|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Bit offset | 0–3 | 4-7 | | 8–15 | | 16–31 |
| 0 | TAG | SALT | | | | |
| 32 | Destination Address | | | | | |
| 64 | Zeros | | Protocol | | TCP length | |
| 96 | Source port | | | Destination port | | |
| 128 |  | | | | | |
| 160 |  | | | | | |
| 192 |  | | | | | |
| 224 |  | | | | | |
|  |  | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | File Format (Header Fields) | | | | TAG | 4 bytes | The 4 ASCII Characters ‘PWS3’ | | SALT | 32 bytes | 256 random bit value generated at file creation | | ITER | 32 bit LE value | number of rounds in the key stretch algorithm | |  |  |  | |  |  |  | |  |  |  | |  |  |  |   **File Format (Header Fields)** | | |
| TAG | 4 bytes | The 4 ASCII Chacters ‘PWS3’ |
| SALT | 32 bytes | 256 random bit value generated at file creation |
| ITER | 32 bit LE value | number of rounds in the key stretch algorithm |
| H(P’) | 32 bytes | SHA-256 of the user’s passphrase |
| B1 | 16 bytes | Encrypted 128 random value using P’ with Twofish algorithm |
| B2 | 16 bytes | Encrypted 128 random value using P’ with Twofish algorithm |
| B3 | 16 bytes | Encrypted 128 random value using P’ with Twofish algorithm |
| B4 | 16 bytes | Encrypted 128 random value using P’ with Twofish algorithm |
| Init Vector | 16 bytes | 128 bit random value that is the Initiazliation Vector for the content’s encryption |
| Header | N bytes | General information for the database |
| Records | N bytes | The records in the database |
| EOF | unencrypted string “PWS3-EOFPWS3-EOF” |  |
| HMAC | 32 bytes | 256 bit SHA-256 hash of the plaintext contents, starting with the version number in the header and ending with the last field of the last record |