



Computer Engineering II

Solution to Exercise Sheet 3

1 Quiz Questions

- a) The server sets a cookie with a session ID associated with the server side information about the user, i.e., the session data. Basic Auth, i.e., including the username and password in the URL, is not commonly used since it shows a popup that cannot be integrated into the look and feel of the webpage. Furthermore, copy-pasting a URL somewhere may result in the credentials being leaked.
- b) It may be ambiguous whether the client is using encrypted or unencrypted requests. The age of the protocol is not the cause since it is trivial to introduce an upgrade command which bootstraps the encrypted communication, e.g., STARTTLS for SMTP upgrades a plaintext connection after the initial handshake to use Transport Layer Security (TLS).
- c) No. Nowadays most users deliver outgoing mails to their provider's outgoing mailserver which then takes care of forwarding the mail to the destination. This adds authentication since the outgoing mailserver can now certify that the mail was sent by a legitimate user and it may attempt delivery multiple times should the destination mailserver not be reachable.
- d) Yes, the server may have a cached response to the resolution request and respond directly without having to perform the entire resolution. Should the server not have a cached response the overhead of using an intermediate server is minimal since the ISP is on the communication path to the authoritative nameserver anyway.
- e) There are at least 3 connections being opened:
 - The first connection is opened to retrieve `http://google.ch/`. This page redirects (status code 301) to `http://www.google.com/` which may not be served by the same server.
 - The second connection is opened to retrieve `http://www.google.ch/` (port 80) redirects to `https://www.google.com/` (port 443) which is not on the same port.
 - The third connection actually retrieves the content of the webpage, but additional connection may be opened to retrieve referenced resources in parallel.

2 Send me a comment

- a) Depending on the website you visited there will be an initial connection to retrieve the HTML page followed by a cascade of resources referenced in the HTML page. Since each of the resources may themselves reference some other resources it is not uncommon to see multiple waves of parallel requests.

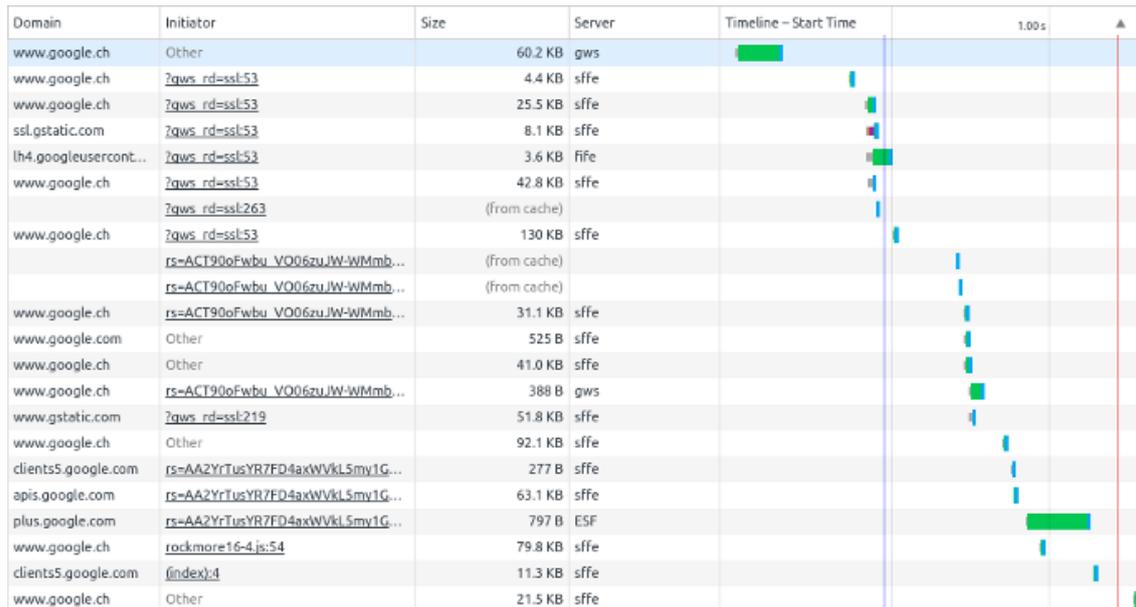


Figure 1: The waterfall of requests when opening a simple webpage.

b) The following is an example HTTP request and response:

```

1 # telnet pc-10367.ethz.ch 80
2 Trying 82.130.102.226...
3 Connected to pc-10367.ethz.ch.
4 GET / HTTP/1.1
5 Host: pc-10367.ethz.ch
6
7 HTTP/1.1 200 OK
8 Transfer-Encoding: chunked
9 Date: Wed, 09 Mar 2016 15:15:54 GMT
10 Content-Type: text/html
11 Server: TwistedWeb/15.5.0
12
13 249
14
15 <html>
16   <head>
17     <title>Disco Comments</title>
18     <link href="http://getbootstrap.com/dist/css/bootstrap.min.css" rel
19         ="stylesheet" />
20   </head>
21   <body lang="en">
22     <header class="navbar navbar-static-top">
23       <div class=container>
24         <div class=navbar-header>
25           <div class=navbar-brand>Disco Comments</div>
26         </div>
27       </header>
28       <div class=container>
29         <div class="col-md-12">

```

```

30         <dl>
31             <dt id="mid-0">Disco</dt>
32             <dd>Welcome to the Disco Comment page</dd>
33         </dl>
34     </div>
35 </div>
36 </body>
37 </html>
38 0
39
40 Connection closed.

```

The request (lines 4-6) specifies that HTTP/1.1 is to be used, hence the connection will remain open for a few seconds before the server closes it due to a timeout. The response header (lines 7-12) returns some information about the server and metadata about the response. Notice that the Transfer-Encoding is set to **chunked** which means that the server returns the response in multiple chunks, each prefixed with the number of bytes on a separate line. In this case we have two chunks, one of 249 bytes starting at line 13 and another chunk of 0 bytes, indicating the end of the response, starting at line 38.

- c) As mentioned we need to construct a PUT request to resource /. The following sends the message `hello world` to the server.

```

1 # telnet pc-10367.ethz.ch 80
2 Trying 82.130.102.226...
3 Connected to pc-10367.ethz.ch.
4 PUT / HTTP/1.1
5 Host: pc-10367.ethz.ch
6 Content-Length: 11
7
8 hello world
9 HTTP/1.1 201 Created
10 Transfer-Encoding: chunked
11 Date: Wed, 09 Mar 2016 15:30:37 GMT
12 Content-Type: text/html
13 Server: TwistedWeb/15.5.0
14
15 18
16 Comment added with ID 3
17
18 0

```

The request now includes a **Content-Length** option which tells the server how many bytes to read. The request spans lines 4-8, including the payload on line 8.

3 Send me a mail

- a) Simply sending a mail to `somebody@pc-10367.ethz.ch` will not work because when searching for the responsible mailserver for the domain `pc-10367.ethz.ch` using DNS no MX record is returned hence the sender is unable to find the responsible server.
- b) The following is a valid SMTP session:

```

1 telnet pc-10367.ethz.ch 25
2 Trying 82.130.102.226...

```

```
3 Connected to pc-10367.ethz.ch.
4 220 cd652f72069f NO UCE NO UBE NO RELAY PROBES ESMTP
5 EHLO pc-5305.ethz.ch
6 250 cd652f72069f Hello 82.130.102.226, nice to meet you
7 MAIL FROM: someone@student.ethz.ch
8 250 Sender address accepted
9 RCPT TO: recipient@pc-10367.ethz.ch
10 250 Recipient address accepted
11 DATA
12 354 Continue
13 This is a test message
14 that spans multiple lines
15 .
16 250 Delivery in progress
17 QUIT
18 221 See you later
19 Connection closed by foreign host.
```

This is an interactive session with the SMTP server, lines starting with a number are sent by the server. The client needs to identify itself using the `EHLO` command on line 5. On lines 7 and 9 we specify sender and recipient, notice that the sender needs to be specified before the recipient. The `DATA` command is then used to start the content transfer, which is terminated on line 15 with a single dot on a line.