1. FTP

2. FTP is insecure because it does not use encryption and everything is in plain text (usernames and passwords for authentication)

3. SFTP

4. 192.168.1.220 (destination of first TCP request)

5. Username: stefani
   Password: BadRomance1

6. 6 files

7. I was able to determine the type of each file but running the 'file' command

8. 76,409 packets

9. 1 username-password pair
   Username: wbgapp31216
   Password: Q827wO6656!nW99_a1

10. Protocol: HTTP
    Server IP: 176.58.103.138 (???)
    Domain Name: utils.wbg-server.se
    Port Number: 80

11. The only username-password pair found was legitimate

12. # TShark hosts output
    #
    # Host data gathered from set2.pcap

    52.94.224.25 mads.amazon.com
    72.21.91.113 cs84.wac.edgecastcdn.net
    23.45.86.46 e4478.a.akamaiedge.net
    31.13.77.49 mmx-ds.cdn.whatsapp.net
    23.203.180.198 e6858.dsce9.akamaiedge.net
    169.46.12.93 api.south.kontagent.net
    169.46.12.69 api.south.kontagent.net

87.240.165.81 api.vk.com
115.231.99.203 ps.cname2.igexin.com
17.178.96.59 apple.com
104.27.182.94 warl0ck.gam3z.com
216.115.100.123 fd-geoycpi-uno.gycpi.b.yahoodns.net
17.139.246.6 mt-ingestion-service-pv.itunes-apple.com.akadns.net
23.253.220.65 schemaverse.marcneuwirth.com
172.217.4.129 googlehosted.l.googleusercontent.com
172.217.5.202 googleapis.l.google.com
172.217.5.74 googleapis.l.google.com
17.253.23.207 cdn-icloud-content.g.aaplimg.com
23.203.233.109 e2546.dsce4.akamaiedge.net
216.58.193.202 googleapis.l.google.com
169.46.12.68 api.south.kontagent.net
169.46.12.84 api.south.kontagent.net
17.172.224.47 apple.com
104.27.183.94 warl0ck.gam3z.com
151.101.193.181 prod.taboola.map.fastly.net
17.139.246.5 mt-ingestion-service-pv.itunes-apple.com.akadns.net
151.101.65.181 prod.taboola.map.fastly.net
17.173.66.102 p51-buy.itunes-apple.com.akadns.net
34.201.64.150 lc80.dsr.livefyre.com
192.31.80.30 d.gtld-servers.NET
192.33.14.30 b.gtld-servers.NET
17.56.160.246 api.smoot-apple.com.akadns.net
17.253.23.205 cdn-icloud-content.g.aaplimg.com
192.12.94.30 e.gtld-servers.NET
95.213.11.139 api.vk.com
169.46.12.66 api.south.kontagent.net
169.46.12.74 api.south.kontagent.net
208.71.44.31 fd-geoycpi-uno.gycpi.b.yahoodns.net
172.217.4.142 clients.l.google.com
192.26.92.30 c.gtld-servers.NET
104.68.97.2 e12930.ksd.akamaiedge.net
107.23.77.203 gregord-elb-298228113.us-east-1.elb.amazonaws.com
192.5.6.30 a.gtld-servers.NET
208.71.44.30 fd-geoycpi-uno.gycpi.b.yahoodns.net
64.4.54.254 cy2.vortex.data.microsoft.com.akadns.net
104.244.46.231 wildcard.twimg.com
104.244.46.39 wildcard.twimg.com

104.244.46.71 wildcard.twimg.com
17.125.252.5 sp11p03sa.guzzoni-apple.com.akadns.net
169.46.12.72 api.south.kontagent.net
169.46.12.88 api.south.kontagent.net
216.58.216.46 connectivitycheck.android.com
17.142.160.59 apple.com
151.101.129.181 prod.taboola.map.fastly.net
54.239.17.86 completion.amazon.com
23.215.130.192 a1089.d.akamai.net
23.215.130.184 a1089.d.akamai.net
115.233.212.147 ps.cname2.igexin.com
218.205.81.155 ps.cname2.igexin.com
151.101.1.181 prod.taboola.map.fastly.net
169.46.12.79 api.south.kontagent.net
72.21.206.140 s.amazon-adsystem.com
74.125.28.188 mobile-gtalk.l.google.com
172.217.4.131 gstaticadssl.l.google.com
52.45.146.29 gregord-elb-298228113.us-east-1.elb.amazonaws.com
104.41.208.54 production-roundrobin.skype-registar.akadns.net
23.5.251.27 e8218.dscb1.akamaiedge.net
184.24.107.198 e1879.e7.akamaiedge.net
172.217.11.170 googleapis.l.google.com
172.217.11.74 googleapis.l.google.com
172.217.11.66 pagead46.l.doubleclick.net
169.46.12.70 api.south.kontagent.net
165.227.0.37 vtfbctf.com
23.203.204.8 e673.e9.akamaiedge.net
216.58.216.4 www.google.com
216.115.100.124 fd-geoycpi-uno.gycpi.b.yahoodns.net
17.139.246.7 mt-ingestion-service-pv.itunes-apple.com.akadns.net

13. 3 username-password pairs
    Username: brodgers
    Password: TheyPlayedWithGreatCharacter

    Username: dmoyes
    Password: IAmAFootballGenius

    Username: aoursler
    Password: Id10tExpert

14. *each corresponds to the respective username-password pair above
    Protocol: HTTP
    Server IP: 130.64.23.35
    Domain Name: www.eecs.tufts.edu
    Port Number: 80

    Protocol: HTTP
    Server IP: 130.64.23.35
    Domain Name: www.eecs.tufts.edu
    Port Number: 80

    Protocol: HTTP
    Server IP: 130.64.23.35
    Domain Name: www.eecs.tufts.edu
    Port Number: 80

15. None of the username-password pairs that I found were legitimate

16. Username-password pairs should be encrypted before being sent to the server (use HTTPS)