HTTP Security

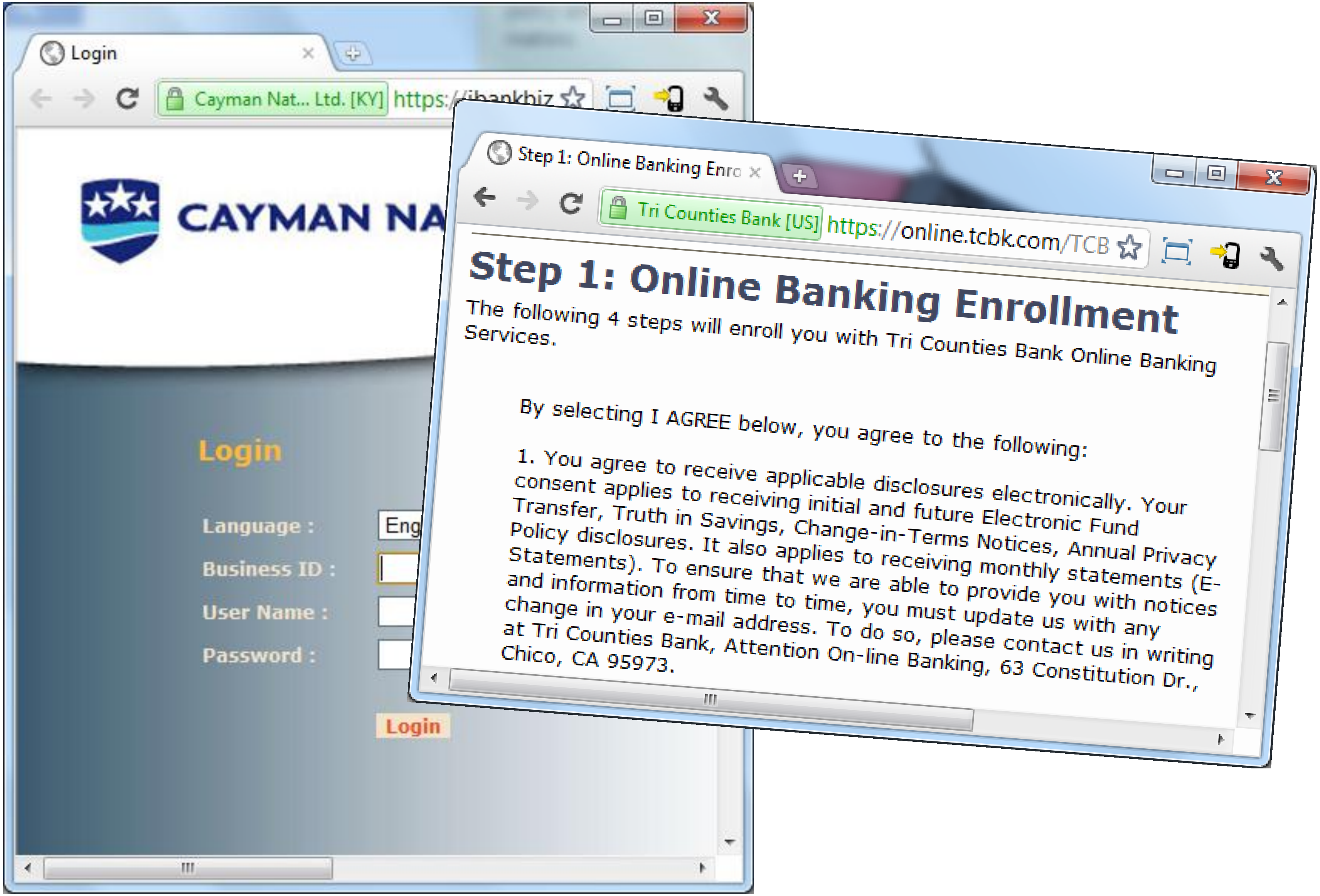
Cookies and Authentication

K. Scott Allen

pluralsight
hardcore developer training

```
GET /maps?q=deep+dish+pizza HTTP/1.1
Host: maps.google.com
Accept-Language: fr-FR
Date: Fri, 9 Jul 2012 23:59:59 GMT
```

```
HTTP/1.1 200 OK
Date: Wed, 25 Jan 2012 22:09:33 GMT
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Content-Length: 68927
```



Step 1: Online Banking Enrollment

The following 4 steps will enroll you with Tri Counties Bank Online Banking Services.

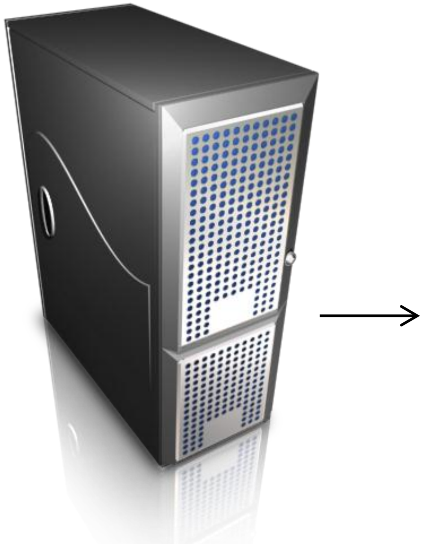
By selecting I AGREE below, you agree to the following:

1. You agree to receive applicable disclosures electronically. Your consent applies to receiving initial and future Electronic Fund Transfer, Truth in Savings, Change-in-Terms Notices, Annual Privacy Policy disclosures. It also applies to receiving monthly statements (E-Statements). To ensure that we are able to provide you with notices and information from time to time, you must update us with any change in your e-mail address. To do so, please contact us in writing at Tri Counties Bank, Attention On-line Banking, 63 Constitution Dr., Chico, CA 95973.

Saving State

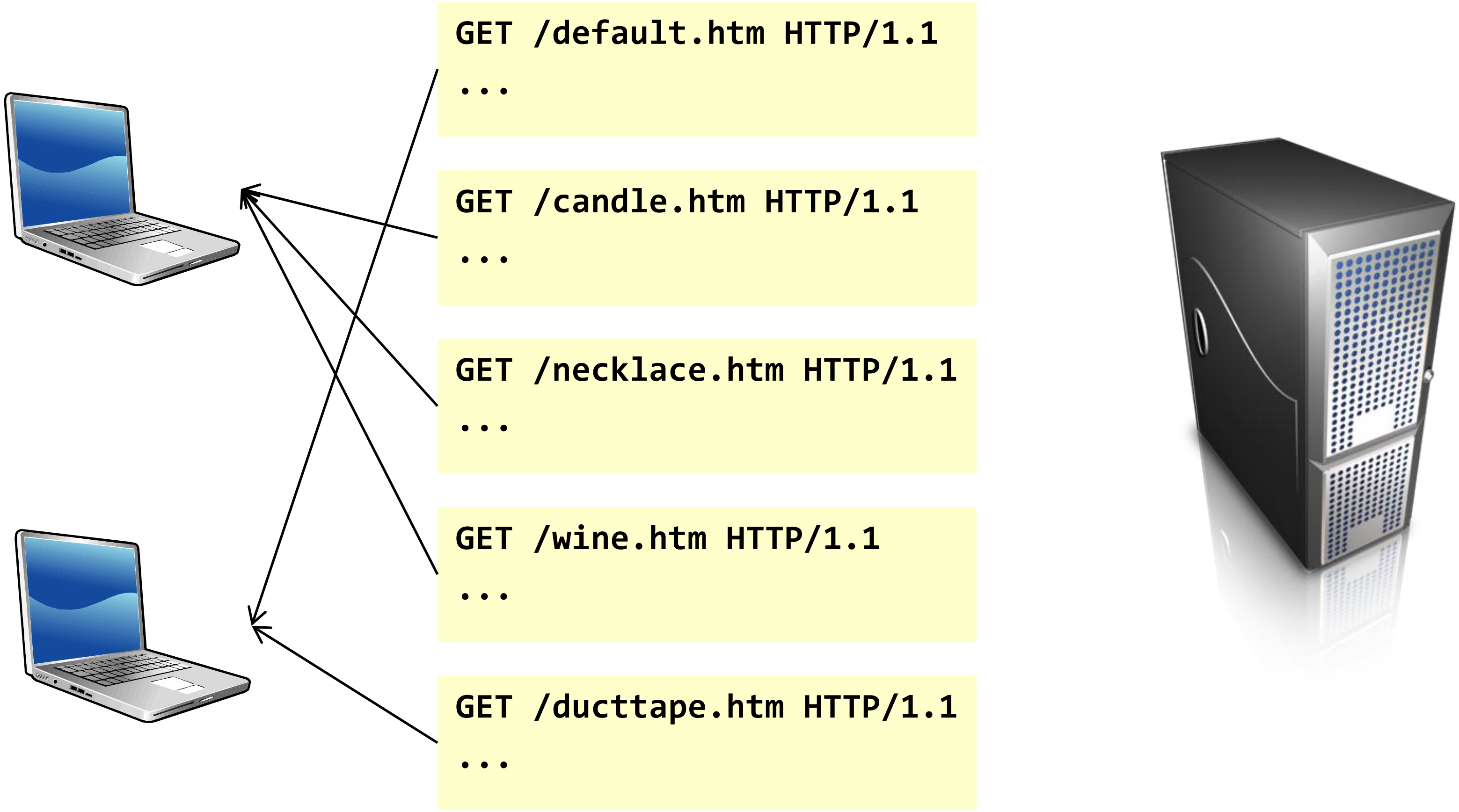
```
<input type="hidden"
       name="__VIEWSTATE"
       id="__VIEWSTATE“
       value="/wEPDwUENTM4MWRkqhRIs/GwciLBJk9VVTvoDb/bsLk=" />
```

```
INSERT INTO Users(email) VALUES
       ('simonfinklesporker@hotmail.com')
```



Session State Store

ID	Data
1	Name=Karthik; CartItems=3
2	Name=Diana; CartItems=5
3	Name=Vishrutha; CartItems=1
...	...



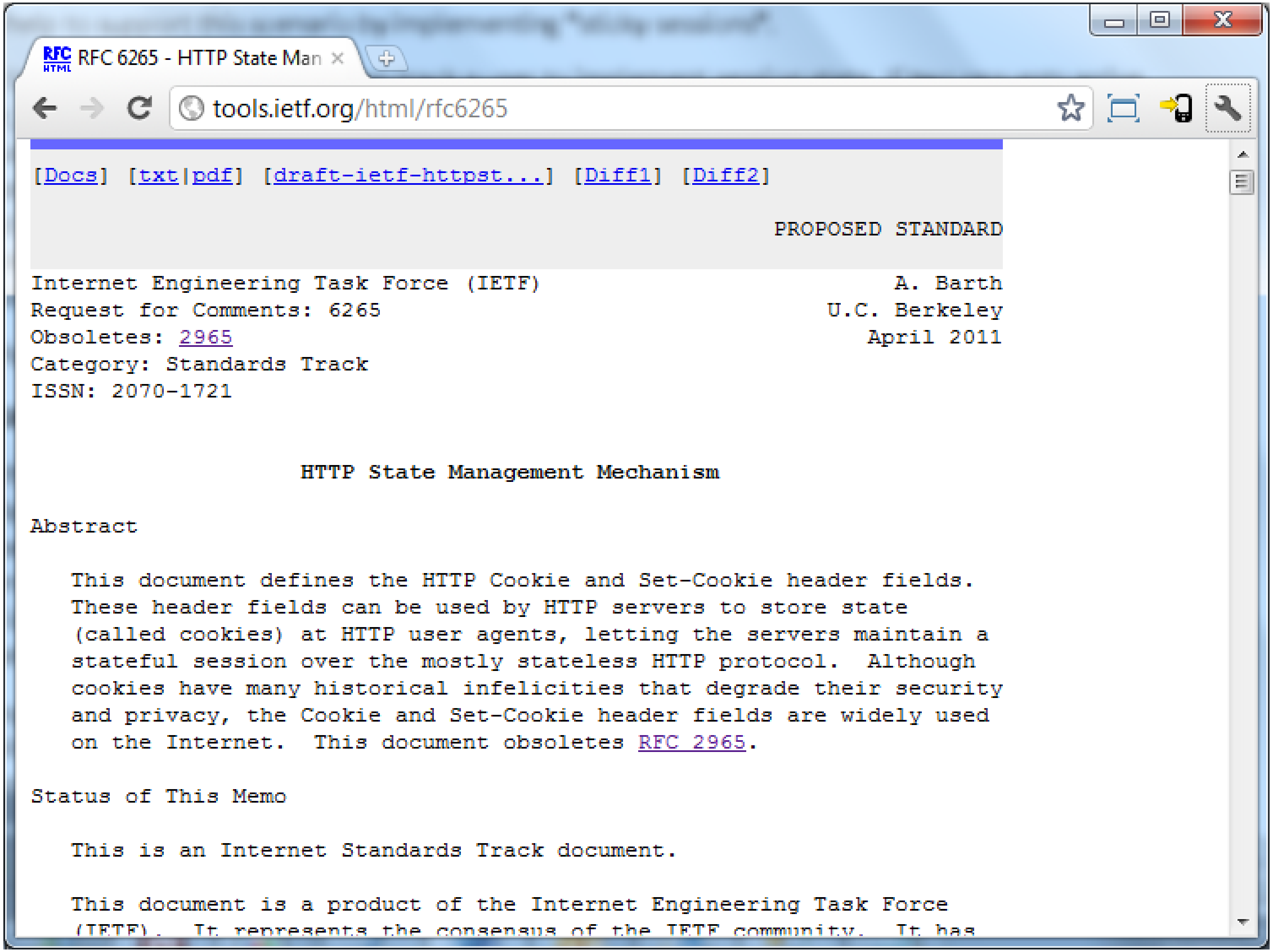
```
GET /default.htm HTTP/1.1
...
```

```
GET /candle.htm HTTP/1.1
...
```

```
GET /necklace.htm HTTP/1.1
...
```

```
GET /wine.htm HTTP/1.1
...
```

```
GET /ducttape.htm HTTP/1.1
...
```



[Docs] [txt|pdf] [draft-ietf-httpst...] [Diff1] [Diff2]

PROPOSED STANDARD

Internet Engineering Task Force (IETF) A. Barth
Request for Comments: 6265 U.C. Berkeley
Obsoletes: 2965 April 2011
Category: Standards Track
ISSN: 2070-1721

HTTP State Management Mechanism

Abstract

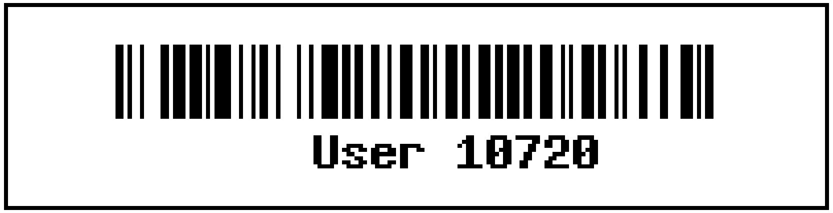
This document defines the HTTP Cookie and Set-Cookie header fields. These header fields can be used by HTTP servers to store state (called cookies) at HTTP user agents, letting the servers maintain a stateful session over the mostly stateless HTTP protocol. Although cookies have many historical infelicities that degrade their security and privacy, the Cookie and Set-Cookie header fields are widely used on the Internet. This document obsoletes RFC 2965.

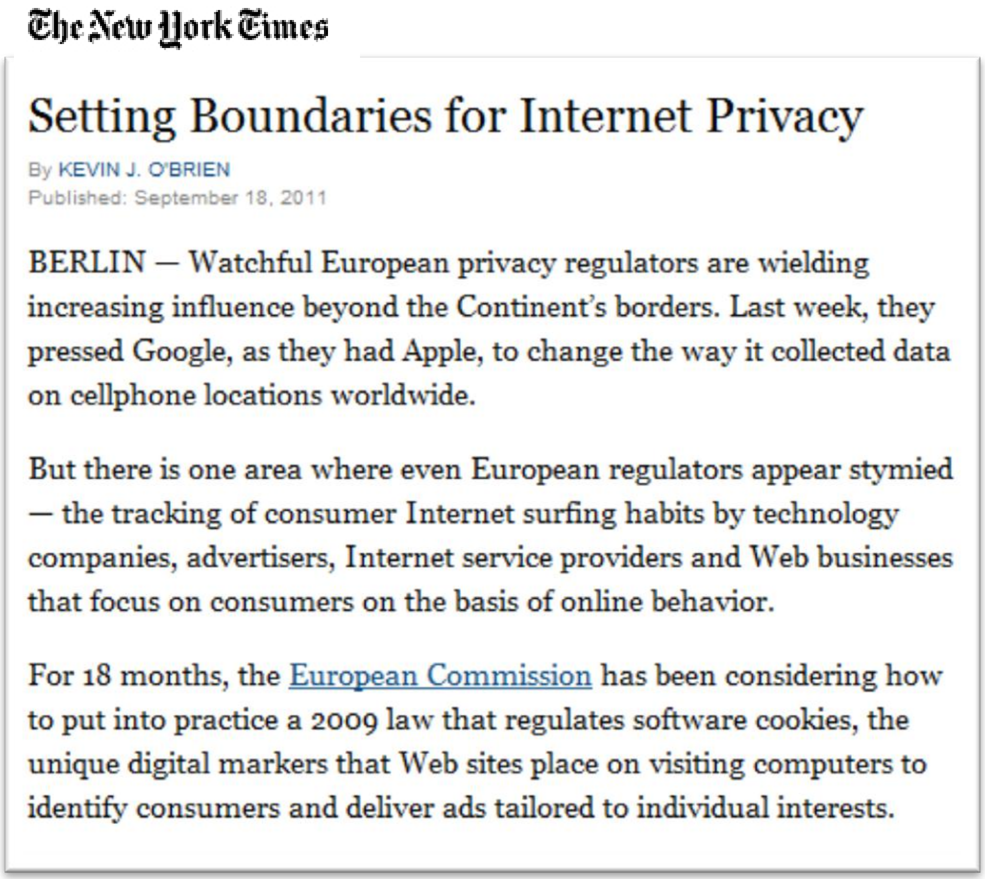
Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has

!=

== 
User 10720



The New York Times

Setting Boundaries for Internet Privacy

By KEVIN J. O'BRIEN
Published: September 18, 2011

BERLIN — Watchful European privacy regulators are wielding increasing influence beyond the Continent's borders. Last week, they pressed Google, as they had Apple, to change the way it collected data on cellphone locations worldwide.

But there is one area where even European regulators appear stymied — the tracking of consumer Internet surfing habits by technology companies, advertisers, Internet service providers and Web businesses that focus on consumers on the basis of online behavior.

For 18 months, the European Commission has been considering how to put into practice a 2009 law that regulates software cookies, the unique digital markers that Web sites place on visiting computers to identify consumers and deliver ads tailored to individual interests.

```
GET /search?q=lyrics HTTP/1.1
Host: searchengine.com
...
```

```
HTTP/1.1 200 OK

Set-Cookie: fname=Scott&lname=Allen;
            domain=.searchengine.com;
            path=/
...
```

```
GET /search?q=lyrics HTTP/1.1
Host: searchengine.com
...
```

```
HTTP/1.1 200 OK

Set-Cookie: GUID=00a48b7f6a4946a8ad...;
            domain=.searchengine.com;
            path=/
...
```

```
GET /search?q=lyrics HTTP/1.1
Host: searchengine.com
Cookie: GUID=00a48b7f6a4946a8ad...;
...
```

```
GET /search?q=lyrics HTTP/1.1
Host: searchengine.com
...
```

```
HTTP/1.1 200 OK

Set-Cookie: GUID=00a48b7f6a4946a8ad...;
            domain=.searchengine.com;
            path=/
...
```

Session Cookie

```
GET /search?q=lyrics HTTP/1.1
Host: searchengine.com
...
```

```
HTTP/1.1 200 OK

Set-Cookie: GUID=00a48b7f6a4946a8ad…;
   domain=.searchengine.com;
   path=/
   expires=Monday, 09-July-2012 21:12:00 GMT
...
```

Persistent Cookie

Basic Authentication

```
GET /account HTTP/1.1
Host: giantbank.com
...
```

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm=“Giant Bank"
```

```
GET /account HTTP/1.1
Host: giantbank.com
Authorization: Basic Z2VudDptaXNzaW5n
```

Digest Authentication

```
GET /account HTTP/1.1
Host: giantbank.com
...
```

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm=“Giant Bank",
     qop="auth,auth-int",
     nonce="dcd98b710…00bfb0c093",
     opaque="5ccc069….e9517f40e41"
```

Windows Authentication

```
GET /account HTTP/1.1
Host: giantbank.com
...
```

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Negotiate
```

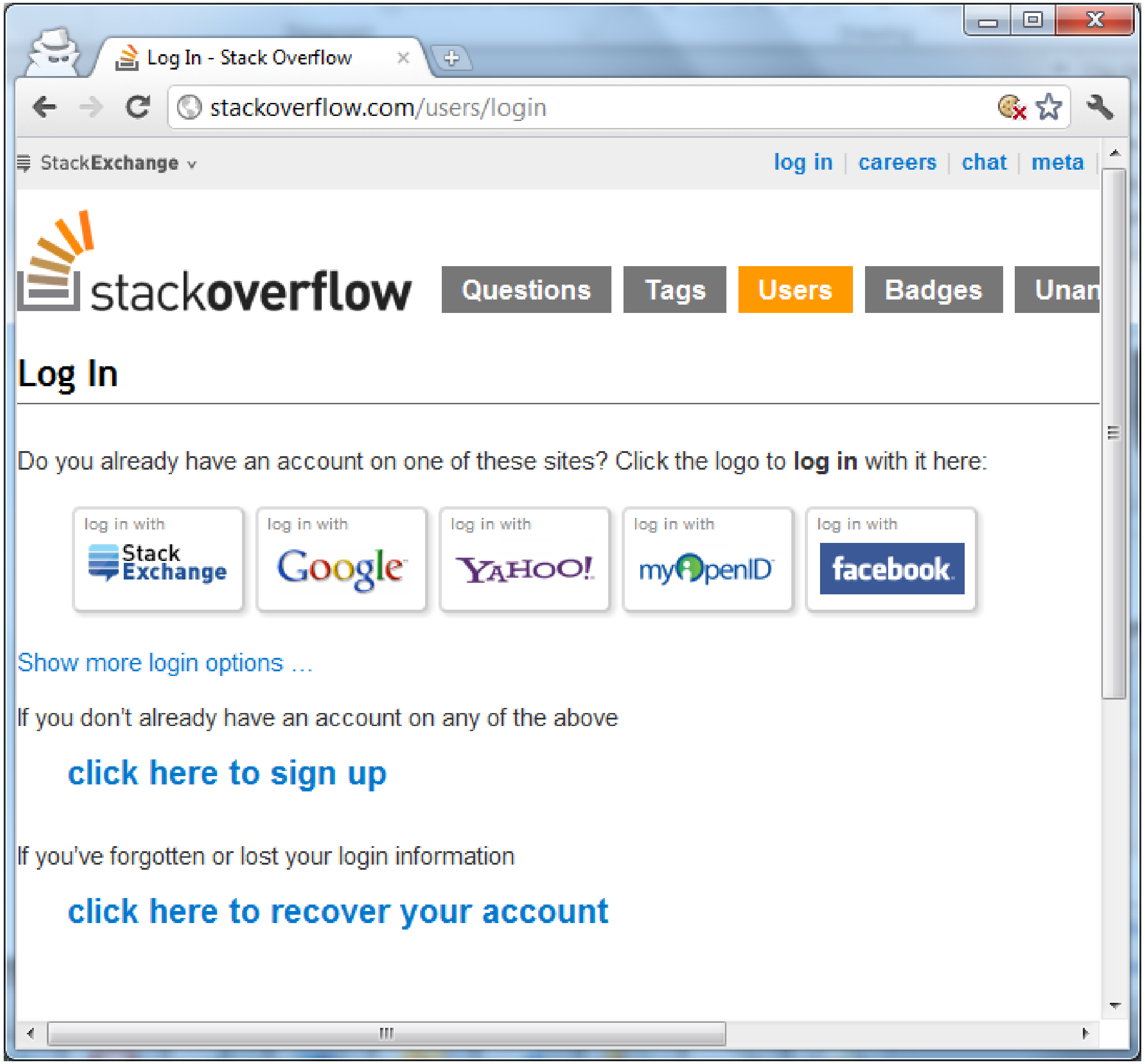
Forms Authentication

```
GET /account HTTP/1.1
Host: giantbank.com
...
```

```
HTTP/1.1 302 Found
Location: /login?ReturnUrl=/account
```

```
<form method="post">

  <input type="text" name="username" />

  <input type="password" name="password" />

  <input type="submit" value="Login" />

</form>
```

Open ID



Log In

Do you already have an account on one of these sites? Click the logo to **log in** with it here:

Show more login options ...

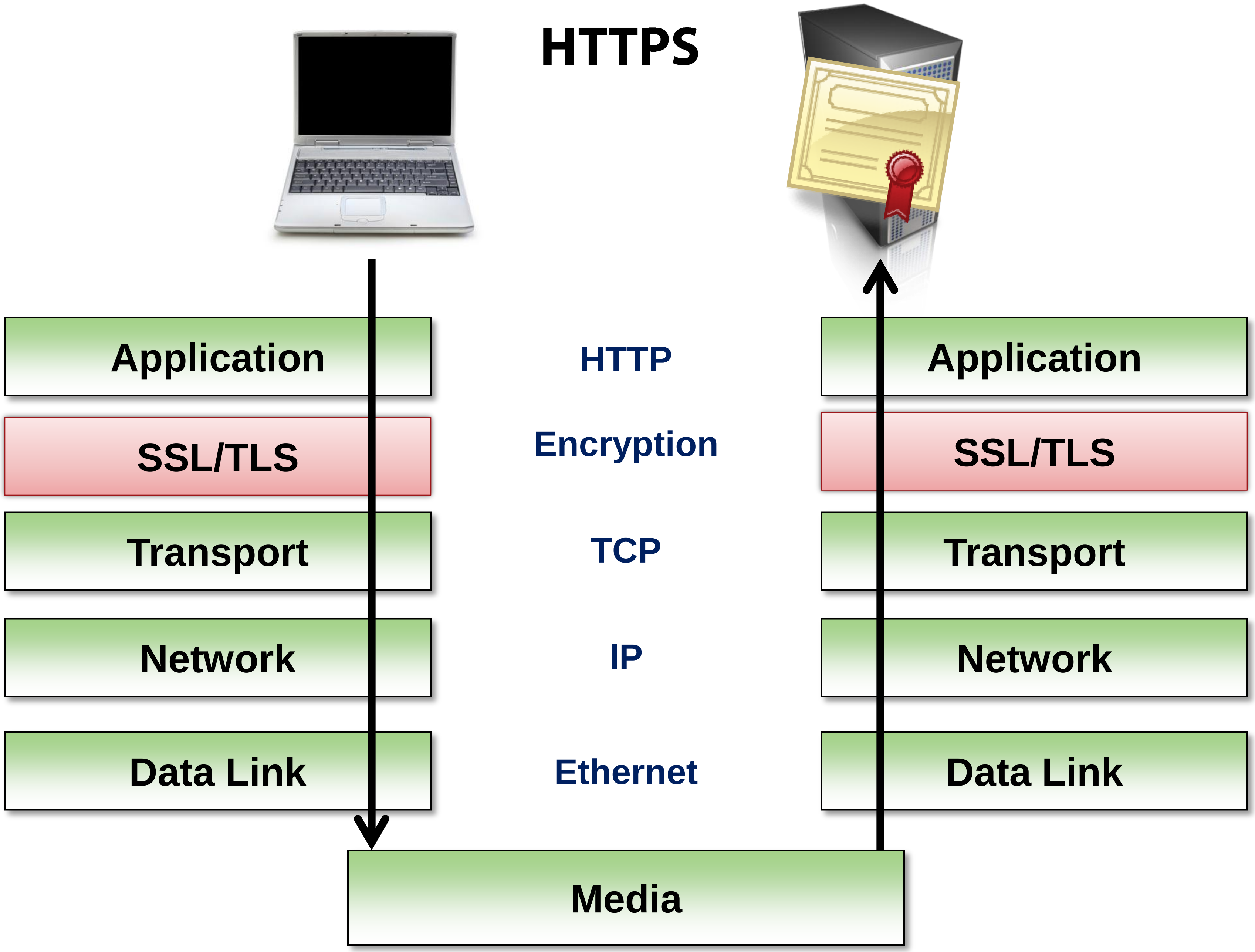
If you don't already have an account on any of the above

click here to sign up

If you've forgotten or lost your login information

click here to recover your account

HTTPS



Application

SSL/TLS

Transport

Network

Data Link

HTTP

Encryption

TCP

IP

Ethernet

Application

SSL/TLS

Transport

Network

Data Link

Media

```
GET /maps?q=deep+dish+pizza HTTP/1.1
Host: maps.google.com
Accept-Language: fr-FR
Date: Fri, 9 Jul 2012 23:59:59 GMT
```

```
HTTP/1.1 200 OK
Date: Wed, 25 Jan 2012 22:09:33 GMT
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Content-Length: 68927
```