课程实验

课程名称 ： **RFID 原理与应用**
实验名称 ： **防碰撞和访问 ISO15693 卡**
学号 ： **21281280**
姓名 ： **柯劲帆**
班级 ： **物联网2101班**
指导老师 ： **赵帅锋**
日期 ： **2024年6月4日**

---

1. 实验环境准备

- **RFID HF Reader 硬件**：MSP370 + TRF7970
- **实验 PC**：Windows 11 笔记本
- **实验软件**：HF.exe

PC 和 RFID HF Reader 通过 USB 口连接，但软件接口其实是 UART 。Reader 端使用 CH340，CH340 和 CPU 通过 UART 连接，对外提供 USB 接口，PC 端安装 CH340 的驱动程序，当 Reader 连接到 USB 口上后，PC 会发现一个 COM 端口，软件使用该 COM 口和 Reader 进行通信。

使用 HF.exe 连接 RFID HF Reader。

2. 命令帧分析

在实验软件的日志框中可以看到 Reader 发送的命令，其帧结构如下：

表 2-1

	SOF	Flag	Cmd	Arguments	Data	CRC16	EOF
长度		8 bits	8 bits			16 bits	

对于 `Flag` 值和 `Cmd` 值，将在以下两节中论述。

对于 `Arguments` 和 `Data` 值，具体见每一个命令。

2.1. Flag 值

对于 8 bits 的 `Flag` 值，其结构定义如下：

表 2-2

位 (bit)	标志名称	值描述	备注
b1	副载波	`0` - VICC 应使用单个副载波频率；`1` - VICC 应使用两个副载波频率	对应 `Request Flag` 框中 `Sub_carrier`
b2	数据速率	`0` - 低速率数据；`1` - 高速率数据	对应 `Request Flag` 框中 `HighData_rate`
b3	目录	`0` - 第 5 到 8 位按照表 A 规定；`1` - 第 5 到 8 位按照表 B 规定	
b4	协议扩展	`0` - 无协议格式扩展；`1` - 协议格式已扩展（保留供以后使用）	

`Flag` 值的第 5 到 8 位依据第 3 位指定，由以下的 A 表或 B 表规定：

- A 表：

表 2-3

位 (bit)	标志名称	值描述	备注
b5	选择	`0` - 根据寻址标志设置，请求将由任何 VICC 执行；`1` - 请求只由处于选择状态的 VICC 执行，寻址标志应设置为 0，UID 域应不包含在请求中	对应 `Request Flag` 框中 `Select`
b6	寻址	`0` - 请求没有寻址。不包括 UID 域。可以由任何 VICC 执行；`1` - 请求有寻址。包括 UID 域。仅由那些自身 UI 与请求中规定的 UID 匹配的 VICC 才能执行	对应 `Request Flag` 框中 `Addressed`

位 (bit)	标志名称	值描述	备注
b7	选择权	`0` - 含义由命令描述定义。如果没有被命令定义，它应设置为0；`1`- 含义由命令描述定义	
b8	RFU	固定为 `0`	

- B 表：

表 2-4

位 (bit)	标志名称	值描述	备注
b5	AFI	`0` - 无指定 AFI 域；`1` - 指定 AFI 域	对应 `Request Flag` 框中 `AFI is present`
b6	Nb_slots	`0` - 有 16 个 slots；`1`- 有 1 个 slots	对应 `Request Flag` 框中 `One_slot`
b7	选择权	`0` - 含义由命令描述定义。如果没有被命令定义，它应设置为0；`1`- 含义由命令描述定义	
b8	RFU	固定为 `0`	

2.2. Cmd 值

对于 8 bits 的 `Flag` 值，其值定义如下：

表 1-5

命令编码	类型	功能
'01'	强制的	目录
'02'	强制的	保持静默
'03' - '1F'	强制的	RFU
'20'	可选的	读单个块
'21'	可选的	写单个块
'22'	可选的	锁定块
'23'	可选的	读多个块
'24'	可选的	写多个块
'25'	可选的	选择
'26'	可选的	复位准备
'27'	可选的	写 AFI

命令编码	类型	功能
'28'	可选的	锁定 AFI
'29'	可选的	写 DSFID
'2A'	可选的	锁定 DSFID
'2B'	可选的	获取系统信息
'2C'	可选的	获取多个块安全状态
'2D' - '9F'	可选的	RFU
'A0' - 'DF'	定制的	IC Mfg 决定
'E0' - 'FF'	私有的	IC Mfg 决定

2. Inventory 命令

`Inventory` 命令用于清点射频场中的卡片。

2.1. 工作原理

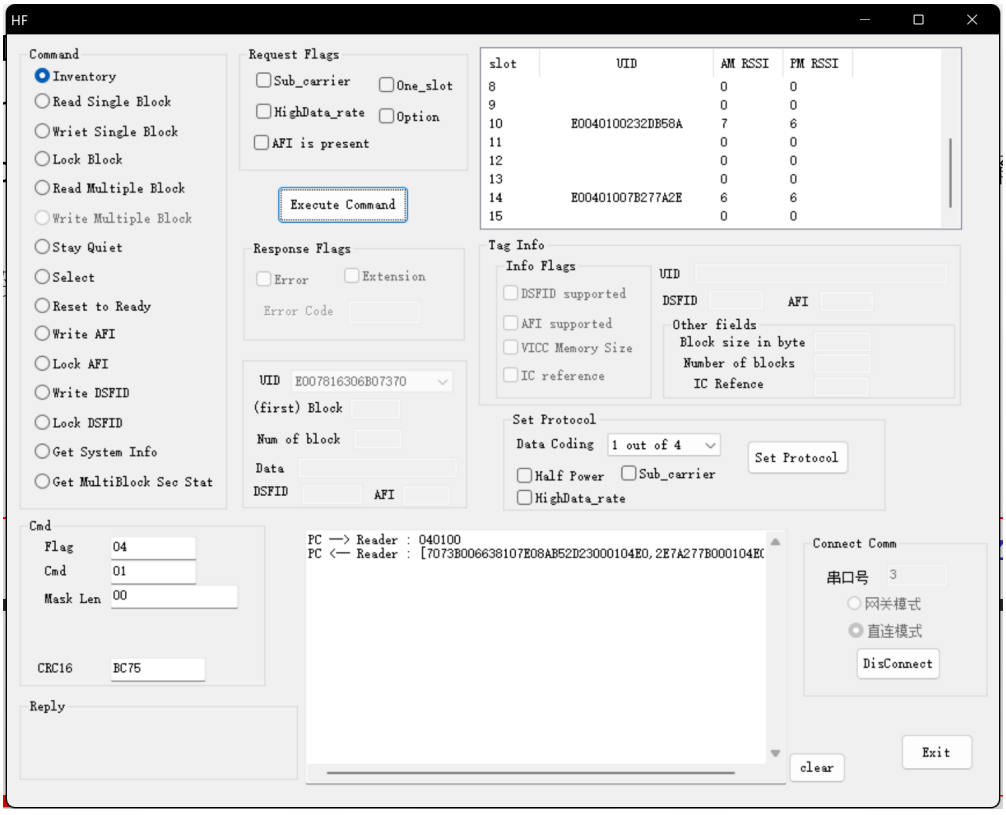
`Inventory` 命令工作原理如下：

- **发送请求**：读写器向射频场中的所有卡片发送一个 `Inventory` 请求命令。
- **范围响应**：指定一个叫号范围（例如0-15），卡片根据序列号最低4位（0000-1111）逐一响应。
- **无冲突响应**：如果某个序列号响应时没有冲突（即只有一张卡片响应），该卡片的序列号（UID）被记录在读写器中。
- **帧结束标志**：读写器发送帧结束标志，通知下一组卡片响应。例如，最低4位为0000的卡片响应后，发送帧结束标志，通知最低4位为0001的卡片响应。
- **重复过程**：重复发送帧结束标志，依次让最低4位为0000到1111的卡片响应，直到所有范围内的卡片都被询问一遍。
- **选择卡片**：在某个响应过程中，如果没有发生冲突，读写器就可以选择该张卡片进行进一步操作。

2.2. 实验过程

将 3 张 ISO I5693 的卡片放到 RFID HF Reader 的射频区域上方。

选择 `Command` 区域中的 `Inventory`，点击 `Execute Command` 按钮。



`Cmd` 区域自动填充命令，日志框中打印 PC 向 Reader 发送了命令 `040100`，PC 收到 Reader 返回的数据。

右上角卡片信息区域显示出 3 张卡，分别为 `E007816306B07370`、`E0040100232DB58A` 和 `E00401007B277A2E`，其最后一个字节并未冲突，分别占据 slot 0、slot 10 和 slot 14。

2.3. 命令帧数据分析

日志框中发送的数据为 `040100`，依照表 2-1：

	SOF	Flag	Cmd	Mask Len	Mask Value	CRC16	EOF
值		`04`	`01`	`00`	-	`BC75`	

- 对于 `Flag` = `04`

  依照表 2-2：

位（bit）	标志名称	值	值描述
b1	副载波	0	VICC 应使用单个副载波频率
b2	数据速率	0	低速率数据
b3	目录	1	第 5 到 8 位按照表 B 规定
b4	协议扩展	0	无协议格式扩展

  和表 2-4：

位（bit）	标志名称	值	值描述
b5	AFI	0	无指定 AFI 域
b6	Nb_slots	0	有 16 个 slots
b7	选择权	0	含义由命令描述定义
b8	RFU	0	固定为 `0`

- 对于 `Cmd` = `01`

  依照表 2-5，表示这是一条目录命令，即为 `Inventory` 命令。

- 对于 `Mask Len` = `00`

  对于一开始查找，`Mask Len` 肯定等于 `00`；查找后发现射频场中的所有卡的最低位并未冲突，所以不需掩蔽任何位。

3. Select 命令

3.1. 工作原理

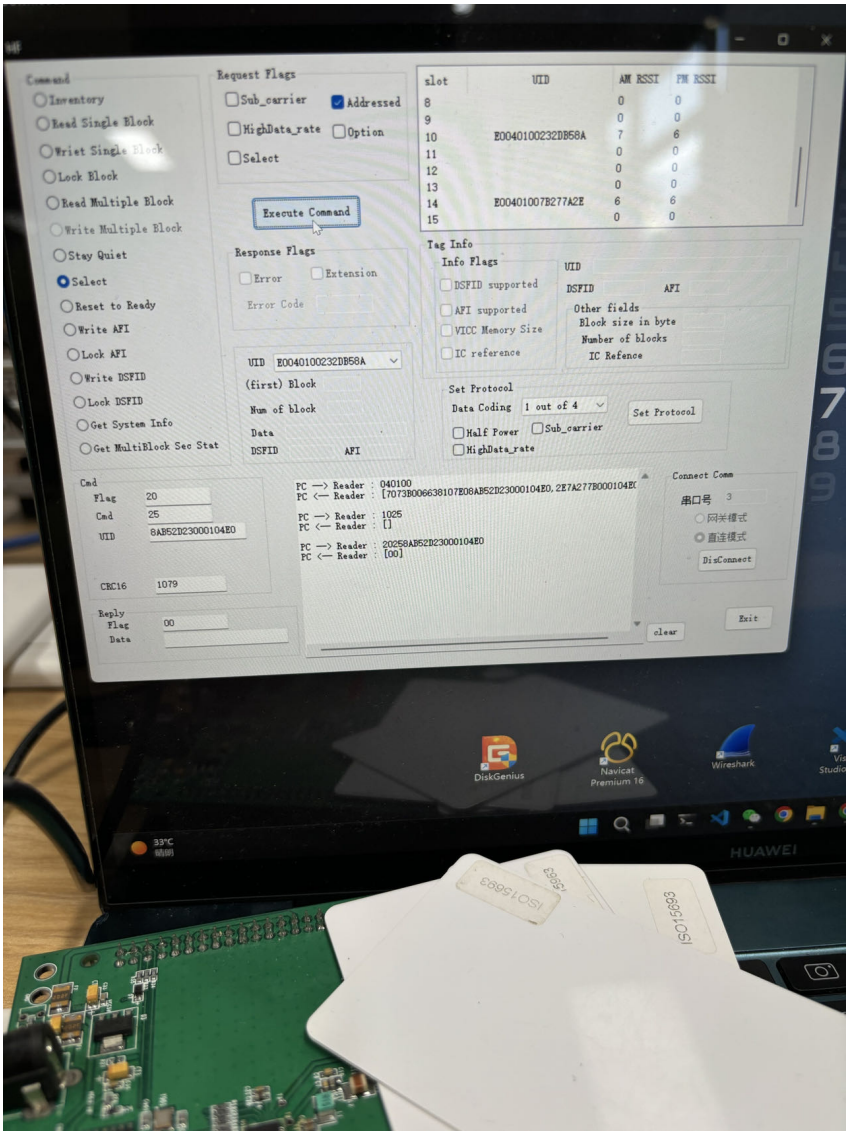
`Select` 命令的工作逻辑如下：

1. **选择标签**：通过 `SELECT` 命令选择一个标签（VICC）。
2. **进入选中状态**：被选中的标签进入 `selected` 状态，确保只有一个标签处于 `selected` 状态。
3. **后续命令指定**：之后发送的命令会直接针对这个处于 `selected` 状态的标签。
4. **响应所有命令**：该标签可以响应所有带有 `select` 或 `addr/uid` 标志的命令。

这种机制确保了特定标签在被选中后可以被直接通信，避免了与其他标签的冲突。

3.2. 实验过程

1. 选择 `Command` 区域中的 `Select`；
2. 勾选 `Request Flags` 区域中的 `Addressed`；
3. 在 `UID` 复选框中选择 `E0040100232DB58A`；
4. 点击 `Execute Command` 按钮。



`Cmd` 区域自动填充命令，日志框中打印 PC 向 Reader 发送了命令 `20258AB52D23000104E0`，PC 收到 Reader 返回的数据 `00`，表示成功选择。

3.3. 命令帧数据分析

日志框中发送的数据为 `20258AB52D23000104E0`：

	SOF	Flag	Cmd	UID	CRC16	EOF
值		`20`	`25`	`8AB52D23000104E0`	`1079`	

- 对于 `Flag` = `20`

  依照表 2-2:

位（bit）	标志名称	值	值描述
b1	副载波	0	VICC 应使用单个副载波频率
b2	数据速率	0	低速率数据
b3	目录	0	第 5 到 8 位按照表 A 规定
b4	协议扩展	0	无协议格式扩展

  和表 2-3:

位 (bit)	标志名称	值	值描述
b5	选择	0	根据寻址标志设置，请求将由任何 VICC 执行
b6	寻址	1	请求有寻址。包括 UID 域。仅由那些自身 UI 与请求中规定的 UID 匹配的 VICC 才能执行
b7	选择权	0	含义由命令描述定义
b8	RFU	0	固定为 `0`

- 对于 `Cmd` = `25`

  依照表 2-5，表示这是一条选择命令，即为 `Select` 命令。

- 对于 `UID` = `8AB52D23000104E0`

  它是 `UID` = `E0040100232DB58A` 的小端字节序。

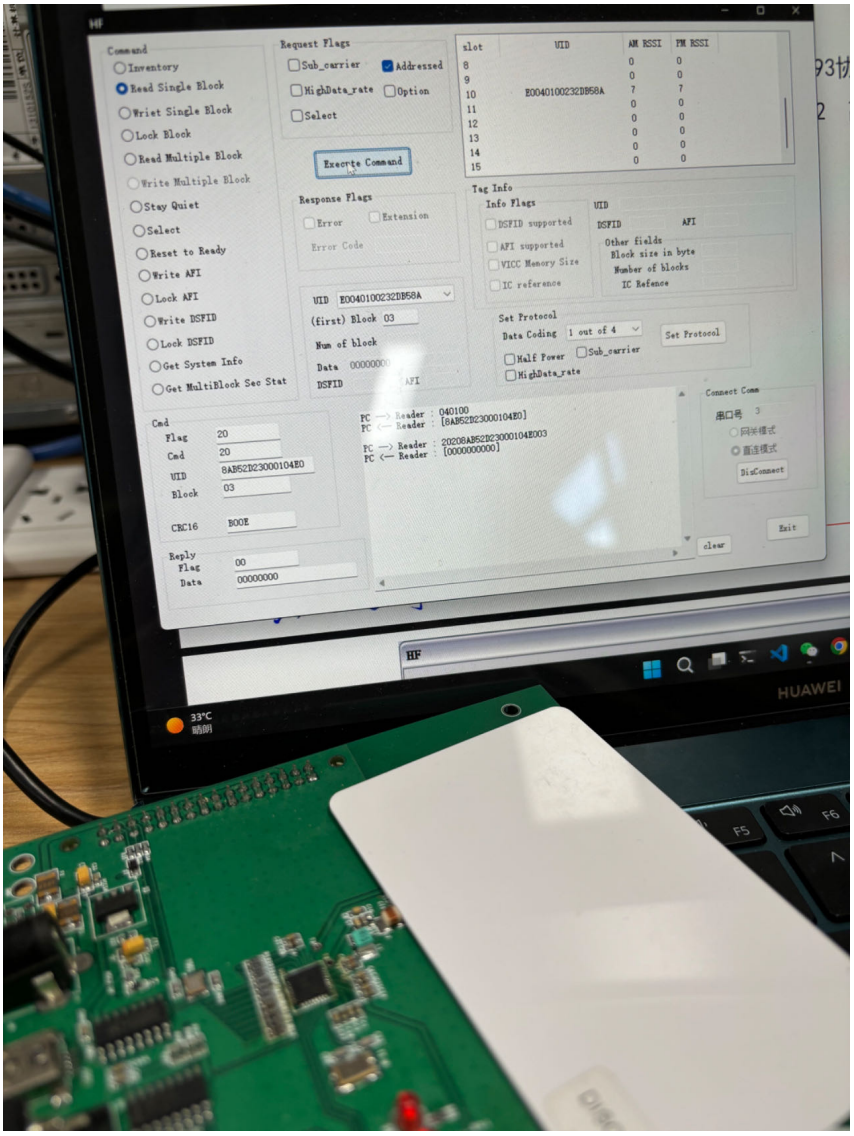
4. Read Single Block 命令

查询指定卡中的指定块中的数据。

4.1. 实验过程

将单张 ISO I5693 的卡片放到 RFID HF Reader 的射频区域上方，经过 `Inventory` 识别后：

1. 选择 `Command` 区域中的 `Read Single Block`；
2. 勾选 `Request Flags` 区域中的 `Addressed`；
3. 在 `UID` 复选框中选择 `E0040100232DB58A`；
4. 在 `(first) Block` 文本框中填写查询的块号 `03`；
5. 点击 `Execute Command` 按钮。



`Cmd` 区域自动填充命令，日志框中打印 PC 向 Reader 发送了命令 `20208AB52D23000104E003`，PC 收到 Reader 返回的数据 `0000000000`。

4.2. 命令帧数据分析

日志框中发送的数据为 `20208AB52D23000104E003`：

	SOF	Flag	Cmd	UID	Block	CRC16	EOF
值		`20`	`20`	`8AB52D23000104E0`	`03`	`B00E`	

- 对于 `Flag` = `20`

  依照表 2-2:

位（bit）	标志名称	值	值描述
b1	副载波	0	VICC 应使用单个副载波频率
b2	数据速率	0	低速率数据
b3	目录	0	第 5 到 8 位按照表 A 规定
b4	协议扩展	0	无协议格式扩展

  和表 2-3:

位 (bit)	标志名称	值	值描述
b5	选择	0	根据寻址标志设置，请求将由任何 VICC 执行
b6	寻址	1	请求有寻址。包括 UID 域。仅由那些自身 UI 与请求中规定的 UID 匹配的 VICC 才能执行
b7	选择权	0	含义由命令描述定义
b8	RFU	0	固定为 `0`

- 对于 `Cmd` = `20`

  依照表 2-5，表示这是一条读单个块命令，即为 `Read Single Block` 命令。

- 对于 `UID` = `8AB52D23000104E0`

  它是 `UID` = `E0040100232DB58A` 的小端字节序。

- 对于 `Block` = `03`

  这是我指定的块序号。

如果在 `Request Flags` 区域中**勾选** `Select` 、**不勾选** `Addressed` 且不必填写 `UID` ，则 `Flag` 会变成 `10` ，表示根据之前被 `Select` 命令选择的卡进行操作；

如果在 `Request Flags` 区域中不**勾选** `Select` 、**不勾选** `Addressed` 且不必填写 `UID` ，则 `Flag` 会变成 `00` ，表示所有卡都要回复指定块的数据。

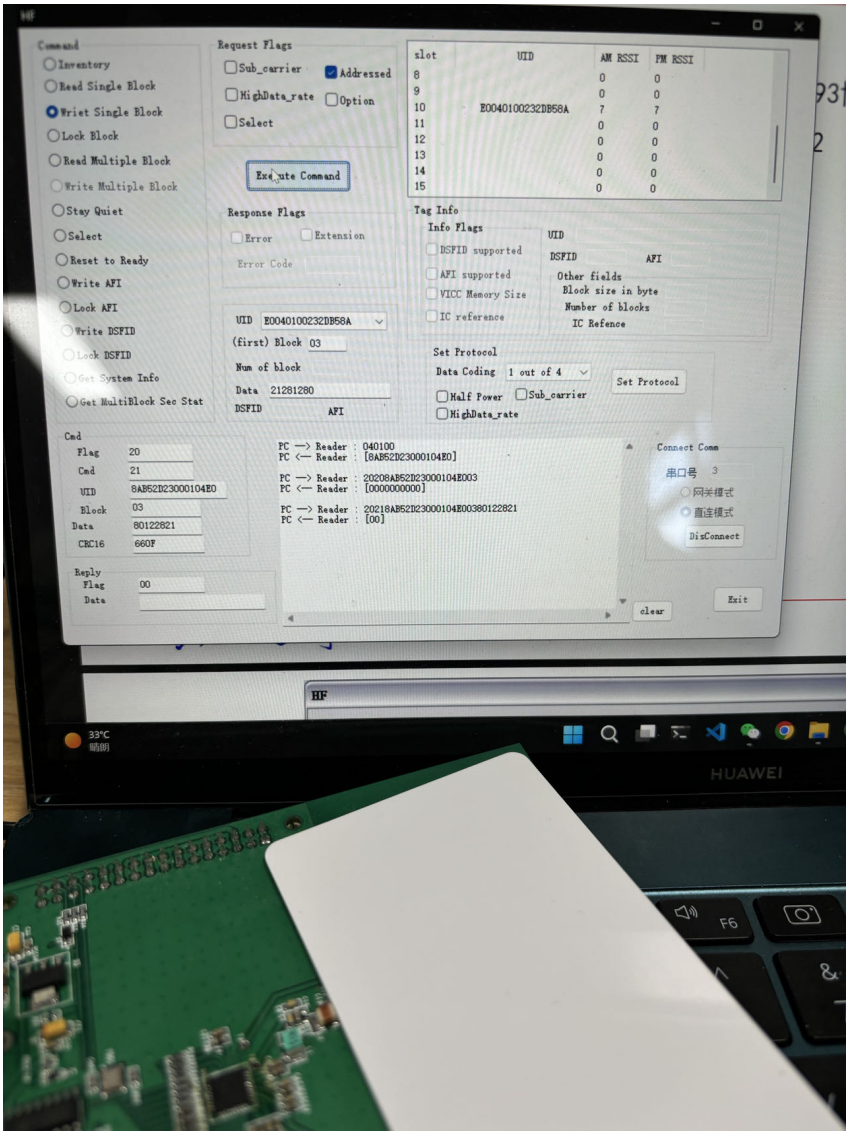
5. Write Single Block 命令

向指定卡中的指定块中写入数据。

5.1. 实验过程

对刚刚读取过的 ISO I5693 的卡片：

1. 选择 `Command` 区域中的 `Write Single Block` ；
2. 勾选 `Request Flags` 区域中的 `Addressed` ；
3. 在 `UID` 复选框中选择 `E0040100232DB58A` ；
4. 在 `(first) Block` 文本框中填写查询的块号 `03` ；
5. 在 `Data` 文本框中填写要写入的数据 `21281280` ；
6. 点击 `Execute Command` 按钮。



`Cmd` 区域自动填充命令，日志框中打印 PC 向 Reader 发送了命令 `20218AB52D23000104E00380122821` ，PC 收到 Reader 返回的数据 `0000000000` 。

5.2. 命令帧数据分析

日志框中发送的数据为 `20208AB52D23000104E003` ：

	SOF	Flag	Cmd	UID	Block	Data	CRC16	EOF
值		`20`	`21`	`8AB52D23000104E0`	`03`	`80122821`	`660F`	

- 对于 `Flag` = `20`

  依照表 2-2:

位（bit）	标志名称	值	值描述
b1	副载波	0	VICC 应使用单个副载波频率
b2	数据速率	0	低速率数据
b3	目录	0	第 5 到 8 位按照表 A 规定
b4	协议扩展	0	无协议格式扩展

  和表 2-3:

位 (bit)	标志名称	值	值描述
b5	选择	0	根据寻址标志设置，请求将由任何 VICC 执行
b6	寻址	1	请求有寻址。包括 UID 域。仅由那些自身 UI 与请求中规定的 UID 匹配的 VICC 才能执行
b7	选择权	0	含义由命令描述定义
b8	RFU	0	固定为 `0`

- 对于 `Cmd` = `21`

  依照表 2-5，表示这是一条写单个块命令，即为 `Write Single Block` 命令。

- 对于 `UID` = `8AB52D23000104E0`

  它是 `UID` = `E0040100232DB58A` 的小端字节序。

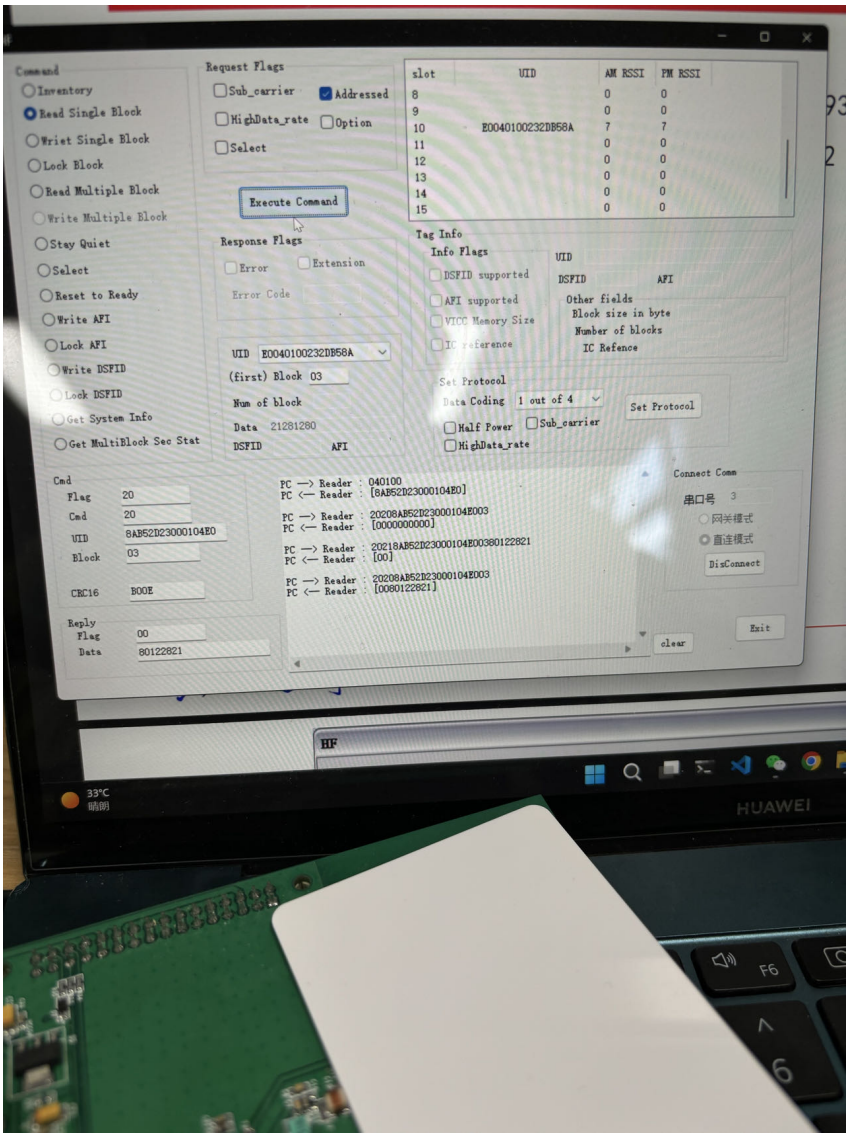
- 对于 `Block` = `03`

  这是我指定的块序号。

- 对于 `Data` = `80122821`

  这是我指定写入的数据 `21281280` 的小端字节序。

再次使用 `Read Single Block` 命令读取写入数据的块:



卡片回复 `0080122821`，可见卡片中第 `03` 个块的低 4 字节已经写入指定数据 `21281280`。

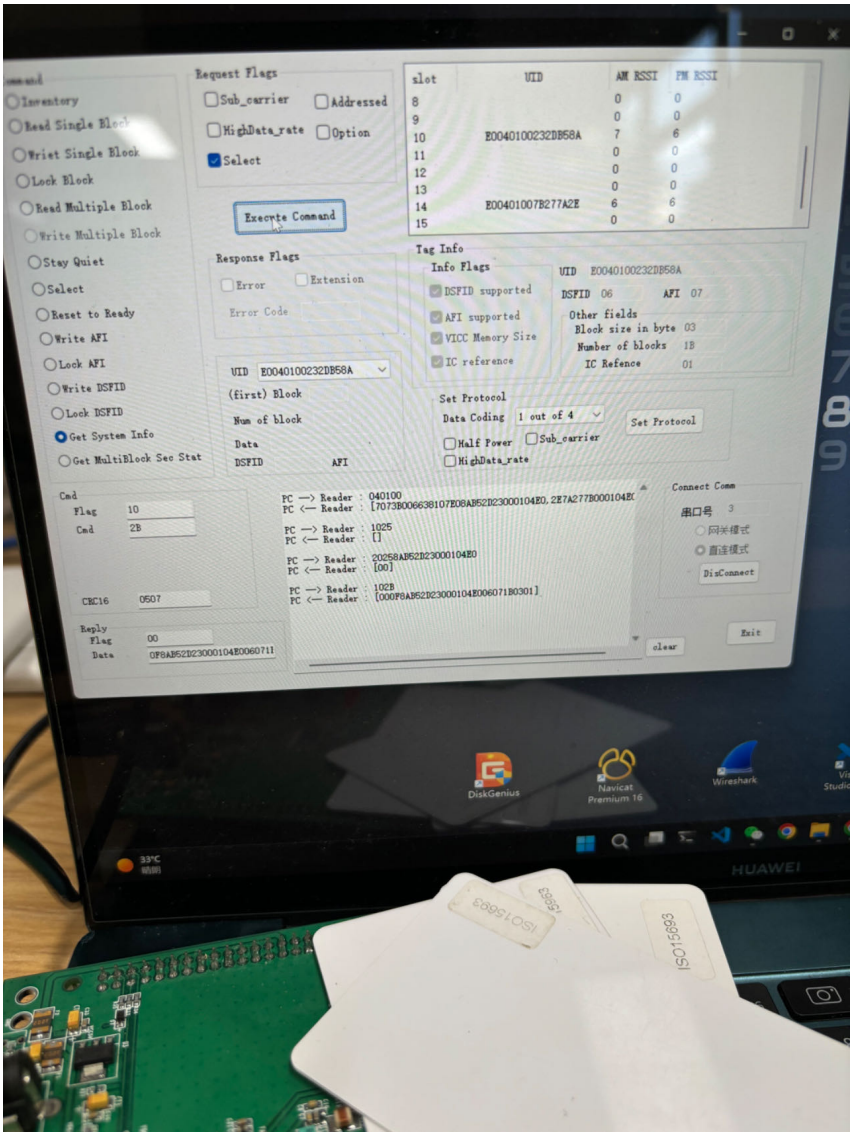
6. Get System Info 命令

该命令用于获取卡片信息。

6.1. 实验过程

将单张 ISO 15693 的卡片放到 RFID HF Reader 的射频区域上方，经过 `Inventory` 识别并 `Select` 后：

1. 选择 `Command` 区域中的 `Get System Info`；
2. 勾选 `Request Flags` 区域中的 `Select`；
3. 点击 `Execute Command` 按钮。



`Cmd` 区域自动填充命令，日志框中打印 PC 向 Reader 发送了命令 `102B`，PC 收到 Reader 返回的数据 `000F8AB52D23000104E006071B0301`。

6.2. 命令帧数据分析

日志框中发送的数据为 `102B`：

	SOF	Flag	Cmd	CRC16	EOF
值		10	2B	0507	

- 对于 `Flag` = `10`

  依照表 2-2：

位（bit）	标志名称	值	值描述
b1	副载波	0	VICC 应使用单个副载波频率
b2	数据速率	0	低速率数据
b3	目录	0	第 5 到 8 位按照表 A 规定
b4	协议扩展	0	无协议格式扩展

  和表 2-3：

位 (bit)	标志名称	值	值描述
b5	选择	1	请求只由处于选择状态的 VICC 执行，寻址标志应设置为 0，UID 域应不包含在请求中
b6	寻址	0	请求没有寻址。不包括 UID 域。可以由任何 VICC 执行
b7	选择权	0	含义由命令描述定义
b8	RFU	0	固定为 `0`

- 对于 `Cmd` = `2B`

  依照表 2-5，表示这是一条获取系统信息命令，即为 `Get System Info` 命令。

4.3. 卡片回复数据分析

日志框中卡片返回的数据为 `000F8AB52D23000104E006071B0301` ，查阅 ISO 15693 标准后分析：

内容	值
SOF	
标志（8 bits）	`00`
信息标志（8 bits）	`0F`
UID	`8AB52D23000104E0`
DSFID（8 bits）	`06`
AFI（8 bits）	`07`
VICC 内存容量信息（16 bits）	`1B03`
IC 参考（8 bits）	`01`
EOF	

- 对于信息标志：

位 (bit)	标志名称	值描述	实验值
b1	DSFID	`0` - 不支持 DSFID。DSFID 域不出现；`1` - 支持 DSFID。DSFID 域出现	1
b2	AFI	`0` - 不支持 AFI。AFI 域不出现；`1` - 支持 AFI。AFI 域出现	1
b3	VICC 内存容量	`0` - 不支持信息的 VICC 内存容量。内存容量域不出现；`1` - 支持信息的 VICC 内存容量。内存容量域出现	1
b4	IC 参考	`0` - 不支持信息的 IC 参考。IC 参考域不出现；`1` - 支持信息的 IC 参考。IC 参考域出现	1
b5	RFU	-	0
b6	RFU	-	0
b7	RFU	-	0
b8	RFU	-	0

- 对于 VICC 内存容量：

	RFU（3 bits）	块容量的字节数（4 bits）	块数目（8 bits）
实验值	`0b000`	`0b11011` = `27`	`0x03` = `3`

注意到 `AFI` = `07` 。

7. Write AFI 命令

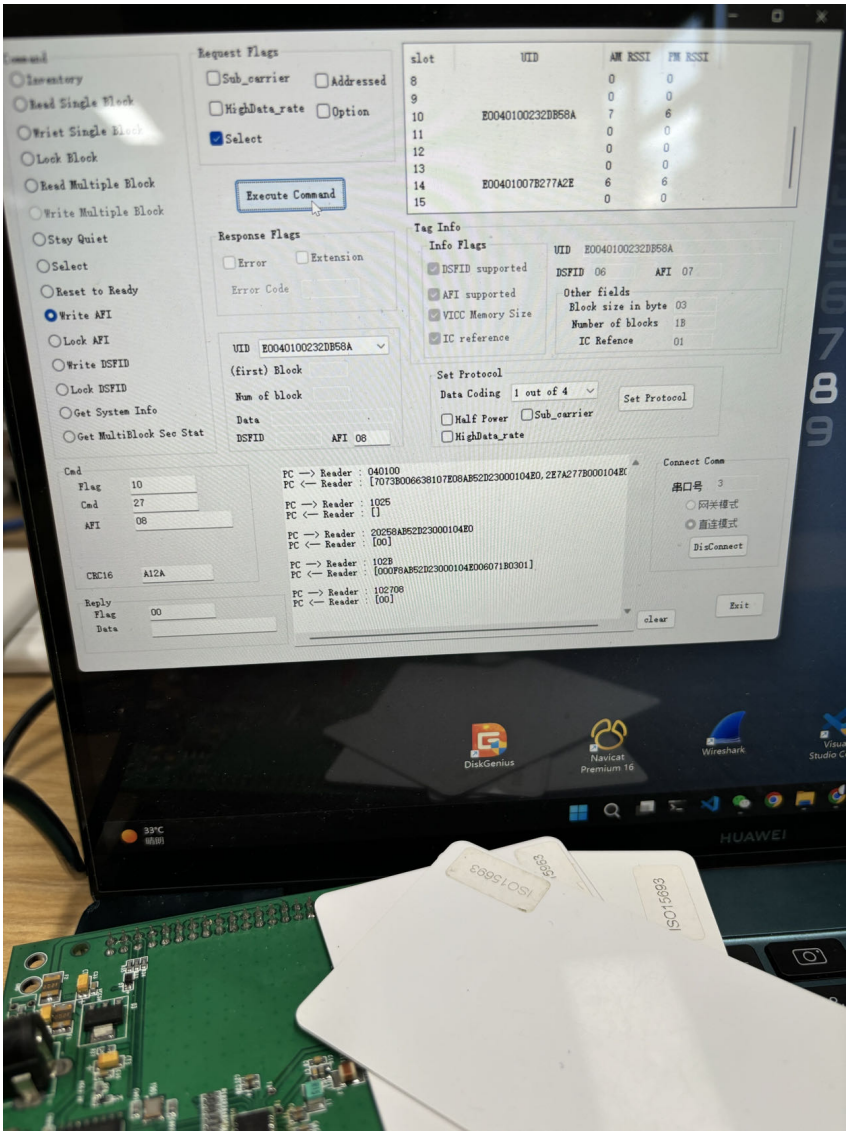
`AFI` 是应用族标识符，用于标志卡片所用的领域。

使用 `Write AFI` 命令可以修改 `AFI`，之后可以使用 `Lock AFI` 命令锁定 `AFI` 使其不可被更改。

7.1. 实验过程

对刚刚读取过系统信息的 ISO I5693 的卡片：

1. 选择 `Command` 区域中的 `Write AFI`；
2. 勾选 `Request Flags` 区域中的 `Select`；
3. 在 `AFI` 文本框中填写要写入的数据 `08`；
4. 点击 `Execute Command` 按钮。



`Cmd` 区域自动填充命令，日志框中打印 PC 向 Reader 发送了命令 `102708`，PC 收到 Reader 返回的数据 `00`，说明写入成功 。

7.2. 命令帧数据分析

日志框中发送的数据为 `20208AB52D23000104E003`：

	SOF	Flag	Cmd	AFI	CRC16	EOF
值		`10`	`27`	`08`	`A12A`	

- 对于 `Flag` = `10`

  依照表 2-2:

位（bit）	标志名称	值	值描述
b1	副载波	0	VICC 应使用单个副载波频率
b2	数据速率	0	低速率数据
b3	目录	0	第 5 到 8 位按照表 A 规定
b4	协议扩展	0	无协议格式扩展

  和表 2-3:

位 (bit)	标志名称	值	值描述
b5	选择	1	请求只由处于选择状态的 VICC 执行，寻址标志应设置为 0，UID 域应不包含在请求中
b6	寻址	0	请求没有寻址。不包括 UID 域。可以由任何 VICC 执行
b7	选择权	0	含义由命令描述定义
b8	RFU	0	固定为 `0`

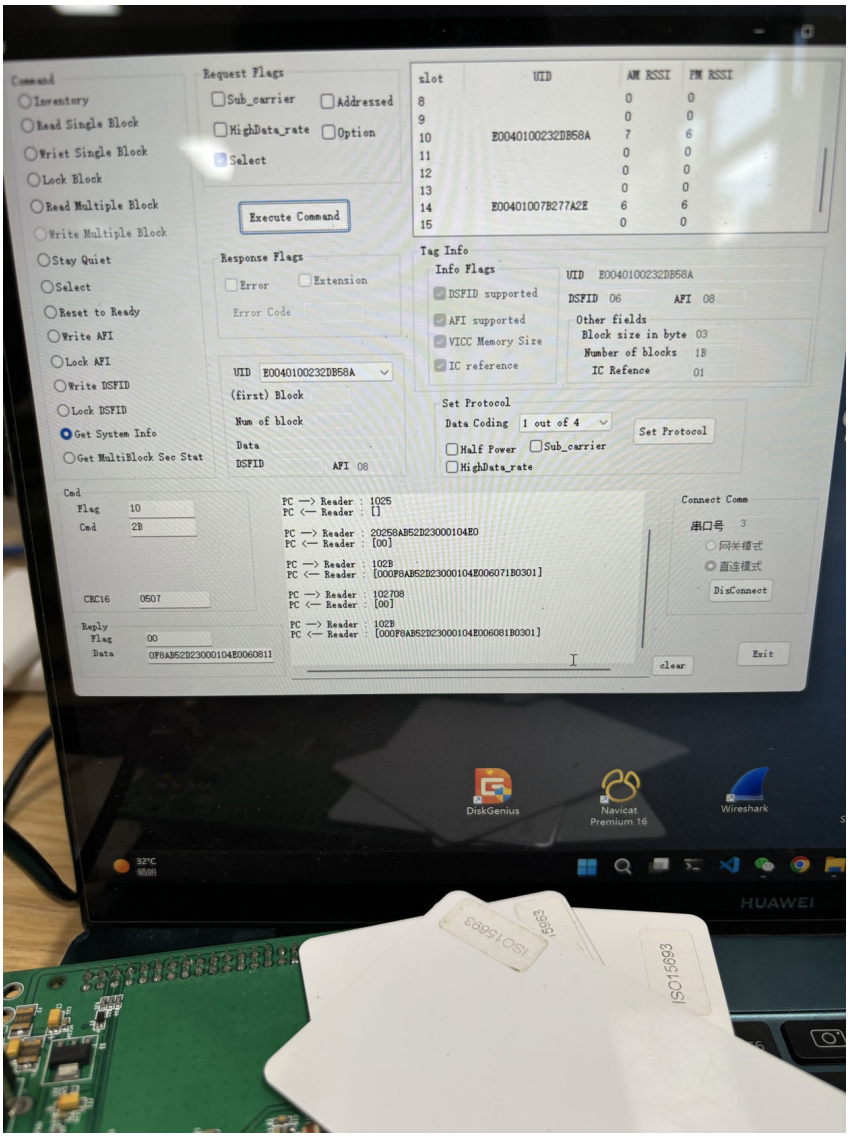
- 对于 `Cmd` = `27`

  依照表 2-5，表示这是一条写 AFI命令，即为 `Write AFI` 命令。

- 对于 `AFI` = `08`

  这是我指定写入的`AFI` = `08` 。

再次使用 `Get System Info` 命令读取卡片系统信息:



卡片回复 `000F8AB52D23000104E006081B0301`，可见卡片中的 `AFI` 已经写入指定 `AFI` = `08` 。

8. 总结

对于其他命令，由于实验过程中忘记拍照，不再展示。

总的来说，这是一次复现实验， Reader 向卡片发送的每一个字节都严格按照 ISO 15693 规范，因此对于其他命令的构造与实验，做法都一样。

我从本次实验中学到了许多东西：

1. 首先是加深了对规范标准的理解。无规矩不成方圆，正是由于设计出了良好的规范，便捷的 RFID 通信得以推广。
2. 其次是巩固了 ISO 15693 协议防碰撞算法的知识：
    - 在 `Inventory` 阶段，ISO 15693 协议通过依次在范围内叫号获得卡片响应，从而有序识别射频场中的各个卡；
    - 在读写阶段，ISO 15693 协议通过 `Flag` 的第 3 个 bit ，指定使用两种方式中的一种来避免碰撞：
        1. 通过 `Select` 命令指定要响应的卡片，然后发送对该卡片的操作命令；
        2. 在命令中添加指定卡片的 `UID` 。

这是一次让我受益匪浅的实验。