

Der Tiptoi-Stift

Spielzeug Reverse Engineering

Joachim Breitner

GPN 15, 6.6.2015



Was ist der Tiptoi-Stift

The image shows the packaging for the Tiptoi Starter-Set. It features a photograph of a young girl in a red jacket using an orange Tiptoi stylus on an open book. A young boy is looking on. The book is titled 'Bauernhof' (Farm) and has a colorful illustration of a farm scene. The Tiptoi stylus is shown emitting concentric green circles, indicating its interactive capabilities. The packaging includes the Tiptoi logo, the text 'macht Wissen lebendig' (makes knowledge alive), and 'Starter-Set mit Stift und Buch!'. It also mentions 'MIT OJD TECHNOLOGIE' and '4-7 Jahre'. A small inset shows the book's cover with the title 'Bauernhof' and a question 'Wieso? Weshalb? Warum?'. The Ravensburger logo is visible in the bottom right corner.

tiptoi®
macht Wissen lebendig

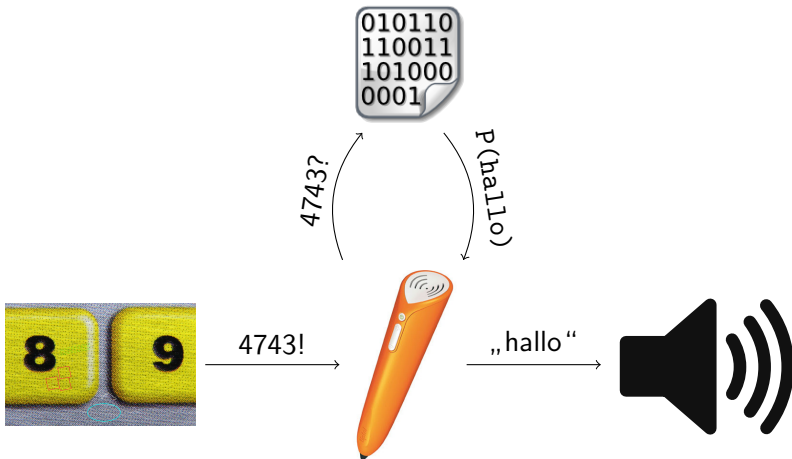
Starter-Set
mit Stift und Buch!

MIT OJD
TECHNOLOGIE

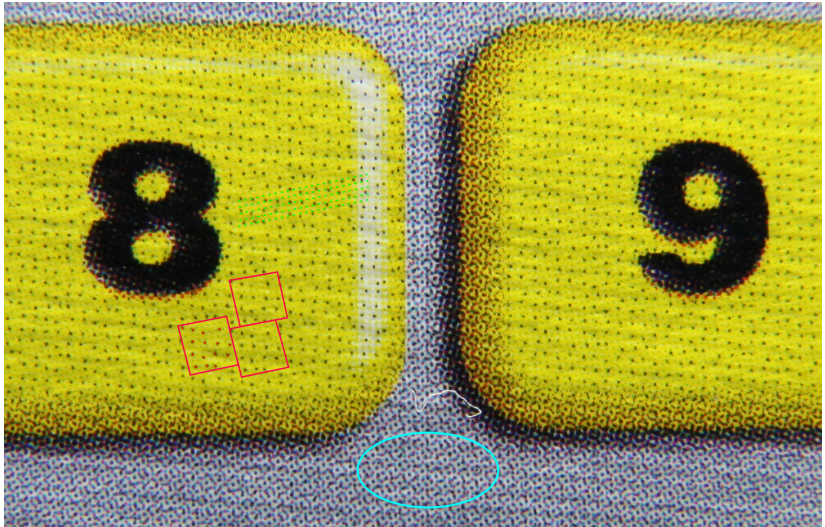
4-7
Jahre

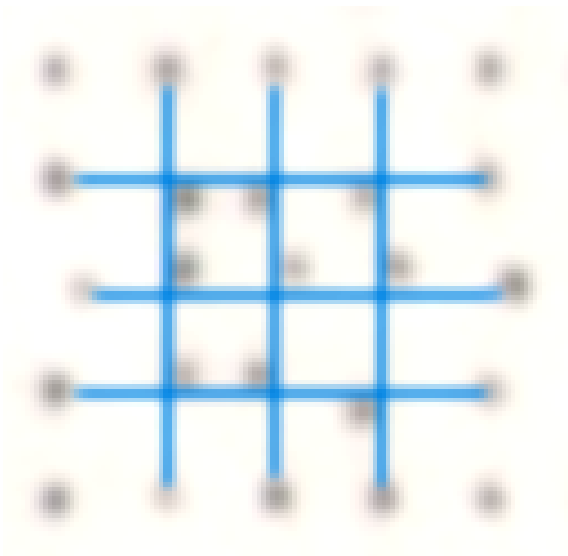
**Das audiodigitale Lernsystem
für Bücher und Spiele**

Ravensburger



Der Code





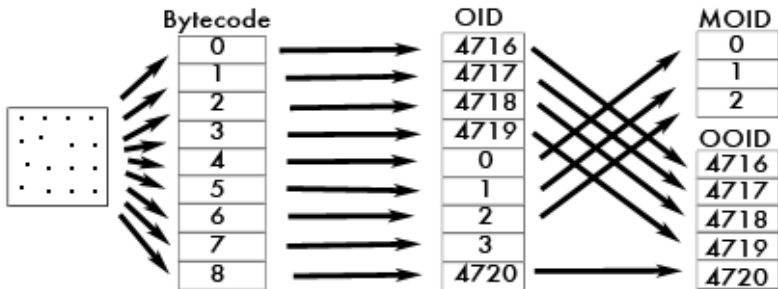
(1 × 1mm, also 600 bis 1200 dpi nötig)

(Oid-Decoder)

1	一	[i]	6	六	[lio]
2	二	[ahr]	7	七	[tschi]
3	三	[sä]	8	八	[pa]
4	四	[sè]	9	九	[tschiou]
5	五	[uoh]	0	零	[liin]

(An und - Gleichzeitig, dann +)

Die mysteriöse Tabelle



Medien und Objekt-IDs

Medien-IDs

0
1
2
:
?

Sprach-IDs

?
:
997
998
999

Objekt-IDs

1000
1001
1002
1003
1004
1005
1006
:

GME-Datei

```
00000000: 0002 0000 1d72 0800 8b23 0000 9901 0800 .....r...#.....
00000010: 9b01 0800 2d00 0000 2d4e 0800 3f00 0000 ....-...-N..?...
00000020: 3143 484f 4d50 5445 4348 2044 4154 4120 1CHOMPTECH DATA
00000030: 464f 524d 4154 2043 6f70 7952 6967 6874 FORMAT CopyRight
00000040: 2032 3030 3920 5665 7232 2e31 302e 3039 2009 Ver2.10.09
00000050: 3031 3230 3133 3132 3131 0000 0000 0000 0120131211.....
00000060: 95b7 0800 0000 0000 0000 0000 0000 0000 .....
00000070: 0021 4e08 0000 0000 0000 0000 0000 0000 .!N.....
00000080: 0000 0000 0000 0000 0000 0000 614f 0800 .....a0..
00000090: 0dc5 ef03 8ddf f003 b5df f003 0000 0000 .....
000000a0: fda5 ef03 0100 0000 a9c0 f003 0000 0000 .....
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000100: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000110: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000120: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000130: 0000 0000 0000 0000 0000 0000 0000 0000 .....
```

...

Was jetzt alles geht

- GME-Dateien analysieren („disassembeln“).
- Darin Logik ändern und Audio-Dateien austauschen.
- Existierende Tiptoi-Produkte komplett neu vertonen.
- Komplette eigene Tiptoi-Werke gestalten.



- Die in der Firmware eingebaute Spiellogik benutzen.
- In die GME-Dateien ARM-Binary-Code einbetten.
- Daher auch kein verlustfreies Round-Tripping

<http://tttool.entropia.de/>

sowie

Workshop um 14:30.

© 2015 Joachim Breitner.

Distributed under the terms of the Creative Commons Attribution license.

Title image, Digitalpapier: by Schwesterschlumpf, © 2013, CC-by-sa

Binary icon: by Darth_Stabro, 2010, CC-by-sa

oid-Code: Thomas, <http://www.mikrocontroller.net/topic/214479>

oid-Schaubild: Alexander H, <http://www.mikrocontroller.net/topic/214479>