

Top 50 acronyms in the world of HTTP(s) proxy debugging

Whether you need an intro or quick refresher, the Fiddler team put together a list of commonly used acronyms encountered in the world of HTTP(s) proxy debugging.

CHEAT SHEET



ADB (Android Debug Bridge)

Android Debug Bridge (adb) is a versatile command-line tool that lets you communicate with a device. The adb command facilitates a variety of device actions, such as installing and debugging apps, and it provides access to a Unix shell that you can use to run a variety of commands on a device.

developer.android.com/studio/command-line/adb

API (Application Programming Interface)

An application programming interface (‘API’) is a computing interface that defines interactions between multiple software intermediaries. It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow, etc.

en.wikipedia.org/wiki/API

CA (Certificate Authorities)

A certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.

en.wikipedia.org/wiki/Certificate_authority

CARP (Cache Array Routing Protocol)

The Cache Array Routing Protocol (CARP) is a standard proposed by Microsoft Corporation and Netscape Communication Corporation to administer a collection of proxy servers such that an array of proxy servers appears to clients as on logical cache.

HTTP: The Definitive Guide: The Definitive Guide (Definitive Guides) 1st Edition by [David Gourley](#) (Author), [Brian Totty](#) (Author), [Marjorie Sayer](#) (Author), [Anshu Aggarwal](#) (Author), [Sailu Reddy](#) (Author)

CGI (Common Gateway Interface)

Common Gateway Interface (CGI) is an interface specification for web servers to execute programs like console applications (also called command-line interface programs) running on a server that generates web pages dynamically.

en.wikipedia.org/wiki/Common_Gateway_Interface

CURL (Client URL)

cURL is a computer software project providing a library (libcurl) and command-line tool (curl) for transferring data using various network protocols. The name stands for ‘Client URL’, which was first released in 1997.

en.wikipedia.org/wiki/CURL

DER (Distinguished Encoding Rules)

DER is a binary format of encoding a data value of any data types including nested data structures.

www.herongyang.com/Cryptography/Certificate-Format-DER-Distinguished-Encoding-Rules.html

DHCP (Dynamic Host Configuration Protocol)

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks, whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on the network, so they can communicate with other IP networks.

en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

DNS (Domain Name System)

The Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

en.wikipedia.org/wiki/Domain_Name_System

EAP (Extensible Authentication Protocol)

The Extensible Authentication Protocol is an authentication framework frequently used in network and internet connections. It is defined in RFC 3748, which made 4 obsolete, and is updated by RFC 5247. EAP is an authentication framework for providing the transport and usage of material and parameters generated by EAP methods.

en.wikipedia.org/wiki/Extensible_Authentication_Protocol

FPSE (FrontPage Server Extensions)

FrontPage Server Extensions are a software technology that allows FrontPage clients to communicate with web servers, and provide additional functionality intended for websites. Frequent security problems have marred the history of this Microsoft proprietary technology. It relies on HTTP protocol for communication, and CGI/POST for server-side processing.

en.wikipedia.org/wiki/Microsoft_FrontPage

gRPC (Google Remote Procedure Call)

gRPC is an open-source remote procedure call (RPC) system initially developed at Google in 2015. It uses HTTP/2 for transport, Protocol Buffers as the interface description language, and provides features such as authentication, bidirectional streaming, and flow control, blocking or nonblocking bindings, and cancellation and timeouts. It generates cross-platform client and server bindings for many languages.

en.wikipedia.org/wiki/gRPC

HAR (HTTP Archive)

The HTTP Archive format is a JSON-formatted archive file format for logging of a web browser's interaction with a site. The format defines an archival format for HTTP transactions that can be used by a web browser to export detailed performance data about web pages it loads.

en.wikipedia.org/wiki/HAR_file_format

HTPC (Hypertext Caching Protocol)

Hypertext Caching Protocol is used for discovering HTTP caches and cached data, managing sets of HTTP caches and monitoring cache activity. It permits full request and response headers to be

used in cache management and expands the domain of cache management to include monitoring a remote cache's additions and deletions, requesting immediate deletions and sending hints about web objects such as the third-party locations of cacheable objects or unavailability of web objects.

en.wikipedia.org/wiki/Hypertext_caching_protocol

HTTP (Hypertext Transfer Protocol)

The Hypertext Transfer Protocol is an application layer protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

HTTPS (Hypertext Transfer Protocol Secure)

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL).

en.wikipedia.org/wiki/HTTPS

IANA (Internet Assigned Number Authority)

IANA is a standards organization that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and Internet numbers.

en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority

ICP (Internet Cache Protocol)

The Internet Cache Protocol is a UDP-based protocol used for coordinating web caches. Its purpose is to find out the most appropriate location to retrieve a requested object in the situation where multiple caches are in use at a single site. The ICP is to use the caches as efficiently as possible, and to minimize the number of remote requests to the originating server.

en.wikipedia.org/wiki/Internet_Cache_Protocol

IETF (The Internet Engineering Task Force)

The Internet Engineering Task Force is the leading Internet standards body. It develops open standards through open processes with one goal in mind: to make the Internet work better.

www.internetsociety.org/about-the-ietf/

IPsec (Internet Protocol Security)

Internet Protocol Security is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks.

en.wikipedia.org/wiki/IPsec

JSON (JavaScript Object Notation)

JSON is an open standard file format, and data interchange format, that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and array data types (or any other serializable value). It is a very common data format, with a diverse range of applications.

en.wikipedia.org/wiki/JSON

LAN (Local Area Network)

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

en.wikipedia.org/wiki/Local_area_network

MAC (Media Access Control)

The medium access control sublayer is the layer that controls the hardware responsible for interaction with the wired, optical, or wireless transmission medium. The MAC sublayer and the logical link control (LLC) sublayer together make up the data link layer.

en.wikipedia.org/wiki/Medium_access_control

MIME (Multipurpose Internet Mail Extensions)

The Multipurpose Internet Mail Extensions is an Internet standard that extends the format of email messages to support text in character sets other than ASCII, as well as attachments of audio, video, images, and application programs. Message bodies may consist of multiple parts, and header information may be specified in non-ASCII character sets.

en.wikipedia.org/wiki/MIME

MITM Proxy (Man-in-the middle)

MITM Proxy is used to intercept, inspect, modify and replay web traffic such as HTTP/2, HTTPS, WebSockets or any other SSL/TLS-protected passwords.

saraswatisrepository.com/tech/what-is-mitm-how-to-intercept-https-traffic-using-mitm-proxy/

NECP (Network Element Control Protocol)

The Network Element Control Panel allows network elements—devices such as routers and switches that forward IP packets to talk with server elements—devices such as web servers and proxy caches that serve application layer requests.

HTTP: The Definitive Guide: The Definitive Guide (Definitive Guides) 1st Edition by [David Gourley](#) (Author), [Brian Totty](#) (Author), [Marjorie Sayer](#) (Author), [Anshu Aggarwal](#) (Author), [Sailu Reddy](#) (Author)

NIO (Non-blocking I/O)

Non-blocking I/O is a collection of Java programming language APIs that offer features for intensive I/O operations. It was introduced with the J2SE 1.4 release of Java by Sun Microsystems to complement an existing standard I/O.

[en.wikipedia.org/wiki/Non-blocking_I/O_\(Java\)](https://en.wikipedia.org/wiki/Non-blocking_I/O_(Java))

NSURL (NextStep Uniform Resource Locator)

An NSURL object is composed of two parts—a potentially nil base URL and a string that is resolved relative to the base URL. An NSURL object is considered absolute if its string part is fully resolved without a base; all other URLs are considered relative.

developer.apple.com/documentation/foundation/nsurl

OSI Model (Open Systems Interconnection)

The Open Systems Interconnection model (OSI model) is a conceptual model that characterises and standardises the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology.

en.wikipedia.org/wiki/OSI_model

PAC (Proxy Auto-Configuration)

A proxy auto-config file defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL.

en.wikipedia.org/wiki/Proxy_auto-config

PEM (Privacy-Enhanced Mail)

Privacy-Enhanced Mail (PEM) is a de facto file format for storing and sending cryptographic keys, certificates, and other data, based on a set of 1993 IETF standards defining “privacy-enhanced mail.”

en.wikipedia.org/wiki/Privacy-Enhanced_Mail

PKCS (Public Key Cryptography Standards)

These are a group of public-key cryptography standards devised and published by RSA Security LLC, starting in the early 1990s. The company published the standards to promote the use of the cryptography techniques to which they had patents, such as the RSA algorithm, the Schnorr signature algorithm and several others.

en.wikipedia.org/wiki/PKCS

PURL (Personalized Uniform Resource Locator)

A persistent uniform resource locator is a uniform resource locator (URL) (i.e., location-based uniform resource identifier or URI) that is used to redirect to the location of the requested web resource. PURLs redirect HTTP clients using HTTP status codes.

en.wikipedia.org/wiki/Persistent_uniform_resource_locator

RPC (Remote Procedure Call)

A remote procedure call is when a computer program causes a procedure (subroutine) to execute in a different address space (commonly on another computer on a shared network), which is coded as if it were a normal (local) procedure call, without the programmer explicitly coding the details for the remote interaction.

en.wikipedia.org/wiki/Remote_procedure_call

RSA (Rivest-Shamir-Adleman)

RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977.

[en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

SAZ Session Archive Zip

(Fiddler coined this acronym) Session Archive Zip (SAZ) files are used to store HTTP(S) traffic for later examination.

SHA-2 (Secure Hash Algorithm 2)

Secure Hash Algorithm 2 is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001.[3][4] They are built using the Merkle–Damgård construction, from a one-way compression function itself built using the Davies–Meyer structure from a specialized block cipher.

en.wikipedia.org/wiki/SHA-2

SSL (Secure Sockets Layer)

Secure Sockets Layer (SSL) is a protocol developed by Netscape for providing a secure connection between two or more devices via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data a public key known to everyone and a private or secret key known only to the recipient of the message.

www.webopedia.com/definitions/ssl/

TCP (Transmission Control Protocol)

The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network.

en.wikipedia.org/wiki/Transmission_Control_Protocol

TLS (Transport Layer Security)

Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols are widely used in applications such as email, instant messaging, and voice over IP, but its use as the Security layer in HTTPS remains the most publicly visible.

en.wikipedia.org/wiki/Transport_Layer_Security

UDP User Datagram Protocol

With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network.

en.wikipedia.org/wiki/User_Datagram_Protocol

URI (Uniform Resource Identifier)

A Uniform Resource Identifier (URI) is a unique identifier used by web technologies. URIs may be used to identify anything, including real-world objects, such as people and places, concepts, or information resources such as web pages and books. Some URIs provide a means of locating and retrieving information resources on a network (either on the Internet or on another private network, such as a computer filesystem or an Intranet), these are Uniform Resource Locators (URLs).

en.wikipedia.org/wiki/Uniform_Resource_Identifier

URL (Uniform Resource Locator)

A Uniform Resource Locator colloquially termed a web address, as a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A URL is a specific type of Uniform Resource Identifier (URI), although many people use the two terms interchangeably.

en.wikipedia.org/wiki/URL

URN (Uniform Resource Name)

A Uniform Resource Name is a Uniform Resource Identifier (URI) that uses the urn scheme. URNs are globally unique persistent identifiers assigned within defined namespaces so they will be available for a long period of time, even after the resource which they identify ceases to exist or becomes unavailable. URNs cannot be used to directly locate an item and need not be resolvable, as they are simply templates that another parser may use to find an item.

en.wikipedia.org/wiki/Uniform_Resource_Name

UTF (Unicode Transformation Format)

The Unicode Transformation Format is a character encoding format which is able to encode all of the possible character code points in Unicode.

www.techopedia.com/definition/976/unicode-transformation-format-utf

VLAN (Virtual Local Area Network)

A virtual LAN is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic.

en.wikipedia.org/wiki/Virtual_LAN

WAN (Wide Area Network)

A wide area network (WAN) is a telecommunications network that extends over a large geographic area for the primary purpose of computer networking. Wide area networks are often established with leased telecommunication circuits.

en.wikipedia.org/wiki/Wide_area_network

WCCP (Web Cache Communication Protocol)

Web Cache Communication Protocol is a Cisco-developed content-routing protocol that provides a mechanism to redirect traffic flows in real-time. It has built-in load balancing, scaling, fault tolerance, and service-assurance (failsafe) mechanisms.

en.wikipedia.org/wiki/Web_Cache_Communication_Protocol

WebDAV (Web-Based Distributed Authoring and Versioning)

The Web Distributed Authoring and Versioning is an extension of the Hypertext Transfer Protocol (HTTP) that allows clients to perform remote Web content authoring operations. WebDAV is defined in RFC 4918 by a working group of the Internet Engineering Task Force.

HTTP: The Definitive Guide: The Definitive Guide (Definitive Guides) 1st Edition by [David Gourley](#) (Author), [Brian Totty](#) (Author), [Marjorie Sayer](#) (Author), [Anshu Aggarwal](#) (Author), [Sailu Reddy](#) (Author)

WPAD (Web Proxy Autodiscovery Protocol)

The Web Proxy Auto-Discovery (WPAD) Protocol is a method used by clients to locate the URL of a configuration file using DHCP and/or DNS discovery methods. Once detection and download of the configuration file is complete, it can be executed to determine the proxy for a specified URL.

HTTP: The Definitive Guide: The Definitive Guide (Definitive Guides) 1st Edition by [David Gourley](#) (Author), [Brian Totty](#) (Author), [Marjorie Sayer](#) (Author), [Anshu Aggarwal](#) (Author), [Sailu Reddy](#) (Author)



If there are other commonly used acronym's that you think would make sense to include, email us at fddler@progress.com and we will update the list



facebook.com/progresssw

twitter.com/@TelerikFiddler

youtube.com/progresssw

linkedin.com/company/progress-software