

inspector 구현 원리 기술 설명서

inspector 는 자체적으로 로그를 적재하여 보관할 로그 서버, 그리고 로그를 분석할 웹 분석툴을 필요로 합니다. 이렇게 두가지의 로그 서버 + 웹 클라이언트 툴을 제공하며 인터페이스는 매우 간단하게 구성되어 있습니다.

일반적으로 사이트에 설치되고 나면 기록하는 정보는 크게 10 가지로 구분할 수 있습니다.

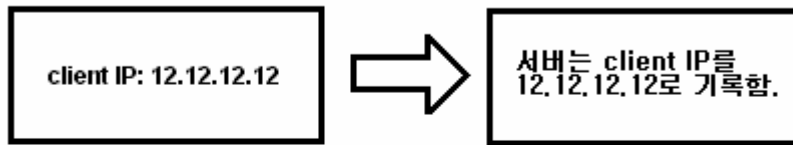
1. IP 주소
2. 식별 코드
3. 접속 시간
4. 웹 브라우저, 운영체제 버전
5. 참조 URL
6. 프록시 서버
7. 실제 IP

이와 같은 정보는 접속해오는 클라이언트를 충분히 구별해주는 주요 정보입니다.

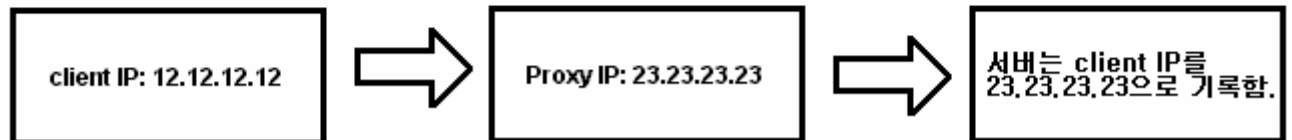
우선, IP 주소는 접속해오는 client 의 일반적인 IP 를 기록합니다.

예를 들어, IP 주소가 12.12.12.12 인 사용자가 접속해올 경우. client 의 IP 는 12.12.12.12 로 기록됩니다. 하지만, 프록시 서버를 경유할 경우, 사용자의 실제 IP(Real IP)가 아닌, 프록시 서버 IP 를 기록하게 됩니다.

✦ 일반적인 경우:



✦ 프록시를 경유했을 경우:



이것이 현재 모든 웹서버 및 공통적으로 로그에 기록되는 방식입니다.

그렇기 때문에 프록시를 경유한 사용자를 추적하는 것은 거의 불가능합니다.

이에 따라 프록시 사용자는 인터넷 상에서 익명을 보장받아 게시판에 악의적인 게시물을 작성하여 올리며, 실제 해킹 공격 시에도 프록시 서버를 경유하는 일이 빈번히 발생하게 되었습니다.

이에 따라, 프록시 사용자를 구분해줄 특별한 코드가 필요하게 되었습니다.

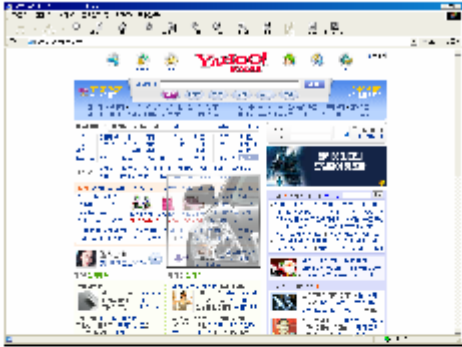
이런 동기에 의해 개발된 아이디어가 바로, 식별 코드입니다.

식별 코드는 사용자가 사이트에 처음 접속 시, 기록되는 고유의 IP를 랜덤 코드(random size)와 결합하여 클라이언트 PC에 저장하게 됩니다.

웹 브라우저 변수 중, 저장에 용이하고, 매우 오랜 기간동안 사용할 수 있는 것이 바로,

cookie 및 session입니다. 그리하여, 저희 INetCop 개발팀은 이 기술을 적용하여 개발했습니다.

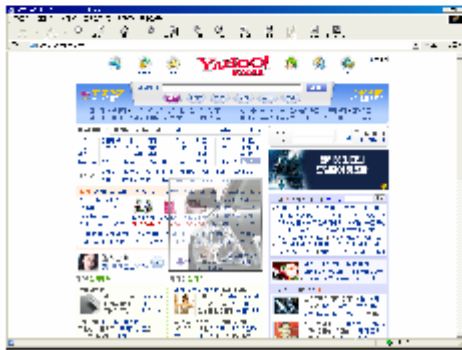
* 해당 사이트에 처음 접속했을 시,



웹 브라우저에 cookie time을 MAX로
설정하여 브라우저 변수로 선언함.

예: 12,12,12,12,10238924

* 해당 사이트에 재접속 시,



프록시를 사용하거나, IP가 변경된 것과
상관없이 여전히 고유 코드로 선언했던

식별 코드: 12,12,12,12,10238924

사용자로 식별하여 구분됨.

위와 같이, 사이트 처음 접속 시 선언된 고유 코드를 통해 이전 사용자와 같은 사용자인지, 다른 사용자인지의 여부를 쉽게 판단할 수 있습니다. 이에 따라, 악의적인 글을 익명으로 남기는 사용자가 동일인인지의 여부를 검사할 수 있게 되었습니다. 또한, 접속 시간, 웹 브라우저, 운영체제 버전을 통해 기본적인 정보 사항을 얻을 수 있습니다.

그럼, 지금부터 프록시에 대해 설명하고, 역추적하는 원리를 간단하게 설명하도록 하겠습니다.

프록시 서버는 크게, 3 가지로 구분되어 있습니다.

그 종류는 프록시 타입에 따른 것으로, 이 프록시 타입에 따라 익명성이 보장되는지의 여부가 판단됩니다.

1. Transparent

이 종류의 프록시는 웹 요청 시도시 서비스요청 헤더 부분에 client의 IP를 함께 포함합니다. 이 때문에 서버에서는 서비스요청을 시도하는 클라이언트가 보내는 패킷의 헤더를 검사하면, 충분히 client의 IP를 추적할 수 있습니다.

헤더 포함 내용: 프록시 서버 종류, client 실제 IP

```
GET /HTTP/1.0
Accept: */*
Referer: http://inetcop.org/
Accept-Language: ko
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)
Host: inetcop.org
Via: 1.0 localhost.localdomain:6501 (Squid/2.2.STABLE4)
X-Forwarded-For: 211.171.151.20
Cache-Control: max-age=259200
Connection: keep-alive
```

분석된 헤더를 살펴보면, "Via:" 부분이 바로 프록시 서버의 종류를 뜻하는 것이고, "X-Forwarded-For:" 부분 다음 부터가 client의 실제 IP를 뜻합니다.

이와 같이 Transparent type proxy는 추적하기가 쉽다는 장점이 있습니다.

참고로, 기존에 존재하고 있는 대부분의 프록시 추적 프로그램이 바로 이 Transparent 역추적 위주의 소프트웨어입니다.

2. Anonymous

이 종류의 프록시는 client의 IP를 완벽하게 숨기지만, 프록시를 사용 중이라는 표시를 헤더에 포함합니다. 예를 들면, 프록시 서버의 종류만 나타나고, 실제 client의 IP는 헤더에 포함하지 않습니다. 바로 이 anonymous type proxy부터, 역추적에 많은 어려움을 겪습니다.

헤더 포함 내용: 프록시 서버 종류

```
GET / HTTP/1.1
Accept: */*
Referer: http://inetcop.org/
Accept-Language: ko
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)
Host: inetcop.org
Cache-Control: max-stale=0
Connection: close
X-BlueCoat-Via: F14E1FDF3145AE51
```

위와 같이 요청 헤더에 Via 코드만 포함됩니다.

이 때문에 서버에서 요청 패킷을 캡처한다해도, 역추적이 불가능합니다.

3. High anonymous

이 종류의 프록시는 client 의 IP 뿐만아니라, 프록시를 사용 중이라는 표시조차되지 않습니다.

헤더는 일반 client 접속과 동일하게 작성되며, 서버에서 요청 패킷을 캡처해도 일반 client 패킷과 전혀 구별되지 않습니다. 이 때문에 현재 기술력으로 서버는 high anonymous type proxy 사용자와 일반 client 사용자를 전혀 구별해낼 수 없습니다.

헤더 포함 내용: 없음

```
GET / HTTP/1.0
Accept: */*
Referer: http://inetcop.org/
Accept-Language: ko
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)
Host: inetcop.org
Pragma: no-cache
Connection: keep-alive
```

요청 헤더에는 일반 client 접속과 구별할만한 포함 내용이 존재하지 않으므로 역추적이 불가능합니다. 이렇게 프록시 종류의 3 가지를 알아본 이유는, 현재 기술적으로 역추적이 가능한 프록시가 매우 적다는 현실을 알리기 위해서 입니다.

이 3 가지 프록시 종류를 완벽하게 파악하고 있는 해커나 전문가, 엘리트 사용자들은 완벽한 익명성을 이용해 인터넷상을 활보하고 있습니다. 하지만 정작 접속해오는 사용자들을 분석하여 로그에 기록하는 서버는 이러한 사실 조차 구분하지 못하며 공격에 시달리고, 악의적인 게시물, 스팸 공격을 받고 있는 것이 현실입니다.

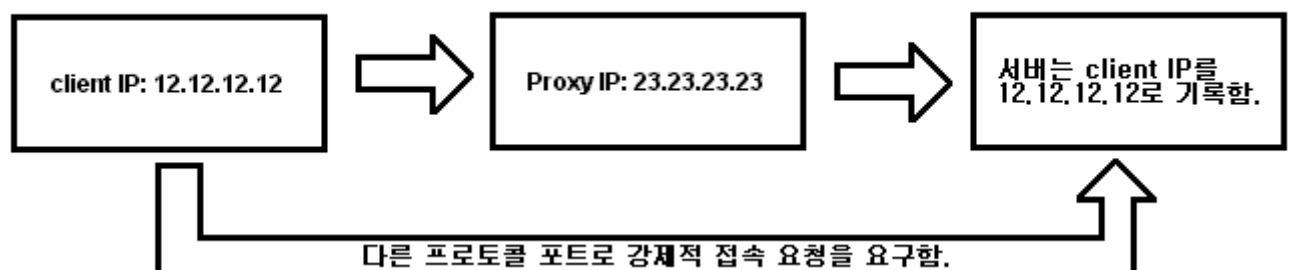
여기서 저희 inspector 솔루션의 추적불가능 프록시를 역추적하는 원리를 간단히 설명드리도록 하겠습니다.

* 해결 방안

우선 기존의 anonymous 는 헤더에 proxy 임을 표시하는 프록시 서버 종류를 포함합니다. 이 덕분에 proxy 사용 여부를 쉽게 판단할 수 있습니다.

우선 프록시 사용자로 밝혀졌을때, 실제 Real IP 를 추적하는 방법은 클라이언트 사용자로 하여금 사용 중인 프록시 웹 브라우저를 벗어나게끔 트릭을 사용하는 것입니다. 즉, 프록시 사용자가 프록시 지원 프로토콜이 아닌 다른 프로토콜 포트로 요청하게끔 요구하는 방식입니다. 이를 통해, 사용자의 실제 Real IP 를 얻을 수 있으며, client 사용자 PC 에 따로 무엇인가를 설정하거나 설치하는 방법이 아니므로, 인터넷을 사용하는 모든 client 의 역추적이 가능합니다.

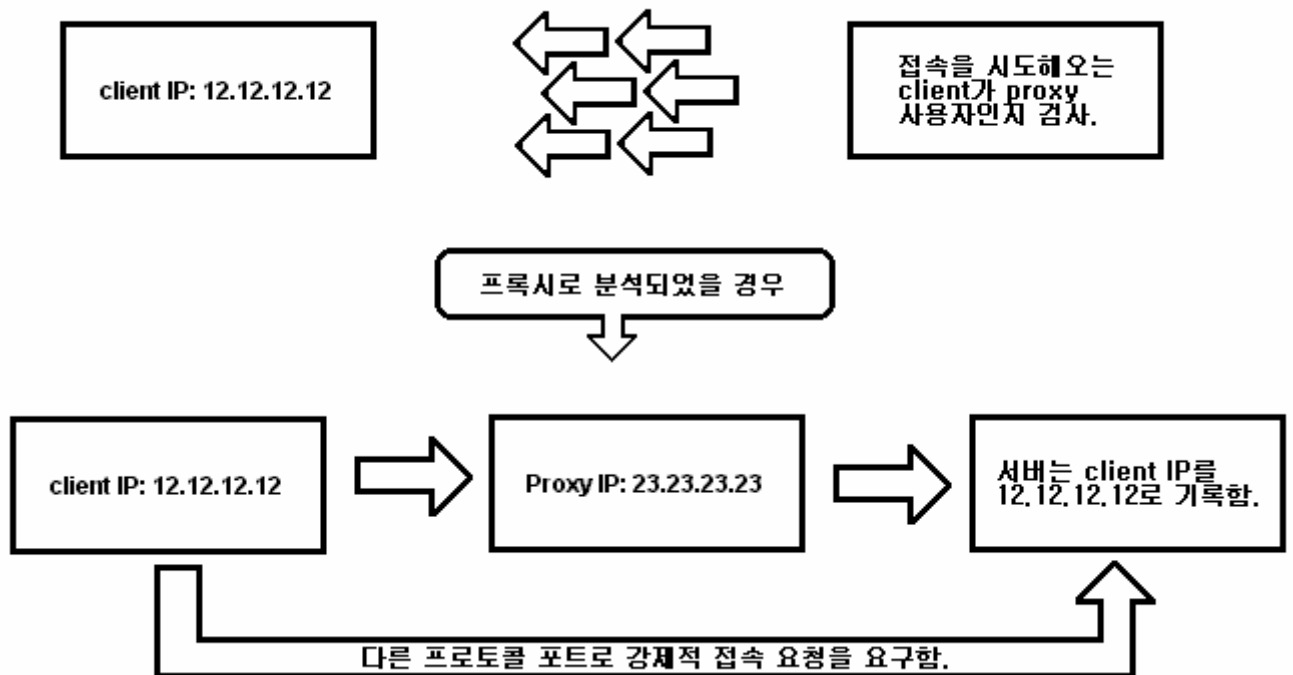
* Anonymous 역추적 방식:



문제는 high anonymous type proxy 의 역추적 가능 여부입니다.

이 proxy 는 속성상 일반 client 와 구별할 수 없는 비슷한 요청을 해오기 때문에 현실적으로 역추적이 불가능합니다. 하지만, 이 client 사용자 역시 접속을 시도하는 port 비교 및 프록시 port 검사 작업을 통해 high anonymous type proxy 사용자인지 구별이 가능합니다. 이렇게 구별된 사용자는 위의 역추적 방식을 그대로 적용하여, 실제 IP 를 얻어낼 수 있습니다.

★ High anonymous 역추적 방식:



이로 인해 client 를 대상으로 하여, 완벽한 역추적이 가능해졌습니다.

* 2005년 03월 추가 내용 *

해커 역 추적 기술로 사용될 수 있는 솔루션의 원리를 2005년 03월 특허로 출원하게 되었습니다.

출원번호통지서

페이지 1 / 1

관인생략 출원번호통지서

출원일자 2005.03.11
특기사항 심사청구(유) 공개신청(무)
출원번호 10-2005-0020368 (접수번호 1-1-2005-0128924-05)
출원인명칭 (주)아이넷캡(1-2005-008762-4)
대리인성명 유기현(9-1999-000242-7)

특 허 청 장

1. 출원번호통지서 출원 이후 심사진행 상황 등을 확인하실 때에는 출원번호가 없으므로 출원 번호통지서는 출원필차기 종료일 때까지 보관하시기 바랍니다.
2. 심사 특허출원은 출원 공개 후 (출원일로부터 1년 6개월 경과) 심사청구순서에 따라, 의장등특 출원 및 상표등특 출원은 출원순서에 따라 심사하여 심사결과를 출원인에게 통지합니다.
3. 심사청구 특허출원은 출원일로부터 5년 이내에 특허법시행규칙 별지 제24호서식에 의거 심사청구를 하지 않으면 그 출원은 출원취하한 것으로 간주하여 처리함을 알려드립니다.
4. 우선심사 특허출원 또는 의장등특출원에 대해 조기에 심사받기를 원하시면 우선심사제도 등에 응하실수 있습니다. (★ 우선심사의 대상, 신청필차 등 자세한 내용은 특허청 홈페이지 <http://www.kipo.go.kr> 지재권제도안내의 우선심사안내코너를 참조하시기 바랍니다.)
5. 기술평가 실용신안의 경우 제3자에 대하여 권리행사를 하기 위해서는 기술평가를 청구하여 등 록유지결정을 받아야 하며 기술평가청구순서에 따라 기술평가를 실시합니다.
6. 주소 등 변경신고 출원인의 주소 등을 변경하고자 하는 경우에는 특허법 시행규칙 별지 제4호 의 2서식에 의한 출원인 정보변경(경정) 신고서를 제출하여야 합니다. 신고서식은 지방 상공회의소에 비치되어 있으며, 특허청 홈페이지(<http://www.kipo.go.kr>)에 게재되어 있습니다.
7. 산업재산권 표시, 광고요청 특허 등 산업재산권을 출원 중에 있는 경우에는 해당 산업재산이 출원상태임을 다음과 같이 표시하여야 하며, 이를 위반할 경우 특허법 제224조 및 제227조에 의거 처벌 받게 됩니다.
예) 특허출원 10-2001-0000001, 실용신안등록출원 20-2001-0000001, 의장등록출원 30-2001-0000001, 상표등록출원 40-2001-0000001
8. 문의처 기타 문의사항이 있으시면 우리청 종합민원실(042-481-5220~2)이나 출원과(042-481-5201~5) 또는 특허청 서울 사무소(02-568-6079)에 문의하시거나 특허청 홈페이지 (<http://www.kipo.go.kr>)를 참고하시기 바랍니다.
9. 특허청 주소 302-701 대전광역시 서구 둔산동 920 정부대전청사 4동
특허청 서울사무소 주소 135-911 서울특별시 강남구 역삼동 647-9 한국지식센터
FAX) 대전 : 042-472-7140, 서울 : 02-568-8454



방 식 심 사 관	당	당	심	사	관

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2005.03.11

【발명의 국문명칭】 웹 접속자 위치 추적 시스템 및 그 추적 방법

【발명의 영문명칭】 System and the method for tracking a position of Web user

【출원인】

【명칭】 (주)아이넷컴

【출원인코드】 1-2005-008762-4

【대리인】

【성명】 유기현

【대리인코드】 9-1999-000242-7

【포괄위임등록번호】 2005-017979-6

【발명자】

【성명의 국문표기】 유동훈

【성명의 영문표기】 YOU, Dong-Hun

【주민등록번호】 [REDACTED]

【우편번호】 [REDACTED]

【주소】 [REDACTED]

【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사를 청구합니다.

대리인

유기현 (인)

