AskApache Web DevelopmentFREE THOUGHT · FREE SOFTWARE · FREE WORLD(http://www.fsf.org/register_form?referrer=7511)

- Skip

Home » Software » HTTP Packet Capturing to debug Apache

HTTP Packet Capturing to debug Apache

« Port RedirectorSpeed Up Sites with php Caching »

by Charles Torvalds3 Comments

This article is a quick and easy HowTo detailing the use of Wireshark(http://wireshark.askapache.com) or another network sniffing program to debug your Apache .htaccess or httpd.conf files.

First some shell based tools.

```
wget -S --spider URL lynx -head -dump URL curl -I URL HEAD URL GET -de URL w3m -dump_head
URL siege -g URL
```

Contents [hide]

> Set Your Capture-filter to `tcp port 80` and then start capturing. Use any of the following display filters to view the data you want.

Display Filters ^

HTTP Display Filter Options ^

- http.accept String Accept
- http.accept_encoding String Accept Encoding
- http.accept_language String Accept-Language
- http.authbasic String Credentials
- http.authorization String Authorization
- http.cache_control String Cache-Control
- http.connection String Connection
- http.content_encoding String Content-Encoding
- http.content_length Unsigned 32-bit integer Content-Length
- http.content_type String Content-Type
- http.cookie String Cookie
- http.date String Date
- http.host String Host
- http.last_modified String Last-Modified
- http.location String Location
- http.notification Boolean Notification
- http.proxy_authenticate String Proxy-Authenticate
- http.proxy_authorization String Proxy-Authorization
- http.referer String Referer
- http.request Boolean Request
- http.request.method String Request Method
- http.request.uri String Request URI
- http.request.version String Request Version
- http.response Boolean Response
- http.response.code Unsigned 16-bit integer Response Code
- http.server String Server
- http.set_cookie String Set-Cookie
- http.transfer_encoding String Transfer-Encoding
- http.user_agent String User-Agent
- http.www_authenticate String WWW-Authenticate
- http.x_forwarded_for String X-Forwarded-For

View All HTTP trafic ^

```
http
```

View all flash video stuff ^

```
http.request.uri contains "flv" or http.request.uri contains "swf" or http.content_type contains "fl
```

Show non-google cache-control ^

```
http.cache_control != "private, x-gzip-ok="""
```

or

```
(((((http.cache_control != "private, x-gzip-ok=""") && !(http.cache_control == "no-cache, no-store,
```

Show only certain responses ^

```
#404: page not found
http.response.code == 404

#200: OK
http.response.code == 200
```

Show only certain HTTP methods ^

```
http.request.method == "POST" || http.request.method == "PUT"
```

Show only filetypes that begin with "text" ^

```
http.content_type[0:4] == "text"
```

Show only javascript ^

```
http.content_type contains "javascript"
```

Show all http with content-type="image/(gif|jpeg|png|etc)" ^

```
http.content_type[0:5] == "image"
```

Show all http with content-type="image/gif" ^

```
http.content_type == "image/gif"
```

Do not show content http, only headers ^

```
http.response !=0 || http.request.method != "TRACE"
```

Setting HTTP Preferences ^

Reassemble HTTP headers spanning multiple TCP segments: ^

When this preference is enabled, then the HTTP dissector will reassemble the HTTP header if it has been transmitted over more than one TCP segment. Although it is unusual for headers span multiple segments, it's not impossible, and this should be checked if you expect to view the contents of the HTTP conversation.

Reassemble HTTP bodies spanning multiple TCP segments: ^

When this preference is enabled, then the HTTP dissector will reassemble the HTTP body if it has been transmitted over more than one TCP segment. All but the smallest of responses will span multiple segments, so this preference should be checked if you expect to view the contents of the HTTP conversation.See TCP Reassembly for an example on how to use this to extract JPEG images from a capture.

Reassemble chunked transfer-coded bodies: ^

When this preference is enabled, any chunked transfer-coding response spanning multiple segments will be decoded and the payload (the body of the response) will be added to the protocol tree. This happens automatically for one segment responses.

Uncompress entity bodies: ^

Enable this preference if gzip or deflate encoded (compressed) HTTP entities should be decoded. This allows the visualisation of the compressed data, and possibly the dissection of it.

Tags ^

January 23rd, 2007

« Port RedirectorSpeed Up Sites with php Caching »

Comments Welcome ^

[hide]