

```
31 4.271211      155.4.140.82      194.9.94.85      HTTP      346      GET / HTTP/1.1
Frame 31: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface 0
Ethernet II, Src: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6), Dst: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f)
Internet Protocol Version 4, Src: 155.4.140.82, Dst: 194.9.94.85
Transmission Control Protocol, Src Port: 63204, Dst Port: 80, Seq: 1, Ack: 1, Len: 292
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
Accept-Language: sv-SE,sv;q=0.8,en-US;q=0.5,en;q=0.3\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; ASTE; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: mrolab.eu\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://mrolab.eu/]
[HTTP request 1/1]
[Response in frame: 32]
32 4.284247      194.9.94.85      155.4.140.82      HTTP      408      HTTP/1.1 302 Moved Temporarily (text/html)
Frame 32: 408 bytes on wire (3264 bits), 408 bytes captured (3264 bits) on interface 0
Ethernet II, Src: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f), Dst: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6)
Internet Protocol Version 4, Src: 194.9.94.85, Dst: 155.4.140.82
Transmission Control Protocol, Src Port: 80, Dst Port: 63204, Seq: 1, Ack: 293, Len: 354
Hypertext Transfer Protocol
HTTP/1.1 302 Moved Temporarily\r\n
Server: nginx/1.12.2\r\n
Date: Wed, 11 Apr 2018 05:33:54 GMT\r\n
Content-Type: text/html\r\n
Content-Length: 161\r\n
Connection: keep-alive\r\n
Location: http://mro.oru.se/\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.013036000 seconds]
[Request in frame: 31]
File Data: 161 bytes
Line-based text data: text/html
43 4.320396      155.4.140.82      130.243.109.196   HTTP      347      GET / HTTP/1.1
Frame 43: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface 0
Ethernet II, Src: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6), Dst: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f)
Internet Protocol Version 4, Src: 155.4.140.82, Dst: 130.243.109.196
Transmission Control Protocol, Src Port: 63206, Dst Port: 80, Seq: 1, Ack: 1, Len: 293
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
Accept-Language: sv-SE,sv;q=0.8,en-US;q=0.5,en;q=0.3\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; ASTE; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: Keep-Alive\r\n
Host: mro.oru.se\r\n
\r\n
[Full request URI: http://mro.oru.se/]
[HTTP request 1/1]
[Response in frame: 57]
57 6.977143      130.243.109.196   155.4.140.82      HTTP      303      HTTP/1.1 301 Moved Permanently
Frame 57: 303 bytes on wire (2424 bits), 303 bytes captured (2424 bits) on interface 0
Ethernet II, Src: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f), Dst: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6)
Internet Protocol Version 4, Src: 130.243.109.196, Dst: 155.4.140.82
Transmission Control Protocol, Src Port: 80, Dst Port: 63206, Seq: 1, Ack: 294, Len: 249
Hypertext Transfer Protocol
HTTP/1.1 301 Moved Permanently\r\n
Date: Wed, 11 Apr 2018 05:33:51 GMT\r\n
Server: Apache/2.4.10 (Debian)\r\n
Location: https://mro.oru.se/\r\n
Content-Length: 0\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 2.656747000 seconds]
[Request in frame: 43]
74 7.064786      155.4.140.82      79.136.61.40      HTTP      302      GET /
MFEwTzBNMEswSTAJBgUrDgMCGGUABBRv9GhNQxLSSGKBnMARPUcsHYovpgQUxKexpHsscfrb4UuQdf%2FEFWCFiRACEAoBQUIAAAFThXNqC4Xspwg%3D HTTP/1.1
Frame 74: 302 bytes on wire (2416 bits), 302 bytes captured (2416 bits) on interface 0
Ethernet II, Src: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6), Dst: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f)
Internet Protocol Version 4, Src: 155.4.140.82, Dst: 79.136.61.40
Transmission Control Protocol, Src Port: 63208, Dst Port: 80, Seq: 1, Ack: 1, Len: 248
Hypertext Transfer Protocol
GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBRv9GhNQxLSSGKBnMARPUcsHYovpgQUxKexpHsscfrb4UuQdf%2FEFWCFiRACEAoBQUIAAAFThXNqC4Xspwg%3D HTTP/1.1\r\n
```

```
Connection: Keep-Alive\r\n
Accept: */*\r\n
User-Agent: Microsoft-CryptoAPI/10.0\r\n
Host: isrg.trustid.ocsp.identrust.com\r\n
\r\n
[Full request URI: http://isrg.trustid.ocsp.identrust.com/
MFEwTzBNMEswSTAJBgUrDgMCGGUABBRv9GhNQxLSSGKBnMARPUcsHYovpgQUxKexpHsscfrb4UuQdf%2FEFWCFiRACEAoBQUIAAAFThXNqC4Xspwg%3D]
[HTTP request 1/1]
[Response in frame: 77]
  77 7.069937      79.136.61.40      155.4.140.82      OCSP      374      Response
Frame 77: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface 0
Ethernet II, Src: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f), Dst: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6)
Internet Protocol Version 4, Src: 79.136.61.40, Dst: 155.4.140.82
Transmission Control Protocol, Src Port: 80, Dst Port: 63208, Seq: 1461, Ack: 249, Len: 320
[2 Reassembled TCP Segments (1780 bytes): #76(1460), #77(320)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Content-transfer-encoding: Binary\r\n
Last-Modified: Sun, 08 Apr 2018 00:08:57 GMT\r\n
ETag: "da80c39672a8657a632e964374a1bb5df27df4c9"\r\n
Content-Type: application/ocsp-response\r\n
Content-Length: 1398\r\n
Cache-Control: public, no-transform, must-revalidate, max-age=6668\r\n
Expires: Wed, 11 Apr 2018 07:25:05 GMT\r\n
Date: Wed, 11 Apr 2018 05:33:57 GMT\r\n
Connection: keep-alive\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.005151000 seconds]
[Request in frame: 74]
File Data: 1398 bytes
Online Certificate Status Protocol
  307 7.506081      155.4.140.82      130.243.109.196      HTTP      419      GET /wp-content/uploads/Publications/
Featured_Articles/husky.png HTTP/1.1
Frame 307: 419 bytes on wire (3352 bits), 419 bytes captured (3352 bits) on interface 0
Ethernet II, Src: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6), Dst: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f)
Internet Protocol Version 4, Src: 155.4.140.82, Dst: 130.243.109.196
Transmission Control Protocol, Src Port: 63218, Dst Port: 80, Seq: 1, Ack: 1, Len: 365
Hypertext Transfer Protocol
GET /wp-content/uploads/Publications/Featured_Articles/husky.png HTTP/1.1\r\n
Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5\r\n
Accept-Language: sv-SE,sv;q=0.8,en-US;q=0.5,en;q=0.3\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; ASTE; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: mro.oru.se\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://mro.oru.se/wp-content/uploads/Publications/Featured_Articles/husky.png]
[HTTP request 1/1]
  309 7.512318      155.4.140.82      130.243.109.196      HTTP      429      GET /wp-content/uploads/Publications/
Featured_Articles/1070541-150x150.jpg HTTP/1.1
Frame 309: 429 bytes on wire (3432 bits), 429 bytes captured (3432 bits) on interface 0
Ethernet II, Src: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6), Dst: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f)
Internet Protocol Version 4, Src: 155.4.140.82, Dst: 130.243.109.196
Transmission Control Protocol, Src Port: 63219, Dst Port: 80, Seq: 1, Ack: 1, Len: 375
Hypertext Transfer Protocol
GET /wp-content/uploads/Publications/Featured_Articles/1070541-150x150.jpg HTTP/1.1\r\n
Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5\r\n
Accept-Language: sv-SE,sv;q=0.8,en-US;q=0.5,en;q=0.3\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; ASTE; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: mro.oru.se\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://mro.oru.se/wp-content/uploads/Publications/Featured_Articles/1070541-150x150.jpg]
[HTTP request 1/1]
[Response in frame: 678]
  325 7.520879      155.4.140.82      130.243.109.196      HTTP      429      GET /wp-content/uploads/Publications/
Featured_Articles/1044252-150x150.jpg HTTP/1.1
Frame 325: 429 bytes on wire (3432 bits), 429 bytes captured (3432 bits) on interface 0
Ethernet II, Src: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6), Dst: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f)
Internet Protocol Version 4, Src: 155.4.140.82, Dst: 130.243.109.196
Transmission Control Protocol, Src Port: 63220, Dst Port: 80, Seq: 1, Ack: 1, Len: 375
Hypertext Transfer Protocol
GET /wp-content/uploads/Publications/Featured_Articles/1044252-150x150.jpg HTTP/1.1\r\n
Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5\r\n
Accept-Language: sv-SE,sv;q=0.8,en-US;q=0.5,en;q=0.3\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; ASTE; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: mro.oru.se\r\n
```

```
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://mro.oru.se/wp-content/uploads/Publications/Featured_Articles/1044252-150x150.jpg]
[HTTP request 1/1]
[Response in frame: 693]
326 7.526848      155.4.140.82      216.58.211.142      HTTP      279      GET /GTSGIAG3/
MEkwrZBFMEMwQTAJBgUrDgMCGGUABBT27bYjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCA8t0Jw6gcvg HTTP/1.1
Frame 326: 279 bytes on wire (2232 bits), 279 bytes captured (2232 bits) on interface 0
Ethernet II, Src: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6), Dst: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f)
Internet Protocol Version 4, Src: 155.4.140.82, Dst: 216.58.211.142
Transmission Control Protocol, Src Port: 63221, Dst Port: 80, Seq: 1, Ack: 1, Len: 225
Hypertext Transfer Protocol
GET /GTSGIAG3/MEkwrZBFMEMwQTAJBgUrDgMCGGUABBT27bYjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCA8t0Jw6gcvg HTTP/1.1\r\n
Connection: Keep-Alive\r\n
Accept: */*\r\n
User-Agent: Microsoft-CryptoAPI/10.0\r\n
Host: ocsf.pki.goog\r\n
\r\n
[Full request URI: http://ocsf.pki.goog/GTSGIAG3/MEkwrZBFMEMwQTAJBgUrDgMCGGUABBT27bYjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCA8t0Jw6gcvg]
[HTTP request 1/1]
[Response in frame: 330]
330 7.530722      216.58.211.142      155.4.140.82      OCSP      773      Response
Frame 330: 773 bytes on wire (6184 bits), 773 bytes captured (6184 bits) on interface 0
Ethernet II, Src: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f), Dst: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6)
Internet Protocol Version 4, Src: 216.58.211.142, Dst: 155.4.140.82
Transmission Control Protocol, Src Port: 80, Dst Port: 63221, Seq: 1, Ack: 226, Len: 719
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Content-Type: application/ocsp-response\r\n
Date: Sat, 07 Apr 2018 23:54:23 GMT\r\n
Server: ocsf_responder\r\n
Content-Length: 463\r\n
X-XSS-Protection: 1; mode=block\r\n
X-Frame-Options: SAMEORIGIN\r\n
Cache-Control: public, max-age=345600\r\n
Age: 279574\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.003874000 seconds]
[Request in frame: 326]
File Data: 463 bytes
Online Certificate Status Protocol
557 7.745641      155.4.140.82      23.46.123.27      HTTP      280      GET /
MFEwTzBNMEswSTAJBgUrDgMCGGUABBSxtDkXkBa3l3lQEffgudSiPNvt7gQUAPkqw0GRtsnCuD5V8sCXER0gByACEAEAIswIsPpZp3fvBXtmJ98%3D HTTP/1.1
Frame 557: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface 0
Ethernet II, Src: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6), Dst: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f)
Internet Protocol Version 4, Src: 155.4.140.82, Dst: 23.46.123.27
Transmission Control Protocol, Src Port: 63225, Dst Port: 80, Seq: 1, Ack: 1, Len: 226
Hypertext Transfer Protocol
GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBSxtDkXkBa3l3lQEffgudSiPNvt7gQUAPkqw0GRtsnCuD5V8sCXER0gByACEAEAIswIsPpZp3fvBXtmJ98%3D HTTP/1.1\r\n
Connection: Keep-Alive\r\n
Accept: */*\r\n
User-Agent: Microsoft-CryptoAPI/10.0\r\n
Host: g.symcd.com\r\n
\r\n
[Full request URI: http://g.symcd.com/
MFEwTzBNMEswSTAJBgUrDgMCGGUABBSxtDkXkBa3l3lQEffgudSiPNvt7gQUAPkqw0GRtsnCuD5V8sCXER0gByACEAEAIswIsPpZp3fvBXtmJ98%3D]
[HTTP request 1/1]
[Response in frame: 560]
560 7.750028      23.46.123.27      155.4.140.82      OCSP      340      Response
Frame 560: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface 0
Ethernet II, Src: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f), Dst: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6)
Internet Protocol Version 4, Src: 23.46.123.27, Dst: 155.4.140.82
Transmission Control Protocol, Src Port: 80, Dst Port: 63225, Seq: 1461, Ack: 227, Len: 286
[2 Reassembled TCP Segments (1746 bytes): #559(1460), #560(286)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Server: nginx/1.12.2\r\n
Content-Type: application/ocsp-response\r\n
Content-Length: 1391\r\n
content-transfer-encoding: binary\r\n
Cache-Control: max-age=493850, public, no-transform, must-revalidate\r\n
Last-Modified: Mon, 9 Apr 2018 22:43:16 GMT\r\n
Expires: Mon, 16 Apr 2018 22:43:16 GMT\r\n
Date: Wed, 11 Apr 2018 05:33:57 GMT\r\n
Connection: keep-alive\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.004387000 seconds]
```

```
[Request in frame: 557]
File Data: 1391 bytes
Online Certificate Status Protocol
 567 7.788288      155.4.140.82      216.58.211.142      HTTP      285      GET /ocsp/
MEKwRzBFMEMwQTAJBgUrdGMCgGUABBTy4Gr5hYodjXCbSRkjeqm1Gih%2BZAQUST0GFhu89mi1dvWBtrtiGrpagS8CCDdf%2FhH14xa%2B HTTP/1.1
Frame 567: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits) on interface 0
Ethernet II, Src: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6), Dst: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f)
Internet Protocol Version 4, Src: 155.4.140.82, Dst: 216.58.211.142
Transmission Control Protocol, Src Port: 63226, Dst Port: 80, Seq: 1, Ack: 1, Len: 231
Hypertext Transfer Protocol
GET /ocsp/MEKwRzBFMEMwQTAJBgUrdGMCgGUABBTy4Gr5hYodjXCbSRkjeqm1Gih%2BZAQUST0GFhu89mi1dvWBtrtiGrpagS8CCDdf%2FhH14xa%2B HTTP/1.1\r\n
Connection: Keep-Alive\r\n
Accept: */*\r\n
User-Agent: Microsoft-CryptoAPI/10.0\r\n
Host: clients1.google.com\r\n
\r\n
[Full request URI: http://clients1.google.com/ocsp/MEKwRzBFMEMwQTAJBgUrdGMCgGUABBTy4Gr5hYodjXCbSRkjeqm1Gih
%2BZAQUST0GFhu89mi1dvWBtrtiGrpagS8CCDdf%2FhH14xa%2B]
[HTTP request 1/1]
[Response in frame: 569]
 569 7.792436      216.58.211.142      155.4.140.82      OCSP      773      Response
Frame 569: 773 bytes on wire (6184 bits), 773 bytes captured (6184 bits) on interface 0
Ethernet II, Src: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f), Dst: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6)
Internet Protocol Version 4, Src: 216.58.211.142, Dst: 155.4.140.82
Transmission Control Protocol, Src Port: 80, Dst Port: 63226, Seq: 1, Ack: 232, Len: 719
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Content-Type: application/ocsp-response\r\n
Date: Sun, 08 Apr 2018 01:12:22 GMT\r\n
Server: ocsp_responder\r\n
Content-Length: 463\r\n
X-XSS-Protection: 1; mode=block\r\n
X-Frame-Options: SAMEORIGIN\r\n
Cache-Control: public, max-age=345600\r\n
Age: 274895\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.004148000 seconds]
[Request in frame: 567]
File Data: 463 bytes
Online Certificate Status Protocol
 678 7.838677      130.243.109.196      155.4.140.82      HTTP      1140      HTTP/1.1 200 OK (JPEG JFIF image)
Frame 678: 1140 bytes on wire (9120 bits), 1140 bytes captured (9120 bits) on interface 0
Ethernet II, Src: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f), Dst: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6)
Internet Protocol Version 4, Src: 130.243.109.196, Dst: 155.4.140.82
Transmission Control Protocol, Src Port: 80, Dst Port: 63219, Seq: 5841, Ack: 376, Len: 1086
[5 Reassembled TCP Segments (6926 bytes): #671(1460), #672(1460), #674(1460), #676(1460), #678(1086)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Wed, 11 Apr 2018 05:33:55 GMT\r\n
Server: Apache/2.4.10 (Debian)\r\n
Last-Modified: Fri, 03 Mar 2017 13:40:52 GMT\r\n
ETag: "19ee-549d3b1c29e9f"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 6638\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: image/jpeg\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.326359000 seconds]
[Request in frame: 309]
File Data: 6638 bytes
JPEG File Interchange Format
 693 8.851256      130.243.109.196      155.4.140.82      HTTP      1218      HTTP/1.1 200 OK (JPEG JFIF image)
Frame 693: 1218 bytes on wire (9744 bits), 1218 bytes captured (9744 bits) on interface 0
Ethernet II, Src: Cisco_ff:e8:3f (00:a2:ee:ff:e8:3f), Dst: AsustekC_72:3f:a6 (2c:56:dc:72:3f:a6)
Internet Protocol Version 4, Src: 130.243.109.196, Dst: 155.4.140.82
Transmission Control Protocol, Src Port: 80, Dst Port: 63220, Seq: 4381, Ack: 376, Len: 1164
[4 Reassembled TCP Segments (5544 bytes): #687(1460), #689(1460), #691(1460), #693(1164)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Wed, 11 Apr 2018 05:33:56 GMT\r\n
Server: Apache/2.4.10 (Debian)\r\n
Last-Modified: Fri, 03 Mar 2017 14:03:12 GMT\r\n
ETag: "1488-549d4019c7a85"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 5256\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
```

Content-Type: image/jpeg\r\n

\r\n

[HTTP response 1/1]

```
[Time since request: 1.330377000 seconds]
```

```
[Request in frame: 325]
```

File Data: 5256 bytes

JPEG File Interchange Format