

# UNIVERSIDAD TÉCNICA DEL NORTE

## FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

### CARRERA DE TELECOMUNICACIONES



## RADIO DEFINIDA POR SOFTWARE

### CAPTURAS NFC

#### **Docente:**

Msc. Edgar Maya.

#### **Estudiante:**

Montezuma Rosero Diego Arbey<sup>1</sup>  
Narváez Guevara Israel Sebastian<sup>2</sup>  
Panamá Chicaiza Anthony Miguel<sup>3</sup>

<sup>1</sup>damontezumar@utn.edu.ec

<sup>2</sup>isnarvaezg@utn.edu.ec

<sup>3</sup>ampanamac@utn.edu.ec

20 de mayo del 2024

## TITULO

### DEMODULACION, DECODIFICACION DE LA TECNOLIGIA NFC - RTL-SDR

## INTRODUCCION

En el siguiente informe, se analiza la comunicación NFC mediante el uso de tarjetas RFID y módulo de lectura de estas, esto mediante el uso de un módulo RTL-SDR para la captura de las señales de radio frecuencia y posterior análisis de paquetes con el software NFC Laboratory, el cual proporciona una interfaz parecida a Wireshark.

El análisis se encamina desde el estado de POWER OFF hasta el estado HALT, se explora cómo los PICCs Tipo A pasan por diferentes estados de funcionamiento en respuesta a las señales del PCD (Dispositivo de Control de Proximidad). Se detallan los comandos esenciales, como REQA, WUPA y ANTICOLLISION, que se utilizan para iniciar la comunicación, detectar PICCs en el campo y seleccionar el PICC deseado para una interacción más profunda.

Además, se analiza la secuencia de selección, que describe el proceso mediante el cual el PCD obtiene el Identificador Único (UID) de un PICC y lo selecciona para la comunicación. Se explican los pasos clave, como la realización de bucles de anticollisión y la transmisión de comandos SELECT, que son fundamentales para garantizar una selección precisa y confiable del PICC.

## OBJETIVOS

### Objetivo General

Realizar un análisis exhaustivo de la comunicación NFC mediante la captura de las señales de radiofrecuencia generadas por las tarjetas RFID utilizando un receptor RTL-SDR. Los datos recolectados se importarán en el software NFC Laboratory, que ofrece herramientas avanzadas para la decodificación y análisis de los protocolos NFC. Dentro del software, se identificarán y documentarán diferentes eventos críticos, asegurando que cada uno de estos eventos se evidencie conforme al standard ISO/IEC 14443, garantizando así la integridad y seguridad de la comunicación y verificando el correcto funcionamiento del sistema según las especificaciones técnicas.

### Objetivos Específicos

- Instalar y familiarizarse con el software NFC Laboratory.
- Realizar las configuraciones con las que se va a realizar el proceso de comunicación.
- Identificar dentro del software NFC laboratory los diferentes eventos que se recolecta al realizar la comunicación entre la tarjeta y el RTL-SDR.
- Realizar un análisis de los diferentes eventos que surgen dentro de la comunicación e ir comparando los eventos dentro del standard utilizado para la práctica.

## MARCO REFERENCIAL

### ¿Qué es el NFC?

NFC, cuyas siglas en inglés representan Near Field Communication, se traduce al español como Comunicación de Campo Cercano. Esta denominación es apropiada, ya que la tecnología opera mediante proximidad, activándose al aproximar un dispositivo a otro. Utiliza una frecuencia alta, específicamente en la banda de los 13.56 MHz (Nur Anissa, 2022).



*Figura 1. Tecnología NFC.*

El NFC se origina a partir de las etiquetas RFID, comúnmente utilizadas en sistemas de transporte y seguridad en tiendas físicas, y ha sido concebido desde su inicio como una plataforma abierta para dispositivos móviles. Básicamente, permite el intercambio de datos entre dispositivos dentro de un radio muy limitado, de aproximadamente 10 a 15 centímetros de distancia para establecer la comunicación (PUBLIC, 2018).

Al acercar los dispositivos, se genera un campo electromagnético por inducción que facilita el intercambio de datos, alcanzando una tasa de transferencia de hasta 424 Kbps. Aunque se emplea para el intercambio de datos, su velocidad limitada lo hace más adecuado para la identificación y validación de dispositivos y personas.

La principal ventaja del NFC es que permite la comunicación instantánea entre dos dispositivos sin necesidad de emparejamiento previo, simplificando el intercambio de datos. No obstante, su uso se ve restringido por su corto alcance, que es inferior a 20 centímetros, lo que lo hace inadecuado para comunicaciones a larga distancia. Este aspecto, sin embargo, tiene el beneficio de garantizar una mayor seguridad, ya que es necesario acercar deliberadamente el dispositivo a otro para intercambiar datos, impidiendo manipulaciones a distancia (IEEE, 2001).

La señal recibida estará constituida por los componentes I y Q, tal como se ilustra en la imagen siguiente.



Figura 2. Señales I y Q.

A partir de estos componentes, se determina la magnitud real mediante la fórmula clásica  $\sqrt{I^2 + Q^2}$ . A continuación, se presenta una captura de la señal recibida en la banda base, tras la conversión de I/Q a magnitud, correspondiente a la instrucción REQA y su respuesta:

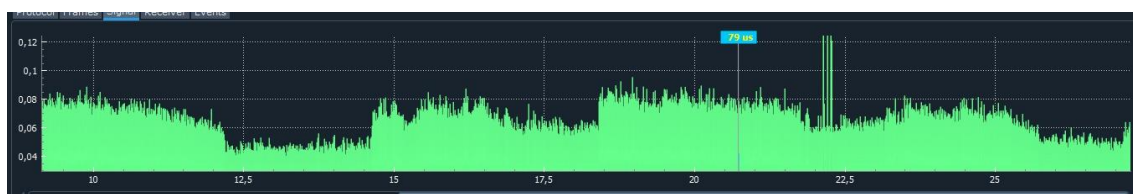


Figura 3. Espectro radioeléctrico.

La señal es modulada en 100% ASK, lo cual corresponde al comando NFC-A REQA 26h según las especificaciones de NFC. La respuesta de la tarjeta emplea una técnica conocida como modulación de carga, que se manifiesta como una serie de pulsos en la señal principal posterior al comando. Esta es la forma de modulación más básica; sin embargo, cada uno de los estándares NFC-A, NFC-B, NFC-F y NFC-V posee características particulares.

### NFC-A

La modulación NFC-A (Near Field Communication tipo A) se rige por la norma ISO/IEC 14443A, que especifica los métodos de modulación y codificación para la comunicación entre dispositivos NFC, como lectores y tarjetas.

## Modulación y Codificación

### • Modulación ASK (Amplitude Shift Keying):

ASK 100%: La modulación emplea una variación del 100% en la amplitud de la señal portadora para representar datos. Esto significa que la señal puede estar completamente presente (valor alto) o ausente (valor bajo).

### • Codificación Miller modificada:

Esta técnica se utiliza para codificar los datos en la transmisión de la señal ASK. La codificación Miller modificada implica los siguientes pasos:

1. Un bit '1' se representa por una transición en el centro del periodo de bit.

- Un bit '0' se representa por una ausencia de transición en el centro del periodo de bit, pero con una transición al comienzo del siguiente periodo de bit si el siguiente bit es '1', o dos periodos de bit más tarde si los siguientes dos bits son '0'.

### Estructura de la Trama

Las tramas del lector en el sistema NFC-A incluyen varias partes clave, cada una de las cuales se modula y codifica según las especificaciones ISO/IEC 14443A:

- Preámbulo: Consiste en una serie de bits que sincronizan el receptor con la señal entrante.
- Código de inicio (Start of Frame, SOF): Indica el comienzo de una trama.
- Datos: Los datos útiles que se están transmitiendo.
- Código de fin (End of Frame, EOF): Indica el final de una trama.

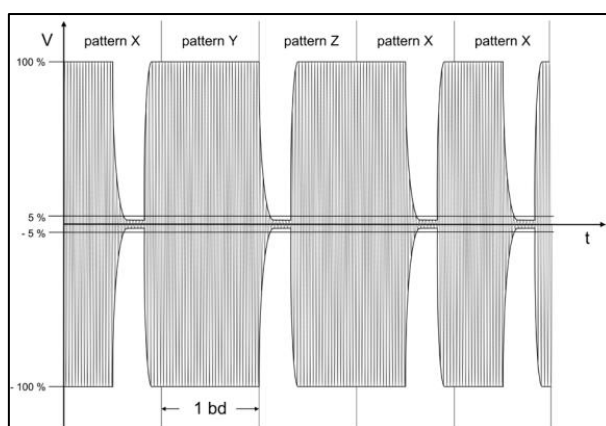


Figura 4. NFC-A (PUBRIC, 2018).

### NFC-B

La modulación NFC-B (Near Field Communication tipo B) se rige por la norma ISO/IEC 14443B, que especifica los métodos de modulación y codificación para la comunicación entre dispositivos NFC, como lectores y tarjetas (PUBRIC, 2018).

### Modulación y Codificación

- Modulación ASK (Amplitude Shift Keying):**

ASK 10%: La modulación emplea una variación del 10% en la amplitud de la señal portadora para representar datos. Esto significa que la señal experimenta una pequeña disminución en su amplitud para indicar un bit '0', mientras que el bit '1' se representa sin cambios en la amplitud (Josevcn, 2023).

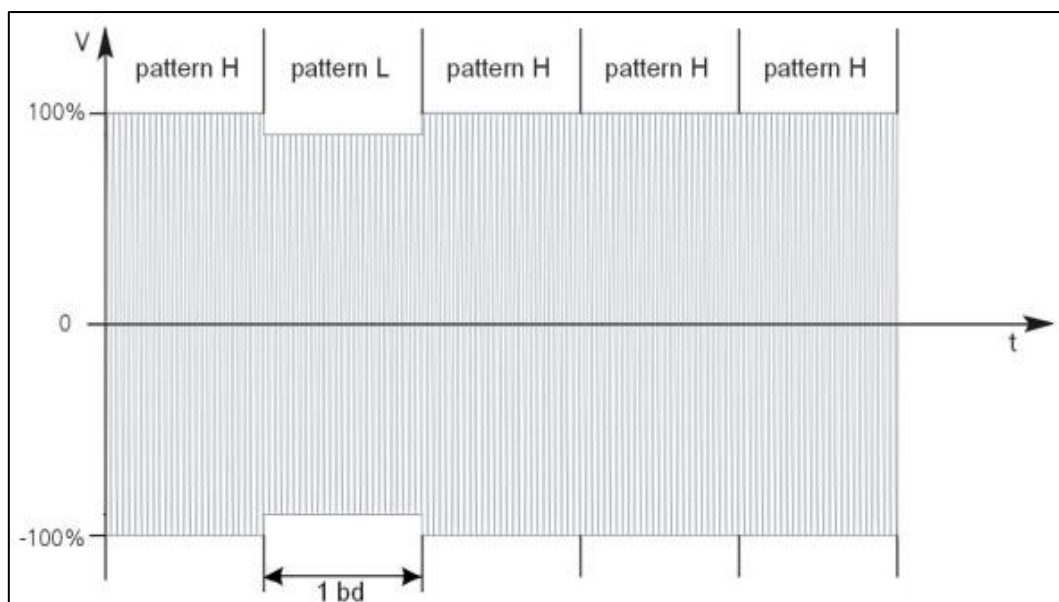
- Codificación NRZ-L (Non-Return-to-Zero Level):**

En esta técnica de codificación, los niveles de voltaje alto y bajo se utilizan directamente para representar bits. Un nivel alto constante (sin cambios) representa un bit '1', y un nivel bajo constante representa un bit '0'. No hay transiciones intermedias o de retorno a un nivel de referencia entre bits, lo que simplifica la generación y detección de la señal.

### Estructura de la Trama.

Las tramas del lector en el sistema NFC-B incluyen varias partes clave, cada una de las cuales se modula y codifica según las especificaciones ISO/IEC 14443B:

1. Preámbulo: Consiste en una serie de bits que sincronizan el receptor con la señal entrante.
2. Código de inicio (Start of Frame, SOF): Indica el comienzo de una trama.
3. Datos: Los datos útiles que se están transmitiendo, codificados en NRZ-L.
4. Código de fin (End of Frame, EOF): Indica el final de una trama



*Figura 5. NFC-B. (PUBLIC, 2018)*

### NFC-F

La modulación NFC-F (también conocida como FeliCa) se rige por las normas ISO/IEC 18092 y JIS X 6319-4, que especifican los métodos de modulación y codificación para la comunicación entre dispositivos NFC.

### Modulación y Codificación

**Modulación FSK:** FSK 212/424 kbps: La modulación emplea cambios en la frecuencia de la señal portadora para representar datos. Se utilizan dos frecuencias distintas para los dos estados binarios:

Para una velocidad de 212 kbps:

- Frecuencia de '0': 13.56 MHz - 424 kHz
- Frecuencia de '1': 13.56 MHz + 424 kHz

Para una velocidad de 424 kbps:

- Frecuencia de '0': 13.56 MHz - 848 kHz
- Frecuencia de '1': 13.56 MHz + 848 kHz

### Codificación Manchester:

En esta técnica de codificación, cada bit se representa por una transición en el centro del periodo de bit. Un bit '1' se representa por una transición de alto a bajo, y un bit '0' se representa por una transición de bajo a alto en el centro del bit. Esta codificación garantiza que haya al menos una transición por bit, lo que facilita la sincronización de la señal.

### Estructura de la Trama

Las tramas en el sistema NFC-F incluyen varias partes clave, cada una de las cuales se modula y codifica según las especificaciones ISO/IEC 18092 y JIS X 6319-4:

1. Preámbulo: Consiste en una serie de bits que sincronizan el receptor con la señal entrante.
2. Código de inicio (Start of Frame, SOF): Indica el comienzo de una trama.
3. Datos: Los datos útiles que se están transmitiendo, codificados en Manchester.
4. Código de fin (End of Frame, EOF): Indica el final de una trama.

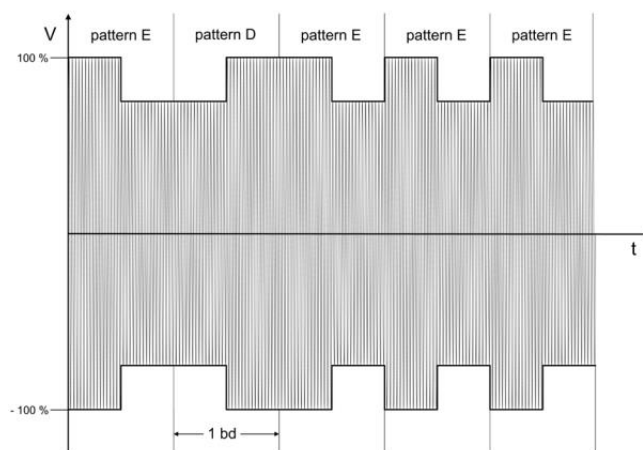


Figura 6.NFC-F (PUBLIC, 2018).

### Modulación NFC-V

La modulación NFC-V (Near Field Communication tipo V) se rige por la norma ISO/IEC 15693, que especifica los métodos de modulación y codificación para la comunicación entre dispositivos NFC, como lectores y tarjetas.

### Modulación y Codificación

- Modulación ASK (Amplitude Shift Keying) y PSK (Phase Shift Keying): ASK 10%: Utiliza una variación del 10% en la amplitud de la señal portadora para representar datos. En ASK, la amplitud de la señal cambia ligeramente para indicar diferentes bits.
- FSK (Frequency Shift Keying): Alternativamente, algunos sistemas NFC-V pueden usar FSK, donde diferentes frecuencias representan diferentes bits.
- Codificación NRZ (Non-Return-to-Zero): En esta técnica de codificación, los bits se representan directamente como niveles de señal altos o bajos sin transiciones intermedias. Un nivel alto constante representa un bit '1' y un nivel bajo constante representa un bit '0'.

### Estructura de la Trama

Las tramas en el sistema NFC-V incluyen varias partes clave, cada una de las cuales se modula y codifica según las especificaciones ISO/IEC 15693:

- Preámbulo: Consiste en una serie de bits que sincronizan el receptor con la señal entrante.
- Código de inicio (Start of Frame, SOF): Indica el comienzo de una trama.
- Datos: Los datos útiles que se están transmitiendo, codificados en NRZ.
- Código de fin (End of Frame, EOF): Indica el final de una trama.

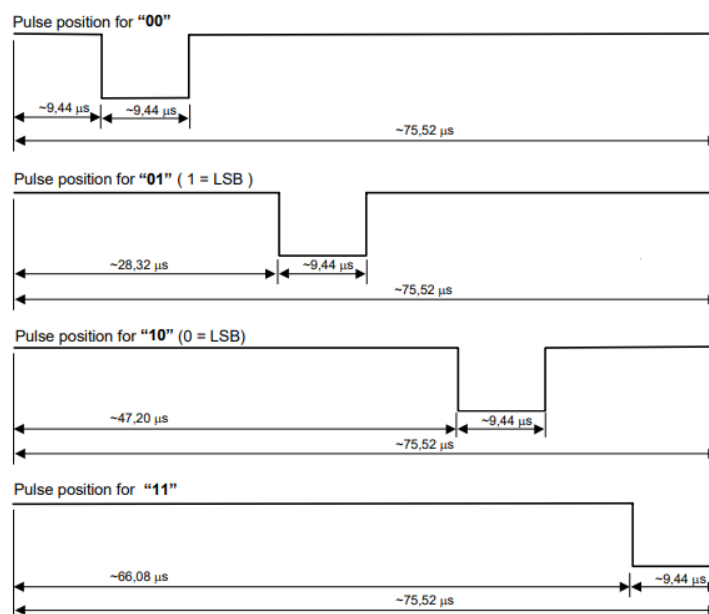


Figura 7. NFC-V. (PUBLIC, 2018)



## RECURSOS MATERIALES Y EQUIPOS

Para el desarrollo de esta práctica es necesario contar con los siguientes materiales:

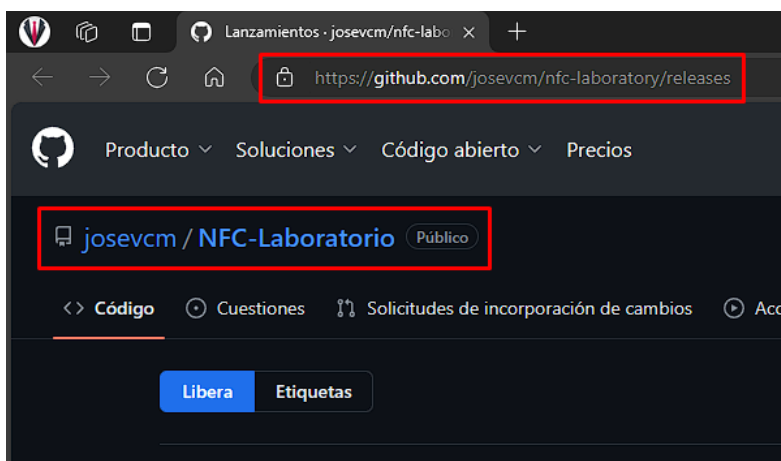
- Computadora personal.
- Software NFC Laboratory.
- RTL-SDR.
- Tarjetas de radiofrecuencia RFID.
- Lector RFID (Smarthpone).

## DESARROLLO

### Instalación de NFC Laboratory

Para comenzar con esta práctica, es necesario realizar la correspondiente instalación del software que vamos a emplear, en este caso NFC Laboratory, al cual podremos acceder mediante el siguiente enlace de github: <https://github.com/josevcm/nfc-laboratory>. Aquí encontraremos las instrucciones necesarias de instalación, pero en consecuencia también es posible realizar una instalación limpia mediante un .exe destinado al sistema operativo Windows, el cual se lo puede encontrar en el siguiente github: <https://github.com/josevcm/nfc-laboratory/releases>.

La versión que vamos a instalar de NFC Laboratory es la 2.8.3, la cual tiene un soporte de muestreo directo para un RTL-SDR. Como primer paso, ingresaremos en el link de descarga como se aprecia a continuación.



*Figura 1. Dirección de información sobre NFC-Labortory.*

Seguidamente vamos a buscar la versión de NFC Laboratory seleccionada, que en este caso es la versión 2.8.3, la cual se puede apreciar en la siguiente figura.

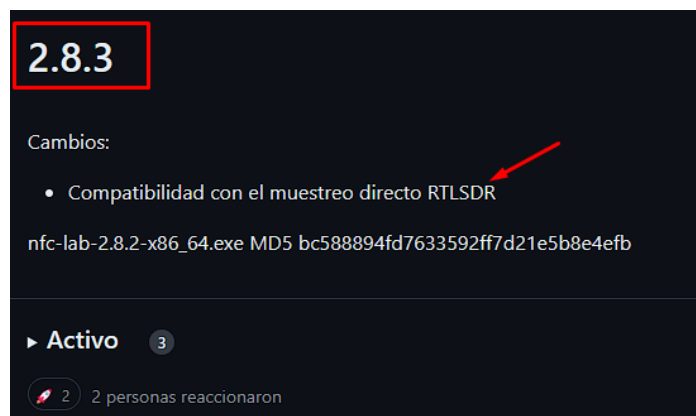


Figura 2. versión de NFC-Laboratory a descargar.

Una vez que hemos seleccionado la versión de instalación, se nos mostraran los distintos archivos de descarga tanto en .tar para Linux como en .exe para Windows. Tal como se aprecia en la siguiente figura.



Figura 3. Archivos de descarga para la instalación.

Una vez descargado el instalador del software, vamos a realizar la ejecución de este, y procedemos a seguir los pasos de instalación correspondientes.

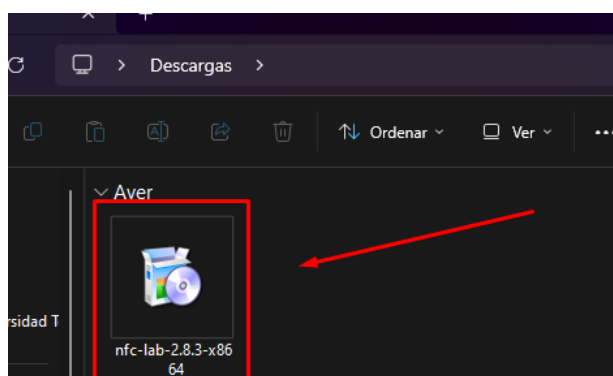
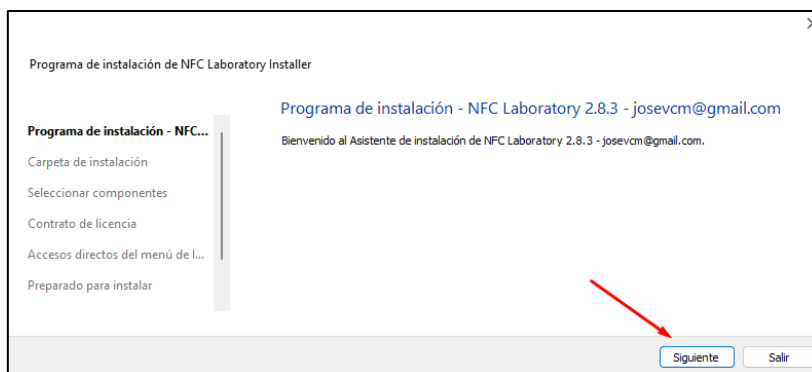


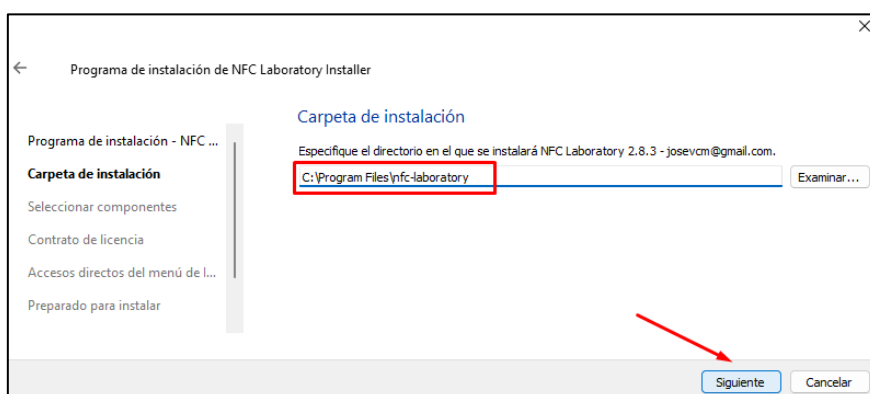
Figura 4. Ejecutable de instalación de NFC-Laboratory para Windows.

Al momento de e iniciar el ejecutable del instalador se nos mostrara la siguiente ventana, en la cual se nos informara que el programa de instalación está listo para iniciar el proceso, daremos en siguiente.



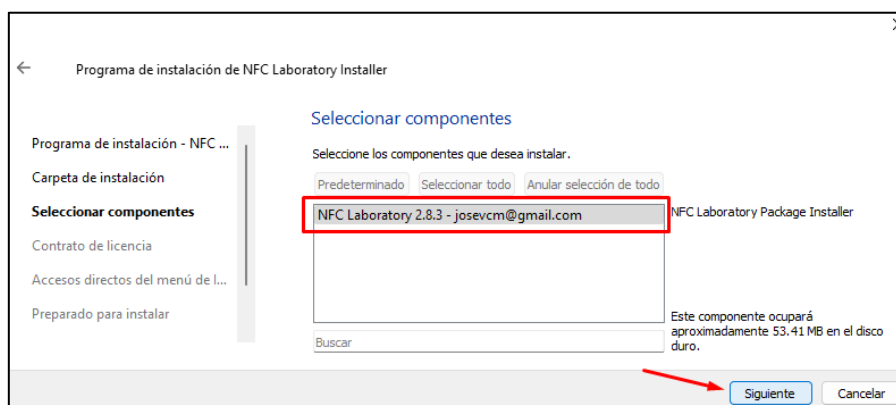
*Figura 5. Inicio de instalación de NFC Laboratory.*

En la siguiente ventana que se nos muestra se pedirá la ruta en la que queremos instalar nuestro software, en este caso la hemos dejado en la ruta por defecto, daremos en siguiente.



*Figura 6. Ruta de instalación de NFC Laboratory.*

En la ventana a continuación se nos pedirá que seleccionemos los componentes que vamos a instalar, en este caso vamos a seleccionar la opción de NFC Laboratory 2.8.3 por josevcm@gmail.com y daremos en siguiente.



*Figura 7. Selección de complementos de NFC Laboratory.*

Seguidamente se nos pedirá que aceptemos el contrato de licencia, tal como se aprecia en la siguiente figura, una vez realizado esto daremos en siguiente



Figura 8. Acuerdo de licencia de NFC Laboratory.

Una vez que hemos configurado todos estos pasos, vamos a realizar la instalación del software dando en el botón de instalar, tal como se aprecia en la siguiente figura.

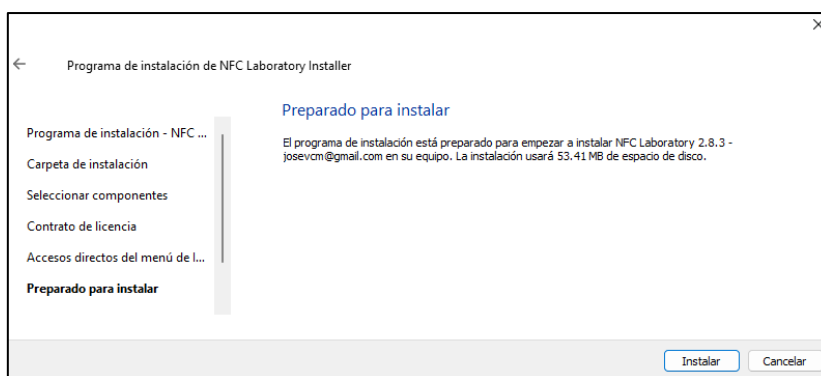


Figura 9. Inicio de instalación de NFC Laboratory.

## Configuración de software.

Una vez que se tiene instalado el software, es necesario dirigirse hacia el directorio de instalación para configurar los parámetros de lectura, en este caso debemos editar el archivo denominado “nfc-lab.conf”, el cual contiene estas configuraciones.

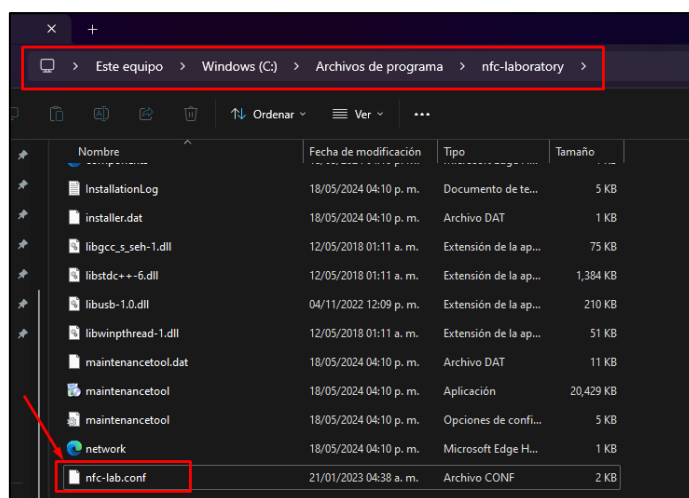
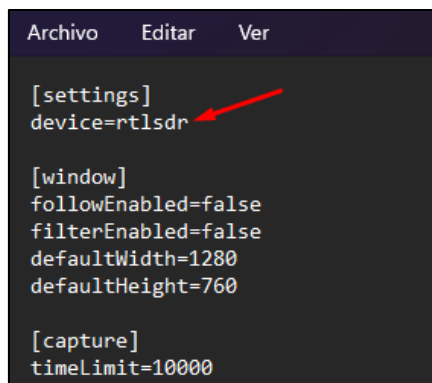


Figura 10. Archivo de configuración de NFC Laboratory.

Una vez abierto este archivo con un editor, en el apartado [settings], vamos a ingresar el tipo de dispositivo que estamos utilizando, en este caso el rtl-sdr, de igual forma en el apartado de [Window] se puede definir los parámetros de ventana del software, mientras que en el apartado [capture] se define el tiempo límite de captura de paquetes, el cual está configurado en 10000 segundos.



```

Archivo  Editar  Ver

[settings]
device=rtlsdr

[window]
followEnabled=false
filterEnabled=false
defaultWidth=1280
defaultHeight=760

[capture]
timeLimit=10000
  
```

*Figura 11. Configuración de parámetros generales de NFC Laboratory*

Mas abajo podremos encontrar los diferentes tipos de decodificadores, entre los cuales el software soporta nfca, nfcb, nfcf y nfcv, la diferencia entre estos se basa en los parámetros, los cuales se detallan a continuación.

- **NFC-A**

1. Estándar: ISO/IEC 14443A.
2. Frecuencia: 13.56 MHz.
3. Velocidad: Hasta 424 Kbps.
4. Modulación: ASK.

- **NFC-B**

1. Estándar: ISO/IEC 14443B.
2. Frecuencia: 13.56 MHz.
3. Velocidad: Hasta 424 Kbps.
4. Modulación: ASK con diferente codificación a NFC-A.

- **NFC-F**

1. Estándar: JIS X 6319-4.
2. Frecuencia: 13.56 MHz.
3. Velocidad: Hasta 424 Kbps y en algunas versiones hasta 848 Kbps.
4. Modulación: FSK.

- **NFC-V**

1. Estándar: ISO/IEC 15693.
2. Frecuencia: 13.56 MHz.
3. Velocidad: Mas lenta que NFC-A.
4. Modulación: ASK.

También se debe habilitar la opción `debugEnabled`, esto para que el software habilite el modo de depuración y pueda generar información adicional que diagnostique y solucione problemas.

```
[decoder]
debugEnabled=true
powerLevelThreshold=0.01

[decoder.nfca]
enabled=true
minimumModulationDeep=0.10
maximumModulationDeep=1.00

[decoder.nfcb]
enabled=true
minimumModulationDeep=0.10
maximumModulationDeep=0.90

[decoder.nfcf]
enabled=true
minimumModulationDeep=0.08
maximumModulationDeep=0.90

[decoder.nfcv]
enabled=true
minimumModulationDeep=0.10
maximumModulationDeep=1.00
```

*Figura 12. Modos de comunicación NFC.*

Mas abajo en el archivo de configuración encontraremos el apartado denominado `[device.rtlsdr]`, aquí vamos a realizar la configuración de los parámetros como la ganancia que se establece en 125, la frecuencia central de escucha que en este caso utilizamos la de NFC-A que es 13.56MHz, la tasa de muestreo a 24 MHz tal como lo recomienda el archivo de GitHub y por último el “`directSampling`” en un valor de 2, esto indicara que vamos a utilizar un muestreo directo en la rama Q y no en la I, esto lo recomienda el archivo de GitHub ya que se obtiene mejores resultados en esta configuración de rama.

```
[device.rtlsdr]
gainMode=1
gainValue=125
tunerAgc=false
mixerAgc=false
centerFreq=13560000
sampleRate=2400000
directSampling=2
```

*Figura 13. Configuración de parámetros de escucha para el RTL-SDR.*

Por último se realiza la configuración del apartado de claves A y B, como se muestra en la siguiente figura, en este caso esto nos demuestra que cada línea representa una clave o un par de claves. El `sXX` indica un índice (donde XX es un número del 00 al 15). `000000000000` es una clave en formato hexadecimal (12 dígitos, lo que equivale a 6 bytes). El formato `000000000000, 000000000000` nos indica que se están definiendo dos claves por cada entrada, una clave A y una clave B, común en configuraciones de acceso a bloques de memoria en tarjetas MIFARE (un tipo de tarjeta RFID).

```
[keys.default]
s00=000000000000, 000000000000
s01=000000000000, 000000000000
s02=000000000000, 000000000000
s03=000000000000, 000000000000
s04=000000000000, 000000000000
s05=000000000000, 000000000000
s06=000000000000, 000000000000
s07=000000000000, 000000000000
s08=000000000000, 000000000000
s09=000000000000, 000000000000
s10=000000000000, 000000000000
s11=000000000000, 000000000000
s12=000000000000, 000000000000
s13=000000000000, 000000000000
s14=000000000000, 000000000000
s15=000000000000, 000000000000
```

Figura 14. Claves A y B para tarjetas RFID.

Una vez que ya tenemos todo configurado y todo instalado, vamos a abrir el software tal y como se aprecia en la siguiente figura, aquí podremos visualizar la interfaz del software.

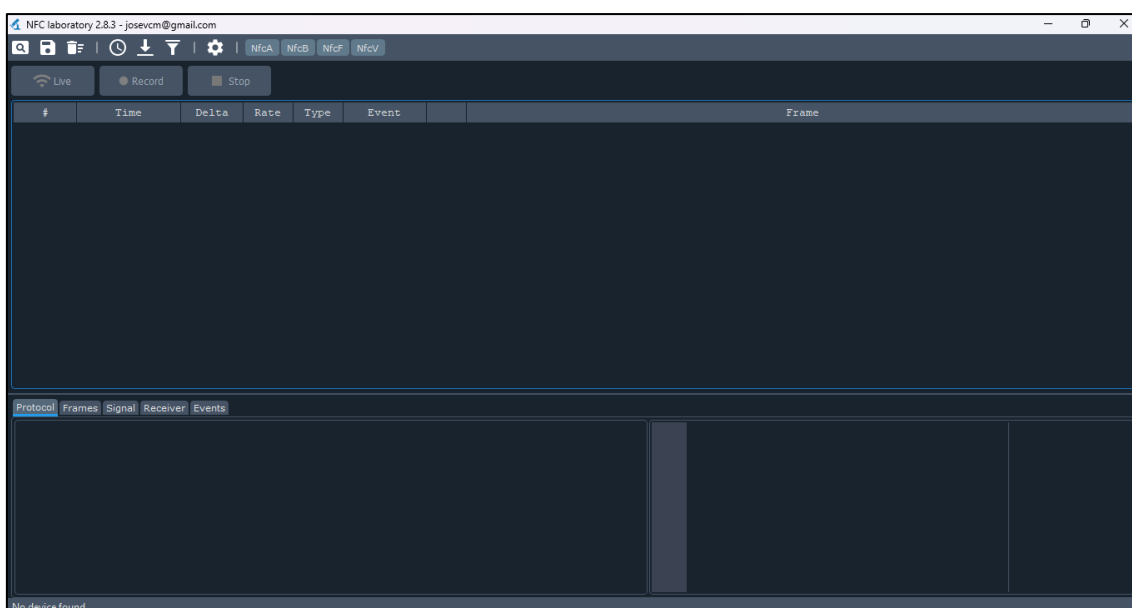
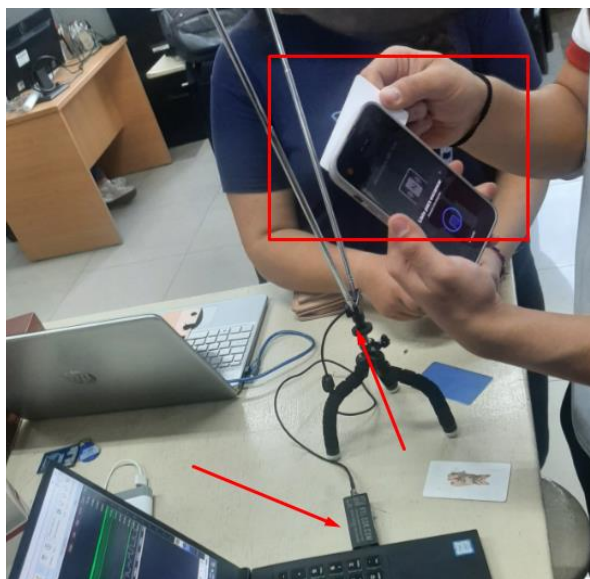


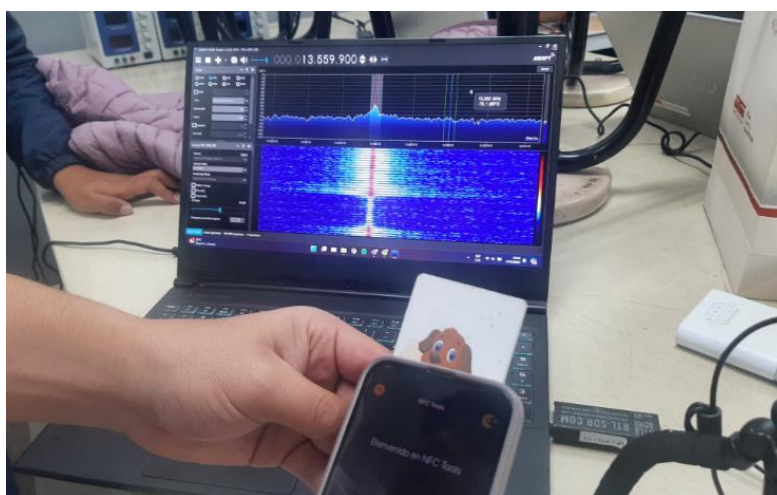
Figura 15. Interfaz de NFC-Laboratory.

En la siguiente figura podemos visualizar la conexión del RTL-SDR y el proceso que se utilizó para la lectura de las tarjetas RTL, para ello utilizamos una antena de tipo conejo conectada al RTL y mediante un Smartphone que acepta la tecnología NFC podemos realizar la lectura de esta tarjeta para que la antena pueda capturar la señal del espectro.



*Figura 16. Conexión de RTL-SDR para lectura de tarjetas RFID.*

En la siguiente figura podemos visualizar la captura del espectro que se realiza mediante el software SDRSharp cuando la tarjeta es leída por el teléfono cerca de la antena del RTL.



*Figura 17. Lectura de tarjeta RFID y espectro en SDRSharp.*

Por último, mediante el software de NFC Laboratory, si damos clic en la sección Live, podremos capturar en vivo los paquetes que está capturando el RTL-SDR, tal como se aprecia en la siguiente figura, entonces ya estaría listo para su uso.



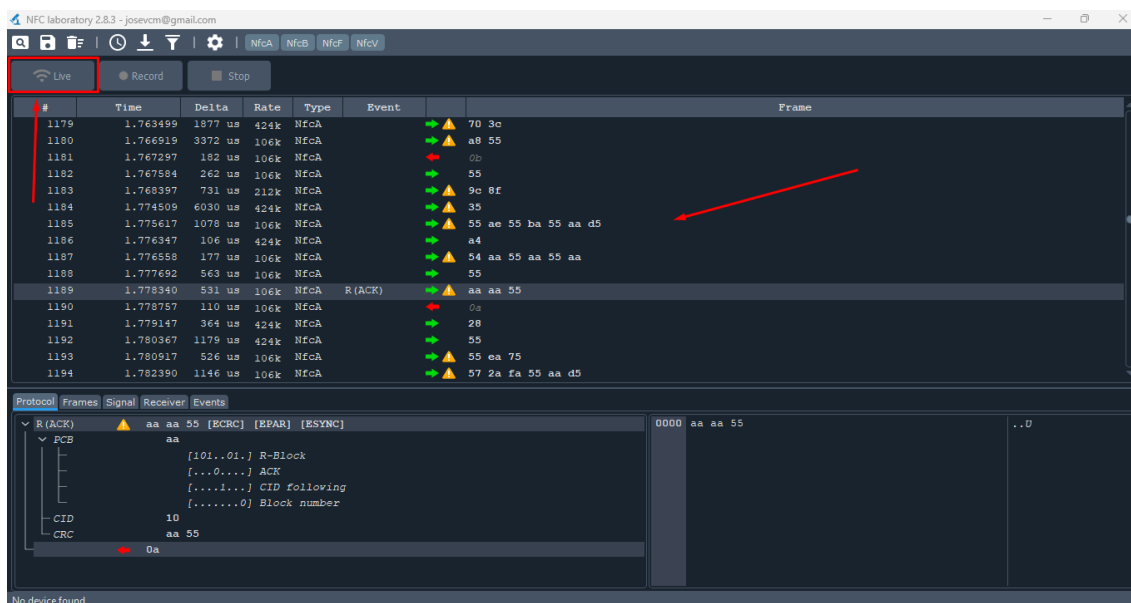


Figura 18. Captura de paquetes NfcA mediante NFC Laboratory.

Los resultados de esta práctica se pueden evidenciar en la siguiente sección, que corresponden a la captura de la señal de las tarjetas RFID mediante el RTL para poder compararlas con el protocolo ISO14443A el cual se señala en el DataSheet MF1S50YYX\_V1.

### Grabación de WAV en SDR Sharp.

Para la grabación de un archivo .wav vamos a realizar la captura de la señal con una frecuencia central en 13.56MHz, en este caso vamos a posicionar las configuraciones de radio en AM y con un ancho de banda de 212KHz y el Sample Rate en 2.4 MSPS.

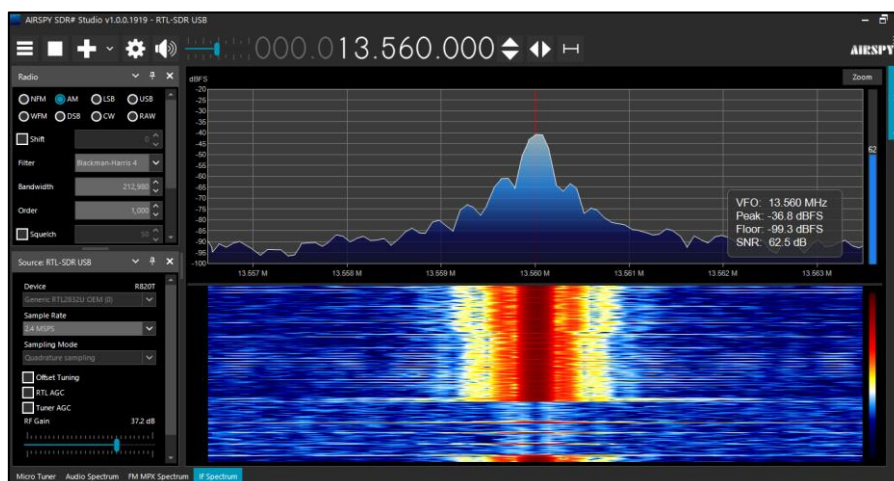


Figura 19. Captura de señal RD mediante SDR Sharp.

Como se puede visualizar en la siguiente figura, mediante el módulo denominado “Baseband Recorder” donde podremos configurar las opciones para la grabación del archivo .WAV.

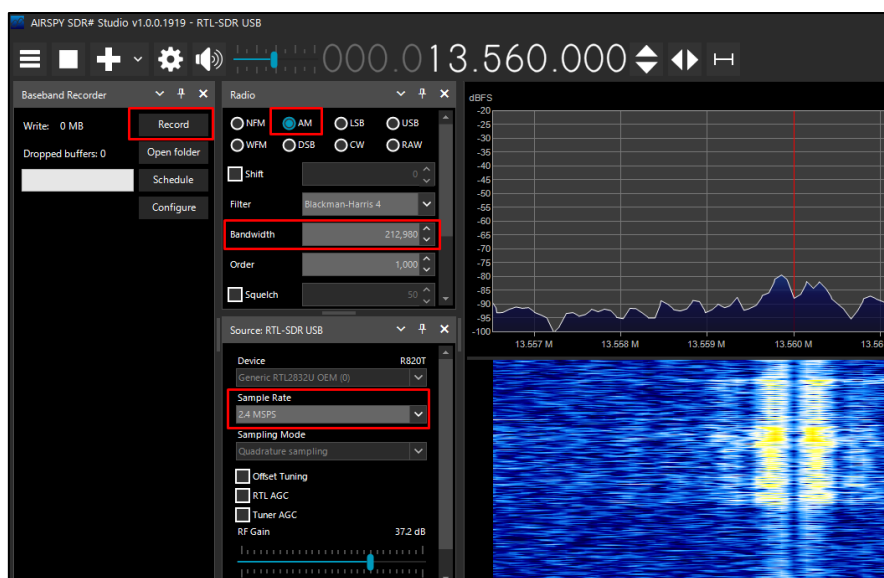


Figura 20. Grabación de archivo .wav

En el cuadro que se ve a continuación podremos seleccionar el formato del audio, este debe estar en formato WAV FULL, de igual forma se selecciona una carpeta para guardar el archivo generado. Una vez tengamos estas configuraciones ya podemos grabar los .wav necesarios.

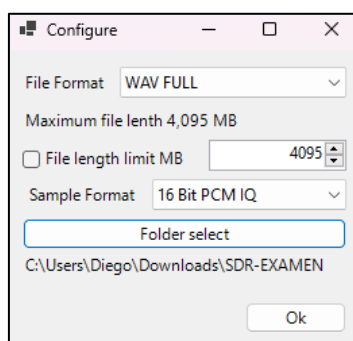


Figura 21. Configuraciones de archivo WAV.

## RESULTADOS

Los resultados de la práctica se basan en el proceso de comunicación que siguen las tarjetas RFID al momento de iniciar la comunicación con un lector, en este caso esta comunicación involucra algunos pasos fundamentales desde que se inicia el proceso hasta el final o cierre de comunicación.

### Proceso de Inicialización y Anticollisión.

#### PASO 1

El paso número 1 el lector se encarga de enviar una trama de solicitud denominada REQA cuando se cuenta con el uso de un NFC-A, esto lo envía para detectar si existe una tarjeta en el campo del lector. Generalmente se envía un REQA con un valor hexadecimal 0x26.

|     |           |         |      |      |      |             |
|-----|-----------|---------|------|------|------|-------------|
| 336 | 27.902197 | 68 ms   | 424k | NfcA |      | 6a          |
| 337 | 27.923526 | 21 ms   | 106k | NfcA | SEL1 | 93 70 d2 eb |
| 338 | 28.002445 | 79 ms   | 424k | NfcA | REQA | 26          |
| 339 | 28.056411 | 54 ms   | 106k | NfcA | HLTA | 50          |
| 340 | 28.065860 | 9374 us | 106k | NfcA | WUPA | 52          |

Protocol Frames Signal Receiver Events

REQA → 26

Figura 22. Captura de paquete con sentencia REQA.

## PASO 2

En el paso número 2 se estima que la tarjeta de una respuesta a la petición anterior, es decir que esta enviara un ATQA (Answer to Request) el cual está compuesto de 2 bytes que indica la presencia de una tarjeta en el campo del lector.

| b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning     |
|----|----|----|----|----|----|----|-------------|
| 0  | 1  | 0  | 0  | 1  | 1  | 0  | '26' = REQA |

|     |           |        |      |      |      |       |
|-----|-----------|--------|------|------|------|-------|
| 266 | 25.225173 | 100 ms | 106k | NfcA | HLTA | 50 00 |
| 267 | 25.286715 | 61 ms  | 424k | NfcA | REQA | 26    |
| 268 | 25.356501 | 70 ms  | 424k | NfcA |      | 55    |

Protocol Frames Signal Receiver Events

REQA → 26

Figura 23. Comparación de sentencia REQA con protocolo ISO/IEC 14443.

## PASO 3

En este paso el lector enviara un SELECT con el objetivo de seleccionar una tarjeta especifica en el campo del lector, para ello se utiliza la denominación SEL1, SEL2 o SEL3 dependiendo el nivel en el que se encuentre la tarjeta, en este caso se enviara un SEL1 con el código hexadecimal (93 20), el cual es un comando de inicio de anticollisión, generalmente este proceso es necesario cuando hay múltiples tarjetas NFC-A dentro del rango del lector.

|    |           |         |      |      |      |                            |
|----|-----------|---------|------|------|------|----------------------------|
| 86 | 34.764427 | 90 us   | 106k | NfcA | ATQA | 04                         |
| 87 | 34.765768 | 1227 us | 106k | NfcA | SEL1 | 93 20                      |
| 88 | 34.766038 | 85 us   | 106k | NfcA |      | 08 04                      |
| 89 | 34.767661 | 1490 us | 106k | NfcA | SEL1 | 93 70 08 b4 d1 b2 df bb 62 |
| 90 | 34.768525 | 86 us   | 106k | NfcA |      | 20 0c                      |
| 91 | 34.769675 | 1022 us | 106k | NfcA | RATS | e0 80 31 73                |
| 92 | 34.770662 | 631 us  | 106k | NfcA |      | 06                         |

Protocol Frames Signal Receiver Events

SEL1 → 93 20

NVB → 2

→ 08 04

Figura 24. Captura de paquete SEL1.

| b8 | b7 | b6 | b5 | b4                                   | b3 | b2 | b1 | Meaning                      |
|----|----|----|----|--------------------------------------|----|----|----|------------------------------|
| 1  | 0  | 0  | 1  | 0                                    | 0  | 1  | 1  | '93': Select cascade level 1 |
| 1  | 0  | 0  | 1  | 0                                    | 1  | 0  | 1  | '95': Select cascade level 2 |
| 1  | 0  | 0  | 1  | 0                                    | 1  | 1  | 1  | '97': Select cascade level 3 |
| 1  | 0  | 0  | 1  | other values except those here above |    |    |    | RFU                          |

|     |           |         |      |      |      |                            |  |
|-----|-----------|---------|------|------|------|----------------------------|--|
| 157 | 21.520318 | 5157 us | 424k | NfcA | SEL2 | 95                         |  |
| 202 | 23.965212 | 1429 us | 106k | NfcA | SEL1 | 93 70 d2 ff 60 1c 51 81 8f |  |
| 263 | 25.092768 | 1407 us | 106k | NfcA | SEL1 | 93 70                      |  |
| 293 | 25.659543 | 1429 us | 106k | NfcA | SEL1 | 93                         |  |
| 306 | 26.508860 | 104 ms  | 106k | NfcA | SEL1 | 93                         |  |
| 310 | 26.791639 | 129 ms  | 106k | NfcA | SEL1 | 93                         |  |
| 332 | 27.781788 | 8580 us | 106k | NfcA | SEL1 | 93                         |  |
| 337 | 27.923526 | 21 ms   | 106k | NfcA | SEL1 | 93 70 d2 eb                |  |
| 344 | 28.207910 | 1429 us | 106k | NfcA | SEL1 | 93                         |  |
| 369 | 29.483060 | 111 ms  | 106k | NfcA | SEL1 | 93 70 d6 ff                |  |
| 482 | 32.151346 | 1632 us | 424k | NfcA | SEL3 | 97                         |  |

Figura 25. Comparación de sentencia SEL con protocolo ISO/IEC 14443

Luego de esto la tarjeta responde con el UID completo o parcial al anterior comando.

|     |           |         |      |      |      |                            |
|-----|-----------|---------|------|------|------|----------------------------|
| 200 | 23.869965 | 134 ms  | 424k | NfcA |      | 2a                         |
| 201 | 23.963707 | 94 ms   | 106k | NfcA | WUPA | 52                         |
| 202 | 23.965212 | 1429 us | 106k | NfcA | SEL1 | 93 70 d2 ff 60 1c 51 81 8f |
| 203 | 24.031401 | 65 ms   | 424k | NfcA |      | 00                         |
| 204 | 24.037256 | 5834 us | 424k | NfcA |      | 6a                         |

| Protocol | Frames                     | Signal | Receiver | Events |
|----------|----------------------------|--------|----------|--------|
| SEL1     | 93 70 d2 ff 60 1c 51 81 8f |        |          |        |
| NVB      | 7                          |        |          |        |
| UID      | d2 ff 60 1c                |        |          |        |
| BCC      | 51                         |        |          |        |
| CRC      | 81 8f                      |        |          |        |

Figura 26. Captura de segundo paquete SEL1.

Una vez que la tarjeta responde con el UID, el SEL1 ahora se envía con un comando hexadecimal x93 0x70 que representa la selección de esta tarjeta, por lo que seguido de esta secuencia se aumentara el UID de la tarjeta seleccionada.

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning                      |
|----|----|----|----|----|----|----|----|------------------------------|
| 1  | 0  | 0  | 1  | 0  | 0  | 1  | 1  | '93': Select cascade level 1 |

|    |           |         |      |      |      |                            |
|----|-----------|---------|------|------|------|----------------------------|
| 55 | 34.529975 | 1530 us | 106k | NfcA | SEL1 | 93 70 08 29 3b 0b 11 24 bf |
| 56 | 34.531988 | 1235 us | 106k | NfcA | RATS | e0 80 31 73                |
| 57 | 34.532966 | 624 us  | 106k | NfcA |      | 0d                         |

| Protocol | Frames                     | Signal | Receiver | Events |
|----------|----------------------------|--------|----------|--------|
| SEL1     | 93 70 08 29 3b 0b 11 24 bf |        |          |        |
| NVB      | 7                          |        |          |        |
| UID      | 08 29 3b 0b                |        |          |        |
| BCC      | 11                         |        |          |        |
| CRC      | 24 bf                      |        |          |        |

Figura 27. Comparación de sentencia SEL1 con protocolo ISO/IEC 14443

## Activación de la tarjeta.

### PASO 4.

En el paso número 4 el lector hace un envío de un RATS con el objetivo de solicitar información de activación de la tarjeta, este lo envía con el parámetro hexadecimal 0xE0. A esta acción la tarjeta responderá con un ATS, el cual proporciona información como el tamaño del FSD y otros parámetros de comunicación.

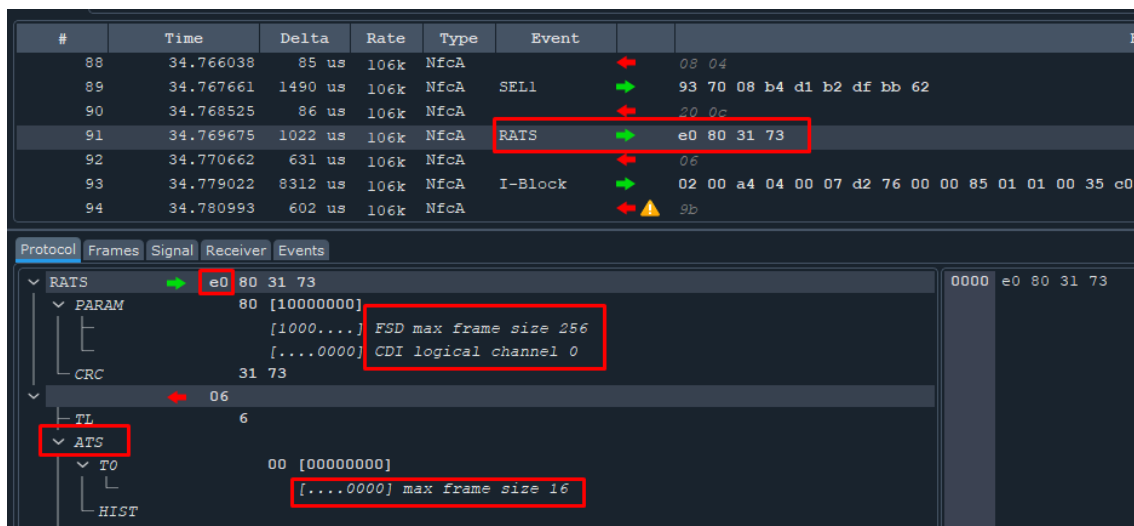


Figura 28. Captura de paquete con sentencia RATS.

## Intercambio de datos

### PASO 5.

En este paso se realiza el intercambio de APDUs, generalmente el comando APDU es CLA, la respuesta a este APDU es un Data.

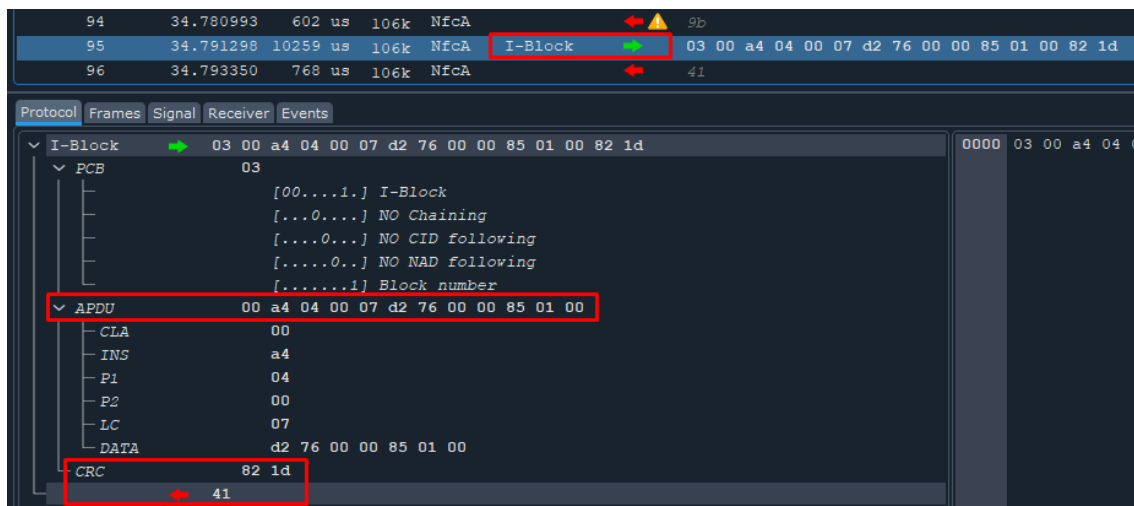


Figura 29. Captura de paquete I-Block, APDU.

## Finalización de la comunicación.

### PASO 6.

En este paso el lector envía un comando denominado DESELECT que termina la comunicación con la tarjeta, generalmente en NFC-A se utiliza el DESELECT con un código hexadecimal 0xC2.

| #   | Time      | Delta    | Rate | Type | Event        |   |          |
|-----|-----------|----------|------|------|--------------|---|----------|
| 104 | 34.982990 | 335 us   | 106k | NfcA |              | ← | fe       |
| 105 | 34.993351 | 10282 us | 106k | NfcA | S (Deselect) | → | c2 e0 b4 |
| 106 | 34.996117 | 2503 us  | 106k | NfcA |              | ← | 03       |
| 107 | 35.004254 | 8117 us  | 106k | NfcA | S (Deselect) | → | c2 e0 b4 |
| 108 | 35.015149 | 10633 us | 106k | NfcA | S (Deselect) | → | c2 e0 b4 |
| 109 | 35.019502 | 4089 us  | 106k | NfcA |              | ← | 08       |
| 110 | 35.026110 | 6563 us  | 106k | NfcA |              | → | 38 6d    |

|                            |        |        |          |        |
|----------------------------|--------|--------|----------|--------|
| Protocol                   | Frames | Signal | Receiver | Events |
| S-Block → c2 e0 b4         |        |        |          |        |
| PCB c2                     |        |        |          |        |
| [11...010] S-Block         |        |        |          |        |
| [...00....] DESELECT       |        |        |          |        |
| [...0...] NO CID following |        |        |          |        |
| CRC e0 b4                  |        |        |          |        |
| ← 03                       |        |        |          |        |

Figura 30. Captura de paquete con sentencia DESELECT.

## Comandos de gestión.

### HALT

El comando HALT es utilizado para poner una tarjeta en estado de reposo, esto permite que el lector pueda gestionar múltiples tarjetas en el campo de radiofrecuencia, lo que permite ignorar una tarjeta específica para evitar las colisiones, generalmente se envía con el código hexadecimal 0x50 0x00.

|                       |           |         |       |      |      |   |             |
|-----------------------|-----------|---------|-------|------|------|---|-------------|
| First bit transmitted |           |         |       |      |      |   |             |
| S                     | '50'      | '00'    | CRC_A | E    |      |   |             |
| 132                   | 36.188302 | 532 ms  | 106k  | NfcA | WUPA | → | 52          |
| 133                   | 36.192313 | 3935 us | 106k  | NfcA | HALT | → | 50 00 57 cd |
| 134                   | 36.227820 | 35 ms   | 106k  | NfcA | WUPA | → | 52          |
| 135                   | 36.229326 | 1430 us | 106k  | NfcA | SEL1 | → | 93 20       |

|                    |        |        |          |        |
|--------------------|--------|--------|----------|--------|
| Protocol           | Frames | Signal | Receiver | Events |
| HLTA → 50 00 57 cd |        |        |          |        |
| CRC 57 cd          |        |        |          |        |

Figura 31. Comparación de sentencia CRC con protocolo ISO/IEC 14443

## WUPA

El comando WUPA por otro lado sirve para despertar a las tarjetas que han sido puestas en estado de reposo, generalmente este se utiliza con el código hexadecimal 0x52, generalmente la tarjeta responderá a este comando con un ATQA.

| b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning     |
|----|----|----|----|----|----|----|-------------|
| 0  | 1  | 0  | 0  | 1  | 1  | 0  | '26' = REQA |
| 1  | 0  | 1  | 0  | 0  | 1  | 0  | '52' = WUPA |

|    |           |         |      |      |      |   |             |
|----|-----------|---------|------|------|------|---|-------------|
| 20 | 21.697878 | 6248 us | 106k | NfcA | REQA | → | 26          |
| 21 | 21.829113 | 131 ms  | 106k | NfcA |      | → | 15 f0 a5    |
| 22 | 21.829847 | 417 us  | 106k | NfcA |      | → | e9          |
| 23 | 21.834852 | 4990 us | 106k | NfcA | WUPA | → | 52          |
| 24 | 21.836392 | 1465 us | 106k | NfcA |      | → | 19 47 fd 1f |

Figura 32. Comparación de sentencia WUPA Y REQA con protocolo ISO/IEC 14443

| b16 | b15 | b14 | b13 | b12                | b11 | b10 | b9 | b8                 | b7 | b6  | b5                      | b4 | b3 | b2 | b1 |
|-----|-----|-----|-----|--------------------|-----|-----|----|--------------------|----|-----|-------------------------|----|----|----|----|
| RFU |     |     |     | Proprietary coding |     |     |    | UID size bit frame |    | RFU | Bit frame anticollision |    |    |    |    |

|     |           |         |      |      |      |   |    |
|-----|-----------|---------|------|------|------|---|----|
| 699 | 65.555715 | 6450 us | 106k | NfcA | WUPA | → | 52 |
| 700 | 65.555945 | 153 us  | 106k | NfcA | ATQA | → | 01 |
| 701 | 65.557459 | 1475 us | 106k | NfcA |      | → | 00 |

| Protocol | Frames | Signal | Receiver | Events                               |
|----------|--------|--------|----------|--------------------------------------|
| WUPA     | →      | 52     |          |                                      |
| ATQA     | →      | 01     |          |                                      |
|          |        |        |          | 0001 [0000000000000001]              |
|          |        |        |          | [...0000.....] proprietary type 0    |
|          |        |        |          | [.....00.....] single size UID       |
|          |        |        |          | [.....00001] bit frame anticollision |

Figura 33. Comparación de sentencia ATQA con protocolo ISO/IEC 14443

## NACK

Dentro de los diferentes eventos se logra visualizar el NACK, lo que se indica aquí, es que el lector NFC está intentando comunicarse con la tarjeta, pero está recibiendo varios mensajes de NACK de vuelta, lo que indica que la tarjeta no está pudiendo procesar correctamente los mensajes que está recibiendo. Este tipo de problemas contiene varios factores, como interferencias, mala calidad de la señal, o problemas con la tarjeta NFC.



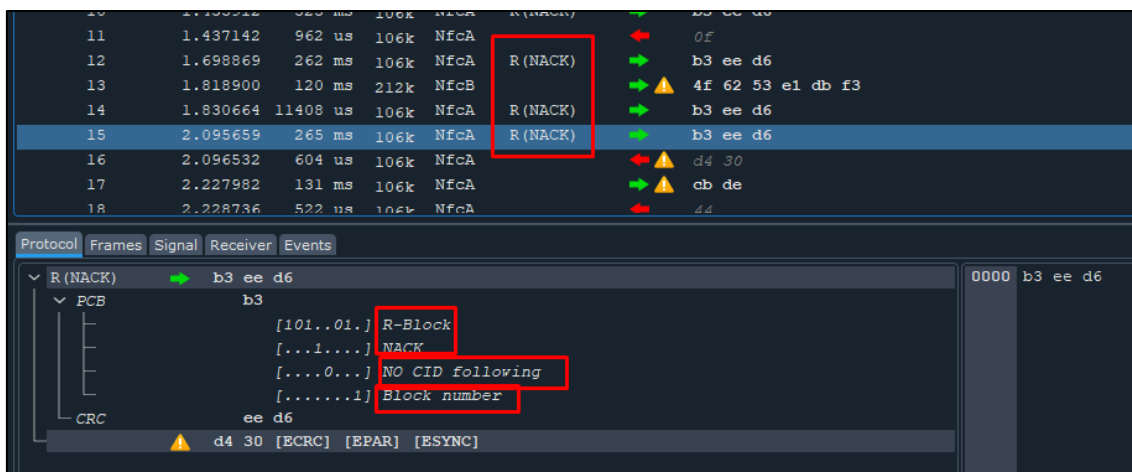


Figura 34. Captura de paquete con sentencia NACK.

Los mensajes se registran con marcas de tiempo, deltas de tiempo, tasas de transmisión y tipos específicos de eventos. Entre los eventos clave se encuentran S(Deselect), WUPA, ATQA, HALT, REQ, SEL1 y RATS, que representan comandos de deselección, activación, respuestas a activación, comandos de parada, solicitudes de comando, selección de nivel 1 y solicitud de parámetros de comunicación, respectivamente. Los íconos de advertencia en algunos mensajes indican posibles errores o eventos inusuales, como el S(Deselect).

Para interpretar técnicamente estos eventos, S(Deselect) se utiliza para deseleccionar la tarjeta NFC, mientras que WUPA y ATQA manejan la activación de la tarjeta. HALT pone la tarjeta en espera, SEL1 selecciona la tarjeta en un nivel específico y RATS negocia las condiciones de comunicación.

| #   | Time      | Delta    | Rate | Type | Event       |   |                            |
|-----|-----------|----------|------|------|-------------|---|----------------------------|
| 147 | 36.268707 | 9541 us  | 106k | NfcA | S(Deselect) | → | c2 e0 b4                   |
| 148 | 36.279558 | 10585 us | 106k | NfcA | S(Deselect) | → | c2 e0 b4                   |
| 149 | 36.290500 | 10679 us | 106k | NfcA | S(Deselect) | → | c2 e0 b4                   |
| 150 | 36.301338 | 10575 us | 106k | NfcA | S(Deselect) | → | c2 e0 b4                   |
| 151 | 36.302631 | 1029 us  | 106k | NfcA | WUPA        | → | 52                         |
| 152 | 36.834006 | 531 ms   | 106k | NfcA | ATQA        | → | e4                         |
| 153 | 36.834173 | 90 us    | 106k | NfcA | HALT        | → | 50 00 57 cd                |
| 154 | 36.838017 | 3721 us  | 106k | NfcA | REQ         | → | 06 00 ff ff 00 03 39 42    |
| 155 | 36.860761 | 22 ms    | 212k | NfcF | WUPA        | → | 52                         |
| 156 | 36.873575 | 12210 us | 106k | NfcA | ATQA        | → | 04                         |
| 157 | 36.873742 | 91 us    | 106k | NfcA | SEL1        | → | 93 20                      |
| 158 | 36.875085 | 1295 us  | 106k | NfcA | SEL1        | → | 08                         |
| 159 | 36.875353 | 86 us    | 106k | NfcA | SEL1        | → | 93 70 08 04 34 d7 ef 55 19 |
| 160 | 36.876976 | 1580 us  | 106k | NfcA | SEL1        | → | 20                         |
| 161 | 36.877840 | 86 us    | 106k | NfcA | RATS        | → | e0 80 31 73                |
| 162 | 36.878992 | 995 us   | 106k | NfcA | S(Deselect) | → | fd                         |
| 163 | 36.880110 | 765 us   | 106k | NfcA | S(Deselect) | → | c2 e0 b4                   |
| 164 | 36.885598 | 5450 us  | 106k | NfcA | WUPA        | → | 02                         |
| 165 | 36.886123 | 261 us   | 106k | NfcA | WUPA        | → | 52                         |
| 166 | 36.888922 | 2752 us  | 106k | NfcA | SEL1        | → | 93 70 08 04 34 d7 ef 55 19 |
| 167 | 36.890426 | 1429 us  | 106k | NfcA | WUPA        | → | 52                         |
| 168 | 36.926843 | 36 ms    | 106k | NfcA | HALT        | → | 50 00 57 cd                |
| 169 | 36.930853 | 3935 us  | 106k | NfcA | REQ         | → | 06 00 ff ff 00 03 39 42    |
| 170 | 36.953597 | 22 ms    | 212k | NfcF | WUPA        | → | 52                         |
| 171 | 36.966412 | 12211 us | 106k | NfcA | SEL1        | → | 93 20                      |
| 172 | 36.967919 | 1431 us  | 106k | NfcA | SEL1        | → | 93 70 08 93 1d aa 2c b5 8b |
| 173 | 36.969811 | 1708 us  | 106k | NfcA | SEL1        | → | e0 80 31 73                |
| 174 | 36.971825 | 1241 us  | 106k | NfcA | RATS        | → | fd                         |
| 175 | 36.972883 | 704 us   | 106k | NfcA | S(Deselect) | → | c2 e0 b4                   |

Figura 35. Captura general de paquetes.



El RATS solicita los parámetros de comunicación de la tarjeta, especificando un tamaño máximo de trama de 256 bytes y un canal lógico de 0. La respuesta ATS indica que la tarjeta soporta una tasa de bits de 424 kbps en ambas direcciones, un tiempo de espera de trama de 0.30 ms, y un tiempo de guardia de inicio de 0.60 ms.

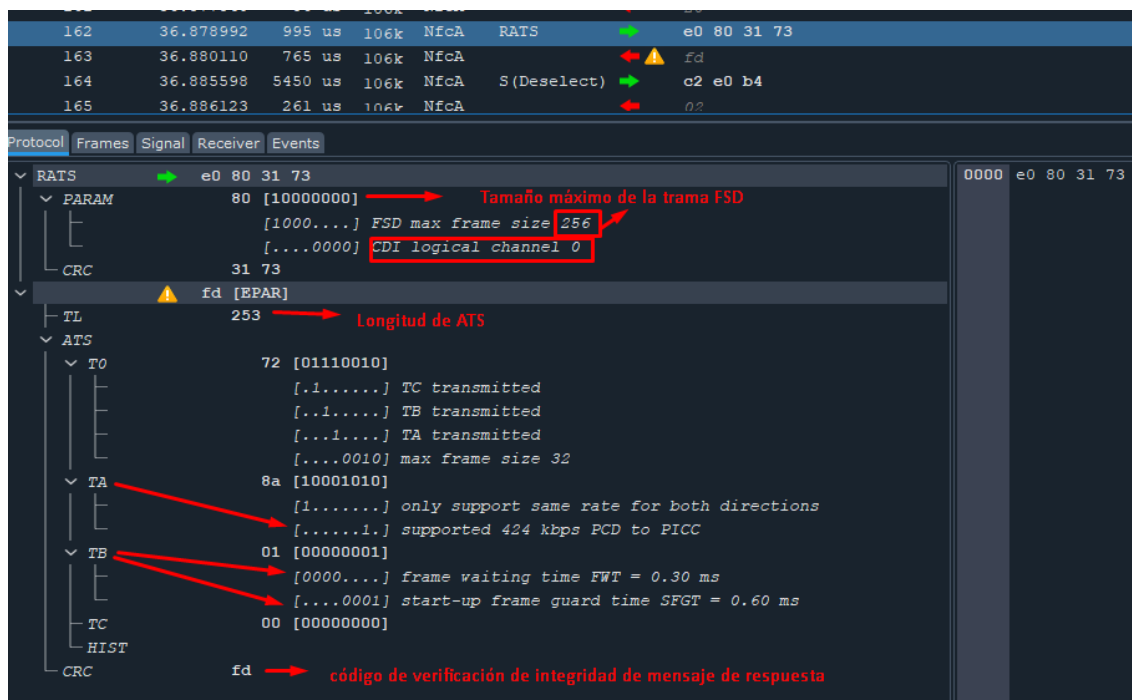


Figura 36. Captura de paquete con sentencia RATS.

## AUTH

Dentro de los diferentes eventos se logra visualizar el evento que indica la comunicación entre el lector NFC y la tarjeta, esto verifica la autenticación con acceso seguro. Al generar el proceso de autenticación se indica un valor de 60 que representa un código de éxito.

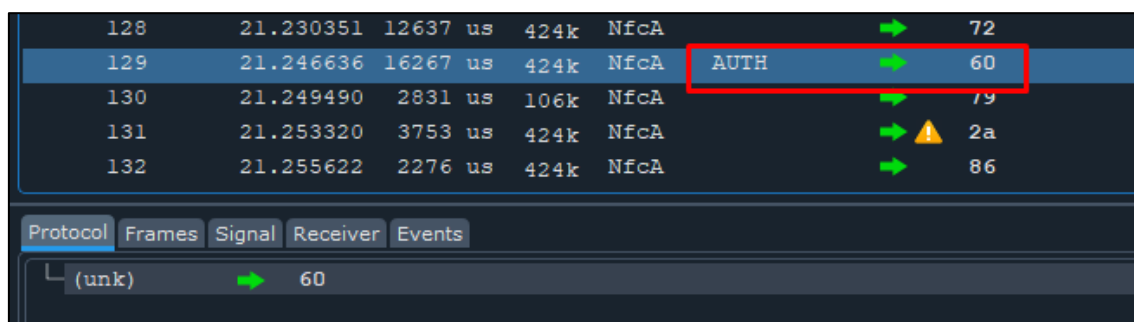


Figura 37. Captura de paquete con sentencia AUTH.

## CONCLUSIONES

La secuencia de selección describe el proceso mediante el cual el PCD obtiene el UID de un PICC y lo selecciona para una comunicación posterior. Desde la transmisión de comandos como REQA y WUPA para sondar los PICCs hasta el manejo de colisiones durante el proceso de anticolisión, se establece un flujo claro para la selección eficiente del PICC deseado.

El diagrama de estado del PICC Tipo A describe los diferentes estados de funcionamiento del PICC, desde POWER-OFF hasta HALT, cada uno con sus condiciones de salida y transiciones definidas. Estos estados, como el IDLE, READY, ACTIVE, y sus variantes, como READY\* y ACTIVE\*, están diseñados para gestionar la comunicación entre el PICC y el PCD de manera eficiente y confiable (ISO/IEC 14443-3).

Se identifican cinco comandos principales utilizados por el PCD para gestionar la comunicación con varios PICCs, que incluyen REQA, WUPA, ANTICOLLISION, SELECT y HLTA. Estos comandos son esenciales para la detección, selección y comunicación con los PICCs, y se definen en función de sus formatos de byte y trama.

## RECOMENDACIONES

Dado que el documento hace referencia a la norma ISO/IEC 14443-3 para describir el comportamiento de los PICCs de Tipo A, sería recomendable estudiar detenidamente esta norma para comprender completamente el funcionamiento de los estados, comandos y secuencias de comunicación mencionados.

Antes de implementar cualquier sistema de comunicación NFC basado en estas especificaciones, se deben realizar pruebas y validaciones rigurosas para garantizar la interoperabilidad y la confiabilidad del sistema. Esto implica probar diferentes escenarios de comunicación y manejo de errores para asegurar un funcionamiento adecuado.

Dado que la comunicación NFC a menudo se utiliza en aplicaciones que involucran datos sensibles, como pagos móviles o acceso seguro, es fundamental seguir las mejores prácticas de seguridad. Esto incluye la implementación de mecanismos de autenticación robustos, el cifrado adecuado de datos y la protección contra ataques de manipulación y clonación de tarjetas.

## BIBLIOGRAFIA

- IEEE. (2001). *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision*. Ginebra, Suiza: ISO/IEC.
- Josevcm. (05 de 09 de 2023). *github.com*. Obtenido de *github.com*: <https://github.com/josevcm/nfc-laboratory>
- PUBLIC, C. (2018). *MIFARE Classic EV1 1K - Mainstream contactless smart card: IC for fast and easy solution development (Rev. 3.2)*. Eindhoven, Países Bajos: NXP Semiconductors.