

dns
✕ ➡ +

No.	Time	Source	Destination	Protocol	Length	Info
62	48.217583373	127.0.0.1	127.0.0.53	DNS	77	Standard query 0x56cd A c.go-mpulse.net
63	48.217899575	192.168.220.136	192.168.220.2	DNS	88	Standard query 0x0a7d A c.go-mpulse.net OPT
64	48.218135682	127.0.0.1	127.0.0.53	DNS	77	Standard query 0x11d8 AAAA c.go-mpulse.net
65	48.218358640	192.168.220.136	192.168.220.2	DNS	88	Standard query 0xf1f0 AAAA c.go-mpulse.net OPT
66	48.218971848	127.0.0.1	127.0.0.53	DNS	77	Standard query 0xf3f0 A c.go-mpulse.net
67	48.220051273	192.168.220.2	192.168.220.136	DNS	182	Standard query response 0x0a7d A c.go-mpulse.net CNAME wilcard.go-mpulse.net.edgekey.net CNAME e45
68	48.220456203	127.0.0.53	127.0.0.1	DNS	171	Standard query response 0xf3f0 A c.go-mpulse.net CNAME wilcard.go-mpulse.net.edgekey.net CNAME e45
69	48.220636830	127.0.0.53	127.0.0.1	DNS	171	Standard query response 0x56cd A c.go-mpulse.net CNAME wilcard.go-mpulse.net.edgekey.net CNAME e45
71	48.221712302	192.168.220.2	192.168.220.136	DNS	227	Standard query response 0xf1f0 AAAA c.go-mpulse.net CNAME wilcard.go-mpulse.net.edgekey.net CNAME
72	48.222157647	192.168.220.136	192.168.220.2	DNS	95	Standard query 0x6eef AAAA e4518.x.akamaiedge.net OPT
73	48.224638680	192.168.220.2	192.168.220.136	DNS	156	Standard query response 0x6eef AAAA e4518.x.akamaiedge.net SOA n0x.akamaiedge.net OPT
74	48.224814708	127.0.0.53	127.0.0.1	DNS	155	Standard query response 0x11d8 AAAA c.go-mpulse.net CNAME wilcard.go-mpulse.net.edgekey.net CNAME
107	62.212401803	127.0.0.1	127.0.0.53	DNS	76	Standard query 0x118b A www.google.com
108	62.212668662	192.168.220.136	192.168.220.2	DNS	87	Standard query 0xb9d1 A www.google.com OPT
109	62.214773139	192.168.220.2	192.168.220.136	DNS	103	Standard query response 0xb9d1 A www.google.com A 216.58.200.100 OPT
110	62.214955598	127.0.0.53	127.0.0.1	DNS	92	Standard query response 0x118b A www.google.com A 216.58.200.100
130	64.401939207	127.0.0.1	127.0.0.53	DNS	87	Standard query 0x5806 A www.i.matheranalytics.com
131	64.402085172	192.168.220.136	192.168.220.2	DNS	98	Standard query 0x4155 A www.i.matheranalytics.com OPT
132	64.402551111	127.0.0.1	127.0.0.53	DNS	87	Standard query 0x3c49 A www.i.matheranalytics.com
133	64.402848653	127.0.0.1	127.0.0.53	DNS	87	Standard query 0x3c0d AAAA www.i.matheranalytics.com
134	64.402943427	192.168.220.136	192.168.220.2	DNS	98	Standard query 0x1046 AAAA www.i.matheranalytics.com OPT
135	64.407212066	192.168.220.2	192.168.220.136	DNS	217	Standard query response 0x4155 A www.i.matheranalytics.com CNAME www-i-1628877250.us-east-1.elb.amaz
136	64.407503470	127.0.0.53	127.0.0.1	DNS	206	Standard query response 0x3c49 A www.i.matheranalytics.com CNAME www-i-1628877250.us-east-1.elb.amaz
137	64.407585175	127.0.0.53	127.0.0.1	DNS	206	Standard query response 0x5806 A www.i.matheranalytics.com CNAME www-i-1628877250.us-east-1.elb.amaz
139	64.439570550	192.168.220.2	192.168.220.136	DNS	235	Standard query response 0x1046 AAAA www.i.matheranalytics.com CNAME www-i-1628877250.us-east-1.elb.amaz

> Frame 62: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface any, id 0

> Linux cooked capture v1

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53

> User Datagram Protocol, Src Port: 37863, Dst Port: 53

> Domain Name System (query)

0000 00 00 03 04 00 06 00 00 00 00 00 00 00

0010 45 00 00 3d 45 9d 40 00 40 11 fc d2 7f

0020 7f 00 00 35 93 e7 00 35 00 29 fe 70 5a

0030 00 01 00 00 00 00 00 00 01 63 09 67 6e

0040 75 6c 73 65 03 6e 65 74 00 00 01 00 00

0000 00 00 03 04 00 06 00 00 00 00 00 00 00

0010 45 00 00 3d 45 9d 40 00 40 11 fc d2 7f

0020 7f 00 00 35 93 e7 00 35 00 29 fe 70 5a

0030 00 01 00 00 00 00 00 00 01 63 09 67 6e

0040 75 6c 73 65 03 6e 65 74 00 00 01 00 00

Domain Name System: Protocol
Packets: 3035 - Displayed: 622 (20.5%)
Profile: Default

Task 3: Finding Web Traffic and inspecting it

See results for destination IP. Used command: "http && ip.dst == 130.195.5.21"

<http&dst=130.195.5.21>

No.	Time	Source	Destination	Protocol	Length	Info
284	17.67975978	192.168.228.136	130.195.5.21	HTTP	486	GET /-jain/cybr17/1ab7/ HTTP/1.1
289	17.14996958	192.168.228.136	130.195.5.21	HTTP	463	GET /-jain/cybr17/1ab7/fixture-map HTTP/1.1
296	17.21879761	192.168.228.136	130.195.5.21	HTTP	463	GET /-jain/ico HTTP/1.1

Frame 284: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits) on interface any, id 0

Ethernet II, Src: Intel(R) Ethernet Controller (P0-P3) 82:00:14:00:00:00, Dst: 130.195.5.21

Internet Protocol Version 4, Src: 192.168.228.136, Dst: 130.195.5.21

Transmission Control Protocol, Src Port: 48726, Dst Port: 80, Seq: 5, Ack: 5, Len: 486

Hypertext Transfer Protocol

GET /-jain/cybr17/1ab7/ HTTP/1.1

Host: homepage.ecs.wisc.edu

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/66.0.3359.139 Chrome/66.0.3359.139 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/svg+xml;q=0.8;q=0.5

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Cookie: ...

[...] request URI: http://homepage.ecs.wisc.edu/-jain/cybr17/1ab7/

HTTP request URI

[Response in Frame 285]

[Next request in Frame 285]

0000 00 04 00 01 00 00 00 00 20 20 45 10 00 00 00 00 ... } ...

0001 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 ... E ...

0002 00 12 00 13 00 54 00 00 00 07 07 03 00 00 07 24 ... P ...

0003 00 10 72 10 74 02 00 00 00 00 00 00 00 00 00 00 ... GET /-jain/

0004 00 2F 03 70 02 72 30 37 31 71 6C 62 37 27 28 ... cybr17/1ab7/

0005 00 54 54 50 27 31 24 50 00 00 07 71 74 30 28 ... HTTP/1.1 Host:

0006 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ... homepage, <script>

0007 00 20 61 52 50 00 00 00 00 00 00 00 00 00 00 ... <script> Comment

0008 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ... <script> <script>

0009 00 16 87 87 82 81 64 83 24 40 89 75 03 63 75 72 ... Upgrade-Insecure

0010 00 54 52 50 71 75 65 75 74 30 28 21 80 65 05 ... <script> <script>

0011 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ... Upgrade-Insecure

0012 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0013 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ... Upgrade-Insecure

0014 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0015 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0016 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0017 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0018 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0019 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0020 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0021 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0022 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0023 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0024 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0025 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0026 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0027 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0028 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0029 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0030 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0031 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0032 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0033 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0034 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0035 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0036 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0037 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0038 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0039 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0040 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0041 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0042 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0043 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0044 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0045 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0046 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0047 00 70 05 72 30 47 03 00 74 30 28 00 07 78 00 00 ... Upgrade-Insecure

0048 00 70 05 72 30 4

Here we can see the result of following HTTP stream-unencrypted and we can see the HTTP stream between the client and web server:

```
GET /-lan/cybr171/lab7/ HTTP/1.1
Host: hompages.ecs.vuw.ac.nz
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/66.0.3359.139 Chrome/66.0.3359.139 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Mon, 21 May 2018 22:30:00 GMT
Server: Apache/2.2.34 (Unix) mod_ssl/2.2.34 OpenSSL/1.0.1u DAV/2 mod_wsgi/4.4.12 Python/2.7.14 mod_fcgid/2.3.9
Last-Modified: Mon, 21 May 2018 18:35:48 GMT
Accept-Ranges: bytes
Content-Length: 81
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html>
<html>
<body>


</body>
</html>
GET /-lan/cybr171/lab7/picture.png HTTP/1.1
Host: hompages.ecs.vuw.ac.nz
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/66.0.3359.139 Chrome/66.0.3359.139 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://hompages.ecs.vuw.ac.nz/~lan/cybr171/lab7/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Mon, 21 May 2018 22:30:00 GMT
Server: Apache/2.2.34 (Unix) mod_ssl/2.2.34 OpenSSL/1.0.1u DAV/2 mod_wsgi/4.4.12 Python/2.7.14 mod_fcgid/2.3.9
Last-Modified: Mon, 21 May 2018 18:28:18 GMT
Accept-Ranges: bytes
Content-Length: 119456
Cache-Control: max-age=864000
Expires: Thu, 31 May 2018 22:30:00 GMT
Keep-Alive: timeout=5, max=99

3 client paks, 3 server paks, 8 turns.
Entire conversation (125 kB)

Find:
Help Filter Out This Stream Print Save as... Back Close

HTTP/1.1 200 OK
Date: Mon, 21 May 2018 22:30:00 GMT
Server: Apache/2.2.34 (Unix) mod_ssl/2.2.34 OpenSSL/1.0.1u DAV/2 mod_wsgi/4.4.12 Python/2.7.14 mod_fcgid/2.3.9
Last-Modified: Mon, 21 May 2018 18:28:18 GMT
Accept-Ranges: bytes
Content-Length: 119456
Cache-Control: max-age=864000
Expires: Thu, 31 May 2018 22:30:00 GMT
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: image/png

.PNG
....
IHDR.....Y.....gAMA.....a.....sRGB.....PLTE.....
....
.....12.....2..1.....+..$.....0.....DED.....74...../..8"".....
.....DC.....G.....
.....0.....
.....NB3.....#564""#.....cee.....).....
.....KFA.....F.....#.....1.....NY:151".....01.....9.....MMK.....[wxRJM.....k]f.....0.....ed|tbIUSLY.....XG.....gbS.....MKC
.....08.....9th.....7.....CPMB_V_SSP.....44.....0.....14/#.....3.....P5VMT(z.....)dn31Y(.....XPG<ahl.....ES_JXBK.....#X(k.....XG1.....xlyxpqj.....(F.....
%P.....^Yp[QwtgBME..z5G(.oJ.....XOB.....h
SF.....g4.....y5P.....p12h.....d8.....C.....Mdi.....U.....[.....0BUV.....g.....uF.....2Ld(9e7t.....,DH3,R.....XHKK.....N7gpAdom.....
...10ATx.....P9.....F.....0.....0.....55.....12.....rB.....5.....1.....ede
F"E.....E.....V.....559.....)10.....
.....J.....B.....5.....1.....2.....V.....95.....)7.....
.....1.....0.....3XK.....b2ny.....
.....M.....B.....120.....xY.....x.....V.....V.....LWtdV.....HvXppD0dxhsh(.....A.#X[
..b..EPPT+12.....z9.....V.....7[0.....d.....7.....GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7.....%.....X8.....ff6[.....Y.....Is.....F.....).....7.....ip.....7.....fs.GGP.....U.....2""bOH.....2ed.....10.....XXXX.....Tr.....
.....q.....4.....Dwd.....C.....01.....
..MF.D.....y.....x.....X.....3.....
.....G.....G.....B.....(.....F.....2.....dk9....."GE.....4.....7
```

Task 4: Extracting HTTP objects from a stream:

Export HTTP Object: Can see JPG to extract by looking through HTTP

The image shows a Wireshark packet capture of an HTTP stream. The packet list on the left shows packet 151, which is a GET request for `/live/32/w/p03zwnhc.jpg`. The packet details pane on the right shows the request structure, including the URL, headers, and body. The packet bytes pane at the bottom shows the raw data of the request.

Export HTTP objects to create HTTP objects list – Preview: p03zwnhc.jpg

The image shows the same Wireshark packet capture as above, but with the "Export - HTTP object list" dialog box open. The dialog shows a list of extracted HTTP objects, including the JPEG image `p03zwnhc.jpg` and the favicon `favicon.ico`. The "Text Filter" field is empty, and the "Content Type" is set to "All Content-Types". The "Preview" button is highlighted.

Preview of HTTP object p03zwnhc.jpg:



Task 5: HTTPS to the rescue

Looked through HTTP:

Wireshark network traffic capture showing an HTTP session. The packet list on the left shows a GET request for /success.txt and a 200 OK response. The packet details pane on the right shows the HTTP response structure, including the status line 'HTTP/1.1 200 OK (text/plain)', content type 'text/plain', and content length '448'. The packet bytes pane at the bottom shows the raw data of the response, including the status line and the body content.

Frame 16: 448 bytes on wire (3520 bits), 448 bytes captured (3520 bits) on interface any, id 0

Internet Protocol Version 4, Src: 192.168.228.136, Dst: 192.168.228.136

Transmission Control Protocol, Src Port: 80, Dst Port: 43164, Seq: 1, Ack: 297, Len: 384

Hypertext Transfer Protocol

Content-Type: text/plain

Content-Length: 448

Last-Modified: Mon, 15 May 2017 18:04:40 GMT

Etag: "ae780585f4904ce444eb7d2806123"

Accept-Ranges: bytes

HTTP/1.1 200 OK (text/plain)

Content-Type: text/plain

Content-Length: 448

Last-Modified: Mon, 15 May 2017 18:04:40 GMT

Etag: "ae780585f4904ce444eb7d2806123"

Accept-Ranges: bytes

Frame 16: 448 bytes on wire (3520 bits), 448 bytes captured (3520 bits) on interface any, id 0

Internet Protocol Version 4, Src: 192.168.228.136, Dst: 192.168.228.136

Transmission Control Protocol, Src Port: 80, Dst Port: 43164, Seq: 1, Ack: 297, Len: 384

Hypertext Transfer Protocol

Content-Type: text/plain

Content-Length: 448

Last-Modified: Mon, 15 May 2017 18:04:40 GMT

Etag: "ae780585f4904ce444eb7d2806123"

Accept-Ranges: bytes

HTTP/1.1 200 OK (text/plain)

Content-Type: text/plain

Content-Length: 448

Last-Modified: Mon, 15 May 2017 18:04:40 GMT

Etag: "ae780585f4904ce444eb7d2806123"

Accept-Ranges: bytes

Attempting to export http objects:

Wireshark - Export - HTTP object list

Text Filter: Content Type: All Content-Types

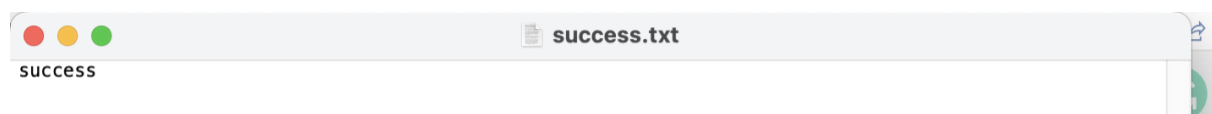
Packet	Hostname	Content Type	Size	Filename
16	detectportal.firefox.com	text/plain	8 bytes	success.txt
67	ocsp.digicert.com	application/ocsp-request	83 bytes	/
69	ocsp.digicert.com	application/ocsp-response	471 bytes	/
79	ocsp.digicert.com	application/ocsp-request	83 bytes	/
81	ocsp.digicert.com	application/ocsp-response	471 bytes	/
214	ocsp.pki.goog	application/ocsp-request	75 bytes	GTSGIAG3
221	ocsp.pki.goog	application/ocsp-response	463 bytes	GTSGIAG3
223	ocsp.pki.goog	application/ocsp-request	75 bytes	GTSGIAG3
241	ocsp.pki.goog	application/ocsp-response	463 bytes	GTSGIAG3
321	ocsp.sca1b.amazontrust.com	application/ocsp-request	83 bytes	/
326	ocsp.sca1b.amazontrust.com	application/ocsp-request	83 bytes	/
339	ocsp.sca1b.amazontrust.com	application/ocsp-response	471 bytes	/
354	ocsp.sca1b.amazontrust.com	application/ocsp-response	471 bytes	/
362	ocsp.sca1b.amazontrust.com	application/ocsp-response	471 bytes	/
374	ocsp.sca1b.amazontrust.com	application/ocsp-response	471 bytes	/
1270	ocsp.digicert.com	application/ocsp-request	83 bytes	/
1275	ocsp.pki.goog	application/ocsp-request	75 bytes	GTSGIAG3
1282	ocsp.digicert.com	application/ocsp-response	471 bytes	/
1301	ocsp.pki.goog	application/ocsp-response	463 bytes	GTSGIAG3
1633	ocsp.pki.goog	application/ocsp-request	75 bytes	GTSGIAG3
1665	ocsp.pki.goog	application/ocsp-request	75 bytes	GTSGIAG3

Wireshark - Export - HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
16	detectportal.firefox.com	text/plain	8 bytes	success.txt
67	ocsp.digicert.com	application/ocsp-request	83 bytes	/

As we can see that not much can be displayed which is likely to the objects are https encrypted compared to the objects in task number 4 where we could see all objects (e.g. jpg) as well as filenames. However here we can see there is only ocsp-requests and responses which are not readable and cannot be previewed(same thing!) apart from one .txt file (success). Here is the success.txt file.



No.	Time	Source	Destination	Protocol	Length	Info
36	0.815491282	192.168.228.136	192.168.228.136	TLSv1.2	443 [SYN]	Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=125571512 WSnd=0 WReq=0
37	0.311117088	192.168.228.136	192.168.228.136	TCP	76	S1466 -> 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=125571512 WSnd=0 WReq=0
38	0.361358858	192.168.228.136	192.168.228.136	TCP	62	443 -> S1466 [SYN, ACK] Seq=451 Acks=1 Win=64208 Len=0 MSS=1468
39	0.361365220	192.168.228.136	192.168.228.136	TCP	56	S1466 -> 443 [ACK] Seq=1 Acks=1 Win=29200 Len=0
40	0.367969424	192.168.228.136	192.168.228.136	TLSv1.2	573	Client Hello
41	0.368437867	192.168.228.136	192.168.228.136	TCP	62	443 -> S1466 [ACK] Seq=1 Acks=51 Win=64208 Len=0
44	0.407432223	192.168.228.136	192.168.228.136	TCP	62	S1466 -> S1466 [ACK] Seq=1 Acks=51 Win=64208 Len=0 MSS=1468
45	0.407547636	192.168.228.136	192.168.228.136	TCP	56	S1466 -> 443 [ACK] Seq=1 Acks=51 Win=29200 Len=0
46	0.419189454	192.168.228.136	192.168.228.136	TLSv1.2	573	Client Hello
47	0.492113541	192.168.228.136	192.168.228.136	TCP	62	443 -> S1466 [ACK] Seq=1 Acks=51 Win=64208 Len=0
48	0.547829793	192.168.228.136	192.168.228.136	TLSv1.2	1316	Server Hello
49	0.547803978	192.168.228.136	192.168.228.136	TCP	56	S1466 -> 443 [ACK] Seq=518 Acks=1461 Win=32128 Len=0
50	0.547850880	192.168.228.136	192.168.228.136	TLSv1.2	1610	Certificate, Server Key Exchange, Server Hello Done
51	0.547875144	192.168.228.136	192.168.228.136	TCP	56	S1466 -> 443 [ACK] Seq=518 Acks=2515 Win=35840 Len=0
52	0.562629540	192.168.228.136	192.168.228.136	TLSv1.2	182	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
53	0.562843414	192.168.228.136	192.168.228.136	TCP	62	443 -> S1466 [ACK] Seq=3815 Acks=644 Win=64208 Len=0
57	0.608572887	192.168.228.136	192.168.228.136	TLSv1.2	1516	Server Hello
58	0.608594786	192.168.228.136	192.168.228.136	TCP	56	S1466 -> 443 [ACK] Seq=518 Acks=1461 Win=32128 Len=0
73	0.669242528	192.168.228.136	192.168.228.136	TLSv1.2	1610	Certificate, Server Key Exchange, Server Hello Done
74	0.669263888	192.168.228.136	192.168.228.136	TCP	56	S1466 -> 443 [ACK] Seq=518 Acks=3815 Win=35840 Len=0
75	0.684813972	192.168.228.136	192.168.228.136	TLSv1.2	182	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
76	0.685881475	192.168.228.136	192.168.228.136	TCP	62	443 -> S1466 [ACK] Seq=3815 Acks=644 Win=64208 Len=0
77	0.690808748	192.168.228.136	192.168.228.136	TCP	638	Application Data
78	0.691807979	192.168.228.136	192.168.228.136	TCP	62	443 -> S1466 [ACK] Seq=3815 Acks=1226 Win=64208 Len=0
82	0.736637566	192.168.228.136	192.168.228.136	TLSv1.2	1877	Application Data
83	0.736895535	192.168.228.136	192.168.228.136	TCP	62	443 -> S1466 [ACK] Seq=3815 Acks=1605 Win=64208 Len=0
87	0.777266881	192.168.228.136	192.168.228.136	TLSv1.2	1877	Change Cipher Spec, Encrypted Handshake Message
86	0.788615422	192.168.228.136	192.168.228.136	TCP	56	S1466 -> 443 [ACK] Seq=1226 Acks=3866 Win=35840 Len=0
87	0.850808552	192.168.228.136	192.168.228.136	TCP	1877	Change Cipher Spec, Encrypted Handshake Message
88	0.908652837	192.168.228.136	192.168.228.136	TCP	56	S1466 -> 443 [ACK] Seq=1605 Acks=3866 Win=35840 Len=0
89	0.914088363	192.168.228.136	192.168.228.136	TLSv1.2	266	Application Data
90	0.914139359	192.168.228.136	192.168.228.136	TCP	56	S1466 -> 443 [ACK] Seq=1226 Acks=3276 Win=37968 Len=0
91	0.935548464	192.168.228.136	192.168.228.136	TLSv1.2	266	Application Data
92	0.935587761	192.168.228.136	192.168.228.136	TCP	56	S1466 -> 443 [ACK] Seq=1605 Acks=3276 Win=37968 Len=0
102	0.952338559	192.168.228.136	192.168.228.136	TCP	76	S1218 -> 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=140