Networking and System Security
Assignment 1

David van Erkelens (10264019)
Department of Computer Science
University of Amsterdam

November 1, 2012

1 Task 1

1. The IP-address of *ss64.com* is 216.92.29.160.
   The IP-adress of the sending computer is 145.18.214.201.

2. There are 8 GET-requests to *ss64.com*
   The filter used to find this result is `http.request && ip.addr == 216.92.29.160`

3. - Ethernet II
   - Internet Protocol Version 4
   - Transmission Control Protocol
   - Hypertext Transfer Protocol

4. There are 8 HTTP OK responses.

2 Task 2

5. 0.434445 seconds.
   Retreived by showing only the HTTP traffic to *ss64.com* and setting the view to `Time Since Last Displayed Package`. The used filter is `ip.addr == 216.92.29.160 && http`

6. Yes, the following images:

   - /images/ss64.gif
   - /images/bash-l.gif
   - /images/syntax-r.gif
   - /images/top-4.gif
   - /images/roll-left.png
   - /images/roll-right.png

7. The requests are included as first-request.txt and first-ok.txt. They are printed by right clicking the package and selecting print, then selecting the print to file option.

3 Task 3

8. There are 77 IPv4 packages send between *ss64.com* and the user, with a total of 38558 bytes. A notable fact is that the number of bytes send to the host is much less than the number of received bytes. This can be explained by that fact that requests are send, and files are returned.

9. The used filters and the colors in which they are displayed in the graph:

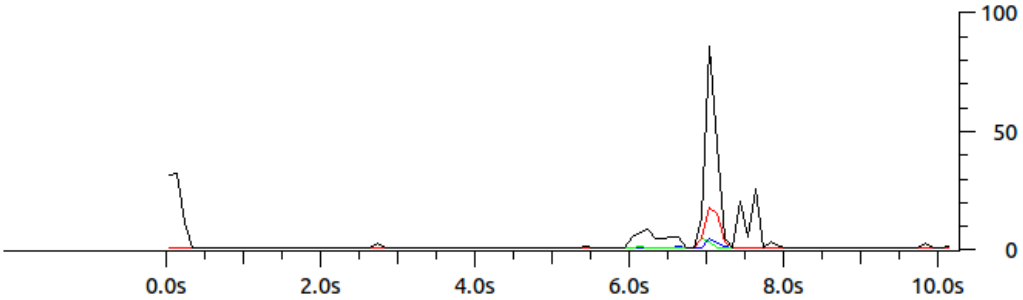
   (a) `No filter added`

   (b) `ip.addr == 216.92.29.160 && tcp`

   (c) `ip.addr == 216.92.29.160 && http.request`

   (d) `ip.addr == 216.92.29.160 && http.response`

   Resulting in the following graph:



   When looking at the times shown at questions 2 and 4 and the times shown in the graph, it can be noticed that the graph is consistent with the earlier answers.

10. There are two cleartext passwords in the packages:

    - wrong!
    - network

    They are found by using the `ip.addr = 128.119.245.12 && http.request` filter, and looking at the Authorization part of the package. When changing the filter to `ip.addr = 128.119.245.12 && http`, it can be noted that "network" is the correct password, since this returns code 200 (OK) instead of code 401 (Authorization Required).