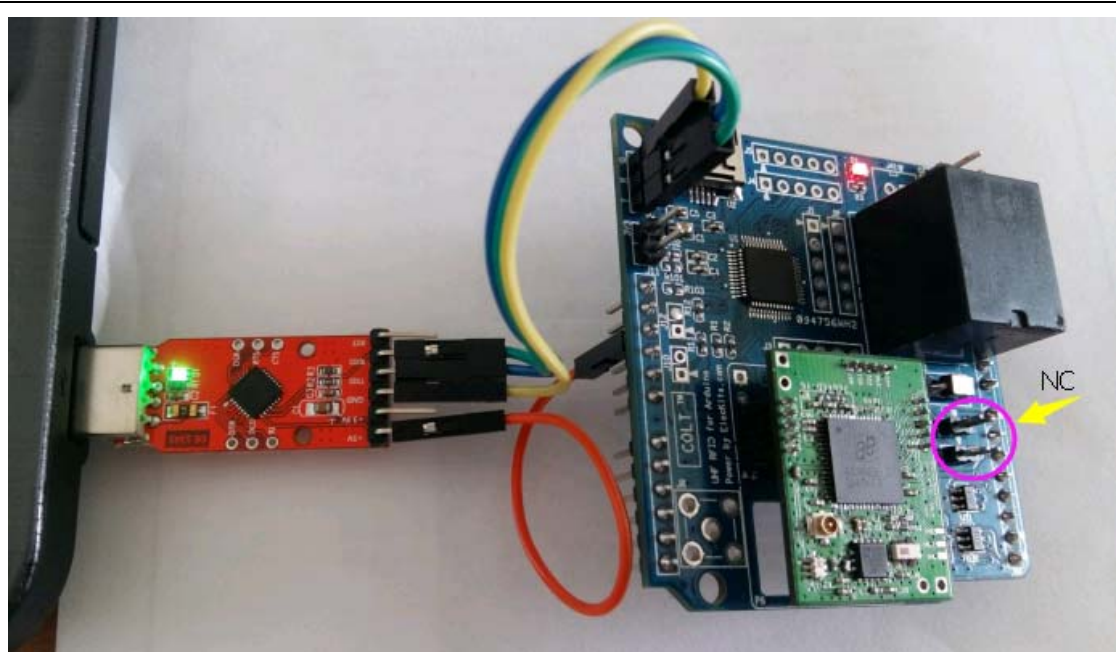


超高频 RFID 读写器读写电子标签的详解

本文主要针对 UHF RFID 读标签数据和写标签数据功能，进行实现和总结。

【硬件部分】:

- 1) [\[url=https://item.taobao.com/item.htm?id=15138367983\]](https://item.taobao.com/item.htm?id=15138367983)Eleckits Roger UHF RFID reader module[/url]
- 2) [\[url=https://item.taobao.com/item.htm?id=521665332439\]](https://item.taobao.com/item.htm?id=521665332439)Eleckits Colt UHF RFID reader module[/url]
- 3) [\[url= https://item.taobao.com/item.htm?id=13640879646\]](https://item.taobao.com/item.htm?id=13640879646) 902 ~ 928MHz 3dBi UHF RFID PCB Antenna[/url]
- 4) [\[url=https://item.taobao.com/item.htm?id=23426460127\]](https://item.taobao.com/item.htm?id=23426460127) 902 ~ 928MHz 5dBi UHF RFID PCB Antenna[/url]
- 5) [\[url=https://item.taobao.com/item.htm?id=22075632296\]](https://item.taobao.com/item.htm?id=22075632296) 902~928MHz 8dBi UHF RFID 右旋圆极化天线[/url]
- 6) [\[url= https://item.taobao.com/item.htm?id=39050409921\]](https://item.taobao.com/item.htm?id=39050409921) USB to uart TTL Adapter[/url]
- 7) [\[url= https://item.taobao.com/item.htm?id=39030802360\]](https://item.taobao.com/item.htm?id=39030802360)EPC UHF G2 电子标签（18000-6C）[/url]



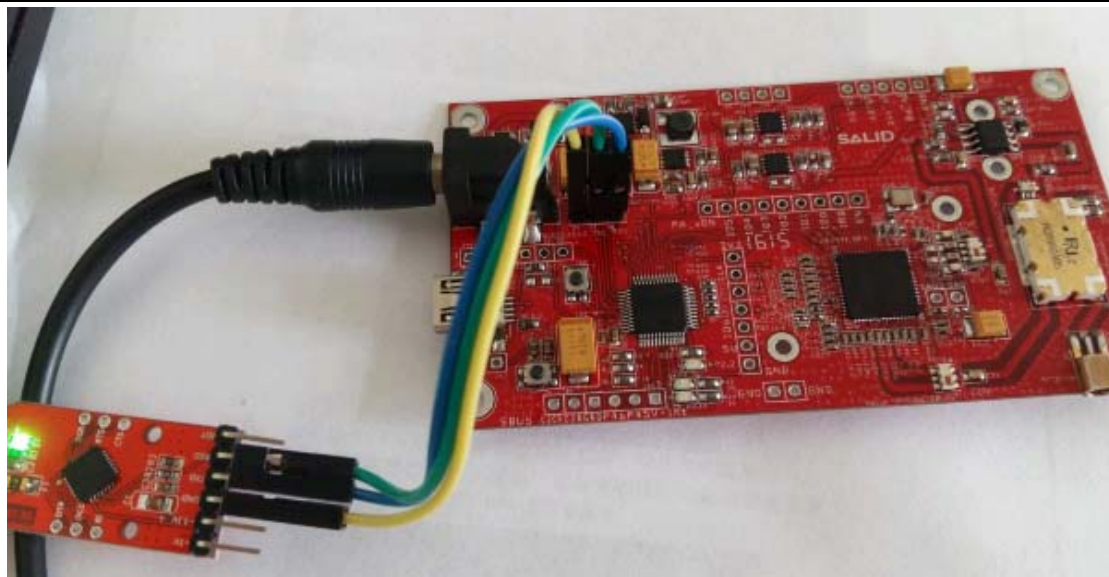
Colt / MIRCO 读写器串口版本连线方式:

1、需要 4 根线，分别连接 5V，TX，RX，GND;

Colt 模块 USB2TTL 转接板

GND ——— GND
T ——— RXD
R ——— TXD
5V (倒数第 3 脚) ——— +5V

- 2、注意 Colt 板上的 J21、J22 两个跳线帽需要取下；
- 3、Colt / Mirco 只需要 USB 5V 供电即可，无需其他供电；
- 4、Colt / Mirco 配套天线标准接口为 IPEX；



Roger 读写器串口版本连线方式：

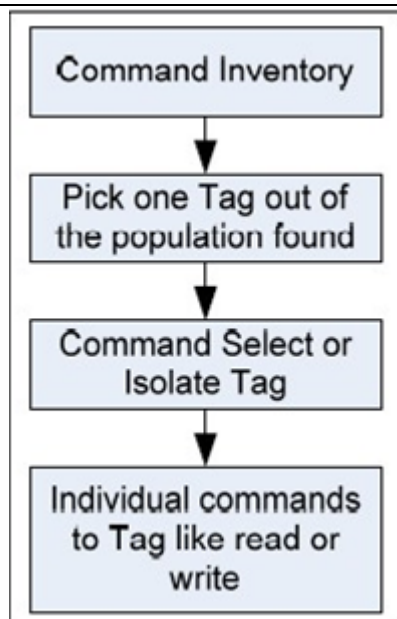
- 1、需要 3 根线，分别连接 TX, RX, GND；

Roger 模块 USB2TTL 转接板

GND ——— GND
TXD ——— RXD
RXD ——— TXD

- 2、Roger 需要一个独立的 **3.7V 2A** 外部电源供电；
- 3、Roger 配套天线标准接口为 MMCX 公头；

要读写标签需要先用 Command Inventory 和 Command Select or Isolate Tag 两个指令选择好你要读写的某个标签（即使读写区域只有一个标签），然后使用读/写标签指令，见下图：



a) 先用 GEN2 标签识别指令（有两个）

Command Inventory :

主机——》读写器

Byte 0/ID	Byte 1	Byte 2
0x31	Frame Length	Start inventory(0x01) / Next tag information(0x02)

读写器——》主机

Byte 0/ID	Byte 1	Byte 2	Byte 3	Byte 4-Byte xx	Byte xx+1..Byte 63
0x32	Frame length	Number of found tags	Length of EPC byte	EPC 1...x	rfu

例如，发送：31 03 01

接收：32 04 00 00

表示未识别到标签

32 12 01 0E 34 00 01 02 03 04 05 06 07 08 09 10 11 23

表示识别到标签，EPC:

01 02 03 04 05 06 07 08 09 10 11 23

Command Inventory with RSSI :

主机——》读写器

Byte 0/ID	Byte 1	Byte 2
0x43	Frame Length	Start inventory (0x01) / Next tag information(0x02)

读写器——》主机

Byte 0/ID	Byte 1	Byte 2	Byte 3	Byte 4~6	Byte 7	Byte 10..Byte 21
0x44	Frame length	Number of found tags	RSSI	frequency	Length of EPC byte and PC byte	EPC

例如，发送：43 03 01

接收：44 05 00 00 00

表示未识别到标签

44 16 01 90 A4 35 0D 0E 34 00 01 02 03 04 05 06 07 08 09 10 11 23

表示识别到标签，EPC：01 02 03 04 05 06 07 08 09 10 11 23

44·16·01·90·A4·35·0D·0E·34·00·01·02·03·04·05·06·07·08·09·10·11·23

注：

90——RSSI

A4 35 0D——工作频率 0D<<16 | 35<<08 | A4 = 0xD35A4=865700KHz=865.7MHz（欧洲频率）

34 00——PC，电子标签的协议-控制字

b) 选标签指令

主机——》读写器

Byte 0	Byte 1	Byte 2	Byte 3	Byte n+4	Byte n+5...byte 63
Report ID 0x33	Frame length	Length of EPC mask	EPC byte 0	EPC byte n	ruf

读写器——》主机

Byte0/ID	Byte1	Byte2
0x34	Frame length	Error byte

例如，要选中 EPC 为 01 02 03 04 05 06 07 08 09 10 11 23 的标签

发送：33 0F 0C 01 02 03 04 05 06 07 08 09 10 11 23

接收：34 03 09

表示此标签无法读写

34 03 00

表示可以读写此标签了（Error byte 为 0x00 表示 No error）

c) 写标签指令

主机——》读写器

Byte 0	Byte1	Byte2	Byte3	Byte[4]— Byte[7]	Byte 8	Byte[9]— Byte[2*n+9]	Byte[2*n+10] ...Byte63
--------	-------	-------	-------	---------------------	--------	-------------------------	---------------------------

Report ID 0x35	Frame Length	Memory bank	Tag memory Address(in words)	Access Password (4 bytes Long)	Data length in words	Data[2×n]	rfu
-------------------	--------------	-------------	------------------------------	--------------------------------	----------------------	-----------	-----

读写器——》主机

Byte0/ID	Byte1	Byte2	Byte3
0x36	Frame length	Error byte	Number of words written

d) 读标签指令

主机——》读写器

Byte 0/ID	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5,6,7,8
0x37	Frame length	Memory bank	Tag memory Address(in words)	Data length in words	rfu

读写器——》主机

Byte 0/ID	Byte 1	Byte 2	Byte 3	Variable
0x38	Frame length	Error byte	Data length in words	Data[n]

读写的详细操作见后面。

注：详细操作指令见 RFID 读写器控制指令集

《UHF RFID 指令集和通讯协议-AS3992 protocol.pdf》

在应用电子标签进行系统应用前，用户需先详细了解 UHF 电子标签的功能、存贮结构以及操作命令。

1、 EPC G2 UHF 标准的接口参数

对于每间公司生产的符合 EPC G2 UHF 标准的电子标签，其功能和性能均应符合 EPC G2 UHF 相关无线接口性能的标准。从用户应用标签的角度来说，我们不需要详细了解该标准的各项参数以及读写器与电子标签之间的无线通信接口的协议。但对以下参数有一个大致的了解，对于用户应用电子标签会有较大的帮助。

以下为 EPC G2 UHF 物理接口概念以及其简要说明，以帮助用户对标准有一个了解。详细说明请参考 EPC G2 UHF 标准文本。

系统介绍

EPC 系统是一个针对电子标签应用的使用规范。一般系统包括有读写器、电子标签、天线以及上层应用接口程序等部份。每家厂商提供的产品应符合国家的相关标准，所提供的设备在性能上有不同，但功能会是相似的。

无线通信过程

读写器向一个或一个以上的电子标签发送访问命令信息，发送方式是采用无线通信的方式调制射频载波信号。标签通过相同的调制射频载波接收功率。

读写器通过发送未调制射频载波和接收由电子标签发射（反向散射）的信息来接收电子标签中的数据。

工作频率：920.125MHz—924.875MHz,20 个频道（国家标准）

865.7MHz—867.5MHz，4 个频道（欧洲标准）

902.75MHz—927.25MHz，50 个频道（美国标准）等

EPC G2 UHF 的标准文本所规定的无线接口频率为：860MHz—960MHz，但每个国家在确定自己的使用频率范围时，会根据自己的情况选择某段频率作为自己的使用频段。

我国目前暂订的使用频率为：920MHz—925MHz。

用户在选用电子标签和读写器时，应选用符合国家标准电子标签及读写器。一般来说，电子标签的频率范围较宽，而读写器在出厂时会严格按照国家标准规定的频率来限定。

频道工作模式：跳频扩频模式

读写器在有效的频段范围内，将该频段分为 20 个或 4 个或 50 个频段，在某个使用的时刻读写器与电子标签的通信只占用一个频道进行通信。为防止占用某个频道时间过长或该频道被其他设备占用而产生的干扰，读写器应用 FHSS 自动跳频技术动态跳到下一个频道。

用户在使用读写器时，如发现某个频道在某地已被其他的设备所占用或某个频道上的信号干扰很大，可在读写器系统参数设定中，先将该频道屏蔽掉，这样读写器在自动跳频时，会自动跳过该频道，以避免与其他设备的应用冲突。

发射功率：最大 2W

读写器的发射功率是一个很重要的参数。读写器对电子标签的操作距离主要由该发射功率来确定，发射功率越大，则操作距离越远。

我国的暂订标准为 2W，读写器的发射功率可以通过系统参数的设置来进行调整。可分为几级或连续可调，用户需根据自己的应用调整该发射功率，使读写器能在用户设定的距离内完成对电子标签的操作。对于满足使用要求的，将发射功率调到较小，会较少能耗。

天线：50Ω，范围为 900—930 MHz

天线是读写系统中非常重要的一部份，它对读写器与电子标签的操作距离有很大的影响。天线的性能越好，则操作距离可能会越远，操作的稳定性会更好。

天线的选择参数包括：天线增益，驻波比及天线的方向性和天线尺寸。一般应选择天线驻波比低的，应小于 1.5。用户在选用时需作较多的关注。

读写器与天线的连接有二种情况，一种是读写器与天线装在一起，称为一体机，另一种是通过 50Ω 的同轴电缆与天线相连，称为分体机。

一个读写器可以同时连接多个天线或只有一个天线，在使用这种含多个天线的读写器时，用户需先设定天线的使用顺序。

密集读写器环境（DRM）

在实际应用场合，可能会同时存在多个读写器在一个空间范围内同时运行，这种情况被称为密集读写器环境，各个读写器会占用各自的操作频道对自己的某类电子标签自行操作。用户在使用时，需根据需要选用可在 DRM 环境下可靠运行的读写器。

数据传输速率：读写器与标签之间交换数据，有高/低两种传输速率。对于一般的厂商提供的标签，我们都首先选择高速数据传输速率。

2、 电子标签的存储器结构

对于每个厂商生产的电子标签，其存储器的结构是相同的，但会存在存储器容量大小的差别。

2.1 电子标签存储器

从逻辑上来说，一个电子标签被分为四个存储体，每个存储体可以由一个或一个以上的存储器字（2 个字节）组成。其存储逻辑图为：

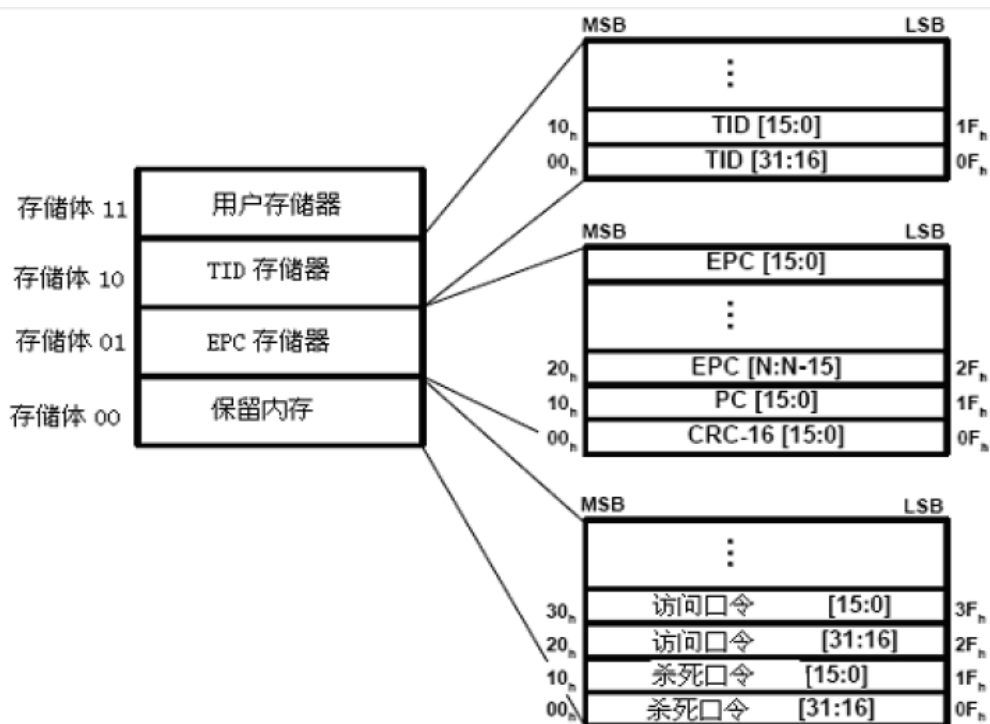


图 1：电子标签存储器结构图

从以上结构图中可以看到，一个电子标签的存储分为四个存储体，分别是：

存储体 0：保留内存（Reserver）

存储体 1：EPC 存储器（EPC）

存储体 2：TID 存储器（TID）

存储体 3：用户存储器（User）

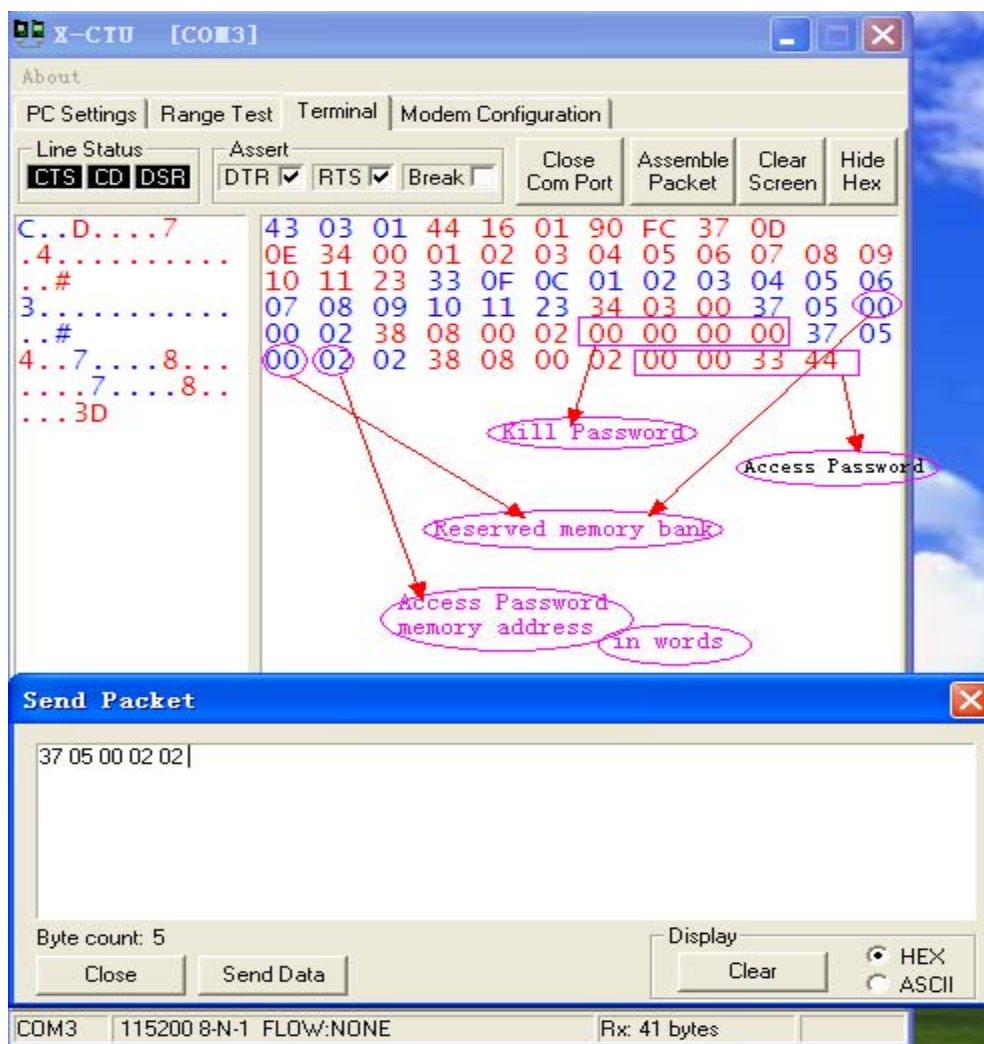
这四个存储体的定义是：

a) 保留内存 保留内存为电子标签存储密码（口令）的部分。包括灭活口令（Kill Password）和访问口令（Access Password）。

灭活口令和访问口令都为 4 个字节。

其中：灭活口令的地址为 00H—03H（以字节为单位）；

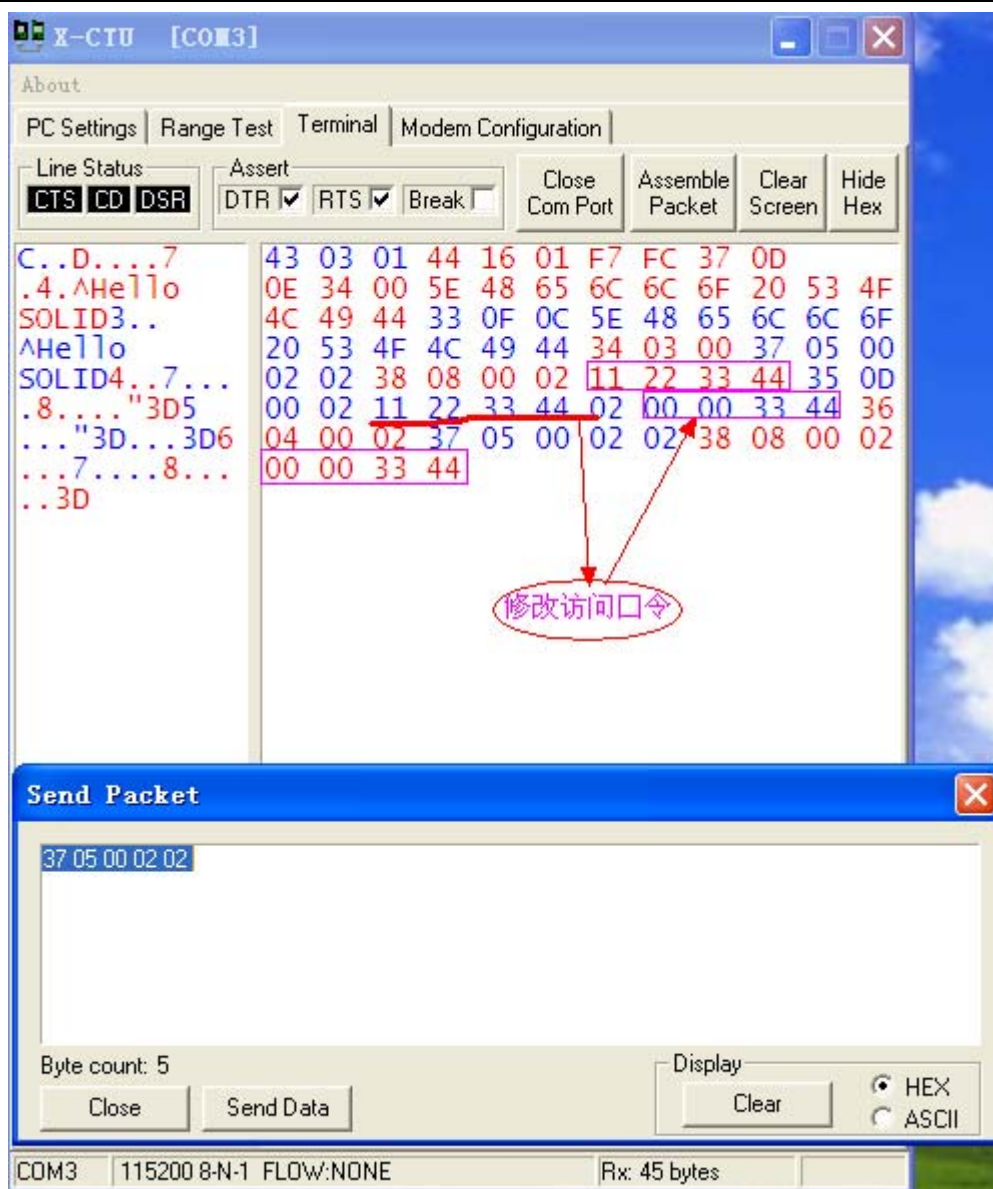
访问口令的地址为 04H—07H。



通常标签的初始访问口令默认为：00 00 00 00，在写标签时会需要这个口令。

你可以根据需要修改访问口令，如

将访问口令 11 22 33 44 改成 00 00 33 44



b) EPC 存储区 EPC 存储区用于存储电子标签的 EPC 编号、PC（协议-控制字）以及本存储块数据的 CRC—16 校验码。

其中：CRC—16：存储地址为 00—01H,2 个字节，CRC—16 为本存储体中存储数据的 CRC 校验码。

PC：电子标签的协议-控制字，存储地址为 02—03H，2 个字节。

PC 是指本电子标签的控制信息，包括如下内容：

PC 为 2 个字节，16 位，其每位的定义为：

00—04 位：电子标签的 EPC 号的数据长度

=00000₂: EPC 为零个字, 0 位

=00001₂: EPC 为一个字, 16 位

=00010₂: EPC 为二个字, 32 位

...

=11111₂: EPC 为 31 个字, 496 位

05—07 位: RFU=000

08—0F 位: =00000000₂

EPC 编号: 若干个字, 由 PC 的值来指定。

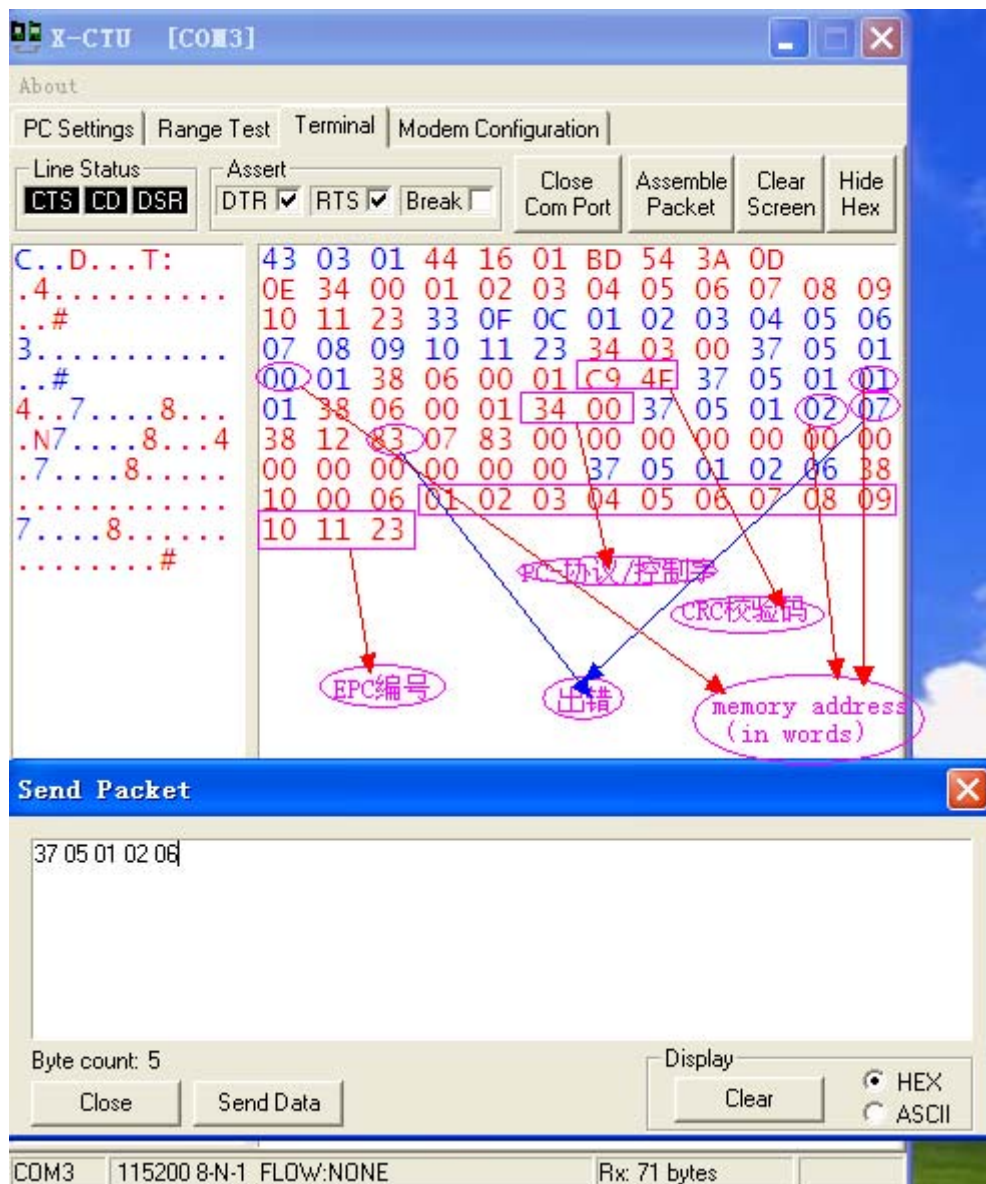
EPC 为本标签的编码。EPC 存储在以 **04H** 字节存储地址开始的 EPC 存储存储器内, **MSB 优先**。

每类电子标签(不同厂商或不同型号)的 EPC 号长度可能会不同。

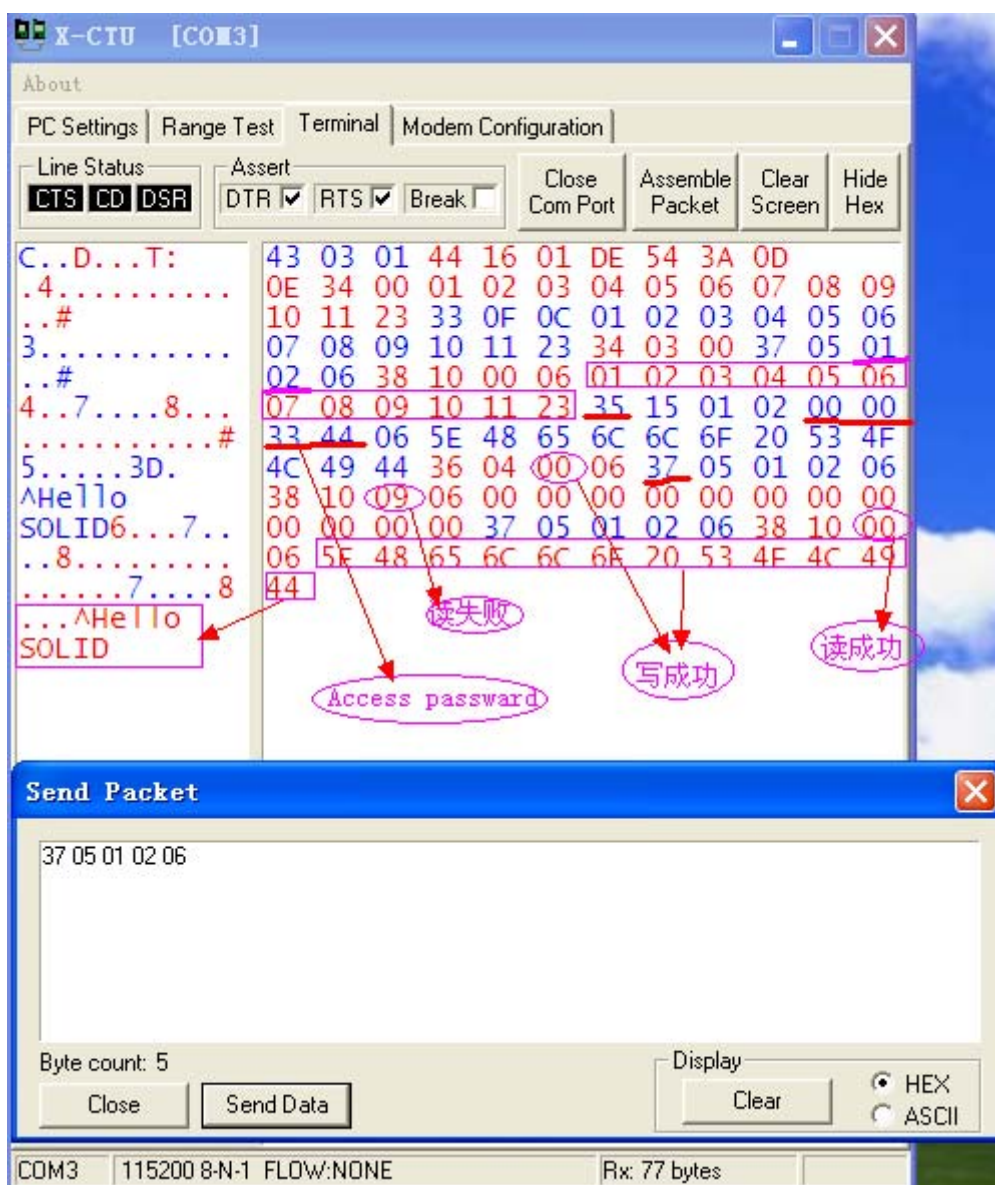
用户通过读该存储器内容命令读取 EPC 号。

在发行标签时, 可通过改写 **EPC 编号**, 使该值在系统中唯一, 以标明每个商品的 **ID 号**。

一般地, EPC 号为 96 位, 12 个字节。



修改 EPC，用写标签指令：

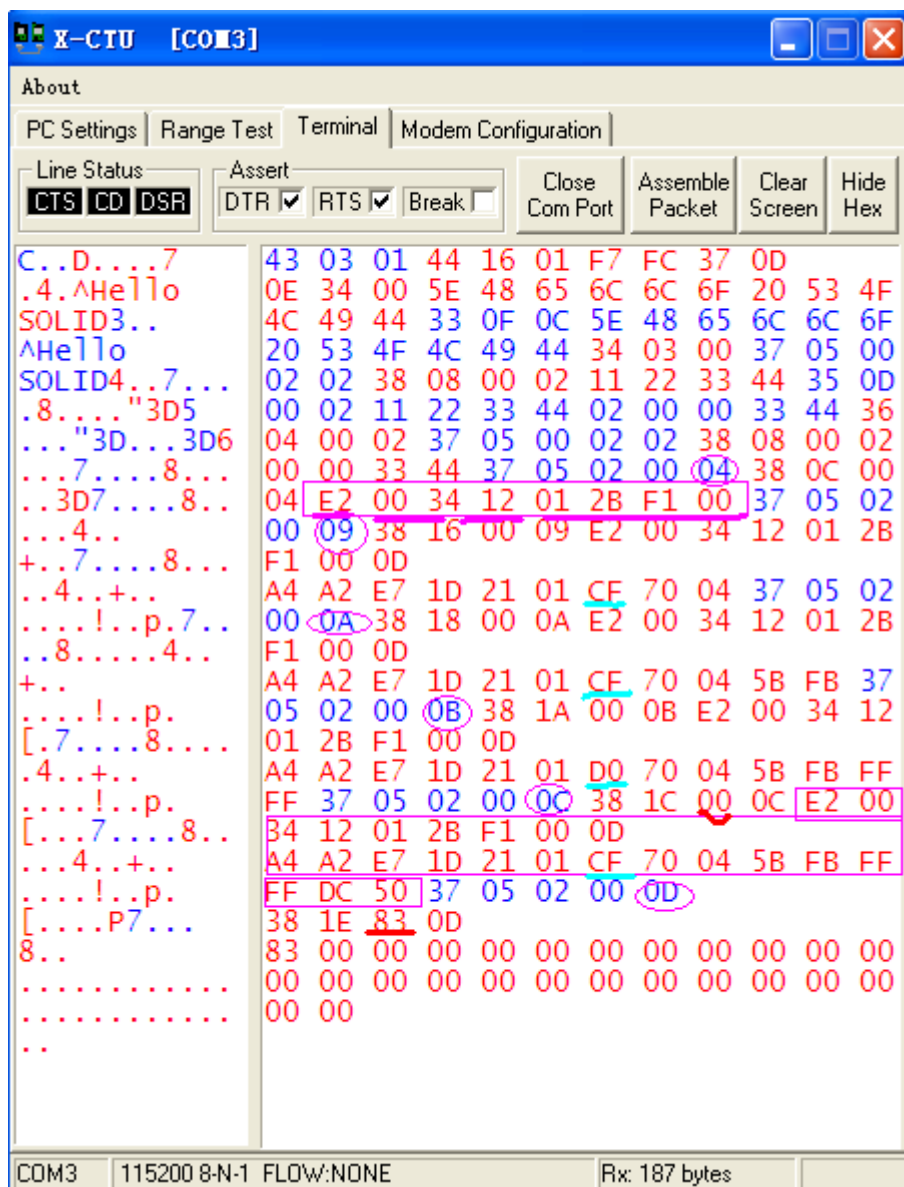


- c) **TID 存储器** 该存储器是指电子标签的产品类识别号,每个生产厂商的 TID 号都会不同。标签生产厂商会在该存储区中存储其自身的产品分类数据及产品供应商的信息。

一般来说, TID 存储区的长度为 4 个字, 8 个字节。但有些电子标签的生产厂商提供的 TID 区会为 2 个字或 5 个字。

该 TID 值在标签出厂时, 往往是有厂商写好, 用户无法再作修改。

用户在使用时, 需根据自己的需要选用相关厂商的产品。

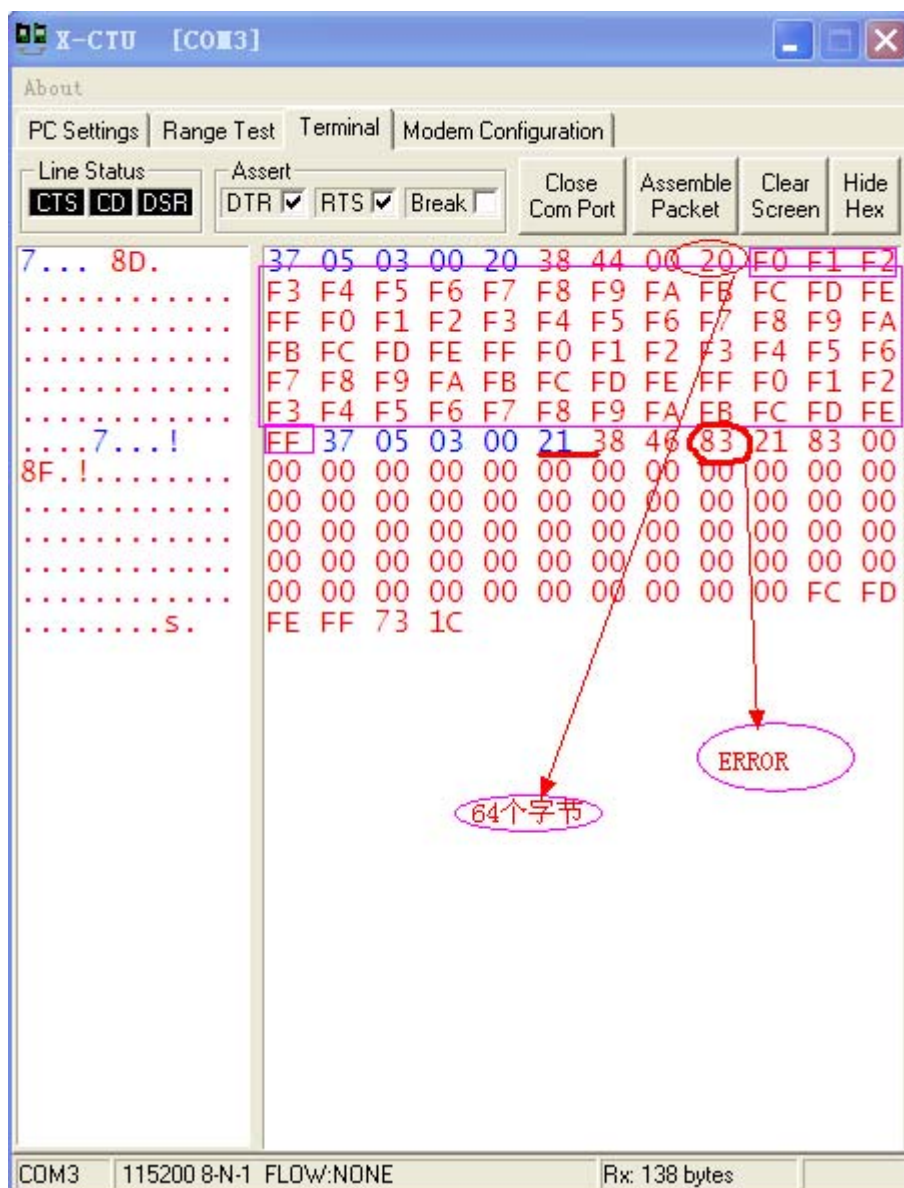


有 12 个字。

d) 用户存储器 该存储区用于存储用户自定义的数据。用户可以对该存储区进行读、写操作。

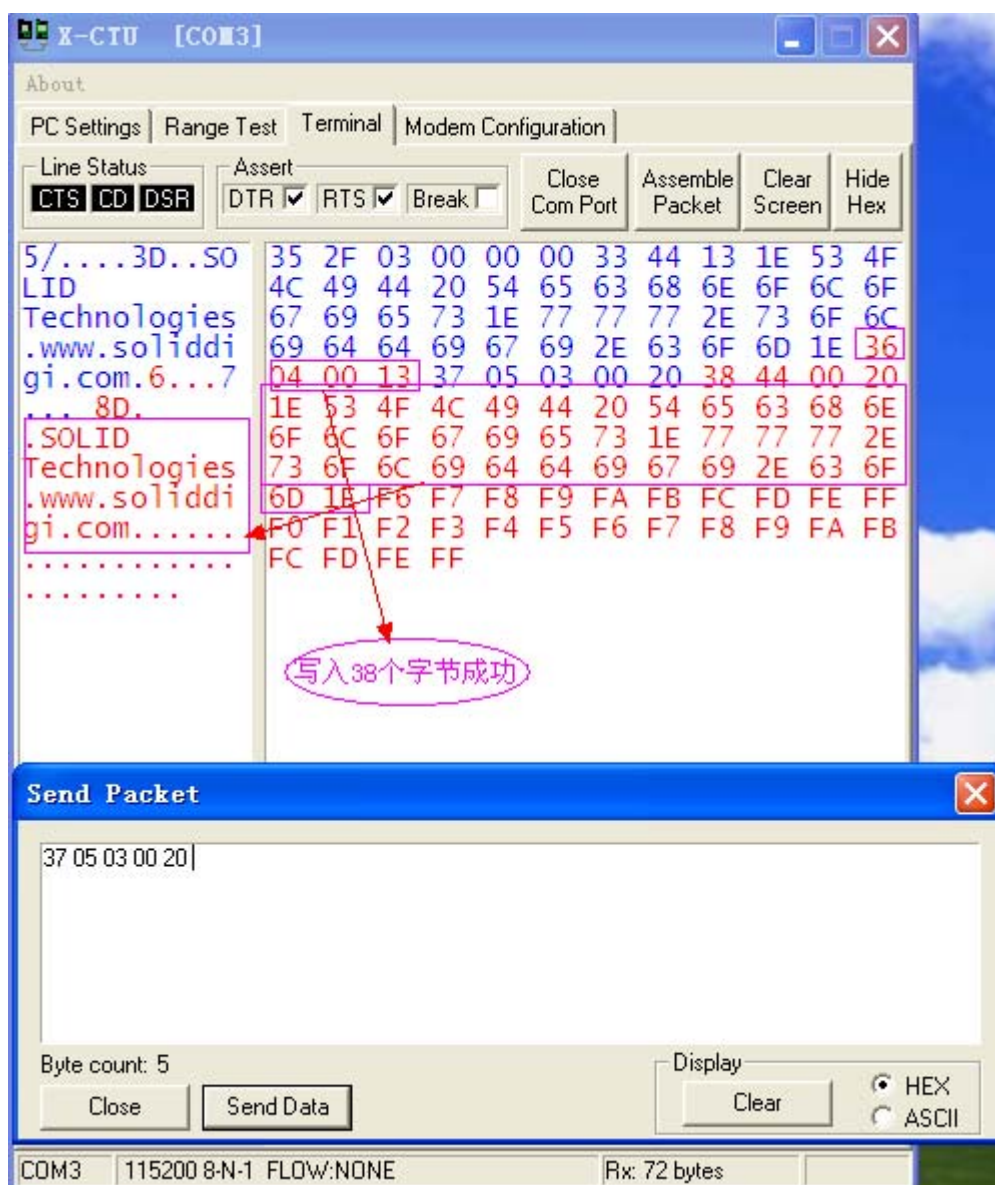
该存储器的长度由各个电子标签的生产厂商确定。每个生产厂商提供的电子标签，其用户存储区的容量会不同。存储容量大的电子标签会贵一些。用户应根据自身应用的需要，来选择符合要求的电子标签，以减低标签的成本。

许多电子标签为低成本的，可能会不包括该用户存储器。



可看出所用的标签用户存储器容量 64 字节。

向用户区写入数据，见下图：



用户区分块读取:

The screenshot shows the X-CTU [COM3] terminal window. The interface includes tabs for PC Settings, Range Test, Terminal, and Modem Configuration. The Terminal tab is active, displaying a hex dump and its corresponding ASCII representation. The hex dump starts at address 35 and ends at address FE. The ASCII representation shows the text "5/...3D..SO LID Technologies .www.soliddi gi.com.6...7 ... 8D. .SOLID Technologies .www.soliddi gi.com..... ..7... ..8*...SOLID Technologies .www.soliddi gi.com.7... 8..".

Annotations on the hex dump highlight the following values:

- Hex value **00** at address **13** (highlighted with a red circle).
- Hex value **13** at address **0D** (highlighted with a red circle).
- Hex value **13** at address **0D** (highlighted with a red circle).
- Hex value **13** at address **0D** (highlighted with a red circle).



Annotations on the ASCII representation highlight the following text:

- "..8*...SOLID Technologies .www.soliddi gi.com.7..." (highlighted with a red box).
- "8.." (highlighted with a red box).
- ".." (highlighted with a red box).

Annotations on the hex dump highlight the following text:

- "用户区第一个字节地址" (User area first byte address) pointing to the hex value **00** at address **13**.
- "13H+0DH=20H=32字, 即64个字节" (13H+0DH=20H=32 words, i.e. 64 bytes) pointing to the hex value **13** at address **0D**.
- "第39个字节地址" (39th byte address) pointing to the hex value **13** at address **0D**.

The status bar at the bottom shows "COM3", "115200 8-N-1 FLOW:NONE", and "Rx: 144 bytes".

矽控电子	
	
微信公众号『矽控电子』	智能硬件 QQ 群: 273156182
http://iot.eleckits.com http://rfid.eleckits.com	
高速 PCB Layout 与制板 工控嵌入式 ARM 定制 UHF RFID 与物联网	