



OPEN THREAT RESEARCH

EMPOWERING THE INFOSEC COMMUNITY

Fundamentos de Lógicas de Detección basadas en Data

SANS Threat Hunting Summit – Español 2021

Quienes somos?



Colaboración y Proyectos Open-Source

Roberto Rodriguez



[@Cyb3rWard0g](#)

- Microsoft Threat Intelligence Center (MSTIC)

Jose Rodriguez



[@Cyb3rPandaH](#)

- ATT&CK Team Member (Data Sources Project)

➤ Colaboración Abierta ❤️

- Open Threat Research
[@OTR_Community](#)
- Proyectos Open-Source
 - Threat Hunter Playbook
[@HunterPlaybook](#)
 - Security Datasets
[@SecDatasets](#)
 - OSSEM
[@OSSEM_Project](#)
 - Simuland
 - Blacksmith & more..

Agenda

- Usas Estadística en el desarrollo de lógicas de detección?
- Que es una lógica de detection?
- Modelos para generar lógicas de detección
 - Impulsado por el Usuario
 - Impulsado por la data
- Cómo empezar a usar el modelo impulsado por data?
 - Entendiendo los tipos de datos
 - Aplicaciones
- Conclusiones

Usas Matemática/Estadística al
desarrollar lógicas de detección?

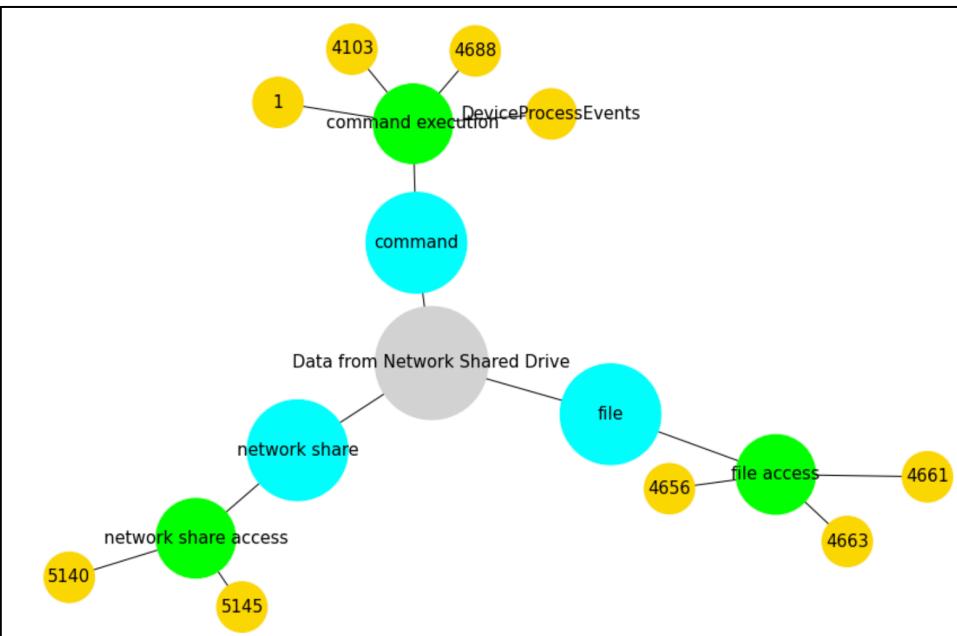
Qué es una lógica de detección?

Lógicas de Detección

Guía o
referencia
sobre

Tecnología,
Técnicas de análisis,
y Procedimientos

Identificación de
actividad maliciosa
en nuestra red



```
df = spark.sql(  
    ...  
    SELECT Image, ImageLoaded, Description, ProcessGuid  
    FROM mordorTable  
    WHERE Channel = "Microsoft-Windows-Sysmon/Operational"  
        AND EventID = 7  
        AND LOWER(ImageLoaded) IN (  
            'c:\windows\system32\wbem\scrcons.exe',  
            'c:\windows\system32\vbscript.dll',  
            'c:\windows\system32\wbem\wbemdisp.dll',  
            'c:\windows\system32\wshom.ocx',  
            'c:\windows\system32\scrrun.dll'  
        )  
    ...  
)  
df.show(10, False)
```

Image	ImageLoaded	Description
C:\Windows\System32\wbem\scrcons.exe C:\Windows\System32\wbem\scrcons.exe	WMI Standard Event Con	
C:\Windows\System32\wbem\scrcons.exe C:\Windows\System32\vbscript.dll	Microsoft ® VBScript	
C:\Windows\System32\wbem\scrcons.exe C:\Windows\System32\wbem\wbemdisp.dll	WMI Scripting	
C:\Windows\System32\wbem\scrcons.exe C:\Windows\System32\wshom.ocx	Windows Script Host Ru	
C:\Windows\System32\wbem\scrcons.exe C:\Windows\System32\scrrun.dll	Microsoft ® Script Run	

Cómo generar una lógica de detección?

2 Modelos para Generación de Lógicas de Detección

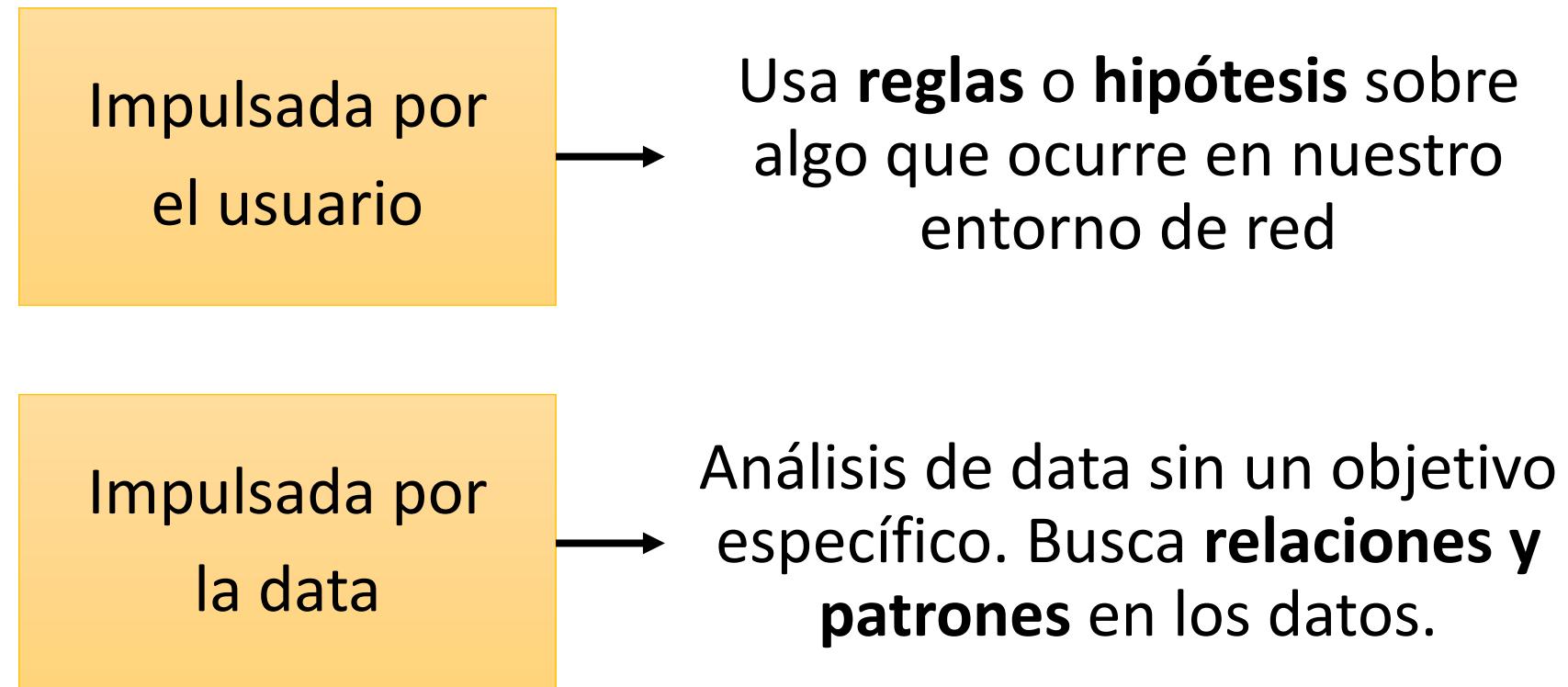
2 Modelos para Generación de Lógicas de Detección

Impulsada por
el usuario

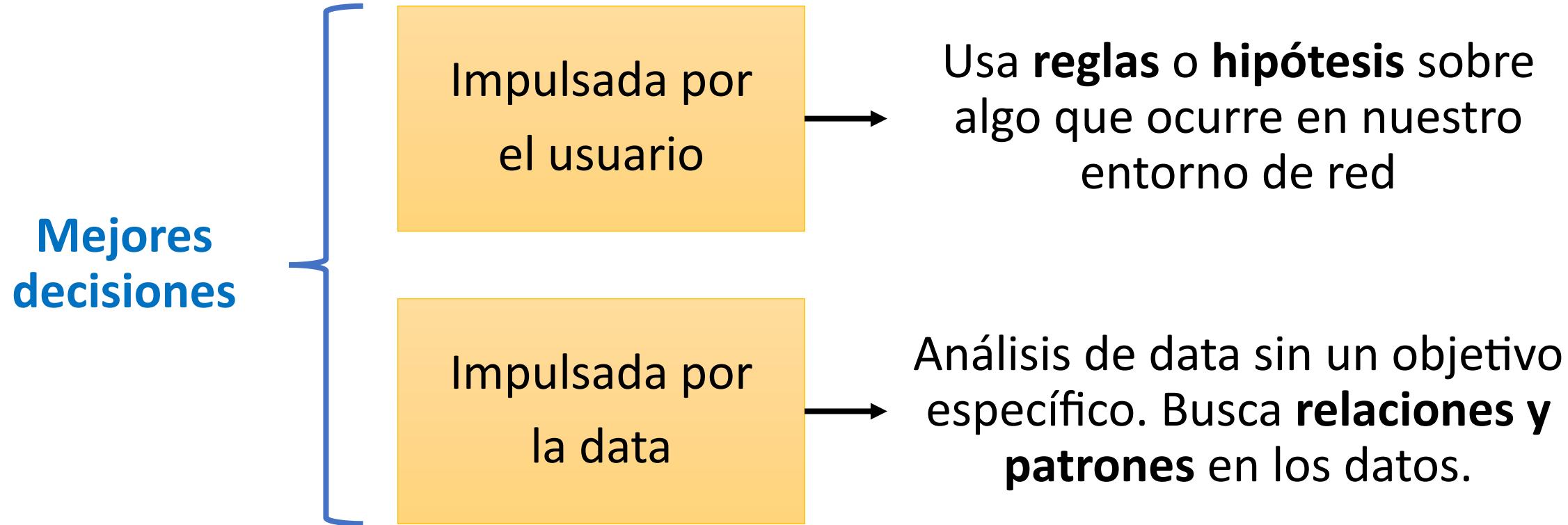


Usa **reglas** o **hipótesis** sobre
algo que ocurre en nuestro
entorno de red

2 Modelos para Generación de Lógicas de Detección



2 Modelos para Generación de Lógicas de Detección



Lógicas de detección impulsadas por el usuario

TTP de un Adversario - ATT&CK®

Abuse Elevation Control Mechanism: Bypass User Account Control

Other sub-techniques of Abuse Elevation Control Mechanism (4)

Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action. ^[1]

If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs can elevate privileges or execute some elevated Component Object Model objects without prompting the user through the UAC notification box. ^[2] ^[3] An example of this is use of [Rundll32](#) to load a specifically crafted DLL which loads an auto-elevated Component Object Model object and performs a file operation in a protected directory which would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user. ^[4]

Many methods have been discovered to bypass UAC. The Github readme page for UACME contains an extensive list of methods^[5] that have been discovered and implemented, but may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as:

- `eventvwr.exe` can auto-elevate and execute a specified binary or script. ^[6] ^[7]

Another bypass is possible through some lateral movement techniques if credentials for an account with administrator privileges are known, since UAC is a single system security mechanism, and the privilege or integrity of a process running on one system will be unknown on remote systems and default to high integrity.^[8]

ID: T1548.002

Sub-technique of: [T1548](#)

- ① Tactics: [Privilege Escalation](#), [Defense Evasion](#)
- ① Platforms: Windows
- ① Permissions Required: Administrator, User
- ① Effective Permissions: Administrator
- ① Data Sources: [Command](#): Command Execution, [Process](#): Process Creation, [Process](#): Process Metadata, [Windows Registry](#): Windows Registry Key Modification
- ① Defense Bypassed: Windows User Account Control

Contributors: Casey Smith; Stefan Kanthak

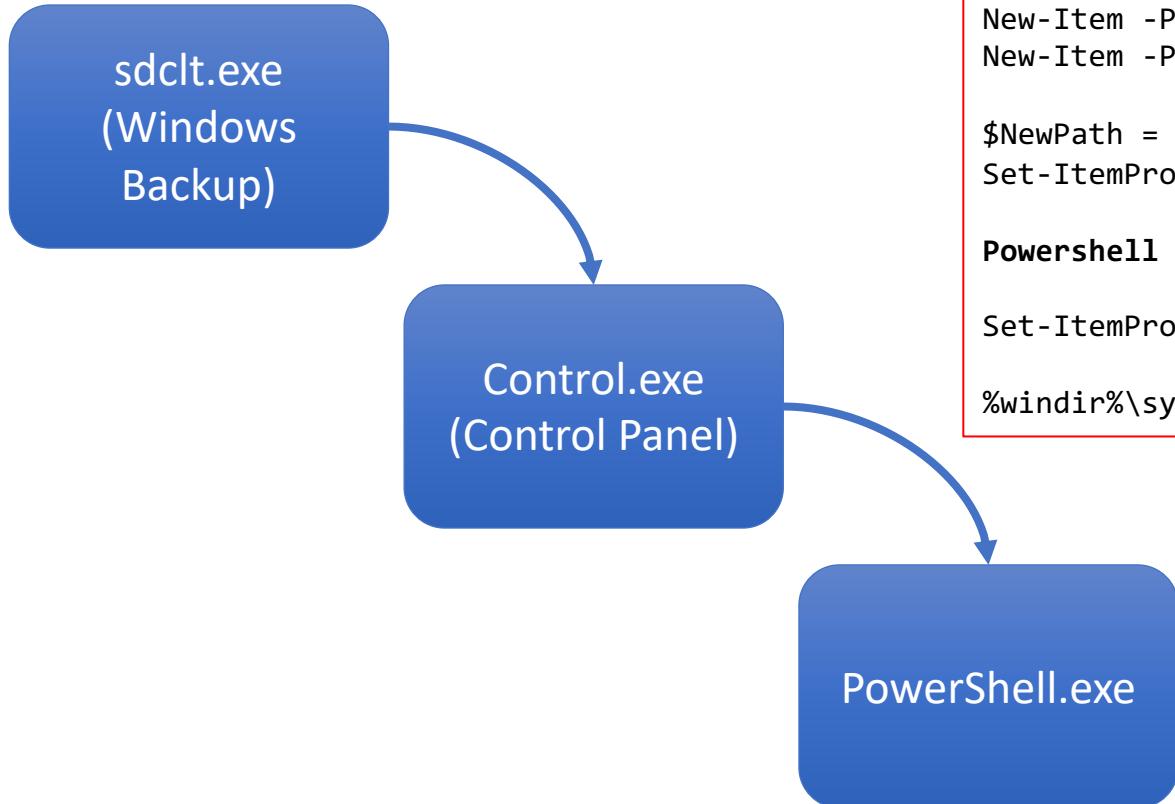
Version: 2.0

Created: 30 January 2020

Last Modified: 22 July 2020

[Version Permalink](#)

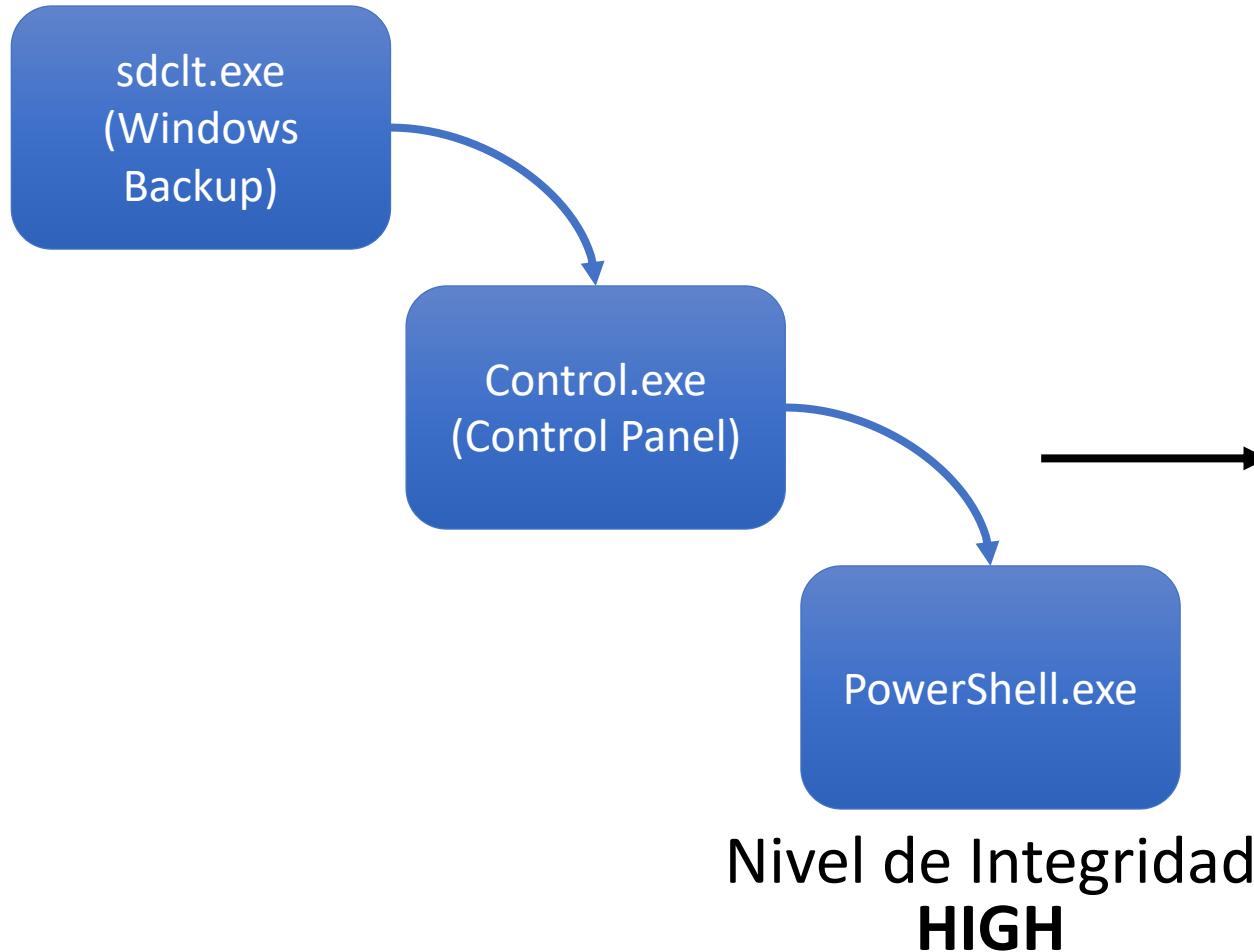
Hipótesis con respecto a Bypass UAC



```
New-Item -Path HKCU:\Software\Classes -Name Folder -Force;  
New-Item -Path HKCU:\Software\Classes\Folder -Name shell -Force;  
New-Item -Path HKCU:\Software\Classes\Folder\shell -Name open -Force;  
New-Item -Path HKCU:\Software\Classes\Folder\shell\open -Name command -Force;  
  
$NewPath = "HKCU:\Software\Classes\Folder\shell\open\command";  
Set-ItemProperty -Path $NewPath -Name "(Default)";  
  
Powershell ...  
  
Set-ItemProperty -Path $NewPath -Name "DelegateExecute" -Force;  
  
%windir%\system32\sdclt.exe
```

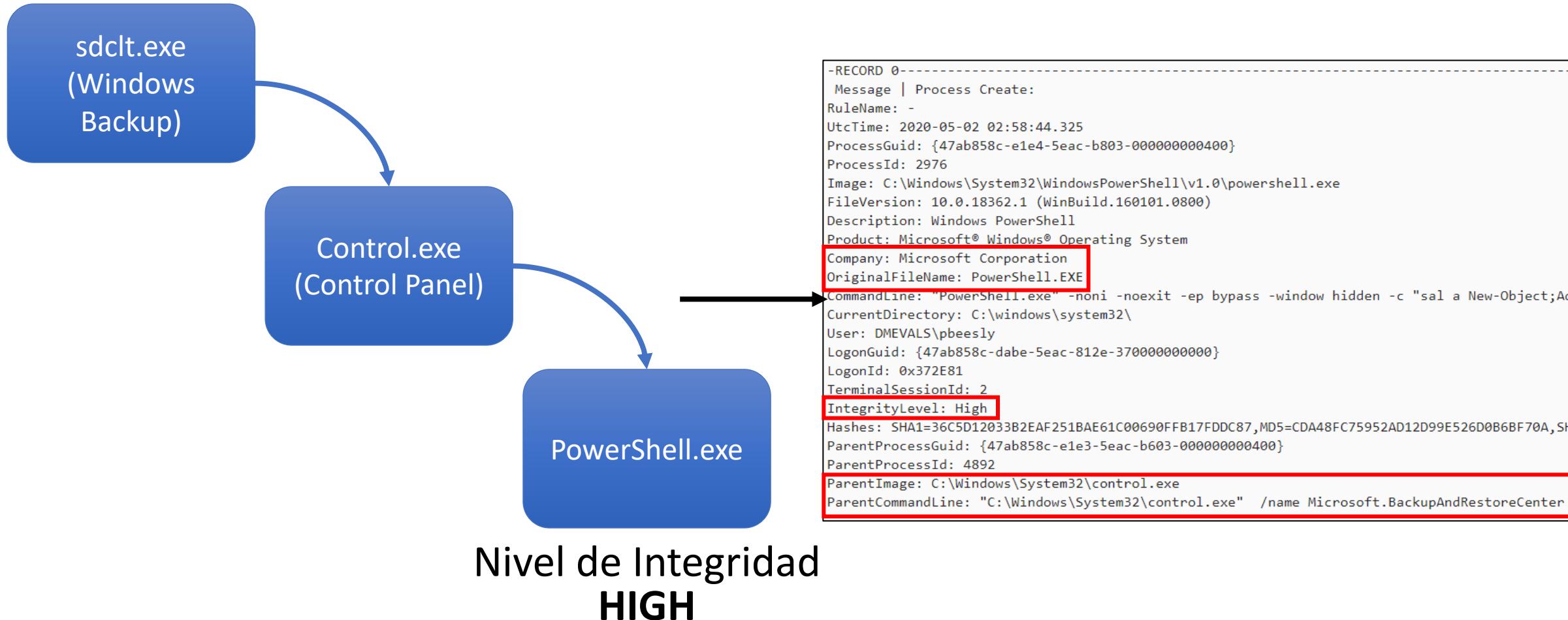
Nivel de Integridad
HIGH

Lógica de Detección con respecto a Bypass UAC



```
df = spark.sql(  
    ...  
    SELECT Message  
    FROM apt29Host a  
    INNER JOIN (  
        SELECT ProcessGuid  
        FROM apt29Host  
        WHERE Channel = "Microsoft-Windows-Sysmon/Operational"  
        AND EventID = 1  
        AND LOWER(Image) LIKE "%control.exe"  
        AND LOWER(ParentImage) LIKE "%sdclt.exe"  
    ) b  
    ON a.ParentProcessGuid = b.ProcessGuid  
    WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"  
    AND a.EventID = 1  
    AND a.IntegrityLevel = "High"  
    ...  
)  
df.show(100,truncate = False, vertical = True)
```

Lógica de Detección con respecto a Bypass UAC



Fue necesario usar
Matemática/Estadística?

Hemos usado lo básico de Matemática

```
df = spark.sql(  
    """  
    SELECT Message  
    FROM apt29Host  
    WHERE Channel = "Microsoft-Windows-Sysmon/Operational"  
        AND EventID = 1  
        AND LOWER(Image) LIKE "%sdclt.exe"  
        AND IntegrityLevel = "High"  
    """  
)  
df.show(100,truncate = False, vertical = True)
```

Hemos usado lo básico de Matemática

```
df = spark.sql(  
    ...  
    SELECT Message  
    FROM apt29Host  
    WHERE Channel = "Microsoft-Windows-Sysmon/Operational"  
        AND EventID = 1  
        AND LOWER(Image) LIKE "%sdclt.exe"  
        AND IntegrityLevel = "High"  
    ...  
)  
df.show(100,truncate = False, vertical = True)
```

**Hemos aplicado teoría
básica de conjuntos**

Hemos usado lo básico de Matemática

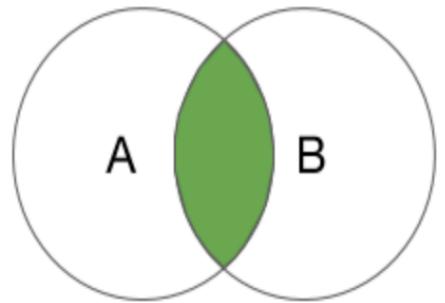
```
df = spark.sql(  
    ...  
    SELECT Message  
    FROM apt29Host  
    WHERE Channel = "Microsoft-Windows-Sysmon/Operational"  
        AND EventID = 1  
        AND LOWER(Image) LIKE "%sdclt.exe"  
        AND IntegrityLevel = "High"  
    ...  
)  
df.show(100,truncate = False, vertical = True)
```

Relación de pertenencia

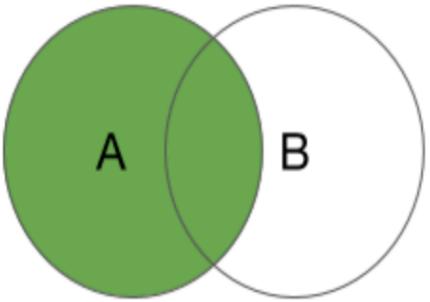
Intersección de condiciones

**Hemos aplicado teoría
básica de conjuntos**

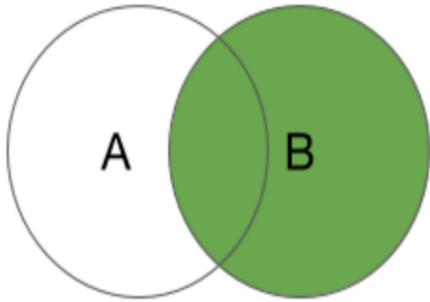
Operaciones con Conjuntos (JOINS)



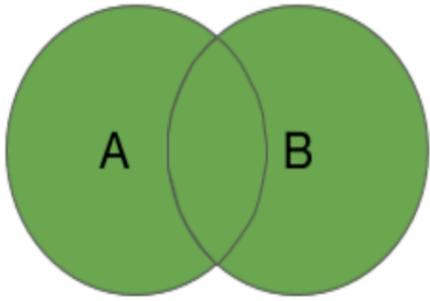
INNER JOIN



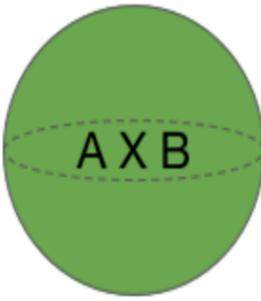
LEFT OUTER JOIN



RIGHT OUTER
JOIN

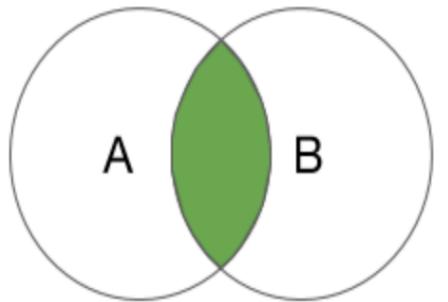


FULL OUTER
JOIN



CARTESIAN
(CROSS) JOIN

Operaciones con Conjuntos (JOINS)



INNER JOIN

```
df = spark.sql(  
    ...  
  
    SELECT Message  
    FROM apt29Host a  
    INNER JOIN '  
        SELECT ProcessGuid  
        FROM apt29Host  
        WHERE Channel = "Microsoft-Windows-Sysmon/Operational"  
            AND EventID = 1  
            AND LOWER(Image) LIKE "%control.exe"  
            AND LOWER(ParentImage) LIKE "%sdclt.exe"  
    ) b  
    ON a.ParentProcessGuid = b.ProcessGuid  
    WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"  
        AND a.EventID = 1  
        AND a.IntegrityLevel = "High"  
    ...  
)  
df.show(100, truncate = False, vertical = True)
```

Nos permite relacionar acciones y representar comportamientos de adversarios

Cómo nos ayuda el modelo “Impulsado por data”?

Análisis Impulsado por **Usuario & Data**

En InfoSec, tendemos a usar el modelo impulsado por el "**usuario**", pero podría ser mejor si lo complementamos con el de "**data**".

Cómo empezar a usar el modelo “impulsado por data”?

YOU SHALL NOT PASS



Debemos tener en cuenta:

- Documentación
- Estandarización
- Modelamiento



<https://ossemproject.com/intro.html>

Cómo empezar a usar el modelo “impulsado por data”?

Entendamos los tipos de datos recolectados

Entendamos los tipos de datos recolectados

```
df = spark.sql(  
    """  
    SELECT Message  
    FROM apt29Host  
    WHERE Channel = "Microsoft-Windows-Sysmon/Operational"  
        AND EventID = 1  
        AND LOWER(Image) LIKE "%sdclt.exe"  
        AND IntegrityLevel = "High"  
    """  
)  
df.show(100,truncate = False, vertical = True)
```

Entendamos los tipos de datos recolectados

```
df = spark.sql(  
    ...  
    "SELECT Message  
    FROM apt29Host  
    WHERE Channel = \"Microsoft-Windows-Sysmon/Operational\"\n        AND EventID = 1  
        AND LOWER(Image) LIKE \"%sdclt.exe\"\n        AND IntegrityLevel = \"High\"\n    ...  
)  
df.show(100,truncate = False, vertical = True)
```

Id de Evento

Nombre de Proceso

Integridad de Proceso

Entendamos los tipos de datos recolectados

Id de Evento : 1

Nombre de Proceso : sdclt.exe

Integridad de Proceso : High

Entendamos los tipos de datos recolectados

Id de Evento : 1

Nombre de Proceso : sdclt.exe

Integridad de Proceso : High

Conexiones de Red : 20

Bytes Transferidos : 100.5

Tiempo de Creación de Evento : 4/11/18 6:04 (UTC)

Datos Categóricos

- Describen cada evento de seguridad a través de categorías o cualidades
- Permiten agrupar y ordenar datos
- Usualmente, sus valores son descritos con letras o palabras.

Id de Evento : 1

Nombre de Proceso : sdclt.exe

Integridad de Proceso : High

Datos Categóricos

- Describen cada evento de seguridad a través de categorías o cualidades
- Permiten agrupar y ordenar datos
- Usualmente, sus valores son descritos con letras o palabras.

Id de Evento :  **Podemos usar Números**

Nombre de Proceso : sdclt.exe

Integridad de Proceso : High

Datos Categóricos

- Describen cada evento de seguridad a través de categorías o cualidades
- Permiten agrupar y ordenar datos
- Usualmente, sus valores son descritos con letras o palabras. Si usamos números, su aritmética (Suma o resta) no agrega contexto.

Id de Evento :  **Podemos usar Números**

Nombre de Proceso : sdclt.exe

Integridad de Proceso : High

Datos Categóricos

- Describen cada evento de seguridad a través de categorías o cualidades
- Permiten **agrupar** y **ordenar** datos
- Usualmente, sus valores son descritos con letras o palabras. Si usamos números, su aritmética (Suma o resta) no agrega contexto.

Datos Nominales

Id de Evento : 1

Nombre de Proceso : sdclt.exe

Integridad de Proceso : High

Datos Ordinales

Datos Categóricos

- Describen cada evento de seguridad a través de categorías o cualidades
- Permiten **agrupar** y **ordenar** datos
- Usualmente, sus valores son descritos con letras o palabras. Si usamos números, su aritmética (Suma o resta) no agrega contexto.

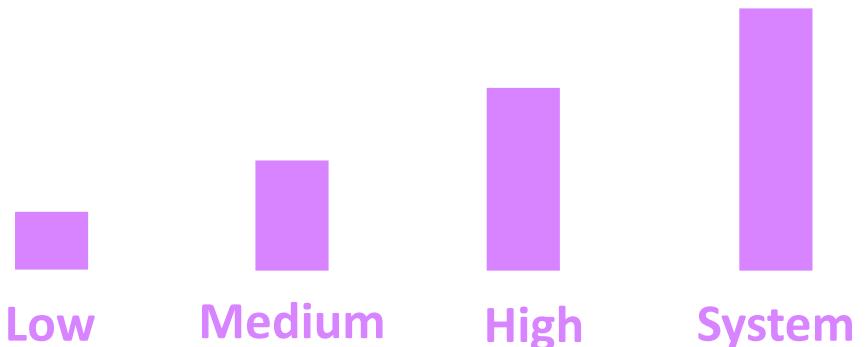
Datos Nominales

Id de Evento : 1

Nombre de Proceso : sdclt.exe

Integridad de Proceso : High

Datos Ordinales



Datos Categóricos

- Describen cada evento de seguridad a través de categorías o cualidades
- Permiten **agrupar** y **ordenar** datos
- Usualmente, sus valores son descritos con letras o palabras. Si usamos números, su aritmética (Suma o resta) no agrega contexto.

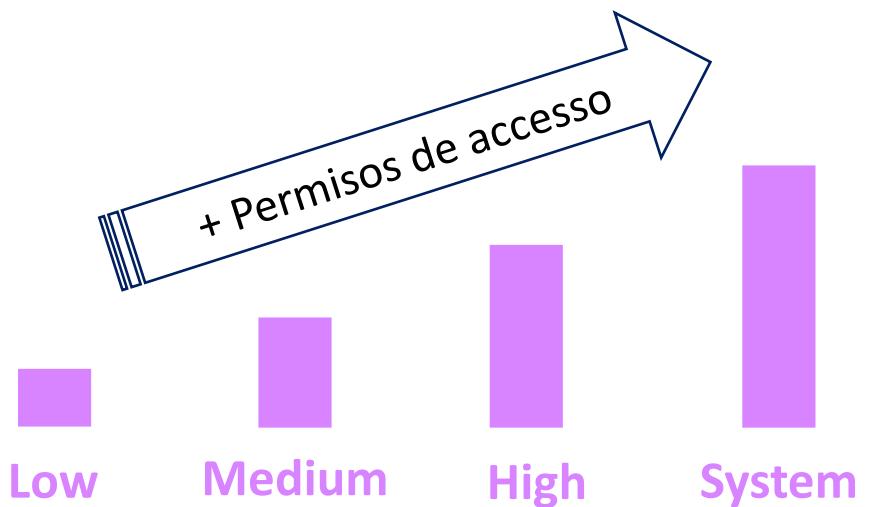
Datos Nominales

Id de Evento : 1

Nombre de Proceso : sdclt.exe

Integridad de Proceso : High

Datos Ordinales



Datos Numéricos

- Describen cada evento de seguridad a través de números o cantidades
- Resultado de conteo o medición
- Permiten agrupar y ordenar datos,
- La aritmética de datos numéricos puede agregar contexto a nuestro análisis

Conexiones de Red : 20

Bytes Transferidos : 100.5

Datos Numéricos

- Describen cada evento de seguridad a través de números o cantidades
- Resultado de conteo o medición
- Permiten agrupar y ordenar datos,
- La aritmética de datos numéricos puede agregar contexto a nuestro análisis

Datos Discretos

Conexiones de Red : 20

Bytes Transferidos : 100.5

Datos Continuos

Datos de Tiempo

- Describen cada evento de seguridad en instantes e intervalos de tiempo.
- Nos permite representar secuencia de eventos. Por ejemplo: comportamiento de un adversario.

Tiempo de Creación de Evento :
4/11/18 6:04 (UTC)

Entendamos los tipos de datos recolectados

Categóricos {

- Id de Evento :** 1
- Nombre de Proceso :** sdclt.exe
- Integridad de Proceso :** High

Numéricos {

- Conexiones de Red :** 20
- Bytes Transferidos :** 100.5

Tiempo → **Tiempo de Creación de Evento :** 4/11/18 6:04 (UTC)

Entendamos los tipos de datos recolectados

Categóricos	Id de Evento : 1	Por qué es importante entender los tipos de datos?
	Nombre de Proceso : sdclt.exe	
	Integridad de Proceso : High	
Numéricos	Conexiones de Red : 20	
	Bytes Transferidos : 100.5	

Tiempo → **Tiempo de Creación de Evento :** 4/11/18 6:04 (UTC)

Nos permite identificar las técnicas de análisis a usar

Categóricos —→ **Ordenamiento, Conteo, frecuencia, correlación**

Numéricos —→ **Tendencia central, variabilidad, correlación**

Tiempo —→ **Series de tiempo**

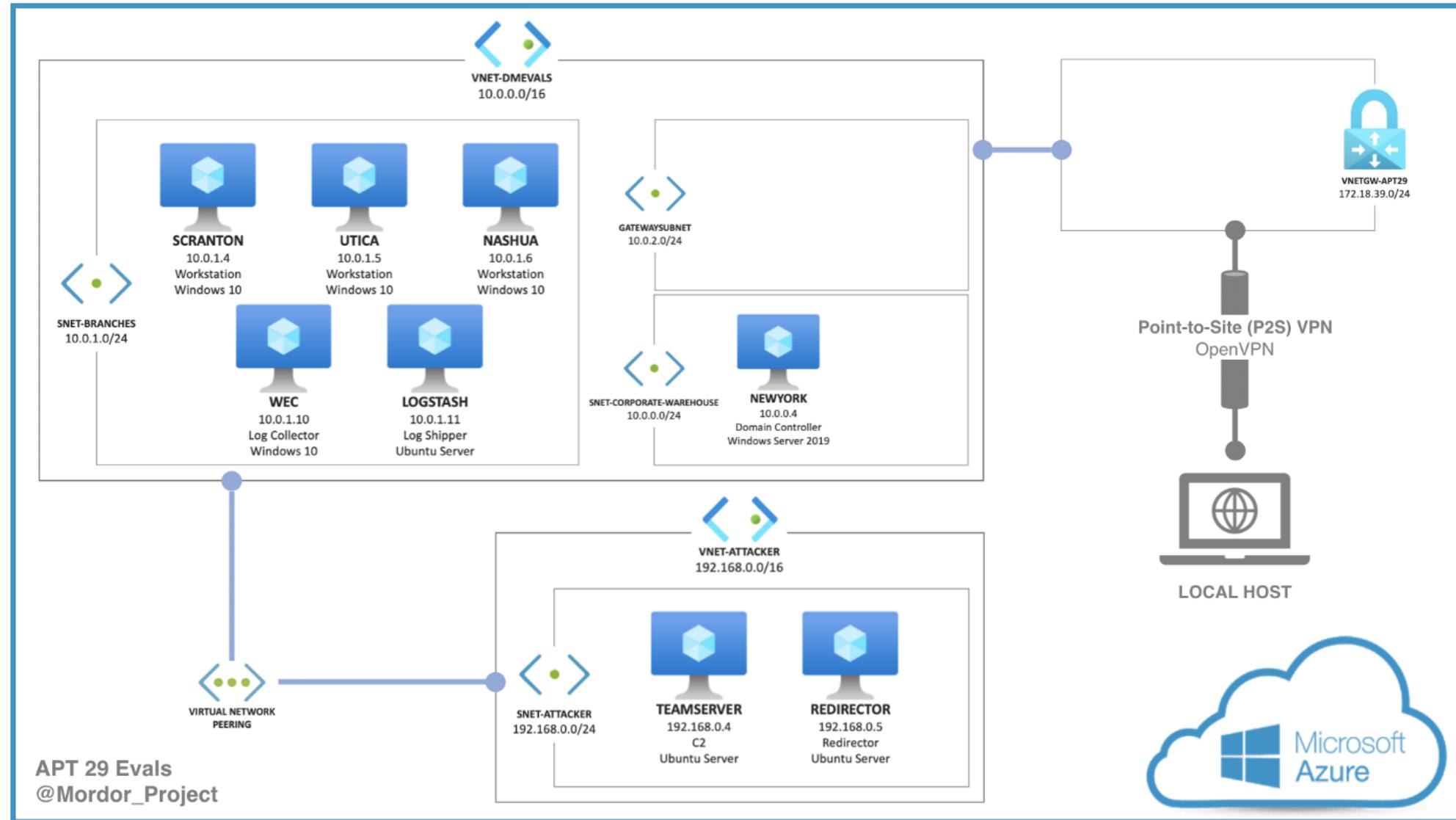


Qué aplicaciones tiene el modelo
“impulsado por data”?

Aplicaciones en InfoSec

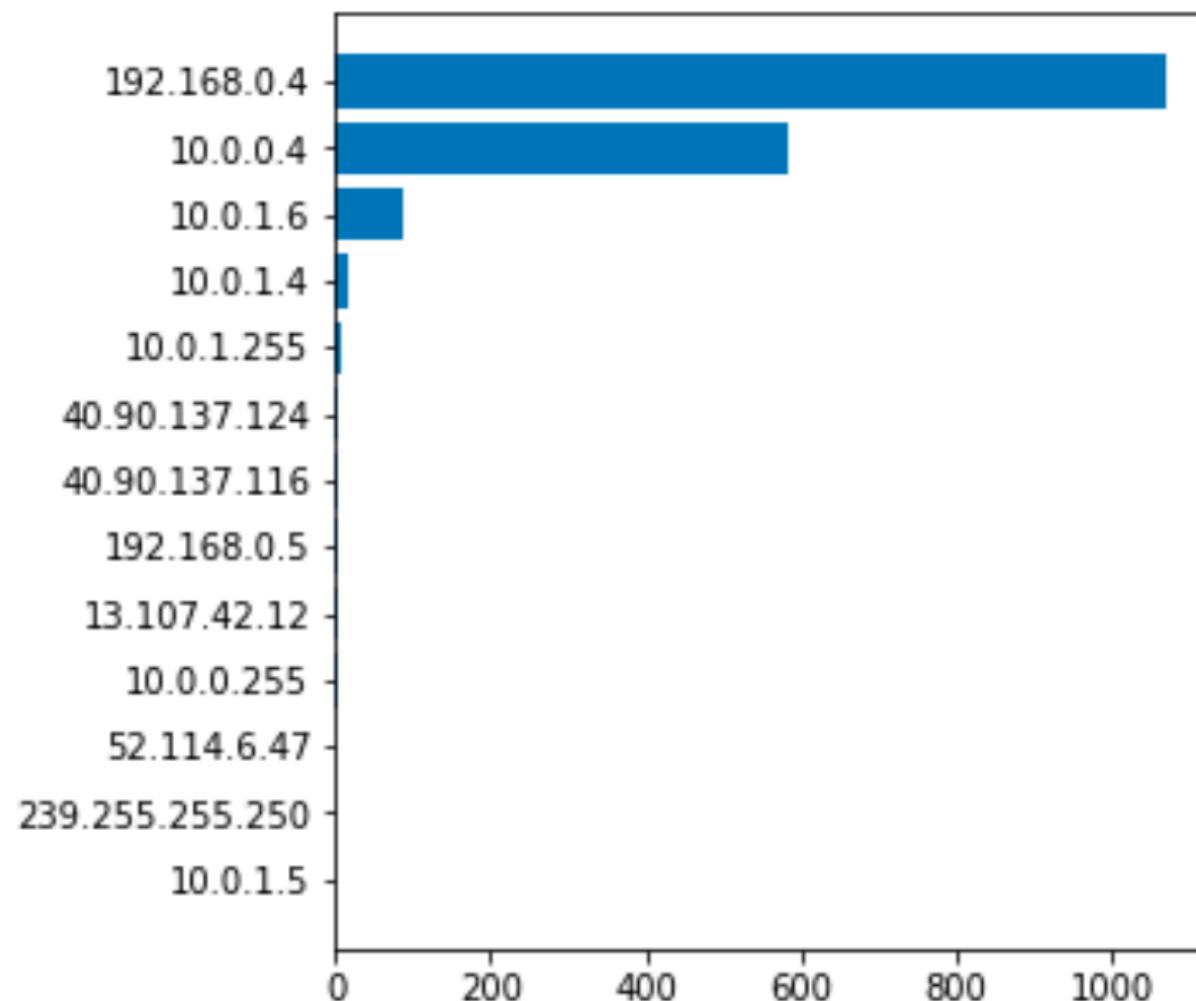
- **Resumiendo y Presentando** data
- Explorando el **Profile** de mi entorno de red
- Identificando nuevas **oportunidades** de investigación

Referencia para ejemplos: APT29 Compound Dataset



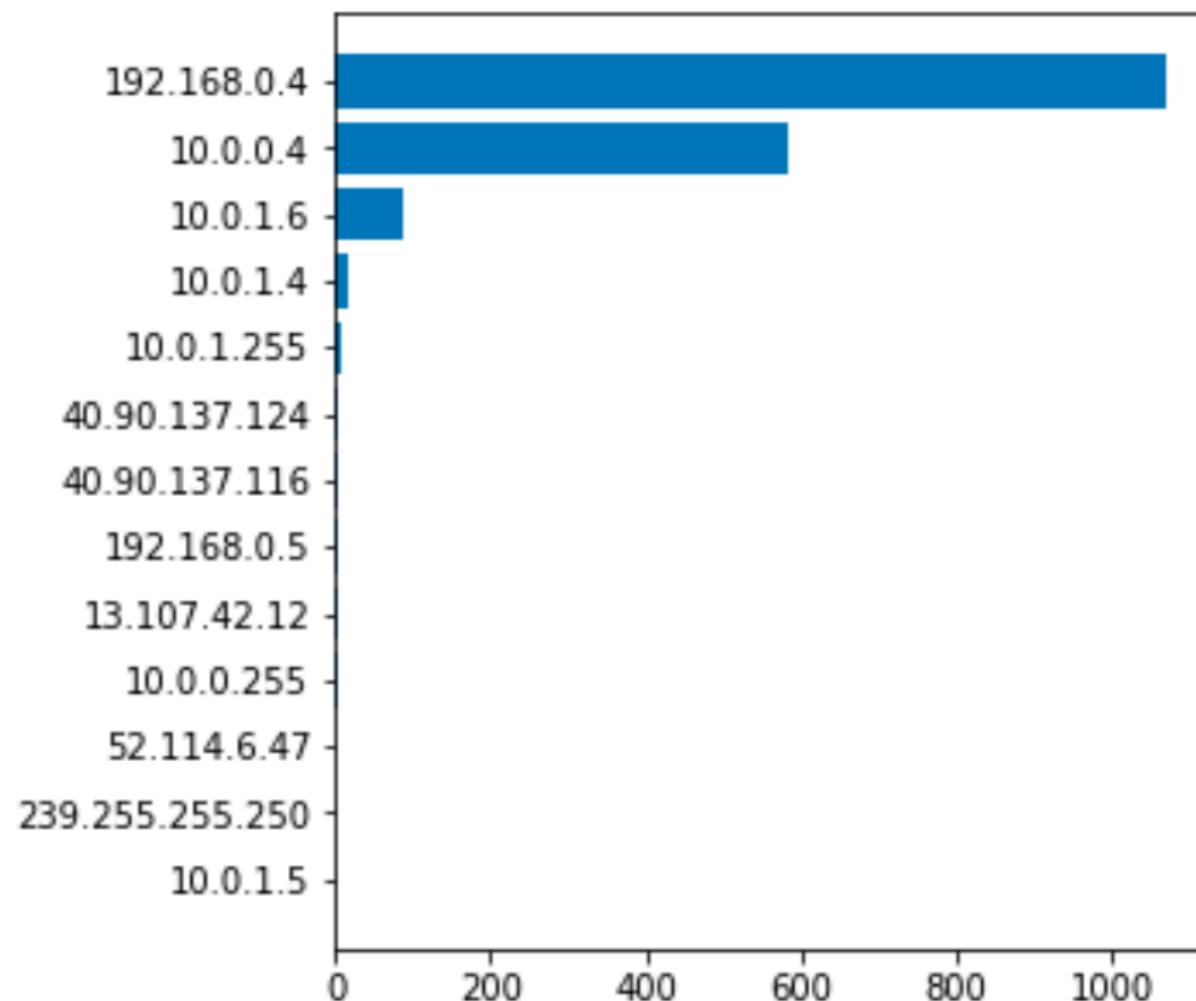
Resumiendo y Presentando Datos Categóricos

Conteo / Frecuencia: IP Address (Outbound)



Conteo Conexiones
192.168.0.4
10.0.0.4
10.0.1.6
10.0.1.4
10.0.1.255
10.0.0.255
13.107.42.12
192.168.0.5
40.90.137.116
40.90.137.124
10.0.1.5
239.255.255.250
52.114.6.47

Conteo / Frecuencia: IP externos



Conteo Conexiones	
192.168.0.4	1069
10.0.0.4	582
10.0.1.6	88
10.0.1.4	18
10.0.1.255	10
10.0.0.255	3
13.107.42.12	3
192.168.0.5	3
40.90.137.116	3
40.90.137.124	3
10.0.1.5	1
239.255.255.2	1
52.114.6.47	1

más frecuentes

menos frecuentes

Tabla Doble Entrada : Integridad de Procesos

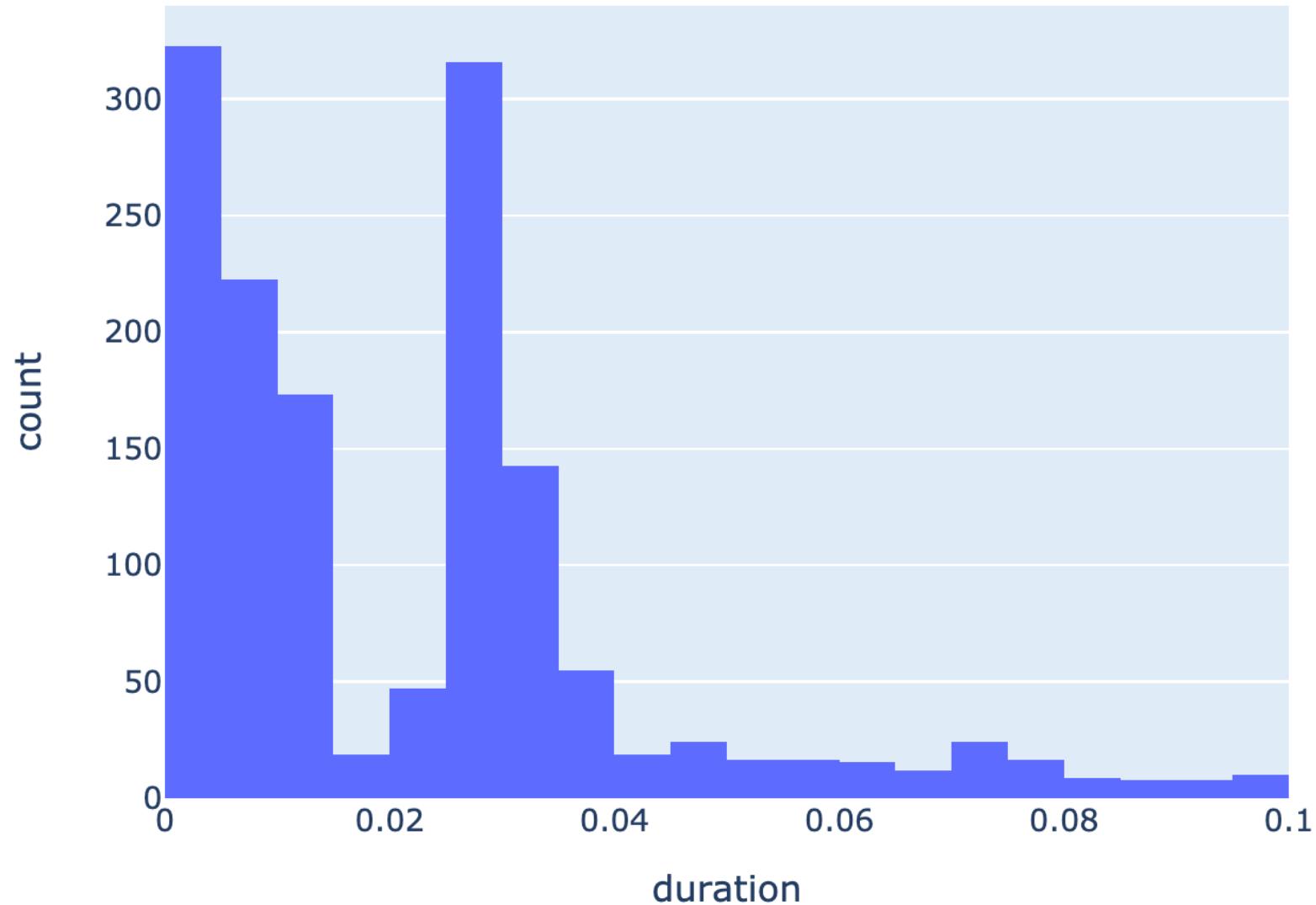
IntegrityLevel	AppContainer	High	Medium	System	All
User					
DMEVALS\dschrute	40	17	85	0	142
DMEVALS\kmalone	0	5	0	0	5
DMEVALS\mscott	48	4	29	0	81
DMEVALS\pbeesly	29	39	73	0	141
Font Driver Host\UMFD-0	2	0	0	0	2
Font Driver Host\UMFD-1	2	0	0	0	2
Font Driver Host\UMFD-2	2	0	0	0	2
NT AUTHORITY\LOCAL SERVICE	2	0	0	70	72
NT AUTHORITY\NETWORK SERVICE	0	0	0	50	50
NT AUTHORITY\SYSTEM	2	0	12	512	526
Window Manager\DWMM-1	0	0	0	2	2
Window Manager\DWMM-2	0	0	0	2	2
All	127	65	199	636	1027

Tabla Doble Entrada : Integridad de Procesos

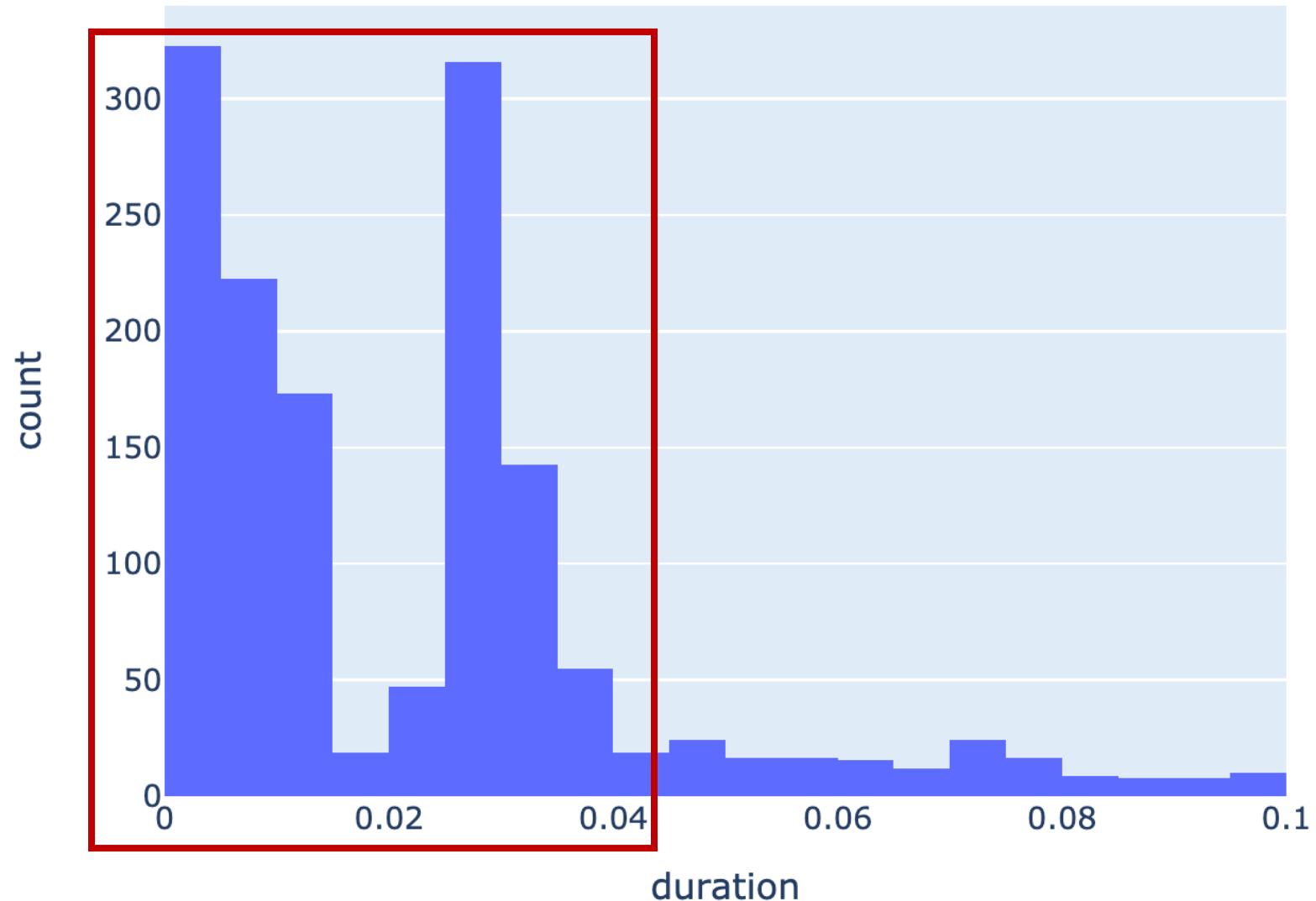
IntegrityLevel	AppContainer	High	Medium	System	All
User					
DMEVALS\dschrute					
DMEVALS\dschrute	40	17	85	0	142
DMEVALS\kmalone	0	5	0	0	5
DMEVALS\mscott	48	4	29	0	81
DMEVALS\pbeesly	29	39	73	0	141
Font Driver Host\UMFD-0	2	0	0	0	2
Font Driver Host\UMFD-1	2	0	0	0	2
Font Driver Host\UMFD-2	2	0	0	0	2
NT AUTHORITY\LOCAL SERVICE	2	0	0	70	72
NT AUTHORITY\NETWORK SERVICE	0	0	0	50	50
NT AUTHORITY\SYSTEM	2	0	12	512	526
Window Manager\DWMM-1	0	0	0	2	2
Window Manager\DWMM-2	0	0	0	2	2
All	127	65	199	636	1027

Resumiendo y Presentando Datos Numéricos

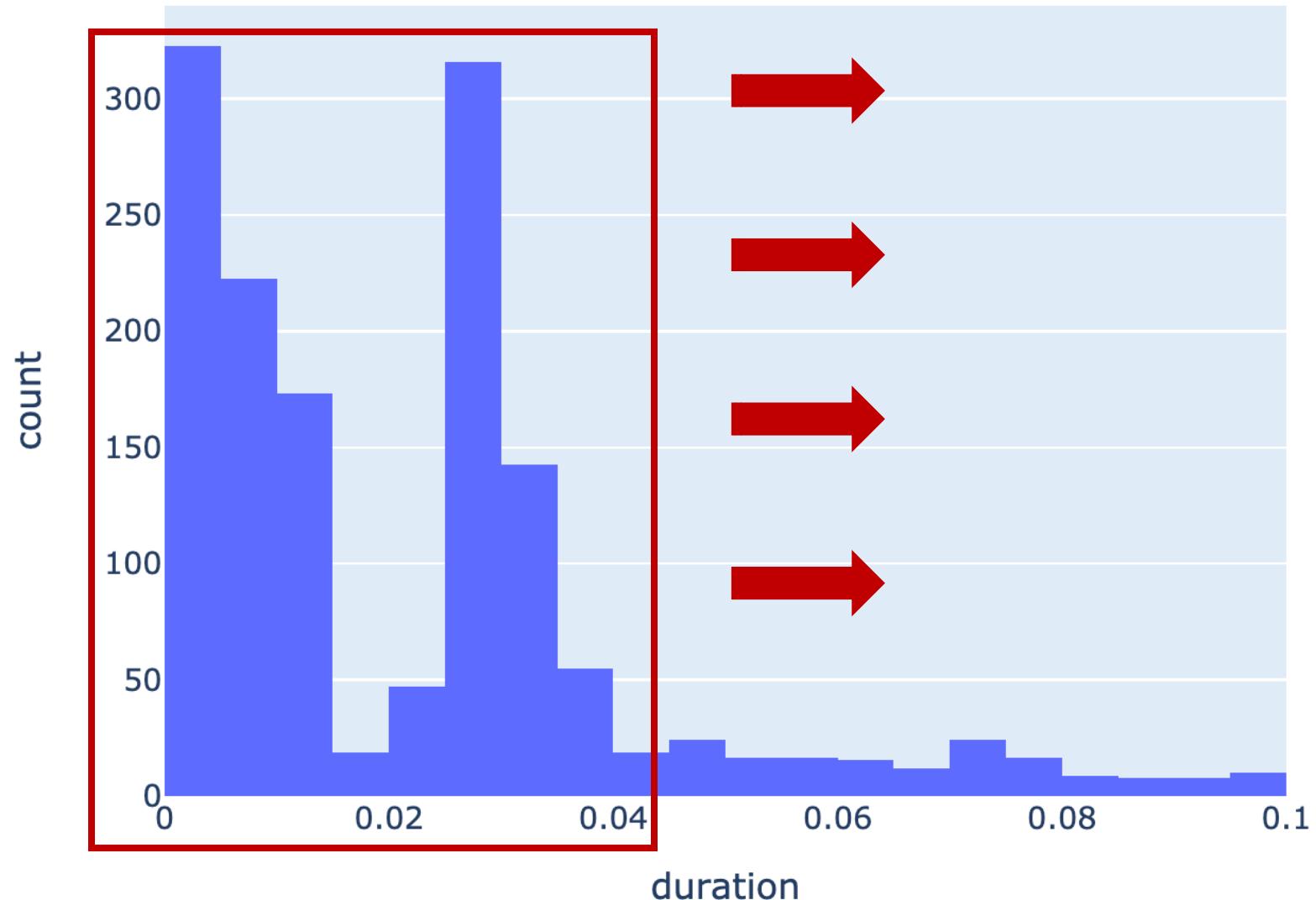
Histograma: Duración de Conexión (Segundos)



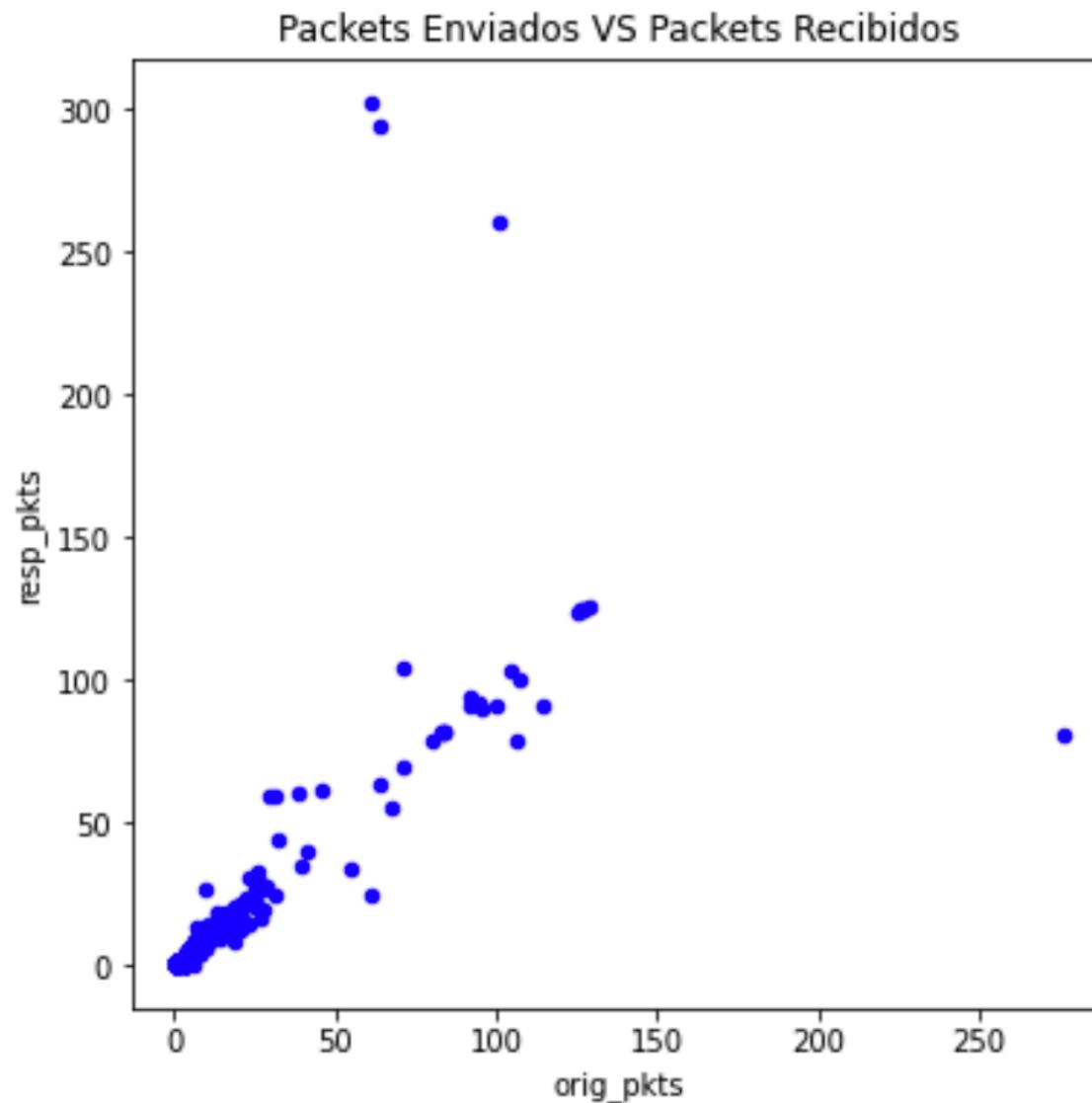
Histograma: Duración de Conexión (Segundos)



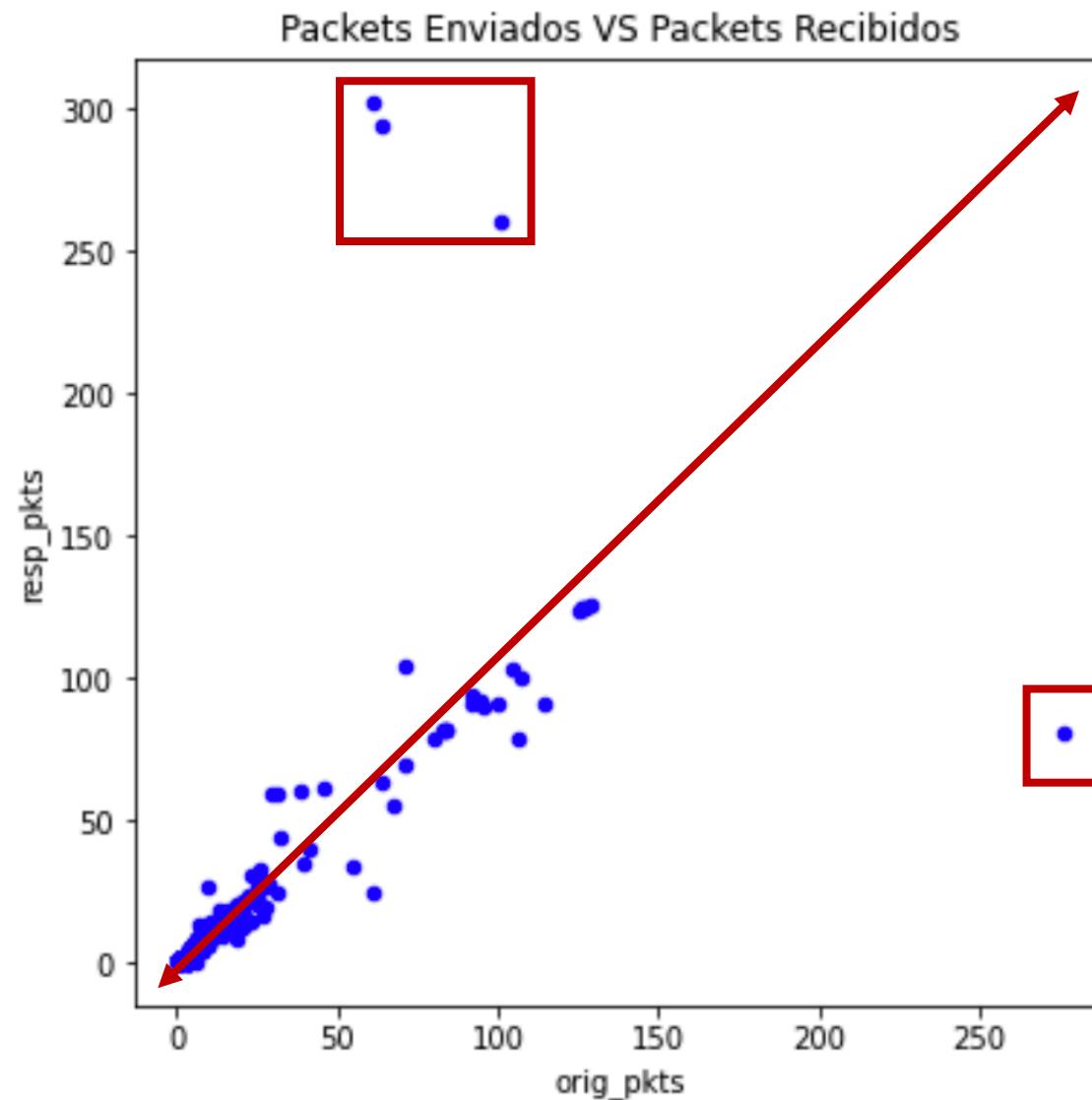
Histograma: Duración de Conexión (Segundos)



Dispersión: Network packets (Enviados Vs Recibidos)

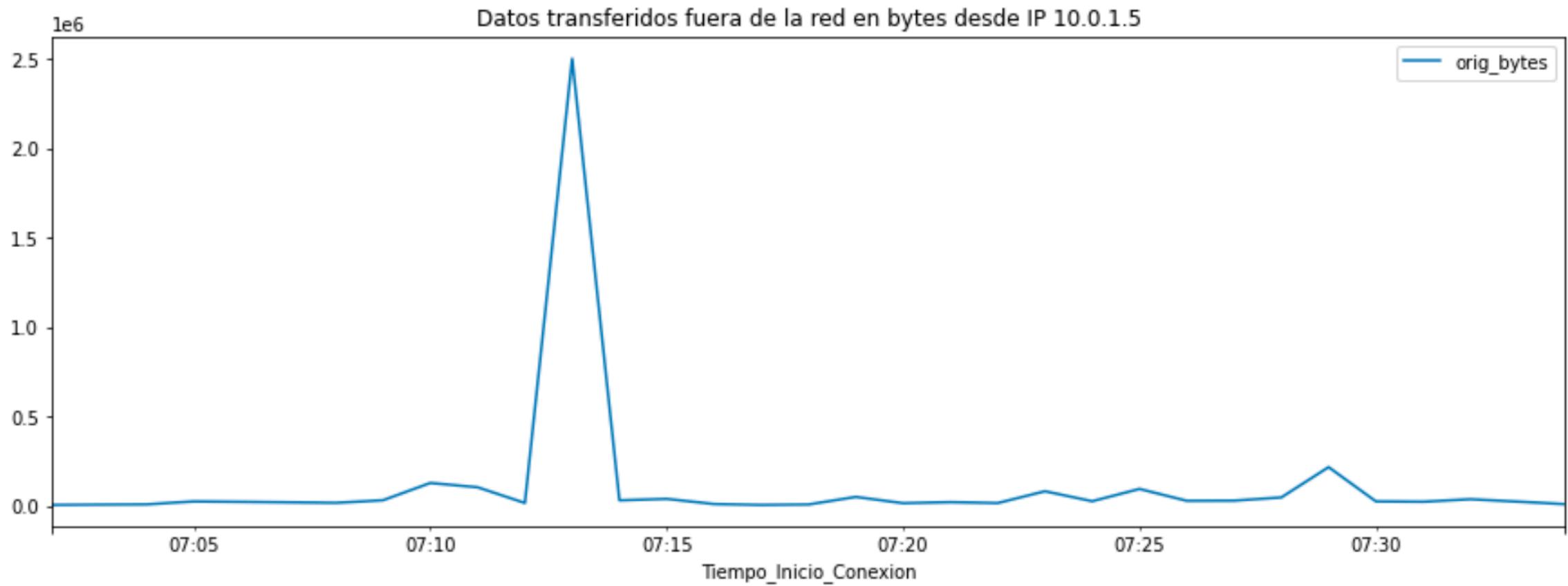


Dispersión: Network packets (Enviados Vs Recibidos)

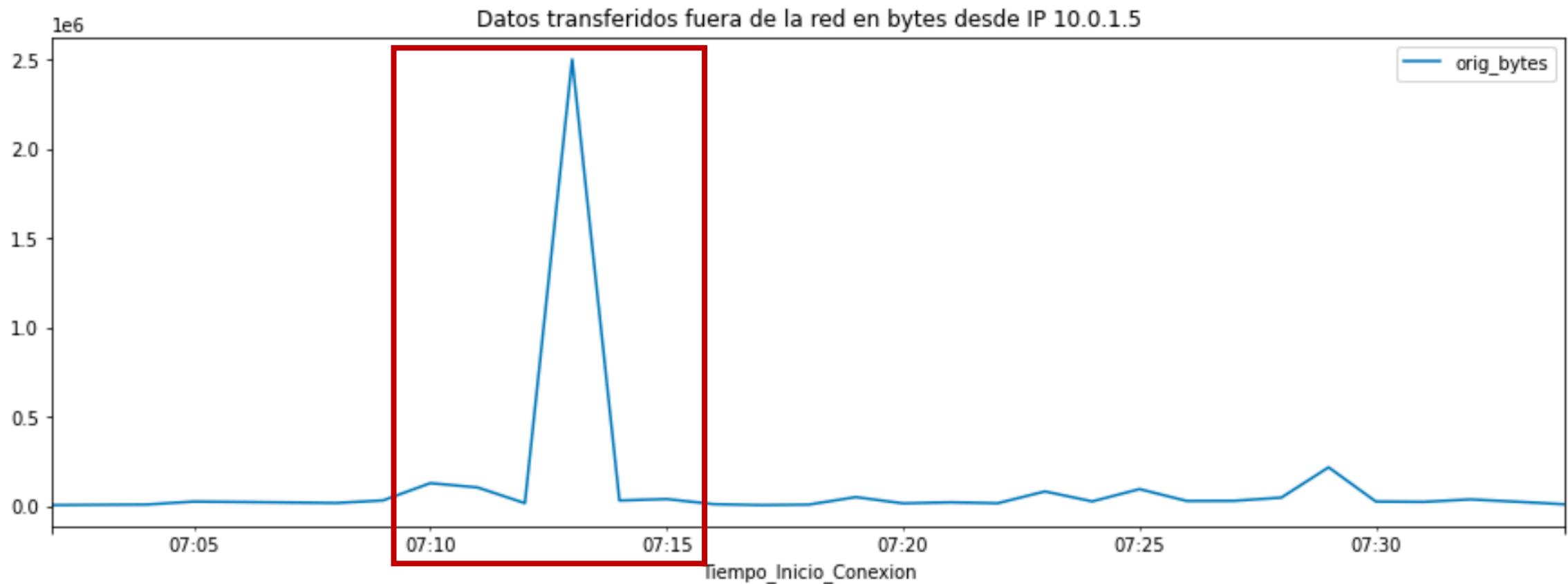


Resumiendo y Presentando Datos Numéricos + Tiempo

Serie Tiempo: Bytes transferidos fuera de la red

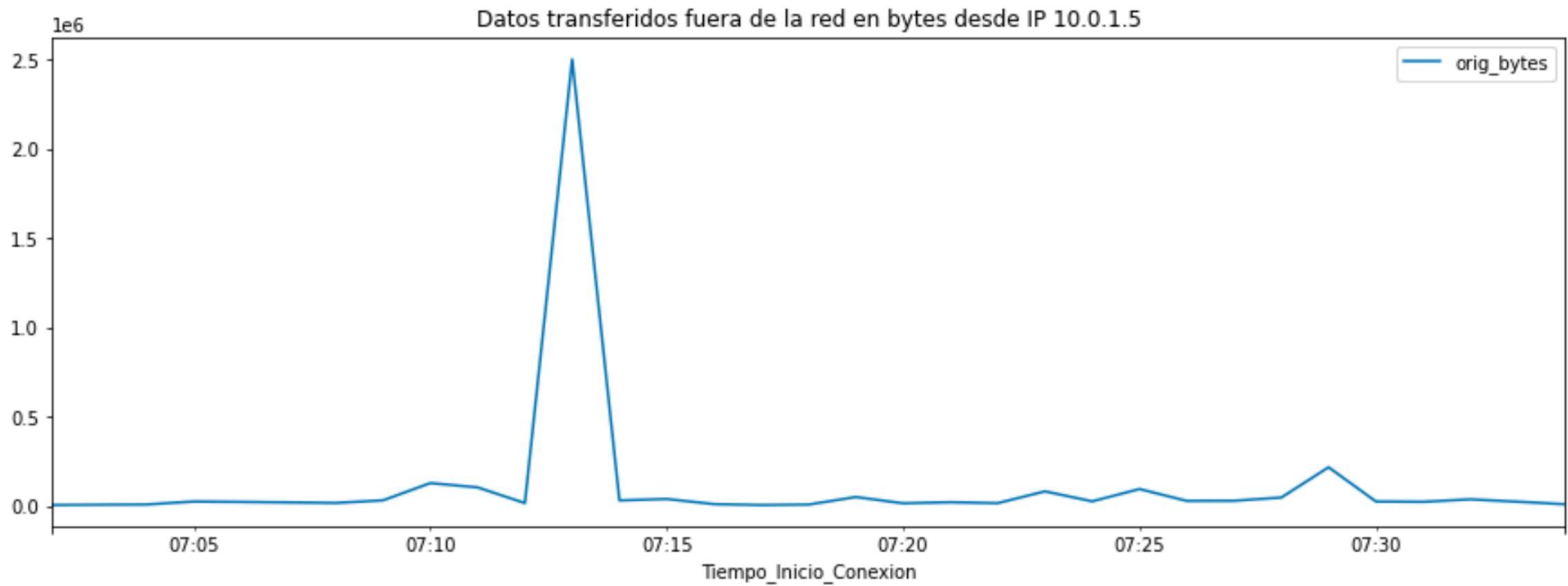


Serie Tiempo: Bytes transferidos fuera de la red

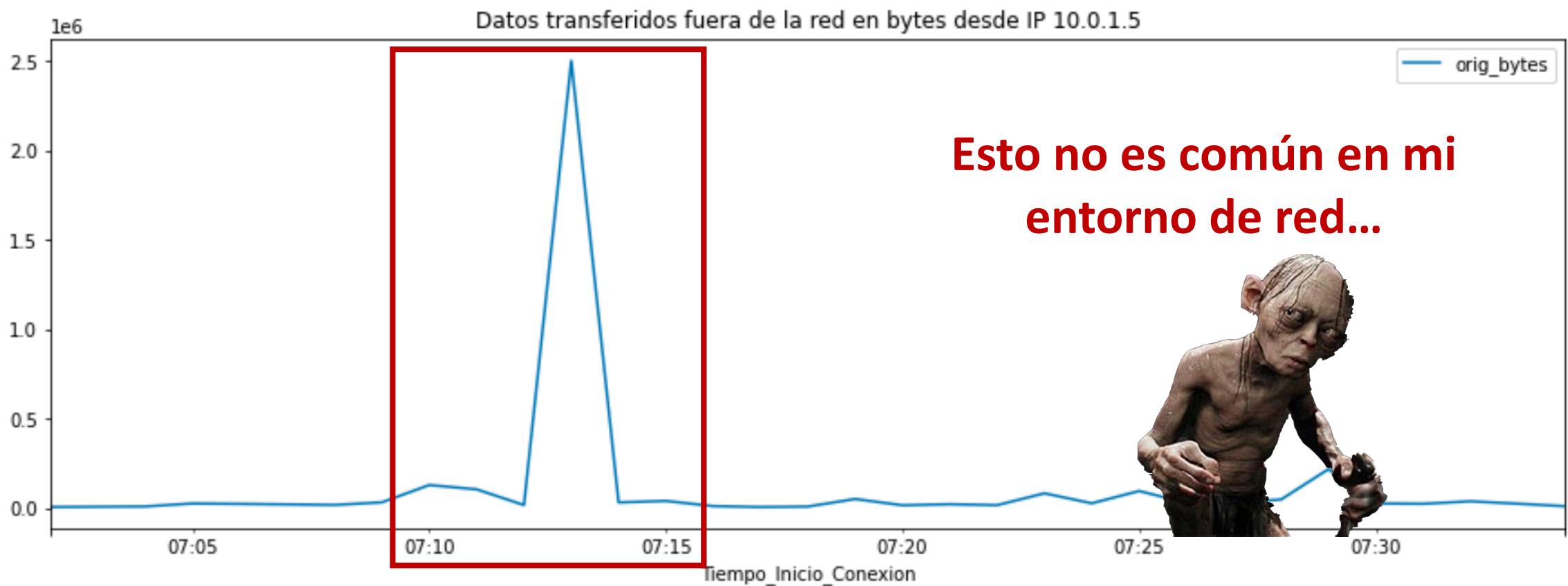


Explorando el Profile de mi Entorno de Red con Datos Numéricos

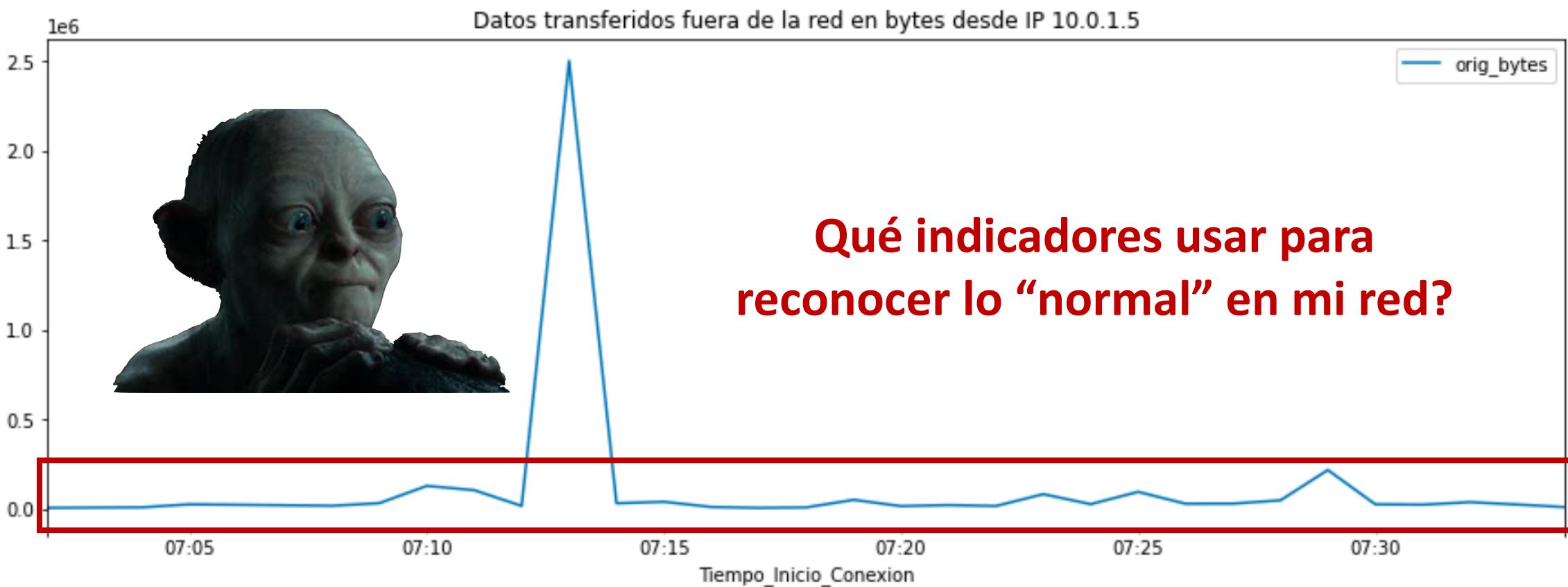
Serie Tiempo: Bytes transferidos fuera de la red



Serie Tiempo: Bytes transferidos fuera de la red

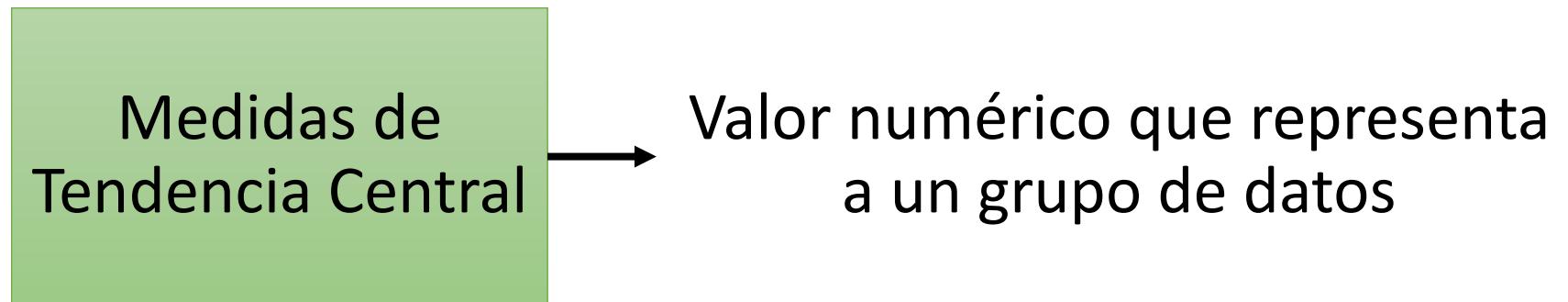


Serie Tiempo: Bytes transferidos fuera de la red

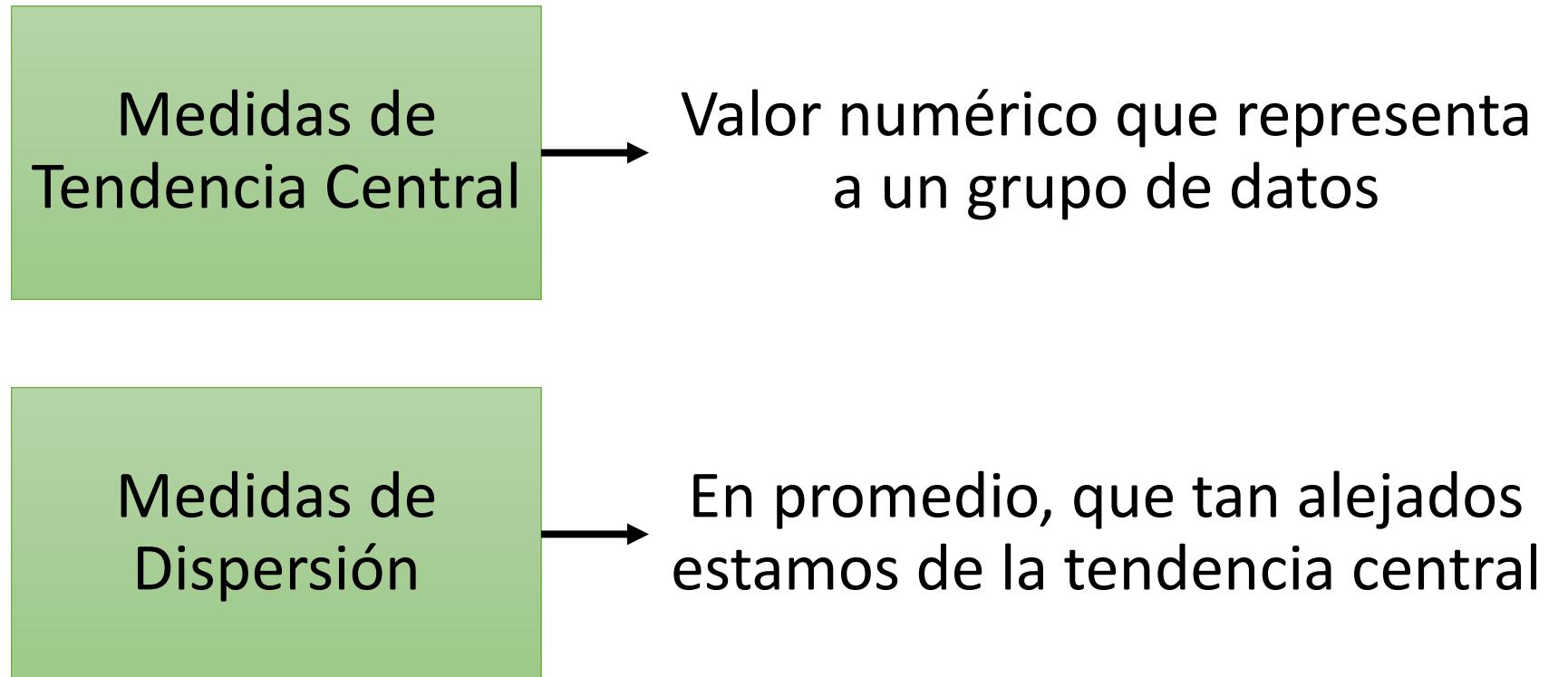


2 Indicadores básicos para crear un profile

2 Indicadores básicos para crear un profile

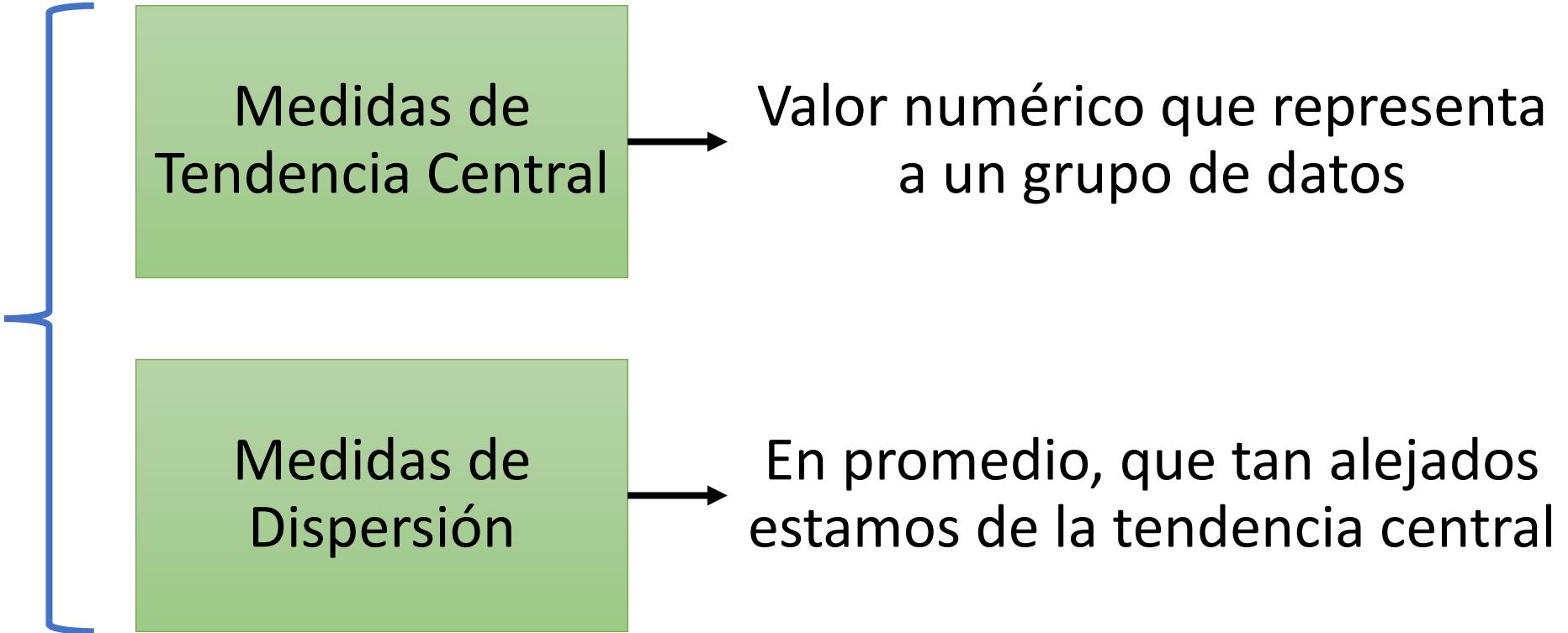


2 Indicadores básicos para crear un profile



2 Indicadores básicos para crear un profile

Describir
nuestro
entorno de
red

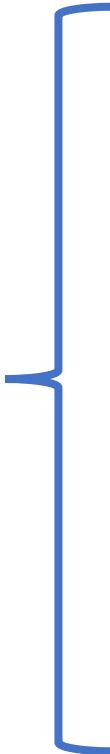


2 Indicadores básicos para crear un profile

Describir
nuestro
entorno de
red



???



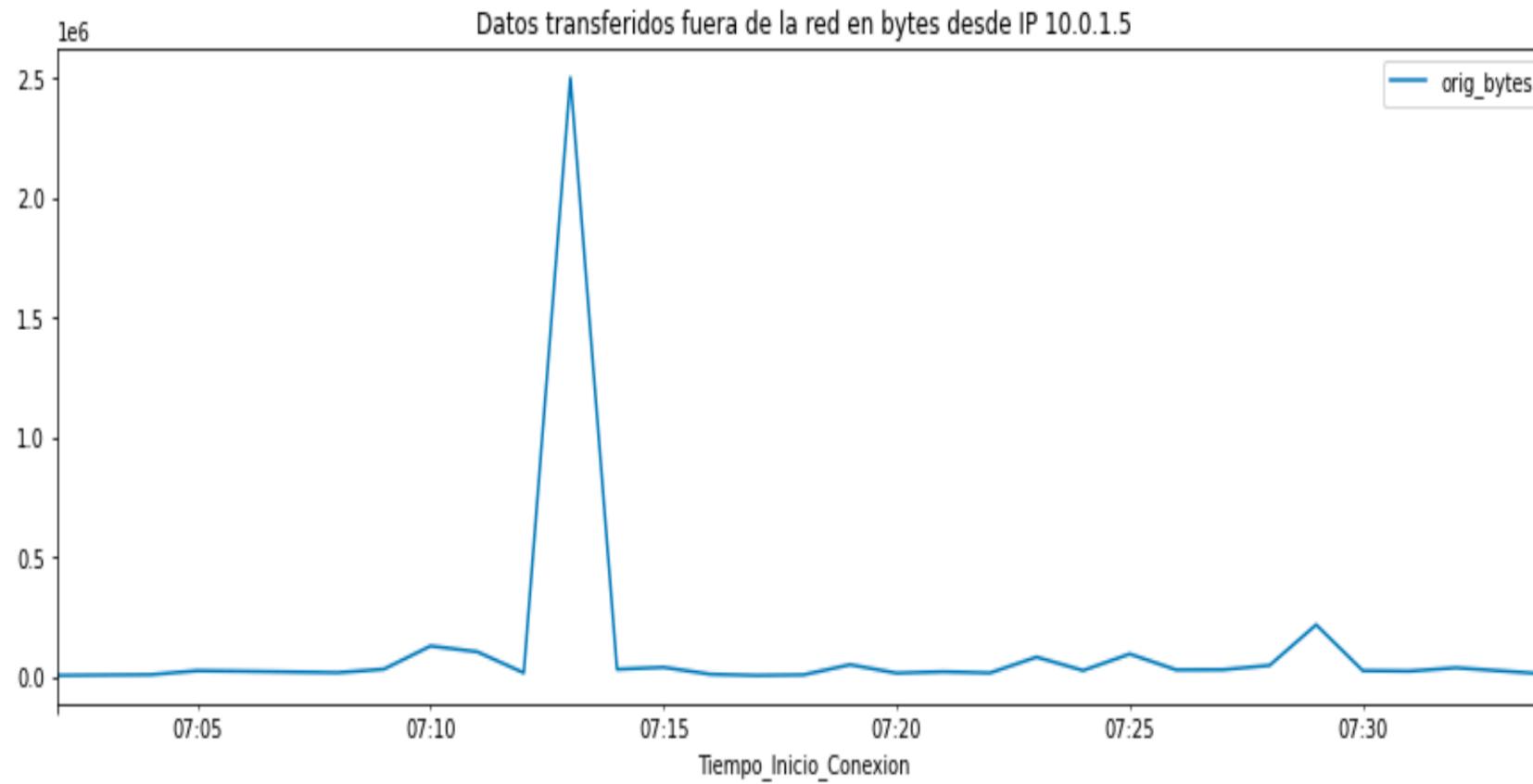
Medidas de
Tendencia Central

Valor numérico que representa
a un grupo de datos

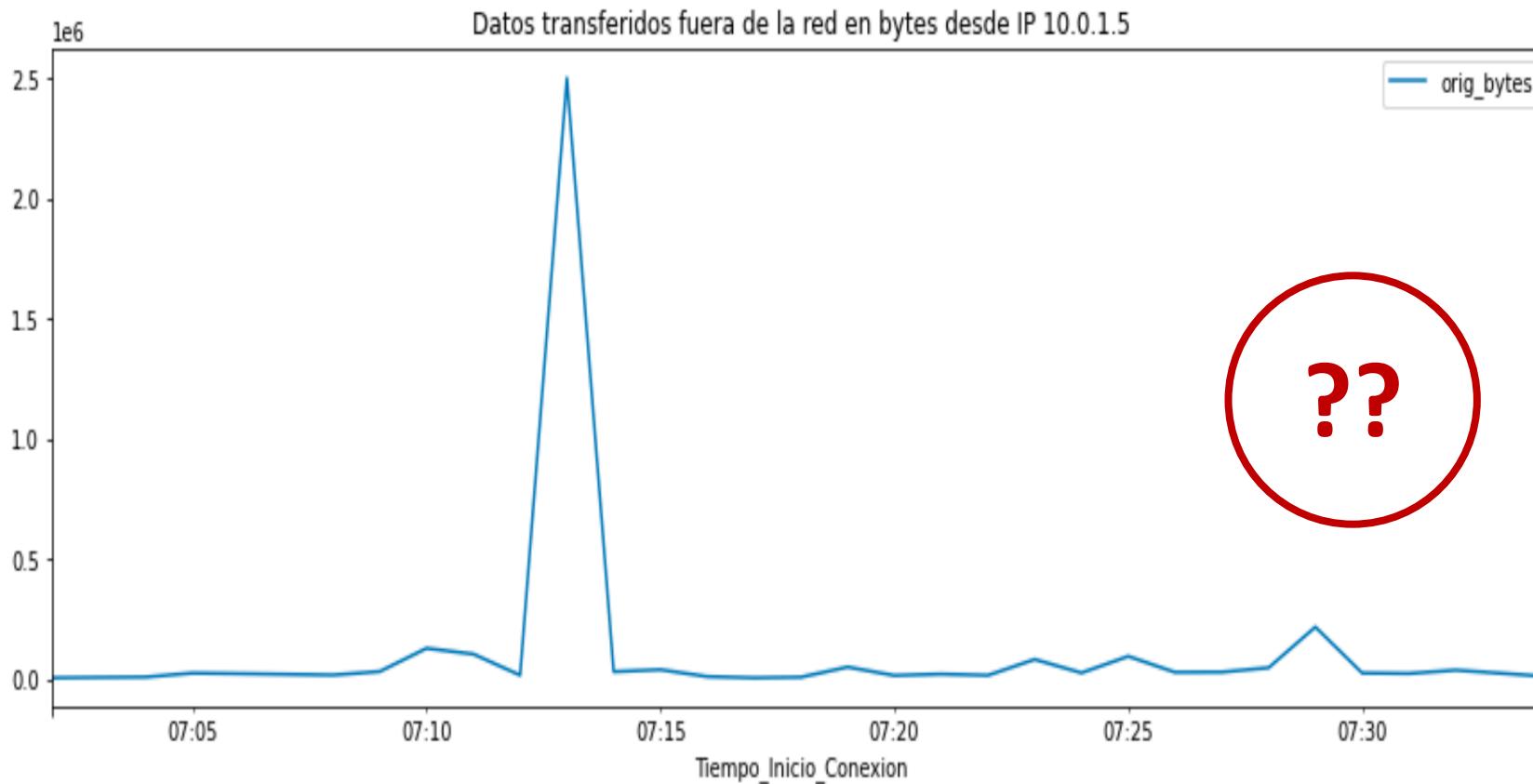
Medidas de
Dispersión

En promedio, que tan alejados
estamos de la tendencia central

Serie Tiempo: Bytes transferidos fuera de la red



Serie Tiempo: Bytes transferidos fuera de la red

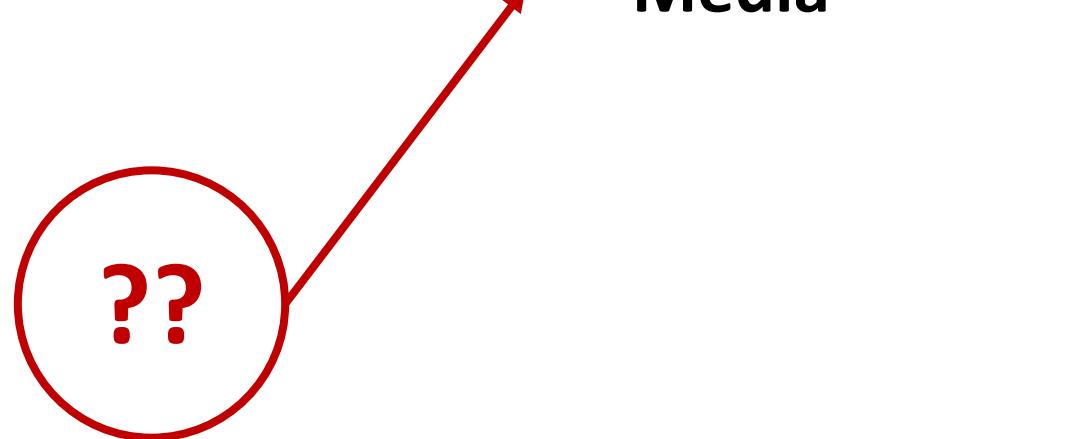


**Un valor único que
represente la data
recolectada?**

Medidas de Tendencia Central



Medidas de Tendencia Central

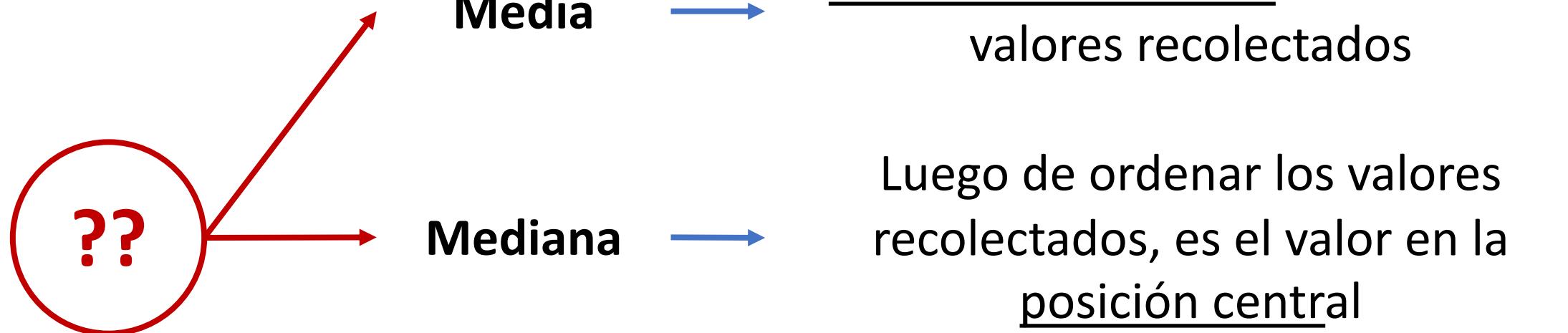


Media

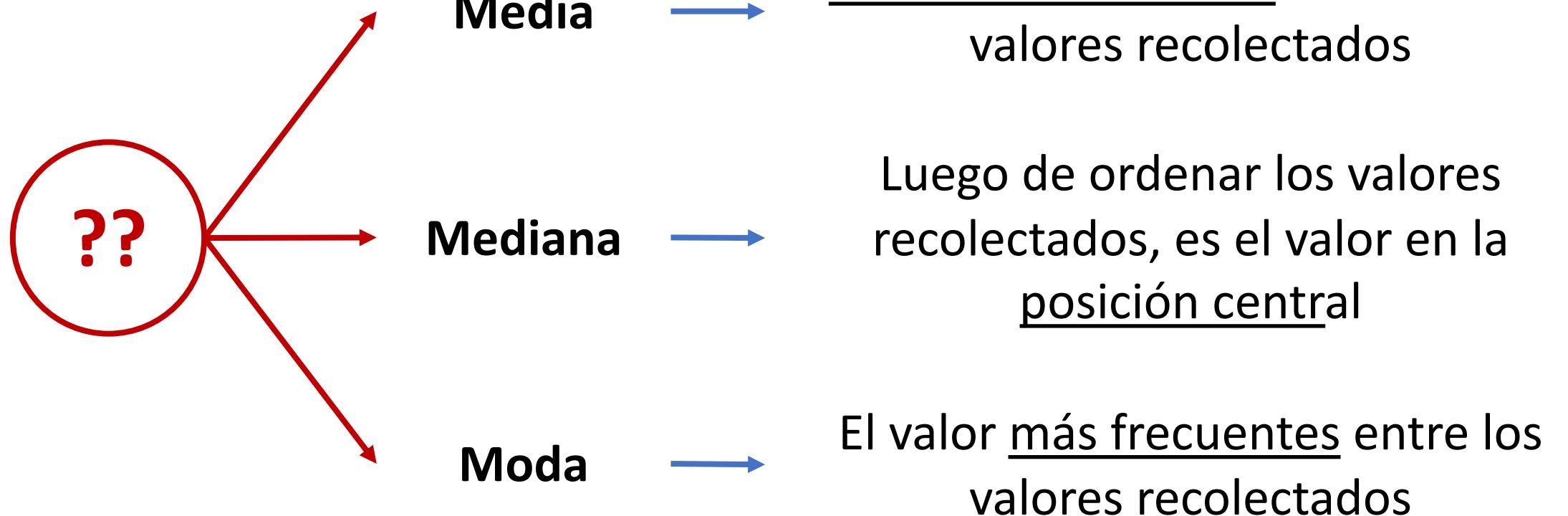


Promedio aritmético de todos los
valores recolectados

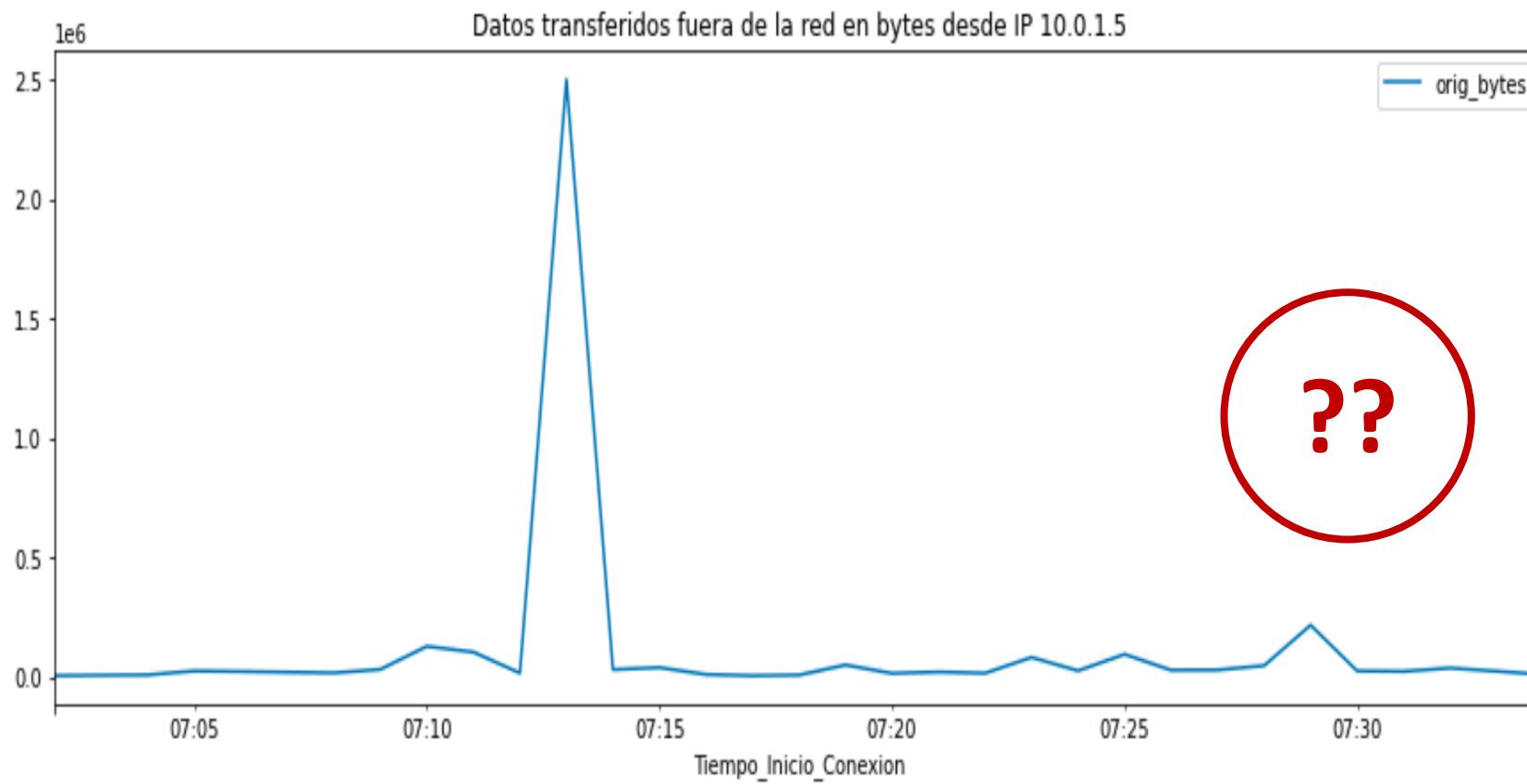
Medidas de Tendencia Central



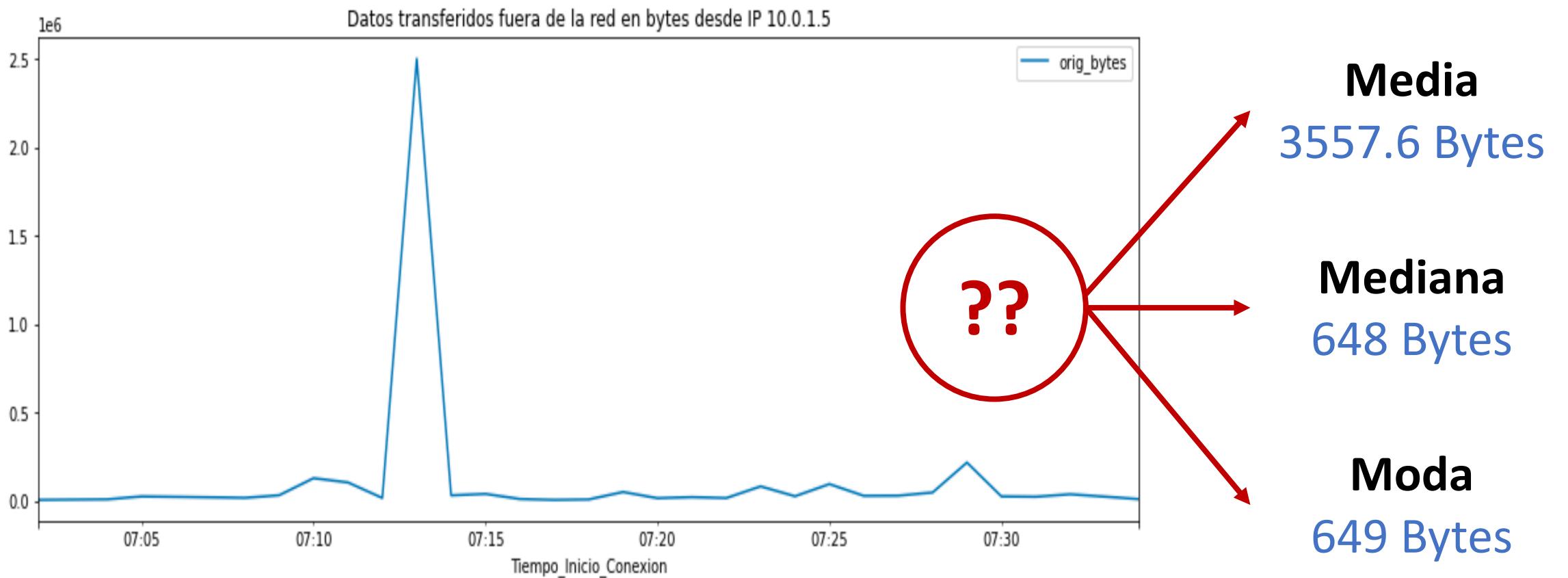
Medidas de Tendencia Central



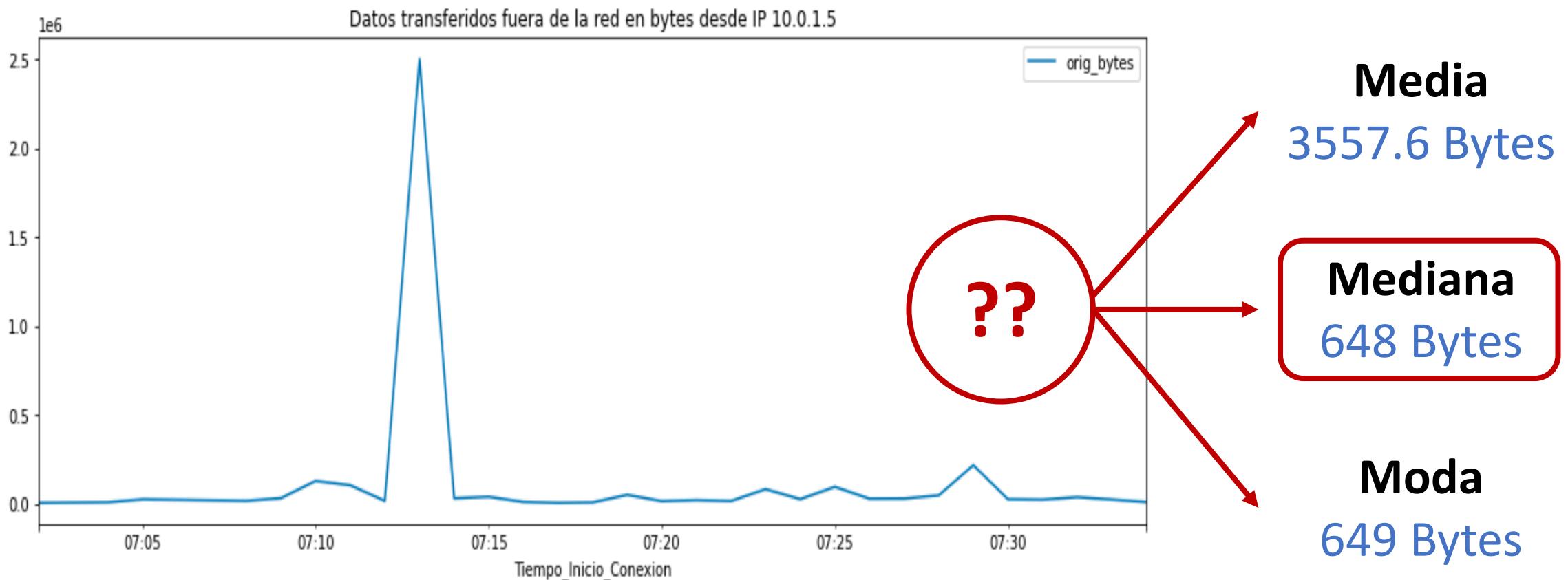
Profile: Bytes transferidos fuera de la red



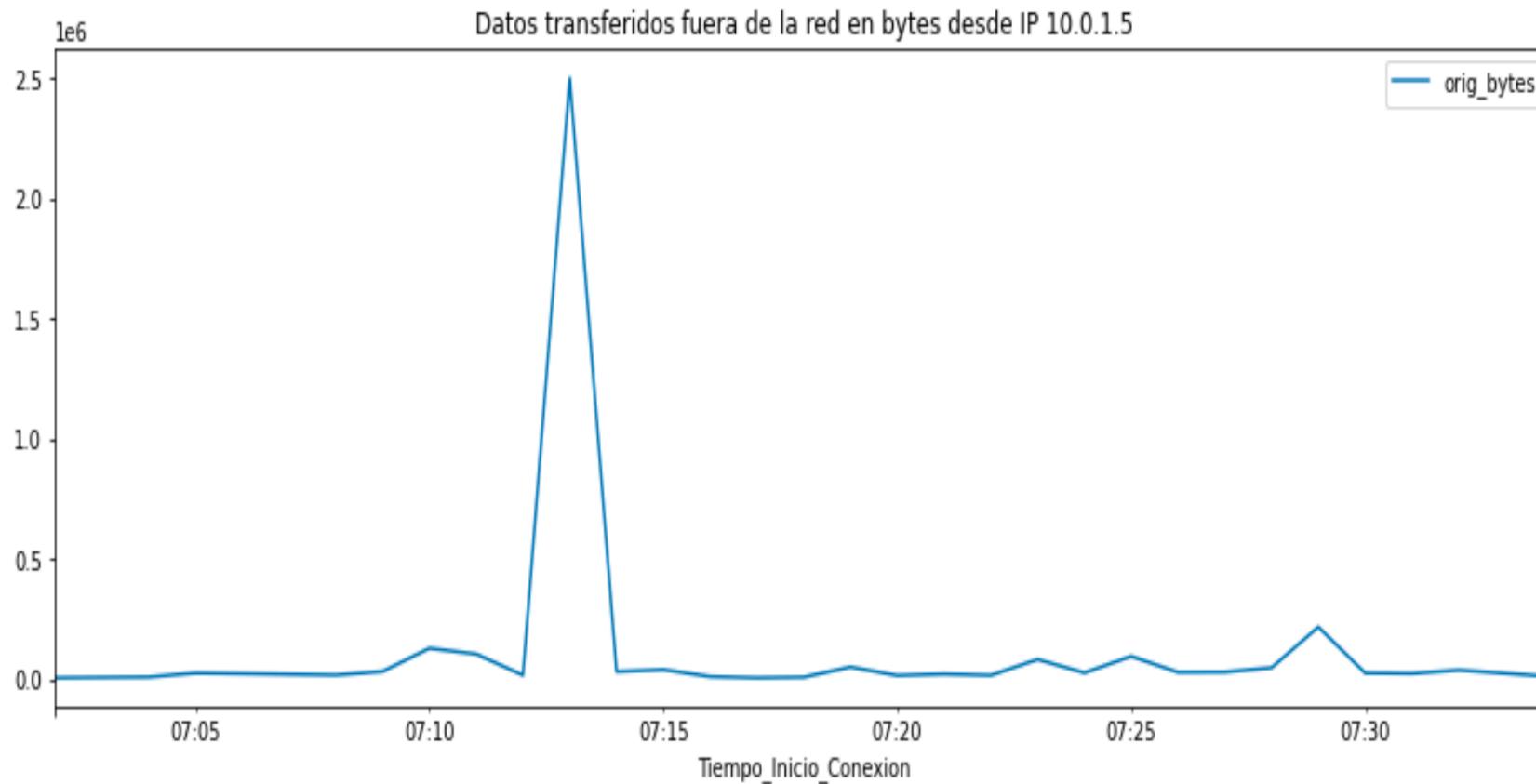
Profile: Bytes transferidos fuera de la red



Profile: Bytes transferidos fuera de la red

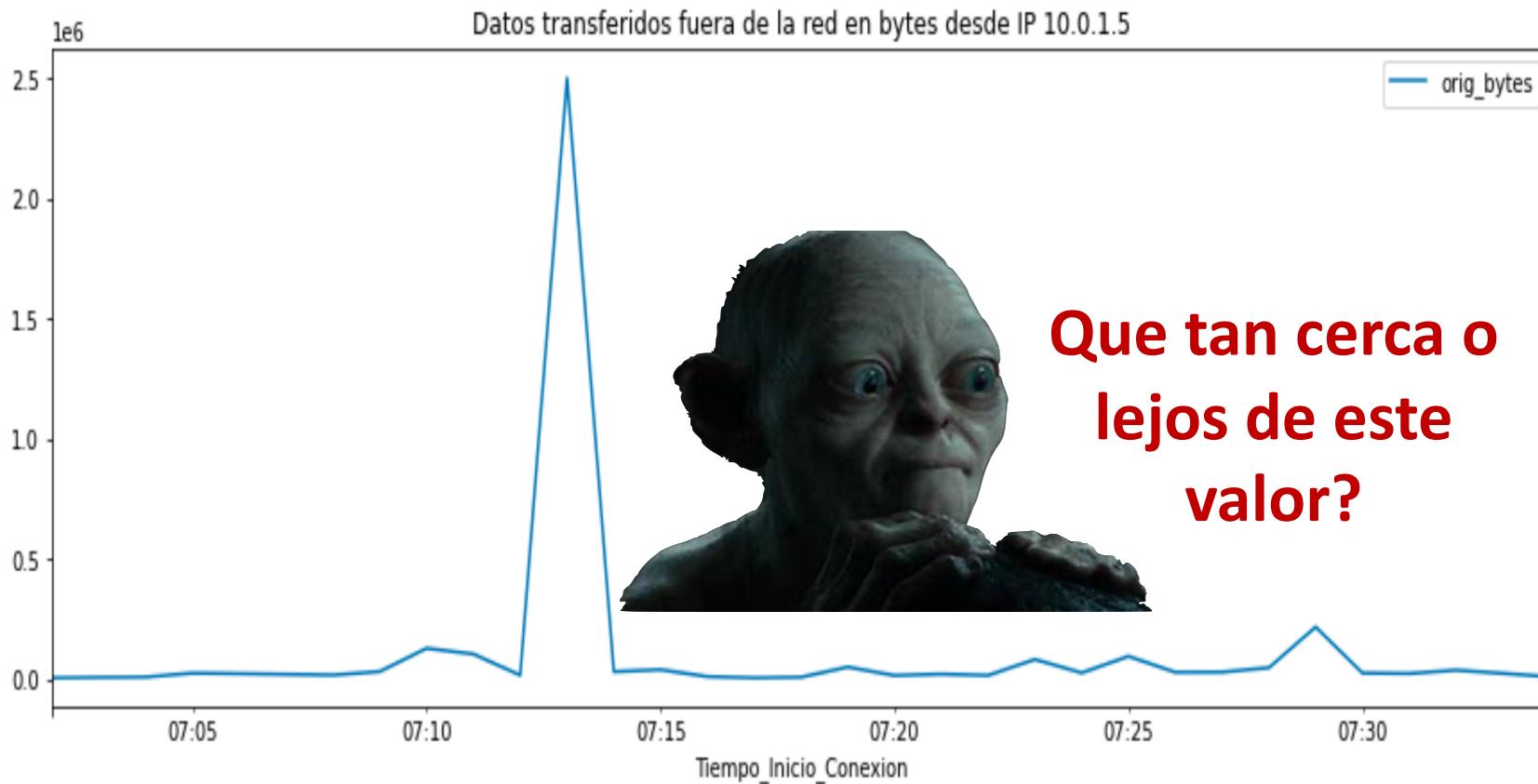


Profile: Bytes transferidos fuera de la red



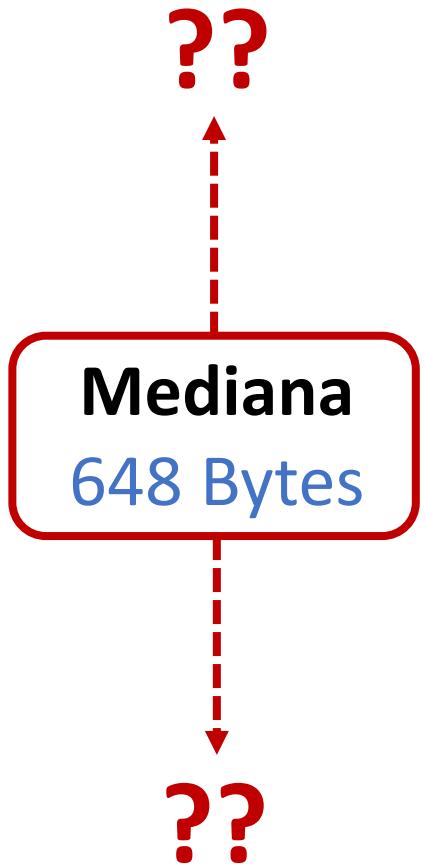
Mediana
648 Bytes

Profile: Bytes transferidos fuera de la red

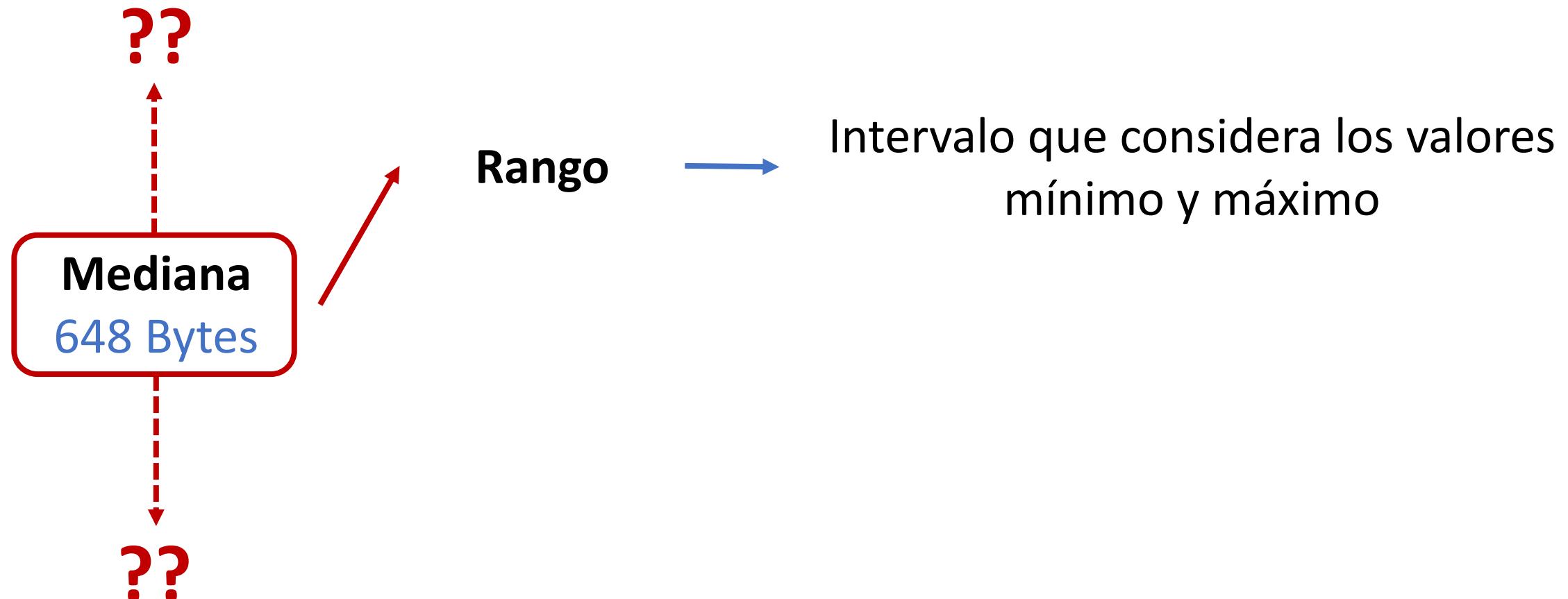


Mediana
648 Bytes

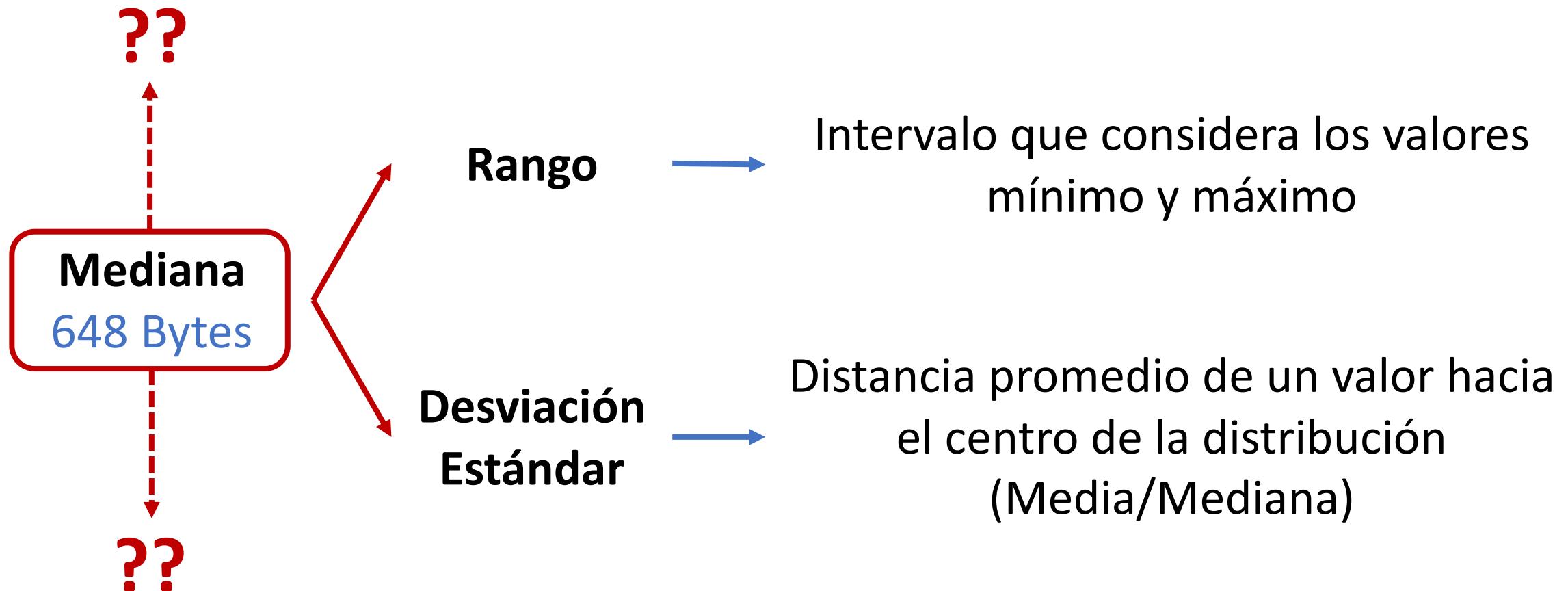
Medidas de dispersión (Variabilidad)



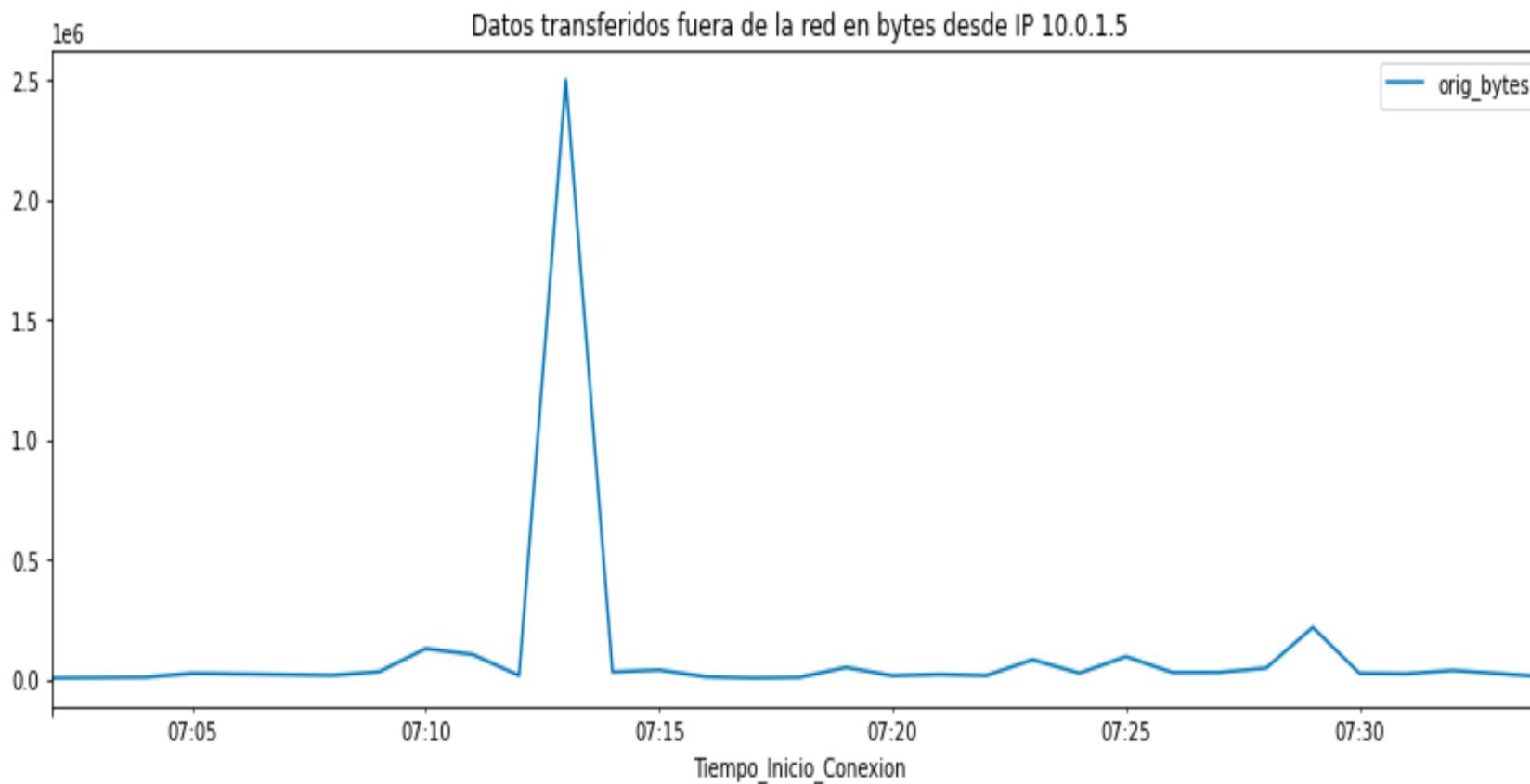
Medidas de dispersión (Variabilidad)



Medidas de dispersión (Variabilidad)



Profile: Bytes transferidos fuera de la red

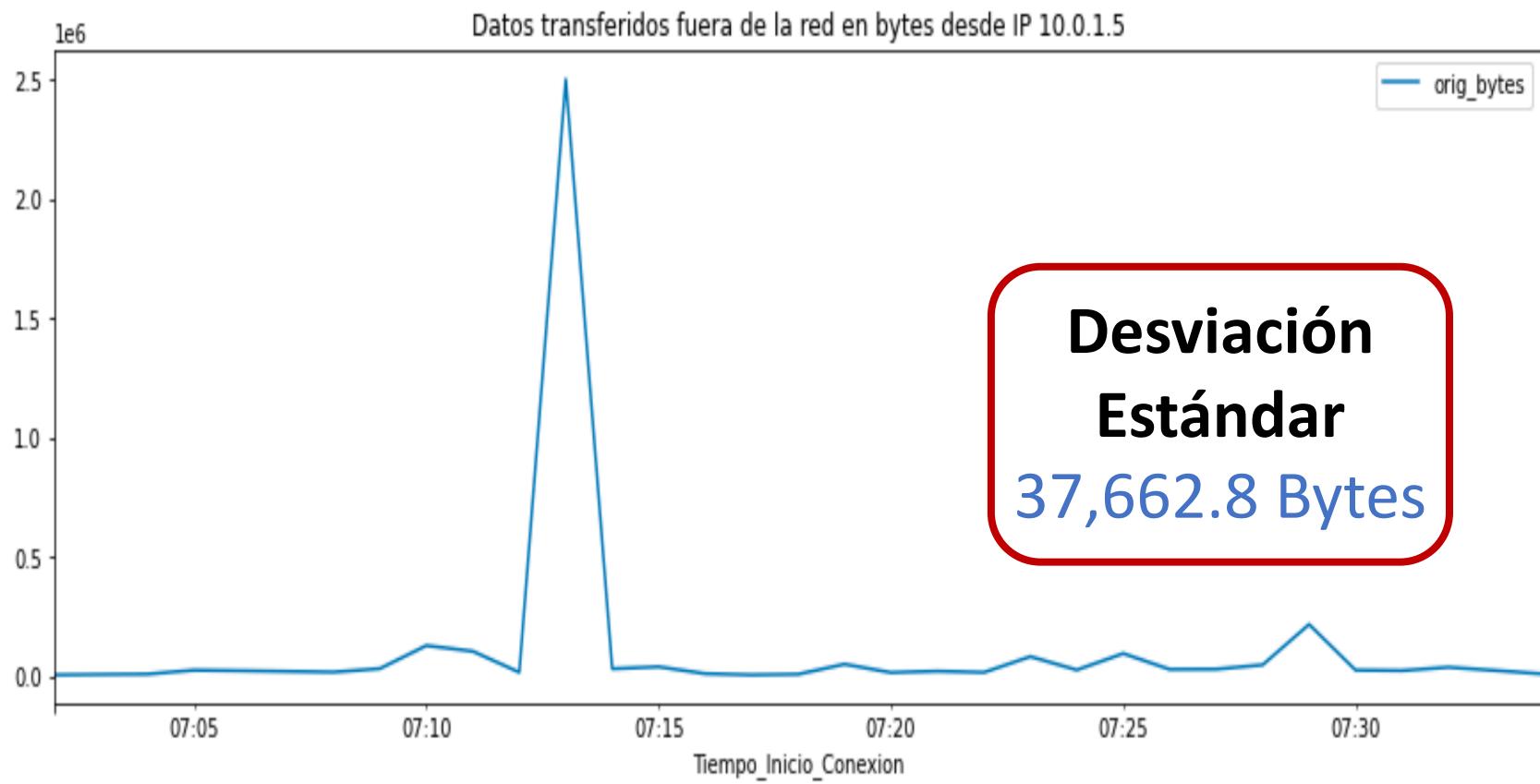


↑
Mediana
648 Bytes
↓

Profile: Bytes transferidos fuera de la red



Profile: Bytes transferidos fuera de la red

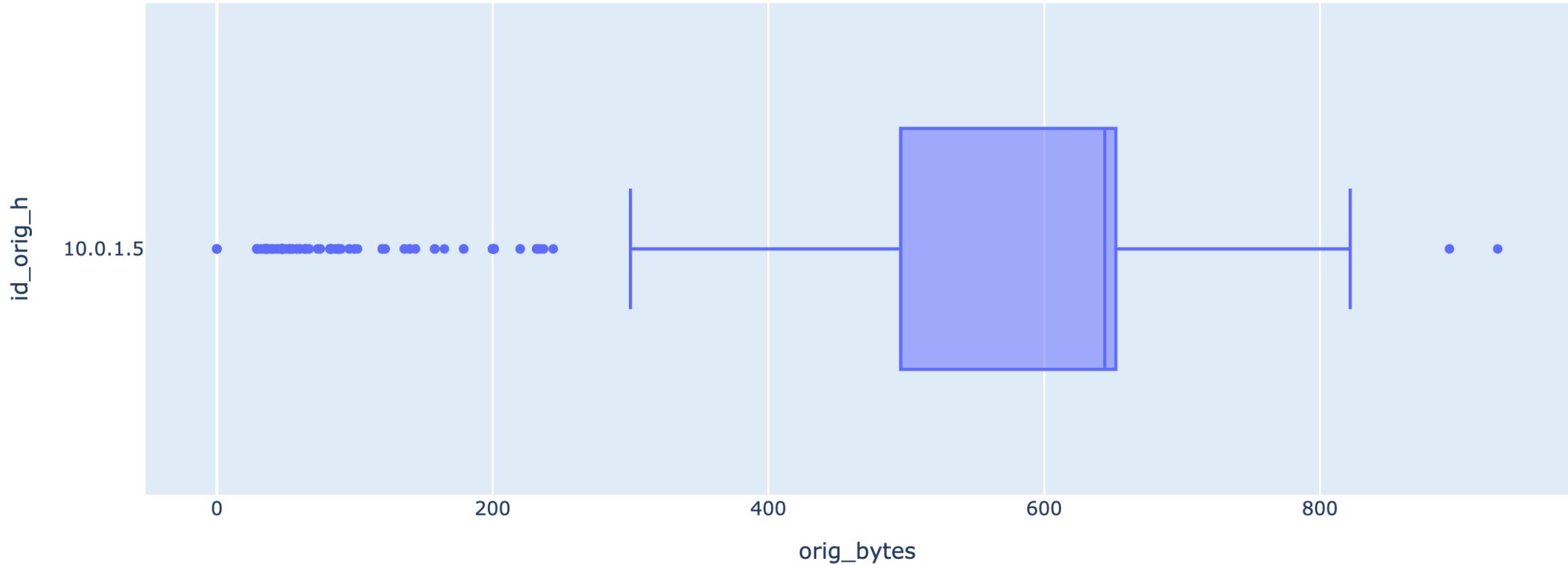


+ 37,662.8 Bytes

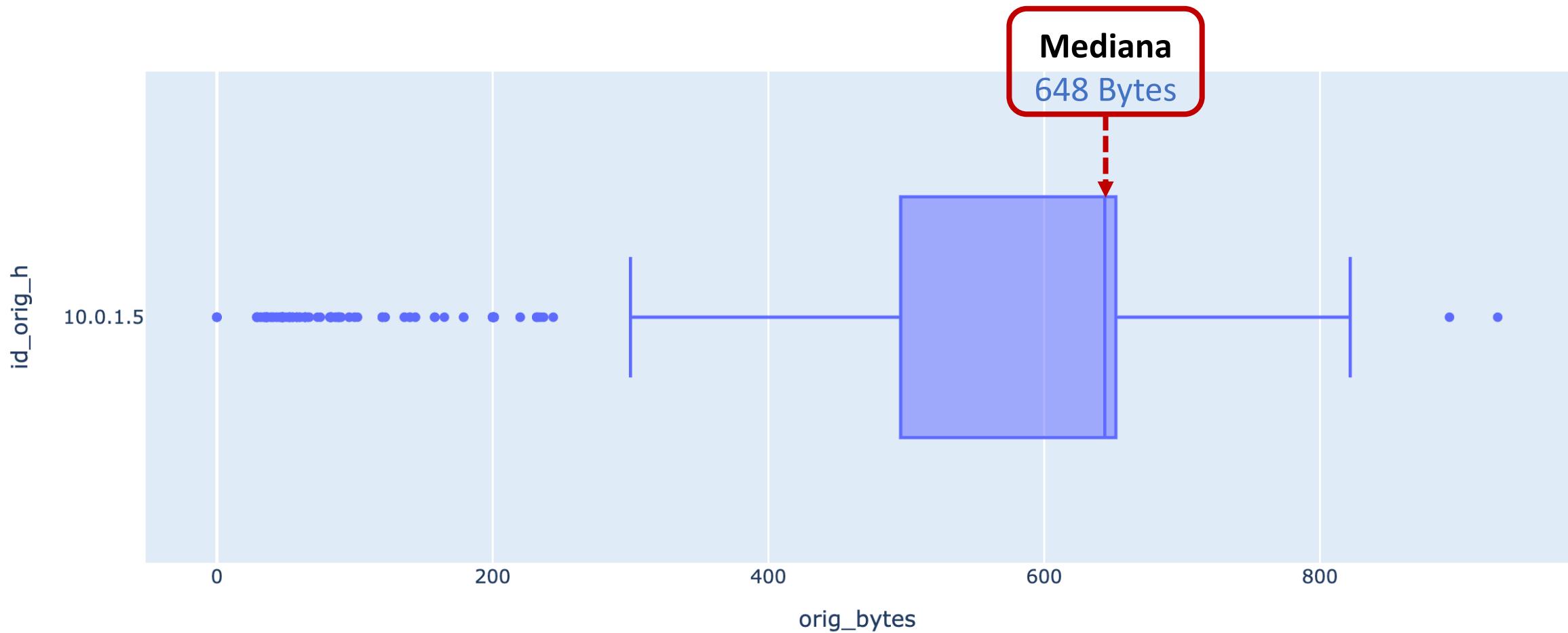
Mediana
648 Bytes

- 37,662.8 Bytes

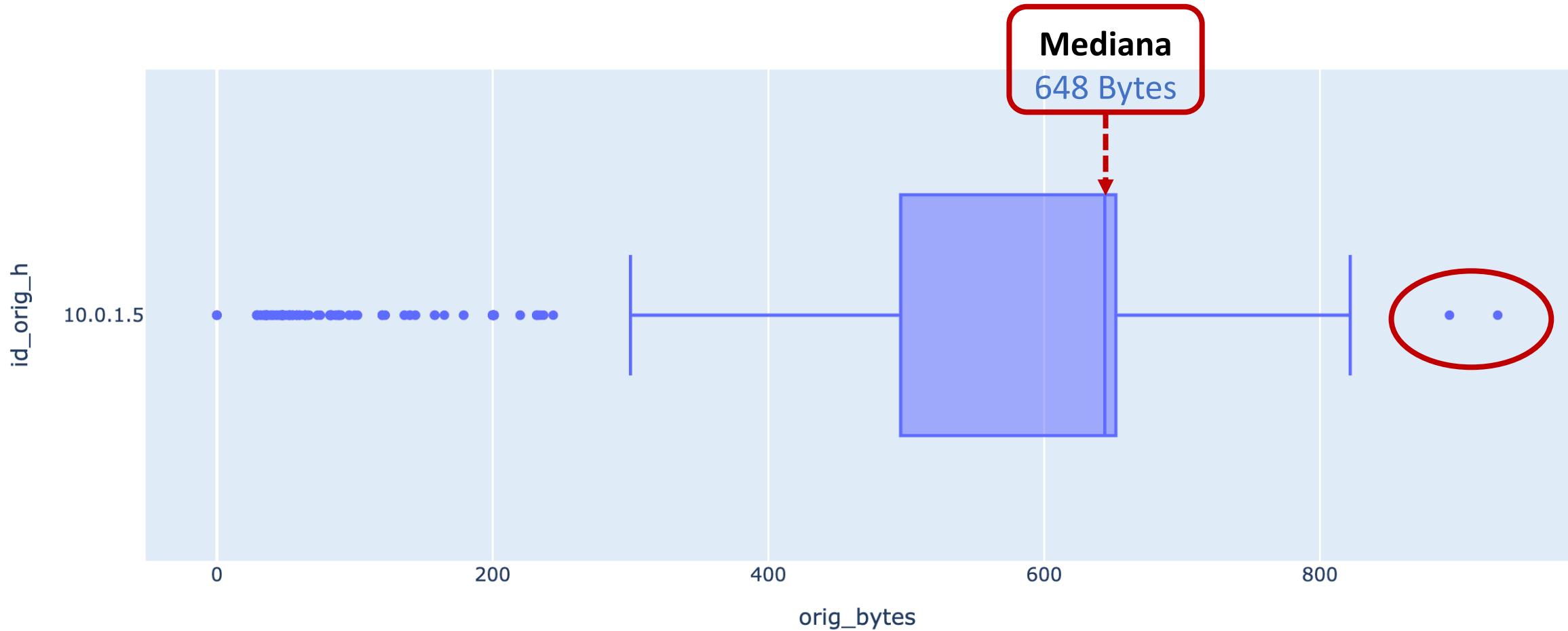
Boxplot: Bytes transferidos fuera de la red



Boxplot: Bytes transferidos fuera de la red

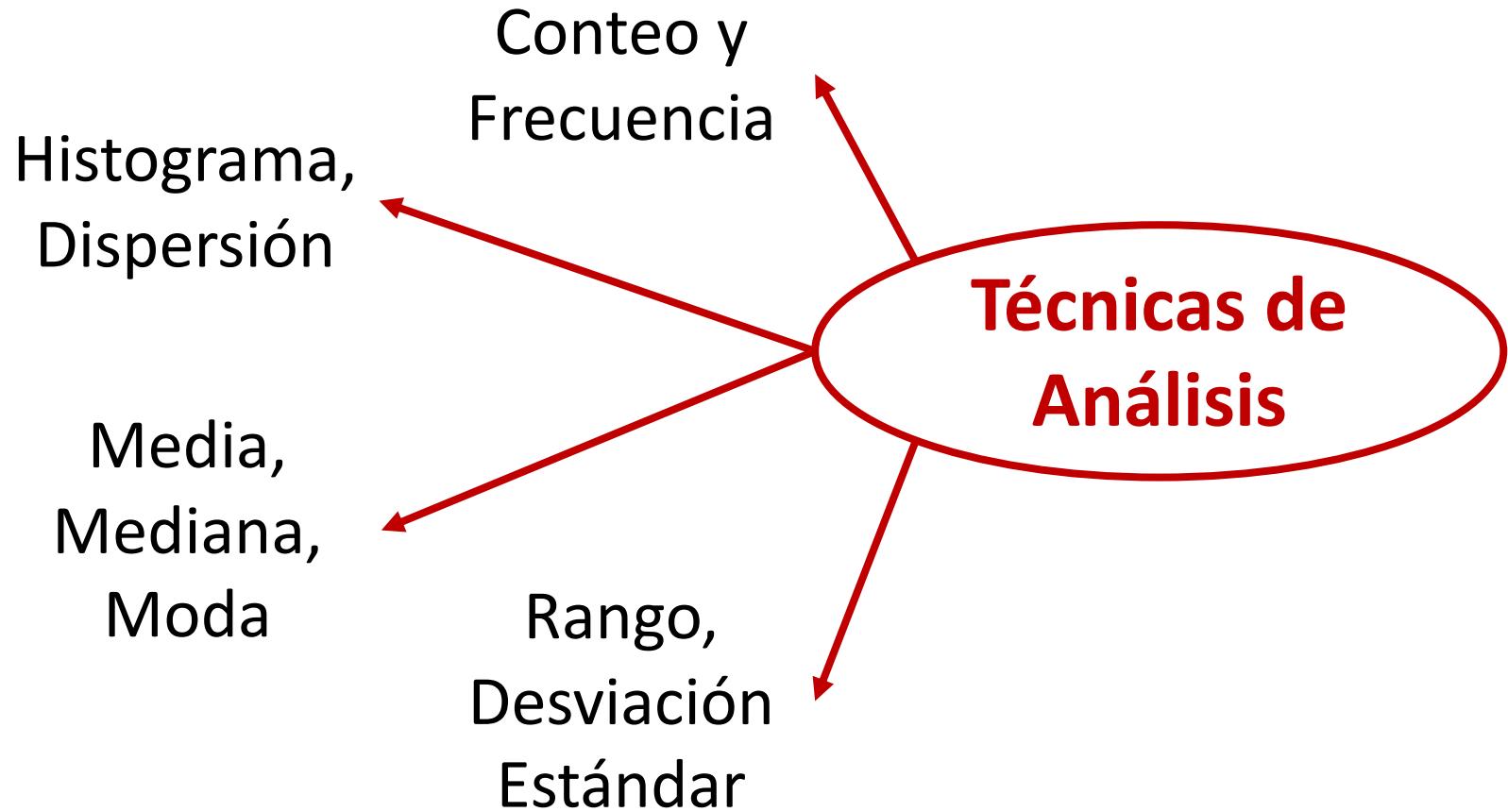


Boxplot: Bytes transferidos fuera de la red

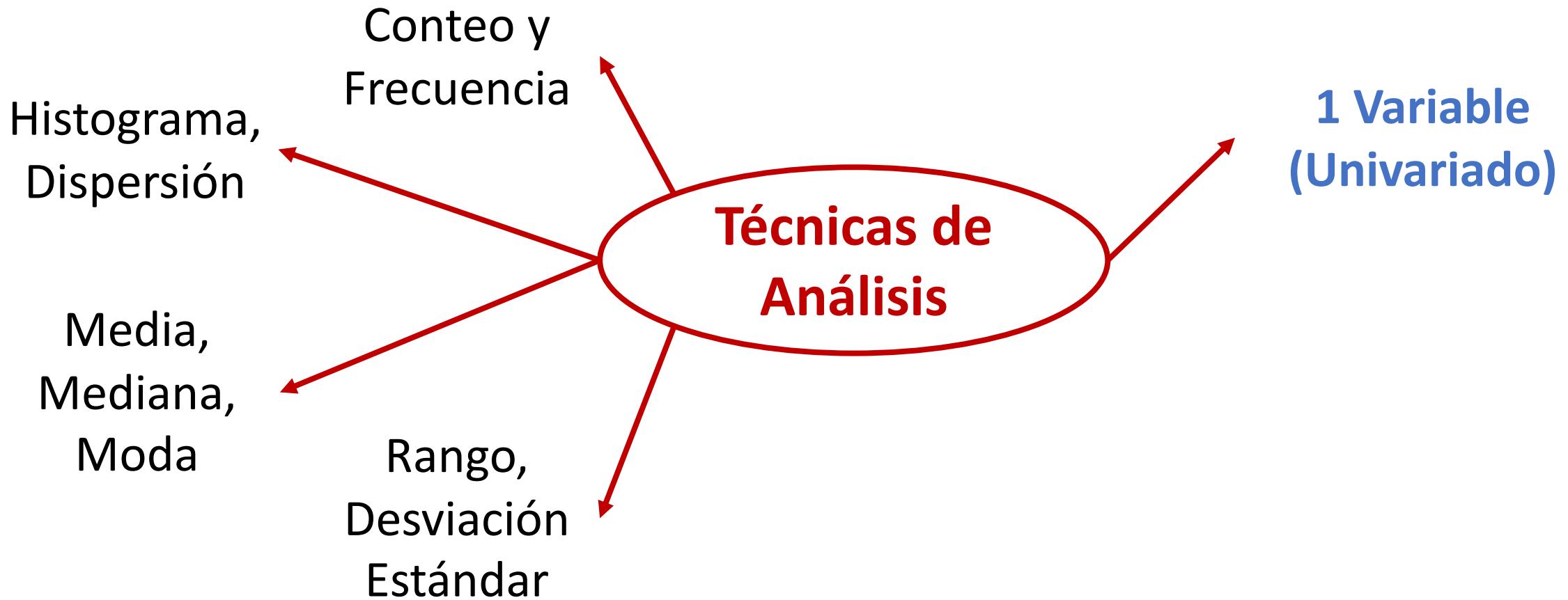


Identificando Nuevas Oportunidades de Investigación

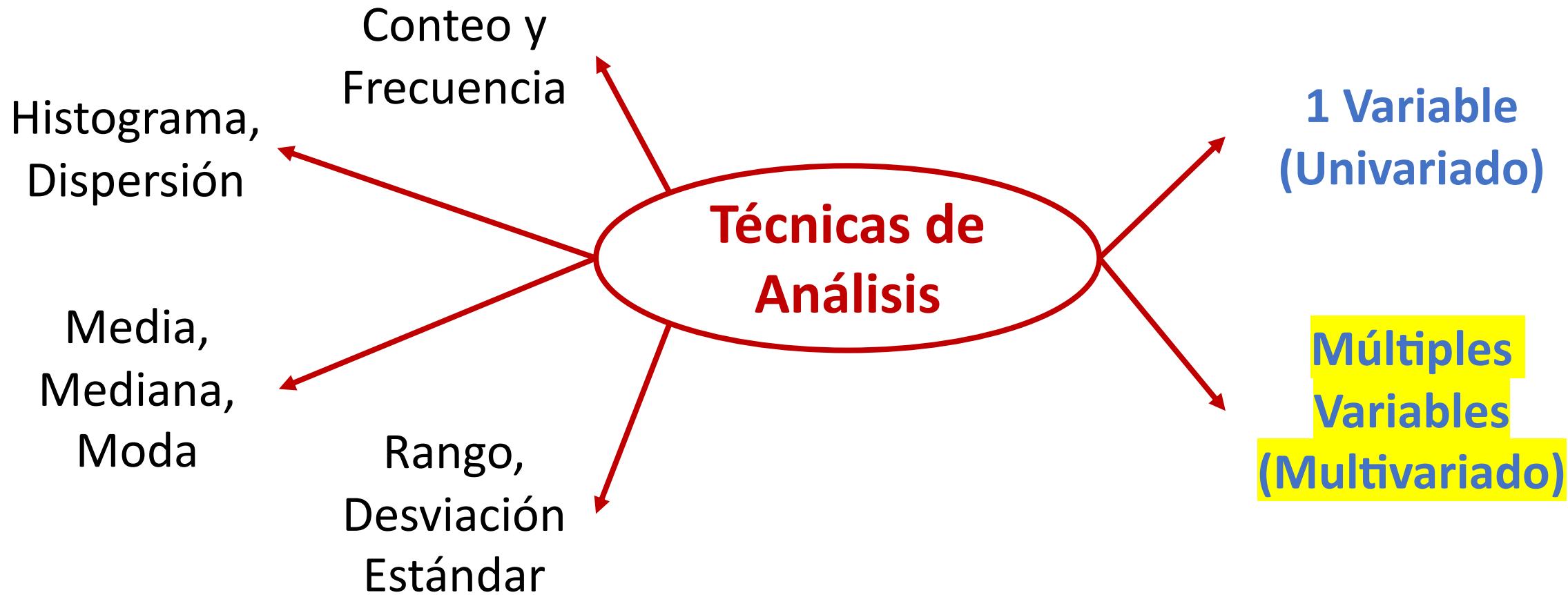
Hagamos un resumen



Hemos analizado variables



Qué hacer cuando recolectamos diversos atributos?



Representando nuestra data como una Matriz

ProcessGuid	Image	ParentCommandLine	network_connection	parent_command_line_length
{47ab858c-e13c-5eac-a903-00000000400}	C:\ProgramData\victim\cod.3aka3.scr	C:\windows\Explorer.EXE	yes	23
{47ab858c-e144-5eac-aa03-00000000400}	C:\Windows\System32\conhost.exe	"C:\ProgramData\victim\cod.3aka3.scr" /S	no	43
{47ab858c-e144-5eac-ab03-00000000400}	C:\Windows\System32\cmd.exe	"C:\ProgramData\victim\cod.3aka3.scr" /S	no	43
{47ab858c-e14e-5eac-ac03-00000000400}	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\windows\system32\cmd.exe"	no	29
{47ab858c-e17d-5eac-ad03-00000000400}	C:\Windows\System32\SearchProtocolHost.exe	C:\windows\system32\SearchIndexer.exe /Embedding	no	48

Representando nuestra data como una Matriz

ProcessGuid	Image	ParentCommandLine	network_connection	parent_command_line_length
{47ab858c-e13c-5eac-a903-00000000400}	C:\ProgramData\victim\@cod.3aka3.scr	C:\windows\Explorer.EXE	yes	23
{47ab858c-e144-5eac-aa03-00000000400}	C:\Windows\System32\conhost.exe	"C:\ProgramData\victim\@cod.3aka3.scr" /S	no	43
{47ab858c-e144-5eac-ab03-00000000400}	C:\Windows\System32\cmd.exe	"C:\ProgramData\victim\@cod.3aka3.scr" /S	no	43
{47ab858c-e14e-5eac-ac03-00000000400}	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\windows\system32\cmd.exe"	no	29
{47ab858c-e17d-5eac-ad03-00000000400}	C:\Windows\System32\SearchProtocolHost.exe	C:\windows\system32\SearchIndexer.exe /Embedding	no	48

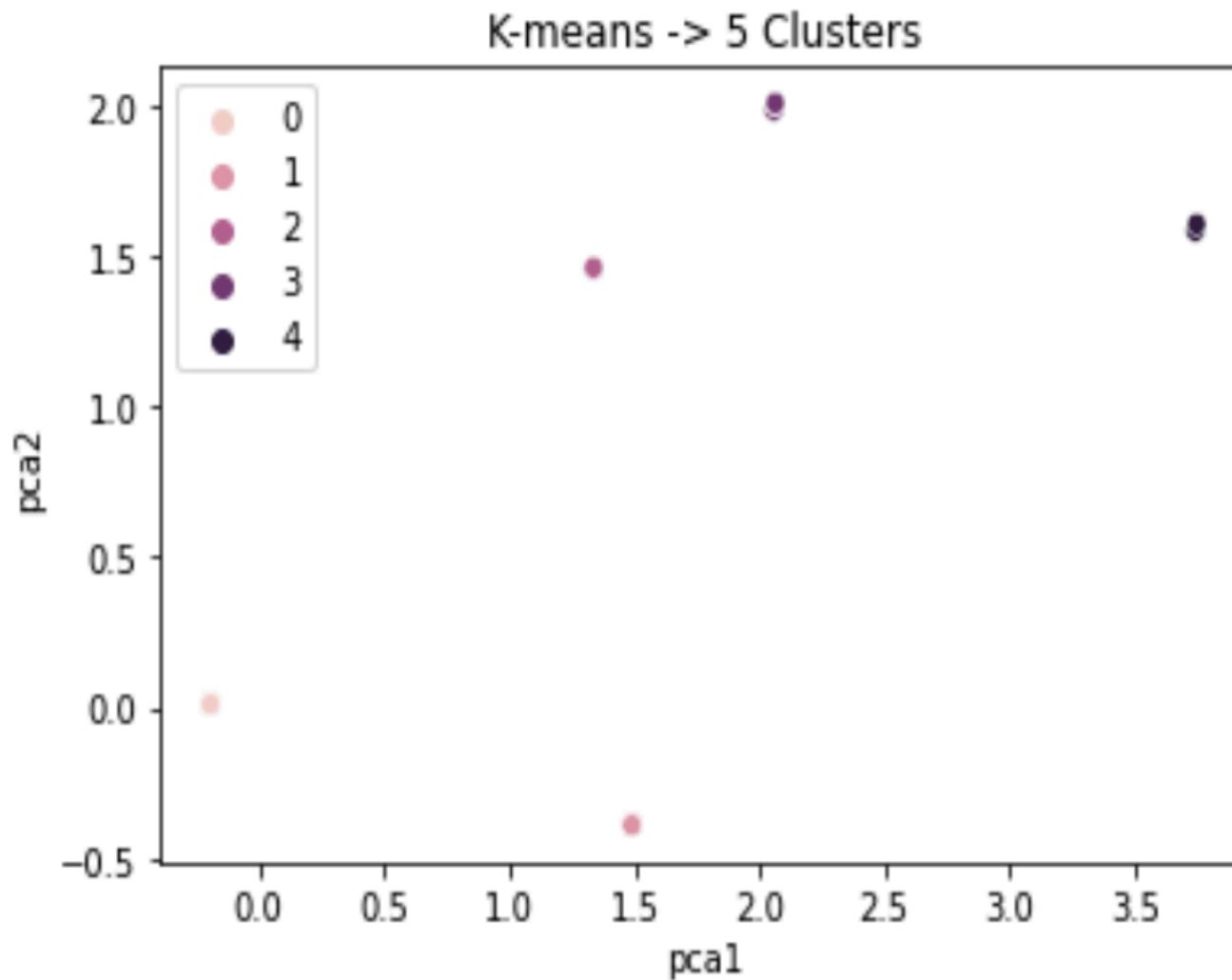
Cada fila representa un proceso & Cada columna representa un atributo

Ingeniería de Características en la Matriz

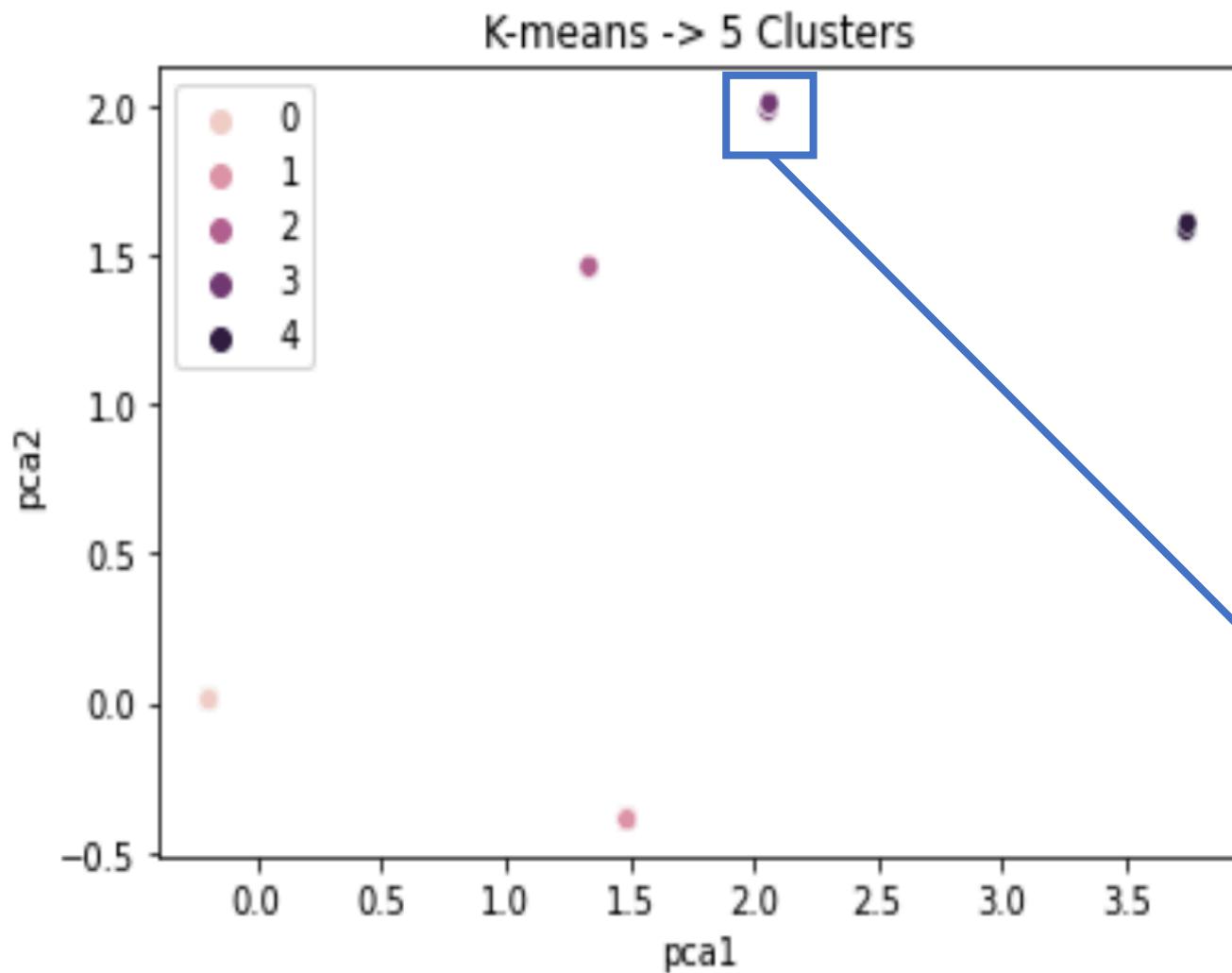
parent_command_line_length	network_connection_no	network_connection_yes
0.009310	0	1
0.017774	1	0
0.017774	1	0
0.011849	1	0
0.019890	1	0
0.019890	1	0
0.017774	1	0
0.017774	1	0
0.011849	1	0
0.011849	1	0

Expresando las variables de interés a través de Números

Modelo básico de agrupamiento: K-means

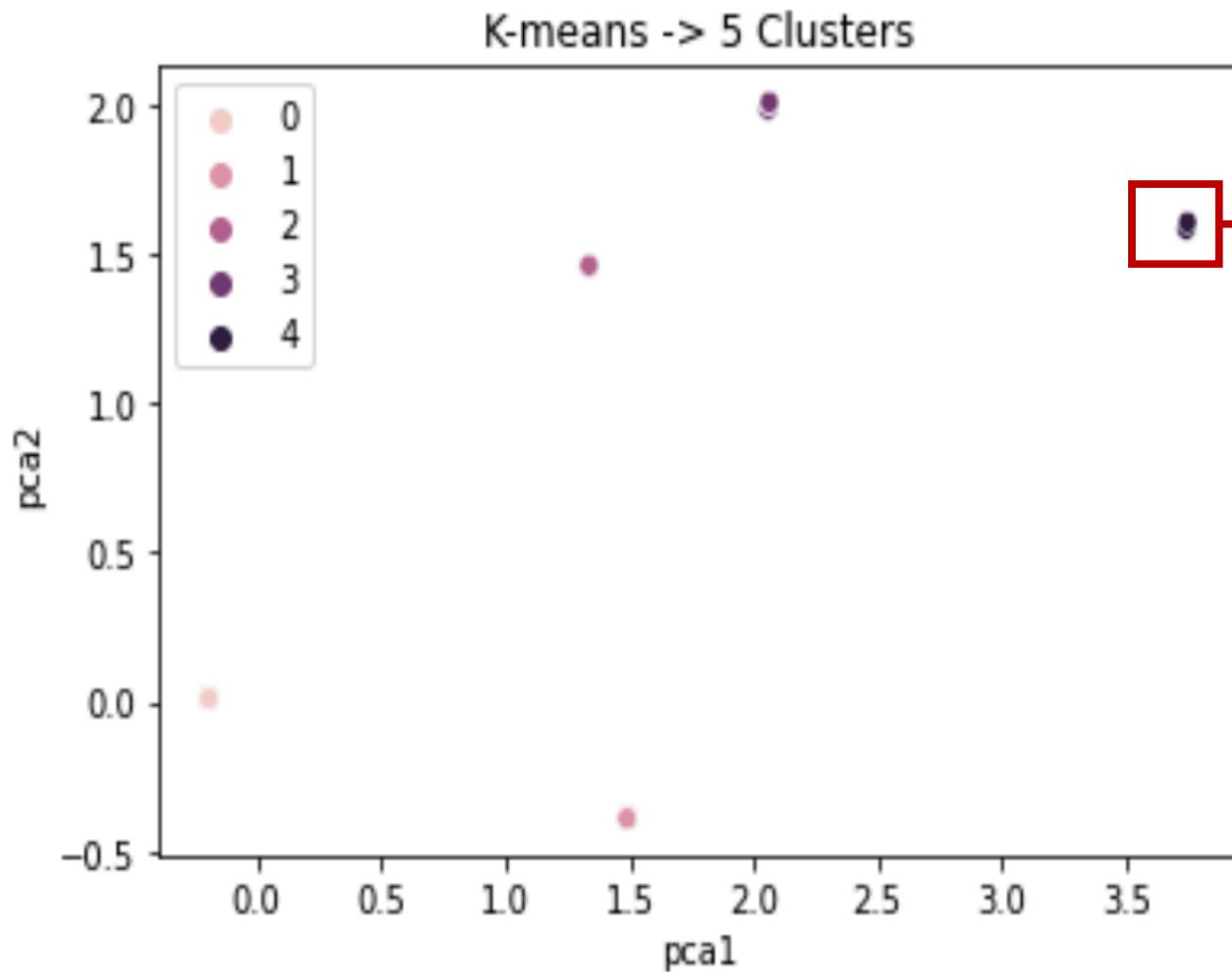


Modelo básico de agrupamiento: K-means



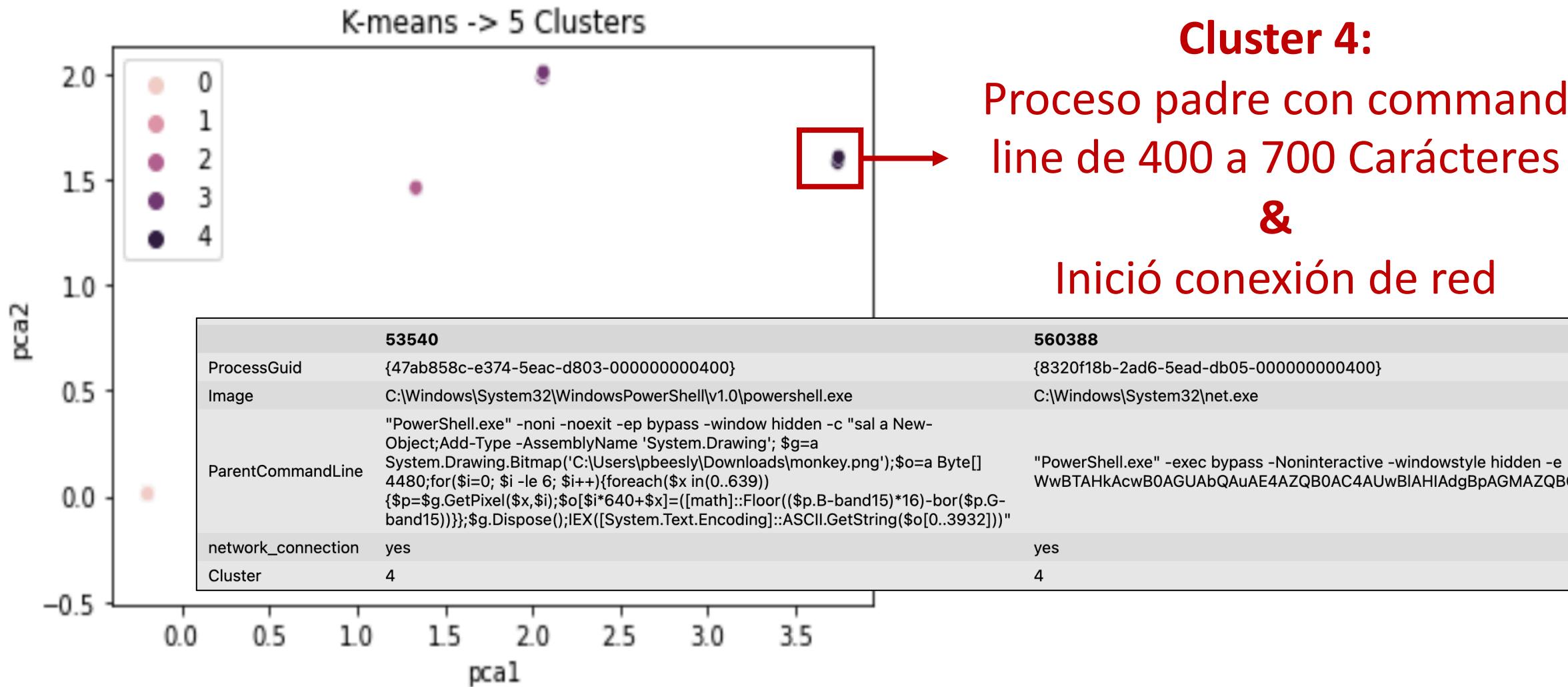
Cluster 3:
Proceso padre con command
line de 400 a 700 Carácteres
&
NO inició conexión de red

Modelo básico de agrupamiento: K-means



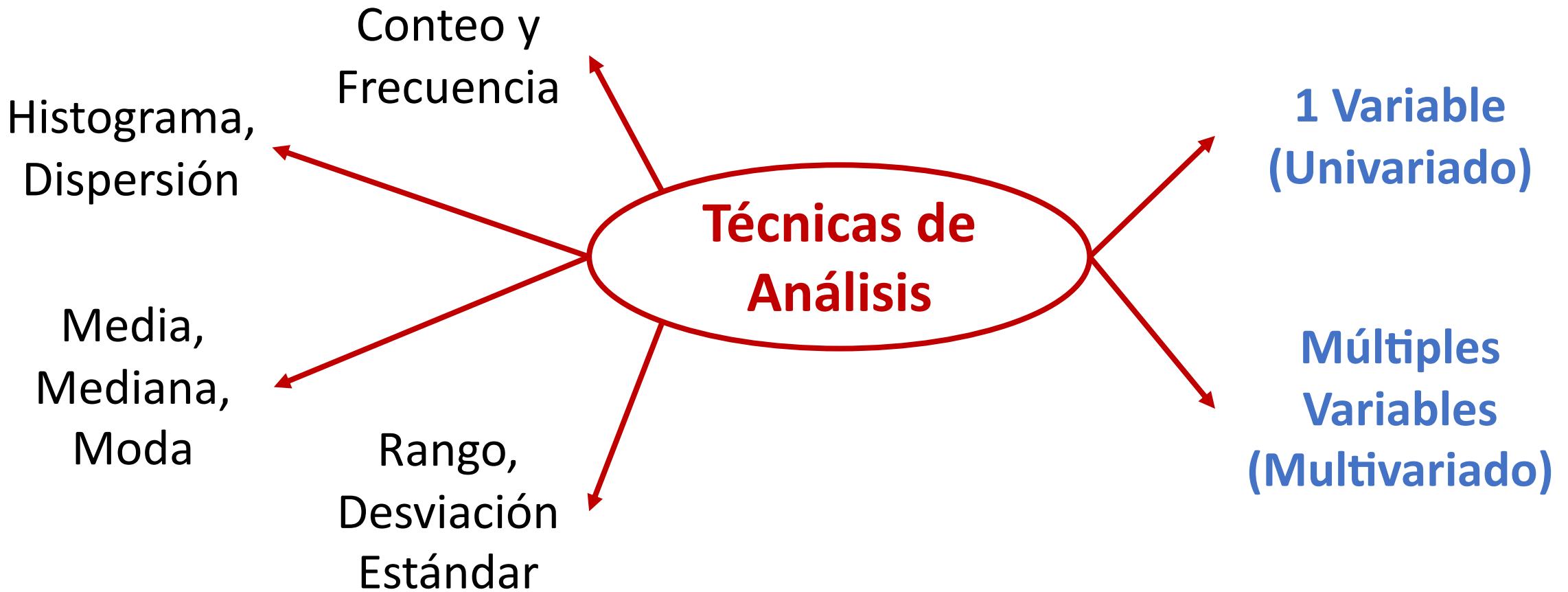
Cluster 4:
Proceso padre con command
line de 400 a 700 Carácteres
&
Inició conexión de red

Modelo básico de agrupamiento: K-means



Conclusiones

Conclusiones



Muchas Gracias 😊



@Cyb3rWard0g
@Cyb3rPandaH
@OTR_Community

