

How to parse the USB/KB encrypted data correctly with Parsomatic?

When I drop swipe data from a USB keyboard interface reader into the tool, it doesn't parse correctly. How can I get the data correctly parsed with Parsomatic?

The output from a USB/keyboard interface reader contains ASCII and HEX combined data. With Parsomatic, it only parses the data correctly when it's all in Hex. What you can do is:

1. Highlight the mask data field which is in ACSII with USB/KB interface reader.

Parsomatic

Version 1.0.9

Parses ID TECH card-reader data streams from AR, GR, NEO, and NGA devices.

To use: Paste data into text area, then type **Enter**. Parsed data will appear underneath the text area. Hover the mouse over color-coded areas to see an explanation of the hex values. Optionally use the tag lookup feature (below) to look up tags at any time.

Tag lookup (e.g. **9F6D**):

Tag	Name	Description	Format	Min. Length	Max. Length	Defined by
-----	------	-------------	--------	-------------	-------------	------------

Paste reader data here, then hit ENTER:

```
02ED01801F4C2800839B%*6010*****8765^0254/SERVICERECOVERYUSD
^*****?
*,6010*****8765=*****?
*95025C86987E4F7DD07D58730EB79FDFB90AB7F23E6ECA6F4F04A67BF511E
E13F950903BDE77624680C460E9C36C4F9136256BB93A38CB98F95626DCFAF
9335CE0A213074CC1CD84CC911398E06756C464AB036B694228ADA7EC018F4
```

Show ASCII SHA-256 TLVs only

2. Click the "Convert ASCII to Hex" button below the data window once you have the ASCII data highlighted. That'll get the ASCII data converted to Hex (in case you don't see the Convert ASCII button on screen, try clicking on free space and after detecting ASCII in the window, it should pop up).

Parsomatic

Version 1.0.9

Parses ID TECH card-reader data streams from AR, GR, NEO, and NGA devices.

To use: Paste data into text area, then type **Enter**. Parsed data will appear underneath the text area. Hover the mouse over color-coded areas to see an explanation of the hex values. Optionally use the tag lookup feature (below) to look up tags at any time.

Tag lookup (e.g. **9F6D**):

Tag	Name	Description
-----	------	-------------

Paste reader data here, then hit ENTER:

```
02ED01801F4C2800839B252A363031302A2A2A2A2A2A383736355E3032
35342F534552564943455245434F564552595553445E2A2A2A2A2A2A
2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A
2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A
3F2A95025C86987E4F7DD07D58730EB79FDFB90AB7F23E6ECA6F4F04A67BF5
11E13F950903BDE77624680C460E9C36C4F9136256BB93A38CB98F95626DC
```

Show ASCII SHA-256 TLVs only

3. Click the "Parse" button to get the Hex data parsed correctly.

```

2A 2A 2A 38 37 36 35 5E 30 32 35 34 2F 53 45 52 56 49 43 45 52
45 43 4F 56 45 52 59 55 53 44 5E 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A
2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A
3F 2A 38 36 30 31 30 2A 2A 2A 2A 2A 2A 2A 2A 38 37 36 35 3D 2A
2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 3F 2A
Parse Clear Show ASCII SHA-256 TLVs only

```

```

02 ED 01 80 1F 4C 28 00 83 9B 25 2A 36 30 31 30 2A 2A 2A 2A 2A 2A
2A 38 37 36 35 5E 30 32 35 34 2F 53 45 52 56 49 43 45 52 45 43 4F 56
45 52 59 55 53 44 5E 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A
2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A
2A 2A 2A 2A 2A 2A 2A 2A 38 37 36 35 3D 2A 2A 2A 2A 2A 2A 2A 2A 2A
2A 2A 2A 2A 2A 2A 2A 2A 3F 2A 85 02 5C 86 98 7E 4F 7D 00 7D 56 73
0E B7 9F DF B9 0A 87 F2 3E 6E CA 6F 4F 04 A6 78 F5 11 EE 13 F9 50 90
3B DE 77 62 46 80 C4 60 E9 C3 6C 4F 91 36 25 6B B9 3A 38 CB 98 F9 56
26 DC FA F9 33 5C E0 A2 13 07 4C C1 CD 84 CC 91 13 98 E0 67 56 C4 64
AB 03 6B 69 42 28 AD A7 EC 01 8F 49 5A 01 3A F8 A0 4C 97 62 88 FE 2F
80 27 1E 6E 53 D9 87 DE 19 AC A2 70 78 FF 2C 78 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 36 31 33 54 35 33 35 36 31 38 62 99 49
00 75 00 02 A0 03 08 10 8E 03

```

STX	02
LENGTH	ED 01
Card Encode Type	80
Track Status (1F)	0----- 0-Reserved for future use -0----- 1: Field 10 "optional bytes length" exists (0: No Field 10) --0----- 1: Track 3 sampling data exists (0: Track 3 sampling data does not exist) ---1---- 1: Track 2 sampling data exists (0: Track 2 sampling data does not exist) ----1--- 1: Track 1 sampling data exists (0: Track 1 sampling data does not exist) -----1- 1: Track 3 decode success (0: Track 3 decode fail) -----1- 1: Track 2 decode success (0: Track 2 decode fail) -----1- 1: Track 1 decode success (0: Track 1 decode fail)
Track 1 Length	4C
Track 2 Length	28
Track 3 Length	00
Clear/Mask Data Sent Status (83)	1----- Bit 7: 1 - Serial Number present; 0-not present -0----- Bit 6: 1- PIN Encryption Key; 0-Data Encryption Key --0----- Bit 5: 1- Chip present on card. (First byte of service code was '2' or '6'.) Use EHV transaction if possible. ---0---- Bit 4: 0 - TDES; 1 - AES ----0--- Bit 3: 1- if fixed key; 0 DUKPT Key Management -----0-- Bit 2: 1- if Track3 clear/mask data present -----1- Bit 1: 1- if Track1 clear/mask data present -----1- Bit 0: 1- if Track1 clear/mask data present
Encrypted/Hash Data Sent Status (9B)	1----- Bit 7: if 1, KSN present -0----- Bit 6: if 1, session ID present --0----- Bit 5: if 1, track2 hash data (SHA digest) present ---1---- Bit 4: if 1, track2 hash data (SHA digest) present ----1--- Bit 3: if 1, track1 hash data (SHA digest) present -----0-- Bit 2: if 1, track3 encrypted data present -----1- Bit 1: if 1, track2 encrypted data present -----1- Bit 0: if 1, track1 encrypted data present
Track1 Data	25 2A 36 30 31 30 2A 2A 2A 2A 2A 2A 2A 2A 2A 38 37 36 35 5E 30 32 35 34 2F 53 45 52 56 49 43 45 52 45 43 4F 56 45 52 59 55 53 44 5E 2A 3F 2A
Track2 Data	3B 36 30 31 30 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 38 37 36 35 3D 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 3F 2A
Track1 Encrypted Data	95 02 5C 86 98 7E 4F 7D 00 7D 58 73 0E B7 9F DF B9 0A B7 F2 8E 6E CA 6F 4F 04 A6 7B F5 11 EE 13 F9 60 90 8B DE 77 62 46 80 C4 60 E9 C3 6C 4F 91 36 25 6B B9 3A 38 CB 98 F9 56 26 DC FA F9 33 5C E0 A2 13 07 4C C1 CD 84 CC 91 13 98 E0 67 56 C4 Decrypt
Track2 Encrypted Data	64 AB 03 6B 69 42 28 AD A7 EC 01 8F 49 5A 01 3A F8 A0 4C 97 62 88 FE 2F 80 27 1E 6E 53 D9 87 DE 19 AC A2 70 7B FF 2C 78 Decrypt this data
Track 1 Hashed	00 00
Track 2 Hashed	00 00
Reader Serial Number	36 31 33 54 35 33 35 36 31 38
KSN	62 99 49 00 75 00 02 A0 03 08
LCR	10
Checksum	8E
ETX	03

Related articles

- How to request an RMA number so I can return a unit (or units) for repair?
- How to re-initialize the MSR key after the VP5300 firmware upgrading?
- How to re-configure the SecureMag from the USB HID to the USB KB mode or vice versa?
- How to use the IDTECH SecureKey USB Demo to collect the required data for troubleshooting?
- How to control the Augusta output speed in QC USB KB mode?