VeraCrypt Volume Format Specification

The format of file-hosted volumes is identical to the format of partition/device-hosted volumes (however, the "volume header", or key data, for a system partition/drive is stored in the last 512 bytes of the first logical drive track). VeraCrypt volumes have no "signature" or ID strings. Until decrypted, they appear to consist solely of random data.

Free space on each VeraCrypt volume is filled with random data when the volume is created.* The random data is generated as follows: Right before VeraCrypt volume formatting begins, a temporary encryption key and a temporary secondary key (XTS mode) are generated by the random number generator (see the section Random Number Generator). The encryption algorithm that the user selected is initialized with the temporary keys. The encryption algorithm is then used to encrypt plaintext blocks consisting of random bytes generated by the random number generator. The encryption algorithm operates in XTS mode (see the section Hidden Volume). The resulting ciphertext blocks are used to fill (overwrite) the free space on the volume. The temporary keys are stored in RAM and are erased after formatting finishes.

VeraCrypt Volume Format Specification:

Offset (bytes)	Size (bytes)	Encryption Status†	Description
0	64	Unencrypted§	Salt
64	4	Encrypted	ASCII string "VERA"
68	2	Encrypted	Volume header format version (2)
70	2	Encrypted	Minimum program version required to open the volume
72	4	Encrypted	CRC-32 checksum of the (decrypted) bytes 256-511
76	16	Encrypted	Reserved (must contain zeroes)
92	8	Encrypted	Size of hidden volume (set to zero in non-hidden volumes)
100	8	Encrypted	Size of volume
108	8	Encrypted	Byte offset of the start of the master key scope
116	8	Encrypted	Size of the encrypted area within the master key scope
124	4	Encrypted	Flag bits (bit 0 set: system encryption; bit 1 set: non-system in-place-encrypted/decrypted volume; bits 2–31 are reserved)
128	4	Encrypted	Sector size (in bytes)
132	120	Encrypted	Reserved (must contain zeroes)
252	4	Encrypted	CRC-32 checksum of the (decrypted) bytes 64-251
256	*Var.*	Encrypted	Concatenated primary and secondary master keys**

512	65024	Encrypted	Reserved (for system encryption, this item is omitted‡‡)
65536	65536	Encrypted / Unencrypted§	Area for hidden volume header (if there is no hidden volume within the volume, this area contains random data††). For system encryption, this item is omitted.‡‡ See bytes 0–65535.
131072	*Var.*	Encrypted	Data area (master key scope). For system encryption, offset may be different (depending on offset of system partition).
S-131072‡	65536	Encrypted / Unencrypted§	Backup header (encrypted with a different header key derived using a different salt). For system encryption, this item is omitted.‡‡ See bytes 0–65535.
S-65536‡	65536	Encrypted / Unencrypted§	Backup header for hidden volume (encrypted with a different header key derived using a different salt). If there is no hidden volume within the volume, this area contains random data.†† For system encryption, this item is omitted.‡‡ See bytes 0–65535.

The fields located at byte #0 (salt) and #256 (master keys) contain random values generated by the random number generator (see the section Random Number Generator) during the volume creation process.

If a VeraCrypt volume hosts a hidden volume (within its free space), the header of the hidden volume is located at byte #65536 of the host volume (the header of the host/outer volume is located at byte #0 of the host volume – see the section Hidden Volume). If there is no hidden volume within a VeraCrypt volume, bytes 65536–131071 of the volume (i.e., the area where the header of a hidden volume can reside) contain random data (see above for information on the method used to fill free volume space with random data when the volume is created). The layout of the header of a hidden volume is the same as the one of a standard volume (bytes 0–65535).

The maximum possible VeraCrypt volume size is 2^{63} bytes (8,589,934,592 GB). However, due to security reasons (with respect to the 128-bit block size used by the encryption algorithms), the maximum allowed volume size is 1 PB (1,048,576 GB).

Embedded Backup Headers

Each VeraCrypt volume contains an embedded backup header, located at the end of the volume (see above). The header backup is *not* a copy of the volume header because it is encrypted with a different header key derived using a different salt (see the section Header Key Derivation, Salt, and Iteration Count).

When the volume password and/or PIM and/or keyfiles are changed, or when the header is restored from the embedded (or an external) header backup, both the volume header and the backup header (embedded in the volume) are re-encrypted with different header keys (derived using newly generated salts – the salt for the volume header is different from the salt for the backup header). Each salt is generated by the VeraCrypt random number generator (see the section Random Number Generator).

For more information about header backups, see the subsection Tools > Restore Volume Header in the chapter Main Program Window.

Next Section >>

---

* Provided that the options *Quick Format* and *Dynamic* are disabled and provided that the volume does not contain a filesystem that has been encrypted in place (note that VeraCrypt does not allow the user to create a hidden volume within such a volume).
† The encrypted areas of the volume header are encrypted in XTS mode using the primary and secondary header keys. For more information, see the section Encryption Scheme and the section Header Key Derivation, Salt, and Iteration Count.
‡ *S* denotes the size of the volume host (in bytes).
§ Note that the salt does not need to be encrypted, as it does not have to be kept secret [7] (salt is a sequence of random values).
** Multiple concatenated master keys are stored here when the volume is encrypted using a cascade of ciphers (secondary master keys are used for XTS mode).
†† See above in this section for information on the method used to fill free volume space with random data when the volume is created.
‡‡ Here, the meaning of "system encryption" does not include a hidden volume containing a hidden operating system.