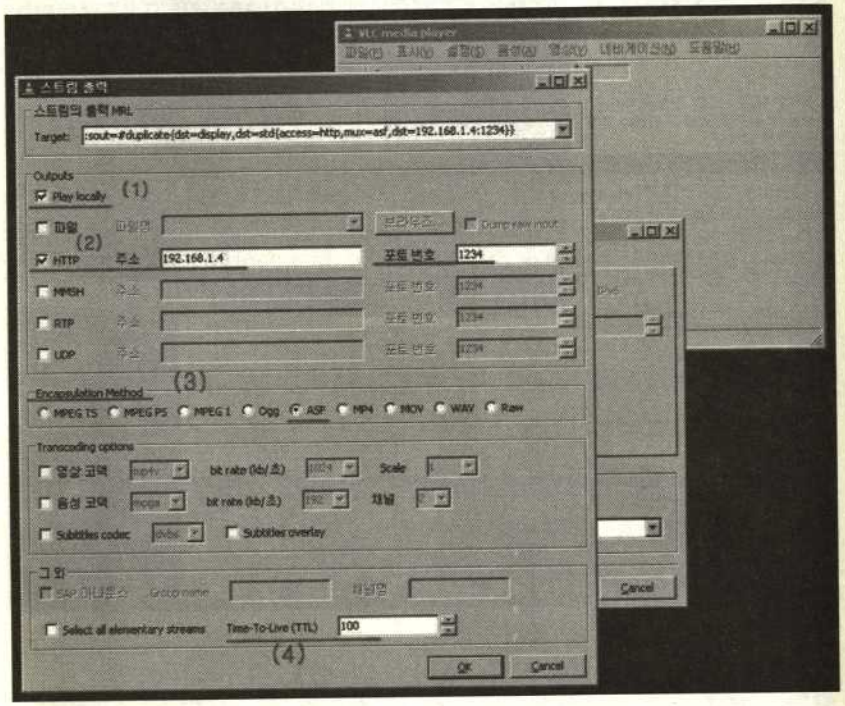
(1) play locally를 클릭합니다.: 이것은 vlc로 생중계를 재전송하면서, 그 생중계를 플레이도 하라는 것입니다.

(2) HTTP 항목에, 인터넷 연결되어 있는 자신의 컴퓨터의 IP주소를 넣습니다. 그리고 포트 번호는 그냥 써 있는 대로 1234로 해도 됩니다.

(3) Encapsulation Method의 경우, 안타깝지만 한국의 경우 주로 윈도우 미디어 플레이어를 사용하니까, 윈도우 미디어를 인코딩하는 ASF를 선택해 줍니다.

(4) 그리고, Time-To-Live의 경우, 얼마나 많은 수의 사람들이 스트리밍을 받을 거냐의 숫자인데요, 1부터 300 정도까지 넣는 것이 보통인 듯합니다. 100으로 넣어봤습니다.

그리고 OK합니다.



그러면, 이제 참세상의 생중계를 보면서, 동시에 나의 컴퓨터로도 생중계를 재전송할 수 있게 되고, 참세상의 서버의 부담을 덜 수 있게 됩니다.

vlc를 통해 재전송하면서, "채팅" 기능 같이 대화를 할 수 있게 텍스트 메시지는 동시에 전송하거나 받을 수 있다면 좋겠지만, 아직까지는 이 정도입니다. 이 정도라도 놀랍니다! 라디오 수신기도 그랬고, "바보상자"로 불렸던 TV 수상기도 역시 경제적인 이유로 송신의 기능은 제거된 채로 생산되어 판매되어 왔습니다. 인터넷을 통해 이제 다시 송수신 모두가 가능한 미디어가 가능하게 되었고, 자유소프트웨어로 개발되어온 vlc는 생중계 – 비디오 스트리밍 차원에서 그런 쌍방향 미디어를 가능하게 하고 있는 것입니다!

자유소프트웨어의 활용은 무엇보다도, 상업적인 서비스의 폐쇄적인 시스템에 비교할 때, 이러한 도구들에 대해 위와 같이, 보다 개방적이고 참여적인 이용자들의 통제를 최대한 가능하게 한다는 것입니다.

Tor 설치매뉴얼

김승욱 | 진보네트워크센터 활동가 saakan99@jinbo.net

1단계: 다운로드

Tor에는 크게 안정화된 버전(stable) 개발 버전(experimental)이 있습니다. 개발 버전이 최신이긴 하지만, 아직 테스트 중인 버전이라 보안문제 등이 있을 수도 있습니다. 물론, 개발버전을 이용하면서 보안문제나 버그등을 신고하는 등 Tor에 기여하는 것도 좋습니다. 현재 Tor의 안정화된 버전은 0.2.0.30 입니다.

윈도우의 경우

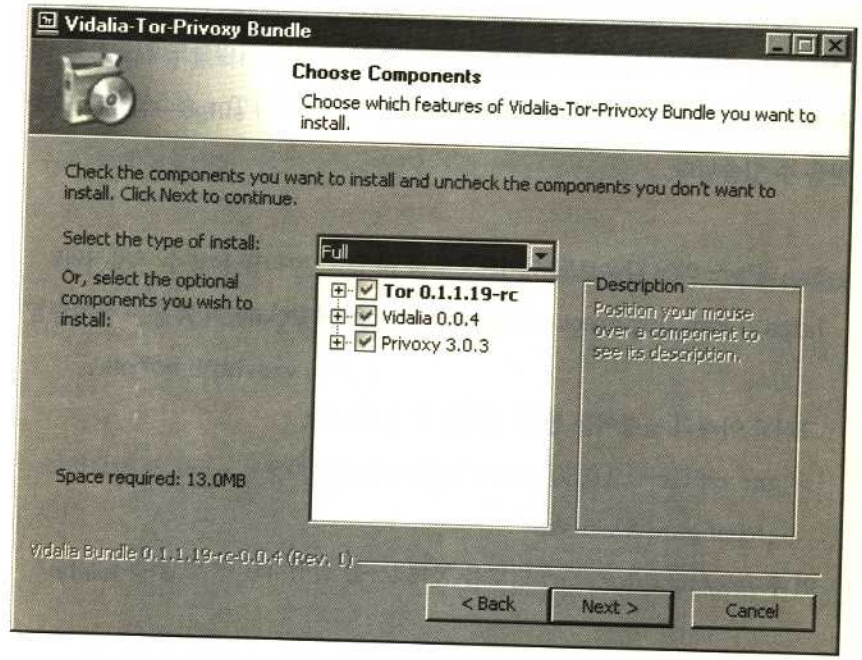
윈도우 버전 통합배포판은 Tor, Vidalia, Privoxy를 포함하고 있습니다. 이들은 모두 자유소프트웨어이고, 따라서 Tor 통합배포판도 자유롭게 사용할 수 있습니다. Vidalia는 Tor를 설정하기 위한 GUI 프로그램이고, Privoxy는 프록

* 편집자주 : 이 매뉴얼은 Tor 클라이언트를 설치하고 사용하기 위한 매뉴얼입니다. Tor가 빠르고 안전하게 유지되기 위해서는 중계서버relay의 역할이 중요한데, 중계서버로 설정하는 방법도 다음 기회에 소개할 것입니다. 웹진 액트온을 놓치지 마세요!

시서버를 이용하여 IP주소를 익명화하고, 불필요하고 위험한 광고/통신을 필터링 해주는 프로그램입니다. 아래의 사이트에서 Tor 통합배포판을 다운받을 수 있습니다.

Tor 다운로드 사이트 : https://www.torproject.org/download.html.ko

Tor를 다운받아 설치를 실행하는 것은 어렵지 않습니다. 만약에 당신의 컴퓨터에 이미 설치된 Tor, Vidalia, Privoxy가 있다면 아래에 보이는 것처럼 대화창에서 해당 프로그램은 제외하고 설치를 진행할 수도 있습니다.



설치가 끝나면 프로그램이 자동으로 실행됩니다.

리눅스의 경우

리눅스의 경우 Tor와 Privoxy를 각각 설치해야 합니다.

Tor 설치

Tor를 설치하기 전에, libevent (http://www.monkey.org/~provos/libevent/)라 는 라이브러리를 먼저 설치해야 합니다. 그리고 openSSL과 zlib이 설치되어 있는지도 확인해야 하구요. ubuntu의 경우 시냅틱 꾸러미 관리자에서 Tor를 바로 설치할 수 있습니다. ubuntu는 위에서 언급했던 libevent 등 필요한 몇가지 파일들도 자동으로 설치해 줄 것입니다. 다른 리눅스의 경우 아래의 사이트에서 Tor 소스코드를 다운받을 수 있습니다.

Tor 리눅스 버전 다운로드 사이트 :
https://www.torproject.org/download-unix.html.en

그리고 아래의 명령어를 통해 설치를 하면 됩니다.

```
tar xzf tor-0.2.0.30.tar.gz; cd tor-0.2.0.30
./configure && make
```

이 후 /etc/init.d/tor start 명령을 통해 tor를 실행시킬 수 있습니다.

Privoxy 설치

ubuntu의 경우 Tor와 마찬가지로 시냅틱 꾸러미 관리자에서 Privoxy를 바로 설치할 수 있습니다. (시냅틱 꾸러미 관리자에서 Pricoxy 검색) 다른 리눅스의 경우 아래의 사이트에서 해당 Privoxy 버전을 다운받을 수 있어요.

Privoxy 홈페이지 : http://www.privoxy.org/

Privoxy는 설치 후 약간의 설정이 필요합니다. Privoxy가 설치된 폴더(/etc/privoxy)에서 config라는 설정파일 엽니다. 그리고 아래의 내용을 파일에 입력합니다. 위치는 상관없지만, 마지막 "."을 빼먹지 않는 것에 주의하세요.

```
forward-socks4a / 127.0.0.1:9050 .
```

그리고 같은 파일에서 아래 두 줄을 찾아서 코멘트 처리해야 합니다. 즉 각 줄의 맨 앞에 #를 입력해야 됩니다.

```
logfile logfile
jarfile jarfile
```

위와 같은 수정이 끝나면, config 파일을 저장하고 닫습니다. 그리고 아래의 명령어를 이용해 Privoxy를 다시 시작해야 합니다.

```
/etc/init.d/privoxy restart
```

이것으로 Privoxy 설정도 끝났습니다.

Vidalia 설치

Tor와 Privoxy의 설정을 도와주는 Vidalia를 설치하고 싶다면, 아래의 소스리스트 추가 후 시냅틱 꾸러미 관리자를 통해 설치할 수 있습니다.

Ubuntu Hardy 사용자들

deb http://ppa.launchpad.net/adnarim/ubuntu hardy main
deb-src http://ppa.launchpad.net/adnarim/ubuntu hardy main

Ubuntu Gutsy 사용자들

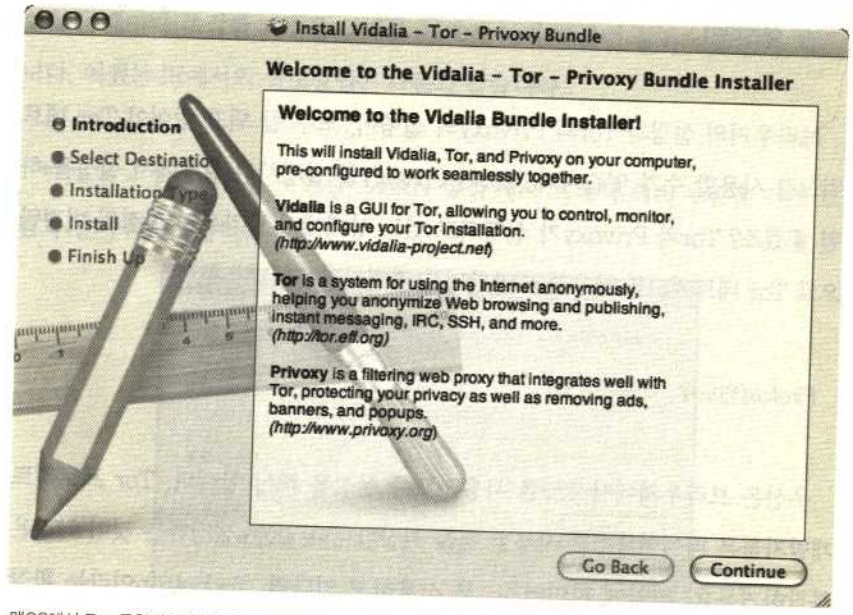
deb http://ppa.launchpad.net/adnarim/ubuntu gutsy main
deb-src http://ppa.launchpad.net/adnarim/ubuntu gutsy main

또는 Tork라는 통합관리툴도 시냅틱 꾸러미 관리자를 통해 설치할 수도 있습니다. 이것들이 필수는 아닙니다. 다만 설정과 관리를 편리하게 도와주는 프로그램들입니다.

맥OS의 경우

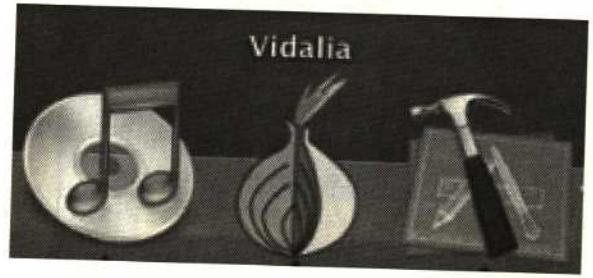
맥OS의 통합배포판에도 Vidalia, Tor, Privoxy가 함께 포함되어 있고, 설치하는 방법은 윈도우와 비슷합니다. 아래의 사이트에서 맥OS 버전 Tor를 다운받을 수 있습니다.

Tor 다운로드 사이트 : https://www.torproject.org/download.html.ko



맥OS에서 Tor 통합배포판 설치모습

설치가 끝난 후 Application 폴더에서 Vidalia를 실행시킬 수 있습니다. X 표시가 된 검정색의 양파 아이콘은 Tor가 실행되지 않고 있음을 의미합니다. 화면 위의 Tor 메뉴를 클릭해서 Tor를 실행시킬 수 있습니다. Tor가 실행 중일 때는 아래처럼 녹색의 양파 아이콘이 나타납니다.

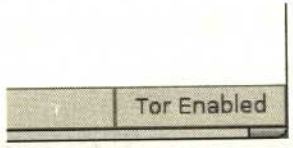


Privoxy는 컴퓨터가 재부팅될 때 자동으로 실행됩니다.

브라우저의 설정과 Tor와 Privoxy의 실행이, 모두 잘 되고 있어야 Tor 네트워크를 사용할 수가 있습니다. Tor와 Privoxy를 실행시킨 상태에서 설정을 하면 좋겠죠? Tor와 Privoxy가 실행되고 있는 상태에서 브라우저 설정의 변경만으로 Tor 네트워크를 사용할지 안할지를 결정할 수 있습니다.

Firefox(윈도우, 리눅스, 맥)

우선은 브라우저에서 Tor를 사용하도록 설정을 해야 합니다. Tor 프로젝트 개발자들은 파이어폭스를 사용할 것을 권장합니다. IE는 설정하는 것이 약간은 복잡하거든요. 만약에 파이어폭스를 사용하고 있다면, Torbutton이라는 확장 기능이 자동으로 설치될 것입니다. 만약에 설치가 안 된다면 파이어폭스 사이트에서 Torbutton을 다운받아 설치하면 됩니다. 이걸로 파이어폭스 Tor설정은 끝입니다.



파이어폭스에 Torbutton이 설치된 모습

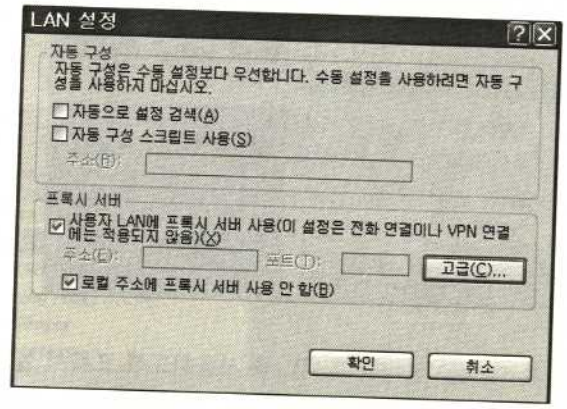
이 후 Torbutton에 마우스 오른 쪽 버튼을 클릭해서 Tor를 활성화시키거나 비활성화시킬 수 있습니다. 이것은 매우 편리한 기능입니다.

Explorer(윈도우)

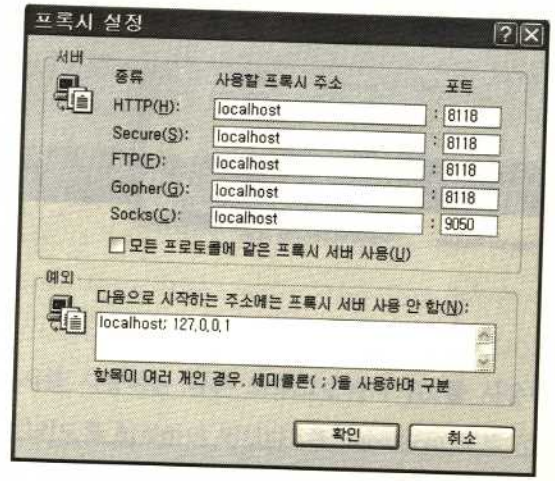
IE에서 Tor를 설정하는 것은 약간 복잡합니다. 또 Tor를 활성화하거나 비활

성화할 때마다 복잡한 과정을 그대로 거쳐야 하기 때문에 골치 아플 수도 있습니다. 어쨌든 IE에서의 설정방법은 다음과 같습니다.:

* "도구 – 인터넷옵션 – 연결 – LAN 설정"에서 프록시 서버 부분을 아래 그림과 같이 체크해줍니다.



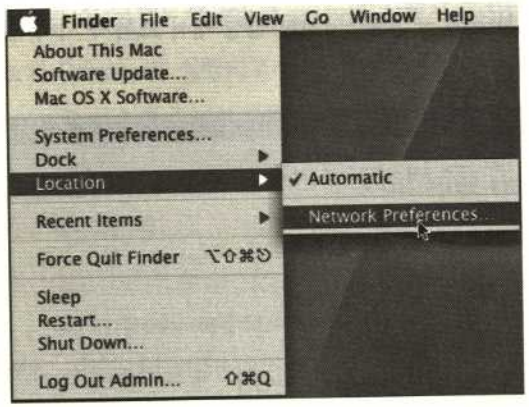
계속해서 프록시 서버 설정의 고급 탭을 클릭한 후 프록시 주소, 포트, 예외사항에 아래 그림과 같이 입력합니다.



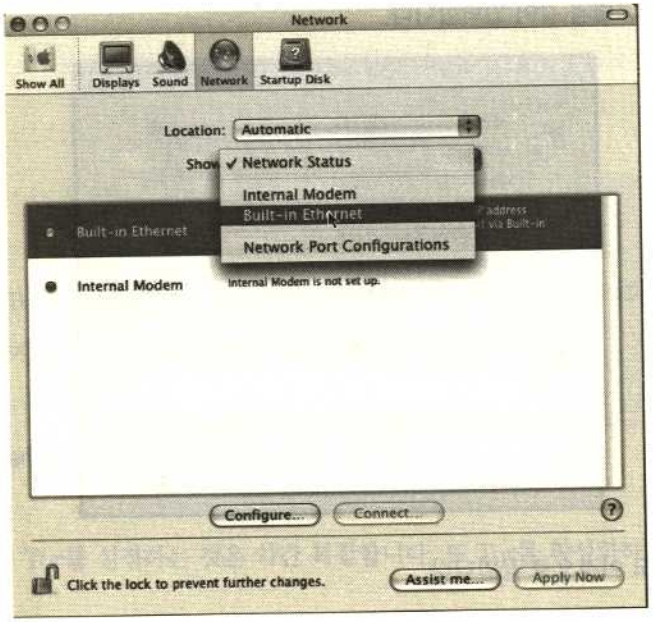
IE 설정도 이것으로 끝입니다.

Safari(맥)

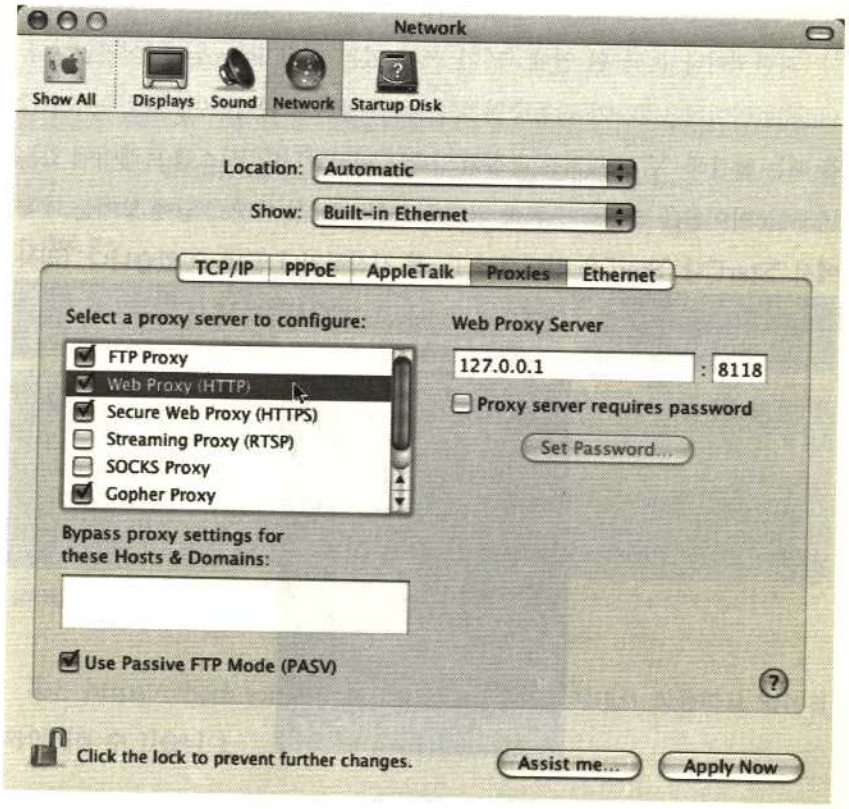
사파리에서 Tor를 사용하려면 네트워크 설정을 변경해줘야 합니다. 아래 그림에 보이는 것처럼 Apple – Location – Network Preference를 선택합니다.



Network Interface를 선택한 후, Tor를 사용하도록 프록시 설정을 변경해줘야 합니다. 만약에 다수의 인터페이스에서 Tor를 사용하고 싶다면 각각의 설정을 변경해줘야 합니다.



웹 프록시(HTTP)와 HTTPS 모두에 127.0.0.1과 포트번호 8118을 입력하세요. FTP 프록시와 Gopher 프록시의 설정도 위와 같이 변경해줘야 합니다.



이것으로 사파리에서도 Tor를 사용할 수 있습니다.

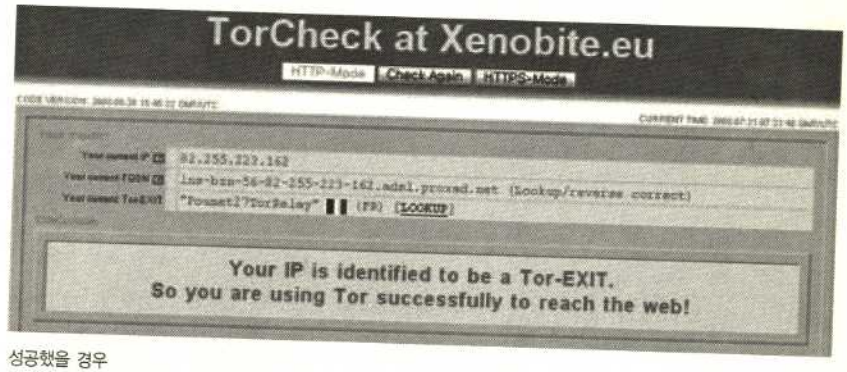
기타

HTTP 프록시를 사용하는 다른 프로그램에서 Tor를 사용하려면, 그들이 Privoxy를 가리키도록 설정하면 됩니다. 즉, localhost 포트 8118으로 연결하면 됩니다. SOCKS를 직접 연결해서 사용하려면(메신저, Jabber, IRC 등), localhost 포트 9050으로 연결시키면 됩니다.

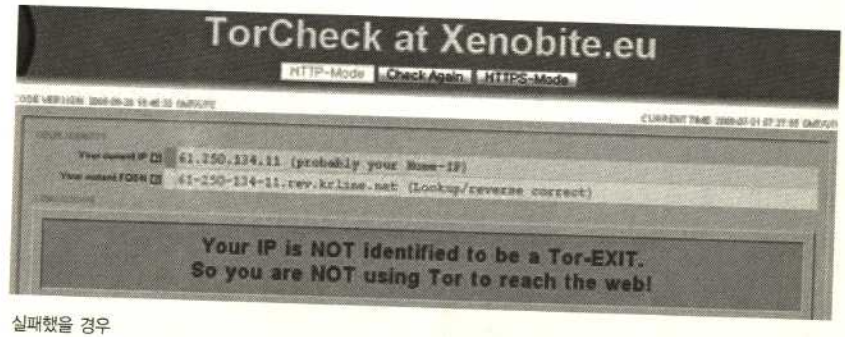
3단계: 확인하기(공통)

설치를 한 후에 Privoxy와 Vidalia가 잘 작동하고 있는지 확인이 필요합니다. 파란색이나 녹색 원 안에 "P"가 쓰여 있는 것이 Privoxy 아이콘입니다. Vidalia 아이콘은 Tor가 작동중일 때는 녹색 양파로 나타나며, 작동중이지 않을 때는 빨간색 "X"가 새겨진 검정색 양파로 나타납니다. 시스템 트레이에 있는 Vidalia 아이콘을 마우스 오른쪽 버튼으로 클릭한 후 아래 그림에 보이는 메뉴에서 "Start"나 "Stop"을 선택해서 Tor를 시작하거나 끝낼 수 있습니다. (리눅스의 경우 Vidalia를 설치 안했다면 Vidalia는 해당사항 없음)

또 IP주소가 제대로 익명화되고 있는지 확인이 필요합니다. 설정이 잘못되었을 경우, 익명화가 되지 않고 이는 Tor를 설치하기 전과 다를 바가 없습니다. Tor의 설치와 설정이 끝낸 후 http://torcheck.xenobite.eu/ 를 방문해보세요. 이 사이트에서는 당신의 IP주소가 무엇인지, 그것이 Tor를 통하여 익명화가 되고 있는지 알려줍니다. 아래와 같은 그림이 나온다면 성공입니다. 실패할 경우 그 아래에 있는 붉은색의 경고메세지가 나올 것입니다.



성공했을 경우



실패했을 경우

혹은 https://check.torproject.org 에서도 Tor가 제대로 작동하고 있는지 확인해볼 수 있습니다.

그리고

Tor의 공식 홈페이지(https://www.torproject.org/)에 서 더 많은 정보들을 확인하실 수 있습니다. 특히 Tor가 무엇을 할 수 있고, 무엇을 할 수 없는지 명확하게 이해하고 사용하는 것이 중요합니다. 이것은 완벽한 보안/프라이버시가 아닐 뿐더러, 잘못 사용할 경우 아무런 기능도 할 수 없습니다. 이 매뉴얼을 따라 잘 안되는 게 있다면, 덧글을 달아주세요. 혹시 해결책을 찾았다면 매뉴얼을