Lab Answers

1. How many packets does the capture contain?
    a. 2195
2. Find and record all the DNS Domain requests and all the IP Addresses returned
    a. market.android.com - 74.125.137.118
    b. xtra2.gpsonextra.net - 72.51.26.219
    c. fineandroid.com - 174.138.168.211
    d. diaobaolediaobaole3.googlecode.com - 74.125.137.82
    e. north-america.pool.ntp.org - 173.255.193.172, 209.114.111.1, 169.229.70.95
    f. www.gstatic.com - 173.194.37.79
    g. clients1.google.com - 173.194.37.37, 173.194.37.38, 173.194.37.39, 173.194.37.40, 173.194.37.41, 173.194.37.46, 173.194.37.32, 173.194.37.33, 173.194.37.34, 173.194.37.35, 173.194.37.36
    h. android.clients.google.com - 74.125.45.113, 74.125.45.138, 74.125.45.139, 74.125.45.100, 74.125.45.101, 74.125.45.102
    i. twitter.com - 199.59.149.230, 199.59.150.7, 199.59.150.39
    j. www.homerchess.com - 82.165.80.40
    k. 113.45.125.74.in-addr.arpa - Domain name: yx-in-f113.1e100.net
3. Record the full URI requests of all the GET requests
    a. http://fineandroid.com/InstallApk/php4sam.php
    b. http://www.google.com/extern_js/f/CgJlbhICdXMrMEU4ACwrMFo4ACwrMA44ACwrMBc4ACwrMDw4ACwrMIcCOAAsKzBROAAsKzAKOACaAgNtb2IsKzCAATgALCswmAE4ACwrMBY4ACwrMBk4ACwrMEE4ACwrME04ACwrME44ACwrMFM4ACwrMFQ4ACwrMGk4ACwrMGs4ACwrMHY4ACwrMHs4ACwrMIQBOAAsKzCMATgALCswkAE4ACwrMJIBOAAsKzCjATgALCswqAE4ACwrMKwBOAAsKzCvATgALCswswE4ACwrML4BOAAsKzDVATgALCsw2AE4ACwrMP0BOAAsKzD_ATgALCswdzgALCswhgE4ACwrMIsBOAAsKzCtATgALCswwAE4ACwrMMQBOAAsKzCkATgALCswGDgALCswJjgALIACa5ACeQ/1nxsDrkZwFg.js?sky=mrdr
    c. http://www.homerchess.com/favicon.ico
    d. http://diaobaolediaobaole3.googlecode.com/files/youni.apk
    e. http://clients1.google.com/generate_204
    f. http://www.google.com/images/nav_logo107.png
    g. http://www.google.com/images/nycli1.gif
    h. http://www.fineandroid.com/inputex/index.php?s=/Interface/keinter/a1/A1000012388937/a2/3100120000006441/a3/ERIS/index/xian1234
    i. http://www.google.com/m?client=ms-android-verizon-us&source=android-home
    j. http://www.homerchess.com/sd-booster/SD-Booster-v1-eng.html
    k. http://www.google.com/webhp?client=ms-android-verizon-us&source=android-home&sky=mrdr&mnfst=1
    l. http://xtra2.gpsonextra.net/xtra.bin
4. What kind of packet is packet number 1400
    a. NTP - Network Time Protocol - Client

5. What is the Reference Time Stamp of packet number 1404
    a. May  8, 2012 09:19:38.163578000
6. Export "app_logo.png" and record the MD5 of the file
    a. 43dd661754ba7a3b75f34999b3f54181
7. Export "SD-Booster-v 1-eng.html" and the record the email and twitter contacts in the document
    a. Email: <a href="mailto:daniel.mehrmann@gmx.de">daniel.mehrmann@gmx.de</a><br>
    b. Twitter: <a href="http://twitter.com/akusari">http://twitter.com/akusari</a><br>