# EJERCICIOS REGEXP #

# Análisis y Procesamiento de Logs con Expresiones Regulares #

/(\w+):\/\/([^\s/]+)\/([^\s]*)/g
/^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}$/
/\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b/
EJERCICIOS REGEXP
Practical Regular Expression Exercises
9 Ejercicios Prácticos
Log Analysis
Pattern Matching

Autor : Unai Rubio
Fecha de publicación: 23 Febrero 2025
LinkedIn: https://www.linkedin.com/in/unaixoc/

# EJERCICIOS REGEXP

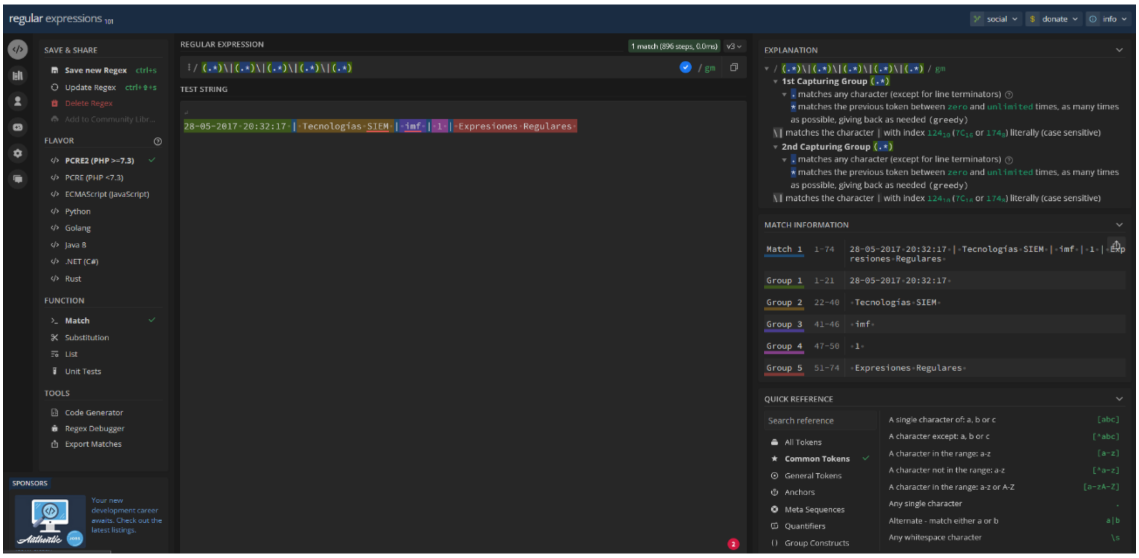
## Prerrequisitos

- **Recursos para RegEx:**
    - https://regex101.com/

## Ejercicio 1

- Desarrollar la expresión regular que parsee el siguiente log:
    - 28-05-2017 20:32:17 | Tecnologías SIEM | imf | 1 | Expresiones Regulares
- (.*)\|(.*)\|(.*)\|(.*)\|(.*)

-Compruebo los resultados arrojados.



REGULAR EXPRESSION 1 match (896 steps, 0.0ms) v3

```
/ (.*)\|(.*)\|(.*)\|(.*)\|(.*) / gm
```

TEST STRING

```
28-05-2017 20:32:17 | Tecnologías SIEM | imf | 1 | Expresiones Regulares
```

EXPLANATION

```
/ (.*)\|(.*)\|(.*)\|(.*)\|(.*) / gm
  1st Capturing Group (.*)
    . matches any character (except for line terminators)
    * matches the previous token between zero and unlimited times, as many times
      as possible, giving back as needed (greedy)
  \| matches the character | with index 124₁₀ (7C₁₆ or 174₈) literally (case sensitive)
  2nd Capturing Group (.*)
    . matches any character (except for line terminators)
    * matches the previous token between zero and unlimited times, as many times
      as possible, giving back as needed (greedy)
  \| matches the character | with index 124₁₀ (7C₁₆ or 174₈) literally (case sensitive)
```

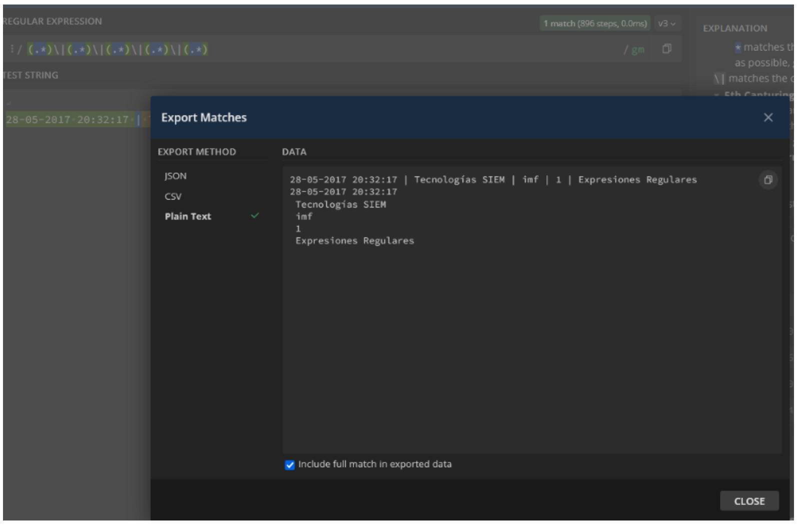
MATCH INFORMATION

```
Match 1   1-74    28-05-2017 20:32:17 | Tecnologías SIEM | imf | 1 | Expresiones Regulares
Group 1   1-21    28-05-2017 20:32:17
Group 2   22-40    Tecnologías SIEM
Group 3   41-46    imf
Group 4   47-50    1
Group 5   51-74    Expresiones Regulares
```

QUICK REFERENCE

Search reference		
All Tokens	A single character of: a, b or c	[abc]
Common Tokens ✓	A character except: a, b or c	[^abc]
General Tokens	A character in the range: a-z	[a-z]
Anchors	A character not in the range: a-z	[^a-z]
Meta Sequences	A character in the range: a-z or A-Z	[a-zA-Z]
Quantifiers	Any single character	.
Group Constructs	Alternate - match either a or b	a|b
	Any whitespace character	\s

-En Match information, clickamos en la flecha para Exportar resultados y nos arrojaría resultados en diferentes formatos ; json, csv, texto plano. En este caso se observa el Texto Plano.



DATA

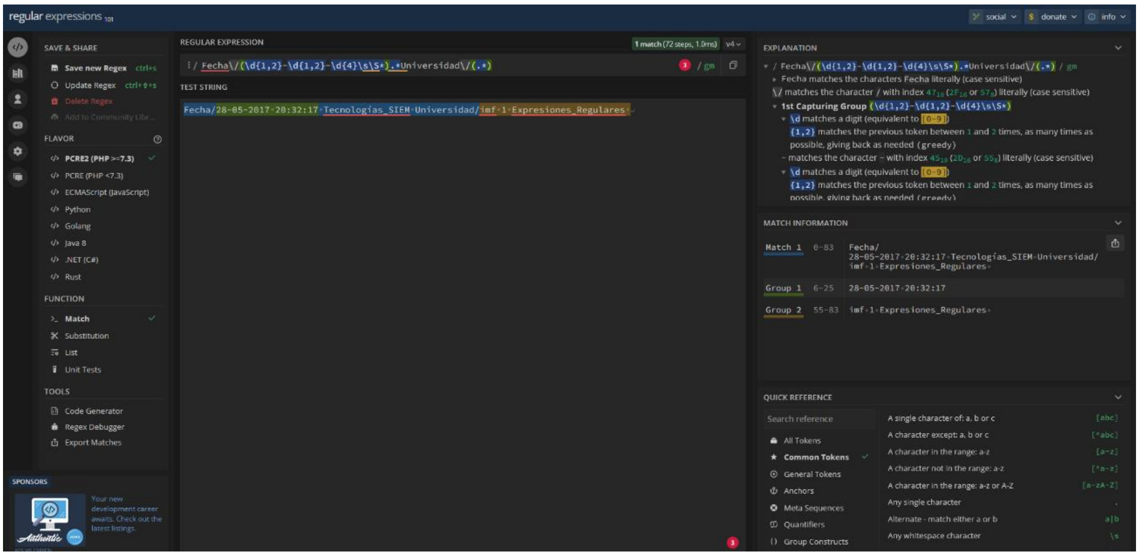
```
28-05-2017 20:32:17 | Tecnologías SIEM | imf | 1 | Expresiones Regulares
28-05-2017 20:32:17
 Tecnologías SIEM
 imf
 1
 Expresiones Regulares
```

☑ Include full match in exported data

## Ejercicio 2

- Desarrollar la expresión regular que parsee el siguiente log:
    - Fecha/28-05-2017 20:32:17 Tecnologías_SIEM Universidad/imf 1 Expresiones_Regulares
- Fecha\/(\d{1,2}-\d{1,2}-\d{4}\s\S*).*Universidad\/(.*)

-Compruebo los resultados arrojados.



REGULAR EXPRESSION

1 match (72 steps, 1.0ms) v4

```
/ Fecha\/(\d{1,2}-\d{1,2}-\d{4}\s\S*).*Universidad\/(.*) /gm
```

TEST STRING

```
Fecha/28-05-2017 20:32:17 Tecnologías_SIEM Universidad/imf 1 Expresiones_Regulares
```

EXPLANATION

- / Fecha\/(\d{1,2}-\d{1,2}-\d{4}\s\S*).*Universidad\/(.*) / gm
    - Fecha matches the characters Fecha literally (case sensitive)
    - \/ matches the character / with index 47_{10} ($2F_{16}$ or 57_8) literally (case sensitive)
    - 1st Capturing Group (\d{1,2}-\d{1,2}-\d{4}\s\S*)
        - \d matches a digit (equivalent to [0-9])
          {1,2} matches the previous token between 1 and 2 times, as many times as possible, giving back as needed (greedy)
        - - matches the character - with index 45_{10} ($2D_{16}$ or 55_8) literally (case sensitive)
        - \d matches a digit (equivalent to [0-9])
          {1,2} matches the previous token between 1 and 2 times, as many times as possible, giving back as needed (greedy)

MATCH INFORMATION

```
Match 1   0-83    Fecha/
                  28-05-2017 20:32:17 Tecnologías_SIEM Universidad/
                  imf 1 Expresiones_Regulares
Group 1   6-25    28-05-2017 20:32:17
Group 2   55-83   imf 1 Expresiones_Regulares
```

QUICK REFERENCE

Search reference

- All Tokens
- Common Tokens ✓
- General Tokens
- Anchors
- Meta Sequences
- Quantifiers
- Group Constructs

A single character of: a, b or c	[abc]
A character except: a, b or c	[^abc]
A character in the range: a-z	[a-z]
A character not in the range: a-z	[^a-z]
A character in the range: a-z or A-Z	[a-zA-Z]
Any single character	.
Alternate - match either a or b	a|b
Any whitespace character	\s

-En este caso , voy a comprobar el JSON :

```
[
  [
    {
      "content": "Fecha/28-05-2017 20:32:17 Tecnologías_SIEM Universidad/imf 1 Expresiones_Regulares ",
      "isParticipating": true,
      "groupNum": 0,
      "startPos": 0,
      "endPos": 83
    },
    {
      "content": "28-05-2017 20:32:17",
      "isParticipating": true,
      "groupNum": 1,
      "startPos": 6,
      "endPos": 25
    },
    {
      "content": "imf 1 Expresiones_Regulares ",
      "isParticipating": true,
      "groupNum": 2,
      "startPos": 55,
      "endPos": 83
    }
  ]
]
```

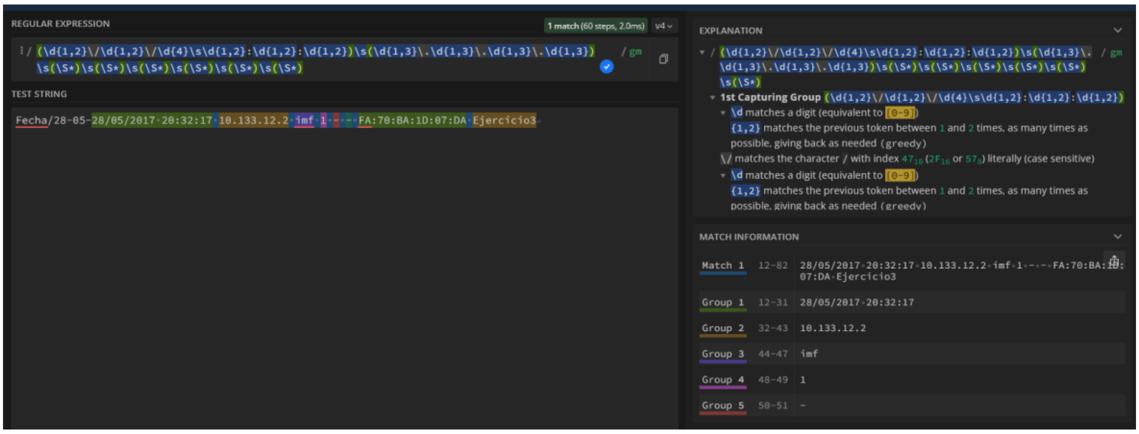
## Ejercicio 3

- Desarrollar la expresión regular que parsee el siguiente log:
    - 28/05/2017 20:32:17 10.133.12.2 imf 1 - - FA:70:BA:1D:07:DA Ejercicio3

-

```
(\d{1,2}\/\d{1,2}\/\d{4}\s\d{1,2}:\d{1,2}:\d{1,2})\s(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s(\S*)\s(\S*)\s(\S*)\s(\S*)\s(\S*)\s(\S*)
```

- Compruebo los resultados arrojados.



```
/ (\d{1,2}\/\d{1,2}\/\d{4}\s\d{1,2}:\d{1,2}:\d{1,2})\s(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s(\S*)\s(\S*)\s(\S*)\s(\S*)\s(\S*)\s(\S*) / gm
```

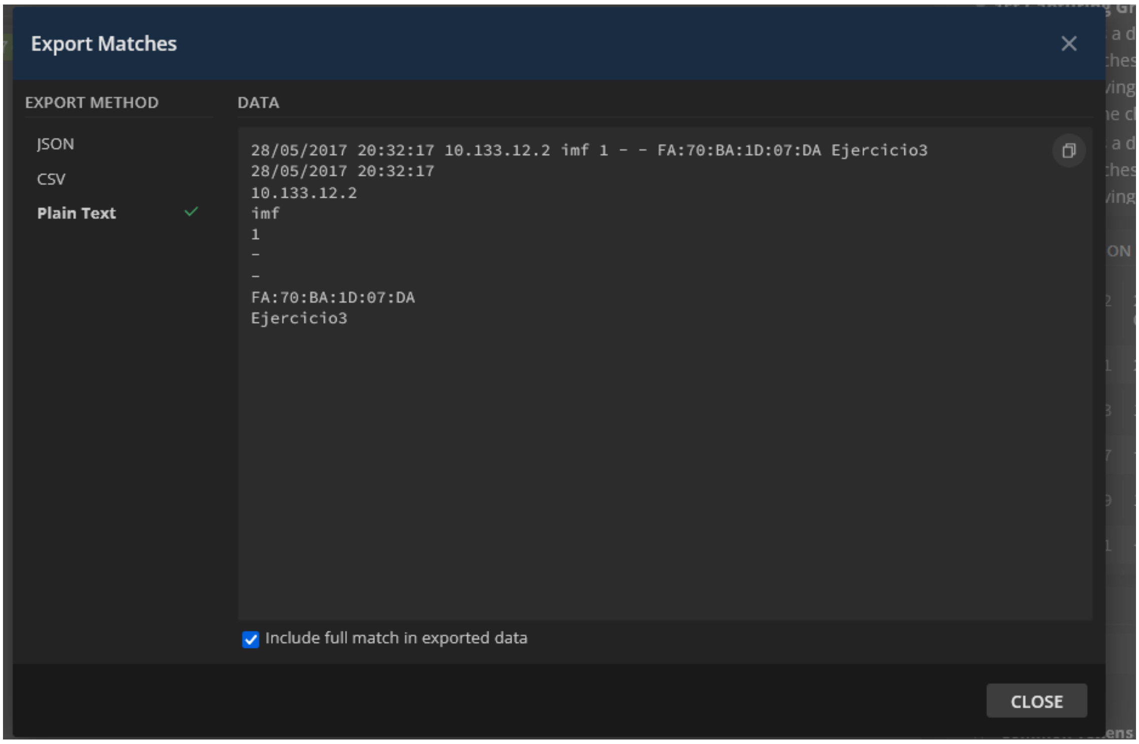
```
Fecha/28-05-28/05/2017 20:32:17 10.133.12.2 imf 1 - - FA:70:BA:1D:07:DA Ejercicio3
```

/ (\d{1,2}\/\d{1,2}\/\d{4}\s\d{1,2}:\d{1,2}:\d{1,2})\s(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s(\S*)\s(\S*)\s(\S*)\s(\S*)\s(\S*)\s(\S*) / gm

- 1st Capturing Group (\d{1,2}\/\d{1,2}\/\d{4}\s\d{1,2}:\d{1,2}:\d{1,2})
    - \d matches a digit (equivalent to [0-9])
      {1,2} matches the previous token between 1 and 2 times, as many times as possible, giving back as needed (greedy)
    - \/ matches the character / with index 47_{10} ($2F_{16}$ or 57_8) literally (case sensitive)
    - \d matches a digit (equivalent to [0-9])
      {1,2} matches the previous token between 1 and 2 times, as many times as possible, giving back as needed (greedy)

Match 1	12-82	28/05/2017 20:32:17 10.133.12.2 imf 1 - - FA:70:BA:1D:07:DA Ejercicio3
Group 1	12-31	28/05/2017 20:32:17
Group 2	32-43	10.133.12.2
Group 3	44-47	imf
Group 4	48-49	1
Group 5	50-51	-

-En Match information, clickamos en la flecha para Exportar resultados.En este caso se observa el Texto Plano y vemos fecha, ip , mac…



```
28/05/2017 20:32:17 10.133.12.2 imf 1 - - FA:70:BA:1D:07:DA Ejercicio3
28/05/2017 20:32:17
10.133.12.2
imf
1
-
-
FA:70:BA:1D:07:DA
Ejercicio3
```

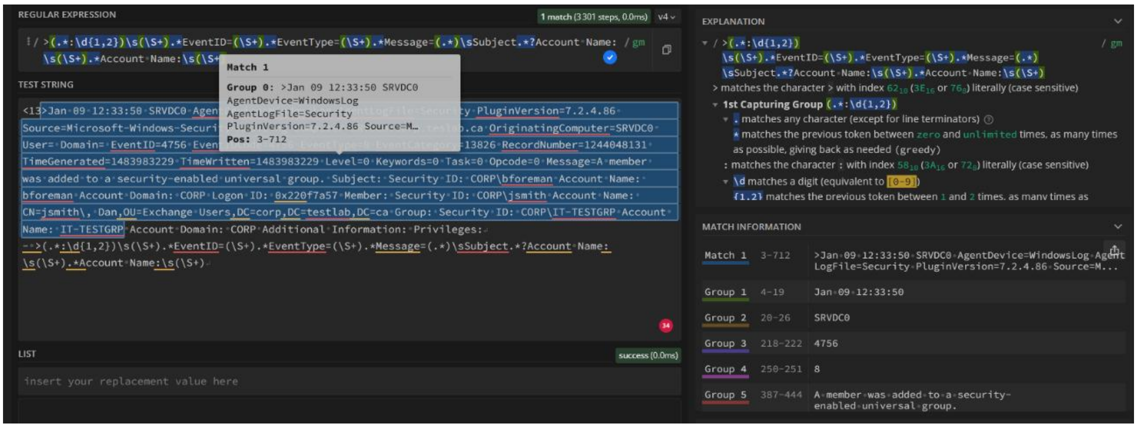
☑ Include full match in exported data

## Ejercicio 4

- Extraer del siguiente log los siguientes campos: timestamp, src.hostname, event.id, event.type, message, attacker.username, target.username, target.groupname.

```
    - <13>Jan 09 12:33:50 SRVDC0 AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.2.4.86 Source=Microsoft-Windows-Security-Auditing Computer=SRVDC0.corp.teslab.ca OriginatingComputer=SRVDC0 User= Domain= EventID=4756 EventIDCode=4756 EventType=8 EventCategory=13826 RecordNumber=1244048131 TimeGenerated=1483983229 TimeWritten=1483983229 Level=0 Keywords=0 Task=0 Opcode=0 Message=A member was added to a security-enabled universal group. Subject: Security ID: CORP\bforeman Account Name: bforeman Account Domain: CORP Logon ID: 0x220f7a57 Member: Security ID: CORP\jsmith Account Name: CN=jsmith\, Dan,OU=Exchange Users,DC=corp,DC=testlab,DC=ca Group: Security ID: CORP\IT-TESTGRP Account Name: IT-TESTGRP Account Domain: CORP Additional Information: Privileges:
- >(.*:\d{1,2})\s(\S+).*EventID=(\S+).*EventType=(\S+).*Message=(.*)\sSubject.*?Account Name:\s(\S+).*Account Name:\s(\S+)
```

-Compruebo los resultados arrojados.



```
/ >(.*:\d{1,2})\s(\S+).*EventID=(\S+).*EventType=(\S+).*Message=(.*)\sSubject.*?Account Name: / gm
\s(\S+).*Account Name:\s(\S+)
```

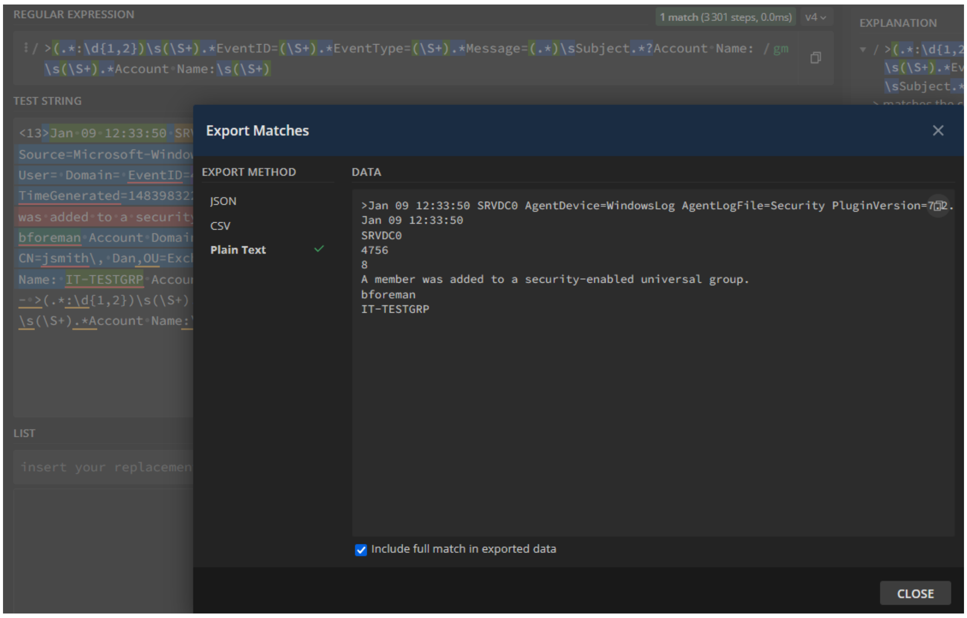
Match 1
Group 0: >Jan 09 12:33:50 SRVDC0 AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.2.4.86 Source=M…
Pos: 3-712

```
<13>Jan 09 12:33:50 SRVDC0 Agen… PluginVersion=7.2.4.86
Source=Microsoft-Windows-Securi… .ca OriginatingComputer=SRVDC0
User= Domain= EventID=4756 Even… 13826 RecordNumber=1244048131
TimeGenerated=1483983229 TimeWritten=1483983229 Level=0 Keywords=0 Task=0 Opcode=0 Message=A member
was added to a security-enabled universal group. Subject: Security ID: CORP\bforeman Account Name:
bforeman Account Domain: CORP Logon ID: 0x220f7a57 Member: Security ID: CORP\jsmith Account Name:
CN=jsmith\, Dan,OU=Exchange Users,DC=corp,DC=testlab,DC=ca Group: Security ID: CORP\IT-TESTGRP Account
Name: IT-TESTGRP Account Domain: CORP Additional Information: Privileges:
- >(.*:\d{1,2})\s(\S+).*EventID=(\S+).*EventType=(\S+).*Message=(.*)\sSubject.*?Account Name:
\s(\S+).*Account Name:\s(\S+)
```

/ >(.*:\d{1,2})\s(\S+).*EventID=(\S+).*EventType=(\S+).*Message=(.*)\sSubject.*?Account Name:\s(\S+).*Account Name:\s(\S+) / gm
> matches the character > with index 62_{10} ($3E_{16}$ or 76_8) literally (case sensitive)
1st Capturing Group (.*:\d{1,2})
. matches any character (except for line terminators)
* matches the previous token between zero and unlimited times, as many times as possible, giving back as needed (greedy)
: matches the character : with index 58_{10} ($3A_{16}$ or 72_8) literally (case sensitive)
\d matches a digit (equivalent to [0-9])
{1,2} matches the previous token between 1 and 2 times, as many times as

Match 1	3-712	>Jan 09 12:33:50 SRVDC0 AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.2.4.86 Source=M...
Group 1	4-19	Jan 09 12:33:50
Group 2	20-26	SRVDC0
Group 3	218-222	4756
Group 4	250-251	8
Group 5	387-444	A member was added to a security-enabled universal group.

-En Match information, clickamos en la flecha para Exportar resultados .En este caso se observa el Texto Plano , en el cual veremos los resultados que nos pide el ejercicio.



```
>Jan 09 12:33:50 SRVDC0 AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.2.
Jan 09 12:33:50
SRVDC0
4756
8
A member was added to a security-enabled universal group.
bforeman
IT-TESTGRP
```

RESULTADOS : (Extraer del siguiente log los siguientes campos: timestamp, src.hostname, event.id, event.type, message, attacker.username, target.username, target.groupname.)

- timestamp: Jan 09 12:33:50
- src.hostname: SRVDC0
- event.id: 4756
- event.type: 8
- message: A member was added to a security-enabled universal group.
- attacker.username: bforeman
- target.username: No se proporciona en el log.
- target.groupname: IT-TESTGRP

-Si observamos el JPSON , encontraremos también los resultados que nos pide el ejercicio.

```
[
  [
    {
      "content": ">Jan 09 12:33:50 SRVDC0 AgentDevice=WindowsLog AgentLogFile=Security
PluginVersion=7.2.4.86 Source=Microsoft-Windows-Security-Auditing
Computer=SRVDC0.corp.teslab.ca OriginatingComputer=SRVDC0 User= Domain= EventID=4756
EventIDCode=4756 EventType=8 EventCategory=13826 RecordNumber=1244048131
TimeGenerated=1483983229 TimeWritten=1483983229 Level=0 Keywords=0 Task=0 Opcode=0
Message=A member was added to a security-enabled universal group. Subject: Security ID:
CORP\\bforeman Account Name: bforeman Account Domain: CORP Logon ID: 0x220f7a57 Member:
Security ID: CORP\\jsmith Account Name: CN=jsmith\\, Dan,OU=Exchange
Users,DC=corp,DC=testlab,DC=ca Group: Security ID: CORP\\IT-TESTGRP Account Name: IT-
TESTGRP",
      "isParticipating": true,
      "groupNum": 0,
      "startPos": 3,
      "endPos": 712
    },
    {
      "content": "Jan 09 12:33:50",
      "isParticipating": true,
      "groupNum": 1,
      "startPos": 4,
      "endPos": 19
    },
    {
      "content": "SRVDC0",
      "isParticipating": true,
      "groupNum": 2,
      "startPos": 20,
      "endPos": 26
    },
    {
      "content": "4756",
      "isParticipating": true,
      "groupNum": 3,
      "startPos": 218,
      "endPos": 222
    },
    {
      "content": "8",
      "isParticipating": true,
      "groupNum": 4,
      "startPos": 250,
      "endPos": 251
    },
    {
      "content": "A member was added to a security-enabled universal group.",
      "isParticipating": true,
      "groupNum": 5,
      "startPos": 387,
      "endPos": 444
    },
    {
      "content": "bforeman",
      "isParticipating": true,
      "groupNum": 6,
      "startPos": 495,
      "endPos": 503
    },
    {
      "content": "IT-TESTGRP",
      "isParticipating": true,
      "groupNum": 7,
      "startPos": 702,
      "endPos": 712
    }
  ]
]
```

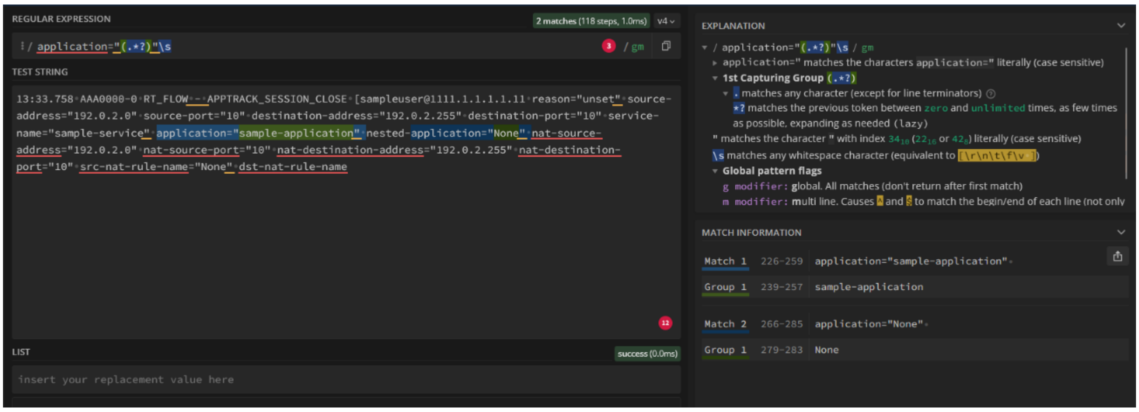
## Ejercicio 5

- Desarrollar la expresión regular que parsee del siguiente log la cadena: `application="NOMBRE_APLICACION"`

    - 13:33.758 AAA0000-0 RT_FLOW - APPTRACK_SESSION_CLOSE [sampleuser@1111.1.1.1.1.11 reason="unset" source-address="192.0.2.0" source-port="10" destination-address="192.0.2.255" destination-port="10" service-name="sample-service" application="sample-application" nested-application="None" nat-source-address="192.0.2.0" nat-source-port="10" nat-destination-address="192.0.2.255" nat-destination-port="10" src-nat-rule-name="None" dst-nat-rule-name

- application="(.*?)"\s

-Compruebo los resultados arrojados.



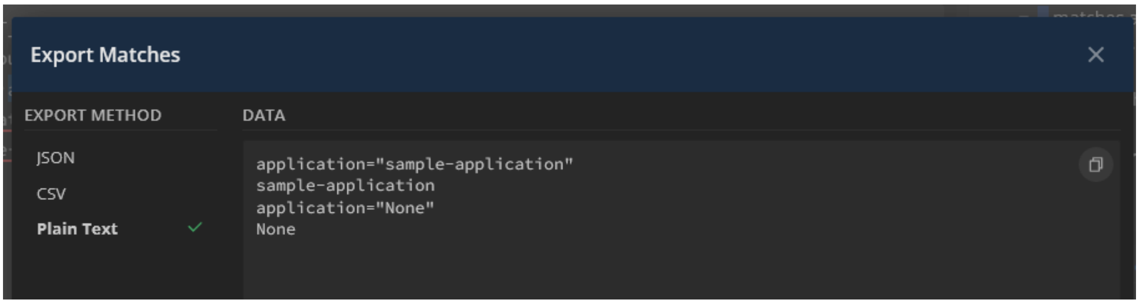
```
/ application="(.*?)"\s / gm
```

```
13:33.758 AAA0000-0 RT_FLOW - APPTRACK_SESSION_CLOSE [sampleuser@1111.1.1.1.1.11 reason="unset" source-
address="192.0.2.0" source-port="10" destination-address="192.0.2.255" destination-port="10" service-
name="sample-service" application="sample-application" nested-application="None" nat-source-
address="192.0.2.0" nat-source-port="10" nat-destination-address="192.0.2.255" nat-destination-
port="10" src-nat-rule-name="None" dst-nat-rule-name
```

```
/ application="(.*?)"\s / gm
  application=" matches the characters application=" literally (case sensitive)
  1st Capturing Group (.*?)
    . matches any character (except for line terminators)
    *? matches the previous token between zero and unlimited times, as few times
    as possible, expanding as needed (lazy)
  " matches the character " with index 34₁₀ (22₁₆ or 42₈) literally (case sensitive)
  \s matches any whitespace character (equivalent to [\r\n\t\f\v ])
  Global pattern flags
    g modifier: global. All matches (don't return after first match)
    m modifier: multi line. Causes ^ and $ to match the begin/end of each line (not only
```

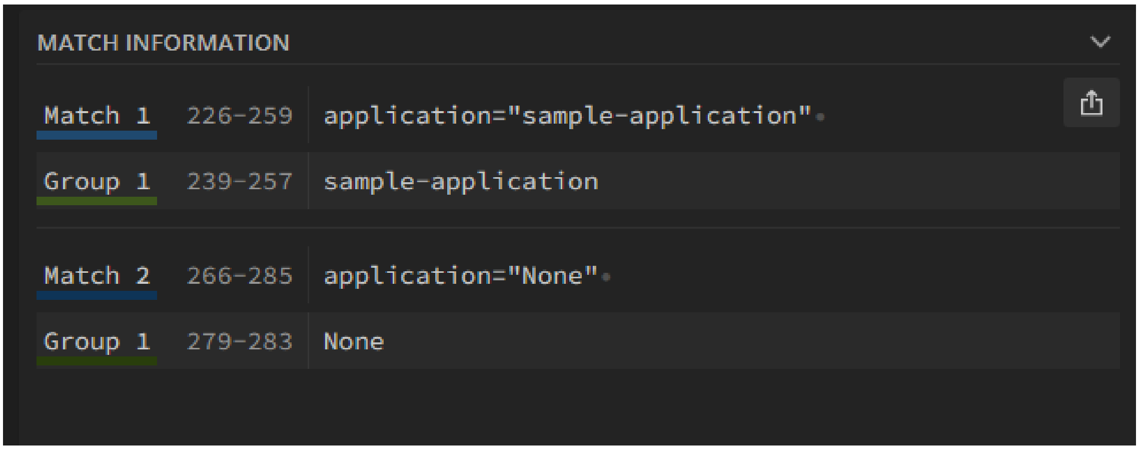
```
Match 1   226-259   application="sample-application"
Group 1   239-257   sample-application

Match 2   266-285   application="None"
Group 1   279-283   None
```

- En Match information, clickamos en la flecha para Exportar resultados .En este caso se observa el Texto Plano , y observaríamos la cadena.



```
application="sample-application"
sample-application
application="None"
None
```

-MATCH INFORMATION :



```
Match 1   226-259   application="sample-application"
Group 1   239-257   sample-application

Match 2   266-285   application="None"
Group 1   279-283   None
```

## Ejercicio 6

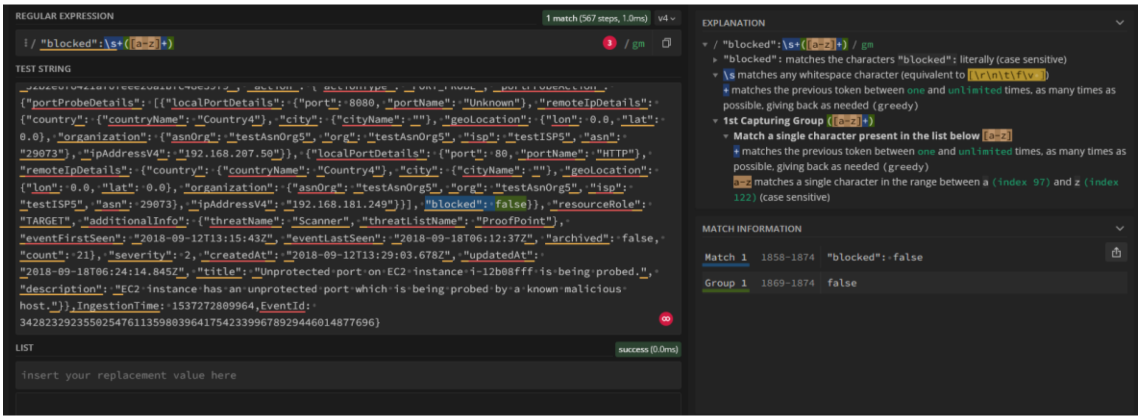
- Desarrollar la expresión regular que parsee del siguiente log si el stream ha sido bloqueado o no (campo blocked)

```
    - {LogStreamName: GuardDutyLogStream,Timestamp: 1537272809958,Message: {"version":
"0", "id": "095aab52-d1cd-2a72-a11a-afda5b22c1f6", "detail-type": "GuardDuty Finding",
"source": "aws.guardduty", "account": "348426448370", "time": "2018-09-18T12:13:17Z",
"region": "us-east-1", "resources": [], "detail": {"schemaVersion": "2.0", "accountId":
"126223755640", "region": "us-east-1", "partition": "aws", "id":
"24b2e6fc47df1e5186fc306f75130143", "arn": "arn:aws:guardduty:us-east-
1:126223755640:detector/32b2e6f6421a70feee26a1bfc48e39f9/finding/24b2e6fc47df1e5186fc30
6f75130143", "type": "Recon:EC2/PortProbeUnprotectedPort", "resource": {"resourceType":
"Instance", "instanceDetails": {"instanceId": "i-12b08fff", "instanceType":
"m3.2xlarge", "launchTime": "2014-10-30T12:03:29Z", "platform": null, "productCodes":
[], "iamInstanceProfile": null, "networkInterfaces": [], "tags": [{"value": "ahl-
production-jira", "key": "Name"}], "instanceState": "running", "availabilityZone": "us-
east-1c", "imageId": "ami-00ab0168", "imageDescription": "null"}}, "service":
{"serviceName": "guardduty", "detectorId": "32b2e6f6421a70feee26a1bfc48e39f9",
"action": {"actionType": "PORT_PROBE", "portProbeAction": {"portProbeDetails":
[{"localPortDetails": {"port": 8080, "portName": "Unknown"}, "remoteIpDetails":
{"country": {"countryName": "Country4"}, "city": {"cityName": ""}, "geoLocation":
{"lon": 0.0, "lat": 0.0}, "organization": {"asnOrg": "testAsnOrg5", "org":
```

```
"testAsnOrg5", "isp": "testISP5", "asn": "29073"}, "ipAddressV4": "192.168.207.50"}},
{"localPortDetails": {"port": 80, "portName": "HTTP"}, "remoteIpDetails": {"country":
{"countryName": "Country4"}, "city": {"cityName": ""}, "geoLocation": {"lon": 0.0,
"lat": 0.0}, "organization": {"asnOrg": "testAsnOrg5", "org": "testAsnOrg5", "isp":
"testISP5", "asn": 29073}, "ipAddressV4": "192.168.181.249"}}], "blocked": false}},
"resourceRole": "TARGET", "additionalInfo": {"threatName": "Scanner", "threatListName":
"ProofPoint"}, "eventFirstSeen": "2018-09-12T13:15:43Z", "eventLastSeen": "2018-09-
18T06:12:37Z", "archived": false, "count": 21}, "severity": 2, "createdAt": "2018-09-
12T13:29:03.678Z", "updatedAt": "2018-09-18T06:24:14.845Z", "title": "Unprotected port
on EC2 instance i-12b08fff is being probed.", "description": "EC2 instance has an
unprotected port which is being probed by a known malicious host."}},IngestionTime:
1537272809964,EventId: 342823292355025476113598039641754233996789294460148776966}
```

- "blocked":\s+([a-z]+)

-Compruebo los resultados arrojados.



REGULAR EXPRESSION

1 match (567 steps, 1.0ms)

```
/ "blocked":\s+([a-z]+) / gm
```

TEST STRING

```
{"portProbeDetails": [{"localPortDetails": {"port": 8080, "portName": "Unknown"}, "remoteIpDetails":
{"country": {"countryName": "Country4"}, "city": {"cityName": ""}, "geoLocation": {"lon": 0.0, "lat":
0.0}, "organization": {"asnOrg": "testAsnOrg5", "org": "testAsnOrg5", "isp": "testISP5", "asn":
"29073"}, "ipAddressV4": "192.168.207.50"}}, {"localPortDetails": {"port": 80, "portName": "HTTP"},
"remoteIpDetails": {"country": {"countryName": "Country4"}, "city": {"cityName": ""}, "geoLocation":
{"lon": 0.0, "lat": 0.0}, "organization": {"asnOrg": "testAsnOrg5", "org": "testAsnOrg5", "isp":
"testISP5", "asn": 29073}, "ipAddressV4": "192.168.181.249"}}], "blocked": false}}, "resourceRole":
"TARGET", "additionalInfo": {"threatName": "Scanner", "threatListName": "ProofPoint"},
"eventFirstSeen": "2018-09-12T13:15:43Z", "eventLastSeen": "2018-09-18T06:12:37Z", "archived": false,
"count": 21}, "severity": 2, "createdAt": "2018-09-12T13:29:03.678Z", "updatedAt":
"2018-09-18T06:24:14.845Z", "title": "Unprotected port on EC2 instance i-12b08fff is being probed.",
"description": "EC2 instance has an unprotected port which is being probed by a known malicious
host."}},IngestionTime: 1537272809964,EventId:
342823292355025476113598039641754233996789294460148776966}
```

LIST

success (0.0ms)

insert your replacement value here

EXPLANATION

- / "blocked":\s+([a-z]+) / gm
  - "blocked": matches the characters "blocked": literally (case sensitive)
  - \s matches any whitespace character (equivalent to [\r\n\t\f\v])
    + matches the previous token between one and unlimited times, as many times as possible, giving back as needed (greedy)
  - 1st Capturing Group ([a-z]+)
    - Match a single character present in the list below [a-z]
      + matches the previous token between one and unlimited times, as many times as possible, giving back as needed (greedy)
      a-z matches a single character in the range between a (index 97) and z (index 122) (case sensitive)

MATCH INFORMATION

```
Match 1   1858-1874   "blocked": false
Group 1   1869-1874   false
```

-Si observamos el JPSON , encontraremos también los resultados que nos pide el ejercicio.

```
[
  [
    {
      "content": "\"blocked\": false",
      "isParticipating": true,
      "groupNum": 0,
      "startPos": 1858,
      "endPos": 1874
    },
    {
      "content": "false",
      "isParticipating": true,
      "groupNum": 1,
      "startPos": 1869,
      "endPos": 1874
    }
  ]
]
```

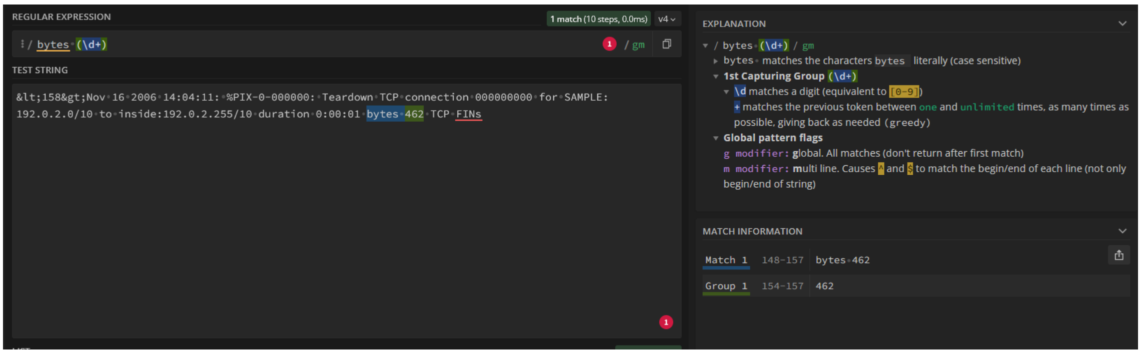
## Ejercicio 7

- Desarrollar la expresión regular que parsee del siguiente log el número de bytes de la conexión (campo bytes)

    - &lt;158&gt;Nov 16 2006 14:04:11: %PIX-0-000000: Teardown TCP connection 000000000 for SAMPLE:192.0.2.0/10 to inside:192.0.2.255/10 duration 0:00:01 bytes 462 TCP FINs

- bytes (\d+)

-Compruebo los resultados arrojados.



REGULAR EXPRESSION

1 match (10 steps, 0.0ms)

```
/ bytes (\d+) / gm
```

TEST STRING

```
&lt;158&gt;Nov 16 2006 14:04:11: %PIX-0-000000: Teardown TCP connection 000000000 for SAMPLE:
192.0.2.0/10 to inside:192.0.2.255/10 duration 0:00:01 bytes 462 TCP FINs
```

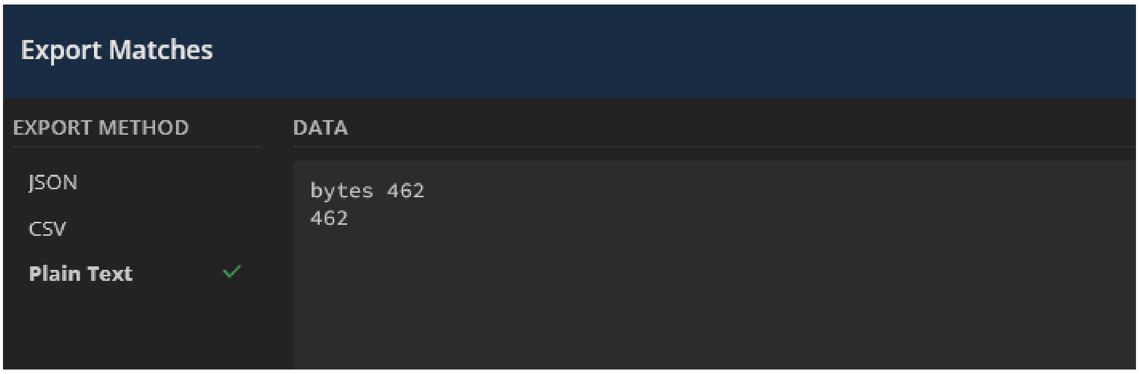
EXPLANATION

- / bytes (\d+) / gm
  - bytes matches the characters bytes literally (case sensitive)
  - 1st Capturing Group (\d+)
    - \d matches a digit (equivalent to [0-9])
    - + matches the previous token between one and unlimited times, as many times as possible, giving back as needed (greedy)
  - Global pattern flags
    - g modifier: global. All matches (don't return after first match)
    - m modifier: multi line. Causes ^ and $ to match the begin/end of each line (not only begin/end of string)

MATCH INFORMATION

Match 1	148-157	bytes 462
Group 1	154-157	462

En Match information, clickamos en la flecha para Exportar resultados .En este caso se observa el Texto Plano , y el numero de bytes de la conexión.



Export Matches

EXPORT METHOD: JSON, CSV, Plain Text ✓

DATA

```
bytes 462
462
```

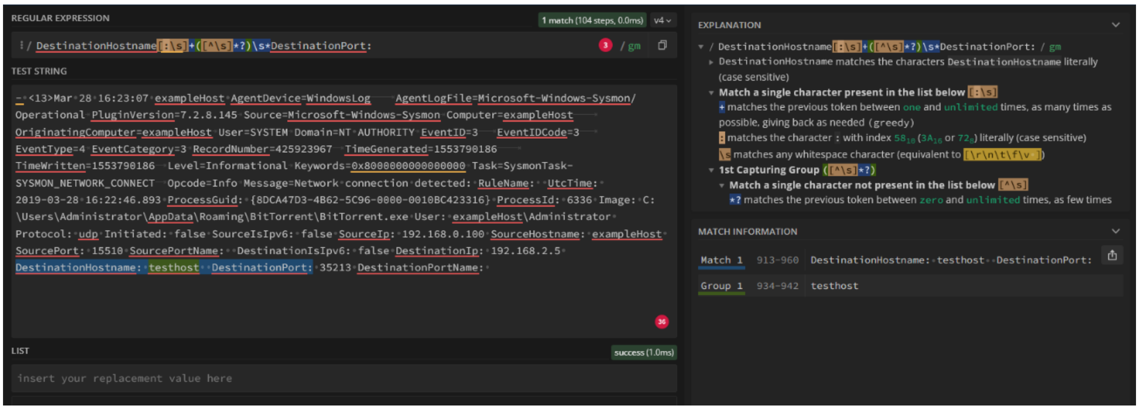
## Ejercicio 8

- Desarrollar la expresión regular que parsee del siguiente log el host de destino de la conexión (campo DestinationHostname)

```
    - <13>Mar 28 16:23:07 exampleHost AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational     PluginVersion=7.2.8.145        Source=Microsoft-Windows-Sysmon  Computer=exampleHost   OriginatingComputer=exampleHost        User=SYSTEM        Domain=NT AUTHORITY     EventID=3       EventIDCode=3   EventType=4        EventCategory=3 RecordNumber=425923967 TimeGenerated=1553790186        TimeWritten=1553790186 Level=Informational     Keywords=0x8000000000000000        Task=SysmonTask-SYSMON_NETWORK_CONNECT Opcode=Info     Message=Network connection detected: RuleName:  UtcTime: 2019-03-28 16:22:46.893 ProcessGuid: {8DCA47D3-4B62-5C96-0000-0010BC423316} ProcessId: 6336 Image: C:\Users\Administrator\AppData\Roaming\BitTorrent\BitTorrent.exe User: exampleHost\Administrator Protocol: udp Initiated: false SourceIsIpv6: false SourceIp: 192.168.0.100 SourceHostname: exampleHost SourcePort: 15510 SourcePortName: DestinationIsIpv6: false DestinationIp: 192.168.2.5 DestinationHostname: testhost DestinationPort: 35213 DestinationPortName:
```

- DestinationHostname[:\s]+([^\s]*?)\s*DestinationPort:

-Compruebo los resultados arrojados.



```
/ DestinationHostname[:\s]+([^\s]*?)\s*DestinationPort:
```

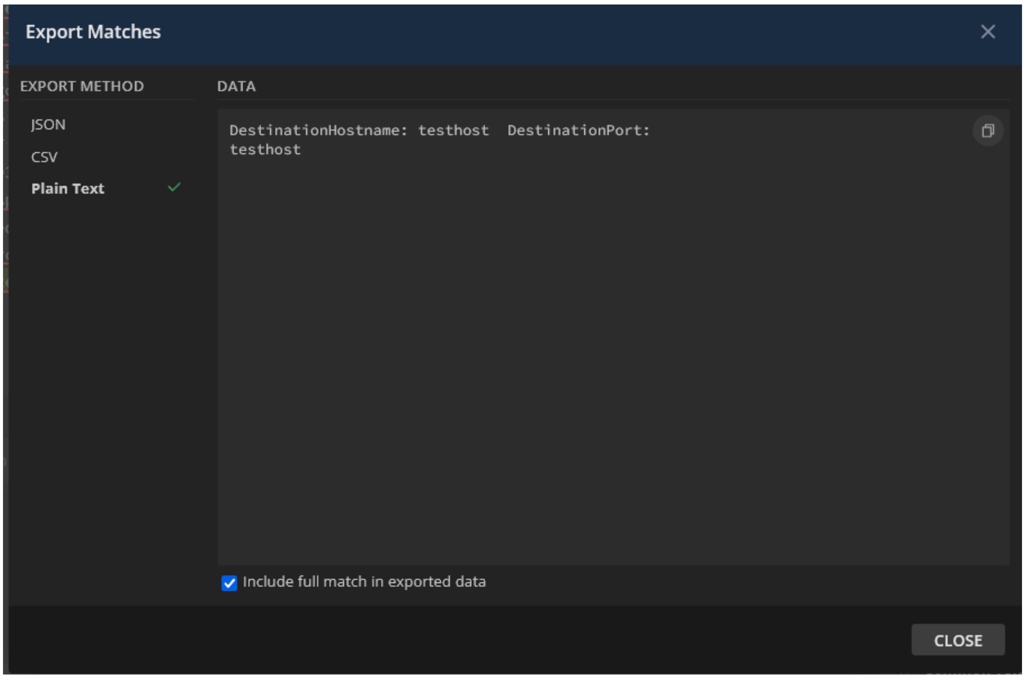
```
- <13>Mar 28 16:23:07 exampleHost AgentDevice=WindowsLog    AgentLogFile=Microsoft-Windows-Sysmon/
Operational PluginVersion=7.2.8.145 Source=Microsoft-Windows-Sysmon Computer=exampleHost
OriginatingComputer=exampleHost User=SYSTEM Domain=NT AUTHORITY EventID=3    EventIDCode=3
EventType=4 EventCategory=3 RecordNumber=425923967  TimeGenerated=1553790186
TimeWritten=1553790186  Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-
SYSMON_NETWORK_CONNECT  Opcode=Info Message=Network connection detected: RuleName:  UtcTime:
2019-03-28 16:22:46.893 ProcessGuid: {8DCA47D3-4B62-5C96-0000-0010BC423316} ProcessId: 6336 Image: C:
\Users\Administrator\AppData\Roaming\BitTorrent\BitTorrent.exe User: exampleHost\Administrator
Protocol: udp Initiated: false SourceIsIpv6: false SourceIp: 192.168.0.100 SourceHostname: exampleHost
SourcePort: 15510 SourcePortName:  DestinationIsIpv6: false DestinationIp: 192.168.2.5
DestinationHostname: testhost  DestinationPort: 35213 DestinationPortName:
```

insert your replacement value here

/ DestinationHostname[:\s]+([^\s]*?)\s*DestinationPort: / gm
- DestinationHostname matches the characters DestinationHostname literally (case sensitive)
- **Match a single character present in the list below** [:\s]
  - + matches the previous token between one and unlimited times, as many times as possible, giving back as needed (greedy)
  - : matches the character : with index 58_{10} ($3A_{16}$ or 72_8) literally (case sensitive)
  - \s matches any whitespace character (equivalent to [\r\n\t\f\v])
- **1st Capturing Group** ([^\s]*?)
  - **Match a single character not present in the list below** [^\s]
    - *? matches the previous token between zero and unlimited times, as few times

Match 1	913-960	DestinationHostname: testhost DestinationPort:
Group 1	934-942	testhost

En Match information, clickamos en la flecha para Exportar resultados .En este caso se observa el Texto Plano , y el host del destino de la conexión.



```
DestinationHostname: testhost  DestinationPort:
testhost
```

☑ Include full match in exported data

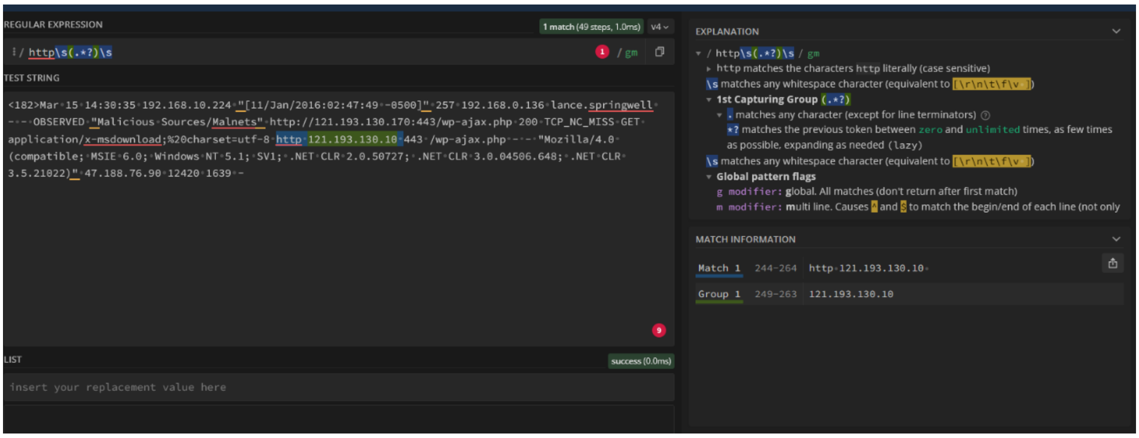
## Ejercicio 9

- Desarrollar la expresión regular que parsee del siguiente log la dirección IP 121.193.130.10

  - <182>Mar 15 14:30:35 192.168.10.224 "[11/Jan/2016:02:47:49 -0500]" 257 192.168.0.136 lance.springwell - - OBSERVED "Malicious Sources/Malnets" http://121.193.130.170:443/wp-ajax.php 200 TCP_NC_MISS GET application/x-msdownload;%20charset=utf-8 http 121.193.130.10 443 /wp-ajax.php - - "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)" 47.188.76.90 12420 1639 -

- http\s(.*?)\s

-Compruebo los resultados arrojados.



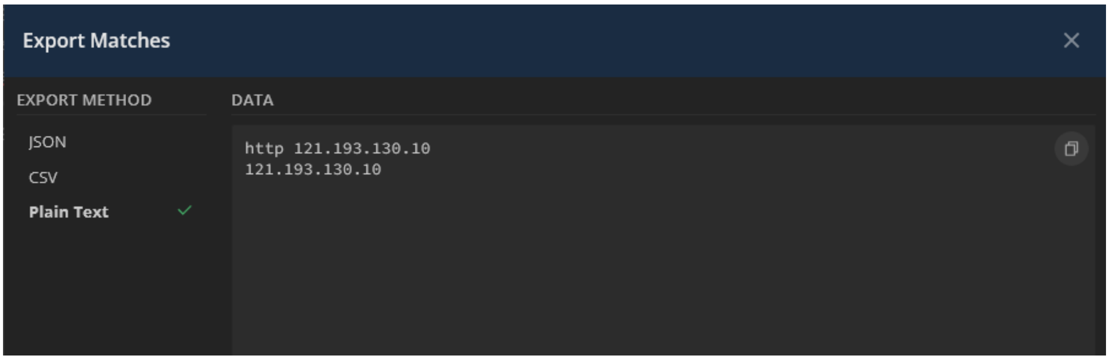
```
/ http\s(.*?)\s / gm
```

```
<182>Mar 15 14:30:35 192.168.10.224 "[11/Jan/2016:02:47:49 -0500]" 257 192.168.0.136 lance.springwell
- - OBSERVED "Malicious Sources/Malnets" http://121.193.130.170:443/wp-ajax.php 200 TCP_NC_MISS GET
application/x-msdownload;%20charset=utf-8 http 121.193.130.10 443 /wp-ajax.php - - "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR
3.5.21022)" 47.188.76.90 12420 1639 -
```

/ http\s(.*?)\s / gm
- http matches the characters http literally (case sensitive)
- \s matches any whitespace character (equivalent to [\r\n\t\f\v])
- 1st Capturing Group (.*?)
  - . matches any character (except for line terminators)
  - *? matches the previous token between zero and unlimited times, as few times as possible, expanding as needed (lazy)
- \s matches any whitespace character (equivalent to [\r\n\t\f\v])
- Global pattern flags
  - g modifier: global. All matches (don't return after first match)
  - m modifier: multi line. Causes ^ and $ to match the begin/end of each line (not only

```
Match 1   244-264   http 121.193.130.10
Group 1   249-263   121.193.130.10
```

-En Match information, clickamos en la flecha para Exportar resultados .En este caso se observa el Texto Plano , y la dirección I.P.



```
http 121.193.130.10
121.193.130.10
```