2. Protocol Analysis

Client **Server**

DNS Request; Query: <synprint.com: type A, class IN> →

← DNS Response; Answer: <192.241.168.54>

HTTP <GET> Request; </ece303/project1/login.html> →

← HTTP <200> Response; Content-Type: <text/html>

HTTP <GET> Request; </ece303/project1/css/login.css> →

← HTTP <200> Response; Content-Type: <text/css>

HTTP <GET> Request; </ece303/project1/js/login.js> →

← HTTP <200> Response; Content-Type: <application/javascript>

HTTP <GET> Request; </favicon.ico> →

← HTTP <200> Response; Content-Type: <image/vnd.microsoft.icon>

HTTP <POST> Request; </ece303/project1/main.php> →

← HTTP <200> Response; Content-Type: <text/html>

---

3. Browser Cookies

Secret=56e41af1f75726cf992d414987602fca

4. Packet Capture Automation

```
import pyshark
import os

def get_org_name(ip):
    command = "whois " + pkt.ip.dst
    process = os.popen(command)
    result = str(process.read())
    marker1 = result.find('Organization:') + 16
    if marker1 > 16:
        marker2 = result.find('RegDate:')
        return result[marker1:marker2]
    else:
        return "unknown" + "\n"


in_name = input("Enter the File and Pathname of the input file: ")
fd1 = open(in_name, "r")

pcap = pyshark.FileCapture(fd1, display_filter='tls.handshake.type==1')
mylist = []

out_name = input("Enter the file name of the output file: ")
fd2 = open(out_name, "w")

for pkt in pcap:
    ip_src = str(pkt.ip.src)
    ip_dst = str(pkt.ip.dst)
    output = ip_src + "\t" +ip_dst + "\t" + pkt.tls.handshake_extensions_server_name +
"\t" + get_org_name(pkt.ip.dst)
    mylist.append(output)

mylist = list(dict.fromkeys(mylist))
print(*mylist, file=fd2)
fd1.close()
fd2.close()
```

192.168.1.7	151.101.209.67	www.cnn.com	Fastly (SKYCA-3)
192.168.1.7	23.192.24.215	cdn.cnn.com	Akamai Technologies, Inc. (AKAMAI)
192.168.1.7	172.217.3.98	www.googletagservices.com	Google LLC (GOGL)
192.168.1.7	99.84.119.138	c.amazon-adsystem.com	Amazon.com, Inc. (AMAZO-4)
192.168.1.7	74.119.119.131	static.criteo.net	Criteo Corp. (CRITE-6)
192.168.1.7	199.232.37.67	www.i.cdn.cnn.com	Fastly (SKYCA-3)
192.168.1.7	152.195.33.69	cdn.cookielaw.org	ANS Communications, Inc (ANS)
192.168.1.7	3.234.31.129	agility.cnn.com	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	192.96.162.40	amplify.outbrain.com	Optimum WiFi (CHL-54)
192.168.1.7	184.87.69.184	cdn3.optimizely.com	Akamai Technologies, Inc. (AKAMAI)
192.168.1.7	172.217.12.194	securepubads.g.doubleclick.net	Google LLC (GOGL)
192.168.1.7	104.16.85.20	cdn.jsdelivr.net	Cloudflare, Inc. (CLOUD14)
192.168.1.7	94.237.48.90	cnn.sdk.beemray.com	unknown
192.168.1.7	184.87.66.86	a125375509.cdn.optimizely.com	Akamai Technologies, Inc. (AKAMAI)
192.168.1.7	34.192.199.170	www.ugdturner.com	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	104.18.252.222	widgets.tree.com	Cloudflare, Inc. (CLOUD14)
192.168.1.7	99.84.41.29	healthguides.cnn.com	Amazon.com, Inc. (AMAZO-4)
192.168.1.7	34.226.15.163	dpm.demdex.net	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	8.43.72.41	fastlane.rubiconproject.com	Level 3 Parent, LLC (LPL-141)
192.168.1.7	52.46.130.13	s.amazon-adsystem.com	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	68.67.179.122	ib.adnxs.com	AppNexus, Inc (APPNE)
192.168.1.7	172.217.12.194	adservice.google.com	Google LLC (GOGL)
192.168.1.7	209.197.3.15	maxcdn.bootstrapcdn.com	Highwinds Network Group, Inc. (HNG-3)
192.168.1.7	3.221.145.39	logx.optimizely.com	Amazon Data Services NoVa (ADSN-1)
192.168.1.7	52.72.119.61	turner2.demdex.net	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	104.17.65.4	cdnjs.cloudflare.com	Cloudflare, Inc. (CLOUD14)
192.168.1.7	3.208.14.195	smetrics.cnn.com	Amazon Data Services NoVa (ADSN-1)
192.168.1.7	99.84.41.30	cdn.adsafeprotected.com	Amazon.com, Inc. (AMAZO-4)
192.168.1.7	192.96.161.160	js-sec.indexww.com	Optimum WiFi (CHL-54)
192.168.1.7	52.86.222.128	ads.yieldmo.com	Amazon Technologies Inc. (AT-88-Z)

192.168.1.7 23.192.31.127 secure-assets.rubiconproject.com Akamai Technologies, Inc. (AKAMAI)
192.168.1.7 151.101.208.175 cdn.krxd.net Fastly (SKYCA-3)
192.168.1.7 99.84.41.135 static.chartbeat.com Amazon.com, Inc. (AMAZO-4)
192.168.1.7 204.79.197.200 bat.bing.com Microsoft Corporation (MSFT)
192.168.1.7 18.235.4.134 pixel.adsafeprotected.com Amazon Technologies Inc. (AT-88-Z)
192.168.1.7 52.22.146.21 match.adsrvr.org Amazon Technologies Inc. (AT-88-Z)
192.168.1.7 52.202.218.23 mid.rkdms.com Amazon Technologies Inc. (AT-88-Z)
192.168.1.7 52.45.205.220 eb2.3lift.com Amazon Technologies Inc. (AT-88-Z)
192.168.1.7 35.244.144.168 tag.bounceexchange.com Google LLC (GOOGL-2)
192.168.1.7 35.190.72.21 api.rlcdn.com Google LLC (GOOGL-2)
192.168.1.7 199.232.36.157 static.ads-twitter.com Fastly (SKYCA-3)
192.168.1.7 104.26.2.116 tru.am Cloudflare, Inc. (CLOUD14)
192.168.1.7 151.101.210.202 mab.chartbeat.com Fastly (SKYCA-3)
192.168.1.7 192.96.161.160 as-sec.casalemedia.com Optimum WiFi (CHL-54)
192.168.1.7 143.204.144.83 cdn.segment.com Amazon Technologies Inc. (AT-88-Z)
192.168.1.7 99.84.112.160 d9t9vcvz5fqud.cloudfront.net Amazon.com, Inc. (AMAZO-4)
192.168.1.7 23.47.146.100 sb.scorecardresearch.com Akamai Technologies, Inc. (AKAMAI)
192.168.1.7 104.20.185.68 geolocation.onetrust.com Cloudflare, Inc. (CLOUD14)
192.168.1.7 3.15.57.168 secure-us.imrworldwide.com Amazon Technologies Inc. (AT-88-Z)
192.168.1.7 99.84.41.15 cdn.boomtrain.com Amazon.com, Inc. (AMAZO-4)
192.168.1.7 104.123.62.65 s.cdn.turner.com Akamai Technologies, Inc. (AKAMAI)
192.168.1.7 192.243.250.58 cm.everesttech.net Adobe Systems Inc. (AS)
192.168.1.7 172.217.10.8 www.googletagmanager.com Google LLC (GOGL)
192.168.1.7 23.208.46.198 eus.rubiconproject.com Akamai Technologies, Inc. (AKAMAI)
192.168.1.7 192.96.162.40 widgets.outbrain.com Optimum WiFi (CHL-54)
192.168.1.7 199.232.36.64 img.bleacherreport.net Fastly (SKYCA-3)
192.168.1.7 34.232.187.93 w.usabilla.com Amazon Technologies Inc. (AT-88-Z)
192.168.1.7 35.172.8.7 people.api.boomtrain.com Amazon Technologies Inc. (AT-88-Z)
192.168.1.7 199.232.37.108 acdn.adnxs.com Fastly (SKYCA-3)
192.168.1.7 54.148.89.138 api.segment.io Amazon Technologies Inc. (AT-88-Z)
192.168.1.7 192.96.160.65 tcheck.outbrainimg.com Optimum WiFi (CHL-54)

192.168.1.7	208.185.50.90	pixel-us-east.rubiconproject.com	Zayo Bandwidth (ZAYOB)
192.168.1.7	64.202.112.31	tr.outbrain.com	Server Central Network (SCN-18)
192.168.1.7	64.202.112.31	amplifypixel.outbrain.com	Server Central Network (SCN-18)
192.168.1.7	34.98.72.95	assets.bounceexchange.com	Google LLC (GOOGL-2)
192.168.1.7	64.202.112.127	log.outbrainimg.com	Server Central Network (SCN-18)
192.168.1.7	54.208.111.65	events.api.boomtrain.com	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	68.67.160.133	secure.adnxs.com	AppNexus, Inc (APPNE)
192.168.1.7	151.101.208.175	consumer.krxd.net	Fastly (SKYCA-3)
192.168.1.7	52.35.128.31	pixel.mtrcs.samba.tv	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	23.192.2.89	weather.com	Akamai Technologies, Inc. (AKAMAI)
192.168.1.7	69.164.46.136	ads.jetpackdigital.com	Limelight Networks, Inc. (LLNW)
192.168.1.7	192.96.162.213	z.moatads.com	Optimum WiFi (CHL-54)
192.168.1.7	172.217.11.33	tpc.googlesyndication.com	Google LLC (GOGL)
192.168.1.7	172.217.10.6	ad.doubleclick.net	Google LLC (GOGL)
192.168.1.7	31.13.71.7	connect.facebook.net	unknown
192.168.1.7	172.217.11.42	fonts.googleapis.com	Google LLC (GOGL)
192.168.1.7	199.232.38.109	cdn.polyfill.io	Fastly (SKYCA-3)
192.168.1.7	8.43.72.97	token.rubiconproject.com	Level 3 Parent, LLC (LPL-141)
192.168.1.7	151.101.210.133	s.w-x.co	Fastly (SKYCA-3)
192.168.1.7	151.101.210.2	odb.outbrain.com	Fastly (SKYCA-3)
192.168.1.7	99.84.41.22	static.adsafeprotected.com	Amazon.com, Inc. (AMAZO-4)
192.168.1.7	13.33.87.44	tracking.jetpackdigital.com	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	52.201.141.233	usermatch.krxd.net	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	216.200.232.114	sync.mathtag.com	Zayo Bandwidth (ZAYOB)
192.168.1.7	23.192.2.89	api.weather.com	Akamai Technologies, Inc. (AKAMAI)
192.168.1.7	52.7.194.184	geo.moatads.com	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	70.42.32.127	mcdp-nydc1.outbrain.com	Internap Corporation (IC-1425)
192.168.1.7	104.19.147.29	www.lendingtree.com	Cloudflare, Inc. (CLOUD14)
192.168.1.7	192.35.249.127	sync.search.spotxchange.com	SpotX, Inc. (SPOTX)
192.168.1.7	63.251.28.140	bea4.v.fwmrm.net	Internap Corporation (IC-1425)
192.168.1.7	3.230.62.22	ps.eyeota.net	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	63.251.88.56	aa.agkn.com	Internap Corporation (IC-1425)

192.168.1.7	104.244.42.195	analytics.twitter.com	Twitter Inc. (TWITT)
192.168.1.7	172.217.12.130	cm.g.doubleclick.net	Google LLC (GOGL)
192.168.1.7	199.232.38.49	sync-tm.everesttech.net	Fastly (SKYCA-3)
192.168.1.7	104.244.42.133	t.co	Twitter Inc. (TWITT)
192.168.1.7	3.85.187.193	sync.crwdcntrl.net	Amazon Data Services NoVa (ADSN-1)
192.168.1.7	8.43.72.97	pixel.rubiconproject.com	Level 3 Parent, LLC (LPL-141)
192.168.1.7	107.23.112.82	beacon.krxd.net	Amazon.com, Inc. (AMAZO-4)
192.168.1.7	172.217.10.98	pagead2.googlesyndication.com	Google LLC (GOGL)
192.168.1.7	31.13.71.36	www.facebook.com	unknown
192.168.1.7	69.147.82.60	ads.yahoo.com	Oath Holdings Inc. (OH-207)
192.168.1.7	74.6.138.75	pr-bh.ybp.yahoo.com	Oath Holdings Inc. (OH-207)
192.168.1.7	184.87.80.47	tags.bluekai.com	Akamai Technologies, Inc. (AKAMAI)
192.168.1.7	64.202.112.31	b1sync.zemanta.com	Server Central Network (SCN-18)
192.168.1.7	35.207.24.140	rtb.mfadsrvr.com	Google LLC (GOOGL-2)
192.168.1.7	52.199.164.64	sync-jp.im-apps.net	Amazon Data Services Japan (AMAZO-49)
192.168.1.7	74.119.119.151	bidder.criteo.com	Criteo Corp. (CRITE-6)
192.168.1.7	35.211.114.141	x.bidswitch.net	Google LLC (GOOGL-2)
192.168.1.7	64.202.112.127	sync.outbrain.com	Server Central Network (SCN-18)
192.168.1.7	74.119.119.150	dis.criteo.com	Criteo Corp. (CRITE-6)
192.168.1.7	172.217.10.238	www.google-analytics.com	Google LLC (GOGL)
192.168.1.7	35.227.229.34	cnn.bounceexchange.com	Google LLC (GOOGL-2)
192.168.1.7	34.234.23.242	sodc.weather.com	Amazon Technologies Inc. (AT-88-Z)
192.168.1.7	169.55.87.99	triggers.wfxtriggers.com	RIPE Network Coordination Centre (RIPE)
192.168.1.7	72.21.91.113	tags.crwdcntrl.net	MCI Communications Services, Inc. d/b/a Verizon Business (MCICS)
192.168.1.7	3.18.57.205	mb.moatads.com	Amazon Technologies Inc. (AT-88-Z)

5. User-Agent Spoofing

Things I Know About You:

Username: song@cooper.edu
Password: IAMTHEOSONG
IP Address: 199.98.27.186
Operating System: iOS
Browser: Mobile Safari 11.0
Favorite Season: Spring
Favorite Class: NetComms
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 11_0 like Mac OS X) AppleWebKit/604.1.34 (KHTML, like Gecko) Version/11.0 Mobile/15A5341f Safari/604.1
Spoofed Secret Key: b92fdbc345f134071cd42da90b1a2760