http.log | HTTP request/reply details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the HTTP request
uid & id		Underlying connection info > **See conn.log**
trans_depth	count	Pipelined depth into the connection
method	string	HTTP Request verb: GET, POST, HEAD, etc
host	string	Value of the Host header
uri	string	URI used in the request
referrer	string	Value of the “Referer” header
user_agent	string	Value of the User-Agent header
request_body_len	count	Uncompressed content size of Orig data
response_body_len	count	Uncompressed content size of Resp data
status_code	count	Status code returned by the server
status_msg	string	Status message returned by the server
info_code	count	Last seen 1xx info reply code by server
info_msg	string	Last seen 1xx info reply message by server
tags	set	Indicators of various attributes discovered
username	string	Username if basic-auth is performed
password	string	Password if basic-auth is performed
proxied	set	Headers indicative of a proxied request
orig_fuids	vector	File unique IDs from Orig
orig_filenames	vector	File names from Orig
orig_mime_types	vector	File types from Orig
resp_fuids	vector	File unique IDs from Resp
resp_filenames	vector	File names from Resp
resp_mime_types	vector	File types from Resp
client_header_names[1]	vector	The names of HTTP headers sent by Orig
server_header_names[1]	vector	The names of HTTP headers sent by Resp
cookie_vars[2]	vector	Variable names extracted from cookies
uri_vars[2]	vector	Variable names extracted from the URI

[1] *If policy/protocols/http/header-names.bro is loaded*

[2] *If policy/protocols/http/var-extraction-uri.bro is loaded*