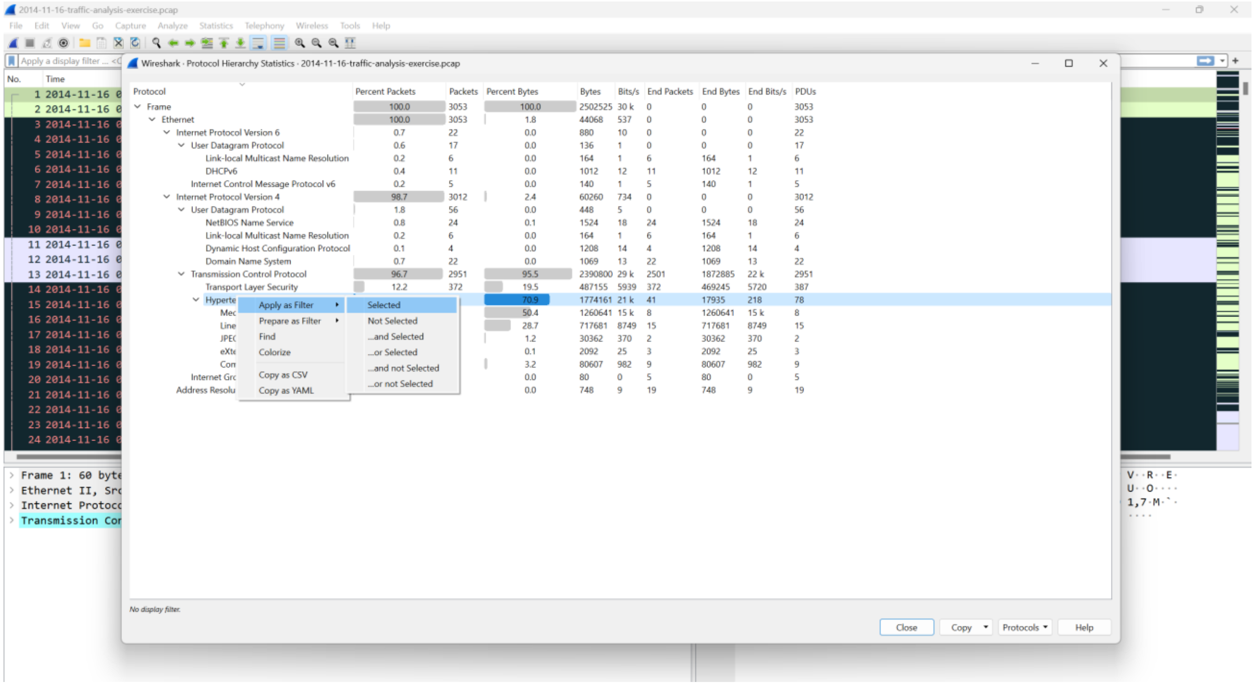
Experiment 3

Objective: Malware Traffic Analysis: Analyze captured traffic to identify signs of malware communication, such as command-and-control traffic or data infiltration.

Package: 2014-11-16-traffic-analysis-exercise.pcp

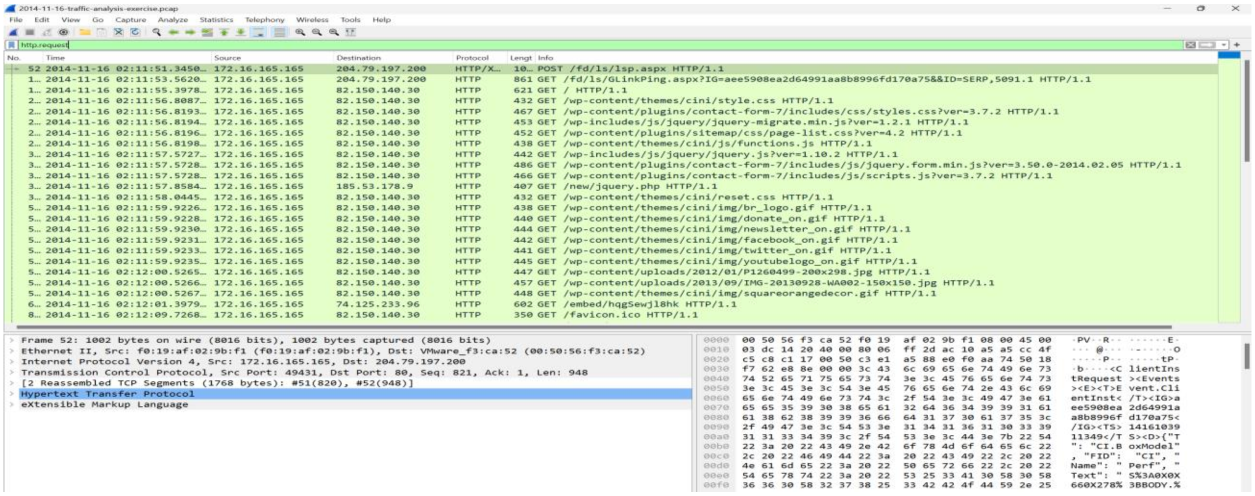
What are we looking for:

1. What are the infected file(s) downloaded and their hashes?
2. What is URL/ Domain of the infected site?
3. What is the IP address of the infected website?
4. What is the IP address of the infected machine ?
5. What is the hostname of the infected machine?
6. What is the mac address of the infected machine ?


2014-11-16-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ...
Wireshark · Protocol Hierarchy Statistics · 2014-11-16-traffic-analysis-exercise.pcap
Apply as Filter
Prepare as Filter
Find
Colorize
Copy as CSV
Copy as YAML
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
No display filter.
Close
Copy
Protocols
Help

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	3053	100.0	2502525	30 k	0	0	0	3053
Ethernet	100.0	3053	1.8	44068	537	0	0	0	3053
Internet Protocol Version 6	0.7	22	0.0	880	10	0	0	0	22
User Datagram Protocol	0.6	17	0.0	136	1	0	0	0	17
Link-local Multicast Name Resolution	0.2	6	0.0	164	1	6	164	1	6
DHCPv6	0.4	11	0.0	1012	12	11	1012	12	11
Internet Control Message Protocol v6	0.2	5	0.0	140	1	5	140	1	5
Internet Protocol Version 4	98.7	3012	2.4	60260	734	0	0	0	3012
User Datagram Protocol	1.8	56	0.0	448	5	0	0	0	56
NetBIOS Name Service	0.8	24	0.1	1524	18	24	1524	18	24
Link-local Multicast Name Resolution	0.2	6	0.0	164	1	6	164	1	6
Dynamic Host Configuration Protocol	0.1	4	0.0	1208	14	4	1208	14	4
Domain Name System	0.7	22	0.0	1069	13	22	1069	13	22
Transmission Control Protocol	96.7	2951	95.5	2390800	29 k	2501	1872885	22 k	2951
Transport Layer Security	12.2	372	19.5	487155	5939	372	469245	5720	387
Hyperte			70.9	1774161	21 k	41	17935	218	78
Mec			50.4	1260641	15 k	8	1260641	15 k	8
Line			28.7	717681	8749	15	717681	8749	15
JPEC			1.2	30362	370	2	30362	370	2
eXte			0.1	2092	25	3	2092	25	3
Con			3.2	80607	982	9	80607	982	9
Internet Grc			0.0	80	0	5	80	0	5
Address Resolu			0.0	748	9	19	748	9	19

To see only Get and Post Request : Filter ---→ http.request


2014-11-16-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

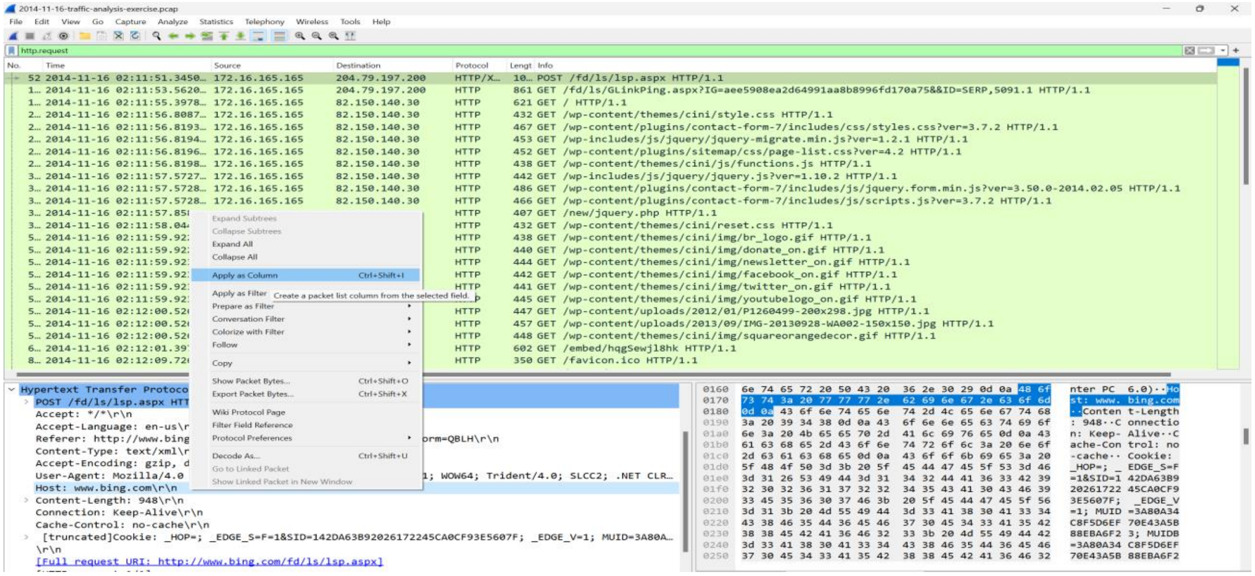
```
http.request

No.  Time                      Source           Destination      Protocol  Lengt Info
 52 2014-11-16 02:11:51.3450… 172.16.165.165   204.79.197.200   HTTP/X…   10… POST /fd/ls/lsp.aspx HTTP/1.1
 1… 2014-11-16 02:11:53.5620… 172.16.165.165   204.79.197.200   HTTP      861 GET /fd/ls/GLinkPing.aspx?IG=aee5908ea2d64991aa8b8996fd170a75&&ID=SERP,5091.1 HTTP/1.1
 1… 2014-11-16 02:11:55.3978… 172.16.165.165   82.150.140.30    HTTP      621 GET / HTTP/1.1
 2… 2014-11-16 02:11:56.8087… 172.16.165.165   82.150.140.30    HTTP      432 GET /wp-content/themes/cini/style.css HTTP/1.1
 2… 2014-11-16 02:11:56.8193… 172.16.165.165   82.150.140.30    HTTP      467 GET /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=3.7.2 HTTP/1.1
 2… 2014-11-16 02:11:56.8194… 172.16.165.165   82.150.140.30    HTTP      453 GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP/1.1
 2… 2014-11-16 02:11:56.8196… 172.16.165.165   82.150.140.30    HTTP      452 GET /wp-content/plugins/sitemap/css/page-list.css?ver=4.2 HTTP/1.1
 2… 2014-11-16 02:11:56.8198… 172.16.165.165   82.150.140.30    HTTP      438 GET /wp-content/themes/cini/js/functions.js HTTP/1.1
 3… 2014-11-16 02:11:57.5727… 172.16.165.165   82.150.140.30    HTTP      442 GET /wp-includes/js/jquery/jquery.js?ver=1.10.2 HTTP/1.1
 3… 2014-11-16 02:11:57.5728… 172.16.165.165   82.150.140.30    HTTP      486 GET /wp-content/plugins/contact-form-7/includes/js/jquery.form.min.js?ver=3.50.0-2014.02.05 HTTP/1.1
 3… 2014-11-16 02:11:57.5728… 172.16.165.165   82.150.140.30    HTTP      466 GET /wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=3.7.2 HTTP/1.1
 3… 2014-11-16 02:11:57.8584… 172.16.165.165   185.53.178.9     HTTP      407 GET /new/jquery.php HTTP/1.1
 3… 2014-11-16 02:11:58.0445… 172.16.165.165   82.150.140.30    HTTP      432 GET /wp-content/themes/cini/reset.css HTTP/1.1
 5… 2014-11-16 02:11:59.9226… 172.16.165.165   82.150.140.30    HTTP      438 GET /wp-content/themes/cini/img/br_logo.gif HTTP/1.1
 5… 2014-11-16 02:11:59.9228… 172.16.165.165   82.150.140.30    HTTP      440 GET /wp-content/themes/cini/img/donate_on.gif HTTP/1.1
 5… 2014-11-16 02:11:59.9230… 172.16.165.165   82.150.140.30    HTTP      444 GET /wp-content/themes/cini/img/newsletter_on.gif HTTP/1.1
 5… 2014-11-16 02:11:59.9231… 172.16.165.165   82.150.140.30    HTTP      442 GET /wp-content/themes/cini/img/facebook_on.gif HTTP/1.1
 5… 2014-11-16 02:11:59.9233… 172.16.165.165   82.150.140.30    HTTP      441 GET /wp-content/themes/cini/img/twitter_on.gif HTTP/1.1
 5… 2014-11-16 02:11:59.9235… 172.16.165.165   82.150.140.30    HTTP      445 GET /wp-content/themes/cini/img/youtubelogo_on.gif HTTP/1.1
 5… 2014-11-16 02:12:00.5265… 172.16.165.165   82.150.140.30    HTTP      447 GET /wp-content/uploads/2012/01/P1260499-200x298.jpg HTTP/1.1
 5… 2014-11-16 02:12:00.5266… 172.16.165.165   82.150.140.30    HTTP      457 GET /wp-content/uploads/2013/09/IMG-20130928-WA002-150x150.jpg HTTP/1.1
 5… 2014-11-16 02:12:00.5267… 172.16.165.165   82.150.140.30    HTTP      448 GET /wp-content/themes/cini/img/squareorangedecor.gif HTTP/1.1
 6… 2014-11-16 02:12:01.3979… 172.16.165.165   74.125.233.96    HTTP      602 GET /embed/hqgSewjl8hk HTTP/1.1
 8… 2014-11-16 02:12:09.7268… 172.16.165.165   82.150.140.30    HTTP      350 GET /favicon.ico HTTP/1.1
```

```
> Frame 52: 1002 bytes on wire (8016 bits), 1002 bytes captured (8016 bits)
> Ethernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: VMware_f3:ca:52 (00:50:56:f3:ca:52)
> Internet Protocol Version 4, Src: 172.16.165.165, Dst: 204.79.197.200
> Transmission Control Protocol, Src Port: 49431, Dst Port: 80, Seq: 821, Ack: 1, Len: 948
> [2 Reassembled TCP Segments (1768 bytes): #51(820), #52(948)]
> Hypertext Transfer Protocol
> eXtensible Markup Language
```

```
0000  00 50 56 f3 ca 52 f0 19  af 02 9b f1 08 00 45 00   ·PV··R·· ······E·
0010  03 dc 14 20 40 00 80 06  ff 2d ac 10 a5 a5 cc 4f   ··· @··· ·-·····O
0020  c5 c8 c1 17 00 50 c3 e1  a5 88 e0 f0 aa 74 50 18   ·····P·· ·····tP·
0030  f7 62 e8 8e 00 00 3c 43  6c 69 65 6e 74 49 6e 73   ·b····<C lientIns
0040  74 52 65 71 75 65 73 74  3e 3c 45 76 65 6e 74 73   tRequest ><Events
0050  3e 3c 45 3e 3c 54 3e 45  76 65 6e 74 2e 43 6c 69   ><E><T>E vent.Cli
0060  65 6e 74 49 6e 73 74 3c  2f 54 3e 3c 49 47 3e 61   entInst< /T><IG>a
0070  65 65 35 39 30 38 65 61  32 64 36 34 39 39 31 61   ee5908ea 2d64991a
0080  61 38 62 38 39 39 36 66  64 31 37 30 61 37 35 3c   a8b8996f d170a75<
0090  2f 49 47 3e 3c 54 53 3e  31 34 31 36 31 30 33 39   /IG><TS> 14161039
00a0  31 31 33 34 39 3c 2f 54  53 3e 3c 44 3e 7b 22 54   11349</T S><D>{"T
00b0  22 3a 20 22 43 49 2e 42  6f 78 4d 6f 64 65 6c 22   ": "CI.B oxModel"
00c0  2c 20 22 46 49 44 22 3a  20 22 43 49 22 2c 20 22   , "FID":  "CI", "
00d0  4e 61 6d 65 22 3a 20 22  50 65 72 66 22 2c 20 22   Name": " Perf", "
00e0  54 65 78 74 22 3a 20 22  53 25 33 41 30 58 30 58   Text": " S%3A0X0X
00f0  36 36 30 58 32 37 38 25  33 42 42 4f 44 59 2e 25   660X278% 3BBODY.%
```

To get the better understanding of destination: Right Click on host user HTTP


2014-11-16-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Create a packet list column from the selected field.
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window

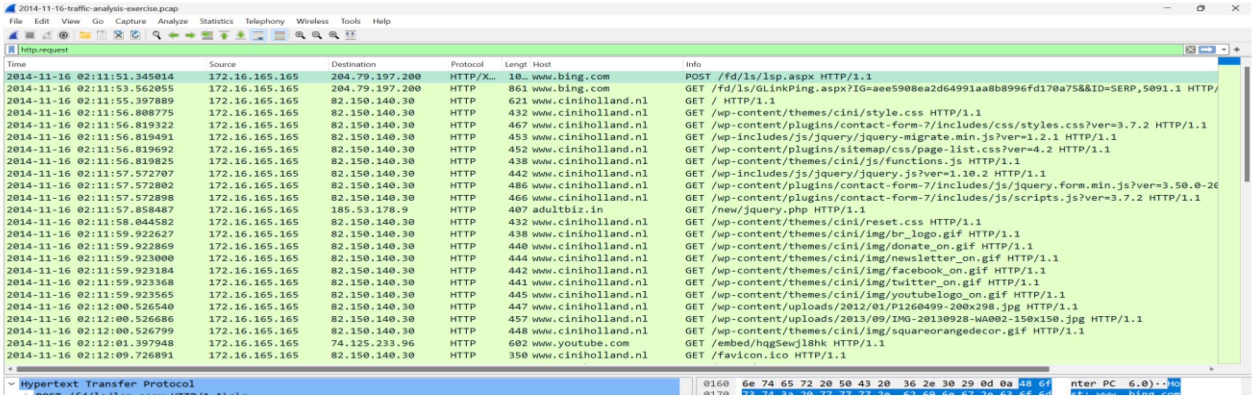
```
http.request

No.  Time                      Source           Destination      Protocol  Lengt Info
 52 2014-11-16 02:11:51.3450… 172.16.165.165   204.79.197.200   HTTP/X…   10… POST /fd/ls/lsp.aspx HTTP/1.1
 1… 2014-11-16 02:11:53.5620… 172.16.165.165   204.79.197.200   HTTP      861 GET /fd/ls/GLinkPing.aspx?IG=aee5908ea2d64991aa8b8996fd170a75&&ID=SERP,5091.1 HTTP/1.1
 1… 2014-11-16 02:11:55.3978… 172.16.165.165   82.150.140.30    HTTP      621 GET / HTTP/1.1
 2… 2014-11-16 02:11:56.8087… 172.16.165.165   82.150.140.30    HTTP      432 GET /wp-content/themes/cini/style.css HTTP/1.1
 2… 2014-11-16 02:11:56.8193… 172.16.165.165   82.150.140.30    HTTP      467 GET /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=3.7.2 HTTP/1.1
 2… 2014-11-16 02:11:56.8194… 172.16.165.165   82.150.140.30    HTTP      453 GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP/1.1
 2… 2014-11-16 02:11:56.8196… 172.16.165.165   82.150.140.30    HTTP      452 GET /wp-content/plugins/sitemap/css/page-list.css?ver=4.2 HTTP/1.1
 2… 2014-11-16 02:11:56.8198… 172.16.165.165   82.150.140.30    HTTP      438 GET /wp-content/themes/cini/js/functions.js HTTP/1.1
 3… 2014-11-16 02:11:57.5727… 172.16.165.165   82.150.140.30    HTTP      442 GET /wp-includes/js/jquery/jquery.js?ver=1.10.2 HTTP/1.1
 3… 2014-11-16 02:11:57.5728… 172.16.165.165   82.150.140.30    HTTP      486 GET /wp-content/plugins/contact-form-7/includes/js/jquery.form.min.js?ver=3.50.0-2014.02.05 HTTP/1.1
 3… 2014-11-16 02:11:57.5728… 172.16.165.165   82.150.140.30    HTTP      466 GET /wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=3.7.2 HTTP/1.1
 3… 2014-11-16 02:11:57.85                                      HTTP      407 GET /new/jquery.php HTTP/1.1
 3… 2014-11-16 02:11:58.04                                      HTTP      432 GET /wp-content/themes/cini/reset.css HTTP/1.1
 5… 2014-11-16 02:11:59.92                                      HTTP      438 GET /wp-content/themes/cini/img/br_logo.gif HTTP/1.1
 5… 2014-11-16 02:11:59.92                                      HTTP      440 GET /wp-content/themes/cini/img/donate_on.gif HTTP/1.1
 5… 2014-11-16 02:11:59.92                                      HTTP      444 GET /wp-content/themes/cini/img/newsletter_on.gif HTTP/1.1
 5… 2014-11-16 02:11:59.92                                      HTTP      442 GET /wp-content/themes/cini/img/facebook_on.gif HTTP/1.1
 5… 2014-11-16 02:11:59.92                                      HTTP      441 GET /wp-content/themes/cini/img/twitter_on.gif HTTP/1.1
 5… 2014-11-16 02:11:59.92                                                445 GET /wp-content/themes/cini/img/youtubelogo_on.gif HTTP/1.1
 5… 2014-11-16 02:12:00.52                                      HTTP      447 GET /wp-content/uploads/2012/01/P1260499-200x298.jpg HTTP/1.1
 5… 2014-11-16 02:12:00.52                                      HTTP      457 GET /wp-content/uploads/2013/09/IMG-20130928-WA002-150x150.jpg HTTP/1.1
 5… 2014-11-16 02:12:00.52                                      HTTP      448 GET /wp-content/themes/cini/img/squareorangedecor.gif HTTP/1.1
 6… 2014-11-16 02:12:01.39                                      HTTP      602 GET /embed/hqgSewjl8hk HTTP/1.1
 8… 2014-11-16 02:12:09.72                                      HTTP      350 GET /favicon.ico HTTP/1.1
```

```
v Hypertext Transfer Protoco
  > POST /fd/ls/lsp.aspx HTT
    Accept: */*\r\n
    Accept-Language: en-us\r
    Referer: http://www.bing                                orm=QBLH\r\n
    Content-Type: text/xml\r
    Accept-Encoding: gzip, d
    User-Agent: Mozilla/4.0                                 1; WOW64; Trident/4.0; SLCC2; .NET CLR…
    Host: www.bing.com\r\n
  > Content-Length: 948\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
  >  [truncated]Cookie: _HOP=; _EDGE_S=F=1&SID=142DA63B92026172245CA0CF93E5607F; _EDGE_V=1; MUID=3A80A…
    \r\n
    [Full request URI: http://www.bing.com/fd/ls/lsp.aspx]
```

```
0160  6e 74 65 72 20 50 43 20  36 2e 30 29 0d 0a 48 6f   nter PC  6.0)··Ho
0170  73 74 3a 20 77 77 77 2e  62 69 6e 67 2e 63 6f 6d   st: www. bing.com
0180  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ··Conten t-Length
0190  3a 20 39 34 38 0d 0a 43  6f 6e 6e 65 63 74 69 6f   : 948··C onnectio
01a0  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 43   n: Keep- Alive··C
01b0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6e 6f   ache-Con trol: no
01c0  2d 63 61 63 68 65 0d 0a  43 6f 6f 6b 69 65 3a 20   -cache·· Cookie: 
01d0  5f 48 4f 50 3d 3b 20 5f  45 44 47 45 5f 53 3d 46   _HOP=; _ EDGE_S=F
01e0  3d 31 26 53 49 44 3d 31  34 32 44 41 36 33 42 39   =1&SID=1 42DA63B9
01f0  32 30 32 36 31 37 32 32  34 35 43 41 30 43 46 39   20261722 45CA0CF9
0200  33 45 35 36 30 37 46 3b  20 5f 45 44 47 45 5f 56   3E5607F;  _EDGE_V
0210  3d 31 3b 20 4d 55 49 44  3d 33 41 38 30 41 33 34   =1; MUID =3A80A34
0220  43 38 46 35 44 36 45 46  37 30 45 34 33 41 35 42   C8F5D6EF 70E43A5B
0230  38 38 45 42 41 36 46 32  33 3b 20 4d 55 49 44 42   88EBA6F2 3; MUIDB
0240  3d 33 41 38 30 41 33 34  43 38 46 35 44 36 45 46   =3A80A34 C8F5D6EF
0250  37 30 45 34 33 41 35 42  38 38 45 42 41 36 46 32   70E43A5B 88EBA6F2
```

Now check Host Column

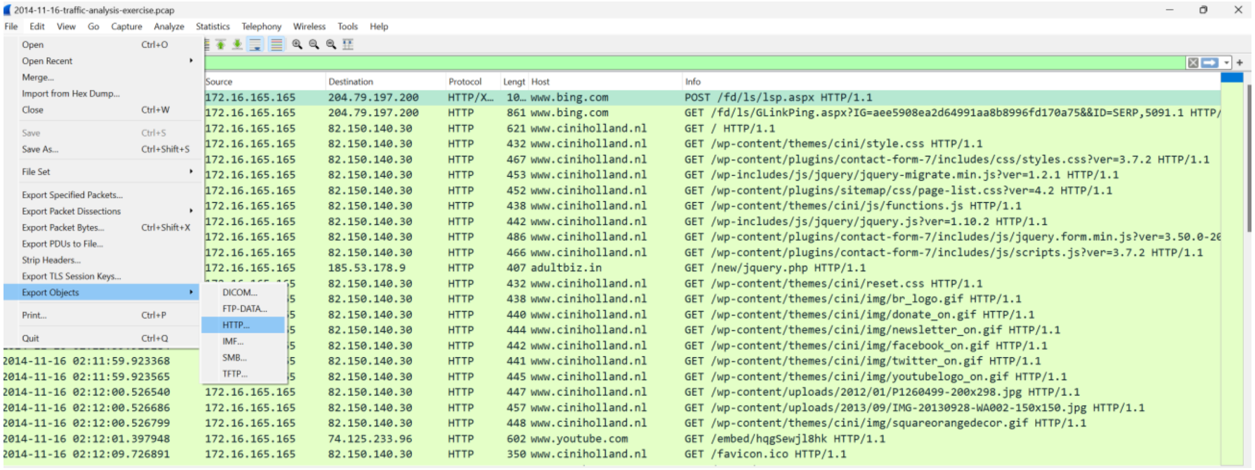

2014-11-16-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request

Time                        Source           Destination      Protocol  Lengt Host                  Info
2014-11-16 02:11:51.345014  172.16.165.165   204.79.197.200   HTTP/X…   10… www.bing.com          POST /fd/ls/lsp.aspx HTTP/1.1
2014-11-16 02:11:53.562055  172.16.165.165   204.79.197.200   HTTP      861 www.bing.com          GET /fd/ls/GLinkPing.aspx?IG=aee5908ea2d64991aa8b8996fd170a75&&ID=SERP,5091.1 HTTP/
2014-11-16 02:11:55.397889  172.16.165.165   82.150.140.30    HTTP      621 www.ciniholland.nl    GET / HTTP/1.1
2014-11-16 02:11:56.808775  172.16.165.165   82.150.140.30    HTTP      432 www.ciniholland.nl    GET /wp-content/themes/cini/style.css HTTP/1.1
2014-11-16 02:11:56.819322  172.16.165.165   82.150.140.30    HTTP      467 www.ciniholland.nl    GET /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=3.7.2 HTTP/1.1
2014-11-16 02:11:56.819491  172.16.165.165   82.150.140.30    HTTP      453 www.ciniholland.nl    GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP/1.1
2014-11-16 02:11:56.819692  172.16.165.165   82.150.140.30    HTTP      452 www.ciniholland.nl    GET /wp-content/plugins/sitemap/css/page-list.css?ver=4.2 HTTP/1.1
2014-11-16 02:11:56.819825  172.16.165.165   82.150.140.30    HTTP      438 www.ciniholland.nl    GET /wp-content/themes/cini/js/functions.js HTTP/1.1
2014-11-16 02:11:57.572707  172.16.165.165   82.150.140.30    HTTP      442 www.ciniholland.nl    GET /wp-includes/js/jquery/jquery.js?ver=1.10.2 HTTP/1.1
2014-11-16 02:11:57.572802  172.16.165.165   82.150.140.30    HTTP      486 www.ciniholland.nl    GET /wp-content/plugins/contact-form-7/includes/js/jquery.form.min.js?ver=3.50.0-20
2014-11-16 02:11:57.572898  172.16.165.165   82.150.140.30    HTTP      466 www.ciniholland.nl    GET /wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=3.7.2 HTTP/1.1
2014-11-16 02:11:57.858487  172.16.165.165   185.53.178.9     HTTP      407 adultbiz.in           GET /new/jquery.php HTTP/1.1
2014-11-16 02:11:58.044582  172.16.165.165   82.150.140.30    HTTP      432 www.ciniholland.nl    GET /wp-content/themes/cini/reset.css HTTP/1.1
2014-11-16 02:11:59.922627  172.16.165.165   82.150.140.30    HTTP      438 www.ciniholland.nl    GET /wp-content/themes/cini/img/br_logo.gif HTTP/1.1
2014-11-16 02:11:59.922869  172.16.165.165   82.150.140.30    HTTP      440 www.ciniholland.nl    GET /wp-content/themes/cini/img/donate_on.gif HTTP/1.1
2014-11-16 02:11:59.923000  172.16.165.165   82.150.140.30    HTTP      444 www.ciniholland.nl    GET /wp-content/themes/cini/img/newsletter_on.gif HTTP/1.1
2014-11-16 02:11:59.923184  172.16.165.165   82.150.140.30    HTTP      442 www.ciniholland.nl    GET /wp-content/themes/cini/img/facebook_on.gif HTTP/1.1
2014-11-16 02:11:59.923368  172.16.165.165   82.150.140.30    HTTP      441 www.ciniholland.nl    GET /wp-content/themes/cini/img/twitter_on.gif HTTP/1.1
2014-11-16 02:11:59.923565  172.16.165.165   82.150.140.30    HTTP      445 www.ciniholland.nl    GET /wp-content/themes/cini/img/youtubelogo_on.gif HTTP/1.1
2014-11-16 02:12:00.526540  172.16.165.165   82.150.140.30    HTTP      447 www.ciniholland.nl    GET /wp-content/uploads/2012/01/P1260499-200x298.jpg HTTP/1.1
2014-11-16 02:12:00.526686  172.16.165.165   82.150.140.30    HTTP      457 www.ciniholland.nl    GET /wp-content/uploads/2013/09/IMG-20130928-WA002-150x150.jpg HTTP/1.1
2014-11-16 02:12:00.526799  172.16.165.165   82.150.140.30    HTTP      448 www.ciniholland.nl    GET /wp-content/themes/cini/img/squareorangedecor.gif HTTP/1.1
2014-11-16 02:12:01.397948  172.16.165.165   74.125.233.96    HTTP      602 www.youtube.com       GET /embed/hqgSewjl8hk HTTP/1.1
2014-11-16 02:12:09.726891  172.16.165.165   82.150.140.30    HTTP      350 www.ciniholland.nl    GET /favicon.ico HTTP/1.1
```

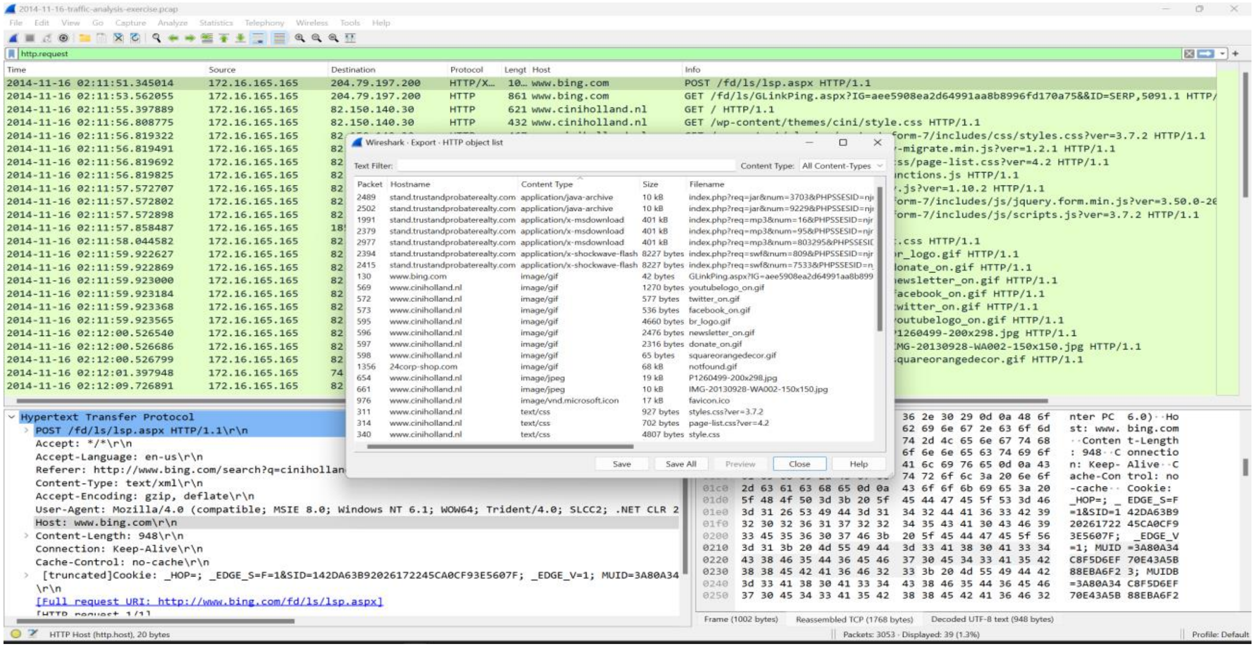
```
v Hypertext Transfer Protocol
```

```
0160  6e 74 65 72 20 50 43 20  36 2e 30 29 0d 0a 48 6f   nter PC  6.0)··Ho
```



```
Source           Destination     Protocol  Lengt Host                 Info
172.16.165.165   204.79.197.200  HTTP/X…   10…   www.bing.com         POST /fd/ls/lsp.aspx HTTP/1.1
172.16.165.165   204.79.197.200  HTTP      861   www.bing.com         GET /fd/ls/GLinkPing.aspx?IG=aee5908ea2d64991aa8b8996fd170a75&&ID=SERP,5091.1 HTTP/
172.16.165.165   82.150.140.30   HTTP      621   www.ciniholland.nl   GET / HTTP/1.1
172.16.165.165   82.150.140.30   HTTP      432   www.ciniholland.nl   GET /wp-content/themes/cini/style.css HTTP/1.1
172.16.165.165   82.150.140.30   HTTP      467   www.ciniholland.nl   GET /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=3.7.2 HTTP/1.1
172.16.165.165   82.150.140.30   HTTP      453   www.ciniholland.nl   GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP/1.1
172.16.165.165   82.150.140.30   HTTP      452   www.ciniholland.nl   GET /wp-content/plugins/sitemap/css/page-list.css?ver=4.2 HTTP/1.1
172.16.165.165   82.150.140.30   HTTP      438   www.ciniholland.nl   GET /wp-content/themes/cini/js/functions.js HTTP/1.1
172.16.165.165   82.150.140.30   HTTP      442   www.ciniholland.nl   GET /wp-includes/js/jquery/jquery.js?ver=1.10.2 HTTP/1.1
172.16.165.165   82.150.140.30   HTTP      486   www.ciniholland.nl   GET /wp-content/plugins/contact-form-7/includes/js/jquery.form.min.js?ver=3.50.0-20
172.16.165.165   82.150.140.30   HTTP      466   www.ciniholland.nl   GET /wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=3.7.2 HTTP/1.1
172.16.165.165   185.53.178.9    HTTP      407   adultbiz.in          GET /new/jquery.php HTTP/1.1
             5   82.150.140.30   HTTP      432   www.ciniholland.nl   GET /wp-content/themes/cini/reset.css HTTP/1.1
             5   82.150.140.30   HTTP      438   www.ciniholland.nl   GET /wp-content/themes/cini/img/br_logo.gif HTTP/1.1
             5   82.150.140.30   HTTP      440   www.ciniholland.nl   GET /wp-content/themes/cini/img/donate_on.gif HTTP/1.1
             5   82.150.140.30   HTTP      444   www.ciniholland.nl   GET /wp-content/themes/cini/img/newsletter_on.gif HTTP/1.1
             5   82.150.140.30   HTTP      442   www.ciniholland.nl   GET /wp-content/themes/cini/img/facebook_on.gif HTTP/1.1
2014-11-16 02:11:59.923368     5   82.150.140.30   HTTP      441   www.ciniholland.nl   GET /wp-content/themes/cini/img/twitter_on.gif HTTP/1.1
2014-11-16 02:11:59.923565     5   82.150.140.30   HTTP      445   www.ciniholland.nl   GET /wp-content/themes/cini/img/youtubelogo_on.gif HTTP/1.1
2014-11-16 02:12:00.526540  172.16.165.165   82.150.140.30   HTTP   447   www.ciniholland.nl   GET /wp-content/uploads/2012/01/P1260499-200x298.jpg HTTP/1.1
2014-11-16 02:12:00.526686  172.16.165.165   82.150.140.30   HTTP   457   www.ciniholland.nl   GET /wp-content/uploads/2013/09/IMG-20130928-WA002-150x150.jpg HTTP/1.1
2014-11-16 02:12:00.526799  172.16.165.165   82.150.140.30   HTTP   448   www.ciniholland.nl   GET /wp-content/themes/cini/img/squareorangedecor.gif HTTP/1.1
2014-11-16 02:12:01.397948  172.16.165.165   74.125.233.96   HTTP   602   www.youtube.com      GET /embed/hqgSewjl8hk HTTP/1.1
2014-11-16 02:12:09.726891  172.16.165.165   82.150.140.30   HTTP   350   www.ciniholland.nl   GET /favicon.ico HTTP/1.1
```

Sort column by Content type



http.request

```
Time                          Source
2014-11-16 02:11:51.345014    172.16.165.165
2014-11-16 02:11:53.562055    172.16.165.165
2014-11-16 02:11:55.397889    172.16.165.165
2014-11-16 02:11:56.808775    172.16.165.165
2014-11-16 02:11:56.819322    172.16.165.165
2014-11-16 02:11:56.819491    172.16.165.165
2014-11-16 02:11:56.819692    172.16.165.165
2014-11-16 02:11:56.819825    172.16.165.165
2014-11-16 02:11:57.572707    172.16.165.165
2014-11-16 02:11:57.572802    172.16.165.165
2014-11-16 02:11:57.572898    172.16.165.165
2014-11-16 02:11:57.858487    172.16.165.165
2014-11-16 02:11:58.044582    172.16.165.165
2014-11-16 02:11:59.922627    172.16.165.165
2014-11-16 02:11:59.922869    172.16.165.165
2014-11-16 02:11:59.923000    172.16.165.165
2014-11-16 02:11:59.923184    172.16.165.165
2014-11-16 02:11:59.923368    172.16.165.165
2014-11-16 02:11:59.923565    172.16.165.165
2014-11-16 02:12:00.526540    172.16.165.165
2014-11-16 02:12:00.526686    172.16.165.165
2014-11-16 02:12:00.526799    172.16.165.165
2014-11-16 02:12:01.397948    172.16.165.165
2014-11-16 02:12:09.726891    172.16.165.165
```

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
2489	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=3703&PHPSSESID=nj
2502	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=9229&PHPSSESID=nj
1991	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=16&PHPSSESID=njr
2379	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=95&PHPSSESID=njr
2977	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=803295&PHPSSESID
2394	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=809&PHPSSESID=njr
2415	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=7533&PHPSSESID=n
130	www.bing.com	image/gif	42 bytes	GLinkPing.aspx?IG=aee5908ea2d64991aa8b899
569	www.ciniholland.nl	image/gif	1270 bytes	youtubelogo_on.gif
572	www.ciniholland.nl	image/gif	577 bytes	twitter_on.gif
573	www.ciniholland.nl	image/gif	536 bytes	facebook_on.gif
595	www.ciniholland.nl	image/gif	4660 bytes	br_logo.gif
596	www.ciniholland.nl	image/gif	2476 bytes	newsletter_on.gif
597	www.ciniholland.nl	image/gif	2316 bytes	donate_on.gif
598	www.ciniholland.nl	image/gif	65 bytes	squareorangedecor.gif
1356	24corp-shop.com	image/gif	68 kB	notfound.gif
654	www.ciniholland.nl	image/jpeg	19 kB	P1260499-200x298.jpg
661	www.ciniholland.nl	image/jpeg	10 kB	IMG-20130928-WA002-150x150.jpg
976	www.ciniholland.nl	image/vnd.microsoft.icon	17 kB	favicon.ico
311	www.ciniholland.nl	text/css	927 bytes	styles.css?ver=3.7.2
314	www.ciniholland.nl	text/css	702 bytes	page-list.css?ver=4.2
340	www.ciniholland.nl	text/css	4807 bytes	style.css

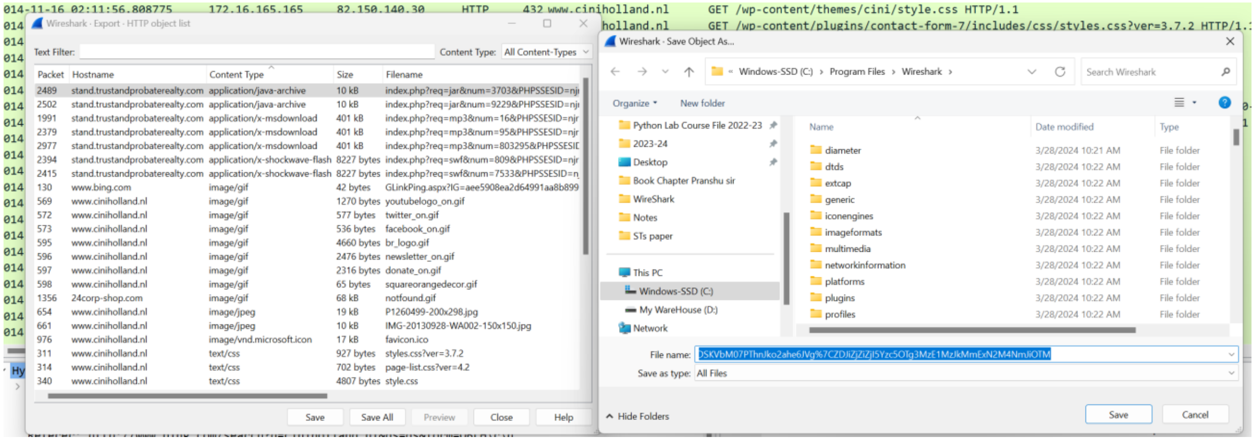
```
Hypertext Transfer Protocol
  POST /fd/ls/lsp.aspx HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Language: en-us\r\n
    Referer: http://www.bing.com/search?q=ciniholland
    Content-Type: text/xml\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2
    Host: www.bing.com\r\n
  Content-Length: 948\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
  [truncated]Cookie: _HOP=; _EDGE_S=F=1&SID=142DA63B92026172245CA0CF93E5607F; _EDGE_V=1; MUID=3A80A34
    \r\n
    [Full request URI: http://www.bing.com/fd/ls/lsp.aspx]
    [HTTP request 1/1]
```

HTTP Host (http.host), 20 bytes

Frame (1002 bytes)   Reassembled TCP (1768 bytes)   Decoded UTF-8 text (948 bytes)

Packets: 3053 · Displayed: 39 (1.3%)   Profile: Default

We can save all suspicious files



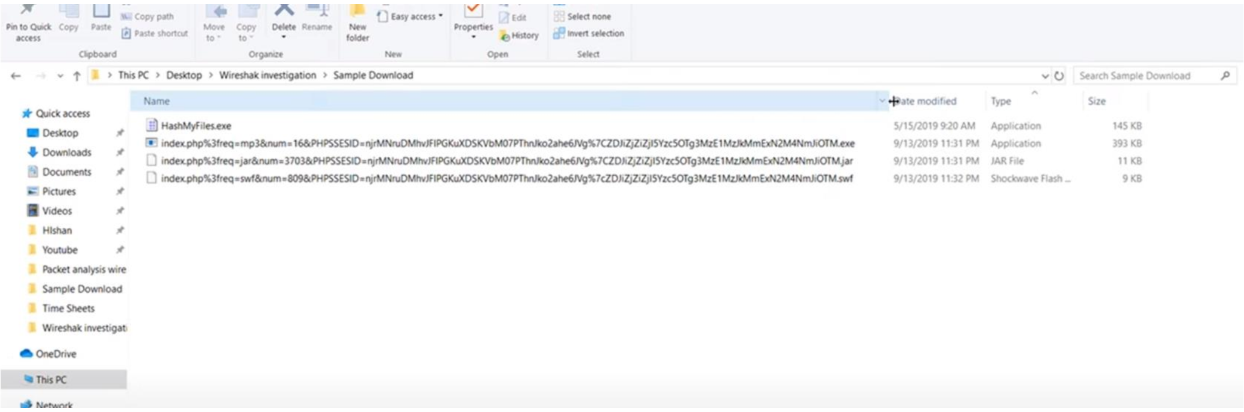
Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
2489	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=3703&PHPSSESID=nj
2502	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=9229&PHPSSESID=nj
1991	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=16&PHPSSESID=njr
2379	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=95&PHPSSESID=njr
2977	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=803295&PHPSSESID
2394	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=809&PHPSSESID=njr
2415	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=7533&PHPSSESID=n
130	www.bing.com	image/gif	42 bytes	GLinkPing.aspx?IG=aee5908ea2d64991aa8b899
569	www.ciniholland.nl	image/gif	1270 bytes	youtubelogo_on.gif
572	www.ciniholland.nl	image/gif	577 bytes	twitter_on.gif
573	www.ciniholland.nl	image/gif	536 bytes	facebook_on.gif
595	www.ciniholland.nl	image/gif	4660 bytes	br_logo.gif
596	www.ciniholland.nl	image/gif	2476 bytes	newsletter_on.gif
597	www.ciniholland.nl	image/gif	2316 bytes	donate_on.gif
598	www.ciniholland.nl	image/gif	65 bytes	squareorangedecor.gif
1356	24corp-shop.com	image/gif	68 kB	notfound.gif
654	www.ciniholland.nl	image/jpeg	19 kB	P1260499-200x298.jpg
661	www.ciniholland.nl	image/jpeg	10 kB	IMG-20130928-WA002-150x150.jpg
976	www.ciniholland.nl	image/vnd.microsoft.icon	17 kB	favicon.ico
311	www.ciniholland.nl	text/css	927 bytes	styles.css?ver=3.7.2
314	www.ciniholland.nl	text/css	702 bytes	page-list.css?ver=4.2
340	www.ciniholland.nl	text/css	4807 bytes	style.css

Name	Date modified	Type
diameter	3/28/2024 10:21 AM	File folder
dtds	3/28/2024 10:22 AM	File folder
extcap	3/28/2024 10:22 AM	File folder
generic	3/28/2024 10:22 AM	File folder
iconengines	3/28/2024 10:22 AM	File folder
imageformats	3/28/2024 10:22 AM	File folder
multimedia	3/28/2024 10:22 AM	File folder
networkinformation	3/28/2024 10:22 AM	File folder
platforms	3/28/2024 10:22 AM	File folder
plugins	3/28/2024 10:22 AM	File folder
profiles	3/28/2024 10:22 AM	File folder

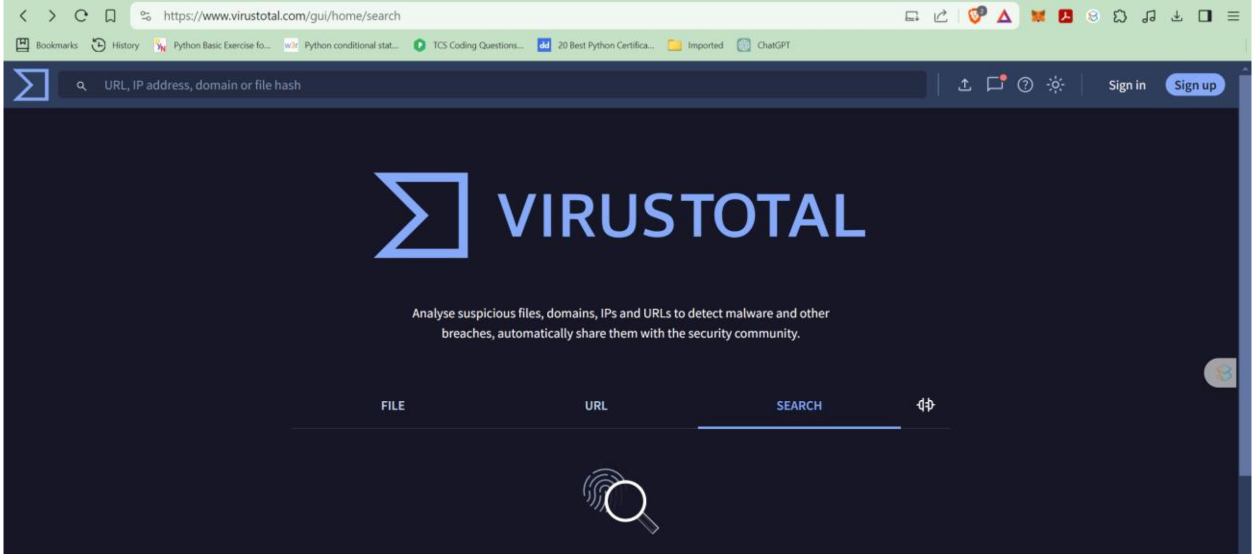
File name: DSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM

Save as type: All Files

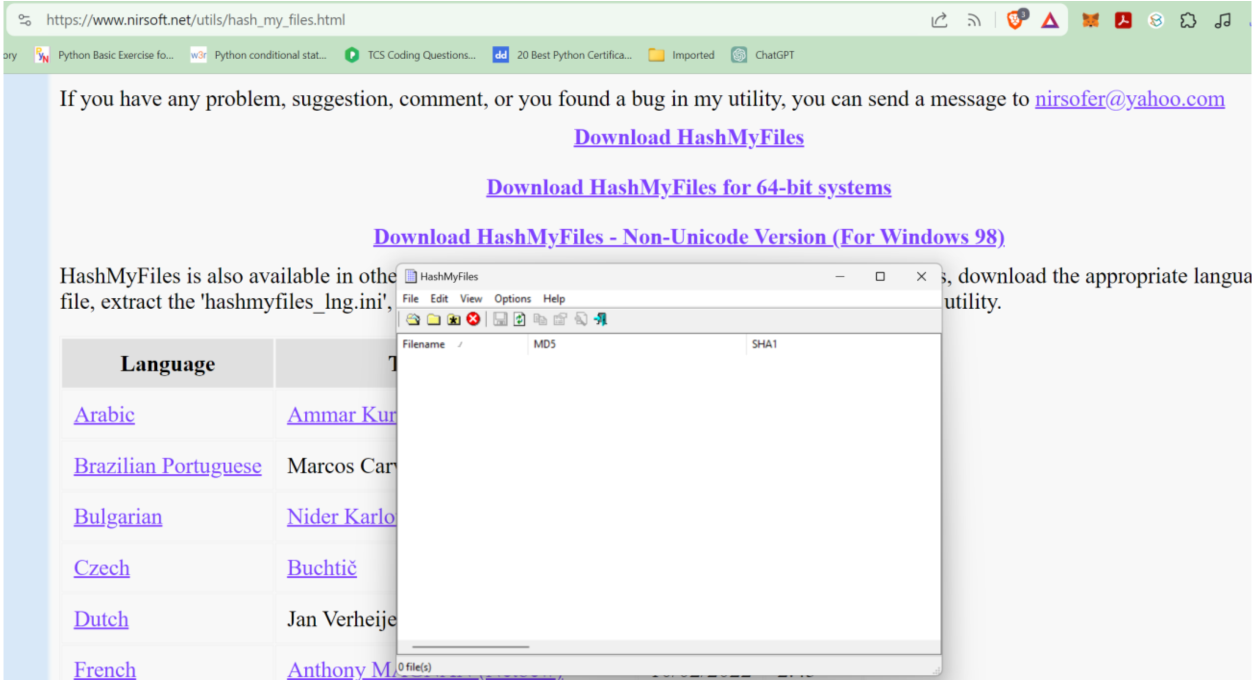


Name	Date modified	Type	Size
HashMyFiles.exe	5/15/2019 9:20 AM	Application	145 KB
index.php%3freq=mp3&num=16&PHPSSESID=njrMNruDMhvJFlPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM.exe	9/13/2019 11:31 PM	Application	393 KB
index.php%3freq=jar&num=3703&PHPSSESID=njrMNruDMhvJFlPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM.jar	9/13/2019 11:31 PM	JAR File	11 KB
index.php%3freq=swf&num=809&PHPSSESID=njrMNruDMhvJFlPGKuXDSKVbM07PThnJko2ahe6JVg%7cZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM.swf	9/13/2019 11:32 PM	Shockwave Flash ...	9 KB

We can directly upload the files to virus total but we avoid due to confidentiality, instead we find the hash of file and then check for malicious activity.


https://www.virustotal.com/gui/home/search
Bookmarks
History
Python Basic Exercise fo...
Python conditional stat...
TCS Coding Questions...
20 Best Python Certifica...
Imported
ChatGPT
URL, IP address, domain or file hash
Sign in
Sign up
VIRUSTOTAL
FILE
URL
SEARCH

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.



https://www.nirsoft.net/utils/hash_my_files.html
ory
Python Basic Exercise fo...
Python conditional stat...
TCS Coding Questions...
20 Best Python Certifica...
Imported
ChatGPT

If you have any problem, suggestion, comment, or you found a bug in my utility, you can send a message to nirsofer@yahoo.com

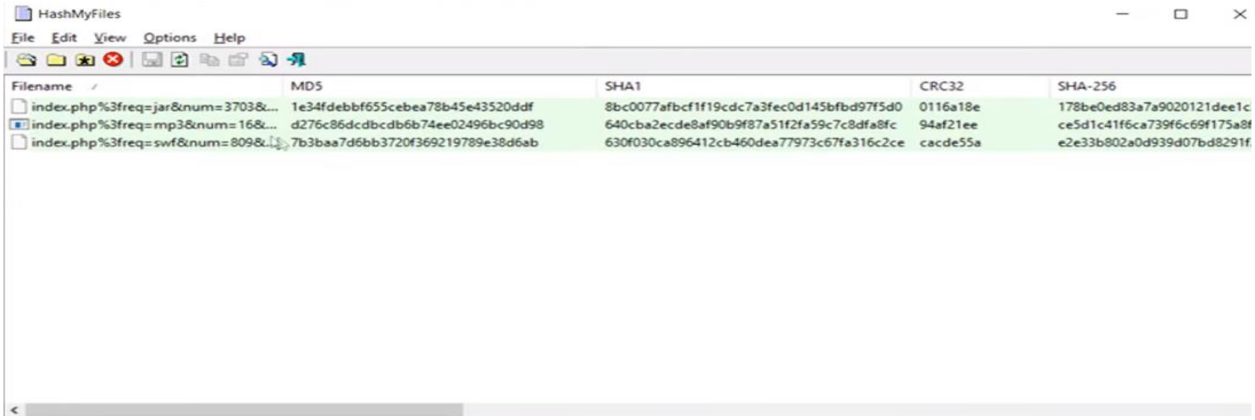
Download HashMyFiles

Download HashMyFiles for 64-bit systems

Download HashMyFiles - Non-Unicode Version (For Windows 98)

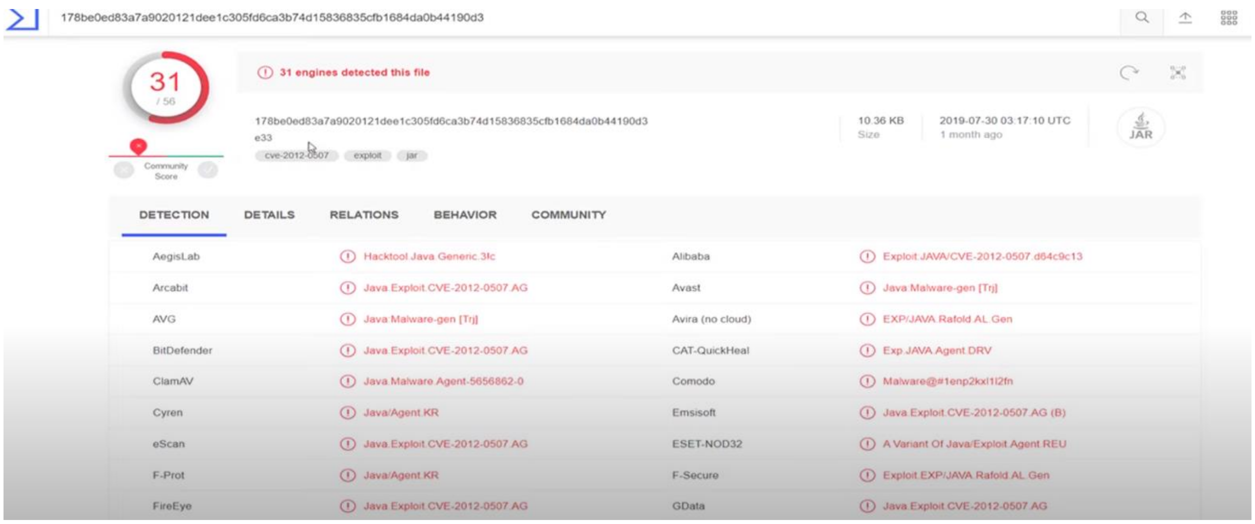
HashMyFiles is also available in othe… s, download the appropriate langua… file, extract the 'hashmyfiles_lng.ini', … utility.

Language	T
Arabic	Ammar Kur
Brazilian Portuguese	Marcos Car
Bulgarian	Nider Karlo
Czech	Buchtič
Dutch	Jan Verheije
French	Anthony M



Filename	MD5	SHA1	CRC32	SHA-256
index.php%3freq=jar&num=3703&...	1e34fdebbf655cebea78b45e43520ddf	8bc0077afbcf1f19cdc7a3fec0d145bfbd97f5d0	0116a18e	178be0ed83a7a9020121dee1c
index.php%3freq=mp3&num=16&...	d276c86dcdbcdb6b74ee02496bc90d98	640cba2ecde8af90b9f87a51f2fa59c7c8dfa8fc	94af21ee	ce5d1c41f6ca739f6c69f175a8f
index.php%3freq=swf&num=809&...	7b3baa7d6bb3720f369219789e38d6ab	630f030ca896412cb460dea77973c67fa316c2ce	cacde55a	e2e33b802a0d939d07bd8291f

Now, we checked the hash in virus total and found it infected.



178be0ed83a7a9020121dee1c305fd6ca3b74d15836835cfb1684da0b44190d3

31 / 56

31 engines detected this file

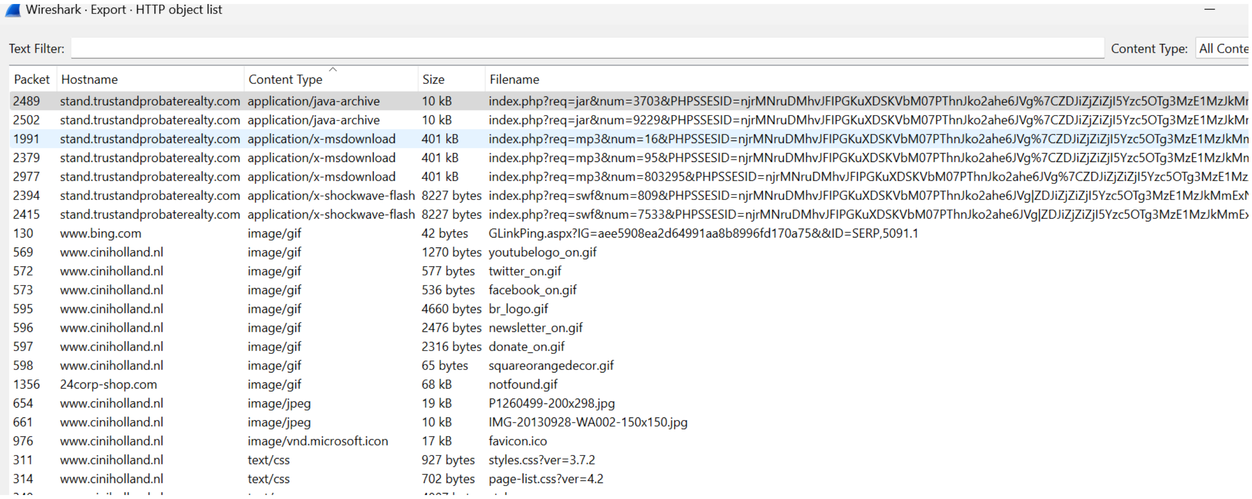
178be0ed83a7a9020121dee1c305fd6ca3b74d15836835cfb1684da0b44190d3
e33
cve-2012-0507 exploit jar

10.36 KB
Size

2019-07-30 03:17:10 UTC
1 month ago

AegisLab	Hacktool.Java.Generic.3!c	Alibaba	Exploit:JAVA/CVE-2012-0507.d64c9c13
Arcabit	Java.Exploit.CVE-2012-0507.AG	Avast	Java:Malware-gen [Trj]
AVG	Java:Malware-gen [Trj]	Avira (no cloud)	EXP/JAVA.Rafold.AL.Gen
BitDefender	Java.Exploit.CVE-2012-0507.AG	CAT-QuickHeal	Exp.JAVA.Agent.DRV
ClamAV	Java.Malware.Agent-5656862-0	Comodo	Malware@#1enp2kxl1l2fn
Cyren	Java/Agent.KR	Emsisoft	Java.Exploit.CVE-2012-0507.AG (B)
eScan	Java.Exploit.CVE-2012-0507.AG	ESET-NOD32	A Variant Of Java/Exploit.Agent.REU
F-Prot	Java/Agent.KR	F-Secure	Exploit.EXP/JAVA.Rafold.AL.Gen
FireEye	Java.Exploit.CVE-2012-0507.AG	GData	Java.Exploit.CVE-2012-0507.AG

2. What is URL/ Domain of the infected site?
   Answer: see the host name of infected file.
   stand.trustandprobaterealty.com



Wireshark · Export · HTTP object list

Text Filter: Content Type: All Conte

Packet	Hostname	Content Type	Size	Filename
2489	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=3703&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMr
2502	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=9229&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMr
1991	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=16&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMn
2379	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=95&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMn
2977	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=803295&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1Mz
2394	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=809&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN
2415	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=7533&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmEx
130	www.bing.com	image/gif	42 bytes	GLinkPing.aspx?IG=aee5908ea2d64991aa8b8996fd170a75&&ID=SERP,5091.1
569	www.ciniholland.nl	image/gif	1270 bytes	youtubelogo_on.gif
572	www.ciniholland.nl	image/gif	577 bytes	twitter_on.gif
573	www.ciniholland.nl	image/gif	536 bytes	facebook_on.gif
595	www.ciniholland.nl	image/gif	4660 bytes	br_logo.gif
596	www.ciniholland.nl	image/gif	2476 bytes	newsletter_on.gif
597	www.ciniholland.nl	image/gif	2316 bytes	donate_on.gif
598	www.ciniholland.nl	image/gif	65 bytes	squareorangedecor.gif
1356	24corp-shop.com	image/gif	68 kB	notfound.gif
654	www.ciniholland.nl	image/jpeg	19 kB	P1260499-200x298.jpg
661	www.ciniholland.nl	image/jpeg	10 kB	IMG-20130928-WA002-150x150.jpg
976	www.ciniholland.nl	image/vnd.microsoft.icon	17 kB	favicon.ico
311	www.ciniholland.nl	text/css	927 bytes	styles.css?ver=3.7.2
314	www.ciniholland.nl	text/css	702 bytes	page-list.css?ver=4.2

3. What is the IP address of the infected website?
   37.200.69.143

4. What is the IP address of the infected machine ?

   172.16.165.165

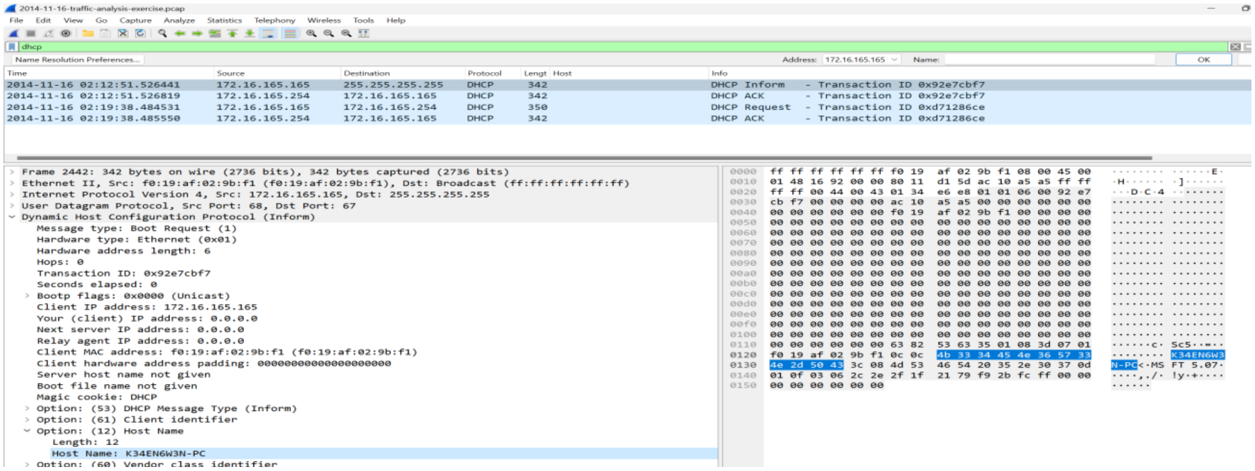
5. What is the hostname of the infected machine?

   K34EN6W3N-PC

6. What is the mac address of the infected machine ?

   f0:19:af:02:9b:f1

   Host name using DHCP:



2014-11-16-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Name Resolution Preferences...
OK

dhcp

Address: 172.16.165.165 Name:

Time	Source	Destination	Protocol	Lengt	Host	Info
2014-11-16 02:12:51.526441	172.16.165.165	255.255.255.255	DHCP	342		DHCP Inform - Transaction ID 0x92e7cbf7
2014-11-16 02:12:51.526819	172.16.165.254	172.16.165.165	DHCP	342		DHCP ACK - Transaction ID 0x92e7cbf7
2014-11-16 02:19:38.484531	172.16.165.165	172.16.165.254	DHCP	350		DHCP Request - Transaction ID 0xd71286ce
2014-11-16 02:19:38.485550	172.16.165.254	172.16.165.165	DHCP	342		DHCP ACK - Transaction ID 0xd71286ce

```
> Frame 2442: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.16.165.165, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Inform)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x92e7cbf7
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 172.16.165.165
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Inform)
  > Option: (61) Client identifier
  v Option: (12) Host Name
      Length: 12
      Host Name: K34EN6W3N-PC
  > Option: (60) Vendor class identifier
```

```
0000  ff ff ff ff ff ff f0 19  af 02 9b f1 08 00 45 00   ········ ······E·
0010  01 48 16 92 00 00 80 11  d1 5d ac 10 a5 a5 ff ff   ·H······ ·]······
0020  ff ff 00 44 00 43 01 34  e6 e8 01 01 06 00 92 e7   ···D·C·4 ········
0030  cb f7 00 00 00 00 ac 10  a5 a5 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 f0 19  af 02 9b f1 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 08 3d 07 01   ······c· Sc5··=··
0120  f0 19 af 02 9b f1 0c 0c  4b 33 34 45 4e 36 57 33   ········ K34EN6W3
0130  4e 2d 50 43 3c 08 4d 53  46 54 20 35 2e 30 37 0d   N-PC<·MS FT 5.07·
0140  01 0f 03 06 2c 2e 2f 1f  21 79 f9 2b fc ff 00 00   ····,./· !y·+····
0150  00 00 00 00 00 00                                  ······
```