Project 2a

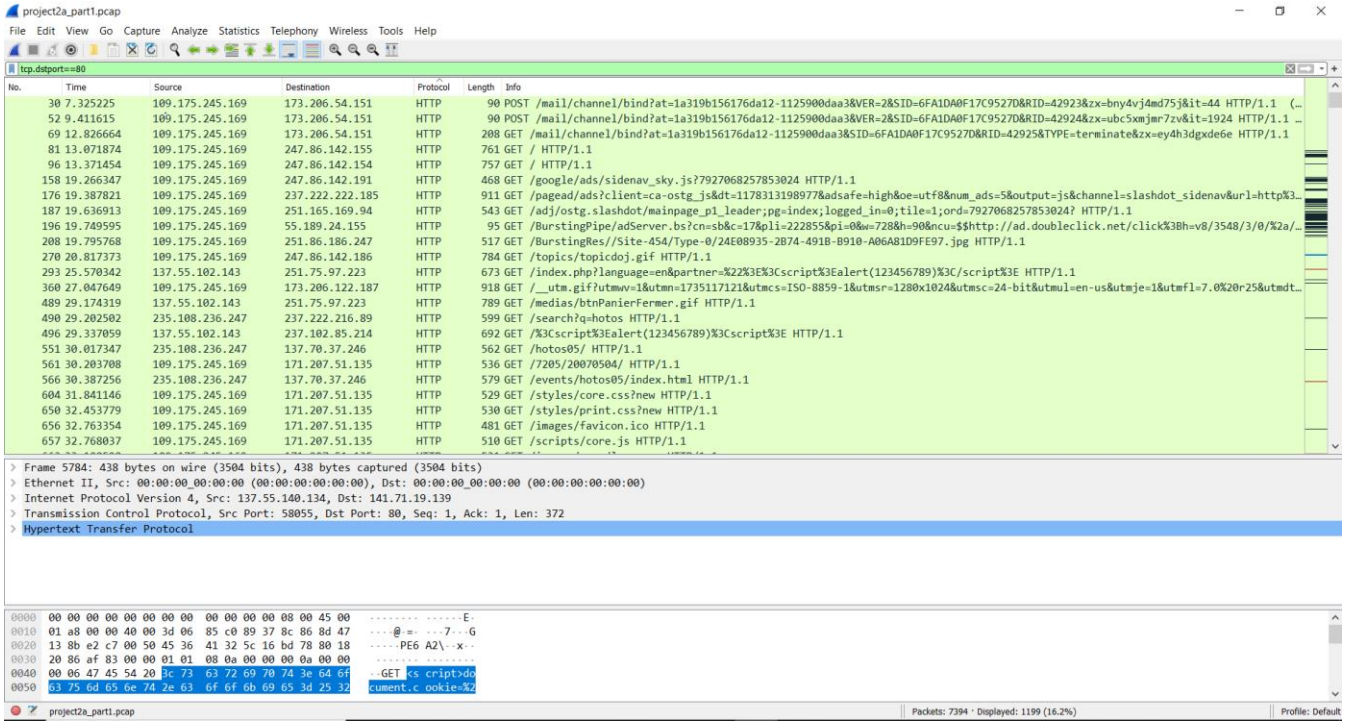
Part 1. Automating the Exploration of Network Traces

1. HTTP Sessions

Filter command: tcp.port==80 (ordered by HTTP protocol)

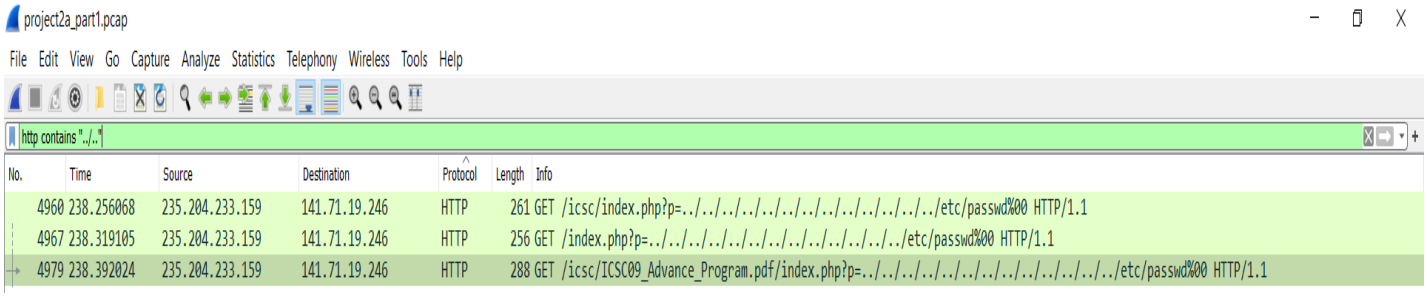
173.206.54.151
247.86.142.155
247.86.142.154
247.86.142.191
237.222.222.185
251.165.169.94
55.189.24.155
251.86.186.247
247.86.142.186
251.75.97.223
173.206.122.187
237.222.216.89
237.102.85.214
137.70.37.246
171.207.51.135
139.55.37.106
139.55.37.91
75.87.179.110
137.119.164.250
249.214.208.238
141.86.181.111
137.111.102.158
235.108.236.198
237.222.216.122
169.37.55.223
137.103.75.142
169.37.25.187
169.37.7.119
75.87.30.111
139.175.119.91
185.204.160.139
45.212.75.86
173.223.40.79
249.205.224.159
175.245.254.78
175.245.254.91
235.110.220.142

235.108.232.138
141.71.19.139



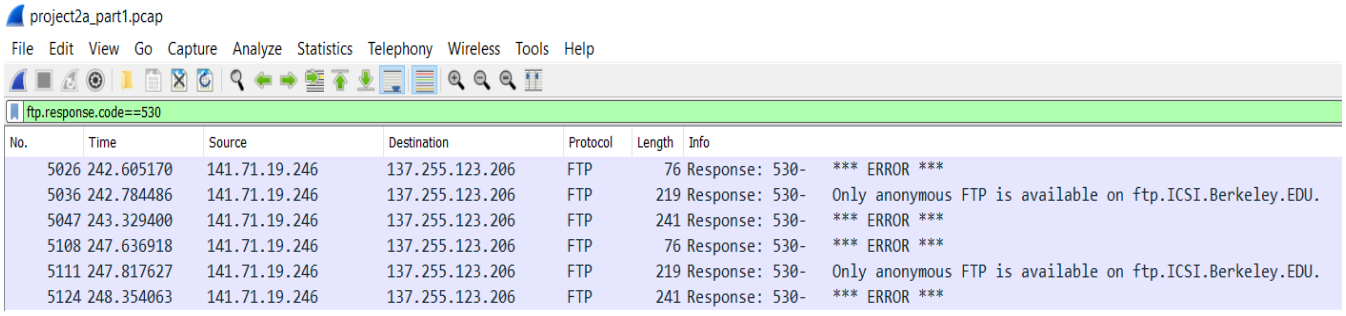
2. Directory Traversal

Filter command: http contains "../.."
235.204.233.159



3. Password Guessing

Filter command: ftp.response.code==530
141.71.19.246

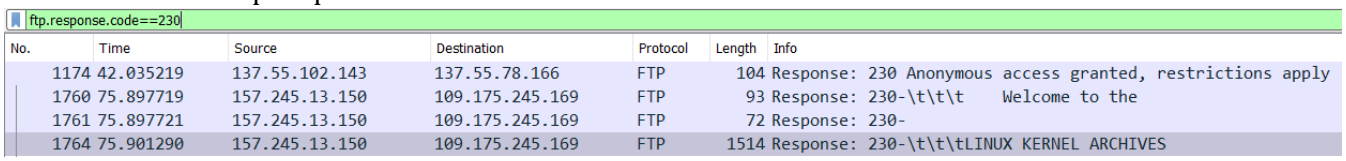


No.	Time	Source	Destination	Protocol	Length	Info
5026	242.605170	141.71.19.246	137.255.123.206	FTP	76	Response: 530- *** ERROR ***
5036	242.784486	141.71.19.246	137.255.123.206	FTP	219	Response: 530- Only anonymous FTP is available on ftp.ICSI.Berkeley.EDU.
5047	243.329400	141.71.19.246	137.255.123.206	FTP	241	Response: 530- *** ERROR ***
5108	247.636918	141.71.19.246	137.255.123.206	FTP	76	Response: 530- *** ERROR ***
5111	247.817627	141.71.19.246	137.255.123.206	FTP	219	Response: 530- Only anonymous FTP is available on ftp.ICSI.Berkeley.EDU.
5124	248.354063	141.71.19.246	137.255.123.206	FTP	241	Response: 530- *** ERROR ***

4. Unencrypted Usernames and Passwords

Username: calrules
Password: thisissosecure

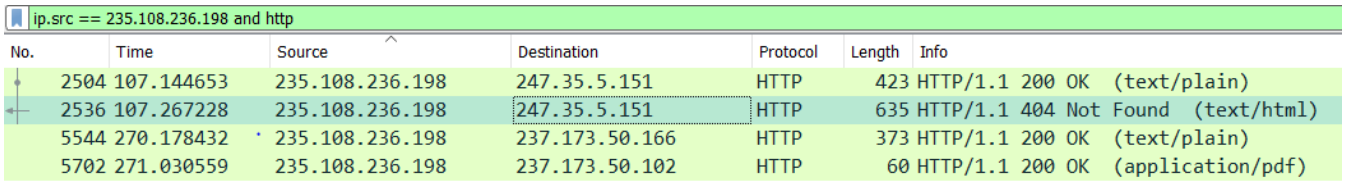
Filter command: ftp.response.code==230



No.	Time	Source	Destination	Protocol	Length	Info
1174	42.035219	137.55.102.143	137.55.78.166	FTP	104	Response: 230 Anonymous access granted, restrictions apply
1760	75.897719	157.245.13.150	109.175.245.169	FTP	93	Response: 230-\t\t\t Welcome to the
1761	75.897721	157.245.13.150	109.175.245.169	FTP	72	Response: 230-
1764	75.901290	157.245.13.150	109.175.245.169	FTP	1514	Response: 230-\t\t\tLINUX KERNEL ARCHIVES

5. Service Versions

Filter command: http.server contains "Apache/1.3.28"
235.108.236.198



No.	Time	Source	Destination	Protocol	Length	Info
2504	107.144653	235.108.236.198	247.35.5.151	HTTP	423	HTTP/1.1 200 OK (text/plain)
2536	107.267228	235.108.236.198	247.35.5.151	HTTP	635	HTTP/1.1 404 Not Found (text/html)
5544	270.178432	235.108.236.198	237.173.50.166	HTTP	373	HTTP/1.1 200 OK (text/plain)
5702	271.030559	235.108.236.198	237.173.50.102	HTTP	60	HTTP/1.1 200 OK (application/pdf)

6. DNS and Source Port Randomization

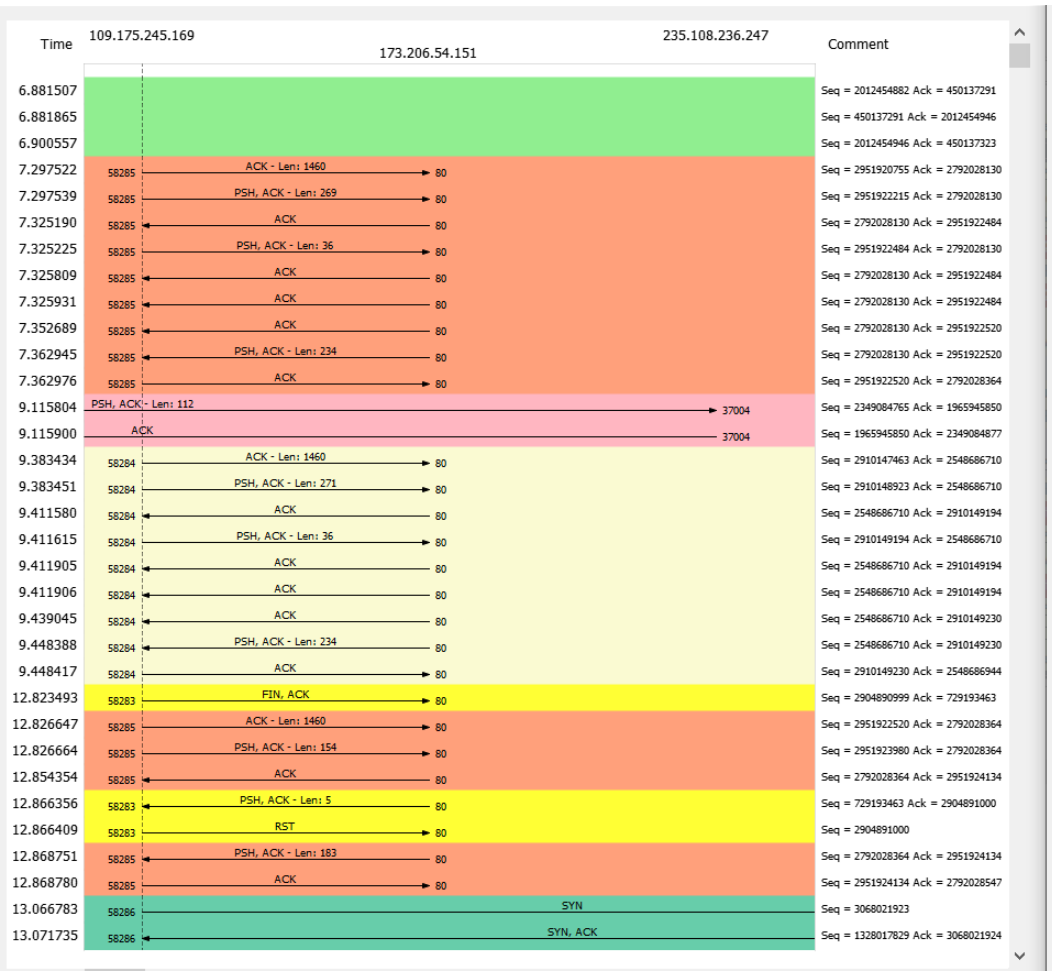
Filter command: udp.srcport != 53 and dns (added source port column)
235.108.236.198
235.108.236.247

udp and dns

No.	Time	Source	Destination	Protocol	Length	Source Port	Info
4924	233.220211	137.55.102.78	137.55.102.143	DNS	138	53	Standard query response 0x9377 No such name A asdlf
4926	233.220622	137.55.102.78	137.55.102.143	DNS	141	53	Standard query response 0x2d13 No such name A asdlf
4928	233.221026	137.55.102.78	137.55.102.143	DNS	146	53	Standard query response 0x8584 No such name A asdlf
4930	233.221399	137.55.102.78	137.55.102.143	DNS	145	53	Standard query response 0xdb1a No such name A asdlf
4932	233.223120	137.55.102.78	137.55.102.143	DNS	141	53	Standard query response 0xed22 No such name A asdlf
4933	233.226520	137.55.102.78	137.55.102.143	DNS	147	53	Standard query response 0x1ba0 No such name A asdlf
5494	265.301760	235.108.236.198	235.108.80.202	DNS	82	33814	Standard query 0xc9ea AAAA footstool.stanford.edu
5496	265.302713	235.108.236.198	235.108.80.202	DNS	82	33814	Standard query 0xba8d A footstool.stanford.edu
546	29.987406	235.108.236.247	235.108.80.86	DNS	74	32927	Standard query 0x18aa A www.usenix.org
1810	79.747060	235.108.236.247	235.108.80.86	DNS	68	32927	Standard query 0x6464 A sosp.org
3438	200.145702	235.108.236.247	235.108.80.86	DNS	73	32927	Standard query 0x982d A sb.google.com
3632	206.757828	235.108.236.247	235.108.80.86	DNS	75	32927	Standard query 0x19e7 A www.sigcomm.org
4672	224.318623	235.108.236.247	235.108.80.86	DNS	79	32927	Standard query 0x7725 AAAA sighup.stanford.edu
4711	229.318626	235.108.236.247	235.108.80.86	DNS	79	32927	Standard query 0x7725 AAAA sighup.stanford.edu
4751	231.665282	235.108.236.247	235.108.80.86	DNS	86	32927	Standard query 0x75a1 A proxy-service.stanford.edu
4762	231.720456	235.108.236.247	235.108.80.86	DNS	81	32927	Standard query 0x3e17 A weblogin.stanford.edu
5293	260.836407	235.108.236.247	235.108.80.86	DNS	82	32927	Standard query 0x7561 A sigcomm06.stanford.edu

7. TCP Sequence Numbers

109.175.245.169
235.108.236.247



Ethernet · 1 | IPv4 · 178 | IPv6 · 2

Address	Port	Packets	Byt
235.108.236.247	33303	241	18
137.103.75.142	80	204	13
235.108.236.198	80	193	15
137.55.102.143	42949	184	18
157.245.13.150	20	184	13
251.75.97.223	80	184	18
137.55.78.166	47935	171	1
137.55.102.143	21	171	1
237.173.50.102	53706	169	15
43.229.106.187	22	162	3
141.71.19.139	80	162	3
235.108.236.247	37004	162	3
109.175.245.169	58310	136	11
109.175.245.169	58296	132	10
235.108.236.247	33297	122	9
109.175.245.169	39197	118	79
235.108.232.206	23	118	79
109.175.245.169	54556	86	91
157.245.13.150	21	86	91
109.175.245.169	58289	67	4
237.222.222.185	80	67	4
235.110.220.181	443	61	2
109.175.245.169	58292	57	4
235.108.236.247	33298	57	3
251.86.186.247	80	57	4
141.71.19.246	80	54	2
237.222.216.89	80	53	2
137.119.164.250	80	44	2
141.71.19.246	21	39	35
137.55.102.143	60385	37	2
109.175.245.169	58287	36	1
247.86.142.154	80	36	1
137.111.102.158	80	35	1
235.108.236.247	48580	35	1
137.55.102.143	53745	34	1
237.102.85.214	80	34	1
235.110.220.142	80	33	86

8. Traceroute Scanning

Filter command: icmp

109.175.254.169
159.53.251.121

icmp

No.	Time	Source	Destination	Protocol	Length	Source Port	Info
5509	266.492204	109.175.245.169	159.53.251.121	ICMP	98		Echo (ping) request
5514	267.498150	109.175.245.169	159.53.251.121	ICMP	98		Echo (ping) request
5526	268.508177	109.175.245.169	159.53.251.121	ICMP	98		Echo (ping) request
5533	269.518120	109.175.245.169	159.53.251.121	ICMP	98		Echo (ping) request
5551	270.528125	109.175.245.169	159.53.251.121	ICMP	98		Echo (ping) request
5724	271.538136	109.175.245.169	159.53.251.121	ICMP	98		Echo (ping) request
2069	98.867687	137.54.159.182	141.71.17.218	ICMP	98		Echo (ping) request
2084	99.882986	137.54.159.182	141.71.17.218	ICMP	98		Echo (ping) request
5510	266.496679	159.53.251.121	109.175.245.169	ICMP	98		Echo (ping) reply
5515	267.502592	159.53.251.121	109.175.245.169	ICMP	98		Echo (ping) reply
5527	268.511963	159.53.251.121	109.175.245.169	ICMP	98		Echo (ping) reply
5534	269.522080	159.53.251.121	109.175.245.169	ICMP	98		Echo (ping) reply
5552	270.532201	159.53.251.121	109.175.245.169	ICMP	98		Echo (ping) reply
5725	271.542195	159.53.251.121	109.175.245.169	ICMP	98		Echo (ping) reply

9. Cross-Site Scripting

Filer command: http.request.uri contains "<script>"
141.71.19.139

http.request.uri contains "<script>"

No.	Time	Source	Destination	Protocol	Length	Source Port	Info
5745	275.936048	137.55.140.134	141.71.19.139	HTTP	452		GET /v9j2h7a7.cgi?<script>document.cookie=%22testhzlg=9267;%22</script> HTTP/1.1
5784	280.356662	137.55.140.134	141.71.19.139	HTTP	438		GET <script>document.cookie=%22testhzlg=9267;%22</script> HTTP/1.1
5794	280.360718	137.55.140.134	141.71.19.139	HTTP	440		GET /?<script>document.cookie=%22testhzlg=9267;%22</script> HTTP/1.1
5910	309.264438	137.55.140.134	141.71.19.139	HTTP	441		GET /kqwjy4bc.cgi?<script>cross_site_scripting.nasl</script> HTTP/1.1
5920	313.712048	137.55.140.134	141.71.19.139	HTTP	427		GET <script>cross_site_scripting.nasl</script> HTTP/1.1
5930	313.728796	137.55.140.134	141.71.19.139	HTTP	429		GET /?<script>cross_site_scripting.nasl</script> HTTP/1.1
5943	316.312343	137.55.140.134	141.71.19.139	HTTP	394		GET /index.html?urlmaskfilter=<script>foo</script> HTTP/1.1
5965	319.964998	137.55.140.134	141.71.19.139	HTTP	390		GET /viewcvs.cgi/?cvsroot=<script>foo</script> HTTP/1.1
5975	320.557461	137.55.140.134	141.71.19.139	HTTP	452		GET /pub/bootstrap/?"><script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1
5985	320.564503	137.55.140.134	141.71.19.139	HTTP	442		GET /pub/?"><script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1
5995	320.651537	137.55.140.134	141.71.19.139	HTTP	419		GET /swsrv.cgi?wg=<script>foo</script> HTTP/1.1
6005	320.802890	137.55.140.134	141.71.19.139	HTTP	438		GET /?"><script>alert('struts_sa_surl_xss.nasl')</script> HTTP/1.1
6018	321.095998	137.55.140.134	141.71.19.139	HTTP	429		GET /pub/bootstrap?username="<script>foo</script HTTP/1.1
6028	321.104065	137.55.140.134	141.71.19.139	HTTP	419		GET /pub?username="<script>foo</script HTTP/1.1
6038	321.352898	137.55.140.134	141.71.19.139	HTTP	415		GET ?username="<script>foo</script HTTP/1.1

Part 2. Interpreting Network Traces

1. Multiple devices are connected to the local network. What are their MAC and IP addresses?

Source MAC: Apple_e5:66:07 (00:26:08:e5:66:07)
Source IP: 10.0.2.1

dhcp

No.	Time	Source	Destination	Protocol	Length	Source Port	Info
6582	54.531396	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd3
6592	55.895439	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd3
6613	58.295061	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd3
8187	63.048086	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd3
11153	71.850864	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd3
13320	80.366471	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd3
14771	89.052251	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd3
15953	97.134588	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd3
16248	105.563669	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd3
16405	113.646091	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd3
22423	181.856377	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd4
22441	183.164441	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd4
22503	186.083002	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd4
22612	190.085313	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd4
22635	198.094377	0.0.0.0	255.255.255.255	DHCP	342	68	DHCP Discover - Transaction ID 0xc5381dd4

Source MAC: IntelCor_50:f0:a6 (8c:a9:82:50:f0:a6)
Source IP: 10.0.2.3

tcp

No.	Time	Source	Destination	Protocol	Length	Source Port	Info
4527	41.013503	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
4543	41.765177	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
4544	42.517178	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
4590	43.519020	10.0.2.1	10.0.2.255	NBNS	92	137	Name query NB <01><02>__MSBROWSE__<02><01>
4591	43.547107	10.0.2.1	10.0.2.255	NBNS	92	137	Name query NB MYGROUP<1d>
4594	43.573081	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
4610	44.323071	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
4611	44.323411	10.0.2.1	10.0.2.255	NBNS	92	137	Name query NB <01><02>__MSBROWSE__<02><01>
4622	45.073690	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
4624	45.074444	10.0.2.1	10.0.2.255	NBNS	92	137	Name query NB <01><02>__MSBROWSE__<02><01>
4660	46.139490	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
4680	46.882752	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
4711	47.632255	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
4759	48.687645	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
4791	49.437269	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
4845	50.187818	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
5330	51.242320	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
6165	51.994197	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
6470	52.744111	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
6580	53.798057	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
6583	54.548403	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>
6586	55.302956	10.0.2.3	10.0.2.255	NBNS	92	137	Name query NB WPAD<00>

Source MAC: Apple_d8:0f:fa (04:0c:ce:d8:0f:fa)
Source IP: 10.0.2.2

http.request and !(ssdp)

No.	Time	Source	Destination	Protocol	Length	Source Port	Info
4824	50.132698	10.0.2.3	74.125.225.209	HTTP	1117		GET /search?hl=en&rlz=1C1CHKZ_enUS430US430&sc
4886	50.253724	10.0.2.2	74.125.225.143	HTTP	580		GET /gb/images/j_e6a6aca6.png HTTP/1.1
4911	50.314226	10.0.2.2	74.125.225.211	HTTP	848		GET /blank.html HTTP/1.1
4914	50.338786	10.0.2.2	74.125.225.211	HTTP	800		GET /images/nav_logo114.png HTTP/1.1
4982	50.587951	10.0.2.2	74.125.225.211	HTTP	992		GET /xjs/_/js/s/s,jsa,c,sb,hv,wta,cr,cdos,nos
5169	50.726726	10.0.2.2	74.125.225.211	HTTP	314		GET /sdch/D-t65Pri.dct HTTP/1.1
5233	50.875568	10.0.2.3	74.125.225.209	HTTP	1266		GET /csi?v=3&s=web&action=&ei=RllyUJTFMeLByQH
5239	50.917831	10.0.2.3	74.125.225.209	HTTP	1070		GET /url?sa=f&rct=j&url=http://articles.cnn.c
5240	50.922419	10.0.2.2	74.125.225.211	HTTP	820		GET /extern_chrome/190c3c85d32a41e8.js?ie=UTF
5273	51.034884	10.0.2.2	74.125.225.211	HTTP	804		GET /textinputassistant/tia.png HTTP/1.1

2. **What type of network does this appear to be (e.g., a large corporation, an ISP backbone, etc.)? Point to evidence from the trace that supports this.**

Each interaction in this network trace has an endpoint in the local network, which indicates that it may be a router; every packet analyzed is either going out from a local host or coming into a local host.

3. **One of the clients connects to an FTP server during the trace.**
   (a) What is the DNS hostname of the server it connects to?

By filtering for FTP and then filtering for DNS, we can find the request for the IP resolution. The hostname of the site is download.xs4all.nl.

(b) Is the connection using Active or Passive FTP?

Active FTP - the client uses a PORT command and not a PASV command. In active FTP the user specifies the port on their machine that is awaiting the connection and the server connects to it. In passive FTP the user specifies PASV and the server send the user a port that they should look for data from.

(c) Based on the packet capture, what's one major vulnerability of the FTP protocol?

The bytes transferred are in plaintext; anyone who sniffs the bytes can read the content. For example, in the given network trace, we can see that the client tried to log in with username laticia.langhans and password goblue3859.

(d) Name at least two network protocols that can be used in place of FTP to provide secure file transfer.

Secure File Transfer Protocol (SFTP) and Secure Copy (SCP) are protocols that use SSH when transferring data, and thus are assumed to provide authentication and confidentiality.

4. One of the clients makes a number of requests to Facebook.

(a) Even though logins are processed over HTTPS, what is insecure about the way the browser is authenticated to Facebook?

The browser uses a cookie to authenticate to Facebook, and this cookie is visible when the user sends other requests through HTTP.

(b) How would this let an attacker impersonate the user on Facebook?

An attacker could grab the user's cookie and use it as their own.

(c) How can users protect themselves against this type of attack?

Users can't protect themselves from this type of attack, but Facebook can protect their users by using HTTPS for all their requests.

(e) What did the user do while on the Facebook site?

The user goes to the main page and searches for someone's name (Zakir Durum). The user goes to Zakir's page and sends him a message with an attachment.