Workgroup: Network Working Group
Internet-Draft:
draft-multiformats-multihash-03
Published: August 2021
Intended Status: Informational
Expires: 16 February 2022
Authors: J.B. Benet M.S. Sporny
Protocol Labs Digital Bazaar

The Multihash Data Format

Abstract

Cryptographic hash functions often have multiple output sizes and encodings. This variability makes it difficult for applications to examine a series of bytes and determine which hash function produced them. Multihash is a universal data format for encoding outputs from hash functions. It is useful to write applications that can simultaneously support different hash function outputs as well as upgrade their use of hashes over time; Multihash is intended to address these needs.

Feedback

This specification is a joint work product of Protocol Labs, the W3C Digital Verification Community Group, and the W3C Credentials Community Group. Feedback related to this specification should logged in the issue tracker or be sent to public-credentials@w3.org. .

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 2 February 2022.

Copyright Notice

Table of Contents

1. Introduction

Multihash is particularly important in systems which depend on cryptographically secure hash functions. Attacks may break the cryptographic properties of secure hash functions. These cryptographic breaks are particularly painful in large tool ecosystems, where tools may have made assumptions about hash values,

such as function and digest size. Upgrading becomes a nightmare, as all tools which make those assumptions would have to be upgraded to use the new hash function and new hash digest length. Tools may face serious interoperability problems or error-prone special casing.

How many programs out there assume a git hash is a SHA-1 hash?

How many scripts assume the hash value digest is exactly 160 bits?

How many tools will break when these values change?

How many programs will fail silently when these values change?

This is precisely why Multihash was created. It was designed for seamlessly upgrading systems that depend on cryptographic hashes.

When using Multihash, a system warns the consumers of its hash values that these may have to be upgraded in case of a break. Even though the system may still only use a single hash function at a time, the use of multihash makes it clear to applications that hash values may use different hash functions or be longer in the future. Tooling, applications, and scripts can avoid making assumptions about the length, and read it from the multihash value instead. This way, the vast majority of tooling - which may not do any checking of hashes - would not have to be upgraded at all. This vastly simplifies the upgrade process, avoiding the waste of hundreds or thousands of software engineering hours, deep frustrations, and high blood pressure.

2. The Multihash Fields

A multihash follows the TLV (type-length-value) pattern and consists of several fields composed of a combination of unsigned variable length integers and byte information.

2.1. Multihash Core Data Types

The following section details the core data types used by the Multihash data format.

2.1.1. unsigned variable integer

A data type that enables one to express an unsigned integer of variable length.

When encoding an unsigned variable integer, the unsigned integer is serialized seven bits at a time, starting with the least significant bits. The most significant bit in each output byte indicates if there is a continuation byte. It is not possible to express a signed integer with this data type.

Value	Encoding (bits)	hexadecimal notation
1	00000001	0x01
127	01111111	0x7F
128	10000000 00000001	0x8001
255	11111111 00000001	0xFF01
300	10101100 00000010	0xAC02
16384	10000000 10000000 00000001	0x808001

Table 1: Examples of Unsigned Variable Integers

Implementations MUST restrict the size of the varint to a max of nine bytes (63 bits). In order to avoid memory attacks on the encoding, the aforementioned practical maximum length of nine bytes is used. There is no theoretical limit, and future specs can grow this number if it is truly necessary to have code or length values larger than 2^31.

2.2. Multihash Fields

A multihash follows the TLV (type-length-value) pattern.

2.2.1. Hash Function Identifier

The hash function identifier is an unsigned variable integer identifying the hash function. The possible values for this field are provided in The Multihash Identifier Registry.

2.2.2. Digest Length

The digest length is an unsigned variable integer counting the length of the digest in bytes.

2.2.3. Digest Value

The digest value is the hash function digest with a length of exactly what is specified in the digest length, which is specified in bytes.

2.3. A Multihash Example

For example, the following is an expression of a SHA2-256 hash in hexadecimal notation (spaces added for readability purposes):

```
0x12 20 41dd7b6443542e75701aa98a0c235951a28a0d851b11564d20022ab11d2589a8
```

The first byte (0x12) specifies the SHA2-256 hash function. The second byte (0x20) specifies the length of the hash, which is 32 bytes. The rest of the data specifies the value of the output of the hash function.

3. References

3.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

[RFC7693] Saarinen, M-J., Ed. and J-P. Aumasson, "The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)", RFC 7693, DOI 10.17487/RFC7693, November 2015, <https://www.rfc-editor.org/info/rfc7693>.

3.2. Informative References

[RFC6150] Turner, S. and L. Chen, "MD4 to Historic Status", RFC 6150, DOI 10.17487/RFC6150, March 2011, <https://www.rfc-editor.org/info/rfc6150>.

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, DOI 10.17487/RFC6151, March 2011, <https://www.rfc-editor.org/info/rfc6151>.

Appendix A. Security Considerations

There are a number of security considerations to take into account when implementing or utilizing this specification. TBD

Appendix B. Test Values

The multihash examples are chosen to show different hash functions and different hash digest lengths at play. The input test data for all of the examples in this section is:

Merkle–Damgård

B.1. SHA-1

0x11148a173fd3e32c0fa78b90fe42d305f202244e2739

The fields for this multihash are - hashing function: sha1 (0x11), length: 20 (0x14), digest: 0x8a173fd3e32c0fa78b90fe42d305f202244e2739

B.2. SHA-256

```
0x122041dd7b6443542e75701aa98a0c235951a28a0d851b11564d20022ab11d2589a8
```

The fields for this multihash are - hashing function: sha2-256 (0x12), length: 32 (0x20), digest: 0x41dd7b6443542e75701aa98a0c235951a28a0d851b11564d20022ab11d2589a8

B.3. SHA-512/256

```
0x132052eb4dd19f1ec522859e12d89706156570f8fbab1824870bc6f8c7d235eef5f4
```

The fields for this multihash are - hashing function: sha2-512 (0x13), length: 32 (0x20), digest: 0x52eb4dd19f1ec522859e12d89706156570f8fbab1824870bc6f8c7d235eef5f4

B.4. SHA-512

```
0x134052eb4dd19f1ec522859e12d89706156570f8fbab1824870bc6f8c7d235eef5f4c2
```

The fields for this multihash are - hashing function: sha2-512 (0x13), length: 64 (0x40), digest: 0x52eb4dd19f1ec522859e12d89706156570f8fbab1824870bc6f8c7d235eef5f4c2cbbafd365f96fb12b1d98a0334870c2ce90355da25e6a1108a6e17c4aaebb0

B.5. blake2b512

```
0xb24040d91ae0cb0e48022053ab0f8f0dc78d28593d0f1c13ae39c9b169c136a779f21a
```

The fields for this multihash are - hashing function: blake2b-512 (0xb240), length: 64 (0x40), digest: 0xd91ae0cb0e48022053ab0f8f0dc78d28593d0f1c13ae39c9b169c136a779f21a0496337b6f776a73c1742805c1cc15e792ddb3c92ee1fe300389456ef3dc97e2

B.6. blake2b256

```
0xb220207d0a1371550f3306532ff44520b649f8be05b72674e46fc24468ff74323ab030
```

The fields for this multihash are - hashing function: blake2b-256 (0xb220), length: 32 (0x20), digest: 0x7d0a1371550f3306532ff44520b649f8be05b72674e46fc24468ff74323ab030

B.7. blake2s256

```
0xb26020a96953281f3fd944a3206219fad61a40b992611b7580f1fa091935db3f7ca13d
```

The fields for this multihash are - hashing function: blake2s-256 (0xb260), length: 32 (0x20), digest: 0xa96953281f3fd944a3206219fad61a40b992611b7580f1fa091935db3f7ca13d

B.8. blake2s128

```
0xb250100a4ec6f1629e49262d7093e2f82a3278
```

The fields for this multihash are - hashing function: blake2s-128 (0xb250), length: 16 (0x10), digest: 0x0a4ec6f1629e49262d7093e2f82a3278

Appendix C. Acknowledgements

The editors would like to thank the following individuals for feedback on and implementations of the specification (in alphabetical order).

Appendix D. IANA Considerations

D.1. The Multihash Identifier Registry

The Multihash Identifier Registry contains hash functions supported by Multihash each with its canonical name, its value in hexadecimal notation, and its status. The following initial entries should be added to the registry to be created and maintained at (the suggested URI) http://www.iana.org/assignments/multihash-identifiers:

Name	Identifier	Status	Specification
identity	0x00	active	Unknown
sha1	0x11	active	RFC 6234 [RFC6234]
sha2-256	0x12	active	RFC 6234 [RFC6234]
sha2-512	0x13	active	RFC 6234 [RFC6234]
sha3-512	0x14	active	Unknown
sha3-384	0x15	active	Unknown
sha3-256	0x16	active	Unknown
sha3-224	0x17	active	Unknown
shake-128	0x18	active	Unknown
shake-256	0x19	active	Unknown
keccak-224	0x1a	active	Unknown
keccak-256	0x1b	active	Unknown
keccak-384	0x1c	active	Unknown
keccak-512	0x1d	active	Unknown
blake3	0x1e	active	Unknown
murmur3-128	0x22	active	Unknown
murmur3-32	0x23	active	Unknown
dbl-sha2-256	0x56	active	Unknown
md4	0xd4	deprecated	RFC 6150 [RFC6150]

Name	Identifier	Status	Specification
md5	0xd5	deprecated	RFC 6151 [RFC6151]
bmt	0xd6	active	Unknown
sha2-256-trunc254-padded	0x1012	active	RFC 6234 [RFC6234]
ripemd-128	0x1052	active	Unknown
ripemd-160	0x1053	active	Unknown
ripemd-256	0x1054	active	Unknown
ripemd-320	0x1055	active	Unknown
x11	0x1100	active	Unknown
kangarootwelve	0x1d01	active	Unknown
sm3-256	0x534d	active	Unknown
blake2b-8	0xb201	active	RFC 7693 [RFC7693]
blake2b-16	0xb202	active	RFC 7693 [RFC7693]
blake2b-24	0xb203	active	RFC 7693 [RFC7693]
blake2b-32	0xb204	active	RFC 7693 [RFC7693]
blake2b-40	0xb205	active	RFC 7693 [RFC7693]
blake2b-48	0xb206	active	RFC 7693 [RFC7693]
blake2b-56	0xb207	active	RFC 7693 [RFC7693]
blake2b-64	0xb208	active	RFC 7693 [RFC7693]
blake2b-72	0xb209	active	RFC 7693 [RFC7693]
blake2b-80	0xb20a	active	RFC 7693 [RFC7693]
blake2b-88	0xb20b	active	RFC 7693 [RFC7693]
blake2b-96	0xb20c	active	RFC 7693 [RFC7693]
blake2b-104	0xb20d	active	RFC 7693 [RFC7693]
blake2b-112	0xb20e	active	RFC 7693 [RFC7693]
blake2b-120	0xb20f	active	RFC 7693 [RFC7693]
blake2b-128	0xb210	active	RFC 7693 [RFC7693]
blake2b-136	0xb211	active	RFC 7693 [RFC7693]

Name	Identifier	Status	Specification
blake2b-144	0xb212	active	RFC 7693 [RFC7693]
blake2b-152	0xb213	active	RFC 7693 [RFC7693]
blake2b-160	0xb214	active	RFC 7693 [RFC7693]
blake2b-168	0xb215	active	RFC 7693 [RFC7693]
blake2b-176	0xb216	active	RFC 7693 [RFC7693]
blake2b-184	0xb217	active	RFC 7693 [RFC7693]
blake2b-192	0xb218	active	RFC 7693 [RFC7693]
blake2b-200	0xb219	active	RFC 7693 [RFC7693]
blake2b-208	0xb21a	active	RFC 7693 [RFC7693]
blake2b-216	0xb21b	active	RFC 7693 [RFC7693]
blake2b-224	0xb21c	active	RFC 7693 [RFC7693]
blake2b-232	0xb21d	active	RFC 7693 [RFC7693]
blake2b-240	0xb21e	active	RFC 7693 [RFC7693]
blake2b-248	0xb21f	active	RFC 7693 [RFC7693]
blake2b-256	0xb220	active	RFC 7693 [RFC7693]
blake2b-264	0xb221	active	RFC 7693 [RFC7693]
blake2b-272	0xb222	active	RFC 7693 [RFC7693]
blake2b-280	0xb223	active	RFC 7693 [RFC7693]
blake2b-288	0xb224	active	RFC 7693 [RFC7693]
blake2b-296	0xb225	active	RFC 7693 [RFC7693]
blake2b-304	0xb226	active	RFC 7693 [RFC7693]
blake2b-312	0xb227	active	RFC 7693 [RFC7693]
blake2b-320	0xb228	active	RFC 7693 [RFC7693]

Name	Identifier	Status	Specification
blake2b-328	0xb229	active	RFC 7693 [RFC7693]
blake2b-336	0xb22a	active	RFC 7693 [RFC7693]
blake2b-344	0xb22b	active	RFC 7693 [RFC7693]
blake2b-352	0xb22c	active	RFC 7693 [RFC7693]
blake2b-360	0xb22d	active	RFC 7693 [RFC7693]
blake2b-368	0xb22e	active	RFC 7693 [RFC7693]
blake2b-376	0xb22f	active	RFC 7693 [RFC7693]
blake2b-384	0xb230	active	RFC 7693 [RFC7693]
blake2b-392	0xb231	active	RFC 7693 [RFC7693]
blake2b-400	0xb232	active	RFC 7693 [RFC7693]
blake2b-408	0xb233	active	RFC 7693 [RFC7693]
blake2b-416	0xb234	active	RFC 7693 [RFC7693]
blake2b-424	0xb235	active	RFC 7693 [RFC7693]
blake2b-432	0xb236	active	RFC 7693 [RFC7693]
blake2b-440	0xb237	active	RFC 7693 [RFC7693]
blake2b-448	0xb238	active	RFC 7693 [RFC7693]
blake2b-456	0xb239	active	RFC 7693 [RFC7693]
blake2b-464	0xb23a	active	RFC 7693 [RFC7693]
blake2b-472	0xb23b	active	RFC 7693 [RFC7693]
blake2b-480	0xb23c	active	RFC 7693 [RFC7693]
blake2b-488	0xb23d	active	RFC 7693 [RFC7693]
blake2b-496	0xb23e	active	RFC 7693 [RFC7693]
blake2b-504	0xb23f	active	RFC 7693 [RFC7693]

Name	Identifier	Status	Specification
blake2b-512	0xb240	active	RFC 7693 [RFC7693]
blake2s-8	0xb241	active	RFC 7693 [RFC7693]
blake2s-16	0xb242	active	RFC 7693 [RFC7693]
blake2s-24	0xb243	active	RFC 7693 [RFC7693]
blake2s-32	0xb244	active	RFC 7693 [RFC7693]
blake2s-40	0xb245	active	RFC 7693 [RFC7693]
blake2s-48	0xb246	active	RFC 7693 [RFC7693]
blake2s-56	0xb247	active	RFC 7693 [RFC7693]
blake2s-64	0xb248	active	RFC 7693 [RFC7693]
blake2s-72	0xb249	active	RFC 7693 [RFC7693]
blake2s-80	0xb24a	active	RFC 7693 [RFC7693]
blake2s-88	0xb24b	active	RFC 7693 [RFC7693]
blake2s-96	0xb24c	active	RFC 7693 [RFC7693]
blake2s-104	0xb24d	active	RFC 7693 [RFC7693]
blake2s-112	0xb24e	active	RFC 7693 [RFC7693]
blake2s-120	0xb24f	active	RFC 7693 [RFC7693]
blake2s-128	0xb250	active	RFC 7693 [RFC7693]
blake2s-136	0xb251	active	RFC 7693 [RFC7693]
blake2s-144	0xb252	active	RFC 7693 [RFC7693]
blake2s-152	0xb253	active	RFC 7693 [RFC7693]
blake2s-160	0xb254	active	RFC 7693 [RFC7693]
blake2s-168	0xb255	active	RFC 7693 [RFC7693]
blake2s-176	0xb256	active	RFC 7693 [RFC7693]

Name	Identifier	Status	Specification
blake2s-184	0xb257	active	RFC 7693 [RFC7693]
blake2s-192	0xb258	active	RFC 7693 [RFC7693]
blake2s-200	0xb259	active	RFC 7693 [RFC7693]
blake2s-208	0xb25a	active	RFC 7693 [RFC7693]
blake2s-216	0xb25b	active	RFC 7693 [RFC7693]
blake2s-224	0xb25c	active	RFC 7693 [RFC7693]
blake2s-232	0xb25d	active	RFC 7693 [RFC7693]
blake2s-240	0xb25e	active	RFC 7693 [RFC7693]
blake2s-248	0xb25f	active	RFC 7693 [RFC7693]
blake2s-256	0xb260	active	RFC 7693 [RFC7693]
skein256-8	0xb301	active	Unknown
skein256-16	0xb302	active	Unknown
skein256-24	0xb303	active	Unknown
skein256-32	0xb304	active	Unknown
skein256-40	0xb305	active	Unknown
skein256-48	0xb306	active	Unknown
skein256-56	0xb307	active	Unknown
skein256-64	0xb308	active	Unknown
skein256-72	0xb309	active	Unknown
skein256-80	0xb30a	active	Unknown
skein256-88	0xb30b	active	Unknown
skein256-96	0xb30c	active	Unknown
skein256-104	0xb30d	active	Unknown
skein256-112	0xb30e	active	Unknown
skein256-120	0xb30f	active	Unknown
skein256-128	0xb310	active	Unknown
skein256-136	0xb311	active	Unknown
skein256-144	0xb312	active	Unknown
skein256-152	0xb313	active	Unknown
skein256-160	0xb314	active	Unknown
skein256-168	0xb315	active	Unknown
skein256-176	0xb316	active	Unknown
skein256-184	0xb317	active	Unknown
skein256-192	0xb318	active	Unknown
skein256-200	0xb319	active	Unknown
skein256-208	0xb31a	active	Unknown

Name	Identifier	Status	Specification
skein256-216	0xb31b	active	Unknown
skein256-224	0xb31c	active	Unknown
skein256-232	0xb31d	active	Unknown
skein256-240	0xb31e	active	Unknown
skein256-248	0xb31f	active	Unknown
skein256-256	0xb320	active	Unknown
skein512-8	0xb321	active	Unknown
skein512-16	0xb322	active	Unknown
skein512-24	0xb323	active	Unknown
skein512-32	0xb324	active	Unknown
skein512-40	0xb325	active	Unknown
skein512-48	0xb326	active	Unknown
skein512-56	0xb327	active	Unknown
skein512-64	0xb328	active	Unknown
skein512-72	0xb329	active	Unknown
skein512-80	0xb32a	active	Unknown
skein512-88	0xb32b	active	Unknown
skein512-96	0xb32c	active	Unknown
skein512-104	0xb32d	active	Unknown
skein512-112	0xb32e	active	Unknown
skein512-120	0xb32f	active	Unknown
skein512-128	0xb330	active	Unknown
skein512-136	0xb331	active	Unknown
skein512-144	0xb332	active	Unknown
skein512-152	0xb333	active	Unknown
skein512-160	0xb334	active	Unknown
skein512-168	0xb335	active	Unknown
skein512-176	0xb336	active	Unknown
skein512-184	0xb337	active	Unknown
skein512-192	0xb338	active	Unknown
skein512-200	0xb339	active	Unknown
skein512-208	0xb33a	active	Unknown
skein512-216	0xb33b	active	Unknown
skein512-224	0xb33c	active	Unknown
skein512-232	0xb33d	active	Unknown
skein512-240	0xb33e	active	Unknown
skein512-248	0xb33f	active	Unknown
skein512-256	0xb340	active	Unknown
skein512-264	0xb341	active	Unknown
skein512-272	0xb342	active	Unknown
skein512-280	0xb343	active	Unknown
skein512-288	0xb344	active	Unknown
skein512-296	0xb345	active	Unknown
skein512-304	0xb346	active	Unknown
skein512-312	0xb347	active	Unknown

Name	Identifier	Status	Specification
skein512-320	0xb348	active	Unknown
skein512-328	0xb349	active	Unknown
skein512-336	0xb34a	active	Unknown
skein512-344	0xb34b	active	Unknown
skein512-352	0xb34c	active	Unknown
skein512-360	0xb34d	active	Unknown
skein512-368	0xb34e	active	Unknown
skein512-376	0xb34f	active	Unknown
skein512-384	0xb350	active	Unknown
skein512-392	0xb351	active	Unknown
skein512-400	0xb352	active	Unknown
skein512-408	0xb353	active	Unknown
skein512-416	0xb354	active	Unknown
skein512-424	0xb355	active	Unknown
skein512-432	0xb356	active	Unknown
skein512-440	0xb357	active	Unknown
skein512-448	0xb358	active	Unknown
skein512-456	0xb359	active	Unknown
skein512-464	0xb35a	active	Unknown
skein512-472	0xb35b	active	Unknown
skein512-480	0xb35c	active	Unknown
skein512-488	0xb35d	active	Unknown
skein512-496	0xb35e	active	Unknown
skein512-504	0xb35f	active	Unknown
skein512-512	0xb360	active	Unknown
skein1024-8	0xb361	active	Unknown
skein1024-16	0xb362	active	Unknown
skein1024-24	0xb363	active	Unknown
skein1024-32	0xb364	active	Unknown
skein1024-40	0xb365	active	Unknown
skein1024-48	0xb366	active	Unknown
skein1024-56	0xb367	active	Unknown
skein1024-64	0xb368	active	Unknown
skein1024-72	0xb369	active	Unknown
skein1024-80	0xb36a	active	Unknown
skein1024-88	0xb36b	active	Unknown
skein1024-96	0xb36c	active	Unknown
skein1024-104	0xb36d	active	Unknown
skein1024-112	0xb36e	active	Unknown
skein1024-120	0xb36f	active	Unknown
skein1024-128	0xb370	active	Unknown
skein1024-136	0xb371	active	Unknown
skein1024-144	0xb372	active	Unknown
skein1024-152	0xb373	active	Unknown
skein1024-160	0xb374	active	Unknown

Name	Identifier	Status	Specification
skein1024-168	0xb375	active	Unknown
skein1024-176	0xb376	active	Unknown
skein1024-184	0xb377	active	Unknown
skein1024-192	0xb378	active	Unknown
skein1024-200	0xb379	active	Unknown
skein1024-208	0xb37a	active	Unknown
skein1024-216	0xb37b	active	Unknown
skein1024-224	0xb37c	active	Unknown
skein1024-232	0xb37d	active	Unknown
skein1024-240	0xb37e	active	Unknown
skein1024-248	0xb37f	active	Unknown
skein1024-256	0xb380	active	Unknown
skein1024-264	0xb381	active	Unknown
skein1024-272	0xb382	active	Unknown
skein1024-280	0xb383	active	Unknown
skein1024-288	0xb384	active	Unknown
skein1024-296	0xb385	active	Unknown
skein1024-304	0xb386	active	Unknown
skein1024-312	0xb387	active	Unknown
skein1024-320	0xb388	active	Unknown
skein1024-328	0xb389	active	Unknown
skein1024-336	0xb38a	active	Unknown
skein1024-344	0xb38b	active	Unknown
skein1024-352	0xb38c	active	Unknown
skein1024-360	0xb38d	active	Unknown
skein1024-368	0xb38e	active	Unknown
skein1024-376	0xb38f	active	Unknown
skein1024-384	0xb390	active	Unknown
skein1024-392	0xb391	active	Unknown
skein1024-400	0xb392	active	Unknown
skein1024-408	0xb393	active	Unknown
skein1024-416	0xb394	active	Unknown
skein1024-424	0xb395	active	Unknown
skein1024-432	0xb396	active	Unknown
skein1024-440	0xb397	active	Unknown
skein1024-448	0xb398	active	Unknown
skein1024-456	0xb399	active	Unknown
skein1024-464	0xb39a	active	Unknown
skein1024-472	0xb39b	active	Unknown
skein1024-480	0xb39c	active	Unknown
skein1024-488	0xb39d	active	Unknown
skein1024-496	0xb39e	active	Unknown
skein1024-504	0xb39f	active	Unknown
skein1024-512	0xb3a0	active	Unknown
skein1024-520	0xb3a1	active	Unknown

Name	Identifier	Status	Specification
skein1024-528	0xb3a2	active	Unknown
skein1024-536	0xb3a3	active	Unknown
skein1024-544	0xb3a4	active	Unknown
skein1024-552	0xb3a5	active	Unknown
skein1024-560	0xb3a6	active	Unknown
skein1024-568	0xb3a7	active	Unknown
skein1024-576	0xb3a8	active	Unknown
skein1024-584	0xb3a9	active	Unknown
skein1024-592	0xb3aa	active	Unknown
skein1024-600	0xb3ab	active	Unknown
skein1024-608	0xb3ac	active	Unknown
skein1024-616	0xb3ad	active	Unknown
skein1024-624	0xb3ae	active	Unknown
skein1024-632	0xb3af	active	Unknown
skein1024-640	0xb3b0	active	Unknown
skein1024-648	0xb3b1	active	Unknown
skein1024-656	0xb3b2	active	Unknown
skein1024-664	0xb3b3	active	Unknown
skein1024-672	0xb3b4	active	Unknown
skein1024-680	0xb3b5	active	Unknown
skein1024-688	0xb3b6	active	Unknown
skein1024-696	0xb3b7	active	Unknown
skein1024-704	0xb3b8	active	Unknown
skein1024-712	0xb3b9	active	Unknown
skein1024-720	0xb3ba	active	Unknown
skein1024-728	0xb3bb	active	Unknown
skein1024-736	0xb3bc	active	Unknown
skein1024-744	0xb3bd	active	Unknown
skein1024-752	0xb3be	active	Unknown
skein1024-760	0xb3bf	active	Unknown
skein1024-768	0xb3c0	active	Unknown
skein1024-776	0xb3c1	active	Unknown
skein1024-784	0xb3c2	active	Unknown
skein1024-792	0xb3c3	active	Unknown
skein1024-800	0xb3c4	active	Unknown
skein1024-808	0xb3c5	active	Unknown
skein1024-816	0xb3c6	active	Unknown
skein1024-824	0xb3c7	active	Unknown
skein1024-832	0xb3c8	active	Unknown
skein1024-840	0xb3c9	active	Unknown
skein1024-848	0xb3ca	active	Unknown
skein1024-856	0xb3cb	active	Unknown
skein1024-864	0xb3cc	active	Unknown
skein1024-872	0xb3cd	active	Unknown
skein1024-880	0xb3ce	active	Unknown

Name	Identifier	Status	Specification
skein1024-888	0xb3cf	active	Unknown
skein1024-896	0xb3d0	active	Unknown
skein1024-904	0xb3d1	active	Unknown
skein1024-912	0xb3d2	active	Unknown
skein1024-920	0xb3d3	active	Unknown
skein1024-928	0xb3d4	active	Unknown
skein1024-936	0xb3d5	active	Unknown
skein1024-944	0xb3d6	active	Unknown
skein1024-952	0xb3d7	active	Unknown
skein1024-960	0xb3d8	active	Unknown
skein1024-968	0xb3d9	active	Unknown
skein1024-976	0xb3da	active	Unknown
skein1024-984	0xb3db	active	Unknown
skein1024-992	0xb3dc	active	Unknown
skein1024-1000	0xb3dd	active	Unknown
skein1024-1008	0xb3de	active	Unknown
skein1024-1016	0xb3df	active	Unknown
skein1024-1024	0xb3e0	active	Unknown
poseidon-bls12_381-a2-fc1	0xb401	active	Unknown
poseidon-bls12_381-a2-fc1-sc	0xb402	active	Unknown

Table 2: Multihash Identifier Registry

NOTE: The most up to date place for developers to find the table above is https://github.com/multiformats/multicodec/blob/master/table.csv.

D.2. The 'mh' Digest Algorithm

This memo registers the "mh" digest-algorithm in the HTTP Digest Algorithm Values registry with the following values:

Digest Algorithm: mh

Description: The multibase-serialized value of a multihash-supported algorithm.

References: this document

Status: standard

Authors' Addresses

Juan Benet
Protocol Labs
548 Market Street, #51207
San Francisco, CA 94104

United States of America

Phone: +1 619 957 7606
Email: juan@protocol.ai
URI: http://juan.benet.ai/

Manu Sporny
Digital Bazaar
203 Roanoke Street W.
Blacksburg, VA 24060
United States of America

Phone: +1 540 961 4469
Email: msporny@digitalbazaar.com
URI: http://manu.sporny.org/