11. 클라이언트 식별과 쿠키

웹 서버는 요청을 보낸 사용자를 식별하거나 방문자가 보낸 연속적인 요청을 추적하기 위해 약간의 정보를 이용할 수 있다.
아마존과 같이 웹 사이트들은 개인화된 서비스를 제공하고 싶어 하는데, 이 때 HTTP에서 사용자 식별이 가능하도록 정보를 제공한다.

- 사용자 식별 관련 정보를 전달하는 HTTP 헤더들
- 클라이언트 IP 주소 추적으로 알아낸 IP 주소로 사용자를 식별
- 사용자 로그인을 통한 사용자 식별
- URL에 식별자를 포함하는 기술인 fat URL
- 식별 정보를 지속해서 유지하는 강력하면서도 효율적인 기술인 쿠키

11.2 HTTP 헤더

사용자 식별에 활용되는 헤더는 From, User-Agent, Referer 3가지 이다.

헤더 이름	헤더 타입	설명
From	요청	사용자의 이메일 주소
User-Agent	요청	사용자의 브라우저
Referer	요청	사용자가 현재 링크를 타고 온 근원 페이지
Authorization	요청	사용자 이름과 비밀번호(뒤에서 다룸)
Client-ip	확장(요청)	클라이언트의 IP 주소(뒤에서 다룸)
X-Forwarded-For	확장(요청)	클라이언트의 IP 주소(뒤에서 다룸)
Cookie	확장(요청)	서버가 생성한 ID 라벨(뒤에서 다룸)

표 11-1 사용자에 대한 정보를 전달하는 HTTP 헤더

11.3 클라이언트 IP 주소

세션 간 사용자를 추적하기 위해 클라이언트 IP 주소를 사용하는 웹사이트가 있지만, 제대로 동작하지 않을 가능성이 있기에 사용하지 않는다.

11.4 사용자 로그인

사용자 이름과 비밀번호 인증 (로그인) 을 요구하여 명시적인 식별 정보를 요청할 수 있다. 사이트에 한 번만 로그인하면, 브라우저는 요청마다 해당 사용자의 식별정보 토큰을 Authorization 헤더에 담아 서버로 전송하여 한 세션이 진행되는 내내 그 사용자에 대한 식별을 유지한다.

11.5 뚱뚱한 URL

URL에 식별번호를 추가하여 사용자를 추적한다. 웹 서버와 통신하는 독립적인 HTTP 트랜잭션을 하나의 '세션' 혹은 '방문'으로 묶는 용도로 뚱뚱한 URL을 사용할 수 있다.

11.6 쿠키

쿠키는 사용자를 식별하고 세션을 유지하는 방식 중 현재까지 가장 널리 사용하는 방식이다.

11.6.1 쿠키의 타입

- 세션 쿠키: 사용자가 사이트를 탐색할 때, 관련한 설정과 선호 사항들을 저장하는 임시 쿠키. 사용자가 브라우저를 닫으면 삭제된다. Discard 파라미터가 설정되어 있거나, 파기되기까지 남은 시간을 가리키는 Expires 혹은 Max-Age 파라미터가 없으면 세션 쿠키가 된다.
- 지속 쿠키: 삭제되지 않고 더 길게 유지된다. 디스크에 저장되어 브라우저를 닫거나 컴퓨터를 재시작해도 남아있다.

11.6.2 쿠키는 어떻게 동작하는가

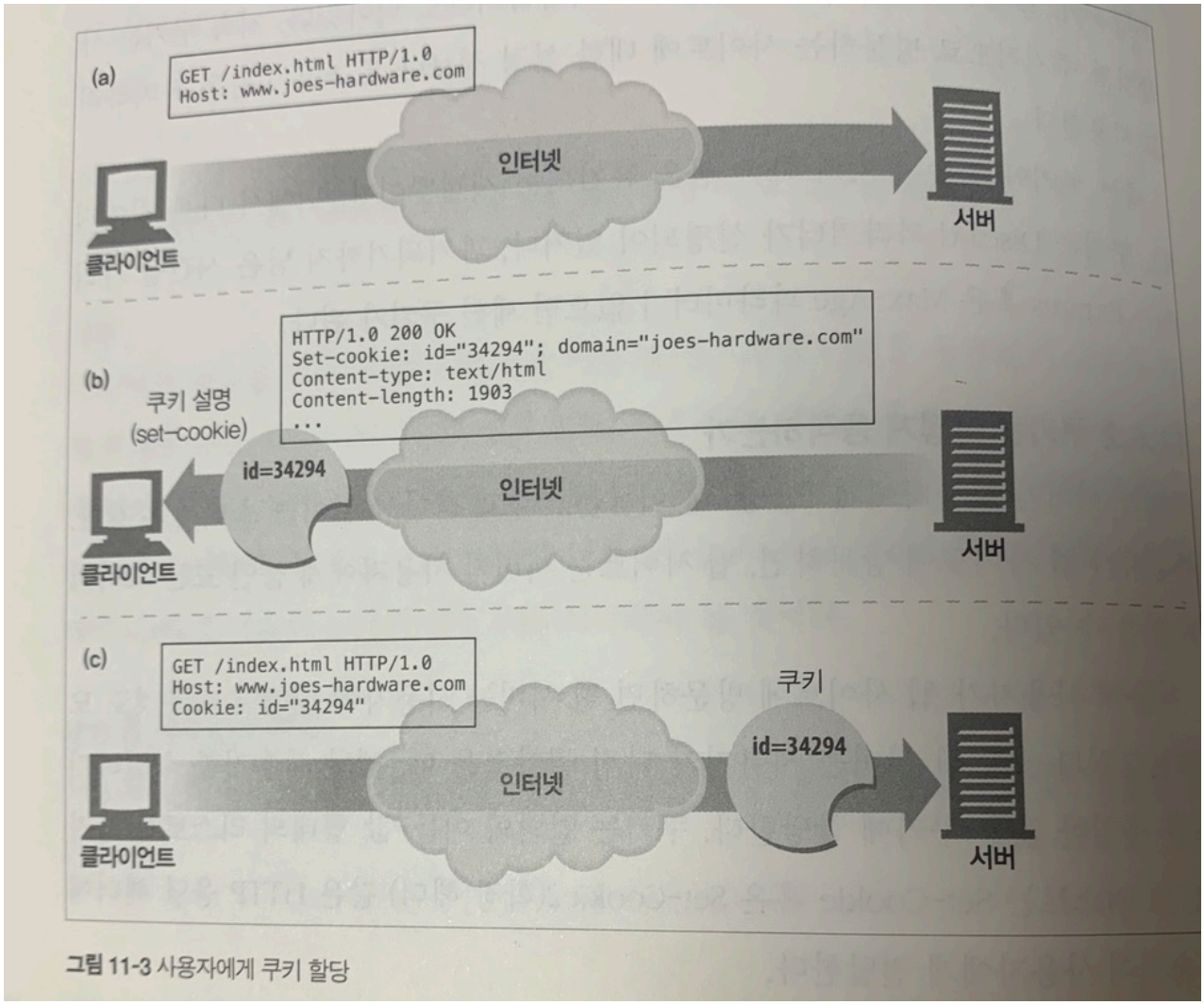
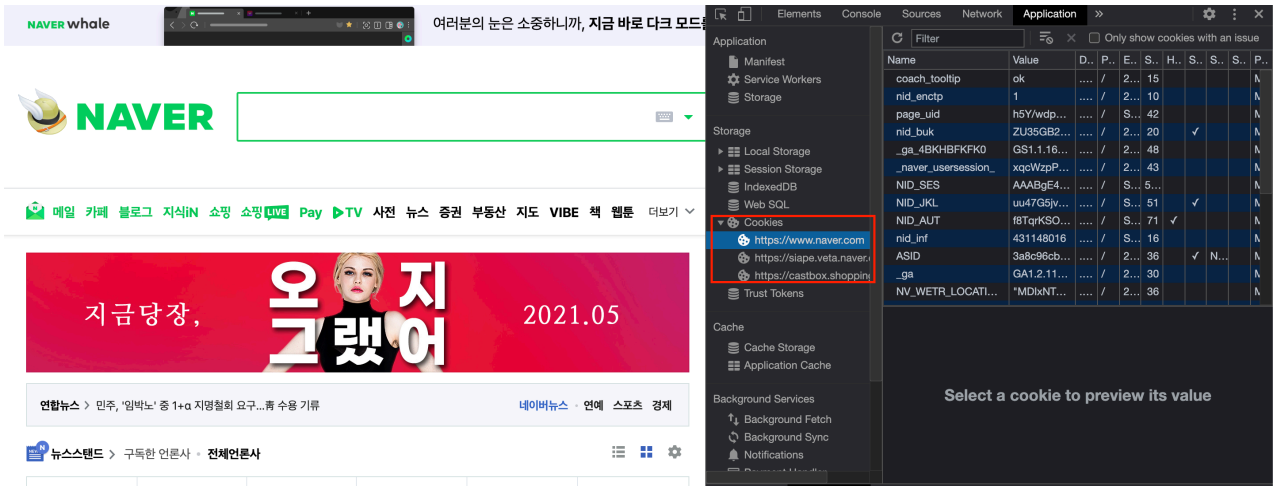


그림 11-3 사용자에게 쿠키 할당

11.6.3 쿠키 상자: 클라이언트 측 상태

쿠키의 기본적인 발상은 브라우저가 서버 관련 정보를 저장하고, 사용자가 해당 서버에 접근할 때 마다 그 정보를 함께 전송하게 하는 것이다.

ex - 구글 크롬 쿠키



11.6.4 사이트마다 각기 다른 쿠키들

브라우저는 쿠키를 생성한 서버에게만 쿠키에 담긴 정보를 전달한다.

11.6.8 쿠키와 세션 추적

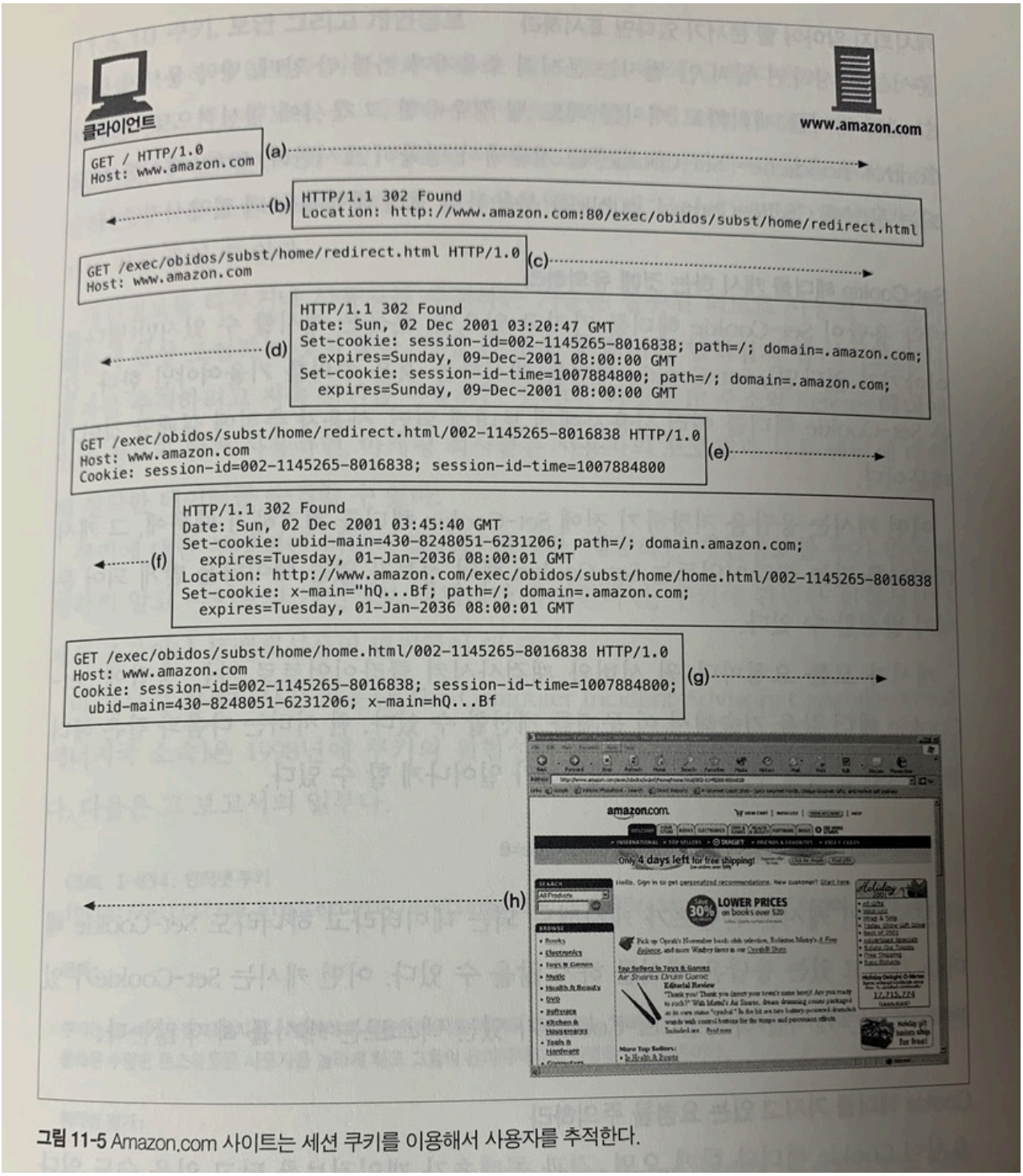


그림 11-5 Amazon.com 사이트는 세션 쿠키를 이용해서 사용자를 추적한다.

그림 11-5는 Amazon.com에 방문하면 일어나는 트랜잭션들의 연속을 보여준다.

- 그림 11-5a : 브라우저가 Amazon.com의 루트 페이지를 처음 요청한다.
- 그림 11-5b : 서버는 클라이언트를 전자상거래 소프트웨어 URL로 리다이렉트 시킨다.
- 그림 11-5c : 클라이언트는 리다이렉트 URL로 요청 보낸다.
- 그림 11-5d : 서버는 응답에 두 개의 세션 쿠키를 기술하고 사용자를 다른 URL로 리다이렉트 시키며, 클라이언트는 다시 이 쿠키들을 첨부하여 요청을 보낸다. 새로운 URL은 자체에 어떤 상태 정보를 가지고 있으므로 뚱뚱한 URL이라고 할 수 있다. 만약 클라이언트가 쿠키를 사용하지 않게 설정되어 있다면, 사용자가 Amazon.com에서 생성한 뚱뚱한 URL을 따라 리다이렉트 하면서도 사이트를 떠나지 않는 한, 기본 식별 절차는 계속 진행된다.
- 그림 11-5e : 클라이언트는 새로운 URL을 요청을 앞서 받은 두 개의 쿠키와 함께 보낸다.
- 그림 11-5f : 서버는 home.html 페이지로 리다이렉트시키고 쿠키 두 개를 더 첨부한다.
- 그림 11-5g : 클라이언트는 home.html 페이지를 가져오고 총 네 개의 쿠키를 전달한다.
- 그림 11-5h : 서버는 콘텐츠를 보낸다.

11.6.9 쿠키와 캐싱

쿠키 트랜잭션과 관련된 문서를 캐싱하는 것은 주의해야 한다. (개인정보 이슈)

11.6.10 쿠키, 보안, 그리고 개인정보

개인정보를 다루거나 사용자를 추적하는 기술은 잘못된 의도로 사용될 수 있기에 항상 조심해야 한다.